Citrix DaaS

Contents

Überblick

March 30, 2024

Einführung

Citrix DaaS ist ein Dienst, der Anwendungs- und Desktop-Virtualisierung bietet und der IT die Kontrolle über On-Premises- oder Cloud-gehostete virtuelle Maschinen, Anwendungen und Sicherheit gibt und gleichzeitig den Zugriff von jedem Gerät und von überall aus ermöglicht. Endbenutzer können Anwendungen und Desktops unabhängig vom Betriebssystem und von der Benutzeroberfläche eines Geräts verwenden.

Mit Citrix DaaS können Sie für jedes Gerät sichere virtuelle Apps und Desktops bereitstellen und die Installation, Einrichtung und Upgrades größtenteils Citrix überlassen. Sie behalten die vollständige Kontrolle über Anwendungen, Richtlinien und Benutzer und bieten auf jedem Gerät die beste Benutzererfahrung.

Mit Citrix DaaS können Sie Workloads aus dem On-Premises-Datencenter und der öffentlichen Cloud in einer Hybridbereitstellung gemeinsam verwalten. Sie können eine Verbindung mit Microsoft Azure, Amazon Web Services (AWS) und Google Cloud sowie Hypervisors wie XenServer, Microsoft Hyper-V, Nutanix AHV und VMware vSphere herstellen. Das Multicloud-Konzept ermöglicht die flexible Bereitstellung von Anwendungen an weltweit verteilten Ressourcenstandorten.

Citrix DaaS bietet mehrere Möglichkeiten zur Bereitstellung von Apps und Desktops.

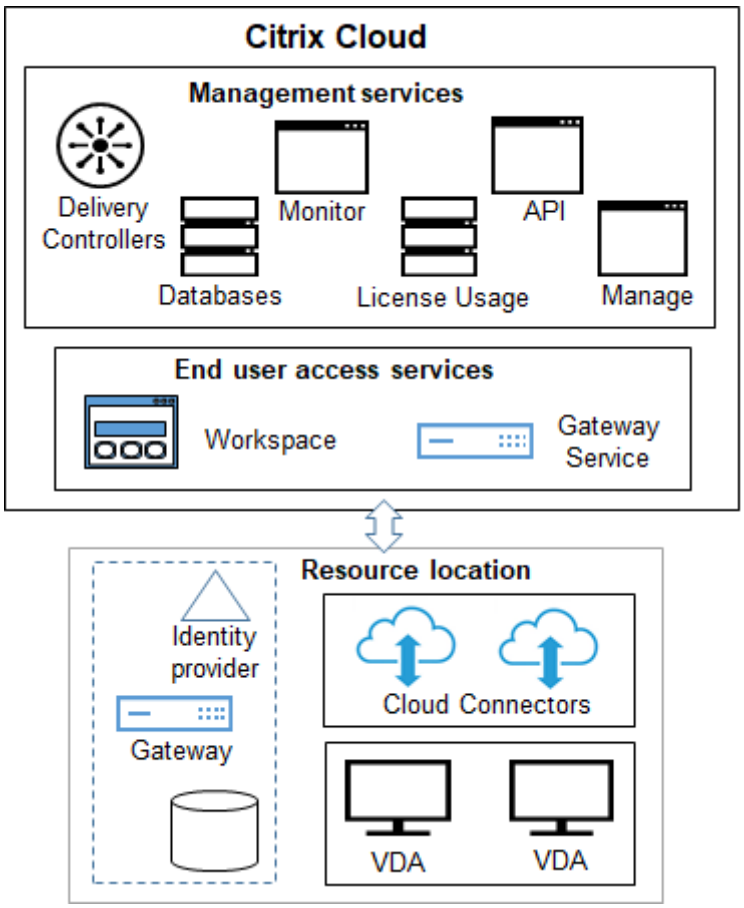
- Unter Bereitstellungsmethoden werden die primären Methoden einschließlich Anwendungsfällen, Vorteilen und Nachteilen erläutert.
- Der Artikel Bereitstellungsmodelle enthält eine Liste weiterer Möglichkeiten und einen VDI-Modellvergleich.

Citrix Managed Azure vereinfacht die Bereitstellung von virtuellen Apps und Desktops weiter. Citrix Managed Azure wird von Citrix auch für das Hosting von Azure-Workloads eingesetzt.

Informationen zu den Vorteilen des Service.

Siteüberblick

Die folgende Abbildung zeigt die Dienste und Komponenten, mit denen Citrix Administratoren in einer Citrix DaaS-Produktionsbereitstellung (= “Site”) arbeiten.



Wie die Abbildung zeigt, verwaltet Citrix die Dienste und Komponenten für Benutzerzugriff und -verwaltung in Citrix Cloud. Die den Benutzern bereitgestellten Anwendungen und Desktops sind auf Maschinen an einem oder mehreren Ressourcenstandorten. In Citrix DaaS-Bereitstellungen enthalten Ressourcenstandorte Komponenten aus dem Zugriffslayer und dem Ressourcenlayer: Jeder Ressourcenstandort wird als Zone betrachtet.

Wenn Sie kürzlich eine Migration von Citrix Virtual Apps and Desktops durchgeführt haben, werden Sie feststellen, dass Citrix DaaS die in einer On-Premises-Bereitstellung erforderliche Einrichtung von Komponenten größtenteils überflüssig macht.

Von Citrix verwaltete Komponenten und Dienste

- **Delivery Controller:** Citrix DaaS bietet Funktionen wie den Lastausgleich von Anwendungen und Desktops, die Authentifizierung von Benutzern und das Brokering oder Priorisieren von Verbindungen direkt aus der Cloud, ohne Verwaltung von Delivery Controllern, wie in Citrix Virtual Apps and Desktops.
- **Datenbanken:** Daten zur Sitekonfiguration, Überwachung und Konfigurationsprotokollierung werden vom Cloud-Dienst gespeichert, wodurch die SQL-Datenbankanforderung der

On-Premises-Version von Citrix Virtual Apps and Desktops entfällt.

- **Lizenzierung:** Verwaltet Lizenzen und stellt Nutzungsstatistiken bereit.
- **Managementschnittstellen:** Siehe Managementschnittstellen. Viele Aufgaben sind auch in Service-APIs verfügbar.
- **Überwachungskonsole:** Die Konsole Überwachen ermöglicht es Support- und Helpdesk-Teams die Umgebung zu überwachen, rechtzeitig potenzielle Probleme zu behandeln und Supportaufgaben für die Endbenutzer auszuführen. Es wird Folgendes angezeigt:
  - Echtzeit-Sitzungsdaten vom Brokerdienst auf dem Controller, einschließlich Daten vom Brokeragent auf dem Virtual Delivery Agent (VDA)
  - Historische Daten vom Überwachungsdienst auf dem Controller
  - Daten zum HDX-Verkehr (auch "ICA-Verkehr")
- **Cloud Connectors:** Ein Cloud Connector ist der Kommunikationskanal zwischen den Komponenten in der Citrix Cloud und den Komponenten am Ressourcenstandort. Am Ressourcenstandort fungiert der Cloud Connector als Proxy für den Delivery Controller in Citrix Cloud.

  Jeder Ressourcenstandort enthält mindestens einen Cloud Connector. Zwei oder mehr Cloud Connectors werden zu Redundanzzwecken empfohlen.

  - Wenn Sie die vollständige Konfiguration zum Maschinen-Provisioning verwenden, installieren Sie zuerst Cloud Connectors über die Citrix Cloud-Konsole. Einzelheiten finden Sie unter "Cloud Connectors".
  - Wenn Sie Azure-Maschinen mit Quick Deploy bereitstellen, erstellt Citrix den Ressourcenstandort und Cloud Connectors für Sie, wenn Sie den Katalog erstellen.

  Nach der Installation der Cloud Connectors werden diese von Citrix verwaltet und aktualisiert. Der Kunde muss sich lediglich um Windows-Updates und -Patches für den Cloud Connector kümmern.

Managementschnittstellen

Auf der Registerkarte **Verwalten** von Citrix DaaS können Sie die folgenden Schnittstellen auswählen.

Vollständige Konfiguration

Die Oberfläche **Verwalten > Vollständige Konfiguration** ermöglicht Folgendes:

- Anzeigen eines Überblicks über Ihre Citrix DaaS-Bereitstellung und die neuesten Features über die Homepage.

- Erstellen und Verwalten von Verbindungen mit Hosts.
- Erstellen und Verwalten von Katalogen für die Maschinen, welche die den Benutzern zur Verfügung gestellten Apps und Desktops enthalten.
- Erstellen und Verwalten von Bereitstellungsgruppen und (optional) Anwendungsgruppen.
- Erstellen und Verwalten von Citrix Richtlinien, die die Verwendung und das Verhalten von HDX-Technologien und -Features steuern sowie Verwaltung auf Siteebene. Dazu gehören Richtlinieneinstellungen für Sitzungen, adaptiven Transport, Geräte, Grafiken, Multimedia, Inhaltsumleitung und VDAs.
- Konfiguration des Features delegierte Administration, um rollenbasierte Administratoren zu erstellen, die über bestimmte Berechtigungsbereiche verfügen.
- Verwalten des Features Autoscale zur proaktiven Energieverwaltung von Maschinen, die Apps und Desktops bereitstellen.
- Lastausgleich bei Maschinen
- Systemintegritätsprüfungen auf den VDAs zur Diagnose und Behebung von Problemen.
- Anzeigen des Konfigurationsprotokolls zur Überprüfung des Zeitpunkts und Urhebers von Konfigurationsänderungen und anderen Verwaltungsaktivitäten.

Quick Deploy

Über die Oberfläche **Verwalten > Quick Deploy** können Sie Microsoft Azure-Workloads mit Citrix Managed Azure-Abonnement oder Ihrem eigenen Azure-Abonnement mühelos bereitstellen und verwalten. Weitere Informationen finden Sie unter Quick Deploy und Citrix Managed Azure. In Quick Deploy ist Folgendes möglich:

- Erstellen und Verwalten von Katalogen.
- Erstellen und Anpassen von Images auf der Grundlage von Images, die von Citrix vorbereitet wurden, oder solchen, die Sie aus Ihrem Azure-Abonnement importieren.

Weitere Informationen finden Sie unter Quick Deploy.

Umgebungsverwaltung

Über die **Umgebungsverwaltung** können Sie mithilfe der Technologien zur intelligenten Ressourcen- und Profilverwaltung die optimale Leistung sowie die bestmöglichen Desktopanmeldezeiten und Anwendungsreaktionszeiten erzielen. Weitere Informationen finden Sie unter Workspace Environment Management.

Vom Kunden verwaltete Komponenten und Technologien

- **Citrix Gateway:** Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in Citrix DaaS mit Citrix Gateway und TLS geschützt werden. Das Citrix Gateway bzw. das virtuelle VPX-Gerät ist ein SSL-VPN-Gerät, das in der DMZ bereitgestellt wird. Es bietet einen sicheren Einzelzugangspunkt durch die Unternehmensfirewall.

  Citrix installiert und verwaltet den Citrix Gateway Service in Citrix Cloud. Sie können Citrix Gateway optional auch an Ressourcenstandorten installieren.

- **Active Directory:** Active Directory wird für die Authentifizierung und Autorisierung verwendet. Es authentifiziert Benutzer und stellt sicher, dass sie Zugriff auf die richtigen Ressourcen erhalten. Die Identität der Abonnenten legt fest, auf welche Citrix Cloud-Services sie zugreifen können. Die Identität entstammt Active Directory-Domänenkonten, die über die Domänen im Ressourcenstandort bereitgestellt werden.

- **Identitätsanbieter (IdP):** Der IdP ist die letzte Instanz im Hinblick auf die Identität von Benutzern. Unterstützt werden folgende Identitätsanbieter: On-Premises-Active Directory, Active Directory plus Token, Azure Active Directory, Citrix Gateway und Okta. Weitere Informationen:

  - Workspace Identity
  - Identitäts- und Zugriffsverwaltung

- **Virtual Delivery Agents (VDAs):** Auf jeder physischen oder virtuellen Maschine, die Ressourcen (Anwendungen und Desktops) bereitstellt, muss ein Citrix VDA installiert sein. VDAs erstellen und verwalten die Verbindung zwischen der Maschine, auf denen sie installiert sind, und dem Benutzergerät und wenden die für die Sitzung konfigurierten Richtlinien an.

  Der VDA registriert sich unter Verwendung eines Cloud Connectors am Ressourcenstandort als Proxy bei einem Delivery Controller.

  Es stehen mehrere VDA-Typen zur Verfügung:

  - Mit VDAs für Multisitzungs-Windows-OS können mehrere Benutzer gleichzeitig eine Verbindung mit dem Server herstellen. Dieser VDA-Typ wird normalerweise auf Windows-Servern installiert.
  - Mit VDAs für Einzelsitzungs-Windows-OS kann jeweils ein Benutzer eine Verbindung zu einer Maschine herstellen. Dieser VDA-Typ wird normalerweise für VDI verwendet.

    Eine Kernversion dieses VDA-Typs ist für die Verwendung mit dem Feature Remote-PC-Zugriff verfügbar. Sie enthält eine Teilmenge der Features des vollständigen Einzelsitzungs-VDA.
  - Linux VDAs unterstützen virtuelle Apps und Desktops auf der Basis von RHEL, CentOS, SUSE und Ubuntu.

In der vorliegenden Dokumentation wird mit "VDA"sowohl der Agent als auch die Maschine, auf der dieser installiert ist, bezeichnet.

- **Hypervisors und Clouddienste:** In den meisten Produktionssites werden die App- und Desktop-Instanzen (Workloads), die Sie den Benutzern zur Verfügung stellen ("veröffentlichen"), von einem unterstützten Hypervisor oder Clouddienst gehostet. (Das Feature Remote-PC-Zugriff wird normalerweise für physische Maschinen verwendet. Daher nutzt es keine Hypervisors oder Clouddienste für die Maschinenbereitstellung.)

  - Wenn Sie die Oberfläche der vollständigen Konfiguration verwenden, erstellen Sie zunächst eine Verbindung zu einem unterstützten Host-Hypervisor oder Clouddienst. Verwenden Sie dann ein über diesen Host erstelltes Image, um in der vollständigen Konfiguration einen Katalog von Maschinen mit den App- und Desktop-Instanzen zu erstellen. Anschließend erstellen Sie eine Bereitstellungsgruppe. Citrix bietet viele Tools, die die Erstellung und Wartung solcher Sitzungshosts vereinfachen.
  - Wenn Sie Quick Deploy zur Bereitstellung von Azure-Workloads verwenden, müssen Sie nur den Katalog erstellen. Sie können zwar beim Erstellen des Katalogs Ihr eigenes Azure-Abonnement verwenden, die Verwendung eines Citrix Managed Azure-Abonnements macht aber auch die Verwaltung des Hosts überflüssig.

  Die von Ihnen veröffentlichten App- und Desktop-Instanzen können in On-Premises-Bereitstellungen, öffentlichen Clouds oder Hybridumgebungen gehostet werden.

- **Citrix StoreFront:** Citrix StoreFront ist der Vorgänger des cloudgehosteten Citrix Workspace. Es wird als Webinterface für den Zugriff auf Anwendungen und Desktops verwendet.

  Sie können StoreFront-Server optional in Ressourcenstandorten installieren. Lokale Stores können bei Netzwerkausfällen zur Bereitstellung von Apps und Desktops beitragen. Für das Feature Lokaler Hostcache ist an jedem Ressourcenstandort (jeder Zone) ein kundenverwaltetes StoreFront erforderlich.

  Informationen zur Verwendung von StoreFront in einer Service-Umgebung finden Sie unter Benutzerzugriff.

Von Ihnen konfigurierte Objekte für die Bereitstellung von Desktops und Anwendungen

Sie konfigurieren die folgenden Elemente für die Bereitstellung von Apps und Desktops in einer Produktionsumgebung.

- **Hostverbindung:** Eine Hostverbindung (siehe oben) unterstützt die Kommunikation zwischen Komponenten in der Steuerungsebene (Citrix Cloud) und den VDAs an einem Ressourcenstandort. Die Verbindungsspezifikationen umfassen:

  - Adresse und Anmeldeinformationen für den Zugriff auf den Host
  - Speichermethode und Maschinen für die Speicherung
  - Netzwerk zur Verwendung durch die VMs

  Hinweis: Wenn Sie Quick Deploy verwenden, müssen Sie keine Verbindung erstellen. Und wenn Sie Citrix Managed Azure verwenden, verwaltet Citrix auch das Hosting.

- **Katalog:** In den Oberflächen der vollständigen Konfiguration und der Überwachung werden Kataloge als "Maschinenkataloge"bezeichnet.
  Ein Katalog ist eine Sammlung von virtuellen oder physischen Maschinen, die den gleichen Betriebssystemtyp haben (z. B. Multisitzungs-Windows-OS oder Einzelsitzungs-Ubuntu)

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

  For more information about MCS, see Image management.

- **Bereitstellungsgruppe:** Über Bereitstellungsgruppen wird Folgendes spezifiziert:

  - Eine oder mehrere Maschinen aus einem Katalog
  - Benutzer, die auf Maschinen zugreifen dürfen.
  - Anwendungen und Desktops, auf die Benutzer über Workspace zugreifen können.

  Bei Verwendung von Quick Deploy wird automatisch eine Bereitstellungsgruppe erstellt. (Erscheint nur in der Oberfläche der vollständigen Konfiguration.)

- **Anwendungsgruppe:** Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden. Anwendungsgruppen sind optional.

Citrix Managed Azure

Citrix Managed Azure steht optional in mehreren Citrix DaaS-Editionen zur Verfügung. Citrix Managed Azure vereinfacht die Bereitstellung von virtuellen Apps und Desktops aus Azure. Citrix verwaltet die Infrastruktur für das Hosting von Azure-Workloads.

Mit Citrix Managed Azure erhalten Sie ein dediziertes von Citrix verwaltetes Azure-Abonnement und einen Ressourcenstandort. In dem Azure-Abonnement erstellen Sie einen Katalog mit VMs. Sie haben folgende Möglichkeiten:

- Bereitstellen von Einzelsitzungs- und Multisitzungs-Windows-OS-Maschinen oder Linux-OS-Maschinen aus diversen unterstützten Versionen
- Auswahl aus einer kuratierten Liste von Rechenarten und Speicheroptionen in ausgewählten Regionen
- Bereitstellen persistenter oder nicht persistenter Workloads auf den Maschinen
- Auswahl aus mehreren von Citrix bereitgestellten Images, auf denen der neueste VDA installiert ist Anschließend erstellen Sie über die Citrix Oberfläche Ihr eigenes Image aus dieser Vorlage und passen es an. Sie können Images auch aus Ihrem Azure-Abonnement importieren und verwenden.

Citrix verwaltet zwar Azure-Kapazität, doch können Sie zur Verbindung von Ressourcen Azure VNet-Peering verwenden, wenn Sie mit Ressourcen in Ihrem Azure-Abonnement kommunizieren möchten. Sie können auch eine direkte Verbindung mit On-Premises-Ressourcen über Citrix SD-WAN herstellen.

Informationen zu Sicherheit und Zuständigkeiten bei der Verwendung von Citrix Managed Azure finden Sie unter Technical security overview for Citrix Managed Azure.

Bestellung von Citrix Managed Azure

Für ein Citrix Managed Azure-Abonnement müssen Sie ein unterstütztes Citrix Serviceangebot abonnieren und dann Citrix Managed Azure Consumption Funds bestellen. Sie können Citrix DaaS und Consumption Funds über Citrix oder bei Azure Marketplace bestellen.
Citrix Managed Azure wird bei den folgenden Service-Angeboten unterstützt:

- Citrix Workspace Premium Plus
- Citrix DaaS-, Advanced-, Advanced Plus- und Premium-Editionen
- Citrix DaaS Standard für Azure Edition

Weitere Informationen finden Sie unter Sign up for Citrix DaaS.

Vorteile von Citrix Managed Azure

Die Verwendung von Citrix Managed Azure bietet mehrere Vorteile:

- Schnellster Weg zu den Vorzügen einer Hybrid-Cloud
- Auslagerung der IT-Infrastrukturverwaltung. Die IT hat die Kontrolle ohne die Herausforderungen rund um Verwaltung und Wartung bewältigen zu müssen.
- Schnelles Skalieren von Arbeitslösungen
- Separates, von Citrix verwaltetes und gepflegtes Azure-Abonnement. Bietet eine Trennung von anderen Azure-Abonnements.
- Flexible Erstellung und Verwaltung von Workloads mit eigenen Azure-Abonnements. Ihre Bereitstellung kann Workloads umfassen, die das Citrix Managed Azure-Abonnement verwenden und solche, die Ihre eigenen Azure-Abonnements verwenden.
- Verwendung eines verbrauchsbasierten IaaS-Modells.
- Mit verschiedenen Technologien können Verbindungen zu Ihren On-Premises-Netzwerken hergestellt werden (etwa Azure VNet-Peering und SD-WAN). Auf diese Weise können die Benutzer auf die Ressourcen Ihres Netzwerks wie Dateiserver zugreifen.

Zum Bereitstellen und Verwalten von Citrix Managed Azure von diesem Dienst aus wird die Managementschnittstelle Quick Deploy verwendet.

Weitere Informationen erhalten Sie von Ihrem Citrix Vertreter.

Bereitstellen von Anwendungen und Desktops für die Benutzer

Citrix Workspace

Abonnenten (Benutzer) greifen über Citrix Workspace auf ihre Desktops und Anwendungen zu.

Nach der Installation und Konfiguration von Citrix DaaS erhalten Sie einen URL-Link für den Workspace. Die Workspace-URL wird an zwei Stellen angezeigt:

- Klicken Sie in der Citrix Cloud-Konsole im Menü links oben auf **Workspacekonfiguration**. Die Registerkarte **Zugriff** enthält die Workspace-URL.
- Auf dem **Begrüßungsbildschirm** von Citrix DaaS wird am unteren Seitenrand die Workspace-URL angezeigt.

Testen Sie den Link für die Workspace-URL und geben Sie ihn dann für Ihre Abonnenten (Benutzer) frei, damit diese Zugriff auf ihre Apps und Desktops erhalten. Ihre Abonnenten können ohne zusätzliche Konfiguration auf die Workspace-URL zugreifen.

Workspaces konfigurieren Sie in Citrix Cloud.

- Angeben, welche Services mit Citrix Workspace integriert sind.

- Die URL anpassen, die Ihre Abonnenten für den Zugriff auf ihren Workspace verwenden.
- Das Erscheinungsbild der Workspaces der Abonnenten anpassen, z. B. Logos, Farben und Voreinstellungen.
- Angeben, wie sich Abonnenten für bei dem Workspace authentifizieren, z. B. mit Active Directory oder Azure Active Directory.
- Angeben, welche externe Konnektivität für Ressourcenstandorte von Ihren Abonnenten verwendet wird.

Weitere Informationen finden Sie unter Citrix Workspace.

Citrix Workspace-App

Benutzerseitig wird die Citrix Workspace-App auf Benutzergeräten, virtuellen Desktops und ähnlichen Endpunkten installiert. Die Citrix Workspace-App bietet Benutzern schnellen und sicheren Self-Service-Zugriff auf Dokumente, Anwendungen und Desktops über jedes beliebige Gerät (Smartphone, Tablet, PC usw.). Citrix Workspace-App bietet bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen.

Bei Geräten, auf denen die Citrix Workspace-App-Software nicht installiert werden kann, ermöglicht die Citrix Workspace-App für HTML5 eine Verbindung über einen HTML5-kompatiblen Webbrowser.

Die Citrix Workspace-App ist für verschiedene Betriebssysteme verfügbar. Einzelheiten finden Sie unter Citrix Workspace-App.

Servicelevelziele

Citrix DaaS basiert auf bewährten Methoden der Branche, um eine Cloudskalierung und einen hohen Grad an Serviceverfügbarkeit zu erreichen.

Ausführliche Informationen zur Verpflichtung von Citrix bezüglich Verfügbarkeit von Citrix Cloud-Diensten finden Sie unter Servicelevelziele.

Die Erfüllung dieses Ziels kann laufend unter https://status.cloud.com überwacht werden.

Einschränkungen

Die Kalkulation des Servicelevelziels schließt den Verlust der Verfügbarkeit unter folgenden Bedingungen aus:

- Die in der Produktdokumentation unter https://docs.citrix.com angegebenen Konfigurationsanforderungen von Citrix DaaS wurden vom Kunden nicht erfüllt.

- Der Ausfall wurde durch eine nicht von Citrix verwaltete Komponente verursacht, einschließlich, aber nicht beschränkt auf vom Kunden gesteuerte physische und virtuelle Maschinen, vom Kunden installierte und gepflegte Betriebssysteme, vom Kunden installierte und gesteuerte Netzwerkgeräte oder andere Hardware, vom Kunden definierte und gesteuerte Sicherheitseinstellungen, Gruppenrichtlinien und andere Konfigurationsrichtlinien, mit dem Anbieter der öffentlichen Cloud oder dem Internetdienstanbieter zusammenhängende Störungen sowie andere Ausfälle und Störungen, die sich der Kontrolle von Citrix entziehen.
- Serviceunterbrechungen, deren Ursachen sich der Kontrolle von Citrix entziehen, z. B. Naturkatastrophen, Kriege, Terrorakte oder Handlungen von Behörden/Regierungsorganen.

Weitere Informationen

- Diagramme für Citrix DaaS
- Referenzarchitektur und Bereitstellungsmethoden für Citrix DaaS
- Technische Sicherheit
- Netzwerkports
- Hinweise zu Drittanbietern
- Systemanforderungen
- Features
  - Eine Einführung in HDX-Technologien sowie Details zu Geräten, Grafiken und Multimedia.
  - Remote-PC-Zugriff: Ermöglicht, dass Endbenutzer sich remote von jedem Standort aus an einem physischen Windows-PC im Büro anmelden. Sie können Remote-PC-Zugriff über die vollständige Konfiguration oder Quick Deploy konfigurieren.
  - Inhalt veröffentlichen: Veröffentlichen Sie eine Anwendung, bei der es sich einfach um einen URL- oder UNC-Pfad zu einer Ressource handelt.
  - Server-VDI: Stellen Sie einen Desktop von einem Serverbetriebssystem für einen einzelnen Benutzer bereit.
- Informationen zu Citrix DaaS Standard für Azure finden Sie in der zugehörigen Produktdokumentation.
- Weitere Informationen zur Verfügbarkeit von Features in Citrix DaaS-Produkten und Editionen finden Sie in der Featurematrix für Citrix DaaS.
- Citrix Cloud Learning Series bietet Schulungen zu Citrix Cloud und den zugehörigen Services. Sie können alle Module, von der Einführung bis zu Planung und Aufbau nacheinander durcharbeiten. Alternativ können Sie einzelne Module oder aufgabenspezifische Teile von Modulen nutzen. Siehe Cloud Learning Series.

Erste Schritte

Informationen zum Einrichten Ihrer Bereitstellung finden Sie unter Planen und Erstellen einer Bereitstellung. Diese Zusammenfassung führt Sie durch die wichtigsten Schritte des Prozesses und bietet Links zu weiteren Informationen und detaillierten Anleitungen.

Was ist neu

June 13, 2024

Das Ziel von Citrix ist es, Citrix DaaS-Kunden Neue Features und Produktupdates unverzüglich zur Verfügung zu stellen. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern. Regelmäßige Updates für Citrix DaaS werden ca. alle drei Wochen veröffentlicht.

Der Prozess ist für Sie transparent. Erste Updates werden nur auf interne Sites von Citrix angewendet und erst danach schrittweise auf Kundenumgebungen. Durch diese schrittweise Bereitstellung von Updates wird die Produktqualität sichergestellt und die Verfügbarkeit maximiert.

Informationen zum Servicelevelziel für die Cloudskalierung und Serviceverfügbarkeit finden Sie unter Servicelevelziele. Informationen zu Serviceunterbrechungen und geplanten Wartungsmaßnahmen finden Sie im Dienstzustandsdashboard.

Virtual Delivery Agents (VDAs)

Releases für VDAs für Windows-Maschinen werden in der Regel zur gleichen Zeit wie Citrix Virtual Apps and Desktops veröffentlicht.

- Informationen zu neuen VDA- und HDX-Features finden Sie in den Artikeln Neue Features und Bekannte Probleme für das aktuelle Release von Citrix Virtual Apps and Desktops.
- Informationen zu nicht mehr unterstützten VDA-Plattformen und -Features finden Sie unter Einstellung von Features und Plattformen. Dieser Artikel umfasst auch Plattformen und Features, die in zukünftigen Versionen nicht mehr unterstützt werden (z. B. Betriebssysteme für die VDA-Installation).

> **Wichtig:**
>
> Wurde die PvD-Komponente (persönliche vDisk) jemals auf einem VDA installiert, kann dieser nicht auf Version 1912 LTSR oder höher aktualisiert werden. Um den neuen VDA zu verwenden, müssen Sie den bestehenden VDA deinstallieren und dann den neuen VDA installieren. (Dies

> ist auch dann erforderlich, wenn Sie PvD zwar installiert, aber nie verwendet haben.) Weitere Informationen finden Sie unter Bei Installation einer persönlichen vDisk auf dem VDA.

Juni 2024

Neue und erweiterte Features

Unterstützung für die Erstellung von Ressourcengruppen während der Azure-Katalogerstellung (für PVS). Bisher mussten Sie beim Erstellen von Azure-Katalogen mit der vollständigen Konfiguration die Ressourcengruppen mit PowerShell-Befehlen erstellen. Mit diesem Feature können Sie jetzt im Rahmen der Katalogerstellung in Web Studio nahtlos eine Ressourcengruppe erstellen. Diese Erweiterung vereinfacht den gesamten Workflow bei der Erstellung. Weitere Informationen finden Sie unter Citrix Provisioning-Katalog mit der Schnittstelle zur vollständigen Konfiguration erstellen.

Mai 2024

Neue und erweiterte Features

Secure HDX (Preview). Sie können dieses Feature jetzt verwenden, um zu verhindern, dass Netzwerkelemente im Datenverkehrspfad den HDX-Verkehr überprüfen können. Weitere Informationen finden Sie unter Secure HDX.

Unterstützung für den Azure-GPU-Ruhezustand (Preview). Sie haben jetzt die Möglichkeit, den Ruhezustand für Azure-Maschinen-SKUs zu unterstützen, die GPU unterstützen.
Weitere Informationen zu den unterstützten VM-Größen finden Sie in der Microsoft-Dokumentation.

Die Unterstützung von Citrix Provisioning-Katalogen für hybride Azure AD-Joins wurde auf "Vollständige Konfiguration"erweitert. Wenn Sie einen Citrix Provisioning-Katalog erstellen, ist der **Azure Active Directory-Hybrideinbindung**-Identitätstyp jetzt auf der Seite **Maschinenkatalogerstellung > Maschinenidentitäten** verfügbar. Mit dieser neuen Option können Sie hybride, mit Azure AD verbundene Maschinen über Citrix Provisioning erstellen. Weitere Informationen finden Sie unter Citrix Provisioning-Architektur.

Verbesserungen der Kontexthilfe zur vollständigen Konfiguration. Wir haben das Hilfefenster neu gestaltet, um es informativer zu machen. Es bietet gezielte Informationen für jeden Knoten in der vollständigen Konfiguration. Wenn Sie auf einem beliebigen Knoten auf das Hilfesymbol klicken, können Sie jetzt auf eine umfassende Sammlung von Ressourcen zugreifen, die Ihnen eine zentrale Lernerfahrung bieten und Ihnen helfen, verwandte Features besser zu verstehen:

- Greifen Sie auf wichtige Dokumente zu, die sich speziell auf den ausgewählten Knoten beziehen.
- Bleiben Sie über Serviceupdates wie Citrix Roadmap, Bekannte Probleme, Grenzwerte, Systemanforderungen und neue Funktionen auf dem Laufenden.

- Greifen Sie auf erweiterte Ressourcen wie Citrix Blogs, Citrix Community, Citrix Feature Explained, Citrix Produktdokumentation, Citrix Support und Entwicklerdokumentation zu.

Verbesserte Konfigurationsprotokollierung: Nachverfolgen von Mitgliedschaftsänderungen für Bereitstellungsgruppen. Mit dieser Erweiterung erfasst und zeigt die Konfigurationsprotokollierung jetzt Benutzer- und Gruppen-IDs an, die zu Bereitstellungsgruppen hinzugefügt oder aus Bereitstellungsgruppen entfernt wurden. Um Konfigurationsprotokolle anzuzeigen, gehen Sie zu **Vollständige Konfiguration > Protokollierung > Ereignisse**.

Reihenfolge der Registerkarten im Knoten Suchen anpassen. Sie können jetzt die Reihenfolge der Registerkarten im **Suchknoten** an Ihre Nutzungsmuster anpassen und so das Surferlebnis verbessern. Klicken Sie dazu auf das Dreipunktsymbol neben den Tabs, ziehen Sie die Tabs in die gewünschte Reihenfolge und klicken Sie dann auf **Anwenden**.

Zwischenspeichern von Daten für den Knoten Maschinenkataloge. Wir haben das Datencaching für den Citrix DaaS-Knoten **Maschinenkataloge** eingeführt. Diese Erweiterung reduziert die Seitenladezeiten erheblich, wenn Sie zum Knoten **Maschinenkataloge** navigieren, und verbessert so die allgemeine Benutzererfahrung.

Unterstützung für die Erstellung von Citrix Provisioning-Katalogen mit MCS PowerShell-Befehlen in VMware. Sie können jetzt Citrix Provisioning-Kataloge mit MCS PowerShell-Befehlen in VMware erstellen.

Diese Implementierung bietet Ihnen die folgenden Vorteile:

- Eine einzige, einheitliche Konsole zur Verwaltung von MCS- und Citrix Provisioning-Katalogen.
- Neue Features für Citrix Provisioning-Kataloge, wie eine Identitätsverwaltungslösung, On-Demand-Provisioning und so weiter.

Weitere Informationen finden Sie unter Citrix Provisioning-Kataloge in Citrix Studio erstellen.

Fehlererkennung und -behebung im VDA Upgrade Service während des VDA-Upgrade-Vorgangs (Preview). Unser Service beinhaltet jetzt fortschrittliche Erkennungsmechanismen. Wenn Probleme festgestellt werden, die möglicherweise zum Ausfall der VDA-IPU führen und den VDA unbrauchbar machen könnten, ergreift der Dienst proaktive Maßnahmen. Die Aktualisierung zusätzlicher Computer wird eingestellt und der aktuelle Arbeitsablauf wird ordnungsgemäß beendet. Dieser proaktive Ansatz zielt darauf ab, die Auswirkungen zu minimieren und ein reibungsloses Erlebnis zu gewährleisten, auch im Falle unerwarteter Herausforderungen, wodurch der potenzielle Wirkungsradius aller aufgetretenen Probleme verringert wird. Weitere Informationen finden Sie unter Fehlererkennung und -behebung im VDA Upgrade Service

Unterstützung von VDA-Updates von einer lokalen Dateifreigabe, auf die VDAs zugreifen können (Preview). Mit Enhanced VDA Installer Access Control haben Sie jetzt mehr Flexibilität und Kontrolle darüber, welche VDAs eine Verbindung herstellen und die erforderlichen Download-MSIs abrufen können, ohne sich Gedanken darüber machen zu müssen, VDAs Netzwerkzugriff zu

gewähren, um Updates vom Citrix Managed Azure CDN abzurufen. Auf diese Weise können Sie strengere Netzwerkregeln durchsetzen und gleichzeitig einen nahtlosen Zugriff auf wichtige Updates sicherstellen. Weitere Informationen finden Sie unter Unterstützung von VDA-Updates von einer lokalen Dateifreigabe aus, auf die VDAs zugreifen können

Vollständige Konfigurationsunterstützung für die Bereitstellung von Anwendungspaketen auf statischen Desktops und Büro-PCs mit einer Sitzung. Dank dieser Erweiterung können Sie jetzt mit der vollständigen Konfiguration Anwendungspakete für alle Arten von Desktops bereitstellen. Zu den Vorteilen der Bereitstellung von Anwendungspaketen *auf statischen Desktops mit einer Sitzung* gehören:

- Anwendungen sind bei der Anmeldung auf dem VDA verfügbar und werden nicht bei Bedarf über Workspace oder StoreFront bereitgestellt.
- Startzeit ist beim Zugriff auf die Anwendungspakete verkürzt.
- Die unabhängige Wartung der Anwendungspakete wird getrennt vom Basisimage des VDA erleichtert.

Um Anwendungspakete auf Desktops bereitzustellen, fügen Sie diese Anwendungen auf folgende Weise zu den Bereitstellungsgruppen hinzu:

- Fügen Sie Anwendungen bei der Erstellung der Bereitstellungsgruppe hinzu.
- Fügen Sie Anwendungen mithilfe eines der folgenden Einträge zu einer vorhandenen Bereitstellungsgruppe hinzu: **Bereitstellungsgruppen > Anwendungen hinzufügen > Anwendungen**, **Anwendungen > Eigenschaften > Gruppen** oder **App-Pakete > Pakete > Bereitstellungsgruppen hinzufügen**.

Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen, Bereitstellungsgruppen verwalten und Anwendungen zu Bereitstellungsgruppen hinzufügen.

Vollständige Konfigurationsunterstützung für die Bereitstellung von Anwendungspaketen im FlexApp-Format. Unter **Vollständige Konfiguration > App-Pakete** können Sie jetzt FlexApp-Paketanwendungen in Citrix Cloud hochladen und sie Ihren Benutzern bereitstellen. Weitere Informationen finden Sie unter App-Pakete.

OData-Paginierung. Überwachung erhöht das Limit der OData-Paginierung. Alle OData v4-Endpunkte geben maximal 1000 Datensätze pro Seite mit einem Link zu den nächsten 1000 Datensätzen in der Antwort zurück. Da jede Seite große Datensätze zurückgibt, können Sie mit weniger OData-Abfragen dieselbe Gesamtdatenmenge abrufen. Somit reduziert dieses Feature die Zeit zum Abrufen der Gesamtdaten und verbessert daher die Benutzererfahrung. Weitere Informationen finden Sie in der Dokumentation zu Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Unterstützung für die Erstellung und Verwaltung vertraulicher Azure-VMs mithilfe der vollständigen Konfiguration. Vertrauliche Azure-VMs bieten eine starke, hardwaregestützte Grenze, um

Ihre Sicherheitsanforderungen zu erfüllen. Mit der Benutzeroberfläche für die vollständige Konfiguration können Sie jetzt vertrauliche VMs in Azure erstellen und verwalten. Weitere Informationen finden Sie unter Vertrauliche Azure-VMs (Preview).

Unterstützung für die Anzeige von Client-IPs in Konfigurationsprotokollen. Unter **Vollständige Konfiguration > Protokollierung > Ereignisse**können Sie jetzt IP-Adressdetails in Protokollen anzeigen, was die Verfolgung der Aktionsursprünge erleichtert. Um die IP-Adressspalte in der Hauptansicht anzuzeigen, klicken Sie oben rechts in den Protokollen auf das Symbol **Anzuzeigende Spalten** und wählen Sie dann **Client-IP** aus. Weitere Informationen finden Sie unter Inhalt des Konfigurationsprotokolls anzeigen.

Unterstützung für die Erfassung zusätzlicher Eigenschaften mithilfe der Maschinenprofilquelle in AWS. In AWS-Umgebungen können Sie mit dieser Erweiterung jetzt einen maschinenprofilbasierten Katalog erstellen oder aktualisieren, um Folgendes einzuschließen:

- Aufzeichnung von CPU-Optionen, Tenancy-Typ und Ruhezustandsfähigkeit aus der Maschinenprofilquelle, während Sie einen MCS-Maschinenkatalog erstellen.
- Den Tenancy-Typ der Maschinenprofilquelle ändern, während Sie einen MCS-Maschinenkatalog bearbeiten. Diese Funktion gilt nur für die neuen VMs, die dem Katalog hinzugefügt wurden.
- Ändern Sie die Ruhezustandsfunktion der Maschinenprofilquelle, während Sie einen MCS-Maschinenkatalog bearbeiten. Diese Funktion gilt nur für die neuen VMs, die dem Katalog hinzugefügt wurden.

Die Maschinenprofilquelle kann eine VM- oder Startvorlagenversion sein. Diese Funktion gilt sowohl für persistente als auch für nicht persistente Kataloge.

Weitere Informationen finden Sie unter Erstellen Sie einen auf Maschinenprofilen basierenden Maschinenkatalog mit PowerShell.

Identitätsinformationen aktiver Computerkonten in AWS reparieren. In AWS-Umgebungen können Sie jetzt die Identitätsinformationen von aktiven Computerkonten mit Identitätsproblemen zurücksetzen. Sie können wählen, ob Sie nur das Maschinenkennwort und die vertrauenswürdigen Schlüssel-IDs oder die gesamte Konfiguration des Identitätsdatenträgers zurücksetzen möchten. Diese Implementierung gilt für persistente und nicht persistente MCS-Maschinenkataloge. Derzeit wird das Feature nur für AWS-, Azure- und VMware-Virtualisierungsumgebungen unterstützt. Weitere Informationen finden Sie unter Identitätsinformationen aktiver Computerkonten reparieren.

Unterstützung für die Verschlüsselung des ID-Datenträgers einer MCS-Maschinenkatalog-VM in AWS. Bisher erlaubte MCS in AWS-Umgebungen nur die Verschlüsselung des Betriebssystemdatenträgers der bereitgestellten VMs. Mit dieser Funktion können Sie jetzt zusätzlich zum Betriebssystemdatenträger auch den ID-Datenträger verschlüsseln. Mit dieser Funktion können Sie AWS-KMS-Schlüssel (vom Kunden verwalteter Schlüssel und AWS-verwalteter Schlüssel) verwenden, um kryptografische Operationen auf den an eine VM angeschlossenen Datenträgern durchzuführen.

Für die Verschlüsselung von Betriebssystem- und ID-Datenträgern konfigurieren Sie eine der folgenden Optionen:

- Verwenden Sie ein verschlüsseltes Masterimage (z. B. ein AMI, das aus einer Instanz oder einem Snapshot erstellt wurde und ein mit einem KMS-Schlüssel verschlüsseltes Root-Volume enthält)
- Verwenden Sie eine Maschinenprofilquelle (VM oder Startvorlage), die ein verschlüsseltes Root-Volume enthält.

Weitere Informationen finden Sie unter Betriebssystem- und ID-Datenträger verschlüsseln.

Konfigurieren Sie Sicherheitsgruppen pro Netzwerkschnittstelle in AWS. Wenn Sie eine Hostverbindung für AWS-Umgebungen bearbeiten, können Sie jetzt mithilfe eines PowerShell-Befehls die maximal zulässige Anzahl von Sicherheitsgruppen pro Elastic Network Interface (ENI) konfigurieren. Wenn Sie das Kontingent Ihrer Sicherheitsgruppen pro Netzwerkschnittstelle erhöhen, können Sie daher denselben Wert für die Hosting-Verbindung konfigurieren. Informationen zur Konfiguration finden Sie unter Sicherheitsgruppen pro Netzwerkschnittstelle konfigurieren.

Kostenoptimierung [Preview]. Die Seite **Kostenoptimierung** bietet eine visuelle Darstellung der Infrastruktureinsparungen, die in einem ausgewählten Zeitraum angefallen sind, und prognostiziert die erwarteten Einsparungen für die verbleibenden Tage. Durch die Analyse der Maschinennutzung und der Sitzungen hilft Ihnen diese Seite dabei, erzielte Einsparungen und Möglichkeiten zur Kostensenkung zu identifizieren. Diese Seite bietet:

- Einblicke in die Optimierung von Infrastrukturkosten
- Der eingesparte Betrag
- Informationen zu einer Reihe von Szenarien, die zu einer Überschreitung der prognostizierten Kosten führen könnten
- Möglichkeiten zur Identifizierung und strategischen Planung zur Realisierung von Einsparungen bei Infrastrukturkosten

Die Seite **Kostenoptimierung** enthält **geschätzte Einsparungen** und den **Autoscale-Sparbericht**.

Die **geschätzten Einsparungen** helfen bei der Bewertung der effizienten Nutzung der Infrastrukturressourcen. Die Kosteneinsparungen werden entweder in US-Dollar oder als Prozentsatz der angefallenen Kosten angezeigt. Sie können die Ergebnisse der letzten 3, 6 und 12 Monate anzeigen. Das Diagramm **Geschätzte Einsparungen** enthält folgende Informationen:

- Geschätzte Einsparungen: Zeigt die Höhe der Einsparungen an, die in der Infrastruktur für den ausgewählten Zeitraum erzielt wurden.
- Maschinen mit Energieverwaltung: Zeigt die Gesamtzahl der Maschinen mit Energieverwaltung an.
- Voraussichtliche Einsparungen: Zeigt an, wie viele Infrastruktureinsparungen für die verbleibende Dauer erzielt werden können.

Der **Autoscale-Sparbericht** zeigt Informationen über die Bereitstellungsgruppe an, für die Autoscale konfiguriert und aktiviert ist. Dieser Bericht gilt nur für Maschinen mit Energieverwaltung. Weitere Informationen finden Sie auf der Seite Kostenoptimierung.

Maschinen mit kürzlich erfolgten Energieaktionen überprüfen. Sie können jetzt Maschinen mit erfolgreichen und fehlgeschlagenen Energieaktionen überprüfen. Mit diesem Feature können Sie Folgendes analysieren:

- Stromausfall, der Benutzerprobleme verursacht
- Fehler beim Abschalten, der die Kosten erhöht

> **Hinweis:**
>
> Daten sind nur für eine energieverwaltete Maschine verfügbar. Daten über Energieaktionen, die vor der Unterstützung des Features durchgeführt wurden, sind nicht verfügbar.

Sie können den Status der Energieaktionen auf Maschinen wie folgt anzeigen:

- Über die Registerkarte **Filter** -> **Maschinen**. In diesem Fall sind standardmäßig die Spalten **Power Action Time** und **Power Action Result** sichtbar. Sie können auswählen, welche Spalten sichtbar sein sollen.
- Auf der Registerkarte **Kostenoptimierung**. In diesem Fall ist der Standardfilter **Power Action Triggered by** auf *Autoscale* und das **Power Action Result** auf *Failed* gesetzt.

Mit diesem Feature können Sie die Details der Energieaktionsbefehle anzeigen. Sie können beispielsweise sehen, wer die Aktion ausgelöst hat, welche Aktion den Energiezustand geändert hat, den Grund für den Ausfall und den Zeitpunkt, zu dem die Aktion abgeschlossen ist. Sie können diese Details auch exportieren.

Weitere Informationen finden Sie unter Maschinen mit kürzlich erfolgten Energieaktionen überprüfen.

April 2024

Neue und erweiterte Features

Unterstützung für die neuere Version von Microsoft Teams. Citrix Monitor unterstützt jetzt Microsoft Teams Version 2.1 oder früher.

Datenträgerverschlüsselung in Azure ändern. Mit dieser Funktion können Sie jetzt die Datenträgerverschlüsselung in Azure-Virtualisierungsumgebungen ändern. Sie können die folgenden Aktionen ausführen:

- Erstellen Sie einen MCS-Maschinenkatalog mit einem Datenträgerverschlüsselungssatz (DES), der sich vom Masterimage-DES unterscheidet.

- Ändern Sie den Datenträgerverschlüsselungstyp von einem DES-Schlüssel zu einem anderen DES-Schlüssel eines vorhandenen MCS-Maschinenkatalogs und vorhandener VMs.
- Aktualisieren Sie einen MCS-Maschinenkatalog und eine VM, für die zuvor nicht CMEK aktiviert war, für Verschlüsselung (DES) mit einem vom Kunden verwalteten Verschlüsselungsschlüssel (CMEK), Datenträgerverschlüsselung auf dem Host oder doppelter Verschlüsselung.
- Aktualisieren Sie einen vorhandenen MCS-Maschinenkatalog und eine VM, die zuvor verschlüsselt waren, sodass sie unverschlüsselt sind.
- Aktivieren Sie die Datenträgerverschlüsselung mit privatem Endpunkt (einem MCS-Maschinenkatalog, der eine mit `ProxyHypervisorTrafficThroughConnector` aktivierte Hostverbindung verwendet hat).

Weitere Informationen finden Sie unter Datenträgerverschlüsselung ändern.

Unterstützung für das Ändern der Auslagerungsdateieinstellungen. Mit dieser Funktion können Sie die Auslagerungsdateieinstellungen der neu zu einem vorhandenen Katalog hinzugefügten VMs ändern, ohne das Masterimage zu aktualisieren. Dieses Feature gilt derzeit nur für Azure-Umgebungen.

Zum Ändern der Auslagerungsdateieinstellungen benötigen Sie VDA-Version 2311 oder höher. Sie können die Auslagerungsdateieinstellungen mithilfe der PowerShell-Befehle ändern. Weitere Informationen zum Ändern der Auslagerungsdateieinstellungen finden Sie unter Auslagerungsdateieinstellungen ändern.

In VMware nach mehreren Netzwerkkarten suchen. In VMware-Umgebungen wurden verschiedene vorbereitende Prüfungen eingeführt, wenn die Hostingeinheit und die Maschinenprofilvorlage über mehrere Netzwerke verfügen und der Parameter `-NetworkMapping` in den Befehlen `New-ProvScheme` und `Set-ProvScheme` verwendet wird. Weitere Informationen zur vorbereitenden Prüfung für mehrere Netzwerkkarten finden Sie unter Nach mehreren Netzwerkkarten suchen.

Unterstützung für die Erstellung von Windows 11-VMs in GCP. Sie können jetzt Windows 11-VMs in GCP erstellen. Wenn Sie Windows 11 auf dem Masterimage installieren, müssen Sie vTPM während der Erstellung des Masterimages aktivieren. Außerdem müssen Sie vTPM auf der Maschinenprofilquelle (VM oder Instanzvorlage) aktivieren.

Dieses Feature gilt für:

- Persistente und nicht persistente MCS-Maschinenkataloge.
- Nur Einzelmandantenknotengruppe.

Informationen zum Erstellen von Windows 11-VMs auf dem Einzelmandantenknoten finden Sie unter Windows 11-VMs auf dem Einzelmandantenknoten erstellen.

Unterstützung von Umgebungsvariablen durch die Positivliste für virtuelle Kanäle.
Sie können jetzt Systemumgebungsvariablen im Pfad der vertrauenswürdigen Prozesse verwenden.

Weitere Informationen finden Sie unter Verwenden von Systemumgebungsvariablen.

Veraltete Features in der vollständigen Konfiguration. Die folgenden Funktionen und Einstellungen sind in der vollständigen Konfiguration veraltet:

Unterstützung für HDX Plus für Windows 365-Cloud-PCs und Azure Virtual Desktops. Monitor unterstützt jetzt HDX Plus für Windows 365-Cloud-PCs und Azure Virtual Desktops (AVD). Weitere Informationen finden Sie unter Problembehandlung bei Maschinen.

Änderung des Cloud Build Service-Kontos. Ab dem 29. April 2024 führt GCP für neu erstellte Projekte Änderungen am Standardverhalten von Cloud Build Services und der Verwendung von Dienstkonten ein. Weitere Informationen finden Sie unter Änderungen des Cloud Build-Dienstkontos. Ihre vorhandenen Google-Projekte und Citrix-Kataloge sind von dieser Änderung jedoch nicht betroffen. Weitere Informationen:

- Dienstkonten konfigurieren und aktualisieren
- Erforderliche GCP-Berechtigungen

Unterstützung für HDX Plus für Windows 365-Cloud-PCs und Azure Virtual Desktops. Monitor unterstützt jetzt HDX Plus für Windows 365-Cloud-PCs und Azure Virtual Desktops (AVD). Weitere Informationen finden Sie unter Problembehandlung bei Maschinen.

VDA-Umgebungen mit Proxys für Internet- und URL-Filterung (Preview). Sie können den VDA-Upgradedienst jetzt verwenden, um VDAs zu aktualisieren, wenn Sie Proxys für Internetkonnektivität und Webfilterung haben. Der in der Richtlinie konfigurierte Proxy hat Vorrang vor dem in der Registrierung konfigurierten Proxy. Weitere Informationen finden Sie unter Installieren von VDAs. Sehen Sie sich auch die Liste der URLs an, die im Proxy auf die Positivliste gesetzt werden müssen.

Änderung des Cloud Build Service-Kontos. Ab dem 29. April 2024 führt GCP für neu erstellte Projekte Änderungen am Standardverhalten von Cloud Build Services und der Verwendung von Dienstkonten ein. Weitere Informationen finden Sie unter Änderungen des Cloud Build-Dienstkontos. Ihre vorhandenen Google-Projekte und Citrix-Kataloge sind von dieser Änderung jedoch nicht betroffen. Weitere Informationen:

- Dienstkonten konfigurieren und aktualisieren
- Erforderliche GCP-Berechtigungen

März 2024

Neue und erweiterte Features

Dynamische Sitzungsaufzeichnung Sie können jetzt die aktuelle aktive Sitzung mithilfe der Steuerelemente für die Sitzungsaufzeichnung im Bildschirm **Benutzerdetails** aufzeichnen, ohne die Sitzung erneut einrichten zu müssen. Dieses Feature ermöglicht eine schnellere und effektivere

Behebung von Problemen, die sich auf die Benutzeroberfläche beziehen. Dies ist nützlich, um Probleme zu debuggen, die schwer zu reproduzieren sind.

Weitere Informationen zur dynamischen Sitzungsaufzeichnung finden Sie im Artikel zum Sitzungsaufzeichnungsdienst.

Registrierungstool zum Registrieren von VDAs mit WebSockets für Maschinenkataloge. Sie können dieses Registrierungstool jetzt verwenden, um Ihre nicht domänengebundenen VDAs sicher in Maschinenkatalogen zu registrieren. Diese Funktion bietet den Vorteil, dass nur der TLS-Port 443 für die Kommunikation vom VDA zum Delivery Controller verwendet und der Verkehr über Port 80 entfernt wird. Weitere Informationen finden Sie unter Maschinen mit dem WebSocket VDA-Registrierungstool für Kataloge registrieren.

Vereinfachte Subnetzaktualisierungen für Maschinenkataloge. Bisher mussten Sie einen Maschinenkatalog löschen und neu erstellen, um die Subnetzeinstellungen zu ändern. Mit diesem Feature können Sie jetzt dieselbe Funktionalität erreichen, indem Sie den Katalog bearbeiten. Beachten Sie, dass sich nur neue virtuelle Maschinen, die im Rahmen des Katalogs erstellt wurden, in den neu verknüpften Subnetzen befinden. Diese Verbesserung reduziert die Notwendigkeit, den Katalog und die damit verbundenen Aufgaben zu löschen. Weitere Informationen finden Sie unter Bearbeiten eines Katalogs.

Vollständige Konfiguration: Unterstützung zur Aktualisierung weiterer Azure-VM-Einstellungen mit Maschinenprofilen. Mit der vollständigen Konfiguration können Sie jetzt eine breitere Palette von Einstellungen für von MCS bereitgestellte Azure-VMs über Maschinenprofile aktualisieren, darunter:

- Maschinengröße
- Lizenztyp
- Verfügbarkeitszone
- ID der dedizierten Hostgruppe

Nachdem Sie das Maschinenprofil aktualisiert haben, vergleicht die vollständige Konfiguration die aktuellen Einstellungen mit den neuen. Wenn Unterschiede bestehen, werden Sie aufgefordert, zu bestätigen, welche gelten sollen. Dieses Design gewährleistet transparente und effiziente Aktualisierungen der VM-Einstellungen.

Vollständige Konfiguration: Unterstützung für das Ändern der Einstellungen des Zurückschreibcaches für von MCS bereitgestellte Azure-VMs. Für Azure-VMs, die mit Maschinenerstellungsdiensten bereitgestellt wurden, können Sie jetzt ihre Eigenschaften für den Zurückschreibcache über die vollständige Konfiguration ändern, z. B. **Größe des Datenträgercaches**, **Größe des Speichercaches** und **Einsparung von Speicherkosten aktivieren**. Wenn Sie eine neue Maschinengröße oder ein neues Maschinenprofil für diese VMs auswählen, überprüft die vollständige Konfiguration außerdem die Einstellungen des Zurückschreibcaches, um Konflikte zu vermeiden, z. B. das Überschreiten

des Speicherlimits der neuen Auswahl. Wenn Konflikte auftreten, werden Sie aufgefordert, die Einstellungen des Zurückschreibcaches neu zu konfigurieren.

Februar 2024

Neue und erweiterte Features

Virtuelle Maschinen über die Workspace-Oberfläche anhalten. Sie können jetzt persistente VMs mit aktiven Sitzungen über die Workspace-Benutzeroberfläche anhalten. Diese Verbesserung bietet die folgenden Vorteile:

- Setzen Sie das System dort fort, wo Sie aufgehört haben.
- Dies bewirkt eine schnellere Startzeit im Vergleich zu einer gestoppten Maschine, deren Zuweisung aufgehoben wurde.
- Kostengünstig und energieeffizient.
- Effiziente Ressourcenzuweisung mithilfe des Autoscale-Features.

Neue Unterstützung für Machine Creation Services (MCS) Storage Optimization (MCSIO): Sie haben jetzt die Möglichkeit, dass der Image Portability Service MCSIO hinzufügt oder entfernt, wenn Sie ein Image für die MCS-Bereitstellung vorbereiten.
Weitere Informationen finden Sie unter VDA-Konfiguration automatisieren.

Verbesserungen des Überblicks über Tests: Eine Zusammenfassung der Testmetriken und der Testausfallphasen ist jetzt auf der Seite **Test** > **Übersicht** verfügbar. Die Testmetriken zeigen die Anzahl der geplanten, fehlgeschlagenen, übersprungenen und erfolgreichen Testläufe. Die grafische Darstellung der Ausfallphasen hilft bei der Analyse der Phasen, in denen die meisten Fehler aufgetreten sind. Diese Informationen tragen zu einer schnelleren Fehlerbehebung aufgrund der Testergebnisse bei. Weitere Informationen finden Sie unter Anwendungs- und Desktoptests.

Imageinformationen auf der Seite "Maschinenkataloge". Sie können jetzt die folgenden Imageinformationen über die **Vorlageneigenschaften** eines Maschinenkatalogs anzeigen:

- Betriebssystem
- Maschinenidentitätsdienst
- Speicher für Maschinenerstellungsdienste
- Dateipfad für `pagefile.sys` für Azure-Bereitstellungen

Durch diese Verbesserung werden die Imageinformationen übersichtlicher dargestellt und Administratoren können alle Informationen über einen Maschinenkatalog zentral anzeigen.

Unterstützung der vollständigen Konfiguration für die Verwaltung von VDA-Registrierungstoken. Die tokenbasierte VDA-Registrierung reduziert die Belastung der Cloud Connectors und verringert potenzielle Fehlerquellen. Dies ist ideal für Anwendungsfälle, in denen Sie die Maschinen mit einer

Technologie vorbereiten, die nicht von Citrix Provisioning stammt. Mit der vollständigen Konfiguration können Sie jetzt Registrierungstoken für nicht von Citrix bereitgestellte VDAs generieren und verwalten und so die auf Registrierungstoken basierenden Bereitstellungen optimieren. Weitere Informationen finden Sie unter Registrierungstoken generieren und verwalten.

PowerShell-Protokollierung. In der vollständigen Konfiguration können Sie jetzt die PowerShell-Befehle anzeigen, die Ihren täglichen Aktionen auf der Benutzeroberfläche entsprechen. Mit diesem Feature erhalten Sie zu Lernzwecken Einblicke in die zugrunde liegenden PowerShell-Befehle. Um die PowerShell-Protokolle anzuzeigen, gehen Sie zu **Protokollieren > PowerShell**. Weitere Informationen finden Sie unter Konfigurationsprotokollierung.

Aktivieren Sie Local Host Cache (LHC) für gepoolte Einzelsitzungs-VDAs über die vollständige Konfiguration. Standardmäßig sind gepoolte Einzelsitzungs-VDAs, die mit MCS oder Citrix Provisioning bereitgestellt wurden, im LHC-Modus nicht verfügbar. Mit der vollständigen Konfiguration können Sie dieses Standardverhalten jetzt pro Bereitstellungsgruppe außer Kraft setzen, sodass diese VDAs während des LHC-Betriebs für neue Verbindungen verfügbar sind. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen und Bereitstellungsgruppen verwalten.

Citrix Hypervisor wurde in der vollständigen Konfiguration in XenServer umbenannt. Gemäß unserer Rebranding-Strategie haben wir alle Instanzen von Citrix Hypervisor in der vollständigen Konfiguration auf XenServer aktualisiert.

Durchgängige Netzwerkhopansicht. Eine durchgängige Netzwerkhopansicht ist der nächste Schritt zur Verbesserung der Workflows zur Problembehandlung in Citrix Monitor. Der Abschnitt **Benutzerdetails** > **Sitzungsleistung** > **Sitzungstopologie** bietet eine visuelle Darstellung der durchgängigen Netzwerkhopansicht für verbundene HDX-Sitzungen. Der sitzungsinterne Pfad hilft dabei, die am Sitzungspfad beteiligten Komponenten mit ihren Metadaten, den Link zwischen den Komponenten und den auf dem VDA veröffentlichten Anwendungen zu verstehen. Die Sitzungstopologie unterstützt den Datenfluss und hilft dabei, den spezifischen Hop zu identifizieren, der zu Leistungsproblemen führen könnte.

Darüber hinaus werden die ICA-Latenz und ICA-RTT-Kennzahlen für die Sitzung angezeigt, wenn diese verbunden ist. Weitere Informationen finden Sie unter Durchgängige Netzwerkhopansicht.

Verwenden Sie die Datenträgerverschlüsselungssatz-ID (DES ID) des Masterimages, um alle Datenträger der Katalog-VMs zu verschlüsseln. In Azure-Umgebungen wurde bisher die Datenträgerverschlüsselungssatz-ID (DES ID) eines MCS-Maschinenkatalogs aus einem Maschinenprofil oder benutzerdefinierten Eigenschaften abgeleitet. Mit diesem Feature kann ein Maschinenkatalog auch die DES-ID vom Masterimage ableiten, um alle Datenträger der VMS in einem Katalog zu verschlüsseln.

Aktualisieren Sie die MCS-Tags, um verwaiste Ressourcen nach der Migration zu erkennen. Wenn Sie von einer On-Premises Konfiguration zu einer Cloudsite oder von Ihrer Cloudkonfiguration zu einer anderen Cloudsite migrieren, werden die verwaisten Ressourcen aufgrund des alten

Site-ID-Tags nicht richtig erkannt. Mit diesem Feature können Sie über einen PowerShell-Befehl die MCS-Site-ID-Tags eines persistenten Katalogs nach der Migration aktualisieren, sodass verwaiste Ressourcen korrekt erkannt werden können. Derzeit ist dieses Feature für Azure verfügbar. Weitere Informationen finden Sie unter MCS-Tags aktualisieren, um verwaiste Ressourcen nach der Migration zu erkennen.

Überprüfen Sie die Konfiguration, bevor Sie einen MCS-Maschinenkatalog erstellen. Mit diesem Feature können Sie jetzt die Konfigurationseinstellungen überprüfen, bevor Sie einen MCS-Maschinenkatalog erstellen, indem Sie den Parameter `-validate` im Befehl `New-ProvScheme` verwenden. Nachdem Sie diesen PowerShell-Befehl mit dem Parameter ausgeführt haben, erhalten Sie eine entsprechende Fehlermeldung, wenn ein falscher Parameter verwendet wird oder ein Parameter mit einem anderen Parameter in Konflikt steht. Anschließend können Sie die Fehlermeldung verwenden, um das Problem zu beheben und mithilfe von PowerShell erfolgreich einen MCS-Maschinenkatalog zu erstellen.

Derzeit ist dieses Feature auf Azure-, GCP- und VMware-Virtualisierungsumgebungen anwendbar. Weitere Informationen finden Sie unter Konfiguration überprüfen, bevor Sie einen MCS-Maschinenkatalog erstellen.

Unterstützung für das Kopieren von Tags von einer Maschinenprofilquelle auf eine VM in AWS. Mit diesem Feature können Sie in AWS-Virtualisierungsumgebungen im Maschinenprofil angegebene Tags auf Netzwerkkarten und Datenträgern (Identitätsdatenträger, Zurückschreibcachedatenträger und OS-Datenträger) auf neu erstellte VMs in einem MCS-Maschinenkatalog kopieren. Sie können diese Tags in jeder Maschinenprofilquelle (AWS EC2-Instanz oder AWS-Startvorlagenversion) angeben. Dieses Feature gilt für persistente und nicht persistente Maschinenkataloge und VMs. Weitere Informationen finden Sie unter Tags auf VMs kopieren.

SCVMM-Unterstützung für Maschinenprofile. Mit diesem Feature können Sie jetzt ein Maschinenprofil verwenden, um einen MCS-Maschinenkatalog in System Center Virtual Machine Manager-(SCVMM)-Umgebungen zu erstellen und zu aktualisieren. Sie können auch verschachtelte Virtualisierung und vTPM aktivieren. Weitere Informationen finden Sie unter Maschinenkatalog mit einem Maschinenprofil erstellen.

Azure-Unterstützung für die Verwendung von Spot-VMs mit MCS. Mit Azure Spot-VMs können Sie die ungenutzte Rechenkapazität von Azure zu erheblichen Kosteneinsparungen nutzen. Aufgrund der Entfernungsrichtlinie eignen sich Azure Spot-VMs demgemäß gut für einige unkritische Anwendungen und Desktops.

Mit diesem Feature können Sie mit einem Maschinenprofil (VM- oder Vorlagenspezifikation) einen MCS-Maschinenkatalog von Azure Spot-VMs erstellen. Sie können einen vorhandenen Katalog so aktualisieren, dass Azure Spot-VMs als neu erstellte VMs verwendet werden, oder zu Standard-Azure-VMs wechseln. Sie können auch vorhandene VMs zu Azure Spot-VMs aktualisieren. Weitere Informationen finden Sie unter Katalog mit Azure Spot-VMs erstellen.

Unterstützung für die Erfassung von Diagnoseeinstellungen aus einem Maschinenprofil. In Azure-Umgebungen unterstützt MCS jetzt die Erfassung von Diagnoseeinstellungen auf VMs und Netzwerkkarten aus einem Maschinenprofil beim Erstellen oder Aktualisieren eines MCS-Maschinenkatalogs oder beim Aktualisieren vorhandener VMs. Daher können mit dieser Implementierung die Diagnosedaten zur eingehenden Analyse und Visualisierung nahtlos an bestimmte Azure-Zielendpunkte wie Protokollanalysen-Workspaces oder Event Hubs übertragen werden. Weitere Informationen finden Sie unter Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen.

MCS-Unterstützung für die Verwaltung verschiedener Versionen eines Maschinenkatalogs. Mit diesem Feature können Sie die Konfigurationsversionen eines Maschinenkatalogs mit PowerShell-Befehlen verwalten. Jede Konfigurationsänderung unter Verwendung der `Set-ProvScheme`-Ergebnisse führt zu einer neuen Konfigurationsversion. Sie haben folgende Möglichkeiten:

- Liste der Versionen anzeigen.
- Eine frühere Version verwenden, um einen Maschinenkatalog zu aktualisieren.
- Eine Version manuell löschen, wenn sie nicht von einer VM verwendet wird.
- Maximale Anzahl von Versionen ändern, die vom Maschinenkatalog beibehalten werden sollen.

Weitere Informationen finden Sie unter Versionen eines Maschinenkatalogs verwalten.

Veröffentlichen Sie App-V-, MSIX- und MSIX-App-Attach-Anwendungspakete auf Einzelsitzungs- und gemeinsam genutzten Desktop-VDAs. Sie können jetzt auf Anwendungspakete zugreifen, z. B. App-V, MSIX und MSIX App Attach auf den Einzelsitzungs- und gemeinsam genutzten Desktop-VDAs. Diese Erweiterung stellt sicher, dass die Anwendungspakete sofort verfügbar sind, wenn Sie sich anmelden. Diese Funktion ermöglicht den schnelleren Start von Anwendungspaketen und verbessert Ihre Benutzererfahrung erheblich, da sie dem Zugriff auf eine lokal installierte Anwendung näher kommt. Weitere Informationen finden Sie unter Anwendungspakete auf Einzelsitzungs- oder gemeinsam genutzten Desktop-VDAs veröffentlichen.

Wiedergabe von Live- und aufgezeichneten Sitzungen: Citrix Monitor unterstützt jetzt die Wiedergabe von aufgezeichneten und Live-Benutzersitzungen, die mit dem Sitzungsaufzeichnungsdienst aufgezeichnet wurden. Die Sitzungsprobleme, auf die der Benutzer gestoßen ist, können Sie anhand der Wiederholung schnell nachvollziehen. Mit diesem Feature erhalten Sie direkten Zugriff auf Aufzeichnungen und sitzungsbezogene Messwerte in der Minotor-Konsole. Die in den Aufzeichnungen festgestellten Probleme lassen sich so mit den Leistungskennzahlen verknüpfen. Es entfällt die Notwendigkeit, auf mehreren Sitzungsaufzeichnungsservern nach Aufzeichnungen zu suchen oder nach Apps von Drittanbietern aufzurufen, um die Aufzeichnungen anzuzeigen.

Für dieses Feature sind der VDA und der Sitzungsaufzeichnungsserver Version 2308 oder höher erforderlich.

Monitor speichert die Aufzeichnungen in einem zentralen Repository und zeigt sie im **Sitzungsauswahl**-Modal an. Der Link **Sitzungen mit Aufzeichnungen** zeigt die Aufzeichnungen der Sitzungen an, die

in den letzten 24 Stunden oder den letzten 2 Tagen aktiv waren. Die Aufzeichnung wird auf einer neuen Registerkarte mit dem Wiedergabeserver der Citrix Sitzungsaufzeichnung wiedergegeben.

Weitere Informationen finden Sie unter Sitzungen aufzeichnen.

Microsoft Teams-Optimierung: Monitor zeigt den Status der HDX-Optimierung an, die für Microsoft Teams verfügbar ist. Die neue **Microsoft Teams-Optimierung** kann auf der Seite mit den **Benutzerdetails** im Bereich **Sitzungsdetails** eingesehen werden. Monitor zeigt den Status der Microsoft Teams-Optimierung nur an, wenn Microsoft Teams als veröffentlichte App oder auf einem veröffentlichten Desktop ausgeführt wird. Diese Verbesserung bietet Administratoren Einblick, sodass sie Probleme mit der Sitzungsleistung in Microsoft Teams beheben können, die von Benutzern gemeldet wurden. Weitere Informationen finden Sie unter Behandeln von Benutzerproblemen.

Verbesserungen der Benutzeroberfläche: Die Citrix Monitor-Benutzeroberfläche wurde jetzt aktualisiert und bietet ein modernes Erscheinungsbild. Die neue und verbesserte Benutzeroberfläche bietet eine einfachere Navigation und eine bessere Datendarstellung. Die verbesserte Benutzererfahrung ist intuitiv und so konzipiert, dass die Daten, die zur Überwachung und Fehlerbehebung einer Citrix-Sitzung erforderlich sind, leicht verstanden werden können.

Optimale Bildschirmauflösung: Die empfohlene optimale Bildschirmauflösung für die Citrix Monitor-Anzeige wurde auf 1440 x 1024 aktualisiert.

Januar 2024

Neue und erweiterte Features

Verbesserte bidirektionale Inhaltsumleitung konfigurieren Bisher mussten für die Konfiguration der bidirektionalen Inhaltsumleitung drei verschiedene Richtlinien verwaltet werden: Bidirektionale Inhaltsumleitung zulassen, Umleitung von URLs zum VDA zulassen und Umleitung von URLs zum Client zulassen. Diese Richtlinien erfordern Konfigurationen sowohl auf der Serverseite (konfiguriert unter **DaaS > Vollständige Konfiguration**) als auch auf der Clientseite (konfiguriert über Gruppenrichtlinien). Ab dieser Version wurden alle drei Richtlinien in einer einzigen, einheitlichen Richtlinie zusammengefasst. Dies vereinfacht und verbessert nicht nur den Konfigurationsprozess, sondern macht auch clientseitige Konfigurationen überflüssig. Weitere Informationen finden Sie unter Bidirektionale Inhaltsumleitung konfigurieren.

Unterstützung für das Neustarten und Herunterfahren von Einzelsitzungsmaschinen über die Registerkarte Sitzungen des Suchknotens. Auf der Registerkarte **Sitzungen** des **Suchknotens** können Sie jetzt nach Benutzersitzungen suchen, die sich in einem fehlerhaften Zustand befinden, und die zugehörigen Einzelsitzungsmaschinen auf derselben Registerkarte nahtlos neu starten oder herunterfahren. Diese Funktion erhöht die Effizienz und ermöglicht schnelle Maßnahmen bei erkannten Sitzungsproblemen über eine einzige Oberfläche.

Unterstützung für den Zugriff auf den Global App Configuration Service über "Vollständige Konfiguration". In der Benutzeroberfläche "Vollständige Konfiguration"wurden Aktionspunkte bereitgestellt, um Sie mit dem Global App Configuration Service zu verbinden. Mit dieser Integration können Sie ganz einfach auf den Global App Configuration Service zugreifen, um die Endbenutzereinstellungen über "Vollständige Konfiguration"zu verwalten.

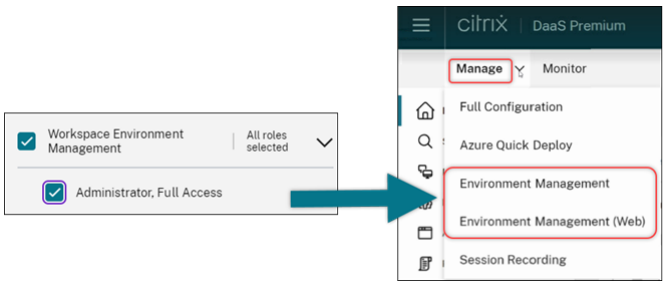
Um von der Benutzeroberfläche "Vollständige Konfiguration"aus auf diesen Dienst zuzugreifen, haben Sie zwei Möglichkeiten:

- Wählen Sie den **StoreFront**-Knoten aus, klicken Sie auf einen Serverdatensatz und wählen Sie dann in der Aktionsleiste **Clienteinstellungen konfigurieren** aus.
- Wählen Sie den Knoten **Richtlinien** und dann in der Aktionsleiste **Clienteinstellungen konfigurieren** aus.

Unterstützung für die Verwaltung von Benutzerzuweisungen für von Citrix Cloud verwaltete Bereitstellungsgruppen über "Vollständige Konfiguration". Im Rahmen unseres Plans, die Benutzerzuweisungsverwaltung von der Cloudbibliothek zu "Vollständige Konfiguration"zu migrieren, können Sie jetzt Benutzerzuweisungen für von Citrix Cloud verwaltete Bereitstellungsgruppen über "Vollständige Konfiguration"verwalten. Bearbeiten Sie dazu eine Zielbereitstellungsgruppe unter **Vollständige Konfiguration > Bereitstellungsgruppen** und legen Sie über eines der folgenden Menüs Benutzer fest, die Desktops oder Anwendungen verwenden dürfen: **Desktops** (oder **Desktop-Zuweisungsregeln**) oder **Anwendungszuweisungsregel**. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

In einem Portal vorgenommene Aktualisierungen werden nahtlos mit dem anderen synchronisiert, sodass konsistente Aktualisierungen auf beiden Portalen gewährleistet sind.

Beschränken Sie den Zugriff auf die WEM-Konsole auf die Rolle WEM-Vollzugriffsadministrator. Die Zugriffskontrolle für die Workspace Environment Management (WEM)-Konsolen wurde aktiviert, um unbefugten Zugriff zu verhindern. Nur Benutzer mit der Rolle **Workspace Environment Management Vollzugriffadministrator** können jetzt **DaaS > Verwalten** verwenden, um auf die WEM-Konsolen zuzugreifen.



Vollständige Konfiguration: Azure-Kataloge unterstützen das Erben von DES-Einstellungen von Masterimages. Bisher wurden bei der vollständigen Konfiguration die Standard-DES-Einstellungen der Azure-Kataloge nur auf der Grundlage von Maschinenprofilen festgelegt. Diese Funktion wurde

jetzt erweitert. Mit dieser Verbesserung legt die vollständige Konfiguration in den folgenden Fällen die Standard-DES-Einstellungen eines Azure-Katalogs direkt auf der Grundlage des Masterimages fest:

- Wenn kein Maschinenprofil ausgewählt ist
- Wenn das Profil einen Platform Managed Key (PMK) angibt

Weitere Informationen finden Sie unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.

Verbesserte Suche: Mehr Filter für mehr Präzision. Die Suche im Suchknoten wurde um zwei neue Filter, Zone und Bereitstellungstyp, erweitert, um die Präzision und Benutzerfreundlichkeit zu verbessern.

Vollständige Konfiguration: Unterstützung für die Auswahl des Google Cloud-Maschinentyps für GCP-Maschinenkataloge. Mit dieser Funktion haben Administratoren die Flexibilität, die erforderliche Speicher- und Prozessorkonfigurationen für bereitgestellte GCP-VMs auszuwählen und sie an spezifische Betriebsanforderungen anzupassen. Weitere Informationen finden Sie unter Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration erstellen.

Unterstützung für globale und regionale kundenverwaltete Verschlüsselungsschlüssel (CMEK) für die Bereitstellung von GCP-VMs. Sie können jetzt globale und regionale CMEK-Schlüssel für die Bereitstellung von VMs aus jedem Bereitstellungsprojekt verwenden. Diese Erweiterung bietet mehr Flexibilität bei der Schlüsselauswahl für die Bereitstellung von VMs und die Verbesserung der VM-Sicherheit.

Dezember 2023

Neue und erweiterte Features

Fortschritt beim Senden einer Nachricht. Sie können jetzt den Fortschritt des Vorgangs **Nachricht senden** unter **Überwachen** > **Filter** anzeigen. Dieser Vorgang hilft beim Senden von Massennachrichten an alle verbundenen Sitzungen auf Ihrer Site. Der Fortschritt des Vorgangs wird in Prozent angezeigt. Sobald der Vorgang abgeschlossen ist, zeigt das System die Anzahl der gesendeten Nachrichten und die Anzahl der fehlgeschlagenen Nachrichten angezeigt. Der Status "Nachricht senden"ist hilfreich, wenn Sie große Sites verwalten. Sie können damit erkennen, ob die Nachricht erneut an bestimmte Benutzer gesendet werden muss. Das Senden von Nachrichten kann fehlschlagen, wenn die Maschinen nicht registriert oder die Sitzungen fehlerhaft sind. Weitere Informationen über das Versenden von Nachrichten finden Sie unter Nachrichten an Benutzer senden.

Unterstützung der Citrix Probe Agent-Authentifizierung über Citrix Gateway mit Domänenanmeldeinformationen und Multifaktorauthentifizierung.

Der Citrix Probe Agent für Anwendungs- und Desktoptests unterstützt jetzt die Multifaktorauthentifizierung mit Citrix Gateway. Dieses Feature ist nützlich für die Ausführung des Probe Agent auf

Maschinen, die über Citrix Gateway mit StoreFront verbunden sind. Die umfassenden Testergebnisse im Überwachungsfeature helfen, Probleme bei Anwendungen, Hostcomputern oder Verbindung zu beheben, bevor sie sich bei den Benutzern bemerkbar machen. Die Unterstützung für Citrix Gateway mit Multifaktorauthentifizierung ist nur für ein Citrix Gateway verfügbar, das mit LDAP und nativem OTP unter Verwendung von Single Login Schema konfiguriert ist. Weitere Informationen finden Sie unter Anwendungs- und Desktoptests

Überarbeitete Benutzeroberfläche für Zugriffsrichtlinien für eine flexiblere Ressourcenzugriffskontrolle. Die Benutzeroberfläche **Bereitstellungsgruppe bearbeiten > Zugriffsrichtlinie** wurde neu gestaltet, um Ihnen mehr Flexibilität bei der Verwaltung des Ressourcenzugriffs für Bereitstellungsgruppen zu bieten. Im Folgenden sind die Hauptfeatures aufgeführt, die mit dem neuen Design verfügbar sind:

- **Unterstützung für das Hinzufügen von Richtlinien.** Sie können jetzt Zugriffsrichtlinien hinzufügen, um den Ressourcenzugriff auf der Grundlage der Attribute von Benutzerverbindungen einzuschränken. Eine Richtlinie kann aus zwei Arten von Kriterien bestehen:
  - **Einschlusskriterien.** Ermöglicht die Angabe von Benutzerverbindungen, die auf die Bereitstellungsgruppe zugreifen dürfen.
  - **Ausschlusskriterien.** Ermöglicht die Angabe von Benutzerverbindungen, die nicht auf die Bereitstellungsgruppe zugreifen dürfen.
- **Erweiterte Filterunterstützung.** Sie können jetzt Einschluss- und Ausschlusskriterien mit einer Reihe von SmartAccess-Filtern definieren. Zu diesen Filtern gehören Workspace-Filter wie `Citrix.Workspace.UsingDomain` und `Citrix-Via-Workspace` sowie Filter für den standortbasierten adaptiven Netzwerkzugriff.
- **Logikunterstützung "Übereinstimmung mit allen"für eingeschlossene Kriterien.** Die neue Logik ermöglicht es Ihnen, ein hohes Maß an Präzision und Kontrolle bei der Angabe zulässiger Benutzerverbindungen für Bereitstellungsgruppen zu erreichen.

Weitere Informationen finden Sie unter Zugriff auf Ressourcen in einer Bereitstellungsgruppe einschränken.

November 2023

Neue und erweiterte Features

Unterstützung für die Erstellung von Citrix Provisioning-Katalogen über die Benutzeroberfläche "Vollständige Konfiguration". Um einen Citrix Provisioning-Katalog zu erstellen, mussten Sie bisher den Setupassistenten für Citrix Virtual Apps and Desktops verwenden. Mit diesem Feature können Sie jetzt einen Citrix Provisioning-Katalog mithilfe der Benutzeroberfläche "Vollständige Konfiguration"und PowerShell erstellen.

Diese Implementierung bietet Ihnen die folgenden Vorteile:

- Eine einzige, einheitliche Konsole zur Verwaltung von MCS- und Citrix Provisioning-Katalogen.
- Neue Features für Citrix Provisioning-Kataloge, wie eine Identitätsverwaltungslösung, On-Demand-Provisioning und so weiter.

Derzeit ist dieses Feature nur für Azure-Workloads verfügbar. Weitere Informationen finden Sie unter Citrix Provisioning-Kataloge in Citrix Studio erstellen.

Einführung der Suche nach Anwendungsgruppen. Die Suchfunktion für Anwendungsgruppen im Knoten **Anwendungen** wurde eingeführt. Mit dieser Erweiterung können Sie jetzt direkt in einem beliebigen Anwendungsordner nach einer Anwendungsgruppe suchen. Weitere Informationen finden Sie unter Nach Anwendungsgruppen suchen.

Geänderte Konfigurationslimits. In der folgenden Tabelle werden die an den DaaS-Konfigurationslimits zur Leistungsverbesserung und Erhöhung der Kosteneffektivität vorgenommenen Änderungen beschrieben.

Ressource	Altes Limit	Neues Limit
Active Directory-Domänen	85	100
Kataloge	1.000	2.000
Bereitstellungsgruppen	1.000	2.000
Ressourcenstandort	85	100
Ressourcenstandort -> Sitzungen insgesamt	20.000	25.000

Weitere Informationen finden Sie unter Limits.

Eine Option, um VM und Systemdatenträger während Energiezyklen beizubehalten. Das Starten einer vorhandenen VM in Azure ist jetzt schneller als das Starten einer neuen VM, sodass es effizienter ist, virtuelle Maschinen über Energiezyklen hinweg beizubehalten. Daher haben wir die Optionen **VMs während Energiezyklen beibehalten** und **Systemdatenträger während Energiezyklen beibehalten** zu einer Einzeloption **VM und Systemdatenträger während Energiezyklen beibehalten** zusammengefasst. Wenn Sie diese Option wählen, um die Neustartzeiten von VMs durch die Beibehaltung der Systemdatenträger zu reduzieren, werden Ihre VMs ebenfalls beibehalten.

Neues Feature in der vollständigen Konfiguration zum Filtern nach Maschinengröße basierend auf der Eigenschaft *Verschlüsselung auf dem Host* in Maschinenprofilen (Azure-VM-spezifisch). Wenn Sie bei der Erstellung oder Verwaltung eines Azure-Maschinenkatalogs ein Maschinenprofil auswählen, bei dem die *Verschlüsselung auf dem Host* aktiviert ist, werden nur Maschinengrößen angezeigt, die dieses Feature unterstützen.

Backup- und Wiederherstellungsaktionen auf die Rolle des Volladministrators beschränkt. Wir haben die Zugriffssteuerung für Backup- und Wiederherstellungsaktionen verbessert. Nur Benutzer mit der Volladministratorrolle können jetzt auf den Knoten **Backup + Wiederherstellen** zugreifen, wodurch unbefugte Aktionen verhindert werden.

Datencaching für den Suchknoten. Wir haben Datencaching für den **Suchknoten** in Citrix DaaS eingeführt. Dies verbessert die Leistung der Suche. Anwendungsfälle, die Routineaufgaben erleichtern:

- Schnelle Anzeige der Suchergebnisse, nachdem diese erstmals abgerufen wurden.
- Beibehaltung der Paginierungsergebnisse, wenn Sie vom Knoten **Suchen** weg- und wieder zurückgehen.

Imageinformationen auf der Seite "Maschinenkataloge". Sie können jetzt die folgenden Imageinformationen über die **Vorlageneigenschaften** eines Maschinenkatalogs anzeigen:

- Betriebssystem
- Maschinenidentitätsdienst
- Speicher für Maschinenerstellungsdienste
- `pagefile.sys`-Dateipfad für Azure-Bereitstellungen.

Durch diese Verbesserung werden die Imageinformationen übersichtlicher dargestellt und Administratoren können alle Informationen über einen Maschinenkatalog zentral anzeigen.

Unterstützung für das Anheften von Suchfiltern. Zur Beschleunigung der Suche können Sie mit der vollständigen Konfiguration Ihre Suchfilter anheften. Das Anheften gestattet den einfachen Zugang zu häufig verwendeten Suchfiltern auf der Seite. Diese Erweiterung ist in den Suchbereichen der folgenden Knoten verfügbar:

- **Suche**
- **Maschinenkataloge**
- **Bereitstellungsgruppen**
- **Anwendungen**

Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Unterstützung für die Zuordnung von Metadaten zu Konfigurationsprotokollen. Mit dieser Verbesserung können Sie jetzt Metadaten an die Konfigurationsprotokolle anfügen, indem Sie High-Level-Operationen ein `name=value`-Paar zuordnen. Weitere Informationen finden Sie unter Metadaten zu Konfigurationsprotokollen zuordnen.

Verwaiste Ressourcen mit einem bestimmten Tag ignorieren. In Azure-Umgebungen wird eine vom Kunden verwaltete Ressource, die mit allen Citrix Tags gekennzeichnet ist, als verwaiste Ressource erkannt. Wenn Sie der Ressource jedoch mithilfe dieses Features das Tag

`CitrixDetectIgnore` mit dem Wert "true"hinzufügen, wird die Ressource bei der Erkennung verwaister Ressourcen ignoriert.

Lösung für das Problem duplizierter SCCM-GUIDs. Nach dem Erstellen mehrerer VMs mit MCS zeigte System Center Configuration Manager (SCCM) aufgrund doppelter GUIDs nur eine VM an. Dieses Problem wurde durch Hinzufügen eines Schritts in der Image-Erstellung behoben. Durch diesen Schritt werden die vorhandenen Zertifikate und GUID-Informationen im Masterimage gelöscht. Der Schritt ist standardmäßig aktiviert.

Identitätsinformationen aktiver Computerkonten reparieren. Mit diesem Feature können Sie die Identitätsinformationen von aktiven Computerkonten mit Identitätsproblemen zurücksetzen. Sie können wählen, ob Sie nur das Maschinenkennwort und die vertrauenswürdigen Schlüssel-IDs oder die gesamte Konfiguration des Identitätsdatenträgers zurücksetzen möchten. Diese Implementierung gilt für persistente und nicht persistente Maschinenkataloge. Derzeit wird das Feature nur für Azure- und VMware-Virtualisierungsumgebungen unterstützt. Weitere Informationen finden Sie unter Identitätsinformationen aktiver Computerkonten reparieren.

Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen. In Azure-Umgebungen können Sie mithilfe dieses Features jetzt über PowerShell-Befehle feststellen, ob die Verschlüsselung auf dem Host für eine Maschinenprofileingabe (VM oder Vorlagenspezifikation) aktiviert ist. Weitere Informationen finden Sie unter Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen.

Reparieren der Benutzerzertifikate der Identitäten von Maschinen mit Azure AD-Hybrid-Einbindung. Mit diesem Feature können Sie über einen Powershell-Befehl die Benutzerzertifikate der Identitäten von Maschinen mit Azure AD-Hybrid-Einbindung reparieren, falls diese beschädigt oder abgelaufen sind. Weitere Informationen finden Sie unter Kataloge mit Hybrideinbindung in Azure Active Directory erstellen.

Unterstützung von Zertifikatablaufwarnungen für hybride Azure AD-verbundene Maschinenkataloge. "Vollständige Konfiguration"warnt jetzt einen Monat im Voraus vor Ablauf von Benutzerzertifikaten für Hybrid-Maschinenkataloge, die mit Azure AD verbunden sind. Diese Verbesserung zielt darauf ab, das Risiko von Betriebsunterbrechungen aufgrund des Ablaufs des Zertifikats zu verringern. Um die Details und empfohlenen Aktionen anzuzeigen, wechseln Sie zum Knoten **Maschinenkataloge**, wählen Sie den Maschinenkatalog aus und klicken Sie dann auf die Registerkarte **Problembehandlung**.

Sie können den Befehl `Get-ProvScheme` ausführen, um Informationen über das Ablaufdatum des Benutzerzertifikats eines Maschinenkatalogs mit Azure AD-Hybrid-Einbindung zu erhalten.

Unterstützung für vertrauliche Azure-VMs (Preview). Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist. Mit diesem Feature können Sie jetzt MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen

Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Weitere Informationen finden Sie unter Vertrauliche Azure-VMs (Preview).

Unterstützung für die Konvertierung eines Maschinenkatalogs, der nicht auf Maschinenprofilen basiert, in einen maschinenprofilbasierten Maschinenkatalog in einer AWS-Umgebung. In einer AWS-Umgebung können Sie jetzt eine VM oder eine Startvorlage als Maschinenprofileingabe verwenden, um einen Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog zu konvertieren. Neue dem Katalog hinzugefügte virtuelle Maschinen übernehmen Eigenschaftswerte aus dem Maschinenprofil. Weitere Informationen finden Sie unter Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog in einer Azure-Umgebung konvertieren.

Unterstützung für das von Citrix verwaltete HPE Moonshot-Plug-In (Preview). Bisher haben Sie das von HPE verwaltete Moonshot-Plug-In (HPE Moonshot Machine Manager) verwendet, das von Hewlett Packard Enterprise (HPE) verwaltet wird, um Energieverwaltungsaktionen am HPE Moonshot Chassis durchzuführen. Das Plug-In basiert auf veralteten APIs, was MCS-Infrastrukturprojekte erschwerte. Mit diesem Feature wird ein von Citrix verwaltetes HPE Moonshot-Plug-In (HPE Moonshot) eingeführt. Mit diesem Plug-In können Sie Verbindungen zu Ihrem HPE Moonshot Chassis herstellen, Kataloge erstellen und die Energieverwaltung von Maschinen im Katalog über die Schnittstelle zur vollständigen Konfiguration und PowerShell-Befehle steuern. Weitere Informationen:

- HPE Moonshot-Virtualisierungsumgebungen (Preview)
- Verbindung zu HPE Moonshot (Preview)
- HPE Moonshot-Maschinenkatalog erstellen (Preview)
- HPE Moonshot-Katalog verwalten (Preview)

Möglichkeit, Speicher- und Datenträgercachegröße zu ändern. Mit diesem Feature können Sie jetzt mithilfe eines PowerShell-Befehls die Speicher- und Datenträgercachegröße des Zurückschreibcaches ändern (sofern MCSIO aktiviert ist), ohne einen neuen Maschinenkatalog zu erstellen. Diese Implementierung hilft beim Erzielen einer optimierten, für die jeweiligen Geschäftsanforderungen geeigneten Cachekonfiguration. Dieses Feature gilt für:

- GCP- und Microsoft Azure-Umgebungen sowie
- nicht persistenter Katalog mit aktiviertem MCSIO

Weitere Informationen finden Sie unter Cachekonfiguration eines Maschinenkatalogs ändern.

Unterstützung für das Erstellen Katalogs mit einem vom Kunden verwalteten Verschlüsselungsschlüssel. In Azure-Umgebungen können Sie jetzt mithilfe der Benutzeroberfläche für die vollständige Konfiguration und von PowerShell-Befehlen einen Citrix Provisioning-Katalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen. Weitere Informationen finden Sie unter Katalog mit vom Kunden verwaltetem Verschlüsselungsschlüssel erstellen.

Weitere Informationen finden Sie unter **Möglichkeit, Tags an alle Ressourcen in Azure zu kopieren**. Mit diesem Feature können Sie in einer Azure-Umgebung in einem Maschinenprofil angegebene Tags an alle Ressourcen (z. B. mehrere Netzwerkkarten und Betriebssystem-, Identitäts- und Zurückschreibdatenträger) einer neuen VM oder bestehenden VM in einem Maschinenkatalog kopieren.

Die Maschinenprofilquelle kann eine VM oder ARM-Vorlagenspezifikation sein. Weitere Informationen finden Sie Tags an alle Ressourcen kopieren.

Aktualisierung des Sitzungsstatus auf "Getrennt"nach dem Anhalten einer Maschine. Bisher wurde eine Sitzung nach dem Anhalten einer VM weiterhin als **Aktiv**angezeigt. Mit dieser Verbesserung wird der Zustand der zugehörigen Sitzung nach dem Anhalten einer VM jetzt als **Getrennt** angezeigt.

Unterstützung für die Erstellung von für den Ruhezustand geeigneten AWS-VMs. Sie können jetzt Maschinenkataloge erstellen, die den Ruhezustand von VMs in AWS-Umgebungen unterstützen, wodurch die Gesamtkosteneffektivität Ihrer Bereitstellung verbessert wird. Sie können bestehende Kataloge auch bearbeiten, sodass sie für den Ruhezustand geeignete VMs enthalten, sofern das zugehörige Maschinenprofil dieses Feature unterstützt. Weitere Informationen finden Sie unter Energieverwaltung von AWS-VMs.

Unterstützung für die Konfiguration von Lastausgleichsmethoden auf Bereitstellungsgruppenebene (Preview). Mit diesem Feature können Sie die **Methode für den vertikalen Lastausgleich** auf Bereitstellungsgruppenebene auswählen. Jede Maschine wird dann am maximalen Lastindex ausgerichtet, bevor die nächste Maschine eingeschaltet wird. Autoscale und der vertikale Lastausgleich steuern, wann die nächste Maschine eingeschaltet wird. Das Feature ermöglicht die maximale Auslastung jeder Maschine und Kosteneinsparungen in öffentlichen Clouds. Es bietet mehr Flexibilität bei der Verwaltung der Lastausgleichsstrategien für Maschinen.

Sie können eine Bereitstellungsgruppe so konfigurieren, dass sie die Lastausgleichsmethode von den Einstellungen auf Siteebene übernimmt oder die Außerkraftsetzung der Lastausgleichsmethode auf Siteebene wählen und stattdessen den vertikalen oder den horizontalen Lastausgleich wählen. Weitere Informationen siehe Schritt 2. Lastausgleich.

Unterstützung von für den Ruhezustand geeigneten VMs in Azure (Preview). In Azure-Umgebungen können Sie einen MCS-Maschinenkatalog erstellen, der den Ruhezustand unterstützt. Mit diesem Feature können Sie eine VM anhalten und dann wieder mit dem vorherigen Status der VM verbinden, wenn sich ein Benutzer erneut anmeldet. Weitere Informationen finden Sie unter Für den Ruhezustand geeignete VMs erstellen (Preview).

Leitfaden "Erste Schritte mit DaaS" Wir haben einen neuen Leitfaden eingeführt, um die Bereitstellung und Konfiguration von DaaS für neue und für erfahrene Administratoren zu optimieren und zu vereinfachen. Er bietet die folgenden Hauptvorteile:

- **Einfacher Einstieg.** Das auf der Beantwortung von Fragen basierende Schritt-für-Schritt-

Konzept vereinfacht die Einrichtung von Bereitstellungen für neue Administratoren. Eine Kontexthilfe erläutert wichtige Konzepte und Terminologie im gesamten Leitfaden.

- **Vereinfacht komplexe Konfigurationen.** Der Leitfaden enthält nach Bedarf vorkonfigurierte Einstellungen und bietet Zugriff auf die Benutzeroberfläche für die vollständige Konfiguration für erweiterte Einstellungen. Erfahrene Administratoren können ihn als Grundlage für komplexere Konfigurationen verwenden.

Weitere Informationen finden Sie im Leitfaden "Erste Schritte mit DaaS"verwenden.

Zuweisen von Laufwerksbuchstaben zu Zurückschreibcache-Datenträgern mit der vollständigen Konfiguration Bisher konnten Sie dem Zurückschreibcache-Datenträger nur mithilfe eines PowerShell-Cmdlets einen Laufwerksbuchstaben zuweisen. Sie können dies jetzt mit der vollständigen Konfiguration ausführen. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Unterstützung für das Ändern diverser Azure-Maschineneigenschaften mit der vollständigen Konfiguration. Für per MCS bereitgestellte Azure-Maschinen können Sie jetzt die folgenden Eigenschaftseinstellungen mit der vollständigen Konfiguration ändern:

- Speichertyp
- Dedizierte Hostgruppe
- Azure Compute Gallery-Einstellungen

Wenn Sie eine dieser Einstellungen ändern, identifiziert die vollständige Konfiguration automatisch zugehörige Einstellungen und bietet eine automatische Synchronisierung bzw. fordert Sie auf, die zugehörigen Einstellungen erneut auszuwählen. So wird gewährleistet, dass alle Einstellungen auf die gleiche Weise geändert und Konfigurationsfehler vermieden werden. Weitere Informationen finden Sie unter Bearbeiten eines Katalogs.

Verwenden bestehender Identitätspools, um Identitäten für MCS-bereitgestellte Maschinen zu erstellen Wenn Sie mit der vollständigen Konfiguration in AD eingebundene Kataloge erstellen oder diesen Maschinen hinzufügen, können Sie jetzt Maschinenidentitäten unter Einsatz eines bestehenden Identitätspools zuweisen. Das Feature gestattet die Anwendung eines konsistenten Benennungsschemas für Maschinenkonten in mehreren Katalogen. Weitere Informationen finden Sie unter Maschinenidentitäten.

Sitzungstopologie. Die Ansicht "Sitzungstopologie"ist der nächste Schritt zur Verbesserung der Workflows zur Problembehandlung in der Überwachung. Sie bietet eine visuelle Darstellung des sitzungsinternen Pfads für verbundene HDX-Sitzungen. Sie können über **Benutzerdetails > Sitzungsleistung** auf die Topologieansicht zugreifen.

Für eine verbundene HDX-Sitzung zeigt die Sitzungstopologie die am Sitzungspfad beteiligten Komponenten mit zugehörigen Metadaten, die Verbindung zwischen den Komponenten und die auf dem VDA veröffentlichten Anwendungen. Darüber hinaus werden die ICA-Latenz und ICA-RTT-Kennzahlen für die Sitzung angezeigt, wenn diese verbunden ist.

Anhand der Ansicht "Sitzungstopologie"sehen Sie, durch welche Komponenten die Sitzungsdaten übertragen werden, und können Hops identifizieren, die ggf. Leistungsprobleme verursachen. Weitere Informationen finden Sie unter Sitzungstopologie.

Oktober 2023

Neue und erweiterte Features

Feinsteuerung der Autoscale-Einstellungen anhand historischer Nutzung. Eine neue Registerkarte mit **Einblicke in Autoscale** bietet ein detailliertes Diagramm für den visuellen Vergleich der Autoscale-Einstellungen und Gerätenutzungsdaten der Vorwoche. Anhand des Diagramms können Sie die Effektivität der Autoscale-Einstellungen prüfen:

- **Nicht kosteneffektiv**. Finanzielle Verschwendung aufgrund einer Überversorgung mit Kapazitäten.
- **Schlechte Benutzererfahrung**. Beeinträchtigung der Benutzererfahrung durch Unterversorgung mit Kapazitäten.
- **Gutes Gleichgewicht zwischen Benutzererfahrung und Kosten**. Die bereitgestellte Kapazität entspricht der historischen Nutzung.

Weitere Informationen finden Sie unter Wirksamkeit von Autoscale-Einstellungen analysieren.

Unterstützung mehrerer Netzwerkkarten für Azure-VMs. Mit der vollständigen Konfiguration können Sie jetzt Azure-VMs mit mehreren Netzwerkkarten erstellen. Die maximale Anzahl der Netzwerkkarten einer VM wird durch die Einstellung der Maschinengröße bestimmt. Die tatsächlich zulässige Anzahl wird durch die Einstellung des Maschinenprofils definiert. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Informationen zum Erstellen oder Aktualisieren eines Katalogs mit mehreren Netzwerkkarten pro VM mithilfe von PowerShell-Befehlen finden Sie unter Katalog mit mehreren Netzwerkkarten pro VM erstellen oder aktualisieren.

Trends für Sitzungsleistungsmetriken. Auf der Registerkarte **Benutzerdetails > Sitzungsleistung** der Überwachung wurden die Workflows zur Fehlerbehebung verbessert, etwa durch die Möglichkeit, Echtzeitmetriken zur Identifizierung von Problemen in Benutzersitzungen zu korrelieren. Die Informationen zur Sitzungserfahrung enthalten jetzt Sitzungsmetriktrends: ICARTT, ICA-Latenz, Frames pro Sekunde, verfügbare Ausgabebandbreite und verbrauchte Ausgabebandbreite. Das Feature reduziert durch das Korrelieren mehrerer Leistungsmetriken in einer Ansicht die durchschnittliche Zeit für die Problemlösung bei der Sitzungserfahrung. Weitere Informationen finden Sie im Artikel Benutzerprobleme.

Unterstützung für VDA-Version auf der Seite für Einstellungen beim Erstellen/Bearbeiten von Richtlinien. Beim Erstellen einer Richtlinie und Konfigurieren der Einstellungen bietet das

System eine Option zum Anzeigen des Einstellungstyps. Sie können den folgenden Einstellungstyp anzeigen:

- Alle Einstellungen: Alle Einstellungen für alle VDA-Versionen anzeigen
- Nur aktuelle Einstellungen: Nur Einstellungen für aktuelle VDA-Versionen anzeigen
- Nur Legacy-Einstellungen: Nur Einstellungen für veraltete VDA-Versionen anzeigen

Weitere Informationen finden Sie unter Richtlinien erstellen.

Einschränkung der Sichtbarkeit von Anwendungen nur für Active Directory-Konten unterstützt. Die Möglichkeit, die Sichtbarkeit von Anwendungen einzuschränken, ist nur für Active Directory-Benutzerkonten verfügbar, nicht für Azure Active Directory- und Okta-Konten. Zur Unterstützung des Features müssen im Workflow für Anwendungseinstellungen auf der Seite "Benutzer oder Gruppen auswählen"im Feld **Identitätstyp auswählen** die Optionen **Azure Active Directory**und **Okta** deaktiviert sein.

Neue UI-Option zum Löschen von VM-Einträgen nur aus der Citrix-Sitedatenbank. Wenn das Löschen von Katalogen und VMs aufgrund eines nicht erreichbaren Hypervisors fehlschlägt, können Sie jetzt festlegen, dass VM-Einträge nur aus der Citrix-Sitedatenbank gelöscht werden, sodass die VMs auf dem Host intakt bleiben. Weitere Informationen finden Sie unter Löschen eines Katalogs.

Unterstützung für das Erstellen leerer Maschinenkataloge für nicht mit MCS bereitgestellte Maschinen. Das Erstellen leerer Maschinenkataloge erstreckt sich jetzt auch auf Maschinen, die nicht über MCS bereitgestellt wurden, einschließlich:

- Virtuelle Maschinen oder Bladeserver, die mit einem anderen Verfahren als MCS bereitgestellt wurden.
- Physische Maschinen ohne Energieverwaltung durch Citrix DaaS
- Maschinen mit Remote-PC-Zugriff

Mit diesem Feature können Sie jetzt Maschinenkataloge erstellen, ohne ihnen bei der Katalogerstellung Maschinen hinzufügen zu müssen.

Verbesserungen bei der Imageaktualisierung. Bisher wurden beim Aktualisieren von Images alle Images in der Imagestruktur aktualisiert, unabhängig davon, ob ein bestimmter Knoten in der Struktur ausgewählt wurde. Mit der aktuellen Verbesserung können Sie einen Knoten auswählen und nur die Images in diesem Knoten aktualisieren. Dies gewährleistet einen gezielteren Aktualisierungsprozess und beschleunigt das Aktualisieren von Images erheblich. Außerdem können Sie jetzt die Auswahl eines Knotens in der Imagestruktur aufheben, indem Sie bei gedrückter STRG-Taste auf den Knoten klicken. Weitere Informationen finden Sie unter Masterimage.

Eingeschaltete zugewiesene Maschinen zu Spitzenzeiten automatisch skalieren. Wenn persistente Desktops eingeschaltet sind, aber nicht genutzt werden, oder wenn sich kein Benutzer anmeldet, können die Administratoren eine Wartezeit für Aktionen wie "Keine Aktion", "Anhalten" oder "Herunterfahren"definieren.

Für eingeschaltete zugewiesene Maschinen, mit denen innerhalb der festgelegten Zeit nach Beginn der Spitzenzeit keine Sitzung verbunden wird, können Sie auf Bereitstellungsgruppenebene eine Richtlinie zum Ausschalten der Maschine hinzufügen.

Für fortgesetzte zugewiesene Maschinen, mit denen innerhalb der festgelegten Zeit nach Beginn der Spitzenzeit keine Sitzung verbunden wird, können Sie auf Bereitstellungsgruppenebene eine Richtlinie zum Anhalten der Maschine hinzufügen.

Dieses Feature ist hilfreich, wenn ein Endbenutzer abwesend oder nicht angemeldet ist, oder wenn ein Unternehmen ein langes Wochenende plant. Sie können eine Wartezeit festlegen und welche Maßnahmen zum Trennen der Maschinenverbindung zu ergreifen sind, um die Azure-Verbrauchskosten zu senken. Weitere Informationen finden Sie unter Zufällige Einzelsitzungs-OS-Bereitstellungsgruppen und Statische Einzelsitzungs-OS-Bereitstellungsgruppen.

Überwachen mehrerer Citrix DaaS-Instanzen (Preview). Mit der Citrix-Überwachungsfunktion können Sie jetzt mehrere Citrix DaaS-Instanzen gleichzeitig überwachen und Probleme instanzenübergreifend beheben. Citrix DaaS ermöglicht Kunden die Aggregation mehrerer Dienstinstanzen über ein Hub-Spoke-Modell. Mit dieser Konfiguration können Administratoren von einer einzigen Überwachungskonsole aus eine Helpdesksuche auf allen konfigurierten DaaS-Instanzen durchführen. Weitere Informationen zur erforderlichen Konfiguration für die Aggregation von Spoke-Dienstinstanzen unter einem Hub finden Sie unter Aggregate multiple Citrix Virtual Apps and Desktops service instances. "Überwachen"unterstützt die Aggregation von bis zu vier DaaS-Mandanten (Spokes) unter einem einzigen DaaS-Mandanten (Hub).
Verwenden Sie eine bidirektionale Enumeration der Hub- und Spoke-Instanzen, um eine einheitliche Überwachung aller DaaS-Mandanten zu gewährleisten. Weitere Informationen finden Sie unter Aggregierte Suche über mehrere DaaS-Instanzen hinweg (Preview).

Unterstützung für vSAN 8.0. Sie können jetzt mit MCS VMs in einer vSAN 8.0-Umgebung bereitstellen.

Beibehalten von NIC-Einstellungen auf bereitgestellten VMs. Die Masterimage-NIC-Einstellungen wurden zuvor für bereitgestellte VMs nicht beibehalten. Wenn Sie beispielsweise die DNS-Einstellungen auf dem Masterimage konfiguriert hatten, wurden diese auf den bereitgestellten VMs nicht beibehalten. Mit diesem Feature bleiben nun die NIC-Einstellungen des Masterimages auf bereitgestellten VMs erhalten. Die Einstellungen bleiben auch nach einem Windows-Update erhalten. Der Filtertreiber wird automatisch installiert, wenn Sie eine Neuinstallation des VDAs der Version 2308 oder höher auf einer mit Hyper-V bereitgestellten Maschine über die MCS-Masterimage-Installationen durchführen. Wenn Sie derzeit jedoch ein Upgrade einer älteren VDA-Version (unter 2308) durchführen und den Filtertreiber installieren möchten, müssen Sie beim Upgrade auf der Seite **Zusätzliche Komponenten** das Kontrollkästchen **Citrix HyperV Filter Driver** aktivieren. Weitere Informationen finden Sie unter Zusätzliche Komponenten installieren.

Dieses Feature gilt für:

- Hyper-V-VMs (einschließlich Azure und SCVMM)
- Persistente und nicht persistente MCS-Maschinenkataloge
- Nicht persistente MCS-Maschinenkataloge mit MCSIO
- Masterimages mit mehreren Netzwerkkarten

Verwaiste Azure-Ressourcen erkennen. Mit diesem Feature können Sie jetzt verwaiste Ressourcen in Ihrer Azure-Bereitstellung erkennen und so für eine effiziente Ressourcenverwaltung sorgen. Nachdem die verwaisten Ressourcen identifiziert wurden, können Sie weitere Maßnahmen ergreifen, um die Produktivität zu steigern und die Kosten zu senken. Weitere Informationen finden Sie unter Verwaiste Azure-Ressourcen in Ihrer Bereitstellung erkennen.

Neuer Imageupdatestatus. Beim Überwachen des Imageupdatestatus für Kataloge unter "Vollständige Konfiguration"können Sie jetzt zusätzlich zu den vorhandenen Statusanzeigen **Vollständig aktualisiert**, **Teilweise aktualisiert** und **Update ausstehend** den neuen Status **Image vorbereiten** anzeigen. Weitere Informationen finden Sie unter Masterimage ändern.

PowerShell-Befehle zum Erstellen von Auto-Tags (Preview). Mit diesem Feature können Sie jetzt mithilfe eines PowerShell-Befehls automatisch Tags erstellen. Weitere Informationen finden Sie unter Automatische Tags.

Benachrichtigungssymbol für Benutzer oder Bereitstellungsgruppe angezeigt. Wenn beim Erstellen oder Ändern einer Richtlinie und beim Konfigurieren der Einstellungen alle Bereitstellungsgruppen deaktiviert sind, wird eine Warnmeldung angezeigt, dass kein Element im Filter aktiviert ist. Wenn mindestens eine Bereitstellungsgruppe aktiviert ist, wird kein Warnsymbol angezeigt. Weitere Informationen finden Sie unter Richtlinieneinstellungen.

September 2023

Neue und erweiterte Features

PowerShell-Befehle zur Verwaltung des lokalen Hostcache (LHC). Sie können jetzt PowerShell-Befehle verwenden, um den lokalen Hostcache auf Citrix Cloud Connectors zu verwalten. Weitere Informationen finden Sie unter PowerShell-Befehle für den lokalen Hostcache.

Unterstützung für das Erstellen leerer Maschinenkataloge. In "Vollständige Konfiguration"können Sie jetzt einen Maschinenkatalog ohne sofortiges Erstellen von VMs erstellen. Mit diesem Feature können Sie die VM-Erstellung verschieben, bis die Back-End-Hosts vollständig vorbereitet sind oder das VM-Provisioning abgeschlossen ist. Dies sorgt für mehr Flexibilität beim Erstellen von Katalogen. Derzeit gilt dieses Feature nur für Kataloge, die mit Maschinenerstellungsdiensten (MCS) bereitgestellt werden. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Datencaching für den Home-Knoten. Wir haben das Datencaching für den **Home-Knoten** von Citrix DaaS eingeführt. Dies verbessert die Benutzererfahrung, da die Seite schneller geladen wird, wenn Sie zum **Home-Knoten** navigieren.

Verbesserungen der Suche für Anwendungen. Wir haben die Suchfunktion im Knoten **Anwendungen** überarbeitet, um sie an das neue Design anzupassen, das im **Suchknoten** eingeführt wurde. Das neue Feature verbessert die Anwendungssuche und vereinheitlicht den Suchprozess in DaaS. Das Schlüsselwort **Anwendungsname** im Filterausdruck wird in **Name** umbenannt, wobei die ursprüngliche Bedeutung beibehalten wurde. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Verbesserte Bereichsverwaltung: Objektanzeige in Ordneransicht. Auf den Seiten zur Erstellung und Verwaltung von Bereichen werden Maschinenkataloge, Bereitstellungsgruppen und Anwendungsgruppen jetzt in Ordnerstrukturen angezeigt, die auf ihre Verwaltung in DaaS abgestimmt sind. Diese Ordneransicht vereinfacht die Auswahl von Objekten für die Erstellung und Verwaltung von Bereichen und macht Ihre Auswahl intuitiver und übersichtlicher. Weitere Informationen finden Sie unter Erstellen und Verwalten von Geltungsbereichen.

Option "Benutzerverwaltung mit Citrix Cloud"wurde entfernt. Beim Erstellen einer Bereitstellungsgruppe unter "Verwalten > Vollständige Konfiguration"wird diese Option auf der Seite "Benutzer"nicht mehr unterstützt. In Bereitstellungsgruppen, bei denen Benutzer über Citrix Cloud zugewiesen wurden, verwalten Sie Benutzerzuweisungen weiterhin in der Citrix Cloud-Bibliothek.

Die Option "Azure Deutschland"wurde entfernt. Im Zuge der Schließung von Microsoft Cloud Deutschland am 29. Oktober 2021 haben wir die Option **Azure Deutschland** von der Seite zur Erstellung von Hostverbindungen entfernt.

Proaktive Servicewarnungen in "Vollständige Konfiguration". Es gibt zwei Arten von Benachrichtigungen: Siteübergreifende Benachrichtigungen werden auf der Homepage angezeigt (Flaggensymbol). Zonenbezogene Benachrichtigungen werden auf der Registerkarte "Problembehandlung"jeder Zone angezeigt. Derzeit werden Sie mit diesem Feature proaktiv informiert, ob Ihr lokaler Hostcache und die Zonen korrekt konfiguriert sind, damit der lokale Hostcache bei einem Ausfall funktioniert und Ihre Benutzer nicht davon betroffen sind. Weitere Informationen finden Sie unter Benachrichtigungen zum Dienststatus und Zonen.

August 2023

Neue und erweiterte Features

Vollständige Konfiguration: Unterstützung für das Provisioning von AWS- und GCP-VMs mithilfe von Maschinenprofilen. Bei der Bereitstellung von AWS- oder GCP-VMs mithilfe von Maschinenerstellungsdiensten (MCS) können Sie jetzt eine vorhandene VM als Maschinenprofil auswählen, sodass andere VMs im Katalog Einstellungen von der ausgewählten VM übernehmen (erben) können.

- Für GCP-VMs umfasst dies die Einstellungen "ID des Datenträgerverschlüsselungssatzes", "Maschinengröße", "Speichertyp"und "Zone".

- Bei AWS-VMs variieren die vererbten Einstellungen je nach Phase:
  - Bei der Katalogerstellung: Maschinengröße, Mandantenmodell, Sicherheitsgruppe und Anzahl der Netzwerkkarten.
  - Bei der Katalogbearbeitung: Maschinengröße und Sicherheitsgruppe.

Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Einführung der Suchfunktion in den Knoten für Maschinenkataloge und Bereitstellungsgruppen. Sie können jetzt innerhalb der Knoten **Maschinenkataloge** und **Bereitstellungsgruppen** direkt nach Maschinenkatalogen und Bereitstellungsgruppen suchen. Die Suchfunktion in diesen Knoten bietet dieselbe Oberfläche wie der **Suchknoten**, was die Suche in DaaS vereinheitlicht und erleichtert. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Anzeigen des Status von Endgeräten in der Sitzungsstartdiagnose mithilfe von Device Posture. Die Sitzungsstartdiagnose in der Überwachung hilft dabei, die Komponente und Phase zu isolieren, wenn ein Sitzungsfehler aufgetreten ist. Auf diese Weise können Sie den genauen Grund für einen Sitzungsstartfehler ermitteln und die empfohlenen Maßnahmen ergreifen.

Um diese Prüfung für alle an der Sitzungsstartsequenz beteiligten Komponenten auszuführen, können Sie jetzt die Ergebnisse der Überprüfung der Endpunkte einsehen. Durch Klicken auf **Endpoint Device** in der Liste der Komponenten wird der Status der Device Posture-Überprüfung angezeigt. Der Device Posture-Dienst überprüft das Endgerät auf der Grundlage der vom Administrator definierten Richtlinien auf Richtlinientreue.

Stellen Sie sicher, dass der Device Posture-Dienst mit DaaS konfiguriert (siehe Device Posture). Eine Beschreibung der von Device Posture protokollierte Fehler finden Sie unter Device Posture Error Logs.

Weitere Informationen finden Sie unter Schritte zur Fehlerdiagnose beim Sitzungsstart

Neue Optionen in der vollständigen Konfiguration zum Routing von API-Anforderungen an Azure und GCP über Citrix Cloud Connectors. Bisher konnten API-Anforderungen an Azure und GCP nur über öffentliche Endpunkte geleitet werden. Mit der neuen Option unter **Vollständige Konfiguration > Verbindung und Ressourcen hinzufügen** können Sie sich jetzt für mehr Sicherheit entscheiden, indem Sie sie über Citrix Cloud Connectors leiten. Weitere Informationen finden Sie unter Dienstprinzipal und Verbindung gemeinsam in "Vollständige Konfiguration"erstellen.

Verbesserungen von Suche und Filtern. Die folgenden Verbesserungen wurden vorgenommen, um die Suche zu verbessern:

- **Vereinfachte Suche**: Für die Suche ohne Filter wurden die Suchempfehlungen entfernt, sodass eine übersichtliche und unkomplizierte Suche möglich ist.

- **AND/OR-Operatoren**: Die Optionen "Übereinstimmung mit allen (AND-Operator)"und "Beliebige Übereinstimmung (OR-Operator)"sind jetzt im Filterbereich per Mausklick auf das Filtersymbol verfügbar.
- **Optimierte Filterkonfiguration:** Im Filterbereich können Sie jetzt mehrere Filter nahtlos angeben und anwenden.
- **Übersichtlichere Oberfläche:** Die Funktion zum Anheften von Filtern wurde entfernt, wodurch die Benutzeroberfläche übersichtlicher und die Suche intuitiver wurde.
- **Schnelles Hinzufügen von Filtern**: Nachdem Sie Filter angewendet haben, können Sie jetzt das Pluszeichen verwenden, um schnell einen weiteren Filter hinzuzufügen.
- **Gespeicherte Filtersätze löschen**: Sie können gespeicherte Filtersätze jetzt ganz einfach über das Suchmenü löschen, ohne zu **Filtersätze verwalten** zu wechseln.

Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

VDA-Upgrade-Unterstützung für mit Azure Quick Deploy erstellte Maschinenkataloge. Mit der vollständigen Konfiguration können Sie jetzt **VDA-Upgrade** für Maschinenkataloge aktivieren, die mit Azure Quick Deploy erstellt wurden, und dann über die Option **VDA aktualisieren** sofortige oder geplante Upgrades durchführen. Weitere Informationen finden Sie unter Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration".

Zurücksetzen des OS-Datenträgers einer persistenten VM in einem mit MCS erstellten Maschinenkatalog in SCVMM. Sie können jetzt den PowerShell-Befehl `Reset-ProvVMDisk` verwenden, um den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog zurückzusetzen. Das Feature automatisiert den Vorgang des Zurücksetzens des OS-Datenträgers. Beispielsweise hilft es beim Zurücksetzen der VM auf den Anfangsstatus eines persistenten Entwicklungsdesktopkatalogs, der mit MCS erstellt wurde. Derzeit ist dieses Feature auf Azure-, Citrix Hypervisor-, SCVMM- und VMware-Virtualisierungsumgebungen anwendbar. Weitere Informationen zum Verwenden des PowerShell-Befehls zum Zurücksetzen des OS-Datenträgers finden Sie unter OS-Datenträger zurücksetzen.

Eigenschaften einzelner VMs aktualisieren. Sie können jetzt die Eigenschaften einzelner VMs in einem persistenten MCS-Maschinenkatalog mithilfe eines PowerShell-Befehls aktualisieren. Mithilfe dieser Implementierung können Sie einzelne VMs effizient verwalten, ohne den gesamten Maschinenkatalog aktualisieren zu müssen. Derzeit gilt dieses Feature nur für die Azure-Umgebung. Weitere Informationen finden Sie unter Eigenschaften einzelner VMs aktualisieren.

Einschränken von Up- und Download verwalteter Datenträger. Gemäß Azure-Richtlinie können Sie nicht mehr als fünf Datenträger oder Snapshots gleichzeitig mit demselben Datenträgerzugriffsobjekt hoch- oder herunterladen. Mit diesem Feature wird das Limit von fünf gleichzeitigen Uploads oder Downloads nicht durchgesetzt, wenn Sie:

- `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` konfiguri-

eren und

- die Azure-Richtlinie nicht so konfigurieren, dass Datenträgerzugriffe für jeden neuen Datenträger zur Verwendung privater Endpunkte automatisch erstellt werden.

Unterstützung für die Zuweisung eines Laufwerksbuchstabens zu einem MCS-E/A-Zurückschreibcache-Datenträger. Bisher wies Windows dem MCS-E/A-Zurückschreibcache-Datenträger automatisch einen Laufwerksbuchstaben zu. Mit diesem Feature können Sie jetzt dem MCS-E/A-Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zuweisen. Diese Implementierung hilft bei der Vermeidung von Konflikten zwischen dem Laufwerksbuchstaben verwendeter Anwendungen und dem Laufwerksbuchstaben des MCS-E/A-Zurückschreibcache-Datenträgers. Das Feature gilt nur für Windows-Betriebssysteme. Weitere Informationen finden Sie unter Laufwerksbuchstaben zu einem MCS-E/A-Zurückschreibcache-Datenträger zuweisen.

Unterstützung für Maschinenprofile in Citrix Hypervisor. In Citrix Hypervisor können Sie jetzt einen MCS-Maschinenkatalog mithilfe eines Maschinenprofils erstellen. Die Quelle der Eingabe des Maschinenprofils ist eine VM. Das Maschinenprofil erfasst die Hardwareeigenschaften aus einer VM-Vorlage und wendet sie auf die neu bereitgestellten virtuellen Maschinen im Katalog an. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Maschinenprofils.

Wiederholung der Katalogerstellung nach Fehler. Wenn die Katalogerstellung fehlschlägt, können Sie jetzt erneut versuchen, den Katalog zu erstellen. Zur Gewährleistung einer erfolgreichen Erstellung prüfen Sie die Informationen zur Problembehandlung und beheben Sie die Probleme. Die Informationen beschreiben die Probleme und enthalten Empfehlungen zu deren Behebung. Fehlerhafte Kataloge sind mit einem Fehlersymbol gekennzeichnet. Zum Anzeigen von Details gehen Sie zur Registerkarte **Problembehandlung** des jeweiligen Katalogs. Weitere Informationen finden Sie unter Verwalten von Maschinenkatalogen.

Berechtigung zur Verwaltung von Konfigurationssätzen. Um eine präzise Steuerung der Verwaltung von WEM-Konfigurationssätzen zu ermöglichen, gibt es jetzt die neue Berechtigung **Konfigurationssätze verwalten** für den **Maschinenkatalog**-Berechtigungssatz. Diese Berechtigung gewährt Benutzern exklusiven Zugriff, die Aufgaben wie das Binden oder Aufheben der Bindung eines Konfigurationssatzes und das Wechseln zu einem anderen Konfigurationssatz für Kataloge ausführen können. Weitere Informationen finden Sie unter Verwalten eines Konfigurationssatzes für einen Katalog.

Neue Option in der vollständigen Konfiguration zur Bereinigung veralteter, in Azure AD eingebundener Geräte. In der vollständigen Konfiguration gibt es eine neue Option zur Vereinfachung der Bereinigung veralteter, in Azure AD eingebundener Geräte in Citrix DaaS. Bisher mussten Sie hierzu ein benutzerdefiniertes PowerShell-Skript ausführen. Wenn Sie die Option aktivieren, können Verbindungen veraltete, in Azure AD eingebundene Geräte automatisch bereinigen. Weitere Informationen finden Sie unter Azure-Hostverbindungen.

Überwachen des Imageupdatestatus für Kataloge mit der vollständigen Konfiguration. Sie

können jetzt den Imageupdatestatus für nicht persistente Maschinenkataloge über die neue Spalte **Imageupdate** überwachen. Diese Spalte gibt an, ob die Images eines Katalogs **vollständig aktualisiert** oder **teilweise aktualisiert** sind oder ihr **Update ausstehend** ist.

Gehen Sie wie folgt vor, um die Spalte in der Tabelle **Maschinenkataloge** anzuzeigen:

1. Wählen Sie im Knoten **Maschinenkataloge** das Symbol **Anzuzeigende Spalten** in der Aktionsleiste aus.
2. Wählen Sie **Maschinenkatalog > Imagestatus**.
3. Klicken Sie auf **Speichern**.

Das Anzeigen der Spalte **Imageupdate** kann die Leistung der Konsole beeinträchtigen. Wir empfehlen, sie nur bei Bedarf anzuzeigen.

Sichere Umgebung für von GCP verwalteten Netzwerkverkehr. Mit diesem Feature können Sie jetzt den Google-Zugriff auf Ihre Google Cloud-Projekte auf den privaten Zugriff einschränken. Diese Implementierung erhöht die Sicherheit beim Umgang mit vertraulichen Daten. Fügen Sie hierfür bei einer Citrix Cloud-Bereitstellung `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` hinzu. Wenn Sie einen privaten Pool verwenden, fügen Sie `UsePrivateWorkerPool` zu `CustomProperties` hinzu. Weitere Informationen finden Sie unter Sichere Umgebung für von GCP verwalteten Netzwerkverkehr erstellen.

Juli 2023

Neue und erweiterte Features

Unterstützung für das Abrufen einer Liste verwaister Ressourcen in Azure. In Azure-Umgebungen können Sie jetzt eine Liste der verwaisten Ressourcen abrufen, die von MCS erstellt wurden, aber nicht mehr verwendet werden. Das Feature hilft, unnötige Kosten zu vermeiden. Weitere Informationen finden Sie unter Liste verwaister Ressourcen abrufen.

Unterstützung für das Erstellen persistenter Maschinen mit Multisitzungs-OS in "Vollständige Konfiguration". Wenn Sie einen Katalog mit Maschinen mit Multisitzungs-OS erstellen, können Sie jetzt angeben, ob sie persistent sein sollen. Beachten Sie bei persistenten Maschinen mit Multisitzungs-OS, dass vom Benutzer am Desktop vorgenommene Änderungen gespeichert werden und für alle autorisierten Benutzer zugänglich sind. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Neue Funktion zum Filtern des AWS-AMI-Inventars in "Vollständige Konfiguration". Bei Auswahl von Maschinenvorlagen während der AWS-Katalogerstellung können Sie jetzt das AWS-AMI-Inventar anhand folgender Suchkriterien nach einer Zielvorlage filtern:

- Imagename

- Image-ID
- Image-Tags

Die Maschinenvorlagenliste wird dynamisch geladen, wenn Sie in der Liste nach unten scrollen. Zunächst werden 25 Elemente geladen, die beim Scrollen um weitere ergänzt werden.

Unterstützung für das Löschen von Azure AD-Geräten. Mit diesem Feature können veraltete Azure AD-Geräte fortlaufend gelöscht werden, indem dem Dienstprinzipal die Rolle "Cloud Device Administrator"zugewiesen und die benutzerdefinierte Eigenschaft der Hostverbindung geändert wird. Wenn Sie veraltete Azure AD-Geräte nicht löschen, bleibt die zugehörige nicht-persistente VM im Initialisierungsstatus, bis Sie sie manuell aus dem Azure AD-Portal entfernen. Weitere Informationen finden Sie unter Kataloge mit Einbindung in Azure Active Directory erstellen.

Unterstützung für Maschinenprofile in AWS-Umgebungen. Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS in AWS erstellen, können Sie jetzt ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer EC2-Instanz (VM) oder einer Startvorlagenversion erfasst und auf die bereitgestellten VMs anwendet. Erfasst werden können beispielsweise EBS-Volumeeigenschaften, Instanztyp, EBS-Optimierung und weitere unterstützte AWS-Konfigurationen. Beim Bearbeiten eines Katalogs kann das Maschinenprofil der Maschinen geändert werden, indem eine andere VM oder Startvorlage bereitgestellt wird. Weitere Informationen finden Sie unter Maschinenkatalog mithilfe eines Maschinenprofils erstellen.

Das Exportlimit für Suchergebnisse wurde von 10.000 auf 30.000 erhöht. Wir haben das Exportlimit für Suchergebnisse erhöht. Bisher war das Exportlimit auf 10.000 Elemente beschränkt. Jetzt können Sie bis zu 30.000 Elemente in eine CSV-Datei exportieren. Weitere Informationen finden Sie unter Suchergebnissen in eine CSV-Datei exportieren.

Option zur Imageaktualisierung. Bei der Auswahl von Masterimages für Maschinenkataloge können Sie jetzt mit der Option **Aktualisieren** (oben rechts im Bildschirm) schnell die aktuelle Liste mit Masterimages abrufen. Beachten Sie, dass die Option **Aktualisieren** für AWS-Kataloge nicht verfügbar ist. Zusätzlich ist eine Option zum **Aktualisieren** für Maschinenprofile und Hostgruppen in Azure-Katalogen verfügbar.

Juni 2023

Neue und erweiterte Features

Unterstützung für das Abrufen benutzerdefinierter Eigenschaften aus der Maschinenprofileingabe in GCP. Bisher mussten Sie in GCP-Umgebungen beim Erstellen eines MCS-Maschinenkatalogs mithilfe einer Maschinenprofileingabe die benutzerdefinierten Eigenschaften explizit angeben. Dies bedeutete zusätzliche Arbeit. Mit diesem Feature können Sie jetzt die folgenden benutzerdefinierten Eigenschaften abrufen, ohne sie explizit anzugeben:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

Wenn Sie die Befehle `New-ProvScheme` und `Set-ProvScheme` ausführen und die benutzerdefinierten Eigenschaften nicht explizit angeben, werden die Werte aus der Eingabe des Maschinenprofils abgerufen.

`New-ProvScheme -MachineProfile` schreibt beispielsweise den Maschinentyp im Maschinenprofil in die Eigenschaft `ServiceOffering` des Provisioningschemas, es sei denn, Sie geben `ServiceOffering` im Befehl `New-ProvScheme` an. Wenn Sie `Set-ProvVMScheme` zweimal ausführen, wird der neueste Befehl wirksam.

Tags in AWS-Umgebungen entfernen. Bisher wurden mit den PowerShell-Befehlen `Remove-ProvVM` und `Remove-ProvScheme` mit dem Parameter `ForgetVM` die VMs und Maschinenkataloge aus der Citrix Datenbank entfernt. Die Tags wurden jedoch nicht entfernt. Die nicht vollständig aus allen Ressourcen entfernten VMs und Maschinenkataloge mussten einzeln behandelt werden. Mit diesem Feature können Sie Folgendes verwenden:

- `Remove-ProvVM` mit dem Parameter `ForgetVM` zum Entfernen von VMs und Tags aus einer einzelnen VM oder einer Liste von VMs aus einem Maschinenkatalog.
- `Remove-ProvScheme` mit Parameter `ForgetVM` zum Entfernen eines Maschinenkatalogs aus der Citrix Datenbank und von Ressourcen aus einem Maschinenkatalog.

Diese Implementierung hilft bei Folgendem:

- Identifizierung von Ressourcenlecks
- Vermeidung von Kosten für die Wartung nicht benötigter Ressourcen

Dieses Feature ist nur für persistente VMs verfügbar. Weitere Informationen finden Sie unter Tags entfernen.

Möglichkeit, historische Fehler und Warnungen für einen MCS-Maschinenkatalog abzurufen. Bisher wurden nur die neuesten Warnungen und Fehler für Maschinenkataloge angezeigt. Mit diesem Feature können Sie jetzt eine Liste der historischen Warnungen und Fehler für einen MCS-Maschinenkatalog abrufen. Anhand der Liste können Sie Probleme mit dem MCS-Maschinenkatalog diagnostizieren und beheben.

Weitere Informationen finden Sie unter Mit einem Katalog verknüpfte Fehler und Warnungen abrufen.

Höhere Kapazität mit verbesserter Leistung für Citrix in Google Cloud. Citrix kann jetzt Kataloge mit bis zu 3.000 VDAs in einem Google Cloud-Projekt unterstützen. Dieses Update bedeutet eine Leistungsverbesserung für die Bereitstellung und die Energieverwaltung.

Zurücksetzen des OS-Datenträgers einer persistenten VM in einem mit MCS erstellten Maschinenkatalog in einer Google Cloud- oder AWS-Umgebung. Sie können jetzt den PowerShell-Befehl `Reset-ProvVMDisk` verwenden, um den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog zurückzusetzen. Das Feature automatisiert den Vorgang des Zurücksetzens des OS-Datenträgers. Beispielsweise hilft es beim Zurücksetzen der VM auf den Anfangsstatus eines persistenten Entwicklungsdesktopkatalogs, der mit MCS erstellt wurde. Derzeit ist dieses Feature auf AWS-, Azure-, Citrix Hypervisor-, Google Cloud- und VMware-Virtualisierungsumgebungen anwendbar. Weitere Informationen zum Verwenden des PowerShell-Befehls zum Zurücksetzen des OS-Datenträgers finden Sie unter OS-Datenträger zurücksetzen.

Unterstützung für das Ändern datenträgerbezogener benutzerdefinierter Eigenschaften eines Katalogs und der VMs des Katalogs in GCP. Bisher konnten Sie in GCP-Umgebungen benutzerdefinierte Eigenschaften nur bei der Erstellung eines MCS-Maschinenkatalogs hinzufügen. Mit diesem Feature können Sie nun die folgenden datenträgerbezogenen benutzerdefinierten Eigenschaften eines Katalogs und der VMs des Katalogs ändern.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

Diese Implementierung hilft Ihnen, auch nach der Erstellung eines Katalogs verschiedene Speichertypen für verschiedene Datenträger auszuwählen und so den Preisen für die verschiedenen Speichertypen Rechnung zu tragen. Weitere Informationen finden Sie unter Datenträgerbezogene benutzerdefinierte Eigenschaften eines Katalogs ändern.

Unterstützung für dynamisches Sitzungstimeout erweitert auf VDA-Version 2203 LTSR CU3 und höher. Für Bereitstellungsgruppen mit Einzelsitzungs-OS gilt dieses Feature jetzt für VDAs ab Version 2206 CR oder 2203 LTSR CU3 oder höher. Weitere Informationen finden Sie unter Dynamische Sitzungstimeouts.

Erstellen von Hostverbindungen in "Vollständiger Konfiguration"verbessert. Nach der Auswahl eines Ressourcenstandorts werden jetzt in der Dropdownliste **Verbindungstyp** alle von Citrix unterstützten Hypervisors und Clouddienste angezeigt, deren Verfügbarkeit von folgenden Faktoren abhängt:

- Für einen Ressourcenstandort ohne Zugriff auf Cloud Connectors sind nur Hypervisors und Clouddienste verfügbar, die Bereitstellungen ohne Connector unterstützen.
- Für einen Ressourcenstandort mit Zugriff auf Cloud Connectors sind nur Hypervisors und Clouddienste verfügbar, deren Plug-Ins ordnungsgemäß auf den Connectors installiert sind.

Weitere Informationen finden Sie unter Verbindungen erstellen und verwalten.

Zusätzliche Komponentenauswahl beim VDA-Upgrade. Bei einem VDA-Upgrade können Sie jetzt auswählen, welche zusätzlichen Komponenten aktualisiert oder installiert werden sollen. Weitere Informationen finden Sie unter Automatische Upgrades für VDAs konfigurieren.

> **Wichtig:**
>
> Um das Feature für zusätzliche Komponenten zu nutzen, müssen Sie den VDA-Upgrade-Agent Version 7.34 oder höher verwenden, der im VDA-Installationsprogramm Version 2206 oder höher enthalten ist.

Unter "Vollständige Konfiguration"sind jetzt bestimmte Einstellungen für Azure-Maschinen auf der Basis von Maschinenprofilen vorkonfiguriert. Beim Provisioning von Azure-VMs sind jetzt in "Vollständige Konfiguration"die folgenden Einstellungen je nach gewähltem Maschinenprofil vorkonfiguriert:

- Hostgruppe
- Datenträgerverschlüsselungssatz
- Verfügbarkeitszone
- Lizenztyp

Unterstützung für den Ruhezustand von AWS-Instanzen. Sie können jetzt AWS-Instanzen starten, sie wie gewünscht einrichten und in den Ruhezustand versetzen. Beim Ruhezustand wird der In-Memory-Status der Instanz samt privater und elastischer IP-Adressen gespeichert, sodass Benutzer genau dort weitermachen kann, wo sie aufgehört haben. Weitere Informationen zum Erstellen von VMs, die den Ruhezustand unterstützen, finden Sie unter Ruhezustand von Instanzen.

Unterstützung für das Optimieren der AWS-Drosselung. Sie können jetzt eine große Anzahl Maschinen in einem AWS-Katalog ein- und ausschalten, ohne dass Drosselungsprobleme auftreten. Drosselungsprobleme treten auf, wenn die Anzahl der an AWS gesendeten Anforderungen die Anzahl von Anforderungen überschreitet, die der Server verarbeiten kann. Dieses Feature erhöht die Effizienz, da die Anzahl der AWS-Aufrufe zum massenhaften Ein- und Ausschalten von Maschinen reduziert wird. Das Ein- und Ausschalten von Maschinen in persistenten Katalogen wird ebenfalls deutlich beschleunigt.

Sichere Umgebung für von Azure verwalteten Netzwerkverkehr. Bisher mussten Sie auf das öffentliche Internet vertrauen, um Ihre Azure-Endgeräte mit Ressourcen in Ihrer Umgebung interagieren zu lassen. Infolgedessen wurden Sicherheitsbedenken laut, da auf das öffentliche Internet zugegriffen wurde. Mit diesem Feature ermöglicht MCS die Weiterleitung von Netzwerkverkehr über Citrix Cloud Connectors in Ihrer Umgebung. Dies macht die Umgebung sicher, da jetzt der gesamte von Azure verwaltete Netzwerkverkehr aus Ihrer eigenen Umgebung stammt. Fügen Sie hierfür `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` hinzu. Weitere Informationen finden Sie unter Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen.

Nachdem Sie die benutzerdefinierten Eigenschaften festgelegt haben, können Sie Azure-Richtlinien konfigurieren, um einen privaten Zugriff auf Azure Managed Disks einzurichten.

Unterstützung für das Provisioning von Katalog-VMs mit Azure Monitor Agent. Azure Monitor Agent (AMA) sammelt Überwachungsdaten und übermittelt sie an Azure Monitor. Mit diesem Feature können Sie MCS-Maschinenkatalog-VMs (persistent und nicht persistent) bereitstellen, auf denen AMA als Erweiterung installiert ist. Die Überwachung wird durch eindeutige Identifizierung der VMs in den Überwachungsdaten ermöglicht. Weitere Informationen zu AMA finden Sie unter Azure Monitor Agent overview.

Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Weitere Informationen zum Provisioning von Maschinenkatalog-VMs mit aktiviertem AMA finden Sie unter Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent.

Neustartzeitplan für einen MCS-Katalog aktivieren. Bisher konnten Sie für Image-Updates auf den nächsten Neustart warten oder einen sofortigen Neustart aller VMs auslösen. Mit diesem Feature können Sie nun einen einmaligen Katalogneustart planen, der an einem gewünschten Datum und zu einer gewünschten Uhrzeit ausgelöst wird, um MCS-Imageupdates zu ermöglichen. Verwenden Sie den Befehl `BrokerCatalogRebootSchedule`, um einen Neustartzeitplan zu erstellen. Weitere Informationen finden Sie unter Masterimage ändern.

Verwalten abgelaufener geheimer Clientschlüssel in Azure Quick Deploy. In Azure Quick Deploy können Sie sich jetzt durch Benachrichtigungen informieren lassen, wenn geheime Clientschlüssel ablaufen, und diese mühelos aktualisieren, um einen kontinuierlichen Zugriff auf Azure-Ressourcen zu gewährleisten. Weitere Informationen finden Sie unter Abgelaufene geheime Clientschlüssel aktualisieren.

Mai 2023

Neue und erweiterte Features

Verbesserung der Suche. Dieses Feature verbessert die Darstellung und die Interaktionen für Filter und erleichtert so die Suche. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Neue Richtlinie zum Ausschluss von Benutzern, mit deren Hilfe Sie Pfade definieren können, die nicht an den Benutzerlayer umgeleitet werden. Benutzerausschlüsse gelten für den Benutzerpersonalisierungslayer (UPL), nicht jedoch für den Sitzungshost. Logoff.txt enthält jetzt alle aktiven Benutzerausschlüsse. Weitere Informationen finden Sie unter Benutzerpersonalisierungslayer.

Unterstützung für die Aktualisierung der Hardwareversion neuer VMs, die in einem MCS-Maschinenkatalog hinzugefügt wurden. In einer VMware-Umgebung können Sie jetzt die Hardwareversion der neuen, einem MCS-Maschinenkatalog hinzugefügten virtuellen Maschinen

mithilfe einer Maschinenprofilquelle aktualisieren. Sie müssen keinen neuen Maschinenkatalog erstellen, um die Hardwareversion der einem Katalog hinzugefügten VMs zu aktualisieren. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um dieses Feature zu nutzen.

Unterstützung für das Filtern von AWS-VM-Instanzen. Bei Verwendung einer AWS-VM-Instanz als Maschinenprofileingabe bei der Erstellung eines MCS-Maschinenkatalogs wurde der Katalog bisher möglicherweise nicht richtig erstellt oder funktionierte nicht richtig, weil die Maschinenprofileingabe ungültig war. Mit diesen Feature können Sie jetzt die AWS-VM-Instanzen auflisten, die als gültige Maschinenprofil-VMs verwendet werden können. Verwenden Sie dazu den Befehl `Get-HypInventoryItem`. Weitere Informationen finden Sie unter VM-Instanzen filtern.

Unterstützung für die Konvertierung eines Maschinenkatalogs, der nicht auf Maschinenprofilen basiert, in einen maschinenprofilbasierten Maschinenkatalog in einer Azure-Umgebung. In der Azure-Umgebung können Sie jetzt eine VM oder eine Vorlagenspezifikation als Maschinenprofileingabe verwenden, um einen Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog zu konvertieren. Vorhandene und neue virtuelle Maschinen, die dem Katalog hinzugefügt werden, übernehmen Eigenschaftswerte aus dem Maschinenprofil, sofern sie nicht durch explizite benutzerdefinierte Eigenschaften überschrieben werden. Weitere Informationen finden Sie unter Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog in einer Azure-Umgebung konvertieren.

Unterstützung für doppelte Verschlüsselung auf verwalteten Datenträgern in der Azure-Umgebung. In der Azure-Umgebung können Sie jetzt einen MCS-Maschinenkatalog mit doppelter Verschlüsselung erstellen. Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der vom Kunden verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt. Weitere Informationen finden Sie unter Doppelte Verschlüsselung verwalteter Datenträger.

Unterstützung für Maschinenprofile in VMware. In VMware-Umgebungen können Sie jetzt einen MCS-Maschinenkatalog mithilfe eines Maschinenprofils erstellen. Die Quelle der Eingabe des Maschinenprofils ist eine VMware-Vorlage. Das Maschinenprofil erfasst die Hardwareeigenschaften aus einer VMware-Vorlage und wendet sie auf die neu bereitgestellten virtuellen Maschinen im Katalog an. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Maschinenprofils.

Möglichkeit, den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog in Azure und Citrix Hypervisor zurückzusetzen. Sie können jetzt den PowerShell-Befehl `Reset-ProvVMDisk` verwenden, um den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog zurückzusetzen. Das Feature automatisiert den Vorgang

des Zurücksetzens des OS-Datenträgers. Beispielsweise hilft es beim Zurücksetzen der VM auf den Anfangsstatus eines persistenten Entwicklungsdesktopkatalogs, der mit MCS erstellt wurde. Derzeit ist dieses Feature auf Azure-, Citrix Hypervisor- und VMware-Virtualisierungsumgebungen anwendbar. Weitere Informationen zum Verwenden des PowerShell-Befehls zum Zurücksetzen des OS-Datenträgers finden Sie unter OS-Datenträger zurücksetzen.

Verbesserte Erfahrung beim Erstellen von Hostverbindungen. Sie können jetzt die folgenden Informationen abrufen, während Sie eine Hostverbindung erstellen:

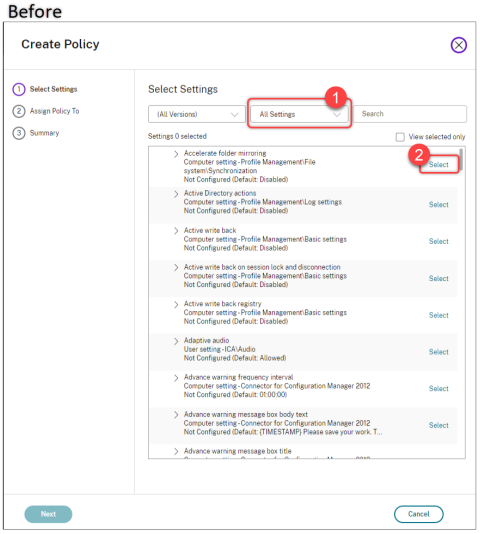
- Liste aller von Citrix unterstützten Hypervisor-Plug-Ins, einschließlich derer von Drittanbietern
- Verfügbarkeit von Hypervisor-Plug-Ins. Wenn der Verfügbarkeitsstatus "false"ist, könnte dies daran liegen, dass der Cloud Connector nicht installiert ist.

Dieses Feature hilft Ihnen bei der korrekten Einrichtung eines Ressourcenstandorts und somit bei der Erstellung einer Hostverbindung. Weitere Informationen finden Sie unter Schritt 1. Verbindung.

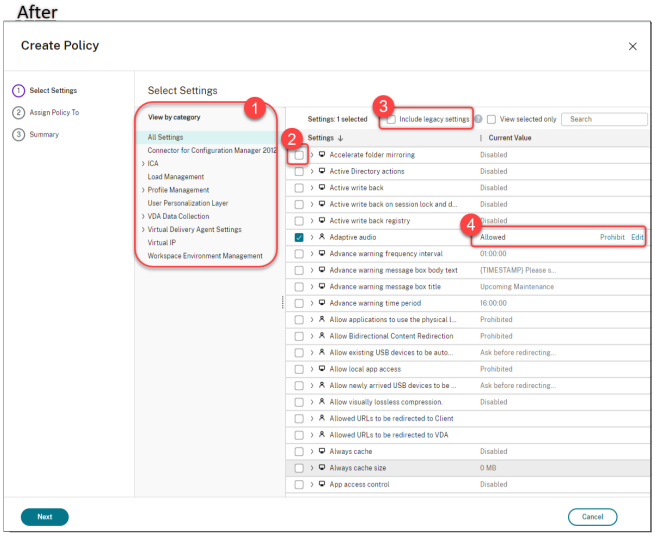
Verbesserungen der Benutzererfahrung für den Knoten "Richtlinien". Zur Verbesserung der Benutzererfahrung und zur effizienteren Richtlinienverwaltung haben wir die folgenden Verbesserungen am Knoten **Vollständige Konfiguration > Richtlinien** vorgenommen:

- Neues UI-Design für die Aktionen **Richtlinie erstellen** und **Vorlage erstellen**:
  - Erweiterbare Ordneranzeige für Richtlinieneinstellungen. Auf der Seite **Einstellungen auswählen** werden alle Einstellungen nach Kategorien in einer erweiterbaren Strukturansicht angezeigt, sodass sie sich leichter finden lassen.
  - Um eine Einstellung auszuwählen, klicken Sie einfach auf ein Kontrollkästchen, anstatt auf die Schaltfläche **Auswählen**.
  - Legacy-Einstellungen sind standardmäßig ausgeblendet, sodass nur die relevantesten Einstellungen angezeigt werden. Wenn Legacy-Einstellungen erforderlich sind, wählen Sie **Legacy-Einstellungen einschließen**.
  - Neben einer booleschen Einstellung gibt es nun eine Aktionsschaltfläche zur direkten Änderung des Werts in der Einstellungsliste.

Before

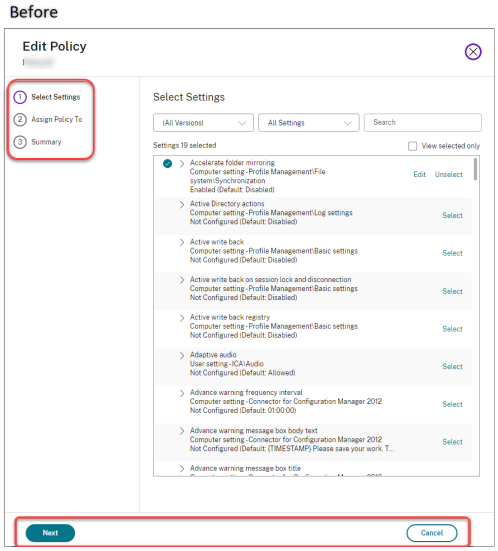


After

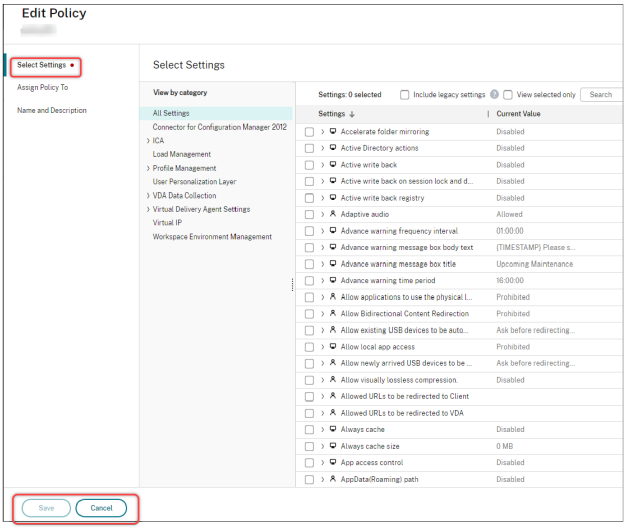


- Neues UI-Design für die Aktion **Richtlinie bearbeiten**:
  - Das Navigationsmenü wurde in eine ungeordnete Liste geändert. Jedes Listenelement enthält jetzt eine Schaltfläche **Speichern** auf seiner Seite. Dank dem neuen Design können Sie an einem Element vorgenommene Änderungen speichern, ohne durch alle Elemente im Navigationsmenü gehen zu müssen. Diese Änderung macht die Richtlinienverwaltung effizienter und rationeller.
  - Rote Punkte neben Navigationselementen weisen auf Einstellungsfehler hin.

Before



After



- Richtlinien können per Ziehen mit der Maus neu priorisiert werden. In der Prioritätenliste können Sie jetzt die Priorität einer Richtlinie ändern, indem Sie sie an die gewünschte Position ziehen.

Neue Option zum Deaktivieren der erzwungenen Benutzerabmeldung für AutoScale. Die neue Option **Weder benachrichtigen noch Benutzerabmeldung erzwingen** ist jetzt auf der Seite **Au-**

toscale verwalten > Abmeldebenachrichtigungen für Benutzer verfügbar. Wird diese Option ausgewählt, erzwingt Autoscale keine Abmeldung der Benutzer von Maschinen im Drainingzustand und es sendet keine Benachrichtigung an die Benutzer, dass sie sich abmelden und bei einer anderen Maschine anmelden sollen. Weitere Informationen finden Sie unter Benachrichtigungen zur Benutzerabmeldung.

Möglichkeit zum Neustarten von Windows 365 Cloud-PCs. Sie können jetzt Citrix DaaS verwenden, um Windows 365-Cloud-PCs neu zu starten.

Zusätzliche Sitzungsdetails. Wenn Sie eine Sitzung unter **Vollständige Konfiguration > Suchen > Sitzungen** anzeigen, enthält die Sitzungsansicht (im unteren Bereich) jetzt weitere Sitzungsdetails, die Ihnen bei der Behebung und Identifizierung von Clientproblemen helfen:

- **Wiederverbindungszeit.** Zeitpunkt, zu dem eine Sitzung nach dem Trennen wiederverbunden wurde.
- **Clientplattform.** Plattform, auf der die Sitzung gestartet wurde.
- **Clientversion.** Version der Clientplattform, die zum Starten der Sitzung verwendet wurde.
- **Remotehost-IP.** IP-Adresse des Remotehosts, auf dem Citrix Workspace gehostet wird.

Unterstützung für das Umbenennen von Azure AD-Sicherheitsgruppen für VMs. Für VMs, die über Citrix DaaS zu einer Azure AD-Sicherheitsgruppe hinzugefügt wurden, können Sie die Sicherheitsgruppe jetzt über **Vollständige Konfiguration > Maschinenkatalog bearbeiten** umbenennen. Der neue Name tritt in Kraft, wenn Sie die Änderung gespeichert haben.

Standarddomänenauswahl für Maschinenkonten. Wenn Sie einen Katalog erstellen, wird die Domäne, in der sich die Ressource (Verbindung) befindet, standardmäßig für Maschinenkonten ausgewählt.

Möglichkeit, Azure AD-zugewiesene Sicherheitsgruppen anzuzeigen, denen VMs beitreten können. Wenn Sie in der vollständigen Konfiguration mit Azure Active Directory verbundene VMs erstellen, steht jetzt die Option **Einer zugewiesenen Sicherheitsgruppe als Mitglied beitreten** zur Verfügung, mit der Sie die Azure AD-Sicherheitsgruppe, in der die VMs residieren, einer zugewiesenen Sicherheitsgruppe hinzufügen können. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Unterstützung für das Wechseln des Netzwerks für Verbindungen. In der vollständigen Konfiguration können Sie jetzt die Netzwerke für eine Verbindung ändern. Sie können die Verknüpfung von Netzwerken mit einer Verbindung nicht aufheben, wenn die Netzwerke in Verwendung sind. Weitere Informationen finden Sie unter Netzwerk bearbeiten.

Möglichkeit, Tags in Azure-Umgebungen zu entfernen. Bisher wurden mit den PowerShell-Befehlen `Remove-ProvVM` und `Remove-ProvScheme` mit dem Parameter `ForgetVM` die VMs und Maschinenkataloge aus der Citrix Datenbank entfernt. Die Tags wurden jedoch nicht von den Ressourcen entfernt. Die nicht vollständig aus allen Ressourcen gelöschten VMs und

Maschinenkataloge mussten einzeln behandelt werden. Mit diesem Feature können Sie Folgendes verwenden:

- `Remove-ProvVM` mit dem Parameter `ForgetVM` zum Entfernen von VMs und für die Ressourcen erstellten Tags aus einer einzelnen VM oder einer Liste von VMs aus einem Maschinenkatalog.
- `Remove-ProvScheme` mit Parameter `ForgetVM` zum Entfernen eines Maschinenkatalogs aus der Citrix Datenbank und von für die Ressourcen erstellten Tags aus einem gesamten Maschinenkatalog.

Diese Implementierung hilft bei der Identifizierung verwaister Ressourcen, die von MCS erstellt wurden aber nicht mehr von MCS verwendet werden.

Dieses Feature ist nur für persistente VMs verfügbar. Weitere Informationen finden Sie unter Tags entfernen.

Warnung "Fehlerhafte Maschinen". Das Feature für Proaktive Benachrichtigungen und Warnmeldungen in Director wurde um die neue Warnung "Fehlerhafte Maschinen (in %)"erweitert, die auf dem Prozentsatz fehlerhafter Maschinen in einer Bereitstellungsgruppe basiert. Mit der neuen Warnbedingung können Sie Schwellenwerte für Warnungen als Prozentsatz fehlerhafter Maschinen in einer Bereitstellungsgruppe konfigurieren. Weitere Informationen finden Sie im Abschnitt Fehlerhafte Maschinen im Artikel zu Warnungen.

April 2023

Neue und erweiterte Features

Veröffentlichen in spezifischen Cloudplattformen mithilfe von Citrix Provisioning in Image Portability Service. Workflows zur Verwendung von Image Portability Service für die Veröffentlichung in AWS, Azure und Google Cloud sind jetzt verfügbar. Darüber hinaus wurden die erforderlichen Berechtigungen für Azure und Netzwerke aktualisiert. Weitere Informationen finden Sie unter Workloads in die öffentliche Cloud migrieren.

Unterstützung für die Ermittlung der Ursache für Maschinen im Wartungsmodus. Bisher war es nur mit PowerShell möglich, die Ursache für den Wartungsmodus von Maschinen zu ermitteln. Jetzt ist dies auch in der Schnittstelle "Vollständige Konfiguration"möglich:

1. Verwenden Sie Suchen, um die Maschine zu finden.
2. Überprüfen Sie im unteren Bereich auf der Registerkarte **Details** die Option **Wartungsgrund**. Oder zeigen Sie mit der Maus auf die Spalte **Wartungsmodus**. Die folgenden Informationen können angezeigt werden:

- By Administrator: Ein Administrator hat die Maschine in den Wartungsmodus versetzt.

- Maximum Failed Registrations: Die Maschine hat die maximal zulässige Anzahl an Registrierungsversuchen überschritten.

Außerdem ist jetzt ein Filter für den **Wartungsgrund** verfügbar. Sie können ihn verwenden, um die Zielmaschinen zu identifizieren.

Anhand dieses Features können Administratoren Probleme mit Maschinen im Wartungsmodus beheben.

Verwenden von Variablen, um Benutzer über die verbleibende Zeit zu informieren, bevor sie abgemeldet werden. Wenn Sie die Benutzerabmeldung erzwingen, können Sie jetzt `%s%` oder `%m%` als Variablen verwenden, um die angegebene Uhrzeit in der Benachrichtigung anzugeben. Um die Zeit in Sekunden auszudrücken, verwenden Sie `%s%`. Um die Zeit in Minuten auszudrücken, verwenden Sie `%m%`. Weitere Informationen finden Sie unter Benachrichtigungen zur Benutzerabmeldung.

Unterstützung für die Anpassung des Einschaltverhaltens bei einem Fehler beim Ändern des Speichertyps. Beim Einschalten kann der Speichertyp eines verwalteten Datenträgers aufgrund eines Fehlers in Azure möglicherweise nicht in den gewünschten Typ geändert werden. Bisher würde die VM ausgeschaltet bleiben, und Sie würden eine Fehlermeldung erhalten. Mit diesem Feature können Sie die VM entweder einschalten (auch wenn der Speicher nicht auf den konfigurierten Typ wiederhergestellt werden kann) oder die VM ausgeschaltet lassen. Weitere Informationen finden Sie unter Einschaltverhalten beim Fehlschlagen der Änderung des Speichertyps anpassen.

Unterstützung für die MAK-Aktivierung. Sie können jetzt persistente und nicht persistente Maschinenkataloge mit virtuellen Maschinen bereitstellen, die über den Mehrfachaktivierungsschlüssel (MAK) aktiviert wurden. Mit diesem Feature kann MCS jetzt auch mit bereitgestellten VMs kommunizieren. Diese Implementierung hilft bei der Aktivierung des Windows-Systems, ohne dass die Aktivierungsanzahl verloren geht. Weitere Informationen finden Sie unter Aktivierung der Volumenlizenzierung.

Unterstützung für Azure-Datenträgerverschlüsselung auf dem Host. Mit diesem Feature können Sie einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Sie können eine VM oder eine Vorlagenspezifikation als Eingabe für ein Maschinenprofil verwenden. Weitere Informationen finden Sie unter Azure-Datenträgerverschlüsselung auf dem Host.

Bei diesem Verschlüsselungsverfahren werden die Daten auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten. Weitere Informationen finden Sie unter Verschlüsselung auf dem Host: End-to-End-Verschlüsselung für Ihre VM-Daten.

Unterstützung für GCP-Instanzvorlage als Eingabe für das Maschinenprofil. Mit diesem Feature können Sie eine GCP-Instanzvorlage als Eingabe für das Maschinenprofil auswählen. Instanzvorlagen sind schlanke Ressourcen in GCP und daher sehr kostengünstig. Verwenden Sie dazu PowerShell-Befehle. Weitere Informationen zur Verwendung von PowerShell-Befehlen zum Erstellen und Aktu-

alisieren von Maschinenkatalogen durch Auswahl einer GCP-Instanzvorlage finden Sie unter Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen.

Unterstützung für die Änderung des Namens der dynamischen Azure AD-Sicherheitsgruppe. Sie können den Namen einer dynamischen Azure AD-Sicherheitsgruppe im Azure-Portal ändern oder löschen. Diese Aktion kann dazu führen, dass der Name der dynamischen Azure AD-Sicherheitsgruppe nicht mehr mit der dynamischen Sicherheitsgruppe synchronisiert ist, die einem Maschinenkatalog zugeordnet ist. Mit diesem Feature können Sie jetzt den Namen der einem Maschinenkatalog zugeordneten dynamischen Azure AD-Sicherheitsgruppe ändern.

Diese Änderung trägt dazu bei, dass die im Azure AD-Identitätspoolobjekt gespeicherten Azure AD-Sicherheitsgruppeninformationen mit den im Azure-Portal gespeicherten Informationen konsistent bleiben. Weitere Informationen finden Sie unter Namen der dynamischen Azure AD-Sicherheitsgruppe ändern.

In GCP erforderliche Berechtigungen hinzugefügt. Die für die folgenden Aktionen erforderlichen Berechtigungen wurden jetzt hinzugefügt:

- Erstellen der Hostverbindung
- Energieverwaltung virtueller Maschinen
- Bereitstellung von Katalogen

Weitere Informationen finden Sie unter Informationen zu GCP-Berechtigungen.

Handhabung von Anmeldeinformationen. Aus Sicherheitsgründen werden Anmeldeinformationen von Benutzern, die sich nicht in derselben Domäne wie ihre VDAs befinden, standardmäßig nicht an die Cloud weitergeleitet. Anmeldeversuche schlagen fehl, wenn alle der folgenden Bedingungen erfüllt sind:

- Der Benutzer befindet sich in einer anderen Domäne als der VDA.
- Zwischen den Domänen besteht kein Vertrauen.
- StoreFront ist in derselben Domäne wie der VDA installiert.

Bisher konnten Benutzer unter diesen Bedingungen nicht bei StoreFront authentifiziert werden. Der Cloud Connector leitete die Benutzeranmeldeinformationen an die Cloud weiter, um die Authentifizierungsanfrage an das richtige Ziel für den jeweiligen Benutzer weiterzuleiten. Dieses Verhalten kann bei Bedarf weiterhin konfiguriert werden. Weitere Informationen finden Sie im Parameter `CredentialForwardingToCloudAllowed` von Set-Brokersite im DaaS PowerShell SDK.

März 2023

Neue und erweiterte Features

Unterstützung für die Konfiguration von Rollen und Geltungsbereichen für Administratoren. Citrix Cloud bietet jetzt ein höheres Maß an Flexibilität und Anpassung bei der Konfiguration des Zugriffs

für Administratoren. Bisher konnten Sie nur vordefinierte Rollen-/Geltungsbereichspaare auswählen. Mit dieser Erweiterung können Sie eine Rolle auswählen und mit einem Geltungsbereich Ihrer Wahl kombinieren.

Weitere Informationen finden Sie unter Konfigurieren von benutzerdefiniertem Zugriff für einen Administrator.

Unterstützung der Erstellung einer dynamischen Sicherheitsgruppe unter einer vorhandenen zugewiesenen Sicherheitsgruppe. Bisher konnten Sie dynamische Azure AD-Sicherheitsgruppen für einen Maschinenkatalog erstellen. Mit diesem Feature können Sie dynamische Azure AD-Sicherheitsgruppe auch unter einer vorhandenen Azure AD-Sicherheitsgruppe hinzufügen. Sie können die folgenden Aktionen ausführen:

- Informationen zur Sicherheitsgruppe abrufen.
- Rufen Sie alle zugewiesenen Azure AD-Sicherheitsgruppen ab, die vom On-Premises-AD-Server synchronisiert werden, oder die zugewiesenen Sicherheitsgruppen, denen Azure AD-Rollen zugewiesen werden können.
- Alle dynamischen Azure AD-Sicherheitsgruppen abrufen.
- Die dynamische Azure AD-Sicherheitsgruppe als Mitglied der zugewiesenen Azure AD-Gruppe hinzufügen.
- Die Mitgliedschaft zwischen der dynamischen Azure AD-Sicherheitsgruppe und der zugewiesenen Azure AD-Sicherheitsgruppe entfernen, wenn die dynamische Azure AD-Sicherheitsgruppe zusammen mit dem Maschinenkatalog gelöscht wird.

Weitere Informationen finden Sie unter Dynamische Azure AD-Sicherheitsgruppe unter einer vorhandenen Azure AD-Sicherheitsgruppe erstellen.

Unterstützung für die dynamische Azure AD-Sicherheitsgruppe für virtuelle Maschinen mit Azure AD-Bindung. Citrix unterstützt jetzt dynamische Sicherheitsgruppen für Kataloge bei der Erstellung eines MCS-Maschinenkatalogs. Dynamische Sicherheitsgruppenregeln ordnen die virtuellen Maschinen im Katalog einer dynamischen Sicherheitsgruppe zu, basierend auf dem Benennungsschema des Maschinenkatalogs. Dies ist nützlich, wenn Sie VMs über Azure Active Directory (Azure AD) verwalten möchten. Dies ist auch nützlich, wenn Sie Richtlinien für bedingten Zugriff anwenden oder Apps aus Intune verteilen möchten, indem Sie die VMs anhand der dynamischen Azure AD-Sicherheitsgruppe filtern. Wenn Sie einen Katalog löschen, wird die dynamische Sicherheitsgruppe ebenfalls gelöscht. Weitere Informationen finden Sie unter Dynamische Azure Active Directory-Sicherheitsgruppe.

Informationen zu den Lizenzanforderungen für die Verwendung dynamischer Sicherheitsgruppen finden Sie in dem Microsoft-Dokument Erstellen oder Aktualisieren einer dynamischen Gruppe in Azure Active Directory.

Unterstützung für das Hinzufügen von VMs zu Azure AD-Sicherheitsgruppenüber "Vollständige Konfiguration". Beim Erstellen von VMs mit Azure-Bindung steht jetzt die Option **Azure AD-**

Sicherheitsgruppe zur Verfügung. Mit dieser Option können Sie die VMs basierend auf ihrem Benennungsschema zu einer Azure AD-Sicherheitsgruppe hinzufügen. Weitere Informationen finden Sie unter Microsoft Azure-Katalog erstellen.

Unterstützung für das Ändern des Speichertyps vorhandener VMs in eine niedrigere Ebene beim Herunterfahren in Azure-Umgebungen. In Azure-Umgebungen können Sie jetzt Speicherkosten sparen, indem Sie den Speichertyp vorhandener VMs beim Herunterfahren der VMs in eine niedrigere Ebene ändern. Verwenden Sie dazu die benutzerdefinierte Eigenschaft StorageTypeAtShutdown. Weitere Informationen finden Sie unter Ändern des Speichertyps vorhandener VMs auf eine niedrigere Ebene beim Herunterfahren.

Unterstützung für das Zulassen von Sicherheits-IDs beim Erstellen virtueller Maschinen. Bisher konnten Sie beim Erstellen neuer virtueller Maschinen mit der durch ein Provisioningschema angegebenen Konfiguration dem Befehl `NewProvVM` keine Sicherheits-ID (`ADAccountSid`) hinzufügen. Mit diesem Feature können Sie jetzt den Parameter `ADAccountSid` hinzufügen, um die Maschinen beim Erstellen neuer virtueller Maschinen eindeutig zu identifizieren. Weitere Informationen finden Sie unter SIDs beim Erstellen virtuelle Maschinen hinzufügen.

Möglichkeit, Warnungen zu MCS-Katalogen abzurufen. Bisher gab es keine Informationen zur Anzeige von Problemen mit dem Maschinenkatalog. Mit diesem Feature können Sie Warnungen erhalten, um aufgetretene Probleme mit Ihren MCS-Katalogen zu verstehen und diese zu beheben.

Warnungen führen im Unterschied zu Fehlern nicht dazu, dass eine initiierte Provisioningaufgabe fehlschlägt.

Verwenden Sie PowerShell-Befehle, um Warnungen zu erhalten. Weitere Informationen finden Sie unter Mit einem Katalog verknüpfte Warnungen abrufen.

Freigegebene Mandanten für Verbindungen. Sie können jetzt Mandanten und Abonnements hinzufügen, die sich die Azure Compute Gallery mit dem Abonnement der Verbindung teilen. Sie können dann beim Erstellen oder Aktualisieren von Katalogen freigegebene Images aus diesen Mandanten und Abonnements auswählen. Weitere Informationen finden Sie unter Bearbeiten von Verbindungseinstellungen.

Unterstützung für Änderung des Betriebssystemtyps für Azure-Kataloge wurde entfernt. Beim Ändern von Katalogimages werden nur Images angezeigt, die denselben Betriebssystemtyp haben wie das verwendete Image. Diese Erweiterung bedeutet, dass Citrix DaaS das Ändern des Betriebssystemtyps für Azure-Kataloge nach der Katalogerstellung, z. B. den Wechsel vom Windows-Betriebssystemtyp zu Linux und umgekehrt, nicht mehr unterstützt.

Februar 2023

Neue und erweiterte Features

Unterstützung für die Image-Freigabe unter Azure-Mandanten. Bisher konnten Sie in Azure-Umgebungen Images nur mit freigegebenen Abonnements über die Azure Compute Gallery freigeben. Mit diesem Feature können Sie nun in der Azure Compute Gallery ein Image auswählen, das zu einem anderen freigegebenen Abonnement in einem anderen Mandanten gehört, um damit einen MCS-Katalog zu erstellen und zu aktualisieren. Weitere Informationen finden Sie unter Image-Freigabe unter Azure-Mandanten.

Richtlinienmodellierung. Die Richtlinienmodellierung ist jetzt allgemein verfügbar. Sie können Richtlinien zu Planungs- und Testzwecken simulieren. Weitere Informationen finden Sie unter Assistenten für die Richtlinienmodellierung verwenden.

Möglichkeit, Preview-Features ein- oder auszuschalten. Als Citrix Cloud-Administrator mit Vollzugriff können Sie unter "Vollständige Konfiguration > Home"Preview-Features ein- oder ausschalten, ohne Citrix zu kontaktieren. Weitere Informationen finden Sie unter Homepage für die Oberfläche "Vollständige Konfiguration".

Sitzungsdiagnose nach Benutzernamen suchen. Dieses Feature ermöglicht die Verwendung der Sitzungsstartdiagnose anhand des Benutzernamens, wenn Sie keine Transaktions-ID haben. Das Feature ist besonders für Helpdesk-Administratoren nützlich, um fehlgeschlagene Sitzungen zu prüfen, wenn der Endbenutzer die Transaktions-ID nicht erfasst hat.
Sie können nach einem Benutzernamen suchen und aus einer Liste der fehlgeschlagenen Sitzungen, die der Benutzer in den letzten 48 Stunden zu starten versucht hat, eine Sitzung auswählen. Auf der Seite "Sitzungsstartdiagnose"werden die Details der fehlgeschlagenen Sitzung angezeigt. Es werden die Komponente und der Schritt aufgeführt, bei denen der Fehler aufgetreten ist. Weitere Informationen finden Sie unter Sitzungsstartdiagnose.

Stellen Sie Secure Web- und SaaS-Apps mit Secure Private Access bereit. Auf der Registerkarte **Vollständige Konfiguration > Anwendungen > Anwendungen** ist jetzt die neue Option **Web-/SaaS-Anwendungen hinzufügen** in der Aktionsleiste verfügbar. Mit dieser Option können Sie Secure Web- und SaaS-Apps mit Secure Private Access bereitstellen. Citrix Secure Private Access bietet Remotebenutzern eine einfache, flexible Möglichkeit, mithilfe eines Zero-Trust-Ansatzes auf Web-, SaaS- und Clientserver-Apps zuzugreifen. Es ermöglicht Single Sign-On für Web- und SaaS-Apps sowie granulare Sicherheitskontrollen wie Wasserzeichen und Kontrollen beim Kopieren/Einfügen/Drucken zusätzlich zu anderen Sicherheitsfunktionen. Mit Citrix Secure Private Access können Sie alle virtualisierten und nicht virtualisierten Anwendungen an einem Ort kombinieren und das Endbenutzererlebnis verbessern. Siehe Citrix Secure Private Access

Protokollinhalt nach Zeitdauer filtern. Die neue Option **Benutzerdefiniert** ist jetzt in der Zeitdauerliste unter **Vollständige Konfiguration > Protokollierung > Ereignisse** verfügbar. Mit ihr

können Sie einen Zeitraum für Ereignisse angeben, nach dem Sie Ihre Suche filtern möchten. Weitere Informationen finden Sie unter Konfigurationsprotokollierung.

Updates für Autoscale. Die Option **Steuern, wann Autoscale mit dem Einschalten von getaggten Maschinen beginnt** ist jetzt leichter verständlich. Sie steuert, wann Autoscale (basierend auf dem Prozentsatz der Kapazität ungetaggter Maschinen) mit dem Einschalten von getaggten Maschinen beginnt. Wenn der Prozentsatz unter den Schwellenwert fällt (Standardwert ist 10 %), beginnt Autoscale, die Maschinen mit Tag einzuschalten. Wenn der Prozentsatz den Schwellenwert überschreitet, wechselt Autoscale in den Ausschaltmodus. Weitere Informationen finden Sie unter Autoscale von getaggten Maschinen (Cloudburst)

App-Schutzrichtlinien. Sie können jetzt den App-Schutz aktivieren, wenn Sie eine Bereitstellungsgruppe erstellen oder bearbeiten. Zwei Richtlinien bieten Keyloggingschutz und Screenshotschutz für Clientsitzungen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen und Bereitstellungsgruppen verwalten.

GPU-Auslastung in Echtzeit für AMD-GPUs verfügbar. Sie können jetzt die GPU-Auslastung von AMD Radeon Instinct MI25-GPUs und AMD EPYC 7V12-CPUs (Rom) unter "Überwachen"anzeigen. "Überwachen"unterstützt bereits die NVIDIA Tesla M60-GPUs. Die GPU-Auslastung zeigt Diagramme mit der prozentualen Auslastung von GPU in Echtzeit, GPU-Speicher und Encoder sowie Decoder. Anhand dieser Informationen können Sie GPU-Probleme auf Multisitzungs-OS- oder Einzelsitzungs-OS-VDAs behandeln. Die Diagramme zur AMD-GPU-Auslastung sind nur für VDAs verfügbar, auf denen 64-Bit-Windows und Citrix Virtual Apps and Desktops 7 2212 oder höher ausgeführt wird. Weitere Informationen finden Sie unter GPU-Auslastung.

Unterstützung der Planung von Konfigurationsupdates in Azure. In Azure-Umgebungen können Sie jetzt mit dem PowerShell-Befehl `Schedule-ProvVMUpdate` ein Zeitfenster für die Konfigurationsupdates der vorhandenen, von MCS bereitgestellten Maschinen festlegen. Während dieses Zeitfensters wird dann bei jedem Einschalten oder Neustart ein geplantes Update des Provisioningschemas auf eine Maschine angewendet. Mit `Cancel-ProvVMUpdate` können Sie das Konfigurationsupdate auch vor dem geplanten Zeitpunkt abbrechen.

Sie können das Konfigurationsupdate für Folgendes planen oder abbrechen:

- Eine einzelne VM oder mehrere VMs
- Einen ganzen Katalog

Weitere Informationen finden Sie unter Konfigurationsupdates planen.

Unterstützung für die Verwendung von einsatzbereiten Citrix-Images direkt aus dem Google Cloud Marketplace. Sie können jetzt von Citrix im Google Cloud Marketplace angebotene Images durchsuchen und auswählen, um damit MCS-Kataloge zu erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Weitere Informationen finden Sie unter Google Cloud Marketplace.

Hostgruppenbereich in SCVMM-Hostverbindung beschränken. Bisher musste der Administrator für die Hostverbindung zum SCVMM über eine einzelne Hostgruppe der obersten Ebene verfügen. Der Administrator erhielt damit Einsicht in alle Hostgruppen, Cluster oder Hosts, die dieser Hostgruppe der obersten Ebene untergeordnet waren. Mit diesem Feature können Sie nun in großen Bereitstellungen, in denen ein SCVMM mehrere Cluster in unterschiedlichen Datencentern verwaltet, den Hostgruppenbereich für Administratoren beschränken. Verwenden Sie hierfür die Rolle "Delegierter Administrator"in der Konsole von Microsoft System Center Virtual Machine Manager (VMM), und wählen Sie die Hostgruppen aus, auf die ein Administrator Zugriff erhalten muss. Weitere Informationen finden Sie unter Hypervisor installieren und konfigurieren.

Unterstützung für zonenredundanten Speicher in Azure. Bisher bot MCS nur lokal redundanten Speicher an. Mit diesem Feature ist jetzt auch zonenredundanter Speicher in Azure verfügbar, sodass Sie je nach gewünschter Redundanz den passenden Speichertyp auswählen können. Mit zonenredundantem Speicher wird Ihre Azure Managed Disk über mehrere Verfügbarkeitszonen repliziert, sodass Sie Ihre Daten bei einem Ausfall in einer Zone mithilfe der Redundanz in den übrigen Zonen wiederherstellen können. Weitere Informationen finden Sie unter Zonenredundanten Speicher aktivieren.

Januar 2023

Neue und erweiterte Features

Option zum Herabstufen des Speicherdatenträgers auf Standard-HDD beim Herunterfahren von VMs. Auf der Seite **Datenträgereinstellungen** ist beim Erstellen oder Aktualisieren von Azure-Katalogen jetzt die neue Option **Einsparung von Speicherkosten aktivieren** verfügbar. Diese Option senkt die Speicherkosten, indem der Speicher- und Zurückschreibcache-Datenträger beim Herunterfahren der VM auf Standard-HDD herabgestuft wird. Beim Neustart wechselt die VM wieder zu den ursprünglichen Einstellungen. Weitere Informationen finden Sie unter Microsoft Azure-Katalog erstellen.

Unterstützung für die Konfiguration von Sitzungsroaming in "Vollständige Konfiguration" . Bisher konnten Sie das Sitzungsroaming für Anwendungen und Desktops nur per PowerShell konfigurieren. Jetzt ist dies auch in **Vollständige Konfiguration** möglich. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

Umbenennung einiger Aktionen zur Anpassung an ihre tatsächliche Bedeutung. Folgende Aktionen in **Vollständige Konfiguration > Maschinenkataloge** und **Vollständige Konfiguration > Bereitstellungsgruppen** wurden umbenannt. Die Workflows zum Ausführen der Aktionen bleiben unverändert.

- **Maschinen aktualisieren** wurde umbenannt in **Masterimage ändern**
- **Rollback für Maschinenupdate** wurde umbenannt in **Rollback für Masterimage ausführen**
- **Katalog aktualisieren** wurde umbenannt in **Funktionsebene ändern**

- **Upgrade von Bereitstellungsgruppe durchführen** wurde umbenannt in **Funktionsebene ändern**
- **Upgrade von Katalog rückgängig machen** wurde umbenannt in **Änderung der Funktionsebene rückgängig machen**
- **Upgrade von Bereitstellungsgruppe rückgängig machen** wurde umbenannt in **Änderung der Funktionsebene rückgängig machen**

Unterstützung für die Verwendung von Ordnern zur Organisation von Anwendungsgruppen. Sie können jetzt verschachtelte Ordner erstellen, um den Zugriff auf Anwendungsgruppen zu vereinfachen. Weitere Informationen finden Sie unter Anwendungsgruppen mit Ordnern organisieren.

Verbesserung an Einschränkungen für Bereitstellungsgruppen. Bisher konnten Sie zur Beschränkung der Verwendung von Apps oder Desktops für eine Bereitstellungsgruppe nur autorisierte Benutzer und Benutzergruppen in einer Bereitstellungsgruppe angeben. Jetzt können Sie auch Benutzer und Benutzergruppen hinzufügen, die Sie blockieren möchten. Diese Verbesserung ist nützlich, wenn Sie einer Positivliste eine Benutzergruppe hinzufügen und gleichzeitig eine Teilmenge dieser Benutzer auf der Positivliste blockieren möchten. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

Zugriff auf Sitzungsdetails aus Citrix Analytics für Leistung in "Überwachen". Die Seite "Sitzungsdetails"in Citrix Analytics für Leistung ist jetzt in "Überwachen"integriert. Klicken Sie in "Überwachen"auf der Seite "Sitzungen"auf **Sitzungszeitachse anzeigen**, um die Seite "Sitzungsdetails"von Citrix Analytics für Leistung in "Überwachen"zu öffnen. Sie benötigen hierfür einen gültigen Anspruch auf Citrix Analytics für Leistung. Die Sitzungsdetails sind für Sitzungen verfügbar, die in Citrix Analytics für Leistung als "Ausgezeichnet", "Ausreichend"oder "Schlecht"eingestuft sind.

Sie können für die Sitzung einen Trend der Sitzungserfahrung für die letzten drei Tage anzeigen, zusammen mit den zugehörigen Einflussfaktoren. Diese Informationen ergänzen die in "Überwachen" verfügbaren Livedaten, die vom Helpdeskadministrator verwendet werden, um Probleme im Zusammenhang mit der Sitzungserfahrung zu beheben.

Weitere Informationen finden Sie im Artikel zu Siteanalyse.

Nicht persistente virtuelle Maschinen werden aus Hypervisors oder Clouddiensten gelöscht, wenn Sie sie oder die zugehörigen Maschinenkataloge in der vollständigen Konfiguration löschen. Die Option, VMs in Hypervisors oder Clouddiensten beizubehalten, ist jetzt nur für persistente VMs verfügbar. Weitere Informationen finden Sie unter Verwalten von Maschinenkatalogen.

Dezember 2022

Neue und erweiterte Features

Unterstützung für das Erstellen von Katalogen (in Azure AD bzw. Azure AD Hybrid eingebunden oder mit aktiviertem Microsoft Intune) mit in Azure AD eingebundenen Master-VMs. Sie können

jetzt Kataloge, die in Azure AD oder Azure AD Hybrid eingebunden sind bzw. Kataloge mit aktiviertem Microsoft Intune mit Master-VMs erstellen, die in Azure AD bzw. Azure AD Hybrid eingebunden oder nicht domänengebunden sind. Um eine Master-VM mit Microsoft Intune zu verwalten, verwenden Sie VDA-Version 2212 und höher und überspringen nicht die Imagevorbereitung, während Sie Maschinenkataloge erstellen oder aktualisieren.

Weitere Informationen zu Maschinenidentitäten finden Sie unter In Azure Active Directory eingebunden, Microsoft Intune und Azure Active Directory-Hybrideinbindung.

Unterstützung in den Maschinenerstellungsdiensten (MCS) für das Löschen von VM-Objekten ohne Zugriff auf den Hypervisor. Sie können jetzt VM-Objekte in MCS löschen, ohne Zugriff auf den Hypervisor zu haben. Beim Löschen einer VM oder eines Provisioningschemas muss MCS die Tags entfernen, damit die Ressourcen nicht mehr nachverfolgt oder identifiziert werden. Bisher wurden die Fehler beim Entfernen von Tags ignoriert, wenn auf den Hypervisor nicht zugegriffen werden konnte. Mit diesem Feature: Kann nicht auf den Hypervisor zugegriffen werden, wenn der Befehl `Remove-ProvVM` ausgeführt wird, schlägt das Entfernen des Tags fehl. Mit der Option `PurgeDBOnly` können Sie das VM-Ressourcenobjekt jedoch trotzdem aus der Datenbank löschen. Weitere Informationen finden Sie unter Maschinen ohne Hypervisor-Zugriff löschen.

November 2022

Neue und erweiterte Features

Unterstützung für die Bereitstellung von MSIX-Paketen sowie von mit dem MSIX-Feature zum Anfügen von Apps verpackten Apps. Unter **Vollständige Konfiguration > App-Pakete** können Sie jetzt MSIX-Pakete sowie mit dem MSIX-Feature zum Anfügen von Apps verpackte Apps in Citrix Cloud hochladen und den Benutzern bereitstellen. Weitere Informationen finden Sie unter App-Pakete.

Verweis auf nicht unterstützte VDA-Versionen und Funktionsebenen. Die Oberfläche "Vollständige Konfiguration"informiert Sie jetzt über nicht unterstützte VDA-Versionen und Funktionsebenen. So vermeiden Sie potenzielle Probleme:

- Wenn auf einer Maschine eine nicht unterstützte VDA-Version ausgeführt wird, werden Sie aufgefordert, ein Upgrade auf eine unterstützte Version durchzuführen.
- Wenn die Funktionsebene eines Katalogs oder einer Bereitstellungsgruppe nicht unterstützt wird, werden Sie aufgefordert, eine höhere Ebene festzulegen.

> **Tipp:**
>
> Für VDAs gelten die CR- und LTSR-Lebenszyklen für Citrix Virtual Apps and Desktops.

Kommentieren von Masterimages jetzt auch bei der Katalogerstellung möglich. Beim Erstellen eines MCS-Katalogs in **Vollständige Konfiguration** können Sie jetzt das zugehörige Masterimage kommentieren. Weitere Informationen finden Sie unter Masterimage.

Unterstützung für den Export von Desktopzuweisungsdaten über "Vollständige Konfiguration" . Beim Anzeigen von Desktopzuweisungen für eine Einzelsitzungs-OS-Bereitstellungsgruppe können Sie jetzt die Zuweisungsdaten zu Auditzwecken in eine CSV-Datei exportieren. Wählen Sie dazu die Bereitstellungsgruppe in **Vollständige Konfiguration > Bereitstellungsgruppe** aus und klicken Sie auf der Registerkarte **Desktops** links oben auf **Exportieren**.

Zusammenfassen der Registerkarten "Alle Anwendungen"und "Anwendungsordner"zu einer Registerkarte. In **Vollständige Konfiguration > Anwendungen** wurden die Registerkarten **Alle Anwendungen** und **Anwendungsordner** in der Registerkarte **Anwendungen** zusammengefasst. Diese Änderung vereinheitlicht die Verwaltung der Ordneransicht für Benutzer über Knoten in "Vollständige Konfiguration"hinweg.

Unterstützung für das Ändern des Speichertyps in eine niedrigere Ebene beim Herunterfahren einer VM in Azure-Umgebungen. In Azure-Umgebungen können Sie jetzt Speicherkosten sparen, indem Sie beim Herunterfahren einer VM den Speichertyp eines verwalteten Datenträgers auf eine niedrigere Ebene umstellen. Verwenden Sie dazu die benutzerdefinierte Eigenschaft `StorageTypeAtShutdown`. Der Speichertyp des Datenträgers ändert sich in eine niedrigere Ebene (wie in der benutzerdefinierten Eigenschaft `StorageTypeAtShutdown` angegeben), wenn Sie die VM herunterfahren. Nach dem Einschalten der VM ändert sich der Speichertyp in den ursprünglichen Speichertyp zurück (wie in der benutzerdefinierten Eigenschaft `StorageType`oder `WBCDiskStorageType` angegeben). Weitere Informationen finden Sie unter Speichertyps beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern.

Aktualisierungen in der Anzeige "Filter". Die Seite "Filter"in "Überwachen"enthält nun separate Listen für gespeicherte Filter und Standardfilter, um die Visualisierung und den Zugriff auf Filter zu verbessern. Sie können eine Ansicht für Maschinen, Sitzungen, Verbindungen oder Anwendungsinstanzen auswählen. Sie können dann einen Filter aus der Liste "Gespeicherte Filter"oder "Standardfilter"auswählen, um die gefilterte Datenliste anzuzeigen. Mithilfe der Dropdownlisten können Sie die Filterkriterien verfeinern oder vorhandene Kriterien bearbeiten. Sie können Ihren Filter dann in der Liste "Gespeicherte Filter"speichern. Weitere Informationen finden Sie im Artikel Filter.

Zurücksetzen des OS-Datenträgers einer persistenten VM in einem mit MCS erstellten Maschinenkatalog. In VMware-Virtualisierungsumgebungen können Sie jetzt den PowerShell-Befehl `Reset-ProvVMDisk` verwenden, um den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog zurückzusetzen. Das Feature automatisiert den Vorgang des Zurücksetzens des OS-Datenträgers. Beispielsweise hilft es beim Zurücksetzen der VM auf den Anfangsstatus eines persistenten Entwicklungsdesktopkatalogs, der mit MCS erstellt wurde.

Weitere Informationen zum Zurücksetzen des OS-Datenträgers per PowerShell-Befehl finden Sie unter Zurücksetzen des OS-Datenträgers.

Unterstützung für die Aktualisierung des Maschinenprofils und weiterer benutzerdefinierter Eigenschaften von mit MCS bereitgestellten Maschinen in Azure-Umgebungen. Bisher konnten Sie in Azure-Umgebungen die benutzerdefinierte Eigenschaft `ServiceOffering` einer mit MCS

bereitgestellten Maschine mit `Request-ProvVMUpdate` aktualisieren. Jetzt können Sie auch das Maschinenprofil und die folgenden benutzerdefinierten Eigenschaften aktualisieren:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

Weitere Informationen finden Sie unter Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema.

Unterstützung für Maschinenprofile in GCP. Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS in Google Cloud Platform-Umgebungen erstellen, können Sie jetzt ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer virtuellen Maschine erfasst und auf neu bereitgestellte VMs im Katalog anwendet. Wenn der Parameter `MachineProfile` nicht verwendet wird, werden die Hardwareeigenschaften von der Masterimage-VM oder dem Snapshot erfasst.

Maschinenprofile funktionieren sowohl mit Linux- als auch mit Windows-Betriebssystemen.

Informationen zum Erstellen von Maschinenkatalogen mit einem Maschinenprofil finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Maschinenprofils.

Unterstützung für die Aktualisierung von mit MCS bereitgestellten Maschinen in GCP-Umgebungen. In GCP-Umgebungen ändert `Set-ProvScheme` die Vorlage (Provisioningschema) und wirkt sich nicht auf vorhandene Maschinen aus. Mit dem PowerShell-Befehl `Request-ProvVMUpdate` können Sie jetzt das aktuelle Provisioningschema auf eine oder mehrere vorhandene Maschine(n) anwenden. Die derzeit in GCP von diesem Feature unterstützte aktualisierte Eigenschaft ist das Maschinenprofil. Weitere Informationen finden Sie unter Aktualisieren bereitgestellter Maschinen mit PowerShell.

Oktober 2022

Neue und erweiterte Features

Unterstützung für die gleichzeitige Verwendung von Maschinenprofilen und Hostgruppen. Wenn Sie einen Katalog mit einem Azure Resource Manager-Masterimage erstellen, können Sie jetzt gleichzeitig ein Maschinenprofil und eine Hostgruppe verwenden. Dies ist nützlich, wenn Sie durch vertrauenswürdige Starts die Sicherheit erhöhen und gleichzeitig die Maschinen auf dedizierten

Hosts ausführen möchten. Weitere Informationen finden in dem Artikel zu Microsoft Azure Resource Manager-Virtualisierungsumgebungen.

Unterstützung für die Verwendung von Ordnern zur Organisation von Bereitstellungsgruppen. Sie können jetzt eine Ordnerstruktur erstellen, um den Zugriff auf Bereitstellungsgruppen zu vereinfachen. Weitere Informationen finden Sie unter Bereitstellungsgruppen mit Ordnern organisieren.

Unterstützung für einen einmaligen geplanten Neustart von Maschinen über "Vollständige Konfiguration". Beim Erstellen von Neustartzeitplänen für Bereitstellungsgruppen ist jetzt die neue Option **Einmal** verfügbar. Mit dieser Option können Sie planen, dass Maschinen in einer Bereitstellungsgruppe zu einem bestimmten Zeitpunkt einmal neu gestartet werden. Weitere Informationen finden Sie unter Erstellen eines Neustartzeitplans.

Erweiterte Testplanung. Die Planung von Anwendungs- und Desktoptests wurde verbessert und kann jetzt in "Überwachen"durchgeführt werden. Mit diesem Feature kann Citrix Probe Agent so konfiguriert werden, dass Tests an bestimmten Wochentagen ausgeführt und in einem festgelegten Intervall während des Tages wiederholt werden. So können Sie für einzelne Tests festlegen, dass sie zu bestimmten Zeiten am Tag und in der Woche wiederholt werden. Sie können jetzt die Integrität der Site proaktiv überprüfen, indem Sie Tests konfigurieren, die regelmäßig zu geeigneten Zeiten ausgeführt werden. Dieses Feature vereinfacht das Einrichten und Verwalten von Tests unter "Überwachen" . Weitere Informationen finden Sie unter Anwendungs- und Desktoptests.

September 2022

Neue und erweiterte Features

Ältere Versionen des Remote PowerShell SDKs laufen aus. Wenn Sie eine veraltete Version verwenden, funktioniert das SDK nicht mehr und Sie werden in einer Fehlermeldung aufgefordert, die aktuelle Version herunterzuladen. Laden Sie in diesem Fall das aktuelle Remote PowerShell SDK von der Citrix-Website herunter.

Maschinenkataloge mit vertrauenswürdigem Start in Azure. In Azure-Umgebungen können Sie Maschinenkataloge erstellen, für die vertrauenswürdige Start aktiviert ist, und mit der VM-Bestandseigenschaft `SupportsTrustedLaunch` die VM-Größen ermitteln, die den vertrauenswürdigen Start unterstützen.

Mit vertrauenswürdigen Starts lässt sich die Sicherheit von VMs der zweiten Generation weiter verbessern. Der vertrauenswürdige Start schützt vor fortschrittlichen und persistenten Angriffstechniken. Weitere Informationen finden Sie unter Maschinenkataloge mit vertrauenswürdigem Start.

Unterstützung für die Identifizierung von mit MCS erstellten Microsoft System Center Virtual Machine Manager-Ressourcen. Sie können jetzt Microsoft System Center Virtual Machine Manager-Ressourcen, die mit MCS erstellt wurden, mit Tags identifizieren. Weitere Informationen zu den

Tags, die MCS zu den Ressourcen hinzufügt, finden Sie unter Identifizieren der von MCS erstellten Ressourcen.

Unterstützung für die Identifizierung von mit MCS erstellten VMware-Ressourcen. Sie können nun mit Tags VMware-Ressourcen identifizieren, die mit MCS erstellt wurden. Weitere Informationen zu den Tags, die MCS zu den Ressourcen hinzufügt, finden Sie unter Identifizieren der von MCS erstellten Ressourcen.

Unterstützung für das Optimieren der AWS Workspace-Drosselung. Sie können jetzt eine große Anzahl Maschinen in einem AWS Workspace ein- und ausschalten, ohne dass Drosselungsprobleme auftreten. Drosselungsprobleme treten auf, wenn die Anzahl der an AWS Workspace gesendeten Anforderungen die Anzahl von Anforderungen überschreitet, die der Server verarbeiten kann. Aus diesem Grund kombiniert Citrix jetzt mehrere Anforderungen in eine Anforderung, bevor sie an das AWS Workspace SDK gesendet wird.

Möglichkeit zur Überprüfung von Maschinendetails bei der Anzeige der Anzahl Maschinen in Home. Wenn Sie die Anzahl Maschinen nach Verfügbarkeitsstatus in **Home** anzeigen, können Sie jetzt auf einen Status klicken, um die Details der Maschinen mit diesem Status anzuzeigen. Weitere Informationen finden Sie unter Homepage für die Oberfläche "Vollständige Konfiguration".

Unterstützung für das Erstellen von Maschinenkatalogen mit einem Image aus einem anderen Abonnement im selben Azure-Mandanten. Bisher konnten Sie in Azure-Umgebungen nur ein Image aus Ihrem Abonnement auswählen, um einen Maschinenkatalog zu erstellen. Mit diesem Feature können Sie nun in Azure Compute Gallery (zuvor "Shared Imaged Gallery") ein Image auswählen, das zu einem anderen freigegebenen Abonnement gehört, um MCS-Kataloge zu erstellen und zu aktualisieren.

Weitere Informationen zum Erstellen eines Katalogs finden Sie unter Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images erstellen.

Informationen zum Freigeben von Images für andere Dienstprinzipals im selben Mandanten finden Sie unter Freigeben von Images für andere Dienstprinzipals im selben Mandanten.

Informationen zum Auswählen von Images aus einem anderen Abonnement mit PowerShell-Befehlen finden Sie unter Auswahl eines Images aus einem anderen Abonnement mit PowerShell.

Weitere Informationen zu Azure Compute Gallery finden Sie unter Azure Shared Image Gallery.

August 2022

Neue und erweiterte Features

Unterstützung der Identifizierung der von MCS erstellten Citrix Hypervisor-Ressourcen. Sie können nun mit Tags Citrix Hypervisor-Ressourcen identifizieren, die mit MCS erstellt wurden. Weitere

Informationen zu den Tags, die MCS zu den Ressourcen hinzufügt, finden Sie unter Identifizieren der von MCS erstellten Ressourcen.

Unterstützung der gleichzeitigen Verwendung von Hostgruppen- und Azure-Verfügbarkeitszonen. In Azure-Umgebungen können Sie nun im Voraus prüfen, ob ein Maschinenkatalog mit der in der benutzerdefinierten Eigenschaft angegebenen Azure-Verfügbarkeitszone und der Zone der Hostgruppe erstellt werden kann. Die Katalogerstellung schlägt fehl, wenn die Verfügbarkeitszone der benutzerdefinierten Eigenschaft nicht mit der Hostgruppenzone übereinstimmt.

Eine Hostgruppe ist eine Ressource, die eine Sammlung dedizierter Hosts darstellt. Ein dedizierter Host ist ein Dienst, der physische Server bereitstellt, die eine oder mehrere virtuelle Maschinen hosten.
Azure-Verfügbarkeitszonen sind physisch getrennte Standorte innerhalb jeder Azure-Region, die lokale Ausfälle tolerieren können.

Weitere Informationen zu den verschiedenen Kombinationen aus Verfügbarkeits- und Hostgruppenzone, die zum Erfolg oder Fehlschlagen einer Maschinenkatalogerstellung führen, finden Sie unter Gleichzeitige Verwendung von Hostgruppen- und Azure-Verfügbarkeitszonen.

Unterstützung für die Ordner-ID-Aktualisierung eines Maschinenkatalogs in VMware. In VMware-Virtualisierungsumgebungen können Sie jetzt die Ordner-ID eines MCS-Maschinenkatalogs über die benutzerdefinierte Eigenschaft `FolderID` in `Set-ProvScheme` aktualisieren. Die nach dem Aktualisieren der Ordner-ID erstellten VMs werden unter dieser neuen Ordner-ID erstellt. Wenn diese Eigenschaft nicht in `CustomProperties` angegeben ist, werden VMs in dem Ordner erstellt, in dem das Masterimage ist. Weitere Informationen zum Aktualisieren der Ordner-ID finden Sie unter Aktualisieren der Ordner-ID eines Maschinenkatalogs.

Einrichten von Zeitzonen. Mit der Einstellung **Datum und Uhrzeit** können Sie jetzt das Datums- und Uhrzeitformat der Oberfläche an Ihre Präferenzen anpassen. Weitere Informationen finden Sie unter Einrichten von Zeitzonen.

Image Portability Service (IPS) unterstützt jetzt Amazon Web Services (AWS). Durch die Konfiguration der erforderlichen Berechtigungen und Komponenten für AWS können IPS-Workflows mit einem AWS-Konto verwendet werden. Weitere Informationen finden Sie unter Migration von Workloads in die öffentliche Cloud.

Einrichten der Auslagerungsdatei während der Imagevorbereitung in Azure-Umgebungen. In Azure-Umgebungen können Sie nun mögliche Verwechslungen beim Speicherort der Auslagerungsdatei vermeiden. Zu diesem Zweck bestimmt MCS nun den Speicherort der Auslagerungsdatei, wenn Sie das Provisioningschema während der Imagevorbereitung erstellen. Diese Berechnung basiert auf bestimmten Regeln. Da Features wie der kurzlebige Betriebssystemdatenträger (EOS) und MC-E/A einen bestimmten Speicherort voraussetzen, schließen sie einander aus. Wenn Sie zudem die Imagevorbereitung von der Erstellung des Provisioningschemas trennen, bestimmt MCS den Speicherort der Auslagerungsdatei korrekt. Weitere Informationen zum Speicherort der

Auslagerungsdatei finden Sie unter Speicherort der Auslagerungsdatei.

Unterstützung für das Aktualisieren der Auslagerungsdateieinstellung in Azure-Umgebungen. Während Sie einen Katalog in einer Azure-Umgebung erstellen, können Sie jetzt die Einstellung für die Auslagerungsdatei, einschließlich Speicherort und Größe, mit PowerShell-Befehlen festlegen. Diese Einstellung überschreibt die MCS-Konfiguration. Hierfür führen Sie den Befehl `New-ProvScheme` mit den folgenden benutzerdefinierten Eigenschaften aus:

- `PageFileDiskDriveLetterOverride`: Laufwerksbuchstabe für Speicherort der Auslagerungsdatei
- `InitialPageFileSizeInMB`: Anfangsgröße der Auslagerungsdatei (in MB)
- `MaxPageFileSizeInMB`: Maximalgröße der Auslagerungsdatei (in MB)

Weitere Informationen zum Aktualisieren der Einstellung für die Auslagerungsdatei finden Sie unter Aktualisieren der Einstellung für die Auslagerungsdatei.

Aktualisierungen auf der Homepage. Das Aussehen des Widgets "Erste Schritte" wurde neu gestaltet. Weitere Aktualisierungen auf der Homepage sind:

- Die neu hinzugefügten Symbole für "Aktualisieren" und "Hilfe" in der oberen rechten Ecke.
- Klickbare Ressourcen zum schnellen Zugriff auf relevante Ressourcenseiten.
- Verbessertes "Gefällt mir nicht"-Symbol. Wenn Sie eine Empfehlung ablehnen, verschwindet die Empfehlung. Wenn Sie das Empfehlungswidget ablehnen, verschwindet das Widget.

Weitere Informationen finden Sie unter Homepage.

Unterstützung für das Aktivieren von Azure VM-Erweiterungen. Wenn Sie eine ARM-Vorlagenspezifikation als Maschinenprofil zum Erstellen eines Maschinenkatalogs verwenden, können Sie den VMs im Katalog jetzt Azure VM-Erweiterungen hinzufügen, die Liste der unterstützten Erweiterungen anzeigen und hinzugefügte Erweiterungen entfernen. Azure VM-Erweiterungen sind kleine Anwendungen, die nach der Bereitstellung Konfigurations- und Automatisierungsaufgaben auf Azure-VMs bereitstellen. Sie können VM-Erweiterungen verwenden, wenn für eine VM beispielsweise eine Softwareinstallation, ein Antivirenprogramm oder die Ausführbarkeit eines Skripts in der VM erforderlich ist. Weitere Informationen zum Aktivieren von Azure-VM-Erweiterungen finden Sie unter Verwenden von PowerShell zum Aktivieren von Azure-VM-Erweiterungen.

Unterstützung für vertrauenswürdige Starts bei kurzlebigen Betriebssystemdatenträgern. Sie können jetzt mit vertrauenswürdigen Starts Provisioningschemata erstellen, die einen kurzlebigen Betriebssystemdatenträger unter Windows verwenden. Mit vertrauenswürdigen Starts lässt sich die Sicherheit von VMs der zweiten Generation weiter verbessern. Das Feature schützt vor erweiterten und dauerhaften Angriffstechniken und verknüpft Technologien, die unabhängig voneinander aktiviert werden können, zum Beispiel "Sicherer Start" und vTPM, die virtualisierte Version des Trusted Platform Module. Weitere Informationen zum Erstellen eines Maschinenkatalogs finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Juli 2022

Neue und erweiterte Features

Dynamische Sitzungstimeouts für Maschinen mit Einzelsitzungs-OS. Dynamische Sitzungstimeouts unterstützen jetzt Maschinen mit Einzelsitzungs-OS. Eine Bereitstellungsgruppe mit mindestens einem VDA der Version 2206 oder höher ist erforderlich. Stellen Sie sicher, dass sich diese VDAs mindestens einmal in Citrix Cloud registriert haben. Weitere Informationen finden Sie unter Dynamische Sitzungstimeouts.

Abmeldeerinnerungen in Autoscale senden, ohne die Benutzerabmeldung zu erzwingen. Ein neues Feature ist jetzt in **Benachrichtigungen zur Benutzerabmeldung** (früher **Erzwingen von Benutzerabmeldungen**) in Autoscale verfügbar. Mit diesem Feature können Sie Abmeldeerinnerungen an Benutzer senden, ohne sie zum Abmelden zu zwingen. Dadurch wird ein potenzieller Datenverlust vermieden, der dadurch entsteht, dass Benutzer gezwungen werden, sich von ihren Sitzungen abzumelden. Weitere Informationen finden Sie unter Benachrichtigungen zur Benutzerabmeldung.

Wählbarkeit des Linux OS-Lizenztyps beim Erstellen von Linux-VM-Katalogen in Azure. Auf der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie jetzt beim Erstellen von Linux-VM-Katalogen in Azure auch den Linux OS-Lizenztyp wählen. Sie haben zwei Auswahlmöglichkeiten für selbst bereitgestellte Linux-Lizenzen: Red Hat Enterprise Linux und SUSE Linux Enterprise Server. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Verbesserte Suche in "Vollständige Konfiguration". Der Knoten "Suchen"bietet die folgenden neuen Features und Verbesserungen:

- **Möglichkeit zum Exportieren von Suchergebnissen**. Sie können jetzt Suchergebnisse exportieren. Klicken Sie dazu auf das Exportsymbol in der oberen rechten Ecke.
- **Neuer Filter verfügbar**. Der Filter "Ausstehende Energieaktion"steht jetzt zur Verfügung. Verwenden Sie den Filter, um Ihre Suche zu verfeinern.
- **Unterstützung für "Enthält nicht"für bestimmte Elemente**. Elemente wie Maschinennamen und Tags unterstützen jetzt das Suchkriterium "Enthält nicht".
- **Unterstützung für die Suche nach Objekten beim Hinzufügen von Filtern**. Beim Hinzufügen von Filtern für die folgenden Objekte können Sie nun nach diesen suchen: Verbindungen, Maschinenkataloge, Bereitstellungsgruppen, Anwendungsgruppen und Tags.

Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Unterstützung für VMware-Speicherprofile. Wenn Sie einen Maschinenkatalog mit einem Masterimage in einem vSAN-Datenspeicher erstellen, können Sie jetzt die Speicherrichtlinie wie die RAID-1-

oder RAID-5-Informationen aus dem Masterimage auf die erstellten Zielgeräte kopieren. Bei vorhandenen Katalogen bleibt die Speicherrichtlinie unverändert, auch wenn Sie den Katalog aktualisieren.

Unterstützung für RestrictedKrbHost-SPN-Registrierung. Alle von Citrix MCS erstellten Computerkonten sind jetzt mit `RestrictedKrbHost`-Dienstprinzipalnamen (SPN) registriert. Dadurch wird vermieden, dass der Befehl `setspn` zum Registrieren des SPN für die Computerkonten ausgeführt werden muss, nachdem MCS sie erstellt hat.

Bereitstellen von verpackten Microsoft-Anwendungen über App-Pakete in "Vollständige Konfiguration". Der App-V-Knoten wurde in "App-Pakete"umbenannt und neu gestaltet, damit mehr Arten von Microsoft-Anwendungspaketen berücksichtigt werden. Bisher mussten Sie das Discoverymodul verwenden, um Ihrer Umgebung App-V-Anwendungspakete zur Bereitstellung hinzuzufügen. Sie können die Apps jetzt an einem Ort hinzufügen und bereitstellen, indem Sie den Knoten "App-Pakete" verwenden. Weitere Informationen finden Sie unter App-Pakete.

Unterstützung für die Verwendung von ARM-Vorlagenspezifikationen als Maschinenprofile. Bisher konnten Sie nur VMs als Maschinenprofile verwenden. Sie können jetzt auch ARM-Vorlagenspezifikationen als Maschinenprofile beim Erstellen von Azure-Maschinenkatalogen verwenden. Mit diesem Feature können Sie die Azure ARM-Vorlagenfunktionen wie Versionsverwaltung nutzen. Um sicherzustellen, dass die ausgewählte Spezifikation korrekt konfiguriert ist und die erforderlichen Konfigurationen enthält, führen wir eine Validierung durch. Schlägt die Validierung fehl, werden Sie aufgefordert, ein anderes Maschinenprofil auszuwählen. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Unterstützung für Validierung der ARM-Vorlagenspezifikation. Sie können jetzt die ARM-Vorlagenspezifikation validieren, um sicherzustellen, dass sie als Maschinenprofil zum Erstellen eines Maschinenkatalogs verwendet werden kann. Es gibt zwei Möglichkeiten zur Validierung der ARM-Vorlagenspezifikation:

- Verwenden der Verwaltungsoberfläche "Vollständige Konfiguration"
- Verwenden des PowerShell-Befehls

Weitere Informationen zum Validieren der ARM-Vorlagenspezifikation finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Juni 2022

Neue und erweiterte Features

Unterstützung für Neustartzeitplan für Maschinen mit Einzelsitzungs-OS. Bisher war das Feature für Neustartzeitpläne nur für Maschinen mit Multisitzungs-OS verfügbar. Es ist jetzt auch für Maschinen mit Einzelsitzungs-OS verfügbar. Sie können jetzt Neustartzeitpläne für Bereitstellungsgruppen

erstellen, die Maschinen mit Einzelsitzungs-OS enthalten. Weitere Informationen finden Sie unter Erstellen und Verwalten von Neustartzeitplänen für Maschinen in einer Bereitstellungsgruppe.

Option zum Überprüfen des Benutzernamens. Beim Eingeben der Domänenanmeldeinformationen ist jetzt die Option **Name überprüfen** verfügbar. Mit dieser Option können Sie überprüfen, ob der Benutzername gültig oder eindeutig ist. Diese Option kann in folgenden Situationen von Nutzen sein:

- Der Benutzername existiert in mehreren Domänen. Sie werden aufgefordert, den gewünschten Benutzer auszuwählen.
- Sie können sich nicht an den Domänennamen erinnern. Sie können den Benutzernamen ohne Angabe des Domänennamens eingeben. Bei erfolgreicher Überprüfung wird der Domänenname automatisch eingegeben.

Weitere Informationen finden Sie unter Domänenanmeldeinformationen.

Möglichkeit der Änderung der Netzwerkeinstellung für ein vorhandenes Provisioningschema. Sie können jetzt die Netzwerkeinstellung für ein vorhandenes Provisioningschema ändern, sodass die neuen VMs im neuen Subnetz erstellt werden. Verwenden Sie den Parameter `-NetworkMapping` im Befehl `Set-ProvScheme`, um die Netzwerkeinstellung zu ändern. Nur die neu bereitgestellten VMs aus dem Schema haben die neuen Subnetzeinstellungen. Stellen Sie auch sicher, dass die Subnetze sich unter derselben Hostingeinheit befinden. Weitere Informationen finden Sie unter Ändern der Netzwerkeinstellung für ein vorhandenes Provisioningschema.

Informationen über Namen der Region für Azure-VMs, verwaltete Datenträger, Snapshots, Azure VHD und ARM-Vorlage abrufen. Sie können jetzt Angaben zum Regionsnamen für Azure-VMs, verwaltete Datenträger, Snapshots, Azure VHD und ARM-Vorlagen anzeigen. Diese Informationen werden für Ressourcen im Masterimage angezeigt, wenn ein Maschinenkatalog zugewiesen wird. Weitere Informationen finden Sie unter Abrufen des Regionsnamen für Azure-VMs, verwaltete Datenträger, Snapshots, Azure VHD und ARM-Vorlagen.

Möglichkeit, Eigenschaftswerte des Maschinenprofils in einer Azure-Umgebung zu verwenden. Beim Erstellen eines Azure-Katalogs mit einem Maschinenprofil können Sie jetzt die Eigenschaftswerte über die ARM-Vorlagenspezifikation oder VM festlegen (je nachdem, was als Maschinenprofil verwendet wird), falls diese Werte nicht explizit in den benutzerdefinierten Eigenschaften definiert sind. Folgende Eigenschaften sind von diesem Feature betroffen:

- Verfügbarkeitszone
- ID der dedizierten Hostgruppe
- ID des Datenträgerverschlüsselungssatzes
- Betriebssystemtyp
- Lizenztyp
- Dienstangebot
- Speichertyp

Wenn einige der Eigenschaften im Maschinenprofil fehlen und nicht in den benutzerdefinierten Eigenschaften definiert sind, wird der Standardwert der Eigenschaften angewendet, soweit zutreffend. Weitere Informationen finden Sie unter Verwenden von Eigenschaftswerten für Maschinenprofile.

Erweiterte Unterstützung für VDA-Upgrade. Mit der Oberfläche "Vollständige Konfiguration"können Sie jetzt von MCS bereitgestellte persistente Maschinen aktualisieren. Das Upgrade ist pro Katalog oder pro Maschine möglich. Weitere Informationen finden Sie unter Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration".

Citrix Probe Agent in Steuerungsebenen für Citrix Cloud Japan und Citrix Cloud Government. Citrix Probe Agent unterstützt jetzt Sites, die auf den Steuerungsebenen für Citrix Cloud Japan und Citrix Cloud Government gehostet werden. Um den Testagent in diesen Steuerungsebenen zu verwenden, wählen Sie im Pfad "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" den Registrierungswert 2 für die Region Japan und 3 für "Government". Der Citrix Probe Agent automatisiert die Zustandsüberprüfung virtueller Apps und Desktops, die auf einer Site veröffentlicht sind. Weitere Informationen finden Sie unter Anwendungs- und Desktoptests.

Anpassen des für die Kommunikation zwischen VDAs und Cloud Connectors verwendeten Ports. Sie können den Port, den der VDA für die Kommunikation mit Cloud Connectors verwendet, jetzt entsprechend Ihren spezifischen Sicherheitsanforderungen anpassen. Dieses Feature ist nützlich, wenn Ihr Sicherheitsteam das Öffnen des Standardports (Port 80) nicht zulässt oder wenn der Standardport bereits verwendet wird. Weitere Informationen finden Sie unter Anpassen des Ports für die Kommunikation mit Cloud Connectors.

Unterstützung für das Organisieren von Maschinenkatalogen mit Ordnern. Sie können jetzt verschachtelte Ordner erstellen, um Maschinenkataloge für einfachen Zugriff zu organisieren. Weitere Informationen finden Sie unter Organisieren von Katalogen mit Ordnern.

Unterstützung für SCVMM 2022. Citrix DaaS unterstützt jetzt System Center Virtual Machine Manager (SCVMM) 2022 von Microsoft. SCVMM bietet eine Reihe von Services, darunter die Wartung der Ressourcen, die Sie für die Bereitstellung von VMs benötigen. Weitere Informationen zu den neuen in SCVMM 2022 unterstützten Features finden Sie unter Neuheiten in System Center Virtual Machine Manager.

Unterstützung eines Parameters zum Konfigurieren einer Höchstanzahl gleichzeitiger Provisioningvorgänge in AWS. Citrix DaaS unterstützt jetzt `MaximumConcurrentProvisioningOperations` als konfigurierbare benutzerdefinierte Eigenschaft für MCS in AWS. Die Eigenschaft `MaximumConcurrentProvi` legt fest, wie viele VMs Sie gleichzeitig erstellen oder löschen können. MCS unterstützt standardmäßig bis zu 100 gleichzeitige Provisioningvorgänge. Diesen Wert können Sie jetzt durch Eingabe von PowerShell-Befehlen weiter anpassen. Sie können einen Bereich von 1 bis 1000 eingeben. Durch Festlegen dieser Eigenschaft auf den von gewünschten Wert steuern Sie, wie viele Aufgaben Sie beim Erstellen oder Löschen von VMs parallel ausführen können. Weitere Details zur Konfiguration der Höchstanzahl gleichzeitiger Provisioningvorgänge finden Sie unter Standardwerte für Hostverbindungen.

May 2022

Neue und erweiterte Features

Verbesserte Sitzungsstartdiagnose. Citrix DaaS unterstützt jetzt detaillierte Diagnosedaten für Sitzungsstartfehler. Sie können jetzt die Komponenten anzeigen, die an der Sitzungsstartsequenz beteiligt sind. Die Komponenten, die den zuletzt generierten Fehlercodes verursacht haben, werden hervorgehoben. Auf diese Weise können Sie den genauen Grund für einen Sitzungsstartfehler ermitteln und die empfohlenen Maßnahmen ergreifen.

Die Transaktionsseite wurde um den Bereich "Transaktionsdetails"erweitert, der eine Liste von Komponenten enthält und auf den aufgetretenen Fehler hinweist. Durch Klicken auf den Komponentennamen werden die Komponentendetails und die Details des letzten bekannten Fehlers angezeigt. Der Fehlergrund und der Fehlercode werden angezeigt. Wenn Sie auf den Link für weitere Informationen klicken, wird der spezifische Fehlercode angezeigt, mit einer detaillierten Beschreibung und empfohlene Maßnahmen. Weitere Informationen finden Sie unter Sitzungsdiagnose.

Unterstützung für Set-ProvServiceConfigurationData im Remote PowerShell SDK. Sie können jetzt `Set-ProvServiceConfigurationData` mit dem Remote PowerShell SDK verwenden, um die Einstellungen für alle anwendbaren Parameter vorzunehmen. Mit diesem Befehl können Sie auch das Aktivieren von DHCP während der Imagevorbereitung überspringen. Es folgt die Liste der Einstellungen, die mit `Set-ProvServiceConfigurationData` unterstützt werden:

- Timeout für Imagevorbereitung ändern: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- Aktivieren von DHCP überspringen: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value EnableDHCP`
- Zurücksetzen von Microsoft Windows KMS überspringen: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Zurücksetzen von Microsoft Office KMS überspringen: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`
- Automatisches Herunterfahren der Vorbereitungs-VM deaktivieren: `Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown –Value true`
- Deaktivieren von Domäneneinschleusung: `Set-ProvServiceConfigurationData –Name DisableDomainInjection –Value true`

Wählbarkeit des Linux-Lizenztyps beim Erstellen von Linux-Maschinenkatalogen über PowerShell-Befehle. Mit PowerShell-Befehlen können Sie den Linux-Lizenztyp beim Erstellen von Linux-Maschinenkatalogen festlegen. Sie haben zwei Auswahlmöglichkeiten für selbst bere-

itgestellte Linux-Lizenzen: RHEL_BYOS und SLES_BYOS. Die Standardeinstellung ist die Azure Linux-Lizenzierung. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Unterstützung der Identifizierung aller von MCS erstellten Azure-Ressourcen. Mit dem Tag `provschemeID` können Sie jetzt alle von den Maschinenerstellungsdiensten (MCS) erstellten Azure-Ressourcen (z. B. Image, ID-Datenträger, OS-Datenträger, Netzwerkkarte, VM usw.) identifizieren, die mit einem ProvScheme verknüpft sind. Weitere Informationen zu den Tags, die MCS zu den Ressourcen hinzufügt, finden Sie unter Identifizieren der von MCS erstellten Ressourcen.

Unterstützung für Azure Stack HCI-Provisioning über SCVMM. MCS unterstützt jetzt das Provisioning von Azure Stack HCI über Microsoft System Center Virtual Machine Manager (SCVMM). Sie können den Azure Stack HCI-Cluster mit vorhandenen Tools wie SCVMM verwalten. Weitere Informationen finden Sie unter Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen.

Unterstützung für das manuelle Hinzufügen von Nicht-Active Directory-Benutzern. Mit der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie jetzt eine durch Semikolon getrennte Liste von Benutzernamen eingeben, wenn Sie Nicht-Active Directory-Benutzer für einen Katalog hinzufügen. Beachten Sie das Format, wenn Sie Benutzer hinzufügen, die sich in verschiedenen Verzeichnissen befinden. Wenn sich die Benutzer beispielsweise in Active Directory befinden, geben Sie die Namen direkt ein. Falls nicht, geben Sie die Namen in diesem Format ein: `<identity provider>:<user name>`. Beispiel: `AzureAD:username`. Weitere Informationen finden Sie unter Erstellen des Maschinenkatalogs.

April 2022

Neue und erweiterte Features

Homepage für die Oberfläche "Vollständige Konfiguration". Die vollständige Konfiguration hat nun eine Homepage, welche einen Überblick über Ihre Citrix DaaS-Bereitstellung und Workloads sowie Informationen bietet, mit deren Hilfe Sie Ihr Abonnement optimal nutzen können. Die Seite besteht aus den folgenden Bereichen:

- **Serviceübersicht**. Bietet einen Überblick über Ihre Citrix DaaS-Bereitstellung und Ihre Workloads.
- **Empfehlungen**. Empfiehlt Features, die mit Ihrem Abonnement verfügbar sind, und erfasst Ihr Feedback.
- **Neue Features**. Zeigt die neuesten Features an.
- **Preview-Features**. Zeigt Features an, die sich derzeit in der Preview befinden.
- **Erste Schritte**. Führt Sie durch die Ersteinrichtung.

Weitere Informationen finden Sie unter Homepage.

Zeigt den Fortschritt der Katalogerstellung und Aktualisierungen an. Mit der vollständigen Konfiguration bleiben Sie jetzt über die Erstellung und Aktualisierung von Katalogen informiert. Sie können sich einen Überblick über den Erstellungs- und Aktualisierungsprozess verschaffen, den Verlauf der ausgeführten Schritte anzeigen und den Fortschritt und die Ausführungszeit des aktuellen Schritts überwachen. Weitere Informationen finden Sie unter Beginnen der Katalogerstellung.

Anzeige verfügbarer Hypervisors und Cloudservices basierend auf der ausgewählten Zone. In der vollständigen Konfiguration müssen Sie beim Erstellen von Hostingverbindungen eine Zone auswählen, bevor Sie einen Verbindungstyp auswählen. In der Dropdownliste "Verbindungstyp" werden Hypervisors und Clouddienste angezeigt, die mit der Zone verfügbar sind. Bisher mussten Sie das zugehörige Plug-In in jeder Zone installieren, damit in der Liste der Verbindungstypen der erforderliche Hypervisor oder Cloudservice angezeigt wurde. Bei dieser neuen Konfigurationsfolge können Sie das Plug-In jetzt nur in der erforderlichen Zone installieren.

Sie können auch mit einem PowerShell-Befehl die Liste der Hypervisor-Plug-Ins abrufen, die in der ausgewählten Zone verfügbar sind. Weitere Informationen finden Sie unter Erstellen einer Verbindung und von Ressourcen.

Unterstützung für Nicht-On-Premises-AD-Benutzer in der vollständigen Konfiguration. Das neue Feld, **Identitätstyp auswählen**, ist in den Schnittstellen verfügbar, in denen Sie Benutzer bereitgestellten Desktops oder Apps bzw. Bereitstellungsgruppen oder Anwendungsgruppen zuweisen. Über das Feld können Sie jetzt Benutzerkonten von jedem der folgenden Identitätsanbieter auswählen, mit dem Ihre Citrix Cloud verbunden ist:

- Active Directory
- Azure Active Directory
- Okta

Möglichkeit, ungültige benutzerdefinierte Eigenschaften auf Google Cloud Platform (GCP) und in und Azure-Umgebungen abzulehnen. Sie können jetzt Probleme vermeiden, wenn benutzerdefinierte, für `New-ProvScheme` und `Set-ProvScheme` festgelegte Eigenschaften nicht wirksam werden. Wenn Sie eine nicht vorhandene benutzerdefinierte Eigenschaft angeben, wird eine Fehlermeldung angezeigt. Weitere Informationen finden Sie unter Richtlinien zum Festlegen benutzerdefinierter Eigenschaften.

Unterstützung für das Erstellen von Maschinen mit Azure Active Directory-Einbindung (Preview). Wenn Sie in der **vollständigen Konfiguration** einen Katalog erstellen, ist jetzt der Identitätstyp **In Azure Active Directory eingebunden** unter **Maschinenidentitäten**verfügbar. Über diesen Identitätstyp können Sie mit MCS Maschinen erstellen, die in Azure Active Directory eingebunden sind. Mit der zusätzlichen Option **Maschinen bei Microsoft Intune registrieren** können Sie die Maschinen in Microsoft Intune für die Verwaltung registrieren.

Informationen zum Erstellen von in Azure Active Directory eingebundenen Katalogen finden Sie unter Erstellen von Maschinenkatalogen. Informationen zu Anforderungen und Überlegungen zu Azure Ac-

tive Directory finden Sie unter In Azure Active Directory eingebunden.

Unterstützung für das Erstellen von Maschinen mit Azure Active Directory-Hybrideinbindung (Preview). Wenn Sie in der **vollständigen Konfiguration** einen Katalog erstellen, ist jetzt der Identitätstyp **Azure Active Directory-Hybrideinbindung** unter **Maschinenidentitäten**verfügbar. Über diesen Identitätstyp können Sie mit MCS Maschinen erstellen, die eine Azure Active Directory-Hybrideinbindung haben. Diese Maschinen gehören einer Organisation und sind mit einem Active Directory Domain Services-Konto dieser Organisation angemeldet.

Informationen zum Erstellen von in Katalogen mit Azure Active Directory-Hybrideinbindung finden Sie unter Erstellen von Maschinenkatalogen. Informationen zu Anforderungen und Überlegungen zu Azure Active Directory-Hybrideinbindungen finden Sie unter Azure Active Directory-Hybrideinbindung.

Unterstützung vertrauenswürdiger Starts in Azure für Snapshots. Vertrauenswürdiger Start von Azure ist neben Images jetzt auch für Snapshots verfügbar. Wenn Sie einen Snapshot mit aktiviertem vertrauenswürdigen Start auswählen, ist die Verwendung eines Maschinenprofils obligatorisch. Außerdem müssen Sie ein Maschinenprofil mit aktiviertem vertrauenswürdigen Start auswählen. Weitere Informationen finden Sie im Artikel Microsoft Azure Resource Manager-Cloudumgebungen.

Export von Maschinen. Sie können jetzt Maschinen, die auf der Seite **Maschinen** des **Assistenten für die Einrichtung von Maschinenkatalogen** aufgeführt werden, in eine CSV-Datei exportieren, um sie als Vorlage beim Hinzufügen großer Mengen von Maschinen zu einem Katalog zu verwenden. Weitere Informationen finden Sie unter Hinzufügen von Maschinen zum Maschinenkatalog.

Option zum Zugriff auf die Workspace Environment Management-Webkonsole. Das Menü der Registerkarte **Verwalten** enthält jetzt die Option "Environment Management (Web)". Mit dieser können Sie die neue webbasierte Workspace Environment Management-Konsole aufrufen. Verwenden Sie das **Environment Management**, um auf die Legacy-Konsole zuzugreifen. Wir sind dabei, sämtliche Funktionen von der Legacykonsole zu der neuen Webkonsole zu migrieren. Die Webkonsole reagiert in der Regel schneller als die Legacykonsole. Weitere Informationen finden Sie unter Workspace Environment Management Service.

Möglichkeit der Verwaltung von ProvScheme-Parametern. Wenn Sie Kataloge mit MCS erstellen, wird jetzt eine Fehlermeldung angezeigt, wenn Sie die Parameter für `New-ProvScheme` in nicht unterstützten Hypervisors bei der Maschinenkatalogerstellung festlegen oder die Parameter für `Set-ProvScheme` nach Erstellung des Maschinenkatalogs aktualisieren. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Höhere Limits für Ressourcenstandorte. Ressourcenstandortlimits für Einzelsitzungs-VDAs und Multisitzungs-VDAs wurden jetzt auf 10.000 bzw. 1.000 erhöht. Weitere Informationen finden Sie unter Limits.

Unterstützung für den Neustart nicht energieverwalteter Maschinen nach dem Draining der Sitzungen. Mit Citrix DaaS können Sie jetzt Neustartzeitpläne für nicht energieverwaltete Maschinen

nach dem Draining aller Sitzungen von den Maschinen erstellen. Wählen Sie in der Oberfläche "Vollständige Konfiguration"**Alle Maschinen nach dem Draining der Sitzungen neu starten** für **Neustartdauer**. Weitere Informationen finden Sie unter Erstellen eines Neustartzeitplans.

Unterstützung für das Upgrade von VDA-Maschinen (Preview). Mit der Oberfläche "Vollständige Konfiguration"können Sie jetzt ein Upgrade von VDA-Maschinen für Ihre Citrix DaaS-Bereitstellung ausführen. Das Upgrade ist pro Katalog oder pro Maschine möglich. Das Feature gilt für nicht mit MCS erstellte Maschinen (z. B. physische Maschinen). Weitere Informationen finden Sie unter Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration".

Maschinen werden bei einem Ausfall nicht heruntergefahren. Citrix DaaS verhindert jetzt, dass virtuelle Maschinen vom Broker heruntergefahren werden, wenn es in ihrer Zone zu einem Ausfall kommt. Nach dem Ende des Ausfalls werden die Maschinen automatisch für Verbindungen verfügbar. Sie müssen keine Maßnahmen ergreifen, um die Maschinen nach dem Ausfall verfügbar zu machen.

Sitzungsstartdiagnose Citrix DaaS unterstützt jetzt eine erweiterte Fehlerdiagnose beim Sitzungsstart. Verwenden Sie die von der Citrix Workspace-App generierte 32-stellige (8-4-4-4-12) Transaktions-ID aus Citrix Monitor (also dem Citrix Director-Dienst), um präzise einzugrenzen, welche Komponente und Phase das Problem verursacht, und wenden Sie die angegebenen Lösungsvorschläge an. Weitere Informationen finden Sie unter Sitzungsstartdiagnose.

Option zum Zugriff auf den Sitzungsaufzeichnungsdienst. Das Menü der Registerkarte **Verwalten** enthält jetzt die Option "Sitzungsaufzeichnung". Der neu eingeführte Sitzungsaufzeichnungsdienst ermöglicht die zentrale Verwaltung von Richtlinien, Wiedergabe und Serverkonfigurationen. Er entlastet IT-Administratoren, indem er einen einheitlichen Einstiegspunkt für die Verwaltung und Überwachung der verteilten Objekte in Ihrem Unternehmen bietet. Weitere Informationen finden Sie unter Sitzungsaufzeichnungsdienst (Preview).

Umbenennung von Citrix Virtual Apps and Desktops Service. **Citrix Virtual Apps and Desktops Service** wurde umbenannt in **Citrix DaaS**. Weitere Informationen zur Namensänderung finden Sie in der Ankündigung in unserem Blog.

Die folgenden Angebote im Citrix Virtual Apps and Desktops Service wurden umbenannt.

- **Citrix Virtual Apps Service Advanced** wurde umbenannt in **Citrix DaaS Advanced**.
- **Citrix Virtual Apps Service Premium** wurde umbenannt in **Citrix DaaS Premium**.
- **Citrix Virtual Desktops Service** wurde umbenannt in **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops Service Advanced** wurde umbenannt in **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops Service Premium** ist jetzt als **Citrix DaaS Premium und Citrix DaaS Premium Plus** verfügbar.
- **Citrix Virtual Apps and Desktops Standard für Azure** wurde umbenannt in **Citrix DaaS Standard für Azure**.

- **Citrix Virtual Apps and Desktops Standard für Google Cloud** wurde umbenannt in **Citrix DaaS Standard für Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium für Google Cloud** wurde umbenannt in **Citrix DaaS Premium für Google Cloud**.

Die Implementierung dieser Umstellung in unsere Produkte und deren Dokumentation ist ein kontinuierlicher Prozess. Wir danken Ihnen für Ihre Geduld während dieser Umstellung.

- Die Benutzeroberfläche, produktinterne Inhalte sowie Bilder und Anweisungen in der Produktdokumentation werden in den kommenden Wochen aktualisiert.
- Es ist möglich, dass einige Elemente (z. B. Befehle und MSIs) ihre früheren Namen beibehalten, damit vorhandene Kundenskripts auch weiter funktionieren.
- Die zugehörige Produktdokumentation und andere Ressourcen (z. B. Videos und Blogposts), zu denen es Links in dieser Produktdokumentation gibt, verwenden möglicherweise weiterhin die früheren Namen.

> **Hinweis:**
>
> Der Name des On-premises-Produkts **Citrix Virtual Apps and Desktops** bleibt unverändert.

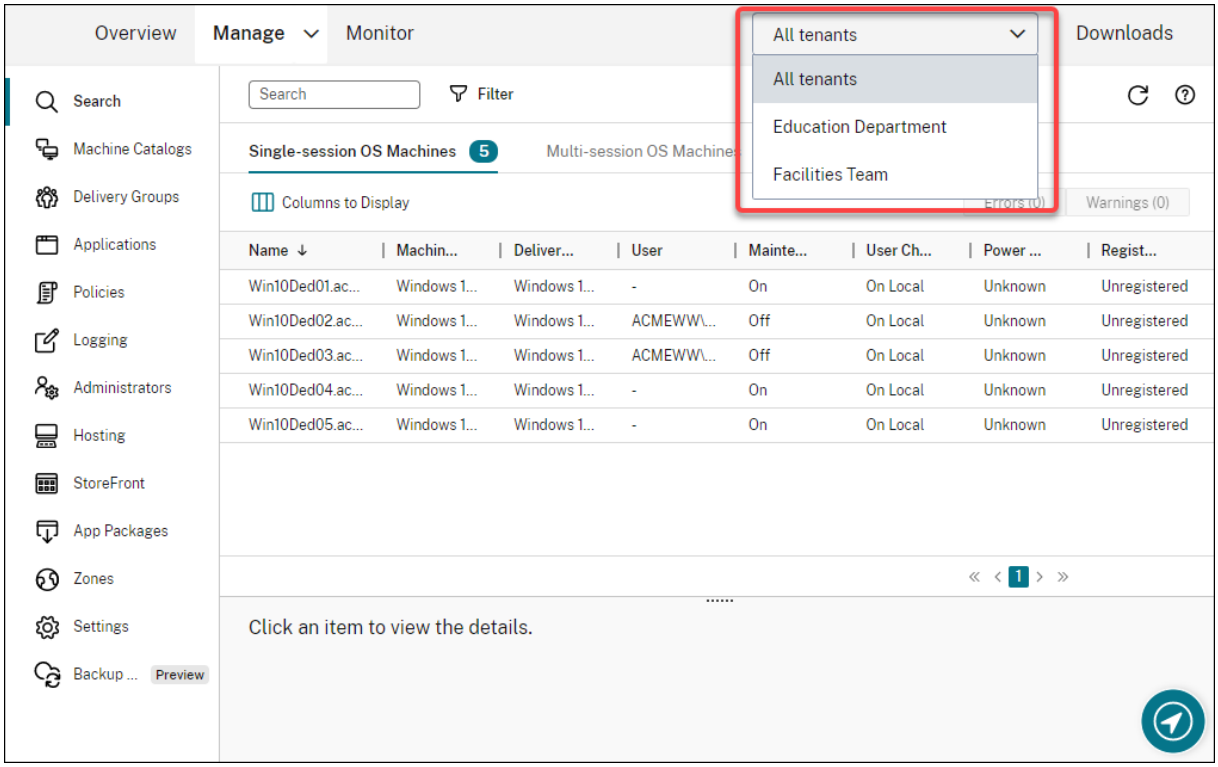
Mandantenunterstützung in "Vollständige Konfiguration" Sie können jetzt Konfigurationspartitionen innerhalb einer einzigen Citrix DaaS-Instanz erstellen. Hierfür erstellen Sie unter **Administratoren > Geltungsbereiche** einzelne Mandantenbereiche, denen Sie dann zugehörige Konfigurationsobjekte (z. B. Maschinenkataloge und Bereitstellungsgruppen) zuordnen. Administratoren mit Zugriff auf einen Mandanten können damit nur die Objekte verwalten, die mit dem Mandanten verknüpft sind. Das Feature ist in folgenden Fällen besonders nützlich:

- Ihre Organisation besitzt mehrere Geschäftssilos (unabhängige Abteilungen oder separate IT-Teams) oder
- Ihre Organisation betreibt mehrere On-Premises-Sites und möchte dasselbe Setup in einer einzigen Citrix DaaS-Instanz beibehalten.

Auf der Oberfläche "Vollständige Konfiguration"können Sie zudem Mandantenkunden nach Namen filtern. Standardmäßig werden auf der Oberfläche Informationen zu allen Mandanten angezeigt.

Das Feature ist für Citrix Service Provider (CSPs) und für Nicht-CSPs verfügbar. Die Oberfläche in einer CSP-Umgebung entspricht im Wesentlichen der in einer Nicht-CSP-Umgebung, mit Ausnahme der Methode, mit der Mandanten erstellt werden.

- CSPs integrieren Mandantenkunden per Onboarding in Citrix DaaS und konfigurieren dann den Administratorzugriff auf Citrix DaaS. Weitere Informationen finden Sie unter Citrix DaaS für Citrix Service Provider.
- Nicht-CSPs erstellen Mandantenkunden, indem sie zunächst Geltungsbereiche erstellen und dann den benutzerdefinierten Zugriff für die jeweiligen Administratoren konfigurieren. Weitere Informationen finden Sie unter Erstellen und Verwalten von Geltungsbereichen.



Updates für Autoscale. Autoscale wurde aktualisiert und bietet jetzt einen benutzerfreundlichen Blattstil. Die Workflows zur Konfiguration bleiben unverändert. Weitere Updates von Autoscale:

- Die Funktion **Autoscale einschränken** wurde zum besseren Verständnis umbenannt in **Autoscale getaggte Maschinen**.
- Die Option **Steuern, wann Autoscale mit dem Einschalten von getaggten Maschinen beginnt** wurde neu hinzugefügt. Mit dieser Option können Sie steuern, wann Autoscale (basierend auf der Nutzung von ungetaggten Maschinen) mit dem Einschalten von getaggten Maschinen beginnt.

Weitere Informationen zu diesem Feature finden Sie unter Autoscale getaggte Maschinen.

Prüfung der Lizenzgültigkeit. Auf der Oberfläche "Vollständige Konfiguration"wird jetzt automatisch die Gültigkeit von Lizenzen geprüft, die von Hostverbindungen verwendet werden. Hostverbindungen mit ungültiger Lizenz werden in den Wartungsmodus versetzt. Sie können dann bestimmte Vorgänge nicht ausführen, z. B. die Verbindung bearbeiten und den Wartungsmodus ausschalten. Eine Lizenz wird beispielsweise ungültig in diesen Fällen:

- Die Lizenz ist abgelaufen. Wenden Sie sich in diesem Fall an Ihren Citrix Vertriebsmitarbeiter, um die Lizenz zu verlängern oder neue Lizenzen zu erwerben.
- Die Lizenz wurde vom Lizenzserver gelöscht.

Anwendung des Blattstils auf Knoten für Maschinenkataloge und Richtlinien. Blattstile werden jetzt auf alle Knoten in "Vollständige Konfiguration"angewendet.

Unterstützte Aktualisierung von mit MCS bereitgestellten Maschinen in Azure-Umgebungen. `Set-ProvScheme` ändert die Vorlage (Provisioningschema) und wirkt sich nicht auf vorhandene Maschinen aus. Mit dem Befehl Request-ProvVMUpdate können Sie jetzt das aktuelle Provisioningschema auf eine oder mehrere vorhandene Maschine(n) anwenden. Die derzeit von diesem Feature unterstützte aktualisierte Eigenschaft ist `ServiceOffering`. Weitere Informationen finden Sie unter Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema.

März 2022

Neue und erweiterte Features

Citrix Virtual Apps and Desktops für Google Cloud ist im Google Cloud Marketplace verfügbar. Citrix Virtual Apps and Desktops Premium für Google Cloud kann jetzt im Google Cloud Marketplace erworben werden. Citrix Virtual Apps and Desktops Premium für Google Cloud führt die Dienststeuerungsebene für Citrix Virtual Apps and Desktops in Google Cloud aus.

Unterstützung für vertrauenswürdige Starts in Azure. Die Verwaltungsoberfläche "Vollständige Konfiguration"bietet jetzt Unterstützung für vertrauenswürdige Starts von Azure. Wenn Sie ein Image mit aktiviertem vertrauenswürdigen Start auswählen, ist die Verwendung eines Maschinenprofils obligatorisch. Außerdem müssen Sie ein Maschinenprofil mit aktiviertem vertrauenswürdigen Start auswählen. Weitere Informationen finden Sie im Artikel Microsoft Azure Resource Manager-Cloudumgebungen.

Der Blattstil wird bei "Vollständiger Konfiguration"in drei weiteren Knoten auf Assistenten angewendet. Die Knoten sind **Suchen**, **Bereitstellungsgruppen** und **Anwendungen**.

Image Portability Service (IPS) ist jetzt allgemein verfügbar. Mit IPS können Sie Images einfacher plattformübergreifend verwalten. Das Feature erleichtert das Verwalten von Images zwischen einem on-premises bereitgestellten Ressourcenstandort und der öffentlichen Cloud. REST-APIs für Citrix Virtual Apps and Desktops ermöglichen die automatisierte Verwaltung von Ressourcen innerhalb einer Citrix Virtual Apps and Desktops-Site. Weitere Informationen finden Sie unter Migration von Workloads in die öffentliche Cloud.

Februar 2022

Neue und erweiterte Features

Azure-Berechtigungen. Aufgrund von Sicherheitsanforderungen und zur Minimierung des Risikos sind zwei Gruppen von Berechtigungen erforderlich.

- Mindestberechtigungen: Diese Berechtigungen bieten eine bessere Sicherheitskontrolle. Neue Features, die zusätzliche Berechtigungen erfordern, schlagen jedoch fehl, wenn nur die Mindestberechtigungen verwendet werden.
- Allgemeine Berechtigungen: Diese Berechtigungen hindern Sie nicht daran, neue Erweiterungsvorteile zu erhalten.

Weitere Informationen finden Sie unter Informationen zu Azure-Berechtigungen.

Unterstützte Verwendung des temporären VM-Datenträgers als Host des Zurückschreibcache-datenträgers in Azure-Umgebungen. Wir haben die Option **Nicht-persistenten Datenträger für Zurückschreibcache verwenden** zur Seite **Maschinenkatalogerstellung > Datenträgereinstellungen** der Oberfläche **Verwalten > Vollständige Konfiguration** hinzugefügt. Wählen Sie diese Option, wenn der Datenträger für den Zurückschreibcache für die bereitgestellten VMs nicht persistent sein soll. Wenn die Option ausgewählt ist, wird der temporäre Datenträger der VM zum Host für den Zurückschreibcache, sofern der Datenträger über ausreichend Speicherplatz verfügt. Dies ermöglicht Ihnen eine Kostenersparnis. Weitere Informationen finden Sie im Artikel Microsoft Azure Resource Manager-Cloudumgebungen.

Aktualisierung der Standardeinstellungen für AWS-Hostverbindungen. Die Standardeinstellungswerte für die AWS-Hostverbindung wurden erhöht und sind höchstwahrscheinlich für alle AWS-Cloudplattformen identisch. Dies erleichtert das Erstellen von Hostverbindungen in AWS-Cloudumgebungen, ohne die Standardeinstellungswerte entsprechend der individuellen Einrichtung auszuwerten und zu konfigurieren. Weitere Informationen finden Sie unter Standardwerte für Hostverbindungen.

Verschiedene Speicherebenen in GCP-Umgebungen jetzt unterstützt. Sie können jetzt die folgenden benutzerdefinierten Eigenschaften in den GCP-Umgebungen angeben, um den Speichertyp der Datenträger festzulegen, die mit der neu erstellten VM verbunden sind:

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Service-SDK.

VM-Einstellungen nach dem Erstellen von Azure VM-Katalogen ändern. Mit der Verwaltungsoberfläche “Vollständige Konfiguration”können Sie jetzt nach dem Erstellen eines Katalogs folgende Einstellungen ändern:

- Maschinengröße
- Verfügbarkeitszonen
- Maschinenprofil
- Windows-Lizenzen

Wählen Sie dazu den Katalog im Knoten **Maschinenkataloge** aus und wählen Sie dann in der Aktionsleiste **Maschinenkatalog bearbeiten**. Weitere Informationen finden Sie unter Bearbeiten eines Katalogs.

Unterstützung für Speicherung kurzlebiger Azure-Betriebssystemdatenträger auf Cachedatenträger oder temporärem Datenträger. Mit dem Citrix Virtual Apps and Desktops Service können Sie jetzt den kurzlebigen Azure-Betriebssystemdatenträger entweder auf dem Cache-Datenträger oder auf einem temporären Datenträger für eine virtuelle Azure-Maschine speichern. Dies ist nützlich für Azure-Umgebungen, die anstelle von Standard-HDD-Datenträgern leistungsstärkere SSD-Datenträger erfordern. Weitere Informationen finden Sie im Artikel Microsoft Azure Resource Manager-Cloudumgebungen.

Unterstützung für Nutanix-Cluster auf AWS. Citrix Virtual Apps and Desktops Service unterstützt Nutanix-Cluster auf AWS. Nutanix-Cluster vereinfachen das Ausführen von Anwendungen in privaten oder mehreren öffentlichen Clouds. Weitere Informationen finden Sie unter Nutanix-Cluster auf AWS.

Unterstützung für VMware-Cloud auf Amazon Web Services (AWS). Mit VMware-Cloud on Amazon Web Services (AWS) können Sie VMware-basierte, on-premises bereitgestellte Citrix Workloads zur AWS-Cloud und Ihre Citrix Virtual Apps and Desktops-Kernumgebung zu Citrix Virtual Apps and Desktops Service migrieren. Weitere Informationen finden Sie unter VMware-Cloud auf Amazon Web Services (AWS)

Unterstützung für die Konfiguration eines Zurückschreibcache-Datenträgers für Maschinen, die unter Google Cloud Platform (GCP) ausgeführt werden. In der Managementbenutzeroberfläche für die vollständige Konfiguration können Sie jetzt beim Provisioning von Maschinen auf GCP die folgenden Einstellungen für den Zurückschreibcache-Datenträger konfigurieren:

- Datenträgergröße
- Dem Cache zugewiesener Speicher
- Typ des Datenträgerspeichers
- Datenträger-Persistenz

Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs im Artikel Google Cloud Platform-Virtualisierungsumgebungen.

Januar 2022

Neue und erweiterte Features

Unterstützung für Nutanix-Cluster auf AWS. Citrix Virtual Apps and Desktops Service unterstützt jetzt Nutanix-Cluster auf AWS. Diese Unterstützung bietet dieselbe Funktionalität wie ein on-premises

bereitgestellter Nutanix-Cluster. Es wird nur ein einziger Cluster unterstützt: *Prism Element*. Weitere Informationen finden Sie unter Nutanix-Virtualisierungsumgebungen.

Neue Features in Cloud Health Check. Cloud Health Check wurde aktualisiert. Zu den Features gehören:

- **Automatischer Fix.** Die Cloud-Integritätsprüfung unterstützt jetzt die automatische Erkennung und Behebung bestimmter Probleme auf den Maschinen, auf denen sie ausgeführt wird. Es gibt jetzt einen Ergebnisbericht, der zeigt, welche spezifischen Maßnahmen ergriffen wurden. Weitere Informationen finden Sie unter Automatischer Fix.
- **Unterstützung der Befehlszeile.** Cloud Health Check kann jetzt über die Befehlszeile ausgeführt werden. Weitere Informationen finden Sie unter Ausführen von Cloud Health Check an der Befehlszeile.
- **Status von Citrix Universal Injection Driver** Cloud Health Check zeigt jetzt den Citrix UVI-Treiberstatus an und bietet eine entsprechende Ereignisprotokollprüfung für Citrix UVI-Treiber.
- **Prüfung auf Registrierungseinstellungen für den Sitzungsstart.** Cloud Health Check prüft jetzt auf Registrierungseinstellungen für den Sitzungsstart.
- **Neues am Prüfungsbericht.** Bei Prüfelementen mit mehreren Prüfpunkten listet der abschließende Prüfungsbericht nun alle Prüfungen auf, um zu zeigen, welche Aktionen bei der Integritätsprüfung durchgeführt wurden.

Weitere Informationen finden Sie unter Cloud Health Check.

Behandlung von Problemen bei der VDA-Registrierung und beim Sitzungsstart über "Vollständige Konfiguration". Mit der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie jetzt die Integrität von VDAs überprüfen. Bei VDA-Integritätsprüfungen wird die mögliche Ursache häufiger Probleme bei der VDA-Registrierung und beim Sitzungsstart gesucht. Sie können Integritätsprüfungen einzeln und in Gruppen durchführen. Weitere Informationen finden Sie unter VDA-Integritätsprüfungen.

Angeben des Ablaufdatums des Azure-Geheimnisses für vorhandene Verbindungen. Mit der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie jetzt das Datum angeben, an dem das Anwendungsgeheimnis abläuft. Informationen zum Anzeigen des Ablaufdatums des Geheimnisses finden Sie unter Microsoft Azure Resource Manager-Cloudumgebungen. Beachten Sie bei der Verwendung dieses Features die folgenden Unterschiede:

- Das Ablaufdatum manuell in Azure erstellter Dienstprinzipale können Sie direkt auf der Seite **Verbindung bearbeiten > Verbindungseigenschaften** bearbeiten.
- Wenn Sie das Ablaufdatum für Dienstprinzipale, die für Sie über die Oberfläche "Vollständige Konfiguration"erstellt wurden, erstmals ändern möchten, gehen Sie zu **Verbindung bearbeiten > Einstellungen bearbeiten > Vorhandene verwenden**. Weitere Änderungen können Sie dann auf der Seite **Verbindung bearbeiten > Verbindungseigenschaften** vornehmen.

Schaltfläche zum Hinzufügen von Administratoren. Eine Schaltfläche **Administrator hinzufügen** ist nun auf der Registerkarte **Vollständige Konfiguration > Administratoren > Administratoren** verfügbar. Über sie gelangen Sie schnell zu **Identitäts- und Zugriffsverwaltung > Administratoren**, wo Sie Administratoren hinzufügen (einladen) können. Weitere Informationen finden Sie unter Hinzufügen von Administratoren.

Neugestaltung der Assistenten in der vollständigen Konfiguration. Das Design der Assistenten an den folgenden Knoten wurde mit neuen Farben, Schriftarten und Formatierungsänderungen zur Verbesserung der Benutzererfahrung aufgewertet: **Administratoren**, **Hosting**, **StoreFront**, **App-Pakete**, **Zones**und **Einstellungen**. Die neuen Assistenten werden in breiteren Blattansichten und somit mit mehr Inhalt pro Ansicht angezeigt. Die Workflows zur Konfiguration bleiben unverändert.

Unterstützung für das Beibehalten des Systemdatenträgers, wenn MCS-I/O für Maschinen aktiviert ist, die auf Google Cloud Platform (GCP) ausgeführt werden. In der Verwaltungsschnittstelle "Vollständige Konfiguration"können Sie beim Maschinen-Provisioning in GCP jetzt den Systemdatenträger bei Energiezyklen beibehalten, wenn die MCS-Speicheroptimierung (MCS-E/A) aktiviert ist. Weitere Informationen finden Sie unter Aktivieren der neuen MCS-Speicheroptimierung.

Unterstützung für direkten Upload oder Download von EBS auf Amazon Web Services (AWS). AWS bietet jetzt eine API zum direkten Erstellen des EBS-Volumes mit dem gewünschten Inhalt. Sie können jetzt die API verwenden, um die Volumeworker-Anforderung für die Katalogerstellung und das Hinzufügen von virtuellen Maschinen zu vermeiden. Informationen zu den hierfür erforderlichen AWS-Berechtigungen finden Sie unter Amazon Web Services Cloudumgebungen.

Möglichkeit des Identifizierens von über MCS erstellte Amazon Web Services-Ressourcen. Es gibt das neue Tag `CitrixProvisioningSchemeID` zur Identifizierung von MCS erstellter AWS-Ressourcen. Weitere Informationen finden Sie unter Identifizieren der von MCS erstellten Ressourcen.

Möglichkeit der Konfiguration des Zugriffs auf Verwaltung und Überwachung. Die Oberfläche "Vollständige Konfiguration"bietet jetzt zusätzliche Optionen zur Steuerung des Zugriffs auf **Verwalten** und **Überwachen**. Weitere Informationen finden Sie unter Erstellen und Verwalten von Rollen.

Dezember 2021

Neue und erweiterte Features

Unterstützung für Google Cloud VMware Engine. Mit der Plattform können Sie jetzt VMware-basierte On-Premises-Citrix Workloads zu Google Cloud und Ihre Citrix Virtual Apps and Desktops-Kernumgebung zu Citrix Virtual Apps and Desktops Service migrieren. Weitere Informationen finden Sie unter Unterstützung für Google Cloud Platform (GCP) VMware Engine.

Bei der Angabe eines Benennungsschemas Angeben des Beginns von Kontonamen. Ab diesem Release gibt es auf der Seite **Maschinenkatalogerstellung > Maschinenidentitäten** der Verwaltung-

soberfläche “Vollständige Konfiguration”eine neue Option. Mit dieser Option können Sie Zahlen oder Buchstaben für den Beginn von Kontonamen angeben und haben so mehr Kontrolle darüber, wie Maschinenkonten bei der Katalogerstellung benannt werden. Weitere Informationen finden Sie unter Maschinenidentitäten.

Unterstützung für die Erstellung von Nutanix AHV XI- und Nutanix AHV Prism Central (PC)-Verbindungen. In der Oberfläche “Vollständige Konfiguration”können Sie jetzt Nutanix AHV XI- und Nutanix AHV PC-Verbindungen erstellen. Weitere Informationen finden Sie unter Nutanix-Virtualisierungsumgebungen.

Unterstützung für die Auswahl des Speichertyps für Betriebssystemdatenträger bei der Bereitstellung von VMs auf GCP. In der Verwaltungsoberfläche “Vollständige Konfiguration”können Sie jetzt beim Provisioning von VMs in GCP den Speichertyp für den Betriebssystemdatenträger auswählen. Auf der Seite **Maschinenkatalogerstellung > Speicher** werden die Speicheroptionen **Persistente Standarddatenträger**, **Persistente ausbalancierte Datenträger** und **Persistente SSD-Datenträger** angeboten. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Die Oberfläche “Vollständige Konfiguration”unterstützt jetzt kurzlebige Azure-Datenträger. Zuvor konnten Maschinen mit kurzlebigen Betriebssystemdatenträgern nur mit PowerShell erstellt werden. Auf der Seite **Maschinenkatalogerstellung > Speicher- und Lizenztypen** wurde die neue Option **Kurzlebiger Azure-Betriebssystemdatenträger** hinzugefügt. Wählen Sie diese Option, wenn der lokale Datenträger der VM zum Hosten des Betriebssystemdatenträgers verwendet werden soll. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Schützen mit MCS verwalteter Ressourcen vor versehentlichem Löschen. Sie können jetzt mit MCS verwaltete Ressourcen auf Google Cloud Platform (GCP) durch Anwenden des für die VMs aktivierten GCP-Flags `deletionProtection` schützen. Mit der Berechtigung `compute.instances.setDeletionProtection` oder die IAM-Rolle “Compute-Administrator”können Sie das Flag zurücksetzen, damit eine Ressource gelöscht werden kann. Die Funktion gilt für persistente und nicht persistente Kataloge. Weitere Informationen finden Sie unter Schutz vor versehentlichem Löschen von Maschinen.

November 2021

Neue und erweiterte Features

Kommentieren von Images beim Aktualisieren von Maschinen. In der Oberfläche “Vollständige Konfiguration”können Sie jetzt Images kommentieren, indem Sie beim Aktualisieren eines mit MCS erstellten Katalogs einen Hinweis hinzufügen. Bei jeder Aktualisierung des Katalogs wird ein Hinweis-Eintrag erstellt, unabhängig davon, ob Sie einen Hinweis hinzufügen. Wenn Sie beim Aktualisieren des

Katalogs keinen Hinweis hinzuzufügen, wird der Eintrag als Null (-) angezeigt. Um den Hinweisverlauf für ein Image anzuzeigen, wählen Sie den Katalog, klicken Sie im unteren Bereich auf **Vorlageneigenschaften** und klicken Sie dann auf **Hinweisverlauf anzeigen**. Weitere Informationen finden Sie unter Aktualisieren von Maschinenkatalogen.

Unterstützung für Multi-Typ-Lizenzierung. Die Verwaltungsschnittstelle der vollständigen Konfiguration unterstützt jetzt die Multityplizenzierung, sodass Sie angeben können, welche Lizenzberechtigung die Site (d. h. die Bereitstellung eines Citrix Virtual Apps and Desktops Service-Produkts) und welche Bereitstellungsgruppen verwenden sollen.

- Auf Site-Ebene legen Sie fest, welche Lizenz Site-übergreifend verwendet werden soll, wenn Benutzer eine App oder einen Desktop auf ihren Geräten starten. Die ausgewählte Lizenz gilt für alle Bereitstellungsgruppen, mit Ausnahme derer, für die eine eigene Lizenz konfiguriert wurde.
- Auf Bereitstellungsgruppenebene legen Sie fest, welche Lizenz die Bereitstellungsgruppe verwenden soll. So profitieren Sie von der Flexibilität und den Vorteilen der Multityplizenzierung.

Weitere Informationen finden Sie unter Multityplizenzierung.

Unterstützung für die Anzeige von Azure Marketplace-Planinformationen. In der Benutzeroberfläche für die vollständige Konfiguration können Sie beim Erstellen von Maschinenkatalogen jetzt Preisplandaten für Masterimages anzeigen, die von Azure Marketplace-Images stammen.

Oktober 2021

Neue und erweiterte Features

Funktion zum Aktualisieren persistenter MCS-Kataloge. Wir haben die Option **Maschinen aktualisieren** für persistente MCS-Kataloge in der Verwaltungsoberfläche "Vollständige Konfiguration" eingeführt. Mit dieser Option können Sie das Image oder die Vorlage verwalten, die der Katalog verwendet. Beachten Sie beim Aktualisieren eines persistenten Katalogs, dass das neue Image oder die neue Vorlage nur zum Erstellen später hinzugefügter Maschinen verwendet wird. Das Update wird nicht auf vorhandene Maschinen im Katalog angewendet. Weitere Informationen finden Sie unter Aktualisieren von Maschinenkatalogen.

Option zur Bereitstellung von VMs auf einem dedizierten Azure-Host. Auf der Seite **Maschinenkatalogerstellung > Masterimage** der Verwaltungsoberfläche "Vollständige Konfiguration" wurde die Option **Hostgruppe verwenden** hinzugefügt. Mit dieser Option können Sie festlegen, welche Hostgruppe Sie beim Provisioning von VMs in Azure-Umgebungen verwenden möchten. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Leistungsverbesserung durch Beibehalten einer bereitgestellten VM bei Energiezyklen. Auf der Seite **Maschinenkatalogerstellung > Datenträgereinstellungen** der Verwaltungsoberfläche "Voll-

ständige Konfiguration"wurde die Einstellung **VMs während Energiezyklen beibehalten** hinzugefügt. Mit dieser Einstellung können Sie eine bereitgestellte VM bei Energiezyklen (Neustarts) in Azure-Umgebungen beibehalten. Weitere Informationen finden Sie unter MCS-Speicheroptimierung. Alternativ können Sie das Feature mit PowerShell konfigurieren. Weitere Informationen finden Sie unter Beibehalten einer bereitgestellten virtuellen Maschine bei Energiezyklen.

Binden eines Maschinenkatalogs an einen Workspace Environment Management-Konfigurationssatz. Wenn Sie einen Maschinenkatalog erstellen, können Sie ihn jetzt an einen Workspace Environment Management-Konfigurationssatz binden. Auf diese Weise bieten Sie Ihren Benutzern mit dem Workspace Environment Management Service die bestmögliche Workspace-Erfahrung. Sie können den Katalog auch nach dem Erstellen des Katalogs binden. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

September 2021

Neue und erweiterte Features

Hinzufügen von Beschreibungen für Image-Updates. Sie können jetzt Informationen zu Änderungen im Zusammenhang mit Image-Updates für Maschinenkataloge hinzufügen. Das Feature ist nützlich für Administratoren, die Informationen (z. B. *Office 365 installiert*) hinzufügen möchten, wenn sie ein für einen Katalog verwendetes Image aktualisieren. Mit PowerShell-Befehlen können Sie diese Nachrichten erstellen und anzeigen. Weitere Informationen finden Sie unter Hinzufügen einer Beschreibung zu einem Image.

Integration von Azure VMware Solution (AVS). Citrix Virtual Apps and Desktops Service unterstützt AVS (Azure VMware Solution). AVS bietet Cloudinfrastruktur mit vSphere-Clustern, die von Azure erstellt wurden. Nutzen Sie Citrix Virtual Apps and Desktops Service, um AVS für das Provisioning der VDA-Workload auf die gleiche Weise zu verwenden, in der Sie vSphere in On-Premises-Umgebungen verwenden würden. Weitere Informationen finden Sie unter Integration von Azure VMware Solution.

Dieselbe Ressourcengruppe für mehrere Kataloge. Sie können jetzt dieselbe Ressourcengruppe zum Aktualisieren und Erstellen von Katalogen im Citrix Virtual Apps and Desktops Service verwenden. Dieser Prozess:

- gilt für jede Ressourcengruppe, die einen oder mehrere Maschinenkataloge enthält.
- unterstützt Ressourcengruppen, die nicht vom Maschinenerstellungsdienst erstellt wurden.
- erstellt die VM und die zugehörigen Ressourcen.
- löscht Ressourcen in der Ressourcengruppe, wenn die VM oder der Katalog entfernt wird.

Weitere Informationen finden Sie unter Azure-Ressourcengruppen.

Abrufen von Informationen für Azure-VMs, Snapshots, Betriebssystemdatenträger und Katalogimagedefinition. Sie können Informationen für Azure-VMs, Betriebssystemdatenträger, Snapshots und Katalogimagedefinition anzeigen. Diese Informationen werden für Ressourcen im Masterimage angezeigt, wenn ein Maschinenkatalog zugewiesen wird. Verwenden Sie diese Funktion, um entweder ein Linux- oder ein Windows-Image anzuzeigen und auszuwählen. Weitere Informationen finden Sie unter Abrufen von Informationen für Azure-VMs, Snapshots, Betriebssystemdatenträger und Katalogimagedefinition.

Neues Update für automatische Konfiguration. Die automatische Konfiguration wurde auf eine neue Version aktualisiert. Zu den Features gehören:

- Unterstützung für Maschinenerstellungsdienste (MCS): Die automatische Konfiguration unterstützt jetzt MCS-Kataloge. Weitere Informationen finden Sie unter Grundlegendes zur Migration von mit Maschinenerstellungsdiensten bereitgestellten Katalogen.

Weitere Neuerungen der automatischen Konfiguration sind:

- Verbesserte Zonenunterstützung durch Ausfüllen der Datei ZoneMapping.yml mit den Namen von On-Premises-Zonen während des Exports und Cloud-Ressourcenstandorten beim Sichern.
- StoreFront wurde zu einer auf der obersten Ebene verwaltbaren Komponente gemacht. Zuvor wurde StoreFront als Teil von Bereitstellungsgruppen verwaltet. Diese Trennung erleichtert das Zusammenführen von Sites.
- `AddMachinesOnly` wurde in `MergeMachines` geändert, um dem Muster für aktuelle und neue Zusammenführungsoptionen zu entsprechen.
- Verwendung der Datei SecurityClient.csv zum Importieren von "ClientId"und "Secret"hinzugefügt, wenn CustomerInfo.yml bei Verwendung der Support-Cmdlets erstellt und aktualisiert wird.
- Migration der Benutzerzonenpräferenzen wurde hinzugefügt.
- Unterstützung für die japanische Steuerungsebene wurde korrigiert.
- Weitere Fixes und Verbesserungen.

Herunterladen der automatischen Konfiguration von Citrix Downloads. Weitere Informationen zur automatischen Konfiguration finden Sie unter Migration der Konfiguration zu Citrix Cloud.

Weitere Planungsoptionen, die mit Neustartzeitplänen verfügbar sind. Die Benutzeroberfläche "Vollständige Konfiguration"bietet jetzt zusätzliche Optionen, um den Zeitpunkt geplanter Neustarts zu steuern. Neben täglich wiederkehrenden Neustarts können Sie jetzt wöchentliche und monatliche Wiederholungen festlegen. Weitere Informationen finden Sie unter Erstellen eines Neustartzeitplans.

Beibehalten benutzerdefinierter Spalten, die die Leistung beeinträchtigen. Bisher wurden im Knoten **Suchen** der Oberfläche "Vollständige Konfiguration"benutzerdefinierte Spalten, die die Leistung beeinträchtigen, ausgeblendet, nachdem das Browserfenster aktualisiert wurde oder der Benutzer sich von der Konsole ab- und wieder angemeldet hatte. Sie können jetzt auswählen, ob diese

Spalten beibehalten werden sollen. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Automatisierten Konfigurationstools für Backup und Wiederherstellen verwenden. Der Oberfläche "Vollständigen Konfiguration"wurde der Knoten **Backup und Wiederherstellen** hinzugefügt. Der Knoten aggregiert alle mit dem automatisierten Konfigurationstool verbundenen Ressourcen, einschließlich Informationen für Folgendes:

- Planen automatischer Backups der Citrix Virtual Apps and Desktops-Konfiguration mit einem einzigen Befehl
- Wiederherstellen eines Backups bei Bedarf
- Granulares Backup und Wiederherstellen
- Andere unterstützte Anwendungsfälle

Weitere Informationen zur automatisierten Konfiguration finden Sie unter Automatische Konfiguration.

Unterstützung für nicht in Domänen eingebundene Kataloge. Der Seite **Maschinenkatalogerstellung > Maschinenidentitäten** der Oberfläche "Vollständige Konfiguration"wurde der Identitätstyp **Gehört keiner Domäne an** hinzugefügt. Über diesen Identitätstyp können Sie mit MCS Maschinen erstellen, die keiner Domäne angehören. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Unterstützung für die Verwendung eines Maschinenprofils. Der Seite **Maschinenkatalogerstellung > Masterimage** der Oberfläche "Vollständige Konfiguration"wurde die Option **Ein Maschinenprofil verwenden** hinzugefügt. Über die Option können Sie angeben, von welchem Maschinenprofil die VMs bei der Erstellung von VMs in Azure-Umgebungen die Konfiguration übernehmen sollen. Die virtuellen Maschinen im Katalog können dann folgende Konfigurationen vom ausgewählten Maschinenprofil übernehmen: Konfigurationsbeispiele:

- Beschleunigtes Netzwerk
- Startdiagnose
- Caching des Hostdatenträgers (bei OS- und MCSIO-Datenträgern)
- Maschinengröße (sofern nicht anders angegeben)
- Für VM platzierte Tags

Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Unterstützung von Windows Server 2022: Erfordert mindestens VDA 2106.

August 2021

Neue und erweiterte Features

Anzahl sortierbarer Elemente von 500 auf 5000 erhöht. Im Knoten **Suchen** der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie jetzt bis zu 5000 Elemente nach Spaltenüberschrift sortieren. Übersteigt die Zahl der Elemente 5000, filtern Sie sie, um die Anzahl auf maximal 5000 zu reduzieren und eine Sortierung zu ermöglichen. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Unterstützung zusätzlicher Azure-Speichertypen. Sie können jetzt verschiedene Speichertypen für virtuelle Maschinen in Azure-Umgebungen mit MCS wählen. Weitere Informationen finden Sie unter Speichertypen.

Unterstützung für die Auswahl des Speichertyps für den Zurückschreibcache-Datenträger. In der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie jetzt beim Erstellen eines MCS-Katalogs den Speichertyp für den Zurückschreibcache-Datenträger auswählen. Verfügbare Speichertypen: Premium SSD, Standard SSD und Standard HDD. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Abschalten angehaltener Maschinen. In der Schnittstelle **Verwalten > Vollständige Konfiguration** gibt es die neue Option **Wenn keine erneute Verbindung in (Minuten)** auf der Seite **Lastbasierte Einstellungen** von "Autoscale verwalten"für Einzelsitzungs-OS-Bereitstellungsgruppen. Die Option wird verfügbar, wenn Sie **Anhalten** ausgewählt haben, und ermöglicht Ihnen anzugeben, wann die angehaltenen Maschinen heruntergefahren werden sollen. Angehaltene Maschinen stehen zur Wiederverbindung durch getrennte Benutzer zur Verfügung, jedoch nicht für neue Benutzer. Durch das Herunterfahren der Maschinen werden diese wieder für alle Workloads verfügbar. Weitere Informationen finden Sie unter Autoscale.

Unterstützung der Verwendung von CSV-Dateien, um große Mengen von Maschinen zu einem Katalog hinzuzufügen. Die Oberfläche **Verwalten > Vollständige Konfiguration** ermöglicht jetzt mit CSV-Dateien ein Massenhinzufügen von Maschinen in Ihrem Datencenter zu einem Katalog, in dem diese Maschinen energieverwaltet werden. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

Juli 2021

Neue und erweiterte Features

Konfigurationsprotokollierung. Die Benutzeroberfläche der **Protokollierung** hat sich unter **Verwalten > Vollständige Konfiguration** geändert. Sie umfasst die folgenden drei Registerkarten:

- **Ereignisse** (zuvor "Konfigurationsprotokollierung"). Auf dieser Registerkarte können Sie Konfigurationsänderungen und Verwaltungsaktivitäten verfolgen.
- **Aufgaben**. Auf dieser Registerkarte können Sie Aufgaben im Zusammenhang mit Maschinenkatalogen anzeigen.
- **APIs**. Auf dieser Registerkarte werden die während eines bestimmten Zeitraums aufgetretenen REST-API-Anforderungen angezeigt.

Weitere Informationen finden Sie unter Konfigurationsprotokollierung.

Autoscale bietet jetzt Optionen für dynamische Sitzungstimeouts. Sie können Timeouts für getrennte Sitzungen und Leerlaufsitzungen für Neben- und Spitzenzeiten konfigurieren, um ein schnelleres Maschinendraining und Kosteneinsparungen zu erzielen. Weitere Informationen finden Sie unter Dynamische Sitzungstimeouts.

Unterstützung für vom Kunden verwaltete Verschlüsselungsschlüssel (Customer Managed Encryption Keys, CMEK) von Google Cloud Platform (GCP). Sie können jetzt CMEK von Google für MCS-Kataloge verwenden. CMEK bietet mehr Kontrolle über Schlüssel, die zur Verschlüsselung von Daten in einem Google Cloud-Projekt verwendet werden. Weitere Informationen finden Sie unter Vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK). Informationen zum Konfigurieren dieses Features finden Sie unter Verwenden vom Kunden verwalteter Verschlüsselungsschlüssel (CMEK). Das Feature steht auf der Seite **Maschinenkatalogerstellung > Datenträgereinstellungen** der Schnittstelle **Verwalten > Vollständige Konfiguration** zur Verfügung.

> **Hinweis:**
>
> Dieses Feature ist als Preview verfügbar.

Änderungen an der Registerkarte "Verwalten". Wir haben die Optionen im Menü der Registerkarte **Verwalten** aktualisiert:

- **Vollständige Konfiguration**: Diese Option führte Sie zuvor zur Legacy-Konsole. Sie gelangen nun zur neuen, webbasierten Konsole (Web Studio). Die webbasierte Konsole hat volle Parität mit der Legacy-Konsole und enthält mehrere Verbesserungen. Wir empfehlen Ihnen, sie ab jetzt zu verwenden.
- **Legacy-Konfiguration**: Mit dieser Option gelangen Sie zur Legacy-Konsole, die im September 2021 planmäßig entfernt wird. Danach ist die **Vollständige Konfiguration** die einzige Oberfläche, die Zugriff auf sämtliche Konfigurations- und Verwaltungsaktionen bietet.

Web Studio unterstützt jetzt die Auswahl einer Energieverwaltungsverbindung für einen Katalog mit Remote-PC-Zugriff. Zuvor konnten Sie mit Studio eine Wake-On-LAN-Hostverbindung zu Ihrem Ressourcenstandort erstellen (mit Auswahl von **Remote-PC Wake-On-LAN** als Verbindungstyp). Sie konnten die Verbindung jedoch nur mit PowerShell einem Katalog mit Remote-PC-Zugriff zuzuordnen. Dies ist jetzt auch mit Studio möglich. Weitere Informationen finden Sie unter Konfigurieren von Wake-On-LAN in der Oberfläche "Vollständige Konfiguration".

Juni 2021

Neue und erweiterte Features

Zugriff auf Azure Shared Image Gallery-Images. Wenn Sie einen Maschinenkatalog erstellen, können Sie jetzt im Bildschirm "Masterimage"auf Images aus der Azure Shared Image Gallery zugreifen. Details siehe Zugriff auf Images aus Azure Shared Image Gallery.

Unterstützung abgeschirmter virtueller Maschinen auf Google Cloud Platform (GCP). Sie können abgeschirmte virtuelle Maschinen auf GCP bereitstellen. Eine abgeschirmte virtuelle Maschine wird durch Sicherheitskontrollen gehärtet, die eine überprüfbare Integrität der Compute Engine-Instanzen über erweiterte Plattformsicherheitsfunktionen wie Sicherer Start, ein virtuelles Trusted Platform Module, UEFI-Firmware und Integritätsüberwachung bieten. Weitere Informationen finden Sie unter Shield VMs.

Erzwingen von HTTPS oder HTTP. Verwenden Sie Registrierungseinstellungen zum Erzwingen von HTTPS- oder HTTP-Datenverkehr über den XML-Dienst.

Verwenden Sie immer Standard-SSDs für Identitätsdatenträger, um die Kosten in Azure-Umgebungen zu senken. Maschinenkataloge verwenden den Speichertyp Standard-SSD für Identitätsdatenträger. Azure-Standard-SSDs sind eine kostengünstige Speicheroption, die für Workloads optimiert ist, die eine gleichmäßige Leistung bei niedrigeren IOPS-Raten erfordern. Weitere Informationen zu Speichertypen finden Sie unter Azure Resource Manager-Masterimage.

> **Hinweis:**
>
> Weitere Informationen zur Preislegung für verwaltete Azure-Datenträger finden Sie unter Verwaltete Datenträger –Preise.

Neues Feature in Web Studio. Die folgenden Features sind jetzt in der webbasierten Konsole verfügbar:

- **Studio unterstützt jetzt die Authentifizierung bei Azure zum Erstellen eines Dienstprinzipals.** Sie können jetzt eine Hostverbindung zu Azure herstellen, indem Sie sich bei Azure authentifizieren, um einen Dienstprinzipal zu erstellen. Dadurch wird die manuelle Erstellung eines Dienstprinzipals in Ihrem Azure-Abonnement, bevor eine Verbindung in Studio hergestellt wird, überflüssig. Weitere Informationen finden in dem Artikel zu Microsoft Azure Resource Manager-Virtualisierungsumgebungen.
- **Studio unterstützt jetzt das Klonen von Maschinenkatalogen.** Mit diesem Feature können Sie einen Maschinenkatalog klonen und den Klon als Vorlage verwenden, ohne ähnliche Kataloge von Grund auf neu erstellen zu müssen. Beim Klonen eines Katalogs können Sie die Einstellungen für das Betriebssystem und die Maschinenverwaltung nicht ändern. Der Klon erbt diese Einstellungen vom Original. Weitere Informationen finden Sie unter Klonen eines Katalogs.

- **Ein neuer Knoten "Einstellungen"ist jetzt im Studio-Navigationsbereich verfügbar.** Mit dem Knoten **Einstellungen** können Sie Einstellungen für die gesamte Site (d. h. Ihre Bereitstellung von Citrix Virtual Apps and Desktops Service) konfigurieren. Die folgenden Einstellungen sind verfügbar:

  - **Lastausgleich bei Multisitzungs-Katalogen.** Wählen Sie die Ihren Anforderungen entsprechende Lastausgleichsoption aus. Diese Einstellung gilt für alle Kataloge. Zuvor klickten Sie zur Verwendung des Features auf das Zahnradsymbol rechts oben in der Konsole. Weitere Informationen finden Sie unter Lastausgleich bei Maschinen.

- **Verbesserte Suche in Studio.** In diesem Release wurde die Suche in Studio verbessert. Wenn Sie Filter für eine erweiterte Suche verwenden, wird das Fenster Filter hinzufügen im Vordergrund angezeigt, wobei die Hintergrundansicht unverändert bleibt. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

- **Anhalten und Fortsetzen von Google Cloud-VMs in MCS**. Sie können jetzt Google Cloud-VMs wie jede andere VM in MCS anhalten und fortsetzen. Weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen. Zum Aktivieren dieser Funktion legen Sie die Berechtigungen `compute.instances.suspend` und `compute.instances.resume` im Google Cloud-Dienstkonto fest. Die Compute Admin-Rolle hat diese Berechtigungen.

  In Citrix Virtual Apps and Desktops können Sie VMs auch mit dem PowerShell-Befehl `New-BrokerHostingPowerAction` anhalten und fortsetzen. Weitere Informationen finden Sie unter New-Brokerhostingpoweraction.

  Google Cloud erzwingt Einschränkungen hinsichtlich der Art und Konfiguration von Instanzen, die angehalten werden können. Weitere Informationen finden Sie auf der Google Cloud-Website unter Instanz anhalten und fortsetzen.

Mai 2021

Neue und erweiterte Features

Wiederverbinden von Sitzungen nach der Trennung von einer Maschine im Wartungsmodus. Bisher konnten Benutzer mit gepooltem (zufälligem) Einzelsitzungsdesktop (VDI), die von einer Maschine im Wartungsmodus getrennt wurden, sich nicht erneut mit einer Maschine im Pool verbinden. Für Multisitzungs- und statische Einzelsitzungsmaschinen war hingegen die Wiederverbindung von Sitzungen unter diesen Umständen immer möglich.

Jetzt können Sie mit PowerShell auf Bereitstellungsgruppenebene steuern, ob eine Sitzung nach der Trennung von einer Maschine im Wartungsmodus die Verbindung wiederherstellen kann. Dies gilt für alle VDAs in der Gruppe (Einzelsitzung und Multisitzung).

Weitere Informationen finden Sie unter Wiederverbinden von Sitzungen nach der Trennung von einer Maschine im Wartungsmodus.

Unterstützung für Anwendungstests und Desktoptests in allen Citrix Virtual Apps and Desktops Service-Editionen. Zusätzlich zur bestehenden Unterstützung in der **Premium** Edition sind Anwendungs- und Desktoptests jetzt auch in den Editionen **Citrix Virtual Apps Advanced Service** und **Citrix Virtual Apps and Desktops Advanced Service** verfügbar.

Neues Feature in Web Studio. Das folgende Feature ist jetzt in der webbasierten Konsole verfügbar:

- **Studio unterstützt jetzt die Auswahl von Azure-Verfügbarkeitszonen**. Bisher war das Provisioning von Maschinen in spezifischen Azure-Verfügbarkeitszone nur per PowerShell möglich. Wenn Sie Studio zum Erstellen eines Maschinenkatalogs verwenden, können Sie jetzt eine oder mehrere Verfügbarkeitszone für das Provisioning von Maschinen auswählen. Wenn keine Zonen angegeben werden, lässt Maschinenerstellungsdienste (MCS) Azure die Maschinen innerhalb der Region platzieren. Werden mehrere Zonen angegeben, verteilt MCS die Maschinen nach dem Zufallsprinzip in den Zonen. Weitere Informationen finden Sie unter Provisioning von Maschinen in spezifischen Verfügbarkeitszonen.

Kurzlebiger Azure-Datenträger. Der Citrix Virtual Apps and Desktops Service unterstützt kurzlebige Azure-Datenträger. Ein kurzlebiger Datenträger ermöglicht die Umnutzung des Cachedatenträgers zum Speichern des Betriebssystemdatenträgers für eine virtuelle Azure-Maschine. Dies ist nützlich für Azure-Umgebungen, die anstelle von Standard-HDD-Datenträgern leistungsstärkere SSD-Datenträger erfordern.

> **Hinweis:**
>
> Persistente Kataloge unterstützen keine kurzlebigen Betriebssystemdatenträger. Berücksichtigen Sie bei der Verwendung dieses Features außerdem, dass der leistungsstärkere Datenträger zusätzliche Kosten verursacht. Es ist besser, den Cachedatenträger zum Speichern des Betriebssystemdatenträgers wiederzuverwenden, statt für einen weiteren verwalteten Datenträger zu bezahlen.

Kurzlebige Betriebssystemdatenträger erfordern ein Provisioningschema mit verwalteten Datenträgern und Shared Image Gallery. Weitere Informationen finden Sie unter Kurzlebige Azure-Datenträger.

Verbesserte Leistung für per MCS verwaltete VDAs in Azure. Citrix Virtual Apps and Desktops Service verbessert die Leistung für VDAs, die mit Maschinenerstellungsdienste (MCS) in Azure verwaltet werden. Der Standardwert für *Gleichzeitige Aktionen - absolut* für die Hostingverbindung beträgt jetzt 500 und derjenige für *Höchstanzahl neue Aktionen pro Minute* beträgt 2000. Zur Nutzung dieser Verbesserung ist keine manuelle Konfiguration erforderlich. Weitere Informationen finden Sie unter Azure-Drosselung.

Neue Features in Cloud Health Check. Cloud Health Check wurde aktualisiert. Zu den Features gehören:

- **Automatisches Erkennen von VDA-Maschinen**. Die Cloud-Integritätsprüfung kann VDAs jetzt automatisch in Citrix Virtual Apps and Desktops Service-Bereitstellungen erkennen und aus diesen abrufen. Weitere Informationen finden Sie unter Abrufen von VDA-Maschinen.
- **Planen von Integritätsprüfungen**. Mit der Cloud-Integritätsprüfung können Sie jetzt Zeitpläne zur Durchführung regelmäßiger Integritätsprüfungen einrichten. Weitere Informationen finden Sie unter Zeitplaner für Cloud-Integritätsprüfung.
- **Versionsinformationen für die Cloud-Integritätsprüfung**. Sie können jetzt überprüfen, welche Version der Cloud-Integritätsprüfung Sie verwenden. Klicken Sie hierfür auf das Zahnradsymbol oben rechts im Hauptfenster der Cloud-Integritätsprüfung.
- **Automatischer Fix**. Die Cloud-Integritätsprüfung unterstützt jetzt die automatische Erkennung und Behebung bestimmter Probleme auf den Maschinen, auf denen sie ausgeführt wird. Weitere Informationen finden Sie unter Automatischer Fix.

  > **Hinweis:**
  >
  > Automatischer Fix ist als Vorschau verfügbar.

April 2021

Neue und erweiterte Features

Abrufen dynamischer Instanzen über AWS-API. Der Citrix Virtual Apps and Desktops Service ruft Instanztypen jetzt bei AWS ab. Dadurch wird die Erstellung einer benutzerdefinierten `InstanceTypes.xml`-Datei für Kunden überflüssig, die Maschinengrößen verwenden möchten, die über die in Citrix Virtual Apps and Desktops Service definierten Größen hinausgehen. Diese Informationen wurden zuvor von über die `InstanceTypes.xml`-Datei bereitgestellt. Zur Erleichterung des dynamischen Zugriffs auf die verfügbaren AWS-Instanztypen müssen die Berechtigungen des Dienstprinzipals um die Berechtigung `ec2:DescribeInstanceTypes` erweitert werden. Zur Gewährleistung von Abwärtskompatibilität für Kunden, die die Berechtigungen des Dienstprinzipals nicht aktualisieren möchten, werden die in der Datei `InstanceTypes.xml` aufgeführten AWS-Instanztypen verwendet. Dabei wird eine Warnmeldung im MCS-CDF-Protokoll generiert.

> **Hinweis:**
>
> Citrix Studio zeigt die Warnmeldung des CDF-Protokolls nicht an.

Weitere Informationen zu Berechtigungen finden Sie unter Definieren von IAM-Berechtigungen und Informationen zu AWS-Berechtigungen.

Neues Feature in Web Studio. Das folgende Feature ist jetzt in der webbasierten Konsole verfügbar:

- **In Studio werden jetzt Datum und Uhrzeit der lokalen Zeitzone angezeigt.** Bisher wurden Datum und Uhrzeit in Studio auf Basis der Systemuhr und Zeitzone angezeigt. Studio unterstützt jetzt die Anzeige des Datums und der Uhrzeit der lokalen Zeitzone beim Zeigen mit der Maus auf ein Ereigniselement. Die Zeit wird in Form der koordinierten Weltzeit angegeben.

MCS-E/A-Unterstützung für Azure-VMs ohne temporären Speicher. MCS-E/A unterstützt jetzt die Erstellung von Maschinenkatalogen für VMs, die keine temporären Datenträger oder angefügte Speicher haben. Dies bedeutet:

- Der Snapshot (verwalteter Datenträger) wird von der Quell-VM *ohne* temporären Speicher abgerufen. Die VMs im Maschinenkatalog haben keinen temporären Speicher.
- Der Snapshot (verwalteter Datenträger) wird von der Quell-VM *mit* temporärem Speicher abgerufen. Die VMs im Maschinenkatalog haben einen temporären Speicher.

Weitere Informationen finden Sie unter MCS-Speicheroptimierung.

Neues Feature in Web Studio. Das folgende Feature ist jetzt in der webbasierten Konsole verfügbar:

- **Erzwingen von Abmeldungen.** Mit Autoscale können Sie jetzt Sitzungen auf Maschinen bei Erreichen der festgelegten Frist zwangsweise abmelden, sodass die Maschinen heruntergefahren werden können. Dadurch kann Autoscale Maschinen schneller abschalten und so die Kosten reduzieren. Sie können Benachrichtigungen an Benutzer senden, bevor diese abgemeldet werden. Weitere Informationen finden Sie unter Autoscale.

Neues Update für automatische Konfiguration. Die automatische Konfiguration wurde auf eine neue Version aktualisiert. Zu den Features gehören:

- **Zusammenführen von Sites:** Sie können mehrere Sites zu einer zusammenführen und durch Verwendung von Präfixen und Suffixen Namenskonflikte vermeiden. Weitere Informationen finden Sie unter Zusammenführen mehrerer Sites.
- **Siteaktivierung:** Sie können auswählen, ob die On-Premises- oder die Cloud-Bereitstellung Ressourcen wie Neustartpläne und Energieschemata steuern soll. Weitere Informationen zum Aktivieren von Sites finden Sie unter Aktivieren von Sites.

Weitere Neuerungen der automatischen Konfiguration sind:

- Migration von Administratorrollen und -bereichen.
- Parameter `Quiet` für ausgewählte Cmdlets zur Unterdrückung der Konsolenprotokollierung.
- Parameter `SecurityFileFolder` zum Speichern der Datei CvadAcSecurity.yml in einer sicheren Netzwerkdateifreigabe, die Authentifizierung erfordert.

- Filtern nach Maschinennamen in Maschinenkatalogen und Bereitstellungsgruppen.
- Verbesserte Parameter zur Komponentenauswahl durch Switch-Parameter-Methode, die keine Angabe von `$true` nach Komponentennamen erfordert.
- Neues Cmdlet (`New-CvadAcZipInfoForSupport`) zum Komprimieren der Protokolldateien vor der Übermittlung an den Citrix Support.

Herunterladen der automatischen Konfiguration von Citrix Downloads. Weitere Informationen zur automatisierten Konfiguration finden Sie unter Migrieren in die Cloud.

Beibehalten von GCP-Instanzen über Energiezyklen hinweg. Nicht persistente GCP-Instanzen (Google Cloud Platform) werden beim Ausschalten nicht mehr gelöscht. Stattdessen werden diese Instanzen über Energiezyklen hinweg beibehalten. Wenn eine nicht persistente Instanz ausgeschaltet wird, wird der Betriebssystemdatenträger getrennt und gelöscht. Wird die Instanz eingeschaltet, wird der Betriebssystemdatenträger vom Basisdatenträger neu erstellt und an die Instanz angefügt.

Unterstützung für Azure Gen2-Images. Sie können jetzt per Snapshot oder verwalteten Datenträger (jeweils der zweiten Generation) einen VM-Katalog der zweiten Generation bereitstellen, um die Startzeitleistung zu verbessern. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen. Die folgenden Betriebssysteme werden für Azure-Images der zweiten Generation unterstützt:

- Windows Server 2019, 2016, 2012 und 2012 R2
- Windows 10

> **Hinweis:**
>
> Das Erstellen eines Maschinenkatalogs der zweiten Generation mit einem Snapshot oder verwalteten Datenträger der ersten Generation wird nicht unterstützt. Umgekehrt wird das Erstellen eines Maschinenkatalogs der ersten Generation mit einem Snapshot oder verwalteten Datenträger der zweiten Generation ebenfalls nicht unterstützt. Weitere Informationen finden Sie unter Unterstützung für VMs der zweiten Generation in Azure

Deaktivieren von Tabellenspeicherkonten. Maschinenerstellungsdienste (MCS) erstellt für Kataloge, die zum Provisioning von VDAs in Azure verwaltete Datenträger verwenden, keine Tabellenspeicherkonten mehr. Weitere Informationen finden Sie unter Azure-Tabellenspeicher.

Eliminierung von Sperren in Speicherkonten. Wenn Sie einen Katalog in Azure mit einem verwalteten Datenträger erstellen, wird kein Speicherkonto mehr erstellt. Für bestehende Kataloge erstellte Speicherkonten bleiben unverändert. Diese Änderung gilt nur für verwaltete Datenträger. Für nicht verwaltete Datenträger gilt die Änderung nicht. Maschinenerstellungsdienste (MCS) erstellt weiterhin Speicherkonten und Sperren.

Neue Features in Web Studio. Die folgenden Features sind jetzt in der webbasierten Konsole verfügbar:

- **Verwenden eines vom Kunden verwalteten Schlüssels zur Verschlüsselung von Daten auf Maschinen**. In Studio gibt es jetzt die Einstellung **Vom Kunden verwalteter Verschlüsselungsschlüssel** auf der Seite **Maschinenkatalogerstellung > Datenträgereinstellungen**. Mit der Einstellung können Sie wählen, ob Daten auf den im Katalog bereitzustellenden Maschinen verschlüsselt werden sollen. Weitere Informationen finden Sie unter Vom Kunden verwalteter Verschlüsselungsschlüssel.
- **Studio unterstützt jetzt die Beschränkung von Autoscale auf Maschinen mit Tag**. Bisher mussten Sie PowerShell zum Beschränken von Autoscale auf bestimmte Maschinen in einer Bereitstellungsgruppe verwenden. Jetzt können Sie auch Studio verwenden. Weitere Informationen finden Sie unter Einschränken von Autoscale auf bestimmte Maschinen in einer Bereitstellungsgruppe.

März 2021

Neue und erweiterte Features

Dedizierte Azure-Hosts. Dedizierte Azure-Hosts ermöglichen das Provisioning virtueller Maschinen auf Hardware, die nur für einen Kunden verwendet wird. Bei Verwendung eines dedizierten Hosts gewährleistet Azure, dass die virtuellen Maschinen als einzige auf dem Host ausgeführt werden. Die Kunden profitieren so von mehr Kontrolle und Transparenz und können eventuelle gesetzliche bzw. interne Sicherheitsanforderungen erfüllen. Bei Verwendung des Parameters `HostGroupId` ist eine vorkonfigurierte Azure-Hostgruppe in der Region der Hostingeinheit erforderlich. Außerdem ist die automatische Platzierung von Azure erforderlich. Weitere Informationen finden Sie unter Dedizierte Azure-Hosts.

> **Tipp:**
>
> Wenn Sie dedizierte Azure-Hosts verwenden, hat die Auswahl der **Azure-Verfügbarkeitszone** keine Auswirkungen. Virtuelle Maschinen werden per automatischer Azure-Platzierung platziert.

Unterstützung für serverseitige Azure-Verschlüsselung. Citrix Virtual Apps and Desktops Service unterstützt vom Kunden verwaltete Schlüssel für verwaltete Azure-Datenträger. Mit dieser Unterstützung können Sie Ihre Unternehmens- und Compliance-Anforderungen verwalten, indem Sie die verwalteten Datenträger des Maschinenkatalogs mit Ihrem eigenen Schlüssel verschlüsseln. Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

Provisioning von Maschinen in spezifischen Verfügbarkeitszonen in Azure. Sie können Maschinen jetzt in spezifischen Verfügbarkeitszonen in Azure-Umgebungen bereitstellen. Mit dieser Funktionalität ist Folgendes möglich:

- Sie können eine oder mehrere Verfügbarkeitszone in Azure angeben. Maschinen sind gleichmäßig auf alle Zonen verteilt, wenn mehr als eine angegeben wird.

- Die virtuelle Maschine und der zugehörige Datenträger werden in der angegebenen Zone (bzw. in den angegebenen Zonen) platziert.
- Sie können Verfügbarkeitszonen nach einem bestimmten Serviceangebot oder einer Region durchsuchen. Gültige Verfügbarkeitszonen werden mit PowerShell-Befehlen angezeigt. Anzeigen der Elemente des Serviceangebots mit `Get-Item`.

Weitere Informationen finden Sie unter Provisioning von Maschinen in spezifischen Verfügbarkeitszonen in Azure.

Neue Features in Web Studio. Die folgenden Features sind jetzt in der webbasierten Konsole verfügbar:

- **Studio unterstützt jetzt das Verknüpfen von Apps mit benutzerdefinierten Symbolen**. Bisher mussten Sie PowerShell verwenden, um benutzerdefinierte Symbole für veröffentlichte Anwendungen hinzuzufügen. Jetzt können Sie hierfür auch Studio verwenden. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.
- **Studio unterstützt jetzt das Anwenden von Tags auf Maschinenkataloge**. Bisher konnten Sie mit Studio Tags für einen Katalog erstellen oder löschen. Um Tags auf den Katalog anzuwenden, mussten Sie jedoch PowerShell verwenden. Jetzt können Sie wie bei Bereitstellungsgruppen Studio verwenden, um Tags auf einen Katalog anzuwenden oder um sie aus einem Katalog zu entfernen. Weitere Informationen finden Sie unter Anwenden von Tags auf Maschinenkataloge.
- **Studio unterstützt jetzt den Wechsel zwischen dem horizontalen und dem vertikalen Lastenausgleich**. Zuvor war dieser Wechsel nur mit PowerShell möglich. Studio bietet jetzt mehr Flexibilität bei der Steuerung des Lastausgleichs für Multisitzungs-OS-Maschinen. Weitere Informationen finden Sie unter Lastausgleich bei Maschinen.
- **Studio unterstützt jetzt das Einbinden von Maschinen im Wartungsmodus in Neustartzeitpläne**. Bisher konnten Sie geplante Neustarts für Maschinen im Wartungsmodus nur mit PowerShell konfigurieren. Jetzt können Sie auch mit Studio steuern, ob diese Maschinen in einen Neustartzeitplan aufzunehmen sind. Weitere Informationen finden Sie unter Erstellen eines Neustartzeitplans.
- **Studio unterstützt jetzt das Konfigurieren von Wake-On-LAN für Remote-PC-Zugriff**. Bisher mussten Sie PowerShell verwenden, um Wake-On-LAN für Remote-PC-Zugriff zu konfigurieren. Jetzt können Sie das Feature auch mit Studio konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Wake-On-LAN.
- **Studio unterstützt jetzt das Anwenden von AWS-Instanzeigenschaften und Tagging von Betriebsressourcen**. Wenn Sie einen Katalog zum Bereitstellen von Maschinen in AWS über die Maschinenerstellungsdienste erstellen, können Sie festlegen, ob Sie auf diese Maschinen die IAM-Rolle und Tag-Eigenschaften anwenden. Außerdem können Sie festlegen, ob

Sie Maschinen-Tags auf Betriebsressourcen anwenden. Die folgenden zwei Optionen sind verfügbar:

- **Maschinenvorlageneigenschaften auf virtuelle Maschinen anwenden**
- **Maschinen-Tags auf Betriebsressourcen anwenden**

Weitere Informationen finden Sie unter Anwenden von AWS-Instanzeigenschaften und Tagging von Betriebsressourcen

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops Service unterstützt die Azure Shared Image Gallery als veröffentlichtes Imagerepository für Maschinen, die mit MCS in Azure bereitgestellt werden. Administratoren haben die Möglichkeit, ein Image im Katalog zu speichern, um das Erstellen und die Hydration von Betriebssystemdatenträgern zu beschleunigen. Dieser Prozess verkürzt die System- und Anwendungsstartzeiten für nicht-persistente VMs. Weitere Informationen zu diesem Feature finden Sie unter Azure Shared Image Gallery.

> **Hinweis:**
>
> Die Shared Image Gallery-Funktion ist mit verwalteten Datenträgern kompatibel. Sie ist nicht für Legacy-Maschinenkataloge verfügbar.

Storage-Buckets, die in derselben Google Cloud Platform-Region wie der Maschinenkatalog erstellt wurden. In früheren Versionen erstellte MCS beim Provisioning temporäre Storage-Buckets während des Datenträger-Uploads. Diese Buckets umfassten mehrere Regionen, von Google definiert als großes geografisches Gebiet mit zwei oder mehr geografischen Orten. Diese temporären Buckets befanden sich stets in den USA, unabhängig davon, wo der Katalog bereitgestellt wurde. MCS erstellt jetzt Storage-Buckets in der gleichen Region, in der Sie Ihre Kataloge bereitstellen. Storage-Buckets werden nicht mehr temporär angelegt, sondern verbleiben nach Abschluss des Provisionings in Ihrem Google Cloud Platform-Projekt. Zukünftige Provisioningvorgänge nutzen den vorhandenen Storage-Bucket (sofern es eines in der Region gibt). Wenn in der angegebenen Region kein Storage-Bucket existiert, wird eines erstellt.

Februar 2021

Neue und erweiterte Features

Unterstützung für Azure Gen2-Images. Sie können jetzt verwaltete Datenträger unter Einsatz von VMs der zweiten Generation in Azure-Umgebungen bereitstellen, um die Startzeitleistung zu verbessern. Folgende Betriebssysteme werden unterstützt:

- Windows Server 2019, 2016, 2012 und 2012 R2
- Windows 10

> **Hinweis:**
>
> Die Unterstützung gilt nur für eine Teilmenge von VMs. Manche VMs können sowohl zur ersten als auch zur zweiten Generation gehören, während andere nur Generation 1 angehören. Weitere Informationen finden Sie unter Unterstützung für VMs der zweiten Generation in Azure

Zeitpläne für den Maschinenneustart. Citrix Studio enthält jetzt die Option **Starten Sie alle Maschinen nach dem Draining der Sitzungen neu** im Menü **Neustartdauer**. Über die Option können Sie auswählen, ob alle Maschinen nach dem Draining aller Sitzungen neu gestartet werden sollen. Bei Erreichen der Neustartzeit werden Maschinen in den Drainingzustand versetzt und neu gestartet, sobald alle Sitzungen abgemeldet sind. Weitere Informationen finden Sie unter Erstellen eines Neustartzeitplans.

Neue Features in Web Studio. Die folgenden Features sind jetzt in der webbasierten Konsole verfügbar:

- **Studio unterstützt jetzt die Verwendung von CSV-Dateien, um große Mengen von Maschinen zu einem Katalog hinzuzufügen**. Mit diesem Feature können Sie eine CSV-Datei für Folgendes verwenden:
  - Massenhinzufügen von Maschinen zu einem Multisitzungs-OS- oder Einzelsitzungs-OS-Katalog, wobei keine Energieverwaltung der Maschinen über Studio erfolgt.
  - Massenhinzufügen von Maschinen zu einem Remote-PC-Zugriff-Katalog. Bisher mussten Sie Organisationseinheiten auswählen, um große Mengen von Maschinen zu einem Remote-PC-Zugriff-Katalog hinzuzufügen. In Szenarios mit Einschränkungen der Organisationseinheitsstruktur ist dies jedoch nicht einfach. Das Feature bietet Ihnen mehr Flexibilität beim Massenhinzufügen von Maschinen. Sie können entweder nur Maschinen hinzufügen (zur Verwendung mit automatischen Benutzerzuweisungen) oder Maschinen und Benutzerzuweisungen gemeinsam hinzufügen.

  Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.
- **Erweiterter Support für Citrix Managed Azure.** Citrix Managed Azure ist jetzt in den folgenden Editionen von Citrix Virtual Apps and Desktops Service verfügbar: Standard für Azure, Advanced, Premium und Workspace Premium Plus.
- **Unterstützung für das Platzieren von Masterimages in der Azure Shared Image Gallery**. Studio bietet Ihnen jetzt die Möglichkeit, Masterimages in der Azure Shared Image Gallery (SIG) zu platzieren. SIG ist ein Repository zum Verwalten und Freigeben von Images. Damit können Sie Images in Ihrer gesamten Organisation verfügbar machen. Wir empfehlen Ihnen, beim Erstellen großer nicht-persistenter Maschinenkataloge ein Masterimage in SIG zu speichern, da sich VDA-Betriebssystemdatenträger dadurch schneller zurücksetzen

lassen. Weitere Informationen finden in dem Artikel zu Microsoft Azure Resource Manager-Virtualisierungsumgebungen.

- **Beibehalten des Systemdatenträgers für MCS-Maschinenkataloge in Azure.** Mit Studio können Sie jetzt steuern, ob bei Energiezyklen Systemdatenträger für VDAs beibehalten werden sollen. Normalerweise werden Systemdatenträger beim Herunterfahren gelöscht und beim Starten neu erstellt. Dies stellt sicher, dass der Datenträgercache immer in bereinigtem Zustand ist, der Neustart von VMs dauert jedoch länger. Wenn Systemschreibvorgänge zum Cache umgeleitet und auf den Cachedatenträger zurückgeschrieben werden, bleibt der Systemdatenträger unverändert. Zur Vermeidung unnötiger Datenträger-Neuerstellungen verwenden Sie die Option **Systemdatenträger während Energiezyklen beibehalten** auf der Seite **Maschinenkatalogerstellung > Datenträgereinstellungen**. Die Aktivierung dieser Option verringert die Neustartdauer für VMs, erhöht allerdings auch die Speicherkosten. Die Option kann in Umgebungen mit Neustart-empfindlichen Workloads nützlich sein. Weitere Informationen finden Sie unter MCS-Speicheroptimierung.
- **Studio unterstützt jetzt das Erstellen von MCS-Maschinenkatalogen mit persistentem Datenträger für Zurückschreibcache**. Bisher konnten Sie nur PowerShell zum Erstellen eines Katalogs mit persistentem Zurückschreibcachedatenträger verwenden. Sie können jetzt beim Erstellen eines Katalogs über Studio steuern, ob der Zurückschreibcachedatenträger für die in Azure bereitgestellten VMs erhalten bleibt. Wenn die Option "Persistenter Datenträger für Zurückschreibcache"deaktiviert ist, wird der Datenträger bei Energiezyklen gelöscht und alle an ihn umgeleiteten Daten gehen verloren. Um die Daten zu behalten, aktivieren Sie die Option **Persistenter Datenträger für Zurückschreibcache** auf der Seite **Maschinenkatalogerstellung > Datenträgereinstellungen**. Weitere Informationen finden Sie unter MCS-Speicheroptimierung.

App-Schutz-Unterstützung für Citrix Virtual Apps and Desktops Service mit StoreFront. Weitere Informationen finden Sie unter App-Schutz.

Januar 2021

Neue Features in Web Studio. Die folgenden Features sind jetzt in der webbasierten Konsole verfügbar:

- **Studio unterstützt jetzt das Verknüpfen von Apps mit benutzerdefinierten Symbolen**. Bisher mussten Sie PowerShell verwenden, um benutzerdefinierte Symbole für veröffentlichte Anwendungen hinzuzufügen. Jetzt können Sie hierfür auch Studio verwenden. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.
- **Studio unterstützt jetzt das Anwenden von Tags auf Maschinenkataloge**. Bisher konnten Sie mit Studio Tags für einen Katalog erstellen oder löschen. Um Tags auf den Katalog anzuwen-

den, mussten Sie jedoch PowerShell verwenden. Jetzt können Sie wie bei Bereitstellungsgruppen Studio verwenden, um Tags auf einen Katalog anzuwenden oder um sie aus einem Katalog zu entfernen. Weitere Informationen finden Sie unter Anwenden von Tags auf Maschinenkataloge.

- **Studio unterstützt jetzt den Wechsel zwischen dem horizontalen und dem vertikalen Lastenausgleich**. Zuvor war dieser Wechsel nur mit PowerShell möglich. Studio bietet jetzt mehr Flexibilität bei der Steuerung des Lastausgleichs für Multisitzungs-OS-Maschinen. Weitere Informationen finden Sie unter Lastausgleich bei Maschinen.
- **Studio unterstützt jetzt das Einbinden von Maschinen im Wartungsmodus in Neustartzeitpläne**. Bisher konnten Sie geplante Neustarts für Maschinen im Wartungsmodus nur mit PowerShell konfigurieren. Jetzt können Sie auch mit Studio steuern, ob diese Maschinen in einen Neustartzeitplan aufzunehmen sind. Weitere Informationen finden Sie unter Erstellen eines Neustartzeitplans.
- **Studio unterstützt jetzt das Konfigurieren von Wake-On-LAN für Remote-PC-Zugriff**. Bisher mussten Sie PowerShell verwenden, um Wake-On-LAN für Remote-PC-Zugriff zu konfigurieren. Jetzt können Sie das Feature auch mit Studio konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Wake-On-LAN.
- **Studio unterstützt jetzt das Anwenden von AWS-Instanzeigenschaften und Tagging von Betriebsressourcen**. Wenn Sie einen Katalog zum Bereitstellen von Maschinen in AWS über die Maschinenerstellungsdienste erstellen, können Sie festlegen, ob Sie auf diese Maschinen die IAM-Rolle und Tag-Eigenschaften anwenden. Außerdem können Sie festlegen, ob Sie Maschinen-Tags auf Betriebsressourcen anwenden. Die folgenden zwei Optionen sind verfügbar:

  - **Maschinenvorlageneigenschaften auf virtuelle Maschinen anwenden**
  - **Maschinen-Tags auf Betriebsressourcen anwenden**

  Weitere Informationen finden Sie unter Anwenden von AWS-Instanzeigenschaften und Tagging von Betriebsressourcen
- **Dedizierter AWS-Host:** In Citrix Studio gibt es jetzt die Option **Dedizierten Host verwenden** auf der Seite **Maschinenkatalogerstellung > Sicherheit**. Diese Einstellung eignet sich für Bereitstellungen mit Lizenzbeschränkungen oder Sicherheitsanforderungen, die die Verwendung eines dedizierten Hosts erfordern. Ein dedizierter Host wird ausschließlich für Sie verwendet und nach Stunden in Rechnung gestellt. Bei einem solchen Host können Sie ohne zusätzliche Kosten so viele EC2-Instanzen einrichten, wie der Host zulässt. Weitere Informationen finden Sie unter AWS-Tenancy.
- **Studio unterstützt jetzt das sofortige Ausführen eines Neustartzeitplans**. In Studio können Sie einen Neustartzeitplan sofort ausführen, um die enthaltenen Maschine neu zu starten. Weitere Informationen finden Sie unter Sofortiges Ausführen eines Neustartzeitplans.

- **Autoscale.** Autoscale bietet die folgenden neuen Features und Verbesserungen:
  - **Studio unterstützt jetzt die Anzeige von Maschinen im Drainingzustand**. Zuvor war dies nur mit PowerShell möglich. Sie können jetzt Studio verwenden, um Maschinen im Drainingzustand zu identifizieren. Weitere Informationen finden Sie unter Anzeigen von Maschinen im Drainingzustand.
  - **Studio unterstützt jetzt das Definieren von Spitzenzeiten auf einer Detailebene von 30 Minuten für VDI-Bereitstellungsgruppen**. Bisher mussten Sie PowerShell verwenden, um die Spitzenzeiten für die Tage in einem Zeitplan auf einer Detailebene von 30 Minuten für VDI-Bereitstellungsgruppen zu definieren. Jetzt können Sie hierfür auch Studio verwenden. Sie können die Mindestanzahl ausgeführter Maschinen in einer VDI-Bereitstellungsgruppe für jede halbe Stunde des Tages separat festlegen.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops Service unterstützt die Azure Shared Image Gallery als veröffentlichtes Imagerepository für Maschinen, die mit MCS in Azure bereitgestellt werden. Administratoren haben die Möglichkeit, ein Image im Katalog zu speichern, um das Erstellen und die Hydration von Betriebssystemdatenträgern vom Masterimage zu beschleunigen. Dieser Prozess verkürzt die System- und Anwendungsstartzeiten für nicht-persistente VMs.

Der Katalog enthält die folgenden drei Elemente:

- Katalog. Hier werden Images gespeichert. MCS erstellt je eine Gallery für jeden Maschinenkatalog.
- Katalogimagedefinition. Diese Definition enthält Informationen zum Masterimage (Betriebssystemtyp/-zustand, Azure-Region). MCS erstellt eine Imagedefinition für jedes Masterimage, das für den Katalog erstellt wurde.
- Katalogimageversion. Jedes Image in einer Shared Image Gallery kann mehrere Versionen haben, und jede Version kann mehrere Replikate in verschiedenen Regionen haben. Jedes Replikat ist eine vollständige Kopie des Masterimages. Citrix Virtual Apps and Desktops Service erstellt immer für jedes Image eine Standard_LRS-Imageversion (Version 1.0.0) mit der entsprechenden Anzahl von Replikaten in der Region des Katalogs. Diese Konfiguration basiert auf der Maschinenanzahl im Katalog, der konfigurierten Replikatquote und der konfigurierten Anzahl maximaler Replikate.

> **Hinweis:**
>
> Die Shared Image Gallery-Funktion kann nur mit verwalteten Datenträgern verwendet werden. Sie ist nicht für Legacy-Maschinenkataloge verfügbar.

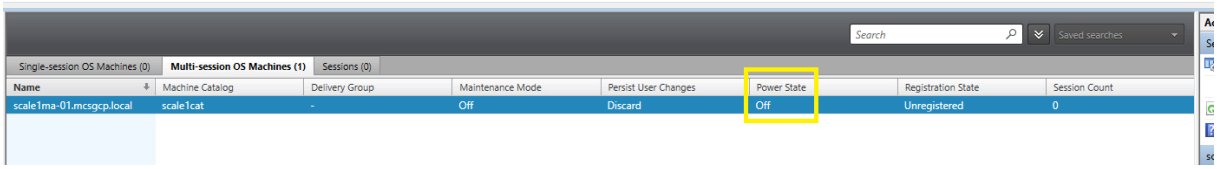
Weitere Informationen zu diesem Feature finden Sie unter Konfigurieren der Shared Image Gallery.

Storage-Buckets, die in derselben Google Cloud Platform-Region wie der Maschinenkatalog erstellt wurden. In früheren Versionen erstellte MCS beim Provisioning temporäre Storage-Buckets

während des Datenträger-Uploads. Diese Buckets umfassten mehrere Regionen, von Google definiert als großes geografisches Gebiet mit zwei oder mehr geografischen Orten. Diese temporären Buckets befanden sich stets in den USA, unabhängig davon, wo der Katalog bereitgestellt wurde. MCS erstellt jetzt Storage-Buckets in der gleichen Region, in der Sie Ihre Kataloge bereitstellen. Storage-Buckets werden nicht mehr temporär angelegt, sondern verbleiben nach Abschluss des Provisionings in Ihrem Google Cloud Platform-Projekt. Zukünftige Provisioningvorgänge nutzen den vorhandenen Storage-Bucket. Wenn in der angegebenen Region kein Storage-Bucket existiert, wird ein neuer Bucket erstellt.

PowerShell-Option, die festlegt, dass standardmäßig gepoolte VDAs während eines Ausfalls wiederverwendet werden. Die neue PowerShell-Befehlsoption `-DefaultReuseMachinesWithoutShutdo` erweitert die standardmäßige Wiederverwendung von Desktop-VDAs, die während eines Ausfalls nicht heruntergefahren wurden. Siehe Unterstützung für Anwendungen und Desktops.

Google Cloud Platform –bedarfsgesteuertes Provisioning. Citrix Virtual Apps and Desktops Service aktualisiert das Bereitstellen von Maschinenkatalogen in Google Cloud Platform (GCP). Beim Erstellen eines Maschinenkatalogs wird die entsprechende Maschineninstanz nicht in GCP erstellt und der Energiezustand wird auf **Aus** gesetzt. Maschinen werden nicht beim Erstellen des Katalogs bereitgestellt, sondern beim ersten Einschalten der Maschinen. Nachdem Sie beispielsweise einen Katalog erstellt haben, wird der VM-Energiezustand auf **Aus** gesetzt:

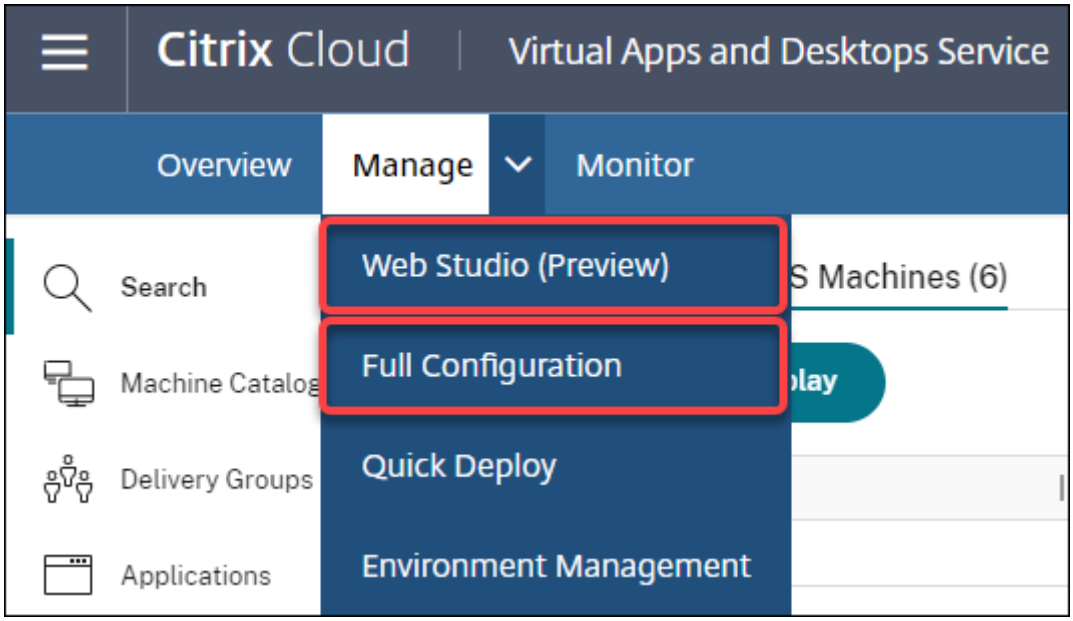


Dezember 2020

Neue und erweiterte Features

Web Studio ist als Vorschau verfügbar. Eine neue webbasierte Konsole ist jetzt verfügbar. Wir sind dabei, sämtliche Studio-Funktionen von der Legacykonsole zu der neuen webbasierten Konsole zu migrieren. Die webbasierte Konsole reagiert in der Regel schneller als die Legacykonsole. Standardmäßig erfolgt die Anmeldung automatisch bei der webbasierten Konsole. Sie können über die Registerkarte **Verwalten** mühelos zwischen der webbasierten Konsole und der Legacykonsole wechseln, um Konfigurations- oder Siteverwaltungsaufgaben zu erledigen. Klicken Sie auf den Abwärtspfeil neben **Verwalten** und wählen Sie eine Option aus:

- **Web Studio (Preview).** Führt zur neuen webbasierten Konsole.
- **Vollständige Konfiguration.** Führt zur Legacykonsole.



Die folgenden Features sind nur in der webbasierten Konsole verfügbar:

- **Unterstützung von Standard-SSD-Datenträgern für Azure**. Studio unterstützt jetzt standardmäßige SSD-Datenträger. Azure-Standard-SSDs sind eine kostengünstige Speicheroption, die für Workloads optimiert ist, die eine gleichmäßige Leistung bei niedrigeren IOPS-Raten erfordern. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Masterimages.
- **Studio unterstützt jetzt die Konfiguration einer Ausschaltverzögerung für statische VDI-Bereitstellungsgruppen**. Bisher konnten Sie die Ausschaltverzögerung für statische VDI-Bereitstellungsgruppen nur über das PowerShell-SDK konfigurieren. Mit Studio können Sie jetzt die Ausschaltverzögerung in der Autoscale-Benutzeroberfläche für statische VDI-Bereitstellungsgruppen konfigurieren. Weitere Informationen finden Sie unter Autoscale.

Oktober 2020

Neue und erweiterte Features

Verwerfen mehrerer Hypervisorwarnungen: Citrix Monitor unterstützt jetzt das automatische Verwerfen von Hypervisorwarnungen, die älter als einen Tag sind. Weitere Informationen finden Sie unter Überwachung von Hypervisor-Warnungen.

Externe IP-Adresse entfernen. Eine externe IP-Adresse auf temporären virtuellen Maschinen, die zur Vorbereitung eines bereitgestellten Images in Google Cloud Platform (GCP) verwendet werden, ist nicht mehr erforderlich. Über die externe IP-Adresse können temporäre virtuelle Maschinen auf die öffentliche Google-API zugreifen, um das Provisioning abzuschließen.

Aktivieren Sie den privaten Google-Zugriff, damit eine VM auf die öffentliche Google-API direkt aus dem Subnetz zugreifen kann. Weitere Informationen finden Sie unter Aktivieren des privaten Google-Zugriffs.

Neues Modell zur Verwaltung von Maschinenidentitäten. In Maschinenkatalogen verwendete Maschinenidentitäten wurden mit Active Directory verwaltet. Alle von MCS erstellten Maschinen werden nun Active Directory hinzugefügt. Das neue Modell von Citrix Virtual Apps and Desktops Service verändert die Verwaltung von Maschinenidentitäten. Das Modell ermöglicht die Erstellung von Maschinenkatalogen unter Verwendung von Maschinen in *Arbeitsgruppen* oder solchen, die nicht zur Domäne gehören.

> **Tipp:**
>
> Diese Funktion unterstützt den neuen Identitätsdienst (*FMA-Vertrauensstellung*), der Citrix Cloud für nicht zur Domäne gehörende Maschinen hinzugefügt wurde.

MCS kommuniziert mit dem neuen FMA-Dienst für die Identitätsverwaltung. Identitätsinformationen werden auf dem Identitätsdatenträger in Form eines GUID-/privater Schlüssel-Paars gespeichert (anstelle der in Active Directory üblichen Domänen-SID plus Maschinenkonto). VDAs, die nicht zur Domäne gehörende Maschinen verwenden, verwenden die Kombination aus GUID und privatem Schlüssel für die Brokerregistrierung. Weitere Informationen finden Sie unter Konfigurieren der Unterstützung für nicht zur Domäne gehörende Kataloge.

Direkter Upload für Azure Managed Disks. In diesem Release können Sie beim Erstellen verwalteter Datenträger in einer Azure-Umgebung einen direkten Upload verwenden. Die Funktion reduziert die mit zusätzlichen Speicherkonten verbundenen Kosten. Sie müssen für die virtuelle Festplatte nicht mehr ein Staging in ein Speicherkonto durchführen, bevor Sie sie in einen verwalteten Datenträger konvertieren. Durch den direkten Upload ist es außerdem nicht mehr erforderlich, einer virtuellen Maschine einen leeren verwalteten Datenträger anzufügen. Der direkte Upload in Azure Managed Disks vereinfacht den Workflow, da virtuelle On-Premises-Festplatten direkt zur Verwendung als verwaltete Datenträger kopiert werden können. Unterstützt werden die Ebenen HDD Standard, SSD Standard und SSD Premium.

Weitere Informationen zu dem Feature finden Sie im Microsoft Azure-Blog.

Weitere Informationen zu verwalteten Azure-Datenträgern finden Sie auf der Dokumentationsseite.

Einzelne Ressourcengruppe in Azure. Sie können jetzt eine einzelne Azure-Ressourcengruppe zum Aktualisieren und Erstellen von Katalogen in Citrix Virtual Apps and Desktops erstellen und verwenden. Diese Erweiterung gilt für Dienstprinzipale mit vollem und mit eingeschränktem Gültigkeitsbereich. Die bisherige Beschränkung auf 240 VMs pro 800 verwaltete Datenträger pro Azure-Ressourcengruppe gibt es nicht mehr. Es gibt keine Beschränkung mehr für die Anzahl der virtuellen Maschinen, verwalteten Datenträger, Snapshots und Images pro Azure-Ressourcengruppe.

Weitere Informationen finden in dem Artikel zu Microsoft Azure Resource Manager-Virtualisierungsumgebungen.

September 2020

Neue und erweiterte Features

Quick Deploy. Das neue Feature Quick Deploy ersetzt das frühere Azure Quick Deploy. Das neue Feature bietet einen schnellen Einstieg in den Citrix Virtual Apps and Desktops Service mit Microsoft Azure. Mit Quick Deploy können Sie Desktops und Apps bereitstellen und den Remote-PC-Zugriff konfigurieren.

Sitzungsadministrator (integrierte Rolle). Citrix Studio fügt den **Sitzungsadministrator** als neue integrierte Rolle hinzu. Die Rolle ermöglicht es Administratoren, Bereitstellungsgruppen anzuzeigen und die zugehörigen Sitzungen und Maschinen auf der Seite **Filter** der Registerkarte **Überwachen** zu verwalten. Mit dieser Funktion können Sie die Zugriffsberechtigungen vorhandener oder eingeladener Administratoren an ihre Rolle in der Organisation angleichen. Weitere Informationen zur integrierten Rolle finden Sie unter Integrierte Rollen und Bereiche. Informationen zum Zuweisen der integrierten Rolle zu einem Administrator finden Sie unter Delegierte Administration und Überwachung.

Um eine genauere Kontrolle über den Zugriff auf die Seite **Filter** für Sitzungen und Maschinen zu erhalten, erstellen Sie eine benutzerdefinierte Rolle und wählen eine der folgenden Optionen für das Director-Objekt: **Filterseite anzeigen –Nur Maschinen**, **Filterseite anzeigen –Nur Sitzungen**. Weitere Informationen zum Erstellen einer benutzerdefinierten Rolle finden Sie unter Erstellen und Verwalten von Rollen.

Unterstützung für einen neuen Maschinentyp. Dieses Release unterstützt nun AMD-Maschinen des Typs NV v4 und DA v4, wenn Premium-Datenträger für einen Maschinenkatalog konfiguriert werden. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

August 2020

Neue und erweiterte Features

Eingeschränkter Zugriff auf das Remote PowerShell SDK bei Ausfall. Bisher konnten Sie PowerShell-Befehle bei einem Ausfall nicht verwenden. Der lokale Hostcache ermöglicht nun während eines Ausfalls eingeschränkten Zugriff auf das Remote PowerShell SDK. Siehe Auswirkungen eines Ausfalls.

Unterstützung für zwei neue Citrix Virtual Apps and Desktops Service-Editionen. Citrix Monitor unterstützt jetzt zwei neue Citrix Virtual Apps and Desktops Service-Editionen: **Citrix Virtual Apps Advanced Service** und **Citrix Virtual Apps and Desktops Advanced Service**. Weitere Informationen finden Sie in der Featurekompatibilitätsmatrix für Citrix Monitor.

Unterstützung freigegebener virtueller privater Clouds (VPCs) in Google Cloud Platform. Citrix Virtual Apps and Desktops Service unterstützt jetzt freigegebene VPCs auf Google Cloud Platform als Hostressource. Sie können Maschinenerstellungsdienste (MCS) verwenden, um Maschinen in einer freigegebenen VPC bereitzustellen und die Maschinen mit Citrix Studio verwalten. Informationen zu freigegebenen VPCs finden Sie unter Freigegebene virtuelle private Cloud.

Unterstützung für die Zonenauswahl für Google Cloud Platform. Citrix Virtual Apps and Desktops Service unterstützt die Zonenauswahl auf Google Cloud Platform. Mit diesem Feature können Administratoren eine oder mehrere Zonen innerhalb einer Region für die Katalogerstellung angeben.

Für Einzelmandanten-VMs können Administrator über die Zonenauswahl Einzelmandantenknoten in Zonen ihrer Wahl platzieren. VMs anderen Typs als Einzelmandanten-VMs können mit der Zonenauswahl deterministisch über Zonen verteilt werden und eine Bereitstellung so flexibler gestaltet werden. Informationen zur Konfiguration finden Sie unter Aktivieren der Zonenauswahl.

Außerdem:

- Die Einzelmandantenfähigkeit bietet exklusiven Zugriff auf einen Knoten für einzelne Mandanten, bei dem es sich um einen physischen Compute Engine-Server handelt, der ausschließlich VMs Ihres Projekts hostet. Mit diesen Knoten können Sie Ihre VMs auf derselben Hardware gruppieren oder von VMs in anderen Projekten trennen.
- Knoten für einzelne Mandanten können dazu beitragen, die Anforderungen bezüglich dedizierter Hardware in Bring Your Own License (BYOL)-Szenarien zu erfüllen. Sie ermöglichen außerdem die Erfüllung von Richtlinien zur Netzwerkzugriffssteuerung und Sicherheit sowie von Datenschutzanforderungen wie etwa HIPAA.

> **Hinweis:**
>
> Die Nutzung der Einzelmandantenfähigkeit ist die einzige Möglichkeit der Bereitstellung einer Windows 10-VDI in Google Cloud. Auch die Server-VDI unterstützt diese Methode. Eine detaillierte Beschreibung der Einzelmandantenfähigkeit finden Sie auf der Google-Dokumentationsseite.

Verbesserte Startleistung für Azure-Systemdatenträger. Dieses Release unterstützt eine verbesserte Startleistung für Citrix Cloud-Implementierungen mit Azure, wenn MCSIO aktiviert ist. Mit dieser Unterstützung können Sie den Systemdatenträger beibehalten. Die Vorteile:

- Der Start von VMs und Anwendungen erfolgt jetzt mit einer dem Gold-Image ähnlichen Leistung.
- Gesenkter API-Kontingentverbrauch beim Löschen und Erstellen des Systemdatenträgers und geringere Zustandsübergangsverzögerung beim Löschen einer VM.

Verwenden Sie zum Beispiel die benutzerdefinierte PowerShell-Eigenschaft `PersistOSDisk` im Befehl `New-ProvScheme`, um dieses Feature zu konfigurieren:


```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>'
<!--NeedCopy-->
```

Weitere Konfigurationsinformationen finden Sie unter Verbessern der Startleistung.

Juli 2020

Neue und erweiterte Features

Unterstützung für granularen, rollenbasierten Zugriff auf die Seite "Filter". Citrix Studio bietet jetzt eine gezieltere Zugriffssteuerung für die Seite **Überwachung > Filter** bei Erstellung einer benutzerdefinierten Rolle. Sie können einer benutzerdefinierten Rolle Berechtigungen zum Anzeigen einer beliebige Kombination von **Maschinen**, **Sitzungen**, **Verbindungen**und **Anwendungsinstanzen** zuweisen. Es gibt folgende vier zusätzliche Optionen für das Objekt **Director** im Fenster **Rolle erstellen**:

- Filterseite anzeigen –Nur Anwendungsinstanzen
- Filterseite anzeigen –Nur Verbindungen
- Filterseite anzeigen –Nur Maschinen
- Filterseite anzeigen –Nur Sitzungen

Weitere Informationen zum Erstellen von Rollen finden Sie unter Erstellen und Verwalten von Rollen.

Unterstützung der Ausschaltverzögerung für zugewiesene VDI-Maschinen (nur PowerShell). In früheren Versionen wurde die Ausschaltverzögerung nur auf nicht zugewiesene Maschinen angewendet. Ab diesem Release gilt die Ausschaltverzögerung sowohl für zugewiesene als auch nicht zugewiesene Maschinen. Weitere Informationen finden Sie unter Energieverwaltung von Maschinen durch Autoscale.

Unterstützung für Windows Client-Lizenzen. Citrix Virtual Apps and Desktops Service unterstützt jetzt die Verwendung von Windows-Clientlizenzen zum Bereitstellen von VMs in Azure. Zum Ausführen von Windows 10-VMs in Azure vergewissern Sie sich, dass Ihre Volumenlizenzvereinbarung mit Mi-

crosoft diese Verwendung autorisiert. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Masterimages.

Mai 2020

Neue und erweiterte Features

Zeitpläne für den Maschinenneustart. Sie können nun angeben, ob sich ein Neustartzeitplan auf Maschinen im Wartungsmodus auswirkt. Dieses Feature ist nur über PowerShell verfügbar. Weitere Informationen finden Sie unter Geplante Neustarts für Maschinen im Wartungsmodus.

Ressourcenverfügbarkeit Sie können jetzt die Ressourcenverfügbarkeit während eines Ausfalls sicherstellen, ohne Ressourcen in jeder Zone (jedem Ressourcenstandort) veröffentlichen zu müssen. Weitere Informationen finden Sie unter Ressourcenverfügbarkeit.

April 2020

Neue und erweiterte Features

Planungsgranularität für VDI-Bereitstellungsgruppen (nur PowerShell) verbessert. AutoScale unterstützt jetzt das Festlegen von Spitzenzeiten für die Tage in einem Zeitplan auf einer Detailebene von 30 Minuten. Sie können die Mindestanzahl ausgeführter Maschinen in einer VDI-Bereitstellungsgruppe für jede halbe Stunde separat festlegen. Außerdem kann AutoScale jetzt die Anzahl der eingeschalteten Maschinen in VDI-Bereitstellungsgruppen auf halbstündlicher statt stündlicher Basis nach oben oder unten skalieren. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.

MTU-Discovery. Das Citrix Protokoll Enlightened Data Transport (EDT) verfügt nun über MTU-Discovery. Mit der MTU-Discovery kann EDT die Nutzlastgröße einer Sitzung automatisch erkennen und festlegen. Das Feature ermöglicht es der ICA-Sitzung, sich an Netzwerke mit nicht standardmäßigen Anforderungen an die maximale Übertragungseinheit bzw. Segmentgröße (MTU bzw. MSS) anzupassen. Durch dies Anpassung wird eine Paketfragmentierung vermieden, die zu einer Leistungsminderung oder einem Fehler beim Einrichten einer ICA-Sitzung führen kann. Das Update erfordert mindestens die Citrix Workspace-App 1911 für Windows. Bei Verwendung von Citrix Gateway ist mindestens Citrix ADC-Firmware-Version 13.0.52.24 oder 12.1.56.22 erforderlich. Weitere Informationen finden Sie unter MTU-Discovery durch EDT.

März 2020

Neue und erweiterte Features

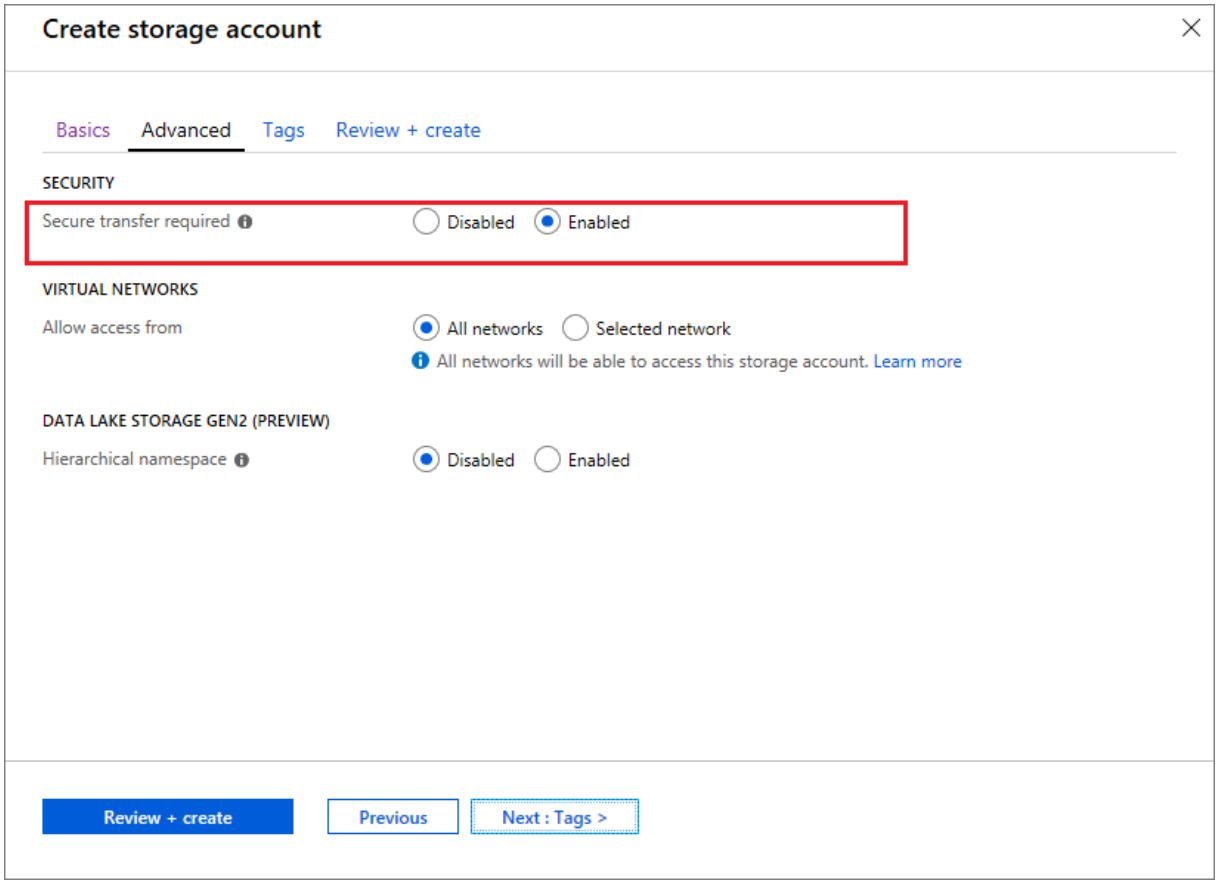
Metriken der PVS-Zielgeräte. Die Seite "Maschinendetails"der Citrix Überwachung bietet nun einen Bereich für PVS-Zielgeräte. In dem Bereich wird der Status der Provisioning-Zielgeräte für Einzelsitzungs-OS- und Multisitzungs-OS-Maschinen angezeigt. In diesem Bereich stehen Metriken für Netzwerk, Start und Cache zur Verfügung. Mit diesen Metriken können Sie PVS-Zielgeräte überwachen und Probleme beheben, um den ordnungsgemäßen Betrieb zu gewährleisten. Weitere Informationen finden Sie unter Metriken der PVS-Zielgeräte.

Erfassung der AWS-Instanzeigenschaft. MCS liest jetzt Eigenschaften aus der Instanz, aus der das AMI stammt, und wendet die IAM-Rolle und -Tags der Maschine auf die für einen bestimmten Katalog bereitgestellten Maschinen an. Wenn Sie dieses optionale Feature verwenden, findet der Katalogerstellungsprozess die ausgewählte AMI-Quellinstanz und liest einen begrenzten Satz von Eigenschaften. Diese Eigenschaften werden dann in einer AWS-Startvorlage gespeichert, mit der Maschinen für den Katalog bereitgestellt werden. Alle Maschinen im Katalog erben die erfassten Instanzeigenschaften. Weitere Informationen finden Sie unter Erfassung der AWS-Instanzeigenschaft.

Tagging von AWS-Betriebsressourcen. Dieses Release enthält eine neue Option für das Tagging von durch Citrix Komponenten beim Provisioning erstellten Ressourcen. Jedes Tag ist ein Kennzeichen bestehend aus einem vom Kunden definierten Schlüssel und einem optionalen Wert, mit dem Sie Ressourcen verwalten, suchen und filtern können. Weitere Informationen finden Sie unter Tagging von AWS-Betriebsressourcen.

Sichere Übertragung in Azure-Speicher. Maschinenerstellungsdienste (MCS) bietet eine Erweiterung für Speicherkonten, die von per MCS bereitgestellten Katalogen in Azure Resource Manager erstellt wurden. Diese Erweiterung ermöglicht automatisch die Eigenschaft "Sichere Übertragung erforderlich". Diese Option erhöht die Sicherheit des Speicherkontos, indem nur Anforderungen von sicheren Verbindungen zugelassen werden. Weitere Informationen finden Sie unter Erzwingen einer sicheren Übertragung für sichere Verbindungen auf der Microsoft-Website.

Aktivieren Sie die Eigenschaft **Sichere Übertragung erforderlich** beim Erstellen eines Speicherkontos in Azure:



Unterstützung für mit Azure verwaltete SSD-Datenträger. Maschinenerstellungsdienste (MCS) unterstützt standardmäßige verwaltete SSD-Datenträger für virtuelle Azure-Maschinen. Dieser Datenträgertyp bietet konsistente Leistung und eine bessere Verfügbarkeit als HDD-Datenträger. Weitere Informationen finden Sie unter Standard-SSD-Datenträger für virtuelle Azure-Maschinenworkloads.

Verwenden Sie die benutzerdefinierte PowerShell-Eigenschaft `StorageAccountType` im Befehl `New-ProvScheme` oder `Set-ProvScheme`, um dieses Feature zu konfigurieren:

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
<!--NeedCopy-->
```

> **Hinweis:**
>
> Dieses Feature ist nur verfügbar, wenn verwaltete Datenträger verwendet werden, d. h. die benutzerdefinierte Eigenschaft`UseManagedDisks` ist auf **true** festgelegt. Bei nicht verwalteten Datenträgern werden nur Standard- und Premium-SSD unterstützt.

Januar 2020

Neue und erweiterte Features

Sprachenleiste in Citrix Studio hinzugefügt. Ab dieser Version bietet Citrix Studio eine Sprachenleiste zum leichteren Zugriff auf das korrekte Tastaturlayout.

- Wenn Citrix Cloud oder die Browseranzeige die Sprache **Englisch** oder **Japanisch** verwendet, wird die Sprachenleiste nicht angezeigt.
- Wenn Citrix Cloud oder die Browseranzeige die Sprache **Deutsch**, **Spanisch** oder **Französisch** verwendet, wird die Sprachenleiste nach dem Anmelden bei Citrix Studio angezeigt. In der Sprachenleiste sind zwei Sprachoptionen aufgelistet. Wählen Sie die Sprache aus, die in den Browsereinstellungen an erster Position steht.

  > **Tipp:**
  >
  > - Für die Sprachenleiste konfigurierte Einstellungen sind möglicherweise nicht wirksam. Melden Sie sich in diesem Fall ab und wieder an.
  > - Sie können möglicherweise bestimmte Symbole und lokalisierte Zeichen nicht über die Sprachenleiste eingeben. Um das Problem zu lösen, müssen Sie die Sprache für Citrix Cloud, die Anzeigesprache Ihres Browsers und das lokale Tastaturlayout konfigurieren. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX310743.

Timer für maximale Verzögerung bei Neustarts (nur PowerShell). Für geplante Neustarts von Maschinen in einer Bereitstellungsgruppe, die aufgrund eines Ausfalls der Standortdatenbank nicht beginnen, können Sie angeben, wie lange über die geplante Startzeit hinaus gewartet werden soll. Wenn die Datenbankverbindung während dieses Zeitraums wiederhergestellt wird, beginnt der Neustart. Wenn die Verbindung während des Zeitraums nicht wiederhergestellt wird, beginnen die Neustarts nicht. Weitere Informationen finden Sie unter Verzögerung geplanter Neustarts aufgrund eines Datenbankausfalls.

Vertikaler Lastausgleich (nur PowerShell). Der Service verwendete zuvor den horizontalen Lastausgleich für alle RDS-Starts, bei dem die eingehende Last der am wenigsten belasteten RDS-Maschine zugewiesen wird. Dies bleibt weiterhin Standardeinstellung. In der neuen Version können Sie mit PowerShell den vertikalen Lastausgleich siteübergreifend aktivieren.

Wenn der vertikale Lastausgleich aktiviert ist, weist der Broker die eingehende Last der am stärksten belasteten Maschine zu, die noch keinen oberen Schwellenwert erreicht hat. Dadurch werden vorhandene Maschinen vollständig genutzt, bevor zu neuen Maschinen gewechselt wird. Wenn Benutzer die Verbindung trennen und Maschinen freigeben, wird diesen Maschinen neue Last zugewiesen.

Standardmäßig ist der horizontale Lastausgleich aktiviert. Zum Anzeigen, Aktivieren oder Deaktivieren des vertikalen Lastenausgleichs unterstützen die Cmdlets `Get-BrokerSite` und `Set`

`-BrokerSite` jetzt die Einstellung `UseVerticalScalingForRdsLaunches`. Weitere Informationen finden Sie unter Lastverwaltung von Maschinen in Bereitstellungsgruppen.

Dezember 2019

Neue und erweiterte Features

Service für Citrix Service Providers (CSP). CSPs können jetzt das Onboarding von Mandantenkunden im Virtual Apps and Desktops Service ausführen, den Zugriff der Kundenadministratoren auf den Service konfigurieren und den Benutzern der Kunden über Verbunddomänen gemeinsame und dedizierte Workspaces bereitstellen. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Service für Citrix Service Provider.

Ermittlung des Grundes, aus dem eine Maschine im Wartungsmodus ist (nur PowerShell). Mit PowerShell können Sie nun ermitteln, warum sich eine Maschine im Wartungsmodus befindet. Verwenden Sie dazu den Parameter `-MaintenanceModeReason`. Anhand dieses Features können Administratoren Probleme mit Maschinen im Wartungsmodus beheben. Einzelheiten finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/.

Autoscale. Autoscale bietet nun die Möglichkeit, Maschinen dynamisch zu erstellen und zu löschen. Sie können das Feature mit einem PowerShell-Skript nutzen. Mit dem Skript können Sie die Anzahl der Maschinen in einer Bereitstellungsgruppe basierend auf aktuellen Lastbedingungen dynamisch nach oben oder unten skalieren. Weitere Informationen finden Sie unter Dynamische Bereitstellung von Maschinen mit Autoscale.

Dezember 2019

Neue und erweiterte Features

Unterstützung für GroomStartHour. Die Überwachung unterstützt jetzt **GroomStartHour**, eine neue Konfiguration, mit der die Uhrzeit für den Start der Bereinigung festgelegt werden kann. Weitere Informationen finden Sie in der Dokumentation zum Citrix Virtual Apps and Desktops SDK.

OData-Paginierung. Die Überwachung unterstützt jetzt **OData-Paginierung**. Alle OData v4-Endpunkte geben maximal 100 Datensätze pro Seite mit einem Link zu den nächsten 100 Datensätzen in der Antwort zurück. Weitere Informationen finden Sie unter Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Oktober 2019

Neue und erweiterte Features

App-V. App-V-Funktionalität ist jetzt in Citrix Cloud verfügbar. Sie können dem Delivery Controller in Ihrer Citrix Cloud-Konfiguration App-V-Pakete im Einzel- und Dualverwaltungsmodus hinzufügen. Das *Virtual Apps and Desktops Service-Modul zur App-V-Paketdiscovery* steht auf Citrix Downloads zur Verfügung und ermöglicht den Import von App-V-Paketen sowie die Registrierung von Microsoft App-V-Servern. Die enthaltenen Apps stehen dann den Benutzern zur Verfügung. Mit diesem PowerShell-Modul können Sie Microsoft App-V-Verwaltungsserver und -Veröffentlichungsserver über DNS-URLs registrieren. Dadurch wird vermieden, dass Server in Lastausgleichsgruppen über ihre Maschinen-URL registriert werden müssen. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops –Discovery für App-V-Pakete und Server.

Google Cloud Platform Citrix Virtual Apps and Desktops unterstützt jetzt die Verwendung der Maschinenerstellungsdienste (MCS) für das Provisioning von Maschinen auf der Google Cloud Platform (GCP). Weitere Informationen finden Sie unter Google Cloud Platform-Virtualisierungsumgebungen.

September 2019

Neue und erweiterte Features

VDA-Unterstützung für Azure Virtual Desktop. Informationen zu unterstützten Betriebssystemen und VDA-Versionen siehe VDAs in einer Azure Virtual Desktop-Umgebung.

Verbesserte Energierichtlinie. In früheren Versionen mussten VDI-Maschinen beim Übergang in einen Zeitraum, in dem eine Aktion (Trennaktion = "**Anhalten**"oder "**Herunterfahren**") erforderlich war, eingeschaltet bleiben. Das Szenario trat auf, wenn eine Maschine während eines Zeitraums (Spitzen- oder Nebenzeit) getrennt wurde, in der keine Aktion (Trennaktion = **Nothing**) erforderlich war.

Ab diesem Release wird die Maschine nach Ablauf der festgelegten Trennzeit von Autoscale angehalten oder ausgeschaltet (je nach der für den Zielzeitraum konfigurierten Trennaktion). Weitere Informationen finden Sie unter Energieverwaltung von VDI-Maschinen beim Übergang in einen anderen Zeitraum mit getrennten Sitzungen.

Maschinenkataloge: Tags. Sie können jetzt mit PowerShell Tags auf Maschinenkataloge anwenden. Weitere Informationen finden Sie unter Anwenden von Tags auf Maschinenkataloge.

Sitzungsstartdauer. In "Überwachen"wird nun die Dauer von Sitzungsstarts in Workspace-App- und VDA-Phasen angezeigt. Anhand dieser Daten können Sie Verzögerungen beim Sitzungsstart auf den Grund gehen und beheben. Darüber hinaus lassen sich anhand der Angaben zur Zeitdauer der einzelnen Sitzungsstartphasen Probleme mit diesen Phasen gezielt beheben. Wenn beispielsweise

die Dauer der Laufwerkzuordnung lang ist, können Sie überprüfen, ob alle gültigen Laufwerke im Gruppenrichtlinienobjekt oder Skript korrekt zugeordnet sind. Dieses Feature ist ab VDA-Version 1903 verfügbar. Weitere Informationen finden Sie unter Diagnostizieren von Problemen beim Sitzungsstart.

August 2019

Neue und erweiterte Features

Automatische Sitzungswiederverbindung. Die Seite "Sitzungen"auf der Registerkarte "Trends" enthält jetzt Informationen zur Anzahl der automatischen Wiederverbindungen. Automatische Wiederverbindungen werden versucht, wenn die Richtlinie "Sitzungszuverlässigkeit"oder "Automatische Wiederverbindung von Clients"aktiviert sind. Die Informationen zur automatischen Wiederverbindung ermöglichen die Anzeige und Problembehandlung von Netzwerkverbindungen mit Unterbrechungen und die Analyse von Netzwerken mit nahtloser Erfahrung.

Der Drilldown bietet zusätzliche Informationen wie Sitzungszuverlässigkeit oder automatische Wiederverbindung von Clients, Zeitstempel, IP-Adresse und Name des Endpunkts, auf dem die Workspace-App installiert ist. Das Feature ist für die Citrix Workspace-App für Windows, die Citrix Workspace-App für Mac, Citrix Receiver für Windows und Citrix Receiver für Mac verfügbar. Dieses Feature erfordert VDAs der Version 1906 oder höher. Weitere Informationen:

- Sitzungen
- Automatische Wiederverbindung von Clients - Richtlinieneinstellungen
- Sitzungszuverlässigkeit - Richtlinieneinstellungen
- Automatische Sitzungswiederverbindung

Juli 2019

Neue und erweiterte Features

Konfigurationsprotokollierung. Sie können jetzt das Remote PowerShell SDK verwenden, um den Inhalt der Konfigurationsprotokollierungsdatenbank regelmäßig zu löschen. Weitere Informationen finden Sie unter Periodische Datenlöschung planen.

Autoscale. Autoscale bietet jetzt die Flexibilität, die Energieverwaltung nur für eine Teilmenge der Maschinen in einer Bereitstellungsgruppe durchzuführen. Diese Funktion kann in Anwendungsfällen nützlich sein, in denen Sie On-Premises-Ressourcen verwenden möchten, um Workloads zu verarbeiten, bevor cloudbasierte Ressourcen andere Anforderungen (d. h. Burstworkloads) erfüllen. Weitere Informationen finden Sie unter Einschränken von Autoscale auf bestimmte Maschinen in einer Bereitstellungsgruppe.

Lokaler App-Zugriff und URL-Umleitung. Mit Citrix Studio können Sie nun mit dem PowerShell SDK für Ihre Site die Option "Anwendung für lokalen App-Zugriff hinzufügen"der Studio-Benutzeroberfläche hinzufügen. Weitere Informationen finden Sie unter Zugriffsbeschränkung auf veröffentlichte Anwendungen.

Änderungen am Betriebssystemnamen. Die Betriebssystemnamen auf den Seiten **Maschinenkatalog erstellen > Maschinenkatalogerstellung > Betriebssystem** und **Überwachen** wurden geändert:

- Multisitzungs-OS (früher "Serverbetriebssysteme"): Der Maschinenkatalog mit Betriebssystemen für mehrere Sitzungen stellt gehostete, freigegebene Desktops für großvolumige Bereitstellungen von standardisierten Windows-Betriebssystemen für mehrere Sitzungen oder Linux-OS-Maschinen bereit.
- Einzelsitzungs-OS (früher "Desktopbetriebssysteme"): Der Maschinenkatalog für Einzelsitzungs-OS bietet VDI-Desktops, die sich ideal für diverse Benutzer eignen.

Citrix Profilverwaltung –Verarbeitungsdauer. Unter "Überwachen"wird nun die Dauer der Profilverarbeitung im Balken "Profilladezeit"des Anmeldedauerdiagramms angezeigt. Dabei handelt es sich um die von der Citrix Profilverwaltung für die Verarbeitung von Benutzerprofilen benötigte Zeit. Anhand dieser Informationen ist eine gezieltere Problembehandlung bei langer Profilladedauer möglich. Diese Erweiterung ist bei VDAs der Version 1903 und höher verfügbar. Weitere Informationen finden Sie unter Profilladezeit.

Desktoptests. Desktoptests sind ein Feature von Citrix Virtual Apps and Desktops Service. Es automatisiert das Überprüfen der Integrität der in einer Site veröffentlichten virtuellen Desktops und verbessert so die Benutzererfahrung. Installieren Sie Citrix Probe Agent auf mindestens einem Endpunkt und konfigurieren Sie den Agent, um die Desktoptests zu beginnen. Desktoptests stehen für Sites mit Premium-Lizenz zur Verfügung. Für dieses Feature ist Citrix Probe Agent 1903 oder höher erforderlich. Weitere Informationen finden Sie unter Anwendungs- und Desktoptests.

> **Hinweis:**
>
> Citrix Probe Agent unterstützt jetzt TLS 1.2.

Juni 2019

Neue und erweiterte Features

Beschränken nach Tags. Tags sind Zeichenfolgen zur Identifizierung von Elementen wie z. B. Maschinen, Anwendungen, Desktops, Anwendungsgruppen und Richtlinien. Durch Erstellen und Hinzufügen von Tags können Sie festlegen, dass bestimmte Vorgänge nur an Elementen stattfinden, die ein spezifisches Tag haben. Weitere Informationen finden Sie unter Anwendungsgruppen und Tags.

E-Mail-Benachrichtigungen. Der Citrix Virtual Apps and Desktops Service sendet E-Mail-Benachrichtigungen im Zusammenhang mit Warnungen und Tests direkt. Dadurch ist die Konfiguration des SMTP-E-Mail-Servers überflüssig. Das Feld **Benachrichtigungseinstellungen** ist standardmäßig aktiviert und Citrix Cloud sendet Benachrichtigungen an die E-Mail-Adressen, die im Abschnitt **Benachrichtigungseinstellungen** angegeben wurden. Stellen Sie sicher, dass die E-Mail-Adresse `donotreplynotifications@citrix.com` in Ihrer E-Mail-Bereitstellung auf der Positivliste steht.

Mai 2019

Neue und erweiterte Features

Autoscale. Autoscale ist ein Feature für Citrix Virtual Apps and Desktops Service zur konsistenten und proaktiven Verwaltung Ihrer Maschinen. Es zielt auf eine Balance zwischen Kosten und Benutzererfahrung ab. Autoscale integriert die veraltete Smart Scale-Technologie in die Energieverwaltung von Studio. Weitere Informationen finden Sie unter Autoscale. Sie können die Kennzahlen von mit Autoscale verwalteten Maschinen auf den Seiten "Trends"der Registerkarte **Monitor** überwachen. Weitere Informationen finden Sie unter Überwachen von mit Autoscale verwalteten Maschinen.

Februar 2019

Neue und erweiterte Features

Überwachen von Hypervisorwarnungen. Warnungen von Citrix Hypervisor und VMware vSphere werden jetzt auf der Registerkarte **Überwachen** > **Warnungen** zur Überwachung der folgenden Zustände/Parameter des Hypervisors angezeigt:

- CPU-Nutzung
- Speichernutzung
- Netzwerknutzung
- Hypervisorverbindung nicht verfügbar
- Datenträgernutzung (nur vSphere)
- Hostverbindung oder Energiezustand (nur vSphere)

Weitere Informationen finden Sie im Abschnitt zum Überwachen von Hypervisor-Warnungen unter Warnungen und Benachrichtigungen.

Kommunikation mit älteren TLS- Versionen. Um die Sicherheit des Service weiter zu erhöhen, wird ab dem 15. März 2019 jede Kommunikation über TLS 1.0 und 1.1 von Citrix blockiert. Zulässig ist nur TLS 1.2. Weitere Informationen finden Sie unter TLS-Versionen. Ausführliche Erläuterungen finden Sie unter CTX247067.

Anwendungsgruppen. Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden. Weitere Informationen finden Sie unter Erstellen von Anwendungsgruppen.

Anmeldeleistung –Profildrilldown. Unter **Anmeldedauer** im Bereich **Benutzerdetails** der Registerkarte **Überwachen** werden jetzt Drilldown-Informationen zur **Profilladephase** beim Anmeldeprozess angezeigt. Der Profildrilldown bietet nützliche Informationen zu Benutzerprofilen der aktuellen Sitzung, anhand derer Administratoren Lastprobleme in Bezug auf Profile beheben können. Es wird ein Tooltipp mit folgenden Benutzerprofilinformationen angezeigt:

- Anzahl Dateien
- Profilgröße
- Anzahl großer Dateien

Ein detaillierter Drilldown liefert Informationen zu einzelnen Ordnern, deren Größe und der Anzahl der Dateien. Dieses Feature ist ab VDA-Version 1811 verfügbar. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

Microsoft RDS-Lizenzstatus. Der Lizenzstatus von Microsoft RDS (Remotedesktopdienste) kann im Fenster **Maschinendetails** auf den Seiten "Maschinendetails"und "Benutzerdetails"für Serverbetriebssystemmaschinen überwacht werden. Der Lizenzstatus wird in Form einer Meldung angezeigt. Durch Zeigen auf das Infosymbol können Sie weitere Details anzeigen. Weitere Informationen finden Sie unter Microsoft RDS-Lizenzstatus.

Anwendungstests. Das Feature automatisiert die Untersuchung der Integrität virtueller, in einer Site veröffentlichter Apps.

Starten der Anwendungstests:

- Installieren Sie auf mindestens einer Endpunktmaschine den Citrix Application Probe Agent.
- Konfigurieren Sie den Citrix Application Probe Agent mit den Anmeldeinformationen für Citrix Workspace und Citrix Virtual Apps and Desktops Service.
- Konfigurieren Sie die zu testenden Anwendungen, die Endpunktmaschinen, auf denen der Test ausgeführt werden soll, und den Zeitplan unter **Überwachen** > **Konfiguration** in Citrix Virtual Apps and Desktops Service.

Der Agent testet den Start ausgewählter Anwendungen über Citrix Workspace und meldet das Ergebnis auf der Registerkarte **Überwachen** von Citrix Virtual Apps and Desktops Service:

- Seite "Anwendungen": Daten der letzten 24 Stunden und Seite **Trends** > **Anwendungstestergebnisse**
- Die historischen Testdaten sowie die Phase, in denen Fehler aufgetreten sind: Workspaceerreichbarkeit, Workspaceauthentifizierung, Workspaceenumeration, ICA-Download oder Anwendungsstart

Der Fehlerbericht wird per E-Mail an die konfigurierten Adressen gesendet. Sie können die Durchführung von Anwendungstests für außerhalb der Spitzenzeiten in mehreren geografischen Regionen planen. So können Sie die Testergebnisse nutzen, um Probleme bei Anwendungen, Hostmaschinen oder Verbindungen zu beheben, bevor sie sich bei den Benutzern bemerkbar machen. Weitere Informationen finden Sie unter Anwendungs- und Desktoptests.

Januar 2019

Neue und erweiterte Features

Delegierte Administration mit benutzerdefiniertem Bereich. Die Überwachung unterstützt jetzt benutzerdefinierte Bereiche für integrierte, delegierte Administratorrollen. Weitere Informationen zu den verfügbaren integrierten Rollen für die Überwachung und zu ihrer Zuweisung finden Sie unter Delegierte Administratoren.

Dezember 2018

Neue und erweiterte Features

Das Datum, nach dem Citrix die Kommunikation über TLS (Transport Layer Security) 1.0 und 1.1 blockiert, wurde vom 31. Dezember 2018 auf den 31. Januar 2019 verschoben. Weitere Informationen finden Sie unter Einstellung der Unterstützung von TLS-Versionen.

November 2018

Neue und erweiterte Features

Historische Maschinendaten über OData-API verfügbar: Historische Maschinenanalysedaten sind jetzt über die OData-API verfügbar. Die Daten werden stündlich erfasst und pro Tag angegeben.

- Anzahl der eingeschalteten Maschinen (bei Maschinen mit Energieverwaltung)
- Anzahl der registrierten Maschinen
- Anzahl der Maschinen im Wartungsmodus
- Gesamtanzahl der Maschinen

Die Daten werden für den Zeitraum des Ausführens des Überwachungsdiensts aggregiert. Weitere Informationen zur Verwendung der OData-API und entsprechende Beispiele finden Sie unter Citrix Monitor Service 7 1808. Das Datenbankschema finden Sie unter Monitor Service Schema.

Anmeldungsleistung: Drilldown für interaktive Sitzungen: Der Bereich **Anmeldedauer** in den **Benutzer- und Sitzungsdetails** enthält jetzt Informationen zur **interaktiven Sitzungsphase** des Anmeldeprozesses. Die für die drei Teilphasen **Pre-userinit**, **Userinit** und **Shell** benötigte Zeit wird auf der Leiste **Interaktive Sitzungen** als QuickInfo angezeigt. Dies ermöglicht eine detailliertere Problembehandlung dieser Anmeldungsphase. Es werden außerdem die kumulative Verzögerung zwischen den Teilphasen und ein Link zur Dokumentation angezeigt. Das Feature ist ab Delivery Controller-Version 7 1808 verfügbar. Die Leiste **Interaktive Sitzungen** zeigt nur die Zeitdauer für die aktuelle Sitzung an. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

Anmeldungsleistung: GPO-Drilldown: Der Bereich **Anmeldedauer** in den **Benutzer- und Sitzungsdetails** enthält Informationen zur GPO-Anwendungsdauer. Dabei handelt es sich um die Zeit, die das Anwenden der Gruppenrichtlinienobjekte auf die virtuelle Maschine während der Anmeldung gedauert hat. Sie können jetzt einen Drilldown für jede gemäß CSE (clientseitige Erweiterung) angewendete Richtlinie in Form einer QuickInfo auf der GPO-Leiste sehen. Der Drilldown umfasst Status und Dauer für jede Richtlinienanwendung. Diese zusätzlichen Informationen erleichtern die Problembehandlung bei einer exzessiven GPO-Anwendungsdauer. Die Zeitangaben im Drilldown repräsentieren nur die CSE-Verarbeitungszeit und nicht die gesamte GPO-Dauer. Das Feature ist ab Delivery Controller-Version 7 1808 verfügbar. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

Fixes

Beim Überwachen gespeicherte Abfragen für benutzerdefinierte Berichte sind nach einem Cloud-Upgrade nicht verfügbar. [DNA-23420]

October 2018

Neue und erweiterte Features

Anwendungen: Limit pro Maschine Sie können jetzt die Zahl der Anwendungsinstanzen pro Maschine begrenzen. Das Limit gilt für alle Maschinen der Site. Das Limit gilt zusätzlich zum bestehenden Anwendungslimit für die Benutzer einer Bereitstellungsgruppe und zum Limit pro Benutzer. Diese Funktion ist nur über PowerShell und nicht in Studio verfügbar. Weitere Informationen finden Sie unter Konfigurieren von Anwendungslimits.

Windows Server 2019. Sie können VDAs für Multisitzungs-OS (zuvor "VDAs für Serverbetriebssysteme") jetzt wie unter Systemanforderungen beschrieben auf Maschinen mit Windows Server 2019 installieren.

September 2018

Neue und erweiterte Features

Delegierte Administration. Mit der Delegierten Administration können Sie die Zugriffsberechtigungen aller Administratoren gemäß ihrer Rolle in der Organisation konfigurieren. Weitere Informationen finden Sie unter Delegierte Administration. Die Überwachung unterstützt die Zuweisung integrierter Rollen. Integrierte Rollen sind mit vollem Bereich verfügbar. Weitere Informationen zu den integrierten Rollen für die Überwachung und zu ihrer Zuweisung finden Sie unter Delegierte Administratoren.

Konfigurationsprotokollierung. Mit der Konfigurationsprotokollierung können Administratoren Konfigurationsänderungen und Administratoraktivitäten überwachen. Weitere Informationen finden Sie unter Konfigurationsprotokollierung.

Mehrere bislang deaktivierte PowerShell-Cmdlets in der Remote PowerShell SDK sind jetzt für die Verwendung mit der Konfigurationsprotokollierung aktiviert:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Lokaler Hostcache. Der Lokale Hostcache ist jetzt vollständig verfügbar. Der lokale Hostcache ermöglicht das fortgesetzte Verbindungsbrokering, wenn ein Cloud Connector an einem Ressourcenstandort nicht mit Citrix Cloud kommunizieren kann. Weitere Informationen finden Sie unter Lokaler Hostcache.

Citrix Provisioning. Zur Bereitstellung von VDAs können Sie jetzt das Citrix Provisioning oder vorhandene Maschinenerstellungsdienste (MCS) verwenden. Spezielle Informationen zum Citrix Provisioning für die Cloudumgebung finden Sie unter Citrix Provisioning managed by Citrix Cloud.

Fixes

In früheren Versionen wurden bei Verwendung des bedarfsgesteuerten Provisionings von Azure alle VMs beim Ausschalten gelöscht. Jetzt werden nur gepoolte VMs gelöscht. Persistente (dedizierte) VMs werden beim Ausschalten nicht gelöscht.

August 2018

- **Neue Produktnamen**

Wenn Sie eine Zeit lang Kunde oder Partner von Citrix waren, werden Sie in unseren Produkten und in dieser Produktdokumentation neue Namen bemerken. Wenn Sie mit diesem Citrix Produkt noch nicht vertraut sind, sehen Sie möglicherweise unterschiedliche Namen für ein Produkt oder eine Komponente.

Die neuen Produkt- und Komponentennamen stammen aus der wachsenden Citrix Portfolio- und Cloudstrategie. Artikel in dieser Produktdokumentation verwenden auch die folgenden Namen.

- **Citrix Virtual Apps and Desktops:** Citrix Virtual Apps and Desktops ist eine Lösung für virtuelle Apps und Desktops, die in der Cloud oder lokal bereitgestellt wird und dem Personal von Unternehmen die Möglichkeit bietet, überall auf jedem Gerät zu arbeiten und gleichzeitig zur Senkung der IT-Kosten beiträgt. Stellen Sie Windows-, Linux-, Web- und SaaS-Anwendungen oder vollständige virtuelle Desktops aus jeder Cloud bereit: öffentlich, im eigenen Rechenzentrum oder hybrid. Virtual Apps and Desktops hieß vorher XenApp und XenDesktop.
- **Citrix Workspace-App:** Die Citrix Workspace-App umfasst vorhandene Citrix Receiver-Technologie und anderen Citrix Workspace-Clienttechnologien. Sie wurde um weitere Funktionen erweitert, die Endbenutzern eine einheitliche, kontextbezogene Erfahrung bieten, in der sie mit allen erforderlichen Apps, Dateien und Geräten für ihre Arbeit interagieren können. Weitere Informationen finden Sie in diesem Blogbeitrag.
- **Citrix SD-WAN:** NetScaler SD-WAN, eine wichtige Technologie für unsere Kunden und Partner, die ihre Zweigstellennetzwerke und WANs mit Cloudtechnologie transformieren, ist jetzt Citrix SD-WAN.
- **Citrix Secure Web Gateway:** Im Rahmen der Erweiterung des Citrix Networking-Portfolios bieten wir unseren robusten Citrix Secure Web Gateway-Service an, der zuvor NetScaler Secure Web Gateway hieß.
- **Citrix Gateway:** Das robuste NetScaler Unified Gateway bietet einen sicheren, kontextabhängigen Zugriff auf Apps und Daten und heißt jetzt Citrix Gateway.
- **Citrix Content Collaboration und Citrix Files für Windows:** Die erweiterten ShareFile-Features für Zugriff, Zusammenarbeit, Workflows, Rechteverwaltung und Integration stehen jetzt über die Citrix Content Collaboration-Komponente des sicheren, kontextbezogenen und integrierten Citrix Workspace zur Verfügung. Citrix Files für Windows bietet in einer nativen Windows Explorer-Umgebung direkten Zugriff auf Content Collaboration-Dateien über ein zugeordnetes Laufwerk.
- **Citrix Hypervisor:** Die auf dem XenProject-Hypervisor basierende Technologie von XenServer für die Virtualisierungsinfrastruktur heißt jetzt Citrix Hypervisor.

Kurze Zusammenfassung:

Jetzt	Vorher
Citrix Virtual Apps and Desktops	XenApp und XenDesktop
Citrix Workspace-App	Umfasst Citrix Receiver und umfangreiche Erweiterungen
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files für Windows	ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

Die Implementierung dieser Umstellung in unsere Produkte und deren Dokumentation ist ein kontinuierlicher Prozess.

- Produktinhalte verwenden möglicherweise noch die früheren Namen. Beispielsweise können Sie Instanzen der früheren Namen in Konsolentext, Meldungen und Verzeichnis-/Dateinamen sehen.
- Es ist möglich, dass einige Elemente (z. B. Befehle und MSIs) ihre früheren Namen beibehalten, damit vorhandene Kundenskripts auch weiter funktionieren.
- Die zugehörige Produktdokumentation und andere Ressourcen (z. B. Videos und Blogposts), zu denen es Links in dieser Produktdokumentation gibt, verwenden möglicherweise weiterhin die früheren Namen.
- Citrix Hypervisor: Der neue Name wird seit September 2018 auf der Citrix Website und in Infomaterial zum Produkt verwendet. Der neue Name erscheint außerdem in den Verwaltungskonsolen einiger Citrix Produkte, z. B. Citrix Virtual Apps and Desktops. In der XenServer-Produktversion und der technischen Dokumentation wird bis Anfang 2019 weiterhin die Bezeichnung “XenServer 7.x”verwendet.

Wir danken Ihnen für Ihre Geduld während dieser Umstellung.

Weitere Informationen zu den neuen Namen finden Sie unter https://www.citrix.com/about/citrix-product-guide/.

- **Geänderte Versionsnummern für Produkte und Komponenten**

  Citrix installiert und verwaltet die meisten Citrix Virtual Apps and Desktops-Komponenten, sodass Sie sich mit diesen Versionsnummern nicht befassen müssen. Bei der Installation von

Cloud Connectors und beim Installieren oder Aktualisieren von VDAs in Ressourcenstandorten werden jedoch möglicherweise Versionsnummern angezeigt.

Citrix Virtual Apps and Desktops-Versionsnummern für Produkte und Komponenten haben folgendes Format: ***JJMM.c.m.b***

- JJMM = Jahr und Monat der Freigabe des Produkts oder der Komponente. Ein Release im September 2018 wird beispielsweise mit "1809"angezeigt.
- c = Citrix Cloud-Releasenummer für den Monat.
- m = Wartungsversion (falls zutreffend).
- b = Buildnummer. Dieses Feld wird nur auf der Infoseite der Komponente und im Dialogfeld des Betriebssystems zum Entfernen oder Ändern von Programmen angezeigt.

Citrix Virtual Apps and Desktops 1809.1.0 zeigt beispielsweise an, dass die Komponente im September 2018 veröffentlicht wurde. Der Release ist mit dem Citrix Cloud Release 1 dieses Monats verknüpft und ist keine Wartungsversion. In einigen Anzeigen erscheinen nur Jahr und Monat der Version, beispielsweise **Citrix Virtual Apps and Desktops 1809**.

In früheren Produktversionen (bis 7.18) wurden Versionsnummern im Format "7.*version*" dargestellt, wobei sich der Wert "version"mit jeder Version um eins erhöhte. Auf VDA-Release nach XenApp und XenDesktop 7.17 folgte beispielsweise 7.18. Das Format von älteren Releases (bis 7.18) wird nicht aktualisiert.

- **Einstellung der Unterstützung von TLS-Versionen.** Um die Sicherheit von Citrix Virtual Apps and Desktops weiter zu erhöhen, wird nach dem 31. Dezember 2018 jede Kommunikation über TLS 1.0 und 1.1 von Citrix blockiert. Weitere Informationen finden Sie unter Einstellung der Unterstützung von TLS-Versionen.
- **Google Cloud Platform-Virtualisierungsumgebung.** Der Citrix Virtual Apps and Desktops-Service unterstützt den manuellen Neustart von Virtual Apps and Desktop-VMs auf der Google Cloud Platform (GCP). Weitere Informationen finden Sie unter Google Cloud Platform-Virtualisierungsumgebungen.

Juli 2018

- **Export von Filterdaten.** Sie können jetzt Echtzeit-Überwachungsdaten über die Registerkarte **Überwachen** > **Filter** in eine CSV-Datei exportieren. Die Exportfunktion ist auf den Seiten "Maschinen", "Sitzungen", "Verbindungen"und "Anwendungsinstanzen"verfügbar. Sie können einen vordefinierten Filter oder eigene Filterkriterien sowie die erforderlichen Tabellenspalten auswählen und die Daten exportieren. Daten von bis zu 100.000 Datensätzen können exportiert werden. Die CSV-Exportdateien bieten einen umfassenden Überblick über die Echtzeitdaten und erleichtern die Analyse großer Datenmengen.

Juni 2018

- **Azure Resource Manager-Verbindungen.** Im Studio-Assistenten für die Verbindungserstellung enthält die Azure-Umgebungsauswahl auf der Seite **Verbindung** alle Azure-Clouds, die für Ihr Azure-Abonnement gültig sind. Die allgemeine Verfügbarkeit der Azure US Government Cloud und der Azure Deutschland-Cloud ersetzt die Vorschauversionen dieser beiden Umgebungen in früheren Versionen.

Mai 2018

- **Azure Quick Deploy.** Wenn Ihr Ressourcenstandort Maschinen mit Azure Resource Manager zum Bereitstellen von Anwendungen und Desktops verwendet, haben Sie die Wahl zwischen folgenden Bereitstellungsmethoden:
  - Vollständige Konfiguration: Mit dieser Methode erstellen Sie mit der Studio-Verwaltungskonsole zunächst einen Maschinenkatalog und anschließend eine Bereitstellungsgruppe.
  - Azure Quick Deploy: Diese neue Option beschleunigt die Bereitstellung von Apps und Desktops durch eine vereinfachte Benutzeroberfläche.
- **Link zu Citrix Health Assistant.** Nicht registrierte Maschinen haben jetzt in der Überwachungskonsole auf der Seite "Maschinendetails"die Schaltfläche **Health Assistant**. Aktuell bietet die Schaltfläche einen Link zu den Artikeln Problembehandlung bei Maschinen und Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch im Knowledge Center, wo Sie das Tool herunterladen können. Citrix Health Assistant ist ein Tool zum Beheben von Konfigurationsproblemen bei nicht registrierten VDAs. Durch mehrere automatisierte Systemdiagnosen wird die mögliche Ursache häufiger Konfigurationsprobleme bei der VDA-Registrierung, beim Sitzungsstart und bei der Zeitzonenumleitung gesucht.
- **Drilldown für interaktive Sitzungen.** In der Überwachungskonsole enthält der Bereich **Benutzerdetails > Anmeldedauer** jetzt Informationen zur **interaktiven** Phase des Anmeldeprozesses. Um Probleme in dieser Phase der Anmeldung detaillierter zu behandeln und zu beheben, gibt es für die **interaktive Sitzung** jetzt drei Unterphasen: **Pre-userinit**, **Userinit** und **Shell**. In dieser Version wird durch Zeigen auf **Interaktive Sitzung** eine QuickInfo mit den Unterphasen und einem Link zur Dokumentation angezeigt. Eine Beschreibung der Unterphasen und Informationen zur Verbesserung der Leistung jeder Phase finden Sie unter Diagnose von Benutzeranmeldeproblemen.

März 2018

- **Anwendungsinstanzprognose (Vorschaufunktion).** Dies ist das erste Überwachungsfeature, das auf der vorhersagenden Analyse basiert. Prognosen zu Mustern bei der Ressourcennutzung

sind für Administratoren von Bedeutung, um Ressourcen und die erforderliche Anzahl von Lizenzen für jede Ressource festzulegen. Die Anwendungsinstanzprognose gibt an, wie viele gehostete Anwendungsinstanzen voraussichtlich im Laufe der Zeit pro Site oder Bereitstellungsgruppe gestartet werden. Die Prognose wird über selbstlernende Algorithmen berechnet, deren Datenmodelle auf vorhandenen Verlaufsdaten basieren. Der Toleranzbereich gibt die Prognosequalität an.

Weitere Informationen finden Sie im Kapitel "Director"unter Anwendungsinstanzprognose. Posten Sie Feedback zu Nutzen und Benutzerfreundlichkeit dieses Features im Citrix Cloud-Diskussionsforum.

- **Bereitstellungsgruppen-APIs (Preview)**

  Die Preview zu Bereitstellungsgruppen-APIs umfasst eine Reihe von REST-APIs, mit denen Sie die Verwaltung von Bereitstellungsgruppen automatisieren können. Das vollständige Angebot verfügbarer APIs kann in der Citrix Cloud API-Dokumentation unter https://developer.cloud.com/ angezeigt und getestet werden.

- **Web Studio-Authentifizierung**

  Die Service-Verwaltungskonsole in Citrix Cloud verwendet jetzt einen Bearertoken zur Authentifizierung von Kunden. Der Bearertoken wird benötigt, um den Zugriff auf die REST-API der Bereitstellungsgruppen zu authentifizieren.

- **Zugriff auf Überwachungsdienstdaten mit Version 4 der OData-API(Vorschaufunktion)**

  Sie können mit dem OData V.4-Endpunkt eigene Dashboards zur Überwachung und Berichterstellung auf Basis der Daten des Überwachungsdiensts erstellen. Version 4 von OData basiert auf der ASP.NET-Web-API und unterstützt Aggregationsabfragen. Verwenden Sie Ihren Citrix Cloud-Benutzernamen und den Bearertoken, um auf die Daten mit dem V4-Endpunkt zuzugreifen. Weitere Informationen und Beispiele finden Sie unter Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

  Hinterlassen Sie Feedback zum Nutzen dieses Features im Citrix Cloud-Diskussionsforum.

Fixes

- Sie können Anwendungsordner umbenennen, verschieben und löschen. [#STUD-2376]

Januar 2018

- **Prüfung auf RDS-Lizenz.** Beim Erstellen von Maschinenkatalogen mit Windows-Serverbetriebssystemmasc
  erfolgt jetzt eine automatische RDS-Lizenzprüfung. Jegliche RDS-Lizenzprobleme werden angezeigt, damit Sie geeignete Maßnahmen ergreifen können, um eine Serviceunterbrechung zu vermeiden. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

- **Zugriff auf die Maschinenkonsole über die Überwachung.** Über den Bereich "Maschinendetails"in der Überwachung ist jetzt Zugriff auf die Konsolen von Maschinen möglich, die auf dem XenServer Hypervisor Version 7.3 gehostet werden. Sie können Probleme in VDAs jetzt direkt von der Überwachung aus beheben. Weitere Informationen finden Sie im Abschnitt Zugriff auf Maschinenkonsolen unter "Problembehandlung bei Maschinen".

Dezember 2017

Neue und erweiterte Features

- **Citrix Workspace.** Citrix Workspace steht jetzt für **neue** XenApp und XenDesktop Service-Kunden zur Verfügung. Weitere Informationen finden Sie unter Workspacekonfiguration.
- **Anwendungsanalyse.** Sie können die Leistung von Anwendungen jetzt in Director über die neue Seite "Application Analytics", die über die Registerkarte **Überwachung** > **Anwendungen** aufgerufen wird, effizient analysieren und überwachen. Die Seite bietet eine konsolidierte Übersicht über Integrität und Nutzung aller in Ihrer Site veröffentlichten Anwendungen. Die Ansicht enthält die Zahl der Instanzen pro Anwendung und ähnliche Kennzahlen sowie Informationen zu Fehlern bei veröffentlichten Anwendungen. Dieses Feature erfordert VDAs der Version 7.15 oder höher.

  Weitere Informationen finden Sie unter Anwendungsanalyse in dem Artikel zur Überwachung.

November 2017

Neue und erweiterte Features

- **Lokaler Hostcache.** Der lokale Hostcache ermöglicht das fortgesetzte Verbindungsbrokering, wenn ein Cloud Connector an einem Ressourcenstandort nicht mit Citrix Cloud kommunizieren kann. Weitere Informationen finden Sie unter Lokaler Hostcache.
- **Azure Managed Disks.** Azure Managed Disks werden jetzt standardmäßig für mit MCS bereitgestellte VMs in Azure Resource Manager-Umgebungen verwendet. Optional können Sie herkömmliche Speicherkonten verwenden. Weitere Informationen finden Sie unter Microsoft Azure Resource Manager-Virtualisierungsumgebungen.
- **Helpdeskadministrator:** Bei der Verwaltung von Service-Administratoren für ein Citrix Cloud-Kundenkonto gibt es jetzt die neue Option "Helpdeskadministrator". Ein Helpdeskadministrator kann auf die Überwachungsfunktionen des Service zugreifen. Weitere Informationen finden Sie unter Verwalten.

Fixes

- Sie können jetzt mit dem Assistenten der Service-Verwaltungskonsole Remote-PC-Zugriff-Maschinenkataloge erstellen. In früheren Versionen musste hierfür ein PowerShell-Cmdlet verwendet werden (siehe CTX220737). Anschließend musste eine Bereitstellungsgruppe über die Verwaltungskonsole erstellt werden. Jetzt können Sie Katalog und Bereitstellungsgruppe nacheinander über die Verwaltungskonsole erstellen.
- Für mit MCS erstellte Kataloge können bestehende Active Directory-Maschinenkonten verwendet werden. [#DNA-24566]
- Wenn Sie beim Überwachen einer Bereitstellung in einer sortierten **Trends > Sitzungen**-Tabelle scrollen, werden die exakten Ergebnisse angezeigt. [DNA-51257]

Weitere Informationen

- Bekannte Probleme.
- Informationen zu Drittanbietersoftware, die im Service enthalten ist, finden Sie unter Hinweise zu Drittanbietern.

Bekannte Probleme

May 17, 2024

Bei Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) bestehen die folgenden bekannten Probleme:

- In einer auf AWS gehosteten VMware-Umgebung schlägt die Erstellung des MCS-Maschinenkatalogs fehl, wenn das Masterimage vTPM-aktiviert ist. Informationen zum VMware-Support finden Sie unter Get Support. [PMCS-37603]
- Überwachungsbildschirme werden möglicherweise nicht geladen, wenn die Pendo-URL `https://citrix-cloud-content.customer.pendo.io/` gesperrt ist. [DIR-18482]
- Sie erhalten eine Fehlermeldung, wenn Sie einen Befehl mit `XDHyp:\` im Remote PowerShell SDK ausführen. Lösen des Problems:

  1. Führen Sie einen Befehl mit `Hyp` aus. Beispiel: `Get-HypServiceStatus`
  2. Führen Sie einen Befehl mit `XDHyp:\` aus. Beispiel: `Get-ChildItem XDHyp:\Connections\`

  [BRK-13723]

- Nach Änderungen an der Citrix DaaS-Architektur in Version 2209 wurden die Standardsymbole für Windows-Desktops und für Anwendungen, die vor diesem Release bereitgestellt werden, in generische PC-Desktopsymbole geändert. Diese Änderung gilt nur für Desktops und Anwendungen, die auf das Standardsymbol verweisen. Um Symbole zurück zum Standardsymbol der Windows-Anwendung zu ändern, führen Sie das folgende Skript mit dem Remote PowerShell SDK aus:
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- Der Versuch, den Betriebssystemtyp für Azure-Kataloge unter **Verwalten > Vollständige Konfiguration** zu ändern, schlägt fehl und es wird eine Fehlermeldung angezeigt. Die Änderung des Betriebssystemtyps für Azure-Kataloge wird nicht mehr unterstützt, auch nicht mit PowerShell. [STUD-19819]
- Werden in einer Microsoft Azure-Umgebung der kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A gleichzeitig aktiviert, kann kein Maschinenkatalog erstellt werden. Bestehende Maschinenkataloge können Sie jedoch weiterhin aktualisieren und löschen und ihnen VMs hinzufügen bzw. VMs aus ihnen löschen. [PMCS-21698]
- Das Dropdown-Pfeilsymbol für die Schaltflächen "Durchschnittliche IOPS", "Sitzungssteuerung"und "Energieverwaltung"wird auf den Seiten **Benutzerdetails** und **Maschinendetails** möglicherweise nicht angezeigt. Die Funktion funktioniert jedoch einwandfrei. Um alle Elemente im Menü anzuzeigen, klicken Sie auf eine beliebige Stelle der Schaltfläche. [DIR-11875]
- Wenn Sie Azure AD-Domänendienste verwenden: Anmelde-UPNs für Workspace oder StoreFront müssen den Domänennamen enthalten, der beim Aktivieren der Azure AD-Domänendienste angegeben wurde. Anmeldungen können keine UPNs einer benutzerdefinierten, von Ihnen erstellten Domäne verwenden, selbst wenn diese benutzerdefinierte Domäne als primär gekennzeichnet ist.
- Wenn Sie bei einer Bereitstellung in Azure einen MCS-Katalog ab Version 7.9 mit aktiviertem Zurückschreibcache erstellen und auf dem Masterimage ein VDA 1811 oder früher installiert ist, tritt ein Fehler auf. Außerdem können Sie nichts in Bezug auf Personal vDisk für Microsoft Azure erstellen. Wählen Sie als Workaround eine andere Katalogversion für die Bereitstellung in Azure oder deaktivieren Sie den Zurückschreibcache. Um den Zurückschreibcache beim Erstellen eines Katalogs zu deaktivieren, wählen Sie auf der Seite **Maschinen** die Kontrollkästchen **Dem Cache zugewiesener Speicher** und **Größe des Datenträgercache** ab.
- Der Link **Konsole** unter **Überwachen > Maschinendetails** startet in Microsoft Edge 44 und Firefox ESR 68 nicht die Maschinenkonsole. [DIR-8160]
- Wenn Sie versuchen, die Neustart-Option in Workspace App für Web oder Desktop zu verwenden, wird das Neustart-Dialogfeld nicht wieder geschlossen und es wird kein Erfolg gemeldet.

Der Hypervisor zeigt an, dass die Maschine heruntergefahren aber nicht wieder gestartet wurde. Schließen Sie als Workaround nach einiger Zeit das Neustart-Dialogfeld und starten Sie den Desktop. Dieser wird zwangsweise gestartet. [BRK-5564]

Informationen zu Problemen mit aktuellen VDAs finden Sie unter Bekannte Probleme.

Einstellung von Features und Plattformen

March 6, 2024

Dieser Artikel bietet frühzeitige Informationen über Features von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service), die ausgemustert werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element. Informationen zum Produktlebenszyklussupport finden Sie unter Product Lifecycle Support Policy.

> **Hinweis:**
>
> Informationen zur Einstellung von Features und Plattformen bei Citrix Virtual Apps and Desktops sind in einem gesonderten Artikel unter Einstellung von Features und Plattformen enthalten.

Veraltete und entfernte Produkte und Features

Die in der folgenden Liste aufgeführten Features von Citrix DaaS sind veraltet oder wurden entfernt:

Veraltete Elemente werden nicht sofort entfernt. Citrix setzt den Support fort, aber die Elemente werden in einem zukünftigen Release entfernt.

Entfernte Elemente wurden entfernt oder werden in Citrix DaaS nicht mehr unterstützt. Datumsangaben in **Fettdruck** kennzeichnen die neuesten Updates.

Element	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Unterstützung für die Konfiguration des Zurückschreibcache, sodass er nur einen Datenträgercache und keinen Speichercache enthält	Februar 2024		Verwenden Sie die Konfigurationsoption für die Größe des Speichercaches und geben Sie eine Größe ungleich Null an.
Unterstützung für Azure-Kataloge, die vor der Funktion zur bedarfsgesteuerten Bereitstellung erstellt wurden (“ältere” Kataloge)	Februar 2024		Erstellen Sie ältere Azure-Katalog-VMs neu. Die Kataloge werden nach Bedarf bereitgestellt und helfen, Speicherkosten zu sparen.
Unterstützung für Citrix Connector 3.1 für System Center Configuration Manager	Dezember 2023		Führen Sie das Image- oder Anwendungsupdate manuell durch.
Unterstützung für die Verwendung eines Masterimages in einer anderen Region als der Region, in der der Katalog erstellt wurde	Dezember 2023		Verwenden Sie Azure Compute Gallery, um das Masterimage in die gewünschte Region zu replizieren.
Unterstützung für AWS-Volumeworker	November 2023		Verwenden Sie den direkten Disk-Upload und -Download. Siehe Direkter Disk-Upload und -Download.
Unterstützung für `Leave user management to Citrix Cloud` bei der Erstellung von Bereitstellungsgruppen	September 2023	September 2023	

Element	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Unterstützung für die Verwendung von `AwsCaptureInstanceProperties` in AWS-Umgebungen	August 2023		Verwenden Sie ein Maschinenprofil. Siehe Katalog mithilfe eines Maschinenprofils erstellen.
Unterstützung für VMware vSphere 6.7		Juni 2023	Verwenden Sie höhere Versionen für VMware vSphere.
PowerShell-Befehl `Schedule-ProvVMUpdate`	April 2023		Verwenden Sie den Befehl `Set-ProvVMUpdateTimeWindow`.
PowerShell-Befehl `Request-ProvVMUpdate`	April 2023		Verwenden Sie den Befehl `Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1`.
PowerShell-Befehl `Cancel-ProvVMUpdate`	April 2023		Verwenden Sie den Befehl `Clear-ProvVMUpdateTimeWindow`.
Parameter `DedicatedTenancy`, verwendet im Befehl `New-ProvScheme`	März 2023		Verwenden Sie den Parameter `TenancyType`.
Nicht verwalteter Datenträger zum Erstellen einer VM in der Azure-Umgebung	Juni 2022		

Element	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Unterstützung für vier AWS-spezifische Befehle: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` und `Grant-HypSecurityGroupIngress`	May 2022		
Parameter `StorageAccountType` in Azure-Umgebungen	April 2022		Verwenden Sie `StorageType`.
Legacy-Konsole (MMC-basierte Konsole)	Juli 2021	November 2021	Verwenden Sie **Verwalten > Vollständige Konfiguration**, um auf das gesamte Spektrum der Konfigurations- und Verwaltungsaktionen zuzugreifen.
Azure Quick Deploy	September 2020		Verwenden Sie Quick Deploy.

Element	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Importieren von Citrix Provisioning-Zielgeräten, um Kataloge in Citrix Studio zu erstellen.	August 2020	Februar 2021	Verwenden Sie den Citrix Provisioning-Assistenten zum Exportieren von Geräten, um Citrix Provisioning-VMs zur Katalogerstellung an Delivery Controller/MCS zu übergeben. Siehe Assistent zum Exportieren von Geräten.

Systemanforderungen

June 12, 2024

Einführung

Nicht in diesem Dokument aufgeführte Systemanforderungen (z. B. Citrix Workspace-App und Citrix Provisioning) werden in der jeweiligen Dokumentation beschrieben.

Spezifische Empfehlungen für die Dimensionierung von VMs, die Desktops und Anwendungen bereitstellen, können aufgrund der Komplexität und Dynamik des Hardwareangebots nicht gegeben werden. Jede Bereitstellung hat individuelle Anforderungen. Im Allgemeinen werden VMs auf der Basis der Hardware und nicht der Benutzerarbeitslasten dimensioniert. Ausnahme bildet der RAM, der größer sein muss, wenn RAM-intensive Anwendungen verwendet werden. Aktuelle Informationen zur VDA-Dimensionierung finden Sie in der Citrix Tech Zone.

> **Wichtig:**
>
> Die in diesem Artikel aufgeführten VDA-Versionen unterliegen dem Citrix Produktlebenszyklus. Weitere Informationen finden Sie in der Produktmatrix auf der Citrix Website.

> Informationen zur Verwendung von LTSR-VDAs mit Citrix DaaS finden Sie unter CTX205549.

Nicht vergessen: In einer Bereitstellung von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) müssen Sie die Kernkomponenten (Delivery Controller, Sitedatenbank, Verwaltungs-/Überwachungskonsolen) nicht installieren oder verwalten. Informationen zur Installation von Virtual Delivery Agents finden Sie unter:

- VDAs installieren
- Installieren von VDAs über die Befehlszeile.

Cloud Connectors

Details siehe Technische Daten zu Citrix Cloud Connector.

VDAs in Azure-Umgebungen

Unterstützte Betriebssysteme:

- Windows 11 (Multisitzungs-OS)
- Windows 11 (Einzelsitzungs-OS)
- Windows 10 (Multisitzungs-OS)
- Windows 10 (Einzelsitzungs-OS)
- Windows Server 2022 (erfordert mindestens VDA 2106)
- Windows Server 2019
- Windows Server 2016

Alle VDAs, die das Ende ihrer Lebensdauer noch nicht erreicht haben, werden für die Verwendung mit Citrix DaaS unterstützt. Citrix empfiehlt, LTSR-VDAs mit dem neuesten kumulativen Update zu verwenden. Weitere Informationen zum Lebenszyklus von VDAs finden Sie in der Citrix Produktmatrix.

Windows Server 2012 R2 wird nur mit VDA 1912 (und höhere CUs) unterstützt.

Windows Server erfordert Microsoft RDS-Lizenzierung.

Informationen zu Azure Virtual Desktop finden Sie in der Microsoft-Dokumentation.

VDA für Einzelsitzungs-OS

Die folgenden Informationen gelten für das neueste VDA-Release.

Unterstützte Betriebssysteme:

- Windows 11

- Windows 10
  - Informationen zur Unterstützung von Editionen finden Sie unter CTX224843. Dieser Artikel enthält auch Links zu bekannten Citrix Problemen mit den unterstützten Windows-Versionen.
  - Desktopgestaltungsumleitung und Legacy-Grafikmodus werden unter Windows 10 nicht unterstützt.

Anforderungen:

- Microsoft .NET Framework 4.8 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Wenn die Maschine eine frühere Version dieser Laufzeit enthält (z. B. 2015–2017), wird diese vom Citrix Installationsprogramm aktualisiert.
  - Wenn die Maschine eine Version vor 2015 enthält, installiert Citrix die neuere Version parallel.

Remote-PC-Zugriff verwendet diesen VDA, den Sie auf physischen Büro-PCs installieren. Dieser VDA unterstützt den sicheren Start für Citrix Virtual Desktops-Remote-PC-Zugriff.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, wird die Multimediabeschleunigung nicht installiert und funktioniert nicht. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine. Andernfalls können sich die Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows-Desktopbetriebssystemen ist Media Foundation bereits installiert und kann nicht entfernt werden. N-Editionen enthalten jedoch einige medienbezogene Technologien nicht. Sie können diese Software von Microsoft oder einem Drittanbieter beziehen.

Weitere Informationen:

- Informationen zum Linux VDA finden Sie in der Dokumentation zum Linux Virtual Delivery Agent.
- Zur Verwendung des Server-VDI-Features können Sie über die Befehlszeilenschnittstelle einen Einzelsitzungs-VDA auf einer unterstützten Windows-Maschine installieren. Weitere Informationen finden Sie im Artikel Server-VDI.
- Informationen zum Installieren eines VDA auf einer Maschine mit älterer Windows-Version finden Sie unter Ältere Betriebssysteme.
- Siehe auch VDAs in einer Azure Virtual Desktop-Umgebung.

VDA für Multisitzungs-OS

Die folgenden Informationen gelten für das neueste VDA-Release.

Unterstützte Betriebssysteme:

- Windows Server 2022 (erfordert mindestens VDA 2106)
- Windows Server 2019, Standard und Datacenter Edition
- Windows Server 2016, Standard und Datacenter Edition
- Windows 11
- Windows 10 (64-Bit), alle unterstützten Versionen

Das Installationsprogramm stellt automatisch die folgenden Anforderungen bereit:

- Microsoft .NET Framework 4.8 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Wenn die Maschine eine frühere Version dieser Laufzeit enthält (z. B. 2015–2017), wird diese vom Citrix Installationsprogramm aktualisiert.
  - Wenn die Maschine eine Version vor 2015 enthält, installiert Citrix die neuere Version parallel.

Das Installationsprogramm installiert und aktiviert automatisch die Rollendienste für Remotedesktopdienste, wenn sie nicht bereits installiert und aktiviert sind. Dies löst einen Neustart aus.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, wird die Multimediabeschleunigung nicht installiert und funktioniert nicht. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine. Andernfalls können sich die Benutzer nicht an der Maschine anmelden. Bei den meisten Windows Server-Versionen wird das Media Foundation-Feature über den Server-Manager installiert. N-Editionen enthalten jedoch einige medienbezogene Technologien nicht. Sie können diese Software von Microsoft oder einem Drittanbieter beziehen.

Wenn Media Foundation nicht auf dem VDA vorhanden ist, funktionieren diese Multimediafeatures nicht:

- Flash-Umleitung
- Windows Media-Umleitung
- HTML5-Videoumleitung
- HDX RealTime-Webcamumleitung

Weitere Informationen:

- Informationen über den Linux VDA finden Sie in den Artikeln zu Linux Virtual Delivery Agent.
- Informationen zum Installieren eines VDAs auf einem nicht mehr unterstützten Windows-Betriebssystem finden Sie unter Ältere Betriebssysteme.
- Siehe auch VDAs in einer Azure Virtual Desktop-Umgebung.

Hosts/Virtualisierungsressourcen

Die folgenden Host-/Virtualisierungsressourcen (alphabetisch aufgeführt) werden unterstützt. Wo zutreffend werden die folgenden *major.minor* Versionen unterstützt, einschließlich von Updates für diese Versionen. CTX131239 enthält aktuelle Hypervisorversionsinformationen sowie Links zu bekannten Problemen.

- **Amazon Web Services (AWS)**
  - Sie können Anwendungen und Desktops auf unterstützten Windows Server-Betriebssystemen bereitstellen.
  - Amazon Relational Database Service (RDS) wird nicht unterstützt.

  Weitere Informationen finden Sie unter AWS-Umgebungen.
- **XenServer (ehemals Citrix Hypervisor)**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter XenServer-Virtualisierungsumgebungen.
- **Google Cloud Platform**

  Weitere Informationen finden Sie unter Google Cloud-Umgebungen und Erste Schritte mit Citrix DaaS in Google Cloud.
- **HPE Moonshot**

  Weitere Informationen finden Sie unter HPE Moonshot Virtualisierungsumgebungen.
- **Microsoft Azure Resource Manager**

  Weitere Informationen finden Sie im Artikel Microsoft Azure Resource Manager-Cloudumgebungen.
- **Microsoft System Center Virtual Machine Manager**

  Enthält alle Versionen von Hyper-V, die mit den unterstützten Versionen von System Center Virtual Machine Manager registriert werden können.

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen.

- **Nutanix Acropolis**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter Nutanix-Virtualisierungsumgebungen.

- **VMware Cloud auf AWS**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter VMware-Cloud auf Amazon Web Services (AWS)

- **Azure VMware-Lösung (AVS)**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter Integration von Azure VMware Solution (AVS)

- **Google Cloud VMware Engine**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter Google Cloud VMware Engine.

- **VMware vSphere(vCenter + ESXi)**

  Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter VMware-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie dürfen die VDA-Software nicht auf einem Citrix DDC- oder StoreFront-Server installieren. Der VDA muss ein eigenständiges System sein. Die Installation mehrerer Komponenten auf einer einzelnen VM ist nur im Rahmen einer Machbarkeitsstudie zulässig, oder wenn Sie die Studio-Verwaltungskonsole nur für Administratoren veröffentlichen. In diesem Fall müssen Sie sicherstellen, dass Benutzer ohne Administratorrechte keinen Zugriff auf DDC/StoreFront-VMs haben.

Funktionsebenen von Active Directory

Die folgenden Funktionsebenen werden für Active Directory-Gesamtstrukturen und -Domänen unterstützt:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

Weitere Informationen zu Active Directory finden Sie unter In Active Directory eingebunden.

HDX-Technologien

Informationen zu Unterstützung und Anforderungen für HDX finden Sie unter HDX.

Universeller Druckserver

Der universelle Druckserver umfasst Client- und Serverkomponenten. Die UpsClient-Komponente ist in der VDA-Installation enthalten. Die UpsServer-Komponente wird auf jedem Druckserver installiert, auf dem die freigegebenen Drucker gespeichert sind, die Sie mit dem universellen Druckertreiber von Citrix in Benutzersitzungen bereitstellen möchten.

Die UpsServer-Komponente wird unter folgenden Betriebssystemen unterstützt:

- Windows Server 2019
- Windows Server 2016

Anforderungen:

- Microsoft .NET Framework 4.8 (Mindestversion)
- Microsoft Visual C++ 2015-2022 Redistributable.
  - Wenn die Maschine eine frühere Version dieser Laufzeit enthält (z. B. 2015–2017), wird diese vom Citrix Installationsprogramm aktualisiert.
  - Wenn die Maschine eine Version vor 2015 enthält, installiert Citrix die neuere Version parallel.

Für Multisitzungs-OS-VDAs erfordert die Benutzerauthentifizierung bei Druckvorgängen, dass der universelle Druckserver in der gleichen Domäne ist wie der VDA.

Auch eigenständige Client- und Server-Komponentenpakete stehen zum Download zur Verfügung.

Weitere Informationen finden Sie unter Bereitstellen von Druckern.

Servicekonnektivität

Informationen zur Internetverbindung finden Sie unter Anforderungen an System und Konnektivität. Diese Informationen umfassen Anforderungen, die für die meisten Citrix Cloud-Dienste gelten, sowie spezifische Anforderungen von Citrix DaaS.

Sonstiges

- Die Microsoft-Gruppenrichtlinien-Verwaltungskonsole (GPMC) ist erforderlich, wenn Sie Citrix Richtlinieninformationen in Active Directory und nicht in der Sitekonfigurationsdatenbank spe-

ichern. Auf der Maschine, auf der Sie `CitrixGroupPolicyManagement_x64.msi` installieren, muss Visual Studio 2015 Runtime installiert sein. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

- Dieses Produkt unterstützt die PowerShell-Versionen 3 bis 5.
- Für Produktkomponenten und Features, die Sie auf Windows-Servern installieren können, werden Server Core- und Nano Server-Installationen nicht unterstützt, es sei denn, dies wird ausdrücklich erwähnt.
- Weitere Informationen zu Ressourcenlimits in einer Bereitstellung finden Sie unter Limits.
- Informationen zu unterstützten StoreFront-Versionen finden Sie unter StoreFront-Systemanforderungen.
- Informationen zur Globalisierung finden Sie unter CTX119253.
- Informationen zu den von Citrix DaaS verwendeten Ports finden Sie unter Von Citrix-Technologien verwendete Kommunikationsports.
- Informationen zu den Anforderungen bei Verwendung der Quick Deploy-Verwaltungsschnittstelle finden Sie unter Anforderungen.

Limits

June 12, 2024

Die Werte in diesem Artikel beziehen sich auf eine einzelne Instanz von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Diese Limits wurden von Citrix gründlich getestet und werden für ein optimales Endbenutzer- und Administratorerlebnis empfohlen. Es handelt sich um “weiche Limits” , die nicht technisch durchgesetzt werden (mit Ausnahme der Gesamtzahl der VDAs pro Ressourcenstandort). Wenn die Anzahl gleichzeitiger Benutzer 125,000 überschreitet, kann Citrix mehrere Citrix DaaS-Instanzen kombinieren, um ein einheitliches Erlebnis für jede Größenordnung zu bieten.

Die Angaben in diesem Artikel sind dynamisch. Schauen Sie regelmäßig nach aktuellen Informationen. Wenn Sie aktuelle Anforderungen haben, die hier nicht erfasst sind, wenden Sie sich so bald wie möglich an Ihren Citrix-Mitarbeiter, um weitere Unterstützung zu erhalten.

Konfigurationslimits

Wenn Richtlinien das Limit überschreiten, empfiehlt Citrix die Verwendung von Workspace Environment Management Service oder Active Directory-Gruppenrichtlinienobjekten.

Ressource	Einschränkung
Active Directory-Domänen	100
Anwendungsordner	1.000
Anwendungsgruppen	250
Anwendungen	5.000
Kataloge	2.000
Bereitstellungsgruppen	2.000
Hostverbindungen	200
Ressourcenstandorte	100
Richtlinien für Verwaltungskonsole (vollständige Konfiguration)	200
Tags	10.000
VDAs	100.000

Limits für Ressourcenstandorte

Die folgende Tabelle enthält die Limits für Ressourcen auf Ressourcenstandortebene.

Wenn Ihre Anforderungen diese Limits überschreiten, empfiehlt Citrix die Verwendung zusätzlicher Ressourcenstandorte.

Ressource	Einschränkung
Gesamtzahl der VDAs (festes Limit)	10.000
Sitzungen insgesamt	25.000
Active Directory-Domänen	1
Hostverbindungen	40

Citrix Cloud Connectors werden Ressourcenstandorten zugewiesen und verknüpfen Workloads mit Citrix DaaS. Informationen zu Cloud Connector-Limits finden Sie unter Überlegungen zur Skalierung und Größe für Cloud Connectors.

Provisioning-Limits

Die Provisioning-Limits in der folgenden Tabelle sind die von Citrix empfohlenen Maximalwerte für ein Abonnement eines öffentlichen Anbieters.

Die Quotengrenzen Ihres Cloudanbieters sind wahrscheinlich niedriger. Wenden Sie sich in diesem Fall an den Anbieter, um Ihr Abonnementkontingent zu erhöhen. Für größere Bereitstellungen empfiehlt Citrix ein Hub and Spoke-Modell, bei dem VDAs über mehrere Abonnements und Hostverbindungen verteilt sind.

Weitere Informationen finden Sie in den folgenden Referenzarchitekturen:

- Citrix DaaS auf AWS
- Citrix Virtualisierung in Google Cloud
- Citrix DaaS auf Azure

Ressource	Einschränkung
VDAs pro Amazon Web Services-Konto pro Region	3.000
VDAs pro Google Cloud Platform-Projekt	3.000
VDAs pro Microsoft Azure-Abonnement und Region	5.000

> **Hinweis:**
>
> Die Grenzwerte sind Empfehlungen von Citrix.

Nutzungslimits

Informationen zu Administratorrollen und deren Unterschieden finden Sie unter:

- Administratoren für Verwaltung (vollständige Konfiguration)
- Administratoren für die Überwachung (Director)

Ressource	Einschränkung
Gleichzeitige Volladministratoren für die Überwachung (Director)	40
Gleichzeitige Helpdeskadministratoren für die Überwachung (Director)	200

Ressource	Einschränkung
Gleichzeitige Sitzungsadministratoren für die Überwachung (Director)	50
Gleichzeitige Cloudadministratoren für Verwaltung (vollständige Konfiguration)	100
Gleichzeitige Helpdeskadministratoren für Verwaltung (vollständige Konfiguration)	60
Gleichzeitige Endbenutzer	125.000
Für einen Benutzer veröffentlichte Ressourcen	250
Sitzungsstarts pro Minute	3.000

- Überwachen (Director) unterstützt die Aggregation von bis zu vier Citrix DaaS-Mandanten (Spokes) unter einem einzigen Mandanten (Hub).
- Ein Helpdesk-Administrator auf der Hub-Instanz kann Benutzer, Maschinen, Endpunkte und Transaktionen von allen aggregierten Instanzen (Hub und Spokes) gemäß der Konfiguration der delegierten Administration auf der jeweiligen Instanz überwachen und Fehler beheben.
- Die Anzahl der gleichzeitigen Administratoren pro Citrix DaaS-Instanz entspricht dem Wert in der Tabelle zu Nutzungslimits.

Grenzwert-Änderungsprotokoll

Die folgende Tabelle enthält Informationen zu den geänderten Konfigurationslimits:

Datum	Ressource	Beschreibung
22 Nov 2023	Active Directory-Domänen	Das Limit wurde von 85 auf 100 erhöht.
	Kataloge	Das Limit wurde von 1000 auf 2000 erhöht.
	Bereitstellungsgruppen	Das Limit wurde von 1000 auf 2000 erhöht.
	Ressourcenstandorte	Das Limit wurde von 85 auf 100 erhöht.
	Ressourcenstandort -> Sitzungen insgesamt	Das Limit wurde von 20.000 auf 25.000 erhöht.
07 Dec 2023	Provisioninglimits -> VDAs pro Microsoft Azure-Abonnement und Region	Das Limit wurde von 2500 auf 5000 erhöht.

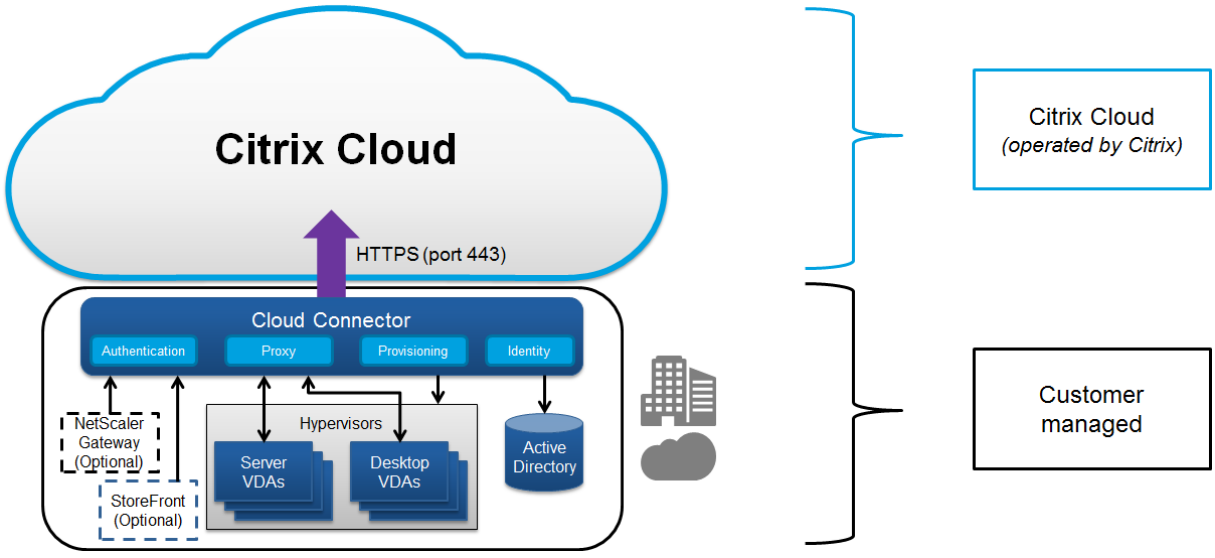
Technische Sicherheit

May 17, 2024

Sicherheitsüberblick

Dieses Dokument gilt für Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) mit Hosting in Citrix Cloud. Diese Informationen umfassen Citrix Virtual Apps Essentials und Citrix Virtual Desktops Essentials.

Citrix Cloud verwaltet den Betrieb der Steuerungsebene von Citrix DaaS-Umgebungen. Zur Steuerungsebene gehören die Delivery Controller, die Verwaltungskonsolen, die SQL-Datenbank, der Lizenzserver sowie optional StoreFront und Citrix Gateway (ehemals NetScaler Gateway). Die Virtual Delivery Agents (VDAs), auf denen die Apps und Desktops gehostet werden, bleiben unter der Kontrolle des Kunden in einem entweder in eigenen Datencenter oder in der Cloud angesiedelten Datencenter seiner Wahl. Diese Komponenten sind über einen Agent ("Citrix Cloud Connector") mit dem Cloud-Service verbunden. Kunden, die Citrix Workspace verwenden, können auch den Citrix Gateway Service verwenden, anstatt Citrix Gateway im eigenen Datencenter auszuführen. Das folgende Diagramm zeigt Citrix DaaS und seine Sicherheitsgrenzen.



Citrix Cloud und Compliance

Stand Januar 2021: Die Verwendung von Citrix Managed Azure-Kapazität mit verschiedenen Citrix DaaS-Editionen und Workspace Premium Plus wurde noch nicht gemäß Citrix SOC 2 (Typ 1 oder 2), ISO 27001, HIPAA oder anderen Cloud-Compliance-Anforderungen bewertet. Im Citrix Trust Center

finden Sie weitere Informationen zu Citrix Cloud-Zertifizierungen sowie regelmäßig aktualisierte Nachrichten.

Datenfluss

Die VDAs werden nicht von Citrix DaaS gehostet, das Hosting der für das Provisioning erforderlichen Anwendungsdaten und Images erfolgt daher immer in der Einrichtung des Kunden. Die Steuerungsebene hat Zugriff auf Metadaten wie Benutzernamen, Maschinennamen und Anwendungsverknüpfungen, wodurch der Zugriff auf das geistige Eigentum des Kunden von der Steuerungsebene aus eingeschränkt wird.

Die Übertragung von Daten zwischen Cloud und Kundenstandort erfolgt über eine sichere TLS-Verbindung über Port 443.

Datenisolierung

In Citrix DaaS werden nur Metadaten gespeichert, die für die Vermittlung und Überwachung der Anwendungen und Desktops benötigt werden. Vertrauliche Informationen wie Images, Benutzerprofile und andere Anwendungsdaten verbleiben am Kundenstandort bzw. in einer von diesem bei einem öffentlichen Anbieter abonnierten Cloud.

Serviceeditionen

Die Funktionalität von Citrix DaaS variiert je nach Edition. Citrix Virtual Apps Essentials unterstützt beispielsweise nur den Citrix Gateway-Service und Citrix Workspace. Die Produktdokumentation enthält weitere Informationen über die unterstützten Funktionen.

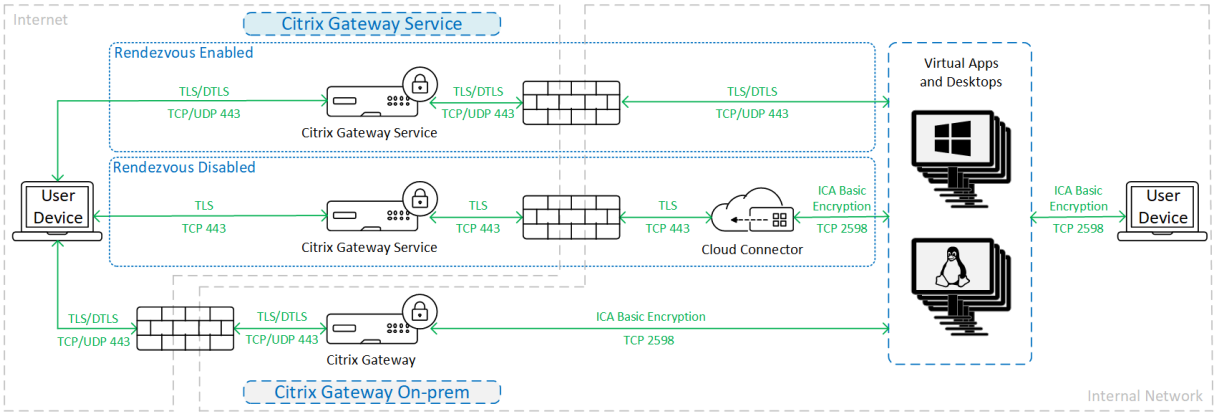
ICA-Sicherheit

Citrix DaaS bietet mehrere Optionen zum Sichern des ICA-Datenverkehrs während der Übertragung. Es stehen folgende Optionen zur Verfügung:

- **Basic-Verschlüsselung:** Standardeinstellung.
- **SecureICA:** Ermöglicht das Verschlüsseln von Sitzungsdaten mit RC5-Verschlüsselung (128 Bit).
- **VDA TLS/DTLS:** Ermöglicht die Verwendung von Verschlüsselung auf Netzwerkebene mit TLS/DTLS.
- **Rendezvous-Protokoll:** Nur verfügbar, wenn Sie Citrix Gateway Service verwenden. Bei Verwendung des Rendezvous-Protokolls werden ICA-Sitzungen End-to-End mit TLS/DTLS verschlüsselt.

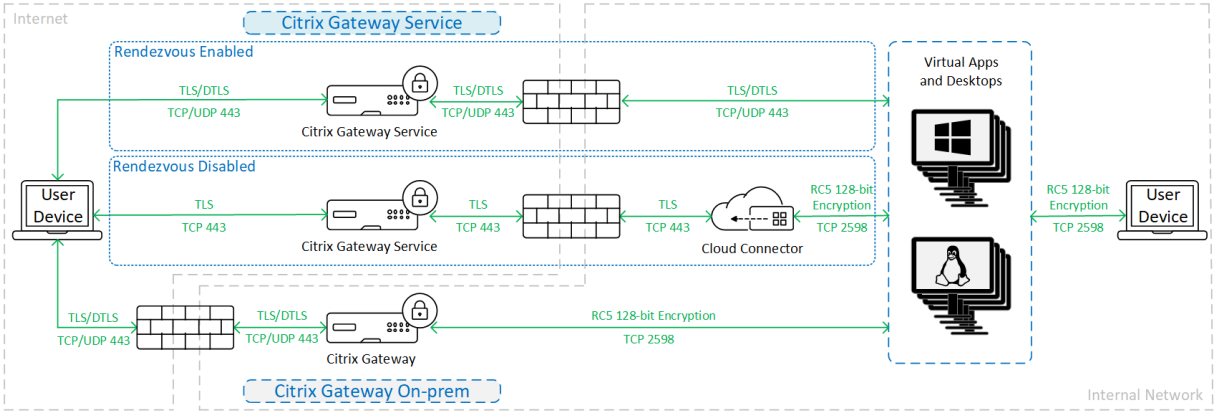
Basic-Verschlüsselung

Bei Verwendung der Basic-Verschlüsselung wird der Datenverkehr wie in der folgenden Grafik dargestellt verschlüsselt.



SecureICA

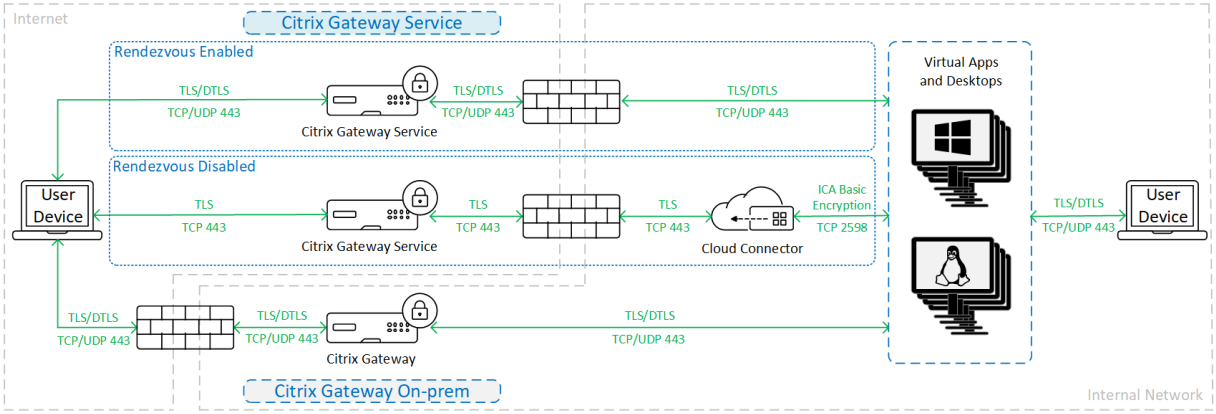
Bei Verwendung der SecureICA-Verschlüsselung wird der Datenverkehr wie in der folgenden Grafik dargestellt verschlüsselt.



> **Hinweis:**
>
> SecureICA wird bei Verwendung der Workspace-App für HTML5 nicht unterstützt.

VDA TLS/DTLS

Bei Verwendung der VDA TLS/DTLS-Verschlüsselung wird der Datenverkehr wie in der folgenden Grafik dargestellt verschlüsselt.



> **Hinweis:**
>
> Bei Verwendung von Gateway Service ohne Rendezvous wird der Datenverkehr zwischen dem VDA und dem Cloud Connector nicht mit TLS verschlüsselt, da der Cloud Connector die Verbindung zum VDA mit Verschlüsselung auf Netzwerkebene nicht unterstützt.

Weitere Ressourcen

Weitere Informationen zu den ICA-Sicherheitsoptionen und deren Konfiguration finden Sie unter:

- SecureICA: Einstellungen der Richtlinie “Sicherheit”
- VDA TLS/DTLS: Transport Layer Security
- Rendezvous-Protokoll: Rendezvous-Protokoll

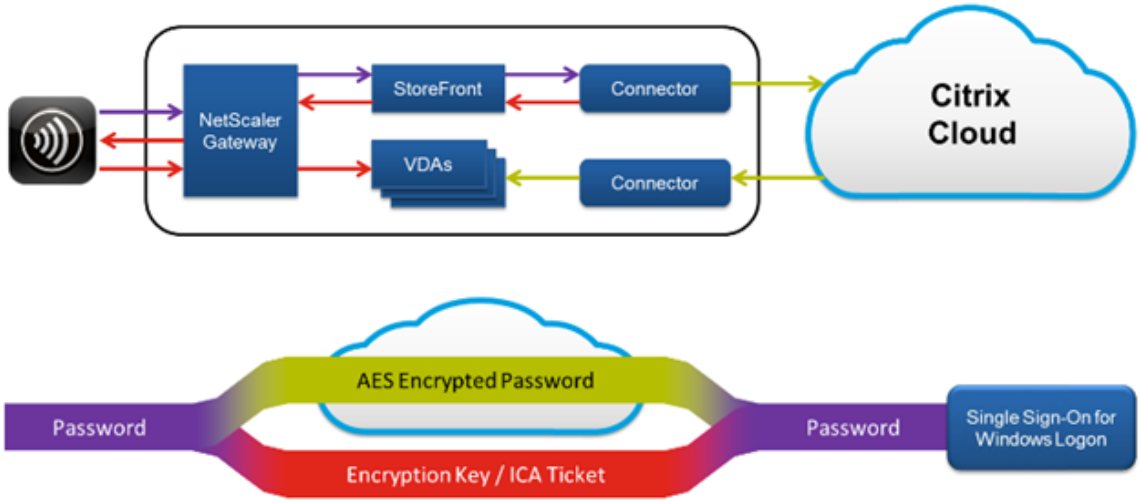
Handhabung von Anmeldeinformationen

Citrix DaaS verarbeitet vier Arten von Anmeldeinformationen:

- Benutzeranmeldeinformationen: Bei Einsatz einer vom Kunden verwalteten StoreFront werden die Benutzeranmeldeinformationen vom Citrix Cloud Connector mit AES-256 und einem zufälligen Einmalschlüssel, der für jeden Start generiert wird, verschlüsselt. Der Schlüssel wird nie in die Cloud übertragen, sondern nur an die Citrix Workspace-App zurückgegeben. Der Schlüssel wird dann von der Citrix Workspace-App zur Entschlüsselung des Benutzerkennworts beim Sitzungsstart für das Single Sign-On an den VDA übergeben. Der Ablauf wird in der folgenden Abbildung dargestellt.

  Standardmäßig werden Benutzeranmeldeinformationen nicht über nicht vertrauenswürdige Domänengrenzen weitergeleitet. Wenn ein VDA und StoreFront in einer Domäne installiert sind und ein Benutzer in einer anderen Domäne versucht, eine Verbindung zum VDA herzustellen, schlägt der Anmeldeversuch fehl, wenn keine Vertrauensstellung zwischen den Domänen hergestellt wurde. Mit dem DaaS PowerShell SDK können Sie dieses Verhalten deaktivieren

und die Weiterleitung von Anmeldeinformationen zwischen nicht vertrauenswürdigen Domänen zulassen. Weitere Informationen finden Sie unter Set-Brokersite.



- Administratoranmeldeinformationen: Administratoren authentifizieren sich über Citrix Cloud. Bei der Authentifizierung wird ein signiertes JSON Web Token (JWT) zur einmaligen Benutzung generiert, das dem Administrator Zugriff auf Citrix DaaS gewährt.
- Hypervisorkennwörter: Für On-Premises-Hypervisors, die ein Kennwort für die Authentifizierung benötigen, wird dieses vom Administrator erstellt und in verschlüsselter Form direkt in der SQL-Datenbank in der Cloud gespeichert. Peerschlüssel werden von Citrix verwaltet, um sicherzustellen, dass Hypervisoranmeldeinformationen nur authentifizierten Prozessen zur Verfügung stehen.
- Active Directory-Anmeldeinformationen: In Maschinenerstellungsdienste wird der Cloud Connector zum Erstellen von Maschinenkonten im AD des Kunden verwendet. Da das Maschinenkonto des Cloud Connectors nur Lesezugriff auf Active Directory hat, wird der Administrator für jede Maschinenerstellungs- und Maschinenlöschoperation zur Eingabe von Anmeldeinformationen aufgefordert. Die Anmeldeinformationen werden nur im Arbeitsspeicher und nur für das jeweilige Provisioningereignis gespeichert.

Überlegungen zur Bereitstellung

Citrix empfiehlt Kunden, bei der Bereitstellung von Citrix Gateway-Anwendungen und VDAs in ihren Umgebungen auf die Dokumentation zu bewährten Methoden zurückzugreifen.

Anforderungen für den Citrix Cloud Connector-Netzwerkzugriff

Die Citrix Cloud Connectors erfordern nur ausgehenden Datenverkehr von Port 443 zum Internet und können hinter einem HTTP-Proxy gehostet werden.

- In Citrix Cloud wird für die HTTPS-Kommunikation TLS verwendet. (Siehe Einstellung der Unterstützung von TLS-Versionen.)
- Im internen Netzwerk muss der Cloud Connector für Citrix DaaS auf Folgendes zugreifen können:
  - VDAs: Port 80, ein- und ausgehend, sowie bei Einsatz von Citrix Gateway Service 1494 und 2598 eingehend
  - StoreFront-Server: Port 80, eingehend
  - Citrix Gateways, falls diese als STA konfiguriert sind: Port 80, eingehend
  - Active Directory-Domänencontroller
  - Hypervisors: Nur ausgehend. Informationen zu spezifischen Ports siehe Von Citrix Technologien verwendete Kommunikationsports.

Der Datenverkehr zwischen den VDAs und Cloud Connectors wird mit Kerberos-Sicherheit auf Nachrichtenebene verschlüsselt.

StoreFront unter Verwaltung des Kunden

Unter Verwaltung des Kunden bietet StoreFront Konfigurationsoptionen für mehr Sicherheit und Flexibilität für die Bereitstellungsarchitektur, einschließlich der Möglichkeit, Benutzeranmeldeinformationen on-premises zu verwalten. StoreFront kann hinter dem Citrix Gateway gehostet werden, um einen sicheren Remotezugriff zu ermöglichen, eine Multifaktorauthentifizierung zu erzwingen und weitere Sicherheitsfeatures zu nutzen.

Citrix Gateway Service

Durch die Verwendung des Citrix Gateway-Service muss Citrix Gateway nicht im Datencenter des Kunden bereitgestellt werden.

Weitere Informationen finden Sie unter Citrix Gateway Service.

Alle TLS-Verbindungen zwischen Cloud Connector und Citrix Cloud werden vom Cloud Connector an Citrix Cloud initiiert. Es ist keine Firewallportzuordnung für eingehenden Datenverkehr erforderlich.

XML-Vertrauenseinstellung

Diese Einstellung ist unter **Vollständige Konfiguration > Einstellungen > XML-Vertrauen aktivieren** verfügbar und standardmäßig deaktiviert. Alternativ können Sie die XML-Vertrauensstellung mit dem Remote PowerShell-SDK von Citrix DaaS verwalten.

Die XML-Vertrauensstellung gilt für Bereitstellungen, die Folgendes verwenden:

- Eine On-Premises-Installation von StoreFront
- Eine (Benutzer-)Authentifizierungstechnologie für Abonnenten ohne erforderliche Kennwörter. Beispiele hierfür sind Lösungen mit Domänen-Passthrough, Smartcards, SAML und Veridium.

Wenn Sie die XML-Vertrauensstellung aktivieren, können Benutzer Anwendungen erfolgreich authentifizieren und starten. Der Cloud Connector stuft die von StoreFront gesendeten Anmeldeinformationen als vertrauenswürdig ein. Aktivieren Sie die XML-Vertrauensstellung nur, wenn die Kommunikation zwischen Citrix Cloud Connectors und StoreFront gesichert ist (durch Firewalls, IPsec oder andere empfohlene Sicherheitsfunktionen).

Diese Einstellung ist standardmäßig deaktiviert.

Verwalten Sie die XML-Vertrauensstellung mit dem Remote PowerShell-SDK von Citrix DaaS.

- Zum Überprüfen des aktuellen Werts der XML-Vertrauensstellung führen Sie `Get-BrokerSite` aus und überprüfen den Wert für `TrustRequestsSentToTheXMLServicePort`.
- Zum Aktivieren der XML-Vertrauensstellung führen Sie `Set-BrokerSite -TrustRequestsSentToTh $true` aus.
- Zum Deaktivieren der XML-Vertrauensstellung führen Sie `Set-BrokerSite -TrustRequestsSentTo $false` aus.

Erzwingen von HTTPS- oder HTTP-Datenverkehr

Um HTTPS- oder HTTP-Datenverkehr über den XML-Dienst zu erzwingen, konfigurieren Sie einen der folgenden Registrierungswertsätze auf jedem Cloud Connector.

Nachdem Sie die Einstellungen konfiguriert haben, starten Sie den Remote Brokeranbieterdienst auf jedem Cloud Connector neu.

In `HKLM\Software\Citrix\DesktopServer\`:

- Zum Erzwingen von HTTPS-Datenverkehr (HTTP ignorieren): Legen Sie `XmlServicesEnableSsl` auf `1` und `XmlServicesEnableNonSsl` auf `0` fest.
- Zum Erzwingen von HTTP-Datenverkehr (HTTPS ignorieren): Legen Sie `XmlServicesEnableNonSsl` auf `1` und `XmlServicesEnableSsl` auf `0` fest.

Einstellung der Unterstützung von TLS-Versionen

Um die Sicherheit von Citrix DaaS weiter zu erhöhen, wird seit dem 15. März 2019 jede Kommunikation über TLS 1.0 und 1.1 von Citrix blockiert.

Für alle Verbindungen mit Citrix Cloud-Diensten über Citrix Cloud Connectors ist TLS 1.2 erforderlich.

Um eine erfolgreiche Verbindung von Benutzergeräten mit Citrix Workspace sicherzustellen, muss die installierte Citrix Receiver-Version mindestens folgende Version aufweisen.

Receiver	Version
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0
Chrome/HTML5	Aktuelle Version (Browser muss TLS 1.2 unterstützen)

Für ein Upgrade auf die neueste Citrix Receiver-Version gehen Sie zu https://www.citrix.com/products/receiver/.

Führen Sie alternativ ein Upgrade auf die Citrix Workspace-App durch, die TLS 1.2 verwendet. Laden Sie die Citrix Workspace-App von https://www.citrix.com/downloads/workspace-app/ herunter.

Wenn Sie TLS 1.0 oder 1.1 weiterhin verwenden müssen (z. B. für einen Thin Client auf Basis einer früheren Version von Receiver für Linux), installieren Sie an Ihrem Ressourcenstandort eine StoreFront. Konfigurieren Sie dann alle Citrix Receiver so, dass sie darauf verweisen.

Weitere Informationen

Die folgenden Ressourcen enthalten Informationen zur Sicherheit:

- Technical security overview for Citrix Managed Azure.
- Citrix-Sicherheitssite:
- Sicherheits- und Compliance-Informationen: Über die Sicherheitsbulletins im Sicherheits- und Compliance-Center können Sie sich auf dem Laufenden halten. Das Center bietet außerdem Dokumentation zu Standards und Zertifizierungen für die Aufrechterhaltung einer sicheren und konformen IT-Umgebung.
- Der Leitfaden zur sicheren Bereitstellung von Citrix Cloud gibt eine Übersicht über bewährte Verfahren zur sicheren Verwendung von Citrix Cloud und beschreibt, welche Daten von Citrix Cloud erfasst und verwaltet werden. Der Leitfaden enthält außerdem Links zu umfassenden Informationen zum Citrix Cloud Connector.
- Anforderungen an System und Konnektivität

- Bewährte Methoden und Überlegungen zur Sicherheit.
- Smartcards.
- Transport Layer Security (TLS).

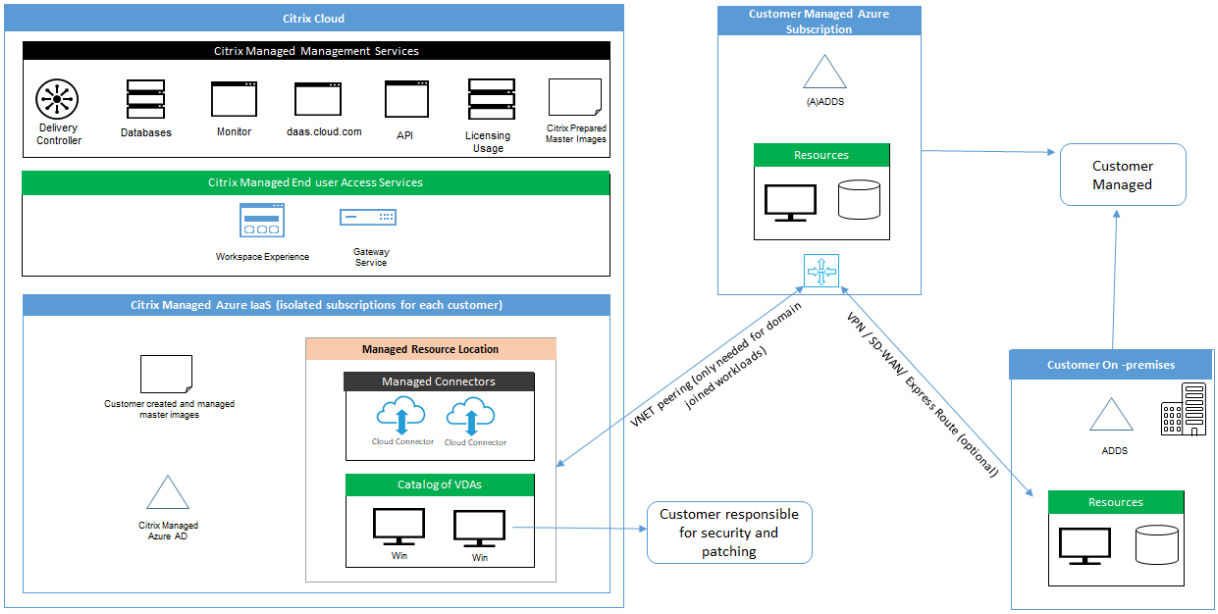
> **Hinweis:**
>
> Dieses Dokument enthält einen Überblick über die Sicherheitsfunktionen von Citrix Cloud sowie Informationen zur Verteilung der Zuständigkeiten zwischen Citrix und dem Kunden im Hinblick auf den Schutz einer Citrix Cloud-Bereitstellung. Es ist nicht als Konfigurations- oder Verwaltungsanleitung für Citrix Cloud oder zugehörige Komponenten und Services gedacht.

Überblick über die technische Sicherheit für Citrix Managed Azure

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Die folgende Grafik zeigt alle Komponenten einer Citrix DaaS-Bereitstellung (ehemals Citrix Virtual Apps and Desktops Service), die Citrix Managed Azure verwendet. In diesem Beispiel wird eine VNet-Peering-Verbindung verwendet.



Mit Citrix Managed Azure werden die Virtual Delivery Agents (VDAs) des Kunden zur Bereitstellung von Desktops und Apps und Citrix Cloud Connectors in einem von Citrix verwalteten Azure-Abonnement/-Mandanten bereitgestellt.

Citrix Cloud und Compliance

Stand Januar 2021: Die Verwendung von Citrix Managed Azure-Kapazität mit verschiedenen Citrix DaaS-Editionen und Workspace Premium Plus wurde noch nicht gemäß Citrix SOC 2 (Typ 1 oder 2), ISO 27001, HIPAA oder anderen Cloud-Compliance-Anforderungen bewertet. Im Citrix Trust Center finden Sie weitere Informationen zu Citrix Cloud-Zertifizierungen sowie regelmäßig aktualisierte Nachrichten.

Verantwortungsbereich von Citrix

Citrix Cloud Connectors für nicht domänengebundene Kataloge

Bei Verwendung eines Citrix Managed Azure-Abonnements stellt Citrix DaaS mindestens zwei Cloud Connectors an jedem Ressourcenstandort bereit. Manche Kataloge eines Kunden verwenden möglicherweise einen Ressourcenstandort gemeinsam, wenn sie sich in der gleichen Region befinden.

Citrix ist für die folgenden Sicherheitsvorgänge an Cloud Connectors für nicht domänengebundene Kataloge verantwortlich:

- Anwenden von Betriebssystemupdates und Sicherheitspatches
- Installieren und Pflege von Antivirensoftware
- Anwenden von Cloud Connector-Softwareupdates

Die Kunden haben keinen Zugriff auf die Cloud Connectors. Daher ist Citrix vollständig für die Leistung von Cloud Connectors für nicht domänengebundene Katalog verantwortlich.

Azure-Abonnement und Azure Active Directory

Citrix ist verantwortlich für die Sicherheit des Azure-Abonnements und Azure Active Directory (AAD) für den Kunden. Citrix gewährleistet die Isolierung der Mandanten, sodass jeder Kunde ein eigenes Azure-Abonnement und AAD hat und kein Austausch zwischen verschiedenen Mandanten stattfindet. Zugriff auf das AAD haben nur Citrix DaaS und Citrix Betriebspersonal. Der Zugriff von Citrix auf Azure-Abonnements von Kunden wird überwacht.

Kunden mit nicht domänengebundenen Kataloge können das von Citrix verwaltete AAD zur Authentifizierung für Citrix Workspace verwenden. Für solche Kunden erstellt Citrix Benutzerkonten mit

eingeschränkten Privilegien in dem von Citrix verwalteten AAD. Weder die Benutzer noch die Administratoren der Kunden können Aktionen an dem von Citrix verwalteten AAD ausführen. Kunden, die ihr eigenes AAD verwenden, sind vollständig für dessen Sicherheit verantwortlich.

Virtuelle Netzwerke und Infrastruktur

Im Citrix Managed Azure-Abonnement des Kunden erstellt Citrix virtuelle Netzwerke zur Isolierung von Ressourcenstandorten. In diesen Netzwerken erstellt Citrix neben Speicherkonten, Key Vaults und anderen Azure-Ressourcen virtuelle Maschinen für die VDAs, Cloud Connectors und Image-Builder-Maschinen. Zusammen mit Microsoft ist Citrix für die Sicherheit der virtuellen Netzwerke und virtuellen Netzwerk-Firewalls verantwortlich.

Citrix sorgt dafür, dass die standardmäßige Azure-Firewallrichtlinie (Netzwerksicherheitsgruppen) so konfiguriert ist, dass sie den Zugriff auf Netzwerkschnittstellen in VNet-Peering- und SD-WAN-Verbindungen einschränkt. Im Allgemeinen steuert dies den eingehenden Datenverkehr an VDAs und Cloud Connectors. Einzelheiten finden Sie in den folgenden Abschnitten:

- Firewall-Richtlinie für Azure VNet-Peering-Verbindungen
- Firewallrichtlinie für SD-WAN-Verbindungen

Die Kunden können die Standard-Firewallrichtlinie nicht ändern, sie können aber zusätzliche Firewallregeln auf von Citrix erstellten VDA-Maschinen bereitstellen, z. B. um ausgehenden Datenverkehr teilweise einzuschränken. Kunden, die auf von Citrix erstellten VDA-Maschinen VPN-Clients oder andere Software installieren, die Firewallregeln umgehen kann, haften für alle daraus entstehenden Sicherheitsrisiken.

Wenn Sie den Image-Builder in Citrix DaaS zum Erstellen und Anpassen eines Maschinenimages verwenden, werden die Ports 3389–3390 vorübergehend im von Citrix verwalteten VNet geöffnet, sodass der Kunde RDP-Zugriff auf die Maschine mit dem neuen Image erhält, um dieses anzupassen.

Verantwortungsbereich von Citrix bei Verwendung von Azure VNet-Peering-Verbindungen

Damit VDAs in Citrix DaaS auf on-premises bereitgestellte Domänencontroller, Dateifreigaben oder andere Intranetressourcen zugreifen können, bietet Citrix DaaS einen VNet-Peering-Workflow als Verbindungsoption. Das von Citrix verwaltete virtuelle Netzwerk des Kunden erhält eine Peer-Stellung mit einem vom Kunden verwalteten virtuellen Azure-Netzwerk. Das vom Kunden verwaltete virtuelle Netzwerk kann Konnektivität mit den On-Premises-Ressourcen des Kunden über eine Cloud-to-On-Premises-Konnektivitätslösung nach Wahl des Kunden wie etwa Azure ExpressRoute oder IPsec-Tunnel ermöglichen.

Die Verantwortung von Citrix für das VNet-Peering beschränkt sich auf die Unterstützung des Workflows und der zugehörigen Azure-Ressourcenkonfiguration zur Herstellung einer Peering-Beziehung

zwischen den von Citrix und vom Kunden verwalteten VNets.

Firewall-Richtlinie für Azure VNet-Peering-Verbindungen Citrix öffnet bzw. schließt die folgenden Ports für über eine VNet-Peering-Verbindung ein- und ausgehenden Datenverkehr.

Von Citrix verwaltetes VNet mit nicht domänengebundenen Maschinen

- Eingehende Regeln
  - Zugelassen: Ports 80, 443, 1494 und 2598, eingehend von VDAs zu Cloud Connectors und von Cloud Connectors zu VDAs.
  - Zugelassen: Ports 49152–65535, eingehend zu VDAs aus einem von der Spiegelung der Überwachung verwendeten IP-Bereich. Siehe Von Citrix-Technologien verwendete Kommunikationsports.
  - Verweigern: sämtlicher anderer eingehender Datenverkehr. Dazu gehört VNet-interner Datenverkehr von VDA zu VDA und VDA zu Cloud Connector.
- Ausgehende Regeln
  - Gesamten ausgehenden Datenverkehr zulassen.

Von Citrix verwaltetes VNet mit domänengebundenen Maschinen

- Eingehende Regeln:
  - Zugelassen: Ports 80, 443, 1494 und 2598, eingehend von VDAs zu Cloud Connectors und von Cloud Connectors zu VDAs.
  - Zugelassen: Ports 49152–65535, eingehend zu VDAs aus einem von der Spiegelung der Überwachung verwendeten IP-Bereich. Siehe Von Citrix-Technologien verwendete Kommunikationsports.
  - Verweigern: sämtlicher anderer eingehender Datenverkehr. Dazu gehört VNet-interner Datenverkehr von VDA zu VDA und VDA zu Cloud Connector.
- Ausgehende Regeln
  - Gesamten ausgehenden Datenverkehr zulassen.

Vom Kunden verwaltetes VNet mit domänengebundenen Maschinen

- Die korrekte Konfiguration des VNets obliegt dem Kunden. Dazu gehört das Öffnen der folgenden Ports für den Domänenbeitritt.
- Eingehende Regeln:

  - Zulassen: eingehenden Datenverkehr an Port 443, 1494 und 2598 von den Client-IPs für interne Starts.
  - Zulassen: eingehenden Datenverkehr an Port 53, 88, 123, 135–139, 389, 445 und 636 von Citrix VNet (vom Kunden spezifizierter IP-Bereich).
  - Zulassen: sämtlichen eingehenden Datenverkehr an Ports, die mit einer Proxykonfiguration geöffnet werden.
  - Andere vom Kunden erstellte Regeln.

- Ausgehende Regeln:

  - Zulassen: ausgehenden Datenverkehr an Port 443, 1494 und 2598 zum Citrix VNet (vom Kunden spezifizierter IP-Bereich) für interne Starts.
  - Andere vom Kunden erstellte Regeln.

Verantwortungsbereich von Citrix bei Verwendung von SD-WAN-Konnektivität

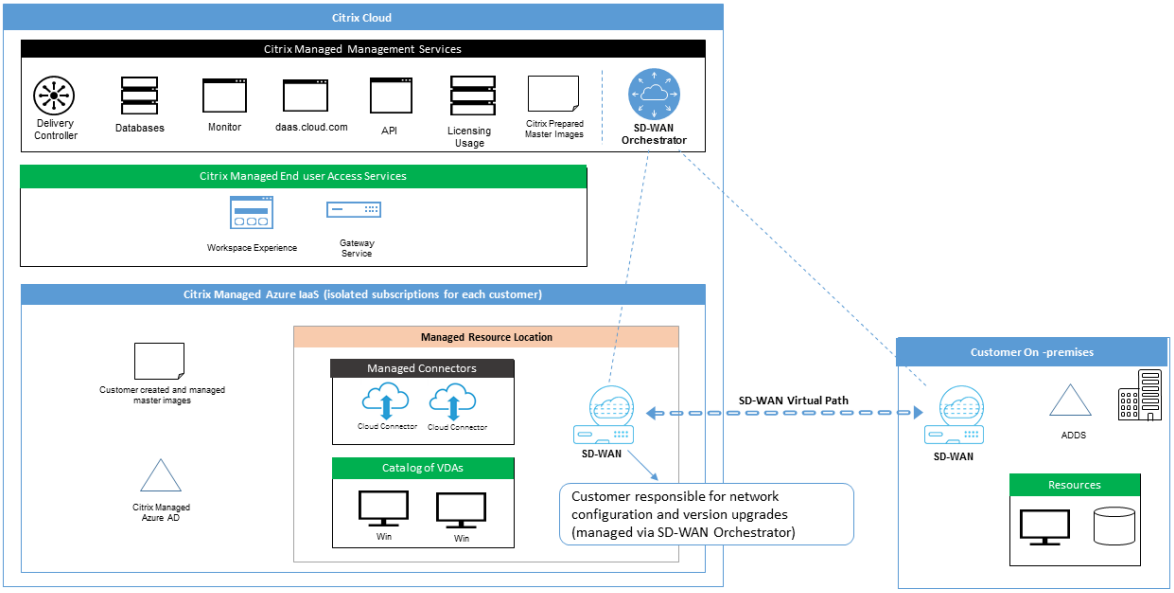
Citrix unterstützt eine vollautomatische Bereitstellung virtueller Citrix SD-WAN-Instanzen für Verbindungen zwischen Citrix DaaS und On-Premises-Ressourcen. Citrix SD-WAN-Konnektivität hat im Vergleich zum VNet-Peering mehrere Vorteile:

Große Zuverlässigkeit und Sicherheit bei den Verbindungen vom VDA an das Datencenter und VDA-zu-Branch-Verbindungen (ICA-Verbindungen).

- Beste Endbenutzererfahrung im Büro mit erweiterten QoS-Funktionen und VoIP-Optimierungen.
- Integrierte Funktionen zur Prüfung und Priorisierung des Citrix HDX-Netzwerkdatenverkehrs sowie anderer Bereiche der Anwendungsnutzung sowie zur Berichterstellung.

Kunden, die die SD-WAN-Konnektivität für Citrix DaaS nutzen möchten, müssen ihre Citrix SD-WAN-Netzwerke mit SD-WAN Orchestrator verwalten.

Das folgende Diagramm zeigt die zusätzlichen Komponenten einer Citrix DaaS-Bereitstellung mit Citrix Managed Azure-Abonnement und SD-WAN-Konnektivität.



Die Citrix SD-WAN-Bereitstellung für Citrix DaaS ähnelt der Standardkonfiguration einer Azure-Bereitstellung für Citrix SD-WAN. Weitere Informationen finden Sie unter Bereitstellen einer Citrix SD-WAN Standard Edition-Instanz in Azure. In Hochverfügbarkeitskonfigurationen wird ein Aktiv-/Standby-SD-WAN-Instanzpaar mit Azure Load Balancern als Gateway zwischen dem Subnetz mit VDAs und Cloud Connectors und dem Internet bereitgestellt. In einer Konfiguration ohne hohe Verfügbarkeit wird nur eine SD-WAN-Instanz als Gateway bereitgestellt. Den Netzwerkschnittstellen der virtuellen SD-WAN-Appliances werden Adressen aus einem separaten kleinen Adressbereich zugewiesen, der in zwei Subnetze aufgeteilt ist.

Bei der Konfiguration der SD-WAN-Konnektivität nimmt Citrix einige Änderungen an der oben beschriebenen Netzwerkkonfiguration verwalteter Desktops vor. Insbesondere wird der gesamte ausgehende Datenverkehr aus dem VNet, einschließlich des Datenverkehrs in das Internet, durch die Cloud-SD-WAN-Instanz geleitet. Die SD-WAN-Instanz wird außerdem als DNS-Server für das von Citrix verwaltete VNet konfiguriert.

Der Verwaltungszugriff auf die virtuellen SD-WAN-Instanzen erfordert ein Administratorkonto. Jeder Instanz von SD-WAN ist ein eindeutiges, zufälliges und sicheres Kennwort zugewiesen, das SD-WAN-Administratoren zur Remote-Anmeldung und Problembehandlung über SD-WAN Orchestrator, die Verwaltungs-UI der virtuellen Appliance und die CLI verwenden können.

Wie andere mandantenspezifische Ressourcen sind virtuelle SD-WAN-Instanzen, die in einem Kunden-VNet bereitgestellt werden, vollständig von allen anderen VNets isoliert.

Wenn ein Kunde die Citrix SD-WAN-Konnektivität aktiviert, automatisiert Citrix die Erstbereitstellung der virtuellen, für Citrix DaaS verwendeten SD-WAN-Instanzen, verwaltet zugrundeliegende Azure-Ressourcen (virtuelle Maschinen, Load Balancer usw.), bietet sichere und effiziente Standardwerte

für die Erstkonfiguration virtueller SD-WAN-Instanzen und ermöglicht die laufende Wartung und Problembehandlung über SD-WAN Orchestrator. Citrix ergreift außerdem angemessene Maßnahmen, um die SD-WAN-Netzwerkkonfiguration automatisch zu validieren, auf bekannte Sicherheitsrisiken zu prüfen und entsprechende Warnungen über SD-WAN Orchestrator anzuzeigen.

Firewallrichtlinie für SD-WAN-Verbindungen Citrix verwendet Azure-Firewallrichtlinien (Netzwerksicherheitsgruppen) und die Zuweisung öffentlicher IP-Adressen, um den Zugriff auf Netzwerkschnittstellen virtueller SD-WAN-Appliances zu beschränken:

- Nur WAN- und Verwaltungsschnittstellen werden öffentliche IP-Adressen zugewiesen und bieten ausgehende Konnektivität mit dem Internet.
- LAN-Schnittstellen, die als Gateways für das von Citrix verwaltete VNet fungieren, können nur Daten mit virtuellen Maschinen im selben VNet austauschen.
- Bei WAN-Schnittstellen ist der eingehende Datenverkehr auf UDP-Port 4980 (von Citrix SD-WAN für virtuelle Pfadkonnektivität verwendet) beschränkt, ausgehender Datenverkehr an das VNet wird verweigert.
- Verwaltungsports lassen eingehenden Datenverkehr an Port 443 (HTTPS) und 22 (SSH) zu.
- Hoch verfügbare Schnittstellen dürfen nur Steuerungsdatenverkehr untereinander austauschen.

Zugriff auf die Infrastruktur

Citrix kann auf die von Citrix verwaltete Infrastruktur (Cloud Connectors) des Kunden zugreifen, um bestimmte Verwaltungsaufgaben (z. B. Sammeln von Protokollen einschließlich Windows-Ereignisanzeige, Neustarten von Diensten etc.) auszuführen, ohne den Kunden zu benachrichtigen. Citrix ist dafür verantwortlich, diese Aufgaben sicher und mit minimalen Auswirkungen auf den Kunden auszuführen. Citrix ist außerdem dafür verantwortlich, dass alle Protokolldateien sicher abgerufen, transportiert und gehandhabt werden. Auf Kunden-VDAs kann auf diese Weise nicht zugegriffen werden.

Backups nicht domänengebundener Kataloge

Citrix ist nicht für Backups nicht domänengebundener Kataloge zuständig.

Backups von Maschinenimages

Citrix ist für die Sicherung aller an Citrix DaaS hochgeladenen Maschinenimages zuständig, einschließlich derer, die mit dem Image Builder erstellt wurden. Citrix verwendet für diese Images lokal redundanten Speicher.

Bastions für nicht domänengebundene Kataloge

Citrix Betriebspersonal kann bei Bedarf eine Bastion für den Zugriff auf das von Citrix verwaltete Azure-Abonnement des Kunden erstellen, um Kundenprobleme (ggf. auch proaktiv) zu diagnostizieren und zu beheben. Citrix benötigt zum Erstellen einer Bastion keine Zustimmung des Kunden. Citrix erstellt ein starkes zufällig generiertes Kennwort für die Bastion und beschränkt den RDP-Zugriff auf Citrix NAT-IP-Adressen. Wenn die Bastion nicht mehr benötigt wird, wird sie von Citrix entfernt und das Kennwort verliert seine Gültigkeit. Die Bastion und zugehörige RDP-Zugangsregeln werden nach Abschluss des Vorgangs entfernt. Citrix kann über die Bastion nur auf die nicht domänengebundenen Cloud Connectors des Kunden zugreifen. Citrix ist nicht in Besitz des Kennworts für die Anmeldung bei nicht domänengebundenen VDAs oder bei domänengebundenen Cloud Connectors und VDAs.

Firewallrichtlinie bei Verwendung von Tools zur Problembehandlung

Wenn ein Kunde die Erstellung einer Bastionmaschine zur Problembehandlung beantragt, werden die folgenden Sicherheitsgruppen-Änderungen am von Citrix verwalteten VNet vorgenommen:

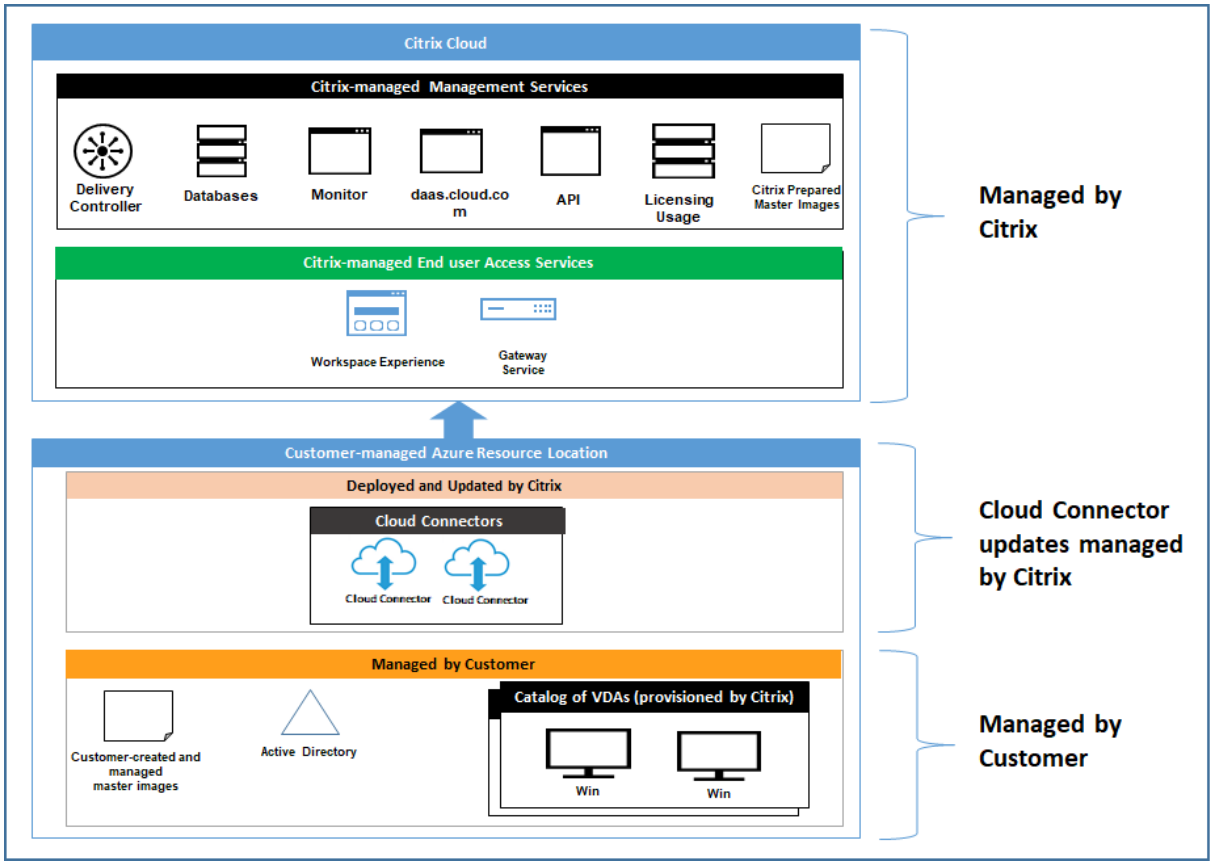
- Vorübergehend wird über Port 3389 eingehender Datenverkehr von dem vom Kunden angegebenen IP-Bereich an die Bastion zugelassen.
- Vorübergehend wird über Port 3389 eingehender Datenverkehr von der IP-Adresse der Bastion an beliebige Adressen im VNet (VDAs und Cloud Connectors) zugelassen.
- RDP-Zugriff zwischen Cloud Connectors, VDAs und anderen VDAs wird weiterhin blockiert.

Wenn ein Kunde RDP-Zugriff zur Problembehandlung ermöglicht, werden die folgenden Sicherheitsgruppen-Änderungen am von Citrix verwalteten VNet vorgenommen:

- Vorübergehend wird über Port 3389 eingehender Datenverkehr von dem vom Kunden angegebenen IP-Adressbereich an beliebige Adressen im VNet (VDAs und Cloud Connectors) zugelassen.
- RDP-Zugriff zwischen Cloud Connectors, VDAs und anderen VDAs wird weiterhin blockiert.

Vom Kunden verwaltete Abonnements

Bei vom Kunden verwalteten Abonnements übernimmt Citrix bei der Bereitstellung der Azure-Ressourcen die oben genannten Aufgaben. Nach der Bereitstellung fallen sämtliche oben genannten Aufgaben in den Verantwortungsbereich des Kunden als Eigentümer des Azure-Abonnements.



Verantwortung des Kunden

VDAs und Maschinenimages

Der Kunde ist für alle Aspekte der auf VDA-Maschinen installierten Software verantwortlich:

- Betriebssystem-Updates und Sicherheitspatches
- Antiviren- und Antimalwareprogramme
- VDA-Softwareupdates und Sicherheitspatches
- Zusätzliche Software-Firewallregeln (insbesondere ausgehender Datenverkehr)
- Befolgen der Anweisungen unter Bewährte Methoden und Überlegungen zur Sicherheit von Citrix

Citrix stellt ein vorbereitetes Image als Ausgangspunkt bereit. Kunden können das Image für Machbarkeitsstudien, zu Demonstrationszwecken oder als Grundlage für die Erstellung eines eigenen Images verwenden. Citrix haftet nicht für die Sicherheit dieses Images. Citrix versucht, das Betriebssystem und die VDA-Software des vorbereiteten Images auf dem neuesten Stand zu halten, und aktiviert Windows Defender.

Verantwortungsbereich des Kunden bei der Verwendung von VNet-Peering

Der Kunde muss alle unter Vom Kunden verwaltetes VNet mit domänengebundenen Maschinen angegebenen Ports öffnen.

Wenn VNet-Peering konfiguriert ist, ist der Kunde für die Sicherheit seines eigenen virtuellen Netzwerks und dessen Konnektivität mit den On-Premises-Ressourcen verantwortlich. Der Kunde ist auch für die Sicherheit des aus dem von Citrix verwalteten virtuellen Peer-Netzwerk eingehenden Datenverkehrs verantwortlich. Citrix unternimmt keine Maßnahmen, um Datenverkehr vom dem von Citrix verwalteten virtuellen Netzwerk zu den On-Premises-Ressourcen des Kunden zu blockieren.

Die Kunden können eingehenden Datenverkehr folgendermaßen beschränken:

- Vergabe eines IP-Blocks an das von Citrix verwaltete virtuelle Netzwerk, der nicht anderswo im On-Premises-Netzwerk des Kunden oder in dem vom Kunden verwalteten virtuellen Netzwerk verwendet wird. Dies ist für VNet-Peering erforderlich.
- Hinzufügen von Azure-Netzwerksicherheitsgruppen und Firewalls im eigenen virtuellen und On-Premises-Netzwerk, um den Datenverkehr aus dem von Citrix verwalteten IP-Block zu blockieren oder einzuschränken.
- Implementieren von Eindringschutzsystemen, Softwarefirewalls, Verhaltensanalyse-Engines o. Ä. im eigenen virtuellen und On-Premises-Netzwerk, die auf den von Citrix verwalteten IP-Block abzielen.

Verantwortungsbereich des Kunden bei Verwendung von SD-WAN-Konnektivität

Ist SD-WAN-Konnektivität konfiguriert, können die Kunden entsprechend ihren Netzwerkanforderungen flexibel virtuelle SD-WAN-Instanzen zur Verwendung für Citrix DaaS konfigurieren, mit Ausnahme einiger Elemente, die für den einwandfreien SD-WAN-Betrieb im vom Citrix verwalteten VNet erforderlich sind. Zu den Aufgaben des Kunden gehört Folgendes:

- Planung und Konfiguration von Routing- und Firewallregeln, einschließlich für DNS und Internetbreakout.
- Wartung der SD-WAN-Netzwerkkonfiguration.
- Überwachung des Netzwerkbetriebsstatus.
- Zeitnahe Bereitstellung von Citrix SD-WAN-Softwareupdates oder Sicherheitsfixes. Da alle Citrix SD-WAN-Instanzen im Kundennetzwerk dieselbe Version der SD-WAN-Software ausführen müssen, sind Updates für Citrix DaaS-SD-WAN-Instanzen vom Kunden gemäß eigener Netzwerkwartungspläne und -beschränkungen zu verwalten.

Ein fehlerhaftes SD-WAN-Routing, falsch konfigurierte Firewallregeln oder schlecht verwaltete SD-WAN-Verwaltungskennwörter bergen Sicherheitsrisiken für virtuelle Ressourcen in Citrix DaaS und für über virtuelle Citrix SD-WAN-Pfade erreichbare On-Premises-Ressourcen. Ein weiteres mögliches

Sicherheitsrisiko besteht im Unterlassen von Updates der Citrix SD-WAN-Software auf das neueste verfügbare Patch-Release. SD-WAN Orchestrator und andere Citrix Cloud-Dienste bieten zwar die Möglichkeit, solche Risiken zu beheben, doch sind die Kunden letztendlich selbst für die korrekte Konfiguration virtueller SD-WAN-Instanzen verantwortlich.

Proxy

Kunden können wahlweise einen Proxy für ausgehenden Datenverkehr vom VDA verwenden. Wenn ein Proxy verwendet wird, ist sind die Kunden für Folgendes verantwortlich:

- Konfigurieren der Proxy-Einstellungen auf dem VDA-Image, bzw. bei domänengebundenen VDAs über die Active Directory-Gruppenrichtlinie.
- Wartung und Sicherheit des Proxys.

Für Citrix Cloud Connectors oder eine andere von Citrix verwaltete Infrastruktur sind Proxys nicht zugelassen.

Katalogresilienz

Citrix bietet drei Arten von Katalogen mit unterschiedlicher Resilienz:

- **Statischer Katalog:** Jeder Benutzer ist einem einzelnen VDA zugewiesen. Dieser Katalogtyp bietet keine hohe Verfügbarkeit. Wenn der VDA eines Benutzers ausfällt, muss er auf einen neuen verlegt . Azure bietet ein SLA von 99,5 % für Einzelinstanz-VMs. Der Kunde kann das Benutzerprofil sichern, doch alle am VDA vorgenommenen Anpassungen (z. B. installierte Programme oder Windows-Konfigurationen) gehen verloren.
- **Zufälliger Katalog:** Jeder Benutzer wird beim Starten nach dem Zufallsprinzip einem Server-VDA zugewiesen. Dieser Katalogtyp bietet hohe Verfügbarkeit per Redundanz. Wenn ein VDA ausfällt, gehen keine Informationen verloren, da sich das Benutzerprofil an anderer Stelle befindet.
- **Windows 10-Multisitzungskatalog:** Dieser Katalogtyp funktioniert wie ein zufälliger Katalog, mit dem Unterschied, dass Windows 10-Workstation-VDAs anstelle von Server-VDAs verwendet werden.

Backups für domänengebundene Kataloge

Verwendet ein Kunde domänengebundene Kataloge mit VNet-Peering, ist er für Backups der Benutzerprofile verantwortlich. Citrix empfiehlt die Einrichtung von On-Premises-Dateifreigaben und von Richtlinien in Active Directory bzw. VDAs zum Abrufen von Benutzerprofilen aus den Dateifreigaben. Die Kunden sind für Backups und Verfügbarkeit dieser Dateifreigaben verantwortlich.

Notfallwiederherstellung

Bei einem Verlust der Azure-Daten stellt Citrix so viele Ressourcen wie möglich in dem von Citrix verwalteten Azure-Abonnement wieder her. Citrix versucht außerdem eine Wiederherstellung der Cloud Connectors und VDAs. Kann Citrix diese Elemente nicht wiederherstellen, obliegt es dem Kunden, einen neuen Katalog zu erstellen. Citrix geht davon aus, dass Maschinenimages gesichert werden und die Kunden ihre Benutzerprofile gesichert haben, sodass der Katalog neu erstellt werden kann.

Beim Verlust einer gesamten Azure-Region obliegt es dem Kunden, das von ihm verwaltete virtuelle Netzwerk in einer neuen Region neu aufzubauen und ein neues VNet-Peering oder eine neue SD-WAN-Instanz in Citrix DaaS zu erstellen.

Gemeinsamer Verantwortungsbereich von Citrix und Kunden

Citrix Cloud Connector für domänengebundene Kataloge

Citrix DaaS installiert mindestens zwei Cloud Connectors an jedem Ressourcenstandort. Manche Kataloge eines Kunden verwenden möglicherweise einen Ressourcenstandort gemeinsam, wenn sie sich in der gleichen Region im gleichen VNet-Peer und in der gleichen Domäne befinden. Citrix konfiguriert die domänengebundenen Cloud Connectors des Kunden für die folgenden Standardsicherheitseinstellungen für das Image:

- Betriebssystem-Updates und Sicherheitspatches
- Antivirensoftware
- Cloud Connector-Softwareupdates

Die Kunden haben normalerweise keinen Zugriff auf Cloud Connectors. Sie können jedoch Zugriff erhalten, indem sie eine Problembehandlung am Katalog ausführen und sich mit Domänenanmeldeinformationen anmelden. Die Kunden sind für alle Änderungen, die sie bei der Anmeldung per Bastion vornehmen, verantwortlich.

Die Kunden haben außerdem über Active Directory-Gruppenrichtlinien Kontrolle über die domänengebundenen Cloud Connectors. Die Kunden sind für die Angemessenheit und Sicherheit der für den Cloud Connector geltenden Gruppenrichtlinien verantwortlich. Deaktiviert ein Kunde beispielsweise Betriebssystemupdates über die Gruppenrichtlinie, ist er für die Durchführung von Betriebssystemupdates an den Cloud Connectors verantwortlich. Die Kunden können über die Gruppenrichtlinie auch strengere Sicherheitseinstellungen als die Cloud Connector-Standardeinstellungen durchsetzen, z. B. durch Installation einer anderen Antivirensoftware. Generell empfiehlt Citrix die Integration von Cloud Connectors ohne Richtlinien in die eigene Active Directory-Organisationseinheit, da so die Standardeinstellungen von Citrix problemlos angewendet werden können.

Problembehandlung

Bei Problemen mit dem Katalog in Citrix DaaS gibt es zwei Möglichkeiten zur Problembehandlung: Bastion oder RDP-Zugriff. Beide Optionen bergen ein Sicherheitsrisiko für den Kunden. Der Kunde muss vor Nutzung einer der Optionen das Risiko kennen und akzeptieren.

Citrix ist dafür zuständig, die zur Problembehandlung erforderlichen Ports zu öffnen und zu schließen und den Zugriff auf Maschinen nach Bedarf einzuschränken.

Sowohl bei Nutzung einer Bastion als auch beim RDP-Zugriff ist der ausführende Benutzer für die Sicherheit der Maschinen verantwortlich, auf die zugegriffen wird. Greift der Kunde per RDP auf den VDA oder Cloud Connector zu und es kommt zu einer Vireninfektion, haftet der Kunde. Wenn Citrix Support-Mitarbeiter auf diese Maschinen zugreifen, liegt es in der Verantwortung dieser Mitarbeiter, Vorgänge sicher durchzuführen. Die Verantwortung für etwaige Schwachstellen, die beim Zugriff auf die Bastion oder andere Maschinen in der Bereitstellung verursacht werden (z. B. Verantwortung des Kunden für die Aufnahme von IP-Bereichen in die Positivliste, Verantwortung von Citrix zur korrekten Implementierung von IP-Bereichen) wird an anderer Stelle in diesem Dokument behandelt.

In beiden Fällen ist Citrix für Erstellung von Firewallausnahmen für den RDP-Datenverkehr verantwortlich. Citrix ist auch für den Widerruf der Ausnahmen verantwortlich, nachdem der Kunde die Bastion entfernt bzw. den RDP-Zugriff über Citrix DaaS beendet hat.

Bastions Citrix kann in dem von Citrix verwalteten virtuellen Netzwerk des Kunden innerhalb des von Citrix verwalteten Abonnements Bastions erstellen, um Probleme proaktiv (ohne Benachrichtigung des Kunden) oder nach einer Meldung vom Kunden zu diagnostizieren und zu beheben. Eine Bastion ist eine Maschine, auf die der Kunde per RDP zugreift und von dort per RDP auf VDAs und (für domänengebundene Kataloge) Cloud Connectors zugreifen kann, um Protokolle zu erfassen, Dienste neu zu starten oder andere Verwaltungsaufgaben auszuführen. Standardmäßig wird beim Erstellen einer Bastion eine externe Firewallregel erstellt, die RDP-Datenverkehr von einem vom Kunden spezifizierten IP-Bereich zur Bastion-Maschine zulässt. Außerdem wird eine interne Firewallregel erstellt, die den RDP-Zugriff auf die Cloud Connectors und VDAs ermöglicht. Diese Regeln bergen ein großes Sicherheitsrisiko.

Der Kunde ist dafür verantwortlich, ein starkes Kennwort für das lokale Windows-Konto einzurichten. Der Kunde ist außerdem dafür verantwortlich, einen externen IP-Adressbereich bereitzustellen, der RDP-Zugriff auf die Bastion ermöglicht. Stellt der Kunde keinen IP-Bereich bereit, sodass jeder RDP-Zugriff hat, haftet der Kunde für jeglichen Zugriff von schädlichen IP-Adressen.

Der Kunde ist dafür verantwortlich, die Bastion nach Abschluss der Fehlerbehandlung zu löschen. Der Bastion-Host legt weitere Angriffsfläche frei, weshalb Citrix die Maschine acht Stunden nach dem Einschalten automatisch herunterfährt. Eine Bastion wird von Citrix jedoch nie automatisch gelöscht. Wenn der Kunde eine Bastion über einen längeren Zeitraum verwendet, ist er für Patches und Updates zuständig. Citrix empfiehlt, eine Bastion nur einige Tage lang zu verwenden und sie dann zu löschen.

Wenn der Kunde eine aktuelle Bastion wünscht, kann er die aktuelle Bastion löschen und eine neue erstellen. Dadurch wird eine neue Maschine mit den neuesten Sicherheitspatches bereitgestellt.

RDP-Zugriff Ist das kundenseitige VNet-Peering für domänengebundene Kataloge funktionsfähig, kann der Kunde den RDP-Zugriff von seinem VNet-Peer auf sein von Citrix verwaltetes VNet aktivieren. Wenn der Kunde diese Option nutzt, ist er für den Zugriff auf die VDAs und Cloud Connectors per VNet-Peering verantwortlich. Es können Quell-IP-Adressbereiche angegeben werden, um den RDP-Zugriff auch im Netzwerks des Kunden weiter einzuschränken. Der Kunde muss Domänenanmeldeinformationen verwenden, um sich bei diesen Maschinen anzumelden. Arbeitet der Kunde zusammen mit dem Citrix Support an einer Problembehebung, muss er die Anmeldeinformationen möglicherweise an Support-Mitarbeiter weitergeben. Nach Behebung des Problems ist der Kunde für die Deaktivierung des RDP-Zugriffs zuständig. Bleibt der RDP-Zugriff über den Netzwerk-Peer oder das On-Premises-Netzwerk des Kunden bestehen, stellt dies ein Sicherheitsrisiko dar.

Domänenanmeldeinformationen

Entscheidet sich der Kunde für die Verwendung eines domänengebundenen Katalogs, muss er Citrix DaaS ein Domänenkonto (Benutzername und Kennwort) mit Berechtigung zum Hinzufügen von Maschinen zur Domäne zuweisen. Bei der Bereitstellung von Domänenanmeldeinformationen muss folgende Sicherheitsprinzipien einhalten:

- **Überprüfbar:** Das Konto muss speziell für die Verwendung durch Citrix DaaS erstellt werden, damit einfach überprüft werden kann, wofür es verwendet wird.
- **Bereichsbezogen:** Das Konto benötigt nur die Berechtigung, Maschinen einer Domäne hinzuzufügen. Es darf kein Volladministrator für die Domäne sein.
- **Sicher:** Für das Konto muss ein starkes Kennwort eingerichtet werden.

Citrix ist für die sichere Speicherung des Domänenkontos in einem Azure Key Vault in dem von Citrix verwalteten Azure-Abonnement des Kunden zuständig. Das Konto wird nur abgerufen, wenn für einen Vorgang das Kennwort des Domänenkontos benötigt wird.

Weitere Informationen

Weitere Informationen finden Sie unter:

- Leitfaden zur sicheren Bereitstellung für die Citrix Cloud-Plattform: Sicherheitsinformationen für die Citrix Cloud-Plattform.
- Technische Sicherheit: Sicherheitsinformationen für Citrix DaaS
- Hinweise zu Drittanbietern

Positivliste für virtuelle Kanäle

May 17, 2024

Die Positivliste für virtuelle Kanäle ist ein Feature, mit dem Sie steuern können, welche virtuellen Kanäle, die nicht von Citrix stammen, in Ihrer Umgebung zulässig sind. Die Positivliste für virtuelle Kanäle ist standardmäßig aktiviert. Daher dürfen in Sitzungen von Citrix Virtual Apps and Desktops nur virtuelle Citrix Kanäle geöffnet werden. Ist die Verwendung benutzerdefinierter virtueller Kanäle erforderlich (eigener oder derer eines Dritten), müssen diese der Positivliste hinzugefügt werden.

Konfiguration

Die Positivliste für virtuelle Kanäle ist standardmäßig deaktiviert. Sie können dieses Feature mithilfe der folgenden Einstellungen in der Citrix-Richtlinie konfigurieren:

- **Positivliste für virtuelle Kanäle**: um die Funktion zu aktivieren oder zu deaktivieren und virtuelle Kanäle zur Liste hinzuzufügen.
- **Protokolldrosselung für virtuelle Kanäle –Positivliste**: legt den Einschränkungszeitraum für die Protokollierung von Listenereignissen für virtuelle Kanäle fest.
- **Positivliste für die Protokollierung**: legt die Protokollierungsstufe für die Positivliste virtueller Kanäle fest.

Hinzufügen virtueller Kanäle zur Positivliste

Sie benötigen die folgenden Informationen, um einen virtuellen Kanal zur Positivliste hinzuzufügen, benötigen:

1. Den Namen des virtuellen Kanals gemäß Definition im Code (bis zu sieben Zeichen lang). Beispiel: `CTXCVC1`.
2. Die Pfade zu den Prozessen, die den virtuellen Kanal auf der VDA-Maschine öffnen. Beispiel: `C:\Program Files\Application\run.exe`.

Wenn Sie die erforderlichen Informationen zur Hand haben, müssen Sie den virtuellen Kanal über die Richtlinieneinstellung für Positivliste virtueller Kanäle der Positivliste hinzufügen. Zum Eintragen eines virtuellen Kanals in die Liste geben Sie den Namen des virtuellen Kanals gefolgt von einem Komma und dem Pfad zu dem Prozess ein, der auf den virtuellen Kanal zugreift. Wenn es mehrere Prozesse gibt, können Sie diese Prozesse hinzufügen, indem Sie sie durch Kommas trennen.

Für einzelne Prozesse

Im Fall der o. g. Beispiele würden Sie der Liste den folgenden Eintrag hinzufügen:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Für mehrere Prozesse

Im Fall mehrerer Prozesse fügen Sie den folgenden Eintrag hinzu:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

Platzhalter verwenden

Die Verwendung von Platzhaltern (*) wird unterstützt. Sie können Platzhalter verwenden, wenn sich die Namen von Verzeichnissen oder ausführbaren Dateien entsprechend der Version der Anwendung ändern oder wenn die Drittanbieterkomponente in den Benutzerprofilen installiert ist.

Sie können Platzhalter in den folgenden Szenarien verwenden:

- Um den vollständigen Verzeichnisnamen zu ersetzen.
  Beispiel: `C:\Program Files\Application\*\run1.exe`
- Um einen Teil des Verzeichnisnamens zu ersetzen.
  Beispiel: `C:\Program Files\Application\v*\run1.exe`
- Um den Namen der ausführbaren Datei zu ersetzen.
  Beispiel: `C:\Program Files\Application\v1.2\*.exe`
- Um einen Teil des Namens der ausführbaren Datei zu ersetzen.
  Beispiel: `C:\Program Files\Application\v1.2\run*.exe`

Es gelten die folgenden Einschränkungen:

- Der Platzhalter kann nur als Ersatz für ein einzelnes Verzeichnis verwendet werden. Beispiel: Die ausführbare Datei befindet sich in `C:\Program Files\Application\v1.2\run1.exe`
  - Zulässig: `C:\Program Files\Application\*\run1.exe`
  - Nicht zulässig: `C:\Program Files\*\run1.exe`
- Die Einträge müssen die Dateinamenserweiterung enthalten.
  - Zulässig: `C:\Program Files\Application\v1.2\*.exe`
  - Nicht zulässig: `C:\Program Files\Application\v1.2\*`
- Alle Pfade müssen lokale Pfade sein.

> **Hinweis:**
>
> - Netzwerkpfade sind nicht zulässig.
> - Wildcard-Unterstützung ist ab Citrix Virtual Apps and Desktops 2206 verfügbar.
> - Wildcard-Unterstützung ist in Citrix Virtual Apps and Desktops 2203 LTSR ab CU2 verfügbar.

Systemumgebungsvariablen verwenden

Sie können Systemumgebungsvariablen verwenden, um die Definition der vertrauenswürdigen Prozesse in Ihrer Positivliste zu vereinfachen. Sie können jede der vorbereiteten Variablen wie, `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` und `%systemroot%`.

Sie können auch benutzerdefinierte Umgebungsvariablen verwenden, sofern sie auf Systemebene definiert sind.

Die folgenden Beispiele zeigen sofort einsatzbereite Umgebungsvariablen:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

Das folgende Beispiel zeigt eine benutzerdefinierte Systemumgebungsvariable:

- Name der benutzerdefinierten Variablen: `app`
- Wert der benutzerdefinierten Variablen: `%programfiles%\Application\`
- Eintrag in Positivliste: `CTXCVC1,%app%\run.exe`

> **Hinweis:**
>
> Benutzerumgebungsvariablen werden nicht unterstützt.
>
> Die Unterstützung von Umgebungsvariablen ist ab Version 2209 von Citrix Virtual Apps and Desktops verfügbar.

Namen und Prozesse virtueller Kanäle erhalten

Die einfachste Art und Weise, den Namen eines virtuellen Kanals und den Prozess, der ihn auf der VDA-Maschine öffnet, in Erfahrung zu bringen, ist den Entwickler oder Drittanbieter des Kanals zu fragen.

Alternativ können Sie diese Informationen erhalten, indem Sie die Protokolle des Features anwenden und die folgenden Schritte einhalten:

1. Sobald die Client- und Serverkomponenten des benutzerdefinierten virtuellen Kanals bereit sind, starten Sie eine virtuelle Anwendung oder einen virtuellen Desktop.

2. Suchen Sie im Systemereignisprotokoll der VDA-Maschine den Namen des benutzerdefinierten virtuellen Kanals und den Prozess, der ihn zu öffnen versucht: Weitere Informationen zu verfügbaren Ereignissen finden Sie unter Ereignisprotokolle.
3. Melden Sie sich von der Sitzung ab.
4. Fügen Sie in der Richtlinieneinstellung für die Positivliste virtueller Kanäle einen Eintrag für den gefundenen virtuellen Kanal und den Prozess hinzu.
5. Starten Sie die Maschine neu.
6. Sobald der VDA registriert ist, führen Sie die virtuelle Anwendung oder den virtuellen Desktop aus, um zu überprüfen, ob die benutzerdefinierten virtuellen Kanäle erfolgreich geöffnet werden.

Überlegungen zu virtuellen Citrix-Kanälen

Alle integrierten virtuellen Citrix Kanäle haben eine Vertrauensstellung und können ohne weitere Konfiguration geöffnet werden. Zwei Features erfordern jedoch aufgrund externer Abhängigkeiten einen expliziten Eintrag in der Positivliste:

- Multimediaumleitung
- HDX RealTime Optimization Pack für Skype for Business

Multimediaumleitung

Wenn Sie einen anderen Media Player als Windows Media Player als System-Media Player verwenden, müssen Sie ihn als vertrauenswürdigen Prozess zur Positivliste hinzufügen. Folgende Informationen sind für den Eintrag in der Positivliste erforderlich:

- Name des virtuellen Kanals: `CTXMM`
- Prozess: Pfad zu dem auf dem VDA verwendeten Media Player. Beispiel: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Eintrag in Positivliste: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack für Skype for Business

Folgende Informationen sind für den Eintrag in der Positivliste erforderlich:

- Name des virtuellen Kanals: `CTXRMEP`
- Prozess: Pfad zu der Exe-Datei von Skype for Business auf der VDA-Maschine. Dieser variiert ggf. je nach Skype for Business-Version bzw. kann ein benutzerdefinierter Installationspfad sein. Zum Beispiel: `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.

- Eintrag in Positivliste: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Bereitstellungsmethoden

December 13, 2022

Eine einzige Bereitstellungsmethode wird wahrscheinlich nicht alle Anforderungen erfüllen.

Es stehen mehrere Methoden für die Anwendungsbereitstellung zur Auswahl. Die Auswahl der geeigneten Methode verbessert Skalierbarkeit, Verwaltung und Benutzererfahrung.

- **Installierte Apps:** Solche Apps sind Teil des grundlegenden Desktopimages. Bei der Installation werden DLL-, EXE- und andere Dateien auf das Image-Laufwerk kopiert und Registrierungsänderungen vorgenommen. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.
- **Gestreamte Apps (Microsoft App-V):** Für solche Apps wird eine Profilerstellung durchgeführt und die App werden bei Bedarf auf den Desktops im Netzwerk bereitgestellt. App-Dateien und Registrierungseinstellungen werden in einem Container auf dem virtuellen Desktop abgelegt und vom Basisbetriebssystem sowie untereinander isoliert. Diese Aktion erleichtert das Beheben von Kompatibilitätsproblemen. Einzelheiten finden Sie unter App-V.
- **Layer-Apps (Citrix App Layering)**: Jeder Layer enthält eine App, einen Agent oder ein Betriebssystem. Durch die Integration eines Betriebssystemlayers, eines Plattformlayers (z. B. VDA) und vieler App-Layer kann ein Administrator problemlos neue Images für die Bereitstellung erstellen. App Layering vereinfacht die Systempflege, da ein Betriebssystem, ein Agent und eine App auf einem einzelnen Layer ist. Wenn Sie den Layer aktualisieren, werden alle bereitgestellten Images aktualisiert, die diesen Layer enthalten. Siehe Citrix App Layering.
- **Gehostete Windows-App:** Eine Anwendung, die auf einem Citrix Virtual Apps-Host mit mehreren Benutzern installiert ist und als Anwendung und nicht als Desktop bereitgestellt wird. Benutzer greifen nahtlos über den VDI-Desktop oder das Endpunktgerät auf gehostete Windows-Apps zu, ohne dass sie bemerken, dass die App remote ausgeführt wird. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.
- **Lokale Apps:** auf dem Endpunktgerät bereitgestellte Apps. Die App-Schnittstelle wird in der gehosteten VDI-Sitzung des Benutzers angezeigt, obwohl die App auf dem Endpunkt ausgeführt wird. Einzelheiten finden Sie unter Lokaler App-Zugriff und URL-Umleitung.

Für Desktops können Sie über Citrix Virtual Apps veröffentlichte Desktops oder VDI-Desktops verwenden.

In Citrix Virtual Apps veröffentlichte Apps und Desktops

Verwenden Sie Multisitzungs-OS-Maschinen zum Bereitstellen von mit Citrix Virtual Apps veröffentlichten Anwendungen und Desktops.

Anwendungsfall:

- Gewünscht wird eine kostengünstige, serverbasierte Bereitstellung, um die Kosten für die Bereitstellung von Anwendungen für zahlreiche Benutzer gering zu halten, und gleichzeitig eine sichere High-Definition-Benutzererfahrung zu bieten.
- Die Benutzer führen vordefinierte Aufgaben aus, es wird keine Personalisierung oder kein Offlinezugriff auf Anwendungen benötigt. Hierzu können aufgabenorientierte Mitarbeiter, wie z. B. Callcenter- und Einzelhandelsarbeitskräfte gehören, oder Benutzer, die Arbeitsstationen gemeinsam verwenden.
- Anwendungstypen: beliebig

Vorteile und Überlegungen:

- Verwaltbare und skalierbare Lösung für das Datenzentrum.
- Kosteneffektivste Lösung für die Anwendungsbereitstellung.
- Gehostete Anwendungen werden zentral verwaltet und Benutzer können die Anwendung nicht ändern, wodurch eine konsistente, sichere und zuverlässige Benutzererfahrung bereitgestellt wird.
- Benutzer müssen online sein, um auf ihre Anwendungen zuzugreifen.

Benutzererfahrung:

- Benutzer fordern eine oder mehrere Anwendungen von StoreFront über ihr Startmenü oder eine von Ihnen vorgegebene URL an.
- Anwendungen werden virtuell bereitgestellt und in High Definition auf Benutzergeräten angezeigt.
- Abhängig von den Profileinstellungen werden Benutzeränderungen gespeichert, wenn die Anwendungssitzung des Benutzers beendet wird. Andernfalls werden die Änderungen werden gelöscht.

Verarbeiten, Hosten und Bereitstellen von Anwendungen:

- Die Anwendungsverarbeitung findet auf den Hostingmaschinen statt, nicht auf den Benutzergeräten. Die Hostingmaschine kann eine physische oder eine virtuelle Maschine sein.
- Anwendungen und Desktops sind auf einer Multisitzungs-OS-Maschine gespeichert.
- Maschinen werden über Maschinenkataloge verfügbar gemacht.
- Maschinen aus Maschinenkatalogen sind in Bereitstellungsgruppen organisiert, die Benutzergruppen dieselben Anwendungen bereitstellen.

- Multisitzungs-OS-Maschinen unterstützen Bereitstellungsgruppen, die Desktops, Anwendungen oder beides hosten.

Sitzungsverwaltung und -zuweisung:

- Auf Multisitzungs-OS-Maschinen werden mehrere Sitzungen auf einer einzelnen Maschine ausgeführt, über die mehrere Anwendungen und Desktops an mehrere, gleichzeitig verbundene Benutzer bereitgestellt werden. Jeder Benutzer benötigt eine einzelne Sitzung, um die gehosteten Anwendungen auszuführen.

  Beispiel: Ein Benutzer meldet sich an und fordert eine Anwendung an. Eine der Sitzungen auf dieser Maschine ist für die anderen Benutzer nicht mehr verfügbar. Ein zweiter Benutzer meldet sich an und fordert eine Anwendung an, die von dieser Maschine gehostet wird. Eine zweite Sitzung auf derselben Maschine ist damit jetzt nicht verfügbar. Wenn beide Benutzer weitere Anwendungen anfordern, werden keine zusätzlichen Sitzungen benötigt, da ein Benutzer mehrere Anwendungen in der gleichen Sitzung ausführen kann. Wenn zwei weitere Benutzer sich anmelden und Desktops anfordern, und zwei Sitzungen auf der Maschine verfügbar sind, hostet diese eine Maschine nun vier Sitzungen für vier verschiedene Benutzer.
- In der Bereitstellungsgruppe, der ein Benutzer zugewiesen ist, wird eine Maschine auf einem Server mit der geringsten Last ausgewählt. Ein Computer mit Sitzungsverfügbarkeit wird nach dem Zufallsprinzip zugewiesen und stellt einem Benutzer bei der Anmeldung Anwendungen bereit.

VM-gehostete Apps

Bereitstellen VM-gehosteter Anwendungen über Einzelsitzungs-OS-Maschinen

Anwendungsfall:

- Gewünscht wird eine clientbasierte Anwendungsbereitstellungslösung, die eine sichere, zentrale Verwaltung bietet und zahlreiche Benutzer pro Hostserver unterstützt. Benutzern sollen Anwendungen bereitstellt werden, die problemlos in High Definition angezeigt werden.
- Benutzer sind interne und externe Auftragnehmer, Partner aus Fremdunternehmen und andere vorläufige Teammitglieder. Sie benötigen keinen Offlinezugriff auf gehostete Anwendungen.
- Anwendungsarten: Anwendungen, die möglicherweise nicht gut mit anderen Anwendungen funktionieren oder mit dem Betriebssystem interagieren, z. B. .NET Framework. Dieser Typ von Anwendungen eignet sich gut für das Hosting auf virtuellen Maschinen.

Vorteile und Überlegungen:

- Anwendungen und Desktops auf dem Image werden sicher verwaltet, gehostet und auf Maschinen im Datenzentrum ausgeführt, womit eine kosteneffektivere Lösung für die Anwendungsbereitstellung bereitgestellt wird.

- Benutzer können bei der Anmeldung willkürlich einer Maschine in einer Bereitstellungsgruppe zugewiesen werden, die für das Hosting einer Anwendung konfiguriert ist. Sie können auch einem einzelnen Benutzer eine einzelne Maschine für die Anwendungsbereitstellung jedes Mal statisch zuweisen, wenn sich der Benutzer anmeldet. Bei statisch zugewiesenen Maschinen kann der Benutzer eigene Anwendungen auf der virtuellen Maschine installieren und verwalten.
- Das Ausführen mehrerer Sitzungen auf Maschinen mit Windows-Einzelsitzungs-OS wird nicht unterstützt. Daher beansprucht jeder Benutzer bei der Anmeldung eine einzelne Maschine innerhalb einer Bereitstellungsgruppe und der Zugriff auf die Anwendungen muss online erfolgen.
- Bei dieser Methode werden die Serverressourcen für die Verarbeitung von Anwendungen sowie der Speicher für die persönlichen vDisks der Benutzer möglicherweise erhöht.

Benutzererfahrung:

- Die gleiche nahtlose Anwendungserfahrung wie mit gehosteten, freigegebenen Anwendungen auf Maschinen mit Windows-Multisitzungs-OS.

Verarbeiten, Hosten und Bereitstellen von Anwendungen:

- Wie bei Maschinen mit Windows-Multisitzungs-OS, außer dass es sich um virtuelle Maschinen mit Windows-Einzelsitzungs-OS handelt.

Sitzungsverwaltung und -zuweisung:

- Maschinen mit Windows-Einzelsitzungs-OS führen eine Desktopsitzung von einer Maschine aus. Nur beim Zugriff auf Anwendungen: Ein Benutzer kann mehrere Anwendungen verwenden (und ist nicht auf eine Anwendung eingeschränkt). Das Betriebssystem sieht jede Anwendung als neue Sitzung an.
- Innerhalb einer Bereitstellungsgruppe erhalten angemeldete Benutzer entweder statischen Zugriff auf eine Maschine (d. h. bei jeder Anmeldung die gleiche Maschine) oder es wird ihnen eine Maschine nach Sitzungsverfügbarkeit zugewiesen.

VDI-Desktops

Verwenden Sie Einzelsitzungs-OS-Maschinen zum Bereitstellen von VDI-Desktops mit Citrix Virtual Desktops.

VDI-Desktops werden auf virtuellen Maschinen gehostet und bieten jedem Benutzer ein Desktopbetriebssystem.

VDI-Desktops benötigen mehr Ressourcen als mit Citrix Virtual Apps veröffentlichte Desktops, aber es ist nicht erforderlich, dass die auf ihnen installierten Anwendungen serverbasierte Betriebssysteme

unterstützen. Abhängig vom ausgewählten Typ des VDI-Desktops können Desktops außerdem einzelnen Benutzern zugewiesen werden. Dadurch können sie von Benutzern in hohem Maße personalisiert werden.

Beim Erstellen eines Maschinenkatalogs für VDI-Desktops erstellen Sie einen der folgenden Desktoptypen:

- **Zufälliger, nicht beständiger Desktop (gepoolter VDI-Desktop):** Jedes Mal, wenn sich ein Benutzer bei einem dieser Desktops anmeldet, wird ein Desktop aus einem Pool ausgewählt. Der Pool basiert auf einem einzelnen Image. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- **Statischer, nicht beständiger Desktop:** Während der ersten Anmeldung wird einem Benutzer ein Desktop aus einem Pool zugewiesen. (Jede Maschine im Pool basiert auf einem einzelnen Image.) Anschließend wird dem Benutzer bei jeder weiteren Anmeldung derselbe Desktop zugewiesen. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- **Statischer, permanenter Desktop:** Im Gegensatz zu anderen VDI-Desktoptypen können diese Desktops vollständig personalisiert werden. Während der ersten Anmeldung wird einem Benutzer ein Desktop aus einem Pool zugewiesen. Bei nachfolgenden Anmeldungen wird dem Benutzer derselbe Desktop wie beim ersten Mal zugewiesen. Alle Änderungen an dem Desktop bleiben erhalten, wenn die Maschine neu gestartet wird.

Remote-PC-Zugriff

Remote-PC-Zugriff ist eine Funktion von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service), mit der Organisationen ihren Mitarbeitern einfach und sicher Zugriff auf Unternehmensressourcen geben können. Die Citrix-Plattform ermöglicht diesen sicheren Zugriff, indem Benutzer Zugriff auf ihre physischen Büro-PCs erhalten. Wenn Benutzer auf ihre Büro-PCs zugreifen können, können sie auf alle Anwendungen, Daten und Ressourcen zugreifen, die sie für ihre Arbeit benötigen. Mit Remote-PC-Zugriff ist das Einführen und Bereitstellen anderer Tools für die Telearbeit überflüssig. Zum Beispiel virtuelle Desktops oder Anwendungen und die zugehörige Infrastruktur.

Remote-PC-Zugriff verwendet dieselben Citrix DaaS-Komponenten zum Bereitstellen von virtuellen Desktops und Anwendungen. Daher sind die Anforderungen und der Prozess für die Bereitstellung und Konfiguration des Remote-PC-Zugriffs die gleichen wie für die Bereitstellung von virtuellen Ressourcen mit Citrix DaaS. Diese Einheitlichkeit bietet eine konsistente und gemeinsame administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Sitzungen verwenden.

Informationen finden Sie unter Remote-PC-Zugriff.

Erste Schritte: Planen und Erstellen einer Bereitstellung

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Wenn Sie mit den Komponenten, der Terminologie und den Objekten von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) nicht vertraut sind, finden Sie entsprechende Informationen unter Citrix DaaS.

Die Customer Journey-Perspektive finden Sie im Citrix Success Center. Das Success Center bietet Unterstützung bei den fünf wichtigsten Phasen der Citrix Journey: Planen, Erstellen, Rollout, Verwalten und Optimieren.

- Die Informationen im Success Center sind eine wichtige Ergänzung dieser Produktdokumentation.
- Die Artikel und Leitfäden im Success Center bieten eine weite, lösungsbasierte Perspektive. Sie enthalten auch Links zu servicespezifischen Details in der vorliegenden Produktdokumentation.

Wenn Sie von einer Citrix Virtual Apps and Desktops-Bereitstellung migrieren, lesen Sie Migrieren in die Cloud.

> **Wichtig:**
>
> Damit Sie wichtige Informationen über Citrix Cloud und die von Ihnen abonnierten Citrix Services erhalten, stellen Sie sicher, dass Sie alle E-Mail-Benachrichtigungen erhalten.
>
> Erweitern Sie in der oberen rechten Ecke der Citrix Cloud-Konsole das Menü rechts neben den Feldern "Kundenname"und "Organisations-ID". Wählen Sie **Kontoeinstellungen**. Wählen Sie auf der Registerkarte **Mein Profil** alle Einträge im Abschnitt **E-Mail-Benachrichtigungen** aus.

Nutzung dieses Artikels

Führen Sie beim Einrichten Ihrer Citrix DaaS-Bereitstellung die nachfolgend aufgeführten Aufgaben aus. Zu den Details jeder Aufgabe werden Links bereitgestellt.

Machen Sie sich mit dem gesamten Prozess vertraut, bevor Sie mit der Bereitstellung beginnen, damit Sie wissen, was zu erwarten ist. Der Artikel enthält auch Links zu anderen Informationsquellen.

> **Hinweis:**
>
> Wenn Sie die Quick Deploy-Schnittstelle zum Bereitstellen von Microsoft Azure-Maschinen verwenden möchten, folgen Sie den Anweisungen zur Einrichtung unter Erste Schritte mit Quick Deploy.

Planung und Vorbereitung

Verwenden Sie die Informationen unter Plan im Success Center, um Ziele festzulegen, Anwendungsfälle und Geschäftsziele zu definieren, potenzielle Risiken zu identifizieren und einen Projektplan zu erstellen.

In der Citrix Tech Zone-Dokumentation finden Sie einen schrittweisen Leitfaden für Service-Machbarkeitsstudien.

Registrierung

Einrichten eines Citrix Kontos und Anfordern einer Citrix DaaS-Demoversion

Ressourcenstandort einrichten

Ein Ressourcenstandort enthält die Ressourcen zur Bereitstellung von Anwendungen und Desktops für Benutzer. Durch das Erstellen von Ressourcenstandorten kann DaaS diese Ressourcen nutzen. Weitere Informationen zu Ressourcenstandorten finden Sie unter Verbinden mit Citrix Cloud.

Bevor Sie Maschinen erstellen, müssen Sie einen Ressourcenstandort mit DaaS verbinden:

- Bei domänengebundenen Maschinen müssen Cloud Connectors am Ressourcenstandort installiert sein. Dies ermöglicht Folgendes:
  - On-Premises-Kataloge mit Einbindung in Active Directory erstellen
  - Kataloge mit Einbindung in Azure Active Directory erstellen
  - Kataloge mit Azure Active Directory-Hybrideinbindung erstellen

  Für eine hohe Verfügbarkeit empfehlen wir, an jedem Ressourcenstandort zwei Cloud Connectors zu installieren. Siehe Cloud Connector-Installation.

  Weitere Informationen:

  - Was sind Ressourcenstandorte und Cloud Connectors?

  - Video zur Installation von Cloud Connectors:

- Nicht domänengebundene Maschinen benötigen keine Cloud Connectors, erfordern jedoch, dass Rendezvous V2 aktiviert ist. Durch das Rendezvous-Protokoll können VDAs die Cloud Connectors umgehen und eine sichere Direktverbindung zu DaaS herstellen. Siehe Rendezvous V2. Dies ermöglicht Folgendes:

  - Nicht in eine Domäne eingebundene Kataloge erstellen

Wenn Sie Azure-VMs mit der Quick Deploy-Schnittstelle bereitstellen, erstellt Citrix den Ressourcenstandort und Cloud Connectors für Sie.

Erstellen einer Verbindung zum Ressourcenstandort

Nachdem Sie einen Ressourcenstandort und Cloud Connectors hinzugefügt haben, erstellen Sie eine Verbindung zum Ressourcenstandort über die Oberfläche "Vollständige Konfiguration"von Citrix DaaS.

Dieser Schritt ist in folgenden Fällen nicht notwendig:

- Sie erstellen eine einfache Machbarkeitsstudie.
- Sie verwenden die Quick Deploy-Schnittstelle zum Bereitstellen von Azure-VMs.

Weitere Informationen:

- Was sind Hosts?
- Was sind Hostverbindungen?

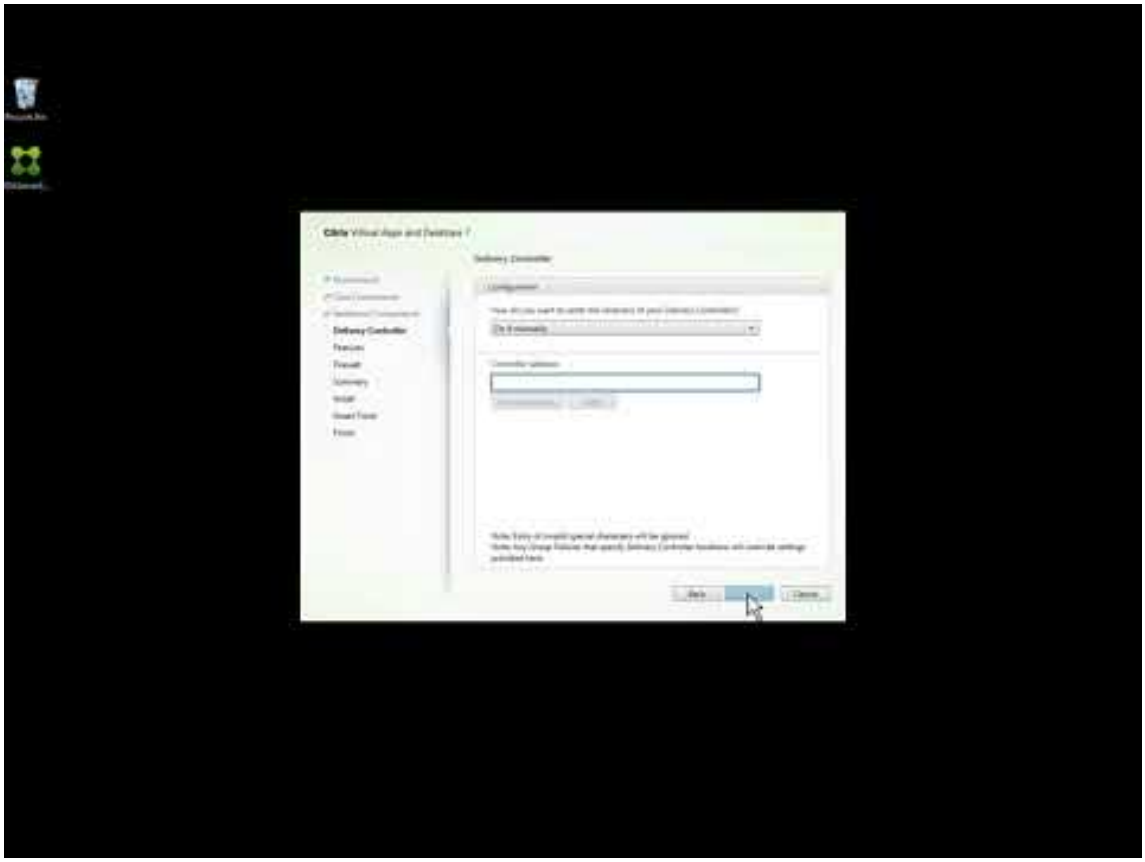
VDAs installieren

Auf jeder Maschine, über die Anwendungen und Desktops bereitgestellt werden, muss ein Citrix Virtual Delivery Agent (VDA) installiert sein.

- Für eine einfache Proof of Concept-Bereitstellung laden Sie einen VDA herunter und installieren Sie ihn auf einer Maschine.
- Wenn Sie VMs über ein Image bereitstellen, installieren Sie auf dem Image einen VDA.
- Installieren Sie für Remote-PC-Zugriff-Bereitstellungen die Kernversion des VDAs für Einzelsitzungs-OS auf jedem Büro-PC.

Anleitungen und weitere Informationen:

- Was sind VDAs?
- Vorbereiten und Durchführen der Installation
- VDA-Installation über die Befehlszeile
- Video zum Herunterladen und Installieren eines VDA:

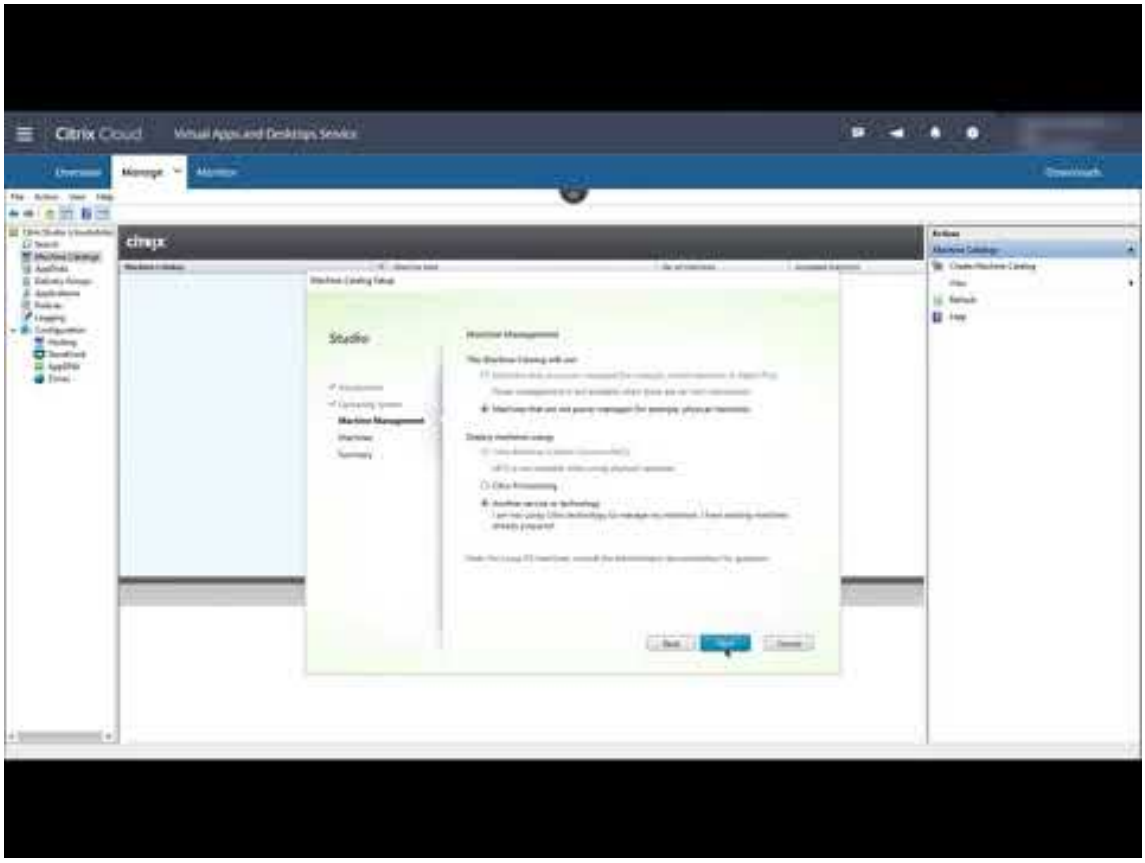


Katalog erstellen

Nach dem Erstellen einer Verbindung zum Resourcenstandort erstellen Sie einen Katalog. Wenn Sie die Oberfläche “Vollständige Konfiguration”verwenden, führt Sie der Workflow automatisch zu diesem Schritt.

Anleitungen und weitere Informationen:

- Was sind Kataloge?
- Katalog erstellen
- Verwenden Sie die Quick Deploy-Oberfläche zur Bereitstellung eines Katalogs mit Azure-VMs.
- Video zum Erstellen eines Katalogs mit der Verwaltungsschnittstelle der vollständigen Konfiguration:



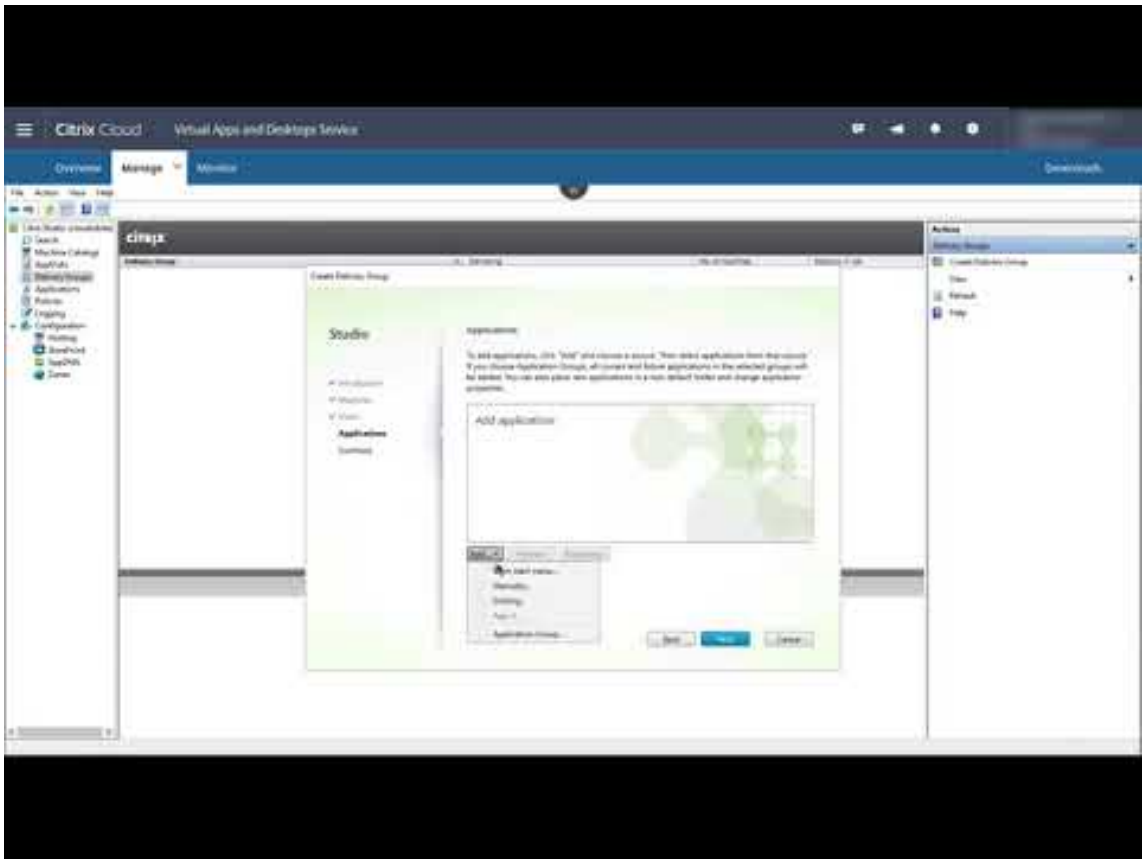
Bereitstellungsgruppe erstellen

Wenn Sie den ersten Katalog erstellt haben, werden Sie vom **Verwalten**-Workflow durch die Erstellung einer Bereitstellungsgruppe geführt.

Dieser Schritt ist nicht erforderlich, wenn Sie die Quick Deploy-Schnittstelle zur Bereitstellung von Azure-VMs verwenden.

Anleitungen und weitere Informationen:

- Was sind Bereitstellungsgruppen?
- Bereitstellungsgruppe erstellen
- Video zum Erstellen einer Bereitstellungsgruppe:



Bereitstellen anderer Komponenten und Technologien

Nachdem Sie die Aufgaben oben ausgeführt haben, die die Citrix DaaS-Bereitstellung einrichten, folgen Sie den Anweisungen im Bereich Build des Citrix Success Centers. Sie finden Informationen zum Provisioning und zur Konfiguration anderer Komponenten und Technologien der Citrix Lösung, z. B.:

- Citrix-Richtlinien
- StoreFront
- App Layering
- Workspace Environment Management (WEM) Service
- Citrix Gateway Service
- Zonen

- Verbundauthentifizierungsdienst (FAS)

Führen Sie andere Aufgaben aus, die möglicherweise auf Ihre Konfiguration zutreffen. Wenn Sie beispielsweise Windows Server-Workloads bereitstellen möchten, konfigurieren Sie einen Microsoft RDS-Lizenzserver.

Starten von Anwendungen und Desktops

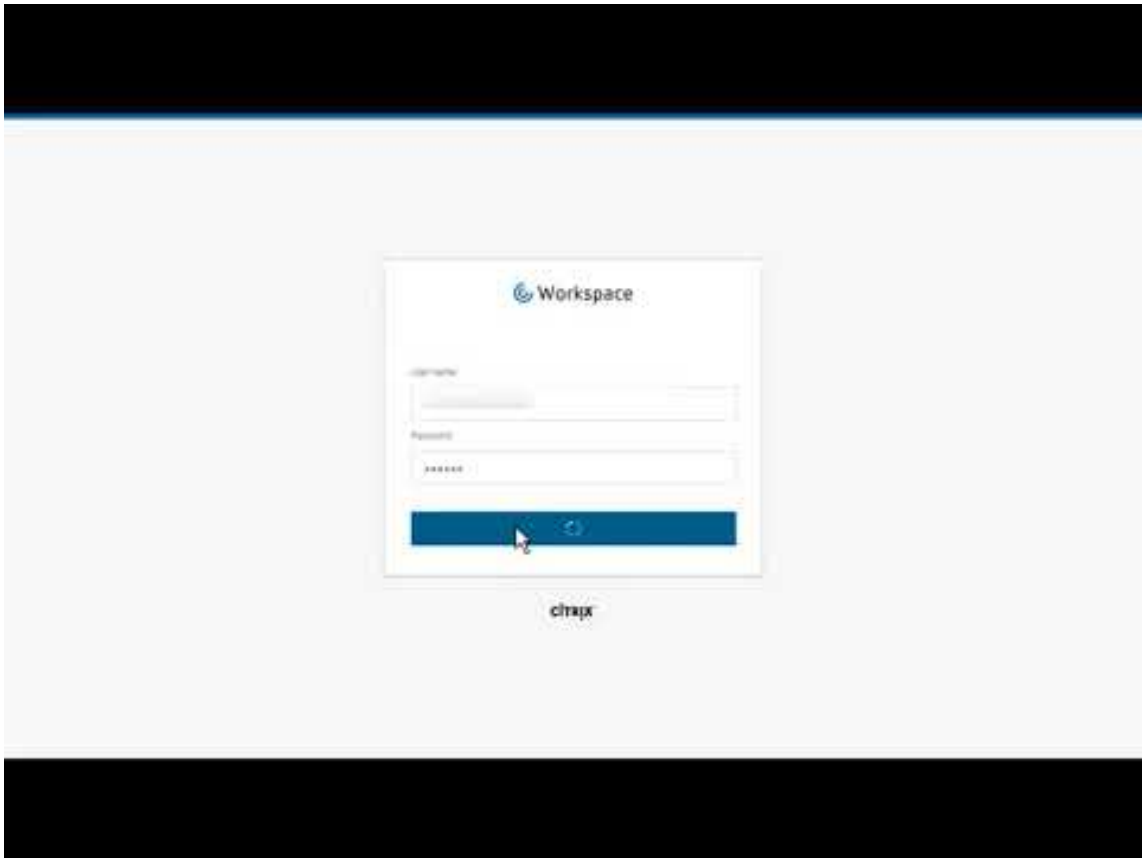
Nachdem Sie Ihre Bereitstellung konfiguriert haben, erfolgt die Veröffentlichung automatisch. Die von Ihnen konfigurierten Anwendungen und Desktops stehen dann Benutzern in ihrem Citrix Workspace zur Verfügung. Ein Benutzer gibt einfach seine Workspace-URL ein und wählt eine Anwendung oder einen Desktop aus, die danach sofort gestartet werden.

Senden Sie die Workspace-URL an die Benutzer. Sie finden die Workspace-URL an zwei Stellen:

- Klicken Sie in der Citrix Cloud-Konsole im Menü links oben auf **Workspacekonfiguration**. Die Registerkarte **Zugriff** enthält die Workspace-URL.
- Auf der Seite **Übersicht** in Citrix DaaS wird im unteren Seitenbereich die Workspace-URL angezeigt.

Weitere Informationen:

- Video zum Starten von Anwendungen und Desktops im Workspace durch Benutzer:



Weitere Informationen

Die Citrix Cloud Learning-Serie bietet Schulungskurse für verschiedene Lernpfade:

- Wenn Sie noch nicht mit Citrix DaaS vertraut sind, lesen Sie den Artikel New to Citrix DaaS Learning Path.
- Wenn Sie von einer Bereitstellung von Citrix Virtual Apps and Desktops migrieren, lesen Sie Migrating Citrix DaaS to Citrix Cloud Learning Path.

Registrierung bei Citrix DaaS

May 25, 2022

Einführung

Sie können Citrix DaaS über Citrix oder über Azure Marketplace abonnieren.

Wenn Sie planen, Citrix Managed Azure zu verwenden, können Sie auch den Citrix Azure Consumption Fund bestellen (über Citrix oder über Azure Marketplace).

- Bei einer Bestellung über Citrix können Sie Citrix DaaS und Citrix Azure Consumption Fund gleichzeitig bestellen.
- Bei einer Bestellung über Azure Marketplace bestellen Sie zuerst Citrix DaaS. Anschließend können Sie separat den Citrix Azure Consumption Fund bestellen.

Wenn Sie zunächst nur Citrix DaaS bestellen, können Sie den Citrix Azure Consumption Fund später über Azure Marketplace oder über Ihren Citrix Kontobetreuer bestellen.

Demos und Testversionen

Sie können Citrix DaaS auf Anfrage über Citrix evaluieren. Sie können eine Testversion in ein kostenpflichtiges Dienstabonnement überführen.

Während Sie eine Testversion verwenden, können Sie optional ein Citrix Managed Azure-Abonnement für Kataloge, Images und Netzwerkverbindungen nutzen. Wenn Sie von Citrix verwaltete Ressourcen verwenden und zu einem kostenpflichtigen Abonnement wechseln, müssen Sie entweder einen Consumption Fund erwerben oder die von Citrix verwalteten Ressourcen löschen. Wenn Sie keinen Consumption Fund erwerben, werden diese Ressourcen automatisch gelöscht, was sich auf Benutzer auswirken kann.

Bei vorhandenem Citrix DaaS-Abonnement

Generell kann mit einem Citrix Cloud-Konto nur ein einziger Citrix DaaS-Service (oder nur eine Edition) pro Citrix OrgID abonniert werden. Sie können beispielsweise Citrix DaaS Premium Edition ODER Citrix DaaS Standard für Azure abonnieren, aber nicht beides.

Wenn Sie bereits einen Citrix DaaS-Service abonnieren und nun diesen Dienst abonnieren möchten, haben Sie zwei Möglichkeiten:

- Abonnieren Sie den Dienst über ein anderes Citrix Cloud-Konto (OrgID).
- Kündigen Sie das bestehende Citrix DaaS-Abonnement, und bestellen Sie dann diesen Dienst. Anweisungen zur Außerbetriebnahme von Diensten finden Sie unter CTX239027.

Bestellen über Citrix

Sie können diesen Dienst (und den Citrix Azure Consumption Fund) über Citrix Cloud oder über Ihren Citrix Kontobetreuer bestellen.

Über Citrix Cloud:

- Folgen Sie den Anweisungen unter Bei Citrix Cloud registrieren, um ein Citrix Cloud-Konto und eine Organisations-ID zu erhalten.
- Sie können eine Demoversion von Citrix DaaS anfordern. Klicken Sie auf der Kachel für Citrix DaaS auf **Demo anfordern**. Geben Sie die angeforderten Informationen an.

  Ein Citrix Mitarbeiter wird sich mit Ihnen in Verbindung setzen, um Ihre Anforderungen, Umgebung und Pläne zu besprechen. Je nach Einschätzung unseres Vertreters erhalten Sie Zugang zu einer Administratordemo oder einer Proof-of-Concept-Testversion. Weitere Informationen finden Sie unter Citrix Cloud Service - Testversionen.

Wenn Sie Zugriff auf die Testversion erhalten, wird auf der Citrix DaaS-Kachel in der Citrix Cloud-Konsole **Verwalten** angezeigt.

Bestellen über Azure Marketplace

Sie können die folgenden Citrix-Angebote über Azure Marketplace bestellen:

- Citrix DaaS für Azure
- Citrix DaaS Advanced Edition
- Citrix DaaS Premium Edition
- Workspace Premium Plus

Wenn Sie planen, Citrix Virtual Apps and Desktops-Workloads auf Microsoft Azure zu hosten und ein Citrix Managed Azure-Abonnement verwenden möchten, bestellen Sie erst Citrix DaaS oder Workspace Premium Plus und dann den Citrix Azure Consumption Fund.

Mit dem Citrix Azure Consumption Fund wird Ihnen jeden Monat Ihr Verbrauch in Rechnung gestellt, der je nach Auswahl der gehosteten Ressourcen und Nutzungszeiten variieren kann. Sie können Ihren Verbrauch über Citrix Cloud prüfen.

Über Azure Marketplace:

- Sie können Citrix DaaS und den Consumption Fund nicht gleichzeitig bestellen.
- Der Bestellprozess für Citrix DaaS und den Citrix Azure Consumption Fund ist zwar im Wesentlichen identisch, Sie müssen jedoch zuerst Citrix DaaS bestellen.

Voraussetzungen für die Bestellung über Azure Marketplace

- Die OrgID Ihres Citrix Cloud-Kontos.
  - Wenn Sie bereits ein Citrix Cloud-Konto haben, finden Sie die OrgID in der rechten oberen Ecke der Citrix Cloud-Konsole. Oder prüfen Sie die E-Mail, die Sie beim Erstellen des Kontos erhalten haben.

  - Wenn Sie noch kein Citrix Cloud-Konto besitzen, befolgen Sie die Anweisungen unter Registrierung bei Citrix Cloud.

- Ein Azure-Konto und mindestens ein Azure-Abonnement in diesem Konto.

Vorgehensweise für die Bestellung über Azure Marketplace

Führen Sie folgende Schritte aus, um Citrix DaaS oder Workspace Premium Plus über Azure Marketplace zu bestellen. (Um Citrix Managed Azure zu verwenden, bestellen Sie zuerst Citrix DaaS und dann in einer zweiten Bestellung den Citrix Azure Consumption Fund.)

1. Melden Sie sich bei Azure Marketplace mit den Anmeldeinformationen Ihres Azure-Kontos an.
2. Suchen Sie nach dem gewünschten Citrix-Angebot und rufen Sie es auf.
3. Wählen Sie **Jetzt herunterladen**.
4. Geben Sie in der Nachricht **One more thing…** die erforderlichen Informationen ein, aktivieren Sie das Kontrollkästchen zur Einwilligung und wählen Sie **Weiter**.
5. Prüfen Sie die Registerkarten mit Informationen zu Produkt, Abonnement, Preisen und Verwendung. Wählen Sie ein Abonnement aus (falls mehrere verfügbar sind) und wählen Sie **Set up + subscribe**.
6. Auf der Registerkarte **Basics**:
   - **Subscription:** Anzeige des ausgewählten Abonnements.
   - **Ressourcengruppe:** Erstellen Sie eine Ressourcengruppe oder wählen Sie eine aus.
   - **Name:** Geben Sie einen Namen für Ihre Abonnementbestellung ein, damit Sie sie später leicht identifizieren können.
   - Unter **Plan** wird der Preis des ausgewählten Abonnements basierend auf dem Abrechnungszeitraum angezeigt. Um die Laufzeit des Abonnements zu ändern, wählen Sie **Change plan**. Wählen Sie die gewünschte Laufzeit und dann **Change plan**.
7. Prüfen Sie auf der Registerkarte **Review + subscribe** die Kontaktinformationen und aktualisieren Sie sie bei Bedarf. Prüfen Sie die allgemeinen Abonnementinformationen. Wählen Sie **Subscribe**.
8. Wählen Sie auf der Seite **Subscription in progress** die Option **Configure account now**. (Warten Sie kurz, falls die Schaltfläche deaktiviert ist.) Sie werden zu einer Citrix Aktivierungsseite weitergeleitet.
9. Auf der Aktivierungsseite:
   - Verwenden Sie den Link **Anmelden**, um sich bei Citrix Cloud anzumelden. Bei einer erfolgreichen Anmeldung wird das Feld **Organisations-ID** automatisch ausgefüllt.

- **Anzahl:** Geben Sie die Anzahl der Benutzer ein. (Eine Erstbestellung muss mindestens 25 Benutzer umfassen.) Ein geschätzter Preis wird angezeigt.
- Stimmen Sie den Geschäftsbedingungen zu und wählen Sie **Activate Order**.

Nach der Bestellung über Azure Marketplace

Sobald der Dienst für Sie bereitgestellt ist, erhalten Sie eine E-Mail von Citrix. Das Provisioning kann eine Weile dauern. Sollten Sie bis zum folgenden Tag keine E-Mail erhalten haben, wenden Sie sich bitte an den Citrix Support. Nachdem Sie die E-Mail von Citrix erhalten haben, können Sie Citrix DaaS verwenden.

Das Freischalten eines bestellten Citrix Azure Consumption Fund dauert nicht lange. Sobald Citrix über Ihre Bestellung informiert ist, wird in der Konsole von Citrix DaaS in einem Banner angezeigt, dass ein Citrix Managed Azure-Abonnement für Sie vorbereitet wird.

Löschen Sie nicht die Citrix DaaS-Ressource in Azure. Durch das Löschen dieser Ressource wird Ihr Abonnement gekündigt.

Bestellung über Google Cloud Marketplace

Sie können die folgenden Citrix-Angebote über Google Cloud Marketplace bestellen:

- Citrix DaaS Standard für Google Cloud
- Citrix DaaS Premium für Google Cloud

Für Bestellungen über Google Cloud Marketplace benötigen Sie Folgendes:

- Die OrgID Ihres Citrix Cloud-Kontos.
  - Wenn Sie bereits ein Citrix Cloud-Konto haben, finden Sie die OrgID in der rechten oberen Ecke der Citrix Cloud-Konsole. Oder prüfen Sie die E-Mail, die Sie beim Erstellen des Kontos erhalten haben.
  - Wenn Sie noch kein Citrix Cloud-Konto besitzen, befolgen Sie die Anweisungen unter Registrierung bei Citrix Cloud.
- Ein Google Cloud-Konto und mindestens ein Google Cloud-Abonnement in diesem Konto.

Schrittfolge zum Aufgeben Ihrer Bestellung:

1. Melden Sie sich bei Google Cloud Marketplace an.
2. Folgen Sie den Anweisungen auf der Seite Citrix DaaS für Google Cloud, um Ihren Kauf zu tätigen.

Sobald der Dienst für Sie bereitgestellt ist, erhalten Sie eine E-Mail von Citrix. Das Provisioning kann eine Weile dauern. Sollten Sie bis zum folgenden Tag keine E-Mail erhalten haben, wenden Sie sich bitte an den Citrix Support. Nachdem Sie die E-Mail von Citrix erhalten haben, können Sie Citrix DaaS verwenden.

Löschen Sie nicht die Citrix DaaS-Ressource in Google Cloud. Durch das Löschen dieser Ressource wird Ihr Abonnement gekündigt.

Nächste Schritte

Nachdem Ihre Bestellung bereitgestellt ist, fahren Sie mit den nächsten Schritten in Planen und Erstellen einer Bereitstellung fort.

Beispiel:

- Wenn Sie nicht bereits einen Hypervisor oder Cloudservice, bzw. Active Directory eingerichtet haben, lesen Sie den Artikel Einrichten des Ressourcenstandorts.
- Wenn die Hostumgebung und Active Directory eingerichtet sind, lesen Sie den Abschnitt Erstellen einer Verbindung.

Citrix HDX Plus für Windows 365

April 18, 2024

Mit Citrix HDX Plus für Windows 365 können Sie Citrix Cloud mit Windows 365 integrieren, um mit Citrix HDX-Technologien den Einsatz von Windows 365 Cloud-PC besser und sicherer zu gestalten und die Verwaltbarkeit mit weiteren Clouddienste zu verbessern.

Weitere Informationen finden Sie unter Citrix HDX Plus für Windows 365.

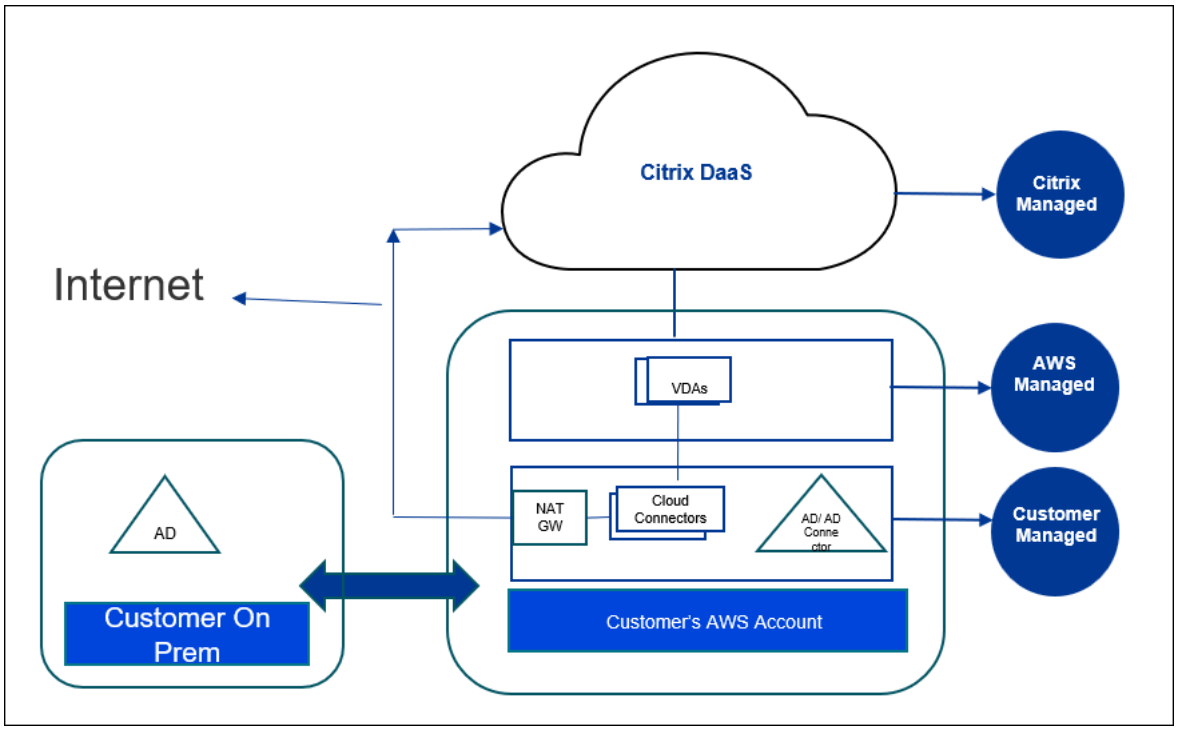
Citrix DaaS für Amazon WorkSpaces Core (Preview)

May 22, 2024

Einführung

In diesem Artikel wird beschrieben, wie Sie eine Bereitstellung mit Citrix für Amazon WorkSpaces Core vorbereiten und erstellen. Amazon WorkSpaces Core befindet sich in Amazon Web Services (AWS).

Das Folgende ist die Darstellung der AWS-Implementierung und ihrer Verwaltung mit Citrix DaaS:



Über diesen Preview

- Wenn Sie während diesem Preview Unterstützung benötigen, wenden Sie sich an den AWS Support oder den Citrix Support.
- Um die Citrix-Umgebung während dieses Previews zu verwalten, verwenden Sie nur die **Verwaltungskonsole** in Citrix DaaS. In diesem Preview werden keine Citrix- oder AWS-APIs unterstützt. (Citrix freut sich über Ihr Feedback zu APIs, die Sie in Zukunft verwenden möchten.)

Bereitstellung vorbereiten und erstellen

Die Bereitstellungscheckliste in der **Quick Deploy**-Benutzeroberfläche enthält Links zu den Verfahren 1-5.

1. Bevor Sie beginnen, erfüllen Sie die Voraussetzungen in Citrix Cloud und AWS.
2. Erstellen Sie einen Ressourcenstandort in Citrix Cloud. (Dieses Verfahren ist ebenfalls als Voraussetzung enthalten.)
3. Verbinden Sie Ihr AWS-Konto. Dieses Verfahren aktiviert Berechtigungen, damit Citrix DaaS eine Verbindung zu AWS herstellen kann.
4. Erstellen Sie eine Verzeichnisverbindung. Dieses Verfahren konfiguriert eine Verbindung, die den Zugriff auf das Active Directory Ihrer Organisation ermöglicht.

5. Importieren Sie ein Image. Mit diesem Verfahren können Sie eine Benutzeroberfläche für die Desktops Ihrer Benutzer erstellen.
6. Erstellen einer Bereitstellung. In diesem Verfahren werden die bereitzustellenden Maschinen und die Benutzer festgelegt, die über Citrix Workspace darauf zugreifen können.

Vorbereitung

Achten Sie darauf, dass Sie die folgenden Aufgaben abgeschlossen haben, bevor Sie mit der Vorbereitung und Erstellung Ihrer Bereitstellung beginnen.

Es gibt eine Ausnahme: Das Erstellen eines Ressourcenstandorts in Citrix Cloud ist unter den Voraussetzungen aufgeführt. Es ist auch das erste Verfahren in der Bereitstellungscheckliste. Wenn Sie also den Ressourcenstandort als Teil der Voraussetzungen erstellen, überspringen Sie dieses Verfahren in der Reihenfolge der Checkliste. Falls Sie es nicht zuvor getan haben, führen Sie es als erstes in der Checkliste aus.

Zu erfüllende Voraussetzungen in Citrix Cloud

- Erstellen Sie ein Citrix Cloud-Konto und abonnieren Sie Citrix DaaS. Ihr Citrix-Vertreter kann Ihnen dabei helfen. Ihr Vertreter aktiviert dieses Preview-Feature auch für Sie.
- Erstellen Sie einen Citrix Cloud-Ressourcenstandort. (Dieses Verfahren ist auch in der Quick Deploy-Benutzeroberfläche verlinkt.)

Zu erfüllende Voraussetzungen in AWS

- Erstellen Sie ein AWS-Benutzerkonto. Das Konto muss über Folgendes verfügen:
  - Rollenberechtigungen für den Citrix API-Client.
  - Berechtigungen für den programmgesteuerten Zugriff. Weitere Informationen finden Sie unter Berechtigungen für den programmgesteuerten Zugriff auf AWS-Konten.
  - Erstellen Sie die Rolle workspaces_DefaultRole. Weitere Informationen finden Sie unter Rolle workspaces_DefaultRole erstellen.
- In Ihrem Active Directory:
  - Verwenden Sie die AD Connector-Option, um Informationen zu speichern und zu verwalten. Weitere Informationen finden Sie unter AD Connector.
  - Erstellen Sie eine Organisationseinheit, in der VMs erstellt werden. Diese Organisationseinheit muss über eine Citrix-Richtlinie für die Kommunikation mit den Cloud Connectors und Citrix Cloud verfügen. Weitere Informationen finden Sie unter den Querverweisen.
  - Richten Sie eine Gruppenrichtlinie für die Citrix Cloud Connector-Konfiguration ein:

1. Laden Sie die neueste Gruppenrichtlinien-Verwaltungskonsole von Citrix (Citrix-GroupPolicyManagement_64.msi) von der Citrix-Downloadsite herunter.
2. Installieren Sie das MSI (auf diesem Computer muss die Visual Studio 2015-Runtime installiert sein). Erstellen Sie dann eine Citrix-Richtlinie, die die Controller-Richtlinieneinstellung enthält. Diese Einstellung gibt die Cloud Connector-Adressen an.

- Erstellen oder verwenden Sie ein vorhandenes NAT-Gateway. Weitere Informationen finden Sie unter NAT-Gateway.
- Erstellen oder verwenden Sie eine oder mehrere vorhandene Sicherheitsgruppen, die es den Citrix Cloud Connectors ermöglichen, mit den bereitgestellten VMs zu kommunizieren. Weitere Informationen finden Sie unter Datenverkehr zu Ihren AWS-Ressourcen mit Sicherheitsgruppen steuern
- Öffnen Sie ein AWS-Support-Ticket, um BYOL in Ihrem Konto zu aktivieren. Um zu beginnen, wenden Sie sich an Ihren AWS-Kundenbetreuer, Vertriebsmitarbeiter oder an das AWS Support Center. Ihr Kontakt wird BYOL verifizieren und aktivieren. Weitere Informationen finden Sie unter BYOL für Ihr Konto für BYOL mithilfe der Amazon WorkSpaces-Konsole aktivieren.

  > **Hinweis:**
  >
  > Die Versionen Windows 10 N und Windows 11 N werden derzeit für BYOL nicht unterstützt.

  - Durch die Verwendung der Citrix DaaS for Amazon WorkSpaces Core-Funktion wird automatisch die BYOP-Funktion (Bring Your Own Protocol) in AWS WorkSpaces Core aktiviert.
  - Sie müssen über ausreichende Windows 10-Lizenzen für die Desktops verfügen, die erstellt werden. Weitere Informationen finden Sie unter Bring Your Own Windows Desktoplizenzen.

Allgemeine Vorbereitung

Überprüfen Sie jedes Verfahren, bevor Sie beginnen. Vorteil: Dadurch können die Prozesse einfach abgeschlossen werden.

Ressourcenstandort erstellen

Sie erstellen einen Ressourcenstandort in Citrix Cloud.

- Ein Ressourcenstandort enthält zwei oder mehr Cloud Connectors, die mit Citrix Cloud kommunizieren. Die Server, auf denen Sie die Cloud Connectors installieren, müssen sich in einer EC2-VPC befinden, einer Domäne angehören und über eine Internetverbindung verfügen. Die Cloud Connectors müssen sich in derselben VPC befinden wie das Verzeichnis, das Sie verwenden möchten.

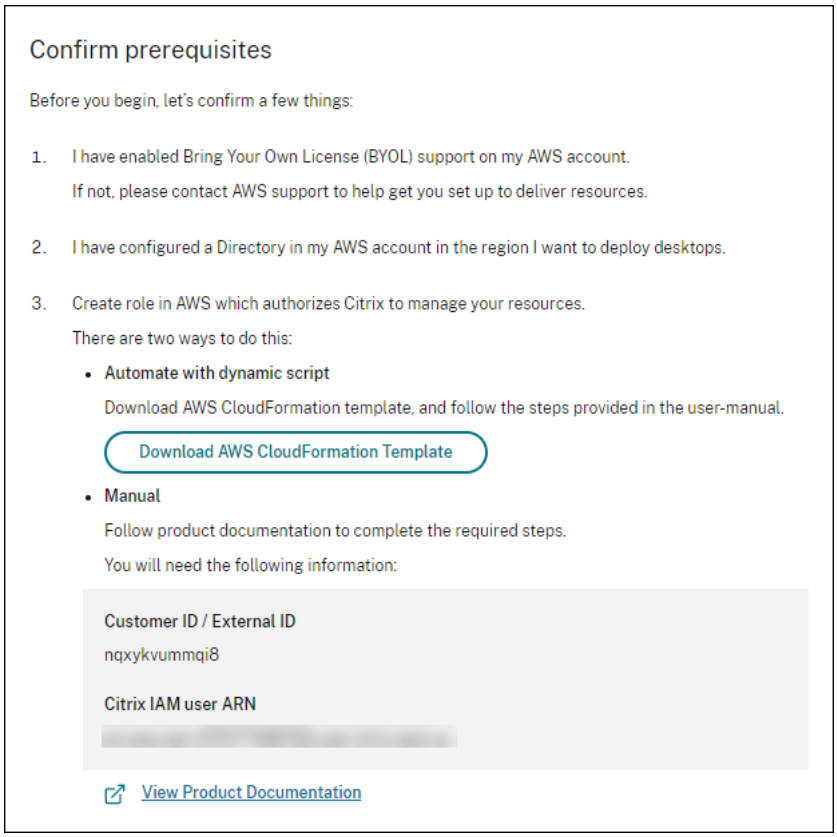
- Weitere Informationen zu Cloud Connectors finden Sie unter Citrix Cloud Connector und dem Verfahren zu deren Bereitstellung.
- Der Ressourcenstandort kann auch Ihre Active Directory-Server enthalten. Weitere Informationen finden Sie unter Active Directory mit Citrix Cloud verbinden.

Ihr AWS-Konto verbinden

Dieses Verfahren aktiviert Berechtigungen für Citrix DaaS, eine Verbindung zu AWS herzustellen.

Gehen Sie folgendermaßen vor, um AssumeRole für AWS WorkSpaces Core zu erstellen:

1. Klicken Sie in Citrix DaaS unter **Verwalten > Quick Deploy > Konten** auf **Konto verbinden**.
2. Klicken Sie auf der Seite **AWS-Konto verbinden** unter **Voraussetzungen bestätigen** auf **AWS CloudFormation-Vorlage herunterladen**. Nachdem die Vorlage heruntergeladen wurde, klicken Sie auf **Weiter**.



1. Informationen zum Hochladen der Vorlage finden Sie unter AssumeRole für die AWS Workspace Core-Integration erstellen.
2. Fügen Sie auf der Seite **Konto authentifizieren** den **Amazon-Ressourcennamen** (ARN) hinzu, der im Feld **Rollen-ID** generiert wurde, geben Sie einen Namen in das Feld **Name** ein und klicken Sie auf **Weiter**. Die Seite **Region auswählen** wird geöffnet.

Die **Rollen-ID** entspricht dem ARN der Rolle, die Citrix zur Verwaltung der Ressourcen autorisiert. Die Rollen-ID finden Sie in der AWS-Managementkonsole, indem Sie zu **IAM > Rollen** navigieren.

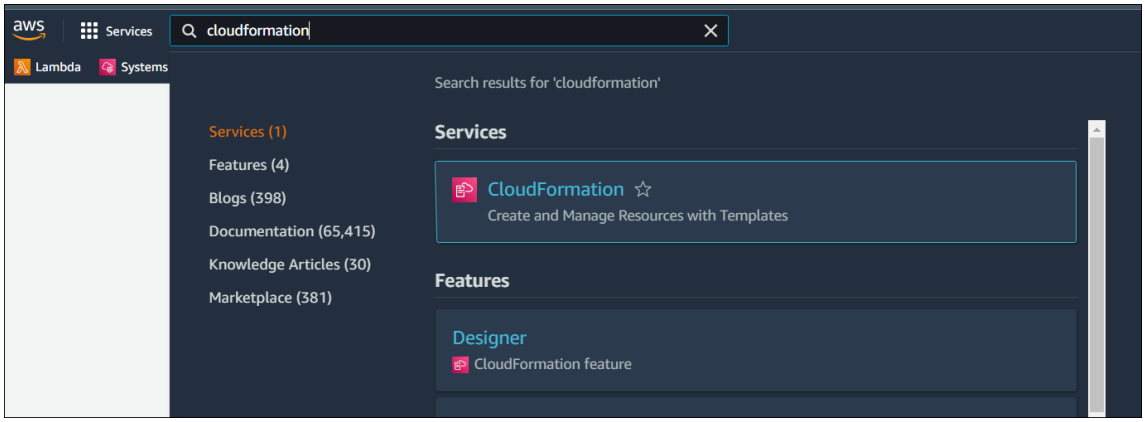
Wenn Sie das Skript `CloudFormation` verwenden, navigieren Sie zu CloudFormation und klicken Sie auf den entsprechenden Stack, der zum Erstellen der Rolle verwendet wurde. Navigieren Sie zur Registerkarte **Ressourcen** und klicken Sie auf die Ressource mit LogicalID `CitrixAssumeRole`.

> **Hinweis:**
>
> Sie können nicht zwei Konten in derselben Region für dasselbe AWS-Konto verbinden.

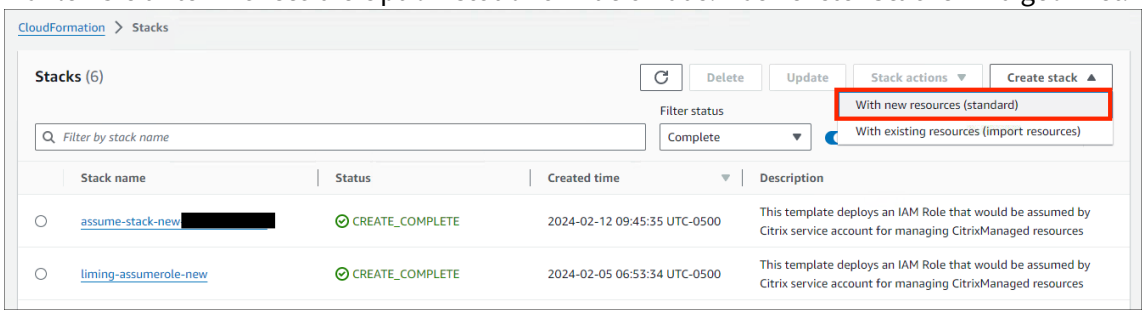
3. Wählen Sie auf der Seite **Region auswählen** die Region aus, in der Sie Ihre Desktops bereitstellen möchten, und klicken Sie auf **Weiter**.
4. Auf der Seite **BYOL-Support konfigurieren** ist zur Konfiguration der BYOL-Unterstützung eine Verwaltungsnetzwerkschnittstelle erforderlich, die mit einem sicheren Amazon-Netzwerk verbunden ist. Wählen Sie einen IP-Adressbereich aus, um nach einer Verwendung als Schnittstelle zu suchen. Wählen Sie dann "Verfügbare CIDR-Blöcke anzeigen"aus. Wenn CIDR-Blöcke im ausgewählten Suchbereich verfügbar sind, wählen Sie einen verfügbaren CIDR-Block aus. Eine Meldung bestätigt, dass Sie erfolgreich einen Suchadressbereich und einen verfügbaren CIDR-Block ausgewählt haben. Klicken Sie auf **Weiter**.
5. Überprüfen Sie auf der Seite **Zusammenfassung** die von Ihnen angegebenen Informationen. Sie können zu den vorherigen Seiten zurückkehren. Wenn Sie fertig sind, klicken Sie auf **Fertigstellen**.
   Es kann mehrere Stunden dauern, bis der Verbindungsvorgang abgeschlossen ist.

AssumeRole für die AWS Workspace Core-Integration erstellen

1. Öffnen Sie in Ihrem Browserfenster die Webite **Amazon Web Services Services** und melden Sie sich an.
2. Geben Sie in das **Suchfeld cloudformation** ein und drücken Sie die **Eingabetaste**.



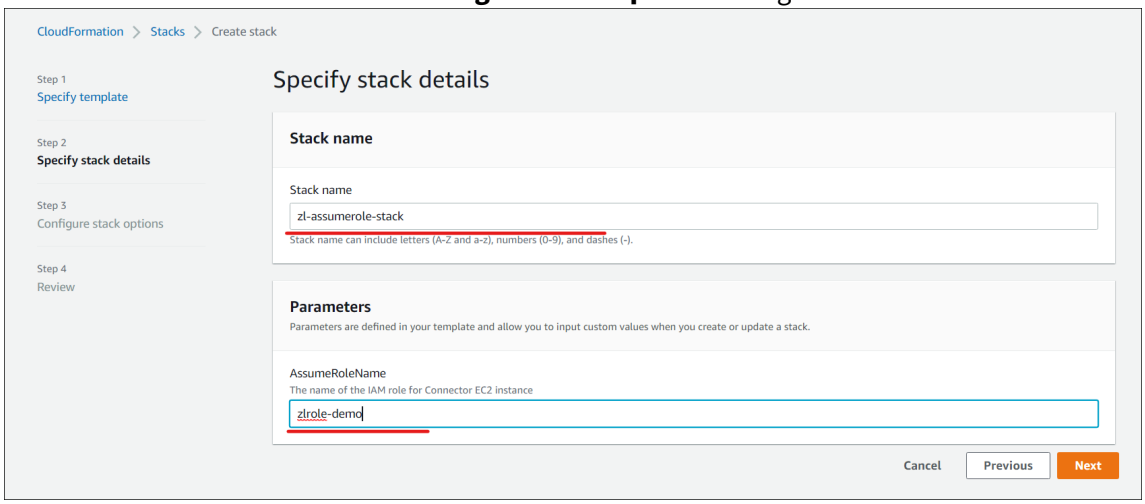
3. Wählen Sie unter **Dienste** die Option **CloudFormation** aus. Das Fenster **Stacks** wird geöffnet.



4. Klicken Sie oben rechts auf **Create stack > With new resources (standard)**. Das Fenster **Create stack** wird geöffnet.

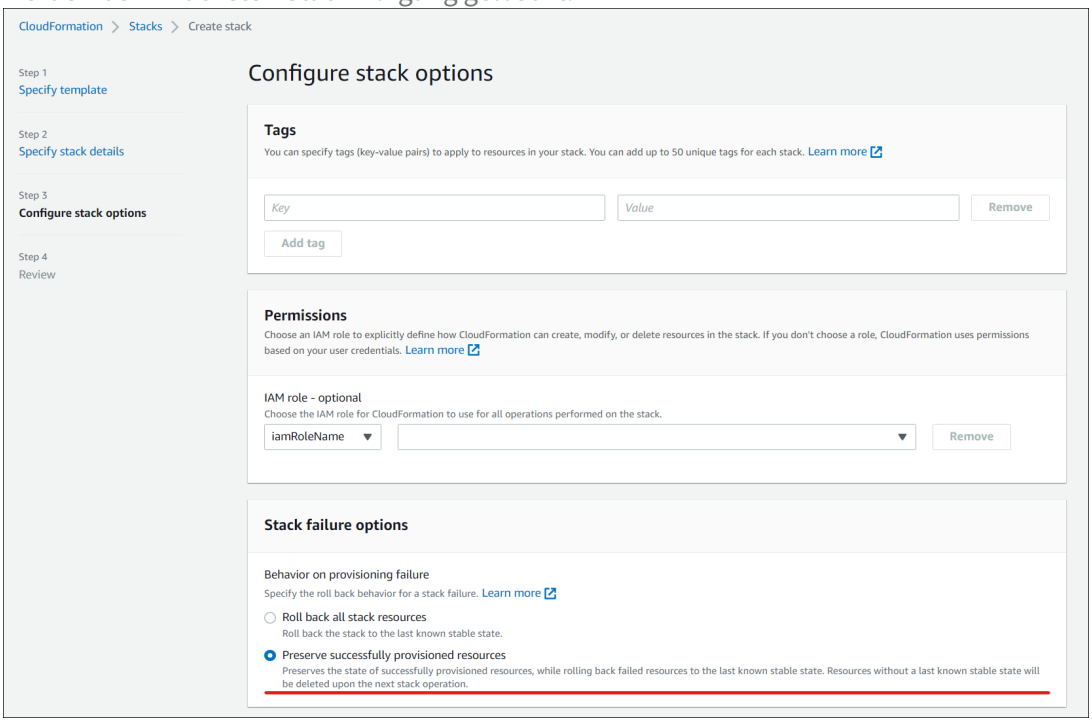
   a) Wählen Sie unter **Prerequisite** –**Prepare template** die Option **Template is ready** aus.
   b) Klicken Sie unter **Specify template** auf **Upload a template file > Choose file** und auf **Next**. Der Bereich **Specify stack details** wird geöffnet.

5. Geben Sie im Bereich **Specify stack details** einen **Stack name** und **AssumeRoleName** ein und klicken Sie auf **Next**. Der Bereich **Configure stack options** wird geöffnet.

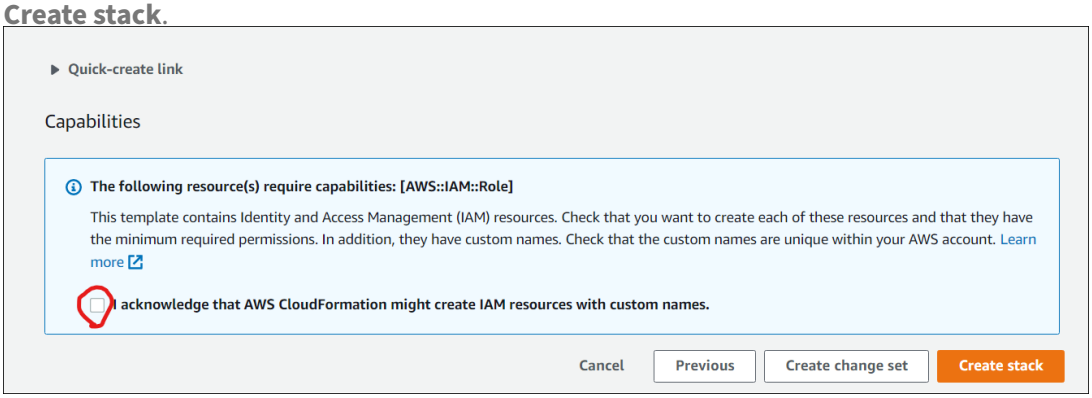


Hinweis:

- Wählen Sie im Bereich **Configure stack options** die Option **Preserve successfully provisioned resources**. Mit dieser Option wird der Status erfolgreich bereitgestellter Ressourcen beibehalten. Ressourcen ohne einen letzten bekannten stabilen Zustand werden beim nächsten Stack-Vorgang gelöscht.

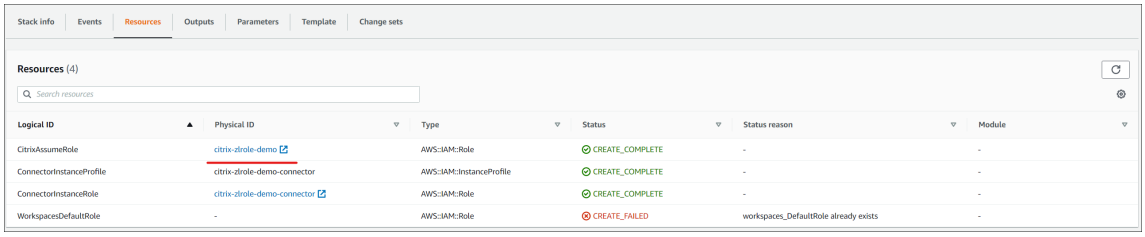


- Wählen Sie im Popup-Fenster **Capabilities** das Kontrollkästchen **I acknowledge that AWS CloudFormation might create IAM resources with custom names** und klicken Sie auf **Create stack**.

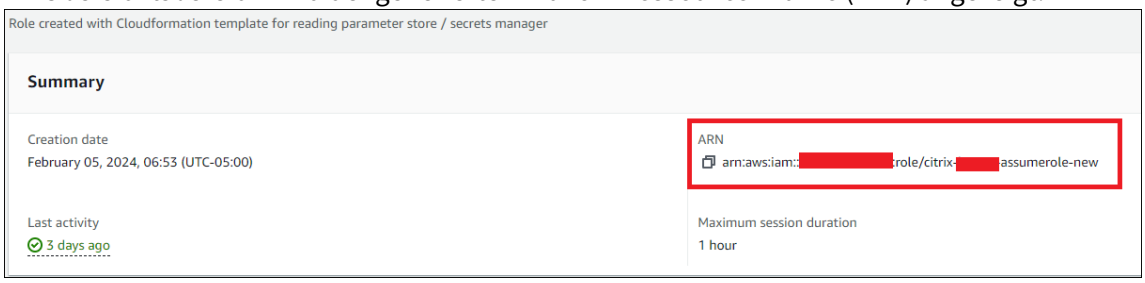


Die Stack-Erstellung kann am Ende fehlschlagen, weil **workspace_DefaultRole** bereits erstellt wurde. Dies hat keinen Einfluss auf die Erstellung von **AssumeRole**.

1. Auf der Registerkarte **Events** wird der Status des erstellten Stacks angezeigt.
2. Wählen Sie auf der Registerkarte **Resources** die physische ID aus, die der erstellten **AssumeRole** entspricht.



3. Im Übersichtsbereich wird der generierte **Amazon-Ressourcenname** (ARN) angezeigt.



4. Setzen Sie das Verfahren ab Schritt 4 unter AWS-Konto verbinden fort.

Verzeichnisverbindung erstellen

> **Hinweis:**
>
> Heben Sie die Registrierung Ihres AWS-Verzeichnisses zu Beginn dieses Schritts auf. Nachdem Sie eine Verzeichnisverbindung mit Citrix DaaS erstellt haben, wird das ausgewählte Verzeichnis registriert, um Amazon WorkSpaces mit Citrix DaaS zu erstellen.

Durch dieses Verfahren wird eine Verbindung hergestellt, die den Zugriff auf das Active Directory Ihrer Organisation ermöglicht.

Voraussetzungen:

- Ein Ressourcenstandort, der zwei Cloud Connectors enthält.
- Eine Sicherheitsgruppe.
- Eine OU in Ihrem Active Directory.

Einzelheiten zu den Voraussetzungen finden Sie unter Bevor Sie beginnen.

Sie können dieses Verfahren an zwei Stellen starten:

- Über einen Link auf der Checkliste “Erste Schritte”.
- Wählen Sie in der DaaS **Verwaltungskonsole** im linken Bereich **Quick Deploy** und **Verzeichnisverbindungen** im Abschnitt **Amazon WorkSpaces Core** aus. Wählen Sie dann **Verzeichnisverbindung erstellen** aus.

Gehen Sie dann so vor, wie unter **Verzeichnisverbindung erstellen** beschrieben:

1. **Voraussetzungen bestätigen:** Wenn Sie die Voraussetzungen erfüllt haben, klicken Sie auf **Weiter**.

2. **Verzeichnis verbinden:** Wählen Sie den Ressourcenstandort, das Konto und das Verzeichnis aus. (Das ausgewählte Konto muss mindestens ein Verzeichnis haben.)
    - Wählen Sie zwei Subnetze aus, in denen die Desktopmaschinen bereitgestellt werden. Die Subnetze müssen sich in den entsprechenden Verfügbarkeitszonen befinden.
    - Geben Sie einen benutzerfreundlichen Namen für diese Verbindung an.
    - Wenn Sie fertig sind, klicken Sie auf **Weiter**.
3. **Einstellungen für virtuelle Maschinen:** Die von Ihnen ausgewählten Einstellungen gelten für alle VMs, die diese Verzeichnisverbindung verwenden.
    - Die ausgewählte Organisationseinheit muss mit der Organisationseinheit übereinstimmen, auf die die Citrix Gruppenrichtlinie abzielt.
    - Wählen Sie eine Sicherheitsgruppe aus.
    - Geben Sie an, ob Sie jedem Benutzer, der VMs zugewiesen ist, Administratorrechte gewähren möchten.

Image importieren

Mit diesem Verfahren können Sie eine Benutzeroberfläche für die Desktops Ihrer Benutzer erstellen.

Voraussetzungen für den Import des Images:

- Es muss ein EC2-Image sein.
- Ein Citrix Virtual Delivery Agent (VDA) muss installiert sein.
- Es muss für BYOL vorbereitet sein. Ein BYOL-Skript ist verfügbar unter: BYOLChecker.zip.

Gehen Sie wie folgt vor, um ein Image zu importieren:

1. **Voraussetzungen bestätigen:** Klicken Sie nach den Schritten mit den Voraussetzungen auf **Weiter**. (Wenn Sie das Image nicht für BYOL vorbereitet haben, können Sie das Skript von dieser Seite herunterladen.) Weitere Informationen finden Sie unter Anforderungen.
2. **Wählen Sie ein Image** und geben Sie einen benutzerfreundlichen Namen für das Image ein. Wählen Sie das Konto, AMI und fügen Sie eine Beschreibung hinzu. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird geöffnet.
3. Überprüfen Sie auf der Seite **Zusammenfassung** die von Ihnen bereitgestellten Informationen. Wählen Sie nach der Überprüfung **Image importieren** aus.

    > **Hinweis:**
    >
    > Das Importieren eines Images kann mehrere Stunden dauern.

Microsoft Office 2019 Image beim Import eines Images integrieren

So integrieren Sie ein Microsoft Office 2019-Image beim Import eines Images:

1. Klicken Sie in **Web Studio > Quick Deploy** auf **Images**.
2. Klicken Sie unter **Meine Images** auf **Image importieren**.
3. Klicken Sie unter **Image importieren > Voraussetzungen** auf **Weiter: Image auswählen**.
4. Unter **Image importieren > Image auswählen:**
    - Wählen Sie ein Konto aus der Dropdownliste **Konto** aus.
    - Wählen Sie ein AMI aus der **AMI**-Dropdownliste aus.
    - Geben Sie den Namen des Images in das Feld **Name** ein.
    - Wählen Sie **Microsoft Office 2019 Professional Plus** im Image aus.
    - Geben Sie eine Beschreibung in das Feld **Beschreibung** ein.
5. Klicken Sie in **Image importieren > Image auswählen** auf **Weiter: Zusammenfassung**.
6. Stellen Sie in **Image auswählen > Zusammenfassung** sicher, dass **Microsoft Office 2019** als **Ausgewählt** angezeigt wird.
7. Klicken Sie unter **Meine Images** auf **Image importieren**.
   Der Status des kürzlich bereitgestellten Images wird solange als **Wird importiert** angezeigt, bis der Importvorgang abgeschlossen ist.
8. Wählen Sie unter **Meine Images** das kürzlich bereitgestellte Image aus und klicken Sie auf **Detail anzeigen**.
9. Im Bereich **Detail** wird **Microsoft Office 2019** als **Integriert** angezeigt.

> **Hinweis:**
>
> Nur die folgenden Versionen des Betriebssystems sind kompatibel:
>
> - Windows 10 Version 21H2 (Update Dezember 2021)
> - Windows 10 Version 22H2 (Update November 2022)
> - Windows 10 Enterprise LTSC 2019 (1809) (1809)
> - Windows 10 Enterprise LTSC 2021 (21H2) (21H2)
> - Windows 11 Version 22H2 (Release Oktober 2022)

Erstellen einer Bereitstellung

Eine Bereitstellung ist eine Gruppe von Desktops, auf die Benutzer von ihrem Citrix Workspace aus zugreifen können. Dieses Verfahren legt die Eigenschaften der virtuellen Maschinen fest, die als Desktops bereitgestellt werden sollen, und welche AD-Benutzer sie verwenden können.

Voraussetzungen

Führen Sie alle unter Bereitstellung vorbereiten und erstellen aufgeführten Schritte aus.

1. Klicken Sie in **Web Studio > Quick Deploy** in der Spalte **Amazon Web Services** auf **Bereitstellungen**. Klicken Sie auf **Bereitstellung erstellen**.
2. **Name und Verbindung:** Geben Sie einen benutzerfreundlichen Namen für diese Maschinengruppe ein. Der Name muss eindeutig sein. Wählen Sie eine Verzeichnisverbindung aus und klicken Sie auf **Weiter: Image und Leistung**.
3. **Image und Leistung:** Wählen Sie das Betriebssystem und die Maschinenleistung für die Maschinen aus. Geben Sie die Standardgröße für das Stammvolume und das Benutzervolume an. Sie können die Volumegröße nicht ändern, nachdem Sie einen Desktop in dieser Gruppe gestartet haben. Geben Sie also die maximale Größe an, die Sie Ihrer Meinung nach benötigen werden. Sie können diese Größen auch pro Benutzer auf der nächsten Seite angeben. Klicken Sie auf **Weiter**: Benutzer.
4. **Benutzer:** Suchen und wählen Sie die Benutzer aus, die auf die Desktops zugreifen dürfen. Wenn Sie die Volumegrößen für einen Benutzer anpassen möchten, wählen Sie **Größe von Benutzer- und Stammvolume bearbeiten** aus und geben Sie dann die Größen an. Klicken Sie auf **Weiter: Zusammenfassung**.
5. **Zusammenfassung:** Überprüfen Sie die von Ihnen angegebenen Informationen und klicken Sie auf **Bereitstellung erstellen**.

Microsoft 365 Windows-Apps integrieren

Informationen zur Integration von Microsoft 365-Apps finden Sie unter Microsoft 365-Apps für Unternehmen jetzt in Amazon WorkSpaces-Diensten verfügbar und Microsoft 365 Bring Your Own License (BYOL) verfügbar.

Maschinen in einer Bereitstellung verwalten

Zusätzlich zu den unter Maschinenkataloge verwalten beschriebenen Features für die Maschinenverwaltung können Sie für einige Aktionen Maschinen zur Verwaltung aus einer Bereitstellung auswählen.

So verwalten Sie Maschinen in einer Bereitstellung:

1. Wählen Sie in **Web Studio > Quick Deploy** die Option **Bereitstellungen** aus.
2. Wählen Sie im Bereich **Bereitstellungen** die Bereitstellung mit Maschinen aus, die Sie verwalten möchten.
3. Klicken Sie auf **Details anzeigen**.
4. Wählen Sie im Bereich **Bereitstellungsdetails** die Maschine aus, die Sie verwalten möchten.
5. Wählen Sie aus den angezeigten Aktionen die Aktion aus, die Sie auf dem Computer ausführen möchten:

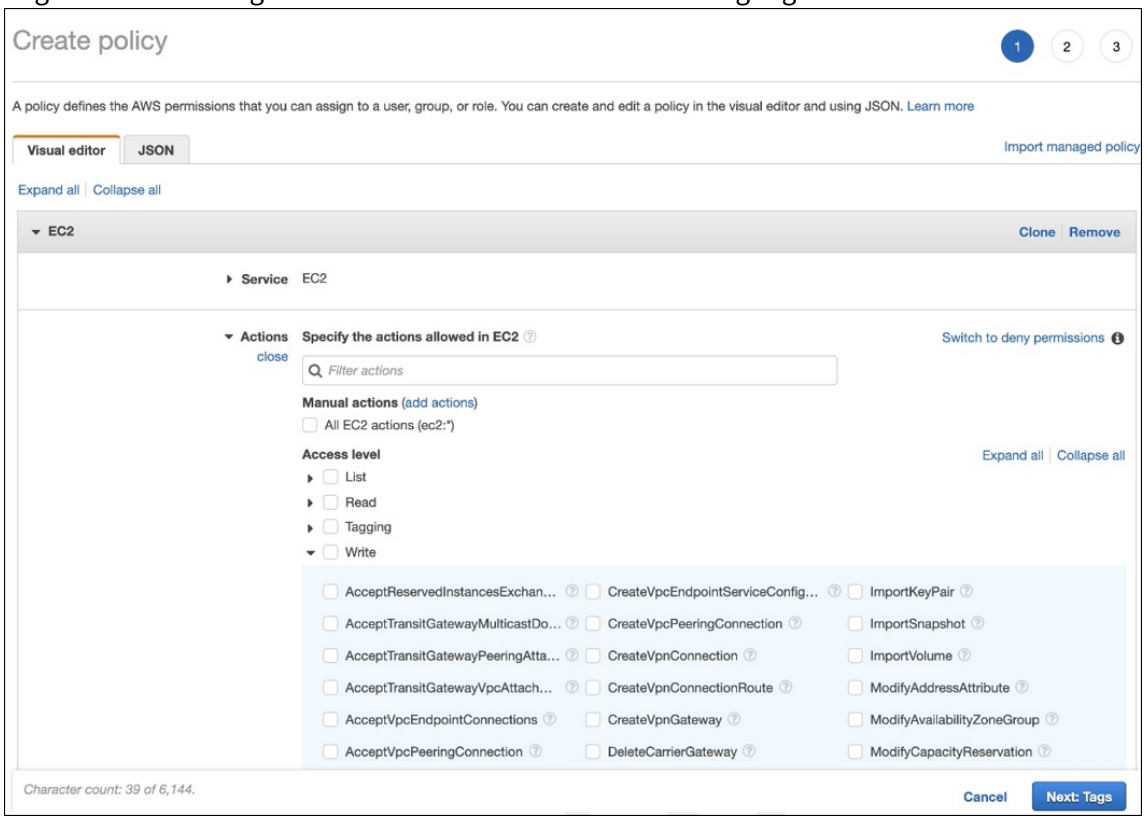
- Klicken Sie auf **Größe der Volumes bearbeiten**, um die Größe des Volumes des Geräts zu ändern.
- Klicken Sie auf **Löschen**, um die Maschine aus der Bereitstellung und aus AWS zu löschen. Wenn sich eine Maschine in einer Bereitstellungsgruppe befindet, kann sie nur gelöscht werden, wenn sie sich im Wartungsmodus befindet.
- Klicken Sie auf **Wartungsmodus ein-/ausschalten:** Dies schaltet den Wartungsmodus für die ausgewählte Maschine ein (falls ausgeschaltet) bzw. aus (falls eingeschaltet).

Referenz

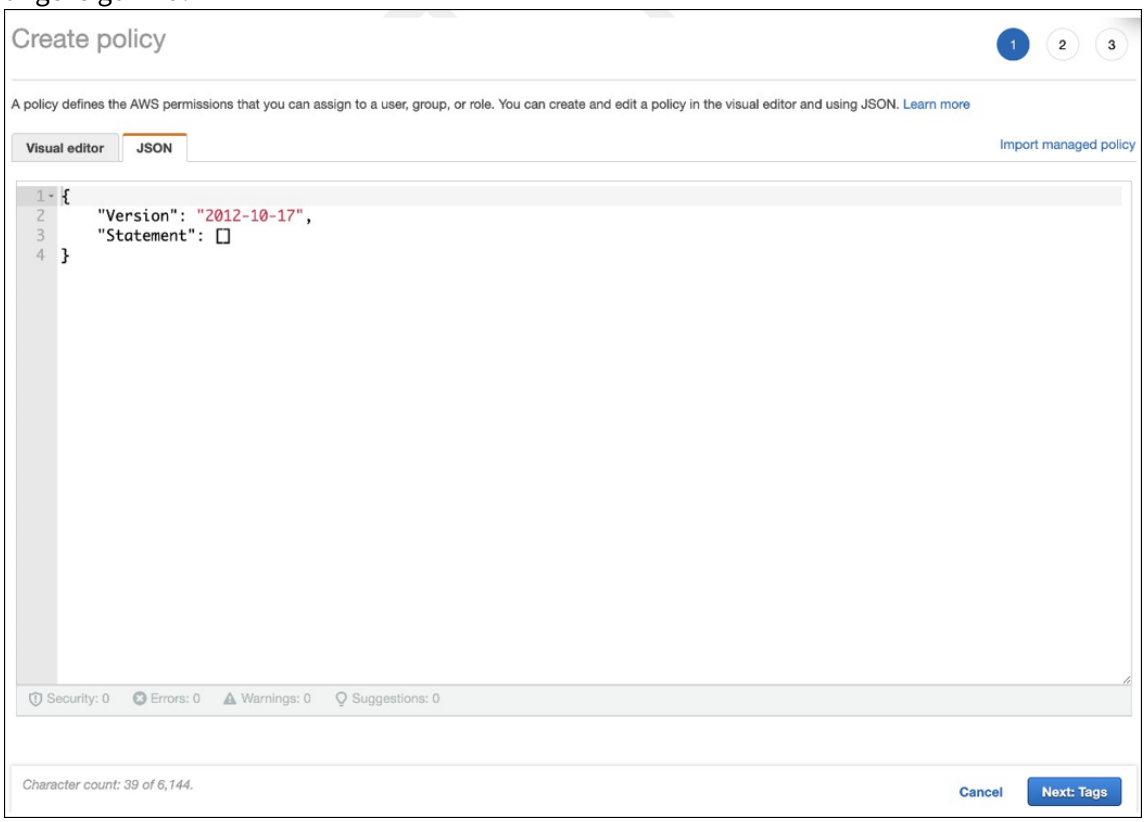
Berechtigungen für den programmgesteuerten Zugriff auf AWS-Konten

Das AWS-Benutzerkonto muss über bestimmte programmatische Zugriffsberechtigungen verfügen, um API-Aufrufe an die AWS-Ressourcenebene zu tätigen. Beim programmatischen Zugriff werden eine Zugriffsschlüssel-ID und ein Zugriffsschlüsselgeheimnis erstellt.
Sie können in der IAM-Konsole eine Richtlinie erstellen, die diese Berechtigungen enthält. Wie in den folgenden Grafiken gezeigt, können Sie den visuellen Editor (um die Berechtigungen nacheinander hinzuzufügen) oder den JSON (mit dem nachstehenden Ausschnitt) verwenden.
Weitere Informationen finden Sie unter IAM-Benutzer in Ihrem AWS-Konto erstellen.

- Fügen Sie auf der Registerkarte **Visueller Editor** die Berechtigungen nacheinander hinzu.



- Fügen Sie auf der Registerkarte **JSON** den Ausschnitt hinzu, der nach der folgenden Grafik angezeigt wird.



Erforderliche Berechtigungen

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                    "workdocs:DeregisterDirectory",
                    "workdocs:RegisterDirectory",
                    "workdocs:AddUserToGroup",
                    "ec2:ImportInstance",
                    "ec2:DescribeImages",
                    "ec2:DescribeImageAttribute"
                    "ec2:CreateKeyPair",
                    "ec2:DescribeKeyPairs",
                    "ec2:ModifyImageAttribute",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeSubnets",
                    "ec2:RunInstances",
                    "ec2:DescribeSecurityGroups",
                    "ec2:CreateTags",
```



```
                    "ec2:DescribeRouteTables",
                    "ec2:DescribeInternetGateways",
                    "ec2:CreateSecurityGroup",
                    "ec2:DescribeInstanceTypes",
                    "servicequotas:ListServices",
                    "servicequotas:GetRequestedServiceQuotaChange",
                    "servicequotas:ListTagsForResource",
                    "servicequotas:GetServiceQuota",
                    "servicequotas:
                       GetAssociationForServiceQuotaTemplate",
                    "servicequotas:ListAWSDefaultServiceQuotas",
                    "servicequotas:ListServiceQuotas",
                    "servicequotas:GetAWSDefaultServiceQuota",
                    "servicequotas:
                       GetServiceQuotaIncreaseRequestFromTemplate",
                    "servicequotas:
                       ListServiceQuotaIncreaseRequestsInTemplate",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistory",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
                    "iam:SimulatePrincipalPolicy"

                ],
                "Resource": "*"
            }

        ]
 }

<!--NeedCopy-->
```

Citrix DaaS für Google Cloud

November 16, 2022

Mit Citrix DaaS für Google Cloud können Sie Google Cloud-Desktops und -Apps über die Verwaltungsoberfläche “Vollständige Konfiguration”von Citrix DaaS bereitstellen. Citrix DaaS für Google Cloud ist in den Editionen Standard und Premium verfügbar.

Informationen zu unterstützten Features finden Sie in der Featurematrix für Citrix Virtual Apps and Desktops.

Sie können Citrix DaaS für Google Cloud im Google Cloud Marketplace bestellen.

Nachdem Sie Citrix DaaS bestellt haben, melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü links oben **Eigene Services > DaaS**.

Folgen Sie den Anweisungen zum Einrichten in dieser Produktdokumentation. Über die Oberfläche "Vollständige Konfiguration"können Sie Verbindungen, Kataloge und Bereitstellungsgruppen erstellen, genau wie bei der Verwendung dieser Oberfläche mit anderen Produkteditionen. (Diese Editionen verfügen derzeit nicht über eine Quick Deploy-Verwaltungsoberfläche.)

Einige Ansichten in der Oberfläche "Vollständige Konfiguration"können sich von denen in der Dokumentation unterscheiden. Wenn Sie beispielsweise eine Verbindung in einer Citrix Virtual Apps and Desktops Edition für Google Cloud herstellen, umfassen die verfügbaren Verbindungstypen die unterstützten Hypervisoren und Google Cloud. Andere Cloudservices sind nicht verfügbar.

Verwenden Sie außerdem die Informationen in der Produktdokumentation, die für unterstützte Hypervisoren und Google Cloud gelten.

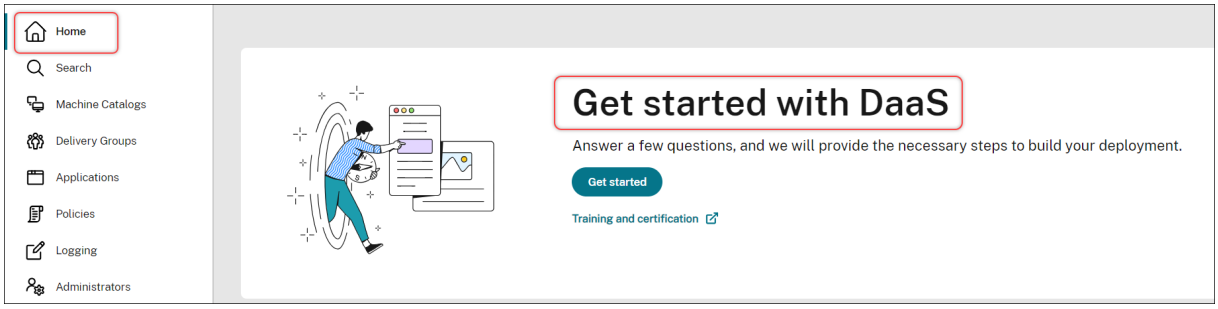
Schrittweise Anweisungen zum Bereitstellen und Konfigurieren von Citrix DaaS in Google Cloud finden Sie in dem Citrix Tech Zone-Artikel Citrix Virtualisierung in Google Cloud. In dem Artikel werden das Definieren der Bereitstellungsarchitektur, das Vorbereiten des Google Cloud-Projekts, das Konfigurieren von Netzwerkdiensten und das Bereitstellen von Active Directory behandelt.

Leitfaden "Erste Schritte mit DaaS"verwenden (Preview)

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Der DaaS-Leitfaden unterstützt die optimierte und vereinfachte DaaS-Bereitstellung durch neue und erfahrene Administratoren. Anhand des Leitfadens können Sie DaaS-Bereitstellungen schnell einrichten, indem Sie eine Reihe von Fragen beantworten.



In diesem Artikel wird die Einrichtung fünf typischer DaaS-Bereitstellungen Schritt für Schritt beschrieben.

Vorteile

Vorteile der Verwendung des Leitfadens:

- **Einfacher Einstieg**. Der Leitfaden bietet einen anhand eines Fragebogens zusammengestellten schrittweisen Workflow. Neue Administratoren können ihre Bereitstellung schnell einrichten und gleichzeitig Konzepte und Begrieffe mithilfe der Kontexthilfe erlernen.
- **Vereinfacht komplexe Konfigurationen**. Der Leitfaden enthält, wo erforderlich, vorkonfigurierte Einstellungen und bietet Zugriff auf die Benutzeroberfläche für die vollständige Konfiguration für erweiterte Konfigurationen. Erfahrene Administratoren können den Leitfaden als Ausgangspunkt für komplexe Konfigurationen verwenden.

Unterstützte Bereitstellungsszenarios

Der Leitfaden bietet schnelle Bereitstellungen für die folgenden Szenarien:

Objekt der Bereitstellung	Gibt es bereits Maschinen?	Maschinentyp	Anmerkung
Virtuelle Apps und Desktops	Nein	Virtuelle Maschinen (von DaaS bereitgestellt)	Mit Energieverwaltung
Virtuelle Apps und Desktops	Ja	Virtuelle Maschinen oder Blade-PCs	Mit Energieverwaltung
Virtuelle Apps und Desktops	Ja	Physische oder virtuelle Maschinen	Ohne Energieverwaltung
Büro-PCs	Ja	Physische Maschinen	Mit Energieverwaltung
Büro-PCs	Ja	Physische Maschinen	Ohne Energieverwaltung

Die folgenden Abschnitte enthalten detaillierte Anleitungen:

- Apps und Desktops von Grund auf neu bereitstellen (mit Energieverwaltung)
- Apps und Desktops anhand vorhandener Maschinen bereitstellen (mit Energieverwaltung)
- Apps und Desktops anhand vorhandener Maschinen bereitstellen (ohne Energieverwaltung)
- Büro-PCs bereitstellen (mit Energieverwaltung)
- Büro-PCs bereitstellen (ohne Energieverwaltung)

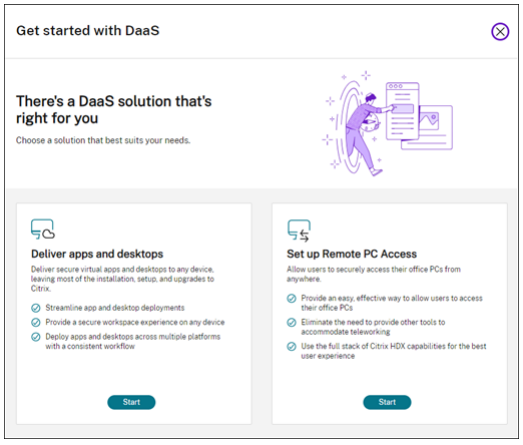
Terminologie

Die folgenden Begriffe sind DaaS-spezifisch:

- **Ressourcenstandort.** Enthält die Ressourcen zur Bereitstellung von Apps und Desktops für Benutzer.
- **Hostverbindung.** Verbindet DaaS mit einem Host (Hypervisor oder Cloudservice) an einem Ressourcenstandort. Das Erstellen von Hostverbindungen ist erforderlich, wenn Sie Maschinen auf Hosts erstellen und verwalten oder die Energiefunktionen vorhandener Maschinen verwalten möchten.
- **Masterimage.** Dient als Vorlage für die Replizierung virtueller Maschinen auf dem Host. Es umfasst das Betriebssystem, Anwendungen, den Virtual Delivery Agent (VDA) und andere Software.
- **Maschinenkatalog:** Sammlung identischer Maschinen. Dabei kann es sich, je nach Bedarf, um virtuelle oder physische Maschinen handeln. Sie können einen Maschinenkatalog erstellen, um Maschinen mit identischer Konfiguration auf einem Host zu erstellen oder Maschinen zur Verwaltung in DaaS zu importieren.
- **Bereitstellungsgruppe.** Enthält Maschinen aus Maschinenkatalogen. Sie gibt außerdem die Benutzer an, die diese Maschinen verwenden können, und welche Anwendungen und Desktops für die Benutzer verfügbar sind.
- **Maschinenprofil.** Gibt die Eigenschaften von virtuellen Maschinen an. VMs in einem Katalog können Eigenschaften eines Maschinenprofils erben.

Leitfaden aufrufen

1. Gehen Sie zu der Seite **DaaS > Home**.
2. Suchen Sie **Erste Schritte mit Citrix DaaS**.
3. Klicken Sie auf **Erste Schritte**, um die Bereitstellung zu starten.



> **Hinweis:**
>
> Sie können den Vorgang jederzeit beenden, indem Sie auf **Schließen** klicken. Ihre Einstellungen werden automatisch gespeichert. Um mit der Konfiguration fortzufahren, klicken Sie auf **Weiter**. Um von vorne zu beginnen, klicken Sie auf **Von vorne**.

Apps und Desktops von Grund auf neu bereitstellen (mit Energieverwaltung)

In diesem Abschnitt wird das Erstellen von VMs und das Bereitstellen von Apps und Desktops mithilfe der VMs erläutert.

Voraussetzungen

Sie benötigen:

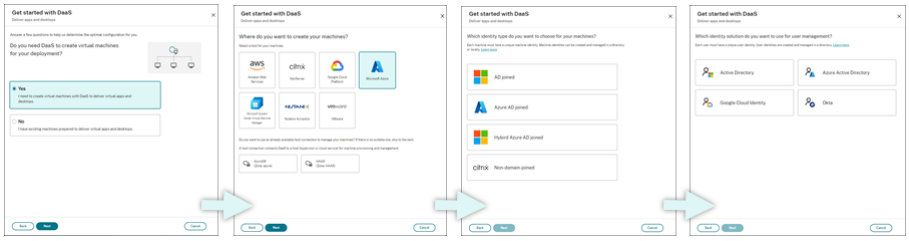
- Verbindung zwischen Citrix Cloud und Ziel-Identitätsanbieter

  Weitere Informationen finden Sie im entsprechenden Abschnitt unter Identitätsanbieter.
- Rolle: Volladministrator oder Cloudadministrator
- Erforderliche Berechtigungen für den Ziel-Hypervisor oder Cloudservice.

  Weitere Informationen finden Sie in den entsprechenden Abschnitten unter Verbindungen erstellen und verwalten.
- Administratoranmeldeinformationen für die Erstellung eines VM-Kontos

Vorbereitung

Beantworten Sie die angezeigten Fragen, um die folgenden Einstellungen auf Infrastrukturebene vorzunehmen. Einzelheiten finden Sie in der folgenden Tabelle.

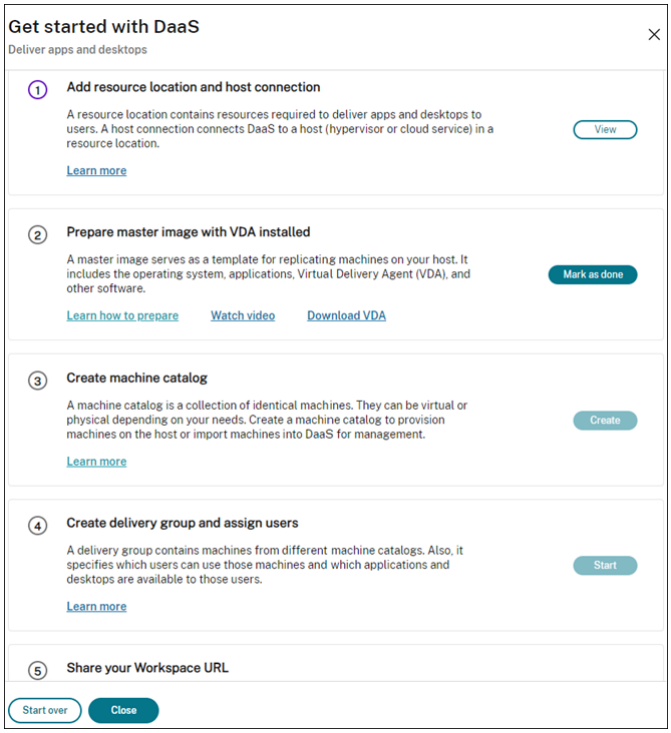


#	Einstellung	Beschreibung
1	Geben Sie an, ob eine VM-Erstellung erforderlich ist	Wählen Sie **Ja**.

#	Einstellung	Beschreibung
2	Hosttyp wählen	Wählen Sie einen Hosttyp für Ihre Bereitstellung. Optionen: AWS, XenServer (zuvor "Citrix Hypervisor"), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis und VMware
3	Maschinen-Identitätstyp wählen	Wählen Sie einen Identitätstyp für die Maschinenverwaltung. Optionen: In AD eingebunden, In Azure AD eingebunden, Azure AD-Hybrideinbindung und Gehört keiner Domäne an
4	Benutzeridentitätstyp wählen	Wählen Sie einen Identitätstyp für die Benutzerverwaltung. Optionen: Active Directory, Azure Active Directory, Google Cloud Identity und Okta

Bereitstellungsschritte

Nachdem Sie die Einstellungen auf Infrastrukturebene vorgenommen haben, werden die für das Bereitstellungsszenario spezifischen Schritte (siehe unten) angezeigt.



Folgen Sie den angezeigten Anweisungen, um die Einstellungen vorzunehmen.

Schritt 1: Ressourcenstandort und Hostverbindungen hinzufügen Richten Sie den Ressourcenstandort ein, indem Sie Cloud Connectors installieren und Verbindungen zu Hypervisors oder Cloudservices dafür konfigurieren.

1. Benennen Sie den Ressourcenstandort.
2. Laden Sie Cloud Connectors herunter und installieren Sie sie auf mindestens zwei Windows Server-Maschinen.
3. Führen Sie die Erkennung installierter Cloud Connectors durch.
4. Fügen Sie Hostverbindungen für den Ressourcenstandort hinzu und konfigurieren Sie sie. Die Verbindungseinstellungen sind:

    - Details wie etwa Verbindungsadresse, Benutzername und Kennwort.
    - Speicherressourcen
    - Netzwerkressourcen

    > **Hinweis:**
    >
    > DaaS erstellt und verwaltet VMs auf Hosts über diese Verbindungen. Sie müssen Verbindungen angeben, wenn Sie Maschinenkataloge erstellen.

Schritt 2: Vorbereiten Ihres Masterimages für die Maschinen Bereiten Sie Masterimages auf VMs an Ihrem Ressourcenstandort vor. Weitere Informationen finden Sie unter Vorbereiten eines Masterimages auf dem Hypervisor bzw. im Clouddienst.

Schritt 3: Maschinenkataloge erstellen Erstellen Sie einen Maschinenkatalog für eine Gruppe identisch konfigurierter Maschinen auf einem Host. Verfahren:

1. Benennen Sie den Katalog.
2. Wählen Sie den Maschinentyp aus.

   Optionen: Multisitzung, Statische Einzelsitzung (persönliche Desktops) und Zufällige Einzelsitzung (gepoolte Desktops).
3. Wählen Sie eine Hostverbindung aus.

   Die Optionen stammen von allen Hostverbindungen, die Sie in Schritt 1 für die Ressourcenstandorte konfiguriert haben.
4. Wählen Sie ein Masterimage.
5. Wählen Sie ein Maschinenprofil.

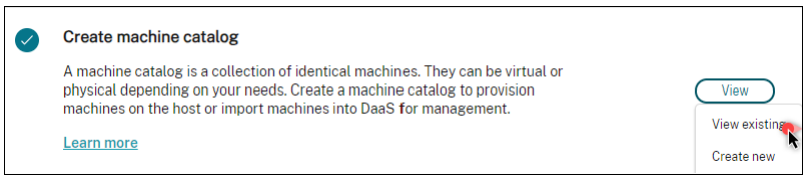
   > **Hinweis:**
   >
   > Maschinenprofile werden derzeit für Azure-, GCP- und AWS-Cloudservices unterstützt, die Verwendung von Maschinenprofilen ist bei GCP optional.

6. Legen Sie fest, wie viele Maschinen Sie erstellen möchten.
7. Legen Sie die Maschinenidentitäten fest.

   Standardmäßig wird der Maschinenidentitätstyp angezeigt, den Sie in der Vorbereitungsphase ausgewählt haben. Geben Sie die erforderlichen Identitätseinstellungen für die VMs an, z. B. Domäne, OU und Benennungsschema.
8. Geben Sie die für die Maschinenerstellung erforderlichen Administratoranmeldeinformationen ein.
9. Klicken Sie auf **Erstellen**.

   > **Tipp:**
   >
   > Die Schaltfläche **Erstellen** ist erst verfügbar, wenn Sie alle erforderlichen Einstellungen vorgenommen haben.

   Um den Fortschritt der Katalogerstellung anzuzeigen, wählen Sie **Ansicht > Vorhandene anzeigen**.



Schritt 4: Bereitstellungsgruppen erstellen und Benutzer zuweisen

> **Tipp:**
>
> Vergewissern Sie sich vor dem Erstellen von Bereitstellungsgruppen, dass mindestens ein Katalog erstellt wurde. Andernfalls werden Sie daran gehindert, Bereitstellungsgruppen zu erstellen.

Das Erstellen einer Bereitstellungsgruppe umfasst die folgenden Unteraufgaben:

- Virtuelle Maschinen zur Gruppe hinzufügen
- Benutzer der Gruppe zuweisen
- Angeben, welche Apps und Desktops zugewiesenen Benutzern zur Verfügung stehen sollen

1. Benennen Sie die Gruppe.
2. Fügen Sie der Gruppe Maschinen hinzu, indem Sie einen Maschinenkatalog auswählen und angeben, wie viele VMs für die Gruppe verfügbar sind.
3. Geben Sie die für die Gruppe verfügbaren Anwendungen und Desktops an:
    - Um Anwendungen von einer Maschine in Ausführung zum ausgewählten Katalog hinzuzufügen, klicken Sie auf **Hinzufügen > Vom Startmenü**.
    - Um in Netzwerkfreigaben bereitgestellte Anwendungen hinzuzufügen, klicken Sie auf **Hinzufügen > Manuell** und geben Sie dann die erforderlichen Einstellungen (Pfad, Arbeitsverzeichnis…) ein.
    - Nur Maschinen mit Multisitzungs-OS: Lassen Sie die Option **Desktopbereitstellung aktivieren** aktiviert.
4. Fügen Sie Benutzer hinzu, die auf Apps und Desktops in dieser Gruppe zugreifen können.

Schritt 5: Workspace-URL den Benutzern mitteilen Gehen Sie zu **Workspace-Konfiguration > Zugriff** und geben Sie den Benutzern die Workspace-URL bekannt.

Apps und Desktops anhand vorhandener Maschinen bereitstellen (mit Energieverwaltung)

In diesem Abschnitt wird das Bereitstellen von Apps und Desktops mithilfe von VMs (mit Energieverwaltung) erläutert.

Voraussetzungen

Sie benötigen:

- Verbindung zwischen Citrix Cloud und Ziel-Identitätsanbieter

  Weitere Informationen finden Sie im entsprechenden Abschnitt unter Identitätsanbieter.
- Rolle: Volladministrator oder Cloudadministrator

Vorbereitung

Beantworten Sie die angezeigten Fragen, um die folgenden Einstellungen auf Infrastrukturebene vorzunehmen.

#	Einstellung	Beschreibung
1	Geben Sie an, ob eine VM-Erstellung erforderlich ist	Wählen Sie **Nein**.
2	Auswählen, ob eine Energieverwaltung erforderlich ist	Wählen Sie **Maschinen mit Energieverwaltung (z. B. virtuelle Maschinen oder Blade-PCs)**.
3	Hostplattform auswählen	Wählen Sie die Hostplattform, auf der sich die Maschinen befinden. Optionen: AWS, Citrix, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis und VMware
4	Benutzeridentitätstyp wählen	Wählen Sie einen Identitätstyp für die Benutzerverwaltung. Optionen: Active Directory, Azure Active Directory, Google Cloud Identity und Okta

Bereitstellungsschritte

Nachdem Sie die Einstellungen auf Infrastrukturebene vorgenommen haben, werden die für das Bereitstellungsszenario spezifischen Schritte angezeigt. Folgen Sie den angezeigten Anweisungen, um die Einstellungen vorzunehmen.

Schritt 1: Ressourcenstandort und Hostverbindungen hinzufügen Richten Sie den Ressourcenstandort ein, indem Sie Cloud Connectors installieren und Verbindungen zu Hypervisors oder Cloudservices dafür konfigurieren.

1. Benennen Sie den Ressourcenstandort.
2. Laden Sie Cloud Connectors herunter und installieren Sie sie auf mindestens zwei Windows Server-Maschinen.
3. Führen Sie die Erkennung installierter Cloud Connectors durch.
4. Fügen Sie Hostverbindungen für den Ressourcenstandort hinzu und konfigurieren Sie sie. Zu den Verbindungseinstellungen gehören beispielsweise die Verbindungsadresse, der Benutzername und das Kennwort.

> **Hinweis:**
>
> Die Energieverwaltung von Maschinen erfolgt bei DaaS über Verbindungen. Sie müssen eine Verbindung angeben, wenn Sie Ihre Maschinen in einen Katalog importieren.

Schritt 2: Maschinenkataloge erstellen Erstellen Sie einen Maschinenkatalog und importieren Sie Ihre Maschinen.

1. Benennen Sie den Katalog.
2. Wählen Sie den Maschinentyp aus.

   Optionen: Multisitzung, Statische Einzelsitzung (persönliche Desktops) und Zufällige Einzelsitzung (gepoolte Desktops).
3. Wählen Sie einen Ressourcenstandort.
4. Importieren Sie Maschinen in den Katalog.
   Maschinen sind nach Hostverbindungen strukturiert. Wählen Sie eine Hostverbindung, um die zugehörigen Maschinen zu importieren.
5. Klicken Sie auf **Erstellen**.

Schritt 3: Bereitstellungsgruppen erstellen und Benutzer zuweisen Um eine Bereitstellungsgruppe zu erstellen, müssen Sie:

- Virtuelle Maschinen zur Gruppe hinzufügen
- Benutzer der Gruppe zuweisen
- Angeben, welche Apps und Desktops zugewiesenen Benutzern zur Verfügung stehen sollen

1. Benennen Sie die Gruppe.
2. Wählen Sie nach Bedarf einen Maschinenkatalog und geben Sie an, wie viele Maschinen für die Bereitstellungsgruppe verfügbar sind.

3. Geben Sie die für die Gruppe verfügbaren Anwendungen und Desktops an:
    - Um Anwendungen von einer Maschine in Ausführung zum ausgewählten Katalog hinzuzufügen, klicken Sie auf **Hinzufügen > Vom Startmenü**.
    - Um in Netzwerkfreigaben bereitgestellte Anwendungen hinzuzufügen, klicken Sie auf **Hinzufügen > Manuell** und geben Sie dann die erforderlichen Einstellungen (Pfad, Arbeitsverzeichnis…) ein.
    - Nur Maschinen mit Multisitzungs-OS: Lassen Sie die Option **Desktopbereitstellung aktivieren** aktiviert.
4. Fügen Sie der Gruppe Benutzer hinzu.

Schritt 4: Workspace-URL den Benutzern mitteilen Gehen Sie zu **Workspace-Konfiguration > Zugriff** und geben Sie den Benutzern die Workspace-URL bekannt.

Apps und Desktops anhand vorhandener Maschinen bereitstellen (ohne Energieverwaltung)

In diesem Abschnitt wird das Bereitstellen von Apps und Desktops mithilfe von VMs (ohne Energieverwaltung) erläutert.

Voraussetzungen

Sie benötigen:

- Verbindung zwischen Citrix Cloud und Ziel-Identitätsanbieter

  For more information, see the corresponding section in Identity providers
- Rolle: Volladministrator oder Cloudadministrator

Vorbereitung

Beantworten Sie die angezeigten Fragen, um die folgenden Einstellungen auf Infrastrukturebene vorzunehmen.

#	Einstellung	Beschreibung
1	Geben Sie an, ob eine VM-Erstellung erforderlich ist	Wählen Sie **Nein**.

#	Einstellung	Beschreibung
2	Auswählen, ob eine Energieverwaltung erforderlich ist	Wählen Sie **Maschinen ohne Energieverwaltung (z. B. physische Maschinen)**.
3	Benutzeridentitätstyp wählen	Wählen Sie einen Identitätstyp für die Benutzerverwaltung. Optionen: Active Directory, Azure Active Directory, Google Cloud Identity und Okta

Bereitstellungsschritte

Nachdem Sie die Einstellungen auf Infrastrukturebene vorgenommen haben, werden die für das Bereitstellungsszenario spezifischen Schritte angezeigt. Folgen Sie den angezeigten Anweisungen, um die Einstellungen vorzunehmen.

Schritt 1: Ressourcenstandort hinzufügen Richten Sie den Ressourcenstandort ein, indem Sie Cloud Connectors installieren.

1. Benennen Sie den Ressourcenstandort.
2. Laden Sie Cloud Connectors herunter und installieren Sie sie auf mindestens zwei Windows Server-Maschinen.
3. Führen Sie die Erkennung installierter Cloud Connectors durch.

> **Hinweis:**
>
> Das Erstellen von Hostverbindungen ist nur erforderlich, wenn Sie die Energieverwaltung für die Maschinen wünschen.

Schritt 2: Erstellen eines Maschinenkatalogs Erstellen Sie einen Maschinenkatalog und importieren Sie Ihre Maschinen.

1. Benennen Sie den Katalog.
2. Wählen Sie den Maschinentyp aus.

   Optionen: Multisitzung, Statische Einzelsitzung (persönliche Desktops) und Zufällige Einzelsitzung (gepoolte Desktops).
3. Wählen Sie einen Ressourcenstandort.

4. Importieren Sie Maschinen in den Katalog.

   Um die Maschinensuche zu vereinfachen, verwenden Sie teilweise Computernamen und die Verzeichnisauswahl.

5. Klicken Sie auf **Erstellen**.

Schritt 3: Bereitstellungsgruppen erstellen und Benutzer zuweisen Um eine Bereitstellungsgruppe zu erstellen, müssen Sie:

- Virtuelle Maschinen zur Gruppe hinzufügen
- Benutzer der Gruppe zuweisen
- Angeben, welche Apps und Desktops zugewiesenen Benutzern zur Verfügung stehen sollen

1. Benennen Sie die Gruppe.
2. Wählen Sie nach Bedarf einen Maschinenkatalog und geben Sie an, wie viele Maschinen für die Bereitstellungsgruppe verfügbar sind.
3. Geben Sie die für die Gruppe verfügbaren Anwendungen und Desktops an:
   - Um Anwendungen von einer Maschine in Ausführung zum ausgewählten Katalog hinzuzufügen, klicken Sie auf **Hinzufügen > Vom Startmenü**.
   - Um in Netzwerkfreigaben bereitgestellte Anwendungen hinzuzufügen, klicken Sie auf **Hinzufügen > Manuell** und geben Sie dann die erforderlichen Einstellungen (Pfad, Arbeitsverzeichnis…) ein.
   - Nur Maschinen mit Multisitzungs-OS: Lassen Sie die Option **Desktopbereitstellung aktivieren** aktiviert.
4. Fügen Sie der Gruppe Benutzer hinzu.

Schritt 4: Workspace-URL den Benutzern mitteilen Gehen Sie zu **Workspace-Konfiguration > Zugriff** und geben Sie den Benutzern die Workspace-URL bekannt.

Büro-PCs bereitstellen (mit Energieverwaltung)

In diesem Abschnitt wird das Bereitstellen von Büro-PCs (mit Energieverwaltung) erläutert.

Voraussetzungen

Voraussetzungen:

- Maschinennamen der PCs.

- Citrix Virtual Delivery Agent (VDA) auf jedem PC installiert. (Dieser Schritt kann nach der Katalogerstellung ausgeführt werden.)

  Weitere Informationen finden Sie unter VDA herunterladen.

Vorbereitung

Beantworten Sie die angezeigten Fragen, um die folgenden Einstellungen auf Infrastrukturebene vorzunehmen.

#	Schritt	Beschreibung
1	Wählen Sie den Maschinenzuteilungstyp aus.	Wählen Sie aus, wie die Maschinen zugewiesen werden sollen. Optionen: Statisch, automatisch zugewiesen, Statisch, vorab zugewiesen und Zufälliger Pool, nicht zugewiesen
2	Festlegen, ob Benutzer Maschinen einschalten dürfen	Wählen Sie **Ich möchte, dass Remotebenutzer ihre Maschinen selbst einschalten können**.
3	Benutzeridentitätstyp wählen	Wählen Sie einen Identitätstyp für die Benutzerverwaltung. Optionen: Active Directory, Azure Active Directory, Google Cloud Identity und Okta

Bereitstellungsschritte

Nachdem Sie die Einstellungen auf Infrastrukturebene vorgenommen haben, werden die für das Bereitstellungsszenario spezifischen Schritte angezeigt. Folgen Sie den angezeigten Anweisungen, um die Einstellungen vorzunehmen.

Schritt 1: Ressourcenstandort und Hostverbindungen hinzufügen Richten Sie den Ressourcenstandort ein, indem Sie Cloud Connectors installieren und eine Verbindung des Typs **Remote-PC Wake-On-LAN** hinzufügen.

1. Benennen Sie den Ressourcenstandort.
2. Laden Sie Cloud Connectors herunter und installieren Sie sie auf mindestens zwei Windows Server-Maschinen.
3. Führen Sie die Erkennung installierter Cloud Connectors durch.
4. Klicken Sie auf **Hinzufügen**, um eine Verbindung hinzuzufügen:

    a) Wählen Sie einen Ressourcenstandort (Zone).
    b) Wählen Sie **Remote-PC Wake-On-LAN** als **Verbindungstyp**.
    c) Geben Sie einen Namen für die Verbindung ein.

> **Hinweis:**
>
> Die Energieverwaltung von Maschinen erfolgt bei DaaS über die konfigurierten Verbindungen. Sie müssen Verbindungen des Typs **Remote-PC Wake-On-LAN** konfigurieren, wenn Sie Remote-PC-Zugriff-Kataloge für Maschinen mit Energieverwaltung erstellen.

Schritt 2: Katalog für den Remote-PC-Zugriff erstellen Erstellen Sie einen Maschinenkatalog und importieren Sie Ihre Büro-PCs.

1. Benennen Sie den Katalog.
2. Wählen Sie einen Ressourcenstandort.
3. Wählen Sie einen Maschinenzuteilungstyp aus. Standardmäßig wird der Typ angezeigt, den Sie in der Vorbereitungsphase ausgewählt haben.
4. Wählen Sie die **Wake-on-LAN-Verbindung**. Die Optionen sind Verbindungen des Typs **Remote-PC Wake-On-LAN**, die Sie für den ausgewählten Standort konfiguriert haben.
5. Importieren Sie die Maschinen.
6. Klicken Sie auf **Erstellen**.

Schritt 3: Bereitstellungsgruppen erstellen und Benutzer zuweisen Erstellen Sie eine Bereitstellungsgruppe für die Maschinen, die Sie bereitstellen möchten, und geben Sie an, wer darauf zugreifen kann.

1. Benennen Sie die Gruppe.
2. Wählen Sie nach Bedarf einen Maschinenkatalog aus. Nur die **Remote-PC-Zugriff**-Kataloge werden angezeigt.
3. Weisen Sie der Gruppe Benutzer zu.

Schritt 4: Workspace-URL den Benutzern mitteilen Gehen Sie zu **Workspace-Konfiguration > Zugriff** und geben Sie den Benutzern die Workspace-URL bekannt.

Büro-PCs bereitstellen (ohne Energieverwaltung)

In diesem Abschnitt wird das Bereitstellen von Büro-PCs (ohne Energieverwaltung) erläutert.

Voraussetzungen

Voraussetzungen:

- Maschinennamen der PCs.
- Citrix Virtual Delivery Agent (VDA) auf jedem PC installiert. (Dieser Schritt kann nach der Katalogerstellung ausgeführt werden.)

  Weitere Informationen finden Sie unter VDA herunterladen.

Vorbereitung

Beantworten Sie die angezeigten Fragen, um die folgenden Einstellungen auf Infrastrukturebene vorzunehmen.

#	Einstellung	Beschreibung
1	Wählen Sie den Maschinenzuteilungstyp aus.	Wählen Sie aus, wie die Maschinen zugewiesen werden sollen. Optionen: Statisch, automatisch zugewiesen, Statisch, vorab zugewiesen und Zufälliger Pool, nicht zugewiesen
2	Festlegen, ob Benutzer Maschinen einschalten dürfen	Lassen Sie **Ich möchte, dass Remotebenutzer ihre Maschinen selbst einschalten können** deaktiviert.
3	Benutzeridentitätstyp wählen	Wählen Sie einen Identitätstyp für die Benutzerverwaltung. Optionen: Active Directory, Azure Active Directory, Google Cloud Identity und Okta

Bereitstellungsschritte

Nachdem Sie die Einstellungen auf Infrastrukturebene vorgenommen haben, werden die für das Bereitstellungsszenario spezifischen Schritte angezeigt. Folgen Sie den angezeigten Anweisungen, um die Einstellungen vorzunehmen.

Schritt 1: Ressourcenstandort hinzufügen Richten Sie den Ressourcenstandort ein, indem Sie Cloud Connectors installieren.

1. Benennen Sie den Ressourcenstandort.
2. Laden Sie Cloud Connectors herunter und installieren Sie sie auf mindestens zwei Windows Server-Maschinen.
3. Führen Sie die Erkennung installierter Cloud Connectors durch.

> **Hinweis:**
>
> Das Erstellen von Hostverbindungen ist nur erforderlich, wenn Sie die Energieverwaltung für die Maschinen wünschen.

Schritt 2: Katalog für den Remote-PC-Zugriff erstellen Erstellen Sie einen Katalog und importieren Sie Ihre Büro-PCs.

1. Benennen Sie den Katalog.
2. Wählen Sie einen Ressourcenstandort.
3. Wählen Sie einen Zuteilungstyp. Standardmäßig wird der Typ angezeigt, den Sie in der Vorbereitungsphase ausgewählt haben.
4. Importieren Sie die Maschinen.
5. Klicken Sie auf **Erstellen**.

Schritt 3: Bereitstellungsgruppen erstellen und Benutzer zuweisen Erstellen Sie eine Bereitstellungsgruppe für die Maschinen, die Sie bereitstellen möchten, und geben Sie an, wer darauf zugreifen kann.

1. Benennen Sie die Gruppe.
2. Wählen Sie nach Bedarf einen Maschinenkatalog aus. Nur die **Remote-PC-Zugriff**-Kataloge werden angezeigt.
3. Weisen Sie der Gruppe Benutzer zu.

Schritt 4: Workspace-URL den Benutzern mitteilen Gehen Sie zu **Workspace-Konfiguration > Zugriff** und geben Sie den Benutzern die Workspace-URL bekannt.

Maschinenidentitäten

November 6, 2023

Jede Maschine muss eine eindeutige Maschinenidentität haben (“Computerkonto”). Maschinenidentitäten können lokal auf der Maschine oder in einem Verzeichnis (z. B. einem On-Premises-Active Directory oder Azure AD) erstellt und verwaltet werden. Citrix unterstützt das Hosten virtueller Anwendungen und Desktops auf in Active Directory oder Azure Active Directory eingebundenen Maschinen, Maschinen mit Azure AD-Hybrideinbindung oder auf Maschinen ohne Domänenbindung.

Maschinenidentitätstypen

Die folgenden Maschinenidentitätstypen werden unterstützt.

Maschinenidentitätstyp	Beschreibung
AD-Einbindung	Die Identitäten werden im On-Premises-Active Directory erstellt und verwaltet. Bereitgestellte Maschinen werden anhand der zugewiesenen Maschinenidentitäten mit dem On-Premises-Active Directory verbunden.
In Azure AD eingebunden	Die Identitäten werden in Azure AD erstellt und verwaltet. Bereitgestellte Maschinen werden anhand der zugewiesenen Maschinenidentitäten mit Azure AD verbunden. Das Importieren von VMs in Citrix DaaS wird nicht unterstützt.
Azure AD-Hybrideinbindung	Die Identitäten werden im On-Premises-Active Directory erstellt und per Azure AD Connect mit Azure AD synchronisiert. Bereitgestellte Maschinen werden anhand der zugewiesenen Maschinenidentitäten mit dem On-Premises-Active Directory und Azure AD verbunden. Die Maschinen besitzen dann eine Azure AD-Hybrideinbindung. Beim Importieren einer VM mit Azure AD-Hybrideinbindung wird die VM von Citrix DaaS wie eine VM mit Active Directory-Einbindung behandelt.

Maschinenidentitätstyp	Beschreibung
Nicht domänengebunden	Die Identitäten werden auf den Maschinen lokal erstellt und verwaltet. Das Importieren von VMs in Citrix DaaS wird nicht unterstützt.

Unterstützte Konfigurationen

Im Folgenden werden die unterstützten Konfigurationen für jedes Szenario erläutert.

Unterstützte Infrastruktur

Maschinenidentität	Citrix DaaS	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
AD-Einbindung	Ja	Ja	Ja	Ja	Ja
In Azure AD eingebunden	Ja	Ja	Nein	Ja	Nein
Azure AD-Hybrideinbindung	Ja	Ja	Ja	Ja	Ja
Nicht domänengebunden	Ja	Ja	Ja	Ja	Ja

> **Hinweis**
>
> Weder “Lokaler Hostcache”noch “Servicekontinuität”sind für nicht domänengebundene Sitzungshosts verfügbar, wenn StoreFront verwendet wird.

Unterstützte Identitätsanbieter für die Workspace-Authentifizierung

Maschinenidentität	Azure Active Directory	Active Directory	Active Directory und Token	Okta	SAML	Citrix Gateway	Adaptive Authen-tifizierung
AD-Einbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
In Azure AD einge-bunden	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Azure AD-Hybrideinbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Nicht domä-nenge-bunden	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Active Directory-Einbindung

July 3, 2023

Die Identitäten werden im On-Premises-Active Directory erstellt und verwaltet. Bereitgestellte Maschinen werden anhand der zugewiesenen Maschinenidentitäten mit dem On-Premises-Active Directory verbunden. Weitere Informationen zu unterstützten Funktionsebenen für Gesamtstruktur und Domäne finden Sie unter Funktionsebenen von Active Directory.

Informationen zum Erstellen von in Active Directory (AD) eingebundenen Katalogen mit Citrix DaaS finden Sie unter Maschinenkataloge erstellen.

In Azure Active Directory eingebunden

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt

> auf Microsoft Entra ID.

Dieser Artikel enthält alle Anforderungen, die zusätzlich zu den Systemanforderungen für Citrix DaaS erforderlich sind, um in Azure Active Directory (AAD) eingebundene Kataloge mit Citrix DaaS zu erstellen.

Anforderungen

- Steuerungsebene: Siehe Unterstützte Konfigurationen.
- VDA-Typ: Einzelsitzung (nur Desktops) und Multisitzung (Apps und Desktops)
- VDA-Version: 2203 oder höher
- Provisioningtyp: Maschinenerstellungsdienste (MCS), persistent und nicht persistent mit Maschinenprofil-Workflow
- Zuweisungstyp: dediziert und gepoolt
- Hostingplattform: nur Azure
- Rendezvous V2 muss aktiviert sein.

Einschränkungen

- Servicekontinuität wird nicht unterstützt.
- Single Sign-On bei virtuellen Desktops wird nicht unterstützt. Die Benutzer müssen ihre Anmeldeinformationen manuell eingeben, wenn sie sich bei ihren Desktops anmelden.
- Die Anmeldung beim virtuellen Desktop mit Windows Hello wird nicht unterstützt. Es werden derzeit nur Benutzername und Kennwort unterstützt. Wenn ein Benutzer versucht, sich mit einem Windows Hello-Verfahren anzumelden, wird gemeldet, dass er nicht der vermittelte Benutzer ist, und die Sitzung wird getrennt. Zugeordnete Verfahren sind PIN, FIDO2-Schlüssel, Multifaktorauthentifizierung usw.
- Unterstützung nur für Microsoft Azure Resource Manager-Cloudumgebungen.
- Beim ersten Start einer virtuellen Desktopsitzung kann zur Windows-Anmeldung die Anmeldeaufforderung für den zuletzt angemeldeten Benutzer angezeigt werden, ohne Option zum Wechseln des Benutzers. Der Benutzer muss warten, bis das Timeout eintritt und der Sperrbildschirm des Desktops angezeigt wird, und dann auf den Sperrbildschirm klicken, um den Anmeldebildschirm wieder anzuzeigen. Er kann dann **Andere Benutzer** auswählen und seine eigenen Anmeldeinformationen eingeben. Dies ist das Verhalten bei jeder neuen Sitzung, wenn die Maschinen nicht persistent sind.

Überlegungen

Imagekonfiguration

- Sie können Ihr Windows-Image bei Bedarf mit Citrix Optimizer optimieren.

In Azure AD eingebunden

- Deaktivieren Sie ggf. Windows Hello, damit Benutzer nicht zur Einrichtung aufgefordert werden, wenn sie sich an ihrem virtuellen Desktop anmelden. Wenn Sie VDA 2209 oder höher verwenden, erfolgt dies automatisch. Bei früheren Versionen haben Sie hierfür zwei Optionen:
  - Gruppenrichtlinie oder lokale Richtlinie
    - Gehen Sie zu **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows Hello for Business**.
    - Legen Sie für **Windows Hello for Business verwenden** Folgendes fest:
      - **Deaktiviert** oder
      - **Aktiviert** und wählen Sie **Do not start Windows Hello provisioning after sign-in**.
  - Microsoft Intune
    - Erstellen Sie ein Geräteprofil, das Windows Hello for Business deaktiviert. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
    - Derzeit unterstützt Microsoft nur die Intune-Registrierung für persistente Maschinen. Sie können nicht persistente Maschinen daher nicht mit Intune verwalten.
- Den Benutzern muss explizit Zugriff in Azure zur Anmeldung bei den Maschinen mit ihren AAD-Anmeldeinformationen gewährt werden. Dies kann erleichtert werden, indem die Rollenzuweisung auf der Ebene der Ressourcengruppen hinzugefügt wird:
  1. Melden Sie sich beim Azure-Portal an.
  2. Wählen Sie **Ressourcengruppen**.
  3. Klicken Sie auf die Ressourcengruppe mit den virtuellen Desktop-Workloads.
  4. Wählen Sie **Access control (IAM)**.
  5. Klicken Sie auf **Add role assignment**.
  6. Wählen Sie in der Liste **Virtual Machine User Login** und klicken Sie auf **Next**.
  7. Wählen Sie **User, group, or service principal**.
  8. Klicken Sie auf **Select members** und wählen Sie die Benutzer und Gruppen, denen Sie Zugriff auf die virtuellen Desktops gewähren möchten.
  9. Klicken Sie auf **Select**.
  10. Klicken Sie auf **Review + assign**.

11. Klicken Sie erneut auf **Review + assign**.

> **Hinweis:**
>
> Wenn Sie MCS die Ressourcengruppe für die virtuellen Desktops erstellen lassen, fügen Sie diese Rollenzuweisung nach Erstellung des Maschinenkatalogs hinzu.

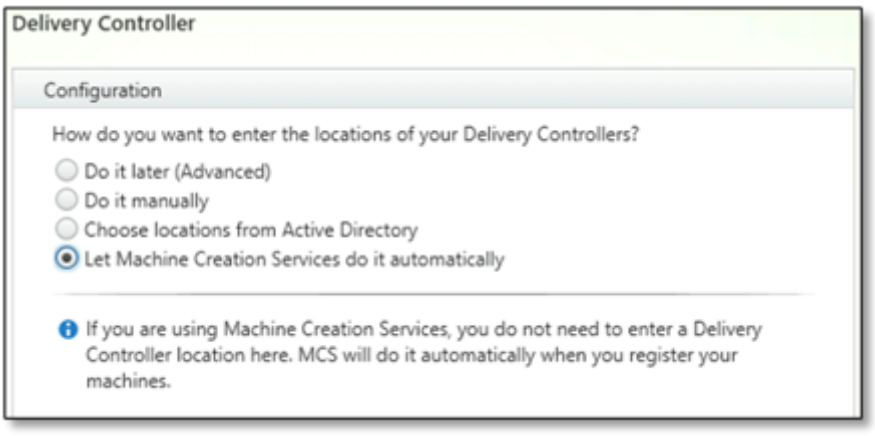
- Master-VMs können in Azure AD eingebunden oder nicht domänengebunden sein. Für diese Funktion ist VDA-Version 2212 oder höher erforderlich.

VDA-Installation und -Konfiguration

Folgen Sie den Schritten zur Installation des VDAs:

1. Wählen Sie im Installationsassistenten die folgenden Optionen aus:
   - Wählen Sie auf der Seite "Umgebung"die Option **MCS-Masterimage erstellen**.

   - Wählen Sie auf der Seite "Delivery Controller"die Option **Automatische Erstellung durch Maschinenerstellungsdienste**.



2. Wenn der VDA installiert ist, fügen Sie den folgenden Registrierungswert hinzu:

   - Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Werttyp: DWORD
   - Wertname: GctRegistration
   - Wertdaten: 1

3. Erstellen Sie auf Master-VMs mit Windows 11 22H2 einen geplanten Task, der den folgenden Befehl beim Systemstart mit dem SYSTEM-Konto ausführt. Das Planen eines Task in der Master-VM ist nur für VDA-Version 2212 oder früher erforderlich.

   ```
   reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
       /d Citrix /f
   <!--NeedCopy-->
   ```

4. Wenn Sie die Master-VM in Azure AD einbinden und das Einbinden dann über das Hilfsprogramm `dsregcmd` manuell aufheben, stellen Sie sicher, dass der Wert `AADLoginForWindowsExtensionJoin` unter HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension Null ist.

So geht es weiter

Sobald der Ressourcenstandort und die Hostingverbindung verfügbar sind, erstellen Sie den Maschinenkatalog. Weitere Informationen zum Erstellen von in Azure Active Directory eingebundenen Maschinenkatalogen finden Sie unter In Azure Active Directory eingebundene Kataloge erstellen.

Microsoft Intune

March 6, 2024

Dieser Artikel enthält alle Anforderungen, die zusätzlich zu den Systemanforderungen von Citrix DaaS erforderlich sind, um für Microsoft Intune aktivierte Kataloge mit Citrix DaaS zu erstellen.

Microsoft Intune ist ein cloudbasierter Service für die Mobilgeräteverwaltung (MDM) und die Mobilanwendungsverwaltung (MAM). Sie können die Verwendung von Geräten Ihres Unternehmens (Mobiltelefone, Tablets, Laptops usw.) steuern. Weitere Informationen finden Sie unter Microsoft Intune. Die Geräte müssen die Mindestsystemanforderungen erfüllen. Weitere Informationen finden Sie in der Microsoft-Dokumentation In Intune unterstützte Betriebssysteme und Browser.

Microsoft Intune nutzt die Funktionalität von Azure AD.

> **Wichtig:**
>
> Bevor Sie das Feature aktivieren, vergewissern Sie sich, dass Ihre Azure-Umgebung die Lizenzanforderungen für die Verwendung von Microsoft Intune erfüllt. Informationen hierzu finden Sie in der Dokumentation von Microsoft: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses Aktivieren Sie das Feature nicht, wenn Sie die entsprechende Intune-Lizenz nicht haben.

Anforderungen

- Steuerungsebene: Citrix DaaS
- VDA-Typ: VDA für Einzelsitzungs-OS
- VDA-Version: 2203 oder höher
- Provisioningtyp: Maschinenerstellungsdienste (MCS), persistent und nur mit dem Maschinenprofil-Workflow
- Zuweisungstyp: dediziert

Einschränkungen

- Unterstützt nur in Azure AD eingebundene persistente VMs mit Einzelsitzungs-OS.
- Unterstützt nur in Azure AD eingebundene persistente VMs mit Einzelsitzungs-OS unter Verwendung von Benutzeranmeldeinformationen oder Geräteanmeldeinformationen mit Mitverwaltungsfunktion. Weitere Informationen finden Sie unter Automatisches Registrieren eines Windows-Geräts mit Gruppenrichtlinie.
- Überspringen Sie nicht die Imagevorbereitung, während Sie Maschinenkataloge erstellen oder aktualisieren.

Überlegungen

- Erstellen Sie ein Geräteprofil, das Windows Hello for Business deaktiviert.
- Verwenden Sie VDA-Version 2212 oder später, wenn Microsoft Intune eine Master-VM verwalten muss.

So geht es weiter

Informationen zum Erstellen von für Microsoft Intune aktivierten Katalogen finden Sie unter Für Microsoft Intune aktivierte Kataloge erstellen.

Azure Active Directory-Hybrideinbindung

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Dieser Artikel enthält alle Anforderungen, die zusätzlich zu den Systemanforderungen für Citrix DaaS erforderlich sind, um Kataloge mit Azure Active Directory-Hybrideinbindung (HAAD) über Citrix DaaS zu erstellen.

Maschinen mit Azure AD-Hybrideinbindung verwenden das On-Premises-AD als Authentifizierungsanbieter. Sie können sie Domänenbenutzern oder Gruppen im On-Premises-AD zuweisen. Um eine nahtlose SSO-Erfahrung für Azure AD zu ermöglichen, müssen die Domänenbenutzer mit Azure AD synchronisiert werden.

> **Hinweis:**
>
> VMs mit Azure AD-Hybrideinbindung werden in Infrastrukturen mit Verbund- und verwalteter Identität unterstützt.

Anforderungen

- Steuerungsebene: Siehe Unterstützte Konfigurationen.
- VDA-Typ: Einzelsitzung (nur Desktops) und Multisitzung (Apps und Desktops)
- VDA-Version: 2212 oder höher
- Provisioningtyp: Maschinenerstellungsdienste (MCS), persistent und nicht persistent
- Zuweisungstyp: dediziert und gepoolt
- Hostingplattform: Beliebiger Hypervisor oder Cloudservice

Einschränkungen

- Wenn Sie den Citrix Verbundauthentifizierungsdienst (FAS) verwenden, wird Single Sign-On an das On-Premises-AD und nicht an Azure AD weitergeleitet. In diesem Fall wird empfohlen, die zertifikatbasierte Azure AD-Authentifizierung zu konfigurieren. Der primäre Aktualisierungstoken (PRT) wird dann bei der Benutzeranmeldung generiert und ermöglicht einen Single Sign-On bei Azure AD-Ressourcen in der Sitzung. Andernfalls fehlt der primäre Aktualisierungstoken (PRT), und der Single Sign-On für Azure AD-Ressourcen funktioniert nicht. Informationen zum

Erreichen von Azure AD Single Sign-On (SSO) bei VDAs mit Hybrideinbindung mithilfe des Citrix Verbundauthentifizierungsdiensts (FAS) finden Sie unter VDAs mit Hybrideinbindung.

- Überspringen Sie nicht die Imagevorbereitung, während Sie Maschinenkataloge erstellen oder aktualisieren. Wenn Sie die Imagevorbereitung überspringen möchten, dürfen die Master-VMs nicht in Azure AD oder Azure AD Hybrid eingebunden sein.

Überlegungen

- Zum Erstellen hybrider Maschinen mit Azure Active Directory-Einbindung ist die Berechtigung `Write userCertificate` in der Zieldomäne erforderlich. Stellen Sie sicher, dass Sie sich bei der Katalogerstellung als Administrator mit dieser Berechtigung anmelden.
- Der Prozess der Azure AD-Hybrideinbindung wird von Citrix verwaltet. Sie müssen das von Windows gesteuerte `autoWorkplaceJoin` auf den Master-VMs wie folgt deaktivieren. Die manuelle Deaktivierung von `autoWorkplaceJoin` ist nur für VDA-Version 2212 oder früher erforderlich.

  1. Führen Sie `gpedit.msc` aus.
  2. Gehen Sie zu **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Geräteregistrierung**.
  3. Legen Sie für **In die Domäne eingebundene Computer als Geräte registrieren** die Option **Deaktiviert** fest.

- Wählen Sie die für die Synchronisierung mit Azure AD konfigurierte Organisationseinheit, wenn Sie die Maschinenidentitäten erstellen.
- Erstellen Sie auf Master-VMs mit Windows 11 22H2 einen geplanten Task, der die folgenden Befehle beim Systemstart mit dem SYSTEM-Konto ausführt. Das Planen eines Task in der Master-VM ist nur für VDA-Version 2212 oder früher erforderlich.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
   Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
       "Provider", $null)
    if ($provider -eq 'Citrix')
    {

```



```
15            break;
16         }
17
18
19        if ($provider -eq 1)
20        {
21
22            Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
                  Provider" -Value "Citrix" -Force
23            Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
                  autoWorkplaceJoin" -Value 1 -Force
24            Start-Sleep 5
25            dsregcmd /join
26            break
27         }
28
29       }
30
31
32      Start-Sleep 1
33     }
34
35   <!--NeedCopy-->
```

So geht es weiter

Weitere Informationen zum Erstellen von Katalogen mit Azure Active Directory-Hybrideinbindung finden Sie unter Kataloge mit Azure Active Directory-Hybrideinbindung erstellen.

Nicht domänengebunden

November 16, 2023

Dieser Artikel enthält alle Anforderungen, die zusätzlich zu den Systemanforderungen für Citrix DaaS erforderlich sind, um nicht domänengebundene Kataloge mit Citrix DaaS zu erstellen.

Anforderungen

- Steuerungsebene: Siehe Unterstützte Konfigurationen.
- VDA-Typ: Einzelsitzung (nur Desktops) und Multisitzung (Apps und Desktops)
- VDA-Version: 2203 oder höher
- Provisioningtyp: Maschinenerstellungsdienste (MCS), persistent und nicht persistent
- Zuweisungstyp: dediziert und gepoolt

- Hostingplattform: alle von MCS unterstützten
- Rendezvous V2 muss aktiviert sein.
- Cloud Connectors: Nur erforderlich, wenn Sie beabsichtigen, Maschinen auf On-premises-Hypervisors bereitzustellen, oder wenn Sie Active Directory als Identitätsanbieter in Workspace verwenden.

Einschränkungen

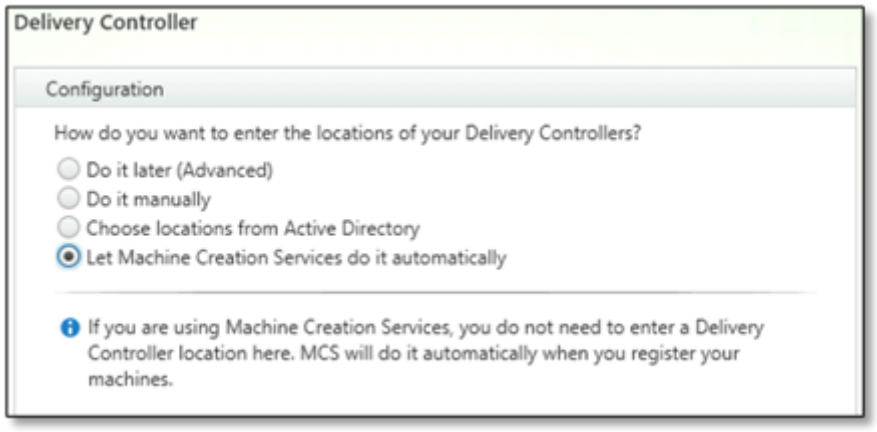
- Servicekontinuität wird nicht unterstützt.
- Bei Verwendung eines nicht domänengebundenen Multisitzungs-VDAs werden die lokalen Benutzerprofildaten beim Abmelden gelöscht.

VDA-Installation und -Konfiguration

Folgen Sie den Schritten zur Installation des VDAs:

1. Wählen Sie im Installationsassistenten die folgenden Optionen aus:
    - Wählen Sie auf der Seite "Umgebung"die Option **MCS-Masterimage erstellen**.

    - Wählen Sie auf der Seite "Delivery Controller"die Option **Automatische Erstellung durch Maschinenerstellungsdienste**.



2. Wenn der VDA installiert ist, fügen Sie den folgenden Registrierungswert hinzu:

    - Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
    - Werttyp: DWORD
    - Wertname: GctRegistration
    - Wertdaten: 1

So geht es weiter

Sobald der Ressourcenstandort und die Hostingverbindung verfügbar sind, erstellen Sie den Maschinenkatalog. Weitere Informationen zum Erstellen nicht domänengebundener Maschinenkataloge finden Sie unter Nicht domänengebundene Kataloge erstellen.

Einrichten von Ressourcenstandorten

June 12, 2024

Ressourcenstandorte enthalten die Ressourcen zur Bereitstellung von Anwendungen und Desktops für Benutzer. Sie verwalten diese Ressourcen über Citrix Cloud. Solche Ressourcen sind in der Regel:

- Hypervisors oder Clouddienste (werden auch als *Hosts* bezeichnet), darunter:
    - Active Directory-Domänencontroller.
    - Virtual Delivery Agents (VDAs): VDAs werden auf einer Maschine installiert, die den Benutzern die Anwendungen und Desktops bereitstellt.
    - Citrix Gateway (optional): Um den sicheren externen Zugriff auf die Anwendungen und Desktops für Benutzer zu ermöglichen, fügen Sie dem Ressourcenstandort ein Citrix Gateway VPX-Gerät hinzu. Richten Sie dann Citrix Gateway ein.

  - Citrix StoreFront-Server.
  - Zur Kommunikation mit Citrix Cloud muss jeder Ressourcenstandort einen Citrix Cloud Connector enthalten. Mindestens zwei Cloud Connectors pro Ressourcenstandort werden empfohlen.

Eine Zone entspricht einem Ressourcenstandort. Wenn Sie einen Ressourcenstandort erstellen und einen Cloud Connector installieren, wird automatisch eine Zone für Sie erstellt. Weitere Informationen finden Sie unter Zonen.

Weitere Informationen zu Ressourcentypen finden Sie unter Verbinden mit Citrix Cloud.

Hostanforderungen

Der Hypervisor oder Clouddienst, für den Sie virtuelle Maschinen bereitstellen, benötigt eigene Berechtigungen oder eine spezielle Einrichtung.

- Wenn der Hypervisor oder Clouddienst virtuelle Netzwerke oder andere Elemente erfordert, folgen Sie den Anweisungen in der zugehörigen Dokumentation.
- Erstellen Sie die entsprechende Virtual Private Cloud (VPC) (für AWS oder GCP) oder Virtual Network (VNET) (für Azure) für die Maschinen, die Sie Ihrem Ressourcenstandort hinzufügen.
- Erstellen Sie die erforderlichen Regeln für den Schutz eingehenden und ausgehenden Datenverkehrs zwischen den Maschinen im virtuellen Netzwerk. Konfigurieren Sie beispielsweise bei Verwendung von AWS Regeln für die VPC-Sicherheitsgruppe, sodass Maschinen in der VPC nur den von Ihnen angegebenen IP-Adressen zugänglich sind.

Die folgenden Hosttypen werden unterstützt:

- Amazon Web Services (AWS)-Virtualisierungsumgebungen
- XenServer-Virtualisierungsumgebungen
- Google Cloud Platform-Virtualisierungsumgebungen
- HPE Moonshot-Virtualisierungsumgebungen
- Microsoft Azure Resource Manager-Virtualisierungsumgebungen
- Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
- Nutanix-Virtualisierungsumgebungen
- Nutanix-Cloud und Partnerlösungen
- VMware-Virtualisierungsumgebungen
- Cloud- und Partnerlösungen von VMware

Active Directory

Stellen Sie einen Windows-Server bereit, installieren Sie Active Directory-Domänendienste (AD DS) und stufen Sie den Server zum Domänencontroller hoch. Anleitungen finden Sie in der Microsoft-

Dokumentation Übersicht über die Active Directory Domain Services.

Die wichtigsten Überlegungen sind:

- Sie müssen mindestens einen Domänencontroller mit Active Directory Domain Services ausführen.
- Installieren Sie keine Citrix Komponenten auf Domänencontrollern.

Weitere Informationen:

- Funktionsebenen von Active Directory
- Identitäts- und Zugriffsverwaltung in Citrix Cloud.
- Verbinden von Active Directory mit Citrix Cloud
- Bereitstellungsszenarios für die Verwendung von Connector Appliances mit Active Directory

Cloud Connectors

Cloud Connectors umfassen mehrere Dienste von Citrix Cloud und ermöglichen die Kommunikation zwischen den VDAs, StoreFront und dem cloudbasierten Delivery Controller. Sie können Cloud Connectors interaktiv oder über die Befehlszeile installieren.

Weitere Informationen zu Cloud Connectors finden Sie unter:

- Citrix Cloud Connector
- Technische Informationen
- Proxy- und Firewall-Konfiguration
- Installation
- Connector-Updates

Überlegungen zu Skalierung und Größe

- Wenn Sie Citrix DaaS auf Größe und Skalierbarkeit prüfen, sollten Sie alle Komponenten berücksichtigen.
- Testen Sie, ob die gewählte Konfiguration aus Cloud Connectors und StoreFront Ihren spezifischen Anforderungen entspricht.
- Zu knapp dimensionierte Maschinen können sich negativ auf die Systemleistung auswirken.

Der Artikel Überlegungen zur Skalierung und Größe für Cloud Connectors enthält:

- Informationen zu Größen- und Skalierungstests
- Getestete Höchstkapazitäten
- Empfehlungen nach bewährten Methoden für die Cloud Connector-Maschinenkonfiguration

Ressourcentyp hinzufügen

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü links oben die Option **Ressourcenstandorte**.
3. Wählen Sie **+ Ressourcenstandorte**, um einen Ressourcenstandort hinzuzufügen.
4. Geben Sie einen Namen für den Ressourcenstandort ein und klicken Sie auf **Speichern**. Was bei der Benennung zu berücksichtigen ist, lesen Sie unter Namenseinschränkungen.
5. Wählen Sie unter dem neuen Ressourcenstandort die Option **Cloud Connectors**.
6. Laden Sie die Cloud Connector-Software herunter und installieren Sie sie auf mindestens zwei Servern in der Domäne, in der sich die Citrix DaaS-Ressourcen befinden.
   - Wählen Sie während der Installation den Ressourcenstandort aus, den Sie in den vorherigen Schritten erstellt haben.
   - Nach der Installation fügt Citrix Cloud die Server zum Ressourcenstandort hinzu und registriert die Domänen, in denen Sie die Cloud Connectors installiert haben.
7. Stellen Sie sicher, dass die registrierten Domänen aktiv sind:
   - Klicken Sie im Menü "Citrix Cloud"auf **Identitäts- und Zugriffsverwaltung**.
   - Wählen Sie **Domänen**. Es wird eine Liste der Domänen angezeigt, in denen Cloud Connectors bereitgestellt wurden.
   - Suchen Sie die Domänen, die Sie mit Citrix DaaS verwenden. Für aktive Domänen wird links vom Domäneneintrag ein grüner Balken angezeigt.

   Wenn für Ihre Domäne der Balken nicht angezeigt wird, ist die Domäne im Status **ungenutzt**. Wenn Sie beim Einrichten des Maschinenkatalogs eine ungenutzte Domäne angeben, schlägt die Katalogerstellung fehl. Folgen Sie den Schritten unter Ungenutzte Domäne aktivieren, um sicherzustellen, dass der Maschinenkatalog erfolgreich eingerichtet werden kann.

   Weitere Informationen finden Sie unter CTX473009: DaaS Catalog Creation Wizard: "Internal Server Error"when creating adding new machine accounts.

Ungenutzte Domäne aktivieren

1. Wählen Sie auf der Registerkarte **Domäne** unter **Identitäts- und Zugriffsverwaltung** die Option **Ungenutzte Domänen anzeigen**. Nachdem Sie diese Option ausgewählt haben, ändert sich die Bezeichnung in **Ungenutzte Domänen ausblenden**.
2. Suchen Sie die ungenutzte Domäne in der Liste. Bei ungenutzten Domänen wird links vom Domäneneintrag ein grauer Balken und auf der rechten Seite ein Dreipunktmenü (…) mit einzelner Option angezeigt.

3. Wählen Sie das Dreipunktmenü und dann **Domäne verwenden**. Der Farbe des Balkens wechselt von Grau zu Grün, und im Dreipunktmenü wird jetzt **Deaktivieren** angezeigt.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Einrichten des Ressourcenstandorts für bestimmte Hosttypen:
  - AWS-Virtualisierungsumgebungen
  - Google Cloud-Virtualisierungsumgebungen
  - HPE Moonshot-Virtualisierungsumgebungen
  - Microsoft Azure Resource Manager-Virtualisierungsumgebungen
  - Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
  - Nutanix-Virtualisierungsumgebungen
  - Nutanix-Cloud und Partnerlösungen
  - VMware-Virtualisierungsumgebungen
  - Cloud- und Partnerlösungen von VMware
  - XenServer-Virtualisierungsumgebungen
- Für eine vollständige Bereitstellung erstellen und verwalten Sie Verbindungen und Ressourcen zu einem Ressourcenstandort.
- Überprüfen Sie alle Schritte des Installations- und Konfigurationsprozesses

AWS-Virtualisierungsumgebungen

March 31, 2024

In diesem Artikel wird beschrieben, wie Sie Ihr AWS-Konto als Ressourcenstandort einrichten, den Sie mit Citrix DaaS verwenden können.

Der Ressourcenstandort enthält eine Reihe grundlegender Komponenten, die sich ideal für Machbarkeitsstudien oder andere Bereitstellungen eignen, bei denen keine Ressourcenverteilung über mehrere Verfügbarkeitszonen erforderlich ist.

Mit den im vorliegenden Artikel aufgeführten Aufgaben wird ein Ressourcenstandort mit folgenden Komponenten erstellt:

- Eine virtuelle private Cloud (VPC) mit öffentlichen und privaten Subnetzen in einer einzelnen Verfügbarkeitszone.

- Eine Instanz, die sowohl als Active Directory-Domänencontroller als auch als DNS-Server ausgeführt wird und im privaten Subnetz der VPC residiert.
- Zwei mit der Domäne verbundene Instanzen, auf denen Citrix Cloud Connector installiert ist und die im privaten Subnetz der VPC residieren.
- Eine Instanz, die als Bastion Host fungiert und im öffentlichen Subnetz der VPC residiert. Mit dieser Instanz werden RDP-Verbindungen zu den Instanzen im privaten Subnetz für Verwaltungszwecke initiiert. Wenn Sie den Ressourcenstandort eingerichtet haben, können Sie diese Instanz herunterfahren, sodass sie nicht mehr ohne Weiteres verfügbar ist. Wenn Sie andere Instanzen im privaten Subnetz verwalten müssen, z. B. VDA-Instanzen, müssen Sie die Bastionshostinstanz neu starten.

Nachdem Sie die Aufgaben ausgeführt haben, können Sie VDAs installieren, Maschinen bereitstellen und Maschinenkataloge sowie Bereitstellungsgruppen erstellen.

Aufgabenüberblick

Einrichten einer virtuellen privaten Cloud (VPC) mit öffentlichen und privaten Subnetzen: Wenn Sie diese Aufgabe ausführen, stellt AWS NAT-Gateways mit einer Elastic IP-Adresse im öffentlichen Subnetz bereit. Dadurch können Instanzen im privaten Subnetz auf das Internet zugreifen. Instanzen im öffentlichen Subnetz sind für eingehenden öffentlichen Datenverkehr zugänglich, Instanzen im privaten Subnetz dagegen nicht.

Konfigurieren von Sicherheitsgruppen. Sicherheitsgruppen fungieren als virtuelle Firewall und steuern den Datenverkehr für die Instanzen in der VPC. Sie fügen den Sicherheitsgruppen Regeln zur Kommunikation zwischen Instanzen im öffentlichen und im privaten Subnetz hinzu. Sie ordnen die Sicherheitsgruppen außerdem jeder Instanz in der VPC zu.

Erstellen eines DHCP-Optionssatzes. Amazon-VPC, DHCP und DNS-Dienste werden standardmäßig bereitgestellt, was sich auf Ihre Konfiguration von DNS auf dem Active Directory-Domänencontroller auswirkt. Amazon-DHCP kann nicht deaktiviert werden und das Amazon-DNS kann nur für die öffentliche DNS-Auflösung, nicht aber für die Active Directory-Namensauflösung verwendet werden. Um die Domänen- und Namenserver anzugeben, die Instanzen über DHCP übergeben werden, erstellen Sie einen DHCP-Optionssatz. Dieser weist das Active Directory-Domänensuffix zu und gibt den DNS-Server für alle Instanzen in der VPC an. Um sicherzustellen, dass Host- (A) und Reverse-Lookup-Datensätze (PTR-Datensätze) automatisch registriert werden, wenn Instanzen der Domäne beitreten, konfigurieren Sie die Netzwerkadaptereigenschaften für jede Instanz, die Sie dem privaten Subnetz hinzufügen.

Fügen Sie einen Bastion Host, Domänencontroller und Cloud Connector zur VPC hinzu. Über den Bastion Host können Sie sich bei Instanzen im privaten Subnetz anmelden, um die Domäne einzurichten, der Domäne Instanzen anzufügen und den Cloud Connector zu installieren.

Aufgabe 1: Einrichten der VPC

1. Wählen Sie in der AWS-Verwaltungskonsole **VPC**.
2. Wählen Sie im VPC-Dashboard die Option **Create VPC**.
3. Wählen Sie **VPC and more**.
4. Wählen Sie unter "NAT gateways ($)"**In 1 AZ** oder **1 per AZ**.
5. Lassen Sie unter "DNS Options"die Option **Enable DNS hostnames** aktiviert.
6. Wählen Sie **Create VPC**. AWS erstellt das öffentliche und private Subnetz, das Internetgateway, die Routingtabellen und die Standardsicherheitsgruppe.

> **Hinweis:**
>
> Wenn Sie den Namen einer AWS Virtual Private Cloud (VPC) in der AWS-Konsole ändern, wird die vorhandene Hostingeinheit in der Citrix Cloud beschädigt. Bei unterbrochener Hostingeinheit können Sie keine Kataloge erstellen oder Maschinen zu Katalogen hinzufügen. Aus bekanntem Problem: PMCS-7701

Aufgabe 2: Konfigurieren von Sicherheitsgruppen

Bei diesem Vorgang werden die folgenden Sicherheitsgruppen für die VPC erstellt und konfiguriert:

- Eine öffentliche Sicherheitsgruppe, die den Instanzen in Ihrem öffentlichen Subnetz zugeordnet werden.
- Eine private Sicherheitsgruppe, die den Instanzen in Ihrem privaten Subnetz zugeordnet werden.

So erstellen Sie die Sicherheitsgruppen:

1. Wählen Sie im VPC-Dashboard **Sicherheitsgruppen**.
2. Erstellen Sie eine Sicherheitsgruppe für die öffentliche Sicherheitsgruppe. Wählen Sie **Create Security Group** und geben Sie einen Namen und eine Beschreibung für die Gruppe ein. Wählen Sie unter "VPC"die VPC aus, die Sie zuvor erstellt haben. Wählen Sie **Yes, Create**.

Öffentliche Sicherheitsgruppe konfigurieren

1. Wählen Sie in der Liste der Sicherheitsgruppen die private Sicherheitsgruppe aus.
2. Wählen Sie die Registerkarte **Inbound Rules** und dann "Edit", um die folgenden Regeln zu erstellen:

Typ	Quelle
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	Wählen Sie die öffentliche Sicherheitsgruppe.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Sitzungszuverlässigkeit)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Wenn Sie fertig sind, wählen Sie **Speichern**.
4. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit**, um die folgenden Regeln zu erstellen:

Typ	Ziel
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Wenn Sie fertig sind, wählen Sie **Speichern**.

Private Sicherheitsgruppe konfigurieren

1. Wählen Sie in der Liste der Sicherheitsgruppen die private Sicherheitsgruppe aus.
2. Wenn Sie den Verkehr von der öffentlichen Sicherheitsgruppe noch nicht eingerichtet haben, müssen Sie TCP-Ports einrichten. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit**, um die folgenden Regeln zu erstellen:

Typ	Quelle
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.

Typ	Quelle
ALL Traffic	Wählen Sie die öffentliche Sicherheitsgruppe.
ICMP	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 53 (DNS)	Wählen Sie die öffentliche Sicherheitsgruppe.
UDP 53 (DNS)	Wählen Sie die öffentliche Sicherheitsgruppe.
80 (HTTP)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 135	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 389	Wählen Sie die öffentliche Sicherheitsgruppe.
UDP 389	Wählen Sie die öffentliche Sicherheitsgruppe.
443 (HTTPS)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 1494 (ICA/HDX)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 2598 (Sitzungszuverlässigkeit)	Wählen Sie die öffentliche Sicherheitsgruppe.
3389 (RDP)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 49152–65535	Wählen Sie die öffentliche Sicherheitsgruppe.

3. Wenn Sie fertig sind, wählen Sie **Speichern**.
4. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit**, um die folgenden Regeln zu erstellen:

Typ	Ziel
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Wenn Sie fertig sind, wählen Sie **Speichern**.

Aufgabe 3: Starten von Instanzen

Im folgenden Verfahren erstellen Sie die vier EC2-Instanzen und das von Amazon generierte Standardadministratorkennwort wird entschlüsselt:

1. Wählen Sie in der AWS-Verwaltungskonsole **EC2**.
2. Wählen Sie im EC2-Dashboard **Launch Instance**.
3. Wählen Sie ein Windows Server-Maschinenimage und einen Instanztyp.
4. Geben Sie auf der Seite **Configure Instance Details** einen Namen für die Instanz ein und wählen Sie die zuvor eingerichtete VPC aus.
5. Treffen Sie unter **Subnet** für jede Instanz folgende Auswahl:
   - Bastion host: Wählen Sie das öffentliche Subnetz
   - Domain controller and Connectors: Wählen Sie das private Subnetz
6. Treffen Sie unter **Auto-assign Public IP address** für jede Instanz folgende Auswahl:
   - Bastion host: Wählen Sie **Enable**
   - Domain controller and Connectors: Wählen Sie **Use default setting** oder **Disable**
7. Geben Sie für **Network Interfaces** eine primäre IP-Adresse innerhalb des IP-Bereichs des privaten Subnetzes für die Domänencontroller- und Cloud Connector-Instanzen ein.
8. Ändern Sie auf der Seite **Add Storage** bei Bedarf die Datenträgergröße.
9. Geben Sie auf der Seite **Tag Instance** einen Anzeigenamen für jede Instanz ein.
10. Wählen Sie auf der Seite **Configure Security Groups** die Option **Select an existing security group** und treffen Sie dann für jede Instanz die folgende Auswahl:
    - Bastion host: Wählen Sie die öffentliche Sicherheitsgruppe.
    - Domain controller and Connectors: Wählen Sie die private Sicherheitsgruppe.
11. Überprüfen Sie Ihre Auswahl und wählen Sie **Launch**.
12. Erstellen Sie ein neues Schlüsselpaar oder wählen Sie ein vorhandenes aus. Wenn Sie ein neues Schlüsselpaar erstellen, laden Sie die private Schlüsseldatei (`.pem`) herunter und bewahren Sie sie an einem sicheren Ort auf. Sie müssen den privaten Schlüssel angeben, wenn Sie das Standardadministratorkennwort für die Instanz beschaffen.
13. Wählen Sie **Launch Instances** aus. Wählen Sie **View Instance**aus, um eine Liste Ihrer Instanzen anzuzeigen. Warten Sie, bis die neu gestartete Instanz alle Statusprüfungen bestanden hat, bevor Sie darauf zugreifen.
14. Beschaffen Sie das Standardadministratorkennwort für jede Instanz.
    a) Wählen Sie die Instanz aus der Liste aus und wählen Sie **Connect**.
    b) Gehen Sie zur Registerkarte **RDP client**, wählen Sie **Get Password** und laden Sie Ihre private Schlüsseldatei (`.pem`) hoch, wenn Sie dazu aufgefordert werden.
    c) Wählen Sie **Decrypt Password**, um das menschenlesbare Kennwort zu erhalten. AWS zeigt das Standardkennwort an.

15. Wiederholen Sie alle Schritte ab Schritt 2, bis Sie vier Instanzen erstellt haben:

    - Eine Bastionshostinstanz in Ihrem öffentlichen Subnetz
    - Drei Instanzen in Ihrem privaten Subnetz, die wie folgt verwendet werden können:
      - eine als Domänencontroller
      - zwei als Cloud Connectors

Aufgabe 4: Erstellen eines DHCP-Optionssatzes

1. Wählen Sie im VPC-Dashboard **DHCP Options Sets**.
2. Geben Sie die folgenden Informationen ein:

    - Name tag: Geben Sie einen Anzeigenamen für den Satz ein.
    - Domain name: Geben Sie den vollqualifizierten Domänennamen ein, den Sie beim Konfigurieren der Domänencontrollerinstanz verwenden möchten.
    - Domain name servers: Geben Sie die private IP-Adresse, die Sie der Domänencontrollerinstanz zugewiesen haben, und die Zeichenfolge **AmazonProvidedDNS** getrennt durch Kommas ein.
    - NTP servers: Lassen Sie dieses Feld leer.
    - NetBIOS name servers: Geben Sie die private IP-Adresse der Domänencontrollerinstanz ein.
    - NetBIOS node type: Geben Sie **2** ein.

3. Wählen Sie **Yes, Create**.
4. Verknüpfen des neuen Satzes mit der VPC:

    a) Wählen Sie im VPC-Dashboard **Your VPCs** und dann die VPC, die Sie zuvor eingerichtet haben.
    b) Wählen Sie **Actions > Edit DHCP Options Set**.
    c) Wenn Sie dazu aufgefordert werden, wählen Sie den neuen Satz, den Sie erstellt haben, und wählen Sie **Save**.

Aufgabe 5: Konfigurieren der Instanzen

1. Stellen Sie mit einem RDP-Clients eine Verbindung mit der öffentlichen IP-Adresse der Bastionhostinstanz her. Geben Sie die Anmeldeinformationen für das Administratorkonto ein, wenn Sie dazu aufgefordert werden.
2. Starten Sie **Remote Desktop Connection** auf der Bastionshostinstanz und stellen Sie eine Verbindung zur privaten IP-Adresse der Instanz her, die Sie konfigurieren möchten. Geben Sie die Anmeldeinformationen für die Instanz ein, wenn Sie dazu aufgefordert werden.

3. Konfigurieren Sie für alle Instanzen im privaten Subnetz folgende DNS-Einstellungen:

   a) Wählen Sie **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**. Doppelklicken Sie auf die angezeigte Netzwerkverbindung.

   b) Wählen Sie **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties**.

   c) Wählen Sie **Advanced > DNS**. Achten Sie darauf, dass die folgenden Einstellungen aktiviert sind, und wählen Sie **OK**:

      - **Register this connection's addresses in DNS**
      - **Use this connection's DNS suffix in DNS registration**

4. Domänencontroller konfigurieren:

   a) Fügen Sie mit Server-Manager die Active Directory-Domänendiensterolle mit allen Standardfeatures hinzu.
   b) Stufen Sie die Instanz auf einen Domänencontroller hoch. Aktivieren Sie im Rahmen der Heraufstufung DNS und verwenden Sie den Domänennamen, den Sie beim Erstellen des DHCP-Optionssatzes festgelegt haben. Starten Sie die Instanz neu, wenn Sie dazu aufgefordert werden.

5. Ersten Cloud Connector konfigurieren:

   a) Fügen Sie die Instanz der Domäne an und führen Sie einen Neustart aus, wenn Sie dazu aufgefordert werden. Stellen Sie auf der Bastionshostinstanz mit RDP die Verbindung zur Instanz wieder her.
   b) Melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü oben links **Ressourcenstandorte**.
   c) Cloud Connector herunterladen
   d) Wenn Sie dazu aufgefordert werden, führen Sie die Datei `cwcconnector.exe` aus und geben Sie Ihre Citrix Cloud-Anmeldeinformationen ein. Folgen Sie die Anweisungen des Assistenten.
   e) Wenn Sie fertig sind, wählen Sie **Aktualisieren**, um die Seite **Ressourcenstandorte** anzuzeigen. Wenn der Cloud Connector registriert ist, wird die Instanz auf der Seite angezeigt.

6. Wiederholen Sie die Schritte zur Konfiguration des Cloud Connectors, um den zweiten Cloud Connector zu konfigurieren.

7. Hängen Sie eine IAM-Richtlinie an die Cloud Connectors an, um AWS-Hostingverbindungen mit rollenbasierter Autorisierung zu unterstützen. An einem Resosurcenstandort muss dieselbe IAM-Richtlinie an alle Cloud Connectors angehängt werden. Weitere Informationen zu den AWS-Berechtigungen finden Sie unter Erforderliche AWS-Berechtigungen.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Weitere Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu AWS.
- Überprüfen Sie alle Schritte des Installations- und Konfigurationsprozesses

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Google Cloud-Virtualisierungsumgebungen

May 17, 2024

Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) ermöglicht das Provisioning und Verwalten von Maschinen in Google Cloud.

Voraussetzungen

Bevor Sie mit der Bereitstellung der VMs für die Google Cloud Platform (GCP) beginnen, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind.

1. Das Citrix-Abonnement muss Unterstützung für hybride Multi-Cloud-Workloads beinhalten. Weitere Informationen finden Sie unter Citrix-Abonnementfunktionen vergleichen.
2. Das Administratorkonto muss über ausreichende Berechtigungen verfügen, um Hostverbindungen, Maschinenkataloge und Bereitstellungsgruppen zu erstellen. Weitere Informationen finden Sie unter Delegierte Administration konfigurieren.
3. Identifizieren Sie ein Google Cloud-Projekt, in dem alle mit dem Maschinenkatalog verknüpften Rechenressourcen gespeichert sind. Dies kann ein bestehendes oder ein neues Projekt sein. Weitere Informationen finden Sie unter Google Cloud -Projekte.
4. Aktivieren Sie die Google Cloud-APIs, die für die Integration in Citrix DaaS erforderlich sind. Weitere Informationen finden Sie unter Google Cloud-APIs aktivieren.
5. Erstellen Sie die Dienstkonten in Google Cloud und gewähren Sie die entsprechenden Berechtigungen. Weitere Informationen finden Sie unter Dienstkonten konfigurieren und aktualisieren.

6. Laden Sie die Schlüsseldatei für das Citrix Cloud-Dienstkonto herunter. Weitere Informationen finden Sie unter Citrix Cloud-Dienstkontoschlüssel.
7. Die virtuellen Maschinen müssen Zugriff auf die Google-APIs ohne öffentliche IP-Adresse haben. Weitere Informationen finden Sie unter Aktivieren des privaten Google-Zugriffs.

Google Cloud-Projekte

Es gibt grundsätzlich zwei Arten von Google Cloud-Projekten:

- Bereitstellungsprojekt: Hier besitzt das aktuelle Administratorkonto die bereitgestellten Maschinen im Projekt. Das Projekt wird auch als "lokales Projekt"bezeichnet.
- Freigegebene-VPC-Projekt: Projekt, in dem im Bereitstellungsprojekt erstellte Maschinen die VPC aus dem Freigegebene-VPC-Projekt verwenden. Das für das Bereitstellungsprojekt verwendete Administratorkonto hat in diesem Projekt eingeschränkte Berechtigungen, spezifisch hat es nur Berechtigungen zur Verwendung der VPC.

Service-Endpunkt-URLs

Sie müssen Zugriff auf die folgenden URLs haben:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Aktivieren von Google Cloud-APIs

Um die Google Cloud-Funktionalität über die Oberfläche "Vollständige Konfiguration"von Citrix DaaS zu verwenden, müssen Sie diese APIs in Ihrem Google Cloud-Projekt aktivieren:

- Compute Engine-API
- Cloud Resource Manager-API
- Identitäts- und Zugriffsverwaltung (IAM)-API
- Cloud Build-API

Führen Sie in der Google Cloud-Konsole die folgenden Schritte aus:

1. Wählen Sie im oberen linken Menü **APIs und Services > Enabled APIs & services**.
2. Stellen Sie im Bildschirm **Enabled APIs & services** sicher, dass die Compute Engine-API aktiviert ist. Wenn nicht, führen Sie folgende Schritte aus:

a) Gehen Sie zu **APIs & Services > Library**.
b) Geben Sie im Suchfeld den Begriff *Compute Engine* ein.
c) Wählen Sie in den Suchergebnissen **Compute Engine API**.
d) Wählen Sie **Enable** auf der Seite **Compute Engine API**.

3. Aktivieren Sie die Cloud Resource Manager-API.

a) Gehen Sie zu **APIs & Services > Library**.
b) Geben Sie im Suchfeld den Begriff *Cloud Resource Manager* ein.
c) Wählen Sie in den Suchergebnissen **Cloud Resource Manager API**.
d) Wählen Sie **Enable** auf der Seite **Cloud Resource Manager-API**. Der Status der API wird angezeigt.

4. Aktivieren Sie auf ähnliche Weise die **Identity and Access Management-API (IAM)** und die **Cloud Build API** sowie die **Cloud Key Management Service-API (KMS)**.

Sie können die APIs auch mit Google Cloud Shell aktivieren. Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie die Google-Konsole und laden Sie die Cloud Shell.
2. Führen Sie in der Cloud Shell folgende vier Befehle aus:

- gcloud services enable compute.googleapis.com
- gcloud services enable cloudresourcemanager.googleapis.com
- gcloud services enable iam.googleapis.com
- gcloud services enable cloudbuild.googleapis.com
- gcloud services enable cloudkms.googleapis.com

3. Klicken Sie auf **Authorize**, wenn Sie die Cloud Shell dazu auffordert.

Dienstkonten konfigurieren und aktualisieren

> **Hinweis:**
>
> Ab dem 29. April 2024 führt GCP Änderungen am Standardverhalten von Cloud Build Services und der Verwendung von Dienstkonten ein. Weitere Informationen finden Sie unter Änderungen des Cloud Build-Dienstkontos. Ihre bestehenden Google-Projekte mit aktivierter Cloud Build API vor dem 29. April 2024 sind von dieser Änderung nicht betroffen. Wenn Sie jedoch das bestehende Cloud Build Service-Verhalten nach dem 29. April beibehalten möchten, können Sie die Organisationsrichtlinie erstellen oder anwenden, um die Durchsetzung der Einschränkungen zu deaktivieren, bevor Sie die Cloud Build API aktivieren. Daher ist der folgende Inhalt zweigeteilt: Vor dem 29. April 2024 und Nach dem 29. April 2024. Wenn Sie die neue Organisationsrichtlinie festlegen, folgen Sie dem Abschnitt Vor dem 29. April 2024.

Vor dem 29. April 2024

Citrix Cloud verwendet drei separate Dienstkonten im Google Cloud-Projekt:

- *Citrix Cloud-Dienstkonto:* Dieses Dienstkonto ermöglicht Citrix Cloud den Zugriff auf das Google-Projekt, sowie Provisioning und Verwaltung von Maschinen. Dieses Dienstkonto authentifiziert sich bei Google Cloud mit einem von Google Cloud generierten Schlüssels.

  Sie müssen dieses Dienstkonto manuell erstellen, wie hier beschrieben. Weitere Informationen finden Sie unter Citrix Cloud-Dienstkonto erstellen.

  Sie können dieses Dienstkonto mit einer E-Mail-Adresse identifizieren. Beispiel: `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cloud Build-Dienstkonto:* Dieses Dienstkonto wird automatisch bereitgestellt, nachdem Sie alle unter Enable Google Cloud APIs aufgeführten APIs aktiviert haben. Um alle automatisch erstellten Dienstkonten anzuzeigen, navigieren Sie in der **Google Cloud**-Konsole zu **IAM & Admin > IAM** und aktivieren Sie das Kontrollkästchen **Include Google-provided role grants**.

  Sie können dieses Dienstkonto durch eine E-Mail-Adresse identifizieren, die mit der **Projekt-ID** und dem Wort **cloudbuild** beginnt. Zum Beispiel: `<project-id>@cloudbuild.gserviceaccount.com`

  Überprüfen Sie, ob dem Dienstkonto die folgenden Rollen gewährt wurden. Wenn Sie Rollen hinzufügen müssen, folgen Sie den Schritten unter Cloud Build-Dienstkonto Rollen hinzufügen.

  - Cloud Build-Dienstkonto
  - Compute Instance-Administrator
  - Dienstkontobenutzer

- *Cloud Compute-Dienstkonto*: Dieses Dienstkonto wird von Google Cloud zu Instanzen hinzugefügt, die in Google Cloud erstellt wurden, sobald die Compute-API aktiviert wird. Dieses Konto hat die einfache IAM-Bearbeiterrolle, um die Operationen auszuführen. Wenn Sie jedoch die Standardberechtigung löschen, um eine präzisere Kontrolle zu haben, müssen Sie die **Speicheradministratorrolle** hinzufügen, für die die folgenden Berechtigungen erforderlich sind:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Sie können dieses Dienstkonto durch eine E-Mail-Adresse identifizieren, die mit der **Projekt-ID** und dem Wort **compute** beginnt. Beispiel: `<project-id>-compute@developer.gserviceaccount.com`.

Citrix Cloud-Dienstkonto erstellen Führen Sie folgende Schritte aus, um ein Citrix Cloud-Dienstkonto zu erstellen:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > Service accounts**.
2. Wählen Sie auf der Seite **Service accounts CREATE SERVICE ACCOUNT**.
3. Geben Sie auf der Seite **Create service account** die erforderlichen Informationen ein und wählen Sie dann **CREATE AND CONTINUE**.
4. Klicken Sie auf der Seite **Grant this service account access to project** auf das Dropdownmenü **Select a role** und wählen Sie die erforderlichen Rollen aus. Klicken Sie auf **+ADD ANOTHER ROLE**, wenn Sie weitere Rollen hinzufügen möchten.

   Jedes Konto (persönlich oder Service) hat verschiedene Rollen, die das Management des Projekts definieren. Gewähren Sie diesem Dienstkonto die folgenden Rollen:

   - Compute Admin
   - Speicher-Administrator
   - Cloud Build-Editor
   - Dienstkontobenutzer
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   Der Cloud KMS Crypto Operator benötigt die folgenden Berechtigungen:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > **Hinweis:**
   >
   > Aktivieren Sie alle APIs, um die vollständige Liste der beim Erstellen eines neuen Dienstkontos verfügbaren Rollen abzurufen.

5. Klicken Sie auf **CONTINUE**
6. Fügen Sie auf der Seite **Grant users access to this service account** Benutzer oder Gruppen hinzu, um ihnen Zugriff auf Aktionen in diesem Dienstkonto zu gewähren.
7. Klicken Sie auf **DONE**.
8. Navigieren Sie zur IAM-Hauptkonsole.
9. Identifizieren Sie das erstellte Dienstkonto.
10. Überprüfen Sie, ob die Rollen erfolgreich zugewiesen wurden.

Überlegungen:

Beachten Sie beim Erstellen des Servicekontos Folgendes:

- Die Schritte **Grant this service account access to project** und **Grant users access to this service account** sind optional. Wenn Sie diese optionalen Konfigurationsschritte überspringen, wird das neu erstellte Servicekonto nicht auf der Seite **IAM & Admin > IAM** angezeigt.
- Um die mit dem Servicekonto verknüpften Rollen anzuzeigen, fügen Sie die Rollen hinzu, ohne die optionalen Schritte zu überspringen. Dadurch wird sichergestellt, dass Rollen für das konfigurierte Servicekonto angezeigt werden.

Citrix Cloud-Dienstkontoschlüssel Der Citrix Cloud-Dienstkontoschlüssel ist erforderlich, um eine Verbindung in Citrix DaaS herzustellen. Der Schlüssel ist in einer Anmeldeinformationsdatei (.json) enthalten. Nachdem Sie den Schlüssel erstellt haben, wird die Datei automatisch heruntergeladen und im Ordner **Downloads** gespeichert. Stellen Sie beim Erstellen des Schlüssels sicher, dass der Schlüsseltyp auf JSON festgelegt wird. Andernfalls kann die Citrix Oberfläche "Vollständige Konfiguration" sie nicht analysieren.

Um einen Dienstkontoschlüssel zu erstellen, navigieren Sie zu **IAM & Admin > Dienstkonten** und klicken Sie auf die E-Mail-Adresse des Citrix Cloud-Dienstkontos. Wechseln Sie zur Registerkarte **Schlüssel** und wählen Sie **Schlüssel hinzufügen > Neuen Schlüssel erstellen**. Achten Sie darauf, **JSON** als Schlüsseltyp auszuwählen.

> **Tipp:**
>
> Erstellen Sie Schlüssel auf der Seite **Service accounts** in der Google Cloud-Konsole. Es wird empfohlen, Schlüssel aus Sicherheitsgründen regelmäßig zu ändern. Sie stellen der Citrix Virtual Apps and Desktops-Anwendung neue Schlüssel durch Bearbeiten einer vorhandenen Google Cloud-Verbindung bereit.

Citrix Cloud-Dienstkonto Rollen hinzufügen So fügen Sie einem Citrix Cloud-Dienstkonto Rollen hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM > PERMISSIONS** das erstellte Dienstkonto, erkennbar an der E-Mail-Adresse.

   Zum Beispiel: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um den Zugriff auf den Prinzipal des Dienstkontos zu bearbeiten.

4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

Cloud Build-Dienstkonto Rollen hinzufügen So fügen Sie einem Cloud Build-Dienstkonto Rollen hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM** das Cloud Build-Dienstkonto, erkennbar an einer E-Mail-Adresse, die mit der **Projekt-ID** und dem Wort **cloudbuild** beginnt.

   Zum Beispiel: `<project-id>@cloudbuild.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um die Cloud Build-Kontorollen zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Cloud Build-Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

   > **Hinweis:**
   >
   > Aktivieren Sie alle APIs, um die vollständige Liste der Rollen abzurufen.

Nach dem 29. April 2024

Citrix Cloud verwendet zwei separate Dienstkonten im Google Cloud-Projekt:

- *Citrix Cloud-Dienstkonto:* Dieses Dienstkonto ermöglicht Citrix Cloud den Zugriff auf das Google-Projekt, sowie Provisioning und Verwaltung von Maschinen. Dieses Dienstkonto authentifiziert sich bei Google Cloud mit einem von Google Cloud generierten Schlüssels.

  Sie müssen dieses Dienstkonto manuell erstellen.

  Sie können dieses Dienstkonto mit einer E-Mail-Adresse identifizieren. Beispiel: `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Cloud Compute-Dienstkonto*: Dieses Dienstkonto wird automatisch bereitgestellt, nachdem Sie alle unter Enable Google Cloud APIs aufgeführten APIs aktiviert haben. Um alle automatisch erstellten Dienstkonten anzuzeigen, navigieren Sie in der **Google Cloud**-Konsole zu **IAM & Admin > IAM** und aktivieren Sie das Kontrollkästchen **Include Google-provided role grants**. Dieses Konto hat die einfache IAM-Bearbeiterrolle, um die Operationen auszuführen. Wenn Sie jedoch die Standardberechtigung löschen, um eine präzisere Kontrolle zu haben, müssen Sie die **Speicheradministratorrolle** hinzufügen, für die die folgenden Berechtigungen erforderlich sind:

  - resourcemanager.projects.get

- storage.objects.create
- storage.objects.get
- storage.objects.list

Sie können dieses Dienstkonto durch eine E-Mail-Adresse identifizieren, die mit der **Projekt-ID** und dem Wort **compute** beginnt. Zum Beispiel: `<project-id>-compute@developer.gserviceaccount.com`.

Überprüfen Sie, ob dem Dienstkonto die folgenden Rollen gewährt wurden.

- Cloud Build-Dienstkonto
- Compute Instance-Administrator
- Dienstkontobenutzer

Citrix Cloud-Dienstkonto erstellen Führen Sie folgende Schritte aus, um ein Citrix Cloud-Dienstkonto zu erstellen:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > Service accounts**.
2. Wählen Sie auf der Seite **Service accounts CREATE SERVICE ACCOUNT**.
3. Geben Sie auf der Seite **Create service account** die erforderlichen Informationen ein und wählen Sie dann **CREATE AND CONTINUE**.
4. Klicken Sie auf der Seite **Grant this service account access to project** auf das Dropdownmenü **Select a role** und wählen Sie die erforderlichen Rollen aus. Klicken Sie auf **+ADD ANOTHER ROLE**, wenn Sie weitere Rollen hinzufügen möchten.

   Jedes Konto (persönlich oder Service) hat verschiedene Rollen, die das Management des Projekts definieren. Gewähren Sie diesem Dienstkonto die folgenden Rollen:

   - Compute Admin
   - Speicher-Administrator
   - Cloud Build-Editor
   - Dienstkontobenutzer
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   Der Cloud KMS Crypto Operator benötigt die folgenden Berechtigungen:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **Hinweis:**
>
> Aktivieren Sie alle APIs, um die vollständige Liste der beim Erstellen eines neuen Dienstkontos verfügbaren Rollen abzurufen.

5. Klicken Sie auf **CONTINUE**
6. Fügen Sie auf der Seite **Grant users access to this service account** Benutzer oder Gruppen hinzu, um ihnen Zugriff auf Aktionen in diesem Dienstkonto zu gewähren.
7. Klicken Sie auf **DONE**.
8. Navigieren Sie zur IAM-Hauptkonsole.
9. Identifizieren Sie das erstellte Dienstkonto.
10. Überprüfen Sie, ob die Rollen erfolgreich zugewiesen wurden.

Überlegungen:

Beachten Sie beim Erstellen des Servicekontos Folgendes:

- Die Schritte **Grant this service account access to project** und **Grant users access to this service account** sind optional. Wenn Sie diese optionalen Konfigurationsschritte überspringen, wird das neu erstellte Servicekonto nicht auf der Seite **IAM & Admin > IAM** angezeigt.
- Um die mit dem Servicekonto verknüpften Rollen anzuzeigen, fügen Sie die Rollen hinzu, ohne die optionalen Schritte zu überspringen. Dadurch wird sichergestellt, dass Rollen für das konfigurierte Servicekonto angezeigt werden.

Citrix Cloud-Dienstkontoschlüssel Der Citrix Cloud-Dienstkontoschlüssel ist erforderlich, um eine Verbindung in Citrix DaaS herzustellen. Der Schlüssel ist in einer Anmeldeinformationsdatei (.json) enthalten. Nachdem Sie den Schlüssel erstellt haben, wird die Datei automatisch heruntergeladen und im Ordner **Downloads** gespeichert. Stellen Sie beim Erstellen des Schlüssels sicher, dass der Schlüsseltyp auf JSON festgelegt wird. Andernfalls kann die Citrix Oberfläche "Vollständige Konfiguration" sie nicht analysieren.

Um einen Dienstkontoschlüssel zu erstellen, navigieren Sie zu **IAM & Admin > Dienstkonten** und klicken Sie auf die E-Mail-Adresse des Citrix Cloud-Dienstkontos. Wechseln Sie zur Registerkarte **Schlüssel** und wählen Sie **Schlüssel hinzufügen > Neuen Schlüssel erstellen**. Achten Sie darauf, **JSON** als Schlüsseltyp auszuwählen.

> **Tipp:**
>
> Erstellen Sie Schlüssel auf der Seite **Service accounts** in der Google Cloud-Konsole. Es wird empfohlen, Schlüssel aus Sicherheitsgründen regelmäßig zu ändern. Sie stellen der Citrix Virtual Apps and Desktops-Anwendung neue Schlüssel durch Bearbeiten einer vorhandenen

> Google Cloud-Verbindung bereit.

Citrix Cloud-Dienstkonto Rollen hinzufügen So fügen Sie einem Citrix Cloud-Dienstkonto Rollen hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM > PERMISSIONS** das erstellte Dienstkonto, erkennbar an der E-Mail-Adresse.

   Zum Beispiel: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um den Zugriff auf den Prinzipal des Dienstkontos zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

Rollen zum Cloud Compute-Dienstkonto hinzufügen So fügen Sie Rollen zum Cloud Compute-Dienstkonto hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM** das Cloud Build-Dienstkonto, erkennbar an einer E-Mail-Adresse, die mit der **Projekt-ID** und dem Wort **compute** beginnt.

   Zum Beispiel: `<project-id>-compute@developer.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um die Cloud Build-Kontorollen zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Cloud Build-Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

   > **Hinweis:**
   >
   > Aktivieren Sie alle APIs, um die vollständige Liste der Rollen abzurufen.

Speicherberechtigungen und Bucket-Verwaltung

Citrix DaaS verbessert die Fehlermeldung im Cloud-Build für den Google Cloud-Dienst. Der Dienst führt Builds in Google Cloud aus. Citrix DaaS erstellt ein Storage-Bucket mit dem Namen `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }`, in dem die Google Cloud-Dienste Protokollinformationen für den Build erfassen. Für das Bucket ist festgelegt, dass

dessen Inhalt nach 30 Tagen gelöscht wird. Für diesen Vorgang muss die Google Cloud-Berechtigung des für die Verbindung verwendeten Dienstkontos auf `storage.buckets.update` festgelegt sein. Hat das Dienstkonto diese Berechtigung nicht, ignoriert Citrix DaaS Fehler und setzt die Katalogerstellung fort. Ohne diese Berechtigung werden Build-Protokolle immer größer und erfordern eine manuelle Bereinigung.

Aktivieren des privaten Google-Zugriffs

Wenn der Netzwerkschnittstelle einer VM keine externe IP-Adresse zugewiesen ist, werden Pakete nur an andere interne IP-Adressenziele gesendet. Wenn Sie den privaten Zugriff aktivieren, stellt die VM eine Verbindung zu den von der Google-API und den zugehörigen Diensten verwendeten externen IP-Adressen her.

> **Hinweis:**
>
> Unabhängig davon, ob der private Google-Zugriff aktiviert ist, müssen alle VMs mit und ohne öffentliche IP-Adresse auf öffentliche Google-APIs zugreifen können, vor allem dann, wenn Netzwerkgeräte von Drittanbietern in der Umgebung installiert sind.

Damit eine VM im Subnetz ohne öffentliche IP-Adresse für das MCS-Provisioning auf die Google-APIs zugreifen kann, führen Sie folgende Schritte aus:

1. Rufen Sie in Google Cloud **VPC network configuration** auf.
2. Identifizieren Sie die verwendeten Subnetze oder die Citrix-Umgebung auf der Registerkarte **Subnetze im aktuellen Projekt**.
3. Klicken Sie auf den Namen der Subnetze und aktivieren Sie den **privaten Google-Zugriff**.

Weitere Informationen finden Sie unter Konfigurieren des privaten Google-Zugriffs.

> **Wichtig:**
>
> Wenn Ihr Netzwerk so konfiguriert ist, dass der VM-Zugriff auf das Internet unterbunden wird, stellen Sie sicher, dass Ihre Organisation das mit der Aktivierung des privaten Google-Zugriffs für das Subnetz der VMs verbundene Risiko einzugehen bereit ist.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu Google-Cloudumgebungen.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

HPE Moonshot-Virtualisierungsumgebungen

June 12, 2024

Citrix DaaS verwaltet Ihre HPE Moonshot-Workloads über ein von Citrix verwaltetes HPE Moonshot-Plug-In, das in der DaaS-Steuerungsebene vorhanden ist. Mit diesem Plug-In können Sie Verbindungen zu Ihrem HPE Moonshot Chassis herstellen, Kataloge erstellen und die Energieverwaltung von Maschinen im Katalog steuern.

Wichtige Schritte

1. Richten Sie Ihre HPE-Umgebungen ein.
2. Stellen Sie eine Verbindung zum HPE Moonshot Chassis her.

   > **Hinweis:**
   >
   > Nachdem Sie das Feature aktiviert haben, wird das von Citrix verwaltete HPE Moonshot-Plug-In automatisch installiert. Sie können daher den vorhandenen Maschinenkatalog mit dem von Citrix verwalteten Moonshot-Plug-In anstelle des von HPE verwalteten Plug-Ins weiter verwenden.

3. Erstellen Sie einen Maschinenkatalog.

   > **Hinweis:**
   >
   > Stellen Sie vor dem Erstellen eines Katalogs sicher, dass Sie über einen oder mehrere HPE Moonshot Cartridge-Knoten verfügen, und installieren Sie VDAs auf diesen Knoten. Sie können das HPE Moonshot Chassis als Hypervisor und die Cartridge-Knoten als VMs betrachten.

4. Erstellen Sie eine Bereitstellungsgruppe.
5. Migrieren Sie die übrigen nicht verwalteten HPE Moonshot-Knoten in den verwalteten Katalog oder die Bereitstellungsgruppe.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu HPE Moonshot.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Microsoft Azure Resource Manager-Virtualisierungsumgebungen

May 17, 2024

Wenn Sie mit Microsoft Azure Resource Manager virtuelle Maschinen in Ihrer Citrix DaaS-Umgebung bereitstellen, sollten Sie mit Folgendem vertraut sein:

- Was ist Microsoft Entra ID?
- Leitfaden für die ersten Schritte zur Integration von Microsoft Entra ID in Anwendungen
- Anwendungs- und Dienstprinzipalobjekte in Microsoft Entra ID

Informationen zum Einrichten Ihres Microsoft Azure Resource Manager finden Sie unter Ressourcenstandort einrichten.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu Microsoft Azure.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten

- Maschinenkataloge erstellen
- CTX219211: Ein Microsoft Entra ID-Konto einrichten
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen

February 21, 2024

Folgen Sie den nachfolgenden Anweisungen, wenn Sie Hyper-V mit Microsoft System Center Virtual Machine Manager (VMM) zur Bereitstellung von virtuellen Maschinen verwenden.

UnterSystemanforderungen sind die unterstützten VMM-Versionen aufgeführt.

Verwenden Sie Maschinenerstellungsdienste (MCS) oder Citrix Provisioning (früher "Provisioning Services") zum Bereitstellen folgender Elemente:

- Desktop- oder Serverbetriebssystem-VM der ersten Generation
- VMs der zweiten Generation mit Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10 und Windows 11 (mit oder ohne sicheren Start)

Installieren und Konfigurieren eines Hypervisors

Installieren Sie die Microsoft Hyper-V-Rolle und VMM auf Ihren Servern.

Überprüfen Sie die folgenden Kontoinformationen:

Das Konto, das Sie beim Erstellen einer Verbindung in **Verwalten > Vollständige Konfiguration** verwenden, muss ein VMM-Administrator oder ein delegierter VMM-Administrator für die relevanten Hyper-V-Maschinen sein. Wenn dieses Konto nur über die delegierte Administratorrolle in VMM verfügt, werden die Speicherdaten in der Schnittstelle **Vollständige Konfiguration** beim Erstellen der Verbindung nicht aufgeführt.

Das Benutzerkonto muss außerdem Mitglied der lokalen Administratorsicherheitsgruppe auf jedem Hyper-V-Server sein, um zur Lebenszyklusverwaltung von VM (z. B. VM erstellen, aktualisieren und löschen) berechtigt zu sein.

In großen Bereitstellungen, in denen ein SCVMM mehrere Cluster in verschiedenen Datencentern verwaltet, können Sie den Hostgruppenbereich für die Administratoren beschränken.

Verwenden Sie zum Beschränken des Hostgruppenbereichs die Rolle "Delegierter Administrator"in der Konsole des Microsoft System Center Virtual Machine Manager (SCVMM).

1. Wählen Sie im **Assistenten zum Erstellen von Benutzerrollen** die Benutzerrolle **Fabric-Administrator (delegierter Administrator)**.
2. Fügen Sie unter **Mitglieder** das Benutzerkonto im Active Directory hinzu, das Sie als delegierten Administrator verwenden möchten.
3. Wählen Sie in **Geltungsbereich** die Hostgruppen aus, auf die der delegierte Administrator Zugriff erhalten soll.
4. Erstellen Sie ein neues **Ausführendes Konto** mit den Benutzeranmeldeinformationen des delegierten Administrators. Verwenden Sie diese Anmeldeinformationen, um später eine Hypervisor-Verbindung herzustellen. Verwenden Sie nicht die Konten der Rolle "Hauptadministrator".

VMM-Konsole installieren

Installieren Sie auf jedem Server mit Citrix Cloud Connector eine System Center Virtual Machine Manager-Konsole.

Die Konsolenversion muss mit der Version des Verwaltungsservers übereinstimmen. Obwohl eine frühere Konsole eine Verbindung zum Verwaltungsserver herstellen kann, schlägt die Bereitstellung von VDAs fehl, wenn die Versionen sich unterscheiden.

Azure Stack HCI-Provisioning über SCVMM

Azure Stack HCI ist eine Clusterlösung mit hyperkonvergenter Infrastruktur (HCI), die virtualisierte Windows- und Linux-Workloads und deren Speicher in einer hybriden On-Premises-Umgebung hostet.

Azure-Hybriddienste erweitern den Cluster durch Funktionen wie Cloud-basierte Überwachung, Site-Wiederherstellung und VM-Backups. Sie können auch eine zentrale Ansicht aller Azure Stack HCI-Bereitstellungen im Azure-Portal einrichten.

Integration von Azure Stack HCI mit SCVMM

Um Azure Stack HCI mit SCVMM zu integrieren, müssen Sie zuerst einen Azure Stack HCI-Cluster erstellen und diesen Cluster dann mit SCVMM integrieren.

1. Informationen zum Erstellen des Azure Stack HCI-Clusters und seiner Registrierung bei Azure finden Sie im Microsoft-Dokument Herstellen einer Verbindung von Azure Stack HCI mit Azure.
2. Schrittfolge zum Integrieren von Azure Stack HCI-Cluster mit SCVMM:

    a) Melden Sie sich bei der Maschine an, die für das Hosten des SCVMM-Servers vorbereitet wurde, und installieren Sie SCVMM 2019 UR3 oder höher.

> **Hinweis:**
>
> Installieren Sie die Administratorkonsole für SCVMM 2019 UR3 oder höher in den Cloud Connector-VMs.

b) Erstellen Sie auf der Seite **Einstellungen** der VMM-Konsole ein ausführendes Konto.

c) Führen Sie die folgenden PowerShell-Befehle mit Administratorrechten auf dem SCVMM-Server aus, um den Azure Stack HCI-Cluster als Host hinzuzufügen:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
   VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
   $true
<!--NeedCopy-->
```

d) Sie können jetzt den Azure Stack HCI-Cluster samt Knoten in der VMM-Konsole sehen.

e) Erstellen Sie die SCVMM-Hostverbindung in der Oberfläche **Vollständige Konfiguration**.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu Microsoft System Center Virtual Machine Manager.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Nutanix-Virtualisierungsumgebungen

February 14, 2024

Folgen Sie diesen Anleitungen, wenn Sie mit Nutanix Acropolis virtuelle Maschinen in Ihrer Citrix DaaS-Bereitstellung bereitstellen. Der Einrichtungsvorgang umfasst die Installation und Registrierung des Nutanix-Plug-ins in Ihrer Citrix DaaS-Umgebung.

Weitere Informationen finden Sie in der Installationsdokumentation zum Nutanix Acropolis MCS-Plug-In im Nutanix Support Portal.

> **Wichtig:**
>
> Installieren Sie das Nutanix-Plug-In auf allen Cloud Connectors, bei denen Citrix DaaS eine Hostverbindung zu dem Ressourcenstandort herstellen muss, der über einen Nutanix-Hypervisor verfügt.

Installieren und Registrieren des Nutanix-Plug-Ins

Führen Sie die Vorgang aus, um das Nutanix-Plug-In bei allen Cloud Connectors zu installieren und zu registrieren. Erstellen Sie mit den Funktionen unter **Verwalten** in Citrix Cloud eine Verbindung zu Nutanix.

Informationen zur Installation des Nutanix-Plug-Ins finden Sie in der Nutanix-Dokumentation.

Weitere Informationen zum Einrichten Ihrer Nutanix-Virtualisierungsumgebungen finden Sie unter Ressourcentyp hinzufügen oder eine ungenutzte Domäne in Citrix Cloud aktivieren.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu Nutanix.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Nutanix-Cloud und Partnerlösungen

January 25, 2024

Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unterstützt die folgende Nutanix-Cloud und Partnerlösung:

- Nutanix Cloud Clusters in AWS

Nutanix Cloud Clusters in AWS

Citrix DaaS unterstützt Nutanix Cloud Clusters auf AWS. Nutanix-Cluster vereinfachen das Ausführen von Anwendungen in privaten oder mehreren öffentlichen Clouds. Weitere Informationen zu Nutanix Cloud Clusters auf AWS finden Sie unter Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Tipp:**
>
> Diese Unterstützung bietet dieselbe Funktionalität wie ein on-premises bereitgestellter Nutanix-Cluster. Es wird nur ein einziger Cluster unterstützt: *Prism Element*. Weitere Informationen finden Sie hier.

Anforderungen

Sie benötigen folgende Konten, um Nutanix-Cluster auf AWS zu verwenden:

- Ein Nutanix-Konto
- Ein AWS-Konto mit den folgenden Berechtigungen:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Erstellen eines Nutanix-Clusters

Schrittfolge zum Erstellen eines Nutanix-Clusters:

1. Melden Sie sich bei Ihrem Nutanix-Konto an.
2. Suchen Sie die Option **Nutanix cluster** und klicken Sie auf **Launch**. Die **Nutanix-Konsole** wird geöffnet. Weitere Informationen finden Sie unter Get Started with Nutanix Cluster on AWS.
3. Erstellen Sie eine **neue virtuelle private Cloud (VPC)**.

Das Erstellen des Clusters schlägt möglicherweise fehl, wobei folgende Fehlermeldungen angezeigt werden:

- Cluster konnte nicht innerhalb der vorgegebenen Zeit erstellt werden. Der Cluster wird gelöscht.

- Host-Nutanix-Cluster –Knoten `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Host-Nutanix-Cluster –Knoten `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

Wenn der Cluster nicht erstellt werden konnte:

- Versuchen Sie, den Cluster in einer anderen Region neu zu erstellen.
- Löschen Sie den Nutanix-CloudFormation-Stack (CFS), bevor Sie den Versuch wiederholen.

Zusätzlich zu anderen Ressourcen erstellt der Nutanix-CFS Folgendes:

- 1 virtuelle private Cloud mit dem Namen *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 Subnetze: 10.0.128.0/24 und 10.0.129.0/24
- 1 Internetgateway
- 1 NAT-Gateway

Rufen Sie nach dem Erstellen des Clusters die Adresse von **Nutanix Prism** ab:

1. Wechseln Sie zur **Nutanix-Konsole**.
2. Zeigen Sie mit der Maus auf den Link **Launch Prism Element** rechts oben auf der Konsole und kopieren Sie die URL.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu Nutanix-Cloud und Partnerlösungen.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

VMware-Virtualisierungsumgebungen

January 25, 2024

Folgen Sie diesen Anweisungen, wenn Sie zur Bereitstellung von virtuellen Maschinen VMware verwenden.

Installieren Sie vCenter Server und die Verwaltungstools. (Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.)

> **Hinweis:**
>
> Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.

Wenn Sie Maschinenerstellungdienste (MCS) verwenden möchten, deaktivieren Sie nicht das Datastore Browser-Feature in vCenter Server, wie unter vCenter Server Datastore Browser deaktiveren beschrieben. Wenn Sie das Feature deaktivieren, funktioniert MCS nicht richtig.

Weitere Informationen zum Einrichten Ihrer VMware-Virtualisierungsumgebungen finden Sie unter Ressourcentyp hinzufügen oder eine ungenutzte Domäne in Citrix Cloud aktivieren.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu VMware.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

VMware-Cloud und Partnerlösungen

January 25, 2024

Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unterstützt die folgende VMware Cloud samt Partnerlösungen:

- Azure VMware-Lösung (AVS)
- Google Cloud VMware Engine
- VMware-Cloud auf Amazon Web Services (AWS)

Verwenden Sie Citrix DaaS für die Migration von VMware-basierten, on-premises bereitgestellten Citrix Workloads zu den jeweiligen VMware-Partnerlösungen.

Integration von Azure VMware Solution (AVS)

Citrix DaaS unterstützt AVS. AVS bietet Cloudinfrastruktur mit vSphere-Clustern, die von der Azure-Infrastruktur erstellt wurden. Nutzen Sie Citrix DaaS, um AVS für das Provisioning der VDA-Workload auf die gleiche Weise zu verwenden, in der Sie vSphere in On-Premises-Umgebungen verwenden würden.

AVS-Cluster einrichten

Führen Sie die folgenden Schritte in Azure aus, damit Citrix DaaS AVS verwenden kann:

- Hostkontingent anfordern
- `Microsoft.AVS`-Ressourcenanbieter registrieren
- Checkliste für die Netzwerkplanung überprüfen
- Netzwerk-Checkliste
- AVS Private Cloud erstellen
- Auf die AVS Private Cloud zugreifen
- Konfigurieren des Netzwerks für Ihre private VMware-Cloud in Azure
- DHCP für AVS konfigurieren
- Ein Netzwerksegment in AVS hinzufügen
- AVS-Umgebung überprüfen

Hostkontingent für Kunden von Azure Enterprise Agreement anfordern Wählen Sie auf der Seite **Hilfe + Support** des Azure-Portals **Neue Supportanfrage** aus und fügen Sie die folgenden Informationen hinzu:

- Problemtyp: Technisch
- Abonnement: Wählen Sie Ihr Abonnement
- Dienst:**Alle Dienste > Azure VMware Solution**
- Ressource: Allgemeine Frage
- Zusammenfassung: Kapazität erforderlich
- Problemtyp: Kapazitätsverwaltungsprobleme
- Problemuntertyp: Kundenanfrage für zusätzliches Hostkontingent/zusätzliche Hostkapazität

Geben Sie in der **Beschreibung** des Supporttickets auf der Registerkarte **Details** die folgenden Informationen an:

- Proof of Concept oder Produktion

- Name der Region
- Anzahl von Hosts
- Weitere Details

> **Hinweis:**
>
> AVS erfordert mindestens drei Hosts und empfiehlt eine Redundanz von N+1 Hosts.

Wenn Sie die Details für das Supportticket angegeben haben, wählen Sie **Überprüfen und erstellen** aus, um die Anforderung an Azure zu senden.

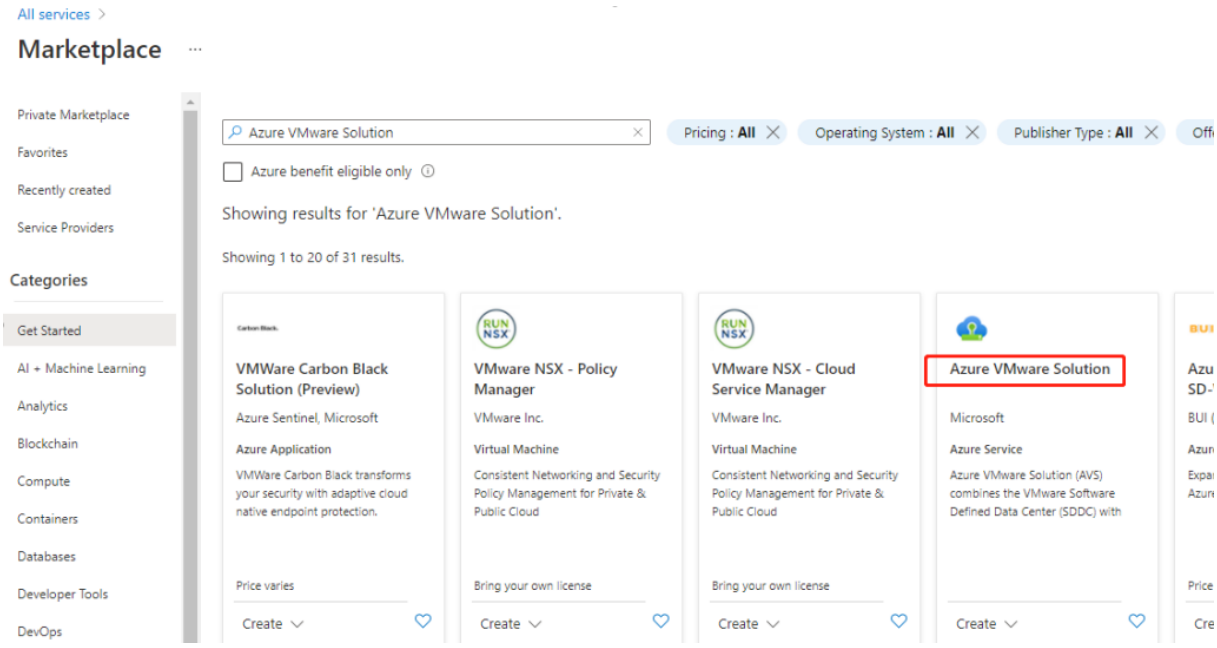
Registrieren des Microsoft.AVS-Ressourcenanbieters Nach Anforderung des Hostkontingents müssen Sie den Ressourcenanbieter registrieren:

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie im Menü des Azure-Portals **Alle Dienste** aus.
3. Geben Sie im Menü **Alle Dienste** das Abonnement ein und wählen Sie **Abonnements** aus.
4. Wählen Sie das Abonnement aus der Abonnementliste aus.
5. Wählen Sie **Ressourcenanbieter** aus und geben Sie **Microsoft.AVS** als Suchbegriff in die Suchleiste ein.
6. Wählen Sie **Registrieren** aus, falls der Ressourcenanbieter nicht registriert ist.

Überlegungen zum Netzwerk AVS bietet Netzwerkdienste an, die bestimmte Netzwerkadressbereiche und Firewallports erfordern. Weitere Informationen finden Sie unter Checkliste für die Netzwerkplanung für Azure VMware Solution.

AVS Private Cloud erstellen Erstellen Sie nach Prüfung der Netzwerkanforderungen für Ihre Umgebung eine private ASV-Cloud:

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie **Neue Ressource erstellen** aus.
3. Geben Sie im Textfeld **Marketplace durchsuchen** den Text *Azure VMware Solution* ein und wählen Sie **Azure VMware Solution** in der Liste aus.



Im Fenster **Azure VMware Solution**:

1. Wählen Sie **Create**.
2. Gehen Sie zur Registerkarte **Basics**.
3. Geben Sie Werte für die Felder ein. Verwenden Sie dazu die Informationen in der folgenden Tabelle:

Feld	Wert
Abonnement	Wählen Sie das Abonnement aus, das Sie für die Bereitstellung verwenden möchten. Alle Ressourcen in einem Azure-Abonnement werden gemeinsam abgerechnet.
Ressourcengruppe	Wählen Sie die Ressourcengruppe für Ihre private Cloud aus. Eine Azure-Ressourcengruppe ist ein logischer Container, in dem Azure-Ressourcen bereitgestellt und verwaltet werden. Alternativ können Sie eine neue Ressourcengruppe für Ihre private Cloud erstellen.
Ort	Wählen Sie einen Standort aus (beispielsweise USA, Osten). Dies ist die Region, die Sie während der Planungsphase definiert haben.
Ressourcenname	Geben Sie den Namen Ihrer privaten Azure VMware Solution-Cloud an.

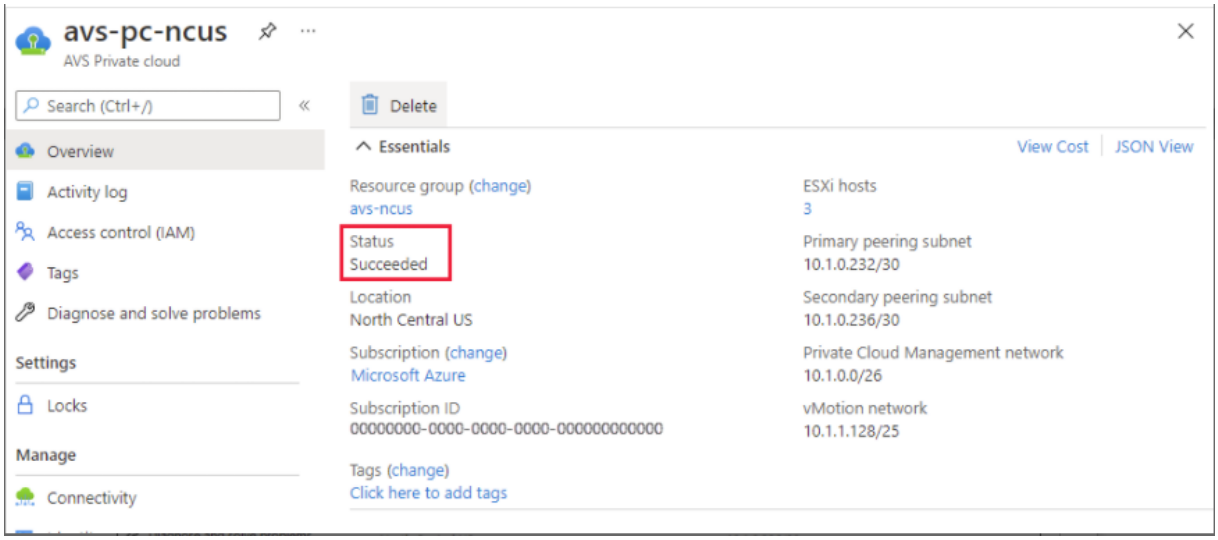
Feld	Wert
Größe des Hosts	Wählen Sie die Größe nach Ihren Bedürfnissen.
Anzahl von Hosts	Zeigt die Anzahl der Hosts an, die dem privaten Cloudcluster zugeordnet sind. Der Standardwert ist 3. Sie können den Wert nach der Bereitstellung erhöhen oder verringern.
Adressblock für Private Cloud	Geben Sie einen IP-Adressblock für die private Cloud an. CIDR stellt das Verwaltungsnetzwerk der privaten Cloud dar und wird für die Clusterverwaltungsdienste wie vCenter Server und NSX-T Manager verwendet. Geben Sie einen /22-Adressraum an, beispielsweise 10.175.0.0/22. Die Adresse muss eindeutig sein und darf sich nicht mit anderen Azure Virtual Networks und On-Premises-Netzwerken überschneiden.

Auf dem Bildschirm **Erstellen einer privaten Cloud**:

1. Wählen Sie im Feld **Standort** die Region aus, in der sich das AVS befindet. Die Ressourcengruppenregion ist dieselbe wie die AVS-Region.
2. Wählen Sie im Feld **Größe des Hosts** eine Größe aus, die Ihren Anforderungen entspricht.
3. Geben Sie im Feld **Adressblock für Private Cloud** eine IP-Adresse an. Beispiel: 10.15.0.0/22.
4. Wählen Sie **Überprüfen und erstellen** aus.
5. Klicken Sie nach dem Überprüfen der Informationen auf **Erstellen**.

> **Tipp:**
>
> Das Erstellen einer privaten Cloud kann 3 bis 4 Stunden dauern. Das Hinzufügen eines einzelnen Hosts zum Cluster kann 30 bis 45 Minuten dauern.

Vergewissern Sie sich, dass die Bereitstellung erfolgreich war. Navigieren Sie zu der von Ihnen erstellten Ressourcengruppe und wählen Sie Ihre private Cloud aus. Wenn der **Status Erfolgreich** angezeigt wird, ist die Bereitstellung abgeschlossen.



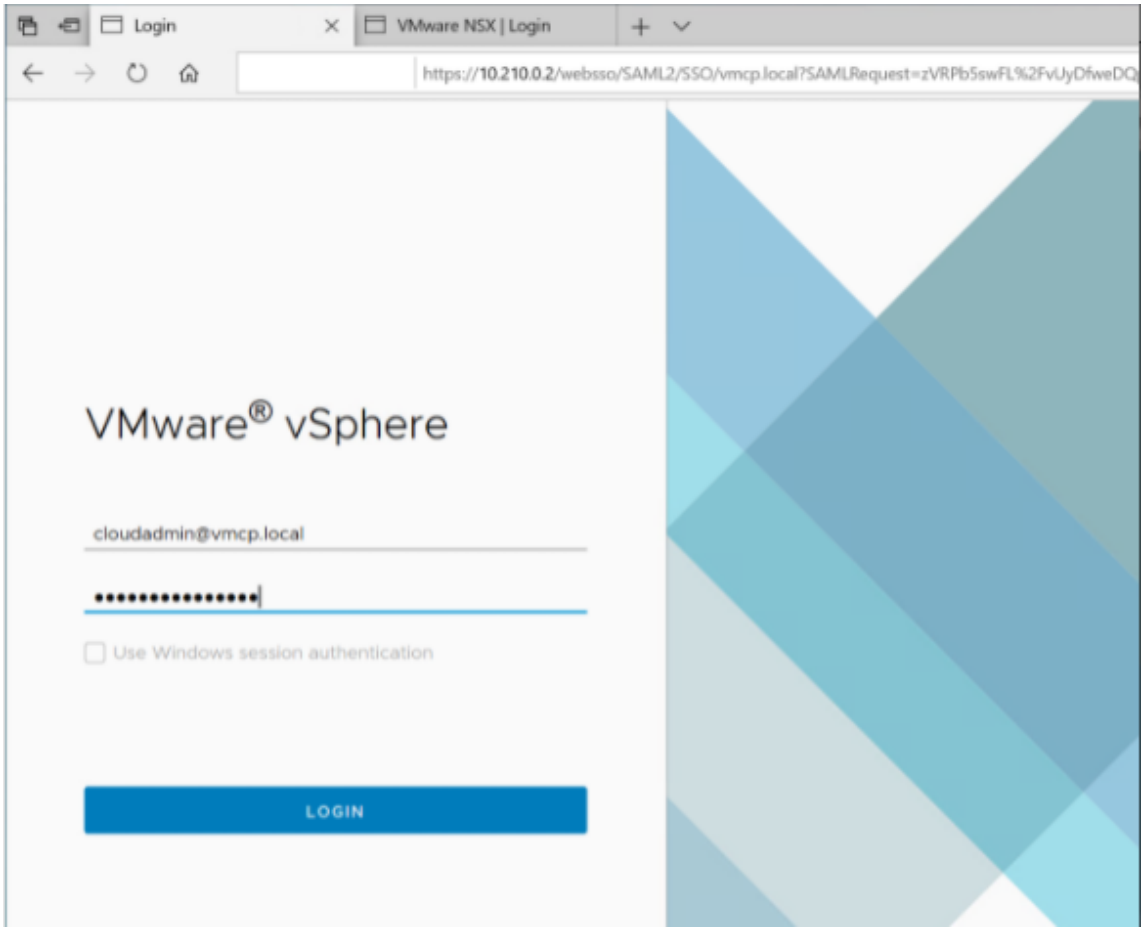
Auf die AVS Private Cloud zugreifen Erstellen Sie nach dem Erstellen einer privaten Cloud eine Windows-VM und stellen Sie eine Verbindung zum lokalen vCenter Ihrer privaten Cloud her.

Erstellen einer neuen virtuellen Windows-Maschine

1. Wählen Sie in der Ressourcengruppe **+ Hinzufügen** aus, suchen Sie nach **Microsoft Windows 10/11 oder Windows Server 2016/2019** und wählen Sie es aus.
2. Geben Sie die erforderlichen Informationen ein und wählen Sie dann **Überprüfen + erstellen** aus.
3. Wählen Sie nach erfolgreicher Validierung **Erstellen** aus, um den Erstellungsprozess der virtuellen Maschine zu starten.

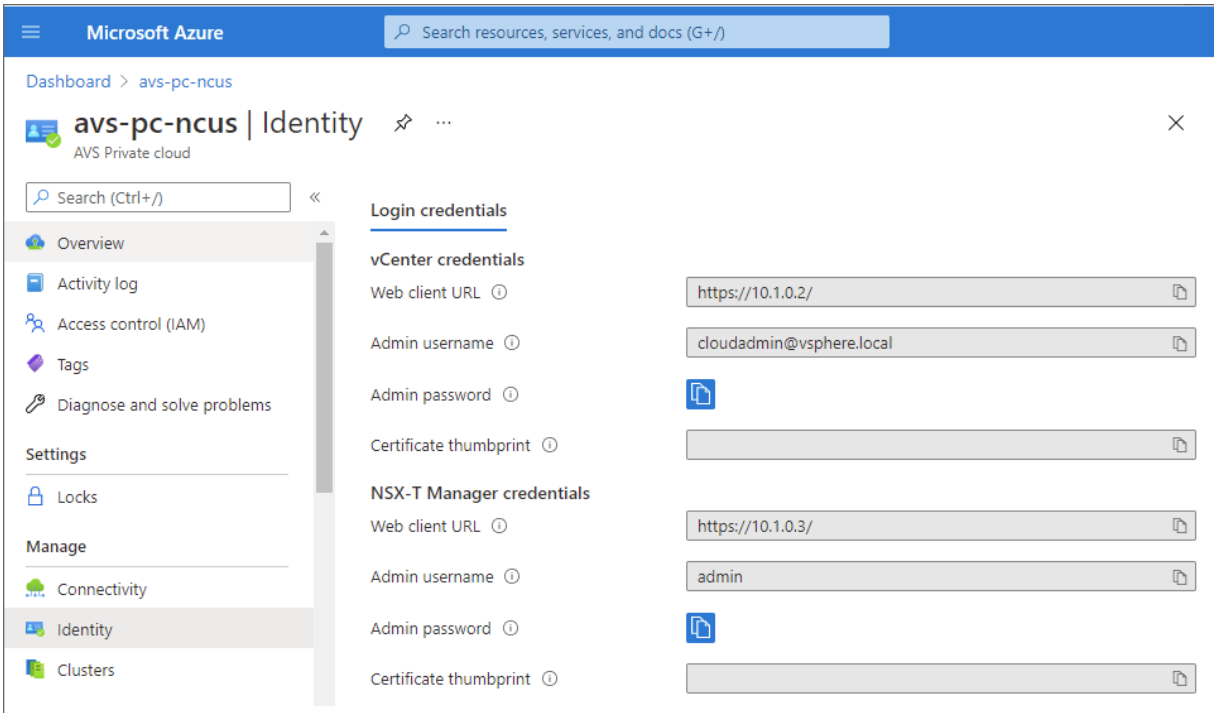
Herstellen einer Verbindung mit dem lokalen vCenter Ihrer privaten Cloud

1. Melden Sie sich als Cloudadministrator mit **VMware vCenter SSO beim vSphere-Client** an.



2. Wählen Sie im Azure-Portal Ihre private Cloud aus und wählen Sie dann **Verwalten > Identität**.

Die URLs und Benutzeranmeldeinformationen für vCenter und NSX-T Manager der privaten Cloud werden angezeigt:



Display private cloud vCenter and NSX Manager URLs and credentials.

Nach der Bestätigung der URLs und Benutzeranmeldeinformationen:

1. Navigieren Sie zu der VM, die Sie im vorherigen Schritt erstellt haben, und stellen Sie eine Verbindung zur virtuellen Maschine her.
2. Öffnen Sie in der Windows-VM einen Browser und navigieren Sie auf zwei Browserregisterkarten zu den URLs für vCenter- und NSX-T Manager. Geben Sie auf der Registerkarte "vCenter"die Benutzeranmeldeinformationen für *cloudadmin@vmcp.local* aus dem vorherigen Schritt ein.

Konfigurieren des Netzwerks für Ihre private VMware-Cloud in Azure Konfigurieren Sie nach dem Zugriff auf eine private ASV-Cloud das Netzwerk, indem Sie ein virtuelles Netzwerk und ein Gateway erstellen.

Erstellen eines virtuellen Netzwerks

1. Melden Sie sich beim Azure-Portal an.
2. Navigieren Sie zu der zuvor erstellten Ressourcengruppe.
3. Wählen Sie **+ Hinzufügen** aus, um eine neue Ressource zu definieren.
4. Geben Sie im Textfeld **Marketplace durchsuchen** den Text *Virtuelles Netzwerk* ein. Suchen Sie nach der Ressource für virtuelle Netzwerke und wählen Sie sie aus.
5. Wählen Sie auf der Seite **Virtuelles Netzwerk** die Option **Erstellen** aus, um das virtuelle Netzwerk für Ihre private Cloud einzurichten.

6. Geben Sie auf der Seite **Virtuelles Netzwerk erstellen** die Details für Ihr virtuelles Netzwerk ein.
7. Geben Sie auf der Registerkarte **Grundlagen** einen Namen für das virtuelle Netzwerk ein, wählen Sie die entsprechende Region aus und klicken Sie auf **Weiter: IP-Adressen**.
8. Geben Sie auf der Registerkarte **IP-Adressen** unter "IPv4-Adressraum"die zuvor erstellte Adresse ein.

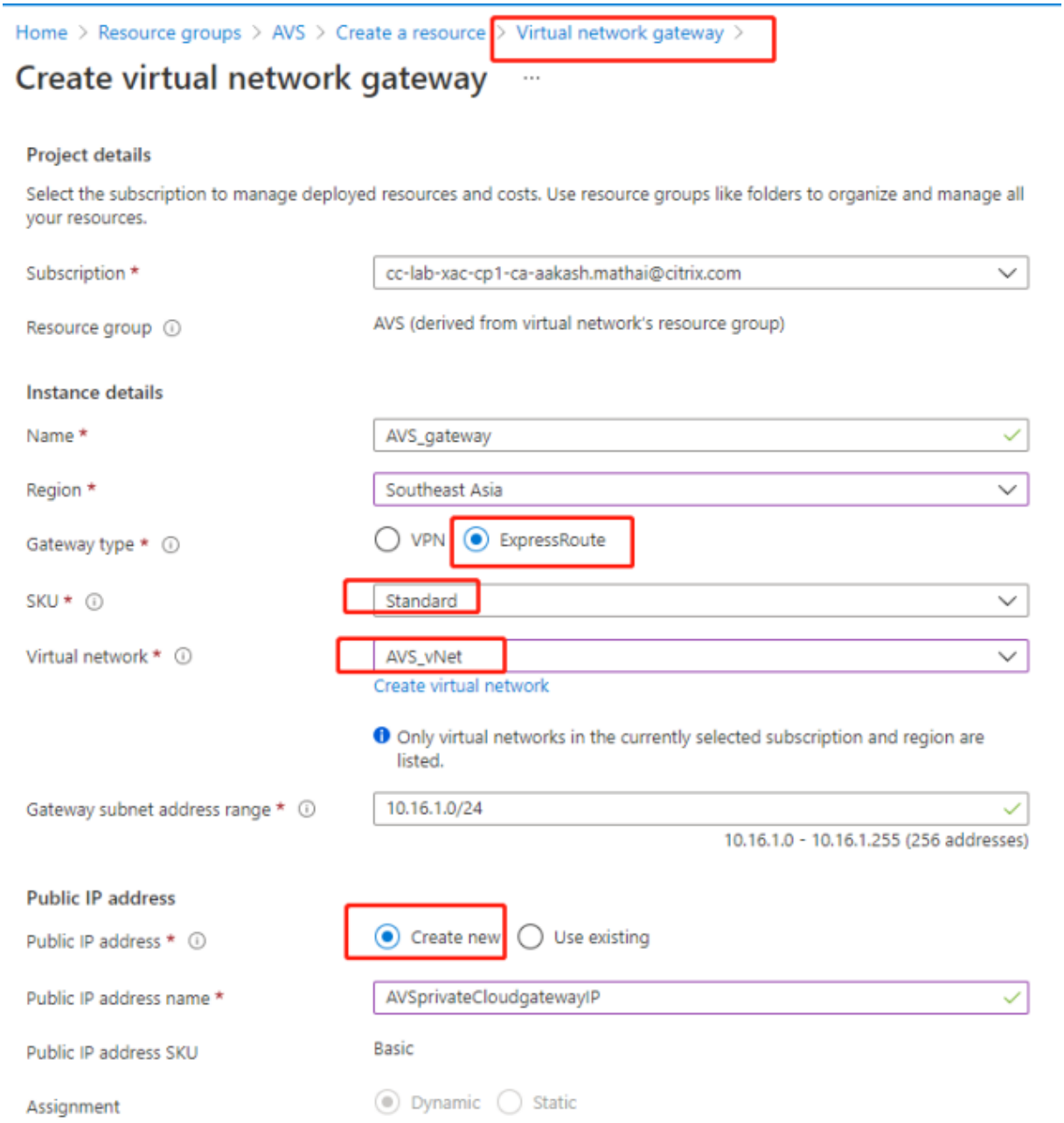
> **Wichtig:**
>
> Verwenden Sie eine Adresse, die sich nicht mit dem Adressraum überschneidet, den Sie bei der Erstellung Ihrer privaten Cloud verwendet haben.

Nach Eingabe des Adressraums:

1. Wählen Sie **+ Subnetz hinzufügen** aus.
2. Geben Sie auf der Seite **Subnetz hinzufügen** einen Namen und einen entsprechenden Adressbereich für das Subnetz an.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie **Überprüfen und erstellen** aus.
5. Überprüfen Sie die Angaben und klicken Sie auf **Erstellen**. Nach Abschluss der Bereitstellung wird das virtuelle Netzwerk in der Ressourcengruppe angezeigt.

Erstellen eines Gateways für das virtuelle Netzwerk Erstellen Sie nach dem Erstellen eines virtuellen Netzwerks ein Gateway für das virtuelle Netzwerk.

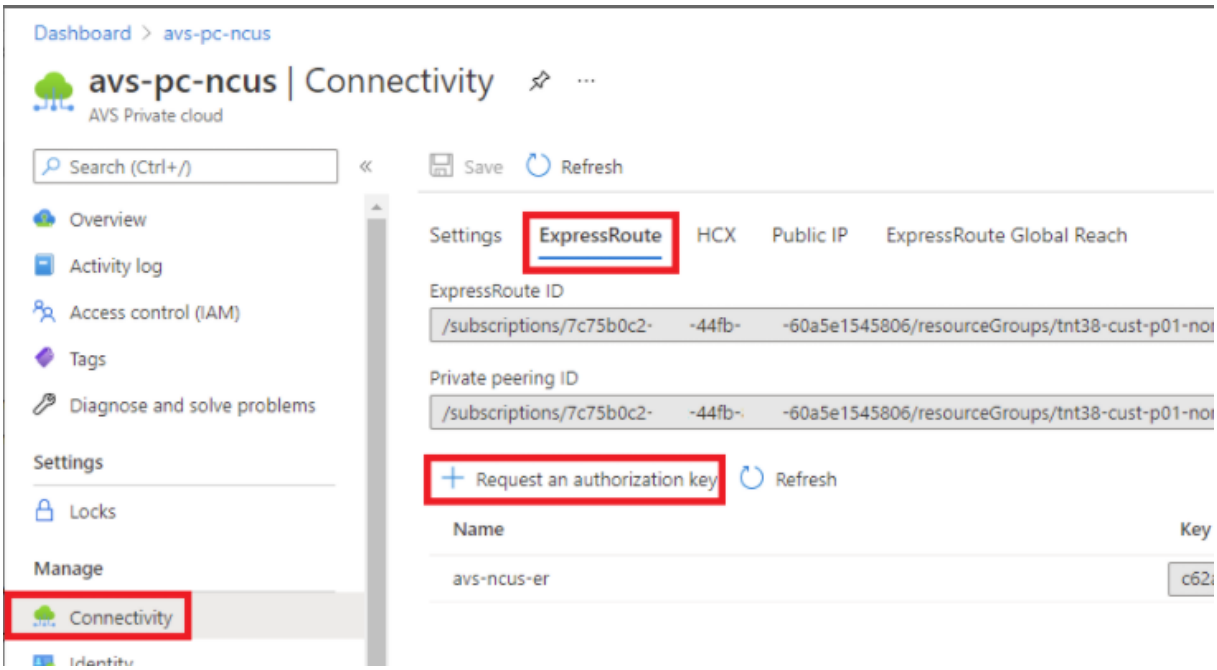
1. Wählen Sie in der Ressourcengruppe **+ Hinzufügen** aus, um eine neue Ressource hinzuzufügen.
2. Geben Sie im Textfeld **Marketplace durchsuchen** den Text *Gateway für virtuelle Netzwerke* ein. Suchen Sie nach der Ressource für virtuelle Netzwerke und wählen Sie sie aus.
3. Klicken Sie auf der Seite **Gateway für virtuelle Netzwerke** auf **Erstellen**.
4. Geben Sie auf der Registerkarte **Grundlagen** der Seite **Gateway für virtuelle Netzwerke erstellen** Werte für die Felder an.
5. Klicken Sie auf **Überprüfen und erstellen**.



Klicken Sie nach der Überprüfung der Konfiguration des Gateways für virtuelle Netzwerke auf **Erstellen**, um die Bereitstellung des Gateways für virtuelle Netzwerke zu starten.
Verbinden Sie nach Abschluss der Bereitstellung Ihre **ExpressRoute**-Verbindung mit dem Gateway für virtuelle Netzwerke, das Ihre private Azure AVS-Cloud enthält.

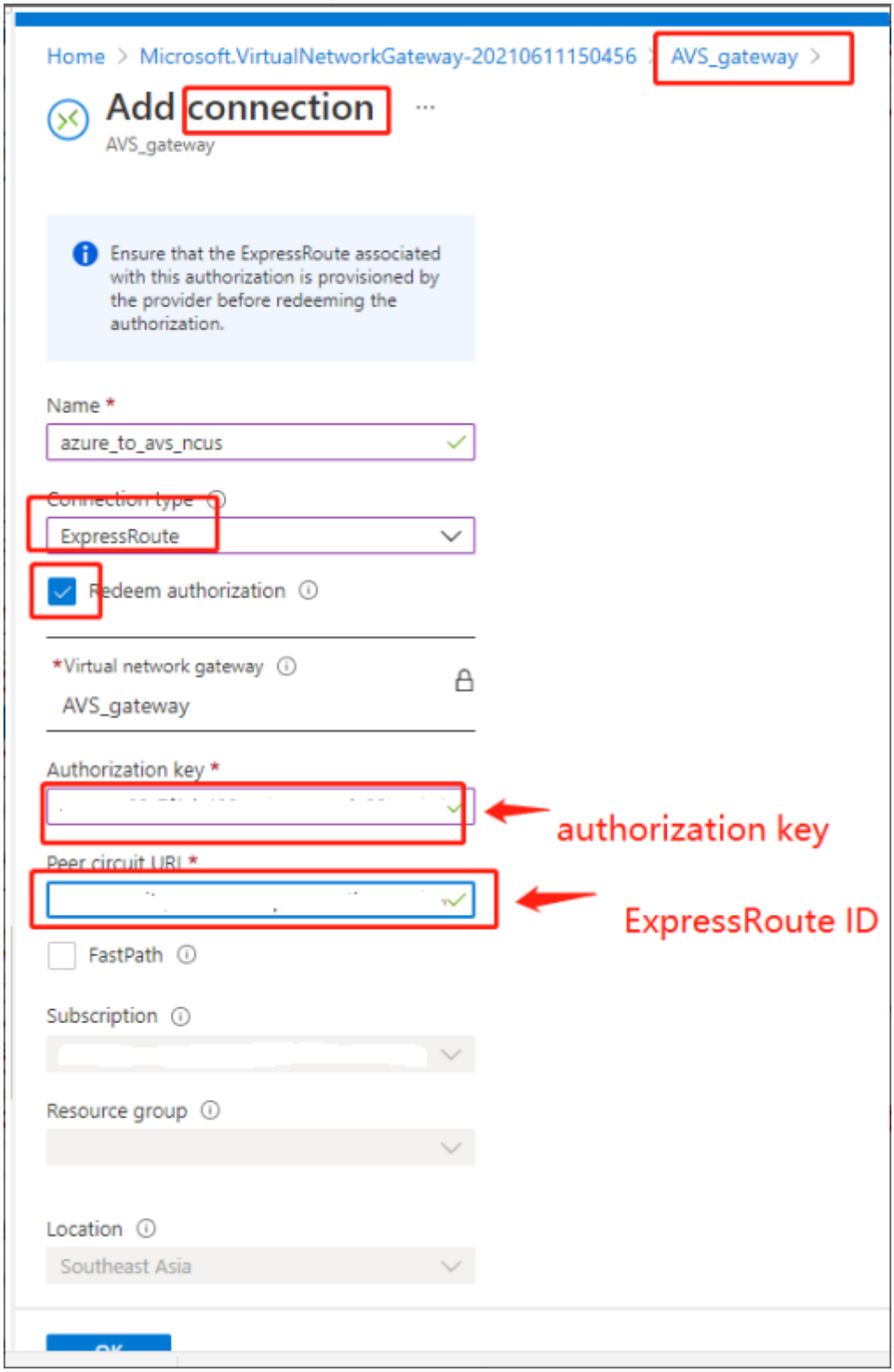
Verbinden von ExpressRoute mit dem Gateway für virtuelle Netzwerke Fügen Sie nach der Bereitstellung eines Gateways für virtuelle Netzwerke eine Verbindung zwischen dem Gateway und Ihrer privaten Azure AVS-Cloud hinzu:

1. Fordern Sie einen ExpressRoute-Autorisierungsschlüssel an.
2. Navigieren Sie im Azure-Portal zur **privaten Azure VMware Solution-Cloud**. Wählen Sie **Verwalten > Konnektivität > ExpressRoute** und anschließend **+ Autorisierungsschlüssel anfordern** aus.

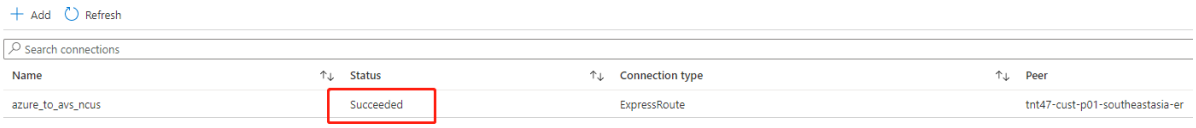


Nach dem Anfordern eines Autorisierungsschlüssels:

1. Geben Sie einen Namen für den Schlüssel ein und klicken Sie auf **Erstellen**. Das Erstellen des Schlüssels kann etwa 30 Sekunden dauern. Nach der Erstellung wird der neue Schlüssel in der Liste der Autorisierungsschlüssel für die private Cloud angezeigt.
2. Kopieren Sie den **Autorisierungsschlüssel** und die **ExpressRoute-ID**. Diese Angaben benötigen Sie, um den Peering-Prozess abzuschließen. Der Autorisierungsschlüssel wird nach einiger Zeit nicht mehr angezeigt. Kopieren Sie ihn daher, sobald er erscheint.
3. Navigieren Sie zu dem **Gateway für virtuelle Netzwerke**, das Sie verwenden möchten, und wählen Sie **Verbindungen > + Hinzufügen** aus.
4. Geben Sie auf der Seite **Verbindung hinzufügen** Werte für die Felder ein und wählen Sie **OK** aus.



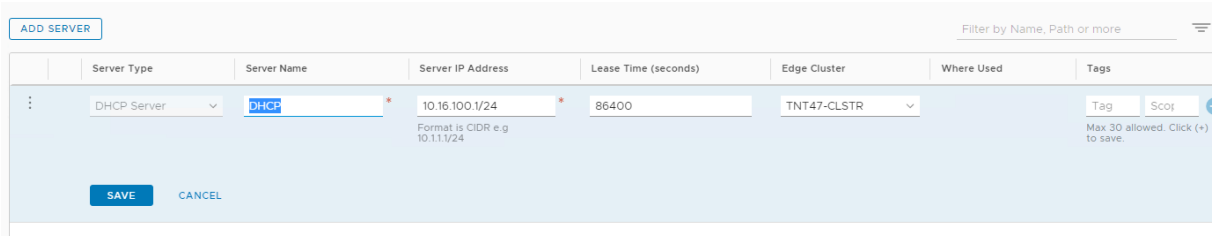
Die Verbindung zwischen Ihrer ExpressRoute-Leitung und Ihrem virtuellen Netzwerk wird hergestellt:



Konfigurieren von DHCP für Azure VMware Solution Konfigurieren Sie DHCP, nachdem Sie ExpressRoute mit dem virtuellen Gateway verbunden haben.

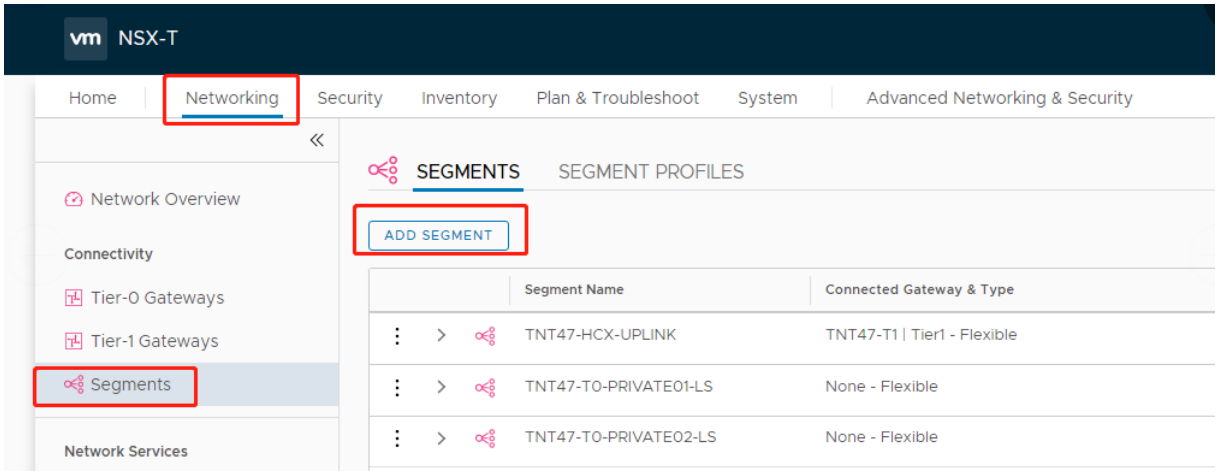
Verwenden von NSX-T zum Hosten Ihres DHCP-Servers In NSX-T Manager:

1. Wählen Sie **Networking > DHCP** und dann **Add Server** aus.
2. Wählen Sie **DHCP** unter **Server Type** aus und geben Sie den Servernamen und die IP-Adresse an.
3. Klicken Sie auf **Speichern**.
4. Wählen Sie **Tier-1 Gateways** aus. Wählen Sie dann die vertikalen Auslassungspunkte für das Tier-1-Gateway und anschließend **Edit** aus.
5. Wählen Sie **No IP Allocation Set** aus, um ein Subnetz hinzuzufügen.
6. Wählen Sie **DHCP Local Server** unter **Type** aus.
7. Wählen Sie für **DHCP Server** die Option **Default DHCP** aus und klicken Sie dann auf **Save**.
8. Klicken Sie erneut auf **Save** und wählen Sie dann **Close Editing** aus.



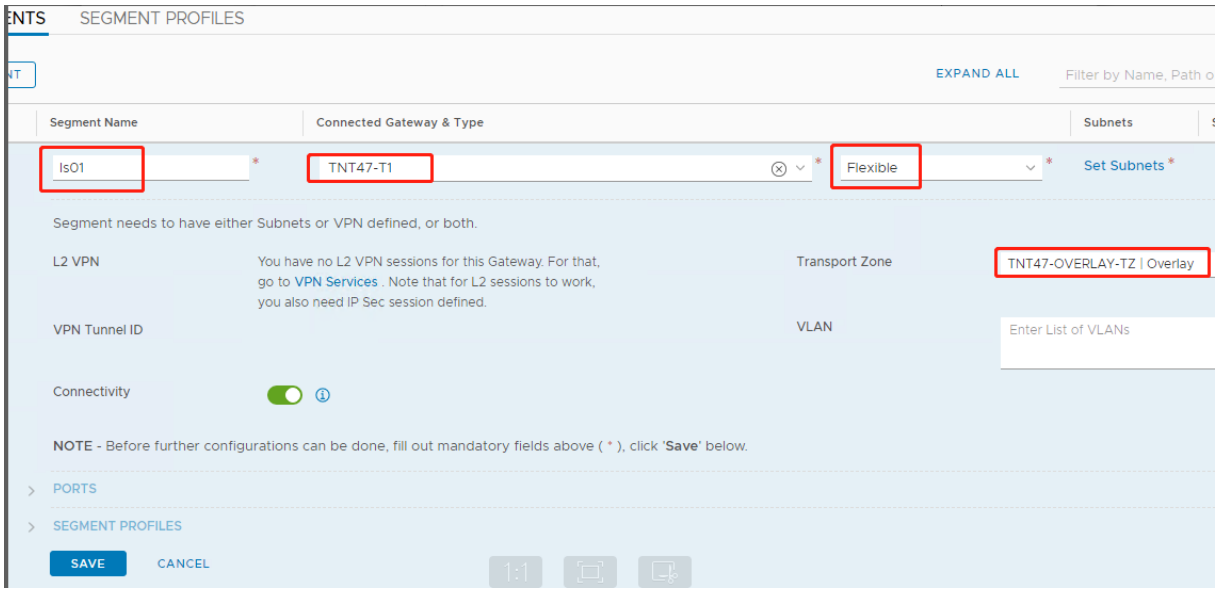
Netzwerksegment in Azure VMware Solution hinzufügen Fügen Sie nach dem Einrichten von DHCP ein Netzwerksegment hinzu.

Zum Hinzufügen eines Netzwerksegments wählen Sie in NSX-T Manager **Networking > Segments** aus und klicken dann auf **Add Segment**.



Auf dem Bildschirm **Segment Profiles**:

1. Geben Sie einen **Namen** für das Segment ein.
2. Wählen Sie unter **Connected Gateway** das **Tier-1 Gateway (TNTxx-T1)** aus und übernehmen Sie für **Type** die Option **Flexible**.
3. Wählen Sie die vorkonfigurierte **Transport Zone(TNTxx-OVERLAY-TZ)** für die Überlagerung aus.
4. Klicken Sie auf **Set Subnets**.



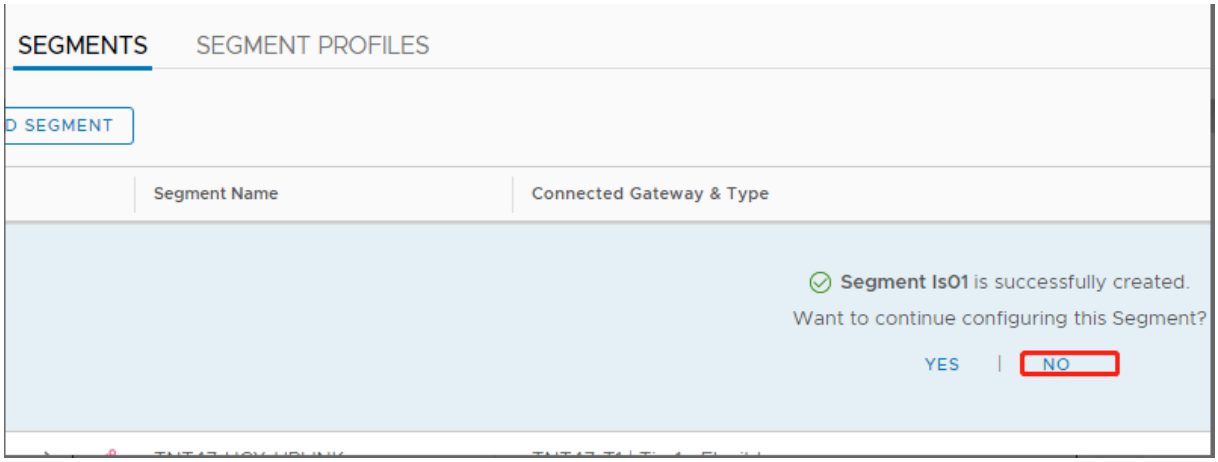
Im Abschnitt **Subnets**:

1. Geben Sie die IP-Adresse des Gateways ein.
2. Wählen Sie **Hinzufügen** aus.

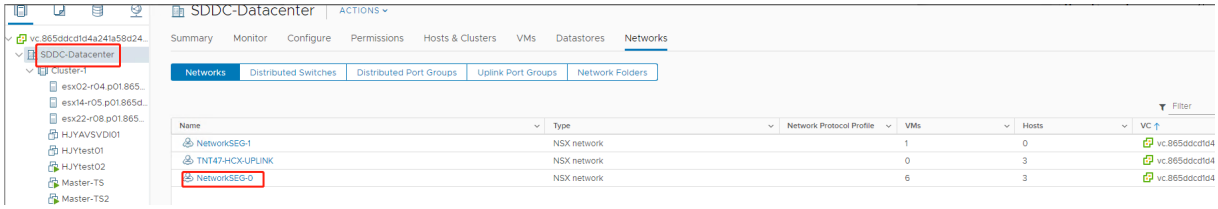
> **Wichtig:**
>
> Diese Segment-IP-Adresse muss Teil der Azure-Gateway-IP-Adresse 10.15.0.0/22 sein.

Der DHCP-Bereich muss zur Segment-IP-Adresse gehören:

Wählen Sie **No** aus, um die Option zur weiteren Konfiguration des Segments abzulehnen:



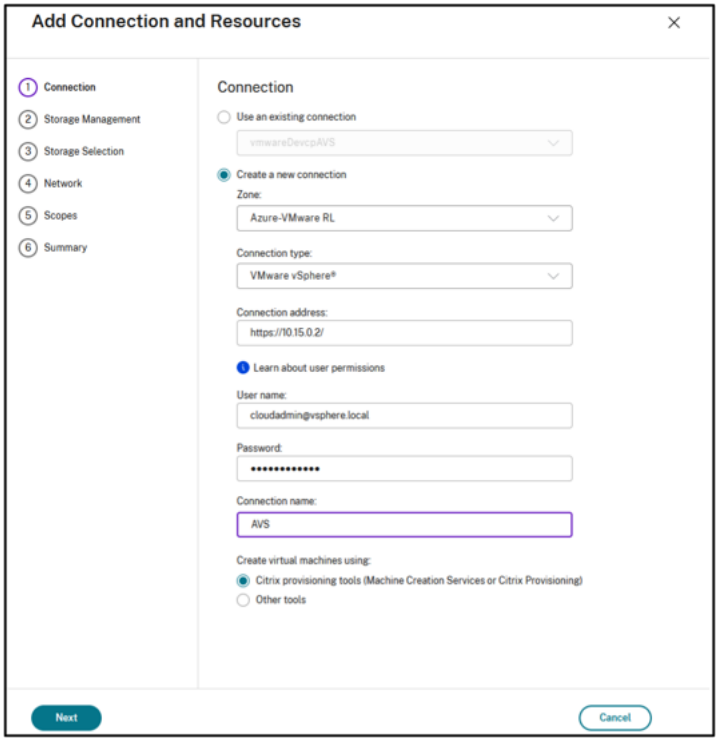
Wählen Sie in vCenter **Networking > SDDC-Datacenter** aus:



AVS-Umgebung überprüfen Richten Sie den Ressourcenstandort für die AVS Private Cloud ein und installieren Sie ein Paar Cloud Connectors.

AVS-Verbindung in Citrix Studio erstellen

1. Erstellen Sie eine Maschine in vCenter und installieren Sie auf ihr den Cloud Connector. Weitere Informationen finden Sie unter Instanzen konfigurieren.
2. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich Hosting.
3. Wählen Sie den Hostingknoten und klicken Sie auf **Verbindung und Ressourcen hinzufügen**.
4. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen** und machen Sie folgenden Eingaben:



a) Wählen Sie für **Verbindungstyp** die Option **VMware vSphere**.
b) Geben Sie unter **Verbindungsadresse** die private vCenter-IP-Adresse ein.
c) Geben Sie die vCenter-Anmeldeinformationen ein.
d) Geben Sie einen Verbindungsnamen ein.
e) Wählen Sie das Tool zum Erstellen virtueller Maschinen aus.

5. Wählen Sie auf der Seite **Netzwerk** das auf dem NSX-T-Server erstellte Subnetz aus.
6. Schließen Sie den Assistenten ab.

Google Cloud VMware Engine

Mit Citrix DaaS können Sie VMware-basierte Citrix On-Premises-Workloads in Google Cloud VMware Engine migrieren.

Google Cloud VMware Engine konfigurieren

Nachfolgend wird beschrieben, wie Sie Cluster in Google Cloud VMware Engine erhalten und einrichten.

Zugriff auf das VMware Engine-Portal

1. Klicken Sie in der **Google Cloud-Konsole** auf das Navigationsmenü.

2. Klicken Sie im Abschnitt **Compute** auf **VMware Engine**, um VMware Engine in einer neuen Browserregisterkarte zu öffnen.

Anforderungen zum Erstellen der ersten privaten Cloud Sie benötigen Zugriff auf Google Cloud VMware Engine, verfügbares VMware Engine-Knotenkontingent und eine geeignete IAM-Rolle. Treffen Sie folgende Vorbereitungen, bevor Sie mit der Erstellung Ihrer privaten Cloud fortfahren:

1. Fordern Sie API-Zugriff und Knotenkontingent an. Weitere Informationen finden Sie unter Requesting API access and quota.
2. Notieren Sie die Adressbereiche, die Sie für VMware-Verwaltungsgeräte und das HCX-Bereitstellungsnetzwerk verwenden möchten. Weitere Informationen finden Sie unter Networking requirements.

   > **Hinweis:**
   >
   > Die HCX-Bereitstellung gilt nur für IP Plan Version 1.0.

3. Beschaffen Sie sich die IAM-Rolle eines VMware Engine Service-Administrators.

Erstellen der ersten privaten Cloud

1. Rufen Sie das VMware Engine-Portal auf.
2. Klicken Sie auf der VMware Engine-Homepage auf **Create a private cloud**. Der Hostingstandort und die Hardwareknotentypen werden aufgeführt.
3. Wählen Sie die Anzahl der Knoten für die private Cloud aus. Mindestens drei Knoten sind erforderlich.
4. Geben Sie einen CIDR-Bereich für das VMware-Verwaltungsnetzwerk ein.
5. Geben Sie einen CIDR-Bereich für das HCX-Bereitstellungsnetzwerk ein.

   > **Wichtig:**
   >
   > - Der CIDR-Bereich darf sich mit keinem Ihrer On-Premises- oder Cloudsubnetze überschneiden. Der CIDR-Bereich muss /27 oder höher sein.
   > - Die HCX-Bereitstellung gilt nur für IP Plan Version 1.0.

6. Wählen Sie **Review and create**.
7. Prüfen Sie die Einstellungen. Um Einstellungen zu ändern, klicken Sie auf **Back**.
8. Klicken Sie auf **Create**, um die private Cloud zu erstellen.

Beim Erstellen der privaten Cloud stellt VMware Engine VMware-Komponenten bereit und richtet erste Autoscale-Richtlinien für Cluster in der privaten Cloud ein. Die Erstellung einer privaten Cloud kann eine halbe bis zwei Stunden dauern. Nach Abschluss des Vorgangs erhalten Sie eine E-Mail.

Einrichten des Google Cloud VMware Engine-VPN-Gateways Um eine erste Verbindung zu Google Cloud VMware Engine herzustellen, können Sie ein VPN-Gateway verwenden. Es handelt sich um ein OpenVPN-basiertes Client-VPN, mit dem Sie eine Verbindung zu Ihrem VMware Software Defined Data Center vCenter herstellen und jede erforderliche Erstkonfiguration vornehmen können.

Konfigurieren Sie vor Bereitstellung des VPN-Gateways den **Edge Services**-Bereich für die Region, in der Ihr SDDC bereitgestellt wird. Gehen Sie hierzu folgendermaßen vor:

1. Melden Sie sich beim **Google Cloud VMware Engine**-Portal an und gehen Sie zu **Network > Regional Settings**. Klicken Sie auf **Add Region**.
2. Wählen Sie die Region, in der Ihr SDDC bereitgestellt wird, und aktivieren Sie **Internet Access** sowie **Public IP Service**.
3. Geben Sie den bei der Planung notierten Edge Services-Bereich an, und klicken Sie auf **Submit**. Die Aktivierung dieser Services dauert 10—15 Minuten.

   Sobald der Vorgang abgeschlossen ist, werden die Edge Services auf der Seite "Regional Settings"als **Enabled** angezeigt. Durch die Aktivierung dieser Einstellungen können Ihrem SDDC öffentliche IPs zugewiesen werden, was für die Bereitstellung eines VPN-Gateways erforderlich ist.

VPN-Gateway bereitstellen

1. Gehen Sie im **Google Cloud VMware Engine**-Portal zu **Network > VPN Gateways**. Klicken Sie auf **Create New VPN Gateway**.
2. Geben Sie den Namen für das VPN-Gateway und das bei der Planung reservierte Clientsubnetz an. Der Standort des VPN muss mit dem Standort der Region der privaten Cloud übereinstimmen. Klicken Sie auf **Weiter**.
3. Wählen Sie Benutzer aus, die VPN-Zugriff erhalten sollen. Klicken Sie auf **Weiter**.
4. Geben Sie die Netzwerke an, die für das VPN zugänglich sein müssen. Klicken Sie auf **Weiter**.
5. Eine Zusammenfassung wird angezeigt. Überprüfen Sie die Auswahl und klicken Sie auf **Submit**, um das VPN-Gateway zu erstellen. Die Seite "VPN Gateways"wird angezeigt, der Status des neuen VPN-Gateways lautet **Creating**.
6. Wenn der Status in **Operational** wechselt, klicken Sie auf das neue VPN-Gateway.
7. Klicken Sie auf **Download my VPN configuration**, um eine ZIP-Datei mit vorkonfigurierten OpenVPN-Profilen für das VPN-Gateway herunterzuladen. Es stehen Profile für die Verbindung über UDP/1194 und TCP/443 zur Verfügung. Importieren Sie die bevorzugte Option in Open VPN und stellen Sie eine Verbindung her.
8. Gehen Sie zu **Resources** und wählen Sie Ihr SDDC aus.

VPN verbinden

1. Stellen Sie über das VPN-Gateway-Setup eine Point-to-Site-Verbindung zwischen Ihrem On-Premises-Netzwerk und der privaten Cloud her. Siehe Einrichten des Google Cloud VMware Engine-VPN-Gateways.
2. Laden Sie die VPN-Konfiguration hoch, die Sie unter Einrichten des Google Cloud VMware Engine-VPN-Gateways heruntergeladen haben.
3. Importieren Sie sie in Ihren VPN-Client, zum Beispiel OpenVPN Connect.

Weitere Informationen finden Sie unter Verbindung über VPN herstellen.

Erstellen des ersten Subnetzes

Zugriff auf NSX-T Manager über das VMware Engine-Portal Das Subnetz wird in NSX-T erstellt, auf das Sie über VMware Engine zugreifen. Gehen Sie wie folgt vor, um auf NSX-T Manager zuzugreifen.

1. Melden Sie sich beim **Google Cloud VMware Engine**-Portal an.
2. Rufen Sie im Hauptmenü **Resources** auf.
3. Klicken Sie unter **Private cloud name** auf die private Cloud, in der Sie das Subnetz erstellen möchten.
4. Klicken Sie auf der Detailseite der privaten Cloud auf die Registerkarte **vSphere Management Network**.
5. Klicken Sie auf den **FQDN** des NSX-T Managers.
6. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein. Wenn Sie vIDM eingerichtet und mit einer Identitätsquelle wie Active Directory verbunden haben, verwenden Sie stattdessen Ihre Anmeldeinformationen für diese Identitätsquelle.

   > **Erinnerung:**
   >
   > Sie können generierte Anmeldeinformationen von der Detailseite der privaten Cloud abrufen.

Einrichten von DHCP für das Subnetz Bevor Sie ein Subnetz erstellen können, richten Sie einen DHCP-Dienst ein:

In NSX-T Manager:

1. Gehen Sie zu **Network > DHCP**. Das Netzwerkdashboard zeigt an, dass der DHCP-Dienst ein Tier-0- und ein Tier-1-Gateway erstellt.
2. Klicken Sie auf **Add Server**, um mit dem Provisioning des DHCP-Servers zu beginnen.

3. Wählen Sie **DHCP** unter **Server Type** aus und geben Sie den Servernamen und die IP-Adresse an.
4. Klicken Sie auf **Save**, um den DHCP-Dienst zu erstellen.

Gehen Sie wie folgt vor, um den DHCP-Dienst dem Tier-1-Gateway anzufügen. Ein standardmäßiges Tier-1-Gateway wurde bereits vom DHCP-Dienst bereitgestellt:

1. Wählen Sie **Tier-1 Gateways** aus. Wählen Sie dann die vertikalen Auslassungspunkte für das Tier-1-Gateway und anschließend **Edit** aus.
2. Wählen Sie im Feld **IP Address Management** die Option **No IP Allocation Set**.
3. Wählen Sie **DHCP Local Server** unter **Type** aus.
4. Wählen Sie den unter **DHCP Server** erstellten DHCP-Server.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Close Editing**.

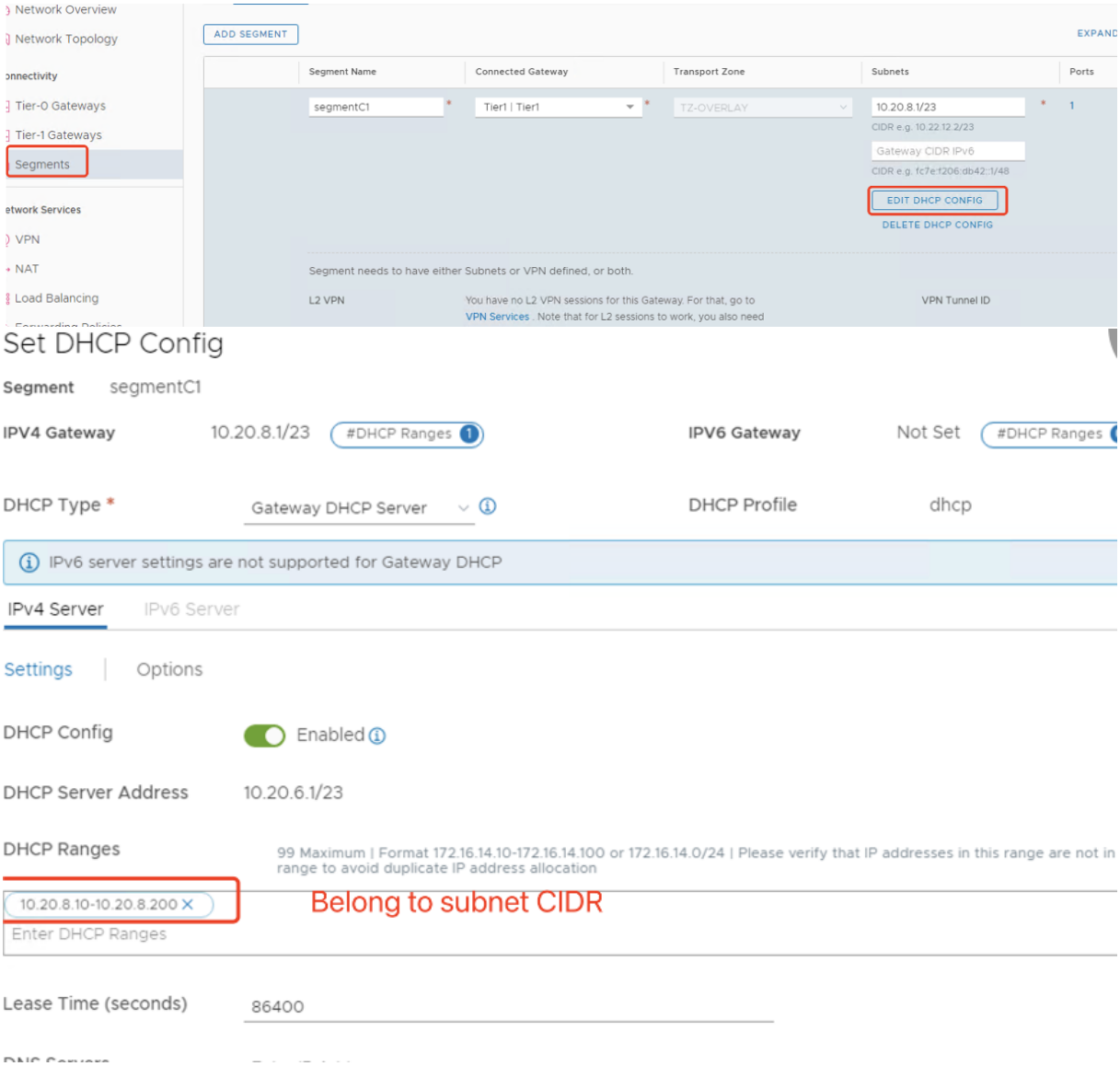
Sie können jetzt ein Netzwerksegment in NSX-T erstellen. Weitere Informationen zu DHCP in NSX-T finden Sie in der VMware-Dokumentation für DHCP.

Erstellen eines Netzwerksegments in NSX-T Für Workload-VMs erstellen Sie Subnetze als NSX-T-Netzwerksegmente für Ihre private Cloud:

1. Gehen Sie in NSX-T Manager zu **Networking > Segments**.
2. Klicken Sie auf **Add Segment**.
3. Geben Sie einen Namen für das Segment ein.
4. Wählen Sie unter **Connected Gateway** die Option **Tier-1** und übernehmen Sie als Typ die Option **Flexible**.
5. Klicken Sie auf **Set Subnets**.
6. Klicken Sie auf **Add Subnets**.
7. Geben Sie unter **Gateway IP/Prefix Length** den Subnetzbereich ein. Geben Sie den Subnetzbereich mit **.1** als letztes Oktett an. Beispiel: **10.12.2.1/24**.
8. Geben Sie die DHCP-Bereiche ein und klicken Sie auf **ADD**.
9. Wählen Sie in **Transport Zone** in der Dropdownliste **TZ-OVERLAY**.
10. Klicken Sie auf **Speichern**. Sie können das Netzwerksegment jetzt in vCenter auswählen, wenn Sie eine VM erstellen.

Sie können pro Region maximal 100 einmalige Routen von VMware Engine zu Ihrem VPC-Netzwerk mit Zugriff auf private Dienste einrichten. Dazu gehören beispielsweise IP-Adressbereiche für die Verwaltung der privaten Cloud, NSX-T-Workload-Netzwerksegmente und HCX-Netzwerk-IP-Adressbereiche. Dieses Limit umfasst alle privaten Clouds in der Region.

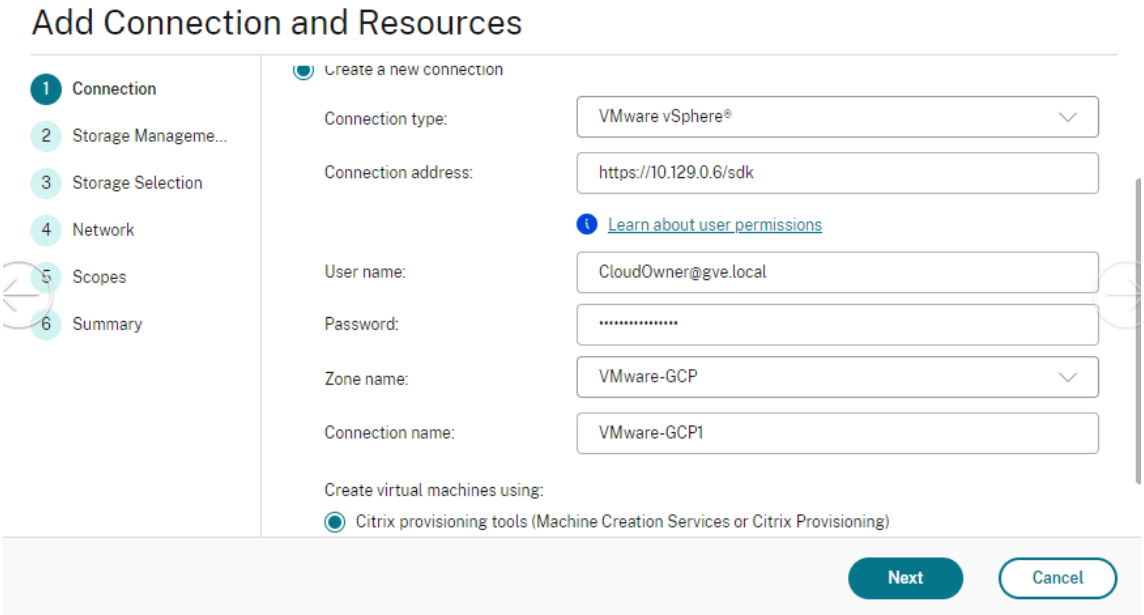
> **Hinweis:**
>
> Aufgrund eines Google Cloud-Konfigurationsproblems müssen Sie die DHCP-Bereiche mehrmals konfigurieren. Konfigurieren Sie daher die DHCP-Bereichseinstellung nach der Google Cloud-Konfiguration. Klicken Sie auf **EDIT DHCP CONFIG**, um die DHCP-Bereiche zu konfigurieren.



Erstellen der Google Cloud-VMware-Verbindung in Citrix Studio

1. Erstellen Sie eine Maschine in vCenter und installieren Sie auf ihr den Cloud Connector. Weitere Informationen finden Sie unter Instanzen konfigurieren.
2. Starten Sie Citrix Studio.
3. Wählen Sie den Hostingknoten und klicken Sie auf **Verbindung und Ressourcen hinzufügen**.

4. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen** und machen Sie folgenden Eingaben:



   a) Wählen Sie für **Verbindungstyp** die Option **VMware vSphere**.
   b) Geben Sie unter **Verbindungsadresse** die private vCenter-IP-Adresse ein.
   c) Geben Sie die vCenter-Anmeldeinformationen ein.
   d) Geben Sie einen Verbindungsnamen ein.
   e) Wählen Sie das Tool zum Erstellen virtueller Maschinen aus.

5. Wählen Sie auf der Seite **Netzwerk** das auf dem NSX-T-Server erstellte Subnetz aus.
6. Schließen Sie den Assistenten ab.

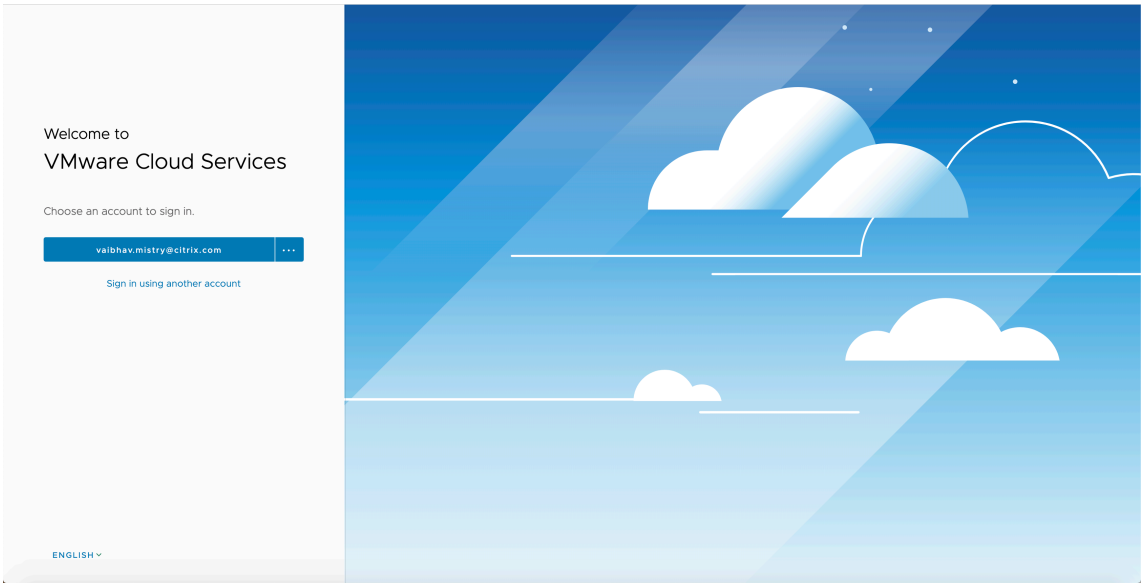
VMware-Cloud auf Amazon Web Services (AWS)

Mit VMware-Cloud auf Amazon Web Services (AWS) können Sie VMware-basierte, on-premises bereitgestellte Citrix Workloads zur AWS-Cloud und Ihre Citrix Virtual Apps and Desktops-Kernumgebung zu Citrix DaaS migrieren.

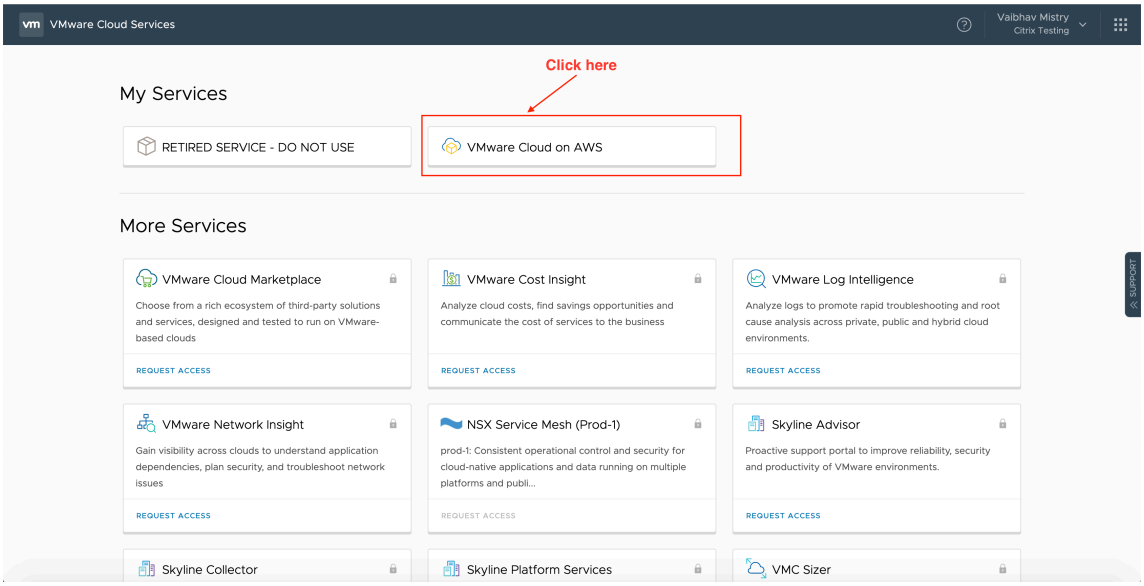
In diesem Artikel wird das Verfahren zum Einrichten einer VMware-Cloud auf AWS beschrieben.

Zugriff auf die VMware-Cloudumgebung

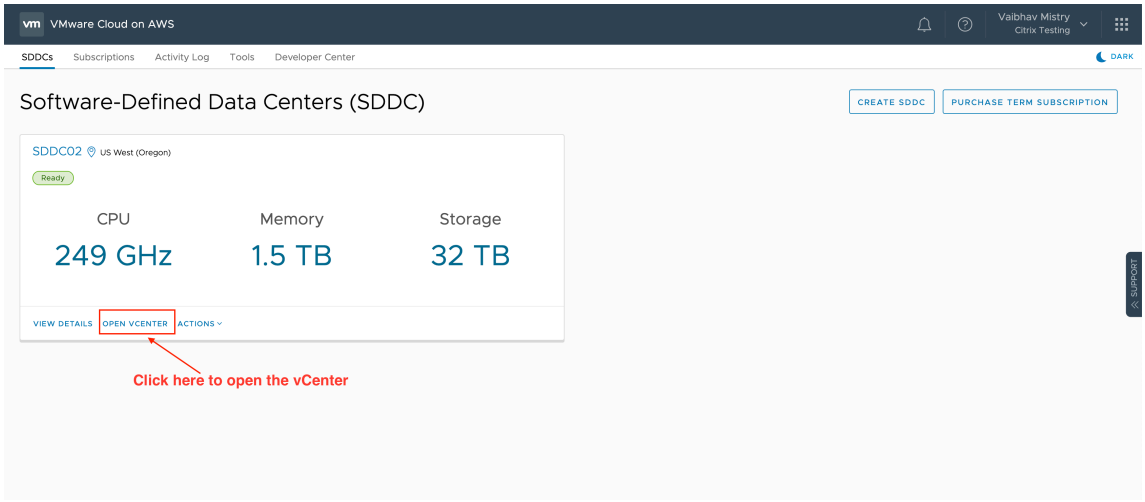
1. Melden Sie sich mit der URL https://console.cloud.vmware.com/ bei den VMware-Clouddiensten an.

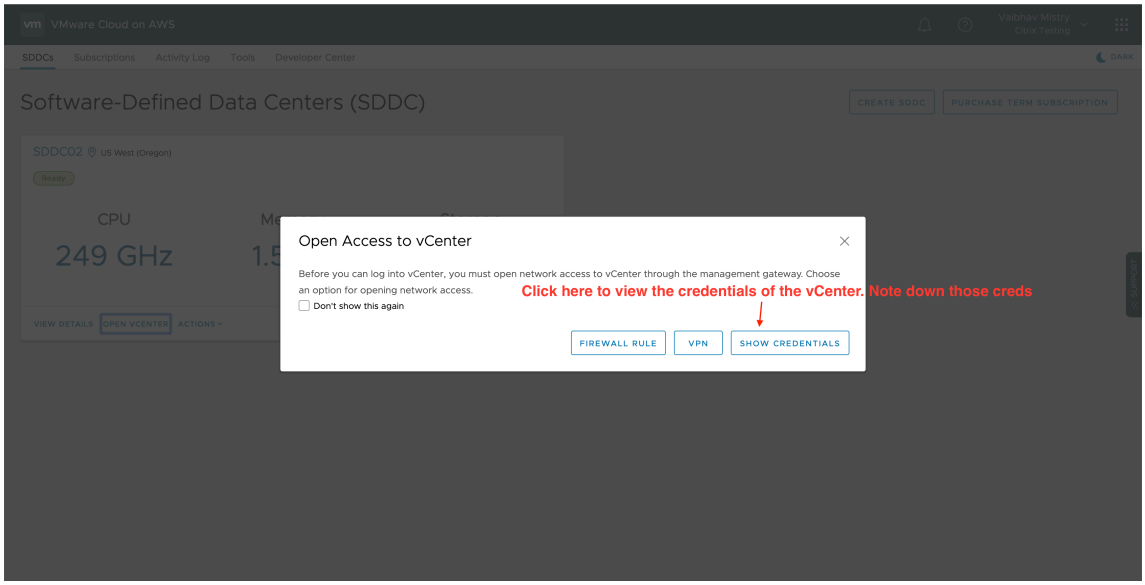


2. Klicken Sie auf **VMware Cloud on AWS**. Die Seite “Software-Defined Data Centers (SDDC)”wird angezeigt.

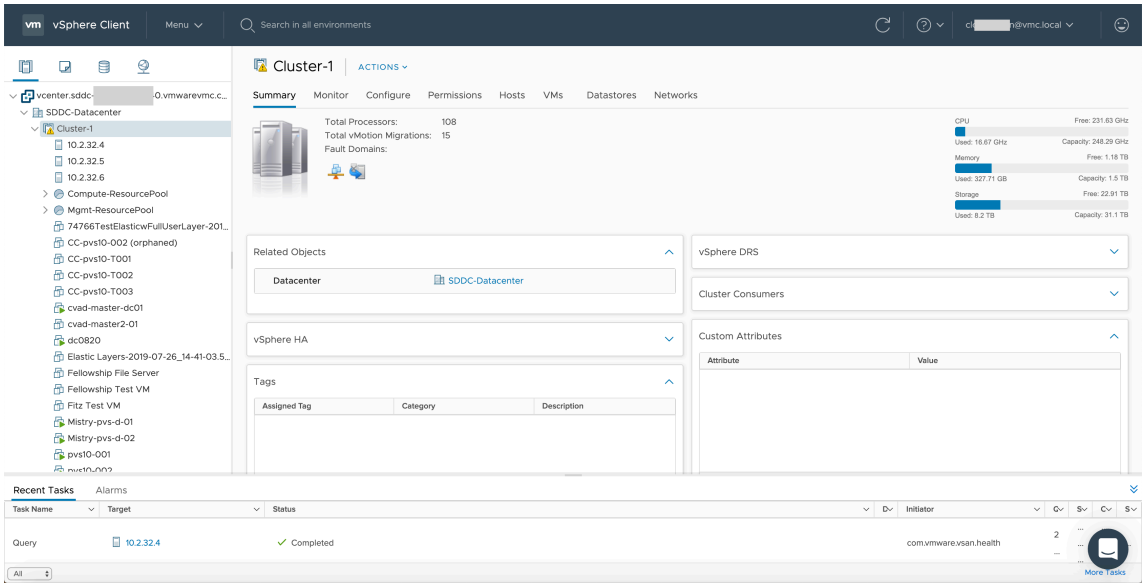


3. Klicken Sie auf **OPEN VCENTER** und dann auf **SHOW CREDENTIALS**. Notieren Sie sich die Anmeldeinformationen zur späteren Verwendung.





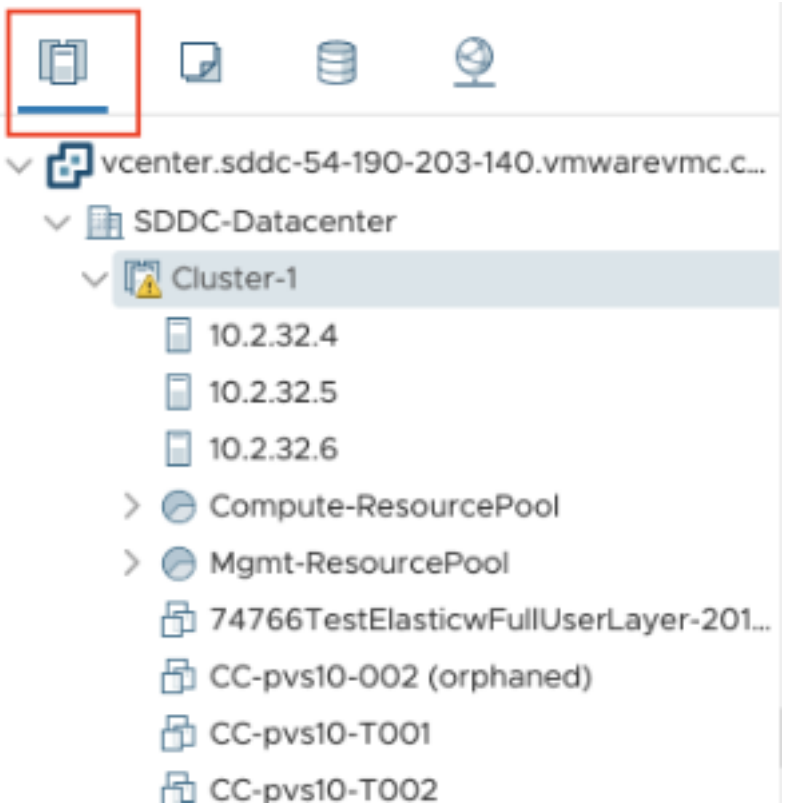
4. Öffnen Sie einen Webbrowser und geben Sie die URL für vSphere Web Client ein.
5. Geben Sie die zuvor notierten Anmeldeinformationen ein und klicken Sie auf **Login**. Die Webseite des vSphere-Clients ähnelt der On-Premises-Umgebung.



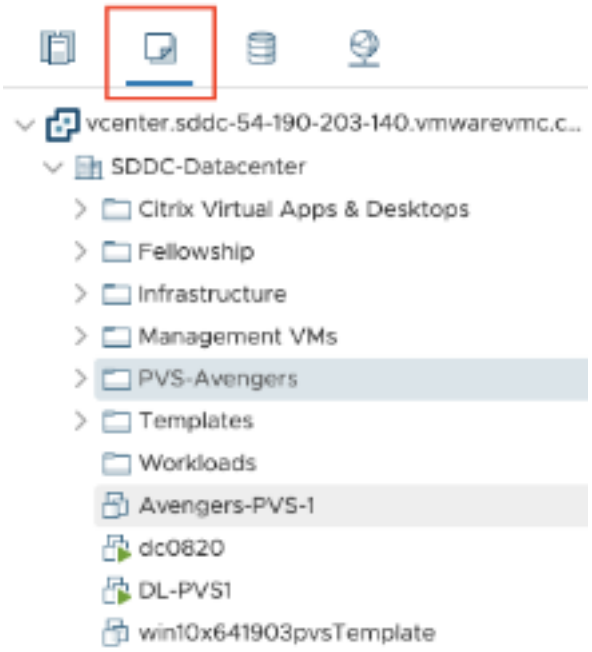
Informationen zur VMware-Cloudumgebung

Auf der Webseite des vSphere-Clients gibt es vier Ansichten.

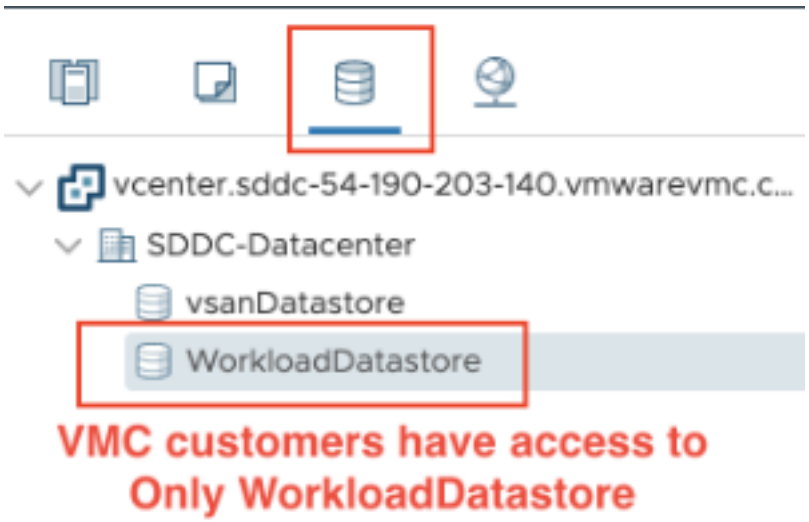
- Host- und Clusteransicht: Sie können keinen neuen Cluster erstellen, der Cloudadministrator kann jedoch mehrere Ressourcenpools erstellen.



- VM- und Vorlagenansicht: Der Cloudadministrator kann viele Ordner erstellen.



- Speicheransicht: Wählen Sie den Speicher **WorkloadDatastore**, wenn Sie eine Hosteinheit in Citrix Studio hinzufügen, da Sie nur Zugriff auf Workload Datastore haben.



- Netzwerkansicht: Die Symbole für VMware-Cloudnetzwerke und Opaque-Netzwerke sind unterschiedlich.

Nach dem Einrichten des Clusters finden Sie unter VMware-Virtualisierungsumgebungen weitere Informationen zum Hinzufügen von Verbindungen und Ressourcen.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.

- Informationen zum Erstellen und Verwalten einer Verbindung finden Sie unter Verbindung zu VMware-Cloud und Partnerlösungen.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

XenServer-Virtualisierungsumgebungen

January 25, 2024

XenServer vereinfacht Ihr Betriebsmanagement und gewährleistet ein hochauflösendes Benutzererlebnis für intensive Workloads.

Informationen zum Einrichten Ihres XenServer finden Sie unter Ressourcentyps hinzufügen.

So geht es weiter

- Für eine einfache Machbarkeitsstudie installieren Sie einen VDA auf einer Maschine, die Apps oder einen Desktop bereitstellen soll.
- Weitere Informationen zum Erstellen und Verwalten von Verbindungen finden Sie unter Verbindung zu XenServer.
- Überprüfen Sie alle Schritte im Installations- und Konfigurationsprozess.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Überlegungen zur Skalierung und Größe für Cloud Connectors

January 25, 2024

Wenn Sie Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) auf Größe und Skalierbarkeit prüfen, sollten Sie alle Komponenten berücksichtigen. Testen Sie, ob die gewählte Konfiguration aus

Citrix Cloud Connectors und StoreFront Ihren spezifischen Anforderungen entspricht. Die Bereitstellung unzureichender Ressourcen für Größe und Skalierbarkeit beeinträchtigt die Leistung Ihrer Bereitstellung.

> **Hinweis:**
>
> - Diese Empfehlungen gelten für Citrix DaaS Standard für Azure zusätzlich zu Citrix DaaS.
> - Die Tests und Empfehlungen in diesem Artikel sind Richtlinien, die Ihnen den Einstieg mit Tests erleichtern sollen. Wir empfehlen, dass Sie die Tests in Ihrer Umgebung durchführen, um die richtige Connectorgröße zu validieren.

Dieser Artikel erläutert die getesteten maximalen Kapazitäten und enthält Empfehlungen zu bewährten Methoden für die Konfiguration der Cloud Connector-Maschinen. Tests wurden für Bereitstellungen durchgeführt, die mit StoreFront und lokalem Hostcache (LHC) konfiguriert wurden.

Die Informationen gelten für Bereitstellungen, in denen jeder Ressourcenstandort entweder VDI-Workloads oder RDS-Workloads enthält. Wenn Ressourcenstandorte gemischte Workloads enthalten (VDI und RDS), wenden Sie sich an Citrix Consulting Services.

Der Cloud Connector verknüpft Ihre Workloads auf folgende Weise mit Citrix DaaS:

- Er stellt einen Proxy für die Kommunikation zwischen Ihren VDAs und Citrix DaaS bereit.
- Er stellt einen Proxy für die Kommunikation zwischen Citrix DaaS und Ihrem Active Directory (AD) und Hypervisors bereit.
- In Bereitstellungen, die StoreFront-Server enthalten, dient der Cloud Connector als temporärer Sitzungsbroker bei Cloudausfällen und bietet Benutzern damit kontinuierlichen Zugriff auf Ressourcen.

Es ist wichtig, dass Ihre Cloud Connectors Ihren spezifischen Anforderungen entsprechend dimensioniert und konfiguriert sind.

Jeder Cloud Connector-Satz ist einem Ressourcenstandort (auch bekannt als Zone) zugewiesen. Ein Ressourcenstandort ist eine logische Trennung, die angibt, welche Ressourcen mit diesem Cloud Connector-Satz kommunizieren. Für die Kommunikation mit Active Directory (AD) ist mindestens ein Ressourcenstandort pro Domäne erforderlich.

Jeder Maschinenkatalog und jede Hostverbindung ist einem Ressourcenstandort zugewiesen.

Weisen Sie bei Bereitstellungen mit mehr als einem Ressourcenstandort den Ressourcenstandorten Maschinenkataloge und VDAs zu, um die Fähigkeit des lokalen Hostcache (LHC) zur Vermittlung von Verbindungen bei Ausfällen zu optimieren. Weitere Informationen zum Erstellen und Verwalten von Ressourcenstandorten finden Sie unter Herstellen einer Verbindung mit Citrix Cloud. Konfigurieren Sie zur Gewährleistung der optimalen Leistung Ihre Cloud Connectors über Verbindungen mit niedriger Latenz zu VDAs, AD-Servern und Hypervisors.

Empfohlene Prozessoren und Speicher

Verwenden Sie moderne Prozessoren, die SHA-Erweiterungen unterstützen, um eine ähnliche Leistung wie in diesen Tests zu erzielen. SHA-Erweiterungen reduzieren die kryptografische Last auf der CPU. Zu den empfohlenen Prozessoren gehören:

- Advanced Micro Devices (AMD) Zen und neuere Prozessoren
- Intel Ice Lake und neuere Prozessoren

Die empfohlenen Prozessoren laufen effizient. Sie können ältere Prozessoren verwenden, dies kann jedoch zu einer höheren CPU-Last führen. Wir empfehlen, die Anzahl Ihrer vCPUs zu erhöhen, um dies auszugleichen.

Die in diesem Artikel beschriebenen Tests wurden mit AMD EPYC- und Intel Cascade Lake-Prozessoren durchgeführt.

Cloud Connectors haben eine hohe kryptografische Last bei der Kommunikation mit der Cloud. Bei Cloud Connectors, die Prozessoren mit SHA-Erweiterungen verwenden, ist die CPU-Auslastung geringer, was sich in einer geringeren CPU-Auslastung durch den LSASS von Windows (Subsystemdienst für die lokale Sicherheitsautorität) äußert.

Citrix empfiehlt die Verwendung von modernem Speicher mit ausreichenden E/A-Vorgängen pro Sekunde (IOPS), insbesondere für Bereitstellungen, die LHC verwenden. Festkörperlaufwerke (Solid State Drives, SSDs) werden empfohlen, Premium-Cloudspeicherebenen werden jedoch nicht benötigt. Höhere IOPS-Werte sind in LHC-Szenarios erforderlich, wenn der Cloud Connector eine kleine Kopie der Datenbank ausführt. Diese Datenbank wird regelmäßig mit Änderungen der Sitekonfiguration aktualisiert und bietet Brokerfunktionen für den Ressourcenstandort in Zeiten von Ausfällen der Citrix Cloud.

Empfohlene Rechenkonfiguration für den lokalen Hostcache

Der lokale Hostcache (LHC) gewährleistet eine hohe Verfügbarkeit, indem er das Verbindungsbrokering in einer Bereitstellung aufrechterhält, wenn ein Cloud Connector nicht mit Citrix Cloud kommunizieren kann.

Cloud Connectors führen Microsoft SQL Express Server LocalDB aus. Die Datenbank wird automatisch installiert, wenn Sie den Cloud Connector installieren. Die CPU-Konfiguration des Cloud Connectors, insbesondere die Anzahl der für SQL Express Server LocalDB verfügbaren Kerne, wirkt sich direkt auf die Leistung des lokalen Hostcache aus. Die Anzahl der für SQL Server Express Server LocalDB verfügbaren CPU-Kerne wirkt sich noch stärker auf die LHC-Leistung aus als die Speicherzuweisung. Der CPU-Mehraufwand tritt nur im LHC-Modus auf, wenn Citrix DaaS nicht erreichbar und der LHC-Broker aktiv ist. Für Bereitstellungen mit LHC empfiehlt Citrix vier Kerne pro Socket mit mindestens vier

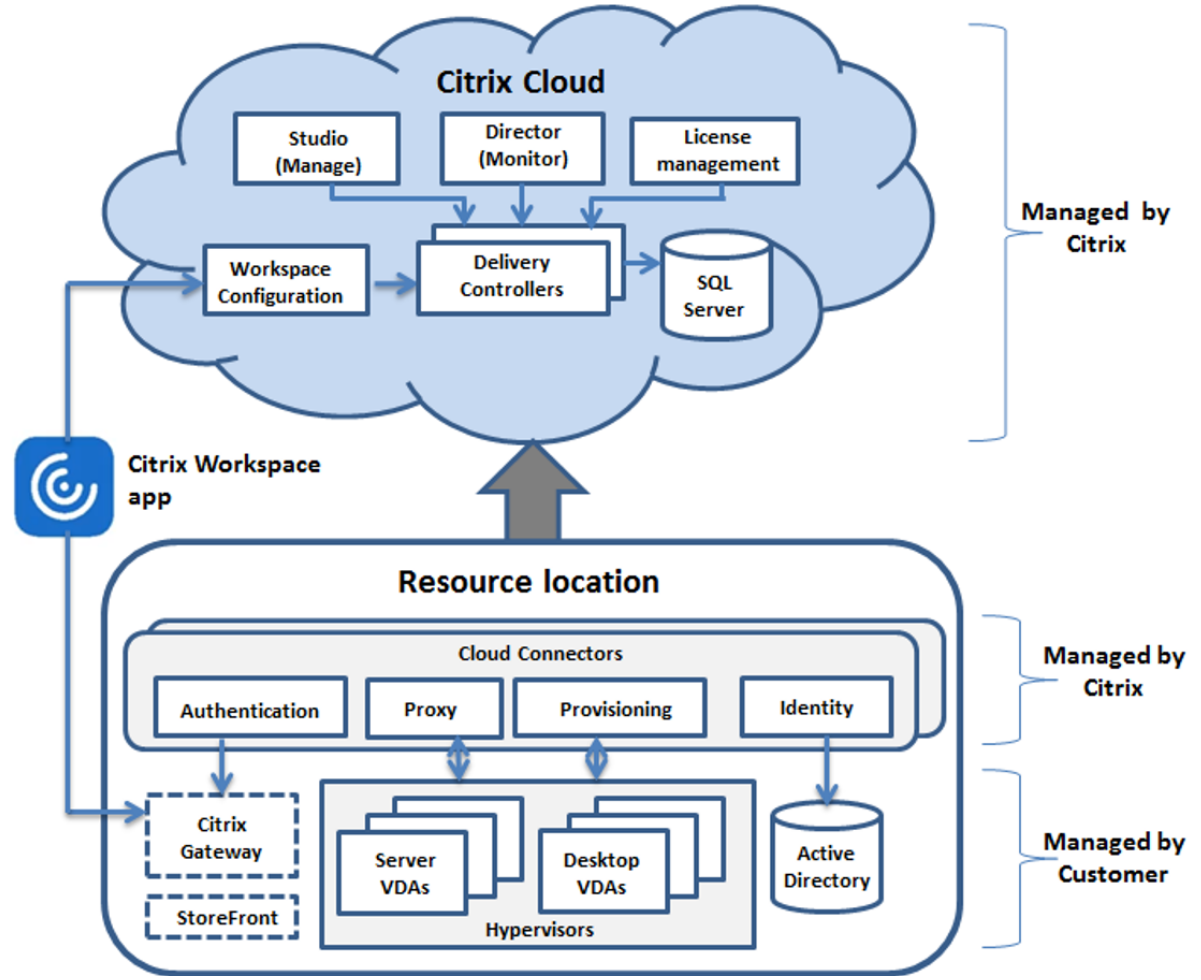
CPU-Kernen pro Cloud Connector. Informationen zur Konfiguration von Rechenressourcen für SQL Express Server LocalDB finden Sie unter Rechenkapazitätsgrenzen von bestimmten Editionen von SQL Server.

Wenn die für SQL Express Server LocalDB verfügbaren Rechenressourcen falsch konfiguriert sind, kann die Zeit für die Konfigurationssynchronisierung erhöht und die Leistung bei Ausfällen reduziert sein. In einigen virtualisierten Umgebungen kann die Rechenkapazität von der Anzahl der logischen Prozessoren und nicht der CPU-Kerne abhängen.

Zusammenfassung der Testergebnisse

Alle Ergebnisse in dieser Zusammenfassung basieren auf den Erkenntnissen aus der im Folgenden beschriebenen Testumgebung. Die hier angezeigten Ergebnisse beziehen sich auf einen einzelnen Ressourcenstandort. Andere Systemkonfigurationen führen möglicherweise zu anderen Ergebnissen.

Diese Abbildung gibt einen grafischen Überblick über die getestete Konfiguration.



Diese Tabelle enthält eine Kurzanleitung zur Dimensionierung Ihres Ressourcenstandorts. 10.000 ist das Maximum für einen einzelnen Ressourcenstandort. Informationen zu den Grenzwerten für den Ressourcenstandort finden Sie unter Limits.

> **Hinweis:**
>
> Eine Überschreitung des Grenzwerts kann zu Verbindungs- und Leistungsproblemen während eines Ausfalls führen. Daher dürfen Sie den empfohlenen Grenzwert nicht überschreiten, da dies zu nicht registrierten VDAs führen kann.

Die Ergebnisse basieren auf internen Tests von Citrix. Die beschriebenen Konfigurationen wurden mit unterschiedlichen Workloads getestet, darunter Sitzungsstarttests mit hoher Rate und Registrierungsansturm.

	Medium	Groß	Maximum
VDAs	1000 VDI oder 250 RDS	5000 VDI oder 500 RDS	10000 VDI oder 1000 RDS
Hostverbindungen	20	40	40
CPUs für Connectors	4 vCPUs	4 vCPUs	8 vCPUs
Speicher für Connectors	6 GB	8 GB	10 GB

Testmethode

In den Tests wurde die Leistung der Umgebungskomponenten nach Hinzufügen von Last gemessen. Zur Überwachung der Komponenten wurden Leistungsdaten und die erforderliche Zeit für bestimmte Prozesse (z. B. Anmeldezeit und Registrierungszeit) erfasst. In einigen Fällen werden firmeneigene Simulationstools von Citrix verwendet, um VDAs und Sitzungen zu simulieren. Diese Tools beanspruchen Citrix Komponenten auf dieselbe Weise wie herkömmliche VDAs und Sitzungen, jedoch ohne Einsatz der für das Hosten echter Sitzungen und VDAs erforderlichen Ressourcen. Die Tests wurden sowohl im Cloud-Brokering-Modus als auch im Modus mit lokalem Hostcache (LHC) für Szenarios mit Citrix StoreFront durchgeführt.

Die Empfehlungen für die Cloud Connector-Dimensionierung in diesem Artikel basieren auf Daten aus diesen Tests.

Die folgenden Tests wurden durchgeführt:

- **Sitzungsanmeldungs-/Sitzungsstartansturm:** Dieser Test simuliert ein hohes Aufkommen an gleichzeitigen Anmeldungen.

- **VDA-Registrierungsansturm:** Dieser Test simuliert ein hohes Aufkommen an gleichzeitigen VDA-Registrierungen. Beispielsweise nach einem Upgradezyklus oder beim Übergang zwischen Cloud-Brokering-Modus und Modus mit lokalem Hostcache.
- **VDA-Energieaktionsansturm:** Dieser Test simuliert ein hohes Aufkommen an VDA-Energieaktionen.

Testszenarien und Bedingungen

Diese Tests wurden mit konfiguriertem lokalem Hostcache durchgeführt. Weitere Informationen zur Verwendung des lokalen Hostcache finden Sie im Artikel Lokaler Hostcache. Für den lokalen Hostcache ist ein On-Premises-StoreFront-Server erforderlich. Ausführliche Informationen zu StoreFront finden Sie in der StoreFront-Produktdokumentation.

Empfehlungen für StoreFront-Konfigurationen:

- Wenn Sie über mehrere Ressourcenstandorte mit einem einzelnen StoreFront-Server oder einer Servergruppe verfügen, aktivieren Sie die Option für die erweiterte Systemintegritätsprüfung für den StoreFront-Store. Siehe StoreFront im Artikel "Lokaler Hostcache".
- Verwenden Sie für höhere Sitzungsstartraten eine StoreFront-Servergruppe. Siehe Konfigurieren von Servergruppen in der StoreFront-Produktdokumentation.

Testbedingungen:

- CPU- und Speicheranforderungen gelten nur für das Basisbetriebssystem und die Citrix-Dienste. Für Apps und Dienste von Drittanbietern sind möglicherweise zusätzliche Ressourcen erforderlich.
- VDAs sind virtuelle oder physische Maschinen, auf denen Citrix Virtual Delivery Agent ausgeführt wird.
- Tests werden nur mit Windows-VDAs durchgeführt.
- Die Energieverwaltung aller getesteten VDAs erfolgte mit Citrix DaaS.
- Workloads von 1000 bis 10.000 VDI- und 250 bis 1000 RDS-Servern mit 1000 bis 20.000 Sitzungen wurden getestet.
- RDS-Sitzungen wurden mit bis zu 20.000 pro Ressourcenstandort getestet.
- Die Tests wurden mit einem Cloud Connector (im normalen Betrieb und beim Ausfall) durchgeführt. Citrix empfiehlt die Verwendung von mindestens zwei Cloud Connectors, um eine hohe Verfügbarkeit zu gewährleisten. Im Ausfallmodus wird nur einer der Connectors für VDA-Registrierungen und Brokering verwendet.
- Tests wurden mit dem Cloud Connector durchgeführt, der mit Intel Cascade Lake-Prozessoren konfiguriert ist.
- Die Sitzungen wurden über einen einzelnen Citrix StoreFront-Server gestartet.
- LHC-Ausfall-Sitzungsstarttests wurden nach der erneuten Registrierung der Maschinen durchgeführt.

Die Zahl der RDS-Sitzungen ist eine Empfehlung, kein Limit. Testen Sie Ihr RDS-Sitzungslimit in Ihrer Umgebung.

> **Hinweis:**
>
> Die Sitzungsanzahl und die Startrate sind für RDS wichtiger als die VDA-Anzahl.

Mittlere Workloads

Diese Workloads wurden mit 4 vCPUs und 6 GB Speicher getestet.

Test-Workloads	Zustand der Site	VDA-Registrierungszeit	CPU- und Speicher-auslastung bei Reg-istrierung	Länge Starttest	CPU- und Speicher-auslastung beim Sitzungsstart	Startrate
1000 VDI	Online	5 Minuten	CPU-Maximum = 36 %, CPU-Durchschnitt = 33 %, Speicher-maximum = 5,3 GB	2 Minuten	CPU-Maximum = 29 %, CPU-Durchschnitt = 27 %, Speicher-maximum = 3,7 GB	500 pro Minute
1000 VDI	Ausfall	4 Minuten	CPU-Maximum = 11 %, CPU-Durchschnitt = 10 %, Speicher-maximum = 4,5 GB	2 Minuten	CPU-Maximum = 42 %, CPU-Durchschnitt = 28 %, Speicher-maximum = 4,0 GB	500 pro Minute
250 RDS, 5000 Sitzungen	Online	3 Minuten	CPU-Maximum = 14 %, CPU-Durchschnitt = 4 %, Speicher-maximum = 3,5 GB	9 Minuten	CPU-Maximum = 46 %, CPU-Durchschnitt = 21 %, Speicher-maximum = 3,7 GB	555 pro Minute

Test-Workloads	Zustand der Site	VDA-Registrierungszeit	CPU- und Speicher-auslastung bei Reg-istrierung	Länge Starttest	CPU- und Speicher-auslastung beim Sitzungsstart	Startrate
250 RDS, 5000 Sitzungen	Ausfall	3 Minuten	CPU-Maximum = 15 %, CPU-Durchschnitt = 5 %, Speicher-maximum = 3,7	9 Minuten	CPU-Maximum = 51 %, CPU-Durchschnitt = 32 %, Speicher-maximum = 4,2 GB	555 pro Minute

Große Workloads

Diese Workloads wurden mit 4 vCPUs und 8 GB Arbeitsspeicher getestet.

Test-Workloads	Zustand der Site	VDA-Registrierungszeit	CPU- und Speicher-auslastung bei Reg-istrierung	Länge Starttest	CPU- und Speicher-auslastung beim Sitzungsstart	Startrate
5000 VDI	Online	3—4 Minuten	CPU-Maximum = 45 %, CPU-Durchschnitt = 25 %, Speicher-maximum = 7,0 GB	5 Minuten	CPU-Maximum = 75 %, CPU-Durchschnitt = 55 %, Speicher-maximum = 7,0 GB	1000 pro Minute

Test-Workloads	Zustand der Site	VDA-Registrierungszeit	CPU- und Speicher-auslastung bei Reg-istrierung	Länge Starttest	CPU- und Speicher-auslastung beim Sitzungsstart	Startrate
5000 VDI	Ausfall	4—6 Minuten	CPU-Maximum = 15 %, CPU-Durchschnitt = 5 %, Speicher-maximum = 7,5 GB	5 Minuten	CPU-Maximum = 45 %, CPU-Durchschnitt = 40 %, Speicher-maximum = 7,5 GB	1000 pro Minute
500 RDS, 10.000 Sitzungen	Online	3 Minuten	CPU-Maximum = 45 %, CPU-Durchschnitt = 25 %, Speicher-maximum = 7,0 GB	10 Minuten	CPU-Maximum = 75 %, CPU-Durchschnitt = 55 %, Speicher-maximum = 7,0 GB	1000 pro Minute
500 RDS, 10.000 Sitzungen	Ausfall	3 Minuten	CPU-Maximum = 15 %, CPU-Durchschnitt = 5 %, Speicher-maximum = 7,5	10 Minuten	CPU-Maximum = 45 %, CPU-Durchschnitt = 40 %, Speicher-maximum = 7,5 GB	1000 pro Minute

Maximale Workloads

Diese Workloads wurden mit 8 vCPUs und 10 GB Speicher getestet.

Test-Workloads	Zustand der Site	VDA-Registrierungszeit	CPU- und Speicher-auslastung bei Reg-istrierung	Länge Starttest	CPU- und Speicher-auslastung beim Sitzungsstart	Startrate
10.000 VDI	Online	3—4 Minuten	CPU-Maximum = 85 %, CPU-Durchschnitt = 10 %, Speicher-maximum = 8,5 GB	7 Minuten	CPU-Maximum = 66 %, CPU-Durchschnitt = 28 %, Speicher-maximum = 7,0 GB	1400 pro Minute
10.000 VDI	Ausfall	4–5 Minuten	CPU-Maximum = 90 %, CPU-Durchschnitt = 17 %, Speicher-maximum = 8,2 GB	5 Minuten	CPU-Maximum = 90 %, CPU-Durchschnitt = 45 %, Speicher-maximum = 8,5 GB	2000 pro Minute
1000 RDS, 20.000 Sitzungen	Online	1—2 Minuten	CPU-Maximum = 60 %, CPU-Durchschnitt = 20 %, Speicher-maximum = 8,6 GB	17 Minuten	CPU-Maximum = 66 %, CPU-Durchschnitt = 25 %, Speicher-maximum = 6,8 GB	1200 pro Minute
1000 RDS, 20.000 Sitzungen	Ausfall	3—4 Minuten	CPU-Maximum = 22 %, CPU-Durchschnitt = 10 %, Speicher-maximum = 8,5	21 Minuten	CPU-Maximum = 90 %, CPU-Durchschnitt = 50 %, Speicher-maximum = 7,5 GB	1000 pro Minute

> **Hinweis:**
>
> Die hier gezeigten Workloads sind die maximal empfohlenen Workloads für einen Ressourcenstandort. Um größere Workloads zu unterstützen, fügen Sie weitere Ressourcenstandorte hinzu.

Ressourcennutzung der Konfigurationssynchronisierung

Durch den Prozess der Konfigurationssynchronisierung werden die Cloud Connectors mit Citrix DaaS auf dem neuesten Stand gehalten. Updates werden automatisch an die Cloud Connectors gesendet, um sicherzustellen, dass die Cloud Connectors bereit sind, bei einem Ausfall das Brokering zu übernehmen. Die Konfigurationssynchronisierung aktualisiert die Datenbank des lokalen Hostcache, SQL Express Server LocalDB. Der Prozess importiert die Daten in eine temporäre Datenbank und wechselt dann nach dem Import zu dieser Datenbank. Dadurch wird sichergestellt, dass immer eine Datenbank des lokalen Hostcache zur Übernahme bereit ist.

Die CPU-, Speicher- und Datenträgerauslastung ist vorübergehend erhöht, während Daten in die temporäre Datenbank importiert werden.

Testergebnisse:

- **Datenimportzeit:** 7—10 Minuten
- **CPU-Auslastung:**
  - Maximum = 25 %
  - Durchschnitt = 15 %
- **Speicherauslastung:**
  - Maximum = 9 GB
  - Anstieg von etwa 2 GB auf 3 GB
- **Datenträgerauslastung:**
  - 4 MB/s Spitze beim Lesen von Datenträger
  - 18 MB/s Spitze beim Schreiben auf Datenträger
  - 70 MB/s Spitze beim Schreiben auf Datenträger während des Herunterladens und Schreibens von XML-Konfigurationsdateien
  - 4 MB/s Spitze beim Lesen von Datenträger nach Abschluss des Imports
- **Größe der Datenbank des lokalen Hostcache:**
  - 400—500 MB Datenbankdatei
  - 200—300 MB Protokolldatenbank

Testbedingungen:

- Getestet auf 8 vCPU AMD EPYC
- Die importierte Sitekonfigurationsdatenbank war für eine Umgebung mit insgesamt 80.000 VDAs und 300.000 Benutzern (drei Schichten von 100.000 Benutzern) vorgesehen.
- Die Datenimportzeit wurde an einem Ressourcenstandort mit 10.000 VDI getestet.

Zusätzliche Überlegungen zur Ressourcennutzung:

- Während des Imports werden die vollständigen Sitekonfigurationsdaten heruntergeladen. Dieser Download kann je nach Sitegröße zu einer Speichernutzungsspitze führen.
- Die getestete Site verwendete ungefähr 800 MB für die Datenbank- und Datenbankprotokolldateien zusammen. Während einer Konfigurationssynchronisierung werden diese Dateien mit einer maximalen kombinierten Größe von ungefähr 1600 MB dupliziert. Stellen Sie sicher, dass Ihr Cloud Connector über ausreichend Speicherplatz für die duplizierten Dateien verfügt. Die Konfigurationssynchronisierung schlägt fehl, wenn der Datenträger voll ist.

VDAs installieren

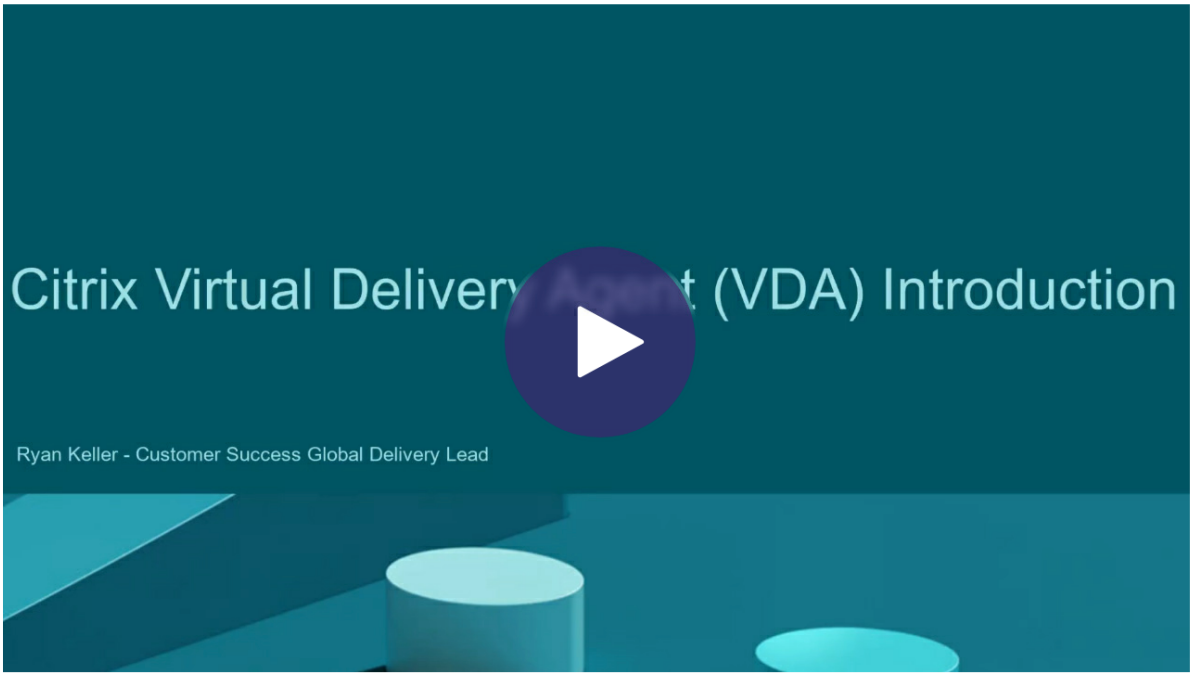
May 17, 2024

Einführung

Dieser Artikel beginnt mit einer Beschreibung der Windows-VDAs und der VDA-Installationsprogramme. Anschließend werden die im VDA-Installationsassistenten auszuführenden Schritte erläutert. Die entsprechenden Befehle für die Befehlszeile werden ebenfalls angegeben. Weitere Informationen finden Sie unter Installieren von VDAs über die Befehlszeile.

Informationen zu Linux VDAs finden Sie unter Linux Virtual Delivery Agent.

Video mit Einführung zu VDAs:



Überlegungen zur Installation

Unter Citrix DaaS werden Zweck und Funktion von VDAs beschrieben. Hier finden Sie weitere Informationen.

- **Sammeln von Analysedaten:** Wenn Sie die Komponenten installieren oder aktualisieren, werden automatisch Analysedaten gesammelt. Standardmäßig werden die Daten automatisch an Citrix hochgeladen, wenn die Installation abgeschlossen ist. Bei der Installation von Komponenten werden Sie außerdem automatisch beim Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) angemeldet, in dessen Rahmen anonyme Daten hochgeladen werden. Während einer Installation oder eines Upgrades wird Ihnen außerdem die Möglichkeit geboten, sich bei Call Home anzumelden.

  Wenn eine VDA-Installation fehlschlägt, wird das Protokoll des fehlerhaften MSI von einem Analysetool analysiert und der exakte Fehlercode angezeigt. Das Tool empfiehlt einen CTX-Artikel, wenn es sich um ein bekanntes Problem handelt. Das Tool sammelt außerdem anonymisierte Daten über den Fehlercode. Diese Daten werden anderen, vom CEIP gesammelten Daten beigefügt. Wenn Sie die Registrierung beim CEIP beenden, werden die gesammelten MSI-Analysedaten nicht mehr an Citrix gesendet.

  Informationen zu diesen Programmen finden Sie unter Citrix Insight Services.

- **Citrix Workspace-App:**Die Citrix Workspace-App für Windows wird nicht standardmäßig bei Installation eines VDAs installiert. Sie können die Citrix Workspace-App für Windows und anderen

Citrix Workspace-App-Versionen von der Citrix Website herunterladen und installieren bzw. aktualisieren. Alternativ können Sie diese Citrix Workspace-Apps über den Workspace oder einen StoreFront-Server zur Verfügung stellen.

- **Druckspoolerdienst:** Der Microsoft Druckspoolerdienst muss aktiviert sein. Wenn dieser Dienst deaktiviert ist, können Sie keinen VDA installieren.
- **Microsoft Media Foundation:** Bei den meisten unterstützten Windows-Editionen ist Media Foundation bereits installiert. Wenn Microsoft Media Foundation auf der Maschine, auf der Sie einen VDA installieren, nicht installiert ist (z. B. N-Editionen), werden mehrere Multimediafeatures nicht installiert und sind nicht funktionsfähig.

  - Flash-Umleitung
  - Windows Media-Umleitung
  - HTML5-Videoumleitung
  - HDX RealTime-Webcamumleitung

  Sie können diese Einschränkung bestätigen oder die VDA-Installation beenden und später, nach der Installation von Media Foundation neu beginnen. Diese Auswahl wird bei der grafischen Oberfläche per Meldung angeboten. In der Befehlszeile können Sie zum Bestätigen der Einschränkung die Option `/no_mediafoundation_ack` verwenden.
- **Lokale Benutzergruppe:** Wenn Sie VDA installieren, wird automatisch eine neue lokale Benutzergruppe namens "Benutzer mit direktem Zugriff"erstellt. Auf Einzelsitzungs-OS-VDAs gilt diese Gruppe nur für RDP-Verbindungen. Auf Multisitzungs-OS-VDAs gilt diese Gruppe nur für ICA- und RDP-Verbindungen.
- **Cloud Connector-Adresse:** Der VDA muss mindestens eine gültige Cloud Connector-Adresse (am selben Ressourcenstandort) haben, mit der er kommunizieren kann. Andernfalls können Sitzungen nicht eingerichtet werden. Cloud Connector-Adressen geben Sie bei der Installation des VDA an. Informationen zu anderen Methoden zur Angabe von Cloud Connector-Adressen, bei denen sich VDAs registrieren können, finden Sie unter VDA-Registrierung.
- **Überlegungen zum Betriebssystem:**

  - Informationen zu den unterstützten Betriebssystemen, Plattformen und Versionen finden Sie unter Systemanforderungen.
  - Stellen Sie sicher, dass für jedes Betriebssystem immer die neuesten Updates installiert werden.
  - Stellen Sie sicher, dass die Systemuhren der VDAs synchronisiert sind. Die Kerberos-Infrastruktur, die die Kommunikation zwischen den Maschinen sichert, muss synchronisiert werden.
  - Optimierungsempfehlungen für Windows 10-Maschinen finden Sie unter CTX216252.

  - Wenn Sie versuchen, einen Windows-VDA unter einem für die VDA-Version nicht unterstützten Betriebssystem zu installieren (bzw. ein VDA-Upgrade auszuführen) werden Ihnen durch eine Meldung diverse Optionen präsentiert. Wenn Sie beispielsweise versuchen, den neuesten VDA auf einer Maschine mit einer älteren Windows-Version zu installieren, werden Sie durch eine Meldung zu CTX139030 geführt. Weitere Informationen finden Sie unter Ältere Betriebssysteme.

- **Installierte MSIs:** Mehrere MSIs werden automatisch installiert, wenn Sie einen VDA installieren. Sie können die Installation spezifischer MSIs auf der Seite **Zusätzliche Komponenten** der grafischen Oberfläche oder mit der Option `/exclude` in der CLI verhindern. Die Installation der übrigen MSIs kann nur über die CLI-Option `/exclude` verhindert werden.
- **Domänengebunden:** Stellen Sie vor der Installation der VDA-Software sicher, dass die Maschine in eine Domäne eingebunden ist.

VDA Supportability Tools

Alle VDA-Installationsprogramme enthalten ein Supportability-MSI mit Citrix Tools zum Überprüfen der VDA-Leistung (allgemeiner Zustand, Verbindungsqualität usw.). Die Installation des MSI können Sie auf der Seite **Zusätzliche Komponenten** der grafischen Oberfläche des VDA-Installationsprogramms aktivieren oder deaktivieren. Über die Befehlszeile können Sie die Installation mit der Option `/exclude "Citrix Supportability Tools"` ausschließen.

Standardmäßig wird die MSI des Unterstützungsprogramms in `C:\Program Files (x86)\Citrix\Supportability Tools\` installiert. Sie können den Pfad auf der Seite **Komponenten** der grafischen Oberfläche des VDA-Installationsprogramms oder mit der Befehlszeilenoption `/installdir` ändern. Ein geänderter Pfad gilt für alle installierten VDA-Komponenten und nicht nur für die Supportability Tools.

Aktuelle Tools im Supportability-MSI:

- Citrix Health Assistant: Informationen finden Sie unter CTX207624.
- VDA Cleanup Utility: Informationen finden Sie unter CTX209255.

Wenn Sie die Tools bei der VDA-Installation nicht installieren, finden Sie in dem CTX-Artikel einen Link zum aktuellen Downloadpaket.

Neustarts während der VDA-Installation

Bei der VDA-Installation ist zum Abschluss ein Neustart erforderlich. Das Neustart erfolgt standardmäßig automatisch.

Um während der Installation möglichst wenige weitere Neustarts durchführen zu müssen, führen Sie folgende Schritte aus:

- Stellen Sie vor der VDA-Installation sicher, dass eine unterstützte Microsoft .NET Framework-Version installiert ist.
- Installieren und aktivieren Sie auf Maschinen mit Windows-Multisitzungs-OS vor der VDA-Installation die Rollendienste für Remotedesktopdienste.

Wenn Sie diese Voraussetzungen nicht vor dem VDA installieren:

- Wenn Sie die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle ohne `/noreboot` verwenden, wird die Maschine nach Installation der Voraussetzung automatisch neu gestartet.
- Wenn Sie die Befehlszeilenschnittstelle mit `/noreboot` verwenden, müssen Sie den Neustart selbst ausführen.

Nach jedem Neustart wird die VDA-Installation fortgesetzt. Wenn Sie über die Befehlszeile installieren, können Sie die automatische Wiederaufnahme mit der Option `/noresume` verhindern.

Beim Upgrade auf VDA-Version 7.17 (oder eine spätere unterstützte Version) tritt ein Neustart auf. Dieser Neustart kann nicht vermieden werden.

Wiederherstellung bei Installations- oder Upgradefehler

> **Hinweis:**
>
> Diese Funktion ist nur für Einzelsitzungs-VDAs verfügbar.

Wenn das Installieren oder Aktualisieren eines Einzelsitzungs-VDAs fehlschlägt und das Feature "Wiederherstellung bei Fehler"aktiviert ist, wird die Maschine auf einen zuvor festgelegten Wiederherstellungspunkt zurückgesetzt.

Wenn das Feature beim Start einer Installation oder eines Upgrades für Einzelsitzungs-VDAs aktiviert ist, erstellt das Installationsprogramm zunächst einen Systemwiederherstellungspunkt. Wenn die anschließende VDA-Installation oder das Upgrade fehlschlägt, wird die Maschine in den Zustand des Wiederherstellungspunkts zurückgesetzt. Der Ordner `%temp%/Citrix` enthält Bereitstellungsprotokolle und andere Informationen zur Wiederherstellung.

Standardmäßig ist dieses Feature deaktiviert.

Wenn Sie dieses Feature aktivieren möchten, müssen Sie sicherstellen, dass die Systemwiederherstellung nicht über eine GPO-Einstellung deaktiviert ist (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

Aktivieren des Features beim Installieren oder Aktualisieren eines Einzelsitzungs-VDA:

- Wenn Sie die grafische Benutzeroberfläche eines VDA-Installationsprogramms (z. B. **Autostart** oder den Befehl `XenDesktopVDASetup.exe` ohne Optionen für Wiederherstellung und

stillen Modus) verwenden, aktivieren Sie auf der Seite **Zusammenfassung** das Kontrollkästchen **Wiederherstellung bei Fehler aktivieren**.

Nach dem erfolgreichen Abschluss der Installation oder des Upgrades wird der Wiederherstellungspunkt nicht verwendet, aber beibehalten.

- Führen Sie ein VDA-Installationsprogramm mit der Option `/enablerestore` oder `/enablerestorecleanup` aus.
  - Wenn Sie die Option `/enablerestorecleanup` verwenden, wird der Wiederherstellungspunkt nach dem erfolgreichem Abschluss der Installation oder des Upgrades automatisch entfernt.
  - Wenn Sie die Option `/enablerestore` verwenden, wird der Wiederherstellungspunkt nach dem erfolgreichem Abschluss der Installation oder des Upgrades nicht verwendet, aber beibehalten.

VDA-Installationsprogramme

VDA-Installationsprogramme können direkt von der Citrix Cloud-Konsole heruntergeladen werden.

Standardmäßig werden die selbstextrahierenden Installationsprogramme in den Ordner `Temp` extrahiert. In den Ordner `Temp` extrahierte Dateien werden automatisch gelöscht, wenn die Installation abgeschlossen ist. Alternativ können Sie den Befehl `/extract` mit einem absoluten Pfad verwenden.

Drei eigenständige VDA-Installationsprogramme stehen zum Herunterladen zur Verfügung.

VDAServerSetup.exe Installiert einen Multisitzungs-OS-VDA.

VDAWorkstationSetup.exe Installiert einen Einzelsitzungs-OS-VDA.

VDAWorkstationCoreSetup.exe: Installiert einen Einzelsitzungs-OS-VDA, der für Remote-PC-Zugriff-Bereitstellungen oder Kern-VDI-Installationen optimiert ist. Remote PC Access verwendet physische Maschinen. Kern-VDI-Installationen sind VMs, die nicht als Image verwendet werden. Es werden nur die für VDA-Verbindungen erforderlichen Kerndienste installiert. Daher unterstützt es nur einen Teil der Optionen des Installationsprogramms VDAWorkstationSetup.exe.

Dieses Installationsprogramm für die aktuelle Version installiert oder enthält nicht die Komponenten für:

- App-V.
- Profilverwaltung. Das Ausschließen der Citrix Profilverwaltung bei der Installation hat Auswirkungen auf die Anzeigen der Überwachung.
- Maschinenidentitätsdienst.
- Citrix Workspace-App für Windows

- Citrix Supportability Tools
- Citrix Files für Windows
- Citrix Files für Outlook.
- MCSIO-Schreibcache für Speicheroptimierung.

Dieses Installationsprogramm enthält und installiert keine Citrix Workspace-App für Windows.

Die Browserinhaltsumleitung-MSI wird vom Installationsprogramm automatisch installiert. Die automatische Installation erfolgt in unterstützten VDA-Releases ab Release 2003.

`VDAWorkstationCoreSetup.exe` entspricht dem Installationsprogramm `VDAWorkstationSetup.exe` zum Installieren eines Einzelsitzungs-OS-VDAs und eine der folgenden Optionen:

- Grafische Oberfläche: Auswahl der Option **Remote-PC-Zugriff** auf der Seite **Umgebung**.
- Befehlszeile: Geben Sie die Option `/remotepc` an.
- Befehlszeilenschnittstelle: Angeben von `/components vda` und `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"`.

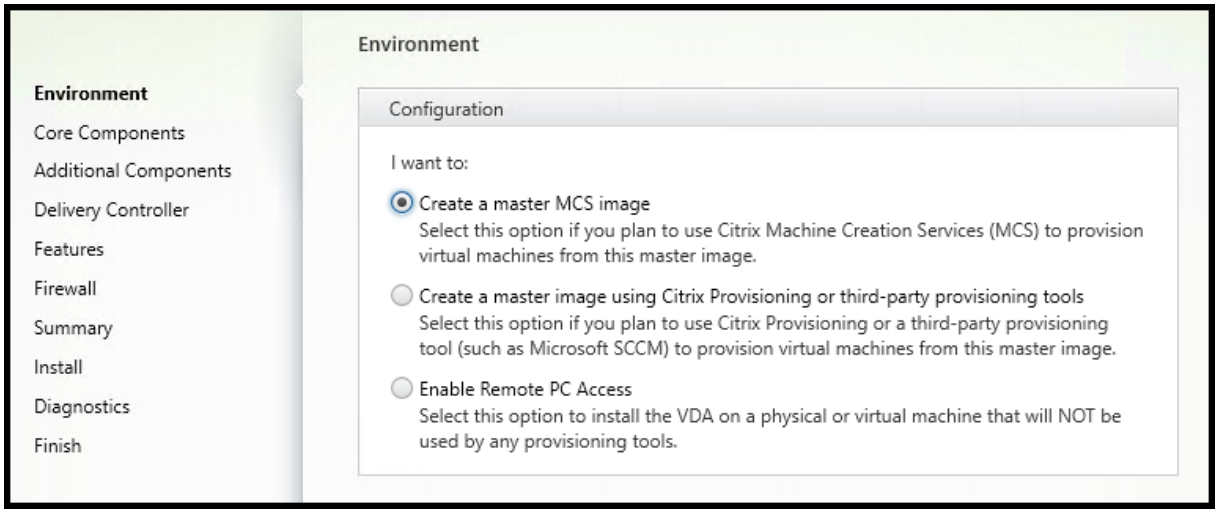
Wenn Sie einen VDA mit dem Installationsprogramm `VDAWorkstationCoreSetup.exe` installieren und später mit dem Installationsprogramm `VDAWorkstationSetup.exe` aktualisieren, können Sie zuvor ausgelassene Komponenten und Features installieren.

Schritt 1: Produktsoftware herunterladen und Assistent starten

1. Melden Sie sich auf der Maschine, auf der Sie den VDA installieren möchten, bei Citrix Cloud an.
2. Wählen Sie im Menü links oben Citrix DaaS in der Liste **Eigene Services** aus.
3. Klicken Sie rechts auf **Downloads** und wählen Sie **Download VDA**. Sie werden auf die VDA-Downloadseite weitergeleitet. Suchen Sie das gewünschte VDA-Installationsprogramm und wählen Sie **Datei herunterladen**.
4. Klicken Sie nach Abschluss des Downloads mit der rechten Maustaste auf die Datei und wählen Sie **Als Administrator ausführen**. Der Installationsassistent wird gestartet.

Alternativ zu den Schritten 1–3 können Sie den VDA auch direkt von der Citrix Downloadseite herunterladen.

Schritt 2: Art der VDA-Verwendung angeben



Geben Sie auf der Seite **Umgebung** an, wie Sie den VDA verwenden werden, und ob Sie die Maschine als Image für das Provisioning von Maschinen verwenden möchten. Je nach gewählter Option werden dann automatisch Citrix Provisioning-Tools installiert (falls notwendig) und die Standardwerte auf der Seite **Zusätzliche Komponenten** im VDA-Installationsprogramm festgelegt.

Wählen Sie eine der folgenden Optionen:

- **MCS-Masterimage erstellen:** Wählen Sie diese Option, um einen VDA auf einem VM-Image zu installieren, wenn Sie Maschinenerstellungsdienste (MCS) für das Provisioning von VMs verwenden. Mit dieser Option wird der Maschinenidentitätsdienst installiert. Dies ist die Standardoption.

  Befehlszeilenoption: `/mastermcsimage` oder `/masterimage`

- **Masterimage mit Citrix Provisioning oder Bereitstellungstools von Drittanbietern erstellen:** Wählen Sie diese Option, um einen VDA auf einem VM-Image zu installieren, wenn Sie Citrix Provisioning oder eine Drittanbieteranwendung (z. B. Microsoft System Center Configuration Manager) verwenden. Verwenden Sie diese Option für zuvor bereitgestellte VMs, die von einem Citrix Provisioning-Lese-/Schreibdatenträger gestartet wurden.

  Befehlszeilenoption: `/masterpvsimage`

- (Wird nur auf Maschinen mit Multisitzungs-OS angezeigt) **Vermittelte Verbindungen zu einem Server aktivieren:** Wählen Sie diese Option, um einen VDA auf einer physischen oder virtuellen Maschine zu installieren, die nicht als Image verwendet werden soll.

  Befehlszeilenoption: `/remotepc`

- (Wird nur auf Maschinen mit Multisitzungs-OS angezeigt.) **Remote-PC-Zugriff aktivieren:** Wählen Sie diese Option, um einen VDA auf einer physischen Maschine zur Verwendung mit Remote-PC-Zugriff zu installieren.

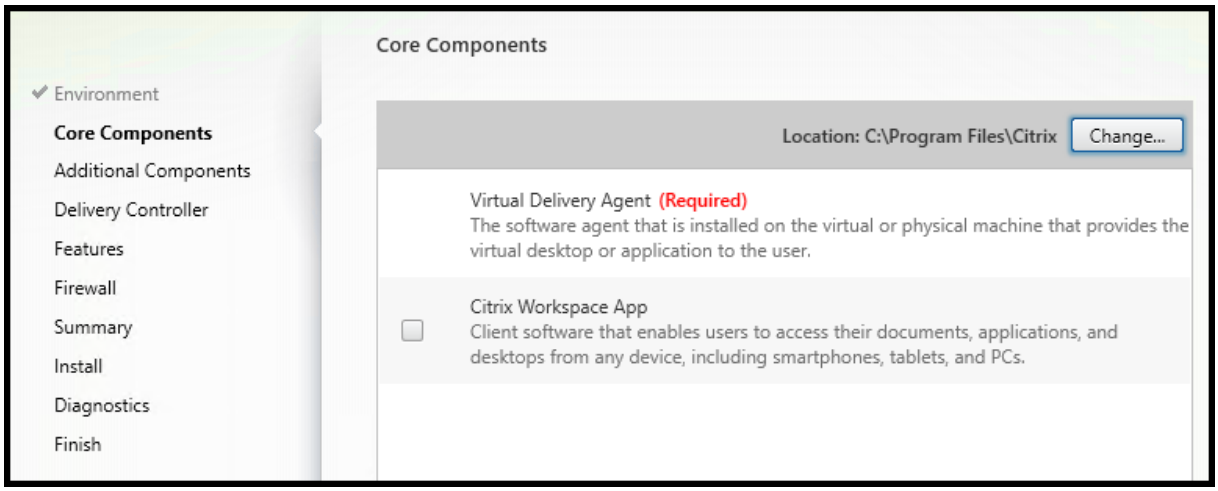
Befehlszeilenoption: `/remotepc`

Wählen Sie **Weiter**.

Die Seite wird in folgenden Fällen nicht angezeigt:

- Beim Upgrade eines VDAs.
- Bei Verwendung des Installationsprogramms `VDAWorkstationCoreSetup.exe`.

Schritt 3: Auswählen der Komponenten und des Speicherorts für die Installation



Treffen Sie auf der Seite **Kernkomponenten** folgende Auswahl:

- **Speicherort:** Standardmäßig werden die Komponenten in `C:\Program Files\Citrix` installiert. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Wenn Sie einen anderen Speicherort während der Installation angeben, muss dieser Speicherort Ausführenberechtigung für den Netzwerkdienst haben.

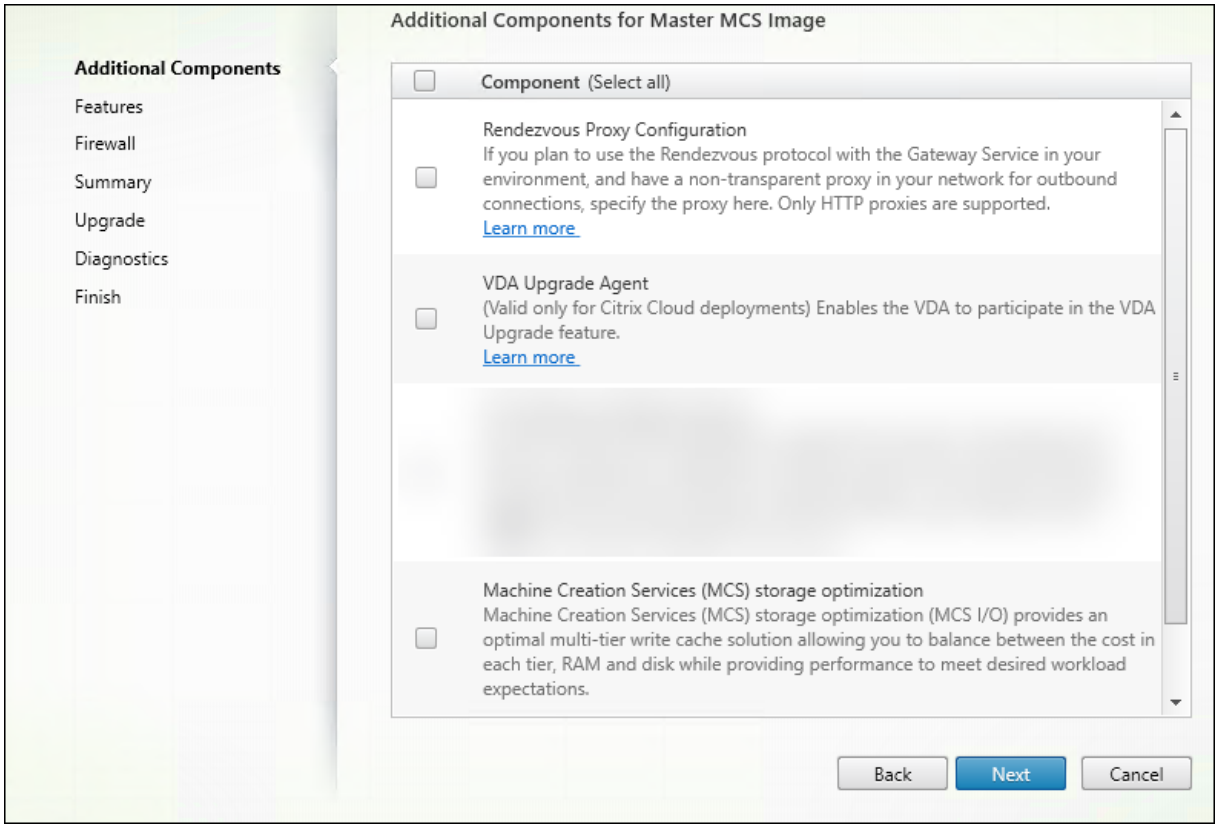
  Befehlszeilenoption: `/installdir`

- **Komponenten:** Standardmäßig wird die Citrix Workspace-App für Windows nicht mit dem VDA installiert. Wenn Sie das Installationsprogramm `VDAWorkstationCoreSetup.exe` verwenden, wird die Citrix Workspace-App für Windows nie installiert, daher wird dieses Kontrollkästchen nicht angezeigt.

  Befehlszeilenoption: `/components vda,plugin` zum Installieren des VDAs und der Citrix Workspace-App für Windows

Wählen Sie **Weiter**.

Schritt 4: Installation zusätzlicher Komponenten



Die Seite **Zusätzliche Komponenten** enthält Kontrollkästchen zum Aktivieren oder Deaktivieren der Installation weiterer Features und Technologien mit dem VDA. Bei einer Befehlszeileninstallation können Sie die Option `/exclude` oder `/includeadditional` verwenden, um Komponenten aus- oder einzuschließen.

In der Tabelle unten werden die Standardeinstellungen der Elemente auf dieser Seite aufgeführt. Die jeweilige Standardeinstellung hängt von der auf der Seite **Umgebung** ausgewählten Option ab.

Seite "Zusätzliche Komponenten"	Seite "Umgebung": "Masterimage mit MCS"oder "Masterimage mit Citrix Provisioning"ausgewählt	Seite "Umgebung": "Vermittelte Verbindungen zu einem Server aktivieren" (Windows-Multisitzungs-OS) oder "Remote-PC-Zugriff" (Windows-Einzelsitzungs-OS) ausgewählt
Citrix Personalisierung für App-V	Nicht ausgewählt	Nicht ausgewählt
Benutzerpersonalisierungslayer	Nicht ausgewählt	Nicht angezeigt, da für diesen Anwendungsfall nicht gültig.

Seite "Zusätzliche Komponenten"	Seite "Umgebung": "Masterimage mit MCS"oder "Masterimage mit Citrix Provisioning"ausgewählt	Seite "Umgebung": "Vermittelte Verbindungen zu einem Server aktivieren" (Windows-Multisitzungs-OS) oder "Remote-PC-Zugriff" (Windows-Einzelsitzungs-OS) ausgewählt
Citrix Supportability Tools	Ausgewählt	Nicht ausgewählt
Citrix Profilverwaltung	Ausgewählt	Nicht ausgewählt
Citrix Profile Management WMI Plug-In	Ausgewählt	Nicht ausgewählt
Citrix VDA Upgrade Agent	Nicht ausgewählt	Nicht ausgewählt
Citrix Backup and Restore	Nicht ausgewählt	Nicht ausgewählt
Citrix Files für Windows	Nicht ausgewählt	Nicht ausgewählt
Citrix Files für Outlook	Nicht ausgewählt	Nicht ausgewählt
MCS-Speicheroptimierung	Nicht ausgewählt	Nicht ausgewählt
Konfiguration des Rendezvousprotokolls	Nicht ausgewählt	Nicht ausgewählt

Die Seite wird in folgenden Fällen nicht angezeigt:

- Sie verwenden das Installationsprogramm `VDAWorkstationCoreSetup.exe`. Außerdem sind die Befehlszeilenoptionen für die zusätzlichen Komponenten mit diesem Installationsprogramm nicht gültig.
- Beim Upgrade eines VDAs, wenn alle zusätzlichen Komponenten bereits installiert sind. Wenn einige zusätzliche Komponenten bereits installiert sind, werden auf der Seite nur die Komponenten angezeigt, die nicht installiert sind.

Die Komponentenliste kann umfassen:

- **Citrix Personalisierung für App-V:** Installieren Sie diese Komponente zur Verwendung von Anwendungen aus Microsoft App-V-Paketen. Einzelheiten finden Sie unter App-V.

  Befehlszeilenoption: `/includeadditional "Citrix Personalization for App-V – VDA"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Personalization for App-V – VDA"`, um die Komponenteninstallation zu verhindern

- **Citrix Benutzerpersonalisierungslayer:** Installiert das MSI für den Benutzerpersonalisierungslayer. Weitere Informationen finden Sie unter Benutzerpersonalisierungslayer.

Diese Komponente wird nur angezeigt, wenn ein VDA auf einer Maschine mit Windows 10-Einzelsitzungs-OS installiert wird.

Befehlszeilenoption: `/includeadditional "User Personalization Layer"`, um die Komponenteninstallation zu aktivieren, `/exclude "User Personalization Layer"`, um die Komponenteninstallation zu verhindern

- **Citrix Supportability Tools:** installiert die MSI mit Citrix Unterstützbarkeitstools.

  Befehlszeilenoption: `/includeadditional "Citrix Supportability Tools"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Supportability Tools"`, um die Komponenteninstallation zu verhindern

- **Citrix Profilverwaltung:** Diese Komponente verwaltet die Einstellungen für Benutzeranpassungen in Benutzerprofilen. Einzelheiten finden Sie unter Profilverwaltung.

  Das Ausschließen der Citrix Profilverwaltung bei der Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs in Citrix Cloud.

  - Auf den Seiten **Benutzerdetails** und **Endpunkte**der **Registerkarte Überwachen** treten Fehler in den Bereichen **Personalisierung** und **Anmeldedauer** auf.
  - Auf den Seiten **Dashboard** und **Trends** werden im Bereich **Durchschnittliche Anmeldedauer** nur Daten für Maschinen angezeigt, auf denen die Profilverwaltung installiert ist.

  Selbst bei Verwendung der Profilverwaltungslösung eines Drittanbieters empfiehlt Citrix, dass Sie die Citrix Profilverwaltung installieren und ausführen. Die Citrix Profilverwaltung muss nicht aktiviert werden.

  Befehlszeilenoption: `/includeadditional "Citrix Profile Management"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Profile Management "`, um die Komponenteninstallation zu verhindern

- **Citrix User Profile Management WMI Plug-In:** Dieses Plug-In stellt Laufzeitinformationen zur Profilverwaltung in WMI-Objekten (Windows Management Instrumentation) bereit, z. B. Profilanbieter, Profiltyp, Größe und Datenträgernutzung. WMI-Objekte stellen Sitzungsinformationen für Citrix Director bereit.

  Befehlszeilenoption: `/includeadditional "Citrix Profile Management WMI Plugin"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Profile Management WMI Plugin"`, um die Komponenteninstallation zu verhindern

- **VDA Upgrade Agent:** Ermöglicht dem VDA die Verwendung des Features VDA-Upgrade (nur für Citrix DaaS-Bereitstellungen anwendbar). Sie können dieses Feature für das Upgrade der VDAs eines Katalogs über die Verwaltungskonsole verwenden, entweder sofort oder zu einem geplanten Zeitpunkt. Wenn dieser Agent nicht installiert ist, können Sie einen VDA aktualisieren, indem Sie das VDA-Installationsprogramm auf der Maschine ausführen.

Befehlszeilenoptionen: `/includeadditional "Citrix VDA Upgrade Agent"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix VDA Upgrade Agent"` um die Komponenteninstallation zu verhindern

- **Citrix Files für Windows:** Mit dieser Komponente können Benutzer eine Verbindung mit ihrem Citrix Files-Konto herstellen. Sie können dann über ein zugeordnetes Laufwerk im Windows-Dateisystem ohne Erfordernis einer vollständigen Synchronisierung ihrer Inhalte mit Citrix Files interagieren.

  Befehlszeilenoptionen: `/includeadditional "Citrix Files for Windows"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Files for Windows"` um die Komponenteninstallation zu verhindern

- **Citrix Files für Outlook:** Mit dieser Komponente können Sie Dateigrößenbeschränkungen umgehen und Ihre Anlagen oder E-Mails sicherer über Citrix Files versenden. Sie können direkt in Ihrer E-Mail eine Anfrage für sicheren Dateiupload bereitstellen. Weitere Informationen finden Sie unter Citrix Files für Outlook.

  Befehlszeilenoptionen: `/includeadditional "Citrix Files for Outlook"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Files for Outlook"` um die Komponenteninstallation zu verhindern

- **Speicheroptimierung für Maschinenerstellungsdienste (MCS):** Installiert den Citrix MCS-E/A-Treiber. Weitere Informationen finden Sie unter Für Hypervisors freigegebener Speicher und Konfigurieren eines Cache für temporäre Daten.

  Befehlszeilenoptionen: `/includeadditional "Citrix MCS IODriver"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix MCS IODriver"` um die Komponenteninstallation zu verhindern

- **Proxykonfiguration:** Installieren Sie diese Komponente, wenn Sie das Rendezvous-Protokoll mit Citrix Gateway Service in Ihrer Umgebung verwenden möchten und in Ihrem Netzwerk einen nicht transparenten Proxy für ausgehende Verbindungen verwenden. Es werden nur HTTP-Proxys unterstützt.

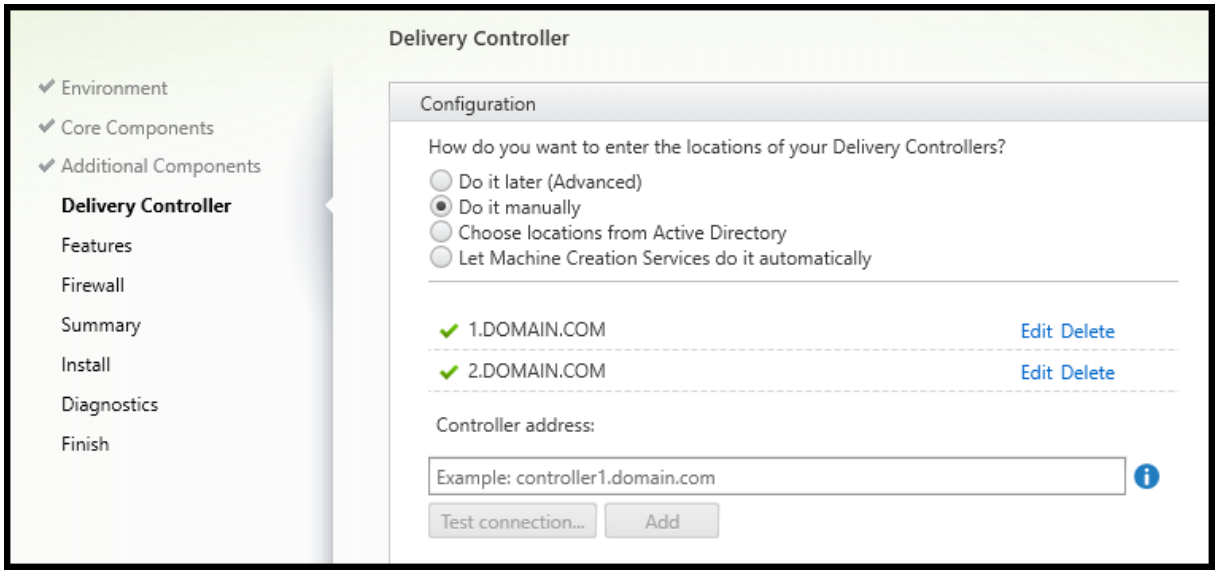
  Wenn Sie diese Komponente installieren, geben Sie auf der Seite **Rendezvousproxykonfiguration** die Proxyadresse oder den Pfad der PAC-Datei an. Einzelheiten zu dem Feature finden Sie unter Rendezvousprotokoll.

  Befehlszeilenoption: `/includeadditional "Citrix Rendezvous V2"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Rendezvous V2"`, um die Komponenteninstallation zu verhindern

- **Citrix Backup and Restore:** Wenn eine VDA-Installation oder ein VDA-Upgrade fehlschlägt, kann diese Komponente die Maschine auf ein vor der Installation bzw. dem Upgrade erstelltes Backup zurücksetzen.

Befehlszeilenoption: `/includeadditional "Citrix Backup and Restore"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Backup and Restore "`, um die Komponenteninstallation zu verhindern.

Schritt 5: Cloud Connector-Adressen



Wählen Sie auf der Seite **Delivery Controller** die Option **Manuell**. Geben Sie den DNS-Namen eines installierten Cloud Connectors ein und wählen Sie **Hinzufügen**. Wenn Sie zusätzliche Cloud Connectors am Ressourcenstandort installiert haben, fügen Sie deren DNS-Namen hinzu.

Wählen Sie **Weiter**.

Überlegungen:

- Die Adresse darf nur alphanumerische Zeichen enthalten.
- Zur VDA-Registrierung müssen außerdem die Firewallports für die Kommunikation mit dem Cloud Connector geöffnet sein. Diese Aktion ist standardmäßig auf der Seite **Firewall** des Assistenten aktiviert.

Befehlszeilenoption: `/controllers`

Schritt 6: Proxykonfiguration

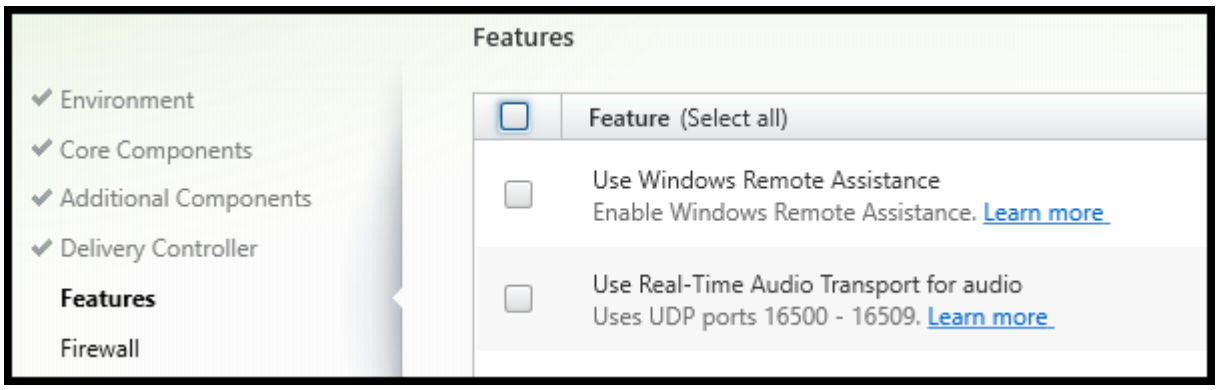
Die Seite **Rendezvousproxykonfiguration** wird nur angezeigt, wenn Sie auf der Seite **Zusätzliche Komponenten** das Kontrollkästchen **Rendezvousproxykonfiguration** aktiviert haben.

1. Wählen Sie aus, ob Sie die Proxyquelle anhand der Proxyadresse oder des PAC-Dateipfads angeben möchten.
2. Geben Sie die Proxyadresse bzw. den PAC-Dateipfad an.
    - Proxy-Adressformat: `http://<url-or-ip>:<port>`
    - PAC-Dateiformat: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

Die Firewall muss für den Proxyport geöffnet sein, damit der Verbindungstest ausgeführt werden kann. Kann keine Verbindung zum Proxy hergestellt werden, können Sie wählen, ob Sie mit der VDA-Installation fortfahren möchten.

Befehlszeilenoption: `/proxyconfig`

Schritt 7: Aktivieren oder Deaktivieren von Features



Verwenden Sie auf der Seite **Features** die Kontrollkästchen, um die Features zu aktivieren oder zu deaktivieren, die Sie verwenden möchten.

- **Windows-Remoteunterstützung verwenden:** Wenn dieses Feature aktiviert ist, wird die Windows-Remoteunterstützung mit dem Feature zum Spiegeln von Benutzern der Komponente Director in Citrix Cloud verwendet. Die Windows-Remoteunterstützung öffnet die dynamischen Ports in der Firewall. (Standard = deaktiviert)

  Befehlszeilenoption: /`enable_remote_assistance`

- **Echtzeitaudioübertragung für Audio verwenden:** Aktivieren Sie dieses Feature, wenn im Netzwerk häufig VoIP verwendet wird. Das Feature verringert die Latenz und verbessert die Audioresilienz in verlustreichen Netzwerken. Es ermöglicht die Datenübertragung mit RTP über UDP. (Standard = deaktiviert)

  Befehlszeilenoption: /`enable_real_time_transport`

- **Bildschirmfreigabe verwenden:** Wenn diese Option aktiviert ist, werden die von der Bildschirmfreigabe verwendeten Ports in der Windows-Firewall geöffnet. (Standard = deaktiviert)

  Befehlszeilenoption: /`enable_ss_ports`

- **Ist dieser VDA auf einer VM in der Cloud installiert:** Mit dieser Einstellung kann Citrix für Telemetriezwecke die korrekten Ressourcenstandorte für VDA-Bereitstellungen entweder on-premises oder als Service (Citrix Cloud) erkennen. Dieses Feature hat keine Auswirkungen auf die kundenseitige Nutzung. Aktivieren Sie diese Einstellung, wenn Ihre Bereitstellung Citrix DaaS verwendet. (Standard = deaktiviert)

  Befehlszeilenoption: /`xendesktopcloud`

Wählen Sie **Weiter**.

Wenn diese Seite das Feature **MCS E/A** enthält, verwenden Sie es nicht. Die MCS-E/A-Feature wird auf der Seite **Zusätzliche Komponenten** konfiguriert.

Schritt 8: Firewallports

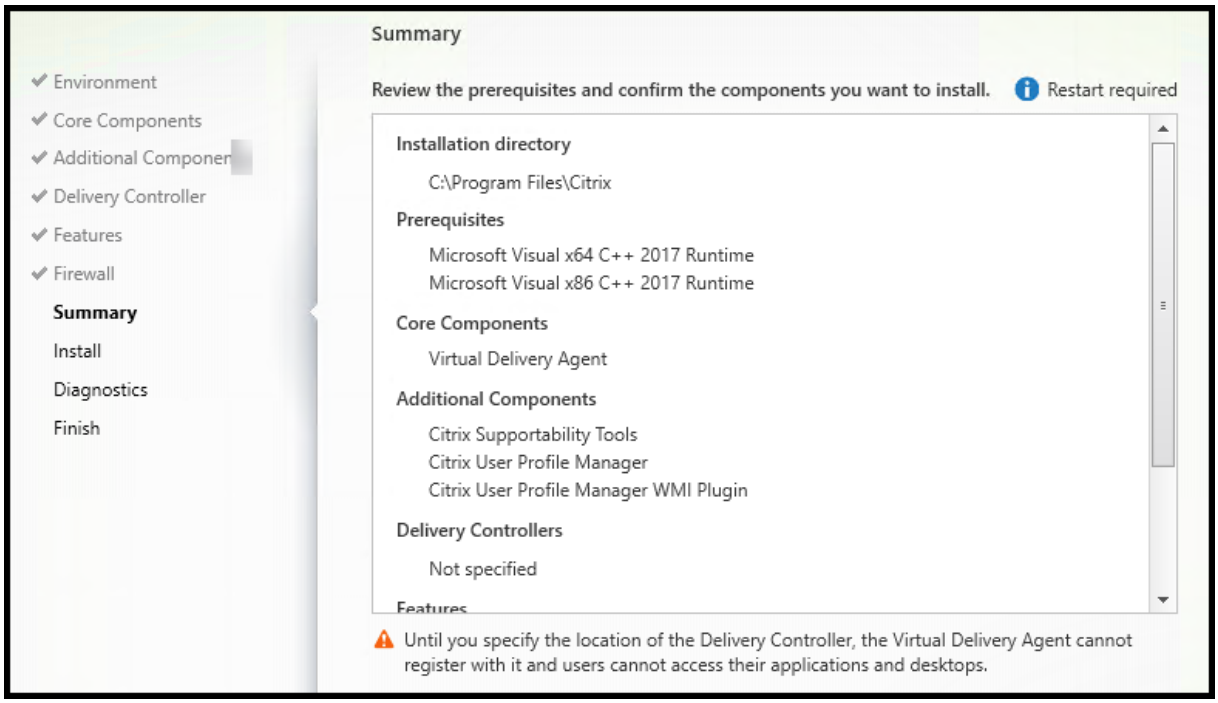
Auf der Seite **Firewall** wird angezeigt, welche Ports für die Kommunikation zwischen VDA und Cloud Connectors verwendet werden. Standardmäßig werden diese Ports automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet.

Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Wählen Sie **Weiter**.

Befehlszeilenoption: `/enable_hdx_ports`

Schritt 9: Überprüfen der Voraussetzungen und Bestätigen der Installation

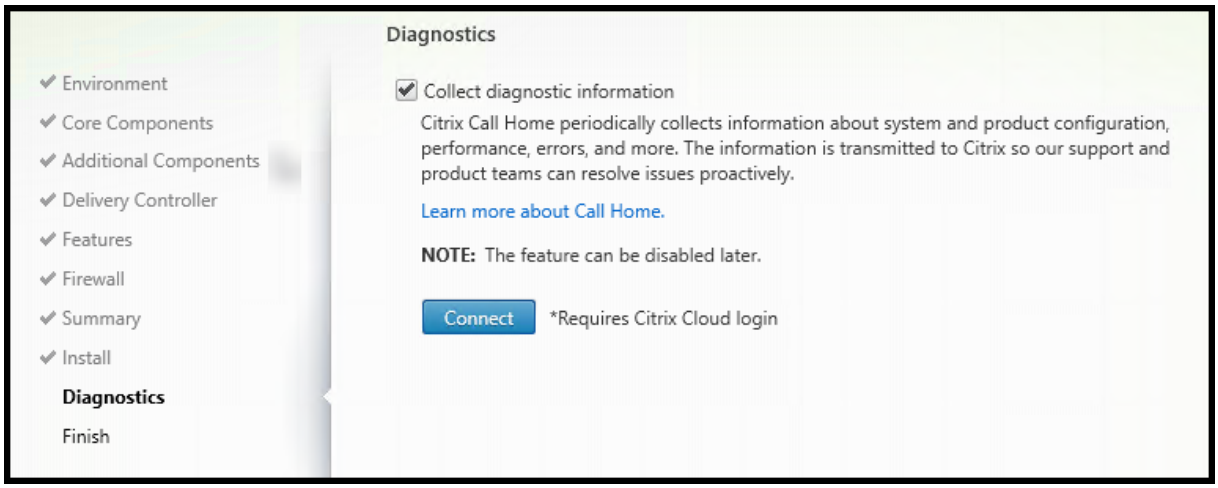


Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können, falls erforderlich, zu früheren Assistentenseiten zurückkehren und die Auswahl ändern.

(Nur für Einzelsitzungs-VDAs) Aktivieren Sie ggf. das Kontrollkästchen **Wiederherstellung bei Fehler aktivieren**. Weitere Informationen finden Sie unter Wiederherstellung bei Installations- oder Upgradefehlern.

Wenn Sie bereit sind, wählen Sie **Installieren**.

Schritt 10: Diagnose

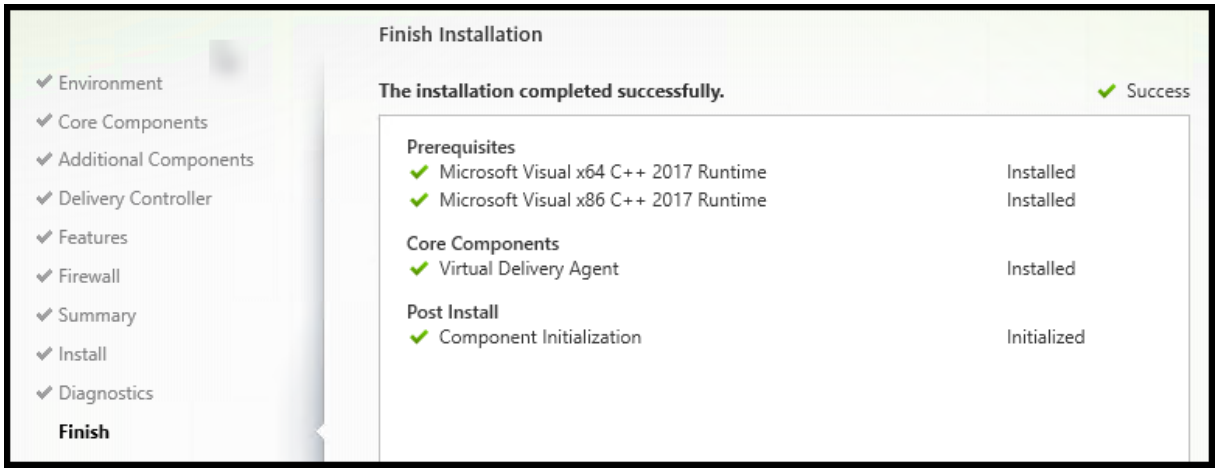


Geben Sie auf der Seite **Diagnose** an, ob Sie bei Citrix Call Home teilnehmen möchten. Wenn Sie teilnehmen möchten (Standardeinstellung), wählen Sie **Verbinden**. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein.

Wenn Ihre Anmeldeinformationen überprüft sind (bzw. wenn Sie nicht teilnehmen), wählen Sie **Weiter**.

Weitere Informationen finden Sie unter Call Home.

Schritt 11: Abschließen der Installation



Die Seite **Fertigstellen** zeigt grüne Häkchen für alle Voraussetzungen und Komponenten, die erfolgreich installiert und initialisiert werden konnten.

Wählen Sie **Fertig stellen**. Standardmäßig wird die Maschine automatisch neu gestartet. Sie können den Neustart zwar deaktivieren, doch kann der VDA dann solange nicht verwendet werden, bis ein Neustart erfolgt.

Wenn Sie den VDA statt auf einem Image auf einzelnen Maschinen installieren, wiederholen Sie die oben genannten Schritte, um nach Bedarf VDAs auf anderen Maschinen zu installieren.

Problembehandlung

In der Anzeige **Verwalten > Vollständige Konfiguration** wird im Bereich "Details"für Bereitstellungsgruppen unter **Installierte VDA-Version** möglicherweise nicht die auf den Maschinen installierte Version angezeigt. In der Maschine wird in Windows unter "Programme und Features"die tatsächliche VDA-Version angezeigt.

Citrix Optimizer

Citrix Optimizer ist ein Tool für Windows-Betriebssysteme, das verschiedene Komponenten entfernt bzw. optimiert und Citrix-Administratoren dadurch das Optimieren von VDAs erleichtert.

Nach der Installation des VDAs und dem letzten Neustart können Sie Citrix Optimizer herunterladen und installieren. Siehe CTX224676. Der CTX-Artikel enthält das Download-Paket sowie Anweisungen zur Installation und Verwendung von Citrix Optimizer.

Anpassen eines VDA

So ändern Sie die Informationen für installierte VDAs

1. Klicken Sie in Windows im Dialogfeld zum Hinzufügen oder Entfernen von Programmen mit der rechten Maustaste auf **Citrix Virtual Delivery Agent** oder **Citrix Remote PC Access/VDI Core Services VDA**. Klicken Sie auf mit der rechten Maustaste und wählen Sie **Ändern**.
2. Wählen Sie **Virtual Delivery Agent-Einstellungen anpassen**.

Wenn das Installationsprogramm gestartet ist, ändern Sie Einstellungen nach Bedarf.

Anpassen des Ports für die Kommunikation mit Cloud Connectors

Sie können den Port, den VDAs für die Kommunikation mit Cloud Connectors verwenden, entsprechend Ihren spezifischen Sicherheitsanforderungen anpassen. Dieses Feature ist nützlich, wenn Ihr Sicherheitsteam das Öffnen des Standardports (Port 80) nicht zulässt oder wenn der Standardport bereits verwendet wird.

Führen Sie die folgenden Schritte aus, um den Port anzupassen:

1. Fügen Sie die Controller-Portnummer auf Citrix Cloud Connectors hinzu.
2. Fügen Sie die VDA-Portnummer auf VDAs hinzu.

Hinzufügen der Controller-Portnummer auf Citrix Cloud Connectors

Gehen Sie zum Citrix Cloud Connector und führen Sie die folgenden beiden PowerShell-Befehle aus:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

Beispiel:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

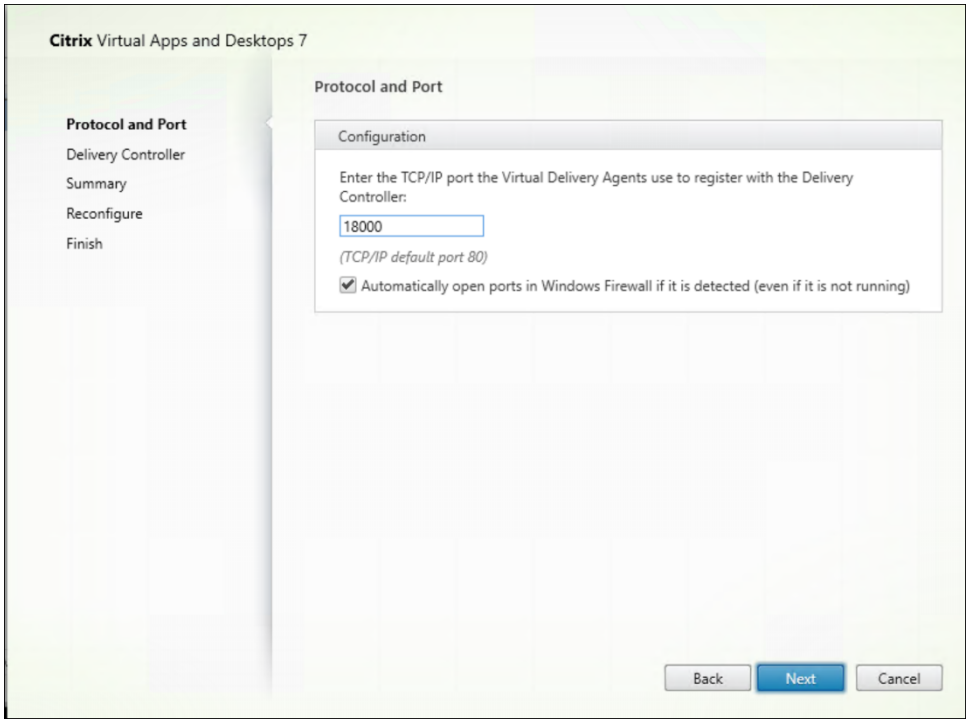
Beachten Sie beim Anpassen des Port Folgendes:

- Sie müssen in beiden Befehlen dieselbe Portnummer verwenden.
- Sie müssen beide Befehle *auf allen Cloud Connectors* ausführen.
- Stellen Sie für eine erfolgreiche Kommunikation mit Cloud Connectors sicher, dass alle VDAs dieselbe Portnummer verwenden.
- Der von Ihnen konfigurierte Port bleibt für alle Connector-Updates bestehen.

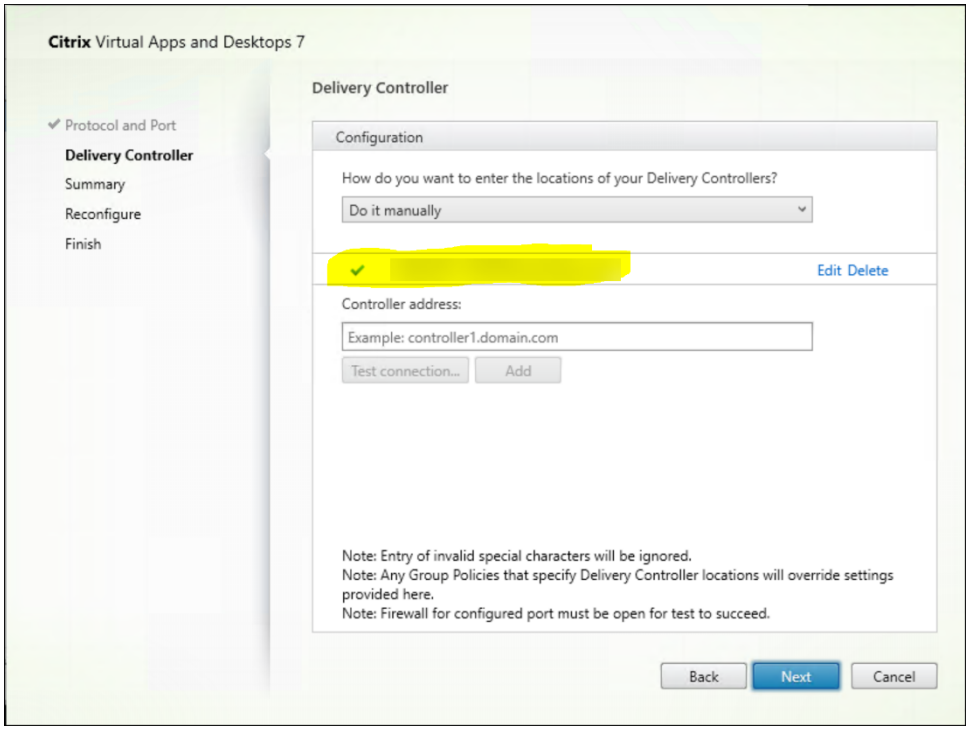
Hinzufügen der VDA-Portnummer auf VDAs

Installieren Sie den VDA mit den Standardeinstellungen und konfigurieren Sie ihn wie folgt. Wenn der VDA bereits installiert ist, fahren Sie mit den folgenden Schritten fort.

1. Öffnen Sie auf dem VDA die Datei **XenDesktopVdaSetup.exe**, die sich unter `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe` befindet.
2. Fügen Sie auf der Seite **Protokoll und Port** die benutzerdefinierte Portnummer hinzu.



3. Geben Sie auf der Seite **Delivery Controller** den FQDN des Controllers ein.



4. Klicken Sie auf **Weiter**, um die folgenden Schritte im Assistenten auszuführen und die Konfiguration abzuschließen.

Die Portnummern sind dann neu konfiguriert.

> **Hinweis:**
>
> Beim Testen einer Controllerverbindung wird möglicherweise die folgende Fehlermeldung angezeigt: Keine ausgeführte Instanz von Controller auf < von Ihnen eingegebene Controlleradresse > gefunden. Wenn die Adresse korrekt ist, können Sie die Nachricht verwerfen.

Problembehandlung

Um zu überprüfen, ob die benutzerdefinierten Ports korrekt konfiguriert sind, gehen Sie zum Cloud Connector und führen Sie die folgenden Schritte zur Problembehandlung aus:

1. Überprüfen Sie, ob die folgenden zwei Registrierungsschlüssel vorhanden sind.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Name: CustomVDAPortNumber
   Typ: REG_DWORD
   Daten: 18000

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Name: CustomVDAPortNumberHA

Typ: REG_DWORD
Daten: 18000

2. Führen Sie den folgenden Befehl aus, um eine TXT-Datei zu erstellen.

   - `netsh http show urlacl > <filepath>.txt`

   Beispiel:

   - `netsh http show urlacl > c:\reservations.txt`

3. Öffnen Sie die TXT-Datei und überprüfen Sie die folgenden vier URLs, um sicherzustellen, dass der richtige Port verwendet wird.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Überprüfen Sie, ob die folgenden zwei Firewallregeln erstellt wurden und die erforderlichen Ports geöffnet sind.

   - Citrix XaXdProxy
   - Citrix Brokerdienst (TCP-Ein)

Weitere Informationen

- Nach Installation eines VDAs können Sie die Integrität und Verfügbarkeit der Site und ihrer Komponenten per Cloud-Integritätsprüfung überprüfen.

So geht es weiter

Erstellen Sie Maschinenkataloge.

Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.

VDAs über die Befehlszeile installieren

June 5, 2023

Einführung

Dieser Artikel gilt für die Installation, das Upgrade und die Anpassung von VDAs (Virtual Delivery Agents) auf Maschinen mit Windows-Betriebssystem.

In diesem Artikel wird die Verwendung von VDA-Installationsbefehlen beschrieben. Bevor Sie mit der Installation beginnen, lesen Sie die Informationen zu Installationsproblemen, Installationsprogrammen und während der Installation erforderlichen Angaben unter Installieren von VDAs.

Installieren eines VDA über die Befehlszeile

Zum Installieren eines VDAs und um den Fortschritt der Befehlsausführung und die Rückgabewerte anzuzeigen, benötigen Sie erhöhte Administratorrechte bzw. müssen die Option **Als Administrator ausführen** verwenden.

1. Melden Sie sich auf der Maschine, auf der Sie den VDA installieren möchten, bei Citrix Cloud an.
2. Wählen Sie im Menü links oben **Eigene Services > DaaS**.
3. Klicken Sie oben rechts auf **Downloads** und wählen Sie **Download VDA**. Sie werden auf die VDA-Downloadseite weitergeleitet. Suchen Sie das gewünschte VDA-Installationsprogramm und klicken Sie auf **Datei herunterladen**.
4. Führen Sie das Programm nach dem Download aus. Verwenden Sie die im vorliegenden Artikel beschriebenen Optionen.
    - Führen Sie für Multisitzungs-OS-VDAs `VDAServerSetup.exe` aus.
    - Führen Sie für Einzelsitzungs-OS-VDAs `VDAWorkstationSetup.exe` aus.
    - Führen Sie für Einzelsitzungs-OS-VDAs mit Core Services `VDAWorkstationCoreSetup.exe` aus.

Verwenden Sie zum Extrahieren der Dateien vor der Installation `/extract` mit dem absoluten Pfad, z. B.: `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` (Das Verzeichnis muss vorhanden sein. Andernfalls schlägt die Extrahierung fehl.) Führen Sie dann separat den entsprechenden Befehl mit den gültigen Optionen aus, die in diesem Artikel aufgeführt sind.

- Für `VDAServerSetup_XXXX.exe` führen Sie `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` aus.
- Für `VDAWorkstationCoreSetup_XXXX.exe` führen Sie `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` aus.

- Für `VDAWorkstationSetup_XXXX.exe` führen Sie `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` aus.

Befehlszeilenoptionen zur VDA-Installation

Die folgenden Optionen sind für einen oder mehrere der folgenden Befehle gültig: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` und `VDAWorkstationCoreSetup.exe`.

- **/components** *component*[,*component*]

  Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte:

  - **VDA:** Virtual Delivery Agent
  - **PLUGINS:** Citrix Workspace-App für Windows

  Zum Installieren des VDAs und der Citrix Workspace-App geben Sie `/components vda,plugins` an.

  Ohne Angabe der Option `plugins` wird nur der VDA installiert (nicht die Citrix Workspace-App).

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Mit dem Installationsprogramm kann die Citrix Workspace-App nicht installiert werden.

- **/controllers** "*controller* [*controller*]…"

  Durch Leerzeichen getrennte FQDNs der Citrix Cloud Connectors, mit denen der VDA kommunizieren kann; von geraden Anführungszeichen umschlossen. Geben Sie nicht sowohl die Option `/site_guid` als auch die Option `/controllers` an.

- **/disableexperiencemetrics**

  Verhindert das automatische Senden der bei Installation, Upgrade oder Deinstallation erfassten Analysedaten an Citrix.

- **/enable_hdx_ports**

  Öffnet die erforderlichen Ports in der Windows-Firewall für den VDA und aktivierte Features (mit Ausnahme von Windows-Remoteunterstützung), wenn die Windows-Firewall erkannt wird (selbst wenn sie nicht aktiviert ist). Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

  Zum Öffnen der UDP-Ports, die der adaptive HDX-Transport verwendet, geben Sie zusätzlich zu `/enable_hdx_ports` die Option `/enable_hdx_udp_ports` an.

- **/enable_hdx_udp_ports**

  Öffnet die für den adaptiven HDX-Transport erforderlichen UDP-Ports in der Windows-Firewall, wenn der Windows-Firewalldienst erkannt wird, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

  Zum Öffnen weiterer Ports für den VDA geben Sie zusätzlich zu `/enable_hdx_udp_ports` die Option `/enable_hdx_ports` an.

- **/enable_real_time_transport**

  Aktiviert oder deaktiviert die Verwendung von UDP für Audiopakete (RealTime Audio Transport für Audio). Das Aktivieren dieses Features kann die Audioleistung verbessern. Verwenden Sie die Option `/enable_hdx_ports`, wenn Sie möchten, dass die UDP-Ports automatisch bei Erkennung des Windows-Firewalldiensts geöffnet werden.

- **/enable_remote_assistance**

  Aktiviert das Spiegelungsfeature in der Microsoft-Remoteunterstützung für die Verwendung mit den Funktionen unter **Überwachen**. Wenn Sie diese Option angeben, öffnet die Windows-Remoteunterstützung die dynamischen Ports in der Firewall.

- **/enablerestore** oder **/enablerestorecleanup**

  (Gilt nur für Einzelsitzungs-VDAs) Ermöglicht die automatische Rückkehr zum Wiederherstellungspunkt, wenn die VDA-Installation oder das Upgrade fehlschlägt.

  Beim erfolgreichen Abschluss von Installation oder Upgrade:

  - `/enablerestorecleanup` weist an, dass der Wiederherstellungspunkt entfernt wird.
  - `/enablerestore` weist an, dass der nicht genutzte Wiederherstellungspunkt beibehalten wird.

  Weitere Informationen finden Sie unter Wiederherstellung bei Installations- oder Upgradefehlern.

- **/enable_ss_ports**

  Öffnet, wenn der Windows-Firewalldienst erkannt wird, die für die Bildschirmfreigabe erforderlichen Ports in der Windows-Firewall, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden.

- **/exclude** "*component*"[,"*component*"]

  Verhindert die Installation der jeweils in geraden Anführungszeichen angegebenen (durch Kommas getrennten) optionalen Komponenten. Beispiel: Installieren oder Aktualisieren eines VDAs auf einem mit MCS verwalteten Image erfordert die Maschinenidentitätsdienst-Komponente. Gültige Werte:

  - Maschinenidentitätsdienst
  - Citrix Profilverwaltung
  - Citrix Profile Management WMI Plug-In
  - Citrix Personalisierung für App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS-E/A-Treiber
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2

  Das Ausschließen der Citrix Profilverwaltung bei der Installation (`/exclude "Citrix Profile Management"`) hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs über die Registerkarte **Überwachen**. Auf den Seiten **Benutzerdetails** und **Endpunkt** treten Fehler in den Bereichen "Personalisierung"und "Anmeldedauer"auf. Auf den Seiten **Dashboard** und **Trends** werden im Bereich "Durchschnittliche Anmeldedauer"nur Daten für Maschinen angezeigt, auf denen Profilverwaltung installiert ist.

  Selbst bei Verwendung der Profilverwaltungslösung eines Drittanbieters empfiehlt Citrix, dass Sie die Citrix Profilverwaltung installieren und ausführen. Die Citrix Profilverwaltung muss nicht aktiviert werden.

  Wenn Sie MCS zum Bereitstellen von VMs verwenden möchten, schließen Sie den Maschinenidentitätsdienst nicht aus.

  Wenn Sie sowohl `/exclude` als auch `/includeadditional` mit demselben Komponentennamen angeben, wird diese Komponente nicht installiert.

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Das Installationsprogramm schließt viele dieser Elemente automatisch aus.

- **/h** oder **/help**

  Zeigt die Hilfe für Befehle an.

- **/includeadditional** "*component*"[,"*component*"] …

  Bewirkt die Installation der jeweils in geraden Anführungszeichen angegebenen (durch Kommas getrennten) optionalen Komponenten. Bei Komponentennamen muss die Groß- und Kleinschreibung beachtet werden.

  Die Option kann hilfreich sein, wenn Sie eine Remote-PC-Zugriff-Bereitstellung erstellen und Komponenten installieren möchten, die standardmäßig nicht enthalten sind. Gültige Werte:

  - Citrix Profilverwaltung
  - Citrix Profile Management WMI Plug-In
  - Citrix Personalisierung für App-V - VDA

  - Citrix Supportability Tools
  - Citrix MCS-E/A-Treiber
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2
  - Benutzerpersonalisierungslayer
  - Citrix Web Socket VDA-Registrierungstool

  Wenn Sie sowohl /`exclude` als auch /`includeadditional` mit demselben Komponentennamen angeben, wird diese Komponente nicht installiert.

- **/installdir** *directory*

  Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standard: C:\Programme\Citrix

- **/install_mcsio_driver**

  Nicht verwenden. Verwenden Sie stattdessen /`includeadditional "Citrix MCS IODriver"` oder /`exclude "Citrix MCS IODriver"`.

- **/logpath** *path*

  Speicherort der Protokolldateien. Der angegebene Ordner muss vorhanden sein. Er wird von dem Installationsprogramm nicht erstellt. Standard = "%TEMP%\Citrix\XenDesktop Installer"

  Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

- **/masterimage**

  Gilt nur für die Installation von VDAs auf einer VM. Richtet den VDA als Image ein. Diese Option entspricht /`mastermcsimage`.

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden.

- **/mastermcsimage**

  Gibt an, dass die Maschine als Image zum Provisioning mit MCS verwendet wird. Diese Option entspricht /`masterimage`.

- **/masterpvsimage**

  Gibt an, dass die Maschine als Image und Citrix Provisioning oder das Tool eines Fremdherstellers (z. B. Microsoft System Center Configuration Manager) verwendet wird.

- **/no_mediafoundation_ack**

  Bestätigt, dass Microsoft Media Foundation nicht installiert ist und mehrere HDX-Multimediafeatures nicht installiert werden und nicht funktionieren. Wenn diese Option ausgelassen wird und Media Foundation nicht installiert ist, schlägt die VDA-Installation fehl. Bei den meisten

unterstützten Windows-Editionen ist Media Foundation bereits installiert. Eine Ausnahme bilden die N-Editionen.

- **/nodesktopexperience**

  Gilt nur für die Installation von Multisitzungs-OS-VDAs. Verhindert das Aktivieren der Enhanced Desktop Experience. Dieses Feature wird auch über die Citrix Richtlinieneinstellung Enhanced Desktop Experience gesteuert.

- **/noreboot**

  Verhindert einen Neustart nach der Installation. Der VDA kann erst nach einem Neustart verwendet werden.

- **/noresume**

  Wenn während einer Installation ein Maschinenneustart erforderlich ist, wird das Installationsprogramm automatisch fortgesetzt, sobald der Neustart abgeschlossen ist. Um den Standardwert zu überschreiben, geben Sie `/noresume` an. Dies kann hilfreich sein, wenn Sie das Medium neu laden müssen oder während einer automatischen Installation Informationen erfassen möchten.

- **/portnumber** *port*

  Gilt nur, wenn die Option `/reconfig` angegeben wurde. Portnummer für die Kommunikation zwischen VDA und dem Controller. Der zuvor konfigurierte Port wird deaktiviert, es sei denn, es handelt sich um Port 80.

- **/proxyconfig** "*Adresse oder PAC-Dateipfad*"

  Nur gültig, wenn der Befehl `/includeadditional "Citrix Rendezvous V2"` enthält. Die Adresse oder der PAC-Dateipfad des Proxys zur Verwendung mit Rendezvous. Einzelheiten zu dem Feature finden Sie unter Rendezvousprotokoll.

  - Proxy-Adressformat: `http://<url-or-ip>:<port>`
  - PAC-Dateiformat: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** oder **/passive**

  Während der Installation wird keine Benutzeroberfläche angezeigt. Der einzige Hinweis auf den Installations- und Konfigurationsvorgang ist im Windows Task-Manager. Wenn diese Option ausgelassen wird, wird die grafische Oberfläche gestartet.

- **/reconfigure**

  Passt die zuvor konfigurierten VDA-Einstellungen an, wenn der Befehl mit den Optionen `/portnumber`, `/controllers` oder `/enable_hdx_ports` verwendet wird. Wenn Sie diese Option ohne die Option `/quiet` angeben, wird die grafische Oberfläche zum Anpassen von VDA gestartet.

- **/remotepc**

  Gilt nur für Remote-PC-Zugriff-Bereitstellungen (Einzelsitzungs-OS) oder vermittelte Verbindungen (Multisitzungs-OS).

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Das Installationsprogramm schließt diese Komponenten automatisch aus.

- **/remove_appdisk_ack**

  Autorisiert den VDA-Installer, das AppDisks VDA-Plug-In, sofern installiert, zu deinstallieren.

- **/remove_pvd_ack**

  Autorisiert den VDA-Installer, Personal vDisk, sofern installiert, zu deinstallieren.

- **/remove**

  Entfernt die mit `/components` angegebenen Komponenten.

- **/removeall**

  Entfernt den VDA. Ist die Citrix Workspace App installiert, wird sie nicht entfernt.

- **/sendexperiencemetrics**

  Sendet automatisch bei Installation, Upgrade oder Deinstallation erfasste Analysedaten an Citrix. Wenn diese Option ausgelassen wird (oder die Option `/disableexperiencemetrics` angegeben wird), werden Analysedaten lokal erfasst, aber nicht automatisch gesendet.

- **/servervdi**

  Installiert einen Einzelsitzungs-OS-VDA auf einem unterstützten Windows-Server. Lassen Sie diese Option aus, wenn Sie einen Multisitzungs-OS-VDA auf einem Windows-Server installieren. Lesen Sie vor dem Verwenden dieser Option Server-VDI.

- **/site_guid** *guid*

  GUID (Globally Unique Identifier) der Website Active Directory Organisationseinheit (OU). Dabei wird ein virtueller Desktop einer Site zugeordnet, wenn Active Directory für die Discovery verwendet wird (das Feature für automatische Updates ist die empfohlene und Discovery-Standardmethode). Die Site-GUID ist eine Site-Eigenschaft, die unter **Verwalten > Vollständige Konfiguration** angezeigt wird. Geben Sie nicht sowohl die Option `/site_guid` als auch die Option `/controllers` an.

- **/tempdir** *directory*

  Das Verzeichnis für die temporären Dateien während der Installation. Standard = C:\Windows\Temp.

  Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

- **/virtualmachine**

Gilt nur für die Installation von VDAs auf einer VM. Überschreibt das Erkennen einer physischen Maschine durch den Installer. Dabei werden BIOS-Informationen an die VMs weitergegeben, sodass sie als physische Maschinen erscheinen.

Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

- **/xendesktopcloud**

  Zeigt an, dass der VDA in Citrix DaaS (Citrix Cloud) installiert ist.

Beispiele: Installieren eines VDAs

- **VDA unter einem Multisitzungs-OS installieren.** Mit dem folgenden Befehl wird ein VDA unter einem Multisitzungs-OS installiert.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  Der VDA wird als Image verwendet.

- **Multisitzungs-OS-VDA oder Einzelsitzungs-OS-VDA installieren.** Mit dem folgenden Befehl wird ein Multisitzungs-OS-VDA oder Einzelsitzungs-OS-VDA installiert.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com",
  "ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /
  enable_real_time_transport /enable_ss_ports /noreboot
  ```

  Trennen Sie die einzelnen Delivery Controller-FQDN durch Kommas. `XXXX` steht für die VDA-Version.

- **Kernkomponenten-VDA unter Einzelsitzungs-OS-Betriebssystem installieren.** Mit dem folgenden Befehl wird ein Kernkomponenten-VDA unter einem Einzelsitzungs-OS zur Verwendung in einer Remote-PC-Zugriff- oder VDA-Bereitstellung installiert.

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
  domain.com"/enable_hdx_ports /noreboot
  ```

  Die Citrix Workspace-App und andere, nicht zu den Kernkomponenten gehörenden Dienste werden nicht installiert. Die Adresse eines Cloud Connectors wird automatisch angegeben und die Ports der Windows-Firewall werden automatisch geöffnet. Der Administrator steuert die Neustarts.

Anpassen eines VDAs über die Befehlszeile

Nachdem VDA installiert wurde, können Sie einige Einstellungen anpassen. Führen Sie `XenDesktopVDASetup.exe` aus und legen Sie dabei eine oder mehrere der folgenden Optionen fest:

- /reconfigure (zum Anpassen des VDAs erforderlich)
- /h oder /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

So geht es weiter

- Maschinenkataloge erstellen
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.

Verbindungen und Ressourcen erstellen und verwalten

February 22, 2024

Einführung

Beim Konfigurieren einer Verbindung wählen Sie den Typ der Verbindung aus der Liste unterstützter Hypervisors und Clouddienste sowie die gewünschte Sprache und die Netzwerkressourcen für diese Verbindung aus.

> **Hinweis:**
>
> Sie benötigen volle Administratorrechte, um Aufgaben im Zusammenhang mit der Verbindungs- und Ressourcenverwaltung ausführen zu können.

Informationen zu Verbindungstypen

Die Systemanforderungen enthalten eine Liste der unterstützten Hypervisors und Clouddienstversionen sowie Links zu Artikeln für jeden spezifischen Host.

Hostspeicher

Speicherprodukte werden unterstützt, wenn sie von einem unterstützten Hypervisor verwaltet werden. Citrix Support unterstützt nur die Anbieter solcher Speicherprodukte bei der Problembehandlung und -lösung und dokumentiert diese Probleme und Lösungen bei Bedarf im Knowledge Center.

Beim Provisioning von Maschinen werden die Daten nach Typ klassifiziert:

- Betriebssystem (OS): beinhaltet Images
- Temporäre Daten beinhalten alle nicht persistenten Daten, die auf mit MCS bereitgestellten Maschinen geschrieben werden, Windows-Seitendateien und alle Daten, die mit ShareFile synchronisiert werden. Diese Daten werden beim Neustart einer Maschine verworfen. Wenn das Basisimage Benutzerprofildaten enthält, bleiben diese Daten persistent. Wenn eine zentralisierte Benutzerprofillösung verwendet wird, werden die Benutzerprofildaten mit dem externen Profilspeicher synchronisiert. Die lokal zwischengespeicherten Benutzerprofildaten werden bei jedem Computerneustart verworfen.

Die Zuweisung unterschiedlicher Speicherressourcen für verschiedene Datentypen kann die Systemlast minimieren und die IOPS-Leistung (Input/Output Operations Per Second) auf jedem Speichergerät verbessern. Diese strategische Zuteilung nutzt die verfügbaren Ressourcen des Hosts optimal. Außerdem ermöglicht sie die Auswahl des am besten geeigneten Speichermediums auf der Grundlage der spezifischen Anforderungen jedes Datentyps, z. B. eine höhere Persistenz oder Resilienz für bestimmte Arten von Daten.

- Optionen für gemeinsamen und lokalen Speicher: Speicherressourcen können entweder zentralisiert, d. h. getrennt von jedem Host und von allen Hosts verwendet werden, oder auf einen bestimmten Hypervisor lokalisiert werden. Zu den zentralisierten Optionen gehören gemeinsam genutzte Windows-Cluster-Volumes, die möglicherweise über zusätzlichen angeschlossenen Speicher verfügen, oder Appliances von Speicheranbietern. Zentralisierte Speicherlösungen bieten möglicherweise erweiterte Funktionen für Optimierungen, z. B. Hypervisor-spezifische Speichersteuerungspfade und direkten Plug-In-Zugriff.
- Vorteile und Nachteile des lokalen Speichers: Durch das lokale Speichern temporärer Daten wird vermieden, dass der Zugriff auf gemeinsam genutzten Speicher über das Netzwerk erfolgt, wodurch die IOPS-Belastung der gemeinsam genutzten Ressourcen reduziert wird. Zentraler Speicher kann teurer sein, daher ist die Verwendung von lokalem Speicher eine kostengünstige Alternative. Diese Vorteile müssen gegen die Verfügbarkeit von genügend Speicher auf den Hypervisorservern abgewogen werden.

Für Hypervisors freigegebener Speicher

Bei für Hypervisors freigegebenem Speicher werden Daten, die länger erhalten bleiben sollen, zentral gespeichert und bieten zentrale Backup- und Verwaltungsmöglichkeiten. Dieser Speicher enthält die Betriebssystemdatenträger.

Bei dieser Methode können Sie wählen, ob Sie lokalen Speicher (auf Servern im gleichen Hypervisorpool) für temporäre Daten verwenden. Diese Daten erfordern keine Persistenz und weniger Resilienz als Daten im freigegebenen Speicher. Dies ist der *temporäre Datencache*. Der lokale Datenträger reduziert den Datenverkehr zum Hauptbetriebssystemspeicher. Dieser Datenträger wird nach dem Neustart einer Maschine gelöscht. Auf den Datenträger wird über einen Write-through-Speichercache zugegriffen. Wenn Sie lokalen Speicher für temporäre Daten verwenden, ist der bereitgestellte VDA an einen bestimmten Hypervisorhost gebunden. Wenn der Host ausfällt, kann die VM nicht gestartet werden.

Ausnahme: Wenn Sie geclusterte Speichervolumes (CSV) verwenden, gestattet Microsoft System Center Virtual Machine Manager nicht, dass temporäre Datenträgercaches auf dem lokalen Speicher erstellt werden.

Wenn Sie temporäre Daten lokal speichern, können Sie benutzerdefinierte Werte für die Größe des Cachedatenträgers und des Speichers jeder VM aktivieren und konfigurieren, wenn Sie einen Maschinenkatalog erstellen, der diese Verbindung verwendet. Die Standardwerte sind jedoch auf den Verbindungstyp zugeschnitten und in den meisten Fällen ausreichend.

Der Hypervisor kann auch Optimierungstechnologien über In-Memory-Lese-Caching der Datenträgerimages bieten. XenServer bietet beispielsweise IntelliCache. Dies kann auch den Netzwerkdatenverkehr zum zentralen Speicher reduzieren.

Lokaler Speicher auf dem Hypervisor

Bei der Methode mit lokalem Speicher auf dem Hypervisor werden Daten lokal auf dem Hypervisor gespeichert. Images und andere Betriebssystemdaten werden dann an alle Hypervisors in der Site übermittelt, sowohl bei der anfänglichen Maschinenerstellung als auch bei zukünftigen Imageupdates. Dies führt zu intensivem Datenverkehr auf dem Verwaltungsnetzwerk. Imageübertragungen sind zeitaufwändig und die Images werden jedem Host zu einem anderen Zeitpunkt zur Verfügung gestellt.

Erstellen einer Verbindung und von Ressourcen

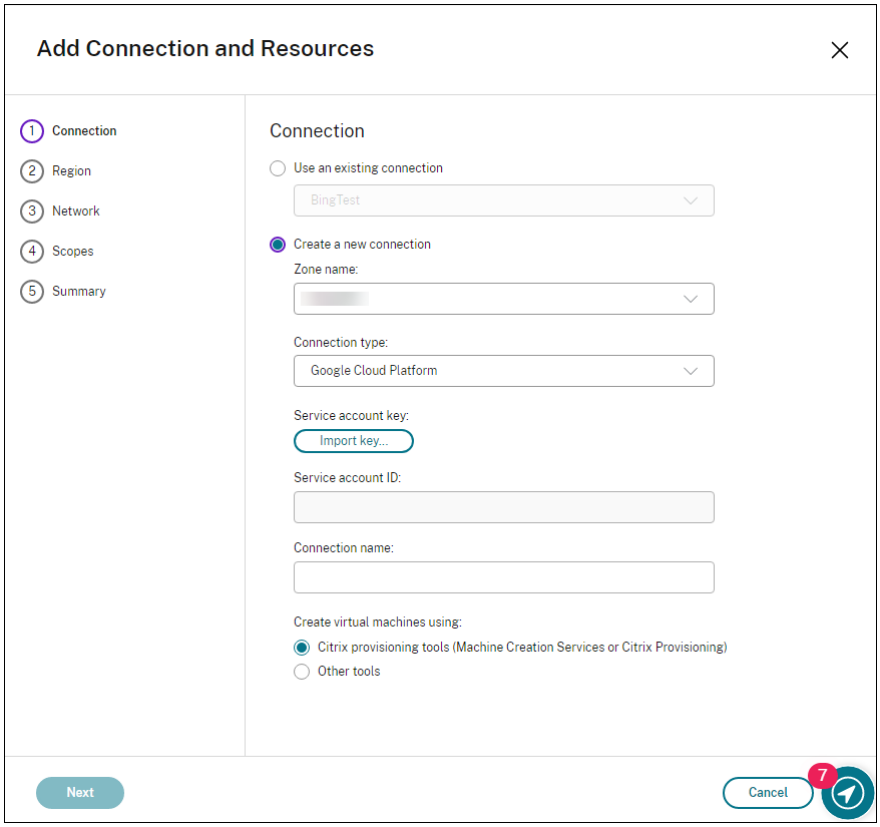
> **Wichtig:**
>
> Die Hostressourcen (Speicher und Netzwerk) am Ressourcenstandort müssen verfügbar sein,

> bevor Sie eine Verbindung erstellen.

1. Melden Sie sich bei Citrix Cloud an.
2. Navigieren Sie zum Menü oben links und wählen Sie **Meine Services > DaaS** aus.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste die Option **Verbindungen und Ressourcen hinzufügen**.
5. Der Assistent führt Sie durch den in den folgenden Schritten beschriebenen Konfigurationsprozess. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **Weiter**, bis Sie zur letzten Seite **Zusammenfassung** gelangen.

> **Hinweis:**
>
> Der Inhalt der einzelnen Seiten im Assistenten hängt von der Art der Verbindung ab, die Sie ausgewählt haben.

Schritt 1: Verbindung



Auf der Seite **Verbindung**:

- Um eine neue Verbindung zu erstellen, wählen Sie **Neue Verbindung erstellen**. Um eine Verbindung zu erstellen, die auf derselben Hostkonfiguration wie eine bestehende

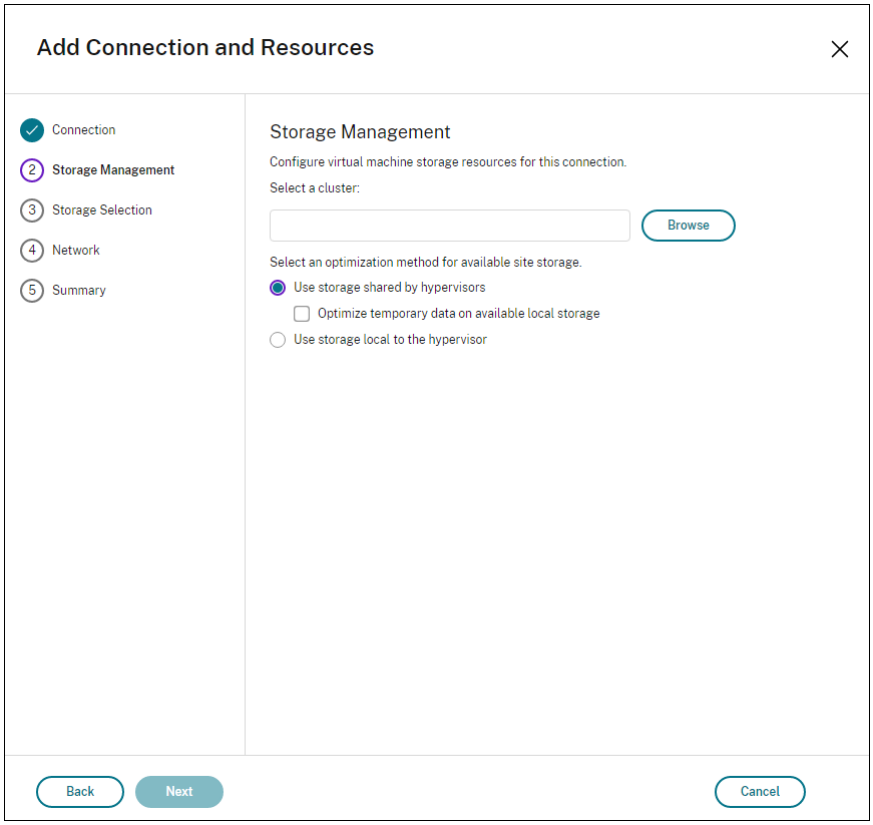
Verbindung basiert, klicken Sie auf **Vorhandene Verbindung verwenden** und wählen dann die entsprechende Verbindung.

- Wählen Sie im Feld **Zonenname** eine Zone. Die Optionen sind alle von Ihnen konfigurierten Ressourcenstandorte.
- Wählen Sie im Feld **Verbindungstyp** den Hypervisor oder Clouddienst. Die Optionen umfassen alle von Citrix unterstützten Hypervisors und Clouddienste:
  - Für einen Ressourcenstandort ohne Zugriff auf Cloud Connectors sind nur Hypervisors und Clouddienste verfügbar, die Bereitstellungen ohne Connector unterstützen.
  - Für einen Ressourcenstandort mit Zugriff auf Cloud Connectors sind nur Hypervisors und Clouddienste verfügbar, deren Plug-Ins ordnungsgemäß auf den Connectors installiert sind.

  Alternativ können Sie mit dem PowerShell-Befehl `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` (false oder true) die Liste der verfügbaren Hypervisors und Clouddienste abrufen.
- Geben Sie einen Verbindungsnamen ein. Dieser Name wird in **Hosting** angezeigt.
- Wählen Sie ein Tool zum Erstellen virtueller Maschinen aus.

> **Hinweis:**
>
> Die Informationen auf der Seite **Verbindung** variieren je nach verwendetem Host (Verbindungstyp). Wenn Sie beispielsweise Azure Resource Manager verwenden, können Sie einen vorhandenen Dienstprinzipal verwenden oder einen neuen erstellen. Einzelheiten finden Sie unter Verbindung zu Microsoft Azure.

Schritt 2: Speicherverwaltung



Informationen zur Speicherverwaltungstypen und -methoden finden Sie unter Hostspeicher.

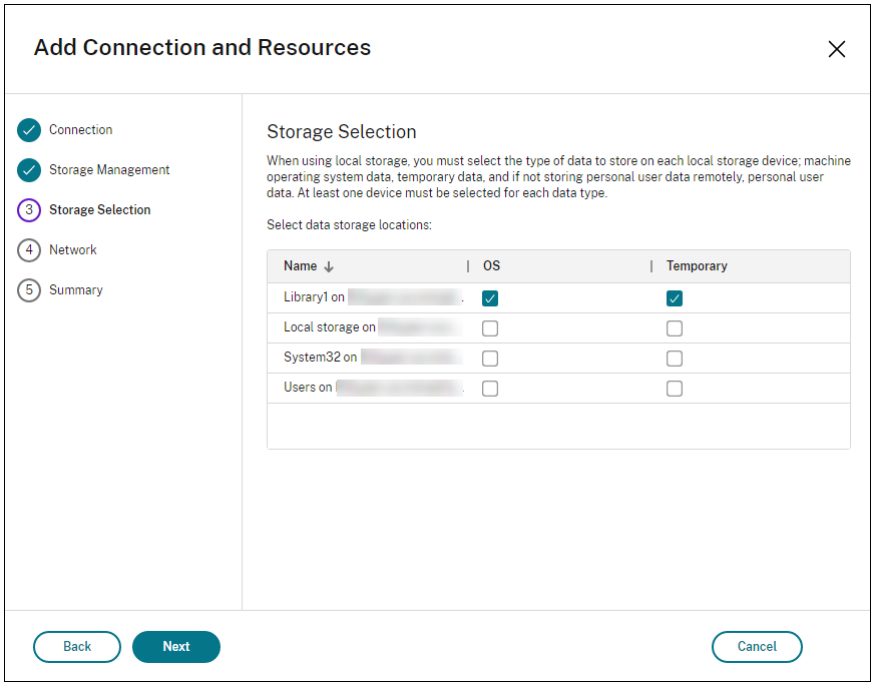
Wenn Sie eine Verbindung zu einem Hyper-V- oder VMware-Host konfigurieren, navigieren Sie zu einem Clusternamen und wählen Sie ihn aus. Andere Verbindungstypen erfordern keine Clusternamen.

Wählen Sie eine Speicherverwaltungsmethode: für Hypervisors freigegebener Speicher oder lokaler Speicher auf dem Hypervisor.

Weitere Informationen finden Sie unter Von Hypervisors gemeinsam genutzter Speicher und Lokaler Speicher für den Hypervisor.

Wenn Sie freigegebenen Speicher auf einem XenServer-Pool verwenden, geben Sie an, ob Sie IntelliCache zum Reduzieren der Last auf dem freigegebenen Speichergerät verwenden. Weitere Informationen finden Sie unter Verwenden von IntelliCache für XenServer-Verbindungen.

Schritt 3: Speicherauswahl



Weitere Informationen zur Speicherauswahl finden Sie unter Hostspeicher.

Wählen Sie mindestens ein Hostspeichergerät für jeden verfügbaren Datentyp. Die auf der vorherigen Seite ausgewählte Speicherverwaltungsmethode bestimmt, welche Datentypen Sie auf dieser Seite auswählen können. Wählen Sie mindestens ein Speichergerät für jeden unterstützten Datentyp, bevor Sie mit der nächsten Seite im Assistenten fortfahren.

Weitere Konfigurationsoptionen finden Sie auf der Seite **Speicherauswahl**, wenn Sie **Für Hypervisors freigegebener Speicher verwenden** aktivieren und auf der Seite **Speicherverwaltung** die Option **Temporäre Daten in verfügbarem lokalem Speicher optimieren** auswählen. Sie können die lokalen Speichergeräte (im gleichen Hypervisorpool) für temporäre Daten auswählen.

Die Anzahl der zurzeit ausgewählten Speichergeräte wird angezeigt (siehe Abbildung: “1 Speichergerät ausgewählt”). Wenn Sie mit dem Mauszeiger darauf zeigen, werden die Namen der ausgewählten Geräte angezeigt, es sei denn, es sind keine Geräte konfiguriert.

1. Wählen Sie **Auswählen**, um die verwendeten Speichergeräte zu ändern.
2. Aktivieren oder deaktivieren Sie im Dialogfeld **Speicher auswählen** die Kontrollkästchen für Speichergeräte, und wählen Sie **OK**.

Schritt 4: Region

> **Hinweis:**
>
> Die Seite **Region** wird nur für einige Hosttypen angezeigt.

Die Auswahl der Region bestimmt, wo VMs bereitgestellt werden. Wählen Sie im Idealfall eine Region in der Nähe des Standorts, an dem die Benutzer auf ihre Anwendungen zugreifen.

Schritt 5: Netzwerk

Geben Sie einen Namen für die Ressourcen ein. Dieser Name wird in der Verwaltungskonsole angezeigt, um die Speicher- und Netzwerkkombination zu identifizieren, die der Verbindung zugeordnet sind.

Wählen Sie mindestens ein Netzwerk für die VMs aus.

Für manche Verbindungstypen (z. B. Azure Resource Manager) werden außerdem von den VMs verwendete Subnetze aufgeführt. Wählen Sie mindestens ein Subnetz aus.

Schritt 6: Zusammenfassung

Überprüfe Sie Ihre Auswahl. Wenn Sie Änderungen vornehmen möchten, kehren Sie zu den vorherigen Seiten des Assistenten zurück. Wählen Sie zum Abschluss **Fertig stellen**.

> **Hinweis:**
>
> - Beim lokalen Speichern temporärer Daten können Sie benutzerdefinierte Werte für den temporären Datenspeicher konfigurieren, wenn Sie den Katalog mit den Maschinen für diese Verbindung erstellen.
> - Für Administratoren mit Vollzugriff wird kein Geltungsbereich angezeigt. Weitere Informationen finden Sie unter Administratoren, Rollen und Geltungsbereiche.

Bearbeiten von Verbindungseinstellungen

Sie können dieses Verfahren für folgenden Vorgänge nicht verwenden:

- Verbindung umbenennen oder eine neue erstellen.
- GPU-Einstellungen für eine Verbindung ändern. Kataloge, die auf diese Ressource zugreifen, müssen ein geeignetes GPU-spezifisches Image verwenden. Wenn Sie die GCP-Einstellungen ändern möchten, erstellen Sie daher eine neue Verbindung, anstatt eine bestehende Verbindung zu bearbeiten.

Verbindung bearbeiten

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung bearbeiten** aus.
3. Verwenden Sie die Seite **Verbindungseigenschaften**, um die Verbindungsadresse und die Anmeldeinformationen zu ändern. Ändern Sie die Adresse nur, wenn die aktuelle Hostmaschine eine neue Adresse hat. Durch die Eingabe der Adresse einer anderen Maschine werden die Maschinenkataloge der Verbindung fehlerhaft.
   - Wählen Sie **Einstellungen bearbeiten…** aus und geben Sie dann die neuen Informationen ein.
   - Für die Eingabe eines Servers mit hoher Verfügbarkeit für eine XenServer-Verbindung klicken Sie auf **Server bearbeiten…** und wählen dann die Server aus. Citrix empfiehlt, dass Sie alle Server im Pool auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.

     > **Hinweis:**
     >
     > Wenn Sie HTTPS verwenden und Server mit hoher Verfügbarkeit konfigurieren möchten, installieren Sie nicht ein Platzhalterzertifikat für alle Server in einem Pool. Für jeden Server ist ein individuelles Zertifikat erforderlich. Weitere Informationen finden Sie unter Verbindung zu XenServer erstellen.

4. Verwenden Sie die Seite **Erweitert**, um die Einstellungen zu bearbeiten und eine maximale Anzahl gleichzeitiger Aktionen (oder gleichzeitiger Maschinen) pro Hostingverbindung anzugeben. Diese Einstellungen können nützlich sein, wenn durch die Energieverwaltungseinstellungen der gleichzeitige Start zu vieler oder zu weniger Maschinen zugelassen wird. Für jeden Verbindungstyp gibt es bestimmte Standardwerte, die in den meisten Fällen geeignet sind. In der Regel müssen sie nicht geändert werden.
   - Über **Gleichzeitige Aktionen (alle Typen)** und **Gleichzeitige Updates für Personal vDisk-Inventar** wird Folgendes festgelegt: die maximale absolute Zahl Aktionen/Updates, die gleichzeitig an dieser Verbindung auftreten dürfen, und den maximalen Prozentsatz aller Maschinen, die diese Verbindung verwenden. Sie müssen sowohl ganze als auch prozentuale Werte angeben. Der Grenzwert ist der niedrigere Wert.

     Beispiel: Wird in einer Bereitstellung mit 34 Maschinen die Einstellung **Gleichzeitige Aktionen (alle Typen)** auf einen absoluten Wert von 10 und einen Prozentsatz von 10 festgelegt, wird als tatsächliches Limit 3 angewendet (d. h. 10 Prozent von 34 auf die nächste Ganzzahl gerundet –ein kleinerer Wert als die absolute Zahl von 10 Maschinen).
   - Die **Höchstanzahl neue Aktionen pro Minute** ist eine absolute Zahl. Es gibt keinen Prozentwert.

- Geben Sie die Informationen in **Verbindungsoptionen** nur unter der Anleitung eines Supportmitarbeiters von Citrix ein.

5. Verwenden Sie die Seite **Geltungsbereiche**, um einen oder mehrere Geltungsbereiche für diesen Host auszuwählen.

   > **Hinweis:**
   >
   > Für Administratoren mit Vollzugriff wird kein Geltungsbereich angezeigt. Diese Administratoren haben per Definition Zugriff auf alle kundenverwalteten Objekte in Citrix Cloud und in abonnierten Diensten.

   Weitere Informationen finden Sie unter Administratoren, Rollen und Geltungsbereiche.

6. Auf der Seite **Freigegebene Mandanten** können Sie Mandanten und Abonnements hinzufügen, die sich die Azure Compute Gallery mit dem Abonnement dieser Verbindung teilen.

   a) Geben Sie das **Anwendungsgeheimnis** für die Anwendung ein, die dieser Verbindung zugeordnet ist. Mit diesen Informationen können Sie sich bei Azure authentifizieren. Es wird empfohlen, Schlüssel regelmäßig zu ändern, um die Sicherheit zu gewährleisten.
   b) Fügen Sie freigegebene Mandanten und Abonnements hinzu. Sie können bis zu acht freigegebene Mandanten hinzufügen. Für jeden Mandanten können Sie maximal acht Abonnements hinzufügen.

7. Klicken Sie auf **Speichern** und **Anwenden**, damit die Änderungen übernommen werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Aktivieren und Deaktivieren des Wartungsmodus für eine Verbindung

Wenn Sie den Wartungsmodus für eine Verbindung aktivieren, können keine neuen Energieaktionen auf in dieser Verbindung gespeicherten Maschinen stattfinden. Benutzer können keine Verbindung mit einer Maschine herstellen, wenn sie im Wartungsmodus ist. Wenn Benutzer bereits verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung aus. Zum Aktivieren des Wartungsmodus wählen Sie in der Aktionsleiste **Wartungsmodus einschalten**. Zum Deaktivieren des Wartungsmodus wählen Sie **Wartungsmodus ausschalten**.

Sie können den Wartungsmodus auch für einzelne Maschinen ein- und ausschalten. Sie können den Wartungsmodus für Maschinen in Maschinenkatalogen und Bereitstellungsgruppen aktivieren oder deaktivieren.

Löschen einer Verbindung

> **Achtung:**
>
> Das Löschen einer Verbindung kann zur Folge haben, dass eine große Zahl von Maschinen gelöscht wird, Datenverlust eingeschlossen. Stellen Sie sicher, dass die Benutzerdaten auf den betroffenen Maschinen gesichert wurden oder nicht mehr benötigt werden.

Vor dem Löschen einer Verbindung müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind von den in dieser Verbindung gespeicherten Maschinen abgemeldet.
- Es werden keine getrennten Benutzersitzungen ausgeführt.
- Der Wartungsmodus wird für gepoolte und dedizierte Maschinen aktiviert.
- Alle Maschinen in den von der Verbindung verwendeten Maschinenkatalogen sind ausgeschaltet.

Ein Maschinenkatalog kann nicht mehr verwendet werden, wenn Sie eine Verbindung löschen, auf die dieser Katalog verweist. Verweist ein Katalog auf diese Verbindung, können Sie den Katalog löschen. Stellen Sie vor dem Löschen eines Katalogs sicher, dass er nicht von anderen Verbindungen verwendet wird.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung löschen**.
3. Wenn für die Verbindung Maschinen gespeichert sind, werden Sie gefragt, ob Sie die Maschinen löschen möchten. Wenn dies der Fall ist, geben Sie an, was mit dem zugewiesenen Active Directory-Computerkonten geschehen soll.

Umbenennen einer Verbindung

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann **Verbindung umbenennen** aus.

Verbindung testen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann **Verbindung testen** aus.

Anzeigen von Maschinendetails für eine Verbindung

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Maschinen anzeigen**.

Im oberen Bereich werden die Maschinen angezeigt, auf die über die Verbindung zugegriffen wird. Wählen Sie eine Maschine aus, um die Details im unteren Bereich anzuzeigen. Für geöffnete Sitzungen werden auch Sitzungsdetails angezeigt.

Sie können das Suchfeature verwenden, um Maschinen schnell aufzufinden. Wählen Sie entweder eine gespeicherte Suche aus der Liste im oberen Bereich des Bildschirms aus oder erstellen Sie eine neue Suche. Sie können nach dem Maschinennamen suchen, indem Sie den ganzen Namen oder einen Teil des Namens eingeben. Alternativ können Sie auch einen Ausdruck für eine erweiterte Suche erstellen. Um einen Ausdruck zu erstellen, wählen Sie die **Erweiterungsschaltfläche** und dann Eigenschaften und Operatoren aus den angezeigten Listen.

Verwalten von Maschinen einer Verbindung

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie eine Verbindung und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Wählen Sie in der Aktionsleiste eine der folgenden Optionen aus. Abhängig vom Maschinenzustand und dem Verbindungshosttyp sind einige Aktionen möglicherweise nicht verfügbar.

    - **Starten:** Die Maschine wird gestartet, wenn sie ausgeschaltet oder angehalten ist.
    - **Anhalten:** Die Maschine wird ohne Herunterfahren angehalten die Liste der Maschinen wird aktualisiert.
    - **Herunterfahren:** Das Betriebssystem wird aufgefordert, herunterzufahren.
    - **Herunterfahren erzwingen:** Die Maschine wird zwingend abgeschaltet und die Liste der Maschinen wird aktualisiert.
    - **Neu starten:** Das Betriebssystem wird heruntergefahren und die Maschine wird neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt der Desktop im aktuellen Zustand.
    - **Wartungsmodus aktivieren:** Stoppt vorübergehend Verbindungen mit einer Maschine. Benutzer können keine Verbindung mit einer Maschine in diesem Zustand herstellen. Wenn Benutzer verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden. Sie können den Wartungsmodus auch für alle Maschinen aktivieren bzw. deaktivieren, auf die über eine Verbindung zugegriffen wird (siehe oben).
    - **Aus Bereitstellungsgruppe entfernen:** Beim Entfernen einer Maschine aus einer Bereitstellungsgruppe wird sie nicht aus dem von der Bereitstellungsgruppe verwendeten Maschinenkatalog gelöscht. Sie können Maschinen nur entfernen, wenn kein Benutzer mit ihnen verbunden ist. Aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie eine Maschine entfernen.
    - **Löschen:** Wenn Sie eine Maschine löschen, können Benutzer nicht mehr darauf zugreifen und die Maschine wird aus dem Maschinenkatalog gelöscht. Stellen Sie vor dem Löschen einer Maschine sicher, dass alle Benutzerdaten gesichert wurden oder nicht mehr

benötigt werden. Sie können eine Maschine nur löschen, wenn keine Benutzer mit ihr verbunden sind. Aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine löschen.

Bei Aktionen, bei denen eine Maschine heruntergefahren wird, wird diese ausgeschaltet, wenn das Herunterfahren nicht innerhalb von 10 Minuten erfolgt. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

Bearbeiten des Speichers

Sie können den Status der Server anzeigen, auf denen das Betriebssystem sowie temporäre und persönliche Daten (PvD) für VMs gespeichert werden, die eine Verbindung verwenden. Sie können auch festlegen, welche Server für die Speicherung der jeweiligen Datentypen verwendet werden.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Speicher bearbeiten**.
3. Wählen Sie im linken Bereich den Datentyp: Betriebssystem oder temporär.
4. Aktivieren oder deaktivieren Sie für den ausgewählten Datentyp das Kontrollkästchen für mindestens ein Speichergerät.
5. Wählen Sie **OK**.

Jedes Speichergerät in der Liste enthält den Namen und Speicherstatus. Gültige Speicherstatuswerte sind Folgende:

- **Wird verwendet**: Der Speicher wird zum Erstellen von Maschinen verwendet.
- **Abgelöst:** Der Speicher wird nur für vorhandene Maschinen verwendet. Diesem Speicher werden keine neuen Maschinen hinzugefügt.
- **Nicht verwendet:** Der Speicher wird nicht zum Erstellen von Maschinen verwendet.

Wenn Sie das Kontrollkästchen für ein Gerät deaktivieren, das den Status **Wird verwendet** hat, ändert sich der Status in **Abgelöst**. Vorhandene Maschinen verwenden dieses Speichergerät weiterhin (und können Daten darauf schreiben). Der Speicher kann daher selbst dann seine Kapazitätsgrenze erreichen, wenn er nicht mehr zum Erstellen von Maschinen verwendet wird.

Verwaiste Azure-Ressourcen erkennen

Verwaiste Ressourcen sind ungenutzte Ressourcen im System, die zu unnötigen Kosten führen können.

Mit diesem Feature können Sie verwaiste Azure-Ressourcen in den Hosts auf Ihrer Cloudsite erkennen.

Folgen Sie den Schritten auf Citrix DaaS:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie eine Verbindung aus und wählen Sie in der Aktionsleiste die Option **Verwaiste Ressourcen erkennen**. Im Dialogfeld **Verwaiste Ressourcen erkennen** wird der Bericht zu verwaisten Ressourcen angezeigt.
3. Um den Bericht zu verwaiste Ressourcen anzuzeigen, wählen Sie **Bericht anzeigen**.

Alternativ können Sie verwaiste Azure-Ressourcen auch mithilfe von PowerShell erfassen. Weitere Informationen finden Sie unter Liste verwaister Ressourcen abrufen.

Weitere Informationen zu den Ursachen für verwaiste Ressourcen und zur weiteren Vorgehensweise finden Sie unter Efficiently manage Orphaned Azure resources with Citrix.

Verbindungstimer

Sie können mit Citrix Richtlinieneinstellungen drei Verbindungstimer konfigurieren:

- **Timer für längste Verbindung:** Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop fest. Verwenden Sie die Richtlinieneinstellungen **Sitzungsleerlauftimer** und **Sitzungsleerlauf - Timerintervall**.
- **Timer für inaktive Verbindung:** Legt fest, wie lange eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem virtuellen Desktop erhalten wird, wenn keine Eingabe vom Benutzer erfolgt. Verwenden Sie die Richtlinieneinstellungen **Sitzungsleerlauftimer** und **Sitzungsleerlauf - Timerintervall**.
- **Timer für getrennte Sitzung:** Legt fest, wie lange ein getrennter virtueller Desktop gesperrt bleibt, bis die Sitzung abgemeldet wird. Verwenden Sie die Richtlinieneinstellungen **Timer für getrennte Sitzung** und **Getrennte Sitzungen - Timerintervall**.

Wenn Sie eine dieser Einstellungen aktualisieren, achten Sie darauf, dass sie in der ganzen Bereitstellung konsistent sind.

Weitere Informationen finden Sie in der Dokumentation für die Richtlinieneinstellungen.

Ressourcennetzwerke bearbeiten

Sie können die Netzwerke für eine Verbindung ändern. Führen Sie folgende Schritte aus:

1. Gehen Sie zu **Verwalten > Vollständige Konfiguration > Hosting**.
2. Wählen Sie die Zielressourcen unter der Verbindung und dann in der Aktionsleiste die Option **Netzwerk bearbeiten**.
3. Wählen Sie mindestens ein Netzwerk aus, das die VMs verwenden sollen.
4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern und den Vorgang zu beenden.

Löschen, Umbenennen oder Testen von Ressourcen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie unter der Verbindung die Zielressourcen und dann in der Aktionsleiste den entsprechenden Eintrag aus:
    - **Ressourcen löschen**
    - **Ressourcen umbenennen**
    - **Ressourcen testen**

Liste verwaister Ressourcen abrufen

Sie können eine Liste der verwaisten Ressourcen abrufen, die von MCS erstellt wurden, aber nicht mehr von MCS verfolgt werden. Dies gilt derzeit für Azure-Umgebungen. Um die Liste abzurufen, können Sie PowerShell-Befehle verwenden. Sie können anhand von Verbindungen filtern.

> **Hinweis:**
>
> Der PowerShell-Befehl wird zurückgewiesen, wenn ein Provisioning oder ein Imageupdate im Gang ist.

Einschränkungen

- Nur ein Administrator mit der integrierten Rolle eines Administrators mit vollen Rechten oder eines Cloudadministrator kann den PowerShell-Befehl zum Abrufen der Liste verwaister Ressourcen ausführen.
- Um eine fälschliche Erkennung verwaister Ressourcen zu vermeiden, schalten Sie virtuelle Maschinen nicht ein, während Sie verwaiste Ressourcen filtern.
- Rund 2000 Datensätze werden im Falle einer möglichen hohen Workload als verwaist angezeigt.

Liste der verwaisten Ressourcen anzeigen

Um die Liste der verwaisten Ressourcen anzuzeigen, gehen Sie wie folgt vor

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Führen Sie die folgenden Befehle aus:
    a) Ruft die Verbindungs-UID ab. Die Verbindungs-UID ist der Wert des HypervisorConnectionUid-Attributs.


```
Get-ChildItem xdhyp:\connections | where {
  $_.PluginId -like 'Azure*'  }
 "
<!--NeedCopy-->
```

b) Rufen Sie die Liste der verwaisten Ressourcen ab.

```
get-provorphanedresource
-HypervisorConnectionUid <connection uid>
<!--NeedCopy-->
```

Liste der verwaisten Ressourcen einer Abonnement-ID anzeigen

Um die Liste der verwaisten Ressourcen einer Abonnement-ID anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Führen Sie die folgenden Befehle aus:

   a) Suchen Sie die Verbindungs-UID anhand der Abonnement-ID. Die Verbindungs-UID ist der Wert des HypervisorConnectionUid-Attributs.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.CustomProperties -match '<subscriptionId>'  }

   <!--NeedCopy-->
   ```

   b) Rufen Sie die Liste der verwaisten Ressourcen ab.

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
      uid>
   <!--NeedCopy-->
   ```

> **Hinweis:**
>
> Überprüfen Sie die Ressourcen sorgfältig, bevor Sie sie löschen.

So geht es weiter

- Informationen zur Verbindung zu bestimmten Hosttypen finden Sie unter:
  - Verbindung zu AWS
  - Verbindung zu Google-Cloudumgebungen
  - Verbindung zu Microsoft Azure
  - Verbindung zu Microsoft System Center Virtual Machine Manager

- Verbindung zu Nutanix
- Verbindung zu Nutanix-Cloud und Partnerlösungen
- Verbindung zu VMware
- Verbindung zu VMware-Cloud und Partnerlösungen
- Verbindung zu XenServer

Wenn dies die erste Bereitstellung ist, erstellen Sie zunächst einen Maschinenkatalog.

Verbindung zu AWS

May 17, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf AWS-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu AWS herstellen, müssen Sie zunächst Ihr AWS als Ressourcenstandort eingerichtet haben. Weitere Informationen finden Sie unter AWS-Virtualisierungsumgebungen.

Verbindung erstellen

Beim Erstellen einer Verbindung über die Oberfläche "Vollständige Konfiguration":

- Sie müssen den API-Schlüssel und die geheimen Schlüsselwerte angeben. Sie können die Schlüsseldatei mit diesen Werten aus AWS exportieren und anschließend importieren. Sie müssen auch die Werte für Region, Verfügbarkeitszone, VPC-Namen, Subnetzadressen, Domänenname, Namen der Sicherheitsgruppen und Anmeldeinformationen angeben.
- Die für das AWS-Rootkonto von der AWS-Konsole abgerufene Anmeldeinformationsdatei hat nicht das gleiche Format wie die Anmeldeinformationsdateien, die für Standard-AWS-Benutzer heruntergeladen werden. Die Datei kann darum von Citrix DaaS nicht zum Ausfüllen der Felder API-Schlüssel und "Geheimer Schlüssel"verwendet werden. Verwenden Sie AWS Identity Access Management (IAM)-Anmeldeinformationsdateien.

> **Hinweis:**
>
> Nachdem Sie eine Verbindung hergestellt haben, kann die Aktualisierung des API-Schlüssels und des geheimen Schlüssels fehlschlagen. Um das Problem zu beheben, überprüfen Sie Ihren Prox-

> yserver oder die Firewall-Beschränkungen und stellen Sie sicher, dass die folgende Adresse erreichbar ist: `https://*.amazonaws.com`.

Einschränkung

Wenn Sie den Namen einer AWS Virtual Private Cloud (VPC) in der AWS-Konsole ändern, wird die vorhandene Hostingeinheit in Citrix Cloud unterbrochen. Bei unterbrochener Hostingeinheit können Sie keine Kataloge erstellen oder Maschinen zu Katalogen hinzufügen. Um das Problem zu beheben, ändern Sie den Namen der AWS-VPC wieder auf den ursprünglichen Namen.

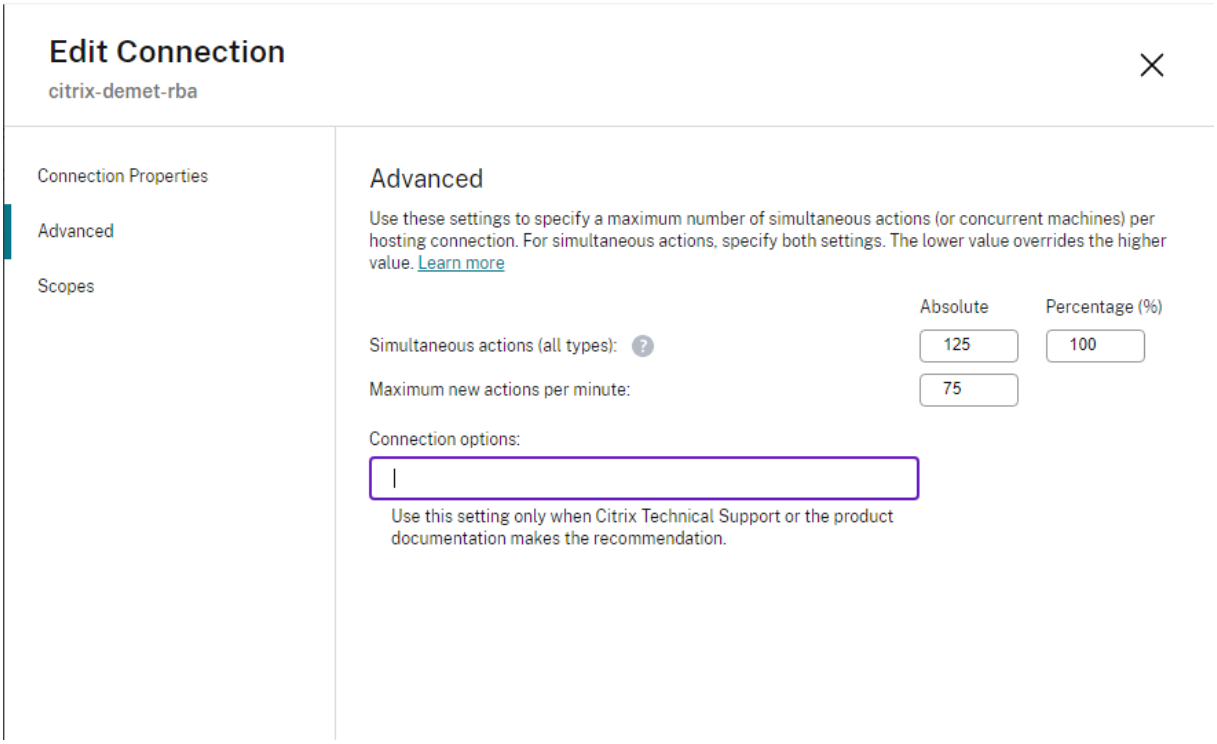
Standardwerte für Hostverbindungen

Wenn Sie Hostverbindungen in der Oberfläche "Vollständige Konfiguration"der AWS-Cloudumgebung erstellen, werden die folgenden Standardwerte angezeigt:

Option	Absolut	Prozent
Gleichzeitige Aktionen (alle Typen)	125	100
Höchstanzahl neue Aktionen pro Minute	150	–
Höchstanzahl gleichzeitiger Bereitstellungsvorgänge	100	–

MCS unterstützt standardmäßig maximal 100 gleichzeitige Provisioningvorgänge.

Sie können diese Werte in Citrix Studio im Abschnitt **Erweitert** unter **Verbindung bearbeiten** konfigurieren:



Alternativ können Sie mit dem Remote PowerShell SDK die maximale Anzahl gleichzeitiger Vorgänge festlegen, um die Einstellungen für Ihre Umgebung zu optimieren.

Geben Sie über die benutzerdefinierte PowerShell-Eigenschaft `MaximumConcurrentProvisioningOperat` die maximale Anzahl gleichzeitiger AWS-Provisioningvorgänge an.

Vor der Konfiguration:

- Sie müssen PowerShell SDK für Cloud installiert haben.
- Der Standardwert für `MaximumConcurrentProvisioningOperations` ist 100.

Führen Sie die folgenden Schritte aus, um den Wert `MaximumConcurrentProvisioningOperations` anzupassen:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Geben Sie `cd xdhyp:\Connections\` ein.
4. Geben Sie `dir` ein, um die Verbindungen aufzulisten.
5. Ändern oder initialisieren Sie die Zeichenfolge “Custom Properties”:
    - Wenn für die Zeichenfolge “Custom Properties”ein Wert festgelegt ist, kopieren Sie “Custom Properties”in den Editor. Ändern Sie dann die Eigenschaft `MaximumConcurrentProvisionir` auf Ihren bevorzugten Wert. Sie können einen Wert zwischen 1 und 1000 eingeben.

Beispiel: <Property xsi:type="IntProperty"Name="MaximumConcurrentProvision
"Value="xyz"/>.

- Wenn die Zeichenfolge "Custom Properties"leer/null ist, müssen Sie die Zeichenfolge initialisieren, indem Sie die richtige Syntax für das Schema und die Eigenschaft `MaximumConcurrentProvisioningOperations` eingeben.

6. Fügen Sie im **PowerShell-Fenster** die geänderte Zeichenfolge für "Custom Properties"aus dem Editor ein, und weisen Sie ihr eine Variable zu. Wenn Sie "Benutzerdefinierte Eigenschaft"initialisiert haben, fügen Sie die folgenden Zeilen nach der Syntax hinzu:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
   org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'.
   ```

   Durch diese Zeichenfolge wird die Eigenschaft `MaximumConcurrentProvisioningOperations` auf 100 festgelegt. In der Zeichenfolge "Custom Properties"müssen Sie die Eigenschaft `MaximumConcurrentProvisioningOperations` auf einen Wert festlegen, der Ihren Bedürfnissen entspricht.

7. Geben Sie `Get-XDAuthentication` ein, und Sie werden zur Eingabe Ihrer Anmeldeinformationen aufgefordert.

8. Führen Sie `$cred = Get-Credential` aus, und Sie werden möglicherweise nur zur Eingabe eines Kennworts (oder eines Namens und eines Kennworts) aufgefordert. Möglicherweise müssen Sie auch die Anwendungs-ID und den zugehörigen geheimen Schlüssel eingeben. Verbindungen mit rollenbasierter Authentifizierung erfordern für **role_based_auth** den Namen und das Kennwort. Andernfalls geben Sie die AWS-API-ID und den geheimen Schlüssel ein.

9. Führen Sie `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password` aus. Für *<connection-name>* müssen Sie den Namen der Verbindung eingeben.

10. Geben Sie `dir` ein, um die aktualisierte Zeichenfolge "CustomProperties"zu überprüfen.

Sicherheitsgruppen pro Netzwerkschnittstelle konfigurieren

Wenn Sie eine Hostverbindung bearbeiten, können Sie jetzt mithilfe eines PowerShell-Befehls die maximal zulässige Anzahl von Sicherheitsgruppen pro Elastic Network Interface (ENI) konfigurieren. Informationen zu Kontigenten für AWS-Sicherheitsgruppen finden Sie unter Sicherheitsgruppen.

So konfigurieren Sie Sicherheitsgruppen pro Netzwerkschnittstelle:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie `cd xdhyp:\Connections\` aus.
4. Führen Sie `dir` aus, um die Verbindungen aufzulisten.
5. Führen Sie den folgenden PowerShell-Befehl aus, um Sicherheitsgruppen pro Netzwerkschnittstelle zu konfigurieren:

```
1 Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws
     -Name "Citrix_MachineManagement_Options" -Value "
     AwsMaxENISecurityGroupLimit=<number>"
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie keinen Wert für `AwsMaxENISecurityGroupLimit` festlegen, wird der Standardwert von 5 verwendet.

Service-Endpunkt-URL

Standard-Service-Endpunkt-URL

Wenn Sie MCS verwenden, werden neue AWS-Verbindungen mit einem API-Schlüssel und einem API-Geheimnis hinzugefügt. Anhand dieser Informationen und des authentifizierten Kontos fragt MCS bei AWS mit dem AWS-API-Aufruf DescribeRegions EC2 die unterstützten Zonen ab. Die Abfrage erfolgt mit der generischen EC2-Service-Endpunkt-URL `https://ec2.amazonaws.com/`. Wählen Sie über MCS die Zone für die Verbindung aus der Liste der unterstützten Zonen aus. Die bevorzugte AWS-Service-Endpunkt-URL wird automatisch für die Zone ausgewählt. Nach dem Erstellen der Service-Endpunkt-URL können Sie diese nicht mehr ändern.

Nicht standardmäßige Service-Endpunkt-URL

In manchen Situationen wird keine automatisch gewählte AWS-Service-Endpunkt-URL für die Verbindung benötigt. In diesem Fall können Sie mit dem Citrix Cloud-SDK und PowerShell eine Verbindung mit einer nicht standardmäßigen Service-Endpunkt-URL herzustellen. Zum Erstellen einer Verbindung mit der Service-Endpunkt-URL `https://ec2.cn-north-1.amazonaws.com.cn` gehen Sie beispielsweise folgendermaßen vor:

1. Richten Sie den von AWS gehosteten Cloud Connector ein und stellen Sie sicher, dass er verbunden ist.

2. Führen Sie die folgenden PowerShell-Befehle aus, um die Liste der Cloud Connectors anzuzeigen.

```
1  PS C:> asnp citrix.*
2  PS C:> Get-XDAuthentication
3  PS C:> Get-ConfigEdgeServer
4 <!--NeedCopy-->
```

3. Suchen Sie die ZoneUid des neu erstellten Cloud Connectors und geben Sie sie in den folgenden PowerShell-Befehlen ein. Ersetzen Sie die kursiv dargestellten Elemente durch die entsprechenden Werte.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidZoneUid-
Name"My New Connection"-ConnectionType "AWS"-HypervisorAddress @
("https://ec2.cn-north-1.amazonaws.com.cn")-UserName"APIkey" -
Password"API Secret" -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
 $hyp. HypervisorConnectionUid
```

4. Aktualisieren Sie die Registerkarte **Vollständige Konfiguration > Hosting**, um zu überprüfen, ob die EC2-Verbindung erstellt wurde.
5. Fügen Sie unter Verwendung der neuen Verbindung einen Ressourcenstandort hinzu.

IAM-Berechtigungen definieren

Anhand der Informationen in diesem Abschnitt können Sie IAM-Berechtigungen für Citrix DaaS in AWS definieren. Der IAM-Dienst von Amazon gestattet Konten mit mehreren Benutzern, die in Gruppen organisiert werden können. Die Benutzer können verschiedene Berechtigungen für die Durchführung von Vorgängen haben, die mit dem Konto verknüpft sind. Weitere Informationen zu IAM-Berechtigungen finden Sie unter IAM-JSON-Richtlinienreferenz.

Gehen Sie zum Anwenden der IAM-Berechtigungsrichtlinie auf eine neue Benutzergruppe folgendermaßen vor:

1. Melden Sie sich bei der AWS-Verwaltungskonsole an und wählen Sie **IAM service** aus der Dropdownliste aus.
2. Wählen Sie **Create a New Group of Users**.
3. Geben Sie einen Namen für die neue Benutzergruppe ein und wählen Sie **Continue**.
4. Wählen Sie auf der Seite **Permissions** die Option **Custom Policy** und dann **Select**.
5. Geben Sie einen Namen für die **Berechtigungsrichtlinie**ein.
6. Geben Sie im Abschnitt **Richtliniendokument** die relevanten Berechtigungen ein.

Nach Eingabe der Richtlinieninformationen wählen Sie **Weiter**, um die Anwendung der IAM-Berechtigungsrichtlinie auf die Benutzergruppe abzuschließen. Den Benutzern in der Gruppe

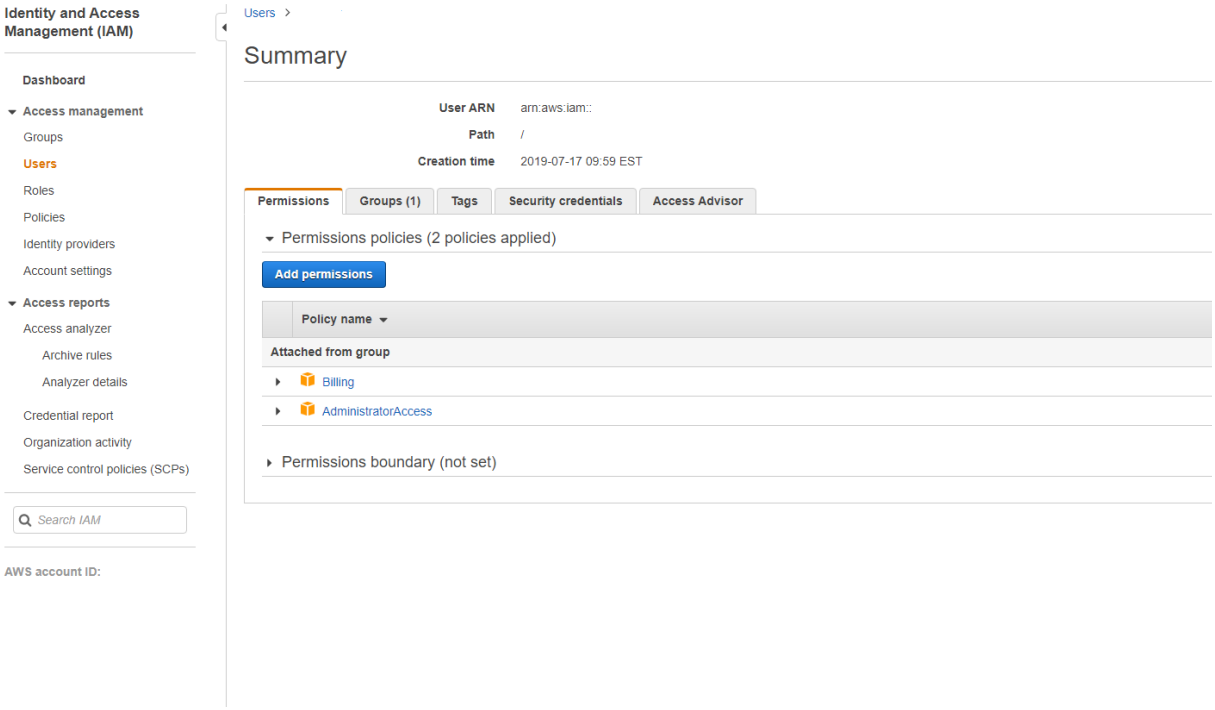
werden nur die Berechtigungen erteilt, die sie zur Ausführung der für Citrix DaaS erforderlichen Aktionen benötigen.

> **Wichtig:**
>
> Verwenden Sie den Richtlinientext im nachstehenden Beispiel, um die von Citrix DaaS in einem AWS-Konto durchgeführten Aktionen aufzulisten, ohne diese auf bestimmte Ressourcen zu beschränken. Citrix empfiehlt die Verwendung des Beispiels zu Testzwecken. Für Produktionsumgebungen können Sie weitere Beschränkungen für Ressourcen hinzufügen.

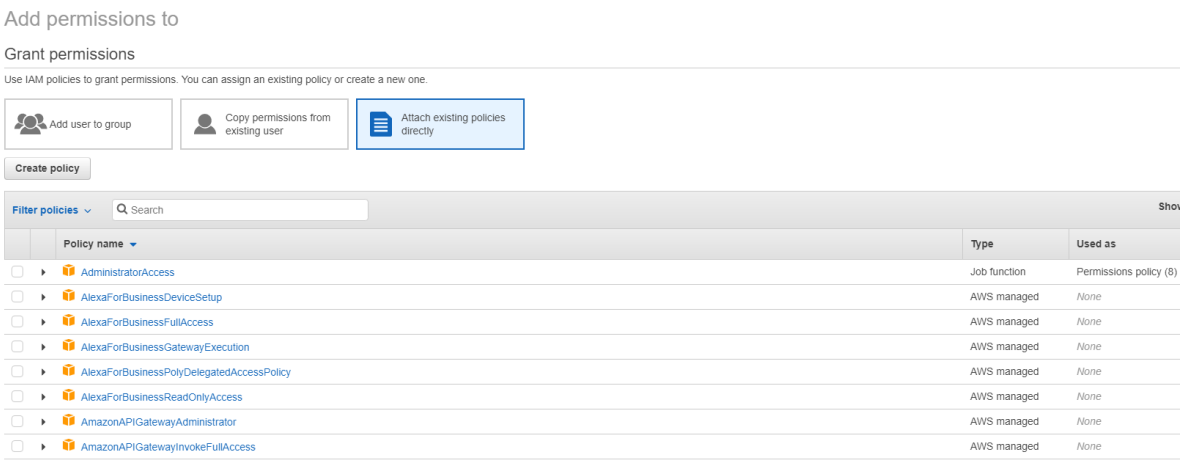
IAM-Berechtigungen hinzufügen

Fügen Sie die Berechtigungen im Bereich **IAM** der AWS Management Console hinzu:

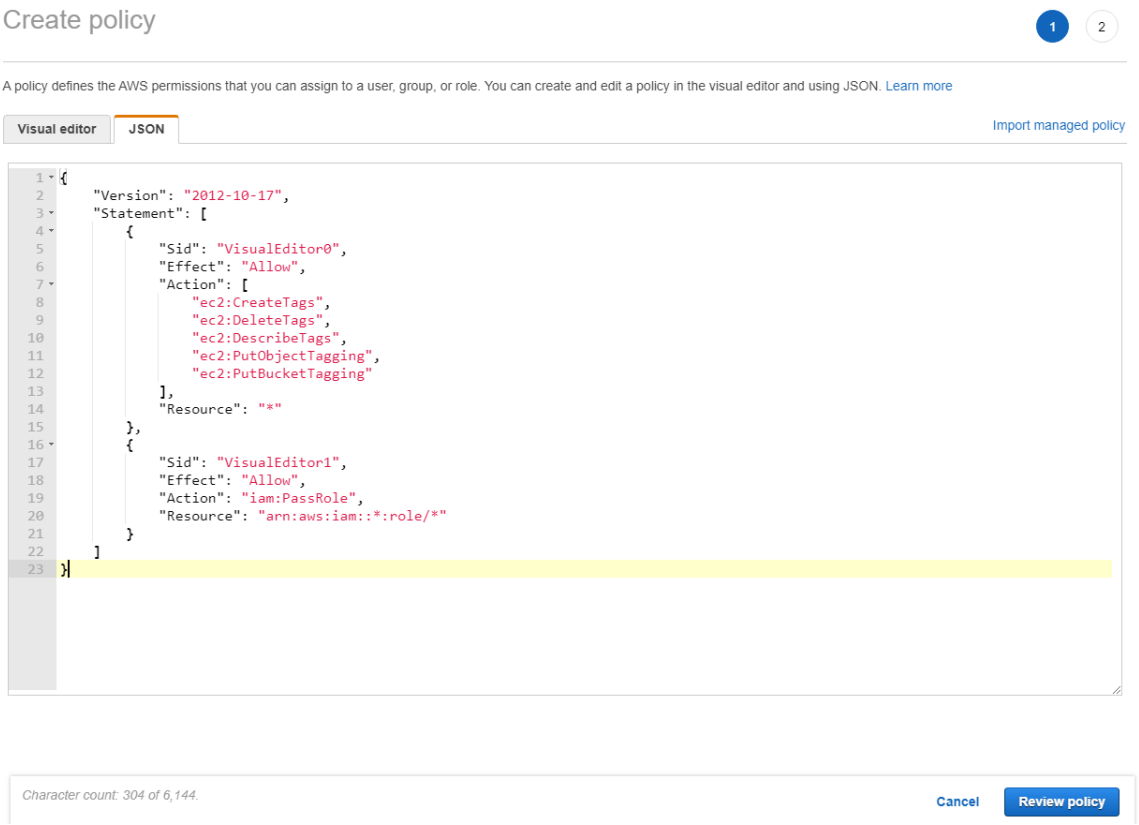
1. Wählen Sie im Bereich **Summary** die Registerkarte **Permissions**.
2. Wählen Sie **Add Permissions**.



Erteilen Sie im Fenster **Add Permissions to** folgende Berechtigungen:



Verwenden Sie Folgendes als Beispiel für die Registerkarte **JSON**:



> **Tipp:**
>
> Das JSON-Beispiel enthält möglicherweise nicht alle Berechtigungen für Ihre Umgebung. Weitere Informationen finden Sie unter Über AWS-Berechtigungen.

Erforderliche AWS-Berechtigungen

Dieser Abschnitt enthält die vollständige Liste der AWS-Berechtigungen. Verwenden Sie sämtliche Berechtigungen, wie im Abschnitt angegeben, um eine ordnungsgemäße Funktionalität sicherzustellen.

> **Hinweis:**
>
> Die Berechtigung *iam:PassRole* wird nur für **role_based_auth** benötigt.

Hostverbindung erstellen

Eine neue Hostverbindung wird unter Verwendung der von AWS abgerufenen Informationen hinzugefügt.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Energieverwaltung virtueller Maschinen

Maschineninstanzen werden ein- oder ausgeschaltet.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
```



```
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Erstellen, Aktualisieren oder Löschen von VMs

Ein Maschinenkatalog wird mit VMs erstellt, aktualisiert oder gelöscht, die als AWS-Instanzen bereitgestellt werden.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
```



```
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

```



```
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--NeedCopy-->
```

> **Hinweis:**
>
> - Der Abschnitt zu EC2, der sich auf SecurityGroups bezieht, wird nur benötigt, wenn während der Katalogerstellung eine Isolationssicherheitsgruppe für die Vorbereitungs-VM erstellt werden muss. Sobald dies abgeschlossen ist, sind diese Berechtigungen nicht erforderlich.

Direkter Disk-Upload und -Download Durch den direkten Disk-Upload entfällt die Volumeworker-Anforderung beim Provisioning von Maschinenkatalogen. Stattdessen werden von AWS bereitgestellte öffentliche APIs verwendet. Diese Funktion reduziert die mit zusätzlichen Speicherkonten verbundenen Kosten und die komplexe Verwaltung von Volumeworker-Prozessen.

> **Hinweis:**
>
> Die Volumeworker-Unterstützung ist veraltet.

Folgende Berechtigungen müssen zur Richtlinie hinzugefügt werden:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **Wichtig:**
>
> - Sie können eine neue VM zu vorhandenen Maschinenkatalogen ohne Volumeworker-Ressourcen wie Volumeworker-AMI und Volumeworker-VM hinzufügen.
> - Wenn Sie einen vorhandenen Katalog löschen, in dem Volumeworker verwendet wurde, werden alle mit dem zugehörigen Volumeworker zusammenhängenden Artefakte gelöscht.

EBS-Verschlüsselung erstellter Volumes

EBS kann neu erstellte Volumes automatisch verschlüsseln, wenn das AMI verschlüsselt ist oder EBS zur Verschlüsselung aller neuen Volumes konfiguriert ist. Zum Implementieren der Funktionalität müssen jedoch die folgenden Berechtigungen in der IAM-Richtlinie enthalten sein.

```
{

      "Version": "2012-10-17",
      "Statement": [
         {

             "Effect": "Allow",
             "Action": [
                  "kms:CreateGrant",
                  "kms:Decrypt",
                  "kms:DescribeKey",
                  "kms:GenerateDataKeyWithoutPlainText",
                  "kms:GenerateDataKey",
                  "kms:ReEncryptTo",
                  "kms:ReEncryptFrom"
             ],
             "Resource": "*"
          }

     ]
 }

<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Berechtigungen können durch Hinzufügen eines Abschnitts “Resource”und “Condition” nach Ermessen des Benutzers auf bestimmte Schlüssel beschränkt werden. Beispiel: **KMS-Berechtigungen mit Bedingung**:

```
{

      "Version": "2012-10-17",
      "Statement": [
         {
```



```
6
7               "Effect": "Allow",
8               "Action": [
9                    "kms:CreateGrant",
10                   "kms:Decrypt",
11                   "kms:DescribeKey",
12                   "kms:GenerateDataKeyWithoutPlainText",
13                   "kms:GenerateDataKey",
14                   "kms:ReEncryptTo",
15                   "kms:ReEncryptFrom"
16              ],
17              "Resource": [
18                  "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                       -456d-a12b-a123b4cd56ef"
19              ],
20              "Condition": {
21
22                  "Bool": {
23
24                      "kms:GrantIsForAWSResource": true
25                   }
26
27               }
28
29          }
30
31      ]
32   }
33
34  <!--NeedCopy-->
```

Die folgende Schlüsselrichtlinienanweisung ist die komplette Standardrichtlinie für KMS-Schlüssel, die erforderlich ist, damit das Konto unter Einsatz von IAM-Richtlinien Berechtigungen für alle Aktionen (kms: *) für den KMS-Schlüssel delegieren kann.

```
1  {
2
3  "Sid": "Enable IAM policies",
4  "Effect": "Allow",
5  "Principal": {
6
7  "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10 "Action": "kms:",
11 "Resource": ""
12  }
13
14 <!--NeedCopy-->
```

Weitere Informationen finden Sie in der offiziellen AWS-Dokumentation unter AWS Key Management Service.

Rollenbasierte IAM-Authentifizierung

Die folgenden Berechtigungen werden zur Unterstützung der rollenbasierten Authentifizierung hinzugefügt.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
 }

<!--NeedCopy-->
```

Richtlinie für Mindest-IAM-Berechtigungen

Die folgende JSON kann für alle derzeit unterstützten Features verwendet werden. Unter Verwendung der Richtlinie können Sie Hostverbindungen erstellen, VMs erstellen, aktualisieren und löschen und die Energieverwaltung durchführen.
Die Richtlinie kann auf die Benutzer angewendet werden (siehe Definieren von IAM-Berechtigungen) oder Sie können die rollenbasierte Authentifizierung über den Sicherheitsschlüssel **role_based_auth** und den geheimen Schlüssel verwenden.

> **Wichtig:**
>
> Um **role_based_auth** zu verwenden, konfigurieren Sie beim Einrichten des Cloud Connectors zunächst die gewünschte IAM-Rolle für die EC2-Instanz des Cloud Connectors. Fügen Sie unter Verwendung von Citrix Studio die Hostingverbindung hinzu und geben Sie role_based_auth für den Authentifizierungsschlüssel und das Geheimnis an. Eine Hostingverbindung mit diesen Einstellungen verwendet dann die rollenbasierte Authentifizierung.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
```



```
                    "ec2:AuthorizeSecurityGroupEgress",
                    "ec2:AuthorizeSecurityGroupIngress",
                    "ec2:CreateImage",
                    "ec2:CreateLaunchTemplate",
                    "ec2:CreateNetworkInterface",
                    "ec2:CreateTags",
                    "ec2:CreateVolume",
                    "ec2:DeleteLaunchTemplate",
                    "ec2:DeleteNetworkInterface",
                    "ec2:DeleteSecurityGroup",
                    "ec2:DeleteSnapshot",
                    "ec2:DeleteTags",
                    "ec2:DeleteVolume",
                    "ec2:DeregisterImage",
                    "ec2:DescribeAccountAttributes",
                    "ec2:DescribeAvailabilityZones",
                    "ec2:DescribeIamInstanceProfileAssociations",
                    "ec2:DescribeImages",
                    "ec2:DescribeInstances",
                    "ec2:DescribeInstanceTypes",
                    "ec2:DescribeLaunchTemplates",
                    "ec2:DescribeLaunchTemplateVersions",
                    "ec2:DescribeNetworkInterfaces",
                    "ec2:DescribeRegions",
                    "ec2:DescribeSecurityGroups",
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeSubnets",
                    "ec2:DescribeTags",
                    "ec2:DescribeSpotInstanceRequests",
                    "ec2:DescribeInstanceCreditSpecifications",
                    "ec2:DescribeInstanceAttribute",
                    "ec2:GetLaunchTemplateData",
                    "ec2:DescribeVolumes",
                    "ec2:DescribeVpcs",
                    "ec2:DetachVolume",
                    "ec2:DisassociateIamInstanceProfile",
                    "ec2:RebootInstances",
                    "ec2:RunInstances",
                    "ec2:StartInstances",
                    "ec2:StopInstances",
                    "ec2:TerminateInstances"
                ],
                "Effect": "Allow",
                "Resource": "*"
            }
    ,
            {

                "Action": [
                    "ec2:AuthorizeSecurityGroupEgress",
                    "ec2:AuthorizeSecurityGroupIngress",
                    "ec2:CreateSecurityGroup",
                    "ec2:DeleteSecurityGroup",
```



```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
,
```



```
116          {
117
118              "Effect": "Allow",
119              "Action": "iam:PassRole",
120              "Resource": "arn:aws:iam::*:role/*"
121           }
122
123      ]
124  }
125
126  <!--NeedCopy-->
```

Hinweis:

- Der Abschnitt zu EC2, der sich auf SecurityGroups bezieht, wird nur benötigt, wenn während der Katalogerstellung eine Isolationssicherheitsgruppe für die Vorbereitungs-VM erstellt werden muss. Sobald dies abgeschlossen ist, sind diese Berechtigungen nicht erforderlich.
- Der KMS-Abschnitt ist nur bei Verwendung der EBS-Volume-Verschlüsselung erforderlich.
- Der Berechtigungsbereich `iam:PassRole` wird nur für **role_based_auth** benötigt.
- Anstelle eines Vollzugriffs können spezifische Berechtigungen auf Ressourcenebene gemäß Ihren Anforderungen und Ihrer Umgebung hinzugefügt werden. Weitere Informationen finden Sie in den AWS-Dokumenten Demystifying EC2 Resource-Level Permissions und Access management for AWS resources.
- Verwenden Sie die Berechtigungen `ec2:CreateNetworkInterface` und `ec2:DeleteNetworkInterface` nur, wenn Sie die Volumeworker-Methode verwenden.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- AWS-spezifische Informationen finden Sie unter AWS-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- AWS-Virtualisierungsumgebungen

Verbindung zu Google-Cloudumgebungen

April 18, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Google-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Google-Cloudumgebungen herstellen, müssen Sie zunächst Ihr Google-Cloudkonto als Ressourcenstandort eingerichtet haben. Weitere Informationen finden Sie unter Google Cloud-Virtualisierungsumgebungen.

Hinzufügen einer Verbindung

Folgen Sie in der Oberfläche "Vollständige Konfiguration"den Anweisungen unter Verbindung und Ressourcen erstellen und verwalten. Die folgende Beschreibung erläutert, wie Sie eine Hostverbindung einrichten:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie auf der Seite **Verbindung** die Optionen **Neue Verbindung erstellen** und **Citrix-Provisioningtools** und wählen Sie **Weiter**.

    - **Zonename**. Wählen Sie eine Zone (entspricht einem Ressourcenstandort) für Ihre Hostressourcen aus. Zonen werden automatisch erstellt, wenn Sie einen Ressourcenstandort erstellen und einen Cloud Connector hinzufügen. Weitere Informationen finden Sie unter Zonen.
    - **Verbindungstyp**. Wählen Sie im Menü die Option **Google Cloud Platform**.
    - **Dienstkontoschlüssel**. Importieren Sie den Schlüssel, der in Ihrer Anmeldeinformationsdatei (.json) enthalten ist. Sie können entweder den Schlüssel aus der Anmeldeinformationsdatei einfügen oder zur Anmeldeinformationsdatei navigieren. So fügen Sie den Schlüssel ein:

        a) Suchen Sie Ihre Anmeldeinformationsdatei
        b) Öffnen Sie die Datei mit Notepad (oder einem beliebigen Texteditor)
        c) Kopieren Sie den Inhalt.
        d) Kehren Sie zur Seite **Verbindung** zurück, wählen Sie **Schlüssel hinzufügen**, fügen Sie den Inhalt ein und wählen Sie **Fertig**.

    - **Dienstkonto-ID**. Das Feld wird automatisch mit Informationen aus dem Dienstkontoschlüssel ausgefüllt.
    - **Verbindungsname**. Geben Sie einen Namen für die Verbindung ein.

- **Datenverkehr über Citrix Cloud Connectors weiterleiten**. Um die API-Anforderungen über einen verfügbaren Citrix Cloud Connector zu leiten, aktivieren Sie dieses Kontrollkästchen. Für eine zusätzliche Sicherheitsebene können Sie auch das Kontrollkästchen **Google Cloud Build zur Verwendung privater Pools aktivieren** aktivieren.

  Alternativ können Sie das Feature mit PowerShell aktivieren. Weitere Informationen finden Sie unter Sichere Umgebung für von GCP verwalteten Netzwerkverkehr erstellen.

> **Hinweis:**
>
> Diese Option ist nur verfügbar, wenn die Bereitstellung aktive Citrix Cloud Connectors enthält. Derzeit wird dieses Feature für Connector Appliances nicht unterstützt.

- **VMs erstellen mit:** Wählen Sie eine Methode zum Erstellen virtueller Maschinen aus.

4. Wählen Sie auf der Seite **Region** einen Projektnamen aus dem Menü aus, wählen Sie die Region, in der sich die gewünschten Ressourcen befinden, und wählen Sie **Weiter**.
5. Geben Sie auf der Seite **Netzwerk** einen Ressourcennamen ein, wählen Sie ein virtuelles Netzwerk aus dem Menü aus, wählen Sie einen Teilbereich (Subset) und wählen Sie **Weiter**. Mit dem Ressourcennamen kann diese Kombination von Region und Netzwerk identifiziert werden. Virtuelle Netzwerke mit dem Namenssuffix *(Shared)* sind freigegebene VPCs. Wenn Sie eine IAM-Rolle auf Subnetzebene für eine freigegebene VPC konfigurieren, werden nur bestimmte Subnetze der freigegebenen VPC in der Subnetzliste angezeigt.

> **Hinweis:**
>
> - Der Ressourcenname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen, und folgende Zeichen sind nicht erlaubt: `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und wählen Sie **Fertig stellen**, um das Fenster **Verbindung und Ressourcen hinzufügen** zu schließen.

Nach dem Erstellen der Verbindung und der Ressourcen wird die erstellte Verbindung samt Ressourcen aufgelistet. Wählen Sie zum Konfigurieren der Verbindung diese aus und wählen Sie in der Aktionsleiste die entsprechende Option.

Sie können außerdem die unter der Verbindung erstellten Ressourcen löschen, umbenennen oder testen. Wählen Sie hierfür die Ressource unter der Verbindung aus und wählen Sie in der Aktionsleiste die entsprechende Option.

Sichere Umgebung für von GCP verwalteten Netzwerkverkehr erstellen

Sie können den Google-Zugriff auf Ihre Google Cloud-Projekte auf den privaten Zugriff einschränken. Diese Implementierung erhöht die Sicherheit beim Umgang mit vertraulichen Daten. Gehen Sie hierzu

folgendermaßen vor:

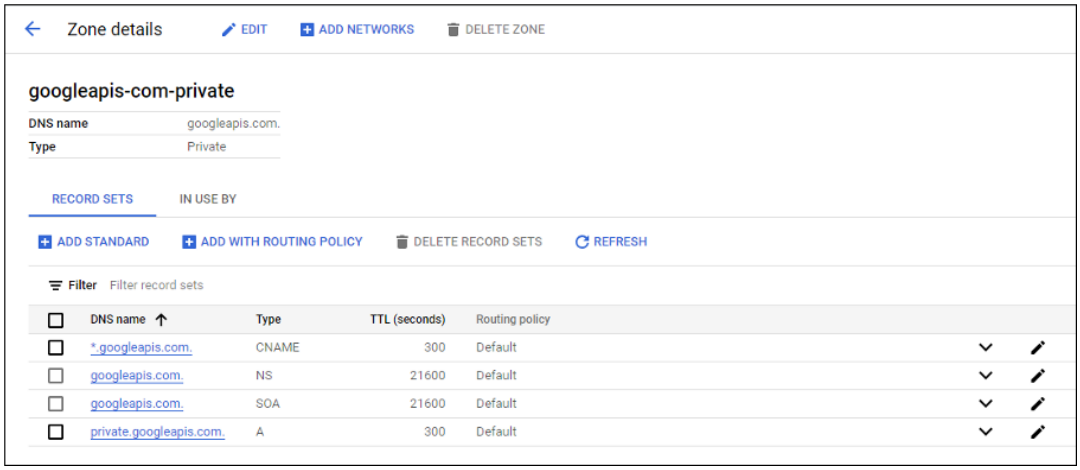
1. Installieren Sie Cloud Connectors in der VPC, in der Sie die VPC Service Controls durchsetzen möchten. Weitere Informationen finden Sie unter VPC Service Controls.
2. Fügen Sie für eine Citrix Cloud-Bereitstellung `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` hinzu. Wenn Sie einen privaten Pool verwenden, fügen Sie `UsePrivateWorkerPool` zu `CustomProperties` hinzu. Informationen zum privaten Workerpool finden Sie unter Private Pools –Übersicht.

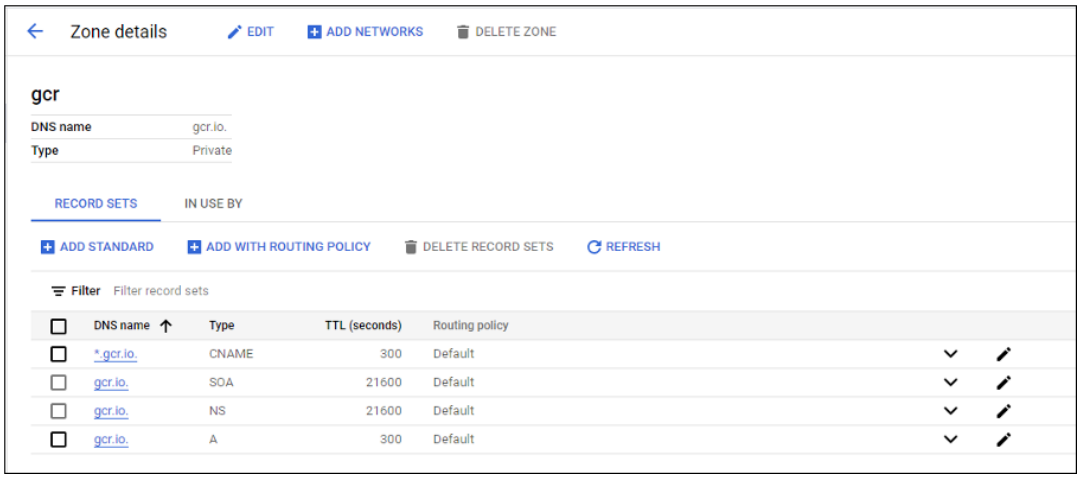
> **Hinweis:**
>
> Derzeit wird dieses Feature für die Connector Appliance nicht unterstützt.

Anforderungen für die Schaffung einer sicheren Umgebung für den von GCP verwalteten Netzwerkverkehr

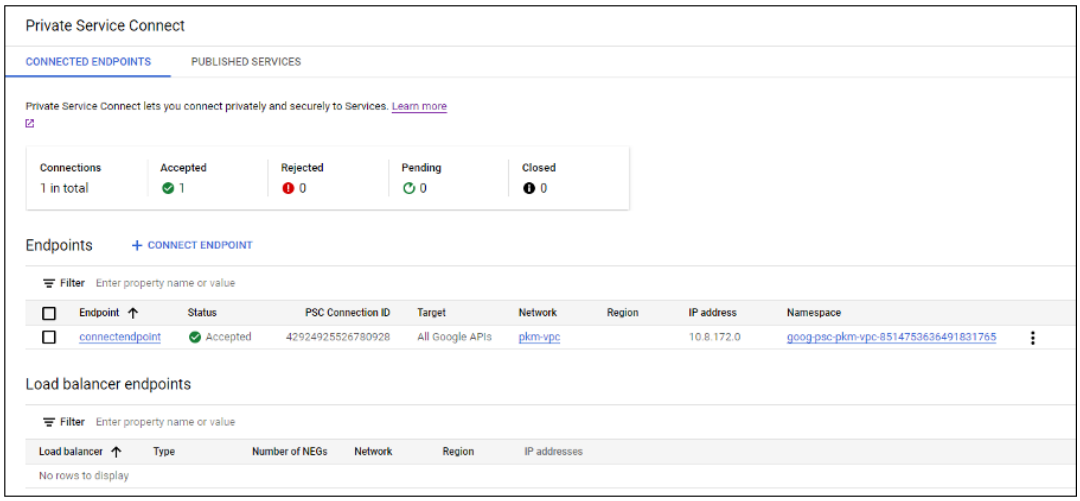
Für die Schaffung einer sicheren Umgebung für den von GCP verwalteten Netzwerkverkehr gelten folgende Anforderungen:

- Die Hostingverbindung muss sich im Wartungsmodus befinden, wenn Sie die benutzerdefinierten Eigenschaften aktualisieren.
- Um private Workerpools verwenden zu können, sind die folgenden Änderungen erforderlich:
  - Fügen Sie für das Citrix Cloud Service-Konto die folgenden IAM-Rollen hinzu:
    - Cloud Build-Dienstkonto
    - Compute Instance-Administrator
    - Dienstkontobenutzer
    - Dienstkonto-Token-Ersteller
    - Inhaber von Cloud Build-Workerpools
  - Erstellen Sie das Citrix Cloud Service-Konto in demselben Projekt, das Sie für die Erstellung einer Hostingverbindung verwenden.
  - Richten Sie DNS-Zonen für **`private`**`.googleapis.com` und `gcr.io` ein (siehe DNS-Konfiguration).

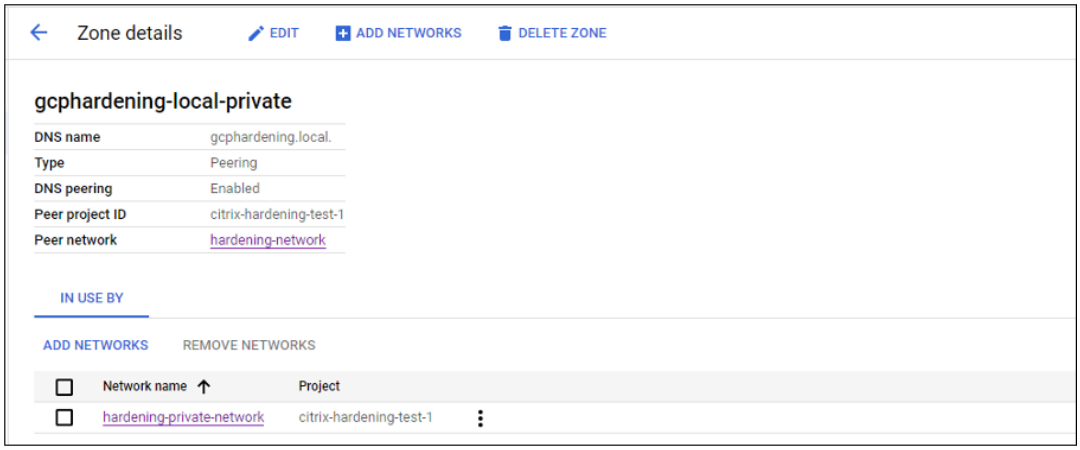




- Richten Sie die private Netzwerkadressübersetzung (NAT) ein oder verwenden Sie Private Service Connect. Weitere Informationen finden Sie unter Zugriff auf Google-APIs über Endpunkte.



- Wenn Sie eine Peering-VPC verwenden, erstellen Sie ein Cloud-DNS-Zonen-Peering zur Peering-VPC. Weitere Informationen finden Sie unter Peering-Zone erstellen.



- Richten Sie in VPC Service Controls Ausgangsregeln ein, damit die APIs und VMs mit dem Internet kommunizieren können. Eingangsregeln sind optional. Beispiel:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

Proxy aktivieren

Um den Proxy zu aktivieren, legen Sie die benutzerdefinierten Eigenschaften für die Hostverbindung wie folgt fest:

1. Öffnen Sie ein PowerShell-Fenster auf dem Delivery Controller-Host, oder verwenden Sie das Remote PowerShell-SDK. Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.
2. Führen Sie die folgenden Befehle aus:
   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Kopieren Sie die `CustomProperties` von der Verbindung in einen Editor.
4. Hängen Sie die Eigenschaftseinstellung wie folgt an:
   - Bei Cloudbereitstellungen (mit öffentlichen Pools): Hängen Sie den `CustomProperties` die Eigenschaftseinstellung `<Property xsi:type="StringProperty"Name="`

ProxyHypervisorTrafficThroughConnector"Value="True"/> an, um den Proxy zu aktivieren. Beispiel:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
   -instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

Erstellen Sie eine Zulassen-Eingangsregel für Cloud Build-Dienstkonto im VPC-Dienstperimeter. Beispiel:

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
<!--NeedCopy-->
```

Informationen zum VPC-Dienstperimeter finden Sie unter Details und Konfiguration von Dienstperimetern.

- Bei Cloudbereitstellungen mit einem privaten Workerpool hängen Sie den CustomProperties die Eigenschaftseinstellungen <Property xsi:type="StringProperty"Name ="ProxyHypervisorTrafficThroughConnector"Value="True"/> und <Property xsi:type="StringProperty"Name="UsePrivateWorkerPool "Value="True"/> an, um den Proxy zu aktivieren. Beispiel:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
   -instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
<Property xsi:type="StringProperty" Name="
   UsePrivateWorkerPool" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

5. Weisen Sie im PowerShell-Fenster den geänderten benutzerdefinierten Eigenschaften eine Variable zu. Beispiel:
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Führen Sie `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL`

HERE>" aus.

7. Führen Sie `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"` aus.
8. Führen Sie `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force` aus.
9. Führen Sie den folgenden Befehl aus, um eine bestehende Hostverbindung zu aktualisieren:

```
Set-Item -PassThru -Path @('XDHyp:\Connections\<ENTER YOUR
    CONNECTION NAME HERE>') -SecurePassword $securePassword -
    UserName $gcpServiceAccount -CustomProperties $customProperty
<!--NeedCopy-->
```

Erforderliche GCP-Berechtigungen

Dieser Abschnitt enthält die vollständige Liste der GCP-Berechtigungen. Verwenden Sie sämtliche Berechtigungen, wie im Abschnitt angegeben, um eine ordnungsgemäße Funktionalität sicherzustellen.

> **Hinweis:**
>
> Ab dem 29. April 2024 führt GCP Änderungen am Standardverhalten von Cloud Build Services und der Verwendung von Dienstkonten ein. Weitere Informationen finden Sie unter Änderungen des Cloud Build-Dienstkontos. Ihre bestehenden Google-Projekte mit aktivierter Cloud Build API vor dem 29. April 2024 sind von dieser Änderung nicht betroffen. Wenn Sie jedoch das bestehende Cloud Build Service-Verhalten nach dem 29. April beibehalten möchten, können Sie die Organisationsrichtlinie erstellen oder anwenden, um die Durchsetzung der Einschränkungen zu deaktivieren, bevor Sie die API aktivieren. Wenn Sie die neue Organisationsrichtlinie festlegen, können Sie weiterhin den vorhandenen Berechtigungen in diesem Abschnitt und den Elementen folgen, die als **Vor der Änderung des Cloud Build Service-Kontos** markiert sind. Wenn nicht, folgen Sie den vorhandenen Berechtigungen und Elementen, die als **Nach der Änderung des Cloud Build Service-Kontos**markiert sind.

Hostverbindung erstellen

- Mindestberechtigungen für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
```



```
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Admin berechnen
- Cloud Datastore User

- Weitere für die freigegebene VPC für das Citrix Cloud-Dienstkonto im Freigegebene-VPC-Projekt erforderliche Berechtigungen:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Network User

Energieverwaltung virtueller Maschinen

Mindestberechtigungen, die für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt erforderlich sind, wenn Kataloge nur mit Energieverwaltung verwendet werden:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Admin berechnen
- Cloud Datastore User

VMs erstellen, aktualisieren oder löschen

- Mindestberechtigungen für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt:


```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
```



```
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use

<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Admin berechnen
- Speicher-Administrator
- Cloud Build-Editor
- Dienstkontobenutzer
- Cloud Datastore User

- Weitere für die freigegebene VPC für das Citrix Cloud-Dienstkonto im Freigegebene-VPC-Projekt erforderliche Berechtigungen zur Erstellung einer Hostingeinheit unter Verwendung der VPC und des Subnetzes aus dem Freigegebene-VPC-Projekt:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```


Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

  - Compute Network User
  - Cloud Datastore User

- (Vor der Änderung des Cloud Build Service-Kontos): Mindestberechtigungen für das Cloud Build-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Build-Dienst beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:
- (Nach der Änderung des Cloud Build Service-Kontos): Mindestberechtigungen für das Cloud Compute-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Compute Service beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
```



```
40  storage.objects.list
41  <!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Cloud Build Service-Konto (Nach der Änderung des Cloud Build Service-Kontos ist es das Cloud Compute Service-Konto)
- Compute Instance-Administrator
- Dienstkontobenutzer

- Mindestberechtigungen für das Cloud Compute-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Build-Dienst beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

```
1  resourcemanager.projects.get
2  storage.objects.create
3  storage.objects.get
4  storage.objects.list
5  <!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- (Vor der Änderung des Cloud Build Service-Kontos): Zusätzliche Berechtigungen für die freigegebene VPC für das Cloud Build-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Build-Dienst beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

- (Nach der Änderung des Cloud Build Service-Kontos): Zusatzberechtigungen für das Cloud Compute-Dienstkonto für Shared VPC im Bereitstellungprojekt, die vom Google Cloud Compute Service beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

```
1  compute.firewalls.list
2  compute.networks.list
3  compute.subnetworks.list
4  compute.subnetworks.use
5  resourcemanager.projects.get
6  <!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- Zusätzliche Berechtigungen für den Cloud-Schlüsselverwaltungsdienst (KMS) für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

  Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

  - Compute KMS Viewer

Allgemeine Berechtigungen

Im Folgenden sind die Berechtigungen für das Citrix Cloud-Dienstkonto im Provisioning-Projekt für alle in MCS unterstützten Funktionen aufgeführt. Diese Berechtigungen ab jetzt die beste Kompatibilität:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
```



```
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
```



```
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
<!--NeedCopy-->
```

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezielle Informationen zur Google Cloud Platform (GCP) finden Sie unter Google Cloud Platform-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Google Cloud-Virtualisierungsumgebungen.

Verbindung zu HPE Moonshot

May 17, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf HPE Moonshot.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu HPE Moonshot herstellen, müssen Sie Ihr HPE-Konto einrichten. Siehe HPE Moonshot Virtualisierungsumgebungen.

Verbindung erstellen

Sie können zum Einrichten einer Verbindung zu HPE Moonshot Folgendes verwenden:

- Benutzeroberfläche für die vollständige Konfiguration
- PowerShell-Befehle

Verbindung mit der Schnittstelle “Vollständige Konfiguration”erstellen

1. Wählen Sie auf der Seite **Verbindung und Ressourcen hinzufügen** den Verbindungstyp **HPE Moonshot**.
2. Geben Sie die Verbindungsadresse Ihres Moonshot iLO Chassis Managers ein. Sie können eine IP-Adresse, einen Hostnamen oder einen FQDN für die Adresse verwenden.
3. Geben Sie Ihre Chassis-Administratoranmeldeinformationen und einen Verbindungsanzeigenamen ein.

Die Einrichtung der Verbindung endet, wenn eine der folgenden Situationen eintritt:

- DaaS erhält ein von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat mit Fehlern: Eine Fehlermeldung wird angezeigt. Folgen Sie den angezeigten Anweisungen, um das Problem zu lösen. Andernfalls können Sie mit der Verbindungserstellung nicht fortfahren.
- DaaS erhält ein von einer privaten Zertifizierungsstelle signiertes Zertifikat. Eine Warnseite wird angezeigt. Vergleichen Sie den empfangenen Fingerabdruck mit dem des Servers, um die Gültigkeit des Zertifikats zu ermitteln. Wenn es gültig ist, wählen Sie **Zertifikat vertrauen** und klicken Sie auf **OK**, um mit der Verbindungserstellung fortzufahren. DaaS vertraut dann dem Zertifikat und speichert den Fingerabdruck für eine zukünftige Validierung.

Verbindung mithilfe von PowerShell-Befehlen erstellen

Wenn Sie eine Verbindung über PowerShell erstellen, geben Sie die folgenden Informationen an:

- IP: HPE Server-IP-Adresse
- Username: HPE-Benutzername
- Password: HPE-Kennwort

Beispiel:

```
1 New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
2  "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
3   -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
       HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
       $UserName -sslthumbprint $SslThumbprint New-
       BrokerHypervisorConnection -HypHypervisorConnectionUid
       $HypervisorConnectionID
4 <!--NeedCopy-->
```

> **Hinweis:**
>
> Der Parameter `sslthumbprint` ist nur für von privaten ZS signierte Zertifikate erforderlich.

Zertifikat- und Fingerabdruckvalidierung

Um eine Verbindung zu **HPE Moonshot** herzustellen, darf das Zertifikat keine Fehler enthalten und der Fingerabdruck muss einen korrekten Wert haben. Im Folgenden sind die Anwendungsfälle für die Zertifikat- und Fingerabdruckvalidierung aufgeführt:

- Das von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat weist Fehler auf. Die Verbindung wird nicht erstellt. Sehen Sie sich die Fehlerdetails an und beheben Sie das Problem.
- Von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat ohne Fehler. Die Verbindung wird erstellt und der Wert von `SslThumbprints` ist **Null**.
- Von einer privaten Zertifizierungsstelle signiertes Zertifikat ohne Fehler und Wert `sslthumbprint`. Die Verbindung wird mit einem korrekten `SslThumbprints`-Wert erstellt.
- Von einer privaten ZS signiertes Zertifikat mit einem falschen Fingerabdruckwert. Die Verbindung wird nicht erstellt.
- Von einer privaten Zertifizierungsstelle signiertes Zertifikat ohne Fehler. Die Verbindung wird erstellt. `SSlThumbprints` ist **Null**, wenn die Verbindung erstellt wird. `SSlThumbprints` wird vom Sitedienst auf einen Wert aktualisiert.

Verbindungen verwalten

In diesem Abschnitt erfahren Sie, wie Sie Verbindungen verwalten können:

- Zertifikatprobleme mit der Benutzeroberfläche für die vollständige Konfiguration beheben
- Fingerabdruckwert mithilfe von PowerShell aktualisieren

Probleme mit Zertifikaten beheben

DaaS blockiert eine HPE Moonshot-Verbindung, wenn Probleme mit dem Zertifikat auftreten, und verhindert, dass Sie Workloads auf zugehörigen HPE Moonshot-Knoten bereitstellen und verwalten können. In der Liste der **Hostverbindungen** wird neben der Verbindung ein Fehlersymbol angezeigt. In der folgenden Tabelle finden Sie spezifische Probleme und Lösungen.

Problem	Lösung
Fehler im von einer öffentlichen Zertifizierungsstelle signierten Zertifikat	Klicken Sie auf die Verbindung und wählen Sie die Registerkarte **Problembehandlung**. Sehen Sie sich die Fehlerdetails an und beheben Sie das Problem.

Problem	Lösung
Empfangenes Zertifikat wurde von einer privaten Zertifizierungsstelle signiert oder ist abgelaufen.	Bearbeiten Sie die Hostverbindung, um den Fingerabdruck des Zertifikats zu aktualisieren. Verfahren 1. Wählen Sie die Verbindung und klicken Sie auf **Verbindung bearbeiten**. 1. Klicken Sie auf der Seite **Verbindungseigenschaften** auf **Einstellungen bearbeiten**. 1. Geben Sie das Kennwort ein, um eine Verbindung zum HPE Moonshot-Chassis herzustellen, und klicken Sie auf **Speichern**. 1. Vergleichen Sie auf der Seite **Warnung** den empfangenen Fingerabdruck mit dem des Servers hinsichtlich der Gültigkeit des Zertifikats. 1. Sind beide identisch, wählen Sie **Zertifakt vertrauen** und klicken Sie auf **OK**.

Fingerabdruckwert aktualisieren

Nach dem Erstellen einer Verbindung können Sie deren Fingerabdruckwert mithilfe des PowerShell-Befehls `Set-Item` aktualisieren. Führen Sie beispielsweise die folgenden Befehle aus:

1. Abrufen der Verbindungsdetails. Beispiel:

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
2 <!--NeedCopy-->
```

2. Aktualisieren des Fingerabdruckwerts. Beispiel:

```
1 Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
      Administrator -SslThumbprint
     xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
2 <!--NeedCopy-->
```

3. Überprüfen des aktualisierten Fingerabdruckwerts. Beispiel:

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```



```
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Update schlägt fehl, wenn der Befehl `Set-Item` einen falschen Fingerabdruckwert enthält.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezifische Informationen zu HPE Moonshot finden Sie unter HPE Moonshot-Maschinenkatalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- HPE Moonshot-Virtualisierungsumgebungen

Verbindung zu Microsoft Azure

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Microsoft Azure herstellen, müssen Sie Ihr Azure-Konto als Ressourcenstandort eingerichtet haben. Weitere Informationen finden Sie unter Microsoft Azure Resource Manager-Virtualisierungsumgebungen.

Dienstprinzipale und Verbindungen erstellen

Bevor Sie Verbindungen erstellen, müssen Sie Dienstprinzipale einrichten, über die Verbindungen auf Azure-Ressourcen zugreifen. Es gibt zwei Optionen zum Erstellen einer Verbindung:

- Dienstprinzipal und Verbindung gemeinsam in "Vollständige Konfiguration"erstellen
- Verbindung mithilfe eines zuvor erstellten Dienstprinzipals erstellen

In diesem Abschnitt erfahren Sie, wie Sie diese Aufgaben ausführen:

- Dienstprinzipal und Verbindung gemeinsam in "Vollständige Konfiguration"erstellen
- Dienstprinzipal mithilfe von PowerShell erstellen
- Anwendungsgeheimnis in Azure abrufen
- Verbindung mithilfe von vorhandenem Dienstprinzipal erstellen

Überlegungen

Bevor Sie beginnen, sollten Sie Folgendes berücksichtigen:

- Citrix empfiehlt, Dienstprinzipale mit der Rolle *Mitwirkender* zu verwenden. Beachten Sie jedoch die Liste der Mindestberechtigungen im Abschnitt Mindestberechtigungen.
- Beim Erstellen der ersten Verbindung fordert Azure Sie auf, die erforderlichen Berechtigungen zu erteilen. Sie müssen sich für zukünftige Verbindungen neu authentifizieren, Ihre Zustimmung wird jedoch in Azure gespeichert und die Aufforderung nicht wieder angezeigt.
- Nachdem Sie sich zum ersten Mal bei Azure authentifiziert haben, wird eine Citrix-eigene Mehrmandanten-Anwendung (ID: `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`) im Namen des authentifizierten Kontos in Ihr Azure Active Directory eingeladen. Citrix verwendet diese Anwendung, um neue Dienstprinzipale zu erstellen und die richtigen Berechtigungen für die Workload-Bereitstellung und die Azure AD-Geräteverwaltung zu gewähren, wenn Sie auf der Seite **Verbindungsdetails** die Option **Verwaltung in Azure AD eingebundener Geräte aktivieren** auswählen.
- Für die Authentifizierung verwendete Konten müssen Co-Administrator des Abonnements sein.
- Das für die Authentifizierung verwendete Konto muss Mitglied des Verzeichnisses des Abonnements sein. Es gibt zwei Arten von Konten, auf die Sie achten sollten: "Arbeitsplatz oder Schule"und "Persönliches Microsoft-Konto". Weitere Informationen finden Sie unter CTX219211.
- Sie können zwar ein bestehendes Microsoft-Konto als Mitglied des Abonnementverzeichnisses hinzufügen und verwenden, doch kann es zu Komplikationen kommen, wenn dem Konto zuvor Gastzugriff auf eine der Verzeichnisressourcen gewährt worden war. In diesem Fall besitzt das Konto möglicherweise einen Platzhaltereintrag im Verzeichnis, der nicht die erforderlichen Berechtigungen gewährt, und es wird ein Fehler zurückgegeben.

  Entfernen Sie die Ressourcen aus dem Verzeichnis und fügen Sie sie wieder hinzu, um das Problem zu beheben. Dabei ist jedoch Vorsicht geboten, denn dies hat unbeabsichtigte Auswirkungen auf andere Ressourcen, auf die das Konto zugreifen kann.

- Es gibt ein bekanntes Problem, bei dem bestimmte Konten, die eigentlich Mitglieder sind, als Verzeichnisgäste erkannt werden. Konfigurationen wie diese treten normalerweise bei älteren Verzeichniskonten auf. Fügen Sie als Workaround dem Verzeichnis jeweils ein Konto hinzu, das den richtigen Mitgliedschaftswert erhält.
- Ressourcengruppen sind Container für Ressourcen und können Ressourcen aus ihrer eigenen und aus anderen Regionen enthalten. Dies kann Verwirrung auslösen, wenn Sie erwarten, dass die in der Region einer Ressourcengruppe angezeigten Ressourcen verfügbar sind.
- Stellen Sie sicher, dass Ihr Netzwerk und Subnetz groß genug zum Hosten der benötigten Maschinenzahl ist. Dies erfordert einiges an Vorausschau, doch Microsoft kann Ihnen bei der Wahl der richtigen Werte und der Planung der erforderlichen Adressraumkapazität helfen.

Dienstprinzipal und Verbindung gemeinsam in "Vollständige Konfiguration"erstellen

> **Wichtig:**
>
> Dieses Feature ist für chinesische Azure-Abonnements noch nicht verfügbar.

In "Vollständige Konfiguration"können Sie Dienstprinzipal und Verbindung in einem einzigen Workflow erstellen. Dienstprinzipale gewähren Verbindungen Zugriff auf Azure-Ressourcen. Wenn Sie sich bei Azure authentifizieren, um einen Dienstprinzipal zu erstellen, wird eine Anwendung in Azure registriert. Für die registrierte Anwendung wird ein geheimer Schlüssel erstellt (*geheimer Clientschlüssel* oder *Anwendungsgeheimnis*). Die registrierte Anwendung (in diesem Fall eine *Verbindung*) verwendet den geheimen Clientschlüssel zur Authentifizierung bei Azure AD.

Stellen Sie vor Beginn sicher, dass Sie die folgenden Voraussetzungen erfüllen:

- Sie haben ein Benutzerkonto des Azure Active Directory-Mandanten Ihres Abonnements.
- Das Azure Active Directory-Benutzerkonto ist Co-Administrator des Azure-Abonnements, das Sie für die Bereitstellung von Ressourcen verwenden möchten.
- Sie haben globale Administrator-, Anwendungsadministrator- oder Anwendungsentwicklerberechtigungen für die Authentifizierung. Die Berechtigungen können widerrufen werden, nachdem Sie eine Hostverbindung erstellt haben. Weitere Informationen zu Rollen finden Sie unter Integrierte Azure AD-Rollen.

Verwenden Sie den Assistenten für **Verbindung und Ressourcen hinzufügen**, um Dienstprinzipal und Verbindung gemeinsam zu erstellen:

1. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen**, als Verbindungstyp **Microsoft Azure** und Ihre Azure-Umgebung.
2. Wählen Sie die Tools, die zum Erstellen der virtuellen Maschinen verwendet werden sollen, und wählen Sie dann **Weiter**.

3. Erstellen Sie auf der Seite **Verbindungsdetails** einen Dienstprinzipal und legen Sie den Verbindungsnamen wie folgt fest:

   a) Zum Gewähren der Verbindungsberechtigung für die automatische Bereinigung veralteter in Azure AD eingebundener Geräte wählen Sie **Verwaltung in Azure AD eingebundener Geräte aktivieren**. Wir empfehlen, diese Option auszuwählen, wenn Sie über diese Verbindung in Azure AD eingebundene Maschinen erstellen möchten. Weitere Informationen finden Sie unter Verwaltung in Azure AD eingebundener Geräte aktivieren.

   b) Geben Sie die ID Ihres Azure-Abonnements und einen Namen für die Verbindung ein. Nachdem Sie die Abonnement-ID eingegeben haben, wird die Schaltfläche **Neu erstellen** verfügbar.

   > **Hinweis:**
   >
   > Der Verbindungsname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } " '()'`

   a) Wählen Sie **Neu erstellen** und geben Sie den Benutzernamen und das Kennwort des Azure Active Directory-Kontos ein.

   b) Wählen Sie **Anmelden**.

   c) Wählen Sie **Akzeptieren**, um Citrix DaaS die aufgelisteten Berechtigungen zu erteilen. In Azure wird ein Dienstprinzipal erstellt, der Citrix DaaS die Verwaltung von Azure-Ressourcen für den angegebenen Benutzer ermöglicht.

   d) Nach Auswahl von **Akzeptieren** kehren Sie zur Seite **Verbindungsdetails** zurück.

   > **Hinweis:**
   >
   > Nachdem Sie sich bei Azure authentifiziert haben, werden die Schaltflächen **Neu erstellen** und **Vorhandene verwenden** ausgeblendet. Der Text **Verbindung erfolgreich** und ein grünes Häkchen zeigen die erfolgreiche Verbindung mit Ihrem Azure-Abonnement an.

   e) Um API-Anforderungen über Citrix Cloud Connectors an Azure weiterzuleiten, aktivieren Sie das Kontrollkästchen **Datenverkehr über Citrix Cloud Connectors weiterleiten**.

   Alternativ können Sie das Feature mit PowerShell aktivieren. Weitere Informationen finden Sie unter Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen.

   > **Hinweis:**

> Diese Option ist nur verfügbar, wenn die Bereitstellung aktive Citrix Cloud Connectors enthält. Derzeit wird dieses Feature für Connector Appliances nicht unterstützt.

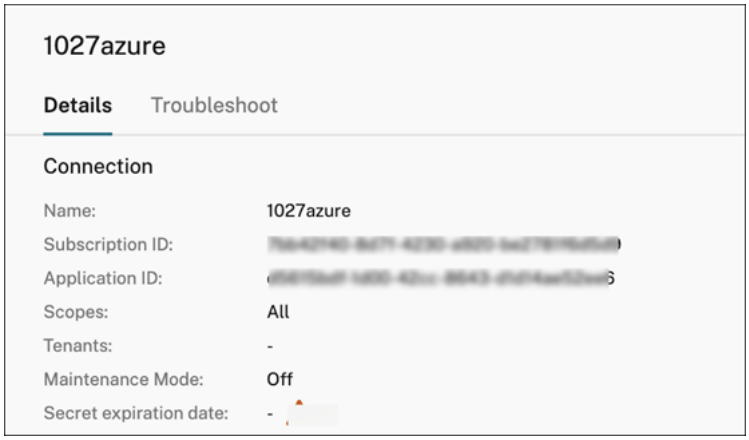
f) Wählen Sie **Weiter**.

> **Hinweis:**
>
> Sie können im Assistenten erst fortfahren, wenn Sie sich bei Azure authentifiziert und die Erteilung der erforderlichen Berechtigungen akzeptiert haben.

4. Konfigurieren Sie die Verbindungsressourcen wie folgt:
   - Wählen Sie auf der Seite **Region** eine Region aus.
   - Gehen Sie auf der Seite **Netzwerk** wie folgt vor:
     - Geben Sie einen Ressourcennamen zur Identifizierung der Kombination aus Region und Netzwerk ein. Der Name muss aus 1–64 Zeichen bestehen. Der Ressourcenname darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } "'()'`.
     - Wählen Sie eine Kombination aus virtuellem Netzwerk und Ressourcengruppe. (Wenn Sie mehrere virtuelle Netzwerke mit dem gleichen Namen haben, erzielen Sie durch die Kombination aus Netzwerknamen und Ressourcengruppe Einmaligkeit.) Wenn die auf der vorherigen Seite ausgewählte Region keine virtuellen Netzwerke enthält, kehren Sie zu der Seite zurück und wählen Sie eine Region, die virtuelle Netzwerke enthält.
5. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen und wählen Sie **Fertig stellen**, um die Einrichtung abzuschließen.

Anzeigen der Anwendungs-ID Nachdem Sie eine Verbindung erstellt haben, können Sie die Anwendungs-ID einsehen, die die Verbindung für den Zugriff auf Azure-Ressourcen verwendet.

Wählen Sie in der Liste **Verbindung und Ressourcen hinzufügen** die Verbindung aus, um die Details anzuzeigen. Auf der Registerkarte **Details** wird die Anwendungs-ID angezeigt.



Dienstprinzipal mithilfe von PowerShell erstellen

Zum Erstellen eines Dienstprinzipals mit PowerShell stellen Sie zunächst eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her. Verwenden Sie dann die nachfolgend aufgeführten PowerShell-Cmdlets.

Stellen Sie sicher, dass Sie diese Elemente verfügbar haben:

- **SubscriptionId:** Azure Resource Manager-`SubscriptionID` des Abonnements, für das Sie VDAs bereitstellen möchten.
- **ActiveDirectoryID:** Mandanten-ID der Anwendung ein, die Sie bei Azure AD registriert haben.
- **ApplicationName:** Name der Anwendung, die in Azure AD erstellt werden soll.

Verfahren:

1. Stellen Sie eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her.

   ```
   Connect-AzAccount
   ```

2. Wählen Sie das Azure Resource Manager-Abonnement, in dem Sie den Dienstprinzipal erstellen möchten.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

3. Erstellen Sie die Anwendung im AD-Mandanten.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. Erstellen Sie einen Dienstprinzipal.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. Weisen Sie dem Dienstprinzipal eine Rolle zu.


```
New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
 $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
```

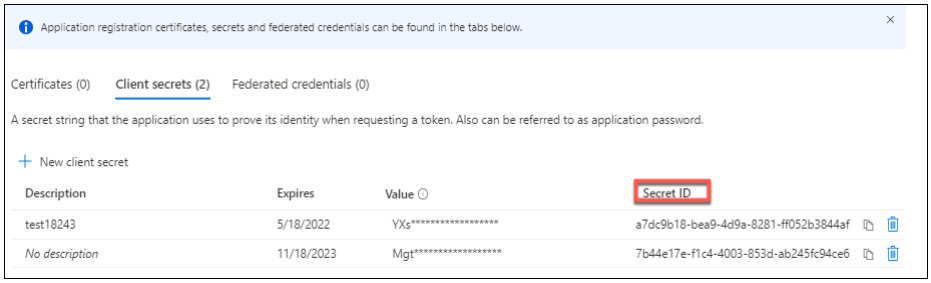
6. Notieren Sie die im Ausgabefenster der PowerShell-Konsole angezeigte Anwendungs-ID (ApplicationId). Sie müssen diese ID beim Erstellen der Hostverbindung angeben.

Anwendungsgeheimnis in Azure abrufen

Um eine Verbindung über einen vorhandenen Dienstprinzipal herzustellen, müssen Sie zunächst die Anwendungs-ID und das Anwendungsgeheimnis des Dienstprinzipals im Azure-Portal abrufen.

Verfahren:

1. Rufen Sie die **Anwendungs-ID** über die Benutzeroberfläche “Vollständige Konfiguration”oder mithilfe von PowerShell ab.
2. Melden Sie sich beim Azure-Portal an.
3. Wählen Sie in **Azure Active Directory**.
4. Wählen Sie in Azure AD unter **App registrations** Ihre Anwendung aus.
5. Gehen Sie zu **Certificates & secrets**.
6. Klicken Sie auf **Client secrets**.



Verbindung mithilfe von vorhandenem Dienstprinzipal erstellen

Wenn Sie bereits über einen Dienstprinzipal verfügen, können Sie ihn verwenden, um in “Vollständige Konfiguration”eine Verbindung herzustellen.

Stellen Sie sicher, dass Sie diese Elemente verfügbar haben:

- Abonnement-ID
- ActiveDirectory-ID (Mandanten-ID)
- Anwendungs-ID
- Anwendungsgeheimnis

  Weitere Informationen finden Sie unter Anwendungsgeheimnis abrufen.

- Ablaufdatum des Geheimnisses

Verfahren:

Führen Sie im Assistenten **Verbindung und Ressourcen hinzufügen** folgende Schritte aus:

1. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen**, als Verbindungstyp **Microsoft Azure** und Ihre Azure-Umgebung.
2. Wählen Sie die Tools, die zum Erstellen der virtuellen Maschinen verwendet werden sollen, und wählen Sie dann **Weiter**.
3. Geben Sie auf der Seite **Verbindungsdetails** die ID Ihres Azure-Abonnements und einen Namen für die Verbindung ein.

   > **Hinweis:**
   >
   > Der Verbindungsname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } " '()'`

4. Wählen Sie **Vorhandene verwenden**. Geben Sie im Fenster **Vorhandene Dienstprinzipaldetails** die folgenden Einstellungen für den bestehenden Dienstprinzipal ein. Nachdem Sie die Details eingegeben haben, ist die Schaltfläche **Speichern** aktiviert. Wählen Sie **Speichern**. Sie können erst fortfahren, wenn Sie gültige Angaben gemacht haben.

   - **Abonnement-ID**. Geben Sie Ihre Azure-Abonnement-ID ein. Um Ihre Abonnement-ID zu erhalten, melden Sie sich beim Azure-Portal an und gehen Sie zu **Abonnements > Übersicht**.
   - **Active Directory-ID** (Mandanten-ID). Geben Sie die Verzeichnis-ID (Mandanten-ID) der Anwendung ein, die Sie bei Azure AD registriert haben.
   - **Anwendungs-ID**. Geben Sie die Anwendungs-ID (Client-ID) der Anwendung ein, die Sie bei Azure AD registriert haben.
   - **Anwendungsgeheimnis**. Geben Sie einen geheimen Clientschlüssel ein. Die registrierte Anwendung verwendet den Schlüssel zur Authentifizierung bei Azure AD. Es wird empfohlen, Schlüssel aus Sicherheitsgründen regelmäßig zu ändern. Speichern Sie den Schlüssel unbedingt, da Sie ihn später nicht abrufen können.
   - **Ablaufdatum des Geheimnisses.** Geben Sie das Datum ein, nach dem das Anwendungsgeheimnis abläuft. Sie erhalten eine Warnung in der Konsole, bevor der geheime Schlüssel abläuft. Wenn der geheime Schlüssel abläuft, erhalten Sie Fehler.

> **Hinweis:**
>
> Aus Sicherheitsgründen darf das Ablaufdatum nicht mehr als zwei Jahre in der Zukunft liegen.

- **Authentifizierungs-URL**. Dieses Feld wird automatisch ausgefüllt und kann nicht bearbeitet werden.
- **Verwaltungs-URL**. Dieses Feld wird automatisch ausgefüllt und kann nicht bearbeitet werden.
- **Speichersuffix**. Dieses Feld wird automatisch ausgefüllt und kann nicht bearbeitet werden.

  Für die Erstellung eines MCS-Katalogs in Azure ist Zugriff auf die folgenden Endpunkte erforderlich. Durch Zugriff auf diese Endpunkte wird die Konnektivität zwischen Ihrem Netzwerk und dem Azure-Portal und seinen Diensten optimiert.

  - Authentifizierungs-URL: https://login.microsoftonline.com/
  - Verwaltungs-URL: https://management.azure.com/. Dies ist eine Anforderungs-URL für Azure Resource Manager-Anbieter-APIs. Der Endpunkt für die Verwaltung hängt von der Umgebung ab. Für Azure Global ist dies beispielsweise https://management.azure.com/, und für Azure US Government ist es https://management.usgovcloudapi.net/.
  - Speichersuffix: https://*.core.windows.net./. Dieses (*) ist ein Platzhalterzeichen für das Speichersuffix. Beispiel: https://demo.table.core.windows.net/.

5. Nachdem Sie **Speichern** gewählt haben, wird die Seite **Verbindungsdetails** wieder angezeigt. Wählen Sie **Weiter**, um mit der nächsten Seite fortzufahren.
6. Konfigurieren Sie die Verbindungsressourcen wie folgt:

   - Wählen Sie auf der Seite **Region** eine Region aus.
   - Gehen Sie auf der Seite **Netzwerk** wie folgt vor:
     - Geben Sie einen Ressourcennamen zur Identifizierung der Kombination aus Region und Netzwerk ein. Der Name muss aus 1–64 Zeichen bestehen. Der Ressourcenname darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } "'()'`.
     - Wählen Sie eine Kombination aus virtuellem Netzwerk und Ressourcengruppe. (Wenn Sie mehrere virtuelle Netzwerke mit dem gleichen Namen haben, erzielen Sie durch die Kombination aus Netzwerknamen und Ressourcengruppe Einmaligkeit.) Wenn die auf der vorherigen Seite ausgewählte Region keine virtuellen Netzwerke enthält, kehren Sie zu der Seite zurück und wählen Sie eine Region, die virtuelle Netzwerke enthält.

7. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen und wählen Sie **Fertig stellen**, um die Einrichtung abzuschließen.

Dienstprinzipale und Verbindungen verwalten

In diesem Abschnitt erfahren Sie, wie Sie Dienstprinzipale und Verbindungen verwalten können:

- Einstellungen für Azure-Drosselung konfigurieren
- Verwaltung in Azure AD eingebundener Geräte aktivieren
- Dienstprinzipal einer bestehenden Hosting-Verbindung verwalten
- Imagefreigabe in Azure aktivieren
- Gemeinsam genutzte Mandanten mithilfe der vollständigen Konfiguration zu einer Verbindung hinzufügen
- Image-Freigabe mithilfe von PowerShell implementieren
- Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen
- Anwendungsgeheimnis und Ablaufdatum für Geheimnis verwalten

Einstellungen für Azure-Drosselung konfigurieren

Azure Resource Manager drosselt Anforderungen von Abonnements und Mandanten durch das Routing von Datenverkehr gemäß Grenzwerten, die auf die spezifischen Anforderungen des Anbieters zugeschnitten sind. Weitere Informationen finden Sie auf der Website von Microsoft unter Drosseln von Resource Manager-Anforderungen. Es gibt Grenzwerte für Abonnements und Mandanten, wenn die Verwaltung zahlreicher Maschinen problematisch werden kann. Beispielsweise können bei einem Abonnement mit zahlreichen Maschinen Leistungsprobleme im Zusammenhang mit Energievorgängen auftreten.

> **Tipp:**
>
> Weitere Informationen finden Sie unter Verbessern der Azure-Leistung mit Maschinenerstellungsdiensten.

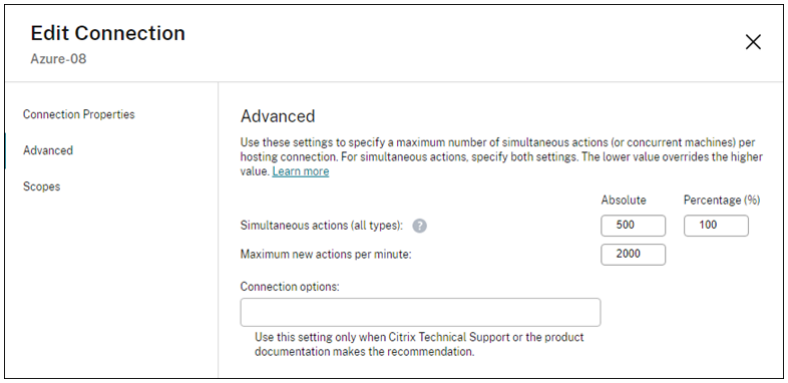
Zur Lösung solcher Probleme können Sie in Citrix DaaS die interne MCS-Einschränkung entfernen, um das Azure-Anforderungskontingent stärker zu nutzen.

Für große Abonnements (z. B. mit 1000 oder mehr VMs) empfehlen wir die folgenden optimalen Einstellungen für das Ein- und Ausschalten von VMs:

- Absolute gleichzeitige Operationen: 500
- Maximale neue Operationen pro Minute: 2000
- Maximale Gleichzeitigkeit von Operationen: 500

Verwenden Sie die Oberfläche “Vollständige Konfiguration”, um Azure-Operationen für eine Hostverbindung zu konfigurieren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie eine Azure-bezogene Verbindung zur Bearbeitung aus.
3. Wählen Sie **Erweitert** im Assistenten **Verbindung bearbeiten**.
4. Geben Sie auf der Seite **Erweitert** die Anzahl gleichzeitiger Aktionen, die maximale Anzahl neuer Aktionen pro Minute und ggf. weitere Verbindungsoptionen an.



MCS unterstützt standardmäßig maximal 500 gleichzeitige Vorgänge. Alternativ können Sie mit dem Remote PowerShell SDK die maximale Anzahl gleichzeitiger Vorgänge festlegen.

Geben Sie über die **PowerShell**-Eigenschaft `MaximumConcurrentProvisioningOperations` die maximale Anzahl gleichzeitiger Azure-Provisioningvorgänge an. Beachten Sie Folgendes bei der Verwendung dieser Eigenschaft:

- Der Standardwert von `MaximumConcurrentProvisioningOperations` ist 500.
- Konfigurieren Sie den Parameter `MaximumConcurrentProvisioningOperations` mit dem PowerShell-Befehl `Set-item`.

Verwaltung in Azure AD eingebundener Geräte aktivieren

Veraltete, in Azure AD eingebundene Geräte können den Beitritt neuer Maschinen zu Azure AD verhindern und dazu führen, dass diese nicht ordnungsgemäß funktionieren. Um Probleme zu vermeiden, können Sie zulassen, dass Verbindungen in Azure AD eingebundene Geräte verwalten. Mit dieser Berechtigung können Verbindungen veraltete, in Azure AD eingebundene Geräte automatisch bereinigen.

> **Hinweis:**
>
> In Azure AD eingebundene Geräte können nicht aus Azure AD gelöscht werden, wenn Sie Maschinen oder Maschinenkataloge löschen.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich “Hosting”aus.

2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung bearbeiten** aus.
3. Wählen Sie im linken Bereich **Verbindungseigenschaften**.
4. Gehen Sie auf der Seite **Verbindungseigenschaften** wie folgt vor:

    a) Wählen Sie **Verwaltung in Azure AD eingebundener Geräte aktivieren**.

    b) Klicken Sie auf **Speichern**.

    c) Geben Sie in dem nun angezeigten Azure-Anmeldefenster Ihr Abonnementkennwort ein und klicken Sie auf **Anmelden**.

    Nach Abschluss der Anmeldung wird wieder die Liste der Hostingverbindungen und Ressourcen angezeigt. Klicken Sie in der Liste auf die Verbindung und dann im unteren Bereich auf die Registerkarte **Details**. Sie können sehen, dass das Feld für die **Verwaltung in Azure AD eingebundener Geräte** als **Aktiviert** angezeigt wird.

Wenn Sie in "Vollständige Konfiguration"die Verwaltung in Azure AD eingebundener Geräte aktivieren, müssen Sie sich unabhängig vom gewählten Verfahren zur Erstellung der Hostverbindung ("Neu erstellen"oder "Vorhandene verwenden") bei Azure AD authentifizieren. Die in Azure AD integrierte Rolle **Cloudgeräteadministrator** ist dem Dienstprinzipal zugewiesen. Um stattdessen Mindestberechtigungen zur Verwaltung in Azure AD eingebundener Geräte festzulegen, können Sie die zugewiesene Rolle **Cloudgeräteadministrator** manuell aus dem Dienstprinzipal entfernen, eine benutzerdefinierte Azure AD-Rolle erstellen, die nur die Mindestberechtigungen enthält, und diese dem Dienstprinzipal zuweisen.

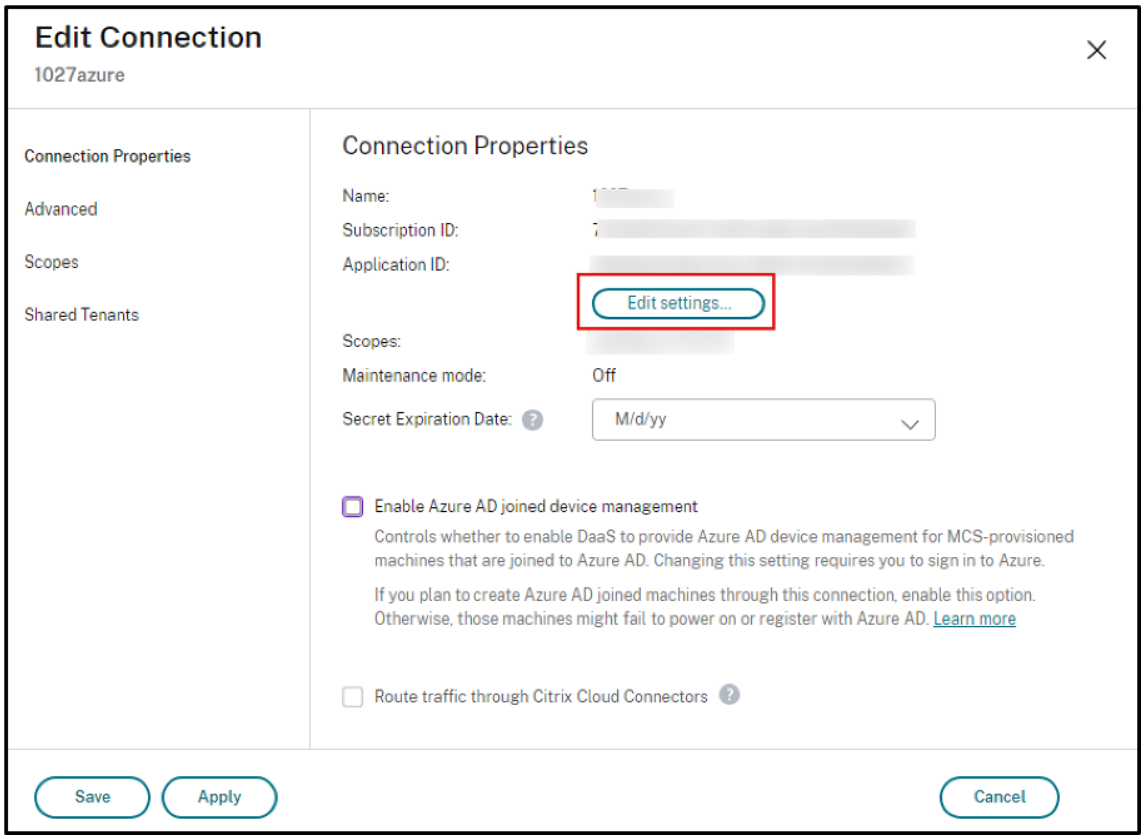
> **Hinweis:**
>
> - Die Mindestberechtigungen zur Verwaltung in Azure AD eingebundener Geräte sind Azure AD-Berechtigungen und nicht die Azure Resource Manager-Berechtigungen. Sie können einem Dienstprinzipal nicht explizit zugewiesen werden. Sie müssen in Azure AD eine benutzerdefinierte Rolle erstellen, die diese Berechtigungen enthält, und diese Rolle dem Dienstprinzipal zuweisen. Weitere Informationen finden Sie unter Create and assign a custom role in Azure Active Directory.
> - Um eine benutzerdefinierte Rolle in Azure AD zu erstellen, benötigen Sie eine Azure AD Premium P1- oder P2-Lizenz.

Dienstprinzipal einer bestehenden Hosting-Verbindung verwalten

Nachdem Sie eine Hosting-Verbindung mit einem Dienstprinzipal erstellt haben, können Sie die Hosting-Verbindung so bearbeiten, dass sie über Folgendes verfügt:

- Neuer Dienstprinzipal
- Verwenden Sie einen anderen vorhandenen Dienstprinzipal

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting** aus.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung bearbeiten** aus.
3. Wählen Sie im linken Bereich **Verbindungseigenschaften**.
4. Klicken Sie auf der Seite **Verbindungseigenschaften** auf **Einstellungen bearbeiten**. Sie können jetzt wählen, ob Sie einen neuen Dienstprinzipal erstellen oder einen anderen vorhandenen Dienstprinzipal verwenden möchten.



- Klicken Sie auf **Dienstprinzipal erstellen**, um einen neuen Dienstprinzipal zu erstellen. Folgen Sie der Aufforderung, um sich bei Ihrem Azure AD-Benutzerkonto anzumelden. Citrix verwendet die Mehrmandanten-Anwendungs-ID `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`, um einen neuen Dienstprinzipal für die bestehende Hostverbindung zu erstellen und die entsprechenden Berechtigungen zu erteilen.

  Wenn Sie auf der Seite **Verbindungseigenschaften** die Option **Verwaltung in Azure AD eingebundener Geräte aktivieren** auswählen, wird die in Azure AD integrierte Cloud-Geräteadministrator-Rolle dem neu erstellten Dienstprinzipal zugewiesen.

- Klicken Sie auf **Vorhandene verwenden**, um einen anderen vorhandenen Dienstprinzipal für diese Hosting-Verbindung zu verwenden. Es gibt jedoch zwei Szenarien:

  - Wenn Sie **Verwaltung in Azure AD eingebundener Geräte aktivieren** auswählen, werden Sie aufgefordert, sich bei Ihrem Azure AD-Benutzerkonto anzumelden. Citrix

verwendet die Mehrmandanten-Anwendungs-ID `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`, um dem vorhandenen Dienstprinzipal die in Azure AD integrierte Cloud-Geräteadministrator-Rolle zuzuweisen.

- Wenn Sie **Verwaltung in Azure AD eingebundener Geräte aktivieren** nicht auswählen, werden Sie nicht aufgefordert, sich bei Ihrem Azure AD-Benutzerkonto anzumelden. Geben Sie die Anwendungs-ID und das Geheimnis für diesen vorhandenen Dienstprinzipal ein.

Weitere Informationen zur Aktivierung der Verwaltung in Azure AD eingebundener Geräte finden Sie unter Verwaltung in Azure AD eingebundener Geräte aktivieren.

Imagefreigabe in Azure aktivieren

Beim Erstellen oder Aktualisieren von Maschinenkatalogen können Sie per Azure Compute Gallery freigegebene Images aus anderen Azure-Mandanten und -Abonnements auswählen. Um die Imagefreigabe innerhalb oder zwischen Mandanten zu aktivieren, müssen Sie die erforderlichen Einstellungen in Azure vornehmen:

- Images innerhalb eines Mandanten freigeben (abonnementübergreifend)
- Images mandantenübergreifend freigeben

Images innerhalb eines Mandanten freigeben (abonnementübergreifend) Um ein Image in Azure Compute Gallery auszuwählen, das zu einem anderen Abonnement gehört, muss es für den Dienstprinzipal (SPN) dieses Abonnements freigegeben werden.

Dienstprinzipal SPN 1 ist in Studio beispielsweise wie folgt konfiguriert:

Dienstprinzipal: SPN 1

Abonnement: Abonnement 1

Mandant: Mandant 1

Das Image ist in einem anderen Abonnement, was in Studio wie folgt konfiguriert ist:

Abonnement: Abonnement 2

Mandant: Mandant 1

Wenn Sie das Image in Abonnement 2 für Abonnement 1 (SPN 1) freigeben möchten, gehen Sie zu Abonnement 2 und geben Sie die Ressourcengruppe für SPN1 frei.

Die Imagefreigabe muss über die rollenbasierte Zugriffssteuerung (RBAC) von Azure erfolgen. Azure RBAC ist das bei der Verwaltung des Zugriffs auf Azure-Ressourcen verwendete Autorisierungssystem. Weitere Informationen zu Azure RBAC finden Sie im Microsoft-Dokument Was ist die rollenbasierte Zugriffssteuerung in Azure (Azure Role-Based Access Control, Azure RBAC)?. Um Zugriff zu gewähren,

weisen Sie Dienstprinzipals Rollen im Bereich der Ressourcengruppe mit der Rolle "Mitwirkender" zu. Um Azure-Rollen zuzuweisen, benötigen Sie die Berechtigung `Microsoft.Authorization/roleAssignments/write` (z. B. als Benutzerzugriffsadministrator oder Besitzer). Weitere Informationen zum Freigeben von Images für andere SPNs finden Sie im Microsoft-Dokument Zuweisen von Azure-Rollen über das Azure-Portal.

Images mandantenübergreifend freigeben Um Images mit Azure Compute Gallery für andere Mandaten freizugeben, erstellen Sie eine Anwendungsregistrierung.

Wenn beispielsweise zwei Mandanten vorliegen (Mandant 1 und Mandant 2) und Sie Ihren Image-Katalog mit Mandant 1 teilen möchten, gehen Sie wie folgt vor:

1. Erstellen Sie eine Anwendungsregistrierung für Mandant 1. Weitere Informationen finden Sie unter Create the app registration.
2. Fordern Sie über einen Browser eine Anmeldung an, um Mandant 2 Zugriff auf die Anwendung zu geben. Ersetzen Sie `Tenant2 ID` durch die ID von Mandant 1. Ersetzen Sie `Application (client) ID` durch die Anwendungs-ID der von Ihnen erstellten Anwendungsregistrierung. Wenn Sie die IDs ersetzt haben, fügen Sie die URL in einen Browser ein und folgen Sie den Schritten zum Anmelden bei Mandant 2. Beispiel:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
       client_id=<Application (client) ID>&response_type=code&
       redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   <!--NeedCopy-->
   ```

   Weitere Informationen finden Sie unter Give Tenant 2 access.
3. Gewähren Sie der Anwendung Zugriff auf die Ressourcengruppe von Mandant 2. Melden Sie sich als Mandant 2 an und gewähren Sie der Anwendungsregistrierung Zugriff auf die Ressourcengruppe, die das Katalogimage enthält. Weitere Informationen finden Sie unter Authenticate requests across tenants.

Gemeinsam genutzte Mandanten mithilfe der vollständigen Konfiguration zu einer Verbindung hinzufügen

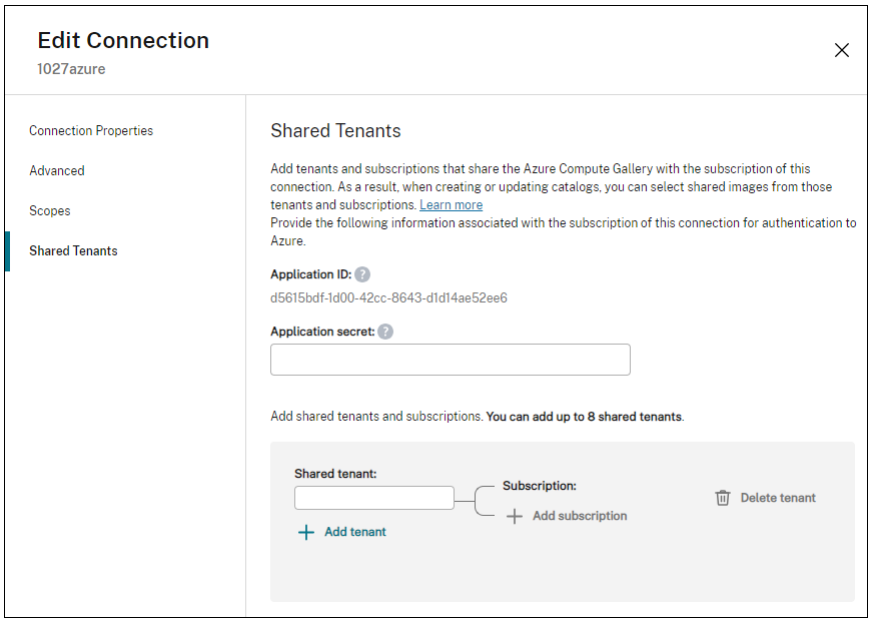
Beim Erstellen oder Aktualisieren von Maschinenkatalogen in der Benutzeroberfläche für die vollständige Konfiguration können Sie per Azure Compute Gallery freigegebene Images aus anderen Azure-Mandanten und -Abonnements auswählen. Für dieses Feature müssen Sie Informationen zu freigegebenen Mandanten und Abonnements für zugehörige Hostverbindungen angeben.

> **Hinweis:**
>
> Vergewissern Sie sich, dass Sie die erforderlichen Einstellungen in Azure vorgenommen haben,

> um die Imagefreigabe innerhalb oder zwischen Mandanten zu aktivieren. Weitere Informationen finden Sie unter Images mandantenübergreifend freigeben.

Führen Sie die folgenden Schritte für eine Verbindung aus:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung bearbeiten** aus.



3. Führen Sie unter **Freigegebene Mandanten** die folgenden Schritte aus:
   a) Geben Sie die dem Abonnement der Verbindung zugeordnete Anwendungs-ID und das Anwendungsgeheimnis an. DaaS verwendet diese Informationen zur Authentifizierung bei Azure AD.
   b) Fügen Sie Mandanten und Abonnements hinzu, die sich die Azure Compute Gallery mit dem Abonnement der Verbindung teilen. Sie können bis zu acht freigegebene Mandanten und acht Abonnements für jeden Mandanten hinzufügen.
4. Abschließend wählen Sie entweder **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Image-Freigabe mithilfe von PowerShell implementieren

Dieser Abschnitt erläutert die Prozesse zur Image-Freigabe mithilfe von PowerShell:

- Image aus einem anderen Abonnement auswählen

- Benutzerdefinierte Eigenschaften der Hostverbindung mit IDs für freigegebene Mandanten aktualisieren
- Image eines anderen Mandanten auswählen

Image aus einem anderen Abonnement auswählen Sie können in Azure Compute Gallery ein Image auswählen, das zu einem anderen freigegebenen Abonnement im selben Azure-Mandanten gehört, um MCS-Kataloge mit PowerShell-Befehlen zu erstellen und zu aktualisieren.

1. Im Stammordner der Hostingeinheit erstellt Citrix einen neuen freigegebenen Abonnementordner unter dem Namen `sharedsubscription`.
2. Listen Sie alle freigegebenen Abonnements im Mandanten auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
<!--NeedCopy-->
```

3. Wählen Sie ein freigegebenes Abonnement und listen Sie dann alle freigegebenen Ressourcengruppen dieses Abonnements auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
<!--NeedCopy-->
```

4. Wählen Sie eine Ressourcengruppe und listen Sie dann alle Kataloge in der Ressourcengruppe auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Wählen Sie einen Katalog und listen Sie dann alle Imagedefinitionen des Katalogs auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Wählen Sie eine Imagedefinition und listen Sie dann alle Imageversionen der Imagedefinition auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
<!--NeedCopy-->
```

7. Zum Erstellen und Aktualisieren eines MCS-Katalogs verwenden Sie die folgenden Elemente:

   - Ressourcengruppe
   - Katalog

- Katalogimagedefinition
- Katalogimageversion

Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Benutzerdefinierte Eigenschaften der Hostverbindung mit IDs für freigegebene Mandanten aktualisieren Mit `Set-Item` können Sie die benutzerdefinierten Eigenschaften der Hostverbindung mit den IDs der freigegebenen Mandanten und den Abonnement-IDs aktualisieren. Fügen Sie eine Eigenschaft `SharedTenants` in `CustomProperties` hinzu. Das Format von `Shared Tenants` ist:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

Beispiel:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```


> **Hinweis:**
>
> Sie können mehrere Mandanten hinzufügen. Jeder Mandant kann mehrere Abonnements haben.

Image eines anderen Mandanten auswählen Sie können in der Azure Compute Gallery mit PowerShell-Befehlen ein Image auswählen, das zu einem anderen Azure-Mandanten gehört, um MCS-Kataloge zu erstellen und zu aktualisieren.

1. Im Stammordner der Hostingeinheit erstellt Citrix einen neuen freigegebenen Abonnementordner unter dem Namen `sharedsubscription`.
2. Listen Sie alle freigegebenen Abonnements auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
<!--NeedCopy-->
```

3. Wählen Sie ein freigegebenes Abonnement und listen Sie dann alle freigegebenen Ressourcengruppen dieses Abonnements auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Wählen Sie eine Ressourcengruppe und listen Sie dann alle Kataloge in der Ressourcengruppe auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Wählen Sie einen Katalog und listen Sie dann alle Imagedefinitionen des Katalogs auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Wählen Sie eine Imagedefinition und listen Sie dann alle Imageversionen der Imagedefinition auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Zum Erstellen und Aktualisieren eines MCS-Katalogs verwenden Sie die folgenden Elemente:
   - Ressourcengruppe
   - Katalog

- Katalogimagedefinition
- Katalogimageversion

Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen

MCS ermöglicht das Weiterleiten von Netzwerkverkehr (API-Aufrufe von Citrix Cloud an Azure-Hypervisor) über Cloud Connectors in Ihrer Umgebung. Diese Implementierung hilft Ihnen, Ihr Azure-Abonnement zu sperren, um Netzwerkverkehr von bestimmten IP-Adressen zuzulassen. Fügen Sie hierfür `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` hinzu. Nachdem Sie die benutzerdefinierten Eigenschaften festgelegt haben, können Sie Azure-Richtlinien konfigurieren, um einen privaten Zugriff auf Azure Managed Disks einzurichten.

Wenn Sie die Azure-Richtlinie so konfigurieren, dass Datenträgerzugriffe für jeden neuen Datenträger zur Verwendung privater Endpunkte automatisch erstellt werden, können Sie maximal fünf Datenträger oder Snapshots gleichzeitig mit demselben Datenträgerzugriffsobjekt hoch- oder herunterladen (Azure-Einschränkung). Dieses Limit gilt für jeden Maschinenkatalog, wenn Sie die Azure-Richtlinie auf Ressourcengruppenebene konfigurieren, und für alle Maschinenkataloge, wenn Sie die Azure-Richtlinie auf Abonnementebene konfigurieren.
Wenn Sie die Azure-Richtlinie nicht so konfigurieren, dass Datenträgerzugriffe für jeden neuen Datenträger zur Verwendung privater Endpunkte automatisch erstellt werden, wird das Limit von fünf gleichzeitigen Vorgängen nicht durchgesetzt.

> **Hinweis:**
>
> Derzeit wird dieses Feature für die Connector Appliance nicht unterstützt. Informationen zu Azure-Einschränkungen im Zusammenhang mit diesem Feature finden Sie unter Import-/Exportzugriff für verwaltete Datenträger mit Azure Private Link einschränken.

Proxy aktivieren Um den Proxy zu aktivieren, legen Sie die benutzerdefinierten Eigenschaften für die Hostverbindung wie folgt fest:

1. Öffnen Sie ein PowerShell-Fenster mit dem Remote PowerShell SDK. Weitere Informationen finden Sie unter https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/.
2. Führen Sie die folgenden Befehle aus:

```
Add-PSSnapin citrix*.
cd XDHyp:\Connections\
```



```
dir
<!--NeedCopy-->
```

3. Kopieren Sie die `CustomProperties` aus der Verbindung in einen Editor und hängen Sie die Eigenschaftseinstellung `<Property xsi:type="StringProperty"Name ="ProxyHypervisorTrafficThroughConnector"Value="True"/>` an die `CustomProperties` an, um den Proxy zu aktivieren. Beispiel:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value="
    4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>
<!--NeedCopy-->
```

4. Weisen Sie im PowerShell-Fenster den geänderten benutzerdefinierten Eigenschaften eine Variable zu. Beispiel:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value
    ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Führen Sie `$cred = Get-Credential` aus. Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen für die Verbindung ein. Die Anmeldeinformationen sind Azure-Anwendungs-ID und das Geheimnis.

6. Führen Sie `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password` aus.

   > **Wichtig:**
   >
   > Wenn in einer Meldung angezeigt wird, dass `SubscriptionId` fehlt, ersetzen Sie in der benutzerdefinierten Eigenschaft alle doppelten Anführungszeichen (“) durch Graviszeichen plus doppelte Anführungszeichen (“`). Beispiel:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`" xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value=`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`" Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />
</CustomProperties>
<!--NeedCopy-->
```

7. Führen Sie `dir` aus, um die aktualisierten Einstellungen für `CustomProperties` zu überprüfen.

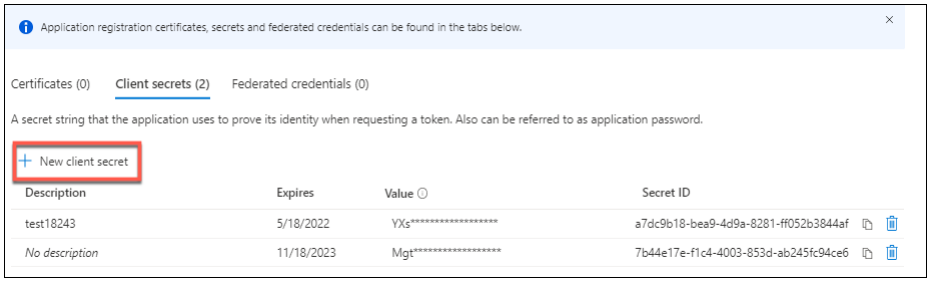
Anwendungsgeheimnis und Ablaufdatum für Geheimnis verwalten

Sie müssen das Anwendungsgeheimnis für eine Verbindung vor Ablauf des Geheimnisses ändern. Sie werden in der Benutzeroberfläche “Vollständige Konfiguration”benachrichtigt, bevor der geheime Schlüssel abläuft.

Anwendungsgeheimnis in Azure erstellen Sie können über das Azure-Portal ein Anwendungsgeheimnis für eine Verbindung erstellen.

1. Wählen Sie **Azure Active Directory**.
2. Wählen Sie in Azure AD unter **App registrations** Ihre Anwendung aus.
3. Gehen Sie zu **Certificates & secrets**.

4. Klicken Sie auf **Client secrets > New client secret**.



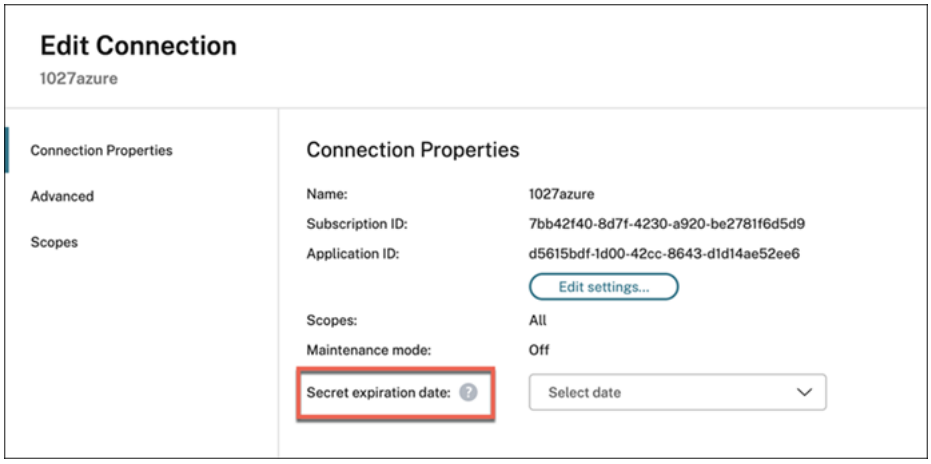
5. Geben Sie eine Beschreibung des geheimen Schlüssels ein und legen Sie eine Dauer fest. Wenn Sie fertig sind, wählen Sie **Hinzufügen**.

> **Hinweis:**
>
> Speichern Sie den geheimen Clientschlüssel unbedingt, da Sie ihn später nicht abrufen können.

6. Kopieren Sie das Clientgeheimnis und das Ablaufdatum.
7. Bearbeiten Sie in der Schnittstellen "Volle Konfiguration"die entsprechende Verbindung und ersetzen Sie den Inhalt in den Feldern **Anwendungsgeheimnis** und **Ablaufdatum des Geheimnisses** durch die Werte, den Sie kopiert haben.

Ändern des Ablaufdatums des Geheimnisses Sie können die Oberfläche "Vollständige Konfiguration"verwenden, um das Ablaufdatum für das verwendete Anwendungsgeheimnis hinzuzufügen oder zu ändern.

1. Klicken Sie im Assistenten **Verbindung und Ressourcen hinzufügen** mit der rechten Maustaste auf eine Verbindung und dann auf **Verbindung bearbeiten**.
2. Klicken Sie auf der Seite **Verbindungseigenschaften** auf **Ablaufdatum des Geheimnisses**, um das Ablaufdatum für das verwendete Anwendungsgeheimnis hinzuzufügen oder zu ändern.



Erforderliche Azure-Berechtigungen

Dieser Abschnitt enthält die für Azure erforderlichen Mindestberechtigungen und allgemeinen Berechtigungen.

Mindestberechtigungen

Mindestberechtigungen ermöglichen eine bessere Sicherheitskontrolle. Neue Features, die zusätzliche Berechtigungen erfordern, schlagen jedoch fehl, wenn nur Mindestberechtigungen erteilt sind. Dieser Abschnitt enthält die Mindestberechtigungen pro Aktion.

Hostverbindung erstellen Fügen Sie eine Hostverbindung unter Verwendung der von Azure abgerufenen Informationen hinzu.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/tenants/read"
<!--NeedCopy-->
```

Energieverwaltung virtueller Maschinen Schalten Sie die Maschineninstanzen ein oder aus.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Erstellen, Aktualisieren oder Löschen von VMs Nach dem Erstellen eines Maschinenkatalogs können Sie Maschinen hinzufügen, löschen und aktualisieren und den Maschinenkatalog löschen.

Die folgende Liste umfasst notwendige Mindestberechtigungen, wenn Masterimages verwaltete Datenträger oder Snapshots sind, die sich in derselben Region wie die Hostverbindung befinden.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Compute/virtualMachines/read",
```



```
6  "Microsoft.Compute/virtualMachines/write",
7  "Microsoft.Compute/virtualMachines/delete",
8  "Microsoft.Compute/virtualMachines/deallocate/action",
9  "Microsoft.Compute/snapshots/read",
10 "Microsoft.Compute/snapshots/write",
11 "Microsoft.Compute/snapshots/delete",
12 "Microsoft.Compute/snapshots/beginGetAccess/action",
13 "Microsoft.Compute/snapshots/endGetAccess/action",
14 "Microsoft.Compute/disks/read",
15 "Microsoft.Compute/disks/write",
16 "Microsoft.Compute/disks/delete",
17 "Microsoft.Compute/disks/beginGetAccess/action",
18 "Microsoft.Compute/disks/endGetAccess/action",
19 "Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
      read",
20 "Microsoft.Compute/skus/read",
21 "Microsoft.Compute/virtualMachines/extensions/read",
22 "Microsoft.Compute/virtualMachines/extensions/write",
23 "Microsoft.Features/providers/features/read",
24 "Microsoft.Network/virtualNetworks/read",
25 "Microsoft.Network/virtualNetworks/subnets/join/action",
26 "Microsoft.Network/virtualNetworks/subnets/read",
27 "Microsoft.Network/networkSecurityGroups/read",
28 "Microsoft.Network/networkSecurityGroups/write",
29 "Microsoft.Network/networkSecurityGroups/delete",
30 "Microsoft.Network/networkSecurityGroups/join/action",
31 "Microsoft.Network/networkInterfaces/read",
32 "Microsoft.Network/networkInterfaces/write",
33 "Microsoft.Network/networkInterfaces/delete",
34 "Microsoft.Network/networkInterfaces/join/action",
35 "Microsoft.Network/locations/usages/read",
36 <!--NeedCopy-->
```

Für die folgenden Features benötigen Sie zusätzlich zu den Mindestberechtigungen die folgenden Berechtigungen:

- Wenn das Masterimage eine virtuelle Festplatte (VHD) in einem Speicherkonto ist, das sich in derselben Region wie die Hostverbindung befindet:

```
1  "Microsoft.Storage/storageAccounts/read",
2  "Microsoft.Storage/storageAccounts/listKeys/action",
3  <!--NeedCopy-->
```

- Wenn das Masterimage eine ImageVersion aus Azure Compute Gallery (früher Shared Image Gallery) ist:

```
1  "Microsoft.Compute/galleries/read",
2  "Microsoft.Compute/galleries/images/read",
3  "Microsoft.Compute/galleries/images/versions/read",
4  <!--NeedCopy-->
```

- Wenn das Masterimage ein verwalteter Datenträger, ein Snapshot oder ein virtueller Daten-

träger ist, die sich in einer anderen Region als die Hostverbindung befinden:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
<!--NeedCopy-->
```

- Wenn Sie eine von Citrix verwaltete Ressourcengruppe verwenden:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Wenn Sie das Masterimage in Azure Compute Gallery (früher Shared Image Gallery) in einem freigegebenen Mandanten oder Abonnement platzieren:

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
<!--NeedCopy-->
```

- Wenn Sie dedizierte Azure-Hosts unterstützen:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Wenn Sie die serverseitige Verschlüsselung (SSE) mit vom Kunden verwalteten Schlüsseln (CMK) verwenden:

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- Wenn Sie VMs mit ARM-Vorlagen (Maschinenprofil) bereitstellen:

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
```



```
<!--NeedCopy-->
```

- Wenn Sie die Azure-Vorlagenspezifikation als Maschinenprofil verwenden:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Erstellen, Aktualisieren und Löschen von Maschinen mit nicht verwaltetem Datenträger Die folgende Liste umfasst notwendige Mindestberechtigungen, wenn das Masterimage eine VHD ist und die vom Administrator bereitgestellte Ressourcengruppe verwendet wird:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

In Azure AD eingebundene Geräte verwalten Die folgende Liste enthält die Mindestberechtigungen, die für die Verwaltung der in Azure AD eingebundenen Geräte erforderlich sind:

```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```


Allgemeine Berechtigungen

Die Rolle “Mitwirkender”erhält Vollzugriff zur Verwaltung aller Ressourcen. Dieser Satz von Berechtigungen hindert Sie nicht daran, Was ist neu zu erhalten.

Die folgenden Berechtigungen bieten die beste Kompatibilität für die zukünftige Verwendung, obwohl sie mehr Berechtigungen umfassen, als für aktuelle Features erforderlich sind:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
```



```
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Azure AD-Berechtigung Wenn Sie Kataloge für in Azure AD eingebundene Maschinen erstellen, erfolgt die Verwaltung der Azure AD-Geräte über MCS, wenn Sie die Verwaltung in Azure AD eingebundener Geräte aktivieren. Die in Azure AD integrierte Rolle **Cloudgeräteadministrator** bietet langfristig die beste Kompatibilität, obwohl sie mehr Berechtigungen umfasst, als für die aktuellen Features erforderlich sind.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Azure-spezifische Informationen finden Sie unter Microsoft Azure-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten

- Microsoft Azure Resource Manager-Virtualisierungsumgebungen

Verbindung zu Microsoft System Center Virtual Machine Manager

January 25, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft System Center Virtual Machine Manager (VMM).

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu VMM herstellen, müssen Sie zunächst Ihr VMM als Ressourcenstandort eingerichtet haben. Siehe Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen.

Verbindung erstellen

Wenn Sie VMs mit MCS bereitgestellt haben, führen Sie im Assistenten zur Erstellung von Verbindungen folgende Schritte aus:

- Geben Sie die Adresse als vollqualifizierten Domänennamen des Hostservers ein.
- Geben Sie die Anmeldeinformationen für das zuvor erstellte Administratorkonto ein. Das Konto muss Berechtigung zum Erstellen neuer VMs haben.
- Wählen Sie im Dialogfeld “Hostdetails”den Cluster oder eigenständigen Host aus, der beim Erstellen der VMs verwendet werden soll.

  > **Wichtig!**
  >
  > Sie müssen auch dann zu einem Cluster oder eigenständigen Host navigieren, wenn Sie eine Bereitstellung mit einem einzelnen Hyper-V-Host verwenden.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Informationen zum Erstellen von Maschinenkatalogen mit MCS auf SMB 3-Dateifreigaben finden Sie unter Microsoft System Center Virtual Machine Manager-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen.

Verbindung zu Nutanix

January 25, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Nutanix.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Nutanix herstellen, müssen Sie zunächst Ihr Nutanix-Konto als Ressourcenstandort eingerichtet haben. Siehe Nutanix-Virtualisierungsumgebungen.

Erstellen einer Verbindung mit Nutanix

Die folgenden Informationen ergänzen die Anweisungen unter Erstellen und Verwalten von Verbindungen. Folgen Sie zum Erstellen einer Nutanix-Verbindung den allgemeinen Anweisungen in dem Artikel. Beachten Sie besonders die Nutanix-spezifischen Details.

Wählen Sie im Assistenten **Verbindung und Ressourcen hinzufügen** auf der Seite **Verbindung** den Verbindungstyp **Nutanix**. Geben Sie dann die Adresse und Anmeldeinformationen sowie einen Namen für die Verbindung ein. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

Folgende Anschlusstypen stehen zur Auswahl: **Nutanix AHV**, **Nutanix AHV DRaaS** und **Nutanix AHV PC**.

- Geben Sie für **Nutanix AHV** die Prism Element (PE)-Clusteradresse und die Anmeldeinformationen an.
- Geben Sie für **Nutanix AHV PC** die Hypervisoradresse und die Anmeldeinformationen an.

  > **Hinweis:**
  >
  > Derzeit wird der Verbindungstyp **Nutanix AHV PC** nur zum Herstellen einer Verbindung zum Nutanix Cloud Cluster (NC2) auf Azure verwendet. Außerdem kann ein Maschinenkatalog nur auf einem einzelnen Cluster in einer NC2-on-Azure-Verbindung gehostet werden.

- Geben Sie für **Nutanix AHV DRaaS** Ihre Adresse und Ihren Benutzernamen an und importieren Sie dann die öffentlichen und privaten Schlüssel aus den Nutanix DRaaS-Anmeldeinformationsdateien (`.pem`). (Öffentliche und private Schlüssel werden in der Nutanix DRaaS-Cloud von Nutanix DRaaS-Administratoren generiert.)

  – Suchen Sie zum Importieren der Schlüssel die Anmeldeinformationsdatei, öffnen Sie sie mit Notepad (oder einem anderen Texteditor) und kopieren Sie den Inhalt. Kehren Sie anschließend zur Seite **Verbindung** zurück, wählen Sie **Schlüssel importieren**, fügen Sie den Inhalt ein und wählen Sie **Speichern**.

Achtung: Ändern Sie weder den Inhalt noch das Format der Anmeldeinformationen.

> **Tipp:**
>
> Wenn Sie Maschinen mit Nutanix AHV (Prism Element) als Ressource bereitstellen, wählen Sie den Container aus, in dem sich der VM-Datenträger befindet.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezielle Informationen zu Nutanix finden Sie unter Nutanix-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Nutanix-Virtualisierungsumgebungen
- Nutanix-Cloud und Partnerlösungen

Verbindung zu Nutanix-Cloud und Partnerlösungen

January 25, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Nutanix-Cloud und Partnerlösungen.

Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unterstützt die folgende Nutanix-Cloud und Partnerlösung:

- Nutanix Cloud Clusters in AWS

> **Hinweis:**
>
> - Bevor Sie eine Verbindung zu Nutanix-Cloud und Partnerlösung herstellen, müssen Sie zunächst Ihr entsprechendes Konto als Ressourcenstandort eingerichtet haben. Siehe Nutanix-Cloud und Partnerlösungen.
> - Die neuesten Informationen zur Einrichtung von Nutanix in der Cloud finden Sie im aktuellen Nutanix-Handbuch.

Herstellen einer Verbindung zu Nutanix Prism

Nachdem Sie einen Nutanix-Cluster erstellt haben, stellen Sie eine Verbindung zu Nutanix Prism her. Schrittfolge zum Herstellen einer Verbindung zu Nutanix Prism:

1. Erstellen Sie eine Bastion-VM im Subnetz 10.0.129.0/24.
2. Stellen Sie mit RDP eine Verbindung zur Bastion-VM her und rufen Sie die URL von **Prism Element** auf, die Sie im vorherigen Abschnitt kopiert haben.
3. Melden Sie sich mit den Standardanmeldeinformationen an: `admin:nutanix/4u`. Denken Sie daran, das Kennwort zu ändern.

Erstellen einer VM im Nutanix-Cluster

Nachdem Sie eine Verbindung zu **Nutanix Prism** hergestellt haben, erstellen Sie VMs im Nutanix-Cluster.

Wenn die VM einen Internetzugang benötigt

1. Rufen Sie die AWS-Konsole auf.
2. Erstellen Sie das neue Subnetz 10.0.130.0/24 in derselben virtuellen privaten Cloud, die von Nutanix CFS erstellt wurde.
3. Fügen Sie der Routing-Tabelle dieses Subnetzes eine Route hinzu, um den gesamten nicht lokalen Datenverkehr zum oben genannten NAT-Gateway zu leiten.
4. Stellen Sie mit RDP eine Verbindung zur Bastion-VM her, rufen Sie die URL von **Prism Element** auf, die Sie im vorherigen Abschnitt kopiert haben und melden Sie sich an.
5. Fügen Sie ein neues Netzwerk hinzu. Gehen Sie zu **Settings > Network Configuration > Create Subnet**. Verwenden Sie dasselbe Subnetz 10.0.130.0/24, das auch in AWS verwendet wird.
6. Erstellen Sie alle virtuellen Maschinen (AD, CC, VDA usw.) in diesem neuen Subnetz.

Wenn die VM keinen Internetzugang benötigt

1. Stellen Sie mit RDP eine Verbindung zur Bastion-VM her, rufen Sie die URL von **Prism Element** auf, die Sie im vorherigen Abschnitt kopiert haben und melden Sie sich an.
2. Fügen Sie ein neues Netzwerk hinzu. Gehen Sie zu **Settings > Network Configuration > Create Subnet**. Verwenden Sie das Subnetz 10.0.129.0/24.
3. Erstellen Sie alle virtuellen Maschinen (AD, CC, VDA usw.) in diesem Subnetz.

> **Tipp:**
>
> Stellen Sie sicher, dass Uhrzeit und Zeitzone in den VMs korrekt eingerichtet sind. Dies gilt insbesondere für AD.

Erstellen der Hostverbindung

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
2. Klicken Sie auf **Verbindungen und Ressourcen hinzufügen**.
3. Wählen Sie im Bildschirm **Verbindung** die Option **Neue Verbindung erstellen** und geben Sie unter **Verbindungsadresse** Folgendes ein: `https://xxx.xxx.xxx.xxx:9440`.
4. Folgen Sie der Benutzeroberfläche, um den Assistenten abzuschließen.

> **Hinweis:**
>
> Auf allen Connector-VMs muss das Nutanix-Plug-In installiert sein, damit die Nutanix-Option in Citrix Studio verfügbar ist, selbst dann, wenn die Plug-Ins nicht in der Nutanix-Zone verwendet werden.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezielle Informationen zu Nutanix finden Sie unter Nutanix-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Nutanix-Virtualisierungsumgebungen
- Nutanix-Cloud und Partnerlösungen

Verbindung zu VMware

May 17, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf VMware-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu VMware herstellen, müssen Sie zunächst Ihr VMware-Konto als Ressourcenstandort eingerichtet haben. Siehe VMware-Virtualisierungsumgebungen.

Erforderliche Berechtigungen

Erstellen Sie ein VMware-Benutzerkonto und mindestens eine VMware-Rolle mit einigen oder allen Berechtigungen, die in diesem Artikel aufgeführt sind. Berücksichtigen Sie bei der Rollenerstellung die erforderliche Granularität für die Benutzerberechtigungen zum jederzeitigen Anfordern der verschiedenen Citrix DaaS-Vorgänge. Zum Gewähren spezifischer Berechtigungen für jeden Zeitpunkt weisen Sie dem Benutzer die entsprechende Rolle mindestens auf Datencenterebene zu, wobei die Option **An untergeordnete Elemente weitergeben** aktiviert ist.

Die folgenden Tabellen zeigen die Zuordnungen zwischen Citrix DaaS-Vorgängen und die erforderlichen VMware-Mindestberechtigungen.

Verbindungen und Ressourcen hinzufügen

SDK	Benutzeroberfläche
System.Anonymous, System.Read und System.View	Automatisch hinzugefügt. Kann die integrierte Lesezugriff-Rolle verwenden.

Energieverwaltung

SDK	Benutzeroberfläche
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On

SDK	Benutzeroberfläche
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
Datastore.Browse	Datastore > Browse datastore

Bereitstellen von Maschinen (Maschinenerstellungsdienste)

Für das Provisioning von Maschinen mit MCS sind die folgenden Berechtigungen erforderlich:

SDK	Benutzeroberfläche
Datastore.AllocateSpace	Datastore > Allocate Space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
Virtual machine.Config > Add or remove device	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

SDK	Benutzeroberfläche
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1 und vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot; vSphere 8.0: Virtual machine > Snapshot management > Create snapshot

Updates und Rollbacks von Images

SDK	Benutzeroberfläche
Datastore.AllocateSpace	Datastore > Allocate Space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing

SDK	Benutzeroberfläche
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Löschen bereitgestellter Maschinen

SDK	Benutzeroberfläche
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Speicherprofil (vSAN)

Zum Anzeigen, Erstellen oder Löschen von Speicherrichtlinien bei der Katalogerstellung in einem vSAN-Datenspeicher sind die folgenden Berechtigungen obligatorisch:

SDK	Benutzeroberfläche
StorageProfile.Update	PROFILE-DRIVEN STORAGE > Profile-driven storage update. vSphere 8: VM storage policies > Update VM storage policies
StorageProfile.View	PROFILE-DRIVEN STORAGE > Profile-driven storage view. vSphere 8: VM storage policies > View VM storage policies

Tags und benutzerdefinierte Attribute

Mithilfe von Tags und benutzerdefinierten Attributen können Sie Metadaten an die im vSphere-Bestand erstellten VMs anhängen und das Suchen und Filtern dieser Objekte vereinfachen. Zum

Erstellen, Bearbeiten, Zuweisen und Löschen von Tags oder Kategorien sind die folgenden Berechtigungen erforderlich:

SDK	Benutzeroberfläche
InventoryService.Tagging.CreateTag	vSphere Tagging > Create vSphere Tag
InventoryService.Tagging.CreateCategory	vSphere Tagging > Create vSphere Tag Category
InventoryService.Tagging.EditTag	vSphere Tagging > Edit vSphere Tag
InventoryService.Tagging.EditCategory	vSphere Tagging > Edit vSphere Tag Category
InventoryService.Tagging.DeleteTag	vSphere Tagging > Delete vSphere Tag
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Delete vSphere Tag Category
InventoryService.Tagging.AttachTag	vSphere Tagging > Assign or Unassign vSphere Tag
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Assign or Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Manage custom attributes

> **Hinweis:**
>
> Wenn MCS einen Maschinenkatalog erstellt, weist es den Ziel-VMs Namens-Tags zu. Anhand der Tags wird das Masterimage von mit MCS erstellten VMs unterschieden und verhindert, dass letztere für die Imageerstellung verwendet werden. Sie können den Unterschied anhand des Attributs `XdProvisioned` in vCenter identifizieren. Das Attribut ist **True**, wenn MCS VMs erstellt.

Kryptographische Verfahren

Berechtigungen für kryptografische Verfahren legen fest, welcher Benutzer welche Art von kryptografischem Verfahren an welchem Objekttyp ausführen kann. vSphere Native Key Provider verwendet die `Cryptographer.*`-Berechtigungen. Die folgenden Mindestberechtigungen sind für kryptographische Verfahren erforderlich:

> **Hinweis:**
>
> Diese Berechtigungen sind für die Erstellung von MCS-Maschinenkatalogen mit VMs mit vTPM erforderlich.

SDK	Benutzeroberfläche
Cryptographic operations.Direct Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographic operations.Add disk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographic operations.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographic operations.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographic operations.Encrypt new	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographic operations.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographic operations.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographic operations.Read KMS information	Privileges > All Privileges > Cryptographic operations > Read KMS information

Bereitstellen von Maschinen (Citrix Provisioning)

Um VMs über die Citrix Provisioning-Konsole mit dem Citrix Virtual Apps and Desktops-Setupassistenten und dem Assistenten zum Exportieren von Geräten bereitzustellen, sind diese Berechtigungen zum Klonen und Bereitstellen einer Vorlage erforderlich. Legen Sie die Berechtigungen fest, während Sie eine Hostingverbindung herstellen.
Sie benötigen alle Berechtigungen von "Bereitstellen von Maschinen (Maschinenerstellungsdienste)" sowie folgende:

SDK	Benutzeroberfläche
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template

SDK	Benutzeroberfläche
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
vApp.Export	vApp > Export

> **Hinweis:**
>
> `vApp.Export` ist für die Erstellung von MCS-Maschinenkatalogen mithilfe von Maschinenprofilen erforderlich.

Schützen von Verbindungen zur VMware Umgebung

Die Verwendung von HTTPS/SSL-Verbindungen zu vCenter erfordert, dass Citrix DaaS der Verbindung vertraut.

Es gibt zwei Optionen:

- (Empfohlen) In der Citrix DaaS-Datenbank ist der SSL-Fingerabdruck installiert. Der Fingerabdruck wird zur Herstellung einer Vertrauensstellung zwischen Citrix DaaS auf jedem Cloud Connector und Verbindungen mit vCenter verwendet.
- (Alternative) Jeder Cloud Connector vertraut dem vCenter-Zertifikat und die Dienste auf dem Connector verwenden diese Vertrauensstellung. Die Vertrauensstellung kann auf Folgendem basieren:
  - vCenter-Zertifikat, das von der Zertifizierungsstelle ausgestellt und von Windows als vertrauenswürdig eingestuft wird, was zu einer Vertrauensstellung zwischen Windows und vCenter führt.
  - Unter Windows installiertes vCenter-Zertifikat, das zu einer Vertrauensstellung zwischen Windows und vCenter.OT führt

> **Hinweis:**
>
> vCenter-Zertifikat und VMware-SSL-Fingerabdruck sind für VMware Cloud und seine Partnerlösungen nicht erforderlich.

VMware SSL-Fingerabdruck

Mit dem VMware SSL-Fingerabdruckfeature wurde ein häufig aufgetretener Fehler beim Erstellen einer Hostverbindung mit einem VMware vSphere-Hypervisor behoben. Bisher musste der Administrator eine Vertrauensstellung zwischen den von Citrix verwalteten Delivery Controllern der Site und

dem Hypervisor-Zertifikat vor dem Erstellen einer Verbindung manuell erstellen. Dank VMware SSL-Fingerabdruck ist dies nicht mehr nötig. Der Fingerabdruck des nicht vertrauenswürdigen Zertifikats wird in der Sitedatenbank gespeichert, damit der Hypervisor zwar nicht von den Controllern, jedoch von Citrix DaaS immer als vertrauenswürdig eingestuft wird.

Beim Erstellen einer vSphere-Hostverbindung wird ein Dialogfeld mit dem Zertifikat der Maschine angezeigt, mit der Sie eine Verbindung herstellen. Sie können dann wählen, ob sie als vertrauenswürdig gelten soll.

Der VMware SSL-Fingerabdruck kann später mit dem PowerShell-SDK `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>` aktualisiert werden.

> **Tipp:**
>
> Der Fingerabdruck des Zertifikats muss aus Großbuchstaben bestehen.

Zertifikat beschaffen und importieren

Um die vSphere-Kommunikation zu schützen, empfiehlt Citrix die Verwendung von HTTPS statt HTTP. HTTPS benötigt digitale Zertifikate. Citrix empfiehlt die Verwendung eines digitalen Zertifikats, das von einer Zertifizierungsstelle unter Berücksichtigung der Sicherheitsrichtlinie Ihrer Organisation erstellt wurde.

Wenn Sie kein digitales Zertifikat verwenden können, das von einer Zertifizierungsstelle ausgestellt wurde, können Sie das mit VMware installierte selbstsignierte Zertifikat verwenden, vorausgesetzt, die Sicherheitsrichtlinie Ihrer Organisation lässt dies zu. Fügen Sie das VMware vCenter-Zertifikat jedem Cloud Connector hinzu.

1. Fügen Sie den vollqualifizierten Domänennamen (FQDN) des Computers, auf dem vCenter Server ausgeführt wird, der Hostdatei auf dem Server im Verzeichnis %SystemRoot%/WINDOWS/system32/Drivers/etc/ hinzu. Dieser Schritt ist nur erforderlich, wenn der FQDN des Computers, auf dem vCenter Server ausgeführt wird, nicht bereits im Domänennamensystem vorhanden ist.
2. Rufen Sie das vCenter-Zertifikat mit einer der folgenden drei Methoden ab:

   Führen Sie auf dem vCenter-Server folgende Schritte aus:

   a) Kopieren Sie die Datei rui.crt vom vCenter-Server zu einem Speicherort, auf den Ihre Cloud Connectors zugreifen können.
   b) Navigieren Sie auf dem Cloud Connector zu dem Speicherort des exportierten Zertifikats und öffnen Sie die Datei rui.crt.

Laden Sie das Zertifikat über einen Webbrowser herunter: Bei Verwendung von Internet Explorer müssen Sie (abhängig von Ihrem Benutzerkonto) ggf. in Internet Explorer mit der rechten Maustaste klicken und **Als Administrator ausführen** wählen, um das Zertifikat herunterzuladen und zu installieren.

a) Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her (z. B. https://server1.domain1.com).
b) Akzeptieren Sie die Sicherheitswarnungen.
c) Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
d) Klicken Sie auf **Zertifikat ist nicht gültig** und klicken Sie dann auf die Registerkarte **Details**.
e) Klicken Sie auf **Exportieren..**
f) Speichern Sie das exportierte Zertifikat.
g) Navigieren Sie auf den Speicherort des exportierten Zertifikats und öffnen Sie die CER-Datei.

Direkter Import von Internet Explorer, der als Administrator ausgeführt wird:

a) Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her (z. B. https://server1.domain1.com).
b) Akzeptieren Sie die Sicherheitswarnungen.
c) Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
d) Zeigen Sie das Zertifikat an.

3. Importieren des Zertifikats in den Zertifikatspeicher jedes Cloud Connectors:

a) Klicken Sie auf **Zertifikat installieren**, wählen Sie **Lokaler Computer** und klicken Sie dann auf **Weiter**.
b) Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie dann auf **Durchsuchen**. Spätere unterstützte Version: Wählen Sie **Vertrauenswürdige Personen** und klicken Sie dann auf **OK**. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

> **Wichtig:**
>
> Wenn Sie den Namen des vSphere-Servers nach der Installation ändern, müssen Sie ein neues selbstsigniertes Zertifikat auf diesem Server erstellen, bevor Sie das neue Zertifikat importieren.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- VMware-spezifische Informationen finden Sie unter VMware-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- VMware-Virtualisierungsumgebungen
- Cloud- und Partnerlösungen von VMware

Verbindung zu VMware-Cloud und Partnerlösungen

January 25, 2024

Nachdem Sie den Azure VMware Solution (AVS)-Cluster, die Google Cloud VMware Engine und VMware Cloud auf AWS eingerichtet haben, erstellen Sie die Verbindungen. Informationen zum Erstellen von Verbindungen finden Sie im Artikel zur Verbindung zu VMware-Virtualisierungsumgebungen.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- VMware-spezifische Informationen finden Sie unter VMware-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- VMware-Virtualisierungsumgebungen.
- VMware-Cloud und Partnerlösungen

Verbindung zu XenServer

April 18, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Bevor Sie eine Verbindung zu XenServer (früher Citrix Hypervisor) herstellen, müssen Sie zunächst die Einrichtung Ihres XenServer als Host abschließen. Weitere Informationen finden Sie unter Ressourcentyp hinzufügen oder eine unbenutzte Domäne in Citrix Cloud aktivieren.

Erstellen einer Verbindung zu XenServer

Beim Erstellen einer Verbindung zu XenServer müssen Sie die Anmeldeinformationen eines Hauptadministrators einer virtuellen Maschine (VM-Hauptadministrator) oder eines höherrangigen Benutzers eingeben.

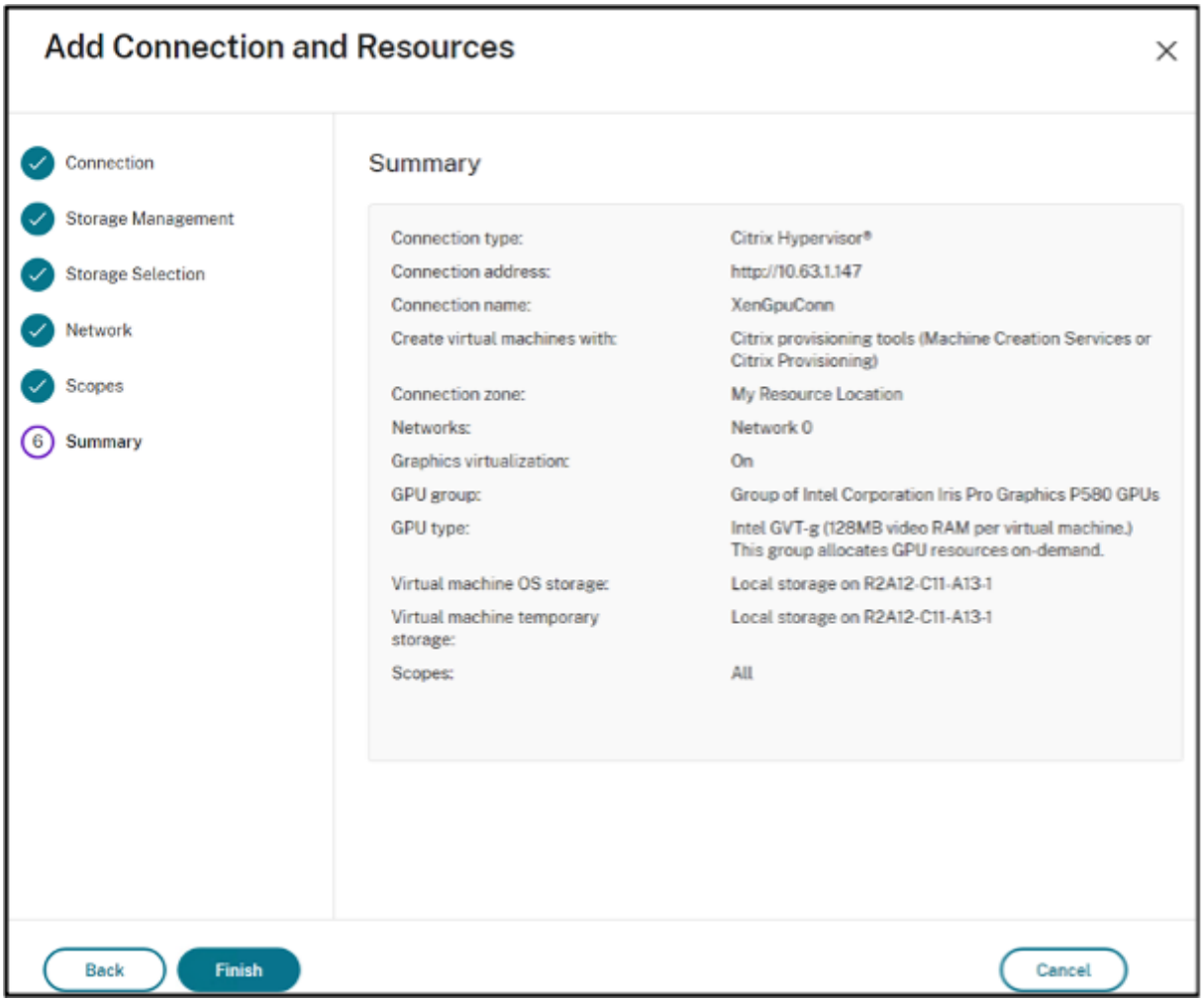
Citrix empfiehlt, HTTPS zum Sicheren der Kommunikation mit XenServer zu verwenden. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit XenServer installierte TLS-Zertifikat ersetzen. Weitere Informationen finden Sie unter Install a TLS certificate on your server.

Sie können hohe Verfügbarkeit konfigurieren, wenn dies auf dem XenServer-Server aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über **Server mit hoher Verfügbarkeit bearbeiten**) auswählen, um die Kommunikation mit dem XenServer-Server zu ermöglichen, wenn der Poolmaster ausfällt.

> **Hinweis:**
>
> Wenn Sie HTTPS verwenden und Server mit hoher Verfügbarkeit konfigurieren möchten, installieren Sie nicht ein Platzhalterzertifikat für alle Server in einem Pool. Für jeden Server ist ein individuelles Zertifikat erforderlich.

Wenn Sie auf XenServer-Hosts lokalen Speicher für die temporäre Datenspeicherung verwenden, stellen Sie sicher, dass jeder Speicherort im Pool einen eindeutigen Namen hat. (Sie ändern einen Namen in XenCenter, indem Sie mit der rechten Maustaste auf den Speicher klicken und die Nameneigenschaft bearbeiten.)

Wenn Sie eine Verbindung mit dem XenServer herstellen, der vGPU unterstützt, können Sie die GPU-Gruppe und den GPU-Typ auf der **Übersichtsseite** des Assistenten zum Herstellen einer Verbindung überprüfen.



Verwenden von IntelliCache für XenServer-Verbindungen

Durch den Einsatz von IntelliCache werden gehostete VDI-Bereitstellungen kostengünstiger, da eine Kombination aus freigegebenem und lokalem Speicher verwendet werden kann. Dies verbessert die Leistung und reduziert den Datenverkehr im Netzwerk. Das Masterimage aus dem freigegebenen Speicher wird im lokalen Speicher zwischengespeichert, wodurch die Anzahl der Lesevorgänge im freigegebenen Speicher reduziert wird. Bei gemeinsam genutzten Desktops werden Schreibvorgänge auf den differenzierender Datenträgern in den lokalen Speicher auf dem Host und nicht in den gemeinsam genutzten Speicher geschrieben.

Die wichtigsten Überlegungen sind:

- Der freigegebene Speicher muss NFS sein, wenn Sie IntelliCache verwenden.
- Citrix empfiehlt die Verwendung eines lokalen Speichergeräts mit hoher Leistung, um eine schnellstmögliche Datenübertragung zu gewährleisten.

Um IntelliCache zu verwenden, aktivieren Sie IntelliCache wie beschrieben:

- Wählen Sie bei der Installation von XenServer **Thin Provisioning aktivieren** aus. Weitere Informationen zur Installation des XenServer-Hosts von lokalen Medien finden Sie unter XenServer-Host installieren. Citrix bietet keine Unterstützung für gemischte Serverpools, bei denen auf einigen Servern IntelliCache aktiviert ist und auf anderen nicht.
- In Citrix DaaS ist IntelliCache standardmäßig deaktiviert. Sie können die Einstellung nur ändern, wenn Sie eine XenServer-Verbindung erstellen. Sie können IntelliCache später nicht deaktivieren. Gehen Sie folgendermaßen vor, wenn Sie eine XenServer-Verbindung erstellen:
  - Wählen Sie als Speichertyp **Freigegeben** aus.
  - Aktivieren Sie das Kontrollkästchen **IntelliCache verwenden**.

Weitere Informationen finden Sie unter IntelliCache.

Erforderliche XenServer-Berechtigungen

Die XenServer-Berechtigungen sind rollenbasiert (RBAC). Mit der Funktion Role-Based Access Control (RBAC) in XenServer können Sie Ihren Benutzern Rollen und Berechtigungen zuweisen, um zu steuern, wer Zugriff auf Ihren XenServer hat und welche Aktionen sie ausführen können. Das XenServer RBAC-System ordnet einen Benutzer (oder eine Gruppe von Benutzern) definierten Rollen (einem benannten Satz von Berechtigungen) zu. Den Rollen sind XenServer-Berechtigungen zugeordnet, um bestimmte Operationen auszuführen.

Weitere Informationen finden Sie unter Rollenbasierte Zugriffskontrolle.

Die Rollenhierarchie lautet in der Reihenfolge steigender Berechtigungen: Schreibgeschützt → VM-Operator → VM-Hauptadministrator → Pooloperator → Pooladministrator.

Im folgenden Abschnitt wird die Mindestrolle zusammengefasst, die für jede Bereitstellungsaufgabe erforderlich ist.

Hostverbindung erstellen

Aufgabe	Erforderliche Mindestrolle
Hostverbindung unter Verwendung der von XenServer abgerufenen Informationen hinzufügen	Schreibgeschützt
Benutzer und ihre zugewiesene Rolle anzeigen	Schreibgeschützt

Energieverwaltung virtueller Maschinen

Aufgabe	Erforderliche Mindestrolle
VMs ein- oder ausschalten	VM-Operator

VMs erstellen, aktualisieren oder löschen

Aufgabe	Erforderliche Mindestrolle
VMs zu bestehenden Snapshot-Zeitplänen hinzufügen oder daraus entfernen	VM-Hauptadministrator
Snapshot-Zeitpläne hinzufügen, ändern und löschen	Pooloperator
Masterimage veröffentlichen	Pooloperator (Switch-Port-Sperre erforderlich)
Maschinenkatalog erstellen	Poolbetreiber: Switch-Port-Sperre erforderlich
VMs hinzufügen oder entfernen (keine GPU-fähigen VMs)	VM-Administrator
VMs hinzufügen oder entfernen (GPU-fähige VMs)	Pooloperator
Virtuelle Datenträger oder CD-Geräte hinzufügen, entfernen oder konfigurieren	VM-Administrator
Tags verwalten	VM-Operator

Weitere Informationen zu RBAC-Rollen und -Berechtigungen finden Sie unter RBAC-Rollen und -Berechtigungen.

Informationen zum Sperren von Switch-Ports finden Sie unter Switch-Port-Sperre verwenden.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Alle XenServer-spezifischen Informationen finden Sie unter XenServer-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- XenServer-Virtualisierungsumgebungen

Maschinenkataloge erstellen

June 13, 2024

> **Hinweis:**
>
> In diesem Artikel wird beschrieben, wie Sie Kataloge mit der Schnittstelle "Vollständige Konfiguration"erstellen. Wenn Sie Quick Deploy zum Erstellen von Azure-Ressourcen verwenden, folgen Sie den Anweisungen unter Erstellen von Katalogen mit Quick Deploy.

Sammlungen von physischen oder virtuellen Maschinen werden als Einheit in einem sogenannten Maschinenkatalog verwaltet. Innerhalb eines Maschinenkatalogs haben alle Maschinen einen gemeinsamen Betriebssystemtyp, bei dem es sich entweder um ein Multisitzungs-OS oder ein Einzelsitzungs-OS handeln kann, wie z. B. Windows- oder Linux-basierte Systeme.

Die Oberfläche **Verwalten > Vollständige Konfiguration** führt Sie durch das Erstellen des ersten Maschinenkatalogs. Nach dem Erstellen des ersten Maschinenkatalogs erstellen Sie die erste Bereitstellungsgruppe. Später können Sie den erstellten Katalog ändern und weitere Kataloge erstellen.

Übersicht

Wenn Sie einen Katalog virtueller Maschinen erstellen, geben Sie an, wie diese VMs bereitgestellt werden sollen. Sie können Maschinenerstellungsdienste (MCS) verwenden. Alternativ können Sie eigene Tools verwenden.

- Bei Verwendung von Maschinenerstellungsdiensten (MCS) stellen Sie ein Image (bzw. einen Snapshot) zum Erstellen identischer virtueller Maschinen im Katalog bereit. Bevor Sie den Katalog erstellen, müssen Sie erst eine Hostingverbindung zum Hypervisor oder Clouddienst Ihrer Wahl einrichten. Anschließend müssen Sie das Masterimage auf demselben erstellen und konfigurieren. Für die Konfiguration des Masterimages sind Aufgaben wie der Domänenbeitritt bei Bedarf, die Installation der erforderlichen Treiber, die zu veröffentlichenden Anwendungen und die Bereitstellung des Virtual Delivery Agent (VDA) auf dem Image erforderlich.
- Nachdem Sie das Masterimage erstellt haben, erstellen Sie den Maschinenkatalog in der Benutzeroberfläche **Verwalten > Vollständige Konfiguration**. Sie wählen das Image (bzw. einen Image-Snapshot) und geben die Anzahl der in dem Katalog zu erstellenden VMs und weitere Informationen an.
- Selbst wenn Sie die Maschinen bereits haben, erstellen Sie mindestens einen Maschinenkatalog, um diese VMs in den Katalog zu importieren.

Wenn Sie die Maschinenerstellungsdienste zum Erstellen des ersten Katalogs verwenden, geben Sie eine Hostingeinheit an, die Sie zuvor erstellt haben. Die Hostingeinheit stellt die Ressourcenkonfiguration bereit, mit der Sie eine virtuelle Maschine erstellen können. Nach dem Erstellen des ersten

Katalogs und der ersten Bereitstellungsgruppe können Sie die Informationen über die Hostingeinheit oder die übergeordnete Hostverbindung ändern oder weitere Verbindungen und Hostingeinheiten erstellen.

Wenn ein Cloud Connector nicht ordnungsgemäß funktioniert, dauern MCS-Provisioningvorgänge (z. B. Katalogaktualisierungen) länger und die Leistung der Verwaltungsoberfläche wird erheblich beeinträchtigt.

Prüfung auf RDS-Lizenz

Beim Erstellen von Maschinenkatalogen mit Windows-Maschinen für Multisitzungs-OS erfolgt eine automatische Prüfung auf gültige Microsoft RDS-Lizenzen. Der Katalog wird nach einer eingeschalteten und registrierten Maschine durchsucht, um die Prüfung durchzuführen.

- Wird keine eingeschaltete, registrierte Maschine gefunden, wird per Warnung gemeldet, dass die RDS-Lizenzprüfung nicht durchgeführt werden kann.
- Wird eine Maschine gefunden und ein Fehler festgestellt, dann ist unter **Verwalten > Vollständige Konfiguration** eine Warnmeldung bezüglich des Katalogs mit dem erkannten Problem zu sehen. Um eine RDS-Lizenzwarnung aus einem Katalog zu entfernen (sodass sie nicht mehr in der Anzeige erscheint), wählen Sie den Katalog aus. Wählen Sie **RDS-Lizenzwarnung entfernen**. Bestätigen Sie die Aktion, wenn Sie dazu aufgefordert werden.

VDA-Registrierung

Ein VDA muss bei einem Cloud Connector registriert sein, damit er beim Start gebrokerter Sitzungen in die Auswahl kommt. Nicht registrierte VDAs können eine mangelnde Auslastung verfügbarer Ressourcen zur Folge haben. Es gibt eine Reihe von Gründen, warum ein VDA nicht registriert sein könnte. Viele können Sie beheben. Informationen zur Problembehandlung werden im Assistenten für die Katalogerstellung angezeigt, und nachdem ein Katalog zu einer Bereitstellungsgruppe hinzugefügt wurde.

Im Assistenten zum Erstellen von Maschinenkatalogen wird nach dem Hinzufügen vorhandener Maschinen in der Liste der Computerkontonamen angezeigt, ob die einzelnen Maschinen zum Hinzufügen zu dem Katalog geeignet sind. Zeigen Sie auf das Symbol neben jeder Maschine, um Informationen dazu einzublenden.

Wenn die Nachricht eine problematische Maschine identifiziert, können Sie diese Maschine entweder entfernen (über die Schaltfläche **Entfernen**) oder die Maschine hinzufügen. Wird beispielsweise gemeldet, dass die Maschineninformationen nicht abgerufen werden können (z. B. weil die Maschine nie registriert wurde), können Sie die Maschine auf Wunsch dennoch hinzufügen.

Weitere Informationen zur Fehlerbehebung bei der VDA-Registrierung finden Sie unter CTX136668.

Überblick über die Katalogerstellung mit MCS

Nachdem Sie Informationen im Assistenten zum Erstellen von Maschinenkatalogen eingegeben haben, erfolgen die nachfolgend aufgeführten Standardaktionen in MCS.

- Wenn Sie ein Image anstelle eines Snapshots auswählen, erstellt MCS einen Snapshot.
- MCS erstellt eine vollständige Kopie des Snapshots und fügt diese an jedem in der Hostverbindung definierten Speicherort hinzu.
- MCS fügt Active Directory Maschinen hinzu, wodurch eindeutige Identitäten erstellt werden.
- MCS erstellt die im Assistenten angegebene Anzahl VMs mit jeweils zwei Datenträgern. Zusätzlich zu den beiden Datenträgern pro VM wird auch die vollständige Kopie des Snapshots oder Masterimages am selben Speicherort gespeichert. Wenn Sie mehrere Speicherorte definiert haben, werden an jedem die folgenden Datenträgertypen erstellt:
  - Vollständige Kopie des Snapshots (siehe oben); diese ist schreibgeschützt und wird von allen gerade erstellten VMs gemeinsam genutzt.
  - Eine eindeutige 16-MB-Identitätsdisk, durch die jede VM eine eindeutige Identität erhält. Jede VM erhält eine Identitätsdisk.
  - Ein eindeutiger differenzierender Datenträger zum Speichern der auf der VM erfolgten Schreibvorgänge. Dieser Datenträger ist, sofern dies vom Hostspeicher unterstützt wird, für schlanke Speicherzuweisung geeignet und kann bei Bedarf auf die maximale Größe des Masterimages anwachsen. Jede virtuelle Maschine erhält einen differenzierenden Datenträger. Der differenzierende Datenträger enthält die im Lauf von Sitzungen gemachten Änderungen. Er ist für dedizierte Desktops permanent. Für gepoolte Desktops wird er nach jedem Neustart gelöscht und neu erstellt.

Alternativ können Sie beim Erstellen von VMs für statische Desktops auf der Seite **Maschinen** des Assistenten zum Erstellen von Maschinenkatalogen Thick Clones (vollständige Kopie) festlegen. Thick Clones erfordern keine Beibehaltung des Masterimages in jedem Datenspeicher. Jede VM hat ihre eigene Datei.

Überlegungen zum MCS-Speicher

Es gibt viele Faktoren bei der Entscheidung über Speicherlösungen, Konfigurationen und Kapazitäten für MCS. Die folgenden Informationen enthalten Überlegungen zur Speicherkapazität:

Kapazitätsüberlegungen:

- Datenträger

  Die Delta- oder Differenzdatenträger (Diff) benötigen den meisten Speicherplatz in den meisten MCS-Bereitstellungen für jede VM. Jede VM, die von MCS erstellt wurde, erhält beim Erstellen mindestens 2 Datenträger.

  - Disk0 = Diff Disk: Enthält das Betriebssystem, wenn von dem Basismasterimage kopiert.
  - Disk1 = Identitätsdatenträger: 16 MB, enthält Active Directory-Daten für jede VM.

  Im Laufe der Weiterentwicklung des Produkts, müssen Sie möglicherweise zusätzliche Datenträger hinzufügen, um den Verbrauch bestimmter Anwendungsfälle und Features abzudecken. Beispiel:

  - Die MCS-Speicheroptimierung erstellt einen Schreibcachedatenträger für jede VM.
  - Bei MCS können jetzt vollständige Klons verwendet werden, im Gegensatz zum Szenario mit Deltadatenträgern, das im vorherigen Abschnitt beschrieben wurde.

  Hypervisorfeatures spielen auch eine Rolle. Beispiel:

  - XenServer IntelliCache erstellt für jeden XenServer einen Lesedatenträger im lokalen Speicher. Diese Option spart IOPS gegen das Image, das möglicherweise an einem freigegebenen Speicherort ist.

- Mehraufwand für den Hypervisor

  Unterschiedliche Hypervisors verwenden bestimmte Dateien, die einen Mehraufwand für VMs verursachen. Hypervisors verwenden auch Speicher für Verwaltungs- und allgemeine Protokollierungsvorgänge. Berücksichtigen Sie beim Speicherplatz den Mehraufwand für:

  - Protokolldateien
  - Hypervisor-spezifische Dateien. Beispiel:
    * VMware fügt dem **VM-Speicherordner** zusätzliche Dateien hinzu. Siehe VMware Best Practices.
    * Berechnen Sie erforderliche Gesamtgröße für virtuelle Maschinen. Vorschlag für die virtuelle Maschine: 20 GB für den virtuellen Datenträger, 16 GB für die Auslagerungsdatei der virtuellen Maschine und 100 MB für Protokolldateien (insgesamt 36,1 GB).
  - Snapshots for XenServer; Snapshots for VMware.

- Mehraufwand für die Verarbeitung

  Das Erstellen eines Katalogs, Hinzufügen einer Maschine und Aktualisieren eines Katalogs haben spezielle Auswirkungen auf den Speicher. Beispiel:

  - Für die anfängliche Katalogerstellung muss eine Kopie des Basisdatenträgers an jeden Speicherort kopiert werden.
    * Außerdem müssen Sie vorübergehend eine Vorbereitungs-VM erstellen.
  - Das Hinzufügen einer Maschine zu einem Katalog erfordert nicht das Kopieren der Basisdatenträger an jeden Speicherort. Die Katalogerstellung variiert je nach ausgewählten Features.

  - Beim Aktualisieren des Katalogs wird für jeden Speicherort ein zusätzlicher Basisdatenträger erstellt. Für Katalogupdates kommt es zu einer vorübergehenden Speicherverbrauchspitze, bei der jede VM im Katalog für eine bestimmte Zeit 2 Diff-Datenträger hat.

Weitere Überlegungen:

- **RAM-Dimensionierung:** Beeinflusst die Größe bestimmter Hypervisordateien und -datenträger, einschließlich E/A-Optimierungsdatenträger, Schreibcache und Snapshotdateien.
- **Thin / Thick Provisioning:** NFS-Speicher wird wegen der schlanke Speicherzuweisungsfunktionen bevorzugt.

MCS-Speicheroptimierung

Die Funktion zur MCS-Speicheroptimierung wird auch als MCS E/A bezeichnet. Diese Funktion ist nur auf Azure, GCP, XenServer, VMware und SCVMM verfügbar.

- Der Schreibcachecontainer ist jetzt wie bei Citrix Provisioning *dateibasiert*. Beispielsweise lautet der Name des Citrix Provisioning-Schreibcache `D:\vdiskdif.vhdx` und der des MCS-E/A-Schreibcache `D:\mcsdif.vhdx`.
- Verbesserte Diagnose durch die Unterstützung einer im Schreibcachedatenträger gespeicherten Windows-Absturzabbilddatei.
- MCS E/A behält die Technologie *Cache im RAM mit Überlauf auf Festplatte* bei, um die optimale Schreibcachelösung auf mehreren Ebenen bereitzustellen. Mit dieser Funktion können Administratoren die Kosten in den Bereichen RAM, Datenträger und Leistung ausgleichen, um die Workload-Erwartungen zu erfüllen.

Die Aktualisierung der Schreibcachemethode von *datenträgerbasiert* auf *dateibasiert* erfordert die folgenden Änderungen:

1. MCS-E/A unterstützt einen ausschließlich RAM-basierten Cache nicht mehr. Geben Sie bei der Erstellung des Maschinenkatalogs eine Datenträgergröße an.
2. Der VM-Schreibcachedatenträger wird beim ersten Starten einer VM automatisch erstellt und formatiert. Sobald die VM läuft, wird die Schreibcachedatei `mcsdif.vhdx` in das formatierte Volume `MCSWCDisk` geschrieben.
3. Die Auslagerungsdatei wird an das formatierte Volume `MCSWCDisk` umgeleitet. Daher umfasst diese Datenträgergröße die Gesamtmenge des Speichers. Sie umfasst somit die Differenz zwischen der Datenträgergröße und der generierten Workload plus Auslagerungsdatei. Dies ist in der Regel mit der VM-RAM-Größe verknüpft.

Aktualisierungen der MCS-Speicheroptimierung aktivieren Zum Aktivieren der MCS E/A-Speicheroptimierung aktualisieren Sie den Delivery Controller und den VDA auf die neueste Version

von Citrix DaaS.

> **Hinweis:**
>
> Wenn Sie eine vorhandene Bereitstellung aktualisieren, in der MCS E/A aktiviert ist, ist keine zusätzliche Konfiguration erforderlich. Der VDA und das Delivery Controller-Upgrade behandeln das MCS-E/A-Upgrade.

Weitere Informationen über die Zuweisung eines Laufwerksbuchstaben an einen Zurückschreibcache-Datenträger finden Sie unter Laufwerksbuchstaben einem MCS-E/A-Zurückschreibcache-Datenträger zuweisen.

Vorbereiten eines Masterimages auf dem Hypervisor bzw. im Clouddienst

Das Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, den VDA und andere Software.

Nützliche Info:

- Masterimages werden ggf. auch als Klonimage, Golden Image, Basis-VM oder Basisimage bezeichnet. Hosthersteller und Clouddienstanbieter verwenden andere Bezeichnungen.
- Stellen Sie sicher, dass der Hypervisor oder Clouddienst über genügend Prozessoren, Arbeitsspeicher und Datenspeicher für die erstellten Maschinen verfügt.
- Konfigurieren Sie die für Desktops und Anwendungen benötigte Menge an Festplattenspeicher. Dieser Wert kann später nicht mehr geändert werden (auch nicht im Maschinenkatalog).
- Bei Remote-PC-Zugriff-Maschinenkatalogen werden keine Masterimages verwendet.
- Hinweise zur Microsoft Key Management Server-Aktivierung bei Verwendung der Maschinenerstellungsdienste: Wenn Ihre Bereitstellung 7.x-VDAs mit einem XenServer 6.1- oder 6.2-Host, einem vSphere-Host oder einem Microsoft System Center Virtual Machine Manager-Host enthält, müssen Sie kein manuelles Rearm für Microsoft Windows oder Microsoft Office durchführen.

Installieren und konfigurieren Sie die folgende Software auf dem Masterimage:

- Integrationstools für den Hypervisor (z. B. Citrix VM Tools, Hyper-V-Integrationsdienste oder VMware-Tools). Wenn Sie diesen Schritt auslassen, funktionieren die Anwendungen und Desktops unter Umständen nicht richtig.
- Einen VDA: Citrix empfiehlt die Installation der neuesten Version des VDA, damit die neuesten Features verfügbar sind. Wird kein VDA auf dem Masterimage installiert, schlägt die Katalogerstellung fehl.
- Tools von Drittanbietern, zum Beispiel Antivirensoftware oder Agents zur elektronischen Softwareverteilung. Konfigurieren Sie Dienste mit den für Benutzer und Maschinentyp geeigneten Einstellungen (z. B. Featureupdates).

- Anwendungen von Drittanbietern, die Sie nicht virtualisieren möchten. Citrix empfiehlt, dass Sie Anwendungen virtualisieren. Die Virtualisierung von Anwendungen senkt Kosten, denn das Masterimage muss nach dem Hinzufügen oder Neukonfigurieren einer Anwendung nicht aktualisiert werden. Außerdem belegen weniger installierte Anwendungen weniger Platz auf Masterimage-Festplatten, wodurch Speicherkosten eingespart werden.
- App-V-Clients mit den empfohlenen Einstellungen, wenn Sie App-V-Anwendungen veröffentlichen möchten. Der App-V-Client ist bei Microsoft erhältlich.
- Wenn Sie MCS verwenden und Microsoft Windows in lokalisierter Version ausführen möchten, installieren Sie die Gebietsschemas und Sprachpakete. Wenn ein Snapshot beim Provisioning erstellt wird, verwenden die bereitgestellten VMs die installierten Gebietsschemas und Sprachpakete.

> **Wichtig:**
>
> Wenn Sie MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.

Vorbereiten eines Masterimages

1. Erstellen Sie mit dem Verwaltungstool des Hypervisors ein Masterimage und installieren Sie dann das Betriebssystem sowie alle Service Packs und Updates. Geben Sie die Anzahl der vCPUs an. Sie können den vCPU-Wert auch festlegen, wenn Sie den Maschinenkatalog mit PowerShell erstellen. Beim Erstellen eines Maschinenkatalogs über **Verwalten > Vollständige Konfiguration** können Sie die Anzahl der vCPUs nicht angeben. Konfigurieren Sie die für Desktops und Anwendungen benötigte Menge an Festplattenspeicher. Dieser Wert kann später nicht mehr geändert werden (auch nicht im Maschinenkatalog).
2. Vergewissern Sie sich, dass die Festplatte am Gerätestandort 0 verbunden ist. Dieser Standort ist in den meisten Standardmasterimagevorlagen automatisch konfiguriert; in einigen benutzerdefinierten Vorlagen ist dies jedoch nicht unbedingt der Fall.
3. Installieren und konfigurieren Sie die oben aufgeführte Software auf dem Masterimage.
4. Wenn Sie MCS nicht verwenden, fügen Sie das Masterimage der Domäne hinzu, zu der die Anwendungen und Desktops gehören. Vergewissern Sie sich, dass das Masterimage auf dem Host verfügbar ist, auf dem die Maschinen erstellt werden. Wenn Sie MCS verwenden, ist das Hinzufügen des Masterimages zu einer Domäne nicht erforderlich. Die bereitgestellten Maschinen werden Mitglied der im Assistenten zum Erstellen von Maschinenkatalogen angegebenen Domäne.
5. Citrix empfiehlt, dass Sie einen Snapshot des Masterimages erstellen und benennen, damit es künftig identifiziert werden kann. Wenn Sie beim Erstellen eines Maschinenkatalogs keinen Snapshot, sondern ein Masterimage angeben, erstellt die Verwaltungsoberfläche automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Aktivierung der Volumenlizenzierung

MCS unterstützt die Aktivierung der Volumenlizenzierung, mit der die Aktivierung von Windows-Betriebssystemen und Microsoft Office automatisiert und verwaltet werden kann. Es werden drei Modelle zur Aktivierung der Volumenlizenzierung unterstützt:

- Key Management Service (KMS)
- Active Directory-basierte Aktivierung (ADBA)
- Multiple Activation Key (MAK)

Sie können die Aktivierungseinstellung ändern, nachdem Sie den Maschinenkatalog erstellt haben.

Key Management Service (KMS)

Der KMS-Dienst erfordert kein dediziertes System und kann problemlos mit anderen Diensten auf einem System gehostet werden. Die Funktion wird von allen von Citrix unterstützten Windows-Versionen unterstützt. Während der Image-Vorbereitung werden Microsoft Windows KMS und Microsoft Office KMS durch MCS zurückgesetzt. Mit dem Befehl `Set-Provserviceconfigurationdata` können Sie das Zurücksetzen überspringen. Weitere Informationen zum Zurücksetzen von Microsoft Windows KMS und Microsoft Office KMS während der Image-Vorbereitung finden Sie unter Machine Creation Services: Image Preparation Overview and Fault-Finding. Weitere Informationen zur KMS-Aktivierung finden Sie unter Aktivieren mit dem Schlüsselverwaltungsdienst.

> **Hinweis:**
>
> Alle Maschinenkataloge, die nach dem Ausführen des Befehls `Set-Provserviceconfigurationdata` erstellt wurden, verwenden die im Befehl angegebene Einstellung.

Active Directory-basierte Aktivierung (ADBA)

Mit ADBA können Sie Maschinen über deren Domänenverbindungen aktivieren. Die Maschinen werden sofort aktiviert, wenn sie einer Domäne beitreten. Die Maschinen bleiben so lange aktiviert, wie sie mit der Domäne verbunden und in Kontakt bleiben. Die Funktion wird von allen von Citrix unterstützten Windows-Versionen außer Windows Server 2022 unterstützt. Weitere Informationen zur Active Directory-basierten Aktivierung finden Sie unter Aktivierung über Active Directory.

Multiple Activation Key (MAK)

Mit dem Mehrfachaktivierungsschlüssel (oder MAK-Schlüssel) können Sie den Microsoft-Server nutzen, um Volumes zu aktivieren und das Windows-System zu authentifizieren. Der MAK-Schlüssel muss von Microsoft erworben werden, und jedem Schlüssel ist eine feste Anzahl von Aktivierungen

zugewiesen. Mit jeder Aktivierung eines Windows-Systems verringert sich die Aktivierungsanzahl. Es gibt zwei Möglichkeiten zur Aktivierung des Systems:

- Online-Aktivierung: Wenn das Windows-System, das Sie aktivieren möchten, über einen Internetzugang verfügt, wird Windows automatisch bei der Installation des Produktschlüssels aktiviert. Dabei verringert sich die Aktivierungsanzahl für den entsprechenden MAK-Schlüssel um 1.
- Offline-Aktivierung: Wenn das Windows-System keine Verbindung zum Internet herstellen kann, erhält MCS vom Microsoft-Server eine Bestätigungs-ID und eine Installations-ID, um so das Windows-System zu aktivieren. Diese Art der Aktivierung ist für nicht-persistente Maschinenkataloge geeignet.

> **Hinweis:**
>
> - MCS unterstützt die Microsoft Office-Aktivierung mit MAK nicht.
> - Die erforderliche Mindestversion des VDA ist 2303.

Hauptanforderungen

- Der Delivery Controller muss über einen Internetzugang verfügen.
- Erstellen Sie einen neuen Katalog, wenn das Update einen anderen MAK-Schlüssel als das Original-Image verwendet.
- Installieren Sie den MAK-Schlüssel auf dem Masterimage. Die Schritte zur Installation des MAK-Schlüssels auf einem Windows-System finden Sie unter Deploy MAK Activation.
- Wenn Sie keine Imagevorbereitung verwenden:

  1. Fügen Sie den Registrierungs-DWORD-Wert `Manual` unter `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation` hinzu.
  2. Setzen Sie den Wert auf 1.

Anzahl der Aktivierungen Verwenden Sie das Tool für die Volumenaktivierungsverwaltung (VAMT), um die Anzahl der verbleibenden Aktivierungen für den MAK-Schlüssel anzuzeigen oder um zu überprüfen, ob eine VM mehrere Aktivierungen verbraucht. Siehe Installieren von VAMT.

Windows-System mit MAK-Schlüssel aktivieren Aktivieren des Windows-Systems mit MAK-Schlüssel:

1. Installieren Sie den Produktschlüssel auf dem Masterimage. Dabei verringert sich die Aktualisierungsanzahl um 1.

2. Erstellen Sie einen MCS-Maschinenkatalog.
3. Wenn Sie keine Imagevorbereitung verwenden:

   a) Fügen Sie den Registrierungs-DWORD-Wert `Manual` unter `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation` hinzu.
   b) Setzen Sie den Wert auf 1.

   Dadurch wird die Option der Online-Aktivierung deaktiviert.
4. Fügen Sie dem Maschinenkatalog virtuelle Maschinen hinzu.
5. Schalten Sie die VMs ein.
6. Das Windows-System wird nun je nach geplanter Aktivierungsart (online oder offline) aktiviert.

   - Bei einer Online-Aktivierung wird das Windows-System aktiviert, nachdem der Produktschlüssel installiert wurde.
   - Bei einer Offline-Aktivierung kommuniziert MCS mit den bereitgestellten VMs, um den Aktivierungsstatus des Windows-Systems abzurufen. MCS ruft dann vom Microsoft-Server eine Bestätigungs-ID und eine Installations-ID ab. Diese IDs werden verwendet, um das Windows-System zu aktivieren.

Problembehandlung Wenn die bereitgestellte VM nicht mit dem installierten MAK-Schlüssel aktiviert ist, führen Sie den Befehl `Get-ProvVM` oder `Get-ProvScheme` in einem PowerShell-Fenster aus.

- Befehl `Get-ProvScheme`: Siehe Parameter `WindowsActivationType`, der dem MCS-Maschinenkatalog vom neuesten Masterimage zugeordnet ist.
- Befehl `Get-ProvVM`. Siehe Parameter `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` und `WindowsActivationStatusError`.

Sie können den Fehler und die Schritte zur Behebung des Problems überprüfen.

Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration erstellen

Vor dem Erstellen eines Katalogs:

- Stellen Sie sicher, dass Sie eine Verbindung zum Hypervisor, Cloudservice und anderen Ressourcen hergestellt haben, die Ihre Maschinen hosten.
- Vergewissern Sie sich, dass Sie ein Masterimage für die Bereitstellung von Maschinen erstellt haben. Stellen Sie sicher, dass Sie einen VDA auf diesem Masterimage installiert haben.

> **Hinweis:**
>
> Wenn Sie VMs über eine einen Clouddienst oder Hypervisor hosten, kann der Assistent zum Erstellen von Maschinenkatalogen zusätzliche Seiten für den spezifischen Host umfassen. Wenn Sie z. B. ein Azure Resource Manager-Masterimage verwenden, enthält der Assistent die Seite **Speicher- und Lizenztypen**. Hostspezifische Informationen finden Sie in den entsprechenden Artikeln unter Nächste Vorgänge.

Assistenten zum Erstellen von Katalogen starten

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
2. Wählen Sie **Verwalten**.
3. Wenn Sie den ersten Katalog erstellen, werden Sie zur richtigen Auswahl weitergeleitet (z. B. "Einrichten der Maschinen und Erstellen von Maschinenkatalogen zum Ausführen von Apps und Desktops"). Der Assistent zum Erstellen von Katalogen wird geöffnet.
4. Wenn Sie bereits einen Katalog erstellt haben und einen weiteren erstellen möchten, gehen Sie wie folgt vor:
    a) Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
    b) Um Kataloge mit Ordnern zu organisieren, erstellen Sie Ordner im Standardordner **Maschinenkataloge**. Weitere Informationen finden Sie unter Erstellen von Katalogordnern.
    c) Wählen Sie den Ordner aus, in dem Sie den Katalog erstellen möchten, und klicken Sie dann auf **Maschinenkatalog erstellen**. Der Assistent zum Erstellen von Katalogen wird geöffnet.

Der Assistent führt Sie durch die in den folgenden Abschnitten beschriebenen Seiten. Die angezeigten Seiten können sich je nach der von Ihnen vorgenommenen Auswahl und der verwendeten Verbindung (zu einem Host) unterscheiden. Hosts/Virtualisierungsressourcen listet Informationsquellen für die unterstützten Hosttypen auf.

Wählen Sie einen Maschinentyp

Jeder Katalog darf nur Maschinen eines Betriebssystemtyps enthalten. Wählen Sie auf der Seite **Maschinentyp** eine der folgenden Optionen aus:

- **Multisitzungs-OS:** Ein Katalog für Multisitzungs-OS bietet gehostete freigegebene Desktops. Auf den Maschinen können die unterstützten Versionen von Windows oder Linux ausgeführt

werden, ein Katalog kann jedoch nicht sowohl ein Windows- oder Linux-Betriebssystem enthalten.

- **Einzelsitzungs-OS:** Ein Einzelsitzungs-OS-Katalog stellt VDI-Desktops bereit, die Sie verschiedenen Benutzern zuweisen können.
- **Remote-PC-Zugriff:** Ein Remote-PC-Zugriff-Katalog bietet Benutzern Remotezugriff auf ihre physischen Büro-Desktopmaschinen. Bei Remote-PC-Zugriff wird VPN nicht für die Sicherheit benötigt.

Maschinenverwaltungsoptionen auswählen

> **Hinweis:**
>
> Die Seite **Maschinenverwaltung** wird nicht angezeigt, wenn Sie auf der Seite **Maschinentyp** die Option **Remote-PC-Zugriff** auswählen.

Auf der Seite **Maschinenverwaltung** wird angegeben, wie die Maschinen verwaltet und mit welchem Tool sie bereitgestellt werden.

Wählen Sie eine der Optionen aus, um anzugeben, wie die Energieverwaltung der Maschinen über die Benutzeroberfläche für die vollständige Konfiguration erfolgen muss:

- **Maschinen mit Energieverwaltung (beispielsweise virtuelle Maschinen oder Blade-PCs)**: Diese Option ist nur verfügbar, wenn bereits eine Verbindung zu einem Hypervisor oder Clouddienst konfiguriert wurde.
- **Maschinen ohne Energieverwaltung (beispielsweise physische Maschinen)**

Wenn Sie die Option **Wählen Sie Maschinen mit Energieverwaltung (beispielsweise virtuelle Maschinen oder Blade-PCs)** wählen, müssen Sie auch ein Tool auswählen, mit dem VMs erstellt werden:

- **Citrix Maschinenerstellungsdienste (MCS):** verwendet ein Masterimage zum Erstellen und Verwalten virtueller Maschinen. Bei Maschinenkatalogen in Cloudumgebungen wird MCS verwendet. MCS ist für physische Maschinen nicht verfügbar.
- **Anderer Dienst oder andere Technologie:** Ein Tool, das Maschinen verwaltet, die sich bereits im Datencenter befinden. Citrix empfiehlt die Verwendung von Microsoft System Center Configuration Manager oder einer anderen Drittanbieteranwendung, um sicherzustellen, dass die Maschinen im Katalog konsistent sind.

> **Hinweis:**
>
> Informationen zu Linux-Betriebssystemmaschinen finden Sie unter Linux VDAs über die Maschinenerstellungsdienste (MCS) erstellen.

Desktoperfahrung auswählen

> **Hinweis:**
>
> Die Optionen auf der Seite **Desktoperfahrung** variieren je nach dem Maschinentyp, den Sie auf der Seite **Maschinentyp** auswählen.

- **Bei Maschinen mit Multisitzungs-OS** wird Benutzern bei jeder Anmeldung ein zufälliger Desktop zugewiesen. Auf der Seite **Desktoperfahrung** stehen Ihnen die folgenden Optionen zur Verfügung:
  - Änderungen auf dem lokalen Datenträger der Maschine speichern, auf der virtuelle Desktops gehostet werden: Persistent
  - Änderungen verwerfen und virtuelle Desktops bei Abmeldung entfernen: Nicht persistent

  > **Hinweis:**
  >
  > Bei persistenten Maschinen mit Multisitzungs-OS werden vom Benutzer am Desktop vorgenommene Änderungen gespeichert und sind für alle autorisierten Benutzer zugänglich.

- Für Maschinen mit Einzelsitzung-OS stehen auf der Seite **Desktoperfahrung** die folgenden Optionen zur Verfügung:
  - Benutzer stellen bei jeder Anmeldung eine Verbindung mit einem neuen (zufälligen) Desktop her.
  - Benutzer stellen bei jeder Anmeldung eine Verbindung mit dem gleichen (statischen) Desktop her.

  Sie können außerdem entscheiden, ob von Benutzern vorgenommene Änderungen nach der Abmeldung gespeichert oder verworfen werden.

Image auswählen

> **Hinweis:**
>
> - Diese Seite wird nur angezeigt, wenn Sie auf der Seite **Maschinenverwaltung Citrix Maschinenerstellungsdienste (MCS)** auswählen.
> - Die auf dieser Seite verfügbaren Optionen variieren je nach Hypervisor oder Clouddienst.

Führen Sie diese Schritte aus, um die Einstellungen auf dieser Seite abzuschließen:

1. Wählen Sie einen Imagetyp für den Maschinenkatalog und dann ein Image aus. Zwei Imagetypen sind verfügbar:

- **Masterimage**: Ein Snapshot oder eine VM, die als Masterimage erstellt wurde. Zu Beginn der Katalogerstellung wird das Image automatisch vorbereitet. Sie können bei Bedarf einen Hinweis für das ausgewählte Image hinzufügen.

  > **Hinweis:**
  >
  > – Wenn Sie MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.
  > – Wenn Sie keinen Snapshot, sondern ein Masterimage angeben, erstellt die Verwaltungsoberfläche automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.
  > – Eine Fehlermeldung wird angezeigt, wenn Sie einen Snapshot oder eine VM auswählen, der bzw. die nicht mit dem zuvor im Assistenten ausgewählten Tool zur Maschinenverwaltung kompatibel ist.
  > – Um Images in einem Image-Knoten zu aktualisieren, wählen Sie ihn in der Struktur aus und klicken dann rechts oben auf die Option **Aktualisieren**. Wenn Sie keinen Image-Knoten auswählen, werden durch Klicken auf **Aktualisieren** alle Images in der Struktur aktualisiert. Um die Auswahl eines ausgewählten Knotens in der Struktur aufzuheben, klicken Sie bei gedrückter **STRG**-Taste auf den Knoten.

- **Vorbereitetes Image**: Ein Image, das einer Imagevorbereitung unterzogen wurde und direkt bei der VM-Erstellung verwendet werden kann. Wenn Sie sich bei der Katalogerstellung für vorbereitete Images statt für Masterimages entscheiden, wird eine schnellere und zuverlässigere Maschinenkatalogerstellung sowie ein optimiertes Imagelebenszyklusmanagement gewährleistet.

Weitere Informationen zur Imagevorbereitung finden Sie unter Maschinenerstellungsdienst: Imagevorbereitung – Überblick und Fehlersuche.

2. Um VM-Einstellungen von einem Maschinenprofil zu erben, wählen Sie **Maschinenprofil verwenden** und wählen Sie dann eine VM- oder ARM-Vorlagenspezifikation (spezifisch für Azure) aus, die als Maschinenprofil verwendet werden soll.

   > **Hinweis:**
   >
   > Derzeit ist die Verwendung von Maschinenprofilen auf Azure-, AWS- und GCP-VMs beschränkt.

3. Wählen Sie die Mindestfunktionsebene für den Katalog. Damit Sie die neuesten Produktfeatures verwenden können, muss auf dem Masterimage die aktuelle VDA-Version installiert sein.

Maschinen konfigurieren

> **Hinweis:**
>
> - Der Titel der Seite hängt von der Auswahl ab, die Sie auf der Seite **Maschinenverwaltung** getroffen haben: **Maschinen**, **Virtuelle Maschinen** oder **Maschinen und Benutzer**.
> - Diese Seite wird nicht angezeigt, wenn Sie auf der Seite **Maschinentyp** die Option **Remote-PC-Zugriff** auswählen.
> - Sie können einen leeren Katalog erstellen, d. h. einen Katalog, der keine Maschinen enthält.

- **Bei Verwendung von MCS führen Sie folgende Schritte aus:**
  - Legen Sie fest, wie viele virtuelle Maschinen erstellt werden sollen. Geben Sie **0** (Null) ein, wenn Sie keine Maschine erstellen möchten. Um später virtuelle Maschinen für einen leeren Katalog zu erstellen, können Sie **Maschinen hinzufügen** ausführen.
  - Wählen Sie die Menge Arbeitsspeicher in MB für jede VM.

    > **Wichtig:**
    >
    > Jede erstellte VM hat eine Festplatte. Deren Größe wird im Masterimage festgelegt. Sie können die Festplattengröße im Katalog nicht ändern.

  - Wenn Sie auf der Seite **Desktoperfahrung** festlegen, dass Benutzeränderungen an statischen Desktops auf einer separaten persönlichen vDisk gespeichert werden sollen, geben Sie die Größe des virtuellen Datenträgers in GB und den Laufwerksbuchstaben an.
  - Wenn Ihre Bereitstellung mehrere Zonen (Ressourcenstandorte) enthält, können Sie eine Zone für den Katalog wählen.
  - Wenn Sie VMs mit statischen Desktops erstellen, wählen Sie einen Kopiermodus für die VMs. Siehe Kopiermodus für virtuelle Maschinen.
  - Wenn Sie VMs mit zufälligen, nicht persistenten Desktops erstellen, können Sie den Zurückschreibcache für temporäre Daten auf Maschinen aktivieren und konfigurieren, um die E/A-Leistung zu verbessern. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.
- **Bei Verwendung anderer Tools führen Sie folgende Schritte aus:**

  Fügen Sie eine Liste der Maschinenkontonamen hinzu (bzw. importieren Sie eine Liste). Sie können den Kontonamen von VMs nach dem Hinzufügen bzw. Importieren ändern. Wenn Sie auf der Seite **Desktoperfahrung** statische Maschinen angegeben haben, können Sie optional den Benutzernamen für jede hinzugefügte VM angeben.

  > **Tipp:**
  >
  > Um Benutzer hinzuzufügen, können Sie zu den Benutzern navigieren oder manuell eine durch Semikolon getrennte Liste von Benutzernamen eingeben. Wenn sich die Benutzer

> in Active Directory befinden, geben Sie die Namen direkt ein. Falls nicht, geben Sie die Namen in diesem Format ein: `<identity provider>:<user name>`. Beispiel: `AzureAD:username`.

Nachdem Sie Namen hinzugefügt oder importiert haben, können Sie mit der Schaltfläche **Entfernen** Namen aus der Liste löschen, während Sie noch auf dieser Assistentenseite sind.

- **Schrittfolge bei der Verwendung anderer Tools (nicht MCS):**

  Ein Symbol und eine QuickInfo für jede hinzugefügte (bzw. importierte) Maschine lassen solche Maschinen erkennen, die dem Katalog möglicherweise nicht hinzugefügt oder nicht bei einem Cloud Connector registriert werden können.

Kopiermodus für virtuelle Maschinen Über den auf der Seite **Maschinen** ausgewählten Kopiermodus wird festgelegt, ob MCS Thin Clones (Schnellkopien) oder Thick Clones (vollständige Kopien) des Masterimages erstellen soll. Standardmäßig werden Thin Clones erstellt.

- Thin Clones bieten eine effizientere Speichernutzung und eine schnellere Maschinenerstellung.
- Thick Clones bieten eine bessere Unterstützung für Datenwiederherstellung und Migration, jedoch ggf. bei geringeren IOPS nach Maschinenerstellung.

Konfigurieren eines Cache für temporäre Daten Wenn Sie zufällige, nicht persistente Maschinen mit MCS in einem Katalog verwalten, können Sie den Zurückschreibcache für Maschinen aktivieren, um die E/A-Leistung zu verbessern.

Der Zurückschreibcache wird als MCSIO bezeichnet. Weitere Informationen finden Sie in diesem Blogbeitrag.

Voraussetzungen Zum Aktivieren des Zurückschreibcaches muss der Katalog die folgenden Anforderungen erfüllen:

- Verwendet eine Verbindung, die den Speicher für temporäre Daten angibt. Weitere Informationen finden Sie unter Verbindungen und Ressourcen.
- VDAs müssen mindestens Version 7.9 sein und mit einem aktuellen MCSIO-Treiber installiert sein.

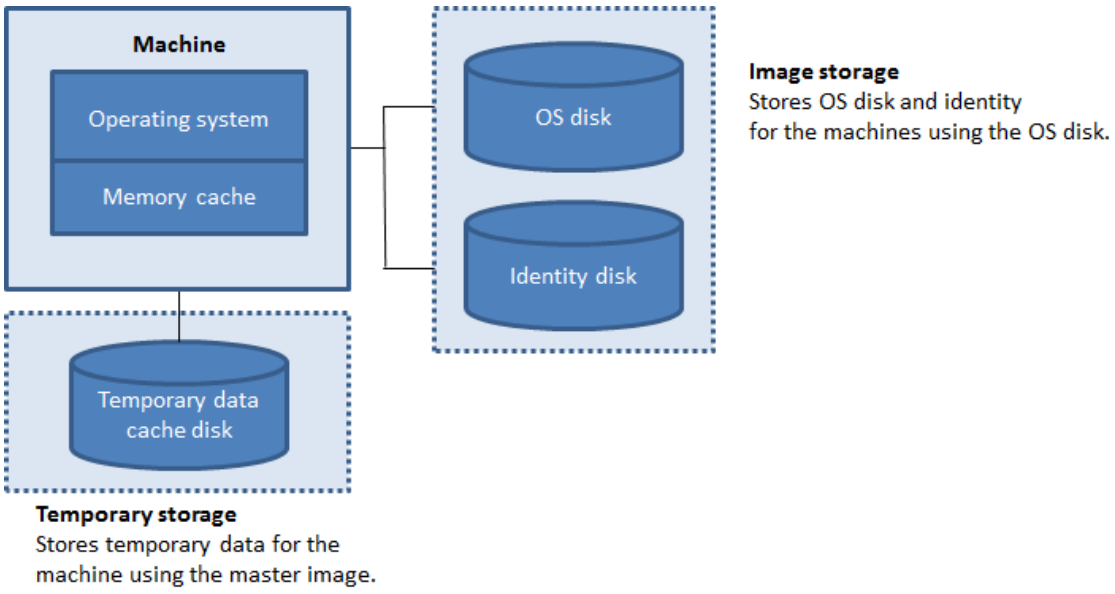
  > **Hinweis:**
  >
  > Die Installation dieses Treibers ist eine Option, wenn Sie einen VDA installieren oder aktualisieren. Standardmäßig wird der Treiber nicht installiert.

- Um die Zuweisung von Laufwerksbuchstaben für Datenträgercaches zu aktivieren, müssen virtuelle Maschinen die folgenden zusätzlichen Anforderungen erfüllen:

- Betriebssystem: Windows
- VDA-Version: 2305 oder höher

Überlegungen

- Zurückschreibcaches beziehen sich auf den *Speichercache* und den *Datenträgercache*. Die Standardwerte unterscheiden sich je nach Verbindungstyp. Die Standardwerte sind in den meisten Fällen ausreichend. Allerdings muss der für Folgendes erforderliche Speicherplatz berücksichtigt werden:
  - Von Windows selbst erstellte temporäre Datendateien, einschließlich der Windows-Auslagerungsdatei
  - Benutzerprofildaten
  - ShareFile-Daten, die mit Benutzersitzungen synchronisiert werden
  - Gegebenenfalls von einem Sitzungsbenutzer erstellte oder kopierte Daten und Daten von Anwendungen, die Benutzer möglicherweise sitzungsintern installieren



- Die Konfiguration des Zurückschreibcaches mit nur einem Datenträgercache und ohne Speichercache ist veraltet. Um einen Cache für temporäre Daten zu aktivieren, wird empfohlen, die **Datenträgercachegröße (GB)** und die Größe des dem **Cache zugewiesenen Speichers (MB)** auszuwählen und einen Wert größer als 0 für den Speichercache anzugeben. Temporäre Daten werden zunächst in den Speichercache geschrieben. Wenn der Speichercache seinen konfigurierten Grenzwert erreicht, werden die ältesten Daten zum temporären Datencache-Datenträger verschoben.
- Der Speichercache ist Teil der Gesamtspeichermenge auf jeder Maschine. Wenn Sie das Kontrollkästchen **Größe des Speichercaches (MB) (empfohlen)** aktivieren, sollten Sie daher erwägen,

den Gesamtspeicher auf jeder Maschine zu erhöhen.

- Das Ändern des Standardwerts von **Datenträgercachegröße** kann sich auf die Leistung auswirken. Die Größe muss gemäß den Anforderungen der Benutzer und der Maschinenlast gewählt werden.

  > **Wichtig:**
  >
  > Wenn auf dem Datenträgercache nicht mehr genügend Speicherplatz vorhanden ist, wird die Sitzung des Benutzers unbrauchbar.

- Wenn Sie das Kontrollkästchen **Größe des Datenträgercaches** deaktivieren, wird kein Datenträgercache erstellt. In diesem Fall geben Sie einer Wert für **Dem Cache zugewiesener Speicher** an, der groß genug ist, um alle temporären Daten zu speichern. Dies ist nur möglich, wenn für jede VM eine große Menge RAM zum Zuweisen verfügbar ist.
- Wenn Sie beide Kontrollkästchen deaktivieren, werden temporäre Daten nicht zwischengespeichert. Für jede VM wird auf den differenzierenden Datenträger (im Betriebssystemspeicher) geschrieben. (Dies ist die Provisioning-Aktion in Releases vor 7.9.)
- Aktivieren Sie die Zwischenspeicherung nicht, wenn ein Katalog zum Erstellen von AppDisks verwendet werden soll.
- Die Cachewerte für einen Maschinenkatalog können nach dessen Erstellung nicht geändert werden.

Verwenden von CSV-Dateien zum Massenhinzufügen von Maschinen Bei Verwendung der Verwaltungsschnittstelle **Vollständige Konfiguration** können Sie Maschinen mit CSV-Dateien in großer Zahl hinzufügen. Das Feature steht für alle Katalogen mit Ausnahme solcher zur Verfügung, die per MCS erstellt wurden.

Dies ist ein allgemeiner Workflow zum Massenhinzufügen von Maschinen mit CSV-Dateien:

1. Wählen Sie auf der Seite **Maschinen** die Option **CSV-Datei hinzufügen**. Das Fenster **Maschinen in Massen hinzufügen** wird angezeigt.
2. Wählen Sie **CSV-Vorlage herunterladen**.
3. Füllen Sie die Vorlagendatei aus.
4. Navigieren Sie zu der Datei, um sie hochzuladen (oder verwenden Sie Drag & Drop).
5. Wählen Sie **Validieren**, um Ihren Import zu überprüfen.
6. Wählen Sie zum Abschluss **Importieren**.

Weitere Überlegungen zu CSV-Dateien finden Sie unter Überlegungen zum Hinzufügen von Maschinen über CSV-Dateien.

Sie können Maschinen auch aus einem Katalog auf derselben Seite “Maschinen”exportieren. Die CSV-Datei mit exportierten Maschinen kann dann als Vorlage verwendet werden, wenn Maschinen in

großen Mengen hinzugefügt werden. Gehen Sie zum Exportieren von Maschinen folgendermaßen vor:

1. Wählen Sie auf der Seite **Maschinen** die Option **Als CSV-Datei exportieren**. Eine CSV-Datei mit einer Liste der Maschinen wird heruntergeladen.
2. Öffnen Sie die CSV-Datei, um Maschinen nach Bedarf hinzuzufügen oder zu bearbeiten. Informationen zum Massenhinzufügen von Maschinen mit der gespeicherten CSV-Datei finden Sie im vorherigen Abschnitt Verwenden von CSV-Dateien zum Massenhinzufügen von Maschinen.

> **Hinweis:**
>
> - Das Feature ist für Remote-PC-Zugriff-Kataloge nicht verfügbar.
> - Der Export und Import von Maschinen in CSV-Dateien wird nur zwischen Katalogen desselben Typs unterstützt.

Netzwerkkarten für die Maschinen konfigurieren

Die Seite **Netzwerkkarten** wird nicht angezeigt, wenn Sie auf der Seite **Maschinentyp** die Option **Remote-PC-Zugriff** auswählen.

Wenn Sie mehrere Netzwerkkarten verwenden möchten, weisen Sie jeder ein virtuelles Netzwerk zu. Sie können beispielsweise einer Karte ein bestimmtes sicheres Netzwerk und einer anderen ein häufiger verwendetes Netzwerk zuweisen. Auf dieser Seite können Sie auch Netzwerkkarten hinzufügen und entfernen.

Maschinenkonten hinzufügen

> **Hinweis:**
>
> Die Seite **Computerkonten** wird nur angezeigt, wenn Sie auf der Seite **Maschinentyp** die Option **Remote-PC-Zugriff** auswählen.

Fügen Sie die Active Directory-Maschinenkonten oder Organisationseinheiten (OUs) hinzu. Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten.

Sie können eine zuvor konfigurierte Energieverwaltungsverbindung auswählen oder die Energieverwaltung nicht verwenden. Wenn Sie die Energieverwaltung verwenden möchten, jedoch noch keine geeignete Verbindung konfiguriert wurde, können Sie die Verbindung später erstellen und dann die Energieverwaltungseinstellungen des Maschinenkatalogs entsprechend bearbeiten.

Sie können auch CSV-Dateien zum Massenhinzufügen von Maschinen verwenden. Dies ist ein allgemeiner Workflow dafür:

1. Wählen Sie auf der Seite **Maschinenkonten** die Option **CSV-Datei hinzufügen**. Das Fenster **Maschinen in Massen hinzufügen** wird angezeigt.
2. Wählen Sie **CSV-Vorlage herunterladen**.
3. Füllen Sie die Vorlagendatei aus.
4. Navigieren Sie zu der Datei, um sie hochzuladen (oder verwenden Sie Drag & Drop).
5. Wählen Sie **Validieren**, um Ihren Import zu überprüfen.
6. Wählen Sie zum Abschluss **Importieren**.

Weitere Überlegungen zu CSV-Dateien finden Sie unter Überlegungen zum Hinzufügen von Maschinen über CSV-Dateien.

Identitäten für Maschinen im Katalog konfigurieren

> **Hinweis:**
>
> - Die Seite **Maschinenidentitäten** wird nur angezeigt, wenn Sie auf der Seite **Maschinentyp** nicht **Remote-PC-Zugriff** und auf der Seite **Maschinenverwaltung** die Option **Citrix Maschinenerstellungsdienst (MCS)** auswählen.

Jede Maschine im Katalog muss eine eindeutige Identität haben. Auf dieser Seite können Sie Identitäten für Maschinen im Katalog konfigurieren. Die Maschinen werden nach ihrem Provisioning mit der Identität verbunden. Sie können den Identitätstyp nicht mehr ändern, wenn Sie den Katalog erstellt haben.

Der allgemeine Workflow zum Konfigurieren von Einstellungen auf dieser Seite ist folgender:

1. Sie wählen eine Identität aus der Liste aus.
2. Sie geben an, ob neue Konten erstellt oder vorhandene Konten verwendet werden sollen, und Sie geben den Speicherort (Domäne) für diese Konten an.

Sie können eine der folgenden Optionen auswählen:

- **On-premises Active Directory**: Maschinen, die der Organisation gehören und mit einem Active Directory-Konto dieser Organisation angemeldet sind. Sie existieren on-premises.

  > **Hinweis:**
  >
  > Standardmäßig ist die Domäne ausgewählt, in der sich die Ressource (Verbindung) befindet.

- **In Azure AD eingebunden**: Maschinen, die der Organisation gehören und mit einem Azure Active Directory-Konto dieser Organisation angemeldet sind. Sie existieren nur in der Cloud. Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter In Azure Active Directory eingebunden.

> **Hinweis:**
>
> Für diese Option muss das Masterimage die Voraussetzung für das Betriebssystem erfüllen. Weitere Informationen finden Sie in der Microsoft-Dokumentation Microsoft Entra joined devices.

- **Azure Active Directory-Hybrideinbindung**. Maschinen, die der Organisation gehören und mit einem Active Directory Domain Services-Konto dieser Organisation angemeldet sind. Sie existieren in der Cloud und on-premises. Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter Azure Active Directory-Hybrideinbindung.

  > **Hinweis:**
  >
  > – Vor Verwendung der Azure Active Directory-Hybrideinbindung müssen Sie sicherstellen, dass Ihre Azure-Umgebung die Voraussetzungen erfüllt. Weitere Informationen finden Sie unter Microsoft Entra-Hybrid-Einbindung konfigurieren.
  > – Für diese Option muss das Masterimage die Voraussetzung für das Betriebssystem erfüllen. Weitere Informationen finden Sie unter Eingebundene Microsoft Entra-Hybridgeräte.

- **Nicht domänengebunden.**. Maschinen, die keiner Domäne angehören Informationen zu Anforderungen und Einschränkungen finden Sie unter Nicht domänengebunden.

> **Wichtig:**
>
> - Wenn Sie **On-Premises-Active Directory** oder **Azure Active Directory-Hybrideinbindung** als Identittätstyp auswählen, benötigt jede Maschine im Maschinenkatalog ein Active Directory-Computerkonto.
> - Für den Identitätstyp **Gehört keiner Domäne an** ist VDA-Version 1811 oder höher als Mindestfunktionsebene für den Katalog erforderlich. Zur Bereitstellung aktualisieren Sie die Mindestfunktionsebene.
> - Die Identitätstypen **In Azure Active Directory eingebunden** und **Azure Active Directory-Hybrideinbindung** erfordern VDA-Version 2203 oder höher als minimale Funktionsebene für den Katalog. Zur Bereitstellung aktualisieren Sie die Mindestfunktionsebene.

Beim Erstellen von Konten müssen Sie berechtigt sein, Computerkonten in der Organisationseinheit zu erstellen, in der sich die Maschinen befinden. Jede Maschine im Katalog muss einen eindeutigen Namen haben. Geben Sie das Kontobenennungsschema für die Maschinen an, die Sie erstellen möchten. Weitere Informationen finden Sie unter Benennungsschema für Maschinenkonten.

> **Hinweis:**

> Vergewissern Sie sich, dass OU-Namen keine Schrägstriche (/) enthalten.

Wenn Sie bestehende Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf **Importieren** und geben Sie eine `.csv`-Datei mit den Kontonamen an. Die importierte Datei muss folgendes Format haben: `[ADComputerAccount] ADcomputeraccountname.domain`

Vergewissern Sie sich, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Die Konten werden in der Oberfläche "Vollständige Konfiguration"verwaltet. Gestatten Sie darum der Oberfläche, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort an (muss für alle Konten gleich sein).

Bei Katalogen mit physischen oder vorhandenen Maschinen wählen Sie vorhandene Konten aus oder importieren Sie diese, und weisen Sie jeder Maschine sowohl ein Active Directory-Computerkonto als auch ein Benutzerkonto zu.

Benennungsschema für Maschinenkonten Jede Maschine in einem Katalog muss einen eindeutigen Namen haben. Sie müssen ein Benennungsschema für Maschinenkonten angeben, wenn Sie einen Katalog erstellen. Verwenden Sie Platzhalter (Rauten) für fortlaufende Zahlen oder Buchstaben, die im Namen vorkommen.

Beachten Sie bei der Angabe eines Benennungsschemas Folgendes:

- Die maximal zulässige Anzahl von Zeichen ist 15.
- Das Benennungsschema muss mindestens einen Platzhalter enthalten. Alle Platzhalter müssen zusammen sein.
- Der Name muss einschließlich Platzhaltern aus 2 bis 15 Zeichen bestehen. Es muss mindestens ein nicht numerisches Zeichen und ein #-Zeichen (Platzhalter) enthalten.
- Der Name darf keine Leerzeichen und keines der folgenden Zeichen enthalten: `,~!@'$%^&.()} { \/*?"<>|=+[];:_".`
- Der Name darf nicht mit einem Bindestrich (-) enden.
- Die Anzahl der Zeichen steigt mit der Anzahl der Maschinenkonten. Wenn Sie beispielsweise 1.000 Maschinenkonten mit dem Schema "veryverylong#"erstellen, enthält der zuletzt erstellte Kontoname (veryverylong1000) 16 Zeichen, was die Anzahl der maximal zulässigen Zeichen überschreitet.

Sie können angeben, ob es sich bei den sequentiellen Werten um Zahlen (0–9) oder Buchstaben (A–Z) handelt.

- **0-9**. Bei Auswahl dieser Option werden die angegebenen Platzhalter in fortlaufende Nummern aufgelöst.

> **Hinweis:**
>
> Wenn nur ein Platzhalter (#) vorhanden ist, beginnen Kontonamen mit 1. Bei zwei vorhandenen Platzhaltern beginnen Kontonamen mit 01. Bei drei vorhandenen Platzhaltern beginnen Kontonamen mit 001 usw.

- **A-Z**. Bei Auswahl dieser Option werden die angegebenen Platzhalter in fortlaufende Buchstaben aufgelöst.

Beispiel: Das Benennungsschema "PC-Vertrieb-##"(und Aktivieren von **0-9**) bewirkt eine Benennung der Konten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03"usw.

Optional können Sie angeben, womit die Kontonamen beginnen sollen.

- Wenn Sie **0-9** auswählen, werden die Konten sequentiell, beginnend mit den angegebenen Zahlen benannt. Geben Sie eine oder mehrere Zahlen ein, je nachdem, wie viele Platzhalter Sie verwenden. Wenn Sie beispielsweise zwei Platzhalter verwenden, geben Sie mindestens zwei Zahlen ein.
- Wenn Sie **A-Z** auswählen, werden die Konten sequentiell, beginnend mit den angegebenen Buchstaben benannt. Geben Sie eine oder mehrere Buchstaben ein, je nachdem, wie viele Platzhalter Sie verwenden. Wenn Sie beispielsweise zwei Platzhalter verwenden, geben Sie mindestens zwei Buchstaben ein.

Domänenanmeldeinformationen hinzufügen

Wählen Sie **Anmeldeinformationen eingeben** und geben Sie die Anmeldeinformationen eines Administrators mit der Berechtigung zum Ausführen von Kontovorgängen in der Active Directory-Zieldomäne ein.

Überprüfen Sie mit der Option **Name überprüfen**, ob der Benutzername gültig oder eindeutig ist. Diese Option kann in folgenden Situationen von Nutzen sein:

- Der Benutzername existiert in mehreren Domänen. Sie werden aufgefordert, den gewünschten Benutzer auszuwählen.
- Sie können sich nicht an den Domänennamen erinnern. Sie können den Benutzernamen ohne Angabe des Domänennamens eingeben. Bei erfolgreicher Überprüfung wird der Domänenname automatisch eingegeben.

> **Hinweis:**
>
> Wenn Sie unter **Maschinenidentitäten** den Identitätstyp **Azure Active Directory-Hybrideinbindung** ausgewählt haben, muss den von Ihnen eingegebenen Anmeldeinformationen die Berechtigung `Write userCertificate` erteilt worden sein.

Wählen Sie einen Workspace Environment Management-Konfigurationssatz aus (optional)

Die Seite **WEM** wird nur angezeigt, wenn Sie die Advanced oder Premium Edition von Citrix DaaS verwenden.

Wählen Sie einen WEM-Konfigurationssatz (Workspace Environment Management) aus, an den der Katalog gebunden werden soll. Ein Konfigurationssatz ist ein logischer Container zum Organisieren eines Satzes von WEM-Konfigurationen. Durch Binden eines Katalogs an einen Konfigurationssatz können Sie mit WEM den Benutzern die bestmögliche Workspace-Erfahrung bieten.

> **Wichtig:**
>
> - Bevor Sie einen Katalog an einen Konfigurationssatz binden können, müssen Sie Ihre WEM Service-Bereitstellung einrichten. Melden Sie sich bei Citrix Cloud an und starten Sie dann den WEM Service. Weitere Informationen finden Sie unter Erste Schritte mit dem Workspace Environment Management Service.
> - Wenn Sie WEM bereits verwenden, sind die Maschinen im Katalog, die Sie bereitstellen möchten, möglicherweise bereits in einem Konfigurationssatz vorhanden. Zum Beispiel über Active Directory. In diesem Fall empfehlen wir, die Konfiguration konsequent mit Active Directory durchzuführen und diese Konfiguration zu überspringen.

Wenn der ausgewählte Konfigurationssatz keine mit der Grundkonfiguration von WEM verbundenen Einstellungen enthält, wird die folgende Option angezeigt:

- **Grundeinstellungen auf Konfigurationssatz anwenden**. Mit dieser Option werden Grundeinstellungen auf den Konfigurationssatz angewendet, was einen schnellen Einstieg in WEM ermöglicht. Zu den Grundeinstellungen gehören Schutz vor CPU-Spitzen, automatische Verhinderung von CPU-Spitzen und intelligente CPU-Optimierung. Klicken Sie zum Anzeigen der Grundeinstellungen auf den Link *hier*. Sie können die Grundeinstellungen mit der WEM-Konsole ändern.

VDA aktualisieren (optional)

> **Wichtig:**
>
> - Um ein reibungsloses Upgrade zu gewährleisten, stellen Sie sicher, dass die Voraussetzungen erfüllt sind, und prüfen Sie bekannte Probleme, bevor Sie VDAs auf CR- oder LTSR-CU-Versionen aktualisieren. Siehe Aktualisieren von VDAs über die Benutzeroberfläche “Vollständige Konfiguration”
> - Achten Sie beim Upgrade von LTSR-VDAs auf LTSR Cumulative Update-Versionen darauf, dass die Version der auf den VDAs ausgeführten VDA Upgrade Agents 7.36.0.7 oder höher ist. Weitere Informationen finden Sie unter Aktualisieren von VDAs über die Benutzerober-

> fläche “Vollständige Konfiguration”.

Dieses Feature gilt für die folgenden Maschinentypen:

- Mit MCS bereitgestellte persistente Maschinen. Sie stellen sie bei der Katalogerstellung mit **Citrix Maschinenerstellungsdiensten (MCS)** auf der Seite **Maschinenverwaltung** bereit.
- Maschinen, die nicht mit MCS erstellt wurden (z. B. physische Maschinen). Sie stellen sie während der Katalogerstellung mit **Anderer Dienst oder andere Technologie** auf der Seite **Maschinenverwaltung** bereit.

Weitere Informationen zu den beiden Optionen finden Sie unter Maschinenverwaltung.

Wählen Sie auf der Seite **VDA-Upgrade** die gewünschte VDA-Version aus. Falls angegeben, können die VDAs in dem Katalog, auf denen der VDA Upgrade Agent installiert ist, sofort oder zu einem geplanten Zeitpunkt auf die ausgewählte Version aktualisiert werden.

> **Hinweis:**
>
> - Dieses Feature unterstützt nur Upgrades auf den neuesten VDA. Der Zeitpunkt, zu dem Sie einen VDA-Upgradezeitplan erstellen oder einen VDA aktualisieren, bestimmt die neueste Version des VDA.
> - Nach dem Konfigurieren der VDA-Upgradeeinstellungen kann es bis zu 15 Minuten dauern, bis das Feld **VDA-Upgrade** entsprechend aktualisiert wird. Zur Anzeige der Spalte **VDA-Upgrade** klicken Sie auf das Symbol “Anzuzeigende Spalten”in der oberen rechten Ecke, wählen Sie **Maschinenkatalog > VDA-Upgrade** aus und klicken Sie auf **Speichern**.

Wählen Sie einen für Ihre Bereitstellung geeigneten VDA-Track:

> **Wichtig:**
>
> Sie können zwischen CR VDA und LTSR VDA wechseln, sofern Sie von einer früheren Version zu einer späteren wechseln. Sie können nicht von einer späteren Version zu einer früheren Version wechseln, da dies als Downgrade betrachtet wird. Sie können beispielsweise nicht von 2212 CR auf 2203 LTSR (alle CUs) wechseln, ein Upgrade von 2112 CR auf 2203 LTSR (alle CUs) ist dagegen möglich.

- **Neuester CR VDA**. Aktuelle Releases bieten die neuesten und innovativsten Virtualisierungsfeatures für Apps, Desktops und Server.
- **Neuester LTSR VDA**. Long Term Service Releases (LTSRs) werden empfohlen für Produktionsumgebungen großer Unternehmen, die dieselbe Basisversion für einen längeren Zeitraum beibehalten möchten.

Nach der Katalogerstellung können Sie VDAs nach Bedarf aktualisieren. Weitere Informationen finden Sie unter Upgrade von VDAs.

Wenn Sie das VDA-Upgrade später aktivieren möchten, können Sie zu dieser Seite zurückkehren, indem Sie den Katalog nach der Katalogerstellung bearbeiten. Weitere Informationen finden Sie unter Konfigurieren von VDA-Upgradeeinstellungen durch Bearbeiten des Katalogs.

Einstellungen überprüfen

Überprüfen Sie auf der Seite **Zusammenfassung** die von Ihnen angegebenen Informationen. Geben Sie einen Namen und eine Beschreibung für den Katalog ein. Diese Informationen werden in der Verwaltungsoberfläche "Vollständige Konfiguration"angezeigt.

Wenn Sie fertig sind, wählen Sie **Fertig stellen**, um das Erstellen des Katalogs zu starten.

In **Maschinenkataloge** wird der neue Katalog mit einem Fortschrittsbalken angezeigt.

Gehen Sie zum Anzeigen von Details zum Erstellungsfortschritt folgendermaßen vor:

1. Zeigen Sie mit der Maus auf den Maschinenkatalog.
2. Klicken Sie in der angezeigten QuickInfo auf **Details anzeigen**.

   Ein Fortschrittsdiagramm wird angezeigt, in dem Sie Folgendes sehen können:

   - Geschichte der Schritte
   - Fortschritt und Laufzeit des aktuellen Schritts
   - Restliche Schritte

MCS-Maschinenkatalog mit PowerShell-Befehlen erstellen

Sie können den MCS-Maschinenkatalog auch mit PowerShell-Befehlen erstellen. Weitere Informationen:

- SDKs und APIs
- Citrix DaaS mit Remote PowerShell SDKs verwalten
- Neues ProvScheme

Laufwerksbuchstaben zu einem MCS-E/A-Zurückschreibcache-Datenträger zuweisen

Sie können dem MCS-E/A-Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zuweisen. Diese Implementierung hilft bei der Vermeidung von Konflikten zwischen dem Laufwerksbuchstaben verwendeter Anwendungen und dem Laufwerksbuchstaben des MCS-E/A-Zurückschreibcache-Datenträgers. Sie können dazu PowerShell-Befehle verwenden. Die unterstützten Hypervisors sind Azure, GCP, VMware, SCVMM und XenServer.

> **Hinweis:**
>
> Für dieses Feature ist VDA-Version 2305 oder höher erforderlich.

Einschränkungen

- Gilt nur für Windows-Betriebssysteme
- Möglicher Laufwerksbuchstabe für Zurückschreibcache-Datenträger: E bis Z
- Nicht möglich bei Verwendung des temporären Azure-Datenträgers als Zurückschreibcache-Datenträger
- Gilt nur, wenn Sie einen neuen Maschinenkatalog erstellen

Einem Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zuweisen Gehen Sie zum Zuweisen eines Laufwerksbuchstabens zum Zurückschreibcache-Datenträger folgendermaßen vor:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden. Weitere Informationen finden Sie unter Katalog erstellen.
4. Erstellen Sie mit dem Befehl `New-ProvScheme` mit der Eigenschaft `WriteBackCacheDriveLetter` ein Provisioningschema. Beispiel:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
```



```
14 <Property xsi:type="StringProperty" Name="OsType" Value="Windows"
      />
15 <Property xsi:type="StringProperty" Name="StorageType" Value="
      Premium_LRS"/>
16 <Property xsi:type="StringProperty" Name="PersistWBC" Value="false
      " />
17 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
      false" />
18 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"
       />
19 <Property xsi:type="StringProperty" Name="WBCDiskStorageType"
      Value="Premium_LRS" />
20 <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
      ="false" />
21 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
      abcd-group1" />
22 <Property xsi:type="StringProperty" Name="LicenseType" Value="
      Windows_Client" />
23 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
       />
24 </CustomProperties>'
25 <!--NeedCopy-->
```

5. Beenden Sie die Erstellung des Maschinenkatalogs.

Richtlinien zum Festlegen benutzerdefinierter Eigenschaften

Benutzerdefinierte Eigenschaften müssen bei `New-ProvScheme` und `Set-ProvScheme` in GCP- und Azure-Umgebungen korrekt festgelegt sein. Wenn Sie nicht vorhandene benutzerdefinierte Eigenschaften angeben, wird die folgende Fehlermeldung angezeigt, und die Befehle werden nicht ausgeführt.

```
Invalid property found: <invalid property>. Ensure that the CustomProperties
 parameter supports the property.
```

Wichtige Überlegungen zum Festlegen von ProvScheme-Parametern

Wenn Sie einen Katalog mit MCS erstellen, wird in folgenden Fällen eine Fehlermeldung angezeigt:

- Sie legen die folgenden `New-ProvScheme`-Parameter in nicht unterstützten Hypervisors fest, wenn Sie einen Maschinenkatalog erstellen:

Parameter	Unterstützter Hypervisor
`UseWriteBackCache`	VMware Hyper-V

Parameter	Unterstützter Hypervisor
	XenServer
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP
	AWS
`UseFullDiskCloneProvisioning`	VMware
	Hyper-V
	XenServer

- Sie aktualisieren die folgenden `Set-ProvScheme`-Parameter, nachdem Sie den Maschinenkatalog erstellt haben:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

SIDs beim Erstellen virtueller Maschinen hinzufügen

Sie können den Parameter `ADAccountSid` hinzufügen, um die Maschinen beim Erstellen neuer virtueller Maschinen eindeutig zu identifizieren.

Gehen Sie hierzu folgendermaßen vor:

1. Erstellen Sie einen Katalog mit dem unterstützten Identitätstyp.
2. Fügen Sie dem Katalog mit `NewProvVM` Maschinen hinzu. Beispiel:

```
1 New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
     )  -RunAsynchronously
2 <!--NeedCopy-->
```


Folgendes können Sie nicht auf einer Maschine bereitstellen:

- Ein AD-Konto, das sich nicht im Katalogidentitätspool befindet.
- Ein AD-Konto, das nicht im Status “Verfügbar”ist

Überprüfen Sie die Konfiguration, bevor Sie einen MCS-Maschinenkatalog erstellen

Sie können die Konfigurationseinstellungen überprüfen, bevor Sie einen MCS-Maschinenkatalog erstellen, indem Sie den Parameter `-validate` im Befehl `New-ProvScheme` verwenden. Nachdem Sie diesen PowerShell-Befehl mit dem Parameter ausgeführt haben, erhalten Sie eine entsprechende Fehlermeldung, wenn ein falscher Parameter verwendet wird oder ein Parameter mit einem anderen Parameter in Konflikt steht. Anschließend können Sie die Fehlermeldung verwenden, um das Problem zu beheben und mithilfe von PowerShell erfolgreich einen MCS-Maschinenkatalog zu erstellen. Derzeit ist dieses Feature auf Azure-, GCP- und VMware-Virtualisierungsumgebungen anwendbar.

> **Hinweis:**
>
> Während der Validierung dürfen Sie keinen tatsächlichen MCS-Maschinenkatalog erstellen. Sie müssen das Ergebnis des Befehls verwenden, um die Fehler zu beheben und dann einen erfolgreichen Katalog zu erstellen. Verwenden Sie daher beim Ausführen des Befehls `New-ProvScheme` einen falschen Identitätspoolnamen.

Gehen Sie wie folgt vor, um die Konfiguration zu überprüfen:

1. Öffnen Sie ein PowerShell-Fenster vom Delivery Controller-Host aus.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den Befehl `New-ProvScheme` aus und verwenden Sie den Parameter `-validate`. Geben Sie einen falschen Identitätspoolnamen an, damit der Befehl funktioniert. Zum Beispiel:

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
    Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
    FunctionalLevel "L7_20" -Validate
$result.TerminatingError | Format-List -Property *
<!--NeedCopy-->
```

Fehlermeldung:


```
ErrorData    : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
Operation    : ValidatingInputs
<!--NeedCopy-->
```

4. Nach der Validierung der Konfigurationseinstellung können Sie einen MCS-Maschinenkatalog mit einem echten Identitätspoolnamen und korrekten Parametern erstellen.

So geht es weiter

Informationen zum Erstellen bestimmter Hypervisor-Kataloge finden Sie unter:

- AWS-Katalog erstellen
- Google Cloud Platform-Katalog erstellen
- Microsoft Azure-Katalog erstellen
- Microsoft System Center Virtual Machine Manager-Katalog erstellen
- Nutanix-Katalog erstellen
- VMware-Katalog erstellen
- XenServer-Katalog erstellen

Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.

Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.

Sie können einen Citrix Provisioning-Katalog mithilfe der Benutzeroberfläche “Vollständige Konfiguration”und PowerShell erstellen.
Diese Implementierung bietet Ihnen die folgenden Vorteile:

- Eine einzige, einheitliche Konsole zur Verwaltung von MCS- und Citrix Provisioning-Katalogen.

- Neue Features für Citrix Provisioning-Kataloge, wie eine Identitätsverwaltungslösung, On-Demand-Provisioning und so weiter.

Derzeit ist dieses Feature nur für Azure- und VMware-Workloads verfügbar. In VMware-Umgebungen können Sie die Kataloge derzeit jedoch nur mit PowerShell-Befehlen erstellen. Weitere Informationen finden Sie unter Citrix Provisioning-Kataloge in Citrix Studio erstellen.

Weitere Informationen

- Citrix Virtual Apps and Desktops Image Management
- Verbindungen und Ressourcen erstellen und verwalten
- Mit Maschinenidentitäten verbundene Kataloge erstellen
- Maschinenkataloge verwalten

AWS-Katalog erstellen

May 17, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf AWS-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen AWS-Katalog erstellen, müssen Sie eine Verbindung zu AWS hergestellt haben. Siehe Verbindung zu AWS.

Netzwerkeinstellung während der Imagevorbereitung

Während der Imagevorbereitung wird eine virtuelle Vorbereitungsmaschine (Vorbereitungs-VM) basierend auf der ursprünglichen VM erstellt. Diese Vorbereitungs-VM ist vom Netzwerk getrennt. Zum Trennen des Netzwerks von der Vorbereitungs-VM wird eine Netzwerksicherheitsgruppe erstellt, um den gesamten eingehenden und ausgehenden Datenverkehr zu blockieren. Diese Netzwerksicherheitsgruppe bleibt bestehen und wird wiederverwendet. Der Name der Netzwerksicherheitsgruppe lautet `Citrix.XenDesktop.IsolationGroup-GUID`, wobei die GUID nach dem Zufallsprinzip generiert wird.

AWS-Tenancy

AWS bietet die folgenden Tenancy-Optionen an: Freigegeben (Standardoption) und Dediziert. Bei einer freigegebenen Tenancy können sich die Amazon EC2-Instanzen mehrerer Kunden auf derselben

physischen Hardware befinden. Bei der dedizierten Tenancy ist die Hardware zur Ausführung der EC2-Instanzen und anderer, vom Kunden entwickelter Instanzen nur einem Kunden vorbehalten. Sie wird nicht von anderen Kunden verwendet.

Sie können MCS verwenden, um dedizierte AWS-Hosts über die Benutzeroberfläche für die vollständige Konfiguration oder PowerShell bereitzustellen.

Anforderungen für die Bereitstellung für AWS-Hosts

- Ein importiertes Bring Your Own License-Image (AMI). Mit dedizierten Hosts können Sie Ihre vorhandenen Lizenzen verwenden und verwalten.
- Eine Zuordnung dedizierter Hosts mit ausreichender Nutzungskapazität.
- Aktivierung von **Automatische Platzierung**.

Konfigurieren der dedizierten AWS-Hostmandantenschaft über die Benutzeroberfläche für die vollständige Konfiguration

Wenn Sie mit MCS Kataloge zur Bereitstellung von Maschinen in AWS erstellen, werden auf der Seite **Maschinenkatalogerstellung > Sicherheit** die folgenden Optionen angezeigt:

- **Freigegebene Hardware verwenden:** Diese Einstellung ist für die meisten Bereitstellungen geeignet. Mehrere Kunden teilen sich Hardware, ohne jedoch miteinander zu interagieren. Die Verwendung gemeinsam genutzter Hardware ist die kostengünstigste Amazon EC2-Option.
- **Dedizierten Host verwenden:** Ein dedizierter Amazon EC2-Host ist ein physischer Server mit EC2-Instanzkapazität, der vollständig dediziert ist und die Verwendung vorhandener Socket- oder VM-Softwarelizenzen gestattet. Für dedizierte Hosts gilt eine voreingestellte Nutzung basierend auf dem Instanztyp. Ein einzelner dedizierter Host des Instanztyps C4 Large ist beispielsweise auf die Ausführung von 16 Instanzen beschränkt. Weitere Informationen finden Sie auf der AWS-Website.
- **Dedizierte Instanz verwenden**. Diese Einstellung ist für Bereitstellungen geeignet, die bestimmten Sicherheitsanforderungen oder rechtlichen Bestimmungen genügen müssen. Bei einer dedizierten Instanz profitieren Sie von der Trennung des Hosts von dem anderer AWS-Kunden, zahlen aber nicht für den gesamten Host. Sie müssen sich keine Gedanken um die Kapazität des Hosts machen, für die Instanzen wird jedoch eine höhere Gebühr berechnet.

  Diese Einstellung eignet sich für Bereitstellungen mit Lizenzbeschränkungen oder Sicherheitsanforderungen, die die Verwendung eines dedizierten Hosts erfordern. Ein dedizierter Host wird ausschließlich für Sie verwendet und nach Stunden in Rechnung gestellt. Bei einem solchen Host können Sie ohne zusätzliche Kosten so viele EC2-Instanzen einrichten, wie der Host zulässt.

> **Hinweis:**
>
> Sie können alle verfügbaren Identitätsdatenträger zur Vorbereitung löschen, wenn keine laufende Aufgabe zur Katalogerstellung oder Image-Aktualisierung läuft.

Dedizierte AWS-Hostmandanten mit PowerShell konfigurieren

Alternativ können Sie dedizierte AWS-Hosts über PowerShell bereitstellen. Verwenden Sie das `New-ProvScheme`-Cmdlet, wobei der Parameter `TenancyType` auf `Host` festgelegt ist.

AWS-Instanzeigenschaft erfassen

Wenn Sie einen Katalog für die Bereitstellung von Maschinen über Maschinenerstellungsdienste (MCS) in AWS erstellen, wählen Sie ein AMI (Amazon Machine Image) als Masterimage des Katalogs. Von diesem AMI verwendet MCS einen Snapshot des Datenträgers.

> **Tipp:**
>
> Zur Verwendung der Erfassung der AWS-Instanzeigenschaft benötigen Sie eine VM, die dem AMI zugeordnet ist.

MCS liest Eigenschaften aus der Instanz, aus der das AMI stammt, und wendet die IAM-Rolle und -Tags (Identity and Access Management) der Maschine auf die für einen bestimmten Katalog bereitgestellten Maschinen an. Wenn Sie dieses optionale Feature verwenden, findet der Katalogerstellungsprozess die ausgewählte AMI-Quellinstanz und liest einen begrenzten Satz von Eigenschaften. Diese Eigenschaften werden dann in einer AWS-Startvorlage gespeichert, mit der Maschinen für den Katalog bereitgestellt werden. Alle Maschinen im Katalog erben die erfassten Instanzeigenschaften.

Erfasste Eigenschaften sind:

- IAM-Rollen – auf bereitgestellte Instanzen angewendet.
- Tags – auf bereitgestellte Instanzen, deren Datenträger und Netzwerkkarten angewendet. Die Tags werden auf flüchtige Citrix Ressourcen angewendet: S3-Bucket und -Objekte sowie AMIs, Snapshots und Startvorlagen.

> **Tipp:**
>
> Das Tagging flüchtiger Citrix Ressourcen ist optional und kann über die benutzerdefinierte Eigenschaft `AwsOperationalResourcesTagging` konfiguriert werden. Um Tags erfolgreich anzuwenden und einen AWS-Katalog mit Tagging von Betriebsressourcen zu erstellen, löschen Sie nicht die EC2-Instanz, die zum Erstellen des AMI-Images verwendet wurde.

AWS-Instanzeigenschaft erfassen

Sie können dieses Feature über die Spezifizierung der benutzerdefinierten Eigenschaft `AwsCaptureInstanceP` beim Erstellen eines Provisioningschemas für eine AWS-Hostingverbindung nutzen:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Weitere Informationen finden Sie unter New-ProvScheme.

> **Hinweis:**
>
> `AwsCaptureInstanceProperties` ist veraltet. Wir empfehlen, stattdessen Maschinenprofile zu verwenden, um Maschineneigenschaften für virtuelle Maschinen anzugeben.

AWS-Betriebsressource taggen

Ein Amazon Machine Image (AMI) ist eine virtuelle Appliance, die zum Erstellen einer virtuellen Maschine in der Amazon Cloud-Umgebung EC2 verwendet wird. Sie verwenden ein AMI, um Dienste bereitzustellen, die die EC2-Umgebung verwenden. Wenn Sie einen Katalog für die Bereitstellung von Maschinen über MCS für AWS erstellen, wählen Sie ein **AMI** als Gold-Image des Katalogs.

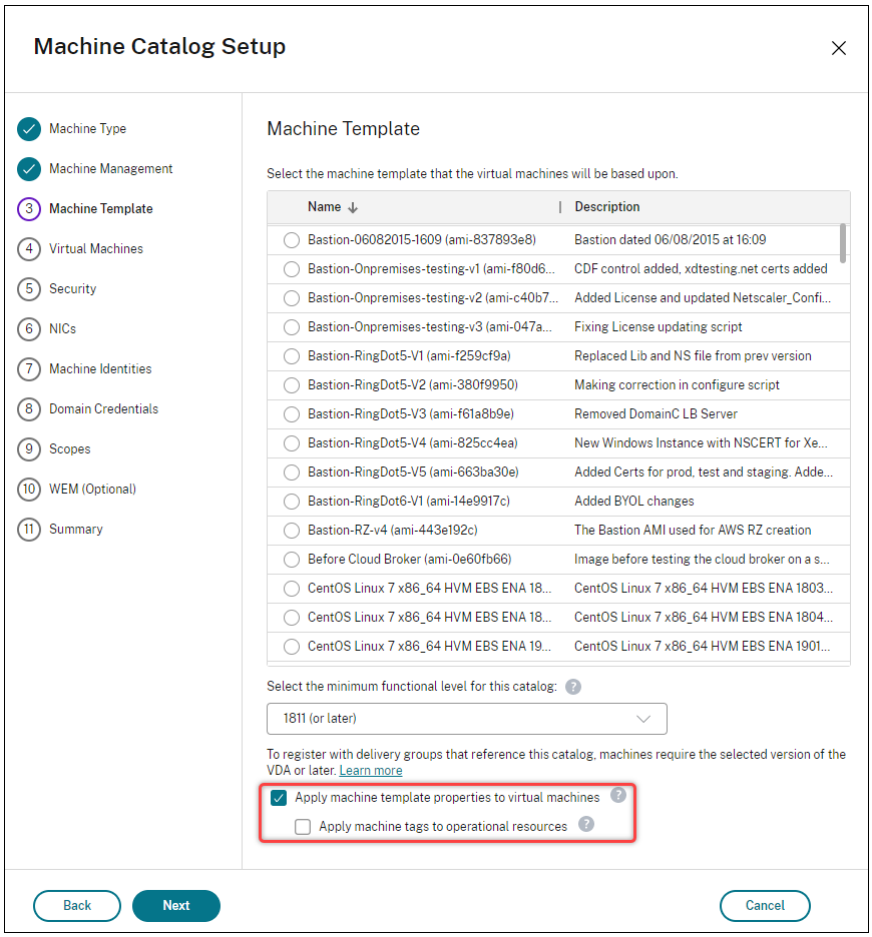
> **Wichtig:**
>
> Das Erstellen von Katalogen durch Erfassen einer Instanzeigenschaft und einer Startvorlage ist für die Verwendung des Taggings von Betriebsressourcen erforderlich.

Um einen AWS-Katalog zu erstellen, müssen Sie zunächst ein AMI für die Instanz erstellen, die als Gold-Image fungieren soll. MCS liest die Tags dieser Instanz und fügt sie in die Startvorlage ein. Die Startvorlagen-Tags werden dann auf alle in der AWS-Umgebung erstellten Citrix Ressourcen angewendet:

- Virtuelle Maschinen
- VM-Datenträger
- VM-Netzwerkschnittstellen
- S3-Buckets
- S3-Objekte
- Startvorlagen
- AMIs

AWS-Instanzeigenschaften anwenden und Betriebsressourcen in der Oberfläche “Vollständige Konfiguration”taggen

Wenn Sie einen Katalog zum Bereitstellen von Maschinen in AWS über die Maschinenerstellungsdienste erstellen, können Sie festlegen, ob Sie auf diese Maschinen die IAM-Rolle und Tag-Eigenschaften anwenden. Außerdem können Sie festlegen, ob Sie Maschinen-Tags auf Betriebsressourcen anwenden. Die folgenden zwei Optionen sind verfügbar:



- **Maschinenvorlageneigenschaften auf virtuelle Maschinen anwenden**
  - Steuert, ob die IAM-Rolle und die Tag-Eigenschaften, die der ausgewählten Maschinenvorlage zugeordnet sind, auf virtuelle Maschinen in diesem Katalog angewendet werden.
- **Maschinen-Tags auf Betriebsressourcen anwenden**
  - Steuert, ob Maschinen-Tags auf jedes Element in der AWS-Umgebung angewendet werden, das das Provisioning von Maschinen ermöglicht. Betriebsressourcen werden bei der Katalogerstellung als Nebenprodukte erstellt. Sie umfassen temporäre und persistente Ressourcen, zum Beispiel die Vorbereitungs-VM-Instanz und AMI.

Betriebsressource mit PowerShell taggen

Tagging von Ressourcen mit PowerShell:

1. Öffnen Sie ein PowerShell-Fenster vom DDC-Host aus.
2. Führen Sie den Befehl `asnp citrix` aus, um Citrix spezifische PowerShell-Module zu laden.

Verwenden Sie die benutzerdefinierte Eigenschaft `AwsOperationalResourcesTagging`, um eine Ressource für eine bereitgestellte VM zu taggen. Eigenschaftssyntax:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" ...<standard provscheme parameters
>
```

Erstellen Sie einen auf Maschinenprofilen basierenden Maschinenkatalog mit PowerShell

Sie können ein Maschinenprofil verwenden, um die Hardwareeigenschaften einer EC2-Instanz (VM) oder einer Startvorlagenversion zu erfassen und auf die bereitgestellten Maschinen anzuwenden. Erfasst werden können beispielsweise EBS-Volumeeigenschaften, Instanztyp, EBS-Optimierung, CPU-Optionen, Tenancy-Typ, Ruhezustandsfähigkeiten und weitere unterstützte AWS-Konfigurationen.

Sie können die Version einer AWS EC2-Instanz (VM) oder einer AWS-Startvorlage als Maschinenprofileingabe verwenden.

> **Hinweis:**
>
> EBS-Volumeeigenschaften werden nur aus einem Maschinenprofil abgeleitet.

Wichtige Überlegungen

Wichtige Überlegungen bei der Erstellung eines MCS-Maschinenkatalogs:

- Wenn Sie die Parameter für die Maschinenhardware-Eigenschaft in den Befehlen `New-ProvScheme` und `Set-ProvScheme` hinzufügen, überschreiben die in den Parametern angegebenen Werte die Werte im Maschinenprofil.
- Wenn Sie `AwsCaptureInstanceProperties` auf **`true`** festlegen, die Eigenschaft `MachineProfile` jedoch nicht festlegen, werden nur IAM-Rollen und -Tags erfasst.
- Sie können `AwsCaptureInstanceProperties` und `MachineProfile` nicht gleichzeitig festlegen.

> **Hinweis:
>
> `AwsCaptureInstanceProperties` ist veraltet.

- Wenn kein Maschinenprofil bereitgestellt wird, müssen Sie die Werte der folgenden Eigenschaften explizit angeben:
  - Sicherheitsgruppe
  - ENI oder Virtuelles Netzwerk
- Sie können `AwsOperationalResourcesTagging` nur aktivieren, wenn Sie `AwsCaptureInstanceP` aktivieren oder ein Maschinenprofil angeben.

Wichtige Überlegungen nach der Erstellung eines MCS-Maschinenkatalogs:

- Ein Maschinenkatalog, der auf einem Maschinenprofil basiert, kann nicht in einen Maschinenkatalog geändert werden, der nicht auf einem Maschinenprofil basiert.

Maschinenkatalog mit einem Maschinenprofil erstellen

So erstellen Sie einen Maschinenkatalog mit einem Maschinenprofil:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden. Zum Beispiel:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain abcdf -NamingSchemeType Numeric
<!--NeedCopy-->
```

4. Führen Sie den Befehl New-ProvScheme aus. Beispiel:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1
-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
-CleanOnBoot
-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
    demet-ami.0 (ami-0ca813xxxxxx061ef).template'
-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
    -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
    vm'
<!--NeedCopy-->
```

5. Schließen Sie das Erstellen des Katalogs ab.

Aktualisieren des Maschinenprofils

Gehen Sie zum Aktualisieren des Maschinenprofils in einem Katalog, der mit einem Maschinenprofil bereitgestellt wurde, wie folgt vor: Sie können auch den Tenancy-Typ und die Ruhezustandsfähigkeit der Maschinenprofilquelle ändern, während Sie einen MCS-Maschinenkatalog bearbeiten.

1. Führen Sie den Befehl `Set-ProvScheme` aus. Zum Beispiel:

```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
   availabilityzone\citrix-cvad-machineprofile-instance (i-0
   xxxxxxxx).vm"
<!--NeedCopy-->
```

Mit PowerShell einen Katalog mit Startvorlagenversion erstellen

Sie können einen MCS-Maschinenkatalog mit einer Startvorlagenversion als Maschinenprofileingabe erstellen. Sie können auch die Eingabe eines Maschinenprofilkatalogs von einer VM auf eine Startvorlagenversion und von einer Startvorlagenversion auf eine VM aktualisieren.

Auf der AWS EC2-Konsole können Sie die Instanzkonfigurationsangaben einer Startvorlage zusammen mit der Versionsnummer angeben. Wenn Sie beim Erstellen oder Aktualisieren eines Maschinenkatalogs die Startvorlagenversion als Maschinenprofileingabe angeben, werden die Eigenschaften aus dieser Startvorlagenversion auf die bereitgestellten VDA-VMs kopiert.

Die folgenden Eigenschaften können mithilfe der Maschinenprofileingabe oder explizit als Parameter in `New-ProvScheme`- oder `Set-ProvScheme`-Befehlen bereitgestellt werden. Wenn sie in `New-ProvScheme`- oder `Set-ProvScheme`-Befehlen bereitgestellt werden, haben sie Vorrang vor den Eigenschaftswerten im Maschinenprofil.

- Dienstangebot
- Netzwerke
- Sicherheitsgruppen
- Mandantenmodell

> **Hinweis:**
>
> Wenn das Dienstangebot nicht in der Startvorlage für das Maschinenprofil oder als Parameter im Befehl `New-ProvScheme` angegeben ist, wird eine Fehlermeldung angezeigt.

Erstellen eines Katalog mit der Startvorlagenversion als Maschinenprofileingabe:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.

3. Rufen Sie die Liste der Startvorlagenversionen einer Startvorlage auf. Beispiel:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Erstellen Sie einen Identitätspool (falls nicht vorhanden). Beispiel:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. Erstellen Sie ein Provisioningschema mit einer Startvorlagenversion als Maschinenprofileingabe. Beispiel:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

6. Registrieren Sie das Provisioningsschema als Brokerkatalog. Beispiel:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Schließen Sie das Erstellen des Katalogs ab.

Maschinenprofilquelle aktualisieren

Sie können auch die Eingabe eines Maschinenprofilkatalogs von einer VM auf eine Startvorlagenversion und von einer Startvorlagenversion auf eine VM aktualisieren. Beispiel:

- Aktualisieren der Eingabe eines Maschinenprofilkatalogs von einer VM auf eine Startvorlagenversion:


```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

- Aktualisieren der Eingabe eines Maschinenprofilkatalogs von einer Startvorlagenversion auf eine VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
<!--NeedCopy-->
```

Betriebssystem- und ID-Datenträger verschlüsseln

Sie können einen persistenten und nicht persistenten Katalog von VMs mit AWS-KMS-Schlüsseln (vom Kunden verwalteter Schlüssel und von AWS verwalteter Schlüssel) erstellen, die zum Verschlüsseln des Betriebssystemdatenträgers und des ID-Datenträgers verwendet werden können.

- Von AWS verwaltete Schlüssel werden jedes Jahr automatisch rotiert.
- Für vom Kunden verwaltete Schlüssel ist die automatische Rotation optional und sie können manuell verwaltet werden.

Weitere Informationen zu KMS-Schlüsseln finden Sie in den folgenden AWS-Dokumenten:

- AWS KMS-Konzepte
- So funktioniert die automatische Schlüsselrotation

Für die Verschlüsselung von Betriebssystem- und ID-Datenträgern konfigurieren Sie eine der folgenden Optionen:

- Verwenden Sie ein verschlüsseltes Masterimage (z. B. ein AMI, das aus einer Instanz oder einem Snapshot erstellt wurde und ein mit einem KMS-Schlüssel verschlüsseltes EBS-Root-Volume enthält)
- Verwenden Sie eine Maschinenprofilquelle (VM oder Startvorlage), die ein verschlüsseltes EBS-Root-Volume enthält.

Einschränkungen

Es gelten folgende Einschränkungen:

- MCS unterstützt derzeit nur einen Datenträger auf dem Master-Image-AMI.
- Sie können vorhandene unverschlüsselte EBS-Volumes oder Snapshots nicht direkt verschlüsseln oder den KMS-Schlüssel eines vorhandenen verschlüsselten Volumes ändern. Um das zu tun, müssen Sie:

  1. Einen neuen Snapshot dieses Volumes erstellen
  2. Ein neues Volume aus diesem Snapshot erstellen
  3. Das neue Volume verschlüsseln.

Lesen Sie die folgenden AWS-Dokumente:

- Unverschlüsselte Ressourcen verschlüsseln
- Einschränkungen der automatischen oder standardmäßigen Verschlüsselung von EBS-Volumes: Automatische Verschlüsselung vorhandener und neuer Amazon EBS-Volumes.

Einen Katalog mit Datenträgerverschlüsselung erstellen

Sie können einen MCS-Maschinenkatalog mit Datenträgerverschlüsselung erstellen, indem Sie Folgendes verwenden:

- Masterimage
- Maschinenprofil

Bei der Verwendung der Maschinenprofileingabe sind folgende Überlegungen zu berücksichtigen:

- Der KMS-Schlüssel der Maschinenprofileingabe hat Vorrang vor dem KMS-Schlüssel des Masterimages.
- Wenn keine Maschinenprofileingabe bereitgestellt wird, wird der KMS-Schlüssel des Master-Image-AMI verwendet, um die Datenträger der Katalog-VMs zu verschlüsseln.
- Wenn im Maschinenprofil Blockgerätzuordnungen vorhanden sind, müssen die Blockgeräte in der Master-Image-Vorlage (AMI) und im Maschinenprofil übereinstimmen. Wenn für AMI beispielsweise ein Gerät in `/dev/sda1` definiert ist, muss für das Maschinenprofil auch ein Gerät in `/dev/sda1` definiert sein.
- Wenn die Maschinenprofilquelle keinen Schlüssel enthält und das Masterimage unverschlüsselt ist, werden die Datenträger der Katalog-VMs nicht verschlüsselt.
- Wenn das Masterimage verschlüsselt ist, muss eine Maschinenprofil-Quell-VM oder eine Startvorlage über ein verschlüsseltes Root-Volume verfügen, um als gültige Eingabe betrachtet zu werden.

Einen vorhandenen Katalog ändern

Sie können einen vorhandenen Katalog mit dem PowerShell-Befehl `Set-ProvScheme` so ändern, dass er Folgendes umfasst:

- Eine Maschinenprofileingabe mit einem Volume, das einen neuen KMS-Schlüssel enthält.
- Ein Master-Image-Vorlagen-AMI, das mit einem neuen KMS-Schlüssel verschlüsselt ist.

Wichtige Überlegungen:

- Die Volumes neuer VMs, die dem Katalog hinzugefügt wurden, werden mit dem neuen KMS-Schlüssel verschlüsselt.
- Um die Verschlüsselungseinstellungen zu aktualisieren, wenn ein Maschinenprofil vorhanden ist, führen Sie `Set-ProvScheme` mit einem neuen Maschinenprofil aus.
- Sie können einen vorhandenen Katalog nicht von verschlüsselten Volumes zu unverschlüsselten Volumes ändern.
  Sie können kein Image-Update von einem verschlüsselten Master-AMI auf ein unverschlüsseltes Master-AMI durchführen.

Tags auf VMs kopieren

Sie können im Maschinenprofil angegebene Tags auf Netzwerkkarten und Datenträgern (Identitätsdatenträger, Zurückschreibcachedatenträger und OS-Datenträger) auf neu erstellte VMs in einem MCS-Maschinenkatalog kopieren. Sie können diese Tags in jeder Maschinenprofilquelle (AWS VM-Instanz oder AWS-Startvorlagenversion) angeben. Dieses Feature gilt für persistente und nicht persistente Maschinenkataloge und VMs.

> **Hinweis:**
>
> - Auf der AWS EC2-Konsole können Sie die Werte für **Tag Network Interfaces** unter den **Launch Template Version Resource Tags** nicht sehen. Sie können jedoch den PowerShell-Befehl `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` ausführen, um die Tagspezifikationen anzuzeigen.
> - Wenn eine Maschinenprofilquelle (VM- oder Startvorlagenversion) zwei Netzwerkschnittstellen (eni-1 und eni-2) hat, eni-1 das Tag t1 und eni-2 das Tag t2 hat, dann erhält die VM die Tags der beiden Netzwerkschnittstellen.

VM-Instanzen mit PowerShell filtern

Eine AWS-VM-Instanz, die Sie als Maschinenprofil-VM verwenden, muss kompatibel sein, damit der Maschinenkatalog erstellt werden kann und ordnungsgemäß funktioniert. Zum Auflisten der

AWS-VM-Instanzen, die als Eingabe-VMs für Maschinenprofile verwendet werden können, können Sie den Befehl `Get-HypInventoryItem` verwenden. Mit dem Befehl kann der Bestand der auf einer Hostingeinheit verfügbaren virtuellen Maschinen paginiert und gefiltert werden.

Paginierung:

Get-HypInventoryItem unterstützt zwei Paginierungsmodi:

- Der Seitenmodus verwendet die Parameter `-MaxRecords` und `-Skip`, um Gruppen von Elementen zurückzugeben:
  - `-MaxRecords`: Der Standardwert ist **1**. Dies steuert, wie viele Elemente zurückgegeben werden sollen.
  - `-Skip`: Der Standardwert ist **0**. Dies steuert, wie viele Elemente ab dem absoluten Anfang (oder absoluten Ende) der Liste im Hypervisor übersprungen werden sollen.
- Der Scrollmodus verwendet die Parameter `-MaxRecords`, `-ForwardDirection` und `-ContinuationToken`, um das Scrollen der Datensätze zu ermöglichen:
  - `-ForwardDirection`: Der Standardwert ist **True**. Dies wird zusammen mit `-MaxRecords` verwendet, um den nächsten Satz oder den vorherigen Satz übereinstimmender Datensätze zurückzugeben.
  - `-ContinuationToken`: Gibt die Elemente unmittelbar danach zurück (oder davor, falls `ForwardDirection` = **false**), jedoch ohne das in `ContinuationToken` angegebenen Element.

Beispiele der Paginierung:

- Um einen einzelnen Datensatz mit der Maschinenvorlage mit dem niedrigsten Namen zurückzugeben. Das Feld `AdditionalData` enthält `TotalItemsCount` und `TotalFilteredItemsCount`:

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template
2  <!--NeedCopy-->
```

- Ausgabe von 10 Datensätzen der Maschinenvorlage mit dem niedrigsten Namen:

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template -MaxRecords 10 | select Name
2  <!--NeedCopy-->
```

- Um ein Array von Datensätzen zurückzugeben, die mit dem höchsten Namen enden:

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template -ForwardDirection $False -MaxRecords 10
        | select Name
2  <!--NeedCopy-->
```


- Um ein Array von Datensätzen zurückzugeben, beginnend mit der Maschinenvorlage, die dem `ContinuationToken` zugeordnet ist:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

Filtern:

Die folgenden zusätzlichen optionalen Parameter werden für die Filterung unterstützt. Sie können diese Parameter mit den Paginierungsoptionen kombinieren.

- `-ContainsName "my_name"`: Wenn die angegebene Zeichenfolge einem Teil eines AMI-Namens entspricht, wird das AMI in das `Get`-Ergebnis aufgenommen. Beispiel:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ‘ apollo ’
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '` : Wenn ein AMI mindestens eines dieser Tags hat, wird es in das `Get` -Ergebnis aufgenommen. Beispiel:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Hinweis:**
>
> Zwei Tag-Werte werden unterstützt. Der Wert **Not Tagged** entspricht Elementen, die das angegebene Tag nicht in ihrer Tag-Liste haben. Der Wert **All Values** entspricht Elementen, die das Tag haben, unabhängig von dessen Wert. Andernfalls gilt es nur als Übereinstimmung, wenn das Element das Tag hat und der Wert der Angabe im Filter entspricht.

- `-Id "ami-0a2d913927e0352f3"`: Wenn das AMI mit der angegebenen ID übereinstimmt, wird es in das `Get`-Ergebnis aufgenommen. Beispiel:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```

Filtern nach dem Parameter “AdditionalData”:

Der Filterparameter `AdditionalData` listet Vorlagen oder VMs auf der Grundlage ihrer Funktionen, ihres Dienstangebots oder einer beliebigen Eigenschaft in “AdditionalData”auf. Beispiel:


```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
    AdditionalData
<!--NeedCopy-->
```

Sie können auch einen Parameter `-Warn` hinzufügen, um die nicht kompatiblen VMs anzugeben. Die VMs sind in einem `AdditionalData`-Feld mit dem Namen **Warning** enthalten. Beispiel:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und AWS-Katalog verwalten.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu AWS
- Maschinenkataloge erstellen

Google Cloud Platform-Katalog erstellen

May 22, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Google-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Google Cloud Platform (GCP)-Katalog erstellen, müssen Sie eine Verbindung zu GCP hergestellt haben. Siehe Verbindung zu Google-Cloudumgebungen.

Vorbereiten einer Master-VM-Instanz und eines nichtflüchtigen Speichers

> **Tipp:**
>
> Nichtflüchtiger Speicher (Persistent Disk) ist der Google Cloud-Begriff für den virtuellen Datenträger.

Zur Vorbereitung Ihrer Master-VM-Instanz erstellen und konfigurieren Sie zunächst eine VM-Instanz mit Eigenschaften, die der gewünschten Konfiguration für die geklonten VDA-Instanzen im geplanten Maschinenkatalog entsprechen. Die Konfiguration gilt nicht nur für Größe und Typ der Instanz. Sie umfasst auch Instanzattribute wie Metadaten, Tags, GPU-Zuweisungen, Netzwerktags und Dienstkontoeigenschaften.

MCS verwendet dann Ihre Master-VM-Instanz, um die Google Cloud-*Instanzvorlage* zu erstellen. Auf der Basis der Instanzvorlage werden dann die geklonten VDA-Instanzen erstellt, die den Maschinenkatalog umfassen. Geklonte Instanzen erben die Eigenschaften der Master-VM-Instanz (mit Ausnahme der Eigenschaften für VPC, Subnetz und nichtflüchtigen Speicher), aus der die Instanzvorlage erstellt wurde.

Nachdem Sie die Eigenschaften der Master-VM-Instanz konfiguriert haben, starten Sie die Instanz und bereiten den nichtflüchtigen Speicher für die Instanz vor.

Es wird empfohlen, manuell einen Snapshot des Speichers zu erstellen. Dies ermöglicht eine aussagekräftige Benennung zum Nachverfolgen von Versionen, bietet mehr Optionen zum Verwalten früherer Versionen des Masterimages und spart Zeit beim Erstellen des Maschinenkatalogs. Wenn Sie keinen eigenen Snapshot erstellen, erstellt MCS einen temporären Snapshot, der bei Abschluss der Bereitstellung gelöscht wird.

Aktivieren der Zonenauswahl

Citrix DaaS unterstützt die Zonenauswahl. Bei der Zonenauswahl geben Sie die Zonen an, in denen VMs erstellt werden sollen. Mithilfe der Zonenauswahl können Administratoren die Einzelmandantenknoten in Zonen ihrer Wahl platzieren. Um die Einzelmandantenfähigkeit zu konfigurieren, müssen Sie folgende Schritte in Google Cloud ausführen:

- Reservieren eines Google Cloud-Knotens für einzelne Mandanten
- Erstellen des VDA-Masterimages

Reservieren eines Google Cloud-Knotens für einzelne Mandanten

Informationen zum Reservieren eines Einzelmandantenknotens finden Sie in der Dokumentation zu Google Cloud.

> **Wichtig:**
>
> Eine Knotenvorlage wird zur Bezeichnung der Leistungsmerkmale des Systems verwendet, das in der Knotengruppe reserviert ist. Zu diesen Merkmalen gehören die Anzahl der virtuellen GPUs, der dem Knoten zugewiesene Arbeitsspeicher und der für die auf dem Knoten erstellten Maschinen verwendete Maschinentyp. Weitere Informationen finden Sie in der Dokumentation zu Google Cloud.

Erstellen des VDA-Masterimages

Um Maschinen auf dem Knoten für einzelne Mandanten erfolgreich bereitzustellen, müssen Sie beim Erstellen eines Master-VM-Images zusätzliche Schritte ausführen. Maschineninstanzen in Google Cloud besitzen die Eigenschaft *node affinity labels*. Bei Instanzen, die als Masterimage für auf Knoten für einzelne Mandanten bereitgestellte Kataloge verwendet werden, muss das *Knotenaffinitätslabel* mit dem Namen der **Zielknotengruppe** übereinstimmen. Um dies zu erreichen, beachten Sie Folgendes:

- Legen Sie für neue Instanzen das Knotenaffinitätslabel bei deren Erstellung in der Google Cloud-Konsole fest. Weitere Informationen finden Sie unter Festlegen des Knotenaffinitätslabels beim Erstellen einer Instanz.
- Legen Sie für bestehende Instanzen das Knotenaffinitätslabel über die **gcloud**-Befehlszeile fest. Weitere Informationen finden Sie unter Festlegen des Knotenaffinitätslabels für eine bestehende Instanz.

> **Hinweis:**
>
> Wenn Sie die Einzelmandantenfähigkeit mit einer freigegebenen VPC verwenden möchten, lesen Sie den Abschnitt Freigegebene virtuelle private Cloud.

Festlegen des Knotenaffinitätslabels beim Erstellen einer Instanz Zum Festlegen des Knotenaffinitätslabels führen Sie folgende Schritte aus:

1. Navigieren Sie in der Google Cloud-Konsole zu **Compute Engine > VM instances**.
2. Wählen Sie auf der Seite **VM instances** die Option **Create instance**.
3. Geben Sie auf der Seite **Instance creation** die erforderlichen Informationen an und wählen Sie **management, security, disks, networking, sole tenancy**, um das Einstellungsfenster zu öffnen.
4. Wählen Sie **Browse** auf der Registerkarte **Sole tenancy**, um die verfügbaren Knotengruppen im aktuellen Projekt anzuzeigen. Die Seite **Sole-tenant node** wird mit einer Liste der verfügbaren Knotengruppen angezeigt.

5. Wählen Sie auf der Seite **Sole-tenant node** die gewünschte Knotengruppe aus der Liste aus und wählen Sie **Select**, um zur Registerkarte **Sole tenancy** zurückzukehren. Das Feld "node affinity labels"wird mit den ausgewählten Informationen ausgefüllt. Mit dieser Einstellung wird sichergestellt, dass aus der Instanz erstellte Maschinenkataloge für die ausgewählte Knotengruppe bereitgestellt werden.
6. Wählen Sie **Create**, um die Instanz zu erstellen.

Festlegen des Knotenaffinitätslabels für eine bestehende Instanz Zum Festlegen des Knotenaffinitätslabels führen Sie folgende Schritte aus:

1. Legen Sie im Google Cloud Shell-Terminalfenster ein Knotenaffinitätslabel mit dem Befehl *gcloud compute instances* fest. Der **gcloud**-Befehl muss die folgenden Informationen enthalten:

   - **Name der VM.** Verwenden Sie beispielsweise eine bestehende VM namens `s*2019-vda-base`.*
   - **Name der Knotengruppe.** Verwenden Sie den zuvor erstellten Knotengruppennamen. Beispiel: `mh-sole-tenant-node-group-1`.
   - **Die Zone, in der sich die Instanz befindet**. Die VM kann sich beispielsweise in `*us-east-1b* zone` befinden.

   Geben Sie beispielsweise den folgenden Befehl im Terminalfenster ein:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Weitere Informationen zum Befehl *gcloud compute instances* finden Sie in der Google Developer Tools-Dokumentation unter https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.
2. Navigieren Sie zu der Seite **VM instance details** der Instanz und prüfen Sie, ob das Feld **Node Affinities** das Label enthält.

Maschinenkatalog erstellen

> **Hinweis:**
>
> Erstellen Sie Ihre Ressourcen, bevor Sie einen Maschinenkatalog erstellen. Verwenden Sie bei der Konfiguration von Maschinenkatalogen die von Google Cloud festgelegten Namenskonventionen. Weitere Informationen finden Sie unter Richtlinien zur Bucket- und Objektbenennung.

Sie können einen Maschinenkatalog auf zweierlei Art erstellen:

- Benutzeroberfläche für die vollständige Konfiguration

- PowerShell. Weitere Informationen finden Sie unter Citrix DaaS mit Remote PowerShell SDKs verwalten. Informationen zur Implementierung bestimmter Funktionen mit PowerShell finden Sie unter PowerShell verwenden

Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration erstellen

Folgen Sie den Anweisungen unter Erstellen von Maschinenkatalogen. Die folgende Beschreibung gilt nur für Google Cloud-Kataloge.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie in der Aktionsleiste **Maschinenkatalog erstellen**.
3. Wählen Sie auf der Seite **Maschinentyp** die Option **Multisitzungs-OS** und wählen Sie **Weiter**. Citrix DaaS unterstützt auch Einzelsitzungs-OS.
4. Wählen Sie auf der Seite **Maschinenverwaltung** die Optionen **Maschinen mit Energieverwaltung** und **Citrix Maschinenerstellungsdienste** und wählen Sie **Weiter**. Bei mehreren vorhandenen Ressourcen wählen Sie eine Ressource im Menü aus.
5. Führen Sie auf der Seite **Image** diese Schritte nach Bedarf aus und klicken Sie dann auf **Weiter**.

   a) Wählen Sie einen Snapshot oder eine VM als Masterimage aus. Wenn Sie die Einzelmandantenfunktion verwenden möchten, wählen Sie ein Image, dessen Knotengruppeneigenschaft korrekt konfiguriert ist. Siehe Aktivieren der Zonenauswahl.

   b) Um eine vorhandene VM als Maschinenprofil zu verwenden, wählen Sie **Maschinenprofil verwenden** und anschließend die VM aus.

   > **Hinweis:**
   >
   > Derzeit übernehmen VMs in diesem Katalog die Einstellungen "ID des Datenträgerverschlüsselungssatzes", "Maschinengröße", "Speichertyp"und "Zone"vom Maschinenprofil.

   c) Wählen Sie die Mindestfunktionsebene für den Katalog.

6. Wählen Sie auf der Seite **Speicher** den Speichertyp für das Betriebssystem für den Maschinenkatalog aus. Für die folgenden Speicheroptionen gelten jeweils eigene Preis- und Leistungsmerkmale. Ein Identitätsdatenträger wird immer mit dem persistenten Standarddatenträger der Zone erstellt.

   - Persistenter Standarddatenträger
   - Ausbalancierter persistenter Datenträger
   - Persistenter SSD-Datenträger

Informationen zu den Optionen für Google Cloud Speicher finden Sie unter Speicheroptionen.

7. Geben Sie auf der Seite **Virtuelle Maschinen** an, wie viele VMs Sie erstellen möchten, zeigen Sie die Spezifikation der VMs an, wählen Sie den Google Cloud-Maschinentyp und wählen Sie **Weiter**. Wenn Sie für Maschinenkataloge Knotengruppen für einzelne Mandanten verwenden, wählen Sie **ausschließlich** die Zonen, in denen reservierte Knoten für einzelne Mandanten verfügbar sind. Siehe Aktivieren der Zonenauswahl.
8. Auf der Seite **Datenträgereinstellungen** können Sie die folgenden Einstellungen vornehmen:
   - Wählen Sie aus, ob der Zurückschreibcache aktiviert werden soll. Nach dem Aktivieren des Zurückschreibcache können Sie Folgendes tun:
     - Konfigurieren Sie die Größe des Datenträgers und des RAM, die zum Zwischenspeichern temporärer Daten verwendet werden. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.
     - Wählen des Speichertyps für den Datenträger für den Zurückschreibcache. Die folgenden Speichertypen stehen für den Zurückschreibcache-Datenträger zur Verfügung:
       * Persistenter Standarddatenträger
       * Ausbalancierter persistenter Datenträger
       * Persistenter SSD-Datenträger

       Informationen zu den Optionen für Google Cloud Speicher finden Sie unter Speicheroptionen.
     - Wählen Sie einen Datenträgertyp für den Zurückschreibcache aus.
       * **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**. Wenn diese Option ausgewählt ist, wird der Zurückschreibcache-Datenträger für die bereitgestellten VMs nicht beibehalten. Der Datenträger wird während Energiezyklen gelöscht und alle Daten, die auf den Datenträger umgeleitet wurden, gehen verloren.
       * **Persistenter Datenträger für Zurückschreibcache.** Wenn diese Option ausgewählt ist, wird der Zurückschreibcache-Datenträger für die bereitgestellten VMs beibehalten. Die Aktivierung dieser Option erhöht die Speicherkosten.
   - Bei aktivierter MCS-Speicheroptimierung (MCS-E/A) können Sie wählen, ob die Systemdatenträger für VDAs während Energiezyklen beibehalten werden sollen. Weitere Informationen finden Sie unter Aktivieren der neuen MCS-Speicheroptimierung.
   - Wählen Sie aus, ob Sie Ihren eigenen Schlüssel zum Schutz von Datenträgerinhalten verwenden möchten. Um das Feature nutzen zu können, müssen Sie zuerst eigene Verschlüsselungsschlüssel (CMEKs) erstellen. Weitere Informationen finden Sie unter Verwenden vom Kunden verwalteter Verschlüsselungsschlüssel (CMEK).

> **Hinweis:**
>
> Es ist nur über die Schnittstelle **Verwalten > Vollständige Konfiguration** verfügbar.

Nachdem Sie die Schlüssel erstellt haben, können Sie einen davon aus der Liste auswählen. Sie können den Schlüssel nicht mehr ändern, wenn Sie den Katalog erstellt haben. Google Cloud unterstützt keinen Wechsel von Schlüsseln für bestehende persistente Datenträger bzw. Images. Ein bereitgestellter Katalog ist daher an eine bestimmte Version des Schlüssels gebunden. Wird der Schlüssel deaktiviert oder zerstört, werden die damit verschlüsselten Instanzen und Datenträger so lange unbrauchbar, bis der Schlüssel wieder aktiviert bzw. wiederhergestellt wird.

9. Wählen Sie auf der Seite **Maschinenidentitäten** ein Active Directory-Konto aus und wählen Sie **Weiter**.
    - Wenn Sie **Neue Active Directory-Konten erstellen** auswählen, wählen Sie eine Domäne und geben Sie dann die Zeichenfolge ein, die das Benennungsschema für die bereitgestellten, in Active Directory erstellten VM-Computerkonten darstellt. Das Kontenbenennungsschema schreibt 1–64 Zeichen und ausschließlich ASCII-Zeichen vor, der Name darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten:
    - Bei Auswahl von **Vorhandene Active Directory-Konten verwenden** wählen Sie **Durchsuchen**, um die vorhandenen Active Directory-Computerkonten für die ausgewählten Maschinen aufzurufen.
10. Wählen Sie auf der Seite **Domänenanmeldeinformationen** die Option **Anmeldeinformationen eingeben**. Geben Sie den Benutzernamen und das Kennwort ein, wählen Sie **Speichern** und dann **Weiter**.
    - Die eingegebene Anmeldeinformationen müssen über Berechtigungen zum Ausführen von Active Directory-Kontovorgängen verfügen.
11. Wählen Sie auf der Seite **Geltungsbereiche** Geltungsbereiche für den Maschinenkatalog aus und wählen Sie **Weiter**.
    - Wählen Sie optionale Geltungsbereiche aus oder wählen Sie **Benutzerdefinierter Geltungsbereich**, um Geltungsbereiche nach Bedarf anzupassen.
12. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung**, geben Sie einen Namen für den Katalog ein und wählen Sie **Fertigstellen**.

> **Hinweis:**
>
> Der Katalogname muss aus 1–39 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen, und folgende Zeichen sind nicht erlaubt: `\ / ; : # . * ? = < >`


```
| [ ] { } "' ( )' ).
```

Die Erstellung des Maschinenkatalogs kann lange dauern. Wenn sie abgeschlossen ist, wird der Katalog aufgelistet. Sie können in der Google Cloud-Konsole überprüfen, ob die Maschine auf den Zielknotengruppen erstellt wurden.

Importieren manuell erstellter Google Cloud-Maschinen

Mit dem Feature ist Folgendes möglich:

- Manuell erstellte Google Cloud-Maschinen mit Multisitzungs-OS in einen Citrix DaaS-Maschinenkatalog importieren.
- Manuell erstellte Google Cloud-Maschinen mit Multisitzungs-OS aus einem Citrix DaaS-Maschinenkatalog entfernen.
- Energieverwaltung von Multisitzungs-OS-Maschinen in Google Cloud über vorhandene Energieverwaltungsfunktionen von Citrix DaaS verwenden. Richten Sie beispielsweise einen Neustartplan für diese Maschinen ein.

Hierfür ist es nicht erforderlich, vorhandene Bereitstellungsworkflows für Citrix DaaS zu ändern oder vorhandene Features zu entfernen.

Es wird empfohlen, Maschinen mit MCS in der Benutzeroberfläche “Vollständige Konfiguration”von Citrix DaaS bereitzustellen, anstatt manuell erstellte Google Cloud-Maschinen zu importieren.

Freigegebene virtuelle private Cloud

Freigegebene VPCs umfassen ein Hostprojekt, aus dem die freigegebenen Subnetze zur Verfügung gestellt werden, sowie mindestens ein Dienstprojekt, das die Ressource verwendet. Freigegebene VPCs sind gute Optionen für größere Installationen, da sie eine zentrale Steuerung, Nutzung und Verwaltung gemeinsam genutzter Google-Cloud-Ressourcen bieten. Weitere Informationen finden Sie auf der Google-Dokumentationssite.

Mit diesem Feature unterstützt Maschinenerstellungsdienste (MCS) das Provisioning und die Verwaltung von Maschinenkatalogen, die in freigegebenen VPCs bereitgestellt werden. Diese Unterstützung entspricht funktional der derzeitigen für lokale VPCs, weist aber in zwei Bereichen Unterschiede auf:

- Sie müssen dem Dienstkonto, das zum Erstellen der Hostverbindung verwendet wird, zusätzliche Berechtigungen erteilen. Dadurch kann MCS auf freigegebene VPC-Ressourcen zugreifen und diese nutzen. Weitere Informationen finden Sie unter Neue Berechtigungen erforderlich.

- Sie müssen zwei Firewallregeln (eine für den eingehenden und eine für den ausgehenden Datenverkehr) erstellen. Die Firewallregeln werden beim Imagemastering verwendet. Weitere Informationen finden Sie unter Firewallregeln.

Informationen zur Konfiguration einer gemeinsam genutzten VPC finden Sie unter Gemeinsam genutzte VPC konfigurieren.

Neue Berechtigungen erforderlich

Beim Erstellen der Hostverbindung ist ein Google Clouddienstkonto mit bestimmten Berechtigungen erforderlich. Diese zusätzlichen Berechtigungen müssen allen Dienstkonten erteilt werden, die zum Erstellen von Hostverbindungen für die freigegebene VPC verwendet werden.

> **Tipp:**
>
> Die zusätzlichen Berechtigungen sind für Citrix DaaS nicht neu. Sie werden verwendet, um die Verwendung lokaler VPCs zu erleichtern. Bei freigegebenen VPCs ermöglichen die zusätzlichen Berechtigungen den Zugriff auf andere freigegebene VPC-Ressourcen.

Dem Dienstkonto, das der Hostverbindung zugeordnet ist, müssen bis zu vier zusätzliche Berechtigungen erteilt werden, um eine freigegebene VPC zu unterstützen:

- **compute.firewalls.list:** Diese Berechtigung ist obligatorisch. Mit ihr kann MCS die Liste der Firewallregeln auf der freigegebenen VPC abrufen.
- **compute.networks.list:** Diese Berechtigung ist obligatorisch. Damit kann MCS die freigegebenen VPC-Netzwerke identifizieren, die dem Dienstkonto zur Verfügung stehen.
- **compute.subnetworks.list:** Diese Berechtigung ist je nach Verwendung der VPCs optional. Damit kann MCS die Subnetze der sichtbaren, freigegebenen VPCs identifizieren. Diese Berechtigung ist für die Verwendung lokaler VPCs erforderlich, muss aber auch im Hostprojekt für freigegebene VPCs zugewiesen werden.
- **compute.subnetworks.use:** Diese Berechtigung ist je nach Verwendung der VPCs optional. Sie ist zur Verwendung von Subnetzressourcen in den bereitgestellten Maschinenkatalogen erforderlich. Diese Berechtigung ist für die Verwendung lokaler VPCs erforderlich, muss aber auch im Hostprojekt für freigegebene VPCs zugewiesen werden.

Berücksichtigen Sie bei der Verwendung dieser Berechtigungen, dass es, basierend auf dem Berechtigungstyp, verschiedene Ansätze zum Erstellen des Maschinenkatalogs gibt:

- Berechtigung auf Projektebene:
  - Ermöglicht Zugriff auf alle freigegebenen VPCs im Hostprojekt.
  - Erfordert, dass dem Dienstkonto die Berechtigungen `compute.subnetworks.list` und `compute.subnetworks.use` zugewiesen sind.

- Berechtigung auf Subnetzebene:
  - Ermöglicht den Zugriff auf einzelne Subnetze in der freigegebenen VPC.
  - Die Berechtigungen `compute.subnetworks.list` und `compute.subnetworks.use` gehören zur Zuweisung auf Subnetzebene und müssen daher dem Dienstkonto nicht direkt zugewiesen werden.

Wählen Sie das Konzept aus, der Ihren Anforderungen und Sicherheitsstandards entspricht.

> **Tipp:**
>
> Weitere Informationen zu den Unterschieden zwischen Berechtigungen auf Projektebene und Subnetzebene finden Sie unter Dienstprojektadministratoren.

Firewallregeln

Bei der Vorbereitung eines Maschinenkatalogs wird ein Maschinenabbild vorbereitet, das als Masterimage-Systemdatenträger für den Katalog dient. Bei diesem Vorgang wird der Datenträger vorübergehend an eine virtuelle Maschine angefügt. Die VM muss in einer isolierten Umgebung ausgeführt werden, die jeglichen eingehenden und ausgehenden Netzwerkdatenverkehr verhindert. Dies wird durch zwei Alles-abweisen-Firewallregeln verwirklicht: eine für eingehenden und eine für ausgehenden Datenverkehr. Bei Verwendung Google Cloud-lokaler VCPs erstellt MCS diese Firewall im lokalen Netzwerk und wendet sie für das Mastering auf die Maschine an. Nach Abschluss des Masterings werden die Firewallregeln aus dem Image entfernt.

Es wird empfohlen, die Anzahl der neuen Berechtigungen, die für die Verwendung freigegebener VPCs erforderlich sind, auf ein Minimum zu beschränken. Freigegebene VPCs sind wichtige Unternehmensressourcen, für die in der Regel strenge Sicherheitsprotokolle gelten. Erstellen Sie daher im Hostprojekt zwei Firewallregeln für die freigegebenen VPC-Ressourcen: eine für eingehenden und eine für ausgehenden Datenverkehr. Weisen Sie diesen die höchste Priorität zu. Wenden Sie auf beide Regeln über den folgenden Wert ein neues Ziel-Tag an:

```
citrix-provisioning-quarantine-firewall
```

Wenn MCS einen Maschinenkatalog erstellt oder aktualisiert, sucht es nach Firewallregeln mit diesem Ziel-Tag. Es prüft die Regeln auf Richtigkeit und wendet sie auf die Maschine an, die zur Vorbereitung des Masterimages für den Katalog verwendet wird. Werden die Firewallregeln nicht gefunden oder die gefundenen Regeln haben die falsche Priorität, wird folgende Meldung (oder eine mit ähnlichem Wortlaut) angezeigt:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag ‘citrix-provisioning-
```



```
quarantine-firewall'and proper priority." "Refer to Citrix Documentation
 for details."
```

Freigegebene VPC konfigurieren

Führen Sie vor dem Hinzufügen der freigegebenen VPC als Hostverbindung in der Oberfläche "Vollständige Konfiguration"von Citrix DaaS die folgenden Schritte aus, um die Dienstkonten aus dem betreffenden Projekt hinzuzufügen:

1. IAM-Rolle erstellen.
2. Ein Dienstkonto zur IAM-Rolle des Hostprojekts hinzufügen
3. Das Cloud Build-Dienstkonto zur freigegebenen VPC hinzufügen
4. Firewallregeln erstellen.

IAM-Rolle erstellen Ermitteln Sie die Zugriffsebene der Rolle:

- *Zugriff auf Projektebene* oder
- Ein eingeschränkteres Modell, das *Zugriff auf Subnetzebene* verwendet.

Zugriff auf Projektebene für die IAM-Rolle. Weisen Sie einer IAM-Rolle auf Projektebene die folgenden Berechtigungen zu:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Führen Sie zum Erstellen einer IAM-Rolle auf Projektebene folgende Schritte aus:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > Roles**.
2. Wählen Sie **CREATE ROLE** auf der Seite **Roles**.
3. Geben Sie auf der Seite **Create Role** einen Rollennamen ein. Wählen Sie **ADD PERMISSIONS**.
    a) Fügen Sie auf der Seite **Add permissions** der Rolle Berechtigungen hinzu. Um eine Berechtigung hinzuzufügen, geben Sie deren Namen in das Feld **Filter table** ein. Wählen Sie die Berechtigung aus und wählen Sie **ADD**.
    b) Wählen Sie **CREATE**.

IAM-Rolle auf Subnetzebene. Bei dieser Rolle werden die Berechtigungen `compute.subnetworks.list` und `compute.subnetworks.use` nach Auswahl von **CREATE ROLE** ausgelassen. Für diese IAM-Zugriffsebene müssen die Berechtigungen `compute.firewalls.list` und `compute.networks.list` auf die neue Rolle angewendet werden.

Führen Sie zum Erstellen einer IAM-Rolle auf Subnetzebene folgende Schritte aus:

1. Navigieren Sie in der Google Cloud-Konsole zu **VPC network** > **Shared VPC**. Auf der Seite **Shared VPC** werden die Subnetze der freigegebenen VPC-Netzwerke des Hostprojekts angezeigt.
2. Wählen Sie auf der Seite **Shared VPC** das Subnetz aus, auf das Sie zugreifen möchten.
3. Wählen Sie oben rechts **ADD MEMBER**, um ein Dienstkonto hinzuzufügen.
4. Führen Sie auf der Seite **Add members** die folgenden Schritte aus:

    a) Geben Sie im Feld **New members** den Namen des Dienstkontos ein und wählen Sie dann im Menü das Dienstkonto aus.
    b) Wählen Sie das Feld **Select a Roll** und dann **Compute Network User**.
    c) Wählen Sie **SAVE**.

5. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin** > **Roles**.
6. Wählen Sie **CREATE ROLE** auf der Seite **Roles**.
7. Geben Sie auf der Seite **Create Role** einen Rollennamen ein. Wählen Sie **ADD PERMISSIONS**.

    a) Fügen Sie auf der Seite **Add permissions** der Rolle Berechtigungen hinzu. Um eine Berechtigung hinzuzufügen, geben Sie deren Namen in das Feld **Filter table** ein. Wählen Sie die Berechtigung aus und wählen Sie **ADD**.
    b) Wählen Sie **CREATE**.

Hinzufügen eines Dienstkontos zur IAM-Rolle des Hostprojekts Führen Sie nach dem Erstellen einer IAM-Rolle die folgenden Schritte aus, um ein Dienstkonto für das Hostprojekt hinzuzufügen:

1. Gehen Sie in der Google Cloud-Konsole zum Hostprojekt und dann zu **IAM & Admin > IAM**.
2. Wählen Sie auf der Seite **IAM** die Option **ADD**, um ein Dienstkonto hinzuzufügen.
3. Führen Sie auf der Seite **Add members** folgende Schritte aus:

    a) Geben Sie im Feld **New members** den Namen des Dienstkontos ein und wählen Sie dann im Menü das Dienstkonto aus.
    b) Wählen Sie ein Rollenfeld, geben Sie die erstellte IAM-Rolle ein und wählen Sie dann im Menü die Rolle.
    c) Wählen Sie **SAVE**.

Das Dienstkonto ist damit für das Hostprojekt konfiguriert.

Cloud Build-Dienstkonto zur freigegebenen VPC hinzufügen Jedes Google Cloud-Abonnement hat ein Dienstkonto, das denselben Namen trägt wie die Projekt-ID, gefolgt von `cloudbuild.gserviceaccount`. Beispiel: `705794712345@cloudbuild.gserviceaccount`.

Sie können die Projekt-ID-Nummer für Ihr Projekt ermitteln, indem Sie in der Google Cloud-Konsole zu **Cloud Overview > Dashboard** navigieren. Die Projekt-ID und die Projektnummer werden auf der Projektinfokarte des Projekt-Dashboards angezeigt:

Zum Hinzufügen des Cloud Build-Dienstkontos zur freigegebenen VPC führen Sie folgende Schritte aus:

1. Gehen Sie in der Google Cloud-Konsole zum Hostprojekt und dann zu **IAM & Admin** > **IAM**.
2. Wählen Sie **ADD** auf der Seite **Permissions**, um ein Konto hinzuzufügen.
3. Führen Sie auf der Seite **Add members** die folgenden Schritte aus:

    a) Geben Sie im Feld **New members** den Namen des Cloud Build-Kontos ein und wählen Sie dann im Menü das Dienstkonto aus.
    b) Wählen Sie das Feld **Select a role**, geben Sie `Computer Network User` ein und wählen Sie dann im Menü die Rolle.
    c) Wählen Sie **SAVE**.

Erstellen von Firewallregeln Beim Mastering kopiert MCS das ausgewählte Maschinenabbild und bereitet damit den Masterimage-Systemdatenträger für den Katalog vor. Beim Masterings fügt MCS den Datenträger an eine temporäre virtuelle Maschine an und führt dann Vorbereitungsskripts aus. Die VM muss in einer isolierten Umgebung ausgeführt werden, die jeglichen eingehenden und ausgehenden Netzwerkdatenverkehr verhindert.

Um eine isolierte Umgebung zu erstellen, erfordert MCS zwei *Alles-abweisen*-Firewallregeln (eine Eingangsregel und eine Ausgangregel). Erstellen Sie daher zwei Firewallregeln (eingehend und ausgehend) im *Hostprojekt*:

1. Gehen Sie in der Google Cloud-Konsole zum Hostprojekt und dann zu **VPC network > Firewall**.
2. Wählen Sie auf der Seite **Firewall** die Option **CREATE FIREWALL RULE**.
3. Führen Sie auf der Seite **Create a firewall rule** die folgenden Schritte aus:

    - **Name**. Geben Sie einen Namen für die Regel ein.
    - **Network**. Wählen Sie das freigegebene VPC-Netzwerk aus, für das die Firewallregel für eingehenden Datenverkehr gilt.
    - **Priority**. Je kleiner der Wert ist, desto höher ist die Priorität der Regel. Citrix empfiehlt einen kleinen Wert (z. B. 10).
    - **Direction of traffic**. Wählen Sie **Ingress**.
    - **Action on match**. Wählen Sie **Deny**.
    - **Targets**. Verwenden Sie die Standardeinstellung **Specified target tags**.
    - **Target tags**. Geben Sie `citrix-provisioning-quarantine-firewall` ein.
    - **Source filter**. Verwenden Sie die Standardeinstellung **IP ranges**.
    - **Source IP ranges**. Geben Sie einen Bereich ein, der den gesamten Datenverkehr abdeckt. Geben Sie `0.0.0.0/0` ein.
    - **Protocols and ports**. Wählen Sie **Deny all**.

4. Wählen Sie **CREATE**, um die Regel zu erstellen.

5. Wiederholen Sie die Schritte, um eine weitere Regel zu erstellen. Wählen Sie für **Direction of traffic** die Option **Egress**.

Vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) verwenden

Sie können vom Kunden verwaltete Verschlüsselungsschlüssel (Customer Managed Encryption Keys, CMEK) für MCS-Kataloge verwenden. Wenn Sie das Feature verwenden, weisen Sie dem Compute Engine Service-Agent die Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter`-Rolle zu. Das Citrix DaaS-Konto muss über die richtigen Berechtigungen in dem Projekt verfügen, in dem der Schlüssel gespeichert ist. Weitere Informationen finden Sie unter Berechtigungen zum Citrix DaaS-Konto zuweisen. Weitere Informationen finden Sie unter Ressourcen mit Cloud KMS-Schlüsseln schützen.

Ihr Compute Engine Service Agent folgt folgendem Format: `service-<Project _Number>@compute-system.iam.gserviceaccount.com`. Dieses unterscheidet sich von dem standardmäßigen Compute Engine Service-Konto.

> **Hinweis:**
>
> Dieses Compute Engine Service-Konto wird möglicherweise nicht in den **IAM-Berechtigungen** der Google-Konsole angezeigt. Verwenden Sie in solchen Fällen den Befehl `gcloud`, wie unter Ressourcen mit Cloud KMS-Schlüsseln schützen beschrieben.

Zuweisen von Berechtigungen zum Citrix DaaS-Konto

Google Cloud KMS-Berechtigungen können auf verschiedene Art und Weise konfiguriert werden. Sie können entweder die KMS-Berechtigungen auf *Projektebene* oder auf *Ressourcenebene* bereitstellen. Weitere Informationen finden Sie unter Berechtigungen und Rollen.

KMS-Berechtigungen auf Projektebene Sie können dem Citrix DaaS-Konto Berechtigungen auf Projektebene zum Durchsuchen von Cloud KMS-Ressourcen zuweisen. Erstellen Sie dazu eine benutzerdefinierte Rolle und fügen Sie die folgenden Berechtigungen hinzu:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Weisen Sie die benutzerdefinierte Rolle Ihrem Citrix DaaS-Konto zu. Dadurch können Sie regionale Schlüssel im relevanten Projekt im Bestand durchsuchen.

KMS-Berechtigungen auf Ressourcenebene Gehen Sie für die zweite Option –Berechtigungen auf Ressourcenebene –in der Google Cloud-Konsole zu dem `cryptoKey`, den Sie für die MCS-Bereitstellung verwenden. Fügen Sie das Citrix DaaS-Konto einem Schlüsselbund oder Schlüssel hinzu, den Sie für die Katalogbereitstellung verwenden.

> **Tipp:**
>
> Mit dieser Option können Sie keine regionalen Schlüssel für Ihr Projekt im Bestand durchsuchen, da das Citrix DaaS-Konto keine Listenberechtigungen auf Projektebene für die Cloud KMS-Ressourcen hat. Sie können jedoch Kataloge mit CMEK bereitstellen, indem Sie in den benutzerdefinierten Eigenschaften für `ProvScheme` das korrekte `cryptoKeyId` angeben. Weitere Informationen finden Sie unter Katalog mit CMEK und benutzerdefinierten Eigenschaften erstellen.

Wechsel vom Kunden verwalteter Schlüssel

Google Cloud unterstützt keinen Wechsel von Schlüsseln für bestehende persistente Datenträger bzw. Images. Sobald eine Maschine bereitgestellt ist, ist sie an die zum Zeitpunkt ihrer Erstellung verwendete Schlüsselversion gebunden. Es kann jedoch eine neue Schlüsselversion erstellt werden, die dann für neu bereitgestellte Maschinen bzw. Ressourcen verwendet, die erstellt werden, wenn ein Katalog mit einem neuen Masterimage aktualisiert wird.

Wichtige Überlegungen zu Schlüsselbunden Schlüsselbunde können nicht umbenannt oder gelöscht werden. Außerdem können bei ihrer Konfiguration unerwartete Gebühren anfallen. Wenn Sie einen Schlüsselbund löschen, zeigt Google Cloud eine Fehlermeldung an:

```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> **Tipp:**

> Weitere Informationen finden Sie unter Bearbeiten oder Löschen eines Schlüsselbunds von der Konsole.

Kompatibilität mit einheitlichem Zugriff auf Bucket-Ebene

Citrix DaaS ist kompatibel mit der Richtlinie zum einheitlichen Zugriff auf Bucket-Ebene von Google Cloud. Diese Funktion erweitert die Verwendung der IAM-Richtlinie, die Berechtigungen für ein Dienstkonto erteilt, um die Bearbeitung von Ressourcen (einschließlich Storage-Buckets) zu ermöglichen. Durch einheitlichen Zugriff auf Bucket-Ebene können Sie in Citrix DaaS per Zugriffssteuerungsliste (ACL) den Zugriff auf Storage-Buckets oder darin gespeicherte Objekte zu steuern. Einen Überblick über den einheitlichen Zugriff auf Bucket-Ebene in Google Cloud finden Sie unter Einheitlicher Zugriff auf Bucket-Ebene. Informationen zur Konfiguration finden Sie unter Anfordern des einheitlichen Zugriffs auf Bucket-Ebene.

PowerShell verwenden

In diesem Abschnitt wird beschrieben, wie Sie die folgenden Aufgaben mit PowerShell ausführen:

- Katalog mit persistentem Zurückschreibcachedatenträger erstellen
- Startleistung mit MCSIO verbessern
- Katalog mit CMEK und benutzerdefinierten Eigenschaften erstellen
- Maschinenkatalog mit einem Maschinenprofil erstellen
- Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen
- Katalog mit Shielded VM erstellen
- Windows 11-VMs auf dem Einzelmandantenknoten erstellen

Katalog mit persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Befehl `New-ProvScheme CustomProperties`.

> **Tipp:**
>
> Verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties` nur für cloudbasierte Hostverbindungen. Wenn Sie Maschinen mit persistentem Zurückschreibcachedatenträger für eine On-Premises-Lösung (z. B. XenServer) bereitstellen möchten, wird PowerShell nicht benötigt, da der Datenträger automatisch persistent ist.

Dieser Befehl unterstützt die zusätzliche Eigenschaft `PersistWBC`, welche bestimmt, ob der Zurückschreibcachedatenträger bei von MCS-bereitgestellten Maschinen persistent oder flüchtig ist. Die Eigenschaft `PersistWBC` wird nur verwendet, wenn der Parameter `UseWriteBackCache`

angegeben wird und Parameter `WriteBackCacheDiskSize` so konfiguriert ist, dass ein Datenträger erstellt wird.

> **Hinweis:**
>
> Dieses Verhalten gilt für Azure und GCP, bei dem der standardmäßige MCSIO-Zurückschreibcachedatenträger beim Aus- und Wiedereinschalten gelöscht und neu erstellt wird. Sie können den Datenträger als persistent konfigurieren, um das Löschen und neu Erstellen des MCSIO-Zurückschreibcachedatenträger zu vermeiden.

Beispiele für Eigenschaften im Parameter `CustomProperties` vor Unterstützung von `PersistWBC`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Dieses Beispiel gilt nur für Azure. Die Eigenschaften sind in der GCP-Umgebung anders.

Berücksichtigen Sie bei Verwendung dieser Eigenschaften deren Standardwerte, wenn die Eigenschaften im Parameter `CustomProperties` ausgelassen werden. Die Eigenschaft `PersistWBC` hat zwei mögliche Werte: **true** oder **false**.

Bei der Einstellung von `PersistWBC` auf **true** wird der Zurückschreibcachedatenträger nicht gelöscht, wenn der Citrix DaaS-Administrator die Maschine über die Verwaltungsoberfläche herunterfährt.

Bei der Einstellung von `PersistWBC` auf **false** wird der Zurückschreibcachedatenträger gelöscht, wenn der Citrix DaaS-Administrator die Maschine über die Verwaltungsoberfläche herunterfährt.

> **Hinweis:**
>
> Wird die Eigenschaft `PersistWBC` nicht angegeben, so gilt der Standardwert **false** und der Zurückschreibcachedatenträger wird beim Herunterfahren der Maschine über die Verwaltungsoberfläche gelöscht.

Beispiel der Verwendung des Parameters `CustomProperties` zur Einstellung von `PersistWBC` auf “true”:


```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Wichtig:**
>
> Die Eigenschaft `PersistWBC` kann nur mit dem PowerShell-Cmdlet `New-ProvScheme` festgelegt werden. Eine Änderung der `CustomProperties` eines Provisioningschemas nach der Erstellung hat keine Auswirkungen auf den Maschinenkatalog und die Permanenz des Zurückschreibcachedatenträger beim Herunterfahren von Maschinen.

Beispiel der Einstellung von `New-ProvScheme` zur Verwendung des Zurückschreibcache und Einstellung von `PersistWBC` auf "true":

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```


Startleistung mit MCSIO verbessern

Sie können die Startleistung für in Azure oder GCP verwaltete Datenträger verbessern, wenn MCSIO aktiviert ist. Verwenden Sie die benutzerdefinierte PowerShell-Eigenschaft `PersistOSDisk` im Befehl `New-ProvScheme`, um dieses Feature zu konfigurieren: Optionen für `New-ProvScheme`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
``````<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Um dieses Feature zu aktivieren, legen Sie die benutzerdefinierte Eigenschaft `PersistOSDisk` auf **true** fest. Beispiel:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

#### Katalog mit CMEK und benutzerdefinierten Eigenschaften erstellen

Geben Sie beim Erstellen Ihres Provisioningschemas über PowerShell eine `CryptoKeyId`-Eigenschaft in `ProvScheme CustomProperties` an. Beispiel:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
       yourCryptoKeyId>" />
</CustomProperties>'
<!--NeedCopy-->
```

Die `cryptoKeyId` muss im folgenden Format angegeben werden:

`projectId:location:keyRingName:cryptoKeyName`

Wenn Sie beispielsweise den Schlüssel `my-example-key` im Schlüsselbund `my-example-key-ring` in der Region `us-east1` und Projekt-ID `my-example-project-1` verwenden möchten, sehen die benutzerdefinierten `ProvScheme`-Einstellungen in etwa so aus:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
<!--NeedCopy-->
```

Alle zu dem Provisioningschema gehörenden, per MCS bereitgestellten Datenträger und Images verwenden diesen kundenverwalteten Verschlüsselungsschlüssel.

> **Tipp:**
>
> Wenn Sie globale Schlüssel verwenden, muss der Kundeneigenschaftenort anstelle des Namens der **Region** (im obigen Beispiel **us-east1**) `global` sein. Beispiel: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

### Maschinenkatalog mit einem Maschinenprofil erstellen

Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS erstellen, können Sie ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer virtuellen Maschine erfasst und auf neu bereitgestellte VMs im Katalog anwendet. Wenn der Parameter `MachineProfile` nicht verwendet wird, werden die Hardwareeigenschaften von der Masterimage-VM oder dem Snapshot erfasst.

Einige Eigenschaften, die Sie explizit definieren (beispielsweise `StorageType`, `CatalogZones` und `CryptoKeyId`) werden im Maschinenprofil ignoriert.

- Verwenden Sie den Befehl `New-ProvScheme`, um einen Katalog mit einem Maschinenprofil zu erstellen. Beispiel: `New-ProvScheme –MachineProfile "path to VM"`. Wenn Sie den Parameter `MachineProfile` nicht angeben, werden Hardwareeigenschaften von der Masterimage-VM erfasst.
- Verwenden Sie den Befehl `Set-ProvScheme`, um einen Katalog mit einem neuen Maschinenprofil zu aktualisieren. Beispiel: `Set-ProvScheme –MachineProfile "path to` **`new`** `VM"`. Dieser Befehl ändert das Maschinenprofil der vorhandenen VMs im Katalog nicht. Nur neu erstellte VMs, die dem Katalog hinzugefügt werden, haben das neue Maschinenprofil.
- Sie können auch das Masterimage aktualisieren, allerdings werden hierbei die Hardwareeigenschaften nicht aktualisiert. Wenn Sie die Hardwareeigenschaften aktualisieren möchten, müssen Sie das Maschinenprofil mit dem Befehl `Set-ProvScheme` aktualisieren. Die Änderungen gelten nur für die neuen Maschinen im Katalog. Um die Hardwareeigenschaften einer vorhandenen Maschine zu aktualisieren, können Sie den Befehl `Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1` verwenden.

  > **Hinweis:**
  >
  > - `StartsNow` gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
  > - `DurationInMinutes` mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

## Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen

Sie können eine GCP-Instanzvorlage als Eingabe für das Maschinenprofil auswählen. Instanzvorlagen sind schlanke Ressourcen in GCP und daher sehr kostengünstig.

### Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Suchen Sie mit dem folgenden Befehl eine Instanzvorlage in Ihrem GCP-Projekt:

   ```
   cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
   <!--NeedCopy-->
   ```

4. Erstellen Sie mit dem Befehl NewProvScheme einen neuen Maschinenkatalog mit Maschinenprofil als Instanzvorlage:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName>\Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

Weitere Hinweise zum Befehl New-ProvScheme finden Sie unter https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Beenden Sie das Erstellen des Maschinenkatalogs mithilfe von PowerShell-Befehlen.

#### Maschinenkatalog aktualisieren, damit eine Instanzvorlage als Maschinenprofil verfügbar ist

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den folgenden Befehl aus:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

Weitere Informationen zum Befehl Set-ProvScheme finden Sie unter https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Katalog mit Shielded VM erstellen

Sie können einen MCS-Maschinenkatalog mit Shielded VM-Eigenschaften erstellen. Eine abgeschirmte virtuelle Maschine wird durch Sicherheitskontrollen gehärtet, die eine überprüfbare Integrität der Compute Engine-Instanzen über erweiterte Plattformsicherheitsfunktionen wie Sicherer Start, ein virtuelles Trusted Platform Module, UEFI-Firmware und Integritätsüberwachung bieten.

MCS unterstützt die Erstellung des Katalogs mithilfe des Maschinenprofil-Workflows. Wenn Sie den Maschinenprofil-Workflow verwenden, müssen Sie die Shielded VM-Eigenschaften für eine VM-Instanz aktivieren. Sie können diese VM-Instanz dann als Eingabe für das Maschinenprofil verwenden.

#### MCS-Maschinenkatalog mit Shielded VM erstellen

1. Aktivieren Sie die Shielded VM-Optionen für eine VM-Instanz in der Google Cloud-Konsole. Weitere Informationen finden Sie unter Kurzanleitung: Shielded VM-Optionen aktivieren.

2. Erstellen Sie mithilfe der VM-Instanz einen MCS-Maschinenkatalog mit dem Maschinenprofil-Workflow.

   a) Öffnen Sie ein PowerShell-Fenster.

   b) Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.

   c) Erstellen Sie einen Identitätspool, falls noch nicht vorhanden.

   d) Führen Sie den Befehl `New-ProvScheme` aus. Beispiel:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-machine.vm
<!--NeedCopy-->
```

3. Beenden Sie die Erstellung des Maschinenkatalogs.

#### Maschinenkatalog mit einem neuen Maschinenprofil aktualisieren

1. Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.vm
<!--NeedCopy-->
```

Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` aus, um die in `Set-ProvScheme` vorgenommene Änderung auf die vorhandenen VMs anzuwenden.

1. Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` aus. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Starten Sie die VMs neu.

### Windows 11-VMs auf dem Einzelmandantenknoten erstellen

Sie können Windows 11-VMs in GCP erstellen. Wenn Sie jedoch Windows 11 auf dem Masterimage installieren, müssen Sie vTPM während der Erstellung des Masterimages aktivieren. Außerdem müssen Sie vTPM auf der Maschinenprofilquelle (VM oder Instanzvorlage) aktivieren.

Die wichtigsten Schritte zum Erstellen von Windows 11-VMs auf dem Knoten für einzelne Mandanten sind:

1. Richten Sie Google Cloud-Virtualisierungsumgebungen ein. Weitere Informationen finden Sie unter Google Cloud-Umgebungen.
2. Installieren Sie einen VDA. Weitere Informationen finden Sie unter VDAs installieren.
3. Erstellen Sie eine Verbindung zu Google-Cloudumgebungen. Weitere Informationen finden Sie unter Verbindung zu Google-Cloud-Umgebungen.
4. Erstellen Sie ein Windows 11 Bring Your Own License (BYOL) -Masterimage und importieren Sie das Image in Google Cloud. Weitere Informationen finden Sie unter Windows 11 BYOL-Masterimage erstellen.
5. Erstellen Sie die Maschinenprofilquelle: Stellen Sie die VM auf dem Einzelmandantenknoten bereit und aktivieren Sie das vTPM des Quellmaschinenprofils. Weitere Informationen finden Sie unter VM auf einem Einzelmandantenknoten bereitstellen.
6. Erstellen Sie einen MCS-Maschinenkatalog mit der Windows 11-Maschinenprofilquelle, die mit vTPM aktiviert ist. Die Maschinenprofilquelle muss denselben Instanztyp haben, der im Knoten für den Einzelmandanten beschrieben ist. Weitere Informationen finden Sie unter MCS-Maschinenkatalog mit der Windows 11-Maschinenprofilquelle erstellen.

#### Windows 11 BYOL-Masterimage erstellen

Es gibt zwei Optionen, um ein Windows 11 BYOL-Masterimage zu erstellen und das Masterimage in Google Cloud zu importieren:

- Google Cloud Build Tools erstellen
- Masterimage auf einem anderen Hypervisor erstellen

#### Google Cloud Build Tools erstellen

1. Laden Sie die Windows 11-ISO-, GCP SDK-, .NET Framework- und PowerShell-Installationsdateien in den GCP-Speicher-Bucket hoch.
2. Geben Sie den Speicherort der Datei in der `.yaml`-Cloud-Build-Datei als Parameter an.
3. Führen Sie den folgenden Cloud Build über die Befehlszeile aus, um das endgültige Windows 11-Image zu erstellen. GCP bootet und erstellt das Masterimage im ausgewählten Projekt mit dem Daisy-Workflow in GCP. Das Masterimage wird in GCP importiert.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Hinweis:**
>
> Ersetzen Sie den gesamten Großbuchstabentext durch die tatsächlichen Ressourcende-

> tails.

Vollständige Informationen finden Sie unter Benutzerdefinierte Windows BYOL-Images erstellen.

#### Masterimage auf einem anderen Hypervisor erstellen

1. Erstellen Sie das Windows 11-Masterimage mit einem anderen Hypervisor.
2. Exportieren Sie das Masterimage in einem OVF-Format auf der lokalen Maschine.
3. Laden Sie die OVF-Dateien über die lokale gcloud-Befehlszeilenschnittstelle in den GCP-Speicherbucket hoch.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
<!--NeedCopy-->
```

4. Führen Sie den folgenden Cloud Build über die Befehlszeile aus, um das endgültige Windows 11-Image zu erstellen. GCP bootet und erstellt das Masterimage im ausgewählten Projekt mit dem Daisy-Workflow in GCP. Das Masterimage wird in GCP importiert.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Hinweis:**
>
> Ersetzen Sie den gesamten Großbuchstabentext durch die tatsächlichen Ressourcendetails.

#### VM auf einem Einzelmandantenknoten bereitstellen

Verwenden Sie Knoten für einzelne Mandanten, um Ihre VMs physisch von VMs in anderen Projekten zu trennen, oder um Ihre VMs auf derselben Hosthardware zu gruppieren. Informationen zum Einzelmandantenknoten finden Sie im GCP-Dokument Sole-Tenancy Overview.

Informationen zur Bereitstellung einer VM (Maschinenprofilquelle) auf dem Einzelmandantenknoten finden Sie im GCP-Dokument Provisioning VMs on Sole-Tenant Nodes.

> **Hinweis:**
>
> - Wählen Sie denselben Instanztyp und dieselbe Region wie für die Knotengruppe aus.
> - Aktivieren Sie vTPM im Abschnitt Shielded VM. Weitere Informationen finden Sie unter Kurzanleitung: Shielded VM-Optionen aktivieren.
> - Deaktivieren Sie den Bitlocker auf der Quell-VM.

#### MCS-Maschinenkatalog mit der Windows 11-Maschinenprofilquelle erstellen

Sie können einen MCS-Maschinenkatalog erstellen, um Windows 11-VMs mithilfe der Benutzeroberfläche für die vollständige Konfiguration oder von PowerShell-Befehlen zu erstellen.

> **Hinweis:**
>
> - Wählen Sie für das Masterimage den Windows 11-Snapshot oder die VM aus.
> - Wählen Sie für die Maschinenprofilquelle die Windows 11-VM als Maschinenprofil aus. Die Maschinenprofilquelle muss denselben Instanztyp haben, der im Knoten für den Einzelmandanten beschrieben ist.

Informationen zur Verwendung der Benutzeroberfläche für die vollständige Konfiguration finden Sie unter Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration erstellen.

Informationen zu PowerShell-Befehlen finden Sie unter Maschinenkatalog mit einem Maschinenprofil erstellen.

Nachdem Sie den Katalog erstellt und die VMs eingeschaltet haben, können Sie sehen, dass die Windows 11-VMs auf dem Einzelmandantenknoten in der Google Cloud-Konsole ausgeführt werden.

### Google Cloud Marketplace

Im Google Cloud Marketplace können Sie von Citrix angebotene Images durchsuchen und auswählen, um damit Maschinenkataloge zu erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature.

Um über den Google Cloud Marketplace nach einem Citrix VDA-VM-Produkt zu suchen, gehen Sie zu https://console.cloud.google.com/marketplace/.

Sie können ein benutzerdefiniertes Image oder ein einsatzbereites Citrix-Image im Google Cloud Marketplace verwenden, um das Image eines Maschinenkatalogs zu aktualisieren.

> **Hinweis:**
>
> Wenn das Maschinenprofil keine Angaben zum Speichertyp enthält, wird der Wert aus benutzerdefinierten Eigenschaften abgeleitet.

Die unterstützten Google Cloud Marketplace-Images sind:

- Windows 2019 Einzelsitzung
- Windows 2019 Multisitzung
- Ubuntu

Beispiel für das Erstellen eines Maschinenkatalogs basierend auf einem einsatzbereiten Citrix-Image:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und Google Cloud Platform-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Google-Cloudumgebungen
- Maschinenkataloge erstellen

## HPE Moonshot-Maschinenkatalog erstellen

May 17, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf HPE Moonshot-Umgebungen.

> **Hinweis:**
>
> - Verbindung zu HPE Moonshot herstellen
> - Vergewissern Sie sich, dass mindestens ein HPE Moonshot-Knoten verfügbar ist, und installieren Sie VDAs auf dem Knoten.
> - Informationen zur Erstellung des ersten HPE Moonshot Cartridge-Images finden Sie im Benutzerhandbuch zur Betriebssystembereitstellung von HP.

Sie können einen HPE Moonshot-Maschinenkatalog unter Verwendung von Folgendem erstellen:

- Benutzeroberfläche für die vollständige Konfiguration
- PowerShell-Befehle

### Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration erstellen

Führen Sie im **Assistenten für die Maschinenkatalogerstellung** folgende Schritte aus:

1. Wählen Sie auf der Seite **Betriebssystem** die Option **Einzelsitzungs-OS** oder **Multisitzungs-OS**.
2. Wählen Sie auf der Seite **Maschinenverwaltung** die Option **Maschinen mit Energieverwaltung** und **Anderer Dienst oder andere Technologie**.
3. Fügen Sie auf der Seite **Virtuelle Maschinen** Maschinen und deren Active Directory-Maschinenkonten hinzu. Sie haben folgende Wahl:
    - Klicken Sie auf **Maschinen hinzufügen**, um Maschinen manuell hinzuzufügen. Das Fenster **VMs auswählen** wird angezeigt. Erweitern Sie die HPE Moonshot Chassis-Verbindung, die Sie zuvor erstellt haben, und wählen Sie die Knoten (VMs), die Sie hinzufügen möchten. Fügen Sie dann die zugehörigen Maschinenkontonamen hinzu.
    - Klicken Sie auf **CSV-Datei hinzufügen**, um Maschinen en gros hinzuzufügen. Informationen zur Verwendung von CSV-Dateien zum Hinzufügen von Maschinen finden Sie unter Verwenden von CSV-Dateien zum Massenhinzufügen von Maschinen zu einem Katalog.

Die Seiten **Geltungsbereiche** und **Zusammenfassung** enthalten keine HPE Moonshot-spezifischen Informationen.

### Maschinenkatalog mit PowerShell-Befehlen erstellen

Führen Sie die PowerShell-Befehle `New-BrokerCatalog` und `New-BrokerMachine` aus, um einen Brokerkatalog zu erstellen und Maschinen darin zu importieren.

Beispiel:

```
1 New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und HPE Moonshot-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu HPE Moonshot
- Maschinenkataloge erstellen

## Microsoft Azure-Katalog erstellen

June 13, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Microsoft Azure-Katalog erstellen, müssen Sie eine Verbindung zu Microsoft Azure hergestellt haben. Siehe Verbindung zu Microsoft Azure.

### Maschinenkatalog erstellen

Sie können einen Maschinenkatalog auf zweierlei Art erstellen:

- Benutzeroberfläche für die vollständige Konfiguration.

- PowerShell. Weitere Informationen finden Sie unter Citrix DaaS mit Remote PowerShell SDKs verwalten. Informationen zur Implementierung bestimmter Funktionen mit PowerShell finden Sie unter PowerShell verwenden.

### Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen

Diese Informationen ergänzen die Anleitungen unter Erstellen von Maschinenkatalogen.

Ein Image kann ein Datenträger, ein Snapshot oder eine Imageversion einer Imagedefinition in Azure Compute Gallery sein, das zum Erstellen der VMs in einem Maschinenkatalog verwendet wird.

Erstellen Sie vor dem Erstellen des Maschinenkatalogs ein Image in Azure Resource Manager.

> **Hinweis:**
>
> - Das VM-Provisioning mit nicht verwalteten Datenträgern wird nicht länger unterstützt.
> - Die Unterstützung für die Verwendung eines Masterimages aus einer anderen Region als der in der Hostverbindung konfigurierten Region ist veraltet. Verwenden Sie Azure Compute Gallery, um das Masterimage in die gewünschte Region zu replizieren.

Während der Imagevorbereitung wird eine virtuelle Vorbereitungsmaschine (Vorbereitungs-VM) basierend auf der ursprünglichen VM erstellt. Diese Vorbereitungs-VM ist vom Netzwerk getrennt. Zum Trennen des Netzwerks von der Vorbereitungs-VM wird eine Netzwerksicherheitsgruppe erstellt, um den gesamten eingehenden und ausgehenden Datenverkehr zu blockieren. Die Netzwerksicherheitsgruppe wird automatisch einmal pro Katalog erstellt. Der Name der Netzwerksicherheitsgruppe lautet `Citrix-Deny-All-a3pgu-GUID`, wobei die GUID nach dem Zufallsprinzip generiert wird. Beispiel: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

Assistent für die Maschinenkatalogerstellung:

1. Die Seiten **Maschinentyp** und **Maschinenverwaltung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.
2. Wählen Sie auf der Seite **Image** das Image, das Sie als Masterimage für alle Maschinen im Katalog verwenden möchten. Der **Assistent zur Imageauswahl** wird angezeigt. Gehen Sie wie folgt vor, um ein Image auszuwählen:

   a) (Gilt nur für Verbindungen mit innerhalb oder zwischen Mandanten freigegebenen Images) Wählen Sie das Abonnement, in dem sich das Image befindet.
   b) Wählen Sie eine Ressourcengruppe.
   c) Gehen Sie zur Azure Managed Disks, zur Azure Compute Gallery oder zur Azure-Imageversion.

   Beachten Sie bei der Imageauswahl Folgendes:

- Vergewissern Sie sich, dass ein Citrix VDA auf dem Image installiert ist.
- Wenn Sie einen Datenträger auswählen, der an eine VM angeschlossen ist, müssen Sie die VM herunterfahren, bevor Sie mit dem nächsten Schritt fortfahren.

> **Hinweis:**
>
> - Das Abonnement, das der Verbindung (Host) entspricht, die die Maschinen im Katalog erstellt hat, ist mit einem grünen Punkt gekennzeichnet. Bei den anderen Abonnements handelt es sich um diejenigen, die die Azure Compute Gallery mit diesem Abonnement teilen. In diesen Abonnements werden nur geteilte Kataloge angezeigt. Informationen zur Konfiguration freigegebener Abonnements finden Sie unter Images innerhalb eines Mandanten freigeben (abonnementübergreifend) und Images mandantenübergreifend freigeben.
> - Sie können ein Provisioningschema mit einem kurzlebigen Betriebssystemdatenträger unter Windows mit vertrauenswürdigem Start erstellen. Wenn Sie ein Image mit vertrauenswürdigem Start auswählen, müssen Sie ein Maschinenprofil mit vertrauenswürdigem Start auswählen, das mit vTPM aktiviert ist. Informationen zum Erstellen von Maschinenkatalogen mit kurzlebigem Betriebssystemdatenträger finden Sie unter Erstellen von Maschinen mit kurzlebigem Betriebssystemdatenträger.
> - Während der Imagereplikation können Sie das Image als Masterimage auswählen und das Setup abschließen. Die Katalogerstellung kann jedoch länger dauern, während das Image repliziert wird. MCS erfordert, dass die Replikation innerhalb einer Stunde ab Katalogerstellung abgeschlossen ist. Tritt bei der Replikation ein Timeout auf, schlägt die Katalogerstellung fehl. Sie können den Replikationsstatus in Azure überprüfen. Versuchen Sie es erneut, wenn die Replikation noch aussteht oder nach dem Abschluss der Replikation.
> - Sie können einen VM-Katalog der zweiten Generation mithilfe eines Images der zweiten Generation bereitstellen, um die Startzeitleistung zu verbessern. Das Erstellen eines Maschinenkatalogs der zweiten Generation mit einem Image der ersten Generation wird nicht unterstützt. Das Erstellen eines Maschinenkatalogs der ersten Generation mit einem Image der zweiten Generation wird ebenfalls nicht unterstützt. Außerdem werden ältere Images ohne Generationsangabe als Image der ersten Generation behandelt.

Wählen Sie aus, ob virtuelle Maschinen im Katalog die Konfigurationen eines Maschinenprofils übernehmen sollen. Standardmäßig ist das Kontrollkästchen **Maschinenprofil verwenden (obligatorisch für Azure Active Directory)** aktiviert. Klicken Sie auf **Wählen Sie ein Maschinenprofil**, um eine VM- oder ARM-Vorlagenspezifikation aus einer Liste mit Ressourcengruppen auszuwählen.

Beispiele für Konfigurationen, die VMs von einem Maschinenprofil übernehmen können:

- Beschleunigtes Netzwerk
- Startdiagnose
- Caching des Hostdatenträgers (bei OS- und MCSIO-Datenträgern)
- Maschinengröße (sofern nicht anders angegeben)
- Für VM platzierte Tags

> **Hinweis:**
>
> - Wenn Sie ein Masterimage für Maschinenkataloge in Azure auswählen, wird das Maschinenprofil auf der Grundlage des ausgewählten Masterimages gefiltert. Beispielsweise wird das Maschinenprofil basierend auf dem Windows-Betriebssystem, Sicherheitstyps, der Unterstützung für den Ruhezustand und der Datenträgerverschlüsselungssatz-ID des Masterimages gefiltert.
> - Die Verwendung eines Maschinenprofils mit vertrauenswürdigem Start als **Sicherheitstyp** ist obligatorisch, wenn Sie ein Image oder einen Snapshot auswählen, für das bzw. den der vertrauenswürdige Start aktiviert ist. Sie können dann SecureBoot und vTPM aktivieren oder deaktivieren, indem Sie die zugehörigen Werte im Maschinenprofil angeben. Informationen zu vertrauenswürdigen Starts in Azure finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Validieren Sie die ARM-Vorlagenspezifikation, um sicherzustellen, dass sie als Maschinenprofil zum Erstellen eines Maschinenkatalogs verwendet werden kann. Informationen zum Erstellen einer Azure-Vorlagenspezifikation finden Sie unter Azure-Vorlagenspezifikation erstellen.

Es gibt zwei Möglichkeiten zur Validierung der ARM-Vorlagenspezifikation:

- Klicken Sie nach Auswahl der ARM-Vorlagenspezifikation aus der Liste der Ressourcengruppen auf **Weiter**. Wenn die ARM-Vorlagenspezifikation Fehler enthält, werden Fehlermeldungen angezeigt,
- Führen Sie einen der folgenden PowerShell-Befehle aus:
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

  Beispiel:

```
Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
    InventoryPath machineprofile.folder/vdi01-d-rg.
    resourcegroup/VDD-templ-spec.templatespec/1.5.
    templatespecversion
<!--NeedCopy-->
```

Nachdem Sie den Katalog erstellt haben, können Sie die Konfigurationen anzeigen, die das Image vom Maschinenprofil erbt. Wählen Sie auf dem Knoten **Maschinenkataloge** den Katalog aus, um die Details im unteren Bereich anzuzeigen. Klicken Sie dann auf die Registerkarte **Vorlageneigenschaften**, um die Eigenschaften des Maschinenprofils anzuzeigen. Im Abschnitt **Tags** werden bis zu drei Tags angezeigt. Zum Anzeigen aller auf der VM platzierten Tags klicken Sie auf **Alle anzeigen**.

Um VMs mit Maschinenerstellungsdiensten (MCS) auf einem dedizierten Azure-Host bereitzustellen, aktivieren Sie das Kontrollkästchen **Hostgruppe verwenden** und wählen dann eine Hostgruppe aus der Liste aus. Eine Hostgruppe ist eine Ressource, die eine Sammlung dedizierter Hosts darstellt. Ein dedizierter Host ist ein Dienst, der physische Server bereitstellt, die eine oder mehrere virtuelle Maschinen hosten. Ihr Server ist für Ihr Azure-Abonnement reserviert und wird nicht mit anderen Abonnenten geteilt. Bei Verwendung eines dedizierten Hosts stellt Azure sicher, dass nur Ihre VMs auf diesem Host ausgeführt werden. Dieses Feature eignet sich für Szenarios, in denen Sie regulatorische oder interne Sicherheitsanforderungen erfüllen müssen. Weitere Informationen zu Hostgruppen und Überlegungen zu ihrer Verwendung finden Sie unter VMs auf dedizierten Azure-Hosts bereitstellen.

> **Wichtig:**
>
> - Es werden nur Hostgruppen mit aktivierter automatischer Azure-Platzierung angezeigt.
> - Durch Verwendung einer Hostgruppe wird die Seite **Virtuelle Maschinen** geändert, die später im Assistenten angezeigt wird. Auf dieser Seite werden nur die Maschinengrößen angezeigt, die in der ausgewählten Hostgruppe enthalten sind. Außerdem sind Verfügbarkeitszonen automatisch ausgewählt und nicht wählbar.

3. Die Seite **Speicher- und Lizenztypen** wird nur angezeigt, wenn Sie ein Azure Resource Manager-Image verwenden.

   Für den Maschinenkatalog können Sie die folgenden Speichertypen verwenden:

   - **Premium-SSD.** Bietet Datenträgerspeicherung mit hoher Leistung und niedriger Latenz für VMs mit E/A-intensiven Workloads.
   - **Standard-SSD.** Kostengünstige Speicheroption, die für Workloads geeignet ist, die eine gleichmäßige Leistung bei niedrigeren IOPS-Raten erfordern.
   - **Standard-HDD.** Zuverlässiger, kostengünstiger Datenträgerspeicher, der für VMs mit latenzunempfindlichen Workloads geeignet ist.
   - **Kurzlebiger Azure-Betriebsystemdatenträger**. Kostengünstige Speicheroption mit Wiederverwendung des lokalen VM-Datenträgers zum Hosten des Betriebssystemdatenträgers. Alternativ können Sie mit PowerShell Maschinen mit kurzlebigen Betriebsystemdatenträgern erstellen. Weitere Informationen finden Sie unter Kurzlebige

Azure-Datenträger. Beachten Sie bei der Verwendung kurzlebiger Betriebssystemdatenträger Folgendes:

- Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.
- Zum Aktualisieren von Maschinen, die kurzlebige Betriebssystemdatenträger verwenden, müssen Sie ein Image auswählen, dessen Größe die des Cachedatenträgers bzw. des temporären Datenträgers der VM nicht übersteigt.
- Sie können die später im Assistenten angebotene Option **VM und Systemdatenträger während Energiezyklen beibehalten** nicht verwenden.

> **Hinweis:**
>
> Der Identitätsdatenträger wird unabhängig vom gewählten Speichertyp immer mit Standard-SSD erstellt.

Der gewählte Speichertyp bestimmt, welche Maschinengrößen auf der Seite **Virtuelle Maschinen** des Assistenten angeboten werden. MCS konfiguriert Premium- und Standarddatenträger für die Verwendung von lokal redundantem Speicher (LRS). LRS erstellt mehrere synchrone Kopien Ihrer Daten in einem Datencenter. Bei kurzlebigen Azure-Betriebssystemdatenträgern wird das Betriebssystem auf dem lokalen VM-Datenträger gespeichert. Weitere Informationen über Speichertypen und Speicherreplikation bei Azure finden Sie in den folgenden Artikeln:

- Einführung in Azure Storage
- Azure Storage Premium: Design für hohe Leistung
- Azure Storage-Redundanz

Wählen Sie aus, ob vorhandene Windows- oder Linux-Lizenzen verwendet werden sollen:

- Windows-Lizenzen: Mit Windows-Lizenzen und Windows-Images (Azure- oder benutzerdefinierte Images) können Sie Windows-VMs in Azure zu geringeren Kosten ausführen. Es gibt zwei Arten von Lizenzen:
  - **Windows Server-Lizenz**. Ermöglicht die Verwendung Ihrer Windows Server- oder Azure Windows Server-Lizenzen und somit die Nutzung des Azure-Hybridvorteils. Einzelheiten finden Sie unter https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Der Azure-Hybridvorteil senkt die Kosten des Ausführens von VMs in Azure auf die Grundgebühr für Computekapazität, da keine Gebühren für zusätzliche Windows Server-Lizenzen aus dem Azure-Katalog erhoben werden.
  - **Windows-Clientlizenz**. Ermöglicht die Verwendung Ihrer Windows 10- und Windows 11-Lizenzen in Azure und somit die Ausführung von Windows 10- und Windows 11-VMs in Azure ohne Erfordernis zusätzlicher Lizenzen. Weitere Informationen finden Sie unter Clientzugriffslizenzen und Verwaltungslizenzen.

- Linux-Lizenzen: Bei Verwendung eigener Linux-Lizenzen (Bring Your Own Subscription oder BYOS) müssen Sie für die Software nicht zahlen. Die BYOS-Gebühr umfasst nur die Hardware für die Rechenleistung. Es gibt zwei Arten von Lizenzen:
  - **RHEL_BYOS**: Um den Typ RHEL_BYOS zu verwenden, aktivieren Sie Red Hat Cloud Access in Ihrem Azure-Abonnement.
  - **SLES_BYOS**: Die BYOS-Versionen von SLES beinhalten Unterstützung von SUSE.

Beispiel:

- Windows-Lizenz überprüfen
- Linux-Lizenz konfigurieren

Lesen Sie die folgenden Dokumente, um mehr über Lizenztypen und ihre Vorteile zu erfahren:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery ist ein Repository zum Verwalten und Freigeben von Images. Damit können Sie Images in Ihrer gesamten Organisation verfügbar machen. Wir empfehlen Ihnen, beim Erstellen großer nicht-persistenter Maschinenkataloge ein Image in Azure Compute Gallery zu speichern, da sich VDA-Betriebssystemdatenträger dadurch schneller zurücksetzen lassen. Nachdem Sie **Vorbereitetes Image in der Azure Compute Gallery platzieren** ausgewählt haben, wird der Abschnitt **Azure Compute Gallery-Einstellungen** angezeigt, in dem Sie weitere Azure Computer Gallery-Einstellungen angeben können:

- **Verhältnis von virtuellen Maschinen zu Imagereplikaten**. Hier können Sie das Verhältnis von virtuellen Maschinen zu Imagereplikaten angeben, die Azure beibehalten soll. Standardmäßig speichert Azure ein Imagereplikat pro 40 nicht-persistente Maschinen. Bei persistenten Maschinen ist diese Zahl voreingestellt auf 1000.
- **Maximale Replikate**. Hier können Sie die maximale Anzahl von Image-Replikaten angeben, die Azure speichern soll. Der Standardwert ist 10.

Weitere Informationen zu Azure Compute Gallery finden Sie unter Azure Compute Gallery.

4. Geben Sie auf der Seite **VMs** an, wie viele VMs Sie erstellen möchten und wie groß sie sein sollen. Nach der Katalogerstellung können Sie die Maschinengröße durch Bearbeiten des Katalogs ändern.
5. Die Seite **Netzwerkkarten** enthält keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.

6. Wählen Sie auf der Seite **Datenträgereinstellungen**, ob der Zurückschreibcache aktiviert werden soll. Wenn die MCS-Speicheroptimierung aktiviert ist, können Sie beim Erstellen eines Katalogs folgende Einstellungen konfigurieren. Diese Einstellungen gelten für Azure- und für GCP-Umgebungen.

   Nach dem Aktivieren des Zurückschreibcache können Sie Folgendes tun:

   - Konfigurieren Sie die Größe des Datenträgers und des RAM, die zum Zwischenspeichern temporärer Daten verwendet werden. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.
   - Wählen des Speichertyps für den Datenträger für den Zurückschreibcache. Die folgenden Speichertypen stehen für den Zurückschreibcache-Datenträger zur Verfügung:
     - Premium-SSD
     - Standard-SSD
     - Standard-HDD
   - Wählen eines persistenten Datenträgers für den Zurückschreibcache für die bereitgestellten VMs (bei Bedarf). Wählen Sie **Zurückschreibcache aktivieren**, um die Optionen verfügbar zu machen. Die Standardeinstellung ist **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**.
   - Wählen Sie einen Datenträgertyp für den Zurückschreibcache aus.
     - **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**. Wenn diese Option ausgewählt ist, wird der Datenträger für den Zurückschreibcache während Energiezyklen gelöscht. Alle darauf umgeleitete Daten gehen verloren. Wenn auf dem temporären Datenträger der VM ausreichend Speicherplatz vorhanden ist, wird er als Host für den Zurückschreibcachedatenträger verwendet, da dies Ihre Kosten reduziert. Nach der Katalogerstellung können Sie überprüfen, ob die bereitgestellten Maschinen den temporären Datenträger verwenden. Klicken Sie dazu auf den Katalog und überprüfen Sie die Informationen auf der Registerkarte **Vorlageneigenschaften**. Bei Verwendung des temporären Datenträgers wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Ja (mit dem temporären Datenträger der VM)** angezeigt. Wenn er nicht verwendet wird, wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Nein (nicht mit dem temporären Datenträger der VM)** angezeigt.
     - **Persistenter Datenträger für Zurückschreibcache.** Wenn diese Option ausgewählt ist, wird der Zurückschreibcache-Datenträger für die bereitgestellten VMs beibehalten. Die Aktivierung dieser Option erhöht die Speicherkosten.
   - Wählen Sie aus, ob VMs und Systemdatenträger für VDAs bei Energiezyklen beibehalten werden sollen.

**VM und Systemdatenträger während Neustarts beibehalten.** Verfügbar, wenn Sie **Zurückschreibcache aktivieren** ausgewählt haben. Standardmäßig werden VMs und die Systemdatenträger beim Herunterfahren gelöscht und beim Starten neu erstellt. Wenn Sie die VM-Neustartzeiten reduzieren möchten, wählen Sie diese Option. Allerdings erhöht die Aktivierung dieser Option auch die Speicherkosten.

- Wählen Sie aus, ob Sie die **Einsparung von Speicherkosten aktivieren** möchten. Wenn diese Option aktiviert ist, wird der Speicherdatenträger beim Herunterfahren der VM auf Standard-HDD herabgestuft, um Speicherkosten zu senken. Beim Neustart wechselt die VM wieder zu den ursprünglichen Einstellungen. Die Option lässt sich auf Speicher- und Zurückschreibcache-Datenträger anwenden. Alternativ können Sie auch PowerShell verwenden. Siehe Speichertyp beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern.

  > **Hinweis:**
  >
  > Bei Microsoft gelten Einschränkungen für die Änderung des Speichertyps beim Herunterfahren einer VM. Es ist auch möglich, dass Microsoft künftig Änderungen des Speichertyps blockiert. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

- Wählen Sie aus, ob Daten auf Maschinen in diesem Katalog verschlüsselt werden sollen und welcher Verschlüsselungsschlüssel verwendet werden soll. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel (CMK) ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Die Standardeinstellungen werden vom Maschinenprofil oder vom Masterimage übernommen, wobei das Profil Vorrang hat:

  - Wenn Sie ein *Maschinenprofil* mit einem *CMK* verwenden, wird die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln** automatisch ausgewählt und verwendet standardmäßig den Schlüssel aus dem *Maschinenprofil*.
  - Wenn Sie ein *Maschinenprofil* mit einem von einer Plattform verwalteten Schlüssel (PMK) verwenden und das *Masterimage CMK*-verschlüsselt ist, wird die Option**Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln** automatisch ausgewählt und verwendet standardmäßig den Schlüssel aus dem Masterimage.
  - Wenn Sie *kein Maschinenprofil* verwenden und das *Masterimage CMK-verschlüsselt* ist, wird die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln** automatisch ausgewählt und verwendet standardmäßig den Schlüssel aus dem *Masterimage*.

Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

7. Wählen Sie auf der Seite **Ressourcengruppe** aus, ob Sie neue Ressourcengruppen erstellen oder vorhandene verwenden.

   - Wenn Sie Ressourcengruppen erstellen möchten, wählen Sie **Weiter**.
   - Wenn Sie vorhandene Ressourcengruppen verwenden möchten, wählen Sie Gruppen in der Liste **Zum Bereitstellen verfügbare Ressourcengruppen** aus.

   > **Hinweis:**
   >
   > Wählen Sie genügend Gruppen aus, um die Maschinen aufzunehmen, die Sie im Katalog erstellen. Wenn sie nicht ausreichen, werden Sie in einer Meldung darauf hingewiesen. Wählen Sie ggf. mehr als die erforderliche Mindestanzahl aus, wenn Sie dem Katalog später weitere VMs hinzufügen möchten. Sie können einem Katalog nach dessen Erstellung keine weiteren Ressourcengruppen mehr hinzufügen.

   Weitere Informationen finden Sie unter Azure-Ressourcengruppen.

8. Wählen Sie auf der Seite **Maschinenidentitäten** einen Identitätstyp und konfigurieren Sie Identitäten für Maschinen in dem Katalog. Wenn Sie die VMs als **In Azure Active Directory eingebunden** festlegen, können Sie sie zu einer Azure AD-Sicherheitsgruppe hinzufügen. Verfahren:

   a) Wählen Sie im Feld **Identitätstyp** die Option **In Azure Active Directory eingebunden**. Die Option **Azure AD-Sicherheitsgruppe (optional)** wird angezeigt.
   b) Klicken Sie auf **Azure AD-Sicherheitsgruppe: Neu erstellen**.
   c) Geben Sie einen Gruppennamen ein und klicken Sie auf **Erstellen**.
   d) Folgen Sie den angezeigten Anweisungen, um sich bei Azure anzumelden.
      Wenn der Gruppenname in Azure nicht vorliegt, erscheint ein grünes Symbol. Andernfalls erscheint eine Fehlermeldung, in der Sie aufgefordert werden, einen neuen Namen einzugeben.
   e) Um die Sicherheitsgruppe einer zugewiesenen Sicherheitsgruppe hinzuzufügen, wählen Sie **Einer zugewiesenen Sicherheitsgruppe als Mitglied beitreten** und klicken Sie dann auf **Gruppe auswählen**, um eine zugewiesene Gruppe auszuwählen.
   f) Geben Sie das Benennungsschema für Maschinenkonten für die VMs ein.

   Nach der Katalogerstellung greift Citrix DaaS für Sie auf Azure zu und erstellt die Sicherheitsgruppe und eine dynamische Mitgliedschaftsregel für die Gruppe. Basierend auf der Regel werden virtuelle Maschinen mit dem in diesem Katalog angegebenen Benennungsschema automatisch zur Sicherheitsgruppe hinzugefügt.

   Um dem Katalog virtuelle Maschinen mit einem anderen Benennungsschema hinzuzufügen, müssen Sie sich bei Azure anmelden. Citrix DaaS kann dann auf Azure zugreifen und eine dynamische Mitgliedschaftsregel erstellen, die auf dem neuen Benennungsschema basiert.

   Beim Löschen des Katalogs ist für das Löschen der Sicherheitsgruppe aus Azure ebenfalls eine Anmeldung bei Azure erforderlich.

> **Hinweis:**
>
> Um die Azure AD-Sicherheitsgruppe nach der Katalogerstellung umzubenennen, bearbeiten Sie den Katalog und wechseln Sie im linken Bereich zu **Azure AD-Sicherheitsgruppe**. Namen von Azure AD-Sicherheitsgruppen dürfen die folgenden Zeichen nicht enthalten: `@ "\ / ; : # . * ? = < > | [ ] ( )'`.

- Die Seiten **Domänenanmeldeinformationen** und **Zusammenfassung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.

Schließen Sie den Assistenten ab.

### Azure-Vorlagenspezifikation erstellen

Sie können eine Azure-Vorlagenspezifikation im Azure-Portal erstellen und sie in der Schnittstelle "Vollständige Konfiguration"und in den PowerShell-Befehlen verwenden, um einen MCS-Maschinenkatalog zu erstellen oder zu aktualisieren.

Azure-Vorlagenspezifikation für eine vorhandene VM erstellen:

1. Gehen Sie zum Azure-Portal. Wählen Sie eine Ressourcengruppe und dann die VM und die Netzwerkschnittstelle aus. Klicken Sie oben im Menü **...** auf **Export template**.
2. Deaktivieren Sie das Kontrollkästchen **Include parameters**, wenn Sie eine Vorlagenspezifikation für die Katalogbereitstellung erstellen möchten.
3. Klicken Sie auf **Add to library**, um die Vorlagenspezifikation später zu ändern.
4. Geben Sie auf der Seite **Importing template** die erforderlichen Informationen wie **Name**, **Subscription**, **Subscription**, **Location** und **Version** ein. Klicken Sie auf **Next: Edit Template**.
5. Sie benötigen außerdem eine Netzwerkschnittstelle als unabhängige Ressource, wenn Sie Kataloge bereitstellen möchten. Daher müssen Sie alle `dependsOn`-Elemente in der Vorlagenspezifikation entfernen. Beispiel:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
<!--NeedCopy-->
```

6. Wählen Sie **Review + Create** und erstellen Sie die Vorlagenspezifikation.
7. Überprüfen Sie auf der Seite **Template Specs** die erstellte Vorlagenspezifikation. Klicken Sie auf die Vorlagenspezifikation. Klicken Sie im linken Bereich auf **Versions**.
8. Sie können eine neue Version erstellen, indem Sie auf **Create new version** klicken. Geben Sie eine neue Versionsnummer an, nehmen Sie Änderungen an der aktuellen Vorlagenspezifikation

vor und klicken Sie auf **Review + Create**, um die neue Version der Vorlagenspezifikation zu erstellen.

Mit den folgenden PowerShell-Befehlen können Sie Informationen zur Vorlagenspezifikation und Vorlagenversion abrufen:

- Um Informationen über die Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- Um Informationen über die Version der Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
<!--NeedCopy-->
```

#### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Sie können hierfür die Schnittstelle Vollständige Konfiguration oder PowerShell verwenden.

- Weitere Informationen zur Verwendung der Schnittstelle **Vollständige Konfiguration** finden Sie unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.
- PowerShell: Weitere Informationen finden Sie unter Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

### Provisioning von Maschinen in spezifischen Verfügbarkeitszonen

Sie können das Provisioning von Maschinen auch in spezifischen Verfügbarkeitszonen in Azure-Umgebungen ausführen. Dies können Sie mit der Oberfläche “Vollständige Konfiguration”oder PowerShell erreichen.

> **Hinweis:**
>
> Wenn keine Zonen angegeben werden, lässt MCS Azure die Maschinen innerhalb der Region platzieren. Werden mehrere Zonen angegeben, verteilt MCS die Maschinen nach dem Zufallsprinzip in den Zonen.

#### Verfügbarkeitszonen in der Oberfläche "Vollständige Konfiguration"konfigurieren

Beim Erstellen eines Maschinenkatalogs können Sie Verfügbarkeitszonen für das Provisioning von Maschinen angeben. Wählen Sie auf der Seite **Virtuelle Maschinen** eine oder mehrere Verfügbarkeitszonen aus, in denen Sie Maschinen erstellen möchten.

Es gibt zwei Gründe, aus denen keine Verfügbarkeitszonen verfügbar sind: Die Region hat keine Verfügbarkeitszonen oder die ausgewählte Maschinengröße ist nicht verfügbar.

Informationen zur Konfiguration mit dem PowerShell-Befehl finden Sie unter Verfügbarkeitszonen mit PowerShell konfigurieren.

### Kurzlebige Azure-Datenträger

Ein kurzlebiger Azure-Datenträger ermöglicht die Umnutzung des Cachedatenträgers oder temporären Datenträgers zum Speichern des Betriebssystemdatenträgers für eine virtuelle Azure-Maschine. Dies ist nützlich für Azure-Umgebungen, die anstelle von Standard-HDD-Datenträgern leistungsstärkere SSD-Datenträger erfordern. Informationen zum Erstellen eines Katalogs mit einem kurzlebigen Azure-Datenträger finden Sie unter Katalog mit kurzlebigem Azure-Datenträger erstellen.

> **Hinweis:**
>
> Persistente Kataloge unterstützen keine kurzlebigen Betriebssystemdatenträger.

Kurzlebige Betriebssystemdatenträger erfordern ein Provisioningschema mit verwalteten Datenträgern und eine Azure Compute Gallery. Weitere Informationen finden Sie unter Azure Shared Image Gallery.

#### Temporären kurzlebigen OS-Datenträger speichern

Sie können einen kurzlebigen OS-Datenträger auf dem Temp- bzw. Ressourcendatenträger der VM speichern. So können Sie einen kurzlebigen OS-Datenträger mit VMs verwenden, die über keinen oder nur unzureichenden Cache verfügen. Solche VMs verfügen über einen Temp- bzw. Ressourcendatenträger zum Speichern eines kurzlebigen OS-Datenträgers (z. B. `Ddv4`).

Beachten Sie Folgendes:

- Kurzlebige Datenträger werden entweder auf dem VM-Cachedatenträger oder auf dem temporären bzw. Ressourcendatenträger der VM gespeichert. Die Cachedatenträger ist dem temporären Datenträger vorzuziehen, es sei denn, der Cachedatenträger ist zu klein für den Inhalt des Betriebsystemdatenträgers.

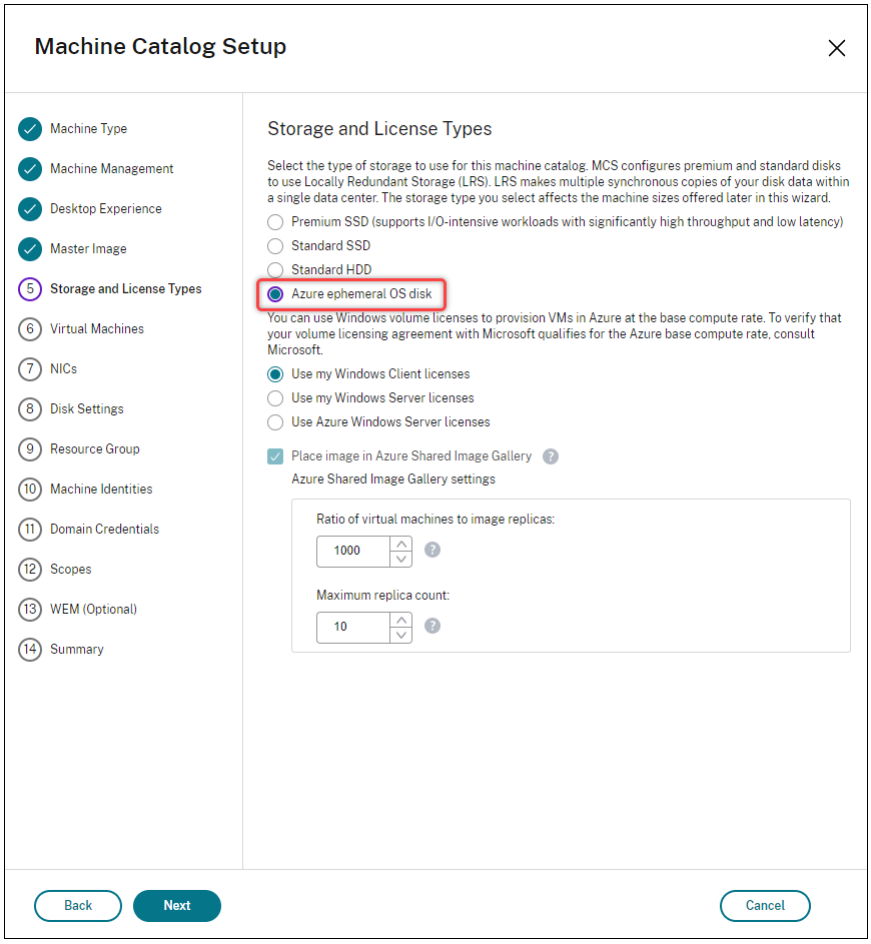
- Entsteht bei Updates ein neues Image, das größer als der Cachedatenträger und kleiner als der Temp-Datenträger ist, wird der kurzlebige OS-Datenträger durch den Temp-Datenträger der VM ersetzt.

### Kurzlebige Azure-Betriebssystemdatenträger und MCS-Speicheroptimierung (MCS-E/A)

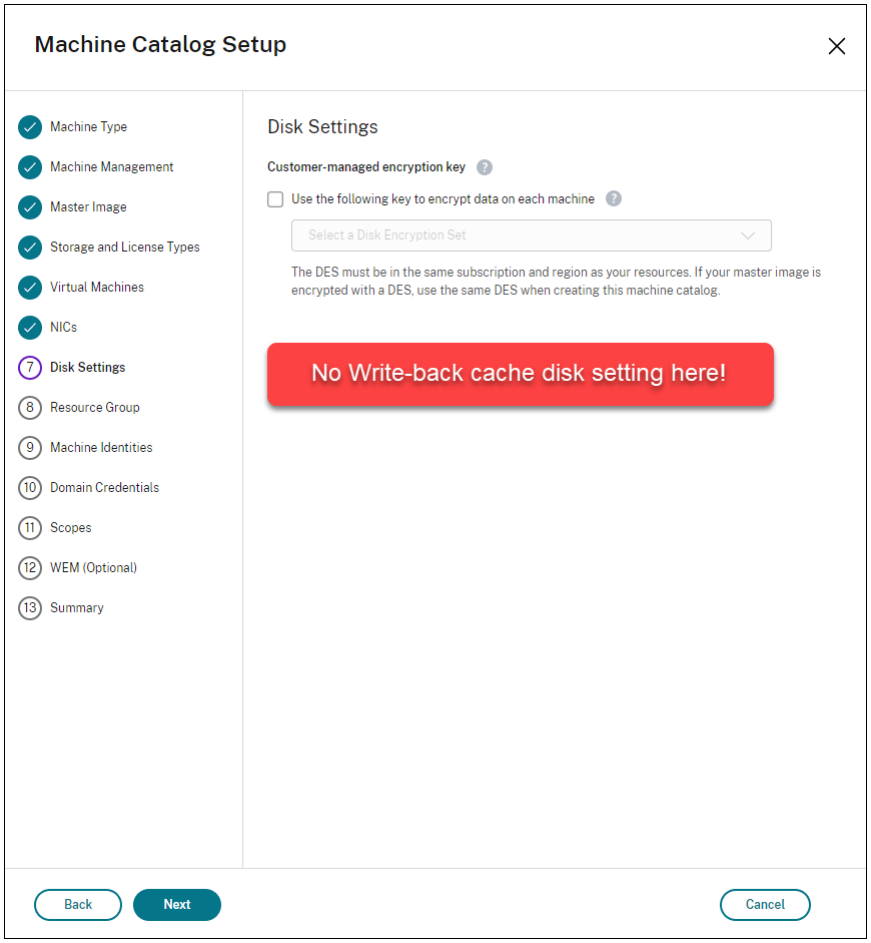
Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.

Wichtige Punkte:

- Sie können keinen Maschinenkatalog mit gleichzeitig aktiviertem kurzlebigem Betriebssystemdatenträger und MCS-E/A erstellen.
- Wenn Sie im **Assistenten zum Einrichten eines Maschinenkatalogs** auf der Seite **Speicher- und Lizenztypen** die Option **Kurzlebiger Azure-Betriebssystemdatenträger** auswählen, werden auf der Seite **Datenträgereinstellungen** keine Optionen für den Zurückschreibcache-Datenträger angezeigt.






- Die PowerShell-Parameter (`UseWriteBackCache` und `UseEphemeralOsDisk`), die in `New-ProvScheme` oder `Set-ProvScheme` auf **true** gesetzt sind, schlagen mit entsprechender Fehlermeldung fehl.
- Bei bestehenden Maschinenkatalogen, für die bei der Erstellung beide Features aktiviert wurden, ist weiterhin Folgendes möglich:
  - Aktualisieren des Maschinenkatalogs
  - Hinzufügen oder Löschen von VMs
  - Löschen des Maschinenkatalogs

### Azure Compute Gallery

Verwenden Sie Azure Compute Gallery (früher Shared Image Gallery) als Repository mit veröffentlichten Images für per MCS bereitgestellte Maschinen in Azure. Sie können ein veröffentlichtes Image in der Image Gallery speichern, um die Erstellung und Hydration von Betriebssystemdatenträgern zu beschleunigen und die OS- und Anwendungsstartzeiten nicht persistenter VMs zu verbessern. Azure Compute Gallery enthält die folgenden drei Elemente:

- Gallery: Hier werden Images gespeichert. MCS erstellt je eine Gallery für jeden Maschinenkatalog.
- Imagedefinition: Diese Definition enthält Informationen zum veröffentlichten Image (Betriebssystemtyp/-zustand, Azure-Region). MCS erstellt eine Imagedefinition für jedes Image, das für den Katalog erstellt wurde.
- Gallery Image Version: Jedes Image in einer Azure Compute Gallery kann mehrere Versionen haben, und jede Version kann mehrere Replikate in verschiedenen Regionen haben. Jedes Replikat ist eine vollständige Kopie des veröffentlichten Images. Citrix DaaS erstellt für jedes Image eine Standard_LRS-Imageversion (Version 1.0.0) mit der entsprechenden Anzahl von Replikaten in der Region des Katalogs, basierend auf der Maschinenanzahl im Katalog, der konfigurierten Replikatquote und der konfigurierten Anzahl maximaler Replikate.

> **Hinweis:**
>
> Die Azure Compute Gallery-Funktion ist nur mit verwalteten Datenträgern kompatibel. Sie ist nicht für Legacy-Maschinenkataloge verfügbar.

Weitere Informationen finden Sie unter Übersicht über Azure Shared Image Gallery.

#### Zugriff auf Images aus Azure Compute Gallery

Als Image zum Erstellen eines Maschinenkatalogs können Sie Images auswählen, die Sie in der Azure Compute Gallery erstellt haben. Diese Images sind auf der Seite **Image** des Assistenten zum Erstellen von Maschinenkatalogen aufgelistet.

Damit diese Images angezeigt werden, müssen Sie folgende Schritte ausführen:

1. Richten Sie Citrix DaaS ein.
2. Stellen Sie eine Verbindung mit Azure Resource Manager her.
3. Erstellen Sie im Azure-Portal eine Ressourcengruppe. Weitere Informationen finden Sie unter Erstellen einer Azure Shared Image Gallery über das Portal.
4. Erstellen Sie in der Ressourcengruppe eine Azure Compute Gallery.
5. Erstellen Sie in der Azure Compute Gallery eine Imagedefinition.
6. Erstellen Sie in der Imagedefinition eine Imageversion.

Weitere Informationen zur Konfiguration von Azure Compute Gallery finden Sie unter Azure Compute Gallery konfigurieren.

### Bedingungen für die Verwendung eines temporären Azure-Datenträgers als Datenträger für den Zurückschreibcache

Sie können den temporären Azure-Datenträger nur dann als Datenträger für den Zurückschreibcache verwenden, wenn alle der folgenden Bedingungen erfüllt sind:

- Der Datenträger für den Zurückschreibcache darf nicht persistent sein, da der temporäre Azure-Datenträger nicht für persistente Daten geeignet ist.
- Die gewählte Azure-VM-Größe muss einen temporären Datenträger einschließen.
- Der kurzlebige Betriebsystemdatenträger muss nicht aktiviert sein.
- Stimmen Sie zu, dass die Datenträgerdatei für den Zurückschreibcache auf dem temporären Azure-Datenträger platziert wird.
- Der temporäre Azure-Datenträger muss größer sein als der Gesamtwert für (Größe des Datenträgers des Zurückschreibecache + reservierter Speicherplatz für Auslagerungsdatei + 1 GB Pufferspeicher).

#### Szenarios mit nicht persistentem Datenträger für den Zurückschreibcache

Die folgende Tabelle enthält drei Szenarios, in denen beim Erstellen des Maschinenkatalogs der temporäre Datenträger für den Zurückschreibcache (WBC) verwendet wird.

| Szenario | Ergebnis |
|---|---|
| Alle Bedingungen zur Verwendung des temporären Datenträgers für den Zurückschreibcache sind erfüllt. | Die WBC-Datei `mcsdif.vhdx` wird auf dem temporären Datenträger abgelegt. |
| Der temporäre Datenträger hat nicht genügend Speicherplatz für den Zurückschreibcache. | Ein VHD-Datenträger "MCSWCDisk"wird erstellt und die WBC-Datei `mcsdif.vhdx` wird auf diesem Datenträger abgelegt. |
| Der temporäre Datenträger hat genügend Speicherplatz für den Zurückschreibcache, `UseTempDiskForWBC` ist jedoch auf False gesetzt. | Ein VHD-Datenträger "MCSWCDisk"wird erstellt und die WBC-Datei `mcsdif.vhdx` wird auf diesem Datenträger abgelegt. |

Weitere Informationen finden Sie in den folgenden PowerShell-Themen:

- Maschinenkatalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen
- Maschinenkatalog mit persistentem Zurückschreibcachedatenträger erstellen

### Azure-serverseitige Verschlüsselung

Citrix DaaS unterstützt vom Kunden verwaltete Schlüssel für Azure Managed Disks über Azure Key Vault. Mit dieser Unterstützung können Sie Ihre Unternehmens- und Compliance-Anforderungen verwalten, indem Sie die verwalteten Datenträger des Maschinenkatalogs mit Ihrem eigenen Schlüssel verschlüsseln. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung von Azure Disk Storage.

Bei Verwendung dieses Features für verwaltete Datenträger gilt Folgendes:

- Um den Schlüssel zu ändern, mit dem ein Datenträger verschlüsselt ist, ändern Sie den aktuellen Schlüssel im `DiskEncryptionSet`. Alle dem `DiskEncryptionSet` zugeordneten Ressourcen werden dann mit dem neuen Schlüssel verschlüsselt.
- Wenn Sie den Schlüssel deaktivieren oder löschen, werden alle VMs mit Datenträgern, die den Schlüssel verwenden, automatisch heruntergefahren. Nach dem Herunterfahren können die VMs erst wieder verwendet werden, wenn Sie den Schlüssel wieder aktivieren oder einen neuen Schlüssel zuweisen. Kataloge, die den Schlüssel verwenden, können nicht aktiviert werden und Sie können solchen Katalogen keine VMs hinzufügen.

#### Wichtige Überlegungen bei der Verwendung vom Kunden verwalteter Schlüssel

Beachten Sie die folgenden Punkte bei der Verwendung dieses Features:

- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Datenträger, Snapshots und Images, die mit kundenverwalteten Schlüsseln verschlüsselt wurden, können nicht in anderen Ressourcengruppen oder Abonnements verschoben werden.
- Auf der Microsoft-Website finden Sie Informationen zu Limits für Datenträgerverschlüsselungssätze pro Region.

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren der Azure-serverseitigen Verschlüsselung finden Sie unter Schnellstart: Key Vault-Erstellung mit dem Azure-Portal .

#### Vom Kunden verwalteter Schlüssel für Azure

Beim Erstellen eines Maschinenkatalogs können Sie wählen, ob Daten auf den im Katalog bereitzustellenden Maschinen verschlüsselt werden sollen. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter

Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Ein Datenträgerverschlüsselungssatz (DES) repräsentiert einen vom Kunden verwalteten Schlüssel. Um das Feature zu nutzen, müssen Sie zuerst einen DES in Azure erstellen. Ein DES hat folgendes Format:

- /subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption

Wählen Sie einen DES aus der Liste aus. Der ausgewählte DES muss sich im selben Abonnement und in derselben Region wie Ihre Ressourcen befinden.

Wenn Sie einen Katalog mit einem Schlüssel erstellen und später den entsprechenden DES in Azure deaktivieren, können Sie die Maschinen im Katalog nicht mehr einschalten und diesem keine Maschinen mehr hinzufügen.

Weitere Informationen finden Sie unter Maschinenkatalog mit einem vom Kunden verwalteten Schlüssel erstellen.

### Azure-Datenträgerverschlüsselung auf dem Host

Sie können einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Sie können eine VM oder eine Vorlagenspezifikation als Eingabe für ein Maschinenprofil verwenden.

Bei diesem Verschlüsselungsverfahren werden Daten nicht über den Azure-Speicher verschlüsselt. Die Daten werden auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten.

**Einschränkungen:**

Die Azure-Datenträgerverschlüsselung auf dem Host:

- wird nicht für alle Azure-Maschinengrößen unterstützt.
- ist nicht kompatibel mit der Azure-Datenträgerverschlüsselung.

Weitere Informationen:

- Maschinenkatalog mit Verschlüsselung auf dem Host erstellen.
- Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen

### Doppelte Verschlüsselung auf verwalteten Datenträgern

Sie können einen Maschinenkatalog mit doppelter Verschlüsselung erstellen. Bei mit diesem Feature erstellten Katalogen werden alle Datenträger serverseitig mit plattformseitig und kundenseitig ver-

walteten Schlüsseln verschlüsselt. Sie besitzen und verwalten den Azure Key Vault, den Verschlüsselungsschlüssel und die Datenträgerverschlüsselungssätze (DES).

Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der vom Kunden verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt.

> **Hinweis:**
>
> - Sie können einen Maschinenkatalog mit doppelter Verschlüsselung über die Benutzeroberfläche für die vollständige Konfiguration und mit PowerShell-Befehlen erstellen und aktualisieren.
> - Sie können einen nicht auf Maschinenprofilen basierenden Workflow oder einen auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog mit doppelter Verschlüsselung zu erstellen oder zu aktualisieren.
> - Wenn Sie einen nicht auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog zu erstellen, können Sie die gespeicherte `DiskEncryptionSetId` wiederverwenden.
> - Wenn Sie ein Maschinenprofil verwenden, können Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

**Einschränkungen**

- Die doppelte Verschlüsselung wird für Ultra Disk- und Premium SSD v2-Datenträgern nicht unterstützt.
- Die doppelte Verschlüsselung wird für nicht verwaltete Datenträger nicht unterstützt.
- Wenn Sie den Schlüssel für einen Datenträgerverschlüsselungssatz deaktivieren, der mit einem Katalog verknüpft ist, werden die VMs des Katalogs deaktiviert.
- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Sie können maximal 50 Datenträgerverschlüsselungssätze pro Region und Abonnement erstellen.

Weitere Informationen finden Sie in den folgenden PowerShell-Themen:

- Maschinenkatalog mit doppelter Verschlüsselung erstellen
- Unverschlüsselten Katalog zur Verwendung der doppelten Verschlüsselung konvertieren
- Überprüfen, ob ein Katalog doppelt verschlüsselt ist

## Azure-Ressourcengruppen

Azure Provisioning-Ressourcengruppen sind eine Methode des Provisionings von VMs, über die Benutzern Anwendungen und Desktops bereitgestellt werden. Wenn Sie einen MCS-Maschinenkatalog erstellen, können Sie vorhandene, leere Azure-Ressourcengruppen hinzufügen oder neue erstellen. Informationen zu Azure-Ressourcengruppen finden Sie in der Dokumentation von Microsoft.

### Verwendung von Azure-Ressourcengruppen

Es gibt keine Beschränkung für die Anzahl der virtuellen Maschinen, verwalteten Datenträger, Snapshots und Images pro Azure-Ressourcengruppe. (Die Beschränkung auf 240 VMs pro 800 verwaltete Datenträger pro Azure-Ressourcengruppe wurde entfernt.)

- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit vollem Gültigkeitsbereich verwenden, erstellen die Maschinenerstellungsdienste nur eine Azure-Ressourcengruppe und verwenden nur diese Gruppe für den Katalog.
- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit eingeschränktem Gültigkeitsbereich verwenden, müssen Sie eine leere, vorab erstellte Azure-Ressourcengruppe für den Katalog angeben.

## Azure Marketplace

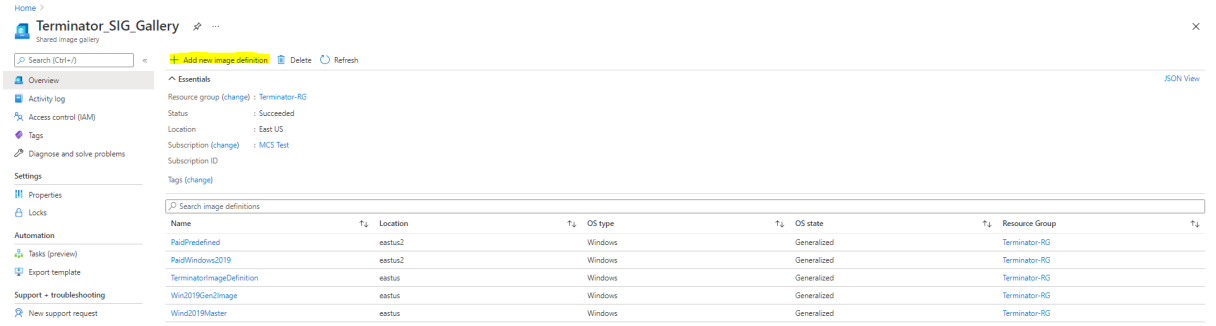
Citrix DaaS unterstützt die Verwendung eines Masterimages mit Abonnementinformationen zum Erstellen von Maschinenkatalogen in Azure. Weitere Informationen finden Sie unter Microsoft Azure Marketplace.

> **Tipp:**
>
> Manchen Images im Azure-Marketplace (z. B. Standard-Windows Server-Image) sind keine Abonnementinformationen angefügt. Das Citrix DaaS-Feature ist für kostenpflichtige Images vorgesehen.

### Das in der Azure Compute Gallery erstellte Image auf Azure-Abonnementinformationen überprüfen

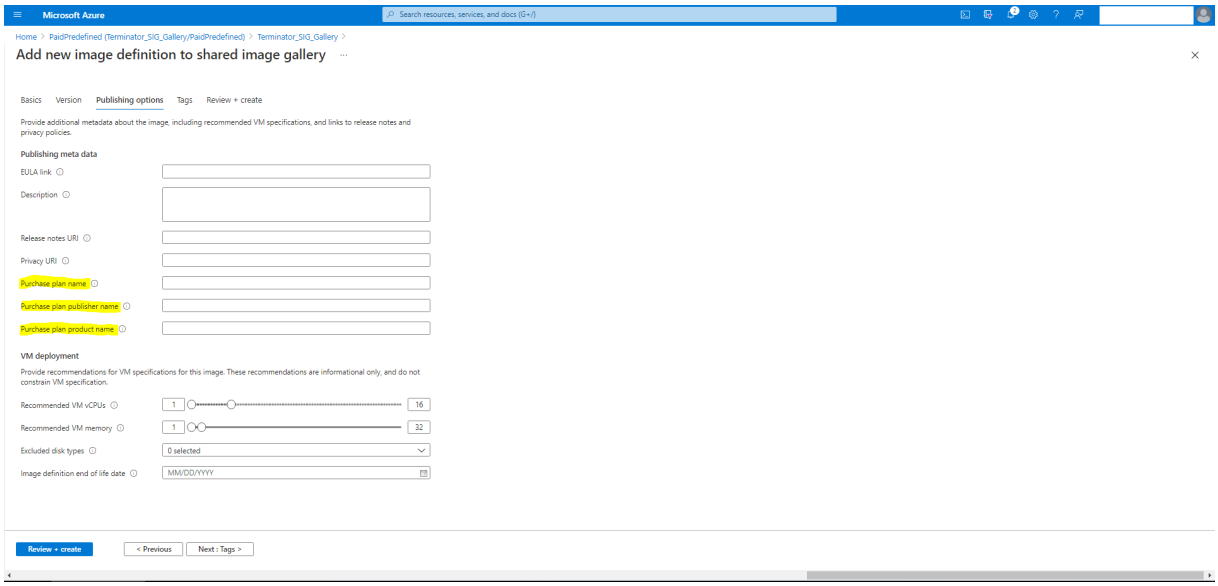
Gehen Sie wie in diesem Abschnitt beschrieben vor, um Images der Azure Compute Gallery in der Oberfläche für die vollständige Konfiguration anzuzeigen. Diese Images können für ein Masterimage verwendet werden. Um das Image in einer Azure Compute Gallery abzulegen, erstellen Sie in der Gallery eine Imagedefinition.



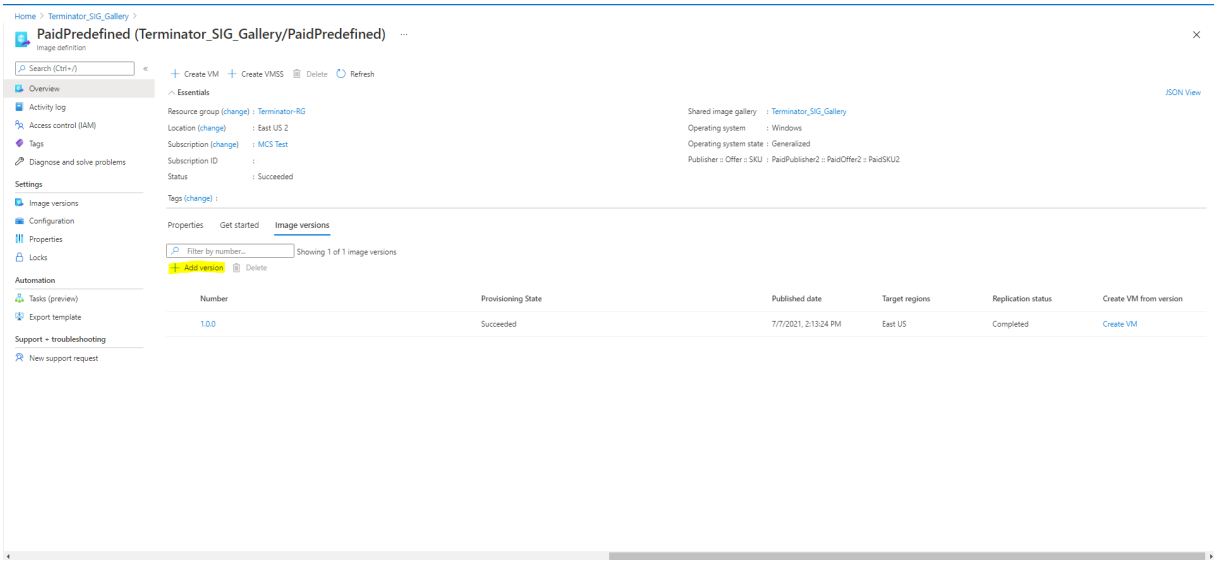

Überprüfen Sie auf der Seite **Veröffentlichungsoptionen** die Informationen zum Abonnement.

Die Informationsfelder sind zunächst leer. Füllen Sie diese Felder mit den Abonnementinformationen für das Image aus. Werden die Informationen nicht angegeben, kann der Maschinenkatalogprozess fehlschlagen.

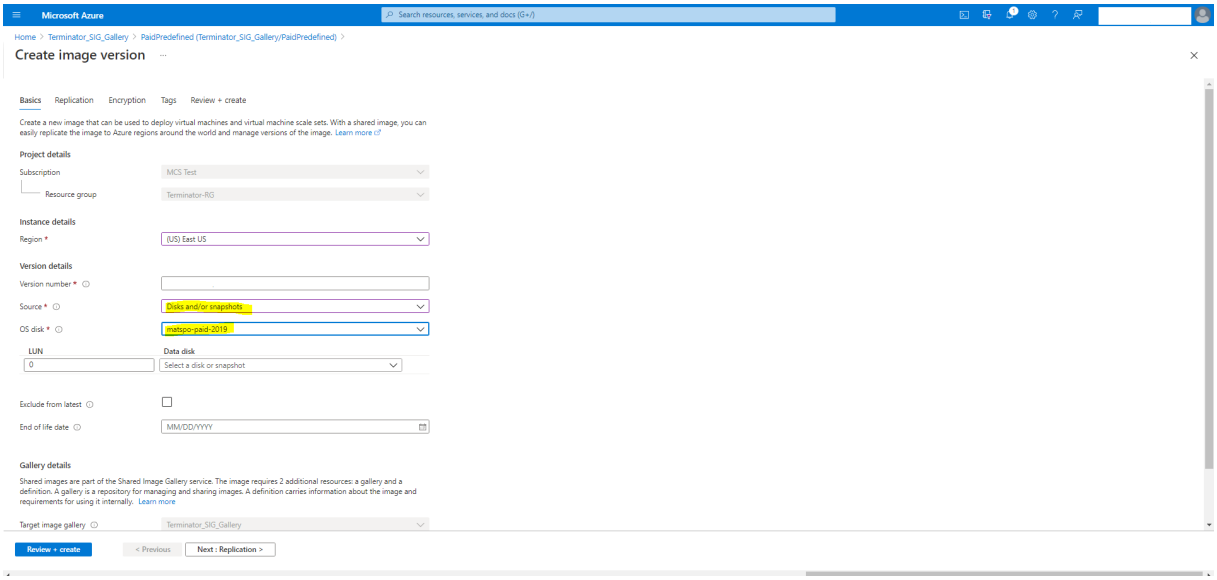



Nach dem Prüfen der Abonnementinformationen erstellen Sie eine Imageversion in der Definition. Diese wird als Masterimage verwendet. Klicken Sie auf **Add Version**:




Wählen Sie im Abschnitt **Version details** den Image-Snapshot oder verwalteten Datenträger als Quelle aus:




## Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent

Azure Monitoring ist ein Dienst, mit dem Sie Telemetriedaten aus Ihren Azure-und On-Premises-Umgebungen erfassen, analysieren und umsetzen können.

Azure Monitor Agent (AMA) sammelt Überwachungsdaten aus Rechenressourcen wie virtuellen Maschinen und übermittelt die Daten an Azure Monitor. Derzeit unterstützt der Dienst das Erfassen von Ereignisprotokollen sowie Syslog- und Leistungsmetriken, die dann an die Datenquellen Azure Monitor Metrics und Azure Monitor Logs gesendet werden.

Die Überwachung wird durch eindeutige Identifizierung der VMs in den Überwachungsdaten ermöglicht. Hierfür können Sie die VMs eines MCS-Maschinenkatalogs mit AMA als installierter Erweiterung bereitstellen.

**Anforderungen**

- Berechtigungen: Vergewissern Sie sich, dass Sie über die unter Informationen zu Azure-Berechtigungen angegebenen Azure-Mindestberechtigungen und über die folgenden Berechtigungen zur Verwendung von Azure Monitor verfügen:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Datensammlungsregel: Richten Sie eine Datensammlungsregel im Azure-Portal ein. Informationen zum Einrichten einer Datensammlungsregel finden Sie unter Create a data collection rule. Datensammlungsregeln sind plattformspezifisch (Windows oder Linux). Vergewissern Sie sich, dass Sie eine Datensammlungsregel gemäß der erforderlichen Plattform erstellen.
  AMA verwendet Datensammlungsregeln zum Verwalten der Zuordnung zwischen Ressourcen (wie VMs) und Datenquellen (wie Azure Monitor Metrics und Azure Monitor Logs).
- Standard-Workspace: Erstellen Sie einen Workspace im Azure-Portal. Informationen zum Erstellen eines Workspace finden Sie unter Create a Log Analytics workspace. Wenn Sie Protokolle und Daten sammeln, werden die Informationen in einem Workspace gespeichert. Ein Workspace hat eine eindeutige Workspace-ID und Ressourcen-ID. Der Workspace-Name muss für eine bestimmte Ressourcengruppe eindeutig sein. Nachdem Sie einen Workspace erstellt haben, konfigurieren Sie Datenquellen und Lösungen, um ihre Daten im Workspace zu speichern.
- Überwachungserweiterungen in Positivliste: Die Erweiterungen `AzureMonitorWindowsAgent` und `AzureMonitorLinuxAgent` sind von Citrix definierte Erweiterungen auf der Positivliste. Zur Anzeige der Erweiterungen auf der Positivliste verwenden Sie den PowerShell-Befehl `Get-ProvMetadataConfiguration`.
- Masterimage: Microsoft empfiehlt, Erweiterungen von einer vorhandenen Maschine zu entfernen, bevor eine neue Maschine damit erstellt wird. Wenn die Erweiterungen nicht entfernt werden, kann dies zu unerwartetem Verhalten durch verbliebene Dateien führen. Weitere Informationen finden Sie unter If the VM is recreated from an existing VM.

Informationen zum Erstellen eines Katalogs mit aktiviertem AMA mit PowerShell finden Sie unter Katalog-VMs mit aktiviertem AMA bereitstellen.

## Vertrauliche Azure-VMs

Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist.

Sie können MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

### Wichtige Überlegungen zu vertraulichen VMs

Im Hinblick auf unterstützte VM-Größen und die Erstellung von Maschinenkatalogen mit vertraulichen VMs gilt es, Folgendes zu beachten:

- Unterstützte VM-Größen:
  - DCasv5-Serie
  - DCadsv5-Serie
  - ECasv5-Serie
  - ECadsv5-Serie
- Erstellen von Maschinenkatalogen mit vertraulichen VMs.
  - Sie können Maschinenkataloge mit vertraulichen Azure-VMs mithilfe der Schnittstelle "Vollständige Konfiguration"und PowerShell-Befehlen erstellen.
  - Sie müssen einen maschinenprofilbasierten Workflow verwenden, um einen Maschinenkatalog mit vertraulichen Azure-VMs zu erstellen. Sie können eine VM oder eine Vorlagenspezifikation als Maschinenprofileingabe verwenden.
  - Für das Masterimage und das als Eingabe verwendete Maschinenprofil muss derselbe Sicherheitstyp aktiviert werden. Es gibt folgende Sicherheitstypen:
    * VMGuestStateOnly: Vertrauliche VM, bei der nur der VM-Gastzustand verschlüsselt ist
    * DiskWithVMGuestState: Vertrauliche VM, bei der sowohl der Betriebssystemdatenträger als auch der VM-Gastzustand mit einem plattformverwalteten oder einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Es können normale und auch kurzlebige Betriebssystemdatenträger verschlüsselt werden.
  - Über den Parameter "AdditionalData"können Sie Informationen zu vertraulichen VMs verschiedener Ressourcentypen, etwa verwaltete Datenträger, Snapshots, Azure Compute Gallery-Image, VM und ARM-Vorlagenspezifikation abrufen. Beispiel:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
    \image.folder\username-dev-testing-rg.resourcegroup\
    username-dev-tsvda.vm).AdditionalData
<!--NeedCopy-->
```

Es gibt folgende zusätzlichen Daten:

* DiskSecurityType
* ConfidentialVMDiskEncryptionSetId
* DiskSecurityProfiles

Führen Sie folgenden Befehl aus, um die Confidential Compute-Eigenschaft für eine Maschinengröße abzurufen: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

Das "additional data"-Feld ist `ConfidentialComputingType`.

- Sie können den Sicherheitstyp eines Masterimages oder eines Maschinenprofils nicht von "vertraulich"in "nicht vertraulich"oder umgekehrt ändern.
- Für jede falsche Konfiguration erhalten Sie eine entsprechende Fehlermeldung.

#### Masterimages und Maschinenprofile vorbereiten

Bevor Sie einen Satz vertraulicher VMs erstellen, gehen Sie wie folgt vor, um ein Masterimage und ein Maschinenprofil für sie vorzubereiten:

1. Erstellen Sie im Azure-Portal eine vertrauliche VM mit bestimmten Einstellungen wie:

   - **Sicherheitstyp**: Vertrauliche virtuelle Maschinen
   - **Vertrauliche Betriebssystem-Datenträgerverschlüsselung**: Aktiviert.
   - **Schlüsselverwaltung**: Vertrauliche Datenträgerverschlüsselung mit einem plattformverwalteten Schlüssel
     Weitere Informationen zum Erstellen vertraulicher VMs finden Sie in diesem Microsoft-Artikel.

2. Bereiten Sie das Masterimage auf der erstellten VM vor. Installieren Sie die erforderlichen Anwendungen und den VDA auf der erstellten VM.

   > **Hinweis:**
   >
   > Das Erstellen vertraulicher VMs mit VHD wird nicht unterstützt. Verwenden Sie stattdessen Azure Compute Gallery, verwaltete Datenträger oder Snapshots für diesen Zweck.

3. Erstellen Sie das Maschinenprofil auf eine der folgenden Arten:

- Verwenden Sie die in Schritt 1 erstellte vorhandene VM, wenn sie die erforderlichen Maschineneigenschaften besitzt.
- Wenn Sie sich für eine ARM-Vorlagenspezifikation als Maschinenprofil entscheiden, erstellen Sie die Vorlagenspezifikation wie erforderlich. Konfigurieren Sie insbesondere Parameter, die Ihre Anforderungen für vertrauliche VMs erfüllen, wie *SecurityEncryptionType* und *diskEncryptionSet* (für vom Kunden verwaltete Schlüssel). Weitere Informationen finden Sie unter Azure-Vorlagenspezifikation erstellen.

  > **Hinweis:**
  >
  > – Stellen Sie sicher, dass das Masterimage und das Maschinenprofil denselben Sicherheitsschlüsseltyp haben.
  > – Um vertrauliche virtuelle Maschinen zu erstellen, die eine vertrauliche Betriebssystem-Datenträgerverschlüsselung mit einem vom Kunden verwalteten Schlüssel erfordern, stellen Sie sicher, dass die IDs des Datenträgerverschlüsselungssatzes im Masterimage und im Maschinenprofil identisch sind.

#### Vertrauliche VMs mithilfe der vollständigen Konfiguration oder von PowerShell-Befehlen erstellen

Um eine Reihe vertraulicher VMs zu erstellen, erstellen Sie einen Maschinenkatalog mit einem Masterimage und einem Maschinenprofil, das von der gewünschten vertraulichen VM abgeleitet wurde.

Um den Katalog mit der vollständigen Konfiguration zu erstellen, folgen Sie den unter Maschinenkataloge erstellen beschriebenen Schritten. Beachten Sie die folgenden Überlegungen:

- Wählen Sie auf der Seite **Image** ein Masterimage und ein Maschinenprofil aus, das Sie für die Erstellung der vertraulichen VM vorbereitet haben. Die Auswahl des Maschinenprofils ist obligatorisch und es stehen nur Profile zur Auswahl, die den gleichen Sicherheitsverschlüsselungstyp wie das ausgewählte Masterimage haben.
- Auf der Seite **Virtuelle Maschinen** werden nur Maschinengrößen zur Auswahl angezeigt, die vertrauliche VMs unterstützen.
- Auf der Seite **Datenträgereinstellungen** können Sie den Datenträgerverschlüsselungssatz nicht angeben, da er vom ausgewählten Maschinenprofil übernommen wurde.

### PowerShell verwenden

In diesem Abschnitt wird beschrieben, wie Sie die folgenden Aufgaben mit PowerShell ausführen:

- Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

- Azure-VM-Erweiterungen aktivieren
- Maschinenkataloge mit vertrauenswürdigem Start
- Eigenschaftswerte für Maschinenprofile verwenden
- Verfügbarkeitszonen mit PowerShell konfigurieren
- VMs auf dedizierten Azure-Hosts bereitstellen
- Speichertypen konfigurieren
- Zonenredundanten Speicher aktivieren
- Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen
- Windows-Lizenz überprüfen
- Linux-Lizenz konfigurieren
- Maschinenkatalog mit kurzlebigem Azure-Datenträger erstellen
- Azure Compute Gallery konfigurieren
- Katalog mit mehreren Netzwerkkarten pro VM erstellen oder aktualisieren
- Maschinenkatalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen
- Maschinenkatalog mit persistentem Zurückschreibcachedatenträger erstellen
- Startleistung mit MCSIO verbessern
- Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen
- Maschinenkatalog mit Verschlüsselung auf dem Host erstellen
- Maschinenkatalog mit doppelter Verschlüsselung erstellen
- Speicherort der Auslagerungsdatei bestimmen
- Szenarien zum Einrichten der Auslagerungsdatei
- Auslagerungsdateieinstellung angeben
- Auslagerungsdateieinstellungen ändern
- Katalog-VMs mit aktiviertem AMA bereitstellen
- Katalog mit Azure Spot-VMs erstellen
- Tags in allen Ressourcen kopieren

### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Sie können hierfür die Schnittstelle Vollständige Konfiguration oder PowerShell verwenden.

Informationen zur Benutzeroberfläche für die vollständige Konfiguration finden Sie unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.

Mit PowerShell:

1. Öffnen Sie das **PowerShell**-Fenster.

2. Führen Sie `asnp citrix*` aus.
3. Erstellen oder aktualisieren Sie einen Katalog.

   - Gehen Sie zum Erstellen eines Katalogs wie folgt vor:

     a) Verwenden Sie den Befehl `New-ProvScheme` mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

     ```
     New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
         image.folder/fgthj.resourcegroup/nab-ws-
         vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/test.templatespec/V1.
         templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     b) Beenden Sie die Erstellung des Maschinenkatalogs.

   - Verwenden Sie zum Aktualisieren eines Katalogs den Befehl `Set-ProvScheme` mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

     ```
     Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
         Us.region/vm.folder/MasterDisk.vm'
     MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/testing.templatespec/V1.
         templatespecversion'
     [-ProvisioningSchemeName] <String>
     [-CustomProperties <String>][-ServiceOffering <String>] [-
         PassThru]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

### Azure-VM-Erweiterungen aktivieren

Führen Sie nach Auswahl der ARM-Vorlagenspezifikation die folgenden PowerShell-Befehle aus, um Azure-VM-Erweiterungen zu verwenden:

- Anzeige der Liste der unterstützten Azure VM-Erweiterungen: `Get-ProvMetadataConfiguration`

- Hinzufügen von zusätzlichen VM-Erweiterungen: `Add-ProvMetadataConfiguration`. Zum Beispiel: `Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  Beim Versuch, eines der folgenden Elemente hinzuzufügen, wird eine Fehlermeldung angezeigt:

  - Von Citrix definierte Erweiterung.
  - Vorhandene benutzerdefinierte Erweiterung.
  - Nicht unterstützte Konfigurationsschlüssel. Derzeit ist der unterstützte Konfigurationsschlüssel `Extension`.

- Entfernen von Erweiterungen aus der Liste: `Remove-ProvMetadataConfiguration`. Sie können die selbst hinzugefügten Erweiterungen entfernen.

### Maschinenkataloge mit vertrauenswürdigem Start

Zur problemlosen Erstellung eines Maschinenkatalogs mit vertrauenswürdigem Start verwenden Sie:

- Ein Maschinenprofil mit vertrauenswürdigem Start
- Eine VM-Größe, die vertrauenswürdigen Start unterstützt
- Eine Windows-VM-Version, die vertrauenswürdigen Start unterstützt. Derzeit unterstützen Windows 10, Windows 11, Windows Server 2016, 2019 und 2022 den vertrauenswürdigen Start.

> **Wichtig:**
>
> MCS unterstützt die Erstellung eines neuen Katalogs mit VMs, für die vertrauenswürdiger Start aktiviert ist. Um einen vorhandenen persistenten Katalog und vorhandene VMs zu aktualisieren, müssen Sie jedoch das Azure-Portal verwenden. Sie können den vertrauenswürdigen Start eines nicht persistenten Katalogs nicht aktualisieren. Weitere Informationen finden Sie im Microsoft-Dokument Enable Trusted launch on existing Azure VMs.

Führen Sie den folgenden Befehl aus, um den Bestand des Citrix DaaS-Angebots anzuzeigen und zu ermitteln, ob die VM-Größe den vertrauenswürdigen Start unterstützt:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den folgenden Befehl aus:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
   .folder"<VM size>".serviceoffering)
<!--NeedCopy-->
```

4. Führen Sie `$s | select -ExpandProperty Additionaldata` aus.
5. Prüfen Sie den Wert des Attributs `SupportsTrustedLaunch`.
   - Wenn `SupportsTrustedLaunch` **True** ist, unterstützt die VM-Größe den vertrauenswürdigen Start.

- Wenn `SupportsTrustedLaunch` **False**ist, unterstützt die VM-Größe den vertrauenswürdigen Start nicht.

Bei Azure-PowerShell können Sie den folgenden Befehl verwenden, um die VM-Größen zu ermitteln, die den vertrauenswürdigen Start unterstützen:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Die folgenden Beispiele veranschaulichen, welche von dem Azure PowerShell-Befehl zurückgegebenen VMs den vertrauenswürdigen Start unterstützen.

- *Beispiel 1*: Wenn die Azure-VM nur Generation 1 unterstützt, unterstützt die VM keinen vertrauenswürdigen Start. Daher wird `TrustedLaunchDisabled` nicht angezeigt, wenn Sie den Azure PowerShell-Befehl ausgeführt haben.
- *Beispiel 2*: Wenn die Azure-VM nur Generation 2 unterstützt und der Wert von `TrustedLaunchDisabled` **True** ist, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start nicht.
- *Beispiel 3*: Wenn die Azure-VM nur Generation 2 unterstützt und `TrustedLaunchDisabled` nicht angezeigt wird, wenn Sie den PowerShell-Befehl ausgeführt haben, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start.

Weitere Informationen zum vertrauenswürdigen Start für virtuelle Azure-Maschinen finden Sie in dem Microsoft-Dokument Vertrauenswürdiger Start für Azure-VMs.

#### Maschinenkatalog mit vertrauenswürdigem Start erstellen

1. Erstellen Sie ein Masterimage, für das vertrauenswürdiger Start aktiviert ist. Weitere Informationen finden Sie in der Microsoft-Dokumentation Unterstützte Images für VMs mit vertrauenswürdigem Start.
2. Erstellen Sie eine VM oder Vorlagenspezifikation mit Sicherheitstyp als **virtuelle Maschinen mit vertrauenswürdigem Start**. Weitere Informationen zum Erstellen einer VM oder Vorlagenspezifikation finden Sie im Microsoft-Dokument Bereitstellen eines virtuellen Computers mit vertrauenswürdigem Start.
3. Erstellen Sie einen Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration oder von PowerShell-Befehlen.

   - Wenn Sie die Benutzeroberfläche für die vollständige Konfiguration nutzen möchten, finden Sie weitere Informationen unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.

- Wenn Sie PowerShell-Befehle verwenden möchten, verwenden Sie den Befehl `New-ProvScheme` mit der VM oder Vorlagenspezifikation als Maschinenprofileingabe. Eine vollständige Liste der Befehle zum Erstellen eines Katalogs finden Sie unter Erstellen eines Katalogs.

  Beispiel für `New-ProvScheme` mit VM als Maschinenprofileingabe:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
    folder<def.resourcegroup><machine profile vm.vm>"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

  Beispiel für `New-ProvScheme` mit Vorlagenspezifikation als Maschinenprofileingabe:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

### Fehler beim Erstellen von Maschinenkatalogen mit vertrauenswürdigem Start

Beim Erstellen eines Maschinenkatalogs mit vertrauenswürdigem Start treten in den folgenden Szenarien Fehler auf:

| Szenario | Fehler |
| --- | --- |
| Sie wählen beim Erstellen eines nicht verwalteten Katalogs ein Maschinenprofil aus. | `MachineProfileNotSupportedForUnmanagedCata` |

| Szenario | Fehler |
| --- | --- |
| Sie wählen beim Erstellen eines Katalogs mit einem nicht verwalteten Datenträger als Masterimage ein Maschinenprofil, das den vertrauenswürdigen Start unterstützt. | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Sie wählen beim Erstellen eines verwalteten Katalogs mit einer Masterimagequelle, deren Sicherheitstyp “vertrauenswürdiger Start”ist, kein Maschinenprofil aus. | `MachineProfileNotFoundForTrustedLaunchMaste` |
| Sie wählen ein Maschinenprofil aus, dessen Sicherheitstyp sich von dem des Masterimages unterscheidet. | `SecurityTypeConflictBetweenMasterImageAndMa` |
| Sie wählen eine VM-Größe, die den vertrauenswürdigen Start nicht unterstützt, verwenden aber beim Erstellen eines Katalogs ein Masterimage, das den vertrauenswürdigen Start unterstützt. | `MachineSizeNotSupportTrustedLaunch` |

### Eigenschaftswerte für Maschinenprofile verwenden

Der Maschinenkatalog verwendet die folgenden Eigenschaften, die in den benutzerdefinierten Eigenschaften definiert sind:

- Verfügbarkeitszone
- ID der dedizierten Hostgruppe
- ID des Datenträgerverschlüsselungssatzes
- Betriebssystemtyp
- Lizenztyp
- Speichertyp

Wenn diese benutzerdefinierten Eigenschaften nicht explizit definiert sind, werden die Eigenschaftswerte über die ARM-Vorlagenspezifikation oder VM festgelegt, je nachdem, was als Maschinenprofil verwendet wird. Wenn `ServiceOffering` nicht angegeben ist, wird der Wert über das Maschinenprofil festgelegt.

> **Hinweis:**
>
> Wenn einige der Eigenschaften im Maschinenprofil fehlen und nicht in den benutzerdefinierten

> Eigenschaften definiert sind, werden die Standardwerte der Eigenschaften angewendet, soweit zutreffend.

Im folgenden Abschnitt werden einige Szenarios für `New-ProvScheme` und `Set-ProvScheme` beschrieben, wenn für `CustomProperties` entweder alle Eigenschaften definiert sind oder Werte aus dem MachineProfile abgeleitet werden.

- New-ProvScheme-Szenarios
  - Im MachineProfile sind alle Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    ```
    Get-ProvScheme | select CustomProperties
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
    <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
       -value>"/>
    <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
       " Value="<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="
       DedicatedHostGroupId" Value="<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
       value>"/>
    </CustomProperties>
    <!--NeedCopy-->
    ```

  - Im MachineProfile sind einige Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel: Im MachineProfile sind nur LicenseType und OsType festgelegt.

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    ```
    Get-ProvScheme | select CustomProperties
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
    ```

```
3   <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
       -value>"/>
4   <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpA-value>"/>
5   </CustomProperties>
6   <!--NeedCopy-->
```

- Sowohl im MachineProfile als auch in CustomProperties sind alle Eigenschaften definiert. Beispiel:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Benutzerdefinierte Eigenschaften haben Priorität. Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  ```
  1   Get-ProvScheme | select CustomProperties
  2   <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
         machinecreation" xmlns:xsi="http://www.w3.org/2001/
         XMLSchema-instance">
  3   <Property xsi:type="StringProperty" Name="StorageAccountType"
          Value="<CustomPropertiesA-value>"/>
  4   <Property xsi:type="StringProperty" Name="OSType" Value="<
         CustomPropertiesA-value>"/>
  5   <Property xsi:type="StringProperty" Name="LicenseType" Value=
         "<CustomPropertiesA-value>"/>
  6   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
         " Value="<CustomPropertiesA-value>"/>
  7   <Property xsi:type="StringProperty" Name="
         DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  8   <Property xsi:type="StringProperty" Name="Zones" Value="<
         CustomPropertiesA-value>"/>
  9   </CustomProperties>
  10  <!--NeedCopy-->
  ```

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Beispiel:

  * CustomProperties definieren LicenseType und StorageAccountType
  * MachineProfile definiert LicenseType, OsType und Zonen

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  ```
  1   Get-ProvScheme | select CustomProperties
  ```

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
    -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Darüber hinaus ist ServiceOffering nicht definiert. Beispiel:
  - CustomProperties definieren StorageType
  - MachineProfile definiert LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
    serviceoffering.folder<explicit-machine-size>.
    serviceoffering"
<!--NeedCopy-->
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- Wenn der OsType weder in CustomProperties noch im MachineProfile definiert ist, gilt Folgendes:
  - Der Wert wird aus dem Masterimage gelesen.
  - Ist das Masterimage ein nicht verwalteter Datenträger, ist der OsType auf Windows eingestellt. Beispiel:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
```

```
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

Der Wert aus dem Masterimage wird in die benutzerdefinierten Eigenschaften geschrieben, in diesem Fall Linux.

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="
      Linux"/>
4  </CustomProperties>
5  <!--NeedCopy-->
```

- Set-ProvScheme-Szenarios
  - Ein vorhandener Katalog mit:
    - CustomProperties für `StorageAccountType` und OsType
    - MachineProfile `mpA.vm`, das Zonen definiert
  - Updates:
    - MachineProfile mpB.vm, das StorageAccountType definiert
    - Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der LicenseType und OsType definiert

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6       </CustomProperties>
7  <!--NeedCopy-->
```

  - Ein vorhandener Katalog mit:

    * CustomProperties für `StorageAccountType` und OsType
    * MachineProfile `mpA.vm`, das StorageAccountType und LicenseType definiert

- Updates:

    * Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der StorageAccountType und OsType definiert.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
    CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mp-A-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Ein vorhandener Katalog mit:

    * CustomProperties für `StorageAccountType` und OsType
    * MachineProfile `mpA.vm`, das Zonen definiert

- Updates:

    * Ein MachineProfile mpB.vm, das StorageAccountType und LicenseType definiert
    * `ServiceOffering` ist nicht angegeben

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.
    serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<mpB-value>"/>
```

```
<Property xsi:type="StringProperty" Name="OSType" Value="<
    prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

### Verfügbarkeitszonen mit PowerShell konfigurieren

Mit `Get-Item` in PowerShell können Sie die Elemente des Citrix DaaS-Angebots anzeigen. Um beispielsweise das *Serviceangebot Eastern US* `Standard_B1ls` anzuzeigen:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
    name\East US.region\serviceoffering.folder\Standard_B1ls.
    serviceoffering"
<!--NeedCopy-->
```

Zum Anzeigen der Zonen verwenden Sie den Parameter `AdditionalData`:

```
$serviceOffering.AdditionalData
```

Werden keine Verfügbarkeitszone angegeben, bleibt die Art und Weise, wie Maschinen bereitgestellt werden, unverändert.

Um Verfügbarkeitszonen über PowerShell zu konfigurieren, verwenden Sie die benutzerdefinierte Eigenschaft **Zones** von `New-ProvScheme`. Die Eigenschaft **Zones** definiert eine Liste von Verfügbarkeitszonen für das Provisioning von Maschinen. Diese Zonen können eine oder mehrere Verfügbarkeitszonen enthalten. Beispiel: `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` für die Zonen 1 und 3.

Verwenden Sie den Befehl `Set-ProvScheme`, um die Zonen für ein Provisioningschema zu aktualisieren.

Wird eine ungültige Zone angegeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung mit Anweisungen zur Korrektur des ungültigen Befehls angezeigt.

> **Tipp:**
>
> Wenn Sie eine ungültige benutzerdefinierte Eigenschaft angeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung angezeigt.

#### Ergebnis der gleichzeitigen Verwendung von Hostgruppen- und Azure-Verfügbarkeitszonen

Sie können im Voraus überprüfen, ob ein Maschinenkatalog mit der in der benutzerdefinierten Eigenschaft angegebenen Verfügbarkeitszone und der Zone der Hostgruppe erstellt werden kann. Die Katalogerstellung schlägt fehl, wenn die Verfügbarkeitszone der benutzerdefinierten Eigenschaft nicht mit der Hostgruppenzone übereinstimmt.

Informationen zum Konfigurieren von Verfügbarkeitszonen über PowerShell finden Sie unter Konfigurieren von Verfügbarkeitszonen über PowerShell.

Informationen zu dedizierten Azure-Hosts finden Sie unter Dedizierte Azure-Hosts.

Die folgende Tabelle beschreibt die verschiedenen Kombinationen aus Verfügbarkeits- und Hostgruppenzone und zeigt an, wann die Maschinenkatalogerstellung gelingt bzw. fehlschlägt.

| Hostgruppenzone | Verfügbarkeitszone in benutzerdefinierter Eigenschaft | Ergebnis der Maschinenkatalogerstellung |
|---|---|---|
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Nicht angegeben | Erfolgreich. Maschinen werden in der Hostgruppenzone erstellt. |
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Mit Hostgruppenzone identisch. Die Zone in der benutzerdefinierten Eigenschaft ist beispielsweise auf 1 festgelegt. | Erfolgreich. Maschinen werden in Zone 1 erstellt. |
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Nicht mit Hostgruppenzone identisch. Die Zone in der benutzerdefinierten Eigenschaft ist beispielsweise auf 2 festgelegt. | Da Verfügbarkeitszone und Hostgruppenzone nicht übereinstimmen, schlägt die Katalogerstellung bei der Vorabprüfung aufgrund eines relevanten Fehlers fehlt. |
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Es sind mehrere Zonen festgelegt. Beispielsweise sind Zonen in den benutzerdefinierten Eigenschaften auf 1,2 oder 2,3 festgelegt. | Da Verfügbarkeitszone und Hostgruppenzone nicht übereinstimmen, schlägt die Katalogerstellung bei der Vorabprüfung aufgrund eines relevanten Fehlers fehlt. |
| Nicht festgelegt. Die Zone der Hostgruppe ist beispielsweise None. | Nicht angegeben | Wenn die festgelegte Verfügbarkeitszone mit der Hostgruppenzone übereinstimmt (d. h. keine Zone), ist die Katalogerstellung erfolgreich. Maschinen werden in keiner Zone erstellt. |

| Hostgruppenzone | Verfügbarkeitszone in benutzerdefinierter Eigenschaft | Ergebnis der Maschinenkatalogerstellung |
|---|---|---|
| Nicht festgelegt. Die Zone der Hostgruppe ist beispielsweise `None`. | Festgelegt. Beispielsweise sind die Zonen in der benutzerdefinierten Eigenschaft auf eine oder mehrere Zonen festgelegt. | Da Verfügbarkeitszone und Hostgruppenzone nicht übereinstimmen, schlägt die Katalogerstellung bei der Vorabprüfung aufgrund eines relevanten Fehlers fehlt |

### VMs auf dedizierten Azure-Hosts bereitstellen

Sie können mit MCS das Provisioning von VMs auf dedizierten Azure-Hosts ausführen. Vor dem Provisioning von VMs auf dedizierten Azure-Hosts führen Sie folgende Schritte aus:

- Erstellen Sie eine Hostgruppe.
- Erstellen Sie Hosts in der Hostgruppe.
- Vergewissern Sie sich, dass genügend Hostkapazität für die Erstellung von Katalogen und virtuellen Maschinen reserviert ist.

Sie können einen Katalog mit Maschinen erstellen, deren Host-Tenancy über das folgende PowerShell-Skript definiert wird:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

Wenn Sie mit MCS virtuelle Maschinen auf dedizierten Azure-Hosts bereitstellen, berücksichtigen Sie Folgendes:

- Ein *dedizierter Host* ist eine Katalogeigenschaft und kann nach der Katalogerstellung nicht mehr geändert werden. Dedizieren für Mandanten wird derzeit in Azure nicht unterstützt.
- Bei Verwendung des Parameters `HostGroupId` ist eine vorkonfigurierte Azure-Hostgruppe in der Region der Hostingeinheit erforderlich.
- Die automatische Platzierung in Azure ist erforderlich. Das Feature beantragt das Onboarding des mit der Hostgruppe verknüpften Abonnements. Weitere Informationen finden Sie unter VM Scale Set on Azure Dedicated Hosts - Public Preview. Wenn die automatische Platzierung nicht aktiviert ist, tritt in MCS bei der Katalogerstellung ein Fehler auf.

### Speichertypen konfigurieren

Wählen Sie Speichertypen für virtuelle Maschinen in Azure-Umgebungen, die MCS verwenden. Für Ziel-VMs unterstützt MCS Folgendes:

- OS-Datenträger: SSD Premium, SSD oder HDD
- Zurückschreibcache-Datenträger: SSD Premium, SSD oder HDD

Berücksichtigen Sie bei Verwendung dieser Speichertypen Folgendes:

- Ihre VM muss den ausgewählten Speichertyp unterstützen.
- Wenn Ihre Konfiguration einen kurzlebigen Azure-Datenträger enthält, wird keine Option für die Einstellung des Zurückschreibcache-Datenträgers angeboten.

> **Tipp:**
>
> `StorageType` ist für einen Betriebssystemspeichertyp und mit Speicherkonto konfiguriert. `WBCDiskStorageType` ist für den Zurückschreibcache konfiguriert. Für einen normalen Katalog ist `StorageType` erforderlich. Wenn `WBCDiskStorageType` nicht konfiguriert ist, wird `StorageType` als Standard für `WBCDiskStorageType` verwendet.

Wenn WBCDiskStorageType nicht konfiguriert ist, wird StorageType als Standard für WBCDiskStorageType verwendet.

#### Speichertypen für VMs konfigurieren

Verwenden Sie den Parameter `StorageType` in `New-ProvScheme`, um Speichertypen für VMs zu konfigurieren. Verwenden Sie den `Set-ProvScheme`-Befehl, um den Wert des `StorageType` -Parameters in einem bestehenden Katalog auf einen der unterstützten Speichertypen zu aktualisieren.

Im Folgenden finden Sie einen Beispielsatz für den Parameter `CustomProperties` in einem Provisioningschema:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```

### Zonenredundanten Speicher aktivieren

Sie können bei der Katalogerstellung einen zonenredundanten Speicher (ZRS) auswählen. Ihre Azure Managed Disk wird dann synchron über mehrere Verfügbarkeitszonen repliziert, sodass Sie Ihre Daten bei einem Ausfall in einer Zone mithilfe der Redundanz in den übrigen Zonen wiederherstellen können.

In den benutzerdefinierten Speichertypeigenschaften können Sie **Premium_ZRS** und **Standard-SSD_ZRS** angeben. Der ZRS-Speicher kann mithilfe vorhandener benutzerdefinierter Eigenschaften oder über die Vorlage **MachineProfile** festgelegt werden. Der ZRS-Speicher wird auch mit dem Befehle `Set-ProvVMUpdateTimeWindow` und den Parametern `-StartsNow` und `-DurationInMinutes -1` unterstützt. Sie können bestehende VMs von LRS- auf ZRS-Speicher umstellen.

> **Hinweis:**
>
> - `StartsNow` gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
> - `DurationInMinutes` mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

**Einschränkungen:**

- Nur für verwaltete Datenträger unterstützt
- Nur mit Premium- und Standard-SSDs unterstützt
- Keine Unterstützung mit `StorageTypeAtShutdown`
- Nur in bestimmten Regionen verfügbar.
- Beim Erstellen großer Mengen an ZRS-Datenträgern sinkt die Leistung von Azure. Fahren Sie die Maschinen daher beim ersten Einschalten gestaffelt hoch (weniger als 300 Maschinen gleichzeitig).

#### Zonenredundanten Speicher als Datenträgerspeichertyp festlegen

Sie können einen zonenredundanten Speicher bei der Katalogerstellung auswählen oder den Speichertyp in einem vorhandenen Katalog aktualisieren.

#### Zonenredundanten Speicher mithilfe von PowerShell-Befehlen auswählen

Wenn Sie einen neuen Katalog in Azure mit dem Powershell-Befehl `New-ProvScheme` erstellen, verwenden Sie für `StorageAccountType` den Wert `Standard_ZRS`.
Beispiel:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

Nach Auswahl dieses Werts prüft eine dynamische API, ob er ordnungsgemäß verwendet werden kann. Folgende Ausnahmen können auftreten, wenn ZRS für Ihren Katalog nicht zulässig ist:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: Die benutzerdefinierte Eigenschaft "StorageTypeAtShutdown"kann nicht mit ZRS verwendet werden.
- **StorageAccountTypeNotSupportedInRegion**: Diese Ausnahme tritt auf, wenn Sie versuchen, ZRS in einer nicht unterstützten Azure-Region zu verwenden.
- **ZrsRequiresManagedDisks**: Sie können zonenredundanten Speicher nur mit verwalteten Datenträgern verwenden.

Sie können den Datenträgerspeichertyp mit den folgenden benutzerdefinierten Eigenschaften festlegen:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Hinweis:**
>
> Bei der Katalogerstellung wird der Betriebssystemdatenträger `StorageType` des Maschinenprofils verwendet, wenn die benutzerdefinierten Eigenschaften nicht festgelegt sind.

### Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen

Sie können Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen, während Sie einen Maschinenkatalog erstellen, einen vorhandenen Maschinenkatalog aktualisieren und vorhandene VMs aktualisieren.

Sie können eine VM- oder Vorlagenspezifikation als Maschinenprofilquelle erstellen.

#### Wichtige Schritte

1. Richten Sie die erforderlichen IDs in Azure ein. Sie müssen diese IDs in der Vorlagenspezifikation angeben.
    - Speicherkonto
    - Protokollanalysen-Workspace
    - Event Hub-Namespace mit den Standardtarifpreisen

2. Erstellen Sie eine Maschinenprofilquelle.
3. Erstellen Sie einen neuen Maschinenkatalog, aktualisieren Sie einen vorhandenen Katalog oder aktualisieren Sie vorhandene VMs.

#### Erforderliche IDs in Azure einrichten

Richten Sie eine der folgenden Optionen in Azure ein:

- Speicherkonto
- Protokollanalysen-Workspace
- Event Hub-Namespace mit den Standardtarifpreisen

**Speicherkonto einrichten** Erstellen Sie ein Standardspeicherkonto in Azure. Geben Sie in der Vorlagenspezifikation die vollständige Resourcen-ID für das Speicherkonto als `storageAccountId` an.

Sobald VMs so eingerichtet sind, dass sie Daten im Speicherkonto protokollieren, finden Sie die Daten unter dem Container `insights-metrics-pt1m`.

**Workspace für Protokollanalysen einrichten** Erstellen Sie einen Workspace für Protokollanalysen. Geben Sie in der Vorlagenspezifikation die vollständige Ressourcen-ID für den Protokollanalysen-Workspace als workspaceId an.

Sobald VMs so eingerichtet sind, dass sie Daten im Workspace protokollieren, können Daten unter “Protokolle”in Azure abgefragt werden. Sie können den folgenden Befehl in Azure unter “Protokolle” ausführen, um die Anzahl aller von einer Ressource protokollierten Metriken anzuzeigen:

‘AzureMetrics
| summarize Count=count() by ResourceId# Microsoft Azure-Katalog erstellen

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Microsoft Azure-Katalog erstellen, müssen Sie eine Verbindung zu Microsoft Azure hergestellt haben. Siehe Verbindung zu Microsoft Azure.

### Maschinenkatalog erstellen

Sie können einen Maschinenkatalog auf zweierlei Art erstellen:

- Benutzeroberfläche für die vollständige Konfiguration.
- PowerShell. Weitere Informationen finden Sie unter Citrix DaaS mit Remote PowerShell SDKs verwalten. Informationen zur Implementierung bestimmter Funktionen mit PowerShell finden Sie unter PowerShell verwenden.

### Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen

Diese Informationen ergänzen die Anleitungen unter Erstellen von Maschinenkatalogen.

Ein Image kann ein Datenträger, ein Snapshot oder eine Imageversion einer Imagedefinition in Azure Compute Gallery sein, das zum Erstellen der VMs in einem Maschinenkatalog verwendet wird.

Erstellen Sie vor dem Erstellen des Maschinenkatalogs ein Image in Azure Resource Manager.

> **Hinweis:**
>
> - Das VM-Provisioning mit nicht verwalteten Datenträgern wird nicht länger unterstützt.
> - Die Unterstützung für die Verwendung eines Masterimages aus einer anderen Region als der in der Hostverbindung konfigurierten Region ist veraltet. Verwenden Sie Azure Compute Gallery, um das Masterimage in die gewünschte Region zu replizieren.

Während der Imagevorbereitung wird eine virtuelle Vorbereitungsmaschine (Vorbereitungs-VM) basierend auf der ursprünglichen VM erstellt. Diese Vorbereitungs-VM ist vom Netzwerk getrennt. Zum Trennen des Netzwerks von der Vorbereitungs-VM wird eine Netzwerksicherheitsgruppe erstellt, um den gesamten eingehenden und ausgehenden Datenverkehr zu blockieren. Die Netzwerksicherheitsgruppe wird automatisch einmal pro Katalog erstellt. Der Name der Netzwerksicherheitsgruppe lautet <!JEKYLL@5180@0>, wobei die GUID nach dem Zufallsprinzip generiert wird. Beispiel: <!JEKYLL@5180@1>.

Assistent für die Maschinenkatalogerstellung:

1. Die Seiten **Maschinentyp** und **Maschinenverwaltung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.

2. Wählen Sie auf der Seite **Image** das Image, das Sie als Masterimage für alle Maschinen im Katalog verwenden möchten. Der **Assistent zur Imageauswahl** wird angezeigt. Gehen Sie wie folgt vor, um ein Image auszuwählen:

   a) (Gilt nur für Verbindungen mit innerhalb oder zwischen Mandanten freigegebenen Images) Wählen Sie das Abonnement, in dem sich das Image befindet.
   b) Wählen Sie eine Ressourcengruppe.
   c) Gehen Sie zur Azure Managed Disks, zur Azure Compute Gallery oder zur Azure-Imageversion.

   Beachten Sie bei der Imageauswahl Folgendes:

   - Vergewissern Sie sich, dass ein Citrix VDA auf dem Image installiert ist.
   - Wenn Sie einen Datenträger auswählen, der an eine VM angeschlossen ist, müssen Sie die VM herunterfahren, bevor Sie mit dem nächsten Schritt fortfahren.

   > **Hinweis:**
   >
   > - Das Abonnement, das der Verbindung (Host) entspricht, die die Maschinen im Katalog erstellt hat, ist mit einem grünen Punkt gekennzeichnet. Bei den anderen Abonnements handelt es sich um diejenigen, die die Azure Compute Gallery mit diesem Abonnement teilen. In diesen Abonnements werden nur geteilte Kataloge angezeigt. Informationen zur Konfiguration freigegebener Abonnements finden Sie unter Images innerhalb eines Mandanten freigeben (abonnementübergreifend) und Images mandantenübergreifend freigeben.
   > - Sie können ein Provisioningschema mit einem kurzlebigen Betriebssystemdatenträger unter Windows mit vertrauenswürdigem Start erstellen. Wenn Sie ein Image mit vertrauenswürdigem Start auswählen, müssen Sie ein Maschinenprofil mit vertrauenswürdigem Start auswählen, das mit vTPM aktiviert ist. Informationen zum Erstellen von Maschinenkatalogen mit kurzlebigem Betriebssystemdatenträger finden Sie unter Erstellen von Maschinen mit kurzlebigem Betriebssystemdatenträger.
   > - Während der Imagereplikation können Sie das Image als Masterimage auswählen und das Setup abschließen. Die Katalogerstellung kann jedoch länger dauern, während das Image repliziert wird. MCS erfordert, dass die Replikation innerhalb einer Stunde ab Katalogerstellung abgeschlossen ist. Tritt bei der Replikation ein Timeout auf, schlägt die Katalogerstellung fehl. Sie können den Replikationsstatus in Azure überprüfen. Versuchen Sie es erneut, wenn die Replikation noch aussteht oder nach dem Abschluss der Replikation.
   > - Sie können einen VM-Katalog der zweiten Generation mithilfe eines Images der zweiten Generation bereitstellen, um die Startzeitleistung zu verbessern. Das Er-

> stellen eines Maschinenkatalogs der zweiten Generation mit einem Image der ersten Generation wird nicht unterstützt. Das Erstellen eines Maschinenkatalogs der ersten Generation mit einem Image der zweiten Generation wird ebenfalls nicht unterstützt. Außerdem werden ältere Images ohne Generationsangabe als Image der ersten Generation behandelt.

Wählen Sie aus, ob virtuelle Maschinen im Katalog die Konfigurationen eines Maschinenprofils übernehmen sollen. Standardmäßig ist das Kontrollkästchen **Maschinenprofil verwenden (obligatorisch für Azure Active Directory)** aktiviert. Klicken Sie auf **Wählen Sie ein Maschinenprofil**, um eine VM- oder ARM-Vorlagenspezifikation aus einer Liste mit Ressourcengruppen auszuwählen.

Beispiele für Konfigurationen, die VMs von einem Maschinenprofil übernehmen können:

- Beschleunigtes Netzwerk
- Startdiagnose
- Caching des Hostdatenträgers (bei OS- und MCSIO-Datenträgern)
- Maschinengröße (sofern nicht anders angegeben)
- Für VM platzierte Tags

> **Hinweis:**
>
> - Wenn Sie ein Masterimage für Maschinenkataloge in Azure auswählen, wird das Maschinenprofil auf der Grundlage des ausgewählten Masterimages gefiltert. Beispielsweise wird das Maschinenprofil basierend auf dem Windows-Betriebssystem, Sicherheitstyps, der Unterstützung für den Ruhezustand und der Datenträgerverschlüsselungssatz-ID des Masterimages gefiltert.
> - Die Verwendung eines Maschinenprofils mit vertrauenswürdigem Start als **Sicherheitstyp** ist obligatorisch, wenn Sie ein Image oder einen Snapshot auswählen, für das bzw. den der vertrauenswürdige Start aktiviert ist. Sie können dann SecureBoot und vTPM aktivieren oder deaktivieren, indem Sie die zugehörigen Werte im Maschinenprofil angeben. Informationen zu vertrauenswürdigen Starts in Azure finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Validieren Sie die ARM-Vorlagenspezifikation, um sicherzustellen, dass sie als Maschinenprofil zum Erstellen eines Maschinenkatalogs verwendet werden kann. Informationen zum Erstellen einer Azure-Vorlagenspezifikation finden Sie unter Azure-Vorlagenspezifikation erstellen.

Es gibt zwei Möglichkeiten zur Validierung der ARM-Vorlagenspezifikation:

- Klicken Sie nach Auswahl der ARM-Vorlagenspezifikation aus der Liste der Ressourcengruppen auf **Weiter**. Wenn die ARM-Vorlagenspezifikation Fehler enthält, werden Fehlermeldungen angezeigt,

- Führen Sie einen der folgenden PowerShell-Befehle aus:
  - <!JEKYLL@5180@2>
  - <!JEKYLL@5180@3>

  Beispiel:

  <!JEKYLL@5180@4>

Nachdem Sie den Katalog erstellt haben, können Sie die Konfigurationen anzeigen, die das Image vom Maschinenprofil erbt. Wählen Sie auf dem Knoten **Maschinenkataloge** den Katalog aus, um die Details im unteren Bereich anzuzeigen. Klicken Sie dann auf die Registerkarte **Vorlageneigenschaften**, um die Eigenschaften des Maschinenprofils anzuzeigen. Im Abschnitt **Tags** werden bis zu drei Tags angezeigt. Zum Anzeigen aller auf der VM platzierten Tags klicken Sie auf **Alle anzeigen**.

Um VMs mit Maschinenerstellungsdiensten (MCS) auf einem dedizierten Azure-Host bereitzustellen, aktivieren Sie das Kontrollkästchen **Hostgruppe verwenden** und wählen dann eine Hostgruppe aus der Liste aus. Eine Hostgruppe ist eine Ressource, die eine Sammlung dedizierter Hosts darstellt. Ein dedizierter Host ist ein Dienst, der physische Server bereitstellt, die eine oder mehrere virtuelle Maschinen hosten. Ihr Server ist für Ihr Azure-Abonnement reserviert und wird nicht mit anderen Abonnenten geteilt. Bei Verwendung eines dedizierten Hosts stellt Azure sicher, dass nur Ihre VMs auf diesem Host ausgeführt werden. Dieses Feature eignet sich für Szenarios, in denen Sie regulatorische oder interne Sicherheitsanforderungen erfüllen müssen. Weitere Informationen zu Hostgruppen und Überlegungen zu ihrer Verwendung finden Sie unter VMs auf dedizierten Azure-Hosts bereitstellen.

> **Wichtig:**
>
> - Es werden nur Hostgruppen mit aktivierter automatischer Azure-Platzierung angezeigt.
> - Durch Verwendung einer Hostgruppe wird die Seite **Virtuelle Maschinen** geändert, die später im Assistenten angezeigt wird. Auf dieser Seite werden nur die Maschinengrößen angezeigt, die in der ausgewählten Hostgruppe enthalten sind. Außerdem sind Verfügbarkeitszonen automatisch ausgewählt und nicht wählbar.

3. Die Seite **Speicher- und Lizenztypen** wird nur angezeigt, wenn Sie ein Azure Resource Manager-Image verwenden.

   Für den Maschinenkatalog können Sie die folgenden Speichertypen verwenden:

   - **Premium-SSD.** Bietet Datenträgerspeicherung mit hoher Leistung und niedriger Latenz für VMs mit E/A-intensiven Workloads.
   - **Standard-SSD.** Kostengünstige Speicheroption, die für Workloads geeignet ist, die eine gleichmäßige Leistung bei niedrigeren IOPS-Raten erfordern.

- **Standard-HDD.** Zuverlässiger, kostengünstiger Datenträgerspeicher, der für VMs mit latenzunempfindlichen Workloads geeignet ist.
- **Kurzlebiger Azure-Betriebsystemdatenträger**. Kostengünstige Speicheroption mit Wiederverwendung des lokalen VM-Datenträgers zum Hosten des Betriebssystemdatenträgers. Alternativ können Sie mit PowerShell Maschinen mit kurzlebigen Betriebsystemdatenträgern erstellen. Weitere Informationen finden Sie unter Kurzlebige Azure-Datenträger. Beachten Sie bei der Verwendung kurzlebiger Betriebssystemdatenträger Folgendes:
  - Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.
  - Zum Aktualisieren von Maschinen, die kurzlebige Betriebssystemdatenträger verwenden, müssen Sie ein Image auswählen, dessen Größe die des Cachedatenträgers bzw. des temporären Datenträgers der VM nicht übersteigt.
  - Sie können die später im Assistenten angebotene Option **VM und Systemdatenträger während Energiezyklen beibehalten** nicht verwenden.

> **Hinweis:**
>
> Der Identitätsdatenträger wird unabhängig vom gewählten Speichertyp immer mit Standard-SSD erstellt.

Der gewählte Speichertyp bestimmt, welche Maschinengrößen auf der Seite **Virtuelle Maschinen** des Assistenten angeboten werden. MCS konfiguriert Premium- und Standarddatenträger für die Verwendung von lokal redundantem Speicher (LRS). LRS erstellt mehrere synchrone Kopien Ihrer Daten in einem Datencenter. Bei kurzlebigen Azure-Betriebssystemdatenträgern wird das Betriebssystem auf dem lokalen VM-Datenträger gespeichert. Weitere Informationen über Speichertypen und Speicherreplikation bei Azure finden Sie in den folgenden Artikeln:

- Einführung in Azure Storage
- Azure Storage Premium: Design für hohe Leistung
- Azure Storage-Redundanz

Wählen Sie aus, ob vorhandene Windows- oder Linux-Lizenzen verwendet werden sollen:

- Windows-Lizenzen: Mit Windows-Lizenzen und Windows-Images (Azure- oder benutzerdefinierte Images) können Sie Windows-VMs in Azure zu geringeren Kosten ausführen. Es gibt zwei Arten von Lizenzen:
  - **Windows Server-Lizenz**. Ermöglicht die Verwendung Ihrer Windows Server- oder Azure Windows Server-Lizenzen und somit die Nutzung des Azure-Hybridvorteils. Einzelheiten finden Sie unter https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Der Azure-Hybridvorteil senkt die Kosten des Ausführens von VMs in Azure

auf die Grundgebühr für Computekapazität, da keine Gebühren für zusätzliche Windows Server-Lizenzen aus dem Azure-Katalog erhoben werden.

  - **Windows-Clientlizenz**. Ermöglicht die Verwendung Ihrer Windows 10- und Windows 11-Lizenzen in Azure und somit die Ausführung von Windows 10- und Windows 11-VMs in Azure ohne Erfordernis zusätzlicher Lizenzen. Weitere Informationen finden Sie unter Clientzugriffslizenzen und Verwaltungslizenzen.

- Linux-Lizenzen: Bei Verwendung eigener Linux-Lizenzen (Bring Your Own Subscription oder BYOS) müssen Sie für die Software nicht zahlen. Die BYOS-Gebühr umfasst nur die Hardware für die Rechenleistung. Es gibt zwei Arten von Lizenzen:
  - **RHEL_BYOS**: Um den Typ RHEL_BYOS zu verwenden, aktivieren Sie Red Hat Cloud Access in Ihrem Azure-Abonnement.
  - **SLES_BYOS**: Die BYOS-Versionen von SLES beinhalten Unterstützung von SUSE.

Beispiel:

- Windows-Lizenz überprüfen
- Linux-Lizenz konfigurieren

Lesen Sie die folgenden Dokumente, um mehr über Lizenztypen und ihre Vorteile zu erfahren:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery ist ein Repository zum Verwalten und Freigeben von Images. Damit können Sie Images in Ihrer gesamten Organisation verfügbar machen. Wir empfehlen Ihnen, beim Erstellen großer nicht-persistenter Maschinenkataloge ein Image in Azure Compute Gallery zu speichern, da sich VDA-Betriebssystemdatenträger dadurch schneller zurücksetzen lassen. Nachdem Sie **Vorbereitetes Image in der Azure Compute Gallery platzieren** ausgewählt haben, wird der Abschnitt **Azure Compute Gallery-Einstellungen** angezeigt, in dem Sie weitere Azure Computer Gallery-Einstellungen angeben können:

- **Verhältnis von virtuellen Maschinen zu Imagereplikaten**. Hier können Sie das Verhältnis von virtuellen Maschinen zu Imagereplikaten angeben, die Azure beibehalten soll. Standardmäßig speichert Azure ein Imagereplikat pro 40 nicht-persistente Maschinen. Bei persistenten Maschinen ist diese Zahl voreingestellt auf 1000.
- **Maximale Replikate**. Hier können Sie die maximale Anzahl von Image-Replikaten angeben, die Azure speichern soll. Der Standardwert ist 10.

Weitere Informationen zu Azure Compute Gallery finden Sie unter Azure Compute Gallery.

4. Geben Sie auf der Seite **VMs** an, wie viele VMs Sie erstellen möchten und wie groß sie sein sollen. Nach der Katalogerstellung können Sie die Maschinengröße durch Bearbeiten des Katalogs ändern.
5. Die Seite **Netzwerkkarten** enthält keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.
6. Wählen Sie auf der Seite **Datenträgereinstellungen**, ob der Zurückschreibcache aktiviert werden soll. Wenn die MCS-Speicheroptimierung aktiviert ist, können Sie beim Erstellen eines Katalogs folgende Einstellungen konfigurieren. Diese Einstellungen gelten für Azure- und für GCP-Umgebungen.

   Nach dem Aktivieren des Zurückschreibcache können Sie Folgendes tun:

   - Konfigurieren Sie die Größe des Datenträgers und des RAM, die zum Zwischenspeichern temporärer Daten verwendet werden. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.
   - Wählen des Speichertyps für den Datenträger für den Zurückschreibcache. Die folgenden Speichertypen stehen für den Zurückschreibcache-Datenträger zur Verfügung:
     - Premium-SSD
     - Standard-SSD
     - Standard-HDD
   - Wählen eines persistenten Datenträgers für den Zurückschreibcache für die bereitgestellten VMs (bei Bedarf). Wählen Sie **Zurückschreibcache aktivieren**, um die Optionen verfügbar zu machen. Die Standardeinstellung ist **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**.
   - Wählen Sie einen Datenträgertyp für den Zurückschreibcache aus.
     - **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**. Wenn diese Option ausgewählt ist, wird der Datenträger für den Zurückschreibcache während Energiezyklen gelöscht. Alle darauf umgeleitete Daten gehen verloren. Wenn auf dem temporären Datenträger der VM ausreichend Speicherplatz vorhanden ist, wird er als Host für den Zurückschreibcachedatenträger verwendet, da dies Ihre Kosten reduziert. Nach der Katalogerstellung können Sie überprüfen, ob die bereitgestellten Maschinen den temporären Datenträger verwenden. Klicken Sie dazu auf den Katalog und überprüfen Sie die Informationen auf der Registerkarte **Vorlageneigenschaften**. Bei Verwendung des temporären Datenträgers wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Ja (mit dem temporären Datenträger der VM)** angezeigt. Wenn er nicht verwendet wird, wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Nein (nicht mit dem temporären Datenträger der VM)** angezeigt.

  - **Persistenter Datenträger für Zurückschreibcache.** Wenn diese Option ausgewählt ist, wird der Zurückschreibcache-Datenträger für die bereitgestellten VMs beibehalten. Die Aktivierung dieser Option erhöht die Speicherkosten.

- Wählen Sie aus, ob VMs und Systemdatenträger für VDAs bei Energiezyklen beibehalten werden sollen.

  **VM und Systemdatenträger während Neustarts beibehalten.** Verfügbar, wenn Sie **Zurückschreibcache aktivieren** ausgewählt haben. Standardmäßig werden VMs und die Systemdatenträger beim Herunterfahren gelöscht und beim Starten neu erstellt. Wenn Sie die VM-Neustartzeiten reduzieren möchten, wählen Sie diese Option. Allerdings erhöht die Aktivierung dieser Option auch die Speicherkosten.

- Wählen Sie aus, ob Sie die **Einsparung von Speicherkosten aktivieren** möchten. Wenn diese Option aktiviert ist, wird der Speicherdatenträger beim Herunterfahren der VM auf Standard-HDD herabgestuft, um Speicherkosten zu senken. Beim Neustart wechselt die VM wieder zu den ursprünglichen Einstellungen. Die Option lässt sich auf Speicher- und Zurückschreibcache-Datenträger anwenden. Alternativ können Sie auch PowerShell verwenden. Siehe Speichertyp beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern.

  > **Hinweis:**
  >
  > Bei Microsoft gelten Einschränkungen für die Änderung des Speichertyps beim Herunterfahren einer VM. Es ist auch möglich, dass Microsoft künftig Änderungen des Speichertyps blockiert. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

- Wählen Sie aus, ob Daten auf Maschinen in diesem Katalog verschlüsselt werden sollen und welcher Verschlüsselungsschlüssel verwendet werden soll. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel (CMK) ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Die Standardeinstellungen werden vom Maschinenprofil oder vom Masterimage übernommen, wobei das Profil Vorrang hat:

  - Wenn Sie ein *Maschinenprofil* mit einem *CMK* verwenden, wird die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln** automatisch ausgewählt und verwendet standardmäßig den Schlüssel aus dem *Maschinenprofil*.
  - Wenn Sie ein *Maschinenprofil* mit einem von einer Plattform verwalteten Schlüssel (PMK) verwenden und das *Masterimage CMK*-verschlüsselt ist, wird die Option**Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln** automatisch ausgewählt und verwendet standardmäßig den Schlüssel aus dem Masterimage.

- Wenn Sie *kein Maschinenprofil* verwenden und das *Masterimage CMK-verschlüsselt* ist, wird die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln** automatisch ausgewählt und verwendet standardmäßig den Schlüssel aus dem *Masterimage*.

Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

7. Wählen Sie auf der Seite **Ressourcengruppe** aus, ob Sie neue Ressourcengruppen erstellen oder vorhandene verwenden.

   - Wenn Sie Ressourcengruppen erstellen möchten, wählen Sie **Weiter**.
   - Wenn Sie vorhandene Ressourcengruppen verwenden möchten, wählen Sie Gruppen in der Liste **Zum Bereitstellen verfügbare Ressourcengruppen** aus.

   > **Hinweis:**
   >
   > Wählen Sie genügend Gruppen aus, um die Maschinen aufzunehmen, die Sie im Katalog erstellen. Wenn sie nicht ausreichen, werden Sie in einer Meldung darauf hingewiesen. Wählen Sie ggf. mehr als die erforderliche Mindestanzahl aus, wenn Sie dem Katalog später weitere VMs hinzufügen möchten. Sie können einem Katalog nach dessen Erstellung keine weiteren Ressourcengruppen mehr hinzufügen.

   Weitere Informationen finden Sie unter Azure-Ressourcengruppen.

8. Wählen Sie auf der Seite **Maschinenidentitäten** einen Identitätstyp und konfigurieren Sie Identitäten für Maschinen in dem Katalog. Wenn Sie die VMs als **In Azure Active Directory eingebunden** festlegen, können Sie sie zu einer Azure AD-Sicherheitsgruppe hinzufügen. Verfahren:

   a) Wählen Sie im Feld **Identitätstyp** die Option **In Azure Active Directory eingebunden**. Die Option **Azure AD-Sicherheitsgruppe (optional)** wird angezeigt.
   b) Klicken Sie auf **Azure AD-Sicherheitsgruppe: Neu erstellen**.
   c) Geben Sie einen Gruppennamen ein und klicken Sie auf **Erstellen**.
   d) Folgen Sie den angezeigten Anweisungen, um sich bei Azure anzumelden.
      Wenn der Gruppenname in Azure nicht vorliegt, erscheint ein grünes Symbol. Andernfalls erscheint eine Fehlermeldung, in der Sie aufgefordert werden, einen neuen Namen einzugeben.
   e) Um die Sicherheitsgruppe einer zugewiesenen Sicherheitsgruppe hinzuzufügen, wählen Sie **Einer zugewiesenen Sicherheitsgruppe als Mitglied beitreten** und klicken Sie dann auf **Gruppe auswählen**, um eine zugewiesene Gruppe auszuwählen.
   f) Geben Sie das Benennungsschema für Maschinenkonten für die VMs ein.

   Nach der Katalogerstellung greift Citrix DaaS für Sie auf Azure zu und erstellt die Sicherheitsgruppe und eine dynamische Mitgliedschaftsregel für die Gruppe. Basierend auf der Regel werden virtuelle Maschinen mit dem in diesem Katalog angegebenen Benennungsschema automatisch zur Sicherheitsgruppe hinzugefügt.

Um dem Katalog virtuelle Maschinen mit einem anderen Benennungsschema hinzuzufügen, müssen Sie sich bei Azure anmelden. Citrix DaaS kann dann auf Azure zugreifen und eine dynamische Mitgliedschaftsregel erstellen, die auf dem neuen Benennungsschema basiert.

Beim Löschen des Katalogs ist für das Löschen der Sicherheitsgruppe aus Azure ebenfalls eine Anmeldung bei Azure erforderlich.

> **Hinweis:**
>
> Um die Azure AD-Sicherheitsgruppe nach der Katalogerstellung umzubenennen, bearbeiten Sie den Katalog und wechseln Sie im linken Bereich zu **Azure AD-Sicherheitsgruppe**. Namen von Azure AD-Sicherheitsgruppen dürfen die folgenden Zeichen nicht enthalten: <!JEKYLL@5180@5>.

- Die Seiten **Domänenanmeldeinformationen** und **Zusammenfassung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.

Schließen Sie den Assistenten ab.

### Azure-Vorlagenspezifikation erstellen

Sie können eine Azure-Vorlagenspezifikation im Azure-Portal erstellen und sie in der Schnittstelle "Vollständige Konfiguration"und in den PowerShell-Befehlen verwenden, um einen MCS-Maschinenkatalog zu erstellen oder zu aktualisieren.

Azure-Vorlagenspezifikation für eine vorhandene VM erstellen:

1. Gehen Sie zum Azure-Portal. Wählen Sie eine Ressourcengruppe und dann die VM und die Netzwerkschnittstelle aus. Klicken Sie oben im Menü **…** auf **Export template**.
2. Deaktivieren Sie das Kontrollkästchen **Include parameters**, wenn Sie eine Vorlagenspezifikation für die Katalogbereitstellung erstellen möchten.
3. Klicken Sie auf **Add to library**, um die Vorlagenspezifikation später zu ändern.
4. Geben Sie auf der Seite **Importing template** die erforderlichen Informationen wie **Name**, **Subscription**, **Subscription**, **Location** und **Version** ein. Klicken Sie auf **Next: Edit Template**.
5. Sie benötigen außerdem eine Netzwerkschnittstelle als unabhängige Ressource, wenn Sie Kataloge bereitstellen möchten. Daher müssen Sie alle <!JEKYLL@5180@6>-Elemente in der Vorlagenspezifikation entfernen. Beispiel:

   <!JEKYLL@5180@7>

6. Wählen Sie **Review + Create** und erstellen Sie die Vorlagenspezifikation.

7. Überprüfen Sie auf der Seite **Template Specs** die erstellte Vorlagenspezifikation. Klicken Sie auf die Vorlagenspezifikation. Klicken Sie im linken Bereich auf **Versions**.
8. Sie können eine neue Version erstellen, indem Sie auf **Create new version** klicken. Geben Sie eine neue Versionsnummer an, nehmen Sie Änderungen an der aktuellen Vorlagenspezifikation vor und klicken Sie auf **Review + Create**, um die neue Version der Vorlagenspezifikation zu erstellen.

Mit den folgenden PowerShell-Befehlen können Sie Informationen zur Vorlagenspezifikation und Vorlagenversion abrufen:

- Um Informationen über die Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

  <!JEKYLL@5180@8>

- Um Informationen über die Version der Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

  <!JEKYLL@5180@9>

#### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Sie können hierfür die Schnittstelle Vollständige Konfiguration oder PowerShell verwenden.

- Weitere Informationen zur Verwendung der Schnittstelle **Vollständige Konfiguration** finden Sie unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.
- PowerShell: Weitere Informationen finden Sie unter Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

### Provisioning von Maschinen in spezifischen Verfügbarkeitszonen

Sie können das Provisioning von Maschinen auch in spezifischen Verfügbarkeitszonen in Azure-Umgebungen ausführen. Dies können Sie mit der Oberfläche "Vollständige Konfiguration"oder PowerShell erreichen.

> **Hinweis:**
>
> Wenn keine Zonen angegeben werden, lässt MCS Azure die Maschinen innerhalb der Region platzieren. Werden mehrere Zonen angegeben, verteilt MCS die Maschinen nach dem Zufallsprinzip in den Zonen.

#### Verfügbarkeitszonen in der Oberfläche "Vollständige Konfiguration"konfigurieren

Beim Erstellen eines Maschinenkatalogs können Sie Verfügbarkeitszonen für das Provisioning von Maschinen angeben. Wählen Sie auf der Seite **Virtuelle Maschinen** eine oder mehrere Verfügbarkeitszonen aus, in denen Sie Maschinen erstellen möchten.

Es gibt zwei Gründe, aus denen keine Verfügbarkeitszonen verfügbar sind: Die Region hat keine Verfügbarkeitszonen oder die ausgewählte Maschinengröße ist nicht verfügbar.

Informationen zur Konfiguration mit dem PowerShell-Befehl finden Sie unter Verfügbarkeitszonen mit PowerShell konfigurieren.

### Kurzlebige Azure-Datenträger

Ein kurzlebiger Azure-Datenträger ermöglicht die Umnutzung des Cachedatenträgers oder temporären Datenträgers zum Speichern des Betriebssystemdatenträgers für eine virtuelle Azure-Maschine. Dies ist nützlich für Azure-Umgebungen, die anstelle von Standard-HDD-Datenträgern leistungsstärkere SSD-Datenträger erfordern. Informationen zum Erstellen eines Katalogs mit einem kurzlebigen Azure-Datenträger finden Sie unter Katalog mit kurzlebigem Azure-Datenträger erstellen.

> **Hinweis:**
>
> Persistente Kataloge unterstützen keine kurzlebigen Betriebssystemdatenträger.

Kurzlebige Betriebssystemdatenträger erfordern ein Provisioningschema mit verwalteten Datenträgern und eine Azure Compute Gallery. Weitere Informationen finden Sie unter Azure Shared Image Gallery.

#### Temporären kurzlebigen OS-Datenträger speichern

Sie können einen kurzlebigen OS-Datenträger auf dem Temp- bzw. Ressourcendatenträger der VM speichern. So können Sie einen kurzlebigen OS-Datenträger mit VMs verwenden, die über keinen oder nur unzureichenden Cache verfügen. Solche VMs verfügen über einen Temp- bzw. Ressourcendatenträger zum Speichern eines kurzlebigen OS-Datenträgers (z. B. <!JEKYLL@5180@10>).

Beachten Sie Folgendes:

- Kurzlebige Datenträger werden entweder auf dem VM-Cachedatenträger oder auf dem temporären bzw. Ressourcendatenträger der VM gespeichert. Die Cachedatenträger ist dem temporären Datenträger vorzuziehen, es sei denn, der Cachedatenträger ist zu klein für den Inhalt des Betriebsystemdatenträgers.

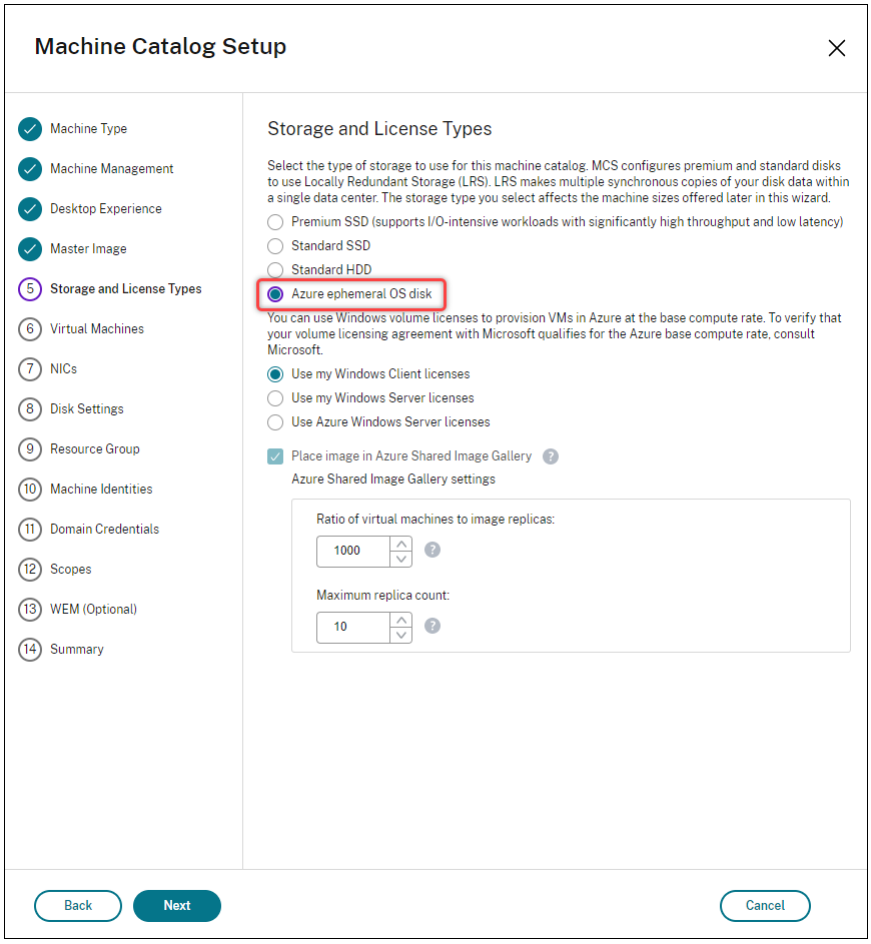
- Entsteht bei Updates ein neues Image, das größer als der Cachedatenträger und kleiner als der Temp-Datenträger ist, wird der kurzlebige OS-Datenträger durch den Temp-Datenträger der VM ersetzt.

### Kurzlebige Azure-Betriebssystemdatenträger und MCS-Speicheroptimierung (MCS-E/A)

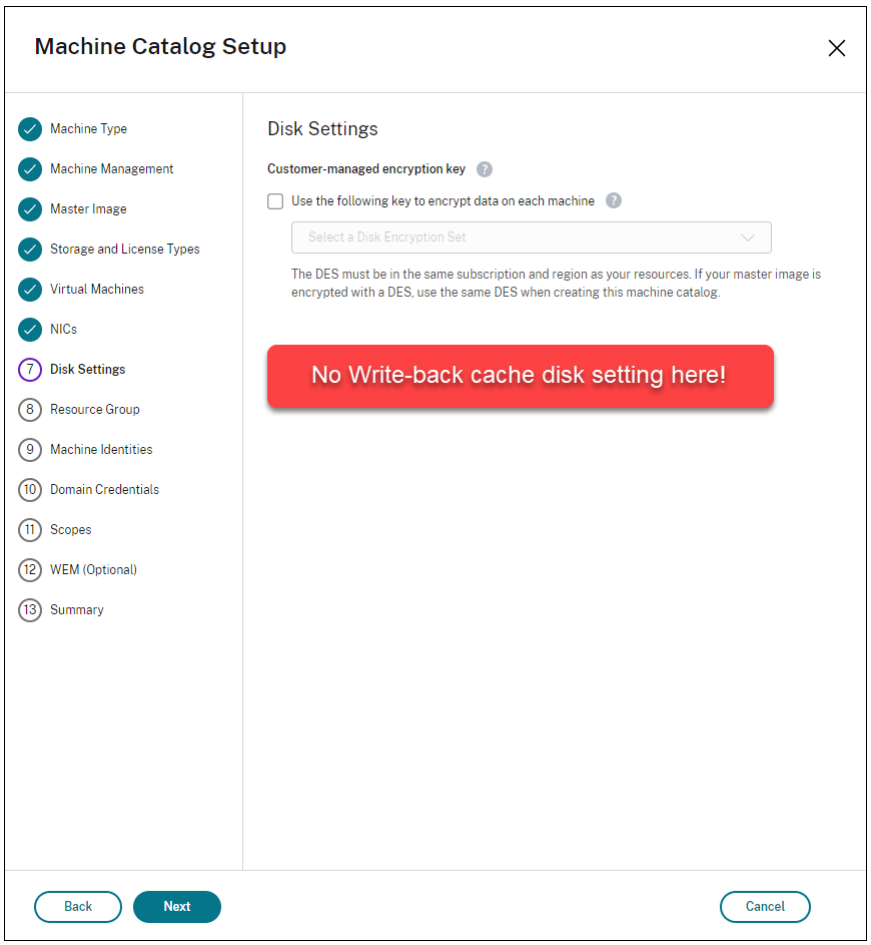
Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.

Wichtige Punkte:

- Sie können keinen Maschinenkatalog mit gleichzeitig aktiviertem kurzlebigem Betriebssystemdatenträger und MCS-E/A erstellen.
- Wenn Sie im **Assistenten zum Einrichten eines Maschinenkatalogs** auf der Seite **Speicher- und Lizenztypen** die Option **Kurzlebiger Azure-Betriebssystemdatenträger** auswählen, werden auf der Seite **Datenträgereinstellungen** keine Optionen für den Zurückschreibcache-Datenträger angezeigt.






- Die PowerShell-Parameter (<!JEKYLL@5180@11> und <!JEKYLL@5180@12>), die in <!JEKYLL@5180@13> oder <!JEKYLL@5180@14> auf **true** gesetzt sind, schlagen mit entsprechender Fehlermeldung fehl.
- Bei bestehenden Maschinenkatalogen, für die bei der Erstellung beide Features aktiviert wurden, ist weiterhin Folgendes möglich:
  - Aktualisieren des Maschinenkatalogs
  - Hinzufügen oder Löschen von VMs
  - Löschen des Maschinenkatalogs

### Azure Compute Gallery

Verwenden Sie Azure Compute Gallery (früher Shared Image Gallery) als Repository mit veröffentlichten Images für per MCS bereitgestellte Maschinen in Azure. Sie können ein veröffentlichtes Image in der Image Gallery speichern, um die Erstellung und Hydration von Betriebssystemdatenträgern zu beschleunigen und die OS- und Anwendungsstartzeiten nicht persistenter VMs zu verbessern. Azure Compute Gallery enthält die folgenden drei Elemente:

- Gallery: Hier werden Images gespeichert. MCS erstellt je eine Gallery für jeden Maschinenkatalog.
- Imagedefinition: Diese Definition enthält Informationen zum veröffentlichten Image (Betriebssystemtyp/-zustand, Azure-Region). MCS erstellt eine Imagedefinition für jedes Image, das für den Katalog erstellt wurde.
- Gallery Image Version: Jedes Image in einer Azure Compute Gallery kann mehrere Versionen haben, und jede Version kann mehrere Replikate in verschiedenen Regionen haben. Jedes Replikat ist eine vollständige Kopie des veröffentlichten Images. Citrix DaaS erstellt für jedes Image eine Standard_LRS-Imageversion (Version 1.0.0) mit der entsprechenden Anzahl von Replikaten in der Region des Katalogs, basierend auf der Maschinenanzahl im Katalog, der konfigurierten Replikatquote und der konfigurierten Anzahl maximaler Replikate.

> **Hinweis:**
>
> Die Azure Compute Gallery-Funktion ist nur mit verwalteten Datenträgern kompatibel. Sie ist nicht für Legacy-Maschinenkataloge verfügbar.

Weitere Informationen finden Sie unter Übersicht über Azure Shared Image Gallery.

#### Zugriff auf Images aus Azure Compute Gallery

Als Image zum Erstellen eines Maschinenkatalogs können Sie Images auswählen, die Sie in der Azure Compute Gallery erstellt haben. Diese Images sind auf der Seite **Image** des Assistenten zum Erstellen von Maschinenkatalogen aufgelistet.

Damit diese Images angezeigt werden, müssen Sie folgende Schritte ausführen:

1. Richten Sie Citrix DaaS ein.
2. Stellen Sie eine Verbindung mit Azure Resource Manager her.
3. Erstellen Sie im Azure-Portal eine Ressourcengruppe. Weitere Informationen finden Sie unter Erstellen einer Azure Shared Image Gallery über das Portal.
4. Erstellen Sie in der Ressourcengruppe eine Azure Compute Gallery.
5. Erstellen Sie in der Azure Compute Gallery eine Imagedefinition.
6. Erstellen Sie in der Imagedefinition eine Imageversion.

Weitere Informationen zur Konfiguration von Azure Compute Gallery finden Sie unter Azure Compute Gallery konfigurieren.

## Bedingungen für die Verwendung eines temporären Azure-Datenträgers als Datenträger für den Zurückschreibcache

Sie können den temporären Azure-Datenträger nur dann als Datenträger für den Zurückschreibcache verwenden, wenn alle der folgenden Bedingungen erfüllt sind:

- Der Datenträger für den Zurückschreibcache darf nicht persistent sein, da der temporäre Azure-Datenträger nicht für persistente Daten geeignet ist.
- Die gewählte Azure-VM-Größe muss einen temporären Datenträger einschließen.
- Der kurzlebige Betriebsystemdatenträger muss nicht aktiviert sein.
- Stimmen Sie zu, dass die Datenträgerdatei für den Zurückschreibcache auf dem temporären Azure-Datenträger platziert wird.
- Der temporäre Azure-Datenträger muss größer sein als der Gesamtwert für (Größe des Datenträgers des Zurückschreibecache + reservierter Speicherplatz für Auslagerungsdatei + 1 GB Pufferspeicher).

### Szenarios mit nicht persistentem Datenträger für den Zurückschreibcache

Die folgende Tabelle enthält drei Szenarios, in denen beim Erstellen des Maschinenkatalogs der temporäre Datenträger für den Zurückschreibcache (WBC) verwendet wird.

| Szenario | Ergebnis |
|---|---|
| Alle Bedingungen zur Verwendung des temporären Datenträgers für den Zurückschreibcache sind erfüllt. | Die WBC-Datei <!JEKYLL@5180@15> wird auf dem temporären Datenträger abgelegt. |
| Der temporäre Datenträger hat nicht genügend Speicherplatz für den Zurückschreibcache. | Ein VHD-Datenträger “MCSWCDisk”wird erstellt und die WBC-Datei <!JEKYLL@5180@16> wird auf diesem Datenträger abgelegt. |
| Der temporäre Datenträger hat genügend Speicherplatz für den Zurückschreibcache, <!JEKYLL@5180@17> ist jedoch auf False gesetzt. | Ein VHD-Datenträger “MCSWCDisk”wird erstellt und die WBC-Datei <!JEKYLL@5180@18> wird auf diesem Datenträger abgelegt. |

Weitere Informationen finden Sie in den folgenden PowerShell-Themen:

- Maschinenkatalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen
- Maschinenkatalog mit persistentem Zurückschreibcachedatenträger erstellen

### Azure-serverseitige Verschlüsselung

Citrix DaaS unterstützt vom Kunden verwaltete Schlüssel für Azure Managed Disks über Azure Key Vault. Mit dieser Unterstützung können Sie Ihre Unternehmens- und Compliance-Anforderungen verwalten, indem Sie die verwalteten Datenträger des Maschinenkatalogs mit Ihrem eigenen Schlüssel verschlüsseln. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung von Azure Disk Storage.

Bei Verwendung dieses Features für verwaltete Datenträger gilt Folgendes:

- Um den Schlüssel zu ändern, mit dem ein Datenträger verschlüsselt ist, ändern Sie den aktuellen Schlüssel im <!JEKYLL@5180@19>. Alle dem <!JEKYLL@5180@20> zugeordneten Ressourcen werden dann mit dem neuen Schlüssel verschlüsselt.
- Wenn Sie den Schlüssel deaktivieren oder löschen, werden alle VMs mit Datenträgern, die den Schlüssel verwenden, automatisch heruntergefahren. Nach dem Herunterfahren können die VMs erst wieder verwendet werden, wenn Sie den Schlüssel wieder aktivieren oder einen neuen Schlüssel zuweisen. Kataloge, die den Schlüssel verwenden, können nicht aktiviert werden und Sie können solchen Katalogen keine VMs hinzufügen.

#### Wichtige Überlegungen bei der Verwendung vom Kunden verwalteter Schlüssel

Beachten Sie die folgenden Punkte bei der Verwendung dieses Features:

- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Datenträger, Snapshots und Images, die mit kundenverwalteten Schlüsseln verschlüsselt wurden, können nicht in anderen Ressourcengruppen oder Abonnements verschoben werden.
- Auf der Microsoft-Website finden Sie Informationen zu Limits für Datenträgerverschlüsselungssätze pro Region.

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren der Azure-serverseitigen Verschlüsselung finden Sie unter Schnellstart: Key Vault-Erstellung mit dem Azure-Portal .

#### Vom Kunden verwalteter Schlüssel für Azure

Beim Erstellen eines Maschinenkatalogs können Sie wählen, ob Daten auf den im Katalog bereitzustellenden Maschinen verschlüsselt werden sollen. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter

Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Ein Datenträgerverschlüsselungssatz (DES) repräsentiert einen vom Kunden verwalteten Schlüssel. Um das Feature zu nutzen, müssen Sie zuerst einen DES in Azure erstellen. Ein DES hat folgendes Format:

- <!JEKYLL@5180@21>

Wählen Sie einen DES aus der Liste aus. Der ausgewählte DES muss sich im selben Abonnement und in derselben Region wie Ihre Ressourcen befinden.

Wenn Sie einen Katalog mit einem Schlüssel erstellen und später den entsprechenden DES in Azure deaktivieren, können Sie die Maschinen im Katalog nicht mehr einschalten und diesem keine Maschinen mehr hinzufügen.

Weitere Informationen finden Sie unter Maschinenkatalog mit einem vom Kunden verwalteten Schlüssel erstellen.

### Azure-Datenträgerverschlüsselung auf dem Host

Sie können einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Sie können eine VM oder eine Vorlagenspezifikation als Eingabe für ein Maschinenprofil verwenden.

Bei diesem Verschlüsselungsverfahren werden Daten nicht über den Azure-Speicher verschlüsselt. Die Daten werden auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten.

**Einschränkungen:**

Die Azure-Datenträgerverschlüsselung auf dem Host:

- wird nicht für alle Azure-Maschinengrößen unterstützt.
- ist nicht kompatibel mit der Azure-Datenträgerverschlüsselung.

Weitere Informationen:

- Maschinenkatalog mit Verschlüsselung auf dem Host erstellen.
- Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen

### Doppelte Verschlüsselung auf verwalteten Datenträgern

Sie können einen Maschinenkatalog mit doppelter Verschlüsselung erstellen. Bei mit diesem Feature erstellten Katalogen werden alle Datenträger serverseitig mit plattformseitig und kundenseitig verwalteten Schlüsseln verschlüsselt. Sie besitzen und verwalten den Azure Key Vault, den Verschlüsselungsschlüssel und die Datenträgerverschlüsselungssätze (DES).

Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der vom Kunden verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt.

> **Hinweis:**
>
> - Sie können einen Maschinenkatalog mit doppelter Verschlüsselung über die Benutzeroberfläche für die vollständige Konfiguration und mit PowerShell-Befehlen erstellen und aktualisieren.
> - Sie können einen nicht auf Maschinenprofilen basierenden Workflow oder einen auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog mit doppelter Verschlüsselung zu erstellen oder zu aktualisieren.
> - Wenn Sie einen nicht auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog zu erstellen, können Sie die gespeicherte <!JEKYLL@5180@22> wiederverwenden.
> - Wenn Sie ein Maschinenprofil verwenden, können Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

**Einschränkungen**

- Die doppelte Verschlüsselung wird für Ultra Disk- und Premium SSD v2-Datenträgern nicht unterstützt.
- Die doppelte Verschlüsselung wird für nicht verwaltete Datenträger nicht unterstützt.
- Wenn Sie den Schlüssel für einen Datenträgerverschlüsselungssatz deaktivieren, der mit einem Katalog verknüpft ist, werden die VMs des Katalogs deaktiviert.
- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Sie können maximal 50 Datenträgerverschlüsselungssätze pro Region und Abonnement erstellen.

Weitere Informationen finden Sie in den folgenden PowerShell-Themen:

- Maschinenkatalog mit doppelter Verschlüsselung erstellen
- Unverschlüsselten Katalog zur Verwendung der doppelten Verschlüsselung konvertieren
- Überprüfen, ob ein Katalog doppelt verschlüsselt ist

## Azure-Ressourcengruppen

Azure Provisioning-Ressourcengruppen sind eine Methode des Provisionings von VMs, über die Benutzern Anwendungen und Desktops bereitgestellt werden. Wenn Sie einen MCS-Maschinenkatalog erstellen, können Sie vorhandene, leere Azure-Ressourcengruppen hinzufügen oder neue erstellen. Informationen zu Azure-Ressourcengruppen finden Sie in der Dokumentation von Microsoft.

### Verwendung von Azure-Ressourcengruppen

Es gibt keine Beschränkung für die Anzahl der virtuellen Maschinen, verwalteten Datenträger, Snapshots und Images pro Azure-Ressourcengruppe. (Die Beschränkung auf 240 VMs pro 800 verwaltete Datenträger pro Azure-Ressourcengruppe wurde entfernt.)

- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit vollem Gültigkeitsbereich verwenden, erstellen die Maschinenerstellungsdienste nur eine Azure-Ressourcengruppe und verwenden nur diese Gruppe für den Katalog.
- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit eingeschränktem Gültigkeitsbereich verwenden, müssen Sie eine leere, vorab erstellte Azure-Ressourcengruppe für den Katalog angeben.

## Azure Marketplace

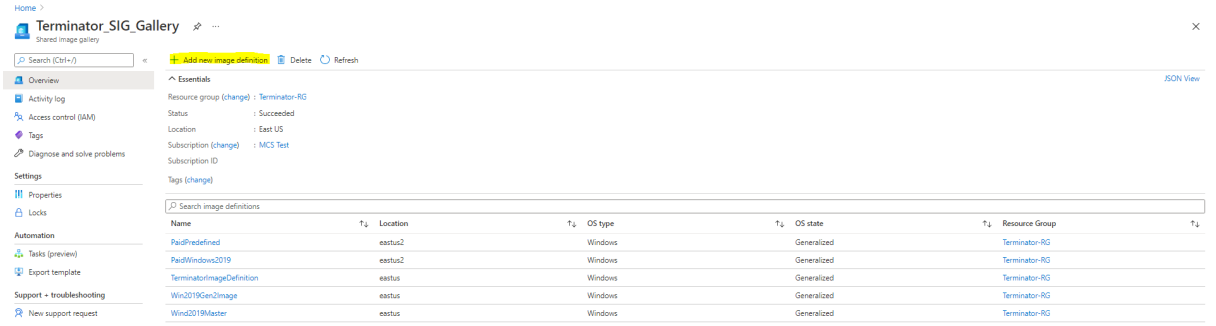
Citrix DaaS unterstützt die Verwendung eines Masterimages mit Abonnementinformationen zum Erstellen von Maschinenkatalogen in Azure. Weitere Informationen finden Sie unter Microsoft Azure Marketplace.

> **Tipp:**
>
> Manchen Images im Azure-Marketplace (z. B. Standard-Windows Server-Image) sind keine Abonnementinformationen angefügt. Das Citrix DaaS-Feature ist für kostenpflichtige Images vorgesehen.

### Das in der Azure Compute Gallery erstellte Image auf Azure-Abonnementinformationen überprüfen

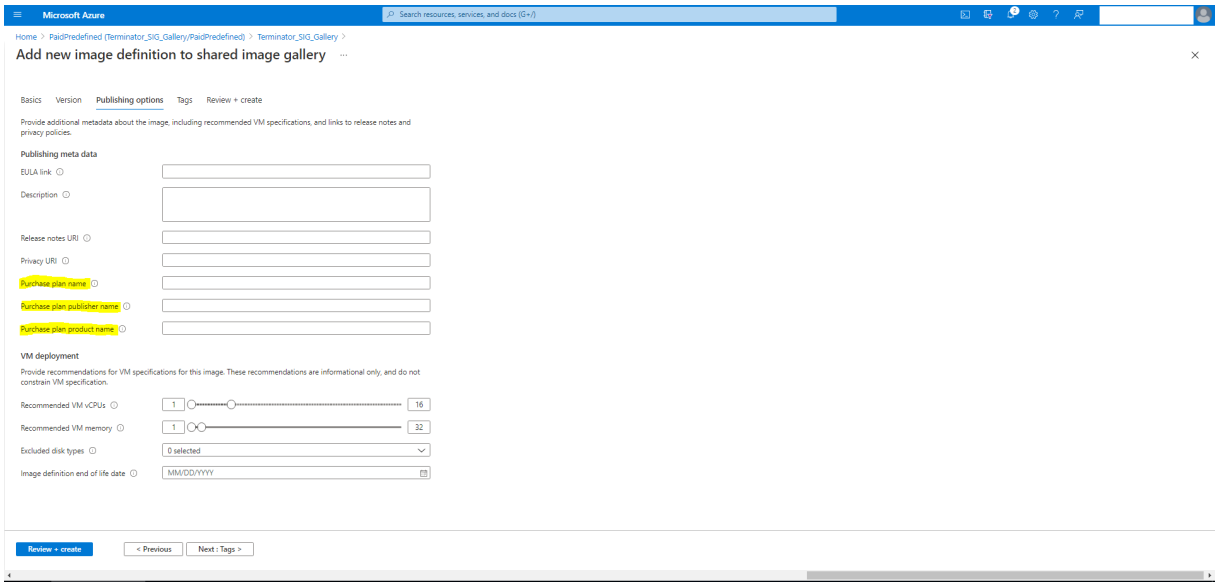
Gehen Sie wie in diesem Abschnitt beschrieben vor, um Images der Azure Compute Gallery in der Oberfläche für die vollständige Konfiguration anzuzeigen. Diese Images können für ein Masterimage verwendet werden. Um das Image in einer Azure Compute Gallery abzulegen, erstellen Sie in der Gallery eine Imagedefinition.



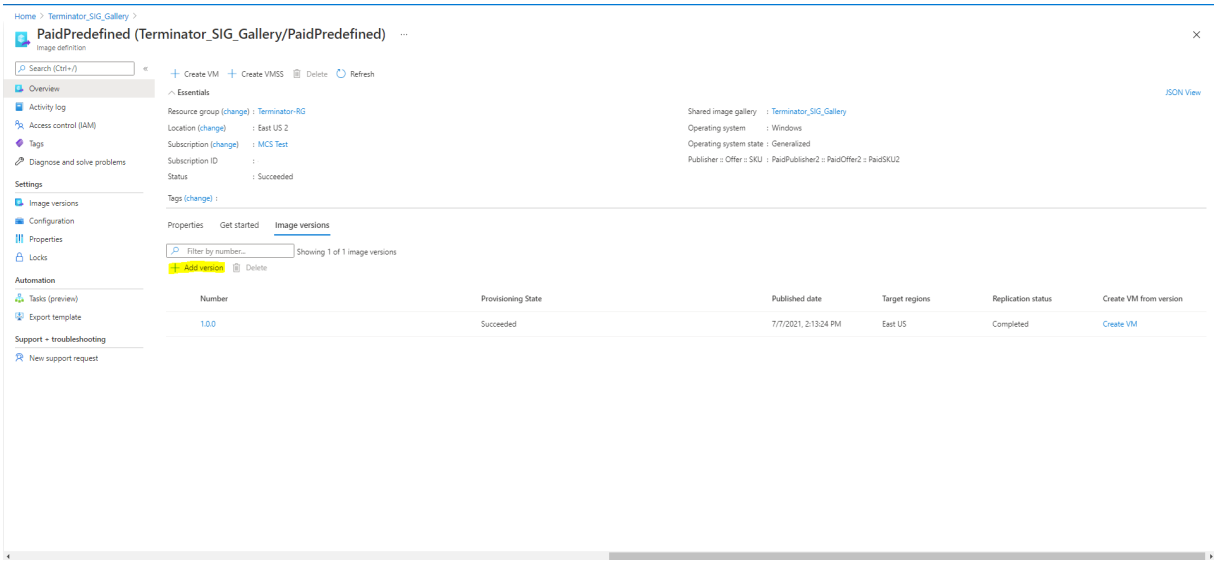

Überprüfen Sie auf der Seite **Veröffentlichungsoptionen** die Informationen zum Abonnement.

Die Informationsfelder sind zunächst leer. Füllen Sie diese Felder mit den Abonnementinformationen für das Image aus. Werden die Informationen nicht angegeben, kann der Maschinenkatalogprozess fehlschlagen.

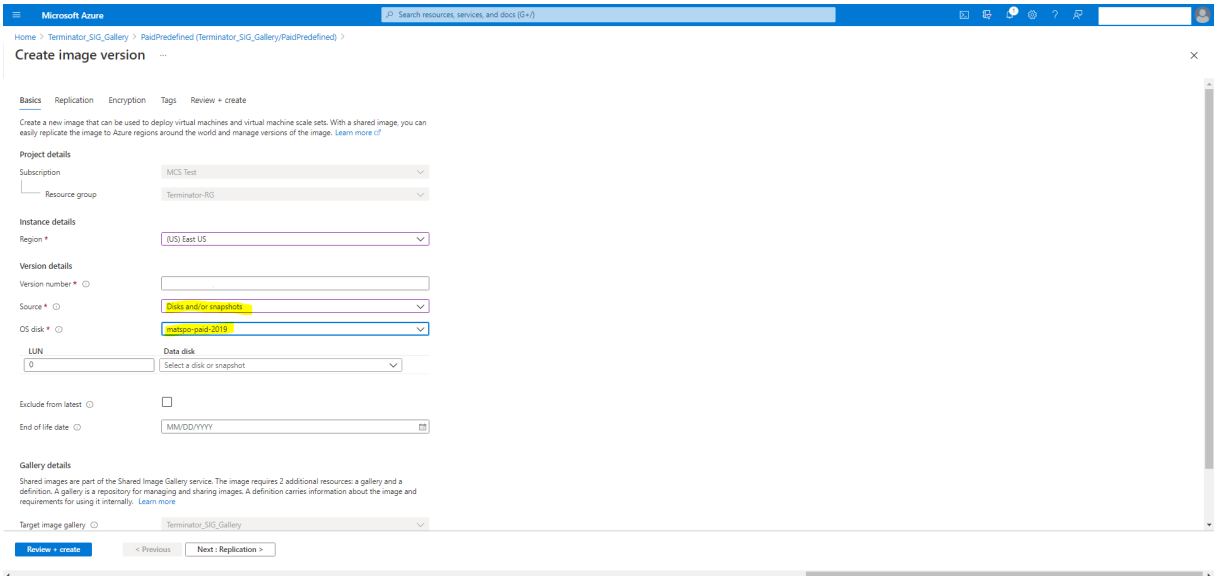



Nach dem Prüfen der Abonnementinformationen erstellen Sie eine Imageversion in der Definition. Diese wird als Masterimage verwendet. Klicken Sie auf **Add Version**:




Wählen Sie im Abschnitt **Version details** den Image-Snapshot oder verwalteten Datenträger als Quelle aus:




## Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent

Azure Monitoring ist ein Dienst, mit dem Sie Telemetriedaten aus Ihren Azure-und On-Premises-Umgebungen erfassen, analysieren und umsetzen können.

Azure Monitor Agent (AMA) sammelt Überwachungsdaten aus Rechenressourcen wie virtuellen Maschinen und übermittelt die Daten an Azure Monitor. Derzeit unterstützt der Dienst das Erfassen von Ereignisprotokollen sowie Syslog- und Leistungsmetriken, die dann an die Datenquellen Azure Monitor Metrics und Azure Monitor Logs gesendet werden.

Die Überwachung wird durch eindeutige Identifizierung der VMs in den Überwachungsdaten ermöglicht. Hierfür können Sie die VMs eines MCS-Maschinenkatalogs mit AMA als installierter Erweiterung bereitstellen.

**Anforderungen**

- Berechtigungen: Vergewissern Sie sich, dass Sie über die unter Informationen zu Azure-Berechtigungen angegebenen Azure-Mindestberechtigungen und über die folgenden Berechtigungen zur Verwendung von Azure Monitor verfügen:
  - <!JEKYLL@5180@23>
  - <!JEKYLL@5180@24>
  - <!JEKYLL@5180@25>
  - <!JEKYLL@5180@26>
  - <!JEKYLL@5180@27>
- Datensammlungsregel: Richten Sie eine Datensammlungsregel im Azure-Portal ein. Informationen zum Einrichten einer Datensammlungsregel finden Sie unter Create a data collection rule. Datensammlungsregeln sind plattformspezifisch (Windows oder Linux). Vergewissern Sie sich, dass Sie eine Datensammlungsregel gemäß der erforderlichen Plattform erstellen.
  AMA verwendet Datensammlungsregeln zum Verwalten der Zuordnung zwischen Ressourcen (wie VMs) und Datenquellen (wie Azure Monitor Metrics und Azure Monitor Logs).
- Standard-Workspace: Erstellen Sie einen Workspace im Azure-Portal. Informationen zum Erstellen eines Workspace finden Sie unter Create a Log Analytics workspace. Wenn Sie Protokolle und Daten sammeln, werden die Informationen in einem Workspace gespeichert. Ein Workspace hat eine eindeutige Workspace-ID und Ressourcen-ID. Der Workspace-Name muss für eine bestimmte Ressourcengruppe eindeutig sein. Nachdem Sie einen Workspace erstellt haben, konfigurieren Sie Datenquellen und Lösungen, um ihre Daten im Workspace zu speichern.
- Überwachungserweiterungen in Positivliste: Die Erweiterungen <!JEKYLL@5180@28> und <!JEKYLL@5180@29> sind von Citrix definierte Erweiterungen auf der Positivliste. Zur Anzeige der Erweiterungen auf der Positivliste verwenden Sie den PowerShell-Befehl <!JEKYLL@5180@30>.
- Masterimage: Microsoft empfiehlt, Erweiterungen von einer vorhandenen Maschine zu entfernen, bevor eine neue Maschine damit erstellt wird. Wenn die Erweiterungen nicht entfernt werden, kann dies zu unerwartetem Verhalten durch verbliebene Dateien führen. Weitere Informationen finden Sie unter If the VM is recreated from an existing VM.

Informationen zum Erstellen eines Katalogs mit aktiviertem AMA mit PowerShell finden Sie unter Katalog-VMs mit aktiviertem AMA bereitstellen.

## Vertrauliche Azure-VMs

Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist.

Sie können MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

### Wichtige Überlegungen zu vertraulichen VMs

Im Hinblick auf unterstützte VM-Größen und die Erstellung von Maschinenkatalogen mit vertraulichen VMs gilt es, Folgendes zu beachten:

- Unterstützte VM-Größen:
  - DCasv5-Serie
  - DCadsv5-Serie
  - ECasv5-Serie
  - ECadsv5-Serie
- Erstellen von Maschinenkatalogen mit vertraulichen VMs.
  - Sie können Maschinenkataloge mit vertraulichen Azure-VMs mithilfe der Schnittstelle "Vollständige Konfiguration"und PowerShell-Befehlen erstellen.
  - Sie müssen einen maschinenprofilbasierten Workflow verwenden, um einen Maschinenkatalog mit vertraulichen Azure-VMs zu erstellen. Sie können eine VM oder eine Vorlagenspezifikation als Maschinenprofileingabe verwenden.
  - Für das Masterimage und das als Eingabe verwendete Maschinenprofil muss derselbe Sicherheitstyp aktiviert werden. Es gibt folgende Sicherheitstypen:
    * VMGuestStateOnly: Vertrauliche VM, bei der nur der VM-Gastzustand verschlüsselt ist
    * DiskWithVMGuestState: Vertrauliche VM, bei der sowohl der Betriebssystemdatenträger als auch der VM-Gastzustand mit einem plattformverwalteten oder einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Es können normale und auch kurzlebige Betriebssystemdatenträger verschlüsselt werden.
  - Über den Parameter "AdditionalData"können Sie Informationen zu vertraulichen VMs verschiedener Ressourcentypen, etwa verwaltete Datenträger, Snapshots, Azure Compute Gallery-Image, VM und ARM-Vorlagenspezifikation abrufen. Beispiel:

    <!JEKYLL@5180@31>

Es gibt folgende zusätzlichen Daten:

* DiskSecurityType
* ConfidentialVMDiskEncryptionSetId
* DiskSecurityProfiles

Führen Sie folgenden Befehl aus, um die Confidential Compute-Eigenschaft für eine Maschinengröße abzurufen: <!JEKYLL@5180@32>

Das “additional data”-Feld ist <!JEKYLL@5180@33>.

- Sie können den Sicherheitstyp eines Masterimages oder eines Maschinenprofils nicht von “vertraulich”in “nicht vertraulich”oder umgekehrt ändern.
- Für jede falsche Konfiguration erhalten Sie eine entsprechende Fehlermeldung.

#### Masterimages und Maschinenprofile vorbereiten

Bevor Sie einen Satz vertraulicher VMs erstellen, gehen Sie wie folgt vor, um ein Masterimage und ein Maschinenprofil für sie vorzubereiten:

1. Erstellen Sie im Azure-Portal eine vertrauliche VM mit bestimmten Einstellungen wie:

   - **Sicherheitstyp**: Vertrauliche virtuelle Maschinen
   - **Vertrauliche Betriebssystem-Datenträgerverschlüsselung**: Aktiviert.
   - **Schlüsselverwaltung**: Vertrauliche Datenträgerverschlüsselung mit einem plattformverwalteten Schlüssel
     Weitere Informationen zum Erstellen vertraulicher VMs finden Sie in diesem Microsoft-Artikel.

2. Bereiten Sie das Masterimage auf der erstellten VM vor. Installieren Sie die erforderlichen Anwendungen und den VDA auf der erstellten VM.

   > **Hinweis:**
   >
   > Das Erstellen vertraulicher VMs mit VHD wird nicht unterstützt. Verwenden Sie stattdessen Azure Compute Gallery, verwaltete Datenträger oder Snapshots für diesen Zweck.

3. Erstellen Sie das Maschinenprofil auf eine der folgenden Arten:

   - Verwenden Sie die in Schritt 1 erstellte vorhandene VM, wenn sie die erforderlichen Maschineneigenschaften besitzt.
   - Wenn Sie sich für eine ARM-Vorlagenspezifikation als Maschinenprofil entscheiden, erstellen Sie die Vorlagenspezifikation wie erforderlich. Konfigurieren Sie insbesondere Parameter, die Ihre Anforderungen für vertrauliche VMs erfüllen, wie *SecurityEncryptionType*

und *diskEncryptionSet* (für vom Kunden verwaltete Schlüssel). Weitere Informationen finden Sie unter Azure-Vorlagenspezifikation erstellen.

> **Hinweis:**
>
> – Stellen Sie sicher, dass das Masterimage und das Maschinenprofil denselben Sicherheitsschlüsseltyp haben.
> – Um vertrauliche virtuelle Maschinen zu erstellen, die eine vertrauliche Betriebssystem-Datenträgerverschlüsselung mit einem vom Kunden verwalteten Schlüssel erfordern, stellen Sie sicher, dass die IDs des Datenträgerverschlüsselungssatzes im Masterimage und im Maschinenprofil identisch sind.

#### Vertrauliche VMs mithilfe der vollständigen Konfiguration oder von PowerShell-Befehlen erstellen

Um eine Reihe vertraulicher VMs zu erstellen, erstellen Sie einen Maschinenkatalog mit einem Masterimage und einem Maschinenprofil, das von der gewünschten vertraulichen VM abgeleitet wurde.

Um den Katalog mit der vollständigen Konfiguration zu erstellen, folgen Sie den unter Maschinenkataloge erstellen beschriebenen Schritten. Beachten Sie die folgenden Überlegungen:

- Wählen Sie auf der Seite **Image** ein Masterimage und ein Maschinenprofil aus, das Sie für die Erstellung der vertraulichen VM vorbereitet haben. Die Auswahl des Maschinenprofils ist obligatorisch und es stehen nur Profile zur Auswahl, die den gleichen Sicherheitsverschlüsselungstyp wie das ausgewählte Masterimage haben.
- Auf der Seite **Virtuelle Maschinen** werden nur Maschinengrößen zur Auswahl angezeigt, die vertrauliche VMs unterstützen.
- Auf der Seite **Datenträgereinstellungen** können Sie den Datenträgerverschlüsselungssatz nicht angeben, da er vom ausgewählten Maschinenprofil übernommen wurde.

### PowerShell verwenden

In diesem Abschnitt wird beschrieben, wie Sie die folgenden Aufgaben mit PowerShell ausführen:

- Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden
- Azure-VM-Erweiterungen aktivieren
- Maschinenkataloge mit vertrauenswürdigem Start
- Eigenschaftswerte für Maschinenprofile verwenden
- Verfügbarkeitszonen mit PowerShell konfigurieren
- VMs auf dedizierten Azure-Hosts bereitstellen
- Speichertypen konfigurieren

- Zonenredundanten Speicher aktivieren
- Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen
- Windows-Lizenz überprüfen
- Linux-Lizenz konfigurieren
- Maschinenkatalog mit kurzlebigem Azure-Datenträger erstellen
- Azure Compute Gallery konfigurieren
- Katalog mit mehreren Netzwerkkarten pro VM erstellen oder aktualisieren
- Maschinenkatalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen
- Maschinenkatalog mit persistentem Zurückschreibcachedatenträger erstellen
- Startleistung mit MCSIO verbessern
- Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen
- Maschinenkatalog mit Verschlüsselung auf dem Host erstellen
- Maschinenkatalog mit doppelter Verschlüsselung erstellen
- Speicherort der Auslagerungsdatei bestimmen
- Szenarien zum Einrichten der Auslagerungsdatei
- Auslagerungsdateieinstellung angeben
- Auslagerungsdateieinstellungen ändern
- Katalog-VMs mit aktiviertem AMA bereitstellen
- Katalog mit Azure Spot-VMs erstellen
- Tags in allen Ressourcen kopieren

### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Sie können hierfür die Schnittstelle Vollständige Konfiguration oder PowerShell verwenden.

Informationen zur Benutzeroberfläche für die vollständige Konfiguration finden Sie unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.

Mit PowerShell:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie <!JEKYLL@5180@34> aus.
3. Erstellen oder aktualisieren Sie einen Katalog.
    - Gehen Sie zum Erstellen eines Katalogs wie folgt vor:
        a) Verwenden Sie den Befehl <!JEKYLL@5180@35> mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:
        <!JEKYLL@5180@36>

b) Beenden Sie die Erstellung des Maschinenkatalogs.

- Verwenden Sie zum Aktualisieren eines Katalogs den Befehl <!JEKYLL@5180@37> mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

  <!JEKYLL@5180@38>

### Azure-VM-Erweiterungen aktivieren

Führen Sie nach Auswahl der ARM-Vorlagenspezifikation die folgenden PowerShell-Befehle aus, um Azure-VM-Erweiterungen zu verwenden:

- Anzeige der Liste der unterstützten Azure VM-Erweiterungen: <!JEKYLL@5180@39>
- Hinzufügen von zusätzlichen VM-Erweiterungen: <!JEKYLL@5180@40>. Zum Beispiel: <!JEKYLL@5180@41>

  Beim Versuch, eines der folgenden Elemente hinzuzufügen, wird eine Fehlermeldung angezeigt:

  - Von Citrix definierte Erweiterung.
  - Vorhandene benutzerdefinierte Erweiterung.
  - Nicht unterstützte Konfigurationsschlüssel. Derzeit ist der unterstützte Konfigurationsschlüssel <!JEKYLL@5180@42>.

- Entfernen von Erweiterungen aus der Liste: <!JEKYLL@5180@43>. Sie können die selbst hinzugefügten Erweiterungen entfernen.

### Maschinenkataloge mit vertrauenswürdigem Start

Zur problemlosen Erstellung eines Maschinenkatalogs mit vertrauenswürdigem Start verwenden Sie:

- Ein Maschinenprofil mit vertrauenswürdigem Start
- Eine VM-Größe, die vertrauenswürdigen Start unterstützt
- Eine Windows-VM-Version, die vertrauenswürdigen Start unterstützt. Derzeit unterstützen Windows 10, Windows 11, Windows Server 2016, 2019 und 2022 den vertrauenswürdigen Start.

> **Wichtig:**
>
> MCS unterstützt die Erstellung eines neuen Katalogs mit VMs, für die vertrauenswürdiger Start aktiviert ist. Um einen vorhandenen persistenten Katalog und vorhandene VMs zu aktualisieren, müssen Sie jedoch das Azure-Portal verwenden. Sie können den vertrauenswürdigen Start eines nicht persistenten Katalogs nicht aktualisieren. Weitere Informationen finden Sie im Microsoft-Dokument Enable Trusted launch on existing Azure VMs.

Führen Sie den folgenden Befehl aus, um den Bestand des Citrix DaaS-Angebots anzuzeigen und zu ermitteln, ob die VM-Größe den vertrauenswürdigen Start unterstützt:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den folgenden Befehl aus:

   <!JEKYLL@5180@44>
4. Führen Sie <!JEKYLL@5180@45> aus.
5. Prüfen Sie den Wert des Attributs <!JEKYLL@5180@46>.

   - Wenn <!JEKYLL@5180@47> **True** ist, unterstützt die VM-Größe den vertrauenswürdigen Start.
   - Wenn <!JEKYLL@5180@48> **False**ist, unterstützt die VM-Größe den vertrauenswürdigen Start nicht.

Bei Azure-PowerShell können Sie den folgenden Befehl verwenden, um die VM-Größen zu ermitteln, die den vertrauenswürdigen Start unterstützen:

<!JEKYLL@5180@49>

Die folgenden Beispiele veranschaulichen, welche von dem Azure PowerShell-Befehl zurückgegebenen VMs den vertrauenswürdigen Start unterstützen.

- *Beispiel 1*: Wenn die Azure-VM nur Generation 1 unterstützt, unterstützt die VM keinen vertrauenswürdigen Start. Daher wird <!JEKYLL@5180@50> nicht angezeigt, wenn Sie den Azure PowerShell-Befehl ausgeführt haben.
- *Beispiel 2*: Wenn die Azure-VM nur Generation 2 unterstützt und der Wert von <!JEKYLL@5180@51> **True** ist, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start nicht.
- *Beispiel 3*: Wenn die Azure-VM nur Generation 2 unterstützt und <!JEKYLL@5180@52> nicht angezeigt wird, wenn Sie den PowerShell-Befehl ausgeführt haben, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start.

Weitere Informationen zum vertrauenswürdigen Start für virtuelle Azure-Maschinen finden Sie in dem Microsoft-Dokument Vertrauenswürdiger Start für Azure-VMs.

#### Maschinenkatalog mit vertrauenswürdigem Start erstellen

1. Erstellen Sie ein Masterimage, für das vertrauenswürdiger Start aktiviert ist. Weitere Informationen finden Sie in der Microsoft-Dokumentation Unterstützte Images für VMs mit vertrauenswürdigem Start.

2. Erstellen Sie eine VM oder Vorlagenspezifikation mit Sicherheitstyp als **virtuelle Maschinen mit vertrauenswürdigem Start**. Weitere Informationen zum Erstellen einer VM oder Vorlagenspezifikation finden Sie im Microsoft-Dokument Bereitstellen eines virtuellen Computers mit vertrauenswürdigem Start.
3. Erstellen Sie einen Maschinenkatalog mithilfe der Benutzeroberfläche für die vollständige Konfiguration oder von PowerShell-Befehlen.

   - Wenn Sie die Benutzeroberfläche für die vollständige Konfiguration nutzen möchten, finden Sie weitere Informationen unter Maschinenkataloge unter Verwendung eines Azure Resource Managerimages über die Benutzeroberfläche für die vollständige Konfiguration erstellen.
   - Wenn Sie PowerShell-Befehle verwenden möchten, verwenden Sie den Befehl <!JEKYLL@5180@53> mit der VM oder Vorlagenspezifikation als Maschinenprofileingabe. Eine vollständige Liste der Befehle zum Erstellen eines Katalogs finden Sie unter Erstellen eines Katalogs.

     Beispiel für <!JEKYLL@5180@54> mit VM als Maschinenprofileingabe:

     <!JEKYLL@5180@55>

     Beispiel für <!JEKYLL@5180@56> mit Vorlagenspezifikation als Maschinenprofileingabe:

     <!JEKYLL@5180@57>

#### Fehler beim Erstellen von Maschinenkatalogen mit vertrauenswürdigem Start

Beim Erstellen eines Maschinenkatalogs mit vertrauenswürdigem Start treten in den folgenden Szenarien Fehler auf:

| Szenario | Fehler |
|---|---|
| Sie wählen beim Erstellen eines nicht verwalteten Katalogs ein Maschinenprofil aus. | <!JEKYLL@5180@58> |
| Sie wählen beim Erstellen eines Katalogs mit einem nicht verwalteten Datenträger als Masterimage ein Maschinenprofil, das den vertrauenswürdigen Start unterstützt. | <!JEKYLL@5180@59> |
| Sie wählen beim Erstellen eines verwalteten Katalogs mit einer Masterimagequelle, deren Sicherheitstyp “vertrauenswürdiger Start”ist, kein Maschinenprofil aus. | <!JEKYLL@5180@60> |

| Szenario | Fehler |
| --- | --- |
| Sie wählen ein Maschinenprofil aus, dessen Sicherheitstyp sich von dem des Masterimages unterscheidet. | <!JEKYLL@5180@61> |
| Sie wählen eine VM-Größe, die den vertrauenswürdigen Start nicht unterstützt, verwenden aber beim Erstellen eines Katalogs ein Masterimage, das den vertrauenswürdigen Start unterstützt. | <!JEKYLL@5180@62> |

### Eigenschaftswerte für Maschinenprofile verwenden

Der Maschinenkatalog verwendet die folgenden Eigenschaften, die in den benutzerdefinierten Eigenschaften definiert sind:

- Verfügbarkeitszone
- ID der dedizierten Hostgruppe
- ID des Datenträgerverschlüsselungssatzes
- Betriebssystemtyp
- Lizenztyp
- Speichertyp

Wenn diese benutzerdefinierten Eigenschaften nicht explizit definiert sind, werden die Eigenschaftswerte über die ARM-Vorlagenspezifikation oder VM festgelegt, je nachdem, was als Maschinenprofil verwendet wird. Wenn <!JEKYLL@5180@63> nicht angegeben ist, wird der Wert über das Maschinenprofil festgelegt.

> **Hinweis:**
>
> Wenn einige der Eigenschaften im Maschinenprofil fehlen und nicht in den benutzerdefinierten Eigenschaften definiert sind, werden die Standardwerte der Eigenschaften angewendet, soweit zutreffend.

Im folgenden Abschnitt werden einige Szenarios für <!JEKYLL@5180@64> und <!JEKYLL@5180@65> beschrieben, wenn für <!JEKYLL@5180@66> entweder alle Eigenschaften definiert sind oder Werte aus dem MachineProfile abgeleitet werden.

- New-ProvScheme-Szenarios
  - Im MachineProfile sind alle Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel:

<!JEKYLL@5180@67>

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

<!JEKYLL@5180@68>

- Im MachineProfile sind einige Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel: Im MachineProfile sind nur LicenseType und OsType festgelegt.

  <!JEKYLL@5180@69>

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5180@70>

- Sowohl im MachineProfile als auch in CustomProperties sind alle Eigenschaften definiert. Beispiel:

  <!JEKYLL@5180@71>

  Benutzerdefinierte Eigenschaften haben Priorität. Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5180@72>

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Beispiel:

  * CustomProperties definieren LicenseType und StorageAccountType
  * MachineProfile definiert LicenseType, OsType und Zonen

  <!JEKYLL@5180@73>

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5180@74>

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Darüber hinaus ist ServiceOffering nicht definiert. Beispiel:

  * CustomProperties definieren StorageType
  * MachineProfile definiert LicenseType

  <!JEKYLL@5180@75>

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5180@76>

  - Wenn der OsType weder in CustomProperties noch im MachineProfile definiert ist, gilt Folgendes:
    * Der Wert wird aus dem Masterimage gelesen.
    * Ist das Masterimage ein nicht verwalteter Datenträger, ist der OsType auf Windows eingestellt. Beispiel:

    <!JEKYLL@5180@77>

    Der Wert aus dem Masterimage wird in die benutzerdefinierten Eigenschaften geschrieben, in diesem Fall Linux.

    <!JEKYLL@5180@78>

- Set-ProvScheme-Szenarios
  - Ein vorhandener Katalog mit:
    * CustomProperties für <!JEKYLL@5180@79> und OsType
    * MachineProfile <!JEKYLL@5180@80>, das Zonen definiert
  - Updates:
    * MachineProfile mpB.vm, das StorageAccountType definiert
    * Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der LicenseType und OsType definiert

    <!JEKYLL@5180@81>

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    <!JEKYLL@5180@82>
  - Ein vorhandener Katalog mit:
    * CustomProperties für <!JEKYLL@5180@83> und OsType
    * MachineProfile <!JEKYLL@5180@84>, das StorageAccountType und LicenseType definiert
  - Updates:
    * Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der StorageAccountType und OsType definiert.

    <!JEKYLL@5180@85>

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    <!JEKYLL@5180@86>

- Ein vorhandener Katalog mit:
  - CustomProperties für <!JEKYLL@5180@87> und OsType
  - MachineProfile <!JEKYLL@5180@88>, das Zonen definiert
- Updates:
  - Ein MachineProfile mpB.vm, das StorageAccountType und LicenseType definiert
  - <!JEKYLL@5180@89> ist nicht angegeben

<!JEKYLL@5180@90>

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

<!JEKYLL@5180@91>

### Verfügbarkeitszonen mit PowerShell konfigurieren

Mit <!JEKYLL@5180@92> in PowerShell können Sie die Elemente des Citrix DaaS-Angebots anzeigen. Um beispielsweise das *Serviceangebot Eastern US* <!JEKYLL@5180@93> anzuzeigen:

<!JEKYLL@5180@94>

Zum Anzeigen der Zonen verwenden Sie den Parameter <!JEKYLL@5180@95>:

<!JEKYLL@5180@96>

Werden keine Verfügbarkeitszone angegeben, bleibt die Art und Weise, wie Maschinen bereitgestellt werden, unverändert.

Um Verfügbarkeitszonen über PowerShell zu konfigurieren, verwenden Sie die benutzerdefinierte Eigenschaft **Zones** von <!JEKYLL@5180@97>. Die Eigenschaft **Zones** definiert eine Liste von Verfügbarkeitszonen für das Provisioning von Maschinen. Diese Zonen können eine oder mehrere Verfügbarkeitszonen enthalten. Beispiel: <!JEKYLL@5180@98> für die Zonen 1 und 3.

Verwenden Sie den Befehl <!JEKYLL@5180@99>, um die Zonen für ein Provisioningschema zu aktualisieren.

Wird eine ungültige Zone angegeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung mit Anweisungen zur Korrektur des ungültigen Befehls angezeigt.

> **Tipp:**
>
> Wenn Sie eine ungültige benutzerdefinierte Eigenschaft angeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung angezeigt.

**Ergebnis der gleichzeitigen Verwendung von Hostgruppen- und Azure-Verfügbarkeitszonen**

Sie können im Voraus überprüfen, ob ein Maschinenkatalog mit der in der benutzerdefinierten Eigenschaft angegebenen Verfügbarkeitszone und der Zone der Hostgruppe erstellt werden kann. Die Katalogerstellung schlägt fehl, wenn die Verfügbarkeitszone der benutzerdefinierten Eigenschaft nicht mit der Hostgruppenzone übereinstimmt.

Informationen zum Konfigurieren von Verfügbarkeitszonen über PowerShell finden Sie unter Konfigurieren von Verfügbarkeitszonen über PowerShell.

Informationen zu dedizierten Azure-Hosts finden Sie unter Dedizierte Azure-Hosts.

Die folgende Tabelle beschreibt die verschiedenen Kombinationen aus Verfügbarkeits- und Hostgruppenzone und zeigt an, wann die Maschinenkatalogerstellung gelingt bzw. fehlschlägt.

| Hostgruppenzone | Verfügbarkeitszone in benutzerdefinierter Eigenschaft | Ergebnis der Maschinenkatalogerstellung |
|---|---|---|
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Nicht angegeben | Erfolgreich. Maschinen werden in der Hostgruppenzone erstellt. |
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Mit Hostgruppenzone identisch. Die Zone in der benutzerdefinierten Eigenschaft ist beispielsweise auf 1 festgelegt. | Erfolgreich. Maschinen werden in Zone 1 erstellt. |
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Nicht mit Hostgruppenzone identisch. Die Zone in der benutzerdefinierten Eigenschaft ist beispielsweise auf 2 festgelegt. | Da Verfügbarkeitszone und Hostgruppenzone nicht übereinstimmen, schlägt die Katalogerstellung bei der Vorabprüfung aufgrund eines relevanten Fehlers fehlt. |
| Festgelegt. Die Hostgruppe befindet sich beispielsweise in Zone 1. | Es sind mehrere Zonen festgelegt. Beispielsweise sind Zonen in den benutzerdefinierten Eigenschaften auf 1,2 oder 2,3 festgelegt. | Da Verfügbarkeitszone und Hostgruppenzone nicht übereinstimmen, schlägt die Katalogerstellung bei der Vorabprüfung aufgrund eines relevanten Fehlers fehlt. |

| Hostgruppenzone | Verfügbarkeitszone in benutzerdefinierter Eigenschaft | Ergebnis der Maschinenkatalogerstellung |
|---|---|---|
| Nicht festgelegt. Die Zone der Hostgruppe ist beispielsweise <!JEKYLL@5180@100>. | Nicht angegeben | Wenn die festgelegte Verfügbarkeitszone mit der Hostgruppenzone übereinstimmt (d. h. keine Zone), ist die Katalogerstellung erfolgreich. Maschinen werden in keiner Zone erstellt. |
| Nicht festgelegt. Die Zone der Hostgruppe ist beispielsweise <!JEKYLL@5180@101>. | Festgelegt. Beispielsweise sind die Zonen in der benutzerdefinierten Eigenschaft auf eine oder mehrere Zonen festgelegt. | Da Verfügbarkeitszone und Hostgruppenzone nicht übereinstimmen, schlägt die Katalogerstellung bei der Vorabprüfung aufgrund eines relevanten Fehlers fehlt |

### VMs auf dedizierten Azure-Hosts bereitstellen

Sie können mit MCS das Provisioning von VMs auf dedizierten Azure-Hosts ausführen. Vor dem Provisioning von VMs auf dedizierten Azure-Hosts führen Sie folgende Schritte aus:

- Erstellen Sie eine Hostgruppe.
- Erstellen Sie Hosts in der Hostgruppe.
- Vergewissern Sie sich, dass genügend Hostkapazität für die Erstellung von Katalogen und virtuellen Maschinen reserviert ist.

Sie können einen Katalog mit Maschinen erstellen, deren Host-Tenancy über das folgende PowerShell-Skript definiert wird:

<!JEKYLL@5180@102>

Wenn Sie mit MCS virtuelle Maschinen auf dedizierten Azure-Hosts bereitstellen, berücksichtigen Sie Folgendes:

- Ein *dedizierter Host* ist eine Katalogeigenschaft und kann nach der Katalogerstellung nicht mehr geändert werden. Dedizieren für Mandanten wird derzeit in Azure nicht unterstützt.
- Bei Verwendung des Parameters <!JEKYLL@5180@103> ist eine vorkonfigurierte Azure-Hostgruppe in der Region der Hostingeinheit erforderlich.
- Die automatische Platzierung in Azure ist erforderlich. Das Feature beantragt das Onboarding des mit der Hostgruppe verknüpften Abonnements. Weitere Informationen finden Sie unter VM

Scale Set on Azure Dedicated Hosts - Public Preview. Wenn die automatische Platzierung nicht aktiviert ist, tritt in MCS bei der Katalogerstellung ein Fehler auf.

## Speichertypen konfigurieren

Wählen Sie Speichertypen für virtuelle Maschinen in Azure-Umgebungen, die MCS verwenden. Für Ziel-VMs unterstützt MCS Folgendes:

- OS-Datenträger: SSD Premium, SSD oder HDD
- Zurückschreibcache-Datenträger: SSD Premium, SSD oder HDD

Berücksichtigen Sie bei Verwendung dieser Speichertypen Folgendes:

- Ihre VM muss den ausgewählten Speichertyp unterstützen.
- Wenn Ihre Konfiguration einen kurzlebigen Azure-Datenträger enthält, wird keine Option für die Einstellung des Zurückschreibcache-Datenträgers angeboten.

> **Tipp:**
>
> <!JEKYLL@5180@104> ist für einen Betriebssystemspeichertyp und mit Speicherkonto konfiguriert. <!JEKYLL@5180@105> ist für den Zurückschreibcache konfiguriert. Für einen normalen Katalog ist <!JEKYLL@5180@106> erforderlich. Wenn <!JEKYLL@5180@107> nicht konfiguriert ist, wird <!JEKYLL@5180@108> als Standard für <!JEKYLL@5180@109> verwendet.

Wenn WBCDiskStorageType nicht konfiguriert ist, wird StorageType als Standard für WBCDiskStorageType verwendet.

### Speichertypen für VMs konfigurieren

Verwenden Sie den Parameter <!JEKYLL@5180@110> in <!JEKYLL@5180@111>, um Speichertypen für VMs zu konfigurieren. Verwenden Sie den <!JEKYLL@5180@112>-Befehl, um den Wert des <!JEKYLL@5180@113>-Parameters in einem bestehenden Katalog auf einen der unterstützten Speichertypen zu aktualisieren.

Im Folgenden finden Sie einen Beispielsatz für den Parameter <!JEKYLL@5180@114> in einem Provisioningschema:

<!JEKYLL@5180@115>

## Zonenredundanten Speicher aktivieren

Sie können bei der Katalogerstellung einen zonenredundanten Speicher (ZRS) auswählen. Ihre Azure Managed Disk wird dann synchron über mehrere Verfügbarkeitszonen repliziert, sodass Sie Ihre Daten

bei einem Ausfall in einer Zone mithilfe der Redundanz in den übrigen Zonen wiederherstellen können.

In den benutzerdefinierten Speichertypeigenschaften können Sie **Premium_ZRS** und **Standard-SSD_ZRS** angeben. Der ZRS-Speicher kann mithilfe vorhandener benutzerdefinierter Eigenschaften oder über die Vorlage **MachineProfile** festgelegt werden. Der ZRS-Speicher wird auch mit dem Befehle <!JEKYLL@5180@116> und den Parametern <!JEKYLL@5180@117> und <!JEKYLL@5180@118> unterstützt. Sie können bestehende VMs von LRS- auf ZRS-Speicher umstellen.

> **Hinweis:**
>
> - <!JEKYLL@5180@119> gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
> - <!JEKYLL@5180@120> mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

**Einschränkungen:**

- Nur für verwaltete Datenträger unterstützt
- Nur mit Premium- und Standard-SSDs unterstützt
- Keine Unterstützung mit <!JEKYLL@5180@121>
- Nur in bestimmten Regionen verfügbar.
- Beim Erstellen großer Mengen an ZRS-Datenträgern sinkt die Leistung von Azure. Fahren Sie die Maschinen daher beim ersten Einschalten gestaffelt hoch (weniger als 300 Maschinen gleichzeitig).

#### Zonenredundanten Speicher als Datenträgerspeichertyp festlegen

Sie können einen zonenredundanten Speicher bei der Katalogerstellung auswählen oder den Speichertyp in einem vorhandenen Katalog aktualisieren.

#### Zonenredundanten Speicher mithilfe von PowerShell-Befehlen auswählen

Wenn Sie einen neuen Katalog in Azure mit dem Powershell-Befehl <!JEKYLL@5180@122> erstellen, verwenden Sie für <!JEKYLL@5180@123> den Wert <!JEKYLL@5180@124>.
Beispiel:

<!JEKYLL@5180@125>

Nach Auswahl dieses Werts prüft eine dynamische API, ob er ordnungsgemäß verwendet werden kann. Folgende Ausnahmen können auftreten, wenn ZRS für Ihren Katalog nicht zulässig ist:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: Die benutzerdefinierte Eigenschaft “StorageTypeAtShutdown”kann nicht mit ZRS verwendet werden.

- **StorageAccountTypeNotSupportedInRegion**: Diese Ausnahme tritt auf, wenn Sie versuchen, ZRS in einer nicht unterstützten Azure-Region zu verwenden.
- **ZrsRequiresManagedDisks**: Sie können zonenredundanten Speicher nur mit verwalteten Datenträgern verwenden.

Sie können den Datenträgerspeichertyp mit den folgenden benutzerdefinierten Eigenschaften festlegen:

- <!JEKYLL@5180@126>
- <!JEKYLL@5180@127>
- <!JEKYLL@5180@128>

> **Hinweis:**
>
> Bei der Katalogerstellung wird der Betriebssystemdatenträger <!JEKYLL@5180@129> des Maschinenprofils verwendet, wenn die benutzerdefinierten Eigenschaften nicht festgelegt sind.

## Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen

Sie können Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen, während Sie einen Maschinenkatalog erstellen, einen vorhandenen Maschinenkatalog aktualisieren und vorhandene VMs aktualisieren.

Sie können eine VM- oder Vorlagenspezifikation als Maschinenprofilquelle erstellen.

### Wichtige Schritte

1. Richten Sie die erforderlichen IDs in Azure ein. Sie müssen diese IDs in der Vorlagenspezifikation angeben.
    - Speicherkonto
    - Protokollanalysen-Workspace
    - Event Hub-Namespace mit den Standardtarifpreisen
2. Erstellen Sie eine Maschinenprofilquelle.
3. Erstellen Sie einen neuen Maschinenkatalog, aktualisieren Sie einen vorhandenen Katalog oder aktualisieren Sie vorhandene VMs.

### Erforderliche IDs in Azure einrichten

Richten Sie eine der folgenden Optionen in Azure ein:

- Speicherkonto
- Protokollanalysen-Workspace
- Event Hub-Namespace mit den Standardtarifpreisen

**Speicherkonto einrichten** Erstellen Sie ein Standardspeicherkonto in Azure. Geben Sie in der Vorlagenspezifikation die vollständige Resourcen-ID für das Speicherkonto als <!JEKYLL@5180@130> an.

Sobald VMs so eingerichtet sind, dass sie Daten im Speicherkonto protokollieren, finden Sie die Daten unter dem Container <!JEKYLL@5180@131>.

**Workspace für Protokollanalysen einrichten** Erstellen Sie einen Workspace für Protokollanalysen. Geben Sie in der Vorlagenspezifikation die vollständige Ressourcen-ID für den Protokollanalysen-Workspace als workspaceId an.

Sobald VMs so eingerichtet sind, dass sie Daten im Workspace protokollieren, können Daten unter "Protokolle"in Azure abgefragt werden. Sie können den folgenden Befehl in Azure unter "Protokolle" ausführen, um die Anzahl aller von einer Ressource protokollierten Metriken anzuzeigen:

'AzureMetrics

**Event Hub einrichten** Gehen Sie wie folgt vor, um einen Event Hub im Azure-Portal einzurichten:

1. Erstellen Sie einen Event Hub-Namespace mit den Standardtarifpreisen.
2. Erstellen Sie einen Event Hub unter dem Namespace.
3. Navigieren Sie im Event Hub zu **Aufzeichnung**. Schalten Sie den Schalter EIN, um mit dem Avro-Ausgabetyp aufzunehmen.
4. Erstellen Sie einen neuen Container in einem vorhandenen Speicherkonto, um die Protokolle zu erfassen.
5. Geben Sie in der Vorlagenspezifikation `eventHubAuthorizationRuleId` im folgenden Format an: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Geben Sie den Namen des Event Hubs an.

Sobald VMs so eingerichtet sind, dass sie Daten im Event Hub protokollieren, werden die Daten im konfigurierten Speichercontainer erfasst.

#### Maschinenprofilquelle erstellen

Sie können eine VM- oder Vorlagenspezifikation als Maschinenprofilquelle erstellen.

**VM-basiertes Maschinenprofil mit Diagnoseeinstellungen erstellen** Wenn Sie eine VM als Maschinenprofil erstellen möchten, richten Sie zunächst die Diagnoseeinstellungen auf der Vorlagen-VM selbst ein. Sie können die detaillierten Anweisungen in der Microsoft-Dokumentation Diagnose-Einstellungen in Azure Monitor nachlesen.

Sie können die folgenden Befehle ausführen, um zu überprüfen, ob der VM oder Netzwerkkarte jetzt Diagnoseeinstellungen zugeordnet sind:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
<!--NeedCopy-->
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
<!--NeedCopy-->
```

**Erstellen Sie ein auf Vorlagenspezifikationen basierendes Maschinenprofil mit Diagnoseeinstellungen** Wenn Sie eine VM verwenden möchten, für die bereits Diagnoseeinstellungen aktiviert sind, und sie in eine ARM-Vorlagenspezifikation exportieren möchten, werden diese Einstellungen nicht automatisch in die Vorlage aufgenommen. Sie müssen die Diagnoseeinstellungen in der ARM-Vorlage manuell hinzufügen oder ändern.

Wenn Sie jedoch eine VM als Maschinenprofil verwenden möchten, stellt MCS sicher, dass die kritischen Diagnoseeinstellungen genau erfasst und auf die Ressourcen in Ihrem MCS-Katalog angewendet werden.

1. Erstellen Sie eine Standardvorlagenspezifikation, die eine VM und mindestens eine Netzwerkkarte definiert.
2. Fügen Sie zusätzliche Ressourcen hinzu, um die Diagnoseeinstellungen gemäß der Spezifikation bereitzustellen: Microsoft.Insights diagnosticSettings. Verweisen Sie für den Bereich anhand des Namens mit einer teilweisen ID entweder auf eine VM oder eine Netzwerkkarte, die in der Vorlage enthalten ist. Um beispielsweise Diagnoseeinstellungen zu erstellen, die an eine VM mit dem Namen Test-VM in der Vorlagenspezifikation angehängt sind, geben Sie den Bereich wie folgt an:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   <!--NeedCopy-->
   ```

3. Verwenden Sie die Vorlagenspezifikation als Maschinenprofilquelle.

#### Katalog mit Diagnoseeinstellungen erstellen oder aktualisieren

Nachdem Sie eine Maschinenprofilquelle erstellt haben, können Sie jetzt einen Maschinenkatalog mit einem `New-ProvScheme`-Befehl erstellen, einen vorhandenen Maschinenkatalog mit einem `Set-ProvScheme`-Befehl aktualisieren und vorhandene VMs mithilfe eines `Request-ProvVMUpdate` -Befehls aktualisieren.

### Windows-Lizenz überprüfen

Sie können mit folgendem PowerShell-Befehl überprüfen, ob eine VM den Lizenzierungsvorteil nutzt: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Bei Windows Server-Lizenzen muss der Lizenztyp **Windows_Server** sein. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Bei Windows-Clientlizenzen muss der Lizenztyp **Windows_Client** sein. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Alternativ können Sie zur Überprüfung das PowerShell-SDK `Get-Provscheme` verwenden. Beispiel: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Weitere Informationen zu diesem Cmdlet finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

### Linux-Lizenz konfigurieren

Bei Verwendung eigener Linux-Lizenzen (Bring Your Own Subscription oder BYOS) müssen Sie für die Software nicht zahlen. Die BYOS-Gebühr umfasst nur die Hardware für die Rechenleistung. Es gibt zwei Arten von Lizenzen:

- **RHEL_BYOS**: Um den Typ RHEL_BYOS zu verwenden, aktivieren Sie Red Hat Cloud Access in Ihrem Azure-Abonnement.
- **SLES_BYOS**: Die BYOS-Versionen von SLES beinhalten Unterstützung von SUSE.

Sie können den LicenseType-Wert unter `New-ProvScheme` und `Set-ProvScheme` auf Linux-Optionen setzen.

Beispiel für das Festlegen von LicenseType auf RHEL_BYOS unter `New-ProvScheme`:

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog" -
    RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
        instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
         Value="true" /><Property xsi:type="StringProperty" Name="
        StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
        StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
         xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
        xsi:type="StringProperty" Name="LicenseType" Value="RHEL_BYOS" /></
        CustomProperties>'
2 <!--NeedCopy-->
```

Beispiel für das Festlegen von LicenseType auf SLES_BYOS unter `Set-ProvScheme`:

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
       '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
       Value="true" /><Property xsi:type="StringProperty" Name="
      StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
       xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
      xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
      CustomProperties>'
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn der Wert `LicenseType` leer ist, werden als Standardwert die Azure Windows-Serverlizenz oder Azure Linux-Lizenz verwendet, abhängig vom OsType-Wert.

Beispiel für einen leeren Wert für LicenseType:

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
       '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
       Value="true" /><Property xsi:type="StringProperty" Name="
      StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
       xsi:type="StringProperty" Name="OsType" Value="Linux" /></
      CustomProperties>'
2 <!--NeedCopy-->
```

### Maschinenkatalog mit kurzlebigem Azure-Datenträger erstellen

Berücksichtigen Sie die folgenden Einschränkungen, wenn Sie das Provisioning kurzlebiger Betriebssystemdatenträger mit `New-ProvScheme` durchführen:

- Die für den Katalog verwendete VM-Größe muss kurzlebige Betriebssystemdatenträger unterstützen.

- Der einer VM-Größe zugeordnete Cachedatenträger oder temporäre Datenträger muss größer oder genauso groß sein wie der Betriebssystemdatenträger.
- Der temporäre Datenträger muss größer als der Cachedatenträger sein.

Beachten Sie auch diese Einschränkungen in folgenden Fällen:

- Provisioningschema erstellen
- Provisioningschema ändern
- Images aktualisieren

Zur Verwendung kurzlebiger Datenträger müssen Sie die benutzerdefinierte Eigenschaft `UseEphemeralOsDisk` bei der Ausführung von `New-ProvScheme` auf **true** festlegen.

> **Hinweis:**
>
> Wenn die benutzerdefinierte Eigenschaft `UseEphemeralOsDisk` auf **false** festgelegt oder kein Wert angegeben wird, verwenden alle bereitgestellten VDAs weiterhin einen bereitgestellten Betriebssystemdatenträger.

Nachfolgend finden Sie Beispiele benutzerdefinierter Eigenschaften zur Verwendung im Provisioningschema:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaMaximum",
```

```
                    "Value": "10"
                }
    ,
                {

                    "Name": "LicenseType",
                    "Value": "Windows_Server"
                }
    ,
                {

                    "Name": "UseEphemeralOsDisk",
                    "Value": "true"
                }

            ],
<!--NeedCopy-->
```

#### Kurzlebigen Datenträger für einen bestehenden Katalog konfigurieren

Verwenden Sie zum Konfigurieren eines kurzlebigen Azure-Betriebssystemdatenträgers für einen bestehenden Katalog den Parameter `UseEphemeralOsDisk` in `Set-ProvScheme`. Setzen Sie den Wert des Parameters `UseEphemeralOsDisk` auf **true**.

> **Hinweis:**
>
> Um dieses Feature zu nutzen, müssen Sie auch die Parameter `UseManagedDisks` und `UseSharedImageGallery` aktivieren.

Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
    "true" />
<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
    true" />
</CustomProperties>'
<!--NeedCopy-->
```

### Azure Compute Gallery konfigurieren

Mit dem Befehl `New-ProvScheme` erstellen Sie ein Provisioningsschema mit Azure Compute Gallery-Unterstützung. Verwenden Sie den Befehl `Set-ProvScheme`, um dieses Feature für ein Provision-

ingschema zu aktivieren bzw. deaktivieren und um die Replikatquote und die Anzahl maximaler Replikate zu ändern.

Zur Unterstützung der Azure Compute Gallery-Funktion wurden Provisioningschemata um drei benutzerdefinierte Eigenschaften erweitert:

`UseSharedImageGallery`

- Legt fest, ob die Azure Compute Gallery zum Speichern der veröffentlichten Images verwendet wird. Bei Auswahl von **True** wird das Image als Azure Compute Gallery-Image gespeichert. Andernfalls wird es als Snapshot gespeichert.
- Gültige Werte sind **True** und **False**.
- Der Standardwert bei nicht definierter Eigenschaft ist **False**.

`SharedImageGalleryReplicaRatio`

- Definiert das Verhältnis von Maschinen zu Replikaten der Galerie-Imageversion.
- Gültige Werte sind ganze Zahlen größer als 0.
- Bei nicht definierter Eigenschaft werden Standardwerte verwendet. Der Standardwert für persistente Betriebssystemdatenträger beträgt 1000 und der Standardwert für nicht-persistente Betriebssystemdatenträger beträgt 40.

`SharedImageGalleryReplicaMaximum`

- Definiert die Anzahl maximaler Replikate für jede Galerie-Imageversion.
- Gültige Werte sind ganze Zahlen größer als 0.
- Der Standardwert bei nicht definierter Eigenschaft ist 10.
- Azure unterstützt derzeit bis zu 10 Replikate pro Galerie-Imageversion. Wenn diese Eigenschaft auf einen Wert festgelegt ist, der den Azure-Höchstwert übersteigt, versucht MCS, den angegebenen Wert zu verwenden. Azure generiert einen Fehler, der von MCS protokolliert wird, und die aktuelle Replikatanzahl wird unverändert beibehalten.

> **Tipp:**
>
> Wenn Sie die Azure Compute Gallery zum Speichern eines veröffentlichten Images für Kataloge verwenden, die mit MCS bereitgestellt werden, legt MCS die Anzahl der Katalogimageversionsreplikate basierend auf der Anzahl der Maschinen im Katalog, der Replikatquote und der Anzahl maximaler Replikate fest. Zur Berechnung der Replikatanzahl wird die Maschinenanzahl im Katalog durch die Replikatquote dividiert (und auf den nächsten Ganzzahlwert aufgerundet) und dann gemäß der Anzahl maximaler Replikate begrenzt. Ein Beispiel: Bei eine Replikatquote von 20 und einem Höchstwert von 5 wird für 0–20 Maschinen ein Replikat erstellt, für 21–40 Maschinen 2 Replikate, für 41–60 Maschinen 3 Replikate, für 61–80 Maschinen 4 Replikate und für 81 Maschinen (und mehr) 5 Replikate.

**Anwendungsfall: Aktualisieren der Azure Compute Gallery-Replikatquote und der Anzahl maximaler Replikate**

Der vorhandene Maschinenkatalog verwendet Azure Compute Gallery. Verwenden Sie den Befehl `Set-ProvScheme`, um die benutzerdefinierten Eigenschaften für alle vorhandenen Maschinen im Katalog und alle zukünftigen Maschinen zu aktualisieren:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

**Anwendungsfall: Konvertieren eines Snapshot-Katalogs in einen Azure Compute Gallery-Katalog**

Führen Sie für diesen Anwendungsfall folgende Schritte aus:

1. Führen Sie `Set-ProvScheme` aus, wobei der Flag `UseSharedImageGallery` auf **True** gesetzt ist. Fügen Sie optional die Eigenschaften `SharedImageGalleryReplicaRatio` und `SharedImageGalleryReplicaMaximum` hinzu.
2. Aktualisieren Sie den Katalog.
3. Starten Sie die Maschinen neu, um ein Update zu erzwingen.

Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Tipp:**
>
> Die Parameter `SharedImageGalleryReplicaRatio` und `SharedImageGalleryReplicaMaximum`

> sind nicht erforderlich. Nach Abschluss des Befehls `Set-ProvScheme` ist das Azure Compute Gallery-Image noch nicht erstellt. Sobald der Katalog für die Verwendung der Galerie konfiguriert ist, speichert das nächste Katalogupdate das veröffentlichte Image in der Galerie. Der Befehl zum Katalogupdate erstellt die Galerie, das Galerie-Image und die Imageversion. Durch den Neustart der Maschinen werden sie aktualisiert, und es wird gegebenenfalls die Replikatanzahl aktualisiert. Alle vorhandenen nicht-persistenten Maschinen werden dann mit dem Azure Compute Gallery-Image zurückgesetzt, und alle neu bereitgestellten Maschinen werden mit diesem Image erstellt. Der alte Snapshot wird innerhalb weniger Stunden automatisch bereinigt.

**Anwendungsfall: Konvertieren eines Azure Compute Gallery-Katalogs in einen Snapshot-Katalog**

Führen Sie für diesen Anwendungsfall folgende Schritte aus:

1. Führen Sie `Set-ProvScheme` aus, wobei der Flag `UseSharedImageGallery` auf **False** gesetzt oder nicht definiert ist.
2. Aktualisieren Sie den Katalog.
3. Starten Sie die Maschinen neu, um ein Update zu erzwingen.

Beispiel:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance"> <Property xsi:type="StringProperty" Name="StorageType"
     Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
     UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
     Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
2 <!--NeedCopy-->
```

> **Tipp:**
>
> Im Gegensatz zum Update von einem Snapshot-Katalog auf einen Azure Image Gallery-Katalog sind die benutzerdefinierten Daten für jede Maschine noch nicht auf die neuen benutzerdefinierten Eigenschaften aktualisiert. Führen Sie den folgenden Befehl aus, um die ursprünglichen benutzerdefinierten Azure Compute Gallery-Eigenschaften anzuzeigen: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Nach Abschluss des Befehls `Set-ProvScheme` ist der Imagesnapshot noch nicht erstellt. Sobald konfiguriert ist, dass der Katalog nicht mehr die Galerie verwendet, speichert das nächste Katalogupdate das veröffentlichte Image als Snapshot. Alle vorhandenen nicht-persistenten Maschinen werden dann mit dem Snapshot zurückgesetzt, und alle neu bereitgestellten Maschinen werden aus dem Snapshot erstellt. Durch Neustart werden die Maschinen aktualisiert. Die benutzerdefinierten Maschinendaten werden dabei aktualisiert und zeigen an, dass `UseSharedImageGallery`

> auf **False** gesetzt ist. Die alten Azure Compute Gallery-Assets (Galerie, Image und Version) werden automatisch innerhalb weniger Stunden bereinigt.

### Katalog mit mehreren Netzwerkkarten pro VM erstellen oder aktualisieren

MCS unterstützt mehrere Netzwerkkarten pro VM. Sie können mehrere Netzwerkkarten einer VM mehreren Subnetzen zuordnen, die sich allerdings im selben virtuellen Netzwerk (VNet) befinden müssen. Sie können für Folgendes einen PowerShell-Befehl verwenden:

- Katalog mit mehreren Netzwerkkarten pro VM erstellen
- Katalogkonfiguration aktualisieren, sodass eine VM mehrere Netzwerkkarten hat, damit neu erstellte VMs über mehrere Netzwerkkarten verfügen
- VM für mehrere Netzwerkkarten aktualisieren

Sie können Maschinenkataloge (auf einem Maschinenprofil basierende und nicht auf einem Maschinenprofil basierende) erstellen bzw. aktualisieren, damit VMs mehrere Netzwerkkarten haben. Derzeit müssen Maschinen in einem auf einem Maschinenprofil basierenden Katalog die gleiche Anzahl an Netzwerkkarten haben, wie die Maschinenprofilquelle.

Eigenschaften wie beschleunigter Netzwerkbetrieb und Netzwerksicherheitsgruppe werden aus der Maschinenprofilquelle abgeleitet.

> **Hinweis:**
>
> Die VM-Größe muss die Anzahl an Netzwerkkarten und den entsprechenden beschleunigten Netzwerkbetrieb unterstützen, andernfalls erhalten Sie eine Fehlermeldung.

Sie können die maximale Anzahl an Netzwerkkarten für bestimmte VM-Größen abrufen. Die PowerShell-Eigenschaft `MaxNetworkInterfaces` zeigt die maximale Anzahl an Netzwerkkarten an, wenn Sie den PowerShell-Befehl `get-item` mit dem Parameter `AdditionalData` ausführen.

#### Maximale Anzahl an Netzwerkkarten abrufen

Gehen Sie zum Abrufen der maximale Anzahl an Netzwerkkarten folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster vom Delivery Controller-Host aus.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den Befehl `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` aus, um alle verfügbaren VM-Größen aufzulisten.

4. Führen Sie `get-item -Path "XDHyp:\Connections\abc-connection\East US .region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering ").AdditionalData` aus.
5. `MaxNetworkInterfaces` zeigt die maximale Anzahl an Netzwerkkarten.

#### Katalog mit mehreren Netzwerkkarten pro VM erstellen

Zum Erstellen eines Katalogs mit mehreren Netzwerkkarten pro VM gehen Sie folgendermaßen vor:

1. Öffnen Sie ein PowerShell-Fenster vom Delivery Controller-Host aus.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden.
4. Erstellen Sie das Provisioningschema:

   - Wenn Sie einen nicht auf Maschinenprofilen basierenden Maschinenkatalog erstellen, führen Sie den Befehl `New-ProvScheme` mit dem Parameter `NetworkMappings` aus. Sie können dem Parameter `NetworkMappings` mehrere Subnetze hinzufügen. Beispiel:

     ```
     New-Provscheme -NetworkMappings @{
     "0"="subnetpath1";"1"="subnetpath1" }

     <!--NeedCopy-->
     ```

   - Wenn Sie einen auf Maschinenprofilen basierenden Maschinenkatalog erstellen gehen Sie folgendermaßen vor:

     a) Erstellen Sie eine VM in Azure mit mehreren Netzwerkkarten. Informationen finden Sie unter Virtuelle Windows-Maschine mit mehreren Netzwerkkarten erstellen und verwalten. Sie können auch eine VM erstellen und ihr dann auf der Seite "Netzwerk" des Azure-Portals eine Netzwerkschnittstelle anfügen.

     b) Führen Sie den Befehl `New-ProvScheme` mit der VM als Maschinenprofileingabe aus.

     > **Hinweis:**
     >
     > Beim Erstellen eines auf Maschinenprofilen basierenden Maschinenkatalogs muss `NetworkMappings` mit `NetworkInterfaceCount` des Maschinenprofils übereinstimmen. `NetworkInterfaceCount` kann aus `AdditionalData` von `Get-item -Path "machine profile path"` abgerufen werden.

5. Beenden Sie die Erstellung des Maschinenkatalogs.

#### Katalog für mehrere Netzwerkkarten pro VM aktualisieren

Zum Aktualisieren eines Katalogs, sodass er mehrere Netzwerkkarten pro VM hat, gehen Sie folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster vom Delivery Controller-Host aus.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Aktualisieren Sie das Provisioningschema:
    - Wenn Sie einen nicht auf Maschinenprofilen basierenden Maschinenkatalog erstellen, führen Sie den Befehl `Set-ProvScheme` mit dem Parameter `NetworkMappings` aus. Sie können dem Parameter `NetworkMappings` mehrere Subnetze hinzufügen. Beispiel:

      ```
      Set-Provscheme -NetworkMappings @{
      "0"="subnetpath1";"1"="subnetpath1" }

      <!--NeedCopy-->
      ```

    - Zum Erstellen eines auf einem Maschinenprofil basierenden Maschinenkatalogs:
        a) Erstellen Sie eine VM in Azure mit mehreren Netzwerkkarten. Informationen finden Sie unter Virtuelle Windows-Maschine mit mehreren Netzwerkkarten erstellen und verwalten.
        b) Führen Sie den Befehl `Set-ProvScheme` mit der VM als Maschinenprofileingabe aus.

#### VM für mehrere Netzwerkkarten aktualisieren

Sie können auch eine VM mit `Set-ProvVMUpdateTimeWindow` aktualisieren und während des Aktualisierungszeitfensters einen Energiezyklus ausführen. Weitere Informationen finden Sie unter Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema.

### Maschinenkatalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit nicht-persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`. Die benutzerdefinierten Eigenschaften sind:

- `UseTempDiskForWBC`. Diese Eigenschaft legt fest, ob der temporäre Azure-Speicher zum Speichern der Zurückschreibcachedatei verwendet werden soll. Sie muss beim Ausführen von

`New-ProvScheme` auf “true”gesetzt sein, wenn Sie den temporären Datenträger als Datenträger für den Zurückschreibcache verwenden möchten. Wenn die Eigenschaft nicht festgelegt ist, wird die Standardeinstellung False für den Parameter verwendet.

Beispiel der Verwendung des Parameters `CustomProperties` zur Einstellung von `UseTempDiskForWBC` auf “true”:

```
    -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance"> `
    <Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
    <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `
    <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
    <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client"/> `
    <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/> `
    </CustomProperties>'
<!--NeedCopy-->
```

> **Hinweis:**
>
> Nachdem Sie für den Maschinenkatalog den lokalen temporären Azure-Speicher als Datenträger für den Zurückschreibecache festgelegt haben, können Sie die Einstellung später nicht in VHD ändern.

### Maschinenkatalog mit persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`.

> **Tipp:**
>
> Verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties` nur für cloudbasierte Hostverbindungen. Wenn Sie Maschinen mit persistentem Zurückschreibcachedatenträger für eine On-Premises-Lösung (z. B. XenServer) bereitstellen möchten, wird PowerShell nicht benötigt, da der Datenträger automatisch persistent ist.

Dieser Parameter unterstützt die zusätzliche Eigenschaft `PersistWBC`, welche bestimmt, ob der Zurückschreibcachedatenträger bei von MCS-bereitgestellten Maschinen persistent oder flüchtig ist.

Die Eigenschaft `PersistWBC` wird nur verwendet, wenn der Parameter `UseWriteBackCache` angegeben wird und Parameter `WriteBackCacheDiskSize` so konfiguriert ist, dass ein Datenträger erstellt wird.

> **Hinweis:**
>
> Dieses Verhalten gilt für Azure und GCP, bei dem der standardmäßige MCSIO-Zurückschreibcachedatenträger beim Aus- und Wiedereinschalten gelöscht und neu erstellt wird. Sie können den Datenträger als persistent konfigurieren, um das Löschen und neu Erstellen des MCSIO-Zurückschreibcachedatenträger zu vermeiden.

Beispiele für Eigenschaften im Parameter `CustomProperties` vor Unterstützung von `PersistWBC`:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```

> **Hinweis:**
>
> Dieses Beispiel gilt nur für Azure. Die Eigenschaften sind in der GCP-Umgebung anders.

Berücksichtigen Sie bei Verwendung dieser Eigenschaften deren Standardwerte, wenn die Eigenschaften im Parameter `CustomProperties` ausgelassen werden. Die Eigenschaft `PersistWBC` hat zwei mögliche Werte: **true** oder **false**.

Bei der Einstellung von `PersistWBC` auf **true** wird der Zurückschreibcachedatenträger nicht gelöscht, wenn der Citrix DaaS-Administrator die Maschine über die Verwaltungsoberfläche herunterfährt.

Bei der Einstellung von `PersistWBC` auf **false** wird der Zurückschreibcachedatenträger gelöscht, wenn der Citrix DaaS-Administrator die Maschine über die Verwaltungsoberfläche herunterfährt.

> **Hinweis:**
>
> Wird die Eigenschaft `PersistWBC` nicht angegeben, so gilt der Standardwert **false** und der Zurückschreibcachedatenträger wird beim Herunterfahren der Maschine über die Verwaltungsoberfläche gelöscht.

Beispiel der Verwendung des Parameters `CustomProperties` zur Einstellung von `PersistWBC` auf “true”:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Wichtig:**
>
> Die Eigenschaft `PersistWBC` kann nur mit dem PowerShell-Cmdlet `New-ProvScheme` festgelegt werden. Eine Änderung der `CustomProperties` eines Provisioningschemas nach der Erstellung hat keine Auswirkungen auf den Maschinenkatalog und die Permanenz des Zurückschreibcachedatenträger beim Herunterfahren von Maschinen.

Beispiel der Einstellung von `New-ProvScheme` zur Verwendung des Zurückschreibcache und Einstellung von `PersistWBC` auf “true”:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
    true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value
    =`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"
    benvaldev5RG3`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
    " />
</CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
```

```
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Startleistung mit MCSIO verbessern

Sie können die Startleistung für in Azure oder GCP verwaltete Datenträger verbessern, wenn MCSIO aktiviert ist. Verwenden Sie die benutzerdefinierte PowerShell-Eigenschaft `PersistOSDisk` im Befehl `New-ProvScheme`, um dieses Feature zu konfigurieren: Optionen für `New-ProvScheme`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Um dieses Feature zu aktivieren, legen Sie die benutzerdefinierte Eigenschaft `PersistOSDisk` auf **true** fest. Beispiel:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
```

```
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

### Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen

Wenn Sie einen Maschinenkatalog über PowerShell-Befehle erstellen, für den der Verschlüsselungsschlüssel kundenseitig verwaltet wird, führen Sie folgende Schritte aus:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Geben Sie `cd xdhyp:/` ein.
4. Geben Sie `cd .\HostingUnits\(your hosting unit)` ein.
5. Geben Sie cd diskencryptionset.folder ein.
6. Geben Sie dir ein, um die Liste der Datenträgerverschlüsselungssets abzurufen.
7. Kopieren Sie die ID eines Datenträgerverschlüsselungssets.
8. Erstellen Sie die Zeichenfolge einer benutzerdefinierten Eigenschaft, die die ID des Datenträgerverschlüsselungssets enthält. Beispiel:

```
1 $customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
    org/2001/XMLSchema-instance`">
2 <Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"
    False`" />
3 <Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
    =`"false`" />
4 <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
5 <Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
6 </CustomProperties>
7 <!--NeedCopy-->
```

9. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden. Beispiel:

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
2 <!--NeedCopy-->
```

10. Führen Sie den Befehl New-ProvScheme aus. Beispiel:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
    def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Beenden Sie die Erstellung des Maschinenkatalogs.

### Maschinenkatalog mit Verschlüsselung auf dem Host erstellen

So erstellen Sie einen Maschinenkatalog mit Verschlüsselung auf dem Host

1. Prüfen Sie, ob die Verschlüsselung auf dem Host für Ihr Abonnement aktiviert ist. Weitere Informationen hierzu finden Sie unter https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Wenn das Feature nicht aktiviert ist, müssen Sie es für das Abonnement aktivieren. Informationen zur Aktivierung des Features für Ihr Abonnement finden Sie unter https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Prüfen Sie, ob die Verschlüsselung auf dem Host für die vorliegende Azure-VM-Größe unterstützt wird. Führen Sie dazu in einem PowerShell-Fenster einen der folgenden Befehle aus:

```
PS XDHyp:\Connections<your connection>\east us.region\
    serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Erstellen Sie eine VM oder Vorlagenspezifikation als Eingabe für das Maschinenprofil im Azure-Portal mit aktivierter Verschlüsselung auf dem Host.

   - Wenn Sie eine VM erstellen möchten, wählen Sie eine VM-Größe, die die Verschlüsselung auf dem Host unterstützt. Nach dem Erstellen der VM ist die VM-Eigenschaft **Encryption at host** aktiviert.

- Wenn Sie eine Vorlagenspezifikation verwenden möchten, weisen Sie dem Parameter `Encryption at Host` den Wert **true** unter `securityProfile` zu.

4. Erstellen Sie einen MCS-Maschinenkatalog mit Maschinenprofilworkflow, indem Sie eine VM oder Vorlagenspezifikation auswählen.

   - Datenträger/Betriebssystemdatenträger: Die Verschlüsselung erfolgt über einen kundenseitig verwalteten Schlüssel und einen plattformseitig verwalteten Schlüssel.
   - Kurzlebiger Betriebssystemdatenträger: Die Verschlüsselung erfolgt nur über einen plattformseitig verwalteten Schlüssel.
   - Cache-Datenträger: Die Verschlüsselung erfolgt über einen kundenseitig verwalteten Schlüssel und einen plattformseitig verwalteten Schlüssel.

   Sie können den Maschinenkatalog über die "Vollständige Konfiguration"oder über PowerShell-Befehle erstellen.

#### Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen

Sie können Informationen zur Verschlüsselung am Host aus einem Maschinenprofil abrufen, wenn Sie den PowerShell-Befehl mit dem Parameter `AdditionalData` ausführen. Ist der Parameter `EncryptionAtHost` **True**, dann ist die Verschlüsselung am Host für das Maschinenprofil aktiviert.

Beispiel: Wenn die Maschinenprofileingabe eine VM ist, führen Sie den folgenden Befehl aus:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
<!--NeedCopy-->
```

Beispiel: Wenn die Maschinenprofileingabe eine Vorlagenspezifikation ist, führen Sie den folgenden Befehl aus:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
<!--NeedCopy-->
```

### Maschinenkatalog mit doppelter Verschlüsselung erstellen

Sie können einen Maschinenkatalog mit doppelter Verschlüsselung über die Benutzeroberfläche für die vollständige Konfiguration und mit PowerShell-Befehlen erstellen und aktualisieren.

Schritte zum Erstellen eines Maschinenkatalogs mit doppelter Verschlüsselung:

1. Erstellen Sie einen Azure Key Vault und DES mit plattformseitig und kundenseitig verwalteten Schlüsseln. Informationen zum Erstellen eines Azure Key Vault und eines DES finden Sie unter Verwenden des Azure-Portals zum Aktivieren der doppelten Verschlüsselung von ruhenden Daten auf verwalteten Datenträgern.
2. Um die in Ihrer Hostingeinheit verfügbaren DES anzuzeigen, gehen Sie wie folgt vor:

   a) Öffnen Sie ein **PowerShell**-Fenster.
   b) Führen Sie die folgenden PowerShell-Befehle aus:

      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName (ex. azure-east)`
      v. `cd diskencryptionset.folder`
      vi. `dir`

   Sie können eine ID des `DiskEncryptionSet` verwenden, um einen Katalog unter Verwendung benutzerdefinierter Eigenschaften zu erstellen oder zu aktualisieren.
3. Wenn Sie einen Maschinenprofilworkflow verwenden möchten, erstellen Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil.

   - Wenn Sie eine VM als Maschinenprofileingabe verwenden möchten:
     a) Erstellen Sie eine VM im Azure-Portal.
     b) Gehen Sie zu **Datenträger > Schlüsselverwaltung**, um die VM direkt mit einem `DiskEncryptionSetID` zu verschlüsseln.
   - Wenn Sie eine Vorlagenspezifikation als Maschinenprofileingabe verwenden möchten:
     a) Fügen Sie in der Vorlage unter `properties>storageProfile>osDisk>managedDisk` den Parameter `diskEncryptionSet` hinzu und fügen Sie die ID des DES für die doppelte Verschlüsselung hinzu.
4. Erstellen Sie den Maschinenkatalog.

   - Wenn Sie die Benutzeroberfläche für die vollständige Konfiguration verwenden, führen Sie zusätzlich zu den Schritten unter Maschinenkataloge erstellen einen der folgenden Schritte aus.
     - Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, wählen Sie auf der Seite **Datenträgereinstellungen** die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln**. Wählen Sie dann den DES für die doppelte Verschlüsselung aus der Dropdownliste aus. Fahren Sie mit der Erstellung des Katalogs fort.

- Wenn Sie den Maschinenprofil-Workflow verwenden, wählen Sie auf der Seite **Image** ein Masterimage (oder "vorbereitetes Image") und ein Maschinenprofil aus. Vergewissern Sie sich, dass die Eigenschaften des Maschinenprofils eine DES-ID enthalten.

Alle im Katalog erstellten Maschinen werden mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

- Wenn Sie PowerShell-Befehle verwenden, führen Sie einen der folgenden Schritte aus:
  - Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, fügen Sie dem Befehl `New-ProvScheme` die benutzerdefinierte Eigenschaft `DiskEncryptionSetId` hinzu. Beispiel:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/
    xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" />
<Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
    DiskEncryptionSetId" Value="/subscriptions/12345678-
    xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
    providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
<!--NeedCopy-->
```

  - Wenn Sie einen Maschinenprofil-basierten Workflow verwenden, verwenden Sie eine Maschinenprofileingabe im Befehl `New-ProvScheme`. Beispiel:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
    \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
    folder\apa-resourceGroup.resourcegroup\apa-
    resourceGroup-vnet.virtualprivatecloud\default.network"
     }
```

```
8
9   -ProvisioningSchemeName aio-test
10  -MachineProfile XDHyp:\HostingUnits\azure-east\
       machineprofile.folder\abc.resourcegroup\abx-mp.
       templatespec\1.0.0.templatespecversion
11  <!--NeedCopy-->
```

Schließen Sie die Katalogerstellung mit dem Remote PowerShell SDK ab. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Alle im Katalog erstellten Maschinen werden mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

#### Unverschlüsselten Katalog zur Verwendung der doppelten Verschlüsselung konvertieren

Sie können den Verschlüsselungstyp eines Maschinenkatalogs aktualisieren (mithilfe von benutzerdefinierten Eigenschaften oder Maschinenprofilen).

- Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, fügen Sie dem Befehl `Set-ProvScheme` die benutzerdefinierte Eigenschaft DiskEncryptionSetId hinzu. Beispiel:

```
1  Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2  -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
      .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
      /2001/XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
      Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
      resourceGroups/Sample-RG/providers/Microsoft.Compute/
      diskEncryptionSets/SampleEncryptionSet" />
4  </CustomProperties>'
5  <!--NeedCopy-->
```

- Wenn Sie einen Maschinenprofil-basierten Workflow verwenden, verwenden Sie eine Maschinenprofileingabe im Befehl `Set-ProvScheme`. Beispiel:

```
1  Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
       XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
      resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
2  <!--NeedCopy-->
```

Alle neuen VMs, die Sie dem Katalog hinzufügen, werden nun mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

#### Überprüfen, ob ein Katalog doppelt verschlüsselt ist

- In der Benutzeroberfläche für die vollständige Konfiguration gehen Sie wie folgt vor:

1. Gehen Sie zu **Maschinenkataloge**.
2. Wählen Sie den Katalog aus, den Sie überprüfen möchten. Klicken Sie am unteren Bildschirmrand auf die Registerkarte **Vorlageneigenschaften**.
3. Überprüfen Sie unter **Azure-Details** die DES-ID in **Datenträgerverschlüsselungssatz**. Ist die DES-ID des Katalogs leer, ist der Katalog nicht verschlüsselt.
4. Vergewissern Sie sich im Azure-Portal, dass es sich bei dem Verschlüsselungstyp des der DES-ID zugeordneten DES um plattformseitig und kundenseitig verwaltete Schlüssel handelt.

- PowerShell-Befehl verwenden:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Verwenden Sie `Get-ProvScheme`, um die Informationen des Maschinenkatalogs abzurufen. Beispiel:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
<!--NeedCopy-->
```

4. Rufen Sie die benutzerdefinierte DES-ID-Eigenschaft des Maschinenkatalogs ab. Beispiel:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
     Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
<!--NeedCopy-->
```

5. Vergewissern Sie sich im Azure-Portal, dass es sich bei dem Verschlüsselungstyp des der DES-ID zugeordneten DES um plattformseitig und kundenseitig verwaltete Schlüssel handelt.

### Speicherort der Auslagerungsdatei bestimmen

Der Speicherort der Auslagerungsdatei wird gemäß dem folgenden Szenario bestimmt:

> **Hinweis:**
>
> Der Standardspeicherort der Auslagerungsdatei ist der Betriebssystemdatenträger.

| Szenario | Ort |
| --- | --- |
| Die Auslagerungsdateieinstellung wird in den benutzerdefinierten Eigenschaften angegeben | Wie in den benutzerdefinierten Eigenschaften angegeben |
| Kurzlebiger Betriebssystemdatenträger oder Ruhezustand ist aktiviert | OS-Datenträger |
| VM hat einen temporären Datenträger | Temporärer Datenträger |
| MCS IO ist aktiviert | WBC-Datenträger |

### Szenarien zum Einrichten der Auslagerungsdatei

Die folgende Tabelle beschreibt einige mögliche Szenarien zum Einrichten der Auslagerungsdatei während der Imagevorbereitung und beim Aktualisieren des Provisioningschemas:

| Während | Szenario | Ergebnis |
| --- | --- | --- |
| Imagevorbereitung | Sie richten die Quellimage-Auslagerungsdatei auf dem temporären Datenträger ein, und die VM-Größe, die Sie im Provisioningschema angeben, umfasst keinen temporären Datenträger. | Auslagerungsdatei wird im Betriebssystem gespeichert. |
| Imagevorbereitung | Sie richten die Quellimage-Auslagerungsdatei auf dem Betriebssystemdatenträger ein, und die VM-Größe, die Sie im Provisioningschema angeben, umfasst einen temporären Datenträger. | Auslagerungsdatei wird auf dem temporären Datenträger gespeichert |

| Während | Szenario | Ergebnis |
|---|---|---|
| Imagevorbereitung | Sie richten die Quellimage-Auslagerungsdatei auf dem temporären Datenträger ein und aktivieren den kurzlebigen Betriebssystemdatenträger im Provisioningschema. | Auslagerungsdatei wird auf dem Betriebssystemdatenträger gespeichert |
| Aktualisierung des Provisioningschemas | Sie versuchen, das Provisioningschema zu aktualisieren, wenn die VDA-Version älter als 2311 ist | Ändert die Auslagerungsdateieinstellung mit einer Warnung |
| Aktualisierung des Provisioningschemas | Sie versuchen, das Provisioningschema zu aktualisieren, wenn die VDA-Version 2311 oder höher ist | Bestimmt den Speicherort der Auslagerungsdatei gemäß Bestimmen des Speicherorts der Auslagerungsdatei |

### Auslagerungsdateieinstellung angeben

Mit PowerShell-Befehlen können Sie Einstellungen für die Auslagerungsdatei angeben, einschließlich Speicherort und Größe. Dies überschreibt die Auslagerungsdateieinstellungen, die von MCS gemäß Bestimmen des Speicherorts der Auslagerungsdatei festgelegt wurden. Führen Sie hierfür beim Erstellen des Maschinenkatalogs den Befehl `New-ProvScheme` aus:

#### Wichtige Überlegungen

Beachten Sie Folgendes, bevor Sie mit der Katalogerstellung fortfahren:

- Sie müssen alle benutzerdefinierten Eigenschaften (‘PageFileDiskDriveLetterOverride’, ‘InitialPageFileSizeInMB’und ‘MaxPageFileSizeInMB’) im Befehl `New-ProvScheme` angeben oder keine davon.
- Dieses Feature wird von Citrix Studio nicht unterstützt.
- Die Anfangsgröße der Auslagerungsdatei muss zwischen 16 MB und 16777216 MB liegen.
- Die Maximalgröße der Auslagerungsdatei muss größer oder gleich der Anfangsgröße der Auslagerungsdatei und kleiner als 16777216 MB sein.
- Sie können die Anfangsgröße und die Maximalgröße der Auslagerungdatei gleichzeitig auf Null setzen.

> **Hinweis:**
>
> Sie können die Auslagerungsdateieinstellungen der neu hinzugefügten VMs eines vorhandenen Katalogs ändern, ohne das Masterimage zu aktualisieren. Zum Ändern der Auslagerungsdateieinstellungen benötigen Sie VDA-Version 2311 oder höher. Sie können die Auslagerungsdateieinstellungen mithilfe der PowerShell-Befehle ändern. Weitere Informationen finden Sie unter Auslagerungsdateieinstellungen ändern.

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
   zijincloud-resources.resourcegroup\
   CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk
   " `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\neal-zijincloud-resources.
    resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\
    default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\
   Standard_B2ms.serviceoffering" `
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
   ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

### Auslagerungsdateieinstellungen ändern

Sie können die Auslagerungsdateieinstellungen der neu zu einem vorhandenen Katalog hinzugefügten VMs ändern, ohne das Masterimage zu aktualisieren. Dieses Feature gilt derzeit nur für Azure-Umgebungen.

Zum Ändern der Auslagerungsdateieinstellungen benötigen Sie VDA-Version 2311 oder höher. Sie können die Auslagerungsdateieinstellungen mithilfe der PowerShell-Befehle ändern.

Im Folgenden sind die verschiedenen Auslagerungsdateieinstellungen aufgeführt, die Sie in der Azure-Umgebung ändern können:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

#### Auslagerungsdateieinstellungen eines vorhandenen Katalogs ändern

Führen Sie den Befehl `Set-ProvScheme` aus, um die Auslagerungsdateieinstellungen eines vorhandenen Maschinenkatalogs zu ändern. In diesem Fall werden die Updates nur auf die neuen VMs angewendet, die dem Katalog hinzugefügt wurden. Beispiel:

```
1  Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties '<
       CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
       instance">
2  <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
        />
3  <Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
4  <Property xsi:type="StringProperty" Name="StorageType" Value="
       StandardSSD_LRS" />
5  <Property xsi:type="StringProperty" Name="
       PageFileDiskDriveLetterOverride" Value="D" />
6  <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
       Value="2048" />
7  <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
       ="8196" />
8  <Property xsi:type="StringProperty" Name="LicenseType" Value="
       Windows_Client" />
9  <Property  xsi:type="StringProperty" Name="Zones" Value="1" />
10 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
       test-group1" />
11 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
12 </CustomProperties>'
13 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie den Zurückschreibcache aktivieren und versuchen, `PageFileDiskDriveLetterOverride` mithilfe des PowerShell-Befehls auf `C:` einzustellen, leitet der MCS IO-Treiber die Auslagerungsdatei automatisch auf ein korrektes Datenträgerlaufwerk und nicht `C:` um.

### Katalog-VMs mit aktiviertem AMA bereitstellen

1. Richten Sie eine Maschinenprofilvorlage ein.

   - Wenn Sie eine VM als Maschinenprofilvorlage verwenden:

     a) Erstellen Sie eine VM im Azure-Portal.
     b) Schalten Sie die VM ein.
     c) Fügen Sie die VM der Datensammlungsregel unter **Ressourcen** hinzu. Dadurch wird der Agent auf der Vorlagen-VM installiert.

   > **Hinweis:**
   >
   > Wenn Sie einen Linux-Katalog erstellen müssen, richten Sie eine Linux-Maschine ein.

   - Wenn Sie eine Vorlagenspezifikation als Maschinenprofilvorlage verwenden möchten:

     a) Richten Sie eine Vorlagenspezifikation ein.

     b) Fügen Sie der generierten Vorlagenspezifikation die folgende Erweiterungs- und Datensammlungsregelzuordnung hinzu:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
```

```
29      "Microsoft.Compute/virtualMachines/<vm-name>/extensions
           /AzureMonitorWindowsAgent"
30      ],
31      "properties": {
32
33         "description": "Association of data collection rule.
               Deleting this association will break the data
              collection for this Arc server.",
34       "dataCollectionRuleId": "/subscriptions/<azure-
            subscription>/resourcegroups/<azure-resource-group
            >/providers/microsoft.insights/datacollectionrules
            /<azure-data-collection-rule>"
35        }
36
37       }
38
39  <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie eine Datensammlungsregel mit einem Microsoft Sentinel-Datenconnector eingerichtet haben, können Sie `dataCollectionRuleAssociation` in der Vorlagenspezifikation auf die gleiche Weise wie bei einer regulären DCR-Verknüpfung hinzufügen. Die Katalog-VMs können dann im Sentinel DCR angezeigt werden und die AMA wird auf diesen VMs installiert. Informationen zu den bewährten Methoden für die Erstellung und Verwaltung von Datensammlungsregeln finden Sie unter Bewährte Methoden für die Erstellung und Verwaltung von Datensammlungsregeln in Azure Monitor.

2. Erstellen oder aktualisieren Sie einen vorhandenen MCS-Maschinenkatalog.

   - Zum Erstellen eines neuen MCS-Katalogs:

     a) Wählen Sie die VM oder Vorlagenspezifikation als Maschinenprofil in der Benutzeroberfläche “Vollständig Konfiguration”.
     b) Fahren Sie mit den nächsten Schritten zur Katalogerstellung fort.

   - Zum Aktualisieren eines vorhandenen MCS-Katalogs verwenden Sie die folgenden PowerShell-Befehle. In diesem Fall erhalten nur die neuen VMs die aktualisierte Maschinenprofilvorlage.

     ```
     1  Set-ProvScheme -ProvisioningSchemeName "name"
     2  -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
           folder\abc.resourcegroup\ab-machine-profile.vm"
     3  <!--NeedCopy-->
     ```

   - Zum Aktualisieren vorhandener VMs mit der aktualisierten Maschinenprofilvorlage führen Sie `Set-ProvScheme` und dann `Set-ProvVMUpdateTimeWindow` aus:

```
Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
    "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.
   resourcegroup\ab-machine-profile.vm"
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

3. Schalten Sie Katalog-VMs ein.
4. Überprüfen Sie im Azure-Portal, ob die Überwachungserweiterung auf der VM installiert ist und die VM unter den Ressourcen der Datensammlungsregel angezeigt wird. Nach einigen Minuten werden die Überwachungsdaten auf dem Azure Monitor angezeigt.

#### Problembehandlung

Informationen zur Problembehandlung für Azure Monitor Agent finden Sie hier:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Katalog mit Azure Spot-VMs erstellen

Mit Azure Spot-VMs können Sie die ungenutzte Rechenkapazität von Azure zu erheblichen Kosteneinsparungen nutzen. Die Fähigkeit, eine Azure Spot-VM zuzuweisen, hängt jedoch von der aktuellen Kapazität und den Preisen ab. Es kann daher sein, dass Azure Ihre laufende VM entfernt, die VM nicht erstellen kann oder die VM gemäß der Entfernungsrichtlinie nicht einschaltet. Azure Spot-VMs eignen sich demgemäß gut für einige unkritische Anwendungen und Desktops. Weitere Informationen finden Sie unter Azure Spot-VMs verwenden.

#### Einschränkungen

- Nicht alle VM-Größen werden für Azure Spot-VMs unterstützt. Weitere Informationen finden Sie unter Einschränkungen.

  Sie können den folgenden PowerShell-Befehl ausführen, um zu überprüfen, ob eine VM-Größe Spot-VMs unterstützt oder nicht. Wenn eine VM-Größe Spot-VM unterstützt, ist `SupportsSpotVM` **True**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
     folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  <!--NeedCopy-->
  ```

- Derzeit unterstützen Azure Spot-VMs den Ruhezustand nicht.

#### Voraussetzung

Beim Erstellen der Maschinenprofilquelle (VM- oder Vorlagenspezifikation) für den Azure Spot-VMs-Katalog müssen Sie Azure Spot Instance auswählen (wenn Sie eine VM verwenden) oder `priority` als `Spot` festlegen (wenn Sie die Vorlagenspezifikation verwenden).

#### Schritte zum Erstellen eines Katalogs mit Azure Spot-VMs

1. Erstellen Sie eine Maschinenprofilquelle (VM oder Startvorlage).
   - Informationen zum Erstellen einer VM über das Azure-Portal finden Sie unter Azure Spot-VMs über das Azure-Portal bereitstellen.
   - Um eine Vorlagenspezifikation zu erstellen, fügen Sie die folgenden Eigenschaften unter **resources > type: Microsoft.Compute/virtualMachines > properties** in der Vorlagenspezifikation hinzu. Beispiel:

```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }

<!--NeedCopy-->
```

> **Hinweis:**
>
> - Die Entfernungsrichtlinie kann auf **Zuweisung aufheben** oder **Löschen** lauten.
>   - Für nicht persistente VMs legt MCS die Entfernungsrichtlinie immer auf **Löschen** fest. Wenn die VM entfernt wird, wird sie zusammen mit allen nicht persistenten Datenträgern (z. B. OS-Datenträger) gelöscht. Alle persistenten Datenträger (z. B. Identitätsdatenträger) werden nicht gelöscht. Ein OS-Datenträger ist jedoch persistent, wenn der Katalogtyp persistent ist oder die benutzerdefinierte Eigenschaft `PersistOsDisk` auf True gesetzt ist. Analog dazu ist ein WBC-Datenträger persistent, wenn die benutzerdefinierte Eigenschaft `PersistWbc` auf **True** gesetzt ist.
>   - Für persistente VMs legt MCS die Entfernungsrichtlinie immer auf "Zuordnung aufheben"fest. Wenn die VM entfernt wird, wird ihre Zuordnung aufgehoben. An den Datenträgern werden keine Änderungen vorgenommen.
> - Der Höchstpreis ist der Preis, den Sie pro Stunde zu zahlen bereit sind. Wenn Sie **Nur**

> **Kapazität** verwenden, ist dies **-1**. Der Höchstpreis kann nur Null, -1 oder eine Dezimalzahl größer als Null sein. Weitere Informationen finden Sie unter Preisgestaltung.

2. Sie können den folgenden PowerShell-Befehl ausführen, um zu überprüfen, ob ein Maschinenprofil Azure Spot-VM-fähig ist oder nicht. Wenn der Parameter `SpotEnabled` auf **True** und `SpotEvictionPolicy` auf **Deallocate** oder **Delete** gesetzt ist, ist das Maschinenprofil für Azure Spot-VM aktiviert. Zum Beispiel:

   - Wenn es sich bei der Maschinenprofilquelle um eine VM handelt, führen Sie den folgenden Befehl aus:

     ```
     1  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
            .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
            AdditionalData
     2  <!--NeedCopy-->
     ```

   - Wenn die Maschinenprofilquelle eine Vorlagenspezifikation ist, führen Sie den folgenden Befehl aus:

     ```
     1  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
            .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
            templatespec\14.0.0-spot-delete.templatespecversion").
            AdditionalData
     2  <!--NeedCopy-->
     ```

3. Erstellen Sie einen Maschinenkatalog unter Verwendung eines Maschinenprofils mit dem PowerShell-Befehl `New-ProvScheme`.

Mit dem Befehl `Set-ProvScheme` können Sie einen Katalog aktualisieren. Vorhandene VMs können Sie auch mit dem PowerShell-Befehl `Set-ProvVmUpdateTimeWindow` aktualisieren. Das Maschinenprofil wird beim nächsten Einschalten aktualisiert.

#### Entfernen von VMs auf einer laufenden Azure Spot-VM

Wenn die Rechenkapazität nicht verfügbar ist oder der Preis pro Stunde höher ist als der konfigurierte Höchstpreis, entfernt Azure eine laufende Spot-VM. Standardmäßig werden Sie nicht über einen Entfernungsvorgang informiert. Die VM friert einfach ein und wird entfernt. Microsoft empfiehlt, geplante Ereignisse zur Überwachung von Entfernungsvorgängen zu verwenden. Weitere Informationen finden Sie unter Entfernungsvorgänge kontinuierlich überwachen. Sie können auch Skripts von einer VM aus ausführen, um vor dem Entfernen eine Benachrichtigung zu erhalten. Microsoft bietet beispielsweise das Python-Abfrageskript ScheduledEvents.cs.

#### Problembehandlung

- Mit dem Befehl `Get-ProvVM` können Sie die Spot-VM-Eigenschaften in den customMachine-Data der bereitgestellten VM anzeigen. Wenn das Feld "Priorität"auf **Spot** gesetzt ist, wird Spot verwendet.
- Sie können im Azure-Portal überprüfen, ob eine VM Spot verwendet:
    1. Suchen Sie die VM im Azure-Portal.
    2. Gehen Sie zur **Übersichtsseite**.
    3. Scrollen Sie nach unten und suchen Sie den Abschnitt **Azure Spot**.
        - Wenn Spot nicht verwendet wird, ist dieses Feld leer.
        - Wenn Spot verwendet wird, sind die Felder **Azure Spot** und **Azure Spot-Entfernungsrichtlinie** gesetzt.

1. Sie können das Abrechnungsprofil oder den Höchstpreis pro Stunde für die VM auf der Konfigurationsseite überprüfen.

### Tags in allen Ressourcen kopieren

Sie können in einem Maschinenprofil angegebene Tags auf alle Ressourcen (z. B. mehrere Netzwerkkarten und Betriebssystem-, Identitäts- und Zurückschreibdatenträger) einer neuen VM oder bestehenden VM in einem Maschinenkatalog kopieren. Die Maschinenprofilquelle kann eine VM oder ARM-Vorlagenspezifikation sein.

> **Hinweis:**
>
> Sie müssen die Richtlinie für die Tags hinzufügen (siehe Zuweisen von Richtliniendefinitionen für Tagkonformität) oder die Tags in einer Maschinenprofilquelle hinzufügen, um die Tags für die Ressourcen beizubehalten.

#### Voraussetzungen

Erstellen Sie die Maschinenprofilquelle (VM oder ARM-Vorlagenspezifikation), um Tags für VM, Datenträger und Netzwerkkarten dieser VM zu haben.

- Wenn Sie eine VM als Maschinenprofil-Eingabe haben möchten, wenden Sie Tags auf die VM und alle Ressourcen im Azure-Portal an. Siehe Anwenden von Tags mit dem Azure-Portal.
- Wenn Sie die ARM-Vorlagenspezifikation als Maschinenprofil-Eingabe verwenden, fügen Sie den folgenden Tag-Block unter jeder Ressource hinzu.

```
 "tags": {

"TagC": "Value3"
 }
,
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Vorlagenspezifikation kann maximal einen Datenträger und muss mindestens eine Netzwerkkarte enthalten.

#### Tags an die Ressourcen einer VM in einem neuen Maschinenkatalog kopieren

1. Erstellen Sie einen nicht persistenten oder persistenten Katalog mit einer VM oder einer ARM-Vorlagenspezifikation als Maschinenprofil-Eingabe.
2. Fügen Sie dem Katalog eine VM hinzu und schalten Sie sie ein. Sie müssen sehen, dass die im Maschinenprofil angegebenen Tags an die entsprechenden Ressourcen der VM kopiert wurden.

   > **Hinweis:**
   >
   > Stimmt die Anzahl der im Maschinenprofil angegebenen Netzwerkkarten nicht mit der Anzahl Netzwerkkarten, die die VMs verwenden sollen, überein, wird eine Fehlermeldung angezeigt.

#### Tags für Ressourcen einer vorhandenen VM ändern

1. Erstellen Sie ein Maschinenprofil mit Tags für alle Ressourcen.
2. Aktualisieren Sie den vorhandenen Maschinenkatalog mit dem aktualisierten Maschinenprofil. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
<!--NeedCopy-->
```

3. Schalten Sie die VM aus, auf der Sie die Updates anwenden möchten.
4. Fordern Sie ein geplantes Update für die VM an. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
<!--NeedCopy-->
```

5. Schalten Sie die VM ein.

6. Sie müssen sehen, dass die im Maschinenprofil angegebenen Tags an die entsprechenden Ressourcen wurden.

> **Hinweis:**
>
> Stimmt die Anzahl der im Maschinenprofil angegebenen Netzwerkkarten nicht mit der in `Set-ProvScheme` angegebenen Anzahl Netzwerkkarten überein, wird eine Fehlermeldung angezeigt.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und Microsoft Azure-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft Azure Resource Manager
- Maschinenkataloge erstellen

## Microsoft System Center Virtual Machine Manager-Katalog erstellen

February 21, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft System Center Virtual Machine Manager (VMM)-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen VMM-Katalog erstellen, müssen Sie eine Verbindung zu VMM hergestellt haben. Siehe Verbindung zu Microsoft System Center Virtual Machine Manager.

### Erstellen einer Master-VM

- Installieren Sie einen VDA auf der Master-VM und wählen Sie die Option zur Desktopoptimierung aus. Dies verbessert die Leistung.
- Erstellen Sie einen Snapshot der Master-VM, um diesen als Backup zu verwenden.
- Erstellen Sie virtuelle Desktops.

### MCS auf SMB 3-Dateifreigaben

Bei Maschinenkatalogen, die mit MCS auf SMB 3-Dateifreigaben für VM-Speicher erstellt wurden, müssen die Anmeldeinformationen die nachfolgenden Anforderungen erfüllen, damit Aufrufe von der XenServer Communications Library (HCL) die Verbindung mit dem SMB-Speicher herstellen können.

- Die VMM-Benutzeranmeldeinformationen müssen vollständigen Lese-/Schreibzugriff auf den SMB-Speicher umfassen.
- Speichervorgänge auf dem virtuellen Datenträger werden bei Vorgängen im Lebenszyklus der VM über den Hyper-V-Server mit den VMM-Anmeldeinformationen durchgeführt.

Weitere Informationen zu SMB 3 finden Sie unter Überblick über die Dateifreigabe mithilfe des SMB 3-Protokolls in Windows Server.

Bei Verwendung von VMM 2012 SP1 mit Hyper-V unter Windows Server 2012: Wenn Sie SMB als Speicher verwenden, aktivieren Sie das Feature "CredSSP"(Credential Security Support Provider) vom Cloud Connector auf den einzelnen Hyper-V-Maschinen. Weitere Informationen finden Sie unter CTX137465.

Über eine standardmäßige PowerShell V3-Remotesitzung verwendet die HCL des Cloud Connectors CredSSP zum Öffnen einer Verbindung mit der Hyper-V-Maschine. Dieses Feature übergibt mit Kerberos verschlüsselte Benutzeranmeldeinformationen an die Hyper-V-Maschine. Die PowerShell-Befehle in dieser Sitzung auf der Remotemaschine mit Hyper-V werden dann unter Verwendung der angegebenen Anmeldeinformationen (in diesem Fall, derer des VMM-Benutzers) ausgeführt, sodass eine ordnungsgemäße Kommunikation mit dem Speicher gewährleistet wird.

Bei den folgenden Aufgaben werden PowerShell-Skripts verwendet, die ihren Ursprung in der HCL haben. Die Skripts werden dann an die Hyper-V-Maschine gesendet, um am SMB 3.0-Speicher ausgeführt.

**Konsolidieren des Masterimages:** Ein Image erstellt ein neues MCS-Provisioningschema (Maschinenkatalog). Die Master-VM wird durch dieses Schema geklont und vereinfacht, damit sie zum Erstellen neuer VM aus dem neu erstellten Datenträger bereit ist (die Abhängigkeit zur ursprünglichen Master-VM wird entfernt).

ConvertVirtualHardDisk im Namespace root\virtualization\v2

Beispiel:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

**Differenzierenden Datenträger erstellen:** Erstellt einen differenzierenden Datenträger aus dem Image, das durch Konsolidierung des Images generiert wurde. Der differenzierende Datenträger wird dann an eine neue VM angeschlossen.

CreateVirtualHardDisk im Namespace root\virtualization\v2

Beispiel:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

**Upload von Identitätsdisks:** Von der HCL kann die Identitätsdisk nicht direkt in den SMB-Speicher hochgeladen werden. Daher muss der Identitätsdatenträger von der Hyper-V-Maschine hochgeladen und in den Speicher kopiert werden. Da die Hyper-V-Maschine den Identitätsdatenträger nicht auf dem Cloud Connector lesen kann, muss er von der HCL zuerst wie folgt über die Hyper-V-Maschine kopiert werden:

1. Upload der Identitätsdisk durch die HCL auf die Hyper-V-Maschine über die Administratorfreigabe.
2. Der Datenträger wird von der Hyper-V-Maschine über ein PowerShell-Skript, das in der Remote-PowerShell-Sitzung ausgeführt wird, in den SMB-Speicher kopiert.

   Auf der Hyper-V-Maschine wird ein Ordner erstellt, dessen Berechtigungen nur für den VMM-Benutzer gesperrt sind (über die remote PowerShell-Verbindung).
3. Die HCL löscht die Datei aus der Administratorfreigabe.
4. Wenn der Upload des Identitätsdatenträgers durch die HCL auf die Hyper-V-Maschine abgeschlossen ist, werden die Identitätsdatenträger von der Remote-PowerShell-Sitzung in den SMB-Speicher kopiert und dann aus der Hyper-V-Maschine gelöscht.

Falls der Ordner des Identitätsdatenträgers gelöscht wird, wird er neu erstellt, damit er zur Wiederverwendung verfügbar ist.

**Download von Identitätsdatenträgern:** Wie beim Upload wird der Identitätsdatenträger über die Hyper-V-Maschine an die HCL übergeben. Beim folgenden Prozess wird, falls noch nicht vorhanden, ein Ordner erstellt, der nur VMM-Benutzerberechtigungen auf dem Hyper-V-Server hat.

1. Der Datenträger wird von der Hyper-V-Maschine aus dem SMB-Speicher in den lokalen Hyper-V-Speicher kopiert, und zwar über ein PowerShell-Skript, das in der Remote-PowerShell V3-Sitzung ausgeführt wird.
2. Die HCL liest den Datenträger aus der Administratorfreigabe der Hyper-V-Maschine in den Speicher.
3. Die HCL löscht die Datei aus der Administratorfreigabe.

### Katalog mit einem Maschinenprofil erstellen

Sie können ein Maschinenprofil verwenden, um einen MCS-Maschinenkatalog in System Center Virtual Machine Manager-(SCVMM)-Umgebungen zu erstellen und zu aktualisieren. Sie können auch verschachtelte Virtualisierung und vTPM aktivieren.

#### Wichtige Überlegungen

- Das Masterimage kann nur ein Snapshot und keine VM sein.
- Sie können VM nur als Maschinenprofilquelle verwenden.
- Sie können VTPM über die Hyper-V-Konsole und nicht über die SCVMM-Konsole konfigurieren.
- Wenn für das Masterimage vTPM aktiviert ist, müssen Sie vTPM auf der Maschinenprofilquelle aktivieren.
- vTPM wird nur auf Maschinen der Generation 2 unterstützt.
- Die folgenden Parameter überschreiben die in einem Maschinenprofil erfassten Werte, sofern sie separat angegeben werden:
  - VMCpuCount
  - VMMemoryMB
  - Datenträgerspeicher
- Sie können einen vorhandenen Katalog mit dem Befehl `Set-ProvScheme` aktualisieren.

#### Vorgehensweise zum Erstellen eines Katalogs mit einem Maschinenprofil

1. Erstellen Sie eine VM als Maschinenprofilquelle. Weitere Informationen finden Sie unter Virtuelle Maschinen in der VMM-Fabric bereitstellen. Sie können die einmal ausgewählte **Generation** nicht mehr ändern.
   - Wenn Sie die verschachtelte Virtualisierung aktivieren möchten, aktivieren Sie auf der Seite **Quelle auswählen** das Kontrollkästchen **Verschachtelte Virtualisierung aktivieren**.

- Wenn Sie vTPM aktivieren möchten, melden Sie sich nach dem Erstellen der VM beim Hyper-V-Host an und suchen Sie Ihre VM im **Hyper-V-Manager**. Klicken Sie mit der rechten Maustaste auf die VM und gehen Sie dann zu **Einstellungen**. Markieren Sie unter **Sicherheit** das Kontrollkästchen **Trusted Platform Module aktivieren**.

2. Öffnen Sie ein **PowerShell**-Fenster.
3. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
4. Erstellen Sie einen Brokerkatalog. In diesem Katalog sind Maschinen eingetragen, die gerade erstellt werden.
5. Erstellen Sie einen Identitätspool. Dieser wird zu einem Container für AD-Konten, die für die zu erstellenden Maschinen erstellt wurden.
6. Erstellen Sie ein Provisioningschema mit dem Maschinenprofil. Beispiel:

```
1 New-ProvScheme -HostingUnitName "<hostingunit name>"
2 -IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
     path to the checkpoint/snapshot>"
3 -ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
     path to the machine profile VM>"
4 <!--NeedCopy-->
```

7. Damit wird der Brokerkatalog mit der eindeutigen ID des Provisioningschemas aktualisiert.
8. Erstellen Sie virtuelle Maschinen und fügen Sie sie dem Katalog hinzu.

Sie können einen vorhandenen Katalog mit dem Befehl Set-ProvScheme aktualisieren. Beispiel:

```
1 Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
     "XDHyp:<path to the machine profile VM>"
2 <!--NeedCopy-->
```

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und Microsoft System Center Virtual Machine Manager-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten

- Verbindung zu Microsoft System Center Virtual Machine Manager
- Maschinenkataloge erstellen

## Nutanix-Katalog erstellen

February 14, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Nutanix-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Nutanix-Katalog erstellen, müssen Sie eine Verbindung zu Nutanix hergestellt haben. Siehe Verbindung zu Nutanix.

### Erstellen eines Maschinenkatalogs mit einem Nutanix-Snapshot

Der von Ihnen ausgewählte Snapshot wird als Vorlage zum Erstellen der VMs im Katalog verwendet. Erstellen Sie erst Images und Snapshots in Nutanix, bevor Sie den Katalog erstellen. Weitere Informationen finden Sie in der Nutanix-Dokumentation.

Im Assistenten für die Katalogerstellung:

- Die Seiten **Betriebssystem** und **Maschinenverwaltung** enthalten keine Nutanix-spezifischen Informationen.
- Die Seiten **Container** bzw. **Cluster und Container** sind Nutanix-spezifisch.
  - Wenn Sie Maschinen über Nutanix AHV XI als Ressourcen bereitstellen, wählen Sie auf der Seite **Container** einen Container für die Identitätsdatenträger der VMs.
  - Wenn Sie Maschinen mit Nutanix AHV Prism Central (PC) als Ressourcen bereitstellen, wird die Seite **Cluster und Container** angezeigt. Wählen Sie den Cluster für die Bereitstellung von VMs und anschließend einen Container.
- Wählen Sie auf der Seite **Image** den Snapshot des Images aus. Verwenden Sie bei Bedarf die Acropolis-Konsole, um die Snapshots umzubenennen. Wenn Sie Snapshots umbenennen, starten Sie den Assistenten zum Erstellen von Katalogen neu, damit eine aktualisierte Liste angezeigt wird.
- Geben Sie auf der Seite **Virtuelle Maschinen** die Anzahl der virtuellen CPUs und die Anzahl der Kerne pro vCPU an.

- Wählen Sie auf der Seite **Netzwerkkarten** den NIC-Typ zum Filtern der zugehörigen Netzwerke. Diese Option ist nur für Nutanix AHV PC-Verbindungen verfügbar. Es gibt zwei Arten von Netzwerkkarten: **VLAN** und **OVERLAY**. Wählen Sie eine oder mehrere Netzwerkkarten, die das Masterimage enthält, und anschließend für jede Netzwerkkarte das zugehörige virtuelle Netzwerk.
- Die Seiten **Maschinenidentitäten**, **Domänenanmeldeinformationen**, **Bereiche** und **Zusammenfassung** enthalten keine Nutanix-spezifischen Informationen.

### Einschränkung

Beim Erstellen eines MCS-Katalogs mit Nutanix-Hostverbindung (insbesondere Nutanix AHV-Plugin 2.7.1 und Nutanix AHV-Plugin 2.5.1) wird die Festplattengröße der bereitgestellten VMs in der Oberfläche "Vollständige Konfiguration"falsch angezeigt.

- Nutanix AHV-Plugin 2.7.1: Die angezeigte Größe ist viel kleiner (1 GB) als die tatsächliche Speichergröße.
- Nutanix AHV-Plugin 2.5.1: Die angezeigte Größe ist viel kleiner (32 GB) als die tatsächliche Speichergröße.

Dies funktioniert jedoch wie vorgesehen, wenn die Masterimage-VM ein Snapshot in VM ist.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Nutanix
- Verbindung zu Nutanix-Cloud und Partnerlösungen
- Maschinenkataloge erstellen

## VMware-Katalog erstellen

May 17, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben.

> **Hinweis:**
>
> Bevor Sie einen VMware-Katalog erstellen, müssen Sie eine Verbindung zu VMware hergestellt haben. Siehe Verbindung zu VMware.

### Maschinenkatalog mit einem Maschinenprofil erstellen

Sie können einen MCS-Maschinenkatalog mithilfe eines Maschinenprofils erstellen. Die Quelle der Eingabe des Maschinenprofils ist eine VMware-Vorlage. Das Maschinenprofil erfasst die Hardwareeigenschaften aus einer VMware-Vorlage und wendet sie auf die neu bereitgestellten virtuellen Maschinen im Katalog an.

> **Hinweis:**
>
> - Die Masterimage-Eingabe (Snapshot) und die Maschinenprofileingabe (VMware-Vorlage) müssen entweder beide vTPM-aktiviert oder beide vTPM-deaktiviert sein. Diese Regel gilt sowohl für `New-ProvScheme` als auch für `Set-ProvScheme`.
> - Wenn das Masterimage vTPM-aktiviert ist, kann die VMware-Vorlage nur aus derselben VM-Quelle stammen wie das Masterimage.
> - Die Speicherverschlüsselungsrichtlinie unterstützt nur vollständige Klons.

Die VMware-Vorlage im Maschinenprofil muss während des Kataloglebenszyklus vorhanden sein, damit virtuelle Maschinen für den Katalog bereitgestellt werden können. Ohne VMware-Vorlage können Sie keine neuen virtuellen Maschinen bereitstellen. Wenn eine VMware-Vorlage gelöscht wird, müssen Sie mithilfe des Befehls `Set-ProvScheme` eine neue Vorlage bereitstellen.

- MCS erfasst die Eigenschaften von VMware-Vorlagen. Mit dem Befehl `Get-Provscheme` können Sie eine VMware-Vorlage mit Verweis auf gespeicherte Eigenschaften der VMware-Vorlage erstellen.
- Wenn der Maschinenkatalog und die bereitgestellten VMs vorhanden sind, kann alternativ eine mit MCS bereitgestellte Maschine verwendet werden, um eine VMware-Vorlage zu erstellen.

Basierend auf verschiedenen Betriebssystemen können Sie einen Maschinenkatalog mit verschiedenen Konfigurationen erstellen:

- Ist Windows 11 auf dem Masterimage installiert, muss vTPM für das Masterimage aktiviert sein. Daher muss an die VMware-Vorlage, die eine Quelle für das Maschinenprofil ist, vTPM angefügt sein.
- Ist Windows 10 auf dem Masterimage ohne angefügtes vTPM installiert, können Sie einen Maschinenkatalog mit einer VMware-Vorlage ohne vTPM als Quelle für das Maschinenprofil erstellen.

Es gibt eine weitere Konfiguration, bei der Sie einen Maschinenkatalog im Komplettklon-Kopiermodus erstellen können, wobei die Maschinenprofilvorlage mit der Speicherverschlüsselungsrichtlinie angewendet wird.

Gehen Sie zu Erstellen eines Maschinenkatalog mit PowerShell und einem Maschinenprofil als Eingabe folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie die folgenden Befehle aus:

   - Gehen Sie zum Erstellen eines Maschinenkatalogs mit einer VMware-Vorlage mit angefügtem vTPM als Quelle für die Maschinenprofileingabe und dem Windows 11-Masterimage wie folgt vor:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
   network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
   ProvisioningType 'MCS'
-Scope @()  -SessionSupport "SingleSession"
-ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Gehen Sie zum Erstellen eines Maschinenkatalogs mit einer VMware-Vorlage ohne vTPM als Quelle für das Maschinenprofil und dem Windows10-Masterimage wie folgt vor:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
     }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
     -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"  -Description "<string>"  -
    IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
    ProvisioningType 'MCS' -Scope @()  -SessionSupport "
    SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Gehen Sie zum Erstellen eines Maschinenkatalogs unter Verwendung des Komplettklon-Kopiermodus und Anwendung der Maschinenprofilvorlage mit der Speicherverschlüsselungsrichtlinie folgendermaßen vor:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
```

```
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
-UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Verwenden Sie den `Set-ProvScheme` Befehl, um ein Maschinenprofil zu aktualisieren. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -
   IdentityPoolName 'name' -MachineProfile 'XDHyp:\
   HostingUnits<hosting unit name><template name>.template
<!--NeedCopy-->
```

### Nach mehreren NICs suchen

Bei den vorbereitenden Checks für mehrere Netzwerkkarten erhalten Sie verschiedene Fehlermeldungen, wenn Sie ein Maschinenprofil und den Parameter `NetworkMapping` in den Befehlen `New-ProvScheme` und `Set-ProvScheme` verwenden.

Die vorbereitende Checkliste für mehrere Netzkkarten lautet wie folgt:

- Nur die Anzahl der Netzwerkkarten aus der Maschinenprofilvorlage wird verwendet und validiert. Das Netzwerk, auf das diese Netzwerkkarten verweisen, wird nicht verwendet oder anhand der Netzwerke der Hostingeinheit validiert.
- Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage größer ist als die Anzahl der Netzwerke in der Hosteinheit, erhalten Sie eine Fehlermeldung.
- Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage null ist, erhalten Sie eine Fehlermeldung.
  Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage eins ist, gilt Folgendes:
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage größer als 1 ist oder die Netzwerkanzahl der Hosteinheit größer als 1 ist, dann gilt Folgendes:
  - Für den Befehl ist eine gültige Netzwerkzuordnung erforderlich, die eine Zuordnung für jede Netzwerkkarte bereitstellen sollte (d. h., die NetworkMapping-Anzahl sollte mit der Anzahl der Netzwerkkarten des Maschinenprofils übereinstimmen).
  - In der Hostingeinheit können nicht mehrere Netzwerkkarten demselben Netzwerk zugeordnet werden.
  - Die Anzahl von `NetworkMapping` und die Anzahl der Netzwerkkarten des Maschinenprofils müssen kleiner oder gleich der Netzwerkanzahl der Hostingeinheit sein.
  - `NetworkMapping` muss für jede ID von 0 bis n-1 angegeben werden, wobei n die Anzahl der Netzwerkadapter in der Maschinenprofilvorlage ist.

### Problembehandlung

Wenn der Katalog nicht erstellt werden kann, lesen Sie bitte CTX294978.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und VMware-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu VMware
- Verbindung zu VMware-Cloud und Partnerlösungen
- Maschinenkataloge erstellen

## XenServer-Katalog erstellen

March 6, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf XenServer-Virtualisierungsumgebungen (früher Citrix Hypervisor).

> **Hinweis:**
>
> Bevor Sie einen XenServer-Katalog erstellen, müssen Sie eine Verbindung zu XenServer hergestellt haben. Weitere Informationen finden Sie unter Verbindung zu XenServer.

### Maschinenkatalog mit einem GPU-fähigen XenServer erstellen

GPU-fähige Maschinen benötigen ein dediziertes Masterimage. Diese VMs erfordern Videotreiber, die GPUs unterstützen. Konfigurieren Sie GPU-fähige Maschinen, damit die VM Software verwenden kann, die die GPU für Vorgänge verwendet.

1. Erstellen Sie in XenCenter eine VM mit Standard-VGA sowie Netzwerken und einer vCPU.
2. Aktualisieren Sie die VM-Konfiguration so, dass die GPU (entweder Passthrough oder vGPU) verwendet werden kann.
3. Installieren Sie ein unterstütztes Betriebssystem und aktivieren Sie RDP.
4. Installieren Sie Citrix VM Tools und NVIDIA-Treiber.
5. Deaktivieren Sie die VNC-Verwaltungskonsole (Virtual Network Computing), um die Leistung zu optimieren, und starten Sie anschließend die VM neu.
6. Sie werden aufgefordert, RDP zu verwenden. Installieren Sie mit RDP den VDA und starten Sie dann die VM neu.
7. Optional können Sie einen Snapshot der VM erstellen und als Vorlage für andere GPU-Masterimages verwenden.
8. Installieren Sie mit RDP kundenspezifische Anwendungen, die in XenCenter konfiguriert werden und GPU-Funktionen verwenden.

### Erstellen Sie einen auf Maschinenprofilen basierenden Maschinenkatalog mit PowerShell

Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS erstellen, können Sie ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer virtuellen Maschine erfasst und auf neu bereitgestellte VMs im Katalog anwendet. Wenn der Parameter `MachineProfile` nicht verwendet wird, werden die Hardwareeigenschaften von der Masterimage-VM oder dem Snapshot erfasst.

> **Hinweis:**
>
> Derzeit können Sie nur einen Snapshot als Maschinenprofileingabe verwenden.

Sie können die folgenden Parameter explizit konfigurieren, um die Werte der Parameter in der Maschinenprofileingabe außer Kraft zu setzen:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

#### Katalog mit einem Maschinenprofil erstellen

1. Öffnen Sie das PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Erstellen Sie einen Identitätspool. Der Identitätspool ist ein Container für die Active Directory-Konten der zu erstellenden VMs. Beispiel:

```
1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
     IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
     -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
2 <!--NeedCopy-->
```

4. Erstellen Sie die erforderlichen AD-Computerkonten in Active Directory.

```
1 $password = "password123" | ConvertTo-SecureString -AsPlainText -
     Force
2 New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
     10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
     -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

5. Führen Sie den Befehl `New-ProvScheme` aus, um einen Katalog zu erstellen. Beispiel:

```
1 New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
     -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
      -CustomProperties '<CustomProperties xmlns="http://schemas.
```

```
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm\ExampleSnapshot.snapshot"
<!--NeedCopy-->
```

6. Registrieren Sie das Provisioningsschema als Brokerkatalog. Beispiel:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
<!--NeedCopy-->
```

7. Fügen Sie die VMs zum Katalog hinzu.

### Katalog mit einem neuen Maschinenprofil aktualisieren

> **Hinweis:**
>
> - Der Befehl `Set-ProvScheme` ändert in diesem Fall das Maschinenprofil der vorhandenen VMs im Katalog nicht. Nur neu erstellte VMs, die dem Katalog hinzugefügt werden, haben das neue Maschinenprofil.
> - Sie können keinen auf einem Maschinenprofil basierenden Maschinenkatalog in einen Maschinenkatalog konvertieren, der nicht auf Maschinenprofilen basiert.

Katalog mit einem neuen Maschinenprofil aktualisieren:

1. Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
<!--NeedCopy-->
```

   Weitere Informationen zum Befehl Set-ProvScheme finden Sie unter Set-ProvScheme.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Planen und Erstellen einer Bereitstellung.
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und XenServer-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu XenServer
- Maschinenkataloge erstellen

## Kataloge mit verschiedenen Einbindungstypen erstellen

July 3, 2023

Mit MCS können Sie Maschinen ohne Domänenbindung, mit On-Premises-AD-Verbindung, mit Azure AD-Verbindung oder mit Azure AD-Hybrideinbindung bereitstellen.

Informationen zum Konfigurieren von Maschinenidentitäten in der Oberfläche "Vollständige Konfiguration"finden Sie unter Erstellen von Maschinenkatalogen.

Weitere Informationen zum Erstellen von mit der Maschinenidentität verbundenen Katalogen finden Sie in den folgenden Abschnitten:

- Kataloge mit Einbindung in Azure Active Directory erstellen
- Kataloge mit aktiviertem Microsoft Intune erstellen
- Kataloge mit Azure Active Directory-Hybrideinbindung erstellen
- Nicht domänengebundene Kataloge erstellen

## Kataloge mit Einbindung in Azure Active Directory erstellen

February 14, 2024

In diesem Artikel wird beschrieben, wie Sie mit Azure Active Directory (AD) verbundene Kataloge mit Citrix DaaS erstellen.

Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter In Azure Active Directory eingebunden.

Vor dem Erstellen des Maschinenkatalogs benötigen Sie Folgendes:

1. Einen neuen Ressourcenstandort
    - Wählen Sie in der Citrix Cloud-Verwaltungsoberfläche im Hamburgermenü oben links **Ressourcenstandorte**.
    - Klicken Sie auf **+ Ressourcenstandort**.
    - Geben Sie den Namen für den neuen Ressourcenstandort ein und klicken Sie auf **Speichern**.
2. Erstellen Sie eine Hostverbindung. Weitere Informationen finden Sie unter Verbindungen erstellen und verwalten. Beachten Sie beim Bereitstellen von Maschinen in Azure auch die Hinweise unter Verbindung mit Azure Resource Manager.
3. Um veraltete Azure AD-Geräte fortlaufend zu löschen und neuen Geräten den Beitritt zu Azure AD zu ermöglichen, können Sie dem Dienstprinzipal des Provisioning Service die Rolle "Cloud Device Administrator"zuweisen. Wenn Sie veraltete Azure AD-Geräte nicht löschen, bleibt die zugehörige nicht-persistente VM im Initialisierungsstatus, bis Sie sie manuell aus dem Azure AD-Portal entfernen. Lassen Sie hierfür die Verwaltung in Azure AD eingebundener Geräte für Hostverbindungen mithilfe der Oberfläche "Vollständige Konfiguration"zu oder führen Sie die folgenden Schritte aus:
    a) Melden Sie sich im Azure-Portal an und navigieren Sie zu **Azure Active Directory > Roles and administrators**.
    b) Suchen Sie nach der integrierten Rolle **Cloud Device Administrator** und klicken Sie auf **Add assignments**, um die Rolle dem Dienstprinzipal der Anwendung zuzuweisen, die von der Hostverbindung verwendet wird.
    c) Führen Sie mit dem Citrix Remote PowerShell SDK die folgenden Befehle aus, um die bestehenden `CustomProperties` der Hostverbindung abzurufen. `${HostingConnectionName}` bezieht sich auf den Namen der Hostverbindung.
        i. Öffnen Sie ein **PowerShell**-Fenster.
        ii. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen **PowerShell**-Module zu laden.
        iii. Führen Sie den folgenden Befehl aus, um die vorhandenen benutzerdefinierten Eigenschaften der Hostverbindung abzurufen.

```
(Get-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

iv. Kopieren Sie die CustomProperties aus der Verbindung in einen Editor und hängen Sie die Eigenschaftseinstellung <Property xsi:type="StringProperty"Name ="AzureAdDeviceManagement"Value="true"/> an.

v. Weisen Sie im **PowerShell**-Fenster den geänderten benutzerdefinierten Eigenschaften eine Variable zu. Beispiel: $UpdatedCustomProperties='< CustomProperties ...</CustomProperties>'.

vi. Setzen Sie die benutzerdefinierte Eigenschaft auf die Hostverbindung zurück:

```
Set-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```

vii. Führen Sie den Befehl (Get-Item -LiteralPath XDHyp:\Connections \${ HostingConnectionName } ).CustomProperties aus, um die aktualisierten Einstellungen der benutzerdefinierten Eigenschaften zu verifizieren.

Sie können in Azure AD eingebundene Kataloge mit der Oberfläche "Vollständige Konfiguration"oder mit **PowerShell** erstellen.

### Verwenden der Benutzeroberfläche für die vollständige Konfiguration

Die folgenden Informationen ergänzen die Anweisungen unter Erstellen von Maschinenkatalogen. Folgen Sie zum Erstellen eines Katalogs mit Azure AD-Einbindung den allgemeinen Anweisungen in dem Artikel. Beachten Sie besonders die spezifischen Details für Kataloge mit Azure AD-Einbindung.

Im Assistenten für die Katalogerstellung:

1. Auf der **Image**:
   - Wählen Sie 2106 oder höher als Funktionsebene.
   - Wählen Sie **Ein Maschinenprofil verwenden** und dann in der Liste die entsprechende Maschine.
2. Wählen Sie auf der Seite **Maschinenidentitäten** die Option **In Azure Active Directory eingebunden**. Erstellte Maschinen gehören einer Organisation und sind mit einem Azure AD-Konto dieser Organisation angemeldet. Sie existieren nur in der Cloud.

   > **Hinweis:**
   >
   > - Der Identitätstyp **In Azure Active Directory eingebunden** erfordert Version 2106 oder

> höher als minimale Funktionsebene für den Katalog.
> - Die Maschinen werden in die Azure AD-Domäne eingebunden, die dem Mandanten zugeordnet ist, an den die Hostingverbindung gebunden ist.

3. Den Benutzern muss explizit Zugriff in Azure zur Anmeldung bei den Maschinen mit ihren AAD-Anmeldeinformationen gewährt werden. Weitere Informationen finden Sie im Abschnitt In Azure Active Directory eingebunden.

### Verwenden von PowerShell

Nachfolgend sind die **PowerShell**-Schritte aufgeführt, die den Verfahren in "Vollständige Konfiguration"entsprechen. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Der Unterschied zwischen mit einem On-Premises-AD verbundenen Katalogen und solchen mit Azure AD-Einbindung liegt in der Erstellung des Identitätspools und des Provisioningschemas.

Zum Erstellen eines Identitätspools für Kataloge mit Azure AD-Einbindung gehen Sie folgendermaßen vor:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
     WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
     NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
     -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Zum Erstellen eines Provisioningschemas für Kataloge mit Azure AD-Einbindung ist der Parameter**MachineProfile** in New-ProvScheme erforderlich:

```
1 New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
     schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.
     w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty
     `" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
     StringProperty`" Name=`"StorageType`" Value=`"StandardSSD_LRS`" /><
     Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
     Windows_Server`" /></CustomProperties>" -HostingUnitName "
     AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
     InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
     AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
     MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
     azuread-rg.resourcegroup\azuread-
     small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
     NetworkMapping @{
2  "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
       US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
      azuread-vnet.virtualprivatecloud\Test_VNET.network" }
```

```
3    -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
        Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
        \AzureResource\serviceoffering.folder\Standard_DS1_v2.
        serviceoffering"
4  <!--NeedCopy-->
```

Alle anderen Befehle zum Erstellen von Katalogen mit Azure AD-Einbindung sind mit denen für herkömmliche On-Premises-AD-Kataloge identisch.

### Anzeigen des Status der Azure AD-Einbindung

In der Schnittstelle "Vollständige Konfiguration"wird der Status der Azure AD-Einbindung angezeigt, wenn die Maschinen mit Azure AD-Einbindung in einer Bereitstellungsgruppe eingeschaltet sind. Um den Status anzuzeigen, identifizieren Sie mit Suchen diese Maschinen und prüfen Sie dann die **Maschinenidentität** für jede Maschine auf der Registerkarte **Details** im unteren Bereich. Die folgenden Informationen können unter **Maschinenidentität** angezeigt werden:

- In Azure AD eingebunden
- Noch nicht mit Azure AD verbunden

> **Hinweis:**
>
> Maschinen ohne Azure AD-Einbindung werden nicht beim Delivery Controller registriert. Ihr Registrierungsstatus wird als **Initialisierung** angezeigt.

In der Oberfläche "Vollständige Konfiguration"können Sie außerdem erfahren, warum Maschinen nicht verfügbar sind. Klicken Sie dazu im Knoten **Suchen** auf eine Maschine, aktivieren Sie im unteren Bereich auf der Registerkarte **Details** die Option **Registrierung**, und lesen Sie dann den Tooltip, um weitere Informationen zu erhalten.

### Bereitstellungsgruppe

Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

### Aktivieren von Rendezvous

Wenn die Bereitstellungsgruppe erstellt ist, können Sie Rendezvous aktivieren. Weitere Informationen finden Sie unter Rendezvous V2.

### Problembehandlung

Wenn Maschinen keine Azure AD-Einbindung aufweisen, gehen Sie wie folgt vor:

- Überprüfen Sie, ob die vom System zugewiesene verwaltete Identität für die Maschinen aktiviert ist. Für mit MCS bereitgestellte Maschinen muss diese automatisch aktiviert sein. Wenn vom System keine verwaltete Identität zugewiesen wurde, schlägt die Einbindung in Azure AD fehl. Wenn die vom System zugewiesene verwaltete Identität für mit MCS bereitgestellte Maschinen nicht aktiviert ist, kann dies folgenden Grund haben:
  - `IdentityType` des Identitätspools, der dem Provisioningschema zugeordnet ist, ist nicht auf `AzureAD` festgelegt. Sie können dies überprüfen, indem Sie `Get-AcctIdentityPool` ausführen.
- Überprüfen Sie bei Katalogen, die Masterimages mit VDA-Version 2206 oder früher verwenden, den Bereitstellungsstatus der **AADLoginForWindows**-Erweiterung für die Maschinen. Wenn die Erweiterung **AADLoginForWindows** nicht vorhanden ist, kann dies folgende Gründe haben:
  - `IdentityType` des Identitätspools, der dem Provisioningschema zugeordnet ist, ist nicht auf `AzureAD` festgelegt. Sie können dies überprüfen, indem Sie `Get-AcctIdentityPool` ausführen.
  - Die Installation der Erweiterung **AADLoginForWindows** wird von der Azure-Richtlinie blockiert.
- Wenn das Provisioning der Erweiterung **AADLoginForWindows** fehlschlägt, können Sie zur Problembehandlung die Protokolle unter `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` auf der mit MCS bereitgestellten Maschine überprüfen.

  > **Hinweis:**
  >
  > MCS ist nicht auf die `AADLoginForWindows`-Erweiterung angewiesen, um eine VM mit Azure AD zu verbinden, wenn ein Masterimage mit VDA-Version 2209 oder höher verwendet wird. In diesem Fall wird die `AADLoginForWindows`-Erweiterung nicht auf der von MCS bereitgestellten Maschine installiert. Daher können keine Protokolle zur Bereitstellung von `AADLoginForWindows`-Erweiterungen gesammelt werden.

- Führen Sie auf der mit MCS bereitgestellten Maschine den Befehl `dsregcmd /status` aus, um den Status der Azure AD-Einbindung und Debugprotokolle zu überprüfen.
- Aktivieren Sie die Windows-Ereignisprotokolle unter **Anwendungs- und Dienstprotokolle > Microsoft > Windows > Benutzergeräteregistrierung**.
- Führen Sie `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }` aus, um die Konfiguration der Azure AD-Geräteverwaltung zu überprüfen.

  Stellen Sie Folgendes sicher:

- Der Wert der Eigenschaft `AzureAdDeviceManagement` in `CustomProperties` ist **true**.
- Der Wert der Eigenschaft `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` in den Metadaten ist **true**.

Wenn `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` auf **false** gesetzt ist, hat der `ServicePrincipal` der von der Hostverbindung verwendeten Anwendung keine ausreichenden Berechtigungen für die Azure AD-Geräteverwaltung. Weisen Sie dem `ServicePrincipal` die Rolle **Cloud Device Administrator** zu, um das Problem zu beheben.

### Dynamische Azure Active Directory-Sicherheitsgruppe

Dynamische Gruppenregeln ordnen die virtuellen Maschinen im Katalog einer dynamischen Sicherheitsgruppe zu, basierend auf dem Benennungsschema des Maschinenkatalogs.

Ist das Benennungsschema des Maschinenkatalogs Test### (# steht für Zahl), erstellt Citrix die dynamische Mitgliedschaftsregel ^*Test[0-9]{3}$* in der dynamischen Sicherheitsgruppe. Liegt der Name einer von Citrix erstellten VM zwischen Test001 und Test999, wird die VM in die dynamische Sicherheitsgruppe aufgenommen.

> **Hinweis:**
>
> Liegt der Name einer von Ihnen manuell erstellten VM zwischen Test001 und Test999, wird die VM ebenfalls in die dynamische Sicherheitsgruppe aufgenommen. Dies ist eine Einschränkung der dynamischen Sicherheitsgruppe.

Dynamische Sicherheitsgruppen sind nützlich, wenn Sie VMs über Azure Active Directory (Azure AD) verwalten möchten. Dies ist auch nützlich, wenn Sie Richtlinien für bedingten Zugriff anwenden oder Apps aus Intune verteilen möchten, indem Sie die VMs anhand der dynamischen Azure AD-Sicherheitsgruppe filtern.

Sie können für Folgendes **PowerShell**-Befehle verwenden:

- Maschinenkatalog mit dynamischer Azure AD-Sicherheitsgruppe erstellen
- Sicherheitsgruppenfeature für einen Azure AD-Katalog aktivieren
- Maschinenkatalog mit dynamischer Azure AD-Sicherheitsgruppe löschen

> **Wichtig:**
>
> - Um einen Maschinenkatalog mit dynamischer Azure AD-Sicherheitsgruppe zu erstellen, Maschinen zum Katalog hinzuzufügen und den Maschinenkatalog zu löschen, benötigen Sie einen Azure AD-Zugriffstoken. Informationen zum Abrufen eines Azure AD-

> Zugriffstokens finden Sie unter https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/.
> - Um einen Zugriffstoken in Azure AD anzufordern, fordert Citrix die Berechtigung **Group.ReadWrite.all** für die Microsoft Graph-API an. Ein Azure AD-Benutzer, der über eine mandantenweite Berechtigung zur Administratoreinwilligung verfügt, kann **Group.ReadWrite.All**-Berechtigung für die Microsoft Graph-API gewähren. Informationen zum Erteilen einer mandantenweiten Administratoreinwilligung für eine Anwendung in Azure Active Directory (Azure AD) finden Sie im Microsoft-Dokument https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/.

**Maschinenkatalog mit dynamischer Azure AD-Sicherheitsgruppe erstellen**

1. Wählen Sie in der Benutzeroberfläche für die Einrichtung des Maschinenkatalogs der webbasierten Konsole auf der Seite **Maschinenidentitäten** die Option **In Azure Active Directory eingebunden**.
2. Melden Sie sich bei Azure AD an.
3. Rufen Sie den Zugriffstoken für die MS Graph-API ab. Verwenden Sie den Zugriffstoken als Wert für Parameter `$AzureADAccessToken` für die **PowerShell**-Befehle.
4. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Name der dynamischen Sicherheitsgruppe im Mandanten vorhanden ist.

```
Get-AcctAzureADSecurityGroup
 –AccessToken  $AzureADAccessToken
 –Name "SecurityGroupName"
<!--NeedCopy-->
```

5. Erstellen Sie einen Maschinenkatalog mit der Mandanten-ID, dem Zugriffstoken und der dynamischen Sicherheitsgruppe. Führen Sie den folgenden Befehl aus, um einen Identitätspool mit `IdentityType=AzureAD` und eine dynamische Sicherheitsgruppe in Azure zu erstellen.

```
New-AcctIdentityPool
-AllowUnicode
-IdentityPoolName "SecurityGroupCatalog"
-NamingScheme "SG-VM-###"
-NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
-WorkgroupMachine
-IdentityType "AzureAD"
-DeviceManagementType "None"
-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupName "SecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Sicherheitsgruppenfeature für einen Azure AD-Katalog aktivieren

Sie können das Feature dynamischer Sicherheitsgruppen für einen Azure AD-Katalog aktivieren, bei dessen Erstellung das Feature nicht aktiviert wurde. Gehen Sie hierzu folgendermaßen vor:

1. Erstellen Sie manuell eine neue dynamische Sicherheitsgruppe. Sie können auch eine vorhandene dynamische Sicherheitsgruppe verwenden.
2. Melden Sie sich bei Azure AD an und rufen Sie den Zugriffstoken für die MS Graph-API ab. Verwenden Sie den Zugriffstoken als Wert für Parameter `$AzureADAccessToken` für die **PowerShell**-Befehle.

   > **Hinweis:**
   >
   > Informationen zu den von dem Azure AD-Benutzer benötigten Berechtigungen finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/.

3. Führen Sie den folgenden Befehl aus, um den Identitätspool mit der erstellten dynamischen Azure AD-Sicherheitsgruppe zu verbinden.

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Wenn Sie das Benennungsschema aktualisieren, aktualisiert Citrix das Benennungsschema an eine neue Mitgliedschaftsregel. Wenn Sie den Katalog löschen, wird die Mitgliedschaftsregel gelöscht nicht aber die Sicherheitsgruppe.

### Maschinenkatalog mit dynamischer Azure AD-Sicherheitsgruppe löschen

Wenn Sie einen Maschinenkatalog löschen, wird die mit Azure AD verbundene Sicherheitsgruppe ebenfalls gelöscht.

Gehen Sie wie folgt vor, um die dynamische Azure AD-Sicherheitsgruppe zu löschen:

1. Melden Sie sich bei Azure AD an.
2. Rufen Sie den Zugriffstoken für die MS Graph-API ab. Verwenden Sie den Zugriffstoken als Wert für Parameter `$AzureADAccessToken` für die **PowerShell**-Befehle.
3. Führen Sie den folgenden Befehl aus:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Dynamische Azure AD-Sicherheitsgruppe unter einer vorhandenen Azure AD-Sicherheitsgruppe erstellen

Sie können eine dynamische Azure AD-Sicherheitsgruppe unter einer vorhandenen Azure AD-Sicherheitsgruppe erstellen. Sie können die folgenden Aktionen ausführen:

- Informationen zur Sicherheitsgruppe abrufen.
- Rufen Sie alle zugewiesenen Azure AD-Sicherheitsgruppen ab, die vom On-Premises-AD-Server synchronisiert werden, oder die zugewiesenen Sicherheitsgruppen, denen Azure AD-Rollen zugewiesen werden können.
- Alle dynamischen Azure AD-Sicherheitsgruppen abrufen.
- Die dynamische Azure AD-Sicherheitsgruppe als Mitglied der zugewiesenen Azure AD-Gruppe hinzufügen.
- Die Mitgliedschaft zwischen der dynamischen Azure AD-Sicherheitsgruppe und der zugewiesenen Azure AD-Sicherheitsgruppe entfernen, wenn die dynamische Azure AD-Sicherheitsgruppe zusammen mit dem Maschinenkatalog gelöscht wird.

Sie können auch explizite Fehlermeldungen sehen, wenn einer der Vorgänge fehlschlägt.

**Voraussetzung:**

Sie benötigen den Zugriffstoken für die MS Graph-API, wenn Sie die **PowerShell**-Befehle ausführen.

Zugriffstoken abrufen:

1. Öffnen Sie den Microsoft Graph-Explorer und melden Sie sich bei Azure AD an.
2. Stellen Sie sicher, dass Sie über Einwilligung für **Group.ReadWrite.all** und **GroupMember.ReadWrite.all** verfügen.
3. Rufen Sie den Zugriffstoken vom Microsoft Graph-Explorer ab. Verwenden Sie den Zugriffstoken für die **PowerShell**-Befehle.

Sicherheitsgruppeninformationen anhand der Gruppen-ID abrufen:

1. Rufen Sie den Zugriffstoken ab.
2. Suchen Sie die Gruppenobjekt-ID im Azure-Portal.
3. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
```

```
<!--NeedCopy-->
```

Sicherheitsgruppen anhand des Anzeigenamens abrufen:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```

Sicherheitsgruppen abrufen, deren Anzeigename eine Teilzeichenfolge enthält:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

Alle Azure AD zugewiesenen vom On-Premises-AD-Server synchronisierten Sicherheitsgruppen oder die zugewiesenen Sicherheitsgruppen, denen Azure AD-Rollen zugewiesen werden können, abrufen:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

Alle dynamischen Azure AD-Sicherheitsgruppen abrufen:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

Azure AD-zugewiesene Sicherheitsgruppen mit maximaler Datensatzanzahl abrufen:

1. Rufen Sie den Zugriffstoken ab.

2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

Eine dynamische Azure AD-Sicherheitsgruppe als Mitglied der Azure AD-zugewiesenen Sicherheitsgruppe hinzufügen:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

Mitglieder der Azure AD-zugewiesenen Sicherheitsgruppe abrufen:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> **Hinweis:**
>
> `Get-AcctAzureADSecurityGroupMember` ruft nur die direkten Mitglieder des Sicherheitsgruppentyps unter der Azure AD-zugewiesenen Sicherheitsgruppe ab.

Mitgliedschaft zwischen der dynamischen Azure AD-Sicherheitsgruppe und der Azure AD-zugewiesenen Sicherheitsgruppe entfernen, wenn die dynamische Azure AD-Sicherheitsgruppe zusammen mit dem Maschinenkatalog gelöscht wird:

1. Rufen Sie den Zugriffstoken ab.
2. Führen Sie in der **PowerShell**-Konsole den folgenden **PowerShell**-Befehl aus:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Namen der dynamischen Azure AD-Sicherheitsgruppe ändern

Sie können den Namen der einem Maschinenkatalog zugeordneten dynamischen Azure AD-Sicherheitsgruppe ändern. Durch diese Änderung werden die im Azure AD-Identitätspoolobjekt gespeicherten Sicherheitsgruppeninformationen mit den im Azure-Portal gespeicherten Informationen konsistent.

> **Hinweis:**
>
> Die dynamischen Azure AD-Sicherheitsgruppen umfassen keine mit dem On-Premises-AD synchronisierten Sicherheitsgruppen oder andere Gruppentypen wie Office 365-Gruppen.

Sie können den Namen der dynamischen Azure AD-Sicherheitsgruppe in der Oberfläche "Vollständige Konfiguration"und mit **PowerShell**-Befehlen ändern.

Gehen Sie zum Ändern des Namens der dynamischen Azure AD-Sicherheitsgruppe mithilfe von **PowerShell** folgendermaßen vor:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen **PowerShell**-Module zu laden.
3. Führen Sie den Befehl `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]` aus.

Sie erhalten eine Fehlermeldung, wenn der Name der dynamischen Azure AD-Sicherheitsgruppe nicht geändert werden kann.

## Kataloge mit aktiviertem Microsoft Intune erstellen

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

In diesem Artikel wird beschrieben, wie Sie mit Citrix DaaS für Microsoft Intune aktivierte Kataloge erstellen. Sie können Microsoft Intune mit der Oberfläche "Vollständige Konfiguration"oder PowerShell aktivieren.

Weitere Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter Microsoft Intune.

### Verwenden der Benutzeroberfläche für die vollständige Konfiguration

Die folgenden Informationen ergänzen die Anweisungen unter Erstellen von Maschinenkatalogen. Das Feature erfordert bei der Katalogerstellung die Auswahl von **In Azure Active Directory eingebunden** für **Maschinenidentitäten**. Folgen Sie den allgemeinen Anweisungen in dem Artikel unter besonderer Beachtung der featurespezifischen Details.

Im Assistenten für die Katalogerstellung:

- Wählen Sie auf der Seite **Maschinenidentitäten** die Option **In Azure Active Directory eingebunden** und dann **Maschinen bei Microsoft Intune registrieren**. Wenn die Option aktiviert ist, registrieren Sie die Maschinen bei Microsoft Intune für die Verwaltung.

### PowerShell verwenden

Nachfolgend sind die PowerShell-Schritte aufgeführt, die den Verfahren in "Vollständige Konfiguration"entsprechen.

Um Maschinen mit dem Remote PowerShell SDK bei Microsoft Intune zu registrieren, verwenden Sie den Parameter `DeviceManagementType` in `New-AcctIdentityPool`. Das Feature erfordert, dass der Katalog Azure AD-eingebunden ist und dass Azure AD über die richtige Microsoft Intune-Lizenz verfügt. Beispiel:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
     IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
     AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
     NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
     ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

### Problembehandlung

Führen Sie folgende Schritte aus, wenn Maschinen nicht bei Microsoft Intune registriert werden können:

- Überprüfen Sie, ob die mit MCS bereitgestellten Maschinen in Azure AD eingebunden sind. Ohne Azure AD-Einbindung können die Maschinen nicht bei Microsoft Intune registriert werden. Informationen zur Vorgehensweise bei Problemen mit der Azure AD-Einbindung finden Sie unter https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html.
- Überprüfen Sie, ob Ihrem Azure AD-Mandanten die passende Intune-Lizenz zugewiesen wurde. Informationen zur Lizenzanforderung von Microsoft Intune finden Sie unter https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses.

- Überprüfen Sie bei Katalogen, die Masterimages mit VDA-Version 2206 oder früher verwenden, den Bereitstellungsstatus der **AADLoginForWindows**-Erweiterung für die Maschinen. Wenn die Erweiterung **AADLoginForWindows** nicht vorhanden ist, kann dies folgende Gründe haben:
  - `IdentityType` des Identitätspools, der dem Provisioningschema zugeordnet ist, ist nicht auf `AzureAD` festgelegt, oder `DeviceManagementType` ist nicht auf `Intune` festgelegt. Sie können dies überprüfen, indem Sie `Get-AcctIdentityPool` ausführen.
  - Die Installation der Erweiterung **AADLoginForWindows** wird von der Azure-Richtlinie blockiert.
- Wenn das Provisioning der Erweiterung **AADLoginForWindows** fehlschlägt, können Sie zur Problembehandlung die Protokolle unter `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` auf der mit MCS bereitgestellten Maschine überprüfen.

  > **Hinweis:**
  >
  > MCS ist nicht auf die `AADLoginForWindows`-Erweiterung angewiesen, um eine VM mit Azure AD zu verbinden und sich bei Microsoft Intune zu registrieren, wenn ein Masterimage mit VDA-Version 2209 oder höher verwendet wird. In diesem Fall wird die `AADLoginForWindows`-Erweiterung nicht auf der von MCS bereitgestellten Maschine installiert. Daher können keine Protokolle zur Bereitstellung von `AADLoginForWindows`-Erweiterungen gesammelt werden.

- Aktivieren Sie die Windows-Ereignisprotokolle unter **Anwendungs- und Dienstprotokolle > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.

## Kataloge mit Azure Active Directory-Hybrideinbindung erstellen

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

In diesem Artikel wird beschrieben, wie Sie Kataloge mit Azure Active Directory-Hybrideinbindung mit Citrix DaaS erstellen.

Sie können in Azure AD eingebundene Kataloge mit der Oberfläche "Vollständige Konfiguration"oder mit PowerShell erstellen.

Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter Azure Active Directory-Hybrideinbindung.

### Verwenden der Benutzeroberfläche für die vollständige Konfiguration

Die folgenden Informationen ergänzen die Anweisungen unter Erstellen von Maschinenkatalogen. Folgen Sie zum Erstellen eines Katalogs mit Azure AD-Hybrideinbindung den allgemeinen Anweisungen in dem Artikel. Achten Sie besonders auf die spezifischen Details für Kataloge mit Azure AD-Hybrideinbindung.

Im Assistenten für die Katalogerstellung:

- Wählen Sie auf der Seite **Maschinenidentitäten** die Option **Azure Active Directory-Hybrideinbindung**. Die erstellten Maschinen gehören einer Organisation und sind mit einem Active Directory Domain Services-Konto dieser Organisation angemeldet. Sie existieren in der Cloud und on-premises.

> **Hinweis:**
>
> Wenn Sie **Azure Active Directory-Hybrideinbindung** als Identitätstyp auswählen, benötigt jede Maschine im Maschinenkatalog ein AD-Computerkonto.

### PowerShell verwenden

Nachfolgend sind die PowerShell-Schritte aufgeführt, die den Verfahren in "Vollständige Konfiguration"entsprechen. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Der Unterschied zwischen mit einem On-Premises-AD verbundenen Katalogen und solchen mit Azure AD-Hybrideinbindung liegt in der Erstellung des Identitätspools und der Maschinenkonten.

Zum Erstellen eines Identitätspools mit den Konten für Kataloge mit Azure AD-Hybrideinbindung gehen Sie folgendermaßen vor:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
```

```
Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
<!--NeedCopy-->
```

> **Hinweis:**
>
> `$password` ist das Kennwort für ein AD-Benutzerkonto mit Schreibberechtigung.

Alle anderen Befehle zum Erstellen von Katalogen mit Azure AD-Hybrideinbindung sind mit denen für herkömmliche On-Premises-AD-Kataloge identisch.

### Anzeigen des Status der Azure AD-Hybrideinbindung

In der Schnittstelle "Vollständige Konfiguration"wird der Status der Azure AD-Hybrideinbindung angezeigt, wenn die Maschinen mit Azure AD-Hybrideinbindung in einer Bereitstellungsgruppe eingeschaltet sind. Um den Status anzuzeigen, identifizieren Sie mit Suchen diese Maschinen und prüfen Sie dann die **Maschinenidentität** für jede Maschine auf der Registerkarte **Details** im unteren Bereich. Die folgenden Informationen können unter **Maschinenidentität** angezeigt werden:

- Azure AD-Hybrideinbindung
- Noch nicht mit Azure AD verbunden

> **Hinweis:**
>
> - Möglicherweise kommt es beim ersten Einschalten einer Maschine zu einer verzögerten Azure AD-Hybrideinbindung. Ursache ist das standardmäßige Synchronisierungsintervall für die Maschinenidentität (30 Minuten in Azure AD Connect). Maschinen erhalten erst dann eine Azure AD-Hybrideinbindung, wenn die Maschinenidentität über Azure AD Connect mit Azure AD synchronisiert wurde.
> - Maschinen ohne Azure AD-Hybrideinbindung werden nicht beim Delivery Controller registriert. Ihr Registrierungsstatus wird als **Initialisierung** angezeigt.

In der Oberfläche "Vollständige Konfiguration"können Sie außerdem erfahren, warum Maschinen nicht verfügbar sind. Klicken Sie dazu im Knoten **Suchen** auf eine Maschine, aktivieren Sie im unteren Bereich auf der Registerkarte **Details** die Option **Registrierung**, und lesen Sie dann den Tooltip, um weitere Informationen zu erhalten.

### Problembehandlung

Wenn Maschinen keine Azure AD-Hybrideinbindung aufweisen, gehen Sie wie folgt vor:

- Überprüfen Sie, ob das Maschinenkonto über das Microsoft Azure AD-Portal mit Azure AD synchronisiert wurde. Bei erfolgter Synchronisierung wird **Noch nicht mit Azure AD verbunden** angezeigt und die Registrierung ist ausstehend.

  Um Maschinenkonten mit Azure AD zu synchronisieren, stellen Sie Folgendes sicher:

  - Das Maschinenkonto befindet sich in der Organisationseinheit, die für die Synchronisierung mit Azure AD konfiguriert ist. Maschinenkonten ohne **userCertificate**-Attribut werden nicht mit Azure AD synchronisiert, selbst wenn sie in der Organisationseinheit sind, die für die Synchronisierung konfiguriert ist.
  - Das Attribut **userCertificate** wird im Maschinenkonto aufgefüllt. Verwenden Sie Active Directory Explorer, um das Attribut anzuzeigen.
  - Azure AD Connect muss nach Erstellung des Maschinenkontos mindestens eine Synchronisierung ausgeführt haben. Ist dies nicht der Fall, führen Sie in der PowerShell-Konsole der Azure AD Connect-Maschine den Befehl `Start-ADSyncSyncCycle -PolicyType Delta` manuell aus, um eine sofortige Synchronisierung auszulösen.

- Überprüfen Sie, ob das von Citrix verwaltete Geräteschlüsselpaar für die Azure AD-Hybrideinbindung einwandfrei an die Maschine übertragen wurde, indem Sie den Wert von **DeviceKeyPairRestored** unter **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** prüfen.

  Vergewissern Sie sich, dass der Wert 1 ist. Falls nicht, sind folgende Gründe möglich:

  - `IdentityType` des Identitätspools, der dem Provisioningschema zugeordnet ist, ist nicht auf `HybridAzureAD` festgelegt. Sie können dies überprüfen, indem Sie `Get-AcctIdentityPool` ausführen.
  - Die Maschine wurde nicht mit dem Provisioningschema des Maschinenkatalogs bereitgestellt.
  - Die Maschine ist nicht mit der lokalen Domäne verbunden. Die Verbindung mit der lokalen Domäne ist eine Voraussetzung für die Azure AD-Hybrideinbindung.

- Überprüfen Sie Diagnosemeldungen mit dem Befehl `dsregcmd /status /debug` auf der per MCS bereitgestellten Maschine.

  - War die Azure AD-Hybrideinbindung erfolgreich, lautet der Wert für **AzureAdJoined** und **DomainJoined** in der Befehlszeilenausgabe **YES**.

  - Falls nicht, konsultieren Sie die Microsoft-Dokumentation zur Problembehandlung: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.

  - Wird die Fehlermeldung **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** angezeigt, führen Sie den folgenden PowerShell-Befehl aus, um das Benutzerzertifikat zu reparieren:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
   UserCertificate
<!--NeedCopy-->
```

Weitere Informationen zu dem Problem mit dem Benutzerzertifikat finden Sie unter CTX566696.

## Erstellen nicht in eine Domäne eingebundener Kataloge

November 9, 2022

In diesem Artikel wird beschrieben, wie Sie nicht mit einer Domäne verbundene Kataloge mit Citrix DaaS erstellen.

Weitere Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter Nicht domänengebunden.

Vor dem Erstellen des Maschinenkatalogs benötigen Sie Folgendes:

1. Einen neuen Ressourcenstandort
   - Wählen Sie in der Citrix Cloud-Verwaltungsoberfläche im Hamburgermenü oben links **Ressourcenstandorte**.
   - Klicken Sie auf **+ Ressourcenstandort**.
   - Geben Sie den Namen für den neuen Ressourcenstandort ein und klicken Sie auf **Speichern**.
2. Erstellen Sie eine Hostverbindung. Weitere Informationen finden Sie unter Verbindungen erstellen und verwalten.

Mit Citrix DaaS können Sie Kataloge auf der Grundlage von Arbeitsgruppen oder nicht domänengebundenen Maschinen erstellen. Das Erstellen von Maschinen ohne Domäne hängt davon ab, wie der Kontoidentitätspool erstellt wird. Der Kontoidentitätspool wird von MCS zum Erstellen und Verfolgen von Maschinennamen während der Katalogbereitstellung verwendet.

Sie können Kataloge ohne Domänenbindung mit der Oberfläche "Vollständige Konfiguration"oder PowerShell erstellen.

### Verwenden der Schnittstelle für die vollständige Konfiguration

Die folgenden Informationen ergänzen die Anweisungen unter Erstellen von Maschinenkatalogen. Folgen Sie zum Erstellen eines Katalogs ohne Domänenbindung die allgemeinen Anweisungen in dem Artikel. Beachten Sie besonders die spezifischen Details für Kataloge ohne Domänenbindung.

Im Assistenten für die Katalogerstellung:

- Wählen Sie auf der Seite **Maschinenidentitäten** die Option **Gehört keiner Domäne an**. Die erstellten Maschinen werden mit keiner Domäne verbunden.

> **Hinweis:**
>
> Für den Identitätstyp **Gehört keiner Domäne an** ist VDA-Version 1811 oder höher als Mindestfunktionsebene für den Katalog erforderlich. Zur Bereitstellung aktualisieren Sie bei Bedarf die Mindestfunktionsebene.

### Verwenden von PowerShell

Nachfolgend werden die den in "Vollständige Konfiguration"ausgeführten Schritten entsprechenden PowerShell-Schritte aufgeführt.

Mit dem Remote PowerShell SDK können Sie einen Identitätspool für Kataloge ohne Domänenbindung erstellen.

In früheren Releases wurden beispielsweise alle Active Directory-Felder in einer einzigen Instanz bereitgestellt:

```
1 New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
      IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
      -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
      Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

In MCS werden jetzt die neuen PowerShell-Parameter **WorkgroupMachine** und **IdentityType** verwendet, um einen Identitätspool für Kataloge ohne Domänenbindung zu erstellen. Bei dem Beispiel oben müssen dank dieser Parameter nicht alle AD-spezifischen Parameter (einschließlich Anmeldeinformationen des Domänenadministrators) angegeben werden:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
      WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
      NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
      ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Alle anderen Befehle zum Erstellen von Katalogen ohne Domänenbindung sind mit denen für Kataloge mit Azure AD-Hybrideinbindung identisch.

## Maschinenkataloge verwalten

June 13, 2024

> **Hinweis:**
>
> In diesem Artikel wird beschrieben, wie Sie Kataloge mit der Benutzeroberfläche "Vollständige Konfiguration"und PowerShell-Befehlen verwalten. Wenn Sie einen Katalog mit Quick Deploy erstellt haben und diese Schnittstelle auch zur Verwaltung des Katalogs verwenden, folgen Sie den Anweisungen unter Verwalten von Katalogen in Quick Deploy.

## Einführung

Sie können Maschinen in Maschinenkatalogen hinzufügen, entfernen und umbenennen, Maschinenbeschreibungen ändern und die Active Directory-Computerkonten des Katalogs verwalten.

Zur Verwaltung von Katalogen gehören ggf. auch die Aktualisierung des Betriebssystems und der Antivirensoftware der enthaltenen Maschinen, ein Upgrade des Betriebssystems und Änderungen an der Konfiguration.

- Maschinenkataloge mit gepoolt-zufälligen Maschinen, die mit Maschinenerstellungsdienste (MCS) erstellt wurden, können Sie pflegen, indem Sie das Image des Katalogs und dann die Maschinen aktualisieren. So können Sie eine große Anzahl Maschinen effizient aktualisieren.
- Bei Katalogen mit statischen (permanent zugewiesenen) Maschinen können Sie das aktuell verwendete Image oder die Vorlage anpassen. Das neue Image oder die neue Vorlage wird jedoch nur auf die später hinzugefügten Maschinen angewandt.
- Bei Katalogen mit Remote-PC-Zugriff verwalten Sie Updates an den Benutzermaschinen außerhalb der Verwaltungsoberfläche "Vollständige Konfiguration". Tun Sie dies für einzelne Maschinen oder für alle Maschinen mit Bereitstellungssoftware von Drittanbietern.

Weitere Informationen zum Erstellen und Verwalten von Verbindungen mit Hosthypervisors und Clouddiensten finden Sie unter Verbindungen und Ressourcen erstellen und verwalten.

> **Hinweis:**
>
> MCS unterstützt Windows 10 IoT Core und Windows 10 IoT Enterprise nicht. Weitere Informationen finden Sie auf der Website von Microsoft.

## Informationen zu persistenten Instanzen

Wird ein Masterimage für einen MCS-Katalog mit persistenten Maschinen aktualisiert, verwenden alle dem Katalog neu hinzugefügten Maschinen das aktualisierte Image. Bereits vorhandene Maschinen verwenden weiterhin das ursprüngliche Masterimage. Das Update eines Images wird für jeden anderen Katalogtyp auf die gleiche Weise durchgeführt. Beachten Sie Folgendes:

- Bei persistenten Datenträgerkatalogen werden die bereits vorhandenen Maschinen nicht auf das neue Image aktualisiert. Alle neu dem Katalog hinzugefügten Maschinen verwenden aber das neue Image.
- Bei nichtpersistenten Datenträgerkatalogen wird das Maschinenimage beim nächsten Neustart nur dann aktualisiert, wenn dieser über in Studio oder PowerShell ausgeführt wird. Wird die Maschine außerhalb von Studio vom Hypervisor neu gestartet, wird der Datenträger nicht zurückgesetzt.
- Bei nichtpersistenten Katalogen müssen Images in separaten Katalogen sein, wenn Sie unterschiedliche Images für verschiedene Maschinen brauchen.

### Maschinenkataloge verwalten

Sie können einen Maschinenkatalog auf zweierlei Art verwalten:

- Benutzeroberfläche für die vollständige Konfiguration
- PowerShell verwenden

### Benutzeroberfläche für die vollständige Konfiguration verwenden

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mithilfe der Oberfläche für die vollständige Konfiguration verwalten können:

- Katalogdetails anzeigen
- Maschinen zum Maschinenkatalog hinzufügen
- Löschen von Maschinen aus einem Maschinenkatalog
- Bearbeiten eines Katalogs
- Umbenennen von Maschinenkatalogen
- Löschen eines Katalogs
- Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog
- Masterimage für einen Katalog ändern
- Funktionsebene ändern oder Änderung rückgängig machen
- Klonen von Katalogen
- Organisieren von Katalogen mit Ordnern
- Automatische Upgrades für VDAs konfigurieren
- Verwalten eines Konfigurationssatzes für einen Katalog
- Katalogerstellung erneut versuchen
- (Nur nicht von Citrix bereitgestellte VDAs) Registrierungstoken generieren und verwalten

### Katalogdetails anzeigen

1. Verwenden Sie die Suchfunktion, um einen bestimmten Maschinenkatalog zu finden. Anweisungen finden Sie unter Nach Instanzen suchen.
2. Wählen Sie aus den Suchergebnissen nach Bedarf einen Katalog aus.
3. In der folgenden Tabelle finden Sie Beschreibungen der Katalogspalten.
4. Klicken Sie im unteren Detailbereich auf eine Registerkarte, um weitere Informationen zu diesem Katalog zu erhalten.

| Spalte | Beschreibung |
| --- | --- |
| Maschinenkatalog | Der Name und der Zuteilungstyp des Katalogs. Zu den Zuteilungstypen gehören Zufällig: Maschinen im Katalog werden einem Benutzer nach dem Zufallsprinzip zugewiesen. Permanent: Maschinen im Katalog sind einem Benutzer dauerhaft zugewiesen. |
| Maschinentyp | Der unterstützte Sitzungstyp der Maschinen im Katalog. Mögliche Werte: Betriebssystemtyp: Multisitzungs-OS (virtuell); Benutzerdaten: Verwerfen. Betriebssystemtyp: Multisitzungs-OS (virtuell); Benutzerdaten: auf lokalem Datenträger Betriebssystemtyp: Einzelsitzungs-OS (Remote-PC-Zugriff) Betriebssystemtyp: Einzelsitzungs-OS (virtuell); Provisioningmethode: Manuell; Betriebssystemtyp: Einzelsitzungs-OS (virtuell); Provisioningmethode: Citrix Provisioning Services (MCS-Maschinen), Benutzerdaten: Verwerfen Betriebssystemtyp: Einzelsitzungs-OS (virtuell); Provisioningmethode: Citrix Provisioning Services (MCS-Maschinen), Benutzerdaten: auf lokalem Datenträger |
| Maschinenanzahl | Die Anzahl der Maschinen im Katalog. |
| Zugewiesene Anzahl | Die Anzahl der Maschinen im Katalog, die einer Bereitstellungsgruppe zugewiesen sind. |
| Ordner | Der Speicherort des Katalogs im **Maschinenkatalogbaum**. Hier wird der Name des Ordners angezeigt, in dem sich der Katalog befindet (einschließlich des abschließenden umgekehrten Schrägstrichs), oder −, wenn sich der Katalog auf der Stammebene befindet. |
| VDA-Upgrade | VDA-Upgradestatus. Mögliche Werte: Nicht konfiguriert, Geplant, Verfügbar und Aktuell. |

| Spalte | Beschreibung |
| --- | --- |
| Imagestatus | Der Status der Imageaktualisierung des Katalogs. Gilt nur für nicht persistente Maschinenkataloge. Mögliche Werte sind: Vollständig aktualisiert, Teilweise aktualisiert, Ausstehende Aktualisierungen, Vorbereitet |

### Maschinen zum Maschinenkatalog hinzufügen

Vorbereitungen:

- Stellen Sie sicher, dass der Virtualisierungshost (Hypervisor oder Clouddienstanbieter) genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der zusätzlichen Maschinen hat.
- Vergewissern Sie sich, dass Sie genügend ungenutzte Active Directory-Computerkonten haben. Wenn Sie bestehende Konten verwenden, können Sie nur so viele Maschinen erstellen, wie Sie Konten haben.
- Wenn Sie mit der Verwaltungsoberfläche "Vollständige Konfiguration"Active Directory-Computerkonten für die zusätzlichen Maschinen erstellen, müssen Sie die erforderlichen Domänenadministratorrechte haben.

> **Tipp:**
>
> Wenn das Citrix DaaS-Konto, das zum Hinzufügen von Maschinen zum Maschinenkatalog verwendet wird, eingeschränkte AD-Berechtigungen hat, fügen Sie alle Cloud Connectors, die Sie verwenden möchten, auf dem Bildschirm **Anmelden bei** hinzu.

Hinzufügen von Maschinen zum Maschinenkatalog

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Maschinenkatalog und dann in der Aktionsleiste die Option **Maschinen hinzufügen**.
3. Wählen Sie auf der Seite **Virtuelle Maschinen** die Anzahl der hinzuzufügenden virtuellen Maschinen aus.
4. Konfigurieren Sie die Einstellungen auf der Seite **Maschinenidentitäten** wie folgt:
    - Sie wählen eine Identität aus der Liste aus.

- Geben Sie ggf. an, ob neue Konten erstellt oder vorhandene verwendet werden sollen, und geben Sie den Ort (die Domäne) der Konten an.

  Gibt es nicht genügend Active Directory-Konten für die Zahl der VMs, die Sie hinzufügen möchten, wählen Sie die Domäne und den Speicherort, an dem Konten erstellt werden sollen.

  Wenn Sie bestehende Active Directory-Konten verwenden, navigieren Sie zu den Konten oder wählen Sie **Importieren** und geben Sie eine `.csv`-Datei mit Kontonamen an. Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Die Konten werden in der Oberfläche "Vollständige Konfiguration"verwaltet. Gestatten Sie der Oberfläche, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort an (muss für alle Konten gleich sein).

- Wenn dieser Identitätspool von anderen Katalogen verwendet wird, können Sie ihn nicht über die vollständige Konfiguration in einen anderen Pool ändern. Verwenden Sie stattdessen das PowerShell-Cmdlet **Set-ProvScheme**. Weitere Informationen finden Sie in der Dokumentation zum Citrix Virtual Apps and Desktops SDK.

- Legen Sie ein Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Beispiel: Das Benennungsschema "PC-Vertrieb-##"(und Aktivieren von 0-9) bewirkt eine Benennung der Computerkonten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03"usw.

- Optional können Sie angeben, womit die Kontonamen beginnen sollen.

  Beachten Sie bei der Angabe, womit die Kontonamen beginnen sollen, Folgendes: Wenn die Startzahlen oder -buchstaben bereits verwendet werden, werden bei der Erstellung des ersten Kontos anschließend die nächsten freien Zahlen bzw. Buchstaben verwendet.

  Weitere Informationen zur Anpassung der Sequenznummer von Maschinen, die mit MCS bereitgestellt werden, mit PowerShell-Befehlen finden Sie unter Sequenznummer des Maschinennamens verwalten.

5. Wählen Sie auf der Seite **Domänenanmeldeinformationen** die Option **Anmeldeinformationen eingeben** und geben Sie Benutzeranmeldeinformationen mit ausreichenden Berechtigungen zum Erstellen von Maschinenkonten ein.

Die Maschinen werden in einem Hintergrundprozess erstellt, der beim Erstellen einer großen Zahl von Maschinen lange dauern kann. Die Maschinenerstellung wird auch dann fortgesetzt, wenn Sie die Verwaltungsoberfläche "Vollständige Konfiguration"schließen.

### Verwenden von CSV-Dateien zum Massenhinzufügen von Maschinen zu einem Katalog

Sie können CSV-Dateien zum Massenhinzufügen von Maschinen verwenden. Das Feature steht für alle Kataloge mit Ausnahme solcher zur Verfügung, die per MCS bereitgestellt wurden.

Führen Sie die folgenden Schritte aus, um Maschinen in Massen zu einem Katalog hinzuzufügen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Maschinenkatalog und dann in der Aktionsleiste die Option **Maschinen hinzufügen**. Das Fenster **Maschine hinzufügen** wird angezeigt.
3. Wählen Sie **CSV-Datei hinzufügen**. Das Fenster **Maschinen in Massen hinzufügen** wird angezeigt.
4. Wählen Sie **CSV-Vorlage herunterladen**.
5. Füllen Sie die Vorlagendatei aus.
6. Navigieren Sie zu der Datei, um sie hochzuladen (oder verwenden Sie Drag & Drop).
7. Wählen Sie **Validieren**, um Ihren Import zu überprüfen.
8. Wählen Sie **Importieren**, um den Vorgang abzuschließen.

### Überlegungen zum Hinzufügen von Maschinen über CSV-Dateien

> **Hinweis:**
>
> - Den Namen von Nicht-Active Directory-Benutzern müssen Sie in diesem Format eingeben: `<identity provider>:<user name>`. Beispiel: `AzureAD:username`.
> - Bei den VM-Namen wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie beim Eingeben von VM-Pfaden die VM-Namen korrekt eingeben.

Bedenken Sie Folgendes beim Bearbeiten der CSV-Vorlagendatei:

- Das Feature bietet Ihnen mehr Flexibilität beim Massenhinzufügen von Maschinen mit einer CSV-Datei. In der Datei können Sie entweder nur Maschinen hinzufügen (zur Verwendung mit automatischen Benutzerzuweisungen) oder Maschinen und Benutzerzuweisungen gemeinsam hinzufügen. Geben Sie Ihre Daten in folgendem Format ein:
  - Paare aus Maschinenkonto und Benutzername (samName):
    - Domain\ComputerName1, Domain\Username1
    - Domain\ComputerName2, Domain\Username1;Domain\Username2
    - Domain\ComputerName3, AzureAD:username
  - Nur Maschinenkonten:
    - Domain\ComputerName1
    - Domain\ComputerName2

  - Paare aus VM und Benutzernamen:
    * XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    * XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer
  - Nur VMs:
    * XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    * XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer

    Beispiel:
    `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    Hierbei gilt:
    * `xpace-scale` ist der ConnectionName: Der Name der Verbindung, die Sie unter **Vollständige Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen** eingegeben haben. Weitere Informationen finden Sie unter Erstellen einer Verbindung und von Ressourcen.
    * `East US.region` ist der RegionName: Der Name der Region mit `.region` als Erweiterung.
    * `wsvdaV3-2.vm` ist der VMName: Der Name der virtuellen Maschine mit `.vm` als Erweiterung.

- Eine Datei kann maximal 1000 Maschinen enthalten. Um mehr als 1000 Maschinen zu importieren, verteilen Sie sie auf mehrere Dateien und importieren diese Dateien dann nacheinander. Wir empfehlen, nicht mehr als 1000 Maschinen zu importieren. Andernfalls kann die Katalogerstellung sehr lange dauern.

Sie können Maschinen auch aus einem Katalog auf derselben Seite **Maschinen hinzufügen** exportieren. Die CSV-Datei mit exportierten Maschinen kann dann als Vorlage verwendet werden, wenn Maschinen in großen Mengen hinzugefügt werden. Gehen Sie zum Exportieren von Maschinen folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Maschinenkatalog und dann in der Aktionsleiste die Option **Maschinen hinzufügen**. Das Fenster **Maschine hinzufügen** wird angezeigt.
3. Wählen Sie **In CSV exportieren**. Eine CSV-Datei mit einer Liste der Maschinen wird heruntergeladen.
4. Öffnen Sie die CSV-Datei, um Maschinen nach Bedarf hinzuzufügen oder zu bearbeiten. Informationen zum Hinzufügen von Maschinen in großen Mengen mit der gespeicherten CSV-Datei finden Sie im vorherigen Abschnitt Verwenden von CSV-Dateien zum Massenhinzufügen von Maschinen zu einem Katalog.

> **Hinweis:**
>
> - Das Feature ist für Remote-PC-Zugriff-Kataloge und mit MCS bereitgestellte Kataloge nicht verfügbar.
> - Der Export und Import von Maschinen in CSV-Dateien wird nur zwischen Katalogen desselben Typs unterstützt.

### Registrieren Sie Maschinen mit dem WebSocket VDA-Registrierungstool für Kataloge

Das WebSocket VDA-Registrierungstool erleichtert die tokenbasierte Registrierung für VDA-Maschinen. Mit diesem Tool können Sie eine Verbindung in eine WebSocket-Verbindung konvertieren, indem Sie den VDA mit dem Registrierungstoken zum Maschinenkatalog hinzufügen.

> **Hinweis:**
>
> Dieses Tool dient zur Registrierung von VDA-Maschinen, die in keinem Maschinenkatalog registriert wurden.

Folgen Sie den Anweisungen, um das Registrierungstool auszuführen:

1. Melden Sie sich beim VDA an.
2. Suchen Sie das Tool `EnrollMachine.exe` in `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Führen Sie das Werkzeug mit den entsprechenden Eingabeparametern aus. Zum Beispiel: `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

In der folgenden Tabelle werden die Eingabeparameter des Registrierungstools beschrieben:

| Parametername | Erforderlich | Beschreibung | Beispiel |
|---|---|---|---|
| `-websocket_token_stdin` | Ja | Liest das Registrierungstoken. | `.\EnrollMachine.exe -websocket_token_stdin` |
| `-websocket_token_string` | | Liest das Registrierungstoken direkt aus dem Befehlszeilenparameter. | `.\EnrollMachine.exe -websocket_token_string:<token>` |

| Parametername | Erforderlich | Beschreibung | Beispiel |
|---|---|---|---|
| -websocket_token_file :[token-file-path] | | Liest das Registrierungstoken aus dem angegebenen Pfad. | .\EnrollMachine.exe -websocket_token_file :C:\token\test2.txt |
| log:[log-file-path] | Nein | Zeigt die Protokolle des Registrierungstools an. | .\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt] |
| -help | Nein | Zeigt einen kurzen Hilfetext an. | .\EnrollMachine.exe -help |

Nach erfolgreicher Registrierung erhalten Sie eine Erfolgsmeldung im Tool und in den Protokollen. Achten Sie darauf, sich bei der vollständigen Konfiguration anzumelden, um sicherzustellen, dass die VDA-Maschine zum Katalog hinzugefügt wurde und der Status der Maschine registriert ist.

**Problembehandlung** Standardmäßig finden Sie die Protokolle des Registrierungstools unter:

C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt

Wenn Sie einen anderen Pfad für die Protokolle angegeben haben, können Sie log:[log-file-path] zum Abrufen Ihrer Protokolle verwenden.

In der folgenden Tabelle sind die vom Registrierungstool zurückgegebenen Codes aufgeführt:

| Code | Zeichenfolge | Beschreibung |
|---|---|---|
| 0 | Erfolg | Der VDA wurde erfolgreich zum Maschinenkatalog hinzugefügt. |
| -1 | InvalidArgument | Der Eingabeparameter im Registrierungstoken ist ungültig. |
| -2 | BrokerAgentNotFound | Der Broker-Agent-Service wurde nicht gefunden. |

| Code | Zeichenfolge | Beschreibung |
|---|---|---|
| -3 | TokenInvalid | Das eingegebene Token ist ungültig. |
| -4 | TokenMissingRequiredClaims | Die erforderlichen Ansprüche für das Token fehlen, z. B. CustomerId oder Enrollment URIs. |
| -5 | InternalError | Ein allgemeiner Fehler ist aufgetreten. |
| -6 | TimedOut | Für die Aufgabe ist ein Timeout aufgetreten. |
| -7 | FailedToDetermineMachineADJoinedStatus | Der Dienst, der den Status “AD Joined”des Computers zurückgibt, ist fehlgeschlagen. |
| -8 | ADMachineFailedToFindSid | Der Dienst, der die AD-Computer-Sid zurückgibt, ist fehlgeschlagen. |
| -9 | EnrollRequestFailed | Die Anfrage ist aufgrund eines HTTP-Fehlers fehlgeschlagen. |
| -10 | EnrollResponseMissingRequiredFields | In der Antwort des Registrierungstools fehlt der Parameter `VirtualSiteId`. |
| -11 | InsufficientPermission | Sie haben nicht die erforderliche Berechtigung, um die Aufgabe auszuführen. |
| -12 | FailedToDetermineMachineAadJoinedStatus | Der Dienst, der den AD-Join-Status des Computers überprüft, gibt einen Fehler aus. |
| -13 | AadMachineFailedToFindDeviceId | Der zusätzliche Parameter `AAD device id`, der vom System hinzugefügt wurde, ist leer. |
| -14 | AadDeviceIdNotValid | Der zusätzliche Parameter `AAD device id`, der vom System hinzugefügt wurde, ist keine gültige GUID. |
| -15 | NoValidMacAddress | Ungültige MAC-Adresse. |

| Code | Zeichenfolge | Beschreibung |
| --- | --- | --- |
| -16 | FailedToGetComputerHostNameFordVdaInstanceName | Der Hostname des Computers konnte nicht abgerufen werden, um den zusätzlichen Parameter `VdaInstanceName` festzulegen. |
| -17 | VirtualDesktopAgentRegistryKeyFailedToOpen | Der VDA-Registrierungsschlüssel konnte nicht geöffnet werden, um die Liste der Delivery Controller zu schreiben. |
| -18 | Das fehlgeschlagene Token hat die maximale Anzahl erreicht | Das fehlgeschlagene Token hat die maximale Anzahl erreicht. |

### Löschen von Maschinen aus einem Maschinenkatalog

Wenn Sie eine Maschine aus einem Maschinenkatalog löschen, können Benutzer nicht mehr darauf zugreifen. Vergewissern Sie sich vor dem Löschen daher, dass folgende Bedingungen erfüllt sind:

- Die Benutzerdaten wurden gesichert oder werden nicht mehr benötigt.
- Alle Benutzer sind abgemeldet. Durch das Aktivieren des Wartungsmodus wird verhindert, dass neue Verbindungen mit einer Maschine hergestellt werden.
- Die Maschinen sind ausgeschaltet.

Löschen von Maschinen aus einem Maschinenkatalog

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Wählen Sie eine oder mehrere Maschinen und dann in der Aktionsleiste **Löschen**.
4. Wenn Sie persistente Maschinen aus dem Katalog löschen, wählen Sie aus, ob diese auch aus dem Hypervisor oder dem Clouddienst gelöscht werden sollen. Sollen sie gelöscht werden, geben Sie an, ob die zugehörigen Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen.

Wenn Sie persistente Maschinen aus einem Azure Resource Manager-Katalog löschen, werden die zugeordneten Maschinen und zugehörigen Ressourcengruppen aus Azure gelöscht, selbst wenn Sie angeben, dass sie beibehalten werden sollen.

Wenn Sie nicht persistente Maschinen aus einem Katalog löschen, werden diese automatisch aus dem Hypervisor oder Clouddienst gelöscht.

### Bearbeiten eines Katalogs

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinenkatalog bearbeiten**.
3. Ändern Sie die Bereiche auf der Seite **Geltungsbereiche**.
4. Führen Sie auf der Seite **Netzwerkkarte** die folgenden Aktionen aus:

   - Um die Subnetzzuordnung einer Netzwerkkarte zu ändern, wählen Sie im Feld **Zugeordnetes Netzwerk** ein Netzwerk aus.
   - Um eine Subnetzzuordnung hinzuzufügen, wählen Sie **Netzwerkkarte hinzufügen** und dann im Feld **Zugeordnetes Netzwerk** ein Netzwerk aus. Klicken Sie auf **Speichern**.

   Im Feld **Zugeordnetes Netzwerk** werden nur die Subnetze angezeigt, die auf dem mit dem Katalog verknüpften Host vorhanden sind.

   Sie können eine Netzwerkkarte nur zu Azure-Maschinenkatalogen ohne Maschinenprofile hinzufügen.

   > **Hinweis:**
   >
   > - Bei AWS-Maschinenkatalogen können Sie dasselbe Subnetz nicht mehreren Netzwerkkarten zuordnen.
   > - Bei Maschinenkatalogen mit Maschinenprofilen muss die Anzahl der Netzwerkkarten im Katalog der Anzahl der Netzwerkkarten im Maschinenprofil entsprechen.
   > - Dieses Feature wird für IBM Cloud-Hypervisors nicht unterstützt.
   > - Dieses Feature wird nur für Nutanix Prism Element im Fall von Nutanix-Hypervisors unterstützt.

5. Ändern Sie auf der Seite **VDA-Upgrade** die zu aktualisierende VDA-Version, oder wählen Sie sie aus. Weitere Informationen finden Sie unter VDA-Upgrade.
6. Je nach Katalogtyp werden möglicherweise zusätzliche Seiten angezeigt.

   Für Kataloge, die mit einem Azure Resource Manager-Image erstellt wurden, werden die folgenden Seiten angezeigt. Denken Sie daran, dass vorgenommene Änderungen nur für Maschinen gelten, die Sie später zum Katalog hinzufügen. Bestehende Maschinen bleiben unverändert.

   - Ändern Sie auf der Seite **Virtuelle Maschinen** die Maschinengröße und wählen Sie Verfügbarkeitszonen aus, in denen Sie Maschinen erstellen möchten.

> **Hinweis:**
>
> – Es werden nur Maschinengrößen angezeigt, die vom Katalog unterstützt werden.
> – Wählen Sie gegebenenfalls **Nur in anderen Maschinenkatalogen verwendete Maschinengrößen anzeigen**, um die Liste der Maschinengrößen zu filtern.

- Wählen Sie auf der Seite **Maschinenprofil**, ob Sie ein Maschinenprofil verwenden oder ändern möchten.
- (Nur wenn der Katalog mit einer dedizierten Hostgruppen konfiguriert ist) Wählen Sie auf der Seite **Dedizierte Hostgruppe** aus, ob eine Hostgruppe geändert werden soll.
- Wählen Sie auf der Seite **Speicher- und Lizenztypen** aus, ob der Speichertyp, der Lizenztyp und die Azure Compute Gallery-Einstellungen geändert werden sollen (nur verfügbar, wenn **Vorbereitetes Image in der Azure Compute Gallery platzieren** verwendet wird).

  > **Hinweis:**
  >
  > Wenn die neue Einstellung die aktuelle Maschinengröße nicht unterstützt, wird eine Warnung angezeigt, dass durch eine Änderung der Einstellung die Maschinengröße zurückgesetzt wird. Wenn Sie fortfahren möchten, erscheint neben dem Menü **Virtuelle Maschinen** ein roter Punkt, durch den Sie aufgefordert werden, eine neue Maschinengröße auszuwählen.

Weitere Informationen zu den auf den Seiten verfügbaren Einstellungen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Images.

Für Remote-PC-Zugriff-Kataloge werden die folgenden Seiten angezeigt:

- Auf der Seite **Energieverwaltung** ändern Sie die Energieverwaltungseinstellungen und wählen eine Energieverwaltungsverbindung aus.
- Verwenden Sie die Seite **Organisationseinheiten** zum Hinzufügen und Entfernen von Active Directory-Organisationseinheiten.

7. Ändern Sie auf der Seite **Beschreibung** die Beschreibung des Maschinenkatalogs.
8. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu übernehmen, und klicken Sie dann auf **Speichern**.

### Umbenennen von Maschinenkatalogen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinenkatalog umbenennen**.
3. Geben Sie den neuen Namen ein.

### Löschen eines Katalogs

Vor dem Löschen eines Katalogs müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind abgemeldet und es werden keine getrennten Sitzungen ausgeführt.
- Der Wartungsmodus ist für alle Maschinen in dem Katalog aktiviert, damit keine neuen Verbindungen hergestellt werden können.
- Alle Maschinen in dem Katalog sind ausgeschaltet.
- Der Katalog ist keiner Bereitstellungsgruppe zugeordnet. Das heißt, keine Bereitstellungsgruppe enthält Maschinen aus dem Katalog.

Löschen eines Maschinenkatalogs

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinenkatalog löschen**.
3. Enthält der Katalog persistente Maschinen, geben Sie an, ob diese Maschinen auch aus dem Hypervisor oder dem Clouddienst gelöscht werden sollen. Sollen sie gelöscht werden, geben Sie an, ob die zugehörigen Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen.
4. Wählen Sie bei Bedarf **Fortschritt ausblenden** aus, um den Löschvorgang im Hintergrund auszuführen.

> **Hinweis:**
>
> - Wenn Sie einen Azure Resource Manager-Katalog löschen, werden die zugeordneten Maschinen und Ressourcengruppen aus Azure gelöscht, selbst wenn Sie angeben, dass sie beibehalten werden sollen.
> - Wenn Sie einen Katalog mit nicht persistenten Maschinen löschen, werden diese Maschinen aus dem Hypervisor oder Clouddienst gelöscht.
> - Wenn der Hypervisor oder der Cloudservice beim Löschen des Katalogs nicht erreichbar ist, können weder der Katalog noch die VM gelöscht werden. Bei Bedarf können Sie festlegen, dass die VM-Einträge nur aus der Datenbank Ihrer Citrix-Site gelöscht werden. Wählen Sie dazu den Maschinenkatalog im Knoten **Maschinenkataloge** aus und führen Sie dann den auf der Registerkarte **Problembehandlung** angezeigten Löschvorgang durch. Beachten Sie, dass bei dieser Aktion die VMs auf dem Host intakt bleiben.

### Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog

Zum Verwalten von Active Directory-Konten in einem Maschinenkatalog haben Sie folgende Möglichkeiten:

- Freigeben nicht verwendeter Maschinenkonten durch Entfernen von Active Directory-Computerkonten aus Einzelsitzungs- und Multisitzungs-Katalogen. Diese Konten können dann für andere Maschinen verwendet werden.
- Hinzufügen von Konten, damit beim Hinzufügen weiterer Maschinen zum Katalog Computerkonten bereit stehen. Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten.

Verwalten von Active Directory-Konten

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Maschinenkatalog und dann in der Aktionsleiste **Active Directory-Konten verwalten**.
3. Entscheiden Sie, ob Sie Computerkonten hinzufügen oder löschen möchten. Wenn Sie Konten hinzufügen, geben Sie an, wie mit den Kennwörtern verfahren werden soll: Setzen Sie entweder alle zurück oder geben Sie ein für alle Konten geltendes Kennwort ein.

   Sie können die Kennwörter zurückzusetzen, wenn Sie die aktuellen Kennwörter nicht kennen. Zum Zurücksetzen von Kennwörtern müssen Sie die entsprechende Berechtigung haben. Wenn Sie ein Kennwort eingeben, wird das Kennwort von Konten beim Importieren geändert. Wenn Sie ein Konto löschen, legen Sie fest, ob das Konto in einem Active Directory beibehalten, deaktiviert oder gelöscht werden soll.

Sie können auch angeben, ob Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen, wenn Sie Maschinen aus einem Katalog entfernen oder einen Katalog löschen.

### Masterimage für einen Katalog ändern

Wir empfehlen, Kopien oder Snapshots von Images zu speichern, bevor Sie das Masterimage für einen Katalog ändern. In der Datenbank wird von jedem Image eines Maschinenkatalogs ein historischer Datensatz beibehalten. Wenn das neu bereitgestellte Image zu Problemen auf den Benutzerdesktops führt, können Sie es die vorherige Version wiederherstellen und damit Ausfallzeiten für Benutzer minimieren. Images dürfen nicht gelöscht, verschoben oder umbenannt werden. Dies würde ein Rollback des Masterimages verhindern.

> **Wichtig:**
>
> Bedenken Sie beim Ändern des Masterimages für einen persistenten Katalog, dass das neue Image nur zum Erstellen später hinzugefügter Maschinen verwendet wird. Das neue Image wird nicht auf vorhandene Maschinen im Katalog angewendet.

Nachdem eine Maschine aktualisiert wurde, wird sie automatisch neu gestartet.

### Aktualisieren oder Erstellen eines Images

Bevor Sie das Masterimage für einen Katalog ändern, müssen Sie ein neues Image auf dem Host-Hypervisor vorbereiten, indem Sie ein vorhandenes Image aktualisieren oder ein neues Image erstellen.

1. Erstellen Sie auf dem Hypervisor bzw. im Clouddienst einen Snapshot der aktuellen VM und geben Sie diesem einen aussagekräftigen Namen. Mit diesem Snapshot kann ggf. ein Rollback für das Masterimage ausgeführt werden.
2. Falls erforderlich, schalten Sie das Image ein und melden Sie sich an.
3. Installieren Sie Updates bzw. nehmen Sie die erforderlichen Änderungen am Image vor.
4. Wenn das Image eine persönliche vDisk verwendet, aktualisieren Sie den Bestand.
5. Schalten Sie die virtuelle Maschine aus.
6. Erstellen Sie einen Snapshot der VM und geben Sie diesem einen aussagekräftigen Namen, den Sie beim Ändern des Masterimages erkennen.

> **Hinweis:**
>
> Sie können zwar mit der Verwaltungsoberfläche einen Snapshot erstellen, wir empfehlen jedoch, dass Sie einen Snapshot mit der Hypervisor-Verwaltungskonsole erstellen und ihn dann in der Verwaltungsoberfläche "Vollständige Konfiguration"auswählen. Dadurch können Sie statt eines automatisch erstellten Namens einen aussagekräftigen Namen und eine Beschreibung zuweisen. Bei GPU-Images können Sie das Image nur über die XenServer XenCenter-Konsole ändern.

### Masterimage ändern

Führen Sie folgende Schritte aus, um ein neues Masterimage auf alle Maschinen im Katalog anzuwenden:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Masterimage ändern**.
3. Wählen Sie auf der Seite **Image** den Host und das Masterimage aus, das Sie verwenden möchten.

   > **Tipp:**
   >
   > Für mit MCS erstellte Kataloge können Sie einen Hinweis zu dem Image angeben. Ein Hinweis kann bis zu 500 Zeichen enthalten. Bei jeder Änderung des Masterimages wird ein Hinweis-Eintrag erstellt, unabhängig davon, ob Sie einen Hinweis hinzufügen. Wenn Sie beim Aktualisieren eines Katalogs keinen Hinweis hinzuzufügen, wird der Eintrag als Null (-) angezeigt. Um den Hinweisverlauf für ein Image anzuzeigen, wählen Sie den Katalog,

> klicken Sie im unteren Bereich auf **Vorlageneigenschaften** und klicken Sie dann auf **Hinweisverlauf anzeigen**.

4. Legen Sie auf der Seite **Rolloutstrategie** fest, wann das neue Image auf die Maschinen im Maschinenkatalog anzuwenden ist: beim nächsten Herunterfahren oder sofort.

   > **Hinweis:**
   >
   > Die Seite **Rolloutstrategie** ist für persistente VMs nicht verfügbar, da das Rollout nur für nicht persistente VMs gilt.

5. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und wählen Sie **Fertig stellen**. Jede Maschine wird nach erfolgter Aktualisierung automatisch neu gestartet.

   Um den Fortschritt des Updates zu verfolgen, suchen Sie den Katalog in **Maschinenkatalogen**, um den Fortschrittsbalken und das Fortschrittsdiagramm anzuzeigen. Bei nicht persistenten Katalogen können Sie den Imageupdatestatus über die Spalte **Imageupdate** verfolgen (**Vollständig aktualisiert**, **Teilweise aktualisiert**, **Ausstehendes Update**) und **Image vorbereiten**.

   > **Tipp:**
   >
   > Zur Anzeige der Spalte **Imageupdate** wählen Sie **Anzuzeigende Spalten** in der Aktionsleiste, dann **Maschinenkatalog > Imagestatus** und klicken Sie auf **Speichern**.

Wenn Sie einen Katalog mit dem PowerShell-SDK aktualisieren, können Sie alternativ zu einem Image bzw. einem Imagesnapshot eine Hypervisorvorlage (`VMTemplates`) angeben.

#### Rolloutstrategie

Die Imageänderung beim nächsten Herunterfahren wirkt sich sofort auf alle Maschinen ohne aktive Benutzersitzung aus. In Verwendung befindliche Systeme erhalten das Update bei Beenden der aktiven Sitzung.

> **Hinweis:**
>
> Die Rolloutstrategie gilt nur für nicht persistente VMs.

Beachten Sie Folgendes:

- Neue Sitzungen können erst gestartet werden, wenn das Update auf einer Maschine abgeschlossen ist.
- Einzelsitzungsmaschinen werden, wenn sie nicht in Verwendung sind bzw. keine Benutzer angemeldet sind, sofort aktualisiert.
- Bei Multisitzungs-OS mit untergeordneten Maschinen werden keine automatischen Neustarts durchgeführt. Sie müssen manuell heruntergefahren und neu gestartet werden.

> **Tipp:**
>
> Zum Beschränken der Anzahl neu gestarteter Maschine können Sie die erweiterten Einstellungen für eine Hostverbindung verwenden. Über diese Einstellungen können Sie die für einen Katalog durchgeführten Aktionen ändern. Erweiterte Einstellungen variieren je nach Hypervisor.

#### Rollback für Masterimage ausführen

Nach Bereitstellung eines aktualisierten oder neuen Images können Sie diese mit einem Rollback rückgängig machen. Dies kann erforderlich sein, wenn Probleme bei den aktualisierten Maschinen auftreten. Bei einem Rollback werden die Maschinen in dem Katalog auf das letzte funktionierende Image zurückgesetzt. Was ist neu, die das neue Image erfordern, stehen dann nicht mehr zur Verfügung. Bei einem Rollback einer Maschine ist ein Neustart erforderlich.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie den Katalog und dann in der Aktionsleiste **Rollback für Masterimage ausführen**.
3. Legen Sie fest, wann das ältere Image auf die Maschinen angewendet werden soll (gemäß den Rollout-Anweisungen).

Das Rollback wird nur auf Maschinen angewendet, die zurückgesetzt werden müssen. Benutzer von Maschinen, die nicht auf das neue oder aktualisierte Image geändert wurden (z. B. weil sie sich nicht abgemeldet hatten), erhalten keine Meldung und müssen sich nicht abmelden.

Um den Rollback-Fortschritt zu verfolgen, suchen Sie den Katalog in **Maschinenkatalogen**, um den Fortschrittsbalken und das Fortschrittsdiagramm anzuzeigen.

In folgenden Szenarios ist kein Rollback möglich. (Die Option **Rollback für Masterimage ausführen** wird nicht angezeigt).

- Sie haben keine Berechtigung zum Rollback.
- Der Katalog wurde nicht mit MCS erstellt.
- Der Katalog wurde mit einem Image des Betriebssystemdatenträgers erstellt.
- Der zum Erstellen des Katalogs verwendete Snapshot ist beschädigt.
- Benutzeränderungen an den Maschinen in dem Katalog bleiben nicht erhalten.
- Maschinen im Katalog werden ausgeführt.

### Funktionsebene ändern oder Änderung rückgängig machen

Ändern Sie die Funktionsebene für den Maschinenkatalog nach dem Upgrade der VDAs auf den Maschinen auf eine neuere Version. Wir empfehlen das Upgrade aller VDAs auf die aktuelle Version, damit Zugriff auf alle neuen Features besteht.

Führen Sie folgende Schritte aus, bevor Sie die Funktionsebene für einen Maschinenkatalog ändern:

- Starten Sie die aktualisierten Maschinen, damit sie sich bei Citrix DaaS registrieren. Auf diese Weise kann die Verwaltungsoberfläche feststellen, dass die Maschinen im Maschinenkatalog aktualisiert werden müssen.

Ändern der Funktionsebene für einen Katalog:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie den Katalog aus. Auf der Registerkarte **Details** im unteren Bereich werden Versionsinformationen angezeigt.
3. Wählen Sie **Funktionsebene ändern**. Wenn die Funktionsebene des Katalogs geändert werden muss, wird von der Managementschnittstelle eine Meldung angezeigt. Folgen Sie den Anweisungen. Kann eine Maschine nicht geändert werden, wird eine Meldung mit einer Erläuterung des Problems angezeigt. Dadurch soll sichergestellt werden, dass alle Maschinen ordnungsgemäß funktionieren. Wir empfehlen Ihnen, diese Probleme zu lösen, bevor Sie auf **Ändern** klicken.

Nach Abschluss des Katalogupgrades können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie zunächst den Maschinenkatalog und dann in der Aktionsleiste **Änderung der Funktionsebene rückgängig machen** wählen.

### Klonen von Katalogen

Beim Klonen von Katalogen ist Folgendes zu berücksichtigen:

- Sie können die Einstellungen für Betriebssystem und Maschinenverwaltung nicht ändern. Der Klon erbt diese Einstellungen vom Original.
- Das Klonen eines Katalogs kann einige Zeit in Anspruch nehmen. Wählen Sie bei Bedarf **Fortschritt ausblenden** aus, um das Klonen im Hintergrund auszuführen.
- Der geklonte Katalog erhält den Namen des Originals und hat das Suffix `Copy`. Der Name kann geändert werden. Weitere Informationen finden Sie unter Umbenennen von Maschinenkatalogen.
- Weisen Sie den geklonten Katalog unbedingt einer Bereitstellungsgruppe zu.
- Sie können einen leeren Katalog durch Klonen erstellen. Beim Klonen von Katalogen können Sie die Anzahl der Maschinen für durch MCS (Maschinenerstellungsdienste) bereitgestellte Kataloge auf Null setzen und keine Maschinen für Kataloge hinzufügen, die nicht von MCS bereitgestellt wurden.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Klonen**.

3. Prüfen Sie im Fenster **Ausgewählten Maschinenkatalog klonen** die Einstellungen für den geklonten Katalog und bearbeiten Sie diese nach Bedarf. Wählen Sie **Weiter**, um mit der nächsten Seite fortzufahren.
4. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen und wählen Sie **Fertigstellen**, um das Klonen zu starten.
5. Wählen Sie bei Bedarf **Fortschritt ausblenden** aus, um das Klonen im Hintergrund auszuführen.

## Organisieren von Katalogen mit Ordnern

Sie können Ordner erstellen, um Kataloge für einfachen Zugriff zu organisieren. Sie können beispielsweise Kataloge nach Imagetyp oder Organisationsstruktur organisieren.

### Erforderliche Rollen

Standardmäßig benötigen Sie zum Erstellen und Verwalten von Katalogordnern die folgende integrierte Rolle: Cloudadministrator, Volladministrator oder Maschinenkatalogadministrator. Bei Bedarf können Sie Rollen für das Erstellen und Verwalten von Katalogordnern anpassen. Weitere Informationen finden Sie unter Erforderliche Berechtigungen.

### Erstellen von Katalogordnern

Planen Sie zunächst, wie Sie Ihre Kataloge organisieren wollen. Beachten Sie Folgendes:

- Sie können Ordner mit einer Tiefe von bis zu fünf Ebenen verschachteln (mit Ausnahme des Standardstammordners).
- Ein Katalogordner kann Kataloge und Unterordner enthalten.
- Alle Knoten in der **Vollständigen Konfiguration** (wie die Knoten **Maschinenkataloge** und **Anwendungen**) teilen sich eine Ordnerstruktur im Back-End. Um Namenskonflikte mit anderen Knoten beim Umbenennen oder Verschieben von Ordnern zu vermeiden, empfehlen wir, Ordnern der ersten Ebene in verschiedenen Knoten unterschiedliche Namen zu geben.

Gehen Sie wie folgt vor, um einen Katalogordner zu erstellen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und klicken Sie dann in der **Aktionsleiste** auf **Ordner erstellen**.
3. Geben Sie einen Namen für den neuen Ordner ein und klicken Sie dann auf **Fertig**.

> **Tipp:**
>
> Wenn Sie einen Ordner an einem falschen Speicherort erstellen, können Sie ihn an den korrekten Speicherort ziehen.

#### Verschieben von Katalogen

Sie können einen Katalog zwischen Ordnern verschieben. Verfahren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Zeigen Sie Kataloge nach Ordnern an. Sie können auch die Option **Alle anzeigen** über der Ordnerhierarchie aktivieren, um alle Kataloge gleichzeitig anzuzeigen.
3. Klicken Sie mit der rechten Maustaste auf einen Katalog und wählen Sie dann **Maschinenkatalog verschieben** aus.
4. Wählen Sie den Ordner aus, in den Sie den Katalog verschieben möchten, und klicken Sie dann auf **Fertig**.

> **Tipp:**
>
> Sie können einen Katalog in einen Ordner ziehen.

#### Verwalten von Katalogordnern

Sie können Katalogordner löschen, umbenennen und verschieben.

Sie können einen Ordner nur löschen, wenn er und seine Unterordner keine Kataloge enthalten.

Gehen Sie wie folgt vor, um einen Ordner zu verwalten:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und wählen Sie dann eine gewünschte Aktion in der **Aktionsleiste** aus:
   - Wählen Sie zum Umbenennen des Ordners **Ordner umbenennen** aus.
   - Wählen Sie zum Löschen des Ordners **Ordner löschen** aus.
   - Wählen Sie zum Verschieben des Ordners **Ordner verschieben** aus.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die restlichen Schritte auszuführen.

### Erforderliche Berechtigungen

In der folgenden Tabelle sind die Berechtigungen aufgeführt, die zum Ausführen von Aktionen für Katalogordner erforderlich sind.

| Aktion | Erforderliche Berechtigungen |
|---|---|
| Katalogordner erstellen | Maschinenkatalogordner erstellen |
| Katalogordner löschen | Maschinenkatalogordner entfernen |
| Katalogordner verschieben | Maschinenkatalogordner verschieben |
| Katalogordner umbenennen | Maschinenkatalogordner bearbeiten |
| Kataloge in Ordner verschieben | Maschinenkatalogordner bearbeiten und Maschinenkatalogeigenschaften bearbeiten |

## Automatische Upgrades für VDAs konfigurieren

> **Wichtig:**
>
> - Um ein reibungsloses Upgrade zu gewährleisten, stellen Sie sicher, dass die Voraussetzungen erfüllt sind, und prüfen Sie bekannte Probleme, bevor Sie VDAs auf CR- oder LTSR-CU-Versionen aktualisieren. Siehe Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration"
> - Achten Sie beim Upgrade von LTSR-VDAs auf LTSR Cumulative Update-Versionen darauf, dass die Version der auf den VDAs ausgeführten VDA Upgrade Agents 7.36.0.7 oder höher ist. Weitere Informationen finden Sie unter Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration".
> - Sie können zwischen CR VDA und LTSR VDA wechseln, sofern Sie von einer früheren Version zu einer späteren wechseln. Sie können nicht von einer späteren Version zu einer früheren Version wechseln, da dies als Downgrade betrachtet wird. Sie können beispielsweise nicht von 2212 CR auf 2203 LTSR (alle CUs) wechseln, ein Upgrade von 2112 CR auf 2203 LTSR (alle CUs) ist dagegen möglich.
> - Sie können VDAs auch mithilfe von PowerShell aktualisieren. Siehe VDAs mit PowerShell aktualisieren.

Das Feature ermöglicht folgende Aktionen:

- Upgrade von VDAs auf Katalogbasis
- Bearbeiten oder Abbrechen geplanter VDA-Upgrades
- Konfigurieren von VDA-Upgradeeinstellungen nach Katalogerstellung
- Upgrade von VDAs auf Maschinenbasis

> **Hinweis:**
>
> - Wenn Sie VDA-Upgrades für einen Katalog planen, können nur VDAs im Katalog aktualisiert werden, auf denen der VDA Upgrade Agent installiert ist.
> - Das VDA-Upgrade schlägt fehl, wenn sich die Maschine im Wartungsmodus befindet oder wenn eine Sitzung auf der Maschine ausgeführt wird.

#### Unterstützte Maschinentypen

Dieses Feature gilt für die folgenden Maschinentypen:

- Mit MCS bereitgestellte persistente Maschinen (In AD eingebunden, in Azure AD eingebunden und nicht domänengebunden). Sie stellen sie bei der Katalogerstellung mit **Citrix Maschinenerstellungsdiensten (MCS)** auf der Seite **Maschinenverwaltung** bereit.
- Maschinen mit Remote-PC-Zugriff
- Maschinen mit Citrix HDX Plus für Windows 365
- Andere persistente Maschinen, die mit nicht von Citrix stammenden Provisioningdiensten oder -technologien bereitgestellt wurden. Sie fügen diese Maschinen in DaaS hinzu, indem Sie bei der Katalogerstellung auf der Seite **Maschinenverwaltung** die Option **Anderer Dienst oder andere Technologie** verwenden.

Weitere Informationen zu den Optionen **Citrix Maschinenerstellungsdienste (MCS)** und **Anderer Dienst oder andere Technologie** finden Sie unter Maschinenverwaltung.

> **Hinweis:**
>
> Für mit MCS bereitgestellte Maschinen werden nur statische persistente Maschinen unterstützt. Zufällig ausgewählte Maschinen werden nicht unterstützt, auch wenn sie persistent sind.

#### Upgrade von VDAs auf Katalogbasis

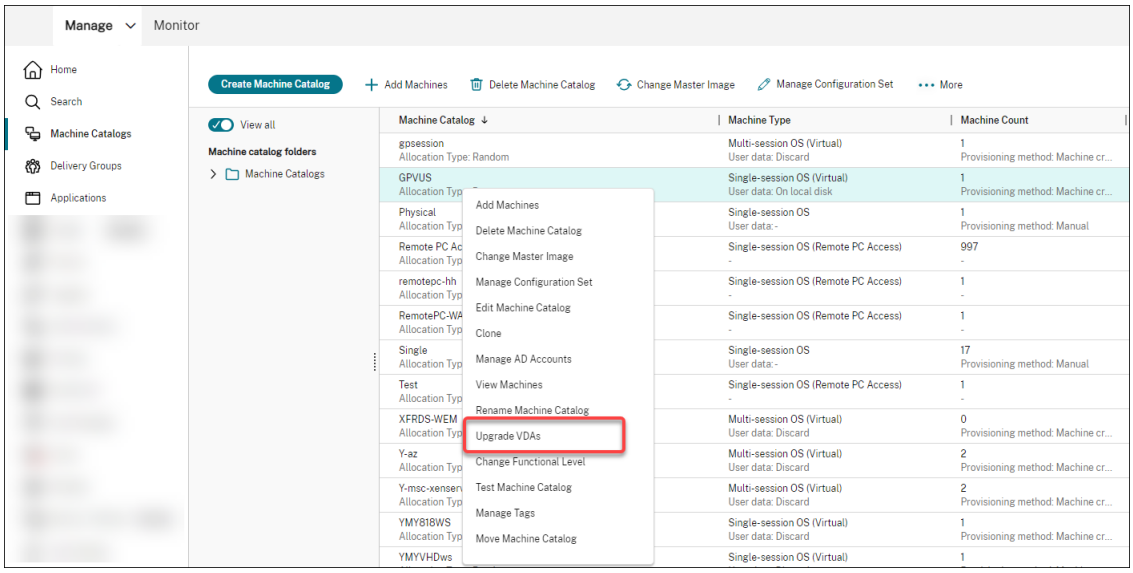
> **Hinweis:**
>
> Beachten Sie bei der Planung von VDA-Upgrades für einen Katalog, dass alle Maschinen im Katalog beim Upgrade berücksichtigt werden. Daher empfehlen wir, diese Maschinen zu sichern, bevor Sie das Upgrade starten.

Nachdem Sie ein VDA-Upgrade für einen Katalog aktiviert haben, können Sie VDAs im Katalog sofort aktualisieren oder Upgrades für den Katalog planen. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** aus.

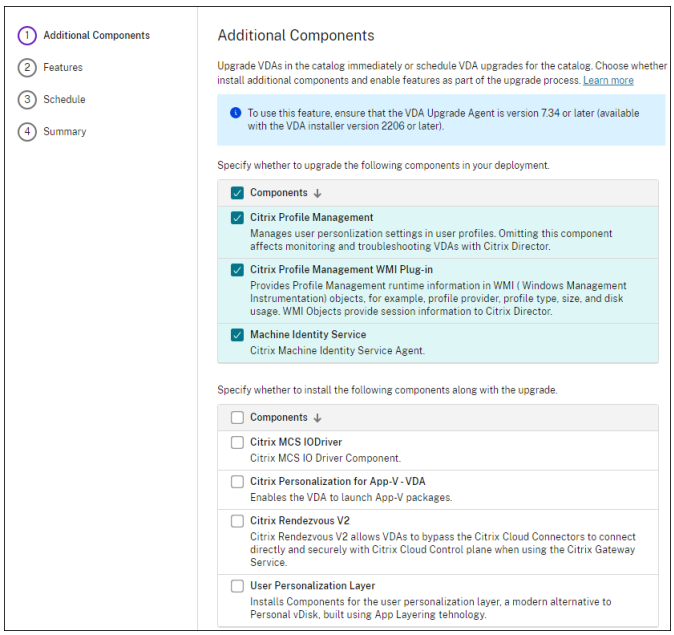
2. Wählen Sie den Katalog und dann in der Aktionsleiste oder im Kontextmenü **VDAs aktualisieren**. (Klicken Sie mit der rechten Maustaste, um das Kontextmenü anzuzeigen.) Das Fenster "VDA-Upgrade"wird angezeigt.




3. Wählen Sie, ob Sie zusätzliche Komponenten in Ihrer Bereitstellung aktualisieren möchten. Sie können auch bestimmte Komponenten zusätzlich zum Upgrade installieren. Wenn eine Komponente konfiguriert werden muss, müssen Sie auf die Schaltfläche **Konfigurieren** klicken und die Einstellungen der Komponente konfigurieren, um fortzufahren. Nach der Konfiguration können Sie auf **Bearbeiten** klicken, um die Konfiguration zu ändern.

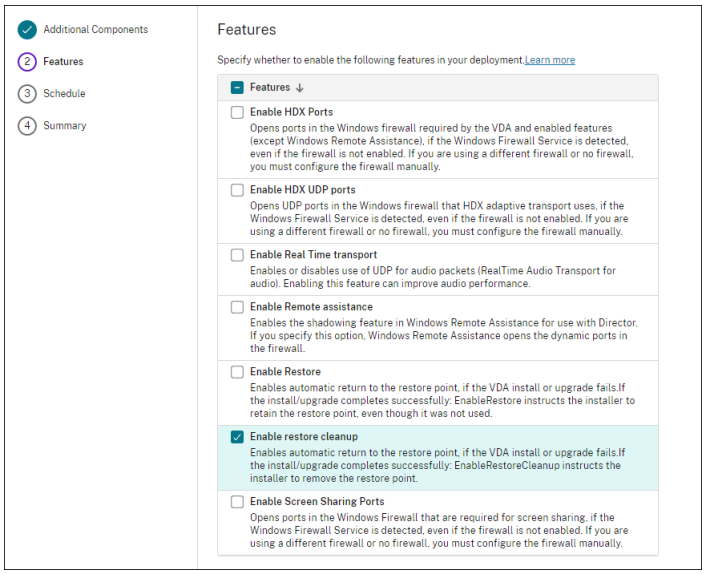
> **Wichtig:**
>
> - Um das Feature für zusätzliche Komponenten zu nutzen, müssen Sie den VDA-Upgrade-Agent Version 7.34 oder höher verwenden, der im VDA-Installationsprogramm Version 2206 oder höher enthalten ist.
>
> **Hinweis:**
>
> - Wenn Sie sich dafür entscheiden, eine Komponente nicht zu aktualisieren, bleibt die Komponente in Ihrer Bereitstellung intakt.
> - Eine Liste aller zusätzlichen Komponenten finden Sie unter VDAs installieren.




4. Klicken Sie auf **Weiter**.
5. Wählen Sie aus, ob Sie eines der aufgelisteten Features aktivieren möchten. Klicken Sie auf **Weiter**.

> **Hinweis:**
>
> Das Kontrollkästchen **Enable restore cleanup** ist standardmäßig aktiviert. Wir empfehlen, die Wiederherstellungsfunktion zu aktivieren. Bei aktiviertem Feature wird vor dem Upgrade ein Systemwiederherstellungspunkt erstellt. Der Wiederherstellungspunkt wird nach erfolgter VDA-Installation gelöscht. Weitere Informationen finden Sie unter Wiederherstellung bei Installations- oder Upgradefehler.



6. Wählen Sie aus, ob die VDAs sofort oder zu einem geplanten Zeitpunkt aktualisiert werden sollen.

   - Um die VDAs sofort zu aktualisieren, wählen Sie **Jetzt aktualisieren** und geben Sie dann eine Dauer an.

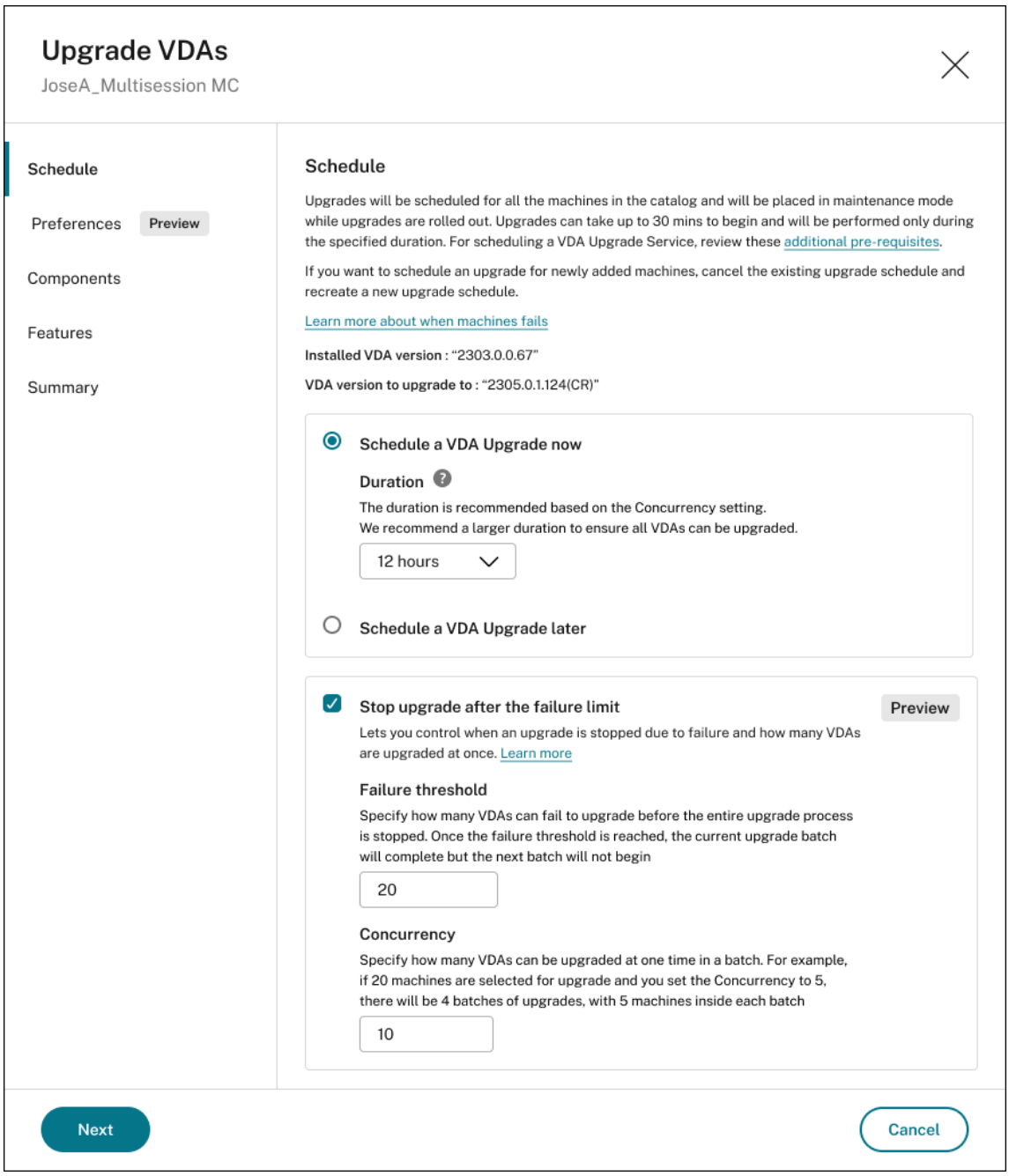
     Die Dauer gibt die Zeit in Stunden an, nach deren Ablauf der Beginn weiterer Upgrades beendet wird. Laufende Upgrades werden bis zum Abschluss ausgeführt. Während dieses Zeitraums beginnt DaaS mit dem Upgrade der VDAs, sobald sie in Frage kommen (z. B., wenn es keine aktiven Sitzungen mehr gibt).

     Je mehr VDAs aktualisiert werden müssen, desto länger ist diese Dauer. Wir empfehlen, einen hohen Wert auszuwählen (z. B. 12 Stunden). Andernfalls kann es je nach Anzahl der VDAs geben, die DaaS in diesem Fenster nicht aktualisieren kann.

   - Um die Upgrades zu planen, wählen Sie **Später aktualisieren** und geben Sie an, wann die Upgrades durchgeführt werden sollen.

     Sie können die Upgrades nur für die nächsten sieben Tage planen. Von Ihnen geplante Upgrades gelten nur für die Maschinen, die sich derzeit im Katalog befinden. Wenn Sie Maschinen zu einem späteren Zeitpunkt zum Katalog hinzufügen und diese auch aktualisieren möchten, brechen Sie das geplante Upgrade ab und erstellen Sie dann einen neuen Zeitplan.




7. Wählen Sie die Option **Upgrade nach dem Ausfalllimit beenden**.

> **Hinweis:**
>
> Das Feature ist standardmäßig deaktiviert, steht aber den Administratoren zur Verfügung.

**Darstellung des Verhaltens**

- Der Fehlerschwellenwert und die Gleichzeitigkeitsebene müssen größer als Null sein.
- Der Fehlerschwellenwert und die Gleichzeitigkeitsebene müssen kleiner oder gleich der

Gesamtzahl der Maschinen sein, für die ein Upgrade geplant ist

| Fehlerschwellenwert | Gleichzeitigkeitsebene | Ergebnis |
|---|---|---|
| Bereitgestellt | Nicht angegeben oder 0 eingegeben | FailureThreshold wird angewendet und ConcurrencyLevel wird wie zuvor vom Load Balancer entschieden. |
| Nicht angegeben oder 0 eingegeben | Bereitgestellt | FailureThreshold ist standardmäßig auf 10000 (Max Machines Per Catalog) voreingestellt und ConcurrencyLevel wird für die Batchverarbeitung verwendet. |
| Nicht angegeben oder 0 eingegeben | Nicht angegeben oder 0 eingegeben | Das Standardverhalten gilt für Gleichzeitigkeitsebenen, die vom Load Balancer aktualisiert werden. |

8. Geben Sie den **FailureThreshold** ein.

   > **Hinweis:**
   >
   > Der Fehlerschwellenwert ist die Anzahl der Fehler, nach denen das VUS alle ausstehenden Upgrade-Installationen von nachfolgenden Batches stoppt, die nicht vom Upgrade-Agent aufgenommen werden.

9. Geben Sie die **Gleichzeitigkeit** ein.

   > **Hinweis:**
   >
   > Gleichzeitiges Upgrade ist die Anzahl der VMs, die zu einem beliebigen Zeitpunkt innerhalb des Upgrade-Fensters gleichzeitig aktualisiert werden können.

10. Klicken Sie auf **Weiter**.
11. Überprüfen Sie Ihre Auswahl auf der **Übersichtsseite** und klicken Sie dann auf **Fertig stellen**, um Ihre Einstellungen anzuwenden und das Fenster zu schließen.

> **Hinweis:**
>
> - Die Option **VDAs aktualisieren** ist erst verfügbar, nachdem Sie das VDA-Upgrade für den Katalog aktiviert haben. Bearbeiten Sie den Katalog, um das VDA-Upgrade zu aktivieren.

> - Alle Maschinen im Katalog werden während der Durchführung von Upgrades in den Wartungsmodus versetzt. Es kann bis zu 30 Minuten dauern, bis die Upgrades beginnen und die Upgrades werden nur während des angegebenen Zeitraums durchgeführt.

Am Knoten **Maschinenkataloge** enthält die Spalte **VDA-Upgrade** VDA-Upgradeinformationen für den Katalog. Die folgenden Informationen können angezeigt werden:

> **Tipp:**
>
> Zur Anzeige der Spalte **VDA-Upgrade** wählen Sie **Anzuzeigende Spalten** in der Aktionsleiste, dann **Maschinenkatalog > VDA-Upgrade** und klicken Sie auf **Speichern**.

- **Verfügbar**: Eine neue VDA-Version ist verfügbar.
- **Geplant**: Das VDA-Upgrade wurde geplant.
- **Nicht konfiguriert**: Wird angezeigt, wenn Sie das VDA-Upgrade für den Katalog nicht aktiviert haben.
- **Aktuell**: Die VDAs des Katalogs sind auf dem neuesten Stand.
- **Unbekannt**: Die für das VDA-Upgrade erforderlichen Informationen können nicht abgerufen werden. Es gibt mehrere mögliche Gründe:
  - Der VDA wurde während des Upgradefensters verwendet.
  - Die Anzahl der laufenden Upgrades hat die Höchstgrenze von 500 erreicht.
  - Der VDA Upgrade Agent reagierte während des Upgradefensters nicht. Stellen Sie sicher, dass der Agent auf dem VDA läuft und mit Citrix DaaS kommunizieren kann.
  - Die Upgrade-Validierungsprüfungen können nicht durchgeführt werden. Weitere Informationen finden Sie unter Anforderungen für VDA-Upgrade.

Sie können auch den Status von VDA-Upgrades für einen Katalog anzeigen. Klicken Sie hierfür auf den Katalog und überprüfen Sie dann die Informationen unter **VDA-Upgradestatus** auf der Registerkarte **Details**. Die folgenden Informationen können angezeigt werden:

- **Nicht geplant:** Sie haben das VDA-Upgrade für den Katalog aktiviert, aber keinen Upgradezeitplan eingerichtet.
- **Geplant**: Sie haben einen Upgradezeitplan für den Katalog erstellt. Wenn Sie beispielsweise als Beginn des Zeitplans `09:00 PM, December 14, 2030` festgelegt haben, wird Folgendes angezeigt: Geplant für `December 14, 2030 09:00 PM UTC`.
- **Wird ausgeführt:** VDA-Upgrades wurden gestartet.
- **Abgebrochen**: Sie haben das geplante Upgrade abgebrochen.
- **Fehlgeschlagen:** Der Katalog enthält mindestens eine Maschine, deren VDA-Upgrade nicht erfolgreich war.
- **Erfolgreich:** Alle VDAs im Katalog wurden aktualisiert.

Sie können auch Probleme mit VDA-Upgrades behandeln und erhalten hierfür Empfehlungen für Maß-

nahmen. Klicken Sie hierfür auf den Katalog und wechseln Sie dann zur Registerkarte **Problembehandlung**.

Für einen schnellen Drilldown zu Katalogen mit einem spezifischen VDA-Upgradestatus können Sie Filter verwenden. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration".

Hinweis:

- Die Filter **VDA-Upgrade** und **VDA-Upgradestatus** stehen nur zur Verwendung mit den folgenden Filtern zur Verfügung: **Name** und **Maschinenkatalog**.
- Wenn Sie den Filter **VDA-Upgrade** oder **VDA-Upgradestatus** verwenden, sind die Filter **Fehler** und **Warnungen** oben rechts nicht verfügbar.

#### Bearbeiten oder Abbrechen geplanter VDA-Upgrades

Nachdem Sie Upgrades für einen Katalog geplant haben, können Sie geplante Upgrade bei Bedarf bearbeiten oder abbrechen. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** aus.
2. Wählen Sie den Katalog und dann in der Aktionsleiste **Geplantes VDA-Upgrade bearbeiten**. Das Fenster "VDA-Upgrade bearbeiten"wird angezeigt. Es enthält Informationen zur installierten VDA-Version und zur VDA-Version, auf die ein Upgrade durchgeführt werden soll.
3. Wählen Sie aus, ob Sie das geplante Upgrade bearbeiten oder abbrechen möchten.
    - Um das Upgrade abzubrechen, klicken Sie auf **Geplantes Upgrade abbrechen**. Hinweis: Wenn Sie ein geplantes Upgrade abbrechen, werden gerade laufende Upgrades nicht angehalten.
4. Klicken Sie auf **Fertig**, um das Fenster zu verlassen.

#### Konfigurieren von VDA-Upgradeeinstellungen durch Bearbeiten des Katalogs

Nach der Katalogerstellung können Sie die VDA-Upgradeeinstellungen konfigurieren, indem Sie den Katalog bearbeiten. Bevor Sie mit der Bearbeitung beginnen, sollten Sie Folgendes beachten:

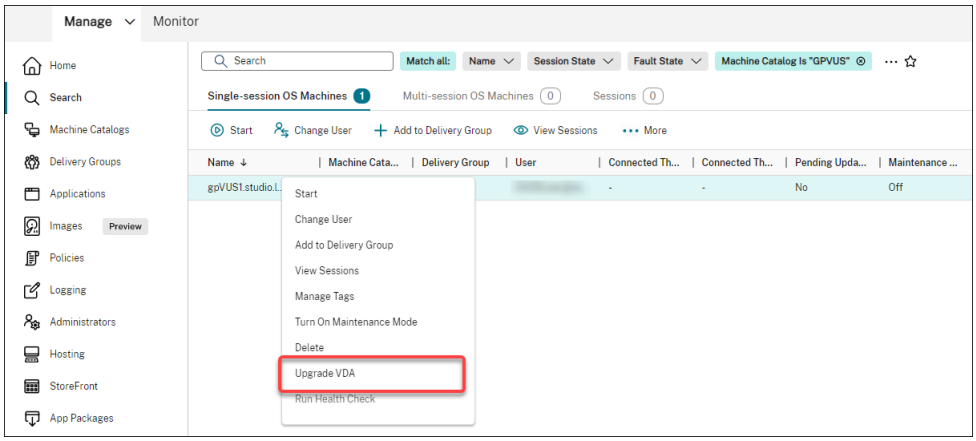
- Stellen Sie sicher, dass auf allen Maschinen im Katalog derselbe VDA-Track (CR oder LTSR) ausgeführt wird. Andernfalls schlagen bestimmte VDA-Upgrades fehl. Wenn Sie beispielsweise **Neuester LTSR VDA** auswählen, schlagen CR-VDA-Upgrades fehl.
- Upgrades einiger Maschinen im Katalog haben möglicherweise begonnen. Laufende Upgrades können nicht geändert werden. Die laufenden Upgrades werden fortgesetzt. Diejenigen, die noch nicht gestartet wurden, werden auf die angegebene Version aktualisiert.

### Upgrade von VDAs auf Maschinenbasis

Nachdem Sie das VDA-Upgrade für einen Katalog aktiviert haben, können Sie die VDAs einzeln oder gruppenweise aktualisieren. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Suchen** aus.
2. Wählen Sie eine oder mehrere Maschinen aus und klicken Sie dann im Kontextmenü oder auf der Aktionsleiste auf **VDA aktualisieren**. (Klicken Sie mit der rechten Maustaste, um das Kontextmenü anzuzeigen.)




> **Hinweis:**
>
> - Damit die Option **VDA-Upgrade** verfügbar ist, stellen Sie sicher, dass Sie das VDA-Upgrade für den Katalog mit den ausgewählten Maschinen aktiviert haben und dass auf diesen Maschinen der VDA Upgrade Agent installiert ist. Um das VDA-Upgrade für den Katalog zu aktivieren, bearbeiten Sie ihn.
> - Die Maschinen werden während der Durchführung von Upgrades in den Wartungsmodus versetzt. Es kann bis zu 30 Minuten dauern, bis die Upgrades beginnen.
> - Wenn Ihre Auswahl Maschinen enthält, für die keine VDA-Upgrades verfügbar sind oder deren Upgrades ausstehen (Status: Geplant, In Bearbeitung oder Erwartet Upgrade), dann überspringen wir Upgrades für diese Maschinen.

Am Knoten **Suchen** können Sie die Spalte **VDA-Upgrade** hinzufügen. Informationen zum Hinzufügen einer benutzerdefinierten Spalte finden Sie unter Anpassen der Spaltenanzeige. Die Spalte ist nützlich. Sie enthält VDA-Upgradeinformationen für die Maschine. Die folgenden Informationen können angezeigt werden:

- **Verfügbar**: Eine neue VDA-Version ist verfügbar.
- **Geplant**: Das VDA-Upgrade wurde geplant.
- **Nicht konfiguriert**: Wird angezeigt, wenn Sie das VDA-Upgrade für die Maschine nicht aktiviert haben.

- **Aktuell**: Der VDA ist auf dem neuesten Stand.
- **Unbekannt**: Informationen zum VDA-Upgrade sind noch nicht verfügbar.

Sie können auch den Status des VDA-Upgrades für eine Maschine anzeigen. Klicken Sie hierfür auf die Maschine und überprüfen Sie dann die Informationen unter **VDA-Upgradestatus** auf der Registerkarte **Details**. Die folgenden Informationen können angezeigt werden:

- **Unbekannt**: Die für das VDA-Upgrade erforderlichen Informationen können nicht abgerufen werden. Es gibt mehrere mögliche Gründe:
  - Der VDA wurde während des Upgradefensters verwendet.
  - Die Anzahl der laufenden Upgrades hat die Höchstgrenze von 500 erreicht.
  - Der VDA Upgrade Agent reagierte während des Upgradefensters nicht. Stellen Sie sicher, dass der Agent auf dem VDA läuft und mit Citrix DaaS kommunizieren kann.
  - Die Upgrade-Validierungsprüfungen können nicht durchgeführt werden. Weitere Informationen finden Sie unter Anforderungen für VDA-Upgrade.
- **Geplant**: Sie haben einen Upgradezeitplan eingerichtet. Wenn Sie beispielsweise als Beginn des Zeitplans `09:00 PM, December 14, 2030` festgelegt haben, wird Folgendes angezeigt: Geplant für `December 14, 2030 09:00 PM UTC`.
- **Erwartet Upgrade:** Die Maschine ist im Wartungsmodus und wartet auf das Upgrade. (Stellen Sie sicher, dass die Benutzer sich von ihren Sitzungen abgemeldet haben, damit das Upgrade stattfinden kann.)
- **Wird ausgeführt:** Das VDA-Upgrade hat begonnen.
- **Upgrade fehlgeschlagen**: Das VDA-Upgrade ist fehlgeschlagen.
- **Validierung fehlgeschlagen:** Validierungsversuche der VDA-Upgradeeinstellungen sind fehlgeschlagen.
- **Abgebrochen:** Das Upgrade für die Maschine wurde abgebrochen.
- **Erfolgreich**: Der VDA wurde aktualisiert.

Sie können auch Probleme mit VDA-Upgrades behandeln und erhalten hierfür Empfehlungen für Maßnahmen. Klicken Sie hierfür auf die Maschine und wechseln Sie dann zur Registerkarte **Problembehandlung**.

Für einen schnellen Drilldown zu Maschinen mit einem spezifischen VDA-Upgradestatus können Sie Filter verwenden. Weitere Informationen finden Sie unter Verwenden der Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration". Hinweis:

- Die Filter **VDA-Upgrade** und **VDA-Upgradestatus** stehen nur zur Verwendung mit den folgenden Filtern zur Verfügung: **Name** und **Maschinenkatalog**.
- Wenn Sie den Filter **VDA-Upgrade** oder **VDA-Upgradestatus** verwenden, sind die Filter **Fehler** und **Warnungen** oben rechts nicht verfügbar.

## Verwalten eines Konfigurationssatzes für einen Katalog

Stellen Sie zunächst sicher, dass Sie Ihre WEM-Dienstbereitstellung eingerichtet haben. Weitere Informationen finden Sie unter Erste Schritte mit dem Workspace Environment Management Service.

> **Hinweis:**
>
> Wenn Sie die Rolle Cloud-Administrator, Administrator mit Vollzugriff oder Maschinenkatalogadministrator haben, können Sie standardmäßig Konfigurationssätze für Kataloge verwalten. Falls erforderlich, können Sie Rollen zur Verwaltung von Konfigurationssätzen berechtigen, indem Sie ihnen die Berechtigung **Konfigurationssätze verwalten** gewähren.

### Binden eines Katalogs an einen Konfigurationssatz

> **Wichtig:**
>
> Wenn sich Ihre Citrix DaaS- und WEM Service-Instanzen nicht in derselben Region befinden, können Sie einen Katalog nicht an einen Konfigurationssatz binden. Migrieren Sie in diesem Fall den WEM Service in dieselbe Region wie Citrix DaaS.

Gehen Sie folgendermaßen vor, um einen Katalog an einen Konfigurationssatz zu binden:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** aus.
2. Wählen Sie den Maschinenkatalog und dann **Konfigurationssatz verwalten** in der Aktionsleiste aus. Das Fenster **Konfigurationssatz verwalten** wird angezeigt.
3. Wählen Sie einen WEM-Konfigurationssatz aus, an den der Katalog gebunden werden soll.

   > **Hinweis:**
   >
   > Wenn der ausgewählte Konfigurationssatz keine mit der Grundkonfiguration von WEM verbundenen Einstellungen enthält, wird die Option **Grundeinstellungen auf Konfigurationssatz anwenden** angezeigt. Wir empfehlen Ihnen, die Option zu wählen, um Grundeinstellungen auf den Konfigurationssatz anzuwenden.

4. Klicken Sie auf **Speichern**, um die Änderung zu speichern.

### Wechseln zu einem anderen Konfigurationssatz

Gehen Sie folgendermaßen vor, um zu einem anderen Konfigurationssatz für einen Katalog zu wechseln:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** aus.
2. Wählen Sie den Maschinenkatalog und dann **Konfigurationssatz verwalten** in der Aktionsleiste aus. Das Fenster **Konfigurationssatz verwalten** wird angezeigt.
3. Wählen Sie einen anderen WEM-Konfigurationssatz aus, an den der Katalog gebunden werden soll.
4. Klicken Sie auf **Speichern**, um die Änderung zu speichern.

#### Aufheben der Bindung eines Katalogs an den Konfigurationssatz

Gehen Sie folgendermaßen vor, um die Bindung eines Katalogs an den Konfigurationssatz aufzuheben:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** aus.
2. Wählen Sie den Maschinenkatalog und dann **Konfigurationssatz verwalten** in der Aktionsleiste aus. Das Fenster **Konfigurationssatz verwalten** wird angezeigt.
3. Klicken Sie auf das X-Symbol auf der rechten Seite des ausgewählten Konfigurationssatzes.
4. Klicken Sie auf **Speichern**, um die Änderung zu speichern.

### Katalogerstellung erneut versuchen

> **Hinweis:**
>
> Dieses Feature gilt nur für MCS-Kataloge.

Fehlerhafte Kataloge sind mit einem Fehlersymbol gekennzeichnet. Zum Anzeigen von Details gehen Sie zur Registerkarte **Problembehandlung** des jeweiligen Katalogs. Beim Neuversuch der Erstellung Klonen von Katalogen ist Folgendes zu berücksichtigen:

- Prüfen Sie zuerst die Informationen zur Problembehandlung und beheben Sie die Probleme. Die Informationen beschreiben die Probleme und enthalten Empfehlungen zu deren Behebung.
- Sie können die Einstellungen für Betriebssystem und Maschinenverwaltung nicht ändern. Der Katalog erbt diese Einstellungen vom Original.
- Es kann einige Zeit dauern, bis die Erstellung abgeschlossen ist. Wählen Sie bei Bedarf **Fortschritt ausblenden** aus, um die Erstellung im Hintergrund auszuführen.

Gehen Sie wie folgt vor, um erneut zu versuchen, einen Katalog zu erstellen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie den Katalog aus und gehen Sie zur Registerkarte **Problembehandlung**.

3. Klicken Sie auf den Hyperlink "Wiederholen", um erneut zu versuchen, den Katalog zu erstellen.
4. Ändern Sie im daraufhin angezeigten Assistenten die Einstellungen bei Bedarf. Wenn Sie keine Änderungen vornehmen müssen, können Sie direkt zur **Übersichtsseite** wechseln.
5. Wenn Sie fertig sind, wählen Sie **Fertig stellen**, um mit der Erstellung zu beginnen.

### (Nur nicht von Citrix bereitgestellte VDAs) Registrierungstoken generieren und verwalten

Nachdem Sie sich entschieden haben, die tokenbasierte Registrierung für Maschinen zu aktivieren, die nicht von Citrix bereitgestellt werden, müssen Sie zunächst Token pro Maschinenkatalog generieren und sie dann für VDA-Installationsadministratoren freigeben.

Ein Registrierungstoken bietet:

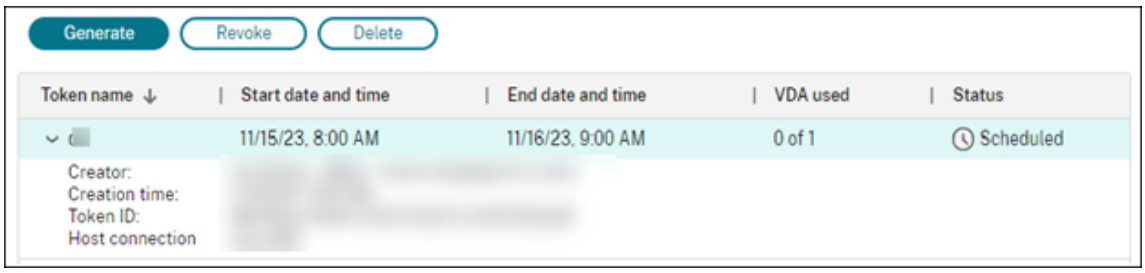
- Registrierungsbereich: 1 bis 100 VDA-Maschinen
- Gültigkeitsdauer: 1 Stunde bis 14 Tage

Gehen Sie folgendermaßen vor, um mithilfe der vollständigen Konfiguration ein Token für einen Katalog zu generieren:

1. Suchen Sie unter **Vollständige Konfiguration > Maschinenkataloge** nach einem nicht von MCS bereitgestellten Katalog, für den in der Spalte **Maschinenanzahl** die Option **Provisioningmethode: Manuell** angezeigt wird.
2. Klicken Sie mit der rechten Maustaste auf den Katalog und wählen Sie dann **Registrierungstoken verwalten** aus.
3. Geben Sie auf der Seite **Registrierungstoken generieren**, die daraufhin angezeigt wird, die folgenden Tokeninformationen ein:
    - Geben Sie einen Namen für das Token ein.
    - Geben Sie den Gültigkeitszeitraum ein. Der Zeitraum muss zwischen einer Stunde und 14 Tagen liegen. Das Token ist nur für den angegebenen Zeitraum gültig.
    - (Optional) Wählen Sie eine Hostverbindung für die Energieverwaltung von VDAs aus, die mit dem Token registriert sind. Zu den Optionen gehören alle Hostverbindungen in der Zone dieses Katalogs.
    - Geben Sie die Grenzwerte für die Tokennutzung ein (zwischen 1 und 100).
4. Klicken Sie auf **Generieren**.
5. Kopieren Sie im daraufhin angezeigten Fenster **Token erfolgreich generiert** das Token und speichern Sie es an einem sicheren Ort, oder klicken Sie auf **Herunterladen**, um es in den **Download**-Ordner herunterzuladen.

   Ein Tokendatensatz wird in der Tokenliste angezeigt.




6. Teilen Sie das Token mit den VDA-Installationsadministratoren.

   Weitere Informationen zur Installation von VDA und einem Token auf Maschinen finden Sie unter VDAs installieren.

#### Token verwalten

Sie haben zwei Möglichkeiten, ein Token zu widerrufen und es für die VDA-Registrierung nicht verfügbar zu machen:

- Widerrufen: Widerrufen Sie das Token, behalten Sie es jedoch zu Protokollierungszwecken in der Liste.
- Löschen: Widerrufen Sie das Token und löschen Sie es aus der Liste.

> **Hinweis:**
>
> Abgelaufene Token werden nach 14 Tagen automatisch gelöscht.

### PowerShell verwenden

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mit PowerShell verwalten:

- PowerShell verwenden, um den VDA-Upgradestatus und die VDA-Version zu überprüfen
- Sequenznummer des Maschinennamens verwalten
- Einmaligen Neustart planen
- Beschreibung zu einem Image hinzufügen
- Zurücksetzen des OS-Datenträgers
- Identitätsinformationen aktiver Computerkonten reparieren
- Netzwerkeinstellung für einen vorhandenen Maschinenkatalog ändern
- Versionen eines Maschinenkatalogs verwalten
- Cachekonfiguration eines vorhandenen Maschinenkatalogs ändern
- Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog in einer Azure-Umgebung konvertieren
- Mit einem Katalog verknüpfte Warnungen und Fehler abrufen
- Maschinen ohne Hypervisor-Zugriff löschen
- VDA-Aktualisierungsunterstützung über lokalen Dateifreigabezugriff

**PowerShell verwenden, um den VDA-Upgradestatus und die VDA-Version zu überprüfen**

Verwenden Sie den PowerShell-Befehl `Get-VusCatalog`, um den VDA-Upgradestatus zu überprüfen. Angenommen, der Katalogname ist `wuhanTestMC1`. An der Eingabeaufforderung können Sie Folgendes eingeben:

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`

```
PS C:\Users\hanw> Get-VusCatalog -Name  wuhanTestMC1


CancelledUpgrades            : 0
DurationInHours              : 8
FailedUpgrades               : 0
InProgressUpgrades           : 0
LastStateChangeInUtc         : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades        : 100
Name                         : wuhanTestMC1
ProvisioningType             : MCS
ScheduledTimeInUtc           : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades  : 0
SessionSupport               : SingleSession
StateId                      : UpgradeSuccessful
SuccessfulUpgrades           : 1
TotalMachines                : 1
Uid                          : 12
UpgradeState                 : UpgradeAvailable
UpgradeType                  : CR
UpgradeVersion               : 2112.0.0.32068
Uuid                         : 339e7bce-271b-4c37-9a1c-bce287008b65
```

In diesem Beispiel gilt für `UpgradeState` der Status `UpgradeAvailable`. Das bedeutet, dass VDA-Upgrade für den Katalog aktiviert ist. `StateId` ist `UpgradeSuccessful`. Das bedeutet, dass der Katalog erfolgreich auf 2112.0.0.32068 (`UpgradeVersion`) aktualisiert wurde.

Verwenden Sie den PowerShell-Befehl `Get-BrokerMachine`, um die aktuelle VDA-Version abzurufen.

```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

Verwenden Sie den PowerShell-Befehl `Get-VusAvailableVdaVersion`, um die neueste VDA-Version abzurufen.

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```

### Sequenznummer des Maschinennamens verwalten

Gehen Sie wie folgt vor, um die Sequenznummer von Maschinen, die mit MCS bereitgestellt werden, mit PowerShell-Befehlen anzupassen:

1. Öffnen Sie Powershell als Administrator auf dem Delivery Controller.
2. Führen Sie den Befehl `asnp citrix*` aus, um die Citrix-Module zu laden.
3. Führen Sie den folgenden Befehl aus, um die Startanzahl für den Identitätspool des Katalogs zu überprüfen:

   ```
   Get-AcctIdentityPool -IdentityPoolName xxx
   <!--NeedCopy-->
   ```

   `IdentityPoolName` ist der Name des Katalogs.
4. Wenn Sie diese Anzahl auf einen anderen Wert setzen möchten, führen Sie den folgenden Befehl aus und geben Sie StartCount als X an:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
   <!--NeedCopy-->
   ```
5. Fügen Sie die Maschinen zum Katalog hinzu, sodass die Maschinen mit der erforderlichen Anzahl erstellt werden.
6. Nachdem Sie die Maschinen erstellt haben, führen Sie den folgenden Befehl aus, um sie auf den ursprünglichen Wert Y zurückzusetzen:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
   <!--NeedCopy-->
   ```

### Einmaligen Neustart planen

Wenn Sie mit PowerShell einen einmaligen Neustart planen möchten, verwenden Sie die folgenden PowerShell-Befehle für `BrokerCatalogRebootSchedule`, um den Plan für einen Neustart zu erstellen, zu ändern und zu löschen:

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

Beispiel:

- Neustart der VMs im Katalog **BankTellers** planen, der am 3. Februar 2022 zwischen 2:00 Uhr und 4:00 Uhr beginnen soll.

```
New-BrokerCatalogRebootSchedule -Name BankTellers
-CatalogName BankTellers
-StartDate "2022-02-03"
-StartTime "02:00"
-Enabled $true
-RebootDuration 120
<!--NeedCopy-->
```

- Neustart der VMs im Katalog mit UID 17 planen, der am 3. Februar 2022 zwischen 1:00 Uhr und 5:00 Uhr beginnen soll. Zehn Minuten vor dem Neustart erscheint auf jeder VM in allen Benutzersitzungen ein Warnhinweis mit dem Titel **WARNUNG: Ausstehender Neustart** und der Nachricht **Speichern Sie Ihre Arbeit**.

```
New-BrokerCatalogRebootSchedule
-Name 'Update reboot'
-CatalogUid 17
-StartDate "2022-02-03"
-StartTime "01:00" -Enabled $true -RebootDuration 240
-WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
<!--NeedCopy-->
```

- Katalogneustartplan umbenennen von **Old Name** in **New Name**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
    Name"
<!--NeedCopy-->
```

- Alle Katalogneustartpläne mit UID 1 anzeigen und Zeitplan für den Katalogneustart mit UID 1 in **New Name** umbenennen.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Meldung mit dem Titel **WARNUNG: Ausstehender Neustart und der Nachricht Speichern Sie Ihre Arbeit** für Katalogneustartplan **Accounting** einrichten und festlegen, dass die Meldung zehn Minuten vor dem Neustart jeder VM angezeigt wird. Die Meldung wird in jeder Benutzersitzung auf dieser VM angezeigt.

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- Alle deaktivierten Neustartpläne anzeigen und anschließend aktivieren.

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
   BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Meldung **Neustart in %m% Minuten** für Katalogneustartplan mit UID 17 einrichten und festlegen, dass die Meldung fünfzehn, zehn und fünf Minuten vor dem Neustart jeder VM angezeigt wird.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
    %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- Zeitzone für den Katalog **MyCatalog** konfigurieren.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

### Beschreibung zu einem Image hinzufügen

Sie können Informationen zu Änderungen im Zusammenhang mit Image-Updates für Maschinenkataloge hinzufügen. Mit dem Feature können Sie beim Erstellen eines Katalogs oder beim Aktualisieren eines bestehenden Masterimages für einen Katalog eine Beschreibung hinzufügen. Sie können auch Informationen für jedes Masterimage im Katalog anzeigen. Das Feature ist nützlich für Administratoren, die Informationen (z. B. *Office 365 installiert*) hinzufügen möchten, wenn sie ein für einen Katalog verwendetes Masterimage aktualisieren. Verwenden Sie die folgenden Befehle, um Imagebeschreibungen hinzuzufügen oder anzuzeigen:

- `NewProvScheme`. Mit dem neuen Parameter `masterImageNote` können Sie einem Image eine Notiz hinzufügen. Beispiel:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
    XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
    XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`. Verwenden Sie diesen Parameter, um die Notiz zu veröffentlichen. Beispiel:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
    MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
    snapshot -MasterImageNote "Visual Studio 2019 installed"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`. Zeigt Informationen für jedes Image an. Beispiel:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5
```

```
4
5  ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42
6
7  ProvisioningSchemeName : MyScheme
8
9  MasterImageVM : /Base.vm/base.snapshot
10
11 Date : 17/05/2021 09:27:50
12
13 MasterImageNote : Office365 installed
14 <!--NeedCopy-->
```

### Zurücksetzen des OS-Datenträgers

Verwenden Sie den PowerShell-Befehl `Reset-ProvVMDisk`, um den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog zurückzusetzen. Derzeit ist dieses Feature auf Azure-, Google Cloud-, SCVMM-, VMware- und XenServer-Virtualisierungsumgebungen anwendbar.

Um den PowerShell-Befehl erfolgreich auszuführen, stellen Sie Folgendes sicher:

- Die Ziel-VMs befinden sich in einem persistenten MCS-Katalog.
- Der MCS-Maschinenkatalog funktioniert einwandfrei. Hierfür müssen das Provisioningschema und der Host vorhanden sein und das Provisioningschema über korrekte Einträge verfügen.
- Der Hypervisor ist nicht im Wartungsmodus.
- Die Ziel-VMs sind ausgeschaltet und im Wartungsmodus.

Führen Sie die folgenden Schritte aus, um den OS-Datenträger zurückzusetzen:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie asnp citrix* aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den PowerShell-Befehl `Reset-ProvVMDisk` auf eine der folgenden Arten aus:
   - Geben Sie die Liste der VMs als durch Trennzeichen getrennte Liste an und führen Sie das Zurücksetzen auf jeder VM durch:

     ```
     1  Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
            ,"def") -OS
     2  <!--NeedCopy-->
     ```

   - Geben Sie die Liste der VMs als Ausgabe des Befehls `Get-ProvVM` an und führen Sie das Zurücksetzen auf jeder VM durch:

     ```
     1  (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
            "abc" -OS
     2  <!--NeedCopy-->
     ```

- Geben Sie eine VM mit Namen an:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS
<!--NeedCopy-->
```

- Erstellen Sie einen eigenen Reset-Task für jede vom Befehl `Get-ProvVM` zurückgegebene VM. Dies ist weniger effizient, da jeder Task dieselben redundanten Prüfungen durchführt (z. B. Hypervisor-Funktionsprüfung und Verbindungsprüfung).

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. Eine Bestätigungsaufforderung wird angezeigt, in der die zurückzusetzenden VMs zusammen mit einer Warnmeldung aufgeführt sind, dass es sich um einen nicht umkehrbaren Vorgang handelt. Wenn Sie keine Antwort geben und die **Eingabetaste**drücken, findet keine weitere Aktion statt.

   Sie können den PowerShell-Befehl `-WhatIf` ausführen, um die auszuführende Aktion zu drucken und den Vorgang ohne Ausführen der Aktion zu beenden.

   Sie können die Bestätigungsaufforderung auch mit einer der folgenden Methoden umgehen:

   - Geben Sie den Parameter `-Force` an:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Force
<!--NeedCopy-->
```

   - Geben Sie den Parameter `-Confirm:$false` an:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
<!--NeedCopy-->
```

   - Ändern Sie `$ConfirmPreference` zu “None”, bevor Sie `Reset-ProvVMDisk` ausführen:

```
PS C:\Windows\system32> $ConfirmPreference='None'
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
<!--NeedCopy-->
```

> **Hinweis:**

> Nehmen Sie VMs erst nach Abschluss der Zurücksetzung aus dem Wartungsmodus und schalten Sie sie ein.

5. Führen Sie `Get-ProvTask` aus, um den Status der von Befehl `Reset-ProvVMDisk` zurückgegebenen Tasks abzurufen.

### Identitätsinformationen aktiver Computerkonten reparieren

Sie können die Identitätsinformationen von aktiven Computerkonten mit Identitätsproblemen zurücksetzen. Sie können wählen, ob Sie nur das Maschinenkennwort und die vertrauenswürdigen Schlüssel-IDs oder die gesamte Konfiguration des Identitätsdatenträgers zurücksetzen möchten. Diese Implementierung gilt für persistente und nicht persistente MCS-Maschinenkataloge.

> **Hinweis:**
>
> Derzeit wird das Feature nur für Azure- und VMware-Virtualisierungsumgebungen unterstützt.

#### Bedingungen

Um den Identitätsdatenträger erfolgreich zurückzusetzen:

- Schalten Sie die VM aus und versetzen Sie sie in den Wartungsmodus.
- Verwendung Sie nicht den Parameter "-OS"im PowerShell-Befehl.

#### Identitätsinformationen zurücksetzen

So setzen Sie die Identitätsinformationen zurück:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Setzen Sie die Identitätsinformationen zurück.
   - Um nur das Maschinenkennwort und Vertrauensschlüssel zurückzusetzen, führen Sie die folgenden Befehle in der Reihenfolge ihrer Aufführung aus:

     ```
     1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
           PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
           $password -Target IdentityInfo
     2  <!--NeedCopy-->
     ```

     Befehlsparameter:

     - `IdentityAccountName`: Name des Identitätskontos, das repariert werden muss.

- `PrivilegedUserName`: Benutzerkonto mit Schreibberechtigung für den Identitätsanbieter (AD oder Azure AD).
- `PrivilegedUserPassword`: Kennwort für PrivilegedUserName.
- `Target`: Ziel für die Reparaturaktion. Dies kann IdentityInfo zur Reparatur von Kontokennwort/Vertrauensschlüssel sein und UserCertificate für Benutzerzertifikatattribute von Maschinenidentitäten mit Hybrid-Azure AD-Verbindung.

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
    > -Identity -ResetIdentityInfo
<!--NeedCopy-->
```

Der Parameter `ResetIdentityInfo` setzt Folgendes zurück:

- Kennwort und Vertrauensschlüssel: wenn die VM einer AD-Domäne angehört (nur Citrix DaaS)
- Nur Vertrauensschlüssel: wenn die VM keiner AD-Domäne angehört (nur Citrix DaaS)
- Nur Kennwort: wenn die VM einer AD-Domäne angehört (nur Citrix Virtual Apps and Desktops)

- Um die gesamte Konfiguration des Identitätsdatenträgers zurückzusetzen, führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. Geben Sie **y** ein, um die Aktion zu bestätigen. Sie können die Bestätigungsaufforderung auch mithilfe des Parameters `-Force` auslassen. Beispiel:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
<!--NeedCopy-->
```

5. Führen Sie den Befehl `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` aus, um die Einstellung des aktualisierten Identitätsdatenträgers zu überprüfen. Die Attribute des Identitätsdatenträgers (z. B. `IdentityDiskId`) müssen aktualisiert worden sein. `StorageId` und `IdentityDiskIndex` dürfen sich nicht ändern.

### Netzwerkeinstellung für einen vorhandenen Maschinenkatalog ändern

Sie können die Netzwerkeinstellung für einen vorhandenen Maschinenkatalog ändern, sodass die neuen VMs im neuen Subnetz erstellt werden. Verwenden Sie den Parameter `-NetworkMapping` im Befehl `Set-ProvScheme`, um die Netzwerkeinstellung zu ändern.

Führen Sie folgende Schritte aus, um die Netzwerkeinstellung für ein vorhandenes Provisioningschema zu ändern:

1. Führen Sie im PowerShell-Fenster den Befehl `asnp citrix*` aus, um die PowerShell-Module zu laden.
2. Führen Sie `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` aus, um zum Netzwerkpfad zu gelangen, den Sie ändern möchten.
3. Weisen Sie der neuen Netzwerkeinstellung eine Variable zu. Beispiel:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Führen Sie `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap` aus.
5. Führen Sie `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` aus, um die neue Netzwerkeinstellung für das vorhandene Provisioningschema zu überprüfen.

### Versionen eines Maschinenkatalogs verwalten

Wenn ein MCS-Maschinenkatalog mit dem Befehl `Set-ProvScheme` aktualisiert wird, wird die aktuelle Konfiguration als Version gespeichert. Anschließend können Sie die verschiedenen Versionen des Maschinenkatalogs mithilfe von PowerShell-Befehlen verwalten. Sie haben folgende Möglichkeiten:

- Liste der Versionen eines Maschinenkatalogs anzeigen
- Eine frühere Version verwenden, um den Maschinenkatalog zu aktualisieren
- Version manuell löschen, wenn sie nicht von einer VM dieses Maschinenkatalogs verwendet wird
- Maximale Anzahl von Versionen ändern, die vom Maschinenkatalog beibehalten werden sollen (Standardeinstellung ist 99)

Eine Version enthält die folgenden Informationen eines Maschinenkatalogs:

- VMCpuCount
- VMMemoryMB

- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Führen Sie die folgenden Befehle (Beispiele werden angezeigt) aus, um die verschiedenen Versionen eines Maschinenkatalogs zu verwalten.

- So zeigen Sie die Konfigurationsdetails der verschiedenen Versionen eines Maschinenkatalogs an:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

- So zeigen Sie die Konfigurationsdetails einer bestimmten Version eines Maschinenkatalogs an:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 2
<!--NeedCopy-->
```

- So zeigen Sie die Gesamtzahl der Versionen an, die einem Maschinenkatalog zugeordnet sind:

  “‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- So aktualisieren Sie den Maschinenkatalog mit einer früheren Version:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
<!--NeedCopy-->
```

- So löschen Sie eine Version manuell, wenn sie nicht von einer VM dieses Maschinenkatalogs verwendet wird:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 3
<!--NeedCopy-->
```

- So legen Sie die maximale Anzahl von Versionen fest, die vom Maschinenkatalog beibehalten werden sollen (Standardeinstellung ist 99). Diese Einstellung wird auf alle Kataloge angewendet. In diesem Fall werden beispielsweise maximal 15 Versionen für alle von MCS bereitgestellten Kataloge beibehalten.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
<!--NeedCopy-->
```

Wenn die Anzahl der Versionen die maximale Anzahl erreicht, kann keine neue Version erstellt werden, solange ältere Versionen von einer der virtuellen Maschinen im Maschinenkatalog verwendet werden.

Führen Sie in diesem Fall einen der folgenden Schritte aus:

- Erhöhen Sie das Limit für die maximale Anzahl von Versionen, die im Maschinenkatalog aufbewahrt werden sollen.
- Aktualisieren Sie einige VMs, die sich auf älteren Versionen befinden, sodass diese älteren Versionen von keiner VM mehr referenziert werden und gelöscht werden können.

### Cachekonfiguration eines vorhandenen Maschinenkatalogs ändern

Nach der Erstellung eines nicht persistenten Katalogs mit aktiviertem MCSIO können Sie mit dem Befehl `Set-ProvScheme` die folgenden Parameter ändern:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Das Feature gilt derzeit für:

- GCP- und Microsoft Azure-Umgebungen sowie
- nicht persistenter Katalog mit aktiviertem MCSIO

#### Anforderungen

Anforderungen zum Ändern der Cachekonfiguration:

- Update auf die neueste VDA-Version (2308 oder höher).
- Aktivieren des Parameters `UseWriteBackCache` für den Maschinenkatalog. Verwendung von `New-ProvScheme`, um einen Maschinenkatalog mit aktiviertem `UseWriteBackCache` zu erstellen. Beispiel:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
    HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```

#### Cachekonfiguration ändern

Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> **Hinweis:**
>
> - Der Wert von `WriteBackCacheDiskSize` muss größer als Null sein, da mindestens 1 GB Cachedatenträgerplatz erforderlich ist.
> - Der Wert von `WriteBackCacheMemorySize` muss kleiner als die Speichergröße des Maschinenkatalogs sein.
> - Diese Änderungen werden nur auf neue VMs anwendet, die dem Katalog hinzugefügt wurden, nachdem die Änderung vorgenommen wurde. Bestehende VMs sind von diesen Änderungen nicht betroffen.

### Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog in einer Azure-Umgebung konvertieren

Sie können eine VM, eine Vorlagenspezifikation (Azure) oder eine Startvorlage (AWS) als Maschinenprofileingabe verwenden, um einen Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog zu konvertieren. Neue dem Katalog hinzugefügte virtuelle Maschinen übernehmen Eigenschaftswerte aus dem Maschinenprofil.

> **Hinweis:**
>
> Ein Maschinenkatalog, der auf einem Maschinenprofil basiert, kann nicht in einen Maschinenkatalog geändert werden, der nicht auf einem Maschinenprofil basiert.

Gehen Sie hierzu folgendermaßen vor:

1. Erstellen Sie einen persistenten oder nicht persistenten Maschinenkatalog mit VMs und ohne Maschinenprofil.
2. Öffnen Sie das **PowerShell**-Fenster.
3. Führen Sie den Befehl `Set-ProvScheme` aus, um die Eigenschaftswerte aus dem Maschinenprofil auf die neuen VMs anzuwenden, die dem Maschinenkatalog hinzugefügt werden. Beispiel:
   - Azure:

     ```
     Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
         -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
         machineprofile.folder<ResourceGroupName><TemplateSpecName
         ><VersionName>
     <!--NeedCopy-->
     ```

- AWS:

```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
    template>.launchtemplate<launch-template-version>.
    launchtemplateversion"
<!--NeedCopy-->
```

### Mit einem Katalog verknüpfte Warnungen und Fehler abrufen

Sie können historische Fehler und Warnungen abrufen, um Probleme mit Ihrem MCS-Maschinenkatalog zu diagnostizieren und zu beheben.

Mithilfe von PowerShell-Befehlen können Sie:

- eine Liste der Fehler und Warnungen abrufen
- Status von Warnungen von **New** in **Acknowledged** ändern
- Fehler oder Warnungen löschen

Ausführen der PowerShell-Befehle:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.

Um eine Liste der Fehler und Warnungen abzurufen:

Führen Sie den Befehl `Get-ProvOperationEvent` aus.

- Ohne Parameter: Ruft alle Fehler und Warnungen ab.
- Mit den Parametern `LinkedObjectType` und `LinkedObjectUid`: Ruft alle Fehler und Warnungen, die mit einem bestimmten Provisioningschema verknüpft sind, ab.
- Mit Parameter `EventId`: Ruft den Fehler bzw. die Warnung mit der entsprechenden Ereignis-ID ab.
- Mit Parameter `Filter`: Ruft Fehler oder Warnungen unter Anwendung eines benutzerdefinierten Filters ab

Statusänderung von Fehlern oder Warnungen von **New** in **Acknowledged**:

Führen Sie den Befehl `Confirm-ProvOperationEvent` aus.

- Mit Parameter `EventId`: Legt den Status des Fehlers bzw. der Warnung mit der entsprechenden Ereignis-ID ab. Sie können die `EventId` eines Fehlers oder einer Warnung als Ausgabe des Befehls `Get-ProvOperationEvent` abrufen.
- Mit den Parametern `LinkedObjectType` und `LinkedObjectUid`: Legt den Status aller Fehler und Warnungen, die mit einem bestimmten Provisioningschema verknüpft sind, fest.
- Mit Parameter `All`: Setzt den Status aller Fehler und Warnungen auf **Acknowledged**.

Fehler oder Warnungen löschen:

Führen Sie den Befehl `Remove-ProvOperationEvent` aus.

- Mit Parameter `EventId`: Entfernt den Fehler bzw. die Warnung mit der entsprechenden Ereignis-ID. Sie können die `EventId` eines Fehlers oder einer Warnung als Ausgabe des Befehls `Get-ProvOperationEvent` abrufen.
- Mit den Parametern `LinkedObjectType` und `LinkedObjectUid`: Löscht alle Fehler und Warnungen, die mit einem bestimmten Provisioningschema verknüpft sind.
- Mit Parameter `All`: Löscht alle Fehler und Warnungen.

Weitere Informationen finden Sie unter Citrix PowerShell SDK.

### Maschinen ohne Hypervisor-Zugriff löschen

Beim Löschen einer VM oder eines Provisioningschemas müssen die Maschinenerstellungsdienste (MCS) Tags von der VM und manchmal auch vom Basisdatenträger entfernen, damit die in den Löschoptionen enthaltenen Ressourcen nicht mehr von MCS verfolgt oder identifiziert werden. Auf einige dieser Ressourcen kann jedoch nur über den Hypervisor zugegriffen werden. Verwenden Sie die Option `PurgeDBOnly` für `Remove-ProvVM` in PowerShell, um VM-Ressourcenobjekte wie VM, Basisdatenträger, Image in ACG usw. aus der Datenbank zu löschen, auch wenn kein Hypervisor-Zugriff besteht.

Diese Option ist aktiviert für:

- Alle unterstützten Hypervisors
- Persistente und nicht persistente VMs

#### Einschränkungen

Sie können die Befehle -PurgeDBOnly und -ForgetVM nicht gleichzeitig verwenden.

#### Befehl PurgeDBOnly verwenden

Beim Ausführen des PowerShell-Befehls `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` kann der Löschvorgang in den folgenden Szenarios fehlschlagen:

- Die Hostverbindung ist im Wartungsmodus
- Ungültige Anmeldeinformationen
- Authentifizierungsfehler
- Nicht autorisierter Betrieb

- Der Hypervisor ist nicht erreichbar

> **Hinweis:**
>
> Remove-provVM -ForgetVM zielt nur auf persistente VMs ab. Wenn eine der VMs in der Liste nicht persistent ist, schlägt der Vorgang fehl.

Wenn der Vorgang fehlschlägt, weil der Hypervisor nicht erreichbar ist, wird die Folgendes angezeigt:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Verwenden Sie die Option `-PurgeDBOnly` mit dem PowerShell-Befehl `Remove-ProvVM`, um Referenzen einer VM aus der MCS-Datenbank zu löschen. Zum Beispiel:

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

### VDA-Aktualisierungsunterstützung über lokalen Dateifreigabezugriff

Geben Sie den Speicherort des VDA-Installationsprogramms mit PowerShell-Cmdlets an, sodass Sie weniger Netzwerkregeln bereitstellen müssen, damit jeder VDA das neue VDA-Installationsprogramm vom Citrix Managed Azure CDN abrufen kann.

#### PowerShell-Cmdlets

Den Cmdlets **New-VusCatalogSchedule** und **New-VusMachineUpgrade** wurden zwei neue optionale Parameter hinzugefügt, mit denen Sie Installationsprogramme von einer lokalen Dateifreigabe aus verwenden können.

- **VdaWorkstationPackageUri**: um den UNIC-Pfad zum VDA-Installationsprogramm für Arbeitsstationsbetriebssysteme anzugeben
- **VdaServerPackageUri**: um den UNC-Pfad zum VDA-Installationsprogramm für das Serverbetriebssystem anzugeben

#### Voraussetzungen

- VDA Upgrade Agent auf Version 7.40.0.35 oder höher (mit dem VDA-Installationsprogramm Version 2311 oder höher)
- Virtual Apps and Desktops Remote PowerShell SDK Version 7.40 oder höher (veröffentlicht am 10. Januar 2024 oder später)
- Remote PowerShell SDK Version 7.42 oder höher (veröffentlicht nach dem 16. Februar 2024)

**So legen Sie Dateifreigabeberechtigungen fest**

Die Netzwerkfreigaben, die VDA-Installationspakete enthalten, müssen Lesezugriff für den VDA Upgrade Agent-Dienst haben, der als Lokales System (NT AUTHORITY\SYSTEM-Prinzipal) ausgeführt wird.

- **Freigabeberechtigung für Dateien, die in eine Domäne eingebunden sind**

  Wenn die VDA-Maschine einer Domäne beigetreten ist, verwendet das **lokale Systemkonto** (VUA wird als lokales System ausgeführt) Computeranmeldeinformationen für den Zugriff auf Netzwerkfreigaben.

  Die geringste Berechtigung kann festgelegt werden, indem Domänencomputern **Lesezugriff** gewährt wird.

  1. Wählen Sie Personen in Ihrem Netzwerk aus, für die Sie die Datei freigeben möchten.
  2. Klicken Sie auf **Erweiterte Freigabeeinstellungen** und aktivieren Sie die **Datei- und Druckerfreigabe**.

- **Erlaubnis zur Freigabe von Dateien, die nicht mit einer Domäne verbunden sind**

  Wenn die VDA-Maschine nicht in eine Domäne eingebunden ist, verwendet das **lokale Systemkonto** (VUA wird als lokales System ausgeführt) **ANONYMOUS LOGON,** wenn auf Netzwerkfreigaben zugegriffen wird.

  1. Wählen Sie einen freigegebenen Ordner aus.
  2. Deaktivieren Sie den Kennwortschutz.
     a) Gehen Sie zum Ordner **Eigenschaften**.
     b) Wählen Sie **Netzwerk- und Freigabecenter** aus.
     c) Schalten Sie **Kennwortgeschützte Freigabe** aus.
  3. Klicken Sie auf **Erweiterte Freigabe**, um eine Freigabeberechtigung zu erteilen.
     a) Wählen Sie **Berechtigungen**.
     b) Erteilen Sie **ANONYMOUS LOGON** eine Freigabe-**Leseberechtigung**.
  4. Wählen Sie die Registerkarte **Sicherheit**, um Ordnerberechtigungen zu gewähren
     a) Klicken Sie auf **Bearbeiten**, um dem freigegebenen Ordner Berechtigungen hinzuzufügen.
     b) Wählen Sie den freigegebenen Ordner aus, um **ANONYMOUS LOGON** Ordnerberechtigungen zu gewähren.
  5. Klicken Sie auf **Erweitert**, um die **Datei- und Druckerfreigabe** zu aktivieren.
  6. Fügen Sie den Namen des freigegebenen Ordners zur **Netzwerkzugriffssicherheitsrichtlinie** hinzu.

> **Hinweis:**
>
> Starten Sie Ihre Maschine neu, damit die Änderung sofort wirksam wird.

#### VDA-Updates von einer lokalen Dateifreigabe

1. Laden Sie das VDA-Installationsprogramm herunter und platzieren Sie es in der freigegebenen Datei.

   > **Hinweis:**
   >
   > Mit Virtual Upgrade Service können Sie zwischen dem Titel Current Release oder LTSR-Track wählen.
   >
   > **Beispiel:** Wenn für den Maschinenkatalog die aktuelle Version 2311 festgelegt ist und die VDA-Version 2305 ist, müssen Sie den VDA auf Version 2311 aktualisieren.

   a) Navigieren Sie zur Seite **Downloads** auf unserer Website.
   b) Wählen Sie **Citrix Virtual Apps and Desktops** als Produkt aus.
   c) Wählen Sie **Citrix Virtual Apps and Desktops 7 2311, alle Editionen**.
   d) Wählen Sie das VDA-Installationsprogramm aus den **Komponenten aus, die sich auf der Produkt-ISO befinden, aber auch separat erweiterbar** sind.

2. Wählen Sie das entsprechende VDA-Installationsprogramm basierend auf dem Katalogtyp aus.

   - Laden Sie das **VDA-Installationsprogramm für Multisitzungs-OS** herunter, wenn der Katalogtyp **Mehrere Sitzungen** ist.
   - Laden Sie das **VDA-Installationsprogramm für Einzelsitzungs-OS** herunter, wenn der Katalogtyp **Einzelsitzung** ist.
   - Laden Sie das **Installationsprogramm des Kernkomponenten-VDA unter Einzelsitzungs-OS-Betriebssystem** herunter, wenn der Katalogtyp **Remote-PC-Zugriff** ist.

> **Hinweis:**
>
> Die Version des Fileshare-Installationsprogramms muss **genau** mit der Version der neuesten Version des Installationsprogramms übereinstimmen, die von VUS in der Cloud veröffentlicht wurde.

## Problembehandlung

- Empfehlungen für Maschinen mit dem Status `Power State Unknown` finden Sie unter CTX131267.

- Informationen zum Beheben von Problemen bei VMs, für die ständig ein unbekannter Energiezustand angezeigt wird, finden Sie unter How to fix VMs that continuously show an unknown power state.
- Wenn ein Cloud Connector nicht ordnungsgemäß funktioniert, dauern MCS-Provisioningvorgänge (z. B. Katalogaktualisierungen) länger und die Leistung der Verwaltungsoberfläche wird erheblich beeinträchtigt.

### So geht es weiter

Informationen zum Verwalten bestimmter Hypervisor-Kataloge finden Sie unter:

- AWS-Katalog verwalten
- Google Cloud Platform -Katalog verwalten
- Microsoft Azure-Katalog verwalten
- Microsoft System Center Virtual Machine Manager-Katalog verwalten
- VMware-Katalog verwalten
- XenServer-Katalog verwalten

## AWS-Katalog verwalten

January 25, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf AWS-Cloudumgebungen.

> **Hinweis:**
>
> Sie müssen einen AWS-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe AWS-Katalog erstellen.

### Tags entfernen

Wenn Sie einen Katalog oder eine VM erstellen, werden Tags für folgende Ressourcen erstellt:

- Virtuelle Maschine
- Stammdatenträger-Volume
- Identitätsdatenträger-Volume
- Elastische Netzwerkschnittstelle (ENI)
- Stammdatenträgerimage (AMI)
- Startvorlage

- Snapshot von AMI oder Stammdatenträger

Sie können VMs und Maschinenkataloge aus der Citrix Datenbank sowie von Citrix erstellte Tags entfernen. Optionen:

- `Remove-ProvVM` mit dem Parameter `ForgetVM` zum Entfernen von VMs und von Citrix erstellten Tags aus einer einzelnen VM oder einer Liste von VMs aus einem Maschinenkatalog.

  > **Hinweis:**
  >
  > Mit dem Parameter `ForgetVM` werden die VMs aus der Datenbank des Provisioningschemas von Citrix entfernt, die VMs verbleiben jedoch weiterhin im Hypervisor.

- `Remove-ProvScheme` mit Parameter `ForgetVM` zum Entfernen eines Maschinenkatalogs aus der Citrix Datenbank und von Ressourcen aus einem Maschinenkatalog.

Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Entsperren Sie die VM, bevor Sie die VMs entfernen. Beispiel:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   <!--NeedCopy-->
   ```

4. Führen Sie einen der folgenden Befehle aus, um VMs, Maschinenkataloge und von Citrix erstellte Tags aus Ressourcen zu entfernen.

   - Führen Sie `Remove-ProvVM` mit `ForgetVM` aus, um VMs aus der Citrix-Datenbank und von Citrix erstellte Tags aus VMs zu entfernen. Beispiel:

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
        >" -ForgetVM
     <!--NeedCopy-->
     ```

   - Führen Sie `Remove-ProvScheme` aus, um einen Maschinenkatalog aus der Citrix Datenbank und Ressourcen aus einem Maschinenkatalog zu entfernen. Beispiel:

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
        ForgetVM
     <!--NeedCopy-->
     ```

5. Vergewissern Sie sich, dass die VM aus dem Delivery Controller, nicht aber dem Hypervisor entfernt wurde.

   a) Führen Sie `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"` aus. Es darf nichts zurückgegeben werden.

b) Rufen Sie die AWS-EC2-Konsole auf. Die VMs müssten angezeigt werden, die von Citrix erstellten Tags sind jetzt jedoch entfernt. Von Citrix erstellte Tags wurden aus den folgenden Ressourcen entfernt:

- Virtuelle Maschine
- Stammdatenträger-Volume
- Identitätsdatenträger-Volume
- ENI

6. Wenn Sie den Maschinenkatalog entfernen, vergewissern Sie sich, dass der Katalog vom Delivery Controller entfernt wurde.

a) Führen Sie `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"` aus. Dies muss einen Fehler zurückgeben.

b) Vergewissern Sie sich in der AWS-EC2-Konsole, dass die folgenden Ressourcen entfernt wurden.

- Stammdatenträgerimage (AMI)
- Startvorlage
- Snapshot von AMI oder Stammdatenträger

### Identifizieren der von MCS erstellten Ressourcen

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen auf der AWS-Plattform hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
|---|---|
| ID-Datenträger | “Name”: “VMName_IdentityDisk” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Image | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| ENI | “Description”: “XD Nic” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| OS-Datenträger | “Name”: “VMName_rootDisk” |

| Ressourcenname | Tag |
| --- | --- |
| | “XdConfig”: “XdProvisioned=True” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | [Wenn AwsCaptureInstanceProperties = true] “Citrix Resource”: “” |
| | [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Vorbereitungs-VM | “Name”: “Preparation - CatalogName - xxxxxxxxxx” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | [Wenn AwsCaptureInstanceProperties = true] “Citrix Resource”: “” |
| | [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Veröffentlichter Snapshot | “XdConfig”: “XdProvisioned=true” |
| | Wenn kein Snapshot für Volumeworker-AMI, dann “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxxxxxx” |
| Vorlage | [Wenn AwsCaptureInstanceProperties = true] “XdConfig”: “XdProvisioned=true” |
| | [Wenn AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | [Wenn AwsCaptureInstanceProperties = true] “CitrixResource”: “” |
| | [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| VM im Katalog | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | [Wenn AwsCaptureInstanceProperties = true] “CitrixResource”: “” |

| Ressourcenname | Tag |
| --- | --- |
| | [Wenn AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [Wenn AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Volumeworker-AMI | “XdConfig”: “XdProvisioned=true” |
| Volumeworker-Bootstrapper | “Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “” |
| Volumeworker-Instanz | “Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true” |

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu AWS
- Maschinenkataloge erstellen
- AWS-Katalog erstellen
- Maschinenkataloge verwalten

## Google Cloud Platform-Katalog verwalten

February 14, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Google-Cloudumgebungen.

> **Hinweis:**
>
> Sie müssen einen Google Cloud Platform-Katalog erstellt haben, bevor Sie ihn verwalten können. Weitere Informationen finden Sie unter Google Cloud Platform-Katalog erstellen.

### Hinzufügen von Maschinen zum Maschinenkatalog

Führen Sie folgende Schritte aus, um Maschinen zu einem Katalog hinzuzufügen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie den Maschinenkatalog aus, dem Sie Maschinen hinzufügen möchten.
3. Wählen Sie in der Aktionsleiste **Maschinen hinzufügen**.
4. Geben Sie auf der Seite **Virtuelle Maschinen** die Anzahl der hinzuzufügenden Maschinen an und wählen Sie **Weiter**.
5. Wählen Sie auf der Seite **Maschinenidentitäten** ein Active Directory-Konto aus und wählen Sie **Weiter**.
6. Wählen Sie auf der Seite **Domänenanmeldeinformationen** die Option **Anmeldeinformationen eingeben**. Geben Sie den Benutzernamen und das Kennwort ein, wählen Sie **Speichern** und dann **Weiter**.
7. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und wählen Sie **Fertig stellen**.

### Maschinen aktualisieren

Dieses Feature kann nützlich sein, wenn Sie Ihr Masterimage oder die Mindestfunktionsebene aktualisieren möchten.

Führen Sie folgende Schritte aus, um Maschinen zu aktualisieren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie den Maschinenkatalog aus, der die zu aktualisierenden Maschinen enthält.
3. Wählen Sie in der Aktionsleiste die Option **Masterimage ändern**.
4. Wählen Sie auf der Seite **Image** eine VM und die Mindestfunktionsebene für den Katalog aus und wählen Sie **Weiter**.
5. Geben Sie auf der Seite **Rolloutstrategie** an, wann die Maschinen aktualisiert werden sollen und wählen Sie **Weiter**.
6. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und wählen Sie **Fertig stellen**.

### Ein Maschinenupdate rückgängig machen

Führen Sie folgende Schritte zum Rollback eines Maschinenupdates aus:

> **Wichtig:**
>
> Masterimages dürfen nicht umbenannt, gelöscht oder verschoben werden. Dies würde ein Rollback des Updates verhindern.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
2. Wählen Sie den Maschinenkatalog aus, für den Sie ein Rollback des Maschinenupdates ausführen möchten.
3. Wählen Sie in der Aktionsleiste **Rollback für Masterimage ausführen**.
4. Überprüfen Sie die Informationen auf der Seite **Übersicht** und wählen Sie **Weiter**.
5. Konfigurieren Sie auf der Seite **Rolloutstrategie** die Rolloutstrategie und wählen Sie **Weiter**.
6. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und wählen Sie **Fertig stellen**.

### Energieverwaltung

Citrix DaaS ermöglicht die Energieverwaltung von Google Cloud-Maschinen. Mit dem Knoten **Suchen** im Navigationsbereich finden Sie die Maschine, für die Sie eine Energieverwaltung festlegen möchten. Folgende Energieaktionen stehen zur Verfügung:

- Löschen
- Starten
- Neustarten
- Neustart erzwingen
- Herunterfahren
- Herunterfahren erzwingen
- Zu Bereitstellungsgruppe hinzufügen
- Tags verwalten
- Wartungsmodus einschalten

Sie können die Energieverwaltung für Google Cloud-Maschinen auch mit Autoscale aktivieren. Fügen Sie hierfür die Google Cloud-Maschinen einer Bereitstellungsgruppe hinzu und aktivieren Sie Autoscale für diese Bereitstellungsgruppe. Weitere Hinweise zu Autoscale finden Sie unter Autoscale.

### Bereitgestellte Maschinen mit PowerShell aktualisieren

Mit dem Befehl `Set-ProvScheme` ändern Sie das Provisioningschema. Dies wirkt sich jedoch nicht auf vorhandene Maschinen aus. Mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` können Sie jetzt das aktuelle Provisioningschema auf eine oder mehrere persistente oder nicht persistente Maschine(n) anwenden. Derzeit werden in GCP von dieser Funktion folgende Eigenschaftenaktualisierungen unterstützt: Maschinenprofil, Serviceangebot und benutzerdefinierte Katalogeinstellungen.

Sie können Folgendes aktualisieren:

- Eine einzelne VM
- Eine Liste bestimmter VMs oder alle VMs, die mit der ID eines Provisioningschemas verknüpft sind.
- Eine Liste bestimmter VMs oder alle VMs, die mit dem Namen eines Provisioningschemas verknüpft sind.

Schrittfolge zum Aktualisieren der vorhandenen VMs:

1. Prüfen Sie die Konfiguration der vorhandenen Maschinen. Beispiel:

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aktualisieren Sie das Provisioningschema. Beispiel:

   - Maschinenprofil aktualisieren

```
`Set-ProvScheme  – ProvisioningSchemeName "my-catalog"  –
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofileinstance.vm"
<!--NeedCopy-->
```

   - Serviceangebot aktualisieren

```
 Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering  “ XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
 <!--NeedCopy-->
```

3. Überprüfen Sie, ob die aktuelle Eigenschaft der VM mit dem aktuellen Provisioningschema übereinstimmt und ob eine Aktualisierungsaktion auf der VM aussteht. Beispiel:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

   Sie können auch Maschinen einer bestimmten Version finden. Beispiel:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Aktualisieren Sie vorhandene Maschinen.

   - Gehen Sie zum Aktualisieren aller vorhandenen Maschinen folgendermaßen vor:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
         -StartsNow -DurationInMinutes -1
     <!--NeedCopy-->
     ```

   - Zum Aktualisieren einer Liste bestimmter Maschinen:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
         -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
        -1
     <!--NeedCopy-->
     ```

   - Zum Aktualisieren von Maschinen basierend auf der Ausgabe von `Get-ProvVM`:

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
        ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
        -StartsNow -DurationInMinutes -1
     <!--NeedCopy-->
     ```

   > **Hinweis:**
   >
   > - `StartsNow` gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
   > - `DurationInMinutes` mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

5. Suchen Sie Maschinen mit einem geplanten Update. Beispiel:

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
       , ProvisioningSchemeUpdateAfter
   <!--NeedCopy-->
   ```

6. Starten Sie die Maschinen neu. Beim nächsten Einschalten werden Eigenschaftsänderungen auf die vorhandenen Maschinen angewendet. Sie können den aktualisierten Status mit dem folgenden Befehl überprüfen:

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
       ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

### Datenträgerbezogene benutzerdefinierte Eigenschaften eines Katalogs ändern

Sie können die folgenden datenträgerbezogenen benutzerdefinierten Eigenschaften eines Katalogs und der VMs des Katalogs ändern:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Hinweis:**
>
> - Die Eigenschaft `StorageType` ist für den OS-Datenträger vorgesehen.
> - Die Eigenschaft `PersistOsDisk` kann nur für nicht persistente Kataloge mit aktiviertem Zurückschreibcache festgelegt werden

Diese Implementierung hilft Ihnen, auch nach der Erstellung eines Katalogs verschiedene Speichertypen für verschiedene Datenträger auszuwählen und so den Preisen für die verschiedenen Speichertypen Rechnung zu tragen.

Verwenden Sie dazu die PowerShell-Befehle `Set-ProvScheme` und `Set-ProvVMUpdateTimeWindow`:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Führen Sie `Get-ProvVM -VMName <VM name>` aus, um die benutzerdefinierten Eigenschaften abzurufen.
4. Ändern Sie die Zeichenfolge der benutzerdefinierten Eigenschaften:
   a) Kopieren Sie die benutzerdefinierten Eigenschaften in einen Editor und ändern Sie die benutzerdefinierten Eigenschaften.
   b) Fügen Sie im **PowerShell-Fenster** die geänderte Zeichenfolge für "Custom Properties"aus dem Editor ein, und weisen Sie ihr eine Variable zu. Beispiel:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
```

```
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aktualisieren Sie den bestehenden Katalog. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
    CustomProperties $cp
<!--NeedCopy-->
```

6. Aktualisieren Sie die vorhandenen VMs. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Starten Sie die VMs neu. Beim nächsten Einschalten werden Änderungen benutzerdefinierter Eigenschaften auf die vorhandenen Maschinen angewendet.

### Schutz vor versehentlichem Löschen von Maschinen

Citrix DaaS ermöglicht den Schutz von MCS-Ressourcen in Google Cloud vor versehentlichem Löschen. Konfigurieren Sie die bereitgestellte VM, indem Sie das Flag `deletionProtection` auf TRUE setzen.

Standardmäßig werden mit MCS oder dem Google Cloud-Plug-In bereitgestellte VMs mit aktiviertem InstanceProtection erstellt. Die Implementierung gilt für persistente und nicht persistente Kataloge. Nicht persistente Kataloge werden aktualisiert, wenn die Instanzen anhand der Vorlage neu erstellt werden. Für bestehende persistente Maschinen können Sie das Flag in der Google Cloud-Konsole festlegen. Weitere Informationen zum Festlegen des Flags finden Sie in der Google-Dokumentation. Neue Maschinen, die zu persistenten Katalogen hinzugefügt wurden, werden mit aktiviertem Flag `deletionProtection` erstellt

Der Versuch, eine VM-Instanz, für die das Flag `deletionProtection` festgelegt ist, zu löschen, schlägt fehl. Wenn Sie jedoch die Berechtigung `compute.instances.setDeletionProtection` oder die IAM-Rolle **Compute-Administrator** haben, können Sie das Flag zurücksetzen, damit die Ressource gelöscht werden kann.

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen auf der GCP-Plattform hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
| --- | --- |
| ID-Datenträger | “CitrixResource”: “internal” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Image | “CitrixResource”: “internal” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| OS-Datenträger | “CitrixResource”: “internal” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Vorbereitungs-VM | “CitrixResource”: “internal” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Veröffentlichter Snapshot | “CitrixResource”: “internal” |
| Speicherbucket | “CitrixResource”: “internal” |
| Vorlage | “CitrixResource”: “internal” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| VM im Katalog | “CitrixResource”: “internal” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. Das Plug-In fügt auch dieses Tag für von MCS bereitgestellte VMs hinzu: “citrix-provisioning-scheme-id”: “provSchemeId”. Sie können es verwenden, um in der GCP-Konsole nach Katalog zu filtern. |
| WBC-Datenträger | “CitrixResource”: “internal” |
| | CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

> **Hinweis:**
>
> Eine VM ist im Citrix-Bestand nicht sichtbar, wenn ein **CitrixResource**-Tag hinzugefügt wird, um sie als eine von MCS erstellte Ressource zu identifizieren. Sie können das Tag entfernen oder umbenennen, um sie sichtbar zu machen.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Google-Cloudumgebungen
- Maschinenkataloge erstellen
- Google Cloud Platform-Katalog erstellen
- Maschinenkataloge verwalten

## Einen HPE Moonshot-Katalog verwalten

May 17, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf HPE Moonshot-Kataloge.

> **Hinweis:**
>
> Sie müssen einen HPE Moonshot-Katalog erstellt haben, bevor Sie ihn verwalten können. Weitere Informationen finden Sie unter HPE Moonshot-Maschinenkatalog erstellen.

### Energieverwaltung

Citrix DaaS ermöglicht die Energieverwaltung von HPE Moonshot-Maschinen. Mit dem Knoten **Suchen** im Navigationsbereich finden Sie die Maschine, für die Sie eine Energieverwaltung festlegen möchten. Folgende Energieaktionen stehen zur Verfügung:

- Starten
- Herunterfahren
- Herunterfahren erzwingen
- Neu starten
- Zurücksetzen

> **Hinweis:**
>
> Die Energieaktionen **Anhalten** und **Fortsetzen** werden nicht unterstützt.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu HPE Moonshot

- Maschinenkataloge erstellen
- HPE Moonshot-Maschinenkatalog erstellen
- Maschinenkataloge verwalten

## Microsoft Azure-Katalog verwalten

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Sie müssen einen Microsoft Azure-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe Microsoft Azure-Katalog erstellen.

### Speichertyps beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern

Sie können Speicherkosten sparen, indem Sie den Speichertyp eines verwalteten Datenträgers auf eine niedrigere Ebene umstellen, wenn Sie eine VM herunterfahren. Verwenden Sie dazu die benutzerdefinierte Eigenschaft `StorageTypeAtShutdown`.

Der Speichertyp des Datenträgers ändert sich in eine niedrigere Ebene (wie in der benutzerdefinierten Eigenschaft `StorageTypeAtShutdown` angegeben), wenn Sie die VM herunterfahren. Nach dem Einschalten der VM ändert sich der Speichertyp in den ursprünglichen Speichertyp zurück (wie in der benutzerdefinierten Eigenschaft `StorageType` oder `WBCDiskStorageType` angegeben).

> **Wichtig:**
>
> - Der Datenträger ist erst vorhanden, wenn die VM mindestens einmal eingeschaltet wurde. Daher können Sie den Speichertyp nicht ändern, wenn Sie die VM zum ersten Mal einschalten.

> - Der Start einer VM kann etwas länger dauern, nachdem Sie den Speichertyp auf eine niedrigere Stufe geändert haben.

### Anforderungen

- Gilt für einen verwalteten Datenträger. Dies bedeutet, dass Sie die benutzerdefinierte Eigenschaft `UseManagedDisks` auf "true"festlegen.
- Gilt für einen persistenten und nicht persistenten Katalog mit einem persistenten OS-Datenträger. Dies bedeutet, dass Sie die benutzerdefinierte Eigenschaft `persistOsDisk` auf "true"festlegen.
- Gilt für einen nicht persistenten Katalog mit einem persistenten WBC-Datenträger. Dies bedeutet, dass Sie die benutzerdefinierte Eigenschaft `persistWBC` auf "true"festlegen.

### Einschränkung

- Gemäß Vorgaben von Microsoft können Sie den Datenträgertyp nur zweimal pro Tag ändern. Siehe Microsoft-Dokumentation. Gemäß Citrix erfolgt das `StorageType`-Update immer dann, wenn eine Aktion zum Starten oder Aufheben der Zuordnung für die VM erfolgt. Beschränken Sie daher die Anzahl der Energieaktionen pro VM auf zwei pro Tag. Beispiel: eine Energieaktion morgens zum VM-Start und eine abends, um die Zuordnung der VM aufzuheben.

### Speichertyp auf eine niedrigere Ebene ändern

Bevor Sie mit den Schritten fortfahren, lesen Sie die Abschnitte Anforderungen und Einschränkungen.

1. Fügen Sie die benutzerdefinierte Eigenschaft `StorageTypeAtShutdown` hinzu, legen Sie den Wert auf Standard_LRS (HDD) fest und erstellen Sie einen Katalog mit `New-ProvScheme`. Informationen zum Erstellen eines Katalogs mit PowerShell finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Hinweis:**
   >
   > Wenn `StorageTypeAtShutdown` einen anderen Wert als leer hat oder Standard_LRS (HDD) ist, schlägt der Vorgang fehl.

   Beispiel für das Festlegen benutzerdefinierter Eigenschaften beim Erstellen eines persistenten Katalogs:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS “  />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
     />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> ’
<!--NeedCopy-->
```

Beispiel für das Festlegen benutzerdefinierter Eigenschaften beim Erstellen eines nicht persistenten Katalogs:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.
    com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
    Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
     />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> ’
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie ein Maschinenprofil verwenden, hat die benutzerdefinierte Eigenschaft Vorrang vor der in `MachineProfile` definierten Eigenschaft.

2. Fahren Sie die VM herunter und überprüfen Sie den Speichertyp der VM im Azure-Portal.

Der Speichertyp des Datenträgers ändert sich in eine niedrigere Ebene, wie in der benutzerdefinierten Eigenschaft `StorageTypeAtShutdown` angegeben.

3. Schalten Sie die VM ein. Der Speichertyp des Datenträgers ändert sich zurück zu dem aufgeführten Speichertyp:

   - Benutzerdefinierte Eigenschaft `StorageType` für OS-Datenträger
   - Benutzerdefinierte Eigenschaft `WBCDiskStorageType` für WBC-Datenträger, nur wenn Sie sie in `CustomProperties` angeben. Andernfalls ändert er sich zurück zum unter `StorageType` angegebenen Speichertyp.

### `StorageTypeAtShutdown` auf einen vorhandenen Katalog anwenden

Bevor Sie mit den Schritten fortfahren, lesen Sie die Abschnitte Anforderungen und Einschränkungen.

Verwenden Sie `Set-ProvScheme`, um `StorageTypeAtShutdown` auf die neuen, einem Katalog hinzugefügten virtuellen Maschinen anzuwenden.

Beispiel für das Festlegen benutzerdefinierter Eigenschaften beim Hinzufügen einer VM zu einem vorhandenen Katalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties> '

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

### Speichertyp vorhandener VMs beim Herunterfahren in niedrigere Ebene ändern

Bevor Sie mit den Schritten fortfahren, lesen Sie die Abschnitte Anforderungen und Einschränkungen.

Sie können Speicherkosten sparen, indem Sie den Speichertyp vorhandener VMs beim Herunterfahren der VMs in eine niedrigere Ebene ändern.

Führen Sie folgende Schritte aus, um den Speichertyp vorhandener Maschinen in einem Katalog beim Herunterfahren der VMs in eine niedrigere Ebene zu ändern:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie `Get-Provscheme -ProvisioningSchemeName $CatalogName` aus.
4. Ändern Sie die Zeichenfolge der benutzerdefinierten Eigenschaften.

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aktualisieren Sie das Provisioningschema des vorhandenen Katalogs. Das Update gilt für neue VMs, die nach dem Ausführen von `Set-ProvScheme` hinzugefügt wurden.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Aktualisieren Sie die vorhandenen VMs, um `StorageTypeAtShutdown` zu aktivieren.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Beim nächsten Einschalten der Maschinen wird die Eigenschaft `StorageTypeAtShutdown` der Maschinen aktualisiert. Der Speichertyp ändert sich beim nächsten Herunterfahren.
8. Führen Sie den folgenden Befehl aus, um den Wert `StorageTypeAtShutdown` für jede VM in einem Katalog anzuzeigen.

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
      ConvertFrom-Json).StorageTypeAtShutdown.
    DiskStorageAccountType; return New-Object psobject -Property
    @{
```

```
    "VMName" = $vmName; "StorageTypeAtShutdown" =
       $storageTypeAtShutdown  }
    }

<!--NeedCopy-->
```

### Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema

Mit dem Befehl `Set-ProvScheme` ändern Sie das Provisioningschema. Dies wirkt sich jedoch nicht auf vorhandene Maschinen aus. Mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` können Sie das aktuelle Provisioningschema auf eine oder mehrere persistente oder nicht persistente Maschine(n) anwenden. Sie können auch ein Zeitfenster für die Konfigurationsupdates der vorhandenen, per MCS bereitgestellten Maschinen festlegen. Während dieses Zeitfensters wird dann bei jedem Einschalten oder Neustart ein geplantes Update des Provisioningschemas auf eine Maschine angewendet. Derzeit können Sie in Azure `ServiceOffering`, `MachineProfile` und die folgenden benutzerdefinierten Eigenschaften aktualisieren:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Hinweis:**
>
> - Sie können nur die benutzerdefinierten Eigenschaften `StorageType`, `WBCDiskStorageType` und `IdentityDiskStorageType` eines Katalogs mit verwaltetem Datenträger in Azure-Umgebungen aktualisieren.
> - Wenn Sie `Set-ProvVMUpdateTimeWindow` zweimal ausführen, wird der neueste Befehl wirksam.

Sie können Folgendes aktualisieren:

- Eine einzelne VM
- Eine Liste bestimmter VMs oder alle VMs, die mit der ID eines Provisioningschemas verknüpft sind.
- Eine Liste bestimmter VMs oder alle VMs, die mit dem Namen eines Provisioningschemas (Maschinenkatalogname) verknüpft sind.

Nachdem Sie die folgenden Änderungen am Provisioningschema vorgenommen haben, wird die VM-Instanz für persistente Kataloge in Azure neu erstellt:

- Ändern Sie `MachineProfile`.
- Entfernen Sie `LicenseType`.
- Entfernen Sie `DedicatedHostGroupId`.

> **Hinweis:**
>
> Der Betriebssystemdatenträger vorhandener Maschinen samt Daten bleibt unverändert, und es wird eine neue VM mit dem Datenträger verbunden.

Bevor Sie die vorhandenen VMs aktualisieren:

1. Prüfen Sie die Konfiguration der vorhandenen Maschinen. Zum Beispiel:

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aktualisieren Sie das Provisioningschema. Zum Beispiel:

   - VM zur Eingabe des Maschinenprofils verwenden:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   virtual-machine>.vm"
<!--NeedCopy-->
```

   - Vorlagenspezifikation zur Eingabe des Maschinenprofils verwenden:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   template-spec>.templatespec<template-spec-version>.
   templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

   - Nur Dienstangebot verwenden:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Überprüfen Sie, ob die aktuelle Eigenschaft der VM mit dem aktuellen Provisioningschema übereinstimmt und ob eine Aktualisierungsaktion auf der VM aussteht. Zum Beispiel:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Sie können auch Maschinen einer bestimmten Version finden. Zum Beispiel:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

Um Updates für bestehende Maschinen anzufordern, die beim nächsten Neustart angewendet werden sollen, gehen Sie wie folgt vor:

1. Führen Sie die folgenden Befehle aus, um bestehende Maschinen zu aktualisieren und die Updates beim nächsten Neustart anwenden zu lassen.

   - Aktualisieren Sie alle vorhandenen Maschinen. Zum Beispiel:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
         -StartsNow -DurationInMinutes -1
     <!--NeedCopy-->
     ```

   - Aktualisieren Sie eine Liste bestimmter Maschinen. Zum Beispiel:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
         -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
        -1
     <!--NeedCopy-->
     ```

   - Aktualisieren Sie Maschinen basierend auf der Ausgabe von Get-ProvVM. Zum Beispiel:

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
        ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
        -StartsNow -DurationInMinutes -1
     <!--NeedCopy-->
     ```

   > **Hinweis:**
   >
   > - `StartsNow` gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
   > - `DurationInMinutes` mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

2. Suchen Sie Maschinen mit einem geplanten Update. Zum Beispiel:

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
       , ProvisioningSchemeUpdateAfter
   <!--NeedCopy-->
   ```

3. Starten Sie die Maschinen neu. Beim nächsten Einschalten werden Eigenschaftsänderungen auf die vorhandenen Maschinen angewendet. Sie können den aktualisierten Status mit dem folgenden Befehl überprüfen. Zum Beispiel:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Zum Planen des Updates einer VM auf die neuesten Provisioningeinstellungen beim nächsten Start im geplanten Zeitfenster:

1. Führen Sie die folgenden Befehle aus:

   - Update mit der aktuellen Uhrzeit als Startzeit planen:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

   - Update an einem Wochenende planen:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022
    9:00am" -DurationInMinutes (New-TimeSpan -Days 2).
    TotalMinutes
<!--NeedCopy-->
```

   > **Hinweis:**
   >
   > - `VMName` ist optional. Wenn nicht angegeben, wird das Update für den gesamten Katalog geplant.
   > - Verwenden Sie statt `StartTimeInUTC` den Befehl `StartsNow`, um anzugeben, dass die geplante Startzeit der aktuellen Uhrzeit entspricht.
   > - `DurationInMinutes` ist optional. Der Standardwert ist 120 Minuten. Eine negative Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

2. Überprüfen Sie den Updatestatus.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Schalten Sie die VM ein. Wenn Sie die Maschine nach dem geplanten Zeitfenster einschalten, wird das Konfigurationsupdate nicht durchgeführt. Wenn Sie die Maschine innerhalb des geplanten Zeitfensters einschalten,

   - Wenn die Maschine ausgeschaltet ist und
     - Sie die Maschine nicht einschalten, wird das Konfigurationsupdate nicht angewendet.

  - Sie die Maschine einschalten, wird das Konfigurationsupdate angewendet.
- Wenn die Maschine eingeschaltet ist und
  - Sie die Maschine nicht neu starten, wird das Konfigurationsupdate nicht angewendet.
  - Sie die Maschine neu starten, wird das Konfigurationsupdate angewendet.

Konfigurationsupdate abbrechen:

Sie können ein Konfigurationsupdate auch für eine einzelne VM, mehrere VMs oder einen gesamten Katalog abbrechen. Konfigurationsupdate abbrechen:

1. Führen Sie `Clear-ProvVMUpdateTimeWindow` aus. Beispiel:
   - Das für eine einzelne VM geplante Konfigurationsupdate abbrechen:

     ```
     1  Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-
        catalog “ -VMName “ vm1 ”
     2  <!--NeedCopy-->
     ```

   - Das für mehrere VMs geplante Konfigurationsupdate abbrechen:

     ```
     1   Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
         catalog" -VMName "vm1","vm2"
     2  <!--NeedCopy-->
     ```

> **Hinweis:**
>
> Die VMs müssen aus demselben Katalog stammen.

### Eigenschaften einzelner VMs aktualisieren

Sie können die Eigenschaften einzelner VMs in einem persistenten MCS-Maschinenkatalog mithilfe des PowerShell-Befehls `Set-ProvVM` aktualisieren. Die Updates werden jedoch nicht sofort angewendet. Sie müssen das Zeitfenster zur Anwendung der Updates mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` festlegen.

Mithilfe dieser Implementierung können Sie einzelne VMs effizient verwalten, ohne den gesamten Maschinenkatalog aktualisieren zu müssen. Derzeit gilt dieses Feature nur für die Azure-Umgebung.

Derzeit können Sie folgende Eigenschaften aktualisieren:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Mit dem Feature ist Folgendes möglich:

- Eigenschaften einer VM aktualisieren
- Aktualisierte Eigenschaften auf einer VM nach dem Aktualisieren des Maschinenkatalogs beibehalten
- Auf eine VM angewendete Konfigurationsupdates rückgängig machen

Vor dem Aktualisieren der Eigenschaften einer VM:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Prüfen Sie die Konfiguration des vorhandenen Maschinenkatalogs. Beispiel:

```
1 Get-ProvScheme -ProvisioningSchemeName AzureCatalog
2 <!--NeedCopy-->
```

4. Überprüfen Sie die Konfiguration der VM, die Sie aktualisieren möchten. Beispiel:

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

### Eigenschaften einer VM aktualisieren

Gehen Sie wie folgt vor, um die Eigenschaften einer VM zu aktualisieren:

1. Schalten Sie die VM aus, auf der Sie die Updates anwenden möchten.
2. Aktualisieren Sie die Eigenschaften der VM. Wenn Sie beispielsweise die benutzerdefinierte Eigenschaft Speichertyp (`StorageType`) der VM aktualisieren möchten, führen Sie Folgendes aus:

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
     CustomProperties "...<Property Name='StorageType' Value='
     Premium_LRS' />..."
2 <!--NeedCopy-->
```

   Sie können die Eigenschaften zweier VMs in einem Maschinenkatalog gleichzeitig aktualisieren. Beispiel:

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
     CustomProperties "...<Property Name='StorageType' Value='
     Premium_LRS' />..."
2 <!--NeedCopy-->
```

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
     CustomProperties "...<Property Name='StorageType' Value='
     StandardSSD_LRS' />..."
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die Updates werden nicht sofort angewendet.

3. Rufen Sie die Liste der zur Aktualisierung angegebenen Eigenschaften und die Konfigurationsversion ab. Beispiel:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

   Überprüfen Sie den Eigenschaftswert von `Version` und die Eigenschaften, die aktualisiert werden sollen (in diesem Fall `StorageType`).

4. Überprüfen Sie die Konfigurationsversion. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Überprüfen Sie den Wert der Eigenschaft `ProvVMConfigurationVersion`. Das Update wurde noch nicht angewendet. Die VM besitzt immer noch die alte Konfiguration.

5. Fordern Sie ein geplantes Update an. Beispiel:

```
 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   Weitere Informationen zu geplanten Updates finden Sie unter Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema.

   > **Hinweis:**
   >
   > Jegliches ausstehende Provisioningschema-Update wird ebenfalls angewendet.

6. Starten Sie die VM neu. Beispiel:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Überprüfen Sie die Konfigurationsversion. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Überprüfen Sie den Wert der Eigenschaft `ProvVMConfigurationVersion`. Das Update wurde angewendet. Die VM hat jetzt die neue Konfiguration.

8. Um weitere Konfigurationsupdates auf der VM anzuwenden, schalten Sie die VM aus und wiederholen Sie die Schritte.

### Aktualisierte Eigenschaften auf einer VM nach dem Aktualisieren des Maschinenkatalogs beibehalten

Gehen Sie wie folgt vor, um die aktualisierten Eigenschaften einer VM beizubehalten:

1. Schalten Sie die VM aus, auf der Sie die Updates anwenden möchten.
2. Aktualisieren Sie den Maschinenkatalog. Wenn Sie beispielsweise die VM-Größe (`ServiceOffering`) und den Speichertyp (`StorageType`) ändern möchten, führen Sie Folgendes aus:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. Rufen Sie die Konfigurationsdetails des Maschinenkatalogs ab. Beispiel:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

   `ProvisioningSchemeVersion` wird jetzt um eins erhöht. Die VM-Größe und der Speichertyp werden ebenfalls aktualisiert.

4. Aktualisieren Sie die Eigenschaften der VM. Stellen Sie der VM beispielsweise ein Maschinenprofil bereit.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```

   > **Hinweis:**
   >
   > Die Maschinenprofileingabe hat ein Tag und eine andere VM-Größe (`ServiceOffering`).

5. Rufen Sie die Liste der Eigenschaften ab, die die VM nach dem Zusammenführen der Konfigurationsupdates auf der VM mit den Maschinenkatalog-Updates haben wird. Beispiel:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   > **Hinweis:**
   >
   > Alle Updates der VM setzen die Updates am Maschinenkatalog außer Kraft.

6. Fordern Sie ein geplantes Update für die VM an. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Starten Sie die VM neu. Beispiel:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

Die VM behält ihre aktualisierte, aus dem Maschinenprofil abgeleitete Größe bei. Die im Maschinenprofil angegebenen Tag-Werte werden ebenfalls auf die VM angewendet. Der Speichertyp wird jedoch aus dem neuesten Provisioningschema abgeleitet.

8. Rufen Sie die Konfigurationsversion der VM ab. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Für `ProvisioningSchemeVersion` und `ProvVMConfigurationVersion` wird jetzt die neueste Version angegeben.

#### Auf eine VM angewendete Konfigurationsupdates rückgängig machen

1. Nachdem Sie die Updates auf eine VM angewendet haben, schalten Sie die VM aus.
2. Führen Sie den folgenden Befehl aus, um die Updates zu entfernen, die auf die VM angewendet wurden. Beispiel:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. Fordern Sie ein geplantes Update für die VM an. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Starten Sie die VM neu. Beispiel:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Überprüfen Sie die Konfigurationsversion der VM. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Der Wert für `ProvVMConfigurationVersion` gibt jetzt die Konfigurationsversion des Maschinenkatalogs wieder.

### Datenträgerverschlüsselung ändern

Sie können die Datenträgerverschlüsselung in Azure-Virtualisierungsumgebungen ändern und wie folgt vorgehen:

- Erstellen Sie mithilfe des Befehls `New-ProvScheme` einen MCS-Maschinenkatalog mit einem Datenträgerverschlüsselungssatz (DES), der sich vom Masterimage-DES unterscheidet. Beispiel:

```
$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
<!--NeedCopy-->
```

- Ändern Sie den Datenträgerverschlüsselungstyp von einem DES-Schlüssel zu einem anderen DES-Schlüssel eines vorhandenen MCS-Maschinenkatalogs und vorhandener VMs mithilfe der Befehle `Set-ProvScheme` und `Set-ProvVMUpdateTimeWindow`. Nachdem Sie die VMs neu gestartet haben, können Sie den aktualisierten DES-Schlüssel anzeigen. Beispiel:

```
$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/providers/Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

```
<!--NeedCopy-->
```

- Aktualisieren Sie einen MCS-Maschinenkatalog und eine VM, für die zuvor nicht CMEK aktiviert war, für Verschlüsselung (DES) mit einem vom Kunden verwalteten Verschlüsselungsschlüssel (CMEK), Datenträgerverschlüsselung auf dem Host oder doppelter Verschlüsselung mit den Befehlen `Set-ProvScheme` und `Set-ProvVMUpdateTimeWindow`. Informationen zu den verschiedenen Verschlüsselungstypen finden Sie unter Azure-serverseitige Verschlüsselung, Azure-Datenträgerverschlüsselung auf dem Host und Doppelte Verschlüsselung auf verwalteten Datenträgern.
- Aktualisieren Sie einen vorhandenen MCS-Maschinenkatalog und virtuelle Maschinen, die zuvor mit den Befehlen `Set-ProvScheme` und `Set-ProvVMUpdateTimeWindow` verschlüsselt wurden, so dass sie unverschlüsselt sind. Beispiel:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Aktivieren Sie die Datenträgerverschlüsselung mit privatem Endpunkt (einem MCS-Maschinenkatalog, der eine mit `ProxyHypervisorTrafficThroughConnector` aktivierte Hostverbindung verwendet hat). Weitere Informationen zu `ProxyHypervisorTrafficThroughConnector` finden Sie unter Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen. Informationen zum Aktivieren der Datenträgerverschlüsselung mit privaten Endpunkten finden Sie unter Datenträgerverschlüsselung mit privatem Endpunkt aktivieren.

#### Datenträgerverschlüsselung mit privatem Endpunkt aktivieren

Gemäß der Azure-Beschränkung können Sie derzeit keine serverseitige Verschlüsselung mit vom Kunden verwalteten Schlüsseln für private Endpunkte verwenden. Sie können jedoch einen vorhandenen MCS-Maschinenkatalog und virtuelle Maschinen mit privaten Endpunkten aktualisieren, um sie mit dem DES-Schlüssel zu verschlüsseln.

**Vorhandenen Maschinenkatalog mit privaten Endpunkten aktualisieren** Die detaillierten Schritte zum Aktualisieren eines vorhandenen Maschinenkatalogs mit privaten Endpunkten lauten wie folgt:

1. Erstellen Sie einen Katalog ohne Datenträgerverschlüsselung durch `ProxyHypervisorTrafficThroug`. Weitere Informationen zu `ProxyHypervisorTrafficThroughConnector` finden Sie unter Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen.
2. Führen Sie `Set-ProvScheme` aus, um den Katalog mit `DiskEncryptionSetId` zu aktualisieren.

   > **Hinweis:**
   >
   > `DiskEcryptionSetId` kann über `CustomProperties` oder `MachineProfile` konfiguriert werden. Wenn sie sowohl in `CustomProperties` als auch in `MachineProfile` definiert ist, werden die in `CustomProperties` definierten Eigenschaften angewendet.

   Beispiel bei der Verwendung von `CustomProperties`:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1"/>
   </CustomProperties>'
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

   Beispiel bei Verwendung von MachineProfile: Verwenden Sie eine VM, bei der die Datenträgerverschlüsselung aktiviert ist, oder eine Vorlagenspezifikation mit Datenträgerverschlüsselungseinstellungen:

   ```
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
       folder\testrg.resourcegroup\new-template.vm"
   <!--NeedCopy-->
   ```

   Alternativ können Sie ein Maschinenprofil über die Benutzeroberfläche für die vollständige Konfiguration aktualisieren.
3. Führen Sie `Set-ProvVMUpdateTimeWindow` aus, um vorhandene Katalog-VMs zu aktualisieren. Beispiel:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
       VMName azu01, azu02 -StartsNow -DurationInMinutes -1
   <!--NeedCopy-->
   ```
4. Nachdem Sie die VMs neu gestartet haben, können Sie die aktualisierte Datenträgerverschlüsselung auf den Datenträgern der VM im Azure-Portal anzeigen.

5. Führen Sie `Set-ProvScheme` aus, um die Datenträgerverschlüsselung aufzuheben, bevor Sie neue Katalog-VMs hinzufügen.

   > **Hinweis:**
   >
   > Dieser Schritt ist erforderlich, da Sie einen Katalog mit privaten Endpunkten aktualisieren. Wenn Sie diesen Schritt nicht ausführen, erhalten Sie beim Versuch, neue virtuelle Maschinen zum Katalog hinzuzufügen, eine Fehlermeldung.

   Beispiel:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="" />
   </CustomProperties>'
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

6. Fügen Sie neue VMs zum Katalog hinzu.

**Einzelne Katalog-VMs aktualisieren** Die detaillierten Schritte zum Aktualisieren einzelner Katalog-VMs lauten wie folgt:

1. Erstellen Sie einen Katalog ohne Datenträgerverschlüsselung durch `ProxyHypervisorTrafficThroug`. Weitere Informationen zu `ProxyHypervisorTrafficThroughConnector` finden Sie unter Sichere Umgebung für von Azure verwalteten Netzwerkverkehr erstellen.
2. Führen Sie `Set-ProvVM` aus, um die Katalog-VM mit `DiskEncryptionSetId` zu aktualisieren.

   > **Hinweis:**
   >
   > Die `DiskEcryptionSetId` kann entweder über `CustomProperties` oder über `MachineProfile` konfiguriert werden.

   Beispiel bei der Verwendung von `CustomProperties`:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1" />
   </CustomProperties>'
   ```

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    CustomProperties $customProperties
<!--NeedCopy-->
```

Beispiel für die Verwendung von MachineProfile:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
<!--NeedCopy-->
```

3. Führen Sie `Set-ProvVMUpdateTimeWindow` aus, um vorhandene Katalog-VMs zu aktualisieren. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Nachdem Sie die VMs neu gestartet haben, können Sie die aktualisierte Datenträgerverschlüsselung auf den Datenträgern der virtuellen Maschinen im Azure-Portal anzeigen.
5. Fügen Sie neue VMs zum Katalog hinzu.

### Abrufen von Informationen für Azure-VMs, Snapshots, Betriebssystemdatenträger und Katalogimagedefinition

Sie können Informationen für eine Azure-VM anzeigen, einschließlich Betriebssystemdatenträger und -typ, Snapshot und Katalogimagedefinition. Diese Informationen werden für Ressourcen im Masterimage angezeigt, wenn ein Maschinenkatalog zugewiesen wird. Verwenden Sie diese Funktion, um entweder ein Linux- oder ein Windows-Image anzuzeigen und auszuwählen. Eine PowerShell-Eigenschaft, `TemplateIsWindowsTemplate`, wurde dem Parameter `AdditionDatafield` hinzugefügt. Dieses Feld enthält Azure-spezifische Informationen: VM-Typ, Betriebssystemdatenträger, Informationen zum Katalogimage und Informationen zum Betriebssystemtyp. Die Einstellung von `TemplateIsWindowsTemplate` auf **True** zeigt an, dass der Betriebssystemtyp Windows ist; die Einstellung von `TemplateIsWindowsTemplate` auf **False** zeigt an, dass der Betriebssystemtyp Linux ist.

> **Tipp:**
>
> Die von der PowerShell-Eigenschaft `TemplateIsWindowsTemplate` angezeigten Informationen werden von der Azure-API abgeleitet. Gelegentlich kann dieses Feld leer sein. Beispiel: Ein Snapshot von einem Datenträger enthält das Feld `TemplateIsWindowsTemplate` nicht, da der Betriebssystemtyp nicht aus einem Snapshot abgerufen werden kann.

Beispiel: Legen Sie den `AdditionData`-Parameter der Azure-VM für den Betriebssystemtyp Windows mit PowerShell auf **True** fest:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

### Abrufen des Regionsnamen für Azure-VMs, verwaltete Datenträger, Snapshots, Azure VHD und ARM-Vorlagen

Sie können Angaben zum Regionsnamen für Azure-VMs, verwaltete Datenträger, Snapshots, Azure VHD und ARM-Vorlagen anzeigen. Diese Informationen werden für Ressourcen im Masterimage angezeigt, wenn ein Maschinenkatalog zugewiesen wird. Die PowerShell-Eigenschaft `RegionName` zeigt den Regionsnamen an, wenn Sie den PowerShell-Befehl mit dem Parameter `AdditionalData` ausführen.

Verwenden Sie beispielsweise den folgenden PowerShell-Befehl, um VM-Informationen in Azure abzurufen.

```
PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).
    AdditionalData
Key Value
HardDiskSizeGB 127
ResourceGroupName HU-DEV-TESTING-RG
RegionName East US
TemplateIsWindowsTemplate True
LicenseType
ServiceOfferingDescription Standard_B2ms
ServiceOfferingMemory 8192
ServiceOfferingCores 2
SupportedMachineGenerations Gen1,Gen2
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SecurityType
SecureBootEnabled
VTpmEnabled
<!--NeedCopy-->
```

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen auf der Azure-Plattform hinzufügt. Die Tags werden in der Tabelle als in der Form "Schlüssel": "Wert"dargestellt.

| Ressourcenname | Tag |
|---|---|
| ID-Datenträger | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Image | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Netzwerkkarte | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| OS-Datenträger | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Vorbereitungs-VM | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Veröffentlichter Snapshot | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Ressourcengruppe | "CitrixResource": "Internal" CitrixSchemaVersion: 2.0 "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Speicherkonto | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| VM im Katalog | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| WBC-Datenträger | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

“CitrixResource”: “Internal”

> **Hinweis:**
>
> Eine VM ist im Citrix-Bestand nicht sichtbar, wenn ein **CitrixResource**-Tag hinzugefügt wird, um sie als eine von MCS erstellte Ressource zu identifizieren. Sie können das Tag entfernen oder umbenennen, um sie sichtbar zu machen.

### Tags entfernen

Wenn Sie einen Katalog oder eine VM erstellen, werden Tags für folgende Ressourcen erstellt:

- Ressourcengruppe
- Virtuelle Maschine
- OS-Datenträger
- Identitätsdatenträger
- Netzwerkschnittstelle
- Speicherkonto

Sie können VMs und Maschinenkataloge aus der Citrix Datenbank sowie Tags entfernen. Optionen:

- `Remove-ProvVM` mit dem Parameter `ForgetVM` zum Entfernen von VMs und Tags aus einer einzelnen VM oder einer Liste von VMs aus einem Maschinenkatalog.
- `Remove-ProvScheme` mit Parameter `ForgetVM` zum Entfernen eines Maschinenkatalogs aus der Citrix Datenbank und von Tags aus einem gesamten Maschinenkatalog.

Dieses Feature ist nur für persistente VMs verfügbar.

Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie `Remove-ProvVM` aus, um VMs aus der Citrix Datenbank und Tags aus VMs zu löschen.
   Beispiel:

   ```
   1 Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -
       VMName “vmname” -ForgetVM
   2 <!--NeedCopy-->
   ```

4. Führen Sie `Remove-ProvScheme` aus, um den Maschinenkatalog aus der Citrix Datenbank und Tags aus den Maschinenkatalogen zu löschen. Beispiel:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
<!--NeedCopy-->
```

> **Hinweis:**
>
> Bei Verwendung des Parameters `ForgetVM` in `Remove-ProvScheme` löscht MCS alle Snapshots einschließlich des Basisdatenträger-Snapshots, wenn das Provisioningschema in der Bring Your Own-Ressourcengruppe (BYORG) oder der von Citrix verwalteten Ressourcengruppe vorliegt.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft Azure
- Maschinenkataloge erstellen
- Microsoft Azure-Katalog erstellen
- Maschinenkataloge verwalten

## Microsoft System Center Virtual Machine Manager-Katalog verwalten

January 25, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft System Center Virtual Machine Manager (VMM)-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie müssen einen VMM-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe Microsoft System Center Virtual Machine Manager-Katalog erstellen.

### Identifizieren der von MCS erstellten Ressourcen

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen auf der SCVMM-Plattform hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
| --- | --- |
| Vorbereitungs-VM | Tagzeichenfolge: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Benutzerdefinierte Eigenschaft: “XdConfig:” XdProvisioned=True” |
| VM im Katalog | Tagzeichenfolge: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Benutzerdefinierte Eigenschaft: “XdConfig:” XdProvisioned=True” |

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft System Center Virtual Machine Manager
- Maschinenkataloge erstellen
- Microsoft System Center Virtual Machine Manager-Katalog erstellen
- Maschinenkataloge verwalten

## VMware-Katalog verwalten

June 12, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf VMware-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie müssen einen VMware-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe VMware-Katalog erstellen.

### Ordner-ID eines Maschinenkatalogs aktualisieren

Sie können die Ordner-ID eines MCS-Maschinenkatalogs aktualisieren, indem Sie `FolderId` in den benutzerdefinierten Eigenschaften des Befehls `Set-ProvScheme` angeben. Die nach dem Aktualisieren der Ordner-ID erstellten VMs werden unter dieser neuen Ordner-ID erstellt. Wenn diese Eigenschaft nicht in `CustomProperties` angegeben ist, werden VMs in dem Ordner erstellt, in dem das Masterimage ist.

Führen Sie folgende Schritte aus, um die Ordner-ID eines Maschinenkatalogs zu aktualisieren.

1. Öffnen Sie einen Webbrowser und geben Sie die URL für den **vSphere Web Client** ein.
2. Geben Sie die Anmeldeinformationen ein und klicken Sie auf **Login**.
3. Erstellen Sie einen VM-Platzierungsordner in **vSphere Web Client**.
4. Öffnen Sie ein PowerShell-Fenster.
5. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
6. Geben Sie `FolderID` in den `CustomProperties` von `Set-ProvScheme` an. In diesem Beispiel ist der Wert für die Ordner-ID `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
     f630687372" -CustomProperties "<CustomProperties xmlns=""http
     ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
     http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
     ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
     CustomProperties>"
2 <!--NeedCopy-->
```

7. Fügen Sie dem Maschinenkatalog mit Studio eine VM hinzu.
8. Überprüfen Sie die neue VM im vSphere Web Client. Die neue VM wird unter dem neuen Ordner erstellt.

#### Ordner-ID mit PowerShell-Befehlen finden

Verwenden Sie den Powershell-Befehl `Get-HypConfigurationDataForItem`, um die Ordner-ID für einen vorhandenen Ordner in einem VMware Hypervisor zu ermitteln.

Erstellen Sie eine Hostingverbindung und eine Ressourcengruppe für einen VMware Hypervisor. Führen Sie dann die folgenden Schritte aus, um die Ordner-ID eines Ordners auf diesem Hypervisor zu ermitteln.

1. Ermitteln Sie den `XDHyp`-Pfad zum Stammverzeichnis des VM-Ordnerbaums. Beispiel:

```
1 XDHyp:\Connections\VMwareConn\Datacenter.datacenter
2 <!--NeedCopy-->
```

2. Verwenden Sie `Get-HypConfigurationDataForItem`, um die Baumstruktur abzurufen. Beispiel:

```
1 Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\
     VMwareConn\Datacenter.datacenter
2 <!--NeedCopy-->
```

3. Führen Sie den folgenden Befehl aus, um die Ordner-ID aus der XML-Ausgabe zu identifizieren. Suchen Sie in diesem Beispiel in der XML-Ausgabe nach der Ordner-ID von `ExampleFolder`.

```
$result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:\
   Connections\VMwareConn\Datacenter.datacenter
$result.VmPlacementFolder
<!--NeedCopy-->
```

**XML-Ausgabe:**

```
<?xml version="1.0" encoding="utf-16"?>
<CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Name>vm</Name>
<Id>group-v4</Id>
<SubFolder>
<CtxVmPlacementFolder>
  <Name>vCLS</Name>
  <Id>group-v75</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>MyOtherFolder</Name>
  <Id>group-v1110</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>ExampleFolder</Name>
  <Id>group-v4658</Id>
  <SubFolder />
</CtxVmPlacementFolder>
</SubFolder>
</CtxVmPlacementFolder>
<!--NeedCopy-->
```

#### Suchen der Ordner-ID in vSphere

Nutzen Sie den MOB auf einem beliebigen ESXi- oder vCenter Server-System zum Erfassen der Ordner-ID der VMs.

Der Browser für verwaltete Objekte (MOB), ist eine webbasierte Serveranwendung, die in alle ESX/ESXi- und vCenter Server-Systeme integriert ist. Mit diesem vSphere-Dienstprogramm können Sie detaillierte Informationen zu Objekten wie VMs, Datenspeichern und Ressourcenpools anzeigen.

1. Öffnen Sie einen Webbrowser und geben Sie `http://x.x.x.x/mob` ein, wobei x.x.x.x die IP-Adresse des vCenter Server oder ESX/ESXi-Hosts ist. Beispiel: https://10.60.4.70/mob.
2. Klicken Sie auf der **Startseite** von MOB auf den Wert der Eigenschaft **content**.
3. Klicken Sie auf den Wert von **rootFolder**.

4. Klicken Sie auf den Wert von **childEntity**.
5. Klicken Sie auf den Wert von **vmFolder**.
6. Sie finden die Ordner-ID im Wert von **childEntity**.

### Speichermigration von VMs

Sie können den Datenträgerspeicher vorhandener VMs von einem alten Speicher in einen neuen Speicher verschieben. Während der Migration behält MCS die VM-Funktionen wie Energieverwaltung, Zurücksetzen des OS-Datenträgers usw. bei. Sie können dem Maschinenkatalog auch mithilfe des neuen Datenträgerspeichers neue VMs hinzufügen. Verwenden Sie dazu den PowerShell-Befehl `Move-ProvVMDisk`.

Derzeit können Sie nur vollständige Klone persistenter VMs migrieren.

Der neue Speicher muss die folgenden Bedingungen erfüllen:

- Er muss sich in demselben Cluster des alten Speichers befinden.
- Der Host, auf dem die VM läuft, muss Zugriff auf den alten und den neuen Datenspeicher haben.

Sie können die folgenden Aufgaben erledigen:

- Datenträgerspeicher migrieren
- Alten Speicher verwerfen

#### Datenträgerspeicher migrieren

So migrieren Sie den Datenträgerspeicher:

1. Fügen Sie einer vorhandenen Hostingeinheit einen neuen Speicher hinzu. Ändern Sie den alten Speicher auf **Ersetzt**. Sie können hierfür die Benutzeroberfläche "Vollständige Konfiguration" oder PowerShell-Befehle verwenden.

    - Wenn Sie die Benutzeroberfläche "Vollständige Konfiguration"verwenden, finden Sie weitere Informationen unter Speicher bearbeiten.
    - Mit PowerShell-Befehlen:
        - Führen Sie `Add-Hyphostingunitstorage` aus, um den neuen Speicher zur vorhandenen Hostingeinheit hinzuzufügen.
        - Führen Sie `Set-Hyphostingunitstorage` mit **Superseded** auf "True"aus, um das Erstellen neuer virtueller Maschinen im alten Speicher zu deaktivieren.

2. Schalten Sie die virtuellen Maschinen aus und den **Wartungsmodus** ein.
3. Verschieben Sie den Datenträgerspeicher der VMs in den neuen Speicher und aktualisieren Sie die Speicherinformationen. Beispiel:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

4. Rufen Sie die Aufgaben-ID der Migration ab. Beispiel:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

5. Überprüfen Sie den Status der Migration.

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: stellt die Liste der VMs mit erfolgreicher Datenträgermigration bereit, einschließlich der VMs, die bereits auf den neuen Speicher migriert wurden.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines` : stellt die Liste der virtuellen Maschinen bereit, bei denen die Migration fehlgeschlagen ist.
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: stellt die Liste der VMs bereit, deren Migration noch nicht gestartet wurde.
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: stellt die aktualisierten VM-Eigenschaften nach der Migration bereit. Überprüfen Sie die Eigenschaften wie `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` und `LastBootTime`.

Nach der Migration der Datenträger der von MCS erstellten VMs mit Snapshot wird möglicherweise die Warnung **Konsolidierung ist erforderlich im vSphere Client** angezeigt. So konsolidieren Sie und vermeiden Datenverlust:

1. Erstellen Sie ein VMware-VM-Backup. Übertragen Sie beispielsweise alle VM-Dateien in einen anderen Ordner auf einem Datenspeicher.
2. Wenn die Warnung angezeigt wird, klicken Sie auf **Konsolidieren** und dann auf **OK**, um die Konsolidierung zu bestätigen.

#### Alten Speicher verwerfen

So verwerfen Sie den alten Speicher nach der Datenträgermigration der virtuellen Maschinen:

1. Rufen Sie die Informationen über die Basisdatenträger und die Anzahl der Maschine in jedem Datenträgerspeicher der Hostingeinheit ab. Beispiel:

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
    xxxxx
```

```
$result
$result.ProvResourceInStorage | Format-List -Property *
<!--NeedCopy-->
```

Nach einer erfolgreichen Migration entfernt MCS automatisch den veralteten Basisdatenträger und im alten Speicher befinden sich keine Maschinen mehr. Stellen Sie daher nach dem Ausführen des Befehls sicher, dass sich im alten Speicher keine Maschinen und kein Basisdatenträger befinden.

2. Führen Sie `Remove-Hyphostingunitstorage` aus, um den alten Speicher vollständig von der Hostingeinheit zu entfernen. Sie können auch die Benutzeroberfläche "Vollständige Konfiguration"verwenden, um den alten Speicher zu entfernen.

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen auf der VMware-Plattform hinzufügt. Die Tags werden in der Tabelle als in der Form "Schlüssel": "Wert"dargestellt.

| Ressourcenname | Tag |
|---|---|
| Vorbereitungs-VM | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |
| VM im Katalog | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu VMware
- Maschinenkataloge erstellen
- VMware-Katalog erstellen
- Maschinenkataloge verwalten

## XenServer-Katalog verwalten

January 25, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf XenServer-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie müssen einen XenServer-Katalog erstellt haben, bevor Sie ihn verwalten können. Weitere Informationen finden Sie unter XenServer-Katalog erstellen.

### Identifizieren der von MCS erstellten Ressourcen

Wenn die Maschinenerstellungsdienste (MCS) Ressourcen wie Datenträger generieren, weisen sie ein ProvisioningScheme-ID-Tag zu, um diese Ressourcen besser nutzen zu können.

Tags sind für Administratoren hilfreich, da sie damit die Ressourcen besser verwalten und organisieren können. Wenn beispielsweise Ressourcen, wie z. B. ungenutzte Datenträger, mit Tags versehen sind, können Administratoren leicht erkennen, wo die Ressource erstellt wurde, wodurch der Bereinigungsprozess effizient wird.

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen auf der XenServer-Plattform hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
|---|---|
| Kopie des Datenträgers in jedem Netzwerk oder lokalen Speicher (nur on-premises) | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| ID-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| OS-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Vorbereitungs-VM | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| VM im Katalog | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| WBC-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

### Informationen zum Provisioningschema abrufen

Führen Sie die folgenden PowerShell-Befehle aus, um detaillierte Informationen zum Provisioningschema abzurufen. Ersetzen Sie xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx durch die tatsächliche Provisioningschema-ID:

1. Platzhalter-ID durch die tatsächliche Provisioningschema-ID ersetzen

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Rufen Sie detaillierte Informationen zum Provisioningschema ab:

```
Get-ProvisioningScheme -Id $provisioningSchemeId
<!--NeedCopy-->
```

### Liste der von MCS erstellten Ressourcen abrufen

Führen Sie die folgenden Befehle aus, um eine umfassende Liste der von MCS erstellten Ressourcen abzurufen.

1. Ersetzen Sie die Platzhalter-ID durch Ihre tatsächliche Provisioningschema-ID.

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Ruft die gesamte Liste der von MCS erstellten Ressourcen ab.

```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
   ConvertTo-JSON -Depth 6
<!--NeedCopy-->
```

   Nach dem Ausführen erhalten Sie die folgende Ausgabe:

   - Name und ID des Bereitstellungsschemas.
   - Liste der Provisioningimageversionen innerhalb des Provisioningschemas. Jeder Eintrag beinhaltet:
     - Name und ID des Images.
     - Datenträger-ID und Speicher-ID des Datenträgers.
   - Liste der bereitstellenden VMs. Jeder Eintrag beinhaltet:
     - Betriebssystemdatenträger-ID und übergeordnete Datenträger-ID des Betriebssystemdatenträgers.
     - Speicher-ID des Betriebssystemdatenträgers.
     - Identitätsdatenträger und seine Speicher-ID.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu XenServer
- Maschinenkataloge erstellen

- XenServer-Katalog erstellen
- Maschinenkataloge verwalten

## Energieverwaltung

December 1, 2023

Mit Citrix DaaS ist die Energieverwaltung per MCS-bereitgestellte VMs über verschiedene unterstützte Hypervisoren und Cloud-Dienste hinweg möglich. Die Energieverwaltung bietet:

- Optimale Benutzererfahrung
- Kostenmanagement und Energieeinsparung

Die verfügbaren Energieaktionen:

- Starten
- Herunterfahren
- Neustarten
- Anhalten
- Fortsetzen
- Neustart erzwingen
- Herunterfahren erzwingen

> **Hinweis:**
>
> - Bei einer nicht persistenten VM führt Abschalten und Wiedereinschalten bzw. Neustarten zum Zurücksetzen des Betriebssystemdatenträgers.
> - Energieaktionen und deren Verhalten variieren je nach Hypervisor und Cloudservice.

In diesem Artikel werden die wichtigsten Energieverwaltungsfunktionen im Zusammenhang mit bestimmten unterstützten Hypervisoren behandelt.

- Energieverwaltung von AWS-VMs
- Energieverwaltung von Azure-VMs

## Energieverwaltung für AWS-VMs

May 17, 2024

Informationen zu den erforderlichen Berechtigungen finden Sie unter Informationen zu AWS-Berechtigungen.

### Ruhezustand von Instanzen

Beim Ruhezustand wird der In-Memory-Status der Instanz samt privater und elastischer IP-Adressen gespeichert, sodass Benutzer genau dort weitermachen kann, wo sie aufgehört haben.

Wenn eine Instanz in den Ruhezustand versetzt wird, schreibt sie ihren In-Memory-Status in eine Datei auf dem EBS-Stammvolume und fährt dann herunter. Ein Amazon EBS-Volume ist ein robuster Blockspeicher, den Sie an Ihre Instanzen anschließen können. Nachdem Sie ein Volume an eine Instanz angeschlossen haben, können Sie es wie eine physische Festplatte verwenden. Verschlüsseln Sie das EBS-Stammvolume der Instanz. Die Verschlüsselung gewährleistet einen angemessenen Schutz vertraulicher Daten, wenn sie aus dem Speicher in das EBS-Volume kopiert werden. Informationen zur EBS-Verschlüsselung finden Sie unter Amazon EBS encryption.

Es gelten folgende Einschränkungen für den unterstützten Ruhezustand von Instanzen:

- Instanzenspeicher (RAM) bis maximal 150 GB unterstützt
- UEFI-Startmodus wird nicht unterstützt
- Es werden nur Allzweck-SSD und Bereitgestellte IOPS-SSD als EBS-Volumetypen unterstützt.

#### VMs mit unterstütztem Ruhezustand erstellen

Erstellen von VMs mit unterstütztem Ruhezustand:

1. Erstellen Sie eine Hostverbindung. Siehe Verbindung zu AWS.
2. Starten Sie eine Instanz mit verschlüsseltem EBS-Stamm und aktivierter Eigenschaft **Stop-Hibernate**. Weitere Informationen:
   - Lebenszyklus der Instanz
   - Amazon EBS-Verschlüsselung
   - Voraussetzungen für den Ruhezustand
   - Ruhezustand für eine Instanz aktivieren
   - On-Demand-Instance oder Spot-Instance in den Ruhezustand versetzen
3. Verwenden Sie diese Instanz als Masterimage, um ein AMI zu erstellen.
4. Bereiten Sie das Masterimage vor:
   a) Installieren Sie einen VDA auf dem Masterimage. Citrix empfiehlt die Installation der neuesten Version, damit die neuesten Features verfügbar sind. Wird kein VDA auf dem Masterimage installiert, schlägt die Katalogerstellung fehl. Weitere Informationen zur Installation eines VDA finden Sie unter Installieren von VDAs.
   b) Fügen Sie das Masterimage der Domäne hinzu, zu der die Anwendungen und Desktops gehören. Vergewissern Sie sich, dass das Masterimage auf dem Host verfügbar ist, auf dem die Maschinen erstellt werden.

5. Erstellen Sie ein AMI aus dieser Instanz. Informationen zum Erstellen eines AMI aus einer Instanz finden Sie unter Create an AMI from an Amazon EC2 Instance.
6. Erstellen Sie mit dem Befehl `New-ProvScheme` einen Maschinenkatalog. Legen Sie die benutzerdefinierte Eigenschaft `AwsCaptureInstanceProperties` auf **True** fest. Informationen zum Aktivieren von AWS-Instanzeigenschaften in der Benutzeroberfläche "Vollständige Konfiguration"finden Sie unter Anwenden von AWS-Instanzeigenschaften und Tagging von Betriebsressourcen in der Benutzeroberfläche "Vollständige Konfiguration".

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

   Hinweise zum Erstellen eines Maschinenkatalogs mithilfe von PowerShell-Befehlen finden Sie unter https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

VMs, die in den Ruhezustand versetzt werden können, werden erstellt, wenn Folgendes gilt:

- Sie wählen ein AMI aus, das aus einem Masterimage mit aktivierter Eigenschaft **Stop-Hibernate** erstellt wurde.
- Die Master-VM ist domänengebunden und hat einen installierten VDA.
- Sie wählen die richtige VM-Größe (Dienstangebot), die den Ruhezustand bewältigen kann.

Der Befehl **New-ProvScheme** schlägt fehl und es wird eine Fehlermeldung angezeigt, wenn Folgendes gilt:

- Die Ruhezustandsfunktion ist für die Master-VM aktiviert, das Dienstangebot kann den Ruhezustand jedoch nicht verarbeiten.
- Die Master-VM ist nicht domänengebunden und hat keinen installierten VDA.

#### Ruhezustandsstatus von Dienstangeboten und AMI

Führen Sie die folgenden Befehle aus, um den Ruhezustandsstatus von Dienstangeboten und AMI (Vorlagen) abzurufen:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

#### Dienstangebot eines bestehenden Provisioningschemas mit unterstütztem Ruhezustand aktivieren

1. Führen Sie den Befehl `Set-ProvScheme` aus. Zum Beispiel:

```
1 Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
     String>
2 <!--NeedCopy-->
```

Das System zeigt eine Ausnahmemeldung an, wenn das Dienstangebot nicht kompatibel ist.

#### Maschinenkatalog mit Unterstützung für den Ruhezustand erstellen

Beim Erstellen von Maschinenkatalogen können Sie ein Maschinenprofil verwenden, das den Ruhezustand unterstützt.

1. Folgen Sie im Assistenten zur Katalogerstellung den Anweisungen bis zur Maschinenprofilauswahl.
2. Klicken Sie auf der Seite **Maschinenvorlage** auf **Wählen Sie ein Maschinenprofil** und wählen Sie ein Maschinenprofil aus.
3. Klicken Sie auf der Seite **Virtuelle Maschine** auf das Symbol **Bearbeiten** und wählen Sie eine VM.

   > **Hinweis:**
   >
   > Wenn für das Maschinenprofil der Ruhezustand aktiviert ist, zeigt das System nur die VMs an, die in den Ruhezustand versetzt werden können.

4. Folgen Sie den angezeigten Anweisungen, um alle Einstellungen vorzunehmen. Auf der Seite **Zusammenfassung** wird der Ruhezustandstatus des Katalogs angezeigt.

   > **Hinweis:**
   >
   > Wenn Sie beim Bearbeiten eines Maschinenkatalogs das Maschinenprofil in eines ändern, das den Ruhezustand unterstützt, werden Sie aufgefordert, Ihre VMs entsprechend neu zu konfigurieren.

#### Update eines Maschinenkatalogs, der den Ruhezustand unterstützt

Wenn Sie versuchen, einen vorhandenen Maschinenkatalog durch einen Maschinenkatalog zu ersetzen, der den Ruhezustand nicht unterstützt, schlägt das Update fehl und es wird eine Fehlermeldung angezeigt.

#### Energieverwaltung von VMs im Ruhezustand

Sie können die folgenden Energieverwaltungsvorgänge auf VMs im Ruhezustand ausführen:

1. Sie können eine laufende VM anhalten.
2. Sie können eine angehaltene VM fortsetzen.
3. Sie können eine angehaltene VM neu starten.

Zur Anzeige der Energieverwaltungsoptionen klicken Sie in der Benutzeroberfläche **Verwalten > Vollständige Konfiguration** mit der rechten Maustaste auf die im Ruhezustand befindlichen VMs.

Sie können auch für jede VM je nach gewählter Operation den Energiezustand als **Anhalten** bzw. **Angehalten** anzeigen.

## Energieverwaltung für Azure-VMs

June 12, 2024

Informationen zu den erforderlichen Berechtigungen finden Sie unter Erforderliche Azure-Berechtigungen.

### Bedarfsgesteuertes Provisioning in Azure

Beim bedarfsgesteuerten Provisioning in Azure werden VMs nur erstellt, wenn Citrix DaaS nach Abschluss des Provisionings eine Einschaltaktion initiiert.

Wenn Sie Maschinenkataloge mit Maschinenerstellungsdiensten (MCS) in Azure Resource Manager erstellen, bietet das bedarfsgesteuerte Provisioning in Azure folgende Vorteile:

- Geringere Speicherkosten
- Schnellere Katalogerstellung

Wenn Sie einen MCS-Katalog erstellen, werden im Azure-Portal die Netzwerksicherheitsgruppen, Netzwerkschnittstellen, Basisimages und Identitätsdatenträger in den Ressourcengruppen angezeigt.

VMs werden erst dann im Azure-Portal angezeigt, wenn Citrix DaaS eine VM-Einschaltaktion startet. Der Status der VM in der Oberfläche "Vollständige Konfiguration"ändert sich dann in **Ein**. Es gibt zwei Arten von Maschinen mit den folgenden Unterschieden:

- Bei gepoolten Maschinen sind OS-Datenträger und Zurückschreibcache nur vorhanden, wenn die VM vorhanden ist. Wenn Sie eine gepoolte Maschine in der Konsole herunterfahren, ist die VM im Azure-Portal nicht sichtbar. Wenn Sie Maschinen routinemäßig herunterfahren (z. B. außerhalb der Arbeitszeit), sparen Sie erhebliche Speicherkosten.
- Bei dedizierten Maschinen wird der Betriebssystemdatenträger beim ersten Einschalten der VM erstellt. Die virtuelle Maschine im Azure-Portal bleibt im Speicher, bis die Maschinenidentität gelöscht wird. Wenn Sie eine dedizierte Maschine in der Konsole herunterfahren, ist die VM weiterhin im Azure-Portal sichtbar.

> **Hinweis:**
>
> Die Unterstützung für Azure-Kataloge, die vor dem Feature zur bedarfsgesteuerten Bereitstellung erstellt wurden ("ältere"Kataloge), ist veraltet. Erstellen Sie daher ältere Azure-Katalog-VMs neu. Die Kataloge werden dann nach Bedarf bereitgestellt, wodurch Speicherkosten gespart werden.

### Beibehalten einer bereitgestellten virtuellen Maschine bei Energiezyklen

Wählen Sie aus, ob eine bereitgestellte virtuelle Maschine bei Energiezyklen (Neustarts) beibehalten werden soll. Verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`. Dieser Parameter unterstützt die zusätzliche Eigenschaft `PersistVm`, mit der festgelegt wird, ob eine bereitgestellte virtuelle Maschine bei Energiezyklen beibehalten werden soll. Setzen Sie die Eigenschaft `PersistVm` auf **true**, um eine virtuelle Maschine beim Ausschalten beizubehalten, oder setzen Sie die Eigenschaft auf **false**, um die virtuelle Maschine beim Ausschalten nicht beizubehalten.

> **Hinweis:**
>
> Die Eigenschaft `PersistVm` gilt nur für ein Provisioningschema mit aktivierten Eigenschaften `CleanOnBoot` und `UseWriteBackCache`. Wenn die Eigenschaft `PersistVm` für nicht persistente virtuelle Maschinen nicht festgelegt ist, werden die Maschinen nach dem Ausschalten aus der Azure-Umgebung gelöscht.

Im folgenden Beispiel ist die Eigenschaft `PersistVm` im Parameter `New-ProvScheme CustomProperties` auf **true** gesetzt:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Standard_LRS" />
```

```
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
    resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

Im folgenden Beispiel behält der Parameter `New-ProvScheme CustomProperties` den Zurückschreibcache bei, indem `PersistVM` auf **true** gesetzt wird:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
    Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    false`" /><Property xsi:type=`"StringProperty`" Name=`"
    PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
    type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
    resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
    LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
-HostingUnitName "demo"
-IdentityPoolName "NonPersistent-MCSIO-PersistVM"
-MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
    resourcegroup\demo-snapshot.snapshot"
-NetworkMapping @ {
"0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
    .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
-ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

> **Tipp:**
>
> Die Eigenschaft `PersistVm` legt fest, ob eine bereitgestellte virtuelle Maschine beibehalten werden soll. Die Eigenschaft `PersistOsdisk` legt fest, ob der Betriebssystemdatenträger beibehalten werden soll. Um eine bereitgestellte virtuelle Maschine beizubehalten, müssen Sie zuerst den Betriebssystemdatenträger beibehalten. Sie können den Betriebssystemdaten-

> träger nur löschen, wenn Sie zuvor die virtuelle Maschine löschen. Sie können die Eigenschaft `PersistOsdisk` verwenden, ohne den Parameter `PersistVm` festzulegen.

### Einschaltverhalten beim Fehlschlagen der Änderung des Speichertyps anpassen

Beim Einschalten kann der Speichertyp eines verwalteten Datenträgers aufgrund eines Fehlers in Azure möglicherweise nicht in den gewünschten Typ geändert werden. In diesen Szenarien würde die VM ausgeschaltet bleiben, und Sie würden eine Fehlermeldung erhalten. Sie können die VM dann entweder einschalten (auch wenn der Speicher nicht auf den konfigurierten Typ wiederhergestellt werden kann) oder die VM ausgeschaltet lassen.

- Wenn Sie die benutzerdefinierte Eigenschaft `FailSafeStorageType` als **true** konfigurieren (Standardeinstellung) oder sie in den Befehlen `New-ProvScheme` oder `Set-ProvScheme` nicht angeben:
  - Beim Einschalten wird die VM mit dem falschen Speichertyp eingeschaltet.
  - Beim Herunterfahren bleibt die VM mit dem falschen Speichertyp ausgeschaltet.
- Wenn Sie die benutzerdefinierte Eigenschaft `FailSafeStorageType` in den Befehlen `New-ProvScheme` oder `Set-ProvScheme` als **falsch** konfigurieren:
  - Beim Einschalten bleibt die VM mit dem falschen Speichertyp ausgeschaltet.
  - Beim Herunterfahren bleibt die VM mit dem falschen Speichertyp ausgeschaltet.

So erstellen Sie einen Maschinenkatalog mit benutzerdefinierten `FailSafeStorageType`-Eigenschaften:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden.
4. Fügen Sie die benutzerdefinierte Eigenschaft in `New-ProvScheme` hinzu. Beispiel:

```
1 New-ProvScheme -HostingUnitName "Azure-Resources-1" -
     IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
     \abc.resourcegroup\def.snapshot"
3 -NetworkMapping @{
4  "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
      resourcegroup\abc-vnet.virtualprivatecloud\default.network" }
5
6 -ProvisioningSchemeName "name"
7 -ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
     serviceoffering.folder\Standard_DS2_v2.serviceoffering"
```

```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
     Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Erstellen Sie den Maschinenkatalog. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Aktualisieren Sie einen vorhandenen Maschinenkatalog, sodass er die benutzerdefinierte Eigenschaft `FailSafeStorageType` enthält. Dieses Update wirkt sich nicht auf bestehende VMs aus.

1. Aktualisieren Sie die benutzerdefinierte Eigenschaft im Befehl `Set-ProvScheme`. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
    Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
    `" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"false`" />
</CustomProperties>"
<!--NeedCopy-->
```

Führen Sie den Befehl `Request-ProvVMUpdate` aus, um die in Set-ProvScheme vorgenommene Änderung auf die vorhandenen VMs anzuwenden.

1. Führen Sie den Befehl Request-ProvVMUpdate aus. Beispiel:

```
Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
    List-Of-Vm-Names>
<!--NeedCopy-->
```

2. Starten Sie die VMs neu.

### Für den Ruhezustand geeignete VMs erstellen

In Azure-Umgebungen können Sie einen MCS-Maschinenkatalog erstellen, der den Ruhezustand unterstützt. Mit diesem Feature können Sie eine VM anhalten und dann wieder mit dem vorherigen Sta-

tus der VM verbinden, wenn sich ein Benutzer erneut anmeldet.

Die Funktion für den Ruhezustand gilt für Folgendes:

- Einzelsitzungs-OS
- Persistente und nicht persistente VMs
- Statische und zufällige (gepoolte) VDI-Desktops

Sie können dieselbe Sitzung fortsetzen, nachdem Sie eine VM in den Ruhezustand versetzt haben, unabhängig davon, ob der VDI-Desktop statisch oder zufällig ist.

In diesem Abschnitt finden Sie Folgendes:

- Voraussetzungen
- Einschränkungen
- Katalog mit für den Ruhezustand geeigneten Maschinen erstellen und verwalten
- Maschinenkatalog für bestehende Maschinen erstellen, die für den Ruhezustand geeignet sind
- Ruhezustand auf bestehenden, per MCS bereitgestellten VMs aktivieren
- Ruhezustand-Eigenschaft überprüfen
- Energieverwaltung von VMs (manuell und automatisch)

#### Voraussetzungen für die Verwendung des Ruhezustands

Führen Sie die folgenden Aufgaben aus, um den Ruhezustand zu verwenden:

- Installieren Sie den Azure VM Agent auf dem Masterimage für Windows und Linux. Die Auslagerungsdatei des Windows-Images kann sich auf dem temporären Datenträger befinden. MCS legt den Speicherort der Auslagerungsdatei auf Laufwerk C: des Basisdatenträgers fest, wenn der Ruhezustand für den Maschinenkatalog aktiviert ist.
- MCS legt die Ruhezustands-Eigenschaft für die generierten Ressourcen automatisch fest. Sie müssen die Eigenschaften der Master-Ressourcen nicht konfigurieren, um den Ruhezustand zu unterstützen.
- Verwenden Sie eine VM-Größe in Ihrem Abonnement, die den Ruhezustand unterstützt.
- Erstellen Sie ein für den Ruhezustand geeignetes Maschinenprofil (VM oder Vorlagenspezifikation), damit VMs die Eignung für den Ruhezustand erben. Informationen zum Erstellen der VM finden Sie unter Erste Schritte mit dem Ruhezustand.

  > **Hinweis:**
  >
  > Gemäß Microsoft können Sie für den Ruhezustand geeignete VMs von einem Betriebssystemdatenträger aus bereitstellen. Das Feature wird derzeit für bestimmte Regionen unterstützt und in Kürze für alle Regionen verfügbar sein. Weitere Informationen finden Sie unter VMs mit aktiviertem Ruhezustand von einem Betriebssystemdatenträger

> bereitstellen.

Gehen Sie wie folgt vor, um die Vorlagenspezifikation zu erstellen:

1. Öffnen Sie das Azure-Portal. Wählen Sie die VM, deren Konfiguration Sie in der Vorlage verwenden möchten. Wählen Sie im linken Bereich **Vorlage exportieren**.
2. Deaktivieren Sie das Kontrollkästchen **Parameter einschließen**. Kopieren Sie den Kontext und speichern Sie ihn als JSON-Datei (beispielsweise `VMExportTemplate.json`).
3. Vergewissern Sie sich, dass der Parameter `hibernationEnabled` für die Vorlage auf **`true`** steht. Wenn der Parameter nicht auf **`true`** steht, überprüfen Sie die verwendete VM-Konfiguration. Sie können eine unterstützte VM-Größe in der Vorlagendatei angeben. Sie können die VM-Größe aber auch beim Erstellen des Katalogs angeben.
4. Fügen Sie der JSON-Datei `VMExportTemplate.json` die Vorlage für die Netzwerkschnittstellenressource hinzu. Dadurch erhalten Sie eine ARM-Vorlagendatei mit zwei Ressourcen.
5. Wählen Sie **Azure-Portal > Vorlagenspezifikationen > Vorlage importieren > Lokale Vorlagendatei auswählen**, um diese Vorlagendatei als ARM-Vorlagenspezifikation zu importieren.
6. Nach Erstellung der ARM-Vorlagenspezifikation können Sie diese als Maschinenprofil verwenden.

> **Hinweis:**
>
> Die Synchronisierung mit Citrix Studio kann einige Minuten dauern.

Informationen hierzu finden Sie bei Microsoft unter Voraussetzungen für die Verwendung des Ruhezustands.

#### Einschränkungen

- Es werden nur Einzelsitzungs-OS-Maschinenkataloge (persistente und nicht persistente) unterstützt.
- Kurzlebige Betriebsystemdatenträger und MCS-E/A-Features unterstützen den Azure-Ruhezustand nicht.
- Während der automatischen Windows-Updates schlägt der Ruhezustand möglicherweise fehl.

Weitere Informationen finden Sie in der Microsoft-Dokumentation.

#### Katalog mit für den Ruhezustand geeigneten Maschinen erstellen und verwalten

Um virtuelle Maschinen mit Eignung für den Ruhezustand zu erstellen, können Sie einen entsprechenden Maschinenkatalog mithilfe einer der folgenden Optionen erstellen:

- Benutzeroberfläche für die vollständige Konfiguration oder
- PowerShell-Befehle

**Katalog mit der Schnittstelle "Vollständige Konfiguration"erstellen**

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
2. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** im linken Bereich.
3. Wählen Sie **Maschinenkatalog erstellen**. Der Assistent zum Erstellen von Katalogen wird geöffnet.
4. Wählen Sie auf der Seite **Maschinentyp** die Option **Einzelsitzungs-OS**.
5. Wählen Sie auf der Seite **Maschinenverwaltung** die Einstellungen wie folgt aus:
   a) Wählen Sie **Maschinen mit Energieverwaltung (z. B. virtuelle Maschinen oder Blade-PCs)**.
   b) Wählen Sie **Citrix Maschinenerstellungsdienste (MCS)**.
6. Wählen Sie auf der Seite **Desktoperfahrung** je nach Bedarf die zufällige oder statische Desktoperfahrung aus.
7. Wählen Sie auf der Seite **Image** ein Masterimage. Aktivieren Sie das Kontrollkästchen **Maschinenprofil verwenden** und wählen Sie ein Maschinenprofil aus, das den Ruhezustand unterstützt. Klicken Sie auf den Tooltip, um zu ermitteln, ob ein Maschinenprofil den Ruhezustand unterstützt.
8. Wählen Sie auf der Seite **Speicher- und Lizenztypen** den für diesen Katalog zu verwendenden Speicher und die Lizenz.
9. Wählen Sie auf der Seite **Virtuelle Maschinen** die Anzahl der VMs, die VM-Größe und die Verfügbarkeitszone.

   > **Hinweis:**
   >
   > Es werden nur Maschinengrößen zur Auswahl angezeigt, die den Ruhezustand unterstützen. Die GPU-VM-Serie wird als Preview veröffentlicht.

10. Fügen Sie auf der Seite **Netzwerkkarten** die Netzwerkkarten hinzu, die die VMs verwenden sollen.
11. Wählen Sie auf der Seite **Datenträgereinstellungen** den Speichertyp und die Größe des Zurückschreibcache-Datenträgers aus.
12. Wählen Sie auf der Seite **Ressourcengruppe** die Ressourcengruppe für die Bereitstellung von VMs aus.

13. Wählen Sie auf der Seite **Maschinenidentitäten** die Option **Neue Active Directory-Konten erstellen**. Geben Sie dann ein Kontobenennungsschema an.
14. Klicken Sie auf der Seite **Domänenanmeldeinformationen** auf **Anmeldeinformationen eingeben**. Geben Sie Ihre Domänenanmeldeinformationen ein, um die Kontenerstellung in der Active Directory-Zieldomäne durchzuführen.
15. Geben Sie auf der Seite **Zusammenfassung** einen Namen für den Maschinenkatalog ein und klicken Sie auf **Fertigstellen**.

Nach Erstellung des MCS-Maschinenkatalogs suchen Sie den Katalog in der Katalogliste und klicken Sie auf die Registerkarte **Vorlageneigenschaften**. Der Wert des Parameters **Ruhezustand** muss **Unterstützt** lauten.

Wenn Sie einen Maschinenkatalog bearbeiten möchten, beachten Sie die folgenden Einschränkungen:

- Wenn der aktuelle Maschinenkatalog den Ruhezustand unterstützt, ist Folgendes nicht möglich:
  - Ändern der VM-Größe auf eine Größe, die nicht für den Ruhezustand geeignet ist.
  - Ändern des Maschinenprofils auf eines, das nicht für den Ruhezustand geeignet ist.
- Wenn der aktuelle Maschinenkatalog den Ruhezustand nicht unterstützt, ist Folgendes nicht möglich:
  - derzeit über die Benutzeroberfläche für die vollständige Konfiguration das Maschinenprofil in ein für den Ruhezustand geeignetes Profil umwandeln. Sie können hierfür jedoch PowerShell-Befehle verwenden. Siehe Ruhezustand für per MCS bereitgestellte Maschinen aktivieren.

**Maschinenkatalog für die Verwaltung bestehender Maschinen erstellen, die für den Ruhezustand geeignet sind** Wenn Sie über virtuelle Maschinen verfügen, die für den Ruhezustand geeignet sind und deren Betrieb anhalten und wieder aufnehmen möchten, erstellen Sie einen Maschinenkatalog, um die VMs für die Energieverwaltung zu importieren.

> **Hinweis:**
>
> Sie können einen Maschinenkatalog erstellen, der sowohl für den Ruhezustand geeignete als auch nicht geeignete VMs enthält. Wenn Sie jedoch die Ruhezustandsfunktionen nutzen möchten, darf der Maschinenkatalog nur VMs enthalten, die für den Ruhezustand geeignet sind.

Um über die Benutzeroberfläche für die vollständige Konfiguration einen Katalog für vorhandene virtuelle Maschinen zu erstellen, die für den Ruhezustand geeignet sind, folgen Sie den angezeigten Anweisungen und achten Sie auf die folgenden wichtigen Einstellungen:

1. Wählen Sie auf der Seite **Maschinenverwaltung** die Option **Maschinen mit Energieverwaltung** und dann **Anderer Dienst oder andere Technologie** als Methode der Maschinenbereitstellung.
2. Fügen Sie auf der Seite **Virtuelle Maschinen** nur die virtuellen Maschinen hinzu (oder importieren Sie Maschinen), die für den Ruhezustand geeignet sind.

**Maschinenkatalog mit PowerShell-Befehlen erstellen** Wenn alle Anforderungen für die Verwendung des Ruhezustands erfüllt sind, können Sie mithilfe des Befehls `New-ProvScheme` einen Maschinenkatalog erstellen, der für den Ruhezustand geeignet ist. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter Citrix DaaS mit Remote PowerShell SDKs verwalten.

Bei der Katalogerstellung können Sie mithilfe der folgenden PowerShell-Befehle überprüfen, ob eine VM-Größe und ein Maschinenprofil den Ruhezustand unterstützen:

- Führen Sie für die VM-Größe den folgenden Befehl aus und überprüfen Sie, ob die Eigenschaft `supportsHibernation` auf **True** steht. Zum Beispiel:

```
1  Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
       VirtualNetwork> \serviceoffering.folder") | select Name,
       AdditionalData | ConvertTo-Json
2  <!--NeedCopy-->
```

- Führen Sie für das Maschinenprofil den folgenden Befehl aus und überprüfen Sie, ob die Eigenschaft `supportsHibernation` auf **True** steht. Zum Beispiel:

```
1  Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
       VirtualNetwork> \machineprofile.folder\abc.resourcegroup")|
       select Name, AdditionalData|ConvertTo-Json
2  <!--NeedCopy-->
```

Wenn Sie einen Maschinenkatalog bearbeiten möchten, beachten Sie die folgenden Einschränkungen:

- Wenn der aktuelle Maschinenkatalog den Ruhezustand unterstützt, ist Folgendes nicht möglich:
  - Ändern der VM-Größe auf eine Größe, die nicht für den Ruhezustand geeignet ist
  - Ändern des Maschinenprofils auf eines, das nicht für den Ruhezustand geeignet ist
- Wenn der aktuelle Maschinenkatalog den Ruhezustand nicht unterstützt, ist Folgendes nicht möglich:
  - derzeit über die Benutzeroberfläche für die vollständige Konfiguration das Maschinenprofil in ein für den Ruhezustand geeignetes Profil umwandeln. Sie können hierfür jedoch PowerShell-Befehle verwenden. Siehe Ruhezustand für per MCS bereitgestellte Maschinen aktivieren.

Informationen zum Ändern der VM-Größe und des Maschinenprofils für einen Katalog mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

#### Ruhezustand auf bestehenden, per MCS bereitgestellten VMs aktivieren

Sie können den Azure-Ruhezustand für Folgendes aktivieren:

- Mit MCS bereitgestellte Windows-VMs eines Maschinenkatalogs ohne temporären Datenträger.
- Mit MCS bereitgestellte Linux-VMs eines Maschinenkatalogs mit oder ohne temporären Datenträger.

> **Hinweis:**
>
> - Auf den über MCS bereitgestellten VMs muss ein Azure-VM-Agent installiert sein.
> - Derzeit können Sie das Feature nur mit dem PowerShell-Befehl aktivieren.

Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um Citrix-spezifische PowerShell-Module zu laden.
3. Prüfen Sie die Konfiguration der vorhandenen Maschinen. Beispiel:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Aktivieren Sie den Ruhezustand für den Maschinenkatalog mit dem Befehl `Set-ProvScheme`. Beispiel:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. Fordern Sie ein Update für VMs in einem Maschinenkatalog an.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
<!--NeedCopy-->
```

6. Starten Sie die VMs neu, um Updates auszulösen. Beispiel:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

### Ruhezustand-Eigenschaft überprüfen

Sie können die Ruhezustand-Eigenschaft eines Maschinenkatalogs, einer VM oder einer Brokermaschine mithilfe der folgenden PowerShell-Befehle überprüfen:

- Führen Sie die folgenden PowerShell-Befehle aus, um die Ruhezustand-Eigenschaft eines Provisioningschemas zu überprüfen. Der Parameter `HibernationEnabled` muss auf `True` festgelegt sein.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
   VMMetadata -join "" |  ConvertFrom-Json | Select
   HibernationEnabled
<!--NeedCopy-->
```

- Führen Sie die folgenden PowerShell-Befehle aus, um die Ruhezustand-Eigenschaft einer Provisioning-VM zu überprüfen. Der Parameter `SupportsHibernation` muss auf `True` festgelegt sein.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- Führen Sie die folgenden PowerShell-Befehle aus, um die Ruhezustand-Eigenschaft einer Brokermaschine zu überprüfen. Die Energieaktionen **Anhalten** und **Fortsetzen** zeigen an, dass der Ruhezustand möglich ist.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

### Energieverwaltung von für den Ruhezustand geeigneten VMs

Sie können die folgenden Energieverwaltungsvorgänge auf für den Ruhezustand geeigneten VMs ausführen:

- Sie können eine ausgeführte VM **anhalten**.
- Sie können eine angehaltene VM **fortsetzen**.
- Sie können das Herunterfahren einer VM im Zustand “Angehalten”**erzwingen**.
- Sie können den Neustart einer VM im Zustand “Angehalten”**erzwingen**.

Weitere Informationen:

- Anhalten
- Fortsetzen

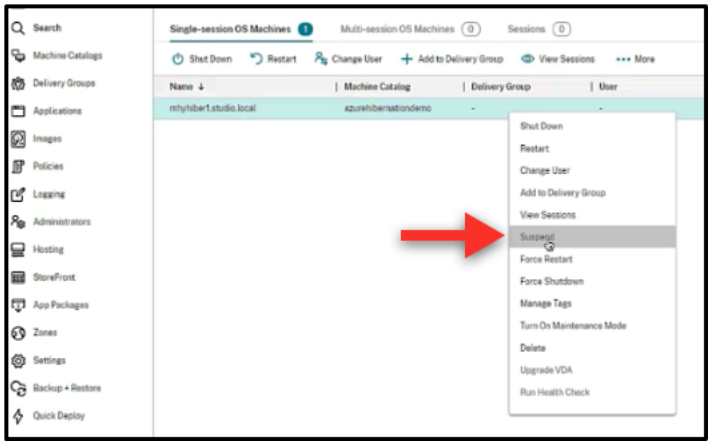
 

**Anhalten** Sie können eine VM auf eine der folgenden Arten anhalten:

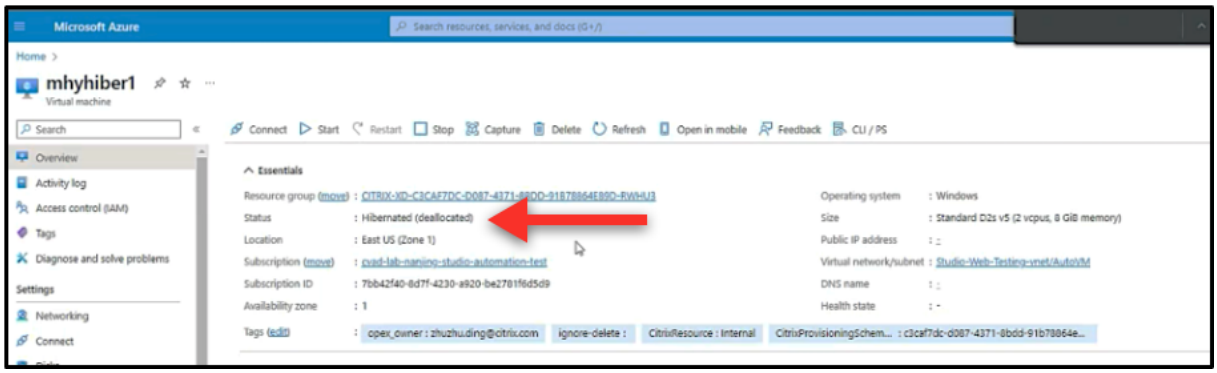
- **Manuell** mit der Benutzeroberfläche für die vollständige Konfiguration
- **Automatisch** mit der Timeout-Richtlinie: Weitere Informationen finden Sie unter Sonstige Einstellungen.

Gehen Sie zum manuellen Anhalten einer VM folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Anhalten**. Klicken Sie auf **Ja**, um die Aktion zu bestätigen. Der **Energiezustand** wechselt von **Wird angehalten** zu **Angehalten**.



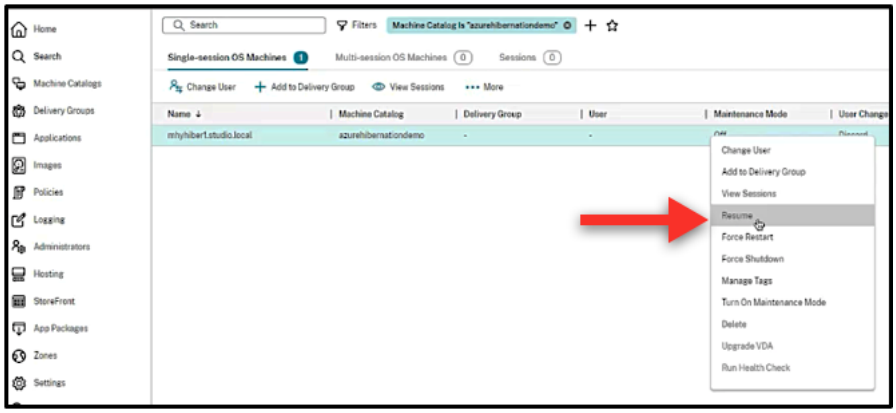

Sie können den Status der VM im Azure-Portal überprüfen.



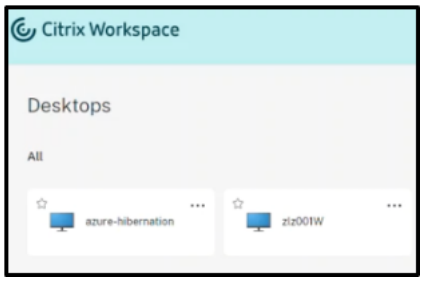

**Fortsetzen** Verwenden Sie eine der folgenden Methoden, um den Betrieb einer VM im Ruhezustand wieder aufzunehmen:

- **Manuell**:
  - Administratoren können den VM-Betrieb über die Benutzeroberfläche für die vollständige Konfiguration fortsetzen.

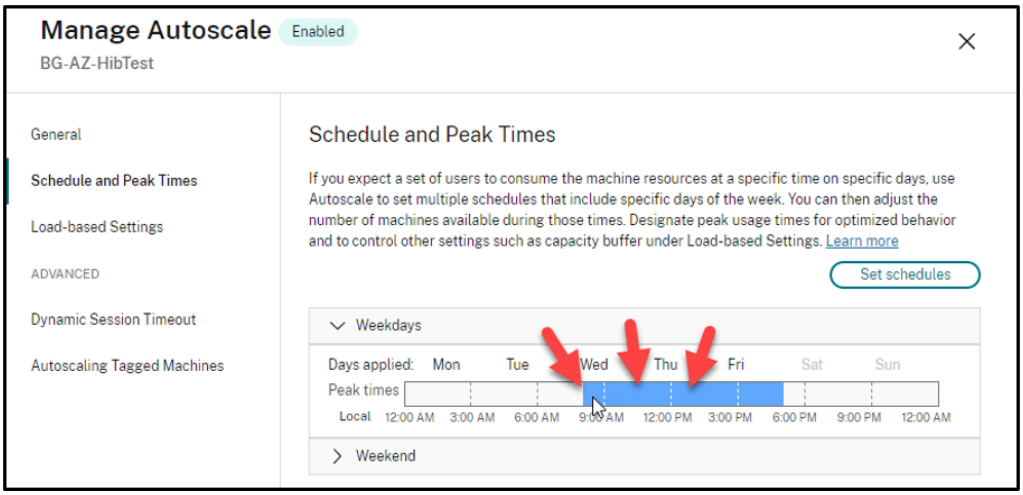
 




- Endbenutzer können eine VM über das Citrix Workspace-Menü starten, wenn sie auf das Desktopsymbol klicken.

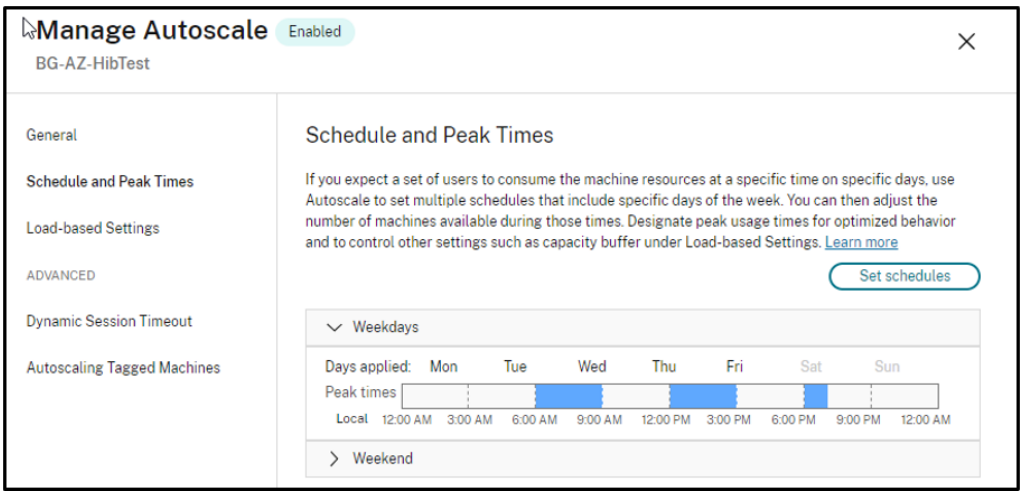



- **Automatisch**:
  - Autoscale kann Maschinen im Ruhezustand automatisch einschalten, wenn Sie die Spitzenzeiten richtig konfigurieren. Sie können die Spitzenzeiten in 30-Minuten-Intervallen festlegen, indem Sie auf den Zeitplan klicken. Jeder blaue Rahmen steht für ein Zeitfenster, das als Spitzenzeit markiert ist. Die Spitzenzeiten können aufeinander folgen oder auch nicht.
    - Aufeinanderfolgende Zeitfenster



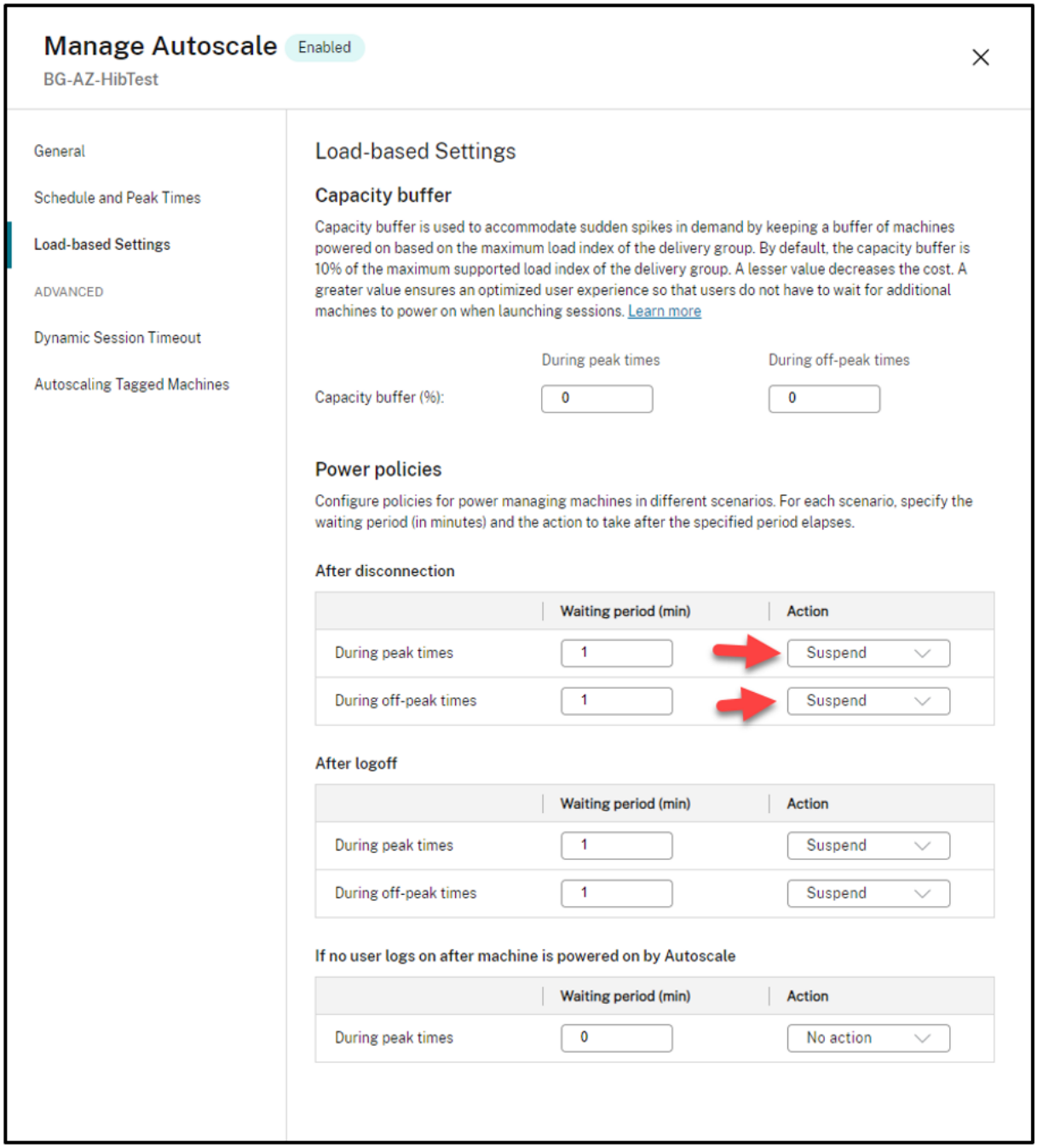

 

* Nicht aufeinanderfolgende Zeitfenster




> **Hinweis:**
>
> Wenn die **Aktion** unter **Autoscale verwalten > Lastbasierte Einstellungen** mit **Anhalten** konfiguriert ist, vergewissern Sie sich, dass alle VMs in der Bereitstellungsgruppe ruhezustandsfähig sind. Andernfalls laufen VMs, die nicht in den Ruhezustand versetzt werden können, weiter.




## Weitere Informationen

Weitere Informationen zum Citrix Azure-Ruhezustand finden Sie in diesem Citrix Tech Zone-Artikel.

# Sicherheitsrichtlinien

April 14, 2023

In diesem Artikel werden die Sicherheitsfeature für verschiedene unterstützte Hypervisoren beschrieben. Dazu gehören:

- Sicherheitsgruppe
- Sicherer Start
- Verschlüsselungsfunktionen

# Sicherheitsgruppe

April 14, 2023

Eine Sicherheitsgruppe ist eine Gruppe von Sicherheitsregeln zum Filtern des Netzwerkdatenverkehrs zwischen Ressourcen in einem virtuellen Netzwerk. Die Sicherheitsregeln erlauben oder verweigern eingehenden und ausgehenden Netzwerkdatenverkehr an und von Ressourcen verschiedener Art. Jede Regel spezifiziert die folgenden Eigenschaften:

- Name: Ein eindeutiger Name innerhalb der Netzwerksicherheitsgruppe
- Priorität: Regeln werden in der Reihenfolge ihrer Priorität verarbeitet, wobei niedrigere Zahlen vor höheren Zahlen verarbeitet werden, da niedrigere Zahlen eine höhere Priorität haben.
- Quelle oder Ziel: Beliebige oder eine einzelne IP-Adresse, ein CIDR-Block (klassenloses domänenübergreifendes Routing, z. B. 10.0.0.0/24), ein Service-Tag oder eine Anwendungssicherheitsgruppe
- Protokoll: Die Protokolle, auf deren Grundlage Sie Regeln für jede Sicherheitsgruppe hinzufügen
- Richtung: Ob die Regel für eingehenden oder ausgehenden Datenverkehr gilt
- Portbereich: Sie können einen einzelnen Port oder einen Bereich von Ports angeben.
- Aktion: Zulassen oder Ablehnen

Weitere Informationen zu unterstützten Hypervisors:

- Sicherheitsgruppe in AWS
- Sicherheitsgruppe in Microsoft Azure
- Sicherheitsgruppe in Google Cloud Platform

### Sicherheitsgruppe in AWS

Sicherheitsgruppen fungieren als virtuelle Firewall und steuern den Datenverkehr für die Instanzen in der VPC. Sie fügen den Sicherheitsgruppen Regeln zur Kommunikation zwischen Instanzen im öffentlichen und im privaten Subnetz hinzu. Sie können die Sicherheitsgruppen außerdem jeder Instanz in der VPC zuordnen. Eingehende Regeln steuern den eingehenden Datenverkehr zu einer Instanz und ausgehende Regeln steuern den ausgehenden Datenverkehr von der Instanz.

Weitere Informationen Netzwerkeinstellung während der Imagevorbereitung finden Sie unter Netzwerkeinstellung während der Imagevorbereitung.

Wenn Sie eine Instanz starten, können Sie eine oder mehrere Sicherheitsgruppen angeben. Informationen zum Konfigurieren von Sicherheitsgruppen finden Sie unter Sicherheitsgruppen konfigurieren.

### Sicherheitsgruppe in Microsoft Azure

Citrix DaaS unterstützt Netzwerksicherheitsgruppen in Azure. Von Netzwerksicherheitsgruppen wird erwartet, dass sie Subnetzen zugeordnet sind. Weitere Informationen finden Sie unter Netzwerksicherheitsgruppen.

Weitere Informationen zu bei der Imageerstellung erstellten Netzwerksicherheitsgruppen finden Sie unter Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images erstellen.

### Sicherheitsgruppe in Google Cloud Platform

Bei der Vorbereitung eines Maschinenkatalogs wird ein Maschinenabbild vorbereitet, das als Masterimage-Systemdatenträger für den Katalog dient. Bei diesem Vorgang wird der Datenträger vorübergehend an eine virtuelle Maschine angefügt. Die VM muss in einer isolierten Umgebung ausgeführt werden, die jeglichen eingehenden und ausgehenden Netzwerkdatenverkehr verhindert. Dies wird durch zwei Alles-abweisen-Firewallregeln erreicht. Weitere Informationen finden Sie unter Firewallregeln.

## Sicherer Start

May 17, 2024

Secure Boot soll dafür sorgen, dass nur vertrauenswürdige Software zum Starten des Systems verwendet wird. Die Firmware verfügt über eine Datenbank mit vertrauenswürdigen Zertifikaten und

überprüft, ob das zu ladende Image mit einem dieser Zertifikate signiert wurde. Wenn ein Image weitere Images lädt, müssen diese auf die gleiche Weise geprüft werden.
vTPM ist eine virtualisierte Softwareinstanz eines herkömmlichen physischen TPM-Moduls. vTPM ermöglicht einen Nachweis durch Messung der gesamten Startkette der VM (UEFI, Betriebssystem, System und Treiber).

Weitere Informationen zu unterstützten Hypervisors:

- Secure Boot in Google Cloud Platform
- Secure Boot in Microsoft Azure
- Secure Boot in VMware

### Secure Boot in Google Cloud Platform

Sie können abgeschirmte virtuelle Maschinen auf GCP bereitstellen. Eine abgeschirmte virtuelle Maschine wird durch Sicherheitskontrollen gehärtet, die eine überprüfbare Integrität der Compute Engine-Instanzen über erweiterte Plattformsicherheitsfunktionen wie Sicherer Start, ein virtuelles Trusted Platform Module, UEFI-Firmware und Integritätsüberwachung bieten.

Weitere Informationen zur Verwendung von PowerShell zum Erstellen eines Katalogs mit Shielded VM finden Sie unter Katalog mit Shielded VM mit PowerShell erstellen.

> **Hinweis:**
>
> Wenn Sie Windows 11 auf dem Masterimage installieren, müssen Sie vTPM während der Erstellung des Masterimages aktivieren. Außerdem müssen Sie vTPM auf der Maschinenprofilquelle (VM oder Instanzvorlage) aktivieren. Informationen zum Erstellen von Windows 11-VMs auf dem Einzelmandantenknoten finden Sie unter Windows 11-VMs auf dem Einzelmandantenknoten erstellen.

### Secure Boot in Microsoft Azure

In Azure-Umgebungen können Sie Maschinenkataloge erstellen, für die vertrauenswürdiger Start aktiviert ist. Mit vertrauenswürdigen Starts in Azure lässt sich die Sicherheit von VMs der zweiten Generation weiter verbessern. Der vertrauenswürdige Start schützt vor fortschrittlichen und persistenten Angriffstechniken. Die Grundlage des vertrauenswürdigen Starts bildet Secure Boot für die VM. Der vertrauenswürdige Start verwendet außerdem vTPM für den Remote-Nachweis durch die Cloud. Dies wird für Plattform-Integritätsprüfungen und für vertrauensbasierte Entscheidungen genutzt. Sie können Secure Boot und vTPM individuell aktivieren.
Weitere Informationen zum Erstellen eines Maschinenkatalogs mit vertrauenswürdigem Start finden Sie unter Maschinenkataloge mit vertrauenswürdigem Start.

### Secure Boot in VMware

MCS unterstützt das Erstellen eines Maschinenkatalogs mit einer VMware-Vorlage mit angefügtem vTPM als Quelle für die Maschinenprofileingabe. Ist Windows 11 auf dem Masterimage installiert, muss vTPM für das Masterimage aktiviert sein. Daher muss an die VMware-Vorlage, die eine Quelle für das Maschinenprofil ist, vTPM angefügt sein. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Maschinenprofils.

## Verschlüsselungsfunktionen

June 12, 2024

Verschlüsselungsfunktionen schützen den Inhalt virtueller Maschinen vor Angriffen böswilliger Gäste auf einem freigegebenen VM-Host und vor Angriffen durch die Hypervisor-Steuerungssoftware, die alle virtuellen Maschinen auf dem Host verwaltet.

Weitere Informationen zu unterstützten Hypervisors:

- Verschlüsselungsfunktionen in AWS
- Verschlüsselungsfunktionen in Google Cloud Platform
- Verschlüsselungsfunktionen in Microsoft Azure

### Verschlüsselungsfunktionen in AWS

In diesem Abschnitt werden die Verschlüsselungsfunktionen in AWS-Virtualisierungsumgebungen beschrieben.

#### Automatische Verschlüsselung

Sie können die automatische Verschlüsselung neuer Amazon EBS-Volumes und Snapshotkopien aktivieren, die in Ihrem Konto erstellt wurden. Weitere Informationen finden Sie unter Automatische Verschlüsselung.

### Verschlüsselungsfunktionen in Google Cloud Platform

In diesem Abschnitt werden die Verschlüsselungsfunktionen in GCP-Virtualisierungsumgebungen beschrieben.

Wenn Sie mehr Kontrolle über Schlüsseloperationen benötigen, als mit den von Google verwalteten Verschlüsselungsschlüsseln möglich ist, können Sie kundenverwaltete Verschlüsselungsschlüssel verwenden. Bei Verwendung kundenverwalteter Verschlüsselungsschlüssel werden Objekte zum Zeitpunkt der Speicherung in einem Bucket von Cloud Storage verschlüsselt und automatisch entschlüsselt, wenn sie Anforderern zugestellt werden. Weitere Informationen finden Sie unter Vom Kunden verwaltete Verschlüsselungsschlüssel.

Sie können vom Kunden verwaltete Verschlüsselungsschlüssel (Customer Managed Encryption Keys, CMEK) für MCS-Kataloge verwenden. Weitere Informationen finden Sie unter Verwenden vom Kunden verwalteter Verschlüsselungsschlüssel (CMEK).

## Verschlüsselungsfunktionen in Microsoft Azure

In diesem Abschnitt werden die Verschlüsselungsfunktionen in Azure-Virtualisierungsumgebungen beschrieben.

### Azure-serverseitige Verschlüsselung

Die meisten Azure-verwalteten Datenträger sind mit der Azure Storage-Verschlüsselung verschlüsselt, bei eine serverseitige Verschlüsselung (SSE) zum Schutz Ihrer Daten und zur Unterstützung Ihrer Maßnahmen für Sicherheit und Compliance verwendet wird. Citrix DaaS unterstützt vom Kunden verwaltete Schlüssel für Azure Managed Disks über Azure Key Vault. Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

### Azure-Datenträgerverschlüsselung auf dem Host

Sie können einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen.

Bei diesem Verschlüsselungsverfahren werden Daten nicht über den Azure-Speicher verschlüsselt. Die Daten werden auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten.

Weitere Informationen zum Erstellen eines MCS-Maschinenkatalogs mit Verschlüsselung auf dem Host finden Sie unter Azure-Festplattenverschlüsselung auf dem Host.

### Doppelte Verschlüsselung in Azure

Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der kundenseitig verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter

Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt. Weitere Informationen finden Sie unter Doppelte Verschlüsselung verwalteter Datenträger.

#### Vertrauliche Azure-VMs

Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist.

Sie können MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

Weitere Informationen finden Sie unter Vertrauliche Azure-VMs.

## Quick Deploy

November 16, 2023

### Einführung

Die Oberfläche **Verwalten > Quick Deploy** in Citrix DaaS ermöglicht das schnelle Bereitstellen von Apps und Desktops, wenn Sie Microsoft Azure als Host für Desktops und Apps verwenden. Diese Schnittstelle ermöglicht eine Grundkonfiguration ohne erweiterte Features.

Verwenden Sie Quick Deploy für Folgendes:

- Provisioning virtueller Maschinen und Kataloge, um in Microsoft Azure gehostete Desktops und Apps bereitzustellen
- Erstellen von Remote-PC-Zugriffskatalogen für vorhandene Maschinen

Mit Quick Deploy können Sie ein Citrix Managed Azure-Abonnement oder Ihr eigenes Azure-Abonnement verwenden.

Quick Deploy ist nicht dasselbe wie die Schnellerstellung von Katalogen in der Quick Deploy-Schnittstelle.

Die alternative Schnittstelle **Vollständige Konfiguration** bietet erweiterte Konfigurationsfeatures. Informationen zu den Optionen der Registerkarte **Verwalten** finden Sie unter Managementschnittstellen.

### Unterschiede zwischen den Managementschnittstellen

In der folgenden Tabelle werden die Schnittstellen "Vollständige Konfiguration"und "Quick Deploy" verglichen.

| Feature | Quick Deploy | Vollständige Konfiguration |
|---|---|---|
| Bereitstellen mit Azure | Ja | Ja * |
| Bereitstellen mit anderen Clouddiensten | Nein | Ja |
| Bereitstellen mit On-Premises-Hypervisors | Nein | Ja |
| Von Citrix erstellte Images verfügbar | Ja | Nein |
| Vereinfachte Benutzererfahrung | Ja | Nein |

*Bei Verwendung eines Citrix Managed Azure-Abonnements müssen Sie Images und Kataloge mit Quick Deploy erstellen.

Wenn Sie mit dem Erstellen und Verwalten von Katalogen über die vollständige Konfiguration vertraut sind, sollten Sie folgende Unterschiede bei Quick Deploy berücksichtigen.

- Unterschiedliche Terminologie.
  - In Quick Deploy erstellen Sie einen Katalog.
  - In der vollständigen Konfiguration erstellen Sie einen Maschinenkatalog. In der Praxis wird meist der Begriff "Katalog"verwendet.
- Ressourcenstandort und Cloud Connectors.
  - Wenn Sie in Quick Deploy den ersten Katalog erstellen, wird automatisch ein Ressourcenstandort mit zwei Cloud Connectors angelegt.
  - In der vollständigen Konfiguration sind das Erstellen eines Ressourcenstandorts und das Hinzufügen von Cloud Connectors separate Schritte, die Sie vor dem Erstellen eines Katalogs in Citrix Cloud ausführen müssen.
- Images zum Erstellen von Katalogen.
  - Quick Deploy bietet mehrere von Citrix erstellte Images für Windows- und Linux-Maschinen. Sie können diese Images verwenden, um Kataloge zu erstellen.

    Sie können auf der Basis dieser Images auch neue Images erstellen und diese an die individuellen Anforderungen Ihrer Bereitstellung anpassen. Das Feature heißt "Image Builder" . Sie können Images auch aus Ihrem Azure-Abonnement importieren.

  - In der vollständigen Konfiguration passen Sie Images von dem verwendeten unterstützten Host an. Von Citrix erstellte Images nicht verfügbar

- Kataloganzeigen:
  - In Quick Deploy erstellte Kataloge werden in Quick Deploy und in der vollständigen Konfiguration angezeigt.
  - Kataloge, die in der vollständigen Konfiguration erstellt werden, sind in Quick Deploy nicht zu sehen.

- Bereitstellungsgruppen:
  - In Quick Deploy erstellen Sie keine Bereitstellungsgruppen. In Quick Deploy geben Sie die Maschinen, Anwendungen, Desktops und Benutzer (Abonnenten) im Katalog an.

    Citrix erstellt automatisch für jeden Katalog von Quick Deploy eine gleichnamige Bereitstellungsgruppe. Diese Aktion findet im Hintergrund statt. Sie müssen nichts unternehmen, um die Bereitstellungsgruppe zu erstellen. Die Bereitstellungsgruppe wird nur in der vollständigen Konfiguration, nicht aber in Quick Deploy angezeigt.
  - In der vollständigen Konfiguration erstellen Sie eine Bereitstellungsgruppe und geben an, welche Maschinen sie enthält. Optional können Sie auch Anwendungen, Desktops und Benutzer angeben. Sie können auch Anwendungsgruppen erstellen.

- Layout und Benutzeroberfläche.
  - Die Benutzeroberfläche von Quick Deploy unterscheidet sich in Layout und Stil von der Oberfläche der vollständigen Konfiguration. Quick Deploy enthält mehr Bildschirmanweisungen.

Die Oberflächen schließen sich jedoch gegenseitig nicht aus. Sie können einige Kataloge mit Quick Deploy und andere Kataloge mit der vollständigen Konfiguration erstellen.

### Verwalten von mit Quick Deploy erstellten Katalogen

Wenn Sie einen Katalog in der Quick Deploy-Schnittstelle erstellen, können Sie ihn dort auch weiterhin verwalten. Weitere Informationen finden Sie unter Verwalten von Katalogen in Quick Deploy. Sie können auch die Schnittstelle für die vollständige Konfiguration verwenden.

Wenn Sie einen Katalog in Quick Deploy erstellen, wird diesem (sowie der im Hintergrund automatisch erstellten Bereitstellungsgruppe und Hosting-Verbindung) der Bereich `Citrix managed object` zugewiesen. Bereiche werden in der delegierten Administration zur Gruppierung von Objekten verwendet.

Bei Katalogen, Bereitstellungsgruppen und Verbindungen mit dem Bereich `Citrix managed object` sind einige Aktionen in der Schnittstelle zur vollständigen Konfiguration nicht zugelassen.

(Die Aktionen sind deaktiviert, da sie die Unterstützung von Quick Deploy und der vollständigen Konfiguration durch das System beeinträchtigen könnten.) Für die Schnittstelle zur vollständigen Konfiguration gilt Folgendes:

- **Katalog:** Die meisten Aktionen zur Katalogverwaltung sind nicht verfügbar. Sie können einen Katalog nicht löschen.
- **Bereitstellungsgruppe:** Die meisten Aktionen zur Bereitstellungsgruppenverwaltung sind verfügbar. Sie können die Bereitstellungsgruppe nicht löschen.
- **Verbindung:** Die meisten Aktionen zur Verbindungsverwaltung sind nicht verfügbar. Sie können eine Verbindung nicht löschen. Sie können keine Verbindung auf Basis einer Verbindung mit Bereich `Citrix managed object` erstellen.

Wenn Sie einen Katalog in Quick Deploy unter Verwendung Ihres eigenen Azure-Abonnements (das Sie zu Quick Deploy hinzugefügt haben) erstellen und den Katalog (sowie dessen Bereitstellungsgruppe und Verbindung) ausschließlich über die Schnittstelle zur vollständigen Konfiguration verwalten möchten, können Sie den Katalog *konvertieren*.

- Das Konvertieren eines Katalogs beschränkt dessen Verwaltung auf die Schnittstelle zur vollständigen Konfiguration. Nach dem Konvertieren eines Katalogs können Sie Quick Deploy nicht mehr für dessen Verwaltung verwenden.
- Nach dem Konvertieren eines Katalogs können Sie die Aktionen verwenden, die in der vollständigen Konfiguration zuvor nicht verfügbar waren. (Der Geltungsbereich `Citrix managed object` wird von dem konvertierten Katalog, der Bereitstellungsgruppe und der Hosting-Verbindung entfernt.)
- Gehen Sie zum Konvertieren eines Katalogs wie folgt vor:

  Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags. Wählen Sie auf der Registerkarte **Details** unter **Erweiterte Einstellungen** die Option **Katalog konvertieren**. Bestätigen Sie die Konvertierung, wenn Sie dazu aufgefordert werden.
- Kataloge, die in Quick Deploy mit einem Citrix Managed Azure-Abonnement erstellt wurden, können nicht konvertiert werden.

#### Ausmusterung der früheren Azure Quick Deploy-Benutzeroberfläche

Quick Deploy ersetzt das früher verwendete Azure Quick Deploy. Die Quick Deploy-Anzeige enthält alle Kataloge, die Sie mit Azure Quick Deploy erstellt haben.

Wenn Sie das Erstellen eines Katalogs in Azure Quick Deploy begonnen und nicht abgeschlossen haben, wird er in der Quick Deploy-Katalogliste angezeigt. Die einzige verfügbare Aktion in Quick Deploy besteht jedoch darin, ihn zu löschen.

## Anforderungen

- Quick Deploy unterstützt nur Azure-Workloads. Für andere Cloud-Hosttypen, Dienste oder Hypervisors ist das Feature nicht verfügbar.
- Quick Deploy ist nur in der Citrix DaaS für Azure-, Premium-, Advanced-Edition und in Workspace Premium Plus verfügbar.
- Sie müssen ein Citrix Cloud-Konto eingerichtet und Citrix DaaS abonniert haben.
- Wenn Sie den Citrix Managed Azure Consumption Fund bestellt haben, können Sie beim Erstellen von Katalogen und Images ein Citrix Managed Azure-Abonnement verwenden.

  Wenn Sie den Consumption Fund nicht bestellt haben (oder lieber Ihr eigenes Azure-Abonnement verwenden), benötigen Sie ein Azure-Abonnement.
- Sie müssen über die entsprechenden Berechtigungen in Citrix DaaS verfügen, um die Registerkarte **Verwalten** anzeigen zu können. Weitere Informationen finden Sie unter Delegierte Administration.

> **Wichtig:**
>
> Damit Sie wichtige Informationen über Citrix Cloud und die von Ihnen abonnierten Citrix Services erhalten, stellen Sie sicher, dass Sie alle E-Mail-Benachrichtigungen erhalten. Citrix sendet beispielsweise monatlich detaillierte Informationen über Ihren Azure-Verbrauch.
>
> Erweitern Sie in der oberen rechten Ecke der Citrix Cloud-Konsole das Menü rechts neben den Feldern “Kundenname”und “Organisations-ID”. Wählen Sie **Kontoeinstellungen**. Wählen Sie auf der Registerkarte **Mein Profil** alle Einträge im Abschnitt **E-Mail-Benachrichtigungen** aus.

### Hinweis zu Citrix Gateway

Wenn Sie Ihr eigenes Citrix Gateway verwenden, muss es Zugriff auf das im Assistenten für die Katalogerstellung angegebene VNet haben. Ein VPN kann diesen Zugriff bereitstellen.

Der Citrix Gateway Service funktioniert automatisch mit Quick Deploy-Katalogen.

## Nächste Schritte

Folgen Sie den Anweisungen zum Einrichten mit Quick Deploy unter Erste Schritte.

Wenn Sie Ihre Bereitstellung mit Quick Deploy eingerichtet haben, können Sie diese Schnittstelle für die folgenden Verwaltungsaufgaben weiterverwenden.

- Katalogverwaltung. Die Katalogverwaltung umfasst Hinzufügen oder Löschen von Maschinen, Verwalten von Apps, Verwalten von Energiezeitplänen.

- Imageverwaltung. Die Verwaltung von Images umfasst das Vorbereiten oder Importieren von Images, das Aktualisieren von Katalogen mit einem neuen Image, das Umbenennen oder Löschen von Images und das Installieren bzw. Aktualisieren von VDAs auf einem Image.
- Hinzufügen oder Entfernen von Benutzern in einem Katalog.
- Verwalten von Ressourcenstandorten.

## Erste Schritte mit Quick Deploy

May 23, 2023

In diesem Artikel werden die Aufgaben zum Einrichten und Bereitstellen von Desktops und Apps über die Verwaltungsoberfläche "Quick Deploy"in Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) aufgeführt. Wir empfehlen, jedes Verfahren vor der Ausführung durchzulesen, damit Sie gut vorbereitet sind.

Informationen zum Einrichten einer Remote-PC-Zugriffsbereitstellung mithilfe von Quick Deploy finden Sie unter Remote-PC-Zugriff.

### Überblick über die Einrichtungsaufgaben

Die folgenden Abschnitte dieses Artikels enthalten Informationen zu den Einrichtungsaufgaben:

1. Lesen Sie Systemanforderungen und Vorbereitung und führen Sie erforderliche Aufgaben aus.
2. Richten Sie eine Bereitstellung für eine schnelle Machbarkeitsstudie oder eine Produktionsbereitstellung ein.
3. Senden Sie die Workspace-URL an die Benutzer.

### Systemvoraussetzungen und Vorbereitung

- Registrieren Sie sich bei Citrix Cloud und Citrix DaaS.

  Wenn Sie Citrix Managed Azure nutzen möchten, bestellen Sie außerdem den Citrix Azure Consumption Fund (zusätzlich zu Citrix DaaS) über Citrix oder über Azure Marketplace.

- **Windows-Lizenzierung:** Stellen Sie sicher, dass Sie eine Lizenz zur Ausführung von Remotedesktopdienste unter Windows Server-Workloads oder Azure Virtual Desktop Licensing für Windows 10 haben. Weitere Informationen finden Sie unter Konfigurieren des Microsoft RDS-Lizenzservers.

- Wenn Sie ein Citrix Managed Azure-Abonnement verwenden und VDAs per Active Directory-Gruppenrichtlinie einer Domäne hinzufügen möchten, müssen Sie ein Administrator sein, der die Berechtigung zum Ausführen dieser Aktion in Active Directory hat. Weitere Informationen finden Sie unter Verantwortung des Kunden.
- Für das Konfigurieren von Verbindungen zu einem On-Premises-Unternehmensnetzwerk bestehen zusätzliche Anforderungen.
  - Alle Verbindungstypen (Azure VNet-Peering oder SD-WAN): Anforderungen für alle Verbindungen.
  - Azure VNet Peeringverbindungen: VNet-Peering –Anforderungen und Vorbereitung.
  - SD-WAN-Verbindungen: SD-WAN-Verbindung –Anforderungen und Vorbereitung
- Wenn Sie beim Erstellen eines Katalogs Ihre eigenen Azure-Images verwenden möchten, müssen diese Images bestimmte Anforderungen erfüllen.
- Anforderungen der Internetverbindung: Anforderungen an System und Konnektivität.
- Ressourcenlimits in einer Citrix DaaS-Bereitstellung: Limits.

#### Unterstützte Betriebssysteme

Bei Verwendung von Quick Deploy mit einem Citrix Managed Azure-Abonnement:

- Windows 10 (Einzelsitzungs-OS)
- Windows 10 (Multisitzungs-OS)
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux und Ubuntu

Bei Verwendung von Quick Deploy mit einem vom Kunden verwalteten Azure-Abonnement:

- Windows 10 Enterprise (Einzelsitzungs-OS)
- Windows 10 Enterprise Virtual Desktop (Multisitzungs-OS)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux und Ubuntu

### Einrichten einer Bereitstellung für eine schnelle Machbarkeitsstudie

Für dieses Verfahren ist ein Citrix Managed Azure-Abonnement erforderlich.

1. Erstellen Sie einen Katalog mit der Schnellerstellung.
2. Fügen Sie die Benutzer zu Managed Azure AD hinzu.
3. Fügen Sie die Benutzer zum Katalog hinzu.
4. Teilen Sie den Benutzern die Workspace-URL mit.

### Einrichten einer Produktionsbereitstellung

1. Wenn Sie Ihr eigenes Active Directory oder Azure Active Directory verwenden, um Benutzer zu authentifizieren, stellen Sie eine Verbindung her und stellen Sie diese Methode in Citrix Cloud ein.
2. Wenn Sie in Domänen eingebundene Maschinen verwenden, vergewissern Sie sich, dass Sie gültige DNS-Servereinträge haben.
3. Wenn Sie Ihr eigenes Azure-Abonnement anstelle eines Citrix Managed Azure-Abonnements verwenden, fügen Sie Ihr Azure-Abonnement hinzu.
4. Erstellen oder importieren Sie ein Image. Sie können zwar die von Citrix erstellten Images in einem Katalog unverändert verwenden, doch sind diese in erster Linie für Machbarkeitsstudien gedacht.
5. Wenn Sie ein Citrix Managed Azure-Abonnement verwenden und die Benutzer auf Objekte in Ihrem Netzwerk (z. B. Dateiserver) zugreifen sollen, richten Sie eine Azure VNet-Peering- oder Citrix SD-WAN-Verbindung ein.
6. Erstellen Sie einen Katalog mit der benutzerdefinierten Erstellung.
7. Wenn Sie einen Katalog mit Multisitzungsmaschinen erstellen, fügen Sie dem Katalog Apps hinzu, falls erforderlich.
8. Wenn Sie Citrix Managed Azure AD zur Authentifizierung der Benutzer verwenden, fügen Sie die Benutzer dem Verzeichnis hinzu.
9. Fügen Sie Benutzer zum Katalog hinzu.
10. Teilen Sie den Benutzern die Workspace-URL mit.

Nach dem Einrichten der Bereitstellung können Sie auf dem Dashboard **Quick Deploy > Überwachen** die Desktopnutzung, Sitzungen und Maschinen anzeigen.

### Workspace-URL

Nachdem Sie Kataloge erstellt und Benutzer hinzugefügt haben, teilen Sie den Benutzern mit, wo sie ihre Desktops und Apps finden: die Workspace-URL. Die Workspace-URL ist für alle Kataloge und Benutzer identisch.

Die Workspace-URL ist an zwei Orten verfügbar:

- Erweitern Sie in Citrix DaaS unter **Verwalten > Quick Deploy** auf der rechten Seite **Benutzerzugriff und Authentifizierung**.

- Klicken Sie in der Citrix Cloud-Konsole im Menü links oben auf **Workspacekonfiguration**. Die Registerkarte **Zugriff** enthält die Workspace-URL.

Informationen zum Anpassen der Workspace-URL finden Sie unter Anpassen der Workspace-URL.

Wenn Benutzer die Workspace-URL aufgerufen und sich authentifiziert haben, können sie ihre Desktops und Apps starten.

### Hilfe und Unterstützung

- Lesen Sie den Artikel Problembehandlung.
- Können die Probleme mit Citrix DaaS nicht gelöst werden, erstellen Sie ein Supportticket. Folgen Sie hierfür den Anweisungen unter Hilfe und Support.

## Kataloge mit Quick Deploy erstellen

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Mit den Verfahren in diesem Artikel können Sie Kataloge für Microsoft Azure-Maschinen mit der Quick Deploy-Verwaltungsschnittstelle erstellen.

Machen Sie sich mit dem gesamten Prozess vertraut, bevor Sie mit der Katalogestellung beginnen, damit Sie wissen, was zu erwarten ist.

Informationen zum Erstellen eines Katalogs mit der Schnittstelle "Vollständige Konfiguration"finden Sie unter Erstellen von Maschinenkatalogen.

### Maschinentypen

Ein Quick Deploy-Katalog kann einen der folgenden Maschinentypen enthalten:

- **Statische Maschinen:** Der Katalog enthält statische Einzelsitzungsmaschinen (diese werden andernorts auch "persönliche", "dedizierte"oder "persistente"Desktops genannt). Statisch bedeutet, dass wenn ein Benutzer einen Desktop startet, dieser zu dem Benutzer "gehört". Alle Änderungen, die der Benutzer an dem Desktop vornimmt, werden bei der Abmeldung beibehalten.

Wenn der Benutzer später zu Citrix Workspace zurückkehrt und einen Desktop startet, handelt es sich um denselben Desktop.

- **Zufällige Maschinen:** Der Katalog enthält zufällige Einzelsitzungsmaschinen (auch "nicht persistente Desktops"). Zufällig bedeutet, dass alle Änderungen, die der Benutzer an dem Desktop vornimmt, nach dem Abmelden verworfen werden. Wenn der Benutzer zu Citrix Workspace zurückkehrt und einen Desktop startet, kann es sich um denselben oder einen anderen Desktop handeln.
- **Multisitzungsmaschinen:** Der Katalog enthält Maschinen mit Apps und Desktops. Auf diese Maschinen können mehrere Benutzer gleichzeitig zugreifen. Die Benutzer können einen Desktop oder Apps von ihrem Workspace aus starten. App-Sitzungen können geteilt werden. Die Sitzungsfreigabe zwischen einer App und einem Desktop ist nicht zulässig.
  - Wenn Sie einen Multisitzungskatalog erstellen, wählen Sie die Arbeitslast aus: leicht (z. B. Dateneingabe), mittel (z. B. Büroanwendungen), hoch (z. B. Maschinenbau) oder benutzerdefiniert. Jede Option steht für eine Anzahl von Maschinen und Sitzungen pro Maschine, woraus sich die Gesamtzahl der von dem Katalog unterstützten Sitzungen ergibt.
  - Wenn Sie die benutzerdefinierte Arbeitslast auswählen, können Sie eine Auswahl aus den verfügbaren Kombinationen aus CPU, RAM und Speicher treffen. Geben Sie die Anzahl von Maschinen und Sitzungen pro Maschine an, woraus sich die Gesamtzahl der von dem Katalog unterstützten Sitzungen ergibt.

Bei der Bereitstellung von Desktops werden die statischen und zufälligen Maschinen manchmal als "Desktoptyp"bezeichnet.

### Möglichkeiten zum Erstellen eines Katalogs mit Quick Deploy

Es gibt mehrere Möglichkeiten, einen Katalog zu erstellen und zu konfigurieren:

- Die **Schnellerstellung** ist der schnellste Einstieg. Sie geben minimale Informationen an und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) kümmert sich um den Rest. Ein per Schnellerstellung erstellter Katalog eignet sich hervorragend für Testumgebungen oder Machbarkeitsstudien.
- Die **benutzerdefinierte Erstellung** enthält mehr Konfigurationsmöglichkeiten als die Schnellerstellung. Sie eignet sich besser für eine Produktionsumgebung als die Schnellerstellung.
- **Remote-PC-Zugriffs-Kataloge** enthalten bestehende (normalerweise physische) Maschinen, auf die die Benutzer remote zugreifen. Weitere Informationen und Anweisungen zu diesen Katalogen finden Sie unter Remote-PC-Zugriff.

Vergleich von Schnellerstellung und benutzerdefinierter Erstellung:

| Schnellerstellung | Benutzerdefinierte Erstellung |
| --- | --- |
| Weniger Informationen anzugeben. | Mehr Informationen anzugeben. |
| Weniger Auswahlmöglichkeiten für einige Features. | Mehr Auswahlmöglichkeiten für einige Features. |
| Von Citrix verwaltete Azure Active Directory-Benutzerauthentifizierung. | Auswahl: von Citrix verwaltetes Azure Active Directory oder eigenes Active Directory/Azure Active Directory. |
| Keine Verbindung zu Ihrem On-Premises-Netzwerk. | Auswahl: Keine Verbindung zu Ihrem On-Premises-Netzwerk, Azure VNet-Peering, SD-WAN. |
| Verwendung eines von Citrix erstellten Windows 10-Images. Das Image enthält einen aktuellen Desktop-VDA. | Auswahl: von Citrix erstellte Images, aus Azure importierte eigene Images oder Images, die Sie in Citrix DaaS aus einem von Citrix erstellten oder importierten Image erstellt haben. |
| Jeder Desktop hat einen Azure-Standarddatenträger (HDD). | Es stehen mehrere Speicheroptionen zur Verfügung. |
| Nur statische Desktops. | Statische, zufällige oder Multisitzungsdesktops. |
| Ein Energieverwaltungszeitplan kann während der Erstellung nicht konfiguriert werden. Die Maschine, die den Desktop hostet, schaltet sich aus, wenn die Sitzung endet. (Sie können diese Einstellung später ändern.) | Ein Energieverwaltungszeitplan kann während der Erstellung konfiguriert werden. (Ein Quick Deploy-Energieverwaltungszeitplan unterscheidet sich von dem über die Schnittstelle für die vollständige Konfiguration erstellten Energieverwaltungszeitplan.) |
| Muss ein Citrix Managed Azure-Abonnement verwenden. | Kann das Citrix Managed Azure-Abonnement oder ein eigenes Azure-Abonnement verwenden. |

Einzelheiten zum Verfahren finden Sie unter:

- Erstellen eines Quick Deploy-Katalogs mit der Schnellerstellung
- Erstellen eines Quick Deploy-Katalogs mit der benutzerdefinierte Erstellung

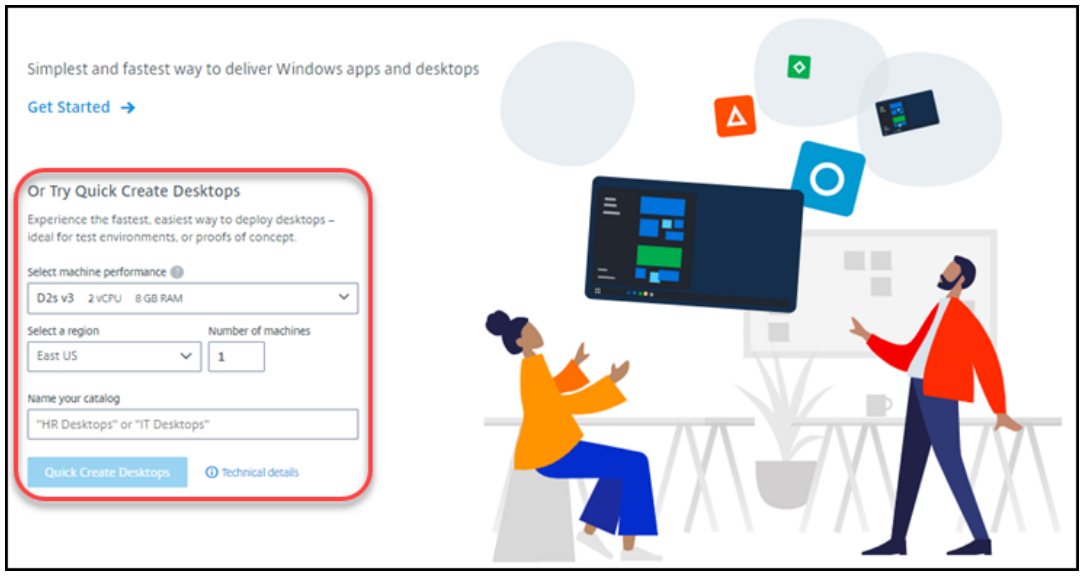
> **Wichtig:**
>
> Wenn Sie zum ersten Mal einen Katalog oder ein Image mit einem Citrix Managed Azure-Abonnement erstellen, müssen Sie den anfallenden Gebühren zustimmen. Erinnerungen an die Zustimmung werden ggf. bei der Erstellung weiterer Kataloge oder Images mit dem Citrix Managed Azure-Abonnement angezeigt.

### Erstellen eines Quick Deploy-Katalogs mit der Schnellerstellung

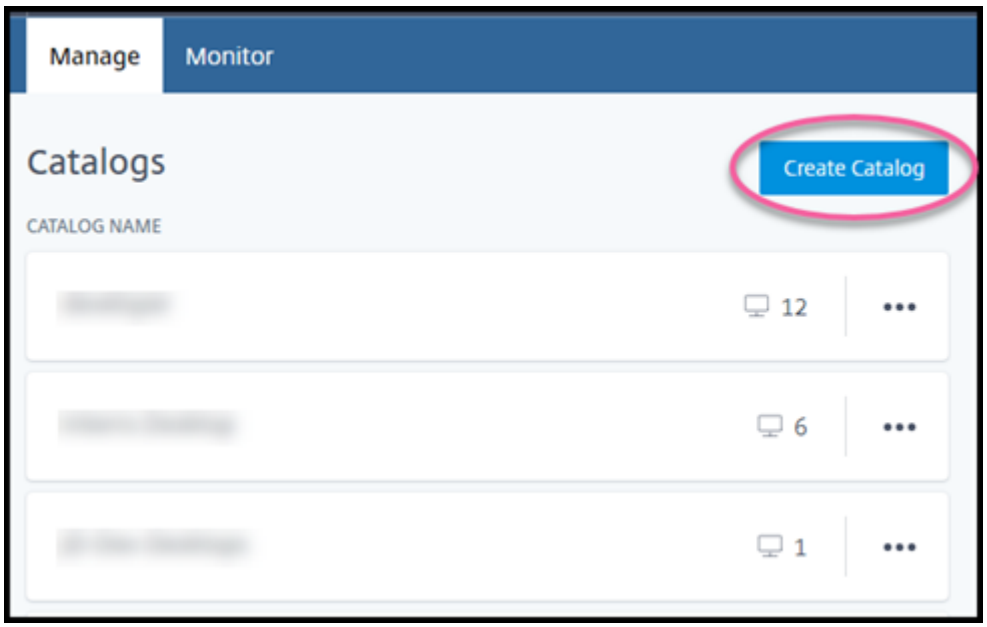
Bei der Schnellerstellung wird ein Katalog mit statischen Maschinen unter Einsatz eines Citrix Managed Azure-Abonnements und eines von Citrix erstellten Windows 10-Images erstellt. Für die Energieverwaltung werden die voreingestellten Werte für "Kostenersparnis"verwendet. Es besteht keine Verbindung zu Ihrem Unternehmensnetzwerk. Die Benutzer müssen mit Citrix Managed Azure AD hinzugefügt werden.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie **Verwalten > Quick Deploy**.
4. Wenn noch kein Katalog erstellt wurde, wird die **Begrüßungsseite** angezeigt. Treffen Sie eine Auswahl:
   - Konfigurieren Sie den Katalog auf dieser Seite. Fahren Sie mit den Schritten 6 bis 10 fort.

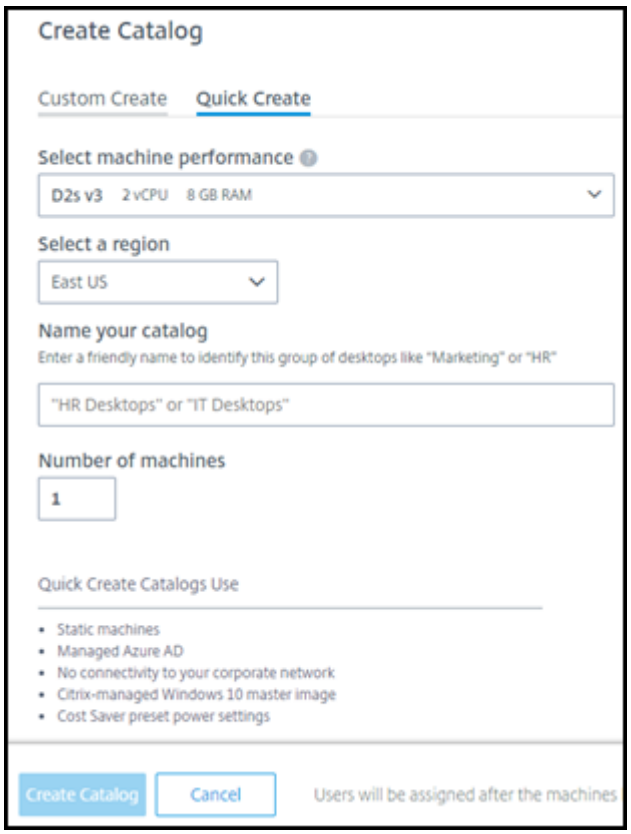



   - Wählen Sie **Erste Schritte** aus. Sie werden zum Dashboard **Verwalten > Quick Deploy** weitergeleitet. Wählen Sie **Katalog erstellen**.
5. Wenn bereits ein Katalog erstellt wurde, werden Sie zum Dashboard **Verwalten > Quick Deploy** weitergeleitet. Wählen Sie **Katalog erstellen**.




6. Wählen Sie oben auf der Seite **Schnellerstellung** (falls die Option noch nicht ausgewählt ist).




- **Maschinenleistung:** Wählen Sie den Maschinentyp aus. Jede Option steht für eine eigene Kombination aus CPU, RAM und Speicher. Maschinen mit höherer Leistung haben höhere monatliche Kosten.
- **Region:** Wählen Sie die Region aus, in der die Maschinen erstellt werden sollen. Sie kön-

nen eine Region in der Nähe der Benutzer auswählen.
- **Name:** Geben Sie einen Namen für den Katalog ein. Dieses Feld ist erforderlich und es gibt keinen Standardwert.
- **Anzahl an Maschinen:** Geben Sie die Anzahl der gewünschten Maschinen ein.

7. Wenn Sie fertig sind, wählen Sie **Katalog erstellen** aus. (Wenn Sie den ersten Katalog über die **Begrüßungsseite** erstellen, wählen Sie **Schnellerstellung von Desktops** aus.)
8. Wenn dies der erste Katalog ist, den Sie mit einem Citrix Managed Azure-Abonnement erstellen, stimmen Sie bei Anzeige der entsprechenden Aufforderung den damit verbundenen Gebühren zu.

Während der Katalog erstellt wird, wird sein Name zur Liste der Kataloge hinzugefügt, was den Fortschritt seiner Erstellung anzeigt.

Citrix DaaS erstellt außerdem automatisch einen Ressourcenstandort mit zwei Citrix Cloud Connectors.

Nachfolgende Schritte:

- Sie können Benutzer zum Managed Azure AD-Verzeichnis hinzufügen, während der Katalog erstellt wird.
- Fügen Sie nach dem Erstellen des Katalogs diesem Benutzer hinzu.

### Erstellen eines Quick Deploy-Katalogs mit der benutzerdefinierte Erstellung

Wenn Sie ein Citrix Managed Azure-Abonnement verwenden und eine Verbindung mit Ihren On-Premises-Netzwerkressourcen verwenden möchten, erstellen Sie die Netzwerkverbindung bevor Sie den Katalog erstellen. Um den Benutzern Zugriff auf Ihre On-Premises- oder andere Netzwerkressourcen zu ermöglichen, benötigen Sie außerdem Active Directory-Informationen für den Standort.

Wenn Sie kein Citrix Managed Azure-Abonnement haben, haben Sie folgende Optionen:

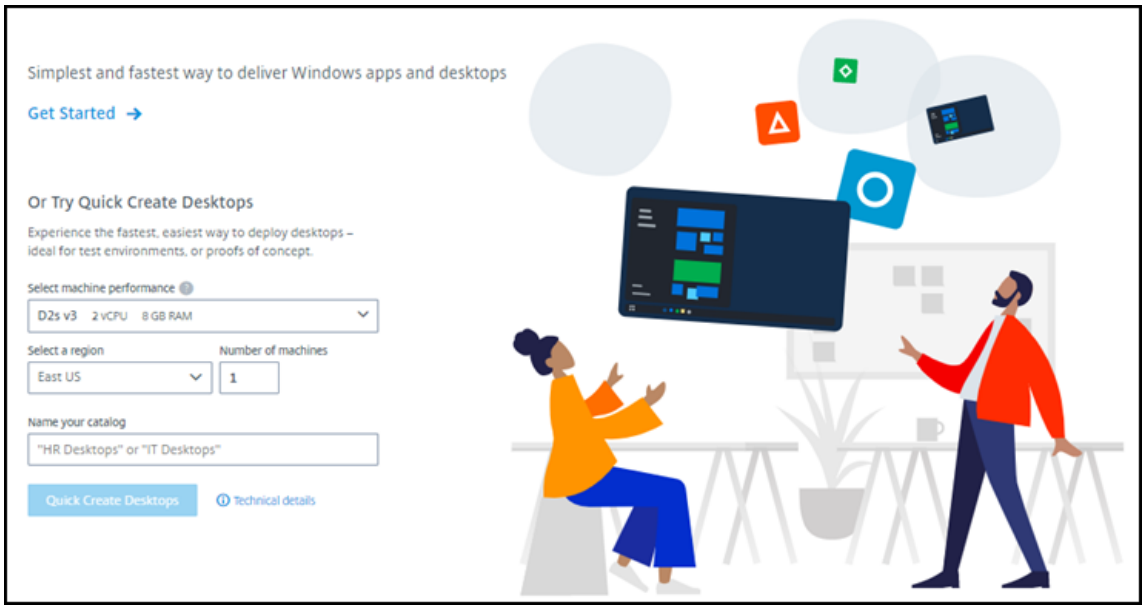
- Bestellen Sie den Azure Consumption Fund über Azure Marketplace, wodurch Sie ein Citrix Managed Azure-Abonnement erhalten.
- Importieren Sie ein oder mehrere eigene Azure-Abonnements in Citrix DaaS und erstellen Sie dann einen Katalog.

Gehen Sie zum Erstellen eines Katalogs wie folgt vor:

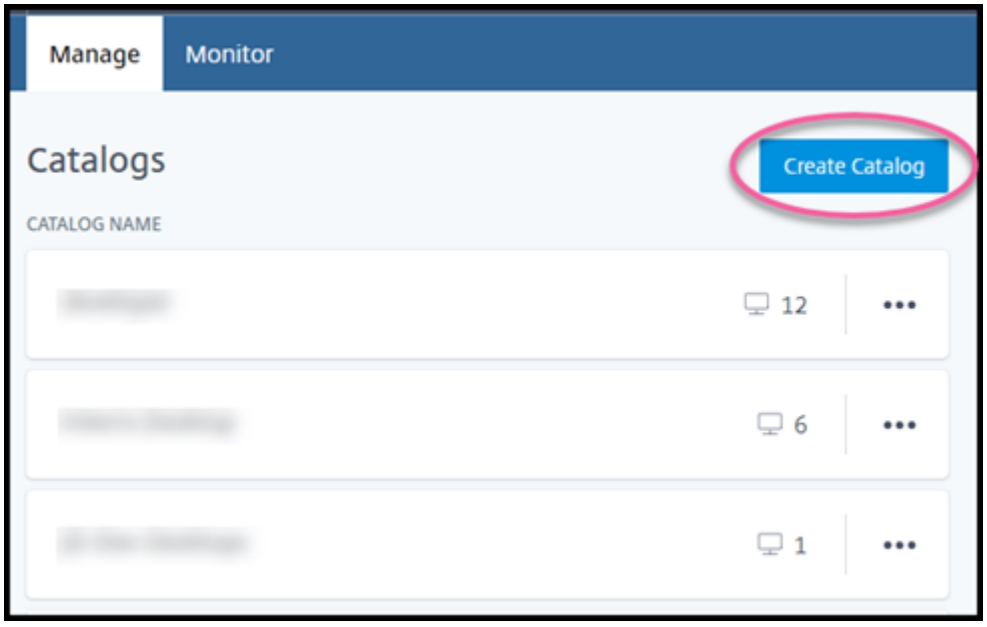
1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie **Verwalten > Quick Deploy**.

4. Wenn noch kein Katalog erstellt wurde, wird die **Begrüßungsseite** angezeigt. Wählen Sie **Erste Schritte** aus. Am Ende der Einführungsseite werden Sie zum Dashboard **Verwalten > Quick Deploy** weitergeleitet. Wählen Sie **Katalog erstellen**.

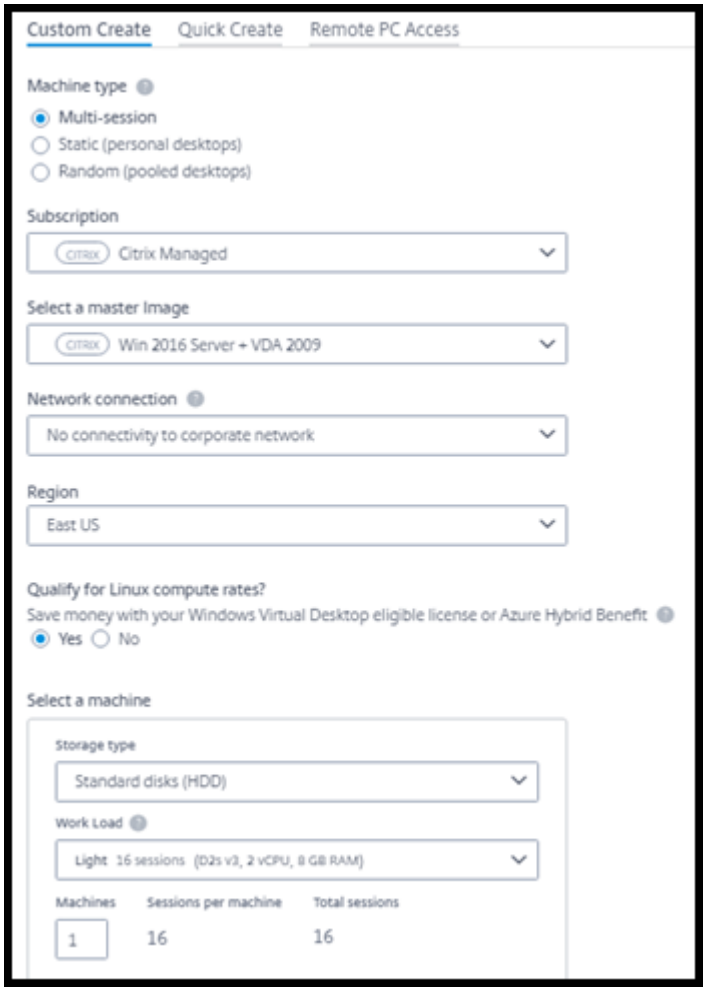



Wenn bereits ein Katalog erstellt wurde, werden Sie zum Dashboard **Verwalten > Quick Deploy** weitergeleitet. Wählen Sie **Katalog erstellen**.




5. Wählen Sie oben auf der Seite **Benutzerdefinierte Erstellung** (falls die Option noch nicht ausgewählt ist).




6. Füllen Sie die folgenden Felder aus. (Einige Felder gelten nur für bestimmte Maschinentypen. Die Feldreihenfolge kann von der hier dargestellten abweichen.)

   - **Maschinentyp:** Wählen Sie einen Maschinentyp. Weitere Informationen finden Sie unter Maschinentypen.
   - **Abonnement:** Wählen Sie ein Azure-Abonnement.
   - **Masterimage:** Wählen Sie ein Betriebssystemimage zur Verwendung für die Maschinen des Katalogs.
   - **Netzwerkverbindung:** Wählen Sie die Netzwerkverbindung, die für den Zugriff auf Ressourcen in Ihrem Netzwerk verwendet werden soll.

     Wenn Sie ein Citrix Managed Azure-Abonnement ausgewählt haben, gibt es folgende Optionen:

     – **Keine Verbindung:** Die Benutzer können nicht auf Standorte und Ressourcen in Ihrem On-Premises-Unternehmensnetzwerk zugreifen.

  - *Verbindungen:* Wählen Sie eine zuvor erstellte Verbindung aus, z. B. ein VNet-Peering- oder SD-WAN-Verbindung.

  Wenn Sie ein vom Kunden verwaltetes Azure-Abonnement ausgewählt haben, wählen Sie die Ressourcengruppe, das virtuelle Netzwerk und das Subnetz aus.

- **Region:** (Nur verfügbar, wenn Sie **Keine Verbindung** für **Netzwerkverbindung**gewählt haben.) Wählen Sie eine Region aus, in der die Desktops erstellt werden sollen. Sie können eine Region in der Nähe der Benutzer auswählen.

  Wenn Sie eine Verbindung in **Netzwerkverbindung** ausgewählt haben, verwendet der Katalog die Region dieses Netzwerks.

- **Qualifizieren Sie sich für Linux-Computetarife?** (Nur verfügbar, wenn Sie ein Windows-Image ausgewählt haben.) Sie können Geld sparen, wenn Sie Ihre Lizenz oder Azure Hybrid Benefit verwenden.

  **Windows Virtual Desktop-Vorteil:** Gültige Windows 10- oder Windows 7-Benutzerlizenzen für:

  - Microsoft 365 E3/ES
  - Microsoft 365 A3/AS/Student Use Benefits
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Enterprise E3/E5
  - Windows 10 Education A3/A5
  - Windows 10 VDA pro Benutzer

  Benutzer- oder Gerätelizenz (RDS CAL) mit Software Assurance für Windows Server-Workloads.

  **Azure-Hybridvorteil:** Windows Server-Lizenzen mit aktiver Software Assurance oder den entsprechenden berechtigten Abonnementlizenzen. Siehe https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Maschine:**

  - **Speichertyp:** HDD oder SSD.
  - **Maschinenleistung** (für **statische** oder **zufällige** Maschinen) bzw. **Workload** (für Multisitzungsmaschinen). Es stehen nur Optionen zur Auswahl, die der Generation (Gen1 oder Gen2) des ausgewählten Images entsprechen.

    Wenn Sie die benutzerdefinierte Workload auswählen, geben Sie die Anzahl Maschinen und Sitzungen pro Maschine in das Feld **Maschinenleistung** ein.
  - **Maschinen**. Anzahl der Maschinen im Katalog.

- **Maschinenbenennungsschema:** Siehe Maschinenbenennungsschema.

- **Name:** Geben Sie einen Namen für den Katalog ein. Der Name wird im Dashboard **Verwalten** angezeigt.
- **Energiezeitplan:** Standardmäßig ist das Kontrollkästchen **Später konfigurieren** aktiviert. Einzelheiten finden Sie unter Energieverwaltungszeitpläne. (Dieser Energieverwaltungszeitplan unterscheidet sich von den Energieverwaltungsfeatures in der Verwaltungsoberfläche "Vollständige Konfiguration"von Citrix DaaS.)
- **Mitglied der lokalen Domäne (Active Directory) werden?** (Nur verfügbar, wenn Sie eine Azure VNet-Peeringverbindung für **Netzwerkverbindung** ausgewählt haben.) Wählen Sie **Ja** oder **Nein**. Wenn Sie **Ja** auswählen, geben Sie Folgendes ein:
  - FQDN der Domain (zum Beispiel Contoso.com).
  - Organisationseinheit: Um die Standard-OU (Computer) zu verwenden, lassen Sie dieses Feld leer.
  - Citrix DaaS-Kontoname: Muss ein Domänen- oder Unternehmensadministrator im Format "name@domäne"oder "domäne\name"sein.
  - Kennwort für den Citrix DaaS-Kontonamen.
- **Erweiterte Einstellungen:** Siehe Einstellungen für den Ressourcenstandort beim Erstellen eines Katalogs.

7. Wenn Sie fertig sind, wählen Sie **Katalog erstellen** aus.
8. Wenn dies der erste Katalog ist, den Sie mit einem Citrix Managed Azure-Abonnement erstellen, stimmen Sie bei Anzeige der entsprechenden Aufforderung den damit verbundenen Gebühren zu.

Im Dashboard **Verwalten > Quick Deploy** wird angezeigt, wenn der Katalog erstellt ist. Citrix DaaS erstellt außerdem automatisch einen Ressourcenstandort mit zwei Citrix Cloud Connectors.

Nachfolgende Schritte:

- Wenn Sie dies noch nicht getan haben, konfigurieren Sie die Authentifizierungsmethode für die Anmeldung der Benutzer bei Citrix Workspace.
- Fügen Sie nach dem Erstellen des Katalogs diesem Benutzer hinzu.
- Wenn Sie einen Multisitzungskatalog erstellt haben fügen Sie Anwendungen hinzu (vor oder nach dem Hinzufügen von Benutzern).

### Einstellungen für den Ressourcenstandort beim Erstellen eines Katalogs

Beim Erstellen eines Katalogs können Sie optional mehrere Ressourcenstandorteinstellungen konfigurieren.

Wenn Sie im Dialogfeld zur Katalogerstellung **Erweiterte Einstellungen** auswählen, ruft Citrix DaaS die Informationen zum Ressourcenstandort ab.

- Wenn Sie bereits einen Ressourcenstandort für die für den Katalog ausgewählte Domäne und Netzwerkverbindung haben, können Sie ihn für den Katalog speichern.

  Besitzt der Ressourcenstandort nur einen Cloud Connector, wird automatisch ein zweiter installiert. Sie können optional erweiterte Einstellungen für den Cloud Connector angeben, den Sie hinzufügen.

- Wenn Sie keinen Ressourcenstandort für die für den Katalog ausgewählte Domäne und Netzwerkverbindung eingerichtet haben, werden Sie aufgefordert, einen zu konfigurieren.

Konfigurieren Sie erweiterte Einstellungen:

- (Nur erforderlich, wenn der Ressourcenstandort bereits eingerichtet ist.) Name für den Ressourcenstandort.
- Typ der externen Verbindung: über den Citrix Gateway-Dienst oder aus Ihrem Unternehmensnetzwerk.
- Cloud Connector-Einstellungen:
  - (Nur verfügbar, wenn Sie ein vom Kunden verwaltetes Azure-Abonnement verwenden) Maschinenleistung. Diese Auswahl wird für die Cloud Connectors am Ressourcenstandort verwendet.
  - (Nur verfügbar, wenn Sie ein vom Kunden verwaltetes Azure-Abonnement verwenden) Azure-Ressourcengruppe. Diese Auswahl wird für die Cloud Connectors am Ressourcenstandort verwendet. Der Standardwert ist die zuletzt vom Ressourcenstandort verwendete Ressourcengruppe (falls zutreffend).
  - Organisationseinheit (OU) Der Standardwert ist die zuletzt vom Ressourcenstandort verwendete OU (falls zutreffend).

Wenn Sie fertig sind, wählen Sie **Speichern**, um zum Dialogfeld zur Katalogerstellung zurückzukehren.

Nachdem Sie einen Katalog erstellt haben, stehen mehrere Aktionen für den Ressourcenstandort zur Verfügung. Weitere Informationen finden Sie unter Aktionen für Ressourcenstandorte.

### Maschinenbenennungsschema

Um beim Erstellen eines Katalogs ein Maschinenbenennungsschema anzugeben, wählen Sie **Maschinenbenennungsschema angeben** aus. Verwenden Sie 1–4 Platzhaltern (Rauten), um die Position fortlaufender Zahlen oder Buchstaben im Namen anzugeben. Regeln:

- Das Benennungsschema muss mindestens einen und maximal vier Platzhalter enthalten. Alle Platzhalter müssen zusammen sein.

- Der gesamte Name, einschließlich Platzhaltern, muss zwischen 2 und 15 Zeichen lang sein.
- Der Name darf Folgendes nicht enthalten: Leerzeichen, Schrägstriche, umgekehrte Schrägstriche, Doppelpunkte, Sternchen, spitze Klammern, Pipes, Kommas, Tilden, Ausrufezeichen, @-Zeichen, Dollarzeichen, Prozentzeichen, Caretzeichen, runde Klammern, geschweifte Klammern und Unterstriche.
- Der Name darf nicht mit einem Punkt beginnen.
- Der Name darf nicht ausschließlich Zahlen enthalten.
- Verwenden Sie am Ende des Namens nicht die folgenden Buchstaben: `-GATEWAY`, `-GW` und `-TAC`.

Geben Sie an, ob es sich bei den sequentiellen Werten um Zahlen (0–9) oder Buchstaben (A–Z) handelt.

Beispiel: Das Benennungsschema `PC-Sales-##` (und Aktivieren von **0-9**) bewirkt eine Benennung der Computerkonten als `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03` usw.

Lassen Sie genug Platz für Wachstum.

- Ein Benennungsschema mit 2 Platzhaltern und 13 anderen Zeichen (z. B. `MachineSales-##`) verwendet beispielsweise die maximale Anzahl von Zeichen (15).
- Wenn der Katalog 99 Maschinen enthält, schlägt die nächste Maschinenerstellung fehl. Citrix DaaS versucht, eine Maschine mit drei Ziffern (100) zu erstellen, doch dadurch würde ein Name mit 16 Zeichen erzeugt. Das Maximum beträgt 15.
- In diesem Beispiel ermöglicht daher ein kürzerer Name (z. B. `PC-Sales-##`) ein Wachstum über 99 Maschinen hinaus.

Wenn Sie kein Maschinenbenennungsschema angeben, verwendet Citrix DaaS das Standardbenennungsschema `DAS%%%%%-**-###`.

- `%%%%%` = fünf zufällige alphanumerische Zeichen, die dem Präfix des Ressourcenstandorts entsprechen
- `**` = zwei zufällige alphanumerische Zeichen für den Katalog
- `###` = drei Ziffern.

### Verwandte Informationen

- Remote-PC-Zugriff-Kataloge
- Erstellen eines Katalogs in einem Netzwerk mit Proxyserver
- Anzeigen von Kataloginformationen
- Kataloge in Quick Deploy verwalten

# Verwalten von Katalogen in Quick Deploy

April 19, 2022

In diesem Artikel werden die Verwaltungsaufgaben für in Quick Deploy erstellte Kataloge beschrieben.

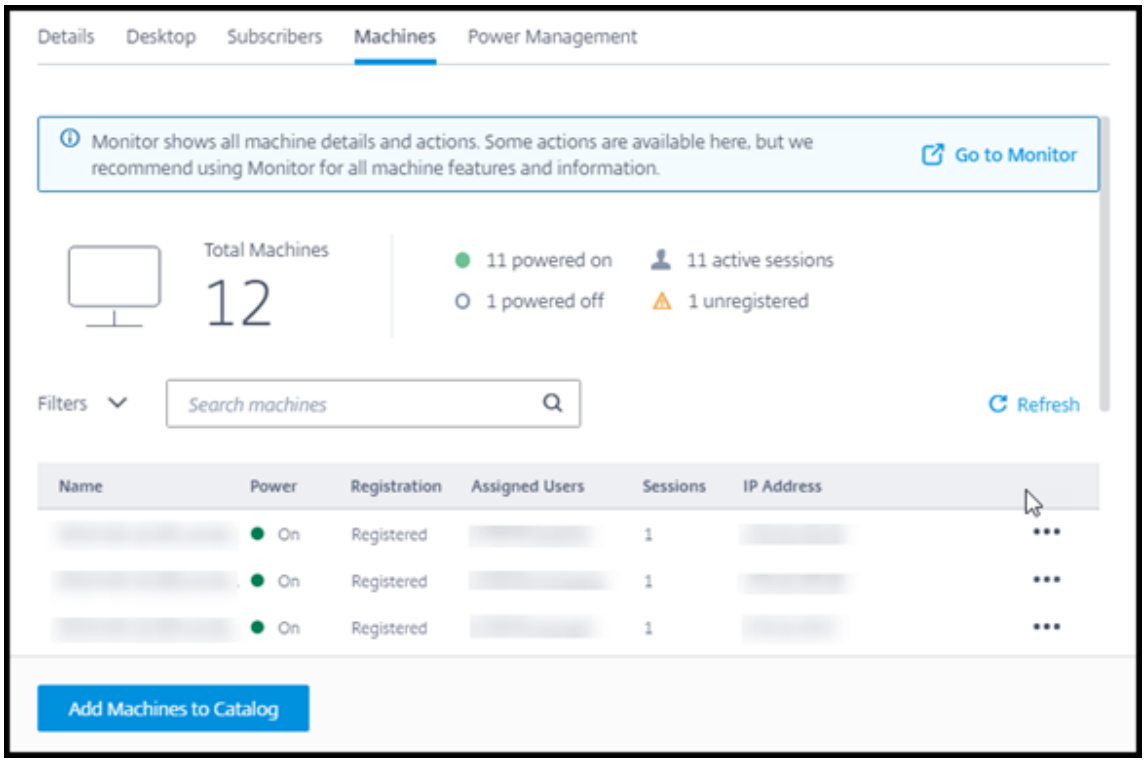
Nicht vergessen: Wenn Sie einen Katalog mit Quick Deploy erstellen und diesen dann über die Schnittstelle "Vollständige Konfiguration"verwalten, können Sie die Quick Deploy-Schnittstelle für diesen Katalog nicht mehr verwenden.

(Informationen zum Verwalten von Katalogen mit der Schnittstelle "Vollständige Konfiguration" finden Sie unter Verwalten von Maschinenkatalogen.)

## Hinzufügen von Maschinen zum Maschinenkatalog

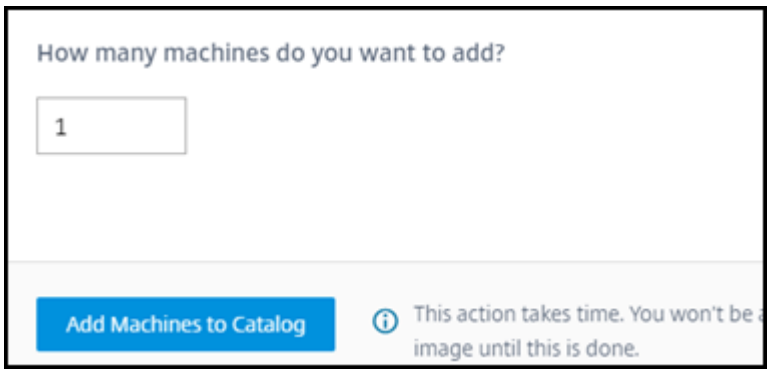
Während Maschinen einem Quick Deploy-Katalog hinzugefügt werden, können Sie keine weiteren Änderungen an diesem Katalog vornehmen.

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Wählen Sie auf der Registerkarte **Maschinen** die Option **Maschinen zu Katalog hinzufügen**.




3. Geben Sie die Anzahl der Maschinen ein, die Sie dem Katalog hinzufügen möchten.




4. (Gilt nur für domänengebundene Kataloge.) Geben Sie den Benutzernamen und das Kennwort für das Citrix DaaS-Konto (ehemals Citrix Virtual Apps and Desktops Service) ein.
5. Wählen Sie **Maschinen zu Katalog hinzufügen**.

Sie können die Maschinenanzahl für einen Katalog nicht reduzieren. Sie können jedoch über die Einstellungen für Energieverwaltungszeitpläne steuern, wie viele Maschinen eingeschaltet sind, oder einzelne Maschinen auf der Registerkarte **Maschinen** löschen. Informationen zum Löschen von Maschinen von der Registerkarte **Maschinen** finden Sie unter Verwalten von Maschinen in einem Katalog.

### Ändern der Anzahl Sitzungen pro Maschine

Das Ändern der Anzahl Sitzungen pro Multisitzungsmaschine kann sich auf die Benutzererfahrung auswirken. Eine Erhöhung des Werts kann die Rechenressourcen reduzieren, die gleichzeitigen Sitzungen zugewiesen sind.

Empfehlung: Ermitteln Sie das geeignete Gleichgewicht zwischen Benutzererfahrung und Kosten anhand der Nutzungsdaten.

1. Wählen Sie unter **Verwalten > Quick Deploy** einen Katalog mit Multisitzungsmaschinen aus.
2. Wählen Sie auf der Registerkarte **Details** neben **Sitzungen pro Maschine** die Option **Bearbeiten**.
3. Geben Sie eine neue Anzahl an Sitzungen pro Maschine ein.
4. Wählen Sie **Anzahl an Sitzungen aktualisieren**.
5. Bestätigen Sie Ihre Anforderung.

Diese Änderung wirkt sich nicht auf aktuelle Sitzungen aus. Wenn Sie die maximale Anzahl an Sitzungen in einen Wert ändern, der niedriger ist als die aktuell aktiven Sitzungen einer Maschine, wird der neue Wert durch den normalen Schwund aktiver Sitzungen implementiert.

Wenn vor Beginn der Aktualisierung ein Fehler auftritt, behält die Anzeige **Details** des Katalogs die richtige Anzahl Sitzungen bei. Wenn während der Aktualisierung ein Fehler auftritt, gibt die Anzeige die Anzahl der gewünschten Sitzungen an.

### Verwalten von Maschinen in einem Katalog

> **Hinweis:**
>
> Viele der unter **Verwalten > Quick Deploy** verfügbaren Aktionen sind auch auf der Registerkarte **Überwachen** in Quick Deploy verfügbar.

Gehen Sie zum Auswählen von Aktionen unter **Verwalten > Quick Deploy** folgendermaßen vor:

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Suchen Sie auf der Registerkarte **Maschinen** die Maschine, die Sie verwalten möchten. Wählen Sie im Menü für die Maschine die gewünschte Aktion aus:

   - **Neustart:** Startet die Maschine neu.
   - **Starten:** Startet die Maschine. Diese Aktion ist nur verfügbar, wenn die Maschine ausgeschaltet ist.
   - **Herunterfahren:** Fährt die Maschine herunter. Diese Aktion ist nur verfügbar, wenn die Maschine eingeschaltet ist.
   - **Wartungsmodus ein-/ausschalten:** Schaltet den Wartungsmodus für die ausgewählte Maschine ein (falls ausgeschaltet) bzw. aus (falls eingeschaltet). Standardmäßig ist der Wartungsmodus ausgeschaltet.

     Durch das Aktivieren des Wartungsmodus wird verhindert, dass neue Verbindungen mit der Maschine hergestellt werden. Die Benutzer können sich mit Sitzungen auf der Maschine verbinden, auf ihr aber keine neuen Sitzungen starten.

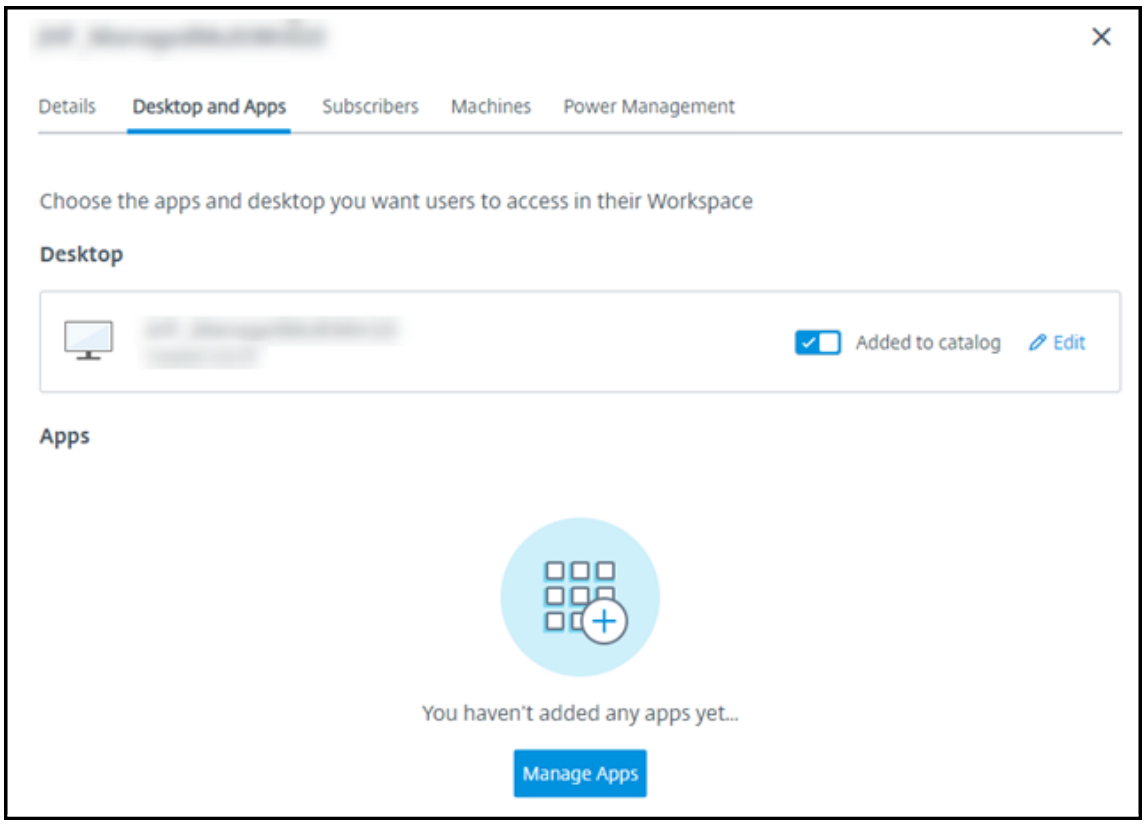
     Möglicherweise möchten Sie eine Maschine in den Wartungsmodus versetzen, bevor Sie einen Patch anwenden oder ein Problem behandeln.
   - **Löschen:** Löscht die Maschine. Diese Aktion ist nur verfügbar, wenn die Sitzungsanzahl Null ist. Bestätigen Sie die Löschung.

     Wenn eine Maschine gelöscht wird, werden alle Daten auf ihr entfernt.
   - **Neustart erzwingen:** Erzwingt einen Neustart der Maschine. Wählen Sie diese Aktion nur aus, wenn die Aktion **Neustart** fehlschlägt.

### Hinzufügen von Apps zu einem Katalog

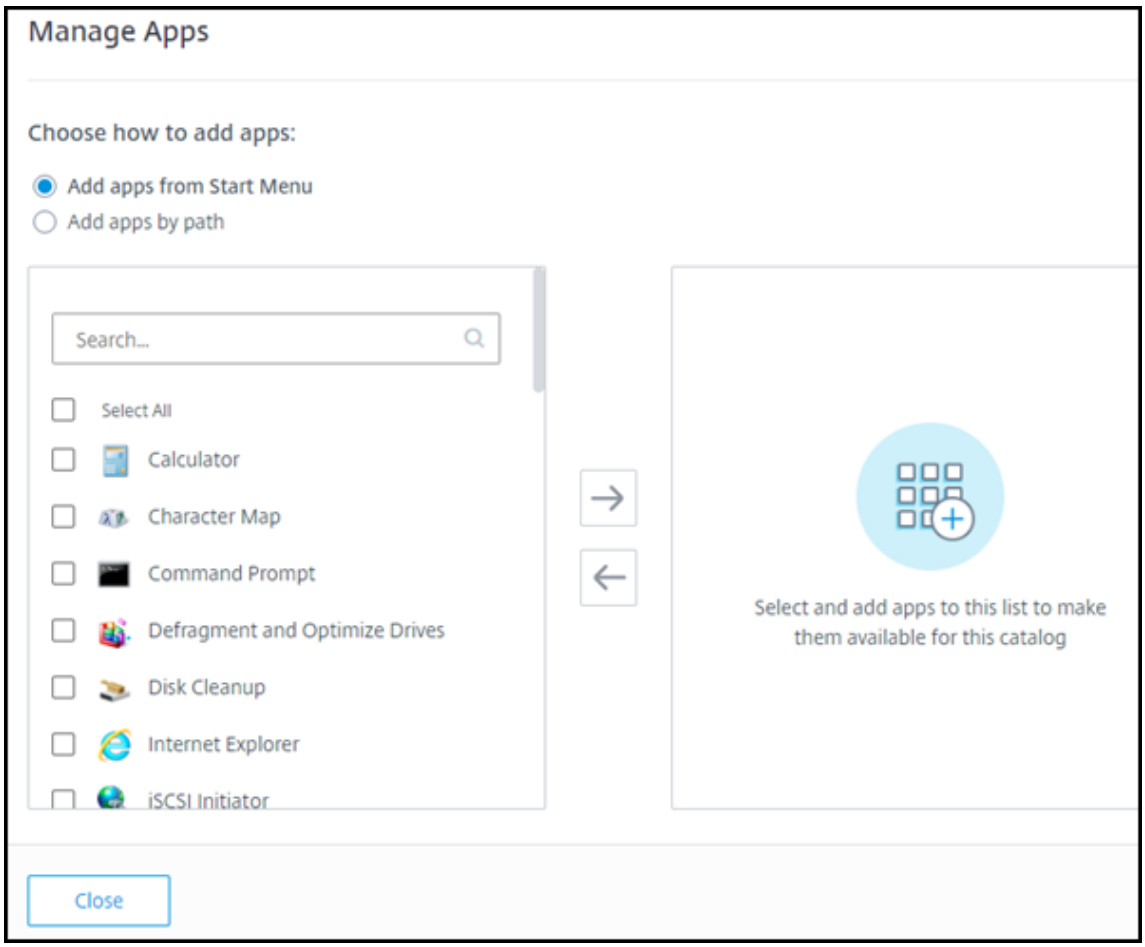
1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Wählen Sie auf der Registerkarte **Desktop und Apps** die Option **Apps verwalten**.




3. Wählen Sie aus, wie Sie Apps hinzufügen möchten: Über das Menü **Start** der Maschinen im Katalog oder aus einem anderen Pfad auf den Maschinen.
4. So fügen Sie Apps über das **Startmenü** hinzu:

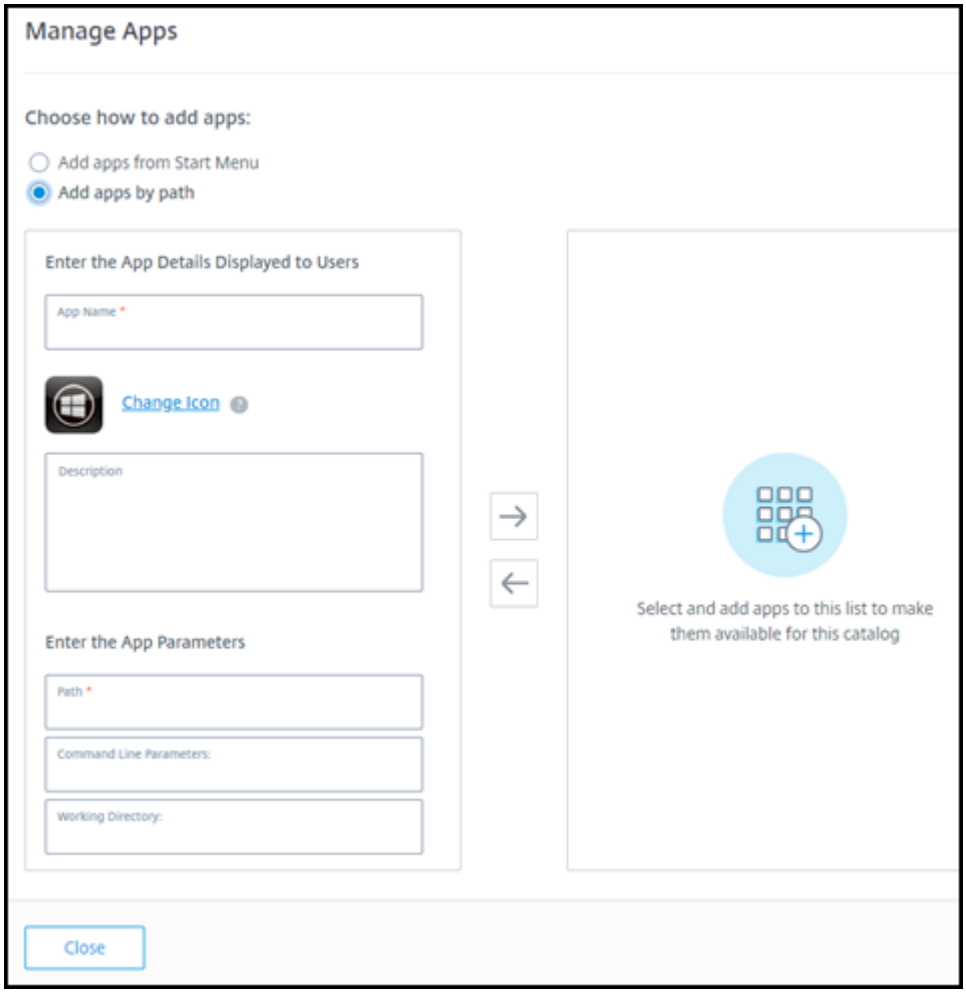
 




- Wählen Sie in der linken Spalte verfügbare Apps aus. (Verwenden Sie die **Suche**, um die App-Liste anzupassen.) Wählen Sie den Pfeil nach rechts zwischen den Spalten. Die ausgewählten Apps werden in die rechte Spalte verschoben.
- Um Apps zu entfernen, wählen Sie sie in der rechten Spalte aus. Wählen Sie den Pfeil nach links zwischen den Spalten.
- Wenn das **Startmenü** mehr als eine Version einer App mit demselben Namen enthält, können Sie nur eine hinzufügen. Um eine weitere Version dieser App hinzuzufügen, ändern Sie deren Namen. Dann können Sie die Version der App hinzufügen.

5. Hinzufügen von Apps nach Pfad:




- Geben Sie den Namen für die App ein. Dieser wird den Benutzer in Citrix Workspace angezeigt.
- Das angezeigte Symbol ist dasjenige, das die Benutzer in Citrix Workspace sehen. Um ein anderes Symbol auszuwählen, wählen Sie **Symbol ändern** und gehen Sie zu dem gewünschten Symbol.
- Geben Sie optional eine Beschreibung der Anwendung ein.
- Geben Sie den Pfad zur App ein. Dieses Feld ist erforderlich. Fügen Sie optional Befehlszeilenparameter und das Arbeitsverzeichnis hinzu. Details zu Befehlszeilenparametern finden Sie unter Übergeben von Parametern an veröffentlichte Anwendungen.

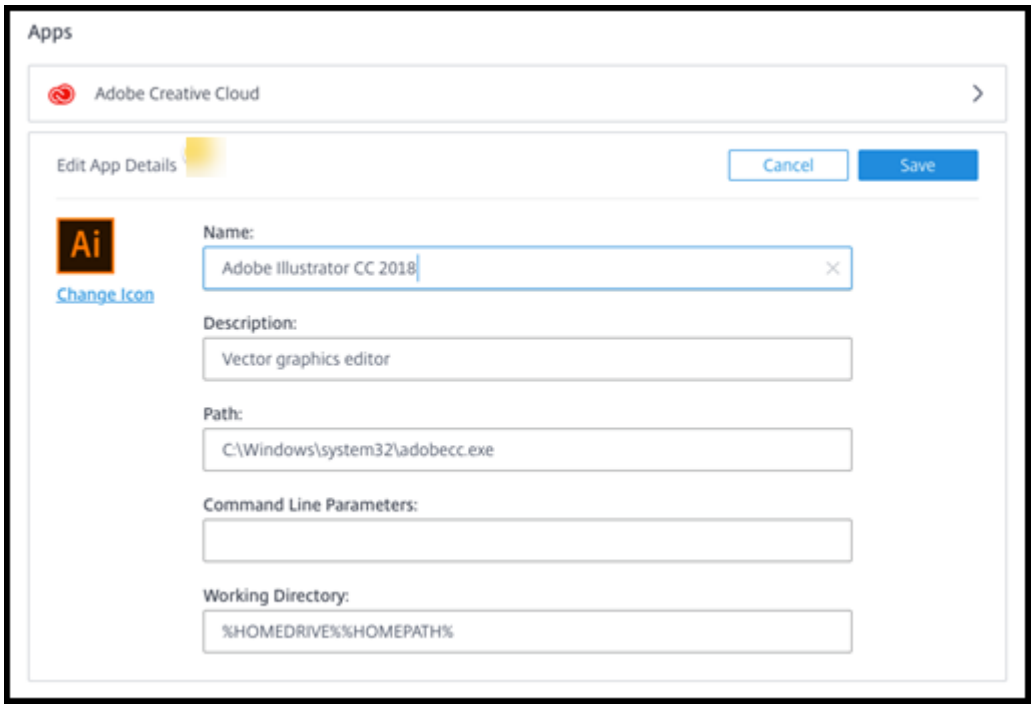
6. Wenn Sie fertig sind, wählen Sie **Schließen**.

Bei VDAs mit Windows Server 2019 werden einige Anwendungssymbole während der Konfiguration und im Workspace des Benutzers möglicherweise nicht korrekt angezeigt. Als Workaround können Sie nach der Veröffentlichung die App bearbeiten und mit dem Feature **Symbol ändern** ein fehlerfrei angezeigtes Symbol zuweisen.

### Bearbeiten einer App in einem Katalog

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Klicken Sie auf der Registerkarte **Desktop und Apps** auf eine beliebige Stelle in der Zeile mit der App, die Sie bearbeiten möchten.
3. Wählen Sie das Stiftsymbol aus.




4. Geben Sie nach Bedarf Änderungen in die folgenden Felder ein:
   - **Name:** Name, der in Citrix Workspace angezeigt wird.
   - **Beschreibung**
   - **Pfad:** Der Pfad zur ausführbaren Datei.
   - **Befehlszeilenparameter:** Details finden Sie unter Übergeben von Parametern an veröffentlichte Anwendungen.
   - **Arbeitsverzeichnis**
5. Um das Symbol in Citrix Workspace angezeigte Symbol zu ändern, wählen Sie **Symbol ändern** und gehen Sie zu dem gewünschten Symbol.
6. Wenn Sie fertig sind, wählen Sie **Speichern**.

#### Übergeben von Parametern an veröffentlichte Anwendungen

Wenn Sie einer veröffentlichten Anwendung bestimmte Dateitypen zuordnen, werden die Prozentzeichen und Sternchen (in Anführungszeichen) an das Ende der Anwendungsbefehlszeile angehängt.

Diese Symbole sind Platzhalter für Parameter, die an Benutzergeräte übergeben werden.

- Sollte eine veröffentlichte Anwendung nicht wunschgemäß starten, prüfen Sie, ob in der Befehlszeile die richtigen Zeichen eingetragen sind. Standardmäßig werden die von Benutzergeräten angegebenen Parameter validiert, wenn die Zeichen angehängt werden.

  Veröffentlichten Anwendungen, die benutzerdefinierte Parameter verwenden, die vom Benutzergerät bereitgestellt werden, werden die Zeichen an die Befehlszeile angehängt, damit die Befehlszeilenüberprüfung übersprungen wird. Sollte die Befehlszeile der betreffenden Anwendung diese Zeichen nicht enthalten, können Sie sie manuell hinzufügen.

- Wenn der Pfad zur ausführbaren Datei der Anwendung Verzeichnisnamen mit Leerzeichen enthält (z. B. `"C:\Program Files"`), setzen Sie die Befehlszeile der Anwendung in Anführungszeichen, um anzuzeigen, dass das Leerzeichen zur Befehlszeile gehört. Setzen Sie vor und nach dem Pfad sowie vor und nach den Prozentzeichen und Sternchen Anführungszeichen. Zwischen dem Anführungszeichen nach dem Pfad und dem Anführungszeichen vor einem Prozentzeichen bzw. Sternchen muss ein Leerzeichen stehen.

  Die Befehlszeile für die veröffentlichte Anwendung Windows Media Player wäre beispielsweise: `"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"`

### Entfernen von Apps aus einem Katalog

Wenn Sie eine App aus einem Katalog entfernen, wird sie nicht von den Maschinen entfernt. Sie wird lediglich nicht mehr in Citrix Workspace angezeigt.

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Wählen Sie auf der Registerkarte **Desktop und Apps** das Papierkorbsymbol neben den Apps aus, die Sie entfernen möchten.

### Löschen eines Katalogs

Wenn Sie einen Katalog löschen, werden alle Maschinen im Katalog dauerhaft zerstört. Das Löschen eines Katalogs kann nicht rückgängig gemacht werden.

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Wählen Sie auf der Registerkarte **Details** den Eintrag **Katalog löschen**.
3. Bestätigen Sie die Löschung.

Um die restlichen Active Directory-Maschinenkonten zu identifizieren, die Sie löschen müssen, können Sie eine Liste der Maschinen- und Cloud Connector-Namen herunterladen.

## Verwalten von Energieverwaltungszeitplänen

Ein Energieverwaltungszeitplan wirkt sich auf alle Maschinen in einem Katalog aus. Zeitpläne bieten Folgendes:

- Optimale Benutzererfahrung: Die Maschinen stehen den Benutzern dann zur Verfügung, wenn sie benötigt werden.
- Sicherheit: Desktopsitzungen, die eine bestimmte Zeit lang im Leerlauf sind, werden getrennt, sodass die Benutzer eine neue Sitzung in ihrem Workspace starten müssen.
- Kostenmanagement und Energieeinsparungen: Maschinen mit Desktops, die länger im Leerlauf sind, werden ausgeschaltet. Die Maschinen werden gemäß dem geplanten und tatsächlichen Bedarf eingeschaltet.

Sie können einen Energiezeitplan konfigurieren, wenn Sie einen benutzerdefinierten Katalog erstellen, oder auch später. Wenn kein Zeitplan ausgewählt oder konfiguriert ist, schalten sich Maschinen ab, wenn eine Sitzung endet.

Sie können keinen Energiesparplan auswählen oder konfigurieren, wenn Sie einen Katalog per Schnellerstellung erstellen. Standardmäßig wird bei der Schnellerstellung die Voreinstellung “Kostenersparnis”verwendet. Sie können später einen anderen Zeitplan für solche Kataloge auswählen oder konfigurieren.

Die Zeitplanverwaltung umfasst Folgendes:

- Wissen, welche Informationen ein Zeitplan enthält
- Erstellen eines Zeitplans

### Informationen in einem Zeitplan

Das folgende Diagramm zeigt die Zeitplaneinstellungen für einen Katalog mit Multisitzungsmaschinen. Die Einstellungen für Kataloge mit Multisitzungsmaschinen (zufällige oder statische Maschinen) unterscheiden sich geringfügig.


Ein Energieverwaltungszeitplan enthält die folgenden Informationen.

**Voreingestellte Zeitpläne** Citrix DaaS bietet mehrere voreingestellte Zeitpläne. Sie können auch eigene Zeitpläne konfigurieren und speichern. Sie können benutzerdefinierte Zeitpläne löschen, nicht aber die von Citrix bereitgestellten.

**Zeitzone** Wird mit der Einstellung "Maschinen einschalten"verwendet, um Arbeitszeiten und arbeitsfreie Zeiten basierend auf der ausgewählten Zeitzone festzulegen.

Die Einstellung gilt für alle Maschinentypen.

**Maschinen einschalten: Arbeitszeit und Nach Geschäftsschluss** Die Wochentage und Anfangs- und Endzeit der Arbeitszeit. Diese bestimmen in der Regel die Intervalle, in denen Maschinen eingeschaltet sein sollen. Zeiten außerhalb dieser Intervalle gelten als arbeitsfreie Zeit. Mehrere Zeitplaneinstellungen ermöglichen das Festlegen eigener Werte für "Arbeitszeit"und "Nach Geschäftsschluss". Andere Einstellungen gelten ständig.

Die Einstellung gilt für alle Maschinentypen.

**Desktopsitzungen im Leerlauf trennen** Zeitspanne, die ein Desktop im Leerlauf bleiben kann (nicht verwendet wird), bevor die Sitzung getrennt wird. Wenn eine Sitzung getrennt wurde, muss der Benutzer zu Workspace gehen und einen neuen Desktop starten. Dies ist eine Sicherheitseinstellung.

Die Einstellung gilt für alle Maschinentypen. Eine Einstellung gilt ständig.

**Desktops im Leerlauf ausschalten** Zeitspanne, die eine Maschine getrennt bleiben kann, bevor sie ausgeschaltet wird. Wenn eine Maschine ausgeschaltet wurde, muss der Benutzer zu Workspace gehen und einen neuen Desktop starten. Dies ist eine Energiespareinstellung.

Beispiel: Sie legen fest, dass Desktops nach 10 Minuten Leerlauf getrennt werden. Nach weiteren 15 Minuten wird die betroffene Maschinen ausgeschaltet, sofern keine Wiederverbindung erfolgt.

Verlässt ein Benutzer seinen Desktop und geht zu einem einstündigen Meeting, wird der Desktop nach 10 Minuten getrennt. Nach weiteren 15 Minuten wird die Maschine ausgeschaltet (insgesamt 25 Minuten).

Aus Sicht des Benutzers haben die beiden Leerlauf-Einstellungen (Trennen und Ausschalten) den gleichen Effekt. Egal, ob sich der Benutzer im Beispiel zwölf Minuten oder eine Stunde von seinem Desktop entfernt, muss er erneut einen Desktop von Workspace aus starten. Der Unterschied der beiden Timer betrifft den Status der virtuellen Maschine, die den Desktop bereitstellt.

Diese Einstellung gilt für Einzelsitzungsmaschinen (statische oder zufällige Maschinen). Sie können Werte für "Arbeitszeit"und "Nach Geschäftsschluss"eingeben.

**Getrennte Sitzungen abmelden** Zeitspanne, die eine Maschine getrennt bleiben kann, bevor sie ausgeschaltet wird.

Diese Einstellung gilt für Multisitzungsmaschinen. Eine Einstellung gilt ständig.

**Ausschaltverzögerung** Mindestzeitspanne, die eine Maschine eingeschaltet bleiben muss, bevor sie ausgeschaltet werden kann (in Kombination mit anderen Kriterien). Diese Einstellung verhindert, dass Maschinen bei schnell wechselnden Sitzungsanforderungen ständig ein- und ausgeschaltet werden.

Diese Einstellung gilt für Multisitzungsmaschinen und wird ständig angewendet.

**Mindestanzahl laufender Maschinen** Anzahl Maschinen, die eingeschaltet bleiben, unabhängig davon, wie lange sie im Leerlauf oder getrennt sind.

Diese Einstellung gilt für zufällige und Multisitzungsmaschinen. Sie können Werte für "Arbeitszeit" und "Nach Geschäftsschluss"eingeben.

**Kapazitätspuffer** Ein Kapazitätspuffer mit Maschinen, die eingeschaltet bleiben, hilft, plötzliche Bedarfsspitzen zu bewältigen. Der Puffer wird als Prozentsatz des aktuellen Sitzungsbedarfs angegeben. Bei 100 aktiven Sitzungen und einem Kapazitätspuffer von 10 % bietet Citrix DaaS beispielsweise eine Kapazität von 110 Sitzungen. Bedarfsspitzen können während der Arbeitszeit oder beim Hinzufügen neuer Maschinen zum Katalog auftreten.

Ein geringerer Wert senkt die Kosten. Ein höherer Wert trägt dazu bei, eine optimierte Benutzererfahrung sicherzustellen. Beim Sitzungsstart müssen die Benutzer nicht warten, bis zusätzliche Maschine eingeschaltet werden.

Sind mehr als genügend Maschinen für einen Katalog eingeschaltet (laut Zeitplan und einschließlich Puffer), werden überzählige Maschinen ausgeschaltet. Das Ausschalten kann aufgrund des Arbeitszeitendes, von Sitzungsabmeldungen oder weniger Maschinen im Katalog auftreten. Der Mechanismus zum Ausschalten einer Maschine muss die folgenden Kriterien erfüllen:

- Die Maschine ist eingeschaltet und nicht im Wartungsmodus.
- Die Maschine ist als verfügbar registriert oder wartet auf die Registrierung nach dem Einschalten.
- Die Maschine hat keine aktiven Sitzungen. Alle verbleibenden Sitzungen wurden beendet. (Die Maschine war für die Leerlaufzeitspanne im Leerlauf.)
- Die Maschine war mindestens X Minuten lang eingeschaltet, wobei X die für den Katalog festgelegte Ausschaltverzögerung ist.

  Wenn alle Maschinen eines statischen Katalogs zugewiesen sind, spielt der Kapazitätspuffer für das Ein- und Ausschalten von Maschinen keine Rolle mehr.

Die Einstellung gilt für alle Maschinentypen. Sie können Werte für "Arbeitszeit"und "Nach Geschäftsschluss"eingeben.

#### Erstellen eines Energieverwaltungszeitplans

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Sehen Sie auf der Registerkarte **Energieverwaltung** nach, ob eine Voreinstellungen (im Menü oben) Ihren Anforderungen entspricht. Wählen Sie eine Voreinstellungen, um deren Werte anzuzeigen. Wenn Sie eine Voreinstellungen verwenden möchten, lassen Sie sie ausgewählt.
3. Wenn Sie einen Wert in einem Feld (Tage, Zeiten oder Intervalle) ändern, ändert sich die Voreinstellung automatisch in **Benutzerdefiniert**. Ein Sternchen zeigt an, dass benutzerdefinierte Einstellungen nicht gespeichert wurden.
4. Legen Sie die gewünschten Werte für den benutzerdefinierten Zeitplan fest.
5. Wählen Sie oben **Benutzerdefiniert** und speichern Sie dann die aktuelle Auswahl als neue Voreinstellung. Geben Sie einen Namen für die neue Voreinstellung ein und wählen Sie das Häkchen.
6. Wenn Sie fertig sind, wählen Sie **Änderungen speichern**.

Später können Sie die benutzerdefinierte Voreinstellung bearbeiten oder löschen, indem Sie das Bleistift- oder das Papierkorbsymbol im Menü **Voreinstellungen** verwenden. Sie können keine allgemeinen Voreinstellungen bearbeiten oder löschen.

### Verwandte Informationen

- Aktualisieren eines Katalogs mit einem neuen Image
- Hinzufügen und Entfernen von Benutzern in einem Katalog

## Azure-Abonnements in Quick Deploy

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

### Einführung

Wenn Sie in Quick Deploy einen Katalog oder ein Image erstellen, wählen Sie ein Azure-Abonnement aus. Quick Deploy unterstützt Citrix Managed Azure-Abonnements und vom Kunden verwaltete Azure-Abonnements.

- Um Ihr eigenes Azure-Abonnement zu verwenden, importieren Sie zuerst ein solches Abonnement (oder mehrere) in Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Dadurch kann Citrix DaaS auf Ihr Azure-Abonnement zugreifen.
- Die Verwendung eines Citrix Managed Azure-Abonnements erfordert keine Abonnementkonfiguration. Ein Citrix Managed Azure-Abonnement ist jedoch nur verfügbar, wenn Sie zusätzlich zu Citrix DaaS den Citrix Azure Consumption Fund bestellen.

Ein paar Features von Citrix DaaS sind unterschiedlich, je nachdem, ob ein Katalog ein Citrix Managed Azure-Abonnement oder Ihr eigenes Azure-Abonnement verwendet.

| Citrix Managed Azure-Abonnement | Kundeneigenes Azure-Abonnement |
|---|---|
| Unterstützt domänengebundene und nicht domänengebundene Maschinen. | Unterstützt nur domänengebundene Maschinen. |
| Unterstützt die Schnellerstellung und die benutzerdefinierte Erstellung von Katalogen. | Unterstützt nur die benutzerdefinierte Erstellung von Katalogen. |
| Immer verfügbar beim Erstellen von Katalogen und Images. | Azure-Abonnement muss zu Citrix DaaS hinzugefügt werden, bevor ein Katalog erstellt wird. |
| Unterstützt für die Benutzerauthentifizierung Citrix Managed Azure Active Directory oder ein kundeneigenes Active Directory. | Kann eine Verbindung mit dem kundeneigenen Active Directory und Azure Active Directory herstellen. |
| Zu den Netzwerkverbindungsoptionen gehört **Keine Konnektivität**. | Als Netzwerkverbindungsoptionen stehen nur die kundeneigenen virtuellen Netzwerke zur Auswahl. |
| Wenn Sie Azure VNet-Peering für die Verbindung zu Ihren Ressourcen verwenden, müssen Sie eine VNet-Peer-Verbindung in Citrix DaaS erstellen. | Wählen Sie ein bestehendes virtuelles Netzwerk aus. |
| Wenn Sie ein Image aus Azure importieren, geben Sie den URI des Images an. | Beim Importieren eines Images können Sie eine virtuelle Festplatte auswählen oder den Azure-Abonnementspeicher durchsuchen. |
| Erstellen einer Bastionsmaschine im Azure-Abonnement des Kunden zur Fehlerbehandlung an Maschinen möglich. | Kein Erfordernis einer Bastionsmaschine, da bereits Zugriff auf die Maschinen in Ihrem Abonnement besteht. |

### Anzeigen von Azure-Abonnements

Um Azure-Abonnementdetails anzuzeigen, erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**. Wählen Sie dann einen Abonnementeintrag aus.

- Die Seite **Details** enthält die Anzahl der Maschine sowie die Anzahl und Namen von Katalogen und Images, von denen das Abonnement verwendet wird.
- Auf der Seite **Ressourcenstandorte** werden die Ressourcenstandorte aufgeführt, an denen das Abonnement verwendet wird.

## Hinzufügen von kundenverwalteten Azure-Abonnements

Um ein vom Kunden verwaltetes Azure-Abonnement zu verwenden, müssen Sie es zu Citrix DaaS hinzufügen, bevor Sie einen Katalog oder ein Image erstellen, der bzw. das dieses Abonnement verwendet. Sie haben zwei Möglichkeiten, wenn Sie Ihre Azure-Abonnements hinzufügen:

- **Wenn Sie globaler Administrator für das Verzeichnis sind und Besitzer-Berechtigungen für das Abonnement haben:** Authentifizieren Sie sich einfach bei Ihrem Azure-Konto.
- **Wenn Sie kein globaler Administrator für das Verzeichnis sind und keine Besitzer-Berechtigungen für das Abonnement haben:** Erstellen Sie eine Azure-App in Ihrem Azure AD und fügen Sie die App als Mitwirkende des Abonnements hinzu, bevor Sie das Abonnement zu Citrix DaaS hinzufügen. Wenn Sie dieses Abonnement zu Citrix DaaS hinzufügen, geben Sie die relevanten App-Informationen an.

### Hinzufügen kundenverwalteter Azure-Abonnements als globaler Administrator

Für diese Aufgabe sind die Berechtigungen “Globaler Administrator”für das Verzeichnis und Besitzer-Berechtigungen für das Abonnement erforderlich.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**.
2. Wählen Sie **Azure-Abonnement**.
3. Wählen Sie auf der Seite **Abonnements hinzufügen** die Option **Hinzufügen Ihrer Azure-Abonnements**.
4. Wählen Sie die Schaltfläche aus, mit der Citrix DaaS für Sie auf Ihre Azure-Abonnements zugreifen kann.
5. Wählen Sie **Azure-Konto authentifizieren**. Sie werden zur Azure-Anmeldeseite weitergeleitet.
6. Geben Sie Ihre Azure-Anmeldeinformationen ein.
7. Sie werden automatisch zu Citrix DaaS zurückgeleitet. Auf der Seite **Abonnement hinzufügen** werden die gefundenen Azure-Abonnements aufgeführt. Verwenden Sie bei Bedarf das Suchfeld, um die Liste zu filtern. Wählen Sie ein oder mehrere Abonnements aus. Wenn Sie fertig sind, wählen Sie **Abonnements hinzufügen**.
8. Bestätigen Sie, dass Sie die ausgewählten Abonnements hinzufügen möchten.

Die von Ihnen ausgewählten Azure-Abonnements werden aufgeführt, wenn Sie **Abonnements** erweitern. Die hinzugefügten Abonnements stehen zur Auswahl, wenn Sie einen Katalog oder ein Image erstellen.

### Hinzufügen kundenverwalteter Azure-Abonnements ohne Konto des globalen Administrators

Das Hinzufügen eines Azure-Abonnements ohne Konto des globalen Administrators besteht aus zwei Teilen:

- Bevor Sie ein Abonnement zu Citrix DaaS hinzufügen, erstellen Sie eine App in Azure AD und fügen diese dann als Mitwirkende des Abonnements hinzu.
- Fügen Sie das Abonnement zu Citrix DaaS hinzu und zwar unter Verwendung von Informationen über die App, die Sie in Azure erstellt haben.

#### Erstellen einer App in Azure AD und Hinzufügen als Mitwirkende

1. Registrieren Sie eine neue App in Azure AD:
   a) Gehen Sie in einem Browser zu https://portal.azure.com.
   b) Wählen Sie im Menü oben links **Azure Active Directory**.
   c) Wählen Sie in der Liste **Verwalten** die Option **App-Registrierungen**.
   d) Wählen Sie **+ New registration**.
   e) Geben Sie auf der Seite **Register an application** die folgenden Informationen an:
      - **Name:** Geben Sie den Verbindungsnamen ein.
      - **Application type::** Wählen Sie **Web app / API**.
      - **Redirect URI:** Lassen Sie das Feld leer.
   f) Wählen Sie **Create**.
2. Erstellen Sie den geheimen Zugriffsschlüssel für die App und fügen Sie die Rollenzuweisung hinzu:
   a) Wählen Sie im vorigen Verfahren **App Registration**, um Details anzuzeigen.
   b) Notieren Sie sich die Angabe für **Application ID** und **Directory ID**. Sie benötigen diese, wenn Sie Ihr Abonnement zu Citrix DaaS hinzufügen.
   c) Wählen **Manage** die Option **Certificates & secrets**.
   d) Wählen Sie auf der Seite **Client secrets** die Option **+ New client secret**.
   e) Geben Sie auf der Seite **Add a client secret** eine Beschreibung ein und wählen Sie ein Ablaufintervall. Wählen Sie dann **Add**.
   f) Notieren Sie sich den geheimen Clientschlüssel. Sie benötigen diese, wenn Sie Ihr Abonnement zu Citrix DaaS hinzufügen.
   g) Wählen Sie das Azure-Abonnement aus, das Sie zu Citrix DaaS hinzufügen möchten, und wählen Sie dann **Access control (IAM)**.

h) Wählen Sie im Feld **Add a role assignment** die Option **Add**.

i) Wählen Sie auf der Registerkarte **Add role assignment** Folgendes aus:

- **Role:** Contributor
- **Assign access to:** Azure AD user, group, oder service principal
- **Select:** Name der Azure-App, die Sie zuvor erstellt haben.

j) Wählen Sie **Speichern**.

**Hinzufügen Ihres Abonnements zu Citrix DaaS** Sie benötigen die Anwendungs-ID, die Verzeichnis-ID und den geheimen Clientschlüssel der App, die Sie in Azure AD erstellt haben.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**.
2. Wählen Sie **Azure-Abonnement**.
3. Wählen Sie auf der Seite **Abonnements hinzufügen** die Option **Hinzufügen Ihrer Azure-Abonnements**.
4. Wählen Sie **Ich habe eine Azure-App mit einer Mitwirkendenrolle für das Abonnement**.
5. Geben Sie die Mandanten-ID (Verzeichnis-ID), die Client-ID (Anwendungs-ID) und den geheimen Clientschlüssel der App ein, die Sie in Azure erstellt haben.
6. Wählen Sie **Abonnement wählen** und dann das gewünschte Abonnement.

Sie können später auf der Seite **Details** des Abonnements im Citrix DaaS-Dashboard über das Dreipunktmenü (…) den geheimen Clientschlüssel aktualisieren oder die Azure-App ersetzen.

Kann Citrix DaaS nach dem Hinzufügen nicht auf das Azure-Abonnement zugreifen, sind mehrere Aktionen zur Katalog-Energieverwaltung und Aktionen an einzelnen Maschinen nicht zulässig. Eine Meldung enthält die Option, das Abonnement erneut hinzuzufügen. Wenn das Abonnement ursprünglich mit einer Azure-App hinzugefügt wurde, können Sie diese ersetzen.

### Hinzufügen von Citrix Managed Azure-Abonnements

Ein Citrix Managed Azure-Abonnement unterstützt eine bestimmte Anzahl Maschinen. (In diesem Zusammenhang bezieht sich der Begriff *Maschine* auf VMs mit einem Citrix VDA. Diese Maschinen stellen Benutzern Apps und Desktops bereit. Es sind keine anderen Maschinen an einem Ressourcenstandort wie Cloud Connectors gemeint.)

Wenn Ihr Citrix Managed Azure-Abonnement bald sein Limit erreicht und Sie genügend Citrix Lizenzen haben, können Sie ein weiteres Citrix Managed Azure-Abonnement anfordern. Im Dashboard wird eine Benachrichtigung angezeigt, wenn das Limit bald erreicht ist.

Sie können keinen Katalog erstellen (bzw. Maschinen zu einem Katalog hinzufügen), wenn die Gesamtzahl der Maschinen aller Kataloge, die das Citrix Managed Azure-Abonnement verwenden, das Limit überschreiten würde.

Beispiel: Sie haben ein Limit von 1.000 Maschinen pro Citrix Managed Azure-Abonnement.

- Sie haben zwei Kataloge (`Cat1` und `Cat2`), die dasselbe Citrix Managed Azure-Abonnement verwenden. `Cat1` enthält 500 Maschinen und `Cat2` 250.
- Bei der Planung für zukünftigen Kapazitätsbedarf fügen Sie 200 Maschinen zu `Cat2` hinzu. Das Citrix Managed Azure-Abonnement unterstützt jetzt 950 Maschinen (500 in `Cat 1` und 450 in `Cat 2`). Das Dashboard zeigt an, dass das Abonnementlimit fast erreicht ist.
- Wenn Sie noch 75 Maschinen benötigen, können Sie das Abonnement nicht zur Erstellung eines Katalogs mit 75 Maschinen (bzw. zum Hinzufügen von 75 Maschinen zu einem vorhandenen Katalog) verwenden. Diese Zahl würde das Abonnementlimit überschreiten. Sie fordern stattdessen ein weiteres Citrix Managed Azure-Abonnement an. Anschließend können Sie einen Katalog in diesem Abonnement erstellen.

Wenn Sie mehrere Citrix Managed Azure-Abonnements haben, gilt Folgendes:

- Zwischen den Abonnements wird nichts geteilt.
- Jedes Abonnement hat einen eindeutigen Namen.
- Sie haben die Citrix Managed Azure-Abonnements (und alle von Ihnen verwalteten Azure-Abonnements, die Sie hinzugefügt haben) zur Auswahl beim:
  - Erstellen eines Katalogs.
  - Erstellen oder Importieren eines Images.
  - Erstellen einer VNet-Peering- oder SD-WAN-Verbindung.

Voraussetzung:

- Sie müssen genügend Citrix Lizenzen zum Hinzufügen eines weiteren Citrix Managed Azure-Abonnements haben. Wenn Sie im obigen Beispiel 2.000 Citrix Lizenzen haben, um mindestens 1.500 Maschinen über Citrix Managed Azure-Abonnements bereitzustellen, können Sie ein weiteres Citrix Managed Azure-Abonnement hinzufügen.

Gehen Sie zum Hinzufügen eines Citrix Managed Azure-Abonnements folgendermaßen vor:

1. Fordern Sie sich bei dem zuständigen Citrix Mitarbeiter ein weiteres Citrix Managed Azure-Abonnement an. Sie werden benachrichtigt, wenn Sie fortfahren können.
2. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**.
3. Wählen Sie **Azure-Abonnement**.
4. Wählen Sie auf der Seite **Abonnements hinzufügen** die Option **Von Citrix verwaltetes Azure-Abonnement hinzufügen**.
5. Wählen Sie unten auf der Seite **Von Citrix verwaltetes Abonnement hinzufügen** die Option **Abonnement hinzufügen**.

Wird bei der Erstellung eines Citrix Managed Azure-Abonnements ein Fehler gemeldet, wenden Sie sich an den Citrix Support.

### Entfernen von Azure-Abonnements

Bevor Sie ein Azure-Abonnement entfernen können, müssen Sie alle Kataloge und Images löschen, die es verwenden.

Wenn Sie ein oder mehrere Citrix Managed Azure-Abonnements haben, können Sie nicht alle entfernen. Sie müssen mindestens eines beibehalten.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**.
2. Wählen Sie den Abonnementeintrag aus.
3. Wählen Sie auf der Registerkarte **Details** die Option **Abonnement entfernen**.
4. Wählen Sie **Azure-Konto authentifizieren**. Sie werden zur Azure-Anmeldeseite weitergeleitet.
5. Geben Sie Ihre Azure-Anmeldeinformationen ein.
6. Sie werden automatisch zu Citrix DaaS zurückgeleitet. Bestätigen Sie den Löschvorgang und wählen Sie dann **Ja, Abonnement löschen**.

### Abgelaufene geheime Clientschlüssel aktualisieren

Wenn der geheime Clientschlüssel eines Abonnements abläuft, können Sie keine Maschinenkataloge dafür erstellen und im Abonnementeintrag wird eine Warnung angezeigt. Zur Problemlösung haben Sie zwei Möglichkeiten:

- Geheimen Clientschlüssel der verwendeten Azure-App aktualisieren
- Zu einer Azure-App mit einem gültigen Ablaufdatum welchseln

#### Geheimen Clientschlüssel der verwendeten Azure-App aktualisieren

Gehen Sie wie folgt vor, um die Azure-App weiterhin für den Zugriff auf Azure-Ressourcen zu verwenden:

1. Erstellen Sie in Azure einen geheimen Clientschlüssel für die Azure-App. Notieren Sie sich den neuen Schlüssel und das Ablaufdatum. Weitere Informationen finden Sie unter Anwendungsgeheimnis in Azure erstellen.
2. Stellen Sie in DaaS den neu erstellten Schlüssel für das Abonnement bereit. Verfahren:
    a) Erweitern Sie unter **Verwalten > Azure Quick Deploy** in Citrix DaaS auf der rechten Seite **Cloud-Abonnements**.
    b) Klicken Sie auf das Abonnement, für das der geheime Schlüssel aktualisiert werden muss.

c) Klicken Sie auf der Abonnementseite im Bereich **Azure-App-Details** auf die Auslassungspunkte und wählen Sie **Geheimen Clientschlüssel aktualisieren**.
d) Geben Sie auf der Seite **Geheimen Clientschlüssel aktualisieren** den neuen **Geheimen Clientschlüssel** und das **Ablaufdatum des geheimen Schlüssels** ein.
e) Klicken Sie auf **Geheimnis aktualisieren**.

#### Zu einer Azure-App mit einem gültigen Ablaufdatum welchseln

Um zu einer gültigen Azure-App für den Zugriff auf Azure-Ressourcen zu wechseln, rufen Sie die erforderlichen App-Informationen ab und stellen Sie sie mithilfe der folgenden Schritte dem Abonnement zur Verfügung:

1. Suchen Sie in Azure eine gültige Azure-App und notieren Sie sich deren Details. Stellen Sie sicher, dass der neuen Azure-App die *Mitwirkendenrolle* zugewiesen ist. Weitere Informationen finden Sie unter Erstellen einer App in Azure AD und Hinzufügen als Mitwirkende
2. Stellen Sie in DaaS die Details zur Azure-App für das Abonnement bereit. Verfahren:
   a) Erweitern Sie unter **Verwalten > Azure Quick Deploy** in Citrix DaaS auf der rechten Seite **Cloud-Abonnements**.
   b) Klicken Sie auf das Abonnement, für das der geheime Schlüssel aktualisiert werden muss.
   c) Klicken Sie auf der Abonnementseite im Bereich **Azure-App-Details** auf die Auslassungspunkte und wählen Sie **Azure-App ersetzen**.
   d) Geben Sie auf der Seite **Azure-App ersetzen** die neuen Azure-App-Details in die Felder für **Verzeichnis-ID (Mandant)**, **Anwendungs-ID (Client)**, **Geheimer Clientschlüssel** und **Ablaufdatum des Geheimnisses** für den Dienstprinzipal ein.
   e) Klicken Sie auf **App ersetzen**.

## Images in Quick Deploy

May 17, 2024

Wenn Sie einen Katalog zur Bereitstellung von Desktops oder Apps erstellen, wird ein Image (mit anderen Einstellungen) als Vorlage zum Erstellen der Maschinen verwendet.

Quick Deploy bietet eine Reihe Images, auf deren Basis Sie ein eigens Image erstellen können. Sie können Images auch aus Ihrem Azure-Abonnement importieren.

### Von Citrix vorbereitete Images

Quick Deploy bietet mehrere von Citrix erstellte Images:

- Windows 11 Pro (Einzelsitzung)
- Virtueller Windows 11 Enterprise-Desktop (Multisitzung)
- Virtueller Windows 11 Enterprise Virtual Desktop (Multisitzung) mit Office 365 ProPlus
- Windows 10 Pro (Einzelsitzung)
- Virtueller Windows 10 Enterprise-Desktop (Multisitzung)
- Virtueller Windows 10 Enterprise-Desktop (Multisitzung) mit Office 365 ProPlus
- Windows Server 2022 (Multisitzung)
- Windows Server 2019 (Multisitzung)
- Windows Server 2016 (Multisitzung)
- Linux Ubuntu 22.04 LTS (Einzelsitzung)
- Linux Ubuntu 22.04 LTS (Multisitzung)

Auf den Images von Citrix sind ein aktueller Citrix Virtual Delivery Agent (VDA) und Tools zur Problembehandlung installiert. Der VDA ist der Kommunikationsmechanismus zwischen den Maschinen der Benutzer und der Citrix Cloud-Infrastruktur von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Von Citrix bereitgestellte Images haben den Vermerk **CITRIX**.

Von Citrix bereitgestellte Images sind in der Oberfläche "Vollständige Konfiguration"von Citrix DaaS nicht verfügbar.

Sie können auch eigene Images aus Azure importieren und verwenden.

### Möglichkeiten zur Verwendung von Images in Quick Deploy

Sie haben folgende Möglichkeiten:

- **Verwenden eines von Citrix bereitgestellten Images beim Erstellen eines Katalogs.** Dies wird nur für Machbarkeitsstudien empfohlen.
- **Verwenden eines von Citrix bereitgestellten Images zur Erstellung eines eigenen.** Wenn das neue Image erstellt ist, passen Sie es an, indem Sie Apps und andere Software hinzufügen, die Ihre Benutzer benötigen. Anschließend können Sie dieses benutzerdefinierte Image beim Erstellen eines Katalogs verwenden.
- **Importieren eines Images aus Azure.** Nachdem Sie ein Image aus Azure importiert haben, können Sie es beim Erstellen eines Katalogs verwenden.

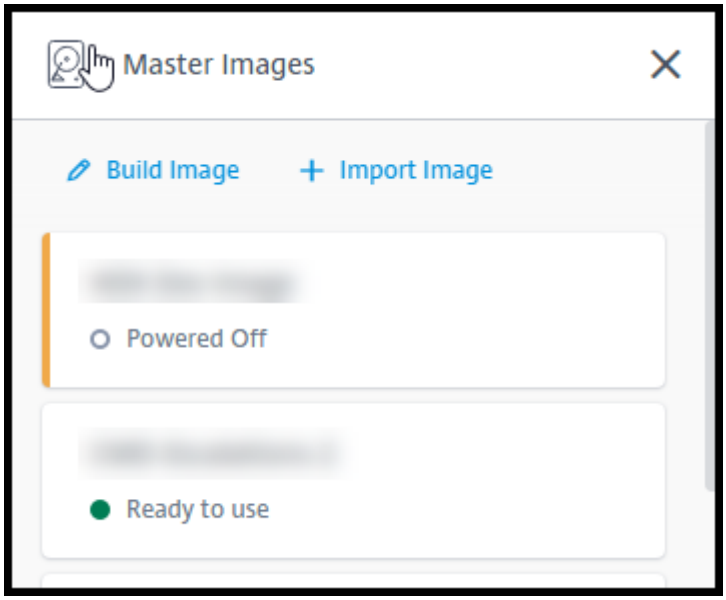
  Alternativ Sie können das Image verwenden, um ein neues zu erstellen und dieses durch Hinzufügen von Apps anzupassen. Anschließend können Sie dieses benutzerdefinierte Image beim Erstellen eines Katalogs verwenden.

Wenn Sie einen Katalog erstellen, überprüft Citrix DaaS (unter anderem), ob das Image ein gültiges Betriebssystem verwendet und ob ein Citrix VDA und Problembehandlungstools installiert sind.

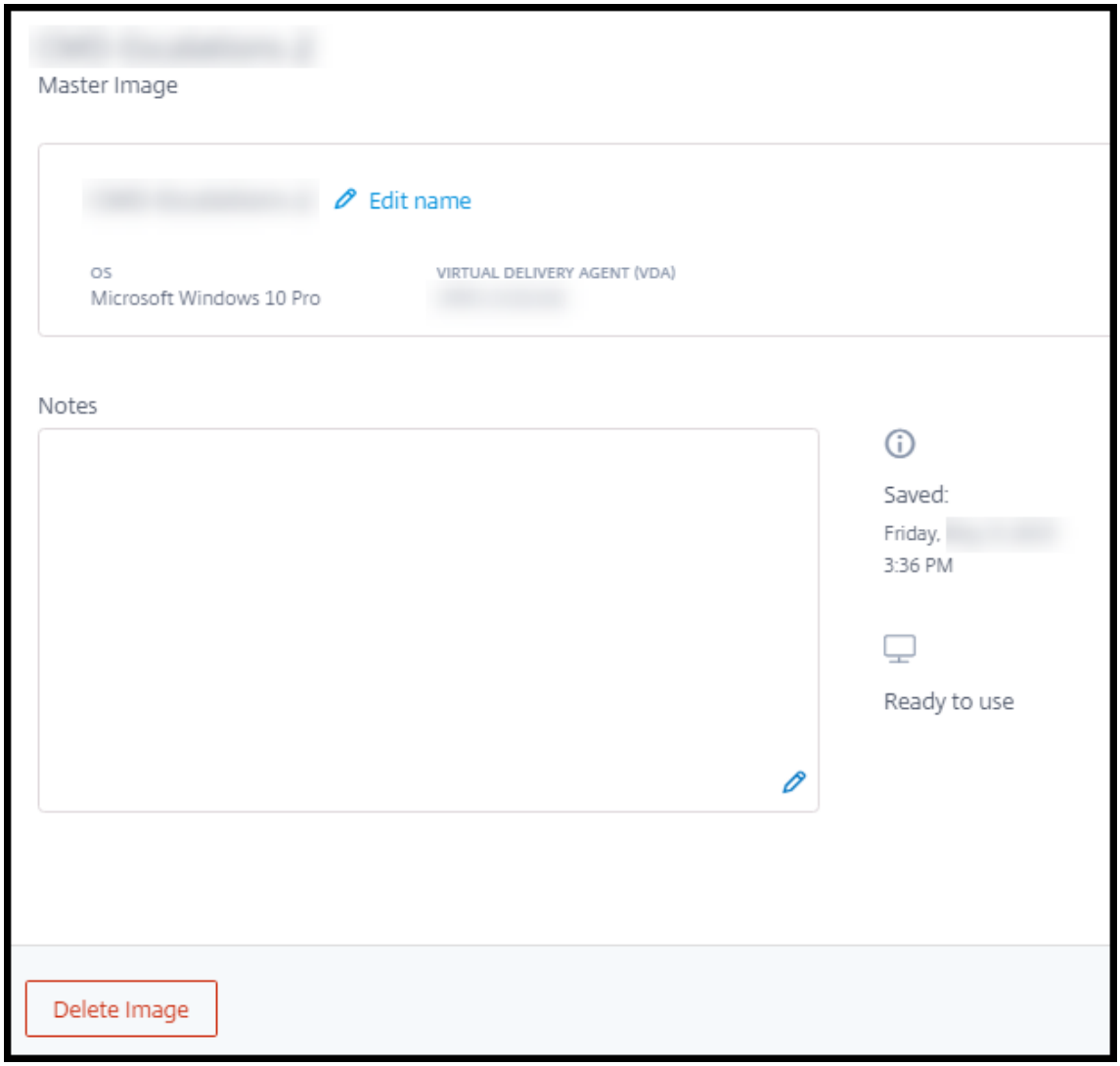
### Anzeigen von Imageinformationen

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Masterimages**. Es werden die von Citrix bereitgestellten Images jegliche von Ihnen importierten Images aufgeführt.




2. Wählen Sie ein Image aus, um zugehörige Details anzuzeigen.




In den Details können Sie folgende Schritte ausführen:

- Image ändern (bearbeiten).
- Notizen hinzufügen bzw. bearbeiten (nur für Images verfügbar, die Sie erstellt oder importiert haben, nicht für solche von Citrix).
- Image löschen.

### Erstellen neuer Images

Das Erstellen eines neuen Images umfasst Erstellung und anschließendes Anpassen. Wenn Sie ein Image erstellen, wird eine neue VM erstellt, um das neue Image zu laden.

Anforderungen:

- Sie kennen die Leistungsmerkmale, die die Maschinen benötigen. Das Ausführen von CAD-Apps erfordert beispielsweise eine andere CPU-, RAM- und Speicherleistung als andere Büro-Apps.

- Wenn Sie eine Verbindung zu Ihren On-Premises-Ressourcen verwenden möchten, richten Sie diese ein, bevor Sie das Image und den Katalog erstellen. Weitere Details finden Sie unter Netzwerkverbindungen.

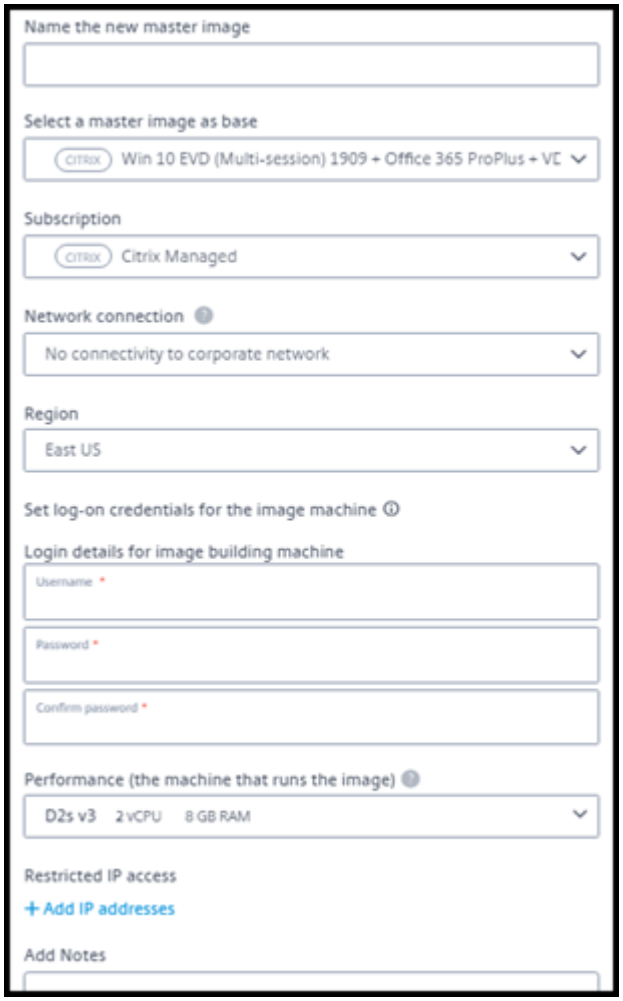
Wenn Sie ein von Citrix erstelltes Ubuntu-Image zum Erstellen eines neuen Images verwenden, wird ein Root-Kennwort für das neue Image erstellt. Sie können dieses Root-Kennwort ändern, allerdings nur während der Erstellung und Anpassung des Images. (Sie können das Root-Kennwort nicht mehr ändern, wenn das Image in einem Katalog verwendet wird.)

- Wenn das Image erstellt wird, wird das von Ihnen angegebene Administratorkonto (**Anmeldeinformationen für die das Image erstellende Maschine**) der Gruppe `sudoers` hinzugefügt.
- Nachdem Sie eine RDP-Verbindung mit der Maschine mit dem neuen Image hergestellt haben, starten Sie die Terminalanwendung und geben Sie sie `sudo passwd root` ein. Geben Sie bei Aufforderung das Kennwort ein, das Sie beim Erstellen des Images angegeben haben. Nach der Überprüfung werden Sie aufgefordert, ein neues Kennwort für den Root-Benutzer einzugeben.

Gehen Sie zum Erstellen eines Images wie folgt vor:

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Masterimages**.
2. Wählen Sie **Image erstellen**.




3. Geben Sie Werte in die folgenden Felder ein:

   - **Name:** Geben Sie einen Namen für das neue Image ein.
   - **Masterimage:** Wählen Sie ein bestehendes Image aus. Dieses dient als Basisimage für das neue Image.
   - **Abonnement:** Wählen Sie ein Azure-Abonnement aus.
   - **Netzwerkverbindung:**
     - Wenn Sie ein Citrix Managed Azure-Abonnement verwenden, wählen Sie **Keine Verbindung** oder eine zuvor erstellte Verbindung.
     - Wenn Sie Ihr eigenes kundenverwaltetes Azure-Abonnement verwenden, wählen Sie Ihre Ressourcengruppe, Ihr virtuelles Netzwerk und Ihr Subnetz aus. Geben Sie dann die Domänendetails ein: FQDN, Organisationseinheit (OU), Citrix DaaS-Kontoname und Anmeldeinformationen.
   - **Region:** Wählen Sie die Region, in der die Maschine mit dem Image erstellt werden soll (nur für **Keine Verbindung** verfügbar).

- **Anmeldeinformationen für die Imagemaschine:** Sie verwenden diese Anmeldeinformationen später, wenn Sie (per RDP) eine Verbindung mit der Maschine mit dem Image herstellen, um Apps und andere Software zu installieren.
- **Maschinenleistung:** Hierbei handelt es sich um Informationen zu CPU, RAM und Speicher der Maschine, auf der das Image ausgeführt wird. Wählen Sie eine Maschinenleistung, die den Anforderungen der Apps entspricht.
- **Eingeschränkter IP-Zugriff:** Wenn Sie den Zugriff auf bestimmte Adressen einschränken möchten, wählen Sie **IP-Adressen hinzufügen** und geben Sie dann eine oder mehrere Adressen ein. Wählen Sie nach dem Hinzufügen der Adressen **Fertig**, um zur Anzeige **Image erstellen** zurückzukehren.
- **Hinweise:** Geben Sie optional eine Notiz (bis zu 1024 Zeichen) ein. Nach dem Erstellen des Images können Sie die Notiz über die Anzeige der Imagedetails aktualisieren.
- **Beitritt zur lokalen Domäne:** Geben Sie an, ob Sie der lokalen Active Directory-Domäne beitreten möchten.
  - Wenn Sie **Ja** auswählen, geben Sie den FQDN, die Organisationseinheit, den Citrix DaaS-Kontonamen und die Anmeldeinformationen ein.
  - Wenn Sie **Nein** auswählen, geben Sie die Anmeldeinformationen für die Hostmaschine ein.

4. Wenn Sie fertig sind, wählen Sie **Image erstellen**.

Das Erstellen eines Images kann bis zu 30 Minuten dauern. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Masterimages**, um den aktuellen Status anzuzeigen (z. B. `Building image` oder `Ready to customize`).

Nächste Schritte: Verbinden mit einem neuen Image und Anpassen des Images.

### Verbinden mit einem neuen Image und Anpassen des Images

Nach dem Erstellen eines Images wird dessen Name in der Imageliste mit dem Status `Ready to customize` o. ä. angezeigt. Zum Anpassen des Images laden Sie zuerst eine RDP-Datei herunter. Wenn Sie eine Verbindung mit dem Image unter Einsatz dieser Datei herstellen, können Sie dem Image Apps und andere Software hinzufügen.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Masterimages**. Wählen Sie das gewünschte Image aus.
2. Wählen Sie **RDP-Datei herunterladen**. Ein RDP-Client wird heruntergeladen.

   Die Imagemaschine schaltet sich möglicherweise aus, wenn Sie nicht kurz nach ihrer Erstellung eine RDP-Verbindung mit ihr herstellen. Das spart Kosten. Wählen Sie in diesem Fall **Einschalten**.

3. Starten Sie den heruntergeladenen RDP-Client. Dieser versucht automatisch, eine Verbindung mit der Maschine herzustellen, die das neue Image enthält. Geben Sie bei entsprechender Aufforderung die Anmeldeinformationen ein, die Sie beim Erstellen des Images angegeben haben.
4. Wenn die Verbindung zur Maschine hergestellt ist, passen Sie sie nach Bedarf an indem Sie Apps hinzufügen oder entfernen, Updates installieren usw.

   Verwenden Sie **nicht** Sysprep für das Image.
5. Wenn Sie fertig sind, kehren Sie zur Anzeige **Masterimages** zurück und wählen Sie **Fertig stellen**. Das neue Image wird automatisch einer Validierung unterzogen.

Wenn Sie anschließend einen Katalog erstellen, wird das neue Image in der Liste der Images zur Auswahl angeboten.

Die Imageanzeige in **Verwalten > Quick Deploy** zeigt an, von wie vielen Katalogen und Maschinen die einzelnen Images verwendet werden.

> **Hinweis:**
>
> Nachdem Sie ein Image fertiggestellt haben, können Sie es nicht bearbeiten. Sie müssen ein neues Image erstellen (Sie können das vorherige Image als Basis verwenden) und dieses dann aktualisieren.

## Importieren eines Images aus Azure

Wenn Sie ein Image mit einem Citrix VDA und Anwendungen für die Benutzer aus Azure importieren, können Sie damit einen Katalog erstellen oder das Image eines vorhandenen Katalogs ersetzen.

### Anforderungen an importierte Images

Citrix führt eine Validierung importierter Images aus. Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, wenn Sie ein Image für den Import in Citrix DaaS vorbereiten.

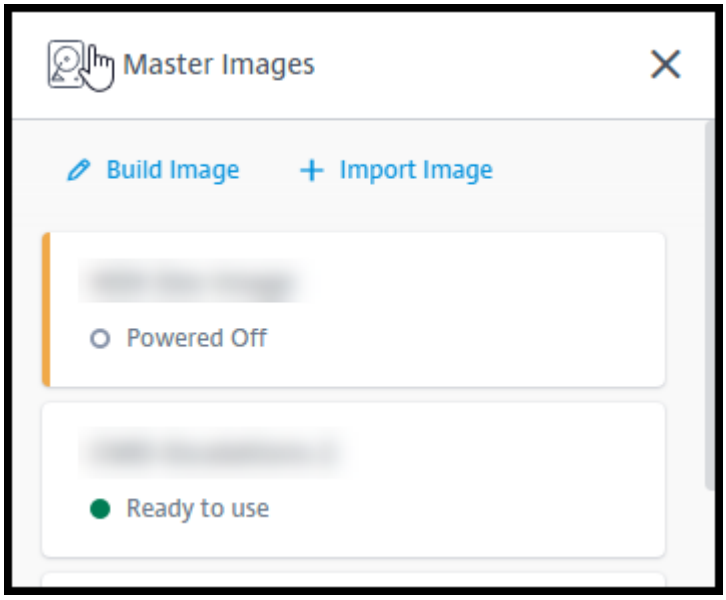
- **Unterstütztes Betriebssystem:** Das Image muss ein unterstütztes OS enthalten. Um die Windows-Betriebssystemversion zu überprüfen, führen Sie `Get-WmiObject Win32_OperatingSyste` aus.
- **Unterstützte Generation:** Virtuelle Maschinen der ersten Generation unterstützen die meisten Gastbetriebssysteme. Virtuelle Maschinen der zweiten Generation unterstützen die meisten 64-Bit-Versionen von Windows und aktuellere Versionen von Linux-Betriebssystemen.
- **Nicht generalisiert:** Das Image darf kein generalisiertes Image sein.

- **Keine konfigurierten Delivery Controller:** Das Image darf keine konfigurierten Citrix Delivery Controller enthalten. Stellen Sie sicher, dass die folgenden Registrierungsschlüssel gelöscht sind.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Datei Personality.ini:** Die Datei `personality.ini` muss auf dem Systemlaufwerk vorhanden sein.
- **Gültiger VDA:** Auf dem Image muss ein Citrix VDA einer neueren Version als 7.11 installiert sein.
  - Windows: Zur Überprüfung verwenden Sie `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Anweisungen zur Installation finden Sie unter Installieren eines Windows-VDAs auf einem Image.
  - Red Hat Enterprise Linux und Ubuntu: Anweisungen zur Installation finden Sie in der Produktdokumentation.
- **Agent für virtuelle Azure-Computer:** Stellen Sie vor dem Importieren von Images sicher, dass der Agent für virtuelle Azure-Computer auf dem Image installiert ist. Weitere Informationen finden Sie im Microsoft-Artikel Übersicht über den Agent für virtuelle Azure-Computer.

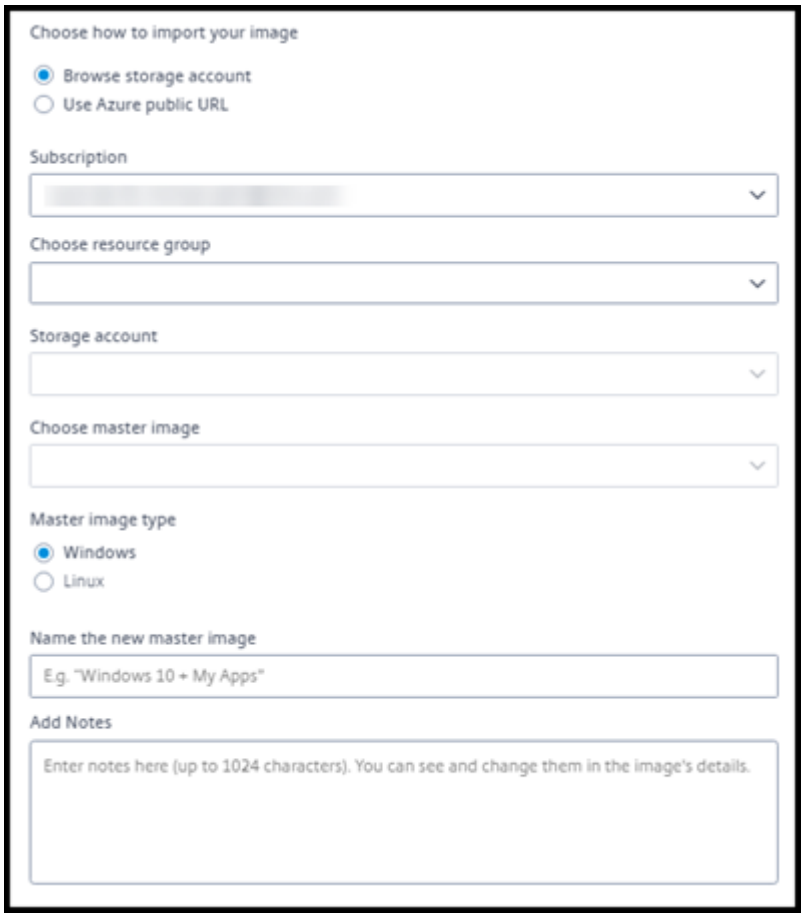
#### Importieren des Images mit Quick Deploy

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Masterimages**.



2. Wählen Sie **Image importieren**.




3. Wählen Sie aus, wie das Image importiert werden soll.

   - Verwenden Sie für verwaltete Datenträger die Exportfunktion, um eine SAS-URL zu generieren. Legen Sie die Ablaufzeit auf mindestens 7200 Sekunden fest.
   - Wählen Sie für VHDs in einem Speicherkonto eine der folgenden Optionen aus:
     - Generieren Sie eine SAS-URL für die VHD-Datei.
     - Aktualisieren Sie die Zugriffsebene eines Blockspeichercontainers auf Blob oder Container. Rufen Sie dann die URL der Datei ab.

4. Wenn Sie **Speicherkonto durchsuchen** ausgewählt haben:

   a) Wählen Sie nacheinander ein Abonnement, eine Ressourcengruppe, ein Speicherkonto und ein Image aus.
   b) Benennen Sie das Image.

5. Wenn Sie **Öffentliche Azure-URL verwenden** ausgewählt haben:

   a) Geben Sie die von Azure generierte URL für die VHD ein. Wählen Sie den Link zum Microsoft-Dokument Herunterladen einer Windows-VHD von Azure, um hilfreiche Hinweise aufzurufen.

b) Wählen Sie ein Abonnement. (Linux-Images können nur importiert werden, wenn Sie ein kundenverwaltetes Abonnement auswählen.)
c) Benennen Sie das Image.

6. Wenn Sie fertig sind, wählen Sie **Image importieren**us.

### Update eines Quick Deploy-Katalogs mit einem neuen Image

Der Katalogtyp bestimmt, welche Maschinen aktualisiert werden, wenn Sie den Katalog aktualisieren.

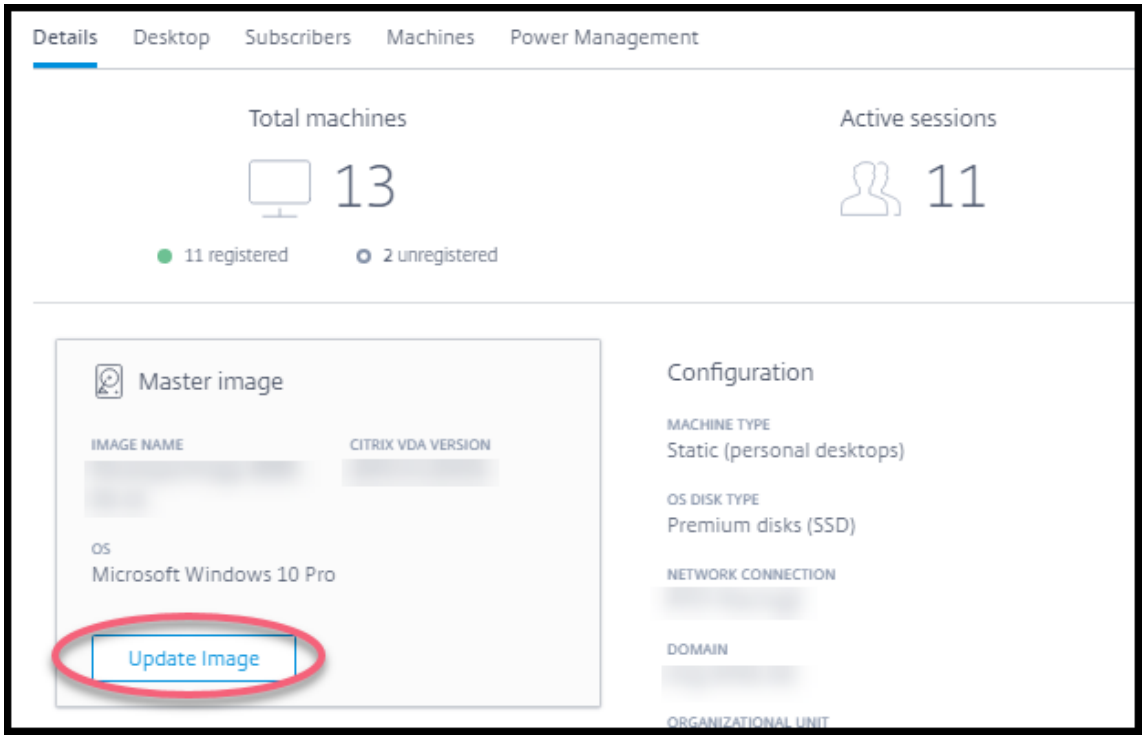
- Bei einem zufälligen Katalog werden alle Maschinen im Katalog mit dem neuesten Image aktualisiert. Wenn Sie dem Katalog weitere Desktops hinzufügen, verwenden diese das neueste Image.
- Bei statischen Katalogen werden die im Katalog befindlichen Maschinen nicht mit dem neuesten Image aktualisiert. Sie verwenden weiterhin das Image, auf dessen Basis sie erstellt wurden. Wenn Sie dem Katalog weitere Maschine hinzufügen, verwenden diese jedoch das neueste Image.

Sie können einen Katalog mit Gen1-Maschinen mit einem Gen2-Image aktualisieren, sofern die Maschinen im Katalog Gen2 unterstützen. Analog dazu können Sie einen Katalog mit Gen2-Maschinen mit einem Gen1-Image aktualisieren, sofern die Maschinen im Katalog Gen1 unterstützen.

Gehen Sie zum Aktualisieren eines Katalogs mit einem neuen Image folgendermaßen vor:

1. Klicken Sie unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags.
2. Wählen Sie auf der Registerkarte **Details** die Option **Image aktualisieren**.




3. Wählen Sie ein Image aus.
4. Zufällige/Mehrsitzungskataloge: Wählen Sie ein Abmeldeintervall aus. Nachdem die anfängliche Imageverarbeitung durch Citrix DaaS abgeschlossen wurde, werden Abonnenten aufgefordert, ihre Arbeit zu speichern und sich von ihren Desktops abzumelden. Das Abmeldeintervall gibt an, wie viel Zeit Abonnenten nach Erhalt der Meldung haben, bis ihre Sitzung automatisch beendet wird.
5. Wählen Sie **Image aktualisieren**.

### Löschen von Images über Quick Deploy

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Masterimages**.
2. Wählen Sie das zu löschende Image aus.
3. Wählen Sie unten **Image löschen**. Bestätigen Sie die Löschung.

### Installieren eines Windows-VDAs auf einem Image

Gehen Sie wie folgt vor, wenn Sie ein Windows-Image für den Import in Citrix DaaS vorbereiten.

Anweisungen zur Linux VDA-Installation finden Sie in der Linux VDA-Produktdokumentation.

1. Stellen Sie in Ihrer Azure-Umgebung eine Verbindung zur Image-VM her (falls Sie noch nicht verbunden sind).

2. Über den Link **Downloads** in der Citrix Cloud-Navigationsleiste können Sie einen VDA herunterladen. Oder navigieren Sie mit einem Browser zur Downloadseite von Citrix DaaS.

   Laden Sie einen VDA auf die VM herunter. Es gibt eigene VDA-Downloadpakete für Desktopbetriebssysteme (Einzelsitzungs-VDA) und Serverbetriebssysteme (Multisitzungs-VDA).

3. Starten Sie das VDA-Installationsprogramm, indem Sie auf die heruntergeladene Datei doppelklicken. Der Installationsassistent wird gestartet.
4. Wählen Sie auf der Seite **Umgebung** die Option zum Erstellen eines Images mit MCS und wählen Sie **Weiter**.
5. Wählen Sie auf der Seite **Kernkomponenten** die Option **Weiter**.
6. Wählen Sie auf der Seite **Delivery Controller** die Option **Automatische Erstellung durch Maschinenerstellungsdienste** und wählen Sie **Weiter**. Bestätigen Sie Ihre Auswahl, wenn Sie dazu aufgefordert werden.
7. Verwenden Sie die Standardeinstellungen auf den Seiten **Zusätzliche Komponenten**, **Features** und **Firewall** (sofern Sie keine anderslautende Anweisung von Citrix erhalten). Wählen Sie auf jeder Seite **Weiter** aus.
8. Wählen Sie auf der Seite **Zusammenfassung** die Option **Installieren**. Die Voraussetzungsdateien werden installiert. Wenn Sie zum Neustart aufgefordert werden, stimmen Sie zu.
9. Die VDA-Installation wird automatisch fortgesetzt. Die Installation der Voraussetzungen wird abgeschlossen und die Komponenten und Features werden installiert. Verwenden Sie auf der Seite **Call Home** die Standardeinstellung (sofern Sie keine anderslautende Anweisung von Citrix erhalten). Nachdem die Verbindung hergestellt ist, wählen Sie **Weiter**.
10. Wählen Sie **Fertig stellen**. Die Maschine wird automatisch neu gestartet.
11. Prüfen Sie die Konfiguration, indem Sie eine oder mehrere auf der VM installierten Anwendungen starten.
12. Fahren Sie die VM herunter. Verwenden Sie nicht Sysprep für das Image.

Weitere Informationen zum Installieren von VDAs finden Sie unter Installieren von VDAs.

## Netzwerkverbindungen in Quick Deploy

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In

> diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

## Einführung

In diesem Artikel erfahren Sie, wie Sie Netzwerkverbindungen zu Ihren Unternehmensressourcen erstellen, wenn Sie ein Citrix Managed Azure-Abonnement verwenden.

Wenn Sie Ihr eigenes kundenverwaltetes Azure-Abonnement verwenden, müssen Sie keine Netzwerkverbindung herstellen.

Wenn Sie einen Quick Deploy-Katalog erstellen, geben Sie an, ob und wie die Benutzer von ihren Citrix Desktops und Apps aus auf Orte und Ressourcen im On-Premises-Unternehmensnetzwerk zugreifen. Wenn Sie eine Verbindung verwenden, müssen Sie diese vor dem Katalog erstellen.

Wenn Sie ein Citrix Managed Azure-Abonnement verwenden, gibt es folgende Optionen:

- Keine Verbindung
- Azure VNet-Peering
- SD-WAN

Sie können den Verbindungstyp eines Katalogs nach dessen Erstellung nicht mehr ändern.

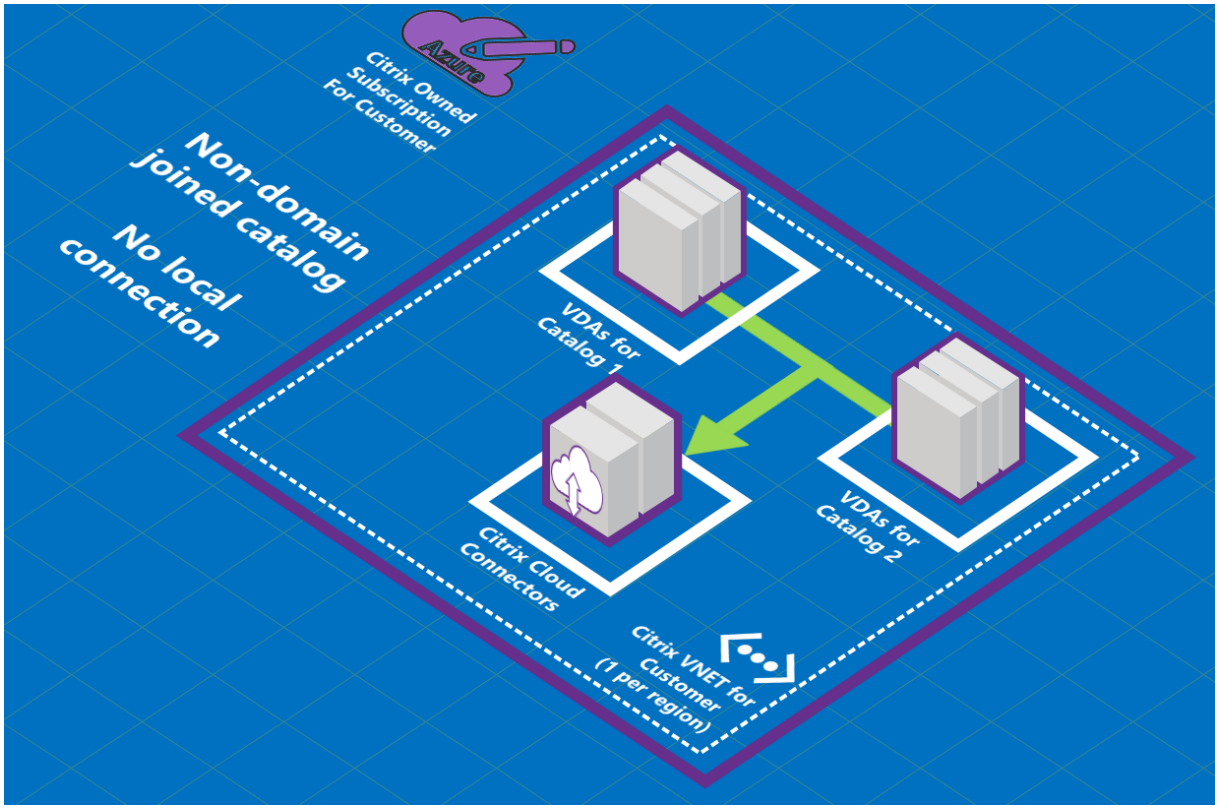
## Anforderungen für alle Netzwerkverbindungen

- Wenn Sie eine Verbindung erstellen, müssen Sie gültige DNS-Servereinträge haben.
- Wenn Sie Secure DNS oder den DNS-Anbieter eines Drittanbieters verwenden, müssen Sie den von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) zu verwendenden Adressbereich den IP-Adressen des DNS-Anbieters in der Positivliste hinzufügen. Dieser Adressbereich wird beim Erstellen einer Verbindung angegeben.
- Alle Service-Ressourcen, die die Verbindung verwenden (domänengebundene Maschinen), müssen in Zugriff auf Ihren NTP-Server haben, um die Zeitsynchronisierung sicherzustellen.

## Keine Verbindung

Wenn ein Katalog mit **Keine Verbindung**konfiguriert ist, können die Benutzer nicht auf Ressourcen in ihrem On-Premises-Netzwerk oder anderen Netzwerken zugreifen. Diese Option ist die einzige Wahl, wenn Sie einen Katalog mit der Schnellerstellung erstellen.

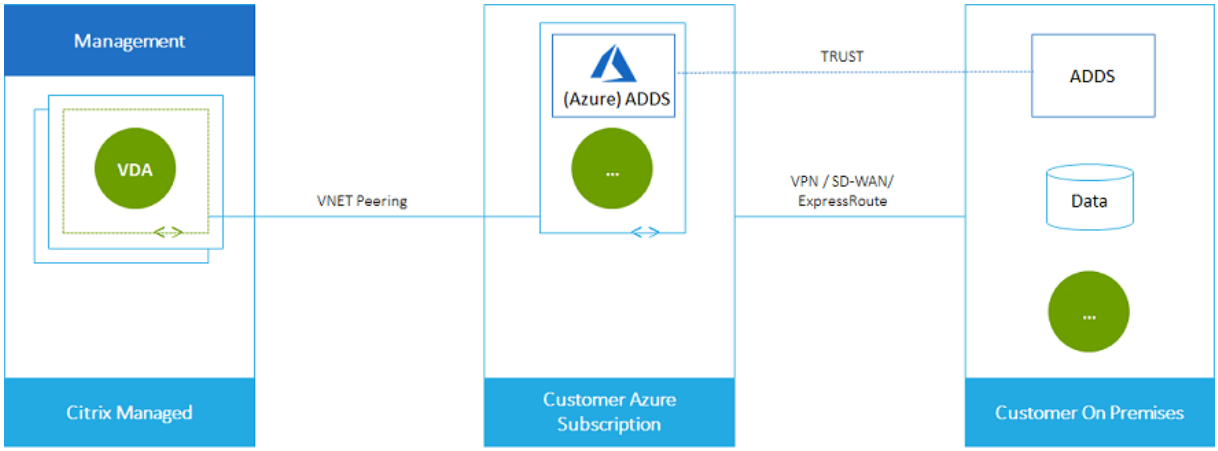
 




### Informationen zu Azure VNet-Peering-Verbindungen

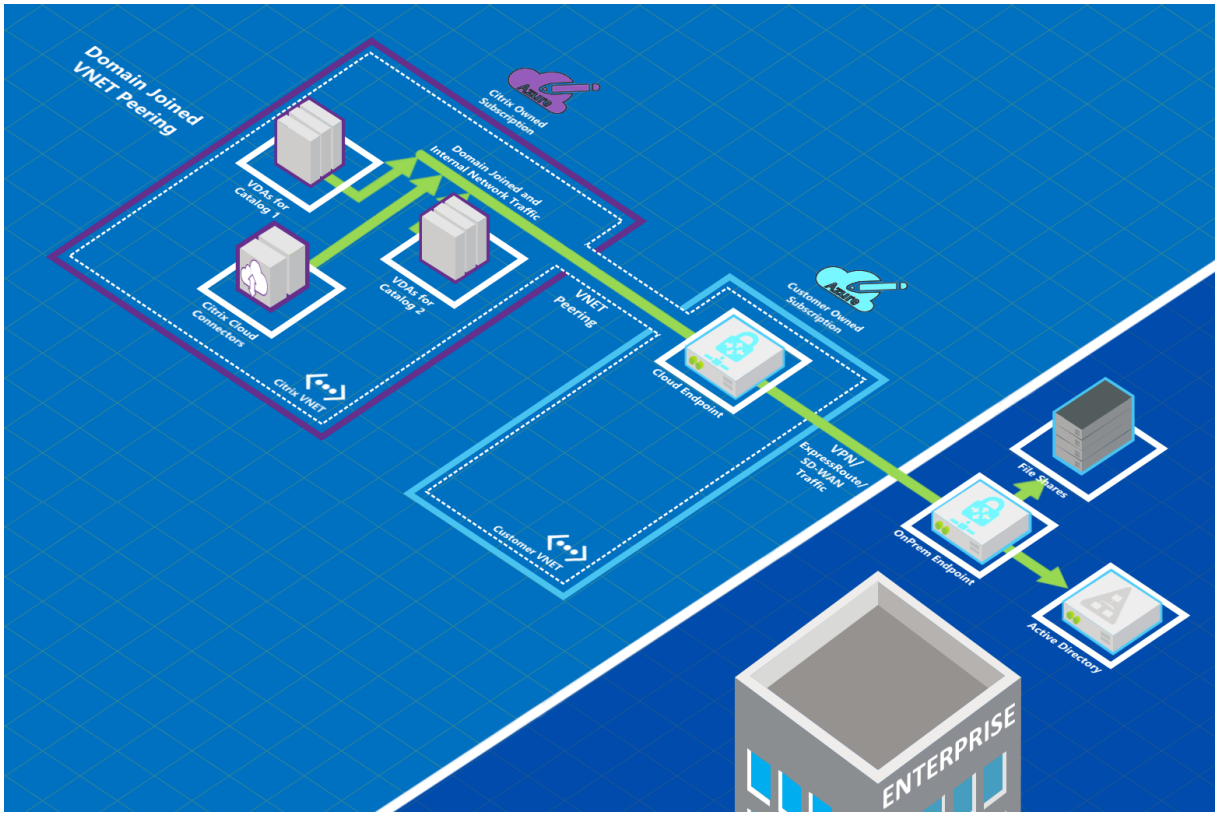
Das VNet-Peering verbindet nahtlos zwei virtuelle Azure-Netzwerke (VNets): Ihr VNet und das VNet von Citrix DaaS. Das Peering ermöglicht außerdem den Benutzern, auf Dateien und andere Elemente aus Ihren On-Premises-Netzwerken zuzugreifen.

Wie in der folgenden Grafik gezeigt, erstellen Sie eine Verbindung per Azure VNet-Peering vom Citrix Managed Azure-Abonnement zum VNet im Azure-Abonnement Ihres Unternehmens.




Hier sehen Sie eine weitere Darstellung des VNet-Peerings.




Die Benutzer können durch einen Domänenbeitritt beim Erstellen des Katalogs auf ihre Netzwerkressourcen (z. B. Dateiserver) zugreifen. (Das heißt, der Beitritt erfolgt bei der AD-Domäne, in der sich Dateifreigaben und andere benötigte Ressourcen befinden.) Ihr Azure-Abonnement stellt eine Verbindung zu diesen Ressourcen her (in der Abbildung per VPN oder Azure ExpressRoute). Beim Erstellen des Katalogs geben Sie die Domäne, die Organisationseinheit und die Anmeldeinformationen an.

> **Wichtig:**
>
> - Machen Sie sich mit Azure VNet Peering vertraut, bevor Sie es im Service verwenden.
> - Erstellen Sie die VNet-Peering-Verbindung vor dem Katalog, der sie verwenden soll.

#### Azure VNet-Peering mit benutzerdefinierten Routen

Benutzerdefinierte Routen setzen die Standardsystemrouten von Azure zur Steuerung des Datenverkehrs zwischen virtuellen Maschinen in einem VNet-Peering-System, On-Premises-Netzwerken und dem Internet außer Kraft. Benutzerdefinierte Routen werden beispielsweise verwendet, wenn es Netzwerke gibt, auf die Citrix DaaS-Ressourcen voraussichtlich zugreifen, die aber nicht direkt per VNet-Peering verbunden sind. Sie können beispielsweise eine benutzerdefinierte Route erstellen, die den Datenverkehr durch eine Netzwerk-Appliance an das Internet oder in ein On-Premises-Subnetz leitet.

Für benutzerdefinierte Routen gilt Folgendes:

- Ihre Citrix DaaS-Umgebung muss ein virtuelles Azure-Netzwerkgateway oder ein Netzwerkgerät wie Citrix SD-WAN enthalten.
- Wenn Sie benutzerdefinierte Routen hinzufügen, müssen Sie die Routing-Tabellen Ihres Unternehmens mit den Ziel-VNet-Informationen von Citrix DaaS aktualisieren, um eine Ende-zu-Ende-Verbindung sicherzustellen.
- Benutzerdefinierte Routen werden in Citrix DaaS in der Reihenfolge angezeigt, in der sie eingegeben werden. Die Anzeigereihenfolge hat keinen Einfluss auf die Reihenfolge, in der Azure Routen auswählt.

Bevor Sie benutzerdefinierte Routen verwenden, lesen Sie den Microsoft-Artikel Routing von Datenverkehr für virtuelle Netzwerke, um mehr über die Verwendung benutzerdefinierter Routen, Typen des nächsten Hops und die Auswahl einer Route für den ausgehenden Datenverkehr durch Azure zu erfahren.

Sie können benutzerdefinierte Routen bestehenden Azure VNet-Peering-Verbindungen in Ihrer Citrix DaaS-Umgebung hinzufügen, oder neuen Verbindungen bei deren Erstellung. Wenn Sie alle Vorbereitungen für benutzerdefinierte Routen mit Ihrem VNet-Peering getroffen haben, lesen Sie die folgenden Abschnitte in diesem Artikel:

- Benutzerdefinierte Routen mit neuen Azure VNet-Peerings: Erstellen einer Azure VNet-Peering-Verbindung
- Benutzerdefinierte Routen mit bestehenden Azure VNet-Peerings: Verwalten benutzerdefinierter Routen für Azure VNet-Peering-Verbindungen

#### Azure VNet-Peering –Anforderungen und Vorbereitung

- Anmeldeinformationen eines Azure-Abonnementbesitzers. Dies muss ein Azure Active Directory-Konto sein. Dieser Service unterstützt keine anderen Kontotypen (live.com oder externe Azure AD-Konten in anderen Mandanten u. ä.).
- Ein Azure-Abonnement, eine Ressourcengruppe und ein virtuelles Netzwerk (VNet).
- Richten Sie die Azure-Netzwerkrouten ein, damit VDAs im Citrix Managed Azure-Abonnement mit Ihren Netzwerkstandorten kommunizieren können.
- Öffnen Sie Azure-Netzwerksicherheitsgruppen von Ihrem VNet zum angegebenen IP-Bereich.
- **Active Directory:** Bei Domäneneinbindung wird empfohlen, dass Sie einen Active Directory-Dienst im durch Peering verbundenen VNet ausführen. Dadurch werden die Vorteile der geringen Latenz der Azure VNet-Peering-Technologie genutzt.

  Die Konfiguration kann beispielsweise Azure Active Directory-Domänendienste (AADDS), eine Domänencontroller-VM im VNet oder Azure AD Connect mit Ihrem On-Premises-Active Directory

umfassen.

Nachdem Sie AADDS aktiviert haben, können Sie Ihre verwaltete Domäne nicht in ein anderes VNet verschieben, ohne sie zu löschen. Daher ist es wichtig, beim Aktivieren der verwalteten Domain das richtige VNet auszuwählen. Bevor Sie fortfahren, lesen Sie den Microsoft-Artikel Überlegungen zum Netzwerk für Azure Active Directory-Domänendienste.

- **VNet-IP-Bereich:** Beim Erstellen der Verbindung müssen Sie einen verfügbaren CIDR-Adressraum (IP-Adresse und Netzwerkpräfix) angeben, der unter den verbundenen Netzwerkressourcen und Azure-VNets eindeutig ist. Dies ist der IP-Bereich, der den VMs im per Peering verbundenen VNet von Citrix DaaS zugewiesen ist.

  Stellen Sie sicher, dass Sie einen IP-Bereich ohne Überschneidung mit Adressen angeben, die Sie in Ihrem Azure- oder On-Premises-Netzwerk verwenden.

  - Hat Ihr Azure-VNet beispielsweise den Adressraum 10.0.0.0 /16, erstellen Sie die VNet-Peering-Verbindung in Citrix DaaS als 192.168.0.0 /24.
  - In diesem Beispiel würde das Erstellen einer Peering-Verbindung mit einem IP-Bereich von 10.0.0.0 /24 als überschneidender Adressbereich gelten.

  Wenn sich Adressbereiche überschneiden, wird die VNet-Peering-Verbindung möglicherweise nicht erfolgreich erstellt. Sie funktioniert außerdem nicht einwandfrei für Site-Verwaltungsaufgaben.

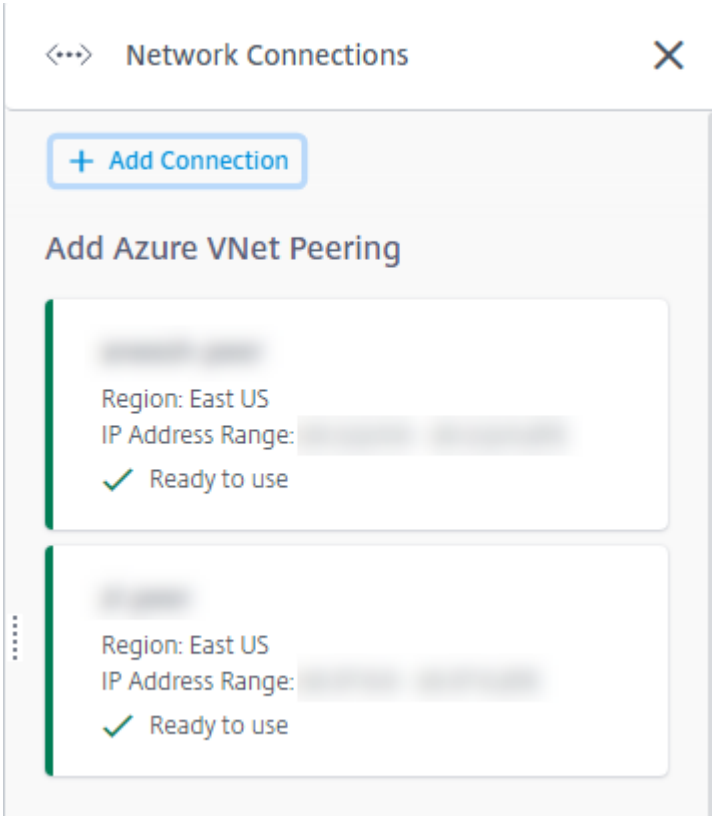
Weitere Informationen zum VNet-Peering finden Sie in den folgenden Microsoft-Artikeln.

- Peering in virtuellen Netzwerken
- Azure VPN Gateway
- Erstellen einer Site-to-Site-Verbindung im Azure-Portal
- Häufig gestellte Fragen zum VPN-Gateway (nach “überlappen”oder “überschneiden”suchen)

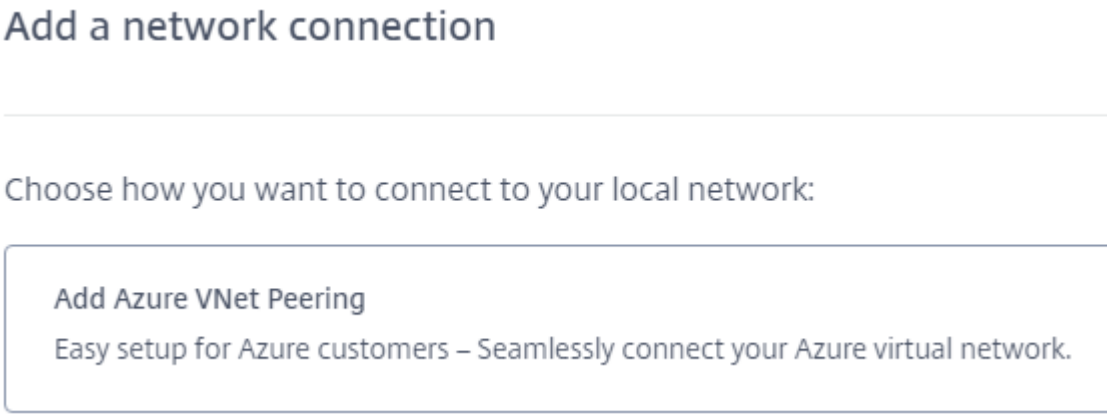
#### Erstellen einer Azure VNet-Peering-Verbindung

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**. Wenn Sie bereits Verbindungen eingerichtet haben, werden diese aufgeführt.

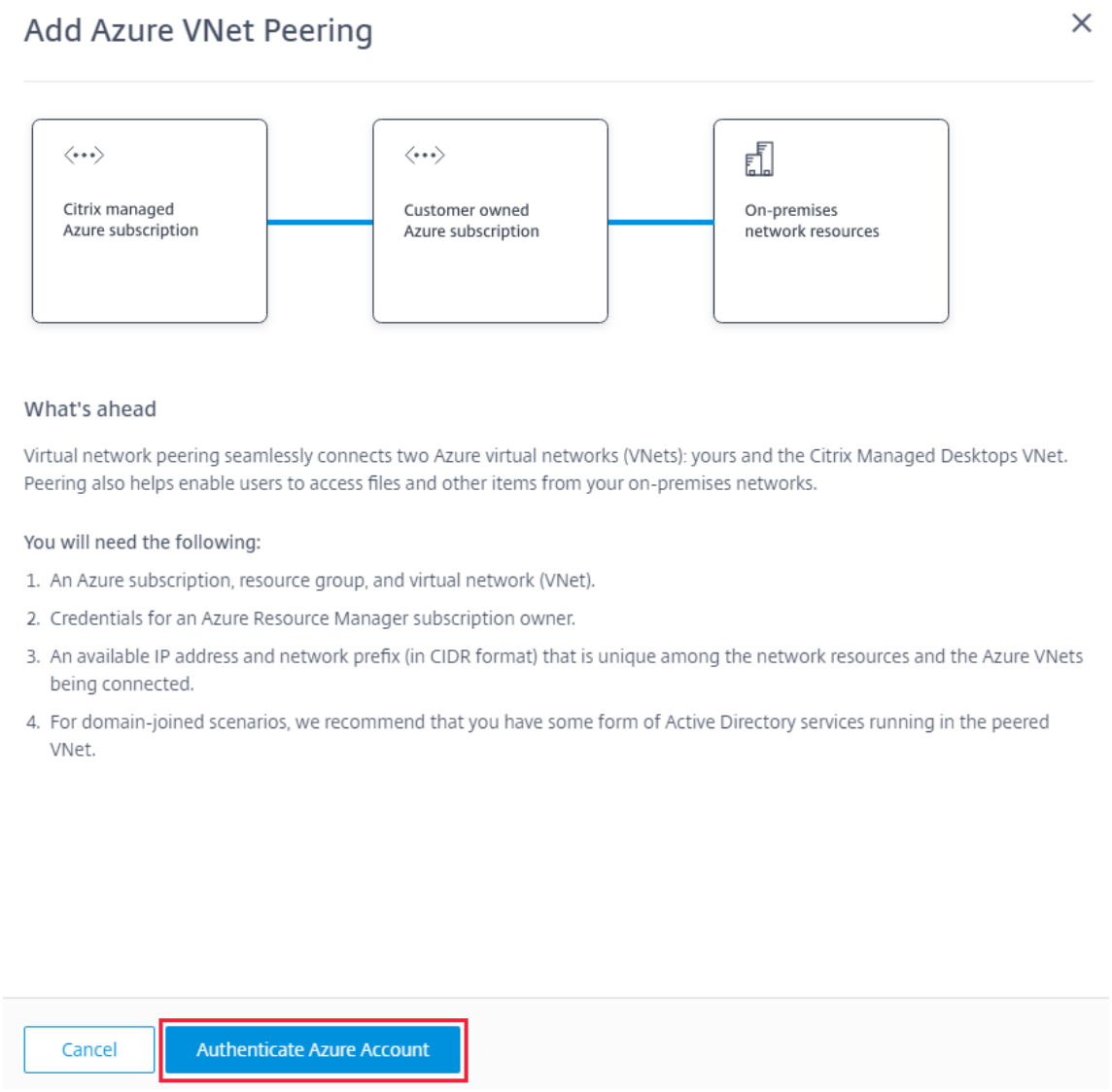



2. Wählen Sie **Verbindung hinzufügen**.
3. Klicken Sie auf eine beliebige Stelle im Feld **Azure VNet-Peering hinzufügen**.



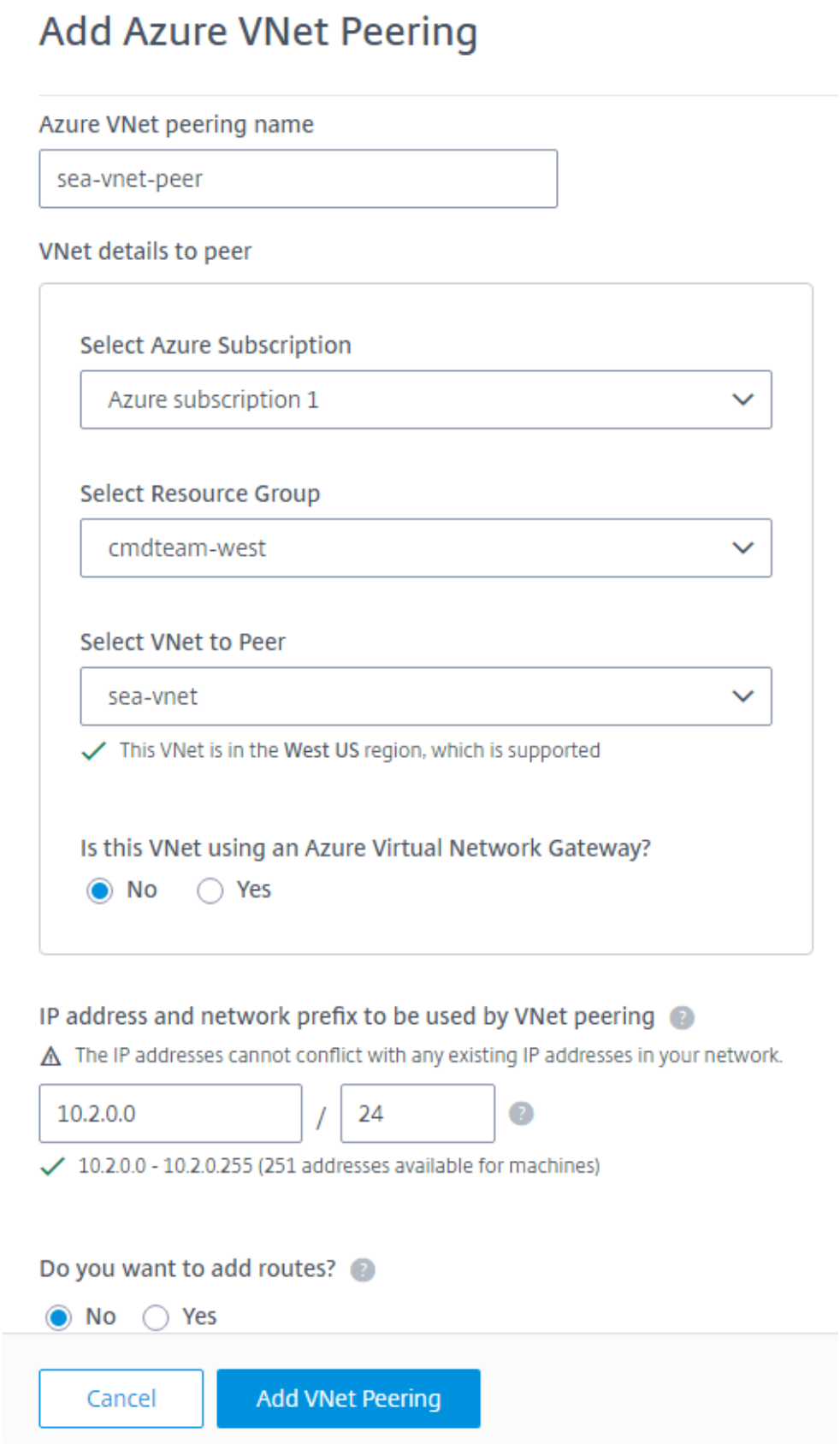

4. Wählen Sie **Azure-Konto authentifizieren**.




5. Sie werden von Citrix DaaS automatisch zur Azure-Anmeldeseite weitergeleitet, um Ihre Azure-Abonnements zu authentifizieren. Nachdem Sie sich bei Azure mit den Anmeldeinformationen des globalen Administratorkontos angemeldet und die Bedingungen akzeptiert haben, werden Sie zum Dialogfeld mit den Details zur Verbindungserstellung zurückgeleitet.



6. Geben Sie einen Namen für den Azure VNet-Peer ein.
7. Wählen Sie das Azure-Abonnement, die Ressourcengruppe und das VNet für das Peering.
8. Geben Sie an, ob das ausgewählte VNet ein Azure-Gateway für virtuelle Netzwerke verwendet. Weitere Informationen finden Sie im Microsoft-Artikel Azure VPN Gateway.
9. Wenn Sie im vorherigen Schritt mit **Ja** geantwortet haben (das VNet verwendet ein Azure-Gateway für virtuelle Netzwerke), geben Sie an, ob Sie die Routenverteilung des Gateways für virtuelle Netzwerke aktivieren möchten. Wenn diese Option aktiviert ist, fügt Azure automatisch alle Routen durch das Gateway hinzu.

   Sie können diese Einstellung später auf der Seite **Details** der Verbindung ändern. Eine Änderung kann jedoch zu Änderungen des Routenmusters und zu Unterbrechungen des VDA-Datenverkehrs führen. Wenn Sie die Option später deaktivieren, müssen Sie Routen manuell zu Netzwerken hinzufügen, die von VDAs verwendet werden.
10. Geben Sie eine IP-Adresse ein und wählen Sie eine Netzwerkmaske aus. Der zu verwendende Adressbereich und die Anzahl der von dem Bereich unterstützten Adressen werden angezeigt. Stellen Sie sicher, dass der IP-Bereich sich mit keinen Adressen überschneidet, die Sie in Ihrem Azure- oder On-Premises-Netzwerk verwenden.

    - Hat Ihr Azure-VNet beispielsweise den Adressraum 10.0.0.0 /16, erstellen Sie die VNet-Peering-Verbindung in Citrix DaaS als 192.168.0.0 /24.
    - In diesem Beispiel wird das Erstellen einer VNet-Peering-Verbindung mit einem IP-Bereich von 10.0.0.0 /24 als überschneidender Adressbereich gelten.

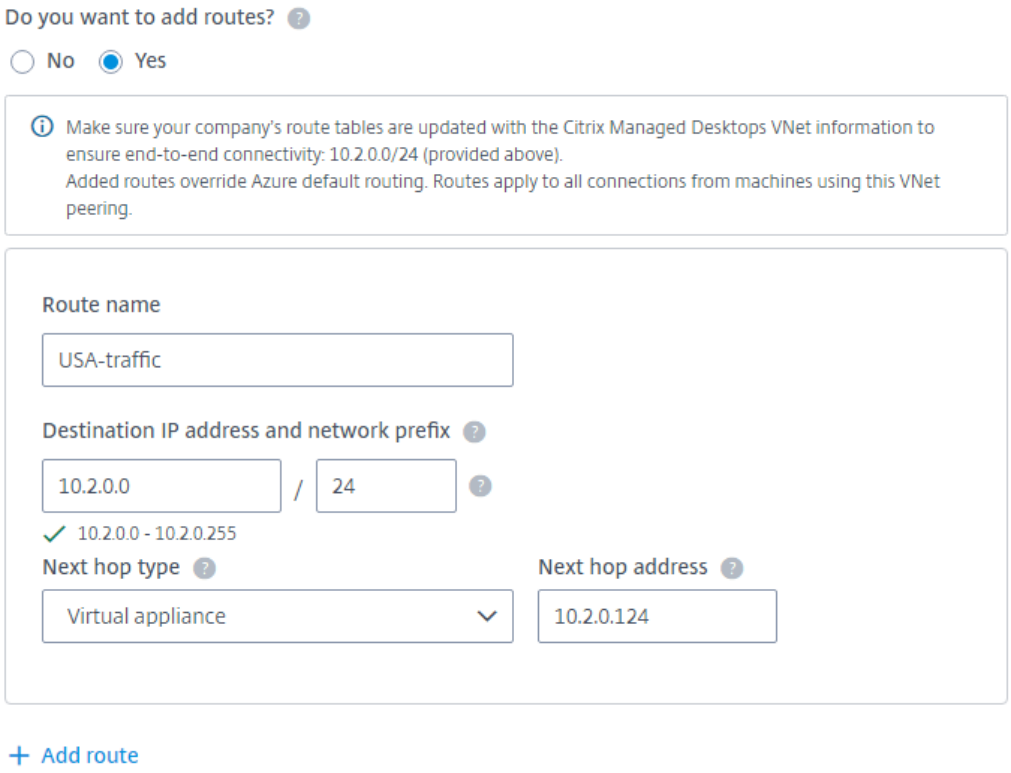
    Wenn sich Adressbereiche überschneiden, wird die VNet-Peering-Verbindung möglicherweise nicht erfolgreich erstellt. Sie funktioniert außerdem nicht einwandfrei für Site-Verwaltungsaufgaben.
11. Geben Sie an, ob Sie der VNet-Peering-Verbindung benutzerdefinierte Routen hinzufügen möchten. Wenn Sie **Ja**wählen, geben Sie die folgenden Informationen ein:

    a) Geben Sie einen Anzeigenamen für die benutzerdefinierte Route ein.

    b) Geben Sie die Ziel-IP-Adresse und das Netzwerkpräfix ein. Das Netzwerkpräfix muss zwischen 16 und 24 liegen.

    c) Wählen Sie einen Typ des nächsten Hops für das Routenziel des Datenverkehrs aus. Wenn Sie **Virtuelle Appliance** auswählen, geben Sie die interne IP-Adresse der Appliance ein.




Weitere Informationen zu Typen des nächsten Hops finden Sie im Abschnitt Benutzerdefinierte Routen des Microsoft-Artikels *Routing von Datenverkehr für virtuelle Netzwerke*.

d) Um eine weitere benutzerdefinierte Route für die Verbindung zu erstellen, wählen Sie **Route hinzufügen**.

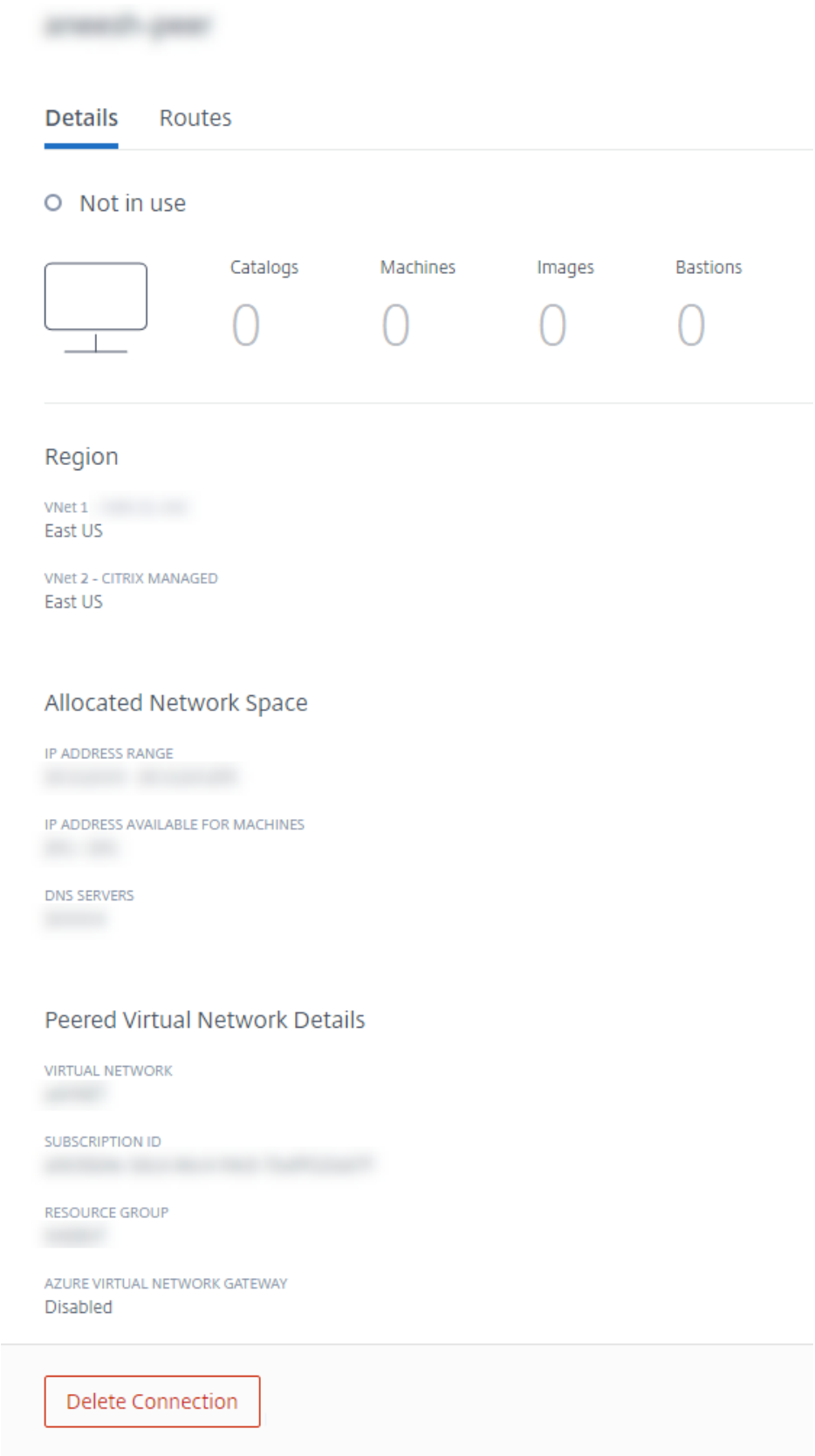
12. Wählen Sie **VNet-Peering hinzufügen**.

Wenn die Verbindung erstellt ist, wird sie unter **Netzwerkverbindungen > Azure VNet-Peers** auf der rechten Seite des Dashboards **Verwalten > Quick Deploy** aufgeführt. Wenn Sie einen Katalog erstellen, wird diese Verbindung in der Liste der verfügbaren Netzwerkverbindungen angezeigt.

**Anzeigen von Azure VNet-Peering-Verbindungsdetails**



1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie die gewünschte Azure VNet-Peering-Verbindung aus.

Es werden folgende Details angezeigt:

- Anzahl der Kataloge, Maschinen, Images und Bastions, von denen die Verbindung verwendet wird.
- Region, zugewiesener Netzwerkspeicher und per Peering verbundene VNets.
- Derzeit für die VNet-Peering-Verbindung konfigurierte Routen.

#### Verwalten benutzerdefinierter Routen für Azure VNet-Peering-Verbindungen

Sie können einer Verbindung neue benutzerdefinierte Routen hinzufügen oder vorhandene benutzerdefinierte Routen ändern, deaktivieren und löschen.

> **Wichtig:**
>
> Das Ändern, Deaktivieren oder Löschen benutzerdefinierter Routen ändert den Datenfluss der Verbindung und wirkt sich möglicherweise störend auf aktive Benutzersitzungen aus.

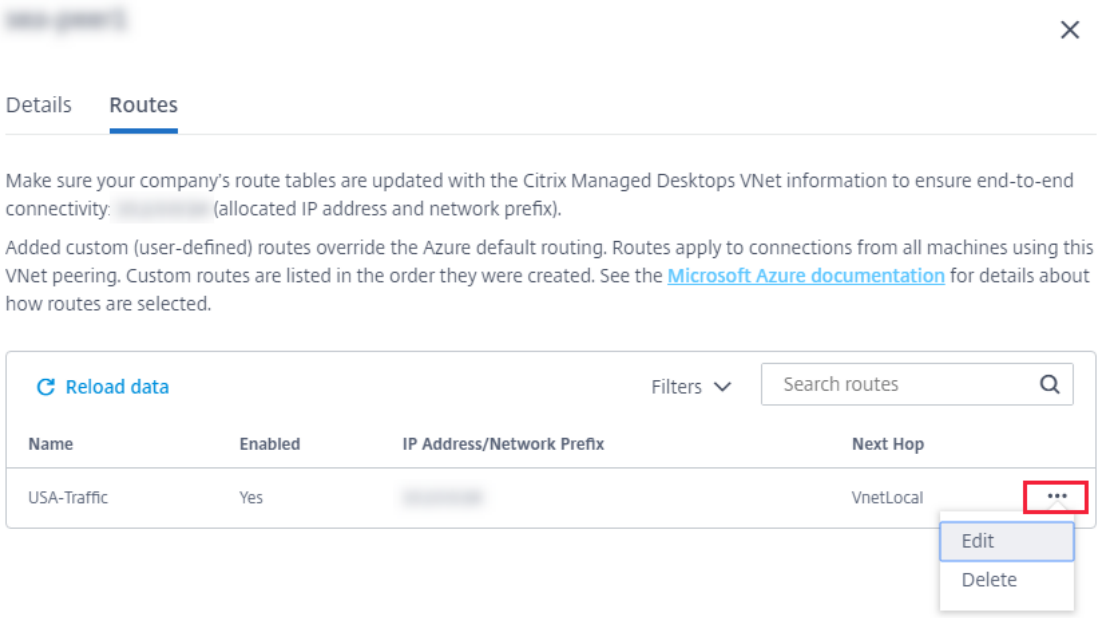
Gehen Sie zum Hinzufügen einer benutzerdefinierten Route folgendermaßen vor:

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie die gewünschte Verbindung aus.
3. Wählen Sie in den Verbindungsdetails **Routen** und dann **Route hinzufügen**.
4. Geben Sie einen Anzeigenamen, die Ziel-IP-Adresse und das Präfix sowie den Typ des nächsten Hops ein. Wenn Sie **Virtuelle Appliance** Typ des nächsten Hops auswählen, geben Sie die interne IP-Adresse der Appliance ein.
5. Geben Sie an, ob Sie die benutzerdefinierte Route aktivieren möchten. Standardmäßig wird die benutzerdefinierte Route aktiviert.
6. Wählen Sie **Route hinzufügen**.

Gehen Sie zum Ändern oder Deaktivieren einer benutzerdefinierten Route folgendermaßen vor:

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie die gewünschte Verbindung aus.
3. Wählen Sie in den Verbindungsdetails **Routen** und suchen Sie die benutzerdefinierte Route, die Sie verwalten möchten.
4. Wählen Sie im Menü die Option **Bearbeiten**.




5. Nehmen Sie bei Bedarf Änderungen an der Ziel-IP-Adresse und dem Präfix oder dem Typ des nächsten Hops vor.
6. Um eine benutzerdefinierte Route zu aktivieren oder zu deaktivieren, wählen Sie unter **Diese Route aktivieren?** die Option **Ja** oder **Nein**.
7. Wählen Sie **Speichern**.

Gehen Sie zum Löschen einer benutzerdefinierten Route folgendermaßen vor:

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie die gewünschte Verbindung aus.
3. Wählen Sie in den Verbindungsdetails **Routen** und suchen Sie die benutzerdefinierte Route, die Sie verwalten möchten.
4. Wählen Sie im Menü die Option **Löschen**.
5. Wählen Sie **Das Löschen einer Route kann die aktiven Sitzungen unterbrechen**, um zu bestätigen, dass Sie die Auswirkungen des Löschens der benutzerdefinierten Route kennen.
6. Wählen Sie **Route löschen**.

### Löschen einer Azure VNet-Peering-Verbindung

Bevor Sie eine Azure VNet-Peering-Verbindung löschen können, entfernen Sie alle damit verbundenen Kataloge. Siehe Löschen eines Katalogs.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie die gewünschte Verbindung aus.
3. Wählen Sie in den Verbindungsdetails die Option **Verbindung löschen**.

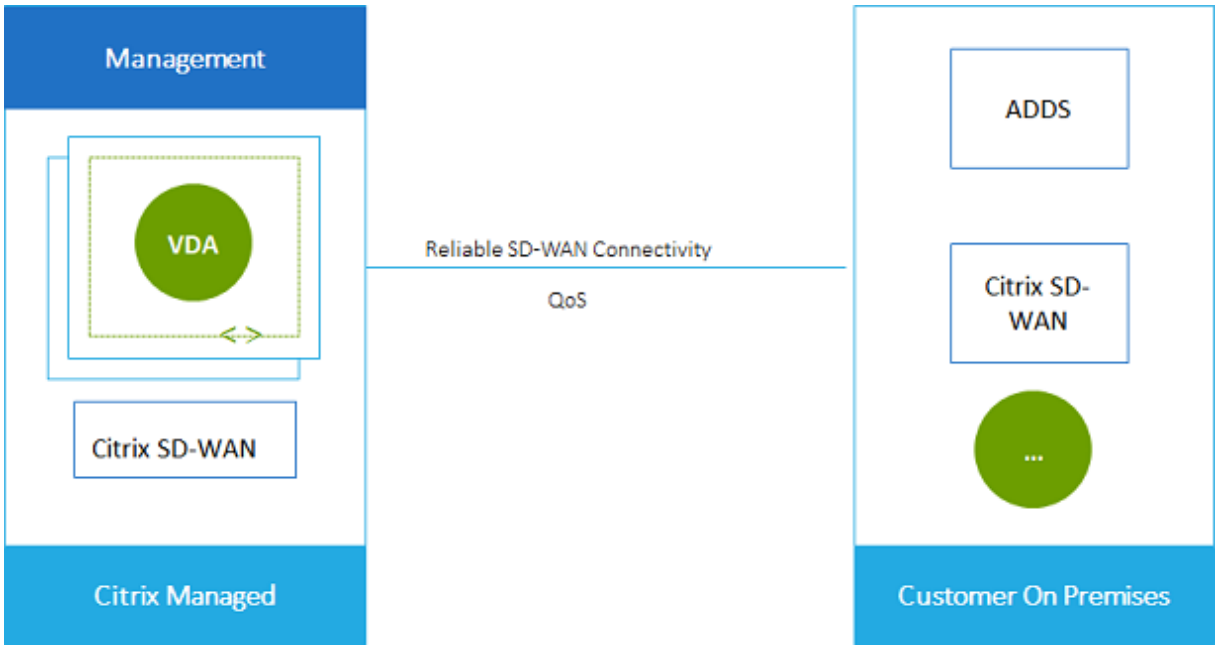
 

### Informationen zu SD-WAN-Verbindungen

Citrix SD-WAN optimiert alle Netzwerkverbindungen, die von Citrix DaaS benötigt werden. Zusammen mit den HDX-Technologien bietet Citrix SD-WAN Servicequalität und Verbindungszuverlässigkeit für den ICA- und Out-of-Band-Citrix-DaaS-Datenverkehr. Citrix SD-WAN unterstützt die folgenden Netzwerkverbindungen:

- Multistream-ICA-Verbindungen zwischen Benutzern und ihren virtuellen Desktops
- Internetzugriff vom virtuellen Desktop an Websites, SaaS-Apps und andere Cloudeigenschaften
- Zugriff vom virtuellen Desktop zurück auf On-Premises-Ressourcen wie Active Directory, Dateiserver und Datenbankserver
- Echtzeit-/interaktiver Datenverkehr über RTP von der Medien-Engine der Workspace-App an Cloudgehostete Unified Communications-Dienste wie Microsoft Teams
- Clientseitiges Abrufen von Videos von Websites wie YouTube und Vimeo

Wie die nachfolgende Grafik zeigt, erstellen Sie eine SD-WAN-Verbindung aus dem Citrix Managed Azure-Abonnement an Ihre Sites. Zusammen mit der Verbindung werden SD-WAN-VPX-Appliances im Citrix Managed Azure-Abonnement erstellt. Aus der SD-WAN-Perspektive wird dieser Standort als Zweig behandelt.




#### SD-WAN-Verbindung –Anforderungen und Vorbereitung

- Wenn die folgenden Anforderungen nicht erfüllt sind, ist die Option der SD-WAN-Netzwerkverbindung nicht verfügbar.

  - Citrix Cloud-Dienstberechtigungen: Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) und SD-WAN Orchestrator.
  - Installierte und konfigurierte SD-WAN-Bereitstellung. Die Bereitstellung muss einen Master Control Node (in der Cloud oder on-premises) enthalten und mit SD-WAN Orchestrator verwaltet werden.

- VNet-IP-Bereich: Geben Sie einen verfügbaren CIDR-Adressraum (IP-Adresse und Netzwerkpräfix) an, der unter den verbundenen Netzwerkressourcen eindeutig ist. Dies ist der IP-Bereich, der den VMs im VNet von Citrix DaaS zugewiesen ist.

  Stellen Sie sicher, dass Sie einen IP-Bereich ohne Überschneidung mit Adressen angeben, die Sie in Ihrem Cloud- oder On-Premises-Netzwerk verwenden.

  - Hat Ihr Netzwerk beispielsweise den Adressraum 10.0.0.0 /16, erstellen Sie die Verbindung in Citrix DaaS als 192.168.0.0 /24.
  - In diesem Beispiel würde das Erstellen einer Verbindung mit einem IP-Bereich von 10.0.0.0 /24 als überschneidender Adressbereich gelten.

  Wenn sich Adressbereiche überschneiden, wird die Verbindung möglicherweise nicht erfolgreich erstellt. Sie funktioniert außerdem nicht einwandfrei für Site-Verwaltungsaufgaben.

- Zur Verbindungskonfiguration gehören Aufgaben, die Sie als Administrator von Citrix DaaS und der SD-WAN Orchestrator-Administrator ausführen müssen. Um Ihre Aufgaben zu erledigen, benötigen Sie außerdem Informationen vom SD-WAN Orchestrator-Administrator.

  Wir empfehlen beiden Administratoren, das vorliegende Dokument und die SD-WAN-Dokumentation zu lesen, bevor Sie eine Verbindung herstellen.

#### Erstellen einer SD-WAN-Verbindung

> **Wichtig:**
>
> Weitere Informationen zur SD-WAN-Konfiguration finden Sie unter SD-WAN-Konfiguration zur Integration von Citrix DaaS.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie **Verbindung hinzufügen**.
3. Klicken Sie auf der Seite **Netzwerkverbindung hinzufügen** auf eine beliebige Stelle im Feld “SD-WAN”.
4. Die nächste Seite enthält eine Zusammenfassung der anstehenden Schritte. Wenn Sie sie gelesen haben, wählen Sie **Konfiguration von SD-WAN starten**.
5. Geben Sie auf der Seite **SD-WAN konfigurieren** die Informationen ein, die vom SD-WAN Orchestrator-Administrator erhalten haben.

- **Bereitstellungsmodus:** Wenn Sie **Hohe Verfügbarkeit** auswählen, werden zwei VPX-Appliances erstellt (für Produktionsumgebungen empfohlen). Wenn Sie **Eigenständig** auswählen, wird eine Appliance erstellt. Sie können diese Einstellung später nicht ändern. Um in den Bereitstellungsmodus zu wechseln, müssen Sie den Zweig und alle zugehörigen Kataloge löschen und neu erstellen.
- **Name:** Geben Sie einen Namen für den SD-WAN-Standort ein.
- **Durchsatz und Anzahl der Bürostandorte:** Diese Informationen werden vom SD-WAN Orchestrator-Administrator bereitgestellt.
- **Region:** Die Region, in der die VPX-Appliances erstellt werden.
- **VDA-Subnetz und SD-WAN-Subnetz:** Diese Informationen werden vom SD-WAN Orchestrator-Administrator bereitgestellt. Weitere Informationen zum Vermeiden von Konflikten finden Sie unter SD-WAN-Verbindung –Anforderungen und Vorbereitung.

6. Wenn Sie fertig sind, wählen Sie **Zweig erstellen**.
7. Auf der nächsten Seite wird zusammengefasst, worauf Sie im Dashboard **Verwalten > Quick Deploy** achten müssen. Wenn Sie die Angaben gelesen haben, wählen Sie **Verstanden**.
8. Unter **Verwalten > Quick Deploy** zeigt der neue SD-WAN-Eintrag unter **Netzwerkverbindungen** den Fortschritt der Konfiguration an. Wenn der Eintrag orange und die Meldung `Awaiting activation by SD-WAN administrator` angezeigt wird, benachrichtigen Sie Ihren SD-WAN Orchestrator-Administrator.
9. Informationen zu den Aufgaben des SD-WAN Orchestrator-Administrators finden Sie in der Produktdokumentation zu SD-WAN Orchestrator.
10. Wenn der SD-WAN Orchestrator-Administrator fertig ist, wird der SD-WAN-Eintrag unter **Netzwerkverbindungen** grün und die Meldung `You can create catalogs using this connection` wird angezeigt.

#### Anzeigen der Details der SD-WAN-Verbindung

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie **SD-WAN**, falls es mehrere Auswahlmöglichkeiten gibt.
3. Wählen Sie die gewünschte Verbindung aus.

Es wird Folgendes angezeigt:

- **Registerkarte "Details":** Informationen, die Sie beim Konfigurieren der Verbindung angegeben haben.
- **Registerkarte "Zweigkonnektivität":** Name, Cloudkonnektivität, Verfügbarkeit, Bandbreitenebene, Rolle und Standort für jeden Zweig und MCN.

### Löschen einer SD-WAN-Verbindung

Bevor Sie eine SD-WAN-Verbindung löschen können, entfernen Sie alle zugehörigen Kataloge. Siehe Löschen eines Katalogs.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
2. Wählen Sie SD-WAN, falls es mehrere Auswahlmöglichkeiten gibt.
3. Wählen Sie die zu löschende Verbindung aus, um die Details zu erweitern.
4. Wählen Sie auf der Registerkarte **Details** die Option **Verbindung löschen**.
5. Bestätigen Sie die Löschung.

## Benutzer und Authentifizierung in Quick Deploy

May 17, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

### Methoden der Benutzerauthentifizierung

Die Benutzer müssen sich authentifizieren, wenn sie sich bei Citrix Workspace anmelden, um ihren Desktop oder ihre Apps zu starten.

Quick Deploy unterstützt die folgenden Benutzerauthentifizierungsmethoden:

- **Managed Azure AD:** Managed Azure AD ist ein von Citrix bereitgestelltes und verwaltetes Azure Active Directory (AAD). Sie müssen keine eigene Active Directory-Struktur bereitstellen. Fügen Sie einfach Ihre Benutzer zum Verzeichnis hinzu.
- **Ihr Identitätsanbieter:** Sie können jede verfügbare Authentifizierungsmethode in Citrix Cloud verwenden.

> **Hinweis:**
>
> - Remote-PC-Zugriff-Bereitstellungen verwenden nur Active Directory. Einzelheiten finden Sie unter Remote-PC-Zugriff.
> - Wenn Sie Azure AD-Domänendienste verwenden: Anmelde-UPNs für Workspace müssen den Domänennamen enthalten, der beim Aktivieren der Azure AD-Domänendienste

> angegeben wurde. Anmeldungen können keine UPNs einer benutzerdefinierten, von Ihnen erstellten Domäne verwenden, selbst wenn diese benutzerdefinierte Domäne als primär gekennzeichnet ist.

Das Einrichten der Benutzerauthentifizierung umfasst die folgenden Verfahren:

1. Konfigurieren Sie die Benutzerauthentifizierungsmethode in Citrix Cloud und Workspace.
2. Wenn Sie Managed Azure AD zur Benutzerauthentifizierung verwenden, fügen Sie die Benutzer dem Verzeichnis hinzu.
3. Fügen Sie einem Katalog Benutzer hinzu.

### Konfigurieren der Benutzerauthentifizierung in Citrix Cloud

Zum Konfigurieren der Benutzerauthentifizierung in Citrix Cloud gehen Sie folgendermaßen vor:

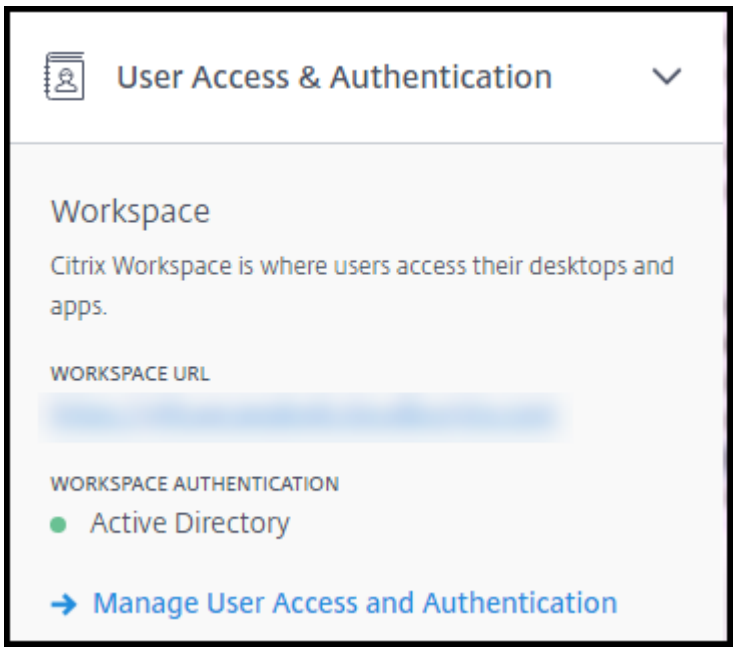
- Stellen Sie eine Verbindung mit der Benutzerauthentifizierungsmethode her, die Sie verwenden möchten. (In Citrix Cloud wird eine "Verbindung"mit einer Authentifizierungsmethode hergestellt bzw. getrennt.)
- Legen Sie in Citrix Cloud die Workspace-Authentifizierung auf die verbundene Methode fest.

> **Hinweis:**
>
> Die Managed Azure AD-Authentifizierungsmethode ist standardmäßig konfiguriert. In anderen Worten: Sie ist automatisch mit Citrix Cloud verbunden und die Workspace-Authentifizierung ist voreingestellt auf die Verwendung von Managed Azure AD für Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Wenn Sie diese Methode verwenden möchten und zuvor keine andere Methode konfiguriert haben, fahren Sie mit den Anweisungen unter Hinzufügen und Löschen von Benutzern in Managed Azure AD fort.
> Wenn Managed Azure AD getrennt wird, wechselt die Workspaceauthentifizierung auf Active Directory. Wenn Sie eine andere Authentifizierungsmethode verwenden möchten, wählen Sie die folgende Schrittfolge.

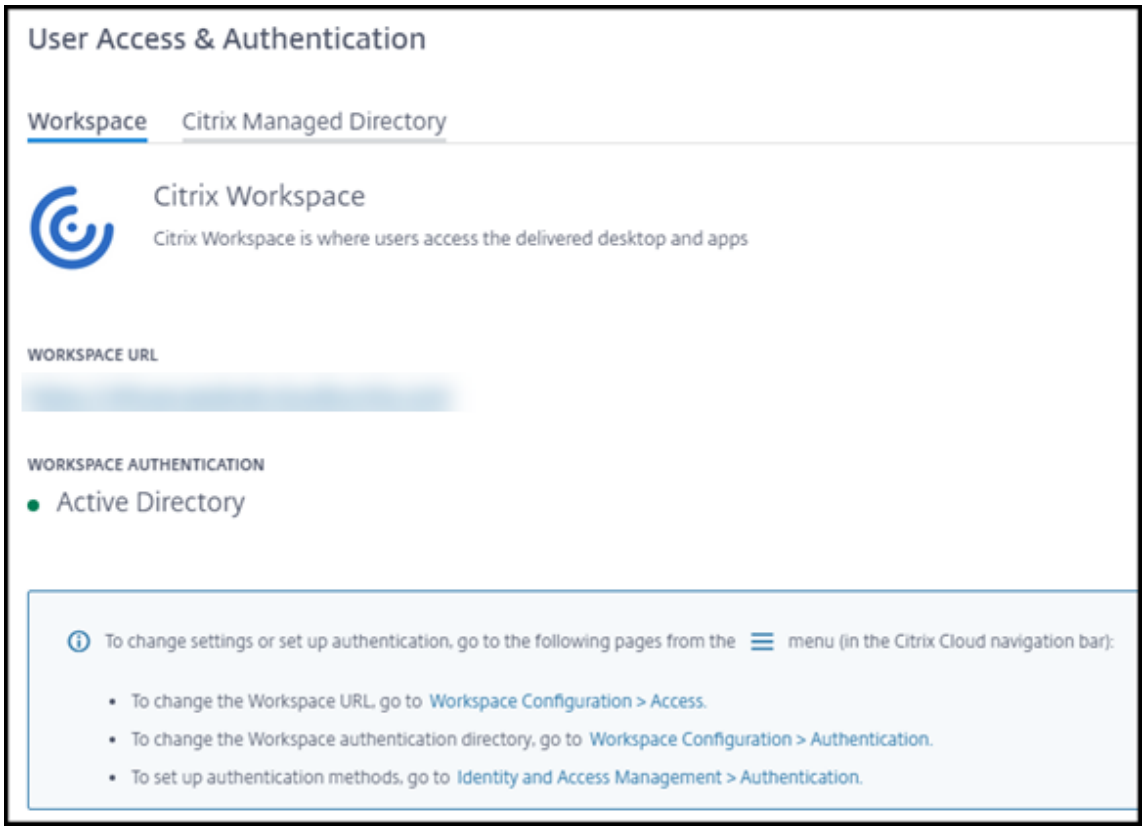
Gehen Sie zum Ändern der Authentifizierungsmethode folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Benutzerzugriff und Authentifizierung**.




2. Wählen Sie **Benutzerzugriff und Authentifizierung verwalten**. Wählen Sie die Registerkarte **Workspace**, falls sie noch nicht ausgewählt ist. (Die andere Registerkarte zeigt an, welche Benutzerauthentifizierungsmethode derzeit konfiguriert ist.)




3. Folgen Sie dem Link **Um Authentifizierungsmethoden einzurichten**. Dieser Link führt Sie zu

Citrix Cloud. Wählen Sie im Menü die Option **Verbinden** für die gewünschte Methode aus.

4. Wählen Sie in Citrix Cloud im Menü links oben **Workspacekonfiguration**. Wählen Sie auf der Registerkarte **Authentifizierung** die gewünschte Methode aus.

Nachfolgende Schritte:

- Wenn Sie Managed Azure AD verwenden, fügen Sie die Benutzer dem Verzeichnis hinzu.
- Für alle Authentifizierungsmethoden fügen Sie Benutzer zum Kataloghinzu.

### Hinzufügen und Löschen von Benutzern in Managed Azure AD

Führen Sie dieses Verfahren nur aus, wenn Sie Managed Azure AD zur Benutzerauthentifizierung bei Citrix Workspace verwenden.

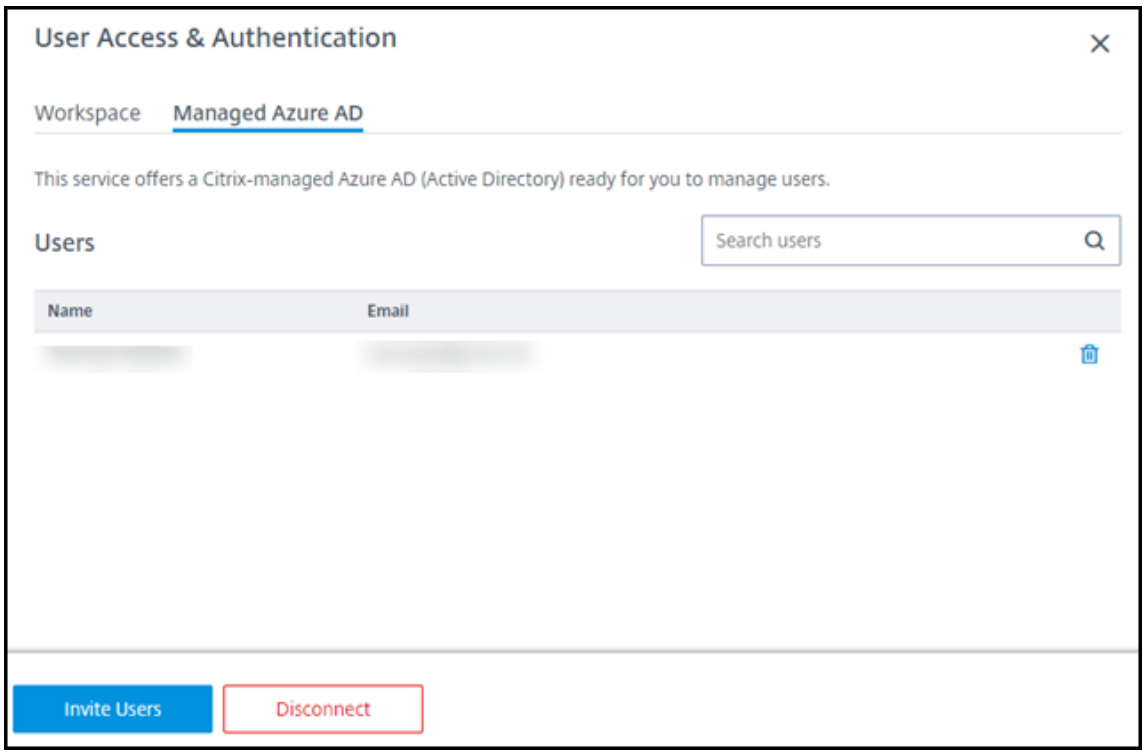
Sie geben die Namen und E-Mail-Adressen der Benutzer an. Citrix sendet dann an jeden per E-Mail eine Einladung. In der E-Mail werden Benutzer angewiesen, einen Link auszuwählen, über den sie in das Citrix Managed Azure AD aufgenommen werden.

- Hat ein Benutzer bereits ein Microsoft-Konto mit der von Ihnen angegebenen E-Mail-Adresse, wird dieses verwendet.
- Hat er kein Microsoft-Konto mit der E-Mail-Adresse, erstellt Microsoft ein Konto.

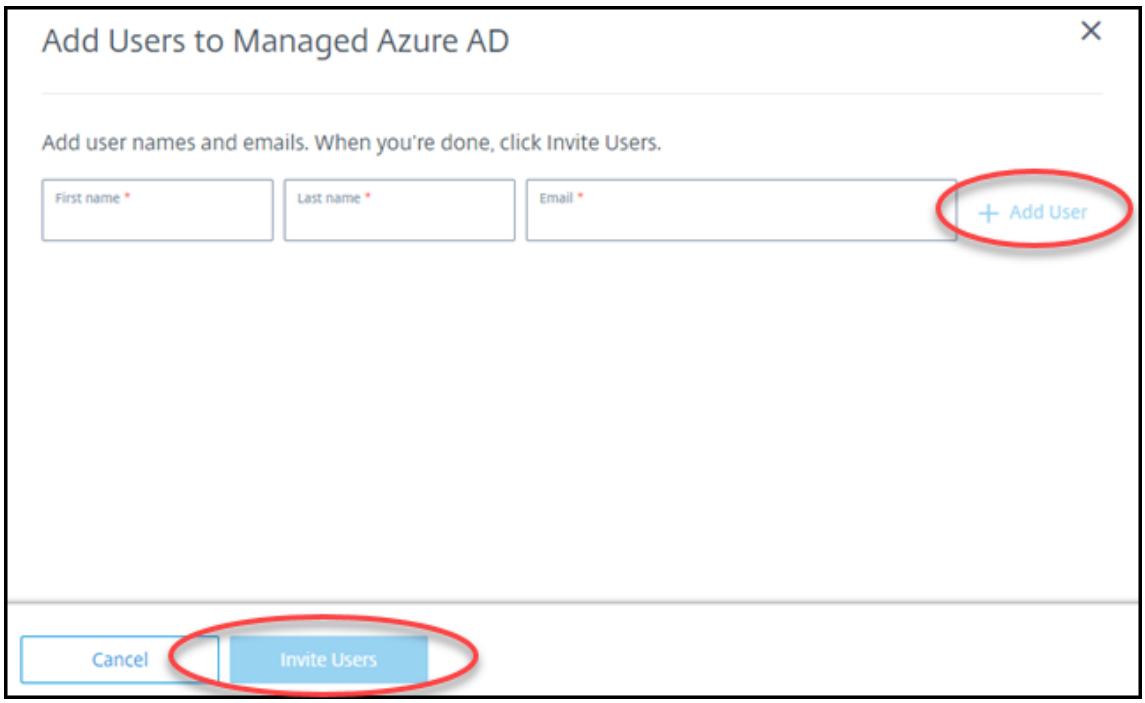
Gehen Sie zum Hinzufügen und Einladen von Benutzern zu Managed Azure AD folgendermaßen vor:

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Benutzerzugriff und Authentifizierung**. Wählen Sie **Benutzerzugriff und Authentifizierung verwalten**.
2. Wählen Sie die Registerkarte **Managed Azure AD**.
3. Wählen Sie **Benutzer einladen**.




4. Geben Sie den Namen und die E-Mail-Adresse eines Benutzers ein und wählen Sie **Benutzer hinzufügen**.




5. Wiederholen Sie den vorherigen Schritt, um weitere Benutzer hinzuzufügen.
6. Wenn Sie mit dem Hinzufügen von Benutzerinformationen fertig sind, wählen Sie unten **Benutzer einladen**.

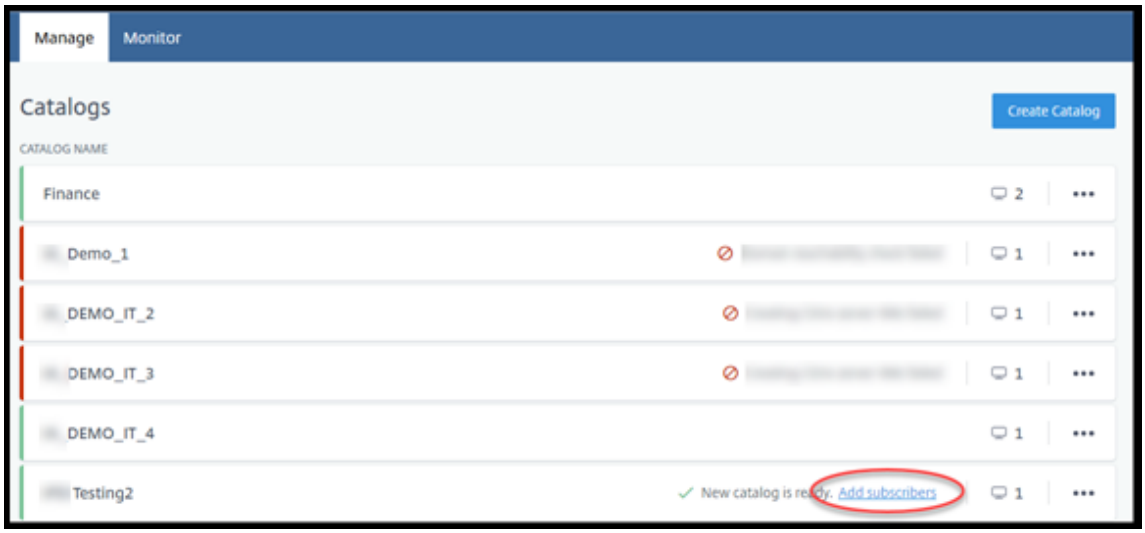
Zum Löschen eines Benutzers aus Managed Azure AD wählen Sie das Papierkorbsymbol neben dem Namen des Benutzers aus. Bestätigen Sie die Löschung.

Nachfolgende Schritte: Benutzer zum Katalog hinzufügen

### Hinzufügen oder Entfernen von Benutzern in einem Katalog

Dieses Verfahren gilt für alle Authentifizierungsmethoden.

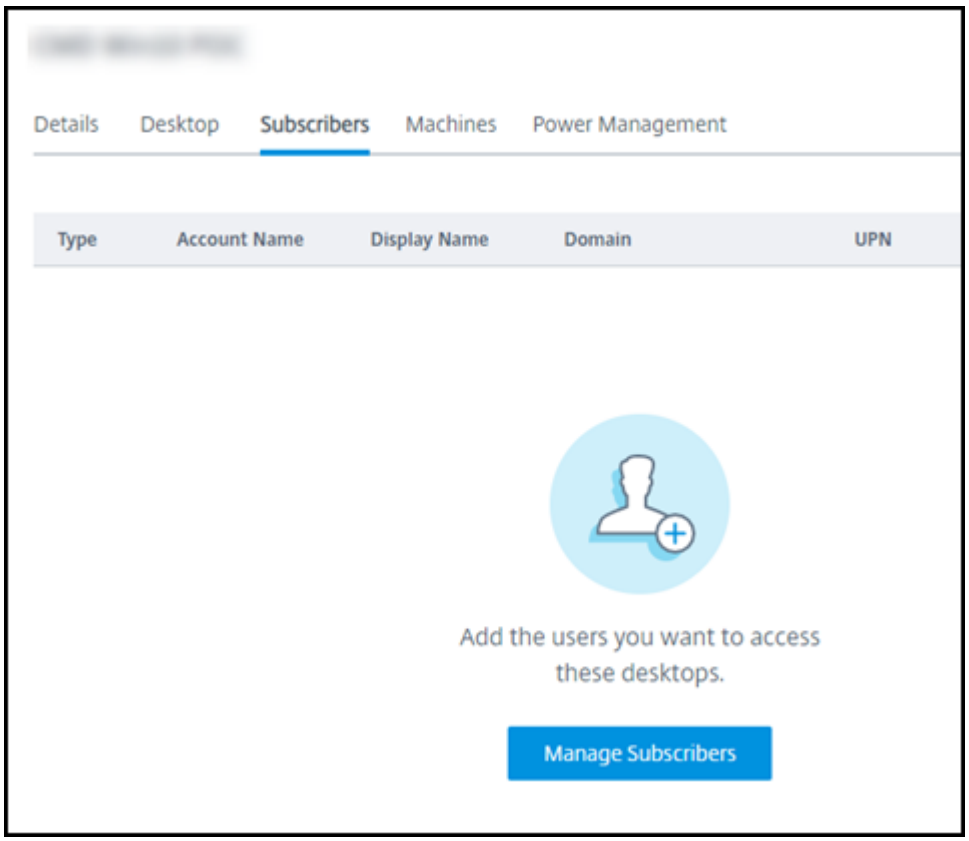
1. Wählen Sie unter **Verwalten > Quick Deploy** die Option **Abonnenten hinzufügen**, wenn Sie noch keine Benutzer zu einem Katalog hinzugefügt haben.



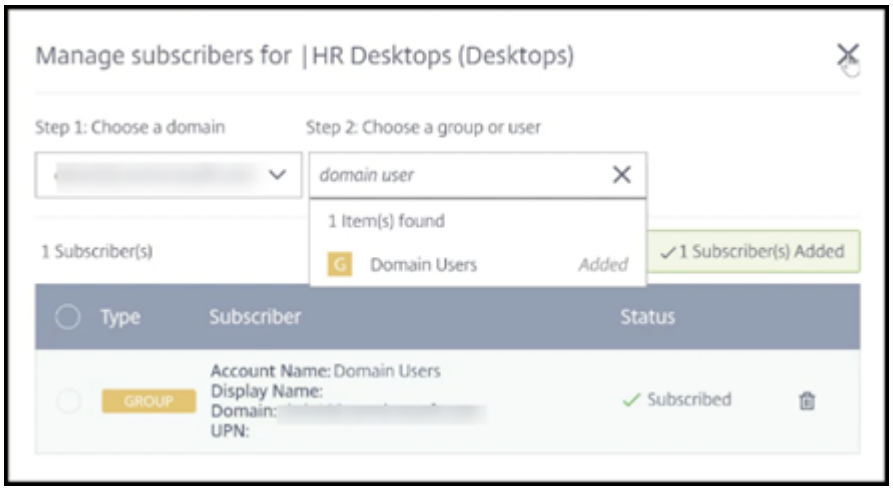

   Sollen Benutzer zu einem Katalog hinzugefügt werden, der bereits Benutzer enthält, klicken Sie auf eine beliebige Stelle im Katalogeintrag.

2. Wählen Sie auf der Registerkarte **Abonnenten** die Option **Abonnenten verwalten**.




3. Wählen Sie eine Domäne aus. (Wenn Sie Managed Azure AD zur Benutzerauthentifizierung verwenden, gibt es nur einen Eintrag im Domänenfeld.) Wählen Sie dann einen Benutzer aus.




4. Wählen Sie nach Bedarf weitere Benutzer aus. Wenn Sie fertig sind, wählen Sie das **X** oben rechts.

Zum Entfernen von Benutzern aus einem Katalog führen Sie die Schritte 1 und 2 aus. Wählen Sie in Schritt 3 das Papierkorbsymbol neben dem Namen des gewünschten Benutzers. Damit wird der Benutzer aus dem Katalog entfernt, nicht aber aus der Quelle (z. B. Managed Azure AD oder Ihr eigenes

AD oder AAD).

Nachfolgende Schritte:

- Bei einem Katalog mit Multisitzungsmaschinen fügen Sie Anwendungen hinzu, falls noch nicht geschehen.
- Bei allen Katalogen senden Sie die Citrix Workspace-URL an die Benutzer.

### Weitere Informationen

Weitere Informationen zur Authentifizierung in Citrix Cloud finden Sie unter Identitäts- und Zugriffsverwaltung.

## Remote-PC-Zugriff in Quick Deploy

August 30, 2023

### Einführung

Mit Citrix Remote-PC-Zugriff können Benutzer physische Windows- oder Linux-Maschinen im Büro remote verwenden. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Sitzungen verwenden.

Remote-PC-Zugriff unterstützt domänengebundene Maschinen.

In diesem Artikel wird beschrieben, wie Sie Remote-PC-Zugriff über die Quick Deploy-Schnittstelle bereitstellen. Informationen zum Bereitstellen von Remote-PC-Zugriff über die Schnittstelle "Vollständige Konfiguration"finden Sie unter Remote-PC-Zugriff.

#### Unterschiede zur Bereitstellung virtueller Desktops und Apps

Das Feature Remote-PC-Zugriff weist im Vergleich zur Bereitstellung virtueller Desktops und Apps mehrere Unterschiede auf:

- Ein Remote-PC-Zugriff-Katalog enthält normalerweise bestehende physische Maschinen. Zur Verwendung von Remote-PC-Zugriff ist demnach keine Imageerstellung und kein Maschinen-Provisioning erforderlich. Das Bereitstellen von Desktops und Apps umfasst normalerweise virtuelle Maschinen, für deren Provisioning ein Image als Vorlage verwendet wird.
- Wenn eine Maschine in einem zufälligen gepoolten Remote-PC-Zugriff-Katalog ausgeschaltet wird, wird sie nicht auf den ursprünglichen Status des Images zurückgesetzt.

- Bei Remote-PC-Zugriff-Katalogen mit statischer Benutzerzuweisung erfolgt die Zuweisung nach der Anmeldung eines Benutzers (an der Maschine oder über RDP). Bei der Bereitstellung von Desktops und Apps erfolgt die Benutzerzuweisung, wenn eine Maschine verfügbar ist.

### Zusammenfassung von Installation und Konfiguration

Lesen Sie diesen Abschnitt, bevor Sie mit der Arbeit beginnen.

1. Vorbereitungen:

   a) Lesen Sie die Anforderungen und Überlegungen.
   b) Führen Sie die Vorbereitungsaufgaben aus.

2. In Citrix Cloud:

   a) Richten Sie ein Citrix Cloud-Konto ein und abonnieren Sie Citrix DaaS.

   b) Richten Sie einen Ressourcenort ein, der auf Ihre Active Directory-Ressourcen zugreifen kann. Installieren Sie mindestens zwei Cloud Connectors am Ressourcenstandort. Die Cloud Connectors kommunizieren mit Citrix Cloud.

      Befolgen Sie die Anweisungen unter Erstellen eines Ressourcenstandorts und Installieren von Cloud Connectors. Diese Informationen umfassen Systemanforderungen, Vorbereitung und Verfahren.

   c) Verbinden Sie Active Directory mit Citrix Cloud.

3. Installieren Sie einen Citrix Virtual Delivery Agent (VDA) auf jeder Maschine, auf die Benutzer remote zugreifen sollen. Die VDAs kommunizieren mit Citrix Cloud über die Cloud Connectors am Ressourcenstandort.

4. Gehen Sie in **Verwalten > Quick Deploy** folgendermaßen vor:

   a) Erstellen Sie einen Katalog für den Remote-PC-Zugriff. In diesem Verfahren geben Sie den Ort des Ressourcenstandorts an und wählen die Benutzerzuweisungsmethode.
   b) Fügen Sie Abonnenten (Benutzer) zum Katalog hinzu, falls erforderlich. Fügen Sie Benutzer zu einem Katalog hinzu, wenn für den Katalog die Zuweisung "Statisch, automatisch zugewiesen"oder "Zufällig (gepoolte Desktops)"verwendet wird. Katalogen mit der Zuweisungsmethode "Statisch, vorab zugewiesen"müssen Sie keine Benutzer hinzufügen.

5. Senden Sie die Workspace-URL an die Benutzer. Über ihren Workspace können sich die Benutzer bei ihren Maschinen im Büro anmelden.

## Anforderungen und Überlegungen

Verweise auf Maschinen in diesem Abschnitt beziehen sich auf diejenigen Maschinen, auf die die Benutzer remote zugreifen.

### General

- Auf den Maschinen muss ein Einzelsitzungs-OS (Windows 10 oder Linux-Betriebssystem –Red Hat Enterprise Linux oder Ubuntu) ausgeführt werden.
- Die Maschinen müssen zu einer Active Directory-Domänendienste-Domäne gehören.
- Das Wake-on-LAN-Feature von Remote-PC-Zugriff für Citrix Virtual Apps and Desktops ist in Citrix DaaS nicht verfügbar.

### Netzwerk

- Die Maschine muss eine aktive Netzwerkverbindung haben. Eine Kabelverbindung wird für eine höhere Zuverlässigkeit und Bandbreite bevorzugt.
- Bei Verwendung von Wi-Fi:
  - Legen Sie die Energieeinstellungen so fest, dass der WLAN-Adapter eingeschaltet bleibt.
  - Konfigurieren Sie den WLAN-Adapter und das Netzwerkprofil so, dass die automatische Verbindung mit dem WLAN-Netzwerk vor der Benutzeranmeldung zulässig ist. Sonst wird der VDA erst registriert, wenn sich der Benutzer anmeldet. Die Maschine ist erst für den Remotezugriff verfügbar, wenn ein Benutzer sich anmeldet.
  - Stellen Sie sicher, dass die Cloud Connectors im Wi-Fi-Netzwerk erreichbar sind.

### Geräte und Peripheriegeräte

- Die folgenden Geräte werden nicht unterstützt:
  - KVM-Switches oder andere Komponenten, die eine Sitzung trennen.
  - Hybrid-PCs, einschließlich All-in-One- und NVIDIA Optimus-Laptops und -PCs.
- Schließen Sie Tastatur und Maus direkt an die Maschine an. Beim Anschließen an den Monitor oder an andere Komponenten, die ausgeschaltet oder getrennt werden können, sind diese Peripheriegeräte dann möglicherweise nicht mehr verfügbar. Wenn Sie Eingabegeräte an Komponenten wie beispielsweise Bildschirme anschließen müssen, schalten Sie diese Komponenten nicht aus.
- Laptops und Surface Pro-Geräte: Stellen Sie sicher, dass der Laptop an eine Stromquelle angeschlossen ist, anstatt mit dem Akku zu arbeiten. Konfigurieren Sie die Energieoptionen von Laptops wie bei Desktopmaschinen. Beispiel:

- Deaktivieren Sie den Ruhezustand.
- Deaktivieren Sie den Energiesparmodus.
- Legen Sie die Aktion beim Schließen des Deckels auf **Nichts tun** fest.
- Legen Sie die Aktion bei **Betätigen der Ein-/Ausschalttaste** auf **Herunterfahren** fest.
- Deaktivieren Sie die Energiesparfunktionen der Netzwerk- und der Grafikkarte.

Wenn Sie eine Dockingstation verwenden, können Sie Laptops abdocken und neu andocken. Wenn Sie einen Laptop abdocken, registriert sich der VDA bei Cloud Connectors neu über das Wi-Fi-Netzwerk. Wenn Sie den Laptop neu andocken, wechselt der VDA allerdings nicht zur Kabelverbindung, es sei denn, Sie trennen den WLAN-Adapter vom Netzwerk. Bei einigen Geräten sorgt eine integrierte Funktion für die Trennung des WLAN-Adapters beim Herstellen einer Kabelverbindung. Bei anderen ist eine benutzerdefinierte Lösung oder ein Hilfsprogramm eines Drittanbieters erforderlich. Konsultieren Sie in diesem Zusammenhang die zuvor erwähnten Wi-Fi-Überlegungen.

Zum Aktivieren des An- und Abdockens von Remote-PC-Zugriff-Geräten führen Sie folgende Schritte aus:

- Wählen Sie unter **Start > Einstellungen > System > Netzbetrieb und Standbymodus** für **Standbymodus** die Einstellung **Nie**.
- Rufen Sie unter **Geräte-Manager > Netzwerkadapter > Ethernet-Adapter** den Bereich **Energieverwaltung** auf und deaktivieren Sie **Computer kann das Gerät ausschalten, um Energie zu sparen**. Stellen Sie sicher, dass **Gerät kann den Computer aus dem Ruhezustand aktivieren** aktiviert ist.

#### Linux VDA

- Verwenden Sie den Linux-VDA auf physischen Maschinen nur im Nicht-3D-Modus. Aufgrund von Einschränkungen des NVIDIA-Treibers kann der lokale Bildschirm des PCs nicht ausgeblendet werden und zeigt die Aktivitäten der Sitzung an, wenn der HDX 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms ist ein Sicherheitsrisiko.
- Für Kataloge mit Linux-Maschinen muss die Benutzerzuweisungsmethode “Statisch, vorab zugewiesen”verwendet werden. Für Kataloge mit Linux-Maschinen können die Methoden “Statisch, automatisch zugewiesen”und “Zufällig (gepoolte Desktops)”nicht verwendet werden.

#### Hinweise zu Workspace

- Mehrere Benutzer mit Zugriff auf denselben Büro-PC sehen in Citrix Workspace dasselbe Symbol. Wenn sich ein Benutzer bei Citrix Workspace anmeldet, wird diese Maschine als nicht verfügbar angezeigt, wenn sie bereits von einem anderen Benutzer verwendet wird.

### Vorbereiten

- Überlegen Sie, wie Sie den VDA auf den Maschinen installieren möchten. Es stehen verschiedene Methoden zur Verfügung:
  - Manuelle Installation auf jeder Maschine.
  - Push-Installation per Gruppenrichtlinie mit einem Skript.
  - Push-Installation mit einem ESD-Tool zur elektronischen Softwareverteilung wie Microsoft System Center Configuration Manager (SCCM). Weitere Informationen finden Sie unter Installieren von VDAs mit SCCM.
- Informieren Sie sich über Methoden der Benutzerzuweisung und entscheiden Sie sich für eine Methode. Sie geben die Methode beim Erstellen eines Remote-PC-Zugriff-Katalogs an.
- Entscheiden Sie, wie sich die Maschinen (d. h. die VDAs auf den Maschinen) sich bei Citrix Cloud registrieren sollen. Die VDA-Registrierung ist für die Kommunikation mit dem Sitzungsbroker in Citrix Cloud erforderlich.

  Die VDAs registrieren sich über die Cloud Connectors an ihrem Ressourcenstandort. Cloud Connector-Adressen können Sie bei der Installation des VDA oder anschließend angeben.

  Für die erste VDA-Registrierung empfiehlt Citrix die Verwendung eines richtlinienbasierten GPO oder LGPO. Für den Zeitraum nach der ersten Registrierung empfiehlt Citrix die Verwendung der automatischen Aktualisierung, die standardmäßig aktiviert ist. Weitere Informationen zur VDA-Registrierung.

### Installieren von VDAs

Laden Sie einen VDA herunter und installieren Sie ihn auf jeder physischen Maschine, auf die Benutzer remote zugreifen sollen.

#### Herunterladen eines VDAs

- Gehen Sie zum Herunterladen eines Windows-VDAs folgendermaßen vor:
  1. Gehen Sie unter Verwendung Ihrer Citrix Cloud-Anmeldeinformationen zur Downloadseite von Citrix DaaS.
  2. Laden Sie den neuesten VDA herunter. Es stehen zwei Installationspaketarten zur Verfügung. Die Jahres- und Monatsangabe im VDA-Namen variieren.
- Zum Herunterladen eines Linux VDAs für Remote-PC-Zugriff folgen Sie den Anweisungen in der Linux VDA-Dokumentation.

**Windows-VDA-Installationspaketarten** Die Citrix Downloadseite bietet zwei Windows-VDA-Installationspaketarten für Remote-PC-Zugriffsmaschinen:

- Basis-Einzelsitzungs-VDA-Installationsprogramm (*Release* ist *jjmm*): `VDAWorkstationCoreSetup_rel.exe`

  Das Basis-Einzelsitzungs-VDA-Installationsprogramm ist speziell für Remote-PC-Zugriff zugeschnitten. Es ist kompakt und einfacher über das Netzwerk auf allen Maschinen bereitzustellen als andere VDA-Installationsprogramme. Es enthält keine Komponenten, die in solchen Bereitstellungen normalerweise nicht benötigt werden (z. B. Citrix Profilverwaltung, Machine Identity Service und die Benutzerpersonalisierungslayer).

  Ohne Citrix Profilverwaltung werden allerdings die Citrix Analytics for Performance-Daten und einige der Überwachungsdetails nicht angezeigt. Weitere Informationen zu diesen Einschränkungen finden Sie im Blogbeitrag Monitor and troubleshoot Remote PC Access machines.

  Wenn Sie vollständige Analyse- und Überwachungsdaten wünschen, verwenden Sie das vollständige Einzelsitzungs-VDA-Installationsprogramm.

- Vollständiges Einzelsitzungs-VDA-Installationsprogramm (*Release* ist *jjmm*): `VDAWorkstationSetup_re.exe`

  Das vollständige Einzelsitzungs-VDA-Installationsprogramm ist zwar größer als die Basis-Variante, doch können Sie nur die Komponenten zur Installation auswählen, die Sie benötigen. Sie können beispielsweise die Komponenten für die Profilverwaltung installieren.

#### Interaktive Installation eines Windows-VDAs für Remote-PC-Zugriff

1. Doppelklicken Sie auf die VDA-Installationsdatei, die Sie heruntergeladen haben.
2. Wählen Sie auf der Seite **Umgebung** die Option **Remote-PC-Zugriff aktivieren** und klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite **Delivery Controller** eine der folgenden Optionen aus:
   - Wenn Sie die Adressen Ihrer Cloud Connectors kennen, wählen Sie **Manuell**. Geben Sie den FQDN eines Cloud Connectors ein und klicken Sie auf **Hinzufügen**. Wiederholen Sie dies für die anderen Cloud Connectors an Ihrem Ressourcenstandort.
   - Wenn Sie wissen, wo die Cloud Connectors in Ihrer AD-Struktur installiert sind, wählen Sie **Standorte aus Active Directory auswählen** und gehen Sie zu diesem Speicherort. Wiederholen Sie dies für die anderen Cloud Connectors.
   - Wenn Sie die Cloud Connector-Adressen in der Citrix Gruppenrichtlinie angeben möchten, wählen Sie **Später (erweitert)** und bestätigen Sie die Auswahl, wenn Sie dazu aufgefordert werden.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

4. Wenn Sie das vollständige Einzelsitzungs-VDA-Installationsprogramm verwenden, wählen Sie auf der Seite **Zusätzliche Komponenten** die Komponenten aus, die Sie installieren möchten (z. B. Profilverwaltung). (Diese Seite wird nicht angezeigt, wenn Sie das Basis-Installationsprogramm verwenden.)
5. Klicken Sie auf der Seite **Features** auf **Weiter**.
6. Wählen Sie auf der Seite **Firewall** die Option **Automatisch** (falls sie noch nicht ausgewählt ist). Klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite **Zusammenfassung** auf **Installieren**.
8. Klicken Sie auf der Seite **Diagnose** auf **Verbinden**. Stellen Sie sicher, dass das Kontrollkästchen aktiviert ist. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein. Wenn Ihre Anmeldeinformationen überprüft sind, klicken Sie auf **Weiter**.
9. Klicken Sie auf der Seite **Fertig stellen** auf **Fertig stellen**.

Informationen zur vollständigen Installation finden Sie unter Installieren von VDAs.

#### Installieren eines Windows-VDAs für Remote-PC-Zugriff über die Befehlszeile

- Basis-Einzelsitzungs-VDA-Installationsprogramm: Führen Sie `VDAWorkstationCoreSetup.exe` unter Verwendung der Optionen `/quiet`, `/enable_hdx_ports` und `/enable_hdx_udp_ports` aus. Verwenden Sie die Option `/controllers`, um Cloud Connector-Adressen anzugeben.

  Beispiel zur Installation eines Basis-Einzelsitzungs-VDAs: Die Citrix Workspace-App und andere, nicht zu den Kernkomponenten gehörenden Dienste werden nicht installiert. Die FQDNs zweier Cloud Connectors werden angegeben und die Ports der Windows-Firewall werden automatisch geöffnet. Der Administrator steuert die Neustarts.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```

- Vollständiges Einzelsitzungs-VDA-Installationsprogramm mit Profilverwaltung (oder anderen optionalen Komponenten): Führen Sie `VDAWorkstationSetup.exe` mit den Optionen `/remotepc` und `/includeadditional` aus. Die Option `/remotepc` verhindert die Installation der meisten zusätzlichen Komponenten. Option `/includeadditional` gibt genau an, welche zusätzlichen Komponenten installiert werden sollen.

  Der folgende Befehl verhindert beispielsweise die Installation aller optionalen Komponenten mit Ausnahme der Profilverwaltung:

```
VDAWorkstationSetup.exe /quiet /remotepc /includeadditional "
Citrix User Profile Manager","Citrix User Profile Manager WMI
Plugin" /controllers "connector.domain.com" "connector2.domain.com
" /enable_hdx_ports /noresume /noreboot
```

Einzelheiten finden Sie unter Befehlszeilenoptionen zur VDA-Installation.

#### Installieren eines Linux VDAs

Folgen Sie die Anweisungen in der Linux-Dokumentation zur interaktiven Installation eines Linux VDAs bzw. zur Installation über die Befehlszeile.

### Erstellen Sie einen Remote-PC-Zugriff-Katalog

Zur Katalogerstellung ist ein Ressourcenstandort mit mindestens zwei Cloud Connectors erforderlich.

> **Wichtig:**
>
> Eine Maschine kann nur jeweils zu einem Maschinenkatalog gehören. Diese Einschränkung wird nicht erzwungen, wenn Sie die Maschinen für einen Katalog angeben. Wenn Sie die Einschränkung jedoch ignorieren, kann dies später zu Problemen führen.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü links oben **Eigene Services > DaaS**.
3. Wenn Sie noch keine Kataloge erstellt haben, klicken Sie auf der **Begrüßungsseite** auf **Erste Schritte**.
4. Wählen Sie **Verwalten > Quick Deploy**.
5. Wählen Sie **Katalog erstellen**.
6. Wählen Sie auf der Registerkarte **Remote-PC-Zugriff** eine Methode zum Zuweisen von Benutzern zu Maschinen.
7. Geben Sie einen Namen für den Katalog ein und wählen Sie den von Ihnen erstellten Ressourcenstandort aus.
8. Fügen Sie Maschinen hinzu.
9. Klicken Sie auf **Katalog erstellen**.
10. Klicken Sie auf der Seite **Ihr Remote-PC-Zugriff-Katalog wird erstellt** auf **Fertig**.

11. Ein Eintrag für den neuen Katalog wird im Dashboard **Verwalten > Quick Deploy** angezeigt.

    Nachdem der Katalog erfolgreich erstellt wurde, klicken Sie auf einen der Links, um Abonnenten (Benutzer) zum Katalog hinzuzufügen. Dieser Schritt gilt, wenn für den Katalog die Zuweisung "Statisch, automatisch zugewiesen"oder "Zufälliger Pool, nicht zugewiesen"verwendet wird.

Wenn Sie den Katalog erstellt und ggf. Benutzer hinzugefügt haben, senden Sie die Workspace-URL an die Benutzer.

### Methoden der Benutzerzuweisung

Die Benutzerzuweisungsmethode, die Sie beim Erstellen eines Katalogs auswählen, gibt an, wie Benutzer Maschinen zugewiesen werden.

- **Statisch, automatisch zugewiesen:** Die Benutzerzuweisung erfolgt, wenn sich ein Benutzer bei einer Maschine anmeldet (nicht über Citrix, sondern persönlich oder per RDP), nachdem ein VDA auf der Maschine installiert wurde. Wenn sich später andere Benutzer bei der Maschine ohne Citrix anmelden, werden sie ebenfalls zugewiesen. Es kann jeweils nur ein Benutzer die Maschine benutzen. Dies ist eine typische Einrichtung für Mitarbeiter, die sich eine Maschine teilen.

  Die Methode wird für Windows-Maschinen unterstützt. Sie kann nicht für Linux-Maschinen verwendet werden.

- **Statisch, vorab zugewiesen:** Benutzer werden Maschinen vorab zugewiesen. (Normalerweise geschieht dies durch Hochladen einer CSV-Datei mit Maschinen/Benutzerzuweisungen.) Nach der Installation des VDAs ist keine Benutzeranmeldung für die Einrichtung der Zuweisung erforderlich. Es ist auch nicht erforderlich, Benutzer dem Katalog zuzuweisen, nachdem dieser erstellt wurde. Diese Option eignet sich am besten für Mitarbeiter in Büros.

  Die Methode wird für Windows- und Linux-Maschinen unterstützt.

- **Zufälliger Pool, nicht zugewiesen:** Die Benutzer werden nach dem Zufallsprinzip einer verfügbaren Maschine zugewiesen. Es kann jeweils nur ein Benutzer die Maschine benutzen. Diese Methode eignet sich ideal für Computerlabore in Bildungseinrichtungen.

  Die Methode wird für Windows-Maschinen unterstützt. Sie kann nicht für Linux-Maschinen verwendet werden.

### Methoden zum Hinzufügen von Maschinen zu einem Katalog

Nicht vergessen: Auf jeder Maschine muss ein VDA installiert sein.

Beim Erstellen oder Bearbeiten eines Katalogs gibt es drei Möglichkeiten, Maschinen hinzuzufügen:

- Auswählen der einzelnen Maschinenkonten.
- Auswählen von Organisationseinheiten.
- Massenzuweisung per CSV-Datei. Für die CSV-Datei gibt es eine Vorlage.

#### Hinzufügen von Maschinennamen

Mit dieser Methode werden Maschinenkonten einzeln hinzugefügt.

1. Wählen Sie Ihre Domäne aus.
2. Suchen Sie das gewünschte Maschinenkonto.
3. Klicken Sie auf **Hinzufügen**.
4. Wiederholen Sie diese Schritte, um weitere Maschinen hinzuzufügen.
5. Wenn Sie fertig sind, klicken Sie auf **Fertig**.

#### Hinzufügen von Organisationseinheiten

Mit dieser Methode werden Maschinenkonten entsprechend ihrer Organisationseinheit hinzugefügt. Wählen Sie bei der Auswahl von Organisationseinheiten solche auf niedrigerer Ebene aus, um eine größere Detailgenauigkeit zu erzielen. Wenn eine solche Genauigkeit nicht erforderlich ist, können Sie übergeordnete Organisationseinheiten auswählen.

Wählen Sie beispielsweise im Fall von `Bank`/`Officers`/`Tellers` die Option `Tellers` aus, um eine größere Genauigkeit zu erzielen. Sonst können Sie `Officers` oder `Bank` wählen, je nach Anforderung.

Das Verschieben oder Löschen von Organisationseinheiten nachdem sie einem Remote-PC-Zugriff-Katalog zugewiesen wurden, wirkt sich auf VDA-Zuordnungen aus und verursacht Probleme mit zukünftigen Zuweisungen. Stellen Sie sicher, dass Ihr AD-Änderungsplan die Aktualisierung der Katalogzuweisung anhand der Organisationseinheit berücksichtigt.

Gehen Sie zum Hinzufügen von Organisationseinheiten folgendermaßen vor:

1. Wählen Sie Ihre Domäne aus.
2. Wählen Sie die Organisationseinheiten mit den gewünschten Maschinenkonten.
3. Geben Sie über das Kontrollkästchen an, ob Unterordner in Ihre Auswahl aufgenommen werden sollen.
4. Wenn Sie fertig sind, klicken Sie auf **Fertig**.

#### Hinzufügen in Massen

1. Klicken Sie auf **CSV-Vorlage herunterladen**.

2. Geben Sie in der Vorlage die Maschinenkonten an (bis zu 100 Einträge). Die CSV-Datei kann auch die Namen der Benutzer enthalten, die den Maschinen zugewiesen sind.
3. Speichern Sie die Datei.
4. Ziehen Sie die Datei mit der Maus auf die Seite **Maschinen in Massen hinzufügen** oder steuern Sie die Datei an.
5. Eine Vorschau des Dateiinhalts wird angezeigt. Wenn die Datei nicht wunschgemäß ist, können Sie eine weitere Datei erstellen und auswählen.
6. Wenn Sie fertig sind, klicken Sie auf **Fertig**.

### Verwalten von Remote-PC-Zugriff-Katalogen

Um die Konfiguration eines Remote-PC-Zugriff-Katalogs anzuzeigen oder zu ändern, wählen Sie den Katalog im Dashboard **Verwalten > Quick Deploy** aus (klicken Sie auf eine beliebige Stelle im Katalogeintrag).

- Auf der Registerkarte **Details** können Sie Maschinen hinzufügen oder entfernen.
- Auf der Registerkarte **Abonnenten** können Sie Benutzer hinzufügen oder entfernen.
- Auf der Registerkarte **Maschinen** haben Sie folgende Möglichkeiten:
  - Maschinen hinzufügen oder entfernen: Schaltfläche **Maschinen hinzufügen oder entfernen**.
  - Benutzerzuweisungen ändern: Papierkorbsymbol für den **Zuweisung entfernen** und **Maschinenzuweisung bearbeiten** im Menü.
  - Anzeigen der Registrierungsinformationen von Maschinen und Aktivieren/Deaktivieren des Wartungsmodus.

## Überwachung in Quick Deploy

May 18, 2022

Im Dashboard **Überwachung** können Sie die Desktopnutzung, Sitzungen und Maschinen in Ihrer Bereitstellung von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) anzeigen. Sie können außerdem Sitzungen steuern, die Energieverwaltung von Maschinen einrichten und laufende Anwendungen sowie laufende Prozesse beenden.

Zum Aufrufen des Dashboards **Überwachung** gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Citrix Cloud an, falls Sie es noch nicht getan haben. Wählen Sie im Menü links oben **Eigene Services > DaaS**.
2. Wählen Sie im Dashboard **Verwalten > Quick Deploy** die Registerkarte **Überwachen**.

## Überwachen der Desktopnutzung

Die Seite wird alle fünf Minuten aktualisiert.

- **Überblick über Maschinen und Sitzungen:** Sie können die Anzeige so wählen, dass Informationen zu allen Katalogen (Standard) oder zu einem ausgewählten Katalog angezeigt werden. Sie können auch den Zeitraum wählen: den letzten Tag, die letzte Woche, den Monat oder das Vierteljahr.

  Zähler im oberen Bereich zeigen die Gesamtzahl der Maschinen sowie die Anzahl der ein- und ausgeschalteten Maschinen. Wenn Sie mit der Maus auf einen Wert zeigen, wird die Zahl der Einzelsitzungs- und der Multisitzungsmaschinen eingeblendet.

  Die Kurve unterhalb der Zähler zeigt die Anzahl der eingeschalteten Maschinen sowie den Spitzenwert gleichzeitiger Sitzungen in regelmäßigen Abständen während des ausgewählten Zeitraums. Zeigen Sie auf einen Punkt auf der Kurve, um die Zähler an dem Punkt anzuzeigen.


- **Top 10:** Um eine Top-10-Anzeige anzupassen, wählen Sie einen Zeitraum aus: die letzte Woche (Standard), den Monat oder drei Monate. Sie können die Anzeige auch so einrichten, dass nur Informationen zu Aktivitäten an Einzelsitzungsmaschinen, Multisitzungsmaschinen oder Anwendungen angezeigt werden.

  - **10 aktivste Benutzer:** Listet die Benutzer auf, die während des Zeitraums am häufigsten Desktops gestartet haben. Durch Zeigen auf eine Zeile wird die Gesamtzahl der Starts angezeigt.
  - **Top 10 der aktiven Kataloge:** Listet die Kataloge mit der längsten Dauer während des ausgewählten Zeitraums auf. Die Dauer drückt die Summe aller Benutzersitzungen aus dem Katalog aus.

#### Bericht über die Desktopnutzung

Um einen Bericht zu Maschinenstarts im letzten Monat herunterzuladen, wählen Sie **Startaktivitäten**. Eine Meldung zeigt an, dass die Anforderung verarbeitet wird. Der Bericht wird automatisch in den Standardordner für Downloads auf der lokalen Maschine heruntergeladen.

### Filter und Suche bei der Überwachung von Maschinen und Sitzungen

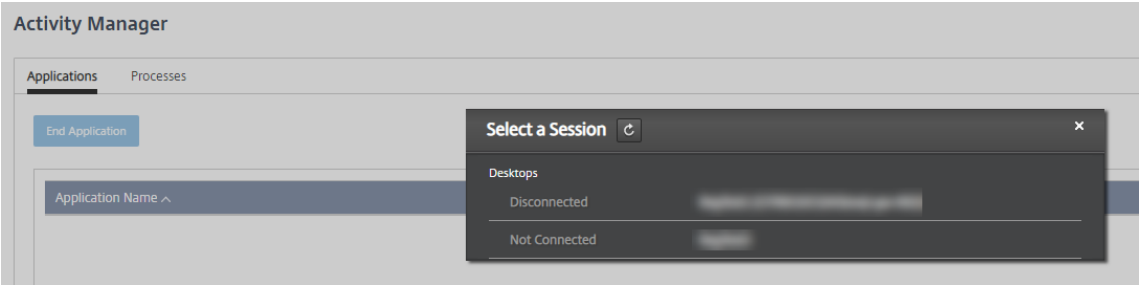
Wenn Sie Sitzungs- und Maschineninformationen überwachen, werden standardmäßig alle Maschinen bzw. Sitzungen angezeigt. Sie haben folgende Möglichkeiten:

- Filtern der Anzeige nach Maschinen, Sitzungen, Verbindungen oder Anwendungen.
- Einrichten der Anzeige von Sitzungen oder Maschine durch Auswahl der gewünschten Kriterien mithilfe von Ausdrücken in einem eigens erstellten Filter.
- Speichern der erstellten Filter zur Wiederverwendung.

### Steuern der Anwendungen eines Benutzers

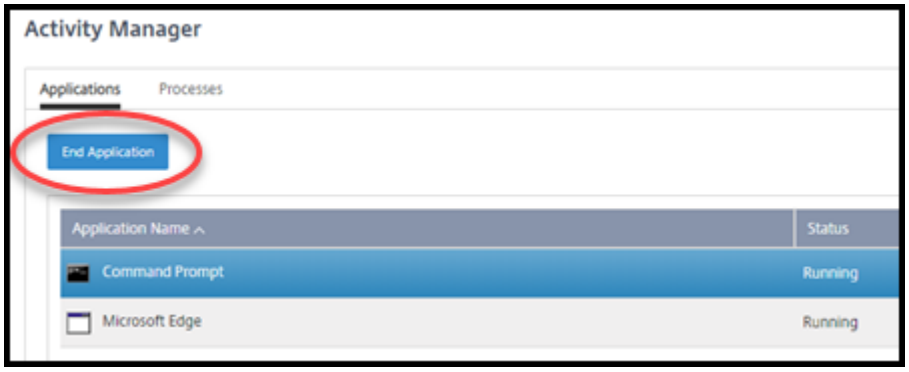
Sie können Anwendungen und Prozesse für einen Benutzer anzeigen und verwalten, der eine laufende Sitzung oder einen zugewiesenen Desktop hat.

1. Wählen Sie im Dashboard **Überwachen** von Citrix DaaS die Option **Suchen** und geben Sie den Benutzernamen (oder die Anfangszeichen des Benutzernamens), die Maschine oder den Endpunkt ein. Wählen Sie im Suchergebnis das gewünschte Objekt. (Um das Suchfeld ohne zu suchen einzuklappen, wählen Sie erneut **Suchen**.)
2. Wählen Sie eine Sitzung.

   Im Aktivitätsmanager werden die Anwendungen und Prozesse für die Sitzung des Benutzers aufgelistet.
3. Um eine Anwendung zu beenden, wählen Sie auf der Registerkarte **Anwendungen** im Aktivitätsmanager die Zeile mit der Anwendung und dann **Anwendung beenden**.




4. Um einen Prozess zu beenden, wählen Sie auf der Registerkarte **Prozesse** im Aktivitätsmanager die Zeile des Prozesses und dann **Prozess beenden**.
5. Um Sitzungsdetails anzuzeigen, wählen Sie oben rechts die Option **Details**. Um zur Anzeige der Anwendungen und Prozesse zurückzukehren, wählen Sie oben rechts "Aktivitätsmanager".
6. Um die Sitzung zu steuern, wählen Sie **Sitzungssteuerung > Abmelden** oder **Sitzungssteuerung > Trennen**.

## Spiegeln von Benutzern

Mit dem Feature zum Spiegeln können Sie die virtuelle Maschine oder Sitzung eines Benutzers direkt anzeigen und darauf arbeiten. Sie können Windows- und Linux-VDAs spiegeln. Der Benutzer muss mit der zu spiegelnden Maschine verbunden sein. Um die Verbindung zu überprüfen, überprüfen Sie den in der `User`-Titelleiste aufgeführten Maschinennamen.

Das Spiegeln wird in einer neuen Browserregisterkarte gestartet. Stellen Sie sicher, dass Ihr Browser Popups der Citrix Cloud-URL zulässt.

Spiegeln wird nur für Benutzer domänengebundener Maschinen unterstützt. Um eine nicht in domänengebundene Maschine zu spiegeln, müssen Sie eine Bastionsmaschine einrichten. Einzelheiten finden Sie unter Bastion-Zugang.

Das Spiegeln muss von einer Maschine im virtuellen Netzwerk der domänengebundenen Maschinen gestartet werden und alle Portanforderungen erfüllen.

### Aktivieren des Features "Spiegeln"

1. Gehen Sie unter **Verwalten > Quick Deploy > Überwachen** zur Ansicht **Benutzerdetails**.
2. Wählen Sie die Benutzersitzung und dann **Spiegeln** in der Ansicht **Aktivitätsmanager** oder im Bereich **Sitzungsdetails**.

#### Spiegeln von Linux-VDAs

Spiegeln ist bei Linux-VDAs ab Version 7.16 möglich, auf denen die Linux-Distribution RHEL7.3 oder Ubuntu Version 16.04 ausgeführt wird.

Der Überwachungsdienst verwendet den FQDN zum Herstellen einer Verbindung mit dem Linux-VDA. Vergewissern Sie sich, dass der Überwachungsclient den FQDN des Linux-VDAs auflösen kann.

- Auf dem VDA müssen die Pakete `python-websockify` und `x11vn` installiert sein.
- Die `noVNC`-Verbindung zum VDA verwendet das WebSocket-Protokoll. Standardmäßig wird das WebSocket-Protokoll `ws://` verwendet. Aus Sicherheitsgründen empfiehlt Citrix, das Protokoll `wss://` zu verwenden. Installieren Sie SSL-Zertifikate auf jedem Überwachungsclient und Linux-VDA.

Folgen Sie den Anweisungen unter "Sitzungsspiegelung", um den Linux VDA für die Spiegelung zu konfigurieren.

1. Wenn Sie die Spiegelung aktiviert haben, wird die Spiegelungsverbindung initialisiert und auf dem Benutzergerät eine Bestätigungsaufforderung angezeigt.
2. Weisen Sie die Benutzer an, **Ja** zu wählen, um die Maschinen- oder die Sitzungsfreigabe zu starten.
3. Der Administrator kann nur die gespiegelte Sitzung anzeigen.

#### Spiegeln von Windows-VDAs

Windows-VDA-Sitzungen werden mithilfe der Windows-Remoteunterstützung gespiegelt. Aktivieren Sie das Feature `Use Windows Remote Assistance` bei der Installation des VDA.

1. Wenn Sie die Spiegelung aktiviert haben, wird die Verbindung initialisiert und es erscheint ein Dialogfeld mit der Aufforderung, die Datei `.msrc incident` zu öffnen oder zu speichern.
2. Öffnen Sie die Datei mit dem Remoteunterstützung-Viewer, wenn er nicht standardmäßig ausgewählt ist. Auf dem Benutzergerät wird eine Bestätigungsaufforderung angezeigt.
3. Weisen Sie die Benutzer an, **Ja** zu wählen, um die Maschinen- oder die Sitzungsfreigabe zu starten.
4. Fordern Sie den Benutzer auf, die Tastatur- und Maussteuerung freizugeben, damit Sie die Steuerung übernehmen können.

### Überwachen und Steuern von Sitzungen

Die Sitzungsanzeige wird jede Minute aktualisiert.

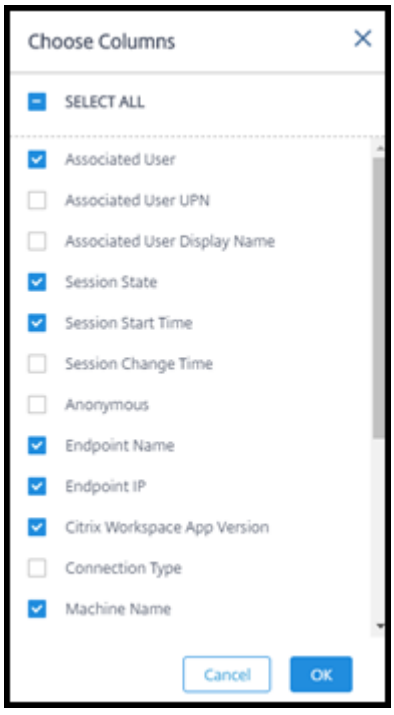
Neben dem Anzeigen von Sitzungen können Sie Sitzungen trennen und Benutzer von Sitzungen abmelden.

1. Wählen Sie unter **Verwalten > Quick Deploy > Überwachen** die Option **Filter**.


2. Wählen Sie die Ansicht **Sitzungen**.


3. Um die Anzeige anzupassen, wählen Sie **Spalten auswählen** und aktivieren Sie die Kontrollkästchen der Elemente, die angezeigt werden sollen. Wenn Sie fertig sind, wählen Sie **OK**. Die Sitzungsanzeige wird automatisch aktualisiert.




4. Aktivieren Sie das Kontrollkästchen links neben jeder Sitzung, die Sie steuern möchten.
5. Um die Sitzung abzumelden oder zu trennen, wählen Sie **Sitzungssteuerung > Abmelden** oder **Sitzungssteuerung > Trennen**.

Auch der Energieverwaltungszeitplan für den Katalog kann das Trennen von Sitzungen und das Abmelden von Benutzern von getrennten Sitzungen steuern.

Alternativ zum obigen Verfahren können Sie auch mit **Suchen** einen Benutzer suchen, die gewünschte Sitzung auswählen und dann die Sitzungsdetails anzeigen. Die Optionen zum Abmelden und Trennen sind hier ebenfalls verfügbar.

#### Bericht über Sitzungsinformationen

Um Sitzungsinformationen herunterzuladen, wählen Sie in der Sitzungsanzeige **Exportieren**. Eine Meldung zeigt an, dass die Anforderung verarbeitet wird. Der Bericht wird automatisch in den Standardordner für Downloads auf der lokalen Maschine heruntergeladen.

### Überwachung und Energiesteuerung von Maschinen

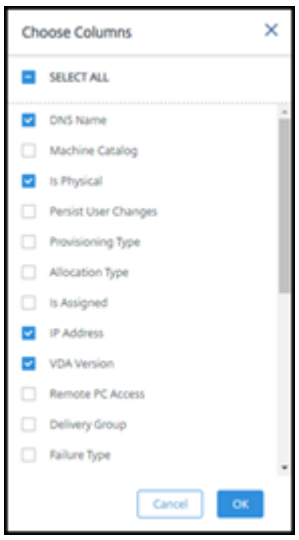
Die Anzeige der Maschinen wird jede Minute aktualisiert.

1. Wählen Sie unter **Verwalten > Quick Deploy > Überwachen** die Option **Filter**.
2. Wählen Sie die Ansicht **Maschinen**.

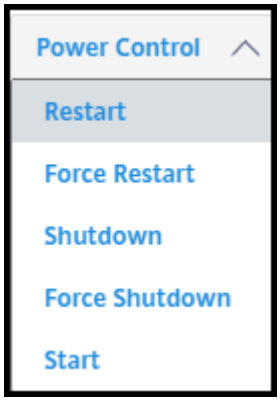

   Standardmäßig werden hier Einzelsitzungs-OS-Maschinen angezeigt. Sie können auch Multisitzungsmaschinen anzeigen.

3. Um die Anzeige anzupassen, wählen Sie **Spalten auswählen** und aktivieren Sie die Kontrollkästchen der Elemente, die angezeigt werden sollen. Wenn Sie fertig sind, wählen Sie **OK**. Die Maschinenanzeige wird automatisch aktualisiert.




4. Zur Energiesteuerung oder um den Wartungsmodus für Maschinen zu aktivieren bzw. zu deaktivieren, aktivieren Sie das Kontrollkästchen links neben jeder gewünschten Maschine.
5. Wählen Sie **Energieverwaltung** und dann eine Aktion.




6. Um den Wartungsmodus für die ausgewählten Maschinen zu aktivieren bzw. zu deaktivieren, wählen Sie **Wartungsmodus > EIN** bzw. **Wartungsmodus > AUS**.

Wenn Sie eine Maschine mit der Suchfunktion suchen und auswählen, werden Maschinendetails, Auslastung, historische Auslastung (der letzten sieben Tage) und durchschnittliche IOPS angezeigt.

### Maschinenbericht

Zum Herunterladen von Sitzungsinformationen wählen Sie auf der Maschinenanzeige **Exportieren** . Eine Meldung zeigt an, dass die Anforderung verarbeitet wird. Der Bericht wird automatisch in den Standardordner für Downloads auf der lokalen Maschine heruntergeladen.

### Überprüfen der Integrität von Apps und Desktops

Das Testfeature automatisiert die Überprüfung der Integrität veröffentlichter Apps und Desktops. Das Ergebnis der Integritätsprüfung steht im Dashboard **Überwachen** zur Verfügung. Einzelheiten finden Sie in den folgenden Abschnitten:

- Anwendungstests
- Desktoptests

## Problembehandlung in Quick Deploy

April 19, 2022

### Einführung

Ressourcenstandorte enthalten die Maschinen zur Bereitstellung von Desktops und Apps. Die Maschinen werden in Katalogen erstellt, daher gelten Kataloge als Teil des Ressourcenstandorts. Jeder Ressourcenstandort enthält außerdem Cloud Connectors. Cloud Connectors ermöglichen die Kommunikation zwischen Citrix Cloud und dem Ressourcenstandort. Normalerweise installiert und aktualisiert Citrix die Cloud Connectors.

Optional können Sie verschiedene Aktionen an Cloud Connectors und Ressourcenstandorten ausführen. Siehe:

- Aktionen für Ressourcenstandorte
- Einstellungen für den Ressourcenstandort beim Erstellen eines Katalogs

Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) bietet Tools zur Problembehandlung und Supportability Tools, mit deren Hilfe Sie Konfigurations- und Kommunikationsprobleme an Maschinen zur Bereitstellung von Desktops und Apps (VDAs) beheben können. Das Erstellen eines Katalogs kann beispielsweise fehlschlagen oder Benutzer können ihren Desktop oder ihre Apps nicht starten.

Zur Problembehandlung gehört der Zugriff auf Ihr Citrix Managed Azure-Abonnement über eine Bastionsmaschine oder eine direkte RDP-Verbindung. Nach dem Zugreifen auf das Abonnement können Sie Citrix Supportability Tools verwenden, um Probleme zu finden und zu beheben. Einzelheiten finden Sie in den folgenden Abschnitten:

- VDA-Problembehandlung mit einer Bastion oder einer direkten RDP-Verbindung
- Bastion-Zugang
- Direkter RDP-Zugriff

### VDA-Problembehandlung mit einer Bastion oder einer direkten RDP-Verbindung

Die Supportability Tools sind für Personen vorgesehen, die Erfahrung mit der Behebung von Citrix Problemen haben. Hierzu gehören:

- Citrix Service Provider und andere Personen mit technischer Kompetenz im Bereich der Citrix DaaS-Produkte.
- Mitarbeiter des Citrix Supports.

Wenn Sie mit der Problembehandlung von Citrix Komponenten nicht vertraut sind, können Sie Hilfe vom Citrix Support anfordern. Citrix Supportmitarbeiter bitten Sie möglicherweise um die Einrichtung einer der in diesem Abschnitt beschriebenen Zugriffsmethoden. Die eigentliche Problembehandlung mit von Citrix Tools und Technologien führen allerdings die Supportmitarbeiter selbst durch.

> **Wichtig:**
>
> Diese Supportability Tools sind nur für domänengebundene Maschinen vorgesehen. Wenn die Maschinen in Ihren Katalogen nicht zur Domäne gehören, werden Sie zur Anforderung von Hilfe beim Citrix Support geleitet.

#### Zugriffsmethoden

Diese Zugriffsmethoden gelten nur für das Citrix Managed Azure-Abonnement. Weitere Informationen finden Sie unter Azure-Abonnements.

Es gibt zwei Zugriffsmethoden.

- Zugreifen über eine Bastionsmaschine im dedizierten Citrix Managed Azure-Abonnement. Die Bastion ist ein einzelner Zugangspunkt zu den Maschinen im Abonnement. Sie stellt eine sichere Verbindung zu diesen Ressourcen bereit, indem sie Remotedatenverkehr von IP-Adressen eines bestimmten Bereichs zulässt.

  Die Schritte dieser Methode sind folgende:

  - Erstellen der Bastionsmaschine
  - Herunterladen eines RDP-Agents
  - Herstellen der RDP-Verbindung zur Bastionsmaschine
  - Herstellen der Verbindung von der Bastionsmaschine mit den anderen Citrix Maschinen im Abonnement

  Die Bastionsmaschine ist für den kurzfristigen Gebrauch vorgesehen. Diese Methode ist für Probleme bei der Erstellung von Katalogen oder Imagemaschinen vorgesehen.

- Direkter RDP-Zugriff auf die Maschinen im dedizierten Citrix Managed Azure-Abonnement. Um RDP-Datenverkehr zuzulassen, muss Port 3389 in der Netzwerksicherheitsgruppe definiert werden.

Diese Methode ist für Probleme mit Katalogen vorgesehen, die nicht mit deren Erstellung verbunden sind, z. B. wenn Benutzer ihre Desktops nicht starten können.

Nicht vergessen: Alternativ zu den beiden Zugriffsmethoden können Sie auch Hilfe vom Citrix Support erhalten.

### Bastion-Zugang

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Problembehandlung & Support**.
2. Klicken Sie auf **Problembehandlungsoptionen anzeigen**.
3. Wählen Sie auf der Seite **Problembehandlung** einen der ersten beiden Problemtypen aus und klicken Sie dann auf **Verwenden Sie unsere Problembehandlungsmaschine**.
4. Wählen Sie auf der Seite **Problembehandlung mit Bastionsmaschine** den Katalog aus.
   - Wenn die Maschinen in dem Katalog nicht zur Domäne gehören, werden Sie angewiesen, sich an den Citrix Support zu wenden.
   - Wurde bereits eine Bastionsmaschine mit RDP-Zugriff auf die Netzwerkverbindung des ausgewählten Katalogs erstellt wurde, fahren Sie mit Schritt 8 fort.
5. Der RDP-Zugriffsbereich wird angezeigt. Wenn Sie den RDP-Zugriff auf einen kleineren Bereich einschränken möchten, als die Netzwerkverbindung zulässt, aktivieren Sie das Kontrollkästchen **RDP-Zugriff auf Computer im IP-Adressbereich beschränken** und geben Sie den gewünschten Bereich ein.
6. Geben Sie einen Benutzernamen und ein Kennwort ein, mit denen Sie sich bei der Bastionsmaschine anmelden werden. Kennwortanforderungen.

   Verwenden Sie keine Unicode-Zeichen im Benutzernamen.
7. Klicken Sie auf **Bastionsmaschine erstellen**.

   Wenn die Bastionsmaschine erstellt ist, ändert sich der Seitentitel in **Bastion - *Verbindung***.

   Wenn die Erstellung der Bastionsmaschine fehlschlägt (oder während deren Betriebs Fehler auftreten), klicken Sie unten in der Fehlermeldung auf **Löschen**. Erstellen Sie dann eine neue Bastionsmaschine.

   Sie können die RDP-Bereichsbeschränkung ändern, nachdem die Bastionsmaschine erstellt wurde. Klicken Sie auf **Edit**. Geben Sie den neuen Wert ein und klicken Sie auf das Häkchen, um die Änderung zu speichern. (Klicken Sie auf **X**, um die Änderung zu verwerfen.)
8. Klicken Sie auf **RDP-Datei herunterladen**.

9. Erstellen Sie eine RDP-Verbindung mit der Bastion unter Verwendung der Anmeldeinformationen, die Sie beim Erstellen der Bastion angegeben haben. (Die Adresse der Bastionsmaschine ist in der heruntergeladenen RDP-Datei eingebettet.)
10. Stellen Sie die Verbindung von der Bastionsmaschine mit den anderen Citrix Maschinen im Abonnement her. Sie können nun Protokolle sammeln und Diagnosen ausführen.

Bastionsmaschinen werden bei Erstellung eingeschaltet. Um Kosten zu sparen, werden die Maschinen automatisch ausgeschaltet, wenn sie nach dem Start im Leerlauf bleiben. Die Maschinen werden nach einigen Stunden automatisch gelöscht.

Mit den Schaltflächen unten auf der Seite können Sie die Energieverwaltung einer Bastionsmaschine steuern oder die Maschine löschen. Wenn Sie eine Bastionsmaschine löschen möchten, müssen Sie bestätigen, dass alle aktiven Sitzungen auf der Maschine automatisch beendet werden. Außerdem werden alle Daten, die auf der Maschine gespeichert wurden, gelöscht.

### Direkter RDP-Zugriff

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Problembehandlung & Support**.
2. Klicken Sie auf **Problembehandlungsoptionen anzeigen**.
3. Wählen Sie auf der Seite **Problembehandlung** die Option **Anderes Katalogproblem**.
4. Wählen Sie auf der Seite **Problembehandlung mit RDP-Zugriff** den Katalog.

   Wurde RDP bereits für die Netzwerkverbindung des ausgewählten Katalogs aktiviert, fahren Sie mit Schritt 7 fort.
5. Der RDP-Zugriffsbereich wird angezeigt. Wenn Sie den RDP-Zugriff auf einen kleineren Bereich einschränken möchten, als die Netzwerkverbindung zulässt, aktivieren Sie das Kontrollkästchen **RDP-Zugriff auf Computer im IP-Adressbereich beschränken** und geben Sie den gewünschten Bereich ein.
6. Klicken Sie auf **RDP-Zugriff aktivieren**.

   Wenn der RDP-Zugriff aktiviert wurde, ändert sich der Seitentitel in **RDP-Zugriff - *Verbindung***.

   Kann der RDP-Zugriff nicht aktiviert werden, klicken Sie unten in der Fehlermeldung auf **Erneut versuchen** .
7. Stellen Sie unter Verwendung Ihrer Active Directory-Administratoranmeldeinformationen eine Verbindung mit Maschinen her. Sie können nun Protokolle sammeln und Diagnosen ausführen.

### Hilfe und Unterstützung

Können Probleme nicht gelöst werden, erstellen Sie ein Supportticket. Folgen Sie hierfür den Anweisungen unter Hilfe und Support.

## Quick Deploy-Referenz

August 8, 2022

### Katalog-Registerkarten im Quick Deploy-Dashboard

Klicken Sie im Dashboard von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unter **Verwalten > Quick Deploy** auf eine beliebige Stelle des Katalogeintrags. Die folgenden Registerkarten enthalten Informationen über den Katalog:

- **Details:** Informationen, die bei der Erstellung des Katalogs (oder seiner letzten Bearbeitung) angegeben wurden. Die Registerkarte enthält auch Informationen über das zum Erstellen des Katalogs verwendete Image.

  Auf dieser Registerkarte können Sie folgende Aufgaben erledigen:

  - Image löschen, das im Katalog verwendet wird.
  - Katalog löschen.
  - Aufrufen der Seite mit Details zu dem vom Katalog verwendeten Ressourcenstandort.

- **Desktop:** Nur für Kataloge verfügbar, die Einzelsitzungsmaschinen (statische oder zufällige Maschinen) enthalten. Auf dieser Registerkarte können Sie den Namen und die Beschreibung des Katalogs ändern.

- **Desktop und Apps:** Die Registerkarte **Desktops und Apps** ist nur für Kataloge mit Multisitzungsmaschinen verfügbar. Auf dieser Registerkarte können Sie folgende Aufgaben erledigen:

  - Anwendungen, auf die Benutzer des Katalogs in Citrix Workspace zugreifen können, hinzufügen, bearbeiten oder entfernen.
  - Den Namen und die Beschreibung des Katalogs ändern.

- **Abonnenten:** Liste aller Benutzer einschließlich Typ (Benutzer oder Gruppe), des Kontonamens, des Anzeigenamens, der zugehörigen Active Directory-Domäne und des Benutzerprinzipalnamens.

  Auf dieser Registerkarte können Sie für einen Katalog Benutzer hinzufügen oder entfernen.

- **Maschinen:** Gesamtzahl der Maschinen im Katalog sowie die Anzahl der registrierten und der nicht registrierten Maschinen und der im Wartungsmodus.

  Für jede Maschine im Katalog werden Name, Betriebszustand (ein/aus), den Registrierungsstatus (registriert/nicht registriert), die zugewiesenen Benutzer, die Sitzungsanzahl (0/1) und der Wartungsmodusstatus (ein- oder ausgeschaltet) angezeigt.

  Auf dieser Registerkarte können Sie folgende Aufgaben erledigen:

  - Maschinen hinzufügen und löschen
  - Maschinen starten, neu starten, einen Neustart erzwingen oder herunterfahren
  - Wartungsmodus ein- und ausschalten

  Einzelheiten finden Sie unter Verwalten von Katalogen. Viele Aktionen an Maschinen sind auch auf der Registerkarte **Überwachen** im Quick Deploy-Dashboard verfügbar. Siehe Überwachung und Energiesteuerung von Maschinen.

- **Energieverwaltung:** Ermöglicht die Steuerung des Ein- und Ausschaltens der Maschinen im Katalog. Ein Zeitplan zeigt an, wann Maschinen im Leerlauf getrennt werden.

  Sie können einen Energiezeitplan konfigurieren, wenn Sie einen benutzerdefinierten Katalog erstellen, oder auch später. Wenn kein Zeitplan festgelegt ist, schalten sich Maschinen ab, wenn eine Sitzung endet.

  Sie können keinen Energiesparplan auswählen oder konfigurieren, wenn Sie einen Katalog per Schnellerstellung erstellen. Standardmäßig wird bei der Schnellerstellung die Voreinstellung “Kostenersparnis”verwendet. Sie können einen Katalog jedoch später bearbeiten und den Zeitplan ändern.

  Einzelheiten finden Sie unter Verwalten von Energieverwaltungszeitplänen.

### DNS-Server

Dieser Abschnitt gilt für alle Bereitstellungen mit domänengebundenen Maschinen. Sie können ihn ignorieren, wenn Sie nur nicht domänengebundene Maschinen verwenden.

1. Bevor Sie einen domänengebundenen Katalog erstellen (oder, im Fall eines Citrix Managed Azure-Abonnements eine Verbindung), prüfen Sie, ob Sie DNS-Servereinträge haben, die öffentliche und private Domänennamen auflösen können.

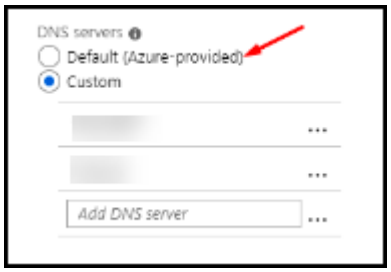
   Bei der Katalog- bzw. Verbindungserstellung muss Citrix DaaS mindestens einen gültigen DNS-Servereintrag finden. Wenn keine gültigen Einträge gefunden werden, schlägt die Erstellung fehl.

   Wo Sie dies prüfen können:

- Wenn Sie Ihr eigenes Azure-Abonnement verwenden, prüfen Sie den Eintrag **DNS-Server** in Ihrem Azure-Konto.
- Wenn Sie ein Citrix Managed Azure-Abonnement haben und eine Azure VNet-Peering-Verbindung erstellen, prüfen Sie den Eintrag **DNS-Server** in dem Azure VNet, das Sie per Peering verbinden.
- Wenn Sie ein Citrix Managed Azure-Abonnement haben und eine SD-WAN-Verbindung erstellen, prüfen Sie die DNS-Servereinträge in SD-WAN Orchestrator.

2. In Azure muss die Einstellung **Benutzerdefiniert** mindestens einen gültigen Eintrag enthalten. Der Service kann nicht mit der Einstellung **Standard (von Azure bereitgestellt)** verwendet werden.




- Wenn **Standard (von Azure bereitgestellt)** aktiviert ist, ändern Sie die Einstellung in **Benutzerdefiniert** und fügen Sie mindestens einen DNS-Servereintrag hinzu.
- Wenn Sie bereits DNS-Servereinträge unter **Benutzerdefiniert** haben, stellen Sie sicher, dass diejenigen, die Sie mit diesem Dienst verwenden möchten, öffentliche und private Domänen-IP-Namen auflösen können.
- Wenn Sie keine DNS-Server haben, die Domänennamen auflösen können, empfiehlt Citrix, einen von Azure bereitgestellten DNS-Server hinzuzufügen, der über diese Funktionen verfügt.

3. Wenn Sie einen DNS-Servereintrag ändern, starten Sie alle Maschinen neu, die mit dem virtuellen Netzwerk verbunden sind. Durch den Neustart werden die neuen DNS-Servereinstellungen zugewiesen. (Die VMs verwenden die aktuellen DNS-Einstellungen weiter, bis sie neu gestartet werden.)

   Ändern von DNS-Adressen nachdem eine Verbindung hergestellt wurde:

- Wenn Sie Ihr eigenes Azure-Abonnement verwenden, können Sie die Adressen in Azure ändern (s. o.). Alternativ können Sie sie im Service ändern.
- Wenn Sie Citrix Managed Azure-Abonnent sind, synchronisiert der Service keine DNS-Adressänderungen, die Sie in Azure vornehmen. Sie können allerdings die DNS-Einstellungen für die Verbindung in diesem Service ändern.

Denken Sie daran, dass das Ändern von DNS-Serveradressen zu Verbindungsproblemen für Maschinen in Katalogen führen kann, die diese Verbindung verwenden.

#### Hinzufügen von DNS-Servern über den Service

Stellen Sie vor dem Hinzufügen einer DNS-Serveradresse zu einer Verbindung sicher, dass der DNS-Server öffentliche und interne Domänennamen auflösen kann. Citrix empfiehlt, die Verbindung zu einem DNS-Server zu testen, bevor Sie ihn hinzufügen.

1. Um eine DNS-Serveradresse beim Erstellen einer Verbindung hinzuzufügen, zu ändern oder zu entfernen, wählen Sie auf der Seite *Verbindungstyp* **hinzufügen** die Option **DNS-Server bearbeiten**. Wird gemeldet, dass keine DNS-Serveradressen gefunden wurden, wählen Sie **DNS-Server hinzufügen**. Fahren Sie mit Schritt 3 fort.
2. Gehen Sie zum Hinzufügen, Ändern oder Entfernen einer DNS-Serveradresse für eine vorhandene Verbindung folgendermaßen vor:
    a) Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Netzwerkverbindungen**.
    b) Wählen Sie die gewünschte Verbindung.
    c) Wählen Sie **DNS-Server bearbeiten**.
3. Fügen Sie Adressen hinzu, bzw. ändern oder entfernen Sie Adressen.
    a) Um eine Adresse hinzuzufügen, wählen Sie **DNS-Server hinzufügen** und geben Sie die IP-Adresse ein.
    b) Um eine Adresse zu ändern, klicken Sie in das Adressfeld und ändern Sie die Werte.
    c) Um eine Adresse zu entfernen, wählen Sie das Papierkorbsymbol neben dem Adresseintrag aus. Sie können nicht alle DNS-Serveradressen entfernen. Die Verbindung benötigt mindestens eine Adresse.
4. Wenn Sie fertig sind, wählen Sie unten auf der Seite **Änderungen bestätigen**.
5. Starten Sie alle Maschinen neu, die die Verbindung verwenden. Durch den Neustart werden die neuen DNS-Servereinstellungen zugewiesen. (Die VMs verwenden die aktuellen DNS-Einstellungen weiter, bis sie neu gestartet werden.)

### Richtlinien

#### Festlegen von Gruppenrichtlinien für nicht domänengebundene Maschinen

1. Stellen Sie eine RDP-Verbindung mit der Maschine her, die für das Image verwendet wird.
2. Installieren Sie Citrix Gruppenrichtlinienverwaltung:
    a) Navigieren Sie zu CTX220345. Laden Sie den Anhang herunter.
    b) Doppelklicken Sie auf die heruntergeladene Datei. Doppelklicken Sie im Ordner `Group Policy Templates` 1912 > `Group Policy Management` auf `CitrixGroupPolicyManagement_x64.msi`.

3. Starten Sie mit dem Befehl **Ausführen** `gpedit.msc`, um den Gruppenrichtlinien-Editor zu öffnen.
4. Wählen Sie in `User Configuration Citrix Policies > Unfiltered` **Richtlinie bearbeiten**.

   Wenn die Gruppenrichtlinien-Verwaltungskonsole ausfällt (wie in CTX225742 beschrieben), installieren Sie Microsoft Visual C++ 2015 Runtime (oder eine höhere Version).
5. Aktivieren Sie Richtlinieneinstellungen nach Bedarf. Beispiel:

   - Wählen Sie unter **Computer Configuration** or **User Configuration** (je nachdem, was Sie konfigurieren möchten) auf der Registerkarte **Settings** in `Category > ICA / Printing` für **Auto-create PDF Universal Printer** die Einstellung `Enabled`.
   - Sollen angemeldete Benutzer Administratoren ihres Desktops sein, fügen Sie die Gruppe **interactive User** der Gruppe der vordefinierten Administratoren hinzu.
6. Wenn Sie fertig sind, speichern Sie das Image.
7. Aktualisieren Sie den vorhandenen Katalog oder erstellen Sie einen neuen Katalog mit dem neuen Image.

#### Festlegen von Gruppenrichtlinien für domänengebundene Maschinen

1. Stellen Sie sicher, dass die Gruppenrichtlinienverwaltung installiert ist.

   - Fügen Sie auf Windows-Multisitzungsmaschinen die Gruppenrichtlinienverwaltung mit dem Windows-Tool zum Hinzufügen von Rollen und Features (z. B. **Rollen und Features hinzufügen**) hinzu.
   - Installieren Sie auf Windows-Einzelsitzungsmaschinen die Remoteserver-Verwaltungstools für das entsprechende Betriebssystem. (Die Installation erfordert Domänenadministratorkonto.) Nach der Installation steht die Gruppenrichtlinienverwaltungskonsole im **Startmenü** zur Verfügung.
2. Laden Sie die Citrix Gruppenrichtlinienverwaltung von der Citrix Downloadseite herunter, installieren Sie das Paket und konfigurieren Sie dann Richtlinieneinstellungen nach Bedarf. Folgen Sie den Anweisungen in Festlegen von Gruppenrichtlinien für nicht domänengebundene Maschinen ab Schritt 2 bis zum Ende.

Die Referenz für Richtlinieneinstellungen enthält Informationen zu den verfügbaren Einstellungen. Alle Richtlinienfeatures sind über die Oberfläche "Vollständige Konfiguration"in Citrix DaaS verfügbar.

## Aktionen für Ressourcenstandorte

Citrix erstellt automatisch einen Ressourcenstandort und zwei Cloud Connectors, wenn Sie den ersten Katalog zum Veröffentlichen von Desktops und Apps erstellen. Sie können beim Erstellen eines Katalogs einige Informationen zum Ressourcenstandort angeben. Siehe Einstellungen für den Ressourcenstandort beim Erstellen eines Katalogs.

Bei Remote-PC-Zugriff erstellen Sie den Ressourcenstandort und die Cloud Connectors.

In diesem Abschnitt werden mögliche Aktionen nach dem Erstellen eines Ressourcenstandorts beschrieben.

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**.
2. Wählen Sie das Abonnement.

    - Auf der Registerkarte **Details** werden die Anzahl und Namen der Kataloge und Images im Abonnement angezeigt. Außerdem wird die Anzahl der Maschinen angezeigt, die Desktops oder Apps bereitstellen können. Diese Angabe umfasst keine für andere Zwecke verwendete Maschinen wie (Images, Cloud Connectors, RDS-Lizenzserver usw.).
    - Auf der Registerkarte **Ressourcenstandorte** werden alle Ressourcenstandorte aufgeführt. Jeder Ressourcenstandorteintrag umfasst den Status und die Adresse aller Cloud Connectors am Ressourcenstandort.

Das Menü für Ressourcenstandorte enthält die folgenden Aktionen.

### Systemintegritätsprüfung ausführen

Bei Auswahl von **Systemintegritätsprüfung ausführen** wird eine sofortige Verbindungsprüfung ausgeführt. Wird die Prüfung nicht bestanden, ist der Status des Cloud Connectors unbekannt, da er nicht mit Citrix Cloud kommuniziert. Es empfiehlt sich in diesem Fall ein Cloud Connector-Neustart.

### Neustarten von Connectors

Citrix empfiehlt, jeweils nur einen Cloud Connector neu zu starten. Durch das Neustarten von Cloud Connectors werden diese offline geschaltet und der Benutzerzugriff und die Maschinenkonnektivität werden unterbrochen.

Aktivieren Sie das Kontrollkästchen für den Cloud Connector, den Sie neu starten möchten. Wählen Sie **Neu starten**.

### Hinzufügen von Connectors

Das Hinzufügen eines Cloud Connectors dauert normalerweise 20 Minuten.

Geben Sie die folgenden Informationen an:

- Wie viele Cloud Connectors hinzugefügt werden sollen.
- Anmeldeinformationen für das Domänendienstkonto, die verwendet werden, um die Cloud Connector-Maschinen der Domäne hinzuzufügen.
- Maschinenleistung.
- Azure-Ressourcengruppe. Der Standardwert ist die Ressourcengruppe, die zuletzt vom Ressourcenstandort verwendet wurde
- Organisationseinheit (OU) Der Standardwert ist die zuletzt vom Ressourcenstandort verwendete OU.
- Ob Ihr Netzwerk einen Proxyserver für die Internetverbindung benötigt. Wenn Sie **Ja** angeben, geben Sie den FQDN oder die IP-Adresse des Proxyservers und die Portnummer an.

Wenn Sie fertig sind, wählen Sie **Connectors hinzufügen**.

### Löschen von Connectors

Wenn ein Cloud Connector nicht mit Citrix Cloud kommunizieren kann und ein Neustart das Problem nicht behebt, empfiehlt der Citrix Support möglicherweise, den Cloud Connector zu löschen.

Aktivieren Sie das Kontrollkästchen für den Cloud Connector, den Sie löschen möchten. Wählen Sie **Löschen**. Bestätigen Sie die Löschung.

Sie können auch einen verfügbaren Cloud Connector löschen. Wenn durch das Löschen eines Cloud Connectors jedoch weniger als zwei verfügbaren Cloud Connectors am Ressourcenstandort verbleiben würden, können Sie den ausgewählten Cloud Connector nicht löschen.

### Wählen der Aktualisierungszeit

Citrix stellt automatisch Softwareupdates für Cloud Connectors bereit. Während eines Updates wird ein Cloud Connector offline geschaltet und aktualisiert, während die anderen weiterarbeiten. Wenn das erste Update abgeschlossen ist, wird der nächste Cloud Connector offline geschaltet und aktualisiert. Dieser Vorgang wird fortgesetzt, bis alle Cloud Connectors am Ressourcenstandort aktualisiert sind. Der beste Startzeitpunkt für Updates liegt normalerweise außerhalb der Geschäftszeiten.

Wählen Sie die Uhrzeit für den Updatestart aus oder geben Sie an, dass Updates beim Verfügbarwerden gestartet werden sollen. Wenn Sie fertig sind, wählen Sie **Speichern**.

#### Umbenennen

Geben Sie den neuen Namen für den Ressourcenstandort ein. Wählen Sie **Speichern**.

#### Konfigurieren der Konnektivität

Geben Sie an, ob die Benutzer über Citrix Gateway oder nur von Ihrem Unternehmensnetzwerk aus auf Desktops und Apps zugreifen können sollen.

### Profilverwaltung

Die Profilverwaltung stellt sicher, dass persönliche Benutzereinstellungen für virtuelle Anwendungen unabhängig vom Standort des Benutzergeräts gelten.

Das Konfigurieren der Profilverwaltung ist optional.

Sie können die Profilverwaltung durch den Profiloptimierungsdienst aktivieren. Dieser Dienst bietet eine zuverlässige Möglichkeit zum Verwalten dieser Einstellungen in Windows. Durch das Verwalten der Profile wird eine konsistente Benutzererfahrung sichergestellt, indem ein einzelnes Profil gepflegt wird, das dem Benutzer folgt. Benutzerprofile werden automatisch konsolidiert und optimiert, um Verwaltungs- und Speicheranforderungen zu minimieren. Der Profiloptimierungsdienst erfordert nur minimale Verwaltung, Unterstützung und Infrastruktur. Auch die An- und Abmeldung wird durch die Profiloptimierung erleichtert.

Der Profiloptimierungsdienst erfordert eine Dateifreigabe, in der alle persönlichen Einstellungen beibehalten werden. Sie verwalten die Dateiserver. Wir empfehlen, eine Netzwerkverbindung einzurichten, um den Zugriff auf diese Dateiserver zu ermöglichen. Sie müssen die Freigabe als UNC-Pfad angeben. Der Pfad kann Systemumgebungsvariablen, Active Directory-Benutzerattribute oder Profilverwaltungsvariablen enthalten. Weitere Informationen zum Format der UNC-Textzeichenfolge finden Sie unter Angeben des Pfads zum Benutzerspeicher.

Beim Aktivieren der Profilverwaltung können Sie das Benutzerprofil weiter optimieren, indem Sie durch eine konfigurierte Ordnerumleitung die Auswirkungen der Benutzerprofilgröße minimieren. Das Anwenden der Ordnerumleitung ergänzt die Profilverwaltungslösung. Weitere Informationen finden Sie unter Microsoft-Ordnerumleitung.

### Konfigurieren des Microsoft RDS-Lizenzservers für Windows Server-Workloads

Dieser Dienst greift bei der Bereitstellung einer Windows Server-Workload (z. B. Windows 2016) auf Windows Server-Remotesitzungsfunktionen zu. Dies erfordert in der Regel eine Clientzugriffslizenz für Remotedesktopdienste (RDS CAL). Die Windows-Maschine mit dem Citrix VDA muss in der Lage sein, RDS-CALs von einem RDS-Lizenzserver anzufordern.

Installieren und aktivieren Sie den Lizenzserver. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Aktivieren des Remotedesktopdienste-Lizenzservers. Für Machbarkeitsstudien können Sie den von Microsoft bereitgestellten Kulanzzeitraum verwenden.

Mit dieser Methode können Sie die Lizenzservereinstellungen in Citrix DaaS anwenden. Sie können den Lizenzserver und den "Pro-Benutzer"-Lizenzmodus in der RDS-Konsole auf dem Image konfigurieren. Sie können den Lizenzserver auch über die Microsoft-Gruppenrichtlinieneinstellungen konfigurieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter License your RDS deployment with client access licenses (CALs).

Konfigurieren des RDS-Lizenzservers über die Gruppenrichtlinieneinstellungen

1. Installieren Sie einen Lizenzserver für die Remotedesktopdienste auf einer der verfügbaren VMs. Diese VM muss immer verfügbar sein. Citrix DaaS-Workloads müssen auf diesen Lizenzserver zugreifen können.
2. Geben Sie über die Microsoft-Gruppenrichtlinie die Lizenzserveradresse ein und legen Sie den "Pro-Benutzer"-Lizenzmodus fest. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Specify the Remote Desktop Licensing Mode for an RD Session Host Server.

Windows 10-Workloads erfordern eine Windows 10-Lizenzaktivierung. Wir empfehlen, dass Sie zum Aktivieren von Windows 10-Workloads die Microsoft-Dokumentation befolgen.

### Verbrauchsverpflichtung

> **Hinweis:**
>
> Dieses Feature ist als Preview verfügbar.

Wählen Sie unter **Verwalten > Quick Deploy** die Registerkarte **Allgemein**. Der Wert für **Verbrauch** gibt den Verbrauch im aktuellen Kalendermonat an. Der Wert beinhaltet die monatliche und die Laufzeitverbrauchsverpflichtung.

Wenn Sie **Allgemein** auswählen, enthält die Registerkarte **Benachrichtigungen** Folgendes:

- Gesamtverbrauch für den Monat (monatlich und Laufzeit).
- Anzahl Einheiten der monatlichen Verbrauchsverpflichtung.
- Anteil an der Laufzeitverbrauchsverpflichtung in Prozent.

Die Werte und Fortschrittsbalken können auf potenzielle oder tatsächliche Nutzungsüberschreitungen hinweisen.

Es kann 24 Stunden dauern, bis die aktuellen Daten erscheinen. Nutzungs- und Abrechnungsdaten gelten 72 Stunden nach Ende eines Kalendermonats als endgültig.

Weitere Informationen zur Nutzung finden Sie unter Überwachen der Lizenzen und der aktiven Nutzung.

Sie können optional die Anzeige von Benachrichtigungen im Dashboard **Verwalten > Quick Deploy** aktivieren, wenn der Verbrauch (monatliche, Laufzeit- oder beides) ein bestimmtes Niveau erreicht. Standardmäßig sind diese Benachrichtigungen deaktiviert.

1. Wählen Sie auf der Registerkarte **Benachrichtigungen** die Option **Benachrichtigungseinstellungen bearbeiten**.
2. Um die Benachrichtigungen zu aktivieren, klicken Sie auf den Schieberegler, damit das Häkchen angezeigt wird.
3. Geben Sie einen Wert ein. Wiederholen Sie dies bei Bedarf für den anderen Verbrauchstyp.
4. Wählen Sie **Speichern**.

Um die Benachrichtigungen zu deaktivieren, klicken Sie auf den Schieberegler, sodass das Häkchen nicht mehr angezeigt wird, und wählen Sie **Speichern**.

### Überwachen der Citrix Lizenznutzung

Befolgen Sie die Anweisungen unter Überwachen der Lizenzen und der aktiven Nutzung, um Informationen zur Citrix Lizenznutzung anzuzeigen. Sie können Folgendes anzeigen:

- Zusammenfassung zur Lizenzierung
- Nutzungsberichte
- Nutzungstrends und Lizenzaktivität
- Lizenzierte Benutzer

Sie können auch Lizenzen freigeben.

### Lastausgleich

Der Lastausgleich gilt nur für Multisitzungsmaschinen, nicht aber für Einzelsitzungsmaschinen.

> **Wichtig:**
>
> Das Ändern der Lastausgleichmethode wirkt sich auf alle Kataloge in Ihrer Bereitstellung aus. Dazu gehören alle Kataloge, die mit einem unterstützten Hosttyp erstellt wurden –cloudbasiert und on-premises und unabhängig von der verwendeten Schnittstelle (z. B. vollständige Konfiguration, Quick Deploy).
>
> Stellen Sie sicher, dass die maximalen Sitzungslimits für alle Kataloge konfiguriert wurden, bevor Sie fortfahren.
>
> - In Quick Deploy finden Sie die Einstellung auf der Registerkarte **Details** jedes Katalogs.

> • Angaben zur vollständigen Konfiguration finden Sie unter Lastausgleich bei Maschinen.

Der Lastausgleich misst die Maschinenlast und bestimmt, welche Multisitzungsmaschine unter den aktuellen Bedingungen für eine eingehende Benutzersitzung ausgewählt werden soll. Die Auswahl basiert auf der konfigurierten Lastausgleichsmethode.

Es stehen zwei Lastausgleichsmethoden zur Auswahl: horizontal und vertikal. Die Methode gilt für alle Multisitzungskataloge (und folglich für alle Multisitzungsmaschinen) in der Citrix DaaS-Bereitstellung.

- **Horizontaler Lastausgleich:** Weist eine eingehende Benutzersitzung der am wenigsten ausgelasteten, eingeschalteten Maschine zu.

  Einfaches Beispiel: Sie haben zwei Maschinen für jeweils zehn Sitzungen konfiguriert. Die erste Maschine verarbeitet die ersten fünf gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet fünf Sitzungen.

  Der horizontale Lastausgleich bietet eine hohe Benutzerleistung, kann jedoch auch die Kosten erhöhen, da mehr Maschinen laufen und genutzt werden.

  Diese Methode ist standardmäßig aktiviert.

- **Vertikaler Lastausgleich:** Eingehende Benutzersitzungen werden der eingeschalteten Maschine mit dem höchsten Lastindex zugewiesen. Citrix DaaS berechnet für jede Multisitzungsmaschine einen Lastindex und weist ihr diesen zu. Die Berechnung berücksichtigt Faktoren wie CPU, Speicher und Gleichzeitigkeit.

  Bei dieser Methode werden vorhandene Maschinen vollständig genutzt, bevor zu neuen Maschinen gewechselt wird. Wenn Benutzer die Verbindung trennen und Kapazität auf Maschinen freigeben, wird diesen Maschinen neue Last zugewiesen.

  Einfaches Beispiel: Sie haben zwei Maschinen für jeweils zehn Sitzungen konfiguriert. Die erste Maschine verarbeitet die ersten zehn gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet die elfte Sitzung.

  Beim vertikalen Lastenausgleich wird die Kapazität der eingeschalteten Maschinen maximiert, was Maschinenkosten sparen kann.

Gehen Sie zum Konfigurieren der Lastausgleichsmethode folgendermaßen vor:

1. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Allgemein**.
2. Wählen Sie unter **Globale Einstellungen** die Option **Alle anzeigen**.
3. Wählen Sie auf der Seite **Globale Einstellungen** unter **Lastausgleich für Multisitzungskataloge** die Lastausgleichsmethode.
4. Wählen Sie **Bestätigen**.

### Erstellen eines Katalogs in einem Netzwerk mit Proxyserver

Gehen Sie wie nachfolgend beschrieben vor, wenn in Ihrem Netzwerk ein Proxyserver für die Internetverbindung verwendet wird und Sie Ihr eigenes Azure-Abonnement nutzen. (Citrix Managed Azure-Abonnements können nicht mit einem Netzwerk mit Proxyserver verwendet werden.)

1. Beginnen Sie unter **Verwalten > Quick Deploy** die Katalogerstellung durch Angeben der erforderlichen Informationen und Auswählen von **Katalog erstellen** unten auf der Seite.
2. Die Katalogerstellung schlägt aufgrund der Anforderung eines Proxys fehl. Es wird jedoch ein Ressourcenstandort erstellt. Der Name des Ressourcenstandorts beginnt mit "DAS", es sei denn, Sie haben beim Erstellen des Katalogs einen Ressourcenstandortnamen angegeben. Erweitern Sie unter **Verwalten > Quick Deploy** auf der rechten Seite **Cloud-Abonnements**. Sehen Sie auf der Registerkarte **Ressourcenstandorte** nach, ob der neu erstellte Ressourcenstandort über Cloud Connectors verfügt. Wenn ja, löschen Sie sie.
3. Erstellen Sie in Azure zwei virtuelle Maschinen (siehe Systemanforderungen für Cloud Connectors). Fügen Sie die Maschinen der Domäne hinzu.
4. Installieren Sie einen Cloud Connector über die Citrix Cloud-Konsole auf jeder VM. Stellen Sie sicher, dass die Cloud Connectors an dem zuvor erstellten Ressourcenstandort sind. Folgen Sie den Anweisungen in folgenden Artikeln:
   - Konfiguration von Cloud Connector-Proxy und Firewall
   - Anforderungen an System und Konnektivität
5. Wiederholen Sie unter **Verwalten > Quick Deploy** die Katalogerstellung. Der erstellte Katalog verwendet den Ressourcenstandort und die Cloud Connectors, die Sie in den vorherigen Schritten erstellt haben.

### Hilfe und Unterstützung

- Lesen Sie den Artikel zur Problembehandlung.
- Wenn Sie weitere Unterstützung bei Citrix DaaS benötigen, können Sie ein Supportticket erstellen, gemäß den Anweisungen unter Hilfe und Support.

## Bereitstellungsgruppen erstellen

June 12, 2024

## Einführung

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Die Bereitstellungsgruppe kann außerdem angeben, welche Benutzer die enthaltenen Maschinen verwenden können und welche Anwendungen bzw. Desktops ihnen zur Verfügung stehen sollen.

Das Erstellen einer Bereitstellungsgruppe ist nach dem Erstellen eines Maschinenkatalogs der nächste Schritt beim Konfigurieren der Bereitstellung. Später können Sie die anfänglichen Einstellungen der ersten Bereitstellungsgruppe ändern und weitere Bereitstellungsgruppen erstellen. Es gibt Features und Einstellungen, die Sie nur beim Bearbeiten einer Bereitstellungsgruppe, nicht aber beim Erstellen konfigurieren können.

Vorbereitung:

- Lesen Sie diesen Abschnitt über die Optionen, die Sie auswählen, und welche Informationen Sie angeben müssen.
- Stellen Sie sicher, dass Sie eine Verbindung zum Hypervisor, Cloudservice oder zu anderen Ressourcen hergestellt haben, die Ihre Maschinen hosten.
- Stellen Sie sicher, dass Sie einen Maschinenkatalog mit virtuellen oder physischen Maschinen erstellt haben.

So starten Sie den Assistenten zum Erstellen von Bereitstellungsgruppen:

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
2. Wählen Sie **Verwalten**.
3. Wenn Sie die erste Bereitstellungsgruppe erstellen, werden Sie zur richtigen Auswahl geführt (z. B. “Bereitstellungsgruppen einrichten und als Dienste anzeigen”). Der Assistent zum Erstellen von Bereitstellungsgruppen wird geöffnet und führt Sie durch die Konfiguration.
4. Wenn Sie bereits eine Bereitstellungsgruppe erstellt haben und eine weitere erstellen möchten, gehen Sie wie folgt vor:
    a) Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
    b) Um Bereitstellungsgruppen mit Ordnern zu organisieren, erstellen Sie Ordner im Standardordner **Bereitstellungsgruppen**. Weitere Informationen finden Sie unter Gruppenordner erstellen.
    c) Wählen Sie den Ordner aus, in dem Sie die Gruppe erstellen möchten, und klicken Sie auf **Bereitstellungsgruppe erstellen**. Der Assistent zum Erstellen von Gruppen wird geöffnet.

Der Assistent führt Sie durch die in den folgenden Abschnitten beschriebenen Seiten. Die angezeigten Assistentenseiten können sich je nach vorgenommener Auswahl unterscheiden.

### Schritt 1: Maschinen

Wählen Sie einen Maschinenkatalog und die Anzahl der Maschinen, die Sie aus dem Katalog verwenden möchten.

Nützliche Info:

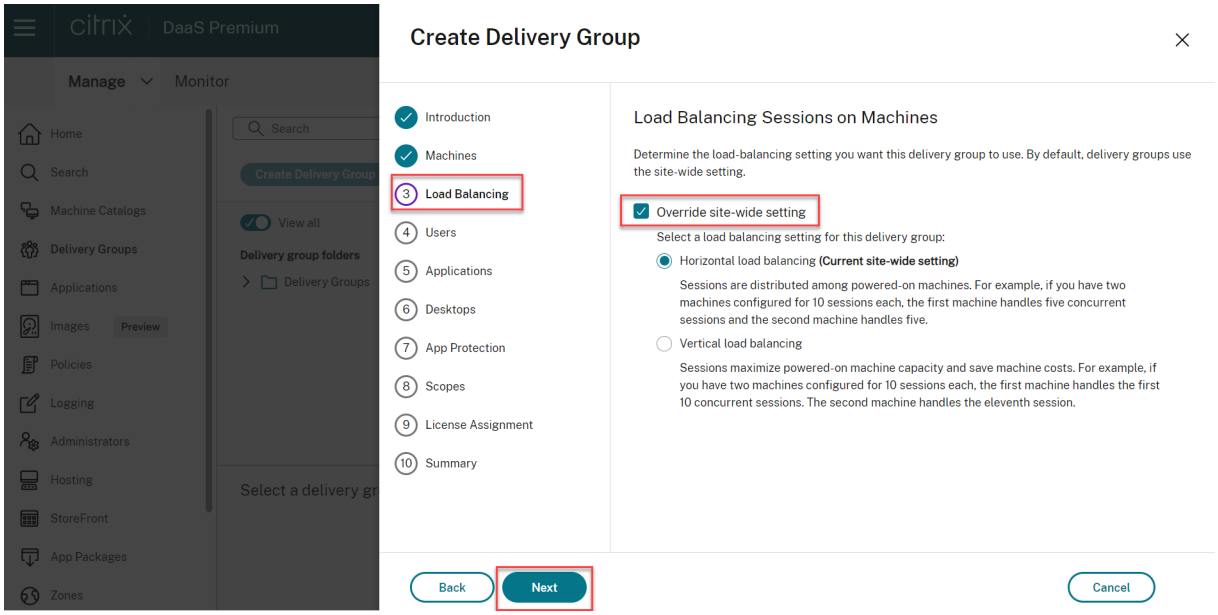
- Mindestens eine Maschine in dem ausgewählten Katalog muss unbenutzt bleiben.
- Ein Katalog kann in mehreren Bereitstellungsgruppen angegeben werden. Eine Maschine kann jedoch nur in einer Bereitstellungsgruppe verwendet werden.
- Eine Bereitstellungsgruppe kann Maschinen aus mehreren Katalogen verwenden. Diese Kataloge müssen allerdings Maschinen desselben Typs enthalten (Multisitzungs-OS- oder Einzelsitzungs-OS-Maschinen oder Remote-PC-Zugriff-Maschinen). Sie können also in einer Bereitstellungsgruppe nicht verschiedene Maschinentypen mischen. Umfasst Ihre Bereitstellung Maschinenkataloge für Windows-Maschinen und solche für Linux-Maschinen, darf eine Bereitstellungsgruppe nur Maschinen eines Betriebssystems enthalten.
- Eine MCS-Bereitstellungsgruppe kann nur einen Katalog des Typs MCS hinzufügen.
- Citrix empfiehlt, dass Sie alle VDAs auf die neueste Version aktualisieren und dann nach Bedarf **Funktionsebene ändern** für Maschinenkataloge und Bereitstellungsgruppen ausführen. Wenn Sie beim Erstellen einer Bereitstellungsgruppe Maschinen mit verschiedenen VDA-Versionen auswählen, ist die resultierende Bereitstellungsgruppe kompatibel mit der ältesten VDA-Version. Wenn auf einer der ausgewählten Maschinen beispielsweise ein VDA der Version 7.1 und auf den anderen eine spätere Version installiert ist, können alle Maschinen der Gruppe nur die Features verwenden, die vom VDA der Version 7.1 unterstützt werden. Das bedeutet, dass einige Features, die spätere VDA-Versionen erfordern, in der Bereitstellungsgruppe möglicherweise nicht zur Verfügung stehen.
- Die folgenden Kompatibilitätsprüfungen werden durchgeführt:
  - MinimumFunctionalLevel muss kompatibel sein
  - SessionSupport muss kompatibel sein
  - AllocationType muss für SingleSession kompatibel sein
  - ProvisioningType muss kompatibel sein
  - PersistChanges muss für MCS und Citrix Provisioning kompatibel sein
  - Der RemotePC-Katalog ist nur mit dem RemotePC-Katalog kompatibel
  - AppDisk-bezogene Überprüfung

### Schritt 2: Load Balancing (Preview)

Gehen Sie wie folgt vor, um die Lastausgleich-Einstellungen beim Erstellen einer Bereitstellungsgruppe zu konfigurieren:

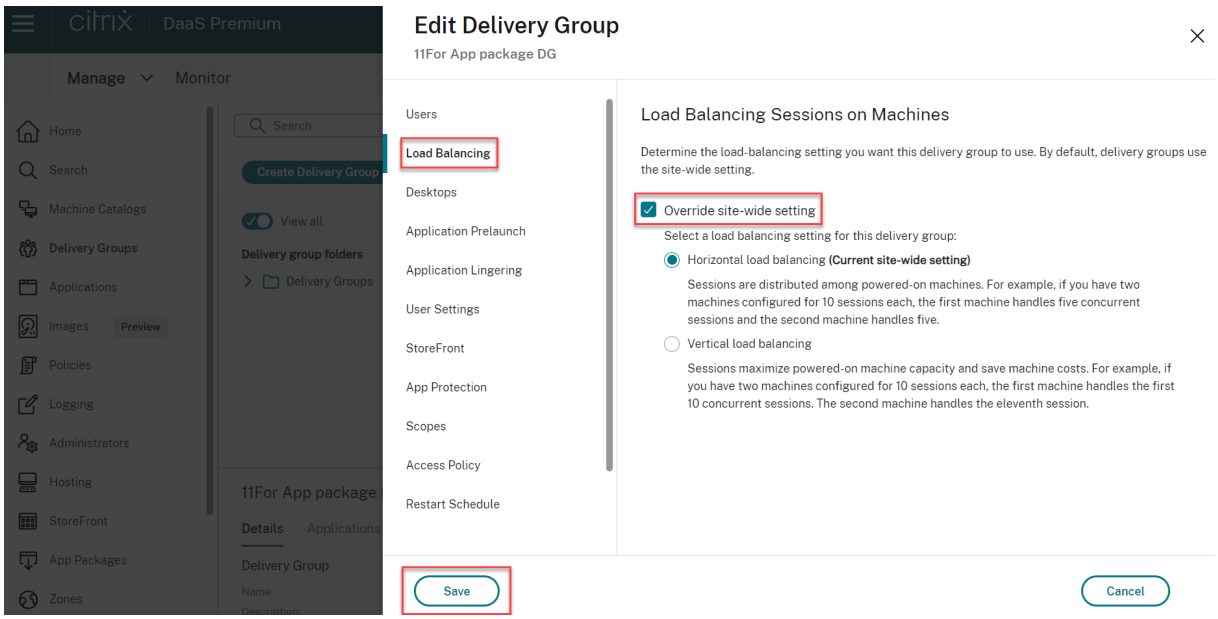
1. Melden Sie sich bei DaaS Premium an.
2. Klicken Sie in der linken Navigationsleiste auf **Bereitstellungsgruppen**.
3. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Bereitstellungsgruppe erstellen**.
4. Klicken Sie im **Assistenten zum Erstellen einer Bereitstellungsgruppe** auf **Weiter**. Der Assistent **Maschinen** wird geöffnet.
5. Wählen Sie im Assistenten **Maschinen** einen erforderlichen Maschinenkatalog und klicken Sie auf **Weiter**. Der Assistent **Lastausgleich** wird geöffnet.
6. Aktivieren Sie im Assistenten **Lastausgleich** das Kontrollkästchen zum **Überschreiben der siteweiten Einstellung**.
7. Wählen Sie je nach Bedarf **Horizontaler Lastenausgleich** oder **Vertikaler Lastenausgleich** und klicken Sie auf **Weiter**.




Gehen Sie wie folgt vor, um die Lastausgleich-Einstellungen beim Bearbeiten einer Bereitstellungsgruppe zu konfigurieren:

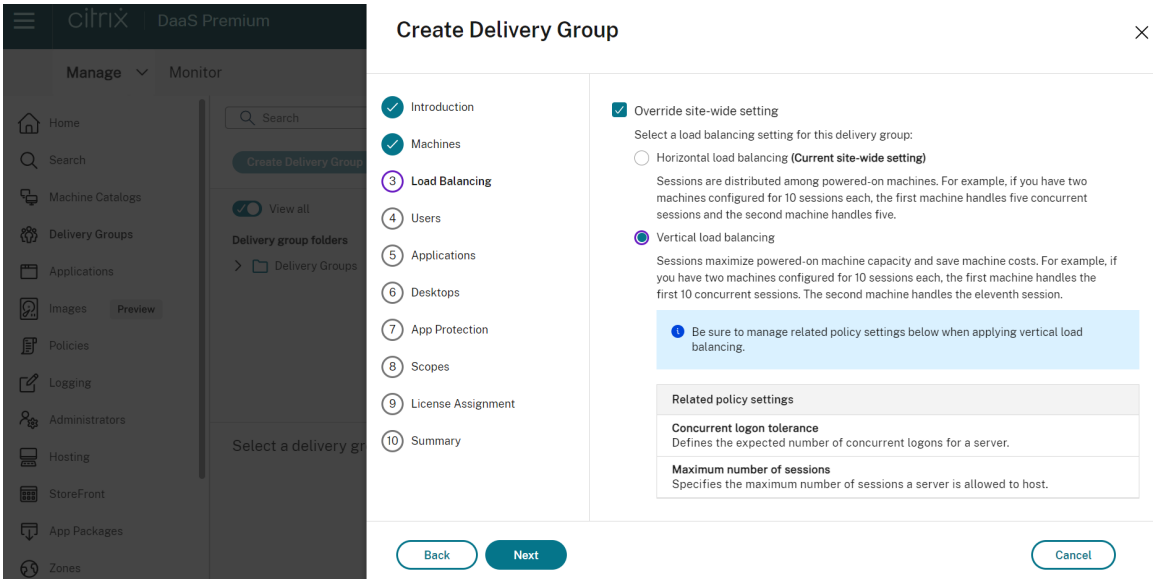
1. Melden Sie sich bei DaaS Premium an.
2. Klicken Sie in der linken Navigationsleiste auf **Bereitstellungsgruppen**.
3. Wählen Sie eine **Bereitstellungsgruppe** aus der Liste aus und klicken Sie auf **Bearbeiten**. Der Assistent zum **Bearbeiten von Bereitstellungsgruppen** wird geöffnet.
4. Klicken Sie auf der Seite **Bereitstellungsgruppe bearbeiten** auf **Lastausgleich**.
5. Aktivieren Sie das Kontrollkästchen zum **Überschreiben der siteweiten Einstellung**.
6. Wählen Sie je nach Bedarf **Horizontaler Lastenausgleich** oder **Vertikaler Lastenausgleich** und klicken Sie auf **Speichern**.




**Hinweis:**

Bei Auswahl des vertikalen Lastenausgleichs achten Sie darauf, dass die Richtlinien für den **Toleranzwert für gleichzeitige Anmeldungen** und die **Sitzungshöchstanzahl** entsprechend konfiguriert sind.




Weitere Informationen zum Lastausgleich auf Site- und Bereitstellungsgruppenebene finden Sie unter Lastausgleich bei Maschinen.

### Schritt 3: Bereitstellungstyp

Diese Seite wird nur angezeigt, wenn Sie einen Maschinenkatalog mit statischen (zugewiesen) Einzelsitzungs-OS-Maschinen auswählen. Wählen Sie entweder **Anwendungen** oder **Desktops**. Sie können nicht beide aktivieren.

Wenn Sie Maschinen aus einem Katalog mit Multisitzungs-OS-Maschinen oder einem Katalog mit nach dem Zufallsprinzip zugewiesenen (gepoolten) Einzelsitzungs-OS-Maschinen ausgewählt haben, wird als Bereitstellungstyp "Anwendungen und Desktops"angenommen. Sie können Anwendungen, Desktops oder beides bereitstellen.

### Schritt 4: AppDisks

Ignorieren Sie diese Seite. Wählen Sie **Weiter**.

### Schritt 5: Benutzer

Geben Sie die Benutzer und Benutzergruppen an, die die Anwendungen und/oder Desktops in der Bereitstellungsgruppe verwenden können.

#### Festlegung von Benutzerlisten

Benutzerlisten werden angegeben, wenn Sie Folgendes erstellen oder bearbeiten:

- Benutzerzugriffsliste für eine Bereitstellung, die nicht über diese Konsole konfiguriert wird. In der Standardeinstellung gilt die Anwendungsanspruch-Richtlinienregel für alle Benutzer. Weitere Informationen finden Sie in den `BrokerAppEntitlementPolicyRule`-Cmdlets des PowerShell-SDKs.
- Bereitstellungsgruppen.
- Anwendungen.

> **Hinweis:**
>
> Wenn Sie eine Benutzerliste angeben, können Sie Benutzerkonten von einem der folgenden Identitätsanbieter auswählen, mit denen Ihr Citrix Cloud-Konto verbunden ist: Active Directory, Azure Active Directory (Microsoft Entra ID) oder Okta.

Die Liste der Benutzer, die Zugriff auf eine Anwendung haben, wird aus der Schnittmenge der oben angegebenen Benutzerlisten erstellt.

**Authentifizierte und nicht authentifizierte Benutzer**

Es gibt zwei Benutzertypen: authentifizierte und nicht authentifizierte Benutzer (nicht authentifizierte Benutzer werden auch als "anonyme"Benutzer bezeichnet). Konfigurieren einen oder beide Typen in einer Bereitstellungsgruppe konfigurieren.

- **Authentifiziert:** Die Benutzer und Gruppenmitglieder, die Sie namentlich festlegen, müssen für den Zugriff auf Anwendungen und Desktops in StoreFront oder der Citrix Workspace-App Anmeldeinformationen, z. B. Smartcard oder Benutzernamen und Kennwort, angeben. (Bei Bereitstellungsgruppen mit Einzelsitzungs-OS-Maschinen können Sie eine Liste der Benutzer später unter Bearbeiten der Bereitstellungsgruppe importieren.)
- **Nicht authentifiziert (anonym):** Bei Bereitstellungsgruppen mit Maschinen mit Multisitzungs-OS können Sie Benutzern Zugriff auf Anwendungen und Desktops gewähren, ohne dass die Benutzer Anmeldeinformationen in StoreFront oder der Citrix Workspace-App eingeben müssen. Beispiel: Beim Zugriff über einen Kiosk werden für die Anwendung Anmeldeinformationen benötigt, nicht aber für das Citrix Zugriffsportal und Citrix Tools. Eine Gruppe anonymer Benutzer wird erstellt, wenn Sie den ersten Delivery Controller installieren.

  Damit nicht authentifizierten Benutzern Zugriff erteilt werden kann, muss auf jeder Maschine in der Bereitstellungsgruppe ein Multisitzungs-OS-VDA installiert sein. Wenn nicht authentifizierte Benutzer aktiviert sind, müssen Sie einen StoreFront-Store ohne Authentifizierung haben.

  Nicht authentifizierte Benutzerkonten werden bei Bedarf beim Start einer Sitzung erstellt und "AnonXYZ"genannt (XYZ ist eineindeutiger dreistelliger Wert).

  Für Benutzersitzungen ohne Authentifizierung gilt ein Standardleerlauftimeout von 10 Minuten. Beim Trennen der Verbindung mit dem Client erfolgt automatisch die Abmeldung. Wiederverbindung, Roaming zwischen Clients und Workspace Control werden nicht unterstützt.

In der folgenden Tabelle werden die Optionen der Seite **Benutzer** erläutert:

| Zugriff aktivieren für | Benutzer und Benutzergruppen hinzufügen/zuweisen? | Kontrollkästchen "Nicht authentifizierte Benutzer zulassen"aktivieren? |
|---|---|---|
| Nur authentifizierte Benutzer | Ja | Nein |
| Nur nicht authentifizierte Benutzer | Nein | Ja |
| Sowohl authentifizierte als auch nicht authentifizierte Benutzer | Ja | Ja |

**Benutzer- oder Gruppenzugriff einschränken**

Sie können die Verwendung einer Bereitstellungsgruppe auch einschränken, indem Sie Benutzer oder Benutzergruppen zur **Positivliste** hinzufügen. Nur Benutzer auf der **Positivliste** können auf Apps und Desktops in der Bereitstellungsgruppe zugreifen. Sie können auch Benutzer und Benutzergruppen einer Sperrliste hinzufügen, indem Sie auf **Sperrliste hinzufügen** klicken. Dadurch wird verhindert, dass Benutzer Apps und Desktops in der ausgewählten Bereitstellungsgruppe verwenden. Eine Sperrliste ist nur zum Blockieren von Benutzern auf der Positivliste sinnvoll.

## Schritt 6: Anwendungen

Nützliche Info:

- Sie können Anwendungspakete zu *statischen Einzelsitzungs-* und *Remote-PC-Zugriff*-Bereitstellungsgruppen hinzufügen. Die Pakete, die diese Anwendungen enthalten, werden jedes Mal automatisch bereitgestellt, wenn sich Benutzer an ihren Desktops oder Remote-PCs anmelden.
- Standardmäßig werden neu hinzugefügte Anwendungen im Ordner "Anwendungen"abgelegt. Sie können einen anderen Ordner angeben. Weitere Informationen finden Sie im Artikel Anwendungen.
- Sie können die Eigenschaften von Anwendung beim Hinzufügen zu einer Bereitstellungsgruppe oder später ändern. Weitere Informationen finden Sie im Artikel Anwendungen.
- Wenn Sie eine Anwendung hinzufügen und es dort bereits eine Anwendung mit dem gleichen Namen gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie dies ablehnen, wird die Anwendung mit einem Suffix hinzugefügt, sodass ihr Name innerhalb des Ordners eindeutig ist.
- Wenn Sie eine Anwendung mehreren Bereitstellungsgruppen hinzufügen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Bereitstellungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Bereitstellungsgruppen, denen die Anwendung hinzugefügt wurde.
- Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie die Eigenschaft "Anwendungsname"(Benutzer). Andernfalls wird den Benutzern der Name in der Citrix Workspace-App doppelt angezeigt.

Wählen Sie das Menü **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

- **Startmenü:** Anwendungen, die auf Maschinen erkannt werden, die von dem Image im ausgewählten Katalog erstellt wurden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Wählen Sie die Anwendungen, die Sie hinzufügen möchten, und wählen Sie **OK**.

- **Manuell:** Anwendungen in der Bereitstellung oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Nach Eingabe dieser Informationen wählen Sie **OK**.
- **Vorhandene:** Anwendungen, die der Bereitstellung bereits hinzugefügt wurden, ggf. in einer anderen Bereitstellungsgruppe. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Wählen Sie die Anwendungen, die Sie hinzufügen möchten, und wählen Sie **OK**.
- **Anwendungspakete:** Anwendungen in App-V-, MSIX-, MSIX App Attach- oder FlexApp-Anwendungspaketen. Wenn Sie diese Quelle auswählen, wird die Seite **Anwendungen aus Paketen hinzufügen** geöffnet. Wählen Sie eine Anwendungspaketquelle und in der daraufhin angezeigten Anzeige die Anwendungen aus, die Sie hinzufügen möchten. Klicken Sie dann auf **OK**

  > **Hinweis:**
  >
  > Um MSIX- oder MSIX-Apps mit App-Anhängen zu veröffentlichen, muss die Funktionsebene der Bereitstellungsgruppe 2106 oder höher sein. Für FlexApp-Apps muss die Funktionsebene 2206 oder höher sein. Wenn eine Anforderung auf Funktionsebene nicht erfüllt ist, sind die entsprechenden Optionen in der Dropdownliste **Quelle des Anwendungspakets** abgeblendet.

- **Anwendungsgruppe:** Anwendungsgruppen, die in der Bereitstellung vorhanden sind.

Ist eine Anwendungsquelle oder Anwendung nicht verfügbar oder ungültig, wird sie nicht angezeigt oder kann nicht ausgewählt werden. Beispiel: Die Quelle **Vorhandene** ist nicht verfügbar, wenn der Bereitstellung keine Anwendungen hinzugefügt wurden. Es kann auch sein, dass eine Anwendung nicht mit den auf Maschinen im ausgewählten Maschinenkatalog unterstützten Sitzungstypen kompatibel ist.

### Schritt 7: App Protection

Die folgenden Informationen ergänzen den Artikel zum App-Schutz in der Dokumentation zu Citrix Virtual Apps and Desktops. Um den App-Schutz in einer Citrix DaaS-Bereitstellung zu verwenden, folgen Sie den allgemeinen Anweisungen in diesem Artikel und beachten Sie dabei die folgenden Details.

- Sie müssen ein gültiges Citrix Cloud-Abonnement und Anspruch auf App-Schutz haben. Um das App-Schutz-Feature zu erwerben, können Sie sich an Ihren Citrix Vertriebsmitarbeiter wenden.
- App Protection erfordert XML-Vertrauen. Um XML-Vertrauen zu aktivieren, gehen Sie zu **Einstellungen > XML-Vertrauen aktivieren**.

- Screenshotschutz:
  - Unter Windows und macOS ist nur das Fenster mit dem geschützten Inhalt leer. Das Feature ist aktiv, wenn ein geschütztes Fenster nicht minimiert ist.
  - Unter Linux ist der gesamte Screenshot leer. Der App-Schutz ist aktiv, unabhängig davon, ob ein geschütztes Fenster minimiert ist.

### Schritt 8: Desktops (oder Desktopzuweisungsregeln)

Der Titel dieser Seite hängt davon ab, welchen Maschinenkatalog Sie zuvor im Assistenten ausgewählt haben:

- Wenn Sie einen Maschinenkatalog mit gepoolten Maschinen gewählt haben, lautet der Titel **Desktops**.
- Wenn Sie einen Katalog mit zugewiesenen Maschinen gewählt und auf der Seite **Bereitstellungstyp** "Desktops"gewählt haben, ist der Titel **Desktopzuweisungsregeln**.
- Wenn Sie einen Katalog mit zugewiesenen Maschinen gewählt und auf der Seite **Bereitstellungstyp** "Anwendungen"gewählt haben, ist der Titel **Anwendungen**.

Wählen Sie **Hinzufügen** aus. Führen Sie folgende Aktionen im Dialogfeld aus:

- Geben Sie in den Feldern **Anzeigename** und **Beschreibung** die Informationen ein, die in der Citrix Workspace-App angezeigt werden sollen.
- Zum Hinzufügen einer Tagbeschränkung zu einem Desktop wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag im Menü aus.
- Über die Optionsfelder stehen folgende Optionen zur Verfügung:
  - **Alle Benutzer mit Zugriff auf diese Bereitstellungsgruppe dürfen einen Desktop verwenden.** Alle Benutzer in der Bereitstellungsgruppe können einen Desktop starten (bei Gruppen mit gepoolten Maschinen) bzw. ihnen kann eine Maschine zugewiesen werden, wenn sie den Desktop starten (bei Gruppen mit zugewiesenen Maschinen).
  - **Desktopverwendung beschränken:** Zum Einschränken der Desktopverwendung durch Hinzufügen von Benutzern und Benutzergruppen zur **Positivliste**. Nur Benutzer auf der **Positivliste** können auf einen Desktop zugreifen. Sie können auch Benutzer und Benutzergruppen einer Sperrliste hinzufügen, indem Sie auf **Sperrliste hinzufügen** klicken. Dadurch wird verhindert, dass Benutzer Desktops in der ausgewählten Bereitstellungsgruppe verwenden. Eine Sperrliste ist nur zum Blockieren von Benutzern auf der Positivliste sinnvoll.
- Wenn die Gruppe zugewiesene Maschinen enthält, geben Sie die maximale Anzahl Desktops pro Benutzer an. Sie müssen eins oder einen höheren Wert eingeben.

- Aktivieren oder deaktivieren Sie den Desktop (bei gepoolten Maschinen) bzw. die Desktopzuordnungsregel (bei zugewiesenen Maschinen). Durch Deaktivieren eines Desktops wird dieser nicht mehr bereitgestellt. Durch Deaktivieren einer Desktopzuordnungsregel wird die automatische Desktopzuweisung beendet.
- Wenn Sie fertig sind, wählen Sie **OK**.

### Schritt 9: Lizenzzuweisung

Entscheiden Sie, welche Lizenz die Bereitstellungsgruppe verwenden soll. Standardmäßig wird für die Bereitstellungsgruppe die Sitelizenz verwendet. Weitere Informationen finden Sie unter Multitypplizenzierung.

### Schritt 10: Einstellung für den lokalen Hostcache

Diese Einstellung ist nur für Bereitstellungsgruppen sichtbar, die energieverwaltete Einzelsitzungspolmaschinen enthalten.

Standardmäßig sind diese Computer im Local Host Cache-(LHC)-Modus aufgrund von Datenrisiken nicht verfügbar. Um das Standardverhalten zu ändern und sie im LHC-Modus für neue Benutzerverbindungen verfügbar zu machen, wählen Sie **Ressourcen verfügbar lassen** aus.

Alternativ können Sie das Standardverhalten mithilfe von PowerShell-Befehlen ändern. Weitere Informationen finden Sie unter Unterstützung für Anwendungen und Desktops.

> **Wichtig:**
>
> Die Aktivierung des Zugriffs auf gepoolte Einzelsitzungsmaschinen mit Energieverwaltung kann dazu führen, dass Daten und Änderungen aus früheren Benutzersitzungen in nachfolgenden Sitzungen wiedergegeben werden.

### Schritt 11: Zusammenfassung

Geben Sie einen Namen für die Bereitstellungsgruppe ein. Sie können optional eine Beschreibung eingeben, die in der Workspace-App und in der Verwaltungsoberfläche “Vollständige Konfiguration” angezeigt wird.

Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig stellen**. Wenn Sie keine Anwendungen gewählt bzw. keinen Desktop zur Bereitstellung angeben haben, werden Sie gefragt, ob Sie fortfahren möchten.

### Weitere Informationen

- Bereitstellungsgruppen verwalten
- Anwendungen

## Bereitstellungsgruppen verwalten

June 12, 2024

### Einführung

In diesem Artikel werden Verfahren zum Verwalten von Bereitstellungsgruppen über die Verwaltungskonsole beschrieben. Sie können die Einstellungen ändern, die Sie beim Erstellen der Gruppe gewählt haben, und Sie können weitere Einstellungen konfigurieren, die beim Erstellen von Bereitstellungsgruppen nicht zur Verfügung stehen.

Die Verfahren sind nach Kategorien geordnet: Allgemeines, Benutzer, Maschinen und Sitzungen. Einige Aufgaben fallen in mehrere Kategorien. Das Thema "Unterbinden der Benutzerverbindung mit Maschinen"wird beispielsweise in der Kategorie "Maschinen"beschrieben, es betrifft aber auch Benutzer. Wenn Sie eine Aufgabe unter einer Kategorie nicht finden, schauen Sie daher unter einer verwandten Kategorie nach.

Auch andere Artikel enthalten verwandte Informationen:

- Unter Anwendungen finden Sie Informationen zur Verwaltung von Anwendungen in Bereitstellungsgruppen.
- Das Verwalten von Bereitstellungsgruppen erfordert die Berechtigungen des Bereitstellungsgruppen-Administrators. Weitere Informationen finden Sie unter Delegierte Administration.

### Allgemein

- Gruppendetails anzeigen
- Bereitstellungsmethode ändern
- StoreFront-Adressen ändern
- Funktionsebene ändern
- Remote-PC-Zugriff-Bereitstellungsgruppen verwalten
- Lizenz für eine Bereitstellungsgruppe ändern
- Bereitstellungsgruppen mit Ordnern organisieren
- App-Schutz verwalten

### Gruppendetails anzeigen

1. Verwenden Sie die Suchfunktion, um eine bestimmte Bereitstellungsgruppe zu finden. Anweisungen finden Sie unter Nach Instanzen suchen.
2. Wählen Sie aus den Suchergebnissen nach Bedarf eine Gruppe aus.
3. In der folgenden Tabelle finden Sie Beschreibungen der Gruppenspalten.
4. Klicken Sie im unteren Detailbereich auf eine Registerkarte, um weitere Informationen zu dieser Gruppe zu erhalten.

| Spalte | Beschreibung |
|---|---|
| Bereitstellungsgruppe | Der Gruppenname und der Sitzungstyp. Zu den Sitzungstypen gehören Einzelsitzungs-OS und Multisitzungs-OS. |
| Bereitstellen | Der Typ der Ressourcen, die von dieser Gruppe bereitgestellt werden. Zu den möglichen Werten gehören Anwendungen, Desktops sowie Anwendungen und Desktops. “Statische Maschinenzuweisung”wird angezeigt, wenn die Bereitstellungsgruppe aus dedizierten Maschinen besteht. |
| Sitzung wird verwendet | Die Anzahl der eingerichteten Maschinen und die Anzahl der Maschinen, die sich im Zustand “Getrennt”befinden. |
| Zugewiesene Anzahl | Die Anzahl der Maschinen im Katalog, die einer Bereitstellungsgruppe zugewiesen sind. |
| Ordner | Die Position der Gruppe in der **Bereitstellungsgruppenstruktur**. Hier wird der Name des Ordners angezeigt, in dem sich die Gruppe befindet (einschließlich des abschließenden umgekehrten Schrägstrichs), oder −, wenn sich die Gruppe auf der Stammebene befindet. |

### Ändern des Bereitstellungstyps von Bereitstellungsgruppen

Der Bereitstellungstyp bestimmt, was eine Gruppe bereitstellen kann: Anwendungen, Desktops oder beides.

Bevor Sie den Typ von **Anwendungen** in **Desktops** ändern, löschen Sie alle Anwendungen aus der

Gruppe.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie auf der Seite **Bereitstellungstyp** den gewünschten Bereitstellungstyp.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

#### StoreFront-Adressen ändern

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Geben Sie auf der Seite **StoreFront** an, ob Sie eine StoreFront-Serveradresse später angeben möchten (**Manuell**), oder wählen Sie **Neu hinzufügen** aus, um die StoreFront-Server anzugeben, die Sie verwenden möchten (**Automatisch**).
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Sie können die StoreFront-Serveradresse auch durch Auswahl von **StoreFront** im linken Bereich der Konsole festlegen.

#### Funktionsebene ändern

Nach dem Upgrade der VDAs auf Maschinen einer Bereitstellungsgruppe sowie auf den Maschinen in den von ihr verwendeten Maschinenkatalogen ändern Sie die Funktionsebene für die Bereitstellungsgruppe.

Vorbereitungen:

- Wenn Sie Citrix Provisioning (zuvor "Provisioning Services") verwenden, aktualisieren Sie die VDA-Version in der Citrix Provisioning Console.
- Starten Sie die Maschinen mit dem aktualisierten VDA, damit sie sich bei Citrix DaaS registrieren können. Dadurch wird in der Konsole erkannt, welche Elemente in der Bereitstellungsgruppe zu ändern sind.
- Wenn Sie ältere VDA-Versionen weiterverwenden müssen, sind neuere Produktfeatures ggf. nicht verfügbar. Weitere Informationen finden Sie in der Upgrade-Dokumentation.

Führen Sie folgende Schritte aus, um die Funktionsebene für eine Bereitstellungsgruppe zu ändern:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann in der Aktionsleiste **Funktionsebene ändern**. Die Aktion **Funktionsebene ändern** wird nur angezeigt, wenn aktualisierte VDAs erkannt werden.

In der Anzeige sehen Sie, für welche Maschinen die Funktionsebene ggf. nicht geändert werden kann, und warum dies nicht möglich ist. Sie können die Änderung dann abbrechen, das Problem auf der Maschine beheben und die Änderung erneut ausführen.

Nach Abschluss der Änderung können Sie die Maschinen in ihren vorherigen Zustand zurückversetzen. Wählen Sie die Bereitstellungsgruppe und dann in der Aktionsleiste **Änderung der Funktionsebene rückgängig machen**.

#### Remote-PC-Zugriff-Bereitstellungsgruppen verwalten

Wenn eine Maschine eines Remote-PC-Zugriff-Maschinenkatalogs keinem Benutzer zugewiesen wurde, wird sie vorübergehend einer Bereitstellungsgruppe zugewiesen, die dem Maschinenkatalog zugeordnet ist. Dadurch kann sie später einem Benutzer zugewiesen werden.

Die Zuweisung der Bereitstellungsgruppe zum Maschinenkatalog ist mit einem Prioritätswert verbunden. Die Priorität bestimmt, welcher Bereitstellungsgruppe eine Maschine zugewiesen ist, die bei der Registrierung beim System oder wenn ein Benutzer eine Maschinenzuweisung benötigt: je geringer der Wert, desto höher die Priorität. Wenn ein Remote-PC-Zugriff-Maschinenkatalog mehrere Bereitstellungsgruppenzuweisungen hat, wird die mit der höchsten Priorität vom System ausgewählt. Die Priorität legen Sie mit dem PowerShell-SDK fest.

Beim Erstellen eines Remote-PC-Zugriff-Maschinenkatalogs wird dieser einer Bereitstellungsgruppe zugeordnet. Diese Zuweisung bedeutet, dass dem Maschinenkatalog später hinzugefügte Maschinenkonten oder Organisationseinheiten in der Bereitstellungsgruppe hinzugefügt werden können. Die Zuordnung kann deaktiviert oder aktiviert werden.

Hinzufügen oder Entfernen der Zuordnung eines Remote-PC-Zugriff-Maschinenkatalogs zu einer Bereitstellungsgruppe

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Remote-PC-Zugriff-Gruppe aus.
3. Wählen Sie im Abschnitt **Details** die Registerkarte **Maschinenkataloge** und dann einen Katalog mit Remote-PC-Zugriff.
4. Um eine Zuordnung hinzuzufügen oder wiederherzustellen, wählen Sie **Desktops hinzufügen**. Zum Entfernen einer Zuordnung wählen Sie **Zuordnung entfernen**.

### Lizenz für eine Bereitstellungsgruppe ändern

Gehen Sie folgendermaßen vor, um die Lizenzberechtigung für eine Bereitstellungsgruppe zu ändern:

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Lizenzzuweisung** die Lizenz für die Gruppe aus.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Weitere Informationen zu Berechtigungen auf Bereitstellungsgruppenebene finden Sie unter Multitylizenzierung.

### Bereitstellungsgruppen mit Ordnern organisieren

Sie können Ordner erstellen, um den Zugriff auf Bereitstellungsgruppen zu vereinfachen.

**Erforderliche Rollen** Standardmäßig benötigen Sie zum Erstellen und Verwalten von Bereitstellungsgruppenordnern die folgende integrierte Rolle: Cloudadministrator, Volladministrator oder Bereitstellungsgruppenadministrator. Bei Bedarf können Sie Rollen für das Erstellen und Verwalten von Bereitstellungsgruppenordnern anpassen. Weitere Informationen finden Sie unter Erforderliche Berechtigungen.

**Bereitstellungsgruppenordner erstellen** Planen Sie zunächst, wie Sie Ihre Bereitstellungsgruppen organisieren wollen. Beachten Sie Folgendes:

- Sie können Ordner bis zu fünf Ebenen tief verschachteln (mit Ausnahme des Standardstammordners).
- Ein Ordner kann Bereitstellungsgruppen und Unterordner enthalten.
- Alle Knoten in der **Vollständigen Konfiguration** (wie die Knoten **Maschinenkataloge**, **Anwendungen** und **Bereitstellungsgruppen**) teilen sich eine Ordnerstruktur im Back-End. Um Namenskonflikte mit anderen Knoten beim Umbenennen oder Verschieben von Ordnern zu vermeiden, empfehlen wir, Ordnern der ersten Ebene in verschiedenen Knoten unterschiedliche Namen zu geben.

Gehen Sie wie folgt vor, um einen Bereitstellungsgruppenordner zu erstellen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und klicken Sie dann in der **Aktionsleiste** auf **Ordner erstellen**.
3. Geben Sie einen Namen für den neuen Ordner ein und klicken Sie dann auf **Fertig**.

> **Tipp:**
>
> Wenn Sie einen Ordner an einem falschen Speicherort erstellen, können Sie ihn an den korrekten Speicherort ziehen.

#### Bereitstellungsgruppe verschieben

Sie können eine Bereitstellungsgruppe zwischen Ordnern verschieben. Verfahren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Zeigen Sie Gruppen nach Ordner sortiert an. Sie können auch die Option **Alle anzeigen** über der Ordnerhierarchie aktivieren, um alle Bereitstellungsgruppen gleichzeitig anzuzeigen.
3. Klicken Sie mit der rechten Maustaste auf eine Gruppe und wählen Sie **Bereitstellungsgruppe verschieben**.
4. Wählen Sie den Ordner aus, in den Sie die Gruppe verschieben möchten, und klicken Sie auf **Fertig**.

> **Tipp:**
>
> Sie können eine Gruppe in einen Ordner ziehen.

#### Bereitstellungsgruppenordner verwalten

Sie können Bereitstellungsgruppenordner löschen, umbenennen und verschieben.

Beachten Sie, dass Sie einen Ordner nur dann löschen können, wenn er und seine Unterordner keine Bereitstellungsgruppen enthalten.

Gehen Sie wie folgt vor, um einen Ordner zu verwalten:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und wählen Sie dann eine gewünschte Aktion in der **Aktionsleiste** aus:

- Wählen Sie zum Umbenennen des Ordners **Ordner umbenennen** aus.
- Wählen Sie zum Löschen des Ordners **Ordner löschen** aus.
- Wählen Sie zum Verschieben des Ordners **Ordner verschieben** aus.

3. Folgen Sie den Anweisungen auf dem Bildschirm, um die restlichen Schritte auszuführen.

**Erforderliche Berechtigungen** In der folgenden Tabelle sind die Berechtigungen aufgeführt, die zum Ausführen von Aktionen für Bereitstellungsgruppenordner erforderlich sind.

| Aktion | Erforderliche Berechtigungen |
|---|---|
| Bereitstellungsgruppenordner erstellen | Bereitstellungsgruppenordner erstellen |
| Bereitstellungsgruppenordner löschen | Bereitstellungsgruppenordner entfernen |
| Bereitstellungsgruppenordner verschieben | Bereitstellungsgruppenordner verschieben |
| Bereitstellungsgruppenordner umbenennen | Bereitstellungsgruppenordner bearbeiten |
| Bereitstellungsgruppen in Ordner verschieben | Bereitstellungsgruppenordner und Bereitstellungsgruppeneigenschaften bearbeiten |

#### App-Schutz verwalten

Die folgenden Informationen ergänzen den Artikel zum App-Schutz in der Dokumentation zu Citrix Virtual Apps and Desktops. Um den App-Schutz in einer Citrix DaaS-Bereitstellung zu verwenden, folgen Sie den allgemeinen Anweisungen in diesem Artikel und beachten Sie dabei die folgenden Details.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Auf der Seite **App Protection** können Sie **Keyloggingschutz** und **Screenshotschutz**aktivieren.

- Sie müssen ein gültiges Citrix Cloud-Abonnement und Anspruch auf App-Schutz haben. Um das App-Schutz-Feature zu erwerben, können Sie sich an Ihren Citrix Vertriebsmitarbeiter wenden.
- App Protection erfordert XML-Vertrauen. Um XML-Vertrauen zu aktivieren, gehen Sie zu **Einstellungen > XML-Vertrauen aktivieren**.
- Screenshotschutz:
  - Unter Windows und macOS ist nur das Fenster mit dem geschützten Inhalt leer. Das Feature ist aktiv, wenn ein geschütztes Fenster nicht minimiert ist.

- Unter Linux ist der gesamte Screenshot leer. Der App-Schutz ist aktiv, unabhängig davon, ob ein geschütztes Fenster minimiert ist.

## Benutzer

> **Hinweis:**
>
> Die Option **Benutzerverwaltung mit Citrix Cloud** wurde entfernt. Um Benutzerzuweisungen für bestehende Bereitstellungsgruppen zu verwalten, für die **Benutzerverwaltung mit Citrix Cloud** festgelegt ist, haben Sie zwei Optionen: Citrix Cloud-Bibliothek oder Vollständige Konfiguration. Weitere Informationen zu Vollständige Konfiguration finden Sie unter Benutzerzuweisungen für von der Citrix Cloud-Bibliothek verwaltete Bereitstellungsgruppen verwalten.

Dieses Thema behandelt die folgenden Abschnitte:

- Benutzereinstellungen ändern
- Benutzer hinzufügen oder entfernen
- Benutzerzuweisungen für von der Citrix Cloud-Bibliothek verwaltete Bereitstellungsgruppen verwalten

### Benutzereinstellungen für eine Bereitstellungsgruppe ändern

Der Name dieser Seite lautet **Benutzereinstellungen** oder **Grundeinstellungen**.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Ändern Sie auf der Seite **Benutzereinstellungen** die folgenden Optionen nach Bedarf.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

| Einstellung | Beschreibung |
|---|---|
| Beschreibung | Text, der in Citrix Workspace (oder StoreFront) angezeigt wird |
| Bereitstellungsgruppe aktivieren | Zeigt an, ob die Bereitstellungsgruppe aktiviert ist. |

| Einstellung | Beschreibung |
| --- | --- |
| Zeitzone | Die Zeitzone, die für die Maschinen dieser Bereitstellungsgruppe gelten muss. Die Option listet die von der Site unterstützten Zeitzonen auf. **Hinweis:**Durch das Ändern der Zeitzone für eine Bereitstellungsgruppe kann ein Neustart der darin enthaltenen Maschinen ausgelöst werden. Um Probleme zu vermeiden, ändern Sie die Zeitzoneneinstellungen außerhalb der Produktionszeiten. |
| Secure ICA aktivieren | Die gesamte Kommunikation zu und von Maschinen in der Bereitstellungsgruppe wird mit SecureICA, das das ICA-Protokoll verschlüsselt, geschützt. Die Standardebene ist 128-Bit. Die Ebene kann über das SDK geändert werden. Citrix empfiehlt die Verwendung zusätzlicher Verschlüsselungsmethoden, z. B. TLS-Verschlüsselung, wenn Datenübertragungen über öffentliche Netzwerke stattfinden. Bei SecureICA wird die Datenintegrität auch nicht geprüft. |
| Maximale Desktops pro Benutzer | Zulässige Anzahl Desktops pro Benutzer. |

### Hinzufügen und Entfernen von Benutzern zu bzw. aus Bereitstellungsgruppen

Ausführliche Informationen zu Benutzern finden Sie unter Benutzer.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bereitstellungsgruppe bearbeiten**.
3. Gehen Sie auf der Seite **Benutzer** folgendermaßen vor:
   - Zum Hinzufügen von Benutzern wählen Sie **Hinzufügen** und geben dann die gewünschten Benutzer an.
   - Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und wählen dann **Entfernen**.

- Aktivieren oder deaktivieren Sie das Kontrollkästchen zur Steuerung des Zugriffs durch nicht authentifizierte Benutzer.

4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

**Benutzerzuweisungen verwalten** Schrittfolge zum Verwalten von Benutzerzuweisungen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Fügen Sie auf der Seite **Maschinenzuteilung** Benutzer hinzu oder entfernen Sie sie. Navigieren Sie zu den Benutzern, die Sie hinzufügen möchten, oder geben Sie eine durch Semikolon getrennte Liste von Benutzernamen ein.

Beachten Sie bei der Eingabe von Benutzernamen Folgendes:

- Wenn sich die Benutzer in Active Directory befinden, geben Sie die Namen direkt ein. Falls nicht, geben Sie die Namen in diesem Format ein: `<identity provider>:<user name>`. Beispiel: `AzureAD:username`.

### Benutzerzuweisungen für von der Citrix Cloud-Bibliothek verwaltete Bereitstellungsgruppen verwalten

Verwenden Sie die Citrix Cloud-Bibliothek oder Vollständige Konfiguration, um Benutzerzuweisungen für von der Citrix Cloud Library verwaltete Bereitstellungsgruppen zu verwalten.

Gehen Sie folgendermaßen vor, um diese Aufgabe mit der vollständigen Konfiguration auszuführen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine von Citrix Cloud verwaltete Bereitstellungsgruppe und dann **Bearbeiten** in der Aktionsleiste aus.
3. Gehen Sie wie folgt vor, um die Verwendung eines Desktops auf bestimmte Benutzer zu beschränken:

   a) Wählen Sie auf der Seite **Desktops** oder **Desktopzuweisungsregeln** den Desktop aus und klicken Sie auf **Bearbeiten**. Die Seite **Desktop bearbeiten** wird mit der ausgewählten Option **Desktopverwendung beschränken** angezeigt.
   b) Klicken Sie auf **Hinzufügen**, wählen Sie je nach Bedarf einen oder mehrere Benutzer aus und klicken Sie dann auf **Fertig**.

c) Klicken Sie auf **OK**.

4. Um die Verwendung von Anwendungen in dieser Gruppe auf bestimmte Benutzer zu beschränken, klicken Sie im linken Bereich auf **Anwendungszuweisungs-Richtlinienregel** und folgen Sie den in Schritt 3 beschriebenen ähnlichen Schritten, um Benutzer hinzuzufügen.

## Maschinen

- Maschinenbenutzerzuweisung ändern
- Lokalen Hostcache für gepoolte Einzelsitzungs-VDAs aktivieren
- Maschine aktualisieren
- Tagbeschränkungen für einen Desktop hinzufügen, ändern oder entfernen
- Maschine entfernen
- Zugriff auf Ressourcen beschränken
- Benutzerverbindung mit Maschinen unterbinden (Wartungsmodus)
- Maschinen herunterfahren und neu starten
- Neustartzeitpläne für Maschinen erstellen und verwalten
- Lastverwaltung bei Maschinen
- Autoscale verwalten

Zusätzlich zu den in diesem Artikel beschriebenen Features finden Sie unter Autoscale Informationen zur proaktiven Energieverwaltung von Maschinen.

### Ändern der Maschinen-Benutzer-Zuweisung in einer Bereitstellungsgruppe

Sie können die Zuweisungen von Maschinen mit Windows-Einzelsitzungs-OS ändern, die mit MCS bereitgestellt wurden. Die Zuweisungen für Maschinen mit Windows-Multisitzungs-OS und mit Citrix Provisioning bereitgestellte Maschinen können Sie nicht ändern.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Geben Sie auf der Seite **Maschinenzuteilung** die neuen Benutzer an.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### Lokalen Hostcache für gepoolte Einzelsitzungs-VDAs aktivieren

Standardmäßig sind gepoolte Maschinen mit Energieverwaltung für Einzelsitzungen nicht verfügbar, wenn sie sich im Modus Lokaler Hostcache befinden. Sie können das Standardverhalten für jede Bere-

itstellungsgruppe außer Kraft setzen. Verfahren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.

   In der Gruppenliste zeigen Gruppen mit gepoolten Einzelsitzungsmaschinen, die von MCS oder Citrix Provisioning bereitgestellt wurden, ein Warnsymbol an.

2. Wählen Sie eine Gruppe und dann in der Aktionsleiste **Bearbeiten** aus.
3. Wählen Sie auf der Seite **Lokaler Hostcache** die Option **Ressourcen verfügbar lassen** aus.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Alternativ können Sie das Standardverhalten mithilfe von PowerShell-Befehlen außer Kraft setzen. Weitere Informationen finden Sie unter Unterstützung für Anwendungen und Desktops.

> **Wichtig:**
>
> Die Aktivierung des Zugriffs auf gepoolte Einzelsitzungsmaschinen mit Energieverwaltung kann dazu führen, dass Daten und Änderungen aus früheren Benutzersitzungen in nachfolgenden Sitzungen wiedergegeben werden.

#### Aktualisieren einer Maschine in einer Bereitstellungsgruppe

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Wählen Sie eine Maschine und dann in der Aktionsleiste **Maschinen aktualisieren**.

Zum Auswählen eines anderen Images wählen Sie **Image** und dann einen Snapshot.

Zum Anwenden der Änderungen und Benachrichtigen der Benutzer der Maschine wählen Sie **Rolloutbenachrichtigung für Endbenutzer**. Geben Sie anschließend Folgendes an:

- Zeitpunkt der Aktualisierung des Images: jetzt oder beim nächsten Neustart
- Neustart-Verteilungszeit (Zeit insgesamt, während derer das Update aller Maschinen beginnen soll)
- Ob Benutzer über den Neustart benachrichtigt werden
- Meldung, die die Benutzer erhalten sollen

### Tagbeschränkungen für einen Desktop hinzufügen, ändern oder entfernen

Das Hinzufügen, Bearbeiten und Entfernen von Tagbeschränkungen kann unerwartete Auswirkungen darauf haben, welche Desktops für den Start in Betracht gezogen werden. Lesen Sie die Informationen und Hinweise unter Tags.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie auf der Seite **Desktops** den Desktop und wählen Sie dann **Bearbeiten**.
4. Zum Hinzufügen einer Tagbeschränkung wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus.
5. Ändern oder Entfernen einer Tagbeschränkung:
   - Wählen Sie ein anderes Tag.
   - Entfernen Sie die Tagbeschränkung durch Deaktivieren von **Starts auf Maschinen mit Tag beschränken**.
6. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### Entfernen von Maschinen aus Bereitstellungsgruppen

Durch Entfernen von Maschinen werden diese aus Bereitstellungsgruppen gelöscht. Sie werden jedoch nicht aus dem Maschinenkatalog der Bereitstellungsgruppe gelöscht. Die Maschine steht daher für Zuweisungen zu anderen Bereitstellungsgruppen zur Verfügung.

Maschinen müssen heruntergefahren werden, bevor sie entfernt werden können. Wenn Sie vorübergehend verhindern möchten, dass Benutzer eine Verbindung mit der Maschine herstellen, während Sie sie löschen, setzen Sie die Maschine in den Wartungsmodus, bevor Sie sie herunterfahren.

Wenn Sie eine Maschine einem anderen Benutzer zuweisen, denken Sie daran, dass Maschinen persönliche Daten enthalten können. Ziehen Sie ggf. ein Reimaging solcher Maschinen in Betracht.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Vergewissern Sie sich, dass die Maschine heruntergefahren ist.
4. Wählen Sie die Maschine aus und wählen Sie in der Aktionsleiste **Aus Bereitstellungsgruppe entfernen**.

Sie können eine Maschine auch über die von der Maschine verwendete Verbindung aus einer Bereitstellungsgruppe entfernen.

### Zugriff auf Ressourcen in einer Bereitstellungsgruppe einschränken

Alle Änderungen zum Einschränken des Zugriffs auf Ressourcen in einer Bereitstellungsgruppe haben Vorrang vor zuvor durchgeführten Einstellungen, unabhängig von der verwendeten Methode. Sie haben folgende Möglichkeiten:

- **Zugriff für Administratoren über Geltungsbereiche für die delegierte Administration einschränken:** Sie können einen Geltungsbereich erstellen und zuweisen, in dem Administratoren auf alle Anwendungen zugreifen können, und einen zweiten Geltungsbereich, der nur den Zugriff auf spezifische Anwendungen zulässt. Weitere Informationen finden Sie unter Delegierte Administration.
- **Zugriff für Benutzer mit Smart Access-Richtlinienausdrücken einschränken:** Sie können Zugriffsrichtlinienregeln konfigurieren, um den Benutzerzugriff auf eine bestimmte Bereitstellungsgruppe zu steuern. Beispiele:
  - Beschränken Sie den Zugriff auf eine Untergruppe von Benutzern und geben Sie zulässige Benutzergeräte an.
  - Beschränken Sie den Zugriff auf Benutzer, die über Workspace (statt StoreFront) verbunden sind.
  - Beschränken Sie den Zugriff auf Benutzer, die über eine bestimmte Workspace-URL verbunden sind.

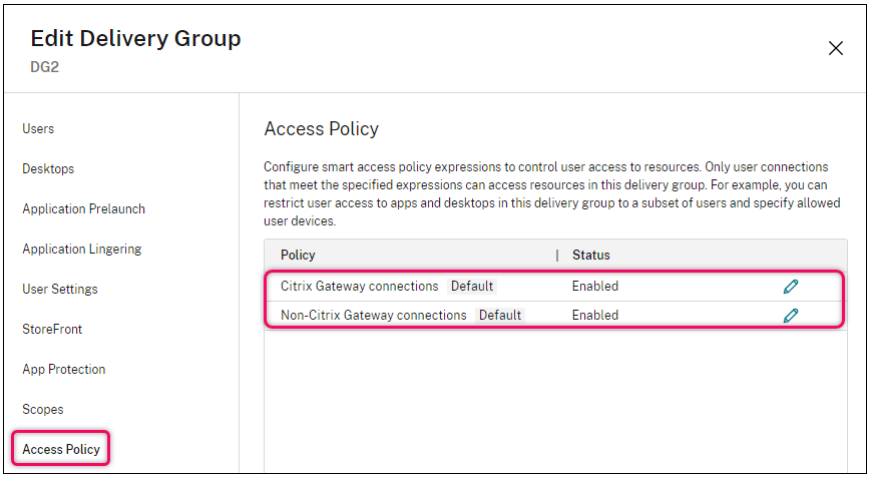
In diesem Abschnitt erfahren Sie, wie Sie den Benutzerzugriff auf Bereitstellungsgruppen mit Zugriffsrichtlinienregeln einschränken können:

- Info über Zugriffsrichtlinienregeln
- Zugriffsrichtlinienregeln hinzufügen
- Zugriffsrichtlinienregeln mit “Vollständige Konfiguration”verwalten
- Richtlinienregeln mit PowerShell hinzufügen und optimieren

**Info über Zugriffsrichtlinienregeln** Sie können mehrere Zugriffsrichtlinienregeln für eine Bereitstellungsgruppe konfigurieren. Apps und Desktops in einer Bereitstellungsgruppe werden in StoreFront oder Workspace eines Benutzers angezeigt, wenn die Verbindung des Benutzers einer Zugriffsrichtlinienregel entspricht, die Sie für die Bereitstellungsgruppe definiert haben, unabhängig von der Reihenfolge.

Jede Regel kann einzeln aktiviert oder deaktiviert werden. Eine deaktivierte Regel wird ignoriert, wenn die Zugriffsrichtlinie ausgewertet wird.




In "Vollständige Konfiguration"enthält die Liste der Zugriffsrichtlinien die folgenden standardmäßigen SmartAccess-Richtlinienregeln. Sie können bei Bedarf weitere hinzufügen.

- **Citrix Gateway-Verbindungen.** Mit dieser Richtlinie können nur Benutzerverbindungen, die über Citrix Gateway hergestellt wurden, auf Ressourcen innerhalb der Bereitstellungsgruppe zugreifen. Benutzerverbindungen, die bei aktiviertem Gerätestatus- oder Netzwerkstandort-Feature über Workspace hergestellt werden, sind ebenfalls als Verbindungen über Citrix Gateway einzustufen.
- **Verbindungen, die nicht über Citrix Gateway hergestellt wurden.** Mit dieser Richtlinie können nur Benutzerverbindungen, die nicht über Citrix Gateway hergestellt wurden, auf Ressourcen innerhalb der Bereitstellungsgruppe zugreifen.

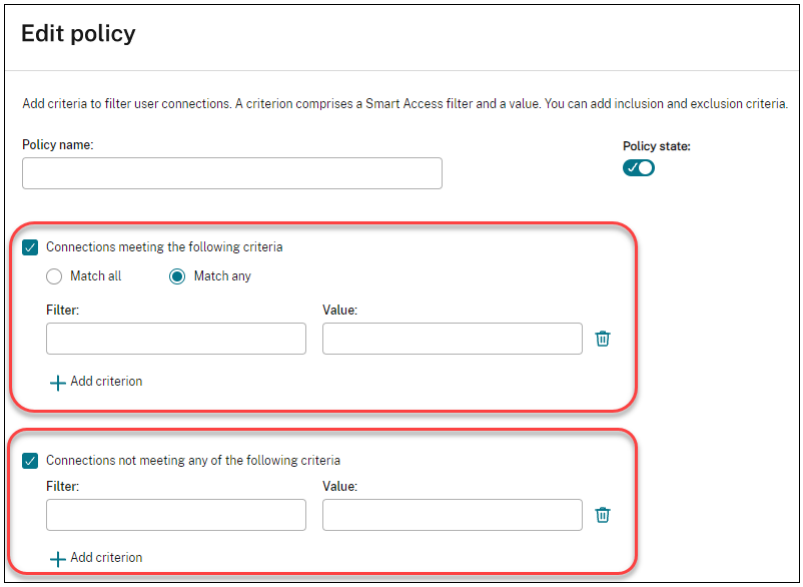
> **Hinweis:**
>
> - Um zu verhindern, dass die Standardregeln eine neu konfigurierte überschreiben, müssen Sie entweder die Standardregeln deaktivieren oder sie optimieren, um die in der neuen Richtlinie verwendeten Filter auszuschließen.
> - Die Standardrichtlinien können nicht gelöscht, aber deaktiviert werden. Um eine Richtlinie zu deaktivieren, klicken Sie auf das Symbol **Bearbeiten** und ändern Sie dann den **Status der Richtlinie** in **Deaktiviert**.
> - Die Richtlinienliste enthält auch Regeln, die mithilfe von PowerShell-Befehlen hinzugefügt wurden. Diese Richtlinien können gelöscht, aber nicht in "Vollständige Konfiguration"bearbeitet werden.

**Zugriffsrichtlinienregeln mit "Vollständige Konfiguration"hinzufügen** Eine Zugriffsrichtlinienregel besteht aus einer Reihe von Filtern. Weitere Informationen zu Filtern finden Sie in diesem Artikel. Beim Hinzufügen einer Zugriffsrichtlinienregel fügen Sie der Regel nach Bedarf mehrere Bedingungsfilter hinzu.

Gehen Sie folgendermaßen vor, um mit "Vollständige Konfiguration"eine Richtlinie für eine Bereitstellungsgruppe hinzuzufügen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Zugriffsrichtlinie** auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.




4. Geben Sie im Feld **Richtlinienname** einen beschreibenden Namen für die Richtlinie ein. Der Name muss in Ihrer Bereitstellung eindeutig sein.
5. Gehen Sie wie folgt vor, um die Kriterien für zulässige Benutzerverbindungen zu definieren:

   a) Wählen Sie **Verbindungen, die eines der folgenden Kriterien erfüllen** aus.

   b) Klicken Sie auf **Kriterium hinzufügen**.

   c) Geben Sie im Feld **Filter** den Namen des Filters ein, den Sie verwenden möchten. Geben Sie im Feld **Wert** einen gewünschten Wert für den Filter ein. Um beispielsweise nur Benutzern, die über Workspace (statt StoreFront) verbunden sind, den Zugriff auf Ressourcen in dieser Bereitstellungsgruppe zu ermöglichen, geben Sie `Citrix-Via-Workspace` für **Filter** und `True` für **Wert** ein.

   d) Um weitere Kriterien hinzuzufügen, wiederholen Sie die Schritte b-c.

   e) Wählen Sie die Beziehung unter den Kriterien aus:

      - **Beliebige Übereinstimmung**. Erlaubt den Zugriff nur, wenn die eingehende Benutzerverbindung eines der konfigurierten Filterkriterien erfüllt.

- **Übereinstimmung mit allen**. Erlaubt den Zugriff nur, wenn die eingehende Benutzerverbindung alle konfigurierten Filterkriterien erfüllt.

6. Gehen Sie wie folgt vor, um die Kriterien für nicht zugelassene Benutzerverbindungen zu definieren:

   a) Wählen Sie **Verbindungen, die keines der folgenden Kriterien erfüllen** aus.

   b) Klicken Sie auf **Kriterium hinzufügen**.

   c) Geben Sie im Feld **Filter** den Namen des Filters ein, den Sie verwenden möchten. Geben Sie im Feld **Wert** einen gewünschten Wert für den Filter ein. Beispielsweise, um Benutzern, die über die Workspace-URL `example.cloud.com` verbunden sind, den Zugriff auf Ressourcen in dieser Bereitstellungsgruppe zu verbieten. Geben Sie `Citrix.Workspace.UsingDomain` für **Filter** und `example.cloud.com` für **Wert** ein.

   d) Um weitere Kriterien hinzuzufügen, wiederholen Sie die Schritte b-c.

   > **Hinweis:**
   >
   > Benutzerverbindungen, die eines der konfigurierten Kriterien erfüllen, sind für Ressourcen in dieser Bereitstellungsgruppe gesperrt.

7. Klicken Sie auf **Fertig**.

   Die neue Richtlinie wird in der Richtlinienliste angezeigt.

8. Überprüfen und optimieren Sie die Standardrichtlinienregeln, um unbeabsichtigte Überschneidungen mit Verbindungen zu vermeiden, die unter diese neue Richtlinie fallen. Verwenden Sie die folgenden Methoden, um die vorhandenen Richtlinien zu verfeinern:

   - Deaktivieren Sie die Standardrichtlinienregeln.
   - Konfigurieren Sie die Standardrichtlinienregeln so, dass die SmartAccess-Filter ausgeschlossen werden, die Sie zu den Einschlusskriterien der neuen Richtlinie hinzugefügt haben. Weitere Informationen finden Sie unter Richtlinienregeln mit “Vollständige Konfiguration”verwalten und Zugriffsrichtlinienregeln mit PowerShell hinzufügen und verwalten.

   > **Wichtig:**
   >
   > Wie unter Info über Zugriffsrichtlinienregeln erklärt, erhält der Benutzer Zugriff auf seine Ressourcen, wenn die Verbindung eines Benutzers einer oder mehreren Richtlinienregeln in einer Bereitstellungsgruppe entspricht. Daher müssen Sie nach dem Erstellen einer Regel die vorhandenen Regeln sorgfältig überprüfen und optimieren, um unbeabsichtigte Überschneidungen mit Verbindungen zu vermeiden, die unter die neue Regel fallen.

**Zugriffsrichtlinienregeln mit "Vollständige Konfiguration"verwalten** Sie können die Einschluss- und Ausschlusskriterien verwenden, um die Standardrichtlinien zu optimieren. Gehen Sie beispielsweise folgendermaßen vor, um den Zugriff auf eine Teilmenge dieser Verbindungen einzuschränken:

1. Bearbeiten Sie eine Standardrichtlinie.
2. Wählen Sie **Verbindungen, die eines der folgenden Kriterien erfüllen** aus.
3. Fügen Sie SmartAccess-Richtlinienausdrücke für zulässige Benutzerzugriffsszenarios hinzu, bzw. bearbeiten oder löschen Sie diese.

Weitere Informationen finden Sie in der Dokumentation zu Citrix Gateway.

**Zugriffsrichtlinienregeln mit PowerShell hinzufügen und verwalten** Sie können die folgenden PowerShell-Cmdlets verwenden, um Zugriffsrichtlinienregeln für Bereitstellungsgruppen hinzuzufügen und zu verwalten:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

Weitere Informationen finden Sie in den entsprechenden Artikeln in der Citrix-Dokumentation für Entwickler.

### Unterbinden der Benutzerverbindung mit Maschinen (Wartungsmodus) in einer Bereitstellungsgruppe

Wenn Sie vorübergehend verhindern möchten, dass neue Verbindungen mit Maschinen hergestellt werden, können Sie den Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe aktivieren. Das ist beispielsweise vor dem Anwenden von Patches oder der Verwendung von Verwaltungstools nützlich.

- Wenn eine Maschine mit Windows-Multisitzungs-OS im Wartungsmodus ist, können Benutzer eine Verbindung mit vorhandenen Sitzungen herstellen, aber keine neuen Sitzungen starten.
- Bei einer Maschine mit Windows-Einzelsitzungs-OS (oder mit Remote-PC-Zugriff) im Wartungsmodus können Benutzer keine Verbindung herstellen. Aktuelle Verbindungen bleiben bis zur Trennung oder Abmeldung erhalten.

Wartungsmodus ein- oder ausschalten:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.

2. Wählen Sie eine Gruppe aus.
3. Zum Aktivieren des Wartungsmodus für alle Maschinen in der Bereitstellungsgruppe wählen Sie in der Aktionsleiste **Wartungsmodus einschalten**.

   Zum Aktivieren des Wartungsmodus für einzelne Maschinen wählen Sie in der Aktionsleiste **Maschinen anzeigen**. Wählen Sie eine Maschine aus und wählen Sie dann in der Aktionsleiste **Wartungsmodus einschalten**.
4. Zum Deaktivieren des Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe folgen Sie den Anweisungen oben, wählen jedoch in der Aktionsleiste die Option **Wartungsmodus ausschalten**.

Einstellungen für Windows-Remotedesktopverbindungen wirken sich auch darauf aus, ob eine Multisitzungs-OS-Maschine im Wartungsmodus ist. Der Wartungsmodus ist in folgenden Fällen aktiviert:

- Der Wartungsmodus wurde wie oben beschrieben aktiviert.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt und für den Anmeldemodus der Remotehostkonfiguration wurde **Neue Verbindungen zulassen, doch neue Anmeldungen verhindern** oder **Neue Verbindungen zulassen, doch Neuanmeldungen bis zum Neustart des Servers verweigern** gewählt.

Sie können den Wartungsmodus auch für Folgendes ein- oder ausschalten:

- Verbindungen, dies wirkt sich auf die Maschinen aus, die die Verbindung verwenden.
- Maschinenkataloge, dies wirkt sich auf die Maschinen in dem betreffenden Katalog aus.

#### Herunterfahren und Neustarten von Maschinen in einer Bereitstellungsgruppe

Dieser Vorgang wird für Remote-PC-Zugriff-Maschinen nicht unterstützt.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Wählen Sie die Maschine aus und wählen Sie dann eine der folgenden Aktionen in der Aktionsleiste aus:

   > **Hinweis:**

> - Die folgenden Aktionen gelten nur für Maschinen mit Energieverwaltung.
> - Einige Optionen sind je nach Maschinenzustand möglicherweise nicht verfügbar.

- **Herunterfahren erzwingen:** Die Maschine wird zwingend abgeschaltet und die Liste der Maschinen wird aktualisiert.
- **Neu starten:** Das Betriebssystem wird heruntergefahren und die Maschine wird neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt die Maschine im aktuellen Zustand.
- **Neustart erzwingen:** Das Betriebssystem wird zwangsweise heruntergefahren und die Maschine dann neu gestartet.
- **Anhalten:** Die Maschine wird ohne Herunterfahren angehalten die Liste der Maschinen wird aktualisiert.
- **Herunterfahren:** Das Betriebssystem wird aufgefordert, herunterzufahren.

Wird bei Aktionen ohne Erzwingen eine Maschine nicht innerhalb von 10 Minuten heruntergefahren, wird sie ausgeschaltet. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

#### Erstellen und Verwalten von Neustartzeitplänen für Maschinen in einer Bereitstellungsgruppe

> **Hinweis:**
>
> - Wenn ein Neustartzeitplan auf eine Bereitstellungsgruppe mit aktiviertem Autoscale angewendet wird, werden die enthaltenen Maschinen ausgeschaltet und von Autoscale neu eingeschaltet.
> - Wenn Neustartzeitpläne auf zufällige Maschinen mit Einzelsitzungs-OS angewendet werden, werden diese Maschinen ausgeschaltet und nicht neu gestartet, um Kosten zu sparen. Wir empfehlen die Verwendung von Autoscale zum Einschalten von Maschinen.
> - Durch das Ändern der Zeitzone für eine Bereitstellungsgruppe kann ein Neustart der darin enthaltenen Maschinen ausgelöst werden. Um Probleme zu vermeiden, ändern Sie die Zeitzoneneinstellungen außerhalb der Produktionszeiten.

Über einen Neustartzeitplan wird der regelmäßige Neustart aller Maschinen in einer Bereitstellungsgruppe festgelegt. Sie können einen oder mehrere Zeitpläne für eine Bereitstellungsgruppe erstellen. Ein Zeitplan kann sich auf Folgendes auswirken:

- Alle Maschinen in der Gruppe
- Eine oder mehrere (aber nicht alle) Maschinen Die Maschinen werden durch ein Tag identifiziert. Es handelt sich hierbei um eine "Tagbeschränkung", da die Aktion auf Elemente (in diesem Fall Maschinen) beschränkt wird, die über das Tag verfügen.

Angenommen, alle Maschinen befinden sich in einer Bereitstellungsgruppe. Sie möchten alle Maschinen mindestens einmal wöchentlich neu starten. Die Maschinen der Buchhaltung sollen täglich neu gestartet werden. Sie richten hierzu einen Zeitplan für alle Maschinen und einen weiteren für die Maschinen der Buchhaltung ein.

Ein Zeitplan enthält Datum und Uhrzeit des Beginns sowie die Dauer des Neustarts. Die Dauer repräsentiert entweder das Neustarten aller betroffenen Maschinen gleichzeitig oder ein Intervall, das voraussichtlich für die Neustarts benötigt wird.

Sie können Zeitpläne aktivieren und deaktivieren. Das Deaktivieren kann beim Testen, während bestimmter Zeiten oder beim Vorbereiten von Zeitplänen hilfreich sein.

Sie können Zeitpläne nicht für das automatisierte Einschalten oder Herunterfahren über die Verwaltungskonsole verwenden, sondern nur für Neustarts.

**Zeitplanüberlagerungen** Mehrere Zeitpläne können einander überschneiden. Im obigen Beispiel wirken sich beide Pläne auf die Maschinen der Buchhaltung aus. Die Maschinen können am Sonntag zweimal neu gestartet werden. Der Zeitplancode ist darauf ausgelegt, unerwünschte Neustarts zu vermeiden, es besteht jedoch keine Garantie, dass dies immer vermieden wird.

- Wenn Start- und Dauer beider Zeitpläne genau übereinstimmen, ist es wahrscheinlicher, dass die Maschinen nur einmal neu gestartet werden.
- Je stärker sich die Zeitpläne unterscheiden, umso wahrscheinlicher wird das Auftreten zweier Neustarts.
- Auch die Zahl der von einem Zeitplan betroffenen Maschinen wirkt sich auf die Möglichkeit einer Überlagerung aus. In dem hier aufgeführten Beispiel kann der wöchentliche Zeitplan für den Neustart aller Maschinen Neustarts schneller auslösen, als der tägliche Zeitplan für die Buchhaltung (je nach der jeweils konfigurierten Dauer).

Weitere Informationen zu Neustartplänen finden Sie unter Reboot schedule internals.

#### Anzeigen von Neustartzeitplänen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie die Seite **Neustartzeitplan**.

Die Seite **Neustartzeitplan** enthält die folgenden Informationen für jeden konfigurierten Zeitplan:

- Zeitplanname
- Gegebenenfalls verwendete Tagbeschränkung
- Anzahl der Maschinenneustarts

- Ob Maschinenbenutzer eine Benachrichtigung erhalten
- Ob der Zeitplan aktiviert ist Das Deaktivieren kann beim Testen, während bestimmter Zeiten oder beim Vorbereiten von Zeitplänen hilfreich sein.

**Hinzufügen (Anwenden) von Tags** Wenn Sie einen Neustartzeitplan mit einer Tagbeschränkung konfigurieren, stellen Sie sicher, dass das Tag den Maschinen hinzugefügt wird (bzw. auf sie angewendet wird), auf die der Zeitplan angewendet werden soll. Im obigen Beispiel wird ein Tag auf jede Maschine der Buchhaltung angewendet. Einzelheiten finden Sie unter Tags.

Sie können zwar mehrere Tags auf eine Maschine anwenden, ein Neustartzeitplan kann jedoch nur ein Tag enthalten.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie die Bereitstellungsgruppe mit den Maschinen, für die Sie den Zeitplan erstellen möchten.
3. Wählen Sie **Maschinen anzeigen** und dann die Maschinen, denen Sie das Tag hinzufügen möchten.
4. Wählen Sie in der Aktionsleiste **Tags verwalten**.
5. Wenn das Tag bereits vorhanden ist, aktivieren Sie das Kontrollkästchen neben dem Tagnamen. Ist das Tag noch nicht vorhanden, wählen Sie **Erstellen** und geben dann einen Namen für das Tag ein. Aktivieren Sie nach dem Erstellen des Tags das Kontrollkästchen neben dessen Namen.
6. Wählen Sie **Speichern** im Dialogfeld **Tags verwalten**.

**Erstellen eines Neustartzeitplans**

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie **Hinzufügen** auf der Seite **Neustartzeitplan**.
4. Führen Sie auf der Seite **Neustartzeitplan** folgende Schritte aus:
    - Aktivieren Sie **Ja**, um den Zeitplan zu aktivieren. Wählen Sie **Nein**, um den Zeitplan zu deaktivieren.
    - Geben Sie einen Namen und eine Beschreibung für den Zeitplan ein.
    - Wenden Sie für **Auf Tag beschränken** eine Tagbeschränkung an.
    - Wählen Sie für **Maschinen im Wartungsmodus einschließen** aus, ob solche Maschinen in dem Zeitplan enthalten sein sollen. Informationen zur Verwendung von PowerShell finden Sie unter Geplante Neustarts für Maschinen im Wartungsmodus.

- Legen Sie unter **Neustartintervall** fest, wie oft der Neustart durchgeführt werden soll: täglich, wöchentlich, monatlich oder einmal. Wenn Sie **Wöchentlich** oder **Monatlich** auswählen, können Sie einen oder mehrere Tage festlegen.
- Geben Sie für **Wiederholung alle** an, wie oft der Zeitplan ausgeführt werden soll.
- Geben Sie für **Startdatum** ein Startdatum für den Zeitplan an.
- Wählen Sie unter **Neustart beginnen um** eine Uhrzeit für den Neustart im 24-Stunden-Format aus.
- Option **Neustartdauer**:
  - Wenn Sie keinen natürlichen Neustart wünschen, wählen Sie **Alle Maschinen gleichzeitig neu starten** oder **Alle Maschinen innerhalb von …Minuten neu starten**.
  - Wenn Sie einen natürlichen Neustart wünschen, wählen Sie **Alle Maschinen nach dem Draining der Sitzungen neu starten**.

    Beim Inkrafttreten eines für den natürlichen Neustart konfigurierten Neustartzeitplans geschieht Folgendes:

    * Alle inaktiven Maschinen, die zur Bereitstellungsgruppe gehören, werden sofort neu gestartet.
    * Jede Maschine in der Bereitstellungsgruppe mit einer oder mehreren aktiven Sitzungen wird neu gestartet, wenn alle Sitzungen abgemeldet sind.

    > **Hinweis:**
    >
    > Sie können diese Option für energieverwaltete und nicht energieverwaltete Maschinen verwenden.

- Wählen Sie unter **Benachrichtigung an Benutzer senden** aus, ob auf den betroffenen Maschinen eine Meldung angezeigt werden soll, bevor der Neustart beginnt. Standardmäßig wird keine Meldung angezeigt.
- Wenn Sie festlegen, dass 15 Minuten vor dem Neustart eine Meldung angezeigt wird, können Sie unter **Benachrichtigungsintervall** vorgeben, dass die Meldung alle fünf Minuten nach Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt.
- Geben Sie den Titel und den Text der Benachrichtigung ein. Es gibt keinen Standardtext.

  Wenn die Meldung einen Countdown bis zum Neustart enthalten soll, verwenden Sie die Variable **%m%**. Sofern Sie keinen gleichzeitigen Neustart aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine zu der richtigen Zeit angezeigt.

5. Klicken Sie auf **Fertig**, um die Konfigurationsänderungen anzuwenden und das Fenster **Neustartzeitplan hinzufügen** zu schließen.

6. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster **Bereitstellungsgruppe bearbeiten** geöffnet bleibt. Alternativ klicken Sie auf **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

**Sofortiges Ausführen eines Neustartzeitplans** Über einen Neustartzeitplan wird der regelmäßige Neustart der Maschinen in einer Bereitstellungsgruppe festgelegt. Sie können einen Neustartzeitplan auch sofort ausführen, um die enthaltenen Maschine neu zu starten.

Um einen Neustart-Zeitplan sofort auszuführen, führen Sie die folgenden Schritte aus:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie die Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie auf der Seite **Neustartplan** einen Zeitplan und dann **Zeitplan jetzt ausführen**.

> **Hinweis:**
>
> - Ein Zeitplan, der mit der Einstellung **Alle Maschinen nach dem Draining der Sitzungen neu starten** konfiguriert ist, kann nicht sofort ausgeführt werden.
> - Sie können **Zeitplan jetzt ausführen** nur jeweils auf einen Zeitplan anwenden.
> - Nachdem Sie einen Zeitplan bearbeitet haben, ist **Zeitplan jetzt ausführen** nicht mehr verfügbar. Wählen Sie **Übernehmen** um ihn verfügbar zu machen.

**Bearbeiten, Entfernen, Aktivieren und Deaktivieren von Neustartzeitplänen**

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie auf der Seite **Neustartzeitplan** das Kontrollkästchen eines Zeitplans.

    - Um den Zeitplan zu bearbeiten, wählen Sie **Bearbeiten**. Aktualisieren Sie die Zeitplankonfiguration gemäß den Anweisungen unter Erstellen eines Neustartzeitplans.
    - Klicken Sie auf **Bearbeiten**, um den Zeitplan zu aktivieren oder zu deaktivieren. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Neustartzeitplan aktivieren**.
    - Zum Entfernen des Zeitplans wählen Sie **Löschen**. Bestätigen Sie das Entfernen. Das Entfernen eines Zeitplans hat keine Auswirkungen auf die auf die betroffenen Maschinen angewendeten Tags.

**Verzögerung geplanter Neustarts aufgrund eines Datenbankausfalls**

> **Hinweis:**
>
> Dieses Feature ist nur über PowerShell verfügbar.

Fällt vor einem geplanten Neustart von Maschinen (VDAs) in einer Bereitstellungsgruppe die Standortdatenbank aus, beginnt der Neustart erst nach Ende des Ausfalls. Diese Aktion kann zu unbeabsichtigten Ergebnissen führen.

Angenommen, Sie haben die Neustarts einer Bereitstellungsgruppe für außerhalb der Produktion (ab 3:00 Uhr nachts) geplant. Ein Ausfall der Standortdatenbank tritt eine Stunde vor Beginn des geplanten Neustarts (um 2:00 Uhr) auf. Der Ausfall dauert sechs Stunden (bis 8:00 Uhr). Der Neustartzeitplan beginnt, wenn die Verbindung zwischen dem Delivery Controller und der Standortdatenbank wiederhergestellt ist. Die VDA-Neustarts beginnen jetzt fünf Stunden nach dem ursprünglich geplanten Zeitpunkt. Diese Aktion kann dazu führen, dass VDAs während der Produktionszeit neu gestartet werden.

Um dies zu vermeiden, können Sie den Parameter `MaxOvertimeStartMins` für die Cmdlets `New-BrokerRebootScheduleV2` und `Set-BrokerRebootScheduleV2` verwenden. Der Wert gibt den maximalen Zeitraum außerhalb der geplanten Startzeit in Minuten an, nach dem ein Neustart-Zeitplan beginnen darf.

- Wenn die Datenbankverbindung innerhalb dieser Zeit wiederhergestellt wird (geplante Zeit + `MaxOvertimeStartMins`), beginnt der VDA-Neustart.
- Wenn die Datenbankverbindung innerhalb dieser Zeit nicht wiederhergestellt wird, beginnt der VDA-Neustart nicht.
- Wird dieser Parameter weggelassen oder hat er einen Null-Wert, beginnt der geplante Neustart unabhängig von der Ausfalldauer, sobald die Verbindung zur Datenbank wiederhergestellt wird.

Weitere Informationen finden Sie in der Hilfe zum Cmdlet. Dieses Feature ist nur über PowerShell verfügbar.

**Geplante Neustarts für Maschinen im Wartungsmodus** Wenn Sie angeben möchten, ob ein Neustartzeitplan auch Maschinen im Wartungsmodus einschließt, verwenden Sie die Option `IgnoreMaintenanceMode` mit den `BrokerRebootScheduleV2`-Cmdlets.

Das folgende Cmdlet erstellt beispielsweise einen Zeitplan für den Neustart von Maschinen im Wartungsmodus und von Maschinen, die nicht im Wartungsmodus sind.

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

Mit dem folgenden Cmdlet wird ein vorhandener Neustartzeitplan geändert.

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Weitere Informationen finden Sie in der Hilfe zum Cmdlet.

#### Lastverwaltung von Maschinen in Bereitstellungsgruppen

Die Lastverwaltung ist nur bei Maschinen mit Windows-Multisitzungs-OS möglich.

Bei der Lastverwaltung wird die Serverlast gemessen und festgelegt, welcher Server unter den aktuellen Umgebungsbedingungen auszuwählen ist. Diese Auswahl basiert auf folgenden Faktoren:

- **Wartungsmodusstatus des Servers:** Eine Maschine mit Windows-Multisitzungs-OS wird nur für den Lastausgleich berücksichtigt, wenn der Wartungsmodus für sie deaktiviert ist.
- **Serverlastindex:** bestimmt, mit welcher Wahrscheinlichkeit ein Server, der Maschinen mit Windows-Multisitzungs-OS bereitstellt, Verbindungen erhält. Der Index basiert auf einer Kombination von Lastauswertungskriterien: Anzahl der Sitzungen sowie Einstellungen für Leistungswerte (z. B. CPU-, Datenträger- und Speichernutzung). Die Lastauswertungskriterien werden in den Richtlinieneinstellungen für die Lastverwaltung festgelegt.

  Ein Serverlastindex von 10.000 bedeutet, dass der Server voll ausgelastet ist. Wenn keine anderen Server verfügbar sind, erhalten die Benutzer beim Starten einer Sitzung u. U. eine Meldung, dass der Desktop oder die Anwendung zurzeit nicht verfügbar ist.

  Sie können den Lastindex in Director (Überwachung), über die Suchfunktion in der Verwaltungsoberfläche "Vollständige Konfiguration"und im SDK überwachen.

  Wählen Sie in Konsolenanzeigen zum Einblenden der Spalte **Lastindex** (die standardmäßig ausgeblendet ist) eine Maschine, klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift und wählen Sie **Spalte auswählen**. Wählen Sie in der Kategorie **Maschine** die Option **Lastindex**.

  Verwenden Sie im SDK das Cmdlet `Get-BrokerMachine`. Weitere Informationen finden Sie unter CTX202150.
- **Richtlinieneinstellung "Toleranzwert für gleichzeitige Anmeldungen":** maximale Anzahl gleichzeitiger Serveranmeldeanforderungen. (Diese Einstellung entspricht der Lastdrosselung in XenApp-Versionen 6.x.)

  Wenn alle Server den Toleranzwert für gleichzeitige Anmeldungen erreichen oder überschreiten, wird die nächste Anmeldeanforderung dem Server mit der niedrigsten Anzahl ausstehender Anmeldungen zugewiesen. Wenn mehrere Server diese Kriterien erfüllen, wird der Server mit dem niedrigsten Lastindex ausgewählt.

#### Autoscale verwalten

Autoscale ist standardmäßig für Bereitstellungsgruppen deaktiviert. Führen Sie folgende Schritte aus, um AutoScale für eine Bereitstellungsgruppe zu verwalten (falls zutreffend):

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe aus und wählen Sie in der Aktionsleiste **Autoscale verwalten**. Das Fenster **Autoscale verwalten** wird angezeigt.
3. Konfigurieren Sie die Einstellungen nach Bedarf. Informationen zu Autoscale-Einstellungen finden Sie unter Autoscale.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Oder wählen Sie **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

## Sitzungen

- Abmelden oder Trennen einer Sitzung oder Senden einer Nachricht an Benutzer
- Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen
- Sitzungsroaming konfigurieren
- Wiederverbinden von Sitzungen nach der Trennung von einer Maschine im Wartungsmodus

### Abmelden oder Trennen einer Sitzung oder Senden einer Nachricht an Benutzer einer Bereitstellungsgruppe

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Zum Abmelden einer Sitzung wählen Sie die Sitzung oder den Desktop und dann in der Aktionsleiste **Abmelden**. Die Sitzung wird geschlossen und die Maschine steht nun anderen Benutzern zur Verfügung, sofern sie nicht einem bestimmten Benutzer zugewiesen ist.
4. Zum Trennen einer Sitzung wählen Sie die Sitzung oder den Desktop und dann in der Aktionsleiste **Trennen**. Anwendungen werden weiter ausgeführt und die Maschine bleibt dem Benutzer zugewiesen. Der Benutzer kann eine Verbindung mit derselben Maschine wiederherstellen.
5. Zum Senden einer Nachricht an die Benutzer wählen Sie die Sitzung, die Maschine oder den Benutzer und dann in der Aktionsleiste **Nachricht senden**. Geben Sie die Nachricht ein.

### Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen in einer Bereitstellungsgruppe

Diese Features werden nur auf Maschinen mit Multisitzungs-OS unterstützt.

Sitzungsvorabstart und Sitzungsfortbestehen helfen bestimmten Benutzern, schnell auf Anwendungen zuzugreifen:

- Starten von Sitzungen, bevor sie angefordert werden (Sitzungsvorabstart)
- Anwendungssitzungen aktiv halten, nachdem ein Benutzer alle Anwendungen schließt (Sitzungsfortbestehen)

Standardmäßig werden Sitzungsvorabstart und Sitzungsfortbestehen nicht verwendet. Eine Sitzung wird gestartet, wenn ein Benutzer eine Anwendung startet und sie bleibt aktiv, bis die letzte geöffnete Anwendung in der Sitzung geschlossen wird.

Überlegungen:

- Die Bereitstellungsgruppe muss Anwendungen unterstützen und auf den Maschinen muss ein VDA für Multisitzungs-OS in mindestens Version 7.6 ausgeführt werden.
- Diese Features werden nur bei Verwendung der Citrix Workspace-App für Windows unterstützt, sie erfordern außerdem zusätzliche Citrix Workspace-App-Konfigurationsschritte. Anweisungen hierzu finden Sie in der Produktdokumentation zu Ihrer Citrix Workspace-App für Windows-Version. Suchen Sie dort nach "Sitzungsvorabstart".
- Die Citrix Workspace-App für HTML5 wird nicht unterstützt.
- Wird eine Maschine in den Modus "Anhalten"oder in den Ruhezustand versetzt, funktioniert der Sitzungsvorabstart unabhängig von den Vorabstarteinstellungen nicht. Die Benutzer können ihre Maschinen/Sitzungen sperren. Wenn sie sich jedoch von der Citrix Workspace-App abmelden, wird die Sitzung beendet und ein Vorabstart ist nicht mehr möglich.
- Wird der Sitzungsvorabstart verwendet, können die Energieverwaltungsfunktionen "Anhalten" und "Ruhezustand"auf physischen Clientcomputern nicht verwendet werden. Clientmaschinenbenutzer können ihre Sitzungen sperren, sollten sich aber nicht abmelden.
- Vorab gestartete und fortbestehende Sitzungen verbrauchen eine Lizenz, jedoch nur wenn sie verbunden sind. Bei Verwendung einer Benutzer-/Gerätelizenz gilt die Lizenz 90 Tage. Nicht genutzte vorab gestartete und fortbestehende Sitzungen werden standardmäßig nach 15 Minuten getrennt. Dieser Wert kann über das PowerShell-Cmdlet `New/Set-BrokerSessionPreLaunch` konfiguriert werden.
- Eine sorgfältige Planung und Überwachung der Aktivitätsmuster von Benutzern ist wichtig, damit diese Features so eingerichtet werden können, dass sie einander ergänzen. In einer optimalen Konfiguration besteht ein Gleichgewicht zwischen dem Vorteil einer schnelleren Anwendungsverfügbarkeit für Benutzer und den durch den Verbrauch von Lizenzen und die fortdauernde Zuteilung von Ressourcen entstehenden Kosten.
- Sie können den Vorabstart von Sitzungen auch für eine spezifische Uhrzeit in der Citrix Workspace-App konfigurieren.

**Dauer des Aktivbleibens nicht genutzter vorab gestarteter und fortbestehender Sitzungen**
Wie lange eine nicht genutzte Sitzung aktiv bleibt, wenn der Benutzer keine Anwendung startet, kann über ein Timeout oder über Serverlast-Schwellenwerte angegeben werden. Sie können alle Parameter konfigurieren. Die Sitzung wird jeweils durch das zuerst auftretende Ereignis beendet.

- **Timeout:** Ein konfiguriertes Timeout gibt die Anzahl der Minuten, Stunden oder Tage an, die eine nicht genutzte, vorab gestartete oder fortbestehende Sitzung aktiv bleibt. Wenn Sie ein zu kurzes Timeout konfigurieren, werden vorab gestartete Sitzungen beendet, bevor der Benutzer in den Genuss des schnelleren Anwendungszugriffs kommt. Ist das Timeout zu lang, werden eingehende Benutzerverbindungen möglicherweise abgewiesen, da der Server nicht genügend Ressourcen hat.

  Sie können dieses Timeout nur über das SDK (`New`/`Set-BrokerSessionPreLaunch` Cmdlet) und nicht über die Verwaltungskonsole aktivieren. Wenn Sie das Timeout deaktivieren, wird es für die betreffende Bereitstellungsgruppe in der Konsole und auf den Seiten zum **Bearbeiten von Bereitstellungsgruppen** nicht angezeigt.

- **Schwellenwerte:** Das automatische Beenden vorab gestarteter und fortbestehender Sitzungen auf der Basis der Serverlast gewährleistet, dass Sitzungen so lange wie möglich geöffnet bleiben (vorausgesetzt, es sind Serverressourcen verfügbar). Nicht genutzte vorab gestartete und fortbestehende Sitzungen verursachen keine Abweisung von Verbindungen, da sie automatisch beendet werden, wenn Ressourcen für neue Benutzersitzungen benötigt werden.

  Sie können zwei Schwellenwerte konfigurieren: die durchschnittliche Last aller Server der Bereitstellungsgruppe und die höchste Last eines Servers in der Bereitstellungsgruppe (beides in Prozent). Wird ein Schwellenwert überschritten, werden jeweils die Sitzungen beendet, die sich am längsten im Zustand “vorab gestartet”bzw. “fortbestehend”befinden. Das Beenden erfolgt einzeln im Minutentakt bis die Last unter den Schwellenwert fällt. Solange der Schwellenwert überschritten ist, werden keine neuen Sitzungen vorab gestartet.

Server mit VDAs, die nicht bei einem Controller registriert sind, und Server im Wartungsmodus gelten als voll ausgelastet. Bei einem ungeplanten Ausfall werden vorab gestartete und fortbestehende Sitzungen automatisch beendet, um Kapazität freizugeben.

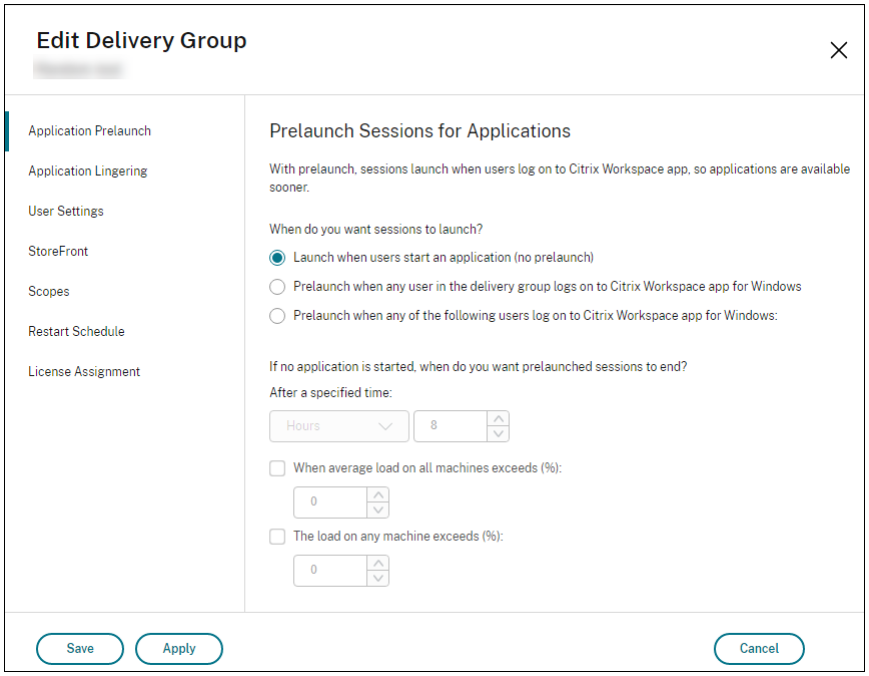
#### Aktivieren des Vorabstarts von Sitzungen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Aktivieren Sie den Vorabstart von Sitzungen, indem Sie auf der Seite **Anwendungsvorabstart** auswählen, wann Sitzungen gestartet werden sollen:

   - Wenn Benutzer eine Anwendung starten. Dies ist die Standardeinstellung. Vorabstartsitzungen sind deaktiviert.
   - Wenn ein Benutzer der Bereitstellungsgruppe sich bei der Citrix Workspace-App für Windows anmeldet.

- Wenn ein beliebiger Benutzer einer Liste mit Benutzern und Bereitstellungsgruppen sich bei der Citrix Workspace-App für Windows anmeldet. Bei Auswahl dieser Option müssen Sie auch die Benutzer oder Benutzergruppen festlegen.




4. Eine vorab gestartete Sitzung wird durch eine normale Sitzung ersetzt, wenn der Benutzer eine Anwendung startet. Wenn der Benutzer keine Anwendung startet (d. h. die vorab gestartete Sitzung wird nicht verwendet), wird durch die folgenden Einstellungen bestimmt, wie lange die Sitzung aktiv bleibt.

   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern: 1–99 Tage, 1–2376 Stunden oder 1–142.560 Minuten.
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1–99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1–99 %) übersteigt.

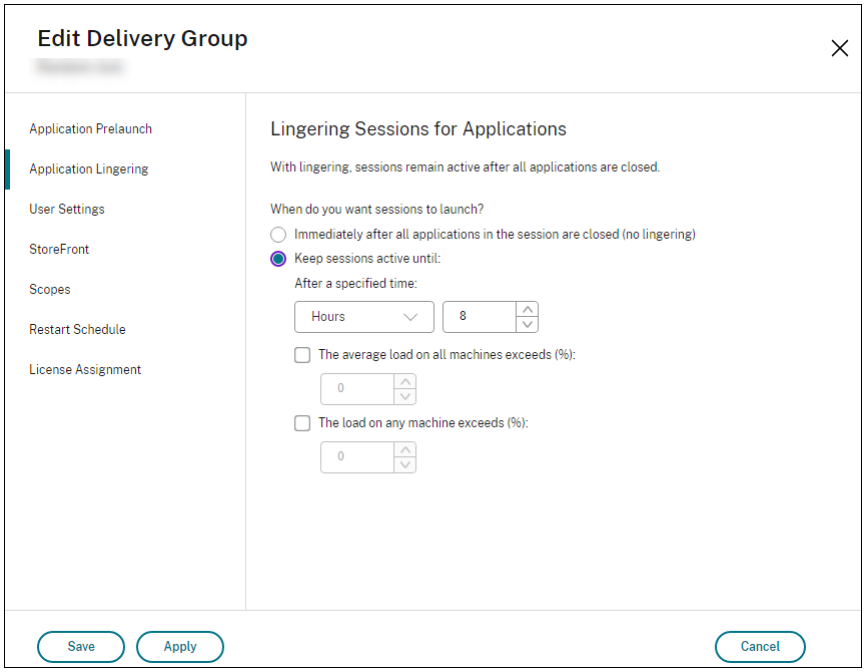
   Eine vorab gestartete Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

### Aktivieren des Sitzungsfortbestehens

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.

3. Aktivieren Sie auf der Seite **Anwendungsfortbestehen** das Sitzungsfortbestehen durch Aktivieren von **Sitzungen bleiben aktiv bis**.




4. Mehrere Einstellungen wirken sich darauf aus, wie lange eine Sitzung aktiv bleibt, wenn der Benutzer keine weitere Anwendung startet.

   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern: 1–99 Tage, 1–2376 Stunden oder 1–142.560 Minuten.
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1–99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1–99 %) übersteigt.

   Eine fortbestehende Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

### Sitzungsroaming konfigurieren

Das Sitzungsroaming ist standardmäßig für Bereitstellungsgruppen aktiviert. Sitzungen wechseln zusammen mit dem Benutzer von Clientgerät zu Clientgerät. Wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet, wird die gleiche Sitzung verwendet und die Anwendungen stehen gleichzeitig auf beiden Geräten zur Verfügung. Sie können die Anwendungen auf mehreren Geräten anzeigen. Die Anwendungen folgen dem Benutzer unabhängig von dem Gerät und davon, ob aktuelle Sitzungen vorhanden sind. Oft folgen auch Drucker und andere Ressourcen, die

einer Anwendung zugewiesen sind. Alternativ können Sie auch PowerShell verwenden. Weitere Informationen finden Sie unter Sitzungsroaming.

**Sitzungsroaming für Anwendungen konfigurieren** Führen Sie folgende Schritte aus, um das Sitzungsroaming für Anwendungen zu konfigurieren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie auf der Seite **Benutzer** das Kontrollkästchen **Sitzungen wechseln mit Benutzern, wenn sie Geräte wechseln**, um das Sitzungsroaming zu aktivieren.
    - Wenn diese Option aktiviert ist, wird auf beiden Geräten die gleiche Sitzung verwendet und angezeigt, wenn ein Benutzer eine Anwendungssitzung startet und dann mit einem anderen Gerät weiterarbeitet. Wenn die Option deaktiviert ist, wechselt die Sitzung nicht mehr zu anderen Geräten.
4. Wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

**Sitzungsroaming für Desktops konfigurieren** Führen Sie folgende Schritte aus, um das Sitzungsroaming für einen Desktop zu konfigurieren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Desktops** den Desktop und wählen Sie dann **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **Sitzungsroaming**, um das Sitzungsroaming zu ermöglichen.
    - Wenn diese Option aktiviert ist, wird die gleiche Sitzung verwendet und die Anwendungen stehen auf beiden Geräten zur Verfügung, wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet. Wenn die Option deaktiviert ist, wechselt die Sitzung nicht mehr zu anderen Geräten.
5. Wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

**Wiederverbinden von Sitzungen nach der Trennung von einer Maschine im Wartungsmodus**

> **Hinweis:**
>
> Dieses Feature ist nur über PowerShell verfügbar.

Legen Sie fest, ob Sitzungen, die von Maschinen im Wartungsmodus getrennt wurden, sich erneut mit Maschinen in der Bereitstellungsgruppe verbinden dürfen.

Bis Ende Mai 2021 war das Wiederverbinden von Sitzungen, die von Maschinen im Wartungsmodus getrennt wurden, auf gepoolten Einzelsitzungsdesktops nicht zulässig. Jetzt kann eine konfigurierte Bereitstellungsgruppe das Wiederverbinden (unabhängig vom Sitzungstyp) nach der Trennung von einer Maschine im Wartungsmodus zulassen oder verhindern.

Beim Erstellen oder Bearbeiten einer Bereitstellungsgruppe (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`) können Sie mit dem Parameter `-AllowReconnectInMaintenanceMode <boolean>` das Wiederherstellen der Verbindung zu einer Maschine im Wartungsmodus zulassen oder verhindern.

- Wenn der Wert auf “true”festgelegt ist, können Sitzungen sich erneut mit Maschinen in der Gruppe verbinden.
- Wenn der Wert auf “false”festgelegt ist, können Sitzungen die Verbindung zu Maschinen in der Gruppe nicht wiederherstellen.

Standardwerte:

- Einzelsitzung: Deaktiviert
- Multisitzung: Aktiviert

## Anwendungen

Zeigen Sie Anwendungen in einer Bereitstellungsgruppe an und fügen Sie bei Bedarf weitere hinzu.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe aus. Wenn diese Gruppe Anwendungen enthält, wird in der Aktionsleiste **Anwendungen anzeigen** angezeigt.
3. Wählen Sie **Anwendungen anzeigen** aus. Sie werden zum Knoten **Anwendungen** weitergeleitet, in dem alle in dieser Gruppe verfügbaren Anwendungen angezeigt werden.
4. Um dieser Gruppe weitere Anwendungen hinzuzufügen, wechseln Sie zum Knoten **Bereitstellungsgruppen**, wählen Sie die Gruppe aus und wählen Sie in der Aktionsleiste **Anwendungen hinzufügen** aus.

### Problembehandlung

- Nicht bei einem Delivery Controller registrierte VDAs kommen beim Start gebrokerter Sitzungen nicht in die Auswahl. Dies hat eine mangelnde Auslastung verfügbarer Ressourcen zur Folge. Es gibt eine Reihe von Gründen, warum ein VDA nicht registriert sein könnte. Viele können vom Administrator behandelt werden. Die Detailanzeige bietet Informationen zur Problembehandlung im Assistenten zum Erstellen von Maschinenkatalogen und nach dem Hinzufügen eines Katalogs zu einer Bereitstellungsgruppe.

  Nach Erstellung einer Bereitstellungsgruppe wird im zugehörigen Detailbereich die Anzahl der Maschinen angezeigt, die registriert sein sollten, es jedoch nicht sind. Es kann beispielsweise Maschinen geben, die eingeschaltet und nicht im Wartungsmodus sind, jedoch nicht bei einem Controller registriert sind. Beim Anzeigen einer Maschine, die eigentlich registriert sein müsste, enthält die Registerkarte **Problembehandlung** im Detailbereich Informationen zu möglichen Ursachen und empfohlene Korrekturmaßnahmen.

  Informationen zu Meldungen zur Funktionsebene finden Sie unter VDA-Versionen und Funktionsebenen.

  Informationen zur Fehlerbehebung bei der VDA-Registrierung finden Sie unter CTX136668.

- Im Detailbereich für Bereitstellungsgruppen unter **Installierte VDA-Version** möglicherweise nicht die tatsächlich auf den Maschinen installierte Version angezeigt. In der Maschine wird in Windows unter “Programme und Features”die tatsächliche VDA-Version angezeigt.
- Empfehlungen für Maschinen mit einem unbekannten Energiezustand finden Sie unter **CTX131267**.

## Anwendungsgruppen erstellen

June 12, 2024

### Einführung

Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden. Anwendungsgruppen sind optional. Sie bieten eine Alternative zum Hinzufügen derselben Anwendungen zu mehreren Bereitstellungsgruppen. Bereitstellungsgruppen können mehreren Anwendungsgruppen und Anwendungsgruppen können mehreren Bereitstellungsgruppen zugeordnet werden.

Die Verwendung von Anwendungsgruppen kann für die Anwendungsverwaltung und Ressourcensteuerung gegenüber der Verwendung weiterer Bereitstellungsgruppen folgende Vorteile bieten:

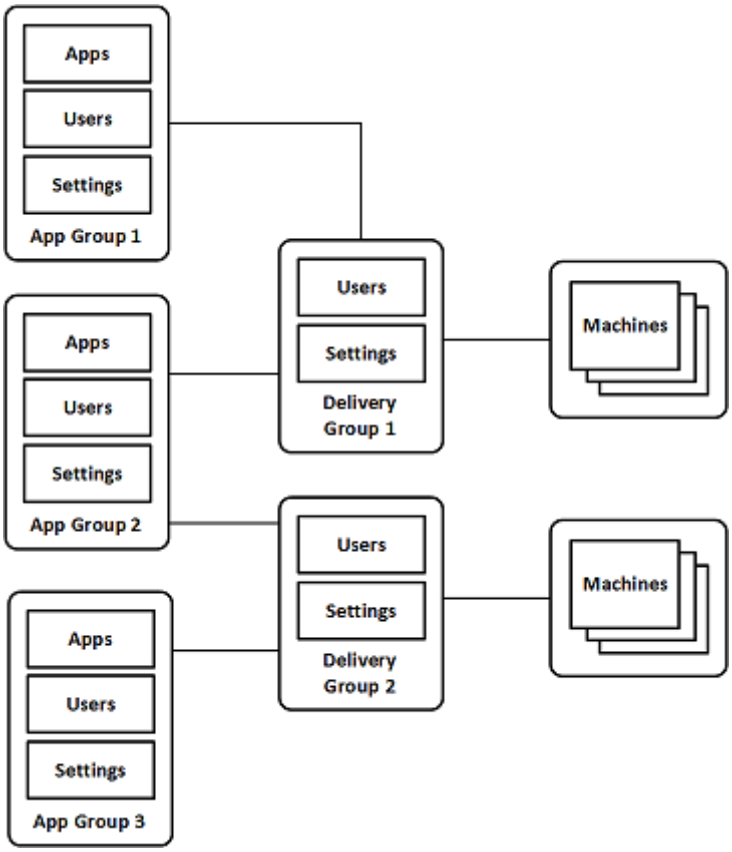
- Durch die logische Gruppierung von Anwendungen und deren Einstellungen können Sie diese als Einheit verwalten. Sie müssen beispielsweise dieselbe Anwendung nicht mehreren Bereitstellungsgruppen einzeln hinzufügen (bzw. für diese veröffentlichen).
- Die Sitzungsfreigabe zwischen den Anwendungsgruppen kann Ressourcen sparen. In anderen Fällen ist das Deaktivieren der Sitzungsfreigabe zwischen Anwendungsgruppen möglicherweise nützlich.
- Mit der Tagbeschränkung können Sie Anwendungen aus einer Anwendungsgruppe nur auf einigen Maschinen in den ausgewählten Bereitstellungsgruppen veröffentlichen. Mit Tagbeschränkungen können Sie Ihre vorhandenen Maschinen für mehrere Veröffentlichungstasks verwenden und sparen so die Kosten für die Bereitstellung und Verwaltung zusätzlicher Maschinen. Die Verwendung von Tagbeschränkungen kann man sich als Unterteilung (oder Partitionierung) der Maschinen in einer Bereitstellungsgruppe vorstellen. Anwendungsgruppen und Desktops mit Tagbeschränkungen können auch zur Isolierung von Maschinengruppen in einer Bereitstellungsgruppe zur Problembehandlung nützlich sein.

## Beispielkonfigurationen

### Beispiel 1

Die folgende Abbildung zeigt eine Bereitstellung mit Anwendungsgruppen:




In dieser Konfiguration werden Anwendungen Anwendungsgruppen und nicht Bereitstellungsgruppen hinzugefügt. Über die Bereitstellungsgruppen wird festgelegt, welche Maschinen verwendet werden. (Obwohl dies nicht ausgezeichnet ist, sind die Maschinen in Maschinenkatalogen.)

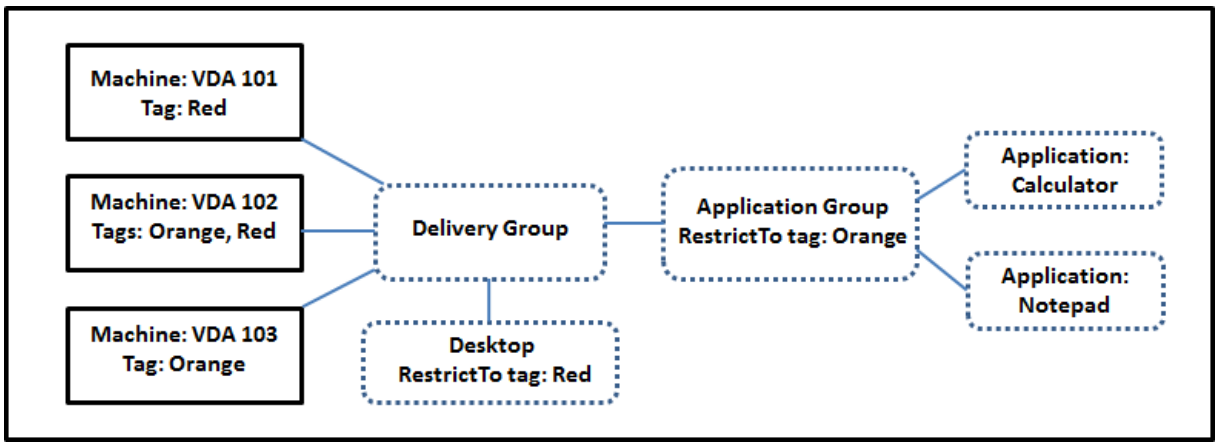
Anwendungsgruppe 1 ist Bereitstellungsgruppe 1 zugeordnet. Die Anwendungen in Anwendungsgruppe 1 sind für Benutzer der Anwendungsgruppe 1 zugänglich, sofern diese auch auf der Benutzerliste von Bereitstellungsgruppe 1 stehen. Diese Struktur folgt der Leitlinie, dass die Benutzerliste einer Anwendungsgruppe eine Teilgruppe (d. h. Einschränkung) der Benutzerlisten der zugeordneten Bereitstellungsgruppen sein muss. Die Einstellungen von Anwendungsgruppe 1 (Sitzungsfreigabe zwischen den Anwendungsgruppen, zugeordnete Bereitstellungsgruppen usw.) gelten für die Anwendungen und Benutzer in der Gruppe. Die Einstellungen in Bereitstellungsgruppe 1 (z. B. Unterstützung für anonyme Benutzer) gelten für die Benutzer in Anwendungsgruppe 1 und 2, da beide Anwendungsgruppen der Bereitstellungsgruppe zugeordnet sind.

Anwendungsgruppe 2 ist den Bereitstellungsgruppen 1 und 2 zugeordnet. Beiden Bereitstellungsgruppen kann in Anwendungsgruppe 2 eine Priorität zugewiesen werden, welche die Reihenfolge vorgibt, in der die Bereitstellungsgruppen beim Starten einer Anwendung geprüft werden. Für Bereitstellungsgruppen mit der gleichen Priorität findet ein Lastausgleich statt. Die Anwendungen in Anwendungsgruppe 2 sind für Benutzer der Anwendungsgruppe 2 zugänglich, sofern diese auch auf den Benutzerlisten von Bereitstellungsgruppe 1 und 2 stehen.

**Beispiel 2**

Diese einfache Anordnung besitzt Tagbeschränkungen, die festlegen, welche Maschinen für bestimmte Desktop- und Anwendungsstarts in Betracht gezogen werden. Die Site hat eine freigegebene Bereitstellungsgruppe, einen veröffentlichten Desktop und eine Anwendungsgruppe mit zwei Anwendungen.




Allen drei Maschinen (VDA 101–103) wurden Tags hinzugefügt.

Die Anwendungsgruppe wurde mit der Tagbeschränkung "Orange"erstellt, sodass alle ihre Anwendungen (Rechner und Editor) nur auf Maschinen gestartet werden können, die das Tag "Orange" haben: VDA 102 und 103.

Detailliertere Beispiele und Informationen über die Verwendung von Tagbeschränkungen für Anwendungsgruppen und Desktops finden Sie unter Tags.

## Empfehlungen und Tipps

Citrix empfiehlt, Anwendungen entweder Anwendungsgruppen oder Bereitstellungsgruppen zuzuordnen, jedoch nicht beidem. Werden dieselben Anwendungen zwei Gruppentypen zugeordnet, kann dies die Verwaltung erschweren.

Standardmäßig sind Anwendungsgruppen aktiviert. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.

Standardmäßig ist die Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert. Weitere Informationen finden Sie unter Sitzungsfreigabe zwischen Anwendungsgruppen.

Citrix empfiehlt, Bereitstellungsgruppen auf die aktuelle Version zu aktualisieren. Dies erfordert Folgendes:

1. Upgrade von VDAs auf den Maschinen in der Bereitstellungsgruppe

2. Wechsel zu einer höheren Funktionsebene für die Maschinenkataloge, die diese Maschinen enthalten
3. Wechsel zu einer höheren Funktionsebene für die Bereitstellungsgruppe.

Weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen.

Zur Verwendung von Anwendungsgruppen müssen die Kernkomponenten mindestens in Version 7.9 vorliegen.

Zum Erstellen von Anwendungsgruppen ist die Berechtigung zur delegierten Administration der integrierten Rolle des Bereitstellungsgruppenadministrators erforderlich. Weitere Informationen finden Sie unter Delegierte Administration.

In diesem Abschnitt wird der Begriff der Zuordnung von Anwendungen zu Anwendungsgruppen verwendet, um den Unterschied zum Hinzufügen einer neuen Anwendungsinstanz aus einer verfügbaren Quelle zu unterstreichen. Das Gleiche gilt für Bereitstellungsgruppen und Anwendungsgruppen. Diese werden einander zugeordnet und nicht als Komponenten hinzugefügt.

### Sitzungsfreigabe und Anwendungsgruppen

Wenn die Sitzungsfreigabe aktiviert ist, starten alle Anwendungen in der gleichen Anwendungssitzung. Dies spart die Kosten für zusätzliche Sitzungen und ermöglicht die Verwendung von Anwendungsfeatures, wie Kopieren und Einfügen, welche die Zwischenablage erfordern. In manchen Situationen ist es jedoch möglicherweise erforderlich, die Sitzungsfreigabe zu deaktivieren.

Bei Verwendung von Anwendungsgruppen können Sie die Sitzungsfreigabe auf dreierlei Weise konfigurieren (eine Erweiterung gegenüber den Möglichkeiten bei bloßer Verwendung von Bereitstellungsgruppen):

- Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert
- Sitzungsfreigabe nur für Anwendungen innerhalb einer Anwendungsgruppe aktiviert
- Sitzungsfreigabe deaktiviert

#### Sitzungsfreigabe zwischen Anwendungsgruppen

Sie können die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen aktivieren oder deaktivieren. In letzterem Fall ist sie nur für Anwendungen in derselben Anwendungsgruppe möglich.

- **Beispielszenario, in dem die Aktivierung der Sitzungsfreigabe zwischen Anwendungsgruppen nützlich ist:**

  Anwendungsgruppe 1 enthält Microsoft Office-Anwendungen, z. B. Microsoft Word und Excel. Anwendungsgruppe 2 enthält andere Anwendungen, z. B. Editor und Rechner. Beide Anwendungsgruppen sind derselben Bereitstellungsgruppe zugewiesen. Ein Benutzer mit Zugriff auf

beide Anwendungsgruppen startet eine Anwendungssitzung mit Word und startet dann Editor. Wenn die Sitzung mit Word zum Ausführen von Editor geeignet ist, wird Editor in der bestehenden Sitzung gestartet. Kann Editor nicht in der vorhandenen Sitzung ausgeführt werden, z. B. weil eine Tagbeschränkung die Maschine ausschließt, auf der die Sitzung ausgeführt wird, wird eine neue Sitzung auf einer geeigneten Maschine erstellt.

- **Beispielszenario, in dem die Deaktivierung der Sitzungsfreigabe zwischen Anwendungsgruppen nützlich ist:**

  Sie haben einige Anwendungen, die mit anderen, auf denselben Maschinen installierten Anwendungen nicht gut zusammenarbeiten, z. B. zwei verschiedene Versionen der gleichen Software oder des gleichen Webbrowsers. Sie möchten nicht, dass ein Benutzer beide Versionen in derselben Sitzung startet.

  Sie erstellen mehrere Anwendungsgruppen und fügen jede Version der Software einer eigenen Anwendungsgruppe hinzu. Wenn die Sitzungsfreigabe zwischen diesen Anwendungsgruppen deaktiviert ist, können die in den Gruppen angegebenen Benutzer Anwendungen der gleichen Version in der gleichen Sitzung ausführen und sie können gleichzeitig andere Anwendungen ausführen, jedoch nicht in der gleichen Sitzung. Wenn ein Benutzer eine der in mehreren Versionen vorliegenden Anwendungen (die in verschiedenen Anwendungsgruppen sind) oder eine nicht in einer Anwendungsgruppe befindliche Anwendung startet, wird diese in einer neuen Sitzung gestartet.

Die Sitzungsfreigabe zwischen Anwendungsgruppen ist keine Sicherheits-Sandbox. Sie ist nicht betriebssicher und kann nicht verhindern, dass Benutzer Anwendungen in ihren Sitzungen über andere Methoden (z. B. über Windows Explorer) starten.

Wenn eine Maschine unter Volllast steht, werden keine neue Sitzungen auf ihr gestartet. Neue Anwendungen werden nach Bedarf in vorhandenen Sitzungen gestartet, vorausgesetzt die hier beschriebenen Bedingungen für die Sitzungsfreigabe sind erfüllt.

Sie können vorab gestartete Sitzungen nur Anwendungsgruppen zur Verfügung stellen, für die die Sitzungsfreigabe zugelassen ist. Sitzungen mit aktiviertem Sitzungsfortbestehen stehen allen Anwendungsgruppen zur Verfügung. Diese Features müssen jedoch in jeder den Anwendungsgruppen zugeordneten Bereitstellungsgruppe aktiviert und konfiguriert werden. Sie können sie nicht in den Anwendungsgruppen konfigurieren.

Die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Dies können Sie bei der Erstellung der Gruppe nicht ändern. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.

#### Deaktivieren der Sitzungsfreigabe innerhalb von Anwendungsgruppen

Sie können die Sitzungsfreigabe zwischen Anwendungen in derselben Anwendungsgruppe verhindern.

- **Beispielszenario, in dem die Deaktivierung der Sitzungsfreigabe innerhalb von Anwendungsgruppen nützlich ist:**

  Die Benutzer sollen simultan auf mehrere Vollbildsitzungen einer Anwendung auf separaten Monitoren zugreifen.

  Sie erstellen eine Anwendungsgruppe und fügen ihr die Anwendungen hinzu. Wenn die Sitzungsfreigabe zwischen den Anwendungen der Anwendungsgruppe nicht zugelassen ist und ein Benutzer Anwendungen nacheinander startet, werden sie in separaten Sitzungen gestartet und der Benutzer kann jede zu einem separaten Monitor verschieben.

Die Anwendungssitzungsfreigabe wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Dies können Sie bei der Erstellung der Gruppe nicht ändern. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.

### Erstellen von Anwendungsgruppen

Erstellen Sie eine Anwendungsgruppe, um Anwendungskategorien in der Citrix Workspace-App zu erstellen. Anwendungskategorien ermöglichen die Verwaltung von Anwendungssammlungen in Citrix Workspace.

Gehen Sie zum Erstellen von Anwendungsgruppen folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Um Anwendungsgruppen mithilfe von Ordnern zu organisieren, erstellen Sie die Ordner im Stammordner **Anwendungsgruppen**.
3. Wählen Sie den Ordner aus, in dem Sie die Gruppe erstellen möchten, und klicken Sie auf **Anwendungsgruppe erstellen**. Der Assistent zum Erstellen von Gruppen wird gestartet und es erscheint eine **Einführungsseite**. Sie können die Seite bei zukünftigen Starts des Assistenten ausblenden.
4. Konfigurieren Sie im Assistenten die Einstellungen auf den unten beschriebenen Seiten. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **Weiter**, bis Sie zur Seite **Zusammenfassung** gelangen.

**Schritt 1: Bereitstellungsgruppen**

Auf der Seite **Bereitstellungsgruppen** werden alle Bereitstellungsgruppen zusammen mit der Anzahl enthaltener Maschinen aufgelistet.

- Die Liste **Kompatible Bereitstellungsgruppen** enthält Bereitstellungsgruppen, die Sie auswählen können. Kompatible Bereitstellungsgruppen enthalten zufällige (nicht dauerhaft oder statisch zugewiesene) Server- oder Desktopbetriebssystemmaschinen.
- Die Liste **Nicht kompatible Bereitstellungsgruppen** enthält Bereitstellungsgruppen, die Sie nicht auswählen können. Jeder Eintrag enthält eine Begründung der Inkompatibilität, z. B. "enthält statisch zugewiesene Maschinen".

Eine Anwendungsgruppe kann Bereitstellungsgruppen zugeordnet werden, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten.

Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, wenn folgende Bedingungen erfüllt sind:

- Die Bereitstellungsgruppe enthält freigegebene Maschinen und wurde mit einer XenDesktop-Version vor 7.9 erstellt.
- Sie haben die Berechtigung zum Bearbeiten der Bereitstellungsgruppe.

Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen"geändert, wenn für den Assistenten zum Erstellen von Gruppen ein Commit ausgeführt wird.

Sie können Anwendungsgruppen erstellen, die keiner Bereitstellungsgruppe zugeordnet sind, z. B. zum Organisieren von Anwendungen oder als Speicher für Anwendungen, die gerade nicht verwendet werden. Anwendungsgruppen können jedoch erst dann zum Bereitstellen von Anwendungen verwendet werden, wenn sie mindestens einer Bereitstellungsgruppe zugeordnet sind. Außerdem können Sie einer Anwendungsgruppe keine Anwendungen aus der Quelle **Vom Startmenü** hinzufügen, wenn keine Bereitstellungsgruppen angegeben sind.

Über die Bereitstellungsgruppen legen Sie fest, welche Maschinen für die Bereitstellung von Anwendungen verwendet werden. Aktivieren Sie die Kontrollkästchen neben den Bereitstellungsgruppen, die Sie der Anwendungsgruppe zuordnen möchten.

Zum Hinzufügen einer Tagbeschränkung wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus der Dropdownliste aus.

**Schritt 2: Benutzer**

Geben Sie an, wer die Anwendungen in der Anwendungsgruppe verwenden kann. Sie können entweder alle Benutzer und Gruppen in den Bereitstellungsgruppen, die Sie auf der vorherigen Seite ausgewählt haben, angeben oder bestimmte Benutzer bzw. Benutzergruppen aus den Bereitstellungsgruppen auswählen. Wenn Sie die Benutzer einschränken, haben nur die in der Bereitstellungsgruppe

und der Anwendungsgruppe angegebenen Benutzer Zugriff auf die Anwendungen in der Anwendungsgruppe. Im Prinzip wirkt die Benutzerliste der Anwendungsgruppe als Filter für die Benutzerlisten in den Bereitstellungsgruppen.

Das Aktivieren oder Deaktivieren der Anwendungsverwendung durch nicht authentifizierte Benutzer ist nur über Bereitstellungsgruppen, nicht aber über Anwendungsgruppen möglich.

Informationen darüber, wo Benutzerlisten festgelegt werden, finden Sie unter Festlegung von Benutzerlisten.

#### Schritt 3: Anwendungen

Nützliche Info:

- Standardmäßig werden neu hinzugefügte Anwendungen im Ordner **Anwendungen** abgelegt. Sie können einen anderen Ordner angeben. Wenn Sie eine Anwendung hinzufügen und es dort bereits eine Anwendung mit dem gleichen Namen gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie den empfohlenen eindeutigen Namen annehmen, wird die Anwendung unter dem Namen hinzugefügt. Andernfalls müssen Sie sie umbenennen, damit sie hinzugefügt werden kann. Weitere Informationen finden Sie unter Verwalten von Anwendungsordnern.
- Sie können Anwendungseigenschaften (Einstellungen) beim Hinzufügen oder später ändern. Weitere Informationen finden Sie unter Ändern der Eigenschaften. Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie in die Oberfläche "Verwalten > Vollständige Konfiguration"die Eigenschaft **Anwendungsname (Benutzer)**. Andernfalls wird den Benutzern der Name in der Citrix Workspace-App doppelt angezeigt.
- Wenn Sie eine Anwendung mehreren Anwendungsgruppen hinzufügen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Anwendungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Gruppen, denen die Anwendung hinzugefügt wurde.

Wählen Sie die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

- **Vom Startmenü:** Anwendungen, die auf einer Maschine in den ausgewählten Bereitstellungsgruppen erkannt werden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und wählen Sie **OK**.

  Diese Quelle steht nicht zur Verfügung, wenn Sie eines der folgenden Elemente ausgewählt haben:

  - Anwendungsgruppen, denen keine Bereitstellungsgruppen zugeordnet sind.

  - Anwendungsgruppen mit zugeordneten Bereitstellungsgruppen, die keine Maschinen enthalten.
  - Eine Bereitstellungsgruppe, die keine Maschinen enthält.

- **Manuell:** Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Nach Eingabe dieser Informationen wählen Sie **OK**.
- **Vorhandene:** Anwendungen, die der Site bereits hinzugefügt wurden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und wählen Sie **OK**. Diese Quelle kann nicht ausgewählt werden, wenn es in der Site keine Anwendungen gibt.
- **Anwendungspakete:** Anwendungen in App-V-, MSIX-, MSIX App Attach- oder FlexApp-Anwendungspaketen. Wenn Sie diese Quelle auswählen, wird die Seite **Anwendungen aus Paketen hinzufügen** geöffnet. Wählen Sie eine Anwendungspaketquelle und in der daraufhin angezeigten Anzeige die Anwendungen aus, die Sie hinzufügen möchten. Klicken Sie dann auf **OK**

  > **Hinweis:**
  >
  > Um MSIX- oder MSIX-Apps mit App-Anhängen zu veröffentlichen, muss die Funktionsebene der Bereitstellungsgruppe 2106 oder höher sein. Für FlexApp-Apps muss die Funktionsebene 2206 oder höher sein. Wenn eine Anforderung auf Funktionsebene nicht erfüllt ist, sind die entsprechenden Optionen in der Dropdownliste **Quelle des Anwendungspakets** abgeblendet.
  >
  > **Hinweis:**
  >
  > VDA-Version 2003 und höher unterstützen das Veröffentlichen von App-V-Paketen aus HTTP-URLs nicht. Sie können diese Anwendungen nicht aus der Liste auswählen.

Wie bereits erwähnt, können Einträge in der Dropdownliste **Hinzufügen** nicht ausgewählt werden, wenn es keine gültige Quelle des jeweiligen Typs gibt. Nicht kompatible Quellen werden nicht aufgelistet (z. B. können Sie Anwendungsgruppen keine Anwendungsgruppen hinzufügen, daher wird diese Quelle nicht angezeigt).

#### Schritt 4: Geltungsbereiche

Diese Seite wird nur angezeigt, wenn Sie zuvor einen benutzerdefinierten Geltungsbereich erstellt haben. Standardmäßig ist der Bereich **Alles** ausgewählt. Weitere Informationen finden Sie unter Delegierte Administration.

**Schritt 5: Zusammenfassung**

Geben Sie einen Namen für die Anwendungsgruppe ein. Sie können optional auch eine Beschreibung eingeben.

Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig stellen**.

# Anwendungsgruppen verwalten

January 31, 2023

## Einführung

Nachfolgend wird die Verwaltung von Anwendungsgruppen beschrieben, die Sie erstellt haben.

Unter Anwendungen finden Sie Informationen zur Verwaltung von Anwendungen in Anwendungsgruppen oder Bereitstellungsgruppen. Es werden u. a. folgende Themen behandelt:

- Hinzufügen und Entfernen von Anwendungen zu bzw. aus Anwendungsgruppen:
- Ändern von Anwendungsgruppenzuordnungen

Zum Verwalten von Anwendungsgruppen sind die Berechtigungen zur delegierten Administration der integrierten Rolle des Bereitstellungsgruppenadministrators erforderlich. Weitere Informationen finden Sie unter Delegierte Administration.

## Aktivieren und Deaktivieren von Anwendungsgruppen

Wenn eine Anwendungsgruppe aktiviert wurde, kann sie die Anwendungen bereitstellen, die ihr hinzugefügt wurden. Durch Deaktivieren einer Anwendungsgruppe werden alle darin enthaltenen Anwendungen deaktiviert. Anwendungen, die auch anderen aktivierten Anwendungsgruppen zugeordnet sind, können über diese Gruppen bereitgestellt werden. Wenn eine Anwendung nicht nur einer Anwendungsgruppe, sondern explizit auch einer mit der Anwendungsgruppe verknüpften Bereitstellungsgruppe hinzugefügt wurde, hat das Deaktivieren der Anwendungsgruppe keine Auswirkungen auf die Anwendung in der Bereitstellungsgruppe.

Anwendungsgruppen werden bei der Erstellung automatisch aktiviert. Dies können Sie bei der Erstellung der Gruppe nicht ändern.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.

2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Anwendungsgruppe aktivieren**.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Aktivieren und Deaktivieren der Anwendungssitzungsfreigabe zwischen Anwendungsgruppen

Die Sitzungsfreigabe zwischen Anwendungsgruppen wird beim Erstellen von Anwendungsgruppen aktiviert. Dies können Sie bei der Erstellung der Gruppe nicht ändern. Weitere Informationen finden Sie unter Sitzungsfreigabe zwischen Anwendungsgruppen.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert**.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Deaktivieren der Anwendungssitzungsfreigabe in einer Anwendungsgruppe

Die Sitzungsfreigabe zwischen Anwendungen in einer Gruppe wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Wenn Sie die Sitzungsfreigabe zwischen Anwendungsgruppen deaktivieren, bleibt sie für Anwendungen in derselben Gruppe aktiviert.

Mit dem PowerShell-SDK können Sie Anwendungsgruppen konfigurieren, bei denen die Sitzungsfreigabe zwischen den enthaltenen Anwendungen deaktiviert ist. In manchen Situationen kann dies vorteilhaft sein. Ein Beispiel wäre, wenn Benutzer Nicht-Seamless-Anwendungen in voller Fenstergröße auf separaten Monitoren öffnen sollen.

Wenn Sie die Sitzungsfreigabe in einer Anwendungsgruppe deaktivieren, wird jede Anwendung in der Gruppe in einer eigenen Anwendungssitzung gestartet. Wenn eine geeignete getrennte Sitzung verfügbar ist, in der dieselbe Anwendung ausgeführt wird, wird eine Verbindung zu dieser Sitzung wiederhergestellt. Wenn Sie beispielsweise Editor starten und es gibt eine getrennte Sitzung, in der

Editor ausgeführt wird, wird keine neue Sitzung gestartet, sondern die Verbindung mit der getrennten Sitzung wiederhergestellt. Sind mehrere geeignete, getrennte Sitzungen verfügbar, wird eine dieser Sitzungen nach dem Zufallsprinzip gewählt. Wenn die Situation unter den gleichen Bedingungen erneut auftritt, wird die gleiche Sitzung gewählt. Ansonsten ist die Wahl nicht vorhersagbar.

Mit dem PowerShell-SDK können Sie die Anwendungssitzungsfreigabe für alle Anwendungen in einer Anwendungsgruppe deaktivieren oder eine Anwendungsgruppe mit deaktivierter Sitzungsfreigabe erstellen.

#### PowerShell-Cmdlet-Beispiele

Verwenden Sie zum Deaktivieren der Sitzungsfreigabe die Broker-PowerShell-Cmdlets New-BrokerApplicationGroup oder Set-BrokerApplicationGroup mit der Einstellung "False"für den Parameter -SessionSharingEnabled und der Einstellung "True"für den Parameter -SingleAppPerSession.

- Beispiel zum Erstellen einer Anwendungsgruppe mit deaktivierter Sitzungsfreigabe für alle enthaltenen Anwendungen:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Beispiel zum Deaktivieren der Sitzungsfreigabe für alle Anwendungen einer Anwendungsgruppe:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

#### Überlegungen

- Um die Eigenschaft `SingleAppPerSession` zu aktivieren, müssen Sie die Eigenschaft `SessionSharingEnabled` auf "False"festlegen. Die beiden Eigenschaften dürfen nicht gleichzeitig aktiviert werden. Der Parameter `SessionSharingEnabled` bezieht sich auf die Sitzungsfreigabe zwischen Anwendungsgruppen.
- Die Sitzungsfreigabe funktioniert nur bei Anwendungen, die Anwendungsgruppen aber keinen Bereitstellungsgruppen zugeordnet sind. Für alle direkt einer Bereitstellungsgruppe zugeordneten Anwendungen ist die Sitzungsfreigabe standardmäßig aktiviert.
- Wenn eine Anwendung mehreren Anwendungsgruppen zugewiesen ist, stellen Sie sicher, dass die Gruppen keine widersprüchlichen Einstellungen aufweisen. Ist die Option beispielsweise für eine Gruppe auf "True"und für eine andere auf "False"festgelegt, führt dies zu unvorhersehbarem Verhalten.

### Umbenennen von Anwendungsgruppen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe umbenennen**.
3. Geben Sie einen neuen eindeutigen Namen ein und wählen Sie **OK**.

### Hinzufügen und Entfernen von Bereitstellungsgruppenzuordnungen für Anwendungsgruppen und Ändern der Priorität von Gruppenzuordnungen

Eine Anwendungsgruppe kann Bereitstellungsgruppen zugeordnet werden, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten.

Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, wenn folgende Bedingungen erfüllt sind:

- Die Bereitstellungsgruppe enthält freigegebene Maschinen und wurde mit einer Version vor 7.9 erstellt.
- Sie haben die Berechtigung zum Bearbeiten der Bereitstellungsgruppe.

Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen"geändert, wenn für das Dialogfeld **Anwendungsgruppe bearbeiten** ein Commit ausgeführt wird.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Bereitstellungsgruppen**.
4. Wählen Sie zum Hinzufügen von Bereitstellungsgruppen **Hinzufügen**. Aktivieren Sie die Kontrollkästchen verfügbarer Bereitstellungsgruppen. (Nicht kompatible Bereitstellungsgruppen können nicht ausgewählt werden.) Wenn Sie fertig sind, wählen Sie **OK**.
5. Zum Entfernen von Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen der gewünschten Gruppen und wählen Sie **Entfernen**. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.
6. Zum Ändern der Priorität von Bereitstellungsgruppen aktivieren Sie das Kontrollkästchen einer Bereitstellungsgruppe und wählen Sie **Priorität bearbeiten**. Geben Sie die Priorität an (0=höchste) und wählen Sie **OK**.
7. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Hinzufügen und Entfernen von Tagbeschränkungen zu bzw. aus Anwendungsgruppen

Das Hinzufügen, Bearbeiten und Entfernen von Tagbeschränkungen kann unerwartete Auswirkungen darauf haben, welche Maschinen für den Anwendungsstart in Betracht gezogen werden. Lesen Sie die Informationen und Hinweise unter Tags.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Bereitstellungsgruppen**.
4. Zum Hinzufügen einer Tagbeschränkung wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus dem Menü aus.
5. Zum Ändern oder Entfernen einer Tagbeschränkung wählen Sie ein anderes Tag aus dem Menü oder entfernen Sie die Tagbeschränkung durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.
6. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Hinzufügen und Entfernen von Benutzern zu bzw. aus Anwendungsgruppen

Ausführliche Informationen zu Benutzern finden Sie unter Erstellen von Anwendungsgruppen.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Benutzer**. Geben Sie an, ob alle Benutzer oder nur bestimmte Benutzer und Gruppen in den zugeordneten Bereitstellungsgruppen Anwendungen in der Anwendungsgruppe verwenden können sollen. Zum Hinzufügen von Benutzern wählen Sie **Hinzufügen** und geben dann die gewünschten Benutzer an. Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und wählen dann **Entfernen**.
4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Hinzufügen, Ändern oder Entfernen eines Anwendungssymbols in einer Anwendungsgruppe

Führen Sie die folgenden Schritte aus, um ein Anwendungssymbol hinzuzufügen, zu ändern oder zu entfernen.

1. Wählen Sie im Navigationsbereich **Anwendungen**.
2. Wählen Sie auf der Registerkarte **Alle Anwendungen** eine Anwendung und dann **Eigenschaften**.

   Um Änderungen auf Anwendungsgruppenebene vorzunehmen, navigieren Sie zur Registerkarte **Anwendungsgruppen**, wählen Sie eine Anwendung in einer Gruppe aus und wählen Sie **Eigenschaften**.
3. Wählen Sie die Seite **Bereitstellung** und dann **Ändern**. Das Fenster **Symbol auswählen** wird angezeigt.
4. Führen Sie im Fenster **Symbol auswählen** einen der folgenden Schritte aus:

   - Um ein Symbol hinzuzufügen, wählen Sie **Hinzufügen** und navigieren dann zum Symbol.
   - Um ein Symbol zu entfernen, wählen Sie es aus und wählen dann **Entfernen**.
   - Um ein Symbol zu ändern, wählen Sie es für die Anwendung aus.

   > **Wichtig:**
   >
   > - Sie können kein Symbol hinzufügen, das größer als 200 KB ist.
   > - Sie können nur ICON-Dateien hinzufügen.
   > - Sie können keine integrierten Symbole entfernen.
   > - Sie können kein Symbol einer aktuell verwendeten Anwendung entfernen.
5. Wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### Ändern der Geltungsbereiche in Anwendungsgruppen

Sie können Geltungsbereiche nur dann ändern, wenn Sie einen Geltungsbereich erstellt haben. Den Geltungsbereich "Alle"können Sie nicht bearbeiten. Weitere Informationen finden Sie unter Delegierte Administration.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann in der Aktionsleiste auf **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Geltungsbereiche**. Aktivieren oder deaktivieren Sie das Kontrollkästchen neben den Geltungsbereichen, die Sie ändern möchten.

4. Wählen Sie **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Löschen von Anwendungsgruppen

Eine Anwendung muss mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe zugeordnet sein. Wenn durch das Löschen einer Anwendungsgruppe eine oder mehrere Anwendungen nicht mehr zu einer Gruppe gehören würden, wird eine Warnung angezeigt, dass mit dem Löschen der Gruppe auch diese Anwendungen gelöscht würden. Sie können den Löschvorgang dann bestätigen oder abbrechen.

Durch das Löschen einer Anwendung wird sie nicht aus ihrer ursprünglichen Quelle gelöscht. Wenn Sie sie jedoch wieder zur Verfügung stellen möchten, müssen Sie sie erneut hinzufügen.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Gruppe löschen**.
3. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.

### Anwendungsgruppen mit Ordnern organisieren

Sie können Ordner erstellen, um den Zugriff auf Anwendungsgruppen zu vereinfachen.

#### Erforderliche Rollen

Standardmäßig benötigen Sie zum Erstellen und Verwalten von Anwendungsgruppenordnern eine der folgenden integrierten Rollen:

- Cloudadministrator
- Volladministrator
- Administrator der Anwendungsgruppe

Sie können benutzerdefinierte Rollen erstellen, um Verwaltungsaktionen an andere Benutzer zu delegieren. In der folgenden Tabelle sind die für jede Aktion erforderlichen Berechtigungen aufgeführt.

| Aktion | Erforderliche Berechtigungen |
|---|---|
| Anwendungsgruppenordner erstellen | Anwendungsgruppenordner erstellen |

| Aktion | Erforderliche Berechtigungen |
| --- | --- |
| Anwendungsgruppenordner löschen | Anwendungsgruppenordner entfernen |
| Anwendungsgruppenordner verschieben | Anwendungsgruppenordner verschieben |
| Anwendungsgruppenordner umbenennen | Anwendungsgruppenordner bearbeiten |
| Anwendungsgruppen in Ordner verschieben | Anwendungsgruppenordner bearbeiten, Anwendungsgruppeneigenschaften bearbeiten |

Weitere Informationen finden Sie unter Erstellen und Verwalten von Rollen.

#### Ordner erstellen und verwalten

Sie können Anwendungsgruppenordner mit der Aktionsleiste oder dem Rechtsklickmenü erstellen und verwalten. Darüber hinaus können Sie eine Anwendungsgruppe oder einen Ordner an die gewünschte Stelle in der Ordnerstruktur ziehen.

Nützliche Info:

- Sie können Ordner bis zu fünf Ebenen tief verschachteln (mit Ausnahme des Standardstammordners).
- Ein Ordner kann Anwendungsgruppen und Unterordner enthalten. Sie können einen Ordner nur dann löschen, wenn er und seine Unterordner keine Anwendungsgruppen enthalten.
- Alle Ressourcen in "Vollständige Konfiguration"(z. B. Maschinenkataloge, Bereitstellungsgruppen, Anwendungen und Anwendungsgruppen) nutzen dieselbe Ordnerstruktur im Back-End. Um Namenskonflikte mit anderen Ressourcenordnern beim Umbenennen oder Verschieben von Ordnern zu vermeiden, empfehlen wir, Ordner der ersten Ebene in verschiedenen Ordnerstrukturen unterschiedlich zu benennen.

## Remote-PC-Zugriff

August 30, 2023

> **Hinweis:**
>
> In diesem Artikel wird beschrieben, wie Sie Remote-PC-Zugriff mit der Schnittstelle "Vollständige Konfiguration"konfigurieren. Wenn Sie Quick Deploy verwenden, folgen Sie den Anweisungen unter Remote-PC-Zugriff in Quick Deploy.

Remote-PC-Zugriff ist eine Funktion von Citrix Virtual Apps and Desktops, mit der Organisationen ihren Mitarbeitern einfach und sicher Zugriff auf Unternehmensressourcen geben können. Die Citrix-Plattform ermöglicht diesen sicheren Zugriff, indem Benutzer Zugriff auf ihre physischen Büro-PCs erhalten. Wenn Benutzer auf ihre Büro-PCs zugreifen können, können sie auf alle Anwendungen, Daten und Ressourcen zugreifen, die sie für ihre Arbeit benötigen. Mit Remote-PC-Zugriff ist das Einführen und Bereitstellen anderer Tools für die Telearbeit überflüssig. Zum Beispiel virtuelle Desktops oder Anwendungen und die zugehörige Infrastruktur.

Remote-PC-Zugriff verwendet dieselben Citrix Virtual Apps and Desktops-Komponenten zum Bereitstellen von virtuellen Desktops und Anwendungen. Daher sind die Anforderungen und der Prozess für die Bereitstellung und Konfiguration des Remote-PC-Zugriffs die gleichen wie für die Bereitstellung von virtuellen Ressourcen mit Citrix Virtual Apps and Desktops. Diese Einheitlichkeit bietet eine konsistente und gemeinsame administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Sitzungen verwenden.

Das Feature besteht aus einem Maschinenkatalog vom Typ **Remote-PC-Zugriff**, der folgende Funktionalität bietet:

- Möglichkeit, Maschinen durch Angeben von Organisationseinheiten hinzuzufügen. Diese Fähigkeit erleichtert das Hinzufügen von PCs in großen Mengen.
- Möglichkeit, Maschinen mithilfe von CSV-Dateien hinzuzufügen. Diese Fähigkeit ermöglicht das Massenhinzufügen von PCs in Szenarios mit Einschränkungen der Organisationseinheitsstruktur.
- Automatische Benutzerzuweisung basierend auf dem Benutzer, der sich am Windows-PC im Büro anmeldet. Wir unterstützen Einzel- und Mehrbenutzerzuweisungen. Standardmäßig weist Citrix DaaS der nächsten nicht zugewiesenen Maschine automatisch mehrere Benutzer zu. Um die automatische Zuweisung auf einen einzelnen Benutzer zu beschränken, gehen Sie zu **Vollständige Konfiguration > Einstellungen** und deaktivieren Sie die Einstellung **Automatische Zuweisung mehrerer Benutzer für Remote-PC-Zugriff aktivieren**.

Citrix Virtual Apps and Desktops weitere Anwendungsfälle für physische PCs über andere Arten von Maschinenkatalogen abdecken. Anwendungsfälle sind unter anderen:

- Physische Linux-PCs
- Gepoolte physische PCs (d. h. zufällig zugewiesen, nicht dediziert)

> **Hinweise:**
>
> Weitere Informationen zu den unterstützten Betriebssystemversionen finden Sie unter Systemanforderungen für den Einzelsitzungs-OS-VDA und Linux VDA.
>
> Bei On-Premises-Bereitstellungen gilt Remote-PC-Zugriff nur für Citrix DaaS Advanced- und Premium-Lizenzen. Sitzungen verbrauchen Lizenzen genau wie andere Citrix Virtual Desktops-

> Sitzungen. Bei Citrix Cloud gilt Remote-PC-Zugriff für Citrix DaaS und Workspace Premium Plus.

## Überlegungen

Während alle technischen Anforderungen und Überlegungen, die allgemein für Citrix Virtual Apps and Desktops und Citrix DaaS gelten, auch für Remote-PC-Zugriff zutreffen, sind einige möglicherweise relevanter oder gelten exklusiv für den Anwendungsfall physischer PCs.

> **Wichtig:**
>
> Physische Windows 11-Systeme (und einige, auf denen Windows 10 ausgeführt wird) verfügen über virtualisierungsbasierte Sicherheitsfeatures, die dazu führen, dass die VDA-Software sie fälschlicherweise als virtuelle Maschinen erkennt. Um dieses Problem zu beheben, haben Sie die folgenden Optionen:
>
> - Verwenden Sie die Option "/physicalmachine"zusammen mit der Option "/remotepc"in der VDA-Befehlszeileninstallation.
> - Fügen Sie nach der Installation des VDA den folgenden Registrierungswert hinzu, falls die oben genannte Option nicht verwendet wurde.
>   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
>   - Name: ForceEnableRemotePC
>   - Typ: DWORD
>   - Daten: 1

## Überlegungen zur Bereitstellung

Beim Planen der Bereitstellung des Remote-PC-Zugriffs treffen Sie einige allgemeine Entscheidungen.

- Sie können den Remote-PC-Zugriff zu einer vorhandenen Bereitstellung von Citrix Virtual Apps and Desktops und Citrix DaaS hinzufügen. Bevor Sie diese Option wählen, sollten Sie Folgendes bedenken:
  - Sind die aktuellen Delivery Controller oder Cloud Connectors entsprechend groß, um die zusätzliche Last zu unterstützen, die durch die Remote-PC-Zugriff-VDAs verursacht wird?
  - Sind die On-Premises-Sitekonfigurationsdatenbanken und Datenbankserver entsprechend groß, um die zusätzliche Last zu unterstützen, die durch die Remote-PC-Zugriff-VDAs verursacht wird?
  - Übersteigen die vorhandenen VDAs und die neuen VDAs für Remote-PC-Zugriff die Anzahl der maximal unterstützten VDAs pro Site?

- Sie müssen den VDA über einen automatisierten Prozess auf Büro-PCs bereitstellen. Die folgenden Optionen sind verfügbar:
  - ESD-Tools (Electronic Software Distribution) wie z. B. SCCM: Installieren von VDAs mit SCCM.
  - Bereitstellungsskripts: Installieren von VDAs mit Skripts.
- Lesen Sie die Sicherheitsüberlegungen für Remote-PC-Zugriff.

### Überlegungen zum Maschinenkatalog

Die Art des erforderlichen Maschinenkatalogs hängt vom Anwendungsfall ab:

- Maschinenkatalog für Remote-PC-Zugriff
  - Dedizierte Windows-/Linux-PCs
  - Dedizierte Windows-/Linux-PCs mit mehreren Benutzern. Dieser Anwendungsfall gilt für physische PCs im Büro, auf die mehrere Benutzer in verschiedenen Schichten remote zugreifen können.
  - Gepoolte Windows-/Linux-PCs. Dieser Anwendungsfall betrifft physische PCs, auf die mehrere beliebige Benutzer zugreifen können (z. B. in Computerräumen).

Wenn Sie den Typ des Maschinenkatalogs identifiziert haben, sollten Sie Folgendes beachten:

- Eine Maschine kann nur jeweils einem Maschinenkatalog zugewiesen sein.
- Um die delegierte Administration zu erleichtern, sollten Sie Maschinenkataloge auf der Grundlage des geografischen Standorts, der Abteilung oder einer anderen Gruppierung erstellen, die die Delegierung der Verwaltung jedes Katalogs an die entsprechenden Administratoren erleichtert.
- Wählen Sie bei der Auswahl der Organisationseinheit, in der die Maschinenkonten sind, Organisationseinheiten auf einer niedrigeren Ebene aus, um eine größere Granularität zu erzielen. Wenn eine solche Granularität nicht erforderlich ist, können Sie übergeordnete Organisationseinheiten auswählen. Wählen Sie beispielsweise im Fall von Bank/Bankbeamte/Kassierer die Option **Kassierer** aus, um eine größere Granularität zu erzielen. Sonst können Sie **Bankbeamte** oder **Bank** wählen, je nach Anforderung.
- Das Verschieben oder Löschen von Organisationseinheiten nachdem sie einem Remote-PC-Zugriffs-Maschinenkatalog zugewiesen wurden, wirkt sich auf VDA-Zuordnungen aus und verursacht Probleme mit zukünftigen Zuweisungen. Daher sollten Sie Zuweisungsupdates von Organisationseinheiten für Maschinenkataloge bei der Active Directory-Änderungsplanung berücksichtigen.
- Sie können Organisationseinheiten auswählen, um Maschinen in Massen zum Maschinenkatalog hinzuzufügen. In einigen Szenarios wird dies durch Einschränkungen der Organisationseinheitsstruktur erschwert. Sie können dann CSV-Dateien zum Massenhinzufügen von Maschinen

verwenden. Dieses Feature bietet Ihnen mehr Flexibilität beim Massenhinzufügen von Maschinen. Sie können entweder nur Maschinen hinzufügen (zur Verwendung mit automatischen Benutzerzuweisungen) oder Maschinen und Benutzerzuweisungen gemeinsam hinzufügen.
- Integriertes Wake-On-LAN ist nur mit einem Maschinenkatalog des Typs **Remote-PC-Zugriff** verfügbar.

### Linux-VDA-Überlegungen

Diese Überlegungen gelten speziell für den Linux-VDA:

- Das Ausblenden physischer Monitore für VDAs mit Remote-PC-Zugriff ist verfügbar, jedoch nicht für alle Linux-Distributionen. Verwenden Sie für nicht unterstützte Linux-Distributionen den Linux VDA auf physischen Maschinen nur im Nicht-3D-Modus. Ansonsten kann es vorkommen, dass aufgrund von Einschränkungen des NVIDIA-Treibers der lokale PC-Bildschirm nicht ausgeblendet wird und die Sitzungsaktivitäten anzeigt, wenn der HDX 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms ist ein Sicherheitsrisiko.
- Citrix empfiehlt für physische Linux-Maschinen die Verwendung von Maschinenkatalogen des Typs “Einzelsitzungs-OS”.

### Technische Anforderungen und Überlegungen

Dieser Abschnitt enthält die technischen Anforderungen und Überlegungen für physische PCs.

- Folgendes wird nicht unterstützt:
  - KVM-Switches oder andere Komponenten, die eine Sitzung trennen.
  - Hybrid-PCs, einschließlich All-in-One- und NVIDIA Optimus-Laptops und -PCs.
  - Dual-Boot-Maschinen.
- Schließen Sie Tastatur und Maus direkt an den PC an. Beim Anschließen an den Monitor oder an andere Komponenten, die ausgeschaltet oder getrennt werden können, sind diese Peripheriegeräte dann möglicherweise nicht mehr verfügbar. Wenn Sie Eingabegeräte an Komponenten wie beispielsweise Bildschirme anschließen müssen, schalten Sie diese Komponenten nicht aus.
- Die PCs müssen zu einer Active Directory-Domänendienste-Domäne gehören.
- Secure Boot wird nur unter Windows 10 unterstützt.
- Der PC muss eine aktive Netzwerkverbindung haben. Eine Kabelverbindung wird für eine höhere Zuverlässigkeit und Bandbreite bevorzugt.
- Bei WLAN-Verbindungen gehen Sie wie folgt vor:

1. Legen Sie die Energieeinstellungen so fest, dass der WLAN-Adapter eingeschaltet bleibt.
2. Konfigurieren Sie den WLAN-Adapter und das Netzwerkprofil so, dass die automatische Verbindung mit dem WLAN-Netzwerk vor der Benutzeranmeldung zulässig ist. Sonst wird der VDA erst registriert, wenn sich der Benutzer anmeldet. Der PC ist erst für den Remotezugriff verfügbar, wenn ein Benutzer sich angemeldet hat.
3. Stellen Sie sicher, dass die Delivery Controller oder Cloud Connectors im Wi-Fi-Netzwerk erreichbar sind.

- Remote-PC-Zugriff kann auf Laptops verwendet werden. Stellen Sie sicher, dass der Laptop an eine Stromquelle angeschlossen ist, anstatt mit dem Akku zu arbeiten. Konfigurieren Sie die Energieoptionen von Laptops wie bei Desktop-PCs. Beispiel:

  1. Deaktivieren Sie den Ruhezustand.
  2. Deaktivieren Sie den Energiesparmodus.
  3. Legen Sie die Aktion beim Schließen des Deckels auf **Nichts tun** fest.
  4. Legen Sie die Aktion bei Betätigen der Ein-/Ausschalttaste auf **Herunterfahren** fest.
  5. Deaktivieren Sie die Energiesparfunktionen der Netzwerk- und der Grafikkarte.

- Remote-PC-Zugriff wird auf Surface Pro-Geräten mit Windows 10 unterstützt. Folgen Sie den gleichen Richtlinien für Laptops, die zuvor erwähnt wurden.

- Wenn Sie eine Dockingstation verwenden, können Sie Laptops abdocken und neu andocken. Wenn Sie einen Laptop abdocken, registriert sich der VDA bei Delivery Controllern bzw. Cloud Connectors neu über das Wi-Fi-Netzwerk. Wenn Sie den Laptop neu andocken, wechselt der VDA allerdings nicht zur Kabelverbindung, es sei denn, Sie trennen den WLAN-Adapter vom Netzwerk. Bei einigen Geräten sorgt eine integrierte Funktion für die Trennung des WLAN-Adapters beim Herstellen einer Kabelverbindung. Bei anderen ist eine benutzerdefinierte Lösung oder ein Hilfsprogramm eines Drittanbieters erforderlich. Konsultieren Sie in diesem Zusammenhang die zuvor erwähnten Wi-Fi-Überlegungen.

  Zum Aktivieren des An- und Abdockens von Remote-PC-Zugriff-Geräten führen Sie folgende Schritte aus:

  1. Wählen Sie im Menü **Start** die Option **Einstellungen > System > Netzbetrieb und Standbymodus** und legen Sie für **Standbymodus** die Einstellung **Nie** fest.
  2. Rufen Sie unter **Geräte-Manager > Netzwerkadapter > Ethernet-Adapter** den Bereich **Energieverwaltung** auf und deaktivieren Sie **Computer kann das Gerät ausschalten, um Energie zu sparen**. Stellen Sie sicher, dass **Gerät kann den Computer aus dem Ruhezustand aktivieren** aktiviert ist.

- Mehrere Benutzer mit Zugriff auf denselben Büro-PC sehen in Citrix Workspace dasselbe Symbol. Wenn sich ein Benutzer bei Citrix Workspace anmeldet, wird diese Ressource als nicht verfügbar angezeigt, wenn sie bereits von einem anderen Benutzer verwendet wird.

- Installieren Sie die Citrix Workspace-App auf jedem Clientgerät (z. B. einem Heim-PC), das auf den Büro-PC zugreift.

### Konfigurationssequenz

Dieser Abschnitt enthält eine Übersicht über das Konfigurieren des Remote-PC-Zugriffs, wenn Sie einen Maschinenkatalog des Typs **Remote-PC-Zugriff** verwenden. Weitere Informationen zum Erstellen anderer Arten von Maschinenkatalogen finden Sie unter Erstellen von Maschinenkatalogen.

1. Nur On-Premises-Site - Um die integrierte Wake-On-LAN-Funktion zu verwenden, konfigurieren Sie die unter Wake-On-LAN beschriebenen Voraussetzungen.
2. Wenn eine neue Citrix Virtual Apps and Desktops-Site für Remote-PC-Zugriff erstellt wurde:

   a) Wählen Sie als Sitetyp **Remote-PC-Zugriff**.
   b) Auf der Seite **Energieverwaltung** aktivieren oder deaktivieren Sie die Energieverwaltung für den Standardmaschinenkatalog für Remote-PC-Zugriff. Sie können diese Einstellung später ändern, indem Sie die Eigenschaften des Maschinenkatalogs bearbeiten. Weitere Informationen zur Konfiguration von Wake-On-LAN finden Sie unter Wake-On-LAN.
   c) Füllen Sie die Seiten **Benutzer** und **Maschinenkonten** aus.

   Mit diesen Schritten werden automatisch ein Maschinenkatalog **Remote-PC-Zugriff-Maschinen** und eine Bereitstellungsgruppe **Remote-PC-Zugriff-Desktops** erstellt.
3. Wenn eine vorhandene Citrix Virtual Apps and Desktops-Site erweitert wird:

   a) Erstellen Sie einen Maschinenkatalog vom Typ **Remote-PC-Zugriff** (im Assistenten auf der Seite "Betriebssystem"). Weitere Informationen zum Erstellen eines Maschinenkatalogs finden Sie unter Erstellen von Maschinenkatalogen. Stellen Sie sicher, dass Sie die richtige Organisationseinheit zuweisen, damit die Ziel-PCs für die Verwendung mit Remote-PC-Zugriff verfügbar sind.
   b) Erstellen Sie eine Bereitstellungsgruppe, um Benutzern Zugriff auf die PCs im Maschinenkatalog zu gewähren. Weitere Informationen zum Erstellen einer Bereitstellungsgruppe finden Sie unter Erstellen von Bereitstellungsgruppen. Stellen Sie sicher, dass Sie die Bereitstellungsgruppe einer Active Directory-Gruppe zuweisen, in der die Benutzer, die Zugriff auf ihre PCs benötigen, enthalten sind.
4. Stellen Sie den VDA auf den Büro-PCs bereit.

   - Wir empfehlen die Verwendung des Kernkomponenten-VDA-Installationsprogramms für Einzelsitzungs-OS (`VDAWorkstationCoreSetup.exe`).
   - Sie können auch das vollständige VDA-Installationsprogramm für Einzelsitzungs-OS (`VDAWorkstationSetup.exe`) mit der Option `/remotepc /physicalmachine`

verwenden. Dadurch wird das gleiche Ergebnis wie mit dem Kernkomponenten-VDA-Installationsprogramm erzielt.

- Erwägen Sie, die Windows-Remoteunterstützung zu aktivieren, damit Helpdeskteams Remotesupport über Citrix Director bereitstellen können. Verwenden Sie dazu die Option `/enable_remote_assistance`. Weitere Informationen finden Sie unter Installieren über die Befehlszeile.
- Um Informationen zur Anmeldedauer in Director anzuzeigen, müssen Sie das vollständige VDA-Installationsprogramm für Einzelsitzungs-OS verwenden und die Komponente **Citrix User Profile Management WMI Plug-In** installieren. Schließen Sie diese Komponente mit der Option `/includeadditional` ein. Weitere Informationen finden Sie unter Installieren über die Befehlszeile.
- Informationen zum Bereitstellen des VDA mit SCCM finden Sie unter Installieren von VDAs mit SCCM.
- Informationen zum Bereitstellen des VDA über Bereitstellungsskripts finden Sie unter Installieren von VDAs mit Skripts.

Nachdem Sie die Schritte 2 bis 4 erfolgreich abgeschlossen haben, werden Benutzer automatisch ihren eigenen Computern zugewiesen, wenn sie sich lokal an den PCs anmelden.

5. Weisen Sie die Benutzer an, auf jedem Clientgerät, das sie für den Remotezugriff auf den Büro-PC verwenden, die Citrix Workspace-App herunterzuladen und zu installieren. Die Citrix Workspace-App ist auf der Citrix-Downloadsite und in den Anwendungsstores für unterstützte Mobilgeräte verfügbar.

## Über die Registrierung verwaltete Features

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### Energiesparmodus (mindestens Version 7.16)

Damit eine Maschine mit Remote-PC-Zugriff in den Energiesparmodus wechseln kann, fügen Sie dem VDA folgende Registrierungseinstellung hinzu und starten die Maschine dann neu. Nach dem Neustart gelten die Energiespareinstellungen des Betriebssystems. Nach Ablauf der konfigurierten Leerlaufzeit

wechselt die Maschine dann in den Energiesparmodus. Wenn die Maschine wieder reaktiviert wird, registriert sie sich erneut beim Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: DisableRemotePCSleepPreventer
- Typ: DWORD
- Wert: 1

**Sitzungsverwaltung**

Standardmäßig wird eine Remotesitzung des Benutzers automatisch getrennt, wenn ein lokaler Benutzer eine Sitzung auf dieser Maschine (durch Drücken von Strg + Alt + Entf) initiiert. Fügen Sie den folgenden Registrierungseintrag auf dem Büro-PC hinzu und starten Sie dann die Maschine neu, um diese automatische Aktion zu verhindern.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: SasNotification
- Typ: DWORD
- Wert: 1

Standardmäßig erhält der Remotebenutzer Vorzug vor dem lokalen Benutzer, wenn die Verbindungsmeldung nicht innerhalb des Timeouts quittiert wird. Verwenden Sie die folgende Einstellung, um das Verhalten zu konfigurieren:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaMode
- Typ: DWORD
- Wert:
  - 1 = Remotebenutzer wird stets bevorzugt, wenn er nicht innerhalb des Timeouts auf die Meldung reagiert. Dies ist das Standardverhalten bei nicht konfigurierter Einstellung.
  - 2 - Lokaler Benutzer wird bevorzugt.

Das Standardtimeout zum Erzwingen des Remote-PC-Zugriffsmodus liegt bei 30 Sekunden. Sie können dieses Zeitlimit konfigurieren, aber keinen Wert unter 30 Sekunden wählen. Verwenden Sie diese Registrierungseinstellung, um das Zeitlimit zu konfigurieren.

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaTimeout
- Typ: DWORD
- Wert: Anzahl der Sekunden für Timeout als Dezimalwert

Wenn ein Benutzer den Zugriff auf die Konsole erzwingen möchte, kann der lokale Benutzer innerhalb von 10 Sekunden zwei Mal Strg + Alt + Entf drücken, um lokal auf die Remotesitzung zuzugreifen und eine Verbindungstrennung zu erzwingen.

Wenn ein lokaler Benutzer nach der Registrierungsänderung und dem Maschinenneustart für die Anmeldung am PC Strg + Alt + Entf drückt und die Maschine von einem Remotebenutzer verwendet wird, wird dem Remotebenutzer eine Bestätigungsaufforderung angezeigt. Die Aufforderung fragt, ob die Verbindung des lokalen Benutzers zugelassen oder verweigert werden soll. Bei der Zulassung der Verbindung wird die Sitzung des Remotebenutzers getrennt.

### Wake-On-LAN

Remote-PC-Zugriff unterstützt Wake-On-LAN, sodass physische PCs remote eingeschaltet werden können. Dieses Feature ermöglicht es Benutzern, ihre Büro-PCs ausgeschaltet zu lassen, wenn diese nicht verwendet werden, um Energiekosten zu sparen. Außerdem ist ein Remotezugriff möglich, wenn Maschinen unabsichtlich ausgeschaltet wurden.

Mit dem Wake-On-LAN-Feature werden die Magic Packets auf Befehl des Delivery Controllers direkt vom VDA, der auf dem PC ausgeführt wird, an das Subnetz gesendet, in dem sich der PC befindet. Dadurch kann das Feature ohne Abhängigkeiten von zusätzlichen Infrastrukturkomponenten oder Drittanbieterlösungen für die Bereitstellung von Magic Packets funktionieren.

Das Wake-On-LAN-Feature unterscheidet sich vom älteren SCCM-basierten Wake-On-LAN-Feature. SCCM-integriertes Wake-On-LAN ist eine Wake-On-LAN-Alternative für Remote-PC-Zugriff, die nur mit on-premises Citrix Virtual Apps and Desktops verfügbar ist. Weitere Informationen zu SCCM-basiertem Wake-on-LAN finden Sie unter Wake-On-LAN –SCCM-integriert.

#### Systemanforderungen

Folgende Systemanforderungen gelten für die Verwendung des Wake-On-LAN-Feature:

- Steuerungsebene:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 oder höher
- Physische PCs:
  - VDA Version 2009 oder höher
  - Windows 10 oder Windows 11. Weitere Informationen zur Unterstützbarkeit finden Sie unter VDA-Systemanforderungen.
  - Wake-On-LAN aktiviert in BIOS/UEFI
  - Wake-On-LAN aktiviert in den Eigenschaften des Netzwerkadapters innerhalb der Windows-Konfiguration

**Konfigurieren von Wake-On-LAN**

Für das Konfigurieren von Wake-On-LAN können Sie die Verwaltungsoberfläche "Vollständige Konfiguration"oder PowerShell verwenden.

**Konfigurieren von Wake-On-LAN in der Oberfläche "Vollständige Konfiguration"** Erstellen der Wake-On-LAN-Verbindung:

1. Gehen Sie zum Knoten **Hosting** links.
2. Wählen Sie **Verbindung und Ressourcen hinzufügen**.
3. Geben Sie auf der Seite **Verbindung** des Assistenten Folgendes an:

    a) Verbindungsart: Remote-PC-Wake-On-LAN
    b) Zonenname: Wählen Sie die Zone, in der sich der Remote-PC-Zugriffs-Katalog befindet.
    c) Verbindungsname: Geben Sie einen Namen für die Wake-On-LAN-Verbindung ein.

4. Führen Sie im Assistenten "Verbindung und Ressourcen hinzufügen"die verbleibenden Schritte aus.

Gehen Sie zum Hinzufügen der Wake-on-LAN-Verbindung zu einem Remote-PC-Zugriffs-Maschinenkatalog folgendermaßen vor:

1. Beim Erstellen eines neuen Maschinenkatalogs für Remote-PC-Zugriff können Sie die Verbindung über die Dropdownliste auf der Seite **Maschinentyp** des Assistenten zum Erstellen von Maschinenkatalogen hinzufügen.
2. Zum Hinzufügen der Wake-on-LAN-Verbindung zu einem bestehenden Maschinenkatalog gehen Sie folgendermaßen vor:

    a) Gehen Sie zum Knoten **Maschinenkataloge** links.
    b) Wählen Sie den Remote-PC-Zugriff-Maschinenkatalog.
    c) Klicken Sie mit der rechten Maustaste auf den Maschinenkatalog oder wählen Sie oben das Menü **Mehr**.
    d) Wählen Sie **Maschinenkatalog bearbeiten**.
    e) Wählen Sie auf der Seite **Energieverwaltung** die Option **Ja**.
    f) Wählen Sie die entsprechende Verbindung aus der Dropdownliste aus.
    g) Wählen Sie **Speichern**.

> **Hinweis:**
>
> Die Konfiguration von Wake-on-LAN über die Oberfläche "Vollständige Konfiguration"ist derzeit nur unter Citrix DaaS verfügbar.

**Konfigurieren von Wake-On-LAN über PowerShell** Konfigurieren von Wake-On-LAN über PowerShell:

1. Erstellen Sie den Maschinenkatalog für den Remote-PC-Zugriff (falls noch nicht vorhanden).
2. Erstellen Sie die Wake-On-LAN-Hostverbindung (falls noch nicht vorhanden).
3. Rufen Sie den eindeutigen Bezeichner der Wake-On-LAN-Hostverbindung ab.
4. Ordnen Sie die Wake-On-LAN-Hostverbindung einem Maschinenkatalog zu.

Erstellen der Wake-On-LAN-Hostverbindung:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
        $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

Wenn die Hostverbindung bereit ist, führen Sie die folgenden Befehle aus, um den eindeutigen Bezeichner der Hostverbindung abzurufen:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Nachdem Sie den eindeutigen Bezeichner der Verbindung abgerufen haben, führen Sie die folgenden Befehle aus, um die Verbindung dem Remote-PC-Zugriff-Maschinenkatalog zuzuordnen:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

### Designüberlegungen

Wenn Sie planen, Wake-On-LAN mit Remote-PC-Zugriff zu verwenden, sollten Sie Folgendes beachten:

- Mehrere Maschinenkataloge können dieselbe Wake-On-LAN-Hostverbindung verwenden.
- Damit ein PC einen anderen PC reaktivieren kann, müssen beide PCs sich im gleichen Subnetz befinden und dieselbe Wake-On-LAN-Hostverbindung verwenden. Die PCs können sich im gleichen oder in unterschiedlichen Maschinenkatalogen befinden.
- Hostverbindungen werden bestimmten Zonen zugewiesen. Wenn Ihre Bereitstellung mehr als eine Zone enthält, benötigen Sie in jeder Zone eine Wake-On-LAN-Hostverbindung. Gleiches gilt für Maschinenkataloge.
- Magic Packets werden mit der globalen Broadcast-Adresse 255.255.255.255 übertragen. Stellen Sie sicher, dass diese Adresse nicht blockiert ist.
- Um Maschinen in einem Subnetz zu reaktivieren, muss in diesem Subnetz (für jede Wake-On-LAN-Verbindung) mindestens ein PC aktiviert sein.

### Operative Überlegungen

Berücksichtigen Sie Folgendes bei der Verwendung des Wake-On-LAN-Features:

- Der VDA muss sich mindestens einmal registrieren, bevor der PC über die integrierte Wake-On-LAN-Funktion reaktiviert werden kann.
- Wake-on-LAN kann nur zum Reaktivieren von PCs verwendet werden. Andere Energieaktionen wie Neustart oder Herunterfahren werden nicht unterstützt.
- Es gibt zwei Situationen, in denen ein Magic Packet gesendet wird:
    1. Ein Benutzer versucht, eine Sitzung auf dem PC zu starten und der VDA ist nicht registriert.
    2. Ein Administrator sendet manuell einen Einschaltbefehl über die Oberfläche “Vollständige Konfiguration”oder PowerShell.
- Da der Delivery Controller den Energiezustand eines PCs nicht kennt, wird in der Oberfläche “Vollständige Konfiguration”unter “Energiezustand”**Nicht unterstützt** angezeigt. Der Delivery Controller ermittelt anhand des VDAs -Registrierungsstatus, ob ein PC ein- oder ausgeschaltet ist.

## Problembehandlung

### Abblenden des Monitors funktioniert nicht

Wenn der lokale Monitor des Windows-PCs während einer aktiven HDX-Sitzung nicht leer ist (der lokale Monitor zeigt an, was in der Sitzung passiert), ist dies wahrscheinlich auf Probleme mit dem Treiber des GPU-Herstellers zurückzuführen. Um das Problem zu beheben, geben Sie dem Citrix Indirect Display-Treiber (IDD) höhere Priorität als der Grafikkartentreiber des Herstellers, indem Sie den folgenden Registrierungswert festlegen:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Name: CitrixIDD
- Typ: DWORD
- Wert: 3

Weitere Informationen zu Anzeigeadapterprioritäten und Monitorerstellung finden Sie im Knowledge Center-Artikel CTX237608.

### Die Sitzung wird getrennt, wenn Sie Strg+Alt+Entf auf der Maschine drücken, auf der die Sitzungsverwaltungsbenachrichtigung aktiviert ist

Die vom Registrierungswert **SasNotification** gesteuerte Sitzungsverwaltungsbenachrichtigung funktioniert nur, wenn der Remote-PC-Zugriffsmodus auf dem VDA aktiviert ist. Wenn auf dem physischen PC die Hyper-V-Rolle oder virtualisierungsbasierte Sicherheitsfeatures aktiviert sind, wird der PC als virtuelle Maschine gemeldet. Wenn der VDA erkennt, dass er auf einer virtuellen Maschine ausgeführt wird, deaktiviert er automatisch den Remote-PC-Zugriff-Modus. Um den Remote-PC-Zugriff-Modus zu aktivieren, fügen Sie folgenden Registrierungswert hinzu:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Typ: DWORD
- Wert: 1

Starten Sie den PC neu, damit die Einstellung wirksam wird.

### Diagnoseinformationen

Diagnoseinformationen zu Remote-PC-Zugriff werden in das Windows-Anwendungsereignisprotokoll geschrieben. Informationsmeldungen werden nicht eingeschränkt. Fehlermeldungen werden durch Löschen doppelter Nachrichten eingeschränkt.

- 3300 (Informationsmeldung): Maschine zum Katalog hinzugefügt
- 3301 (Informationsmeldung): Maschine der Bereitstellungsgruppe hinzugefügt
- 3302 (Informationsmeldung): Maschine dem Benutzer zugewiesen
- 3303 (Fehler): Ausnahme

#### Energieverwaltung

Wenn die Energieverwaltung für Remote-PC-Zugriff aktiviert ist, können Maschinen, die sich in einem anderen Subnetz als der Controller befinden, ggf. nicht per subnetzgesteuertes Broadcast gestartet werden. Wenn Sie eine subnetzübergreifende Energieverwaltung mit subnetzgesteuertem Broadcast benötigen und AMT nicht unterstützt wird, versuchen Sie es mit dem Aktivierungsproxy oder Unicast. Stellen Sie sicher, dass diese Einstellungen in den erweiterten Eigenschaften der Energieverwaltungsverbindung aktiviert sind.

#### Aktive Remotesitzung zeichnet lokale Touchscreeneingabe auf

Wenn der VDA den Remote-PC-Zugriff-Modus aktiviert, ignoriert die Maschine die lokale Touchscreeneingabe während einer aktiven Sitzung. Wenn auf dem physischen PC die Hyper-V-Rolle oder virtualisierungsbasierte Sicherheitsfeatures aktiviert sind, wird der PC als virtuelle Maschine gemeldet. Wenn der VDA erkennt, dass er auf einer virtuellen Maschine ausgeführt wird, deaktiviert er automatisch den Remote-PC-Zugriff-Modus. Um den Remote-PC-Zugriff-Modus zu aktivieren, fügen Sie die folgende Registrierungseinstellung hinzu:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Typ: DWORD
- Wert: 1

Starten Sie den PC neu, damit die Einstellung wirksam wird.

### Weitere Ressourcen

Im Folgenden finden Sie weitere Ressourcen für Remote-PC-Zugriff:

- Solution design guidance: Remote PC Access Design Decisions.
- Remote-PC-Zugriff-Musterarchitekturen: Referenzarchitektur für Citrix Remote-PC-Zugriff-Lösung.

# Entfernen von Komponenten

August 30, 2023

Zum Entfernen von Komponenten, die Sie installiert haben (z. B. VDAs), empfiehlt Citrix die Verwendung der Windows-Funktion zum Entfernen oder Ändern von Programmen. Alternativ können Sie Komponenten über die Befehlszeile oder mit einem Skript entfernen.

Beim Entfernen von Komponenten werden keine Voraussetzungen entfernt und keine Firewalleinstellungen geändert.

Nach dem Entfernen eines VDAs wird die Maschine in der Standardeinstellung automatisch neu gestartet.

## Entfernen von Komponenten mit der Windows-Funktion zum Entfernen oder Ändern von Programmen

Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:

- Klicken Sie zum Entfernen eines VDAs auf**Citrix Virtual Delivery Agent**<*Version*>, klicken Sie mit der rechten Maustaste und wählen Sie **Deinstallieren**. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren.
- Zum Entfernen des universellen Druckservers wählen Sie **Citrix Universeller Druckserver**, klicken Sie mit der rechten Maustaste und wählen Sie **Deinstallieren**.

## Entfernen eines VDAs über die Befehlszeile

Führen Sie den Befehl aus, mit dem der VDA installiert wurde: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` oder `VDAWorkstationCoreSetup.exe`. Syntaxbeschreibungen finden Sie unter Installieren über die Befehlszeile.

- Um nur den VDA oder nur die Citrix Workspace-App zu entfernen, verwenden Sie die Optionen `/remove` und `/components`.
- Um den VDA und die Citrix Workspace-App zu entfernen, verwenden Sie die Option `/removeall`.

Mit dem folgenden Befehl werden beispielsweise der VDA und die Citrix Workspace-App von einer Multisitzungs-OS-Maschine entfernt.

```
VDAServerSetup.exe /removeall
```

Mit dem folgenden Befehl werden beispielsweise der VDA, aber nicht die Citrix Workspace-App für Windows (falls installiert) von einer Einzelsitzungs-OS-Maschine entfernt.

```
VDAWorkstationSetup.exe /remove /components vda
```

Sie können einen VDA auch mit einem von Citrix bereitgestellten Skripts entfernen. Siehe Entfernen von VDAs mit dem Skript.

## Benutzerpersonalisierungslayer

February 14, 2024

Der Benutzerpersonalisierungslayer ist ein Feature für Citrix Virtual Apps and Desktops, das die Funktionen nicht persistenter Maschinenkataloge erweitert, um die Daten der Benutzer und lokal installierte Anwendungen über Sitzungen hinweg zu erhalten. Wie PvD unterstützt der auf Citrix App Layering-Technologie basierende Benutzerpersonalisierungslayer Citrix Provisioning und Maschinenerstellungsdiensten (MCS) in einem nicht persistenten Maschinenkatalog.

Die Komponenten des Benutzerpersonalisierungslayers werden zusammen mit dem Virtual Delivery Agent im Masterimage installiert. Lokal von Benutzern installierte Anwendungen werden in einer VHD-Datei gespeichert. Die auf dem Image bereitgestellte virtuelle Festplatte fungiert als persönliche virtuelle Festplatte des Benutzers.

> **Wichtig:**
>
> Sie können Benutzerpersonalisierungslayer in Citrix Virtual Apps and Desktops oder in einer App Layering-Imagevorlage aktivierte App Layering-Benutzerlayer bereitstellen (nicht beides). Installieren Sie das Benutzerpersonalisierungslayer-Feature nicht auf einem Layer innerhalb von App Layering.

Das Feature ersetzt PvD (persönliche vDisk) und bietet Benutzern in einer nicht persistenten, gepoolten Desktopumgebung eine persistente Workspace-Benutzeroberfläche.

Um die Funktion für die Benutzerpersonalisierungslayer bereitzustellen, installieren und konfigurieren Sie sie mit den im Artikel beschriebenen Schritten. Erst dann steht dieses Feature zur Verfügung.

### Anwendungsunterstützung

Bis auf folgende Ausnahmen werden alle Anwendungen, die ein Benutzer lokal auf dem Desktop installiert, im Benutzerpersonalisierunglayer unterstützt.

#### Ausnahmen

Die folgenden Anwendungen werden nicht im Benutzerpersonalisierungslayer unterstützt:

- Unternehmensanwendungen wie MS Office und Visual Studio.
- Anwendungen, die den Netzwerkstapel oder die Hardware ändern. Beispiel: ein VPN-Client.
- Anwendungen mit Treibern auf Startebene. Beispiel: ein Virenscanner.
- Anwendungen mit Treibern, die den Treiberspeicher verwenden. Beispiel: ein Druckertreiber.

  > **Hinweis:**
  >
  > Sie können Drucker über Windows-Gruppenrichtlinienobjekte (GPO) zur Verfügung stellen.

Nicht unterstützte Anwendungen dürfen *nicht* von Benutzern lokal installiert werden. Installieren Sie diese Anwendungen direkt auf dem Masterimage.

#### Anwendungen mit erforderlichem lokalen Benutzer- oder Administratorkonto

Wenn ein Benutzer eine Anwendung lokal installiert, wechselt die App in seinen Benutzerlayer. Wenn der Benutzer dann einen lokalen Benutzer oder eine lokale Gruppe hinzufügt oder bearbeitet, bleiben diese Änderungen nicht über die Sitzung hinaus bestehen.

> **Wichtig:**
>
> Fügen Sie alle erforderlichen lokalen Benutzer oder Gruppen im Masterimage hinzu.

### Anforderungen

Der Benutzerpersonalisierungslayer erfordert folgende Komponenten:

- Citrix Virtual Apps and Desktops 7 1909 oder höher
- Virtual Delivery Agent (VDA), Version 1912 oder höher
- Citrix Provisioning, Version 1909 oder höher
- Windows-Dateifreigabe (SMB) oder Azure Files mit aktivierter AD-Authentifizierung on premises

Sie können das Feature Benutzerpersonalisierungslayer unter den folgenden Windows-Versionen bereitstellen, sofern das Betriebssystem als Einzelsitzung bereitgestellt wird. Es wird nur ein Benutzer in einer Sitzung unterstützt.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, Version 1607 oder höher
- Windows 10 Multisitzungs-OS (unterstützt Azure Files)
- Windows Server 2016 (unterstützt Azure Files)
- Windows Server 2019 (unterstützt Azure Files)

Citrix Virtual Apps and Desktops 7 unterstützt Azure Files mit Benutzerpersonalisierunglayern unter Windows Server 2019, Windows Server 2016v und Windows 10-Client.

> **Hinweis:**
>
> Wenn Sie ein Serverbetriebssystem verwenden, wird nur Server-VDI unterstützt. Weitere Informationen finden Sie im Artikel Server-VDI.
>
> Ein Benutzerpersonalisierungslayer unterstützt nur einen Benutzer pro Maschine und die Maschine muss neu starten, um die Datenträger zurückzusetzen. Sie können den Benutzerpersonalisierungslayer nur mit Einzelsitzungs-Server-OS nicht aber mit Multisitzungs-Server-OS verwenden. Der Benutzerpersonalisierungslayer funktioniert nur mit nicht beständigen Desktops.

Deinstallieren Sie den Benutzerpersonalisierungslayer, falls das Feature installiert ist. Starten Sie das Masterimage neu, bevor Sie das neueste Release installieren.

## Einrichten der Dateifreigabe

Für Benutzerpersonalisierungslayer ist Windows SMB-Speicher (Server Message Block) erforderlich. Zum Erstellen einer Windows-Dateifreigabe folgen Sie dem bei Ihrem Windows-Betriebssystem üblichen Verfahren.

Weitere Informationen zum Verwenden von Azure-Dateien mit Azure-basierten Katalogen finden Sie unter Einrichten des Azure Files-Speichers für Benutzerpersonalisierungslayer.

## Empfehlungen

Beachten Sie die Empfehlungen in diesem Abschnitt, um den Benutzerpersonalisierungslayer fehlerfrei bereitzustellen.

### Microsoft System Center Configuration Manager

Wenn Sie den Benutzerpersonalisierungslayer mit SCCM verwenden, sollten Sie die Microsoft-Richtlinien zur Image-Vorbereitung in einer VDI-Umgebung beachten. Weitere Informationen finden Sie in diesem Microsoft TechNet-Artikel .

### Benutzerlayergröße

Ein Benutzerlayer ist ein Datenträger mit schlanker Speicherzuweisung, der erweitert wird, wenn Speicherplatz auf dem Datenträger verwendet wird. Die zulässige Standardgröße für einen Benutzerlayer beträgt 10 GB (empfohlenes Minimum).

> **Hinweis:**
>
> Wird der Wert bei der Installation auf Null (0) festgelegt, dann wird der Standardwert von 10 GB für den Benutzerlayer verwendet.

Wenn Sie die Benutzerlayergröße ändern möchten, können Sie einen anderen Wert für die Richtlinie **Größe von Benutzerlayer** in Studio eingeben. Weitere Informationen finden Sie unter **Schritt 5: Erstellen benutzerdefinierter Richtlinien für die Bereitstellungsgruppe** unter **Optional: Klicken Sie neben "Größe von Benutzerlayer in GB"auf "Auswählen":**

#### Tools zum Außerkraftsetzen der Benutzerlayergröße (optional)

Sie können die Benutzerlayergröße außer Kraft setzen, indem Sie mit einem Windows-Tool ein Kontingent für die Benutzerlayer-Dateifreigabe festlegen.

Verwenden Sie eines der folgenden Microsoft-Kontingenttools, um ein festes Kontingent für die Benutzerlayer-Dateifreigabe **Users** festzulegen:

- Ressourcen-Manager für Dateiserver (FSRM)
- Kontingentmanager

> **Hinweis:**
>
> Das Erhöhen des Kontingents wirkt sich auf neue Benutzerlayer aus und erweitert vorhandene Layer. Das Verringern des Kontingents wirkt sich nur auf neue Benutzerlayer aus. Vorhandene Benutzerlayer werden nie verkleinert.

### Bereitstellen eines Benutzerpersonalisierungslayers

Beim Bereitstellen von Benutzerpersonalisierungslayer definieren Sie die Richtlinien in Studio. Anschließend weisen Sie die Richtlinien der Bereitstellungsgruppe zu, die dem Maschinenkatalog zugewiesen ist, für den das Feature bereitgestellt wird.

Wenn kein Benutzerpersonalisierungslayer auf dem Masterimage konfiguriert ist, bleiben die Dienste inaktiv und beeinträchtigen die Erstellungsaktivitäten nicht.

Wenn Sie die Richtlinien im Masterimage festlegen, versuchen die Dienste, einen Benutzerlayer im Masterimage auszuführen und bereitzustellen. Dabei würden beim Masterimage unerwartetes Verhalten und Instabilität auftreten.

Führen Sie diese Schrittfolge aus, um das Benutzerpersonalisierungslayer-Feature bereitzustellen:

- Schritt 1: Überprüfen Sie die Verfügbarkeit einer Citrix Virtual Apps and Desktops-Umgebung.
- Schritt 2: Bereiten Sie Ihr Masterimage vor.

- Schritt 3: Erstellen Sie einen Maschinenkatalog.
- Schritt 4: Erstellen Sie eine Bereitstellungsgruppe.
- Schritt 5: Erstellen Sie benutzerdefinierte Richtlinien für die Bereitstellungsgruppe.

> **Hinweis:**
>
> Nachdem Sie Windows 10 auf dem Image aktualisiert haben, dauert das erste Anmelden länger als gewöhnlich. Der Benutzerlayer muss für die neue Version von Windows 10 aktualisiert werden, wodurch sich die Anmeldezeit verlängert.

#### Schritt 1: Überprüfen der Verfügbarkeit einer Citrix Virtual Apps and Desktops-Umgebung

Stellen Sie sicher, dass Ihre Citrix Virtual Apps and Desktops-Umgebung mit diesem neuen Feature verwendet werden kann. Details zum Einrichten finden Sie unter Installieren und Konfigurieren von Citrix Virtual Apps and Desktops.

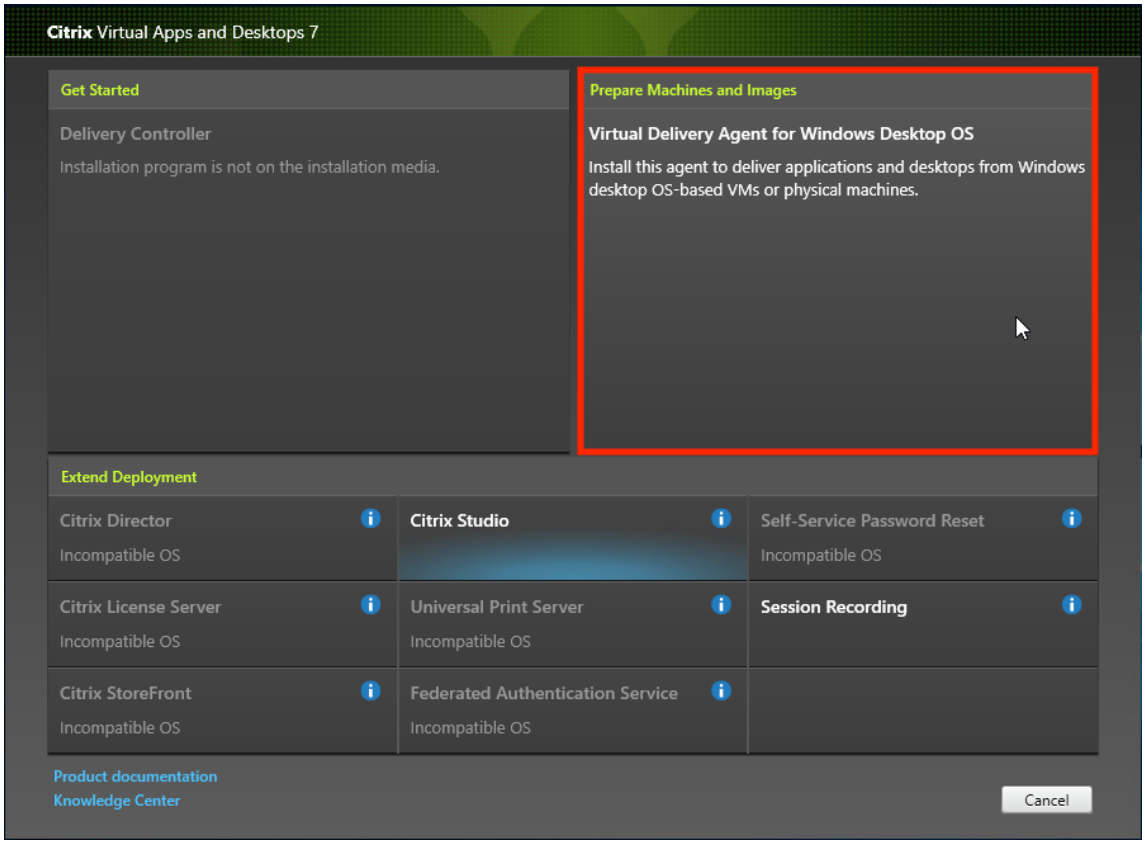
#### Schritt 2: Vorbereiten Ihres Masterimages

Zum Vorbereiten des Masterimages führen Sie folgende Schritte aus:

1. Suchen Sie das Masterimage. Installieren Sie die Unternehmensanwendungen Ihrer Organisation und alle übrigen Apps, die für Benutzer von Nutzen sein könnten.
2. Wenn Sie die Server-VDI bereitstellen, führen Sie die unter Server-VDI aufgeführten Schritte aus. Schließen Sie die optionale Komponente **Benutzerpersonalisierungslayer** ein. Einzelheiten finden Sie unter Befehlszeilenoptionen zur VDA-Installation.
3. Wenn Sie Windows 10 verwenden, installieren Sie Virtual Delivery Agent (VDA) 1912 oder höher. Wenn bereits eine ältere VDA-Version vorhanden ist, deinstallieren Sie diese zunächst. Achten Sie bei der Installation der neuen Version darauf, die optionale Komponente **Citrix User Personalization Layer** wie folgt auszuwählen und zu installieren:

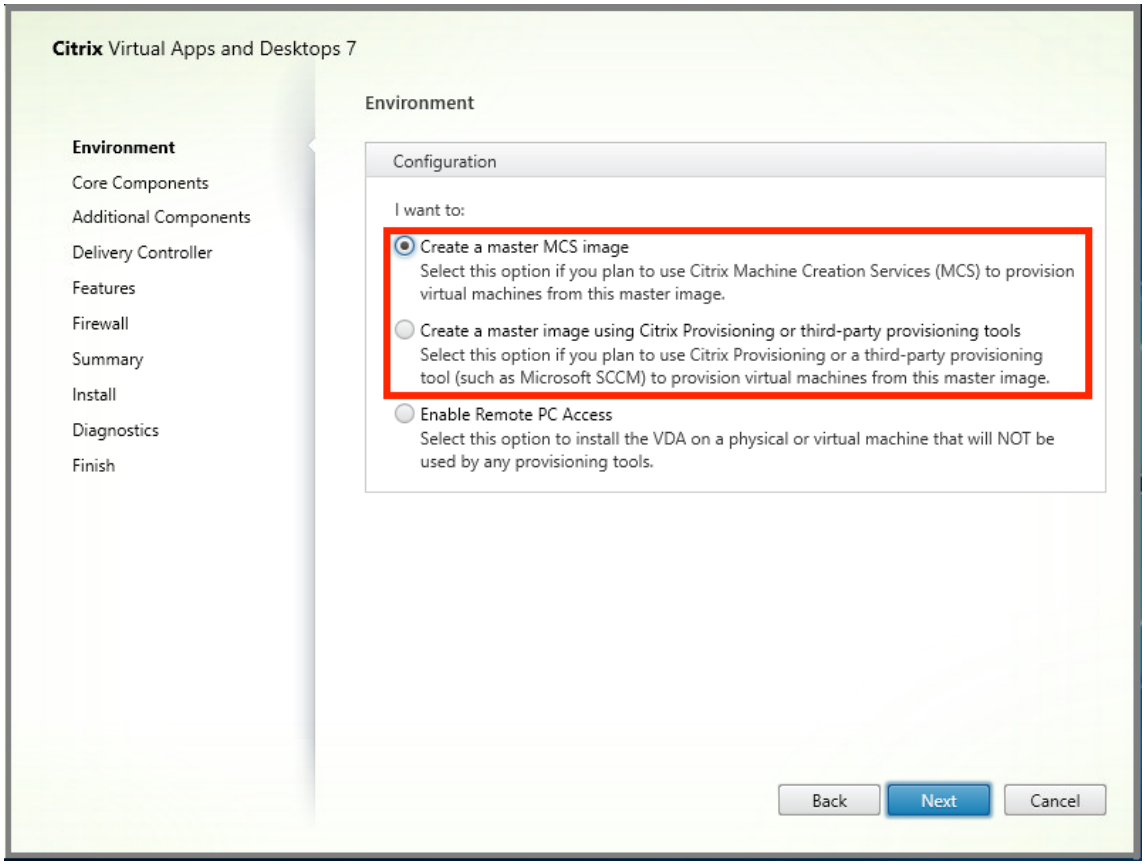
    a) Klicken Sie auf die Kachel **Virtual Delivery Agent für Windows-Desktopbetriebssysteme**.




a) **Umgebung:** Wählen Sie entweder **MCS-Masterimage erstellen** oder **Masterimage mit Citrix Provisioning oder Bereitstellungstools von Drittanbietern erstellen**.

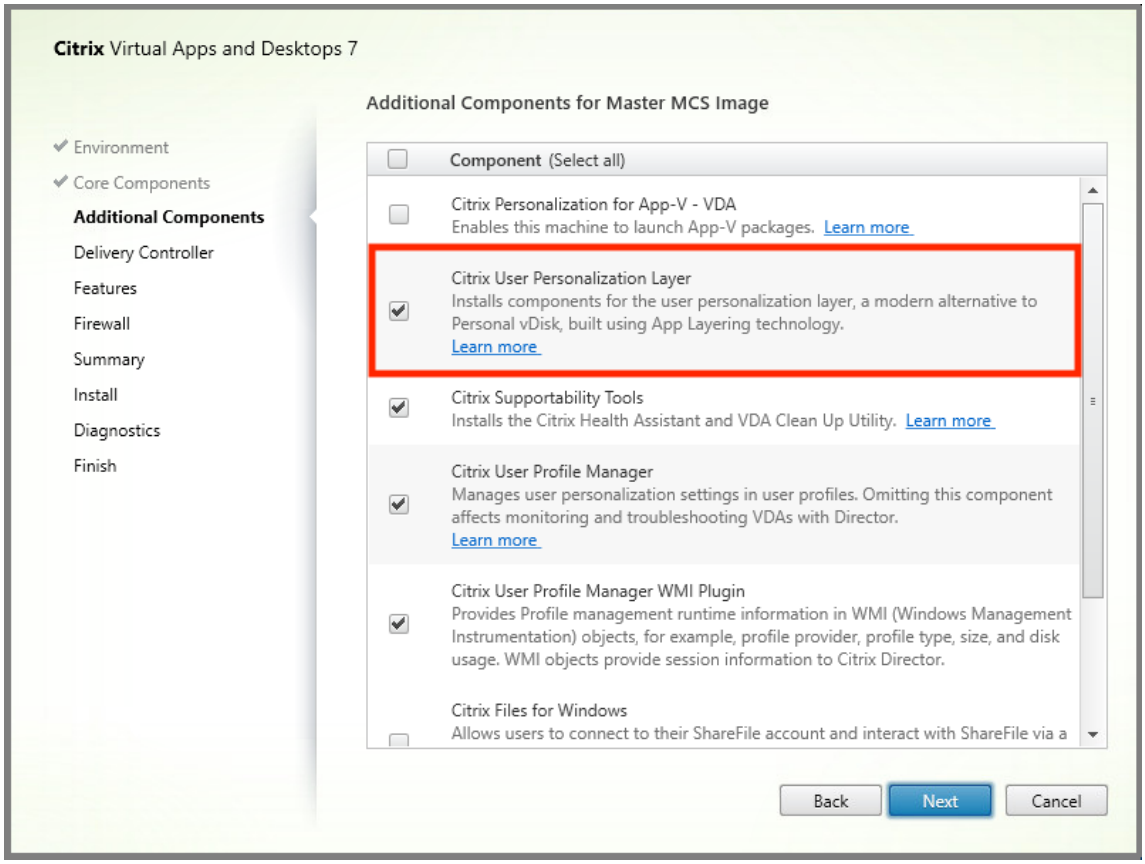
 




a) **Kernkomponenten:** Klicken Sie auf **Weiter**.

b) **Zusätzliche Komponenten:** Aktivieren Sie **Citrix User Personalization Layer**.




a) Konfigurieren Sie den VDA auf den restlichen Installationsbildschirmen nach Bedarf und klicken Sie auf **Installieren**. Das Image wird während der Installation mehrmals neu gestartet.

4. Lassen Sie **Windows-Updates** deaktiviert. Das Installationsprogramm für den Benutzerpersonalisierungslayer deaktiviert Windows-Updates auf dem Image. Lassen Sie die Updatefunktion deaktiviert.

Das Image kann nun in Studio hochgeladen werden.

> **Hinweis:**
>
> Wenn Sie lediglich den Benutzerpersonalisierungslayer (UPL) aktualisieren möchten, können Sie dies mit einer neueren Version des Benutzerpersonalisierungslayer und dem eigenständigen Installationspaket tun. Sie müssen den VDA nicht aktualisieren.

#### Schritt 3: Erstellen eines Maschinenkatalogs

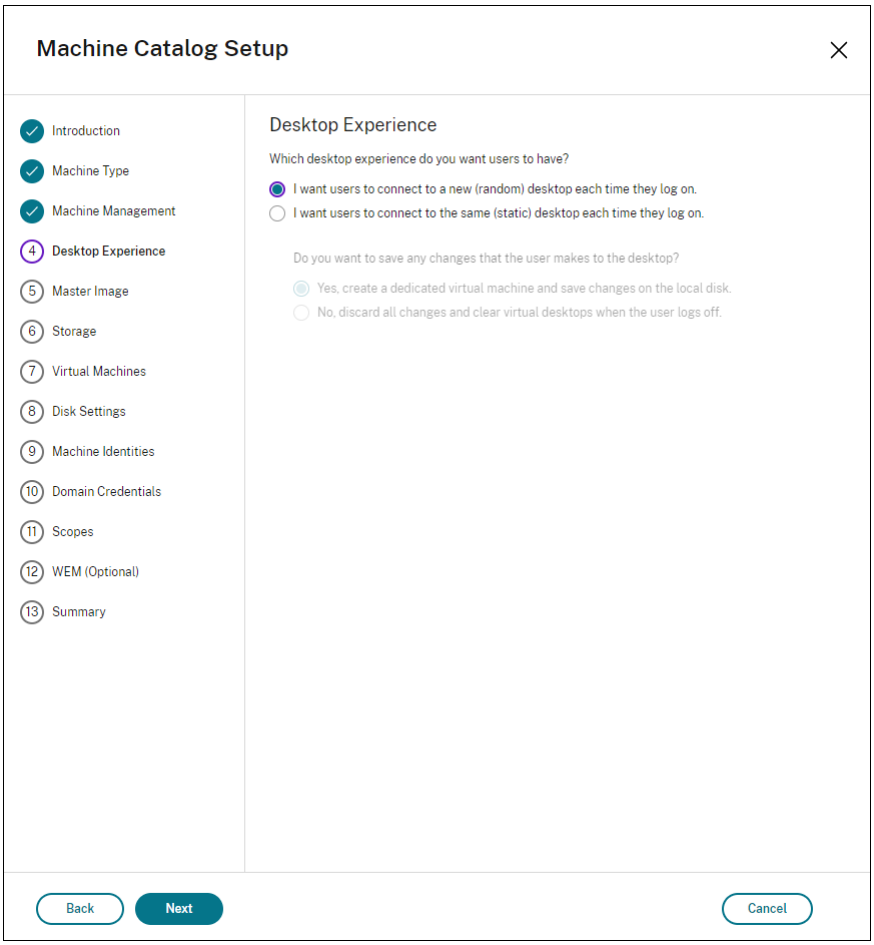
Führen Sie in Studio folgende Schritte aus, um einen Maschinenkatalog zu erstellen. Verwenden Sie die folgenden Optionen während der Katalogerstellung:

1. Wählen Sie unter **Betriebssystem** die Einstellung **Betriebssystem für Einzelsitzungen**.

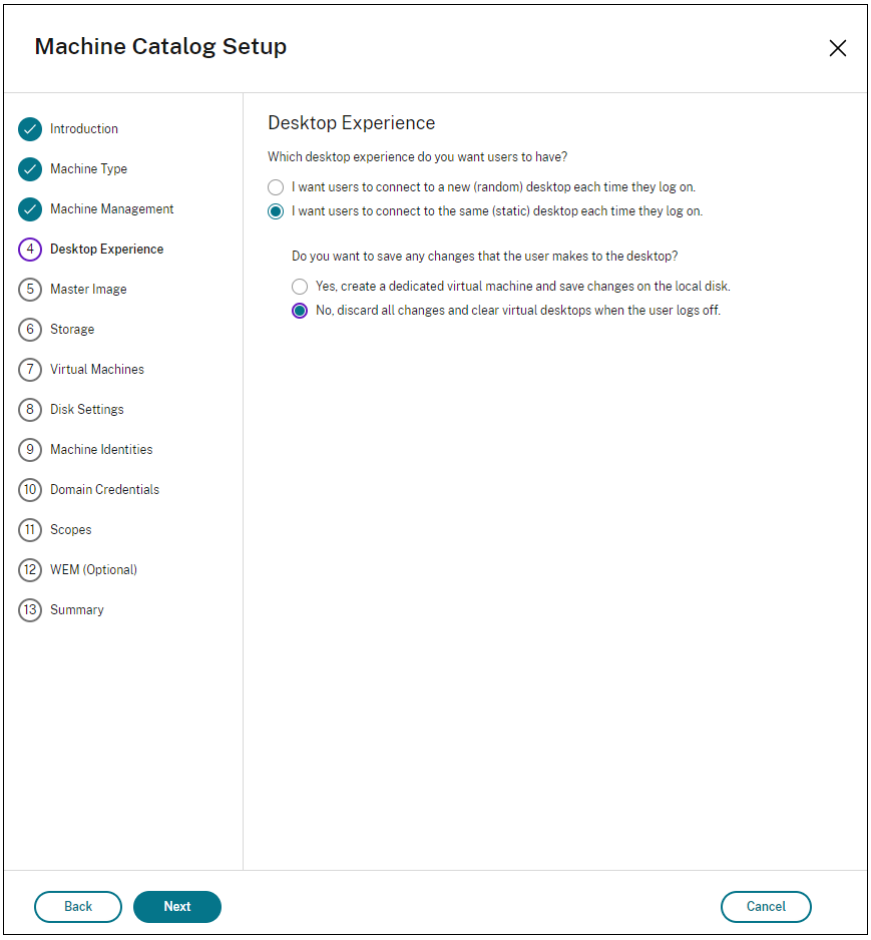
2. Wählen Sie unter **Maschinenverwaltung** die Einstellung **Maschinen mit Energieverwaltung**. Zum Beispiel virtuelle Maschinen oder Blade-PCs.
3. Wählen Sie unter **Desktoperfahrung** den Katalogtyp **Gepoolt-zufällig** oder **Gepoolt-statisch**, wie in den folgenden Beispielen angegeben:

   - **Gepoolt-zufällig:**




   - **Gepoolt-statisch:** Bei Auswahl der gepoolt-statischen Einstellung legen Sie fest, dass beim Abmelden des Benutzers alle Änderungen verworfen und virtuelle Desktops gelöscht werden, wie im folgenden Screenshot angezeigt:




> **Hinweis:**
>
> Der Benutzerpersonalisierungslayer unterstützt keine gepoolt-statischen Kataloge, die zur Verwendung der persönlichen Citrix vDisk konfiguriert oder als dedizierte virtuelle Maschinen zugewiesen wurden.

4. Bei Verwendung von MCS wählen Sie **Image** und den Snapshot für das im vorherigen Abschnitt erstellte Image.
5. Konfigurieren Sie die übrigen Katalogeigenschaften nach Bedarf für Ihre Umgebung.

### Schritt 4: Erstellen einer Bereitstellungsgruppe

Erstellen und konfigurieren Sie eine **Bereitstellungsgruppe**, einschließlich der Maschinen aus dem erstellten Maschinenkatalog. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.

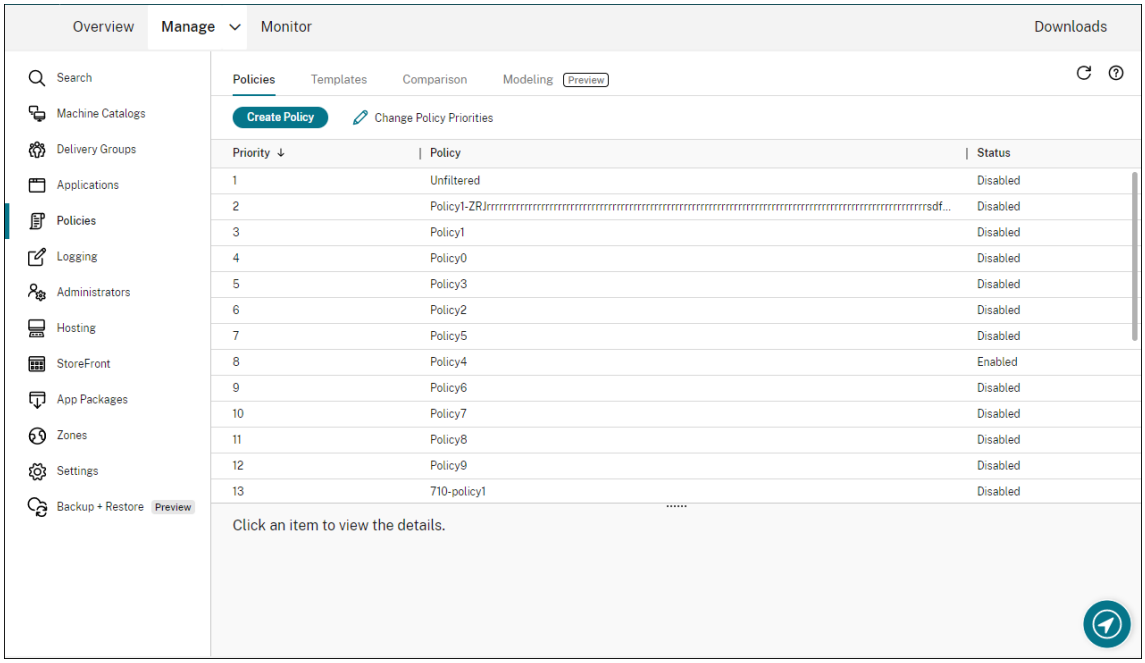
### Schritt 5: Erstellen benutzerdefinierter Richtlinien für die Bereitstellungsgruppe

Um die Bereitstellung von Benutzerlayern in Virtual Delivery Agents zu aktivieren, verwenden Sie die Konfigurationsparameter, um Folgendes zu definieren:

- Wo im Netzwerk auf die Benutzerlayer zugegriffen werden soll.
- Die maximale Größe der Datenträger für die Benutzerlayer.

Die Parameter als benutzerdefinierte Citrix Richtlinien in Web Studio und die Zuweisung zu Ihrer Bereitstellungsgruppe.

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.



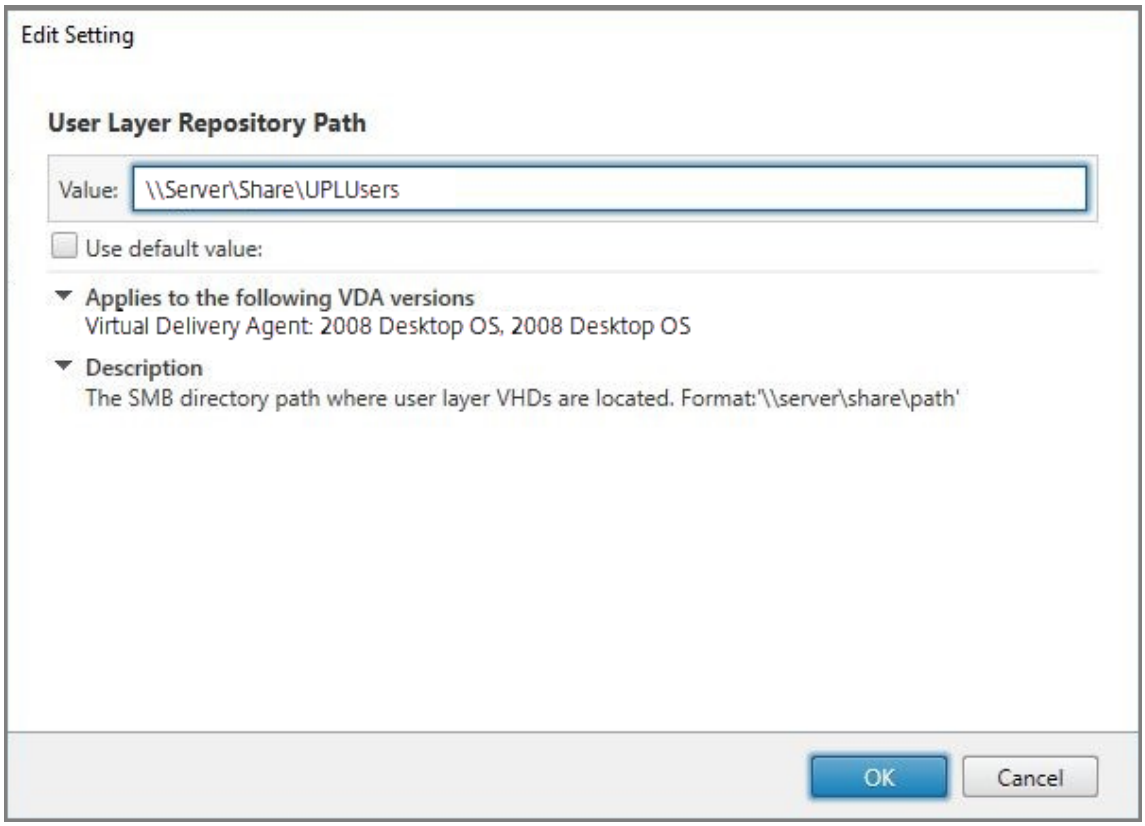

2. Wählen Sie in der Aktionsleiste **Richtlinie erstellen**. Das Fenster Richtlinie erstellen wird angezeigt.
3. Geben Sie in das Suchfeld den Begriff “Benutzerlayer”ein. Drei Richtlinien werden in der Liste der verfügbaren Richtlinien angezeigt:
    - Benutzerlayerausschlüsse
    - Repositorypfad für Benutzerlayer
    - Größe von Benutzerlayer in GB

    > **Hinweis:**
    >
    > Das Erhöhen der Größe wirkt sich auf neue Benutzerlayer aus und erweitert vorhan-

> dene Benutzerlayer. Das Verringern der Größe wirkt sich nur auf neue Benutzerlayer aus. Vorhandene Benutzerlayer werden nie verkleinert.

4. Markieren Sie das Kontrollkästchen neben **Repositorypfad für Benutzerlayer** und klicken Sie auf **Bearbeiten**. Das Fenster Einstellung bearbeiten wird angezeigt.
5. Geben Sie einen Pfad im Feld **Wert** ein und klicken Sie auf **Speichern**:
   - **Pfadformat:** `\\server-name-or-address\share-name\folder`
   - **Pfadbeispiel:** `\\Server\Share\UPLUsers`
   - **Beispiel für resultierende Pfade:** Für den Benutzer **Alex** in **CoolCompanyDomain** würde der Pfad `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK` lauten.



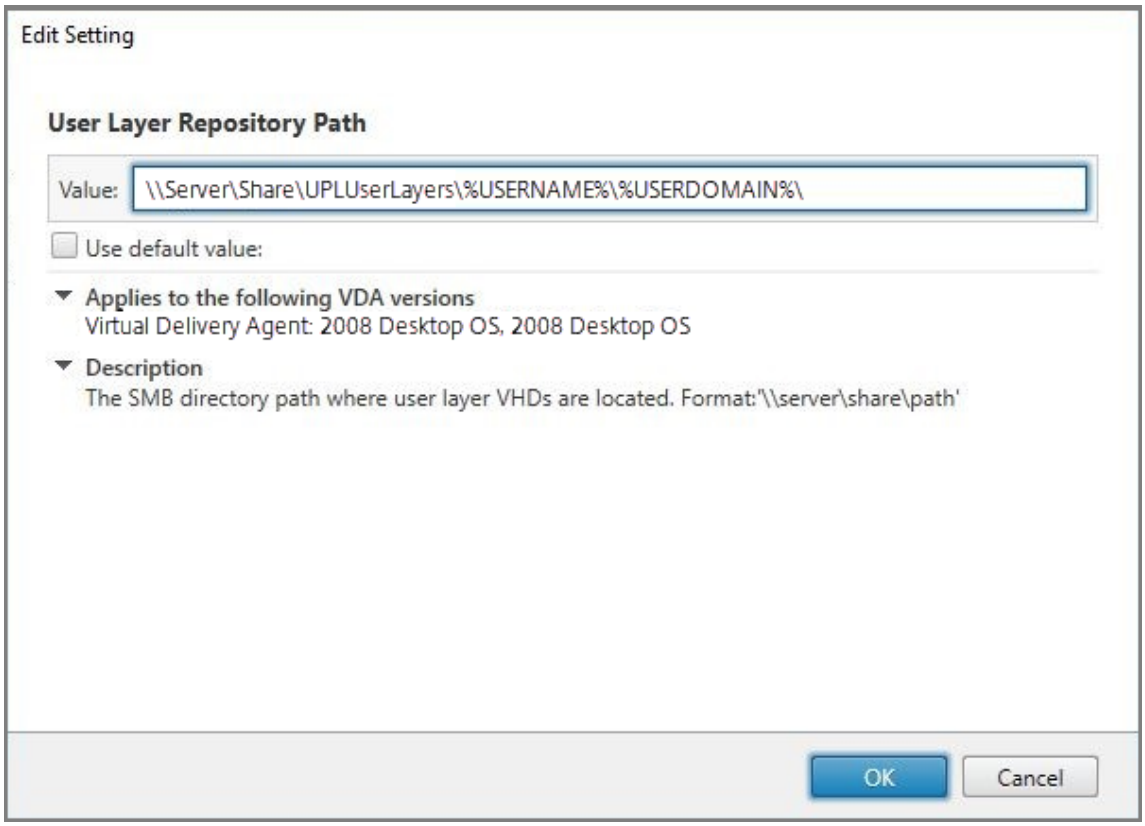

Sie können den Pfad mithilfe der Variablen `%USERNAME%` und `%USERDOMAIN%`, der Maschinenumgebungsvariablen und von Active Directory-Attributen anpassen. Wenn diese Variablen erweitert werden, führen sie zu expliziten Pfaden.

Beispiel für Umgebungsvariablen:

- **Pfadformat:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Pfadbeispiel:** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`

- **Beispiel für resultierende Pfade:** Für den Benutzer **Alex** in **CoolCompanyDomain** würde der Pfad `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK` lauten.

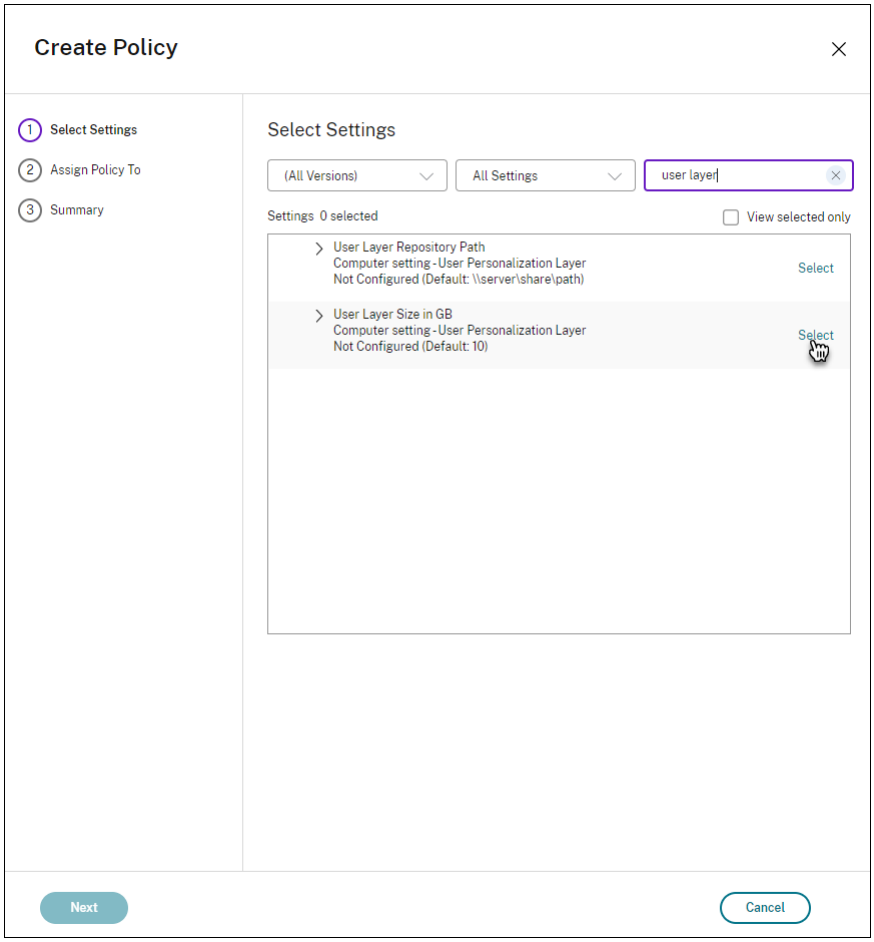



Beispiel für benutzerdefinierte AD-Attribute:

- Pfadformat: `\\Server-name-or-address\share-name\AD-attribute`
- Pfadbeispiel: `\\Server\share\\#sAMAccountName#`
- Beispiel für resultierende Pfade: `\\Server\share\JohnSmith` (wenn #sAMAccount-Name# für den aktuellen Benutzer in JohnSmith aufgelöst wird)

6. Optional: Markieren Sie das Kontrollkästchen neben **Größe von Benutzerlayer in GB** und klicken Sie auf **Bearbeiten**:

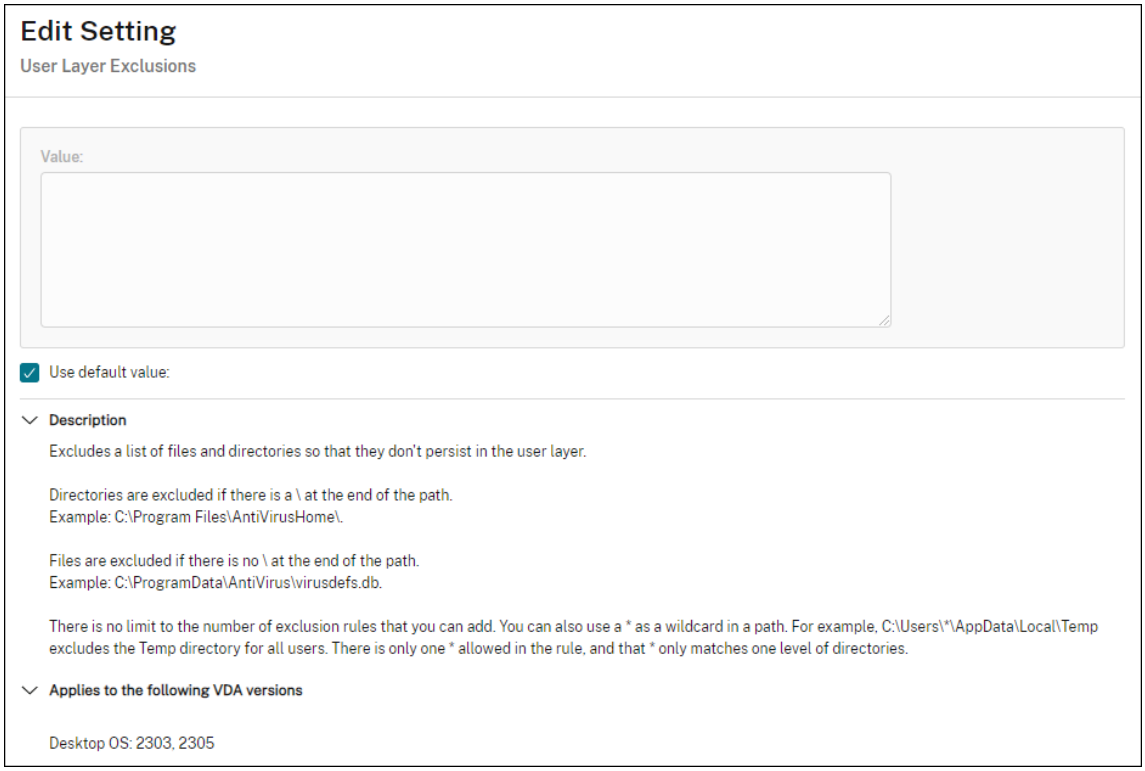
 




Das Fenster “Einstellungen bearbeiten”wird angezeigt.

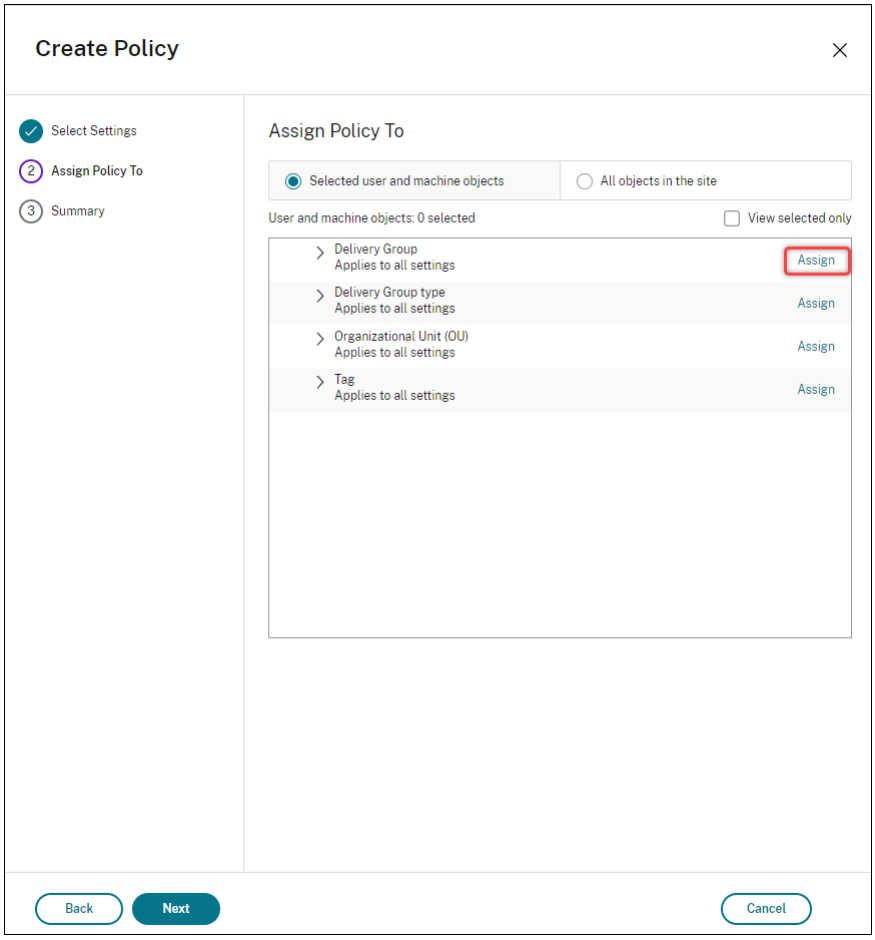
7. Optional: Ändern Sie den Standardwert von **10 GB** auf die maximale Größe, die jeder Benutzerlayer wachsen kann. Klicken Sie auf **Speichern**.
8. Optional: Markieren Sie das Kontrollkästchen neben **Benutzerlayerausschlüsse** und klicken Sie auf **Bearbeiten**.

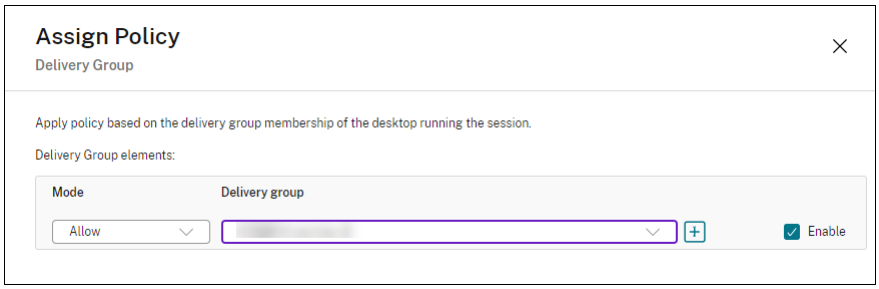



9. Optional: Geben Sie die auszuschließenden Dateien und Ordner an und klicken Sie dann auf **Speichern**. Weitere Informationen finden Sie in der Dokumentation zu Citrix App Layering.
10. Klicken Sie auf **Weiter**, um Benutzer und Maschinen zu konfigurieren, die Sie zuweisen möchten. Klicken Sie neben **Bereitstellungsgruppe** auf den Link “Zuweisen”(im Bild markiert):

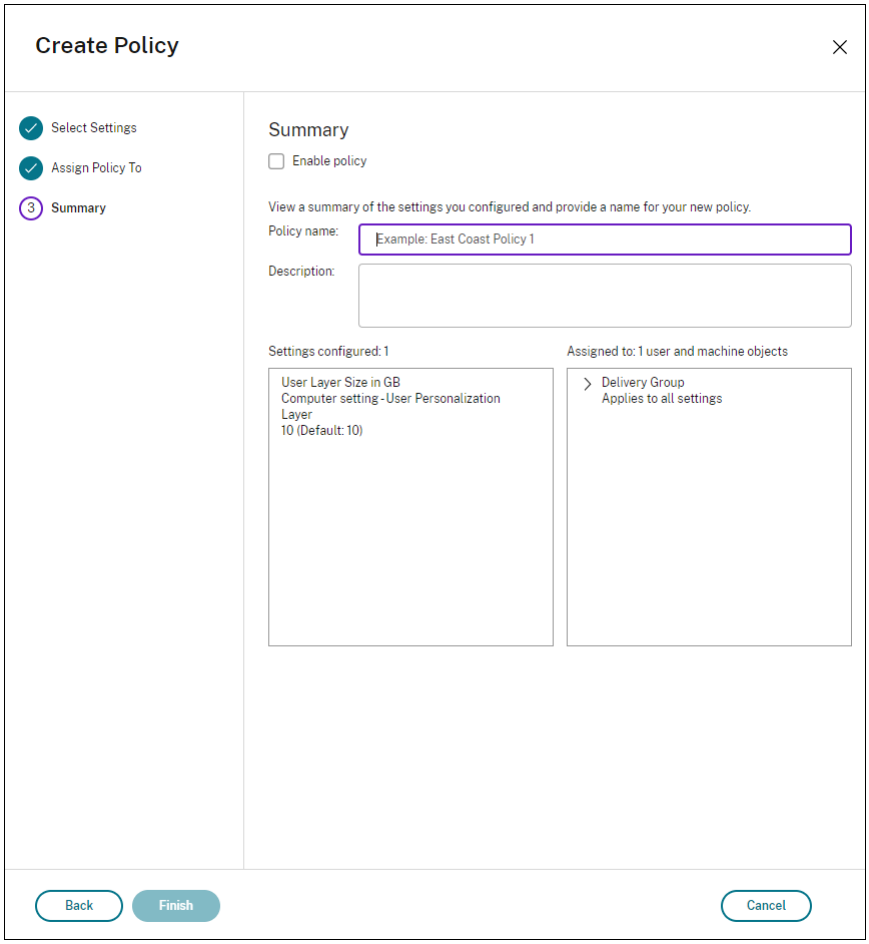



11. Wählen Sie im **Bereitstellungsgruppenmenü** die im vorherigen Abschnitt erstellte Bereitstellungsgruppe aus. Klicken Sie auf **OK**.




12. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie auf das Kontrollkästchen, um die Richtlinie zu aktivieren, und klicken Sie auf **Fertig stellen**.




## Konfigurieren von Sicherheitseinstellungen im Benutzerlayerordner

Als Domänenadministrator können Sie mehrere Speicherorte für Ihre Benutzerlayer angeben. Erstellen Sie einen Unterordner `\Users` für jeden Speicherort (einschließlich des Standardspeicherorts). Schützen Sie jeden Speicherort über die folgenden Einstellungen.

| Einstellungsname | Wert | Anwenden auf |
|---|---|---|
| Ersteller-Besitzer | Ändern | Nur Unterordner und Dateien |
| Besitzerrechte | Ändern | Nur Unterordner und Dateien |
| Benutzer oder Gruppe | Ordner erstellen/Daten anhängen; Ordner durchsuchen/Datei ausführen; Ordner auflisten/Daten lesen; Attribute lesen | Nur ausgewählter Ordner |

| Einstellungsname | Wert | Anwenden auf |
|---|---|---|
| System | Vollzugriff | Ausgewählter Ordner sowie Unterordner und Dateien |
| Domänenadministratoren und ausgewählte Administratorgruppe | Vollzugriff | Ausgewählter Ordner sowie Unterordner und Dateien |

### Benutzerlayermeldungen

Wenn ein Benutzer auf seinen Benutzerlayer nicht zugreifen kann, erhält er eine der folgenden Benachrichtigungen.

- **Benutzerlayer wird verwendet**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **Benutzerlayer nicht verfügbar**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **System wird nach der Benutzerabmeldung nicht zurückgesetzt**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

### Protokolldateien für die Fehlerbehebung

Die Protokolldatei ulayersvc.log enthält die Ausgabe der Benutzerpersonalisierungslayer-Software, in der Änderungen erfasst werden.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

### Einschränkungen

Berücksichtigen Sie folgende Einschränkungen bei der Installation und Verwendung des Benutzerpersonalisierung Features.

- Versuchen Sie *nicht*, die Benutzerpersonalisierungslayer-Software auf einem Layer innerhalb des App Layering bereitzustellen. Stellen Sie Benutzerpersonalisierungslayer in Citrix Virtual Apps and Desktops bereit, oder aktivieren Sie Benutzerlayer in einer App Layering-Imagevorlage (nicht beides). Jeder Prozess erzeugt die Benutzerlayer, die Sie benötigen.
- Konfigurieren Sie den Benutzerpersonalisierungslayer *nicht* mit persistenten Maschinenkatalogen.
- Verwenden Sie *keine* Sitzungshosts.
- Aktualisieren Sie den Maschinenkatalog *nicht* mit einem Image mit neu installiertem Betriebssystem (gilt auch für dieselbe Version von Windows 10). Es wird empfohlen, Betriebssystemaktualisierungen in dem Masterimage anzuwenden, das beim Erstellen des Maschinenkatalogs verwendet wurde.
- Verwenden Sie *keine* Starttreiber oder anderen Personalisierungen, die am Startbeginn aktiv werden.
- Migrieren Sie *keine* Daten einer persönlichen vDisk auf den Benutzerpersonalisierungslayer.
- Migrieren Sie *keine* vorhandenen Benutzerlayer vom vollständigen App Layering-Produkt auf den Benutzerpersonalisierungslayer.
- Ändern Sie *nicht* den Benutzerlayer-SMB-Pfad, um auf Benutzerlayer zuzugreifen, die mit einem anderen Betriebssystem-Masterimage erstellt wurden.
- Wenn sich ein Benutzer von einer Sitzung ab- und wieder anmeldet, wird die neue Sitzung auf einer anderen Maschine im Pool ausgeführt. In VDI-Umgebungen listet Microsoft Software Center eine Anwendung als **Installiert** auf der ersten Maschine auf, auf der zweiten wird sie jedoch als **Nicht verfügbar** angezeigt.

  Weisen Sie den Benutzer an, zur Ermittlung des tatsächlichen Anwendungsstatus die Anwendung im Software Center auszuwählen und auf **Installieren** zu klicken. SCCM aktualisiert dann den Status dann mit dem tatsächlichen Wert.
- Gelegentlich wird das Softwarecenter auf einem VDA mit aktiviertem Benutzerpersonalisierungslayer unmittelbar nach dem Start beendet. Um dieses Problem zu vermeiden, beachten Sie die Empfehlungen von Microsoft zum Implementieren von SCCM in einer XenDesktop VDI-Umgebung. Stellen Sie auch sicher, dass der `ccmexec`-Dienst ausgeführt wird, bevor Sie das Softwarecenter starten.
- In Gruppenrichtlinien (Computereinstellungen) setzen Benutzerlayereinstellungen die Einstellungen für das Masterimage außer Kraft. Daher sind die Änderungen, die Sie unter "Computereinstellungen"mit einem Gruppenrichtlinienobjekt vornehmen, bei der nächsten Sitzungsanmeldung nicht immer für den Benutzer vorhanden.

  Um dieses Problem zu umgehen, erstellen Sie ein Benutzeranmeldeskript, das folgenden Befehl ausgibt:

```
gpupdate /force
```

Ein Kunde hat beispielsweise festgelegt, dass folgender Befehl bei jeder Benutzeranmeldung ausgeführt wird:

```
gpudate /Target:Computer /force
```

Optimale Ergebnisse erzielen Sie, wenn Sie Änderungen unter "Computereinstellungen"direkt auf den Benutzerlayer anwenden, nachdem der Benutzer sich angemeldet hat.

- Der letzte Benutzer, der sich bei einem Masterimage angemeldet hat, darf kein Domänenbenutzerkonto verwendet haben. Andernfalls treten auf den auf Basis dieses Images bereitgestellten Maschinen Probleme auf.
- Benutzerdefinierte Zertifikate bleiben nicht erhalten, wenn UPL in einer reinen Azure AD-Umgebung aktiviert ist. Ursache ist zugrunde liegendes Problem in Windows, das unter Azure ausgeführt wird. Wenn Microsoft dieses Problem in einer zukünftigen Verbesserung behebt, werden wir diesen Artikel aktualisieren.

## Upgrade der VDAs

May 17, 2024

### Einführung

Citrix verwaltet alle Komponenten von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) in Ihrer Bereitstellung, mit Ausnahme von VDAs.

Führen Sie vor Beginn eines VDA-Upgrades folgende Schritte aus:

- Lesen Sie diesen Artikel vollständig durch.
- Lesen Sie die Lebenszyklus-Richtlinie für Citrix DaaS.

Um einen VDA zu aktualisieren, laden Sie ein VDA-Installationsprogramm herunter und führen Sie es auf der Maschine oder dem Image aus. Sie können die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle des Installationsprogramms verwenden. Erläuterungen finden Sie unter:

- VDA-Installationsprogramme
- Installieren von VDAs über die grafische Oberfläche
- VDAs über die Befehlszeile installieren

Wenn der VDA ursprünglich mit `VDAWorkstationCoreSetup.exe` installiert wurde:

- Sie behalten diese Konfiguration bei, wenn Sie den VDA mit der neuesten Version desselben Installationsprogramms aktualisieren.
- Wenn Sie `VDAWorkstationSetup.exe` auf dieser Maschine ausführen, können Sie Features aktivieren, die in `VDAWorkstationCoreSetup.exe` nicht unterstützt werden. Einige dieser Features sind im Installationsprogramm `VDAWorkstationSetup.exe` evtl. standardmäßig aktiviert. Sie können auch die Citrix Workspace-App installieren.

> **Hinweis:**
>
> Beim Upgrade auf VDA-Version 7.17 oder eine spätere unterstützte Version tritt ein Neustart auf. Dieser Neustart kann nicht vermieden werden. Das Upgrade wird nach dem Neustart automatisch fortgesetzt (es sei denn, Sie haben an der Befehlszeile `/noresume` angegeben).

Aktualisieren Sie nach dem Upgrade der VDAs die Images und Maschinenkataloge, die diesen VDA verwenden.

### Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration"

> **Wichtig:**
>
> - Als bewährte Methode empfehlen wir, VDA-Upgrades gründlich zu testen, bevor sie in die Produktion übernommen werden.
> - Sie können zwischen CR VDA und LTSR VDA wechseln, sofern Sie von einer früheren Version zu einer späteren wechseln. Sie können nicht von einer späteren Version zu einer früheren Version wechseln, da dies als Downgrade betrachtet wird. Sie können beispielsweise nicht von 2212 CR auf 2203 LTSR (alle CUs) wechseln, ein Upgrade von 2112 CR auf 2203 LTSR (alle CUs) ist dagegen möglich.
> - On-Demand-Updates (etwa Hotfixes oder Patches zwischen Hauptversionen) werden nicht unterstützt.
> - CVAD 2402 VDA ist über den VDA Upgrade Service verfügbar.

Mit der Benutzeroberfläche "Vollständige Konfiguration"können Sie VDAs pro Katalog oder pro Maschine aktualisieren. Das Upgrade kann sofort oder zu einem festgelegten Zeitpunkt ausgeführt werden.

Weitere Informationen zum VDA-Upgradedienst finden Sie unter Tech Brief: Citrix VDA Upgrade service. Dort finden Sie eine Übersicht über den Dienst, detaillierte Angaben zur Funktion und weitere nützliche Ressourcen.

#### Voraussetzungen

- Steuerungsebene: Citrix DaaS

- VDA-Typ: VDA mit Einzel- oder Multisitzungs-OS Derzeit wird nur Windows VDA unterstützt.
- VDA-Version: 2109 oder höher, oder 2203 LTSR oder höher

  > **Hinweis:**
  >
  > Wir empfehlen, einen VDA mit dem aktuellen Release oder mit dem neuesten LTSR CU zu verwenden.

- Provisioningtyp: Persistente Maschinen (z. B. mit MCS bereitgestellte Maschinen, Remote-PC-Zugriff-Maschinen, Citrix HDX Plus für Windows 365). Siehe Unterstützte Maschinentypen.
- VDA Upgrade Agent muss auf den VDAs installiert sein und der Dienst muss ausgeführt werden.
- Sie vefügen über Berechtigungen zum Upgrade von VDAs.
- Das VDA-Upgrade wurde mit dem richtigen CR oder LTSR in der vollständigen Konfiguration konfiguriert.
- Die VDAs werden nicht verwendet. (Die Benutzer müssen sich von ihnen abmelden.)

  > **Hinweis:**
  >
  > Bei Upgrades werden VDAs übersprungen, die verwendet werden oder deren Verbindung unterbrochen ist. Wir empfehlen, ein Upgradefenster zu planen und die Benutzer aufzufordern, sich von den VDAs abzumelden.

- Die VDAs sind nicht im Wartungsmodus. (Ein VDA kann von einem Administrator in den Wartungsmodus versetzt werden. Ein VDA kann auch automatisch in den Wartungsmodus versetzt werden, wenn er die maximal zulässigen Registrierungsversuche überschritten hat.)
- Relevante URLs wurden zur Positivliste hinzugefügt, sofern die URL-Filterung aktiviert ist. Weitere Informationen finden Sie unter Anforderungen für VDA-Upgrade.
- Die VDAs müssen zu einer Bereitstellungsgruppe gehören und bei DaaS registriert sein.
- Die Funktionsebene ist richtig eingestellt, sodass das VDA-Upgradefeature verwendet werden kann. Siehe VDA-Versionen und Funktionsebenen.
- Der Ziel-VDA unterstützt das Betriebssystem des aktuellen VDAs.

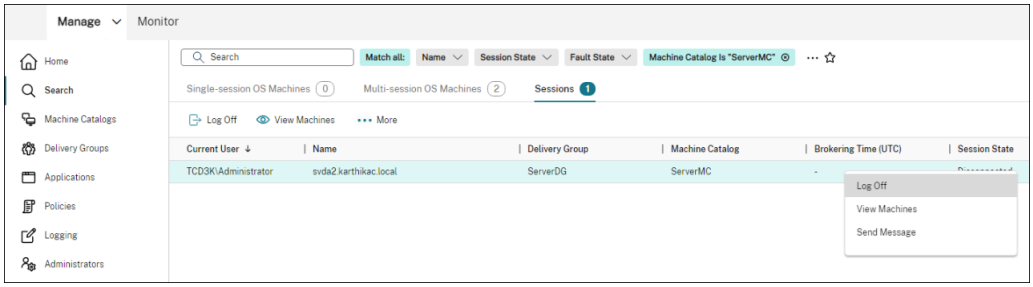
**Bekannte Probleme**

**Problem 1: Das Upgrade von LTSR-VDAs auf LTSR Cumulative Update-Versionen schlägt fehl** Das Upgrade von LTSR-VDAs auf LTSR Cumulative Update-Versionen kann fehlschlagen. Obwohl das Upgrade in der vollständigen Konfiguration anscheinend erfolgreich ausgeführt wird, ändert sich die installierte Version des VDA nicht und der Status wechselt nach ein oder zwei Minuten wieder zu **Upgrade ist verfügbar**. Das Problem tritt bei VDAs mit VDA Upgrade Agent 7.35.0.7 oder einer älteren Version auf.

Um das Problem zu umgehen, melden Sie sich beim VDA an und aktualisieren Sie den VDA Upgrade Agent auf Version 7.37.0.7 oder höher (mit dem VDA-Installationsprogramm ab Version 2303). Ab Version 7.37.0.7 unterstützt der VDA Upgrade Agent automatische Upgrades, sodass auf den VDAs installierte frühere Versionen automatisch auf die neueste Version aktualisiert werden können. Beim automatischen Upgrade überprüft der VDA-Upgrade-Dienst die vom Agent gemeldete VDA-Version und plant dann Upgrades innerhalb einer Stunde, um den Agenten automatisch auf die neueste Version zu aktualisieren. Das automatische Upgrade reduziert den Wartungsaufwand.

Damit der Agent auf dem VDA ein automatisches Upgrade durchführt, müssen Sie Sitzungen abmelden, damit der VDA-Upgrade-Dienst automatische Upgrades einleiten kann. Sie können Sitzungen in der vollständigen Konfiguration abmelden.




Wenn der Agent das automatische Upgrade nicht durchführen kann, melden Sie sich beim VDA an und führen Sie Upgrade des Agents wie folgt manuelle durch:

1. Führen Sie das folgende Cmdlet aus, um den VDA Upgrade Agent unter “Systemsteuerung > Programm deinstallieren oder ändern”anzuzeigen.

```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. Installieren Sie den aktuellen VDA Upgrade Agent. Verwenden Sie das folgende Cmdlet, um eine Installation im Hintergrund durchzuführen:

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

Sie können die Version des VDA Upgrade Agent per Cmdlet oder Skript identifizieren. Siehe Problembehandlung.

**Problem 2: Proxy wird nicht unterstützt** Derzeit unterstützt der VDA Upgrade Agent keine Proxykonfigurationen. Diese Einschränkung kann zu Verbindungsproblemen führen, wenn der Agent versucht, Verbindungen über einen Proxyserver herzustellen.

Sie können das Problem mit einem Workaround umgehen. Führen Sie folgende Schritte aus:

1. Suchen Sie die VDA Upgrade Agent-Konfigurationsdatei in `C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`.
2. Öffnen Sie die Konfigurationsdatei mit einem Texteditor.
3. Fügen Sie am Ende der Datei die folgenden Zeilen hinzu und ersetzen Sie `ProxyServerName` durch den Namen des verwendeten Proxyservers:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
       ="false" />
  </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

4. Starten Sie den Citrix VDA Upgrade Agent-Dienst neu, um die neue Konfiguration zu übernehmen.

### Allgemeiner Arbeitsablauf

Dies ist ein allgemeiner Workflow zum Upgrade von VDAs über die Oberfläche "Vollständige Konfiguration":

1. Aktivieren Sie das VDA-Upgrade für einen Katalog.
   - Sie können das VDA-Upgrade beim Erstellen eines Katalogs aktivieren.
   - Sie können das VDA-Upgrade aktivieren, wenn Sie einen Katalog bearbeiten.
2. Führen Sie das Upgrade der VDAs pro Katalog oder pro Maschine durch. Weitere Informationen finden Sie unter Automatische Upgrades für VDAs konfigurieren.

   > **Hinweis:**
   >
   > Beachten Sie bei der Planung von VDA-Upgrades für einen Katalog, dass alle Maschinen im Katalog beim Upgrade berücksichtigt werden. Daher empfehlen wir, diese Maschinen zu sichern, bevor Sie das Upgrade starten.

### Problembehandlung

Schlägt ein Upgrade fehl, können Sie die folgenden Protokolle verwenden, um Probleme selbst zu beheben, oder sie bereitstellen, wenn Sie sich an den technischen Support von Citrix wenden, um Unterstützung zu erhalten.

- Installationsprotokolle für die erste VDA-Installation unter `%temp%/Citrix/XenDesktop Installer`
- Upgradeprotokolle unter `C:\Windows\Temp\Citrix\XenDesktop Installer`

Verwenden Sie das folgende Cmdlet, um die Version des VDA Upgrade Agent zu überprüfen: `Get-VusComponentVersion -ComponentType VUS`. Es listet alle VDAs und deren VDA Upgrade Agent-Versionen auf.

Verwenden Sie das folgende Cmdlet, um die VDA-Namen zu erhalten: `Get-BrokerMachine -UUID "<version number>"`, wobei `<version number>` für die VDA Upgrade Agent-Version steht, die das Cmdlet `Get-VusComponentVersion` zurückgibt.

Um die VDA Upgrade Agent-Version auf Katalogebene zu überprüfen, können Sie das folgende Skript verwenden:

> **Hinweis:**
>
> Das Skript hat Beispielcharakter und muss möglicherweise an Ihre Umgebung angepasst werden. Wir empfehlen, dass Sie das Skript gründlich testen, bevor Sie es in einer Produktionsumgebung verwenden.

```
Param(
    [Parameter (Mandatory=$true)]
    [string] $CatalogName
)

try
{

    $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-
       Object -Property UUID

    if($Uuids -eq $null)
    {

        throw "Cannot find CatalogName "+$CatalogName
     }

    Write-Output("Catalog Name passed is "+$CatalogName)

   foreach($Uuid in $Uuids)
    {

```

```
22          $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
                -ComponentType VUS
23          $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
24          Write-Output("MachineName: "+$Machine.MachineName+", Machine
               UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
               Version)
25       }
26
27    }
28
29  catch
30  {
31
32      Write-Output("Exception Occured")
33      Write-Host $_
34    }
35
36  <!--NeedCopy-->
```

**Für den VDA Upgrade Agent relevante Protokolle** Sie können auch Protokolle sammeln, die sich auf den VDA Upgrade Agent beziehen. Dazu gehören:

- **Citrix Diagnostic Facility-Tracingberichte.**
- **Windows-Ereignisprotokolle.** In das Windows-Ereignisprotokoll geschriebene Informationen. Zeigen Sie die Protokolle in **Ereignisanzeige > Anwendungs- und Dienstprotokolle > Citrix VDA Upgrade Agent Service** an.

Bei Bedarf können Sie die VDA Upgrade Agent-Konfigurationsdatei ändern, sodass die Protokolle kontinuierlich in eine Datei geschrieben werden. Gehen Sie folgendermaßen vor, um die Protokollierung in einer Datei zu aktivieren:

1. Gehen Sie zum Ordner `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Öffnen Sie die Datei `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Ändern Sie den Wert von `LogToFile` auf `1`.
4. Starten Sie den Citrix VDA Upgrade Agent-Dienst neu. Dadurch wird eine Protokolldatei unter `C:\ProgramData\Citrix\Update Services\Logs` erstellt.

> **Hinweis:**
>
> - Wenn Sie die Protokollierung in einer Datei aktivieren, werden kontinuierlich Protokolle geschrieben, was möglicherweise viel Speicherplatz beansprucht. Denken Sie daran, die Protokollierung zu deaktivieren, nachdem ein Problem behoben wurde. Um die Protokollierung zu deaktivieren, stellen Sie zuerst `LogToFile` auf `0` ein und starten Sie den Citrix VDA Upgrade Agent- Dienst dann neu.

> - Wenn `LogToFile=1` festgelegt ist , werden Protokolle nur in die Datei geschrieben. Sie erscheinen nicht im CDF-Tracingbericht.

**Downloadfehler beim VDA-Upgrade behandeln** Gehen Sie wie folgt vor, um Downloadfehler im Zusammenhang mit der VDA-Upgrade zu diagnostizieren und zu beheben:

1. Vergewissern Sie sich, dass relevante URLs zur Positivliste hinzugefügt wurden, sofern die URL-Filterung aktiviert ist. Weitere Informationen finden Sie unter Anforderungen für VDA-Upgrade.
2. Nachdem Sie die erforderlichen URLs zur Positivliste hinzugefügt haben, versuchen Sie, das VDA-Upgrade neu zu planen.

Sie können die CDF-Ablaufverfolgung aktivieren oder `LogToFile` auf 1 einstellen, um detaillierte Protokolle zur Analyse zu erfassen. Wenn das Problem mit dem Downloadfehler weiterhin besteht, überprüfen Sie die Fehler. Wenn die Fehlermeldung "Download Failed: This access control list is not in canonical form and therefore cannot be modified"angezeigt wird, weist dies darauf hin, dass die Berechtigungen für den Ordner `C:/ProgramData/Citrix/UpgradeServices/Downloads/VDA` falsch sind. Gehen Sie wie folgt vor, um das Problem zu beheben:

- **Option 1:** Setzen Sie die Zugriffskontrolllisten (ACLs) für den Ordner mithilfe des folgenden Befehls zurück. (Der Befehl setzt die ACLs mit standardmäßig vererbten ACLs für alle passenden Dateien zurück.)

  ```
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\
    VDA"/reset /T /C /L /Q
  ```

- **Option 2:** Löschen Sie den VDA-Ordner unter "Downloads"und planen Sie dann das VDA-Upgrade.

**Fehler bei der Überprüfung beim VDA-Upgrade behandeln** Gehen Sie wie folgt vor, um Downloadfehler im Zusammenhang mit der VDA-Upgrade zu diagnostizieren und zu beheben:

1. Stellen Sie sicher, dass die relevanten URLs zur URL-Positivliste hinzugefügt wurden, wenn eine URL-Filterung verwendet wird, insbesondere die URLs der Zertifikatsperrliste und für OCSP (Online Certificate Status Protocol), die für die Sperrprüfung benötigt werden. Weitere Informationen finden Sie unter Anforderungen für VDA-Upgrade.
2. Nachdem Sie die erforderlichen URLs zur Positivliste hinzugefügt haben, versuchen Sie, das VDA-Upgrade neu zu planen.

Wir empfehlen, die CDF-Ablaufverfolgung zu aktivieren oder `LogToFile` auf 1 einzustellen, um detaillierte Protokolle zur Analyse zu erfassen. Die Protokolle können die folgenden Fehler enthalten:

- RevocationStatusUnknown

- Die Sperrfunktion konnte den Sperrstatus für das Zertifikat nicht überprüfen.
- Die Sperrfunktion konnte die Sperrung nicht überprüfen, da der Sperrserver offline war.

Der VDA Upgrade Agent nutzt Windows-Systemaufrufe, um Zertifikate zu validieren und Sperrprüfungen durchzuführen. Die obigen Fehler weisen darauf hin, dass der Agent keine Verbindung zur Zertifikatsperrlisten- oder OCSP-URL herstellen kann.

Der VDA Upgrade Agent unterstützt derzeit keine Proxyeinstellungen. Die ausgehenden Zertifikatsperrlisten- und OCSP-Aufrufe der CryptoAPI nehmen keine Proxykonfiguration zur Kenntnis, was zu Fehlern führen kann.

Wenn Ihre Umgebung über einen Proxy verfügt, können Sie den Systemproxy auf dem VDA konfigurieren, um ausgehende Zertifikatsperrlistenaufrufe zu ermöglichen. Gehen Sie wie folgt vor, um den Systemproxy zu konfigurieren:

```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

### VDAs mit PowerShell aktualisieren

Sie können VDA-Upgrades mit dem Remote PowerShell SDK konfigurieren. Informationen zum Remote PowerShell SDK finden Sie unter Citrix DaaS Remote PowerShell SDK.

Im Folgenden sind die PowerShell-Cmdlets aufgeführt:

- **Get-VusCatalog**

  Verwenden Sie dieses Cmdlet, um Details zu einem Katalog abzurufen: `Name`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR) `Upgrade scheduled` und `StateId` (Status von `Upgrade scheduled`).

- **Get-VusMachine**

  Verwenden Sie dieses Cmdlet, um Details zu einer Maschine abzurufen: `MachineName`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR) und `StateId` (Status von `Upgrade scheduled`).

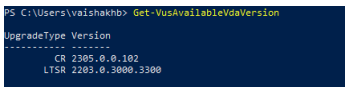
- **Get-VusComponentVersion**

  Verwenden Sie dieses Cmdlet, um zu überprüfen, ob VDAs die Komponentenversionen gemeldet haben. Verwenden Sie `MachineId`, um die VDAs zu filtern. `MachineId` ist die UUID von `Get-BrokerMachine`.

- **Get-VusAvailableVdaVersion**

  Verwenden Sie dieses Cmdlet, um sich über die neueste, über den VDA Update Service veröffentlichte CR/LTSR-Version zu informieren.




- **Set-VusCatalogUpgradeType**

  Verwenden Sie dieses Cmdlet, um den Upgradetyp eines Katalogs auf CR oder LTSR festzulegen. Der Upgradetyp kann nur auf Maschinenkatalogebene festgelegt werden.

- **New-VusMachineUpgrade**

  Verwenden Sie dieses Cmdlet, um VDA-Upgrades auf Maschinenebene zu konfigurieren.

- **New-VusCatalogSchedule**

  Verwenden Sie dieses Cmdlet, um VDA-Upgrades auf Maschinenkatalogebene zu planen.

#### Beispiele für Cmdlets auf Maschinenebene

- Upgradetyp festlegen.

  Beispiel:
  `–Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Verwenden Sie `Get-VusMachine`, um `UpgradeState` der Maschinen in einem Katalog zu überprüfen.

  Beispiel:
  `–Get-VusMachine -CatalogName test-catalog`

```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName       : test-catalog
DNSName           : test-machine-1
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :

CatalogName       : test-catalog
DNSName           : test-machine-2
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :
```

Wenn `UpgradeState` = `Unknown` kann dies daran liegen, dass der auf dem VDA installierte Citrix VDA Upgrade Agent die Version nicht an den VDA Update Service gemeldet hat. Sie können mit dem Cmdlet `Get-VusComponentVersion` überprüfen, ob der VDA Komponentenversionen gemeldet hat.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Wenn keine Ergebnisse angezeigt werden, überprüfen Sie Folgendes:

- Der VDA ist Teil eines Katalog und einer Bereitstellungsgruppe.
- Der VDA Upgrade Agent ist auf dem VDA installiert und wird ausgeführt. Versuchen Sie bei Bedarf, den Agent neu zu starten.

**Hinweis**: Wenn weiterhin keine Ergebnisse angezeigt werden, sammeln Sie beim Neustart des VDA Upgrade Agent die Citrix Diagnostic Facility-Tracingberichte und beheben Sie die Probleme.

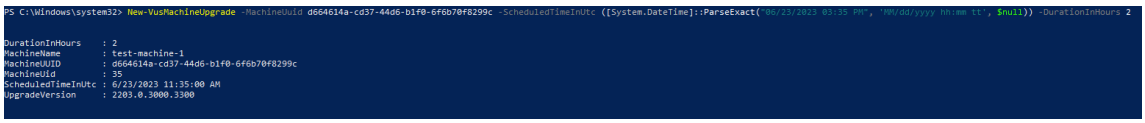
- VDA-Upgrades planen. Bevor Sie beginnen, sollten Sie Folgendes beachten:

  - `DurationInHours`: Dient zum Angeben der Dauer des Upgrade-Vorgangs in Stunden. VDAs werden in den Wartungsmodus versetzt. Das VDA-Installationsprogramm wird heruntergeladen und das Upgrade wird durchgeführt. Geben Sie eine längere Dauer an, wenn viele VDAs aktualisiert werden müssen.
  - `UpgradeNow`: Verwenden Sie diesen Switch, um ein Upgrade sofort zu planen oder legen Sie `ScheduledTimeInUtc` fest.
  - `ScheduledTimeInUtc`: Dient zum Planen eines Upgrades für ein bestimmtes Datum und eine bestimmte Uhrzeit.

  Beispiel:

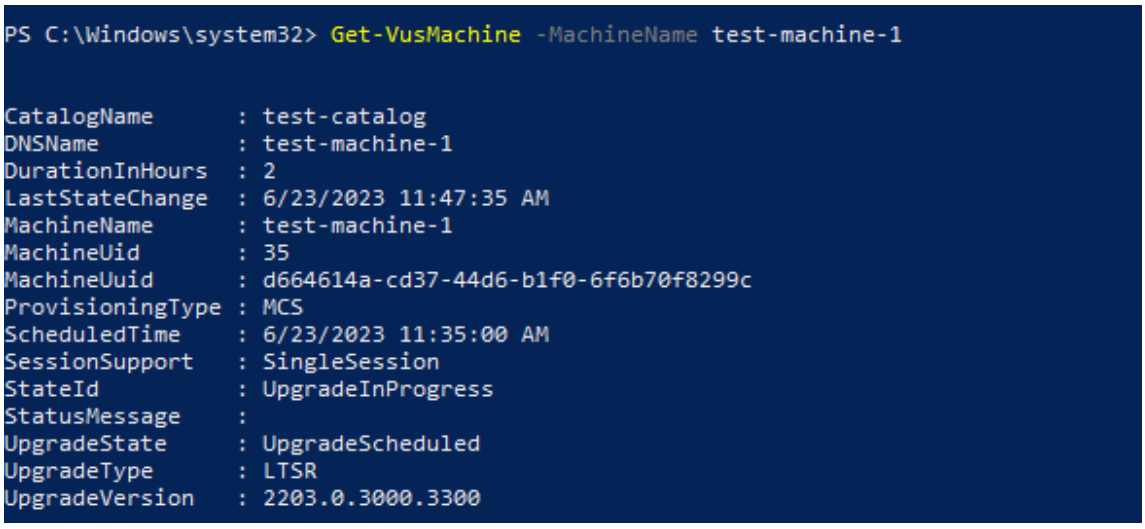
  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  Sie können VDA-Upgrades unter Verwendung von `MachineUuid`, `MachineUid` und `MachineName` planen.

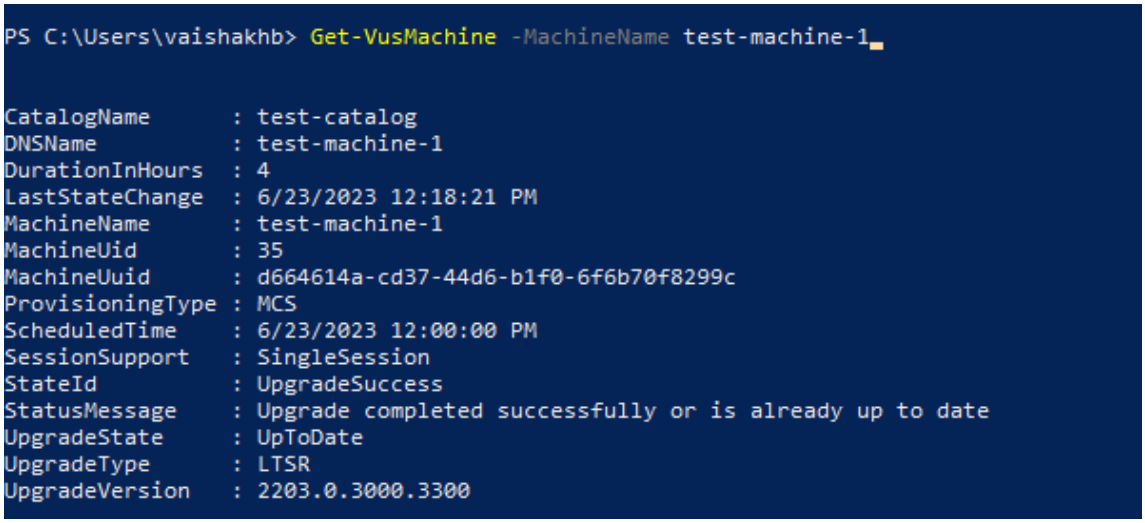



- Upgradestatus überprüfen.

  Beispiel:
  –`Get-VusMachine -MachineName test-machine-1`






**Beispiele für Cmdlets auf Katalogebene**

- Upgradetyp auf Maschinenkatalogebene festlegen.

  Beispiel:

  ```
  –Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType
   LTSR
  ```

- Verwenden Sie `Get-VusCatalog`, um den `UpgradeState` der Maschinen in einem Katalog zu überprüfen:

  Beispiel:

  ```
  –Get-VusCatalog -Name test-catalog
  ```

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

Wenn `UpgradeState` = `Unknown` kann dies daran liegen, dass der auf dem VDA installierte Citrix VDA Upgrade Agent die Version nicht an den VDA Update Service gemeldet hat. Sie können mit dem Cmdlet `Get-VusComponentVersion` überprüfen, ob der VDA Komponentenversionen gemeldet hat.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Wenn keine Ergebnisse angezeigt werden, überprüfen Sie Folgendes:

- Der VDA ist Teil eines Katalog und einer Bereitstellungsgruppe.
- Der VDA Upgrade Agent ist auf dem VDA installiert und wird ausgeführt. Versuchen Sie bei Bedarf, den Agent neu zu starten.

**Hinweis**: Wenn weiterhin keine Ergebnisse angezeigt werden, sammeln Sie beim Neustart des VDA Upgrade Agent die Citrix Diagnostic Facility-Tracingberichte und beheben Sie die Probleme.

- VDA-Upgrades planen. Bevor Sie beginnen, sollten Sie Folgendes beachten:
  - `DurationInHours`: Dient zum Angeben der Dauer des Upgrade-Vorgangs in Stunden. VDAs im Katalog werden in den Wartungsmodus versetzt. Das VDA-Installationsprogramm

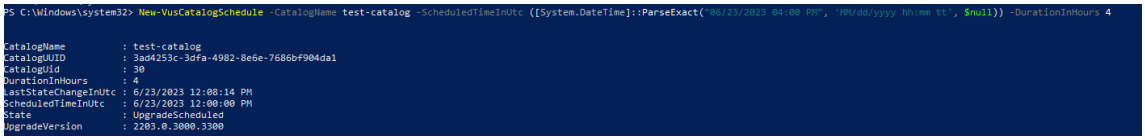
wird heruntergeladen und das Upgrade wird auf jedem VDA durchgeführt. Legen Sie eine längere Dauer fest, wenn der Katalog viele VDAs enthält.

- `UpgradeNow`: Verwenden Sie diesen Switch, um ein Upgrade sofort zu planen oder legen Sie `ScheduledTimeInUtc` fest.
- `ScheduledTimeInUtc`: Dient zum Planen eines Upgrades für ein bestimmtes Datum und eine bestimmte Uhrzeit.

Beispiel:

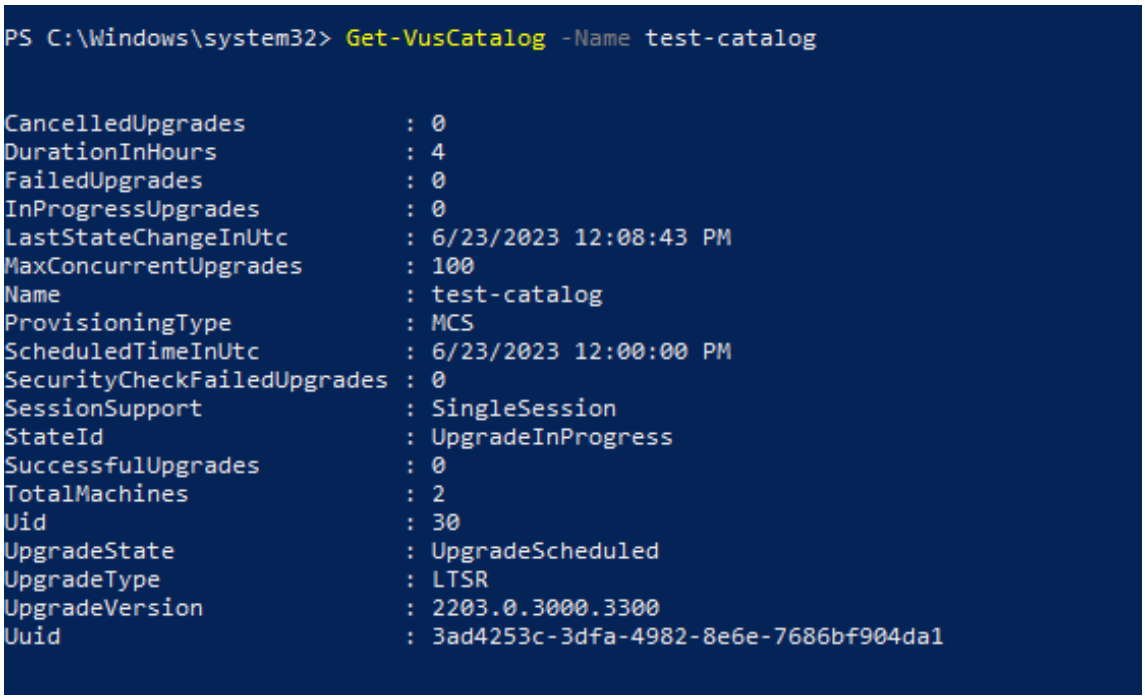
```
- New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc
  ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd
  /yyyy hh:mm tt', $null))-DurationInHours 4
```

Sie können Upgrades unter Verwendung von `CatalogName`, `Uid` und `Uuid` planen.




- Upgradestatus überprüfen. Verwenden Sie das Cmdlet `Get-VusCatalog` oder `Get-VusMachine`, um den VDA-Upgradestatus regelmäßig zu überprüfen. Verwenden Sie `MachineUuid`, `MachineUid` und `MachineName`, um die VDAs zu filtern.

  Beispiel:
  `–Get-VusCatalog -Name test-catalog`



Verwenden Sie `Get-VusMachine`, um den VDA-Upgradestatus jeder Maschine in einem Katalog anzuzeigen.

```
PS C:\Users\vaishakhb> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:17:33 PM
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

### Bei Installation einer persönlichen vDisk auf dem VDA

Wurde die PvD-Komponente (persönliche vDisk) jemals auf einem VDA installiert, kann dieser nicht auf Version 1912 LTSR oder höher aktualisiert werden, bis die Komponente entfernt wird.

Die ist auch dann erforderlich, wenn Sie PvD nie verwendet haben. Wie PvD eventuell in früheren Versionen installiert wurde:

- Auf der grafischen Benutzeroberfläche des VDA-Installationsprogramms war PvD eine Option (Kontrollkästchen auf der Seite **Zusätzliche Komponenten**). In den 7.x-Versionen bis 7.15 LTSR war diese Option standardmäßig aktiviert. Wenn Sie die Standardeinstellungen akzeptiert haben (oder die Option in einem Release explizit aktiviert haben), wurde PvD installiert.
- In der Befehlszeile wurde PvD über die Option `/baseimage` installiert. Wenn Sie diese Option angegeben oder ein Skript verwendet haben, das diese Option enthielt, wurde PvD installiert.

#### Aktion

Erkennt das VDA-Installationsprogramm die PvD-Komponente im aktuell installierten VDA nicht, wird das Upgrade fortgesetzt.

Erkennt das Installationsprogramm die PvD-Komponente im installierten VDA:

- **Grafische Benutzeroberfläche:** Das Upgrade wird angehalten. In einer Meldung werden Sie gefragt, ob die nicht unterstützten Komponente automatisch entfernt werden soll. Wenn Sie auf **OK** klicken, wird die Komponente automatisch entfernt und das Upgrade fortgesetzt.
- **CLI:** Der Befehl schlägt fehl, wenn das Installationsprogramm die PvD-Komponente erkennt. Um ein Fehlschlagen des Befehls zu vermeiden, schließen Sie die folgende Option im Befehl ein: `/remove_pvd_ack`.

Wenn Sie PvD auf Windows 10-Maschinen (bis 1607 ohne Updates) weiterverwenden möchten, ist VDA 7.15 LTSR die neueste unterstützte Version. Das Extended Support-Programm für XenApp und XenDesktop 7.15 LTSR deckt keine mit Citrix DaaS verwendeten VDAs ab. Weitere Informationen finden Sie unter Extended Support Customer Guide im Citrix Support Knowledge Center.

### Ältere Betriebssysteme

Der Artikel Systemanforderungen listet die unterstützten Windows-Betriebssysteme für VDAs der aktuellen Version auf.

- Informationen zu LTSR-VDAs finden Sie im Artikel zu den Systemanforderungen für Ihre LTSR-Version.
- Informationen zu Linux VDAs finden Sie in der Dokumentation zum Linux Virtual Delivery Agent.

Für Windows-Maschinen mit Betriebssystemen, unter denen eine VDA-Installation nicht mehr unterstützt wird, gibt es folgende Optionen.

In Nicht-WVD-Umgebungen:

- Erstellen Sie ein neues Image mit einer unterstützten Windows-Version und installieren Sie dann den neuen VDA.
- Ist es nicht möglich, die Images neu zu erstellen, Sie möchten aber das Betriebssystem aktualisieren, deinstallieren Sie den VDA, bevor Sie das Betriebssystem aktualisieren. Andernfalls wechselt der VDA in einen nicht unterstützten Zustand. Nach dem Upgrade des Betriebssystems installieren Sie den neuen VDA.
- Wenn auf einer Maschine Version 7.15 LTSR installiert ist und Sie versuchen, eine neuere Version zu installieren, werden Sie in einer Meldung darüber informiert, dass Sie die neueste unterstützte Version verwenden.
- Wenn auf der Maschine eine Version vor 7.15 LTSR installiert ist, werden Sie über eine Meldung auf die Informationen unter CTX139030 verwiesen. Sie können VDAs der Version 7.15 LTSR von der Citrix Website herunterladen.

# Konfiguration zu Citrix Cloud migrieren

March 30, 2024

## Gründe für die Verwendung der automatischen Konfiguration

IT-Administratoren, die für große oder komplexe Umgebungen zuständig sind, betrachten Migration oft als mühsamen Prozess. Häufig schreiben sie ihre eigenen Tools, um diese Aufgabe erfolgreich auszuführen, da sie in der Regel für ihre Anwendungsfälle spezifisch ist.

Citrix möchte die Migration durch Automatisierung mit dem Cmdlets des automatisiertes Konfigurationstools vereinfachen. Administratoren können mühelos aktuelle Konfigurationen in Citrix Cloud testen und die Vorteile von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) nutzen, während ihre aktuellen Umgebungen *intakt* bleiben. Es gibt zudem keine Auswirkungen auf Endbenutzer, da die automatische Konfiguration nahtlos im Hintergrund arbeitet. Zu diesen Vorteilen gehören neben anderen eine geringere administrative Überlastung, wenn Citrix einen Teil der Back-End- und Steuerungsebene verwaltet sowie automatische und anpassbare Updates von Citrix Cloud-Komponenten.

Citrix verwendet eine branchenübliche Konfiguration als Code, um einen Mechanismus zur Automatisierung von Migrationsprozessen bereitzustellen. Die automatische Konfiguration erkennt und exportiert eine oder mehrere On-Premises-Sites als Sammlung von Konfigurationsdateien. Die Konfiguration dieser Dateien kann dann in Citrix DaaS importiert werden.

Die automatische Konfiguration gibt Administratoren außerdem die Möglichkeit, mehrere On-Premises-Sites in einer einzigen Site zusammenzuführen und dabei Namenskonflikte zu vermeiden. Administratoren können steuern, ob Ressourcen durch die On-Premises- oder die Cloud-Konfiguration gesteuert werden.

Die automatische Konfiguration ist nicht nur ein einmaliges Migrationstool, sie kann auch die täglichen Konfigurationsaufgaben in Citrix Cloud automatisieren. Das Verschieben der Citrix DaaS-Konfiguration kann mehrere Vorteile bieten:

- Synchronisieren der Site von der Testumgebung in die Produktion
- Backup und Wiederherstellen Ihrer Konfiguration
- Ressourcenlimits werden erreicht
- Migration von Region zu Region

Das folgende *2-minütige* Video bietet einen kurzen Überblick über die automatische Konfiguration.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Weitere Informationen zur automatischen Konfiguration finden Sie unter Proof of Concept: Automated Configuration Tool in der Tech Zone.

Detaillierte Informationen zum Migrieren Ihrer Bereitstellung und zur Vorbereitung der Konfiguration auf die Migration finden Sie unter Migrieren der On-Premises-Version von Citrix Virtual Apps and Desktops zu Citrix Cloud in der Tech Zone.

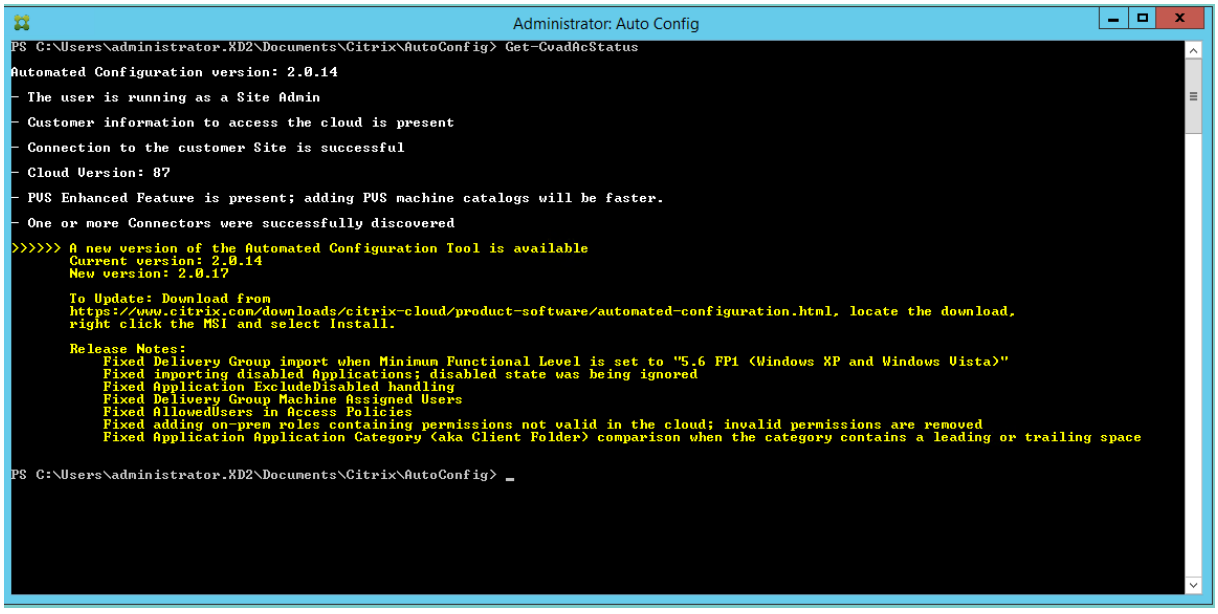
### Herunterladen der automatischen Konfiguration

Laden Sie das automatisierte Konfigurationstool von Citrix Downloads herunter und installieren Sie es.

> **Wichtig:**
>
> Verwenden Sie immer die neueste verfügbare Version der automatischen Konfiguration, um Funktionsfehler zu vermeiden.

### Upgrade der automatischen Konfiguration

Wenn Sie Cmdlets ausführen, die in der automatischen Konfiguration auf die Cloud zugreifen, erhalten Sie von dem Tool eine Benachrichtigung, wenn eine neuere Version zum Download verfügbar ist.




Sie können mit folgendem Verfahren sicherstellen, dass Sie über die neueste Version verfügen:

1. Doppelklicken Sie auf das Symbol **Automatisches Konfigurieren**. Ein PowerShell Fenster wird angezeigt.
2. Führen Sie den folgenden Befehl aus, um die Versionsnummer zu überprüfen.

```
Get-CvadAcStatus
```

3. Prüfen Sie Ihre Version gegen die der in der Warnung oder unter Citrix Downloads aufgeführten Version. Die neueste Version befindet sich dort.
4. Laden Sie die aktuelle Softwareversion des Tools von Citrix herunter und installieren Sie es. Sie müssen hierfür die alte Version *nicht* deinstallieren.

> **Hinweis:**
>
> Die Benachrichtigung wird jedes Mal angezeigt, wenn Sie ein Cmdlet ausführen, das auf die Cloud zugreift. Weitere Informationen zu Cmdlets finden Sie unter Cmdlets des automatisiertes Konfigurationstools.

### Bekannte Einschränkungen

- Für mit Maschinenerstellungsdiensten bereitgestellte Maschinenkataloge gelten besondere Überlegungen. Weitere Informationen zu MCS finden Sie unter Grundlegendes zur Migration von mit Maschinenerstellungsdiensten bereitgestellten Katalogen.

### Unterstützte Migrationsobjekte

Die automatische Konfiguration unterstützt das Verschieben der Konfiguration der folgenden Komponenten:

- Tags
- Delegierter Admin
  - Geltungsbereiche
  - Rollen
- Hostverbindungen
  - Ein einzelner Ressourcenpool
  - Admin-Geltungsbereiche
- Maschinenkataloge
  - Admin-Geltungsbereiche
  - Maschinen
  - Remote-PC-Zugriff, physisch, gepoolt, bereitgestellt, MCS, zugewiesen
- StoreFront
- Bereitstellungsgruppen
  - Zugriffsrichtlinie

  - Admin-Bereichszuweisung
  - Anwendungszugriffsrichtlinie
  - Zuweisungsrichtlinie
  - Anspruch-/Desktoprichtlinie
  - Energiezeitpläne
  - Sitzungsfortbestehen
  - Vorabstart von Sitzungen
  - Neustartzeitpläne
  - Tags
- Anwendungsgruppen
  - Admin-Bereichszuweisung
  - Bereitstellungsgruppen
  - Benutzer und Gruppen
- Anwendungen
  - Anwendungsordner
  - Symbole
  - Anwendungen
  - Per Broker konfigurierte FTAs
  - Tags
- Gruppenrichtlinien
- Benutzerzoneneinstellungen

### Reihenfolge der Komponentenmigration

Die Komponenten und ihre Voraussetzungen sind hier aufgelistet. Abhängigkeiten einer Komponente müssen vor dem Import oder dem Zusammenführen vorhanden sein. Wenn eine Voraussetzung fehlt, kann der Befehl zum Importieren oder Zusammenführen fehlschlagen. Im Abschnitt **Fixups** der Protokolldatei werden bei Fehlschlagen des Imports oder des Zusammenführens fehlende Voraussetzungen aufgelistet.

1. Tags
   - Keine Voraussetzungen
2. Delegierter Admin
   - Keine Voraussetzungen
3. Hostverbindungen
   - Sicherheitsinformationen in CvadAcSecurity.yml

4. Maschinenkataloge
    - In Active Directory vorhandene Maschinen
    - Hostverbindungen
    - Tags
5. StoreFront
6. Bereitstellungsgruppen
    - In Active Directory vorhandene Maschinen
    - In Active Directory vorhandene Benutzer
    - Maschinenkataloge
    - Tags
7. Anwendungsgruppen
    - Bereitstellungsgruppen
    - Tags
8. Anwendungen
    - Bereitstellungsgruppen
    - Anwendungsgruppen
    - Tags
9. Gruppenrichtlinien
    - Bereitstellungsgruppen
    - Tags
10. Benutzerzoneneinstellungen

## Allgemeine Voraussetzungen

Im Folgenden sind einige allgemeine Voraussetzungen aufgeführt, die erfüllt sein müssen, damit die automatische Konfiguration ordnungsgemäß funktioniert. Diese Voraussetzungen gelten sowohl für die Migration von On-Premises in die Cloud als auch für die Migration von Cloud zu Cloud.

### Generieren der Kunden-ID, der Client-ID und des geheimen Schlüssels

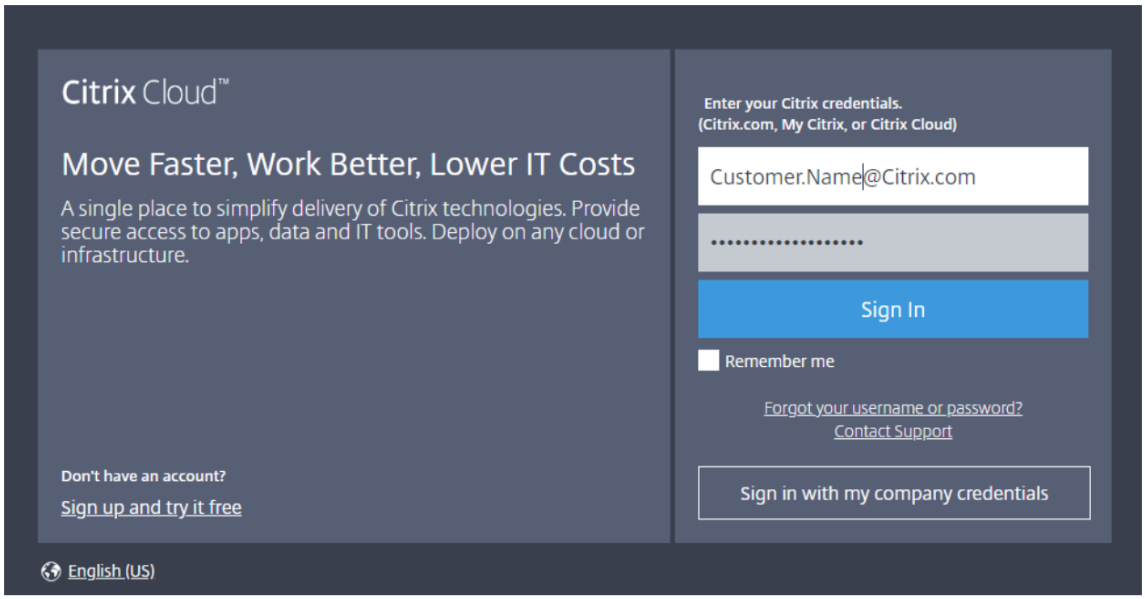
Vor dem Beginn der Migration über die automatischen Konfiguration benötigen Sie Ihre Citrix Cloud-Kunden-ID und müssen eine Client-ID sowie einen geheimen Schlüssel erstellen, um Ihre Konfiguration in Citrix Cloud zu importieren. Alle Cmdlets, die auf die Cloud zugreifen, benötigen diese Werte.

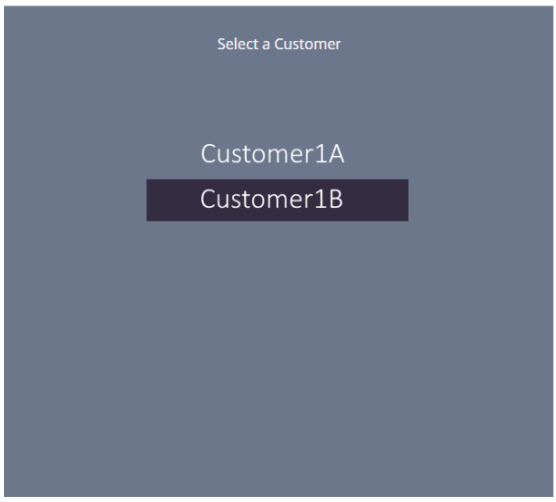
Mit dem folgenden Verfahren können Sie die Kunden-ID abrufen und die Client-ID und den geheimen Schlüssel erstellen.

Zum Abrufen der **Kunden-ID** gehen Sie wie folgt vor:

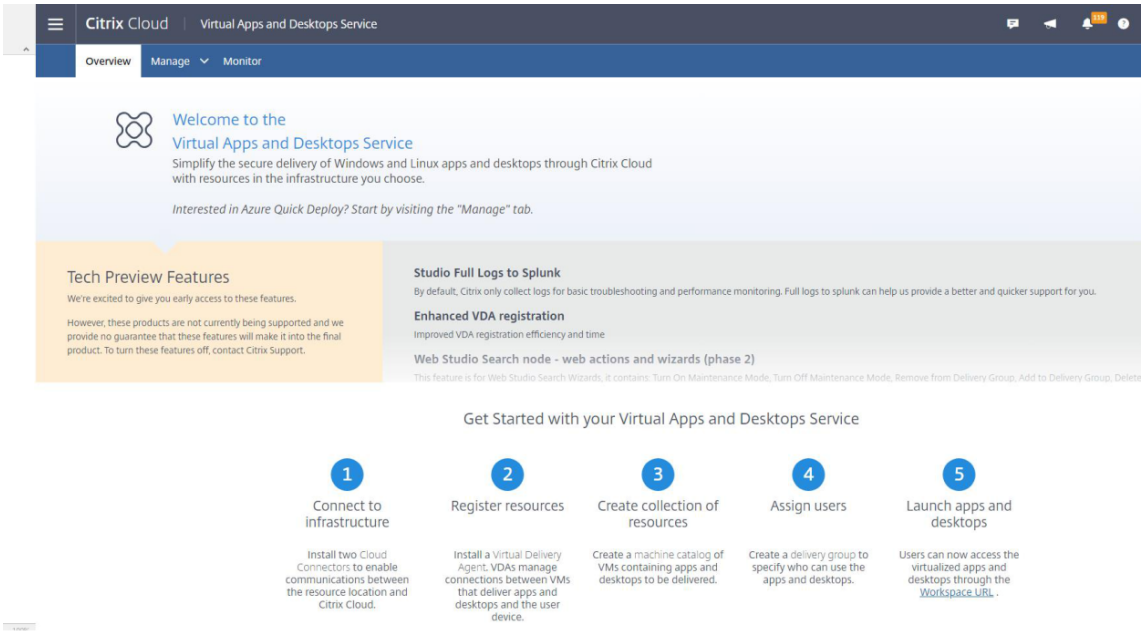
1. Melden Sie sich bei Ihrem Citrix Cloud-Konto an und wählen Sie den Kunden aus.

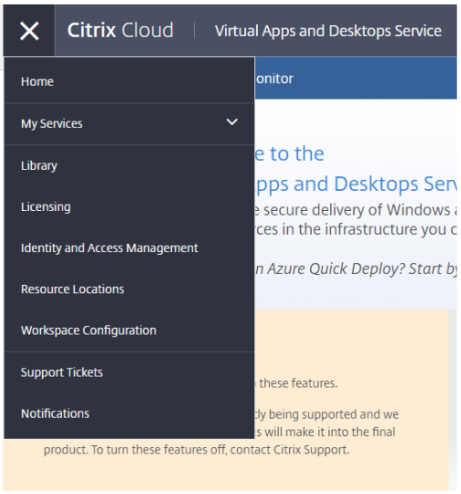


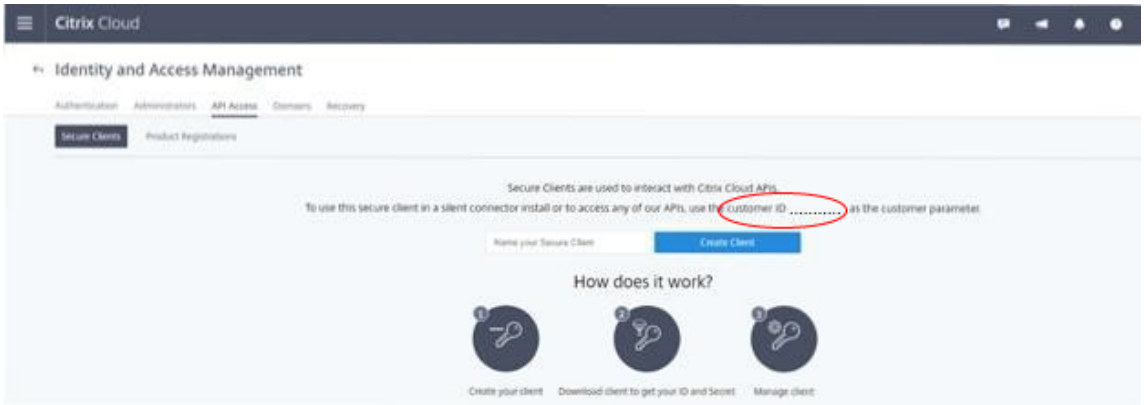

2. Klicken Sie auf das Hamburger-Menü und wählen Sie die Option **Identitäts- und Zugriffsverwaltung**.



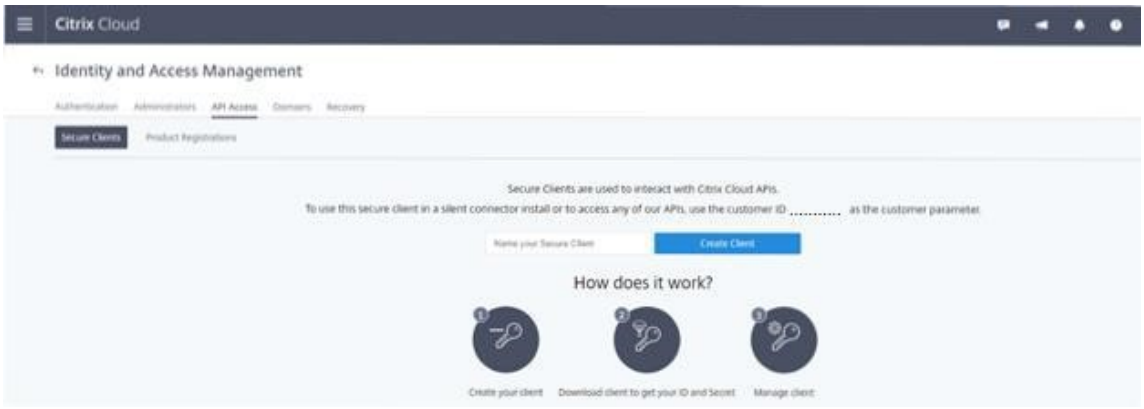

3. Die **Kunden-ID** ist auf der Seite **Identitäts- und Zugriffsverwaltung**.



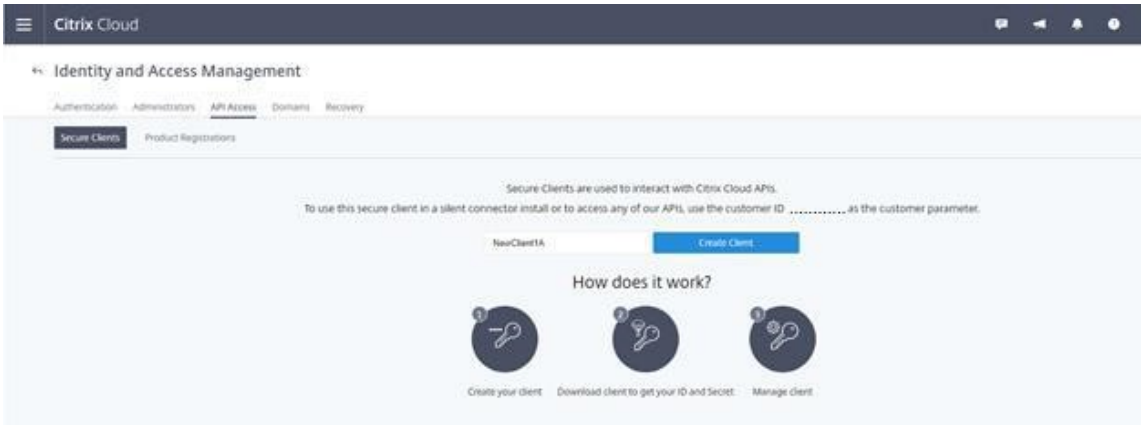

 

Zum Abrufen der **Client-ID** und des **geheimen Schlüssels** gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite **Identitäts- und Zugriffsverwaltung** auf **API-Zugriff**.

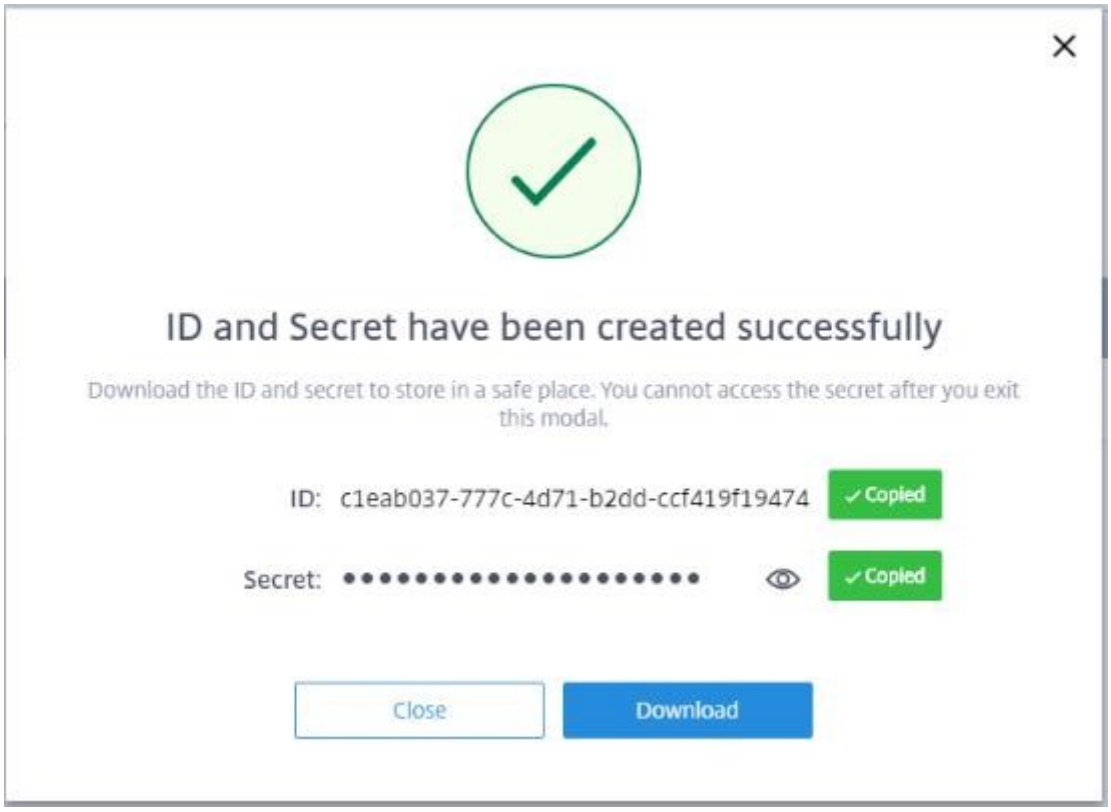



2. Geben Sie einen Namen in das Feld ein. Dieser Name wird zur Unterscheidung zwischen mehreren Client-IDs und geheimen Schlüsseln verwendet. Klicken Sie auf **Client erstellen**, um die Client-ID und den geheimen Schlüssel zu erstellen.

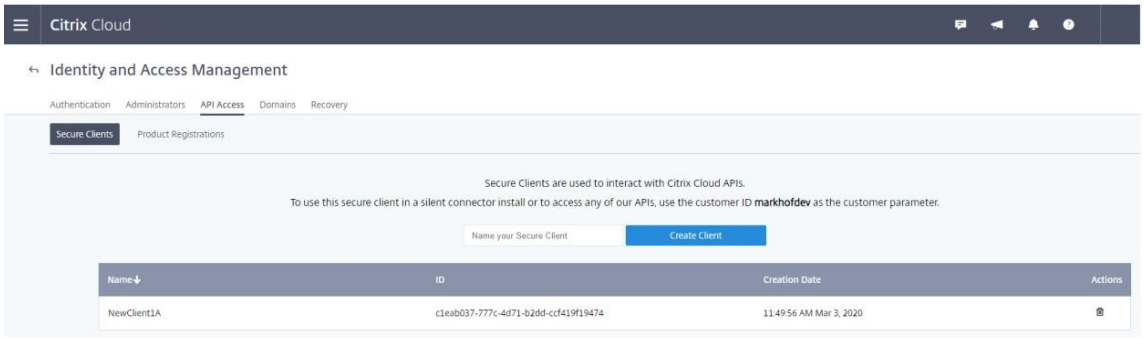



3. Wenn Sie die Client-ID und den geheimen Schlüssel erstellt haben, wird das folgende Dialogfeld angezeigt. Kopieren Sie beide Werte an einen sicheren Speicherort und laden Sie die CSV-Datei herunter, die diese Informationen enthält. Die CSV-Datei kann zum Erstellen der Datei CustomerInfo.yml verwendet werden.




4. Die Client-ID und der geheime Schlüssel werden erfolgreich erstellt.




Speichern Sie diese Werte an einem sicheren Ort und teilen Sie sie nur mit vertrauenswürdigen Personen im Unternehmen, die Zugriff auf das Tool oder auf die Cloud-Rest-APIs benötigen. Die Client-ID und der geheime Schlüssel laufen nicht ab. Werden sie kompromittiert, entfernen Sie sie sofort mit dem **Papierkorb**-Symbol und erstellen Sie neue.

> **Hinweis:**
>
> Der geheime Schlüssel kann nicht wiederhergestellt werden, wenn er verloren geht oder vergessen wird. Er muss zusammen mit der Client-ID und neu erstellt werden.

### Auffüllen der Kundeninformationsdatei

Die Verwendung der Datei CustomerInfo.yml macht das Hinzufügen von Kundeninformationen als Cmdlet-Parameter überflüssig. Jede Kundeninformation kann per Cmdlet-Parameter überschrieben werden.

Erstellen Sie die Datei CustomerInfo.yml mit dem Cmdlet `New-CvadAcCustomerInfoFile`.

> **Wichtig:**
>
> Bearbeiten Sie die Datei CustomerInfo.yml nicht manuell. Dies kann zu unbeabsichtigten Formatierungsfehlern führen.

`New-CvadAcCustomerInfoFile` hat die folgenden erforderlichen Parameter.

- CustomerId: Kunden-ID.
- ClientId: Client-ID des Kunden, die in Citrix Cloud erstellt wurde.
- Secret: Kundengeheimnis, das in Citrix Cloud erstellt wurde.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

Sie können die Datei CustomerInfo.yml auch über den Parameter `SecurityCsvFileSpec` erstellen, der auf die heruntergeladene Datei security.csv verweist. Sie müssen auch die CustomerID angeben.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads/security.csv -CustomerId markhof123
```

Aktualisieren Sie die Datei CustomerInfo.yml mit dem Cmdlet `Set-CvadAcCustomerInfoFile`. Dieses Cmdlet ändert nur die Client-ID.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

Nachfolgend sehen Sie das Beispiel einer CustomerInfo.yml-Datei.

```
# Created/Updated on 2020/01/29 16:46:47
CustomerId: 'markhof123'
ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
Secret: 'TwBLaaabbbaaaaaaaaaaw=='
Environment: Production
AltRootUrl: ''
StopOnError: False
AlternateFolder: ''
Locale: 'en-us'
Editor: 'C:\Program Files\Notepad++\notepad++.exe'
Confirm: True
DisplayLog: True
```

### Auffüllen der Zonenzuordnungsdatei

Die On-Premises-Zone entspricht dem Cloudressourcenstandort. Im Gegensatz zu anderen Sitekomponenten können Sie die On-Premises-Zone nicht automatisch in die Cloud importieren. Sie muss stattdessen manuell über die Datei ZoneMapping.yml zugeordnet werden. Importfehler können auftreten, wenn der Zonenname keinem bestehenden Ressourcenstandort zugewiesen ist.

Bei On-Premises-Sites mit nur einer Zone und Cloudsites mit nur einem Ressourcenstandort führt das automatisierte Konfigurationstool die richtige Zuordnung durch, sodass die ZoneMapping.yml-Datei nicht manuell verwaltet werden muss.

Bei On-Premises-Sites mit mehreren Zonen und bei Cloudsites mit mehreren Ressourcenstandorten muss die ZoneMapping.yml-Datei manuell aktualisiert werden, damit sie die korrekte Zuordnung von On-Premises-Zonen zu Cloud-Ressourcenstandorten widerspiegelt. Dies muss vor dem Import in die Cloud erledigt werden.

Die Datei ZoneMapping.yml ist in *%HOMEPATH%\Documents\Citrix\AutoConfig*. Die YML-Datei beinhaltet ein Wörterbuch mit dem Zonennamen als Schlüssel und dem Ressourcennamen als Wert.

Beispiel: Eine Citrix Virtual Apps and Desktops-On-Premises-Site mit der primären Zone “Zone-1”und der sekundären Zone “Zone-2”wird in eine Citrix DaaS-Bereitstellung mit den beiden neu erstellten Cloud-Ressourcenstandorten “Cloud-RL-1”und “Cloud-RL-2”migriert. In diesem Fall würde ZoneMapping.yml wie folgt konfiguriert:

```
1               Zone-1: Cloud-RL-1
2
3               Zone-2: Cloud-RL-2
```

> **Hinweis:**
>
> Ein Leerzeichen muss zwischen dem Doppelpunkt und dem Namen des Ressourcenstandorts stehen. Wenn ein Zonen- oder Ressourcenstandortname Leerzeichen enthält, setzen Sie den Namen in Anführungszeichen.

### Hostverbindungen

Hostverbindungen und die zugehörigen Hypervisoren können mit der automatischen Konfiguration exportiert und importiert werden.

Das Hinzufügen eines Hypervisors zu einer Hostverbindung erfordert Hypervisortyp-spezifische Sicherheitsinformationen. Diese Informationen können aus Sicherheitsgründen nicht aus der On-Premises-Site exportiert werden. Sie müssen die Informationen manuell bereitstellen, damit die automatische Konfiguration Hostverbindungen und Hypervisors in die Cloudsite importieren kann.

Beim Exportieren wird die Datei CvadAcSecurity.yml in *%HOMEPATH%\Documents\Citrix\AutoConfig* erstellt. Sie enthält Platzhalter für jedes für den spezifischen Hypervisortyp benötigte Sicherheitselement. Sie müssen die Datei CvadAcSecurity.yml vor dem Import in die Cloudsite aktualisieren. Administratorupdates werden über mehrere Exportvorgänge beibehalten und bei Bedarf neue Sicherheitsplatzhalter hinzugefügt. Sicherheitselemente werden nie entfernt. Weitere Informationen finden Sie unter Datei CvadAcSecurity.yml manuell aktualisieren.

```
            HostConn1:
            ConnectionType: XenServer
            UserName: root
            PasswordKey: rootPassword
            HostCon2:
            ConnectionType: AWS
            ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
            SecretKey: TwBLaaaaaaaaaaaaaaaaw==
            Region: East
```

**Hypervisor-spezifische Sicherheitsinformationen** Nachfolgend werden die für die einzelnen Hypervisortypen erforderlichen Sicherheitsinformationen aufgeführt.

- XenServer, Hyper-V, VMware
  - Benutzername
  - Klartextkennwort
- Microsoft Azure
  - Abonnement-ID
  - Anwendungs-ID
  - Anwendungsgeheimnis
- Amazon Web Services
  - Dienstkonto-ID
  - Anwendungsgeheimnis
  - Region

**Besondere Sicherheitsüberlegungen** Alle Sicherheitsinformationen werden als Klartext eingegeben. Wenn Klartext nicht empfohlen wird, können die Hostverbindungen und die zugehörigen Hypervisors manuell über die Oberfläche **Verwalten > Vollständige Konfiguration** erstellt werden. Die Namen von Hostverbindungen und Hypervisors müssen mit ihrem On-Premises-Gegenstück übereinstimmen, damit Maschinenkataloge, die die Hostverbindungen verwenden, erfolgreich importiert werden.

### Aktivieren der Sites

Der Delivery Controller steuert in On-Premises- und Cloudsites Ressourcen wie das Brokering von Desktops und Anwendungen und den Neustart von Maschinen. Probleme treten auf, wenn Ressourcen von zwei oder mehr Sites gesteuert werden. Eine solche Situation kann bei der Migration von einer On-Premises-Site zu einer Cloudsite auftreten. On-Premises- und Cloud-Delivery Controller können die gleichen Ressourcen verwalten. Eine solche duale Verwaltung kann dazu führen, dass Ressourcen nicht mehr verfügbar sind oder nicht mehr verwaltet werden können und dass eine Diagnose schwierig wird.

Durch die Siteaktivierung können Sie vorgeben, wo die aktive Site gesteuert wird.

Die Siteaktivierung wird über den Bereitstellungsgruppen-Wartungsmodus verwaltet. Bereitstellungsgruppen werden in den Wartungsmodus versetzt, wenn die Site inaktiv ist. Der Wartungsmodus wird Bereitstellungsgruppen in aktiven Sites beendet.

Die Siteaktivierung hat weder Einfluss auf die VDA-Registrierung und Maschinenkataloge noch erfolgt durch sie eine Verwaltung dieser Objekte.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

Alle Cmdlets unterstützen `IncludeByName` und `ExcludeByName` Filter. Über diesen Parameter können Sie vorgeben, bei welchen Bereitstellungsgruppen der Wartungsmodus geändert werden kann. Bereitstellungsgruppen können bei Bedarf selektiv geändert werden.

#### Importieren und Übertragen der Steuerung in die Cloud

Im Folgenden finden Sie eine allgemeine Beschreibung des Verfahrens zum Importieren und Übertragen der Steuerung von der On-Premises-Site in die Cloudsite.

1. Exportieren und importieren Sie die On-Premises-Site in die Cloud. Stellen Sie sicher, dass der Parameter `–SiteActive` in keinem der Cmdlets zum Importieren verwendet wird. Die On-Premises-Site ist aktiv und die Cloudsite inaktiv. Standardmäßig befinden sich Cloudsite-Bereitstellungsgruppen im Wartungsmodus.
2. Überprüfen Sie den Inhalt und die Konfiguration der Cloud.
3. Legen Sie die On-Premises-Site außerhalb der Geschäftszeiten auf inaktiv fest. Der Parameter `–SiteActive` darf nicht vorhanden sein. Alle Bereitstellungsgruppen der On-Premises-Site sind im Wartungsmodus.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Legen Sie die Cloudsite auf aktiv fest. Der Parameter `–SiteActive` muss vorhanden sein. Keine Cloudsite-Bereitstellungsgruppe ist im Wartungsmodus.

- `Set-CvadAcSiteActiveStateCloud –SiteActive`

5. Vergewissern Sie sich, dass die Cloudsite aktiv und die On-Premises-Site inaktiv ist.

#### Rückübertragen der Steuerung in die On-Premises-Site

Zum Rückübertragen der Steuerung von der Cloudsite in die On-Premises-Site gehen Sie folgendermaßen vor:

1. Legen Sie die Cloudsite außerhalb der Geschäftszeiten auf inaktiv fest. Alle Cloudsite-Bereitstellungsgruppe sind im Wartungsmodus.
   - `Set-CvadAcSiteActiveStateCloud`
2. Legen Sie die On-Premises-Site auf aktiv fest. Keine Bereitstellungsgruppe der On-Premises-Site ist im Wartungsmodus.
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

#### Zusätzliche Informationen zur Siteaktivierung

- Sind keine Maschinen energieverwaltet und gibt es keine Neustartzeitpläne (was normalerweise bedeutet, dass keine Hostverbindungen bestehen), können alle Cloud-Bereitstellungsgruppen als aktiv importiert werden. Fügen Sie `-SiteActive` zu `Merge-CvadAcToSite`/`Import-CvadAcToSite` hinzu oder führen Sie nach dem Importieren `Set-CvadAcSiteActiveStateCloud -SiteActive` aus.
- Gibt es energieverwaltete Maschinen oder Neustartpläne, ist ein anderer Prozess erforderlich. Legen Sie in diesem Fall beispielsweise beim Umstieg von einer On-Premises-Bereitstellung zur Cloud die On-Premises-Site mit `Set-CvadAcSiteActiveStateOnPrem` auf inaktiv fest. Legen Sie dann die Cloudsite mit `Set-CvadAcSiteActiveStateCloud -SiteActive` auf aktiv fest.
- Die Cmdlets `Set-CvadAcSiteActiveStateCloud` und `Set-CvadAcSiteActiveStateOnPrem` werden auch verwendet, um den Prozess umzukehren. Führen Sie beispielsweise `Set-CvadAcSiteActiveStateCloud` ohne den Parameter `-SiteActive` aus und dann `Set-CvadAcSiteActiveStateOnPrem` mit dem Parameter `-SiteActive`.

### Grundlegendes zur Migration von mit Maschinenerstellungsdiensten bereitgestellten Katalogen

> **Hinweis:**
>
> Dieses Feature ist nur ab Version 3.0 verfügbar. Zur Überprüfung der Version verwenden Sie `Get`

> –`CvadAcStatus` in der automatischen Konfiguration.

MCS-Kataloge erstellen zwei verschiedene Arten von Katalogen:

- Wenn Änderungen an einer Maschine verloren gehen/rückgängig gemacht werden (üblicherweise Server-OS, wo Anwendungen veröffentlicht werden). Dies ist ein gepoolte VDI-/Multisitzung-Anwendungsfall.
- Wenn Änderungen an einer Maschine während des Neustarts beibehalten werden (üblicherweise Client-Betriebssystem mit einem dedizierten Benutzer). Dies ist ein Anwendungsfall für statische VDI.

Der Katalogtyp kann im Katalogknoten in Citrix Studio und anhand des Werts "Benutzerdaten:"des Katalogs überprüft werden.

> **Hinweis:**
>
> Ein Backup der MCS aus der Cloud kann nicht mit der automatischen Konfiguration durchgeführt werden.

#### Gepoolte VDI-/Multisitzungskataloge

Kataloge mit "Benutzerdaten: Verwerfen"sind gepoolte VDI-Kataloge und können nur das Hauptimage und die Konfiguration migrieren. Virtuelle Maschinen in diesen Katalogen werden von der Migration ausgeschlossen. Das liegt daran, dass der Lebenszyklus der virtuellen Maschine von der Site verwaltet wird, von der Sie importieren, was bedeutet, dass sich der Status bei jedem Einschalten der Maschinen ändern kann. Dies macht den Import unmöglich, da die Synchronisierung der Importdaten für die virtuellen Maschinen schnell verloren geht.

Wenn Sie diese Kataloge mit dem Tool migrieren, erstellt das Tool Katalogmetadaten und initiiert die Erstellung des Hauptimages, es werden jedoch keine Maschinen importiert.

Da dieser Prozess je nach der Größe des Hauptimages einige Zeit dauern kann, startet der Importbefehl innerhalb des Tools die Katalogerstellung mit MCS nur, wartet jedoch nicht, bis sie abgeschlossen ist. Überwachen Sie nach Abschluss des Imports den Fortschritt der Katalogerstellung über die Schnittstelle für die vollständige Konfiguration in der Cloud-Bereitstellung.

Sobald das Hauptimage erstellt wurde, können Sie Maschinen bereitstellen. Es müssen Kapazitätsüberlegungen berücksichtigt werden, da Kapazität aus der On-Premises-Nutzung verbraucht wird.

Alle anderen Objekte (Bereitstellungsgruppen/Anwendungen/Richtlinien usw.), die diesen Katalog verwenden, können importiert werden und müssen nicht auf die Erstellung des Hauptimages warten. Wenn die Erstellung des Katalogs abgeschlossen ist, können Maschinen zum importierten Katalog hinzugefügt werden, und dann können Benutzer ihre Ressourcen starten.

> **Hinweis:**
>
> Verwenden Sie dieselben im Tool verfügbaren Befehle zur Migration von Katalogen und allen anderen Objekten.

#### Statische VDI-Kataloge

> **Hinweis:**
>
> Da dieser Vorgang Low-Level-Details importiert, die in der Datenbank gespeichert sind, muss dieser Prozess von einer Maschine mit Datenbankzugriff ausgeführt werden.

Statische VDI-Kataloge migrieren das Hauptimage, die Konfigurationen und alle virtuellen Maschinen. Im Gegensatz zum Anwendungsfall für gepoolte VDI müssen keine Images erstellt werden.

Die VDAs müssen auf den Connector verweisen, damit sie sich bei der Cloud registrieren können.

Aktivieren Sie die Cloudsite anhand der Informationen im Abschnitt Aktivieren der Sites, damit der Neustartzeitplan, die Energieverwaltung und andere Elemente von der Cloud gesteuert werden.

Wenn Sie nach Abschluss der Migration diesen Katalog von Ihrer On-Premises-Site löschen möchten, müssen Sie die Option zum Belassen des VM- und AD-Kontos auswählen. Andernfalls werden sie gelöscht und die Cloudsite würde auf die gelöschte VM verweisen.

### Aktualisieren Sie die MCS-Tags, um verwaiste Ressourcen nach der Migration zu erkennen

Nachdem Sie von der On-Premises-Konfiguration zu einer Cloudsite oder von Ihrer Cloudkonfiguration zu einer anderen Cloudsite migriert haben, müssen Sie bei persistenten VMs die MCS-Site-ID-Tags aktualisieren, damit verwaiste Ressourcen korrekt erkannt werden können. Verwenden Sie dazu den PowerShell-Befehl `Set-ProvResourceTags`. Derzeit ist dieses Feature für Azure verfügbar.

Verfahren:

1. Aktualisieren Sie die MCS-Site-ID-Tags von der neuen Citrix-Site mit dem PowerShell-Befehl `Set-ProvResourceTags`. Beispiel:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <
       String>] [-VMBatchSize XX] [-ResourceType XX]
   <!--NeedCopy-->
   ```

   Oder

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <
       String>] [-VMBatchSize XX] [-ResourceType XX]
   <!--NeedCopy-->
   ```

Die Parameterdetails lauten wie folgt:

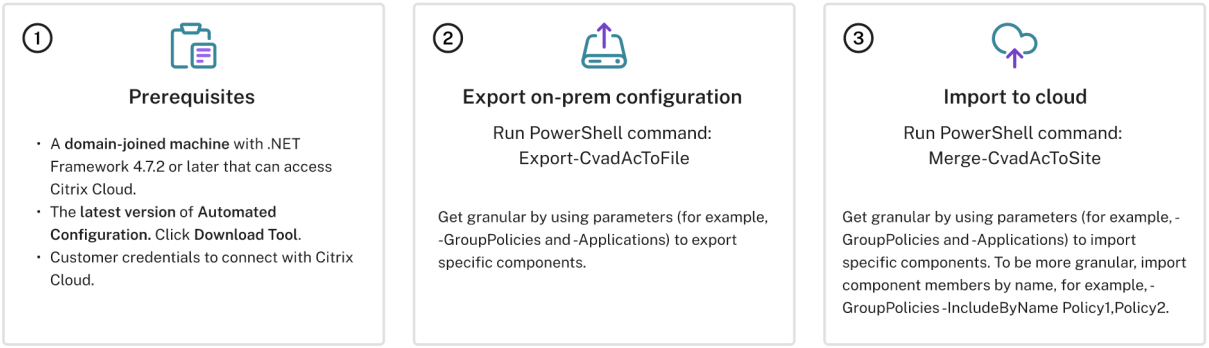
- `ProvisioningSchemeUid` oder `ProvisioningSchemeName` ist ein obligatorischer Parameter.
- `VMName` ist ein optionaler Parameter. Wenn kein `VMName` angegeben ist, werden die Tags aller virtuellen Maschinen dieses Maschinenkatalogs aktualisiert.
- `VMBatchSize` ist ein optionaler Parameter, um alle VMs in Stapel aufzuteilen. Wenn kein `VMBatchSize` angegeben ist, wird der Standardwert (10) angewendet. Der Bereich liegt zwischen 1 und 60.
- `ResourceType` kann einer der folgenden sein:
  - `MachineCatalog`: Zum Aktualisieren von Tags von Maschinenkatalogressourcen.
  - `VirtualMachine`: Zum Aktualisieren von Tags von VM-bezogenen Ressourcen.
  - `All`: (default ResourceType): Zum Aktualisieren von Tags sowohl des Maschinenkatalogs als auch der VM-bezogenen Ressourcen.

## Migration von on-premises in die Cloud

May 17, 2024

Mit der automatischen Konfiguration können Sie das Verschieben der On-Premises-Konfiguration zu einer Cloud-Site automatisieren.

Die folgende Abbildung zeigt eine Übersicht darüber, wie die automatische Konfiguration bei der Migration Ihrer Konfiguration in die Cloud helfen kann.




### Voraussetzungen für die Migration Ihrer Konfiguration

Zum *Exportieren* der Citrix Virtual Apps and Desktops-Konfiguration benötigen Sie:

- Aktuelle Version von Citrix Virtual Apps and Desktops und unmittelbare Vorgängerversion oder Citrix Virtual Apps and Desktops/XenApp und XenDesktop LTSR: alle Versionen
- Eine in die Domäne eingebundene Maschine mit .NET Framework 4.7.2 oder höher und dem Citrix PowerShell SDK. Dieses wird automatisch auf dem Delivery Controller installiert. (Wenn Sie es auf einer anderen Maschine als dem On-Premises-Delivery Controller ausführen möchten, muss Citrix Studio installiert sein, da mit Studio die richtigen PowerShell-Snap-Ins installiert werden. Das Studio-Installationsprogramm ist auf dem Citrix Virtual Apps and Desktops-Installationsmedium.)

Zum *Importieren* der Konfiguration in Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) benötigen Sie:

- Eine Maschine mit Zugriff auf Citrix Cloud. Dabei muss es sich weder um einen Delivery Controller noch um eine mit der Domäne verbundene Maschine handeln.
- Bereitgestelltes Citrix DaaS.
- Ein aktiver Ressourcenstandort mit installiertem Connector; er muss derselben Domäne angehören wie die On-Premises-Bereitstellung.
- Verbindung zu Sites, die auf Citrix Cloud zugreifen, muss zulässig und verfügbar sein. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.

> **Hinweis:**
>
> Die automatische Konfiguration kann nicht auf einem Cloud Connector-System installiert werden.

### Exportieren der On-Premises-Konfiguration von Citrix Virtual Apps and Desktops

> **Wichtig:**
>
> - Sie müssen eine CustomerInfo.yml-Datei mit Ihrer Kunden-ID, Client-ID und dem geheimen Schlüssel haben. Informationen zum Abrufen der Kunden- und Client-ID und des geheimen Schlüssels finden Sie unter Generieren der Kunden-ID, der Client-ID und des geheimen Schlüssels. Weitere Informationen zum Einfügen dieser Informationen in die Datei CustomerInfo.yml finden Sie unter Auffüllen der Kundeninformationsdatei.
> - Die Datei ZoneMapping.yml muss Informationen zur Zuordnung der On-Premises-Zone zu den Ressourcenstandorten in der Cloud enthalten. Weitere Informationen über die Zuordnung von Zonen finden Sie unter Auffüllen der Zonenzuordnungsdatei.
> - Wenn Sie Hostverbindungen haben, müssen Sie die entsprechenden Informationen in CvadAcSecurity.yml eingeben.

1. Installieren Sie die automatische Konfiguration.
2. Doppelklicken Sie auf das Symbol **Automatisches Konfigurieren**. Ein PowerShell Fenster wird angezeigt.

3. Führen Sie den folgenden Befehl aus, um alle Komponenten zu exportieren. Durch Exportieren der On-Premises-Konfiguration wird die Konfiguration *nicht* geändert.

   ```
   Export-CvadAcToFile
   ```

Nach der ersten Ausführung eines Cmdlets wird ein Exportordner mit den YML-Konfigurationsdateien und Protokollen erstellt. Der Ordner ist in *%HOMEPATH%\Documents\Citrix\AutoConfig*. Jeder nachfolgende Export erstellt einen Unterordner. Der übergeordnete Ordner *%HOMEPATH%\Documents\Citrix\AutoConfig* enthält immer die Dateien aus dem zuletzt ausgeführten Export.

> **Hinweis:**
>
> Wenn die automatische Konfiguration nicht auf dem Delivery Controller installiert ist, führen Sie `import-module Citrix.AutoConfig.Commands` aus, bevor Sie das Tool über PowerShell verwenden. Dieser Schritt ist nicht erforderlich, wenn Sie die automatische Konfiguration über das **Auto-Konfig**-Symbol öffnen.

Bei Auftreten von Fehlern oder Ausnahmen konsultieren Sie den Abschnitt **Fixups** in der Protokolldatei.

### Importieren der Konfiguration in Citrix DaaS

> **Wichtig:**
>
> - Sie müssen eine CustomerInfo.yml-Datei mit Ihrer Kunden-ID, Client-ID und dem geheimen Schlüssel haben. Informationen zum Abrufen der Kunden- und Client-ID und des geheimen Schlüssels finden Sie unter Generieren der Kunden-ID, der Client-ID und des geheimen Schlüssels. Weitere Informationen zum Einfügen dieser Informationen in die Datei CustomerInfo.yml finden Sie unter Auffüllen der Kundeninformationsdatei.
> - Die Datei ZoneMapping.yml muss Informationen zur Zuordnung der On-Premises-Zone zu den Ressourcenstandorten in der Cloud enthalten. Weitere Informationen über die Zuordnung von Zonen finden Sie unter Auffüllen der Zonenzuordnungsdatei.
> - Wenn Sie Hostverbindungen haben, müssen Sie die entsprechenden Informationen in CvadAcSecurity.yml eingeben.
> - Stellen Sie bei der Migration einer On-Premises-Bereitstellung in die Cloud sicher, dass die Domänen- und Organisationseinheits-GPOs, die die Citrix-Einstellungen enthalten, in die Cloud migriert werden. Citrix Web Studio unterstützt GPMC nicht und daher sind die Domänen- und Organisationseinheits-GPOs im Web Studio nicht sichtbar. Die Citrix-Richtlinienengine erzwingt die Domänen- und Organisationseinheits-GPOs auf VDAs und Benutzern, die sich in den Domänen und Organisationseinheiten befinden. Nach der Anmeldung bei einem VDA sieht ein Benutzer möglicherweise, dass die Richtlinien der Domänen- und Organisationseinheits-GPOs auf seine Sitzung angewendet werden.

> Administratoren können diese Richtlinien und Einstellungen jedoch nicht sehen, was zu Verwirrung führen kann.

#### Ausführen eines Imports

1. Doppelklicken Sie auf das Symbol **Automatisches Konfigurieren**. Ein PowerShell Fenster wird angezeigt.
2. Führen Sie den folgenden Befehl aus, um alle Komponenten zu importieren.

   ```
   Merge-CvadAcToSite
   ```

Überprüfen Sie den erwarteten Zustand gegen den neuen aktuellen Zustand. Importoptionen steuern, ob die Importergebnisse mit der On-Premises-Site identisch oder eine Teilmenge davon sind.

Nach der Ausführung eines Cmdlets wird ein Exportordner mit den YML-Konfigurationsdateien und Protokollen erstellt. Der Ordner ist in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Bei Auftreten von Fehlern oder Ausnahmen konsultieren Sie den Abschnitt **Fixups** in der Protokolldatei.

> **Hinweis:**
>
> Wenn die automatische Konfiguration nicht auf dem Delivery Controller installiert ist, führen Sie `import-module Citrix.AutoConfig.Commands` aus, bevor Sie das Tool über PowerShell verwenden. Dieser Schritt ist nicht erforderlich, wenn Sie die automatische Konfiguration über das **Auto-Konfig**-Symbol öffnen.

Informationen zum Wiederherstellen der ursprünglichen Citrix DaaS-Konfiguration finden Sie unter Sichern der Citrix DaaS-Konfiguration.

### Importvorgang im Einzelnen

Beim Import werden Updates präzise durchgeführt, es werden nur die erforderlichen Updates durchgeführt und es wird überprüft, ob alle Updates korrekt durchgeführt wurden. Bei allen Importvorgängen werden folgende Schritte ausgeführt.

1. Lesen der exportierten YML-Datei (erwarteter Zustand).
2. Lesen der Cloud (aktueller Zustand).
3. Backup des Cloudzustands vor Import in YML-Dateien (das Backup kann bei Bedarf wiederhergestellt werden).
4. Bewerten der Unterschiede zwischen erwartetem und aktuellem Zustand. Dies bestimmt, welche Aktualisierungen erforderlich sind.
5. Ausführen der Aktualisierungen.

6. Erneutes Lesen der Cloud (neuer aktueller Zustand).
7. Backup des Cloudzustands nach Import in YML-Dateien (das Backup kann bei Bedarf wiederhergestellt werden).
8. Vergleich des erwarteten Zustands und des neuen aktuellen Zustands.
9. Meldung der Vergleichsergebnisse.

### Granulare Migration

> **Wichtig:**
>
> Weitere Informationen zur Reihenfolge der Komponentenmigration finden Sie unter Reihenfolge der Komponentenmigration.

Sie haben die Möglichkeit der selektiven Migration von nur Komponenten oder sogar nur Komponentennamen.

- Zu den unterstützten Komponentenparametern gehören u. a. `MachineCatalogs` und `Tags`.
- Zu den unterstützten Komponentennamenparametern gehören `IncludeByName` und `ExcludeByName`.

Weitere Informationen zu Parametern und deren Verwendung finden Sie unter Parameter für granulare Migration.

### Aktivieren der Sites

Durch die Siteaktivierung können Sie vorgeben, welche Site aktiv ist und Ihre Ressourcen steuert. Weitere Informationen zum Aktivieren von Sites finden Sie unter Aktivieren von Sites.

## Zusammenführen mehrerer Sites

March 30, 2024

Die Multisite-Unterstützung für die automatische Konfiguration bietet eine Methode zum Zusammenführen mehrerer On-Premises-Sites in eine Cloudsite.

Dabei werden den Komponentennamen jeder On-Premises-Site eindeutige Präfixe und Suffixe hinzugefügt, sodass nach der Zusammenführung für Namenseindeutigkeit gesorgt ist.

Präfixe und Suffixe können für jede der folgenden Komponenten pro On-Premises-Site zugewiesen werden.

- `AdminScope`

- AdminRole
- ApplicationAdmin
- ApplicationFolder
- ApplicationGroup
- ApplicationUser
- DeliveryGroup
- GroupPolicy
- HostConnection
- MachineCatalog
- StoreFront
- Tag

Anwendungsordner unterstützen Präfixe, Suffixe und die Modifizierung des Stammordners. Bei der Modifizierung des Stammordners erhält die bestehende Ordnerstruktur einer Anwendung einen zusätzlichen Ordner auf oberster Ebene.

### Regeln für Präfixe und Suffixe

1. Präfixe und Suffixe dürfen keines der folgenden Sonderzeichen enthalten: `\ , / ; : # . * ? = < > | ( )"' { } [ ]`
2. Präfixe und Suffixe dürfen Leerzeichen am Ende enthalten, nicht aber am Anfang.
3. Präfixe und Suffixe mit Leerzeichen am Ende müssen in Anführungszeichen gestellt werden.
4. Präfixe und Suffixe werden beim Import, der Zusammenführung und beim Hinzufügen angewendet. Die Quell-YML-Dateien werden niemals geändert.
5. Bei dem Prozess werden nach Bedarf die Namen abhängiger Komponentennamen automatisch mit Präfixen oder Suffixen versehen. Wird beispielsweise Maschinenkatalognamen das Präfix “Ost”vorangestellt, erhalten Bereitstellungsgruppen, die auf sie verweisen, ebenfalls das Präfix “Ost”.
6. Wenn ein Komponentenname bereits mit dem Präfix oder Suffix beginnt, wird kein Präfix oder Suffix hinzugefügt. Komponentennamen dürfen keine zwei identischen Präfixe bzw. Suffixe enthalten.
7. Präfixe und Suffixe können einzeln oder in Kombination verwendet werden.
8. Die Verwendung eines Präfixes oder Suffixes für eine Komponente ist optional.

> **Hinweis:**
>
> Die Oberfläche der vollständigen Konfiguration zeigt Komponenten in alphabetischer Reihenfolge an.

#### Gruppieren nach Site

Verwenden Sie Präfixe, um Komponenten einer Site visuell zu gruppieren. Jede Site wird als Gruppe aufgeführt, wobei die Reihenfolge der Sitegruppen alphabetisch nach Präfix gesteuert wird.

#### Gruppieren nach Namen

Verwenden Sie Suffixe, um ähnlich benannte Komponenten aus mehreren Sites visuell zu gruppieren. Ähnlich benannte Komponenten verschiedener Sites werden abwechselnd angezeigt.

#### SitePrefixes.yml-Datei

Die Datei SiteMerging.yml enthält die Präfix- und Suffix-Zuordnung für eine oder mehrere On-Premises-Sites. Sie können die Datei "SiteMerging.yml"manuell oder mithilfe der im Abschnitt Cmdlets für das Zusammenführen mehrerer On-Premises-Sites aufgeführten Cmdlets verwalten.

#### Exportieren, Importieren, Zusammenführen und Hinzufügen

Die Zusammenführung kann erst beginnen, wenn Sie eine On-Premises-Site exportiert haben. Informationen zum Exportieren einer On-Premises-Site finden Sie unter Migration von on-premises in die Cloud.

#### Zentraler Exportzielordner

Bei den in diesem Abschnitt beschriebenen Verfahren werden die Exporte mehrerer Sites in eine zentrale Dateifreigabe exportiert. Die Dateien SiteMerging.yml file und CustomerInfo.yml sowie alle Exportdateien befinden sich in der Dateifreigabe, sodass der Import aus diesem von den On-Premises-Sites unabhängigen Speicherort aus möglich ist.

Vorgänge, bei denen auf die Cloud zugegriffen wird, verweisen nie auf die On-Premises-Sites oder Active Directory, sodass Sie solche Vorgänge ortsunabhängig durchführen können.

### Direkte Dateifreigabe

Die Operationen zum Exportieren, Importieren, Zusammenführen und Erstellen/Hinzufügen bieten einen Parameter zur Auswahl eines anderen Ordners als des Standardordners *%HOMEPATH%\Documents\Citrix\AutoConfig* als Ziel oder Quelle. In den folgenden Beispielen wird eine zentrale Dateifreigabe auf `\\share.central.net` verwendet, auf die der Administrator bereits Zugriff hat.

Zum Exportieren in einen sitespezifischen Ordner verwenden Sie den Parameter `–TargetFolder` :

Aus dem Desktop Delivery Controller "East":

```
mkdir \\share.central.net\AutoConfig\SiteEast

Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteEast
```

Aus dem Desktop Delivery Controller "West":

```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteWest
```

Nach Abschluss des Exports erstellen Sie die Dateien CustomerInfo.yml und SiteMerging.yml und speichern sie in `\\share.central.net\AutoConfig`.

> **Hinweis:**
>
> Verwenden Sie bei dem Verfahren mit direktem Dateifreigabeverweis beim Erstellen von SitePrefixes.yml nicht den Parameter `SiteRootFolder`.

Zum Importieren, Zusammenzuführen oder Hinzufügen aus der direkten Dateifreigabe müssen Sie entscheiden, von welcher Maschine aus Sie den Cloudzugriffsvorgang durchführen möchten. Die folgenden Optionen sind verfügbar:

- Eine On-Premises-Desktop Delivery Controller, auf dem das Tool installiert ist.
- Die Maschine, auf der die Dateifreigabe gehostet wird.
- Eine andere Maschine.

Die automatische Konfiguration muss auf der Maschine installiert sein, die auf die Cloud zugreift. Weder das On-Premises-PowerShell SDK, der Desktop Delivery Controller noch Active Directory werden verwendet, sodass die Anforderungen für den Zugriff auf die Cloud zur Ausführung einfacher sind als beim Export.

Zusammenführen des Desktop Delivery Controllers "East"in die Cloud:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \\share.central.
net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Zusammenführen des Desktop Delivery Controllers "West"in die Cloud:

```
Merge-CvadAcToSite –SiteName West –SourceFolder \\share.central.
net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Nachfolgend sehen Sie das Muster der im vorherigen Beispiel verwendeten SitePrefixes.yml-Datei.

```
    East:
      SiteRootFolder: "" # Important: leave this empty
      AdminScopePrefix: "East_"
      AdminRolePrefix: "East_"
      ApplicationAdminPrefix: "East_"
      ApplicationFolderPrefix: "" # Note that a new parent root folder
         is used instead
      ApplicationFolderRoot: "East"
      ApplicationGroupPrefix: "East_"
      ApplicationUserPrefix: "East_"
      DeliveryGroupPrefix: "East_"
      GroupPolicyPrefix: "East_"
      HostConnectionPrefix: "East_"
      MachineCatalogPrefix: "East_"
      StoreFrontPrefix: "East_"
      TagPrefix: "East_"
      AdminScopeSuffix: "_east"
      AdminRoleSuffix: "_east"
      ApplicationAdminSuffix: "_east"
      ApplicationFolderSuffix: "_east"
      ApplicationGroupSuffix: "_east"
      ApplicationUserSuffix: "_east"
      DeliveryGroupSuffix: "_east"
      GroupPolicySuffix: "_east"
      HostConnectionSuffix: "_east"
      MachineCatalogSuffix: "_east"
      StoreFrontSuffix: "_east"
      TagSuffix: "_east"
    West:
      SiteRootFolder: "" # Important: leave this empty
      AdminScopePrefix: "Western "
      AdminRolePrefix: "Western "
      ApplicationAdminPrefix: "Western "
      ApplicationFolderPrefix: "" # Note that a new parent root folder
         is used instead
      ApplicationFolderRoot: "Western"
      ApplicationGroupPrefix: "Western "
      ApplicationUserPrefix: "Western "
      DeliveryGroupPrefix: "Western "
      GroupPolicyPrefix: "Western "
      HostConnectionPrefix: "Western "
      MachineCatalogPrefix: "Western "
      StoreFrontPrefix: "Western "
      TagPrefix: "Western "
      AdminScopeSuffix: ""
      AdminRoleSuffix: ""
      ApplicationAdminSuffix: ""
      ApplicationFolderSuffix: ""
      ApplicationGroupSuffix: ""
      ApplicationUserSuffix: ""
      DeliveryGroupSuffix: ""
      GroupPolicySuffix: ""
```

```
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

### Dateifreigabeverweis mit SiteMerging.yml

Bei dieser Methode wird `SiteRootFolder` aus dem Präfixsatz der Site verwendet. Die Methode ist zwar etwas komplizierter als die mit direkter Dateifreigabe, doch ist das Risiko des Verweises auf den falschen Ordner beim Exportieren, Importieren, Zusammenführen oder Hinzufügen geringer.

Legen Sie zuerst den `SiteRootFolder` für jede Site in der SiteMerging.yml-Datei fest. Sie müssen hierzu den freigegebenen Speicherort verwenden.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \\share.
central.net\AutoConfig\SiteEast -SitePrefixesFolder \\share.central.
net\AutoConfig
```

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -
SitePrefixesFolder \\share.central.net\AutoConfig
```

In diesem Beispiel ist “East”eine vollständig qualifizierte Ordnerangabe und “West”eine relative Ordnerangabe.

Um den Export unter Verwendung der Datei SiteMerging.yml an einen sitespezifischen Ordner zu verweisen geben Sie Folgendes ein:

Aus dem Desktop Delivery Controller “East”:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Aus dem Desktop Delivery Controller “West”:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Das Export-Cmdlet verwendet den Speicherort des Ordners CustomerInfo.yml, um die SiteMerging.yml-Datei zu finden. Im Fall von East ist der `SiteRootFolder` vollqualifiziert. Es wird unverändert verwendet. Im Fall von West ist der `SiteRootFolder` nicht vollqualifiziert. Er wird in Kombination mit dem Speicherort des Ordners CustomerInfo.yml zum Abrufen eines vollqualifizierten Ordnerspeicherorts für West verwendet.

Zusammenführen des Desktop Delivery Controllers “East”in die Cloud:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Zusammenführen des Desktop Delivery Controllers “West”in die Cloud:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Nachfolgend sehen Sie das Muster der im vorherigen Beispiel verwendeten SitePrefixes.yml-Datei.

```
1        East:
2        SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
3        AdminScopePrefix: "East_"
4        AdminRolePrefix: "East_"
5        ApplicationAdminPrefix: "East_"
6        ApplicationFolderPrefix: "" # Note that a new parent root folder
             is used instead
7        ApplicationFolderRoot: "East"
8        ApplicationGroupPrefix: "East_"
9        ApplicationUserPrefix: "East_"
10       DeliveryGroupPrefix: "East_"
11       GroupPolicyPrefix: "East_"
12       HostConnectionPrefix: "East_"
13       MachineCatalogPrefix: "East_"
14       StoreFrontPrefix: "East_"
15       TagPrefix: "East_"
16       AdminScopeSuffix: "_east"
17       AdminRoleSuffix: "_east"
18       ApplicationAdminSuffix: "_east"
19       ApplicationFolderSuffix: "_east"
20       ApplicationGroupSuffix: "_east"
21       ApplicationUserSuffix: "_east"
22       DeliveryGroupSuffix: "_east"
23       GroupPolicySuffix: "_east"
24       HostConnectionSuffix: "_east"
25       MachineCatalogSuffix: "_east"
26       StoreFrontSuffix: "_east"
27       TagSuffix: "_east"
28     West:
29       SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
30       AdminScopePrefix: "Western "
31       AdminRolePrefix: "Western "
32       ApplicationAdminPrefix: "Western "
33       ApplicationFolderPrefix: "" # Note that a new parent root folder
             is used instead
34       ApplicationFolderRoot: "Western"
35       ApplicationGroupPrefix: "Western "
36       ApplicationUserPrefix: "Western "
37       DeliveryGroupPrefix: "Western "
38       GroupPolicyPrefix: "Western "
39       HostConnectionPrefix: "Western "
40       MachineCatalogPrefix: "Western "
41       StoreFrontPrefix: "Western "
```

```
        TagPrefix: "Western "
        AdminScopeSuffix: ""
        AdminRoleSuffix: ""
        ApplicationAdminSuffix: ""
        ApplicationFolderSuffix: ""
        ApplicationGroupSuffix: ""
        ApplicationUserSuffix: ""
        DeliveryGroupSuffix: ""
        GroupPolicySuffix: ""
        HostConnectionSuffix: ""
        MachineCatalogSuffix: ""
        StoreFrontSuffix: ""
        TagSuffix: ""
```

Wenn keine zentrale Dateifreigabe verwendet wird und der Import, die Zusammenführung oder das Hinzufügen von den einzelnen Desktop Delivery Controllern aus durchgeführt wird, erstellen und replizieren Sie die Datei SiteMerging.yml auf jedem Desktop Delivery Controller, der in die Cloud migriert wird. Der Standardpfad ist *%HOMEPATH%\Documents\Citrix\AutoConfig*. Zur Wahl der richtigen Sitepräfixe müssen Sie den Parameter `–SiteName` angeben.

### Zusammenführen der Sites

Citrix empfiehlt, die Cloudvorgänge schrittweise durchzuführen und vor jedem nächsten Schritt eine vollständige Überprüfung durchzuführen. Wenn Sie beispielsweise drei Sites zu einer einzelnen Cloudsite zusammenführen, gehen Sie wie folgt vor:

1. Führen Sie die erste Site unter Verwendung des zugehörigen `SiteName`-Werts mit der Cloud zusammen.
2. Überprüfen Sie die Ergebnisse in der Schnittstelle für die vollständige Konfiguration.
3. Ist das Ergebnis nicht wie erwartet, suchen Sie die Ursache des Fehlers, korrigieren Sie sie und führen Sie die Zusammenführung erneut durch. Entfernen Sie bei Bedarf Cloudkomponenten mit `Remove-CvadAcFromSite` und beginnen Sie von Grund auf neu. Wenn das Ergebnis erwartungsgemäß ausfällt, fahren Sie fort.
4. Wenn die Zusammenführung der ersten Site fehlerfrei erfolgt ist, führen Sie die zweite Site mit der Cloudsite zusammen.
5. Wiederholen Sie die Schritte 2 und 3.
6. Wenn die Zusammenführung der zweiten Site fehlerfrei erfolgt ist, führen Sie die dritte Site mit der Cloudsite zusammen.
7. Wiederholen Sie die Schritte 2 und 3.
8. Überprüfen Sie die Ressourcen aus der Perspektive der Benutzer und vergewissern Sie sich, dass die Anzeige den Soll-Zustand aufweist.

**Entfernen einer Komponente unter Verwendung des Sitepräfixes**

Sie können Komponenten einzelner Sites unter Verwendung des Präfixes im Parameter `–IncludeByName` des Cmdlets `Remove-CvadAcFromSite` selektiv entfernen. Das folgende Beispiel geht von einem Fehler bei den Bereitstellungsgruppen des Desktop Delivery Controllers "West"aus. Um die Bereitstellungsgruppen gezielt für die West-Site zu entfernen gehen Sie folgendermaßen vor:

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName "Western *"
```

Um alle West-Komponenten zu entfernen, führen Sie die folgenden Cmdlets in der angegebenen Reihenfolge aus.

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName "Western *"
Remove-CvadAcFromSite –Applications –IncludeByName "Western *"
Remove-CvadAcFromSite – ApplicationGroups –IncludeByName "Western *"
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName "Western *"
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName "Western *"
Remove-CvadAcFromSite –HostConnections –IncludeByName "Western *"
Remove-CvadAcFromSite –Tags –IncludeByName "Western *"
```

Um Gruppenrichtlinien der East-Komponenten zu entfernen, verwenden Sie das Suffix:

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName "*_east"
```

## Migration von Cloud zu Cloud

April 18, 2024

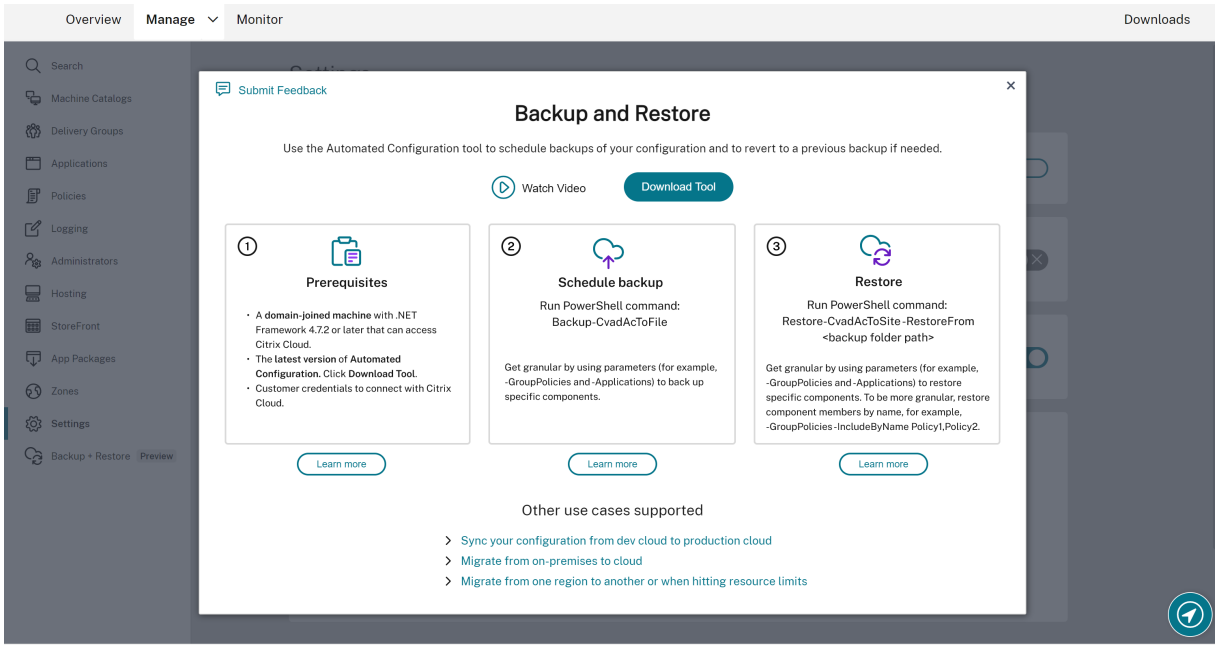
Mit der automatischen Konfiguration können Sie das Verschieben Ihrer Cloud-Konfiguration auf eine andere Cloud-Site automatisieren und Ihre Cloud-Site wiederherstellen.

Durch Verwendung der automatischen Konfiguration können viele Anwendungsfälle gelöst werden:

- Synchronisieren der Site von der Testumgebung in die Produktion
- Backup und Wiederherstellen Ihrer Konfiguration
- Ressourcenlimits werden erreicht
- Migration von Region zu Region

Unter “Vollständige Konfiguration”in Citrix Cloud finden Sie im Knoten “Backup und Wiederherstellung”Informationen zur automatischen Konfiguration und dazu, wie sie für die Migration Ihrer Konfiguration von Cloud zu Cloud verwendet werden kann.




## Voraussetzungen für die Migration Ihrer Konfiguration

Für das Backup und die Wiederherstellung Ihrer Konfiguration benötigen Sie:

- Bereitgestelltes Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service).
- Einen aktiven Ressourcenstandort mit installiertem Connector.
- Verbindung zu Sites, die auf Citrix Cloud zugreifen, muss zulässig und verfügbar sein. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.

> **Hinweis:**
>
> Ein Backup der MCS aus der Cloud kann nicht mit der automatischen Konfiguration durchgeführt werden.

## Sichern der Citrix DaaS-Konfiguration

> **Wichtig:**
>
> - Sie müssen eine CustomerInfo.yml-Datei mit Ihrer Kunden-ID, Client-ID und dem geheimen Schlüssel haben. Informationen zum Abrufen der Kunden- und Client-ID und des geheimen Schlüssels finden Sie unter Generieren der Kunden-ID, der Client-ID und des geheimen Schlüssels. Weitere Informationen zum Einfügen dieser Informationen in die Datei

> CustomerInfo.yml finden Sie unter Auffüllen der Kundeninformationsdatei.
> - Wenn Sie die Backupbefehle ausführen, muss die CustomerInfo.yml die Details des Kunden auf der Quellsite enthalten, von der aus Sie das Backup erstellen.
> - Wenn Sie die Wiederherstellungsbefehle ausführen, muss die CustomerInfo.yml die Details des Kunden auf der Zielsite enthalten, auf der Sie die Konfigurationen wiederherstellen.
> - Die Datei ZoneMapping.yml muss Informationen zur Zuordnung der Ressourcenstandorte in der Cloud enthalten. Weitere Informationen über die Zuordnung von Zonen finden Sie unter Auffüllen der Zonenzuordnungsdatei.
> - Wenn Sie Hostverbindungen haben, müssen Sie die entsprechenden Informationen in CvadAcSecurity.yml eingeben.

1. Installieren Sie die automatische Konfiguration.

   > **Hinweis:**
   >
   > Bei der Cloud-zu-Cloud-Migration kann die automatische Konfiguration auf einer Maschine mit Zugriff auf das Internet installiert werden, auf die der Administrator direkten Zugriff hat.

2. Doppelklicken Sie auf das Symbol **Automatisches Konfigurieren**. Ein PowerShell Fenster wird angezeigt.
3. Führen Sie den folgenden Befehl aus, um ein Backup durchzuführen.

   ```
   Backup-CvadAcToFile
   ```

Nach der ersten Ausführung eines Cmdlets wird ein Exportordner mit den YML-Konfigurationsdateien und Protokollen erstellt. Der Ordner ist in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Bei Auftreten von Fehlern oder Ausnahmen konsultieren Sie den Abschnitt **Fixups** in der Protokolldatei.

### Wiederherstellen einer Konfiguration in Citrix DaaS

1. Doppelklicken Sie auf das Symbol **Automatisches Konfigurieren**. Ein PowerShell Fenster wird angezeigt.
2. Führen Sie den folgenden Befehl aus, um eine Wiederherstellung durchzuführen.

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

Überprüfen Sie den erwarteten Zustand gegen den neuen aktuellen Zustand.

Nach der Ausführung eines Cmdlets wird ein Exportordner mit den YML-Konfigurationsdateien und Protokollen erstellt. Der Ordner ist in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Bei Auftreten von Fehlern oder Ausnahmen konsultieren Sie den Abschnitt **Fixups** in der Protokolldatei.

Der Backup- und Wiederherstellungsprozess schützt vor unbeabsichtigten Änderungen oder Beschädigungen an der Cloud-Sitekonfiguration. Während der Backuperstellung durch die automatische Konfiguration spiegelt das Backup jeweils den Status der Konfiguration der Cloud-Site vor den Änderungen wider. Der Schutz erfordert das regelmäßige Backup der Cloud-Sitekonfiguration und das Speichern der Backups an einem sicheren Ort. Bei Auftreten einer unerwünschten Änderung oder Beschädigung, kann mit dem Backup die Änderung oder Beschädigung auf granularer Ebene oder für die vollständige Konfiguration rückgängig gemacht werden.

## Granulare Migration

> **Wichtig:**
>
> Weitere Informationen zur Reihenfolge der Komponentenmigration finden Sie unter Reihenfolge der Komponentenmigration.

### Wiederherstellen kompletter Komponenten

Beim Wiederherstellen einer Komponente muss mindestens ein Komponentenparameter ausgewählt werden.

Folgen Sie zum Wiederherstellen der gesamten Bereitstellungsgruppen- und Maschinenkatalogkomponenten folgendem Beispiel:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

### Wiederherstellen von Komponentenelementen

Beim Wiederherstellen eines oder mehrerer Komponentenelemente wird das Feature `IncludeByName` verwendet. Das Cmdlet `Restore` wird mit dem Parameter `RestoreFolder`, der ausgewählten Einzelkomponente und der Aufnahmeliste verwendet.

Gehen Sie beispielsweise folgendermaßen vor, um zwei Gruppenrichtlinien aus einem Backup wiederherzustellen:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss

-GroupPolicies -IncludeByName Policy1,Policy2

-DeliveryGroups -MachineCatalogs
```

#### Wiederherstellen der gesamten Cloud-Sitekonfiguration

Zur Wiederherstellung der vollständigen Konfiguration der Cloud-Site werden alle Komponenten ausgewählt.

Folgen Sie zum Wiederherstellen der gesamten Cloudsite-Konfiguration folgendem Beispiel:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

### Aktivieren der Sites

Durch die Siteaktivierung können Sie vorgeben, welche Site aktiv ist und Ihre Ressourcen steuert. Weitere Informationen zum Aktivieren von Sites finden Sie unter Aktivieren von Sites.

## Cmdlets des automatisiertes Konfigurationstools

March 30, 2024

Auf dieser Seite werden alle Cmdlets und Parameter aufgeführt, die von diesem Tool unterstützt werden.

Alle Cmdlets übernehmen Parameter mit einem der folgenden Typen.

- Zeichenfolge
- Liste von Zeichenfolgen
- Boolesch: `$true` oder `$false`
- SwitchParameter: Vorhandensein des Parameters bedeutet `$true`, Fehlen des Parameters bedeutet `$false`

> **Hinweis:**
>
> Die SwitchParameter-Methode wird für die Auswahl von “true”oder “false”bevorzugt, aber aufgrund von Legacyproblemen werden im Tool immer noch boolesche Werte verwendet.

In der folgenden Tabelle sind alle Cmdlets zusammengefasst. In den einzelnen Abschnitten erfahren Sie, von welchen Parametern die Cmdlets jeweils unterstützt werden.

| Kategorie | Cmdlet | Beschreibung |
| --- | --- | --- |
| Migration von On-Premises in die Cloud | `Export-CvadAcToFile` | Exportiert On-Premises-Dateien in YAML-Dateien.<br>`Import-CvadAcToSite`<br>`Merge-CvadAcToSite`<br>`New-CvadAcToSite`<br>`Sync-CvadAcToSite`<br>*Granulare Migration*<br>Verwenden Sie für Komponenten Parameter mit obigen Befehlen. Beispiele: `MachineCatalogs`, `Tags`.<br>Verwenden Sie für Komponentennamen Parameter mit obigen Befehlen. Beispiele: `IncludeByName`, `ExcludeByName`. |
| Cloud zu Cloud-Cmdlets | `Backup-CvadAcToFile` | Sichert die gesamte Konfiguration von Ihrer Cloudsite.<br>`Restore-CvadAcToSite`<br>`Remove-CvadAcFromSite`<br>*Granulare Migration*<br>Verwenden Sie für Komponenten Parameter mit obigen Befehlen. Beispiele: `MachineCatalogs`, `Tags`.<br>Verwenden Sie für Komponentennamen Parameter mit obigen Befehlen. Beispiele: `IncludeByName`, `ExcludeByName`. |
| Andere grundlegende Cmdlets | `Compare-CvadAcToSite` | Vergleicht die On-Premises-YML-Dateien mit der Cloudkonfiguration. |

| Kategorie | Cmdlet | Beschreibung |
| --- | --- | --- |
| Voraussetzungsbezogene Cmdlets | New-CvadAcCustomerInfoFile | Erstellt eine Kundeninformationsdatei. |
| | | Set-CvadAcCustomerInfoFile |
| Cmdlets für Support und Problembehandlung | New-CvadAcZipInfoForSupport | Komprimiert alle Protokoll- und YML-Dateien in einer ZIP-Datei zur Übermittlung an Citrix für Supportmaßnahmen. |
| | | Get-CvadAcStatus |
| | | Test-CvadAcConnectionWithSite |
| | | Find-CvadAcConnector |
| | | Get-CvadAcCustomerSites |
| | | New-CvadAcTemplateToFile |
| | | Show-CvadAcDocument |
| | | Find-CvadAcInFile |
| Cmdlets für die Siteaktivierung | Set-CvadAcSiteActiveStateOnPrem | Legt den Status der On-Premises-Site auf aktiv oder inaktiv fest. |
| | | Set-CvadAcSiteActiveStateCloud |
| Cmdlets für das Zusammenführen mehrerer On-Premises-Sites | New-CvadAcSiteMergingInfo | Erstellt ein Präfix-/Suffix-Infoset zum Zusammenführen von Sites. |
| | | Set-CvadAcSiteMergingInfo |

| Kategorie | Cmdlet | Beschreibung |
|---|---|---|
| | | `Remove-CvadAcSiteMergingInfo` |

Weitere Informationen zu Parametern und deren Verwendung finden Sie unter Parameter für granulare Migration.

## Grundlegende Cmdlets

### On-Premises-zu-Cloud-Cmdlets

- `Export-CvadAcToFile`: Exportiert On-Premises-Dateien in YAML-Dateien.

  Exportiert die Konfiguration aus Ihrem On-Premises-Setup. Dabei handelt es sich um den standardmäßigen Export mit der automatischen Konfiguration. Es werden keine Änderungen an der On-Premises-Sitekonfiguration vorgenommen. Die exportierten Dateien werden im Verzeichnis *%HOMEPATH%\Documents\Citrix\AutoConfig* in einem eindeutig **Export** benannten Unterordner abgelegt. Der Ordner *%HOMEPATH%\Documents\Citrix\AutoConfig* enthält immer die neueste exportierte On-Premises-Sitekonfiguration.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen | | Liste von Zeichenfolgen |
| `TargetFolder` | Gibt den Exportzielordner an. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `AdminAddress` | Gibt das DNS oder die IP-Adresse des Delivery Controllers an, wenn der Export nicht auf dem Delivery Controller ausgeführt wird. | | Zeichenfolge |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `CheckUserAndMachines` | Überprüft, ob Benutzer und Maschinen in Active Directory sind. Nicht in Active Directory enthaltene Benutzer und Maschinen können zu Importfehlern führen. | | `$true` oder `$false` |
| `ZipResults` | Komprimiert Backup von YAML-Dateien in einer einzigen ZIP-Datei. Die Datei befindet sich im selben Ordner wie die gesicherten YAML-Dateien und hat denselben Namen wie der Ordner. | | SwitchParameter |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

Zum Importieren von Daten in die Cloud gibt es drei Möglichkeiten. Das Ausführen bestimmter Cmdlets kann zu einer von drei Aktionskombinationen in der Cloudsite führen:

- Hinzufügen, Aktualisieren und Löschen
- Nur Hinzufügen und Aktualisieren
- Nur Hinzufügen

| Cmdlet | Hinzufügen | Aktualisieren | Löschen |
|---|---|---|---|
| Importieren | X | X | X |
| Merge | X | X | |
| Neu | X | | |

- `Import-CvadAcToSite`: Importiert YAML-Dateien in die Cloud. Unterstützt Erstellungs-, Aktualisierungs- und Löschvorgänge.

  Importiert alle On-Premises-Dateien in die Cloud. Der Befehl stellt sicher, dass der Endstatus in der Cloud dem On-Premises-Status entspricht. Mit dieser Option werden alle Änderungen in der Cloud gelöscht. Importierte Sitekonfigurationsdateien stammen aus *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Mit Vorsicht verwenden!*

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten. | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen. | | Liste von Zeichenfolgen |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff. | | SwitchParameters |
| `SourceFolder` | Identifiziert einen Ersatzstammordner für *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `Merge` | Fügt bei Einstellung auf `$true` der Cloudsite nur Komponenten hinzu. Es werden keine Komponenten entfernt. Legen Sie `$false` fest, um Komponenten zu entfernen. | | `$true` oder `$false` |
| `AddOnly` | Fügt bei Einstellung auf `$true` nur neue Komponenten hinzu, vorhandene Komponenten werden nicht aktualisiert oder gelöscht. Legen Sie `$false` fest, um Aktualisierungen und Löschungen zuzulassen. `Merge` wird ignoriert, wenn dieser Parameter auf `$true` festgelegt ist. | | `$true` oder `$false` |
| `MergePolicies` | Führt Richtlinieneinstellungen und Filter zusammen. Das Zusammenführen erfolgt nur, wenn eine importierte Richtlinie bereits im Cloud-DDC vorhanden ist. Das Ergebnis beim Zusammenführen von Richtlinien ist, dass die Cloud-DDC-Richtlinien die Einstellungen und Filter enthalten, die bereits vorhanden waren, sowie alle neuen Einstellungen und Filter, die importiert werden. Wenn Konflikte zwischen Einstellungen und Filtern auftreten, haben die importierten Werte Vorrang. | | SwitchParameter |
| `OnErrorAction` | Siehe Parameter "OnErrorAction". | | Zeichenfolge |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `Merge-CvadAcToSite`: Importiert YAML-Dateien in die Cloud. Unterstützt Erstellungs- und Aktualisierungsvorgänge.

  Führt die On-Premises-Dateien in der Cloud zusammen, Komponenten in der Cloud oder On-Premises-Site werden jedoch *nicht* gelöscht. Dadurch bleiben in der Cloud bereits vorgenommene Änderungen erhalten. Gibt es in Citrix Cloud eine Komponente mit demselben Namen, kann sie durch den Befehl geändert werden. Dabei handelt es sich um den standardmäßigen Import mit der automatischen Konfiguration. Zusammengeführte Sitekonfigurationsdateien stammen aus *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten. | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen. | | Liste von Zeichenfolgen |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff. | | SwitchParameters |
| `SourceFolder` | Identifiziert einen Ersatzstammordner für *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `Merge` | Fügt bei Einstellung auf `$true` der Cloudsite nur Komponenten hinzu. Es werden keine Komponenten entfernt. Legen Sie `$false` fest, um Komponenten zu entfernen. | | `$true` oder `$false` |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `AddOnly` | Fügt bei Einstellung auf `$true` nur neue Komponenten hinzu, vorhandene Komponenten werden nicht aktualisiert oder gelöscht. Legen Sie `$false` fest, um Aktualisierungen und Löschungen zuzulassen. `Merge` wird ignoriert, wenn dieser Parameter auf `$true` festgelegt ist. | | `$true` oder `$false` |
| `MergePolicies` | Führt Richtlinieneinstellungen und Filter zusammen. Das Zusammenführen erfolgt nur, wenn eine importierte Richtlinie bereits im Cloud-DDC vorhanden ist. Das Ergebnis beim Zusammenführen von Richtlinien ist, dass die Cloud-DDC-Richtlinien die Einstellungen und Filter enthalten, die bereits vorhanden waren, sowie alle neuen Einstellungen und Filter, die importiert werden. Wenn Konflikte zwischen Einstellungen und Filtern auftreten, haben die importierten Werte Vorrang. | | SwitchParameter |
| `OnErrorAction` | Siehe Parameter "OnErrorAction". | | Zeichenfolge |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `New-CvadAcToSite`: Importiert YAML-Dateien in die Cloud. Unterstützt Erstellungs- und Aktualisierungsvorgänge.

  Importiert die On-Premises-Konfiguration in die Cloud, wobei nur neue Komponenten hinzugefügt werden. Vorhandene Cloud-Sitekomponenten werden weder aktualisiert noch gelöscht. Verwenden Sie diesen Befehl, wenn die vorhandenen Cloud-Sitekomponenten unverändert bleiben müssen.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten. | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen. | | Liste von Zeichenfolgen |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff. | | SwitchParameters |
| `SourceFolder` | Identifiziert einen Ersatzstammordner für *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `OnErrorAction` | Siehe Parameter "OnErrorAction". | | Zeichenfolge |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `Sync-CvadAcToSite`: Exportiert und importiert in einem Schritt.

  Die Synchronisierung führt Export und Import in einem Schritt durch. Verwenden Sie den Parameter `SourceTargetFolder`, um den Export-/Importzielordner anzugeben.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen | | Liste von Zeichenfolgen |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `SourceTargetFolder` | Gibt den Export-/Importzielordner an. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `AdminAddress` | Gibt das DNS oder die IP-Adresse des Delivery Controllers an, wenn der Export nicht auf dem Delivery Controller ausgeführt wird. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `Merge` | Fügt bei Einstellung auf `$true` der Cloudsite nur Komponenten hinzu. Es werden keine Komponenten entfernt. Legen Sie `$false` fest, um Komponenten zu entfernen. | | `$true` oder `$false` |
| `AddOnly` | Fügt bei Einstellung auf `$true` nur neue Komponenten hinzu, vorhandene Komponenten werden nicht aktualisiert oder gelöscht. Legen Sie `$false` fest, um Aktualisierungen und Löschungen zuzulassen. `Merge` wird ignoriert, wenn dieser Parameter auf `$true` festgelegt ist. | | `$true` oder `$false` |
| `MergePolicies` | Führt Richtlinieneinstellungen und Filter zusammen. Das Zusammenführen erfolgt nur, wenn eine importierte Richtlinie bereits im Cloud-DDC vorhanden ist. Das Ergebnis beim Zusammenführen von Richtlinien ist, dass die Cloud-DDC-Richtlinien die Einstellungen und Filter enthalten, die bereits vorhanden waren, sowie alle neuen Einstellungen und Filter, die importiert werden. Wenn Konflikte zwischen Einstellungen und Filtern auftreten, haben die importierten Werte Vorrang. | | SwitchParameter |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

**Cloud zu Cloud-Cmdlets**

- `Backup-CvadAcToFile`: Sichert die gesamte Konfiguration von Ihrer Cloudsite.

Exportiert die Cloudkonfiguration in YML-Dateien. Dieses Backup kann bei einem Backup- und Wiederherstellungsprozess zur Wiederherstellung verlorener Komponenten genutzt werden.

Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten | | SwitchParameters |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `TargetFolder` | Gibt den Exportzielordner an. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `ZipResults` | Komprimiert Backup von YAML-Dateien in einer einzigen ZIP-Datei. Die Datei befindet sich im selben Ordner wie die gesicherten YAML-Dateien und hat denselben Namen wie der Ordner. | | SwitchParameter |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `Restore-CvadAcToSite`: Stellt Backup-YAML-Dateien auf der Cloudsite wieder her. Diese Cloudsite kann dieselbe sein wie die Quellcloudsite oder eine andere.

  Stellt die Cloudsite wieder auf die vorherige Konfiguration zurück. Importierte Dateien werden aus dem Ordner bezogen, der mit dem Parameter `-RestoreFolder` angegeben wurde, der den Ordner mit den YML-Dateien zur Wiederherstellung auf der Cloudsite identifiziert. Es muss sich um eine vollständig qualifizierte Ordnerangabe handeln. Dieses Cmdlet kann zum Zurücksetzen auf die vorherige Konfiguration oder für ein Backup und Wiederherstellen der Cloudsite verwendet werden. Dieser Befehl dient zum Hinzufügen, Löschen und Aktualisieren Ihrer Cloudsite.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten. | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen. | | Liste von Zeichenfolgen |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff. | | SwitchParameters |
| `RestoreFolder` | Identifiziert den Ordner mit den YML-Dateien zur Wiederherstellung in die Cloudsite. Es muss sich um eine vollständig qualifizierte Ordnerangabe handeln. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `Merge` | Fügt bei Einstellung auf `$true` der Cloudsite nur Komponenten hinzu. Es werden keine Komponenten entfernt. Legen Sie `$false` fest, um Komponenten zu entfernen. | | `$true` oder `$false` |
| `AddOnly` | Fügt bei Einstellung auf `$true` nur neue Komponenten hinzu, vorhandene Komponenten werden nicht aktualisiert oder gelöscht. Legen Sie `$false` fest, um Aktualisierungen und Löschungen zuzulassen. `Merge` wird ignoriert, wenn dieser Parameter auf `$true` festgelegt ist. | | `$true` oder `$false` |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `MergePolicies` | Führt Richtlinieneinstellungen und Filter zusammen. Das Zusammenführen erfolgt nur, wenn eine importierte Richtlinie bereits im Cloud-DDC vorhanden ist. Das Ergebnis beim Zusammenführen von Richtlinien ist, dass die Cloud-DDC-Richtlinien die Einstellungen und Filter enthalten, die bereits vorhanden waren, sowie alle neuen Einstellungen und Filter, die importiert werden. Wenn Konflikte zwischen Einstellungen und Filtern auftreten, haben die importierten Werte Vorrang. | | SwitchParameter |
| `OnErrorAction` | Siehe Parameter "OnErrorAction". | | Zeichenfolge |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `Remove-CvadAcFromSite`: Entfernt Komponentenelemente aus der Cloud.

  Kann die gesamte Site zurücksetzen oder Elemente aus einer Komponente entfernen (z. B. einen Maschinenkatalog aus der Liste der Kataloge). In Kombination mit dem Parameter `IncludeByName` können so Elemente selektiv entfernt werden.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen | | Liste von Zeichenfolgen |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

**Andere grundlegende Cmdlets**

- `Compare-CvadAcToSite`: Vergleicht die lokalen YML-Dateien mit der Cloud-Konfiguration und erstellt einen Bericht über Änderungen, die von dem Cmdlet `Import`, `Merge` oder `Restore` ausgeführt wurden.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten. | | SwitchParameters |
| Filtern nach Objektnamen | Siehe Filtern nach Objektnamen. | | Liste von Zeichenfolgen |
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff. | | SwitchParameters |
| `SourceFolder` | Identifiziert einen Ersatzstammordner für *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Zeichenfolge |
| `Locale` | Gibt die Sprache des menschenlesbaren Texts an, der exportiert werden kann. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true` oder `$false` |
| `Merge` | Fügt bei Einstellung auf `$true` der Cloudsite nur Komponenten hinzu. Es werden keine Komponenten entfernt. Legen Sie `$false` fest, um Komponenten zu entfernen. | | `$true` oder `$false` |
| `AddOnly` | Fügt bei Einstellung auf `$true` nur neue Komponenten hinzu, vorhandene Komponenten werden nicht aktualisiert oder gelöscht. Legen Sie `$false` fest, um Aktualisierungen und Löschungen zuzulassen. `Merge` wird ignoriert, wenn dieser Parameter auf `$true` festgelegt ist. | | `$true` oder `$false` |
| `OnErrorAction` | Siehe Parameter "OnErrorAction". | | Zeichenfolge |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

## Parameter für die granulare Migration

### Migrieren nach Komponenten

Die folgenden Komponenten können mit den entsprechenden Cmdlets angegeben werden. Die Option `All` wird automatisch ausgewählt, wenn keine Komponentenparameter angegeben werden. Um Fehler zu vermeiden, empfehlen wir, die Komponenten in der folgenden Reihenfolge zu migrieren:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

### Filtern nach Objektnamen

**Migration nach Komponentennamen** Die Parameter `IncludeByName` und `ExcludeByName` und ermöglichen das Ein- und Ausschließen von Elementen in Cmdlets nach Namen. In den unterstützten Cmdlets kann jeweils nur eine Komponente (z. B. Bereitstellungsgruppen) ausgewählt werden. Wenn sich ein Komponentenelement in beiden Bereichen befindet, setzt das Ausschließen alle anderen Parameter außer Kraft und im Abschnitt "Fixups"der Protokolldatei werden die ausgeschlossene Komponente und das ausgeschlossene Element aufgeführt.

`IncludeByName` und `ExcludeByName` akzeptieren eine Liste mit Elementen. Die Name können einen oder mehrere Platzhalter enthalten. Zwei Arten von Platzhaltern werden unterstützt. Die Liste der Komponentenelemente muss in einfache Anführungszeichen gesetzt werden, wenn ein Elementname Sonderzeichen enthält.

- * entspricht einer beliebigen Anzahl von Zeichen

- ? Entspricht einem Zeichen

`IncludeByName` und `ExcludeByName` akzeptieren auch eine Datei mit einer Liste von Elementen, von denen jedes explizit oder mit Platzhaltern angegeben werden kann. Jedes Element muss auf einer eigenen Zeile stehen. Bei Elementnamen werden führende und nachgestellte Leerzeichen gelöscht. Dem Dateinamen muss das @-Zeichen in einfachen Anführungszeichen vorangestellt werden (eine PowerShell-Anforderung, damit das @-Zeichen nicht neu interpretiert wird). Zusätzlich zum Mischen mit Elementnamen können mehrere Dateien aufgelistet werden.

Beispiel zum Zusammenführen aller Bereitstellungsgruppen, deren Namen mit `DgSite1` beginnen und `Home2` enthalten:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

**Nach Bereitstellungsgruppennamen** `ByDeliveryGroupName` filtert nach Bereitstellungsgruppennamen für Anwendungen und Anwendungsgruppen. Dieser Parameter ist immer eine Aufnahmeliste, deren Einträge basierend auf ihrer Bereitstellungsgruppenzuordnung berücksichtigt werden.

`ByDeliveryGroupName` erfasst eine Liste von Bereitstellungsgruppennamen. Die Name können einen oder mehrere Platzhalter enthalten. Zwei Arten von Platzhaltern werden unterstützt.

- * entspricht einer beliebigen Anzahl von Zeichen
- ? entspricht einem einzelnen Zeichen

Im folgenden Beispiel werden alle Anwendungen zusammengeführt, die auf alle Bereitstellungsgruppennamen verweisen, die mit `EastDg` beginnen.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

**Deaktivierte ausschließen** `ExcludeDisabled` schließt alle deaktivierten Anwendungen und Anwendungsgruppen vom Import aus. `ExcludeDisabled` ist standardmäßig auf **`false`** festgelegt, d. h. alle Anwendungen und Anwendungsgruppen werden unabhängig vom Aktivierungsstatus importiert.

**Nach Maschinenname** `ByMachineName` filtert nach dem Maschinennamen für Maschinenkataloge und Bereitstellungsgruppen. Dieser Parameter ist immer eine Aufnahmeliste, deren Einträge basierend auf ihrer Maschinennamenzuordnung berücksichtigt werden.

`ByMachineName` akzeptiert eine Liste von Maschinennamen, die einen oder mehrere Platzhalter enthalten können. Zwei Arten von Platzhaltern werden unterstützt.

- * entspricht einer beliebigen Anzahl von Zeichen

- ? entspricht einem einzelnen Zeichen

Wird beim Exportieren oder Importieren unter Verwendung von `ByMachineName` und eines Maschinennamenfilters keine Maschine im Maschinenkatalog oder in der Bereitstellungsgruppe gefunden, wird der Maschinenkatalog bzw. die Bereitstellungsgruppe vom Export oder Import ausgeschlossen.

> **Hinweis:**
>
> Bei Verwendung von `ByMachineName` in einem Import-Cmdlet wird `MergeMachines` auf `$true` festgelegt.

**Zusammenführen von Maschinen** Wird `MergeMachines` auf `$true` festgelegt, werden Maschinen dem Maschinenkatalog oder der Bereitstellungsgruppe nur hinzugefügt. Es werden keine Maschinen entfernt, sodass inkrementelle Hinzufügungen möglich sind.

`MergeMachines` ist standardmäßig "false", d. h. Maschinen werden entfernt, wenn sie nicht in der YML-Datei des Maschinenkatalogs oder der Bereitstellungsgruppe sind. `MergeMachines` wird bei Verwendung von `ByMachineName` auf `$true` festgelegt, kann aber durch Festlegen von `MergeMachines` auf "false"außer Kraft gesetzt werden.

### Voraussetzungsbezogene Cmdlets

- `New-CvadAcCustomerInfoFile` - Erstellt eine Datei mit Kundeninformationen. Standardmäßig ist diese unter *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `CustomerId` | ID des Kunden. | x | Zeichenfolge |
| `ClientId` | Client-ID des Kunden, die in Citrix Cloud erstellt wurde. Bei Verwendung dieses Parameters müssen "CustomerId"und "Secret"angegeben werden. | Bedingt | Zeichenfolge |

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `Secret` | Geheimer Schlüssel des Kunden, der in Citrix Cloud erstellt wurde. Bei Verwendung dieses Parameters müssen "CustomerId"und "ClientId"angegeben werden. | Bedingt | Zeichenfolge |
| `Environment` | Production-, ProductionGov- oder ProductionJP-Umgebung. | | Enumeration |
| `LogFileName` | Ändert das Protokolldateipräfix "CitrixLog"in ein anderes Präfix. | | Zeichenfolge |
| `AltRootUrl` | Nur unter Anleitung von Citrix verwenden. | | Zeichenfolge |
| `StopOnError` | Stoppt den Vorgang nach dem ersten Fehler. | | `$true` oder `$false` |
| `TargetFolder` | Verwendet anstelle von *%HOMEPATH%\Documents\Citrix\AutoConfig* den angegebenen Ordner als Stammordner. | | Zeichenfolge |
| `Locale` | Verwendet das angegebene Gebietsschema anstelle des vom System, auf dem das Tool ausgeführt wird, abgeleiteten Gebietsschemas. | | Zeichenfolge |
| `Editor` | Verwendet den angegebenen Editor zum Anzeigen des Protokolls nach Abschluss jedes Cmdlets. Notepad.exe ist der Standardeditor. Der Parameter muss die vollständig qualifizierte Dateiangabe für den Editor enthalten und darf ansonsten keinen Einstellung enthalten. | | Zeichenfolge |
| `SecurityCsvFileSpec` | Die vollständig qualifizierte Dateispezifikation, die auf die von Citrix Identitäts- und Zugriffsverwaltung heruntergeladene Datei "SecurityClient.csv"verweist. Bei Verwendung dieses Parameters muss die "CustomerId" angegeben werden. | | Zeichenfolge |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `Set-CvadAcCustomerInfoFile`: Aktualisiert eine bestehende Kundeninformationsdatei. Nur die im Cmdlet angegebenen Parameter werden geändert. Alle nicht angegebenen Parameterwerte bleiben in der Datei "CustomerInfo.yml"unverändert.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `CustomerId` | ID des Kunden. | | Zeichenfolge |
| `ClientId` | Client-ID des Kunden, die in Citrix Cloud erstellt wurde. | | Zeichenfolge |
| `Secret` | Geheimer Schlüssel des Kunden, der in Citrix Cloud erstellt wurde. | | Zeichenfolge |
| `Environment` | Production-, ProductionGov- oder ProductionJP-Umgebung. | | Enumeration |
| `LogFileName` | Ändert das Protokolldateipräfix "CitrixLog"in ein anderes Präfix. | | Zeichenfolge |
| `StopOnError` | Stoppt den Vorgang nach dem ersten Fehler. | | `$true` oder `$false` |
| `TargetFolder` | Verwendet anstelle von *%HOMEPATH%\Documents\Citrix\AutoConfig* den angegebenen Ordner als Stammordner. | | Zeichenfolge |
| `Locale` | Verwendet das angegebene Gebietsschema anstelle des vom System, auf dem das Tool ausgeführt wird, abgeleiteten Gebietsschemas. | | Zeichenfolge |
| `Editor` | Verwendet den angegebenen Editor zum Anzeigen des Protokolls nach Abschluss jedes Cmdlets. Notepad.exe ist der Standardeditor. Der Parameter muss die vollständig qualifizierte Dateiangabe für den Editor enthalten und darf ansonsten keinen Einstellung enthalten. | | Zeichenfolge |
| `SecurityCsvFileSpec` | Die vollständig qualifizierte Dateispezifikation, die auf die von Citrix Identitäts- und Zugriffsverwaltung heruntergeladene Datei "SecurityClient.csv"verweist. Bei Verwendung dieses Parameters muss die "CustomerId" angegeben werden. | | Zeichenfolge |

  Gibt zurück:

  - Siehe Cmdlet-Rückgabewerte

#### Voraussetzungsbezogene Parameter

Zusammen mit den Parametern mit Cloudzugriff können die folgenden Parameter mit den voraussetzungsbezogenen Cmdlets verwendet werden:

- `Environment`: Production- oder ProductionGov-Umgebung.
- `LogFileName`: Ändern des Protokolldateipräfixes "CitrixLog"in ein anderes Präfix.
- `StopOnError`: Stoppt den Vorgang nach dem ersten Fehler.
- `AlternateRootFolder`: Verwendet anstelle von *%HOMEPATH%\Documents\Citrix\AutoConfig* den angegebenen Ordner als Stammordner.
- `Locale`: Verwendet das angegebene Gebietsschema anstelle des vom System, auf dem das Tool ausgeführt wird, abgeleiteten Gebietsschemas.
- `Editor`: Verwendet den angegebenen Editor zum Anzeigen des Protokolls nach Abschluss jedes Cmdlets. Notepad.exe ist der Standardeditor. Der Parameter muss die vollständig qualifizierte Dateiangabe für den Editor enthalten und darf ansonsten keinen Einstellung enthalten.

### Cmdlets für Support und Problembehandlung

- `New-CvadAcZipInfoForSupport`: Komprimiert alle Protokoll- und YML-Dateien in einer ZIP-Datei zur Übermittlung an Citrix für Supportmaßnahmen. Vertrauliche Kundendaten (CustomerInfo.yml und CvadAcSecurity.yml) sind nicht in der ZIP-Datei enthalten. Die Datei Icon.yml ist aufgrund ihrer Größe ebenfalls ausgeschlossen. Die ZIP-Datei wird in *%HOMEPATH%\Documents\Citrix\AutoConfig* gespeichert und erhält den Namen *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* (mit Datums- und Zeitstempel). Diese ZIP-Datei kann auch als Backup dienen.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `TargetFolder` | Gibt einen Zielordner zum Erstellen und Speichern der ZIP-Datei an. | | Zeichenfolge |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |

  Gibt zurück:

  - Die ZIP-Datei mit Namen und Pfad wird in der Eingabeaufforderung angezeigt.

- `Get-CvadAcStatus`: Wird verwendet, um Konnektivität zu testen und sicherzustellen, dass alle Voraussetzungen erfüllt sind. Gibt Informationen über das Tool wie Versionsnummer und Konnektivität sowie Cloud- und Connectorstatus zurück.

Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `SiteId` | Identifiziert die Site, mit der eine Verbindung hergestellt werden soll. | | Zeichenfolge |
| `AdminAddress` | DNS oder IP-Adresse des On-Premises-Delivery Controllers, der zur Überprüfung der Administrator-Zugriffsebene verwendet wird. Dies ist erforderlich, wenn das Tool nicht auf einem Delivery Controller ausgeführt wird. | | Zeichenfolge |

Gibt zurück:

- Zeigt die Ergebnisse für jedes Element an.

- `Test-CvadAcConnectionWithSite`: Test der Verbindung mit der Cloudsite. Das Cmdlet verwendet die Cloudzugriffsparameter oder die Datei CustomerInfo.yml zum Angeben der Kundenverbindungsinformationen.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |

Gibt zurück:

- Die Testergebnisse werden auf der Befehlszeile angezeigt.

- `Find-CvadAcConnector`: Sucht vorhandene Connectors und ermittelt deren Ausführungszustand. Das Cmdlet verwendet Informationen aus der Datei "CustomerInfo.yml" oder aus dem Kunden-ID-Parameter zur Suche der Connectors des Kunden.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `CustomerInfoFileSpe` | Die Dateispezifikation, die auf eine Kundeninformationsdatei verweist, um den Standardspeicherort und den Standardnamen außer Kraft zu setzen. Dieser Parameter wird ignoriert, wenn der Parameter `CustomerId` angegeben wird. | | Zeichenfolge |
| `CustomerId` | Die ID des Kunden. Dieser Parameter setzt den entsprechenden Wert in der Datei "CustomerInfo.yml"außer Kraft. | | Zeichenfolge |

Gibt zurück:

- Die Ergebnisse werden auf der Befehlszeile angezeigt.

- `Get-CvadAcCustomerSites`: Gibt die Liste aller Kundensites zurück. Das Cmdlet verwendet die Cloudzugriffsparameter oder die Datei CustomerInfo.yml zum Angeben der Kundenverbindungsinformationen.

  Parameter:

  - Siehe Parameter mit Cloudzugriff

  Gibt zurück:

  - Zeigt die Liste der gefundenen Kundensite-IDs an.

- `New-CvadAcTemplateToFile`: Erstellt eine Vorlagendatei für ausgewählte Komponenten zur manuellen Erstellung einer Importdatei.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten | | SwitchParameters |
| `TargetFolder` | Gibt den Exportzielordner an. | | Zeichenfolge |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

- `Show-CvadAcDocument`: Zeigt diese Dokumentation im Standardbrowser an.

  Parameter:

  - Keine.

  Gibt zurück:

  - Zeigt diese Webseite im Standardbrowser an.

- `Find-CvadAcInFile`: Durchsucht YAML-Komponentendateien nach Elementen, die einem oder mehreren Namen entsprechen, die Platzhalter enthalten können. Das Ergebnis ist ein Bericht über gefundene Elemente. "Find in File"kann jeweils nur eine Komponente durchsuchen. "Find in File"durchsucht alle YAML-Dateien im aktuellen Ordner und allen Unterordnern. Verwenden Sie `FindSourceFolder`, um die Anzahl der zu durchsuchenden Dateien zu begrenzen.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Migrieren nach Komponenten | Siehe Migrieren nach Komponenten. Hinweis: Der Wert `-All` ist nicht gültig. | | SwitchParameters |
| `IncludeByName` | Eine Liste der Bereitstellungsgruppen, die eingeschlossen werden sollen, wenn die Site auf aktiv festgelegt wird. Die Platzhalter * und ? werden in Namen unterstützt. | | Liste von Zeichenfolgen |
| `Unique` | Meldet nur eindeutig gefundene Elemente. | | SwitchParameter |
| `IncludeYaml` | Schließt die elementspezifische YAML ein. | | SwitchParameter |
| `FindSourceFolder` | Der Ordner, in dem mit der Suche begonnen wird. | | Zeichenfolge |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | SwitchParameter |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |

  Gibt zurück:

  - Erstellt einen Bericht mit gefundenen Elementen für die angegebene Komponente.

### Cmdlets für die Siteaktivierung

Weitere Informationen zum Aktivieren von Sites und zur Verwendung dieser Cmdlets finden Sie unter Aktivieren der Sites.

- `Set-CvadAcSiteActiveStateOnPrem`: Legt den Status der On-Premises-Site auf aktiv oder inaktiv fest.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `SiteActive` | Legt, wenn vorhanden, die On-Premises-Site auf aktiv fest und beendet den Wartungsmodus für alle Bereitstellungsgruppen. Wenn dieser Parameter nicht vorhanden ist, wird der Wartungsmodus für alle Bereitstellungsgruppen aktiviert. | | SwitchParameter |
| `IncludeByName` | Eine Liste der Bereitstellungsgruppen, die eingeschlossen werden sollen, wenn die Site auf aktiv festgelegt wird. Die Platzhalter * und ? werden in Namen unterstützt. | | Liste von Zeichenfolgen |
| `ExcludeByName` | Eine Liste der Bereitstellungsgruppen, die ausgeschlossen werden sollen, wenn die Site auf aktiv festgelegt wird. Die Platzhalter * und ? werden in Namen unterstützt. | | Liste von Zeichenfolgen |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true or $false` |

  Gibt zurück:

  - Siehe Cmdlet-Rückgabewerte

- `Set-CvadAcSiteActiveStateCloud`: Legt den Status der Cloudsite auf aktiv oder inaktiv fest.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| Parameter mit Cloudzugriff | Siehe Parameter mit Cloudzugriff | | SwitchParameters |
| `SiteActive` | Legt, wenn vorhanden, die Cloudsite auf aktiv fest und beendet den Wartungsmodus für alle Bereitstellungsgruppen. Wenn dieser Parameter nicht vorhanden ist, wird der Wartungsmodus für alle Bereitstellungsgruppen aktiviert. | | SwitchParameter |
| `IncludeByName` | Eine Liste der Bereitstellungsgruppen, die eingeschlossen werden sollen, wenn die Site auf aktiv festgelegt wird. Die Platzhalter * und ? werden in Namen unterstützt. | | Liste von Zeichenfolgen |
| `ExcludeByName` | Eine Liste der Bereitstellungsgruppen, die ausgeschlossen werden sollen, wenn die Site auf aktiv festgelegt wird. Die Platzhalter * und ? werden in Namen unterstützt. | | Liste von Zeichenfolgen |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |
| `DisplayLog` | Zeigt die Protokolldatei nach Abschluss des Cmdlets an. Legen Sie den Parameter auf `$false` fest, um die Protokollanzeige zu unterdrücken. | | `$true or $false` |

Gibt zurück:

- Siehe Cmdlet-Rückgabewerte

### Cmdlets für das Zusammenführen mehrerer On-Premises-Sites

Weitere Informationen zum Zusammenführen von Sites mit diesen Cmdlets finden Sie unter Zusammenführen mehrerer Sites.

- `New-CvadAcSiteMergingInfo` erstellt ein Präfix-/Suffix-Infoset zum Zusammenführen von Websites. Zu Beginn müssen nicht alle Präfixe oder Suffixe bekannt sein. Sie können mit `Set-CvadAcSiteMergingInfo` oder durch manuelles Bearbeiten der Datei SiteMerging.yml aktualisiert werden.
  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `SiteName` | Identifiziert das Präfix-/Suffix-Infoset einer spezifischen Site. Eine Übereinstimmung mit dem Namen der Site ist möglich, aber nicht notwendig. | x | Zeichenfolge |
| Parameter zur Sitezusammenführung | Siehe Parameter zur Sitezusammenführung | | SwitchParameters |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |

Gibt zurück:

- Ohne

- `Set-CvadAcSiteMergingInfo` aktualisiert das Präfix-/Suffix-Infoset zur Sitezusammenführung.

  Parameter:

| Name | Beschreibung | Erforderlich? | Typ |
|---|---|---|---|
| `SiteName` | Identifiziert das Präfix-/Suffix-Infoset einer spezifischen Site. Eine Übereinstimmung mit dem Namen der Site ist möglich, aber nicht notwendig. | x | Zeichenfolge |
| Parameter zur Sitezusammenführung | Siehe Parameter zur Sitezusammenführung | | SwitchParameters |
| `Quiet` | Unterdrückt die Protokollierung an die Konsole. | | SwitchParameter |

Gibt zurück:

- Ohne

- `Remove-CvadAcSiteMergingInfo` entfernt das Präfix-/Suffix-Infoset zur Sitezusammenführung.

Parameter:

- `SiteName`: Identifiziert die Sitepräfixe und -suffixe. Dies ist eine erforderliche Zeichenfolge.

Gibt zurück:

- Ohne

**Parameter zur Sitezusammenführung**

Die folgenden Parameter können beim Ausführen der Cmdlets zum Zusammenführen von Sites verwendet werden. Alle aufgelisteten Parameter sind Zeichenfolgen.

- `SiteName` identifiziert das Präfix-/Suffix-Infoset einer spezifischen Site. Eine Übereinstimmung mit dem Namen der Site ist möglich, aber nicht notwendig. SiteName ist ein erforderlicher Parameter.
- `AdminScopedPrefix`: das auf Administratorbereiche anzuwendende Präfix.
- `ApplicationPrefix`: das auf Anwendungen anzuwendende Präfix.
- `ApplicationFolderPrefix`: das auf Anwendungsordner anzuwendende Präfix. `ApplicationFolderPrefix` kann mit `ApplicationFolderRoot` kombiniert werden.
- `ApplicationFolderRoot`: der neue Stammordner für Anwendungsordner. Hierdurch wird eine zusätzliche Ordnerhierarchie erstellt. `ApplicationFolderRoot` kann mit `ApplicationFolderPrefix` kombiniert werden.
- `ApplicationGroupPrefix`: das auf Anwendungsgruppen anzuwendende Präfix.
- `ApplicationUserPrefix`: das auf Anwendungsnamen, die für Benutzer angezeigt werden, anzuwendende Präfix.
- `ApplicationAdminPrefix`: das auf Anwendungsnamen, die für Administratoren angezeigt werden, anzuwendende Präfix.
- `DeliveryGroupPrefix`: das auf Bereitstellungsgruppen anzuwendende Präfix.
- `GroupPolicyPrefix`: das auf Richtliniennamen anzuwendende Präfix.
- `HostConnectionPrefix`: das auf Hostverbindungen anzuwendende Präfix.
- `MachineCatalogPrefix`: das auf Maschinenkataloge anzuwendende Präfix.
- `StoreFrontPrefix`: das auf StoreFront-Namen anzuwendende Präfix.
- `TagPrefix`: das auf Tags anzuwendende Präfix.
- `AdminScopedSuffix`: das auf Administratorbereiche anzuwendende Suffix.
- `ApplicationSuffix`: das auf Anwendungen anzuwendende Suffix.
- `ApplicationFolderSuffix`: das auf Anwendungsordner anzuwendende Suffix. `ApplicationFolderSuffix` kann mit `ApplicationFolderRoot` kombiniert werden.

- `ApplicationGroupSuffix`: das auf Anwendungsgruppen anzuwendende Suffix.
- `ApplicationUserSuffix`: das auf Anwendungsnamen, die für Benutzer angezeigt werden, anzuwendende Suffix.
- `ApplicationAdminSuffix`: das auf Anwendungsnamen, die für Administratoren angezeigt werden, anzuwendende Suffix.
- `DeliveryGroupSuffix`: das auf Bereitstellungsgruppen anzuwendende Suffix.
- `GroupPolicySuffix`: das auf Richtliniennamen anzuwendende Suffix.
- `HostConnectionSuffix`: das auf Hostverbindungen anzuwendende Suffix.
- `MachineCatalogSuffix`: das auf Maschinenkataloge anzuwendende Suffix.
- `StoreFrontSuffix`: das auf StoreFront-Namen anzuwendende Suffix.
- `TagSuffix`: das auf Tags anzuwendende Suffix.
- `SiteRootFolder`: der vollqualifizierte Ordnername für Exporte und Importe (lokaler Ordner oder Dateifreigabe).

### Generische Parameter

#### Parameter mit Cloudzugriff

Alle Cmdlets, die auf die Cloud zugreifen, unterstützen folgende zusätzliche Parameter.

> **Hinweis:**
>
> Die Parameter "CustomerId", "ClientId"und "Secret"können in die Datei "CustomerInfo.yml" eingefügt oder mit den folgenden Parametern im Cmdlet angegeben werden. Bei Angabe an beiden Stellen haben die Cmdlet-Parameter Vorrang.

- `CustomerId`: Die Kunden-ID wird in den Rest-APIs verwendet und ist für den Zugriff auf alle Rest-APIs erforderlich. Die Kunden-ID finden Sie in Citrix Cloud.
- `ClientId`: Die auf der Website Citrix Cloud Identity and Access Management erstellte clientID. Dies ist zum Abrufen des Bearertokens erforderlich, der zur Authentifizierung bei allen Rest-APIs benötigt wird.
- `Secret`: Der auf der Website Citrix Cloud Identity and Access Management erstellte geheime Schlüssel. Dies ist zum Abrufen des Bearertokens erforderlich, der zur Authentifizierung bei allen Rest-APIs benötigt wird.
- `CustomerInfoFileSpec`: Die Dateispezifikation, die auf eine Kundeninformationsdatei verweist, um den Standardspeicherort und den Standardnamen außer Kraft zu setzen.

#### Migrationsmodus-Parameter

Die Cmdlets zur Änderung der Cloudsitekonfiguration (`Import`, `Restore`, `Merge`, `New` und `Sync`) unterstützen folgende Parameter zur Erweiterung der Flexibilität.

- `CheckMode`: Führt den Importvorgang *ohne* Änderungen durch. Alle erwarteten Änderungen werden vor dem Import gemeldet. Sie können den Import vor dessen Ausführung mit diesen Befehl testen.
- `BackupFirst`: Sichert den Cloudinhalt in YML-Dateien, bevor die Cloudkonfiguration geändert wird. Diese Option ist standardmäßig aktiviert.
- `Confirm`: Bei Festlegen auf "true"wird eine Bestätigung zum Ändern der Konfiguration der Cloudsite angefordert. Das Cmdlet `Remove` zeigt aufgrund seiner destruktiven Wirkung eine Aufforderung an. Legen Sie es auf "false"fest, wenn keine Eingabeaufforderung gewünscht wird (z. B. bei Ausführung in einem Skript). `Confirm` ist standardmäßig auf "true"festgelegt.
- `SecurityFileFolder`: Dies ist der vollständig qualifizierte Name des Ordners mit der Datei "CustomerInfo.yml", die auf einen lokalen Ordner oder eine Netzwerkfreigabe mit möglicher Authentifizierungskontrolle verweisen kann. Das Tool fordert nicht zur Eingabe von Anmeldeinformationen auf. Der Zugriff auf Ressourcen mit Authentifizierung muss vor dem Ausführen des Tools bereitgestellt werden.
- `SiteName` gibt das Präfix und Suffix für die Sitezusammenführung beim Import an.
- `SiteActive` gibt an, ob die importierte Site aktiv oder inaktiv ist. Standardmäßig ist dieser Parameter auf `$false` festgelegt und die importierte Site ist inaktiv.

#### Parameter zur Protokollanzeige

Die Cmdlets `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare` und `Remove` zeigen nach Abschluss des Vorgangs die Protokolldatei an. Sie können die Anzeige unterdrücken, indem Sie den Parameter `-DisplayLog` auf `$false` einstellen. Notepad.exe wird standardmäßig zur Anzeige des Protokolls verwendet. Sie können in der Datei CustomerInfo.yml einen anderen Editor angeben.

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

### Cmdlet-Rückgabewerte

#### ActionResult

Alle Cmdlets geben den folgenden Wert zurück.

```
1            public class ActionResult
2            {
3
4                public bool                          Overall_Success;
5                public Dictionary<string, string>   Individual_Success;
6                public object                        CustomResult;
7             }
```

`Overall_Success` gibt einen einzelnen Booleschen Wert zurück, der den Gesamterfolg des Cmdlets für alle ausgewählten Komponenten anzeigt: true = erfolgreich, false = nicht erfolgreich.

`Individual_Success` gibt einen von drei Werten für jede Hauptkomponente zurück. Das Ergebnis kann "Success", "Failure" oder "Skipped" lauten. "Skipped" bedeutet, dass eine Komponente nicht für das Ausführen durch das Cmdlet ausgewählt wurde.

`CustomResult` ist Cmdlet-spezifisch.

#### CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File` und `Remove` geben die folgenden CustomResult-Informationen in einer `EvaluationResultData`-Instanz zurück.

> **Hinweis:**
>
> Die Cmdlets `Export` und `Template` geben kein CustomResult zurück.

```
                public class EvaluationResultData
                {

                    public Dictionary<string, Dictionary<string,
                       ActionResultValues >> EvaluationResults;
                    public int                  Added;
                    public int                  Updated;
                    public int                  Deleted;
                    public int                  NoChange;
                    public int                  TotalChanged;
                    public EvaluationResults     OverallResult;
                    public string               CloudBackupFolder;
                    public string               SourceBackupFolder;
                 }

                Where:
                public enum ActionResultValues
               {

                    Add,
                    Update,
                    Delete,
                    Identical,
                    DoNothing
                 }

                public enum EvaluationResults
                {

                    Success,
                    Failure,
                    Skipped
                 }
```

`EvaluationResults` zeigt eine Liste mit einem Eintrag pro ausgewählter Komponente an. Der

Schlüssel ist der Komponentenname und der Wert eine Liste jedes Komponentenelements und der an diesem ausgeführten Aktion. Die Aktion ist einer der `ActionResultValues`-Werte.

`Added`, `Updated`, `Deleted` und `NoChange` geben die Gesamtzahl der hinzugefügten, aktualisierten, gelöschten und nicht geänderten Komponentenelemente an (in der hier angegebenen Reihenfolge).

`TotalChanged` ist die Summe von `Added`, `Updated` und `Deleted`.

`OverallResult` ist ein Boolescher Wert, der das Ergebnis des Cmdlets beschreibt. "True"bedeutet Erfolg für alle Komponenten, "false"zeigt einen Fehler bei der Verarbeitung mindestens einer Komponente an.

`CloudBackupFolder` ist die vollqualifizierte Dateispezifikation des Backups der Cloudsite-Konfiguration, die vor Ausführung des Cmdlets erstellt wurde.

`SourceBackupFolder` ist die vollqualifizierte Dateispezifikation des Backups der Quelldatei, die nach Ausführung des Cmdlets erstellt wurde. Standardmäßig sind diese Dateien unter *%HOMEPATH%\Documents\Citrix\AutoConfig*.

### Hilfe zu PowerShell

PowerShell-Hilfe ist für jedes Cmdlet verfügbar. Sie enthält eine kurze Erläuterung des Cmdlets und eine Dokumentation aller Parameter. Um auf die Hilfe für ein Cmdlet zuzugreifen, geben Sie vor dem Cmdlet `Get-Help` ein.

```
Get-Help Import-CvadAcToSite
```

## Problembehandlung bei automatischer Konfiguration und zusätzliche Informationen

March 30, 2024

> **Wichtig:**
>
> Häufig auftretende Fehlermeldungen für die automatische Konfiguration und entsprechende Lösungen finden Sie in den *FAQ zur Problembehandlung* im Knowledge Center-Artikel CTX277730.

### Fehler bei Verwendung des automatisierten Konfigurationstools

Mit dem automatisierten Konfigurationstool können gelegentlich Fehler auftreten. Komponenten wie Maschinenkataloge, Bereitstellungsgruppen oder Gruppenrichtlinien können dann nicht korrekt ver-

arbeitet werden. Mit `OnErrorAction` und Fortsetzungsparametern können Sie Fehler, die während der Verarbeitung auftreten, erfassen, beheben und den Prozess fortsetzen.

Der Standardwert für `OnErrorAction` ist `StopCompEnd`. Bei einem Fehler beendet das Tool dann die Verarbeitung der aktuellen Komponente. Es werden keine zusätzlichen Komponenten verarbeitet, und Fehler werden nicht an nachgelagerte, abhängige Komponenten übertragen. Nachdem Sie alle Fehler behoben haben, können Sie Ihre Cmdlets mit angewendetem Fortsetzungsparameter erneut ausführen.

#### Parameter "OnErrorAction"

Sie können Parameterwerte für `OnErrorAction` in Migrationsbefehlen definieren, um festzulegen, wie das Tool auf Fehler reagiert, die beim Verarbeiten von Komponenten erfasst werden.

Diese Tabelle enthält Parameterwerte und ihre Beschreibung:

| Wert | Beschreibung |
|---|---|
| `Continue` | Versucht, möglichst viele Komponenten zu verarbeiten. |
| `Pause` | Hält nach der Verarbeitung an und fordert Sie auf, fortzufahren oder den Vorgang zu beenden. |
| `StopCompEnd` | Versucht, möglichst viel von der Komponente zu verarbeiten. Stoppt nach Abschluss der Komponente. (Standard) |
| `StopImmediately` | Die Verarbeitung wird gestoppt, wenn ein Fehler gefunden wird. |

#### Migrations-Cmdlets

Sie können den Parameter `OnErrorAction` auf die folgenden Migrationsbefehle anwenden:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Beispiel:`Merge-CvadAcToSite -OnErrorAction StopImmediately`

### Wiederaufnahmeparameter

Diese Parameter definieren, wie das Tool einen Vorgang fortsetzt, der aufgrund eines Fehlers angehalten oder beendet wurde.

Sie können Wiederaufnahmeparameter auf Migrations-Cmdlets anwenden, die einen der folgenden Parameterwerte für `OnErrorAction` enthalten:

- `Pause`
- `StopCompEnd`
- `StopImmediately`

Diese Tabelle enthält Parameterwerte und ihre Beschreibung:

| Wert | Beschreibung |
|---|---|
| `-AllRemaining` | Erfordert eine Startkomponente. Die Verarbeitung beginnt bei der Startkomponente und verarbeitet alle verbleibenden Komponenten. Es werden mehrere Komponenten verarbeitet. |
| `-Resume` | Verwendet die Komponente von `CurrentComponent.txt` als Ausgangspunkt. “All Remaining”ist auf “true”festgelegt. Es werden mehrere Komponenten verarbeitet. |
| `-Repeat` | Verwendet die Komponente von `CurrentComponent.txt` als Ausgangspunkt. “All Remaining”ist auf “false”festgelegt. Es wird nur eine Komponente verarbeitet. |

Die zuletzt verarbeitete Komponente wird in der Datei `CurrentComponent.txt` im Ordner “Auto-Config”gespeichert. Das Bearbeiten dieser Datei wird nicht empfohlen.
Wenn Sie `-Resume` oder `-Repeat` festlegen und `CurrentComponent.txt` fehlt oder ungültig ist, wird die Verarbeitung beendet und Sie werden aufgefordert, eine Komponente auszuwählen.

### Einstellen von OnErrorAction in der Datei CustomerInfo.yml

Sie können auch `OnErrorAction`-Werte in der Datei `CustomerInfo.yml` festlegen. Legen Sie die Werte mit den folgenden Cmdlets fest:

- Für eine neue Datei: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

- Für eine vorhandene Datei: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

### Protokolle

Beim Ausführen eines Cmdlets wird immer eine Protokolldatei erstellt und der Hauptverlaufsprotokolldatei ein Eintrag hinzugefügt. Alle Vorgangsprotokolldateien werden in einem Backupordner gespeichert. Alle Protokolldateinamen beginnen mit `CitrixLog`, gefolgt von dem Vorgang der automatischen Konfiguration und dem Datum und der Uhrzeit der Cmdlet-Ausführung. Protokolle werden nicht automatisch gelöscht.

Das Hauptverlaufsprotokoll mit dem Namen **History.Log** bedindet sich im Ordner `*%HOMEPATH%\Documents\Citrix\AutoConfig*`. Jede Cmdlet-Ausführung wird im Hauptverlaufsprotokoll mit Datum, Vorgang, Ergebnis, Backup und Protokolldatei-Speicherorten eingetragen.

Sie können das Cmdlet `New-CvadAcZipInfoForSupport` auch verwenden, um Protokolle zu sammeln, die zwecks Support an Citrix gesendet werden sollen. Dieses Cmdlet komprimiert alle Protokoll- und YML-Dateien in einer einzigen ZIP-Datei. Vertrauliche Kundendaten (CustomerInfo.yml und CvadAcSecurity.yml) sind nicht in der ZIP-Datei enthalten. Die Datei Icon.yml ist aufgrund ihrer Größe ebenfalls ausgeschlossen. Die ZIP-Datei wird in *%HOMEPATH%\Documents\Citrix\AutoConfig* gespeichert und erhält den Namen *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* (mit Datums- und Zeitstempel). Diese ZIP-Datei kann auch als Backup dienen.

Jede Protokolldatei enthält Folgendes:

- Name des Vorgangs und ob der Prüfmodus aktiviert ist
- Datum und Uhrzeit des Starts und Endes
- Einträge für die Aktionen an jeder Komponente und Erfolgs-/Fehlermeldung
- Zusammenfassung der durchgeführten Aktionen, einschließlich Anzahl erstellter Objekte
- Gegebenenfalls Empfehlungen für Fixes
- Gegebenenfalls Speicherort des Backupordners
- Speicherort des Hauptprotokolls
- Dauer

### Diagnosedateien

Diagnosedateien helfen bei der Ermittlung und Behebung von Problemen. Die folgenden Dateien werden erstellt, wenn der betreffende Vorgang ausgeführt wird. Sie sind in dem aktionsspezifischen Unterordner in *%HOMEPATH%\Documents\Citrix\AutoConfig*. Fügen Sie diese Dateien bei, wenn Sie Informationen für den Support zur Problembehebung bereitstellen.

#### Exportieren

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

Diese Datei zählt alle Broker PowerShell SDK-Anrufe, die zum Exportieren der Sitekonfiguration ausgeführt wurden.

#### Import, Merge, Restore, Sync, Backup, Compare

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

Diese Datei dokumentiert jeden Rest API-Aufruf und zugehörige Informationen.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

Diese Datei enthält den Inhalt für alle `Add`-, `Update`- und `Delete`-Rest APIs.

### Durch Voraussetzungen verursachte Probleme

Import und Zusammenführung können aufgrund fehlender Voraussetzungen fehlschlagen. Einige häufig auftretende Probleme:

1. In Gruppenrichtlinien fehlen Bereitstellungsgruppenfilter. Die übliche Ursache sind nicht importierte Bereitstellungsgruppen.
2. Anwendungen können nicht importiert oder zusammengeführt werden. Die übliche Ursache sind nicht importierte Bereitstellungsgruppen oder Anwendungsgruppen.
3. In Anwendungsgruppen fehlt ein RestrictToTag. Die übliche Ursache sind nicht importierte Tags.
4. Hostverbindungen schlagen fehl. Die übliche Ursache sind fehlende Sicherheitsinformationen in der Datei CvadAcSecurity.yml.
5. Maschinenkataloge schlagen fehl. Die übliche Ursache sind nicht importierte Hostverbindungen.
6. In Maschinenkatalogen und Bereitstellungsgruppen fehlen Maschinen. Die übliche Ursache sind Maschine, die nicht in Active Directory gefunden wurden.
7. In Bereitstellungsgruppen fehlen Benutzer. Die übliche Ursache sind Benutzer, die nicht in Active Directory gefunden wurden.

### Empfehlungen

- Führen Sie nicht mehrere Instanzen der automatischen Konfiguration gleichzeitig aus. Das Ausführen mehrerer Instanzen führt zu unvorhersehbaren Ergebnissen in der Cloudsite. Führen Sie

in diesem Fall eine Instanz der automatischen Konfiguration erneut aus, um die Site in den erwarteten Zustand zu versetzen.
- Bearbeiten oder ändern Sie keine Daten auf der Registerkarte "Verwalten"in "Vollständige Konfiguration", während die automatische Konfiguration ausgeführt wird.
- Stellen Sie über eine visuelle Kontrolle der Ergebnisse des Zuammenführens, Importierens oder Wiederherstellens in der vollständigen Konfiguration stets sicher, dass die Cloudsite den Erwartungen entspricht.

## Ordner

### Standard-Stammordner

Alle Vorgänge des automatisierten Konfigurationstools werden im Stammordner oder einem seiner Unterordner ausgeführt. Der Stammordner ist in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

### Exportieren

Alle exportierten Dateien werden zur Gewährleistung der Benutzerfreundlichkeit und zur Bewahrung eines Exportverlaufs in zwei Ordnern gespeichert. Exporte werden immer im Stammordner gespeichert. Kopien werden in dem Unterordner **Export** mit dem Datum und der Uhrzeit des Exports gespeichert.

Der Stammordner enthält immer die zuletzt exportierte On-Premises-Sitekonfiguration. Jeder **Export**-Unterordner enthält den zu dem angegebenen Datum und der angegebenen Uhrzeit erfolgten Export, wodurch ein Exportverlauf bereitgestellt wird. Sie können die Cloudsite unter Verwendung eines beliebigen **Export**-Unterordners konfigurieren. Vorhandene Exportunterordner werden bei der automatischen Konfiguration weder gelöscht noch geändert.

### Importieren, Zusammenführen, Synchronisieren, Vergleichen

Die Vorgänge `Import`, `Merge` und `Compare` erfolgen immer mit Quelldateien im Stammordner. Jeder Vorgang führt zur Erstellung eines Unterordners, in den Dateien aus dem Stammordner kopiert werden, sodass ein Verlauf der Quelldateien der Cloudsite-Änderungen entsteht.

### Wiederherstellen

Der `Restore`-Vorgang verwendet einen bestehenden Unterordner zum Konfigurieren der Cloudsite. Der Quellordner wird mit dem erforderlichen Parameter `-RestoreFolder` angegeben. Im Gegensatz zu anderen Befehlen wird kein Unterordner erstellt, da der `Restore`-Vorgang einen bestehen-

den Unterordner verwendet. Als Wiederherstellungsordner kann der Stammordner verwendet werden, doch auch er muss im `-RestoreFolder`-Parameter angegeben werden.

### Backups

Die automatische Konfiguration initialisiert, aktualisiert und sichert die Cloudsite-Konfiguration. Die Verwendung im Laufe der Zeit kann zu vielen Konfigurationsänderungen bei der Cloudsite führen. Zur Vereinfachung der langfristigen Verwendung speichert die automatische Konfiguration den Änderungsverlauf und bietet eine Methode zum Wiederherstellen früherer Zustände.

Backups der Cloudsite-Konfiguration werden immer in einem Unterordner namens **Backup** mit Datum und Zeitpunkt des Backups gespeichert. Vorhandene Exportunterordner werden bei der automatischen Konfiguration weder gelöscht noch geändert.

Sie können mit den Backups einzelne Komponenten oder die gesamte Konfiguration wiederherstellen. Verwenden Sie zum Wiederherstellen der gesamten Bereitstellungsgruppen- und Maschinenkatalogkomponenten folgendes Cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Hinweis:**
>
> Die Informationen zur Backupdatei im obigen Cmdlet basieren auf Ihren eigenen Backups.

Verwenden Sie zum Wiederherstellen der gesamten Cloudsite-Konfiguration folgendes Cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

> **Hinweis:**
>
> Die Informationen zur Backupdatei im obigen Cmdlet basieren auf Ihren eigenen Backups.

#### Ändern des Standardstammordners

Die Vorgänge `Export`, `Import`, `Merge`, `Sync` und `Compare` können bei Verwendung des Parameters `–AlternateFolder` den Stammordner ändern. Die Erstellung und Verwaltung vorgangsbezogener Unterordner ist weiterhin wie oben beschrieben.

#### In Unterordner kopierte Dateien

Mit Ausnahme der Folgenden werden alle Dateien mit der Erweiterung ".yml"in Vorgangsunterordner kopiert:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

#### Automatisierte, ausfallsichere Cloudsite-Backups

Vor dem Ausführen von Vorgängen, die die Konfiguration ändern, wird ein Backup der Cloudsite-Konfiguration vorgenommen. Dies betrifft die Parameter `Import`, `Merge`, `Sync` und `Restore`. Das Backup ist immer in einem Unterordner des zum Vorgang gehörenden Unterordners.

Bei `Restore` ist der Backupordner ein Unterordner des im Parameter `-RestoreFolder` angegebenen Ordners.

### Automatisierung

Die Cmdlets des automatisierten Konfigurationstools können ohne Administratoreingriff in Skripts ausgeführt werden. Eingabeaufforderungen und die Anzeige der Protokollergebnisse bei Abschluss des Cmdlets werden dann unterdrückt. Sie können für dieselbe Funktion auch Parameter über die Datei CustomerInfo.yml festlegen.

Fügen Sie den folgenden Parameter zu Cmdlets zur Cloudmodifizierung hinzu, um die Anzeige von Eingabeaufforderungen zu unterdrücken.

```
-Confirm $false
```

Fügen Sie den folgenden Parameter zu Cmdlets hinzu, um die Anzeige des Protokolls nach Abschluss des Cmdlets zu unterdrücken.

```
-DisplayLog $false
```

Fügen Sie Cmdlets den folgenden Parameter hinzu, um die Protokollierung im PowerShell-Befehlsfenster zu unterdrücken.

```
-Quiet
```

Alternativ können die folgenden Parameter in die Datei CustomerInfo.yml geschrieben werden.

```
Confirm: False
```

```
DisplayLog: False
```

### Exportieren von anderen PCs als dem Delivery Controller

Das automatisierte Konfigurationstool verwendet mehrere Citrix PowerShell-SDKs, um die Konfiguration der On-Premises-Site zu exportieren. Die SDKs werden automatisch auf dem Delivery Controller installiert, sodass das Tool darauf ohne zusätzliche Aktionen ausgeführt werden kann. Zur Ausführung des Tools auf Maschinen, die kein Delivery Controller sind, müssen Sie die benötigten Citrix PowerShell-SDKs installieren. Die SDKs ist gehören zu Citrix Studio, das vom Citrix Virtual Apps and Desktops-Installationsmedium installiert werden kann.

> **Hinweis:**
>
> Die automatische Konfiguration kann nicht auf dem Cloud Connector ausgeführt werden.

### Umstellung auf Citrix Cloud Government und Japan Control Plane

Die Citrix Cloud Government- und Japan Control Plane-Umgebung verwenden verschiedene Zugriffspunkte zum Authentifizieren und Zuweisen von Zugriffstoken. Diese einmalige Anforderung gilt für jedes automatisierte Konfigurationstool, das auf die Cloud zugreift. Führen Sie die folgenden Schritte aus, um die automatische Konfiguration in diesen Umgebungen zu verwenden.

1. Bearbeiten Sie die Datei CustomerInfo.yml im Ordner *%HOMEPATH%\Documents\Citrix\AutoConfig*.
2. Fügen Sie je nach der Umgebung, mit der Sie eine Verbindung herstellen möchten, eine der folgenden Zeilen zu CustomerInfo.yml hinzu (oder ändern Sie sie, falls bereits vorhanden).

   ```
   Environment: 'ProductionGov'
   ```

   Oder

   ```
   Environment: 'ProductionJP'
   ```

Die automatische Konfiguration kann jetzt in diesen Umgebungen verwendet werden.

### Citrix Cloud-Datenerfassung

Informationen zu den von Citrix Cloud erfassten Informationen finden Sie unter Erfassen von Kundendaten und Protokollen in Citrix Cloud Services.

### Weitere Ressourcen

#### Diskussionsforum

Besuchen Sie das Citrix Diskussionsforum zur automatisierten Konfiguration.

### Video

Schauen Sie sich das Video Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops auf YouTube an.

### Schulung

Das Cloud Learning Center enthält Videos mit schrittweisen Anleitungen zum Aufbau einer Service-Bereitstellung, einschließlich der in diesem Artikel beschriebenen Aufgaben. Siehe Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

## Migration von Workloads zwischen Ressourcenstandorten mit Image Portability Service

May 17, 2024

Mit dem Image Portability Service können Sie Images einfacher plattformübergreifend verwalten. REST-APIs für Citrix Virtual Apps and Desktops ermöglichen die automatisierte Verwaltung von Ressourcen innerhalb einer Citrix Virtual Apps and Desktops-Site.

Der Image Portability-Workflow beginnt, wenn Sie Citrix Cloud verwenden, um die Migration eines Images zwischen zwei Ressourcenstandorten zu starten. Nach dem Export Ihres Images hilft Ihnen Image Portability Service bei der Übertragung und Vorbereitung des Images für die Ausführung auf dem Ziel-Hypervisor oder der Public Cloud. Schließlich stellt Citrix Provisioning oder Machine Creation Services das Image in der Zielumgebung bereit.

### Komponenten

Image Portability Service enthält folgende Komponenten:

- Citrix Cloud Services
- Citrix Credential Wallet
- Citrix Connector Appliance
- Compositing Engine-VM
- PowerShell-Beispielskripte

### Citrix Cloud Services

Die Citrix Cloud Services API ist ein REST-API-Dienst für die Interaktion mit Image Portability Service. Mit dem REST-API-Dienst können Sie Image Portability-Aufträge erstellen und überwachen. Sie können zum Beispiel mit einem API-Aufruf einen Image Portability-Auftrag starten (beispielsweise zum Export eines Datenträgers) und dann mit weiteren Aufrufen den Auftragsstatus abfragen.

### Citrix Credentials Wallet

Der Dienst Citrix Credentials Wallet dient zum sicheren Verwalten von Systemanmeldeinformationen und ermöglicht, das Image Portability Service mit Ihren Assets interagieren kann. Wenn Sie beispielsweise einen Datenträger aus vSphere in eine SMB-Freigabe exportieren, benötigt Image Portability Service die Anmeldeinformationen, um eine Verbindung zur SMB-Freigabe zu öffnen und den Datenträger zu schreiben. Wenn die Anmeldeinformationen in der Credential Wallet gespeichert sind, kann Image Portability Service diese Anmeldeinformationen abrufen und verwenden.

Mit diesem Service können Sie Ihre Anmeldeinformationen vollständig verwalten. Die Cloud Services API fungiert als Zugriffspunkt und bietet Ihnen die Möglichkeit, Anmeldeinformationen zu erstellen, zu aktualisieren und zu löschen.

### Compositing Engine

Die Compositing Engine ist das Kernstück von Image Portability Service. Die Compositing Engine (CE) ist eine einzelne VM, die beim Start eines Export- oder Vorbereitungsauftrag mit Image Portability erstellt wird. Diese virtuellen Maschinen werden in derselben Umgebung erstellt, in der der Auftrag ausgeführt wird. Wenn Sie beispielsweise einen Datenträger aus vSphere exportieren, wird die CE auf dem vSphere-Server erstellt. Wenn Sie hingegen einen Vorbereitungsauftrag in Azure, AWS oder Google Cloud ausführen, wird die CE in Azure, AWS bzw. Google Cloud erstellt. Die CE stellt Ihren Datenträger in sich selbst bereit und bearbeitet ihn anschließend. Nach Abschluss des Vorbereitungs- oder Exportauftrags werden die CE-VM und alle zugehörigen Komponenten gelöscht.

### Connector Appliance

Die Connector Appliance, die Anbietersoftware zum Verwalten von IPS-Ressourcen ausführt, wird in Ihrer Umgebung ausgeführt (sowohl on-premises als auch in Ihrem Azure-, AWS- oder Google Cloud-Abonnement) und fungiert als Controller für einzelne Aufträge. Das Gerät erhält Auftragsanweisungen vom Clouddienst und erstellt und verwaltet die VMs der Compositing Engine. Die Connector Appliance-VM fungiert als ein einziger, sicherer Kommunikationspunkt zwischen den Clouddiensten und Ihren Umgebungen. Stellen Sie mindestens eine Connector Appliance an jedem

Ihrer Ressourcenstandorte bereit (on-premises, Azure, AWS oder Google Cloud). Aus Sicherheitsgründen wird an jedem Ressourcenstandort eine eigene Connector Appliance bereitgestellt. Durch Kombination der Connector Appliance mit der Compositing Engine erhöht sich die Sicherheitslage der Bereitstellung erheblich, da alle Komponenten und die Kommunikation innerhalb Ihres Ressourcenstandorts verbleiben.

#### PowerShell-Module

Wir bieten mehrere PowerShell-Module, die Sie in Skripts als Ausgangspunkt zum Entwickeln einer eigenen Automatisierung verwenden können. Die bereitgestellten Module werden im Originalzustand unterstützt, Sie können sie jedoch je nach Bedarf an Ihre Bereitstellung anpassen.

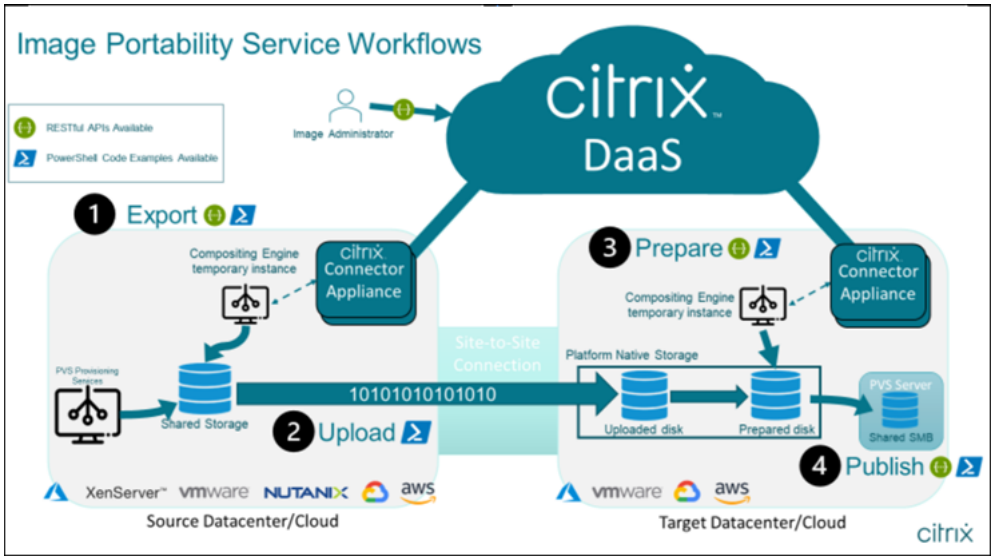
Die PowerShell-Automatisierung erstellt mithilfe bereitgestellter Konfigurationsparameter einen REST-Aufruf an den Citrix Cloud-API-Dienst, um den Auftrag zu starten, und sendet im Verlauf regelmäßige Updates.

Wenn Sie Ihre eigene Automatisierungslösung entwickeln möchten, können Sie Aufrufe an den Clouddienst direkt mit Ihrer bevorzugten Programmiersprache erstellen. Detaillierte Informationen zum Konfigurieren und Verwenden der REST-Endpunkte und PowerShell-Module für Image Portability Service finden Sie im API-Portal.

### Workflows

Image Portability Service nutzt einen mehrstufigen Workflow, um ein Katalog-Masterimage von einem On-Premises-Ressourcenstandort für Ihre abonnierte öffentliche Cloud vorzubereiten. Das Image wird von der On-Premises-Hypervisorplattform exportiert und dann von Ihnen in die abonnierte öffentliche Cloud hochgeladen (Sie können dies mit unserem bereitgestellten PowerShell-Uploadprogramm automatisieren). Anschließend wird die Image-Kompatibilität mit der Plattform Ihrer öffentlichen Cloud vorbereitet. Zum Schluss wird das Image veröffentlicht und kann als neuer Maschinenkatalog in Ihrem Cloud-Ressourcenstandort bereitgestellt werden.




Diese allgemeinen Workflows basieren auf der konfigurierten Quell- und Zielbereitstellung des Images (Maschinenerstellungsdienste oder Citrix Provisioning). Der gewählte Workflow legt fest, welche Schritte für den Image Portability-Auftrag erforderlich sind.

In der folgenden Tabelle sehen Sie, welche Aufträge für jeden unterstützten IPS-Workflow erforderlich sind.

| Workflow (Quelle zum Ziel) | Exportieren | Hochladen | Vorbereiten | Veröffentlichen |
|---|---|---|---|---|
| MCS zu MCS | J | J | J | N |
| PVS zu MCS* | N | J | J | N |
| PVS zu PVS | – | J | J | J |
| MCS zu PVS | J | J | J | J |

*Setzt voraus, dass das Ausgangsimage als vDisk für Citrix Provisioning vorliegt und Sie es nicht direkt aus dem Hypervisor der Quellplattform exportieren müssen.

## Anforderungen

Zum Start von Image Portability müssen die folgenden Anforderungen erfüllt sein:

### Ein Citrix Maschinenkatalog-Image

Für IPS müssen Images in einer der folgenden getesteten Konfigurationen verwendet werden:

- Windows Server 2016, 2019 und 2022H2
- Windows 10 oder 11
- Provisioning mit MCS oder Citrix Provisioning erfolgt
- Citrix Virtual Delivery Agent:
  - Die letzten beiden kumulativen Updates für 1912 und 2203 LTSR
  - Die letzten beiden aktuellen Releases
- Remotedesktopdienste, für Konsolenzugriff in Azure aktiviert

Der Image Portability Service unterstützt die folgenden Hypervisors und Cloudplattformen:

**Quellplattformen:**

- VMware vSphere 7.0 und 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (nur Prism-Element)
- Microsoft Azure
- Google Cloud Platform

**Zielplattformen:**

- VMware vSphere 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (nur Prism-Element)
- Microsoft Azure
- AWS
- Google Cloud Platform

#### Eine Citrix Connector Appliance

Sie benötigen an jedem Ressourcenstandort, an dem Sie Image Portability verwenden möchten, eine installierte und konfigurierte Citrix Connector Appliance. Um beispielsweise mit Image Portability ein Image von vSphere zu Azure, AWS bzw. Google Cloud zu verschieben, benötigen Sie mindestens vier Citrix Connector Appliances:

Detaillierte Anweisungen finden Sie unter Connector Appliances bereitstellen.

#### Eine SMB-Dateifreigabe (Windows)

Sie benötigen eine Windows **SMB-Dateifreigabe** zum Speichern der Ausgabe von Exportjobs. Der Share muss für die Compositing Engine-VM zugänglich sein, die an dem Ressourcenstandort erstellt wird, an dem Sie den Image Portability Service verwenden. Der verfügbare freie Speicherplatz auf der Freigabe muss mindestens doppelt so groß sein wie das konfigurierte Dateisystem Ihres Images.

#### Eine Maschine zum Ausführen von PowerShell-Skripts

Ihre Maschine, auf der die PowerShell-Skripts ausgeführt werden, muss über Folgendes verfügen:

- PowerShell Version 5.1.
- Eine schnelle Netzwerkverbindung zur SMB-Dateifreigabe. Dies kann dieselbe Maschine sein, die die Dateifreigabe hostet.
- Eine schnelle Netzwerkverbindung zu den Plattformen der öffentlichen Cloud, wo Sie Image Portability verwenden möchten. Beispiele sind Azure, AWS und Google Cloud.

  Weitere Informationen zum Herunterladen und Konfigurieren der Image Portability-Module aus der PowerShell Gallery finden Sie im Abschnitt Vorbereiten einer Maschine für PowerShell.

#### Ihre Citrix Cloud-Kunden-ID

Sie müssen über ein gültiges Citrix DaaS-Abonnement verfügen.

Um fortzufahren, benötigen Sie Zugriff auf Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Wenden Sie sich an den zuständigen Citrix Mitarbeiter, wenn Sie keinen Zugriff haben.

Anweisungen zum Erstellen und Konfigurieren eines API-Clients für Image Portability finden Sie in der Einführung zu Citrix Cloud APIs.

#### Erforderliche Azure-Berechtigungen und -Konfiguration

Damit Image Portability Service Aktionen in Ihrer Azure-Ressource ausführen kann, müssen Sie dem von Image Portability Service verwendeten Azure-Dienstprinzipal Berechtigungen für bestimmte Azure-Funktionen erteilen. Eine ausführliche Liste finden Sie unter Erforderliche Microsoft Azure-Berechtigungen.

Sie können dem Dienstprinzipal in der zugehörigen Ressource die Rolle **Mitwirkender** zuweisen. Um die erforderlichen Mindestberechtigungen zuzuweisen, können Sie auch benutzerdefinierte Rollen mit den erforderlichen Berechtigungen erstellen und sie dem Dienstprinzipal mit den entsprechenden Ressourcen als Geltungsbereich zuweisen.

Informationen zum Konfigurieren von Sicherheitsrollen für Ihren Azure-Dienstprinzipal und zum Erstellen von benutzerdefinierten Rollen finden Sie in der Azure-Dokumentation.

#### Erforderliche Google Cloud-Berechtigungen und -Konfiguration

Damit Image Portability Service Aktionen in Ihrem Google Cloud-Projekt ausführen kann, erteilen Sie dem von Image Portability Service verwendeten Google Cloud-Dienstprinzipal Berechtigungen für bestimmte Funktionen erteilen.

Eine ausführliche Liste finden Sie unter Erforderliche Google Cloud-Berechtigungen.

Sie können diese Berechtigungen mit den folgenden Rollen zuweisen:

- Cloud Build-Editor
- Compute Admin
- Speicher-Administrator
- Dienstkontobenutzer

Weitere Informationen zum Konfigurieren von Dienstkontoberechtigungen finden Sie in der Google Cloud-Dokumentation.

#### Erforderliche Berechtigungen und Konfiguration für Amazon Web Services

Um Image Portability Service-Workflows mit einem Amazon Web Services (AWS)-Konto ausführen zu können, muss die entsprechende Identitäts- und Zugriffsverwaltungsidentität (IAM) die richtigen Berechtigungen haben.

Eine detaillierte Liste finden Sie unter Erforderliche AWS-Berechtigungen.

### Einrichten von Image Portability Service

Schrittfolge zum Einrichten von Image Portability Service:

- Connector Appliances bereitstellen
- Maschine für PowerShell vorbereiten
- Hinzufügen von Anmeldeinformationen zur Credential Wallet

#### Connector Appliances bereitstellen

Image Portability benötigt Citrix Connector Appliances, um Image Portability-Aufträge zu erstellen. Connector Appliances unterstützen sichere Interaktionen mit Ihren on-premises vorhandenen und

öffentlichen Cloud-Umgebungen. Die Connector Appliances senden Informationen zum Auftragsstatus und zum allgemeinen Dienstzustand an Image Portability Service.

Folgen Sie den Schritten in Connector Appliance für Cloudservices, um eine Connector Appliance in Ihrer Umgebung bereitzustellen und zu konfigurieren.

Beachten Sie beim Planen Ihrer Bereitstellung die erforderliche Hardwarekonfiguration und den Netzwerkportzugriff für das Connectorgerät.

Wenn Ihr Gerät bereitgestellt und registriert ist, werden die zum Aktivieren von Image Portability erforderlichen Komponenten automatisch installiert.

### Maschine für PowerShell vorbereiten

Um Sie bei der Inbetriebnahme von Image Portability zu unterstützen, haben wir PowerShell-Module erstellt, die Sie anpassen und mit dem Service verwenden können.

In den folgenden Abschnitten wird beschrieben, wie Sie eine Maschine für die Ausführung der PowerShell-Skripts vorbereiten. Diese Skripts sind nur einige Beispiele. Sie können sie an Ihre Bedürfnisse anpassen oder erweitern.

> **Hinweis:**
>
> Verwenden Sie nach der Erstinstallation **Update-Module**, um das PowerShell-Modul zu aktualisieren.

**PowerShell-Anforderungen** Zum Verwenden der PowerShell-Skripts benötigen Sie Folgendes:

- Eine Windows-Maschine zum Ausführen der PowerShell-Skripts, die Image Portability-Aufträge steuern. Dabei gilt für die Maschine:
  - Die aktuelle Version von PowerShell ist installiert.
  - Sie besitzt eine Netzwerkverbindung mit 10 Gbit/s oder besser zur on-premises bereitgestellten SMB-Dateifreigabe und eine schnelle Verbindung zur öffentlichen Cloud (z. B. Azure, AWS oder Google Cloud).
  - Dies kann dieselbe Maschine sein, die die Dateifreigabe hostet.
  - Sie verwendet Windows 10, Windows Server 2019 oder Windows Server 2022 mit den neuesten Microsoft-Patches.
  - Sie kann eine Verbindung zu Microsoft PowerShell Gallery herstellen, um die erforderlichen PowerShell-Bibliotheken herunterzuladen.

Je nach verwendeter Windows-Version müssen Sie möglicherweise die Unterstützung für TLS 1.0/1.1 deaktivieren. Weitere Informationen finden Sie in der Supportdokumentation für Microsoft PowerShell Gallery TLS .

Standardmäßig authentifiziert PowerShell sich nicht automatisch über einen Proxyserver. Stellen Sie sicher, dass Sie Ihre PowerShell-Sitzung zur Verwendung des Proxyservers konfiguriert haben, gemäß den bewährten Methoden von Microsoft und Ihres Proxyanbieters.

Wenn beim Ausführen der PowerShell-Skripts Fehler aufgrund einer fehlenden oder alten Version von PowerShellGet auftreten, müssen Sie die neueste Version wie folgt installieren:

```
Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
    AllowClobber
<!--NeedCopy-->
```

**Installieren von Bibliotheken und Modulen** Image Portability Service nutzt Bibliotheken aus der Microsoft PowerShell Gallery, um Portabilitätsvorgänge durchzuführen.

> **Wichtig:**
>
> Verwenden Sie nach der Erstinstallation **Update-Module**, um neue Versionen zu installieren.

1. Führen Sie den folgenden PowerShell-Befehl aus, um die neuesten Module herunterzuladen:

   ```
   Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
       Uploader" -Scope CurrentUser
   <!--NeedCopy-->
   ```

   - Zum Ändern der Umgebungsvariable PATH:

     Drücken Sie **Y** und dann zum Akzeptieren die **Eingabetaste**.

   - Zum Installieren des NuGet-Anbieters:

     Drücken Sie **Y** und dann zum Akzeptieren die **Eingabetaste**.

   - Beim Verweis auf ein nicht vertrauenswürdiges Repository:

     Drücken Sie **A** (Ja für alle) und dann zum Fortfahren die **Eingabetaste**.

2. Führen Sie folgenden Befehl aus, um sicherzustellen, dass alle erforderlichen Module heruntergeladen wurden:

   ```
   Get-InstalledModule -Name Citrix.*
   <!--NeedCopy-->
   ```

   Dieser Befehl gibt eine Ausgabe zurück, die der folgenden ähnelt:

| Name | Repository | Beschreibung |
| --- | --- | --- |
| Citrix.Image.Uploader | PSGallery | Befehle zum Hochladen einer VHD(x) in ein Azure-Speicherkonto, AWS oder GCP und Abrufen von Informationen über eine VHD(x) |
| Citrix.Workloads.Portability | PSGallery | Eigenständiges Cmdlet für den Image-Auftrag von Citrix Image Portability Service |

**Aktualisieren von Modulen auf die neueste Version** Führen Sie den folgenden Befehl aus, um das Skript auf die neueste Version zu aktualisieren:

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

**Installieren des Citrix Virtual Apps and Desktops Remote PowerShell SDK** Image Portability Service benötigt das Remote PowerShell SDK von Citrix Virtual Apps and Desktops, um Portabilitätsaufträge in Citrix Cloud zu erstellen und zu verwalten.

Laden Sie das Remote PowerShell SDK herunter und installieren Sie es auf Ihrer Maschine.

**Installieren der plattformspezifischen Komponenten von Drittanbietern** Das Image Portability Service PowerShell-Modul installiert keine Abhängigkeiten von Drittanbietern. Daher können Sie die Installation auf die gewünschten Plattformen beschränken. Wenn Sie eine der folgenden Plattformen verwenden, befolgen Sie die entsprechenden Anweisungen für die Installation von Plattformabhängigkeiten:

**VMware** Wenn Sie Image Portability-Aufträge erstellen, die mit Ihrer VMware-Umgebung kommunizieren, führen Sie den folgenden Befehl aus, um die erforderlichen VMware PowerShell-Module zu installieren.

```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

**Amazon Web Services** Wenn Sie Image Portibility-Aufträge in AWS erstellen, laden Sie die AWS-Befehlszeilenschnittstelle herunter und installieren Sie sie. Führen Sie dann die folgenden Befehle aus, um die erforderlichen AWS PowerShell-Module zu installieren:

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```

**Azure** Wenn Sie Image Portability-Aufträge in Azure erstellen, laden Sie die Azure-Befehlszeilenprogramme herunter und installieren Sie sie. Führen Sie die Befehle dann aus, um die erforderlichen Azure PowerShell-Module zu installieren:

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```

**Google Cloud** Wenn Sie Image Portibility-Aufträge in Google Cloud erstellen, laden Sie das Google Cloud SDK herunter und installieren Sie es auf Ihrer Maschine.

**Deinstallation von Skripts und Modulen** Führen Sie die folgenden Befehle aus, um die von der Image Portability-Software verwendeten Module zu deinstallieren.

> **Hinweis:**
>
> Skripts und Komponenten von Drittanbietern werden bei der Deinstallation von IPS-Modulen nicht automatisch entfernt.

Zum Deinstallieren von Modulen:

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images
    .Uploader" | Uninstall-Module
<!--NeedCopy-->
```

#### Hinzufügen von Anmeldeinformationen zur Credential Wallet

Für vollständig automatisierte Szenarios können Sie in Image Portability Service eine interaktionsfreie Authentifizierung bei in Citrix Cloud, Ihrer öffentlichen Cloud und on-premises bereitgestellten Ressourcen konfigurieren. Image Portability Service verwendet zudem die in der Citrix Credential Wallet gespeicherten Anmeldeinformationen, sobald unsere APIs sich direkt bei Ihren on-premises oder in der öffentlichen Cloud bereitgestellten Ressourcen authentifizieren. Das Einrichten von Anmeldeinformationen, wie in diesem Abschnitt beschrieben, ist für das Ausführen von Export-, Vorbereitungs- und Veröffentlichungsaufträgen erforderlich.

Bei der Auftragsausführung benötigt Image Portability Service Zugriff auf Ressourcen, die Sie steuern können. Damit beispielsweise ein Datenträger von einem vSphere-Server in eine SMB-Freigabe exportiert werden kann, benötigt Image Portability Service die Anmeldeinformationen für beide Systeme. Zur Sicherung dieser Kontoinformationen verwendet Image Portability Service den Citrix Credential Wallet-Dienst. Dieser Dienst speichert Ihre Anmeldeinformationen mit einem benutzerdefinierten Namen in der Wallet. Wenn Sie dann einen Auftrag ausführen möchten, geben Sie den Namen der gewünschten Anmeldeinformationen an. Diese Anmeldeinformationen können jederzeit aktualisiert oder aus der Wallet gelöscht werden.

Anmeldeinformationen werden häufig für diese Plattformen gespeichert:

- Microsoft Azure
- AWS
- Google Cloud
- SMB-Freigabe
- VMware vSphere
- Nutanix AHV
- XenServer

Informationen zum Verwalten von Anmeldeinformationen finden Sie im Entwickler-API-Portal im Abschnitt zu Image Portability Service-APIs und unter "Credentials Management".

## Verwendung von Image Portability Service

Um Images in On-Premises-Ressourcenstandorten für Ihre abonnierte öffentliche Cloud vorzubereiten, müssen Sie Image Portability-Aufträge in Citrix Cloud erstellen. Sie können einen Auftrag für direkte API-Aufrufe an den Dienst in Ihrem Skript oder Programm erstellen oder die PowerShell-Beispielmodule verwenden, die wir zur Automatisierung von API-Aufrufen entwickelt haben. Informationen zum Erstellen von IPS-Aufträgen über REST-APIs und PowerShell-Module finden Sie unter Image Portability Service Developer API Portal.

### Maschinenkataloge mit Citrix Provisioning veröffentlichen

Der Image Portability Service (IPS) wird mit Machine Creation Services (MCS) in Azure, AWS, Google Cloud, Nutanix, vSphere und XenServer oder mit Citrix Provisioning (PVS) in Azure, Google Cloud, vSphere und XenServer verwendet. Sie können die hier beschriebenen PowerShell- und REST-Lösungen mit den Tools oder APIs Ihrer Plattform oder den Citrix DaaS-SDKs kombinieren, um einen nahtlosen und automatisierten Komplettworkflow für die Erstellung eines Maschinenkatalogs auf der Grundlage des vorbereiteten Images zu erstellen. Abhängig von der von Ihnen gewählten Cloudplattform können Zwischenschritte zwischen der IPS-Vorbereitung und der Erstellung eines Katalogs oder einer Zuordnung zu einem PVS-Ziel erforderlich sein.

**AWS** IPS-Vorbereitungsaufträge in AWS produzieren ein Volume. Maschinenerstellungsdienste benötigen bei der Katalogerstellung ein Amazon Machine Image (AMI). Um ein AMI aus Ihrem migrierten Image zu generieren, müssen Sie zunächst einen Image-Snapshot aus dem generierten Volume erstellen und dann ein AMI auf der Grundlage dieses Snapshots. Hierfür können Sie die AWS-Befehlszeilenschnittstelle (CLI) verwenden:

```
> aws ec2 create-snapshot --volume-id <VolumeId>
> aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
 SnapshotId=<SnapshotID> }
 '
<!--NeedCopy-->
```

<VolumeId> ist die Ausgabe des IPS-Vorbereitungsauftrags. Das resultierende AMI kann als MCS-Masterimage verwendet werden.

Ein PowerShell-Skriptmuster zur Automatisierung dieses Teils des Workflows ist im Modul Citrix.Workloads.Portability unter dem Namen `New-IpsAwsImage.ps1` enthalten.

**Azure** In Azure erstellt IPS verwaltete Datenträger, die direkt als MCS-Masterimage verwendet werden können. Um das resultierende Image PVS-Zielen zuzuweisen, bietet IPS einen "Veröffentlichen" -Vorgang, mit dem der verwaltete Datenträger in eine VHD(x)-Datei im PVS-Speicher kopiert wird.

**Google Cloud** IPS-Vorbereitungsaufträge in Google Cloud produzieren einen Datenträger. MCS erfordert eine Google Cloud-Instanzvorlage. Der Prozess zum Erstellen einer MCS-Instanzvorlage aus einem Datenträger wird unter Vorbereiten einer Master-VM-Instanz und eines nichtflüchtigen Speichers ausführlich beschrieben.

Für PVS-Ziele in Google Cloud bietet IPS einen "Veröffentlichen"-Vorgang, mit dem der Datenträger in eine VHD(x)-Datei im PVS-Speicher kopiert wird.

#### Automatisieren der VDA-Konfiguration

Wenn Sie ein on-premises erstelltes und von Citrix verwaltetes Image vorbereiten, können Sie den VDA im Image neu konfigurieren, um ihn an die Zielumgebung anzupassen, für die das Image vorbereitet wird. Image Portability Service kann Änderungen der VDA-Konfiguration während der Vorbereitungsphase des Workflows sofort übernehmen. Die folgenden Konfigurationsparameter definieren, wie der VDA im migrierten Image arbeitet: **InstallMisa**, **XdReconfigure** und **InstallMcsio**. In den PowerShell-Beispielen für Image Portability Service finden Sie Informationen zur Definition dieser Parameter beim Erstellen von IPS-Jobs.

**Konfigurationen**

- Wenn Sie **InstallMisa** auf `true` setzen, kann der Image Portability Service fehlende VDA-Komponenten installieren, die für das Provisioning des Images mit MCS erforderlich sind.
- Bei Auswahl von `true` für **InstallMisa** oder `true` für **InstallMcsio** muss **CloudProvisioningType** auf `Mcs` gesetzt werden.
- Wählen Sie für **InstallPvs** die Version des PVS-Servers, auf dem das Image bereitgestellt wird. Wenn **InstallPvs** festgelegt ist, installiert Image Portability Service (IPS) bei Vorbereitungsaufträgen automatisch die angegebene Version der PVS-Zielgerätesoftware im Image. IPS unterstützt die zwei neuesten Builds (Basisversion oder kumulative Updates (CUs)) für die letzten zwei Versionen von Long-Term Service Release (LTSR) und Aktuelles Release (CR).

Beachten Sie Folgendes für **InstallMisa** und **InstallMcsio**:

- Diese Funktionen werden nur für aktuelle LTSR- und CR-Versionen des VDA unterstützt.
- Wenn die erforderlichen Komponenten für den installierten VDA bereits vorhanden sind, werden keine Änderungen vorgenommen, selbst wenn die Parameter konfiguriert sind.
- Bei unterstützten VDA-Versionen installiert Image Portability die entsprechende Version der erforderlichen Komponenten, selbst wenn die notwendigen VDA-Komponenten nicht vorhanden sind.
- Bei nicht unterstützten VDA-Versionen schlägt die Neukonfiguration fehl und es wird eine Meldung protokolliert, falls die notwendigen VDA-Komponenten nicht vorhanden sind. Der Vorbereitungsauftrag wird abgeschlossen, auch wenn die Neukonfiguration des VDAs nicht erfolgt ist.

**XdReconfigure** erfordert einen der folgenden Werte: `controllers` oder `site_guid`. Hier sind Beispiele für Konfigurationsparameter, die die einzelnen Werte verwenden:

Mit **controllers**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'controllers'
        ParameterValue = 'comma-separated-list-of-your-cloud-connectors
           -fqdns'
     }

)
<!--NeedCopy-->
```

**ParameterValue** ist hierbei die Liste der FQDNs der neuen DDCs, auf die der VDA zeigen soll. Es können mehrere DDCs im kommagetrennten Format angegeben werden.

Mit **site_guid**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'site_guid'
        ParameterValue = 'active-directory-site-guid'
     }

)
<!--NeedCopy-->
```

**XdReconfigure** akzeptiert auch Werte, die unterstützt werden, wenn das Programm zur VDA-Installation über die Befehlszeile mit dem Switch **/reconfigure** ausgeführt wird, z. B. **XenDesktopVdaSetup.exe /reconfigure**. Mögliche Werte sind zum Beispiel **wem_agent_port**, **wem_cached_data_sync_port**, **wem_cloud_connectors** oder **wem_server**. Eine vollständige Liste der Befehlszeilenoptionen für die VDA-Neukonfiguration finden Sie in der Dokumentation zum Citrix DaaS-VDA.

Wenn **InstallMcsio** auf `true` konfiguriert ist, wird MCSIO automatisch auf dem Image installiert. Um die automatische MCSIO-Installation auf dem Image zu deaktivieren, konfigurieren Sie **InstallMcsio** auf `false`.

> **Hinweis:**
>
> Sie können bei der Ausführung Ihrer Befehle `-DryRun` verwenden, um Ihre Konfiguration und die Netzwerkeinstellungen der Connector Appliance zu überprüfen.

## Referenz

In diesem Abschnitt finden Sie ausführliche technische Referenzinformationen, angepasst an Ihre Bedürfnisse.

### Erforderliche Berechtigungen für Image Portability Service

Dieser Abschnitt erläutert die Berechtigungen, die von Image Portability Service auf den unterstützten On-Premises- und Cloud-Plattformen benötigt werden.

**Erforderliche Connector Appliance-Berechtigungen** Die Connector Appliance benötigt Zugriff auf die folgenden URLs, um Images im Image Portability Service vorzubereiten:

```
api-ap-s.cloud.com
api-eu.cloud.com
api-us.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
```

```
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

**Erforderliche VMware vCenter-Berechtigungen** Die folgenden vCenter-Berechtigungen sind erforderlich, um den IPS-Auftrag zum Datenträgerexport in einer VMware-Umgebung auszuführen. Sie finden diese Berechtigungen unter **Rollen** im Abschnitt **Zugriffssteuerung** des vCenter-Verwaltungsbereichs.

```
- Cryptographic operations
    - Direct Access

- Datastore
    - Allocate space
    - Browse datastore
    - Low level file operations
    - Remove file

- Folder
    - Create folder
    - Delete folder

- Network
    - Assign network

- Resource
    - Assign virtual machine to resource pool

- Virtual machine
    - Change Configuration
        - Add existing disk
        - Add new disk
        - Remove disk

    - Edit Inventory
        - Create from existing
        - Create new
        - Remove

    - Interaction
        - Power off
        - Power on
<!--NeedCopy-->
```

**Erforderliche Microsoft Azure-Berechtigungen** Zum Verwenden von Image Portability muss Ihr Azure-Dienstkonto über folgende Berechtigungen verfügen.

Wenn die Ressourcengruppe angegeben ist, die für die Compositing Engine verwendet werden soll (in

der Eigenschaft *resourceGroup* in einer REST-Anforderung oder im Parameter *-AzureVmResourceGroup*, wenn die PowerShell-Befehle für Citrix.Workloads.Portability verwendet werden), sind die folgenden Berechtigungen im Geltungsbereich der Ressourcengruppe erforderlich.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/delete
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/delete
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/read
<!--NeedCopy-->
```

Wenn die Ressourcengruppe, die für die Compositing Engine verwendet werden soll, nicht angegeben ist, sind die folgenden Berechtigungen im Geltungsbereich des Abonnements erforderlich.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```

Die folgenden Berechtigungen sind im Geltungsbereich der angegebenen Zielressourcengruppe erforderlich (d. h. der Ressourcengruppe, die in der Eigenschaft *targetDiskResourceGroupName* in einer REST-Anforderung angegeben ist oder im Parameter *-TargetResourceGroup*, wenn die PowerShell verwendet wird).

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

Die folgenden Berechtigungen sind im Geltungsbereich der angegebenen Ressourcengruppe für das virtuelle Netzwerk erforderlich (d. h. der Ressourcengruppe, die in der Eigenschaft *virtualNetworkResourceGroupName* in einer REST-Anforderung angegeben ist oder im Parameter *-AzureVirtualNetworkResourceGroupName*, wenn die PowerShell verwendet wird).

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```

> **Wichtig:**
>
> Die Option `ceVmSku` für die Aufträge “prepare”und “prepareAndPublish”steuert den Typ der Azure-VM, für die der erzeugte verwaltete Datenträger geeignet ist. Sie müssen eine ceVmSku mit der Familie und der Version auswählen die mit denen der VMs, die Sie aus dem Ausgabeimage bereitstellen möchten, identisch sind. Der Standardwert `Standard_D2S_v3` eignet sich für die Ausführung auf allen Maschinen der v3 D-Familie. Die Angabe von Maschinen-SKUs, die keinen temporären Datenträger enthalten, wird nicht unterstützt.

**Erforderliche Google Cloud-Berechtigungen** Zum Verwenden von Image Portability muss Ihr Google Cloud-Dienstkonto über folgende Berechtigungen verfügen:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
```

```
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

**Erforderliche Berechtigungen für AWS** Image Portibility erfordert, dass Sie ein JSON-Richtliniendokument mit der folgenden Konfiguration an den Identitäts- und Zugriffsverwaltungsbenutzer (IAM) anhängen:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--NeedCopy-->
```

> **Hinweis:**
>
> Reduzieren Sie den Umfang der Ressource nach Bedarf weiter.

**Für Nutanix AHV benötigte Genehmigungen** Für Image Portability müssen Sie in Ihrer Nutanix AHV-Konfiguration Cluster-Administrator sein.

**Erforderliche Berechtigungen für XenServer** Für Image Portability benötigen Sie mindestens die Rolle "VM-Administrator"für den Pool, in dem sich der XenServer-Host befindet.

**Netzwerke** Image Portability Service (IPS) erstellt eine Worker-VM ("Compositing Engine", CE), um Image-Operationen durchzuführen. Alle Connector Appliances am zugewiesenen Ressourcenstandort müssen in der Lage sein, über HTTPS mit der Compositing Engine zu kommunizieren.
Die gesamte Kommunikation zwischen einer Connector Appliance (CA) und der Compositing Engine wird von der Connector Appliance initiiert. Die einzige Ausnahme bildet vSphere, wo eine bidirektionale HTTPS-Kommunikation zwischen Compositing Engine und Connector Appliance besteht.

In Cloud-Umgebungen (Azure, AWS, Google Cloud) wird die Compositing Engine mit einer privaten IP-Adresse erstellt. Die CE muss daher in demselben virtuellen Netzwerk wie die Connector Appliance sein oder in einem virtuellen Netzwerk, das von der Connector Appliance aus erreichbar ist.

Darüber hinaus muss sich die Compositing Engine bei Aufträgen, die Dateien auf einer SMB-Freigabe enthalten (z. B. Exportaufträge), in einem Netzwerk mit Konnektivität zur SMB-Freigabe befinden.

Einzelheiten zum Festlegen des Netzwerks, das für die Compositing Engine auf jeder unterstützten Plattform zu verwenden ist, finden Sie in der Dokumentation zur Image Portability Service API.

Bei "prepare"-Aufträgen wird das im Image enthaltene Betriebssystem gestartet (auf der CE), um die Spezialisierung und andere Aufgaben auszuführen. Enthält das Image Verwaltungs- oder Sicherheitsagents, die einen Steuerserver anrufen, können diese Prozesse den Vorbereitungsprozess stören.

Wenn die Option zur Trennung von der Domäne angegeben wird, kann sich die Netzwerkverbindung auf die Ergebnisse auswirken. Kann die Compositing Engine-VM den Active Directory-Domänencontroller über das Netzwerk erreichen kann, entfernt die Option das Computerkonto aus der Domäne. Dadurch wird die Domänenmitgliedschaft der Quell-VM beendet, aus der das Image extrahiert wurde.

Daher empfehlen wir, das Netzwerk für den Betrieb von anderen Netzwerkressourcen zu isolieren. Dies kann durch Subnetzisolierung oder Firewallregeln umgesetzt werden. Weitere Informationen finden Sie unter Netzwerkisolation.

In einigen on-premises bereitgestellten Hypervisorumgebungen kann der Hypervisor mit einem TLS-Serverzertifikat konfiguriert sein, das von den vertrauenswürdigen Stammzertifizierungsstellen der Connector Appliance (CA) als nicht vertrauenswürdig eingestuft wird oder nicht mit dem Hostnamen des Servers übereinstimmt. In diesen Situationen bietet IPS **Eigenschaften für Auftragsanforderungen**, mit denen das Problem umgangen werden kann. Einzelheiten finden Sie unter TLS-Zertifikate.

**Netzwerkproxys** Wenn der Netzwerkverkehr zwischen der ZS und dem Internet einen Proxy durchläuft, der eine TLS-Introspektion durchführt, kann es erforderlich sein, die Stammzertifizierungsstelle des Proxys (d. h. das Zertifikat, das der Proxy zum Signieren der von ihm generierten TLS-Zertifikate verwendet) zu den Stammzertifizierungsstellen der ZS hinzuzufügen. Weitere Informationen finden Sie unter Connector Appliance bei Citrix Cloud registrieren.

### Netzwerkisolation

- Azure

  In Azure wird die CE standardmäßig mit einer Netzwerksicherheitsgruppe (NSG) erstellt, die an die Netzwerkkarte angehängt ist, sofern der verwendete Azure-Dienstprinzipal über die erforderlichen Azure-Berechtigungen [1] verfügt.

  - Microsoft.Network/networkSecurityGroups/join/action
  - Microsoft.Network/networkSecurityGroups/read
  - Microsoft.Network/networkSecurityGroups/write

    Andernfalls gelten die folgenden Berechtigungen im Geltungsbereich des Abonnements, wenn keine explizite Ressourcengruppe verwendet wird:

    * Microsoft.Network/networkSecurityGroups/delete
    * Microsoft.Network/networkSecurityGroups/join/action
    * Microsoft.Network/networkSecurityGroups/read

    * Microsoft.Network/networkSecurityGroups/write

  Diese NSG ist so konfiguriert, dass sie den gesamten Ein-/Ausgangsverkehr der CE blockiert, mit Ausnahme von:

  - SMB (Port 445) ausgehend
  - HTTPS (Port 443) eingehend
  - für interne Azure-Dienste erforderlicher Datenverkehr

  Die Verwendung der NSG kann erzwungen werden, indem die Eigenschaft *networkIsolation* in der Auftragsanforderung auf *true* gesetzt wird. In diesem Fall schlägt der Auftrag fehl, wenn der für den Vorgang verwendete Dienstprinzipal nicht über die erforderlichen Berechtigungen verfügt. Die Verwendung der NSG kann deaktiviert werden, indem die Eigenschaft *networkIsolation* auf *false* gesetzt wird.

- AWS

Um in AWS eine Netzwerkisolation der CE zu erreichen, können Sie eine oder mehrere Netzwerksicherheitsgruppen erstellen, die jeden unerwünschten Datenverkehr blockieren. Die Sicherheitsgruppen weisen Sie dann in der Auftragsanforderung der CE-Instanz zu, unter Verwendung des Anforderungsparameters *SecurityGroupIDs*, der eine Liste von Sicherheitsgruppen-IDs als Wert akzeptiert.

- Google Cloud

Um in Google Cloud eine Netzwerkisolation der CE zu erreichen, können Sie Firewallregeln erstellen, die jeden unerwünschten Datenverkehr blockieren, und die Regeln über Netzwerktags auf die CE anwenden. IPS erstellt dann die CE mit dem Netzwerktag *compositing-engine* und Sie können weitere Netzwerktags mit dem Auftragsanforderungsparameter *networkTags* zuweisen, der eine Liste von Tags als Wert akzeptiert.

**TLS-Zertifikate** Wenn das Serverzertifikat des Hypervisors von einer für die ZS nicht vertrauenswürdigen Authority signiert ist, gibt es zwei Möglichkeiten, das Problem zu beheben.

1. Geben Sie in der Auftragsanforderung ein zusätzliches Zertifikat der Stammzertifizierungsstelle an, das bei der Zertifikatsprüfung zu verwenden ist. Dieses Zertifikat muss zur Stammzertifizierungsstelle gehören, die zum Signieren des Serverzertifikats des Hypervisors verwendet wird.
2. Geben Sie in der Auftragsanforderung den SHA-1-Fingerabdruck des Serverzertifikats des Hypervisors an. In diesem Fall wird bei der Zertifikatsprüfung überprüft, ob der SHA-1-Fingerabdruck des vom Hypervisor zurückgegebenen Zertifikats mit dem Zertifikat in der Auftragsanforderung übereinstimmt. Diese Methode funktioniert möglicherweise nicht, wenn zwischen der CE und dem Hypervisor ein TLS-Abfangproxy installiert ist.

Die Auftragsanforderungsparameter für die obigen Verfahren sind wie folgt (angegeben pro Plattform):

- vSphere
    1. vCenterSslCaCertificate
    2. vCenterSslFingerprint
- Nutanix
    1. prismSslCaCertificate
    2. prismSslFingerprint
- XenServer
    1. xenSslCaCertificate
    2. xenSslFingerprint

Weitere Informationen finden Sie in der Image Portability Service API-Dokumentation.

Fehler bei der Zertifikatsprüfung können auch auftreten, wenn der Hostname des Hypervisorservers und der Hostname im Zertifikat nicht übereinstimmen. In diesem Fall kann der Hostnamenabgleich deaktiviert werden, indem der folgende Parameter in der Auftragsanforderung auf *true* gesetzt wird:

- vSphere
    - vCenterSslNoCheckHostname
- Nutanix
    - prismSslNoCheckHostname
- XenServer
    - xenSslNoCheckHostname

### Zugehörige Dokumentation

- Image Portability Service API-Dokumentation
- Connector Appliance für Cloudservices
- Google Cloud-Dokumentation
- Google Cloud-Dienstkonten
- Registrierung und Authentifizierung der Microsoft Azure-App

1. If Eine explizite Ressourcengruppe wird für den Vorgang verwendet, dann die folgenden Berechtigungen im Geltungsbereich der Ressourcengruppe: 

# Drucken

April 19, 2022

Die Druckerverwaltung in Ihrer Umgebung umfasst verschiedene Stufen:

1. Machen Sie sich, falls erforderlich, mit den Druckkonzepten vertraut.
2. Planen der Druckarchitektur. Dazu gehört die Analyse folgender Faktoren: Unternehmensanforderungen, vorhandene Druckinfrastruktur, derzeitige Interaktion von Benutzern und Anwendungen mit Druckvorgängen und das für Ihre Umgebung am besten geeignete Druckverwaltungsmodell.
3. Konfigurieren Sie die Druckumgebung, indem Sie eine Druckerbereitstellungsmethode auswählen und dann Richtlinien zur Bereitstellung Ihres Druckkonzepts erstellen. Aktualisieren Sie Richtlinien, wenn neue Mitarbeiter oder Server hinzugefügt werden.
4. Testen einer Druckkonfiguration, bevor sie den Benutzern bereitgestellt wird.
5. Pflegen Sie die Citrix Druckumgebung durch Verwalten von Druckertreibern und Optimieren der Druckleistung.
6. Beseitigen Sie evtl. auftretende Probleme.

Umfassende Informationen zum Drucken in einer Umgebung mit Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) finden Sie unter Drucken. Von diesem Artikel aus können Sie fortfahren mit:

- Druckkonfigurationsbeispiele
- Bewährte Methoden
- Druckrichtlinien und Einstellungen
- Bereitstellen von Druckern
- Pflegen der Druckumgebung

## Installieren des universellen Druckservers auf den Druckservern

1. Stellen Sie sicher, dass auf jedem Druckserver Microsoft Virtual C++ Runtime 2017 (32-Bit- und 64-Bit-Edition) installiert ist.
2. Navigieren Sie zur Downloadseite für den universellen Citrix Druckserver und klicken Sie auf **Datei herunterladen**.
3. Führen Sie einen der folgenden Befehle auf jedem Druckserver aus:
   - Für ein 32-Bit-Betriebssystem: **UpsServer_x86.msi**.
   - Für ein 64-Bit-Betriebssystem: **UpsServer_x64.msi**.

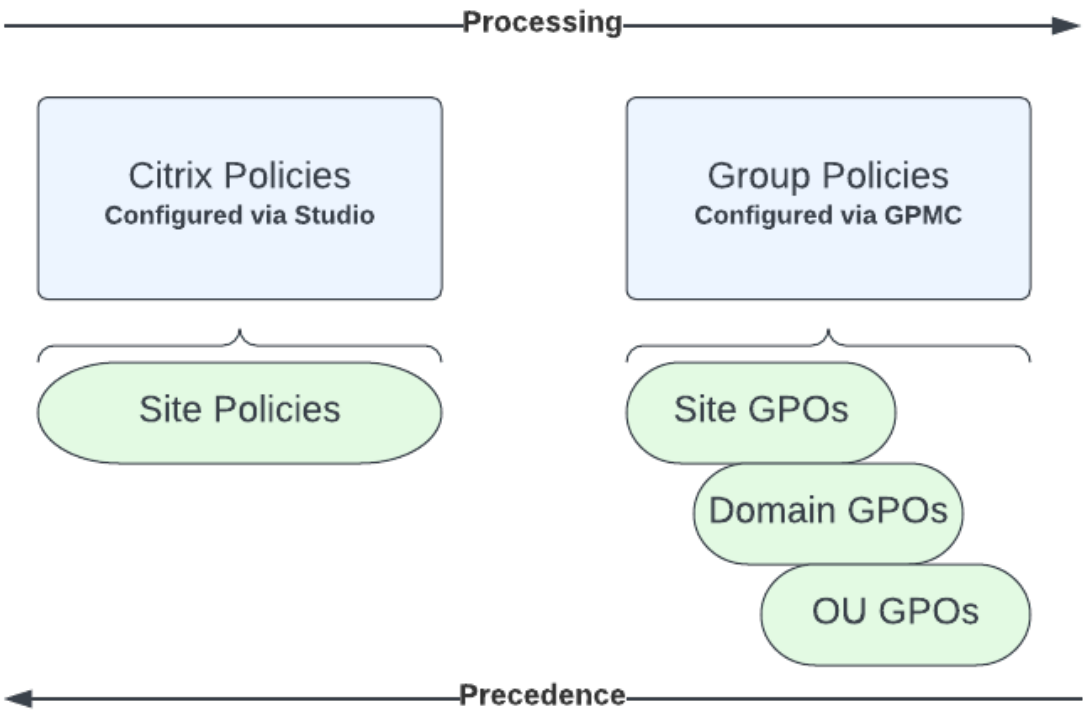
Nach der Installation des universellen Druckservers konfigurieren Sie ihn anhand der Anweisungen unter Bereitstellen von Druckern.

## Richtlinien

April 14, 2023

Richtlinien sind eine Sammlung von Einstellungen, die definieren, wie Sitzungen, Bandbreite und Sicherheit für eine Gruppe von Benutzern, Geräten oder Verbindungstypen verwaltet werden.

Sie können Richtlinieneinstellungen auf VDAs oder auf Benutzer anwenden. Sie können Einstellungen in Web Studio oder in den Active Directory-Gruppenrichtlinienobjekten bearbeiten. Sie können Filter (Objektzuweisungen) für Richtlinien festlegen. Wenn Sie für Richtlinien keine Filter festlegen, gelten die Einstellungen für alle Verbindungen.




Sie können Richtlinien auf unterschiedliche Ebenen des Netzwerks zuweisen. Richtlinieneinstellungen, die auf der GPO-Ebene der Organisationseinheit zugewiesen werden, haben die höchste Priorität im Netzwerk. Richtlinien auf der Domänen-GPO-Ebene überschreiben Richtlinien auf der Ebene der Sitegruppenrichtlinienobjekte. Die Ebene der Sitegruppenrichtlinienobjekte überschreibt alle lokalen Richtlinien von Microsoft und Citrix, die mit ihnen in Konflikt stehen.

Alle Citrix Site-Richtlinien werden in der Web Studio-Konsole erstellt und verwaltet und in der Sitedatenbank gespeichert. Gruppenrichtlinien werden mithilfe der Microsoft-Gruppenrichtlinien-Verwaltungskonsole erstellt und verwaltet und in Active Directory gespeichert. Lokale Microsoft-Richtlinien werden im Windows-Betriebssystem erstellt und in der Registrierung gespeichert.

Mit dem Modellierungsassistenten in Web Studio können Administratoren Konfigurationseinstellungen in Vorlagen und Richtlinien vergleichen, um miteinander in Konflikt stehende und redundante Einstellungen leichter zu eliminieren.

Einstellungen werden entsprechend ihrer Priorität und Bedingung zusammengefasst. Deaktivierte Einstellungen haben Vorrang vor aktivieren Einstellungen mit niedriger Priorität. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

Web Studio-Richtlinien können auch mit Gruppenrichtlinien in Active Directory in Konflikt stehen. Abhängig von der Situation könnten sie einander außer Kraft setzen.

Alle Richtlinien werden in der folgenden Reihenfolge verarbeitet:

1. Der Endbenutzer meldet sich über die Citrix Workspace-App mit Domänenanmeldeinformationen an einem VDA an.
2. Citrix Richtlinien werden für den Endbenutzer und den VDA verarbeitet.
3. Richtlinien werden in der folgenden Reihenfolge angewendet:

    a) Lokale Richtlinien
    b) Siterichtlinien
    c) Domänenrichtlinien
    d) Richtlinien der Organisationseinheit

> **Hinweis:**
>
> - Möglicherweise sind nicht alle Richtlinien auf den vier Ebenen vorhanden. Für die meisten Kunden werden nur Siterichtlinien verwendet. Bei lokalen Richtlinien müssen Benutzer sich am VDA anmelden, um Richtlinien zu bearbeiten. Daher werden diese Richtlinien fast nie verwendet.
> - Das Verwenden von Windows- und Citrix-Richtlinien im gleichen GPO wird nicht unterstützt.

Vollständige Informationen zu Citrix Richtlinien enthalten die folgenden Artikel:

- Richtlinien einsetzen
- Richtlinienvorlagen
- Richtlinien erstllen

- Richtlinien prioritisieren, modellieren und vergleichen sowie Problembehandlung
- Standardrichtlinieneinstellungen
- Referenz für Richtlinieneinstellungen

> **Hinweis:**
>
> Die Richtlinieneinstellungen für Citrix DaaS sind dieselben wie diejenigen für Citrix Virtual Apps and Desktops. Das Kapitel Referenz für Richtlinieneinstellungen in der Dokumentation zu Citrix Virtual Apps and Desktops gilt somit auch für Citrix DaaS.

## Richtlinien einsetzen

May 23, 2023

Durch das Konfigurieren von Citrix Richtlinien steuern Sie den Benutzerzugriff und die Sitzungsumgebung. Citrix Richtlinien sind die effizienteste Methode zum Steuern der Verbindungs-, Sicherheits- und Bandbreiteneinstellungen. Sie erstellen Richtlinien für bestimmte Benutzergruppen, Geräte oder Verbindungstypen. Jede Richtlinie kann mehrere Einstellungen enthalten.

### Tools zum Arbeiten mit Citrix Richtlinien

- Studio: Mit Studio erstellte Richtlinien werden in der Sitedatenbank gespeichert, und die Updates werden an den VDA übertragen, wenn einer der folgenden Fälle eintritt:
  - Der VDA registriert sich beim Controller.
  - Ein Benutzer startet eine Sitzung.
- Gruppenrichtlinien-Verwaltungskonsole: Wenn Sie in Ihrer Netzwerkumgebung Active Directory verwenden und Sie die Berechtigungen zur Verwaltung von Gruppenrichtlinien haben, können Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, um Richtlinien für Ihre Site zu erstellen. In der Konsole können Sie Gruppenrichtlinienobjekte (GPOs) mit den gewünschten Einstellungen und Filtern konfigurieren. Diese Richtlinien haben Vorrang vor den in Studio konfigurierten Richtlinien. Weitere Informationen finden Sie unter CTX238166.

### Reihenfolge und Priorität bei der Richtlinienverarbeitung

Gruppenrichtlinieneinstellungen (GPOs) werden in der folgenden Reihenfolge verarbeitet:

1. Gruppenrichtlinienobjekt der Citrix DaaS-Site (in der Sitedatenbank gespeichert)

2. GPOs auf Domänenebene
3. Organisationseinheiten

Wenn jedoch in zwei Gruppenrichtlinienobjekten unterschiedliche Einstellungen für dieselbe Richtlinie angewendet werden, überschreiben die zuletzt verarbeiteten Richtlinieneinstellungen die zuvor verarbeiteten Einstellungen. Aufgrund dieser Konfiguration gilt für Richtlinieneinstellungen die folgende Rangfolge:

1. Organisationseinheiten
2. GPOs auf Domänenebene
3. Gruppenrichtlinienobjekt der Citrix DaaS-Site (in der Sitedatenbank gespeichert)

Wenn Sie mehrere Richtlinien verwenden, können Sie Richtlinien, deren Einstellungen Konflikte verursachen, Prioritäten zuweisen. Weitere Informationen finden Sie unter Priorisieren, Modellieren, Vergleichen und Problembehandlung für Richtlinien.

### Arbeitsablauf bei Citrix Richtlinien

Der Prozess für das Konfigurieren von Richtlinien ist:

1. Erstellen Sie die Richtlinie.
2. Konfigurieren Sie Richtlinieneinstellungen.
3. Weisen Sie die Richtlinie Benutzer- und Maschinenobjekten zu.
4. Weisen Sie der Richtlinie eine Priorität zu.
5. Prüfen Sie die effektive Richtlinie durch Ausführen des Citrix Gruppenrichtlinien-Modellierungsassistenten.

> **Hinweis:**
>
> Sie öffnen den Citrix Gruppenrichtlinien-Modellierungsassistenten, indem Sie zu der Registerkarte **Richtlinien > Modellierung** gehen und im Bereich **Aktionen** auf **Modellierungsassistenten starten** klicken. Die Registerkarte **Modellierung** ist in Web Studio verfügbar, wenn es auf Wunsch des Kunden in Citrix Cloud gehostet wird.

### Navigieren durch die Citrix Richtlinien und Einstellungen

Richtlinieneinstellungen sind je nach Funktionalität bzw. Feature, für die bzw. das sie gelten, in Kategorien eingeteilt. Beispielsweise umfasst der Bereich Profilverwaltung Richtlinieneinstellungen für die Profilverwaltung.

- Computereinstellungen (Richtlinieneinstellungen für Maschinen) definieren das Verhalten von virtuellen Desktops und werden beim Start eines virtuellen Desktops angewendet. Diese Einstellungen werden auch angewendet, wenn keine aktiven Benutzersitzungen auf dem virtuellen Desktop durchgeführt werden.
- Benutzereinstellungen definieren die Benutzererfahrung. Benutzereinstellungen werden angewendet, wenn ein Benutzer eine Verbindung herstellt oder wiederherstellt.

Sie greifen auf Richtlinien, Einstellungen oder Vorlagen zu, indem Sie im Navigationsbereich von Web Studio **Richtlinien** auswählen.

- Die Registerkarte **Richtlinien** listet alle Richtlinien auf. Bei Auswahl einer Richtlinie werden unten folgende Registerkarten angezeigt:
  - Übersicht –Name, Priorität, Status (aktiviert/deaktiviert) und Beschreibung
  - Einstellungen –Liste aller konfigurierten Einstellungen
  - Zugewiesen zu –Anzeige der Bereitstellungsgruppe. Sie können diese Einstellungen bearbeiten oder entfernen. Die Richtlinie wird angewendet basierend auf der Mitgliedschaft des Desktops, auf dem die Sitzung ausgeführt wird, in einer Bereitstellungsgruppe. Weitere Informationen finden Sie unter Erstellen von Richtlinien.

- Auf der Registerkarte **Vorlagen** sehen Sie von Citrix bereitgestellte Vorlagen und benutzerdefinierte Vorlagen, die Sie erstellt haben. Bei Auswahl einer Vorlage werden unten folgende Registerkarten angezeigt:
  - Beschreibung (wofür Sie die Vorlage verwenden können)
  - Einstellungen (Liste der konfigurierten Einstellungen). Weitere Informationen finden Sie unter Richtlinienvorlagen.
  - Mit der Registerkarte **Vergleich** können Sie die Einstellungen einer Richtlinie oder Vorlage mit den Einstellungen in anderen Richtlinien oder Vorlagen vergleichen. Sie können beispielsweise Einstellungswerte prüfen, um sicherzustellen, dass optimale Verfahren eingehalten werden. Weitere Informationen finden Sie unter Priorisieren, Modellieren, Vergleichen und Problembehandlung für Richtlinien.
  - Auf der Registerkarte **Modellierung** können Sie Verbindungsszenarios mit Citrix Richtlinien simulieren. Weitere Informationen finden Sie unter Priorisieren, Modellieren, Vergleichen und Problembehandlung für Richtlinien.

  Suchen nach einer Einstellung in einer Richtlinie oder Vorlage

  1. Wählen Sie die Richtlinie oder Vorlage aus.
  2. Wählen Sie die Registerkarte **Richtlinie bearbeiten** oder **Vorlage bearbeiten**.
  3. Geben Sie auf der Seite **Einstellungen auswählen** den Namen der Einstellung ein.

  Sie können Ihre Suche verfeinern, indem Sie Folgendes auswählen:

  - Eine Kategorie (z. B. Bandbreite)
  - Das Kontrollkästchen **Nur ausgewählte anzeigen**
  - Sie suchen nur nach Einstellungen, die der ausgewählten Richtlinie hinzugefügt wurden.

- Suchen nach einer Einstellung in einer Richtlinie:

  1. Markieren Sie die Richtlinie.
  2. Geben Sie auf der Registerkarte **Einstellungen** den Namen der Einstellung ein.

Eine Richtlinie ist nach ihrer Erstellung unabhängig von der verwendeten Vorlage. Sie können in das Feld **Beschreibung** eingeben, auf welcher Vorlage die neue Richtlinie basiert.

## Richtlinienvorlagen

November 16, 2022

Vorlagen ermöglichen das Erstellen von Richtlinien von einem vordefinierten Ausgangspunkt aus. Integrierte Citrix Vorlagen sind für bestimmte Umgebungen oder Netzwerkbedingungen optimiert und können für Folgendes verwendet werden:

- Als Ausgangspunkt für das Erstellen Ihrer eigenen Richtlinien und Vorlagen, die Sie für verschiedene Sites freigeben können.
- Als Referenz zum leichteren Vergleich von Bereitstellungen, da Sie sich auf Ergebnisse beziehen können, zum Beispiel "…wenn Sie die Citrix Vorlage x oder y verwenden …".
- Als Methode für das Übermitteln von Richtlinien an Citrix Support oder vertrauenswürdige Dritte. Sie können Vorlagen importieren oder exportieren.

### Integrierte Citrix Vorlagen

Die folgenden Richtlinienvorlagen sind verfügbar:

- **Besonders gute High Definition-Benutzererfahrung**: Diese Vorlage erzwingt Standardeinstellungen, die die Benutzererfahrung optimieren. Verwenden Sie diese Vorlage in Szenarios, in denen mehrere Richtlinien in der Reihenfolge der Priorität verarbeitet werden.
- **Hohe Serverskalierbarkeit**: Mit dieser Vorlage können Sie Serverressourcen sparen, da Benutzererfahrung und Serverskalierbarkeit ausbalanciert werden. Die Vorlage ermöglicht eine gute Benutzererfahrung und erhöht gleichzeitig die Anzahl an Benutzern, die auf einem einzelnen Server gehostet werden können. Diese Vorlage verwendet keinen Videocodec zum Komprimieren von Grafiken und verhindert das serverseitige Multimediarendering.

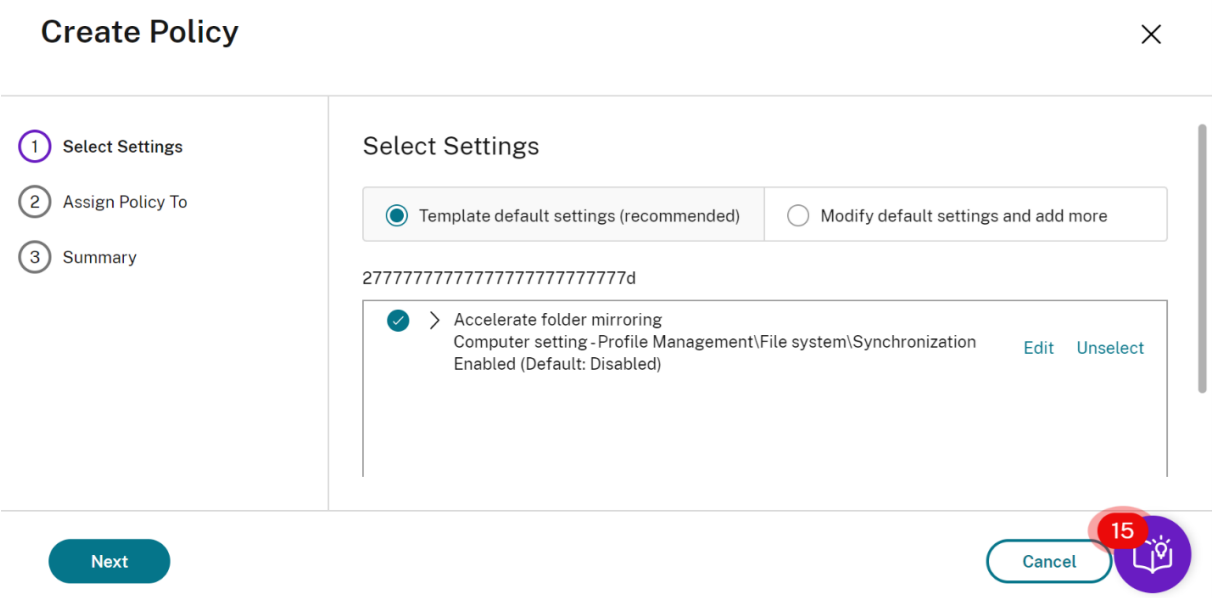
- **Hohe Serverskalierbarkeit –Legacy-OS**: Diese Vorlage für hohe Serverskalierbarkeit gilt nur für VDAs, die unter Windows Server 2008 R2, Windows 7 und älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Für NetScaler SD-WAN optimiert**: Verwenden Sie diese Vorlage für Benutzer, die in Geschäftsstellen arbeiten, in denen die Bereitstellung von Citrix Virtual Desktops durch NetScaler SD-WAN optimiert wird. (NetScaler SD-WAN ist der neue Name für CloudBridge.)
- **Für WAN optimiert**: Diese Vorlage eignet sich für aufgabenorientierte Mitarbeiter, die in Zweigstellen mit gemeinsam genutztem WAN oder an Remotestandorten mit geringer Bandbreite arbeiten. Die Mitarbeiter greifen auf Anwendungen mit grafisch einfachen Benutzeroberflächen und wenig Multimediainhalten zu. Mit dieser Vorlage werden für optimierte Bandbreiteneffizienz Kompromisse bei der Qualität der Videowiedergabe und der Serverskalierbarkeit gemacht.
- **Für WAN optimiert –Legacy-OS**: Die Vorlage gilt nur für VDAs, die auf Server 2008 R2, Windows 7 oder älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Sicherheit und Steuerung**: Verwenden Sie diese Vorlage in Umgebungen mit niedriger Fehlertoleranz, um die in Citrix DaaS standardmäßig aktivierten Features zu minimieren. Diese Vorlage enthält Einstellungen, die den Zugriff auf Folgendes deaktivieren:

  - Drucken
  - Zwischenablage
  - Peripheriegeräte
  - Laufwerkzuordnung
  - Portumleitung
  - Flash-Beschleunigung auf Benutzergeräten

  Bei Anwendung dieser Vorlage wird möglicherweise mehr Bandbreite genutzt und die Benutzerdichte pro Server verringert.

Wir empfehlen zwar, die integrierten Citrix Vorlagen mit den Standardeinstellungen zu verwenden, für einige Einstellungen gibt es jedoch keinen empfohlenen Wert. Ein Beispiel ist die Einstellung **Bandbreitenlimit für Sitzung insgesamt** in der Vorlage "Für WAN optimiert". In diesem Fall wird die Einstellung durch die Vorlage verfügbar gemacht, damit der Administrator die Wirkung dieser Einstellung in diesem Szenario versteht.



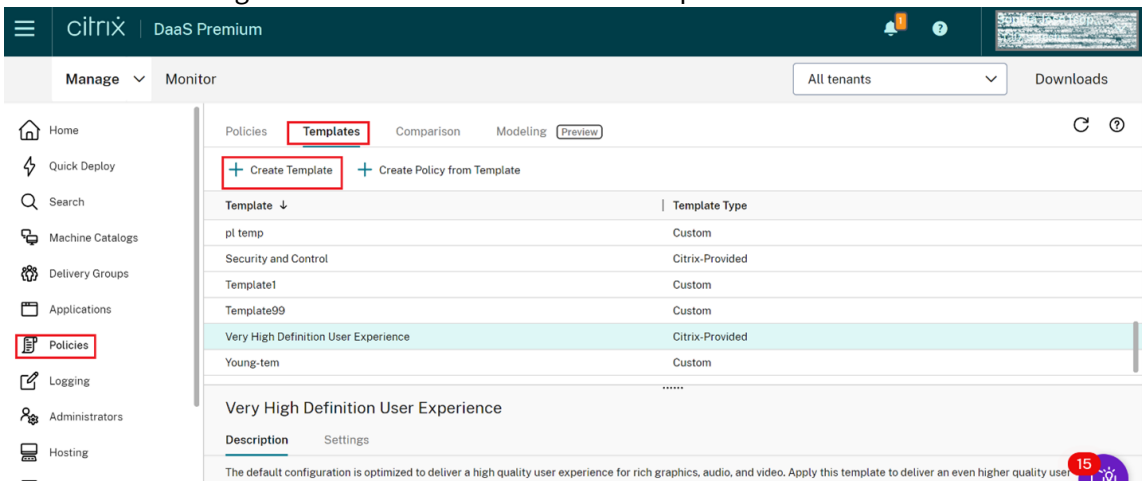

Angenommen, Sie nutzen eine Bereitstellung (Richtlinienverwaltung und VDAs), die älter ist als XenApp und XenDesktop 7.6 FP3. Außerdem benötigen Sie die Vorlagen "Hohe Serverskalierbarkeit" und "Für WAN optimiert". Verwenden Sie in diesem Fall die Legacy-OS-Versionen dieser Vorlagen, wenn sie anzuwenden sind.

> **Hinweis:**
>
> Integrierte Vorlagen werden von Citrix erstellt und aktualisiert. Diese Vorlagen dürfen nicht geändert oder gelöscht werden.

## Vorlagen mit Web Studio erstellen und verwalten

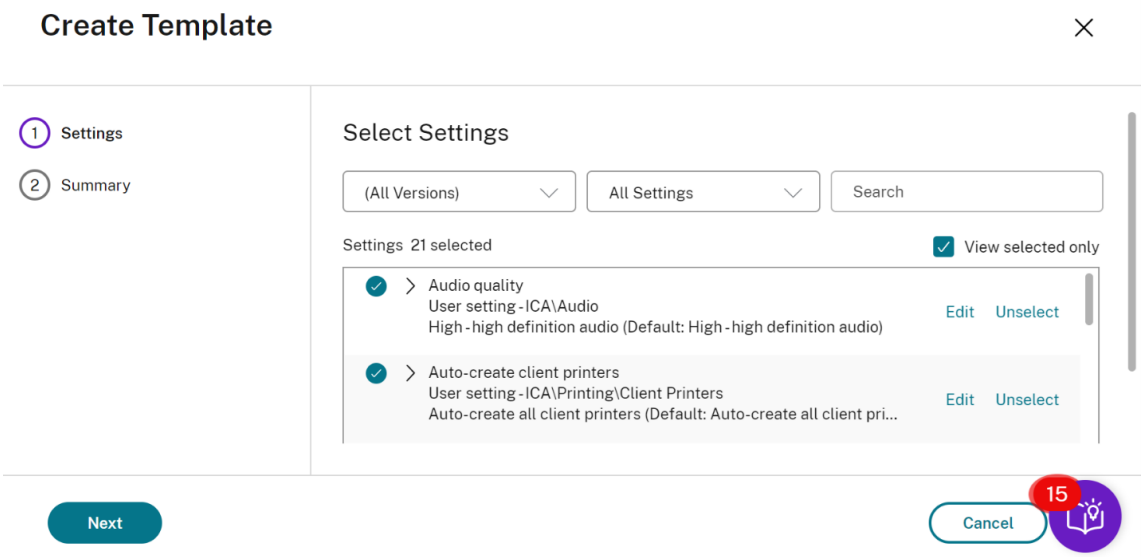
Erstellen einer Vorlage basierend auf einer Vorlage:

1. Wählen Sie im Navigationsbereich von Web Studio die Option **Richtlinien**.



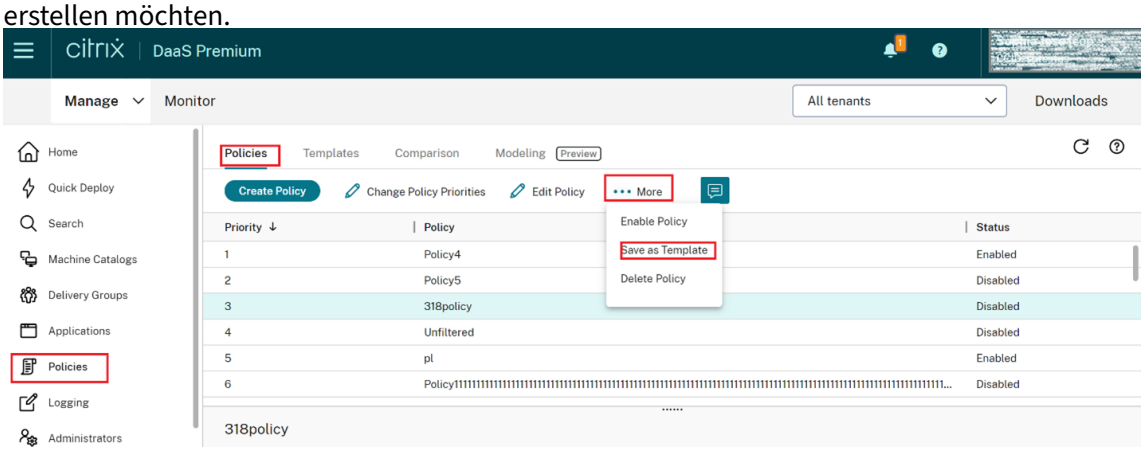
2. Wählen Sie die Registerkarte **Vorlagen** und dann die Vorlage, mit der Sie die Vorlage erstellen möchten.
3. Wählen Sie die Registerkarte **Vorlage erstellen**. Die Seite **Einstellungen auswählen** wird angezeigt.




4. Wählen und konfigurieren Sie die Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten.
5. Klicken Sie auf **Weiter**. Das Fenster **Zusammenfassung** wird angezeigt.
6. Geben Sie einen Namen für die Vorlage ein.
7. Klicken Sie auf **Fertig stellen**. Die neue Vorlage wird auf der Registerkarte “Vorlagen”angezeigt.

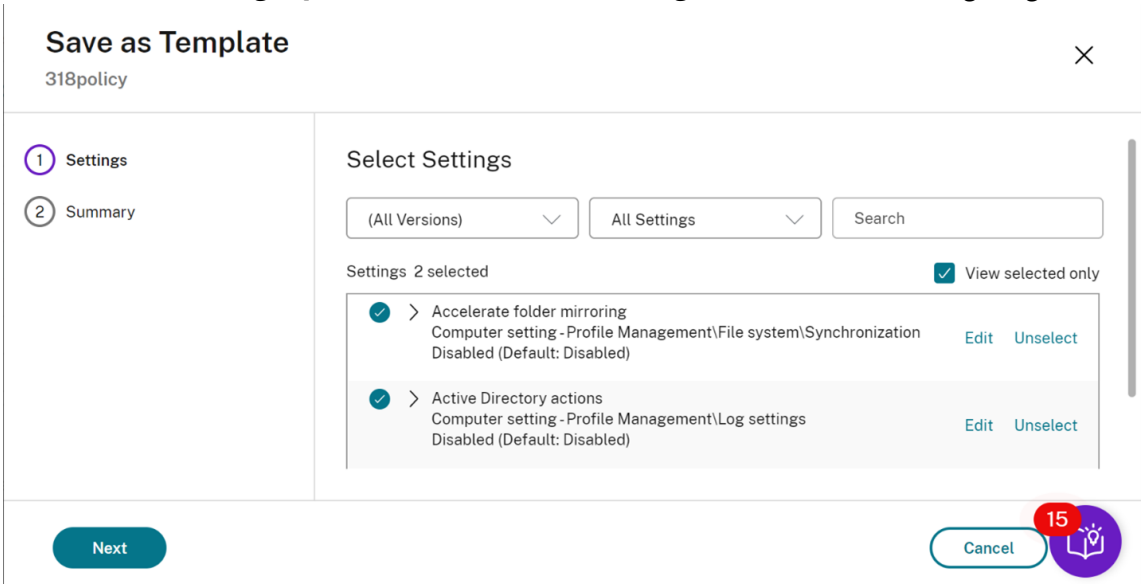
**Erstellen einer Vorlage basierend auf einer Richtlinie**:

1. Wählen Sie im Navigationsbereich von Web Studio die Option **Richtlinien**.
2. Wählen Sie die Registerkarte **Richtlinien** und dann die Richtlinie, mit der Sie die Vorlage erstellen möchten.

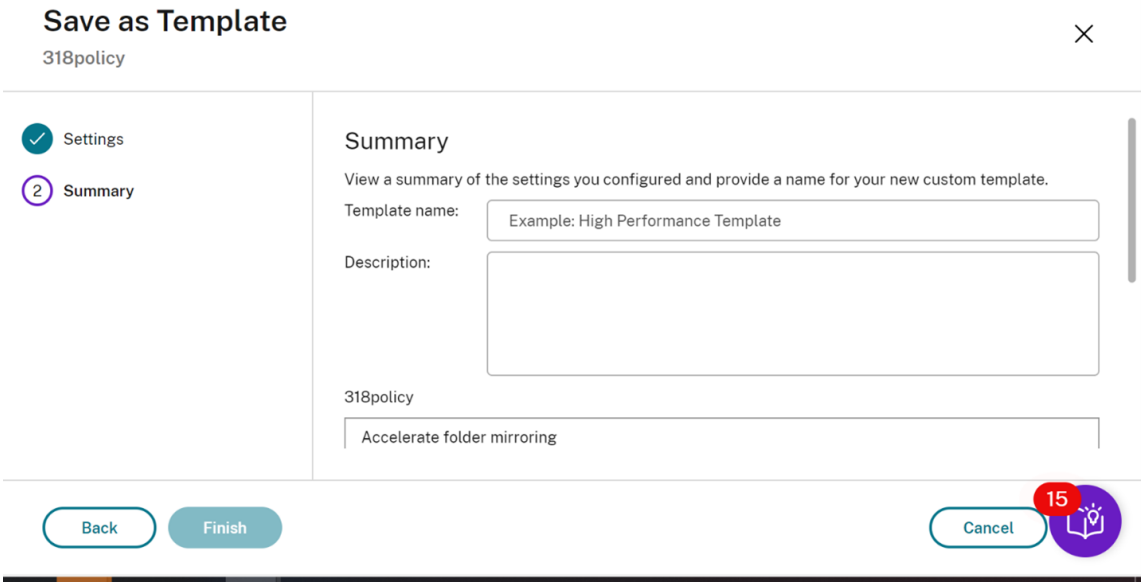


3. Klicken Sie auf die Registerkarte **Mehr**.
4. Wählen Sie **Als Vorlage speichern**. Die Seite **Einstellungen auswählen** wird angezeigt.




5. Wählen und konfigurieren Sie die neuen Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten.
6. Klicken Sie auf **Weiter**. Das Fenster **Zusammenfassung** wird angezeigt.




7. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein und klicken Sie auf **Fertig stellen**.

# Richtlinien erstllen

November 6, 2023

Legen Sie vor dem Erstellen einer Richtlinie fest, für welche Benutzergruppen oder Geräte sie gelten soll. Sie können Richtlinien basierend auf Aufgabenbereich, Verbindungstyp, Benutzergerät oder geografischer Position erstellen.

Wenn Sie bereits eine Richtlinie für eine Gruppe erstellt haben, sollten Sie möglichst diese Richtlinie bearbeiten, statt eine andere Richtlinie zu erstellen. Nach dem Bearbeiten der Richtlinie konfigurieren Sie die entsprechenden Einstellungen. Vermeiden Sie es, eine Richtlinie zu erstellen, deren einziger Zweck ist, eine bestimmte Einstellung zu aktivieren oder bestimmte Benutzer von der Richtlinie auszunehmen.

Sie können eine Richtlinie basierend auf einer Richtlinienvorlage erstellen und die Einstellungen nach Bedarf anpassen. Sie können die Richtlinie aber auch ohne Vorlage erstellen und alle benötigten Einstellungen hinzufügen.

In Citrix Studio werden neu erstellte Richtlinien auf "Deaktiviert"festgelegt, sofern das Kontrollkästchen **Richtlinie aktivieren** nicht explizit aktiviert wird.

Beim Erstellen der Richtlinie und Konfigurieren der Einstellungen bietet das System eine Option zum Anzeigen des Einstellungstyps. Sie können den folgenden Einstellungstyp anzeigen:

- Alle Einstellungen: Alle Einstellungen für alle VDA-Versionen anzeigen
- Nur aktuelle Einstellungen: Nur Einstellungen für aktuelle VDA-Versionen anzeigen
- Nur Legacy-Einstellungen: Nur Einstellungen für veraltete VDA-Versionen anzeigen

Einstellungen beim Konfigurieren der Einstellungen anzeigen:

1. Melden Sie sich bei DaaS Premium an.
2. Klicken Sie in der linken Navigationsleiste auf **Richtlinien**.
3. Klicken Sie auf der Registerkarte **Richtlinien** auf **Richtlinie erstellen**.
4. Klicken Sie in der Tabelle **Einstellungen auswählen** auf das Dropdownmenü neben **Einstellungen**.
5. Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü aus:

    - Alle Einstellungen: Alle Einstellungen für alle VDA-Versionen anzeigen
    - Nur aktuelle Einstellungen: Nur Einstellungen für aktuelle VDA-Versionen anzeigen
    - Nur Legacy-Einstellungen: Nur Einstellungen für veraltete VDA-Versionen anzeigen

6. In der Tabelle "Einstellungen"sind die Einstellungen aufgeführt, die gemäß dem vorherigen Schritt verfügbar sind.

### Richtlinieneinstellungen

Richtlinieneinstellungen können deaktiviert, aktiviert oder nicht konfiguriert sein. Standardmäßig sind Richtlinieneinstellungen nicht konfiguriert, d. h. sie wurden keiner Richtlinie hinzugefügt. Einstellungen werden nur angewendet, wenn sie einer Richtlinie hinzugefügt wurden.

Wenn beim Konfigurieren der Einstellungen zum Erstellen oder Bearbeiten einer Richtlinie alle Bereitstellungsgruppen deaktiviert sind, wird durch ein **Warnsymbol** angezeigt, dass kein Element im Filter aktiviert ist. Wenn mindestens eine Bereitstellungsgruppe aktiviert ist, wird kein Warnsymbol angezeigt.

Warnung beim Erstellen einer Richtlinie anzeigen:

1. Melden Sie sich bei DaaS Premium an.
2. Klicken Sie in der linken Navigationsleiste auf **Richtlinien**.
3. Klicken Sie auf der Registerkarte **Richtlinien** auf **Richtlinie erstellen**.
4. Wählen Sie in der Tabelle **Einstellungen auswählen** eine beliebige Einstellung aus und klicken Sie auf **Weiter**.
5. Wählen Sie in der Tabelle **Richtlinie zuweisen zu** einen Filter aus der Dropdownliste aus.
6. Deaktivieren Sie das Kontrollkästchen **Aktivieren** und klicken Sie auf **Speichern**.

> **Hinweis:**
>
> Nicht alle Filter unterstützen das Deaktivieren des Kontrollkästchens **Aktivieren**.
> In der Tabelle **Filter** wird eine Warnung für den Filter angezeigt.

Warnung beim Bearbeiten einer Richtlinie anzeigen:

1. Melden Sie sich bei DaaS Premium an.
2. Klicken Sie in der linken Navigationsleiste auf **Richtlinien**.
3. Wählen Sie auf der Registerkarte **Richtlinien** eine der aufgelisteten Richtlinien aus und klicken Sie auf **Richtlinie bearbeiten**.
4. Klicken Sie auf der Seite **Richtlinie bearbeiten** im linken Navigationsbereich auf **Richtlinie zuweisen zu**.
5. Wählen Sie in der Tabelle **Filter** den gewünschten Filter aus, oder klicken Sie auf **Bearbeiten**:
   - Wenn ein Filter keine Schaltfläche **Bearbeiten** besitzt, wählen Sie den Filter aus.
   - Wenn für einen Filter eine Schaltfläche **Bearbeiten** vorhanden ist, klicken Sie darauf.
6. Deaktivieren Sie die Option **Aktivieren** und klicken Sie auf **Speichern**.

> **Hinweis:**
>
> Nicht alle Filter unterstützen das Deaktivieren des Kontrollkästchens **Aktivieren**.
> In der Tabelle **Filter** wird eine Warnung für den Filter angezeigt.

Manche Richtlinieneinstellungen können einen der folgenden Zustände haben:

```
- Allowed or Prohibited allows or prevents the action controlled by
  the setting. Sometimes users are allowed or prevented from managing
  the setting's action in a session. For example, if the menu
  animation setting is set to Allowed, users can control menu
  animations in their client environment
- Enabled or Disabled turns the setting on or off. If you disable a
  setting, it is not enabled in lower-ranked policies.
```

Manche Einstellungen steuern außerdem die Wirksamkeit von abhängigen Einstellungen. Die Einstellung Clientlaufwerkumleitung steuert beispielsweise, ob Benutzer auf die Laufwerke ihres Geräts zugreifen können. Sowohl diese Einstellung als auch die Einstellung **Clientnetzlaufwerke** muss der Richtlinie hinzugefügt werden, damit Benutzer auf Netzlaufwerke zugreifen können. Wenn die Einstellung **Clientlaufwerkumleitung** deaktiviert ist, können Benutzer nicht auf ihre Netzlaufwerke zugreifen, selbst wenn die Einstellung **Clientnetzlaufwerke** aktiviert ist.

In der Regel treten Änderungen an Richtlinieneinstellungen, die sich auf Maschinen auswirken, in Kraft, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet. Änderungen an Richtlinieneinstellungen, die Auswirkungen auf Benutzer haben, treten in Kraft, wenn sich die Benutzer das nächste Mal anmelden.

Für manche Richtlinieneinstellungen können Sie einen Wert eingeben oder auswählen, wenn Sie die Einstellung der Richtlinie hinzufügen. Sie können die Konfiguration der Einstellung einschränken, indem Sie "Standardwert verwenden"auswählen. Dadurch deaktivieren Sie die Konfiguration der Einstellung, und es darf nur der Standardwert der Einstellung beim Anwenden der Richtlinie verwendet werden. Diese Auswahl ist unabhängig von dem Wert, der vor dem Aktivieren von "Standardwert verwenden"eingegeben wurde.

Bewährte Methoden:

- Weisen Sie Richtlinien Gruppen statt einzelnen Benutzern zu. Wenn Sie Richtlinien Gruppen zuweisen, werden Zuweisungen automatisch aktualisiert, wenn Sie Benutzer Gruppen hinzufügen oder sie daraus entfernen.
- Deaktivieren Sie Richtlinien, die nicht verwendet werden. Richtlinien, denen keine Einstellungen hinzugefügt wurden, verursachen unnötigen Verarbeitungsaufwand.

### Richtlinienzuweisungen

Wenn Sie eine Richtlinie erstellen, weisen Sie sie Benutzern und Maschinenobjekten zu. Die Richtlinie wird gemäß bestimmter Kriterien oder Regeln auf Verbindungen angewendet. Basierend auf einer Kombination von Kriterien können Sie in der Regel beliebig viele Zuweisungen für eine Richtlinie hinzufügen. Wenn keine Zuweisung angegeben wurde, gilt die Richtlinie für alle Verbindungen.

Wenn Sie keine Zuweisungen angeben oder Zuweisungen angeben, diese aber deaktivieren, wird die Richtlinie auf **alle** Verbindungen angewendet.

> **Hinweis:**
>
> Richtlinienzuweisungen werden auch als Richtlinienfilter bezeichnet. Weitere Informationen finden Sie in den folgenden Artikeln:
>
> - Create, modify, or delete a filter for a policy
> - How do filters get applied?

In der folgenden Tabelle werden verfügbare Zuweisungen aufgelistet:

| Name | Anwendung der Richtlinie basierend auf |
|---|---|
| Zugriffssteuerung | Zugriffssteuerungsbedingungen, unter denen Clients eine Verbindung herstellen<br>*Verbindungstyp*: ob die Richtlinie auf Verbindungen anzuwenden ist, die mit oder ohne NetScaler Gateway hergestellt wurden.<br>*NetScaler Gateway-Farmname*: Name des virtuellen NetScaler Gateway-Servers.<br>*Zugriffsbedingung*: Name der zu verwendenden Endpunktanalyserichtlinie oder Sitzungsrichtlinie. |
| Citrix SD-WAN | Gibt an, ob eine Benutzersitzung über Citrix SD-WAN gestartet wird. **Hinweis:** Sie können einer Richtlinie nur eine einzige Citrix SD-WAN-Zuweisung hinzufügen. |
| Client-IP-Adresse | IP-Adresse des Benutzergeräts, das für die Verbindung mit der Sitzung verwendet wird.<br>IPv4-Beispiele: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6-Beispiele: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |

| Name | Anwendung der Richtlinie basierend auf |
| --- | --- |
| Clientname | Name des Benutzergeräts Genaue Übereinstimmung: ClientABCName. Verwenden von Platzhalter: Client*Name. |
| Bereitstellungsgruppe | Bereitstellungsgruppen-Mitgliedschaft |
| Bereitstellungsgruppentyp | Desktop- oder Anwendungstyp: privater Desktop, freigegebener Desktop, private Anwendung oder freigegebene Anwendung |
| Organisationseinheit | Organisationseinheit |
| Tag | Tags **Hinweis:** Wenden Sie diese Richtlinie auf alle getaggten Maschinen an. Anwendungstags sind nicht enthalten. |
| Benutzer oder Gruppe | Benutzer- oder Gruppenname |

Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet. Jede deaktivierte Richtlinieneinstellung hat Vorrang vor einer aktivierten Richtlinieneinstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert.

> **Wichtig:**
>
> Bei der Konfiguration von Active Directory- und Citrix Richtlinien mit der Gruppenrichtlinien-Verwaltungskonsole werden Zuweisungen und Einstellungen möglicherweise nicht wie erwartet angewendet. Weitere Informationen finden Sie unter CTX127461.

Eine Richtlinie mit dem Namen "Ungefiltert"ist standardmäßig verfügbar.

- Wenn Sie Web Studio zur Verwaltung von Citrix Richtlinien verwenden, werden die Einstellungen, die Sie der Richtlinie "Ungefiltert"hinzufügen, auf alle Server, Desktops und Verbindungen einer Site angewendet.
- Die Sites und Verbindungen müssen zu dem Geltungsbereich der Gruppenrichtlinienobjekte gehören, die die Richtlinie enthält. Beispiel: Die Organisationseinheit (OU) "Verkauf"enthält ein Gruppenrichtlinienobjekt "Verkauf-USA", das alle Mitarbeiter des US-Verkaufsteams einschließt. Das Gruppenrichtlinienobjekt "Verkauf-USA"ist mit einer Richtlinie "Ungefiltert" konfiguriert, die mehrere Benutzerrichtlinieneinstellungen enthält. Wenn der US-Verkaufsleiter sich an der Site anmeldet, werden die Einstellungen der Richtlinie "Ungefiltert"automatisch auf die Sitzung angewendet. Diese Konfiguration basiert darauf, dass der Benutzer Mitglied des Gruppenrichtlinienobjekts "Verkauf-USA"ist.

Der Modus einer Zuweisung entscheidet, ob die Richtlinie nur auf Verbindungen angewendet wird, die alle Zuweisungskriterien erfüllen. Wenn der Modus Zulassen (Standardwert) ist, wird die Richtlinie nur auf Verbindungen angewendet, die die Zuweisungskriterien erfüllen. Wenn der Modus Verweigern ist, wird die Richtlinie angewendet, wenn eine Verbindung die Zuweisungskriterien nicht erfüllt. Das folgende Beispiel zeigt, wie Zuweisungsmodi sich auf Citrix Richtlinien auswirken, wenn mehrere Zuweisungen vorhanden sind.

- **Beispiel: Zuweisungen des gleichen Typs mit unterschiedlichen Modi:** In Richtlinien mit zwei Zuweisungen des gleichen Typs, eine mit der Einstellung "Zulassen"und die andere mit der Einstellung "Verweigern", hat die Zuweisung mit der Einstellung "Verweigern"Vorrang, wenn die Verbindung die Kriterien beider Zuweisungen erfüllt. Beispiel:

  Richtlinie 1 enthält die folgenden Zuweisungen:

  - Zuweisung A bestimmt die Verkaufsgruppe. Der Modus ist auf Zulassen eingestellt.
  - Zuweisung B bestimmt das Konto des Verkaufsleiters. Der Modus ist auf Verweigern eingestellt.

  Da der Modus für Zuweisung B "Verweigern"ist, wird die Richtlinie nicht angewendet, wenn der Verkaufsleiter sich bei der Site anmeldet, obwohl er Mitglied der Verkaufsgruppe ist.

- **Beispiel: Zuweisungen unterschiedlichen Typs mit gleichen Modi:** In Richtlinien mit zwei oder mehr Zuweisungen unterschiedlichen Typs, für die "Zulassen"eingestellt ist, muss die Verbindung die Kriterien von mindestens einer Zuweisung jedes Typs erfüllen, damit die Richtlinie angewendet wird. Beispiel:

  Richtlinie 2 enthält die folgenden Zuweisungen:

  - Zuweisung C ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt. Der Modus ist auf Zulassen eingestellt.
  - Zuweisung D ist eine Client-IP-Adressenzuweisung, die 10.8.169.* festlegt (das Unternehmensnetzwerk). Der Modus ist auf Zulassen eingestellt.

  Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie angewendet, weil die Verbindung die Kriterien beider Zuweisungen erfüllt.

  Richtlinie 3 enthält die folgenden Zuweisungen:

  - Zuweisung E ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt. Der Modus ist auf Zulassen eingestellt.
  - Zuweisung F ist eine Zugriffssteuerungszuweisung, die NetScaler Gateway-Verbindungsbedingungen angibt. Der Modus ist auf Zulassen eingestellt.

  Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie nicht angewendet, weil die Verbindung nicht die Kriterien von Zuweisung F erfüllt.

# Richtliniensätze (Preview)

May 17, 2024

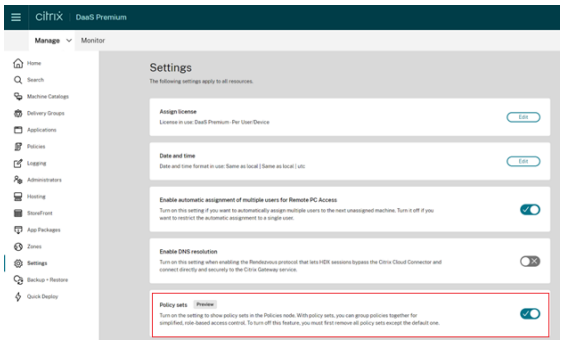
Richtliniensätze sind Objekte in Citrix DaaS, die Richtlinien aggregieren, um einen vereinfachten, rollenbasierten Zugriff und eine einfache Verwaltung zu ermöglichen. Sie können Richtliniensätze anhand der logischen Unterteilungen Ihres Administratorteams und Unternehmens erstellen. Sie können beispielsweise einen Richtliniensatz für jede geografische Region, Geschäftseinheit oder für einen bestimmten Anwendungsfall erstellen. Nach der Erstellung werden Richtliniensätzen Bereiche und Bereitstellungsgruppen zugewiesen, sodass nur autorisierte Administratoren Richtlinien für ihre jeweiligen Benutzer und Maschinen verwalten können.

## Vorteile

- Rollenbasierte Zugriffssteuerung für verteilte Administratorenteams
- Vereinfachte Fusionen, Übernahmen und Konsolidierungen
- Kleinerer Fehlerbereich
- Mehrmandanten-Unterstützung für Richtlinien

## Richtliniensätze aktivieren

Gehen Sie auf der Registerkarte **Verwalten** in Citrix DaaS zu **Einstellungen** und aktivieren Sie die Einstellung **Richtliniensätze**.




> **Hinweis:**
>
> Sie müssen Richtliniensätze aktivieren, bevor Sie einen Richtliniensatz erstellen.

## Featurevergleich

| Vor der Anwendung von Richtliniensätzen | Nach der Anwendung von Richtliniensätzen |
|---|---|
| Richtlinien, Einstellungen, Filter und Richtlinienprioritäten für die gesamte Site werden an einer Stelle in Citrix Studio konfiguriert. | Richtlinien, Einstellungen, Filter und Richtlinienprioritäten werden für jeden Richtliniensatz separat konfiguriert. |
| Wenn Sie eine Richtlinie verwalten, müssen Sie jede Richtlinie verwalten. | Volladministratoren können die Verwaltung eines bestimmten Richtliniensatzes individuell an untergeordnete Administratoren delegieren. |
| Richtlinien in großen und dezentralen Umgebungen werden komplex und schwer zu verwalten. | Richtlinien in großen und dezentralen Umgebungen können einfach aufgeteilt und verwaltet werden. |

## Wie funktionieren Richtliniensätze?

### Allgemeiner Überblick

- Richtliniensätze werden Bereitstellungsgruppen zugewiesen.
- Richtliniensätze haben einen oder mehrere Bereiche.
- Bereitstellungsgruppen, denen kein Richtliniensatz zugewiesen ist, erhalten den Standardrichtliniensatz.
- Einer Bereitstellungsgruppe kann nur ein Richtliniensatz zugewiesen werden.
- Mehrere Bereitstellungsgruppen können denselben Richtliniensatz verwenden.
- Richtliniensätze sind zwar Bereitstellungsgruppen zugewiesen sind, die Richtlinien behalten jedoch ihre Filter bei

Weitere Informationen finden Sie unter Wie werden Filter angewendet? Die Art und Weise, wie Richtlinienzuweisungen oder Richtlinienfilter funktionieren, hat sich für Richtliniensätze nicht geändert. Das heißt, sie funktionieren genauso wie bei Richtlinien.

### Standardrichtliniensatz

- Wenn die Einstellung “Richtliniensatz”aktiviert wird, werden alle vorhandenen Richtlinien im Standardrichtliniensatz zusammengefasst.
- Jede Bereitstellungsgruppe erhält den Standardrichtliniensatz, es sei denn, die Administratoren erstellen einen Richtliniensatz und weisen ihn einer Bereitstellungsgruppe zu.
- Sobald einer Bereitstellungsgruppe ein bestimmter Richtliniensatz zugewiesen ist, erhält sie keine Richtlinien mehr aus dem Standardrichtliniensatz.

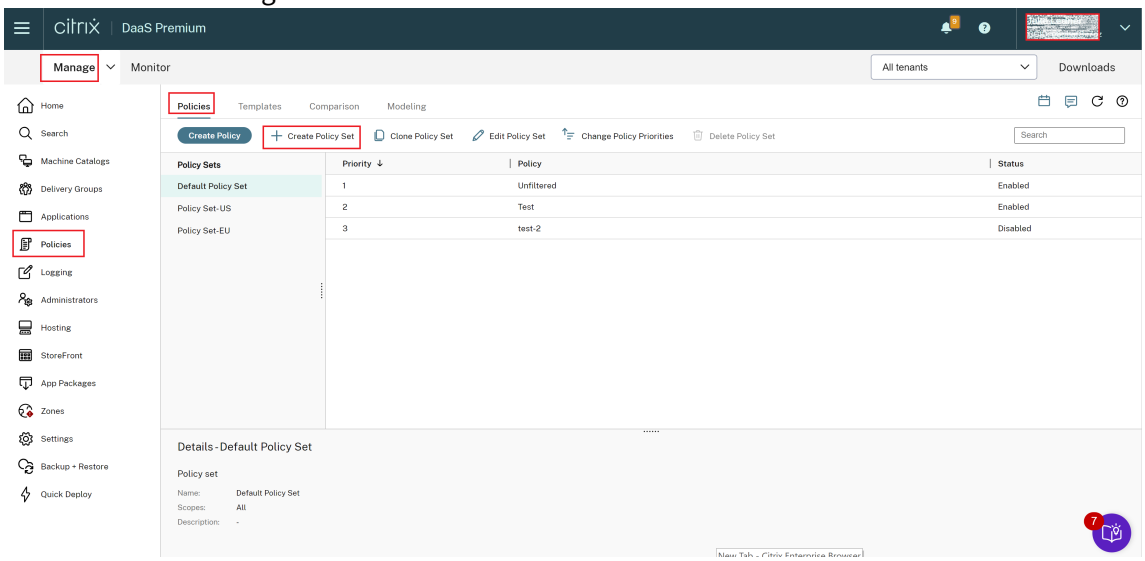
### Richtliniensatzerstellung

Richtliniensätze können auf zweierlei Art erstellt werden:

- Richtliniensatz erstellen: Diese Aktion erstellt einen leeren Richtliniensatz.
- Richtliniensatz klonen: Diese Aktion erstellt einen Richtliniensatz, der auf einem vorhandenen Richtliniensatz basiert.

### Richtliniensätze erstellen

1. Klicken Sie auf der Konfigurationsseite für Citrix DaaS auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Registerkarte **Richtlinien**.




3. Wählen Sie **Richtliniensatz erstellen**. Die Registerkarte **Einführung** wird angezeigt.
4. Klicken Sie auf **Weiter** oder auf die Registerkarte **Name und Beschreibung**.
5. Geben Sie den Namen und die Beschreibung für den Richtliniensatz ein.
6. Klicken Sie auf **Weiter** oder auf die Registerkarte **Zuweisungen**.
7. Wählen Sie eine oder mehrere Bereitstellungsgruppen aus, denen Sie den Richtliniensatz zuweisen möchten.
8. Klicken Sie auf **Weiter** oder auf die Registerkarte **Bereiche**.
9. Wählen Sie die Bereiche des Richtliniensatzes aus.
10. Klicken Sie auf **Erstellen**. Der Richtliniensatz wird mit der ausgewählten Zuweisung und dem ausgewählten Bereich erstellt.

### Richtliniensätze klonen

1. Klicken Sie auf der Konfigurationsseite für Citrix DaaS auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Registerkarte **Richtlinien**.
3. Wählen Sie **Richtliniensatz klonen**.

4. Ändern Sie den Namen des Richtliniensatzes.
5. Ändern oder erstellen Sie Zuweisungen für den Richtliniensatz und klicken Sie auf **Weiter**.
6. Wählen oder deaktivieren Sie die Richtlinien für den geklonten Richtliniensatz.
7. Ändern Sie den Bereich der Richtlinie.
8. Klicken Sie auf **Erstellen**. Der Richtliniensatz wird erstellt.

### Richtliniensätze bearbeiten

1. Klicken Sie auf der Konfigurationsseite für Citrix DaaS auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Registerkarte **Richtlinien**.
3. Wählen Sie **Richtliniensatz bearbeiten**.
4. Ändern Sie den Namen des Richtliniensatzes und klicken Sie auf **Weiter**.
5. Ändern oder erstellen Sie Zuweisungen für den Richtliniensatz und klicken Sie auf **Weiter**.
6. Ändern Sie den Bereich der Richtlinie.
7. Klicken Sie auf **Erstellen**.

### Richtliniensatzzuweisung

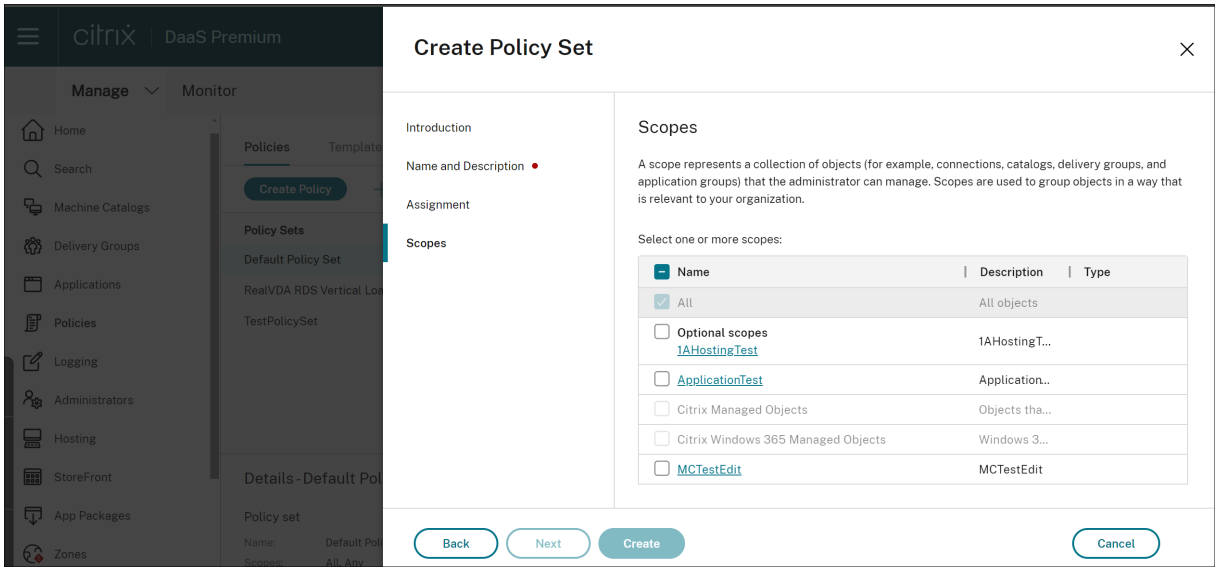
Richtliniensätze werden Bereitstellungsgruppen zugewiesen. Sie können Zuweisungen konfigurieren, wenn der Richtliniensatz erstellt oder bearbeitet wird. Sie können Zuweisungen auch beim Erstellen oder Bearbeiten von Bereitstellungsgruppen konfigurieren.

### Richtliniensatzbereiche

Administratoren können den Bereich eines Richtliniensatzes so definieren, dass nur autorisierte Administratoren ihn anzeigen oder bearbeiten können. Sie können Bereiche konfigurieren, wenn der Richtliniensatz erstellt oder bearbeitet wird.

Mit der Einführung von Richtliniensätzen können Sie Citrix Richtlinien auch mithilfe der API erstellen und verwalten. Weitere Informationen finden Sie unter So erstellen Sie einen Richtliniensatz in Citrix DaaS.




# Richtlinien prioritisieren, modellieren und vergleichen sowie Problembehandlung

June 5, 2023

Mit Richtlinien können Sie Ihre Umgebung an die Anforderungen von Benutzern anpassen, basierend auf Folgendem:

- Jobfunktionen
- Geografischen Standorten
- Verbindungstypen

Beispielsweise können Sie für Benutzergruppen, die regelmäßig mit vertraulichen Daten interagieren, Beschränkungen festlegen und so die Sicherheit steigern.

Sie können auch eine Richtlinie erstellen, die Benutzer daran hindert, vertrauliche Daten auf ihren lokalen Clientlaufwerken zu speichern. Sie können eine weitere Richtlinie für Benutzer in der Benutzergruppe erstellen, die Zugriff auf ihr lokales Laufwerk benötigen. Anschließend können Sie anhand einer Rangfolge definieren, welche der beiden Richtlinien Vorrang haben soll. Wenn Sie mehrere Richtlinien verwenden, müssen Sie Folgendes festlegen:

- Wie Sie die Richtlinienpriorität festlegen
- Wie Sie Ausnahmen erstellen
- Wie Sie die gültige Richtlinie bei einem Richtlinienkonflikt anzeigen

### Festlegen der Richtlinienpriorität

Durch Festlegen der Richtlinienpriorität definieren Sie, welche Richtlinie Vorrang hat, wenn es Konflikte gibt. Wenn ein Benutzer sich am System anmeldet, wird erfasst, welche Richtlinien den Zuweisungen für die Verbindung entsprechen. Die identifizierten Richtlinien und ihre zugehörigen Einstellungen werden in der Reihenfolge der Priorität sortiert. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet.

Sie können Prioritäten für Richtlinien festlegen, indem Sie ihnen in **Web Studio** unterschiedliche Prioritätsziffern zuweisen. Eine neue Richtlinie erhält standardmäßig die niedrigste Priorität. Falls Konflikte zwischen Richtlinieneinstellungen auftreten, setzt eine Richtlinie mit höherer Priorität eine Richtlinie mit niedrigerer Priorität außer Kraft. Eine Richtlinie mit der Prioritätsziffer 1 hat die höchste Priorität. Beim Zusammenführen von Richtlinieneinstellungen werden folgende Faktoren berücksichtigt:

- die Prioritäten der Richtlinien
- und die Bedingungen, die in den Filtern der Richtlinien angegeben sind

Gehen Sie wie folgt vor, um Richtlinien zu priorisieren:

1. Wählen Sie im linken Bereich die Option **Richtlinien**.
2. Wählen Sie auf der Registerkarte **Richtlinien** auf der Aktionsleiste **Richtlinienprioritäten ändern**. Die Seite **Richtlinienprioritäten ändern** wird angezeigt.
3. Ändern Sie in der Prioritätsliste die Priorität für eine Richtlinie wie folgt:
    - Ziehen Sie die Richtlinie an die gewünschte Position.
    - Um sie um eine Position nach oben oder unten zu verschieben, klicken Sie auf das Pfeilsymbol nach oben oder unten.
    - Um sie an den Anfang oder das Ende der Liste zu verschieben, klicken Sie auf das Pfeilsymbol “Oben”oder “Unten”.
    - Um die Prioritätsnummer zu ändern, klicken Sie auf das Symbol **Bearbeiten**, geben Sie eine Nummer ein und klicken Sie dann auf **Speichern**.
4. Klicken Sie auf **Speichern**.

### Ausnahmen

Wenn Sie Richtlinien erstellen und sie mithilfe von Filtern bestimmten Gruppen von Benutzern, Benutzergeräten oder Maschinen zuweisen, müssen Sie für einige Mitglieder einer Gruppe möglicherweise Ausnahmen zu einigen Einstellungen erstellen. Sie können Ausnahmen wie folgt erstellen:

- Erstellen Sie eine Richtlinie nur für bestimmte Gruppenmitglieder, für die Ausnahmen erforderlich sind, und weisen Sie der Richtlinie eine höhere Priorität zu als der Richtlinie für die gesamte Gruppe.
- Verwenden Sie den Modus *Verweigern* in einer Zuweisung, die Sie der Richtlinie hinzufügen.

Die Zuweisung im Modus *Verweigern* wendet eine Richtlinie nur auf Verbindungen an, die nicht den Zuweisungskriterien entsprechen. Beispielsweise kann eine Richtlinie folgende Zuweisungen enthalten:

- *Zuweisung A* ist eine Client-IP-Adressenzuweisung, die den Bereich `208.77.88.*` festlegt. Der Modus ist auf *Zulassen* eingestellt.
- *Zuweisung B* ist eine Benutzerzuweisung, die ein spezifisches Benutzerkonto angibt. Der Modus ist auf *Verweigern* eingestellt.

Die Richtlinie gilt für alle Benutzer, die sich mit IP-Adressen aus dem in *Zuweisung A* festgelegten Bereich bei der Site anmelden. Die Richtlinie gilt jedoch nicht für den Benutzer, der sich mit dem in *Zuweisung B* festgelegten Benutzerkonto anmeldet.

> **Hinweis:**
>
> Wenn Sie im Schritt **Richtlinie zuweisen** das Kontrollkästchen zum Aktivieren deaktivieren, ist die Zuweisung für die Richtlinie deaktiviert. Wenn die einzige Zuweisung für die Richtlinie deaktiviert ist, liegt keine Zuweisung vor und die Richtlinie gilt für alle Objekte der Site.

### Ermitteln der auf eine Verbindung angewendeten Richtlinien

Manchmal reagiert eine Verbindung nicht wie erwartet, weil mehrere Richtlinien gelten. Wenn eine Richtlinie mit einer höheren Priorität auf eine Verbindung angewendet wird, kann sie Einstellungen, die Sie in der ursprünglichen Richtlinie konfigurieren, außer Kraft setzen. Sie können den **Richtlinienergebnissatz** berechnen und so ermitteln, wie die Richtlinieneinstellungen am Ende für eine Verbindung zusammengeführt werden.

Sie berechnen den **Richtlinienergebnissatz** mit folgenden Methoden:

- Verwenden Sie den **Assistenten für die Citrix Gruppenrichtlinienmodellierung**, um ein Verbindungsszenario zu simulieren und festzustellen, wie Citrix Richtlinien angewendet werden. Sie können Bedingungen für ein Verbindungsszenario angeben. Beispiel:
  - Benutzer
  - Citrix Richtlinienzuweisungsbeweiswerte
- Verwenden Sie das Tool **Gruppenrichtlinienergebnisse**, um einen Bericht zu erstellen, der beschreibt, welche Citrix Richtlinien für einen bestimmten Benutzer oder Virtual Delivery Agent (VDA) angewendet werden.

Richtlinieneinstellungen für die Site, die mit **Web Studio** erstellt wurden, werden nicht in den **Richtlinienergebnissatz** einbezogen, wenn Sie den **Assistenten für die Citrix Gruppenrichtlinienmodellierung** über die **Gruppenrichtlinien-Verwaltungskonsole** ausführen. Um zu prüfen, ob Sie den umfassendsten **Richtlinienergebnissatz** erhalten, empfiehlt Citrix das Starten des **Assistenten für die Citrix Gruppenrichtlinienmodellierung** über **Web Studio**, es sei denn, Sie erstellen Richtlinien nur über die **Gruppenrichtlinien-Verwaltungskonsole**.

### Assistenten für die Richtlinienmodellierung verwenden

Mithilfe der Richtlinienmodellierung können Sie aktivierte Richtlinien mit Filtern für Planungs- und Testzwecke simulieren. Nur aktivierte Richtlinien mit Filtern werden modelliert. Deaktivierte Richtlinien werden niemals angewendet und aktivierte Richtlinien ohne Filter werden immer angewendet.

Führen Sie die folgenden Schritte aus, um den **Modellierungsassistenten** zu öffnen:

1. Wählen Sie in der vollständigen Konfiguration die Option **Richtlinien**.
2. Wählen Sie die Registerkarte **Modellierung**.
3. Wählen Sie **Richtlinienmodellierung** in der Aktionsleiste aus.
4. Lesen Sie die **Einführung** und klicken Sie auf **Weiter**.
5. Wählen Sie Benutzer oder Computer aus. Sie können nach Containern oder Benutzern oder Computern suchen. Klicken Sie auf **Weiter**.
6. Wählen Sie Ihre Filterbeweise aus. Sie können Ihre Simulation optional detaillierter gestalten, indem Sie zusätzliche Details wie **Bereitstellungsgruppe**, **Tags**, **Client-IP-Adresse** usw. eingeben. Klicken Sie auf **Weiter**.
7. Überprüfen Sie die Zusammenfassung Ihrer Auswahl und klicken Sie auf **Ausführen**.

Wenn Sie auf **Ausführen** klicken, erstellt der Assistent einen Bericht mit den Modellierungsergebnissen. Beim Anzeigen des Berichts haben Sie folgende Möglichkeiten:

- Wählen Sie im Dropdownmenü aus, ob Sie **Alle Einstellungen**, **Computereinstellungen**oder **Benutzereinstellungen** anzeigen möchten.
- Verwenden Sie die Suchleiste, um nach bestimmten Einstellungen zu suchen.
- Klicken Sie auf eine Einstellung, um deren Details anzuzeigen. Wenn beispielsweise nicht alle Benutzereinstellungen für eine Richtlinie angewendet wurden, wird im Bereich **Details** der Grund hierfür angezeigt.
- Klicken Sie auf **Exportieren**, um die Modellierungsergebnisse im JSON-Format, HTML-Format oder beidem zu exportieren.

Nach ausgeführter Richtlinienmodellierung stehen Ihnen weitere Optionen zur Verfügung. Sie haben folgende Möglichkeiten:

- **Modellierungsbericht anzeigen:** Dadurch wird der o. g. Modellierungsbericht geöffnet, sodass Sie ihn erneut ansehen oder exportieren können.

- **Richtlinienmodellierung erneut ausführen**: Hiermit können Sie die Richtlinienmodellierung mit den zuvor ausgewählten Kriterien erneut ausführen und neue Modellierungsergebnisse generieren. Dies ist nützlich, wenn sich Richtlinien geändert haben und Sie sehen möchten, wie sich diese Änderungen auf Ihr aktuelles Modell auswirken.
- **Modellierungsbericht löschen**: Dadurch wird der aktuelle Modellierungsbericht gelöscht.

### Vergleichen von Richtlinien und Vorlagen

Sie können die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Beispielsweise empfiehlt sich die Prüfung von Einstellungswerten, sodass optimale Verfahren eingehalten werden. Außerdem ist ggf. ein Vergleich von Einstellungen in einer Richtlinie oder Vorlage mit den Standardeinstellungen erforderlich.

1. Wählen Sie im Navigationsbereich von **Web Studio** die Option **Richtlinien**.
2. Klicken Sie auf die Registerkarte **Vergleich** und dann auf **Auswählen**.
3. Wählen Sie die Richtlinien oder Vorlagen aus, die Sie vergleichen möchten. Aktivieren Sie das Kontrollkästchen **Mit Standardeinstellungen vergleichen**, um Standardwerte im Vergleich einzuschließen.
4. Wenn Sie auf **Vergleichen** klicken, werden die konfigurierten Einstellungen in Spalten angezeigt.
5. Zum Anzeigen aller Einstellungen wählen Sie **Alle Einstellungen anzeigen**. Um zur Standardansicht zurückzukehren, wählen Sie **Gemeinsame Einstellungen anzeigen**.

### Problembehandlung bei Richtlinien

Für Benutzer, IP-Adressen und andere zugewiesene Objekte können mehrere Richtlinien gleichzeitig gelten. Dies kann zu Konflikten führen, wenn eine Richtlinie sich nicht wie erwartet verhält. Wenn Sie den **Assistenten für die Citrix Gruppenrichtlinienmodellierung** ausführen, sehen Sie möglicherweise, dass keine Richtlinien auf die Benutzerverbindungen angewendet werden. In diesem Fall gelten Richtlinieneinstellungen nicht für Benutzer, die sich unter Bedingungen, die den Richtlinienkriterien entsprechen, mit Anwendungen und Desktops verbinden. Diese Situation tritt in folgenden Fällen auf:

- Keine Richtlinie hat eine Zuweisung, die den Richtlinienkriterien entspricht.
- Richtlinien, die der Zuweisung entsprechen, haben keine konfigurierten Einstellungen.
- Richtlinien, die der Zuweisung entsprechen, sind deaktiviert.

Wenn Sie Richtlinieneinstellungen auf Verbindungen anwenden möchten, die bestimmten Kriterien entsprechen, stellen Sie Folgendes sicher:

- Die Richtlinien, die auf diese Verbindungen angewendet werden sollen, sind aktiviert.

- In den Richtlinien, die Sie anwenden möchten, sind die geeigneten Einstellungen konfiguriert.

> **Hinweis:**
>
> Bei Double-Hop-Szenarien stellen VDAs für Einzelsitzungs-OS im zweiten Hop eine Verbindung zu einem VDA für Multisitzungs-OS her. In diesem Fall wirken die Citrix Richtlinien auf dem VDA für Einzelsitzungs-OS so, als wäre dieser das Benutzergerät. Beispiel: Richtlinien legen fest, dass Bilder auf dem Benutzergerät zwischengespeichert werden. Die Bilder, die für den zweiten Hop in einem Double-Hop-Szenario zwischengespeichert werden, werden dann auf der Maschine mit dem VDA für Einzelsitzungs-OS zwischengespeichert.

### Director

Nicht-Administratoren können mit Director Richtlinien anzeigen, die für eine Benutzersitzung gelten.

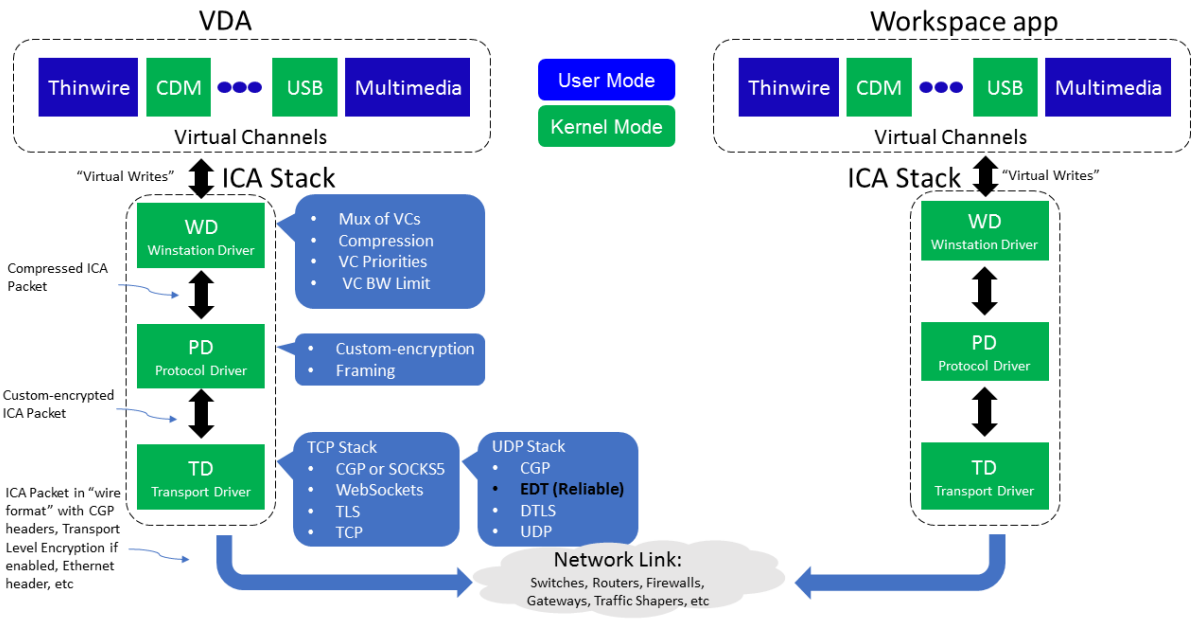
## Überblick über HDX

April 18, 2024

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Citrix HDX bietet Benutzern zentralisierter Anwendungen und Desktops auf jedem Gerät und in jedem Netzwerk vielfältige Technologien für ein High Definition-Erlebnis.



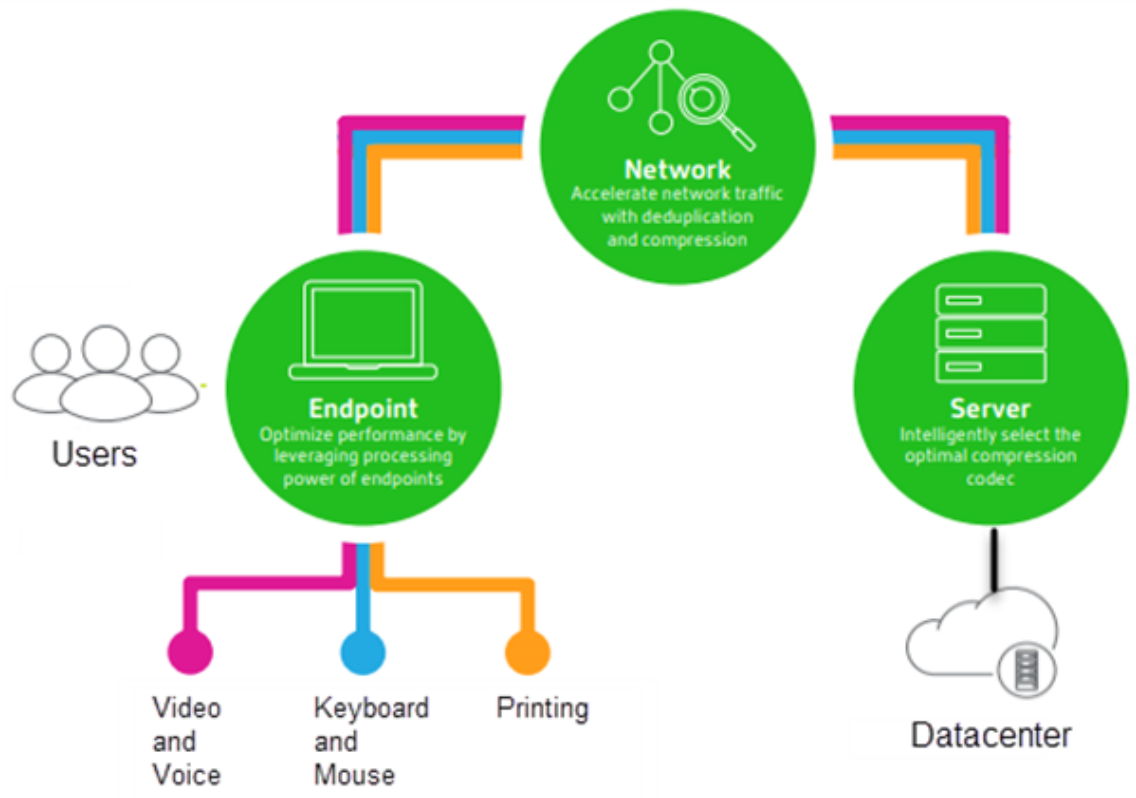

HDX basiert auf drei technischen Prinzipien:

- Intelligente Umleitung
- Adaptive Komprimierung
- Datendeduplizierung

Unter Anwendung in variablen Kombinationen optimieren sie die IT- und Benutzererfahrung, verringern den Bandbreitenverbrauch und erhöhen die Benutzerdichte pro Hostingserver.

- **Intelligente Umleitung:** Hierbei werden Bildschirmaktivität, Anwendungsbefehle, Endpunktgerät und Netzwerk-/Servermerkmale geprüft, um direkt zu bestimmen, wie und wo eine Anwendungs- oder Desktopaktivität gerendert werden soll. Das Rendering kann auf dem Endpunktgerät oder dem Hostingserver erfolgen.
- **Adaptive Komprimierung:** Durch die adaptive Komprimierung kann reichhaltiges Multimedia über schmale Netzwerkverbindungen bereitgestellt werden. HDX wertet zunächst mehrere Variablen aus, z. B. Art der Eingabe, Gerät und Anzeige (Text, Video, Sprache und Multimedia). Es wählt dann den optimalen Komprimierungs-Codec und das besten Verhältnis an CPU- und GPU-Nutzung aus. Es passt sich dann intelligent gemäß dem individuellen Benutzer und der Basis an. Die intelligente Anpassung erfolgt auf Benutzer- oder sogar Sitzungsbasis.




- **Datendeduplizierung:** Die Deduplizierung des Netzwerkverkehrs verringert die zwischen Client und Server gesendeten aggregierten Daten. Hierbei werden wiederholte Muster häufig verwendeter Daten (Bitmaps, Dokumente, Druckaufträge, gestreamte Medien usw.) genutzt. Durch die Zwischenspeicherung der Muster müssen nur die Änderungen über das Netzwerk übertragen werden und die doppelte Übertragung von Daten wird vermieden. HDX unterstützt auch das Multicasting von gestreamtem Multimedia, wenn eine Übertragung von der Quelle von mehreren Teilnehmern an einem Ort angezeigt wird (anstelle einer 1:1-Verbindung für jeden Benutzer).

Weitere Informationen finden Sie unter Boost productivity with a high-definition user workspace.

### Auf dem Gerät

HDX nutzt die Computingfähigkeiten der Benutzergeräte und verbessert und optimiert die Benutzererfahrung. Die HDX-Technologie liefert einen gleichmäßigen Empfang von Multimediainhalten auf virtuellen Desktops und in Anwendungen. Mit Workspace Control können Benutzer virtuelle Desktops und Anwendungen anhalten und auf einem anderen Gerät an derselben Stelle weiterarbeiten.

### Im Netzwerk

HDX enthält erweiterte Optimierungs- und Beschleunigungsfunktionen und gewährleistet die beste Leistung in jedem Netzwerk, auch bei Verbindungen mit niedriger Bandbreite und bei WAN-Verbindungen mit hoher Latenz.

HDX-Features passen sich den Änderungen in der Umgebung an. Sie stimmen Lastausgleich und Bandbreite aufeinander ab. Es werden optimale Technologien für die jeweiligen Benutzerszenarios eingesetzt und zwar sowohl bei lokalem Zugriff auf die Desktops oder Anwendungen im Unternehmensnetzwerk als auch bei Remotezugriff von außerhalb des Unternehmens.

### Im Datencenter

HDX nutzt die Verarbeitungsleistung und die Skalierbarkeit von Servern für eine erweitere Grafikleistung, unabhängig von den Funktionen des Clientgeräts.

Die in Citrix Director bereitgestellte HDX-Kanalüberwachung zeigt den Status der verbundenen HDX-Kanäle auf Benutzergeräten an.

### HDX Insight

HDX Insight ist die Integration von NetScaler Network Inspector und Performance Manager in Director. Es erfasst Daten zum ICA-Datenverkehr und bietet eine Dashboardansicht von Echtzeit- und historischen Daten. Dazu gehören die clientseitige und serverseitige ICA-Sitzungslatenz, die Bandbreitennutzung der ICA-Kanäle und die ICA-Roundtrip-Zeit für jede Sitzung.

Sie können NetScaler zur Verwendung des virtuellen HDX Insight-Kanals aktivieren, um alle erforderlichen Datenpunkte unkomprimiert zu verschieben. Wenn Sie das Feature deaktivieren, entschlüsselt und dekomprimiert das NetScaler-Gerät den ICA-Datenverkehr über verschiedene virtuelle Kanäle hinweg. Die Verwendung des einzelnen virtuellen Kanals verringert die Komplexität, verbessert die Skalierbarkeit und ist kosteneffektiver.

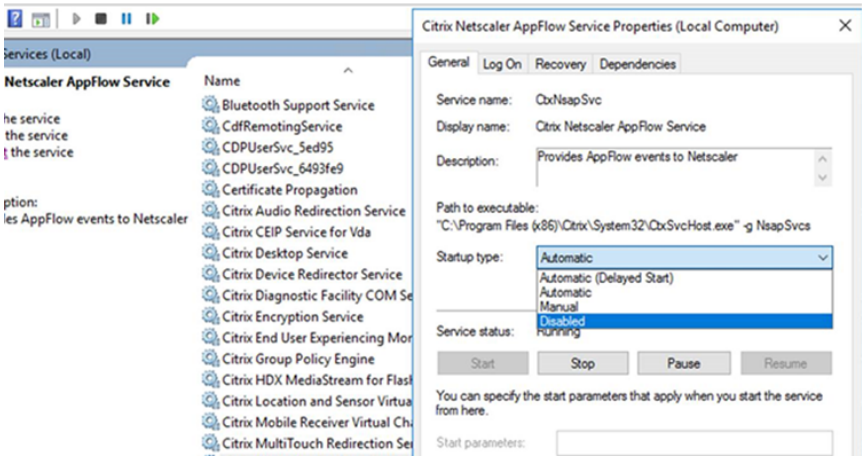
**Mindestanforderungen:**

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp und XenDesktop 7.17
- NetScaler Version 12.0 Build 57.x
- Citrix Workspace-App für Windows 1808
- Citrix Receiver für Windows 4.10
- Citrix Workspace-App für Mac 1808
- Citrix Receiver für Mac 12.8

### Aktivieren oder Deaktivieren des virtuellen HDX Insight-Kanals

Um dieses Feature zu deaktivieren, deaktivieren Sie den Dienst “Citrix NetScaler Application Flow” . Legen Sie den Dienst zum Aktivieren auf “Automatisch”fest. In beiden Fällen wird empfohlen, die Servermaschine nach dem Ändern der Eigenschaft neu zu starten. Der Dienst ist standardmäßig aktiviert (automatisch).




## Erleben von HDX-Funktionen mit Ihrem virtuellen Desktop

- Wenn Sie sehen möchten, wie die Browserinhaltsumleitung, eine von vier HDX-Multimediaumleitungstechno die Bereitstellung von HTML5- und WebRTC-Multimediainhalt beschleunigt:

  1. Laden Sie die Chrome-Browsererweiterung herunter und installieren Sie sie auf dem virtuellen Desktop.
  2. Um zu sehen, wie die Browserinhaltsumleitung die Bereitstellung von Multimediainhalten auf virtuellen Desktops beschleunigt, rufen Sie auf dem Desktop ein Video von einer Website mit HTML5-Videos auf (z. B. YouTube). Die Benutzer wissen nicht, wann die Browserinhaltsumleitung ausgeführt wird. Um zu sehen, ob die Browserinhaltsumleitung verwendet wird, ziehen Sie das Browserfenster schnell über den Bildschirm. Zwischen dem Viewport und Benutzeroberfläche macht sich eine Verzögerung bemerkbar. Sie können auch mit der rechten Maustaste auf die Webseite klicken und im Menü den Eintrag **Info über HDX-Browserumleitung** suchen.

- Um zu sehen, wie HDX HD-Audio bereitstellt führen Sie folgende Schritte aus:

  1. Konfigurieren Sie den Citrix Client für maximale Audioqualität; weitere Informationen hierzu finden Sie in der Citrix Workspace-App-Dokumentation.
  2. Geben Sie Musikdateien mit einem digitalen Audioplayer (z. B. iTunes) auf dem Desktop wieder.

HDX bietet standardmäßig qualitativ hochwertige Grafiken und Videos, für die meisten Benutzer ist keine Konfiguration erforderlich. Die standardmäßig aktivierten Citrix Richtlinieneinstellungen liefern die beste Lösung für die Mehrheit der Fälle.

- HDX wählt automatisch die beste Bereitstellungsmethode basierend auf Client, Plattform, Anwendung und Bandbreite und nimmt dann selbständig entsprechend der geänderten Bedingungen eine Einstellung vor.
- HDX optimiert die Leistung von 2D- und 3D-Grafiken und Video.
- HDX ermöglicht das Streamen von Multimediadateien für die Benutzergeräte direkt vom Quellenanbieter im Internet oder Intranet, ohne dass der Hostserver beteiligt wird. Wenn die Anforderungen für den clientseitigen Inhaltsabruf nicht erfüllt sind, wird bei der Medienbereitstellung automatisch auf serverseitigen Inhaltsabruf und Multimediaumleitung zurückgegriffen. Normalerweise ist keine Änderung der Richtlinien für die Multimediaumleitung erforderlich.
- HDX stellt hochwertige, auf dem Server wiedergegebene Videoinhalte auf virtuellen Desktops bereit, wenn die Multimediaumleitung nicht verfügbar ist: Zeigen Sie ein Video auf einer Website mit HD-Videos an, z. B. http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Nützliche Info:

- Informationen zum Support und zu Systemanforderungen für HDX-Features finden Sie unter Systemanforderungen. Sofern nicht anders angegeben, stehen HDX-Features für unterstützte Maschinen mit Windows-Multisitzungs-OS, Maschinen mit Windows-Einzelsitzungs-OS und Desktops mit Remote-PC-Zugriff zur Verfügung.
- Nachfolgend wird beschrieben, wie Sie die Benutzererfahrung optimieren, die Skalierbarkeit verbessern und die Bandbreitenanforderungen reduzieren können. Weitere Informationen zur Verwendung von Citrix Richtlinien und Richtlinieneinstellungen finden Sie unter Citrix Richtlinien zu diesem Release.
- Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### Automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit

Beim Zugriff auf gehostete Anwendungen oder Desktops können Unterbrechungen der Netzwerkverbindung auftreten. Zur Gewährleistung einer reibungsloseren Wiederverbindung bietet Citrix

die automatische Wiederverbindung von Clients und die Sitzungszuverlässigkeit. In der Standardkonfiguration startet die Sitzungszuverlässigkeit gefolgt von der automatischen Wiederverbinden von Clients.

**Automatische Wiederverbindung von Clients:**

Die automatische Wiederverbindung startet die Clientengine, um die Verbindung mit der getrennten Sitzung wiederherzustellen. Die automatische Wiederverbindung schließt oder trennt die Benutzersitzung, nach der in der Einstellung festgelegten Zeit. Wenn die automatische Wiederverbindung im Gang ist, wird der Benutzer folgendermaßen über die Anwendungs- bzw. Desktopunterbrechung benachrichtigt:

- **Desktops:** Das Sitzungsfenster wird abgeblendet und ein Countdowntimer zeigt die bis zur Wiederverbindung verbleibende Zeit an.
- **Anwendungen.** Das Sitzungsfenster wird geschlossen und ein Dialogfeld mit dem Countdown bis zur Wiederverbindung wird angezeigt.

Bei der automatischen Wiederverbindung des Clients starten Sitzungen und erwarten eine Netzwerkverbindung. Der Benutzer kann während der automatischen Wiederverbindung nicht mit der Sitzung interagieren.

Bei der Wiederverbindung werden die gespeicherten Verbindungsinformationen verwendet. Der Benutzer kann dann normal mit Anwendungen und Desktops interagieren.

Standardeinstellungen der automatischen Wiederverbindung von Clients:

- Timeout beim automatischen Wiederverbinden von Clients: 120 Sekunden
- Automatische Wiederverbindung von Clients: aktiviert
- Authentifizierung bei automatischer Wiederverbindung von Clients: deaktiviert
- Protokollierung der automatischen Wiederverbindung von Clients: deaktiviert

Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients".

**Sitzungszuverlässigkeit:**

Die Sitzungszuverlässigkeit gewährleistet eine nahtlose Wiederverbindung von ICA-Sitzungen bei Netzwerkunterbrechungen. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der in der Einstellung festgelegte Zeitraum abgelaufen ist. Nach Ablauf des Zeitraums werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen. Wenn die Sitzungszuverlässigkeit im Gang ist, wird der Benutzer folgendermaßen über die Anwendungs- bzw. Desktopunterbrechung benachrichtigt:

- **Desktops:** Das Sitzungsfenster wird durchscheinend und ein Countdowntimer zeigt die bis zur Wiederverbindung verbleibende Zeit an.

- **Anwendungen.** Das Fenster wird durchscheinend und im Infobereich wird eine Benachrichtigung über die Verbindungsunterbrechung geöffnet.

Bei laufendem Sitzungszuverlässigkeitsverfahren kann der Benutzer nicht mit der ICA-Sitzung interagieren. Benutzeraktionen wie Tastatureingaben werden jedoch für ein paar Sekunden unmittelbar nach der Netzwerkunterbrechung gepuffert und erneut übertragen, wenn das Netzwerk wieder verfügbar ist.

Bei Wiederverbindung fahren Client und Server an dem Punkt des Austauschprotokolls fort, an dem die Verbindung unterbrochen wurde. Das Sitzungsfenster wird wieder normal angezeigt und im Infobereich werden entsprechende Benachrichtigungen für Anwendungen geöffnet.

Standardeinstellungen für die Sitzungszuverlässigkeit

- Sitzungszuverlässigkeit - Timeout: 180 Sekunden
- UI-Deckkraft während Wiederverbindung: 80 %
- Sitzungszuverlässigkeit - Verbindungen: aktiviert
- Sitzungszuverlässigkeit - Portnummer: 2598

Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Sitzungszuverlässigkeit".

**NetScaler mit automatischer Wiederverbindung von Clients und Sitzungszuverlässigkeit:**

Die Sitzungszuverlässigkeit und die automatische Wiederverbindung von Clients funktionieren nicht, wenn Multistream- und Multiport-Richtlinien auf dem Server aktiviert sind und mindestens eine oder folgenden Bedingungen vorliegt:

- Die Sitzungszuverlässigkeit ist unter NetScaler Gateway deaktiviert.
- Ein Failover findet auf dem NetScaler-Gerät statt.
- NetScaler SD-WAN wird mit NetScaler Gateway verwendet.

### Adaptiver HDX-Durchsatz

Der adaptive HDX-Durchsatz passt den Spitzendurchsatz einer ICA-Sitzung über die Ausgabepuffer intelligent an. Die Anzahl der Ausgabepuffer ist anfangs auf einen hohen Wert eingestellt. Der hohe Wert ermöglicht es insbesondere in Netzwerken mit hoher Latenz, Daten schneller und effizienter an den Client zu übertragen. Die bessere Interaktivität, schnellere Dateiübertragungen, flüssigere Videowiedergabe sowie höhere Framerate und Auflösung sorgen für eine bessere Benutzererfahrung.

Die Sitzungsinteraktivität wird ständig gemessen, um festzustellen, ob Datenströme innerhalb der ICA-Sitzung die Interaktivität beeinträchtigen. Ist dies der Fall, wird der Durchsatz verringert, um die Beeinträchtigungen durch den großen Datenstrom zu verringern und die Interaktivität wiederherzustellen.

> **Wichtig:**
>
> Der adaptive HDX-Durchsatz ändert die Einstellmethode der Ausgabepuffer, durch Übertragung des Mechanismus vom Client auf den VDA. Eine manuelle Konfiguration ist nicht erforderlich.

Dieses Feature erfordert Folgendes:

- VDA-Version 1811 oder höher
- Workspace-App für Windows 1811 oder höher

### Verbessern der Bildqualität an Benutzergeräten

Die folgenden Richtlinieneinstellungen für "Visuelle Anzeige"steuern die Qualität der Bilder, die von virtuellen Desktops auf Benutzergeräte gesendet werden.

- Bildqualität: steuert die visuelle Qualität der Bilder auf dem Benutzergerät: Mittel, Hoch, Immer verlustfrei, Zu verlustfrei verbessern (Standardeinstellung = Mittel). Die tatsächliche Videoqualität bei der Standardeinstellung "Mittel"hängt von der verfügbaren Bandbreite ab.
- Frameratesollwert: gibt die maximale Anzahl von Frames pro Sekunde an, die vom virtuellen Desktop zum Benutzergerät gesendet werden (Standardwert = 30). Bei Geräten mit langsamen CPUs erzielen Sie durch Festlegen eines niedrigeren Werts eine bessere Benutzererfahrung. Die maximal unterstützte Framerate pro Sekunde ist 60.
- Anzeigespeicherlimit: gibt die maximale Größe des Videopuffers (in Kilobyte) für die Sitzung an (Standardwert = 65536 KB). Für Verbindungen, die eine größere Farbtiefe und eine höhere Auflösung erfordern, erhöhen Sie den Grenzwert. Sie können den maximal erforderlichen Speicher berechnen.

### Verbessern der Videokonferenzleistung

Mehrere gebräuchliche Videokonferenzanwendungen wurden für die Multimediaumleitung aus Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) optimiert (z. B. HDX RealTime Optimization Pack). Bei nicht optimierten Anwendungen verbessert die HDX-Webcam-Videokomprimierung die Bandbreiteneffizienz und Latenztoleranz für Webcams bei Videokonferenzen. Bei dieser Technologie werden die Webcamdaten über einen dedizierten virtuellen Multimediakanal gestreamt. Die Technologie beansprucht weniger Bandbreite als die isochrone HDX-Plug-n-Play-USB-Umleitung und funktioniert gut über WAN-Verbindungen.

Citrix Workspace-App-Benutzer können das Standardverhalten außer Kraft setzen, wenn sie in Desktop Viewer unter "Mikrofon & Webcam"die Einstellung **Mikrofon und Webcam nicht verwenden** auswählen. Um zu verhindern, dass Benutzer die HDX-Webcamvideokomprimierung ändern,

deaktivieren Sie die Umleitung von USB-Geräten über die Richtlinieneinstellungen unter ICA > USB-Geräte.

HDX-Webcam-Videokomprimierung erfordert, dass die folgenden Richtlinieneinstellungen aktiviert sind (alle sind standardmäßig aktiviert).

- Clientaudioumleitung
- Clientmikrofonumleitung
- Multimediakonferenzen
- Windows Media-Umleitung

Bei Hardware-verschlüsselungsfähigen Webcams verwendet HDX-Videokomprimierung die Hardware-Codierung standardmäßig. Die Hardwarecodierung kann mehr Bandbreite verbrauchen als die Softwarecodierung. Zum Erzwingen der Softwarekomprimierung fügen Sie dem folgenden Registrierungsschlüssel den folgenden DWORD-Wert hinzu: `HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1`

### Prioritäten für den Netzwerkdatenverkehr

Prioritäten für den Netzwerkdatenverkehr über mehrere Verbindungen für eine Sitzung werden zugewiesen, indem QoS-fähige Router verwendet werden. Vier TCP-Streams und zwei UDP-Streams sind zum Übertragen von ICA-Daten zwischen dem Benutzergerät und dem Server verfügbar.

- TCP-Streams: real time, interactive, background und bulk
- UDP-Streams: Voice und Framehawk-Display-Remoting

Jeder virtuelle Kanal ist mit einer bestimmten Priorität verknüpft und wird von der entsprechenden TCP-Verbindung transportiert. Sie können die Kanäle basierend auf der Portnummer, die für die Verbindung verwendet wird, unabhängig voneinander festlegen.

Gestreamte Mehrkanalverbindungen werden für Virtual Delivery Agents (VDAs) unterstützt, die auf Windows 10- und Windows 8-Maschinen installiert sind. Arbeiten Sie mit dem Netzwerkadministrator Ihres Unternehmens zusammen, um sicherzustellen, dass die in der Einstellung "Multiport-Richtlinie" konfigurierten Common Gateway Protocol (CGP)-Ports auf den Netzwerkroutern richtig zugewiesen sind.

Quality of Service wird nur unterstützt, wenn mehrere Sitzungszuverlässigkeitsports oder CGP-Ports konfiguriert sind.

> **Warnung:**
>
> Verwenden Sie Transportsicherheit, wenn Sie dieses Feature einsetzen. Citrix empfiehlt die Verwendung von Internetprotokollsicherheit (IPsec) oder Transport Layer Security (TLS). TLS-Verbindungen werden nur unterstützt, wenn die Verbindungen durch ein NetScaler Gateway

> passieren, das Multistream-ICA unterstützt. Bei internen Unternehmensnetzwerken werden Multistreamverbindungen mit TLS nicht unterstützt.

Fügen Sie folgende Citrix Richtlinieneinstellungen einer Richtlinie hinzu, um die Servicequalität für mehrere Streamingverbindungen festzulegen (weitere Details finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen"):

- Multiportrichtlinie: Diese Einstellung legt Ports für den ICA-Verkehr über mehrere Verbindungen fest und definiert die Netzwerkpriorität.
  - Wählen Sie in der Liste "CGP-Standardportpriorität"eine Priorität aus. Standardmäßig hat der primäre Port (2598) eine hohe Priorität.
  - Geben Sie in den Feldern "CGP-Port1", "CGP-Port2"und "CGP-Port3"je nach Bedarf zusätzliche CGP-Ports ein und geben Sie entsprechende Prioritäten an. Jeder Port muss eine eindeutige Priorität haben.

  Konfigurieren Sie die Firewalls auf VDAs explizit so, dass zusätzlicher TCP-Datenverkehr zulässig ist.
- Multistreamcomputereinstellung: Diese Einstellung ist standardmäßig deaktiviert. Wenn Sie Citrix NetScaler SD-WAN mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service zu erzielen.
- Multistreambenutzereinstellung: Diese Einstellung ist standardmäßig deaktiviert.

Damit die Richtlinien mit diesen Einstellungen wirksam werden, müssen sich Benutzer abmelden und dann am Netzwerk anmelden.

### Ein- und Ausblenden der Remotesprachenleiste

Remotesprachenleiste ein- und ausblenden: Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Anwendungssitzungen angezeigt. Wenn das Feature aktiviert ist (= Standardeinstellung), können Sie die Sprachenleiste in der Citrix Workspace-App für Windows über **Erweiterte Einstellungen > Sprachenleiste** ein- und ausblenden. Über eine Registrierungseinstellung auf dem VDA können Sie die Steuerung der Sprachenleiste auf dem Client deaktivieren. Wenn das Feature deaktiviert ist, wird die Client-UI-Einstellung nicht wirksam und der Status der Sprachenleiste wird über die für den Benutzer geltende Einstellung bestimmt. Weitere Informationen finden Sie unter Verbessern der Benutzererfahrung.

Deaktivieren der Clientsteuerung der Sprachenleiste über den VDA

1. Navigieren Sie im Registrierungs-Editor zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI.
2. Erstellen Sie den DWORD-Wertschlüssel "SeamlessFlags"und legen Sie ihn auf "0x40000"fest.

## Unicode-Tastaturzuordnung

Citrix Receiver für andere Betriebssysteme als Windows verwenden das lokale Tastaturlayout (Unicode). Ändert ein Benutzer das lokale Tastaturlayout und das Servertastaturlayout (Scancode), erfolgt möglicherweise keine Synchronisierung und die Ausgabe ist falsch. Beispiel: User1 stellt das lokale Tastaturlayout von Englisch auf Deutsch um. User1 stellt dann die serverseitige Tastatur auf Deutsch um. Obwohl beide Tastaturlayouts auf Deutsch eingestellt wurden, sind sie möglicherweise nicht synchron und verursachen eine falsche Zeichenausgabe.

### Aktivieren oder Deaktivieren der Unicode-Tastaturzuordnung

Das Feature ist VDA-seitig standardmäßig deaktiviert. Zum Aktivieren des Features verwenden Sie den Registrierungs-Editor auf dem VDA. Fügen Sie den folgenden Registrierungsschlüssel hinzu:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: EnableKlMap

Typ: DWORD

Wert: 1

Zum Deaktivieren des Features legen Sie **EnableKlMap** auf 0 fest oder löschen Sie den Schlüssel **CtxKlMap**.

### Aktivieren des mit der Unicode-Tastaturzuordnung kompatiblen Modus

Standardmäßig sorgt bei der Unicode-Tastaturzuordnung automatisch eine Windows-API dafür, dass die neue Unicode-Tastaturzuordnung neu geladen wird, wenn Sie das Tastaturlayout serverseitig ändern. Bei einigen Anwendungen ist die hierfür erforderliche Hook-Einbindung nicht möglich. Sie können Sie das Feature in den kompatiblen Modus versetzen, um Anwendungen ohne Hook zu unterstützen. Fügen Sie den folgenden Registrierungsschlüssel hinzu:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: DisableWindowHook

Typ: DWORD

Wert: 1

Legen Sie zur Verwendung der normalen Unicode-Tastaturzuordnung **DisableWindowHook** auf 0 fest.

## Virtuelle ICA-Kanäle von Citrix

March 6, 2024

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

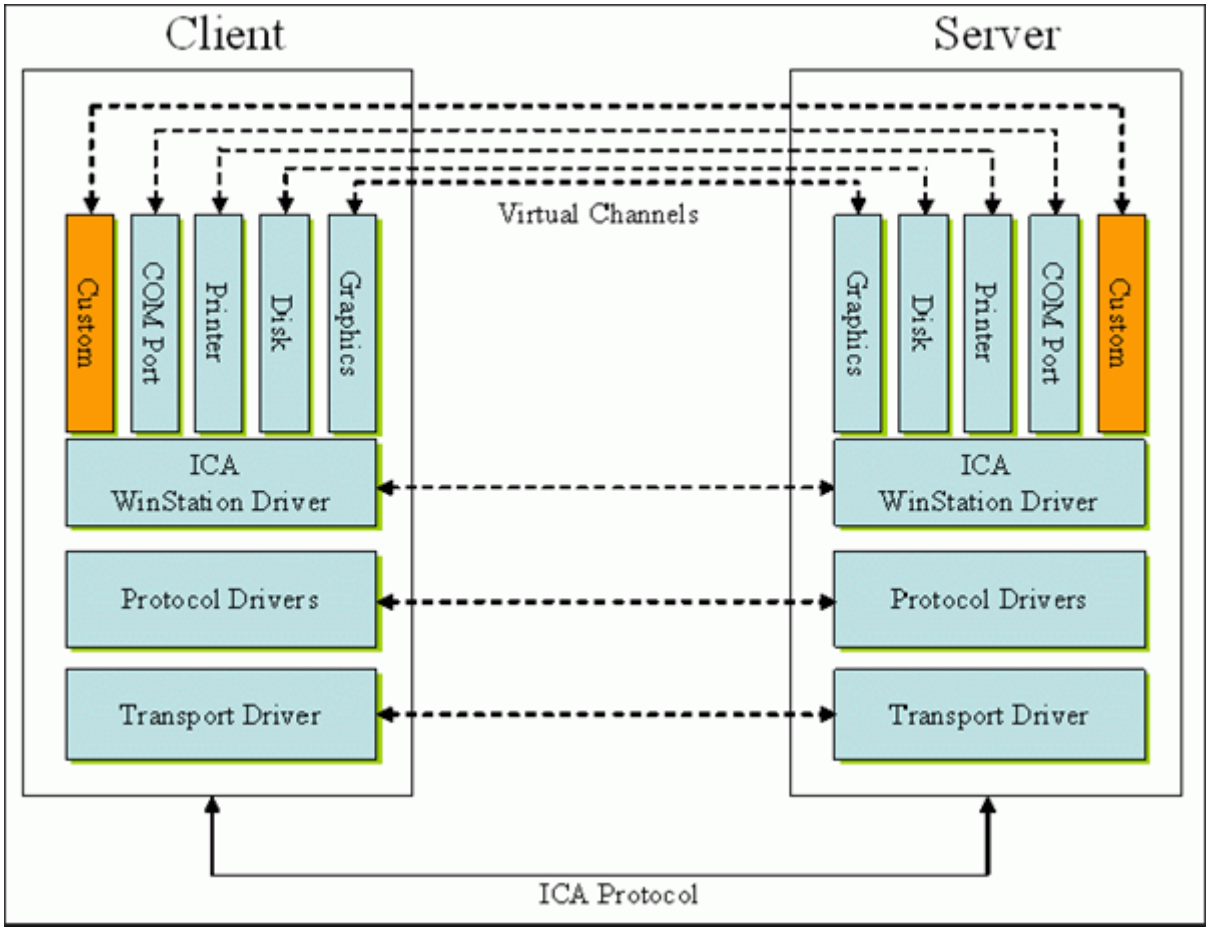
### Was sind virtuelle ICA-Kanäle

Ein großer Teil der Funktionalität und Kommunikation zwischen der Citrix Workspace-App und den Servern von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) erfolgt über virtuelle Kanäle. Virtuelle Kanäle sind erforderlich für den Remotezugriff auf Citrix DaaS-Server. Virtuelle Kanäle werden für Folgendes verwendet:

- Audio
- COM-Ports
- Datenträger
- Grafik
- LPT-Ports
- Drucker
- Smartcards
- Benutzerdefinierte virtuelle Kanäle von Drittanbietern
- Video

Gelegentlich werden neue virtuelle Kanäle mit Citrix DaaS und der Citrix Workspace-App veröffentlicht, um mehr Funktionalität zu bieten.




Ein virtueller Kanal besteht aus einem clientseitigen virtuellen Treiber, der mit einer serverseitigen Anwendung kommuniziert. Im Lieferumfang von Citrix DaaS sind mehrere virtuelle Kanäle enthalten. Diese sollen es Kunden und Drittanbietern ermöglichen, eigene virtuelle Kanäle mit einem der mitgelieferten Software Development Kits (SDKs) zu entwickeln.

Virtuelle Kanäle bieten eine sichere Möglichkeit, verschiedene Aufgaben zu erfüllen. Beispiele sind Anwendungen auf einem Citrix Virtual Apps-Server, die mit einem clientseitigen Gerät kommunizieren, oder Anwendungen, die mit der clientseitigen Umgebung kommunizieren.

Auf der Clientseite entsprechen virtuelle Kanäle virtuellen Treibern. Jeder virtuelle Treiber hat eine bestimmte Funktion. Einige sind für den Normalbetrieb erforderlich, während andere optional genutzt werden können. Virtuelle Treiber agieren auf der Protokollebene der Präsentationsschicht. Durch Multiplexing von Kanälen, die durch die Windows Station (WinStation)-Protokollebene bereitgestellt werden, können jederzeit mehrere Protokolle aktiv sein.

Die folgenden Funktionen sind im Registrierungswert "VirtualDriver"unter diesem Registrierungspfad enthalten:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\
Advanced\Modules\ICA 3.0
```

Oder

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (für 64-Bit-Versionen)

- Thinwire3.0 (erforderlich)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Zwischenablage
- ClientComm
- ClientAudio
- LicenseHandler (erforderlich)
- TWI (erforderlich)
- SmartCard
- ICACTL (erforderlich)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Hinweis:**
>
> Sie können spezielle Clientfunktionen deaktivieren, indem Sie einen oder mehrere dieser Werte aus dem Registrierungsschlüssel entfernen. Wenn Sie beispielsweise die Client-Zwischenablage entfernen möchten, entfernen Sie das Wort **Clipboard**.

Diese Liste enthält die virtuellen Client-Treiberdateien und ihre jeweiligen Funktionen. Citrix Virtual Apps und die Citrix Workspace-App für Windows verwenden diese Dateien. Sie sind als Dynamic Link Libraries (Benutzermodus) und nicht als Windows-Treiber (Kernelmodus) konzipiert, mit Ausnahme von Generischem USB, wie unter "Virtueller Kanal für Generisches USB"beschrieben.

- vd3dn.dll –Virtueller Kanal für Direct3D, verwendet für die Desktopgestaltungsumleitung
- vdcamN.dll –Bidirektionales Audio
- vdcdm30n.dll –Clientlaufwerkzuordnung
- vdcom30N.dll –Client-COM-Portzuordnung
- vdcpm30N.dll –Clientdruckerzuordnung
- vdctln.dll –ICA-Steuerungskanal
- vddvc0n.dll –Dynamischer virtueller Kanal
- vdeuemn.dll –End User Experience Monitoring
- vdgusbn.dll –Virtueller Kanal für Generisches USB
- vdkbhook.dll –Transparentes Schlüsselpassthrough
- vdlfpn.dll –Framehawk-Anzeigekanal mit Übertragung auf UDP-Basis

- vdmmn.dll –Multimedia-Unterstützung
- vdmrvc.dll –Virtueller Kanal für Mobile Receiver
- vdmtchn.dll –Multitouch-Unterstützung
- vdscardn.dll –Smartcard-Unterstützung
- vdsens.dll –Virtueller Kanal für Sensoren
- vdspl30n.dll –Client-UPD
- vdsspin.dll –Kerberos
- vdtuin.dll –Transparente Benutzeroberfläche
- vdtw30n.dll –Client-Thinwire
- vdtwin.dll –Seamless
- vdtwn.dll –Twain

Einige virtuelle Kanäle werden in andere Dateien kompiliert. Die Zwischenablagezuordnung ist beispielsweise in wfica32.exe verfügbar.

#### 64-Bit-Kompatibilität

Die Citrix Workspace-App für Windows ist 64-Bit-kompatibel. Wie für die meisten Binärdateien, die für 32 Bit kompiliert sind, gibt es auch für diese Clientdateien 64-Bit-Äquivalente:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

#### Virtueller Kanal für Generisches USB

Beim Implementieren eines virtuellen Kanals für Generisches USB werden zwei Kernelmodustreiber und der virtuelle Kanaltreiber vdgusbn.dll verwendet:

- ctxusbm.sys
- ctxusbr.sys

### Funktionsweise virtueller ICA -Kanäle

Virtuelle Kanäle werden auf verschiedene Art geladen. Mit der Shell (WFShell für den Server und PicaShell für die Workstation) werden einige virtuelle Kanäle geladen. Einige virtuelle Kanäle werden als Windows-Dienste gehostet.

Beispiele virtueller Kanalmodule, die von der Shell geladen werden:

- EUEM
- TWAIN
- Zwischenablage
- Multimedia
- Seamless-Sitzungsfreigabe
- Zeitzone

Manche werden im Kernelmodus geladen. Beispiel sind:

- CtxDvcs.sys –Dynamischer virtueller Kanal
- Icausbb.sys –Generische USB-Umleitung
- Picadm.sys –Clientlaufwerkzuordnung
- Picaser.sys –COM-Portumleitung
- Picapar.sys –LPT-Portumleitung

### Virtueller Kanal für Grafiken auf der Serverseite

Ab XenApp 7.0 und XenDesktop7.0 hostet `ctxgfx.exe` den virtuellen Grafikkanal für Sitzungen auf Arbeitsstations- und Terminalserverbasis. `Ctxgfx` hostet plattformspezifische Module, die mit dem entsprechenden Treiber interagieren (`Icardd.dll` für RDSH sowie `vdod.dll` und `vidd.dll` für Arbeitsstation).

Für XenDesktop 3D Pro-Bereitstellungen wird ein OEM-Grafiktreiber für den entsprechenden Grafikprozessor auf dem VDA installiert. `Ctxgfx` lädt spezielle Adaptermodule für die Interaktion mit dem OEM-Grafiktreiber.

### Ausführen spezialisierter Kanäle in Windows-Diensten

Auf Citrix DaaS-Servern werden verschiedene Kanäle als Windows-Dienste gehostet. Ein solches Hosting bietet eine Zuordnungssemantik vom Typ 1:n für mehrere Anwendungen in einer Sitzung und für mehrere Sitzungen auf dem Server. Beispiele für derartige Dienste:

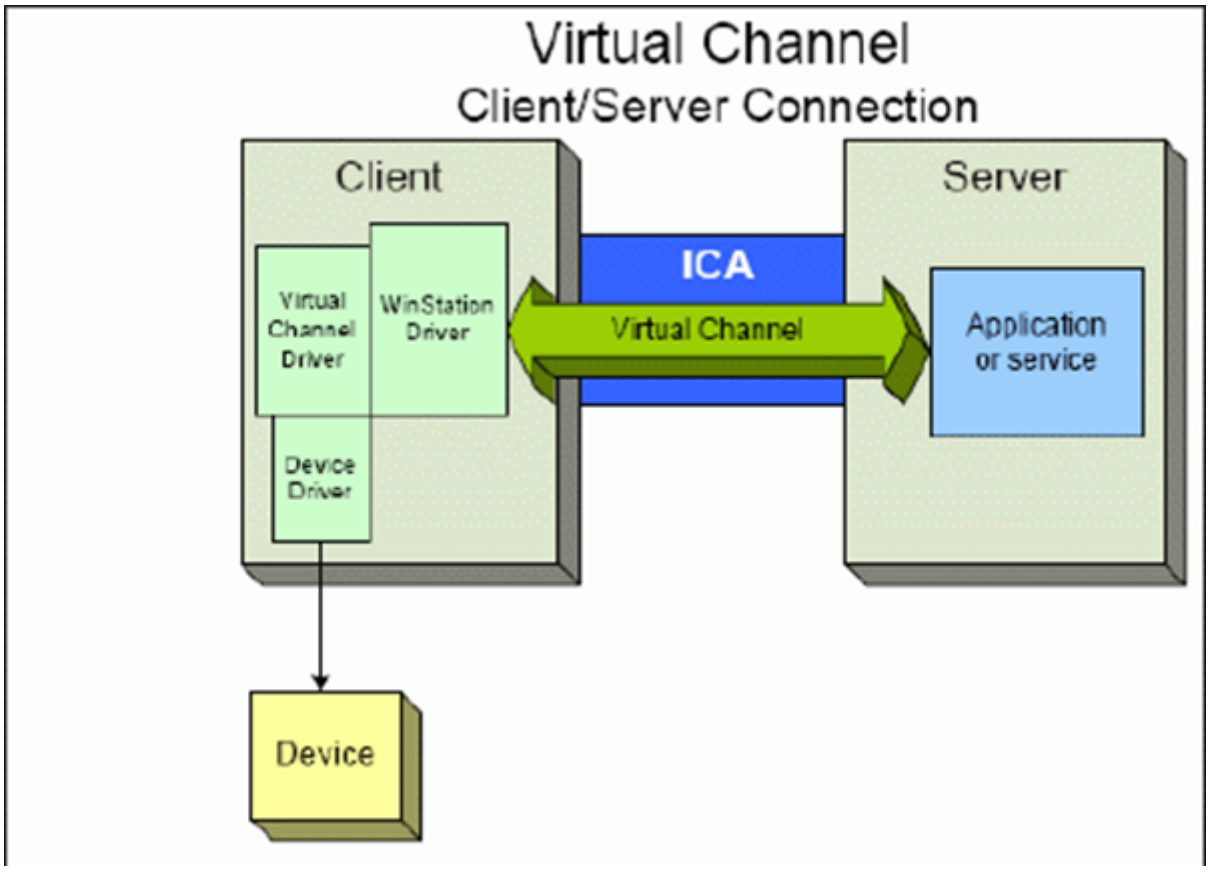
- Citrix-Geräteumleitungsdienst
- Citrix-Dienst für dynamische virtuelle Kanäle

- Citrix-Dienst für End User Experience Monitoring
- Citrix-Dienst für virtuelle Standort- und Sensorkanäle
- Citrix Multitouch-Umleitungsdienst
- Citrix Druckmanagerdienst
- Citrix-Smartcarddienst
- Citrix-Audioumleitungsdienst (nur Citrix Virtual Desktops)
- Citrix ICA Status Channel Service

Der virtuelle Audiokanal in Citrix Virtual Apps wird über den Windows Audiodienst gehostet.

Auf der Serverseite werden alle virtuellen Client-Kanäle über den WinStation-Treiber Wdica.sys geleitet. Auf der Clientseite werden die virtuellen Client-Kanäle vom entsprechenden WinStation-Treiber abgefragt, der in wfica32.exe integriert ist. Dieses Bild veranschaulicht die Client-Server-Verbindung mit virtuellem Kanal.




Diese Übersicht enthält einen Client-Server-Datenaustausch über einen virtuellen Kanal.

1. Der Client stellt eine Verbindung zum Citrix DaaS-Server her. Der Client sendet Informationen zu den unterstützten virtuellen Kanälen an den Server.
2. Die serverseitige Anwendung wird gestartet, erhält ein Handle für den virtuellen Kanal und fragt optional weitere Informationen zum Kanal ab.

3. Der virtuelle Clienttreiber und die serverseitige Anwendung nutzen die folgenden zwei Methoden zur Datenübertragung:

    - Wenn Daten von der Serveranwendung an den Client zu senden sind, werden die Daten sofort übertragen. Wenn der Client die Daten empfängt, werden die über den virtuellen Kanal übertragenen Daten aus dem ICA-Datenstrom vom WinStation-Treiber demultiplext und sofort an den virtuellen Clienttreiber weitergeleitet.
    - Wenn Daten vom virtuellen Clienttreiber an den Server zu senden sind, werden sie bei der nächsten Datenabfrage durch den WinStation-Treiber übertragen. Wenn der Server die Daten empfängt, bleiben sie bis zur Auswertung durch die virtuelle Kanalanwendung in der Warteschlange. Es gibt keine Möglichkeit, die virtuelle Kanalanwendung des Servers über den Datenempfang zu informieren.

4. Nach Abschluss der virtuellen Kanalanwendung auf dem Server werden der virtuelle Kanal geschlossen und alle zugewiesenen Ressourcen freigegeben.

### Erstellen eines eigenen virtuellen Kanals mit dem Virtual Channel SDK

Das Erstellen eines virtuellen Kanals mit dem Virtual Channel SDK erfordert fortgeschrittene Programmierkenntnisse. Verwenden Sie diese Methode, um einen größeren Kommunikationspfad zwischen Client und Server bereitzustellen. Dies gilt beispielsweise beim Implementieren eines Geräts auf dem Client (z. B. eines Scanners), der mit einem Prozess in der Sitzung verwendet werden soll.

> **Hinweis:**
>
> - Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.
> - Aufgrund des erhöhten Sicherheitsniveaus in Citrix DaaS müssen Sie angeben, welche virtuellen Kanäle in einer ICA-Sitzung geöffnet werden dürfen. Weitere Informationen finden Sie unter Richtlinieneinstellungen für Positivliste virtueller Kanäle.

### Erstellen eines eigenen virtuellen Kanals mit dem ICA Client Object SDK

Das Erstellen eines virtuellen Kanals mit dem ICA Client Object (ICO) ist einfacher als die Verwendung des Virtual Channel SDK. Zur Verwendung des ICO erstellen Sie mit dem **CreateChannels**-Verfahren ein benanntes Objekt in Ihrem Programm.

> **Wichtig:**
>
> Aufgrund der erhöhten Sicherheit für Citrix Receiver für Windows ab Version 10.00 (und Citrix Workspace-Apps für Windows) ist bei der Installation eines virtuellen ICO-Kanals ein zusätzlicher

> Schritt erforderlich.

Weitere Informationen finden Sie im Client Object API Specification Programmer's Guide.

### Passthrough-Funktionalität virtueller Kanäle

Bei Verwendung der Citrix Workspace-App für Windows in einer ICA-Sitzung (auch Passthrough-Sitzung genannt) funktionieren die meisten von Citrix bereitgestellten virtuellen Kanäle unverändert. Berücksichtigen Sie jedoch Folgendes, wenn Sie den Client in zusätzlichen Hops verwenden.

Die folgenden Funktionen funktionieren auf die gleiche Weise in einzelnen Hops oder in mehreren Hops:

- Client-COM-Portzuordnung
- Clientlaufwerkzuordnung
- Clientdruckerzuordnung
- Client-UPD
- End User Experience Monitoring
- Standard-USB
- Kerberos
- Multimedia-Unterstützung
- Smartcard-Unterstützung
- Transparentes Schlüsselpassthrough
- TWAIN

Da Latenz und Faktoren wie Komprimierung, Dekomprimierung und Rendering jedoch bei jedem Hop auftreten, kann jeder zusätzliche Client-Hop die Leistung beeinträchtigen. Dies betrifft folgende Bereiche:

- Bidirektionales Audio
- Dateiübertragungen
- Generische USB-Umleitung
- Seamless
- Thinwire

> **Wichtig:**
>
> Standardmäßig sind die von einer Client-Instanz in einer Passthrough-Sitzung zugeordneten Clientlaufwerke auf die Clientlaufwerke des verbindenden Clients beschränkt.

### Passthrough-Funktionalität virtueller Kanäle zwischen einer Citrix Virtual Desktop-Sitzung und einer Citrix Virtual App-Sitzung

Bei Verwendung der Citrix Workspace-App für Windows in einer ICA-Sitzung auf einem Citrix Virtual Desktops-Server (auch Passthrough-Sitzung genannt) funktionieren die meisten von Citrix bereitgestellten virtuellen Kanäle unverändert.

Auf dem Citrix Virtual Desktops-Server gibt es einen speziellen VDA-Hook, der **picaPassthruHook** ausführt. Durch diesen Hook läuft der Client wie auf einem CPS-Server und wird in den traditionellen Passthrough-Modus versetzt.

Wir unterstützen die folgenden traditionellen virtuellen Kanäle und ihre Funktionalität:

- Client
- Client-COM-Portzuordnung
- Clientlaufwerkzuordnung
- Clientdruckerzuordnung
- Generisches USB (leistungsbeschränkt)
- Multimedia-Unterstützung
- Smartcard-Unterstützung
- SSON
- Transparentes Schlüsselpassthrough

### Sicherheit und virtuelle ICA-Kanäle

Bei der Planung, Entwicklung und Implementierung virtueller Kanäle ist eine sichere Nutzung von entscheidender Bedeutung. Dieses Dokument enthält mehrere Verweise auf spezielle Sicherheitsbereiche.

### Bewährte Methoden

Öffnen Sie virtuelle Kanäle beim **Verbinden** und **Wiederverbinden**. Schließen Sie virtuelle Kanäle, wenn Sie sich abmelden und die **Verbindung trennen**.

Beachten Sie die folgenden Richtlinien, wenn Sie Skripts erstellen, die virtuelle Kanalfunktionen verwenden.

**Benennen der virtuellen Kanäle:**

Sie können maximal 32 virtuelle Kanäle erstellen. Siebzehn der 32 Kanäle sind für besondere Zwecke reserviert.

- Die Namen virtueller Kanäle dürfen nicht mehr als sieben Zeichen enthalten.

- Die ersten drei Zeichen sind für den Anbieternamen und die folgenden vier Zeichen für den Kanaltyp reserviert. **CTXAUD** stellt beispielsweise den virtuellen Audiokanal von Citrix dar.

Virtuelle Kanäle werden mit einem ASCII-Namen aus maximal sieben Zeichen bezeichnet. In einigen früheren Versionen des ICA-Protokolls wurden virtuelle Kanäle nummeriert. Die Nummern werden nun dynamisch auf der Basis des ASCII-Namens zugewiesen, da dies die Implementierung vereinfacht. Benutzer, die ihren virtuellen Kanalcode nur für den internen Gebrauch entwickeln, können einen beliebigen Namen aus sieben Zeichen verwenden, sofern kein Konflikt mit vorhandenen virtuellen Kanälen auftritt. Verwenden Sie nur Ziffern sowie Groß- und Kleinbuchstaben im ASCII-Format. Verwenden Sie die bestehende Namenskonvention, wenn Sie eigene virtuelle Kanäle hinzufügen. Es gibt mehrere vordefinierte Kanäle. Die vordefinierten Kanäle beginnen mit der OEM-Kennung CTX und sind nur von Citrix zu verwenden.

**Double-Hop-Unterstützung:**

| Virtueller Kanal | Wird Double Hop unterstützt |
|---|---|
| Audio | Nein |
| Browserinhaltsumleitung | Nein |
| CDM | Ja |
| CEIP | Nein |
| Zwischenablage | Ja |
| Continuum (MRVC) | Nein |
| Control VC | Ja |
| HTML5-Videoumleitung (v1) | Ja |
| Tastatur, Maus | Ja |
| MultiTouch | Nein |
| NSAPVC | Nein |
| Drucken | Ja |
| SensVC | Nein |
| Smartcard | Ja |
| TWAIN | Ja |
| USB VC | Ja |
| WAYCOM-Geräte -K2M mit USB-VC | Ja |
| Webcamvideokomprimierung | Ja |

| | |
|---|---|
| Virtueller Kanal | Wird Double Hop unterstützt |
| Windows Media-Umleitung | Ja |

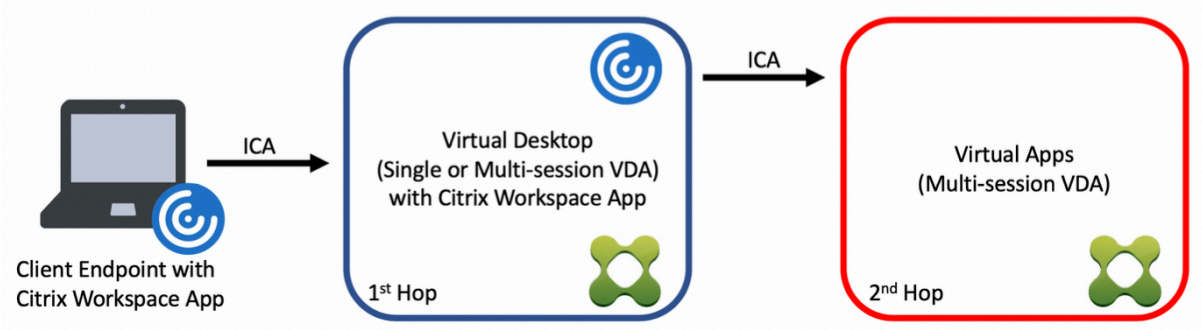
### Siehe auch

- ICA Virtual Channel SDK
- Das Citrix Developer Network umfasst alle technischen Ressourcen und Diskussionen zur Verwendung von Citrix SDKs. Sie erhalten Zugriff auf SDKs, Beispielcode und Skripte, Erweiterungen und Plug-Ins sowie die SDK-Dokumentation. Foren zum Citrix Developer Network mit technischen Diskussionen zu den einzelnen Citrix SDKs sind ebenfalls enthalten.

## Double-Hop in Citrix DaaS

May 17, 2024

Im Kontext mit Citrix Clientsitzungen bezieht sich der Begriff "Double-Hop"auf Citrix Virtual Apps-Sitzungen, die in einer Citrix Virtual Desktops-Sitzung ausgeführt werden. Die folgende Abbildung veranschaulicht einen Double-Hop.




Wenn ein Benutzer in einem Double-Hop-Szenario eine Verbindung zu einem virtuellen Citrix Desktop herstellt, der auf einem Einzelsitzungs-OS-VDA ausgeführt wird ("VDI") bzw. zu einem virtuellen Desktop, der auf einem Multisitzungs-OS-VDA ausgeführt wird ("veröffentlichter Desktop"), gilt dies als erster Hop. Nach Erstellen der Verbindung kann der Benutzer eine Citrix Virtual Apps-Sitzung starten. Dies gilt als zweiter Hop.

Sie können eine Double-Hop-Bereitstellung für verschiedene Anwendungsfälle verwenden. Ein geläufiges Beispiel ist die Verwaltung der Citrix Virtual Desktop- und der Citrix Virtual Apps-Umgebung durch verschiedene Entitäten. Diese Methode kann auch bei der Lösung von Anwendungskompatibilitätsproblemen helfen.

## Systemanforderungen

Alle Editionen von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unterstützen Double-Hop.

Der erste Hop muss eine unterstützte Version des VDAs für Einzelsitzungs-OS bzw. Multisitzungs-OS und der Citrix Workspace-App verwenden. Der zweite Hop muss eine unterstützte Version des VDAs für Multisitzungs-OS verwenden. Informationen zu unterstützten Versionen finden Sie in der Produktmatrix.

Zur Gewährleistung der optimalen Leistung und der Kompatibilität empfiehlt Citrix die Verwendung eines Citrix Clients der gleichen Version wie der des VDAs oder einer höheren Version.

Wenn am ersten Hop eine Lösung für virtuelle Desktops eines Drittanbieters (nicht von Citrix) in Kombination mit einer Citrix Virtual Apps-Sitzung beteiligt ist, beschränkt sich die Unterstützung auf die Citrix Virtual Apps-Umgebung. Bei Problemen im Zusammenhang mit virtuellen Desktops von Drittanbietern (z. B. die Kompatibilität mit der Citrix Workspace-App, die Hardwareumleitung oder die Sitzungsleistung betreffend) kann Citrix nur begrenzt technischen Support leisten. Bei der Problembehandlung ist möglicherweise ein Citrix Virtual Desktop beim ersten Hop erforderlich.

## Bereitstellung von HDX in Double-Hop-Szenarien

Generell ist jede Sitzung in einem Double-Hop einmalig und Client-Server-Funktionen sind auf einen Hop isoliert. Dieser Abschnitt enthält Informationen zu Bereichen, die von Citrix Administratoren besonders berücksichtigt werden müssen. Citrix empfiehlt Kunden, die benötigten HDX-Funktionen gründlich zu testen, um eine angemessene Benutzererfahrung und Leistung für die jeweilige Umgebungskonfiguration sicherzustellen.

### Grafik

Verwenden Sie Standardgrafikeinstellungen (selektive Codierung) für den ersten und zweiten Hop. Für HDX 3D Pro empfiehlt Citrix dringend die lokale Ausführung aller Anwendungen, für die eine Grafikbeschleunigung erforderlich ist, im ersten Hop, wobei dem VDA die benötigten GPU-Ressourcen zur Verfügung stehen müssen.

### Latenz

Die Ende-zu-Ende-Latenz kann sich auf die Benutzererfahrung auswirken. Berücksichtigen Sie die zusätzliche Latenz zwischen dem ersten und dem zweiten Hop. Dies ist besonders wichtig bei der Umleitung von Hardwaregeräten.

### Multimedia

Die serverseitige (sitzungsinterne) Wiedergabe von Audio- und Videoinhalten funktioniert am besten im ersten Hop. Eine Videowiedergabe im zweiten Hop erfordert die De- und Recodierung im ersten Hop, wodurch die Bandbreiten- und Hardwareressourcennutzung erhöht wird. Audio- und Videoinhalte müssen möglichst auf den ersten Hop beschränkt werden.

### USB-Geräteumleitung

HDX umfasst generische und optimierte Umleitungsmodi zur Unterstützung einer Vielzahl von USB-Gerätetypen. Achten Sie auf den in jedem Hop verwendeten Modus und verwenden Sie die folgende Tabelle als Referenz für ein optimales Ergebnis. Weitere Informationen zur generischen und optimierten Umleitung finden Sie unter Generische USB-Geräte.

| Erster Hop (VDI- oder veröffentlichter Desktop) | Zweiter Hop (virtuelle Apps) | Hinweise zur Unterstützung |
|---|---|---|
| Optimiert | Optimiert | Empfohlen (basierend auf Geräteunterstützung). Beispiele: USB-Massenspeicher, TWAIN-Scanner, Webcam, Audio. |
| Generisch | Generisch | Für Geräte, bei denen die Option “Optimiert”nicht verfügbar ist. |
| Generisch | Optimiert | Obwohl anders technisch möglich, wird empfohlen, den Modus “Optimiert”für beide Hops zu verwenden, wenn die Geräteunterstützung verfügbar ist. |
| Optimiert | Generisch | Nicht unterstützt |

> **Hinweis:**
>
> Da USB-Protokolle inhärent gesprächig sind, kann die Leistung über Hops hinweg abnehmen. Funktionalität und Ergebnisse variieren je nach Gerät und Anwendungsanforderungen. Validierungstests werden für jede Geräteumleitung, insbesondere bei Double-Hop-Szenarien, dringend empfohlen.

### Ausnahmen bei der Unterstützung

Double-Hop-Sitzungen unterstützen die meisten HDX-Funktionen mit Ausnahme der folgenden:

- Browserinhaltsumleitung
- Lokaler App-Zugriff
- RealTime Optimization Pack für Skype for Business
- Optimierung für Microsoft Teams

## HDX-Konnektivität

May 17, 2024

Citrix HDX bietet Benutzern zentralisierter Anwendungen und Desktops auf jedem Gerät und in jedem Netzwerk vielfältige Technologien für ein High Definition-Erlebnis.

HDX basiert auf drei technischen Prinzipien:

- Intelligente Umleitung
- Adaptive Komprimierung
- Datendeduplizierung

Unter Anwendung in variablen Kombinationen optimieren sie die IT- und Benutzererfahrung, verringern den Bandbreitenverbrauch und erhöhen die Benutzerdichte pro Hostingserver.

Das HDX-Angebot ermöglicht Ihnen den Verbindungsaufbau über ein einzigartiges, proprietäres Transportprotokoll, die Verwendung der maximalen Anzahl von Übertragungseinheiten beim Einrichten von Sitzungen und eine optimierte Konnektivität mit Citrix SD-WAN.

## Adaptiver Transport

May 17, 2024

Adaptiver Transport ist ein Mechanismus in Citrix Virtual Apps and Desktops, der es ermöglicht, Verbindungen für HDX-Sitzungen über ein bevorzugtes Transportprotokoll herzustellen und gleichzeitig ein Fallback auf TCP bereitzustellen, wenn die Konnektivität mit dem bevorzugten Protokoll nicht verfügbar ist.

Die folgenden Transportprotokolle werden unterstützt:

- Enlightened Data Transport (EDT)
- Übertragungssteuerungsprotokoll (TCP)

### Konfiguration

Der adaptive Transport ist standardmäßig aktiviert. Sie können den adaptiven Transport für folgende Modi konfigurieren:

- **Bevorzugt**: (Standard) Der Client versucht, eine Verbindung mit dem bevorzugten Protokoll herzustellen, und fällt auf TCP zurück, wenn die Konnektivität mit dem bevorzugten Protokoll nicht verfügbar ist.
- **Diagnosemodus**: Der Client versucht nur, eine Verbindung mit dem bevorzugten Protokoll herzustellen. Das Fallback auf TCP wird deaktiviert.
- **Aus**: Der Client versucht nur, eine Verbindung über TCP herzustellen.

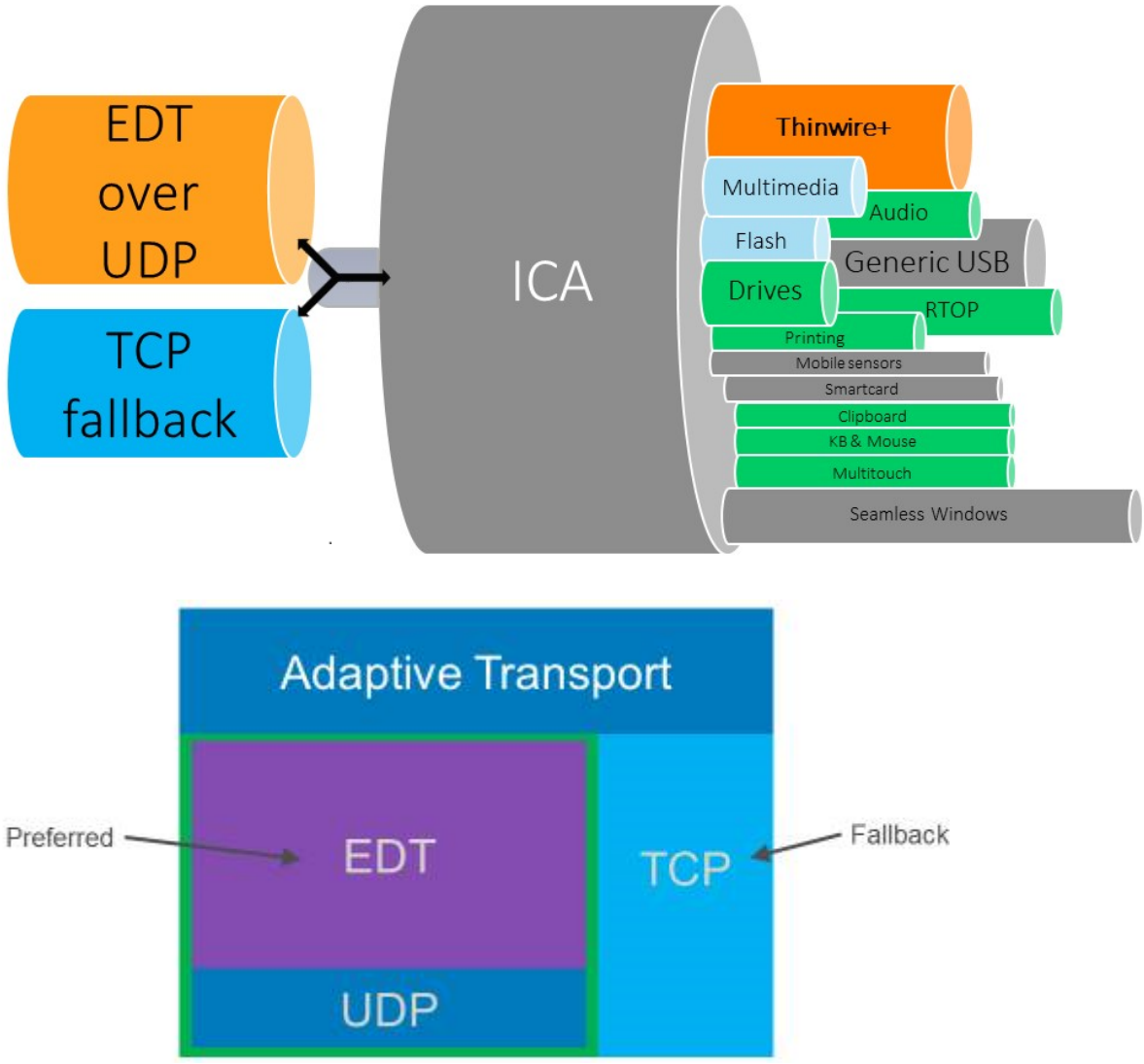
### Funktionsweise

Wenn **Adaptiver Transport** auf `Preferred` eingestellt ist, versucht der Client, eine Verbindung zur Sitzung sowohl mit dem bevorzugten Protokoll als auch mit TCP parallel herzustellen. Auf diese Weise kann die Verbindungszeit optimiert werden, wenn keine Verbindung mit dem bevorzugten Protokoll hergestellt werden kann und der Client auf TCP zurückgreifen muss. Wenn die Verbindung über TCP hergestellt wird, versucht der Client alle fünf Minuten, im Hintergrund eine Verbindung mit dem bevorzugten Protokoll herzustellen.

Wenn **Adaptiver Transport** auf `Diagnostic mode` eingestellt ist, stellt der Client nur mit dem bevorzugten Protokoll eine Verbindung zur Sitzung her. Wenn der Client keine Verbindung mit dem bevorzugten Protokoll herstellen kann, greift er nicht auf TCP zurück und die Verbindung schlägt fehl.

Wenn **Adaptiver Transport** auf `Off` eingestellt ist, ist **Adaptiver Transport** deaktiviert und der Client stellt nur über TCP eine Verbindung zur Sitzung her.




### Systemanforderungen

Dies sind die Anforderungen für den Einsatz von adaptivem Transport und EDT:

- Steuerungsebene
  - Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops: aktuell unterstützte Version
- Virtual Delivery Agent
  - Windows: aktuell unterstützte Version (2402 oder höher empfohlen)
  - Linux: aktuell unterstützte Version (2402 oder höher empfohlen)
- Citrix Workspace-App

  - Windows: aktuell unterstützte Version (2402 oder höher empfohlen)
  - Linux: aktuell unterstützte Version (2402 oder höher empfohlen)
  - Mac: aktuell unterstützte Version (2402 oder höher empfohlen)
  - iOS: aktuell verfügbare Version im Apple App Store
  - Android: aktuell verfügbare Version in Google Play

- Citrix NetScaler Gateway
  - 14.1.12.30 oder höher (empfohlen)
  - 13.1.17.42 oder höher (13.1-52.19 oder höher empfohlen)

> **Hinweis:**
>
> Einzelheiten zu Linux VDA finden Sie in der Dokumentation zu Linux Virtual Delivery Agent.

## Netzwerkanforderungen

In den folgenden Abschnitten sind die Netzwerkanforderungen für die Verwendung von EDT mit adaptivem Transport aufgeführt:

### Sitzungshosts

Wenn Ihre Sitzungshosts über eine Firewall wie die Windows Defender-Firewall verfügen, müssen Sie den folgenden eingehenden Verkehr für interne Verbindungen zulassen.

| Beschreibung | Quelle | Protokoll | Port |
|---|---|---|---|
| Interne Verbindung — Sitzungszuverlässigkeit aktiviert | Client | UDP | 2598 |
| Interne Verbindung — Sitzungszuverlässigkeit deaktiviert | | | 1494 |
| Interne Verbindung — HDX Direct oder VDA SSL | | | 443 |

> **Hinweis:**
>
> Das VDA-Installationsprogramm fügt der Windows Defender-Firewall die entsprechenden Regeln

> für eingehenden Datenverkehr hinzu. Wenn Sie eine andere Firewall verwenden, müssen Sie die obigen Regeln hinzufügen.

#### Internes Netzwerk

Die folgende Tabelle zeigt die Firewallregeln, die für die Verwendung von EDT in Ihrem Netzwerk erforderlich sind:

| Beschreibung | Protokoll | Quelle | Ziel | Zielport |
|---|---|---|---|---|
| Direkte interne Verbindung — Sitzungszuverlässigkeit aktiviert | UDP | Clientnetzwerk | VDA-Netzwerk | 2598 |
| Direkte interne Verbindung — Sitzungszuverlässigkeit deaktiviert | | | | 1494 |
| Direkte interne Verbindung — HDX Direct oder VDA SSL | | | | 443 |
| NetScaler Gateway | | NetScaler-SNIP | | 2598 |
| NetScaler Gateway —VDA SSL | | | | 443 |

> **Hinweis:**
>
> Wenn Sie den Citrix Gateway Service verwenden, müssen Sie **Rendezvous** aktivieren, um EDT als Transportprotokoll zu verwenden. Die System- und Netzwerkanforderungen finden Sie in der Rendezvous-Dokumentation.

#### Clientnetzwerk

In der folgenden Tabelle sind die Konnektivitätsanforderungen für Clientgeräte aufgeführt:

| Beschreibung | Protokoll | Quelle | Ziel | Zielport |
|---|---|---|---|---|
| Interne Verbindung — Sitzungszuverlässigkeit aktiviert | UDP | Client IP | VDA-Netzwerk | 2598 |
| Interne Verbindung — Sitzungszuverlässigkeit deaktiviert | | | | 1494 |
| Interne Verbindung — HDX Direct oder SSL VDA | | | | 443 |
| Externe Verbindung — NetScaler Gateway | | | Öffentliche IP-Adresse von NetScaler Gateway | 443 |
| Externe Verbindung – Citrix Gateway Service | | | Citrix Gateway Service | 443 |

> **Hinweis:**
>
> Wenn Sie den Citrix Gateway Service verwenden, müssen die Clients https://*.*.nssvc.net erreichen können. Wenn Sie nicht alle Unterdomänen mit https://*.*.nssvc.net zulassen können, verwenden Sie stattdessen https://*.c.nssvc.net und https://*.g.nssvc.net. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX270584.

## Enlightened Data Transport (EDT)

May 17, 2024

EDT (Enlightened Data Transport) ist ein Citrix-eigenes Transportprotokoll, das auf UDP (User Datagram Protocol) basiert. Es liefert eine überlegene Benutzererfahrung bei schwierigen Langstreckenverbindungen, ohne Abstriche bei der Serverskalierbarkeit. EDT verbessert den Datendurchsatz für alle virtuellen ICA-Kanäle in instabilen Netzwerken und bietet so einen verlässlicheren Service.

Wenn **Adaptiver Transport** aktiviert ist, ist EDT das bevorzugte Protokoll.

### Nützliche Informationen

- Die **Sitzungszuverlässigkeit** muss aktiviert sein, um **MTU Discovery** und EDT mit NetScaler Gateway und Citrix Gateway Service verwenden zu können.
- Die Paketfragmentierung kann in einigen Fällen zu Leistungseinbußen oder sogar zum Versagen beim Öffnen von Sitzungen führen. Um dies zu verhindern, müssen Sie die EDT-MTU auf einen für Ihre Netzwerke angemessenen Wert einstellen. Sie können EDT MTU Discovery oder eine manuelle Problemumgehung verwenden, die unter So konfigurieren Sie MSS bei Verwendung von EDT in Netzwerken mitnicht stehender MTU beschrieben wird.
- Einzelheiten zur Aktivierung von EDT mit NetScaler Gateway finden Sie unter NetScaler Gateway zur Unterstützung von Enlightened Data Transport konfigurieren.

### MTU-Discovery durch EDT

Mit MTU-Discovery kann EDT beim Einrichten einer Sitzung automatisch die maximale Übertragungseinheit (MTU) ermitteln. Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu einer Leistungsminderung oder einem Fehler beim Einrichten der Sitzung führen kann.

Die MTU-Discovery ist standardmäßig aktiviert. Wenn Sie es deaktivieren müssen, finden Sie weitere Informationen unter HDX-Funktionen, die über die Registrierung verwaltet werden.

> **Hinweis:**
>
> - **Sitzungszuverlässigkeit** muss aktiviert sein, damit MTU-Discovery funktioniert.
> - MTU-Discovery mit Multistream-ICA ist mit VDA-Version 2209 und höher verfügbar.

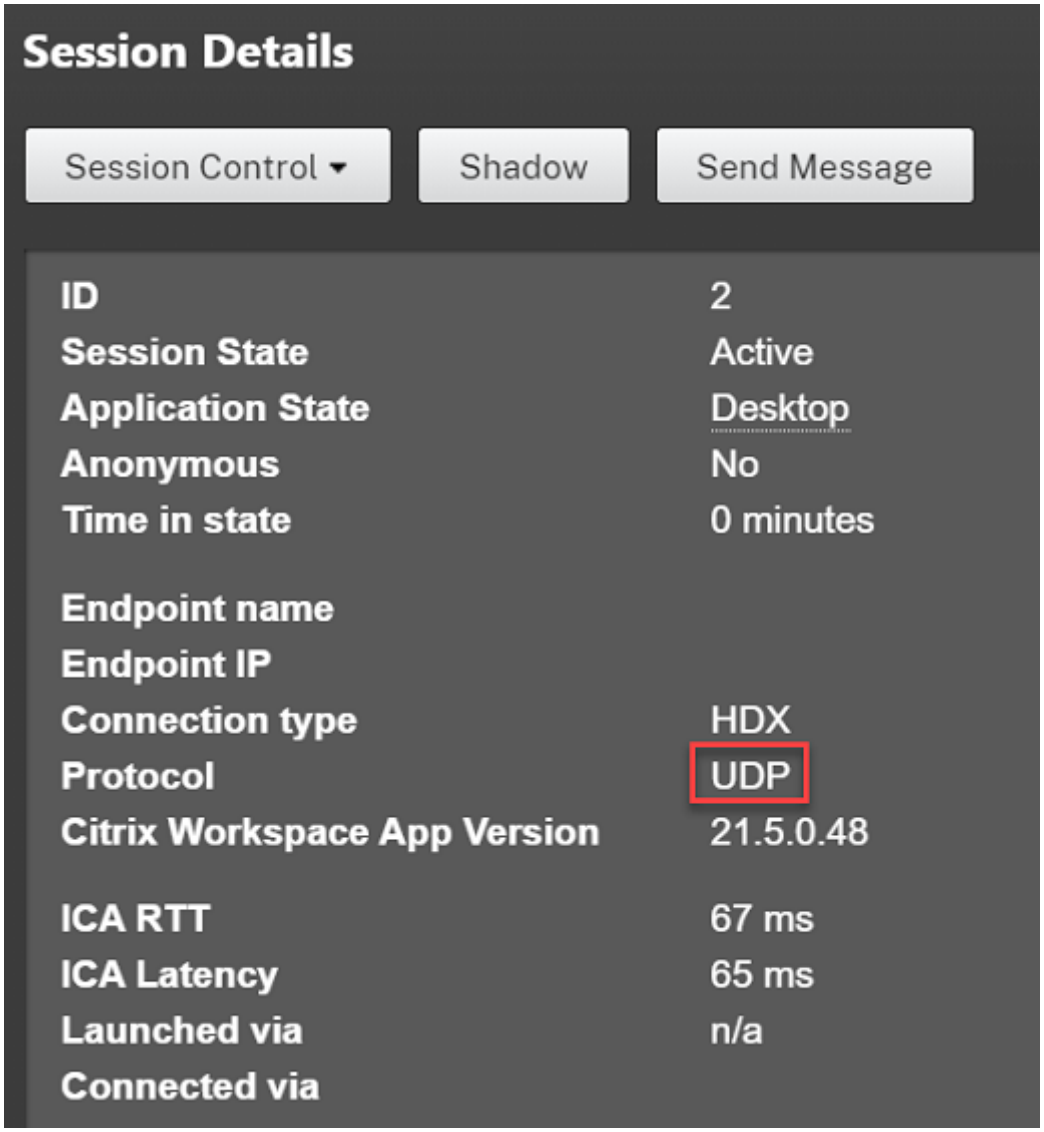
## Problembehandlung

May 17, 2024

Mit Director oder dem Befehlszeilenprogramm `CtxSession.exe` auf dem VDA können Sie bestätigen, dass EDT als Transportprotokoll für die Sitzung verwendet wird.

In Director suchen Sie die Sitzung und wählen dann **Details**. Wenn als **Verbindungstyp** HDX und als **Protokoll** UDP angezeigt ist, wird EDT als Transportprotokoll für die Sitzung verwendet.

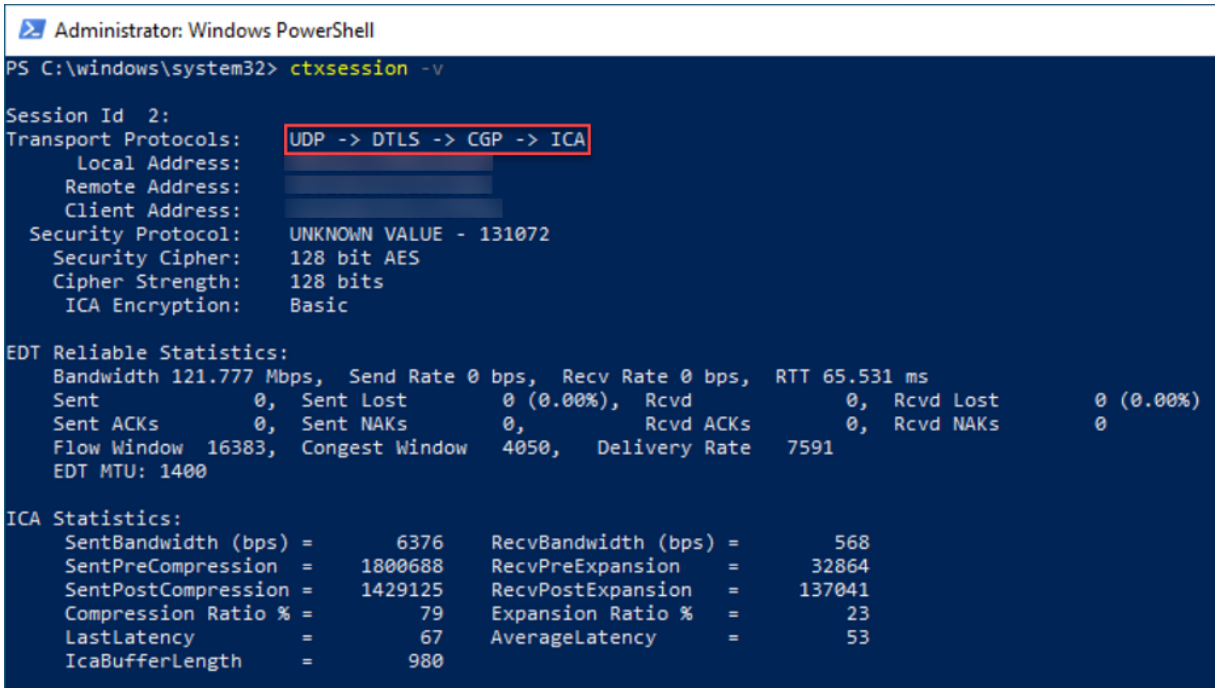
 




Um das Hilfsprogramm CtxSession.exe zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen `ctxsession.exe` aus. Zur Anzeige ausführlicher Statistiken führen Sie `ctxsession.exe -v` aus. Wenn EDT verwendet wird, wird eine der folgenden Optionen im Transportprotokoll angezeigt:

- **UDP > ICA** (Sitzungszuverlässigkeit deaktiviert)
- **UDP > CGP > ICA** (Sitzungszuverlässigkeit aktiviert)
- **UDP > DTLS > CGP > ICA** (ICA ist DTLS-verschlüsselt und Ende-zu-Ende)




### Wenn Sitzungen keine Verbindung mit EDT herstellen können

Folgendes wird zur Problembehandlung beim **adaptiven Transport** und **EDT** empfohlen:

1. Prüfen Sie die Systemanforderungen, Netzwerkanforderungen, Bekannten Probleme und Nützliche Informationen und achten Sie darauf, dass alle Punkte erfüllt sind.
2. Überprüfen Sie, ob vorhandene Citrix-Richtlinien in Studio oder im GPO die gewünschte Einstellung für den **adaptiven HDX-Transport** überschreiben.
3. Überprüfen Sie, ob vorhandene Einstellungen auf dem Client die gewünschte Einstellung für den adaptiven HDX-Transport überschreiben. Dies kann ein Voreinstellung im Gruppenrichtlinienobjekt, eine mit einer optionalen administrativen Vorlage der Workspace-App konfigurierte Einstellung oder eine manuelle Konfiguration der Einstellung **HDXoverUDP** in der Registrierung oder der Konfigurationsdatei des Clients sein.
4. Stellen Sie auf Maschinen mit Multisitzungs-VDA sicher, dass die UDP-Listener aktiv sind. Öffnen Sie eine Eingabeaufforderung in der VDA-Maschine und führen Sie `netstat -a -p udp` aus. Weitere Informationen finden Sie unter How to Confirm HDX Enlightened Data Transport Protocol.
5. Überprüfen Sie, ob die Firewallregeln in den Netzwerk-Firewalls und in den Firewalls, die auf den VDA-Maschinen ausgeführt werden, richtig konfiguriert sind.
6. Starten Sie intern eine direkte Sitzung unter Umgehung von NetScaler Gateway oder Citrix Gateway Service und überprüfen Sie das verwendete Protokoll. Wenn die Sitzung EDT verwendet, ist

der VDA in der Lage, EDT für externe Verbindungen über NetScaler Gateway oder Citrix Gateway Service zu verwenden.

7. Wenn EDT für direkte interne Verbindungen funktioniert und nicht für Sitzungen, die über NetScaler Gateway oder Citrix Gateway Service laufen:

   - Vergewissern Sie sich, dass die **Sitzungszuverlässigkeit** aktiviert ist.
   - Wenn Sie NetScaler Gateway verwenden, vergewissern Sie sich, dass Ihre Konfiguration der erforderlichen Konfiguration entspricht, die unter NetScaler Gateway zur Unterstützung von Enlightened Data Transport und HDX Insight konfigurieren beschrieben ist.

8. Wenn Sie den Citrix Gateway Service verwenden, vergewissern Sie sich, dass Rendezvous aktiviert ist und funktioniert.

9. Überprüfen Sie, ob die Verbindungen Ihrer Benutzer eine nicht standardmäßige MTU benötigen. Verbindungen mit einer effektiven MTU von weniger als 1500 Byte verursachen eine EDT-Paketfragmentierung, die sich auf die Leistung auswirken oder sogar den Sitzungsstart verhindern kann. Dieses Problem tritt häufig auf, wenn VPN, einige WLAN-Zugangspunkte und Mobilfunknetze wie 4G und 5G verwendet werden. Vergewissern Sie sich, dass Sie MTU Discovery aktiviert haben oder eine benutzerdefinierte MTU einrichten, wie unter So konfigurieren Sie MSS bei Verwendung von EDT in Netzwerken mitnicht stehender MTU beschrieben.

### Bekannte Probleme

- Bei asymmetrischen Netzwerkpfaden kann die MTU-Discovery bei Verbindungen fehlschlagen, die nicht über NetScaler Gateway oder Citrix Gateway Service laufen. Führen Sie ein Upgrade auf VDA Version 2103 oder höher durch, um dieses Problem zu beheben. [CVADHELP-16654]
- Bei Verwendung von NetScaler Gateway können asymmetrische Netzwerkpfade dazu führen, dass die MTU-Discovery fehlschlägt. Dies liegt an einem Problem im Gateway, das dazu führt, dass das DF-Bit (don't fragment) im Header der EDT-Pakete nicht verteilt wird. Ein Fix für dieses Problem ist ab Firmware-Release 13.1 Build 17.42 verfügbar. Einzelheiten zur Aktivierung des Fixes finden Sie in der NetScaler Gateway-Dokumentation. [CGOP-18438]
- MTU-Discovery schlägt möglicherweise für Benutzer fehl, die sich über ein DS-Lite-Netzwerk verbinden. Einige Modems ignorieren das DF-Bit bei aktivierter Paketverarbeitung, sodass die MTU-Discovery eine Fragmentierung nicht erkennt. In dieser Situation sind folgende Optionen verfügbar:
  - Deaktivieren Sie die Paketverarbeitung auf dem Modem des Benutzers.
  - Deaktivieren Sie **MTU Discovery** und verwenden Sie eine fest codierte MTU, wie unter So konfigurieren Sie MSS bei Verwendung von EDT in Netzwerken mitnicht stehender MTU beschrieben.

- Deaktivieren Sie den **adaptiven Transport**, um die Verwendung von TCP für Sitzungen zu erzwingen. Wenn nur eine Untergruppe von Benutzern betroffen ist, können Sie sie möglicherweise auf der Clientseite deaktivieren, damit andere Benutzer EDT weiterhin verwenden können.

## Rendezvousprotokoll

June 5, 2023

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll VDAs, die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerungsebene herzustellen.

Es gibt zwei Arten von Datenverkehr, die berücksichtigt werden müssen:

1. Steuerungsverkehr für die VDA-Registrierung und die Sitzungsvermittlung.
2. HDX-Sitzungsverkehr.

Es sind zwei Versionen von Rendezvous verfügbar:

- Version 1 (V1) unterstützt das Umgehen der Citrix Cloud Connectors für den HDX-Sitzungsverkehr.
- Version 2 (V2) unterstützt das Umgehen der Citrix Cloud Connectors für den Steuerungsverkehr und den HDX-Sitzungsverkehr.

Einzelheiten zu Systemanforderungen, Richtlinien und Konfiguration der beiden Rendezvous-Versionen finden Sie in der zugehörigen Dokumentation.

Rendezvous-V1-Dokumentation

Rendezvous-V2-Dokumentation

## Rendezvous V1

April 26, 2023

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll VDAs, die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerungsebene herzustellen.

### Anforderungen

- Zugriff auf die Umgebung mit Citrix Workspace und Citrix Gateway Service.
- Steuerungsebene: Citrix DaaS (Citrix Cloud).
- VDA: Version 1912 oder höher.
  - Version 2012 ist die für EDT Rendezvous erforderliche Mindestversion.
  - Version 2012 ist die für die Unterstützung nicht transparenter Proxys erforderliche Mindestversion (keine Unterstützung für PAC-Dateien).
  - Version 2103 als Minimum für Proxykonfiguration mit PAC-Datei erforderlich.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix Richtlinie. Weitere Informationen finden Sie unter Richtlinieneinstellung für Rendezvous-Protokoll.
- Die VDAs müssen Zugriff auf `https://*.nssvc.net` einschließlich aller Unterdomänen haben. Wenn Sie nicht alle Unterdomänen auf diese Weise auf die Positivliste setzen können, verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Abschnitt Anforderungen an die Internetkonnektivität der Citrix Cloud-Dokumentation (unter "Citrix DaaS") und im Knowledge Center-Artikel CTX270584.
- Die VDAs müssen über TCP 443 für TCP Rendezvous bzw. über UDP 443 für EDT Rendezvous eine Verbindung zu den zuvor genannten Adressen herstellen können.
- Cloud Connectors müssen beim Brokering einer Sitzung die FQDNs der VDAs abrufen. Sie erreichen dies auf einer der folgenden beiden Arten:
  - **Aktivieren Sie die DNS-Auflösung für die Site.** Navigieren Sie zu **Vollständige Konfiguration > Einstellungen** und aktivieren Sie die Einstellung **DNS-Auflösung aktivieren**. Verwenden Sie alternativ das Citrix Virtual Apps and Desktops Remote PowerShell SDK und führen Sie den Befehl `Set-BrokerSite -DnsResolutionEnabled $true` aus. Weitere Informationen zum Citrix Virtual Apps and Desktops Remote PowerShell SDK finden Sie unter SDKs und APIs.
  - **DNS-Reverse-Lookupzone mit PTR-Einträgen für VDAs.** Wenn Sie diese Option wählen, empfehlen wir, VDAs so zu konfigurieren, dass immer versucht wird, PTR-Einträge zu registrieren. Navigieren Sie dazu mit dem Gruppenrichtlinieneditor oder Gruppenrichtlinienobjekt zu **Computerkonfiguration > Administrative Vorlagen > Netzwerk > DNS-Client** und legen Sie **PTR-Einträge registrieren** auf **Aktiviert und Registrieren** fest. Wenn das DNS-Suffix der Verbindung nicht mit dem DNS-Suffix der Domäne übereinstimmt, müssen Sie auch die Einstellung **Verbindungsspezifisches DNS-Suffix** konfigurieren, damit die Maschinen PTR-Einträge erfolgreich registrieren.

> **Hinweis:**
>
> Wenn Sie die DNS-Auflösung verwenden, müssen die Cloud Connectors die vollqualifizierten Domänennamen (FQDNs) der VDA-Maschinen auflösen können. Wenn interne Benutzer eine direkte Verbindung mit VDA-Maschinen herstellen, müssen die Clientgeräte ebenfalls die FQDNs der VDA-Maschinen auflösen können.
>
> Wenn Sie eine DNS-Reverse-Lookupzone verwenden, müssen die FQDNs in den PTR-Einträgen mit den FQDNs der VDA-Maschinen übereinstimmen. Enthält ein PTR-Eintrag einen anderen FQDN, schlägt die Rendezvous-Verbindung fehl. Ist beispielsweise der FQDN der Maschine `vda01.domain.net`, muss der PTR-Eintrag `vda01.domain.net` enthalten. Ein anderer FQDN, etwa `vda01.sub.domain.net`, funktioniert nicht.

## Proxykonfiguration

Der VDA unterstützt den Aufbau von Rendezvous-Verbindungen über einen Proxy.

### Überlegungen zum Proxy

Berücksichtigen Sie Folgendes, wenn Sie Proxys mit Rendezvous verwenden:

- Transparente Proxys, nicht transparente HTTP-Proxys und SOCKS5-Proxys werden unterstützt.
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der ICA-Datenverkehr zwischen dem VDA und Gateway Service nicht abgefangen, entschlüsselt oder überprüft wird. Ansonsten bricht die Verbindung ab.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung mithilfe von Aushandlung und Kerberos- oder NTLM-Authentifizierungsprotokoll.

  Wenn Sie eine Verbindung mit dem Proxyserver herstellen, wählt das Aushandlungsauthentifizierungsschema automatisch das Kerberos-Protokoll aus. Wenn Kerberos nicht unterstützt wird, wählt das Aushandlungsschema die NTLM-Authentifizierung als Fallback.

  > **Hinweis:**
  >
  > Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn mit dem Active Directory-Konto des Proxys verknüpfen. Der VDA generiert den Dienstprinzipalnamen (SPN) im Format `HTTP/<proxyURL>` beim Einrichten einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvousproxy** abgerufen wird. Wenn Sie keinen Dienstprinzipalnamen (SPN) erstellen, wird für die NTLM-Authentifizierung verwendet. In beiden Fällen wird die Identität der VDA-Maschine zur Authentifizierung verwendet.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Bei Verwendung eines SOCKS5-Proxy müssen Sie eine Ausnahme konfigurieren, damit Datenverkehr an die in den Anforderungen angegebenen Gateway Service-Adressen die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

#### Transparenter Proxy

Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist auf dem VDA keine zusätzliche Konfiguration erforderlich.

#### Nicht transparenter Proxy

Wenn Sie einen nicht transparenten Proxy in Ihrem Netzwerk verwenden, konfigurieren Sie die Einstellung Rendezvousproxykonfiguration. Wenn die Einstellung aktiviert ist, geben Sie die HTTP- oder SOCKS5-Proxyadresse oder den Pfad zur PAC-Datei an, um festzulegen, welchen Proxy vom VDA verwendet wird. Beispiel:

- Proxyadresse: `http://<URL or IP>:<port>` oder `socks5://<URL or IP>:<port>`
- PAC-Datei: `http://<URL or IP>/<path>/<filename>.pac`

Wenn Sie die PAC-Datei zum Konfigurieren des Proxys verwenden, definieren Sie den Proxy mit der Syntax, die vom Windows-HTTP-Dienst benötigt wird: `PROXY [<scheme>=]<URL or IP>:<port>`. Beispiel: `PROXY socks5=<URL or IP>:<port>`.

### Rendezvous-Validierung

Wenn alle Anforderungen erfüllt sind, überprüfen Sie folgendermaßen, ob Rendezvous verwendet wird:

1. Starten Sie PowerShell oder eine Eingabeaufforderung innerhalb der HDX-Sitzung.
2. Führen Sie `ctxsession.exe –v` aus.
3. Die verwendeten Transportprotokolle geben die Art der Verbindung an:
    - TCP-Rendezvous: **TCP - SSL - CGP - ICA**
    - EDT-Rendezvous: **UDP > DTLS > CGP > ICA**
    - Proxy über Cloud Connector: **TCP - CGP - ICA**

### Andere Überlegungen

#### Reihenfolge für Windows-Verschlüsselungssammlung

Stellen Sie für eine benutzerdefinierte Verschlüsselungssammlungsreihenfolge sicher, dass Sie die von der VDA unterstützten Verschlüsselungssammlungen aus der folgenden Liste einschließen:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Wenn die benutzerdefinierte Verschlüsselungssammlungsreihenfolge diese Verschlüsselungssammlungen nicht enthält, schlägt die Rendezvous-Verbindung fehl.

#### Zscaler Private Access

Wenn Sie Zscaler Private Access (ZPA) verwenden, wird empfohlen, Umgehungseinstellungen für den Gateway Service zu konfigurieren, um eine erhöhte Latenz und Leistungsminderungen zu vermeiden. Dazu müssen Sie Anwendungssegmente für die Gateway Service-Adressen definieren (in den Anforderungen angegeben) und sie auf "immer umgehen"einstellen. Weitere Informationen zum Konfigurieren von Anwendungssegmenten zur Umgehung von ZPA finden Sie in der Zscaler-Dokumentation.

## Rendezvous V2

May 17, 2024

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll VDAs, die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerungsebene herzustellen.

Rendezvous V2 wird für standardmäßige domänengebundene Maschinen, mit Hybrid Azure AD verbundene Maschinen, mit Azure AD verbundene Maschinen und nicht domänengebundene Maschinen unterstützt.

> **Hinweis:**
>
> Derzeit sind Bereitstellungen ohne Connector nur für *mit Azure AD verbundene* oder *nicht domänengebundene* Maschinen möglich. Maschinen mit Standard-AD-Domänenbindung und mit Hybrid Azure AD verbundene Maschinen benötigen weiterhin Cloud Connectors für die VDA-Registrierung und die Sitzungsvermittlung. Es gibt jedoch keine DNS-Anforderungen für

> die Verwendung von Rendezvous V2.
>
> Die Cloud Connector-Anforderungen für andere Funktionen, die nicht mit der VDA-Kommunikation in Zusammenhang stehen (z. B. das Verbinden mit Ihrer On-Premises-AD-Domäne, das MCS-Provisioning für On-premises-Hypervisors usw.) bleiben unverändert.

### Anforderungen

Anforderungen für die Verwendung von Rendezvous V2:

- Zugriff auf die Umgebung mit Citrix Workspace und Citrix Gateway Service.
- Steuerungsebene: Citrix DaaS
- VDA Version 2203
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix Richtlinie. Weitere Informationen finden Sie unter Richtlinieneinstellung für Rendezvous-Protokoll.
- Sitzungszuverlässigkeit muss auf den VDAs aktiviert sein
- Die VDA-Maschinen benötigen Zugriff auf:
  - `https://*.xendesktop.net` auf `TCP 443`. Wenn Sie nicht alle Unterdomänen auf diese Weise zulassen können, können Sie `https://<customer_ID>.xendesktop.net` verwenden. Hierbei ist "<customer_ID>"Ihre im Citrix Cloud-Administratorportal angezeigte Citrix Cloud-Kunden-ID.
  - `https://*.*.nssvc.net` an `TCP 443` für die Steuerverbindung mit Gateway Service.
  - `https://*.*.nssvc.net` an `TCP 443` und `UDP 443` für HDX-Sitzungen über TCP bzw. EDT.

> **Hinweis:**
>
> Wenn Sie nicht alle Unterdomänen mit `https://*.*.nssvc.net` zulassen können, verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX270584.

### Proxykonfiguration

Der VDA unterstützt die Verbindung über Proxys für Steuerungsverkehr und HDX-Sitzungsverkehr bei Verwendung von Rendezvous. Die Anforderungen und Richtlinien für beide Arten von Datenverkehr sind unterschiedlich. Überprüfen Sie sie daher sorgfältig.

### Richtlinien für Proxys für den Steuerungsverkehr

- Es werden nur HTTP-Proxys unterstützt.
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der Steuerungsdatenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder überprüft wird. Andernfalls schlägt die Verbindung fehl.
- Proxyauthentifizierung wird nicht unterstützt.

### Richtlinien für Proxys für den HDX-Datenverkehr

- HTTP- und SOCKS5-Proxys werden unterstützt.
- EDT kann nur mit SOCKS5-Proxys verwendet werden.
- Standardmäßig verwendet HDX-Datenverkehr den für den Steuerungsverkehr festgelegten Proxy. Wenn Sie einen anderen Proxy für den HDX-Datenverkehr verwenden müssen (einen anderen HTTP-Proxy oder einen SOCKS5-Proxy), verwenden Sie die Richtlinieneinstellung Rendezvous-Proxykonfiguration .
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der HDX-Datenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder überprüft wird. Andernfalls schlägt die Verbindung fehl.
- Die maschinenbasierte Authentifizierung wird nur bei Verwendung von HTTP-Proxys und AD-domänengebundener VDA-Maschinen unterstützt. Es kann die Negotiate/Kerberos- oder die NTLM-Authentifizierung verwendet werden.

  > **Hinweis:**
  >
  > Um Kerberos zu verwenden, erstellen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver und verknüpfen Sie ihn mit dem Active Directory-Konto des Proxys. Der VDA generiert den Dienstprinzipalnamen (SPN) im Format `HTTP/<proxyURL>` beim Einrichten einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung Rendezvous-Proxykonfiguration abgerufen wird. Wenn Sie keinen Dienstprinzipalnamen (SPN) erstellen, wird für die NTLM-Authentifizierung verwendet. In beiden Fällen wird die Identität der VDA-Maschine zur Authentifizierung verwendet.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Bei Verwendung eines SOCKS5-Proxy konfigurieren Sie eine Ausnahme, damit der Datenverkehr an die in den Anforderungen angegebenen Gateway Service-Adressen die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

#### Transparenter Proxy

Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist auf dem VDA keine zusätzliche Konfiguration erforderlich.

#### Nicht transparenter Proxy

Wenn Sie einen nicht transparenten Proxy in Ihrem Netzwerk verwenden, geben Sie den Proxy bei der VDA-Installation an, damit der Steuerungsverkehr die Citrix Cloud-Steuerebene erreichen kann. Machen Sie sich mit den Richtlinien für Proxys für den Steuerungsverkehr vertraut, bevor Sie mit der Installation und Konfiguration fortfahren.

Wählen Sie im VDA-Installationsassistenten auf der Seite **Zusätzliche Komponenten** die Option **Rendezvous-Proxykonfiguration**. Dadurch wird die Seite **Rendezvous-Proxykonfiguration** später im Installationsassistenten verfügbar gemacht. Geben Sie auf dieser die Proxyadresse oder den Pfad der PAC-Datei des vom VDA zu verwendenden Proxys ein. Beispiel:

- Proxyadresse: `http://<URL or IP>:<port>`
- PAC-Datei: `http://<URL or IP>/<path/<filename>.pac`

Wie unter “Richtlinien für Proxys für den HDX-Datenverkehr”erwähnt, verwendet HDX-Datenverkehr standardmäßig den bei der VDA-Installation definierten Proxy. Wenn Sie einen anderen Proxy für den HDX-Datenverkehr verwenden müssen (einen anderen HTTP-Proxy oder einen SOCKS5-Proxy), verwenden Sie die Richtlinieneinstellung Rendezvous-Proxykonfiguration . Wenn die Einstellung aktiviert ist, geben Sie die HTTP- oder SOCKS5-Proxyadresse an. Sie können auch den Pfad der PAC-Datei des vom VDA zu verwendenden Proxys angeben. Beispiel:

- Proxyadresse: `http://<URL or IP>:<port>` oder `socks5://<URL or IP>:<port>`
- PAC-Datei: `http://<URL or IP>/<path/<filename>.pac`

Wenn Sie die PAC-Datei zum Konfigurieren des Proxys verwenden, definieren Sie den Proxy mit der Syntax, die vom Windows-HTTP-Dienst benötigt wird: `PROXY [<scheme>=]<URL or IP>:<port>`. Zum Beispiel: `PROXY socks5=<URL or IP>:<port>`.

### Konfigurieren von Rendezvous

Im Folgenden werden die Schritte zum Konfigurieren von Rendezvous aufgeführt:

1. Achten Sie darauf, dass alle Anforderungen erfüllt sind.
2. Wenn Sie einen nicht transparenten HTTP-Proxy verwenden müssen, konfigurieren Sie diesen bei der VDA-Installation. Einzelheiten finden Sie im Abschnitt Proxykonfiguration.

3. Starten Sie die VDA-Maschine nach Abschluss der Installation neu.
4. Erstellen Sie eine Citrix Richtlinie oder bearbeiten Sie eine vorhandene:

    - Legen Sie die Einstellung **Rendezvous-Protokoll** auf **Zugelassen** fest.
    - Wenn Sie einen HTTP- oder SOCKS5-Proxy für den HDX-Datenverkehr konfigurieren müssen, konfigurieren Sie die Einstellung **Rendezvous-Proxykonfiguration**.
    - Stellen Sie sicher, dass die Citrix Richtlinienfilter richtig eingestellt sind. Die Richtlinie gilt für die Maschinen, für die Rendezvous aktiviert sein muss.

5. Stellen Sie sicher, dass die Citrix Richtlinie die richtige Priorität hat, damit sie keine weitere außer Kraft setzt.

> **Hinweis:**
>
> Wenn Sie VDA-Version 2308 oder älter verwenden, wird standardmäßig V1 verwendet. Weitere Informationen zur Konfiguration der zu verwendenden Version finden Sie unter Über die Registrierung verwaltete HDX-Funktionen.

#### Rendezvous-Validierung

Wenn alle Anforderungen erfüllt sind und Sie die Konfiguration vorgenommen haben, überprüfen Sie folgendermaßen, ob Rendezvous verwendet wird:

1. Öffnen Sie auf dem virtuellen Desktop eine Eingabeaufforderung oder PowerShell.
2. Führen Sie `ctxsession.exe -v` aus.
3. Die angezeigten Transportprotokolle geben die Art der Verbindung an:

    - TCP-Rendezvous: TCP - SSL - CGP - ICA
    - EDT-Rendezvous: UDP > DTLS > CGP > ICA
    - Kein Rendezvous: TCP > CGP > ICA

4. Es wird die verwendete Rendezvous-Version angezeigt.

### Andere Überlegungen

#### Reihenfolge für Windows-Verschlüsselungssammlung

Wenn die Reihenfolge der Verschlüsselungssammlungen auf den VDA-Maschinen geändert wurde, stellen Sie sicher, dass Sie die vom VDA unterstützten Verschlüsselungssammlungen einbeziehen:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Wenn die benutzerdefinierte Verschlüsselungssammlungsreihenfolge diese Verschlüsselungssammlungen nicht enthält, schlägt die Rendezvous-Verbindung fehl.

#### Zscaler Private Access

Wenn Sie Zscaler Private Access (ZPA) verwenden, wird empfohlen, Umgehungseinstellungen für den Gateway Service zu konfigurieren, um eine erhöhte Latenz und Leistungsminderungen zu vermeiden. Dazu müssen Sie Anwendungssegmente für die Gateway Service-Adressen definieren (in den Anforderungen angegeben) und sie auf "immer umgehen"einstellen. Weitere Informationen zum Konfigurieren von Anwendungssegmenten zur Umgehung von ZPA finden Sie in der Zscaler-Dokumentation.

### Bekannte Probleme

#### Im VDA 2203-Installationsprogramm darf kein Schrägstrich (/) in der Proxyadresse eingegeben werden

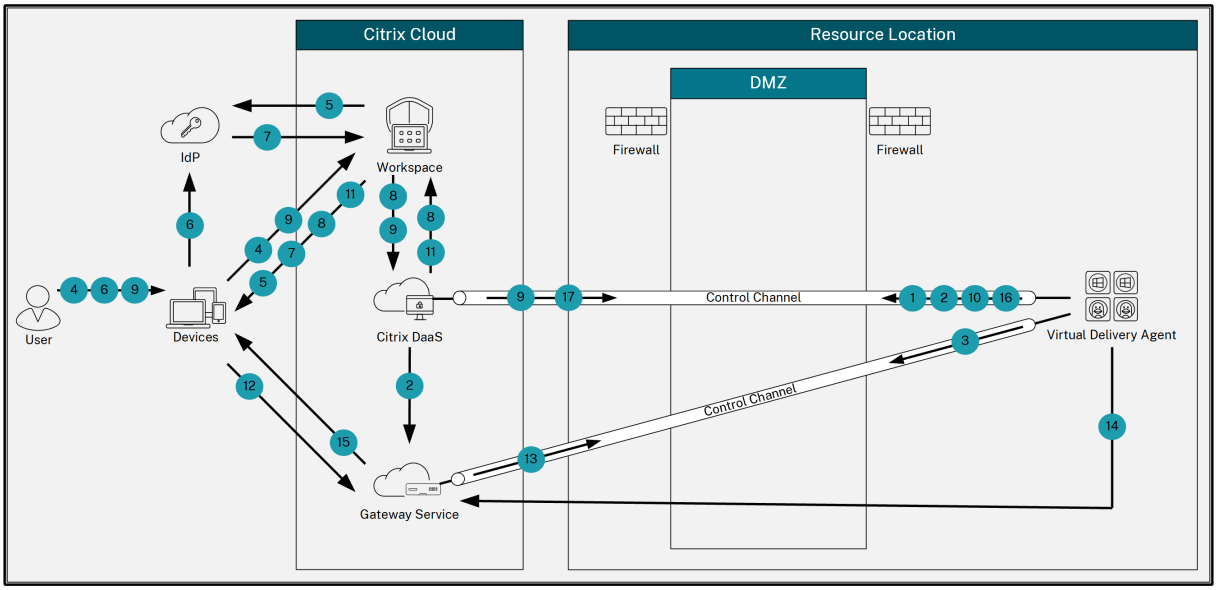
Als Workaround können Sie den Proxy in der Registrierung konfigurieren, nachdem der VDA installiert wurde:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
Value type: String
Value name: ProxySettings
Value data: Proxy address or path to pac file. For example:
    Proxy address: http://squidk.test.local:3128
    Pac file: http://file.test.com/config/proxy.pac
```

### Rendezvous-Verkehrsfluss

Das folgende Diagramm zeigt die Abfolge der Schritte zum Rendezvous-Verkehrsfluss.




1. Der VDA stellt eine WebSocket-Verbindung mit Citrix Cloud her und registriert sich.
2. Der VDA registriert sich beim Citrix Gateway Service und erhält einen dedizierten Token.
3. Der VDA stellt eine persistente Steuerungsverbindung mit Gateway Service her.
4. Der Benutzer navigiert zu Citrix Workspace.
5. Workspace wertet die Authentifizierungskonfiguration aus und leitet Benutzer zur Authentifizierung an den entsprechenden IdP weiter.
6. Der Benutzer gibt die Anmeldeinformationen ein.
7. Nach erfolgreicher Überprüfung der Benutzeranmeldeinformationen wird der Benutzer zu Workspace umgeleitet.
8. Workspace zählt Ressourcen für den Benutzer und zeigt sie an.
9. Der Benutzer wählt einen Desktop oder eine Anwendung in Workspace aus. Workspace sendet die Anfrage an Citrix DaaS, das die Verbindung vermittelt und den VDA anweist, sich auf die Sitzung vorzubereiten.
10. Der VDA reagiert mit der Rendezvous-Funktion und seiner Identität.
11. Citrix DaaS generiert ein Startticket und sendet es über Workspace an das Benutzergerät.
12. Der Endpunkt des Benutzers stellt eine Verbindung zu Gateway Service her und stellt das Startticket zur Authentifizierung und Identifizierung der Ressource bereit, mit der eine Verbindung hergestellt werden soll.
13. Gateway Service sendet die Verbindungsinformationen an den VDA.
14. Der VDA stellt für die Sitzung eine direkte Verbindung mit Gateway Service her.
15. Gateway Service stellt die Verbindung zwischen dem Endpunkt und dem VDA her.
16. Der VDA überprüft die Lizenzierung für die Sitzung.
17. Citrix DaaS sendet die entsprechenden Richtlinien an den VDA.

# HDX Direct (Preview)

June 12, 2024

Beim Zugriff auf von Citrix bereitgestellte Ressourcen ermöglicht HDX Direct sowohl internen als auch externen Clientgeräten, eine sichere direkte Verbindung mit dem Sitzungshost herzustellen, sofern eine direkte Kommunikation möglich ist.

> **Wichtig:**
>
> HDX Direct ist derzeit in der Technical Preview. Dieses Feature wird ohne Unterstützung bereitgestellt und noch nicht für den Einsatz in Produktionsumgebungen empfohlen. Verwenden Sie dieses Formular, um Feedback einzureichen oder Probleme zu melden.

## Systemanforderungen

Für die Verwendung von HDX Direct gelten die folgenden Systemvoraussetzungen:

- Steuerungsebene
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 oder höher
- Virtual Delivery Agent (VDA)
  - Windows: Version 2402 oder höher
- Workspace-App
  - Windows: Version 2402 oder höher
- Zugriffsebene
  - Citrix Workspace mit Citrix Gateway Service
  - Citrix Workspace mit NetScaler Gateway
- Sonstiges
  - Adaptive Transport muss für externe Direktverbindungen aktiviert sein

## Netzwerkanforderungen

Für die Verwendung von HDX Direct gelten die folgenden Netzwerkvoraussetzungen.

### Sitzungshosts

Wenn Ihre Sitzungshosts über eine Firewall wie die Windows Defender-Firewall verfügen, müssen Sie den folgenden eingehenden Verkehr für interne Verbindungen zulassen.

| Beschreibung | Quelle | Protokoll | Port |
|---|---|---|---|
| Direkte interne Verbindung | Client | TCP | 443 |
| Direkte interne Verbindung | Client | UDP | 443 |

> Hinweis:
>
> Das VDA-Installationsprogramm fügt der Windows Defender-Firewall die entsprechenden Regeln für eingehenden Datenverkehr hinzu. Wenn Sie eine andere Firewall verwenden, müssen Sie die obigen Regeln hinzufügen.

### Clientnetzwerk

In der folgenden Tabelle wird das Clientnetzwerk für interne und externe Benutzer beschrieben.

#### Interne Benutzer

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| Direkte interne Verbindung | TCP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |
| Direkte interne Verbindung | UDP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |

#### Externe Benutzer

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| STUN (nur für externe Benutzer) | UDP | Clientnetzwerk | 1024–65535 | Internet (siehe Hinweis unten) | 3478, 19302 |
| Externe Benutzerverbindung | UDP | Clientnetzwerk | 1024–65535 | Öffentliche IP-Adresse des Datencenters | 1024–65535 |

**Datencenternetzwerk**

In der folgenden Tabelle wird das Datencenternetzwerk für interne und externe Benutzer beschrieben.

**Interne Benutzer**

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| Direkte interne Verbindung | TCP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |
| Direkte interne Verbindung | UDP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |

**Externe Benutzer**

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| STUN (nur für externe Benutzer) | UDP | VDA-Netzwerk | 1024–65535 | Internet (siehe Hinweis unten) | 3478, 19302 |
| Externe Benutzerverbindung | UDP | DMZ / Internes Netzwerk | 1024–65535 | VDA-Netzwerk | 55000–55250 |
| Externe Benutzerverbindung | UDP | VDA-Netzwerk | 55000–55250 | Öffentliche IP des Clients | 1024–65535 |

> **Hinweis:**
>
> Sowohl der VDA als auch die Workspace-App versuchen, STUN-Anforderungen in derselben Reihenfolge an die folgenden Server zu senden:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> Wenn Sie den Standardportbereich für externe Benutzerverbindungen mithilfe der Richtlinieneinstellung **HDX Direct-Portbereich** ändern, müssen die entsprechenden Firewallregeln Ihrem benutzerdefinierten Portbereich entsprechen.

### Konfiguration

HDX Direct ist standardmäßig deaktiviert. Sie können das Feature mithilfe der **HDX Direct**-Einstellung der Citrix Richtlinie konfigurieren.

- **HDX Direct**: Zum Aktivieren oder Deaktivieren eines Features.
- **HDX Direct-Modus**: Legt fest, ob **HDX Direct** nur für interne Clients oder sowohl für interne als auch für externe Clients verfügbar ist.
- **HDX Direct-Portbereich**: Definiert den Portbereich, den der VDA für Verbindungen von externen Clients verwendet.

### Überlegungen

Bei der Verwendung von HDX Direct ist Folgendes zu berücksichtigen:

- HDX Direct für externe Benutzer ist nur mit EDT (UDP) als Transportprotokoll verfügbar. Daher muss **Adaptiver Transport** aktiviert sein.
- Wenn Sie **HDX Insight** verwenden, beachten Sie, dass die Verwendung von **HDX Direct** die HDX Insight-Datenerfassung verhindert, weil die Sitzung nicht mehr über NetScaler Gateway als Proxy geleitet würde.
- Wenn Sie nicht persistente Maschinen für Ihre virtuellen Apps und Desktops verwenden, empfiehlt Citrix, **HDX Direct** auf den Sitzungshosts statt im Master-/Vorlagenimage zu aktivieren, damit jede Maschine ihre eigenen Zertifikate generiert.
- Die Verwendung Ihrer eigenen Zertifikate mit HDX Direct wird derzeit nicht unterstützt.

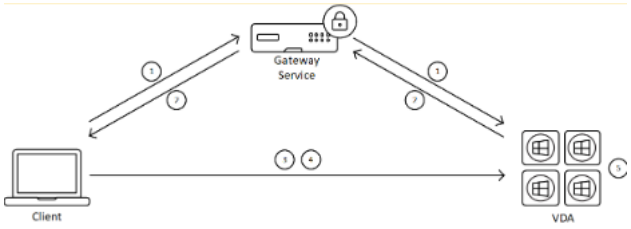
 

## Funktionsweise

HDX Direct ermöglicht es Clients, eine direkte Verbindung zum Sitzungshost herzustellen, wenn eine direkte Kommunikation verfügbar ist. Wenn direkte Verbindungen mit HDX Direct hergestellt werden, werden selbstsignierte Zertifikate verwendet, um die direkte Verbindung mit Verschlüsselung auf Netzwerkebene (TLS/DTLS) zu sichern.

### Interne Benutzer

Das folgende Diagramm zeigt den Überblick über den HDX Direct-Verbindungsprozess interner Benutzer.



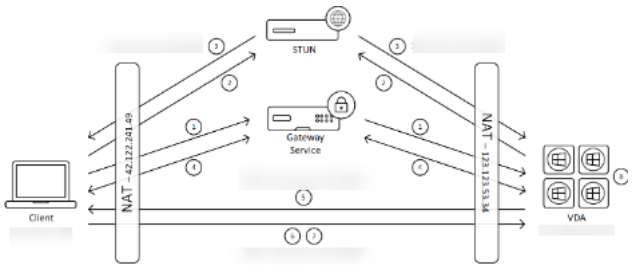

1. Der Client richtet eine HDX-Sitzung über den Gateway Service ein.
2. Nach einer erfolgreichen Verbindung sendet der VDA den FQDN der VDA-Maschine, eine Liste ihrer IP-Adressen und das Zertifikat der VDA-Maschine über die HDX-Verbindung an den Client.
3. Der Client überprüft die IP-Adressen, um festzustellen, ob er den VDA direkt erreichen kann.
4. Wenn der Client den VDA mit einer der gemeinsam genutzten IP-Adressen direkt erreichen kann, stellt der Client eine direkte Verbindung mit dem VDA her, die mit (D) TLS über ein Zertifikat gesichert ist, das dem in Schritt (2) ausgetauschten Zertifikat entspricht.
5. Sobald die direkte Verbindung hergestellt ist, wird die Sitzung an sie übertragen und die Verbindung zu Gateway Service wird beendet.

> **Hinweis:**
>
> Nach dem Herstellen der Verbindung in Schritt 2 oben ist die Sitzung aktiv. Die nachfolgenden Schritte verzögern oder beeinträchtigen nicht die Fähigkeit des Benutzers, die virtuelle Anwendung oder den Desktop zu verwenden. Wenn einer der nachfolgenden Schritte fehlschlägt, wird die Verbindung über das Gateway aufrechterhalten, ohne die Benutzersitzung zu unterbrechen.

### Externe Benutzer

Das folgende Diagramm zeigt den Überblick über den HDX Direct-Verbindungsprozess für externe Benutzer:




1. Der Client richtet eine HDX-Sitzung über den Gateway Service ein.
2. Nach einer erfolgreichen Verbindung senden sowohl der Client als auch der VDA eine STUN-Anforderung, um ihre öffentlichen IP-Adressen und Ports zu ermitteln.
3. Der STUN-Server antwortet dem Client und dem VDA mit ihren entsprechenden öffentlichen IP-Adressen und Ports.
4. Über die HDX-Verbindung tauschen der Client und der VDA ihre öffentlichen IP-Adressen und UDP-Ports aus und der VDA sendet sein Zertifikat an den Client.
5. Der VDA sendet UDP-Pakete an die öffentliche IP-Adresse und den UDP-Port des Clients. Der Client sendet UDP-Pakete an die öffentliche IP-Adresse und den UDP-Port des VDA.
6. Nach Erhalt einer Nachricht vom VDA antwortet der Client mit einer sicheren Verbindungsanforderung.
7. Während des DTLS-Handshakes überprüft der Client, ob das Zertifikat mit dem in Schritt (4) ausgetauschten Zertifikat übereinstimmt. Nach der Validierung sendet der Client sein Autorisierungstoken. Eine sichere Direktverbindung ist jetzt hergestellt.
8. Sobald die direkte Verbindung hergestellt ist, wird die Sitzung an sie übertragen und die Verbindung zu Gateway Service wird beendet.

> **Hinweis:**
>
> Nach dem Herstellen der Verbindung in Schritt 2 oben ist die Sitzung aktiv. Die nachfolgenden Schritte verzögern oder beeinträchtigen nicht die Fähigkeit des Benutzers, die virtuelle Anwendung oder den Desktop zu verwenden. Wenn einer der nachfolgenden Schritte fehlschlägt, wird die Verbindung über das Gateway aufrechterhalten, ohne die Benutzersitzung zu unterbrechen.

## Zertifikatverwaltung

### Sitzungshost

Die folgenden beiden Dienste auf der VDA-Maschine übernehmen die Erstellung und Verwaltung von Zertifikaten. Beide sind so eingerichtet, dass sie beim Maschinenstart automatisch ausgeführt werden:

- Citrix ClxMtp Service: verantwortlich für die Generierung und Rotation von ZS-Zertifikaten.

- Citrix Certificate Manager Service: verantwortlich für die Generierung und Verwaltung des selbstsignierten Stamm-ZS-Zertifikats und der Maschinenzertifikate.

Die folgenden Schritte veranschaulichen den Prozess der Zertifikatsverwaltung:

1. Die Dienste werden beim Start der Maschine gestartet.
2. `Citrix ClxMtp Service` erstellt Schlüssel, falls noch keiner erstellt wurde.
3. Citrix Certificate Manager Service überprüft, ob **HDX Direct** aktiviert ist. Andernfalls stoppt der Dienst selbsttätig.
4. Wenn **HDX Direct** aktiviert ist, prüft Citrix Certificate Manager Service, ob ein selbstsigniertes Stamm-ZS-Zertifikat vorhanden ist. Ist dies nicht der Fall, wird ein selbstsigniertes Stammzertifikat erstellt.
5. Sobald ein Stamm-ZS-Zertifikat verfügbar ist, prüft Citrix Certificate Manager Service, ob ein selbstsigniertes Maschinenzertifikat vorhanden ist. Ist dies nicht der Fall, generiert der Dienst Schlüssel und erstellt mithilfe des Maschinen-FQDN ein Zertifikat.
6. Ist ein von Citrix Certificate Manager Service erstelltes Maschinenzertifikat vorhanden und der Antragstellername stimmt nicht mit dem Maschinen-FQDN überein, wird ein neues Zertifikat generiert.

> **Hinweis:**
>
> Citrix Certificate Manager Service generiert RSA-Zertifikate, die 2048-Bit-Schlüssel nutzen.

#### Clientgerät

Damit eine sichere **HDX Direct**-Verbindung hergestellt werden kann, muss der Client den Zertifikaten vertrauen, die zum Schutz der Sitzung verwendet wurden. Um dies zu ermöglichen, erhält der Client das ZS-Zertifikat für die Sitzung über die ICA-Datei (von Workspace bereitgestellt), sodass es nicht erforderlich ist, ZS-Zertifikate an die Zertifikatsspeicher der Clientgeräte zu verteilen.

## NAT-Kompatibilität

June 12, 2024

Um eine direkte Verbindung zwischen einem externen Benutzergerät und dem Sitzungshost herzustellen, nutzt HDX Direct Hole Punching für NAT-Traversal und STUN, um den Austausch der öffentlichen IP-Adressen und Portzuordnungen für das Clientgerät und den Sitzungshost zu erleichtern. Dies ähnelt der Funktionsweise von VoIP-, Unified Communications- und P2P-Lösungen.

Solange Firewalls und andere Netzwerkkomponenten so konfiguriert sind, dass sie den UDP-Verkehr für die STUN-Anforderungen und die HDX-Sitzungen zulassen, wird erwartet, dass HDX Direct für

externe Benutzer funktioniert. Es gibt jedoch bestimmte Szenarien, in denen die NAT-Typen der Benutzer- und Sitzungshostnetzwerke zu einer inkompatiblen Kombination führen, wodurch HDX Direct ausfällt.

### Validierungen

Sie können den NAT-Typ auf dem Client und dem Sitzungshost validieren, indem Sie das STUN-Clienthilfsprogramm von STUNTMAN verwenden:

1. Laden Sie das entsprechende Paket für die Zielplattform von stunprotocol.org herunter und extrahieren Sie den Inhalt.
2. Öffnen Sie eine Terminal-Eingabeaufforderung und navigieren Sie zu dem Verzeichnis, in das der Inhalt extrahiert wurde.
3. Führen Sie den folgenden Befehl aus:
   `.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. Notieren Sie sich die Ausgabe.

Wenn die Bindungs- und Verhaltenstests erfolgreich sind, melden sowohl der **Bindungstest** als auch der **Verhaltenstest** den Erfolg und ein NAT-Verhalten wird angegeben:


Wenn die Tests fehlschlagen, melden sowohl der **Bindungstest** als auch der **Verhaltenstest** den Fehler.


Anhand der folgenden Tabelle können Sie ausgehend von den Testergebnissen des Clients und des Sitzungshosts ermitteln, ob HDX Direct für externe Benutzer voraussichtlich funktioniert:

| Clientgerät | Sitzungshost | Wird es voraussichtlich funktionieren? |
|---|---|---|
| Endpunktunabhängige Zuordnung | Endpunktunabhängige Zuordnung | Ja |
| Endpunktunabhängige Zuordnung | Endpunktabhängige Zuordnung | Ja |
| Endpunktabhängige Zuordnung | Endpunktunabhängige Zuordnung | Ja |

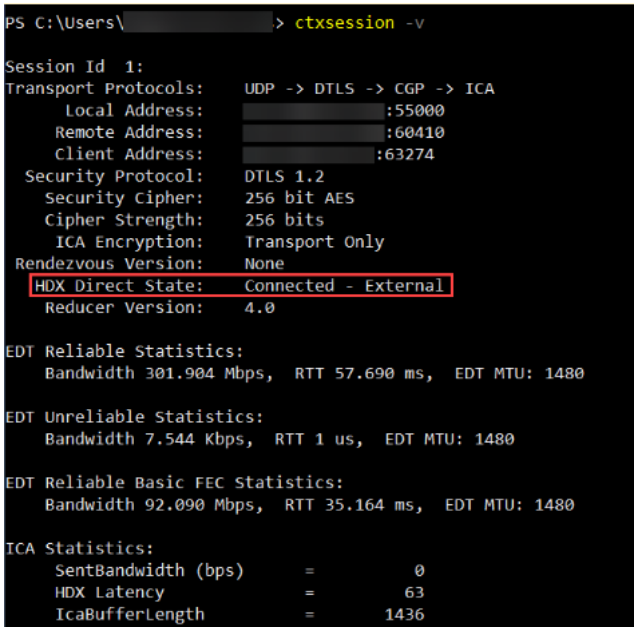
| Clientgerät | Sitzungshost | Wird es voraussichtlich funktionieren? |
|---|---|---|
| Endpunktabhängige Zuordnung | Endpunktabhängige Zuordnung | Nein |
| Adress- und portabhängige Zuordnung | Beliebiger NAT-Typ | Nein |
| Beliebiger NAT-Typ | Adress- und portabhängige Zuordnung | Nein |
| Fehlschlag | Beliebiger NAT-Typ | Nein |
| Beliebiger NAT-Typ | Fehlschlag | Nein |
| Fehlschlag | Fehlschlag | Nein |

## Problembehandlung

January 25, 2024

Verwenden Sie das Hilfsprogramm `CtxSession.exe` auf der VDA-Maschine, um zu überprüfen, ob **HDX Direct** eine direkte Verbindung hergestellt hat.

Um das Hilfsprogramm `CtxSession.exe` zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen Sie `ctxsession.exe -v` aus. Wenn die **HDX Direct**-Verbindung erfolgreich hergestellt wurde, ist der **HDX Direct-Status** `Connected`.



Sie können auch in den Ereignisprotokollen des Sitzungshosts nachlesen, ob die HDX Direct-Verbindung erfolgreich hergestellt wurde oder fehlgeschlagen ist. Einzelheiten finden Sie im Abschnitt **Ereignisprotokolle**.

> Hinweis:
>
> Je nach Umgebung und Anzahl der IP-Adressen, die den Sitzungshosts zur Verfügung stehen, kann es bis zu 5 Minuten dauern, bis die HDX Direct-Verbindung hergestellt ist.

### Wenn HDX Direct keine direkte Verbindung herstellen kann

Wenn HDX Direct keine direkte Verbindung herstellen kann, überprüfen Sie Folgendes:

1. Überprüfen Sie, ob die verwendete VDA-Version und die Workspace-App-Version das Feature gemäß den Systemanforderungen unterstützen.
2. Vergewissern Sie sich, dass auf den VDA eine Richtlinie angewendet wurde, die HDX Direct aktiviert, und keine anderen Richtlinien mit höherer Priorität vorhanden sind, die das Feature deaktivieren.
3. Vergewissern Sie sich, dass auf den VDA eine Richtlinie angewendet wurde, die den gewünschten HDX Direct-Modus festlegt, und keine anderen Richtlinien mit höherer Priorität die Konfiguration überschreiben.
4. Überprüfen Sie, ob der Citrix ClxMtp-Dienst auf dem Sitzungshost ausgeführt wird.
5. Überprüfen Sie, dass der Citrix Certificate Manager Service auf dem Sitzungshost ausgeführt wird. Wenn er nicht läuft, versuchen Sie, ihn manuell zu starten. Der Dienst wird automatisch beendet, wenn HDX Direct deaktiviert ist.
6. Prüfen Sie, ob der Sitzungshost über ein selbstsigniertes Stamm-ZS-Zertifikat verfügt:

    a) Ausgestellt an: `CA-<hostname>` (Zum Beispiel CA-FTLW11-001)
    b) Ausgestellt von: `CA-<hostname>` (Zum Beispiel CA-FTLW11-001)
    c) Angaben zum Aussteller: Die Organisation ist Citrix Systems, Inc.

7. Prüfen Sie, ob der Sitzungshost über ein selbstsigniertes Serverzertifikat verfügt:

    a) Ausgestellt an: `<host FQDN>` (Zum Beispiel FTLW11-001.ctxlab.net)
    b) Ausgestellt von: `CA-<hostname>` (Zum Beispiel CA-FTLW11-001)
    c) Angaben zum Aussteller: Die Organisation ist Citrix Systems, Inc.

8. Wenn die Zertifikate fehlen, wenden Sie sich an den technischen Support von Citrix.
9. Wenn die Zertifikate vorhanden sind:

    a) Stoppen Sie den Citrix Certificate Manager Service auf dem Sitzungshost.
    b) Löschen Sie sowohl das selbstsignierte Stamm-ZS-Zertifikat als auch das selbstsignierte Serverzertifikat.

c) Starten Sie den Citrix Certificate Manager Service auf dem Sitzungshost. Der Dienst erstellt neue Zertifikate, sobald er gestartet wird.

10. Für interne Benutzer:

a) Achten Sie darauf, dass die Firewall des Sitzungshosts den eingehenden Verkehr auf UDP 443 oder TCP 443 für HDX über EDT bzw. HDX über TCP nicht blockiert.
b) Achten Sie darauf, dass Ihre Netzwerkfirewall den Verkehr auf UDP 443 und TCP 443 zwischen dem Netzwerk Ihrer Kunden und dem Netzwerk der Sitzungshosts nicht blockiert.

11. Für externe Nutzer:

a) Überprüfen Sie den NAT-Typ für den Client und den Sitzungshost und stellen Sie sicher, dass die Kombination voraussichtlich funktioniert. Einzelheiten finden Sie im Abschnitt NAT-Kompatibilität.
b) Wenn der NAT-Test entweder auf dem Client oder auf dem Sitzungshost fehlschlägt:
   i. Wenn auf dem System eine Firewall läuft, stellen Sie sicher, dass sie den ausgehenden Verkehr auf UDP 3478 nicht blockiert.
   ii. Stellen Sie sicher, dass Ihre Netzwerkfirewalls den ausgehenden Verkehr auf UDP 3478 nicht blockieren.
   iii. Stellen Sie sicher, dass die Firewalls die Antwort des STUN-Servers nicht blockieren.
c) Stellen Sie sicher, dass für Ihre Netzwerkfirewalls die entsprechenden Regeln konfiguriert sind, um den gesamten erforderlichen Datenverkehr zuzulassen. Einzelheiten finden Sie unter Netzwerkanforderungen.
d) Wenn Sie den Standardportbereich mithilfe der Richtlineneinstellung "HDX Direct-Portbereich"ändern, achten Sie darauf, dass Ihre Firewallregeln für den benutzerdefinierten Portbereich festgelegt sind.

### Ereignisprotokolle

Die folgenden Ereignisse werden im Ereignisprotokoll der VDA-Maschine protokolliert:

| Protokollierung | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| Anwendungs- und Dienstprotokolle > Citrix-HostCore-HDX Direct/Operational | 1 | HDX Direct | Informationen | HDX Direct-Verbindung für internen Benutzer <username> hergestellt. |

| Protokollierung | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| Anwendungs- und Dienstprotokolle > Citrix-HostCore-HDX Direct/Operational | 2 | HDX Direct | Informationen | HDX Direct-Verbindung für externen Benutzer <username> hergestellt. |
| Anwendungs- und Dienstprotokolle > Citrix-HostCore-HDX Direct/Operational | 3 | HDX Direct | Informationen | Die HDX Direct-Verbindung für den Benutzer <username> ist fehlgeschlagen. |

### Bekannte Probleme

HDX Direct funktioniert möglicherweise nicht mehr, nachdem ein direktes Upgrade des VDA auf einer Maschine durchgeführt wurde, auf der **HDX Direct** bereits aktiviert ist.
Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Stoppen Sie den Citrix Certificate Manager Service auf dem Sitzungshost.
2. Löschen Sie das selbstsignierte Stamm-ZS-Zertifikat und das selbstsignierte Serverzertifikat.
3. Öffnen Sie die Registrierung.
4. Löschen Sie den Schlüssel `HKLM\Software\Citrix\HDX-Direct`.
5. Gehen Sie zu `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Setzen Sie den **SSLEnabled**-Wert auf `0`.
7. Löschen Sie den Inhalt des **SSLThumbprint**-Werts.
8. Starten Sie den **Citrix Certificate Manager Service**.

## Secure HDX (Preview)

June 12, 2024

Secure HDX ist eine ALE-Lösung (Application Level Encryption), die verhindert, dass Netzwerkelemente im Datenverkehrspfad den HDX-Verkehr überprüfen können. Dazu wird echte Ende-zu-Ende-Verschlüsselung (E2EE) auf Anwendungsebene zwischen der Citrix Workspace-App (Client) und dem VDA (Sitzungshost) mithilfe der AES-256-GCM-Verschlüsselung bereitgestellt.

> **Wichtig:**
>
> Secure HDX befindet sich derzeit in der Previewversion. Dieses Feature wird ohne Unterstützung bereitgestellt und noch nicht für den Einsatz in Produktionsumgebungen empfohlen. Verwenden Sie dieses Formular, um Feedback einzureichen oder Probleme zu melden.

### Systemanforderungen

Die folgende Liste enthält die Systemanforderungen für die Verwendung von Secure HDX.

- Steuerungsebene
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 oder höher
- Virtual Delivery Agent (VDA)
  - Windows: Version 2402 oder höher
- Workspace-App
  - Windows: Version 2402 oder höher
- Zugriffsebene
  - Citrix Workspace
  - Citrix StoreFront 2402 oder höher

### Konfiguration

Secure HDX ist standardmäßig deaktiviert. Sie können das Feature mit der Secure HDX-Einstellung der Citrix Richtlinie konfigurieren:

**Secure HDX**: Definiert, ob das Feature für alle Sitzungen, nur für direkte Verbindungen, aktiviert oder deaktiviert werden soll.

### Überlegungen

Im Folgenden finden Sie Überlegungen zur Verwendung von Secure HDX:

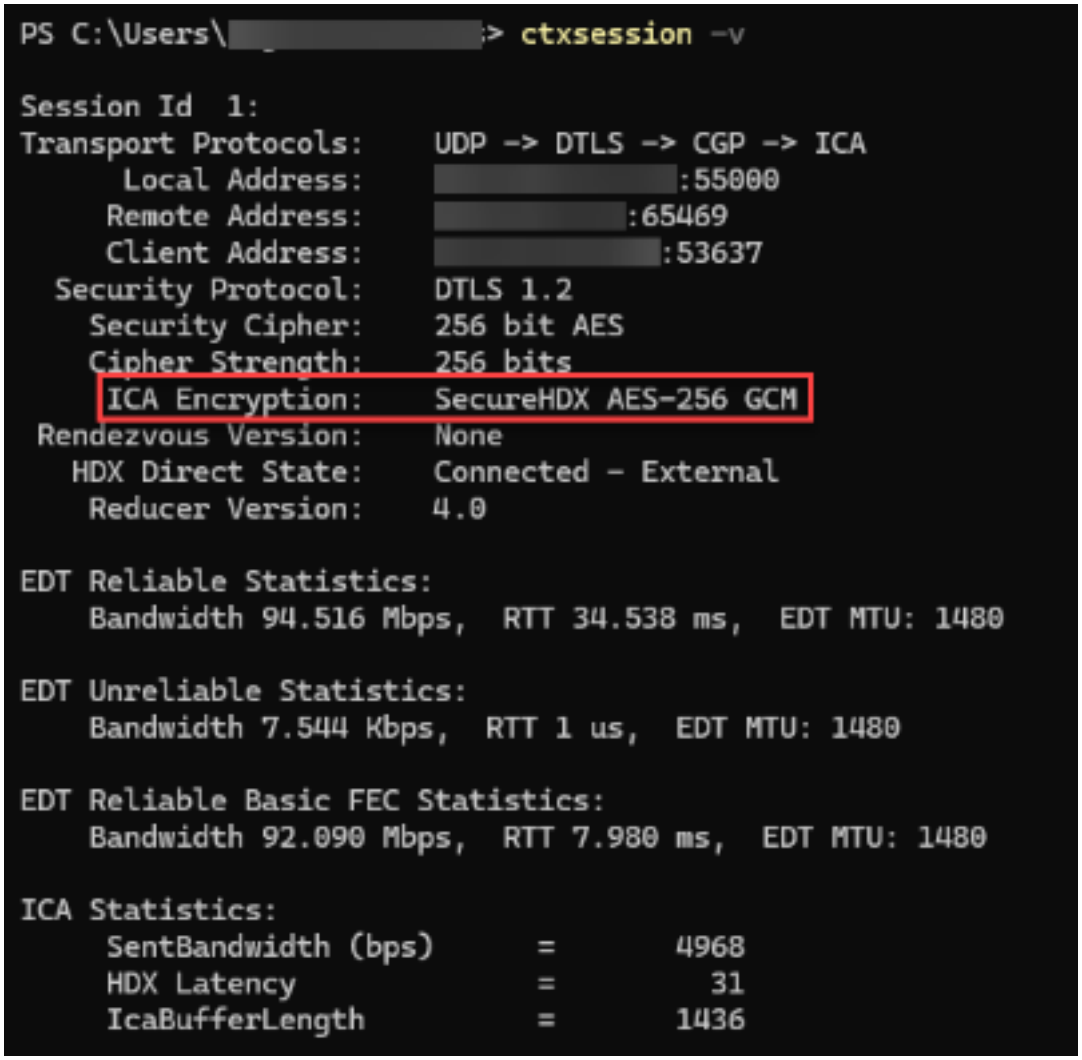
- Wenn ein Benutzer versucht, mit einem Client, der dieses Feature nicht unterstützt, eine Verbindung zu einem Sitzungshost herzustellen, bei dem Secure HDX aktiviert ist, wird die Verbindung verweigert.
- Wenn Sie HDX Insight verwenden, beachten Sie, dass die Verwendung von Secure HDX die HDX Insight-Datenerfassung verhindert, da NetScaler den verschlüsselten HDX-Verkehr nicht überprüfen kann. Wenn Sie HDX Insight verwenden müssen, können Sie Secure HDX so einrichten, dass es nur für direkte Verbindungen aktiviert wird.
- Servicekontinuität wird derzeit mit Secure HDX nicht unterstützt. Wenn Servicekontinuität in Ihrer Citrix Cloud-Umgebung aktiviert ist, können Sie bei einem Ausfall des Clouddienstes möglicherweise keine Verbindung zu Sitzungshosts herstellen, auf denen Secure HDX aktiviert ist.
- Wenn Sie SmartControl verwenden, beachten Sie, dass die Verwendung von Secure HDX verhindert, dass SmartControl funktioniert, da der NetScaler den verschlüsselten HDX-Verkehr nicht überprüfen kann. Wenn Sie SmartControl verwenden müssen, können Sie Secure HDX so einrichten, dass es nur für direkte Verbindungen aktiviert wird.
- Multistream-ICA wird nicht unterstützt, wenn Secure HDX aktiviert ist.
- Bei Verwendung von Drittanbieterlösungen, die auf der Überprüfung des HDX-Datenverkehrs basieren, funktionieren diese nicht mehr, wenn Sie Secure HDX aktivieren, da der HDX-Verkehr verschlüsselt ist.

### Problembehandlung

Um zu bestätigen, dass Secure HDX aktiv ist, können Sie das Hilfsprogramm `ctxsession.exe` auf der VDA-Maschine verwenden.

Um das Hilfsprogramm `CtxSession.exe` zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen `ctxsession.exe -v` aus. Wenn Secure HDX verwendet wird, zeigt die ICA-Verschlüsselung `SecureHDX AES-256 GCM` an.




**Wenn Secure HDX in der Sitzung nicht aktiviert wird**

- Stellen Sie sicher, dass die verwendete VDA-Version das Feature gemäß den Systemanforderungen unterstützt.
- Vergewissern Sie sich, dass auf den VDA eine Richtlinie angewendet wurde, die HDX Direct aktiviert, und keine anderen Richtlinien mit höherer Priorität vorhanden sind, die das Feature deaktivieren.
- Wenn das Clientgerät eine Verbindung über NetScaler Gateway oder Gateway Service herstellt, stellen Sie sicher, dass Secure HDX nicht auf "Nur direkte Verbindungen"eingestellt ist.
- Wenn der Sitzungshost bereits lief, als Sie Secure HDX konfiguriert haben, starten Sie den Computer neu, um sicherzustellen, dass die Änderungen wirksam werden.

# Positivliste für virtuelle Kanäle

May 17, 2024

Die Positivliste für virtuelle Kanäle ist ein Feature, mit dem Sie steuern können, welche virtuellen Kanäle, die nicht von Citrix stammen, in Ihrer Umgebung zulässig sind. Die Positivliste für virtuelle Kanäle ist standardmäßig aktiviert. Daher dürfen in Sitzungen von Citrix Virtual Apps and Desktops nur virtuelle Citrix Kanäle geöffnet werden. Ist die Verwendung benutzerdefinierter virtueller Kanäle erforderlich (eigener oder derer eines Dritten), müssen diese der Positivliste hinzugefügt werden.

## Konfiguration

Die Positivliste für virtuelle Kanäle ist standardmäßig deaktiviert. Sie können dieses Feature mithilfe der folgenden Einstellungen in der Citrix-Richtlinie konfigurieren:

- **Positivliste für virtuelle Kanäle**: um die Funktion zu aktivieren oder zu deaktivieren und virtuelle Kanäle zur Liste hinzuzufügen.
- **Protokolldrosselung für virtuelle Kanäle –Positivliste**: legt den Einschränkungszeitraum für die Protokollierung von Listenereignissen für virtuelle Kanäle fest.
- **Positivliste für die Protokollierung**: legt die Protokollierungsstufe für die Positivliste virtueller Kanäle fest.

## Hinzufügen virtueller Kanäle zur Positivliste

Sie benötigen die folgenden Informationen, um einen virtuellen Kanal zur Positivliste hinzuzufügen, benötigen:

1. Den Namen des virtuellen Kanals gemäß Definition im Code (bis zu sieben Zeichen lang). Beispiel: `CTXCVC1`.
2. Die Pfade zu den Prozessen, die den virtuellen Kanal auf der VDA-Maschine öffnen. Beispiel: `C:\Program Files\Application\run.exe`.

Wenn Sie die erforderlichen Informationen zur Hand haben, müssen Sie den virtuellen Kanal über die Richtlinieneinstellung für Positivliste virtueller Kanäle der Positivliste hinzufügen. Zum Eintragen eines virtuellen Kanals in die Liste geben Sie den Namen des virtuellen Kanals gefolgt von einem Komma und dem Pfad zu dem Prozess ein, der auf den virtuellen Kanal zugreift. Wenn es mehrere Prozesse gibt, können Sie diese Prozesse hinzufügen, indem Sie sie durch Kommas trennen.

#### Für einzelne Prozesse

Im Fall der o. g. Beispiele würden Sie der Liste den folgenden Eintrag hinzufügen:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

#### Für mehrere Prozesse

Im Fall mehrerer Prozesse fügen Sie den folgenden Eintrag hinzu:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

#### Platzhalter verwenden

Die Verwendung von Platzhaltern (*) wird unterstützt. Sie können Platzhalter verwenden, wenn sich die Namen von Verzeichnissen oder ausführbaren Dateien entsprechend der Version der Anwendung ändern oder wenn die Drittanbieterkomponente in den Benutzerprofilen installiert ist.

Sie können Platzhalter in den folgenden Szenarien verwenden:

- Um den vollständigen Verzeichnisnamen zu ersetzen.
  Beispiel: `C:\Program Files\Application\*\run1.exe`
- Um einen Teil des Verzeichnisnamens zu ersetzen.
  Beispiel: `C:\Program Files\Application\v*\run1.exe`
- Um den Namen der ausführbaren Datei zu ersetzen.
  Beispiel: `C:\Program Files\Application\v1.2\*.exe`
- Um einen Teil des Namens der ausführbaren Datei zu ersetzen.
  Beispiel: `C:\Program Files\Application\v1.2\run*.exe`

Es gelten die folgenden Einschränkungen:

- Der Platzhalter kann nur als Ersatz für ein einzelnes Verzeichnis verwendet werden. Beispiel: Die ausführbare Datei befindet sich in `C:\Program Files\Application\v1.2\run1.exe`
  - Zulässig: `C:\Program Files\Application\*\run1.exe`
  - Nicht zulässig: `C:\Program Files\*\run1.exe`
- Die Einträge müssen die Dateinamenserweiterung enthalten.
  - Zulässig: `C:\Program Files\Application\v1.2\*.exe`
  - Nicht zulässig: `C:\Program Files\Application\v1.2\*`
- Alle Pfade müssen lokale Pfade sein.

> **Hinweis:**
>
> - Netzwerkpfade sind nicht zulässig.
> - Wildcard-Unterstützung ist ab Citrix Virtual Apps and Desktops 2206 verfügbar.
> - Wildcard-Unterstützung ist in Citrix Virtual Apps and Desktops 2203 LTSR ab CU2 verfügbar.

#### Systemumgebungsvariablen verwenden

Sie können Systemumgebungsvariablen verwenden, um die Definition der vertrauenswürdigen Prozesse in Ihrer Positivliste zu vereinfachen. Sie können jede der vorbereiteten Variablen wie, `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` und `%systemroot%`.

Sie können auch benutzerdefinierte Umgebungsvariablen verwenden, sofern sie auf Systemebene definiert sind.

Die folgenden Beispiele zeigen sofort einsatzbereite Umgebungsvariablen:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

Das folgende Beispiel zeigt eine benutzerdefinierte Systemumgebungsvariable:

- Name der benutzerdefinierten Variablen: `app`
- Wert der benutzerdefinierten Variablen: `%programfiles%\Application\`
- Eintrag in Positivliste: `CTXCVC1,%app%\run.exe`

> **Hinweis:**
>
> Benutzerumgebungsvariablen werden nicht unterstützt.
>
> Die Unterstützung von Umgebungsvariablen ist ab Version 2209 von Citrix Virtual Apps and Desktops verfügbar.

### Namen und Prozesse virtueller Kanäle erhalten

Die einfachste Art und Weise, den Namen eines virtuellen Kanals und den Prozess, der ihn auf der VDA-Maschine öffnet, in Erfahrung zu bringen, ist den Entwickler oder Drittanbieter des Kanals zu fragen.

Alternativ können Sie diese Informationen erhalten, indem Sie die Protokolle des Features anwenden und die folgenden Schritte einhalten:

1. Sobald die Client- und Serverkomponenten des benutzerdefinierten virtuellen Kanals bereit sind, starten Sie eine virtuelle Anwendung oder einen virtuellen Desktop.

2. Suchen Sie im Systemereignisprotokoll der VDA-Maschine den Namen des benutzerdefinierten virtuellen Kanals und den Prozess, der ihn zu öffnen versucht: Weitere Informationen zu verfügbaren Ereignissen finden Sie unter Ereignisprotokolle.
3. Melden Sie sich von der Sitzung ab.
4. Fügen Sie in der Richtlinieneinstellung für die Positivliste virtueller Kanäle einen Eintrag für den gefundenen virtuellen Kanal und den Prozess hinzu.
5. Starten Sie die Maschine neu.
6. Sobald der VDA registriert ist, führen Sie die virtuelle Anwendung oder den virtuellen Desktop aus, um zu überprüfen, ob die benutzerdefinierten virtuellen Kanäle erfolgreich geöffnet werden.

## Überlegungen zu virtuellen Citrix-Kanälen

Alle integrierten virtuellen Citrix Kanäle haben eine Vertrauensstellung und können ohne weitere Konfiguration geöffnet werden. Zwei Features erfordern jedoch aufgrund externer Abhängigkeiten einen expliziten Eintrag in der Positivliste:

- Multimediaumleitung
- HDX RealTime Optimization Pack für Skype for Business

### Multimediaumleitung

Wenn Sie einen anderen Media Player als Windows Media Player als System-Media Player verwenden, müssen Sie ihn als vertrauenswürdigen Prozess zur Positivliste hinzufügen. Folgende Informationen sind für den Eintrag in der Positivliste erforderlich:

- Name des virtuellen Kanals: `CTXMM`
- Prozess: Pfad zu dem auf dem VDA verwendeten Media Player. Beispiel: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Eintrag in Positivliste: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

### HDX RealTime Optimization Pack für Skype for Business

Folgende Informationen sind für den Eintrag in der Positivliste erforderlich:

- Name des virtuellen Kanals: `CTXRMEP`
- Prozess: Pfad zu der Exe-Datei von Skype for Business auf der VDA-Maschine. Dieser variiert ggf. je nach Skype for Business-Version bzw. kann ein benutzerdefinierter Installationspfad sein. Zum Beispiel: `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.

- Eintrag in Positivliste: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Problembehandlung

May 17, 2024

Wenn der benutzerdefinierte virtuelle Kanal nicht geöffnet werden kann, gehen Sie die folgenden Schritte durch:

1. Vergewissern Sie sich, dass Sie die richtige VDA-Version verwenden.
2. Vergewissern Sie sich, dass auf den VDA eine Richtlinie mit dem benutzerdefinierten virtuellen Kanal in der Positivliste für virtuelle Kanäle angewendet wurde und keine anderen Richtlinien mit höherer Priorität diese Konfiguration überschreiben.
3. Überprüfen Sie das Ereignisprotokoll im VDA und vergewissern Sie sich, dass der gemeldete virtuelle Kanalname mit dem Namen übereinstimmt, der in der Positivliste definiert ist.

    a) Wenn Sie mehrere Prozesse haben, vergewissern Sie sich, dass diese korrekt definiert sind, wie unter Virtuelle Kanäle zur Positivliste hinzufügen beschrieben.
    b) Wenn Sie Platzhalter im definierten Prozesspfad verwenden, achten Sie darauf, dass Sie die Richtlinien für die Verwendung von Platzhaltern einhalten.
    c) Wenn Sie Umgebungsvariablen im definierten Prozesspfad verwenden, achten Sie darauf, dass Sie die Richtlinien unter Systemumgebungsvariablen verwenden einhalten.

### Ereignisprotokolle

Die folgenden Ereignisse werden im Ereignisprotokoll der VDA-Maschine protokolliert:

#### Einzelsitzungs-VDA

Die folgenden Ereignisse werden im Ereignisprotokoll eines Einzelsitzungs-VDAs protokolliert:

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 2001 | Picadd | Informationen | Der benutzerdefinierte virtuelle Kanal <vcName> wurde von Prozess < processName> geöffnet |
| System | 2002 | Picadd | Warnung | Der benutzerdefinierte virtuelle Kanal <vcName> kann von Prozess < processName> nicht geöffnet werden |
| System | 2003 | Picadd | Informationen | <username> hat den benutzerdefinierten Kanal <vcName> geöffnet |
| System | 2004 | Picadd | Warnung | <username> hat versucht, den benutzerdefinierten virtuellen Kanal <vcName> zu öffnen |
| System | 2005 | Picadd | Fehler | Der in Richtlinie < pathInPolicy > angegebene Pfad kann nicht in den Prozesspfad aufgelöst werden |
| System | 2007 | Picadd | Informationen | Der geladene Prozesspfad ist < processPath> |

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 2008 | Picadd | Fehler | Umgebungsvariable <varName> wurde nicht im VC-Richtlinienpfad gefunden |

**Multisitzungs-VDA**

Die folgenden Ereignisse werden im Ereignisprotokoll eines Multisitzungs-VDAs protokolliert:

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 13 | Rpm | Informationen | Der benutzerdefinierte virtuelle Kanal <vcName> wurde von Prozess <processName> geöffnet |
| System | 14 | Rpm | Warnung | Der benutzerdefinierte virtuelle Kanal <vcName> kann von Prozess <processName> nicht geöffnet werden |
| System | 15 | Rpm | Informationen | <username> hat den benutzerdefinierten Kanal <vcName> geöffnet |

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 16 | Rpm | Warnung | <username> hat versucht, den benutzerdefinierten virtuellen Kanal <vcName> zu öffnen |
| System | 17 | Rpm | Fehler | Der in Richtlinie <pathInPolicy> angegebene Pfad kann nicht in den Prozesspfad aufgelöst werden |
| System | 18 | Rpm | Informationen | Der geladene Prozesspfad ist <processPath> |
| System | 19 | Rpm | Fehler | Umgebungsvariable <varName> wurde nicht im VC-Richtlinienpfad gefunden |

## Bekannte virtuelle Kanäle von Drittanbietern

May 17, 2024

Die folgenden Drittanbieterlösungen verwenden bekanntermaßen benutzerdefinierte virtuelle Citrix Kanäle. Diese Liste enthält nicht jede Lösung, die einen benutzerdefinierten virtuellen Citrix Kanal verwendet.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop-Software

- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Midmark IQPath-Clienterweiterungen
- Nuance PowerMic-Clienterweiterungen
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings für VDI
- Ultima IA-Connect

Um Details zum Hinzufügen der zugehörigen virtuellen Kanäle zur Positivliste zu erhalten, wenden Sie sich an die Hersteller der jeweiligen Lösung. Alternativ führen Sie die Schritte unter Erhalt der Namen und Prozesse virtueller Kanäle aus.

## Geräte

August 30, 2023

HDX bietet eine High Definition-Benutzererfahrung auf jedem Gerät an jedem Ort. Im Abschnitt "Geräte"werden folgende Geräte behandelt:

- Clientlaufwerkzuordnung
- Generische USB-Geräte
- Mobile und Touchscreengeräte
- Serielle Geräte
- Spezialtastaturen
- TWAIN-Geräte
- Webcams
- WIA-Geräte

### Vergleich: optimierte und generische USB-Geräte

Ein optimiertes USB-Gerät ist eines, für das die Citrix Workspace-App spezifische Unterstützung bietet. Beispiel ist die Möglichkeit der Webcamumleitung über den virtuellen HDX-Multimediakanal. Für generische USB-Geräte bietet die Citrix Workspace-App keine spezifische Unterstützung.

Standardmäßig kann die generische USB-Umleitung USB-Geräte mit optimierter Unterstützung für virtuelle Kanäle nur nach einem Wechsel in den generischen Modus umleiten.

Im Allgemeinen erzielen Sie im optimierten Modus eine bessere Leistung für USB-Geräte als im generischen Modus. In Einzelfällen bieten USB-Geräte im optimierten Modus jedoch nicht den vollen Funktionsumfang. Es kann ein Wechsel in den generischen Modus erforderlich sein, um vollen Zugriff auf alle Funktionen zu erhalten.

Für USB-Massenspeichergeräte können Sie die Clientlaufwerkzuordnung, die generische USB-Umleitung oder beides über Citrix Richtlinien verwenden. Die Hauptunterschiede sind folgende:

Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der Clientlaufwerkzuordnung umgeleitet.

Wenn folgende Bedingungen erfüllt sind, wird das Massenspeichergerät mit der generischen USB-Umleitung umgeleitet:

- Sowohl die Richtlinie für die generische USB-Umleitung als auch diejenige für die Clientlaufwerkzuordnung ist aktiviert.
- Es ist ein Gerät für die automatische Umleitung konfiguriert.
- Ein Massenspeichergerät wird entweder vor oder nach dem Start einer Sitzung angeschlossen.

Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX123015.

| Feature | Clientlaufwerkzuordnung | Generische USB-Umleitung |
|---|---|---|
| Diese Option ist in der Standardeinstellung aktiviert. | Ja | Nein |
| Konfigurierbare Leserechte | Ja | Nein |
| Verschlüsselter Gerätezugriff | Ja, wenn die Verschlüsselung vor dem Zugriff auf das Gerät in der virtuellen Sitzung entsperrt wird | Nur Citrix Virtual Desktops |

## Clientlaufwerkzuordnung (CDM)

November 6, 2023

Die Clientlaufwerkzuordnung stellt Speicherlaufwerke auf dem Clientendpunkt innerhalb einer Citrix HDX-Sitzung zur Verfügung, sodass Dateien und Ordner zwischen Client und Sitzungshost übertragen werden können. Das Feature ist standardmäßig mit Lese- und Schreibrechten aktiviert. Um zu verhindern, dass Benutzer Dateien und Ordner auf zugeordneten Clientlaufwerken hinzufügen oder ändern,

aktivieren Sie die Richtlinieneinstellung **Schreibgeschützter Zugriff auf Clientlaufwerke**. Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellung **Clientlaufwerkumleitung** auf **Zugelassen** festlegen und zur Richtlinie hinzufügen.

Aus Sicherheitsgründen werden Endpunktlaufwerke standardmäßig ohne Ausführungsberechtigung zugeordnet. Damit Benutzer ausführbare Dateien direkt von den zugeordneten Clientlaufwerken ausführen können, bearbeiten Sie den Registrierungswert **ExecuteFromMappedDrive** auf dem Sitzungshost. Weitere Informationen finden Sie unter Zugeordnete Clientlaufwerke in der Liste **Über die Registrierung verwaltete HDX-Features**.

## Anforderungen

Die folgenden Anforderungen gelten für die Verwendung der Clientlaufwerkzuordnung:

### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 1912 oder höher
- Citrix DaaS

### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows Server 2016 oder höher
  - Linux: Siehe Linux VDA-Systemanforderungen.
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 oder höher
  - Linux: Siehe Linux VDA-Dokumentation.

### Clientgerät

- Betriebssystem
  - Windows 10 1809 oder höher
  - Linux: Siehe Systemanforderungen der Workspace-App für Linux.

### Relevante Richtlinien

Informationen zu den Einstellungen für die Clientlaufwerkzuordnung finden Sie unter Referenz für Richtlinieneinstellungen.

### Double-Hop-Szenarien

Die Clientlaufwerkzuordnung wird in Double-Hop-Szenarien unterstützt. Standardmäßig wird das Laufwerk des Clientendpunkts in der zweiten Hop-Sitzung zugeordnet und die Laufwerke des ersten Hop sind nicht verfügbar. Dies kann jedoch so konfiguriert werden, dass die Laufwerke der ersten Hop-Sitzung in der zweiten Hop-Sitzung anstelle der Laufwerke des Clientendpunkts zugeordnet werden.

Um diese Funktion zu konfigurieren, bearbeiten Sie den folgenden Registrierungswert:

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Adva
- Wertname: NativeDriveMapping
- Werttyp: REG_SZ
- Wertdaten:
  - True: Ordnet die Laufwerke der ersten Hop-Sitzung der zweiten Hop-Sitzung zu.
  - False: Ordnet die Laufwerke des Clientendpunkts in der zweiten Hop-Sitzung zu.

> **Hinweis:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

## Generische USB-Geräte

April 18, 2024

HDX-Technologie bietet **optimierte Unterstützung** für die gebräuchlichsten USB-Geräte. Diese Geräte umfassen:

- Monitore
- Mäuse

- Tastaturen
- VoIP-Telefone
- Headsets
- Webcams
- Scanner
- Kameras
- Drucker
- Laufwerke
- Smartcardleser
- Grafiktablets
- Signaturtablets

Die optimierte Unterstützung bietet eine verbesserte Benutzererfahrung, Leistung und Bandbreiteneffizienz über ein WAN. Die optimierte Unterstützung ist normalerweise, insbesondere aber in Umgebungen mit hoher Latenz oder hohen Sicherheitsanforderungen, die beste Option.

HDX-Technologie bietet **generische USB-Umleitung** für Spezialgeräte ohne optimierte Unterstützung oder wenn diese ungeeignet ist. Weitere Informationen zur generischen USB-Umleitung finden Sie unter Generische USB-Umleitung.

Weitere Informationen zu USB-Geräten und der Citrix Workspace-App für Windows finden Sie unter Konfigurieren der Umleitung von USB-Verbundgeräten und Konfigurieren der USB-Unterstützung.

## Unterstützung für mobile Clientgeräte und Clientgeräte mit Touchscreen

February 21, 2024

Mit Citrix Virtual Apps and Desktops können Benutzer von mobilen Clientgeräten und Clientgeräten mit Touchscreen auf ihre veröffentlichten Anwendungen und Desktops zugreifen.

### Anforderungen

#### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 7.15 oder höher
- Citrix DaaS

#### Sitzungshost

- Betriebssystem
  - Windows 10 1903 oder höher
  - Windows Server 2016 oder höher
- VDA
  - Windows: Version 7.15 oder höher

#### Clientgerät

- Betriebssystem
  - Windows 10 1809 oder höher
- Citrix Workspace-App für Windows Version 1808 oder höher

### Tabletmodus für Touchscreengeräte mit Windows Continuum

Continuum ist ein Windows 10-Feature, das sich an die Art und Weise der Verwendung des Clientgeräts anpasst. Wenn der VDA erkennt, dass eine Tastatur oder Maus an einen Client mit Touchscreen angeschlossen ist, versetzt er den Client in den Desktopmodus. Ist keine Tastatur oder Maus vorhanden, versetzt der VDA den Client in den Tablet-/Mobilgerätemodus. Diese Erkennung erfolgt bei der Verbindung und Wiederverbindung der Sitzung sowie während der Sitzung, wenn eine Tastatur oder Maus angeschlossen oder getrennt wird.

Das Feature ist in der Standardeinstellung aktiviert. Um diese Funktion zu deaktivieren, konfigurieren Sie die Richtlinieneinstellung Tabletmodus ein/aus.

Zusätzlich zu den oben genannten Anforderungen für Touchscreengeräte müssen für Windows Continuum die folgenden Anforderungen erfüllt sein:

#### XenServer

- Citrix Hypervisor 8.2 oder höher
- Führen Sie folgenden XenServer-CLI-Befehl zum Zulassen der Laptop-/Tablet-Umschaltung aus: **xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1**

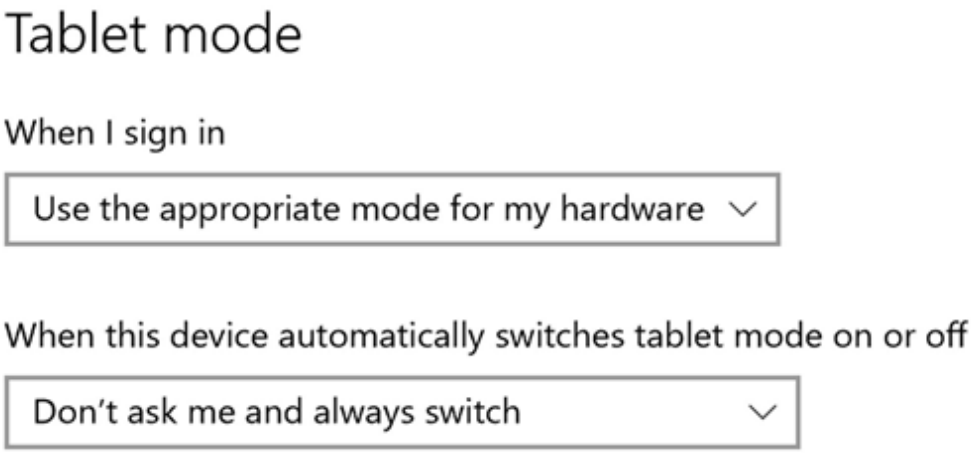
> **Wichtig:**
>
> Das Aktualisieren des Basisimage eines Maschinenkatalogs nach dem Ändern der Metadateneinstellung hat keine Auswirkungen auf zuvor bereitgestellte VMs. Nachdem Sie das XenServer-VM-

> Basisimage geändert haben, erstellen Sie einen Katalog, wählen Sie das Basisimage aus, und stellen Sie eine neue MCS-Maschine bereit.

**Sitzungshost**

- Betriebssystem
  - Windows 10 1903 oder höher
  - Windows 11
- VDA
  - Windows: Version 7.16 oder höher
  - **Aufgrund der aktuellen Einschränkungen in den Betriebssystemkonfigurationen muss der Benutzer nach dem Start der ersten ICA-Sitzung die folgenden Optionen in den Dropdownmenüs festlegen und dann den VDA neu starten:**
    - **Einstellungen > System > Tabletmodus**
      - Passenden Modus für meine Hardware verwenden
      - Nicht fragen und immer wechseln




Der **Tabletmodus** bietet eine für Touchscreens besser geeignete Benutzeroberfläche:

- Die Schaltflächen sind etwas größer
- Die Startseite und alle Apps werden im Vollbildmodus geöffnet
- Die Taskleiste enthält eine Zurück-Schaltfläche
- Die Taskleiste enthält keine Symbole

Es besteht Zugriff auf den Datei-Explorer.

Basierend auf diesem aktualisierten BIOS lädt Windows 10 den GPIO-Treiber auf der Ziel-VM. Er wird für die Umschaltung zwischen Tablet- und Desktopmodus innerhalb der virtuellen Maschine verwendet.

Die Citrix Workspace-App für HTML5 unterstützt keine Windows Continuum-Features.

Der **Desktopmodus** ist die klassische Benutzeroberfläche, bei der die Interaktion wie bei einem PC mit Tastatur und Maus erfolgt.

### Microsoft Surface Pro und Surface Book-Stifte

Standardstiftfunktionen bei Windows Ink-basierten Anwendungen werden unterstützt. Dies umfasst Zeigen, Löschen, Stiftdruck, Bluetooth-Signale und andere Features je nach Betriebssystem-Firmware und Stiftmodell. Der Stiftdruck kann beispielsweise bis zu 4096 Stufen haben. Dieses Feature ist standardmäßig aktiviert.

Im Folgenden sind die Anforderungen für die Unterstützung der Stiftfunktionalität aufgeführt:

#### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 1903 und höher
- Citrix DaaS

#### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher

  - Windows Server 2016 oder höher
  - Windows 11

- VDA
  - Windows: Version 1903 oder höher

**Clientgerät**

- Betriebssystem
  - Windows 10 1809 oder höher
- Citrix Workspace-App für Windows: Mindestversion 1902

Für eine Demonstration von Windows Ink und der Stiftfunktionalität klicken Sie auf folgende Grafik:


Informationen zum Deaktivieren oder Aktivieren dieses Features finden Sie unter Microsoft Surface Pro und Surface Book-Stifte in der Liste der über die Registrierung verwalteten Features.

### Bekannte Probleme

Die folgenden Probleme mit der Stiftunterstützung sind bekannt:

- Aufgrund von Betriebssystembeschränkungen in Windows Server 2k22 können Benutzer keine Stiftverknüpfungen einrichten oder Stift-/Tinteneinstellungen in der Systemsteuerung anpassen, wenn sie eine Verbindung zu 2k22-Serveranwendungen oder Desktops herstellen.
- Stiftverknüpfungen werden von einem für Stifte aktivierten Windows 11-Client aufgrund von Betriebssystemeinschränkungen nicht beachtet.

# Serielle Ports

April 19, 2022

Die meisten neuen PCs haben keine seriellen (COM) Ports. Serielle Ports können problemlos per USB-Konverter hinzugefügt werden. Anwendungen, die für serielle Ports geeignet sind, umfassen häufig Sensoren, Controller, alte Lesegeräte usw. Für manche virtuellen USB-COM-Portgeräte werden herstellerspezifische Treiber anstelle der Windows-Treiber (usbser.sys) verwendet. Mit solchen Treibern können Sie den virtuellen COM-Port des USB-Geräts so festlegen, dass er sich auch bei Anschluss an andere USB-Anschlüsse nicht ändert. Die Einstellung kann über **Geräte-Manager > Anschlüsse (COM & LPT) > Eigenschaften** oder über die Anwendung zur Gerätesteuerung erfolgen.

Mit der Client-COM-Portzuordnung können Geräte, die an einen COM-Port eines Endgeräts angeschlossen sind, in virtuellen Sitzungen verwendet werden. Die Zuordnungen können genau wie andere Netzwerkzuordnungen verwendet werden.

Ein Treiber im Betriebssystem weist jedem COM-Port einen symbolischen Linknamen (COM1, COM2 usw.) zu. Die Anwendungen verwenden den Link, um auf den Port zuzugreifen.

> **Wichtig:**
>
> Geräte können zwar direkt per USB an Endpunkte angeschlossen werden, dies bedeutet aber nicht, dass sie über die generische USB-Umleitung umgeleitet werden können. Manche USB-Geräte fungieren als virtuelle COM-Ports, auf die Anwendungen wie auf physische serielle Ports zugreifen. Das Betriebssystem kann COM-Ports abstrahieren und sie wie Dateifreigaben behandeln. Zwei gebräuchliche Protokolle für virtuelle COM-Ports sind CDC ACM und MCT. Bei Anschluss an eine RS-485-Schnittstelle funktionieren Anwendungen evtl. nicht. Mit einem RS-485-zu-RS232-Konverter können Sie RS-485-Schnittstellen als COM-Port verwenden.
> **Wichtig:**
>
> Einige Anwendungen erkennen ein Gerät (z. B. ein Unterschriftenpad) nur dann zuverlässig, wenn es über COM1 oder COM2 an der Clientarbeitsstation angeschlossen ist.

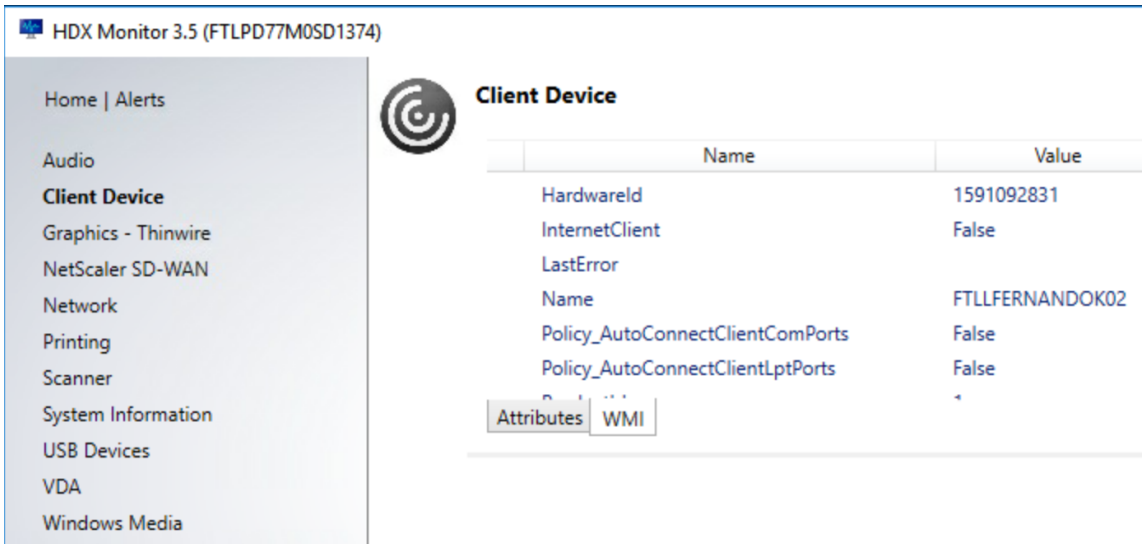
## Zuordnen eines COM-Ports für Clients zu einem Server-COM-Port

Sie können Client-COM-Ports einer Citrix Sitzung auf dreierlei Weise zuordnen:

- Verwalten Sie Konsolenrichtlinien. Weitere Informationen über Richtlinien finden Sie unter Einstellungen der Richtlinie "Portumleitung".
- VDA-Eingabeaufforderung:
- Konfigurationstool für Remotedesktop (Terminaldienste):

1. Aktivieren Sie die Studio-Richtlinien **Client-COM-Portumleitung** und **Client-COM-Ports automatisch verbinden**. Nach der Anwendung stehen diverse Informationen in HDX Monitor zur Verfügung.




2. Wenn der Port durch **Client-COM-Ports automatisch verbinden** nicht zugeordnet werden kann, können Sie ihn manuell oder über Anmeldeskripts zuordnen. Melden Sie sich beim VDA an und geben Sie in einer Eingabeaufforderung Folgendes ein:

   NET USE COMX: \\CLIENT\COMZ:

   oder

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   **X** ist die Nummer des COM-Ports auf dem VDA (Ports 1 bis 9 stehen für die Zuordnung zur Verfügung). **Z** ist der Name des Client-COM-Ports, den Sie zuordnen möchten.

   Um zu überprüfen, ob der Vorgang erfolgreich war, geben Sie **NET USE** an einer VDA-Eingabeaufforderung ein. Die angezeigte Liste enthält zugeordnete Laufwerke, LPT- und zugeordnete COM-Ports.


3. Um den COM-Port auf einem virtuellen Desktop oder in einer Anwendung zu verwenden, installieren Sie die Anwendung und verweisen Sie sie auf den zugeordneten Namen. Wenn Sie beispielsweise Port COM1 auf dem Client dem Port COM3 auf dem Server zuordnen, installieren

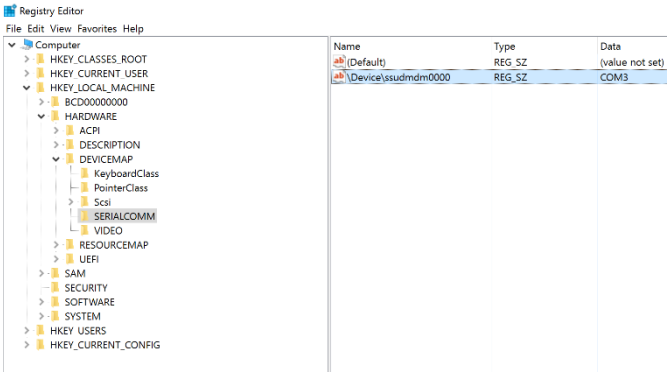
 

Sie die COM-Portanwendung auf dem VDA und verweisen Sie sie in der Sitzung auf COM3. Verwenden Sie diesen zugeordneten COM-Port dann wie einen COM-Port auf dem Benutzergerät.

> **Wichtig:**
>
> Die Zuordnung von COM-Ports ist nicht mit TAPI kompatibel. Sie können TAPI-Geräte (Windows Telephony Application Programming Interface) nicht Client-COM-Ports zuordnen. TAPI definiert eine Standardmethode zur Steuerung von Telefonfunktionen für Daten-, Fax- und Sprachanrufe durch Anwendungen. TAPI übernimmt die Signalverarbeitung (Wählen, Beantworten und Beenden von Anrufen). Außerdem ermöglicht TAPI Dienste wie Halten und Verbinden von Anrufen und Konferenzschaltungen.

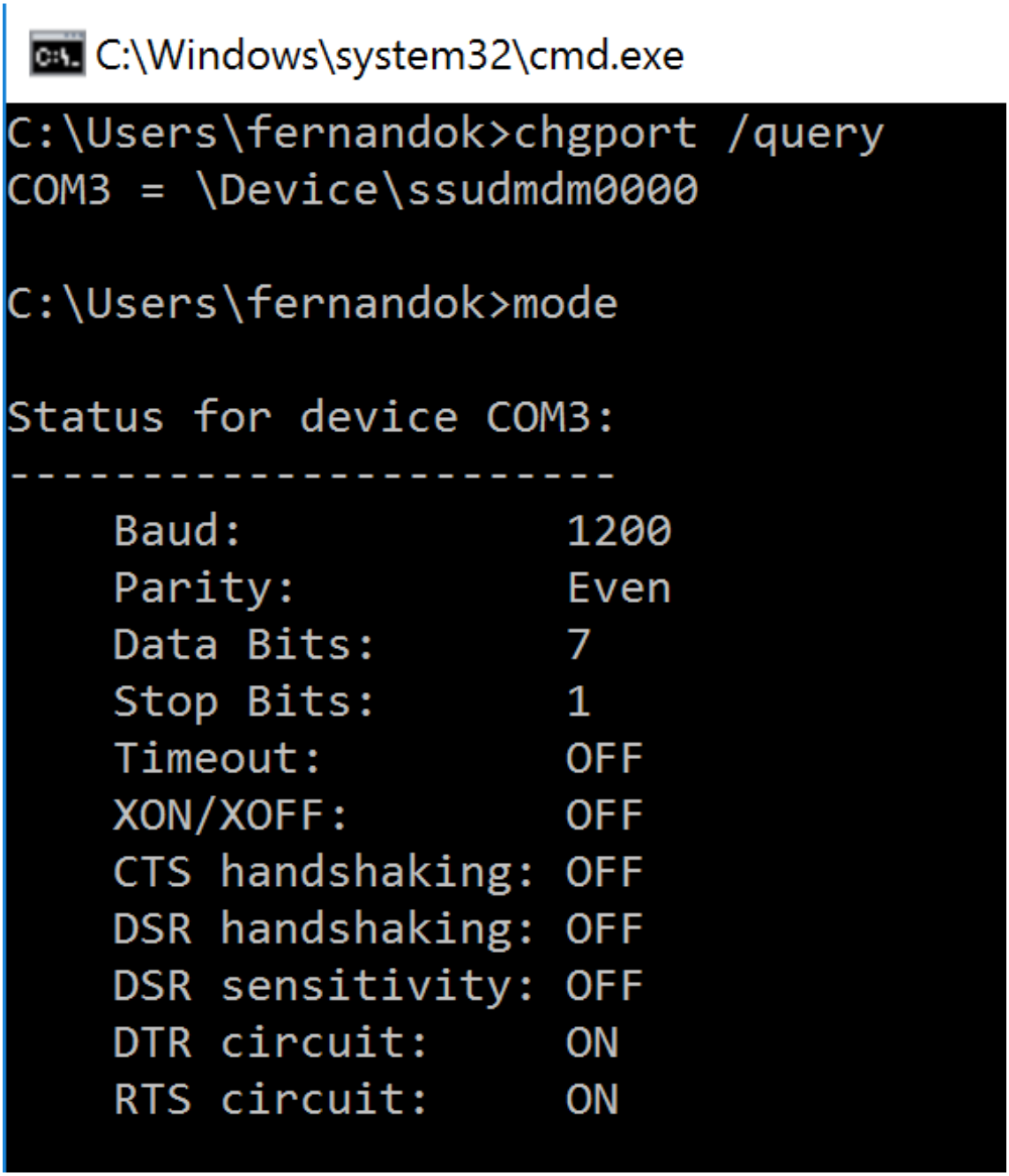
## Problembehandlung

1. Vergewissern Sie sich, dass Sie vom Endpunkt unter Umgehung von Citrix direkt auf das Gerät zugreifen können. Wenn der Port nicht dem VDA zugeordnet ist, sind Sie nicht mit einer Citrix Sitzung verbunden. Folgen Sie allen mit dem Gerät gelieferten Anweisungen zur Problembehandlung und stellen Sie zuerst sicher, dass es lokal funktioniert.
   Wenn ein Gerät an einen seriellen COM-Port angeschlossen wird, wird ein Registrierungsschlüssel mit folgender Struktur erstellt:



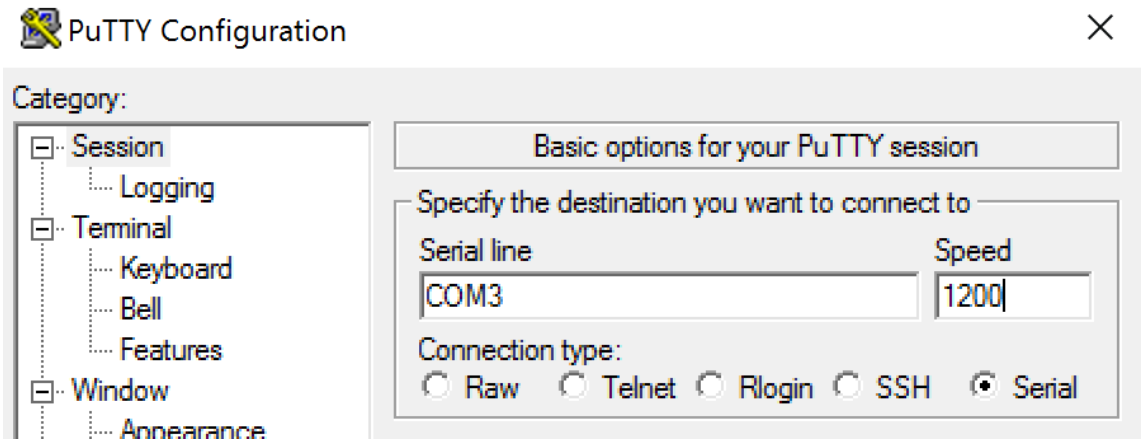

   Sie finden diese Informationen auch durch Ausführen von chgport **/query** an der Eingabeaufforderung.




Stehen keine Anweisungen zur Fehlerbehebung für das Gerät zur Verfügung, versuchen Sie es mit einer PuTTY-Sitzung. Wählen Sie **Session** und geben Sie für **Serial line** Ihren COM-Port an.




Sie können **MODE** in einem lokalen Befehlsfenster ausführen. Die Ausgabe zeigt den verwendeten COM-Port sowie ggf. die für die PuTTY-Sitzung benötigten Baud/Parity/Data Bits/Stop Bits an. Wenn die PuTTY-Verbindung erfolgreich ist, drücken Sie die **Eingabetaste**, um eine Rückmeldung vom Gerät zu erhalten. Von Ihnen eingegebene Zeichen werden ggf. auf dem Bildschirm wiederholt oder beantwortet. Wenn dies nicht möglich ist, können Sie nicht aus virtuellen Sitzungen auf das Gerät zugreifen.

2. Ordnen Sie den lokalen COM-Port dem VDA zu (mithilfe von Richtlinien oder **NET USE COMX: \\CLIENT\COMZ:**) und wiederholen Sie die PuTTY-Prozeduren im vorherigen Schritt, diesmal jedoch per VDA-PuTTY. Schlägt PuTTY mit dem Fehler **Unable to open connection to COM1. Unable to open serial port** fehl, wird COM1 möglicherweise von einem anderen Gerät verwendet.

3. Führen Sie **chgport /query** aus. Wenn der integrierte Windows-Treiber für serielle Ports auf dem VDA COM1 automatisch \Device\Serial0 zuordnet, gehen Sie folgendermaßen vor:
   A. Öffnen Sie CMD auf dem VDA und geben Sie **NET USE** ein.

   B. Löschen Sie eine ggf. vorhandene Zuweisung (z. B. COM1) auf dem VDA.

   **NET USE COM1 /DELETE**

   C. Ordnen Sie das Gerät dem VDA zu.

   **NET USE COM1: \\CLIENT\COM3:**

   D. Verweisen Sie die Anwendung auf dem VDA an COM3.

   Versuchen Sie als Letztes, den lokalen COM-Port (z. B. COM3) einem anderen COM-Port auf dem VDA als COM1 zuzuordnen (z. B. COM3). Stellen Sie sicher, dass Ihre Anwendung darauf verweist:
   **NET USE COM3: \\CLIENT\COM3**

4. Wenn der Port jetzt als zugeordnet erscheint und PuTTY funktioniert aber keine Daten übertragen werden, kann eine Racebedingung vorliegen. Die Anwendung stellt möglicherweise vor der Portzuordnung eine Verbindung her und öffnet den Port, sodass dieser für die Zuordnung gesperrt ist. Versuchen Sie eine der folgenden Möglichkeiten:

- Öffnen Sie eine zweite Anwendung, die auf demselben Server veröffentlicht wurde. Warten Sie einige Sekunden, bis der Port zugeordnet ist, und öffnen Sie dann die eigentliche Anwendung, die den Port verwenden soll.
- Aktivieren Sie die Richtlinien für die COM-Portumleitung über den Gruppenrichtlinien-Editor in Active Directory anstelle der Oberfläche "Verwalten > Vollständige Konfiguration" im Dienst. Es handelt sich um die Studio-Richtlinien **Client-COM-Portumleitung** und **Client-COM-Ports automatisch verbinden**. Auf diese Weise angewendete Richtlinien werden ggf. vor den Richtlinien der Verwaltungskonsole verarbeitet, wodurch sichergestellt wird, dass der COM-Port zugeordnet wird. Citrix Richtlinien werden an den VDA übertragen und an folgenden Orten gespeichert:
  `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Verwenden Sie dieses Anmeldeskript für den Benutzer oder veröffentlichen Sie anstelle der Anwendung ein BAT-Skript, das zuerst alle Zuordnungen auf dem VDA löscht, den virtuellen COM-Anschluss neu zuordnet und anschließend die Anwendung startet:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (bzw. jeweils erforderlicher Wert)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (bzw. jeweils erforderlicher Wert)
START C:\Program Files\<Your Software Path>\
```

5. Als letzte Möglichkeit können Sie den Prozessmonitor von Sysinternals verwenden. Suchen und filtern Sie mit diesem Tool auf dem VDA Objekte wie COM3, picaser.sys, CdmRedirector und insbesondere <Anwendungsname>.exe. Fehler werden in Form von "Zugriff verweigert"oder ähnlich angezeigt.

## Spezialtastaturen

April 18, 2024

### Bloomberg-Tastaturen

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verur-

> sachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Citrix Virtual Apps and Desktops unterstützt die Bloomberg-Tastatur 4 (Starboard) und das ältere Modell 3. Mithilfe der Spezialfunktionen dieser Tastatur können Benutzer im Finanzsektor schnell auf Finanzmarktdaten zugreifen und handeln.

Die Tastatur ist mit den KVM-Switches kompatibel und kann in zwei Modi betrieben werden:

- PC (ein USB-Kabel ohne KVM)
- KVM-Modus (zwei USB-Kabel, eines via KVM)

> **Wichtig:**
>
> Citrix empfiehlt, die Bloomberg-Tastatur nur in einer Sitzung zu verwenden. Von der Verwendung der Tastatur in mehreren Sitzungen gleichzeitig (ein Client für mehrere Sitzungen) wird abgeraten.

Die Bloomberg-Tastatur 4 umfasst als USB-Verbundgerät vier USB-Geräte in einem Gehäuse:

- Tastatur
- Fingerabdruckleser
- Audiogerät mit Tasten zum Erhöhen und Verringern der Lautstärke und zum Stummschalten von Lautsprecher und Mikrofon. Das Gerät umfasst integrierte Lautsprecher, Mikrofon und eine Buchse für Mikrofon und Headset.
- USB-Hub für den Anschluss aller Geräte an das System

**Anforderungen:**

- Die Sitzung, mit der die Citrix Workspace-App für Windows verbunden ist, muss USB-Geräte unterstützen.
- Mindestens Citrix Workspace-App 1808 für Windows oder Citrix Receiver 4.8 zur Unterstützung von Bloomberg-Tastaturmodellen 3 und 4
- Mindestens Citrix Workspace-App 1808 für Windows oder Citrix Receiver 4.12 für den KVM-Modus (zwei USB-Kabel, von denen eines über KVM geleitet wird) für Modell 4

Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen in der Citrix Workspace-App für Windows finden Sie unter Konfigurieren von Bloomberg-Tastaturen.

Informationen zum Aktivieren der Bloomberg-Tastaturunterstützung finden Sie unter Bloomberg-Tastaturen in der Liste der über die Registrierung verwalteten Features.

**Überprüfen der Kompatibilität:**

Um festzustellen, ob die Bloomberg-Tastaturunterstützung in der Citrix Workspace-App aktiviert ist, prüfen Sie, ob im Desktop Viewer die Bloomberg-Tastaturgeräte korrekt angezeigt werden.

Desktop:

Öffnen Sie den Desktop Viewer. Wenn die Unterstützung für die Bloomberg-Tastatur aktiviert ist, werden im Desktop Viewer drei Geräte unter dem USB-Symbol angezeigt:

- Bloomberg-Fingerabdruckscanner
- Bloomberg-Tastaturfeatures
- Bloomberg LP Keyboard 2013

Seamlessanwendung:

Öffnen Sie das Menü **Connection Center** über das Infobereichssymbol der Citrix Workspace-App. Wenn die Unterstützung für die Bloomberg-Tastatur aktiviert ist, werden die drei Geräte im Menü **Geräte** angezeigt.

Ein Häkchen zeigt an, dass das jeweilige Gerät in einer Sitzung verwendet wird.

## TWAIN-Geräte

April 19, 2022

### Anforderungen

- Der Scanner muss TWAIN-kompatibel sein.
- Installieren Sie die TWAIN-Treiber auf dem lokalen Gerät. Auf dem Server sind sie nicht erforderlich.
- Schließen Sie den Scanner lokal an (z. B. über USB).
- Stellen Sie sicher, dass der Scanner den lokalen TWAIN-Treiber und nicht den Windows Image Acquisition-Dienst verwendet.
- Stellen Sie sicher, dass auf das für den Test verwendete Benutzerkonto keine Richtlinie angewendet wird, welche die Bandbreite der ICA-Sitzung begrenzt. Beispiel: Bandbreitenlimit für Client-USB-Geräteumleitung.

Informationen zu Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "TWAIN-Geräte".

# Webcams

August 16, 2022

## HD-Webcamstreaming

Webcams können von innerhalb einer virtuellen Sitzung ausgeführten Videokonferenzanwendungen verwendet werden. Die Anwendung auf dem Server wählt Format und Auflösung von Webcams basierend auf den unterstützten Formatarten. Beim Sitzungsstart sendet der Client die Webcam-Informationen an den Server. Wählen Sie eine Webcam über die Videokonferenzanwendung aus. Wenn Webcam und Anwendung HD-Wiedergabe unterstützen, wird HD in der Anwendung verwendet. Es werden Webcamauflösungen bis zu 1920 x 1080 unterstützt.

Dieses Feature erfordert mindestens Version 4.10 von Citrix Receiver für Windows. Eine Liste der Citrix Workspace-App-Plattformen, die die HDX-Webcamumleitung unterstützen, finden Sie unter Citrix Workspace-App –Featurematrix.

Weitere Informationen zum HD-Webcamstreaming finden Sie unter HDX-Videokonferenzen und Webcam-Videokomprimierung.

Sie können das Feature über einen Registrierungsschlüssel aktivieren und deaktivieren und dann eine spezifische Auflösung konfigurieren. Weitere Informationen finden Sie unter HD-Webcamstreaming und HD-Webcamauflösung in der Liste der Features, die über die Registrierung verwaltet werden.

# WIA-Geräte

April 19, 2022

## Anforderungen

- Der Scanner muss WIA-kompatibel sein.
- Installieren Sie die WIA-Treiber auf dem lokalen Gerät. Auf dem Server sind sie nicht erforderlich.
- Schließen Sie den Scanner lokal an (z. B. über USB).
- Stellen Sie sicher, dass der Scanner den lokalen Windows-Bilderfassungsdienst (Windows Image Acquisition, WIA) und nicht den TWAIN-Treiber verwendet.

- Stellen Sie sicher, dass auf das für den Test verwendete Benutzerkonto keine Richtlinie angewendet wird, welche die Bandbreite der ICA-Sitzung begrenzt. Beispiel: Bandbreitenlimit für Client-USB-Geräteumleitung.

#### Positivliste für WIA-Anwendungen

Mit einer Positivliste können Sie festlegen, welche Anwendungen auf dem VDA auf die WIA-Scannerumleitung zugreifen können. Der Registrierungseditor verwendet Angaben aus der eingestellten Positivliste auf jedem VDA mit Windows-Bilderfassung (WIA). Standardmäßig kann keine Anwendung auf die WIA-Schnittstelle zugreifen.

Informationen zum Anpassen der Windows-Bilderfassung für Anwendungen auf dem VDA finden Sie unter Positivliste für WIA-Anwendungen in der Liste der über die Registrierung verwalteten Features.

Informationen zu Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "WIA-Geräte" .

## Grafik

April 19, 2022

Citrix HDX umfasst vielfältige Technologien zur Grafikbeschleunigung und -codierung, die die Bereitstellung reichhaltiger Grafikanwendungen über Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) optimieren. Die Grafiktechnologien bieten bei der Remotearbeit mit grafikintensiven virtuellen Anwendungen die gleiche Benutzererfahrung wie ein physischer Desktop.

Sie können für das Grafikrendering Software oder Hardware verwenden. Softwarerendering erfordert eine Drittanbieter-Bibliothek ("Softwarerasterizer"). Windows enthält beispielsweise den WARP-Rasterizer für DirectX-basierte Grafiken. Unter Umständen wird ein anderer Softwarerenderer bevorzugt. Hardwarerendering (Hardwarebeschleunigung) erfordert einen Grafikprozessor (GPU).

HDX bietet eine Standardcodierungskonfiguration, die für die häufigsten Anwendungsfälle optimiert ist. Über Citrix Richtlinien können IT-Administratoren grafikbezogene Einstellungen zur Erfüllung verschiedener Anforderungen und Bereitstellung der gewünschten Benutzererfahrung konfigurieren.

### Thinwire

Thinwire ist die in Citrix DaaS verwendete Standardtechnologie von Citrix für das Anzeigeremoting.

Per Anzeigeremoting können auf einer Maschine erzeugte Grafiken (normalerweise über ein Netzwerk) auf eine andere Maschine für die Anzeige übertragen werden. Grafiken werden als Ergebnis von Benutzereingaben, z. B. Tastenanschläge und Mausaktionen, erzeugt.

### HDX 3D Pro

Mit der HDX 3D Pro-Funktion von Citrix DaaS können Desktops und Anwendungen bereitgestellt werden, die mit einem Grafikprozessor (GPU) für die Hardwarebeschleunigung am besten funktionieren. Dazu gehören professionelle, auf OpenGL und DirectX basierende 3D-Grafikanwendungen. Der Standard-VDA unterstützt die GPU-Beschleunigung nur für DirectX.

#### GPU-Beschleunigung für Windows-Einzelsitzungs-OS

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Maschinen mit Einzelsitzungs-OS bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen) und die Virtualisierungstechnologien der Hypervisors XenServer, vSphere und Hyper-V (nur Passthrough).

Mit GPU-Passthrough können Sie VMs mit exklusivem Zugriff auf dedizierte Hardware für die Grafikverarbeitung erstellen. Sie können mehrere GPUs auf dem Hypervisor installieren und VMs jeder dieser GPUs einzeln zuweisen.

Mit GPU-Virtualisierung können mehrere virtuelle Maschinen die Grafikverarbeitungsleistung eines einzelnen physischen GPU direkt nutzen.

#### GPU-Beschleunigung für Windows-Multisitzungs-OS

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Sitzungen mit Windows-Multisitzungs-OS ausgeführt werden, auf der GPU des Servers gerendert werden. Beim Verlagern der Wiedergabe von OpenGL, DirectX, Direct3D und Windows Presentation Foundation (WPF) auf den GPU des Servers wird die CPU des Servers nicht durch die Grafikwiedergabe verlangsamt. Außerdem kann der Server so mehr Grafiken verarbeiten, weil die Arbeitslast zwischen Prozessor und Grafikprozessor aufgeteilt wird.

### Framehawk

> **Wichtig:**
>
> Ab Citrix Virtual Apps and Desktops 7 1903 wird Framehawk nicht mehr unterstützt. Verwenden Sie stattdessen Thinwire mit aktiviertem adaptivem Transport.

Framehawk ist eine Technologie für das Anzeigeremoting für mobile Mitarbeiter mit drahtlosen Breitbandverbindungen (WiFi und 4G/LTE-Mobilfunknetze). Framehawk überwindet die Herausforderungen der spektralen Interferenz und des Mehrwegeempfangs und liefert eine flüssige, interaktive Benutzererfahrung für virtuelle Apps und Desktops.

### Textbasiertes Sitzungswasserzeichen

Textbasierte Sitzungswasserzeichen zur Verhinderung und Verfolgung von Datendiebstahl: Diese verfolgbaren Informationen erscheinen auf dem Sitzungsdesktop als Abschreckung für Personen, die

Daten per Foto oder Screenshot stehlen möchten. Sie können eine Textschicht als Wasserzeichen festlegen. Das Wasserzeichen kann über dem gesamten Sitzungsbildschirm angezeigt werden, ohne das Originaldokument zu ändern. Textbasierte Sitzungswasserzeichen erfordern VDA-Unterstützung.

### Verwandte Informationen

- HDX 3D Pro
- GPU-Beschleunigung für Windows-Einzelsitzungs-OS
- GPU-Beschleunigung für Windows-Multisitzungs-OS
- Thinwire
- Textbasiertes Sitzungswasserzeichen

## HDX 3D Pro

January 25, 2024

Mit der HDX 3D Pro-Funktion von Citrix Virtual Apps and Desktops können Desktops und Anwendungen bereitgestellt werden, die mit einem Grafikprozessor (GPU) für die Hardwarebeschleunigung am besten funktionieren. Dazu gehören professionelle, auf OpenGL und DirectX basierende 3D-Grafikanwendungen. Der Standard-VDA unterstützt die GPU-Beschleunigung nur für DirectX.

Informationen zu den HDX 3D Pro-Richtlinieneinstellungen finden Sie unter Optimierung für 3D-Grafikworkload.

Alle unterstützten Citrix Workspace-App-Versionen können mit 3D-Grafiken verwendet werden. Zur Erzielung der optimalen Leistung in Umgebungen mit komplexen 3D-Anwendungen, hochauflösenden Monitoren, Multimonitorkonfigurationen und Anwendungen mit hohen Framerates empfiehlt Citrix die Verwendung der aktuellen Version der Citrix Workspace-App für Windows bzw. der Citrix Workspace-App für Linux. Informationen zu den unterstützten Versionen der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app.

Beispiele für professionelle 3D-Anwendungen:

- CAD-, CAM- und CAE-Anwendungen
- Geografische Informationssystemsoftware (GIS)
- Bildarchivierungskommunikationssystem (PACS) für bildgebende Diagnostik
- Anwendungen, die die aktuellen Versionen von OpenGL, DirectX, NVIDIA, CUDA, OpenCL und WebGL verwenden
- Rechenintensive Nichtgrafik-Anwendungen, die NVIDIA CUDA-GPUs (Compute Unified Device Architecture) für paralleles Computing verwenden

HDX 3D Pro bietet die beste bandbreitenunabhängige Benutzererfahrung:

- WAN-Verbindungen: Bieten Sie eine interaktive Benutzererfahrung über WAN-Verbindungen mit geringen Bandbreiten bis zu 1,5 MBit/s.
- LAN-Verbindungen: Bieten Sie eine Benutzererfahrung wie bei einem lokalen Desktop bei LAN-Verbindungen.

  Sie können komplexe und teure Arbeitsstationen durch einfache Benutzergeräte ersetzen, da die Grafikverarbeitung in das Datencenter für eine zentralisierte Verwaltung verschoben wird.

HDX 3D Pro stellt die GPU-Beschleunigung für Maschinen mit Windows-Einzelsitzungs-OS und Windows-Multisitzungs-OS bereit. Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Einzelsitzungs-OS sowie GPU-Beschleunigung für Windows-Multisitzungs-OS.

HDX 3D Pro ist mit GPU-Passthrough und der GPU-Virtualisierung folgender Hypervisors und in Bare-Metal-Umgebungen kompatibel:

- XenServer
  - GPU-Passthrough mit NVIDIA GRID, AMD und Intel GVT-d
  - GPU-Virtualisierung mit NVIDIA GRID, AMD und Intel GVT-g
  - Siehe Hypervisor Hardware Compatibility List.

Mit dem HDX Monitor können Sie den Betrieb und die Konfiguration von HDX-Visualisierungstechnologien überprüfen und HDX-Probleme diagnostizieren und beheben. Das Tool und weitere Informationen stehen unter https://taas.citrix.com/hdx/download/ zur Verfügung.

## GPU-Beschleunigung für Windows-Multisitzungs-OS

January 25, 2024

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Sitzungen mit Windows-Multisitzungs-OS ausgeführt werden, auf der GPU des Servers gerendert werden. Beim Verlagern der Wiedergabe von OpenGL, DirectX, Direct3D und Windows Presentation Foundation (WPF) auf den GPU des Servers wird die CPU des Servers nicht durch die Grafikwiedergabe verlangsamt. Außerdem kann der Server so mehr Grafiken verarbeiten, weil die Arbeitslast zwischen Prozessor und Grafikprozessor aufgeteilt wird.

Da Windows Server ein Mehrbenutzer-Betriebssystem ist, kann eine von Citrix Virtual Apps verwendete GPU ohne GPU-Virtualisierung (vGPU) von mehreren Benutzern verwendet werden.

Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich

machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungseditors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungseditors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### GPU Sharing

Die GPU-Freigabe ermöglicht die GPU-Hardwarewiedergabe von OpenGL- und DirectX-Anwendungen in Remotedesktopsitzungen. Sie hat die folgenden Merkmale:

- Verwenden auf Bare-Metal- oder virtuellen Maschinen, um die Anwendungsskalierbarkeit und -leistung zu steigern.
- Mehrere gleichzeitige Sitzungen können GPU-Ressourcen gemeinsam verwenden. (Die meisten Benutzer benötigen nicht die Wiedergabeleistung eines dedizierten GPU).
- Erfordert keine besonderen Einstellungen.

Ein GPU kann der virtuellen Windows Server-Maschine gemäß den Anforderungen des Hypervisor- und GPU-Anbieters im Modus GPU-Passthrough oder Virtual GPU (vGPU) zugewiesen werden. Bare-Metal-Bereitstellungen auf physischen Windows Server-Maschinen werden ebenfalls unterstützt.

GPU Sharing hängt nicht von einer bestimmten Grafikkarte ab.

- Wählen Sie für virtuelle Maschinen eine Grafikkarte, die mit dem verwendeten Hypervisor kompatibel ist. Eine Hardwarekompatibilitätsliste für XenServer finden Sie unter Hypervisor Hardware Compatibility List.
- Bei Ausführung auf Bare-Metal sollte eine Grafikkarte vom Betriebssystem aktiviert sein. Wenn mehrere GPUs auf der Hardware installiert sind, deaktivieren Sie mit dem Device Manager alle außer einem.

Die Skalierbarkeit mit GPU Sharing hängt von folgenden Faktoren ab:

- Ausgeführte Anwendungen
- Verbrauchter Videospeicher
- Verarbeitungsleistung der Grafikkarte

Einige Anwendungen handhaben fehlenden Videospeicher besser als andere. Wenn die Hardware überlastet wird, kann der Grafikkartentreiber instabil werden oder abstürzen. Schränken Sie die Anzahl der gleichzeitigen Benutzer ein, um diese Probleme zu vermeiden.

Sie können die GPU-Beschleunigung mit einem Tool von Drittanbietern bestätigen, z. B. GPU-Z. GPU-Z ist hier verfügbar: http://www.techpowerup.com/gpuz/.

- Zugriff auf einen leistungsfähigen Videoencoder für NVIDIA-GPUs und Intel Iris Pro-Grafikprozessoren. Dieses Feature wird über eine (standardmäßig aktivierte) Richtlinie

gesteuert und ermöglicht die Verwendung der Hardwarecodierung für die H.264-Codierung (falls verfügbar). Ist entsprechende Hardware nicht verfügbar, wird die CPU-basierte Codierung mit dem Software-Videocodec verwendet. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Grafiken".

### Wiedergabe von DirectX, Direct3D und WPF

Die Wiedergabe von DirectX, Direct3D und WPF steht nur auf Servern zur Verfügung, die einen Grafikprozessor haben, der eine Anzeigetreiberschnittstelle (DDI) der Version 9ex, 10 oder 11 unterstützt.

- Unter Windows Server 2008 R2 sind für DirectX und Direct3D keine Sondereinstellungen erforderlich, um einen einzelnen GPU zu verwenden.
- Unter Windows Server 2012 und später verwenden Remotedesktopdienste-Sitzungen auf dem RD-Sitzungshostserver als Standardadapter den Microsoft Basic Render-Treiber. Um den GPU in RDS-Sitzungen unter Windows Server 2012 und später zu verwenden, aktivieren Sie die Einstellung **Use the hardware default graphics adapter for all Remote Desktop Services sessions** in der Gruppenrichtlinie **Lokale Computerrichtlinie** > **Computerkonfiguration** > **Administrative Vorlagen** > **Windows-Komponenten** > **Remotedesktopdienste** > **Remotedesktop-Sitzungshost** > **Remotesitzungsumgebung**.
- Um WPF-Anwendungen mithilfe der Server-GPU zu rendern, erstellen Sie die Einstellungen in der Registrierung des Servers, der die Sitzungen mit Windows-Multisitzungs-OS ausführt. Weitere Informationen zur Registrierungseinstellung finden Sie unter Rendering mit Windows Presentation Foundation (WPF) in der Liste der über die Registrierung verwalteten Features.

### GPU-Beschleunigung für CUDA- oder OpenCL-Anwendungen

Die GPU-Beschleunigung von CUDA- und OpenCL-Anwendungen, die in einer Benutzersitzung ausgeführt werden, ist standardmäßig deaktiviert.

Aktivieren Sie die Registrierungseinstellungen, um die im Rahmen der Machbarkeitsstudie verfügbaren CUDA-Beschleunigungsfeatures zu verwenden. Weitere Informationen finden Sie unter GPU-Beschleunigung für CUDA- oder OpenCL-Anwendungen in der Liste der über die Registrierung verwalteten Features.

## GPU-Beschleunigung für Windows-Einzelsitzungs-OS

January 25, 2024

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Maschinen mit Einzelsitzungs-OS bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen) und die Virtualisierungstechnologien der Hypervisors XenServer, vSphere, Nutanix und Hyper-V (nur Passthrough).

HDX 3D Pro bietet die folgenden Features:

- Adaptive, auf dem H.264- oder H.265-Standard basierende Tiefenkomprimierung für optimale Leistung bei WAN-Verbindungen und drahtlosen Verbindungen. HDX 3D Pro verwendet die CPU-basierte Vollbild-H.264-Komprimierung als Standardkomprimierungsverfahren zur Verschlüsselung. Hardwarecodierung mit H.264 wird für NVIDIA-, Intel- und AMD-Karten verwendet, die NVENC unterstützen. Hardwarecodierung mit H.265 wird für NVIDIA-Karten verwendet, die NVENC unterstützen.
- Verlustfreie Komprimierung für besondere Anwendungsfälle. HDX 3D Pro bietet einen verlustfreien CPU-basierten Codec zur Unterstützung von Anwendungen,in denen pixelgenaue Grafiken unerlässlich sind, z. B. für die medizinische Bilderstellung. Echte verlustfreie Komprimierung wird nur für besondere Anwendungsfälle empfohlen, da sie mehr Netzwerk- und Verarbeitungsressourcen benötigt.

  Bei Verwendung von verlustfreier Komprimierung:

  - Die Anzeige für Verlustfreiheit (Symbol im Infobereich) gibt an, ob es sich bei der Bildschirmanzeige um einen verlustreichen oder verlustfreien Frame handelt. Dies ist hilfreich, wenn die Richtlinieneinstellung **Bildqualität** auf **Zu verlustfrei verbessern** festgelegt ist. Die Anzeige für Verlustfreiheit wird grün, wenn die gesendeten Frames verlustfrei sind.
  - Über die Umschaltung für Verlustfreiheit können die Benutzer jederzeit innerhalb der Sitzung in den immer verlustfreien Modus wechseln. Zum Aktivieren oder Deaktivieren von **Immer verlustfrei in einer Sitzung** klicken Sie mit der rechten Maustaste auf das Symbol und dann auf **Zu pixelgenau wechseln** oder verwenden Sie die Tastenkombination ALT + UMSCHALT + 1.

    Für verlustfreie Komprimierung: HDX 3D Pro verwendet den verlustfreien Codec für die Komprimierung unabhängig von dem durch die Richtlinie ausgewählten Codec.

    Für die verlustreiche Komprimierung: HDX 3D Pro verwendet den ursprünglichen Codec, entweder den Standard oder den über die Richtlinie ausgewählten Codec.

    Einstellungen für die Umschaltung für Verlustfreiheit werden nicht für zukünftige Sitzungen gespeichert. Wenn Sie für alle Verbindungen den verlustfreien Codec verwenden möchten, legen Sie für die Richtlinie **Bildqualität** die Einstellung **Immer verlustfrei** fest.
- Sie können die Standardtastenkombination ALT + UMSCHALT + 1 zum Aktivieren oder Deaktivieren der Option “Verlustfrei”in einer Sitzung außer Kraft setzen. Konfigurieren Sie eine neue Registrierungseinstellung unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.

  - Name: HKEY_LOCAL_MACHINE_HotKey, Typ: String
  - Das Format zum Konfigurieren einer Tastenkombination ist C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val. Schlüssel müssen durch ein Komma (,) getrennt werden. Die Reihenfolge der Tasten ist egal.
  - A, C, S, W und K sind Tasten, wobei Folgendes gilt: C=STRG, A=ALT, S=UMSCHALT, W=Win und K=eine gültige Taste. Zulässige Werte für K sind a-z, 0-9 und jeder virtuelle Tastencode.
  - Beispiel:
    * Taste F10 entspricht K=0x79
    * Taste STRG + F10 entspricht C=1, K=0x79
    * ALT + A entspricht A=1, K=a oder A=1, K=A oder K=A, A=1
    * STRG + ALT + 5 entspricht C=1, A=1, K=5 oder A=1, K=5, C=1
    * STRG + UMSCHALT + F5 entspricht A=1, S=1, K=0x74

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungseditors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungseditors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

- Unterstützung für mehrere Monitore und hochauflösende Monitore: Auf Maschinen mit Einzelsitzungs-OS unterstützt HDX 3D Pro Benutzergeräte mit bis zu vier Monitoren. Benutzer können ihre Monitore beliebig konfigurieren sowie Monitore mit unterschiedlichen Auflösungen und Ausrichtungen kombinieren. Die Anzahl der Monitore wird nur durch die Leistungsfähigkeit des GPU auf dem Hostcomputer, des Benutzergeräts und der verfügbaren Bandbreite begrenzt. HDX 3D Pro unterstützt alle Monitorauflösungen. Einschränkungen bestehen nur hinsichtlich der Leistungsfähigkeit der GPU auf dem Hostcomputer.
- Dynamische Auflösung: Sie können das Fenster des virtuellen Desktops oder der Anwendung auf eine beliebige Auflösung einstellen. **Hinweis**: Die einzige unterstützte Methode zum Ändern der Auflösung ist das Anpassen des VDA-Sitzungsfensters. Das Ändern der Auflösung in der VDA-Sitzung (über **Systemsteuerung > Darstellung** und **Anpassung > Anzeige > Bildschirmauflösung**) wird nicht unterstützt.
- Unterstützung für die NVIDIA vGPU-Architektur HDX 3D Pro unterstützt NVIDIA vGPU-Karten. Weitere Informationen finden Sie unter NVIDIA vGPU für GPU-Passthrough und GPU-Sharing. NVIDIA vGPU ermöglicht mehreren VMs den gleichzeitigen direkten Zugriff auf einen physischen GPU und die Verwendung derselben NVIDIA-Grafiktreiber, die auf nicht-virtualisierten Betriebssystemen bereitgestellt werden.
- Unterstützung für VMware vSphere und VMware ESX mit Virtual Direct Graphics Acceleration

(vDGA): Sie können HDX 3D Pro mit vDGA sowohl für Remotedesktopdienste- als auch für VDI-Arbeitslasten verwenden.

- Unterstützung für VMware vSphere/ESX mit NVIDIA vGPU und AMD MxGPU.
- Unterstützung von Microsoft HyperV mit Discrete Device Assignment in Windows Server 2016:
- Unterstützung von Datencenter-Grafikplattformen der Serie Intel Xeon Processor E3 HDX 3D Pro unterstützt die Verwendung von bis zu 3 Monitoren, das Ausblenden der Konsole, benutzerdefinierte Auflösungen und hohe Frameraten der unterstützten Intel-Serie. Weitere Informationen finden Sie unter http://www.citrix.com/intel und http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Unterstützung für AMD RapidFire auf den Serverkarten der AMD FirePro S-Serie. HDX 3D Pro unterstützt den Betrieb von bis zu 6 Bildschirmen, Console Blanking, benutzerdefinierte Auflösungen und hohe Frameraten. Hinweis: HDX 3D Pro-Unterstützung für AMD MxGPU (GPU-Virtualisierung) funktioniert nur bei VMware vSphere vGPUs. XenServer und Hyper-V werden mit GPU-Passthrough unterstützt. Weitere Informationen finden Sie unter AMD Virtualization Solution.
- Zugriff auf einen leistungsfähigen Videoencoder für NVIDIA-, AMD- und Intel Iris Pro-Grafikprozessoren. Das Feature wird durch eine standardmäßig aktivierte Richtlinieneinstellung gesteuert. Es ermöglicht die Verwendung der H.264-Hardwarecodierung (falls verfügbar). Ist entsprechende Hardware nicht verfügbar, wird die CPU-basierte Codierung mit dem Software-Videocodec verwendet. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Grafiken".

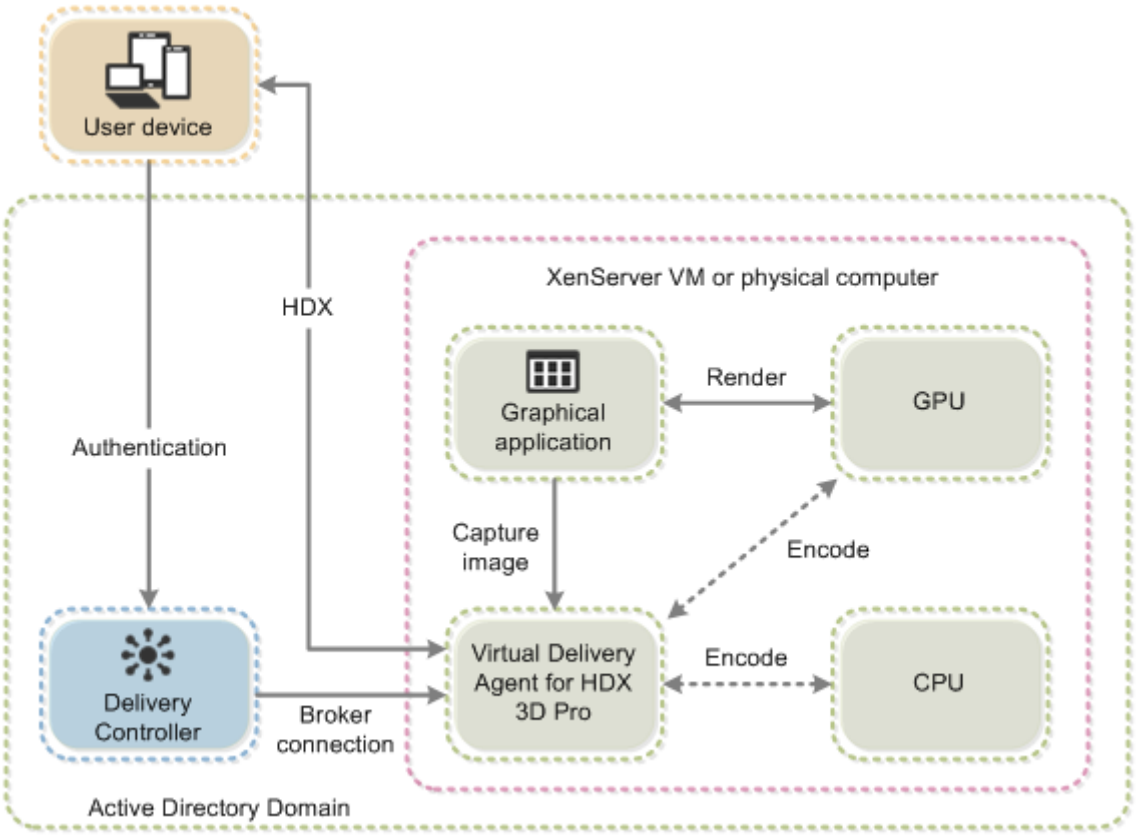
Wie in der folgenden Abbildung dargestellt:

- Wenn sich ein Benutzer bei der Citrix Workspace-App anmeldet und auf die virtuelle Anwendung oder den virtuellen Desktop zugreift, authentifiziert der Controller den Benutzer. Der Controller kontaktiert dann den VDA für HDX 3D Pro, um eine Verbindung mit dem Computer herzustellen, auf dem die grafische Anwendung gehostet wird.

Der VDA für HDX 3D Pro komprimiert mit der entsprechenden Hardware auf dem Host die Ansicht des gesamten Desktops oder nur der grafischen Anwendung.

- Die Desktop- oder Anwendungsansichten und die dazugehörigen Interaktionen der Benutzer werden zwischen dem Hostcomputer und dem Benutzergerät übertragen. Diese Übertragung erfolgt über eine direkte HDX-Verbindung zwischen der Citrix Workspace-App und dem VDA für HDX 3D Pro.




### Optimierung der HDX 3D Pro-Benutzererfahrung

Stellen Sie bei der Verwendung von HDX 3D Pro mit mehreren Monitoren sicher, dass der Hostcomputer mit mindestens so vielen Monitoren konfiguriert ist, wie an den Geräten der Benutzer angeschlossen sind. Die an den Hostcomputer angeschlossenen Monitore können physikalische oder virtuelle Monitore sein.

Schließen Sie Monitore (physikalische oder virtuelle) nicht an Hostcomputer an, während Benutzer mit dem virtuellen Desktop oder der virtuellen Anwendung, die die grafische Anwendung bereitstellen, verbunden sind. Dies kann während der Benutzersitzung zu Instabilität führen.

Teilen Sie den Benutzern mit, dass das Ausführen von Änderungen (von ihnen oder einer Anwendung) an der Desktopauflösung, während eine grafische Anwendungssitzung ausgeführt wird, nicht unterstützt wird. Nach dem Beenden der Anwendungssitzung können Benutzer die Auflösung des Desktop Viewer-Fensters in "Citrix Workspace-App - Desktop Viewer-Einstellungen"ändern.

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfehlen wir, die Richtlinieneinstellung **Bandbreitenlimit für Sitzung insgesamt** zu verwenden, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken. Mit dieser Einstellung wird sichergestellt, dass die verfügbare Bandbreite beim Anmelden und Abmelden

der Benutzer keinen großen Schwankungen unterworfen ist. Da HDX 3D Pro automatische Anpassungen durchführt, um die gesamte Bandbreite auszuschöpfen, kann sich die stark variierende verfügbare Bandbreite während der Benutzersitzungen negativ auf die Leistung auswirken.

Wenn beispielsweise 20 Benutzer eine Verbindung mit 60 MBit/s gemeinsam verwenden, kann die Bandbreite, die den einzelnen Benutzern zur Verfügung steht, abhängig von der Anzahl der gleichzeitigen Benutzer zwischen 3 MBit/s und 60 MBit/s variieren. Um die Benutzererfahrung in diesem Szenario zu optimieren, legen Sie die Bandbreite fest, die zu Spitzenzeiten pro Benutzer erforderlich ist, und stellen Sie sicher, dass die Benutzer diesen Wert nicht überschreiten können.

Wir empfehlen für Benutzer einer 3D-Maus, die Priorität des virtuellen Kanals für die generische USB-Umleitung auf 0 zu erhöhen. Weitere Informationen dazu, wie Sie die Priorität virtueller Kanäle ändern, finden Sie im Knowledge Center-Artikel CTX128190.

## Thinwire

May 23, 2023

### Einführung

Thinwire ist ein Teil der Citrix HDX-Technologie und die in Citrix Virtual Apps and Desktops verwendete Standardtechnologie für das Anzeigeremoting.

Per Anzeigeremoting können auf einer Maschine erzeugte Grafiken (normalerweise über ein Netzwerk) auf eine andere Maschine für die Anzeige übertragen werden.

Eine gute Lösung für das Anzeigeremoting liefert eine hochgradig interaktive Benutzererfahrung –ähnlich wie bei einem lokalen Computer. Bei Thinwire wird dies mit komplexen und effizienten Bildanalyse- und Komprimierungsmethoden erzielt. Thinwire maximiert die Serverskalierbarkeit und verbraucht weniger Bandbreite andere Anzeigeremotingtechnologien.

Dank diesem Gleichgewicht ist Thinwire für die meisten geschäftlichen Anwendungsfälle geeignet und wird als Standardtechnologie für das Anzeigeremoting in Citrix Virtual Apps and Desktops verwendet.

### HDX 3D Pro

In der Standardkonfiguration kann Thinwire 3D- oder hoch interaktive Grafik liefern und, falls vorhanden, eine Grafikprozesseinheit (GPU) verwenden. Citrix empfiehlt jedoch die Aktivierung des HDX 3D Pro-Modus über die Richtlinien **Optimierung für 3D-Grafikworkload** oder **Bildqualität > Zu verlustfrei verbessern** für Szenarien, in denen GPUs vorhanden sind. Diese Richtlinien konfigurieren

Thinwire für die Verwendung eines Videocodecs (H.264 oder H.265) zur Codierung des gesamten Bildschirms mithilfe der Hardwarebeschleunigung, wenn eine GPU vorhanden ist. Dies bietet eine flüssigere Anzeige professioneller 3D-Grafiken. Weitere Informationen finden Sie unter H.264 –Zu verlustfrei verbessern, HDX 3D Pro und GPU-Beschleunigung für Windows-Einzelsitzungs-OS.

### Anforderungen

Thinwire ist optimiert für moderne Betriebssysteme, einschließlich Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 und Windows 10. Für Windows Server 2008 R2 wird der Legacy-Grafikmodus empfohlen. Verwenden Sie die integrierten Citrix Richtlinienvorlagen "Hohe Serverskalierbarkeit –Legacy-OS"und "Für WAN optimiert –Legacy-OS"zum Bereitstellen der von Citrix für solche Anwendungsfälle empfohlenen Kombinationen von Richtlinieneinstellungen.

> **Hinweis:**
>
> In dieser Version wird der Legacygrafikmodus nicht unterstützt. Er ist zum Zweck der Abwärtskompatibilität im Fall einer Verwendung von XenApp 7.15 LTSR, XenDesktop 7.15 LTSR und früheren VDA-Releases enthalten.

- Die Richtlinieneinstellung, die das Verhalten von Thinwire steuert (**Videocodec zur Komprimierung verwenden**), ist in VDA-Versionen in Citrix Virtual Apps and Desktops 7 1808 und höher bzw. XenApp und XenDesktop 7.6 FP3 und höher verfügbar. Die Option **Videocodec verwenden, wenn bevorzugt** ist die Standardeinstellung für die VDA-Versionen in Citrix Virtual Apps and Desktops 7 1808 und höher bzw. in XenApp und XenDesktop 7.9 und höher.
- Alle Citrix Workspace-App-Versionen unterstützen Thinwire. Einige Citrix Workspace-App-Versionen unterstützen unter Umständen manche Thinwire-Features nicht, z. B. 8- oder 16-Bit-Grafiken für eine reduzierte Bandbreitennutzung. Die Unterstützung solcher Features wird automatisch von der Citrix Workspace-App ausgehandelt.
- Thinwire verwendet mehr Serverressourcen (CPU, Speicher) in Umgebungen mit mehreren Monitoren oder hoher Auflösung. Das Maß der Ressourcennutzung durch Thinwire kann eingestellt werden, dabei kann jedoch die Bandbreitennutzung steigen.
- In Umgebungen mit geringer Bandbreite oder hoher Latenz kann sich die Aktivierung von 8- oder 16-Bit-Grafik zur Verbesserung der Interaktivität anbieten. Dadurch wird jedoch evtl. die Anzeigequalität gemindert, insbesondere bei einer 8-Bit-Farbtiefe.

### Codierungsmethoden

Thinwire kann je nach Richtlinie und Clientkapazität in zwei Codierungsmodi ausgeführt werden:

- Thinwire Vollbild H.264 oder H.265
- Thinwire mit selektivem H.264 oder H.265

Bei dem GDI-Remoting älterer Versionen wurde der XPDM-Remotingtreiber und keine Thinwire-Bitmapcodierung verwendet.

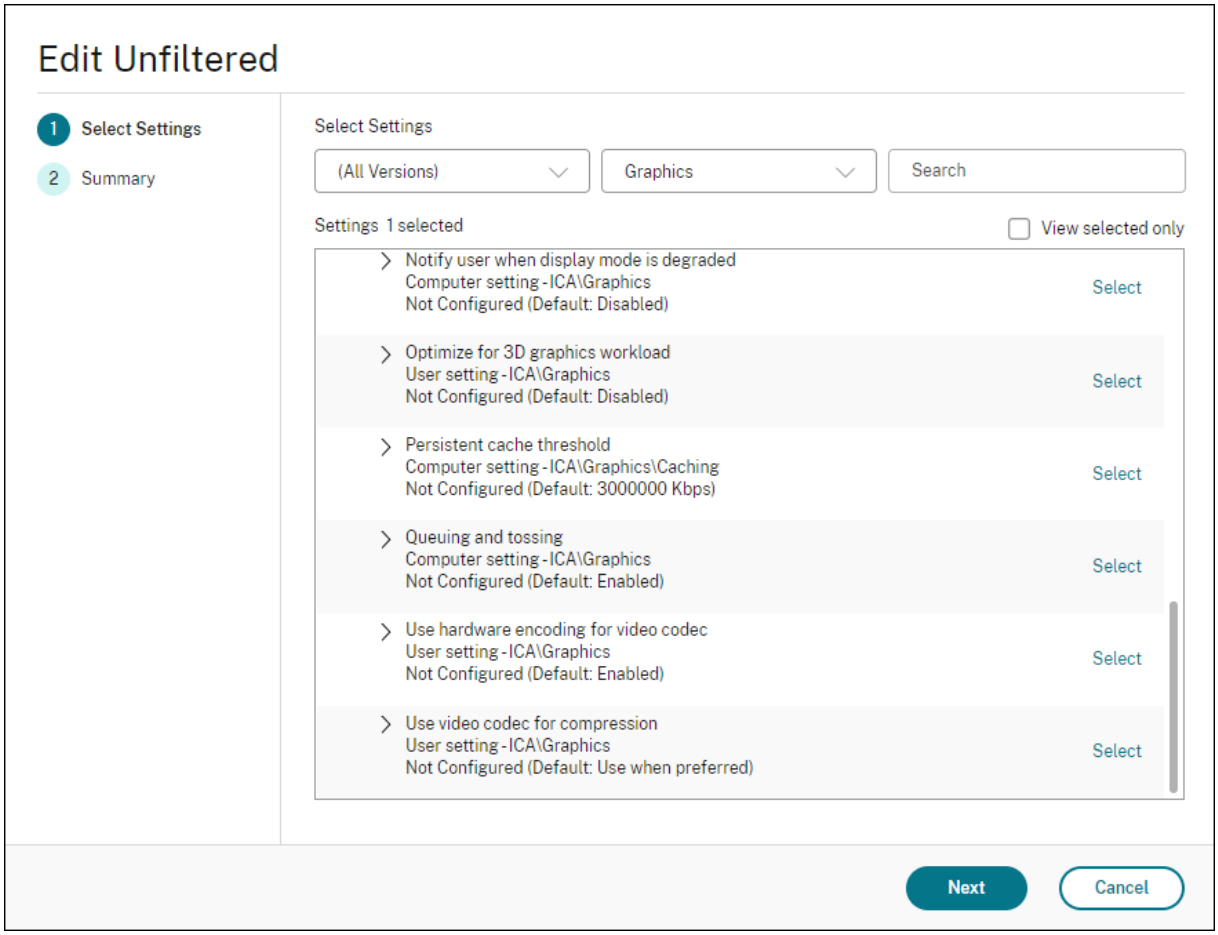
### Konfiguration

Thinwire ist die Standardtechnologie für das Anzeigeremoting.

Die folgende Grafikrichtlinieneinstellung dient zum Festlegen der Standardeinstellung und zur Bereitstellung von Alternativen für verschiedene Anwendungsfälle:

- Videocodec zur Komprimierung verwenden
  - **Videocodec verwenden, wenn bevorzugt**. Dies ist die Standardeinstellung. Eine zusätzliche Konfiguration ist nicht erforderlich. Wenn Sie diese Einstellung als Standard beibehalten, dann wird Thinwire für alle Citrix Verbindungen ausgewählt und für Skalierbarkeit, Bandbreite und bessere Bildqualität bei typischen Desktoparbeitslasten optimiert. Dies ist funktional gleichwertig mit **Für aktive Änderungsbereiche**.
- Von anderen Optionen in dieser Richtlinieneinstellung wird Thinwire auch verwendet und zwar mit anderen Technologien für verschiedene Anwendungsfälle. Beispiel:
  - **Für aktive Änderungsbereiche**. Die Technologie für adaptive Anzeige von Thinwire identifiziert bewegliche Bilder (Video, 3D In Motion) und verwendet H.264 oder H.265 nur in dem Bildschirmbereich, in dem das Bild sich bewegt.
  - **Für den gesamten Bildschirm**. Thinwire wird mit Vollbild-H.264 oder -H.265 zur Optimierung der Benutzererfahrung und Bandbreite bei intensiver 3D-Grafiknutzung verwendet. Bei H.264 4:2:0 (Richtlinie **Visuell verlustfrei** deaktiviert) ist das endgültige Bild nicht pixelgenau (verlustfrei) und für bestimmte Szenarien möglicherweise nicht geeignet. Verwenden Sie in diesen Fällen stattdessen H.264 –Zu verlustfrei verbessern.




Diverse weitere Richtlinieneinstellungen, einschließlich der nachfolgend aufgeführten Einstellungen der Richtlinie "Visuelle Anzeige", können zur Optimierung der Anzeigeremoting-Leistung verwendet werden: Thinwire unterstützt sie alle.

- Bevorzugte Farbtiefe für einfache Grafiken
- Frameratesollwert
- Bildqualität

Zur Aktivierung der von Citrix für verschiedene Anwendungsfälle empfohlenen Kombinationen von Richtlinieneinstellungen verwenden Sie die integrierten Citrix Richtlinienvorlagen. Die Vorlagen **Hohe Serverskalierbarkeit** und **Besonders gute High Definition-Benutzererfahrung** verwenden beide Thinwire mit der optimalen Kombination von Richtlinieneinstellungen für die Prioritäten Ihres Unternehmens und den Erwartungen Ihrer Benutzer.

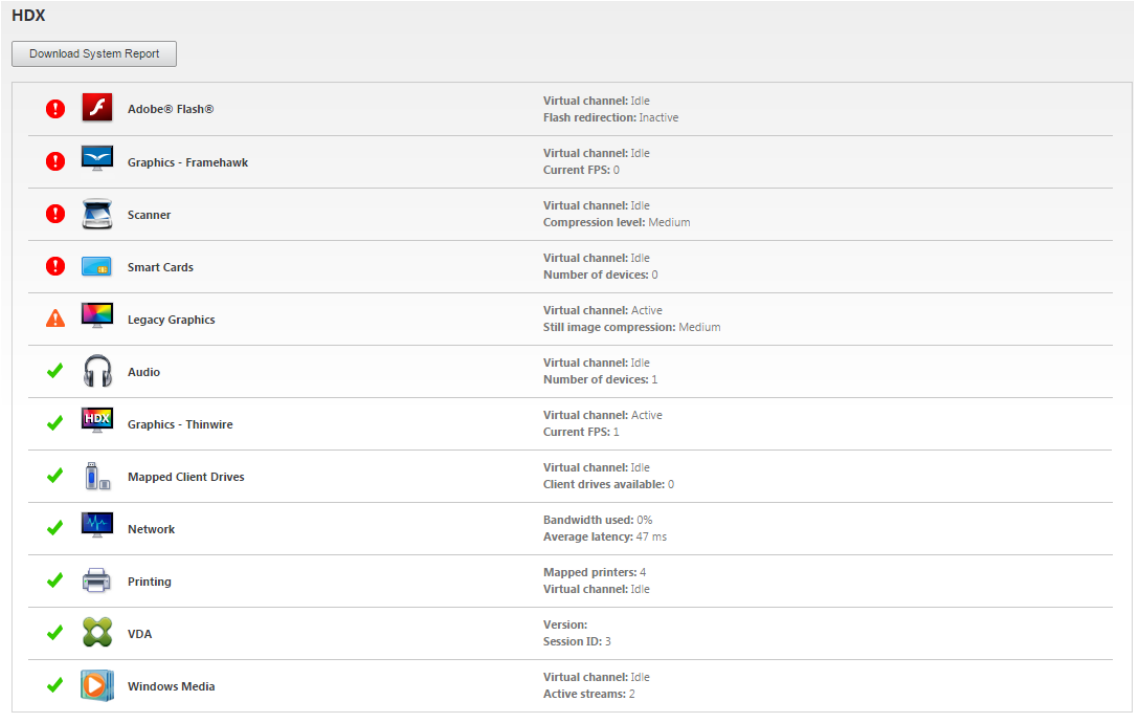
### Überwachen von Thinwire

Sie können die Verwendung und Leistung von Thinwire über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Problembe-

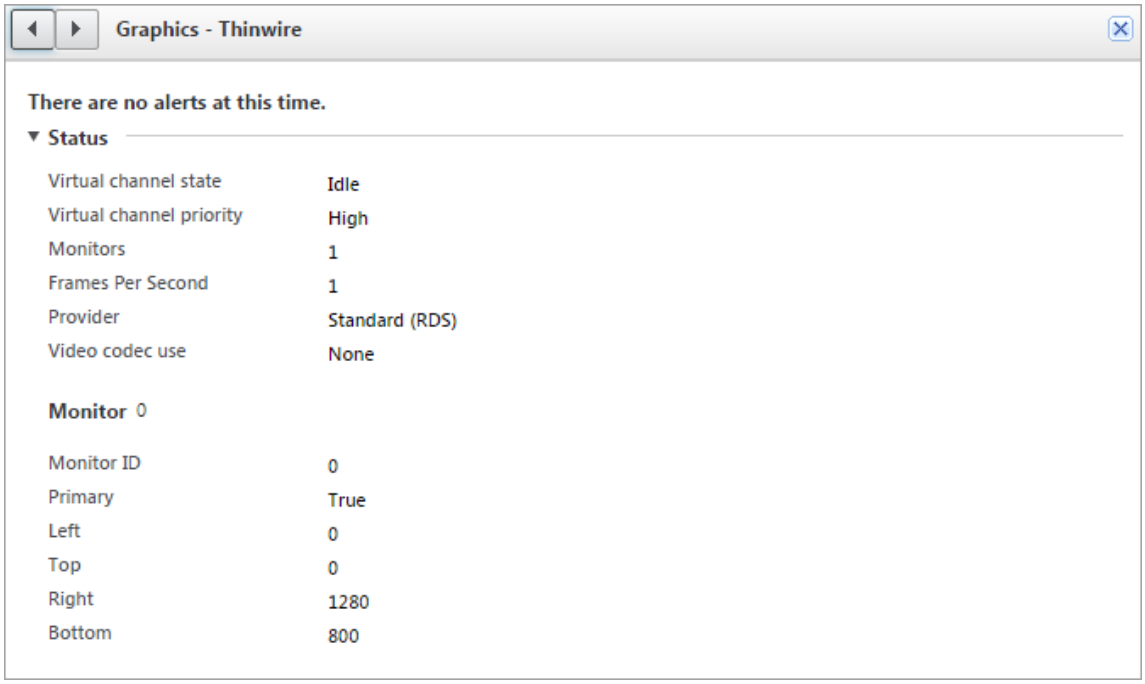
handlung von Thinwire in jeder Sitzung. Gehen Sie zum Anzeigen für Thinwire relevanter Kennzahlen folgendermaßen vor:

1. Suchen Sie in Director einen Benutzer, eine Maschine oder einen Endpunkt, öffnen Sie eine aktive Sitzung und klicken Sie auf **Details**. Oder Sie können **Filter > Sitzung > Alle Sitzungen** wählen, eine aktive Sitzung öffnen und auf **Details** klicken.
2. Führen Sie einen Bildlauf nach unten zum Bereich **HDX** aus.




3. Wählen Sie **Grafiken - Thinwire**.




## Verlustfreier Komprimierungscodec (MDRLE)

In einer normalen Desktopsitzung sind die meisten Bilder einfache Grafiken oder Textbereiche. Thinwire sucht diese Regionen und wählt sie für die verlustfreie Codierung mit dem 2DRLE-Codec aus. Auf dem Citrix Workspace-App-Client werden diese Elemente mit dem 2DRLE-Decoder der Citrix Workspace-App für die Anzeige in der Sitzung decodiert.

XenApp und XenDesktop 7.17 verfügt über einen neuen MDRLE-Codec mit höherer Komprimierungsrate, der bei normalen Desktopsitzungen weniger Bandbreite verbraucht als der 2DRLE-Codec. Der neue Codec hat keine Auswirkungen auf die Serverskalierbarkeit.

Weniger Bandbreite resultiert in der Regel in einer besseren Sitzungsinteraktivität (insbesondere bei gemeinsam genutzten oder eingeschränkten Verbindungen) und geringeren Kosten. Der erwartete Bandbreitenverbrauch des MDRLE-Codecs ist im Vergleich zu XenApp und XenDesktop 7.15 LTSR bei typischen Office-ähnlichen Workloads ca. 10-15 % geringer.

Für den MDRLE-Codec ist keine Konfiguration erforderlich. Wenn die Citrix Workspace-App die MDRLE-Decodierung unterstützt, verwendet der VDA die MDRLE-Codierung und die Citrix Workspace-App die MDRLE-Decodierung. Unterstützt die Citrix Workspace-App die MDRLE-Decodierung nicht, greift der VDA automatisch auf die 2DRLE-Codierung zurück.

**Anforderungen für MDRLE:**

- Citrix Virtual Apps and Desktops-VDAs ab Version 7 1808
- XenApp und XenDesktop-VDAs ab Version 7.17
- Citrix Workspace-App für Windows: Mindestversion 1808

- Citrix Receiver für Windows: Mindestversion 4.11

### Progressiver Modus

In Citrix Virtual Apps and Desktops 1808 wurde der progressive Modus eingeführt. Er ist standardmäßig aktiviert. Unter eingeschränkten Netzwerkbedingungen (Standard: Bandbreite < 2 Mbps oder Latenz > 200 ms) wurde von Thinwire zur Verbesserung der Interaktivität bei Bildschirmaktivitäten die Komprimierung von Text und statischen Bildern erhöht. Stark komprimierter Text und Bilder wurden dann schrittweise in zufälligen Blöcken geschärft, wenn die Bildschirmaktivität beendet wurde. Dieses Verfahren des Komprimierens und Schärfens verbessert zwar die Interaktivität, es reduziert jedoch die Cache-Effizienz und erhöht die Bandbreitennutzung.

Ab Citrix Virtual Apps and Desktops 1906 wurde der progressive Modus standardmäßig deaktiviert. Es kommt nun ein anderes Verfahren zum Einsatz. Die Qualität von Standbildern verbleibt dynamisch basierend auf den Netzwerkbedingungen zwischen einem vordefinierten Mindest- und Maximalwert für jede Einstellung der **visuellen Qualität**. Da es keinen Schärfungsschritt gibt, optimiert Thinwire die Bildbereitstellung unter Beibehaltung der Cache-Effizienz und bietet zugleich nahezu alle Vorteile des progressiven Modus.

#### Ändern des Verhaltens des progressiven Modus

Sie können den Zustand des progressiven Modus über den Registrierungsschlüssel ändern. Weitere Informationen finden Sie unter Progressiver Modus in der Liste der über die Registrierung verwalteten Features.

### H.264 –Zu verlustfrei verbessern

**Zu verlustfrei verbessern** ist eine spezielle Thinwire-Konfiguration, die die Grafikbereitstellung für Interaktivität und endgültige Bildqualität optimiert. Sie können diese Einstellung aktivieren, indem Sie die Richtlinie **Visuelle Qualität** auf **Zu verlustfrei verbessern** festlegen.

Zu verlustfrei verbessern komprimiert die Anzeige mit H.264 (oder H.265) bei Bildschirmaktivität und schärft auf pixelgenau (verlustfrei), wenn die Aktivität beendet wird. Die Bildqualität mit H.264 (oder H.265) wird zur Erhaltung der bestmöglichen Bildrate den verfügbaren Ressourcen angepasst. Das Schärfen erfolgt schrittweise und gestattet eine sofortige Reaktion, wenn der Benutzer die Bildschirmaktivität kurz nach Beginn des Schärfens aufnimmt. Ein Beispiel wäre die Auswahl eines Modells und dessen Drehen.

H.264 –**Zu verlustfrei verbessern** bietet alle Vorteile von Vollbild-H.264 oder -H.265 einschließlich Hardwarebeschleunigung und zusätzlich eine endgültige verlustfreie Anzeige. Dies ist extrem wichtig für 3D-Arbeiten, die ein pixelgenaues Endbild erfordern. Beispiel wäre die Arbeit mit medizinischen

Bildern. Außerdem verbraucht H.264 –**Zu verlustfrei verbessern** weniger Ressourcen als Vollbild-H.264 mit 4:4:4. **Zu verlustfrei verbessern** erzielt in der Regel eine höhere Bildrate als visuell verlustfreies H.264 mit 4:4:4.

> **Hinweis:**
>
> Legen Sie neben der Richtlinie **Visuelle Qualität** die Richtlinie **Videocodec verwenden** auf **Verwenden, wenn bevorzugt** (Standard) oder **Für aktive Änderungsbereiche** fest. Sie können zur Einstellung "Zu verlustfrei verbessern"ohne H.264 zurückkehren, indem Sie die Richtlinie **Videocodec verwenden** auf **Videocodec nicht verwenden** festlegen. Bewegte Bilder werden dann mit JPEG anstelle von H.264 (oder H.265) codiert.

## Textbasiertes Sitzungswasserzeichen

April 1, 2022

Textbasierte Sitzungswasserzeichen zur Verhinderung und Verfolgung von Datendiebstahl: Diese verfolgbaren Informationen erscheinen auf dem Sitzungsdesktop als Abschreckung für Personen, die Daten per Foto oder Screenshot stehlen möchten. Ein Wasserzeichen ist eine Textschicht, die über dem gesamten Sitzungsbildschirm angezeigt wird, ohne eine Änderung des Originaldokuments zu bewirken. Textbasierte Sitzungswasserzeichen erfordern VDA-Unterstützung.

> **Wichtig:**
>
> Textbasierte Sitzungswasserzeichen sind kein Sicherheitsfeature. Sie verhindern einen Datendiebstahl nicht vollständig, bieten jedoch ein gewisses Maß an Abschreckung und Rückverfolgbarkeit. Citrix garantiert bei Verwendung des Features zwar keine vollständige Rückverfolgbarkeit von Informationen, empfiehlt jedoch seine Verwendung nach Bedarf in Kombination mit anderen Sicherheitslösungen.

Ein Sitzungswasserzeichen ist Text, der mit Sitzungen an den Benutzer gesendet wird. Sitzungswasserzeichen enthalten Informationen zur Rückverfolgung von Datendiebstahl. Die wichtigste Angabe ist die Identität des angemeldeten Benutzers, in dessen Sitzung das Bildschirmbild erstellt wurde. Zur besseren Rückverfolgung von Datenlecks sollten Sie weitere Informationen wie die IP-Adresse des Servers oder des Clients und die Verbindungszeit einschließen.

Um die Benutzererfahrung anzupassen, verwenden Sie die Einstellungen der Richtlinie Sitzungswasserzeichen, um die Platzierung und Erscheinung von Wasserzeichen auf dem Bildschirm zu konfigurieren.

**Anforderungen:**

Virtual Delivery Agents:

Multisitzungs-OS 7.17
Einzelsitzungs-OS 7.17

**Einschränkungen:**

- Sitzungswasserzeichen werden nicht in Sitzungen unterstützt, in denen lokaler App-Zugriff, Windows Media-Umleitung, MediaStream, Browserinhaltsumleitung und HTML5-Videoumleitung verwendet werden. Zur Verwendung von Sitzungswasserzeichen müssen Sie diese Features deaktivieren.
- Sitzungswasserzeichen werden nicht unterstützt und angezeigt, wenn eine Sitzung im Vollbildmodus mit Hardwarebeschleunigung ausgeführt wird (Vollbild-H.264- oder -H.265-Codierung).
- Wenn Sie diese HDX-Richtlinien festlegen, werden die Wasserzeicheneinstellungen nicht wirksam es werden keine Wasserzeichen in Sitzungen angezeigt.

**Hardwarecodierung für Videocodec verwenden** auf **Aktiviert**
**Videocodec zur Komprimierung verwenden** auf **Für den gesamten Bildschirm**

- Wenn Sie diese HDX-Richtlinien festlegen, wird das Verhalten gestört und es wird möglicherweise kein Wasserzeichen angezeigt.

  **Hardwarecodierung für Videocodec verwenden** auf **Aktiviert**
  **Videocodec zur Komprimierung verwenden** auf **Videocodec verwenden, wenn bevorzugt**

  Um sicherzustellen, dass Wasserzeichen angezeigt werden, legen Sie **Hardwarecodierung für Videocodec verwenden** auf **Deaktiviert** fest oder **Videocodec zur Komprimierung verwenden** auf **Für aktive Änderungsbereiche** oder **Videocodec nicht verwenden**.
- Das Sitzungswasserzeichen unterstützt nur den Thinwire-Grafikmodus.
- Wenn Sie die Sitzungsaufzeichnung verwenden, enthält die aufgezeichnete Sitzung kein Wasserzeichen.
- Wenn Sie Windows-Remoteunterstützung verwenden, wird das Wasserzeichen nicht angezeigt.
- Wenn ein Benutzer die Taste **Druck/S-Abf** drückt, um eine Bildschirmaufnahme zu erstellen, enthält diese VDA-seitig kein Wasserzeichen. Es wird empfohlen, Maßnahmen zu ergreifen, damit Bildschirmaufnahmen nicht kopiert werden.

## Multimedia

April 1, 2022

Der HDX-Technologiestack unterstützt die Bereitstellung von Multimediaanwendungen über zwei einander ergänzende Methoden:

- Serverseitige Wiedergabe
- Clientseitige Wiedergabe mit Multimediaumleitung

Diese Strategie gewährleistet, dass Sie alle Multimediaformate mit einer guten Benutzererfahrung und bei maximaler Serverskalierbarkeit zu möglichst geringen Kosten pro Benutzer bereitstellen können.

Bei der serverseitigen Wiedergabe werden Audio- und Videoinhalte decodiert und von der Anwendung auf dem Server von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) wiedergegeben. Der Inhalt wird dann komprimiert und unter Einsatz des ICA-Protokolls an die Citrix Workspace-App-Instanz auf dem Benutzergerät gesendet. Diese Methode bietet die größtmögliche Kompatibilität mit verschiedenen Anwendungen und Medienformaten. Da die Videoverarbeitung rechenintensiv ist, profitiert die serverseitige Wiedergabe stark von einer platineninternen Hardwarebeschleunigung. DirectX Video Acceleration (DXVA) entlastet die CPU beispielsweise, da die H.264-Decodierung in einer separaten Hardware erfolgt. Intel Quick Sync, AMD RapidFire und NVIDIA NVENC bieten H.264-Codierung mit Hardwarebeschleunigung.

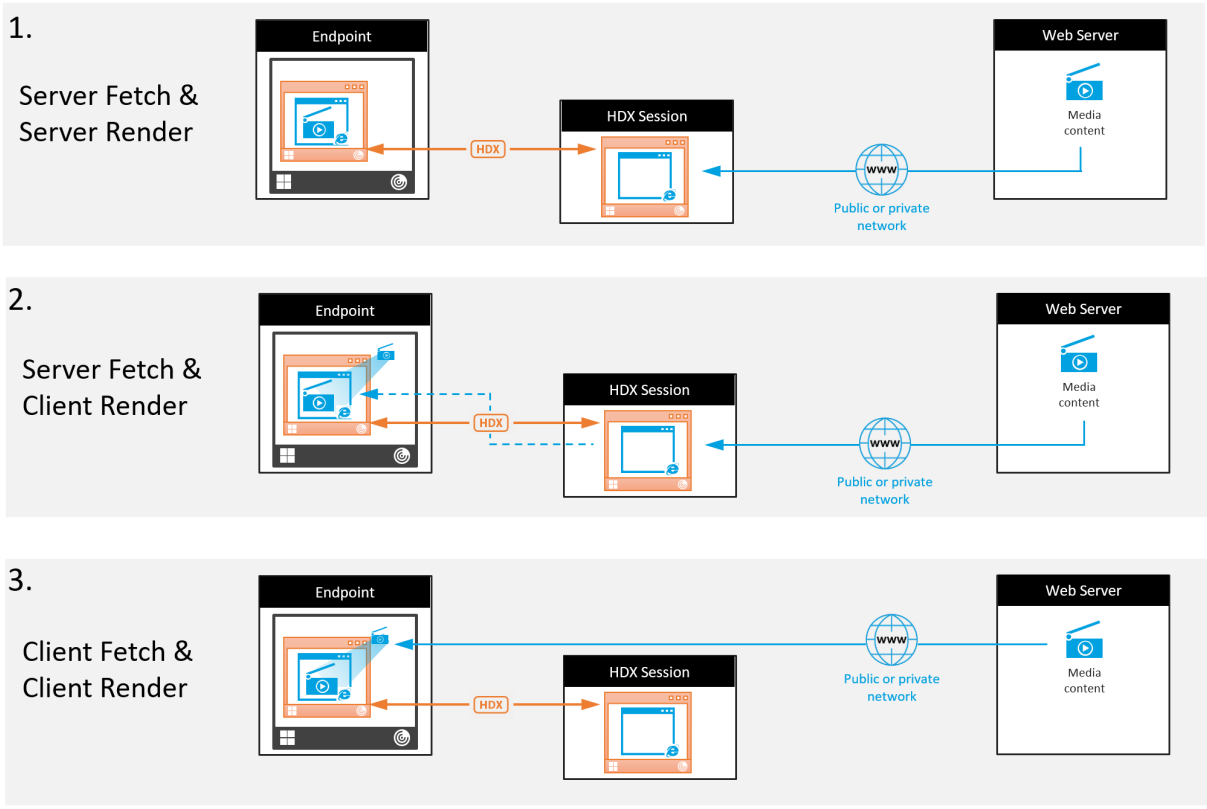
Da die meisten Server keine Hardwarebeschleunigung für die Videokomprimierung bieten, beeinträchtigt eine Abwicklung der gesamten Videoverarbeitung auf der Server-CPU die Serverskalierbarkeit. Zur Wahrung einer hohen Serverskalierbarkeit können viele Multimediaformate zur lokalen Wiedergabe an die Benutzergeräte umgeleitet werden.

- Die Windows Media-Umleitung entlastet den Server bei vielen Medienformaten, die normalerweise Windows Media Player zugeordnet sind.
- HTML5-Video ist mittlerweile gängig und Citrix hat eine Umleitungstechnologie für diese Art von Inhalt eingeführt. Citrix empfiehlt die Umleitung von Browserinhalten für Websites, die HTML5, HLS, DASH oder WebRTC verwenden.
- Sie können die allgemeinen Kontaktumleitungstechnologien der Host-zu-Client-Umleitung und des lokalen App-Zugriffs für Multimediainhalte nutzen.

Wenn Sie keine Umleitung konfigurieren, erfolgt bei HDX die Wiedergabe serverseitig.
Wenn Sie eine Umleitung konfigurieren verwendet HDX entweder den serverseitigen Abruf mit clientseitiger Wiedergabe oder den clientseitigen Abruf mit clientseitiger Wiedergabe. Wenn diese Methoden fehlschlagen, wechselt HDX zu serverseitigen Wiedergabe. Hier kommt dann die Richtlinie zum Verhindern von Videofallback zur Anwendung.

## Beispielszenarios




**Szenario 1. (Serverseitiger Abruf und serverseitige Wiedergabe):**

1. Der Server ruft die Mediendatei von der Quelle ab, decodiert sie und sendet den Inhalt an ein Audio- oder Anzeigegerät.
2. Die Server extrahiert das von dem Gerät erzeugte Bild bzw. Audio.
3. Der Server komprimiert den Inhalt optional und sendet ihn an den Client.

Diese Methode ist mit einer starken CPU-Auslastung und, falls der extrahierte Inhalt nicht effizient komprimiert wurde, einer hohen Bandbreite sowie geringer Serverskalierbarkeit verbunden.

Thinwire und virtuelle Audiokanäle sind bei dieser Methode im Einsatz. Die Methode hat den Vorteil geringerer Anforderungen an Hardware und Software auf dem Client. Die Decodierung erfolgt auf dem Server und die Methode gestattet vielfältigere Geräte und Formate.

**Szenario 2. (Serverseitiger Abruf und clientseitige Wiedergabe):**

Diese Methode stützt sich auf die Möglichkeit, Medieninhalte abzufangen, bevor sie decodiert und auf einem Gerät ausgegeben werden. Die komprimierten Inhalte werden stattdessen an den Client gesendet und dort decodiert und wiedergegeben. Der Vorteil dieses Ansatzes besteht darin, dass sie auf den Clients stattfinden und die Server-CPU entlastet wird.

Sie bedeutet jedoch einige zusätzliche Anforderungen an die Clienthardware und -software. Der Client

muss jedes empfangene Format decodieren können.

**Szenario 3. (Clientseitiger Abruf und clientseitige Wiedergabe):**

Diese Methode stützt sich auf die Möglichkeit, die URL von Medieninhalten abzufangen, bevor diese von der Quelle abgerufen werden. Die URL wird an den Client gesendet, wo die Inhalte dann lokal abgerufen, decodiert und wiedergegeben werden. Das Konzept dieser Methode ist einfach. Sie bietet den Vorteil einer Entlastung der Server-CPU sowie einer geringeren Bandbreitennutzung, da vom Server nur Steuerbefehle gesendet werden. Die Clients können jedoch nicht immer auf Medieninhalte zugreifen.

**Framework und Plattform:**

Einzelsitzungs-Betriebssysteme (Windows, Mac OS X und Linux) bieten Multimediaframeworks zum schnelleren Entwickeln von Multimediaanwendungen. Die nachstehende Tabelle enthält einige gebräuchliche Multimediaframeworks. Bei jedem Framework ist die Medienverarbeitung in mehreren Phasen unterteilt und es wird eine Pipelinearchitektur verwendet.

| Framework | Plattform |
|---|---|
| DirectShow | Windows (98 und höher) |
| Media Foundation | Windows (Vista und höher) |
| Gstreamer | Linux |
| Quicktime | Mac OS X |

## Double-Hop-Unterstützung mit Medienumleitungstechnologien

| | | |
|---|---|---|
| | Audioumleitung | Nein |
| | Browserinhaltsumleitung | Nein |
| | HDX-Webcamumleitung | Ja |
| | HTML5-Videoumleitung | Ja |
| | Windows Media-Umleitung | Ja |

# Audiofeatures

September 26, 2022

Sie können die folgenden Citrix Richtlinieneinstellungen konfigurieren und einer Richtlinie hinzufügen, mit der HDX-Audiofeatures optimiert werden. Nutzungsinformationen sowie Beziehungen mit und Abhängigkeiten von anderen Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "Audio", Einstellungen der Richtlinie "Bandbreite" und Einstellungen der Richtlinie "Multistreamverbindungen".

> **Wichtig:**
>
> Wir empfehlen Audio per User Datagram Protocol (UDP) anstelle von TCP zu senden. Nur der Windows Virtual Delivery Agent (VDA) unterstützt Audio über UDP.
>
> Die UDP-Audioverschlüsselung mit DTLS ist nur zwischen Citrix Gateway und der Citrix Workspace-App möglich. In manchen Fällen ist TCP daher möglicherweise vorzuziehen. TCP unterstützt die lückenlose TLS-Verschlüsselung zwischen VDA und der Citrix Workspace-App.

## Audioqualität

Im Allgemeinen erfordert eine höhere Audioqualität mehr Bandbreite und führt zu einer höheren CPU-Auslastung, da mehr Audiodaten an die Benutzergeräte gesendet werden. Mit der Audiokomprimierung können Sie die Audioqualität und die Sitzungsleistung aufeinander abstimmen; verwenden Sie Citrix Richtlinieneinstellungen, um den Komprimierungsgrad für Audiodateien zu konfigurieren.

Standardmäßig ist die **Richtlinieneinstellung für Audioqualität** bei Verwendung von TCP auf "Hoch - High Definition-Audio"eingestellt. Bei Verwendung von UPD (empfohlen) wird die Richtlinie auf "Mittel - für Sprache optimiert"eingestellt. Die Einstellung **High Definition-Audio** bietet Audio in Hi-Fi-Stereoqualität, verbraucht aber mehr Bandbreite als die anderen Einstellungen. Verwenden Sie diese Audioqualitätseinstellung nicht für nicht optimierte Chat- oder Videochat-Anwendungen (z. B. Softphones). Es kann ansonsten zu Latenzen im Audiopfad kommen, die nicht für die Echtzeitkommunikation geeignet sind. Citrix empfiehlt für Echtzeitaudio die Richtlinieneinstellung "für Sprache optimiert"unabhängig vom ausgewählten Transportprotokoll.

Bei Verbindungen mit begrenzter Bandbreite (z. B. bei Satelliten- oder DFÜ-Verbindungen) kann durch Verringern der Audioqualität auf **Niedrig** sichergestellt werden, dass die geringste Bandbreite verbraucht wird. Erstellen Sie in diesem Fall eigene Richtlinien für Benutzer von Verbindungen mit geringer Bandbreite, damit Benutzer von Verbindungen mit hoher Bandbreite nicht eingeschränkt werden.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

Bandbreitenrichtlinien für Audiowiedergabe und -aufnahme:

- Hohe Qualität (Standard)
  - Bitrate: ~100 KBit/s (min. 75, max. 175 KBit/s) für die Wiedergabe/~ 70 KBit/s für Mikrofonaufnahme
  - Anzahl der Kanäle: 2 (Stereo) für Wiedergabe, 1 (Mono) für Mikrofonaufnahme
  - Frequenz: 44100 Hz
  - Bit-Tiefe: 16 Bit
- Mittlere Qualität (empfohlen für VoIP)
  - Bitrate: ~16 KBit/s (min. 20, max. 40 KBit/s) für die Wiedergabe/~ 16 KBit/s für Mikrofonaufnahme
  - Anzahl der Kanäle: 1 (Mono) für Wiedergabe und Aufnahme
  - Frequenz: 16.000 Hz (Breitband)
  - Bit-Tiefe: 16 Bit
- Niedrige Qualität
  - Bitrate: ~ 11 KBit/s (min. 10; max. 25 KBit/s) für die Wiedergabe, ~ 11 KBit/s für die Mikrofonaufnahme
  - Anzahl der Kanäle: 1 (Mono) für Wiedergabe und Aufnahme
  - Frequenz: 8000 Hz (Schmalband)
  - Bit-Tiefe: 16 Bit

### Clientaudioumleitung

Damit der Audioempfang von einer Anwendung auf dem Server über Lautsprecher oder andere Soundgeräte auf dem Benutzergerät zugelassen wird, übernehmen Sie für die Einstellung **Clientaudioumleitung** den Wert **Zugelassen**. Dies ist die Standardeinstellung.

Die Clientaudiozuordnung belastet Server und Netzwerk zusätzlich. Wenn die Clientaudioumleitung jedoch nicht zugelassen ist, sind alle HDX-Audiofunktionen deaktiviert.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

### Clientmikrofonumleitung

Damit die Audioaufzeichnung mit Eingabegeräten wie Mikrofonen auf dem Benutzergerät zugelassen wird, übernehmen Sie für die Einstellung **Clientmikrofonumleitung** den Standardwert "Zugelassen".

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Geräten haben, auf Mikrofone zugreifen. Die Benutzer können den Zugang akzeptieren oder ablehnen, bevor sie das Mikrofon benutzen. Die Benutzer können die diesbezügliche Warnung in der Citrix Workspace-App deaktivieren.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

### Audio Plug & Play

Die Richtlinie Audio Plug & Play steuert, ob mehrere Audiogeräte zum Aufzeichnen und Wiedergeben zulässig sind. Diese Einstellung ist standardmäßig **aktiviert**. Audio Plug & Play ermöglicht die Erkennung von Audiogeräten. Dies ist selbst dann möglich, wenn diese erst nach Beginn einer Sitzung angeschlossen werden.

Diese Einstellung gilt nur für Maschinen mit Windows-Multisitzungs-OS.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio".

### Bandbreitenlimit für die Audioumleitung und Bandbreitenlimit für die Audioumleitung (Prozent)

Die Richtlinieneinstellung "Bandbreitenlimit für die Audioumleitung"gibt die maximale Bandbreite (in Kilobits pro Sekunde) für die Wiedergabe und Aufzeichnung von Audio in einer Sitzung an.

Die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) gibt die maximale Bandbreite für die Umleitung als Prozentsatz der insgesamt verfügbaren Bandbreite an.

Standardmäßig ist Null (Maximum) für beide Einstellungen angegeben. Wenn beide Einstellungen konfiguriert sind, wird die Einstellung mit dem niedrigsten Bandbreitenlimit verwendet.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Bandbreite". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

### Audio über UDP - Real-time Transport und Audio-UDP-Portbereich

Standardmäßig ist "Audio über UDP mit Real-Time Transport"zulässig (wenn dies bei der Installation ausgewählt wird). Dadurch wird ein UDP-Port auf dem Server für alle Verbindungen geöffnet, die für die Echtzeitübertragung von Audio über UDP konfiguriert wurden. Zur Gewährleistung der besten Benutzererfahrung bei Netzwerküberlastung oder Paketverlust empfiehlt Citrix, dass Sie UDP/RTP für Audio konfigurieren. Für Echtzeitaudio, z. B. Softphone-Anwendungen wird UDP-Audio gegenüber EDT bevorzugt. Bei UDP ist Paketverlust ohne Neuübertragung möglich, sodass bei Verbindungen mit hohen Paketverlusten keine zusätzliche Latenz entsteht.

> **Wichtig:**
>
> Wenn Citrix Gateway nicht im Pfad ist, werden mit UDP übertragene Audiodaten nicht verschlüsselt. Ist Citrix Gateway für den Zugriff auf Citrix Virtual Apps and Desktops-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und Citrix Gateway mittels DTLS gesichert.

Mit der Einstellung "Audio-UDP-Portbereich"geben Sie den Bereich der Portnummern an, die der Windows-VDA zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet.

Der Standardbereich ist 16500 bis 16509.

Weitere Informationen zum Einstellen von Audio über UDP mit Real-Time Transport finden Sie unter Einstellungen der Richtlinie "Audio". Weitere Informationen zum Audio-UDP-Portbereich finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

Audio über UDP benötigt den Windows-VDA. Informationen zu unterstützten Richtlinien auf dem Linux VDA finden Sie unter Liste der unterstützten Richtlinien.

### Audioeinstellungsrichtlinien für Benutzergeräte

1. Laden Sie die Gruppenrichtlinienvorlagen gemäß den Anweisungen unter Konfigurieren der administrativen Gruppenrichtlinienobjektvorlage herunter.
2. Erweitern Sie im Gruppenrichtlinien-Editor **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Wählen Sie für **Clientaudioeinstellungen** die Option **Nicht konfiguriert**, **Aktiviert** oder **Deaktiviert**.
    - **Nicht konfiguriert**. Standardmäßig ist die Audioumleitung mit hoher Qualität oder zuvor konfigurierten benutzerdefinierten Audioeinstellungen aktiviert.
    - **Aktiviert.** Aktiviert die Audioumleitung mit den ausgewählten Optionen.
    - **Deaktiviert.** Deaktiviert die Audioumleitung.
4. Wenn Sie **Aktiviert** eingestellt haben, wählen Sie eine Tonqualität. Verwenden Sie für UDP-Audio die Standardeinstellung **Mittel**.
5. Aktivieren Sie nur für UDP-Audio die Einstellung **Real-Time Transport** und legen Sie den Bereich der eingehenden Ports so fest, dass der Durchgang durch die lokale Windows Firewall gewährleistet ist.
6. Zur Verwendung von UDP-Audio mit Citrix Gateway wählen Sie die Option **Echtzeittransport über Gateway zulassen**. Konfigurieren Sie Citrix Gateway mit DTLS. Weitere Informationen finden Sie in diesem Artikel.

Wenn Sie als Administrator auf Endpunktgeräten solche Änderungen nicht vornehmen können, aktivieren Sie UDP-Audio über die default.ica-Attribute von StoreFront. Beispiel: BYOD-Geräte oder Heimcomputer.

1. Öffnen Sie auf der Maschine mit StoreFront die Datei C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica in einem Texteditor.
2. Fügen Sie unter dem Abschnitt [Application] Folgendes hinzu:

   ; aktiviert Real-Time Transport

   EnableRtpAudio=true

   ; aktiviert Real-Time Transport über Gateway

   EnableUDPThroughGateway=true

   ; legt die Audioqualität auf "Mittel"fest

   AudioBandwidthLimit=1

   ; UDP-Portbereich

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Wird UDP-Audio über die Datei default.ica aktiviert, gilt die Aktivierung für alle Benutzer des Stores.

### Vermeiden von Echo in Multimediakonferenzen

Teilnehmer von Audio- oder Videokonferenzen hören eventuell ein Echo. Echos treten normalerweise auf, wenn der Abstand zwischen Lautsprechern und Mikrofonen nicht groß genug ist. Aus diesem Grund empfiehlt Citrix, dass Sie für Audio- und Videokonferenzen Kopfhörer verwenden.

HDX verfügt über eine Option zur Echounterdrückung (standardmäßig aktiviert), die das Auftreten von Echo minimiert. Die Qualität der Echounterdrückung hängt stark vom Abstand zwischen den Lautsprechern und dem Mikrofon ab. Stellen Sie sicher, dass die Geräte nicht zu nah beieinander oder zu weit voneinander entfernt sind.

Sie können eine Registrierungseinstellung ändern, um die Echounterdrückung zu deaktivieren. Weitere Informationen finden Sie unter Vermeiden von Echo in Multimediakonferenzen in der Liste der über die Registrierung verwalteten Features.

### Softphones

Eine Softphone ist Software, die als Telefonbenutzeroberfläche fungiert. Mit einem Softphone können Anrufe von einem Computer oder einem anderen Gerät über das Internet getätigt werden. Das

Softphone ermöglicht das Wählen einer Telefonnummer und die Nutzung weiterer Telefonfunktionen über einen Bildschirm.

Citrix Virtual Apps and Desktops unterstützt verschiedene Bereitstellungsmethoden für Softphones.

- **Steuermodus:** Das gehostete Softphone steuert ein physisches Telefon. In diesem Modus werden keine Audiodaten über den Citrix Virtual Apps and Desktops-Server gesendet.
- **Softphone-Unterstützung mit HDX RealTime-Optimierung (empfohlen).** Die Media Engine wird auf dem Benutzergerät ausgeführt und der VoIP-Datenverkehr erfolgt Peer-to-Peer. Beispiele:
  - HDX-Optimierung für Microsoft Teams
  - HDX RealTime Optimization Pack zur Optimierung der Bereitstellung von Microsoft Skype for Business.
  - Cisco Jabber Softphone für VDI (früher VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (früher VDI Communicator)
  - Zoom-VDI-Plug-In
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic-Diktiergerät
- **Lokaler App-Zugriff:** Feature in Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service), welche die lokale Ausführung von Softphones und ähnlichen Anwendungen auf dem Windows-Gerät eines Benutzers ermöglicht, wobei die Anwendung nahtlos in dessen virtuellen/veröffentlichten Desktop integriert erscheint. Dadurch wird die gesamte Audioverarbeitung auf das Benutzergerät übertragen. Weitere Informationen finden Sie unter Lokaler App-Zugriff und URL-Umleitung.
- **Generische Softphone-Unterstützung mit HDX RealTime-Optimierung:** VoIP über ICA:

***Generische Softphone-Unterstützung***

Mit der generischen Softphone-Unterstützung können Sie ein unverändertes Softphone unter XenApp oder XenDesktop im Datencenter hosten. Für den Audiodatenverkehr an das Benutzergerät mit der Citrix Workspace-App wird das Citrix ICA-Protokoll (vorzugsweise mit UDP/RTP) verwendet.

Die generische Softphone-Unterstützung ist ein Feature von HDX RealTime. Diese Art der Softphone-Bereitstellung eignet sich besonders in folgenden Fällen:

- Wenn keine optimierte Lösung für die Softphone-Bereitstellung zur Verfügung steht und der Benutzer kein Windows-Gerät verwendet, auf dem der lokale App-Zugriff verwendet werden kann
- Wenn die Media Engine für die optimierte Softphone-Bereitstellung nicht auf dem Benutzergerät installiert ist oder für dessen Betriebssystemversion nicht verfügbar ist In diesem Szenario ist die generische Unterstützung mit HDX RealTime eine nützliche Fallback-Lösung.

Bei der Softphone-Bereitstellung mit Citrix Virtual Apps and Desktops sind zwei Punkte zu beachten:

- Art der Bereitstellung des Softphones auf dem virtuellen/veröffentlichten Desktop
- Art der Übermittlung der Audiodaten zwischen dem Kopfhörer, Mikrofon, Lautsprecher und/oder USB-Telefon des Benutzers

Citrix Virtual Apps and Desktops umfasst zahlreiche Technologien für die generische Softphone-Bereitstellung:

- Sprachoptimierter Codec zur schnellen und bandbreiteneffizienten Echtzeit-Audiocodierung
- Audio Stack mit geringer Latenz
- Serverseitiger Jitter-Puffer zur Audiooptimierung bei schwankender Netzwerklatenz
- Paket-Markierung (DSCP und WMM) für Servicequalität
  - DSCP-Markierung für RTP-Pakete (Layer-3)
  - WMM-Markierung für WLAN

Die Citrix Workspace-App-Versionen für Windows, Linux, Chrome und Mac sind auch VoIP-fähig. Die Citrix Workspace-App für Windows bietet die folgenden Features:

- Clientseitiger Jitter-Puffer zur Audiooptimierung bei schwankender Netzwerklatenz
- Echounterdrückung, die größere Unterschiede beim Abstand zwischen Mikrofon und Lautsprecher ausgleicht, wenn Mitarbeiter kein Headset verwenden
- Audio-Plug & Play, sodass Audiogeräte nicht vor Sitzungsstart angeschlossen werden müssen. Sie können jederzeit angeschlossen werden.
- Audiogeräterouting, sodass die Benutzer den Klingelton an den Lautsprecher und die Sprachausgabe an ihr Headset senden können
- Multistream-ICA für ein flexibles, servicebasiertes Routing über das Netzwerk
- ICA unterstützt vier TCP- und zwei UDP-Streams. Einer der UDP-Streams unterstützt Echtzeit-Audio über RTP.

Eine Übersicht über die Funktionen der Citrix Workspace-App finden Sie in der Citrix Receiver-Featurematrix.

***Empfehlungen für die Systemkonfiguration***

*Clienthardware und -software:*
Zur Gewährleistung der optimalen Audioqualität empfiehlt Citrix die Verwendung der aktuellen Citrix Workspace-App-Version und eines hochwertigen Headsets mit akustischer Echounterdrückung (AEC). Die Citrix Workspace-App-Versionen für Windows, Linux und Mac unterstützen VoIP. Dell Wyse bietet überdies VoIP-Unterstützung für ThinOS (WTOS).

*CPU:*
Überwachen Sie die CPU-Auslastung auf dem VDA, um festzustellen, ob jeder virtuellen Maschine zwei virtuelle CPUs zugewiesen werden müssen. Echtzeit Sprach- und Videoanrufe sind datenintensiv.

Durch Konfigurieren von zwei virtuellen CPUs wird die Latenz beim Threadwechsel reduziert. Daher wird empfohlen, dass Sie in einer Citrix Virtual Desktops-VDI-Umgebung zwei virtuelle CPUs konfigurieren.

Die Konfiguration von zwei virtuellen CPUs bedeutet nicht unbedingt die Verdoppelung der Zahl physischer CPUs, da diese von Sitzungen geteilt werden können.

Auch das für die Sitzungszuverlässigkeit verwendete Citrix Gateway Protocol (CGP) erhöht den CPU-Verbrauch. Bei Netzwerkverbindungen mit hoher Qualität können Sie dieses Feature zum Verringern des CPU-Verbrauchs auf dem VDA deaktivieren. Auf einem leistungsstarken Server ist evtl. keiner der o. g. Schritte erforderlich.

*UDP-Audio:*
Audio über UDP bietet eine hervorragende Toleranz bei starker Netzwerklast und Paketverlusten. Citrix empfiehlt die Verwendung anstelle von TCP, sofern möglich.

*LAN/WAN-Konfiguration:*
Die richtige Konfiguration des Netzwerks ist für eine gute Echtzeit-Audioqualität unerlässlich. Normalerweise müssen Sie virtuelle LANs (VLANs) konfigurieren, da eine hohe Zahl Broadcastpakete Jitter verursachen können. IPv6-aktivierte Geräte können eine hohe Zahl Broadcastpakete generieren. Wenn IPv6 nicht erforderlich ist, können Sie es auf den Geräten deaktivieren. Konfigurieren Sie es für Servicequalitätszwecke.

*Einstellungen für WAN-Verbindungen:*
Sie können Sprach-Chat über das lokale Netzwerk (LAN) und ein Wide Area Network (WAN) verwenden. Bei WAN-Verbindungen hängt die Audioqualität von der Latenz, Paketverlust und Jitter ab. Für die Bereitstellung von Softphones über eine WAN-Verbindung empfiehlt Citrix die Verwendung von NetScaler SD-WAN zwischen dem Datencenter und dem Remotestandort. Dies gewährleistet eine hohe Servicequalität. NetScaler SD-WAN unterstützt Multistream-ICA und UDP. Bei TCP-Einzelstreams kann überdies die Priorität der verschiedenen virtuellen ICA-Kanäle unterschieden werden, um sicherzustellen, dass Echtzeit-Audiodaten mit hoher Priorität bevorzugt werden.

Verwenden Sie Director oder HDX Monitor zum Überprüfen der HDX-Konfiguration.

*Remotebenutzerverbindungen:*
Citrix Gateway unterstützt DTLS für die native (ohne TCP-Einkapselung) Bereitstellung von UDP/RTP-Datenverkehr.
Öffnen Sie Firewalls bidirektional für UDP-Datenverkehr über Port 443.

*Codec-Auswahl und Bandbreitenverbrauch*:
Für den Datenverkehr zwischen dem Benutzergerät und dem VDA im Datencenter empfiehlt Citrix, die Codec-Einstellung **Sprachoptimiert** (= mittlere Audioqualität) zu verwenden. Zwischen VDA und IP-Telefon verwendet das Softphone den konfigurierten oder ausgehandelten Codec. Beispiel:

- G711 bietet eine gute Sprachqualität, erfordert jedoch eine Bandbreite von 80 bis 100 Kilobit pro Sekunde und Anruf (abhängig vom Overhead in Netzwerkschicht 2).

- G729 bietet eine gute Sprachqualität bei geringer Bandbreitennutzung von 30 bis 40 Kilobit pro Sekunde und Anruf (abhängig vom Overhead in Netzwerkschicht 2).

***Bereitstellung von Softphone-Anwendungen auf dem virtuellen Desktop***

Es gibt zwei Methoden zur Bereitstellung von Softphones auf virtuellen XenDesktop-Desktops:

- Die Anwendung kann auf dem virtuellen Desktopimage installiert werden.
- Die Anwendung kann mit Microsoft App-V an den virtuellen Desktop gestreamt werden. Diese Methode ist verwaltungsmäßig besser, da das virtuelle Desktopimage übersichtlich bleibt. Nach dem Streaming an den virtuellen Desktop wird die Anwendung so ausgeführt, als wäre sie normal installiert worden. Nicht alle Anwendungen sind mit App-V kompatibel.

***Übertragen von Audiodaten auf Benutzergeräten***

Generisches HDX RealTime unterstützt zwei Methoden der Audiobereitstellung für Benutzergeräte:

- **Citrix Audio Virtual Channel:** Citrix Audio Virtual Channel wird von Citrix normalerweise empfohlen, da es speziell für die Audioübertragung entwickelt wurde.
- **Generische USB-Umleitung:** unterstützt Audiogeräte mit Tasten und/oder Bildschirm, wenn zwischen Benutzergerät und Citrix Virtual Apps and Desktops-Server eine LAN- oder LAN-ähnliche Verbindung besteht.

***Citrix Audio Virtual Channel***

Der bidirektionale Citrix Audio Virtual Channel (CTXCAM) ermöglicht die effiziente Audioübertragung über das Netzwerk. Mit generischem HDX RealTime werden Audiodaten vom Headset oder Mikrofon des Benutzers komprimiert. Sie werden dann über ICA an die Softphone-Anwendung auf dem virtuellen Desktop gesendet. Die Audioausgabe des Softphones wird ebenfalls komprimiert und in die Gegenrichtung gesendet. Diese Komprimierung ist unabhängig von der Komprimierung des Softphones selbst (z. B. G.729 oder G.711). Sie erfolgt unter Einsatz des sprachoptimierten Codec (mittlere Qualität). Die Eigenschaften sind ideal für VoIP (Voice-over-IP). Die Codierung ist schnell und die Netzwerkbandbreite ist mit nur ca. 56 Kilobit pro Sekunde (28 Kbit/s in jede Richtung) gering. Dieser Codec muss in der Verwaltungskonsole des Diensts ausgewählt werden, da er nicht standardmäßig aktiviert ist. Der Standard-Codec ist HD-Audio (hohe Qualität). Der Codec eignet sich hervorragend für Hi-Fi-Stereosound, ist aber im Vergleich zum sprachoptimierten Codec langsamer.

***Generische USB-Umleitung***

Die generische USB-Umleitung von Citrix (CTXGUSB –virtueller Kanal) bietet eine generische Methode für das Remoting von USB-Geräten, auch für Kombi-Geräte (Audio plus Eingabegerät) sowie isochrone USB-Geräte. Dieser Ansatz beschränkt sich auf Benutzer im LAN. Der Grund dafür ist, dass das USB-Protokoll latenzempfindlich ist und eine beträchtliche Netzwerkbandbreite erfordert. Die isochrone USB-Umleitung funktioniert bei einigen Softphones gut. Diese Umleitung bietet eine hervorragende Sprachqualität und geringe Latenz. Citrix Audio Virtual Channel wird jedoch

bevorzugt, da es für Audiodatenverkehr optimiert ist. Die primäre Ausnahme bildet die Verwendung von Audiogeräten mit Tasten. Beispiel: ein an ein mit dem Datenzentrum über LAN verbundenes Benutzergerät angeschlossenes USB-Telefon. Die generische USB-Umleitung unterstützt in diesem Fall Tasten auf dem Telefon oder Headset zur Steuerung von Features unter Rückgabe eines Signals an das Softphone. Es besteht kein Problem bei Tasten, die lokal auf dem Gerät funktionieren.

### Einschränkung

Nachdem Sie ein Audiogerät auf Ihrem Client installiert, die Audioumleitung aktiviert und eine RDS-Sitzung gestartet haben, schlägt die Wiedergabe von Audiodateien möglicherweise fehl. Fügen Sie als Workaround den Registrierungsschlüssel auf der RDS-Maschine hinzu und starten Sie diese anschließend neu. Weitere Informationen finden Sie unter Audio-Einschränkung in der Liste der über die Registrierung verwalteten Features.

## Umleitung des Browserinhalts

June 30, 2022

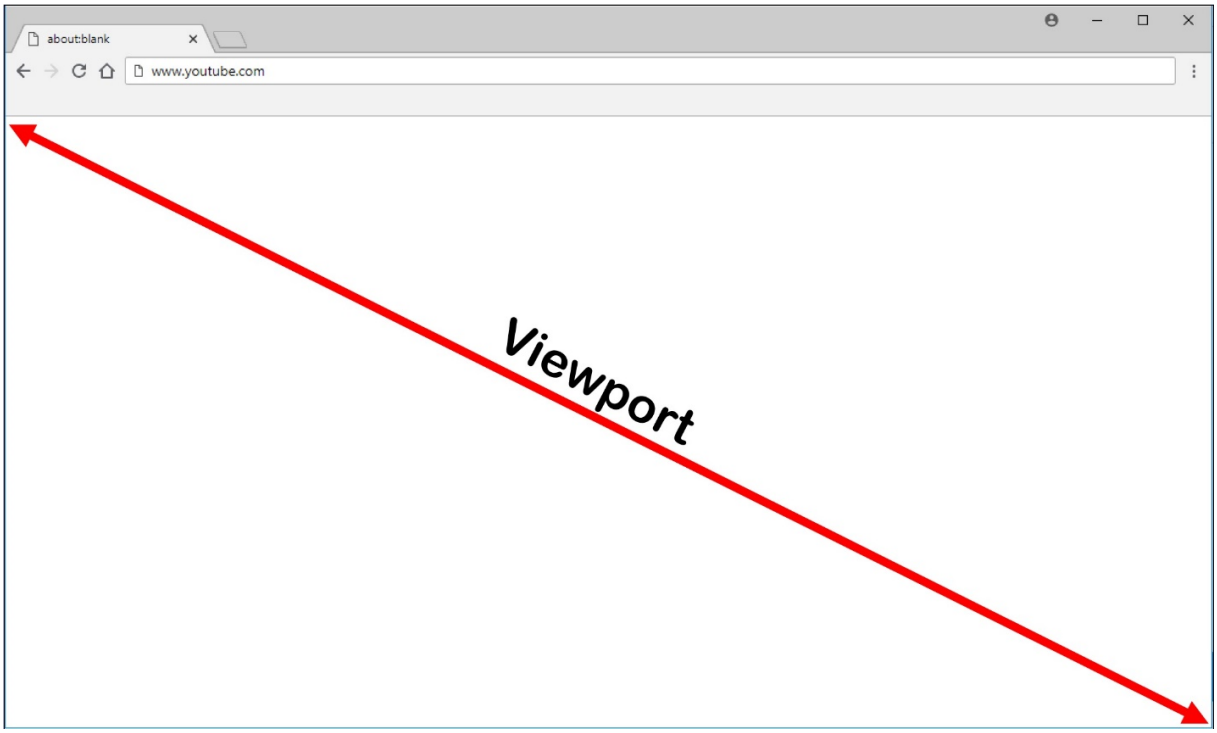
Die Umleitung des Browserinhalts verhindert die VDA-seitige Wiedergabe von Webseiten auf einer Positivliste. Dabei wird von der Citrix Workspace-App clientseitig die Instanz einer entsprechenden Renderingengine erzeugt, die den HTTP- und HTTPS-Inhalt von der URL abruft.

> **Hinweis:**
>
> Sie können festlegen, dass Webseiten mithilfe einer Sperrliste an den VDA (jedoch nicht clientseitig) umgeleitet werden.

Diese Overlay-Weblayoutengine wird statt auf dem VDA auf dem Endpunktgerät ausgeführt und verwendet dessen CPU, GPU, Arbeitsspeicher und Netzwerk.

Es wird nur der Browserviewport umgeleitet. Der Viewport ist der rechteckige Browserbereich, in dem der Inhalt angezeigt wird. Der Viewport enthält keine Elemente wie Adressleiste, Favoriten-Symbolleiste und Statusleiste. Diese Elemente sind Teil der Benutzeroberfläche und werden weiterhin auf dem VDA im Browser ausgeführt.



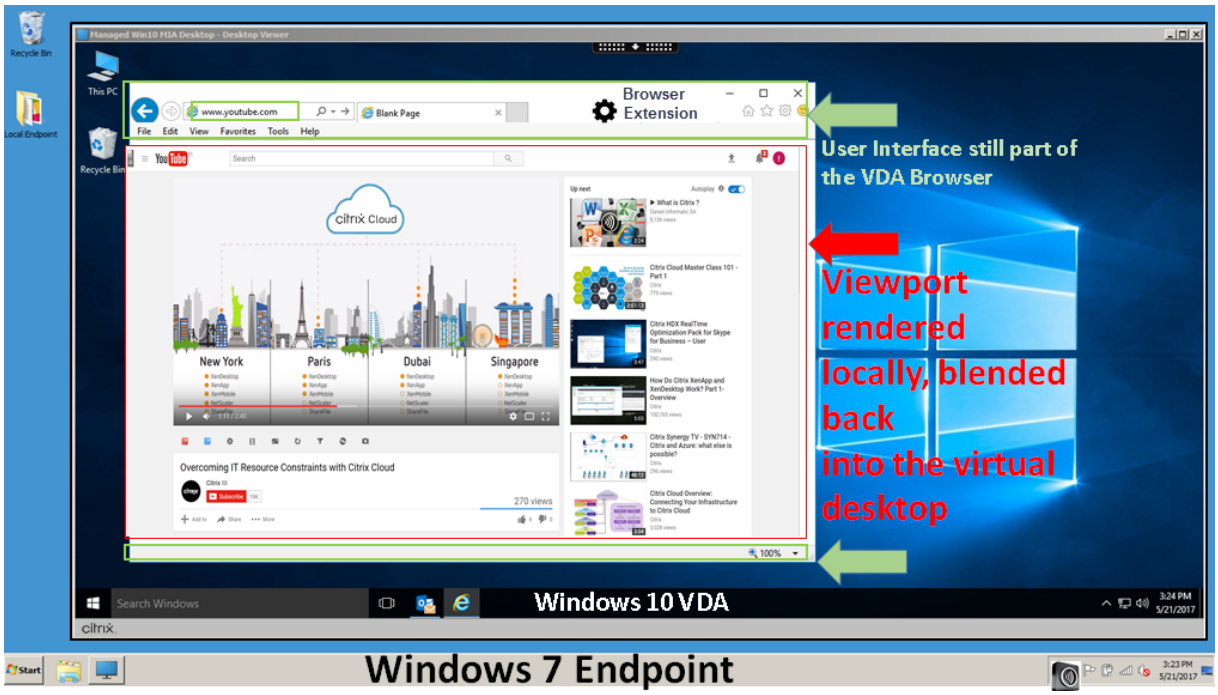

1. Konfigurieren Sie in der Oberfläche “Verwalten > Vollständige Konfiguration”eine Richtlinie, in der die Zugriffssteuerungsliste mit der Positivliste oder der Sperrliste der URLs für die Umleitung angegeben wird. Der Browser auf dem VDA führt den Abgleich der von den Benutzern angesteuerten URLs gegen die Positiv- oder Sperrliste mit einer Browsererweiterung durch. Die Browsererweiterung (BHO) für Internet Explorer 11 ist auf dem Installationsmedium enthalten und wird automatisch installiert. Die Browsererweiterung für Chrome steht im Chrome Web Store zur Verfügung und kann über Gruppenrichtlinien und ADMX-Dateien bereitgestellt werden. Chrome-Erweiterungen werden für einzelne Benutzer installiert. Das Update eines Gold-Masterimages zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich.
2. Wird eine Übereinstimmung in der Positivliste gefunden (z. B. `https://www.mycompany.com/`) und keine Übereinstimmung mit einer URL in der Sperrliste (z. B. `https://www.mycompany.com/engineering`), weist ein virtueller Kanal (CTXCSB) die Citrix Workspace-App an, dass eine Umleitung erforderlich ist und leitet die URL weiter. Die Citrix Workspace-App erzeugt dann eine lokale Renderingengine-Instanz und zeigt die Website an.
3. Anschließend fügt die Citrix Workspace-App die Website nahtlos in den Inhaltsbereich des virtuellen Desktopbrowsers ein.

Die Farbe des Logos gibt den Status der Chrome-Erweiterung an. Folgende drei Farben sind möglich:

- Grün: Aktiv und verbunden.
- Grau: Nicht aktiv/Leerlauf auf der aktuellen Registerkarte.
- Rot: Defekt/außer Betrieb.

Sie können Debugprotokolle mit den **Optionen** im Erweiterungsmenü festlegen.




Szenarien für den Inhaltsabruf durch die Citrix Workspace-App:

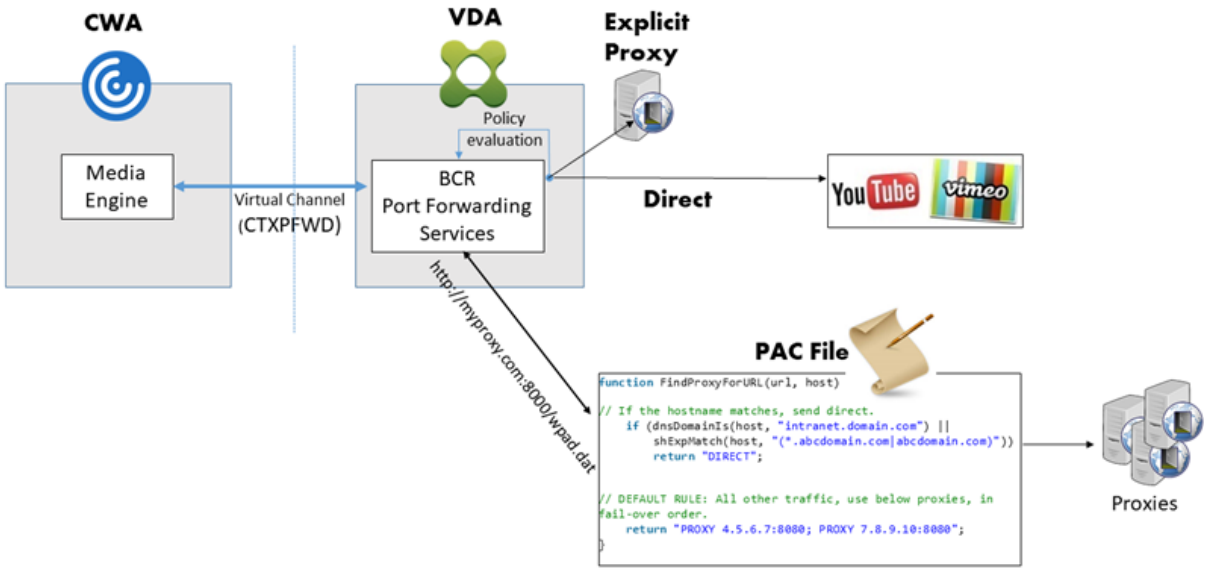
- **Abruf und Wiedergabe auf dem Server:** Es findet keine Umleitung statt, weil die Site nicht auf der Positivliste steht oder ein Fehler aufgetreten ist. Die Wiedergabe findet dann auf dem VDA statt und das Grafikremoting mithilfe von Thinwire. Verwenden Sie Richtlinien, um dieses Fallbackverhalten zu steuern. Es fällt ein hoher CPU-, RAM- und Bandbreitenverbrauch auf dem VDA an.
- **Abruf auf dem Server, Wiedergabe auf dem Client:** Die Citrix Workspace-App ruft den Inhalt über den VDA und einen virtuellen Kanal (CTXPFWD) vom Webserver ab. Diese Option ist nützlich, wenn Clients keinen Internetzugriff haben (z. B. Thin Clients). Der CPU- und RAM-Verbrauch auf dem VDA ist niedrig, jedoch wird Bandbreite im virtuellen ICA-Kanal verbraucht.

  Es gibt drei Betriebsmodi für dieses Szenario. Der Begriff “Proxy”bezieht sich hier auf ein Proxygerät, das der VDA für den Internetzugriff verwendet.

  Geeignete Richtlinienoption:

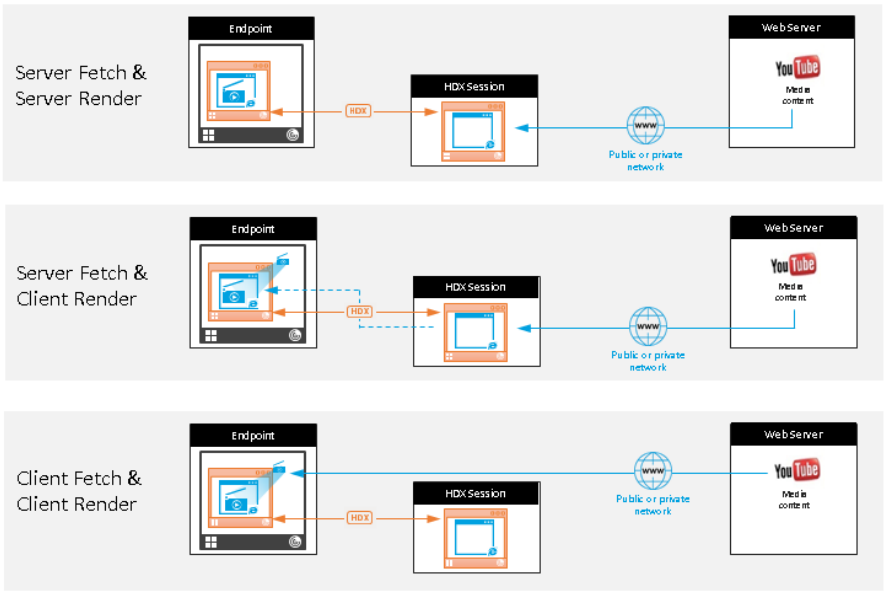
  - Expliziter Proxy: Wenn Sie einen einzelnen expliziten Proxy im Datencenter haben.
  - Direkt oder transparent - Wenn Sie keine Proxys haben oder transparente Proxys verwenden.
  - PAC-Dateien - Wenn Sie PAC-Dateien verwenden, sodass Browser auf dem VDA automatisch den geeigneten Proxyserver zum Abrufen einer angegebenen URL auswählen können.




- **Abruf und Wiedergabe auf dem Client:** Da die Citrix Workspace-App direkt auf den Webserver zugreift, ist Internetzugriff erforderlich. In diesem Szenario wird die gesamte Netzwerk-, CPU- und RAM-Last von der XenApp und XenDesktop-Site abgeladen.

## Redirection scenarios




**Benefits:**

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

**Fallbackmechanismus:**

Es kann vorkommen, dass die Clientumleitung fehlschlägt. Wenn der Client beispielsweise keinen direkten Internetzugriff hat, kann eine Fehlerantwort an den VDA zurückgegeben werden. In einem

solchen Fall kann der Browser auf dem VDA die Seite auf dem Server neu laden und wiedergeben.

Verwenden Sie die Richtlinie **Verhindern von Fallback auf Windows Media**, um eine serverseitige Wiedergabe von Videoelementen zu verhindern. Legen Sie diese Richtlinie auf **Alle Inhalte nur auf Client wiedergeben** oder **Nur Inhalte auf Client wiedergeben, auf die Client Zugriff hat** fest. Diese Einstellungen verhindern die Wiedergabe von Videoelementen auf dem Server, wenn die Clientumleitung fehlschlägt. Diese Richtlinie wird nur wirksam, wenn Sie die Browserinhaltsumleitung aktivieren und die Richtlinie **Zugriffssteuerungsliste** die URL für ein Fallback enthält. Die URL darf nicht Teil der Sperrlistenrichtlinie sein.

**Systemanforderungen:**

Windows-Endpunkte:

- Windows 10 oder 11
- Citrix Workspace-App 1809 für Windows oder höher

> **Hinweis:**
>
> Die Browserinhaltsumleitung wird nur im aktuellen Release der Citrix Workspace-App für Windows unterstützt, nicht jedoch in den LTSR-Releases 1912 und 2203.1 der Citrix Workspace-App.

Linux-Endpunkte:

- Citrix Workspace-App 1808 für Linux oder später
- Citrix Receiver für Linux 13.9 oder später
- Thin Client-Terminals müssen WebKitGTK+ enthalten.

Citrix Virtual Apps and Desktops 7 1808 und XenApp und XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- VDA-Betriebssystem: Windows 10 (mindestens Version 1607), Windows Server 2012 R2, Windows Server 2016
- Browser auf dem VDA:
  - Google Chrome v66 oder höher (Chrome erfordert Citrix Workspace-App 1809 für Windows auf dem Benutzerendpunkt, Citrix Virtual Apps and Desktops 7 1808-VDA und Erweiterung für die Browserinhaltsumleitung)
  - Explorer 11 mit folgender Konfiguration:
    - Deaktivieren von **Erweiterter geschützter Modus** unter **Internetoptionen** > **Erweitert > Sicherheit**
    - Aktivieren von **Browsererweiterungen von Drittanbietern aktivieren** unter **Internetoptionen > Erweitert > Browsen**

## Problembehandlung

Informationen zur Problembehandlung finden Sie im Knowledge Center-Artikel https://support.citrix.com/article/CTX230052.

## Chrome-Erweiterung für die Browserinhaltsumleitung

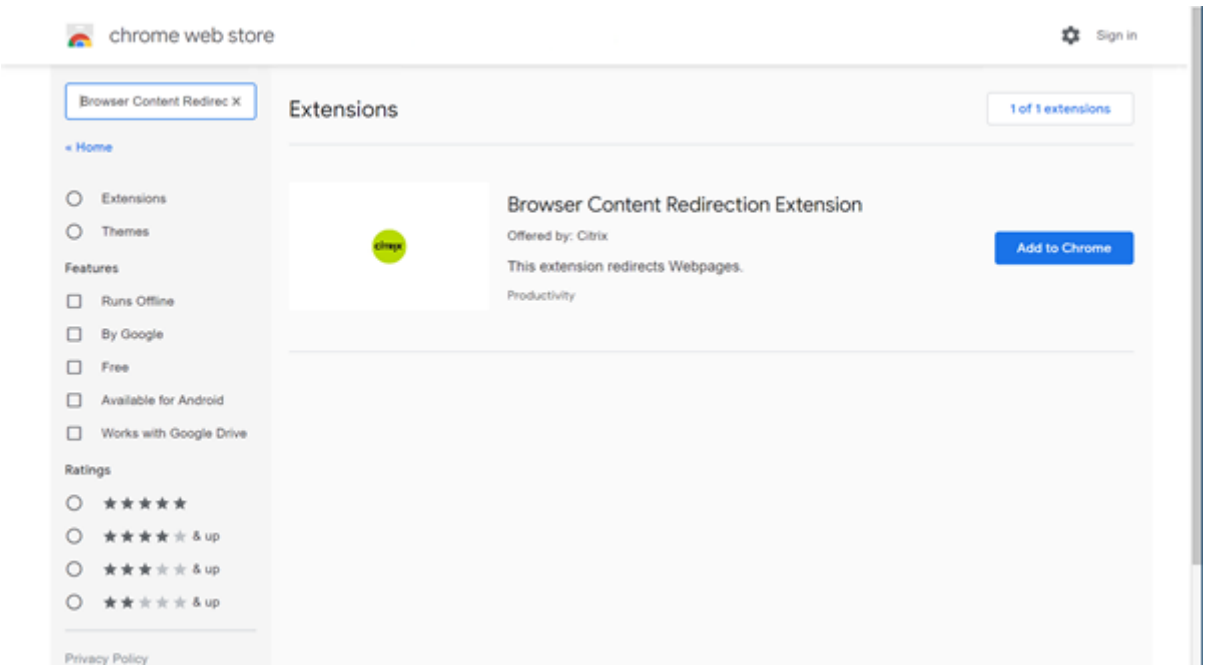
Zur Verwendung der Browserinhaltsumleitung in Chrome fügen Sie die entsprechende Browsererweiterung aus dem Chrome Web Store hinzu. Klicken Sie auf **Zu Chrome hinzufügen** in der Citrix Virtual Apps and Desktops-Umgebung.

Die Erweiterung ist nur auf dem VDA und **nicht** auf dem Client des Benutzers erforderlich.

### Systemanforderungen

- Chrome v66 oder höher
- Erweiterung für die Browserinhaltsumleitung
- Citrix Virtual Apps and Desktops 7 1808 oder höher
- Citrix Workspace-App 1809 für Windows oder höher

> **Hinweis:**
>
> Die Browserinhaltsumleitung wird nur im aktuellen Release der Citrix Workspace-App für Windows unterstützt, nicht jedoch in den LTSR-Releases 1912 und 2203.1 der Citrix Workspace-App.

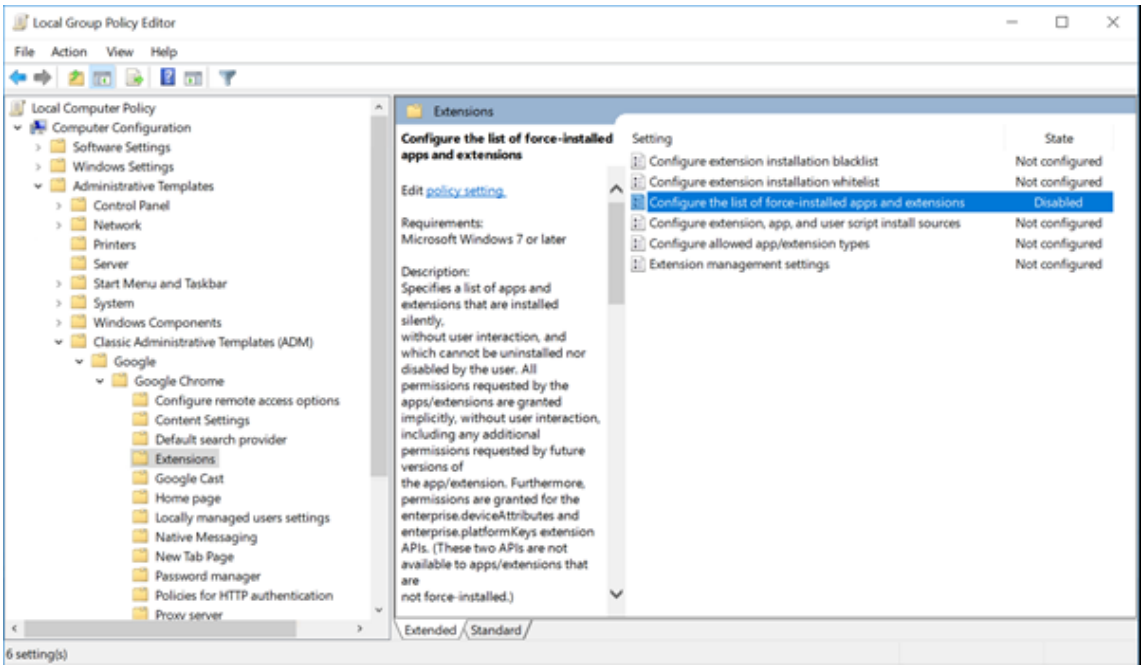


Diese Methode funktioniert für einzelne Benutzer. Um die Erweiterung für eine große Benutzergruppe bereitzustellen, verwenden Sie die Gruppenrichtlinie.

**Bereitstellen der Erweiterung per Gruppenrichtlinie**

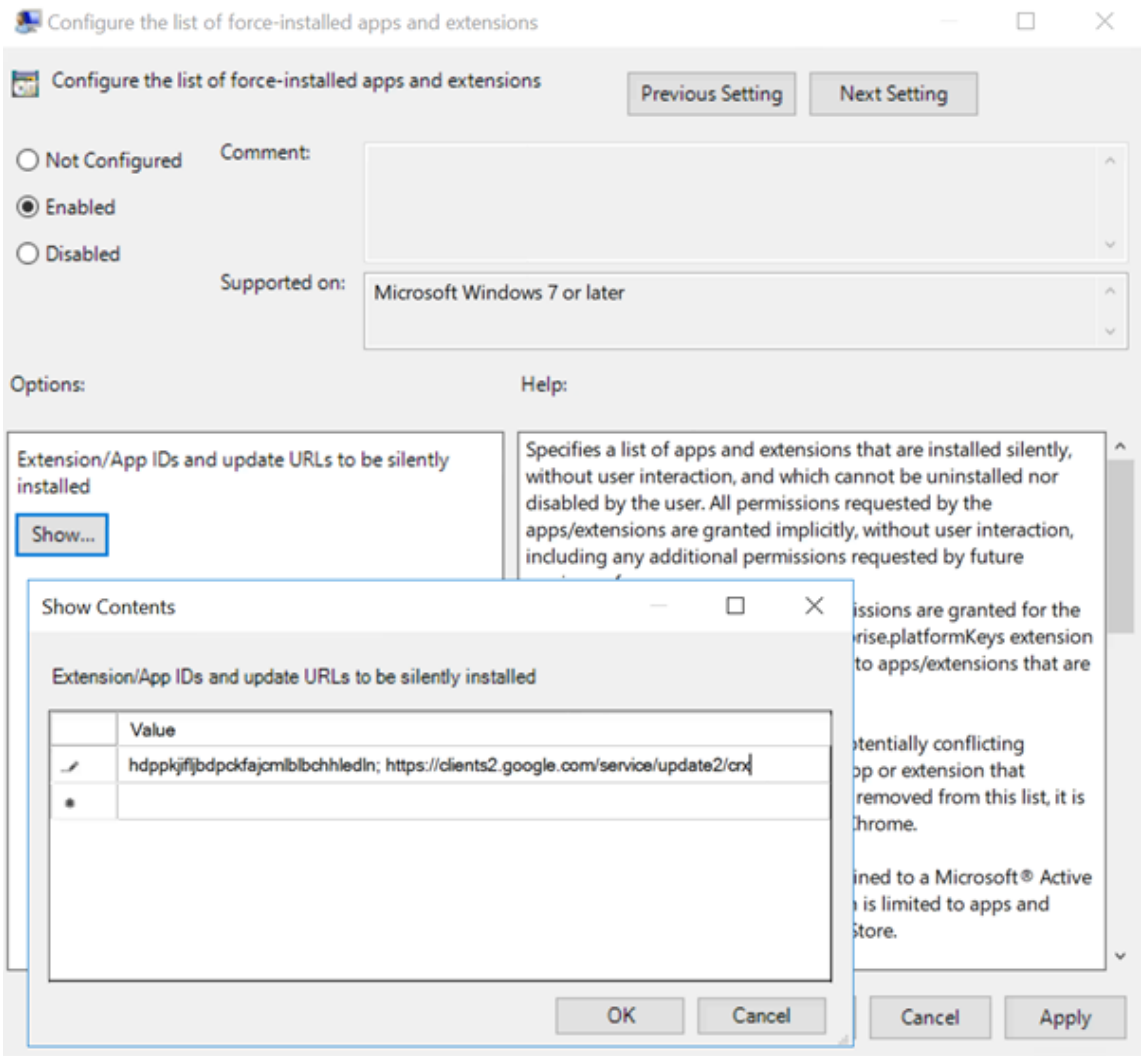
1. Importieren Sie die Google Chrome-ADMX-Dateien in Ihre Umgebung. Informationen zum Herunterladen, Installieren und Konfigurieren von Richtlinienvorlagen im Gruppenrichtlinien-Editor finden Sie unter Set Chrome Browser policies on managed PCs.
2. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole und wechseln Sie zu **Benutzerkonfiguration\Administrative Vorlagen\Klassische administrative Vorlage (ADM)\Google\Google Chrome\Erweiterungen**. Aktivieren Sie die Einstellung **Configure the list of force-installed apps and extensions**.




3. Klicken Sie auf **Show** und geben Sie die folgende Zeichenfolge ein (= Erweiterungs-ID). Aktualisieren Sie die URL für die Browserinhaltsumleitungserweiterung.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```




4. Übernehmen Sie die Einstellung. Nach einer **gpudate**-Aktualisierung erhält der Benutzer automatisch die Erweiterung. Beim Starten des Chrome-Browsers in der Benutzersitzung wird die Erweiterung angewendet und kann vom Benutzer nicht entfernt werden.

   Alle Updates der Erweiterung werden automatisch auf den Maschinen der Benutzer über die Update-URL installiert, die Sie in der Einstellung angegeben haben.

   Wird für die Einstellung **Configure the list of force-installed apps and extensions** der Wert **Disabled** festgelegt, wird die Erweiterung automatisch für alle Benutzer entfernt.

### Edge Chromium-Erweiterung für die Browserinhaltsumleitung

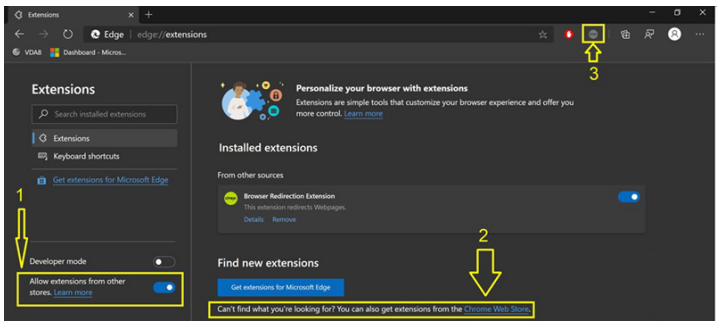
Um die Erweiterung zur Browserinhaltsumleitung in Edge zu installieren, müssen Sie Version **83.0.478.37** oder höher des Edge-Browsers verwenden.

1. Klicken Sie im Menü auf die Option **Extensions**, und aktivieren Sie **Allow extensions from other**

**stores**.

2. Klicken Sie auf den Link **Chrome Web Store** und die Erweiterung wird in der Leiste oben rechts angezeigt.
   Weitere Informationen zu Microsoft Edge-Erweiterungen finden Sie unter Erweiterungen.




## Umleitung des Browserinhalts und DPI

Bei Verwendung der Browserinhaltsumleitung mit einer DPI-Skalierung von mehr als 100 % auf der Maschine des Benutzers wird der umgeleitete Browserinhalt fehlerhaft angezeigt. Richten Sie die DPI nicht ein, wenn Sie die Browserinhaltsumleitung verwenden, um dieses Problem zu vermeiden. Alternativ können Sie die GPU-Beschleunigung der Browserinhaltsumleitung für Chrome deaktivieren, indem Sie den Registrierungsschlüssel auf der Maschine des Benutzers erstellen. Weitere Informationen finden Sie unter Umleitung des Browserinhalts und DPI in der Liste der über die Registrierung verwalteten Features.

## User-Agent-Anforderungsheader

Der User-Agent-Header hilft bei der Identifizierung von HTTP-Anforderungen, die von der Browserinhaltsumleitung gesendet werden. Diese Einstellung kann beim Konfigurieren von Proxy- und Firewallregeln nützlich sein. Wenn der Server beispielsweise von der Browserinhaltsumleitung gesendete Anforderungen blockiert, können Sie eine Regel mit dem User-Agent-Header zum Umgehen bestimmter Anforderungen erstellen.

Nur Windows-Geräte unterstützen den User-Agent-Anforderungsheader.

Standardmäßig ist die Zeichenfolge des User-Agent-Anforderungsheaders deaktiviert. Zum Aktivieren des User-Agent-Headers für vom Client gerenderte Inhalte verwenden Sie den Registrierungs-Editor. Weitere Informationen finden Sie unter User-Agent-Anforderungsheader in der Liste der über die Registrierung verwalteten Features.

# HDX-Videokonferenzen und Webcam-Videokomprimierung

April 1, 2022

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Webcams können in Anwendungen, die innerhalb virtueller Sitzungen ausgeführt werden, unter Einsatz der HDX-Webcamvideokomprimierung oder der per HDX Plug-n-Play verfügbaren generischen USB-Umleitung verwendet werden. Verwenden Sie **Citrix Workspace-App > Einstellungen > Geräte** zum Umschalten zwischen diesen Modi. Citrix empfiehlt, nach Möglichkeit die HDX-Webcamvideokomprimierung zu verwenden. Die generische HDX-USB-Umleitung wird nur empfohlen, wenn Probleme mit der Anwendungskompatibilität bei der HDX-Videokomprimierung auftreten oder wenn Sie erweiterte native Funktionen der Webcam nutzen müssen. Für eine bessere Leistung empfiehlt Citrix, den Virtual Delivery Agent mit mindestens zwei virtuellen CPUs zu konfigurieren.

Um zu verhindern, dass Benutzer die HDX-Webcamvideokomprimierung ändern, deaktivieren Sie die Umleitung von USB-Geräten über die Richtlinieneinstellungen unter **ICA > USB-Geräte**. Citrix Workspace-App-Benutzer können das Standardverhalten außer Kraft setzen, wenn sie in Desktop Viewer unter “Mikrofon & Webcam”die Einstellung **Mikrofon und Webcam nicht verwenden** auswählen.

## HDX-Webcamvideokomprimierung

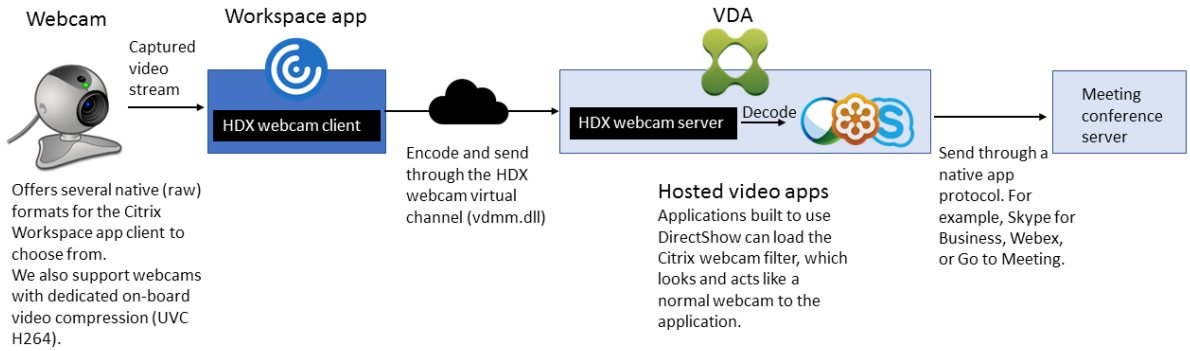
Die HDX-Webcamvideokomprimierung wird auch als **optimierter** Webcammodus bezeichnet. Bei dieser Art der Webcamvideokomprimierung wird das H.264-Video direkt an die Videokonferenzanwendung gesendet, die in der virtuellen Sitzung ausgeführt wird. Zum Optimieren von VDA-Ressourcen wird das Webcamvideo von der HDX-Webcamkomprimierung nicht codiert, transcodiert und decodiert. Das Feature ist in der Standardeinstellung aktiviert.

Um das direkte Videostreaming vom Server zur Videokonferenz-App zu deaktivieren, legen Sie den Registrierungsschlüssel im VDA auf “0”fest. Weitere Informationen finden Sie unter Webcamvideokomprimierung in der Liste der Features, die über die Registrierung verwaltet werden.

Wenn Sie die Standardfunktion zum Streaming von Videoressourcen deaktivieren, verwendet die HDX-Webcamvideokomprimierung die Multimediaframework-Technologie des Clientbetriebssystems, um Video von Aufnahmegeräten zu erfassen, zu transcodieren und zu komprimieren. Hersteller von Aufnahmegeräten liefern die Treiber, die sich in die Betriebssystem-Kernelstreaming-Architektur einfügen.

Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet Videos nur an Server, die es ordnungsgemäß anzeigen können. Der Server ist nicht direkt mit der Webcam verbunden, seine Integration sorgt jedoch dafür, dass die gleiche Erfahrung auf dem Desktop geliefert wird. Die Workspace-App komprimiert Videos zum Einsparen von Bandbreite und zur Gewährleistung einer besseren Ausfallsicherheit in WANs.




HDX-Webcam-Videokomprimierung erfordert, dass die folgenden Richtlinieneinstellungen aktiviert sind (alle sind standardmäßig aktiviert).

- Multimediakonferenzen
- Windows Media-Umleitung

Bei Hardware-verschlüsselungsfähigen Webcams verwendet HDX-Videokomprimierung die Hardware-Codierung standardmäßig. Die Hardwarecodierung kann mehr Bandbreite verbrauchen als die Softwarecodierung. Zum Erzwingen der Softwarekomprimierung bearbeiten Sie den Registrierungsschlüssel auf dem Client. Weitere Informationen finden Sie unter Webcamsoftwarekomprimierung in der Liste der Features, die über die Registrierung verwaltet werden.

### Anforderungen für die HDX RealTime-Webcamvideokomprimierung

Die HDX-Webcam-Videokomprimierung unterstützt die folgenden Versionen der Citrix Workspace-App:

| Plattform | Prozessor |
| --- | --- |
| Citrix Workspace-App für Windows | Die Citrix Workspace-App für Windows unterstützt die Webcam-Videokomprimierung für 32-Bit- und 64-Bit-Apps unter XenApp und XenDesktop 7.17 und höher. Unter früheren Versionen unterstützt die Citrix Workspace-App für Windows nur 32-Bit-Apps. |
| Citrix Workspace-App für Mac | Die Citrix Workspace-App für Mac 2006 und später unterstützt die Webcam-Videokomprimierung für 64-Bit-Apps unter XenApp und XenDesktop 7.17 und höher. Unter früheren Versionen unterstützt die Citrix Workspace-App für Mac nur 32-Bit-Apps. |
| Citrix Workspace-App für Linux | Die Citrix Workspace-App für Linux unterstützt nur 32-Bit-Apps auf dem virtuellen Desktop. |
| Citrix Workspace-App für Chrome | Da manche ARM-Chromebooks die H.264-Codierung nicht unterstützen, können nur 32-Bit-Apps die optimierte HDX-Webcam-Videokomprimierung verwenden. |

Media Foundation-basierte Videoanwendungen unterstützen die HDX-Webcam-Videokomprimierung unter Windows 8.x oder höher und Windows Server 2012 R2 und höher. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX132764.

Andere Anforderungen an Benutzergeräte:

- Geeignete Hardware für die Audiowiedergabe
- DirectShow-kompatible Webcam (Webcam-Standardeinstellungen verwenden). Hardware-codierungsfähige Webcams senken die clientseitige CPU-Nutzung.
- Installieren Sie für die HDX-Webcamvideokomprimierung möglichst die Webcamtreiber des Herstellers auf dem Client. Die Installation der Gerätetreiber ist auf dem Server nicht erforderlich.

Die Bildfrequenz sowie Helligkeits- und Kontraststufen sind bei den einzelnen Webcams unterschiedlich. Die Anpassung des Webcamkontrasts kann den Upstreamverkehr erheblich reduzieren. Citrix verwendet die folgenden Webcams für die Feature-Erstvalidierung:

- Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger

- Logitech C600, C920
- HP Deluxe Webcam

Um die Bildfrequenz anzupassen, bearbeiten Sie den Registrierungsschlüssel auf dem Client. Weitere Informationen finden Sie in der Liste der Features, die über die Registrierung verwaltet werden, unter Bildfrequenz der Webcamvideokomprimierung.

### HD-Webcamstreaming

Die Videokonferenzanwendung auf dem Server wählt Format und Auflösung von Webcams basierend auf den unterstützten Formatarten. Beim Sitzungsstart sendet der Client die Webcam-Informationen an den Server. Sie wählen eine Webcam über die Anwendung aus. Wenn Webcam und Videokonferenzanwendung die Wiedergabe in HD unterstützen, wird HD in der Anwendung verwendet. Es werden Webcamauflösungen bis zu 1920 x 1080 unterstützt.

Dieses Feature erfordert mindestens Citrix Workspace-App für Windows 1808 bzw. Version 4.10 von Citrix Receiver für Windows.

Sie können das Feature über einen Registrierungsschlüssel aktivieren und deaktivieren. Weitere Informationen finden Sie unter HD-Webcamstreaming in der Liste der Features, die über die Registrierung verwaltet werden.

Wenn die Medientypaushandlung fehlschlägt, verwendet HDX die Standardauflösung von 352x288 CIF. Anhand der Registrierungsschlüssel auf dem Client können Sie die Standardauflösung konfigurieren. Stellen Sie sicher, dass die Webcam die angegebene Auflösung unterstützt. Weitere Informationen finden Sie unter HD-Webcamauflösung in der Liste der Features, die über die Registrierung verwaltet werden.

Die HDX-Webcam-Videokomprimierung benötigt im Vergleich zur generischen Plug & Play-USB-Weiterleitung deutlich weniger Bandbreite und funktioniert gut über WAN-Verbindungen. Um die Bandbreite anzupassen, legen Sie den Registrierungsschlüssel auf dem Client fest. Weitere Informationen finden Sie unter HD-Webcambandbreite in der Liste der Features, die über die Registrierung verwaltet werden.

Geben Sie einen Wert in Bits pro Sekunde ein. Wenn Sie die Bandbreite nicht angeben, wird für Videokonferenzanwendungen standardmäßig 350000 Bit/s verwendet.

### Generische HDX-USB-Umleitung für Plug & Play

Die generische HDX-USB-Umleitung für Plug & Play wird auch als **generischer** Webcammodus bezeichnet. Der Vorteil der generischen HDX-USB-Umleitung für Plug & Play besteht darin, dass Sie keine Treiber auf dem Thin Client bzw. Endpunkt installieren müssen. Der USB-Stack wird so virtualisiert,

dass alles, was Sie an den lokalen Client anschließen, an die Remote-VM umgeleitet wird. Auf dem Remotedesktop erscheint dies, als ob Sie das Gerät nativ angeschlossen hätten. Der Windows-Desktop übernimmt die gesamte Interaktion mit der Hardware und sucht anhand der Plug-and-Play-Logik die richtigen Treiber. Die meisten Webcams funktionieren, wenn die Treiber auf dem Server vorhanden sind und über ICA funktionieren. Der generische Webcammodus verbraucht wesentlich mehr Bandbreite (viele Megabits pro Sekunde), da unkomprimierte Videodaten mit dem USB-Protokoll über das Netzwerk gesendet werden.

## HTML5-Multimediaumleitung

June 12, 2024

Die HTML5-Multimediaumleitung ist eine Erweiterung der Multimediaumleitung von HDX MediaStream für HTML5-Audio und -Video. Aufgrund der Zunahme online zur Verfügung gestellter Multimediainhalte (insbesondere für mobile Geräte) haben Browseranbieter effizientere Methoden für die Präsentation von Audio und Video entwickelt.

Der bisherige Standard Flash erfordert ein Plug-In, funktioniert nicht auf allen Geräten und verursacht auf Mobilgeräten einen erhöhten Akkuverbrauch. YouTube, Netflix und neuere Browserversionen von Mozilla, Google und Microsoft verwenden HTML5 als neuen Standard.

HTML5-basiertes Multimedia bietet gegenüber proprietären Plug-Ins zahlreiche Vorteile:

- Unternehmensunabhängige Standards (W3C)
- Vereinfachter DRM-Workflow (Verwaltung digitaler Rechte)
- Bessere Leistung ohne die bei Plug-Ins bestehenden Sicherheitsproblemen

### Progressive Downloads mit HTTP

Progressiver Download ist eine HTTP-basierte Pseudostreamingmethode, die HTML5 unterstützt. Bei einem progressiven Download gibt der Browser eine einzelne Datei wieder (die in einer einzigen Qualität codiert ist), während diese von einem HTTP-Webserver heruntergeladen wird. Das Video wird beim Empfang auf dem Laufwerk gespeichert und von dort abgespielt. Wenn das Video erneut angesehen wird, kann es aus dem Cache geladen werden.

Ein Beispiel für progressiven Download finden Sie auf der Testseite für die HTML5-Videoumleitung. Zum Untersuchen von Videoelementen auf Webseiten und Ermitteln von deren Quelle (ein MP4-Containerformat) im HTML5-Video-Tags verwenden Sie die Browser-Entwicklertools:

### Vergleich von HTML5 und Flash

| Feature | HTML5 | Flash |
|---|---|---|
| Proprietärer Player erforderlich | Nein | Ja |
| Läuft auf Mobilgeräten | Ja | Auf einigen |
| Wiedergabegeschwindigkeit auf unterschiedlichen Plattformen | Hoch | Slow |
| Von iOS unterstützt | Ja | Nein |
| Ressourcennutzung | Weniger | Mehr |
| Schnelleres Laden | Ja | Nein |

### Anforderungen

Citrix unterstützt nur die Umleitung für progressive Downloads im MP4-Format. WebM und Adaptive Bitrate-Streamingtechnologien wie DASH/HLS werden nicht unterstützt.

Folgendes wird unterstützt und durch Richtlinien gesteuert. Weitere Informationen finden Sie unter Richtlinieneinstellungen für Multimedia.

- Serverseitige Wiedergabe
- Serverseitiger Abruf/clientseitige Wiedergabe
- Clientseitiger Abruf und clientseitige Wiedergabe

Mindestversionen von Citrix Workspace-App und Citrix Receiver:

- Citrix Workspace-App 1808 für Windows
- Citrix Receiver für Windows 4.5
- Citrix Workspace-App 1808 für Linux
- Citrix Receiver für Linux 13.5

| Mindest-VDA-Browserversion | Windows-Betriebssystemversion/Build/SP |
|---|---|
| Internet Explorer 11.0 | Windows 10 x86 (1607 RS1) und x64 (1607 RS1);<br>Windows Server 2016 RTM 14393 (1607);<br>Windows Server 2012 R2 |

| Mindest-VDA-Browserversion | Windows-Betriebssystemversion/Build/SP |
|---|---|
| Firefox 47: Fügen Sie die Zertifikate manuell in den Firefox-Zertifikatspeicher ein oder konfigurieren Sie die Firefox-Suche für Zertifikate aus einem vertrauenswürdigen Windows-Zertifikatspeicher. Weitere Informationen finden Sie unter https://wiki.mozilla.org/CA:AddRootToFirefox | Windows 10 x86 (1607 RS1) und x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Chrom 51 | Windows 10 x86 (1607 RS1) und x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |

### Komponenten der HTML5-Videoumleitung

- **HdxVideo.js:** JavaScript-Hook, der Videobefehle auf der Website abfängt. HdxVideo.js kommuniziert mit WebSocketService über Secure WebSockets (SSL/TLS).
- **WebSocket-SSL-Zertifikate**
  - Für die Zertifizierungsstelle (root): **Citrix XenApp/XenDesktop HDX In-Product-Zertifizierungsstelle** (C = USA; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc .; OU = XenApp / XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product-Zertifizierungsstelle)
    Speicherort: Zertifikate (Lokaler Computer)> Vertrauenswürdige Stammzertifizierungsstellen> Zertifikate.
  - Für die Endentität (Blatt): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Speicherort: Zertifikate (Lokaler Computer)> Eigene Zertifikate > Zertifikate.
- **WebSocketService.exe** wird im lokalen System für SSL-Beendigung und Benutzersitzungszuordnung ausgeführt. TLS Secure WebSocket überwacht auf 127.0.0.1 an Port 9001.
- **WebSocketAgent.exe** wird in der Sitzung des Benutzers ausgeführt und gibt das Video gemäß den WebSocketService-Befehlen wieder.

### Aktivieren der HTML5-Videoumleitung

In diesem Release ist dieses Feature nur für Webseiten verfügbar, die unter Ihrer Kontrolle stehen. Die Aktivierung erfordert das Hinzufügen der JavaScript-Datei HdxVideo.js (auf dem Citrix Virtual Apps

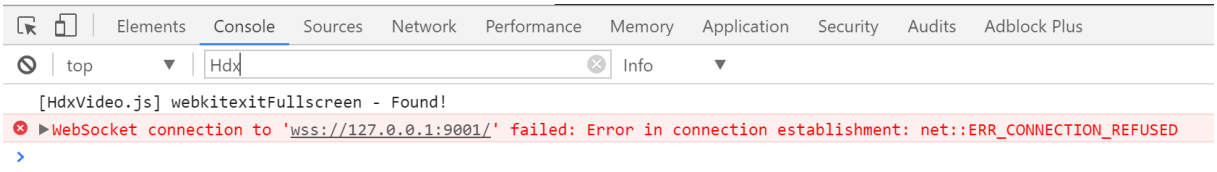
and Desktops-Installationsmedium enthalten) zu Webseiten mit HTML5-Multimediainhalt. Beispiel: Videos auf einer internen Website.

Websites wie youtube.com, die auf adaptive Bitratetechnologien bauen, werden nicht unterstützt (z. B. HTTP Live Streaming (HLS) und Dynamic Adaptive Streaming über HTTP (DASH)).

Weitere Informationen finden Sie unter *Richtlinieneinstellungen für Multimedia*.

### Tipps zur Problembehandlung

Bei dem Versuch, HdxVideo.js auszuführen, können Fehler auftreten. Kann das JavaScript nicht geladen werden, schlägt die HTML5-Umleitung fehl. Prüfen Sie mithilfe der Browser-Entwicklertools HdxVideo.js auf Fehler. Beispiel:




## Optimierung für Microsoft Teams

June 12, 2024

> **Hinweis:**
>
> Das neue Microsoft Teams 2.1 ist jetzt allgemein für VDA verfügbar. Diese Microsoft Teams-Version ist mit Citrix Microsoft Teams Optimization unter Verwendung von WebRTC (VDI 1.0) kompatibel.
>
> Wenn Sie Citrix Virtual Apps and Desktops 2402 verwenden, müssen Sie den Registrierungseintrag `msedgewebview2.exe` nicht mehr manuell konfigurieren, da er standardmäßig auf der Positivliste steht.
>
> Veröffentlichte Apps werden jetzt von Microsoft Teams unterstützt.
>
> Wenn Sie Citrix Virtual Apps and Desktops 2311 oder früher verwenden, ist eine neue Registrierungskonfigurationseinstellung im VDA erforderlich, damit das neue Microsoft Teams auf den virtuellen Citrix Channel zugreifen kann. Um die Optimierung für Microsoft Teams 2.1 zu aktivieren, konfigurieren Sie den folgenden Registrierungsschlüssel im VDA:
>
> **Ort**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
>
> **Schlüssel** (REG_Multi_SZ): `ProcessWhitelist`

> **Wert**: `msedgewebview2.exe`
>
> Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Citrix bietet eine Optimierung für die Verwendung der Desktopversion von Microsoft Teams in Citrix Virtual Apps and Desktops und der Citrix Workspace-App. Standardmäßig werden alle erforderlichen Komponenten in die Citrix Workspace-App und den Virtual Delivery Agent (VDA) gepackt.

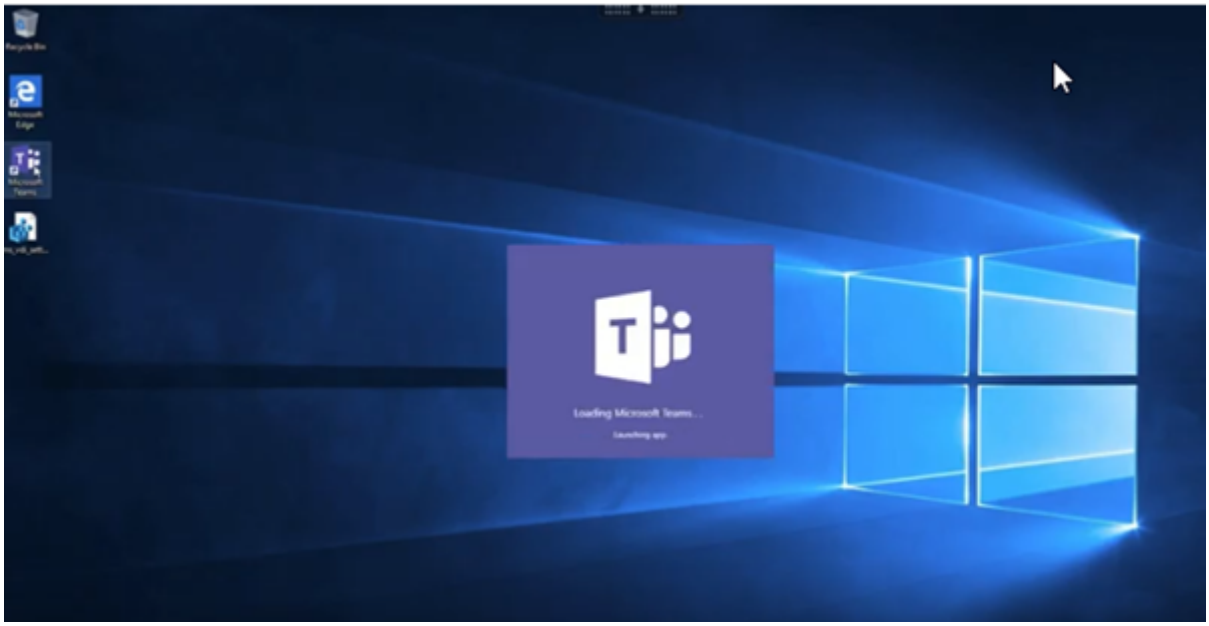
Die Optimierung für Microsoft Teams umfasst VDA-seitige HDX-Dienste und eine API, die als Schnittstelle mit der von Microsoft Teams gehosteten App zum Empfangen von Befehlen fungieren. Diese Komponenten öffnen einen virtuellen Steuerungskanal (CTXMTOP) zur Media Engine der Citrix Workspace-App. Der Endpunkt decodiert Multimediainhalte lokal und stellt sie lokal bereit, wobei das Fenster der Citrix Workspace-App in die gehostete Microsoft Teams-App zurückverschoben wird.

Authentifizierung und Signalisierung erfolgen nativ in der von Microsoft Teams gehosteten App, genau wie die anderen Microsoft Teams-Dienste (zum Beispiel Chat oder Teamarbeit). Die Audio-/Videoumleitung hat auf sie keine Auswirkungen.

`CTXMTOP` ist ein virtueller Command-and-Control-Kanal. Dies bedeutet, dass Medien nicht zwischen der Citrix Workspace-App und dem VDA ausgetauscht werden.

Nur Clientabruf und Clientwiedergabe sind verfügbar.

In diesem Video wird gezeigt, wie Microsoft Teams in einer virtuellen Citrix Umgebung funktioniert.



### Installation von Microsoft Teams

Citrix und Microsoft empfehlen, die neueste verfügbare Version von Microsoft Teams zu verwenden und sie auf dem neuesten Stand zu halten.
Versionen der Microsoft Teams Desktop-App mit einem Veröffentlichungsdatum, das mehr als 90 Tage älter als das Veröffentlichungsdatum der aktuellen Version sind, werden nicht unterstützt.
Nicht unterstützte Versionen der Microsoft Teams Desktop-App zeigen Benutzern eine blockierende Seite und fordern zum Update der App auf.

Informationen zu den neuesten verfügbaren Versionen finden Sie unter Updateverlauf für Teams App (Desktop und Mac).

Wir empfehlen, den Richtlinien zur maschinenweiten Installation von Microsoft Teams zu folgen. Vermeiden Sie die Verwendung des EXE-Installationsprogramms, mit dem Microsoft Teams in `AppData` installiert wird. Installieren Sie die Software stattdessen an der Befehlszeile mit dem Flag `ALLUSER=1` unter `C:\Program Files (x86)\Microsoft\Teams`.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

In diesem Beispiel wird auch der Parameter `ALLUSERS=1` verwendet. Wenn Sie diesen Parameter festlegen, wird das maschinenweite Installationsprogramm von Microsoft Teams für alle Benutzer des Computers in der Systemsteuerung unter **Programme und Funktionen** und in der Windows-**Systemsteuerung** angezeigt. Außerdem in **Apps und Features** in den Windows-Einstellungen für alle Benutzer des Computers. Alle Benutzer können Microsoft Teams dann deinstallieren, wenn sie über Administratorrechte verfügen.

Es ist wichtig, den Unterschied zwischen `ALLUSERS=1` und `ALLUSER=1` zu verstehen. Sie können den Parameter `ALLUSERS=1` in Nicht-VDI- und in VDI-Umgebungen verwenden. Den Parameter `ALLUSER=1` verwenden Sie nur in VDI-Umgebungen, um eine Installation pro Maschine festzulegen.

Im Modus `ALLUSER=1` wird die Microsoft Teams-Anwendung nicht automatisch aktualisiert, sobald eine neue Version vorhanden ist. Wir empfehlen diesen Modus für nicht persistente Umgebungen, z. B. gehostete freigegebene Apps oder Desktops aus zufälligen/gepoolten Katalogen mit Windows Server oder Windows 10. Weitere Informationen finden Sie unter Installieren von Microsoft Teams mit MSI (Abschnitt VDI-Installation).

Angenommen Sie verfügen über dedizierte persistente VDI-Umgebungen mit Windows 10. Wenn Sie die Microsoft Teams-Anwendung automatisch aktualisieren und pro Benutzer unter `Appdata/Local` installieren möchten, verwenden Sie das Microsoft Teams-Installationsprogramm oder die MSI. Verwenden Sie in diesem Fall das `.exe`-Installationsprogramm oder die MSI ohne `ALLUSER=1`
.

> **Hinweis:**
>
> Wir empfehlen, den VDA zu installieren, bevor Microsoft Teams im goldenen Image installiert wird. Diese Installationsreihenfolge ist notwendig, damit das Flag ALLUSER=1 wirksam wird. Wenn Sie Microsoft Teams vor dem VDA auf der virtuellen Maschine installiert haben, deinstallieren Sie Microsoft Teams und installieren Sie es neu.

### Remote-PC-Zugriff

Wir empfehlen die Installation von Microsoft Teams Version 1.4.00.22472 oder später, nachdem Sie den VDA installiert haben. Andernfalls müssen Sie sich abmelden und erneut anmelden, damit Microsoft Teams den VDA wie erwartet erkennen kann. Version 1.4.00.22472 und später enthält erweiterte Logik, die zur Startzeit von Microsoft Teams und zur Anmeldezeit für die VDA-Erkennung ausgeführt wird. Diese Versionen enthalten auch eine Identifizierung des aktiven Sitzungstyps (HDX, RDP oder lokal mit dem Clientcomputer verbunden). Wenn Sie lokal verbunden sind, können frühere Versionen von Microsoft Teams bestimmte Features oder UI-Elemente möglicherweise nicht erkennen und deaktivieren. Beispiele: separate Räume, Pop-Out-Fenster für Besprechungen und Chats oder Reaktionen in Besprechungen.

> **Wichtig:**
>
> Wenn Sie von einer lokalen Sitzung zu einer HDX-Sitzung wechseln und Microsoft Teams geöffnet bleibt und im Hintergrund ausgeführt wird, müssen Sie Microsoft Teams beenden und neu starten, um die Optimierung mit HDX korrekt zu ermöglichen.
> Wenn Sie dagegen Microsoft Teams remote über eine optimierte HDX-Sitzung verwenden, trennen Sie die HDX-Sitzung und stellen Sie die Verbindung lokal auf dem Gerät zu derselben Windows-Sitzung wieder her. Wenn Sie im Büro arbeiten, müssen Sie Microsoft Teams neu starten, damit es den Status des Remote-PCs (HDX oder lokal) korrekt erkennen kann. Microsoft Teams kann den VDI-Modus nur zum Zeitpunkt des App-Starts bewerten und nicht, während es bereits im Hintergrund ausgeführt wird. Ohne einen Neustart kann Microsoft Teams möglicherweise Funktionen wie Pop-Out-Fenster, Gruppenräume oder Besprechungsreaktionen nicht laden.

### App Layering

Wenn Sie Citrix App Layering zum Verwalten von VDA- und Microsoft Teams-Installationen auf verschiedenen Layern verwenden, müssen Sie einen neuen Registrierungsschlüssel auf Windows-VDAs erstellen, bevor Sie Microsoft Teams mit dem Flag ALLUSER=1 über die Befehlszeile installieren. Weitere Informationen finden Sie im Abschnitt *Optimierung für Microsoft Teams mit Citrix App Layering* unter Multimedia.

### Empfehlungen zur Profilverwaltung

Es empfiehlt sich, das maschinenweite Installationsprogramm für Windows Server- und gepoolte VDI-Umgebungen mit Windows 10 zu verwenden.

Wenn das Flag **ALLUSER=1** an der Befehlszeile (maschinenweites Installationsprogramm) an das MSI übergeben wird, wird die Microsoft Teams-App unter `C:\Program Files (x86)` installiert (~300 MB). Die App verwendet `AppData\Local\Microsoft\TeamsMeetingAddin` für Protokolle und `AppData\Roaming\Microsoft\Teams` (~600–700 MB) für benutzerspezifische Konfigurationen, das Zwischenspeichern von Elementen der Benutzeroberfläche usw.

> **Wichtig:**
>
> Wenn Sie das Flag **ALLUSER=1** nicht übergeben, speichert die MSI das Teams.exe-Installationsprogramm und `setup.json` unter `C:\Program Files (x86)\Teams Installer`. Ein Registrierungsschlüssel (TeamsMachineInstaller) wird unter `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run` hinzugefügt.
> Eine nachfolgende Benutzeranmeldung löst stattdessen die endgültige Installation in **AppData** aus.

#### Installationsprogramm für die maschinenweite Installation

Im Folgenden finden Sie ein Beispiel für Ordner, Desktopverknüpfungen und Registrierungen, die bei der Installation von Microsoft Teams mit dem Installationsprogramm für die maschinenweite Installation auf einer VM mit Windows Server 2016 64-Bit erstellt werden:

*Ordner:*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Desktopverknüpfung:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*Registrierung:*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Name:`Teams`
- Typ: `REG_SZ`
- Wert: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Hinweis:**
>
> Das Registrierungsverzeichnis variiert je nach den zugrunde liegenden Betriebssystemen und der Bitanzahl.

### Empfehlungen

- Es wird empfohlen, den automatischen Start durch Löschen der Microsoft Teams-Registrierungsschlüssel zu deaktivieren. Dadurch wird verhindert, dass viele gleichzeitige Anmeldungen (z. B. zu Beginn des Arbeitstags) die CPU der VM überlasten.
- Wenn der virtuelle Desktop keinen GPU/vGPU hat, wird empfohlen, die Einstellung **GPU-Hardwarebeschleunigung deaktivieren** in den **Einstellungen** von Microsoft Teams festzulegen, um die Leistung zu verbessern. Diese Einstellung (`"disableGpu":true`) wird in `%Appdata%\Microsoft\Teams` in `desktop-config.json` gespeichert. Sie können diese Datei mit einem Anmeldeskript bearbeiten und den Wert auf **true** festlegen.
- Wenn Sie Citrix Workspace Environment Management (WEM) verwenden, aktivieren Sie **CPU Spikes Protection**, um die Prozessornutzung durch Microsoft Teams zu verwalten.

### Installationsprogramm pro Benutzer

Bei Verwendung des `.exe`-Installationsprogramms verläuft die Installation anders. Alle Dateien werden unter AppData abgelegt.

*Ordner:*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Desktopverknüpfung:*

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

*Registrierung:*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

**Bewährte Methoden**

Die Empfehlungen bewährter Methoden basieren auf den Anwendungsfällen.
Die Verwendung von Microsoft Teams mit flüchtigem Setup erfordert einen Profilcaching-Manager für die effiziente Synchronisierung der Microsoft Teams-Laufzeitdaten. Mit einem Profilcaching-Manager werden die richtigen benutzerspezifischen Informationen während der Benutzersitzung zwischengespeichert. Zu den benutzerspezifischen Informationen gehören beispielsweise Benutzerdaten, Profil und Einstellungen. Synchronisieren Sie die Daten in den folgenden beiden Ordnern:

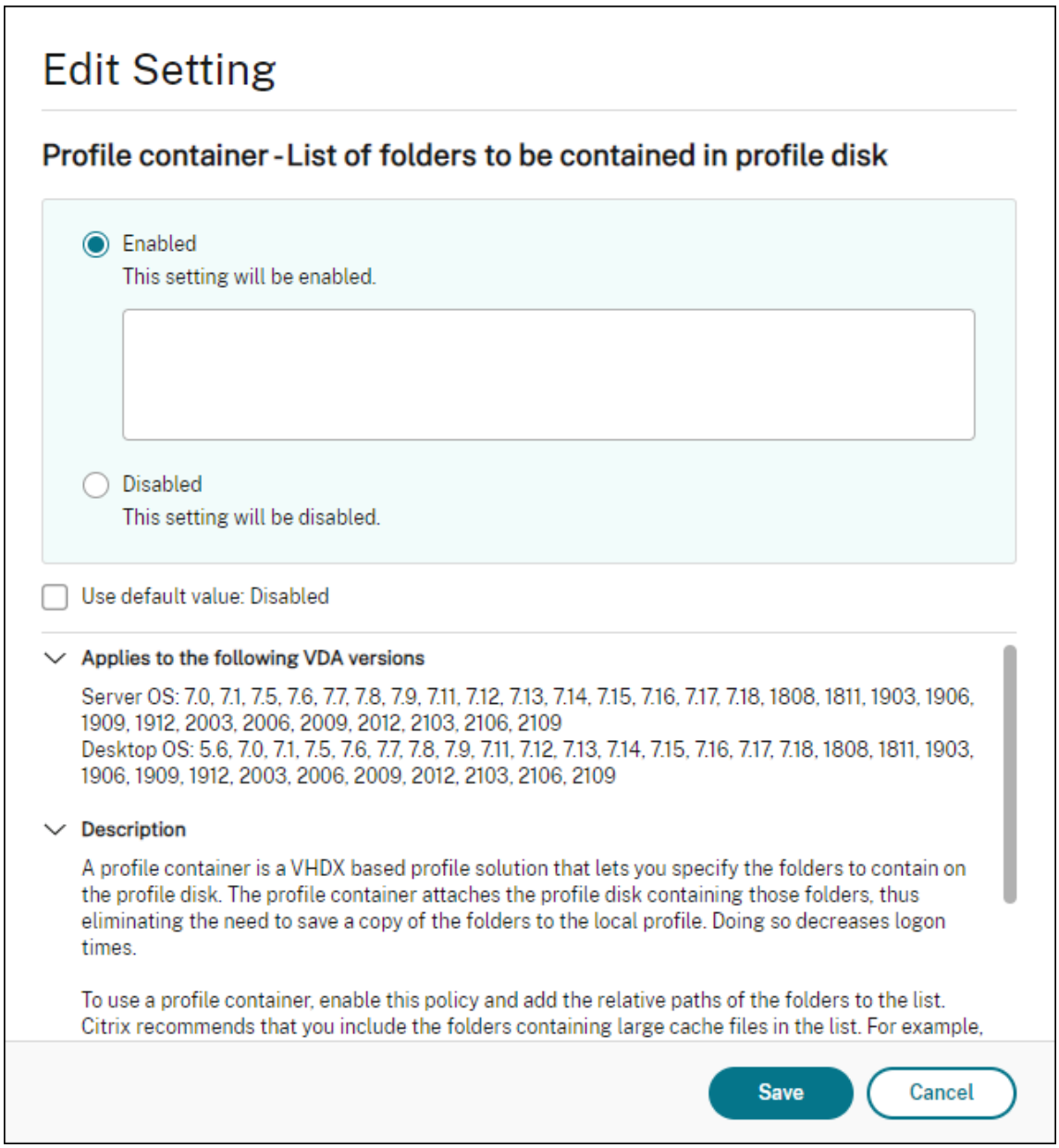
- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

**Ausschlussliste für zwischengespeicherte Microsoft Teams-Inhalte bei beständigem Setup**
Schließen Sie die Dateien und Verzeichnisse aus dem Caching-Ordner von Microsoft Teams aus, wie in der Microsoft-Dokumentation beschrieben. Dadurch wird die Größe des Benutzercaches reduziert und das flüchtige Setup weiter optimiert.

**Anwendungsfall: Einzelsitzung** In diesem Szenario verwendet der Endbenutzer Microsoft Teams an einem Ort. Microsoft Teams muss nicht in zwei Windows-Sitzungen gleichzeitig ausgeführt werden. Gewöhnlich wird jedem Benutzer ein virtueller Desktop zugewiesen und Microsoft Teams im virtuellen Desktop als Anwendung bereitgestellt.
Wir empfehlen, Citrix Profilcontainer zu aktivieren und die unter Installationsprogramm pro Benutzer aufgeführten Benutzerverzeichnisse in den Container umzuleiten.

1. Stellen Sie das maschinenweite Microsoft Teams-Installationsprogramm (**ALLUSER=1**) im Gold-Image bereit.
2. Aktivieren Sie die Citrix Profilverwaltung und richten Sie den Benutzerprofilspeicher mit den korrekten Berechtigungen ein.
3. Aktivieren Sie folgende Richtlinieneinstellung für die Profilverwaltung: **Dateisystem > Synchronisierung > Profilcontainer - Liste der Ordner, die auf dem Profildatenträger enthalten sein sollen**.




Diese Liste muss alle Benutzerverzeichnisse enthalten. Sie können diese Einstellungen mit Citrix Workspace Environment Management (WEM) konfigurieren.

4. Wenden Sie die Einstellungen auf die richtige Bereitstellungsgruppe an.
5. Melden Sie sich an, um die Bereitstellung zu überprüfen.

## Systemanforderungen

### Empfohlene Mindestversion - Delivery Controller (DDCs) 1906.2

Wenn Sie eine frühere Version verwenden, lesen Sie den Artikel Aktivieren der Optimierung für Microsoft Teams:

Unterstützte Betriebssysteme:

- Windows Server 2022, Windows Server 2019, 2016, 2012R2 Standard und Datacenter Edition und mit der Server Core-Option

### Mindestversion –Virtual Delivery Agents (VDAs) 1906.2

Unterstützte Betriebssysteme:

- Windows 11.
- Windows 10 64-Bit, ab Version 1607. VM-gehostete Apps werden von der Citrix Workspace-App für Windows ab Version 2109.1 unterstützt.
- Windows Server 2022, Windows Server 2019, 2016 und 2012 R2, Standard und Datacenter Edition

Anforderungen:

- BCR_x64.msi: Das MSI mit dem Microsoft Teams-Optimierungscode. Es startet automatisch von der GUI. Wenn Sie die Befehlszeilenschnittstelle für die VDA-Installation verwenden, schließen Sie es nicht aus.

### Empfohlene Version –Citrix Workspace-App für Windows, neuestes Release und Mindestversion –Citrix Workspace-App 1907 für Windows

- Windows 11.
- Windows 10 (32-Bit- und 64-Bit-Editionen, einschließlich Embedded-Editionen) (Unterstützung für Windows 7 wurde ab Version 2006 eingestellt) (Unterstützung für Windows 8.1 wurde ab Version 2204.1 eingestellt).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) und 2019 LTSC (v1809).
- Unterstützte Prozessorarchitekturen: x86 und x64 (ARM wird nicht unterstützt).
- Endpunkt: Dual-Core-CPU (ca. 2,2–2,4 GHz), die 720p-HD-Auflösung für Peer-to-Peer-Videokonferenzen unterstützt.
- Dual- oder Quad-Core-CPUs mit niedrigerem Basistakt (~1,5 GHz), ausgestattet mit Intel Turbo Boost oder AMD Turbo Core für eine Steigerung bis mindestens 2,4 GHz.
- HP Thin Clients-geprüft: t630/t640, t730/t740, mt44/mt45.

- Dell Thin Clients-geprüft: 5070, 5470 Mobile TC und AIO.
- 10ZiG Thin Clients-geprüft: 4510 und 5810q.
- Eine vollständige Liste aller geprüften Endpunkte finden Sie unter Thin Clients.
- Die Citrix Workspace-App benötigt mindestens 600 MB freien Speicherplatz und 1 GB RAM.
- Mindestanforderungen für Microsoft .NET Framework ist Version 4.8. Die Citrix Workspace-App lädt .NET Framework automatisch herunter und installiert es, wenn es nicht vorhanden ist.

Administratoren können den Start von Microsoft Teams im optimiertem Modus über die Richtlinie zur Teams-Optimierung aktivieren und deaktivieren. Beim Start in der Citrix Workspace-App im optimierten Modus kann Microsoft Teams nicht deaktiviert werden.

#### Mindestversion —Citrix Workspace-App 2006 für Linux

Software:

- `GStreamer` 1.0 oder höher oder Cairo 2
- libc++-9.0 oder höher
- `libgdk` 3.22 oder höher
- OpenSSL 1.1.1d
- x64 Linux-Distribution

Hardware:

- Mindestens 1,8 GHz Dual-Core-CPU, die 720p HD-Auflösung während eines Peer-to-Peer-Videokonferenzanrufs unterstützen kann
- Dual- oder Quad-Core-CPU mit einer Basisgeschwindigkeit von 1,8 GHz und einer hohen Intel Turbo Boost Geschwindigkeit von mindestens 2,9 GHz

Eine vollständige Liste aller geprüften Endpunkte finden Sie unter Thin Clients.

Weitere Informationen finden Sie unter Voraussetzungen für die Installation der Citrix Workspace-App.

Sie können die Microsoft Teams-Optimierung deaktivieren, indem Sie den Wert des Felds **VDWEBRTC** in der Datei `/opt/Citrix/ICAClient/config/module.ini` ändern. Der Standardwert ist VDWEBRTC=On. Nachdem das Update abgeschlossen ist, starten Sie die Sitzung neu. (Rootberechtigungen erforderlich)

#### Mindestversion –Citrix Workspace-App 2012 für Mac

Unterstützte Betriebssysteme:

- macOS Catalina (10.15).

- macOS Big Sur 11.0.1 und später.
- macOS Monterey.

Unterstützte Features:

- Audio
- Video
- Optimierung der Bildschirmfreigabe (eingehend und ausgehend)

> **Hinweis:**
>
> Die Citrix Viewer-App benötigt Zugriff auf die Einstellungen für macOS-Sicherheit und Datenschutz, damit die Bildschirmfreigabe funktioniert. Die Benutzer konfigurieren diese Einstellung unter **Apple-Menü > Systemeinstellungen > Sicherheit & Datenschutz > Bildschirmaufzeichnung** und wählen **Citrix Viewer**.

Die Optimierung für Microsoft Teams ist bei Verwendung der Citrix Workspace-App 2012 oder später und von macOS 10.15 standardmäßig aktiviert.

Um die Optimierung für Microsoft Teams zu deaktivieren, führen Sie diesen Befehl in einem Terminal aus und starten die Citrix Workspace-App neu:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

**Mindestversion: Neueste Version der Citrix Workspace-App für Chrome OS wird auf der neuesten Version von Chrome OS ausgeführt**

Hardware:

- Prozessoren mit gleichwertiger oder besserer Leistung als Intel i3, Quad Core 2,4 GHz.

Unterstützte Features:

- Audio
- Video
- Optimierung der Bildschirmfreigabe (ein- und ausgehend) - standardmäßig deaktiviert. In diesen Einstellungen finden Sie Anweisungen zum Aktivieren.

## Skalierbarkeit einzelner Server

Dieser Abschnitt enthält Empfehlungen und Orientierung zur Schätzung der Zahl der Benutzer bzw. virtuellen Maschinen (VMs), die auf einem einzelnen physischen Host unterstützt werden können. Dies wird in der Regel als SSS (Citrix Virtual Apps and Desktops Single Server Scalability) bezeichnet. Im Zusammenhang mit Citrix Virtual Apps (CVA) oder der Sitzungsvirtualisierung wird es allgemein

auch als Benutzerdichte bezeichnet. Es geht darum herauszufinden, wie viele Benutzer oder VMs auf einer Hardware mit einem größeren Hypervisor ausgeführt werden können.

> **Hinweis:**
>
> Dieser Abschnitt enthält Orientierung zur Schätzung der SSS. Es geht darum um allgemeine Empfehlungen, die sich nicht unbedingt komplett auf Ihre spezifische Situation bzw. Umgebung anwenden lassen. Citrix Virtual Apps and Desktops-SSS kann nur mit einem Tool für Skalierbarkeitstests oder Lasttests wie Login VSI genau ermittelt werden. Citrix empfiehlt die Verwendung der vorliegenden Empfehlungen nur für schnelle SSS-Schätzungen. Citrix empfiehlt aber, die Ergebnisse insbesondere vor dem Kauf von Hardware oder dem Treffen finanzieller Entscheidungen mit Login VSI oder einem Lasttest-Tool Ihrer Wahl zu validieren.

#### Hardware (Testsystem)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 mit 2,60 GHz (max. Turbo 3,70 GHz), 12 Kerne pro Sockel, Dual-Sockel mit aktiviertem Hyperthreading
- 382 GB RAM
- Lokaler SSD RAID 0-Speicher (11 Datenträger) 6 TB

#### Software

Eine virtuelle Maschine (40 logische Prozessoren) mit Windows 2019 (TSVDA) und Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

#### Terminologie

- Wissensarbeiter-Workload: Umfasst Acrobat Reader, Freemind-/Java-, Fotoviewer-, Edge- und MS Office-Apps (z. B. Excel, Outlook, PowerPoint und Word).
- Baseline: Serverskalierbarkeitstests mit Wissensarbeiter-Workload (ohne Microsoft Teams).
- Microsoft Teams-Workload: Typische Wissensarbeiter-Workload + Microsoft Teams.

#### Belastungstestmethode für Microsoft Teams

- Microsoft Teams ist HDX-optimiert. Daher wird die gesamte Multimedia-Verarbeitung auf den Endpunkt oder Client abgeladen und ist nicht Teil der Messung.
- Alle Microsoft Teams-Prozesse werden gestoppt oder beendet, bevor die Workload startet.
- Öffnen Sie Microsoft Teams (Kaltstart).

- Messen Sie die Zeit, die zum Laden benötigt wird, und aktivieren Sie den Fokus des Microsoft Teams-Hauptfensters.
- Wechseln Sie per Tastenkombination zum Chatfenster.
- Wechseln Sie per Tastenkombination zum Kalenderfenster.
- Senden Sie eine Chat-Nachricht per Tastenkombinationen an einen Benutzer.
- Wechseln Sie per Tastenkombination zum Microsoft Teams-Fenster.

**Ergebnisse**

- 40 % Skalierbarkeitsauswirkung bei Microsoft Teams-Workload (81 Benutzer) im Vergleich zur Baseline (137 Benutzer).
- Durch eine Erhöhung der Serverkapazität (CPU) um ca. 40 % wird die Benutzeranzahl der Baseline-Workload wieder erreicht.
- 20 % zusätzlicher Arbeitsspeicher bei Microsoft Teams-Workload im Vergleich zur Baseline erforderlich.
- Erhöhen Sie die Speichergröße pro Benutzer um 512 bis 1024 MB.
- Ca. 50 % mehr IOPS-Schreibvorgänge, ca. 100 % mehr IOPS-Lesevorgänge. Microsoft Teams kann in einer Umgebung mit langsamerem Speicher erhebliche Auswirkungen haben.

## Featurematrix und Versionsunterstützung

| Feature | Microsoft Teams (Mindestversion) | VDA (Mindestversion) | Citrix Workspace-App für Windows (Mindestversion) | Citrix Workspace-App für Mac (Mindestversion) | Citrix Workspace-App für Linux (Mindestversion) | Citrix Workspace-App für Chrome OS |
|---|---|---|---|---|---|---|
| Audio/Video (P2P und Konferenz) | Aktuelle Version minus 90 Tage | 1906 | 1907 | 2009 | 2004 | 2105.5 |
| Bildschirmfreigabe | Aktuelle Version minus 90 Tage | 1906 | 1907 | 2012 | 2006 | 2105.5 |

| Feature | Microsoft Teams (Mindestversion) | VDA (Mindestversion) | Citrix Workspace-App für Windows (Mindestversion) | Citrix Workspace-App für Mac (Mindestversion) | Citrix Workspace-App für Linux (Mindestversion) | Citrix Workspace-App für Chrome OS |
|---|---|---|---|---|---|---|
| i. Roter Rahmen für Bildschirmanzeige | Aktuelle Version minus 90 Tage | 1906 | 2002 | 2012 | 2006 | Nein |
| ii. Erfassung auf Desktop Viewer beschränken | Aktuelle Version minus 90 Tage | 1906 | 2009.5 | 2012 | 2006 | Nein |
| iii. Mehrere Monitore | Aktuelle Version minus 90 Tage | 1912 CU6+ | 2106 (1) | 2106 | 2106 | Nein |
| Mehrfrequenzwahlverfahren | Aktuelle Version minus 90 Tage | – | 2102 | 2101 | 2101 | 2111.1 |
| Proxyserverunterstützung | Aktuelle Version minus 90 Tage | – | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |
| App-Freigabe | Aktuelle Version minus 90 Tage | 2109 | 2109.1 | 2203.1 | 2209 | Nein |
| Liveuntertitel | Aktuelle Version minus 90 Tage | –(4) | 2109.1 | 2109 | 2109 | 2303 |

| Feature | Microsoft Teams (Mindestversion) | VDA (Mindestversion) | Citrix Workspace-App für Windows (Mindestversion) | Citrix Workspace-App für Mac (Mindestversion) | Citrix Workspace-App für Linux (Mindestversion) | Citrix Workspace-App für Chrome OS |
|---|---|---|---|---|---|---|
| Dynamisches e911 | Aktuelle Version minus 90 Tage | – | 2112.1 | 2112 | 2112 | 2112 |
| Steuerung übergeben | Aktuelle Version minus 90 Tage | – | 2112.1 | 2203.1 | Nein | Nein |
| Steuerung anfordern | Aktuelle Version minus 90 Tage | – | 2112.1 | 2203.1 | 2203 | 2303 |
| Mehrfenstermodus | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Besprechungsaufzeichnung | Aktuelle Version minus 90 Tage | 2112.1, 1912 CU6+ | 2112 | 2203.1 | 2203 | 2303 |
| Hintergrundunschärfe | Aktuelle Version minus 90 Tage | 2112, 1912 CU6+ | 2207 | 2301 | 2212 | 2303 |

1. CD-Viewer nur im Vollbildmodus. UMSCHALT+F2 nicht unterstützt.
2. Negotiate/Kerberos, NTLM, Basic und Digest. Pac-Dateien werden ebenfalls unterstützt.
3. Nur anonym.
4. Wenn die VDA-Version 2112 oder höher ist, funktionieren Liveuntertitel nur, wenn die Citrix Workspace-App-Version 2203.1 für MAC und 2203 Linux oder 2112 für Windows ist. Dies liegt daran, dass sich Liveuntertitel unterschiedlich verhalten, wenn Microsoft Teams im Einzel- oder im Mehrfenstermodus ist.
5. Der Mehrfenstermodus wurde mit VDA 2112 eingeführt, aber auf die Version VDA 1912 LTSR CU6 zurückportiert.

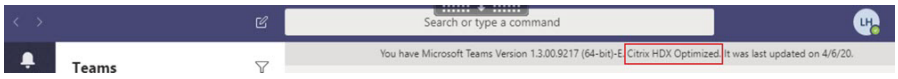
> **Hinweis:**
>
> Alle unter **Citrix Workspace-App für Windows 1912 CU6 (oder höher)** aufgeführten Features gelten für die Citrix Workspace-App für Windows 2203.1 LTSR CU1.

### Aktivieren der Optimierung für Microsoft Teams

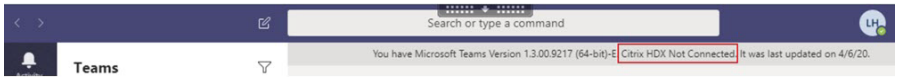
Verwenden Sie die unter Microsoft Teams-Umleitung beschriebene Richtlinie der Verwaltungskonsole, um die Optimierung für Microsoft Teams zu aktivieren. Diese Richtlinie ist standardmäßig auf **EIN** festgelegt. Zusätzlich zu der Aktivierung dieser Richtlinie überprüft HDX, ob die Version der Citrix Workspace-App der Mindestversion entspricht. Wenn Sie die Richtlinie aktiviert haben und die Version der Citrix Workspace-App unterstützt wird, wird **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream** auf dem VDA automatisch auf **1** festgelegt. Microsoft Teams liest den Schlüssel zum Laden im VDI-Modus.

> **Hinweis:**
>
> Wenn Sie VDAs der Version 1906.2 oder später mit älteren Controller-Versionen (z. B. Version 7.15) verwenden, für die die Richtlinie in der Verwaltungskonsole (Studio) nicht verfügbar ist, ist die Optimierung des VDA immer noch möglich. Die HDX-Optimierung für Microsoft Teams ist im VDA standardmäßig aktiviert.

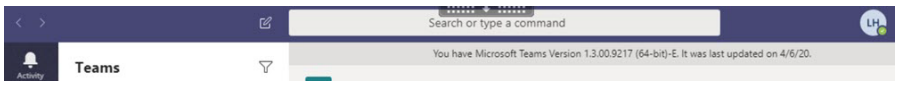
Wenn Sie auf **Info > Version** klicken, wird die Legende **Citrix HDX Optimized** angezeigt:




Wenn **Citrix HDX Not Connected** angezeigt wird, wurde die Citrix API in Microsoft Teams geladen. Das Laden der API ist der erste Schritt der Umleitung. In den nachfolgenden Teilen des Stacks ist ein Fehler aufgetreten. Der Fehler trat höchstwahrscheinlich in VDA-Diensten oder der Citrix Workspace-App auf.




Wenn keine Legende angezeigt wird, konnte Microsoft Teams die Citrix API nicht laden. Klicken Sie mit der rechten Maustaste auf das Symbol für den Infobereich, um Microsoft Teams zu beenden und neu starten. Vergewissern Sie sich, dass die Richtlinie der Verwaltungskonsole nicht auf **Nicht zugelassen** festgelegt ist und dass die Citrix Workspace-App-Version unterstützt wird.



> **Wichtig: Sitzungswiederverbindung**
>
> - Möglicherweise müssen Sie Microsoft Teams neu starten, um eine Sitzung mit HDX-Optimierung zu erhalten, wenn sich die Konnektivität ändert. Beispiel: beim Roaming von einem nicht unterstützten Endpunkt (Workspace-App für iOS, Android oder alte Versionen von Windows/Linux/Mac) zu einem unterstützten Endpunkt (Workspace-App für Windows/Linux/Mac/ChromeOS/HTML5) oder umgekehrt.
> - Ein Neustart von Microsoft Teams ist auch dann erforderlich, wenn Sie die App im VDA mit dem EXE-Installationsprogramm für Microsoft Teams installiert haben. Das EXE-Installationsprogramm wird für persistente VDI-Bereitstellungen empfohlen. In solchen Fällen kann Microsoft Teams automatische Updates durchführen, während sich die HDX-Sitzung im getrennten Zustand befindet. Benutzer, die sich erneut mit einer HDX-Sitzung verbinden, stellen also fest, dass Microsoft Teams nicht optimiert ausgeführt wird.
> - Beim Roaming von einer lokalen Sitzung zu einer HDX-Sitzung müssen Sie Microsoft Teams neu starten, um HDX-Optimierung zu erreichen. Diese Aktion ist bei Remote-PC-Zugriff erforderlich.

### Netzwerkanforderungen

Microsoft Teams benötigt Medienprozessor-Server unter Microsoft 365 für Besprechungen oder Anrufe mit mehreren Teilnehmern. Microsoft Teams benötigt außerdem Microsoft 365-Transport-Relays für folgende Szenarios:

- Zwei Peers in einem Point-to-Point-Anruf ohne direkte Verbindung
- Ein Teilnehmer ohne direkte Verbindung zum Medienprozessor

Daher hängt die Anrufgüte von der Integrität des Netzwerks zwischen dem Peer und der Microsoft 365-Cloud ab. Ausführliche Richtlinien zur Netzwerkplanung finden Sie in den Prinzipien von Microsoft 365-Netzwerkverbindungen.

Wir empfehlen eine Analyse der Umgebung auf Risiken und Anforderungen bezüglich der gesamten Sprach- und Videobereitstellung über die Cloud.
Verwenden Sie das Skype for Business Network Assessment Tool, um zu testen, ob Ihr Netzwerk sich für Microsoft Teams eignet. Weitere Informationen zum Support finden Sie unter Support.

#### Zusammenfassung der wichtigsten Netzwerkempfehlungen für den Datenverkehr mit RTP (Realtime Transport Protocol)

- Stellen Sie von der Zweigstelle eine möglichst direkte Verbindung zum Microsoft 365-Netzwerk her.
- Sie müssen ausreichend Bandbreite für die Zweigstelle einplanen und bereitstellen.

- Überprüfen Sie Qualität und Konnektivität des Netzwerks für jede Zweigstelle.
- Wenn Sie folgende Funktionen in der Zweigstelle verwenden, muss der RTP/UDP Teams-Verkehr (von HdxRtcEngine.exe in der Citrix Workspace-App behandelt) ungehindert erfolgen.
  - Proxyserver umgehen
  - Netzwerk-SSL abfangen
  - DPI-Geräte (Deep Packet Inspection)
  - VPN-Hairpins (nach Möglichkeit Split-Tunneling verwenden)

> **Wichtig: VPN-Split-Tunnelkonfiguration**
>
> Der Datenverkehr von HdxRtcEngine.exe muss vom VPN-Tunnel umgeleitet werden und in der Lage sein, über die lokale Internetverbindung des Benutzers eine direkte Verbindung zum Dienst herzustellen. Wie dies erreicht wird, hängt vom verwendeten VPN-Produkt und der verwendeten Maschinenplattform ab; die meisten VPN-Lösungen ermöglichen jedoch eine einfache Konfiguration der Richtlinie, um diese Logik anzuwenden. Weitere Hinweise zum Festlegen der VPN-spezifischen Split-Tunnelkonfiguration finden Sie in diesem Microsoft-Artikel.

Die WebRTC Media Engine in der Workspace-App (HdxRtcEngine.exe) verwendet das Protokoll SRTP (Secure Real-Time Transport Protocol) für Multimediastreams, die an den Client ausgelagert werden. SRTP bietet Vertraulichkeit und Authentifizierung für RTP. Für dieses Feature werden mit DTLS ausgehandelte, symmetrische Schlüssel zum Verschlüsseln von Medien verwendet und Nachrichten unter Verwendung der AES-Verschlüsselung gesteuert.

Folgende Metriken werden für eine positive Benutzererfahrung empfohlen:

| Metrik | Endpunkt zu Microsoft 365 |
|---|---|
| Latenz (ein Weg) | < 50 ms |
| Latenz (RTT) | < 100 ms |
| Paketverlust | < 1 % während eines Intervalls von 15 s |
| Paket-Interarrival-Jitter | <30 ms während eines Intervalls von 15 s |

Weitere Informationen finden Sie unter Vorbereiten des Netzwerks für Microsoft Teams.

Für Bandbreitenanforderungen kann die Optimierung für Microsoft Teams eine Vielzahl von Codecs für Audio (OPUS/G.722/PCM G711) und Video (H264) verwenden.

Die Peers handeln diese Codecs während der Einrichtung des Anrufs über SDP (Session Description Protocol) aus.
Mindestempfehlungen von Citrix pro Benutzer:

| Typ | Bandbreite | Codec |
|---|---|---|
| Audio (bidirektional) | ~ 90 KBit/s | G.722 |
| Audio (bidirektional) | ~ 60 KBit/s | Opus* |
| Video (bidirektional) | ~ 700 KBit/s | H264 360p bei 30 F/s 16:9 |
| Bildschirmfreigabe | ~ 300 KBit/s | H264 1080p bei 15 F/s |

Opus und H264 sind die bevorzugten Codecs für Peer-to-Peer-Anrufe und Telefonkonferenzen.

> **Wichtig:**
>
> Codierung nimmt mehr CPU-Leistung in Anspruch als die Decodierung auf dem Clientcomputer. Sie können die maximal mögliche Codierungsauflösung in der Citrix Workspace-App für Linux und Windows fest codieren. Siehe Geschätzte Codierungsleistung und Geschätzte Codierungsleistung für Microsoft Teams.

### Proxyserver

Berücksichtigen Sie je nach Standort des Proxys Folgendes:

- Proxykonfiguration auf dem VDA:

  Wenn Sie einen expliziten Proxyserver im VDA konfigurieren und Verbindungen über einen Proxy an localhost weiterleiten, schlägt die Umleitung fehl. Um den Proxy richtig zu konfigurieren, müssen Sie die Einstellung **Proxyserver für lokale Adressen umgehen** unter **Internetoptionen > Verbindungen > LAN-Einstellungen > Proxyserver** auswählen und `127.0.0.1:9002` umgehen.

  Wenn Sie eine PAC-Datei verwenden, muss Ihr VDA-Proxykonfigurationsskript aus der PAC-Datei **DIRECT** für `wss://127.0.0.1:9002` zurückgeben. Wenn nicht, schlägt die Optimierung fehl. Um sicherzustellen, dass das Skript **DIRECT**zurückgibt, verwenden Sie `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Proxykonfiguration in der Citrix Workspace-App:

  Wenn eine Zweigstelle für den Internetzugriff über einen Proxy konfiguriert ist, unterstützen folgende Versionen Proxyserver:

  - Citrix Workspace-App für Windows Version 2012 (Negotiate/Kerberos, NTLM, Basic und Digest. `Pac`-Dateien werden ebenfalls unterstützt.)
  - Citrix Workspace-App für Windows Version 1912 CU5 (Negotiate/Kerberos, NTLM, Basic und Digest. `Pac`-Dateien werden ebenfalls unterstützt.)

- Citrix Workspace-App für Linux Version 2101 (anonyme Authentifizierung)
- Citrix Workspace-App für Mac Version 2104 (anonyme Authentifizierung)

Clientgeräte mit früheren Releases der Citrix Workspace-App können keine Proxykonfigurationen lesen. Diese Geräte senden Datenverkehr direkt an Microsoft 365 TURN-Server.

> **Wichtig:**
>
> - Vergewissern Sie sich, dass das Clientgerät für die DNS-Auflösung eine Verbindung zum DNS-Server herstellen kann. Ein Clientgerät muss die folgenden FQDNs des Microsoft Teams Relay-Servers auflösen können:
>   - `worldaz.relay.teams.microsoft.com`
>   - `inaz.relay.teams.microsoft.com`
>   - `uaeaz.relay.teams.microsoft.com`
>   - `euaz.relay.teams.microsoft.com`
>   - `usaz.relay.teams.microsoft.com`
>   - `turn.dod.teams.microsoft.us`
>   - `turn.gov.teams.microsoft.us`
>
> Wenn DNS-Anfragen nicht erfolgreich sind, schlagen P2P-Anrufe bei externen Benutzern und die Medieneinrichtung für Telefonkonferenzen fehl.
>
> - Der Standort des Konferenzservers wird gemäß dem Standort des virtuellen Desktops des ersten Teilnehmers (und nicht des Clients) ausgewählt.

### Anrufeinrichtung und Medienflusspfad

Wenn möglich, versucht die HDX WebRTC Media Engine in der Citrix Workspace-App (HdxRtcEngine.exe), eine direkte Netzwerkverbindung mit SRTP über UDP in einem Peer-to-Peer-Anruf herzustellen. Wenn die UDP-High-Ports blockiert sind, fällt die Media Engine auf TCP/TLS 443 zurück.

Die HDX Media Engine unterstützt ICE, STUN (Session Traversal Utilities for NAT) und TURN (Traversal Using Relays around NAT) für die Kandidatendiscovery und den Verbindungsaufbau. Der Endpunkt muss daher in der Lage sein, DNS-Auflösungen durchzuführen.

Angenommen, es gibt keinen direkten Pfad zwischen den beiden Peers bzw. zwischen einem Peer und einem Konferenzserver, wenn Sie einem Anruf oder einer Besprechung mit mehreren Teilnehmern beitreten. HdxRtcEngine.exe verwendet einen Microsoft Teams-Transportrelayserver in Microsoft 365, um den anderen Peer bzw. den Medienprozessor zu erreichen, auf dem Besprechungen gehostet werden. Ihr Clientcomputer muss Zugriff auf drei Microsoft 365-Subnetz-IP-Adressbereiche und vier UDP-Ports haben (oder TCP/TLS 443 als Fallback, wenn UDP gesperrt ist). Weitere Informationen finden Sie im Architekturdiagramm im Call Setup und Office 365 URLs and IP address ranges ID 11.

| ID | Kategorie | Adressen | Zielports |
|---|---|---|---|
| 11 | Optimieren erforderlich | 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14 | **UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (Fallback) |

Diese Bereiche enthalten Transport-Relays und Medienprozessoren mit einem Azure Load Balancer-Front-End.
Microsoft Teams Transport-Relays bieten die Funktionen STUN und TURN, sie sind aber keine ICE-Endpunkte. Microsoft Teams Transport-Relays beenden auch keine Medien, TLS und führen keine Transcodierung durch. Relays können als Bridge zwischen TCP (wenn HdxRtcEngine.exe TCP verwendet) und UDP fungieren, wenn sie den Datenverkehr an andere Peers oder Medienprozessoren weiterleiten.

Die WebRTC Media Engine der Workspace-App kontaktiert das nächstgelegene Microsoft Teams Transport-Relay in der Microsoft 365-Cloud. Die Media Engine verwendet Anycast-IP und Port 3478-3481 UDP (verschiedene UDP-Ports pro Workload, wobei Multiplexing möglich ist) oder 443 TCP/TLS für Fallbacks. Die Anrufqualität hängt vom zugrunde liegenden Netzwerkprotokoll ab. Da UDP über TCP immer empfehlenswert ist, sollten Sie Ihre Netzwerke so gestalten, dass UDP-Datenverkehr in der Zweigstelle möglich ist.

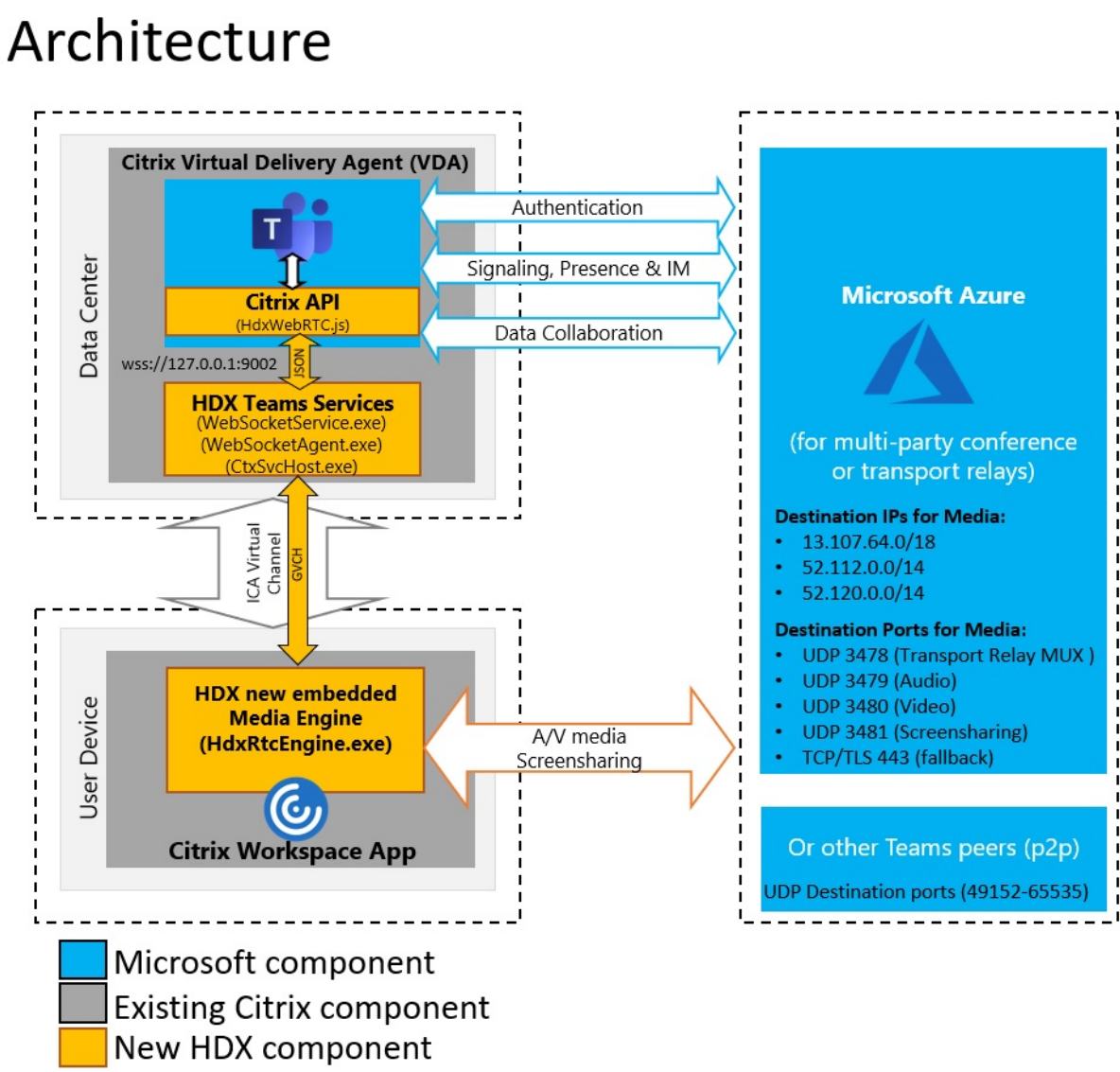
Wurde Microsoft Teams im optimierten Modus geladen und wird HdxRtcEngine.exe auf dem Endpunkt ausgeführt, können ICE-Fehler dazu führen, dass bei der Anrufeinrichtung ein Fehler auftritt oder Audio-/Video-Daten nur in einer Richtung übertragen werden. Wenn ein Anruf nicht zustande kommt oder der Medienfluss keinen vollen Duplexmodus bietet, sollten Sie zuerst die **Wireshark-Trace** auf dem Endpunkt prüfen. Weitere Informationen zum Sammeln von ICE-Kandidaten finden Sie unter “Sammeln von Protokollen”im Abschnitt Support.

> **Hinweis:**
>
> Wenn die Endpunkte keinen Internetzugriff haben, können Benutzer unter Umständen dennoch einen Peer-to-Peer-Anruf tätigen, wenn beide in demselben LAN sind. Besprechungen schlagen fehl. In diesem Fall gibt es ein Timeout von 30 Sekunden, bevor der Anruf eingerichtet wird.

#### Einrichten von Anrufen

Dieses Architekturdiagramm dient als visuelle Referenz für die Flusssequenz bei einem Anruf. Die entsprechenden Schritte sind im Diagramm angegeben.




**Architektur**

1. Sie starten Microsoft Teams.
2. Microsoft Teams authentifiziert sich bei O365. Mandantenrichtlinien werden an den Microsoft Teams-Client übertragen, und relevante TURN- und Signalkanalinformationen werden an die App weitergeleitet.
3. Microsoft Teams erkennt, dass es in einem VDA ausgeführt wird, und sendet API-Aufrufe an die Citrix JavaScript-API.
4. Citrix JavaScript in Microsoft Teams öffnet eine sichere WebSocket-Verbindung zu WebSocket-Service.exe, das auf dem VDA ausgeführt wird. Dies generiert WebSocketAgent.exe in der Benutzersitzung.
5. WebSocketAgent.exe instanziiert einen generischen virtuellen Kanal, indem es den Citrix HDX-Microsoft Teams-Umleitungsdienst (CtxSvcHost.exe) aufruft.

6. Die HDX-Engine der Citrix Workspace-App (wfica32.exe) erzeugt einen neuen Prozess namens HdxRtcEngine.exe. Dies ist die neue WebRTC-Engine, die für die Optimierung für Microsoft Teams verwendet wird.
7. Die Citrix Media Engine und Teams.exe verfügen über einen 2-Wege-Pfad für virtuelle Kanäle und beginnen mit der Verarbeitung von Multimediaanfragen.

   ——Benutzeranrufe——

8. **Peer A** klickt auf die **Anruftaste**. Teams.exe kommuniziert mit den Microsoft Teams-Diensten in Microsoft 365, die einen End-to-End-Signalpfad mit **Peer B** einrichten. Microsoft Teams schickt eine Anfrage an HdxRtcEngine zu diversen unterstützten Anrufparametern (Codecs, Auflösungen usw.). Dies wird auch als Angebot des Protokolls SDP (Session Description Protocol) bezeichnet. Die Anrufparameter werden dann über den Signalpfad an die Microsoft Teams-Dienste in Microsoft 365 und von dort an den anderen Peer weitergeleitet.
9. SDP-Angebot/Antwort (Single-Pass-Verfahren) erfolgt über den Signalkanal, und die ICE-Konnektivitätsprüfungen werden abgeschlossen (Netzwerkadressübersetzung und Firewalldurchquerung durch Bindungsanfragen für STUN). Anschließend erfolgt der Medienfluss per SRTP (Secure Real-Time Transport Protocol) direkt zwischen HdxRtcEngine und dem anderen Peer (oder Microsoft 365-Konferenzservern im Falle einer Besprechung).

## Microsoft-Telefonsystem

Das Microsoft-Telefonsystem aktiviert die Anrufsteuerung und PBX in der Microsoft 365-Cloud mit Microsoft Teams. Die Optimierung für Microsoft Teams unterstützt Microsoft Phone System mit Microsoft 365-Anrufplänen oder Direct Routing. Beim direktem Routing können Sie jeden unterstützten Session Border Controller (SBC) ohne zusätzliche On-Premises-Software mit Microsoft Phone System verbinden.
Anrufwarteschlangen, Übertragen, Weiterleiten, Halten, Stummschalten und Fortsetzen eines Anrufs werden unterstützt.

### Mehrfrequenzwahlverfahren

Das Mehrfrequenzwahlverfahren (DTMF) wird ab den folgenden Versionen der Citrix Workspace-App unterstützt:

- Citrix Workspace-App für Windows Version 2102
- Citrix Workspace-App für Windows LTSR 1912 CU5 (nur Windows 10)
- Citrix Workspace-App für Linux, Version 2101
- Citrix Workspace-App für Mac Version 2101
- Citrix Workspace-App für Chrome OS Version 2111.1

### Unterstützung für dynamischen Notruf

Ab Version 2112 unterstützt die Citrix Workspace-App den dynamischen Notruf. Wenn Sie Microsoft-Anrufpläne, Operator Connect und Direct Routing verwenden, haben Sie folgende Möglichkeiten:

- Konfigurieren und Übermitteln von Notrufen.
- Benachrichtigen von Sicherheitspersonal.

Die Benachrichtigung erfolgt basierend auf dem aktuellen Standort der Citrix Workspace-App auf dem Endpunkt anstelle des Microsoft Teams-Clients, der auf dem VDA ausgeführt wird.

Das US-Gesetz (Ray Baum's Law) schreibt vor, dass der Standort des Notrufanrufers an die entsprechende Einsatzleitstelle (PSAP) übertragen wird. Die Microsoft Teams-Optimierung mit HDX erfüllt die Bestimmungen des Gesetzes Ray Baum's Law bei Nutzung mit folgenden Citrix Workspace-App-Versionen:

- Citrix Workspace-App für Windows Version 2112.1 und später
- Citrix Workspace-App für Linux, Version 2112 und später
- Citrix Workspace-App für Mac Version 2112 und später
- Citrix Workspace-App für Chrome OS Version 2112 und später

Zum Ermöglichen dynamischer Notrufe muss der Administrator im Microsoft Teams Admin Center Folgendes zur Erstellung einer Netzwerk- oder Notfallstandortkarte konfigurieren:

- Netzwerkeinstellungen
- Standortinformationsdienst (LIS)

Weitere Informationen zu dynamischen Notrufen finden Sie in der Dokumentation von Microsoft.

Die Citrix Workspace-App übermittelt folgende Standortinformationen an Microsoft Teams:

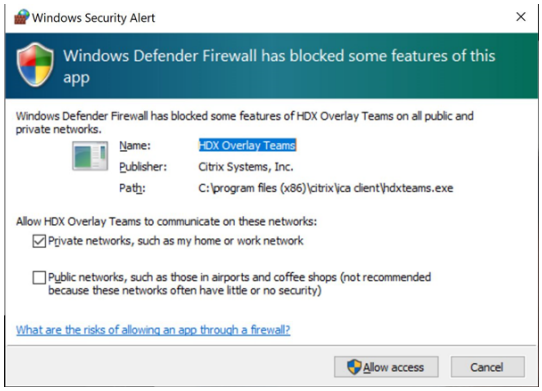
- Gehäuse-ID/Port-ID per Link Layer Discovery Protocol (LLDP) für Ethernet-/Switch-Verbindungen. Ethernet/Switch (LLDP) wird unterstützt unter:
  - Windows-Versionen 8.1 und 10
  - macOS (erfordert LLDP-Aktivierungssoftware). Zum Download der LLDP-Aktivierungssoftware suchen Sie unter `www.microsoft.com` nach LLDP-Aktivierungssoftware.
  - Linux (erfordert LLDP-Bibliothek in der OS-Distribution des Thin Clients)
- WLAN BBSID und {IPv4-IPv6; Subnetz; MAC-Adresse} des Endpunkts, auf dem die Citrix Workspace-App installiert ist.
  - Subnetz- und WLAN-basierte Standorte werden von der Workspace-App für Windows, Linux und Mac unterstützt.
- Breitengrad und Längengrad, wenn die Benutzerberechtigung auf OS-Ebene, auf der die Citrix Workspace-App installiert ist, erteilt wurde.

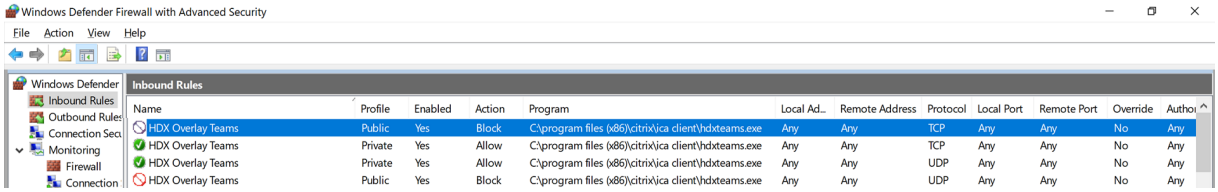
- Dies wird auf allen Workspace-App-Plattformen unterstützt. Für Citrix Workspace für Linux müssen Sie die `libgps`-Bibliothek in die OS-Distribution des Thin Clients aufnehmen (sudo apt-get install libgps23 gpsd lldpd).

### Überlegungen zu Firewalls

Wenn Benutzer zum ersten Mal einen optimierten Anruf mit dem Microsoft Teams-Client initiieren, wird möglicherweise eine Warnung mit den **Windows-Firewalleinstellungen** angezeigt. In der Warnung werden Benutzer aufgefordert, die Kommunikation für HdxTeams.exe oder HdxRtcEngine.exe (HDX Overlay Microsoft Teams) zuzulassen.




Die folgenden vier Einträge werden unter **Eingehende Regeln** in der Konsole **Windows Defender Firewall > Erweiterte Sicherheit** hinzugefügt. Sie können bei Bedarf restriktivere Regeln anwenden.



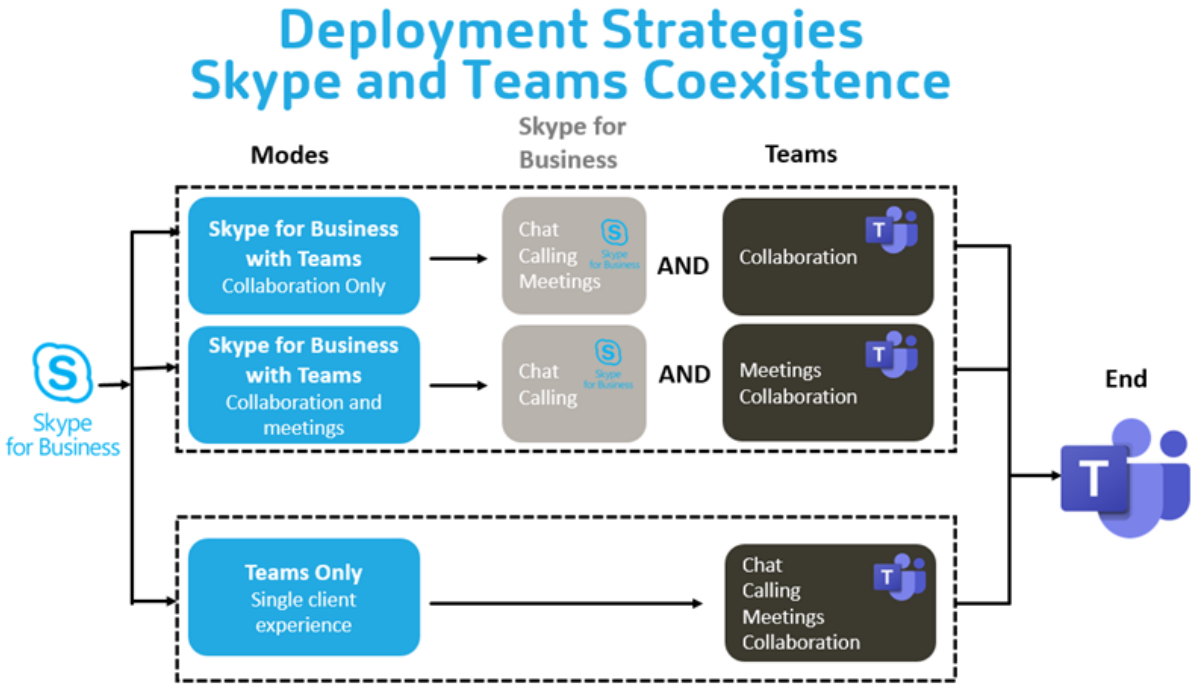

### Koexistenz von Microsoft Teams und Skype for Business

Sie können Microsoft Teams und Skype for Business nebeneinander als separate Lösungen mit Funktionsüberschneidungen bereitstellen.
Weitere Informationen finden Sie unter Hinweise zur Koexistenz und Interoperabilität von Microsoft Teams und Skype for Business.

Das Citrix RealTime Optimization Pack und die HDX-Optimierung für Microsoft Teams-Multimedia-Engines befolgen dann die Konfiguration in Ihrer Umgebung. Beispiele sind Island Mode und Zusammenarbeit zwischen Skype for Business und Microsoft Teams. Außerdem Zusammenarbeit zwischen Skype for Business und Microsoft Teams und Besprechungen.

Zugriff auf Peripheriegeräte kann jeweils nur einer Anwendung gleichzeitig gewährt werden. Wenn beispielsweise die RealTime Media Engine bei einem Anruf auf die Webcam zugreift, wird dadurch das Imaginggerät während des Anrufs gesperrt. Wenn das Gerät freigegeben wird, steht es für Microsoft Teams zur Verfügung.




### Citrix SD-WAN: optimierte Netzwerkkonnektivität für Microsoft Teams

Eine optimale Audio- und Videoqualität erfordert eine Netzwerkverbindung zur Microsoft 365-Cloud mit geringer Latenz, wenig Jitter und geringem Paketverlust. Wenn Citrix Workspace App-Benutzer in Zweigstellen für den Microsoft Teams-RTP-Datenverkehr (Audio/Video) einen Backhaul zum Datencenter benötigen, bevor sie ins Internet gehen, kann dies zu übermäßiger Latenz führen. Es kann auch zu Staus bei WAN-Verbindungen kommen. Citrix SD-WAN optimiert die Konnektivität für Microsoft Teams gemäß den Netzwerkverbindungsprinzipien für Microsoft 365. Citrix SD-WAN verwendet die Microsoft REST-basierte Microsoft 365-IP-Adresse samt Webdienst und naheliegender DNS. Dies dient dazu, den Microsoft Teams-Datenverkehr zu identifizieren, zu kategorisieren und zu steuern.

Breitband-Internetverbindungen von Unternehmen verzeichnen immer wieder Paketverluste, exzessiven Jitter und Ausfälle.

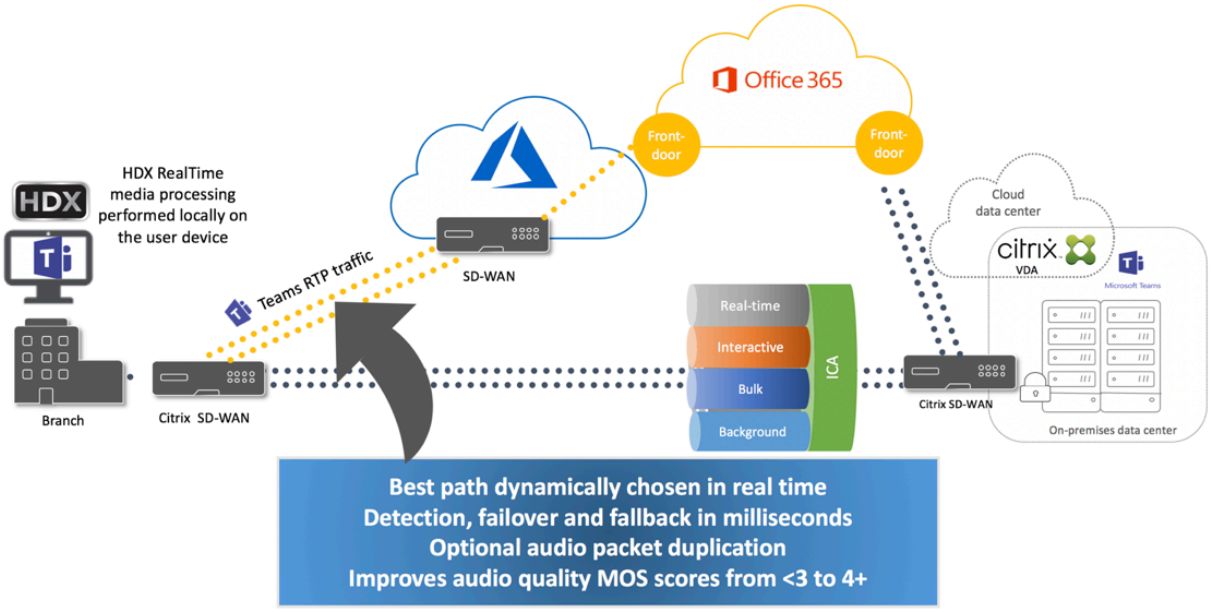
Citrix SD-WAN bietet zwei Lösungen, um die Audio-/Videoqualität in Microsoft Teams auch bei variabler oder verschlechterter Netzwerkintegrität zu erhalten.

- Wenn Sie Microsoft Azure verwenden, bietet ein in Azure VNET bereitgestelltes virtuelles Gerät (Citrix SD-WAN-VPX) erweiterte Möglichkeiten zur Konnektivitätsoptimierung. Dazu gehören ein Seamless-Link-Failover und “Packet Racing”für Audiopakete.

- Citrix SD-WAN-Kunden können sich über Citrix Cloud Direct Service mit Microsoft 365 verbinden. Dieser Dienst bietet eine zuverlässige und sichere Bereitstellung für den gesamten Datenverkehr ins Internet.

Wenn die Qualität der Branch-Internetverbindung kein Problem darstellt, reicht es möglicherweise aus, die Latenz zu minimieren. Leiten Sie den Microsoft Teams-Datenverkehr direkt von der Citrix SD-WAN-Zweigstelle zur nächsten Microsoft 365-Haustür, um die Latenz zu minimieren. Weitere Informationen finden Sie unter Citrix SD-WAN Office 365-Optimierung.




## Meetings und Chat mit mehreren Fenstern

Sie können mehrere Meeting- bzw. Chat-Fenster für Microsoft Teams unter Windows verwenden. Einzelheiten zum Pop-Out-Feature finden Sie unter Microsoft Teams Pop-Out Windows for Chats and Meetings auf der Microsoft 365-Website.

> **Hinweis:**
>
> Das Feature wird für die Citrix Workspace-App für Windows 2112.1, Mac 2203, Linux 2203 und ChromeOS 2303 unterstützt. Es erfordert VDA 2112 oder höher und wurde auf 1912 CU6+ LTSR und VDA 2112 zurückportiert.

## Hintergrundunschärfe und Hintergrundeffekte

Die Citrix Workspace-App für Windows, Mac, Linux und ChromeOS/HTML5 unterstützt Hintergrundunschärfe und Hintergrundeffekte für die Microsoft Teams-Optimierung mit HDX.

Sie können den Hintergrund weichzeichnen oder durch ein Standardbild ersetzen, damit Ablenkungen vermieden und die Konzentration auf die Silhouette (Körper und Gesicht) erleichtert wird. Sie können das Feature für Einzel- und Konferenzgespräche verwenden.

> **Hinweis:**
>
> Dieses Feature ist in die Benutzeroberfläche und die Schaltflächen von Microsoft Teams integriert. Unterstützung für mehrere Fenster ist eine Voraussetzung, die ein VDA-Update auf 2112 oder später erfordert. Weitere Informationen finden Sie unter Meetings und Chat mit mehreren Fenstern.

Für Microsoft Teams-Steuerelemente für Hintergrundunschärfe und -effekte sind die folgenden Mindestversionen erforderlich:

- Citrix Workspace-App für Windows 2207
- Citrix Workspace-App für Mac 2301
- Citrix Workspace-App für Linux 2212
- Citrix Workspace-App für ChromeOS 2303

**Einschränkungen:**

- Der Client muss mit dem Internet verbunden sein, während das Hintergrundbild durch ein Microsoft Teams-Standardbild setzt wird.
- Das Ersetzen durch Administrator- und benutzerdefinierte Hintergrundbilder wird in der Microsoft Teams-Benutzeroberfläche nicht unterstützt. Benutzerdefinierte Hintergrundbilder können über Konfigurationseinstellungen auf dem Client konfiguriert werden, wenn das Bild auch auf dem Client gespeichert ist.

#### Festlegen eines benutzerdefinierten Hintergrundbilds

Die folgenden Registrierungsschlüssel sind nur erforderlich, wenn Sie die Microsoft Teams-Benutzeroberfläche nicht zur Steuerung des Features verwenden möchten oder ein Administrator das Standardverhalten außer Kraft setzen möchte. Deaktivieren Sie beispielsweise die Hintergrundunschärfe, weil der Endpunkt nicht leistungsfähig genug ist.

**Unter Windows** Um ein benutzerdefiniertes Hintergrundbild einzurichten, müssen Administratoren oder Endbenutzer den folgenden Registrierungsschlüssel auf dem Client oder Endpunkt konfigurieren:

Ort: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Name: VideoBackgroundEffect
- Typ: DWORD

- Wert: 0 (deaktiviert), 1 (aktiviert), 2 (Hintergrundbild ersetzen)

Bei einem Wert von 1 wird der Hintergrund unscharf. Dieser Wert kann vom Endbenutzer oder vom Administrator festgelegt werden.

Bei einem Wert von 2 muss auch der Schlüssel **VideoBackgroundImage** vorhanden sein. Nur der Administrator kann diesen Wert festlegen. Der folgende Schlüssel ist nur erforderlich, wenn Sie das Hintergrundbild ersetzen möchten (für das Weichzeichnen ist er nicht erforderlich):

- Name: VideoBackgroundImage
- Typ: REG_SZ
- Wert: my_image_name.jpeg

Das Videohintergrundbild muss im Verzeichnis `C:\Program Files (x86)\Citrix\ICA Client` sein.

Diese Registrierungskonfiguration kann auch verwendet werden, um die Hintergrundunschärfe oder das Ersetzen von Bildern in der Citrix Workspace-App 2206 ohne Microsoft Teams-UI-Selektor zu aktivieren. Das heißt, wenn Ihre Umgebung oder Ihr VDA den Mehrfenstermodus nicht unterstützt, können Sie dennoch das Workaround in der HKCU-Registrierung mit der Citrix Workspace-App 2206 oder höher anwenden, um ein ähnliches Ergebnis zu erzielen, obwohl der Benutzer die Funktionalität während der HDX-Sitzung oder des Microsoft Teams-Anrufs nicht steuern kann.

Änderungen am Registrierungsschlüssel werden nur wirksam, wenn die HDX-Sitzung eine Verbindung herstellt.

**Unter Mac** Speicherort des vom Benutzer heruntergeladenen Bilds: */Users/username/Downloads/any_image.png*

Führen Sie die folgenden Befehle aus, um das benutzerdefinierte Bild als Standardbild festzulegen:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

**Unter Linux** Speicherort des vom Benutzer heruntergeladenen Bilds: */home/username/Downloads/any_image.jpg*

Erstellen Sie die Datei */var/.config/citrix/hdx_rtc_engine/config.json* und fügen Sie die folgenden Konfigurationsschlüssel im JSON-Format hinzu. Zum Beispiel:

```
1 {
2
3
4 "VideoBackgroundEffect":2,
```

```
5
6  "VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
7
8   }
9
10 <!--NeedCopy-->
```

**Unter HTML5** Bei HTML5 wird nur die Hintergrundunschärfe unterstützt. Hintergrundbild ersetzen wird nicht unterstützt.

Gehen Sie wie folgt vor, um die Hintergrundunschärfe zu aktivieren:

1. Gehen Sie zur Datei **configuration.js** im Ordner **HTML5Client**.
2. Fügen Sie das Attribut **backgroundEffects** hinzu und legen Sie es auf **true** fest. Zum Beispiel:

```
1  'features' : {
2
3      'msTeamsOptimization' :
4      {
5
6          'backgroundEffects' : true
7       }
8
9   }
10
11 <!--NeedCopy-->
```

3. Speichern Sie die Änderung.

#### Überlegungen zur Client-CPU-Auslastung

Das Unschärfefeature verwendet die CPU sparsam, sie müssen dennoch mit einem Anstieg des Verbrauchs rechnen. Bei einem Thin Client mit einem Intel® Pentium® Silver-Chip 4 Core und 1,5 GHz und TurboBoost bis zu 2,8 GHz erhöht die Hintergrundunschärfe beispielsweise die CPU-Auslastung um etwa 2%. Die durchschnittliche CPU-Auslastung liegt unter 20%.

### Katalogansicht und aktive Sprecher in Microsoft Teams

Microsoft Teams unterstützt Layouts **Gallery**, **Large gallery** und **Together mode**.

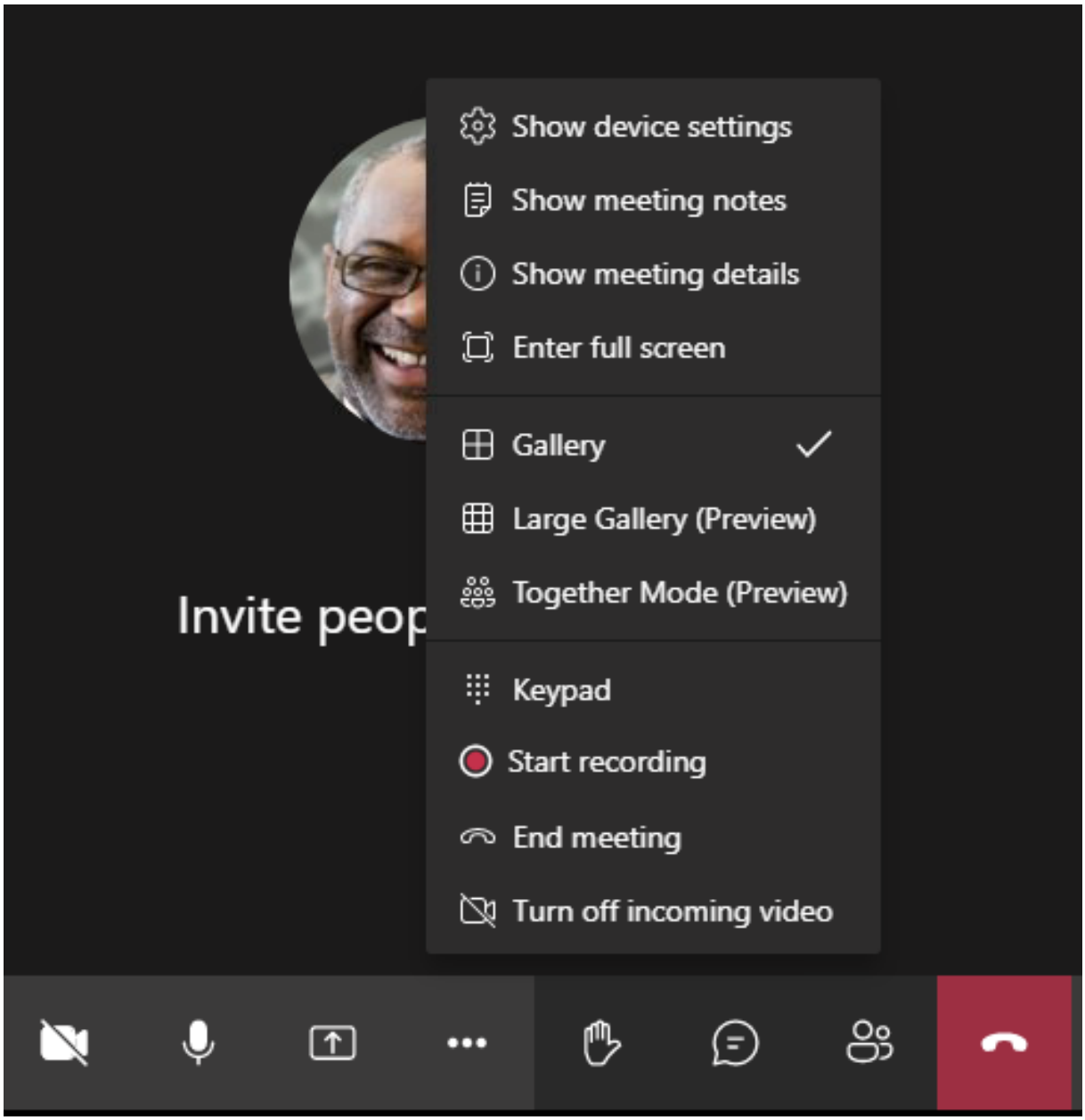
In Microsoft Teams wird ein 2x2-Raster mit Videostreams von vier Teilnehmern angezeigt (= **Gallery**). In diesem Modus sendet Microsoft Teams vier Videostreams zur Decodierung an das Clientgerät. Bei mehr als vier Teilnehmern werden nur die letzten vier aktivsten Sprecher auf dem Bildschirm angezeigt.

Microsoft Teams bietet auch die Ansicht “Large Gallery”mit einem Raster bis zu 7x7. Der Microsoft Teams-Konferenzserver stellt dann einen einzigen Videofeed zusammen und sendet ihn zur Decodierung an das Clientgerät, was zu einem geringeren CPU-Verbrauch führt. Dieser matrixartige Einzelfeed kann auch das Eigenvorschauvideo der Benutzer enthalten.

Microsoft Teams unterstützt auch den **Together**-Modus als Teil der neuen Benutzeroberfläche “New Meeting Experience”. Mit KI-Segmentierungstechnologie zur digitalen Platzierung der Teilnehmer auf einen gemeinsamen Hintergrund werden in Microsoft Teams alle Teilnehmer in dasselbe Auditorium platziert.

Diese Modi können während einer Telefonkonferenz über die Optionen **Gallery**, **Large Gallery** und **Together mode** im Menü (…) auswählt werden.



Einschränkungen bei der Unterstützung des Videoseitenverhältnisses (CWA für Windows 2102, CWA für Linux 2106, CWA für MAC 2106 und später):

- Die Option **Frame ausfüllen** ist in der Ansicht "Galerie"bzw. "Große Galerie"verfügbar. Mit ihr wird die Videogröße so angepasst, dass sie in das Unterfenster passt. Mit der Option **An Frame anpassen** werden schwarze Balken an den Seiten des Videos angezeigt, welches nicht abgeschnitten wird.

Die folgende Tabelle bietet einen Vergleich der Layouts "Galerie"und "Große Galerie":

| | Galerieansicht 2x2 (Standard) | Große Galerieansicht |
|---|---|---|
| Layout/Raster | Zeigt ein 2x2-Raster mit Videostreams von vier Teilnehmern an. Nur die letzten vier aktivsten Sprecher erscheinen auf dem Bildschirm. Andere Teilnehmer werden nicht im Raster angezeigt. | Zeigt ein 7x7-Raster mit Videostreams von 49 Teilnehmern an. |
| Mischtechnik | Ein Medienrouter leitet einzelne Streams von jedem Teilnehmer an jeden Benutzer weiter. | Ein zentraler Konferenzserver mischt und transcodiert alle Audio- oder Videodaten und erstellt für jeden Teilnehmer ein angepasstes zusammengesetztes Layout. Dadurch entsteht etwas zusätzliche Latenz. |
| Aktiver Sprecher | Der neue aktive Sprecher ersetzt den am wenigsten aktiven Lautsprecher im Raster. | Zeigt alle Teilnehmer an, unabhängig davon, ob sie aktiv oder inaktiv sind. |
| Codierung am Endpunkt | Ein oder mehrere Videostreams können am Endpunkt codiert werden, wenn Simulcast aktiviert ist. Weitere Informationen zur Simulcast-Unterstützung finden Sie unter Simulcast. | Ein oder mehrere Videostreams können am Endpunkt codiert werden, wenn Simulcast aktiviert ist. Weitere Informationen zur Simulcast-Unterstützung finden Sie unter Simulcast. |

| | Galerieansicht 2x2 (Standard) | Große Galerieansicht |
|---|---|---|
| Decodierung am Endpunkt | Jeder Teilnehmer erhält bis zu vier einzelne Medienstreams. Dies erhöht den CPU-Verbrauch am Endpunkt um HdxRtcEngine.exe (zum Decodieren/Rendering). | Jeder Teilnehmer erhält nur einen einzigen Stream für Audio und Video. Diese Einstellung senkt den CPU-Verbrauch am Endpunkt. |
| Maximale Auflösung | 720 p. Wenn vier Teilnehmer Videos teilen, beträgt die maximale Auflösung 360p pro Videofeed. Wenn weniger als vier Teilnehmer Videos teilen, ist die Auflösung pro Videofeed möglicherweise höher. | 720p für das zusammengesetzte Layout oder das Mischen. In einem zusammengesetzten Layout ist kein qualitativ hochwertiger Videostream pro Teilnehmer erforderlich. Deshalb reduziert jeder Absender die Auflösung oder die Upload-Bitrate. |
| Problem "Langsamer Benutzer" | Sender ändert Qualität jeder Modalität (Audio/Video/Bild-schirmfreigabe) auf die niedrigste gemeinsame Netzwerkqualität unter den Teilnehmern. Dieser Multimediastream wird dann an alle anderen Teilnehmer weitergeleitet. Infolgedessen wirken sich schlechte Netzwerkbedingungen bei einem Teilnehmer auf die Qualität für alle anderen im Gespräch aus. | Weniger anfällig für das Szenario der niedrigsten gemeinsamen Netzwerkqualität. Der Konferenzserver bietet verschiedene Qualitätsstufen in Abhängigkeit von den Netzwerkbedingungen einzelner Teilnehmer. |
| Eigenvorschau | Zeigt eine Miniaturansicht von Ihnen in Echtzeit an. | Zeigt eine Miniaturansicht von Ihnen und gemischt mit den übrigen Videofeeds an. Infolgedessen sehen Sie sich möglicherweise im Hauptvideolayout mit einer zusätzlichen Verzögerung. |

### Bildschirmfreigabe in Microsoft Teams

Microsoft Teams verwendet die videobasierte Bildschirmfreigabe (VBSS), um den freigegebenen Desktop mit Videocodecs wie H264 zu codieren und einen High-Definition-Stream zu erstellen. Bei der HDX-Optimierung wird die eingehende Bildschirmfreigabe als Videostream behandelt.

Benutzer können in der Citrix Workspace-App ab Version 2109 für Windows, Linux, Mac und Citrix Workspace-App 2303 für ChromeOS ihre Bildschirme und Videokameras gleichzeitig freigeben.

In früheren Versionen wird der Videofeed der ursprünglichen Kamera angehalten, wenn der andere Gesprächsteilnehmer während eines Videoanrufs seinen Desktop freigibt. Stattdessen wird der Videofeed für die Bildschirmfreigabe angezeigt. Der Peer muss die Kamerafreigabe dann manuell fortsetzen.

> **Hinweis für PowerPoint Live**
>
> Diese Einschränkung besteht nicht, wenn Sie Inhalte aus PowerPoint Live freigeben. In diesem Fall können andere Gesprächsteilnehmer weiterhin Ihren Webcamfeed und Ihre Inhalte sehen und zwischen einzelnen Folien wechseln. In diesem Szenario werden die Folien auf dem VDA gerendert. Um auf ein Foliendeck in PowerPoint Live zuzugreifen, klicken Sie auf die Schaltfläche der Freigabeablage (Share tray) und wählen Sie dort eine PowerPoint-Folie aus. Oder klicken Sie auf "Durchsuchen", um die gewünschte PowerPoint-Datei auf Ihrem Computer oder in OneDrive zu lokalisieren.

Die ausgehende Bildschirmfreigabe wird ebenfalls optimiert und in die Citrix Workspace-App ausgelagert. In diesem Fall erfasst und überträgt die Media Engine nur das Fenster des Citrix Desktop Viewer (CDViewer.exe) mit einem roten Rahmen darum. Lokale Anwendungen, die den Desktop Viewer überlappen, werden nicht erfasst.

> **Hinweis**
>
> Legen Sie in der Citrix Workspace-App für Mac spezifische Berechtigungen fest, um die Bildschirmfreigabe zu aktivieren. Weitere Informationen finden Sie unter Systemanforderungen.

#### Mehrere Monitore

Wird der Desktop Viewer (CDViewer.exe) im Vollbildmodus über mehrere Bildschirme hinweg angezeigt, kann in der Citrix Workspace-App 2106 oder später (Windows/Linux/Mac) ausgewählt werden, welcher Bildschirm freigegeben werden soll.

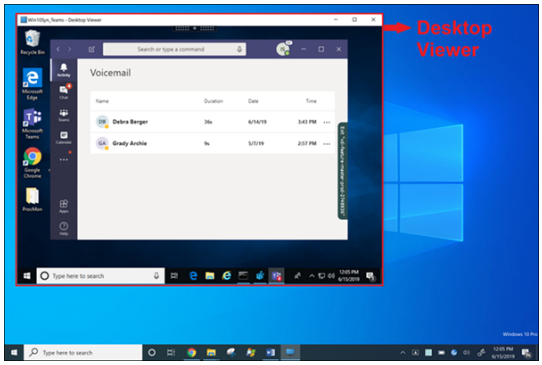
**Bekannte Einschränkung:**

- Wenn Desktop Viewer deaktiviert ist oder Desktop Lock verwendet wird, ist die Multimonitorauswahl in der Microsoft Teams-Bildschirmauswahl nicht verfügbar. Der Desktop Viewer

kann durch Bearbeiten der Dateivorlage `.ICA` oder von `StoreFront web.config` deaktiviert werden. Die Tastenkombination UMSCHALT+F2 ist nicht mit der Multimonitorfreigabe kompatibel.

- In Versionen der Workspace-App, die älter als 2106 ist, wird nur der primäre Bildschirm freigegeben. Ziehen Sie die Anwendung im virtuellen Desktop auf den primären Monitor, damit der andere Gesprächsteilnehmer sie sehen kann.
- Die Multimonitorfreigabe funktioniert möglicherweise nicht, wenn Sie die Citrix Workspace-App mit dem Feature für virtuelles Bildschirmlayout (logische Partition eines einzelnen physischen Monitors) konfigurieren. In diesem Fall werden alle virtuellen Monitore als zusammengesetztes Bild freigegeben.
- Ältere Versionen der Citrix Workspace-App für Windows (1907 bis 2008) teilen auch eine lokale Anwendung, die auf dem Clientcomputer ausgeführt wird. Diese Freigabe ist nur möglich, wenn die lokale App über Desktop Viewer überlagert wurde. Dieses Verhalten wurde in 2009.6 oder höher und in 1912 CU5 oder höher entfernt.
- Wenn Sie während der Bildschirmfreigabe vom Fenstermodus in den Vollbildmodus wechseln, wird die Bildschirmfreigabe beendet. Sie müssen die Bildschirmfreigabe anhalten und neu starten, damit sie funktioniert.




**Bildschirmfreigabe aus Seamlessanwendung:**

Wenn Sie Microsoft Teams als eigenständige Seamlessanwendung veröffentlichen, erfasst die Bildschirmfreigabe den lokalen Desktop Ihres physischen Endpunkts. Dafür ist mindestens Version 1909 der Citrix Workspace-App erforderlich.

### App-Freigabe

Ab der Citrix Workspace-App für Windows 2112 und VDA 2112.1 unterstützt Microsoft Teams die App-Freigabe.

Microsoft Teams unterstützt ab Citrix Workspace-App für Windows 2109, Mac 2203, Linux 2209 und VDA 2109 die Bildschirmfreigabe für bestimmte Apps, die in der virtuellen Sitzung ausgeführt werden. Freigabe einer App:

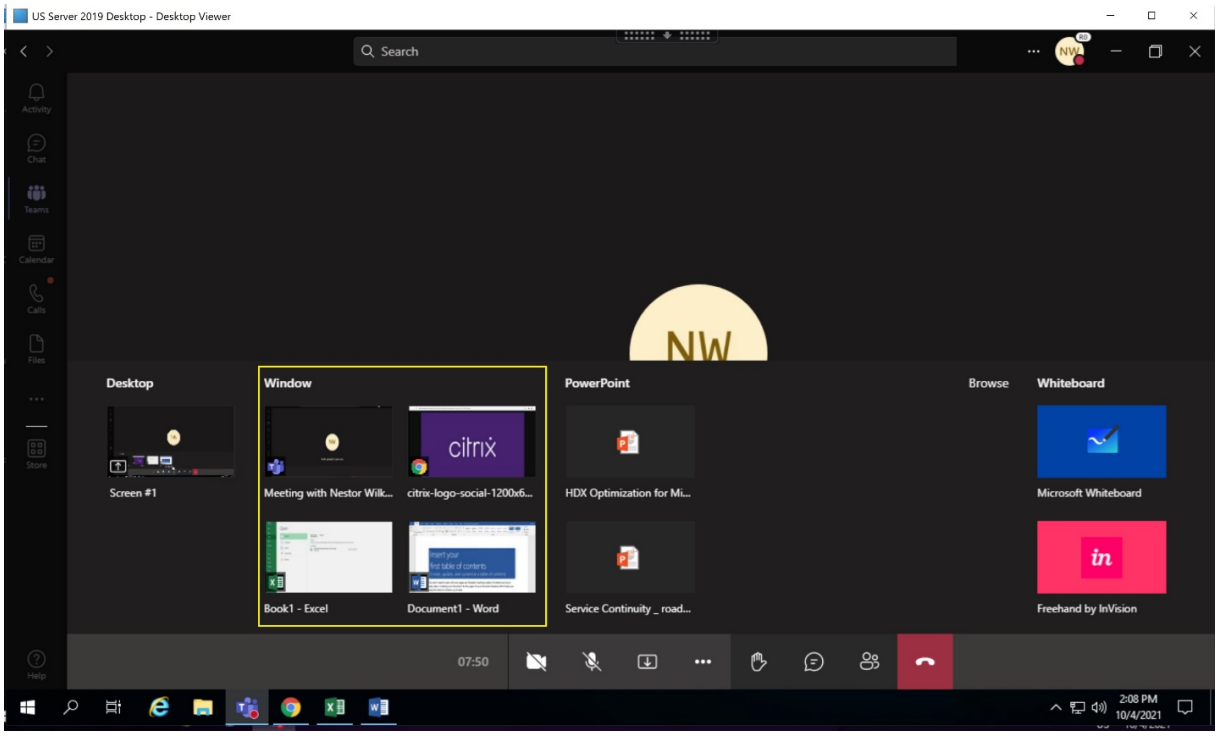
1. Navigieren Sie innerhalb der Remotesitzung zur Microsoft Teams-App.
2. Klicken Sie in der Microsoft Teams-Benutzeroberfläche auf **Inhalt freigeben**.
3. Wählen Sie die App aus, die Sie in der Besprechung freigeben möchten. Die ausgewählte App wird rot umrandet angezeigt, und die übrigen Gesprächsteilnehmer können die freigegebene App sehen.

Um eine andere App freizugeben, klicken Sie erneut auf **Inhalt freigeben** und wählen eine neue App aus.

Wenn Sie die App-Freigabe deaktivieren möchten, erstellen Sie den folgenden Registrierungsschlüssel auf dem VDA unter `HKLM\SOFTWARE\Citrix\Graphics`:
Name: `UseWsProvider`
Typ: `DWORD`
Wert: 0

> **Hinweis:**
>
> - Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.
> - Wenn Sie eine App minimieren, zeigt Microsoft Teams das letzte Bild der freigegebenen App an. Sie können das Fenster maximieren, um die Bildschirmfreigabe fortzusetzen.
> - Die Bildschirmfreigabe hängt von der VDA-seitigen Erfassung des Fensters ab. Der Inhalt wird dann mit einer maximalen Rate (30 Frames pro Sekunde) an die Citrix Workspace-App weitergeleitet. Die Citrix Workspace-App leitet den Inhalt an die Peers oder den Konferenzserver weiter.




**Bekannte Einschränkungen bei der Bildschirmfreigabe einer bestimmten App:**

- Der Mauszeiger ist nicht sichtbar, wenn Sie eine App auf dem Bildschirm freigeben.
- Wenn Sie eine App während der Freigabe minimieren, wird nur das App-Symbol in der Bildschirmauswahl angezeigt. Das Miniaturbild der App ist in der Bildschirmauswahl nicht zu sehen. Sie können den Inhalt nicht teilen und die rote Umrandung wird erst angezeigt, wenn Sie die App maximiert haben.
- Als Apps mit lokalem App-Zugriff werden Apps aufgelistet, die für Desktop-Apps im optimierten Microsoft Teams im VDA freigegeben werden können. Wenn Sie die App jedoch in der Liste auswählen, wird das Ergebnis möglicherweise nicht wie erwartet angezeigt.

**Kompatibilität mit App-Schutz**

Die Bildschirmfreigabe einer bestimmten App ist mit dem App-Schutzfeature in HDX-optimiertem Microsoft Teams kompatibel. Sie können eine bestimmte App auf dem Bildschirm freigeben, wenn Sie die App oder den Desktop aus einer Bereitstellungsgruppe mit aktiviertem App-Schutz gestartet haben.

Wenn Sie in der Microsoft Teams-Benutzeroberfläche auf **Inhalt freigeben** klicken, entfernt die Bildschirmauswahl die Option **Desktop**. Sie können nur die Option **Fenster** auswählen, um eine geöffnete App zu teilen.

> **Hinweis:**
>
> Wenn Sie Apps oder Desktops aus einer Bereitstellungsgruppe mit aktiviertem App-Schutz

> starten, können Sie das eingehende Video bzw. den freigegebenen Bildschirm nicht sehen.

**Übergeben und Anfordern der Steuerung in Microsoft Teams** Dieses Feature wird in den folgenden Versionen der Citrix Workspace-App unterstützt (unabhängig von VDA- oder Betriebssystemversion –Multisitzungs-/Einzelsitzungs-OS):

- Citrix Workspace-App für Windows Version 2112.1 und später
- Citrix Workspace-App für Mac Version 2203.1 und später
- Citrix Workspace-App für Linux, Version 2203 und später
- Citrix Workspace-App für ChromeOS Version 2303 und später

Sie können bei einem Microsoft Teams-Anruf die Steuerung anfordern, wenn ein Teilnehmer den Bildschirm freigibt. Wenn Sie die Steuerung übernommen haben, können Sie auf dem freigegebenen Bildschirm Tastatur- und Mausaktivitäten wie Auswahl, Änderungen usw. vornehmen.

Zum Übernehmen der Steuerung bei Freigabe eines Bildschirms klicken Sie in Microsoft Teams auf **Steuerung anfordern**. Der Teilnehmer des Meetings, der den Bildschirm freigibt, kann die Anforderung akzeptieren oder ablehnen.

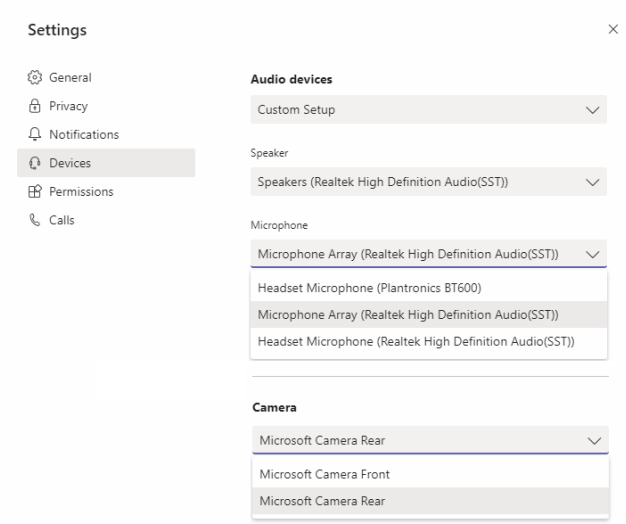
Wenn Sie die Steuerung übernommen haben, können Sie Elemente auf dem freigegebenen Bildschirm auswählen, bearbeiten und andere Änderungen vornehmen. Für diese Aktionen können Sie sowohl die Tastatur als auch die Maus verwenden. Wenn Sie fertig sind, klicken Sie auf **Steuerung anfordern**.

> **Einschränkungen:**
>
> - Übergeben- und Anfordern der Steuerung sind nicht möglich, wenn der Benutzer eine einzelne App teilt (“App-Freigabe”). Der gesamte Desktop oder Bildschirm muss freigegeben werden.
> - Das Feature zum Anheften der Steuerleiste an eine bestimmte Position ist nicht verfügbar.

### Peripheriegeräte in Microsoft Teams

Wenn die Optimierung für Microsoft Teams aktiv ist, greift die Citrix Workspace-App auf die Peripheriegeräte (Headsets, Mikrofone, Kameras, Lautsprecher usw.) zu. Anschließend werden die Peripheriegeräte ordnungsgemäß in der Benutzeroberfläche von Microsoft Teams (**Einstellungen > Geräte**) aufgelistet.




Microsoft Teams greift nicht direkt auf die Geräte zu. Stattdessen verwendet es die WebRTC Media Engine der Workspace-App, um die Medien zu erfassen, aufzuzeichnen und zu verarbeiten. Microsoft Teams listet die Geräte auf, die der Benutzer auswählen kann.

Peripheriegeräte, die angeschlossen werden, während Microsoft Teams aktiv ist, sind standardmäßig nicht ausgewählt. Sie müssen die Peripheriegeräte manuell im Bildschirm **Einstellungen** > **Geräte** der Microsoft Teams-Benutzeroberfläche auswählen. Nachdem das Peripheriegerät ausgewählt ist, speichert Microsoft Teams die Informationen der Peripheriegeräte im Cache. Die Peripheriegeräte werden daher automatisch ausgewählt, wenn Sie sich vom selben Endpunkt aus erneut mit der Sitzung verbinden.

**Empfehlungen:**

- Microsoft Teams-zertifizierte Headsets mit integrierter Echounterdrückung. Bei Konfigurationen mit weiteren Peripheriegeräten, bei denen sich Mikrofon und Lautsprecher in separaten Geräten befinden, kann es zu einem Echo kommen. Dies können zum Beispiel eine Webcam mit integriertem Mikrofon und ein Bildschirm mit Lautsprechern sein. Wenn Sie externe Lautsprecher verwenden, platzieren Sie diese so weit wie möglich weg vom Mikrofon. Stellen Sie sie außerdem nicht in der Nähe von Oberflächen auf, die den Ton in Richtung Mikrofon lenken könnten.
- Microsoft Teams-zertifizierte Kameras, obwohl für Skype for Business zertifizierte Peripheriegeräte mit Microsoft Teams kompatibel sind.
- Eine Entlastung des Hauptprozessors durch Onboard-H.264-Codierung der Webcams (UVC 1.1 und 1.5) kann die Media Engine der Citrix Workspace-App nicht nutzen.

> **Hinweis:**
>
> Die Workspace-App 2009.6 für Windows kann jetzt Peripheriegeräte mit Audioformaten mit 24 Bit oder mit Frequenzen über 96 kHz abrufen.

> HdxTeams.exe (in der Citrix Workspace-App für Windows 2009 oder früher) unterstützt nur diese spezifischen Audiogeräteformate (Kanäle, Bit-Tiefe und Abtastrate):
>
> - Wiedergabegeräte: bis zu 2 Kanäle, 16 Bit, Frequenzen bis 96000 Hz
> - Aufnahmegeräte: bis zu 4 Kanäle, 16 Bit, Frequenzen bis 96000 Hz
>
> Wenn ein Lautsprecher oder Mikrofon nicht mit den erwarteten Einstellungen übereinstimmt, schlägt die Geräteaufzählung in Microsoft Teams fehl und unter **Einstellungen > Geräte** wird **Keine** angezeigt.
>
> **Webrpc**-Protokolle in **HdxTeams.exe** enthalten folgende Art von Informationen:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing ...
> ```
>
> ```
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!
> ```
>
> Deaktivieren Sie als Workaround das Gerät oder:
>
> 1. Öffnen Sie das **Audiosteuerungsfeld** (mmsys.cpl).
> 2. Wählen Sie das Wiedergabe- oder Aufnahmegerät aus.
> 3. Gehen Sie zu **Eigenschaften > Erweitert** und ändern Sie die Einstellungen in einen unterstützten Modus.

#### Fallbackmodus

Wenn Microsoft Teams nicht im optimierten VDI-Modus geladen werden kann (“Citrix HDX Not Connected”in Teams/Info/Version), fällt der VDA ältere HDX-Technologien zurück. Zu älteren HDX-Technologien gehören Webcamumleitung und Clientaudio- sowie Mikrofonumleitung. Wenn Ihre Workspace-App- oder Plattform-OS-Version die Microsoft Teams-Optimierung nicht unterstützt, werden Fallback-Registrierungsschlüssel nicht angewendet.
Im Fallbackmodus werden die Peripheriegeräte dem VDA zugeordnet. Die Peripheriegeräte werden in der Microsoft Teams-App so angezeigt, als wären sie lokal an den virtuellen Desktop angeschlossen.

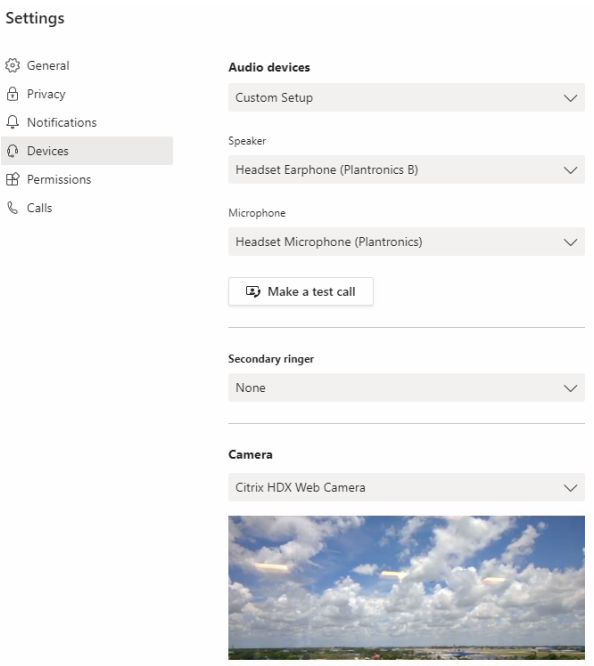
Sie können jetzt den Fallbackmechanismus präzise steuern, indem Sie die Registrierungsschlüssel im VDA festlegen. Weitere Informationen finden Sie unter Fallbackmodus für Microsoft Teams in der Liste der über die Registrierung verwalteten Features.

Für dieses Feature ist die Microsoft Teams-Version 1.3.0.13565 oder höher erforderlich.

Um festzustellen, ob Sie im optimierten oder nicht optimierten Modus sind, ist der größte Unterschied der Kameraname in der Microsoft Teams-App auf der Registerkarte **Einstellungen > Geräte**. Wenn Microsoft Teams im nicht optimierten Modus geladen werden, starten ältere HDX-Technologien. Der Webcam-Name hat das Suffix **Citrix HDX**, wie in der folgenden Grafik dargestellt. Die Lautsprecher-

und Mikrofongerätenamen können sich geringfügig vom optimierten Modus unterscheiden (oder gekürzt angezeigt werden).




Wenn ältere HDX-Technologien verwendet werden, werden die Audio-, Video- und Bildschirmfreigabeverarbeitung von Microsoft Teams nicht auf die WebRTC Media Engine der Citrix Workspace-App des Endpunkts übertragen. Stattdessen verwenden HDX-Technologien serverseitiges Rendering. Erwarten Sie einen hohen CPU-Verbrauch auf dem VDA, wenn Sie Video einschalten. Die Echtzeitaudioleistung ist möglicherweise nicht optimal.

## Bekannte Einschränkungen

### Citrix Einschränkungen

Einschränkungen bei der Citrix Workspace-App:

- HID-Schaltflächen - “Antworten”und “Anruf beenden”werden nicht unterstützt. Der Lautstärkeregler (lauter/leiser) wird unterstützt.
- QoS-Einstellungen im Microsoft Teams Admin Center gelten nicht für VDI-Benutzer.
- App-Schutz-Add-On für die Citrix Workspace-App verhindert ausgehende Bildschirmfreigabe und blockiert die eingehende Bildschirmfreigabe und Videos.
- Benutzer können keine Screenshots von Microsoft Teams-Inhalten machen, wenn sie ein Snipping-Tool auf dem VDA verwenden. Wenn clientseitig jedoch ein Snipping-Tool verwendet wird, können die Inhalte aufgenommen werden.

Beschränkung auf dem VDA:

- Wenn Sie die High DPI-Einstellung der Citrix Workspace-App auf **Ja**konfigurieren, wird das umgeleitete Videofenster fehl am Platz angezeigt. Diese Einschränkung tritt auf, wenn der DPI-Skalierungsfaktor des Monitors auf einen Wert über 100 % festgelegt ist

Einschränkungen bei Citrix Workspace-App und VDA:

- Sie können die Lautstärke bei optimierten Anrufen nur über die Lautstärkeleiste auf dem Client steuern, nicht über die auf dem VDA.

### Simulcast

Die Simulcast-Unterstützung ist für optimierte Microsoft Teams-Videokonferenzen unter Windows und Mac aktiviert. Im Fall von Linux wenden Sie sich an Ihren Thin Client-Anbieter.
Mit Simulcast werden die Qualität und das Erlebnis bei Videokonferenzen an verschiedenen Endpunkten verbessert, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

Dank dieser verbesserten Benutzererfahrung kann jeder Benutzer abhängig von der Endpunktfähigkeit, den Netzwerkbedingungen usw. mehrere Videostreams in unterschiedlichen Auflösungen (z. B. 720p, 360p usw.) senden. Der empfangende Endpunkt fordert dann die maximale Auflösung an, die er verarbeiten kann, sodass alle Benutzer das optimale Videoerlebnis erhalten.

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines Microsoft Teams-Updates verfügbar. Informationen zum voraussichtlichen Releasedatum finden Sie durch Suchen nach "Microsoft 365 roadmap"auf https://www.microsoft.com/. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

### Microsoft-Einschränkungen

- Eine 3x3-Galerieansicht wird nicht unterstützt. Microsoft Teams-Abhängigkeit –wenden Sie sich an Microsoft, wann ein 3x3-Raster erwartet wird
- Die Interoperabilität mit Skype for Business beschränkt sich auf Audioanrufe (kein Videomodus).
- Die maximale Auflösung für eingehende und ausgehende Videostreams beträgt 720 p. Microsoft Teams-Abhängigkeit –wenden Sie sich an Microsoft, wann 1080p erwartet wird
- PSTN-Freizeichen wird nicht unterstützt.
- Medienumgehung für Direct Routing wird nicht unterstützt.
- Die Rollen "producer"und "presenter"für Live-Ereignisse werden nicht unterstützt. Die Teilnehmerrolle wird unterstützt, aber nicht optimiert (das Rendering erfolgt stattdessen auf dem VDA).

- Die Zoomfunktion in Microsoft Teams wird nicht unterstützt.
- Standortbasiertes Routing und Medienumgehung werden nicht unterstützt.
- Das Zusammenführen von Aufrufen wird nicht unterstützt (Option wird nicht in der Benutzeroberfläche angezeigt).

#### Citrix und Microsoft-Einschränkungen

- Bei der Bildschirmfreigabe ist die Option **Systemaudio einschließen** nicht verfügbar.
- Simulcast wird unter ChromeOS nicht unterstützt.

### Angekündigtes EOL für Einzelfenster in Microsoft Teams

Microsoft unterstützt ab 31.01.2024 nur noch den Mehrfenstermodus bei Verwendung von optimiertem Microsoft Teams für VDI. Die Unterstützung der Einzelfenster-Benutzeroberfläche wird eingestellt. Dies wurde am 08.09.2023 im M365s Admin Center (Post-ID: MC674419) von Microsoft bekannt gegeben.
Informationen zum Mehrfensterfeature sind in diesem Tech Community-Artikel veröffentlicht: New Meeting and Calling Experience in Microsoft Teams.

Sie müssen Ihren VDA und die Citrix Workspace-App auf die unterstützten Versionen aktualisieren, um Microsoft Teams weiterhin im optimierten Modus für Videoanrufe und die Bildschirmfreigabe zu verwenden. Wenn Sie Ihre Infrastruktur und Endpunkte nicht so aufrüsten, dass sie mehrere Fenster unterstützen, können Sie nur Audioanrufe einrichten. Sie können die optimierte Video- und Bildschirmfreigabefunktion dann nicht verwenden.

Die folgende Tabelle enthält die erforderliche Mindest-, LTSR- und empfohlene Version von VDA und Citrix Workspace-App, um weiterhin optimierte Anrufe in Microsoft Teams auf Citrix VDI zu verwenden:

| Komponente | Mindestversion | Version für LTSR | Empfohlene Version |
|---|---|---|---|
| Microsoft Teams | 1.5.00.11865 | Nicht zutreffend | Aktuell |
| VDA | 1912 CU6 LTSR, 2203 LTSR, 2112 CR | 1912 CU7+, 2203 CU2+ | 2308 CR+ |
| Citrix Workspace-App für Windows | 2205 CR | 2203 CU2+ | 2309 CR+ |
| Citrix Workspace-App für Mac | 2209 CR | Nicht zutreffend | 2308 CR+ |
| Citrix Workspace-App für Linux | 2209 CR | Nicht zutreffend | 2308 CR+ |

| Komponente | Mindestversion | Version für LTSR | Empfohlene Version |
|---|---|---|---|
| Citrix Workspace-App für ChromeOS oder HTML5 | 2303 CR | Nicht zutreffend | 2309 CR+ |

## Angekündigte Einstellung des SDP-Formats (Plan B) von WebRTC

Das aktuelle SDP-Format (Plan B) von WebRTC wird in zukünftigen Versionen nicht mehr von Citrix unterstützt. Sie müssen Unified Plan in WebRTC verwenden, um optimierte Microsoft Teams-Funktionen zu unterstützen.

### Betroffene Produkte

In einem zukünftigen Release der Citrix Workspace-App werden Anrufe zwischen Endpunkten mit dem kommenden Release der Citrix Workspace-App und Endpunkten mit der Citrix Workspace-App bis Version 2108 nicht unterstützt. Diese Anrufinkompatibilität umfasst Clients mit der Citrix Workspace-App (CWA) 1912 LTSR. Die folgenden CWA-Clients sind betroffen:

- Citrix Workspace-App für Windows
- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac
- Citrix Workspace-App für Chrome

### Ersatz für Plan B

Bei Verwendung der Citrix Workspace-App vor Version 2109 müssen Sie ein Upgrade auf eine unterstützte Version durchführen (vorzugsweise das neueste CR-Release). Andernfalls können alle Anrufe mit einem zukünftigen Release oder neueren Endpunkten fehlschlagen. Anrufe zwischen zukünftigen Releases und Ihren Verbundkommunikationspartnern können ebenfalls fehlschlagen, wenn der Citrix Workspace Ihrer Verbundpartner nicht aktualisiert wurde.

Version 2108 der Citrix Workspace-App wird seit März 2023 nicht mehr unterstützt und muss auf eine neuere Version aktualisiert werden. Weitere Informationen zu unterstützten Versionen der Citrix Workspace-App finden Sie unter Workspace-App.

Weitere Informationen zur eingestellten Unterstützung für Plan B finden Sie in der Dokumentation zu WebRTC.

### Weitere Informationen

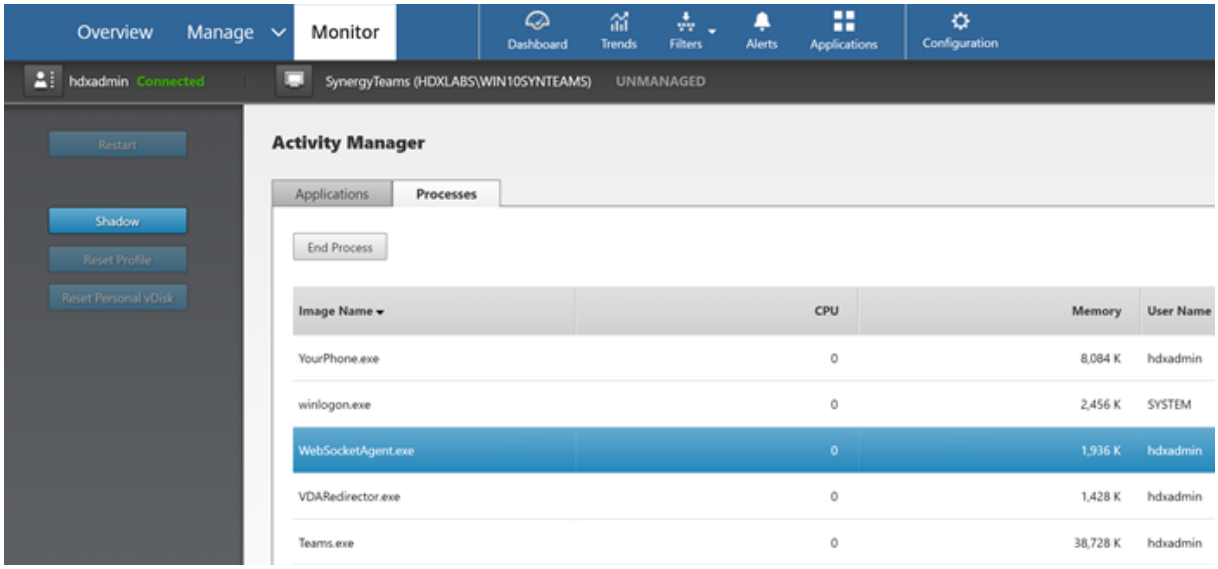
- Microsoft Teams überwachen sowie Problembehandlung und Support
- Bereitstellen der Microsoft Teams-Desktopanwendung auf der VM
- Installieren von Microsoft Teams mit MSI (Abschnitt VDI-Installation)
- Thin Clients
- Skype for Business Network Assessment Tool
- Hinweise zur Koexistenz und Interoperabilität von Microsoft Teams und Skype for Business

## Microsoft Teams überwachen sowie Problembehandlung und Support

April 18, 2024

### Teams überwachen

Dieser Abschnitt enthält Richtlinien zum Überwachen der Microsoft Teams-Optimierung mit HDX. Wenn Sie den optimierten Modus verwenden und auf dem Clientcomputer `HdxRtcEngine.exe` ausgeführt wird, wird in der Sitzung der VDA-Prozess `WebSocketAgent.exe` ausgeführt. Verwenden Sie den **Aktivitätsmanager** in Director, um die Anwendung anzuzeigen.




Mit dem VDA (Mindestversion 1912) können Sie in Teams aktive Anrufe mit Citrix HDX Monitor (Mindestversion 3.11) überwachen. Das ISO-Image von Citrix Virtual Apps and Desktops enthält die neueste Version von `hdxmonitor.msi` im Ordner `layout\image-full\Support\HDX Monitor`.

Weitere Informationen finden Sie im Knowledge Center-Artikel CTX253754 unter *Monitoring*.

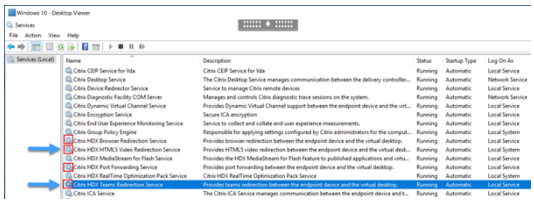
 

## Problembehandlung

Dieser Abschnitt enthält Tipps zur Behandlung von Problemen, die bei der Verwendung der Optimierung für Microsoft Teams auftreten können. Weitere Informationen finden Sie unter CTX253754.

### Virtual Delivery Agent

Von BCR_x64.msi werden vier Dienste installiert. Nur zwei sind für die Microsoft Teams- Umleitung auf dem VDA verantwortlich.



- **Citrix HDX Teams Redirection Service** richtet den virtuellen Kanal ein, der in Microsoft Teams verwendet wird. Der Dienst basiert auf CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** wird als WebSocketService.exe ausgeführt und überwacht 127.0.0.1:9002 TCP. WebSocketService.exe führt zwei Hauptfunktionen aus:

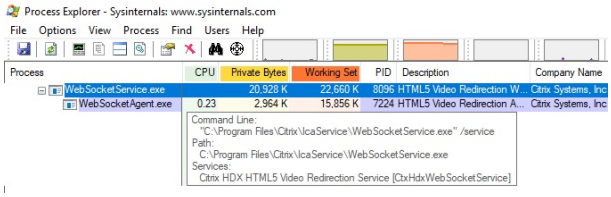
  i. **TLS termination for secure WebSockets** empfängt eine sichere WebSocket-Verbindung von vdiCitrixPeerConnection.js, einer Komponente in der Microsoft Teams-App. Sie können sie mit der Prozessüberwachung verfolgen. Weitere Informationen zu Zertifikaten finden Sie im Abschnitt "TLS- und HTML5-Videoumleitung und Browserinhaltsumleitung"unter Kommunikation zwischen Controller und VDA.

  Einige Antiviren- und Desktop-Sicherheitsprogramme beeinträchtigen die Funktion von `WebSocketService.exe` und zugehörigen Zertifikaten. Während der Citrix HDX HTML5-Videoumleitungsdienst in der Konsole von `services.msc` möglicherweise ausgeführt wird, ist der Localhost-TCP-Socket `127.0.0.1:9002` nie im Listener-Modus, wie in netstat zu sehen ist. Beim versuchten Neustart des Diensts hört er auf zu reagieren ("Stopping …"). Stellen Sie sicher, dass Sie die richtigen Ausschlussbedingungen für den Prozess `WebSocketService.exe` verwenden.

  ii. **Benutzersitzungszuordnung.** Beim Start von Microsoft Teams startet WebSocketService.exe den Prozess WebSocketAgent.exe in der Benutzersitzung auf dem VDA. WebSocketService.exe wird in Sitzung 0 als LocalSystem-Konto ausgeführt.




Sie können mit **netstat** überprüfen, ob der WebSocketService.exe-Dienst auf dem VDA aktiv überwacht.

Führen Sie mit erhöhten Rechten an der Eingabeaufforderung `netstat -anob -p tcp` aus:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

Bei einer erfolgreichen Verbindung ändert sich der Status in ESTABLISHED:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> **Wichtig:**
>
> WebSocketService.exe überwacht die beiden TCP-Sockets 127.0.0.1:9001 und 127.0.0.1:9002. Port 9001 wird für die Browserinhaltsumleitung und die HTML5-Videoumleitung verwendet. Port 9002 wird für die Microsoft Teams-Umleitung verwendet. Stellen Sie sicher, dass das Windows-Betriebssystem des VDAs keine Proxykonfigurationen enthält, die eine direkte Kommunikation zwischen Teams.exe und WebSocketService.exe verhindern. Wenn Sie einen expliziten Proxy in Internet Explorer 11 konfigurieren (**Internetoptionen > Verbindungen > LAN-Einstellungen > Proxyserver**), können Verbindungen eventuell über einen zugewiesenen Proxyserver laufen. Stellen Sie sicher, dass **Proxyserver für lokale Adressen umgehen** aktiviert ist, wenn Sie eine manuelle und explizite Proxyeinstellung verwenden.

### Speicherorte und Beschreibung der Dienste

| Service | Pfad zu Programmdatei in Windows Server-Betriebssystem | Anmelden als | Beschreibung |
|---|---|---|---|
| Citrix HTML5-Videoumleitungsdienst | "C:\Programme (x86)\Citrix\System32\WebSocketService.exe" /service | Lokales Systemkonto | Bietet mehrere HDX Multimedia-Dienste mit dem Framework, das für die Durchführung der Medienumleitung zwischen dem virtuellen Desktop und dem Endgerät erforderlich ist. |
| Citrix HDX-Browserumleitungsdienst | "C:\Programme (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs | Dieses Konto (lokaler Dienst) | Ermöglicht die Browserinhaltsum-leitung zwischen dem Endpunktgerät und dem virtuellen Desktop. |
| Citrix Portweiter-leitungsdienst | "C:\Programme (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs | Dieses Konto (lokaler Dienst) | Ermöglicht die Portweiterleitung zwischen dem Endpunktgerät und dem virtuellen Desktop für die Browserinhaltsum-leitung. |
| Citrix HDX-Teams-Umleitungsdienst | "C:\Programme (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs | Lokales Systemkonto | Ermöglicht die Microsoft Teams-Umleitung zwischen dem Endpunktgerät und dem virtuellen Desktop. |

#### Citrix Workspace-App

Auf dem Endpunkt des Benutzers instanziiert die Citrix Workspace-App für Windows einen neuen Dienst namens HdxTeams.exe. Dies geschieht, wenn Microsoft Teams auf dem VDA gestartet wird und der Benutzer versucht, in der Eigenvorschau einen Anruf zu tätigen oder auf die Peripheriegeräte zuzugreifen. Wenn dieser Dienst nicht angezeigt wird, überprüfen Sie Folgendes:

1. Die Workspace-App Version 1905 für Windows wurde installiert. Enthält der Installationspfad der Workspace-App HDXTeams.exe und die webrpc.dll-Binärdateien?
2. Wenn Sie Schritt 1 überprüft haben, gehen Sie folgendermaßen vor, um zu prüfen, ob HDXTeams.exe gestartet wird.

    a) Beenden Sie Microsoft Teams auf dem VDA.
    b) Starten Sie services.msc auf dem VDA.
    c) Beenden Sie den Citrix HDX-Teams-Umleitungsdienst.
    d) Trennen Sie die ICA-Sitzung.
    e) Verbinden Sie die ICA-Sitzung.
    f) Starten Sie den Citrix HDX-Teams-Umleitungsdienst.
    g) Starten Sie den Citrix HDX HTML5-Videoumleitungsdienst neu.
    h) Starten Sie Microsoft Teams auf dem VDA.

3. Wird HDXTeams.exe auf dem Clientendpunkt immer noch nicht gestartet, gehen Sie wie folgt vor:

    a) Starten Sie den VDA neu.
    b) Starten Sie den Clientendpunkt neu.

### Support

Citrix und Microsoft unterstützen gemeinsam die Bereitstellung von Microsoft Teams über Citrix Virtual Apps and Desktops mithilfe der Optimierung für Microsoft Teams. Diese gemeinsame Unterstützung ist das Ergebnis einer engen Zusammenarbeit zwischen den beiden Unternehmen. Wenn Sie gültige Supportverträge haben und ein Problem mit dieser Lösung auftritt, öffnen Sie ein Supportticket bei dem Anbieter, in dessen Code Sie die Ursache des Problems vermuten. Das heißt, Microsoft für Teams und Citrix für die Optimierungskomponenten.

Citrix oder Microsoft erhält das Ticket, prüft das Problem und eskaliert gegebenenfalls. Sie müssen sich nicht an das Supportteam beider Unternehmen wenden.

Bei Problemen empfehlen wir, in der Teams-Benutzeroberfläche auf **Hilfe > Problem melden** zu klicken. VDA-seitige Protokolle werden automatisch zwischen Citrix und Microsoft geteilt, um technische Probleme schneller zu beheben.

### Sammeln von Protokollen

Die HDX Media Engine-Protokolle sind auf der Benutzermaschine (nicht auf dem VDA). Bei Problemen fügen Sie die Protokolle Ihrem Supportfall bei.

**Windows-Protokolle:**

Windows-Protokolle finden Sie auf der Benutzermaschine unter %TEMP% im Ordner **HDXTeams** (AppData/Local/Temp/HDXTeams oder AppData/Local/Temp/HdxRtcEngine). Suchen Sie die TXT-Datei webrpc_Day_Month_timestamp_Year.txt. Wenn Sie eine neuere Citrix Workspace-App-Version verwenden, z. B. Citrix Workspace-App 2009.5, speichern Sie die Protokolle in AppData\Local\Temp\HdxRtcEngine.

Für jede Sitzung wird ein eigener Protokollordner erstellt.

**Mac-Protokolle:**

1. VDWEBRTC-Protokoll - zeichnet die Ausführung des virtuellen Kanals auf.

   Speicherort /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine log - zeichnet die Ausführung der Prozesse auf HdxRtcEngine auf.

   Ort: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine-Protokollierung ist standardmäßig aktiviert.

3. Webrpc-Protokolle - die wichtigsten Protokolle, die die Ausführung des Wrapups der webrtc-Bibliothek aufzeichnen.

   Ort: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

**Linux-Protokolle:**

Die Linux-Protokolle sind in den Ordnern /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Webrtc-Protokoll: /tmp/webrpc/<current date>/webrtc.log
Kernel-Protokoll: /var/log/syslog

**ICE/STUN/TURN/-Protokolle:**

Beim Einrichten eines Anrufs sind folgende vier ICE-Phasen erforderlich:

- Sammeln der Kandidaten
- Austausch der Kandidaten
- Konnektivitätsprüfungen (STUN-Bind-Anforderungen)
- Einstufung der Kandidaten

In den Protokollen für HdxRtcEngine.exe sind die folgenden Einträge für ICE (Interactive Connectivity Establishment) relevant. Diese Einträge müssen vorhanden sein, damit ein Anruf erfolgreich eingerichtet wurde. Sehen Sie sich folgenden Beispielausschnitt für die Sammelphase an:

```
RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424
    #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering

[...]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[...]
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer

<!--NeedCopy-->
```

Wenn mehrere ICE-Kandidaten vorhanden sind, lautet die Reihenfolge der Präferenz:

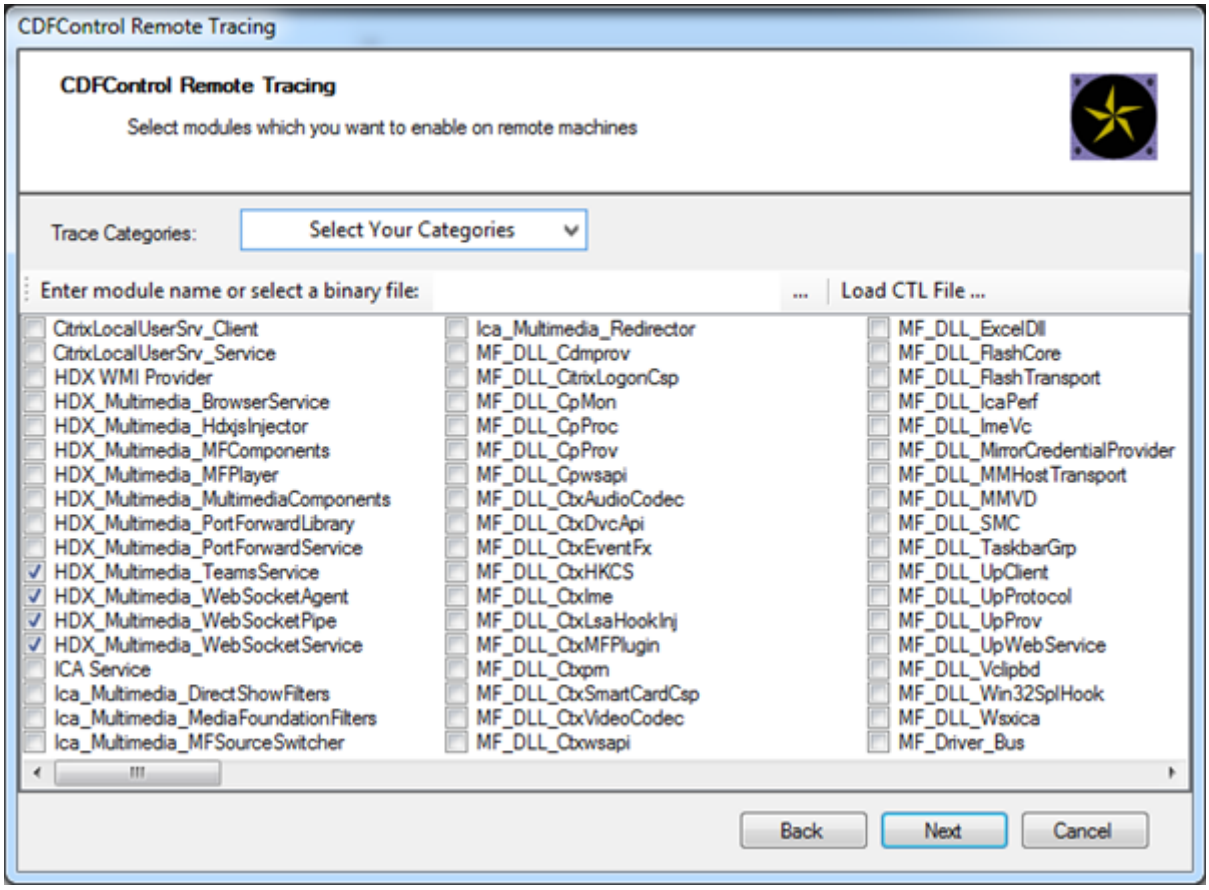
 

1. Host
2. Peer reflexiv
3. Server reflexiv
4. Transport-Relay

Wenn ein Problem auftritt und Sie es reproduzieren können, empfehlen wir, in Teams auf **Hilfe > Problem melden** zu klicken. Protokolle werden zwischen Citrix und Microsoft geteilt, um technische Probleme zu beheben, wenn Sie einen Supportfall bei Microsoft öffnen.
Das Aufzeichnen von CDF-Traces vor der Kontaktaufnahme mit dem Citrix Support ist ebenfalls von Vorteil. Weitere Informationen finden Sie im Knowledge Center-Artikel CDFcontrol.

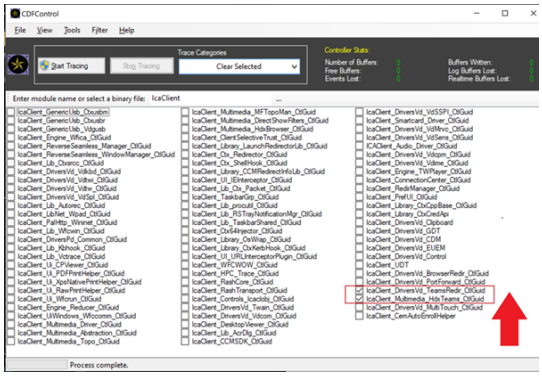
Empfehlungen zur Erzeugung von CDF-Tracingberichten finden Sie im Knowledge Center-Artikel Recommendations for Collecting the CDF Traces.

**VDA-seitige CDF-Tracingberichte –aktivieren Sie die folgenden CDF-Trace-Anbieter:**




**Workspace-App-seitige CDF-Tracingberichte –aktivieren Sie die folgenden CDF-Trace-Anbieter:**



- IcaClient_DriversVd_TeamsRedir (optional)
- IcaClient_Multimedia_HdxTeams (erfordert die Citrix Workspace-App 2012 oder höher)

## Windows Media-Umleitung

April 1, 2022

Die Windows Media-Umleitung steuert und optimiert die Art und Weise, mit der Streamingaudio und -video von Servern bereitgestellt wird. Durch Wiedergabe der Laufzeitdateien von Medieninhalten auf dem Client statt auf dem Server werden die Bandbreitenanforderungen beim Abspielen von Multimediadateien verringert. Windows Media-Umleitung verbessert die Leistung von Windows Media Player und anderen kompatiblen Playern, die auf virtuellen Windows-Desktops ausgeführt werden.

Wenn die Anforderungen des clientseitigen Windows Media-Inhaltsabrufs nicht erfüllt sind, erfolgt automatisch der serverseitige Inhaltsabruf. Diese Methode ist für die Benutzer unsichtbar. Sie können mit Citrix Scout einen CDF-Trace (Citrix Diagnostics Facility) von HostMMTransport.dll durchführen, um zu ermitteln, welche Methode verwendet wird. Weitere Informationen finden Sie unter Citrix Scout.

Die Windows Media-Umleitung fängt die Medienpipeline auf dem Hostserver ab, erfasst Mediendaten im ursprünglichen, komprimierten Format und leitet den Inhalt an das Clientgerät um. Auf dem Clientgerät wird die Medienpipeline zum Dekomprimieren und Wiedergeben der vom Hostserver empfangenen Mediendaten neu erstellt. Die Windows Media-Umleitung funktioniert gut auf Clientgeräten mit Windows-Betriebssystem. Solche Geräte besitzen das erforderliche Multimedia-Framework zum Neuaufbau der Medienpipeline in der Form, wie diese auf dem Hostserver vorhanden war. Linux-Clients verwenden ähnliche Open-Source-Frameworks für den Neuaufbau der Medienpipeline.

Die Richtlinieneinstellung **Windows Media-Umleitung** steuert dieses Feature und ist standardmäßig auf **Zugelassen** festgelegt. Normalerweise erhöht diese Einstellung die Audio- und Videoqualität von vom Server stammenden Medien auf ein mit einer lokalen Wiedergabe vergleichbares Niveau. In Ausnahmefällen kann die Wiedergabe von Medien mit der Windows Media-Umleitung schlechter

scheinen, als bei Verwendung der ICA-Komprimierung und von regulärem Audio. Sie können das Feature deaktivieren, indem Sie einer Richtlinie die Einstellung **Windows Media-Umleitung** hinzufügen und den Wert auf **Nicht zugelassen** festlegen.

Weitere Informationen zu den Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "Multimedia".

**Einschränkung:**

Wenn Sie Windows Media Player mit aktivierten Remote-Audio und Video Erweiterungen (RAVE) in einer Sitzung verwenden wird ggf. ein schwarzer Bildschirm angezeigt. Der schwarze Bildschirm kann angezeigt werden, wenn Sie mit der rechten Maustaste auf den Videoinhalt klicken und **Aktuelle Wiedergabe immer oben anzeigen** wählen.

## Allgemeine Inhaltsumleitung

April 19, 2022

Bei der Inhaltsumleitung können Sie steuern, wie die Benutzer auf die Informationen zugreifen: über die auf den Servern veröffentlichten Anwendungen oder über lokal auf den Benutzergeräten ausgeführte Anwendungen.

### Clientordnerumleitung

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung.

- Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet.
- Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Windows-Desktopgerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

### Host-zu-Client-Umleitung

Ziehen Sie die Host-zu-Client-Umleitung für bestimmte ungewöhnliche Anwendungsfälle in Betracht. In der Regel sind andere Formen der Inhaltsumleitung besser. Diese Umleitungsart wird nur auf VDAs für Multisitzungs-OS und nicht auf VDAs für Einzelsitzungs-OS unterstützt.

### Lokaler App-Zugriff und URL-Umleitung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert. Es ist kein Wechsel zwischen Desktops erforderlich.

HDX-Technologie bietet **generische USB-Umleitung** für Spezialgeräte ohne optimierte Unterstützung oder wenn diese ungeeignet ist.

## Clientordnerumleitung

April 1, 2022

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner werden als UNC-Links in Sitzungen angezeigt. Es ist nicht das komplette Dateisystem auf dem Benutzergerät abgebildet. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt.

Die Clientordnerumleitung wird nur auf Maschinen mit Windows-Einzelsitzungs-OS unterstützt.

Die Clientordnerumleitung für ein externes USB-Laufwerk wird beim Trennen und Wiederverbinden des Geräts nicht gespeichert.

Aktivieren Sie die Clientordnerumleitung auf dem Server. Geben Sie dann auf dem Clientgerät an, welche Ordner umgeleitet werden sollen. Die Anwendung, die Sie zur Angabe der Clientordneroptionen verwenden, ist in diesem Release der Citrix Workspace-App enthalten.

**Anforderungen:**

Server:

- Windows Server 2019, Standard und Datacenter Edition
- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition

Clients:

- Windows 10, 32-Bit- und 64-Bit-Editionen (Mindestversion 1607)
- Windows 8.1, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
- Windows 7, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)

Informationen zum Aktivieren der Clientordnerumleitung auf dem Server finden Sie unter Clientordnerumleitung in der Liste der über die Registrierung verwalteten Features.

Geben Sie auf dem Benutzergerät an, welche Ordner umgeleitet werden sollen.

1. Stellen Sie sicher, dass die neueste Version der Citrix Workspace-App installiert ist.
2. Starten Sie vom Installationsverzeichnis der Citrix Workspace-App aus CtxCFRUI.exe.
3. Wählen Sie das Optionsfeld **Benutzerdefiniert** und fügen Sie Ordner hinzu oder bearbeiten oder entfernen Sie Ordner.
4. Trennen Sie die Sitzungen und stellen Sie dann neue Verbindungen her, damit die Einstellung wirksam wird.

## Bidirektionale Inhaltsumleitung konfigurieren

February 14, 2024

Mit der bidirektionalen Inhaltsumleitung können URLs je nach Konfiguration von Client zu Server oder von Server zu Client umgeleitet werden. Diese Richtlinieneinstellung ersetzt die folgenden drei Einstellungen, die veraltet sind:

- Bidirektionale Inhaltsumleitung zulassen
- Für Umleitung an VDA zulässige URLs
- Für Umleitung an Client zulässige URLs

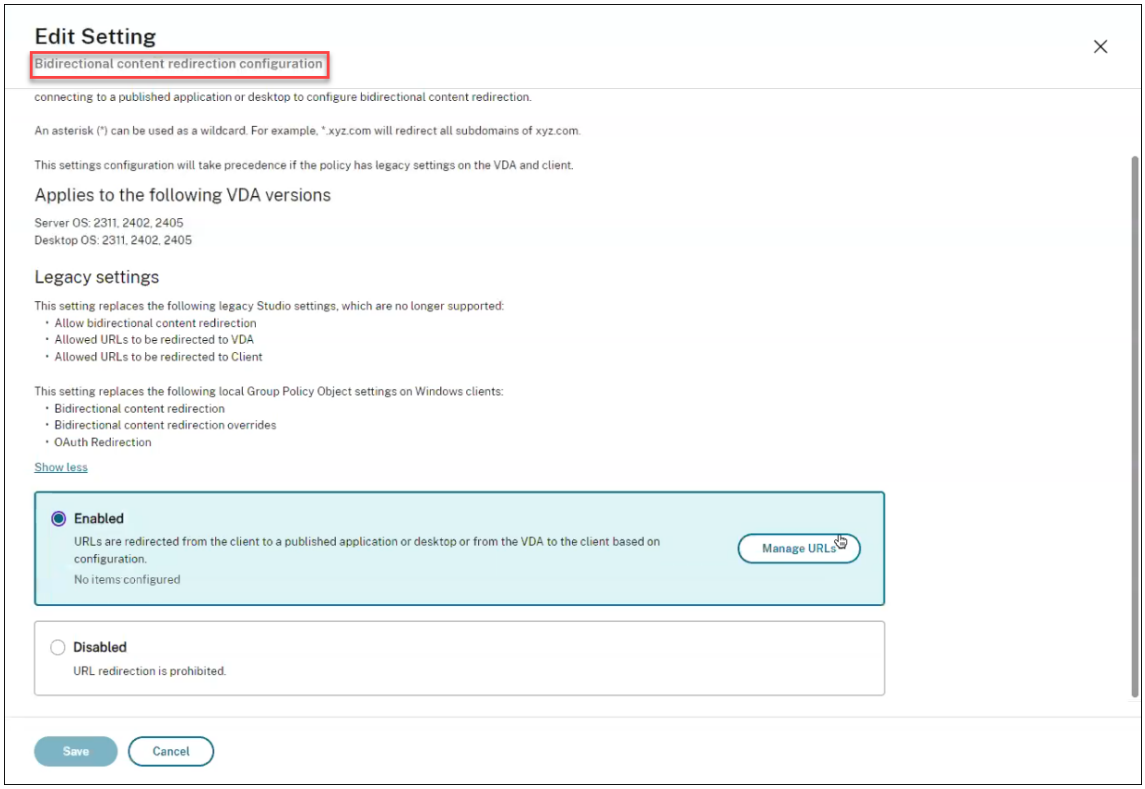
Es ersetzt auch die folgenden drei lokalen GPO-Einstellungen auf Windows-Clients:

- Bidirektionale Inhaltsumleitung
- Außerkraftsetzungen der bidirektionalen Inhaltsumleitung
- OAuth-Umleitung

Wenn diese Einstellung konfiguriert ist, hat sie Vorrang vor den Legacy-Einstellungen in Studio und auf dem Client. Gehen Sie wie folgt vor, um die Richtlinie für die bidirektionale Inhaltsumleitung zu konfigurieren:

1. Klicken Sie auf der Konfigurationsseite für Citrix DaaS auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Registerkarte **Richtlinien**.
3. Klicken Sie auf **Richtlinie erstellen**. Das Blatt **Richtlinie erstellen** wird geöffnet.
4. Suchen Sie im **Suchfeld** nach `Bidirectional content redirection configuration`, aktivieren Sie das Kontrollkästchen und klicken Sie auf **Bearbeiten**.
5. Stellen Sie diese Richtlinie auf der Seite **Einstellungen bearbeiten** auf **Aktiviert** ein und klicken Sie auf **URLs verwalten**.




6. Geben Sie im Blatt **URLs verwalten** für die **VDA-zu-Client-Umleitung** Folgendes an:

   - **URL** (erforderlich): Fügen Sie die URL hinzu, die vom VDA zum Öffnen auf dem Client umgeleitet werden soll. Legen Sie für die OAuth-Umleitung das Authentifizierungsschema und -muster auf dem Client fest, um die Sitzung zurück zum Host umzuleiten.
   - **Muster** (optional): Regulärer URL-Ausdruck, der, wenn er über eine VDA-zu-Client-URL-Umleitung an den Client umgeleitet wird, so verfolgt wird, als ob ein OAuth-Authentifizierungsfluss begonnen hätte. Wenn der Flow abgeschlossen ist (erkannt durch das Öffnen des resultierenden Schemas oder Umleitung-URL-Musters), wird die resultierende URL zurück an den Host-VDA umgeleitet, der diesen Fluss initiiert hat.
   - **Schema** (optional): Wenn ein Schema angegeben ist, wird erwartet, dass die abschließende URL das Format `scheme://<something>` hat. Wenn kein Schema angegeben ist (leer), wird das ursprüngliche resultierende URL-Muster über eine Erfassungsgruppe für reguläre Ausdrücke (muss im Muster angegeben werden) aus dem Muster extrahiert und die ursprüngliche URL wird neu geschrieben, um eine `citrix-oauth-redir://`-Umleitungs-URL zu verwenden. Wenn der Datenfluss abgeschlossen ist, wird die ursprüngliche Umleitungs-URL zurück zum Host (VDA) umgeleitet. In diesem Fall muss jeder OAuth-Autorisierungsserver so konfiguriert sein, dass er `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` Umleitungs-URLs zulässt.

> **Hinweis:**
>
> Obwohl sowohl **Muster** als auch **Schema** optional sind, müssen Sie auch ein **Schema** angeben, wenn **Muster** angegeben ist.

7. Geben Sie im Blatt **URLs verwalten** für die **Client-zu-VDA**-Umleitung Folgendes an:
   - **Typ**: Wählen Sie **Desktop** oder **Anwendung**.
   - **Name**: Geben Sie dem Typ einen Namen.
   - **URL**: Geben Sie die URL an, die Sie zur Quelle umleiten möchten. Sie können mehrere URLs hinzufügen und diejenigen löschen, die nicht benötigt werden
8. Klicken Sie auf **Speichern**. Auf dem Blatt **Einstellung bearbeiten** wird die Anzahl der konfigurierten Elemente angezeigt.
9. Klicken Sie auf **Speichern**. Auf dem Blatt **Richtlinie erstellen** wird der konfigurierte **aktuelle Wert** angezeigt. Klicken Sie auf **Weiter**.
10. Klicken Sie im Schritt **Richtlinie zuweisen zu** auf **Weiter**.
11. Wählen Sie im Schritt **Zusammenfassung** das Kontrollkästchen **Richtlinie aktivieren** aus und geben Sie einen Namen in das Feld **Richtlinienname** ein.
12. Klicken Sie auf **Fertig stellen**. Die neue Richtlinie ist aufgeführt.
13. Wählen Sie die neu erstellte Richtlinie aus, um die konfigurierten Einstellungen zu überprüfen.

Ältere Einstellungen finden Sie unter Host-zu-Client-Umleitung und Bidirektionale Inhaltsumleitung.

## Host-zu-Client-Umleitung

February 14, 2024

> **Hinweis:**
>
> In diesem Artikel werden die älteren Einstellungen für die Host-zu-Client-Inhaltsumleitung beschrieben. Die neuesten Einstellungen finden Sie unter Konfiguration der bidirektionalen Inhaltsumleitung. Die neuen Richtlinieneinstellungen haben Vorrang vor den alten Einstellungen. Citrix empfiehlt, nur die neuen Richtlinieneinstellungen zu verwenden und alle älteren Einstellungen zu löschen, um unerwartetes Verhalten zu vermeiden.

Mit der Host-zu-Client-Umleitung können URLs, die als Hyperlink in einer Citrix Sitzung ausgeführten Anwendungen eingebettet sind, mit der zugehörigen Anwendung auf Benutzergeräten geöffnet werden. Häufige Anwendungsfälle für die Host-zu-Client-Umleitung sind:

- Umleitung von Websites, wenn der Citrix Server keinen Internet- oder Netzwerkzugriff auf die Quelle hat.
- Umleitung von Websites, wenn das Ausführen eines Webbrowsers in Citrix Sitzungen aus Sicherheits-, Leistungs-, Kompatibilitäts- oder Skalierbarkeitsgründen nicht erwünscht ist.
- Umleitung spezifischer URL-Typen für Anwendungen, die nicht auf dem Citrix Server installiert sind.

Die Host-zu-Client-Umleitung ist nicht für URLs vorgesehen, auf die über eine Webseite zugegriffen wird oder die in die Adressleiste des in der Citrix Sitzung ausgeführten Webbrowsers eingegeben werden. Informationen zur URL-Umleitung in Webbrowsern finden Sie unter Bidirektionale URL-Umleitung und Browserinhaltsumleitung.

### Systemanforderungen

- Multisitzungs-OS-VDA
- Unterstützte Clients:
  - Citrix Workspace-App für Windows
  - Citrix Workspace-App für Mac
  - Citrix Workspace-App für Linux
  - Citrix Workspace-App für HTML5
  - Citrix Workspace-App für Chrome

Auf dem Clientgerät muss eine Anwendung zur Verarbeitung der Umleitung der URL-Typen installiert und konfiguriert sein.

### Konfiguration

Verwenden Sie die Citrix Richtlinie Host-zu-Client-Umleitung, um diese Funktionalität zu aktivieren. Die **Host-zu-Client-Umleitung** ist standardmäßig deaktiviert. Nachdem Sie die Richtlinie “Host-zu-Client-Umleitung”aktiviert haben, registriert sich Citrix Launcher beim Windows-Server, damit es URLs abfangen und an das Clientgerät senden kann.

Sie müssen dann die Windows-Gruppenrichtlinie so konfigurieren, dass Citrix Launcher als Standardanwendung für die gewünschten URL-Typen verwendet wird. Erstellen Sie auf dem Citrix Server-VDA die Datei ServerFTAdefaultPolicy.xml und fügen Sie den folgenden XML-Code ein.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />
```

```
6
7  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
8
9  </DefaultAssociations>
10 <!--NeedCopy-->
```

Gehen Sie in der Gruppenrichtlinien-Verwaltungskonsole zu **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Datei-Explorer > Konfigurationsdatei für Standardzuordnungen festlegen** und speichern Sie die Datei ServerFTAdefaultPolicy.xml.

> **Hinweis:**
>
> Wenn ein Citrix Server keine Gruppenrichtlinieneinstellungen hat, werden die Benutzer von Windows aufgefordert, eine Anwendung zum Öffnen von URLs auszuwählen.

Standardmäßig unterstützen wir die Umleitung der folgenden URL-Typen:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Um weitere standardmäßige oder benutzerdefinierte URL-Typen in die Liste für die Umleitung aufzunehmen, erstellen Sie eine neue **Association Identifier**-Zeile in der o. g. Datei ServerFTAdefaultPolicy.xml. Beispiel:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>
```

```
<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

Das Hinzufügen von URL-Typen zur Liste erfordert außerdem eine Clientkonfiguration. Erstellen Sie den folgenden Registrierungsschlüssel mit den folgenden Werten auf dem Windows-Client.

> **Hinweis:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übern-

> immt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Wertname: ExtraURLProtocols
- Werttyp: REG_SZ
- Wertdaten: URL-Typen, durch Semikolon getrennt. Geben Sie alles vor dem authority-Teil der URL ein. Beispiel:
  `ftp://;mailto:;customtype1://;custometype2://`

Sie können URL-Typen nur für Windows-Clients hinzufügen. Clients ohne die obigen Registrierungseinstellungen lehnen die Umleitung zurück an die Citrix Sitzung ab. Auf dem Client muss eine Anwendung installiert und konfiguriert sein, die die angegebenen URL-Typen verarbeiten kann.

Um URL-Typen aus der Standardumleitungsliste zu entfernen, erstellen Sie den folgenden Registrierungsschlüssel mit den folgenden Werten auf dem Server-VDA.

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Wertname: DisableServerFTA
- Werttyp: DWORD
- Wertdaten: 1
- Wertname: NoRedirectClasses
- Werttyp: REG_MULTI_SZ
- Wertdaten: eine beliebige Kombination der Werte –`httphttps`, `rtsp`, `rtspu`, `pnm` oder `mms`. Geben Sie mehrere Werte auf separaten Zeilen an. Beispiel:

```
http
https
rtsp
```

Zum Aktivieren der Host-zu-Client-Umleitung für spezifische Websites erstellen Sie einen Registrierungsschlüssel mit Werten auf dem Server-VDA.

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Wertname: ValidSites
- Werttyp: REG_MULTI_SZ
- Wertdaten: eine beliebige Kombination vollständig qualifizierter Domänennamen (FQDN). Geben Sie mehrere FQDNs auf separaten Zeilen an. Geben Sie nur den FQDN ohne Protokoll

(`http://` oder `https://`) ein. Ein FQDN darf nur an der Stelle ganz links ein Sternchen (*) als Platzhalter enthalten. Der Platzhalter entspricht einer Domänenebene und somit den Vorgaben von RFC 6125. Beispiel:

`www.exmaple.com`

`*.example.com`

> **Hinweis:**
>
> Sie können den Schlüssel **ValidSites** nicht in Kombination mit den Schlüsseln **DisableServerFTA** und **NoRedirectClasses** verwenden.

### Standardbrowserkonfiguration auf dem Server-VDA

Die hier beschriebene Aktivierung der Host-zu-Client-Umleitung ersetzt jede bestehende Standardbrowserkonfiguration auf dem Server-VDA. Wenn eine Web-URL nicht umgeleitet wird, übergibt Citrix Launcher die URL an den im Registrierungsschlüssel `command_backup` konfigurierten Browser. Der Schlüssel verweist standardmäßig auf Internet Explorer, Sie können jedoch den Pfad eines anderen Browsers angeben. Weitere Informationen finden Sie unter Standardbrowserkonfiguration auf dem Server-VDA in der Liste der über die Registrierung verwalteten Features.

## Bidirektionale Inhaltsumleitung

April 18, 2024

> **Hinweis:**
>
> In diesem Artikel werden die älteren Einstellungen für die bidirektionale Inhaltsumleitung beschrieben. Die neuesten Richtlinieneinstellungen finden Sie unter Konfiguration der bidirektionalen Inhaltsumleitung. Die neuen Richtlinieneinstellungen haben Vorrang vor den alten Einstellungen. Citrix empfiehlt, nur die neuen Richtlinieneinstellungen zu verwenden und alle älteren Einstellungen zu löschen, um unerwartetes Verhalten zu vermeiden.

Durch die bidirektionale Inhaltsumleitung können HTTP- oder HTTPS-URLs in Webbrowsern oder in Anwendungen eingebettet zwischen der Citrix VDA-Sitzung und dem Clientendpunkt in beide Richtungen weitergeleitet werden. Eine URL, die in einem in der Citrix Sitzung ausgeführten Browser eingegeben wurde, kann mit dem Standardbrowser des Clients geöffnet werden. Umgekehrt kann eine URL, die in einem auf dem Client ausgeführten Browser eingegeben wurde, in einer Citrix Sitzung geöffnet werden, entweder mit einer veröffentlichten Anwendung oder einem Desktop. Einige gängige Anwendungsfälle für die bidirektionale Inhaltsumleitung sind:

- Umleitung von Web-URLs in Fällen, in denen der Startbrowser keinen Netzwerkzugriff auf die Quelle hat.
- Umleitung von Web-URLs aus Gründen der Browserkompatibilität und der Sicherheit.
- Die Umleitung von Web-URLs, die in Anwendungen eingebettet sind, wenn nicht ein Webbrowser in der Citrix Sitzung oder auf dem Client verwendet werden soll.

### Systemanforderungen

- Einzelsitzungs- oder Multisitzungs-OS-VDAs
- Citrix Workspace-App für Windows

Browser:

- Google Chrome mit der Citrix Browserumleitung-Erweiterung (verfügbar im Google Chrome Web Store)
- Microsoft Edge (Chromium) mit der Citrix Browserumleitung-Erweiterung (verfügbar im Google Chrome Web Store)

### Konfiguration

Die bidirektionale Inhaltsumleitung muss mit der Citrix-Richtlinie sowohl auf dem VDA als auch auf dem Client aktiviert werden, damit die Umleitung funktioniert. Die bidirektionale Inhaltsumleitung ist standardmäßig deaktiviert.

Informationen zur VDA-Konfiguration finden Sie unter Bidirektionale Inhaltsumleitung in den ICA-Richtlinieneinstellungen.

Informationen zur Clientkonfiguration finden Sie unter Bidirektionale Inhaltsumleitung in der Dokumentation von Citrix Workspace-App für Windows.

Browsererweiterungen müssen mit den angezeigten Befehlen registriert werden. Führen Sie die Befehle wie erforderlich auf dem VDA und dem Client aus, basierend auf dem verwendeten Browser.

Um die Browsererweiterungen auf dem VDA zu registrieren, öffnen Sie eine Eingabeaufforderung. Führen Sie dann `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` mit der erforderlichen Browseroption aus, wie in den Beispielen gezeigt:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Um die Erweiterung in allen verfügbaren Browsern zu registrieren, führen Sie Folgendes aus:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Um die Registrierung einer Browsererweiterung aufzuheben, verwenden Sie die Option `/unreg<browser>` wie im Beispiel gezeigt:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Um die Browsererweiterungen auf dem Client zu registrieren, öffnen Sie eine Eingabeaufforderung und führen Sie `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` mit denselben Optionen wie in den Beispielen gezeigt aus.

> **Hinweis:**
>
> Der Registrierungsbefehl veranlasst Chrome- und Edge-Browser die Benutzer beim ersten Start aufzufordern, die Citrix Browserumleitungserweiterung zu aktivieren. Die Browsererweiterung kann auch manuell im Google Chrome Web Store installiert werden.

### Platzhalterumleitung vom Citrix VDA zum Client

Die bidirektionale Inhaltsumleitung unterstützt die Verwendung von Platzhaltern bei der Definition der umzuleitenden URLs. Lesen Sie zum Konfigurieren der bidirektionalen Inhaltsumleitung die Anweisungen zur [Konfiguration] unter (/en-us/citrix-virtual-apps-desktops/general-content-redirection/bidirectional-content-redirection.html#configuration).

Legen Sie in Citrix Studio die Platzhalter-URL unter **Für Umleitung an Client zulässige URLs** fest. Das Sternchen (*) ist das Platzhalterzeichen.

> **HINWEIS:**
>
> - Legen Sie die **Für Umleitung an VDA zulässige URLs** nicht in der Clientrichtlinie fest. Stellen Sie sicher, dass die Sites die **Für Umleitung an VDA zulässige URLs** festlegen, um Endlosschleifen bei der Umleitung zu vermeiden.
> - Top-Level-Domänen werden nicht unterstützt. Beispiel: `https://www.citrix.*` oder `http://www.citrix.co*` wird nicht umgeleitet.

### Umleitung benutzerdefinierter Protokolle vom VDA zum Client

Die bidirektionale Inhaltsumleitung unterstützt die Umleitung benutzerdefinierter Protokolle vom Citrix VDA zum Client. Andere Protokolle als HTTP oder HTTPS werden unterstützt. Lesen Sie zum Konfigurieren der bidirektionalen Inhaltsumleitung die Anweisungen zur [Konfiguration] unter (/en-us/citrix-virtual-apps-desktops/general-content-redirection/bidirectional-content-redirection.html#configuration).

Legen Sie in Citrix Studio das benutzerdefinierte Protokoll unter **Für Umleitung an Client zulässige URLs** fest.

> **HINWEIS:**
>
> - Beim Client muss eine Anwendung registriert sein, damit das Protokoll verarbeitet werden kann. Andernfalls wird die URL zum Client umgeleitet und kann nicht gestartet werden.
> - Benutzerdefinierte Protokoll-URLs, die Sie in den Browsern Chrome und Edge eingeben oder starten, werden nicht unterstützt und nicht umgeleitet.
> - Die folgenden Protokolle werden nicht unterstützt: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

### Andere Überlegungen

- Die Anforderungen und Konfigurationen des Browsers gelten nur für den Browser, der die Umleitung startet. Der Zielbrowser, in dem die URL geöffnet wird, nachdem die Umleitung erfolgreich war, wird bei der Unterstützung nicht berücksichtigt. Beim Umleiten von URLs vom VDA zu einem Client ist nur auf dem VDA eine unterstützte Browserkonfiguration erforderlich. Umgekehrt ist beim Umleiten von URLs vom Client zu einem VDA nur auf dem Client eine unterstützte Browserkonfiguration erforderlich. Umgeleitete URLs werden je nach Richtung an den Standardbrowser auf der Zielmaschine übergeben, entweder der Client oder der VDA. Es ist NICHT erforderlich, denselben Browsertyp auf dem VDA und dem Client zu verwenden.
- Stellen Sie sicher, dass Umleitungsregeln keine Schleifenkonfiguration ergeben. Beispiel: Eine VDA-Richtlinie legt die Umleitung von `https://www.citrix.com` fest. Die Clientrichtlinie ist auch so eingestellt, dass dieselbe URL umgeleitet wird. Damit entsteht eine Endlosschleife.
- Es werden nur URLs im HTTP-/HTTPS-Protokoll unterstützt. URL-Abkürzungsprogramme werden nicht unterstützt.
- Für die Client-zu-VDA-Umleitung muss der Windows-Client mit Administratorrechten installiert sein.
- Wenn der Zielbrowser bereits geöffnet ist, wird die umgeleitete URL auf einer neuen Registerkarte geöffnet. Sonst wird die URL in einem neuen Browserfenster geöffnet.
- Die bidirektionale Inhaltsumleitung funktioniert nicht, wenn lokaler App-Zugriff (LAA) aktiviert ist.

## Lokaler App-Zugriff und URL-Umleitung

June 21, 2022

## Einführung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Desktops nötig ist. Lokaler App-Zugriff ermöglicht Folgendes:

- Direkter Zugriff von virtuellen Desktops auf Anwendungen, die lokal auf einem Laptop, PC oder einem anderen Gerät installiert sind
- Bereitstellung einer flexiblen Anwendungsbereitstellungslösung Wenn Benutzer lokale Anwendungen haben, die Sie nicht virtualisieren können oder die IT nicht verwaltet, verhalten sich diese Anwendungen weiterhin so, als ob sie auf einem virtuellen Desktop installiert wären.
- Eliminieren Sie Doppelhoplatenz bei separat vom virtuellen Desktop gehosteten Anwendungen. Hierfür platzieren Sie eine Verknüpfung mit der veröffentlichten Anwendung auf das Windows-Gerät des Benutzers.
- Unter anderem können die folgenden Anwendungen verwendet werden:
  - Videokonferenzsoftware, z. B. GoToMeeting.
  - Spezial- oder Nischenanwendungen, die noch nicht virtualisiert sind.
  - Anwendungen und Peripheriegeräte, die andernfalls große Datenmengen von einem Benutzergerät zum Server und zurück zum Benutzergerät senden würden. Beispiel hierfür sind DVD-Brenner und TV-Tuner.

In Citrix Virtual Apps and Desktops verwenden gehostete Desktopsitzungen die URL-Umleitung zum Starten von lokalen App-Zugriff-Anwendungen. Durch URL-Umleitung wird die Anwendung unter mehr als einer URL-Adresse bereitgestellt. Durch Auswählen eingebetteter Links in einem Browser in einer Desktopsitzung wird ein lokaler Browser gestartet (basierend auf der URL-Sperrliste des Browsers). Wenn Sie auf eine URL klicken, die nicht auf der Sperrliste steht, wird die URL erneut in der Sitzung geöffnet.

Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen. Für Anwendungssitzungen können Sie nur die Host-zu-Client-Inhaltsumleitung verwenden, wobei es sich um eine Art von Server-Dateitypzuordnung handelt. Diese FTA leitet bestimmte Protokolle an den Client um, z. B. HTTP, HTTPS, RTSP oder MMS. Wenn Sie beispielsweise nur eingebettete Links mit HTTP öffnen, werden die Links direkt in der Clientanwendung geöffnet. URL-Sperr- und Positivlisten werden nicht unterstützt.

Wenn der lokale App-Zugriff aktiviert ist, werden URLs, die Benutzern als Links von lokal ausgeführten Anwendungen oder von den Benutzern gehosteten Anwendungen bzw. als Verknüpfungen auf dem Desktop angezeigt werden, auf eine der folgenden Arten umgeleitet:

- Umleitung vom Computer des Benutzers zum gehosteten Desktop
- Umleitung vom Citrix Virtual Apps and Desktops-Server auf den Computer des Benutzers
- Wiedergabe in der Umgebung, in der sie gestartet werden (keine Umleitung)

Zur Angabe des Pfads für die Inhaltsumleitung von bestimmten Websites konfigurieren Sie die URL-Positivliste und die URL-Sperrliste auf dem Virtual Delivery Agent. Diese Listen enthalten mehrteilige Registrierungsschlüssel, die die Richtlinieneinstellungen für die URL-Umleitung festlegen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Lokaler App-Zugriff".

Mit den folgenden Ausnahmen können URLs auf dem VDA wiedergegeben werden:

- Regions-/Gebietsschemainformationen: Websites, die Gebietsschemainformationen benötigen, wie msn.com oder news.google.com (je nach Region wird eine bestimmte Seite geöffnet). Wenn der VDA beispielsweise von einem Datencenter in Großbritannien bereitgestellt wird und der Client eine Verbindung aus Indien herstellt, würde der Benutzer erwarten, dass die Website in.msn.com erscheint. Stattdessen wird uk.msn.com angezeigt.
- Multimedia-Inhalt: Websites mit Rich-Media-Inhalten, die auf dem Clientgerät wiedergegeben werden, ermöglichen die gewohnte Benutzererfahrung und das Einsparen von Bandbreite während die Funktionalität auch in Netzwerken mit hoher Latenz gewährleistet ist. Dieses Feature leitet Websites mit anderen Medientypen wie Silverlight um. Somit ist die Umgebung sehr sicher. Die vom Administrator genehmigten URLs werden auf dem Client ausgeführt, während die restlichen URLs an VDA weitergeleitet werden.

Zusätzlich zur URL-Umleitung können Sie die Umleitung nach Dateitypzuordnung verwenden. FTA startet lokale Anwendungen, wenn Dateien in einer Sitzung geöffnet werden sollen. Wenn die lokale Anwendung gestartet wird, muss sie Zugriff auf die Datei haben, um sie zu öffnen. Daher können Sie mit lokalen Anwendungen nur Dateien öffnen, die sich auf Netzwerkfreigaben oder auf Clientlaufwerken (mit Clientlaufwerkzuordnung) befinden. Wenn beispielsweise der PDF-Reader eine lokale Anwendung ist und eine PDF-Datei geöffnet werden soll, wird zum Öffnen der Datei der lokale PDF-Reader verwendet. Da die lokale Anwendung direkt auf die Datei zugreifen kann, erfolgt keine Netzwerkübertragung über ICA zum Öffnen der Datei.

### Anforderungen, Faktoren und Einschränkungen

Lokaler App-Zugriff wird für die gültigen Betriebssystemen für VDAs für Windows-Multisitzungs-OS und Windows-Einzelsitzungs-OS unterstützt. Der lokale App-Zugriff erfordert mindestens Version 4.1 der Citrix Workspace-App für Windows. Die folgenden Browser werden unterstützt:

- Edge, neueste Version
- Firefox, neueste Version und Extended Support Release
- Chrome, neueste Version

Beachten Sie die folgenden Punkte und Einschränkungen, wenn Sie lokalen App-Zugriff und URL-Umleitung verwenden.

- Lokaler App-Zugriff ist für virtuelle Desktops im Vollbildmodus unter Einbeziehung aller Monitore gedacht:

  - Die Benutzererfahrung kann beeinträchtigt werden, wenn Sie lokalen App-Zugriff auf einem virtuellen Desktop verwenden, der im Fenstermodus bzw. nicht auf allen Monitoren ausgeführt wird.
  - Bei Verwendung mehrerer Monitore: Der maximierte Monitor ist der Standarddesktop für alle Anwendungen, die in der Sitzung gestartet werden. Dies gilt auch dann, wenn nachfolgende Anwendungen normalerweise auf einem anderen Monitor starten würden.
  - Das Feature unterstützt einen VDA. Es ist keine Integration mit mehreren VDAs gleichzeitig möglich.

- Einige Anwendungen können sich unerwartet verhalten und Benutzer beeinträchtigen:

  - Benutzer können die Laufwerkbuchstaben verwechseln, z. B. das lokale C:-Laufwerk mit dem virtuellen C:-Desktoplaufwerk.
  - Auf virtuellen Desktops verfügbare Drucker sind nicht für die lokalen Anwendungen verfügbar.
  - Anwendungen, die erweiterte Berechtigungen erfordern, können nicht als clientgehostete Anwendungen gestartet werden.
  - Keine spezielle Behandlung von Anwendungen mit einer Instanz (z. B. Windows Media Player).
  - Lokale Anwendungen werden mit dem Windows-Design der lokalen Maschine angezeigt.
  - Vollbildanwendungen werden nicht unterstützt. Dies schließt Anwendungen ein, die im Vollbildmodus geöffnet werden, z. B. PowerPoint-Bildschirmpräsentationen oder Fotoanzeigen, die den gesamten Desktop ausfüllen.
  - Lokaler App-Zugriff kopiert die Eigenschaften der lokalen Anwendung (z. B. die Verknüpfungen auf dem Clientdesktop und im Startmenü) auf dem VDA. Es werden jedoch keine anderen Eigenschaften, wie Tastenkombinationen und schreibgeschützte Attribute, kopiert.
  - Anwendungen, die die Reihenfolge der überlappenden Fenster anpassen, können unvorhersehbare Ergebnisse verursachen. Beispielsweise könnten einige Fenster ausgeblendet werden.
  - Verknüpfungen, einschließlich Arbeitsplatz, Papierkorb, Systemsteuerung, Netzlaufwerkverknüpfungen und Ordnerverknüpfungen werden nicht unterstützt.
  - Die folgenden Dateitypen und Dateien werden nicht unterstützt: benutzerdefinierte Dateitypen, Dateien ohne zugeordnete Programme, ZIP-Dateien und ausgeblendete Dateien.
  - Taskleistengruppierung wird nicht für gemischte 32-Bit/64-Bit-Systeme mit clientgehosteten Anwendungen und VDA-Anwendungen unterstützt. Lokale 32-Bit-Anwendungen können also nicht mit 64-Bit-VDA-Anwendungen gruppiert werden.
  - Anwendungen können nicht mit COM gestartet werden. Beispiel: Wenn Sie auf ein eingebettetes Office-Dokument in einer Office-Anwendung klicken, wird der Prozessstart nicht erkannt und die Integration der lokalen Anwendung schlägt fehl.

- Double-Hop-Szenarien, bei denen ein Benutzer einen virtuellen Desktop aus einer anderen

virtuellen Desktopsitzung startet, werden nicht unterstützt.

- Die URL-Umleitung unterstützt nur explizite URLs, d. h. solche, die in der Adressleiste des Browsers angezeigt werden oder mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen.
- Benutzer haben keine Berechtigung, im lokalen Desktopordner in einer VDA-Sitzung Dateien zu erstellen.
- Mehrere Instanzen einer lokal ausgeführten Anwendung verhalten sich entsprechend den Taskleisteneinstellungen für den virtuellen Desktop. Verknüpfungen mit lokal ausgeführten Anwendungen werden jedoch nicht mit ausgeführten Instanzen dieser Anwendungen gruppiert. Sie werden auch nicht mit ausgeführten Instanzen von gehosteten Anwendungen oder mit an gehosteten Anwendungen angehefteten Verknüpfungen gruppiert. Benutzer können nur Fenster von lokal ausgeführten Anwendungen von der Taskleiste aus schließen. Zwar können Benutzer die Fenster von lokalen Anwendungen in der Desktop-Taskleiste und im Startmenü anheften, jedoch starten die Anwendungen bei Verwendung dieser Verknüpfungen möglicherweise nicht konsistent.
- Wenn Sie die Richtlinieneinstellung **Lokalen App-Zugriff zulassen** auf **Aktiviert** festlegen, wird die Browserinhaltsumleitung nicht unterstützt.

### Interaktion mit Windows

Bei der Interaktion zwischen lokaler App-Zugriff und Windows tritt u. a. das folgende Verhalten auf.

- Verknüpfungen in Windows 8 und Windows Server 2012
  - Windows Store-Apps, die auf dem Client installiert sind, werden nicht als Teil der Verknüpfungen von lokalem App-Zugriff aufgelistet.
  - Bild- und Videodateien werden standardmäßig mit Windows Store-Apps geöffnet. Lokaler App-Zugriff listet die Windows Store-Apps jedoch auf und öffnet Verknüpfungen mit Desktopanwendungen.
- Local Programs
  - In Windows 7 ist der Ordner im Startmenü verfügbar.
  - In Windows 8 ist der Ordner “Local Programs”nur verfügbar, wenn der Benutzer **Alle Apps** als Kategorie auf der Startseite auswählt. Nicht alle Unterordner werden in Local Programs angezeigt.
- Windows 8-Grafikfunktionen für Anwendungen
  - Desktopanwendungen sind auf den Desktopbereich beschränkt und werden von der Startseite bzw. Anwendungen im Windows 8-Stil vollständig abgedeckt.

  - Mit lokalem App-Zugriff verwendete Anwendungen verhalten sich jedoch bei der Verwendung von mehreren Monitoren nicht wie Desktopanwendungen. Bei der Verwendung mehrerer Monitore werden die Startseite und der Desktop auf unterschiedlichen Monitoren angezeigt.

- Windows 8 und lokaler App-Zugriff mit URL-Umleitung
  - Da bei Windows 8 Internet Explorer keine Add-Ons aktiviert sind, müssen Sie den Desktop-Internet Explorer zum Aktivieren von URL-Umleitung verwenden.
  - In Windows Server 2012 werden Add-Ons von Internet Explorer standardmäßig deaktiviert. Um die URL-Umleitung zu implementieren, deaktivieren Sie die verstärkte Sicherheitskonfiguration für Internet Explorer. Setzen Sie die Internet Explorer-Optionen zurück und starten Sie das Programm neu, um sicherzustellen, dass Add-Ons für Standardbenutzer aktiviert sind.

## Konfigurieren von lokalem App-Zugriff und URL-Umleitung

Verwenden von lokalem App-Zugriff und URL-Umleitung für die Citrix Workspace-App:

- Installieren Sie die Citrix Workspace-App auf dem lokalen Client. Sie können beide Features während der Installation der Citrix Workspace-App aktivieren. Alternativ können Sie die Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor aktivieren.
- Legen Sie die Richtlinieneinstellung **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Sie können auch die Richtlinie für URL-Positiv- und -Sperrlisten für die URL-Umleitung konfigurieren. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Lokaler App-Zugriff".

### Aktivieren von lokalem App-Zugriff und URL-Umleitung

Führen Sie die folgenden Schritte aus, um den lokalen App-Zugriff für alle lokalen Anwendungen zu aktivieren:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Richtlinien**.
2. Wählen Sie in der Aktionsleiste **Richtlinie erstellen**.
3. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "Lokalen App-Zugriff zulassen"im Suchfeld ein und klicken Sie auf **Auswählen**.
4. Wählen Sie im Fenster "Einstellung bearbeiten"die Option **Zulässig** aus. Standardmäßig ist die Richtlinie **Lokalen App-Zugriff zulassen** deaktiviert. Wenn diese Einstellung zugelassen wird, können Endbenutzer selbst entscheiden, ob veröffentlichte Anwendungen und Verknüpfungen für den lokalen App-Zugriff in der Sitzung aktiviert sind. (Wenn die Einstellung nicht zulässig ist, sind sowohl veröffentlichte Anwendungen als auch Verknüpfungen für den lokalen App-Zugriff für den VDA deaktiviert.) Diese Richtlinie gilt für die gesamte Maschine und für die URL-Umleitungsrichtlinie.

5. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "URL-Umleitungspositivliste"im Suchfeld ein und klicken Sie auf **Auswählen**. Die URL-Umleitungspositivliste gibt URLs an, die im Standardbrowser der Remotesitzung geöffnet werden können.
6. Klicken Sie im Fenster "Einstellung bearbeiten"auf **Hinzufügen**, um die URLs hinzuzufügen, und klicken Sie auf **OK**.
7. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "URL-Umleitungssperrliste"im Suchfeld ein und klicken Sie auf **Auswählen**. Die URL-Umleitungssperrliste gibt URLs an, die an den Standardbrowser auf dem Endpunkt weitergeleitet werden.
8. Klicken Sie im Fenster "Einstellung bearbeiten"auf **Hinzufügen**, um die URLs hinzuzufügen, und klicken Sie auf **OK**.
9. Klicken Sie auf der Seite "Einstellungen"auf **Weiter**.
10. Weisen Sie die Richtlinie auf der Seite "Benutzer und Maschinen"den entsprechenden Bereitstellungsgruppen zu und klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite "Zusammenfassung"die gewählten Einstellungen und klicken Sie auf **Fertig stellen**.

Führen Sie die folgenden Schritte aus, um bei der Installation der Citrix Workspace-App die URL-Umleitung für alle lokalen Anwendungen zu aktivieren:

1. Aktivieren Sie die URL-Umleitung für alle Benutzer einer Maschine, wenn Sie die Citrix Workspace-App installieren. Dadurch werden auch die für URL-Umleitung erforderlichen Browser-Add-Ons registriert.
2. Führen Sie an der Eingabeaufforderung den jeweiligen Befehl zum Installieren der Citrix Workspace-App mit einer der folgenden Optionen aus:
   - Für CitrixReceiver.exe verwenden Sie `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Für CitrixReceiverWeb.exe verwenden Sie `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

#### Aktivieren der Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor

> **Hinweis:**
>
> - Fügen Sie dem lokalen Gruppenrichtlinienobjekt die Vorlagendateien `receiver.admx`/`adml` hinzu, bevor Sie mit dem Gruppenrichtlinien-Editor die Vorlage für den lokalen App-Zugriff aktivieren. Weitere Informationen finden Sie unter Erste Schritte. Suchen Sie nach *Administrative Gruppenrichtlinienobjektvorlage*.
> - Die Vorlagendateien für die Citrix Workspace-App sind nur dann im lokalen Gruppenrichtlinienobjekt unter **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace** verfügbar, wenn Sie die Dateien `CitrixBase.admx`/`CitrixBse.adml` dem Ordner %systemroot%\policyDefinitions hinzufügen.

Führen Sie folgende Schritte aus, um die Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor zu aktivieren:

1. Führen Sie **gpedit.msc** aus.
2. Navigieren Sie zu **Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Klicken Sie auf **Einstellungen für 'Lokaler App-Zugriff'**.
4. Wählen Sie **Aktiviert** und anschließend **URL-Umleitung zulassen**. Registrieren Sie für die URL-Umleitung Browser-Add-Ons über die Befehlszeile (siehe *Registrieren von Browser-Add-Ons* weiter unten).

#### Zugriffsbeschränkung auf veröffentlichte Anwendungen

Sie können den Zugriff auf veröffentlichte Anwendungen über den Registrierungs-Editor oder über das PowerShell-SDK bereitstellen.

Informationen zum Registrierungs-Editor finden Sie unter Lokaler App-Zugriff für veröffentlichte Anwendungen in der Liste der über die Registrierung verwalteten Features.

Verwendung des PowerShell-SDK:

1. Öffnen Sie PowerShell auf der Maschine mit dem Delivery Controller.
2. Geben Sie den folgenden Befehl ein: `set-configsitemetadata -name "studio_clientHosted"-value "true"`.

Verwenden Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK, um Zugriff auf **Anwendung für lokalen App-Zugriff hinzufügen** in einer Citrix DaaS-Bereitstellung zu erhalten. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Remote PowerShell SDK.

1. Laden Sie das Installationsprogramm herunter:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Führen Sie die folgenden Befehle aus:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Geben Sie den folgenden Befehl ein: `set-configsitemetadata -name "studio_clientHosted" -value "true"`.

Nachdem Sie die zutreffenden Schritte oben ausgeführt haben, führen Sie die folgenden Schritte aus, um fortzufahren.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen**.

2. Klicken Sie im oberen mittleren Bereich mit der rechten Maustaste auf den leeren Bereich, und wählen Sie im Menü **Anwendung für lokalen App-Zugriff hinzufügen**. Sie können auch im Aktionsbereich auf **Anwendung für lokalen App-Zugriff hinzufügen** klicken. Klicken Sie auf **Aktualisieren**, um die Option "Anwendung für lokalen App-Zugriff hinzufügen"im Aktionsbereich anzuzeigen.
3. Veröffentlichen Sie die Anwendung "Lokaler App-Zugriff".
    - Der Assistent zum Hinzufügen von lokalem App-Zugriff wird mit der Einführungsseite gestartet, die Sie für zukünftige Starts des Assistenten deaktivieren können.
    - Der Assistent führt Sie durch die im Folgenden beschriebenen Seiten "Gruppen", "Standort", "Identifizierung", "Bereitstellung"und "Zusammenfassung". Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur Zusammenfassung gelangen.
    - Wählen Sie auf der Seite "Gruppen"eine oder mehrere Bereitstellungsgruppen, den die Anwendungen hinzugefügt werden und klicken Sie dann auf **Weiter**.
    - Geben Sie auf der Seite "Speicherort"den vollständigen Pfad der ausführbaren Datei für die Anwendung auf dem lokalen Computer des Benutzers ein und geben Sie den Pfad zu dem Ordner ein, in dem sich die Anwendung ist. Citrix empfiehlt, für den Systemumgebungsvariablenpfad zu verwenden, z. B. %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
    - Übernehmen Sie auf der Seite "Identifizierung"die Standardwerte oder geben Sie die Informationen ein und klicken Sie dann auf **Weiter**.
    - Konfigurieren Sie auf der Seite "Bereitstellung", wie diese Anwendung an Benutzer bereitgestellt wird, und klicken Sie dann auf **Weiter**. Sie können das Symbol für die ausgewählte Anwendung angeben. Sie können auch angeben, ob die Verknüpfung mit der lokalen Anwendung auf dem virtuellen Desktop im Startmenü, auf dem Desktop oder beiden angezeigt wird.
    - Überprüfen Sie auf der Seite "Zusammenfassung"die gewählten Einstellungen und klicken Sie auf **Fertig stellen**, um den Assistenten für Zugriff auf lokale Anwendungen zu beenden.

#### Registrieren von Browser-Add-Ons

> **Hinweis:**
>
> Die für die URL-Umleitung erforderlichen Browser-Add-Ons werden automatisch registriert, wenn Sie die Citrix Workspace-App über die Befehlszeile mit folgender Option installieren: `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Sie können ein Add-On oder alle mit den folgenden Befehlen registrieren und die Registrierung aufheben:

- Registrieren von Add-Ons auf einem Clientgerät: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- Aufheben der Registrierung von Add-Ons auf einem Clientgerät: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- Registrierung von Add-Ons auf einem VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- Aufheben der Registrierung von Add-Ons auf einem VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

Wobei <*Browser*> Internet Explorer, Firefox, Chrome oder All ist.

Beispiel: Mit dem folgenden Befehl werden Internet Explorer-Add-Ons auf einem Gerät mit der Citrix Workspace-App registriert.

C:\Programme\Citrix\ICA Client\redirector.exe/regIE

Mit dem folgenden Befehl werden alle Add-Ons auf einem VDA für Windows-Multisitzungs-OS registriert.

C:\Programme (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

**URL-Interception in Browsern**

- Standardmäßig wird die angegebene URL von Internet Explorer umgeleitet. Wenn die URL nicht in der Sperrliste enthalten ist und dennoch vom Browser oder der Website an eine andere URL-Adresse umgeleitet wird, wird die endgültige URL nicht umgeleitet. Sie wird nicht umgeleitet, selbst wenn sie in der Sperrliste enthalten ist.

Zum richtigen Funktionieren der URL-Umleitung müssen Sie bei entsprechender Aufforderung durch den Browser das Add-On aktivieren. Wenn die mit Internetoptionen verbundenen Add-Ons bzw. die angeforderten Add-Ons deaktiviert sind, funktioniert die URL-Umleitung nicht richtig.

- Firefox-Add-Ons leiten URLs immer um.

Wenn ein Add-On installiert wurde, bietet Firefox auf einer neuen Registerkarte die Möglichkeit, die Add-On-Installation zuzulassen oder zu verhindern. Lassen Sie das Add-On zu, damit das Feature funktioniert.

- Chrome-Add-Ons leiten die endgültige URL stets um, wenn es sich um geleitete und nicht eingegebene URLs handelt.

Die Erweiterungen wurden extern installiert. Wenn Sie die Erweiterung deaktivieren, funktioniert die URL-Umleitung in Google Chrome nicht. Wenn die URL-Umleitung im Inkognito-Modus erforderlich ist, lassen Sie durch Auswählen dieser Option in den Browsereinstellungen zu, dass die Erweiterung im Inkognito-Modus ausgeführt wird.

**Konfigurieren des Verhaltens von lokalen Anwendungen bei der Abmeldung und Trennung**

> **Hinweis:**
>
> Wenn Sie die Einstellungen nicht mit dem unten aufgeführten Verfahren konfigurieren, werden lokale Anwendungen standardmäßig weiter ausgeführt, wenn ein Benutzer sich abmeldet oder die Verbindung zum virtuellen Desktop trennt. Nach der Wiederverbindung werden lokale Anwendungen wieder integriert, wenn sie auf dem virtuellen Desktop verfügbar sind.

Informationen zum Konfigurieren des Verhaltens lokaler Anwendungen beim Abmelden und Trennen finden Sie unter Verhalten lokaler Anwendungen beim Abmelden und Trennen in der Liste der über die Registrierung verwalteten Features.

## Generische USB-Umleitung und Clientlaufwerke

April 18, 2024

HDX-Technologie bietet **optimierte Unterstützung** für die gebräuchlichsten USB-Geräte. Die optimierte Unterstützung bietet eine verbesserte Benutzererfahrung, Leistung und Bandbreiteneffizienz über ein WAN. Die optimierte Unterstützung ist normalerweise, insbesondere aber in Umgebungen mit hoher Latenz oder hohen Sicherheitsanforderungen, die beste Option.

HDX-Technologie bietet **generische USB-Umleitung** für Spezialgeräte ohne optimierte Unterstützung oder wenn diese ungeeignet ist. Beispiele:

- Ein USB-Gerät hat Merkmale, die nicht von der optimierten Unterstützung abgedeckt werden, z. B. eine Maus oder Webcam mit zusätzlichen Tasten.
- Benutzer benötigen Funktionen, die nicht von der optimierten Unterstützung abgedeckt werden.
- Bei dem USB-Gerät handelt es sich um ein Spezialgerät, z. B. ein Test- oder Messgerät oder ein industrielles Steuergerät.
- Eine Anwendung erfordert direkten Zugriff auf das Gerät als USB-Gerät.
- Für das USB-Gerät gibt es nur einen Windows-Treiber. Ein Smartcardleser kann beispielsweise keinen Treiber für die Citrix Workspace-App für Android haben.
- Die Version der Citrix Workspace-App bietet keine optimierte Unterstützung für solche USB-Geräte.

Vorteile von generischer USB-Umleitung:

- Benutzer müssen keine Gerätetreiber auf den Benutzergeräten installieren.
- USB-Clienttreiber werden auf der VDA-Maschine installiert.

**Wichtig:**

- Die generische USB-Umleitung kann zusammen mit der optimierten Unterstützung verwendet werden. Wenn Sie die generische USB-Umleitung aktivieren, konfigurieren Sie Einstellungen für die Citrix Richtlinie "USB-Geräte" für die generische USB-Umleitung und für die optimierte Unterstützung.
- Die Citrix Richtlinieneinstellung unter Regeln für die USB-Clientgeräteoptimierung ist eine spezifische Einstellung für die generische USB-Umleitung für ein bestimmtes USB-Gerät. Es gilt nicht für die hier beschriebene optimierte Unterstützung.
- Bei Vermittlung einer Sitzung mit Citrix Software an eine virtuelle Azure-Maschine bietet Citrix bestmögliche Unterstützung für die USB-Umleitung an die virtuelle Azure-Maschine. Wir bieten Support bei Problemen der Citrix Software, jedoch nicht für die zugrunde liegende virtuelle Azure-Maschine.
- CD/DVD-Geräte mit Brennfunktionen können umgeleitet werden, die Brennfunktion kann jedoch nicht verwendet werden. Grund dafür sind die Sitzungspufferlimits.

### Überlegungen zur Leistung für USB-Geräte

Bei Verwendung der generischen Umleitung bestimmter USB-Gerätetypen können sich Netzwerklatenz und Bandbreite auf die Benutzererfahrung und den USB-Gerätebetrieb auswirken. Die Funktion zeitempfindlicher Geräte kann beispielsweise bei geringer Bandbreite und hoher Latenz gestört werden. Verwenden Sie, falls möglich, stattdessen die optimierte Unterstützung.

Einige Geräte erfordern eine hohe Bandbreite, z. B. 3D-Mäuse (die mit bandbreitenintensiven 3D-Anwendungen verwendet werden). Kann die Bandbreite nicht erhöht werden, können Sie evtl. die Bandbreitennutzung anderer Komponenten über die Einstellung der Bandbreitenrichtlinie anpassen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Bandbreite" für die Client-USB-Geräteumleitung und unter Einstellungen der Richtlinie "Multistreamverbindungen".

### Überlegungen zur Sicherheit für USB-Geräte

Einige USB-Geräte sind von Haus aus sicherheitsempfindlich, z. B. Smartcardleser, Fingerabdruckleser und Signatur-Tablets. Andere, etwa USB-Speichergeräte, können zur Übertragung vertraulicher Daten verwendet werden.

USB-Geräte werden häufig zur Verbreitung von Schadsoftware verwendet. Über die Konfiguration der Citrix Workspace-App und von Citrix Virtual Apps and Desktops können entsprechende Sicherheitsrisiken vermindert, jedoch nicht eliminiert werden Dies gilt sowohl für die generische USB-Umleitung als auch für die optimierte Unterstützung.

> **Wichtig:**
>
> Verwenden Sie für sicherheitsempfindliche Geräte und Daten immer sichere HDX-Verbindungen mit TLS oder IPsec.
>
> Aktivieren Sie nur Unterstützung für USB-Geräte, die Sie benötigen. Konfigurieren Sie die generische USB-Umleitung und die optimierte Unterstützung für diese Anforderungen.
>
> Informieren Sie die Benutzer über die sichere Verwendung von USB-Geräten:
>
> - Nur USB-Geräte verwenden, die von einer vertrauenswürdigen Quelle stammen.
> - USB-Geräte in zugänglichen Umgebungen (z. B. Internetcafé) nicht unbeaufsichtigt lassen.
> - Erläutern Sie die Risiken der Verwendung eines USB-Geräts auf mehreren Computern.

### Kompatibilität mit der generischen USB-Umleitung

Die generische USB-Umleitung unterstützt USB 2.0- und ältere Geräte. Die generische USB-Umleitung unterstützt außerdem USB 3.0-Geräte, wenn diese an einem USB 2.0- oder USB 3.0-Anschluss angeschlossen sind. Die generische USB-Umleitung bietet keine Unterstützung für USB-Features wie Super Speed, die mit USB 3.0 eingeführt wurden.

Folgende Citrix Workspace-App-Versionen unterstützen die generische USB-Umleitung:

- Citrix Workspace-App für Windows, siehe Konfigurieren der Anwendungsbereitstellung
- Citrix Workspace-App für Mac, siehe Konfigurieren von Citrix Workspace-App für Mac
- Citrix Workspace-App für Linux, siehe Optimieren
- Citrix Workspace-App für Chrome, siehe Citrix Workspace-App für Chrome

Informationen zu den Citrix Workspace-App-Versionen finden Sie unter Citrix Workspace-App-Featurematrix.

Wenn Sie eine ältere Version der Citrix Workspace-App verwenden, prüfen Sie in der zugehörigen Dokumentation, ob die generische USB-Umleitung unterstützt wird. Die Dokumentation zur Citrix Workspace-App enthält Informationen zu allen Einschränkungen für unterstützte USB-Gerätetypen.

Die generische USB-Umleitung unterstützt Desktopsitzungen mit VDAs für Einzelsitzungs-OS ab Version 7.6 bis zur aktuellen Version.

Die generische USB-Umleitung unterstützt Desktopsitzungen mit VDAs für Multisitzungs-OS ab Version 7.6 bis zur aktuellen Version, mit folgenden Einschränkungen:

- Der VDA muss unter Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 oder Windows Server 2022 ausgeführt werden.
- Der USB-Gerätetreiber muss mit dem Remotedesktop-Sitzungshost für das Betriebssystem des VDAs (Windows 2012 R2) einschließlich voller Virtualisierung kompatibel sein.

Einige USB-Gerätetypen werden nicht von der generischen USB-Umleitung unterstützt, da ihre Umleitung nicht nützlich wäre:

- USB-Modems
- USB-Netzwerkadapter
- USB-Hubs. Mit USB-Hubs verbundene USB-Geräte werden separat behandelt.
- Virtuelle USB-COM-Anschlüsse. Verwenden Sie hierfür statt der generischen USB-Umleitung die COM-Anschlussumleitung.

Weitere Informationen zu USB-Geräten, für die die generische USB-Umleitung getestet wurde, finden Sie unter Citrix Ready Marketplace. Einige USB-Geräte funktionieren bei generischer USB-Umleitung nicht einwandfrei.

### Konfigurieren der generischen USB-Umleitung

Sie können festlegen, für welche USB-Gerätetypen die generische USB-Umleitung verwendet werden soll, und sie separat für die einzelnen Gerätetypen konfigurieren.

- Auf dem VDA mit Citrix Richtlinieneinstellungen. Weitere Informationen finden Sie unter Umleitung von Clientlaufwerken und Benutzergeräten und Einstellungen der Richtlinie "USB-Geräte".
- In der Citrix Workspace-App über Citrix Workspace-App-abhängige Mechanismen. Beispielsweise können durch eine administrative Vorlage Registrierungseinstellungen zur Konfiguration der Citrix Workspace-App für Windows gesteuert werden. Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Weitere Informationen finden Sie unter Konfigurieren in der Dokumentation der Citrix Workspace-App für Windows.

Diese separate Konfiguration ist flexibler. Beispiel:

- Wenn zwei verschiedene Abteilungen für die Citrix Workspace-App und den VDA verantwortlich sind, können sie eigene Vorgaben festlegen. Diese Konfiguration gilt dann, wenn ein Benutzer in einer Abteilung auf eine Anwendung in einer anderen Abteilung zugreift.
- Citrix Richtlinieneinstellungen steuern USB-Geräte, die nur für bestimmte Benutzer oder nur für Benutzer, die eine Verbindung über das LAN anstelle von Citrix Gateway herstellen, zugelassen werden sollen.

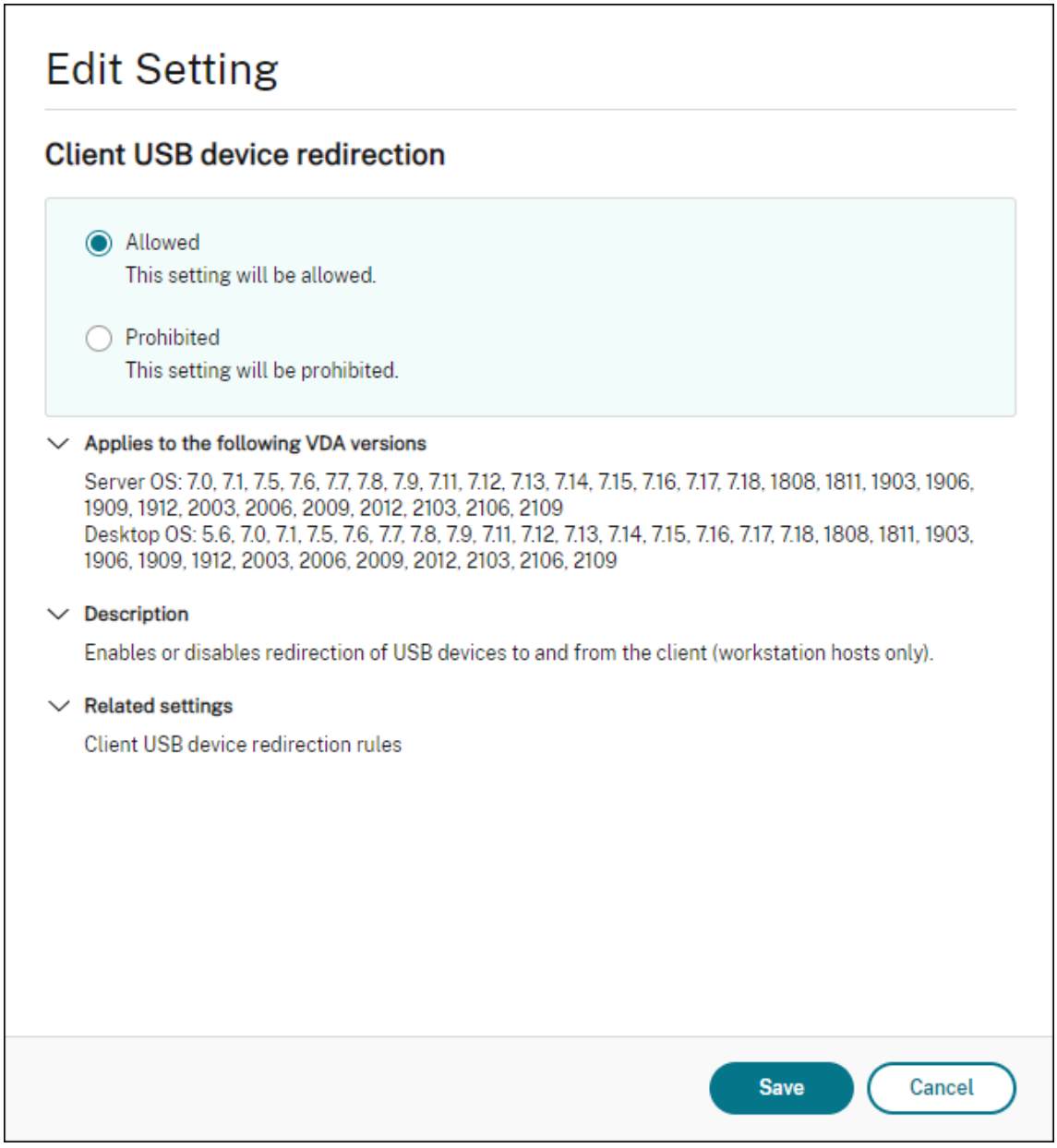
### Aktivieren der generischen USB-Umleitung

Um die generische USB-Umleitung zu aktivieren (= keine manuelle Umleitung durch den Benutzer erforderlich), konfigurieren Sie Citrix Richtlinieneinstellungen und die Verbindungseinstellungen der Citrix Workspace App.

Führen Sie in den Citrix Richtlinieneinstellungen folgende Schritte aus:

1. Fügen Sie die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie den Wert auf **Zugelassen** ein.



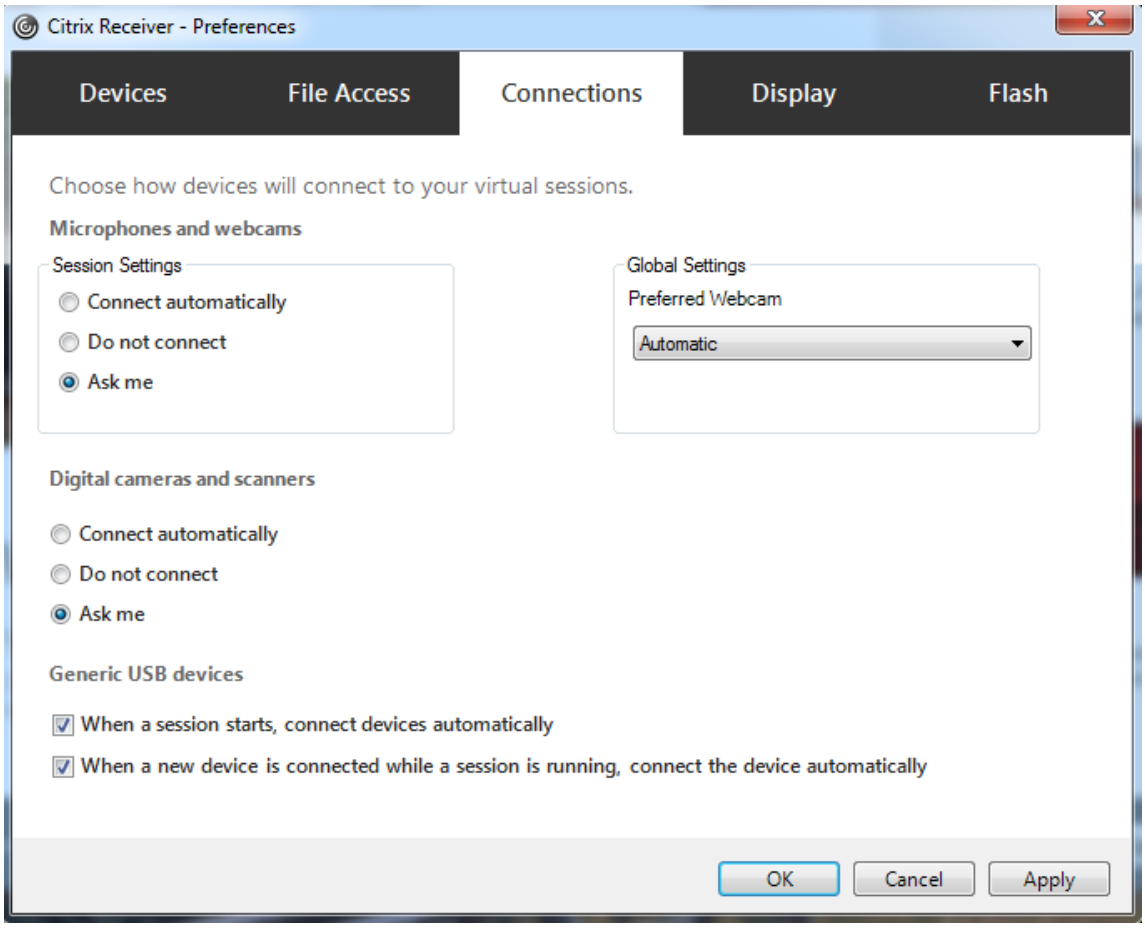

2. Optional: Zum Aktualisieren der Liste der zur Umleitung verfügbaren USB-Geräte fügen Sie die Einstellung Regeln für die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie die USB-Richtlinienregeln ein.

   Gehen Sie in der Citrix Workspace-App folgendermaßen vor:

3. Geben Sie an, dass Geräte automatisch, ohne manuelle Umleitung verbunden werden. Sie können eine administrative Vorlage verwenden oder die Einstellung unter "Citrix Workspace-App

für Windows > Einstellungen > Verbindungen"festlegen.




Wenn Sie im vorigen Schritt die USB-Richtlinienregeln für den VDA festgelegt haben, geben Sie nun die gleichen Richtlinienregeln für die Citrix Workspace-App ein.

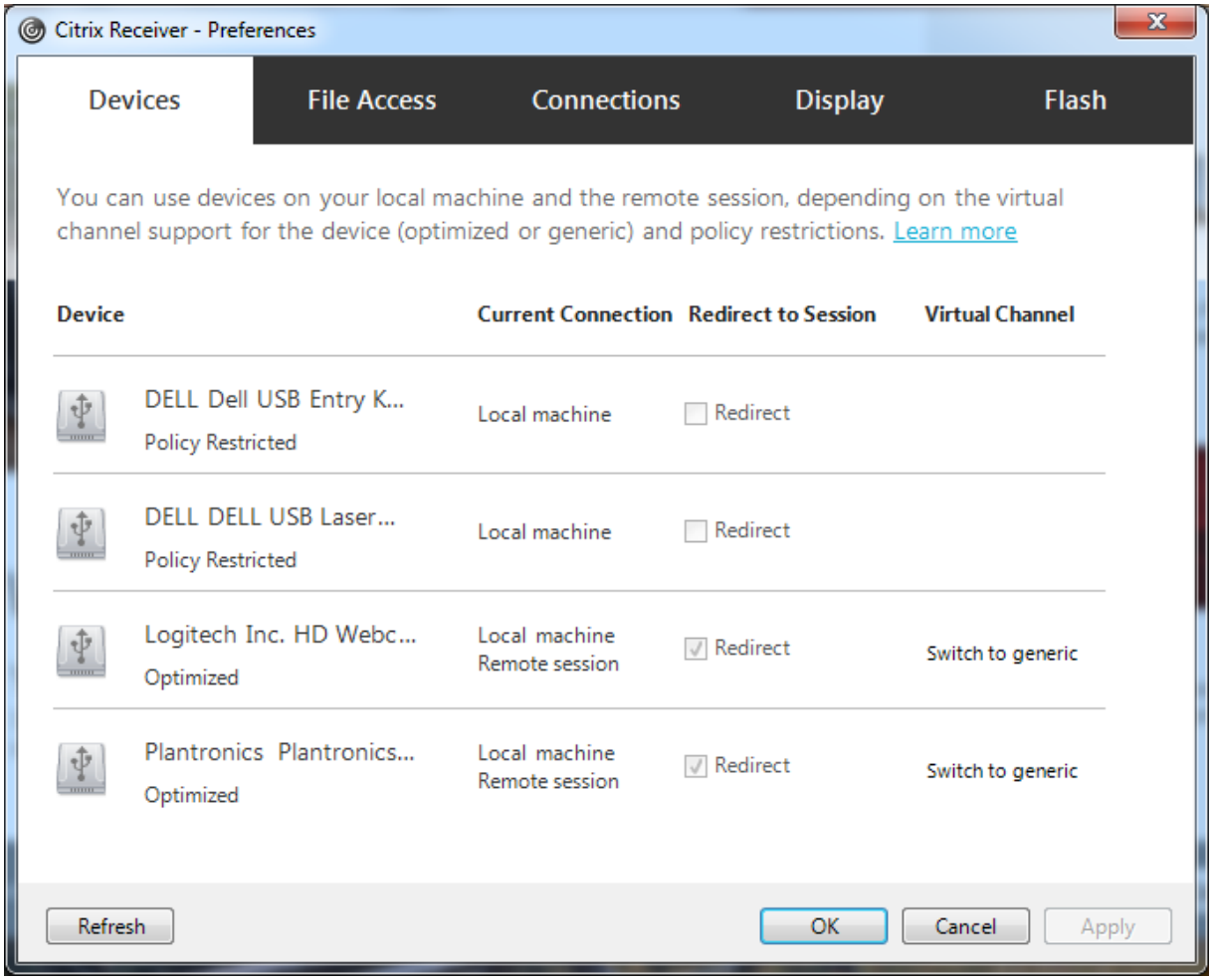
Informationen zur USB-Unterstützung Für Thin Clients und die erforderliche Konfiguration erhalten Sie vom Hersteller.

### Konfigurieren der für die generische USB-Umleitung verfügbaren USB-Gerätetypen

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfiguriert wurden. USB-Geräte werden auch automatisch umgeleitet, wenn der Verbindungsbalken nicht angezeigt wird.

Die Benutzer können Geräte, die nicht automatisch umgeleitet werden, explizit umleiten, indem sie sie aus der USB-Geräteliste auswählen. Weitere Informationen finden Sie unter Anzeigen von Geräten in Desktop Viewer in der Hilfe zur Citrix Workspace-App für Windows.




Verwendung der generischen USB-Umleitung anstelle der optimierten Unterstützung:

- Wählen Sie in der Citrix Workspace-App das USB-Gerät für die generische USB-Umleitung manuell aus und wählen Sie im Dialogfeld “Einstellungen”auf der Registerkarte “Geräte”die Option **Zu allgemein wechseln**.
- Wählen Sie das USB-Gerät für die generische USB-Umleitung automatisch, indem Sie die automatische Umleitung für den entsprechenden USB-Gerätetyp konfigurieren (z. B. AutoRedirectStorage=1) und die USB-Benutzereinstellung auf die automatische Verbindung der USB-Geräte festlegen. Weitere Informationen finden Sie unter Configure automatic redirection of USB devices.

> **Hinweis:**
>
> Konfigurieren Sie die generische USB-Umleitung für Webcams nur dann, wenn die Webcam nicht mit der HDX-Multimediaumleitung kompatibel ist.

Um zu verhindern, dass USB-Geräte je aufgeführt oder umgeleitet werden, können Sie für die Citrix Workspace-App und den VDA spezifische Regeln festlegen.

Für die generische USB-Umleitung benötigen Sie mindestens die USB-Geräteklasse und die Unterklasse. Nicht für alle USB-Geräte wird die Geräteklasse bzw. Unterklasse verwendet, die man vermuten würde. Beispiel:

- Für Stifte wird die Klasse "Maus"verwendet.
- Für Smartcardleser kann eine vom Hersteller definierte Klasse oder die Klasse "HID-Geräte"gelten.

Zur präziseren Steuerung müssen Sie die Hersteller-, Produkt- und Release-ID kennen. Sie erhalten diese Informationen beim Vertreiber des Geräts.

> **Wichtig:**
>
> Manipulierte USB-Geräte können USB-Gerätemerkmale präsentieren, die nicht ihrer beabsichtigten Nutzung entsprechen. Geräteregeln sind nicht zur Verhinderung solcher Fälle vorgesehen.

Die für die generische USB-Umleitung verfügbaren USB-Geräte legen Sie über Regeln für die Client-USB-Geräteumleitung für den VDA und die Citrix Workspace-App fest, welche die USB-Standardrichtlinienregeln außer Kraft setzen.

VDA:

- Bearbeiten Sie die Administrator-Überschreibungsregeln für Maschinen mit Multisitzungs-OS mit den Gruppenrichtlinienregeln. Die Gruppenrichtlinien-Verwaltungskonsole ist auf dem Installationsmedium enthalten:
  - Für x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Für x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Citrix Workspace-App für Windows:

- Bearbeiten Sie die Benutzergeräteregistrierung. Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie das Gerät über die Active Directory-Gruppenrichtlinie ändern können:
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Die Produktstandardregeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. Ändern Sie diese Produktstandardregeln nicht. Verwenden Sie sie als Anleitung zum Erstellen von Administrator-Überschreibungsregeln (siehe Erläuterungen weiter unten). Die GPO-Überschreibungen werden ausgewertet, bevor die Produktstandardregeln angewendet werden.

Die Administrator-Override-Regeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. GPO-Richtlinienregeln haben das Format **{Allow:|Deny:}** gefolgt von *Tag=Wert*-Ausdrücken, die durch Leerzeichen getrennt sind.

Die folgenden Tags werden unterstützt:

| Tag | Beschreibung |
|---|---|
| VID | Vendor-ID vom Gerätedeskriptor |
| PID | Produkt-ID vom Gerätedeskriptor |
| REL | Release-ID vom Gerätedeskriptor |
| Klasse | Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor; verfügbare USB-Klassencodes finden Sie auf der USB-Website unter http://www.usb.org/. |
| SubClass | Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor |
| Prot | Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor |

Wenn Sie Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Einer Regel kann optional ein Kommentar folgen, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen dienen als Trennzeichen, sie können nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class = 08 SubClass=05 eine gültige Regel, Deny: Class=0 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.

> **Hinweis:**
>
> Wenn Sie die ADM-Vorlagendatei verwenden, müssen Sie die Regeln in einer einzigen Zeile mit

> Semikolons getrennt eingeben.

Beispiele:

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für Hersteller- und Produkt-IDs:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für eine definierte Klasse, Unterklasse und ein Protokoll:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

### Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen.

Wenn Sie mit der Citrix Workspace-App für Windows arbeiten, gilt Folgendes:

- Geräte, die nach dem Sitzungsbeginn angeschlossen werden, werden unmittelbar im USB-Menü von Desktop Viewer angezeigt.
- Wenn ein USB-Gerät nicht richtig umgeleitet wird, können Sie das Problem u. U. beheben, indem Sie das Gerät erst nach dem Beginn der virtuellen Sitzung anschließen.
- Um Datenverlust zu verhindern, verwenden Sie das Windows-Symbol "Hardware sicher entfernen", bevor Sie das USB-Gerät entfernen.

### Steuerung der Sicherheit für USB-Massenspeichergeräte

Die optimierte Unterstützung steht für USB-Massenspeichergeräte zur Verfügung. Die Unterstützung ist Teil der Citrix Virtual Apps and Desktops-Clientlaufwerkzuordnung. Laufwerke auf Benutzergeräten werden automatisch Laufwerksbuchstaben auf dem virtuellen Desktop zugeordneten, wenn Benutzer sich anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt. Verwenden Sie die Einstellung **Clientwechseldatenträger**, um die Clientlaufwerkzuordnung zu konfigurieren. Diese Einstellung befindet sich im Bereich Dateiumleitung der ICA-Richtlinieneinstellungen.

Für USB-Massenspeichergeräte können Sie die Clientlaufwerkzuordnung, die generische USB-Umleitung oder beides verwenden. Die Steuerung erfolgt über Citrix Richtlinien. Die Hauptunterschiede sind folgende:

| Feature | Clientlaufwerkzuordnung | Generische USB-Umleitung |
|---|---|---|
| Diese Option ist in der Standardeinstellung aktiviert. | Ja | Nein |
| Konfigurierbare Leserechte | Ja | Nein |
| Verschlüsselter Gerätezugriff | Ja, wenn die Verschlüsselung vor dem Zugriff auf das Gerät entsperrt wird | Ja |
| BitLocker To Go-Geräte | Nein | Nein |
| Sicheres Entfernen des Geräts in einer Sitzung | Nein | Ja, unter der Voraussetzung, dass Benutzer den Empfehlungen des Betriebssystems zum sicheren Entfernen von Geräten folgen. |

Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der Clientlaufwerkzuordnung umgeleitet. Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind, für ein Gerät die automatische Umleitung konfiguriert wurde und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der generischen USB-Umleitung umgeleitet. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123015.

> **Hinweis:**
>
> Die USB-Umleitung wird für Verbindungen mit geringer Bandbreite (z. B. 50 KBit/s) unterstützt. Das Kopieren großer Dateien funktioniert jedoch nicht.

## Verwalten

April 19, 2022

Citrix verwaltet Citrix Virtual Apps and Desktops-Bereitstellungen, indem die Kernkomponenten und Hauptfeatures in Citrix Cloud installiert und gewartet werden.

Sie kümmern sich um die Maschinen (VDAs) an Ressourcenstandorten, mit denen Apps und Desktops bereitgestellt werden. Sie verwalten außerdem Verbindungen zu diesen Ressourcenstandorten sowie die Apps, Desktops und Benutzer.

- **Autoscale:** Feature zur konsistenten und proaktiven Verwaltung Ihrer Maschinen.
- **Anwendungen:** Sie verwalten Anwendungen in Bereitstellungsgruppen.
- **Virtuelle IP-Adresse und virtuelles Loopback:** Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugewiesene IP-Adresse für jede Sitzung bereit. Mit dem virtuellen Loopback von Citrix können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).
- **VDA-Registrierung:** Bevor ein VDA die Bereitstellung von Anwendungen und Desktops unterstützen kann, muss er bei einem Cloud Connector registriert werden (die Kommunikation herstellen). Sie können Cloud Connector-Adressen mit verschiedenen Methoden angeben, die in diesem Artikel beschrieben werden. Wenn Sie Cloud Connectors hinzufügen, müssen VDAs aktuelle Informationen haben.
- **Sitzungen:** Aufrechterhalten der Sitzungsaktivität ist wichtig für die beste Benutzererfahrung. Mit diversen Features können Sie die Sitzungszuverlässigkeit optimieren und damit das Risiko von Problemen, Ausfallzeiten und Produktivitätsverlusten verringern.
- **Suche:** Verwenden Sie die flexible Suchfunktion, um Maschinen, Sitzungen, Maschinenkataloge, Anwendungen oder Bereitstellungsgruppen in der Verwaltungsoberfläche "Vollständige Konfiguration"zu finden.
- **IPv6 und IPv4:** Citrix Virtual Apps and Desktops unterstützt reines IPv4, reines IPv6 und duale Stapelbereitstellungen, die überlappende IPv4- und IPv6-Netzwerke verwenden. Dieser Artikel beschreibt und veranschaulicht diese Bereitstellungen. Außerdem werden die Citrix Richtlinieneinstellungen vorgestellt, mit denen die Verwendung von IPv4 bzw. IPv6 gesteuert wird.
- **Profilverwaltung:** Standardmäßig kann die Citrix Profilverwaltung automatisch bei der Installation eines VDA installiert werden. Wenn Sie diese Benutzerprofillösung verwenden, beachten Sie die Dokumentation.
- **Citrix Insight Services:** Citrix Insight Services (CIS) ist eine Plattform von Citrix für Instrumentierung, Telemetrie und das Generieren von Unternehmensinsights. Analyse- und Diagnoseinformationen werden gesammelt, wenn Sie einen VDA installieren.
- **Lokaler Hostcache:** Der lokale Hostcache ermöglicht das fortgesetzte Verbindungsbrokering, wenn ein Cloud Connector an einem Ressourcenstandort nicht mit Citrix Cloud kommunizieren kann. Skalierung, Größe und andere Überlegungen zur Konfiguration werden ebenfalls zur Verfügung gestellt.
- **Delegierte Administration:** Mit der delegierten Administration können Sie die Zugriffsberechtigungen aller Administratoren gemäß ihrer Rolle in der Organisation konfigurieren.
- **Konfigurationsprotokollierung:** Mit der Konfigurationsprotokollierung werden Konfigurationsänderungen und Administratoraktivitäten überwacht.

- **Ereignisprotokolle:** Dienste in Citrix Virtual Apps and Desktops protokollieren auftretende Ereignisse. Ereignisprotokolle können zur Überwachung und Problembehandlung verwendet werden.
- **Lizenzen:**Sie können Informationen zur Citrix Lizenznutzung für diesen Dienst über die Citrix Cloud-Konsole anzeigen.
- **Lastausgleich bei Maschinen:** Sie können den Lastausgleich von Maschinen steuern.

## Adaptiver Zugriff

June 30, 2022

In der heutigen Zeit, wo Situationen sich ständig ändern, ist die Anwendungssicherheit für Unternehmen von entscheidender Bedeutung. Mit kontextbezogenen Sicherheitsentscheidungen und aktiviertem Zugriff reduzieren Sie verbundene Risiken und ermöglichen Benutzern den Zugriff auf ihre Anwendungen.

Das Feature "Adaptiver Zugriff"schützt Anwendungen durch einen umfassenden Zero-Trust-Ansatz. Mit adaptivem Zugriff können Administratoren den Benutzerzugriff auf Apps je nach Kontext präzise und detailliert anpassen. Der Begriff "Kontext"bezieht sich hierbei auf:

- Benutzer und Gruppen (Benutzer und Benutzergruppen)
- Geräte (Desktop- oder Mobilgeräte)
- Standort (Geolocation oder Netzwerkstandort)
- Gerätestatus (Gerätestatusprüfung)
- Risiko (Benutzerrisikobewertung)

## Gerätestatus

February 21, 2024

Der Citrix Gerätestatusdienst ist eine cloudbasierte Lösung, mit deren Hilfe Administratoren bestimmte Anforderungen an Endgeräte für den Zugriff auf Citrix DaaS-Ressourcen (Citrix Virtual Apps and
Desktops) bzw. Citrix Secure Private Access-Ressourcen (SaaS- und Web-Apps oder TCP- und UDP-Apps) durchsetzen können. Für die Implementierung eines Zero-Trust-Zugriffs ist es von entscheidender Bedeutung, die Vertrauensstellung von Geräten durch Überprüfen des Gerätestatus zu ermitteln. Der Gerätestatusdienst setzt Zero-Trust-Prinzipien im Netzwerk durch, indem er das

Endgerät auf Konformität (verwaltet/BYOD und Sicherheitsstatus) überprüft, bevor der Benutzer sich anmelden kann.

Einzelheiten finden Sie unter Gerätestatus.

## Adaptive Authentifizierung

March 30, 2024

Citrix Cloud-Kunden können mit Citrix Workspace die adaptive Authentifiizierung bei Citrix DaaS bereitstellen. Die adaptive Authentifizierung ist ein Citrix Cloud-Dienst, der Kunden und Benutzern, die sich bei Citrix Workspace anmelden, eine verbesserte Authentifizierung ermöglicht. Die adaptive Authentifizierung ist ein von Citrix verwalteter und von Citrix Cloud gehosteter ADC mit verbesserten Authentifizierungsfunktionen, zum Beispiel:

- Mehrstufige Authentifizierung über verschiedene Authentifizierungsmethoden, darunter AD, RADIUS, Zertifikat, mehrere Drittanbieter-IdPs mit SAML 2.0, OAuth, OIDC, Google Captcha.
- Überprüfen von Benutzeridentität und Autorisierungsstufen basierend auf Faktoren wie Standort, Gerätestatus und Benutzergruppe.
- Kontextbezogener oder intelligenter Zugriff auf DaaS (virtualisiert) und SPA (nicht virtualisierte Ressourcen wie Web- und SaaS-Apps).
- Anpassung der Anmeldeseite

Vollständige Informationen zur adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

## Adaptiver Zugriff nach Benutzer-Netzwerkstandort

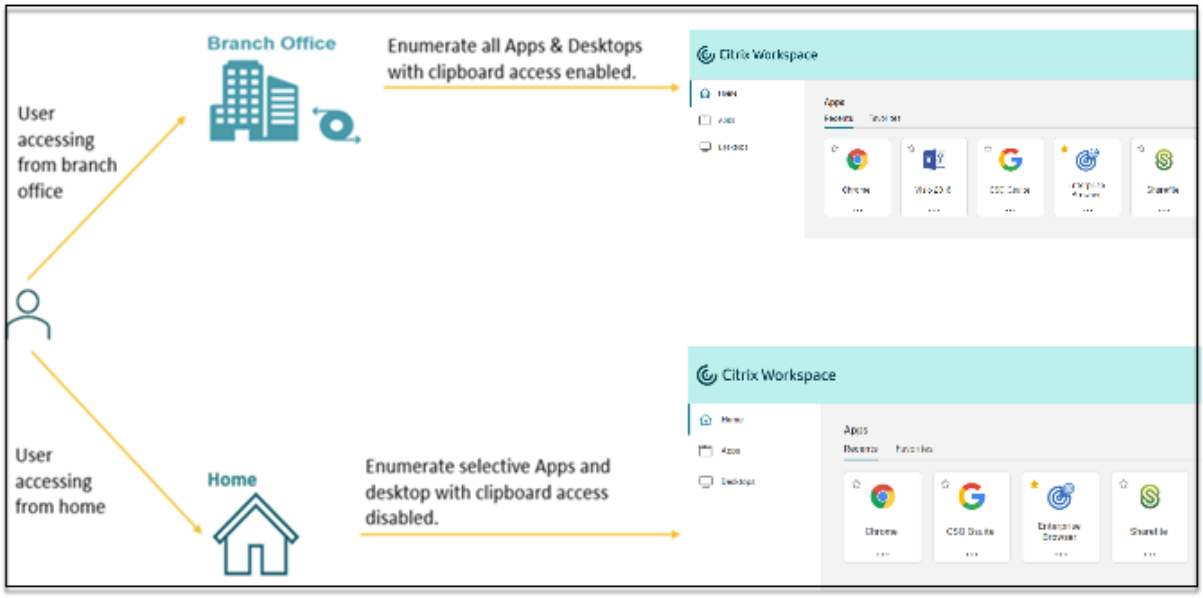
June 12, 2024

Dieses Citrix Workspace-Feature nutzt eine erweiterte Richtlinieninfrastruktur, um den adaptiven Zugriff auf Citrix DaaS basierend auf dem Netzwerkstandort des Benutzers zu ermöglichen. Der Standort wird anhand des IP-Adressbereichs oder der Subnetzadressen definiert.

Administratoren können Richtlinien definieren, um virtuelle Apps und Desktops je nach Netzwerkstandort des Benutzers aufzulisten (oder nicht). Administratoren können auch festlegen, welche Benutzeraktionen möglich sind, indem sie den Zugriff auf Zwischenablage, Drucker, Clientlaufwerkzuordnung usw. je nach Netzwerkstandort des Benutzers aktivieren oder deaktivieren. Beispielsweise können

Administratoren eine Richtlinie einrichten, dass Benutzer, die von zu Hause aus auf Ressourcen zugreifen, eingeschränkten Zugriff auf Anwendungen haben, während Benutzer, die vom Büro aus zugreifen, vollen Zugriff haben.




Ein Administrator kann die folgenden Richtlinien für den Zugriff auf Anwendungen implementieren:

- Auflisten einiger vertraulicher Anwendungen nur vom Unternehmensstandort aus oder auch von Zweigstellen.
- Kein Auflisten vertraulicher Anwendungen, wenn Mitarbeiter von einem externen Netzwerk aus auf den Workspace zugreifen.
- Deaktivieren des Druckerzugriffs von den Zweigstellen aus.
- Deaktivieren des Zugriffs auf die Zwischenablage und den Drucker, wenn Benutzer sich außerhalb des Unternehmensnetzwerks befinden.

### Ansprüche

Der adaptive Zugriff ist für Kunden mit jeder der folgenden Lizenzen verfügbar.

- DaaS Premium/Premium Plus
- Secure Private Access Advanced

### Voraussetzungen

- Stellen Sie sicher, dass **Adaptiver Zugriff** aktiviert ist (**Citrix Workspace > Zugriff > Adaptiver Zugriff**). Einzelheiten siehe Adaptiven Zugriff aktivieren.

Wenn der adaptive Zugriff aktiviert wird, werden die DaaS-Zugriffsrichtlinien zur Verwendung der Option **Über Citrix Gateway hergestellte Verbindungen** aktualisiert.

> **Hinweis:**
>
> NetScaler Gateway ist erforderlich, um Smart Access-Tags in DaaS-Zugriffsrichtlinien hinzuzufügen. Da DaaS jedoch Tags aus den Diensten Gerätestatus, adaptiver Zugriff und adaptive Authentifizierung verwendet, ist kein konfiguriertes NetScaler Gateway erforderlich.

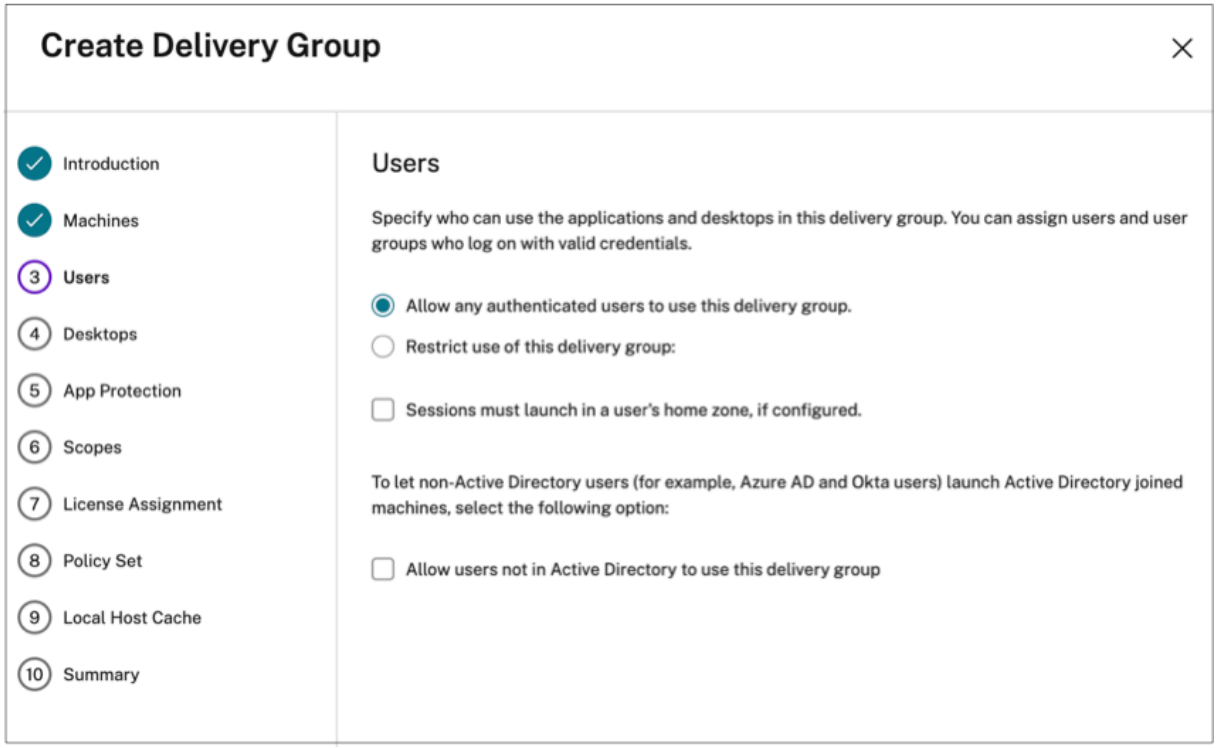
- Kenntnis der Standort-Tags. Einzelheiten siehe Netzwerkstandort-Tags.

### Wichtige Hinweise

Die folgenden Hinweise gelten nur, wenn Sie die Anzeige von Anwendungen auf der Grundlage des Standorts einschränken möchten. Wenn Sie mithilfe des adaptiven Zugriffs Steuerelemente für die Benutzer einschränken möchten (z. B. Deaktivieren des Zugriffs auf die Zwischenablage, die Druckerumleitung und die Clientlaufwerkzuweisung), können Sie diese Hinweise ignorieren.

- Wenn Sie Citrix DaaS je nach Netzwerkstandort selektiv auflisten möchten, muss die Benutzerverwaltung für diese Bereitstellungsgruppen über Citrix Studio-Richtlinien und nicht mit Workspace erfolgen. Wählen Sie beim Erstellen einer Bereitstellungsgruppe unter **Benutzereinstellung** entweder **Verwenden der Bereitstellungsgruppe auf diese Benutzer beschränken** oder **Alle authentifizierten Benutzer dürfen diese Bereitstellungsgruppe verwenden**. Dadurch können Sie den adaptiven Zugriff unter **Bereitstellungsgruppe** auf der Registerkarte **Zugriffsrichtlinie** konfigurieren.



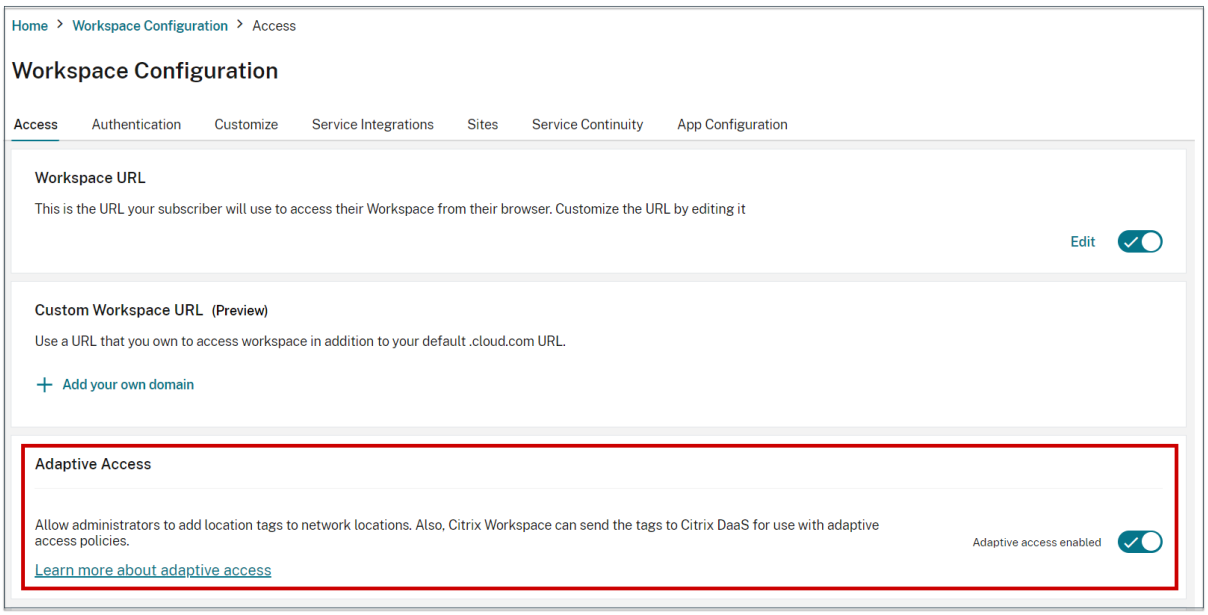

- Ändert sich zu "direkte Workloadverbindung", wenn der adaptive Zugriff aktiviert ist.
  - Das Feld **Tags für den Ort** finden Sie in **Citrix Cloud > Netzwerkstandorte > Netzwerkstandort hinzufügen > Tags für den Ort**.
  - Bestehende Richtlinien für direkte Workloadverbindung funktionieren wie vorgesehen.
  - Neue Richtlinien müssen im Netzwerkstandortdienst (ohne Definition von Tags) und für die Bereitstellungsgruppe erstellt werden. Außerdem muss der Netzwerkverbindungstyp **Intern** sein.
  - Für neue Richtlinien für die direkte Workloadverbindung mit Tags müssen Tags im Netzwerkstandortdienst und identische Tags für die Bereitstellungsgruppe oder Zugriffsrichtlinie in DaaS Studio definiert werden. Außerdem muss der Netzwerkverbindungstyp **Intern** sein. Standort-Tags sind für eine direkte Workloadverbindung nicht relevant.
- Folgendes wird für das Testen der Citrix DaaS-Bereitstellung empfohlen.
  - Identifizieren einer Testbereitstellungsgruppe oder Erstellen einer Bereitstellungsgruppe zum Implementieren dieser Funktion.
  - Erstellen einer Richtlinie oder Identifizieren einer Richtlinie, die mit einer Testbereitstellungsgruppe verwendet werden kann.

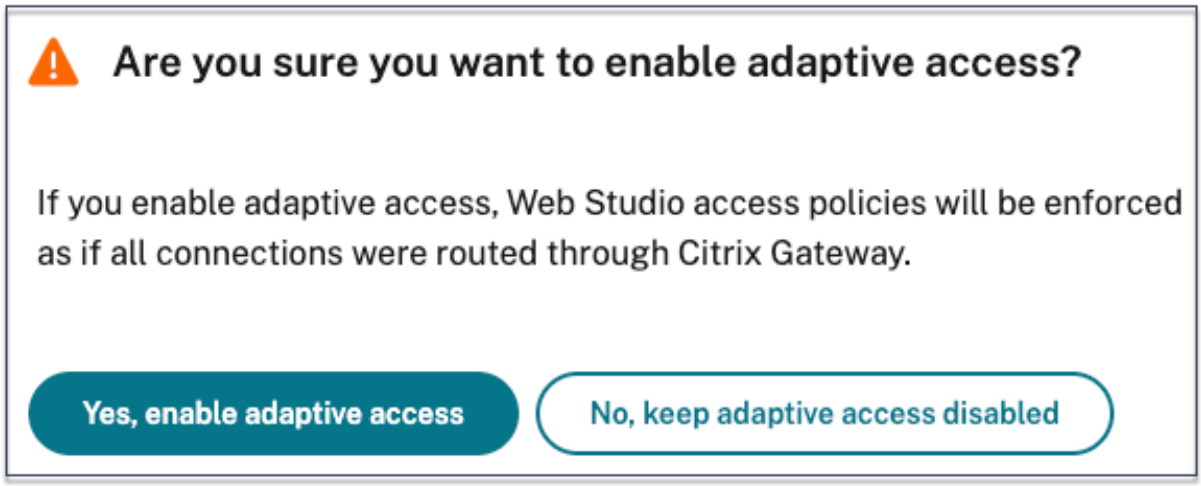
### Adaptiven Zugriff aktivieren

1. Melden Sie sich bei Citrix Cloud an.

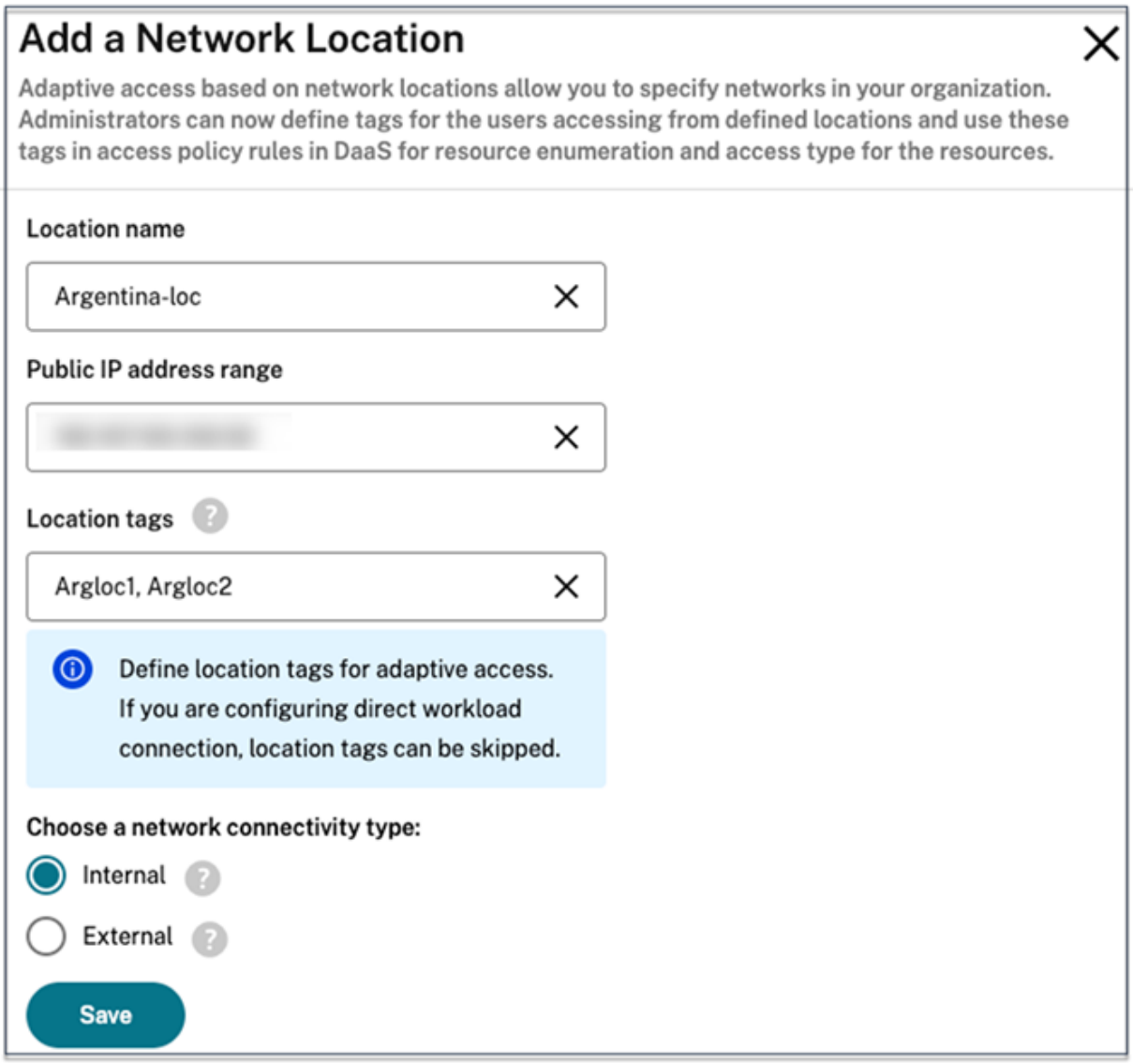
2. Wählen Sie im Hamburger-Menü die Option **Workspacekonfiguration**.
3. Der Umschalter **Adaptiver Zugriff** ist standardmäßig deaktiviert. Aktivieren Sie **Adaptiver Zugriff**.
4. Klicken Sie in der Bestätigungsmeldung auf **Ja, adaptiven Zugriff aktivieren**.



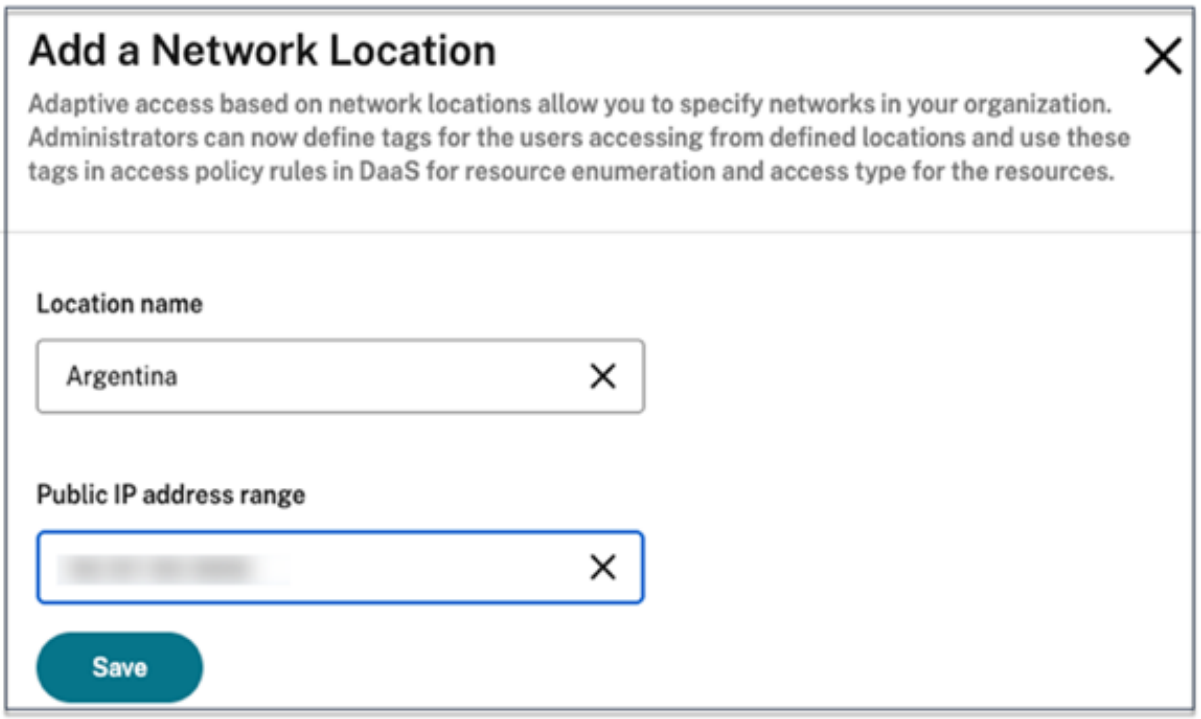

Wenn der adaptive Zugriff aktiviert ist, können Sie die Standort-Tags für den adaptiven Zugriff definieren (**Citrix Cloud > Netzwerkstandorte > Netzwerkstandort hinzufügen > Tags für den Ort**).



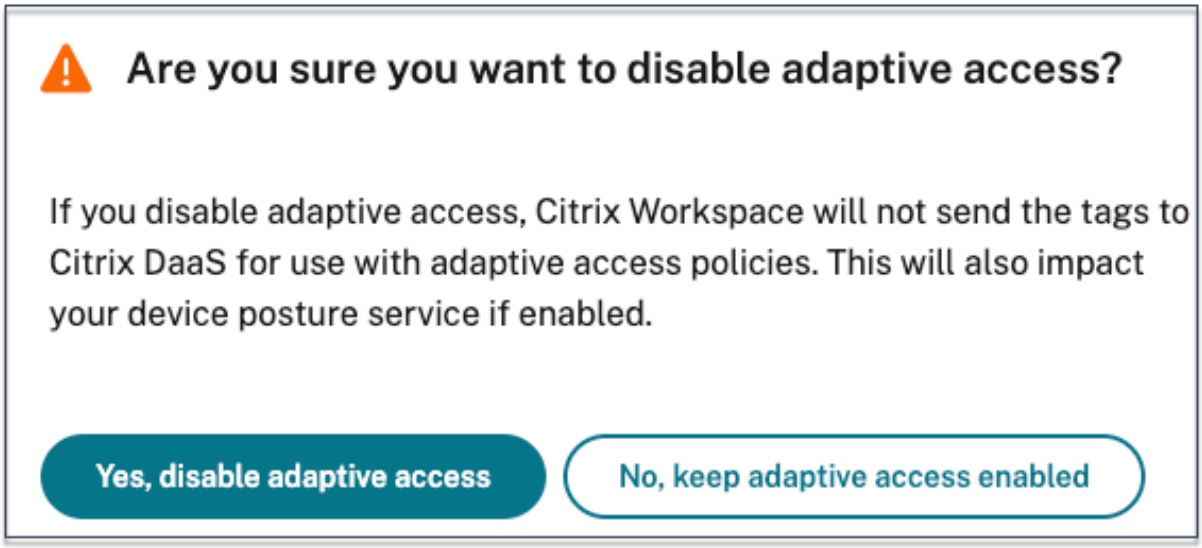

Wenn der adaptive Zugriff deaktiviert ist, können Sie keinen Netzwerkstandort hinzufügen. Standort-Tags sind in diesem Fall nicht anwendbar.




**Wichtig:**

Wenn Sie versuchen, den adaptiven Zugriff zu deaktivieren, wird die folgende Meldung angezeigt. Workspace sendet die Tags für den adaptiven Zugriff nicht an den DaaS, wenn das Feature deaktiviert ist.



## Adaptiven Zugriff konfigurieren

Die Konfiguration des adaptiven Zugriffs auf der Grundlage von Netzwerkstandorten umfasst die folgenden allgemeinen Schritte.

1. Netzwerkstandortrichtlinien definieren
2. Tags in DaaS Studio definieren

Die Erläuterung der Konfiguration erfolgt anhand der Benutzertypen **BranchOffice** und **WorkFromHome**, die ausgewählt werden, um den folgenden Anwendungsfall zu erzielen.

- BranchOffice-Benutzer müssen vollen Zugriff auf Anwendungen haben.
- WorkFromHome-Benutzer dürfen keinen Zugriff auf die Zwischenablage haben.

In diesem Konfigurationsbeispiel heißen die Tags **Home** und **Office**.

### Netzwerkstandortrichtlinien konfigurieren

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie **Netzwerkstandorte** im Hamburger-Menü.
   Stellen Sie sicher, dass der adaptive Zugriff aktiviert ist. Andernfalls wird die Benutzeroberfläche für die direkte Workloadverbindung angezeigt.
3. Klicken Sie auf **Netzwerkspeicherort hinzufügen**.

   - **Standortname:** Geben Sie einen geeigneten Namen für die Richtlinie ein.

     Beispiel: BranchOffice oder WorkFromHome

   - **Öffentlicher IP-Adressbereich:** Definieren Sie den öffentlichen IP-Adressbereich für Ihr Netzwerk.

     Beispiel: 172.9.2.1-172.9.2.30

   - **Tags für den Ort:** Definieren Sie Tags für den Standort. Dies kann ein Name sein, der sich auf Ihren Standort bezieht. Diese Tags werden verwendet, um in Citrix Studio die Richtlinien für den adaptiven Zugriff zu konfigurieren. Einzelheiten finden Sie unter **Tags in Citrix Studio definieren**.

     Beispiel: *BranchOffice* oder *WorkFromHome*

   - **Konnektivitätstyp:** Definieren Sie den Typ des Anwendungsstarts.

   **Intern:** Gateway für den Anwendungsstart umgehen.
   **Extern** Citrix Gateway-Dienst oder ein herkömmliches Gateway für den Anwendungsstart verwenden.

4. Klicken Sie auf **Speichern**.

Sie können diese Tags jetzt in DaaS Studio verwenden, um den adaptiven Zugriff zu aktivieren.

> **Hinweis:**
>
> Achten Sie bei der Definition der Standorttags darauf, dass Sie nur den bevorzugten Tagnamen ohne das Präfix "LOCATION_TAG"eingeben, zum Beispiel "BranchOffice". Bei der Definition von Tags in Citrix Studio müssen Sie dem Tagnamen jedoch "LOCATION_TAG"voranstellen. Zum Beispiel "LOCATION_TAG_BRANCHOFFICE".

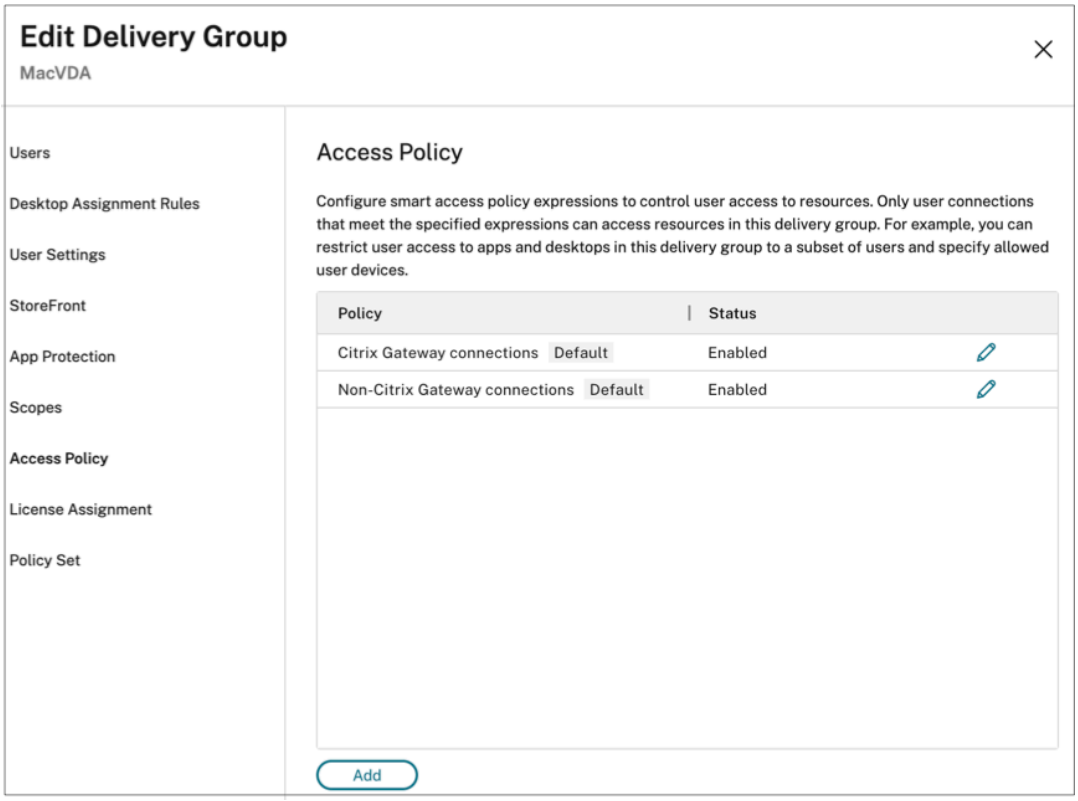
#### Tags in Citrix Studio mithilfe der GUI definieren

In diesem Beispiel werden Tags in den Bereitstellungsgruppen definiert, um die Anwendungsanzeige für Benutzer einzuschränken. Es werden zwei Bereitstellungsgruppen erstellt.

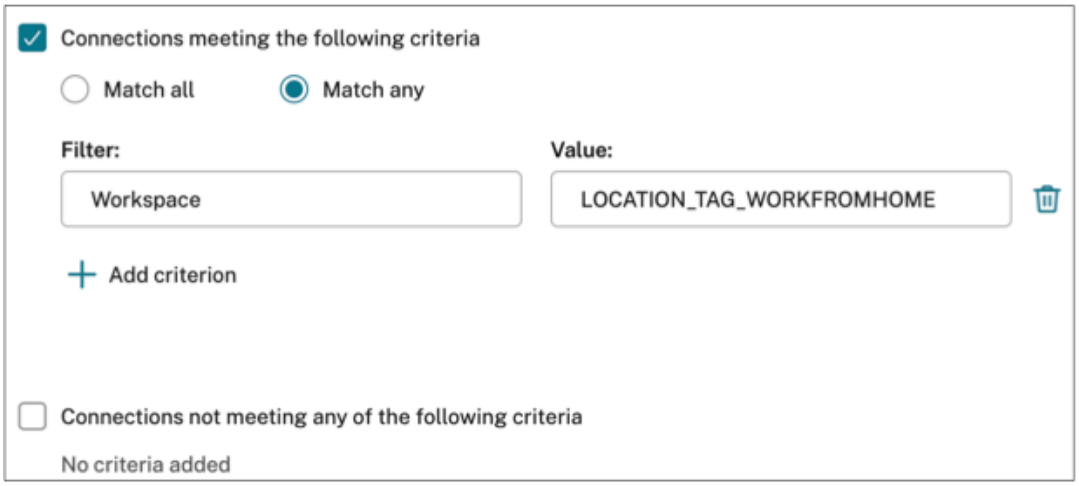
- Bereitstellungsgruppe mit adaptivem Zugriff: für die Benutzer des Standorts **BranchOffice**. Diese Benutzer müssen alle Anwendungen aus der Bereitstellungsgruppe sehen können.
- WFH-Bereitstellungsgruppe: für die Benutzer des Standorts **WorkfromHome**. Diese Benutzer müssen Anwendungen aus der Bereitstellungsgruppe sehen können.

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der **Citrix DaaS**-Kachel auf **Verwalten**.
3. Erstellen Sie eine Bereitstellungsgruppe. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.
4. Wählen Sie die von Ihnen erstellte Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellungsgruppe bearbeiten**.
5. Klicken Sie auf **Zugriffsrichtlinie**.
6. Für Kunden, die den adaptiven Zugriff in der Citrix Workspace-Plattform verwenden, können Sie für eine Bereitstellungsgruppe den Zugriff auf interne Netzwerke wie folgt beschränken:
   a) Klicken Sie mit der rechten Maustaste auf die Bereitstellungsgruppe und wählen Sie **Bearbeiten** aus.
   b) Wählen Sie im linken Bereich die Zugriffsrichtlinie aus.
   c) Klicken Sie auf das Bearbeitungssymbol, um die standardmäßige Citrix Gateway-Verbindungsrichtlinie zu ändern.




d) Wählen Sie auf der Seite **Richtlinie bearbeiten** die Option **Verbindungen, die eines der folgenden Kriterien erfüllen** und dann **Stimmt mit beliebigen dieser Elemente überein** aus und fügen Sie die Kriterien hinzu.




Geben Sie für WorkFromHome-Benutzer die folgenden Werte in den jeweiligen Delivery Controller ein.

**Farm**: Workspace

**Filter**: LOCATION_TAG_WORKFROMHOME

Geben Sie für BranchOffice-Benutzer die folgenden Werte in den jeweiligen Delivery Con-

troller ein.

**Filter**: Workspace

**Wert**: LOCATION_TAG_BRANCHOFFICE

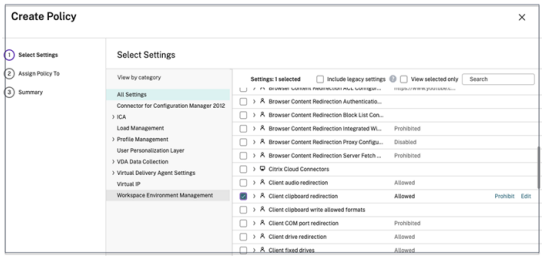
Sie können diese Tags jetzt verwenden, um den Zugriff auf Anwendungen einzuschränken.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie im Feld **Wert** den richtigen Namen für die Standortkennzeichnung eingeben, wie Sie ihn bei der Erstellung von Netzwerkstandortrichtlinien mit dem Präfix "LOCATION_TAG"definiert haben. Wenn Sie beispielsweise das Standorttag als "BranchOffice"definiert haben, müssen Sie "LOCATION_TAG_BRANCHOFFICE"in das Feld **Wert** eingeben. Einzelheiten zur Konfiguration von Standort-Tags finden Sie unter Netzwerkstandortrichtlinien konfigurieren.

### Zugriff auf Anwendungen einschränken

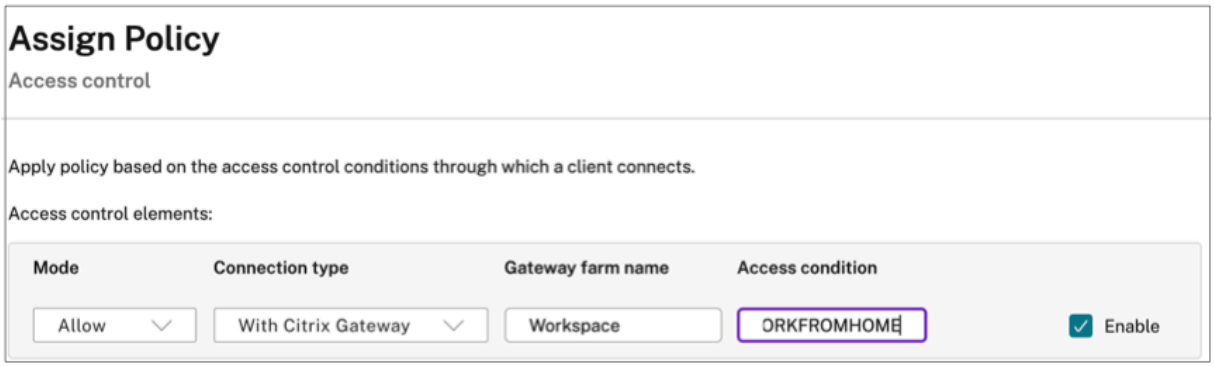
In diesem Beispiel wird die Umleitung der Clientzwischenablage für Benutzer des Standorts "WorkFromHome"deaktiviert.

1. Melden Sie sich bei Citrix DaaS an.
2. Gehen Sie zu **Richtlinien** und klicken Sie auf **Richtlinie erstellen**.
3. Wählen Sie **Clientzwischenablagenumleitung** und klicken Sie auf **Verbieten**.
4. Klicken Sie auf **Weiter**.




1. Wählen Sie auf der Seite **Richtlinie zuweisen** die Option **Zugriffssteuerung**.
2. Definieren Sie die folgenden Werte für die Richtlinie:
   - Modus: **Zulassen**
   - Verbindungstyp: **Mit Citrix Gateway**
   - Gatewayfarmname: **Workspace**
   - Zugriffsbedingung: **LOCATION_TAG_WORKFROMHOME** (alles in Großbuchstaben)




1. Klicken Sie auf **Weiter**.
2. Geben Sie einen Namen für die Richtlinie und eine Richtlinienbeschreibung ein.
3. Klicken Sie auf **Fertigstellen**.

Benutzer des Standorts **WorkFromHome** haben keinen Zugriff auf die Zwischenablage für ihre gestarteten Ressourcen.

#### Richtlinien für die Sitzungsaufzeichnung auf der Grundlage von Tags konfigurieren

Mit der Sitzungsaufzeichnung können Organisationen Benutzeraktivitäten auf dem Bildschirm in virtuellen Sitzungen aufzeichnen. Sie können Tags, einschließlich Netzwerkstandorttags, angeben, wenn Sie eine benutzerdefinierte Sitzungsaufzeichnungsrichtlinie, Ereigniserkennungsrichtlinie oder Ereignisreaktionsrichtlinie erstellen. Ein Beispiel finden Sie unter Benutzerdefinierte Aufzeichnungsrichtlinie erstellen.

### Netzwerkstandort-Tags

Der Netzwerkstandortdienst stellt die folgenden Tags bereit.

- **Standardtags:** Diese Tags sind im Netzwerkstandortdienst definiert. Die folgenden Standardtags sind verfügbar.
  - **Location_internal:** Das Tag wird standardmäßig gesendet, wenn der Netzwerkverbindungstyp auf **INTERNAL** festgelegt ist.
  - **Location_external:**Das Tag wird standardmäßig gesendet, wenn der Netzwerkverbindungstyp auf **EXTERNAL** festgelegt ist.
  - **Location_undefined:** Das Tag wird für eine IP-Adresse gesendet, die nicht in der Richtlinie definiert ist, jedoch über den Netzwerkstandortdienst zugreift. Der Start für diese Benutzer entspricht dem, was in der Ressourcengruppe definiert ist.
- **Benutzerdefinierte Tags:** Administratoren können benutzerdefinierte Tags in den Richtlinien definieren. Beispiel: office, home, branch

**Beispiele:**

Standardtags: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

Benutzerdefinierte Tags: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

> **Hinweis:**
>
> Stellen Sie beim Definieren von Tags für den Netzwerkstandortdienst Folgendes sicher:
>
> - Die Standard-Tags beginnen immer mit dem Präfix "LOCATION_<tag name>". Beispiel: LOCATION_INTERNAL.
> - Die benutzerdefinierten Tags beginnen immer mit dem Präfix "LOCATION_TAG<tag name>". Beispiel: LOCATION_TAG_OFFICE.

### Bekannte Probleme

Wenn Sie den adaptiven Zugriff deaktivieren, nachdem er aktiviert wurde und Regeln festgelegt wurden (Tags und Konnektivitätstyp), werden die Standorte nicht von der Seite "Netzwerkstandorte"entfernt. Die Spalten für die Standort-Tags und den Konnektivitätstyp sind jedoch ausgeblendet. Die Standorte sind jedoch im Back-End deaktiviert. Es handelt sich um einen Schönheitsfehler.

## App-Pakete

June 12, 2024

Es gibt verschiedene Paketierungstechnologien für die Bereitstellung von Anwendungen für Benutzer, darunter App-V, MSIX, MSIX App Attach und FlexApp. In diesem Artikel wird die Bereitstellung solcher Anwendungspakete in der Citrix DaaS-Umgebung erläutert:

- App-V-Anwendungen bereitstellen
- MSIX- und MSIX App Attach-Anwendungen bereitstellen
- FlexApp-Anwendungen bereitstellen

### App-V-Anwendungen bereitstellen

In diesem Abschnitt wird Folgendes behandelt:

- Überblick. Beschreibung der in Citrix DaaS zum Bereitstellen und Verwalten der App-V-Pakete verwendeten Methoden.
- Verfahren. Verfahren zum Bereitstellen der Pakete.

### Übersicht

In diesem Abschnitt werden die in Citrix DaaS zum Bereitstellen und Verwalten der App-V-Pakete verwendeten Methoden beschrieben. Weitere Informationen zu den Komponenten und Konzepten für die Bereitstellung von App-V-Paketanwendungen finden Sie in der Microsoft-Dokumentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Citrix DaaS verwendet zum Bereitstellen und Verwalten der App-V-Pakete die folgenden Methoden:

- **Duale Verwaltung**. Anwendungspakete werden auf App-V-Servern konfiguriert und verwaltet. Citrix DaaS- und App-V-Server arbeiten bei der Bereitstellung und Verwaltung von Paketen zusammen.

  Bei dieser Methode muss Citrix DaaS die Snapshot-Ansicht des Status des App-V-Servers regelmäßig aktualisieren. Dies ist mit Hardware-, Infrastruktur- und Verwaltungsaufwand verbunden. Citrix DaaS- und App-V-Server müssen insbesondere für die Benutzerberechtigungen immer synchronisiert bleiben.

  Duale Verwaltung funktioniert am besten in Bereitstellungen, in denen App-V und Citrix Cloud eng gekoppelt sind:

  - **App-V-Verwaltungsserver**. Veröffentlicht und verwaltet den Lebenszyklus von App-V-Paketen und dynamischen Konfigurationsdateien.
  - **Citrix Personalisierungskomponente**, die auf VDA-Maschinen installiert ist. Verwalten die Registrierung des entsprechenden App-V-Veröffentlichungsservers, der für Anwendungsstarts erforderlich ist.

  Dadurch wird sichergestellt, dass der App-V-Veröffentlichungsserver zum entsprechenden Zeitpunkt für den Benutzer synchronisiert ist. Der Veröffentlichungsserver verwaltet andere Aspekte des Paketlebenszyklus, z. B. Aktualisieren bei Anmeldung und Verbindungsgruppen.

- **Einzelverwaltung**. Anwendungspakete werden in Netzwerkfreigaben gespeichert. Citrix DaaS stellt Pakete unabhängig bereit und verwaltet sie unabhängig.

  Diese Methode reduziert den Mehraufwand, da die App-V-Server und die Datenbankinfrastruktur in der Bereitstellung nicht benötigt werden.

  Bei dieser Methode speichern Sie App-V-Pakete in einer Netzwerkfreigabe und laden deren Metadaten von diesem Speicherort in die Citrix Cloud hoch. Die auf VDA-Maschinen installierte Komponente Citrix Personalisierung verwaltet und stellt Anwendungen wie folgt bereit:

  - Verarbeiten die Bereitstellungskonfigurationsdateien und Benutzerkonfigurationsdateien, wenn eine Anwendung gestartet wird.
  - Verwalten alle Aspekte der Lebenszyklen für Pakete auf der Hostmaschine.

Sie können beide Verwaltungsmethoden parallel verwenden. Das heißt, die einer Bereitstellungsgruppe hinzugefügten Anwendungen dürfen aus App-V-Paketen stammen, die auf App-V-Servern oder in Netzwerkfreigaben vorhanden sind.

> **Hinweis:**
>
> Wenn Sie beide Verwaltungsmethoden gleichzeitig verwenden und das App-V-Paket an beiden Speicherorten eine dynamische Konfigurationsdatei hat, wird die Datei auf dem App-V-Server (duale Verwaltung) verwendet.

#### Verfahren

Zur Unterstützung der Bereitstellung von App-V-Anwendungen müssen Sie die Citrix Personalisierungskomponente auf VDA-Maschinen installieren. Weitere Informationen finden Sie unter Citrix Personalisierungskomponente auf VDA-Maschinen installieren.

Führen Sie die folgenden Schritte aus, um mit App-V verpackte Anwendungen für die Benutzer bereitzustellen:

1. Speichern Sie die Anwendungspakete in Netzwerkfreigaben.
2. Laden Sie die Anwendungspakete in Citrix Cloud hoch.
3. Fügen Sie die Anwendungen zu Bereitstellungsgruppen hinzu.
4. Erstellen Sie Isolationsgruppen, um die automatische Bereitstellung voneinander abhängiger App-V-Pakete zu aktivieren.

Informationen zur Konfiguration des Erkennens und Anwendens dynamischer App-V-Konfigurationsdateien im Einzelverwaltungsmodus in Citrix DaaS finden Sie in diesem Citrix Blog.

### MSIX- und MSIX App Attach-Anwendungen bereitstellen

In diesem Abschnitt wird Folgendes behandelt:

- Überblick. Beschreibung der Verwaltung und Bereitstellung von MSIX-Paketen und von mit dem MSIX-Feature zum Anfügen von Apps erstellten Paketen in Citrix DaaS.
- Verfahren. Verfahren zum Bereitstellen der Pakete.

#### Übersicht

Citrix DaaS stellt MSIX-Anwendungen und mit dem MSIX-Feature zum Anfügen von Apps verpackte Anwendungen über die auf VDA-Maschinen installierte Citrix Personalisierungskomponente bereit. Diese Komponente verwaltet alle Lebenszyklusaspekte der Pakete auf der Hostmaschine.

Weitere Informationen zu MSIX und zum MSIX-Feature zum Anfügen von Apps finden Sie in der Microsoft-Dokumentation unter https://docs.microsoft.com/en-us/windows/msix/ bzw. https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach.

#### Verfahren

Zur Unterstützung der Bereitstellung von MSIX-Paketen und von mit dem MSIX-Feature zum Anfügen von Apps erstellten Paketen müssen Sie die Citrix Personalisierungskomponente auf VDA-Maschinen installieren. Weitere Informationen finden Sie unter Citrix Personalisierungskomponente auf VDA-Maschinen installieren.

Führen Sie folgende Schritte aus, um MSIX-Pakete und mit dem MSIX-Feature zum Anfügen von Apps verpackte Anwendungen für Benutzer bereitzustellen:

1. Speichern Sie die Anwendungspakete in Netzwerkfreigaben.
2. Laden Sie die Anwendungspakete in Citrix Cloud hoch.
3. Fügen Sie die Anwendungen zu Bereitstellungsgruppen hinzu.

### FlexApp-Anwendungen bereitstellen

In diesem Abschnitt wird Folgendes behandelt:

- Überblick. Beschreibt, wie Citrix DaaS die FlexApp-Pakete bereitstellt und verwaltet.
- Verfahren. Verfahren zum Bereitstellen der Pakete.

#### Übersicht

Citrix DaaS stellt Benutzern FlexApp-Anwendungen über die Citrix Personalization-Komponente und den auf VDA-Maschinen installierten FlexApp Delivery Agent bereit. Diese beiden Komponenten verwalten alle Lebenszyklusaspekte der Pakete auf der Hostmaschine.

#### Verfahren

Um die Bereitstellung von FlexApp-Anwendungen zu unterstützen, müssen Sie die folgenden Komponenten auf den VDA-Maschinen installieren:

- Citrix Personalisierungskomponente auf VDA-Maschinen installieren. Weitere Informationen finden Sie unter Citrix Personalisierungskomponente auf VDA-Maschinen installieren.
- FlexApp Agent auf VDAs. Weitere Informationen finden Sie unter FlexApp Agent installieren.

Stellen Sie Ihren Benutzern FlexApp-App-Anwendungspakete zur Verfügung, indem Sie die folgenden Schritte ausführen:

1. Speichern Sie die Anwendungspakete in Netzwerkfreigaben.
2. Laden Sie die Anwendungspakete in Citrix Cloud hoch.
3. Fügen Sie die Anwendungen zu Bereitstellungsgruppen hinzu.

### Citrix Personalisierungskomponente auf VDA-Maschinen installieren

Die Citrix Personalisierungskomponente verwaltet die Veröffentlichung von Anwendungspaketen im App-V-, MSIX- und FlexApp-Format sowie von mit dem MSIX-Feature zum Anfügen von Apps erstellen Paketen. Die Komponente wird bei der Installation eines VDA nicht standardmäßig installiert. Sie können die Komponente während oder nach der VDA-Installation installieren.

Verwenden Sie eine der folgenden Methoden, um die Komponente während der VDA-Installation zu installieren:

- Wechseln Sie im Installationsassistenten zur Seite **Zusätzliche Komponenten**, und aktivieren Sie dann das Kontrollkästchen **Citrix Personalisierung für App-V - VDA**.
- Verwenden Sie in der Befehlszeilenschnittstelle die Option **/includeadditional "Citrix Personalisierung für App-V - VDA"**.

Gehen Sie folgendermaßen vor, um die Komponente nach der VDA-Installation zu installieren:

1. Wechseln Sie auf der VDA-Maschine zu **Systemsteuerung > Programme > Programme und Funktionen**, klicken Sie mit der rechten Maustaste auf **Citrix Virtual Delivery Agent**, und wählen Sie dann **Ändern** aus.
2. Wechseln Sie im angezeigten Assistenten zur Seite **Zusätzliche Komponenten**, und aktivieren Sie dann das Kontrollkästchen **Citrix Personalisierung für App-V - VDA**.

> **Hinweis:**
>
> Microsoft App-V Desktop Client ist die Komponente, die virtuelle Anwendungen aus App-V-Paketen auf Benutzergeräten ausführt. Windows 10 (1607 oder höher), Windows Server 2016 und Windows Server 2019 enthalten diese App-V-Clientsoftware bereits. Sie müssen sie nur auf VDA-Maschinen aktivieren. Weitere Informationen finden Sie in folgendem Artikel der Microsoft-Dokumentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

### Anwendungspakete in Netzwerkfreigaben speichern

Nach dem Einrichten der Infrastruktur generieren Sie die Anwendungspakete und speichern sie an einem Netzwerkspeicherort, z. B. in einer UNC- oder SMB-Netzwerkfreigabe oder einer

Azure-Dateifreigabe.

Verfahren:

1. Generieren Sie Anwendungspakete. Weitere Informationen hierzu finden Sie in der Microsoft Dokumentation.
2. Speichern Sie Anwendungspakete an einem Netzwerkspeicherort:
    - **App-V-Einzelverwaltung:** Speichern Sie die Pakete und die dazugehörigen dynamischen Konfigurationsdateien (App-V) in einer UNC- oder SMB-Netzwerkfreigabe oder einer Azure-Dateifreigabe.
    - **App-V-Dualverwaltung:** Veröffentlichen Sie die Pakete auf dem App-V-Verwaltungsserver über einen UNC-Pfad. (Die Veröffentlichung über HTTP-URLs wird nicht unterstützt.)
    - **MSIX-Pakete und mit dem MSIX-Feature zum Anfügen von Apps erstellte Pakete**: Speichern Sie die Pakete in einer UNC- oder SMB-Netzwerkfreigabe oder einer Azure-Dateifreigabe.
    - **FlexApp**: Speichern Sie die Pakete in einer UNC- oder SMB-Netzwerkfreigabe oder in einer Azure-Dateifreigabe.
3. Stellen Sie sicher, dass der VDA über Leseberechtigung für den Paketspeicherpfad verfügt:
    - Wenn Sie Pakete in einer UNC- oder SMB-Netzwerkfreigabe in Ihrer AD-Domäne speichern, erteilen Sie der VDA-Maschine die Leseberechtigung für den Speicherpfad. Dazu können Sie dem AD-Konto der Maschine explizit die Leseberechtigung für die Freigabe erteilen oder das Konto einer AD-Gruppe hinzufügen, die über diese Berechtigung verfügt.
    - Wenn Sie Pakete in einer Azure-Dateifreigabe speichern, erteilen Sie zunächst einem Benutzerkonto die Leseberechtigung für den Speicherpfad in Azure. Konfigurieren Sie als Nächstes `ctxAppVService` auf der VDA-Maschine so, dass es dieses Benutzerkonto für den Zugriff auf den Paketspeicherpfad verwendet. Die dafür erforderliche Schrittfolge ist im folgenden Abschnitt beschrieben.

#### Ändern des Benutzeranmeldekontos

Der VDA ruft `ctxAppVService` auf, um auf Paketspeicherpfade zuzugreifen. Standardmäßig greift `ctxAppVService` mit dem **lokalen Systemkonto** der Maschine auf Paketspeicherpfade zu. Diese Art der Maschinenauthentifizierung funktioniert in AD-Domänen. Sie funktioniert jedoch nicht in Szenarios mit AD- und Azure AD-Integration, die eine auf Benutzerkonten basierende Authentifizierung erfordern.

Wenn Sie Pakete in einer Azure-Dateifreigabe speichern, ändern Sie das Anmeldekonto für `ctxAppVService` in ein Benutzerkonto, das über Leseberechtigung für den Paketspeicherpfad verfügt. Verfahren:

1. Starten Sie **Dienste**, klicken Sie mit der rechten Maustaste auf **ctxAppVService**, und wählen Sie dann **Eigenschaften** aus.
2. Wählen Sie auf der Registerkarte **Anmelden** die Option **Dieses Konto** aus, geben Sie ein Benutzerkonto mit Leseberechtigung für den Paketspeicherpfad ein, und geben Sie dann das Kennwort des Benutzers zweimal ein.
3. Klicken Sie auf **OK**.

## Hochladen von Anwendungspaketen in Citrix Cloud

Laden Sie die Anwendungspakete nach dem Speichern an einem Netzwerkspeicherort zur Bereitstellung in Citrix Cloud hoch. Verwenden Sie nach Bedarf eine der folgenden Methoden:

- Massenupload
- Upload nacheinander

### Vorbereitungen

Citrix DaaS verwendet eine VDA-Maschine, um die Verbindung zum Netzwerkspeicherort für die Paketdiscovery einzurichten. Erstellen Sie daher vorher eine Bereitstellungsgruppe und stellen Sie sicher, dass mindestens ein VDA in der Gruppe die folgenden Anforderungen erfüllt:

- VDA-Version:
  - Ermitteln von App-V-Paketen: 2203 oder später
  - Ermitteln von MSIX-Paketen und von Paketen, die mit dem MSIX-Feature zum Anfügen von Apps erstellt wurden: 2209 oder später
  - So ermitteln Sie FlexApp-Pakete: 2311 oder höher
- Citrix Personalisierung für App-V: installiert
- Berechtigung für den Paketspeicherort: Lesen (weitere Informationen siehe Schritt 2: Anwendungspakete in Netzwerkfreigaben speichern).
- Eingeschaltet: ja
- Zustand: registriert

### Erforderliche Rollen

Wenn Sie über die Cloudadministrator- oder Volladministratorrolle verfügen, können Sie standardmäßig Anwendungspakete in Citrix Cloud hochladen. Sie können auch benutzerdefinierte

Rollen erstellen, um die Upload-Aktionen auszuführen. In der folgenden Tabelle sind die für die App-Paketaktionen erforderlichen Berechtigungen aufgeführt.

| Aktion | Erforderliche Berechtigung |
|---|---|
| Paket hinzufügen (Upload nacheinander) | Anwendungsdiscoverysitzungen erstellen |
| Quelle hinzufügen (Massenupload) | Anwendungsdiscoveryprofile erstellen |
| Nach Paketupdates suchen | Anwendungsdiscoverysitzungen erstellen |
| Quelle entfernen | Anwendungsdiscoveryprofile entfernen |

#### Massenupload von Anwendungspaketen

Laden Sie Pakete an einem Netzwerkspeicherort in Citrix Cloud hoch. Stellen Sie vor dem Upload sicher, dass die folgenden Elemente bereit sind:

- Eine Bereitstellungsgruppe, die die Anforderungen an die Vorbereitung erfüllt
- Der Netzwerkstandortpfad

Gehen Sie beim Massenupload von Paketen folgendermaßen vor:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **App-Pakete** aus.
2. Klicken Sie auf der Registerkarte **Quellen** auf die Schaltfläche **Quelle hinzufügen**. Die Seite **Quelle hinzufügen** wird angezeigt.
3. Geben Sie im Feld **Name** einen aussagekräftigen Namen für die Quelle des Pakets ein.
4. Klicken Sie im Feld **Bereitstellungsgruppe** auf **Bereitstellungsgruppe wählen**. Wählen Sie als Nächstes eine Bereitstellungsgruppe aus, die die unter Vorbereitung angegebenen Anforderungen erfüllt, und klicken Sie dann auf **OK**.
5. Wählen Sie im Feld **Standorttyp** die Option **Microsoft App-V-Server** oder **Netzwerkfreigabe** aus, je nachdem, wo Sie die Pakete speichern, und legen Sie dann die entsprechenden Einstellungen fest:
   - Geben Sie bei Auswahl von **Microsoft App-V-Server** die folgenden Informationen ein:
     - URL des Verwaltungsservers. Beispiel:`http://appv-server.example.com`
     - Anmeldeinformationen des Verwaltungsserveradministrators.
     - URL und Portnummer des Veröffentlichungsservers. Beispiel:`http://appv-server.example.com:3330`
   - Wenn Sie **Netzwerkfreigabe** ausgewählt haben, geben Sie die folgenden Informationen an:

- Geben Sie den UNC-Pfad der Netzwerkfreigabe ein. Beispiel:`\\Package-Server\apps\`
- Wählen Sie die Typen der Pakete aus, die Sie hochladen möchten. Es stehen die Optionen App-V, MSIX, MSIX App Attach und FlexApp zur Verfügung.
- Geben Sie an, ob Unterordner nach Paketen durchsucht werden sollen.

6. Klicken Sie auf **Quelle hinzufügen**.

   Die Seite "Quelle hinzufügen"wird geschlossen und die neu hinzugefügte Quelle wird in der Liste der Quellen angezeigt. Citrix DaaS lädt die Pakete über einen VDA in der Bereitstellungsgruppe in Citrix Cloud hoch. Nach Abschluss des Uploads wird im Statusfeld *Import war erfolgreich* angezeigt. Die entsprechenden Pakete werden auf der Registerkarte **Pakete** angezeigt.

   > **Hinweis:**
   >
   > Um an einem Quellspeicherort nach Paketupdates zu suchen und diese in Citrix Cloud zu importieren, wählen Sie den Speicherort in der Quellliste aus, und klicken Sie auf **Nach Paketupdates suchen**.

#### Upload von Anwendungspaketen nacheinander

Laden Sie ein Anwendungspaket aus einer Netzwerkfreigabe in Citrix Cloud hoch. Stellen Sie vor dem Upload sicher, dass die folgenden Elemente bereit sind:

- Eine Bereitstellungsgruppe, die die unter Vorbereitung angegebenen Anforderungen erfüllt
- Der Netzwerkstandortpfad

Gehen Sie folgendermaßen vor, um ein Paket in die Citrix Cloud hochzuladen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **App-Pakete** aus.
2. Klicken Sie auf der Registerkarte **Pakete** auf die Schaltfläche **Paket hinzufügen**. Die Seite **Paket hinzufügen** wird angezeigt.
3. Klicken Sie im Feld **Bereitstellungsgruppe** auf **Bereitstellungsgruppe wählen**. Wählen Sie als Nächstes eine Bereitstellungsgruppe aus, die die unter Vorbereitung angegebenen Anforderungen erfüllt, und klicken Sie dann auf **OK**.
4. Geben Sie im Feld **Vollständiger Paketpfad** einen Pfad nach Bedarf ein:

   - Um mehrere Pakete gleichzeitig hochzuladen, geben Sie deren vollständigen Pfad durch Semikolons (`;`) getrennt ein. Beispiel:`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Um alle in einer Netzwerkfreigabe vorhandenen Pakete hochzuladen, geben Sie den Speicherpfad ein. Beispiel: \package-Server\apps\

5. Klicken Sie auf **Paket hinzufügen**.

   Das Anwendungspaket wird auf der Registerkarte **Pakete** angezeigt.

### Anwendungen zu Bereitstellungsgruppen hinzufügen

Fügen Sie die Anwendungen nach dem vollständigen Upload eines Anwendungspakets nach Bedarf einer oder mehreren Bereitstellungsgruppen hinzu. Benutzer, die diesen Bereitstellungsgruppen zugeordnet sind, können dann auf die Anwendungen zugreifen.

> **Hinweis:**
>
> - Sie können Anwendungspakete über Bereitstellungsgruppen auf Einzelsitzungs-VDAs und Mehrsitzungs-VDAs bereitstellen.
> - Standardmäßig haben Endbenutzer Zugriff auf alle Anwendungspakete, die den Bereitstellungsgruppen zugewiesen sind, die ihren *Einzelsitzungs*-VDAs (oder sogenannten *Desktop*-)VDAs zugeordnet sind. Um die Sichtbarkeit einer verpackten Anwendung auf *Desktop*-VDAs auf bestimmte Benutzer oder Gruppen einzuschränken, wechseln Sie zum Knoten **Anwendungen**, wählen Sie die Anwendung aus und wählen Sie dann **Anwendungseigenschaften bearbeiten > Sichtbarkeit einschränken** aus, um Änderungen vorzunehmen.

Gehen Sie folgendermaßen vor, um eine oder mehrere Anwendungen in einem Paket mehreren Bereitstellungsgruppen hinzuzufügen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **App-Pakete** aus.
2. Wählen Sie auf der Registerkarte **Pakete** nach Bedarf ein Paket aus.
3. Klicken Sie in der Aktionsleiste auf **Anwendungen einer Bereitstellungsgruppe zuweisen**. Die Seite "Anwendungen einer Bereitstellungsgruppe zuweisen"wird angezeigt.
4. Wählen Sie nach Bedarf eine oder mehrere Anwendungen im Paket aus, und klicken Sie dann auf **Weiter**.
5. Wählen Sie in der Liste der Bereitstellungsgruppen die Gruppen aus, denen Sie die Anwendungen zuweisen möchten, und klicken Sie dann auf **Weiter**.

   > **Hinweis:**
   >
   > - Wenn Sie ein *MSIX*-Paket oder ein mit dem *MSIX-Feature zum Anfügen von Apps* erstelltes Paket ausgewählt haben, werden nur Bereitstellungsgruppen mit einer Funktionsebene ab 2106 in der Liste angezeigt.

> - Wenn Sie ein *FlexApp*-Paket ausgewählt haben, werden nur Bereitstellungsgruppen in der Liste angezeigt, deren Funktionsebene 2206 oder höher ist.

6. Klicken Sie auf **Fertigstellen**.

Gehen Sie wie folgt vor, um Anwendungen in verschiedenen Paketen mehreren Bereitstellungsgruppen hinzuzufügen:

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen**.
2. Wählen Sie auf der Registerkarte **Anwendungen** die Option **Anwendungen** hinzufügen aus.
3. Wählen Sie auf der Seite **Gruppen** je nach Bedarf eine oder mehrere Bereitstellungsgruppen aus.
4. Wählen Sie auf der Seite **Anwendungen** ein oder mehrere Anwendungspakete wie folgt aus:
   a) Klicken Sie auf **Hinzufügen** und wählen Sie dann **Anwendungspakete** aus.
   b) Wählen Sie den Typ der benötigten Paketquelle aus (z. B. App-V Single Admin). Alle Pakete dieses Typs werden angezeigt.
   c) Wählen Sie je nach Bedarf Pakete aus.
   d) Klicken Sie auf **OK** und dann auf **Weiter**.
   e) Um weitere Anwendungen eines anderen Pakettyps hinzuzufügen, wiederholen Sie die Schritte a bis d.
5. Klicken Sie auf **Fertigstellen**.

Sie können einer Bereitstellungsgruppe auch in folgenden Situationen Anwendungspakete hinzufügen:

- Beim Erstellen einer Bereitstellungsgruppe. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.
- Beim Bearbeiten vorhandener Bereitstellungsgruppen oder Anwendungsgruppen. Weitere Informationen finden Sie unter Hinzufügen von Anwendungen.

### Isolationsgruppen für App-V-Pakete erstellen (optional)

Sie können Isolationsgruppen erstellen, um die automatische Bereitstellung voneinander abhängiger App-V-Pakete zu aktivieren.

> **Hinweis:**
>
> Isolationsgruppen werden für die App-V-Einzelverwaltungsmethode unterstützt. Wenn Sie die duale Verwaltung für App-V verwenden, können Sie dasselbe Ziel erreichen, indem Sie *Verbindungsgruppen* in der Microsoft App-V-Infrastruktur erstellen. Weitere Informationen

> finden Sie in folgendem Artikel der Microsoft-Dokumentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

**Info zu Isolationsgruppen**

Eine Isolationsgruppe ist eine Sammlung voneinander abhängiger Anwendungspakete, die in derselben Windows Sandbox ausgeführt werden müssen, damit eine virtuelle Umgebung erstellt werden kann. Citrix App-V-Isolationsgruppen ähneln App-V-Verbindungsgruppen, sind jedoch nicht mit ihnen identisch. Eine Isolationsgruppe umfasst zwei Typen von Paketen:

- **Explizite** Anwendungspakete. Anwendungen mit spezifischen Lizenzanforderungen. Sie können diese Anwendungen auf einen bestimmten Kreis von Benutzern beschränken, indem Sie sie Bereitstellungsgruppen hinzufügen.
- **Automatische** Anwendungspakete. Anwendungen, die immer für alle Benutzer verfügbar sind, unabhängig davon, ob sie Bereitstellungsgruppen hinzugefügt wurden.

Beispiel: Anwendung app–a erfordert zur Ausführung JRE 1.7. Sie können eine Isolationsgruppe erstellen, die app-a (als *Explizit* gekennzeichnet) und JRE 1.7 (als *Automatisch* gekennzeichnet) enthält. Fügen Sie als Nächstes das App-V-Paket für app–a einer oder mehreren Bereitstellungsgruppen hinzu. Wenn ein Benutzer app-a startet, wird auch JRE 1.7 automatisch bereitgestellt.

Wenn ein Benutzer eine App-V-Anwendung startet, die in einer Isolationsgruppe als *Explizit* gekennzeichnet ist, überprüft Citrix DaaS die Zugriffsberechtigung des Benutzers auf die Anwendung in Bereitstellungsgruppen. Wenn der Benutzer über die Berechtigung zum Zugriff auf die Anwendung verfügt, werden dem Benutzer alle als *Automatisch* gekennzeichneten Anwendungspakete in derselben Isolationsgruppe zur Verfügung gestellt.

Die als *Automatisch* gekennzeichneten Pakete müssen Sie keiner Bereitstellungsgruppe hinzufügen. Wenn die Isolationsgruppe ein anderes *explizites* Anwendungspaket enthält, wird dieses Paket dem Benutzer nur dann zur Verfügung gestellt, wenn es sich in derselben Bereitstellungsgruppe befindet.

Weitere Informationen zu Isolationsgruppen finden Sie in diesem Citrix Blog.

**Erstellen von App-V-Isolationsgruppen** Erstellen Sie eine Isolationsgruppe und fügen Sie ihr voneinander abhängige Anwendungspakete hinzu. Verfahren:

1. Klicken Sie auf der Registerkarte **Isolationsgruppen** auf **Isolationsgruppe hinzufügen**.
2. Geben Sie einen Namen und eine Beschreibung für die Isolationsgruppe ein. Alle Anwendungspakete in Citrix Cloud werden in der Liste **Verfügbare Pakete** angezeigt.
3. Wählen Sie in der Liste **Verfügbare Pakete** nach Bedarf eine Anwendung aus, und klicken Sie dann auf den Pfeil nach rechts. Die ausgewählte Anwendung wird in der Liste **Pakete in Isolationsgruppe** angezeigt.

4. Wählen Sie im Feld **Bereitstellung** die Option **Explizit** oder **Automatisch** für die Anwendung aus.
5. Wiederholen Sie die Schritte 2—3, um weitere Pakete hinzuzufügen.
6. Um die Reihenfolge der Pakete in der Liste anzupassen, klicken Sie auf den Pfeil nach oben oder den Pfeil nach unten.
7. Klicken Sie auf **Speichern**.

> **Hinweis:**
>
> Isolationsgruppenkonfigurationen führen zur Erstellung einer App-V-Verbindungsgruppe auf dem VDA. Bereitstellungsszenarien können komplex sein, und der App-V-Client unterstützt Pakete, die sich jeweils nur in einer aktiven Verbindungsgruppe befinden. Es wird empfohlen, dasselbe Paket nicht zwei verschiedenen Isolationsgruppen hinzuzufügen, die derselben Bereitstellungsgruppe hinzugefügt werden.

## Autoscale

March 6, 2024

Autoscale ist eine leistungsstarke Lösung zur proaktiven Energieverwaltung Ihrer Maschinen. Es zielt auf eine Balance zwischen Kosten und Benutzererfahrung ab. Autoscale integriert die veraltete Smart Scale-Technologie in die Energieverwaltung der **Verwaltungskonsole**.

Autoscale ermöglicht die proaktive Energieverwaltung aller registrierten Maschinen mit Einzelsitzungs- und Multisitzungs-OS in einer Bereitstellungsgruppe.

Zu den Autoscalefeatures gehören folgende:

- Zeitplan- und Lasteinstellungen
- Dynamische Sitzungstimeouts
- Autoscale getaggte Maschinen (Cloudburst)
- Dynamische Maschinenbereitstellung
- Abmeldebenachrichtigungen für Benutzer

### Unterstützte VDA-Hostingplattformen

Autoscale unterstützt alle Plattformen, die Citrix DaaS unterstützt. Dazu gehören diverse Infrastrukturplattformen wie Citrix XenServer (früher Citrix Hypervisor), Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere und viele mehr. Eine vollständige Liste der unterstützten Plattformen finden Sie unter Systemanforderungen für Citrix DaaS.

### Unterstützte Workloads

Autoscale unterstützt Multisitzungs-OS- und Einzelsitzungs-OS-Bereitstellungsgruppen. Es gibt drei relevante Benutzeroberflächen:

- Autoscale-Benutzeroberfläche für Multisitzungs-OS-Bereitstellungsgruppen:
- Autoscale-Benutzeroberfläche für zufällige (gepoolte) Einzelsitzungs-OS-Bereitstellungsgruppen (früher "gepoolte VDI-Bereitstellungsgruppen")
- Autoscale-Benutzeroberfläche für statische Einzelsitzungs-OS-Bereitstellungsgruppen (bisher "statische VDI-Bereitstellungsgruppen")

Weitere Hinweise zu den Benutzeroberflächen für verschiedene Bereitstellungsgruppen finden Sie unter Autoscale-Benutzeroberflächen.

### Vorteile

Das Autoscale-Feature bietet folgende Vorteile:

- Konsistenter Einzelmechanismus zur Verwaltung von Maschinen in einer Bereitstellungsgruppe
- Gewährleistung der Verfügbarkeit und Kostenkontrolle durch Energieverwaltung auf der Basis der Last, eines Zeitplans oder von beidem
- Zur Überwachung von Kennzahlen wie Kosteneinsparungen und Kapazitätsauslastung und Aktivierung von Benachrichtigungen verwenden Sie **Director** auf der Registerkarte Überwachen.

### Sehen Sie sich das 2-minütige Video an

Das folgende Video bietet einen kurzen Überblick über Autoscale.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

## Erste Schritte mit Autoscale

May 12, 2023

Autoscale funktioniert auf Bereitstellungsgruppenebene. Es ermöglicht die proaktive Energieverwaltung von Maschinen in einer Bereitstellungsgruppe nach von Ihnen festgelegten Zeitplänen.

Autoscale gilt für alle Typen von Bereitstellungsgruppen:

- Einzelsitzungs-OS (statisch)

- Einzelsitzungs-OS (zufällig)
- Multisitzungs-OS (zufällig)

In diesem Artikel werden die Grundkonzepte für Autoscale beschrieben und das Aktivieren und Konfigurieren von Autoscale für eine Bereitstellungsgruppe erläutert.

## Grundkonzepte

Betrachten Sie vor dem Start die folgenden Grundkonzepte in Autoscale:

- Zeitpläne
- Kapazitätspuffer
- Lastindex

### Zeitpläne

Autoscale schaltet Maschinen in einer Bereitstellungsgruppe gemäß einem von Ihnen festgelegten Zeitplan ein und aus.

Ein Zeitplan enthält die Anzahl der aktiven Maschinen für jedes Zeitfenster, mit definierten Spitzen- und Nebenzeiten.

Zeitplaneinstellungen variieren je nach Typ der Bereitstellungsgruppe. Weitere Informationen:

- Multisitzungs-OS-Bereitstellungsgruppen
- Zufällige Einzelsitzungs-OS-Bereitstellungsgruppen
- Statische Einzelsitzungs-OS-Bereitstellungsgruppen

### Kapazitätspuffer

Der Kapazitätspuffer dient zum Vorhalten freier Kapazität zur Berücksichtigung dynamischer Laststeigerungen. Es sind zwei Szenarien zu beachten:

- Bei Multisitzungs-OS-Bereitstellungsgruppen wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Bereitstellungsgruppe in Bezug auf den Lastindex definiert.
- Bei Bereitstellungsgruppen mit Einzelsitzungs-OS wird der Kapazitätspuffer als Prozentsatz der Gesamtanzahl von Maschinen in der Bereitstellungsgruppe definiert.

### Lastindex

> **WICHTIG:**
>
> Der Lastindex gilt nur für Multisitzungs-OS-Bereitstellungsgruppen.

Der Lastindexwert legt fest, mit welcher Wahrscheinlichkeit eine Maschine Anmeldeanfragen von Benutzern empfängt. Er wird anhand der in der **Citrix Lastverwaltungsrichtlinie** konfigurierten Einstellungen für gleichzeitige Anmeldungen, Sitzungen, CPU, Datenträger und Speichernutzung berechnet.

Der Lastindex liegt zwischen 0 und 10.000. Standardmäßig gilt eine Maschine als voll ausgelastet, wenn sie 250 Sitzungen hostet.

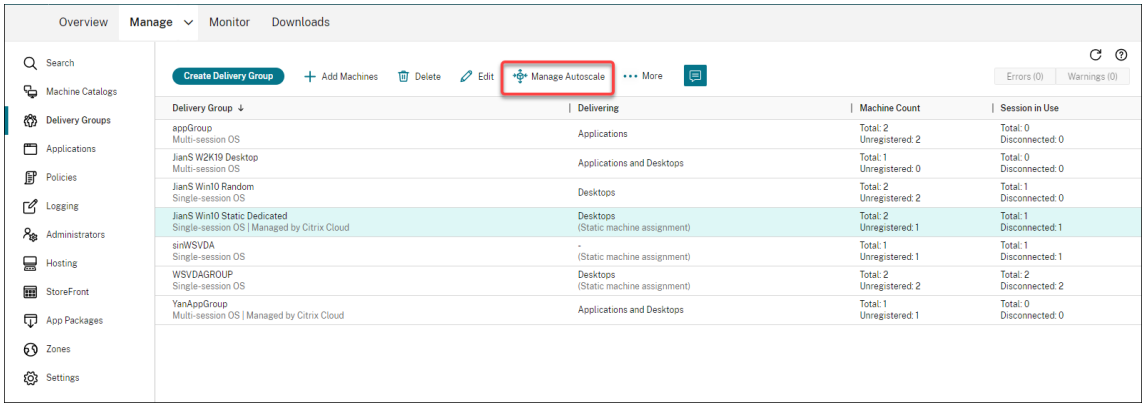
- Die Ziffer "0"bedeutet, dass eine Maschine ohne Last ist. Eine Maschine mit einem Lastindexwert von 0 befindet sich bei einer Basislast.
- Die Ziffer "10.000"bedeutet, dass eine Maschine vollständig ausgelastet ist und keine weiteren Sitzungen ausführen kann.

### Autoscale für eine Bereitstellungsgruppe aktivieren

Autoscale ist standardmäßig deaktiviert, wenn Sie eine Bereitstellungsgruppe erstellen. Führen Sie folgende Schritte aus, um Autoscale in der Oberfläche "Vollständige Konfiguration"für eine Bereitstellungsgruppe zu aktivieren und zu konfigurieren:

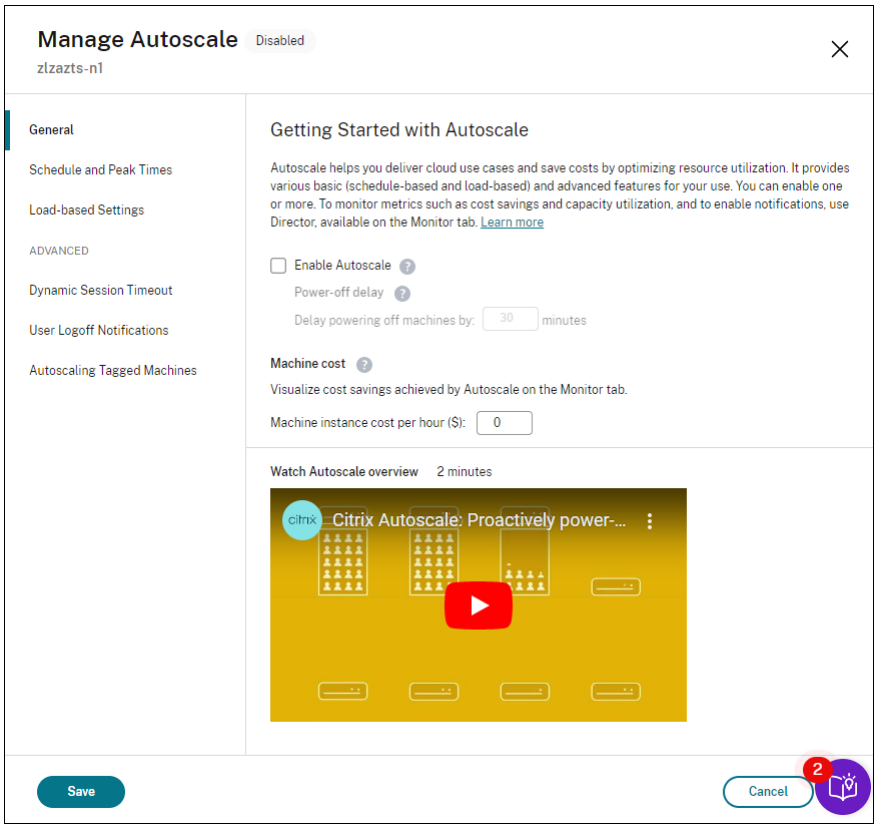
Sie können Autoscale auch mit PowerShell-Befehlen für eine Bereitstellungsgruppe aktivieren und konfigurieren. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie die Bereitstellungsgruppe aus, die Sie verwalten möchten, und klicken Sie auf **Autoscale verwalten**.



3. Aktivieren Sie auf der Seite **Autoscale verwalten** das Kontrollkästchen **Autoscale aktivieren**, um das Feature zu aktivieren. Nachdem Sie Autoscale aktiviert haben, werden die Optionen auf der Seite verfügbar.




4. Um die Standardeinstellungen an die Anforderungen Ihres Unternehmens anzupassen, führen Sie die folgenden Einstellungen aus:

   - Zeitpläne festlegen
   - Um inaktive Maschinen effektiver auszuschalten, verwenden Sie Dynamisches Sitzungstimeout und Benachrichtigungen zur Benutzerabmeldung.
   - Um die Energieverwaltung nur für einen Teil der Maschinen in der Bereitstellungsgruppe durchzuführen, verwenden Sie Autoscale getaggte Maschinen.

Zum Deaktivieren des Features deaktivieren Sie das Kontrollkästchen **Autoscale**. Die Optionen auf der Seite werden grau angezeigt, sodass zu sehen ist, dass Autoscale für die ausgewählte Bereitstellungsgruppe deaktiviert ist.

> **Wichtig:**
>
> - Wenn Sie Autoscale deaktivieren, verbleiben alle über Autoscale verwalteten Maschinen in dem zum Zeitpunkt der Deaktivierung aktiven Zustand.
> - Nachdem Sie Autoscale deaktiviert haben, werden Maschinen im Drainingzustand aus

> diesem genommen. Weitere Hinweise zum Drainingzustand finden Sie unter Drainingzustand.

Sie können Maschinen für die Gruppe dynamisch mit einem PowerShell-Skript bereitstellen. Weitere Informationen finden Sie unter Dynamische Bereitstellung von Maschinen.

### Metriken überwachen

Nachdem Sie Autoscale für eine Bereitstellungsgruppe aktiviert haben, können Sie für die mit Autoscale verwalteten Maschinen folgende Kennzahlen über die Registerkarte **Überwachen** erfassen.

- Maschinennutzung
- Geschätzte Einsparungen
- Warnmeldungsbenachrichtigungen für Maschinen und Sitzungen
- Maschinenstatus
- Lastauswertungstrends

> **Hinweis:**
>
> Wenn Sie die automatische Skalierung für eine Bereitstellungsgruppe anfänglich aktivieren, kann es einige Minuten dauern, bis Überwachungsdaten für diese Bereitstellungsgruppe angezeigt werden.
> Wird Autoscale anschließend wieder deaktiviert, sind die Überwachungsdaten weiterhin verfügbar. Autoscale erfasst Überwachungsdaten in Intervallen von 5 Minuten.

Weitere Informationen zu Metriken finden Sie unter Überwachen von mit Autoscale verwalteten Maschinen.

### Nützliche Info

Autoscale funktioniert auf Bereitstellungsgruppenebene. Es wird für einzelne Bereitstellungsgruppen konfiguriert. Autoscale verwaltet nur die Maschinen in der ausgewählten Bereitstellungsgruppe.

#### Kapazität und Maschinenregistrierung

Autoscale enthält nur Maschinen, die beim Bestimmen der Kapazität in einer Site registriert sind. Eingeschaltete Maschinen, die nicht registriert sind, können keine Sitzungsanfragen annehmen. Daher werden sie nicht in die Gesamtkapazität der Bereitstellungsgruppe einbezogen.

### Einsatz mehrerer Maschinenkataloge

Bei manchen Sites sind einer Bereitstellungsgruppe mehrere Maschinenkataloge zugeordnet. Autoscale schaltet Maschinen aus jedem Katalog nach dem Zufallsprinzip ein, um die Zeitplan- bzw. die Sitzungsanforderungen zu erfüllen.

Beispiel: Eine Bereitstellungsgruppe hat zwei Maschinenkataloge, Katalog A mit drei eingeschalteten Maschinen und Katalog B mit einer eingeschalteten Maschine. Wenn Autoscale eine weitere Maschine einschalten muss, kann es eine aus Katalog A oder Katalog B einschalten.

### Maschinenbereitstellung und Sitzungsbedarf

Der einer Bereitstellungsgruppe zugeordnete Maschinenkatalog muss über genügend Maschinen zum Ein- und Ausschalten bei steigendem und sinkendem Bedarf verfügen. Überschreitet der Sitzungsbedarf die Gesamtzahl der registrierten Maschinen in einer Bereitstellungsgruppe stellt Autoscale sicher, dass alle registrierten Maschinen eingeschaltet werden. **Autoscale stellt jedoch keine zusätzlichen Maschinen bereit.**

Um diesen Engpass zu überwinden, können Sie mit einem PowerShell-Skript Maschinen erstellen und sie dynamisch löschen. Weitere Informationen finden Sie unter Dynamische Bereitstellung von Maschinen.

### Instanzgröße

Sie können Ihre Kosten optimieren, wenn Sie die Größe Ihrer Instanzen in öffentlichen Clouds passend festlegen. Wir empfehlen die Bereitstellung kleinerer Instanzen, sofern diese Ihren Workload-, Leistungs- und Kapazitätsanforderungen entsprechen.

Kleinere Instanzen hosten weniger Benutzersitzungen als größere. Daher versetzt Autoscale Maschinen viel schneller in den Drainingzustand , da die Abmeldung der letzten Benutzersitzung schneller erfolgt. Kleinere Instanzen werden somit schneller ausgeschaltet, wodurch die Kosten gesenkt werden.

### Drainingzustand

Autoscale versucht, die Anzahl der eingeschalteten Maschinen in einer Bereitstellungsgruppe auf die konfigurierte Poolgröße und den Kapazitätspuffer zu beschränken.

Um dies zu erreichen, versetzt Autoscale die überzähligen Maschinen mit den wenigsten Sitzungen in den “Drainingzustand”und schaltet sie aus, sobald alle Sitzungen abgemeldet sind. Dies ist der Fall, wenn der Sitzungsbedarf sinkt und laut Zeitplan weniger Maschinen benötigt werden, als eingeschaltet sind.

Autoscale versetzt überzählige Maschinen nacheinander in den Drainingzustand .

- Sind auf mehren Maschinen gleich viele Sitzungen aktiv, wird die Maschine in den Drainingzustand versetzt, die für die als Ausschaltverzögerung vorgegebene Zeitdauer eingeschaltet war.

  Dadurch wird vermieden, dass kürzlich eingeschaltete Maschinen in den Drainingzustand versetzt werden, da auf ihnen am ehesten weniger Sitzungen aktiv sind.

- Waren mehre Maschinen für die als Ausschaltverzögerung vorgegebene Zeitdauer eingeschaltet, werden sie von Autoscale nach dem Zufallsprinzip einzeln in den Drainingzustand versetzt.

Maschinen im Drainingzustand nehmen keine neuen Sitzungen an und warten auf die Abmeldung bestehender Sitzungen. Es werden nur Maschinen zum Abschalten in Betracht gezogen, wenn alle Sitzungen abgemeldet sind. Stehen keine Maschinen sofort für Sitzungsstarts zur Verfügung, werden Sitzungsstarts von Autoscale bevorzugt an Maschinen im Drainingzustand weitergeleitet, anstatt neue Maschinen einzuschalten.

Eine Maschine wird aus dem Drainingzustand genommen, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Maschine ist ausgeschaltet.
- Autoscale ist für die Bereitstellungsgruppe deaktiviert, zu der die Maschine gehört.
- Autoscale verwendet die Maschine, um die Anforderungen an den Zeitplan oder den Lastbedarf zu erfüllen. Dieser Fall tritt auf, wenn der Zeitplan (planbasierte Skalierung) oder der aktuelle Bedarf (lastbasierte Skalierung) mehr Maschinen benötigt, als derzeit eingeschaltet sind.

> **Wichtig:**
>
> Stehen keine Maschinen sofort für Sitzungsstarts zur Verfügung, werden Sitzungsstarts von Autoscale bevorzugt an Maschinen im Drainingzustand weitergeleitet, anstatt neue Maschinen einzuschalten. Eine Maschine im Drainingzustand, die einen Sitzungsstart hostet, bleibt im Drainingzustand.

Mit dem PowerShell-Befehl `Get-BrokerMachine` können Sie herausfinden, welche Maschinen im Drainingzustand sind. Beispiel: `Get-BrokerMachine -DrainingUntilShutdown $true`. Alternativ können Sie die Verwaltungskonsole verwenden. Siehe Anzeigen von Maschinen im Drainingzustand.

#### Anzeigen von Maschinen im Drainingzustand

> **Hinweis:**
>
> Dieses Feature gilt nur für Multisitzungsmaschinen.

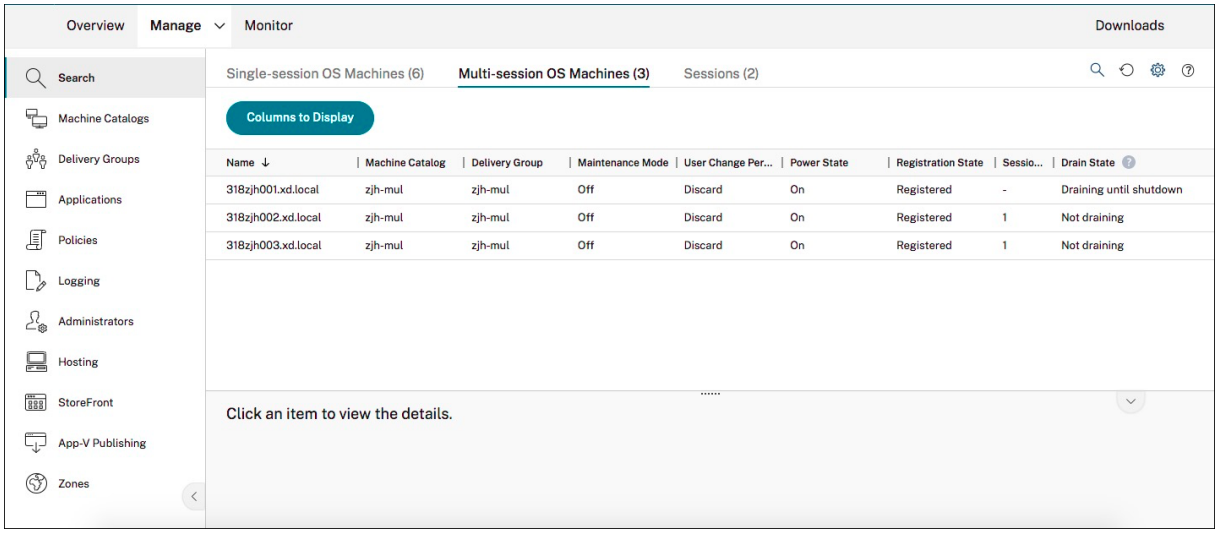
In **Verwalten > Vollständige Konfiguration** können Sie Maschinen im Drainingzustand anzeigen und sehen, welche Maschinen vor dem Herunterfahren stehen. Führen Sie hierzu die folgenden Schritte aus:

1. Navigieren Sie zum Knoten **Suchen** und klicken Sie auf **Anzuzeigende Spalten**.
2. Wählen Sie im Fenster **Anzuzeigende Spalten** das Kontrollkästchen neben **Drainingzustand**.
3. Klicken Sie auf **Speichern**, um das Fenster **Anzuzeigende Spalten** zu schließen.

Die Spalte **Drainingzustand** kann die folgenden Informationen enthalten:

- **Draining bis zum Herunterfahren:** Diese Meldung erscheint für Maschinen im Drainingzustand, bis sie heruntergefahren werden.
- **Nicht Draining:** Diese Meldung erscheint für Maschinen, die noch nicht im Draining sind.




### Weitere Informationen

Weitere Hinweise zu Autoscale finden Sie unter Citrix Autoscale auf Tech Zone.

## Zeitplan- und Lasteinstellungen

November 6, 2023

### Energieverwaltung von Maschinen durch Autoscale

Autoscale schaltet Maschinen basierend auf dem ausgewählten Zeitplan ein und aus. Über Autoscale können Sie mehrere Zeitpläne, z. B. für bestimmte Wochentage, festlegen und die Anzahl der während dieser Zeiten verfügbaren Maschinen vorgeben. Benutzergruppen, die Maschinenressourcen zu einem bestimmten Zeitpunkt an bestimmten Tagen nutzen kann mit Autoscale so eine optimales Benutzererfahrung geboten werden. Maschinen bleiben während des Zeitplans eingeschaltet, unabhängig davon, ob auf ihnen Sitzungen ausgeführt werden.

> **Hinweis:**
>
> AutoScale unterstützt jede energieverwaltete Maschine.

Der Zeitplan basiert auf der **Zeitzone** der Bereitstellungsgruppe. Zum Ändern der Zeitzone können Sie Benutzereinstellungen in einer Bereitstellungsgruppe ändern. Weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen.

Autoscale hat zwei Standardzeitpläne: *Werktage* (Montag bis Freitag) und *Wochenende* (Samstag und Sonntag). Beim Zeitplan **Werktage** ist zu Spitzenzeiten eine Maschine von 7:00 Uhr bis 18:30 Uhr und zu Nebenzeiten keine Maschine eingeschaltet. Der Standardwert für den Kapazitätspuffer ist 10 % in Spitzen- und Nebenzeiten. Beim Zeitplan **Wochenende** ist standardmäßig keine Maschine eingeschaltet.

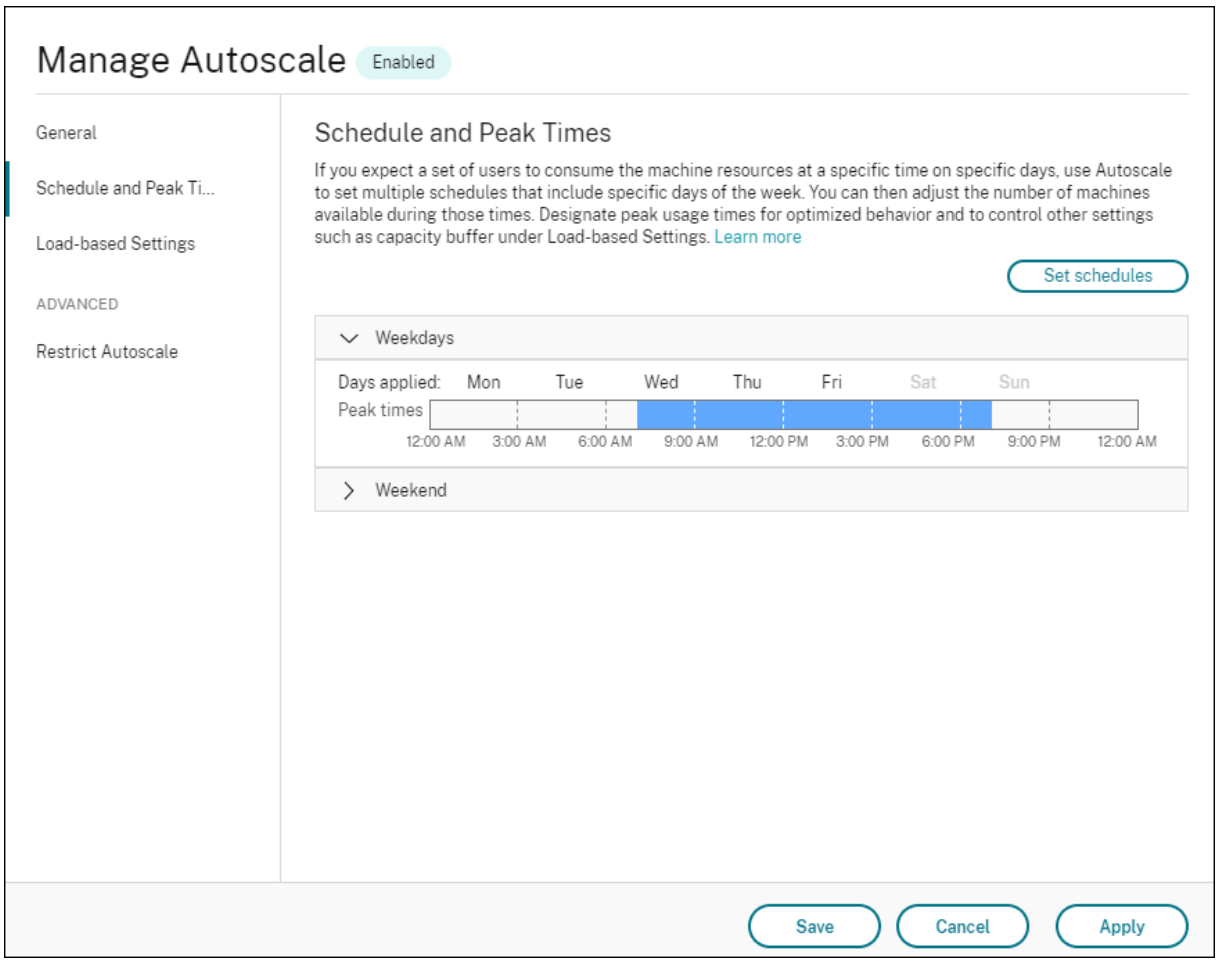
> **Hinweis:**
>
> Autoscale behandelt in seiner Kalkulation nur in der Site registrierte Maschinen als Teil der verfügbaren Kapazität. "Registriert"bedeutet, dass eine Maschine einsatzbereit oder bereits im Einsatz ist. Dadurch wird sichergestellt, dass nur Maschinen, die Benutzersitzungen annehmen können, zur Kapazität für die Bereitstellungsgruppe gezählt werden.

### Benutzeroberflächen

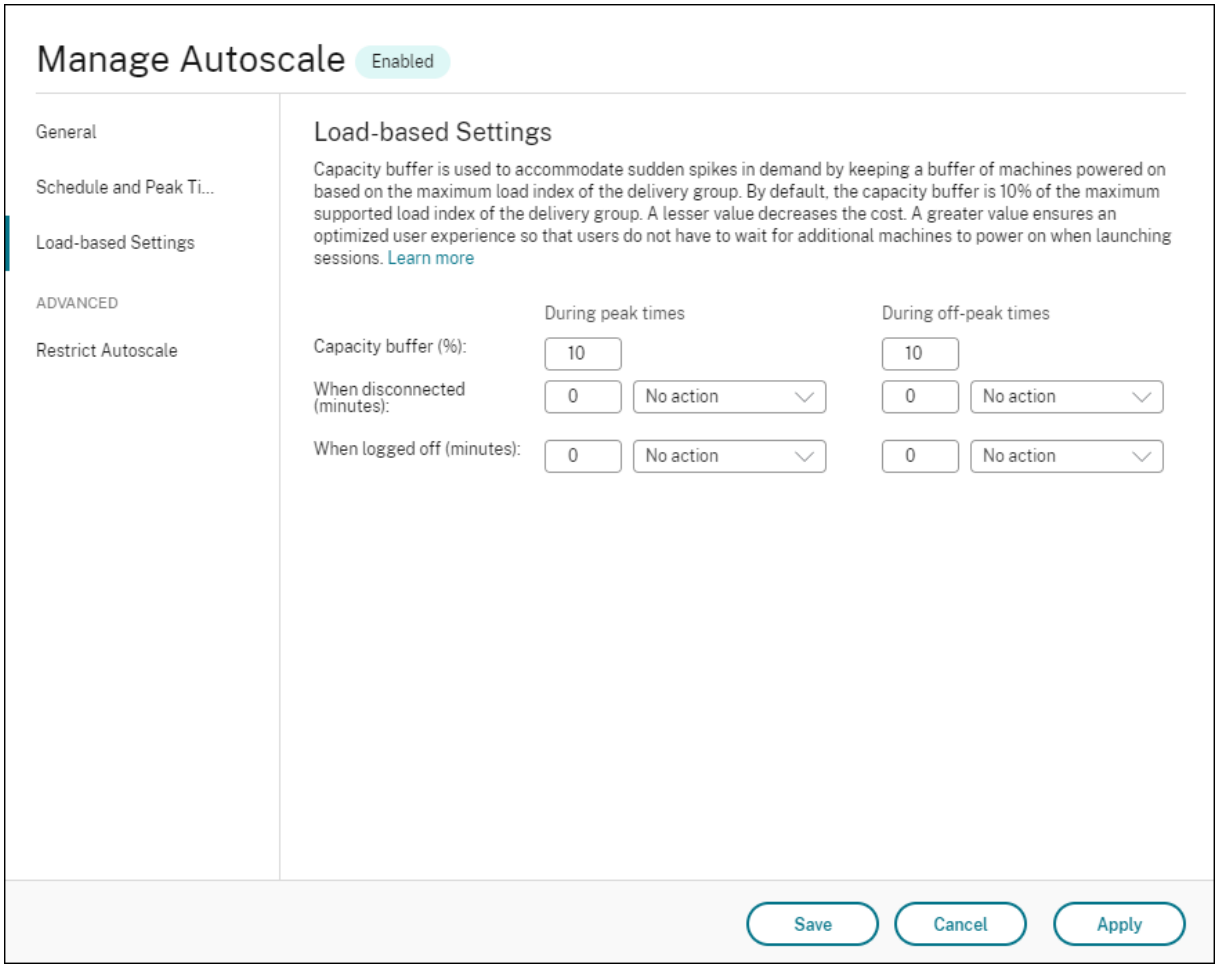
Es gibt drei Benutzeroberflächen.

Benutzeroberfläche für *statische* Einzelsitzungs-OS-Bereitstellungsgruppen:

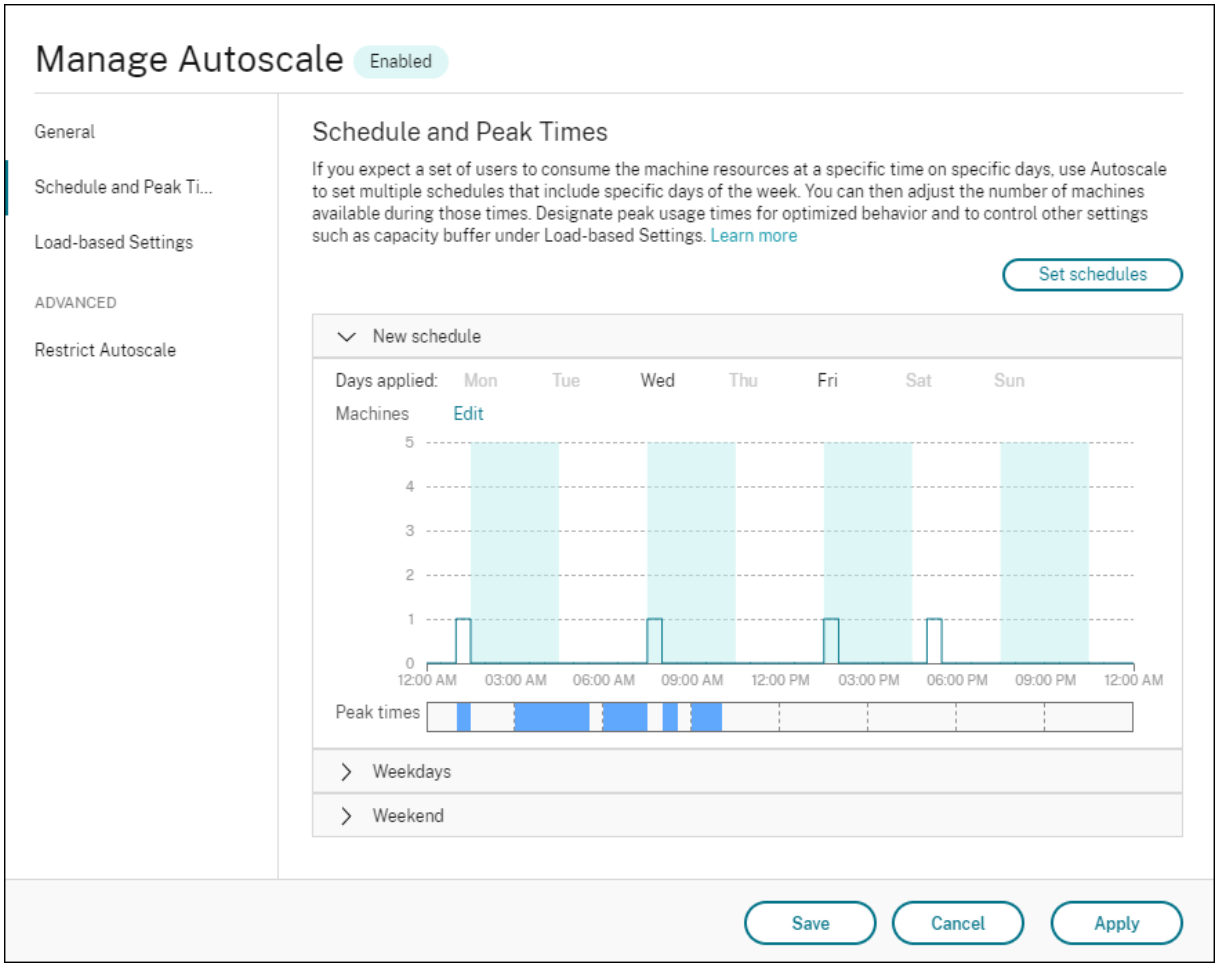


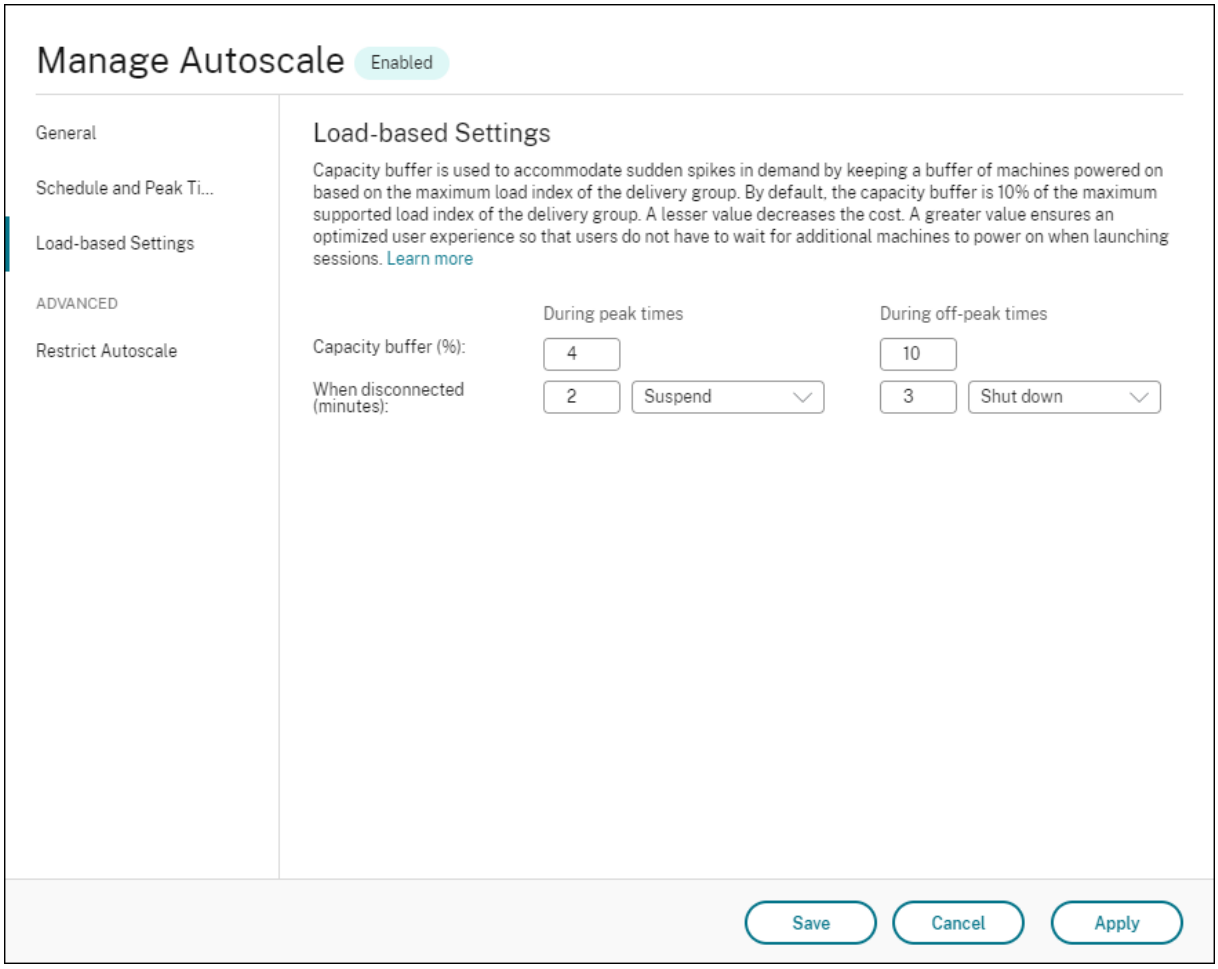



Autoscale-Benutzeroberfläche für *zufällige Einzelsitzungs-OS-Bereitstellungsgruppen*:

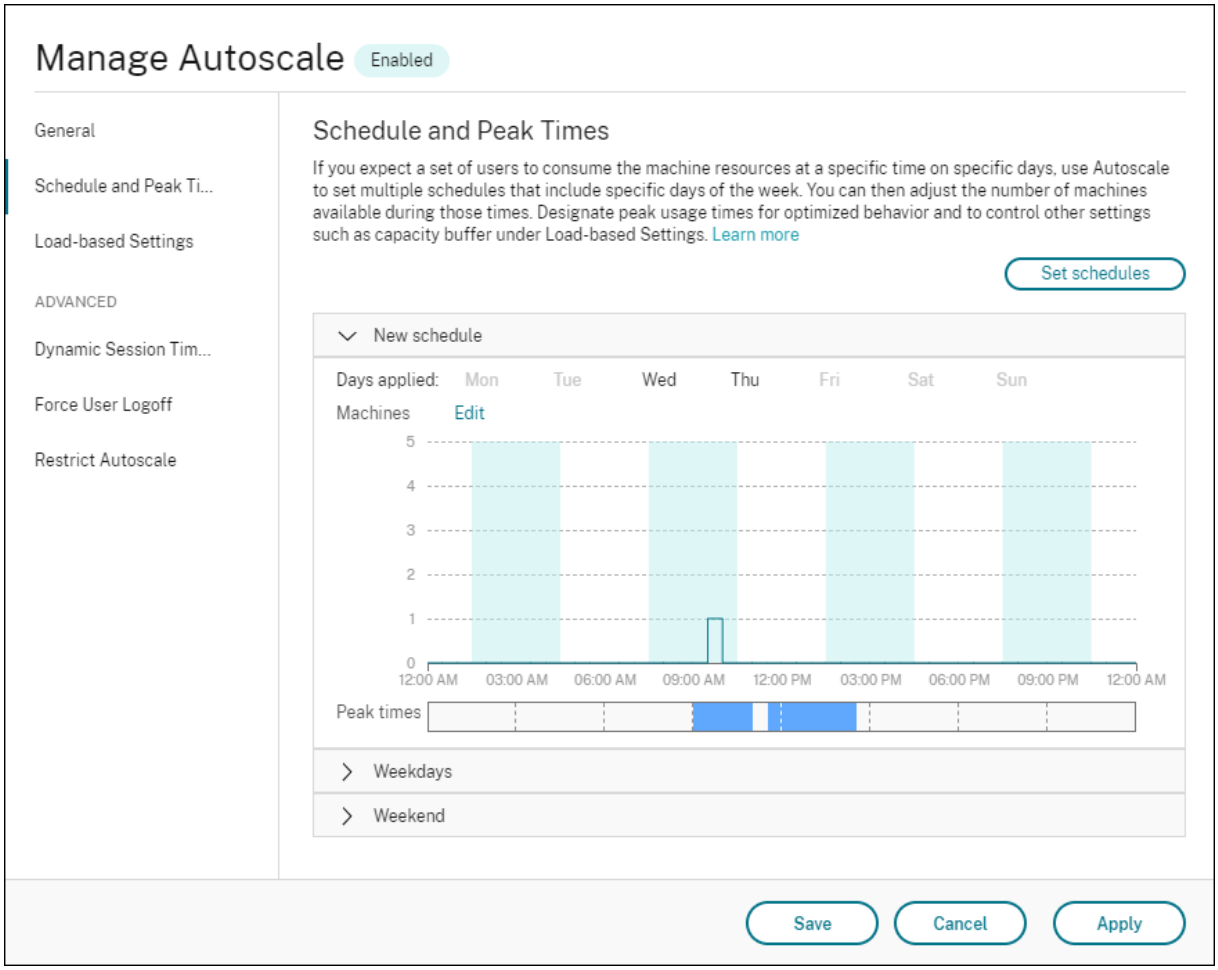


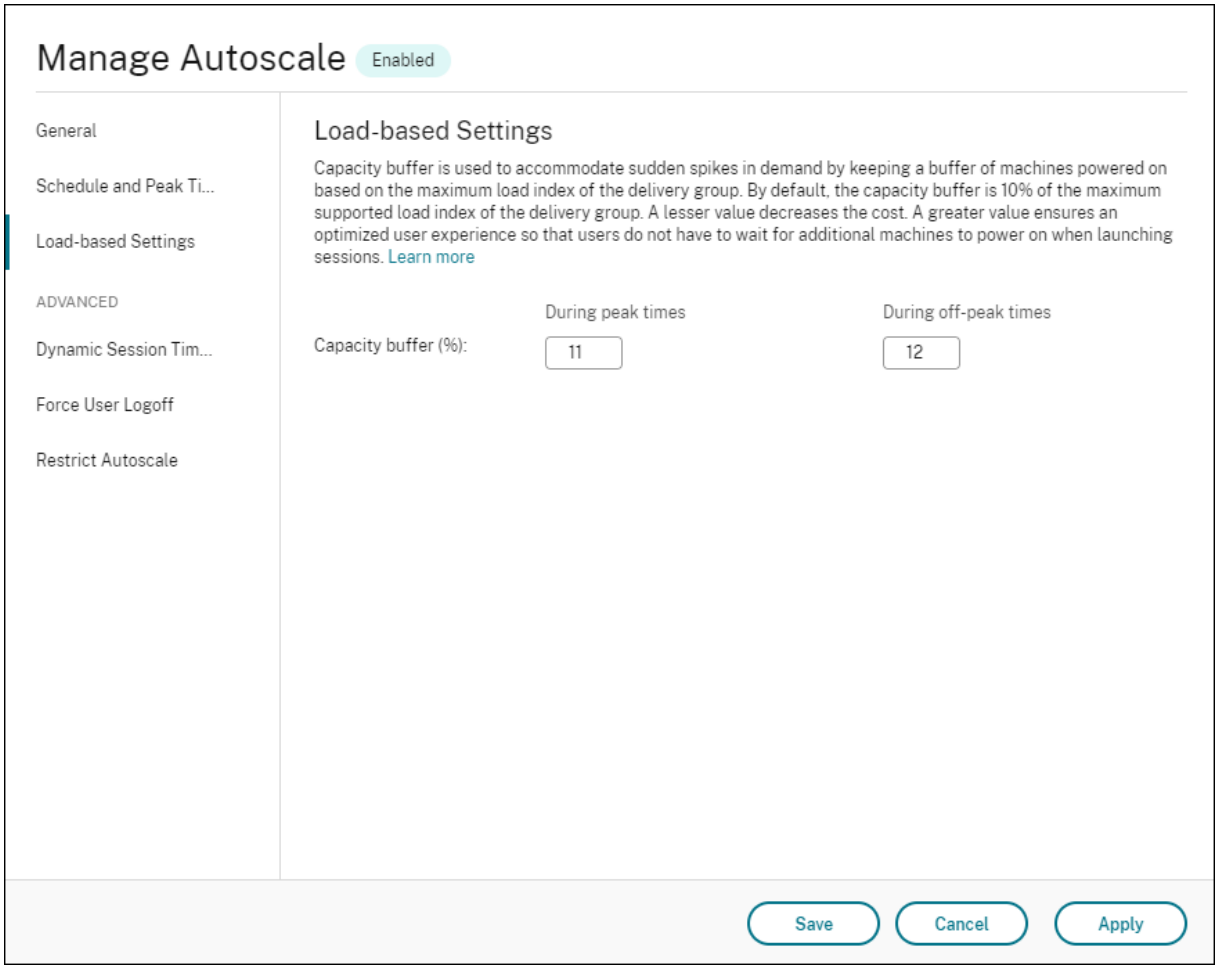



Autoscale-Benutzeroberfläche für *Multisitzungs-OS-Bereitstellungsgruppen*:






### Zeitplanbasierte Einstellungen

**Autoscale-Zeitplan:** Ermöglicht das Hinzufügen, Bearbeiten, Auswählen und Löschen von Zeitplänen.

**Angewendete Tage:** Zur Auswahl der Tage, auf die der ausgewählten Zeitplan angewendet wird. Die restlichen Tage sind ausgegraut.

**Bearbeiten:** Ermöglicht die Zuweisung der Maschinen für jede Stunde oder jede halbe Stunde. Sie können Maschinen nach Zahl oder Prozentsatz zuordnen.

> **Hinweis:**
>
> - Diese Option ist nur in den Autoscale-Benutzeroberflächen für Multisitzungs-OS-Bereitstellungsgruppen und für zufällige Einzelsitzungs-OS-Bereitstellungsgruppen verfügbar.
> - Das Histogramm neben **Bearbeiten** stellt die Anzahl oder den Prozentsatz der Maschinen dar, die in verschiedenen Zeitfenstern ausgeführt werden.

- Sie können **Maschinen jedem Zeitfenster zuweisen**, indem Sie oberhalb von **Spitzenzeiten** auf **Bearbeiten** klicken. Abhängig von der Option, die Sie aus dem Menü im Fenster **Zu startende Maschinen** ausgewählt haben, können Sie Maschinen nach Zahl oder Prozentsatz zuweisen.
- Für Multisitzungs-OS-Bereitstellungsgruppen können Sie die Mindestanzahl ausgeführter Maschinen für alle 30 Minuten separat festlegen. Für Einzelsitzungs-OS-Bereitstellungsgruppen können Sie die Mindestanzahl ausgeführter Maschinen für alle 60 Minuten separat festlegen.

Um eigene Zeitpläne zu definieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Seite **Zeitplan und Spitzenzeiten** des Fensters **Autoscale verwalten** auf **Zeitpläne festlegen**.
2. Wählen Sie im Fenster **Autoscale-Zeitpläne bearbeiten** die Tage aus, die Sie jedem Plan zuordnen möchten. Sie können bei Bedarf auch Zeitpläne löschen.
3. Klicken Sie auf **Fertig stellen**, um die Zeitpläne zu speichern und zur Seite **Zeitplan und Spitzenzeiten** zurückzukehren.
4. Wählen Sie den gewünschten Zeitplan aus und konfigurieren Sie ihn.
5. Klicken Sie auf **Anwenden**, um das Fenster **Autoscale verwalten** zu schließen oder konfigurieren Sie Einstellungen auf anderen Seiten.

**Wichtig:**

- Eine Überlappung von Zeitplänen am selben Tag ist nicht zulässig. Wenn Sie beispielsweise Montag in Zeitplan2 auswählen, nachdem Sie Montag in Zeitplan1 ausgewählt haben, wird Montag in Zeitplan1 automatisch gelöscht.
- Bei Zeitplannamen spielt die Groß- und Kleinschreibung keine Rolle.
- Ein Zeitplanname darf nicht leer sein oder nur Leerzeichen enthalten.
- Leerzeichen zwischen den Zeichen sind zulässig.
- Ein Zeitplanname darf die folgenden Zeichen nicht enthalten: \ / ; : # . * ? = < > | [ ] ( ) { } ‘“‘.
- Autoscale unterstützt keine mehrfach vorkommenden Zeitplannamen. Geben Sie für jeden Zeitplan einen anderen Namen ein.
- Leere Zeitpläne werden nicht unterstützt. Das bedeutet, dass Zeitpläne ohne ausgewählte Tage nicht gespeichert werden.

**Hinweis:**

Die im ausgewählten Zeitplan enthaltenen Tage hervorgehoben und die nicht enthaltenen Tage ausgegraut dargestellt.

### Lastbasierte Einstellungen

**Spitzenzeiten:** Hier können Sie die Spitzenzeiten für die Tage im ausgewählten Zeitplan definieren. Klicken Sie hierzu mit der rechten Maustaste auf das horizontale Balkendiagramm. Nachdem Sie die Spitzenzeiten gewählt haben, werden die verbleibenden, nicht gewählten Zeiten standardmäßig als Nebenzeiten behandelt. **Standardmäßig** gilt der Zeitraum von 7:00 bis 19:00 Uhr als Spitzenzeit für die Tage im ausgewählten Zeitplan.

> **Wichtig:**
>
> - Bei Multisitzungs-OS-Bereitstellungsgruppen wird das Balkendiagramm der Spitzenzeiten für den Kapazitätspuffer verwendet.
> - Bei Einzelsitzungs-OS-Bereitstellungsgruppen wird das Balkendiagramm der Spitzenzeiten für den Kapazitätspuffer verwendet und steuert die Aktionen, die nach Abmeldung und/oder Trennung ausgelöst werden sollen.
> - Sie können für Multisitzungs-OS- und Einzelsitzungs-OS-Bereitstellungsgruppen die Spitzenzeiten für die Tage in einem Zeitplan auf einer Detailebene von 30 Minuten definieren. Alternativ können Sie stattdessen den Befehl `New-BrokerPowerTimeScheme PowerShell` verwenden. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.

**Kapazitätspuffer:** Ermöglicht den Betrieb eines Puffers eingeschalteter Maschinen. Ein geringerer Wert senkt die Kosten. Ein höherer Wert sorgt für eine optimale Benutzererfahrung, da die Benutzer beim Starten von Sitzungen nicht auf das Einschalten zusätzlicher Maschinen warten müssen. Standardmäßig beträgt der Kapazitätspuffer 10 % in Spitzen- und Nebenzeiten. Wenn Sie den Kapazitätspuffer auf 0 setzen, müssen die Benutzer beim Starten von Sitzungen evtl. warten, bis zusätzliche Maschinen hochgefahren sind. In Autoscale können Sie den Kapazitätspuffer für Spitzen- und Nebenzeiten separat festlegen.

### Sonstige Einstellungen

> **Tipp:**
>
> - Sie können die sonstigen Einstellungen mit dem Broker PowerShell SDK konfigurieren. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.
> - Informationen zu den SDK-Befehlen, die mit den Einstellungen "Wenn getrennt"und "Wenn abgemeldet"verknüpft sind, finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

**Wenn getrennt:** Hier können Sie festlegen, wie lange eine getrennte, gesperrte Maschine nach dem Trennen der Sitzung eingeschaltet bleibt, bevor sie angehalten oder heruntergefahren wird. Wenn ein

Zeitwert angegeben wird, wird die Maschine nach Verstreichen dieser Zeit abhängig von der von Ihnen konfigurierten Aktion angehalten oder heruntergefahren. Standardmäßig ist getrennten Maschinen keine Aktion zugewiesen. Sie können für Spitzen- und Nebenzeiten separate Aktionen definieren. Klicken Sie dazu auf den Abwärtspfeil und wählen Sie eine der folgenden Optionen:

- **Keine Aktion**. Die Maschine bleibt nach der Sitzungstrennung eingeschaltet. Es erfolgt keine Aktion durch Autoscale.
- **Anhalten.** Die Maschine wird nach Ablauf der vorgegebenen Zeit automatisch angehalten, jedoch nicht abgeschaltet. Die folgende Option wird verfügbar, nachdem Sie **Anhalten**ausgewählt haben.
  - **Wenn keine erneute Verbindung in (Minuten)**. Angehaltene Maschinen stehen zur Wiederverbindung durch getrennte Benutzer zur Verfügung, jedoch nicht für neue Benutzer. Um Maschinen für alle Workloads wieder verfügbar zu machen, fahren Sie sie herunter. Geben Sie das Timeout in Minuten an, nach dessen Ablauf Autoscale sie herunterfährt.
- **Herunterfahren**. Die Maschine wird nach Ablauf der vorgegebenen Zeit heruntergefahren.

> **Hinweis:**
>
> Diese Option ist nur in den Autoscale-Benutzeroberflächen für Multisitzungs-OS-Bereitstellungsgruppen und für zufällige Einzelsitzungs-OS-Bereitstellungsgruppen verfügbar.

**Wenn abgemeldet:** Hier können Sie festlegen, wie lange eine Maschine nach der Abmeldung der Sitzung eingeschaltet bleibt, bevor sie angehalten oder heruntergefahren wird. Wenn ein Zeitwert angegeben wird, wird die Maschine nach Verstreichen dieser Zeit abhängig von der von Ihnen konfigurierten Aktion angehalten oder heruntergefahren. Standardmäßig ist abgemeldeten Maschinen keine Aktion zugewiesen. Sie können für Spitzen- und Nebenzeiten separate Aktionen definieren. Klicken Sie dazu auf den Abwärtspfeil und wählen Sie eine der folgenden Optionen:

- **Keine Aktion**. Die Maschine bleibt nach der Sitzungsabmeldung eingeschaltet. Es erfolgt keine Aktion durch Autoscale.
- **Anhalten.** Die Maschine wird nach Ablauf der vorgegebenen Zeit automatisch angehalten, jedoch nicht abgeschaltet.
- **Herunterfahren**. Die Maschine wird nach Ablauf der vorgegebenen Zeit heruntergefahren.

> **Hinweis:**
>
> Diese Option ist nur in der Autoscale-Benutzeroberfläche für statische Einzelsitzungs-OS-Bereitstellungsgruppen verfügbar.

**Energieverwaltung von Einzelsitzungs-OS-Maschinen beim Übergang in einen anderen Zeitraum mit getrennten Sitzungen**

> **Wichtig:**
>
> - Diese Erweiterung gilt nur für Einzelsitzungs-OS-Maschinen mit getrennten Sitzungen. Sie gilt nicht für Einzelsitzungs-OS-Maschinen mit abgemeldeten Sitzungen.
> - Damit die Erweiterung wirksam wird, müssen Sie Autoscale für die entsprechende Bereitstellungsgruppe aktivieren. Andernfalls werden beim Übergang die Trennaktionen der Energierichtlinie nicht ausgelöst.

In früheren Versionen blieben Einzelsitzungs-OS-Maschinen beim Übergang in einen Zeitraum, in dem eine Aktion (Trennaktion = "**Anhalten**"oder "**Herunterfahren**") erforderlich war, eingeschaltet. Das Szenario trat auf, wenn eine Maschine während eines Zeitraums (Spitzen- oder Nebenzeit) getrennt wurde, in der keine Aktion (Trennaktion = **Nothing**) erforderlich war.

Ab diesem Release wird die Maschine nach Ablauf der festgelegten Trennzeit von Autoscale angehalten oder ausgeschaltet (je nach der für den Zielzeitraum konfigurierten Trennaktion).

Beispielsweise konfigurieren Sie die folgenden Energierichtlinien für eine Einzelsitzungs-OS-Bereitstellungsgruppe:

- `PeakDisconnectAction` = "Nothing"
- `OffPeakDisconnectAction` = "Shutdown"
- OffPeakDisconnectTimeout = "10"

> **Hinweis:**
>
> Weitere Informationen zur Energierichtlinie mit Trennaktionen finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy und https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

In früheren Versionen blieben Einzelsitzungs-OS-Maschinen, bei denen während der Spitzenzeit eine Sitzung getrennt wurde, beim Übergang von der Spitzen- in die Nebenzeit eingeschaltet. Ab diesem Release werden die Richtlinienaktionen `OffPeakDisconnectAction` und `OffPeakDisconnectTimeout` beim Übergang zu einem neuen Zeitraum auf Einzelsitzungs-OS-Maschinen angewendet. Infolgedessen werden solche Maschine 10 Minuten nach dem Übergang in die Nebenzeit ausgeschaltet.

Wenn Sie zum vorherigen Verhalten zurückkehren möchten (d. h. keine Aktion auf Maschinen mit getrennten Sitzungen beim Übergang von der Spitzen- zur Nebenzeit oder umgekehrt auszuführen), führen Sie einen der folgenden Schritte aus:

- Legen Sie den Registrierungswert "LegacyPeakTransitionDisconnectedBehaviour"auf 1 fest (wahr, d. h. aktiviert das vorherige Verhalten). Standardmäßig ist der Wert 0 (falsch, d. h. löst beim Übergang die Trennaktion der Energierichtlinie aus).
  - Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Name: LegacyPeakTransitionDisconnectedBehaviour
  - Typ: REG_DWORD
  - Wert: 0x00000001 (1)
- Konfigurieren Sie die Einstellung mit dem PowerShell-Befehl `Set-BrokerServiceConfigurationDa` . Beispiel:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Eine Maschine muss die folgenden Kriterien erfüllen, damit Energierichtlinienaktionen beim Zeitraumwechsel auf sie angewendet werden können:

- Es liegt eine getrennte Sitzung vor.
- Es stehen keine Energieaktionen aus.
- Sie gehört zu einer Einzelsitzungs-OS-Bereitstellungsgruppe, die in einen anderen Zeitraum übergeht.
- Es liegt eine Sitzung vor, die während eines bestimmten Zeitraums (Spitzen- oder Nebenzeit) getrennt wurde und die Maschine wechselt zu einem Zeitraum, für den eine Energieaktion zugewiesen ist.

### Funktionsweise des Kapazitätspuffers

Der Kapazitätspuffer dient zum Vorhalten freier Kapazität zur Berücksichtigung dynamischer Laststeigerungen. Es sind zwei Szenarien zu beachten:

- Bei Multisitzungs-OS-Bereitstellungsgruppen wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Bereitstellungsgruppe in Bezug auf den Lastindex definiert. Weitere Hinweise zum Lastindex finden Sie unter Lastindex.
- Bei Einzelsitzungs-OS-Bereitstellungsgruppen wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Bereitstellungsgruppe in Bezug auf die Anzahl der Maschinen definiert.

> **Hinweis:**
>
> Wenn Sie Autoscale auf Maschinen mit Tag beschränken, wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Maschinen mit Tag in der Bereitstellungsgruppe in Bezug auf den Lastindex definiert.

In Autoscale können Sie den Kapazitätspuffer für Spitzen- und Nebenzeiten separat festlegen. Ein niedrigerer Wert im Feld "Kapazitätspuffer"senkt die Kosten, da Autoscale weniger freie Kapazität einschaltet. Ein höherer Wert sorgt für eine optimale Benutzererfahrung, da die Benutzer beim Starten von Sitzungen nicht auf das Einschalten zusätzlicher Maschinen warten müssen. Standardmäßig beträgt der Kapazitätspuffer 10 %.

> **Wichtig:**
>
> Der Kapazitätspuffer bewirkt das Einschalten von Maschinen, sobald die Reservekapazität unter x Prozent der Gesamtkapazität der Bereitstellungsgruppe sinkt. Dadurch wird der erforderliche Prozentsatz an Kapazitätsreserven beibehalten.

## Multisitzungs-OS-Bereitstellungsgruppen

### Wann werden Maschinen eingeschaltet?

> **Wichtig:**
>
> Wenn ein Zeitplan ausgewählt ist, schaltet Autoscale alle im Zeitplan zum Einschalten konfigurierten Maschinen ein. Diese Maschinen bleiben während des Zeitplans lastunabhängig eingeschaltet.

Wenn die Anzahl eingeschalteter Maschinen in der Bereitstellungsgruppe die Pufferkapazität gemäß Lastindex nicht mehr erfüllen kann, schaltet Autoscale weitere Maschinen ein. Angenommen, Ihre Bereitstellungsgruppe hat 20 Maschinen und 3 Maschinen werden im Rahmen der planbasierten Skalierung mit einem Kapazitätspuffer von 20% eingeschaltet. Schließlich werden 4 Maschinen eingeschaltet, wenn keine Last vorhanden ist. Dies liegt daran, dass ein 4 x 10.000 Lastindex als Puffer benötigt wird; daher müssen mindestens 4 Maschinen eingeschaltet werden. Dies kann zu Spitzenzeiten, bei einer höheren Maschinenauslastung, neuen Sitzungsstarts und beim Hinzufügen neuer Maschinen zur Bereitstellungsgruppe eintreten. Autoscale schaltet nur Maschinen ein, die die folgenden Kriterien erfüllen:

- Die Maschinen sind nicht im Wartungsmodus.
- Der Hypervisor, auf dem die Maschinen ausgeführt werden, ist nicht im Wartungsmodus.
- Die Maschinen sind derzeit ausgeschaltet.
- Die Maschinen haben keine ausstehenden Energieaktionen.

### Wann werden Maschinen ausgeschaltet?

> **Wichtig:**
>
> - Wenn ein Zeitplan ausgewählt ist, schaltet Autoscale die Maschinen gemäß diesem Zeitplan aus.
> - Autoscale schaltet keine Maschinen aus, die im Zeitplan als eingeschaltet konfiguriert sind.

Sind mehr als genügend Maschinen (laut Zeitplan und einschließlich Puffer) für eine Bereitstellungsgruppe eingeschaltet, schaltet Autoscale überzählige Maschinen aus. Dies kann zu Nebenzeiten, bei einer gesunkenen Maschinenauslastung, bei Sitzungsabmeldungen und beim Entfernen von Maschinen aus einer Bereitstellungsgruppe eintreten. Autoscale schaltet nur Maschinen aus, die die folgenden Kriterien erfüllen:

- Die Maschinen und der Hypervisor, auf dem sie ausgeführt werden, sind nicht im Wartungsmodus.
- Die Maschinen sind derzeit eingeschaltet.
- Die Maschinen sind als verfügbar registriert oder warten auf die Registrierung nach dem Start.
- Die Maschinen haben keine aktiven Sitzungen.
- Die Maschinen haben keine ausstehenden Energieaktionen.
- Die Maschinen erfüllen die angegebene Ausschaltverzögerung. Dies bedeutet, dass die Maschinen mindestens x Minuten eingeschaltet waren, wobei x die für die Bereitstellungsgruppe festgelegte Ausschaltverzögerung ist.

#### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Bereitstellungsgruppenkonfiguration**. Die Bereitstellungsgruppe, die von Autoscale verwaltet werden soll, enthält 10 Maschinen (M1 bis M10).
- **Autoscale-Konfiguration**
  - Der Kapazitätspuffer ist auf 10 % eingestellt.
  - Im ausgewählten Zeitplan ist keine Maschine enthalten.

Das Szenario hat folgenden Ablauf:

1. Kein Benutzer meldet sich an.
2. Die Anzahl der Benutzersitzungen erhöht sich.
3. Weitere Benutzersitzungen beginnen.
4. Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.

5. Die Benutzersitzungslast nimmt weiter ab, bis sie nur von lokalen Ressourcen getragen wird.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Keine Benutzerlast (Anfangszustand)
  - Eine Maschine (z. B. M1) wird eingeschaltet. Die Maschine wird wegen des konfigurierten Kapazitätspuffers eingeschaltet. In diesem Fall gilt 10 (Anzahl der Maschinen) x 10.000 (Lastindex) x 10 % (konfigurierter Kapazitätspuffer) = 10.000. Daher wird eine Maschine eingeschaltet.
  - Der Lastindexwert der eingeschalteten Maschine (M1) liegt bei einer Basislast (Lastindex = 0).
- Der erste Benutzer meldet sich an.
  - Die Sitzung wird an Maschine M1 zum Hosten geleitet.
  - Der Lastindex der eingeschalteten Maschine M1 erhöht sich und liegt nicht mehr bei der Basislast.
  - Autoscale schaltet eine zusätzliche Maschine (M2) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
  - Der Lastindexwert der Maschine M2 liegt bei einer Basislast.
- Die Benutzerlast steigt.
  - Die Sitzungen werden auf die Maschinen M1 und M2 verteilt. Dadurch steigt der Lastindex der eingeschalteten Maschinen (M1 und M2).
  - Die Kapazitätsreserven liegen nach wie vor auf einem Niveau über 10.000 gemäß Lastindex.
  - Der Lastindexwert der Maschine M2 liegt nicht mehr bei einer Basislast.
- Weitere Benutzersitzungen beginnen.
  - Die Sitzungen werden auf die Maschinen M1 und M2 verteilt. Dadurch steigt der Lastindex der eingeschalteten Maschinen (M1 und M2) weiter.
  - Wenn die gesamte freie Kapazität in Bezug auf den Lastindex auf unter 10.000 sinkt, beginnt Autoscale mit dem Einschalten einer zusätzlichen Maschine (M3), um den Bedarf gemäß konfiguriertem Kapazitätspuffer zu decken.
  - Der Lastindexwert der Maschine M3 liegt bei einer Basislast.
- Weitere Benutzersitzungen beginnen.
  - Die Sitzungen werden auf die Maschinen M1 bis M3 verteilt. Dadurch steigt der Lastindex der eingeschalteten Maschinen (M1 bis M3).
  - Die Kapazitätsreserven liegen auf einem Niveau über 10.000 gemäß Lastindex.
  - Der Lastindexwert der Maschine M3 liegt nicht mehr bei einer Basislast.

- Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.
  - Nachdem Benutzer sich von ihren Sitzungen abgemeldet haben oder diese aufgrund von Timeouts abgemeldet wurden, wird die freigegebene Kapazität auf Maschinen M1 bis M3 für das Hosting neuer Sitzungen wiederverwendet.
  - Steigt die gesamte freie Kapazität auf ein Niveau über 10.000 gemäß Lastindex, versetzt Autoscale eine der Maschinen (z. B. M3) in den Drainingzustand. Von anderen Benutzern gestartete Sitzungen werden nicht mehr an diese Maschine geleitet, sofern keine neuen Änderungen erfolgen. Beispielsweise Endbenutzerlast steigt wieder oder eine Geringauslastung anderer Maschinen
- Die Sitzungslast nimmt weiter ab.
  - Wenn alle Sitzungen auf Maschine M3 beendet wurden und die angegebene Ausschaltverzögerung abgelaufen ist, schaltet Autoscale M3 aus.
  - Wenn weitere Benutzer ihre Sitzungen beenden, wird die freigegebene Kapazität auf den eingeschalteten Maschinen (M1 und M2) für das Hosting neuer Sitzungen anderer Benutzer wiederverwendet.
  - Steigt die gesamte freie Kapazität auf ein Niveau über 10.000 gemäß Lastindex, versetzt Autoscale eine der Maschinen (z. B. M2) in den Drainingzustand. Von anderen Benutzern gestartete Sitzungen werden nicht mehr an diese Maschine geleitet.
- Die Sitzungslast nimmt weiter ab bis es keine Sitzungen mehr gibt.
  - Wenn alle Sitzungen auf Maschine M2 beendet wurden und die angegebene Ausschaltverzögerung abgelaufen ist, schaltet Autoscale M2 aus.
  - Der Lastindexwert der eingeschalteten Maschine (M1) liegt bei einer Basislast. Maschine M1 wird aufgrund des konfigurierten Kapazitätspuffers nicht in den Drainingzustand versetzt.

> **Hinweis:**
>
> Bei Multisitzungs-OS-Bereitstellungsgruppen gehen alle Änderungen am Desktop verloren, wenn Benutzer Sitzungen abmelden. Bei entsprechender Konfiguration werden benutzerspezifische Einstellungen jedoch zusammen mit dem Benutzerprofil weitergegeben.

### Zufällige Einzelsitzungs-OS-Bereitstellungsgruppen

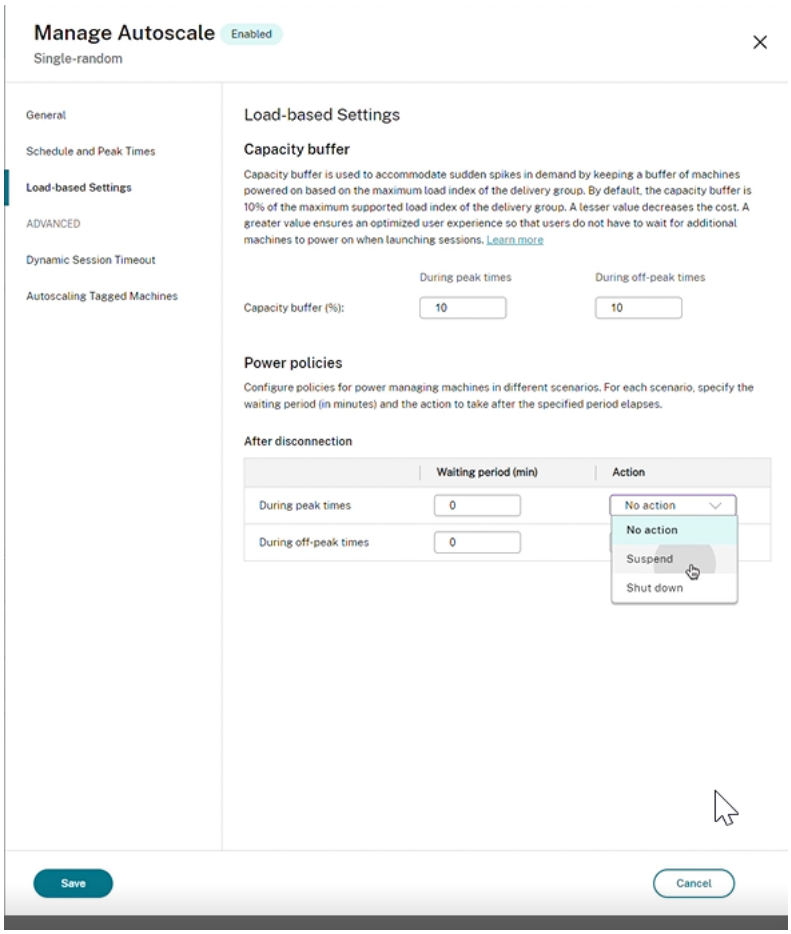
Der Kapazitätspuffer wird verwendet, um plötzliche Nachfragespitzen aufzufangen, indem eine auf der Gesamtzahl der Maschinen in der Bereitstellungsgruppe basierende Zahl von Maschinen eingeschaltet bleibt. Standardmäßig beträgt der Kapazitätspuffer 10 % der Gesamtzahl der Maschinen in der Bereitstellungsgruppe.

Überschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden weitere Maschinen eingeschaltet. Unterschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden die überzähligen Maschinen je nach Konfiguration angehalten oder ausgeschaltet.

**Energierichtlinien**

Konfigurieren Sie Richtlinien, um die Stromversorgung von Maschinen für verschiedene Szenarien zu verwalten. Für jedes Szenario können Sie die Wartezeit (in Minuten) und die Aktion angeben, die nach Ablauf der angegebenen Zeit ausgeführt werden soll. Energierichtlinien gelten für zufällige Bereitstellungsgruppen mit Einzelsitzungs-OS und für statische Bereitstellungsgruppen für Einzelsitzungs-OS.



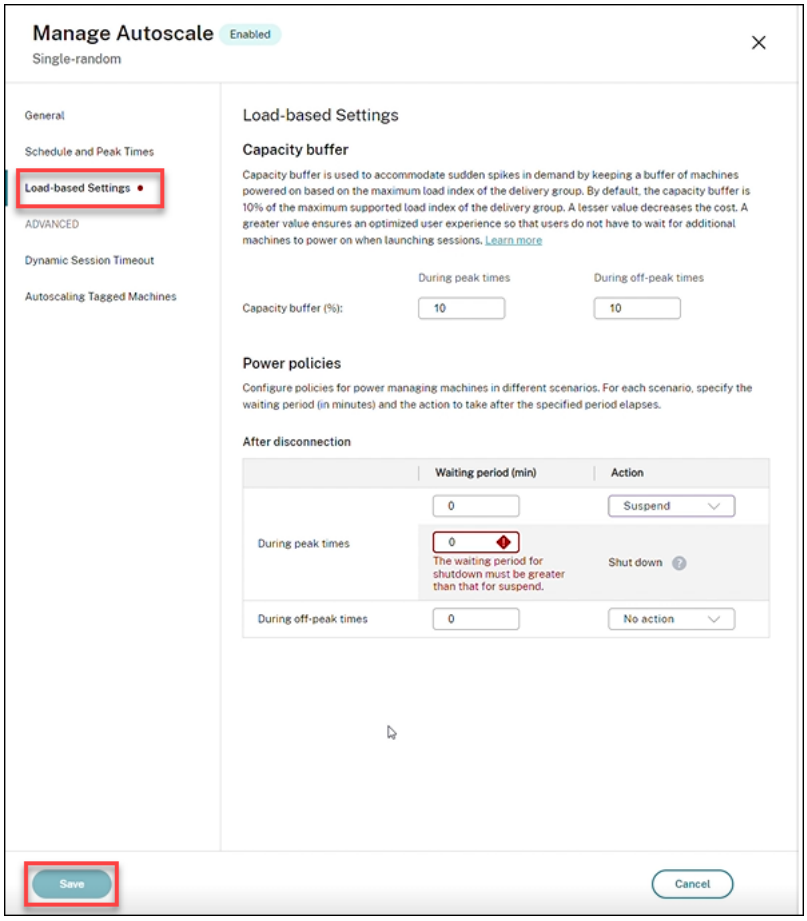

Nach dem Trennen der Verbindung gelten die folgenden Einstellungen für Spitzenzeiten und für Nebenzeiten:

- Sie können die Wartezeit in Minuten und Aktionen wie “Keine Aktion”, “Anhalten”oder “Herunterfahren”in der Dropdownliste festlegen.
- Wenn Sie die Aktion “Anhalten”wählen, konfigurieren Sie eine zusätzliche Wartezeit, um den

Computer herunterzufahren.

> **Hinweis:**
>
> - In Spitzenzeiten und in Nebenzeiten muss die Wartezeit für die Aktion "Herunterfahren" länger sein als die Wartezeit für "Anhalten".
> - Angehaltene Maschinen sind nur für getrennte Benutzer zugänglich, wenn sie die Verbindung wiederherstellen. Um die angehaltenen Maschinen für neue Benutzer verfügbar zu machen, fahren Sie sie herunter.
> - Wenn die Zeiteinstellungen für die Felder "Anhalten"und "Herunterfahren"falsch konfiguriert sind, ist die Option **Speichern** deaktiviert und neben den Navigationselementen erscheint ein roter Punkt, der auf Einstellungsfehler hinweist.




Beispiel:

- Wenn Sie die Wartezeit auf 12 Minuten einstellen und als erste Aktion "Keine Aktion"wählen, ist die Maschine nach Ablauf der 12 Minuten weiterhin eingeschaltet.
- Wenn Sie die Wartezeit auf 15 Minuten einstellen und als erste Aktion "Anhalten"und als zweite Wartezeit 20 Minuten wählen, wird das Gerät nach 15 Minuten angehalten. Nach Ablauf der zweiten Wartezeit wird die Maschine heruntergefahren.

- Wenn Sie die Wartezeit auf 18 Minuten einstellen und als erste Aktion "Herunterfahren"wählen, wird das Gerät nach 18 Minuten heruntergefahren.

#### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Bereitstellungsgruppenkonfiguration**. Die Bereitstellungsgruppe, die von Autoscale verwaltet werden soll, enthält 10 Maschinen (M1 bis M10).
- **Autoscale-Konfiguration**
  - Der Kapazitätspuffer ist auf 10 % eingestellt.
  - Im ausgewählten Zeitplan ist keine Maschine enthalten.

Das Szenario hat folgenden Ablauf:

1. Kein Benutzer meldet sich an.
2. Die Anzahl der Benutzersitzungen erhöht sich.
3. Weitere Benutzersitzungen beginnen.
4. Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.
5. Die Benutzersitzungslast nimmt weiter ab, bis sie nur von lokalen Ressourcen getragen wird.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Keine Benutzerlast (Anfangszustand)
  - Eine Maschine (M1) ist eingeschaltet. Die Maschine wird wegen des konfigurierten Kapazitätspuffers eingeschaltet. In diesem Fall gilt 10 (Anzahl der Maschinen) x 10 % (konfigurierter Kapazitätspuffer) = 1. Daher wird eine Maschine eingeschaltet.
- Der erste Benutzer meldet sich an.
  - Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen Desktop zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die auf den eingeschalteten Maschinen gehostet werden. In diesem Fall wird ihm ein Desktop von Maschine M1 zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (M2) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
- Ein zweiter Benutzer meldet sich an.
  - Dem Benutzer wird ein Desktop von Maschine M2 zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (M3) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.

- Ein dritter Benutzer meldet sich an.
  - Ihm wird ein Desktop von Maschine M3 zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (M4) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
- Ein Benutzer meldet sich ab.
  - Wenn sich ein Benutzer abmeldet oder bei einem Desktop ein Timeout auftritt, steht die freigesetzte Kapazität (z. B. M3) als Puffer zur Verfügung. Infolgedessen schaltet Autoscale Maschine M4 aus, da der Kapazitätspuffer auf 10 % festgelegt ist.
- Weitere Benutzer melden sich ab, bis keine Benutzer mehr vorhanden sind.
  - Wenn sich weitere Benutzer abmelden, schaltet Autoscale Maschinen aus (z. B. M2 oder M3).
  - Selbst wenn keine Benutzer mehr vorhanden sind, schaltet Autoscale die verbleibende Maschine (z. B. M1) nicht aus, da diese als Reserve festgelegt ist.

> **Hinweis:**
>
> Bei zufälligen Einzelsitzungs-OS-Bereitstellungsgruppen gehen alle Änderungen am Desktop verloren, wenn Benutzer Sitzungen abmelden. Bei entsprechender Konfiguration werden benutzerspezifische Einstellungen jedoch zusammen mit dem Benutzerprofil weitergegeben.

### Statische Einzelsitzungs-OS-Bereitstellungsgruppen

Der Kapazitätspuffer wird verwendet, um plötzliche Nachfragespitzen aufzufangen, indem eine auf der Gesamtzahl der nicht zugewiesenen Maschinen in der Bereitstellungsgruppe basierende Zahl nicht zugewiesener Maschinen eingeschaltet bleibt. Standardmäßig beträgt der Kapazitätspuffer 10 % der Gesamtzahl der nicht zugewiesenen Maschinen in der Bereitstellungsgruppe.

> **Wichtig:**
>
> Wenn alle Maschinen einer Bereitstellungsgruppe zugewiesen sind, spielt der Kapazitätspuffer für das Ein- und Ausschalten von Maschinen keine Rolle mehr.

Überschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden weitere nicht zugewiesene Maschinen eingeschaltet. Unterschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden überzählige Maschinen je nach Konfiguration angehalten oder ausgeschaltet.

Autoscale für statische Einzelsitzungs-OS-Bereitstellungsgruppen:

- Schaltet zugewiesene Maschinen zu Spitzenzeiten ein und zu Nebenzeiten aus. Aber nur dann, wenn die Eigenschaft `AutomaticPowerOnForAssigned` der entsprechenden Einzelsitzungs-OS-Bereitstellungsgruppe auf “true”festgelegt ist.

- Schaltet einen Computer während Spitzenzeiten automatisch ein, wenn er ausgeschaltet ist und die Eigenschaft `AutomaticPowerOnForAssignedDuringPeak` der Bereitstellungsgruppe, zu der er gehört, auf "true"gesetzt ist.

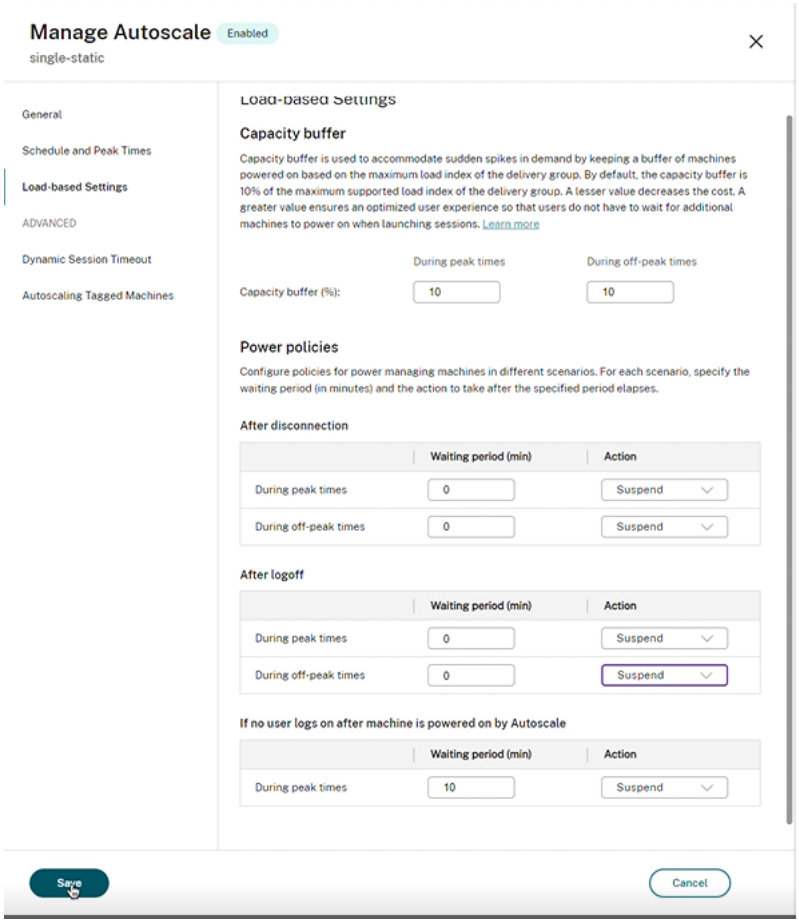
Um zu verstehen, wie der Kapazitätspuffer mit zugewiesenen Maschinen funktioniert, sollten Sie Folgendes beachten:

- Der Kapazitätspuffer funktioniert nur, wenn die Bereitstellungsgruppe mindestens eine nicht zugewiesene Maschinen hat.
- Wenn es in der Bereitstellungsgruppe keine nicht zugewiesenen Maschinen gibt (alle Maschinen in der Bereitstellungsgruppe sind zugewiesen), spielt der Kapazitätspuffer für das Ein- und Ausschalten von Maschinen keine Rolle mehr.
- Die Eigenschaft `AutomaticPowerOnForAssignedDuringPeak` legt fest, ob zugewiesene Maschinen zu Spitzenzeiten eingeschaltet werden. Wenn der Wert auf "True"festgelegt ist, lässt Autoscale die Maschinen zu Spitzenzeiten eingeschaltet. Autoscale schaltet sie außerdem ein, wenn sie ausgeschaltet sind.

#### Energierichtlinien

Konfigurieren Sie Richtlinien, um die Stromversorgung von Maschinen für verschiedene Szenarien zu verwalten. Für jedes Szenario können Sie die Wartezeit (in Minuten) und die Aktion angeben, die nach Ablauf der angegebenen Zeit ausgeführt werden soll. Energierichtlinien gelten für zufällige Bereitstellungsgruppen mit Einzelsitzungs-OS und für statische Bereitstellungsgruppen für Einzelsitzungs-OS.




Für **Nach dem Trennen der Verbindung** und **Nach der Abmeldung** gelten die folgenden Einstellungen für Spitzenzeiten und für Nebenzeiten:

- Sie können die Wartezeit in Minuten und Aktionen wie “Keine Aktion”, “Anhalten”oder “Herunterfahren”in der Dropdownliste festlegen.

**Wenn sich nach dem Einschalten der Maschine durch Autoscale kein Benutzer anmeldet**, gelten die folgenden Einstellungen nur zu Spitzenzeiten:

Sie können die Wartezeit in Minuten und Aktionen wie “Keine Aktion”, “Anhalten”oder “Herunterfahren”in der Dropdownliste festlegen.

### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Bereitstellungsgruppenkonfiguration**. Die Bereitstellungsgruppe, die von Autoscale verwaltet werden soll, enthält 10 Maschinen (M1 bis M10).
- **Autoscale-Konfiguration**
  - Die Maschinen M1 bis M3 sind zugewiesen, die Maschinen M4 bis M10 sind nicht zugewiesen.

  - Der Kapazitätspuffer ist für Spitzen- und Nebenzeiten auf 10 % festgelegt.
  - Gemäß Zeitplan findet die Energieverwaltung von Maschinen durch Autoscale zwischen 09:00 Uhr und 18:00 Uhr statt.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Beginn des Zeitplans: 09:00 Uhr
  - Autoscale schaltet Maschine M1 bis M3 ein.
  - Autoscale schaltet eine zusätzliche Maschine (z. B. M4) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken. Maschine M4 ist nicht zugewiesen.
- Der erste Benutzer meldet sich an.
  - Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen Desktop zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die auf den eingeschalteten, nicht zugewiesenen Maschinen gehostet werden. In diesem Fall wird ihm ein Desktop von Maschine M4 zugewiesen. Bei nachfolgenden Anmeldungen wird dem Benutzer derselbe Desktop wie beim ersten Mal zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (z. B. M5) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
- Ein zweiter Benutzer meldet sich an.
  - Dem Benutzer wird ein Desktop von den nicht zugewiesenen, eingeschalteten Maschinen zugewiesen. In diesem Fall wird ihm ein Desktop von Maschine M5 zugewiesen. Bei nachfolgenden Anmeldungen wird dem Benutzer derselbe Desktop wie beim ersten Mal zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (z. B. M6) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
- Benutzer melden sich ab.
  - Wenn sich Benutzer vom Desktop abmelden oder auf Desktops ein Timeout auftritt, bleiben die Maschinen M1 bis M5 von 09:00 Uhr bis 18:00 Uhr eingeschaltet. Wenn sich Benutzer neu anmelden, stellen sie eine Verbindung mit demselben Desktop her, der ihnen bei der ersten Verwendung zugewiesen wurde.
  - Die nicht zugewiesene Maschine M6 ist für einen neuen, nicht zugewiesenen Benutzer vorgesehen.
- Ende des Zeitplans: 18:00 Uhr
  - Um 18:00 Uhr schaltet Autoscale die Maschinen M1 bis M5 ab.
  - Die nicht zugewiesene Maschine M6 bleibt wegen des konfigurierten Kapazitätspuffers eingeschaltet. Diese Maschine ist für einen neuen, nicht zugewiesenen Benutzer vorgesehen.

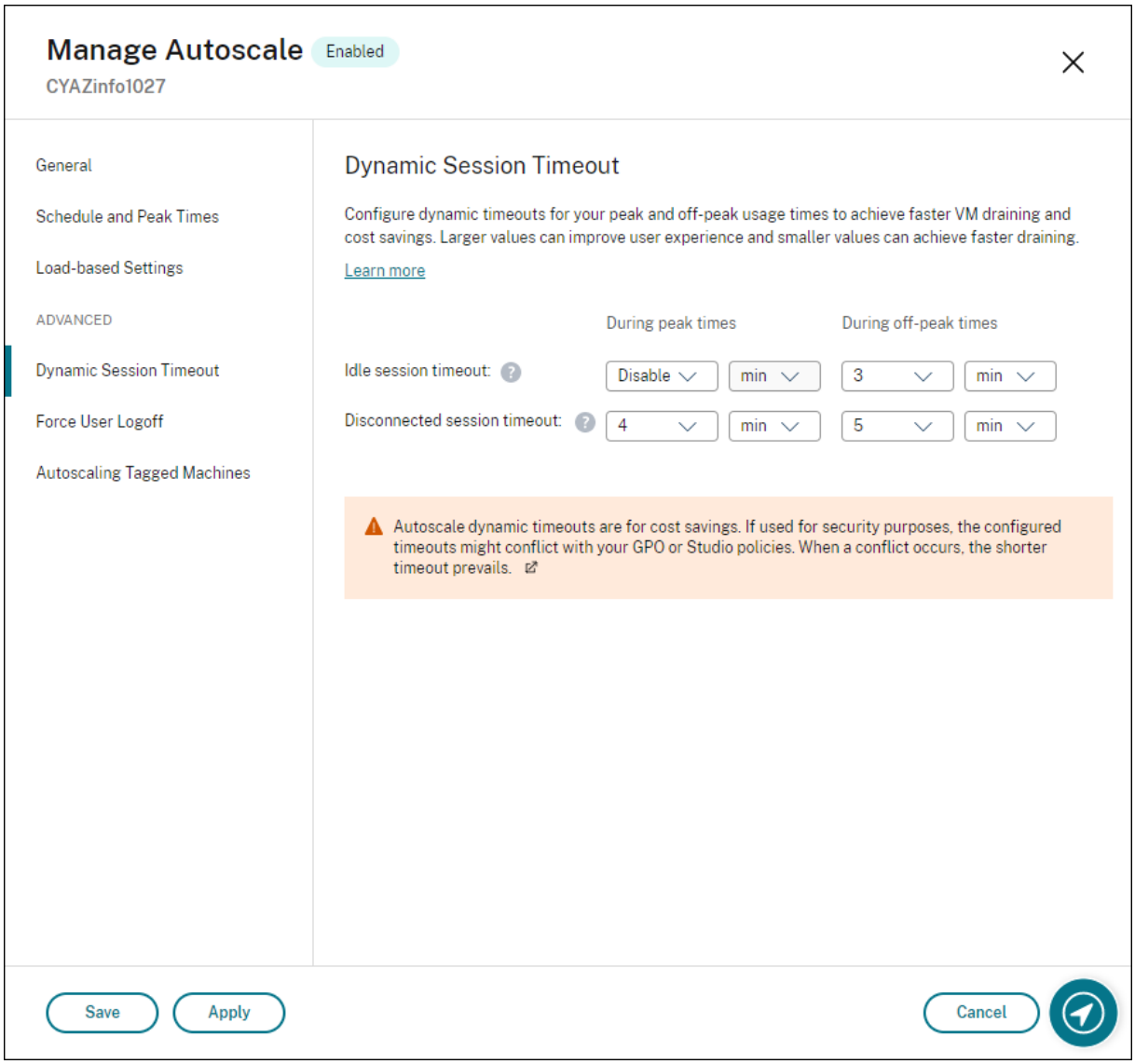
 

- In der Bereitstellungsgruppe sind die Maschinen M6 bis M10 nicht zugewiesen.

## Dynamische Sitzungstimeouts

June 26, 2023

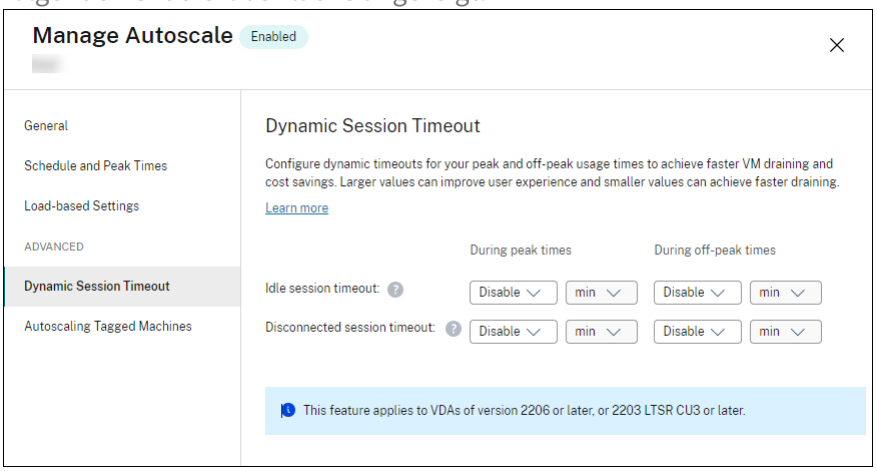
Mit diesem Feature können Sie Timeouts für getrennte Sitzungen und Leerlaufsitzungen für Neben- und Spitzenzeiten konfigurieren, um ein schnelleres Maschinendraining und Kosteneinsparungen zu erzielen. Dieses Feature gilt für Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS. VDAs melden Leerlaufzeiten für Sitzungen, die über 10 Minuten im Leerlauf sind. Durch dynamische Sitzungstimeouts können daher Sitzungen nicht vor Ablauf von 10 Minuten getrennt werden. Ein geringerer Wert trennt Sitzungen früher und senkt so die Kosten.



**Hinweis:**

- Dieses Feature ist immer für Multisitzungs-OS-Bereitstellungsgruppen verfügbar.
- Für Bereitstellungsgruppen mit Einzelsitzungs-OS gilt dieses Feature für VDAs ab Version 2206 CR oder 2203 LTSR CU3 oder höher. Stellen Sie sicher, dass sich diese VDAs mindestens einmal in Citrix Cloud registriert haben. Wenn dieses Feature nicht verfügbar ist, wird die folgende Benutzeroberfläche angezeigt:




- Mit Autoscale festgelegte dynamische Timeouts dienen der Kosteneinsparung. Bei Verwendung aus Sicherheitsgründen können die konfigurierten Timeouts mit Ihren Gruppenrichtlinienobjekt- oder Verwaltungskonsolen-Richtlinien in Konflikt stehen. Bei einem Konflikt wird das kürzere Timeout verwendet.

**Timeout bei Sitzungsleerlauf:** Aktiviert oder deaktiviert einen Timer, der angibt, wie lange eine ununterbrochene Benutzerverbindung erhalten bleibt, wenn keine Benutzereingaben stattfinden. Wenn der Timer abläuft, wird die Sitzung getrennt und der **Timeout für Sitzungstrennung** angewendet. Wenn der **Timeout für Sitzungstrennung** deaktiviert ist, wird die Sitzung nicht abgemeldet.

**Wichtig:**

- Wenn Sie einen Wert angeben, der kleiner oder gleich zehn Minuten (600 Sekunden) ist, trennt Autoscale die Sitzungen nach zehn Minuten Leerlauf. Das liegt daran, dass Autoscale die von VDAs gemeldeten Leerlaufzeiten verwendet. VDAs melden Leerlaufzeiten für Sitzungen, die über 10 Minuten im Leerlauf sind.
- Eine Sitzung im Leerlauf wird auch dann getrennt, wenn der Benutzer in den letzten 5 Minuten vor Erreichen des Leerlauftimeouts mit ihr interagiert.

**Timeout für Sitzungstrennung:** Aktiviert bzw. deaktiviert einen Timer, der angibt, wie lange ein getrennter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird. Wenn der Timer aktiviert ist, wird die getrennte Sitzung abgemeldet, wenn die Zeit abgelaufen ist.

# Autoscale von getaggten Maschinen (Cloudburst)

March 7, 2023

> **Hinweis:**
>
> Dieses Feature hieß bisher "Autoscale einschränken".

## Einführung

Autoscale bietet die Flexibilität, die Energieverwaltung nur für eine Teilmenge der Maschinen in einer Bereitstellungsgruppe durchzuführen. Sie erreichen dies, indem Sie ein Tag auf mindestens eine Maschine anwenden und dann Autoscale so konfigurieren, dass die Energieverwaltung nur für getaggte Maschinen zutrifft.

Diese Funktion kann in Anwendungsfällen nützlich sein, in denen Sie On-Premises-Ressourcen (oder reservierte Public Cloud-Instanzen) verwenden möchten, um Workloads zu verarbeiten, bevor cloudbasierte Ressourcen zusätzliche Anforderungen (d. h. Burstworkloads) erfüllen. Damit Maschinen im eigenen Rechenzentrum (oder reservierte Instanzen) zuerst Workloads verarbeiten, müssen Sie die Tagbeschränkung zusammen mit einer Zonenpräferenzeinstellung verwenden.

Die Tagbeschränkung legt fest, für welche Maschinen Autoscale die Energieverwaltung übernimmt. Die Zonenpräferenz gibt Maschinen in der bevorzugten Zone an, um Benutzerstartanforderungen zu verarbeiten. Weitere Informationen finden Sie unter Tags und Zonenpräferenz.

Um Autoscale auf bestimmte getaggte Maschinen anzuwenden, können Sie die Vewaltungskonsole oder PowerShell verwenden.

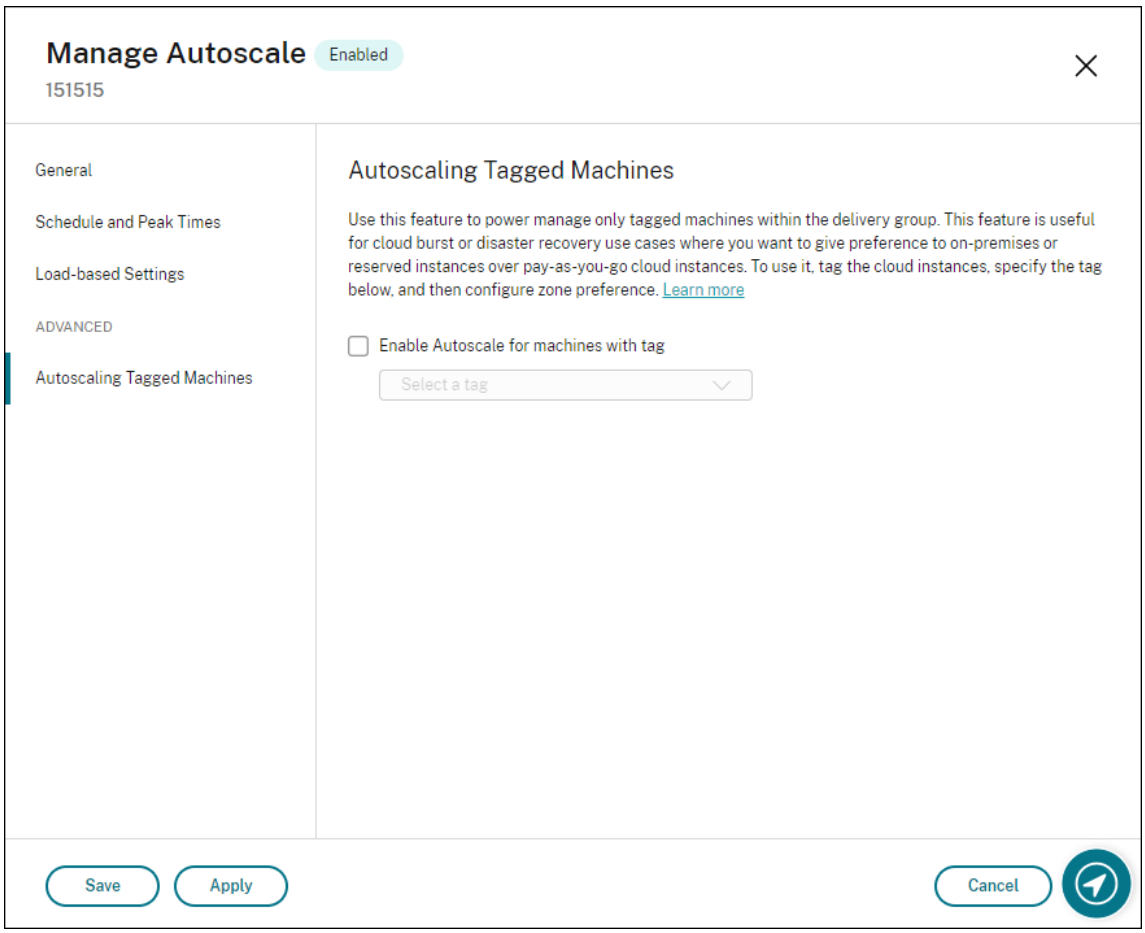
## Autoscale getaggter Maschinen über die Verwaltungskonsole

Führen Sie folgende Schritte aus, um Autoscale auf bestimmte getaggte Maschinen anzuwenden:

1. Erstellen Sie ein Tag und wenden Sie es auf die entsprechenden Maschinen in der Bereitstellungsgruppe an. Weitere Informationen finden Sie unter Verwalten von Tags und Tagbeschränkungen.
2. Wählen Sie die Bereitstellungsgruppe aus und öffnen Sie den Assistenten **Autoscale verwalten**.
3. Wählen Sie auf der Seite **Autoscale getaggte Maschinen** die Option **Autoscale für getaggte Maschinen aktivieren**, wählen Sie ein Tag in der Liste aus und klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

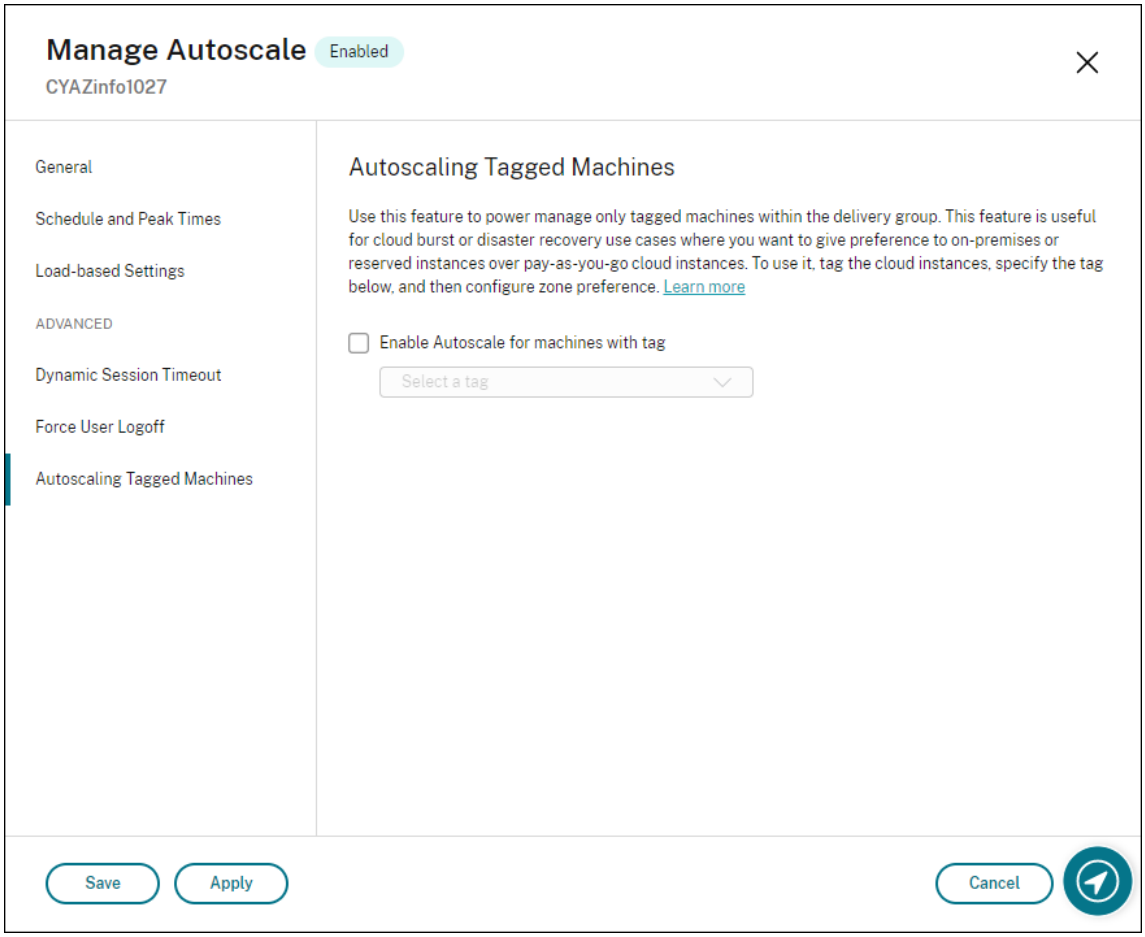
   Benutzeroberfläche für *statische* und *zufällige* Einzelsitzungs-OS-Bereitstellungsgruppen:




Benutzeroberfläche für *Multisitzungs-OS-Bereitstellungsgruppen*:




> **Warnung:**
>
> - Das Anwenden von Autoscale auf Maschinen mit einem bestimmten Tag kann dazu führen, dass das Histogramm automatisch aktualisiert wird, um die Anzahl von Maschinen für dieses Tag anzuzeigen. Auf der Seite **Zeitplan und Spitzenzeiten** können Sie jedem Zeitfenster bei Bedarf Maschinen manuell zuweisen.
> - Sie können ein auf getaggten Maschinen verwendetes Tag nicht löschen. Um ein solches Tag zu löschen, müssen Sie zuerst die Tagbeschränkung entfernen.

Nachdem Sie eine Tagbeschränkung angewendet haben, möchten Sie sie eventuell später aus der Bereitstellungsgruppe entfernen. Gehen Sie hierfür auf die Seite **Autoscale verwalten > Autoscale getaggte Maschinen** und deaktivieren Sie **Autoscale für getaggte Maschinen aktivieren**.

> **Warnung:**
>
> - Wenn Sie das Tag von den entsprechenden Maschinen entfernen, ohne **Autoscale für getaggte Maschinen aktivieren** zu deaktivieren, wird beim Öffnen des Assistenten **Autoscale verwalten** möglicherweise eine Warnung angezeigt. Durch das Entfernen des

> Tags von den Maschinen verbleiben evtl. keine Maschinen für die Autoscaleverwaltung, da das in Autoscale angegebene Tag ungültig ist. Um die Warnung aufzulösen, gehen Sie zur Seite **Autoscale getaggte Maschinen**, entfernen Sie das ungültige Tag und klicken Sie zum Speichern der Änderungen auf **Übernehmen**.

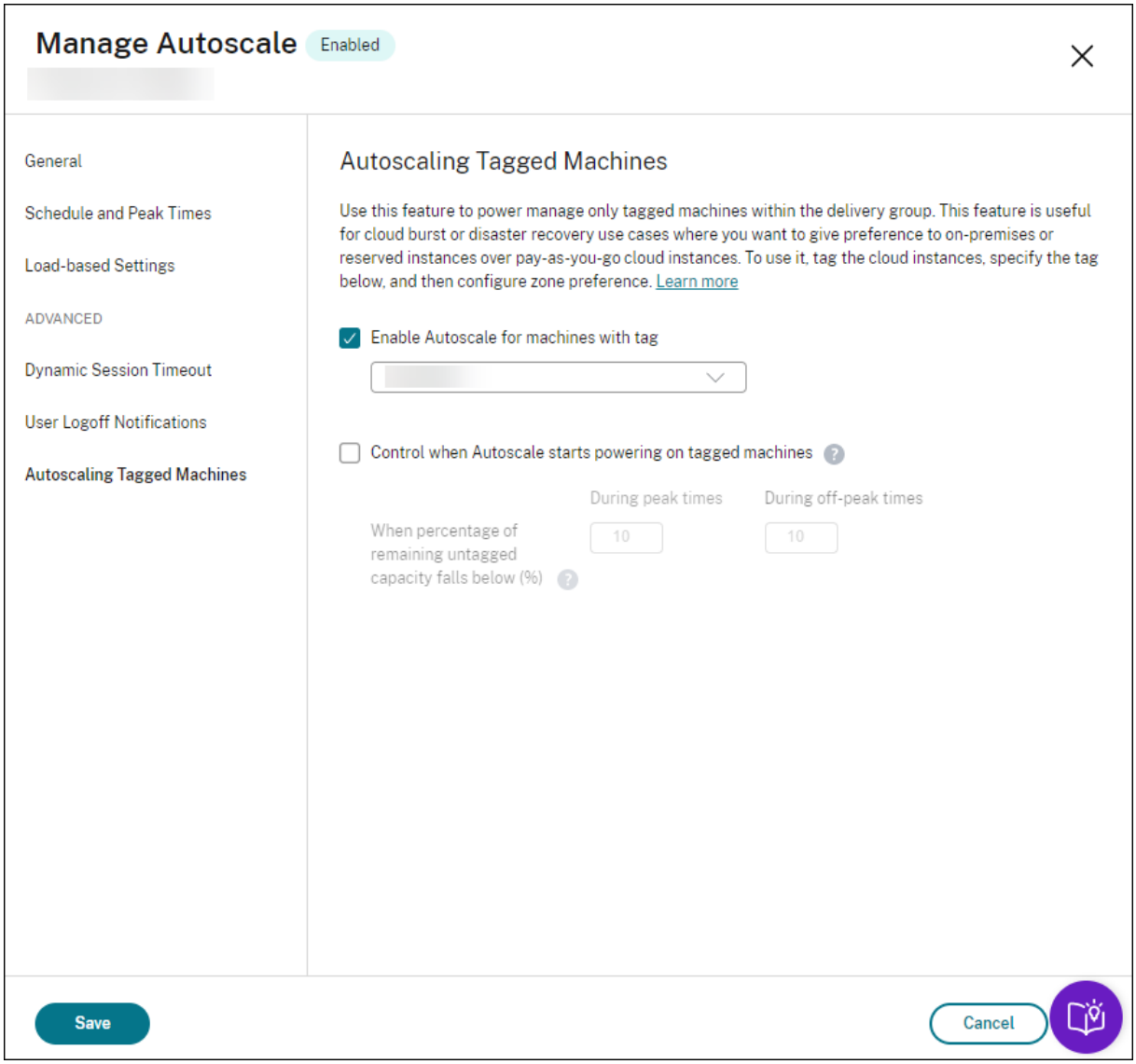
#### Steuerung des Einschaltens von Ressourcen durch Autoscale

Sie können auch steuern, wann Autoscale (basierend auf der Nutzung von ungetaggten Maschinen) mit dem Einschalten von getaggten Maschinen beginnt. Dadurch können Sie den Einsatz von getaggten Workloads oder Workloads in der öffentlichen Cloud weiter optimieren.

Führen Sie hierzu die folgenden Schritte aus:

1. Wählen Sie auf der Seite **Autoscale getaggte Maschinen** die Option **Steuern, wann Autoscale mit dem Einschalten von getaggten Maschinen beginnt**.
2. Geben Sie einen gewünschten Prozentwert für die Nutzung von ungetaggten Maschinen zu Spitzen- und Nebenzeiten ein, und klicken Sie auf **Übernehmen**. Unterstützte Werte: 0 –100.




**Tipp:**

Der Prozentsatz steuert, wann Autoscale mit dem Einschalten von getaggten Maschinen beginnt. Wenn der Prozentsatz unter den Schwellenwert fällt (Standardwert ist 10 %), beginnt Autoscale, die Maschinen mit Tag einzuschalten. Wenn der Prozentsatz den Schwellenwert überschreitet, wechselt Autoscale in den Ausschaltmodus. Bedenken Sie bei der Eingabe des Prozentwerts zwei Szenarios:

- Für Einzelsitzungs-OS-Bereitstellungsgruppen: Der Wert entspricht dem Prozentsatz aller ungetaggten Maschinen im Leerlauf. Beispiel: Sie haben 10 ungetaggte Einzelsitzungs-OS-Maschinen. Wenn nur noch eine ohne Sitzung übrig ist, schaltet Autoscale eine getaggte Maschine ein.
- Für Multisitzungs-OS-Bereitstellungsgruppen: Der Wert entspricht dem Prozentsatz

> der Gesamtkapazität (in Bezug auf den Lastindex) verfügbarer ungetaggter Maschinen. Beispiel: Sie haben 10 ungetaggte Multisitzungs-OS-Maschinen. Wenn sie zu 90 % geladen sind, schaltet Autoscale eine getaggte Maschine ein.

### Autoscale getaggter Maschinen mithilfe von PowerShell

Führen Sie die folgenden Schritte aus, um das PowerShell-SDK direkt zu verwenden:

1. **Erstellen Sie ein Tag.** Verwenden Sie den PowerShell-Befehl New-Brokertag, um ein Tag zu erstellen.
   - Beispiel: `$managed = New-BrokerTag Managed`. In diesem Fall heißt das Tag "Managed". Weitere Hinweise zum PowerShell-Befehl "New-Brokertag"finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Wenden Sie das Tag auf Maschinen an**. Verwenden Sie den PowerShell-Befehl Get-Brokermachine, um das Tag auf Maschinen in einem Katalog anzuwenden, die von Autoscale verwaltet werden sollen.
   - Beispiel: `Get-BrokerMachine -CatalogName "cloud"| Add-BrokerTag $managed.Name`. In diesem Fall hat der Katalog den Namen "Cloud".
   - Weitere Hinweise zum PowerShell-Befehl Get-Brokermachine finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Hinweis:**
   >
   > Sie fügen dem Katalog vielleicht neue Maschinen hinzu, nachdem Sie das Tag angewendet haben. Das Tag wird *NICHT* automatisch auf diese neuen Maschinen angewendet.

3. **Maschinen mit Tags der Bereitstellungsgruppe hinzufügen, die von Autoscale verwaltet werden soll.** Verwenden Sie den PowerShell-Befehl Get-BrokerDesktopGroup, um der Bereitstellungsgruppe, die die Maschinen enthält, eine Einschränkung nach Tag hinzuzufügen (d. h. "Starts auf Maschinen mit Tag beschränken: X").
   - Beispiel: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In diesem Fall ist die UID der Bereitstellungsgruppe 1.
   - Weitere Hinweise zum PowerShell-Befehl Get-BrokerDesktopGroup finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Nachdem Sie eine Tagbeschränkung angewendet haben, möchten Sie sie eventuell später aus der Bereitstellungsgruppe entfernen. Verwenden Sie dazu den PowerShell-Befehl Get-BrokerDesktopGroup.

Beispiel: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscal $null`. In diesem Fall ist die UID der Bereitstellungsgruppe 1.

> **Hinweis:**
>
> Maschinen ohne Tags werden nach dem Ausschalten durch die Benutzer automatisch neu gestartet. Dadurch wird sichergestellt, dass sie schneller für Workloads verfügbar sind. Dies kann für einzelne Desktopgruppen mit der `AutomaticRestartForUntaggedMachines` -Eigenschaft `Set-BrokerDesktopGroup` aktiviert oder deaktiviert werden. Weitere Informationen finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Maschinenkatalogkonfiguration**. Es gibt zwei Maschinenkataloge (C1 und C2).
  - Katalog C1 enthält 5 Maschinen (M1 bis M5), die lokal in den On-Premises-Bereitstellungen sind.
  - Katalog C2 enthält 5 Maschinen (M6 bis M10), die remote in den Cloudbereitstellungen sind.
- **Tagbeschränkung**. Ein Tag mit dem Namen “Cloud”wird erstellt und auf Maschinen M6 bis M10 in Katalog C2 angewendet.
- **Zonenkonfiguration**. Es werden zwei Zonen (Z1 und Z2) erstellt.
  - Zone Z1 mit Katalog C1 entspricht den On-Premises-Bereitstellungen.
  - Zone Z2 mit Katalog C2 entspricht den Cloudbereitstellungen.
- **Bereitstellungsgruppenkonfiguration**
  - Die Bereitstellungsgruppe hat 10 Maschinen (M1 bis M10), 5 Maschinen aus den Katalogen C1 (M1 bis M5) und 5 aus Katalog C2 (M6 bis M10).
  - Die Maschinen M1 bis M5 werden manuell eingeschaltet und bleiben während des gesamten Zeitplans eingeschaltet.
- **Autoscale-Konfiguration**
  - Der Kapazitätspuffer ist auf 10 % eingestellt.

  - Autoscale führt die Energieverwaltung nur für Maschinen mit dem Tag "Cloud"durch. In diesem Fall führt Autoscale die Energieverwaltung für die Cloudmaschinen M6 bis M10 durch.

- **Konfiguration für veröffentlichte Anwendung oder veröffentlichten Desktop**. Zoneneinstellungen werden beispielsweise für die veröffentlichten Desktops konfiguriert. Zone Z1 wird vor Zone Z2 bevorzugt für eine Benutzerstartanforderung.

  - Zone Z1 wird als bevorzugte Zone (Homezone) für die veröffentlichten Desktops konfiguriert.

Das Szenario hat folgenden Ablauf:

1. Kein Benutzer meldet sich an.
2. Die Anzahl der Benutzersitzungen erhöht sich.
3. Die Anzahl der Benutzersitzungen erhöht sich weiter, bis alle verfügbaren On-Premises-Maschinen verbraucht sind.
4. Weitere Benutzersitzungen beginnen.
5. Die Anzahl der Benutzersitzungen nimmt ab, weil Sitzungen beendet werden.
6. Die Benutzersitzungslast nimmt weiter ab, bis sie nur von On-Premises-Maschinen getragen wird.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Keine Benutzerlast (Anfangszustand)
  - Die On-Premises-Maschinen M1 bis M5 sind eingeschaltet.
  - Eine Maschine in der Cloud (z. B. M6) wird eingeschaltet. Die Maschine wird wegen des konfigurierten Kapazitätspuffers eingeschaltet. In diesem Fall gilt 10 (Anzahl der Maschinen) x 10.000 (Lastindex) x 10 % (konfigurierter Kapazitätspuffer) = 10.000. Daher wird eine Maschine eingeschaltet.
  - Der Lastindexwert aller eingeschalteten Maschinen (M1 bis M6) liegt bei einer Basislast (Lastindex = 0).
- Benutzer melden sich an
  - Die Sitzungen werden auf den Maschinen M1 bis M5 gehostet, dies entspricht der konfigurierten Zoneneinstellung, und es findet ein Lastausgleich zwischen diesen On-Premises-Maschinen statt.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) steigt.
  - Der Lastindexwert der eingeschalteten Maschine M6 liegt bei einer Basislast.
- Benutzer erhöhen die Last, alle On-Premises-Ressourcen werden verbraucht

  - Die Sitzungen werden auf den Maschinen M1 bis M5 gehostet, dies entspricht der konfigurierten Zoneneinstellung, und es findet ein Lastausgleich zwischen diesen On-Premises-Maschinen statt.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M6 bleibt bei einer Basislast.

- Ein weiterer Benutzer meldet sich an

  - Die Sitzung übersteigt die Kapazität der bevorzugten Zone und das Hosten wird an die Cloudmaschine M6 geleitet.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M6 erhöht sich und liegt nicht mehr bei einer Basislast. Wenn die gesamte freie Kapazität in Bezug auf den Lastindex auf unter 10.000 sinkt, beginnt Autoscale mit dem Einschalten einer zusätzlichen Maschine (M7), um den Bedarf gemäß konfiguriertem Kapazitätspuffer zu decken. Beachten Sie, dass es einige Zeit dauern kann, bis Maschine M7 eingeschaltet ist. Es könnte also eine Verzögerung geben, bis Maschine M7 bereit ist.

- Weitere Benutzer melden sich an

  - Die Sitzungen werden an Maschine M6 zum Hosten geleitet.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M6 steigt weiter, aber für die gesamte freie Kapazität liegt der Lastindex immer noch auf einem Niveau über 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M7 bleibt bei einer Basislast.

- Noch mehr Benutzer melden sich an

  - Nachdem die Maschine M7 bereit ist, werden die Sitzungen auf den Maschinen M6 und M7 gehostet und es findet ein Lastausgleich zwischen diesen Maschinen statt.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der Maschine M7 liegt nicht mehr bei einer Basislast.
  - Der Lastindexwert der eingeschalteten Maschinen (M6 und M7) steigt.
  - Die Kapazitätsreserven liegen nach wie vor auf einem Niveau über 10.000 gemäß Lastindex.

- Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.

  - Nachdem Benutzer sich von ihren Sitzungen abgemeldet haben oder diese aufgrund von Timeouts abgemeldet wurden, wird die freigegebene Kapazität auf Maschinen M1 bis M7 für das Hosting neuer Sitzungen wiederverwendet.
  - Steigt die gesamte freie Kapazität auf ein Niveau über 10.000 gemäß Lastindex, versetzt Autoscale eine der Cloudmaschinen (M6 bis M7) in den Drainingzustand. Sitzungen, die von anderen Benutzern gestartet wurden, werden dann nicht mehr an diese Maschine (z.

B. M7) weitergeleitet, es sei denn, es treten neue Änderungen auf (beispielsweise Benutzerlast steigt wieder oder andere Cloudmaschinen haben die geringste Last).

- Die Benutzersitzungslast nimmt weiter ab, bis ein oder mehrere Cloudmaschinen nicht mehr benötigt werden
  - Wenn alle Sitzungen auf Maschine M7 beendet wurden und die angegebene Ausschaltverzögerung abgelaufen ist, schaltet Autoscale M7 aus.
  - Der Lastindexwert aller eingeschalteten Maschinen (M1 bis M5) kann unter 10.000 fallen.
  - Der Lastindexwert der eingeschalteten Maschine (M6) nimmt ab.
- Die Anzahl der Benutzersitzungen nimmt weiter ab, bis keine Cloudmaschinen mehr benötigt werden.
  - Obwohl es keine Benutzersitzungen mehr auf Maschine M6 gibt, schaltet Autoscale sie nicht aus, da sie als freie Kapazität reserviert ist.
  - Autoscale behält die nicht zugewiesene Cloudmaschine M6 eingeschaltet aufgrund des konfigurierten Kapazitätspuffers. Diese Maschine wartet darauf, einem neuen Benutzer einen Desktop bereitzustellen.
  - Sitzungen werden nicht zum Hosten an Maschine M6 geleitet, solange die On-Premises-Maschinen verfügbare Kapazität haben.

## Dynamische Bereitstellung von Maschinen

November 28, 2022

Autoscale bietet die Möglichkeit, Maschinen dynamisch zu erstellen und zu löschen. Sie können das Feature mithilfe eines PowerShell-Skripts nutzen. Mit dem Skript können Sie die Anzahl der Maschinen in einer Bereitstellungsgruppe basierend auf aktuellen Lastbedingungen dynamisch nach oben oder unten skalieren.

Das Skript bietet u. a. folgende Vorteile:

- **Senkung der Speicherkosten**. Anders als bei Autoscale, das zur Senkung der Rechenkosten beiträgt, bietet das Skript eine kostengünstigere Lösung für die Bereitstellung von Maschinen.
- **Effektive Handhabung von Laständerungen**. Mit dem Skript können Sie Laständerungen handhaben, indem Sie die Anzahl der Maschinen basierend auf aktuellen Lastbedingungen in einer Bereitstellungsgruppe dynamisch nach oben oder unten skalieren.

### Skript herunterladen

Das PowerShell-Skript ist unter https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs verfügbar.

### Funktionsweise des Skripts

> **Wichtig:**
>
> - Sie können keinen Maschinenkatalog in mehreren Bereitstellungsgruppen für die Verwaltung per Skript angeben. Mit anderen Worten: Wenn mehrere Bereitstellungsgruppen einen Maschinenkatalog verwenden, funktioniert das Skript bei diesen Bereitstellungsgruppen nicht.
> - Sie können das Skript für ein und dieselbe Bereitstellungsgruppe nicht gleichzeitig von mehreren Sites aus ausführen.

Das Skript funktioniert auf Bereitstellungsgruppenebene. Es misst die Last (anhand Lastindex) und bestimmt, ob Maschinen erstellt oder gelöscht werden sollen.

Maschinen, die mit diesem Skript erstellt wurden, erhalten ein eindeutiges Tag (über den Parameter `ScriptTag`) zur späteren Identifizierung. Das Erstellen und Löschen von Maschinen basiert auf:

- **Maximale prozentuale Last einer Bereitstellungsgruppe**. Gibt die maximale Last an, bei der Maschinen für die Handhabung weiterer Last durch Autoscale erstellt werden sollen. Wenn dieser Schwellenwert überschritten wird, werden Maschinen gruppenweise erstellt, damit die aktuelle Last auf oder unter den Schwellenwert fällt.
- **Minimale prozentuale Last einer Bereitstellungsgruppe**. Gibt die minimale Last an, bei der mit dem Skript erstellte Maschinen, die keine aktiven Sitzungen haben, gelöscht werden sollen. Wenn dieser Schwellenwert unterschritten wird, werden Maschinen, die mit dem Skript erstellt wurden und keine aktiven Sitzungen haben, gelöscht.

Das Skript soll eine Bereitstellungsgruppe überwachen und Maschinen erstellen und löschen, wenn das Auslösekriterium erfüllt ist. Es funktioniert auf Ausführungsbasis. Dies bedeutet, dass Sie das Skript regelmäßig ausführen müssen, damit es wie vorgesehen funktioniert. Es wird empfohlen, das Skript in einem Mindestintervall von fünf Minuten auszuführen. Dadurch wird die Reaktionsfähigkeit insgesamt verbessert.

Das Skript verwendet folgende Parameter:

| Parameter | Typ | Standardwert | Beschreibung |
| --- | --- | --- | --- |
| DeliveryGroupName | Zeichenfolge | X | Name der Bereitstellungsgruppe, die auf die aktuelle Last überwacht werden soll. Sie können eine durch Semikola getrennte Liste von Namen angeben. Beispiel: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`. |
| XdProfileName | Zeichenfolge | X | Name des Profils, das für die Authentifizierung bei Remoteservern verwendet werden soll. Weitere Informationen zur Authentifizierung bei Remoteservern mithilfe dieses Parameters finden Sie unter Authentifizierungs-API. |
| HighWatermark | Ganzzahl | 80 | Maximale prozentuale Last (anhand Lastindex), bei der Maschinen für die Handhabung zusätzlicher Last durch Autoscale erstellt werden sollen. |

| Parameter | Typ | Standardwert | Beschreibung |
|---|---|---|---|
| LowWatermark | Ganzzahl | 15 | Minimale prozentuale Last (anhand Lastindex), bei der mit dem Skript erstellte Maschinen, die keine aktiven Sitzungen haben, gelöscht werden sollen. |
| MachineCatalogName | Zeichenfolge | X | Name des Maschinenkatalogs, in dem Maschinen erstellt werden sollen. |
| MaximumCreatedMachines | Ganzzahl | -1 | Maximale Anzahl an Maschinen, die in einer angegebenen Bereitstellungsgruppe erstellt werden können. Ist der Wert gleich oder kleiner 0, verarbeitet das Skript diesen Parameter nicht. |
| ScriptTag | Zeichenfolge | AutoscaledScripted | Tag, das auf Maschinen angewendet wird, die mit dem Skript erstellt werden. |
| EventLogSource | Zeichenfolge | X | Name der Quelle, der in der Windows-Ereignisanzeige angezeigt wird. |

> **Hinweis:**
>
> Ein "X"gibt an, dass für diesen Parameter kein Standardwert angegeben ist.

Standardmäßig erfordert das Skript alle Parameter (mit Ausnahme von `ScriptTag`), wenn es zum ersten Mal ausgeführt wird. Bei nachfolgenden Ausführungen sind nur die Parameter `DeliveryGroupName` und `XdProfileName` erforderlich. Optional können Sie die minimale und

maximale prozentuale Last aktualisieren.

Beim ersten Ausführen des Skripts müssen Sie eine einzelne Bereitstellungsgruppe angeben. Das Skript funktioniert *nicht*, wenn Sie beispielsweise beim ersten Ausführen mit dem folgenden PowerShell-Befehl zwei Bereitstellungsgruppen angeben:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1; dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Geben Sie stattdessen zunächst eine einzelne Bereitstellungsgruppe (in diesem Beispiel dg1) mit dem folgenden Befehl an:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1 '-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Verwenden Sie dann den folgenden Befehl, um das Skript für die zweite Bereitstellungsgruppe (in diesem Beispiel dg2) auszuführen:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

### Voraussetzungen

Um das Skript auszuführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die Maschine befindet sich in der Domäne, in der Maschinen erstellt werden.
- Das Remote PowerShell SDK ist auf dieser Maschine installiert. Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.
- Weitere Voraussetzungen:
  - Zu überwachende Bereitstellungsgruppe
  - Ein mit den Maschinenerstellungsdiensten (MCS) erstellter Maschinenkatalog, der über ein zugeordnetes Provisioningschema (Vorlage) verfügt
  - Ein Identitätspool, der dem Provisioningschema zugeordnet ist
  - Eine zu erstellende Ereignisprotokollquelle, damit das Skript Informationen in das Windows-Ereignisprotokoll schreiben kann
  - Ein sicherer Client, mit dem die Authentifizierung bei Remoteservern möglich ist

### Berechtigungen, Empfehlungen und Hinweise

Beachten Sie beim Ausführen des Skripts Folgendes:

- Zur Authentifizierung bei Remoteservern mit dem Parameter `XdProfileName` müssen Sie ein Authentifizierungsprofil mithilfe eines sicheren API-Zugriffsclients definieren, der in der Citrix Cloud-Konsole erstellt wurde. Weitere Informationen finden Sie unter Authentifizierungs-API.
- Sie benötigen Berechtigungen zum Erstellen und Löschen von Maschinenkonten in Active Directory.
- Es wird empfohlen, das PowerShell-Skript mit der Windows-Aufgabenplanung zu automatisieren. Weitere Informationen finden Sie unter Erstellen einer automatisierten Aufgabe mit der Windows-Aufgabenplanung.
- Wenn Sie das Skript Informationen (z. B. Fehler und Aktionen) in das Windows-Ereignisprotokoll schreiben soll, müssen Sie einen Quellnamen mit dem Cmdlet `New-EventLog` angeben. Zum Beispiel: `New-EventLog -LogName Application –Source <sourceName>`. Sie können die Ereignisse dann im Bereich **Anwendung** der Windows-Ereignisanzeige anzeigen.
- Treten während der Ausführung des Skripts Fehler auf, führen Sie das Skript manuell aus und beheben Sie dann Probleme, indem Sie Skriptüberprüfungen durchführen.

### Authentifizierungs-API

Bevor Sie das Skript ausführen, müssen Sie ein Authentifizierungsprofil mithilfe eines sicheren API-Zugriffsclients definieren. Sie müssen den sicheren Client mit dem Konto erstellen, unter dem das Skript ausgeführt wird.

Der sichere Client muss die folgenden Berechtigungen haben:

- Erstellen und Löschen von Maschinen mit MCS.
- Bearbeiten von Maschinenkatalogen (zum Hinzufügen und Entfernen von Maschinen).
- Bearbeiten von Bereitstellungsgruppen (zum Hinzufügen und Entfernen von Maschinen).

Wenn Sie einen sicheren Client erstellen, stellen Sie sicher, dass Ihr Konto über die oben genannten Berechtigungen verfügt, da der sichere Client automatisch die Berechtigungen von Ihrem aktuellen Konto erbt.

Führen Sie die folgenden Schritte aus, um einen sicheren Client zu erstellen:

1. Melden Sie sich an Citrix Cloud an und navigieren Sie zu **Identitäts- und Zugriffsverwaltung > API-Zugriff**.
2. Geben Sie einen Namen für den sicheren Client ein und klicken Sie auf **Client erstellen**.

Verwenden Sie den PowerShell-Befehl `Set-XDCredentials` für die Authentifizierung bei Remoteservern. Beispiel:

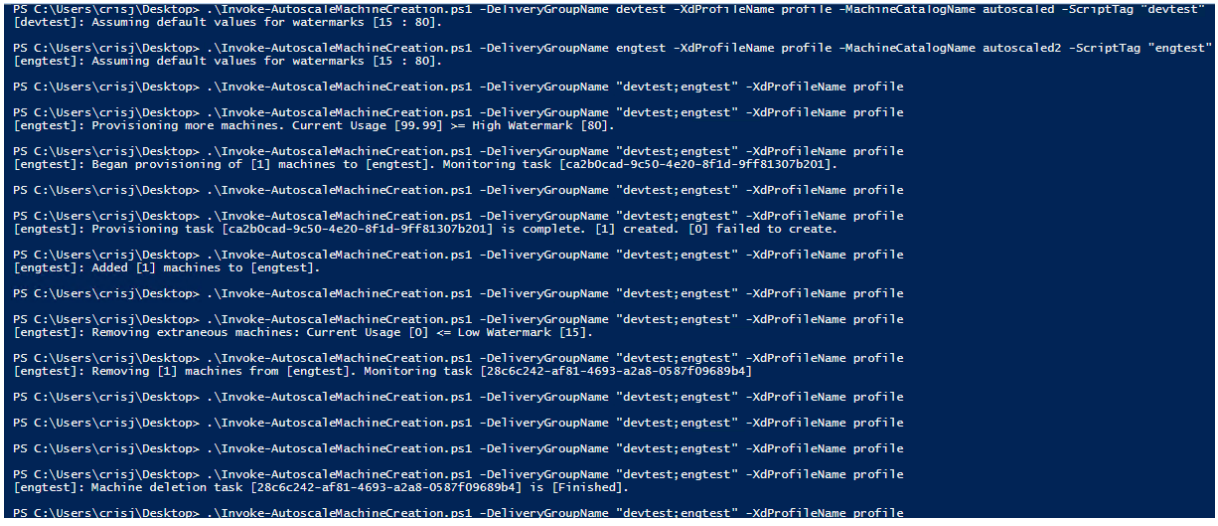
- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

### Erstellen einer automatisierten Aufgabe mit der Windows-Aufgabenplanung

Sie können das PowerShell-Skript mit der Windows-Aufgabenplanung automatisieren. Dadurch kann das Skript automatisch in bestimmten Intervallen oder bei Auftreten bestimmter Bedingungen ausgeführt werden. Um dieses Skript mit der Windows-Aufgabenplanung auszuführen, müssen Sie auf der Registerkarte **Task erstellen > Einstellungen** die Option **Keine neue Instanz starten** auswählen. Dadurch wird verhindert, dass die Windows-Aufgabenplanung eine neue Instanz des Skripts ausführt, wenn dieses bereits ausgeführt wird.

### Beispiel für die Skriptausführung

Unten finden Sie ein Beispiel für die Ausführung des Skripts. Beachten Sie, dass die Skriptdatei mehrmals aufgerufen wird. In diesem Beispiel wird eine Sitzung gestartet und dann beendet, um die Last zu simulieren.




### Prüfliste zur Problembehandlung für das Skript

Das Skript schreibt Informationen (z. B. Fehler und Aktionen) in das Windows-Ereignisprotokoll. Anhand der Informationen können Sie Probleme mit der Skriptausführung behandeln. Dabei kann folgende Prüfliste zur Fehlerbehebung hilfreich sein:

- Fehler bei der Kommunikation mit Remoteservern. Mögliche Maßnahmen:
  - Überprüfen Sie die Verbindung zum Server.

  - Vergewissern Sie sich, dass der verwendete API-Schlüssel gültig ist.

- Fehler beim Erstellen von Maschinen. Mögliche Maßnahmen:
  - Vergewissern Sie sich, dass das Benutzerkonto, auf dem das Skript ausgeführt wird, über ausreichende Berechtigungen zum Erstellen von Benutzerkonten in der Domäne verfügt.
  - Vergewissern Sie sich, dass der Benutzer, der den API-Schlüssel erstellt hat, Berechtigungen zum Bereitstellen von Maschinen mit MCS hat.
  - Überprüfen Sie die Gültigkeit des Maschinenkatalogs (das heißt, das Image ist noch vorhanden und in gutem Zustand).
- Fehler beim Hinzufügen von Maschinen zu einem Maschinenkatalog oder einer Bereitstellungsgruppe. Mögliche Maßnahmen:
  - Vergewissern Sie sich, dass der Benutzer, der den API-Schlüssel erstellt hat, Berechtigungen zum Hinzufügen und Entfernen von Maschinen zu und aus Maschinenkatalogen und Bereitstellungsgruppen verfügt.

## Benachrichtigungen zur Benutzerabmeldung (früher Erzwingen von Benutzerabmeldungen)

June 5, 2023

> **Wichtig:**
>
> Das Feature ist nur in der Autoscale-Benutzeroberfläche für App-basierte Multisitzungs-Bereitstellungsgruppen verfügbar.

Zur Kosteneinsparung können Sie mit Autoscale die Abmeldung von fortbestehenden Sitzungen erzwingen. Sie können hierfür eine benutzerdefinierte Benachrichtigung an die Benutzer senden und einen Kulanzzeitraum angeben, nach dessen Ablauf die Sitzungen zwangsweise abgemeldet werden. Dies geschieht nur bei Maschinen im Drainingzustand und nicht bei allen eingeschalteten Maschinen. Um potenziellen Datenverlust durch erzwungene Benutzerabmeldungen zu vermeiden, können Sie dieses Feature so konfigurieren, dass nur Abmeldeerinnerungen gesendet werden, ohne dass eine Benutzerabmeldung erzwungen wird.

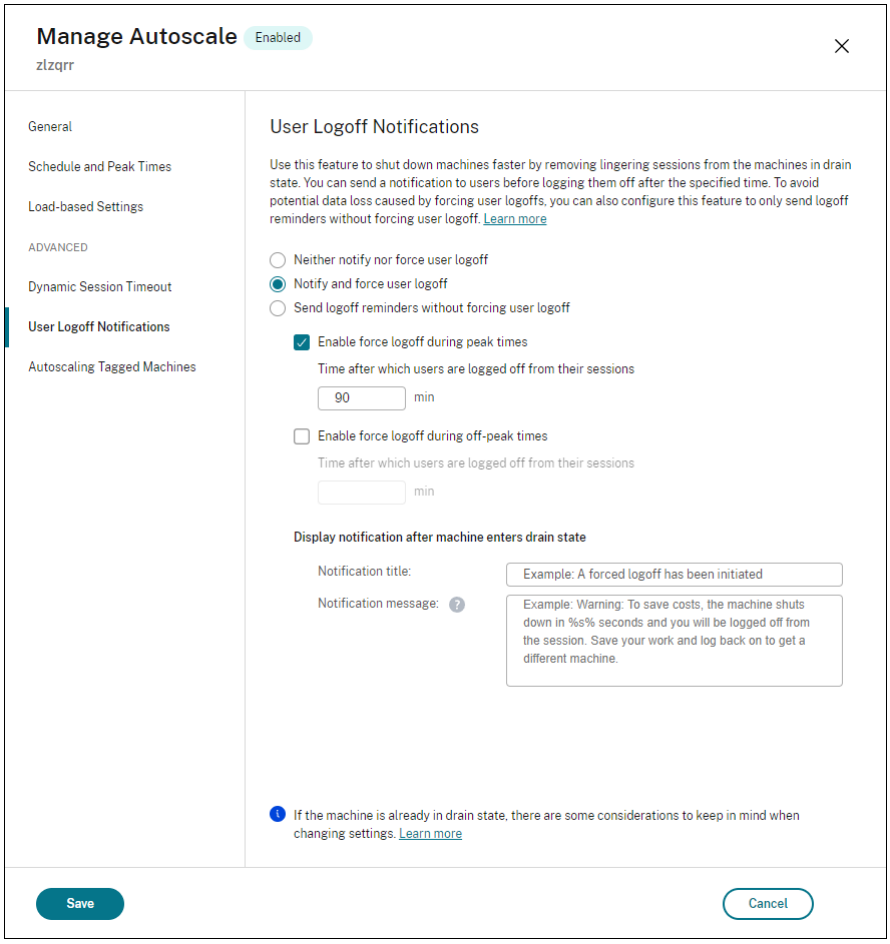
Sie haben folgende Optionen:

- **Benutzer benachrichtigen und Abmeldung erzwingen**
- **Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen**
- **Weder benachrichtigen noch Benutzerabmeldung erzwingen**

### Benutzer benachrichtigen und Abmeldung erzwingen

Wenn diese Option ausgewählt ist, meldet Autoscale Benutzer nach Ablauf der unten angegebenen Zeit von ihren Sitzungen ab.




‘**Abmeldung erzwingen während Spitzenzeit’aktivieren**. Wenn diese Option ausgewählt ist, meldet Autoscale Benutzer in Spitzenzeiten nach Ablauf der angegebenen Zeit von ihren Sitzungen ab.

‘**Abmeldung erzwingen während Nebenzeiten’aktivieren**. Wenn diese Option ausgewählt ist, meldet Autoscale Benutzer in Nebenzeiten nach Ablauf der angegebenen Zeit von ihren Sitzungen ab.

**Benachrichtigung anzeigen, nachdem die Maschine in den Draining-Zustand wechselt** Ermöglicht das Senden von Benachrichtigungen an Benutzer, nachdem ihre Maschine in den Drainingzustand versetzt wurde.

- **Benachrichtigungstitel**. Hier können Sie einen Titel für die Benachrichtigung angeben, die an Benutzer gesendet werden soll. Beispiel:`A forced logoff has been initiated.`
- **Benachrichtigung**. Hier können Sie den Inhalt der Benachrichtigung angeben, die an Be-

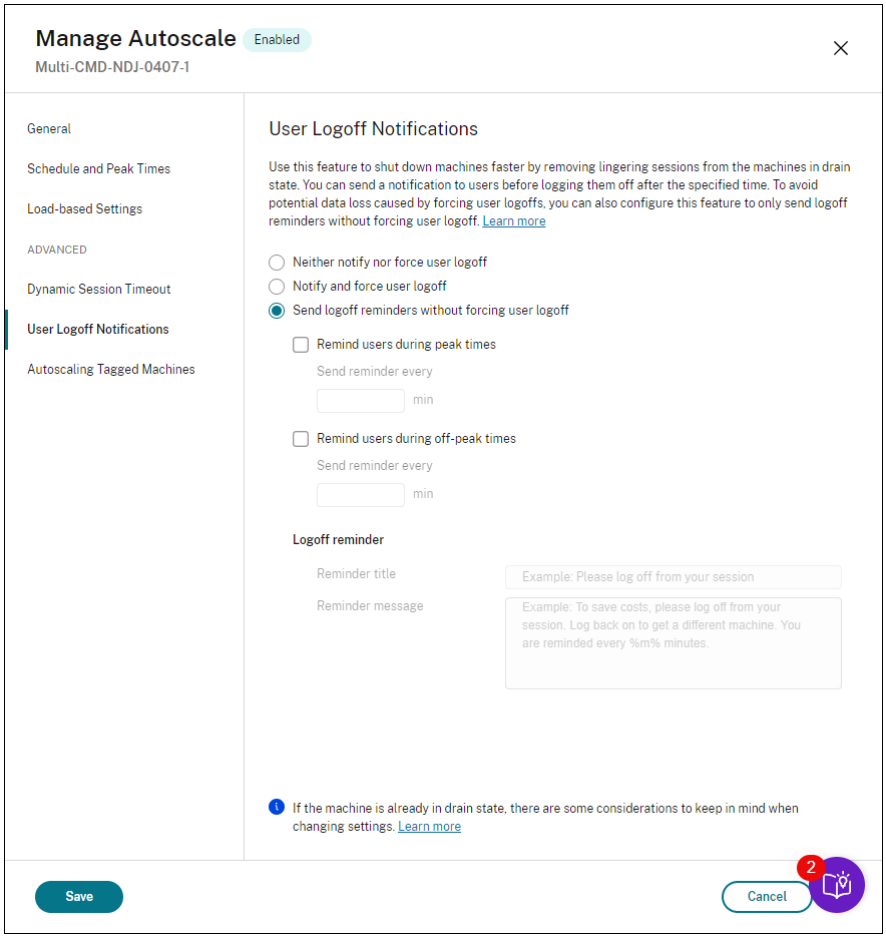
 

nutzer gesendet werden soll. Sie können %s% oder %m% als Variablen verwenden, um die angegebene Uhrzeit in der Nachricht anzugeben. Um die Zeit in Sekunden auszudrücken, verwenden Sie %s%. Um die Zeit in Minuten auszudrücken, verwenden Sie %m%. Beispiel:

```
Warning: To save costs, the machine shuts down in %s% seconds and
 you will be logged off from the session. Save your work and log
back on to get a different machine.
```

### Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen

Wenn diese Option ausgewählt ist, erhalten Benutzer eine Erinnerung, sich von ihrer Maschine abzumelden, nachdem diese in den Drainingzustand versetzt wurde. Diese Erinnerung kann so konfiguriert werden, dass sie in dem unten angegebenen Intervall gesendet wird.




**Benutzer während der Spitzenzeiten erinnern**. Wenn diese Option ausgewählt ist, erhalten Benutzer eine Erinnerung, sich zu Spitzenzeiten alle X Minuten von ihren Sitzungen abzumelden (X steht für die angegebene Zeit).

**Benutzer außerhalb der Spitzenzeiten erinnern**. Wenn diese Option ausgewählt ist, erhalten Benutzer eine Erinnerung, sich während Nebenzeiten alle X Minuten von ihren Sitzungen abzumelden (X

steht für die angegebene Zeit).

**Abmeldeerinnerung**. Ermöglicht das Konfigurieren der Erinnerung, die an Benutzer gesendet wird, nachdem ihre Maschine in den Drainingzustand versetzt wurde.

- **Titel der Erinnerung**. Hier können Sie einen Titel für die Erinnerung angeben, die an Benutzer gesendet werden soll. Beispiel: `Please log off from your session`.
- **Erinnerungsnachricht**. Hier können Sie eine Nachricht angeben, die an Benutzer gesendet werden soll. Beispiel: `Please log off from your session and log back on to save costs`.

### Weder benachrichtigen noch Benutzerabmeldung erzwingen

Wird diese Option ausgewählt, erzwingt Autoscale keine Abmeldung der Benutzer von Maschinen im Drainingzustand und es sendet keine Benachrichtigung zum manuellen Wechsel zu einer anderen Maschine.

### Überlegungen

Wenn sich die Maschine bereits im Drainingzustand befindet, beachten Sie beim Ändern der Einstellungen Folgendes:

- Wenn Sie die Einstellung von **Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen** in **Benutzer benachrichtigen und Abmeldung erzwingen** ändern, wird die neue Einstellung sofort wirksam.
- Wenn Sie die Einstellung von **Benutzer benachrichtigen und Abmeldung erzwingen** in **Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen** ändern, wird die neue Einstellung erst wirksam, wenn die Maschine das nächste Mal in den Drainingzustand wechselt. Der Benutzer wird nach wie vor zur Abmeldung gezwungen.

## Wirksamkeit von Autoscale-Einstellungen analysieren

February 21, 2024

Um diese Funktion zu verwenden, aktivieren Sie den Schalter **Einblicke in Autoscale** in **DaaS > Home > Vorschaufunktionen**. Es kann etwa 15 Minuten dauern, bis **Einblicke in Autoscale** nach der Aktivierung angezeigt wird.

Sie können die Wirksamkeit der Autoscale-Einstellungen anhand der Maschinennutzung in der Vorwoche analysieren. Die Analyse ermöglicht Ihnen folgende Erkenntnisse:

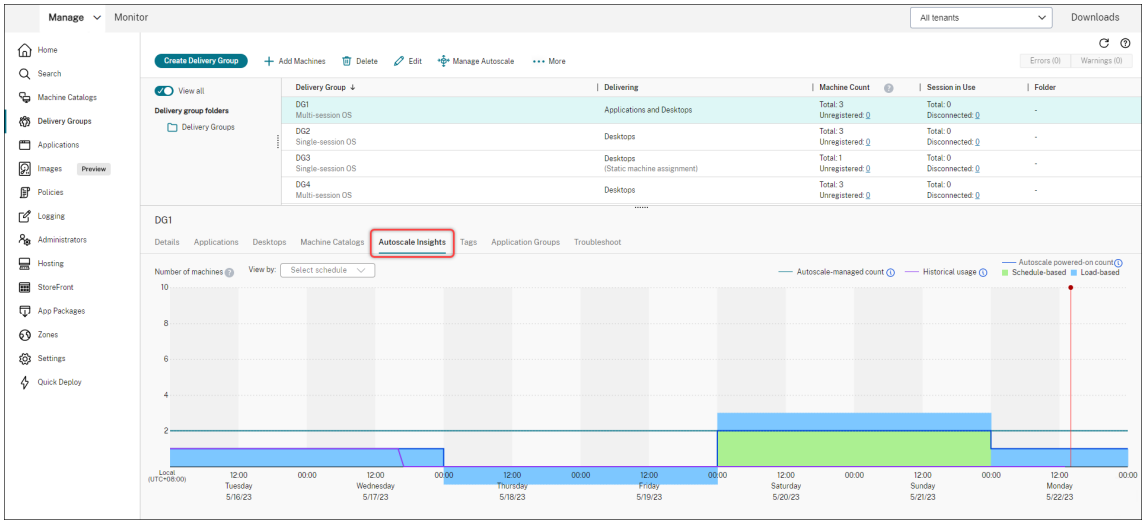
 

- Identifizieren unnötiger Mehrkosten durch Überversorgung.
- Prüfung auf Beeinträchtigung der Benutzererfahrung durch Unterversorgung.
- Sicherstellen, dass die bereitgestellte Kapazität der Maschinennutzung entspricht.

Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

1. Wählen Sie eine Autoscale-fähige Bereitstellungsgruppe aus.
2. Klicken Sie unten auf die Registerkarte **Einblicke in Autoscale**.

   Das angezeigte Diagramm vergleicht die Maschinennutzungsdaten der Vorwoche mit der Maschinenanzahl, die gemäß den Autoscale-Einstellungen eingeschaltet werden soll.




* Die rote vertikale Linie kennzeichnet den aktuellen Zeitpunkt.

Die folgende Tabelle enthält Beschreibungen der im Diagramm dargestellten Metriken.

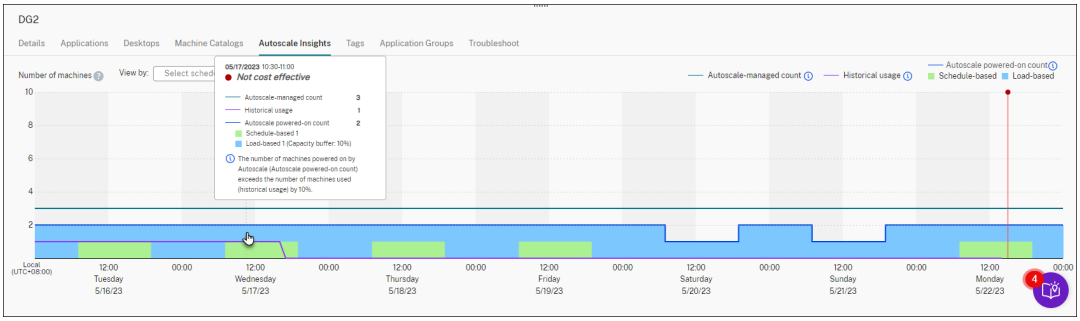
| Metrik | Beschreibung |
| --- | --- |
| Durch Autoscale verwaltet –Anzahl | Gesamtzahl der durch Autoscale verwalteten Maschinen. Anzahl der durch Autoscale verwalteten Maschinen = Sämtliche Maschinen in der Bereitstellungsgruppe —Anzahl der Maschinen im Wartungsmodus —Anzahl der Maschinen, die nicht für Autoscale getaggt sind (bei aktiviertem Autoscale-Feature mit Tags). |

| Metrik | Beschreibung |
| --- | --- |
| Durch Autoscale eingeschaltet –Anzahl | Gesamtzahl der Maschinen, die durch Autoscale eingeschaltet wurden. Anzahl der durch Autoscale eingeschalteten Maschinen = Maschinenanzahl auf Zeitplanbasis + Maschinenanzahl auf Lastbasis. |
| Historische Nutzung | Anzahl der Maschinen, die Benutzern bereitgestellt wurden. |
| Zeitplanbasiert | Anzahl der Maschinen, die gemäß den zeitplanbasierten Autoscale-Einstellungen eingeschaltet werden (**Hinweis:** Zeitplanbasierte Einstellungen gelten nicht für Bereitstellungsgruppen mit statischem Einzelsitzungs-OS). |
| Lastbasiert | Anzahl der Maschinen, die gemäß den lastbasierten Autoscale-Einstellungen eingeschaltet werden. |

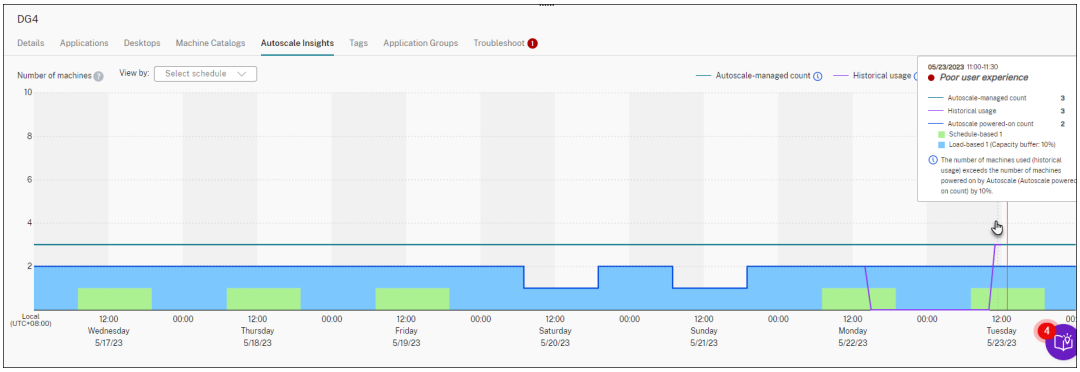
3. Um die Wirksamkeit der Autoscale-Einstellungen zu einem bestimmten Zeitpunkt zu überprüfen, bewegen Sie den Mauszeiger über das Zeitfenster in der Grafik. Es erscheint ein Informationsfeld mit den Vergleichsergebnissen und Details zur Maschinenanzahl:

   - **Nicht kosteneffektiv**. Die historische Nutzung beträgt weniger als 90 % der Autoscale-Einstellungen (“Durch Autoscale eingeschaltet –Anzahl”). Kapazitäten könnten daher verschwendet werden.

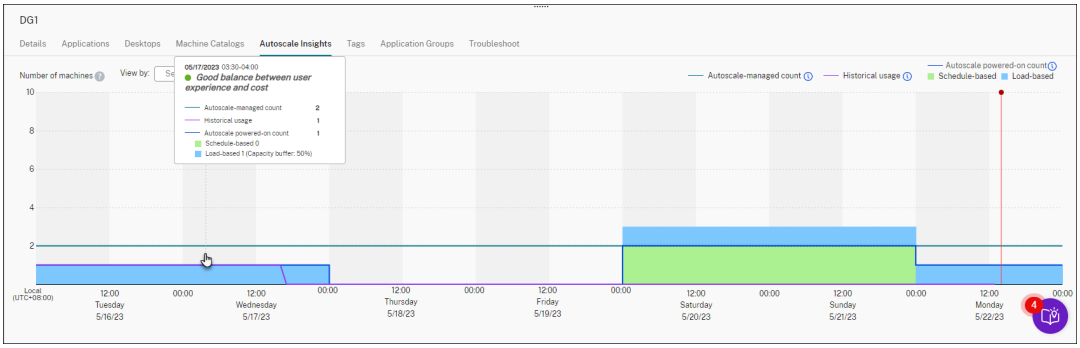



   - **Schlechte Benutzererfahrung**. Die historische Nutzung beträgt mehr als 110 % der Autoscale-Einstellungen (“Durch Autoscale eingeschaltet –Anzahl”). Dies kann beim Einschalten von Maschinen zu längeren Wartezeiten führen.

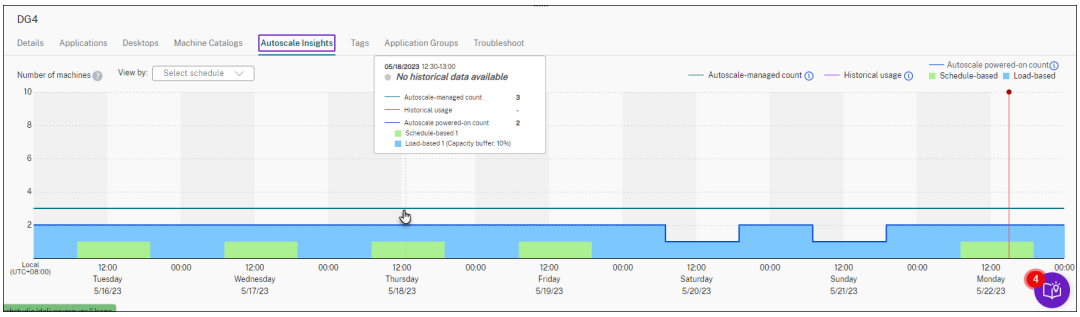
 




- **Gutes Gleichgewicht zwischen Benutzererfahrung und Kosten**. Die Differenz zwischen historischer Nutzung und Autoscale-Einstellungen (“Durch Autoscale eingeschaltet – Anzahl”) beträgt weniger als 10 %. Die Autoscale-Einstellungen sind auf die historische Nutzung abgestimmt.




- **Keine historischen Daten verfügbar**. Es sind keine historischen Daten verfügbar. Dies kann daran liegen, dass Autoscale vor weniger als einer Woche für die Bereitstellungsgruppe aktiviert wurde.




4. Um einen Datumsbereich gemäß einem Autoscale-Zeitplan hervorzuheben, wählen Sie den Zeitplan im Feld **Anzeigen nach**.
5. Passen Sie die Autoscale-Einstellungen gemäß Ihrer Analyse an. Weitere Informationen finden Sie unter Zeitplan- und Lasteinstellungen.

# Broker PowerShell SDK-Befehle

November 16, 2023

Sie können Autoscale für Bereitstellungsgruppen mit dem Broker PowerShell SDK konfigurieren. Um Autoscale mit PowerShell-Befehlen zu konfigurieren, müssen Sie Remote PowerShell SDK Version 7.21.0.12 oder höher verwenden. Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.

## Set-BrokerDesktopGroup

Deaktiviert oder aktiviert vorhandene BrokerDesktopGroup oder ändert deren Einstellungen. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Beispiele

Die folgenden Beispiele verdeutlichen die Verwendung der PowerShell-Cmdlets:

Autoscale aktivieren

- Angenommen, Sie möchten Autoscale für die Bereitstellungsgruppe "MyDesktop"aktivieren. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled $true
    ```

Kapazitätspuffer für Spitzen- und Nebenzeiten separat festlegen

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"den Kapazitätspuffer für Spitzenzeiten auf 20 % und für Nebenzeiten auf 10 % festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10
    ```

Einstellung **Timeout für "Wenn getrennt"** konfigurieren

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"den Wert **Timeout für "Wenn getrennt"** auf 60 Minuten für Spitzenzeiten und auf 30 Minuten für Nebenzeiten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30
    ```

 
    ```

Einstellung **Timeout für "Wenn abgemeldet"** konfigurieren

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"den Wert **Timeout für "Wenn abgemeldet"** auf 60 Minuten für Spitzenzeiten und auf 30 Minuten für Nebenzeiten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

Einstellung **Ausschaltverzögerung** konfigurieren

- Angenommen, Sie möchten die Ausschaltverzögerung für die Bereitstellungsgruppe "MyDesktop"auf 15 Minuten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15`

Konfigurieren eines Zeitraums, in dem die Ausschaltverzögerung nicht angewendet wird

- Angenommen, Sie möchten die Ausschaltverzögerung für die Bereitstellungsgruppe "MyDesktop"auf 30 Minuten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh 30.`

Eigenschaft **Maschineninstanzkosten** konfigurieren

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"die Maschineninstanzkosten pro Stunde auf 0,2 Dollar festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2`

### New-BrokerPowerTimeScheme

Erstellt ein BrokerPowerTimeScheme für eine Bereitstellungsgruppe. Weitere Informationen finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

#### Beispiel

Angenommen, Sie möchten ein Energiezeitschema für die Bereitstellungsgruppe mit dem UID-Wert 3 erstellen. Das neue Schema gilt für Wochenenden, Montage und Dienstage. Der Zeitraum von 8:00 bis 18:30 Uhr gilt als Spitzenzeit für die Tage im ausgewählten Zeitplan. Für Spitzenzeiten beträgt die Poolgröße (die Anzahl der eingeschalteten Maschinen) 20. Für Nebenzeiten sind es 5 Maschinen. Sie können den PowerShell-Befehl `Set-BrokerDesktopGroup` verwenden. Beispiel:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

### Parameter für dynamische Sitzungstimeouts

Die folgenden Broker PowerShell SDK-Cmdlets wurden für dynamische Sitzungstimeouts erweitert, indem mehrere neue Parameter unterstützt werden:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Zu diesen Parametern gehören:

- **DisconnectPeakIdleSessionAfterSeconds:** Zeit in Sekunden, nach der eine Leerlaufsitzung während der Spitzenzeit getrennt wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Spitzenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Spitzenzeit.
- **DisconnectOffPeakIdleSessionAfterSeconds:** Zeit in Sekunden, nach der eine Leerlaufsitzung während der Nebenzeit getrennt wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Nebenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Nebenzeit.
- **LogoffPeakDisconnectedSessionAfterSeconds:** Zeit in Sekunden, nach der eine getrennte Sitzung während der Spitzenzeit beendet wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Spitzenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Spitzenzeit.
- **LogoffOffPeakDisconnectedSessionAfterSeconds:** Zeit in Sekunden, nach der eine getrennte Sitzung während der Nebenzeit beendet wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Nebenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Nebenzeit.

#### Beispiel

Einsatzbeispiel: Sie möchten das Timeout für Leerlaufsitzungen während der Spitzenzeit für die Bereitstellungsgruppe “MyDesktop”auf 3.600 Sekunden einstellen. Verwenden Sie den PowerShell-Befehl

`Set-BrokerDesktopGroup`. Beispiel:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte 3600`

Dadurch werden in der Nebenzeit Sitzungen der Bereitstellungsgruppe “MyDesktop”getrennt, die länger als eine Stunde im Leerlauf sind.

## Cloud Health Check

December 9, 2022

> **Hinweis:**
>
> Cloud Health Check ist in Citrix DaaS integriert. Die Integration ist als Aktion “Systemintegritätsprüfung ausführen”in der Verwaltungsoberfläche “Vollständige Konfiguration”verfügbar. Weitere Informationen finden Sie unter Probleme bei der VDA-Registrierung und beim Sitzungsstart behandeln.

Cloud Health Check prüft die Integrität und Verfügbarkeit der Site und ihrer Komponenten. Sie können Integritätsprüfungen an Virtual Delivery Agents (VDAs), StoreFront-Servern und der Profilverwaltung ausführen. Bei VDA-Integritätsprüfungen wird die mögliche Ursache häufiger Probleme bei der VDA-Registrierung und beim Sitzungsstart gesucht.

Werden während der Prüfungen Probleme gefunden, erzeugt Cloud Health Check einen detaillierten Bericht mit Aktionen zur Problembehebung. Jedes Mal, wenn Cloud Health Check gestartet wird, sucht es im Netzwerk für die Inhaltsübermittlung (CDN) nach der neuesten Version der Skripts und lädt neue Skripts automatisch herunter, wenn sie nicht auf der lokalen Maschine vorliegen. Cloud Health Check wählt immer die neueste lokale Version von Skripts zum Durchführen der Prüfungen.

> **Hinweis:**
>
> Cloud Health Check wird nicht bei jeder Ausführung aktualisiert.

Führen Sie in einer Citrix Cloud-Umgebung Cloud Health Check auf einer zu einer Domäne gehörenden Maschine aus, um Prüfungen auf einem oder mehreren VDAs oder StoreFront-Servern durchzuführen.

> **Hinweis:**
>
> Sie können Cloud Health Check nicht auf einem Cloud Connector installieren oder ausführen.

Das Protokoll für die Cloud-Integritätsprüfung ist in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. Diese Datei kann zur Problembehandlung verwendet werden.

Einführung in die Cloud-Integritätsprüfung:

Einsatz der Cloud-Integritätsprüfung:

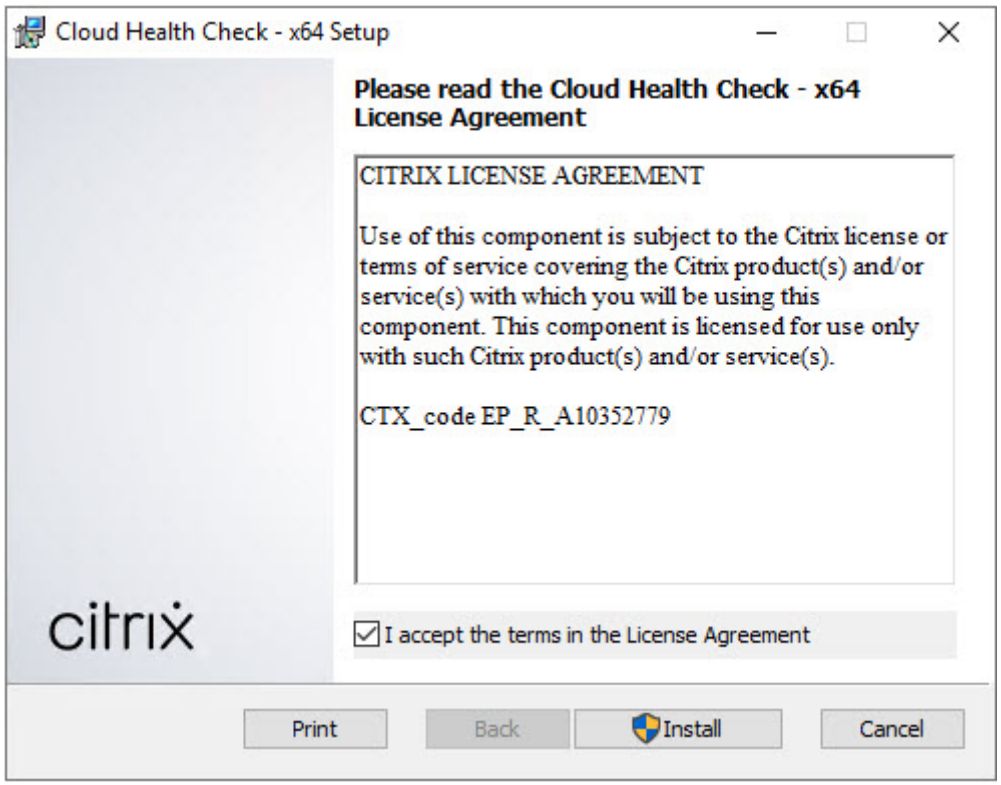
 

### Installation

Um die Umgebung für die Installation von Cloud Health Check vorzubereiten, benötigen Sie eine Windows-Maschine, die zur Domäne gehört.

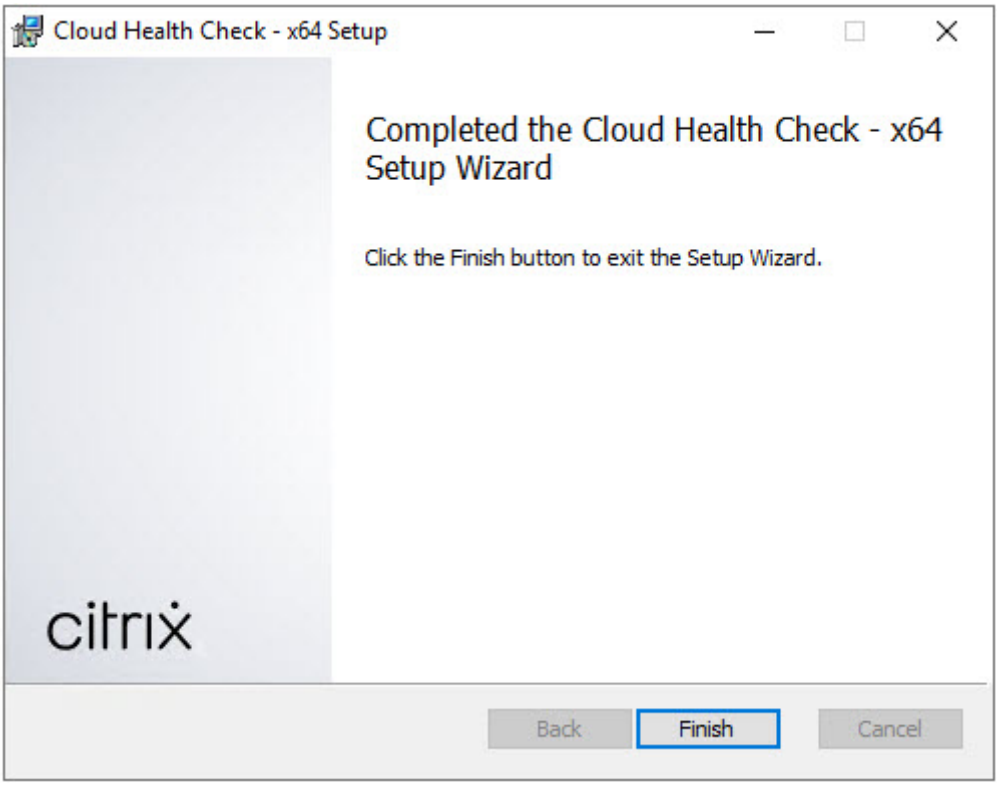
> **Hinweis:**
>
> Sie können Cloud Health Check nicht auf einem Cloud Connector installieren oder ausführen.

1. Laden Sie auf der zur Domäne gehörenden Maschine das Installationsprogramm für Cloud Health Check herunter.
2. Doppelklicken Sie auf die Datei CloudHealthCheckInstaller_x64.msi.
3. Klicken Sie auf das Feld, um die Bedingungen zu akzeptieren.
4. Klicken Sie auf Installieren.




5. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.




### Berechtigungen und Anforderungen

Berechtigungen:

- Ausführen von Integritätsprüfungen:
  - Sie müssen Mitglied der Gruppe “Domänenbenutzer”sein.
  - Sie müssen Volladministrator sein oder eine benutzerdefinierte Rolle mit Lesezugriff und Berechtigung zum **Ausführen von Umgebungstests** für die Site haben.
  - Legen Sie die Skriptausführungsrichtlinie mindestens auf `RemoteSigned` fest, damit die Skripts ausgeführt werden können. Beispiel: `Set-ExecutionPolicy RemoteSigned`. **Hinweis:** Andere Skriptausführungsberechtigungen funktionieren ggf. auch.
- Verwenden Sie **Als Administrator ausführen**, wenn Sie Cloud Health Check starten.

VDA- oder StoreFront-Maschinen, auf denen Sie Integritätsprüfungen ausführen:

- Das Betriebssystem muss 64-Bit sein.
- Cloud Health Check muss mit der Maschine kommunizieren können.
- Die Datei- und Druckerfreigabe muss aktiviert sein.
- PSRemoting und WinRM müssen aktiviert sein. Auf der Maschine muss PowerShell 3.0 oder höher ausgeführt werden.

- WMI-Zugriff (Windows Management Infrastructure) muss auf der Maschine aktiviert sein.

### Informationen zu Integritätsprüfungen

Die Daten der Integritätsprüfung werden in Ordnern unter `C:\ProgramData\Citrix\TelemetryService\` gespeichert.

#### VDA-Integritätsprüfungen

Für die Registrierung auf dem VDA überprüft Cloud Health Check Folgendes:

- Installation der VDA-Software
- Domänenmitgliedschaft der VDA-Maschine
- Verfügbarkeit der VDA-Kommunikationsports
- VDA-Dienststatus
- Konfiguration der Windows-Firewall
- Kommunikation mit dem Controller
- Zeitsynchronisierung mit dem Controller
- VDA-Registrierungsstatus

Bei Sitzungsstarts auf VDAs überprüft Cloud Health Check Folgendes:

- Verfügbarkeit der Sitzungsstart-Kommunikationsports
- Status der Sitzungsstartdienste
- Windows-Firewallkonfiguration für den Sitzungsstart
- Clientzugriffslizenzen für VDA-Remotedesktopdienste
- VDA-Anwendungsstartpfad
- Registrierungseinstellungen für den Sitzungsstart
- Status von Citrix Universal Injection Driver (CTXUVI)

Für die Profilverwaltung auf VDAs überprüft Cloud Health Check Folgendes:

- Hypervisor-Erkennung
- Provisioning-Erkennung
- Citrix Virtual Apps and Desktops
- Konfiguration persönlicher vDisks
- Benutzerspeicher
- Profilverwaltungsdienst-Statuserkennung
- Winlogon.exe-Hookingtest

Für Prüfungen der Profilverwaltung muss diese auf dem VDA installiert und aktiviert sein. Weitere Informationen zur Prüfung der Konfiguration der Profilverwaltung finden Sie im Knowledge Center-Artikel CTX132805.

### StoreFront-Integritätsprüfungen

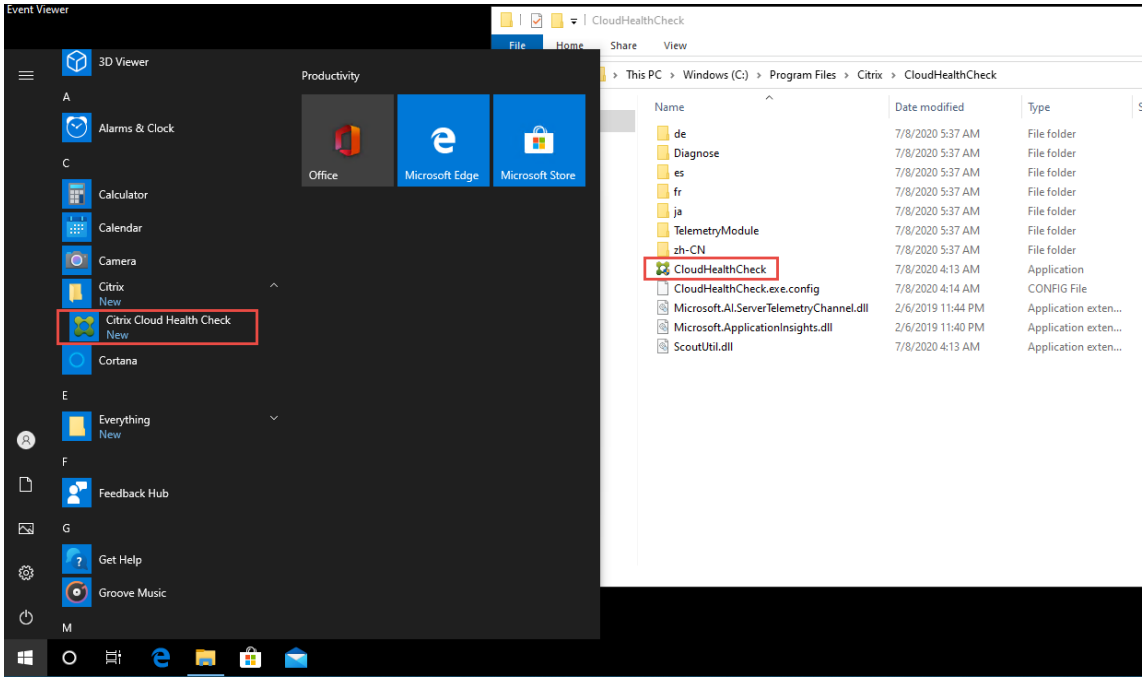
Bei StoreFront-Integritätsprüfungen wird Folgendes überprüft:

- Der Citrix Standarddomänendienst wird ausgeführt.
- Der Citrix Credential Wallet-Dienst wird ausgeführt.
- Die Verbindung vom StoreFront-Server zu Active Directory verwendet Port 88.
- Die Verbindung vom StoreFront-Server zu Active Directory verwendet Port 389.
- Die Verbindung vom StoreFront-Server zu Active Directory verwendet Port 464.
- Die Basis-URL hat einen gültigen FQDN.
- Die korrekte IP-Adresse kann aus der Basis-URL abgerufen werden.
- Der IIS-Anwendungspool verwendet .NET 4.0.
- Das Zertifikat ist an den SSL-Port für die Host-URL gebunden.
- Die Zertifikatskette ist vollständig.
- Die Zertifikate sind abgelaufen.
- Ein Zertifikat läuft bald (innerhalb von 30 Tagen) ab.

## Ausführen von Cloud Health Check

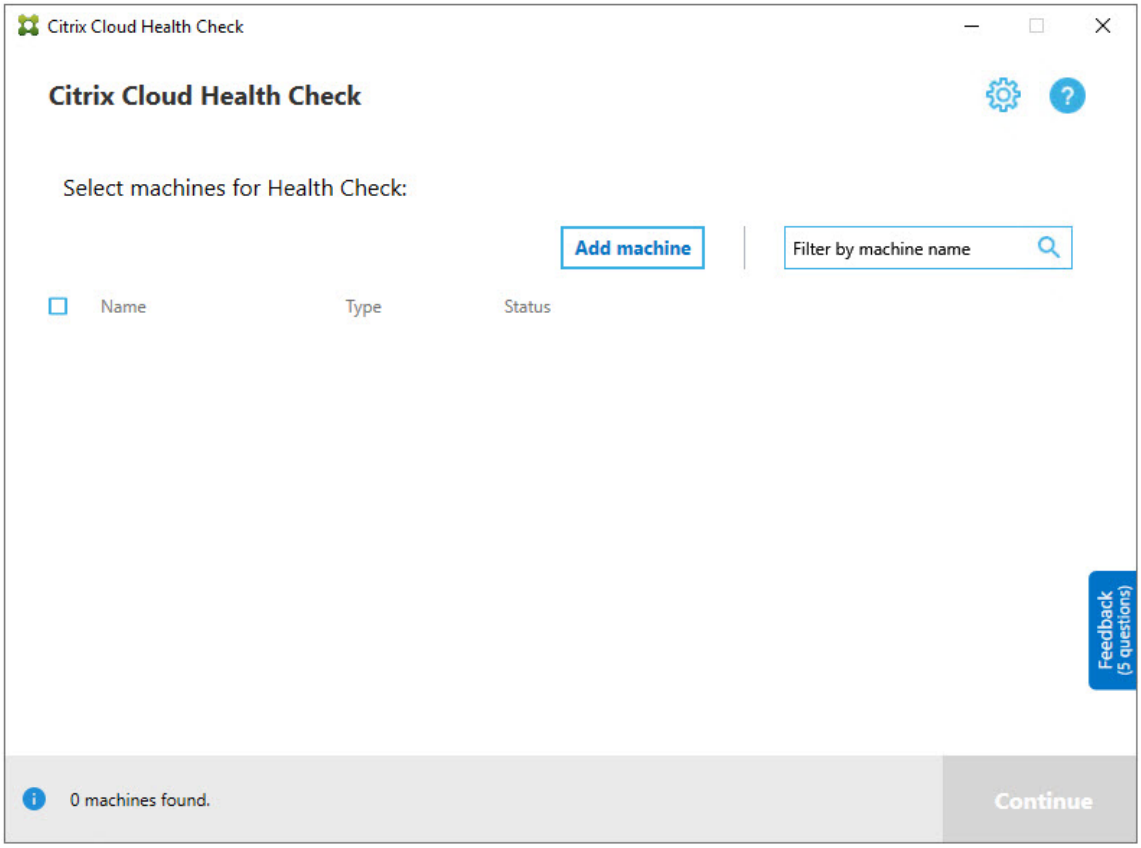
Gehen Sie zum Ausführen von Citrix Cloud Health Check folgendermaßen vor:

1. Wählen Sie im Startmenü der Maschine **Citrix > Citrix Cloud Health Check** oder führen Sie `CloudHealthCheck.exe` in `C:\Program Files\Citrix\CloudHealthCheck` aus.



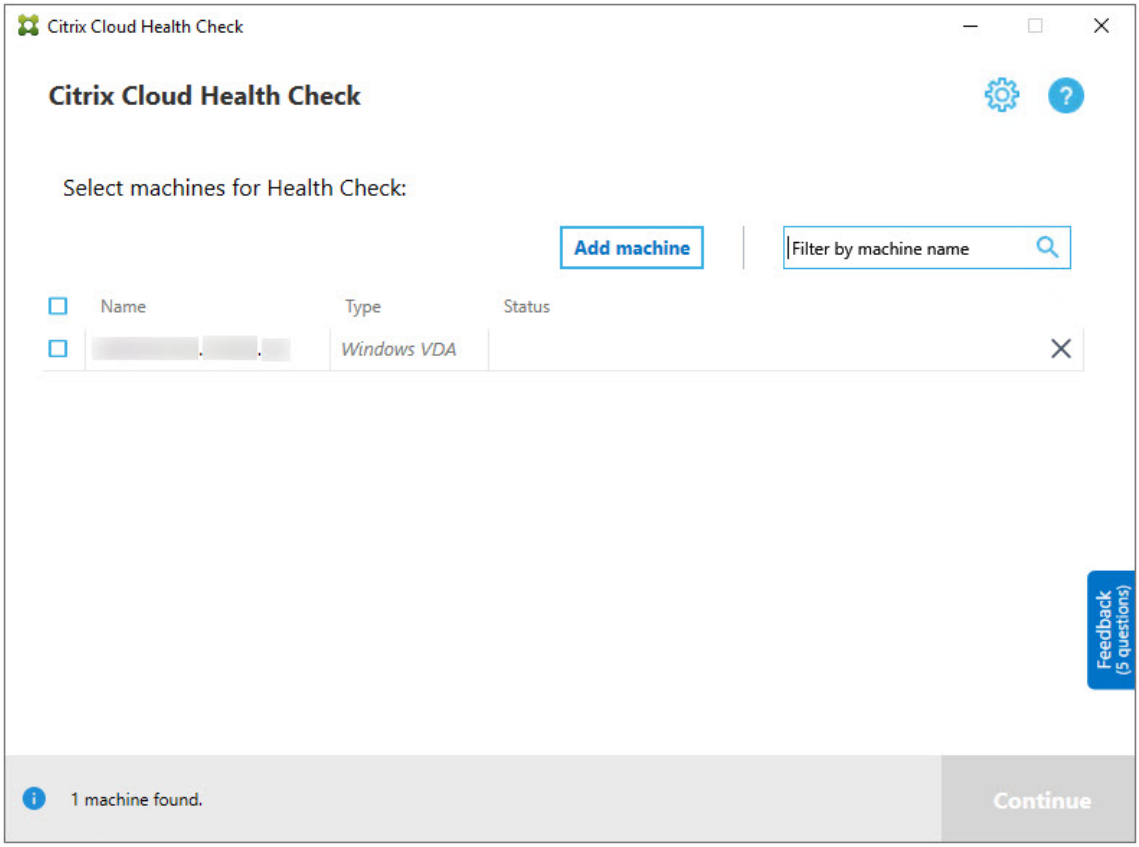

2. Klicken Sie im Hauptbildschirm von Cloud Health Check auf **Maschine hinzufügen**.




3. Geben Sie den FQDN der Maschine ein, die Sie hinzufügen möchten. **Hinweis:** Die Eingabe eines DNS-Alias anstelle eines FQDNs erscheint möglicherweise zwar als gültig, die Integritätsprüfungen können jedoch fehlschlagen.
4. Klicken Sie auf **Weiter**.
5. Wiederholen Sie den Vorgang, um nach Bedarf weitere Maschinen hinzuzufügen.




6. Zum Entfernen einer manuell hinzugefügten Maschine klicken Sie auf das **X** am rechten Zeilenende und bestätigen Sie die Auswahl. Wiederholen Sie diesen Vorgang nach Bedarf, um weitere manuell hinzugefügte Maschinen zu löschen.

Cloud Health Check behält alle manuell hinzugefügte Maschinen in der Liste, bis Sie sie entfernen. Wenn Sie Cloud Health Check schließen und erneut öffnen, werden die manuell hinzugefügten Maschinen weiterhin oben in der Liste aufgeführt.

### Importieren von VDA-Maschinen

Sie können VDA-Maschinen in die Bereitstellung importieren, wenn Sie Integritätsprüfungen ausführen.

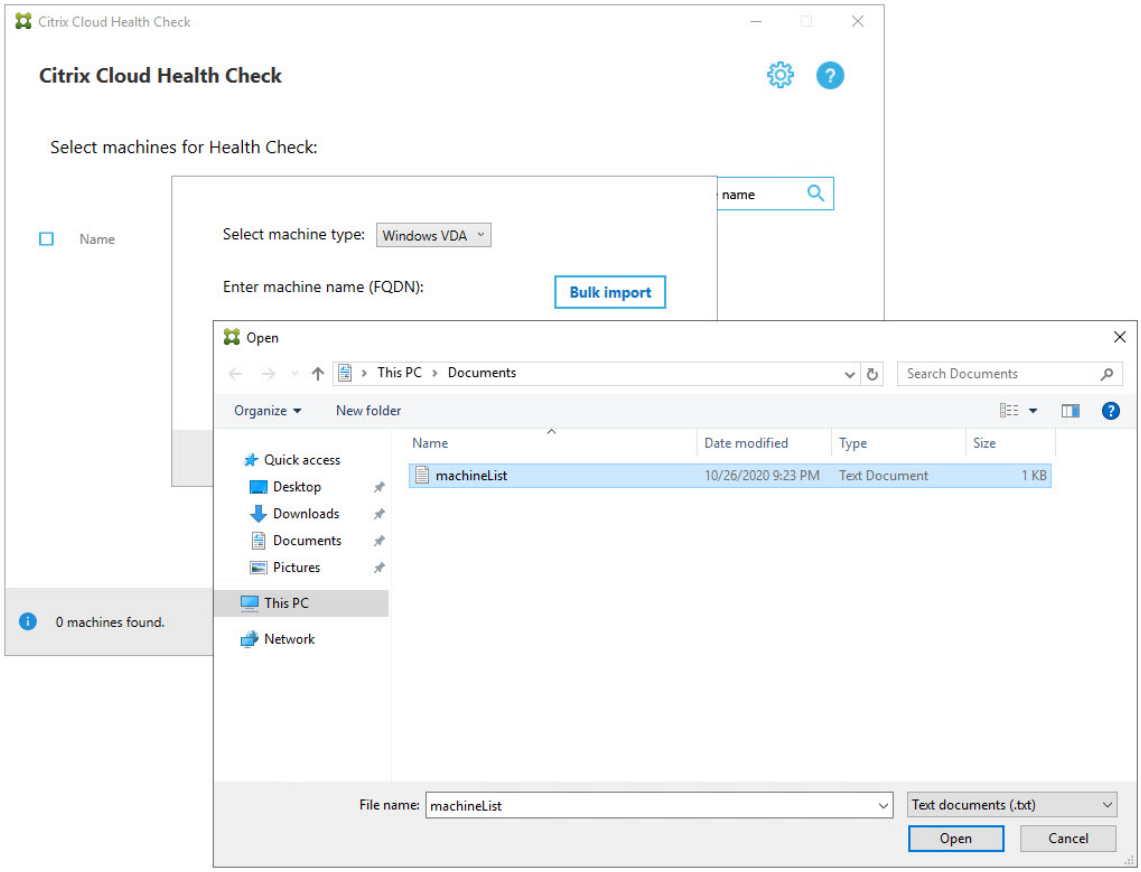
1. Generieren Sie auf dem Connector die Maschinenlistendatei mit dem folgenden PowerShell-Befehl. Auf dem Connector müssen Sie Citrix Anmeldeinformationen eingeben und den Kunden im Dialogfeld auswählen.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.
txt
```

1. Kopieren Sie die Datei machineList.txt auf die domänengebundene Maschine, auf der Sie Cloud Health Check starten möchten.

2. Klicken Sie auf der Cloud Health Check-Seite auf **Maschine hinzufügen**.
3. Wählen Sie den Maschinentyp Windows-VDA aus.
4. Klicken Sie auf **VDA-Maschinen importieren**.
5. Wählen Sie die Datei machineList.txt aus.
6. Klicken Sie auf **Öffnen**.




Die importierten VDA-Maschinen werden auf der Cloud Health Check-Seite aufgeführt.

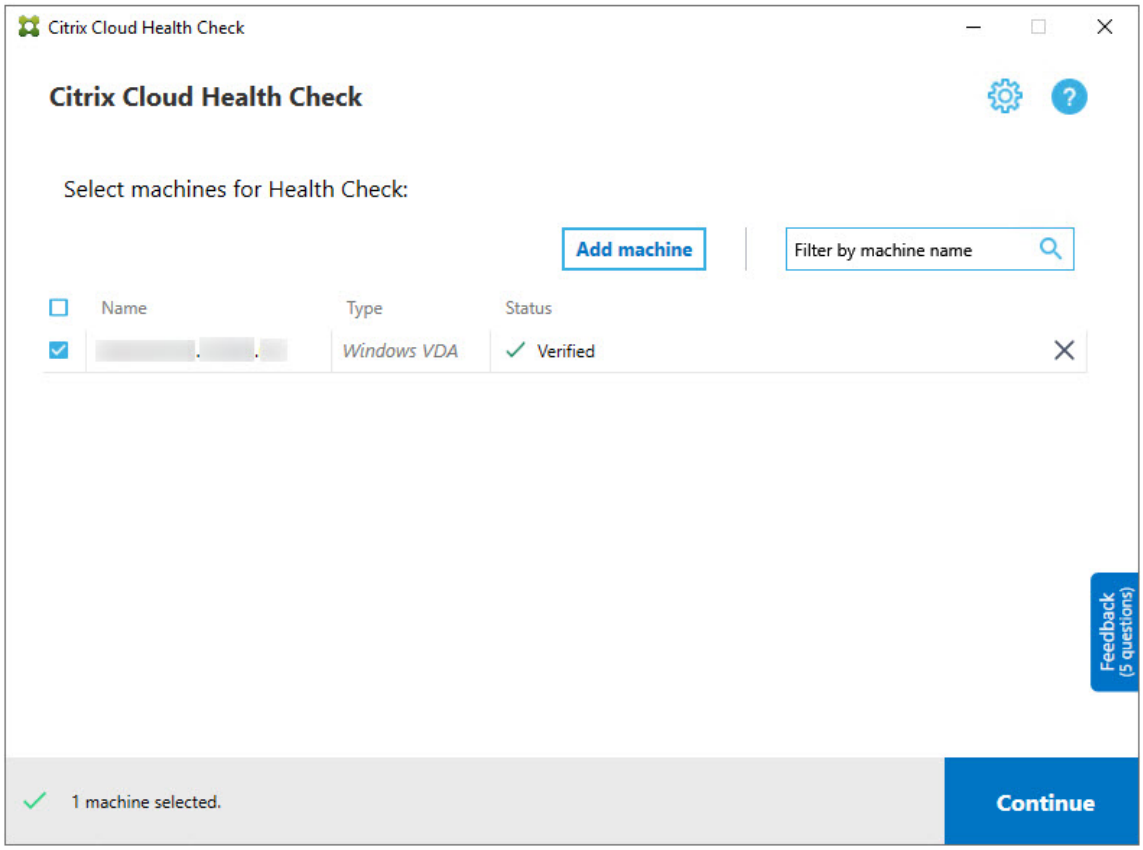
7. Aktivieren Sie das Kontrollkästchen neben jeder Maschine, auf der Sie Cloud Health Check ausführen möchten.

   Cloud Health Check überprüft automatisch jede ausgewählte Maschine auf Erfüllung der unter "Tests zur Überprüfung"aufgeführten Kriterien. Wenn eine Maschine die Überprüfung nicht besteht, wird eine Meldung in der Spalte **Status** angezeigt und das Kontrollkästchen der Maschine ist deaktiviert. Sie haben dann folgende Optionen:

   - Beheben Sie das Problem und aktivieren Sie das Kontrollkästchen erneut. Dadurch wird eine Wiederholung des Tests ausgelöst.
   - Überspringen Sie die Maschine (Kontrollkästchen deaktiviert lassen). Integritätsprüfungen werden für diese Maschine nicht ausgeführt.

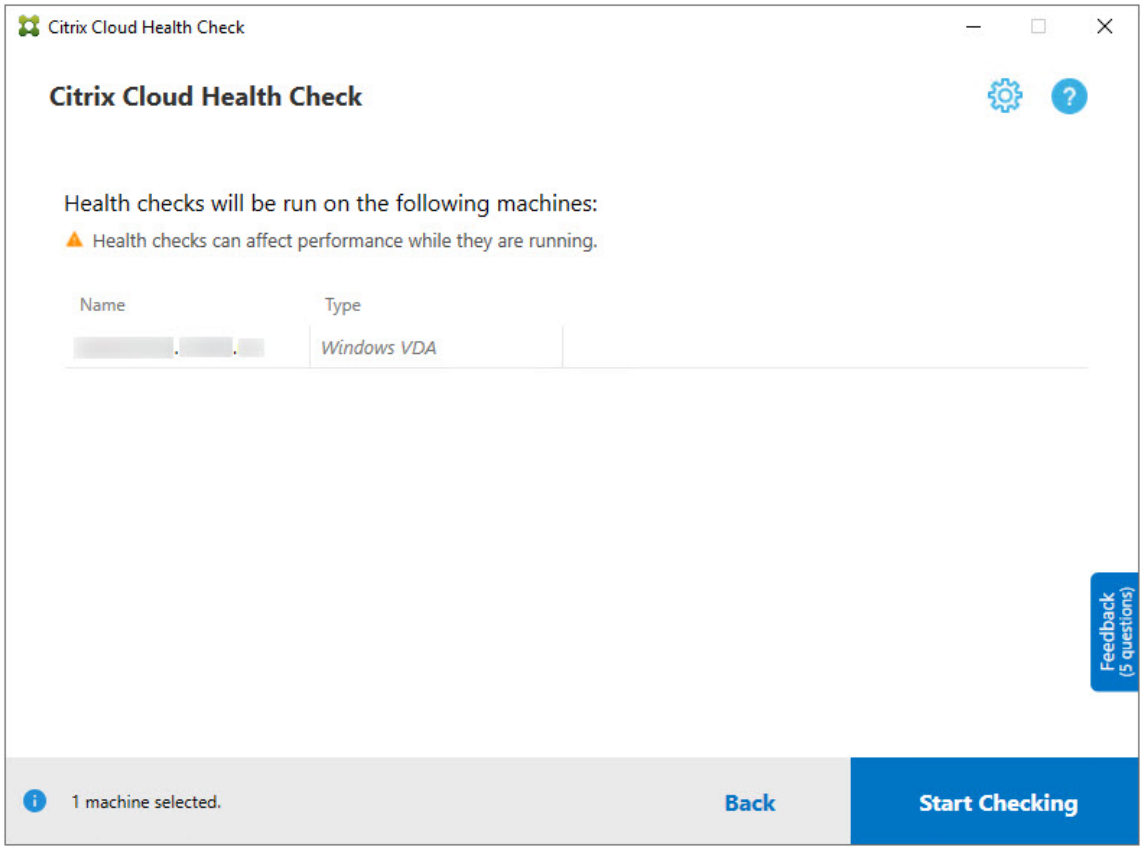
 

8. Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.




9. Führen Sie die Integritätsprüfungen auf den ausgewählten Maschinen aus. In der Zusammenfassung werden die Maschinen aufgelistet, auf denen die Prüfungen ausgeführt werden (d. h. die Maschinen, die Sie ausgewählt haben und die den Test bestanden haben).
10. Klicken Sie auf **Überprüfung starten**.

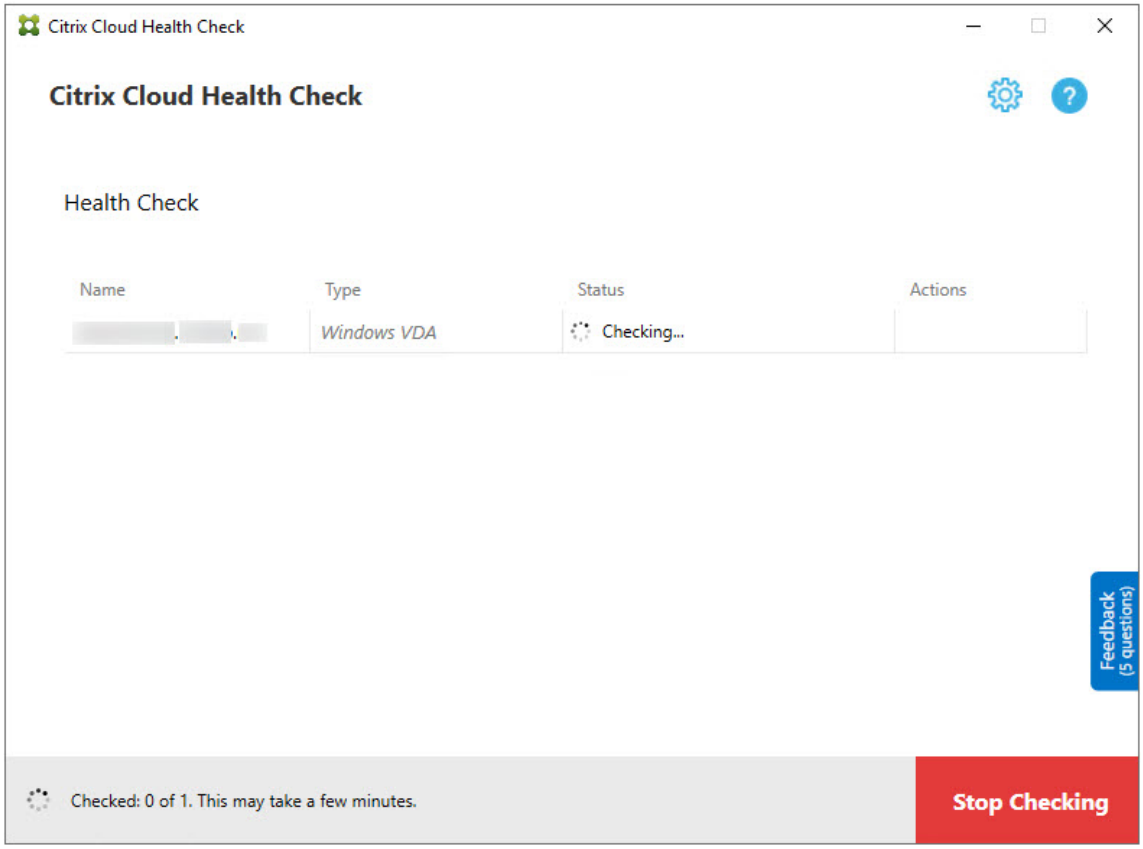
 




Während und nach der Prüfung wird in der Spalte **Status** der aktuelle Status der Prüfung für die Maschinen angezeigt.

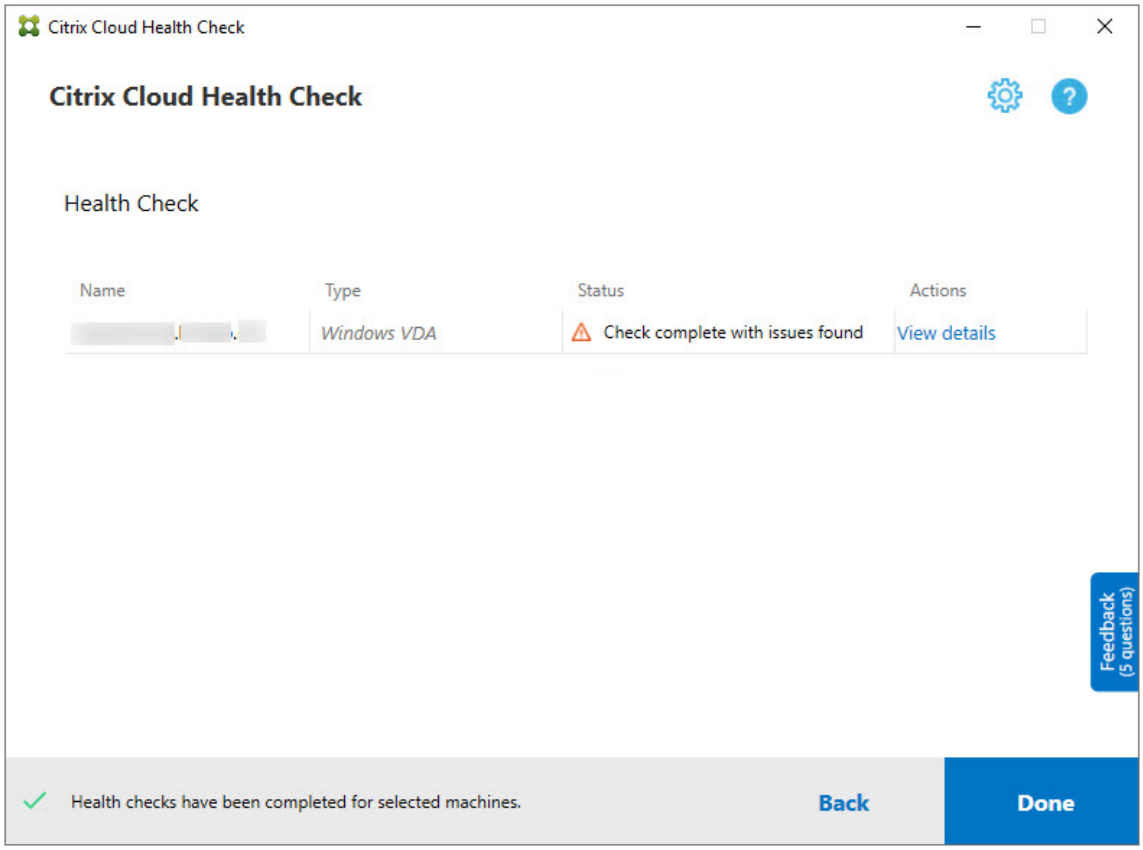
11. Um alle laufenden Prüfungen zu stoppen, klicken Sie unten rechts auf der Seite auf **Überprüfung stoppen**. Sie können die Integritätsprüfung nur für alle ausgewählten Maschinen, nicht aber für einzelne Maschinen stoppen.

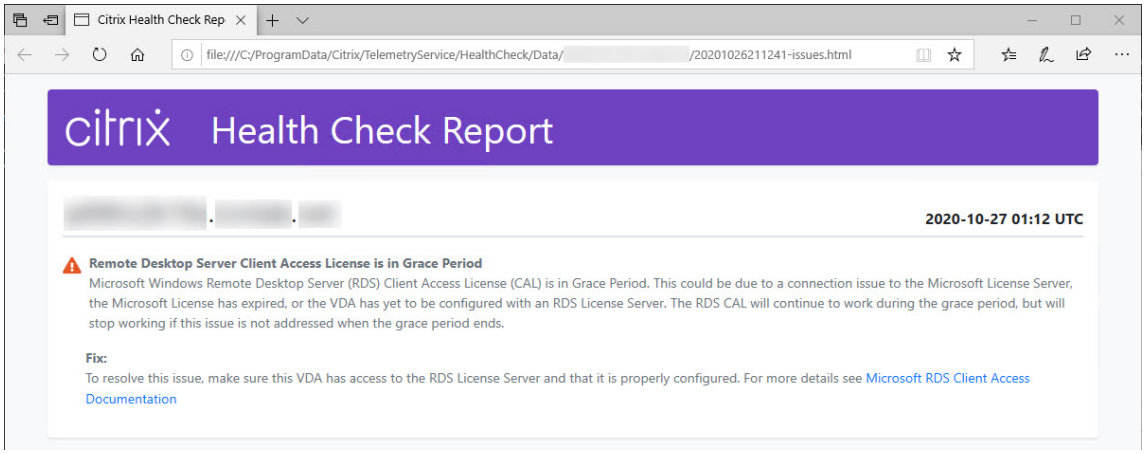



12. Wenn die Überprüfung aller ausgewählten Maschinen abgeschlossen ist, ändert sich die Schaltfläche **Überprüfung stoppen** in der unteren rechten Ecke in **Fertig**.

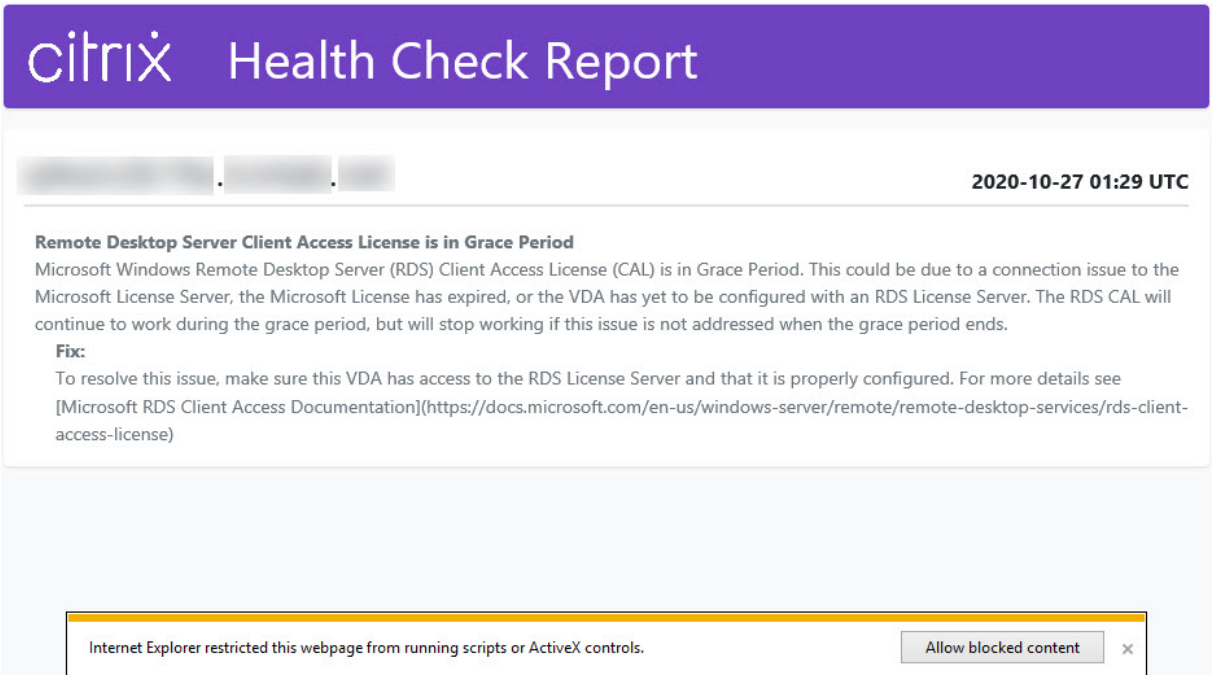



- Schlägt eine Überprüfung fehl, können Sie in der Spalte **Aktion** auf **Wiederholen** klicken.
- Wenn eine Überprüfung abgeschlossen wird und kein Problem gefunden wurde, bleibt die Spalte **Aktion** leer.
- Wird bei einer Überprüfung ein Problem festgestellt, klicken Sie auf **Details anzeigen**, um die Ergebnisse anzuzeigen.




Wenn Sie Internet Explorer zum Anzeigen des Berichts verwenden, müssen Sie auf **Geblockte Inhalte zulassen** klicken, um den Hyperlink anzuzeigen.




Wenn Sie nach Abschluss der Prüfung für alle ausgewählten Maschinen auf **Zurück** klicken, gehen die Prüfergebnisse verloren.

Wenn die Prüfungen abgeschlossen sind, klicken Sie auf **Fertig**, um zum Cloud Health Check-Hauptbildschirm zurückzukehren.

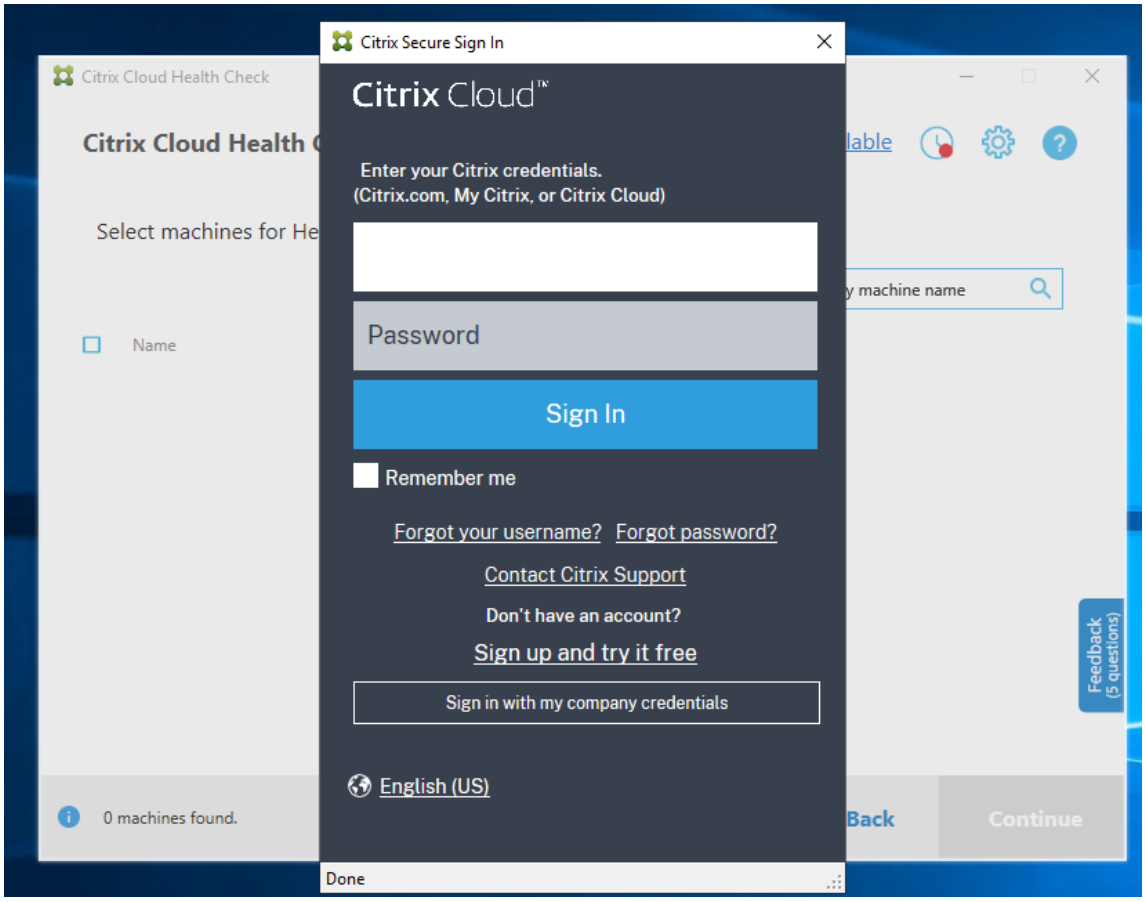
### Abrufen von VDA-Maschinen

Die Cloud-Integritätsprüfung kann VDAs automatisch in Ihren Bereitstellungen von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) erkennen und aus diesen abrufen.

Gehen Sie zum Abrufen von VDAs folgendermaßen vor:

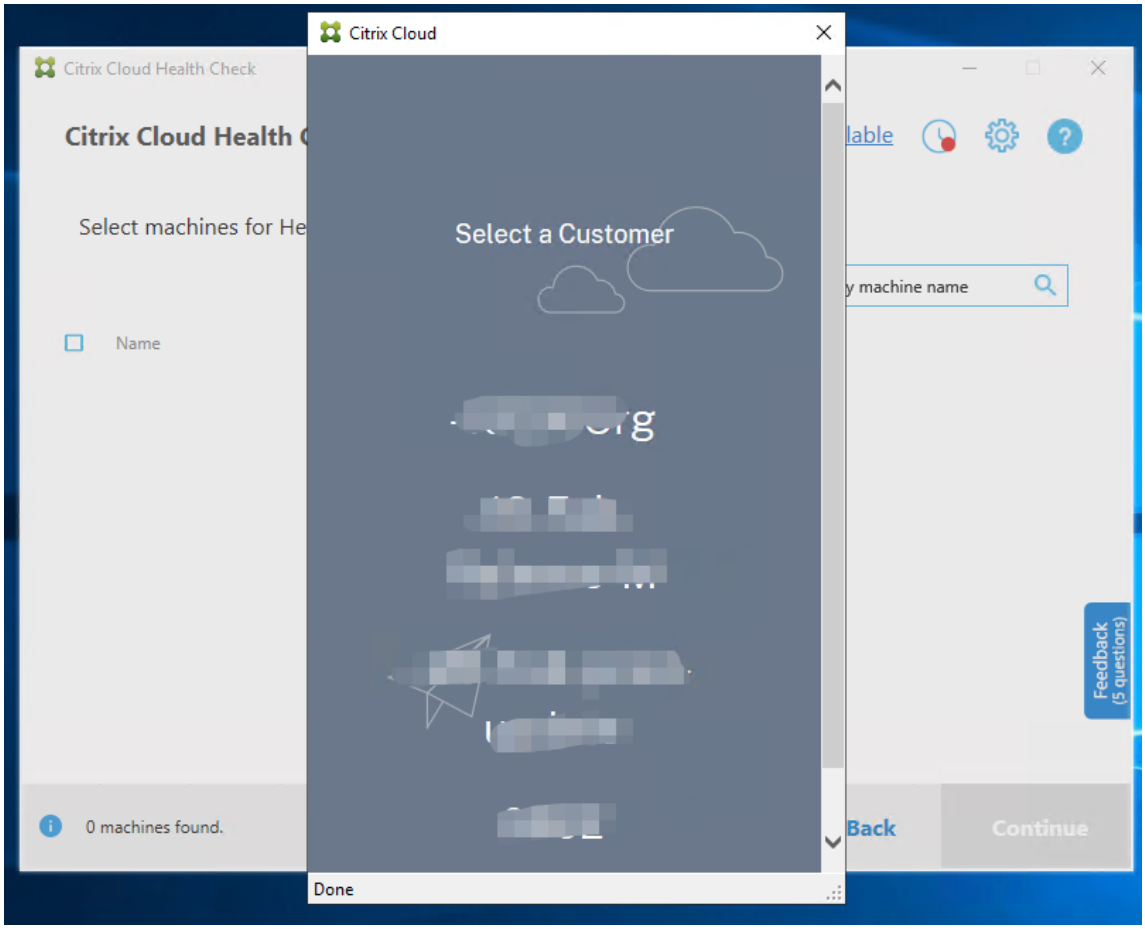
1. Erstellen Sie eine neue Maschine, die mit der gleichen Domänengesamtstruktur verbunden ist, wie diejenige, auf der die Cloud-Integritätsprüfung ausgeführt wird.
2. Öffnen Sie die Cloud-Integritätsprüfung und klicken Sie auf **Maschine suchen**, um sich bei Citrix Cloud anzumelden.



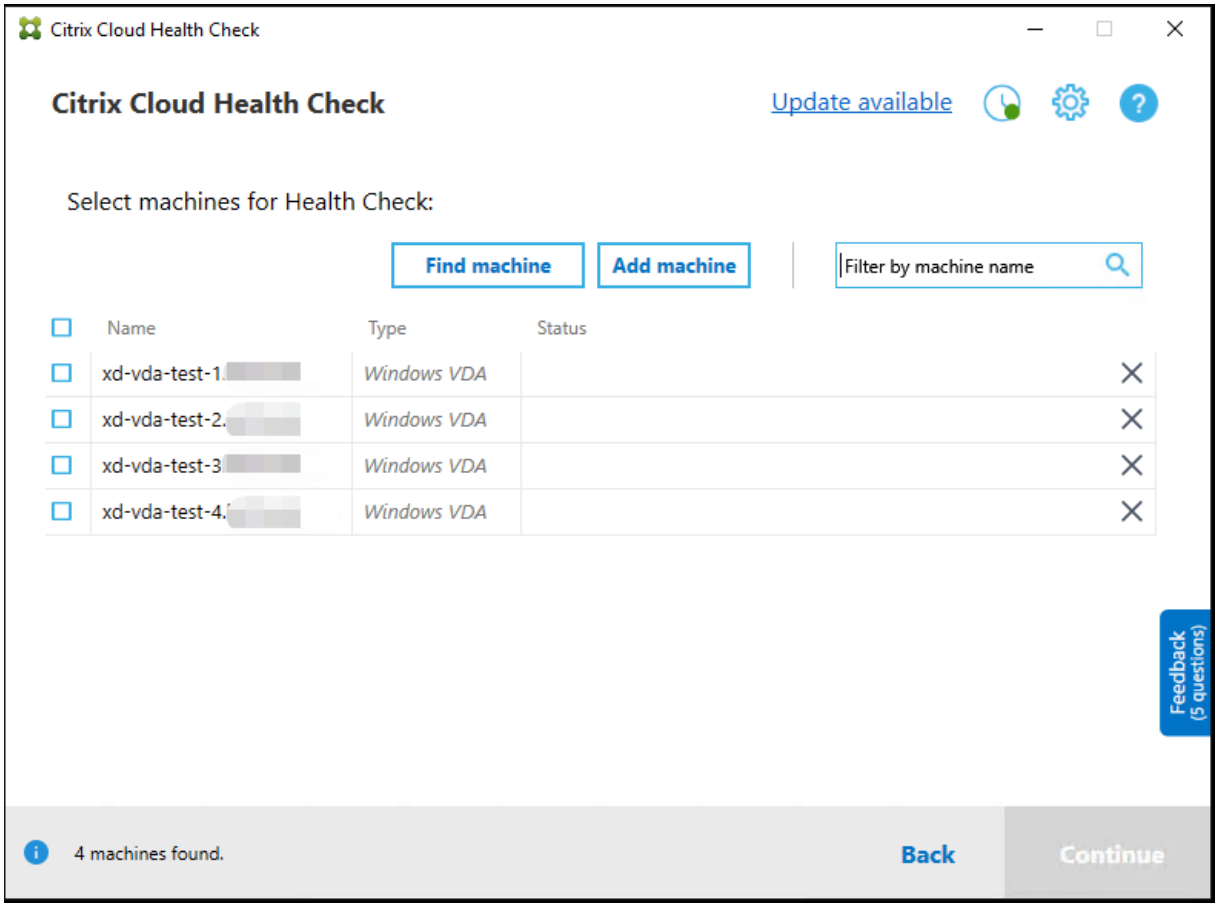

3. Wählen Sie den Kunden mit der Cloudsite für den Abruf aus.




Die VDA-Liste wird in der Cloud-Integritätsprüfung angezeigt. Die Liste wird auch lokal in einer Datei in `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json` gespeichert.

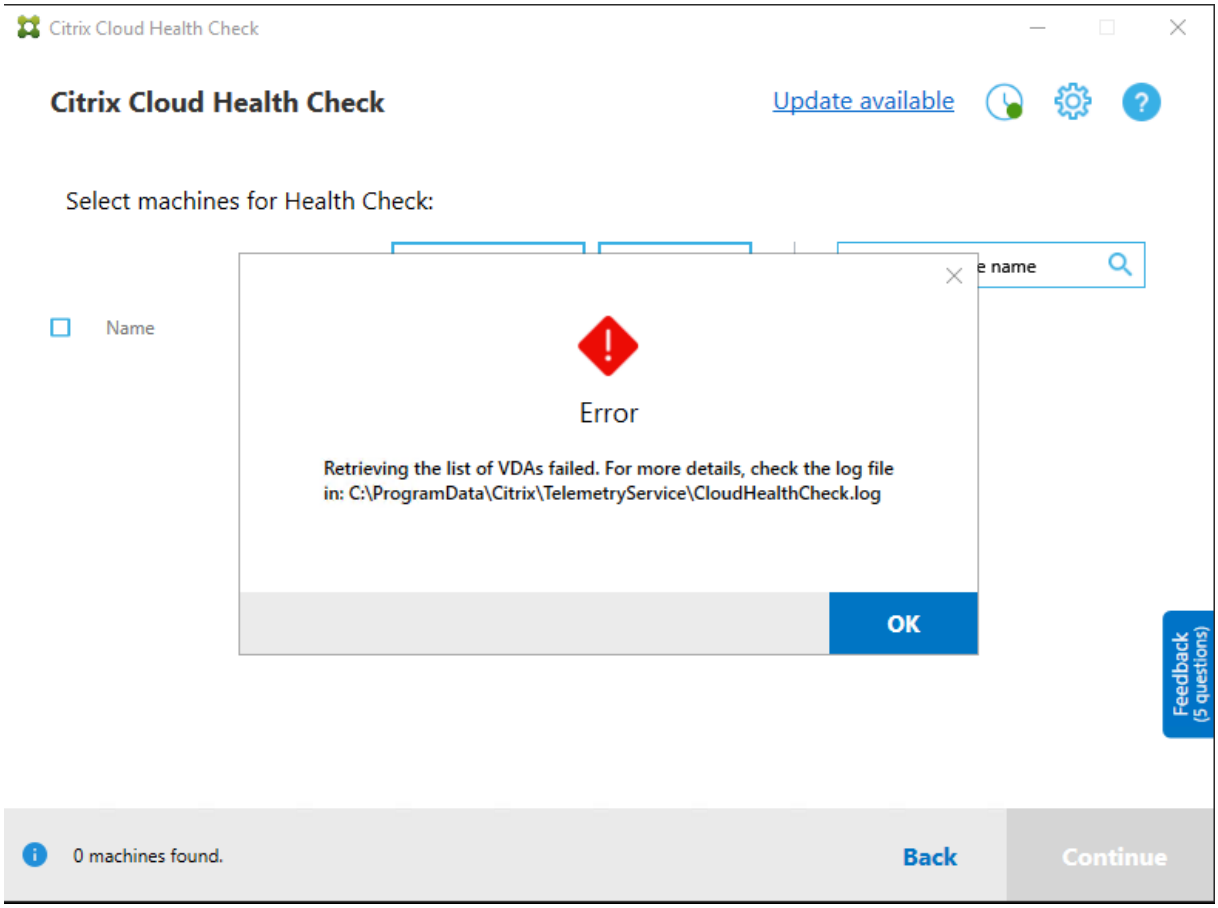
 




Die Maschinenliste lädt den lokalen Cache, wenn Sie die Cloud-Integritätsprüfung erneut öffnen. Wenn Sie in Ihrer Bereitstellung Aktualisierungen vorgenommen haben, müssen Sie auf **Maschine suchen** klicken, um die Maschinenliste zu aktualisieren.

> **Hinweis:**
>
> - Die Cloud-Integritätsprüfung findet nur in der Domänengesamtstruktur Maschinen, in der die Maschine mit der Cloud-Integritätsprüfung residiert.
> - Citrix Cloud-Sitzungen laufen nach einer Stunde ab. Nach einer Stunde müssen Sie erneut auf **Maschine suchen** klicken, um die aktuelle VDA-Liste zu erhalten.
> - Wenn der Abruf der VDA-Liste fehlschlägt, wird eine Fehlermeldung angezeigt. Sie können die Details in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log` überprüfen.




### Ergebnisse der Integritätsprüfung

Berichte von Integritätsprüfungen enthalten die folgenden Elemente:

- Uhrzeit und Datum der Erstellung des Ergebnisberichts
- FQDN der Maschinen, die überprüft wurden
- Auf den Zielmaschinen geprüfte Bedingungen

### Ausführen von Cloud Health Check an der Befehlszeile

Cloud Health Check kann über die Befehlszeile ausgeführt werden, um Kunden bei der Durchführung von Integritätsprüfungen zu unterstützen. Um Cloud Health Check an der Befehlszeile zu verwenden, müssen Sie Administratorrechte auf der Maschine haben, auf der Cloud Health Check ausgeführt wird.

> **Hinweis:**
>
> Wenn Sie Cloud Health Check an der Befehlszeile verwenden, kann jeweils nur eine Maschine

> überprüft werden. Es kann jeweils nur eine Instanz von `CloudHealthCheck.exe` auf der Zielmaschine ausgeführt werden. Wenn Sie mehrere Maschinen überprüfen möchten, müssen die Maschinen nacheinander überprüft werden, indem Sie die Cmdlets in einer Schleife in cmdlet/PowerShell-Skripten umschließen. Geöffnete UI-Instanzen von Cloud Health Check müssen ebenfalls geschlossen werden.

#### Cmdlets

Folgende Cmdlets werden an der Befehlszeile unterstützt:

- `MachineFQDN`: Dieses Cmdlet ist **obligatorisch**. Dies ist der vollqualifizierte Domänenname der Zielmaschine.
- `MachineType`: Dieses Cmdlet ist optional. Der Cmdlet-Wert kann der Windows-VDA (Standardwert) oder StoreFront sein.
- `ReportName`: Dieses Cmdlet ist optional. Der Cmdlet-Wert muss ein gültiger Dateiname unter Windows sein. Der Standardwert ist `HealthCheckReport`.
- `SkipAdminCheck`: Dieses Cmdlet ist optional. Es kann hinzugefügt werden, um die Prüfungen zu überspringen, die Administratorrechte erfordern.
- `UpdateScripts`: Dieses Cmdlet ist optional. Es kann hinzugefügt werden, um die Prüfskripts vom CDN-Server zu aktualisieren.
- `DisableCeip`: Dieses Cmdlet ist optional, wenn CEIP auf der Benutzeroberfläche aktiviert ist. Fügen Sie es hinzu, um CEIP zu deaktivieren.
- `Help`: Zeigt Hilfeinformationen zu Parametern an.

Beispiele:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local

HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName
checkreport

HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck


HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts

HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain
.local,machine3.domain.local

HealthCheckCLI.exe -Help
```

> **Hinweis:**
>
> Bei den Parameternamen wird die Groß-/Kleinschreibung nicht berücksichtigt.

Die Konsolenausgabe wird standardmäßig nicht im Befehlszeilen-Konsolenfenster angezeigt. Sie können die Ausgabe manuell anzeigen, indem Sie `|more` an das Cmdlet anhängen.

Beispiel:`HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

Der Befehlszeilenstandard erfordert Administratorrechte zur Ausführung. Fügen Sie den Parameter `-SkipAdminCheck` hinzu, um die Notwendigkeit von Administratorrechten außer Kraft zu setzen.

#### Exitcodes

Exitcodes erklären das Ergebnis von Cloud Health Check-Prüfungen innerhalb der Befehlszeile. Um den Exitcode abzurufen, müssen Sie `start /wait` vor dem Cmdlet hinzufügen.

Beispiel:`start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

Die Exitcodes sind:

- 0 - Normal: Prüfung erfolgreich abgeschlossen.
- 1 - Leichter Fehler: Prüfung abgeschlossen. Probleme vorhanden.
- 2 - Schwerer Fehler: Prüfung nicht abgeschlossen. Fehler vorhanden.

Mit dem Cmdlet `echo %errorlevel%` können Sie den Exitcode für den zuletzt ausgeführten Befehl abrufen.

#### Berichte

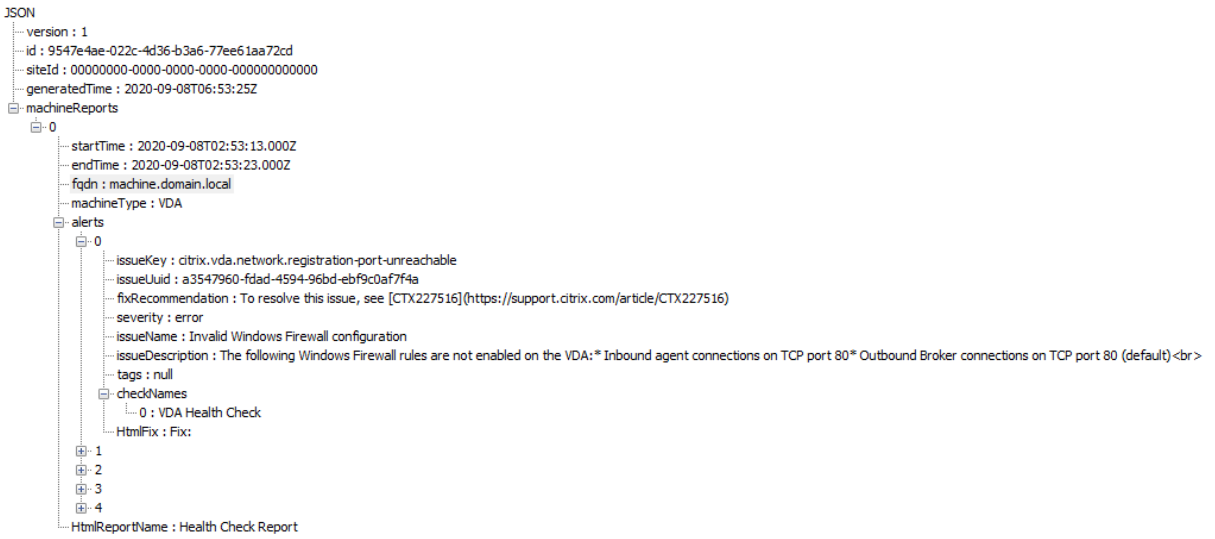
Cloud Health Check erstellt Ordner mit dem Namen der Maschine in `HealthCheckDataFolder` für die Zielmaschine. Eine HTML-Datei und eine JSON-Datei werden auf der Maschine erstellt, auf der Cloud Health Check installiert ist. Integritätsprüfungsberichte befinden sich in `HealthCheckDataFolder` unter `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Berichte werden nur erstellt, wenn auf der Zielmaschine Probleme aufgetreten sind.

> **Hinweis:**
>
> Wenn der angegebene Berichtsname bereits existiert, werden die Berichtsdateien überschrieben.

Warnungen und allgemeine Informationen sind im JSON-Bericht gespeichert.



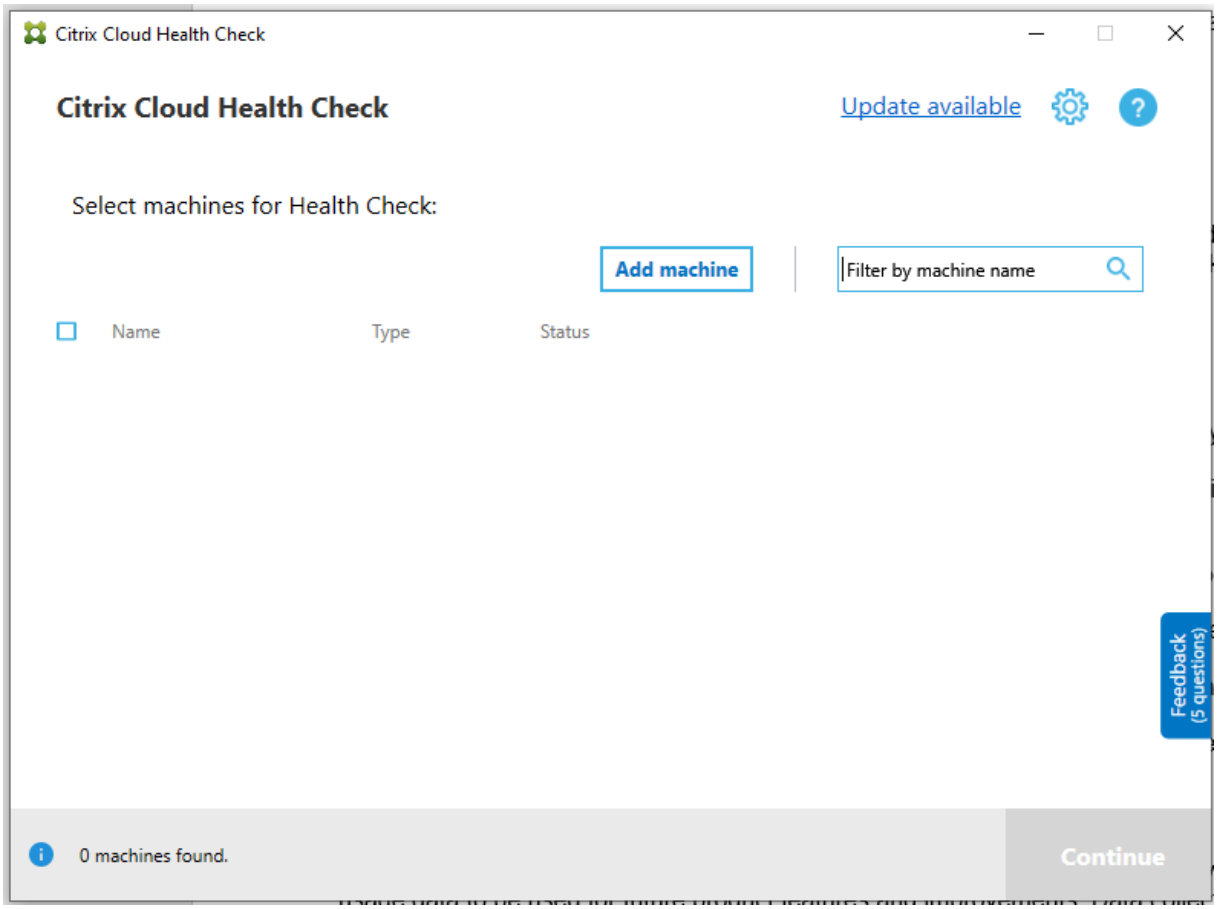

Die Berichtscodes sind:

- **issueKey**: Beschreibung des Problems als Textdatei.
- **issueUuid**: Eindeutige Zeichenfolge zur Identifizierung des Problems.
- **fixRecommendation**: Empfohlener Fix für das Problem.
- **severity**: Hinweis, ob das Problem behoben werden muss. Ein Fehler kann anzeigen, dass die Komponente (VDA oder StoreFront) nicht fehlerfrei funktioniert. Eine Warnung kann anzeigen, dass die Komponente zwar funktioniert, aber möglicherweise Probleme vorliegen.
- **issueName**: Name des Problems.
- **issueDescription**: Detaillierte Beschreibung des Problems.

### Aktualisieren von Cloud Health Check

Wenn eine neue Version von Cloud Health Check verfügbar ist, wird oben rechts im Cloud Health Check-Fenster der Link “Update verfügbar”angezeigt. Klicken Sie auf den Link, um zu Citrix Downloads zu gelangen und die neue Version zu erhalten.



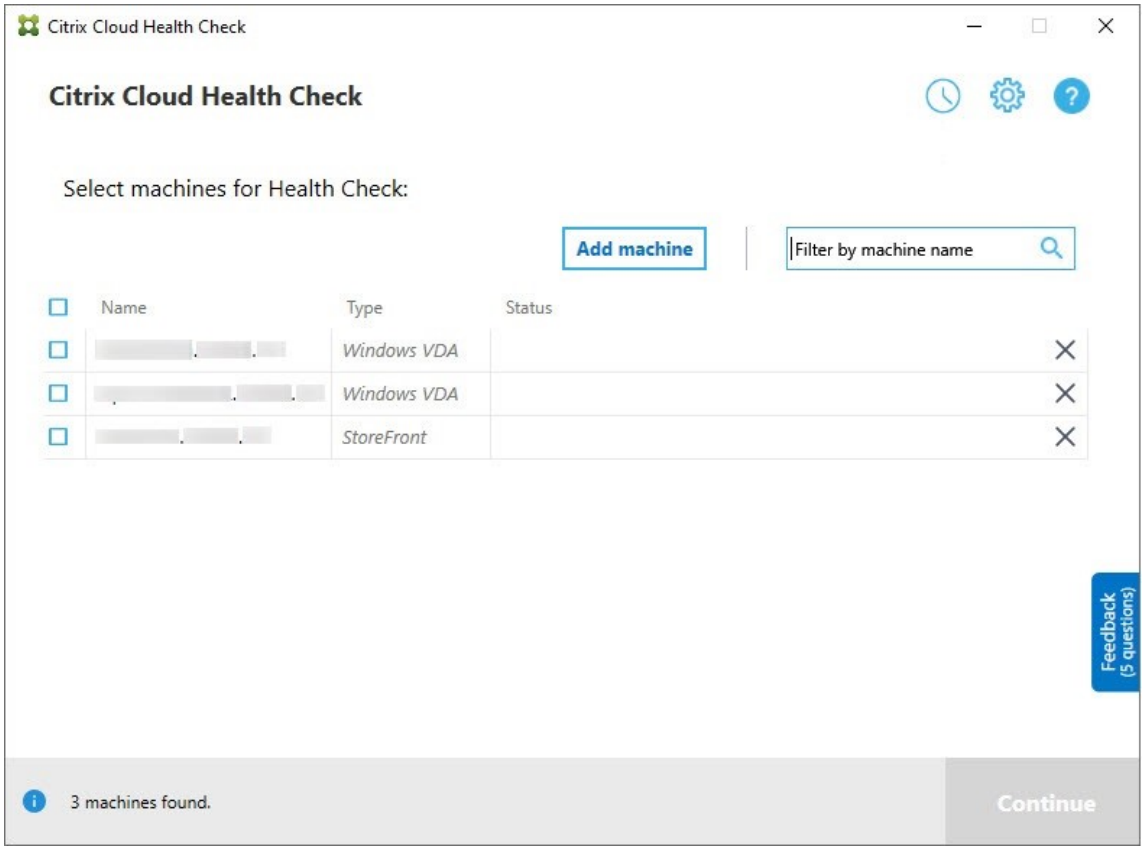

## Zeitplaner für Cloud-Integritätsprüfung

Mit dem Zeitplaner für die Cloud-Integritätsprüfung können Sie regelmäßige Integritätsprüfungen durchführen.

### Einrichten des Zeitplans

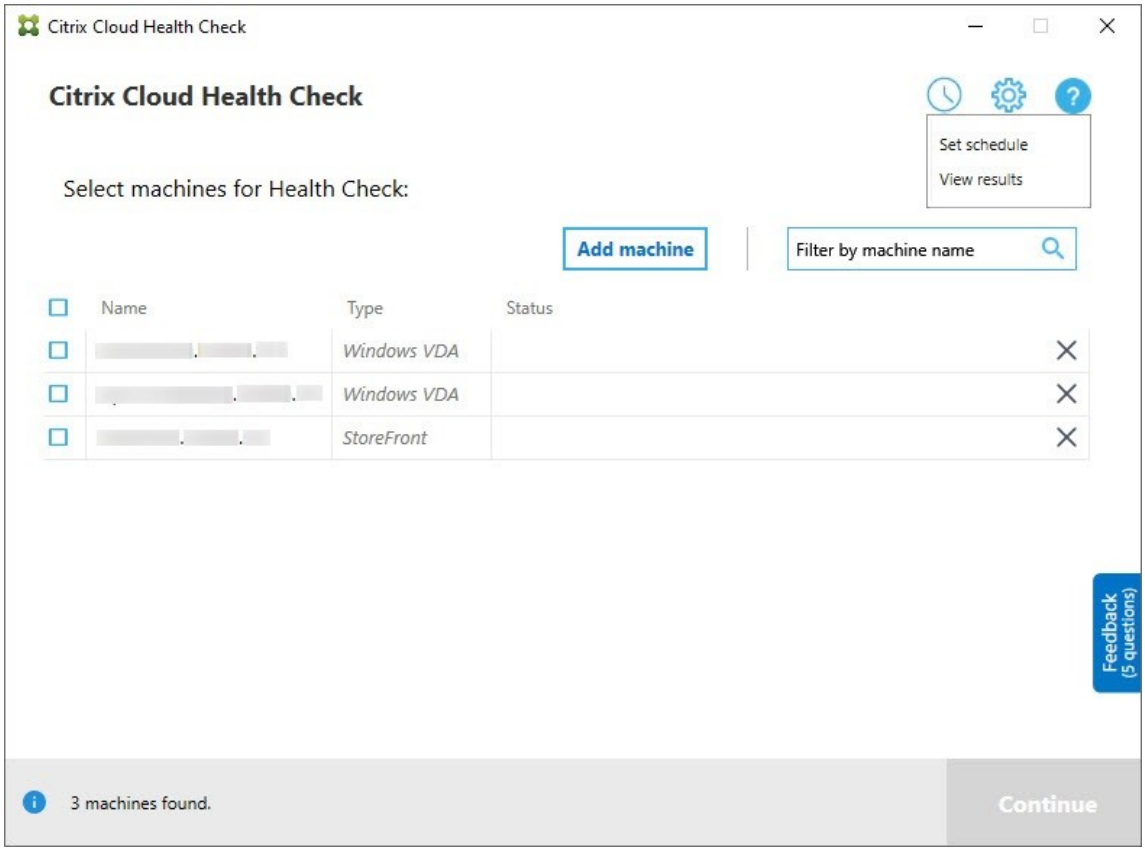
1. Klicken Sie im Hauptfenster der Cloud-Integritätsprüfung auf **Maschine hinzufügen**, um Maschinen hinzuzufügen, die Sie regelmäßig überprüfen möchten.




2. Klicken Sie auf das Uhrensymbol und dann auf **Zeitplan festlegen**.




3. Wählen Sie eine Uhrzeit und klicken Sie auf **Weiter**. Die Aufgabe kann zur wiederholten Ausführung festgelegt werden. Aktivieren Sie hierfür das Kontrollkästchen **Wiederholung alle**.
4. Geben Sie an, ob Ergebnisse im Windows-Ereignisprotokoll verzeichnet werden sollen. Die Aufgabe kann so eingestellt werden, dass die Ergebnisse im Windows-Ereignisprotokoll verzeichnet werden.
5. Wählen Sie, ob nach Abschluss der Überprüfung ein benutzerdefiniertes PowerShell-Skript ausgelöst werden soll, und klicken Sie auf **Weiter**.

   - Klicken Sie bei Bedarf auf **Bearbeiten**, um den Skriptinhalt in Windows PowerShell ISE zu bearbeiten.
   - Klicken Sie auf **Suchen**, um den Speicherort zu öffnen und einen anderen Editor zum Öffnen der Datei zum Bearbeiten des Skripts zu verwenden.
   - Klicken Sie auf **Zurücksetzen**, um das Skript auf seine ursprüngliche Einstellung zurückzusetzen.

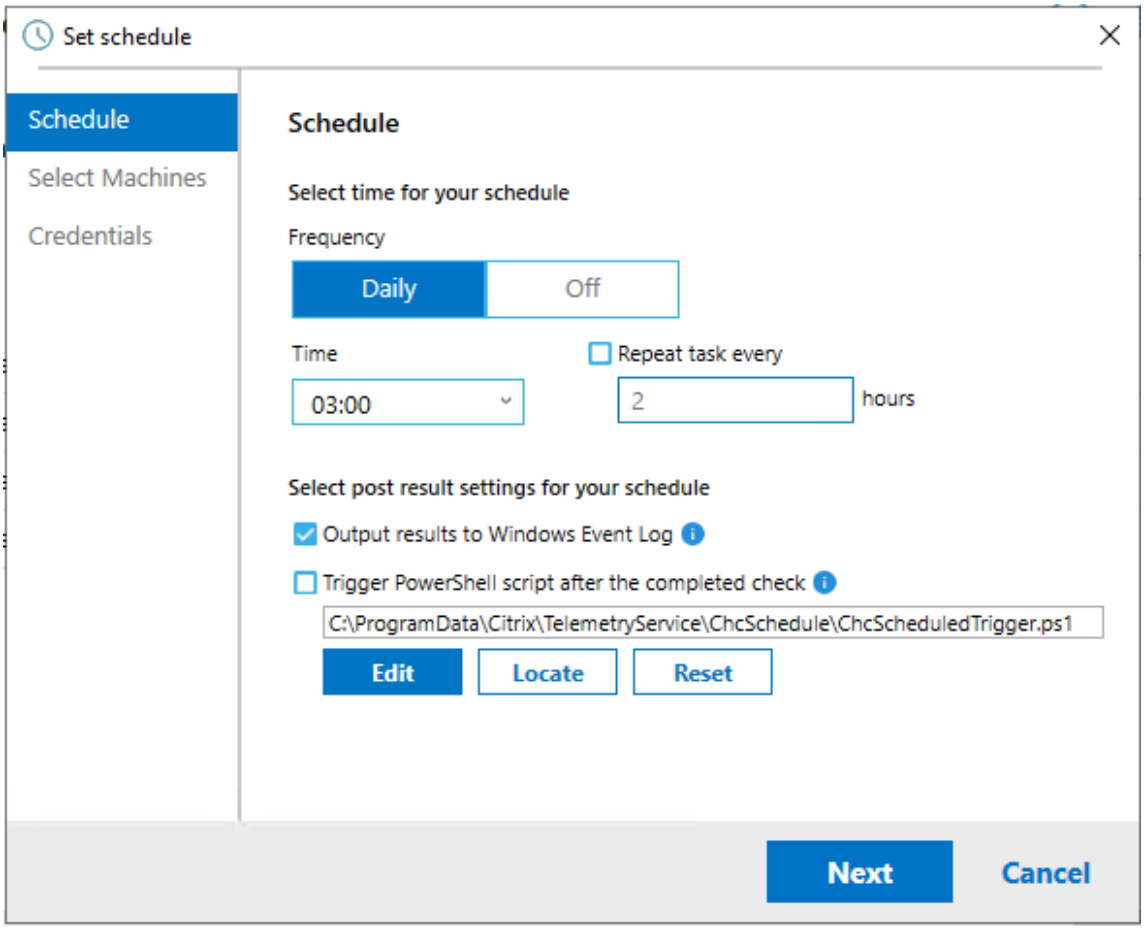
     > **Hinweis:**
     >
     > – Sie können den Skriptnamen und -pfad nicht ändern.
     > – Sie können benutzerdefinierte Aktionen mit dem Skript ChcShceduledTrig-

> ger.ps1 implementieren, z. B. das Senden einer E-Mail, wenn der Prüfbericht fertiggestellt ist. Fügen Sie am Ende des Skripts den folgenden Code hinzu. Bearbeiten Sie den Code unter Verwendung der entsprechenden E-Mail-Konten und SMTP-Serveradresse. Eine E-Mail-Benachrichtigung wird mit den Anmeldeinformationen des Kontos gesendet, das die geplante Aufgabe ausführt.

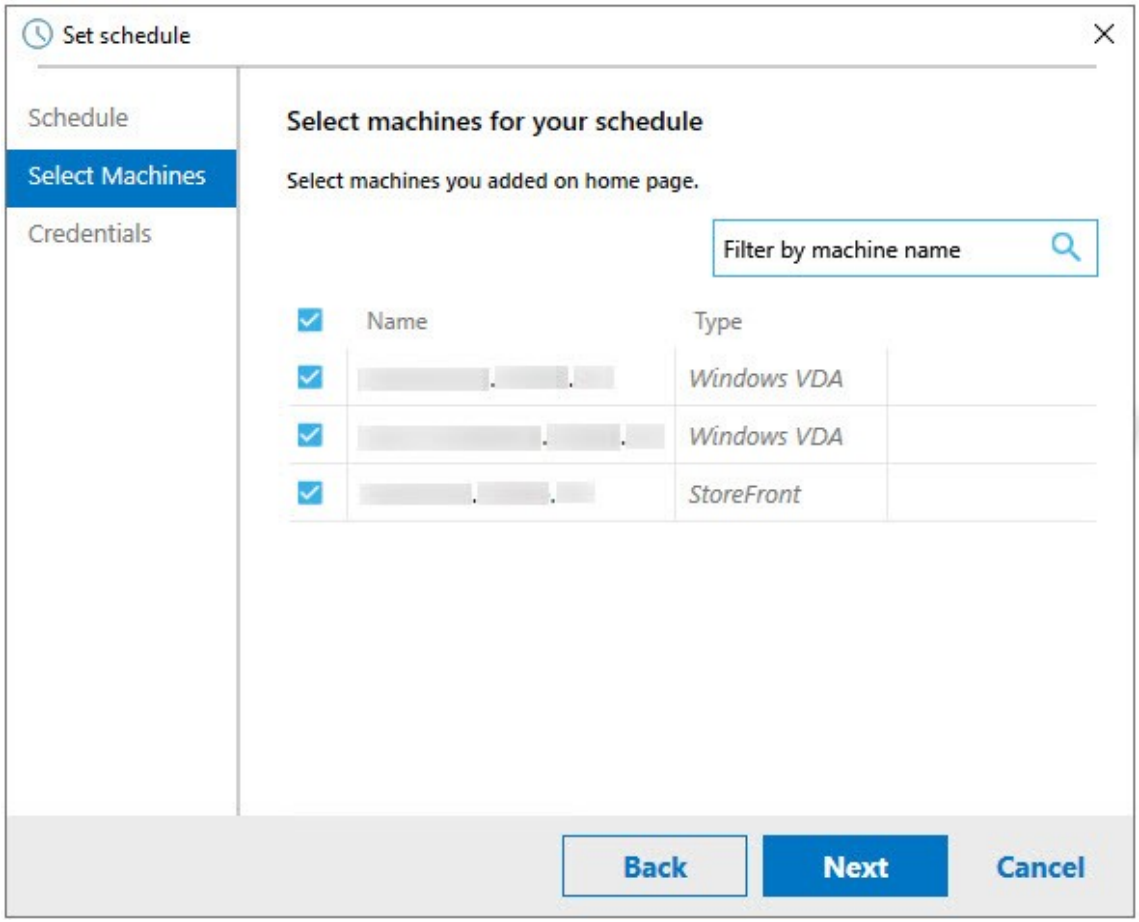
```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
    Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



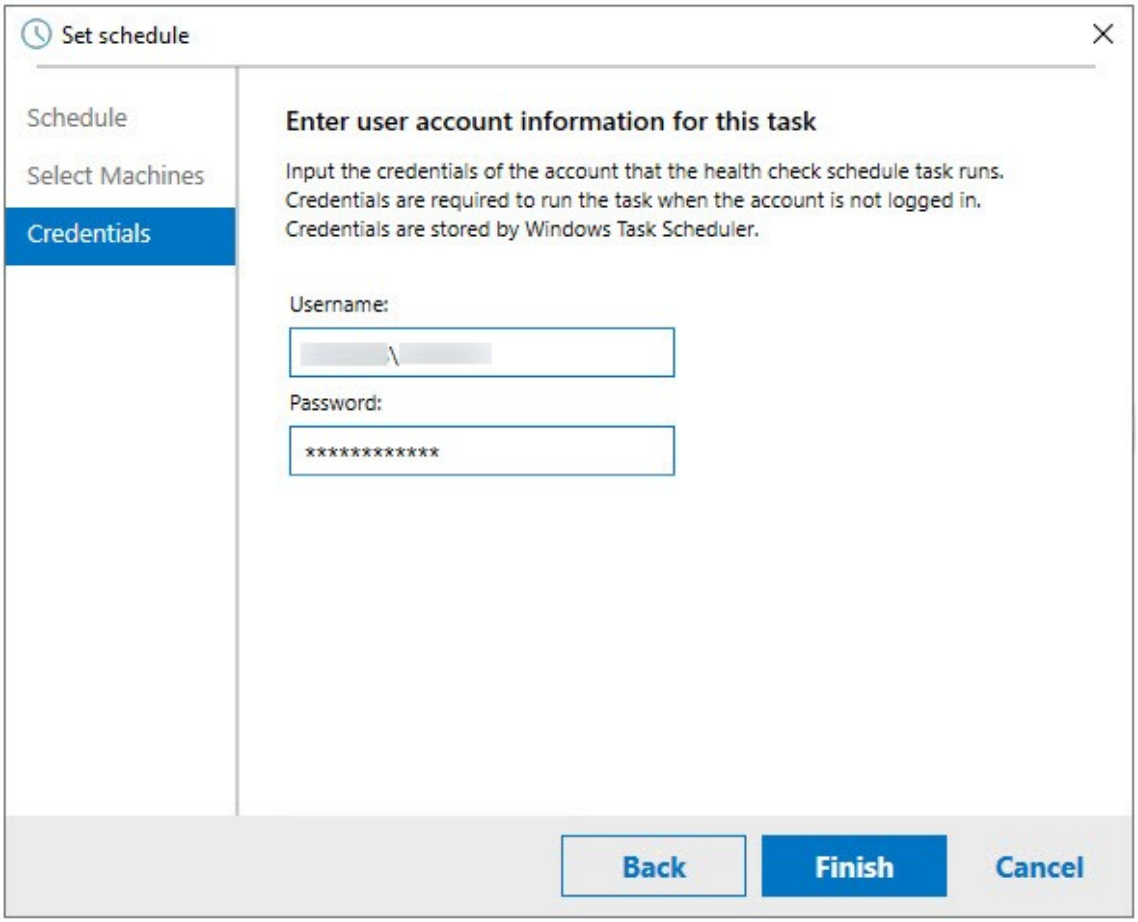

6. Wählen Sie die Maschinen für den Zeitplan und klicken Sie auf **Weiter**.

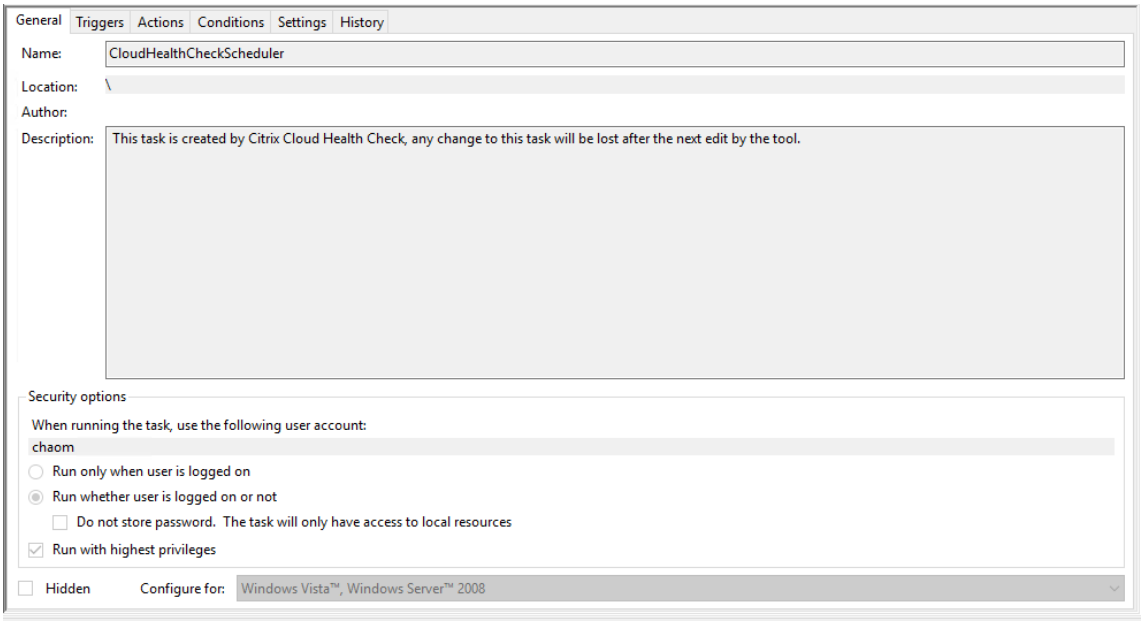



7. Geben Sie die Anmeldeinformationen des Kontos zur Ausführung der Aufgabe ein und klicken Sie auf **Fertig stellen**.



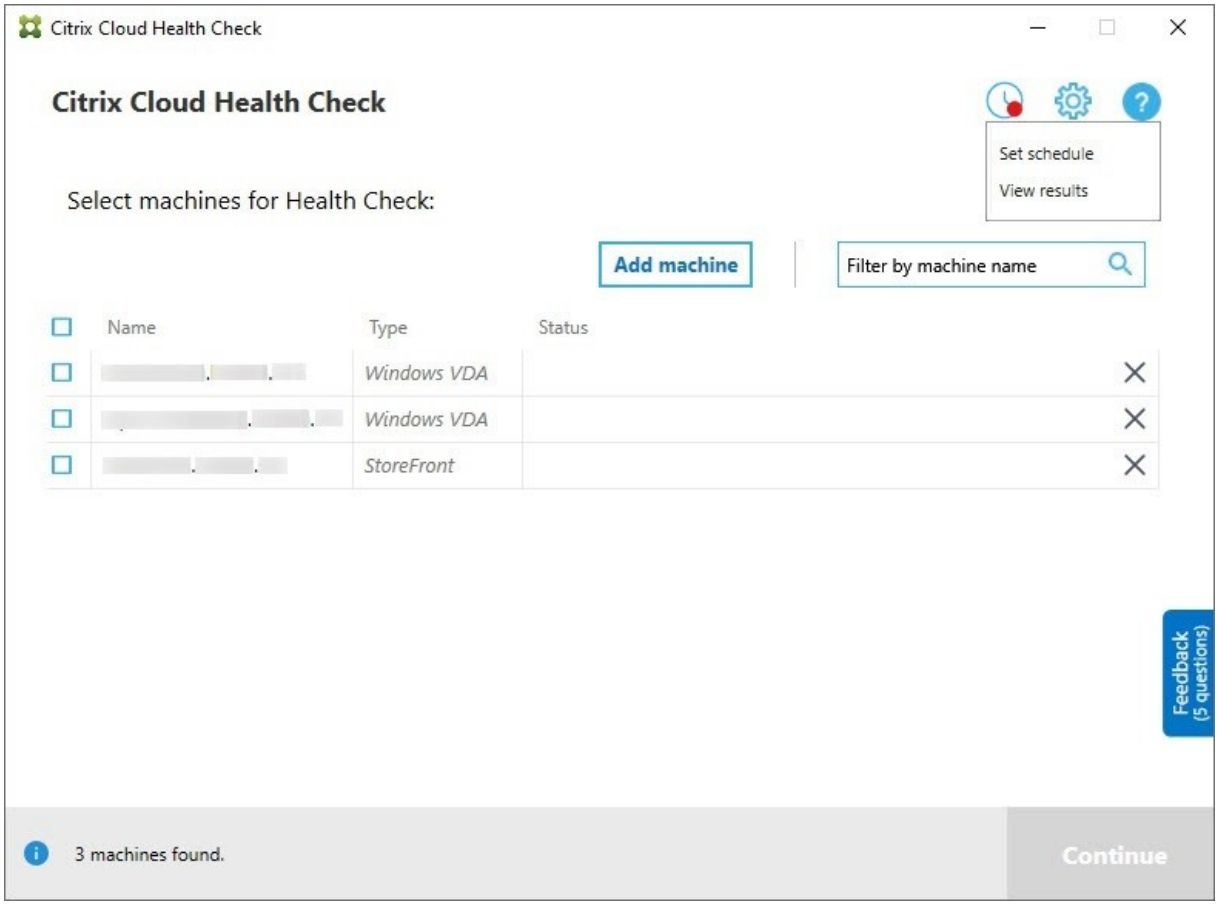

8. Eine CloudHealthCheckScheduler-Aufgabe wird in der Windows-Aufgabenplanung erstellt.



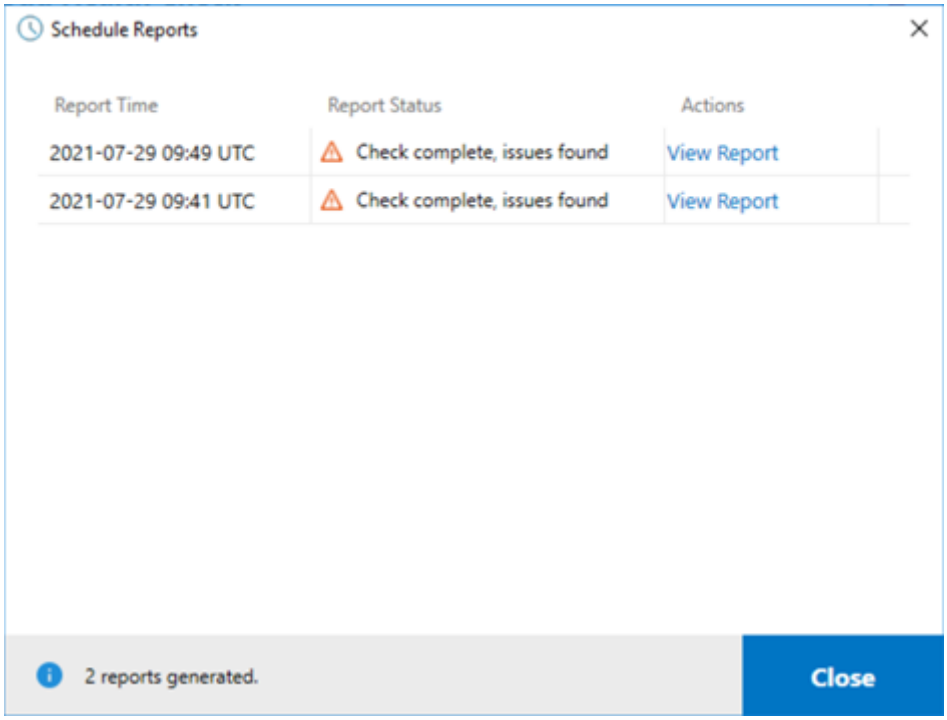
**Anzeigen der Zeitplanergebnisse**

Ein roter Punkt auf dem Uhrensymbol zeigt an, dass bei der letzten Überprüfung Probleme gefunden wurden. Um die Ergebnisse anzuzeigen, klicken Sie auf das Uhrensymbol und dann auf **Ergebnisse anzeigen**.

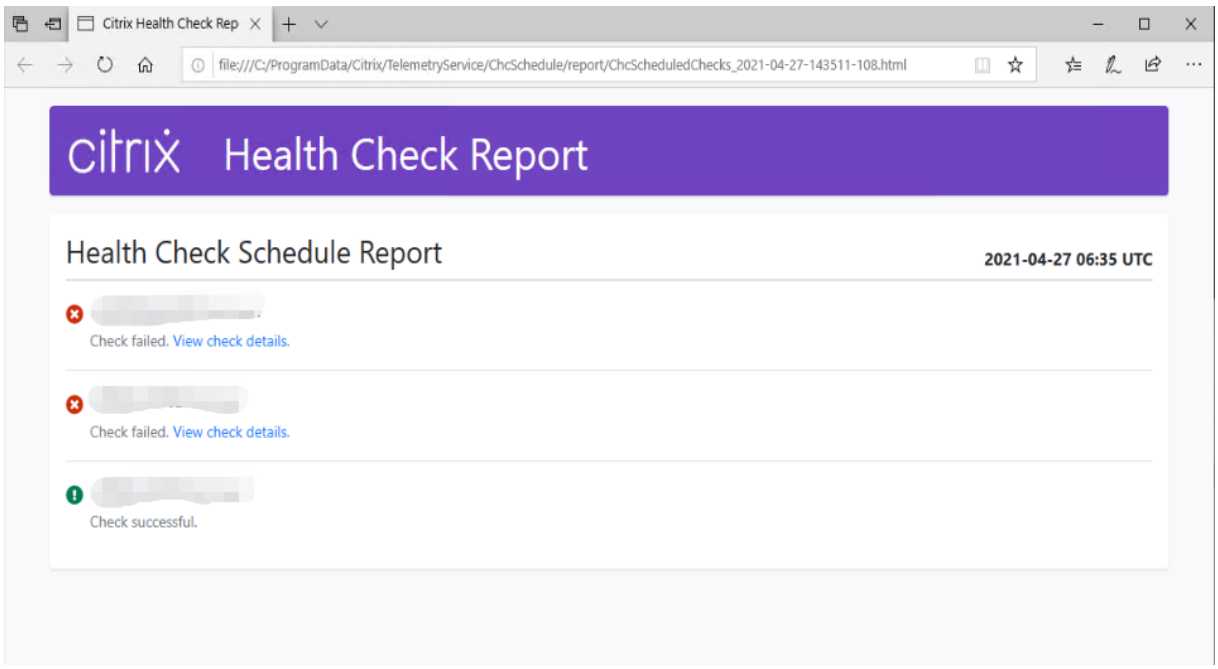



Auf der Seite "Zeitplanberichte"werden die Ergebnisse für alle geplanten Systemintegritätsprüfungstasks angezeigt. Klicken Sie auf **Bericht anzeigen**, um den Bericht für einzelne Zeitpläne anzuzeigen.

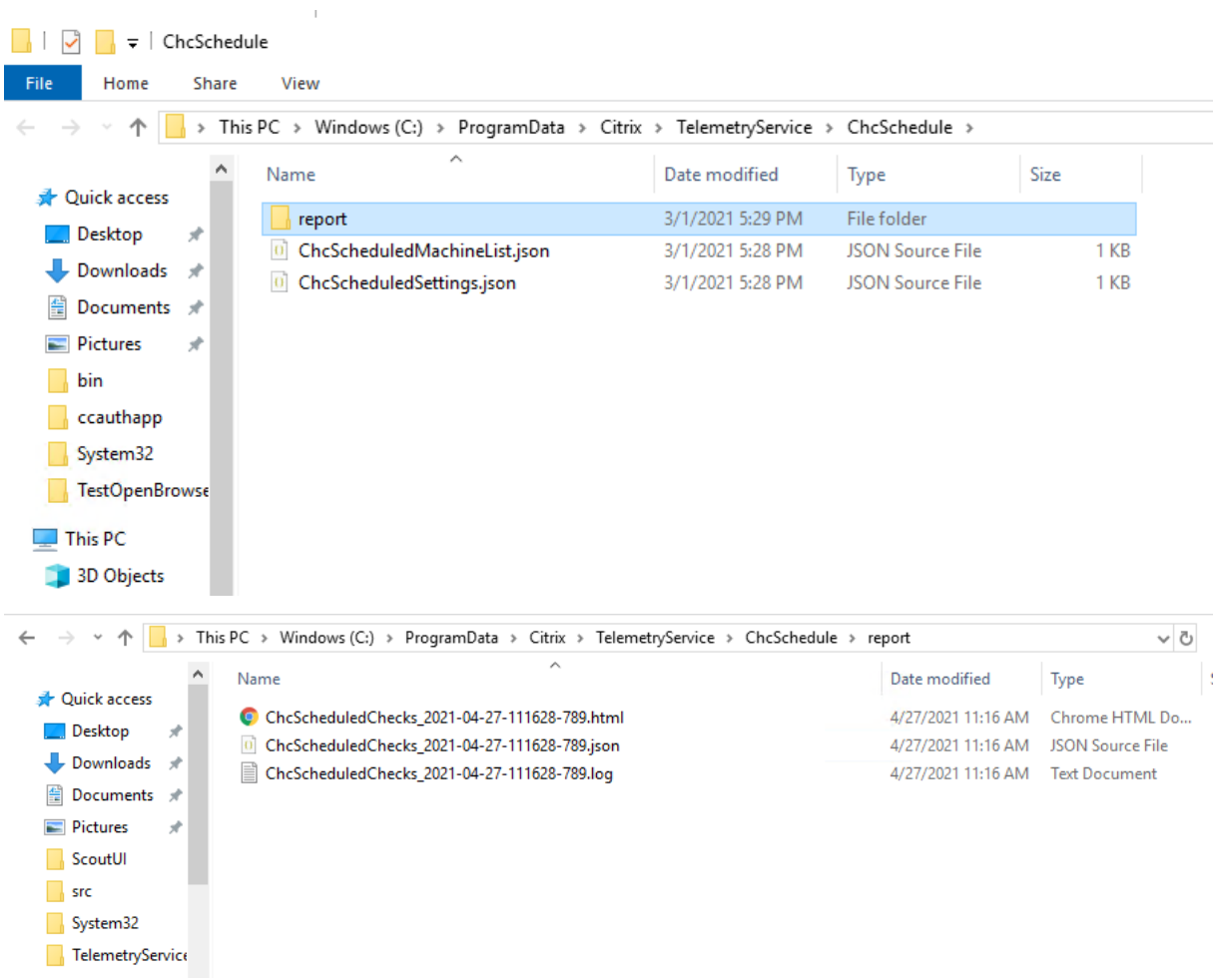



Der HTML-Bericht enthält den Gesamtbericht für jeden Zeitplan. Beispiel eines solchen Berichts:

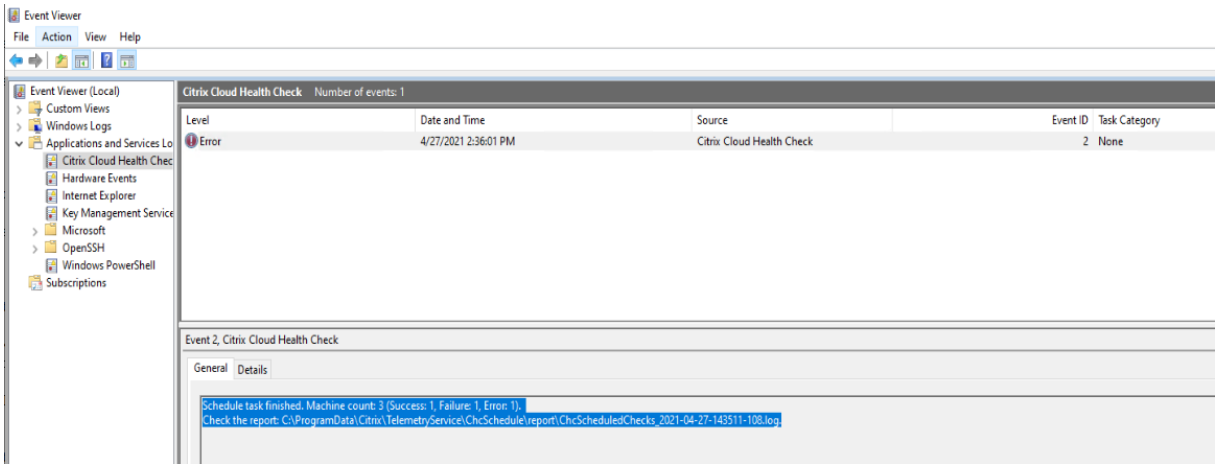



Alle Ergebnisse der Integritätsprüfung werden im Ordner "ChcSchedule"gespeichert. Die Cloud-Integritätsprüfung erstellt bei jeder Überprüfung drei Dateien. Bis zu 500 Iterationsprotokolle werden gespeichert.



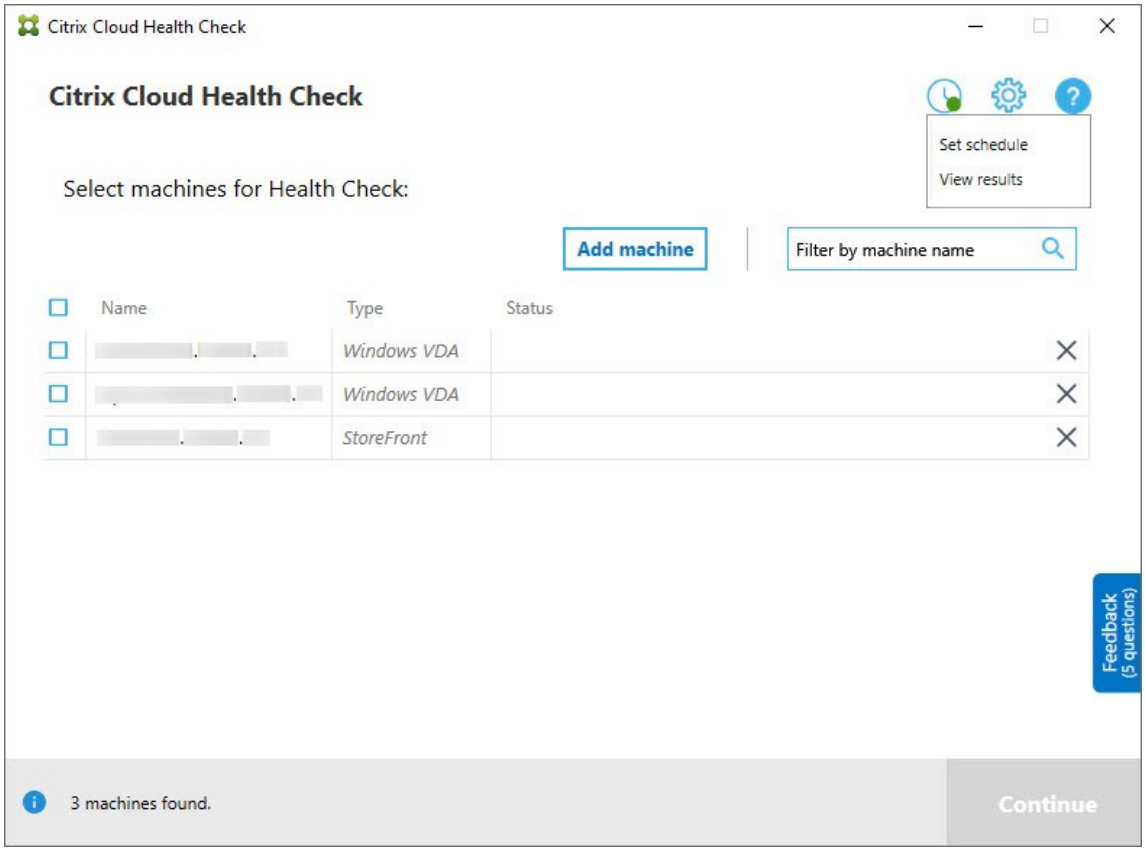

Wenn das Kontrollkästchen **Ausgabe von Ergebnissen in das Windows-Ereignisprotokoll** aktiviert ist, wird das Überprüfungsergebnis auch im Windows-Ereignisprotokoll verzeichnet.



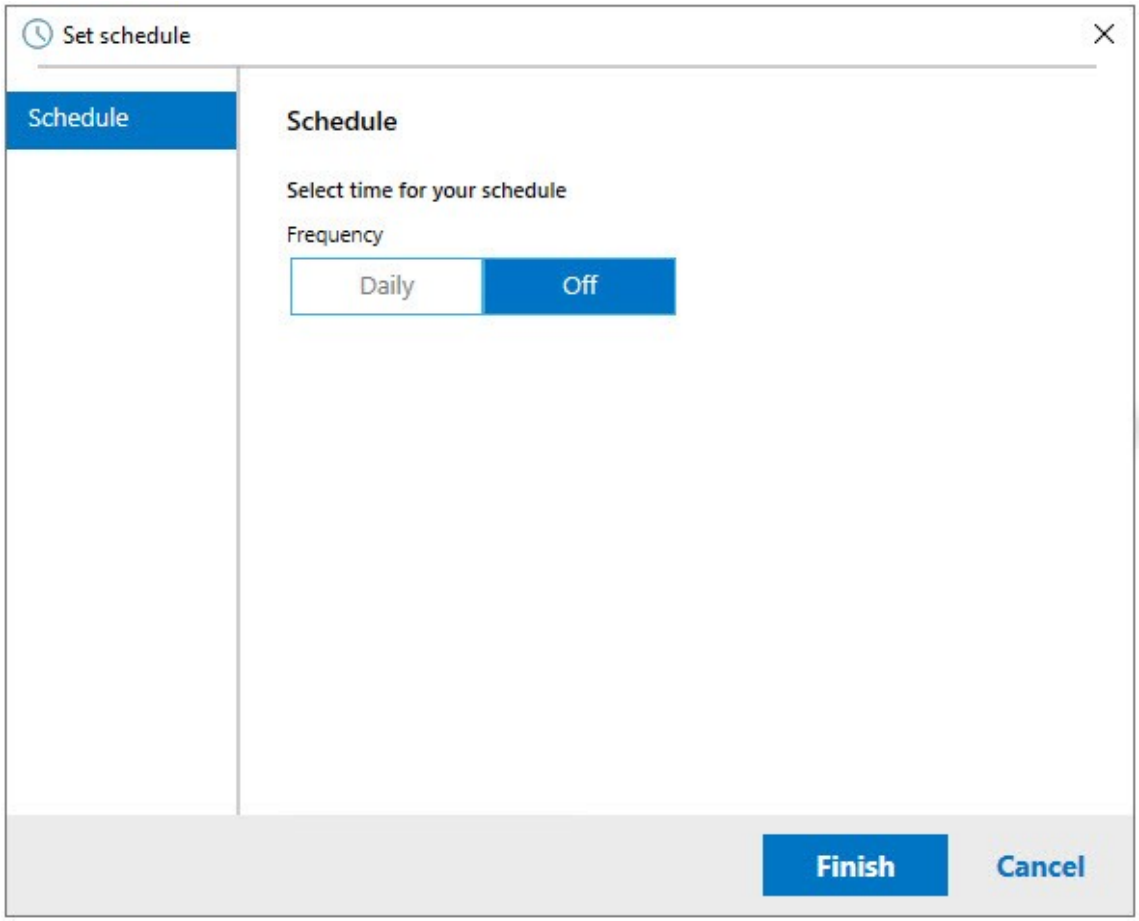
### Deaktivieren von Zeitplänen

1. Klicken Sie auf das Uhrensymbol und dann auf **Zeitplan festlegen**.




2. Klicken Sie auf **Aus** und dann auf **Fertig stellen**, um den Zeitplan zu deaktivieren.




**Weitere Informationen**

- Sie müssen zuerst VDAs zur Cloud-Integritätsprüfung hinzufügen bzw. in sie importieren. Weitere Informationen finden Sie unter Importieren von VDA-Maschinen.
- Der Zeitplaner der Cloud-Integritätsprüfung kann auf einer domänengebundenen Maschine nur jeweils eine Aufgabe planen. Wenn Sie mehrere Zeitpläne festlegen, wird nur der letzte wirksam.

## Tests zur Überprüfung

Vor Ausführung einer Integritätsprüfung wird automatisch jede ausgewählte Maschine überprüft. Diese Prüfung gewährleistet, dass die Anforderungen zum Ausführen der Prüfung erfüllt sind. Besteht eine Maschine den Test nicht, wird in Cloud Health Check eine Meldung mit einem Maßnahmenvorschlag angezeigt.

- **Cloud Health Check kann diese Maschine nicht erreichen:** Stellen Sie Folgendes sicher:
  - Die Maschine ist eingeschaltet.

  - Die Verbindung mit dem Netzwerk funktioniert ordnungsgemäß. (Dazu gehört u. U. eine Überprüfung der ordnungsgemäßen Konfiguration der Firewall.)
  - Datei- und Druckerfreigabe ist aktiviert. Weitere Informationen finden Sie in der Microsoft Dokumentation.

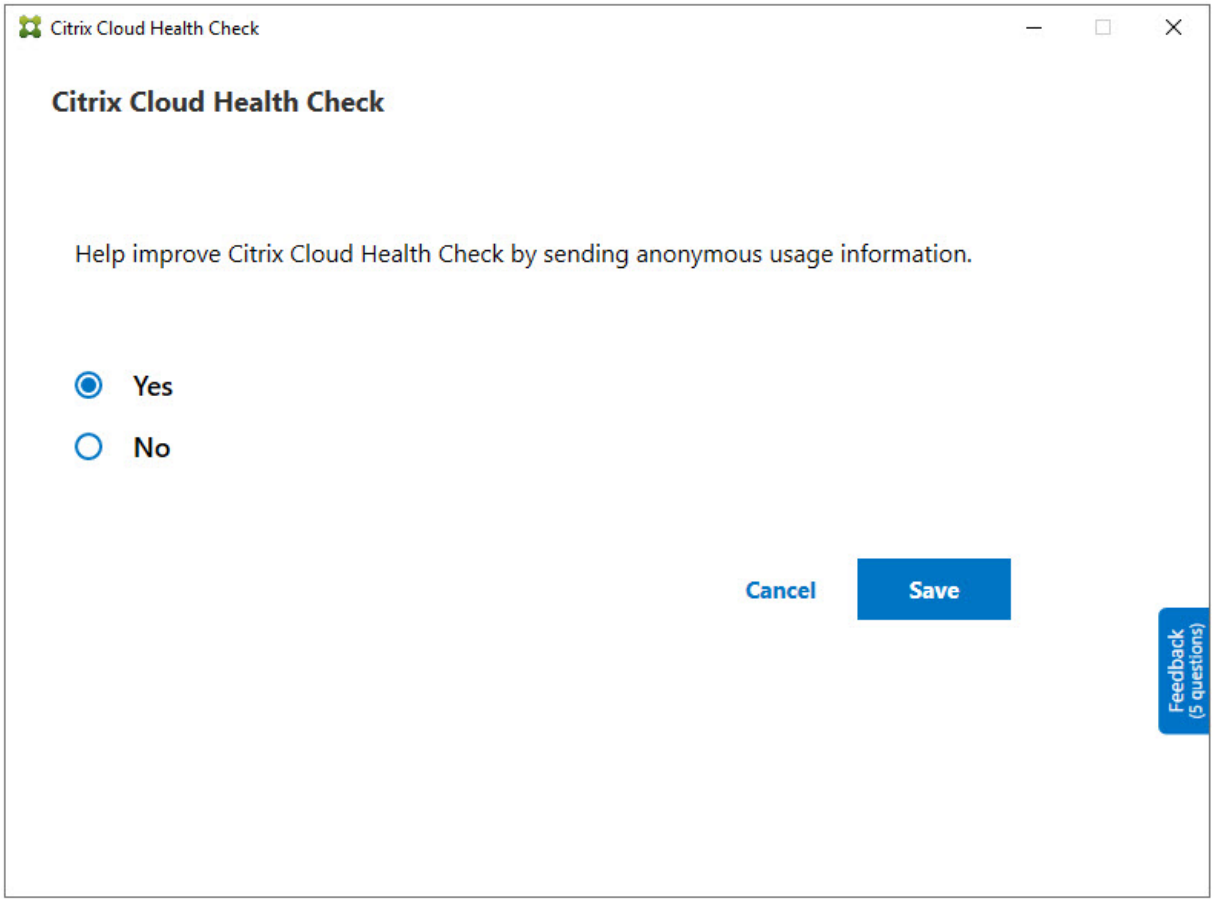
- **Aktivieren von PSRemoting und WinRM:** Sie können PowerShell-Remoting und WinRM aktivieren, indem Sie PowerShell als Administrator ausführen und dann das Cmdlet Enable-PSRemoting ausführen. Weitere Informationen finden Sie in der Microsoft-Hilfe zu dem Cmdlet.
- **Cloud Health Check erfordert PowerShell 3.0 oder später:** Installieren Sie PowerShell 3.0 auf der Maschine und aktivieren Sie dann PowerShell Remoting.
- **WMI wird nicht auf der Maschine ausgeführt:** Stellen Sie sicher, dass der Windows Management Instrumentation-Zugriff aktiviert ist.
- **WMI-Verbindungen blockiert:** Aktivieren Sie WMI im Windows-Firewalldienst.

### Erfassung von Nutzungsdaten

Wenn Sie Cloud Health Check verwenden, erfasst Citrix mit Google Analytics anonyme Nutzungsdaten, die für zukünftige Produktfeatures und Verbesserungen verwendet werden. Die Datenerfassung ist standardmäßig aktiviert.

Um die Erfassung und den Upload von Nutzungsdaten zu ändern, klicken Sie auf das **Einstellungen**-Zahnradsymbol in der Cloud Health Check-Benutzeroberfläche. Wählen Sie dann durch Klicken auf **Ja** oder **Nein** aus, ob die Informationen gesendet werden sollen, und klicken Sie auf **Speichern**.




### Automatischer Fix

Mit dem Feature "automatischer Fix"kann die Cloud-Integritätsprüfung bestimmte Probleme automatisch erkennen und beheben, indem sie Einstellungen ändert oder Dienste neu startet.

Beim automatischen Fix werden die folgenden VDA-Registrierungselemente geprüft und ggf. der empfohlene Fix ausgeführt:

- Domänenmitgliedschaft der VDA-Maschine
  - Fix: Verbindungssicherheitskanal zur Problemlösung mit einem "Reparatur"-Modell testen
- VDA-Dienststatus
  - Fix: BrokerAgent-Dienst neu starten
- Kommunikation mit dem Controller
  - Fix: BrokerAgent-Dienst neu starten
- Zeitsynchronisierung mit dem Controller

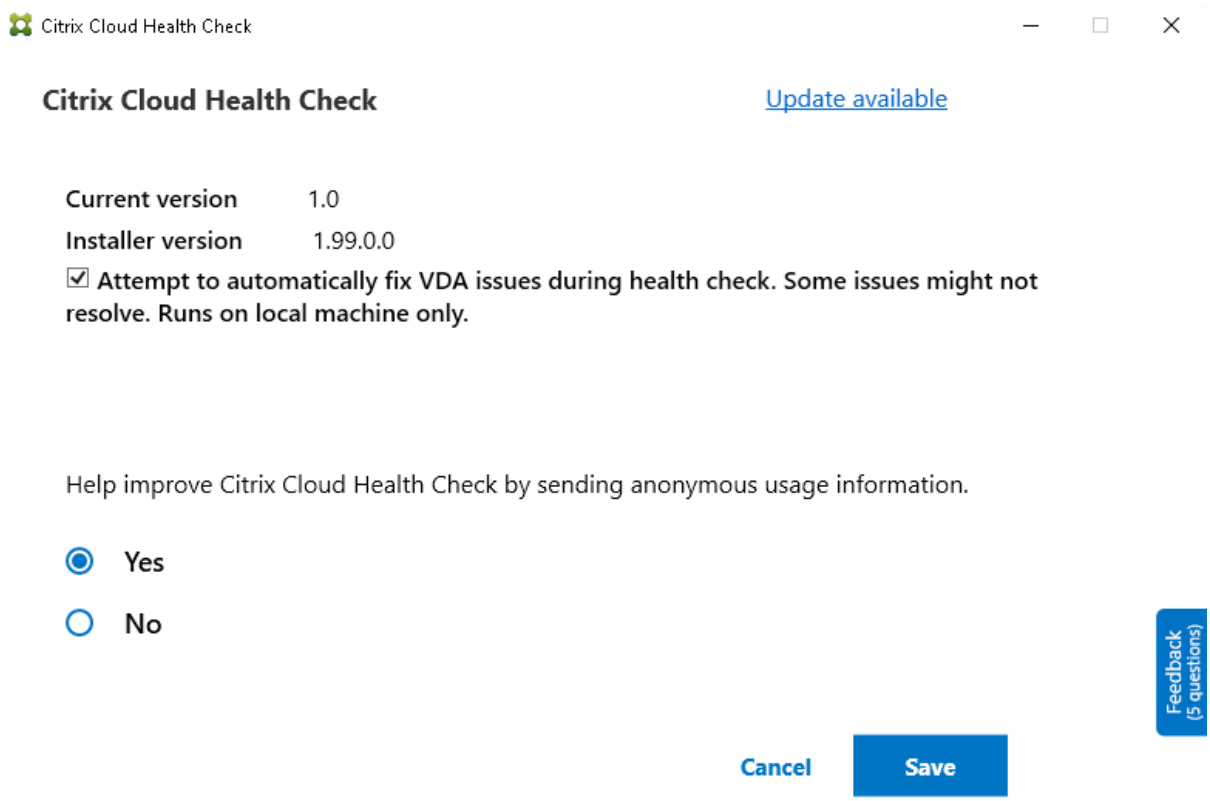
 

- Fix: Befehl “W32tm”ausführen

Bei Sitzungsstarts werden die folgenden Elemente geprüft und ggf. der empfohlene Fix ausgeführt:

- Status des Sitzungsstartdiensts
  - Fix: BrokerAgent-Dienst neu starten

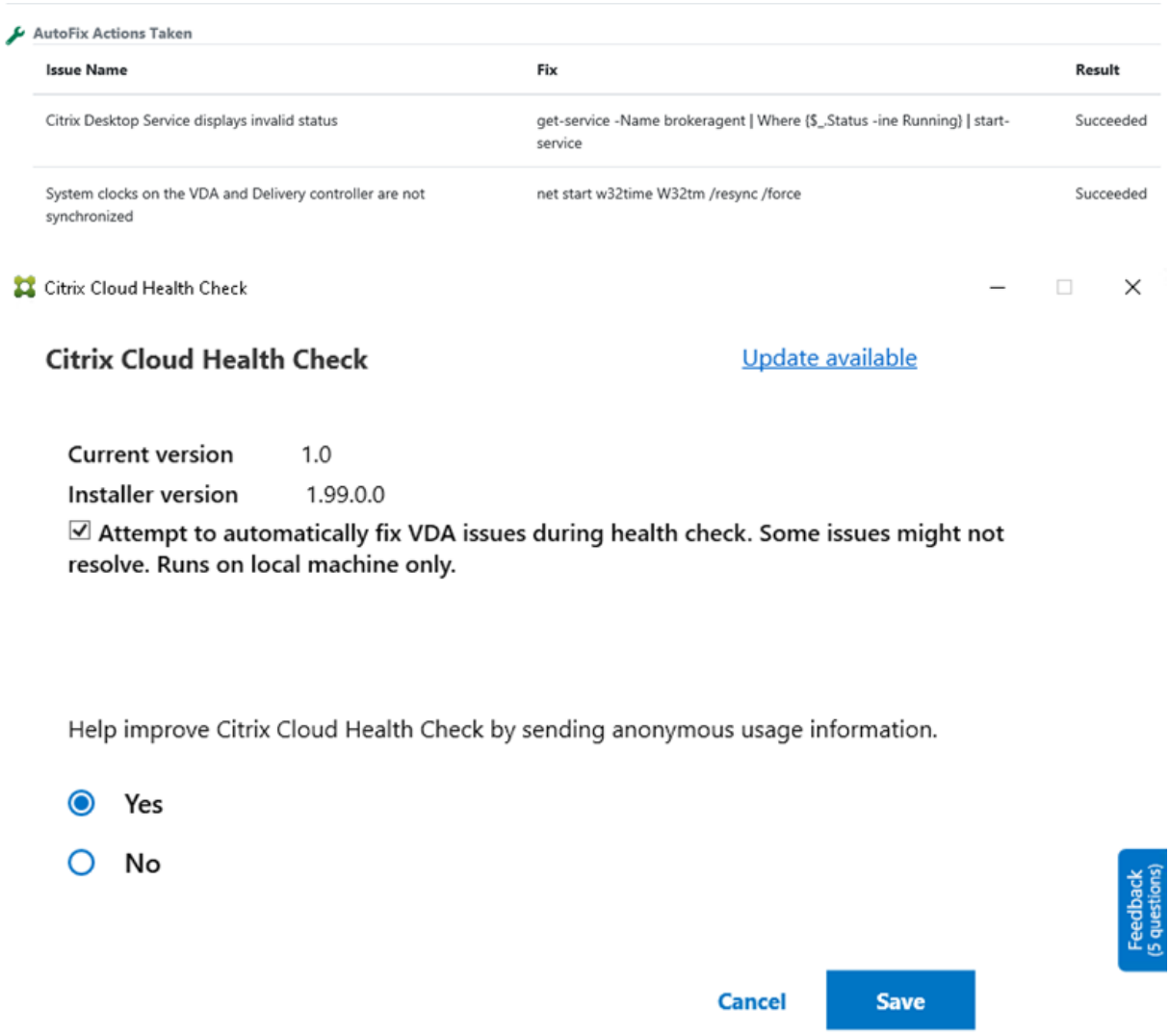
Das Feature ist in der Standardeinstellung aktiviert. Um es zu deaktivieren, klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke des Hauptfensters der Cloud-Integritätsprüfung und deaktivieren Sie **Es wird versucht, VDA-Probleme während der Systemintegritätsprüfung automatisch zu beheben**.




### Ergebnisbericht

Nachdem der automatische Fix ausgeführt wurde, werden die Prüfergebnisse im Bericht angezeigt:




## Problembehandlung

Wenn Cloud Health Check nicht ausgeführt werden kann oder eine Ausnahme auftritt, überprüfen Sie das Cloud Health Check-Protokoll in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

Das Cloud Health Check-Protokoll für jede Zielmaschine ist in `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

Gehen Sie zum Aktivieren des Debugprotokolls folgendermaßen vor:

Bearbeiten Sie `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, aktualisieren Sie `<add name="TraceLevelSwitch"value="3"/> to <add name="TraceLevelSwitch"value="4"/>`, speichern Sie die Datei und öffnen Sie Cloud

Health Check erneut.

### Feedback

Um Feedback zur Cloud-Integritätsprüfung zu hinterlassen, beantworten Sie die Fragen der Citrix Umfrage.

## Konfigurationsprotokollierung

May 17, 2024

> **Hinweis:**
>
> Das Konfigurationsprotokoll wird unabhängig von der für das Citrix Cloud-Konto gewählten Sprache auf Englisch angezeigt. Daten und Uhrzeiten werden im Format MM/TT/JJ sowie UTC (koordinierte Weltzeit) angegeben.

Die Konfigurationsprotokollierung erfasst Konfigurationsänderungen und Administratoraktivitäten in Bereitstellungen von Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) in einer Protokollierungsdatenbank in Citrix Cloud. Sie können den protokollierten Inhalt folgendermaßen verwenden:

- Diagnose und Behandlung von Problemen nach Konfigurationsänderungen. Das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen.
- Bericht über Administratoraktivitäten.

Die Konfigurationsprotokollierung ist in Citrix DaaS immer aktiviert. Sie können die Funktion nicht deaktivieren.

In der Verwaltungsoberfläche "Vollständige Konfiguration"können Sie den Inhalt des Konfigurationsprotokolls anzeigen, gefiltert nach Datumsbereichen oder mit Volltextsuche. Sie können auch einen CSV-Bericht mit PowerShell erstellen. Sie können in dieser Konsole den Protokollinhalt nicht bearbeiten oder löschen. Sie können das Remote PowerShell SDK verwenden, um das periodische Löschen von Daten aus dem Protokoll zu planen.

### Aktualisierung der Aufbewahrung von DaaS-Konfigurationsprotokollen

Um die Leistung der DaaS-Mandanten aufrechtzuerhalten, wird die Aufbewahrung der Konfigurationsprotokolle ab dem 9. September 2024 auf 180 Tage festgelegt.

Protokolle, die am 9. September 2024 älter sind als 180 Tage, werden gelöscht. Da wir unsere DaaS-Limits für einen einzelnen DaaS-Mandanten weiter erhöhen, gewährleistet diese Implementierung die beste Leistung und Belastbarkeit für unsere Kunden.

Als bewährte Methode empfehlen wir unseren Kunden, einen vierteljährlichen Exportmechanismus einzurichten. Dies kann über PowerShell erfolgen, siehe Berichte generieren. Wir empfehlen Kunden außerdem, das regelmäßige Löschen von Daten zu planen, siehe Regelmäßiges Löschen von Daten planen.

Erforderliche Berechtigungen (siehe Delegierte Administration):

- Volladministratoren in Citrix Cloud sowie Lesezugriffadministratoren und Cloudadministratoren für DaaS können Konfigurationsprotokolle in der Konsole **Verwalten** anzeigen.
- Volladministratoren und Cloudadministratoren können zudem mit PowerShell einen CSV-Bericht zur Protokollierungsaktivität herunterladen.

### Gegenstand der Protokollierung

Die folgenden Vorgänge werden protokolliert:

- Konfigurationsänderungen und Verwaltungsaktivitäten, die über die Registerkarten **Verwalten** oder **Überwachen** initiiert wurden
- PowerShell-Skripts
- REST-API-Anforderungen

> **Hinweis:**
>
> Sie können keine Protokolleinträge zu internen Prozessen der Citrix Cloud-Plattform anzeigen, z. B. zur Einrichtung und Verwaltung von Datenbanken.

Konfigurationsänderungen (Erstellen, Bearbeiten, Löschen, Zuweisen) werden beispielsweise für folgende Elemente protokolliert:

- Maschinenkataloge
- Bereitstellungsgruppen (einschließlich Ändern der Energieverwaltungseinstellungen)
- Administratorrollen und Geltungsbereiche
- Hostressourcen und Verbindungen
- Citrix Richtlinien über die Konsole **Verwalten**

Beispiele protokollierter Administratoraktivitäten:

- Energieverwaltung für eine virtuelle Maschine oder einen Benutzerdesktop
- Verwaltung oder Überwachung von Funktionen beim Versand einer Nachricht an einen Benutzer

Die folgenden Vorgänge werden nicht protokolliert (viele sind für Kundenadministratoren nicht verfügbar):

- Automatische Vorgänge wie das Einschalten virtueller Maschinen per Poolverwaltung.
- Über die Gruppenrichtlinien-Verwaltungskonsole implementierte Richtlinienaktionen. Verwenden Sie Microsoft-Tools, um Protokolle dieser Aktionen anzuzeigen.
- Änderungen, die über die Registrierung oder von anderen Quellen als der Verwaltungsoberfläche "Vollständige Konfiguration", Überwachen oder PowerShell vorgenommen wurden.

### Anzeigen des Konfigurationsprotokolls

Gehen Sie folgendermaßen vor, um den Inhalt des Konfigurationsprotokolls anzuzeigen:

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie **Eigene Services > DaaS** im Menü links oben.
2. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Protokollierung > Ereignisse**.

Standardmäßig wird im mittleren Bereich der Protokollinhalt chronologisch (neueste Einträge zuerst), angezeigt, wobei die Einträge durch das Datum getrennt sind. Sie haben folgende Möglichkeiten:

- Sortieren der Anzeige nach Spaltenüberschrift.
- Filtern der Anzeige, indem Sie ein Tagesintervall oder ein benutzerdefiniertes Intervall angeben oder Text in das Feld "Suchen"eingeben. Um nach dem Suchen zur Standardanzeige zurückzukehren, löschen Sie den Text im Feld Suchen.
- Wählen Sie aus, welche Spalten in der Anzeige angezeigt werden, indem Sie das Symbol **Anzuzeigende Spalten** in der oberen rechten Ecke der Tabelle auswählen. Um beispielsweise die IP-Adresse anzuzeigen, die der Administrator für den Zugriff auf DaaS verwendet, klicken Sie auf das Symbol und fügen Sie die Spalte **Client-IP** hinzu.

Anzeigeeigenschaften:

- Bei Verwaltung und Überwachung erstellte High-Level-Operationen werden im oberen mittleren Bereich aufgelistet. Eine High-Level-Operation führt zu mindestens einem Dienst- und PowerShell SDK-Aufruf (dies sind Low-Level-Operationen). Wenn Sie eine High-Level-Operation im oberen mittleren Bereich auswählen, werden im unteren Bereich die Low-Level-Operationen angezeigt.
- Wenn Sie eine Low-Level-Operation in PowerShell erstellen, ohne die übergeordnete High-Level-Operation anzugeben, wird von der Konfigurationsprotokollierung eine Ersatz-High-Level-Operation erstellt.
- Schlägt eine Operation vor der Beendigung fehl, kann die Protokollierung in der Datenbank evtl. nicht abgeschlossen werden. Beispielsweise hat ein Startdatensatz dann keinen entsprechenden Stoppdatensatz. In solchen Fällen wird im Protokoll angezeigt, dass Informationen

fehlen. Wenn Sie Protokolle auf Zeitbereichsbasis anzeigen, werden unvollständige Protokolle angezeigt, wenn die Daten in den Protokollen mit den Kriterien übereinstimmen. Beispiel: Wenn Protokolle für die letzten fünf Tage angefordert werden und ein Protokoll zwar eine in den letzten fünf Tagen gelegene Startzeit, aber keine Endzeit hat, wird dieses ebenfalls angezeigt.

- Nicht vergessen: Sie können keine Protokolleinträge zu internen Prozessen der Citrix Cloud-Plattform anzeigen, z. B. zur Einrichtung und Verwaltung von Datenbanken.

### Anzeigen von Aufgaben im Zusammenhang mit Maschinenkatalogen

Um Aufgaben im Zusammenhang mit Maschinenkatalogen anzuzeigen, gehen **Sie zu Verwalten > Vollständige Konfiguration > Protokollierung > Aufgaben**. Auf der Registerkarte **Aufgaben** werden nur Aufgaben angezeigt, die sich auf mit den Maschinenerstellungsdiensten (MCS) oder Provisioning Services (PVS) erstellte Kataloge beziehen. Es werden Aufgaben zu den folgenden Maschinenkatalogvorgängen angezeigt:

- Kataloge erstellen
- Kataloge klonen
- Maschinen hinzufügen
- Maschinen entfernen
- Aktualisieren eines Katalogs (Images oder Maschinen)
- Rollback von Maschinenupdates

> **Tipp:**
>
> Auf der Registerkarte **Aufgaben** werden nur Aufgaben angezeigt, die sich auf Änderungen des Provisioningschemas beziehen (Erstellen oder Ändern eines Provisioningschemas).

Eine Aufgabe kann sich im folgenden Zustand befinden:

- Erledigt
- Nicht gestartet
- Wird ausgeführt
- Abgebrochen
- Fehler
- Unbekannt

Um eine laufende Aufgabe abzubrechen, wählen Sie die Aufgabe aus und klicken dann auf **Abbrechen**. Das Abbrechen dauert einige Zeit.

Beispiele protokollierter Aufgaben:

- Imageupdate für einen Katalog abgeschlossen

- Fehler beim Aktualisieren des Images für einen Katalog
- Imageupdate für einen Katalog abgebrochen
- Provisioning von VMs für einen Katalog erfolgt
- Entfernen von VMs aus einem Katalog
- Ein Katalog wurde erstellt

Standardmäßig werden die protokollierten Tasks im mittleren Bereich chronologisch (neueste Einträge zuerst), angezeigt, wobei die Einträge durch das Datum getrennt sind. Sie können die Anzeige nach Spaltenüberschrift sortieren. Um abgeschlossene Aufgaben zu löschen, klicken Sie auf der Registerkarte **Aufgaben** auf **Abgeschlossene Aufgaben löschen**. Um auszuwählen, welche Spalten angezeigt werden sollen, wählen Sie das Symbol **Anzuzeigende Spalten** in der oberen rechten Ecke der Tabelle aus.

### Anzeigen von API-Protokollen

Um REST-API-Protokolle anzuzeigen, gehen Sie zu **Verwalten > Vollständige Konfiguration > Protokollierung > APIs**. Auf der Registerkarte **APIs** werden die während eines bestimmten Zeitraums aufgetretenen REST-API-Anforderungen angezeigt.

Hinweis:

- REST API-Protokolle werden gelöscht, nachdem Sie sich von der Konsole abgemeldet haben. (Sie werden auch gelöscht, wenn Sie Ihr Browserfenster aktualisieren.)
- Für jede Operation in der Konsole, die zu einem API-Aufruf führt, wird die entsprechenden API-Anforderung auf der Registerkarte **APIs** angezeigt.
- Die API-Anforderungen werden getrennt nach Datum in chronologischer Reihenfolge angezeigt (neueste Einträge zuerst). Es werden maximal 1.000 API-Anforderungen angezeigt.

### PowerShell-Protokolle anzeigen

Um PowerShell-Befehle anzuzeigen, die den UI-Aktionen entsprechen, die Sie im Laufe des Tages ausgeführt haben, navigieren Sie zur Registerkarte **Verwalten > Vollständige Konfiguration > Protokollierung > PowerShell**.

### Metadaten zu Konfigurationsprotokollen zuordnen

Sie können Metadaten Konfigurationsprotokolle anfügen, indem Sie den Protokolldatensätzen das `MetadataMap`-Paar `name-value` zuordnen.

> **Hinweis:**
>
> - Sie können Metadaten nur High-Level-Operation-Objekten anfügen.
> - Die Metadaten werden den vorhandenen Datensätzen zum Zeitpunkt der Ausführung zugeordnet.

#### Metadaten festlegen

Führen Sie den PowerShell-Befehl `Set-LogHighLevelOperationMetadata` aus, um einem Protokolldatensatz `MetadataMap` anzufügen.
`Set-LogHighLevelOperationMetadata` hat folgende Parameter:

- **Id:** ID der High-Level-Operation.
- **InputObject:** High-Level-Operationen, zu denen Sie die Metadaten hinzufügen. Dies ist eine Alternative zu Parameter `Id`, mit dem ein High-Level-Operationsobjekt (bzw. eine Objektliste) an den PowerShell-Befehl übergeben wird.
- **Name:**Eigenschaftsname der Metadaten, die hinzugefügt werden sollen. Die Eigenschaft muss für die angegebene High-Level-Operation eindeutig sein. Die Eigenschaft darf keines der folgenden Zeichen enthalten:
  `()\/;:#.*?=<>|[]"'`
- **Value**:Wert der Eigenschaft
- **Map:**Wörterbuch von name-value-Paaren für die Eigenschaften. Dies ist eine Alternative zum Festlegen der Metadaten mithilfe der Parameter `-Name` und `-Value`.

Führen Sie beispielsweise den folgenden PowerShell-Befehl aus, um die Metadaten an alle High-Level-Protokolldatensätze mit der ID 40 anzufügen:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

Führen Sie den folgenden PowerShell-Befehl aus, um die Metadaten an den High-Level-Datensatz mit dem Benutzer `abc@example.com` anzufügen:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

#### Anhand von Metadaten abrufen

Führen Sie die folgenden PowerShell-Befehle aus, um Protokolldatensätze anhand der zugehörigen Metadaten abzurufen:

- Suche nach Schlüssel und Wert:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Suche nach Wert und beliebigem Schlüssel:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Suche nach Schlüssel und einem beliebigen Wert:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

#### Metadaten entfernen

Führen Sie den PowerShell-Befehl `Remove-LogHighLevelOperationMetadata` aus, um zugeordnete Metadaten zu entfernen.
`Remove-LogHighLevelOperationMetadata` hat folgende Parameter:

- **Id:** ID der High-Level-Operation.
- **InputObject:** High-Level-Operationen, zu denen Sie die Metadaten hinzufügen. Dies ist eine Alternative zu Parameter `Id`‘, mit dem ein High-Level-Operationsobjekt (bzw. eine Objektliste) an den PowerShell-Befehl übergeben wird.
- **Name:**Eigenschaftsname der Metadaten, die entfernt werden sollen. $null entfernt alle Metadaten aus dem angegebenen Objekt.
- **Map:**Wörterbuch von name-value-Paaren für die Eigenschaften. Dies kann entweder eine Hashtabelle sein (erstellt mit @{“name1”= “val1”; “name2”= “val2”}) oder ein Zeichenkettenwörterbuch (erstellt mit new-object “System.Collections.Generic.Dictionary[String, String]”). Die Eigenschaften, deren Namen mit den Schlüsseln in Map übereinstimmen, werden entfernt.

### Erstellen von Berichten

Verwenden Sie PowerShell-Cmdlets für den ConfigLogging-Service im Citrix Virtual Apps and Desktops Remote PowerShell SDK, um einen CSV- oder HTML-Bericht mit Konfigurationsprotokolldaten zu erstellen. Einzelheiten finden Sie in den folgenden Abschnitten:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

### Periodische Datenlöschung planen

Verwenden Sie das Remote PowerShell SDK, um anzugeben, wie lange Daten in der Datenbank für die Konfigurationsprotokollierung aufbewahrt werden. (Dieses Feature ist in der Verwaltungsoberfläche “Vollständige Konfiguration”nicht verfügbar.) In Citrix DaaS müssen Sie Vollzugriff haben.

Im Cmdlet `Set-LogSite` gibt der Parameter `-LoggingDBPurgeDurationDays` an, wie viele Tage Daten in der Datenbank für die Konfigurationsprotokollierung aufbewahrt werden, bevor sie automatisch gelöscht werden.

- Standardmäßig ist der Wert dieses Parameters 0. Der Wert von Null bedeutet, dass Daten in der Konfigurationsprotokollierungsdatenbank nie automatisch gelöscht werden.
- Wenn Sie einen Wert ungleich Null festlegen, wird die Datenbank alle 120 Minuten überprüft. Daten, die älter als der Aufbewahrungszeitraum sind, werden gelöscht.

Verwenden Sie `Get-LogSite`, um den aktuellen Wert des Parameters anzuzeigen.

### Unterschiede zur On-Premises-Version von Citrix Virtual Apps and Desktops

Die Citrix Cloud-Version weist einige Unterschiede zur Konfigurationsprotokollierung in der On-Premises-Version von Virtual Apps and Desktops auf. In Citrix Cloud:

- Die Konfigurationsprotokollierung ist immer aktiviert. Sie können die Funktion nicht deaktivieren. Verbindliche Protokollierung ist nicht verfügbar.
- Sie können den Speicherort für die Konfigurationsprotokollierungsdatenbank nicht ändern, da die Datenbank in der Citrix Cloud-Plattform verwaltet wird.
- Konfigurationsprotokollanzeigen enthalten keine Vorgänge und Aktivitäten, die innerhalb der Citrix Cloud-Plattform ausgeführt werden.
- CSV- und HTML-Berichte über protokollierte Vorgänge können nur mithilfe von PowerShell erstellt werden. Im On-premises-Produkt können Berichte in Citrix Studio oder PowerShell generiert werden.
- Sie können den Inhalt des Konfigurationsprotokolls nicht löschen.

## Delegierte Administration

March 30, 2024

### Übersicht

Mit der delegierten Administration können Sie in Citrix Cloud die Zugriffsberechtigungen aller Administratoren gemäß ihrer Rolle in der Organisation konfigurieren.

Standardmäßig haben Administratoren Vollzugriff. Diese Einstellung ermöglicht den Zugriff auf alle kundenbezogenen Administrations- und Verwaltungsfunktionen in Citrix Cloud und auf alle abonnierten Dienste. Die Zugriffsrechte eines Administrators lassen sich folgendermaßen anpassen:

- Benutzerdefinierter Zugriff des Administrators auf allgemeine Verwaltungsberechtigungen in Citrix Cloud.

- Benutzerdefinierter Zugriff auf abonnierte Dienste. In Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) können Sie die Zugriffsrechte eines neuen Administrators direkt bei der Einladung benutzerdefiniert festlegen. Sie können den Zugriff eines Administrators später ändern.

Weitere Informationen zur Anzeige der Administratorliste und zum Definieren von Zugriffsberechtigungen finden Sie unter Administratorzugriff auf Citrix Cloud verwalten.

In diesem Artikel wird beschrieben, wie Sie den benutzerdefinierten Zugriff in Citrix DaaS konfigurieren.

## Administratoren, Rollen und Geltungsbereiche

Die Delegierte Administration verwendet drei Konzepte für den benutzerdefinierten Zugriff: Administratoren, Rollen und Geltungsbereiche.

- **Administratoren:** Ein Administrator ist eine Person, die durch ihre Citrix Cloud-Anmeldeinformationen (meist eine E-Mail-Adresse) identifiziert wird. Jeder Administrator ist mit mindestens einem Paar aus Rolle und Geltungsbereich verknüpft.
- **Rollen:** Eine Rolle steht für eine spezielle Jobfunktion, mit der bestimmte Berechtigungen verknüpft sind. Damit sind Aufgaben möglich, die nur für Citrix DaaS gelten. Die Rolle des Bereitstellungsgruppenadministrators berechtigt beispielsweise dazu, Bereitstellungsgruppen zu erstellen oder Desktops aus einer Bereitstellungsgruppe zu entfernen. Ein Administrator kann mehrere Rollen haben. Ein Administrator kann ein Bereitstellungsgruppenadministrator und ein Maschinenkatalogadministrator sein.

  Citrix DaaS bietet auch mehrere integrierte Rollen für den benutzerdefinierten Zugriff. Sie können die Berechtigungen in den vordefinierten Rollen nicht ändern und die Rollen auch nicht löschen.

  Sie können Ihre eigenen benutzerdefinierten Zugriffsrollen erstellen, um die Anforderungen Ihrer Organisation zu erfüllen, und Berechtigungen mit detaillierter delegieren. Verwenden Sie benutzerdefinierte Rollen, um Berechtigungen in der Granularität einer Aktion oder Aufgabe zuzuteilen. Sie können eine benutzerdefinierte Rolle nur löschen, wenn sie keinem Administrator zugewiesen ist.

  Sie können die Rollen jedoch für jeden Administrator anpassen.

  Eine Rolle ist stets mit einem bestimmten Geltungsbereich verknüpft.
- **Geltungsbereiche**: Ein Geltungsbereich steht für eine Sammlung von Objekten. Geltungsbereiche dienen dazu, Objekte auf relevante Weise im Unternehmen zu gruppieren. Objekte können auch in mehreren Geltungsbereichen sein.

Der einzige integrierte Geltungsbereich "Alle"enthält alle Objekte. Citrix Cloud- und Helpdesk-Administratoren sind immer mit dem Geltungsbereich "Alle"verknüpft. Dieser Bereich kann für diese Administratoren nicht geändert werden.

Wenn Sie einen Administrator einladen und zum Service hinzufügen, ist eine Rolle stets mit einem Geltungsbereich verknüpft (standardmäßig mit dem Geltungsbereich "Alle").

Sie erstellen und löschen Geltungsbereiche in der Oberfläche **Verwalten > Vollständige Konfiguration**. Sie erstellen verknüpfte Rollen-/Geltungsbereichspaare in der Citrix Cloud-Konsole.

Für Administratoren mit Vollzugriff wird kein Geltungsbereich angezeigt. Diese Administratoren haben per Definition Zugriff auf alle kundenverwalteten Objekte in Citrix Cloud und in abonnierten Diensten.

### Integrierte Rollen und Bereiche

Folgende Rollen sind in Citrix DaaS vordefiniert.

- **Cloudadministrator:** Kann alle Aufgaben ausführen, die von Citrix DaaS initiiert werden können.

  Kann die Registerkarten **Verwalten** und **Überwachen** in der Konsole sehen. Diese Rolle wird stets mit dem Geltungsbereich "Alle"kombiniert. Sie können diesen Bereich nicht ändern.

  Lassen Sie sich vom Namen der Rolle nicht täuschen. Ein Cloudadministrator mit benutzerdefiniertem Zugriff kann keine Aufgaben auf Citrix Cloud-Ebene durchführen (für Citrix Cloud-Aufgaben ist ein Vollzugriff erforderlich).

- **Lesezugriffsadministrator:** Kann alle Objekte in den angegebenen Geltungsbereichen (und globale Informationen) sehen, aber keine Änderungen vornehmen. Ein Lesezugriffadministrator mit dem Geltungsbereich London kann beispielsweise alle globalen Objekte und alle Objekte für den Geltungsbereich London (z. B. London-Bereitstellungsgruppen) sehen. Dieser Administrator kann jedoch nicht die Objekte im Geltungsbereich "New York"sehen (sofern die Geltungsbereiche "London"und "New York"einander nicht überlappen).

  Kann die Registerkarten **Verwalten** und **Überwachen** in der Konsole sehen.

- **Helpdeskadministrator:** Kann Bereitstellungsgruppen sehen und die diesen Gruppen zugeordneten Sitzungen und Maschinen verwalten. Kann den Maschinenkatalog und die Hostinformationen der überwachten Bereitstellungsgruppen sehen. Kann auch Sitzungsverwaltungs- und Energieverwaltungsvorgänge für die Maschinen in diesen Bereitstellungsgruppen durchführen.

  Kann die Registerkarte **Überwachen** in der Konsole sehen. Kann die Registerkarte **Verwalten** nicht anzeigen. Diese Rolle wird stets mit dem Geltungsbereich "Alle"kombiniert. Sie können diesen Bereich nicht ändern.

- **Maschinenkatalogadministrator:** Kann Maschinenkataloge erstellen und verwalten sowie Maschinen in ihnen bereitstellen. Kann Basisimages verwalten und Software installieren, aber Benutzern keine Anwendungen oder Desktops zuweisen.

  Kann die Registerkarten **Überwachen** und **Verwalten** in der Konsole sehen. Kann die Registerkarte **Überwachen** nicht sehen. Sie können den Geltungsbereich ändern.

- **Bereitstellungsgruppenadministrator:** Kann Anwendungen, Desktops und Maschinen bereitstellen. Kann auch die zugehörigen Sitzungen verwalten. Kann Anwendungs- und Desktopkonfigurationen wie Richtlinien und Energieverwaltungseinstellungen verwalten.

  Kann die Registerkarten **Überwachen** und **Verwalten** in der Konsole sehen. Sie können den Geltungsbereich ändern.

  > **Hinweis:**
  >
  > Sie benötigen die Berechtigung **Maschinenupdate ausführen**, um den Anzeigenamen eines Desktops als Bereitstellungsgruppenadministrator zu ändern. Diese Berechtigung ist erforderlich, weil beim Ändern des Anzeigenamens die Maschineneigenschaft aktualisiert werden muss.

- **Hostadministrator:** Kann Hostverbindungen und ihre zugehörigen Ressourceneinstellungen verwalten. Kann keine Maschinen, Anwendungen oder Desktops für Benutzer bereitstellen.

  Kann die Registerkarten **Verwalten** in der Konsole sehen. Kann die Registerkarte **Überwachen** nicht sehen. Sie können den Geltungsbereich ändern.

- **Sitzungsadministrator:** Kann überwachte Bereitstellungsgruppen sehen und die zugehörigen Sitzungen und Maschinen verwalten.

  Kann die Registerkarte **Überwachen** in der Konsole sehen. Kann die Registerkarte **Verwalten** nicht anzeigen. Sie können diesen Bereich nicht ändern.

- **Volladministrator:** Kann alle Aufgaben und Vorgänge ausführen. Ein Volladministrator wird stets mit dem Geltungsbereich **Alle** kombiniert.

  Kann die Registerkarten **Verwalten** und **Überwachen** in der Konsole sehen. Diese Rolle wird stets mit dem Geltungsbereich **Alle** kombiniert. Sie können diesen Bereich nicht ändern.

- **Volladministrator für "Überwachen":** Hat vollen Zugriff auf alle Ansichten und Befehle auf der Registerkarte **Überwachen**.

  Kann die Registerkarte **Überwachen** in der Konsole sehen. Kann die Registerkarte **Verwalten** nicht anzeigen. Sie können diesen Bereich nicht ändern.

- **Administrator für Probe Agent:** Hat Zugriff auf Probe Agent-APIs.

  Kann die Registerkarten **Überwachen** und **Verwalten** in der Konsole sehen. Hat nur Lesezugriff auf die Seite **Anwendungen** und kann nicht auf andere Ansichten zugreifen.

In der folgenden Tabelle ist zusammengefasst, welche Konsolenregisterkarten für die einzelnen Rollen in Citrix DaaS sichtbar sind und ob die Rolle mit benutzerdefinierten Geltungsbereichen verwendet werden kann.

| Administratorrolle mit benutzerdefiniertem Zugriff | Konsole mit Registerkarte **Verwalten**? | Konsole mit Registerkarte **Überwachen**? | Benutzerdefinierte Geltungsbereiche verwendbar? |
|---|---|---|---|
| Cloudadministrator | Ja | Ja | Nein |
| Lesezugriffadministrator | Ja | Ja | Ja |
| Helpdeskadministrator | Nein | Ja | Nein |
| Maschinenkatalogadministrator | Ja | Ja | Ja |
| Bereitstellungsgruppenadministrator | Ja | Ja | Ja |
| Hostadministrator | Ja | Nein | Ja |
| Sitzungsadministrator | Nein | Ja | Nein |
| Volladministrator | Ja | Ja | Nein |
| Volladministrator für Überwachen | Nein | Ja | Nein |
| Administrator für Probe Agent | Ja | Ja | Nein |

> **Hinweis:**
>
> Außer Cloudadministrator und Helpdeskadministrator sind für Citrix Virtual Apps and Desktops Standard für Azure, Virtual Apps Essentials und Virtual Desktops Essentials keine Administratorrollen mit benutzerdefiniertem Zugriff verfügbar.

Anzeige der zugewiesenen Berechtigungen für eine Rolle:

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie **Eigene Services > DaaS** im Menü links oben.
2. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Administratoren**.
3. Wählen Sie die Registerkarte **Rollen**.
4. Wählen Sie im oberen mittleren Bereich eine Rolle aus. Auf der Registerkarte **Rollendefinition** im unteren Bereich sind alle Kategorien und Berechtigungen aufgelistet. Wählen Sie eine Kategorie aus, um die spezifischen Berechtigungen anzuzeigen. Auf der Registerkarte **Administratoren** sind die Administratoren aufgelistet, denen die ausgewählte Rolle zugewiesen wurde.

   Bekanntes Problem: Ein Volladministrator-Eintrag zeigt nicht den richtigen Berechtigungssatz für einen Citrix DaaS-Administrator mit Vollzugriff an.

### Anzahl der benötigten Administratoren

Die Anzahl der Administratoren und die Granularität der Berechtigungen hängen im Allgemeinen von der Größe und Komplexität der Bereitstellung ab.

- In kleinen Bereitstellungen oder Machbarkeitsstudien übernehmen ein oder wenige Administratoren alle Aufgaben. Es gibt keine benutzerdefinierte Zugriffsdelegierung. In diesem Fall erhält jeder Administrator Vollzugriff, der stets mit dem Geltungsbereich "Alle"verknüpft ist.
- In größeren Bereitstellungen mit mehr Maschinen, Anwendungen und Desktops ist mehr Delegierung erforderlich. Mehrere Administratoren haben möglicherweise bestimmte funktionale Zuständigkeiten (Rollen). Dann haben beispielsweise zwei Administratoren Vollzugriff, während andere als Helpdeskadministratoren fungieren. Auch werden von einem Administrator ggf. nur bestimmte Objektgruppen (Geltungsbereiche) wie Maschinenkataloge in einer bestimmten Abteilung verwaltet. Erstellen Sie in diesem Fall neue Geltungsbereiche und Administratoren, und weisen Sie diesen eine benutzerdefinierte Zugriffsrolle und die entsprechenden Geltungsbereiche zu.

### Zusammenfassung der Administratorverwaltung

Das Einrichten von Administratoren für Citrix DaaS folgt dieser Reihenfolge:

1. Wenn der Administrator eine andere Rolle als Volladministrator (deckt alle abonnierten Dienste in Citrix Cloud ab) oder eine integrierte Rolle haben soll, erstellen Sie eine benutzerdefinierte Rolle.
2. Wenn der Administrator einen anderen Geltungsbereich als "Alle"haben soll (und ein anderer Geltungsbereich für die beabsichtigte Rolle zulässig ist und nicht bereits erstellt wurde): erstellen Sie Geltungsbereiche.
3. Dann können Sie in Citrix Cloud einen Administrator einladen. Wenn der neue Administrator nicht den standardmäßigen Vollzugriff erhalten soll, legen Sie ein benutzerdefiniertes Zugriffsrollen-/Geltungsbereichspaar fest.

Wenn Sie den Zugriff eines Administrators (Rollen und Geltungsbereiche) später ändern möchten, gehen Sie wie unter Konfigurieren von benutzerdefiniertem Zugriff beschrieben vor.

### Administrator hinzufügen

Zum Hinzufügen (Einladen) eines Administrators folgen Sie den Anweisungen unter Hinzufügen von Administratoren zu einem Citrix Cloud-Konto. Ein Teil dieser Informationen wird hier wiederholt.

> **Wichtig:**
>
> Beachten Sie, wie "benutzerdefiniert"und "benutzerdefinierter Zugriff"verwendet werden.
>
> - Beim Erstellen von Administratoren und Zuweisen von Rollen für Citrix DaaS in der Citrix Cloud-Konsole umfasst der Begriff "benutzerdefinierter Zugriff"sowohl vordefinierte Rollen als auch alle zusätzlichen benutzerdefinierten Rollen, die in der Oberfläche **Verwalten > Vollständige Konfiguration** des Diensts erstellt wurden.
> - In der Oberfläche **Verwalten > Vollständige Konfiguration** des Diensts ist eine "benutzerdefinierte"Rolle einfach nur eine Rolle, die nicht integriert ist.

Der allgemeine Workflow beim Hinzufügen von Administratoren ist wie folgt:

1. Melden Sie sich bei **Citrix Cloud** an und wählen Sie im Menü oben links Identitäts- und Zugriffsverwaltung.
2. Wählen Sie auf der Seite **Identitäts- und Zugriffsverwaltung** die Option **Administratoren**. Auf der Registerkarte **Administratoren** werden alle aktuellen Administratoren für das Konto aufgeführt.
3. Wählen Sie auf der Registerkarte **Administratoren** den Identitätstyp aus, geben Sie die E-Mail-Adresse des Administrators ein und klicken Sie dann auf **Einladen**.

- Wählen Sie **Vollzugriff**, wenn der Administrator vollen Zugriff haben soll. Damit kann der Administrator auf alle kundenbezogenen Administrations- und Verwaltungsfunktionen in Citrix Cloud und auf alle abonnierten Dienste zugreifen.
- Wählen Sie **Benutzerdefinierter Zugriff**, wenn der Administrator eingeschränkten Zugriff erhalten soll. Sie können dann ein benutzerdefiniertes Zugriffsrollen-/Bereichspaar auswählen. Auf diese Weise hat der Administrator die gewünschten Berechtigungen, wenn er sich bei Citrix Cloud anmeldet.

1. Klicken Sie auf **Einladung senden**. Citrix Cloud sendet eine Einladung an die von Ihnen angegebene E-Mail-Adresse und fügt den Administrator der Liste hinzu, wenn der Administrator das Onboarding abgeschlossen hat.

Beim Erhalt der E-Mail klickt der Administrator auf den Link **Anmelden**, um die Einladung anzunehmen.

Weitere Informationen zum Hinzufügen von Administratoren finden Sie unter Verwalten von Citrix Cloud-Administratoren.

Klicken Sie alternativ unter **Verwalten > Vollständige Konfiguration > Administratoren > Administratoren** auf **Administrator hinzufügen**. Der Bereich **Identitäts- und Zugriffsverwaltung > Administratoren** wird direkt in einer neuen Browser-Registerkarte geöffnet. Nachdem Sie dort Administratoren hinzugefügt haben, schließen Sie die Registerkarte und kehren Sie zur Konsole zurück, um mit anderen Konfigurationsaufgaben fortzufahren.

### Erstellen und Verwalten von Rollen

Wenn Administratoren eine Rolle erstellen oder bearbeiten, können sie nur die Berechtigungen aktivieren, die sie selbst haben. Dadurch wird verhindert, dass Administratoren eine Rolle mit mehr Berechtigungen erstellen, als sie derzeit haben, und sie dann sich selbst zuweisen (oder eine ihnen bereits zugewiesene Rolle bearbeiten).

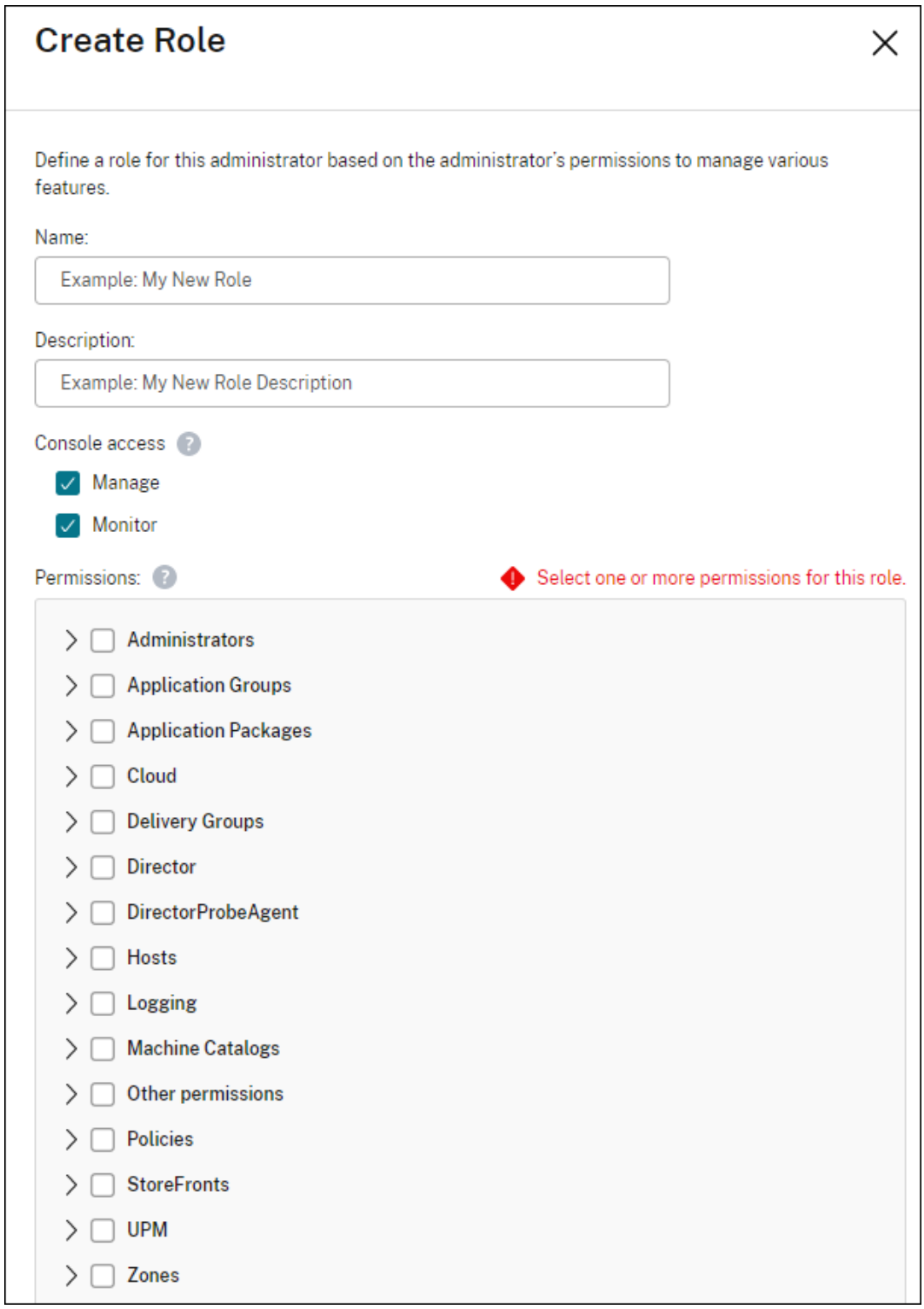
Namen für benutzerdefinierte Rollen können bis zu 64 Unicode-Zeichen haben. Namen dürfen keines der folgenden Zeichen enthalten: umgekehrter Schrägstrich, Schrägstrich, Semikolon, Doppelpunkt, Nummernzeichen, Komma, Sternchen, Fragezeichen, Gleichheitszeichen, Größer-Als- oder Kleiner-Als-Zeichen, senkrechter Strich, eckige Klammern, runde Klammern, Anführungszeichen und Apostroph.

Rollenbeschreibungen können bis zu 256 Unicode-Zeichen haben.

1. Melden Sie sich bei Citrix Cloud an, falls Sie es noch nicht getan haben. Wählen Sie **Eigene Services > DaaS** im Menü links oben.
2. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Administratoren**.
3. Wählen Sie die Registerkarte **Rollen**.
4. Folgen Sie den Anweisungen für die Aufgabe, die Sie ausführen möchten:

   - **Anzeigen von Rollendetails:** Wählen Sie die Rolle im mittleren Bereich aus. Im unteren Teil des mittleren Bereichs werden die Objekttypen und die zugehörigen Berechtigungen für die Rolle angezeigt. Klicken Sie auf die Registerkarte **Administratoren** im unteren Bereich, um eine Liste der Administratoren anzuzeigen, die derzeit diese Rolle haben.
   - **Erstellen einer benutzerdefinierten Rolle**: Wählen Sie in der Aktionsleiste **Rolle erstellen**. Konfigurieren Sie die Einstellungen wie folgt:
     - Geben Sie einen Namen und eine Beschreibung ein.
     - Konfigurieren Sie den Konsolenzugriff. Legen Sie fest, welche Konsolen für die Administratoren sichtbar sein sollen. Sie können fortfahren, ohne eine Konsole auszuwählen. In diesem Fall können Administratoren mit der Rolle nicht auf **Verwalten** und **Überwachen** zugreifen, doch sie können über SDKs und APIs auf Objekte zugreifen, diese anzeigen und verwalten.
     - Wählen Sie die Objekttypen und Berechtigungen aus. Um Vollzugriff auf einen Objekttyp zu gewähren, aktivieren Sie das zugehörige Kontrollkästchen. Um Berechtigungen granular zu gewähren, erweitern Sie den Objekttyp und wählen **Schreibgeschützt** oder einzelne Objekte unter **Verwalten** innerhalb des Typs aus.




- **Kopieren einer Rolle:** Wählen Sie die Rolle im mittleren Bereich aus und wählen Sie in der Aktionsleiste **Rolle kopieren**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf. Wenn Sie fertig sind, wählen Sie **Speichern**.

- **Bearbeiten einer Rolle:** Wählen Sie die Rolle im mittleren Bereich aus und wählen Sie in der Aktionsleiste **Rolle bearbeiten**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf. Sie können eine integrierte Rolle nicht bearbeiten. Wenn Sie fertig sind, wählen Sie **Speichern**.
- **Löschen einer Rolle:** Wählen Sie die Rolle im mittleren Bereich aus und wählen Sie in der Aktionsleiste **Rolle löschen**. Bestätigen Sie die Löschung. Sie können eine integrierte Rolle nicht löschen. Sie können eine benutzerdefinierte Rolle nicht löschen, wenn sie einem Administrator zugewiesen ist.

### Erstellen und Verwalten von Geltungsbereichen

Standardmäßig verwenden alle Rollen den Geltungsbereich Alle für ihre relevanten Objekte. Beispielsweise kann ein Bereitstellungsgruppenadministrator alle Bereitstellungsgruppen verwalten. Für einige Administratorrollen können Sie einen Geltungsbereich erstellen, der dieser Administratorrolle den Zugriff auf einen Teil der relevanten Objekte ermöglicht. Vielleicht möchten Sie einem Maschinenkatalogadministrator nur Zugriff auf die Kataloge gewähren, die einen bestimmten Maschinentyp enthalten.

- Administratoren mit Vollzugriff oder Cloudadministratoren mit benutzerdefiniertem Zugriff können Geltungsbereiche für die Rollen "Lesezugriffadministrator", "Maschinenkatalogadministrator", "Bereitstellungsgruppenadministrator"und "Hostadministrator"erstellen.
- Geltungsbereiche können nicht für Administratoren mit Vollzugriff, Cloudadministratoren oder Helpdeskadministratoren erstellt werden. Diesen Administratoren ist stets der Geltungsbereich "Alle"zugeordnet.

Regeln zum Erstellen und Verwalten von Geltungsbereichen:

- Geltungsbereichsnamen können bis zu 64 Unicode-Zeichen enthalten. Namen dürfen keines der folgenden Zeichen enthalten: umgekehrter Schrägstrich, Schrägstrich, Semikolon, Doppelpunkt, Nummernzeichen, Komma, Sternchen, Fragezeichen, Gleichheitszeichen, Größer-Als- oder Kleiner-Als-Zeichen, senkrechter Strich, eckige Klammern, runde Klammern, Anführungszeichen und Apostroph.
- Geltungsbereichsbeschreibungen können bis zu 256 Unicode-Zeichen enthalten.
- Wenn Sie einen Geltungsbereich kopieren oder bearbeiten, dürfen Sie nicht vergessen, dass Objekte, die aus dem Geltungsbereich entfernt werden, für einen Administrator ggf. nicht mehr zugänglich sind. Ist der bearbeitete Geltungsbereich mit einer oder mehreren Rollen verbunden, müssen Sie sicherstellen, dass kein Rollen-/Geltungsbereichspaar durch Änderungen am Bereich unbrauchbar wird.

Erstellen und Verwalten von Geltungsbereichen:

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie **Eigene Services > DaaS** im Menü links oben.

2. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Administratoren**.
3. Wählen Sie die Registerkarte **Geltungsbereiche**.
4. Folgen Sie den Anweisungen für die Aufgabe, die Sie ausführen möchten:

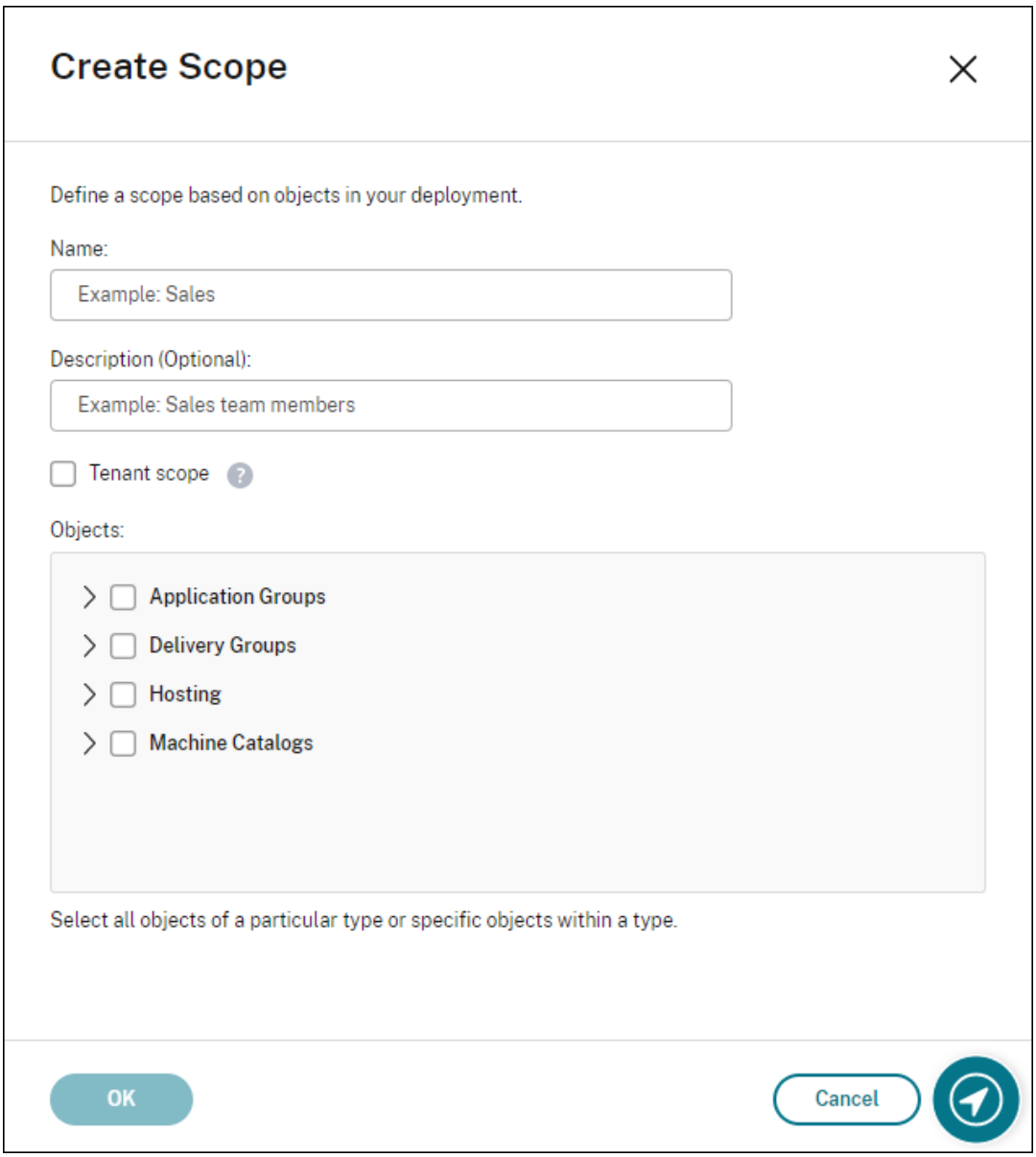
   - **Bereichsdetails anzeigen:** Wählen Sie den Bereich. Im unteren Fensterbereich werden die Objekte und Administratoren mit dem Bereich angezeigt.
   - **Geltungsbereich erstellen:** Wählen Sie in der Aktionsleiste **Geltungsbereich erstellen**. Geben Sie einen Namen und eine Beschreibung ein. Die Objekte sind nach Typ aufgelistet, z. B. Bereitstellungsgruppe und Maschinenkatalog.
     - Zum Einschließen aller Objekte eines bestimmten Typs (z. B. alle Bereitstellungsgruppen) aktivieren Sie das Kontrollkästchen für den Objekttyp.
     - Zum Einschließen einzelner Objekte eines Typs erweitern Sie den Typ und aktivieren die Kontrollkästchen für die Objekte (z. B. bestimmte Bereitstellungsgruppen).

       > **Hinweis:**
       >
       > Anwendungsgruppen, Bereitstellungsgruppen oder Maschinenkataloge werden in Ordnerstrukturen angezeigt, die ihrer Verwaltung in DaaS entsprechen. Sie können einen Ordner auswählen, um alle darin enthaltenen Objekte auszuwählen, oder einen Ordner erweitern, um bestimmte Objekte auszuwählen.

     - Um einen Mandantenkunden zu erstellen, aktivieren Sie das Kontrollkästchen **Mandantenbereich**. Wenn ausgewählt, ist der Name, den Sie für den Geltungsbereich eingegeben haben, der Mandantenname. Weitere Informationen zum Mandantenbereich finden Sie unter Mandantenverwaltung.

   Wenn Sie fertig sind, wählen Sie **OK**.




- **Geltungsbereich kopieren:** Wählen Sie den Geltungsbereich im mittleren Bereich aus und wählen Sie in der Aktionsleiste **Geltungsbereich kopieren**. Ändern Sie den Namen und die Beschreibung. Ändern Sie bei Bedarf die Objekttypen und Berechtigungen. Wenn Sie fertig sind, wählen Sie **Speichern**.
- **Geltungsbereich bearbeiten:** Wählen Sie den Geltungsbereich im mittleren Bereich aus und wählen Sie in der Aktionsleiste **Geltungsbereich kopieren**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Objekte nach Bedarf. Wenn Sie fertig sind, wählen Sie **Speichern**.
- **Geltungsbereich löschen:** Wählen Sie den Geltungsbereich im mittleren Bereich aus und wählen Sie in der Aktionsleiste **Geltungsbereich löschen**. Bestätigen Sie die Löschung.

> Sie können einen Geltungsbereich nicht löschen, wenn er einer Rolle zugewiesen ist. Wenn Sie dies versuchen, wird in einer Fehlermeldung angezeigt, dass Sie hierfür keine Berechtigung haben. Der Fehler tritt auf, weil das zugehörige Rollen-/Geltungsbereichspaar einem Administrator zugewiesen ist. Heben Sie zunächst die Rollen-/Geltungsbereichspaarzuweisung für alle Administratoren auf, die sie verwenden. Löschen Sie dann den Bereich in der Konsole **Verwalten**.

Nachdem Sie einen Bereich erstellt haben, wird er in der Citrix Cloud-Konsole in der Liste **Benutzerdefinierter Zugriff** angezeigt. Sie können ihn dann auswählen, wenn Sie einem Administrator eine Rolle zuweisen.

Angenommen, Sie erstellen den Bereich CAD und wählen dann die Kataloge aus, die für CAD-Anwendungen geeignete Maschinen enthalten. Wenn Sie zur Citrix Cloud-Konsole zurückkehren und **Bereiche bearbeiten** für eine Rolle auswählen, wird in der Liste der verfügbaren Bereiche der zuvor erstellte CAD-Bereich angezeigt.

Cloudadministrator und Helpdeskadministrator haben stets den Bereich "Alle", sodass der CAD-Bereich für sie nicht gilt.

#### Mandantenverwaltung

Mit der Schnittstelle "Vollständige Konfiguration"können Sie einander ausschließende Mandanten in einem Citrix DaaS erstellen. Hierfür erstellen Sie unter **Administratoren > Geltungsbereiche** einzelne Mandantenbereiche, denen Sie dann zugehörige Konfigurationsobjekte (z. B. Maschinenkataloge und Bereitstellungsgruppen) zuordnen. Administratoren mit Zugriff auf einen Mandanten können damit nur die Objekte verwalten, die mit dem Mandanten verknüpft sind.

Das Feature ist in folgenden Fällen besonders nützlich:

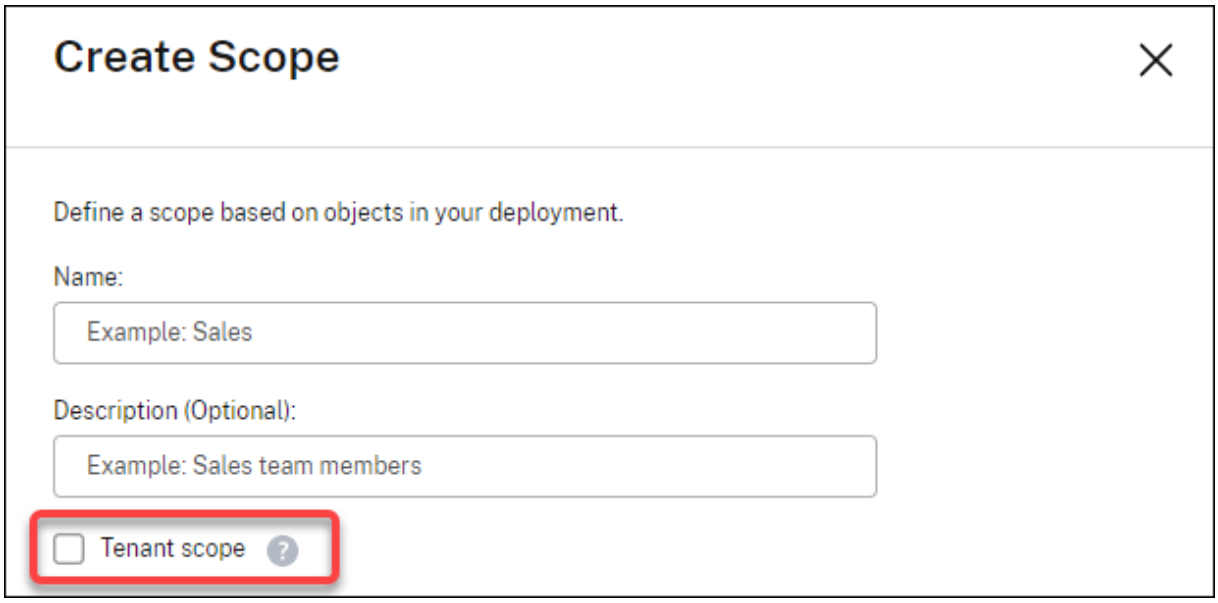
- Ihre Organisation besitzt mehrere Geschäftssilos (unabhängige Abteilungen oder separate IT-Teams) oder
- Ihre Organisation betreibt mehrere On-Premises-Sites und möchte dasselbe Setup in einer einzigen Citrix DaaS-Instanz beibehalten.

Sie können Mandantenkunden auch nach Namen filtern. Standardmäßig werden hier Informationen zu allen Mandantenkunden angezeigt. Um Informationen zu einem bestimmten Mandanten anzuzeigen, wählen Sie ihn in der Liste in der oberen rechten Ecke aus.

**Erstellen eines Mandantenkunden** Um einen Mandantenkunden zu erstellen, aktivieren Sie beim Erstellen eines Geltungsbereichs die Option **Mandantenbereich**. Durch Aktivieren dieser Option erstellen Sie einen eindeutigen Bereichstyp, der für Objekte in Szenarios gilt, wo verschiedene Geschäftseinheiten dieselbe Citrix DaaS-Instanz nutzen und jede Geschäftseinheit unabhängig von den an-

deren ist. Nachdem Sie einen Mandantenbereich erstellt haben, können Sie den Bereichstyp nicht mehr ändern.




Auf der Registerkarte **Geltungsbereiche** sind alle Bereichselemente angezeigt. Der einzige Unterschied zwischen Standardbereichen und Mandantenbereichen besteht in der Spalte **Typ**. Ein leeres Spaltenfeld verweist auf einen Standardbereich. Durch Klicken auf die Spalte **Typ** können Sie Bereichselemente bei Bedarf auch sortieren.

Um die Ressourcen (Objekte) anzuzeigen, die einem Bereich zugeordnet sind, wählen Sie im linken Bereich die Option **Administratoren**. Wählen Sie den Geltungsbereich auf der Registerkarte **Geltungsbereiche** und wählen Sie in der Aktionsleiste **Geltungsbereich bearbeiten**.

> **Tipp:**
>
> Die Mandanteneigenschaft wird auf einer Bereichsebene zugewiesen. Maschinenkataloge, Bereitstellungsgruppen, Anwendungen und Verbindungen erben die Mandanteneigenschaft vom entsprechenden Geltungsbereich.

Beachten Sie bei der Verwendung eines Mandantenbereichs Folgendes:

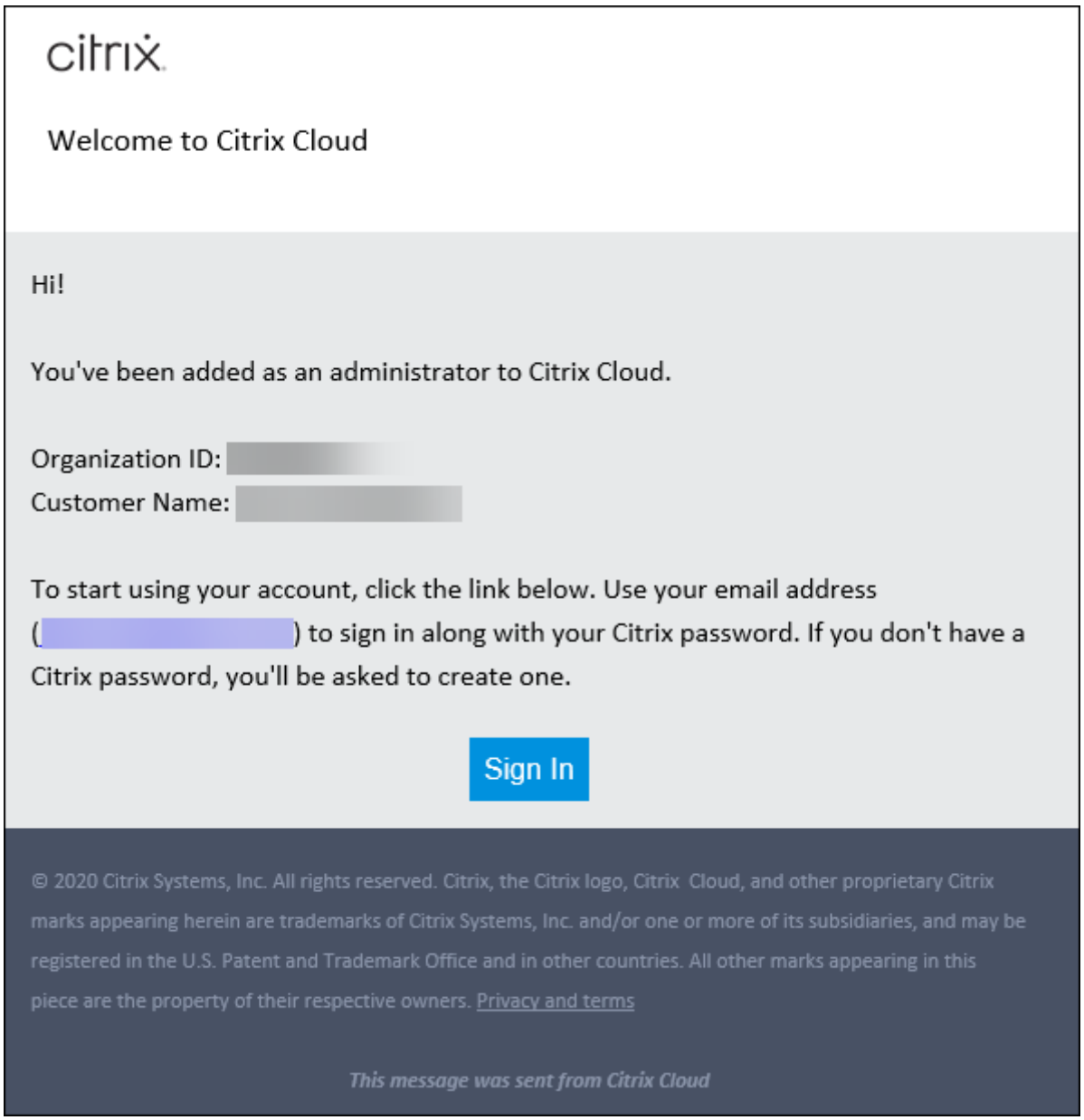
- Die Mandanteneigenschaft wird in der folgenden Reihenfolge zugewiesen: **Hosting > Maschinenkataloge > Bereitstellungsgruppen > Anwendungen**. Untergeordnete Objekte müssen die Mandanteneigenschaft des übergeordneten Objekts übernehmen. Beim Auswählen einer Bereitstellungsgruppe müssen Sie beispielsweise den zugehörigen Hosting- und Maschinenkatalog auswählen. Andernfalls kann die Bereitstellungsgruppe die Mandanteneigenschaft nicht erben.
- Nach dem Erstellen eines Mandantenbereichs können Sie Mandantenzuweisungen bearbeiten, indem Sie Objekte ändern. Eine geänderte Mandantenzuweisung unterliegt weiterhin der Einschränkung, dass sie denselben Mandanten oder einem Teil dieser Mandanten zugewiesen sein

muss. Untergeordnete Objekte werden jedoch nicht neu evaluiert, wenn Mandantenzuweisungen sich ändern. Stellen Sie sicher, dass für Objekte ordnungsgemäße Einschränkungen gelten, wenn Sie Mandantenzuweisungen ändern. Wenn beispielsweise ein Maschinenkatalog für `TenantA` und `TenantB` verfügbar ist, können Sie je eine Bereitstellungsgruppe für `TenantA` und `TenantB` erstellen. (`TenantA` und `TenantB` sind beide mit diesem Maschinenkatalog verknüpft.) Sie können dann den Maschinenkatalog so ändern, dass er nur `TenantA` zugeordnet ist. Infolgedessen wird die `TenantB` zugeordnete Bereitstellungsgruppe ungültig.

**Konfigurieren von benutzerdefiniertem Zugriff für Administratoren** Nach dem Erstellen von Mandantenbereichen konfigurieren Sie den benutzerdefinierten Zugriff für die jeweiligen Administratoren. Weitere Informationen finden Sie unter Konfigurieren von benutzerdefiniertem Zugriff für einen Administrator. Citrix Cloud sendet eine Einladung an die von Ihnen festgelegten Kundenadministratoren und fügt sie der Liste hinzu. Beim Erhalt der E-Mail klicken sie auf **Anmelden**, um die Einladung anzunehmen. Wenn sie sich an der Verwaltungsoberfläche **Vollständige Konfiguration** anmelden, sehen sie die Ressourcen in den zugewiesenen Rollen-/Geltungsbereichspaaren.




Administratoren mit Zugriff auf einen Mandanten können nur die Objekte (z. B. Maschinenkatalog, Bereitstellungsgruppe) verwalten, die mit dem Mandanten verknüpft sind.

### Konfigurieren von benutzerdefiniertem Zugriff für einen Administrator

Mit dieser Funktion können Sie die Zugriffsberechtigungen vorhandener oder eingeladener Administratoren an ihre Rolle in der Organisation angleichen.

Änderungen an Zugriffsberechtigungen benötigen 5 Minuten, bis sie in Kraft treten. Wenn Sie sich von der Verwaltungsoberfläche “Vollständige Konfiguration”ab- und wieder anmelden, werden die Änderungen sofort wirksam. Wenn Administratoren die Verwaltungsoberfläche weiterverwenden, nach-

dem die Änderungen wirksam geworden sind, ohne sich wieder mit ihr zu verbinden, wird eine Warnung angezeigt, wenn sie versuchen, auf Elemente zuzugreifen, für die sie keine Berechtigungen mehr haben.

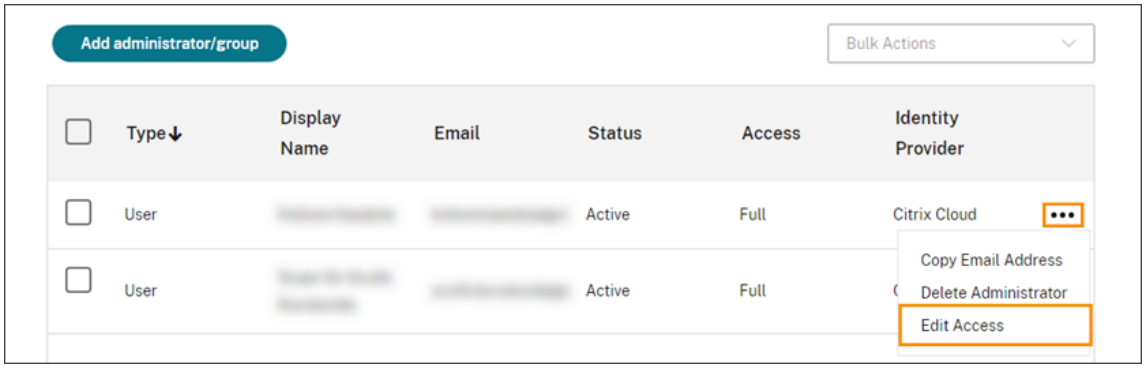
Wenn Sie Administratoren einladen, haben diese standardmäßig Vollzugriff. Administratoren mit Vollzugriff können alle abonnierten Dienste sowie alle Vorgänge in Citrix Cloud (z. B. weitere Administratoren einladen) verwalten. Eine Citrix Cloud-Bereitstellung benötigt mindestens einen Administrator mit Vollzugriff.

Sie können auch benutzerdefinierten Zugriff gewähren, wenn Sie einen Administrator einladen. Durch den benutzerdefinierten Zugriff kann der Administrator nur die Dienste und Operationen verwalten, die Sie angeben.

Wenn Sie eine Rolle oder einen Geltungsbereich in Citrix DaaS erstellt haben, werden sie in der Liste "Benutzerdefinierter Zugriff"angezeigt und können ausgewählt werden. Wenn Sie eine Rolle für einen Administrator auswählen, können Sie die Bereiche an die Rolle des Administrators in Ihrer Organisation anpassen.

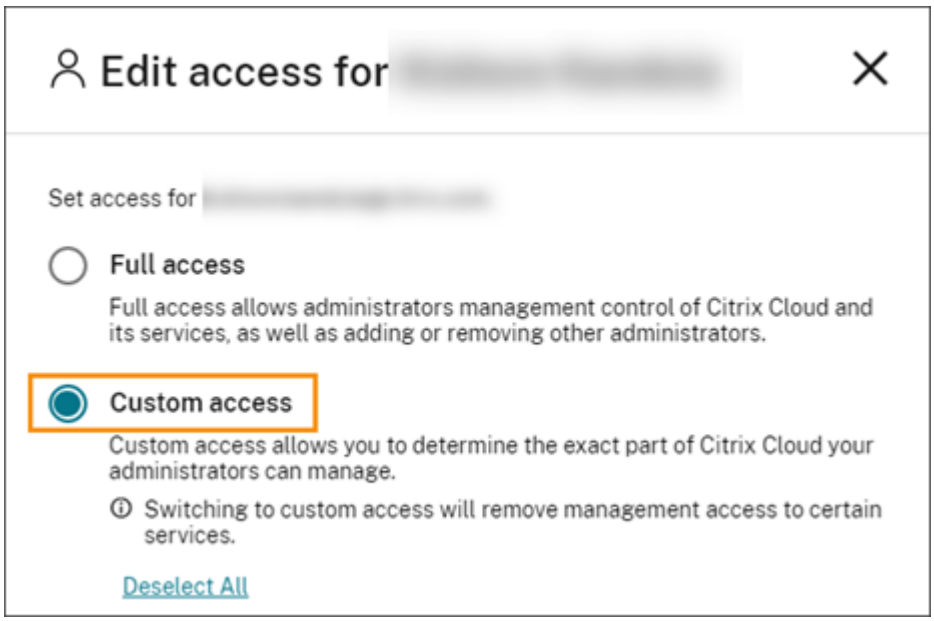
Konfigurieren des benutzerdefinierten Zugriffs für einen Administrator:

1. Melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü links oben **Identitäts- und Zugriffsverwaltung** > **Administratoren**.
2. Suchen Sie den gewünschten Administrator, wählen Sie die drei Punkte (…) und dann **Zugriff bearbeiten**.



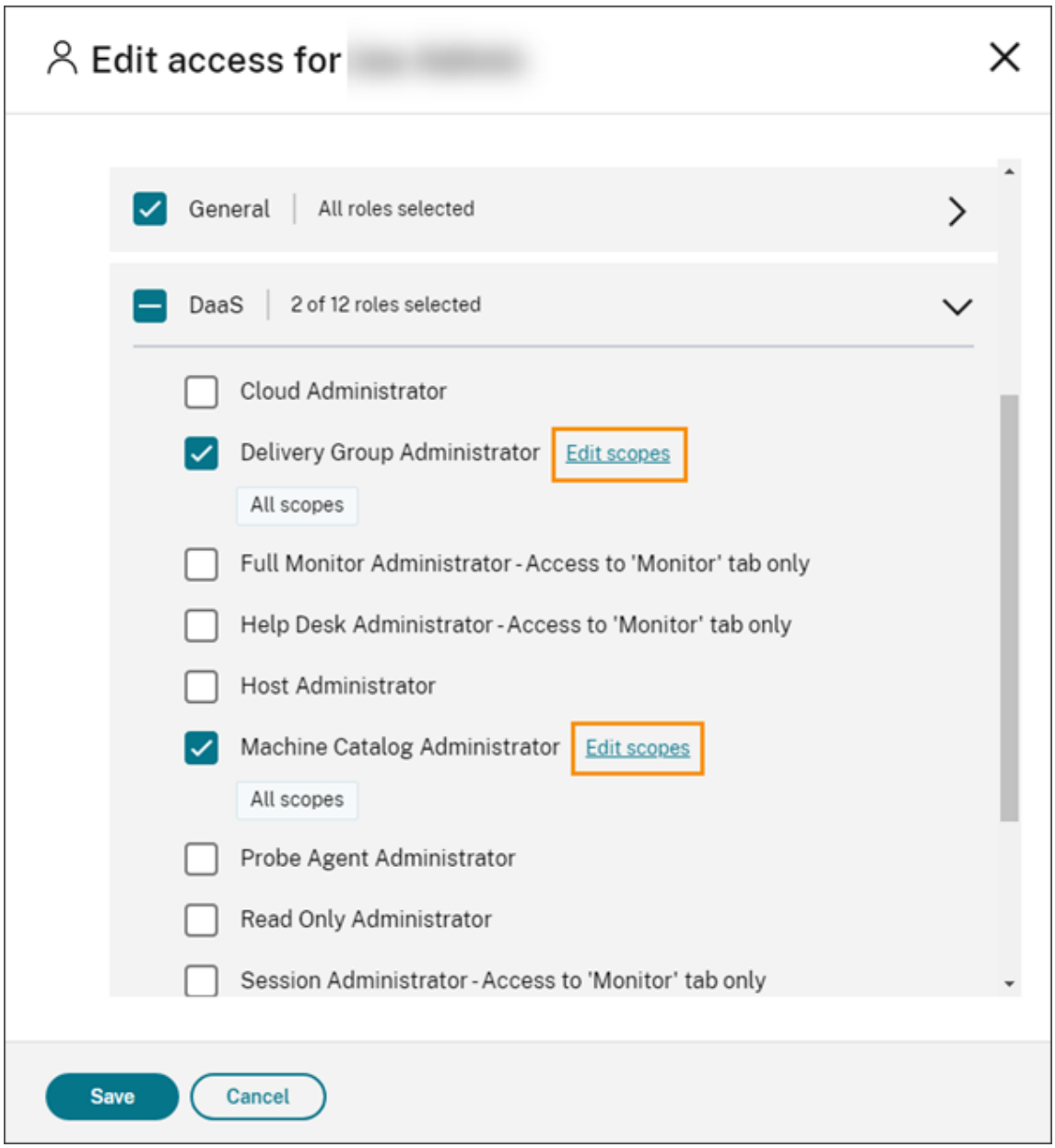

3. Wählen Sie **Benutzerdefinierter Zugriff**.




4. Aktivieren oder deaktivieren Sie unter **DaaS** die Häkchen neben einer oder mehreren Rollen. Um die einer zugewiesenen Rolle zugeordneten Bereiche zu ändern, wählen Sie **Bereiche bearbeiten**.

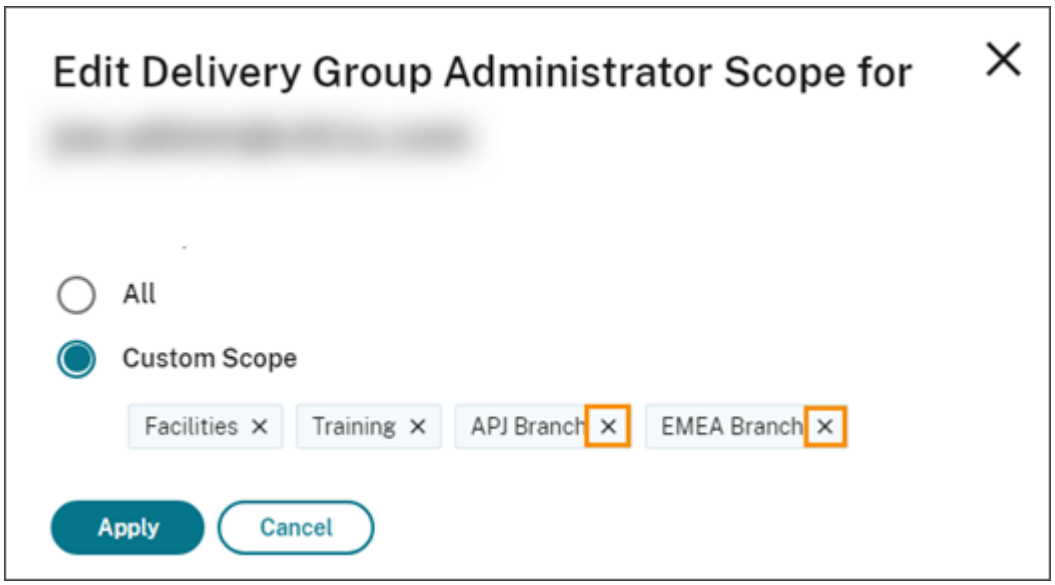
 



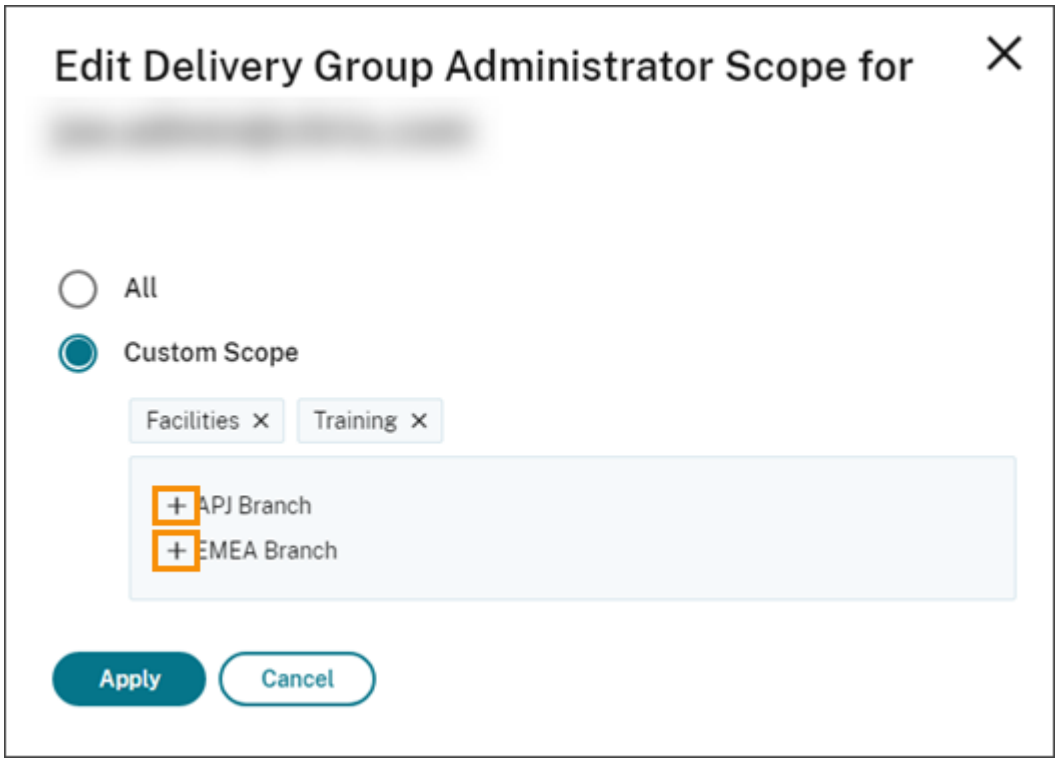

Standardmäßig sind für jede ausgewählte Rolle alle Bereiche ausgewählt (zu sehen an der Angabe **Alle Bereiche**).

5. Um die Bereiche für eine ausgewählte Rolle anzugeben, wählen Sie **Benutzerdefinierter Geltungsbereich** und fügen Sie dann Bereiche nach Bedarf hinzu bzw. entfernen Sie sie. Standardmäßig werden alle benutzerdefinierten Bereiche zu einer Rolle hinzugefügt. Um einen Bereich zu entfernen, klicken Sie auf das zugehörige X-Symbol.




Entfernte Bereiche, die zur Rolle hinzugefügt werden können, werden in einer Liste unterhalb der bereits hinzugefügten Bereiche angezeigt. Um der Rolle einen Bereich hinzuzufügen, wählen Sie das Plussymbol für den Bereich.




6. Wenn Sie mit der Auswahl der Bereiche fertig sind, wählen Sie **Anwenden**.
7. Wählen Sie **Speichern**, um die ausgewählten Rollen für den Administrator zu speichern.

### Unterschiede zur On-Premises-Version von Citrix Virtual Apps and Desktops

Citrix DaaS weist einige Unterschiede zur delegierten Administration im On-Premises-Produkt von Citrix Virtual Apps and Desktops auf.

In Citrix Cloud:

- Administratoren werden mit Citrix Cloud-Anmeldeinformationen und nicht über das Active Directory-Konto identifiziert. Sie können Rollen-/Geltungsbereichspaare für einzelne Active Directory-Benutzer, aber nicht für Gruppen erstellen.
- Administratoren werden nicht in Citrix DaaS, sondern in der Citrix Cloud-Konsole erstellt, konfiguriert und gelöscht.
- Rollen-/Geltungsbereichspaare werden Administratoren nicht in Citrix DaaS, sondern in der Citrix Cloud-Konsole zugewiesen.
- Berichte sind nicht verfügbar. Sie können Administrator-, Rollen- und Bereichsinformationen in der Oberfläche **Verwalten > Vollständige Konfiguration** des Diensts anzeigen.
- Der Cloudadministrator mit benutzerdefiniertem Zugriff ähnelt einem Volladministrator in der On-Premises-Version. Beide verfügen über vollständige Verwaltungs- und Überwachungsberechtigungen für die verwendete Version von Citrix Virtual Apps and Desktops.

  Es gibt jedoch keine Rolle “Volladministrator”in Citrix DaaS. “Vollzugriff”in Citrix Cloud und “Volladministrator”in der On-Premises-Version von Citrix Virtual Apps and Desktops sind nicht identisch. Vollzugriff in Citrix Cloud umfasst Domänen, Bibliothek, Benachrichtigungen und Ressourcenstandorte auf Plattformebene und alle abonnierten Dienste.

### Unterschiede zu früheren Citrix DaaS-Releases

Vor dem Release des erweiterten benutzerdefinierten Zugriffs (September 2018) gab es im Service zwei Administratorrollen mit benutzerdefiniertem Zugriff: Volladministrator und Helpdeskadministrator. Wenn die delegierte Administration in Ihrer Bereitstellung (ein Plattformeinstellung) aktiviert ist, werden diese Rollen automatisch zugeordnet.

- Administratoren mit konfiguriertem benutzerdefiniertem Zugriff im Service **Virtual Apps and Desktops (oder XenApp und XenDesktop): Volladministrator** ist jetzt **Cloudadministrator** mit benutzerdefiniertem Zugriff.
- Administratoren mit konfiguriertem benutzerdefiniertem Zugriff im Service **Virtual Apps and Desktops (oder XenApp und XenDesktop): Helpdeskadministrator** ist jetzt **Helpdeskadministrator** mit benutzerdefiniertem Zugriff.

### Weitere Informationen

Siehe Delegierte Administration und Überwachung für weitere Informationen zu Administratoren, Rollen und Bereichen, die in der Konsole **Überwachen** verwendet werden.

## Homepage für die Oberfläche "Vollständige Konfiguration"

November 6, 2023

Bietet einen Überblick über Ihre Citrix DaaS-Bereitstellung und Workloads sowie Informationen, mit deren Hilfe Sie Ihr Abonnement optimal nutzen können. Die Seite besteht aus den folgenden Bereichen:

- Serviceübersicht
- Benachrichtigungen zum Dienststatus
- Empfehlungen
- Neue Features
- Preview-Features
- Erste Schritte

Gehen Sie folgendermaßen vor, um auf die Homepage zuzugreifen:

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie in der **DaaS**-Kachel auf **Verwalten**.
3. Wählen Sie **Verwalten > Vollständige Konfiguration** aus. Die Homepage wird angezeigt.

### Serviceübersicht

Bietet einen Überblick über Ihre Citrix DaaS-Bereitstellung und Ihre Workloads:

- **Ressourcen**. Zeigt die Anzahl der bereitgestellten Ressourcen und deren Anzahl nach Kategorie an.

| Ressource | Anzahl nach Kategorie anzeigen |
| --- | --- |
| Maschinen | Klicken Sie auf **Maschinen**, wählen Sie einen Status aus, und bewegen Sie den Mauszeiger über das Ringdiagramm, um weitere Informationen zu erhalten. Verfügbare Optionen: **Verfügbarkeitsstatus** (Verfügbar, verwendet, aus oder nicht verfügbar), **Registrierungsstatus** (Registriert oder nicht registriert) und **Wartungsstatus** (Im Wartungsmodus oder nicht im Wartungsmodus). Wenn Sie die Anzahl Maschinen nach Verfügbarkeitsstatus anzeigen, können Sie auf einen Status klicken, um die entsprechenden Maschinendetails anzuzeigen. |
| Anwendungen | Klicken Sie auf **Anwendungen** und bewegen Sie den Mauszeiger über das Ringdiagramm, um Details zu erhalten. |
| Bereitstellungsgruppen | Klicken Sie auf **Bereitstellungsgruppen** und bewegen Sie den Mauszeiger über das Ringdiagramm, um Details zu erhalten. |
| Maschinenkataloge | Klicken Sie auf **Maschinenkataloge** und bewegen Sie den Mauszeiger über das Ringdiagramm, um Details zu erhalten. |

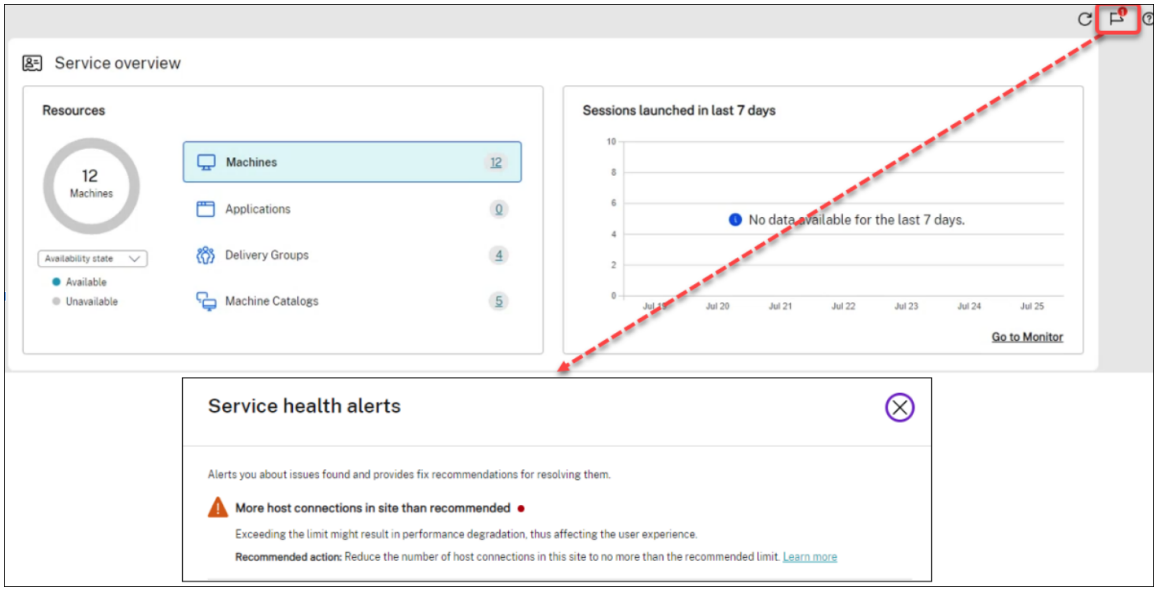
- **In den letzten 7 Tagen gestartete Sitzungen**. Zeigt die Anzahl der in den letzten sieben Tagen täglich gestarteten Desktop- und App-Sitzungen an. Für einen Drilldown zu weiteren Details klicken Sie auf **Zu Überwachen gehen**.

### Benachrichtigungen zum Dienststatus

Benachrichtigt Sie über gefundene Probleme und gibt Empfehlungen zur Problembehandlung. Benachrichtigungen werden mit Warn- und Fehlersymbolen angezeigt.

> **Hinweis:**
>
> Die Diagnosen werden stündlich aktualisiert.
>
> Beispiel für Benachrichtigung:




## Empfehlungen

Empfiehlt Features, die für Ihr Abonnement verfügbar sind, etwa Workspace Environment Management und Autoscale. Sie können mit uns in Kontakt aufnehmen, eine Empfehlung liken oder disliken und Ihr Feedback hinterlassen.

> **Hinweis:**
>
> Wenn Sie eine Empfehlung ablehnen, verschwindet die Empfehlung. Wenn Sie alle Empfehlungen oder das Empfehlungswidget ablehnen, verschwindet das Widget.

## Neue Features

Zeigt eine Auswahlliste der neuesten Citrix DaaS-Features, die für Ihr Unternehmen zutreffen. Verwenden Sie diese Features, um das Meiste aus Ihrem Abonnement zu machen. Eine vollständige Liste der neuen Features finden Sie unter Neue Features.

## Preview-Features

Zeigt Features an, die sich derzeit in der Preview befinden. Als Citrix Cloud-Administrator mit Vollzugriff können Sie Preview-Features ein- oder ausschalten, ohne Citrix zu kontaktieren. Es dauert bis zu 15 Minuten, bis die Änderungen wirksam werden.

Als Preview verfügbare Features werden für die Verwendung in Nicht-Produktionsumgebungen empfohlen. Probleme mit Preview-Features werden vom technischen Support von Citrix nicht unterstützt.

### Erste Schritte

Zeigt Schritte zur ersten Einrichtung von Apps und Desktops an.

Die Einrichtungsschritte sind wie folgt:

1. Ressourcenstandort erstellen

   Ressourcenstandorte sind Orte, die Anwendungen und Desktops enthalten, die Sie Ihren Benutzern bereitstellen möchten. In diesem Schritt können Sie Ihre Ressourcenstandorte DaaS hinzufügen und Cloud Connectors darin installieren. Cloud Connectors dienen als Kanäle, die die gesamte Kommunikation zwischen Citrix Cloud und Ihren Ressourcen authentifizieren und verschlüsseln.

2. Hostverbindung erstellen

   Hosts sind Hypervisors oder Cloudservices, die an Ihren Ressourcenstandorten verwendet werden. In diesem Schritt können Sie Informationen angeben, die DaaS für die Kommunikation mit VMs auf einem Host verwendet. Zu den detaillierten Informationen gehören der Ressourcenstandort, der Hosttyp, die Anmeldeinformationen für den Zugriff, die zu verwendende Speichermethode und die Netzwerke, die die VMs auf dem Host verwenden können.

3. Vorbereiten eines Masterimages

   Ein Masterimage enthält das Betriebssystem, alle erforderlichen Anwendungen und den Virtual Delivery Agent (VDA). VDAs stellen Verbindungen zwischen VMs und Benutzergeräten her und verwalten sie.

4. Maschinenkatalog erstellen

   Ein Maschinenkatalog ist eine Sammlung identischer VMs für Einzelsitzungs- oder Multisitzungs-OS, die Sie Benutzern zuweisen. In diesem Schritt können Sie einen Maschinenkatalog erstellen, indem Sie die Bereitstellungstechnologie, das Masterimage und die VM-Größe angeben.

5. Benutzer zuweisen

   Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. In diesem Schritt können Sie Bereitstellungsgruppen erstellen, um festzulegen, welche Teams, Abteilungen oder Benutzertypen welche Maschinen verwenden können.

6. Workspace konfigurieren

   Teilen Sie die Workspace-URL unter **Workspace-Konfiguration > Zugriff** mit den Benutzern.

## Lizenzen

April 19, 2022

In diesem Artikel werden Aufgaben und Ressourcen rund um Microsoft- und Citrix Lizenzen behandelt.

## Konfigurieren eines Microsoft RDS-Lizenzservers für Windows Server-Workloads

Diese Informationen gelten für die Bereitstellung von Windows Server-Workloads.

Dieser Dienst greift bei der Bereitstellung einer Windows Server-Workload (z. B. Windows 2019) auf Windows Server-Remotesitzungsfunktionen zu. Dies erfordert in der Regel eine Clientzugriffslizenz für Remotedesktopdienste (RDS CAL). Der VDA muss in der Lage sein, RDS-CALs von einem RDS-Lizenzserver anzufordern.

Installieren und aktivieren Sie den Lizenzserver. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Aktivieren des Remotedesktopdienste-Lizenzservers. Für Machbarkeitsstudien können Sie den von Microsoft bereitgestellten Kulanzzeitraum verwenden.

Mit dieser Methode können Sie die Lizenzservereinstellungen mithilfe dieses Service anwenden. Sie können den Lizenzserver und den "Pro-Benutzer"-Lizenzmodus in der RDS-Konsole auf dem Image konfigurieren. Sie können den Lizenzserver auch über die Microsoft-Gruppenrichtlinieneinstellungen konfigurieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter License your RDS deployment with client access licenses (CALs).

Konfigurieren des RDS-Lizenzservers über die Microsoft-Gruppenrichtlinieneinstellungen:

1. Installieren Sie einen Lizenzserver für die Remotedesktopdienste auf einer verfügbaren VM. Diese VM muss immer verfügbar sein. Die Citrix Serviceworkloads müssen auf diesen Lizenzserver zugreifen können.
2. Geben Sie über die Microsoft-Gruppenrichtlinie die Lizenzserveradresse ein und legen Sie den "Pro-Benutzer"-Lizenzmodus fest. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Best practices for setting up RDS licensing across Active Directory domains/forests or work groups.

Windows 10-Workloads erfordern eine Windows 10-Lizenzaktivierung. Wir empfehlen, dass Sie zum Aktivieren von Windows 10-Workloads die Microsoft-Dokumentation befolgen.

## Citrix Lizenznutzung

Informationen zur Citrix-Lizenznutzung finden Sie unter:

- Überwachen von Lizenzen und aktiver Nutzung für Cloud Services
- Überwachen von Lizenzen und aktiver Nutzung für Citrix DaaS

# Multityplizenzierung

August 18, 2023

Die Multityplizenzierung unterstützt den Verbrauch verschiedenartiger Lizenzansprüche in derselben Bereitstellung von Citrix DaaS (früher Citrix Virtual Apps and Desktops Service). Dieser Artikel gilt für Sie, wenn Sie mehr als einen Citrix Lizenzanspruch haben. Ein Citrix-Anspruch ist eine Kombination aus Folgendem:

- Produkt, im aktuellen Kontext von DaaS immer Citrix DaaS
- Service Edition (zum Beispiel: Advanced, Advanced Plus, Premium oder Premium Plus)
- Lizenzmodell (zum Beispiel: Benutzer/Gerät oder Concurrent)

## Regeln für das Kombinieren von Ansprüchen

Die Regeln für das Kombinieren von Serviceeditionen sind:

- Nur die Kombination von DaaS Advanced und Advanced Plus ist erlaubt
- Nur die Kombination von DaaS Premium und Premium Plus ist erlaubt
- DaaS Standard kann nicht mit anderen Editionen kombiniert werden

Sie können die Lizenzmodelle kombinieren, wenn die oben genannten Service Edition-Regeln befolgt werden.

## Anspruch auf der Ebene von Site und Bereitstellungsgruppe

Sie können Lizenzansprüche auf den folgenden beiden Ebenen konfigurieren und verwenden:

- Site (Ihre Bereitstellung des Citrix DaaS-Produkts)
- Bereitstellungsgruppe

Wenn Sie noch keine Site- oder Bereitstellungsgruppenberechtigungen konfiguriert haben, berücksichtigen Sie folgende Standardvorgaben:

- Wenn Sie mehr als einen Anspruch haben, wird der leistungsfähigste der verfügbaren Ansprüche als siteweiter Anspruch ausgewählt, sofern die Ansprüche gleichzeitig bestellt wurden. Andernfalls wird der erste Anspruch zum siteweiten Standard, sofern er nicht später explizit geändert wird.
- Der Siteanspruch wird verwendet, wenn kein Bereitstellungsgruppenanspruch konfiguriert ist.

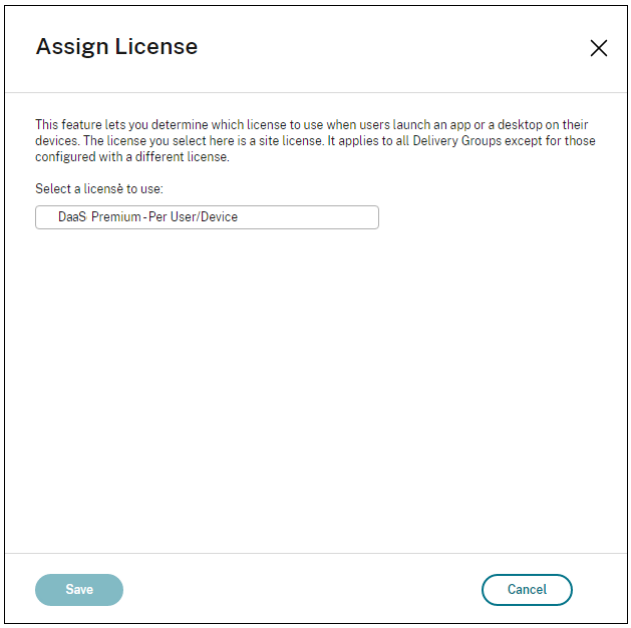
 

> **Hinweis:**
>
> Das Konfigurieren von Ansprüchen für eine Site oder Bereitstellungsgruppe wirkt sich auf die Berechnung des Lizenzverbrauchs in der Lizenzverbrauchsanzeige in Citrix Cloud aus.

### Anzeigen und Aktualisieren des Siteanspruchs

Um anzugeben, welcher Lizenzanspruch für die Site verwendet werden soll, gehen Sie zu **Vollständige Konfiguration > Einstellungen > Lizenz zuweisen** und klicken Sie auf **Bearbeiten**. Das Blatt **Lizenz zuweisen** wird angezeigt. Informationen zum Aufrufen der Seite **Vollständige Konfiguration** finden Sie in der Dokumentation zu Citrix DaaS.

Wählen Sie im Blatt **Lizenz zuweisen** die Lizenz aus, die die Site verwenden soll. Die ausgewählte Lizenz gilt für alle Bereitstellungsgruppen der Site, mit Ausnahme derer, für die eine eigene Lizenz konfiguriert wurde.




Folgende Lizenzen können von Ihnen ausgewählt werden:

- Citrix DaaS Premium —Pro Benutzer/Gerät
- Citrix DaaS Premium —Gleichzeitig
- Citrix DaaS Premium für Google Cloud —Pro Benutzer/Gerät
- Citrix DaaS Premium für Google Cloud —Gleichzeitig
- Citrix DaaS Advanced —Pro Benutzer/Gerät
- Citrix DaaS Advanced —Gleichzeitig
- Citrix DaaS Advanced Plus —Pro Benutzer/Gerät
- Citrix DaaS Advanced Plus —Gleichzeitig
- Citrix DaaS Standard für Azure - Pro Benutzer/Gerät

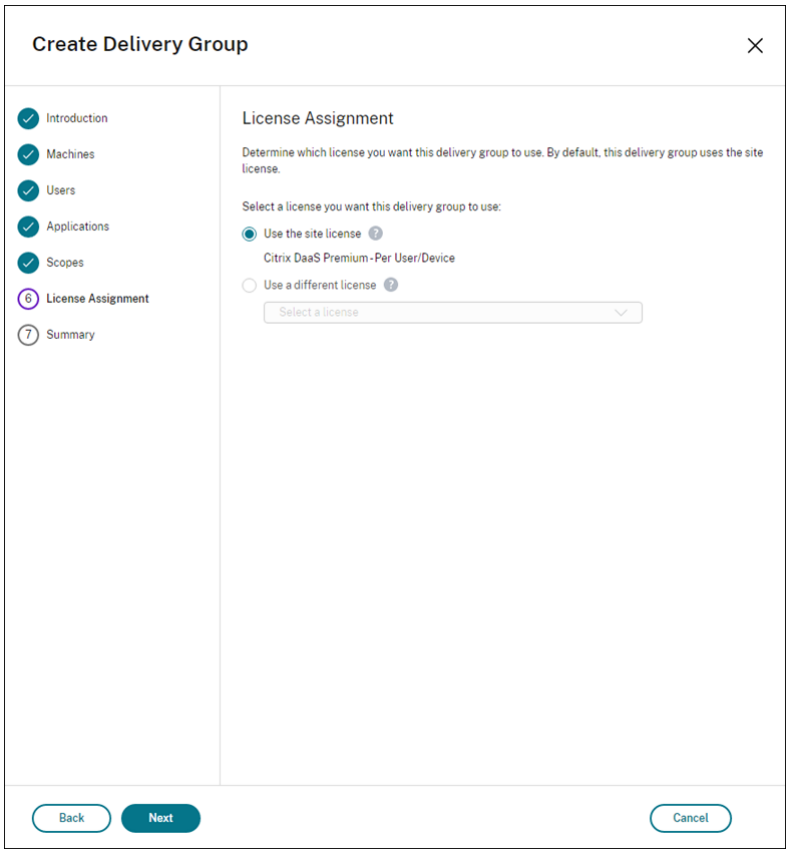
 

- Citrix DaaS Standard für Azure –Gleichzeitig
- Citrix DaaS Standard für Google Cloud —Pro Benutzer/Gerät
- Citrix DaaS Standard für Google Cloud —Gleichzeitig

Wenn Sie Ihre Lizenz abgelaufen ist, wenden Sie sich an Ihren Citrix Vertriebsmitarbeiter, um sie zu verlängern oder um neue Lizenzen zu erwerben.

### Anzeigen und Aktualisieren von Bereitstellungsgruppenberechtigungen

Sie können die Lizenz für eine Bereitstellungsgruppe beim Erstellen oder beim Bearbeiten der Bereitstellungsgruppe angeben. Wählen Sie auf der Seite **Lizenzzuweisung** eine Option aus.




Optionen:

- **Sitelizenz verwenden.** Eine Sitelizenz gilt für alle Bereitstellungsgruppen, mit Ausnahme derer, für die eine eigene Lizenz konfiguriert wurde. Bei der unter dieser Option angezeigten Lizenz handelt es sich um die verwendete Sitelizenz. Um die Standortlizenz zu konfigurieren, gehen Sie zu **Verwalten > Vollständige Konfiguration**, wählen Sie den Knoten **Einstellungen** und bearbeiten Sie **Lizenz zuweisen**.
- **Eine andere Lizenz verwenden.** Mit dieser Option können Sie für die Bereitstellungsgruppe eine andere Lizenz als die Sitelizenz konfigurieren. Ein Lizenzanspruch ist eine Kombination

aus Produktcode, Edition und Lizenz. Für die Bereitstellungsgruppe muss dieselbe Lizenzedition (Standard, Premium oder Advanced) wie für die Site verwendet werden. Ist eine Lizenz konfiguriert, verbraucht die Bereitstellungsgruppe nur die ausgewählte Lizenz. Die Bereitstellungsgruppe greift nicht auf die Sitelizenz zurück, selbst wenn die ausgewählte Lizenz vollständig verbraucht oder ungültig geworden ist.

Standardmäßig wird für die Bereitstellungsgruppe die Sitelizenz verwendet.

Wenn die Lizenz für eine Bereitstellungsgruppe abgelaufen ist, müssen Sie eine andere Lizenz verwenden.

> **Hinweis:**
>
> Wenn Sie später eine andere Lizenz für eine Bereitstellungsgruppe konfigurieren, verlieren Benutzer, die die aktuelle Lizenz nutzen, möglicherweise vorübergehend den Zugriff auf ihre Desktops und Anwendungen.

### Beispiel für das Kombinieren von Ansprüchen

Beispiel: Kunde A hat zunächst die Advanced Edition und später die Advanced Plus Edition gekauft. In diesem Fall hat Kunde A weiterhin nur eine siteweite Lizenz für Advanced Edition. Citrix ändert nicht die Einstellung, die ursprünglich vom Kunden A auf Siteebene festgelegt wurde. Es liegt in der Verantwortung von Kunde A, die Lizenzedition auf Siteebene in Advanced Plus zu ändern.

Ebenso kann Kunde A die Lizenzedition auch in der Bereitstellungsgruppe auf Advanced Plus aktualisieren. Wenn diese Einstellung nicht konfiguriert ist, erbt die Bereitstellungsgruppe die auf Siteebene festgelegte Lizenzedition.

Der Administrator von Kunde A kann die Lizenzversion auf folgende Weise aktualisieren:

- Lizenzversion auf Standortebene aktualisieren –gehen Sie zu **Verwalten > Vollständige Konfiguration**, wählen Sie den Knoten **Einstellungen** und bearbeiten Sie **Lizenz zuweisen**.
- Lizenzedition auf Bereitstellungsgruppenebene aktualisieren –Gehen Sie zu **Verwalten > Vollständige Konfiguration**und wählen Sie den Knoten **Bereitstellungsgruppen**. Bearbeiten Sie die Zielbereitstellungsgruppe, um Änderungen vorzunehmen.

#### Bereitstellungsgruppe mit PowerShell-Befehl aktualisieren

Der PowerShell-Befehl zum Aktualisieren der Bereitstellungsgruppe:

```
Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
    code> -LicenseModel <The type of license model>
<!--NeedCopy-->
```

Aktualisieren Sie den vorherigen Befehl basierend auf Ihren Informationen.

Betrachten Sie zum Beispiel Folgendes:

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null` (Legen Sie die Konfiguration der Bereitstellungsgruppenebene auf die Konfiguration der Siteebene fest)
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

Bedenken Sie, dass das Lizenzmodell und der Produktcode nicht auf Bereitstellungsgruppenebene festgelegt werden. In diesem Szenario werden die auf Siteebene festgelegten Eigenschaften für die Bereitstellungsgruppe verwendet.

Weitere Informationen zum Citrix DaaS Remote PowerShell SDK finden Sie in der SDKs- und API-Dokumentation.

### Weitere Informationen

- Lizenzen
- Bereitstellungsgruppen erstellen
- Bereitstellungsgruppen verwalten

## Lastausgleich bei Maschinen

December 1, 2023

> **Hinweis:**
>
> Diese Funktion gilt für alle Kataloge –also für Kataloge für Einzel- oder Multisitzungs-OS. Der vertikale Lastausgleich gilt nur für Maschinen mit Multisitzungs-OS.

Der Lastausgleich kann auf Siteebene und auf Bereitstellungsgruppenebene konfiguriert werden. Sie haben zwei Möglichkeiten: vertikal und horizontal. Standardmäßig ist der horizontale Lastausgleich aktiviert.

### Lastausgleichseinstellungen auf Siteebene

- **Vertikaler Lastausgleich:** Weist eine eingehende Benutzersitzung der Maschine zu, die am stärksten ausgelastet ist, jedoch die Maximallast noch nicht erreicht hat. Dadurch werden

vorhandene Maschinen vollständig genutzt, bevor zu neuen Maschinen gewechselt wird. Das Trennen der Verbindung von vorhandenen Maschinen durch Benutzer gibt Kapazität auf diesen Maschinen frei. Eingehende Lasten werden dann diesen Maschinen zugewiesen. Der vertikale Lastausgleich beeinträchtigt die Benutzererfahrung, senkt jedoch die Kosten (Sitzungen maximieren die Kapazität der eingeschalteten Maschinen).

Beispiel: Sie haben zwei Maschinen für jeweils zehn Sitzungen konfiguriert. Die erste Maschine verarbeitet die ersten zehn gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet die elfte Sitzung.

> **Tipp:**
>
> Um die maximale Anzahl von Sitzungen anzugeben, die von einer Maschine gehostet werden können, verwenden Sie die Richtlinieneinstellung Sitzungshöchstanzahl.

Alternativ können Sie den vertikalen Lastausgleich mit PowerShell für die gesamte Site aktivieren oder deaktivieren. Verwenden Sie die Einstellung `UseVerticalScalingForRdsLaunches` im Cmdlet `Set-BrokerSite`. Verwenden Sie `Get-BrokerSite`, um den Wert der Einstellung `UseVerticalScalingForRdsLaunches` anzuzeigen. Weitere Informationen finden Sie in der Cmdlet-Hilfe.

- **Horizontaler Lastausgleich:** Weist eine eingehende Benutzersitzung der am wenigsten ausgelasteten, eingeschalteten Maschine zu. Der horizontale Lastausgleich verbessert die Benutzererfahrung, erhöht jedoch die Kosten, da mehr Maschinen eingeschaltet bleiben. Standardmäßig ist der horizontale Lastausgleich aktiviert.

  Beispiel: Sie haben zwei Maschinen für jeweils zehn Sitzungen konfiguriert. Die erste Maschine verarbeitet die ersten fünf gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet ebenfalls fünf Sitzungen.

Um dieses Feature zu konfigurieren, wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Einstellungen**. Wählen Sie eine Option unter **Lastausgleich für Multisitzungskataloge**.

### Lastausgleicheinstellungen auf Bereitstellungsgruppenebene

Wenn Sie den Lastausgleich auf Bereitstellungsgruppenebene konfigurieren, können Sie die von der Siteebene übernommenen Lastausgleicheinstellungen außer Kraft setzen. Sie können die maximale Auslastung für jede Maschine erreichen, wenn Sie den vertikalen Lastausgleich auf Bereitstellungsgruppenebene auswählen. Dies trägt zur Senkung der Kosten in öffentlichen Clouds bei. Diese Konfiguration kann bei Erstellung einer neuen Bereitstellungsgruppe oder der Bearbeitung einer vorhandenen vorgenommen werden.

**Horizontaler Lastausgleich:** Die Sitzungen werden auf die eingeschalteten Maschinen verteilt. Wenn Sie beispielsweise zwei Maschinen für jeweils zehn Sitzungen konfiguriert haben, verarbeitet die erste Maschine fünf gleichzeitige Sitzungen und die zweite Maschine verarbeitet ebenfalls fünf.

**Vertikaler Lastausgleich:** Die Kapazität der eingeschalteten Maschinen werden maximiert, was Maschinenkosten spart. Wenn Sie beispielsweise zwei Maschinen für jeweils zehn Sitzungen konfiguriert haben, verarbeitet die erste Maschine die ersten zehn gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet die elfte Sitzung.

## Lokaler Hostcache

June 12, 2024

> **Tipp:**
>
> In **Vollständige Konfiguration > Homepage** werden Sie durch "Benachrichtigungen zum Dienststatus"proaktiv informiert, ob Ihr lokaler Hostcache und die Zonen korrekt konfiguriert sind. Dies gewährleistet, dass der lokale Hostcache bei einem Ausfall funktioniert und Ihre Benutzer nicht davon betroffen sind. Es gibt zwei Arten von Benachrichtigungen: Siteübergreifende Benachrichtigungen werden auf der Homepage angezeigt (Flaggensymbol). Zonenbezogene Benachrichtigungen werden auf der Registerkarte "Problembehandlung"jeder Zone angezeigt. Weitere Informationen finden Sie unter Zonen.

Der lokale Hostcache (LHC) ermöglicht das fortgesetzte Verbindungsbrokering in einer Bereitstellung von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service), wenn ein Cloud Connector nicht mit Citrix Cloud kommunizieren kann. Der lokale Hostcache wird aktiv, wenn die Netzwerkverbindung für 60 Sekunden unterbrochen wird.

Über den lokalen Hostcache können verbundene Benutzer bei einem Ausfall ohne Unterbrechung weiterarbeiten. Bei Wiederverbindungen und neuen Verbindungen treten minimale Verbindungsverzögerungen auf.

> **Wichtig:**
>
> Wenn Sie eine On-Premises-StoreFront-Bereitstellung verwenden, müssen Sie alle Cloud Connectors, bei denen VDAs registriert sind (oder sein können), zu StoreFront als Delivery Controller hinzufügen. Ein Cloud Connector, der nicht zu StoreFront hinzugefügt wird, kann nicht in den Ausfallmodus wechseln, was zu Startfehlern für Benutzer führen kann.
>
> Verwenden Sie für Bereitstellungen ohne on-premises StoreFront das Servicekontinuität-Feature

> der Citrix Workspace-Plattform, um Benutzern auch bei Ausfällen den Zugriff auf Ressourcen zu ermöglichen. Weitere Informationen finden Sie unter Servicekontinuität.

### Dateninhalt

Der lokale Hostcache enthält folgende Informationen (die eine Teilmenge der Informationen in der Hauptdatenbank sind):

- Identität der Benutzer und Gruppen, denen Rechte für die in der Site veröffentlichte Ressourcen zugewiesen wurden.
- Identität der Benutzer, die Ressourcen der Site gerade verwenden oder kürzlich verwendet haben.
- Identität von VDA-Maschinen (einschließlich Remote-PC-Zugriffsmaschinen), die in der Site konfiguriert sind.
- Identität (Name und IP-Adresse) von Citrix Workspace-App-Clientmaschinen, die aktiv für die Verbindung mit veröffentlichten Ressourcen verwendet werden.

Er enthält außerdem Informationen zu aktiven Verbindungen, die eingerichtet wurden, während die Hauptdatenbank nicht verfügbar war:

- Ergebnisse jeder von der Citrix Workspace-App durchgeführten Clientmaschinen-Endpunktanalyse.
- Identität von Infrastrukturmaschinen (z. B. Citrix Gateway- und StoreFront-Server), die mit der Site zu tun haben.
- Datum, Uhrzeit und Art kürzlich erfolgter Aktivitäten von Benutzern.

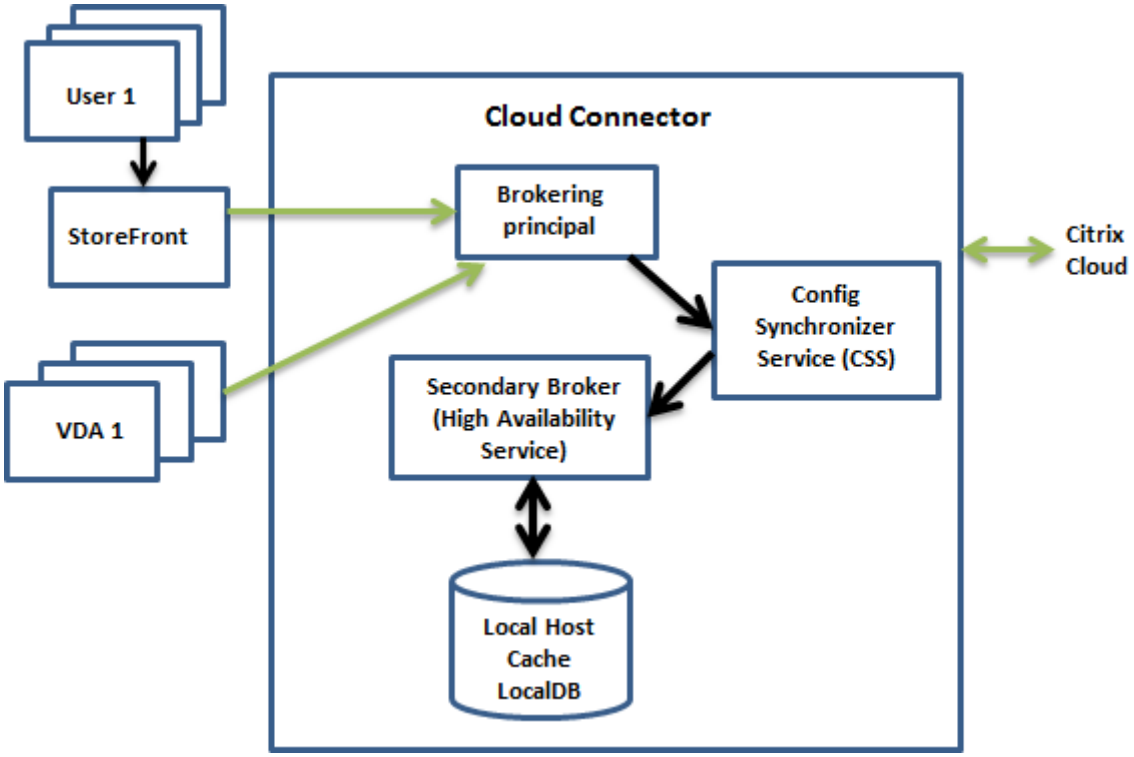
### Funktionsweise

Erfahren Sie, wie der lokale Hostcache mit Citrix Cloud interagiert.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

**Normalbetrieb**




- Der Brokerprinzipal (auch "Citrix Remote Broker Provider Service") auf einem Cloud Connector akzeptiert Verbindungsanfragen von StoreFront. Der Brokering Principal kommuniziert mit Citrix Cloud, um Benutzer mit VDAs zu verbinden, die bei Cloud Connector registriert sind
- Der Citrix Config Synchronizer Service (CSS) überprüft ca. alle 5 Minuten beim Broker in Citrix Cloud, ob Konfigurationsänderungen vorgenommen wurden. Änderungen können von einem Administrator (z. B. Ändern der Eigenschaft einer Bereitstellungsgruppe) oder durch Systemaktionen (z. B. Maschinenzuweisungen) hervorgerufen werden.
- Wenn seit der letzten Überprüfung eine Konfigurationsänderung stattgefunden hat, synchronisiert (kopiert) der CSS die Informationen auf einen sekundären Broker auf dem Cloud Connector. Der sekundäre Broker wird auch als "Dienst für hohe Verfügbarkeit"oder HA-Broker bezeichnet (siehe Abbildung oben).

  Dabei werden nicht nur die seit der letzten Prüfung geänderten Elemente, sondern alle Konfigurationsdaten kopiert. Der CSS importiert die Konfigurationsdaten in eine Microsoft SQL Server Express-LocalDB-Datenbank auf dem Cloud Connector. Diese Datenbank wird als lokale Hostcachedatenbank bezeichnet. Der CSS stellt sicher, dass die Informationen in der lokalen Hostcachedatenbank des sekundären Brokers mit den Informationen in der Sitedatenbank in Citrix Cloud übereinstimmen. Die lokale Hostcachedatenbank wird bei jeder Synchronisierung neu erstellt.

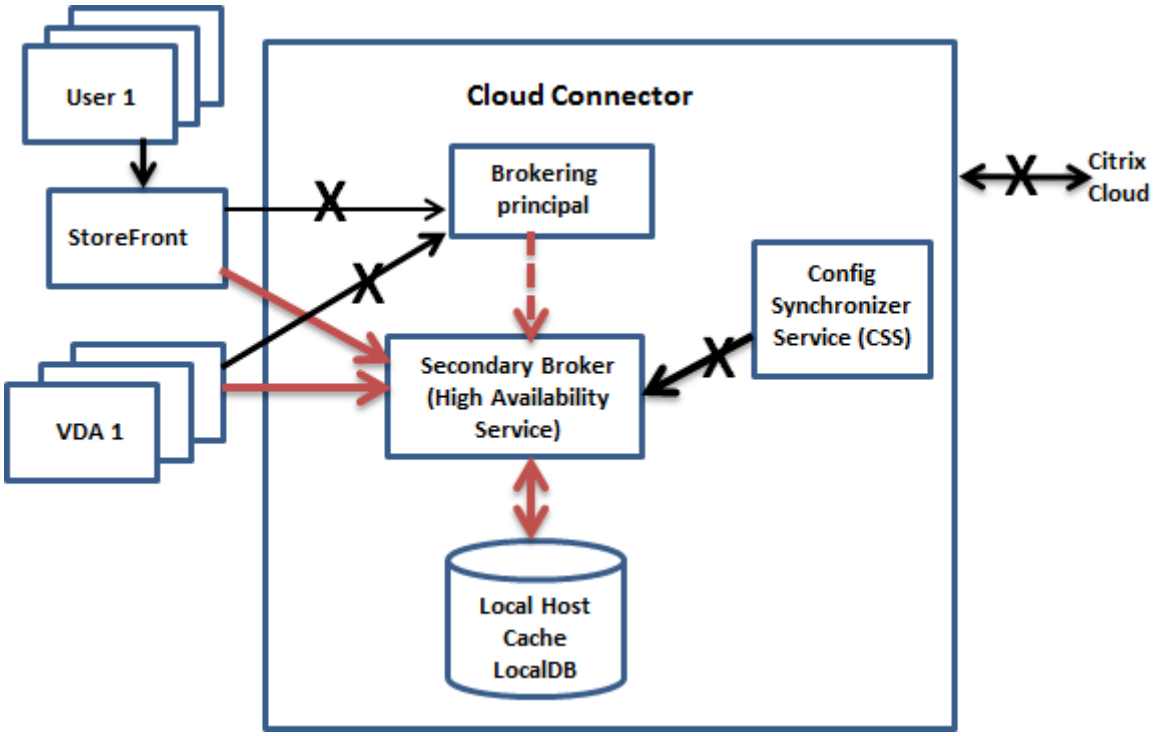
  SQL Server Express LocalDB zur Verwendung mit dem lokalen Hostcache wird automatisch in-

stalliert, wenn Sie einen Cloud Connector installieren. Die lokale Hostcachedatenbank kann nicht für mehrere Cloud Connectors genutzt werden. Sie müssen die lokale Hostcachedatenbank nicht sichern. Sie wird jedes Mal neu erstellt, wenn eine Konfigurationsänderung erkannt wird.

- Wenn seit der letzten Prüfung keine Änderungen erfolgt sind, werden keine Konfigurationsdaten kopiert.

**Bei einem Ausfall**




Wenn ein Ausfall beginnt:

- Der sekundäre Broker beginnt auf Verbindungsanforderungen zu prüfen und diese zu verarbeiten.
- Bei Ausfallbeginn hat der sekundäre Broker keine aktuellen VDA-Registrierungsdaten, doch wenn ein VDA mit ihm kommuniziert, wird eine Registrierung ausgelöst. Während dieses Vorgangs erhält der sekundäre Broker auch aktuelle Sitzungsinformationen zu dem betreffenden VDA.
- Während der sekundäre Broker Verbindungen verarbeitet, überwacht der Brokerprinzipal weiterhin die Verbindung mit Citrix Cloud. Wenn die Verbindung wiederhergestellt ist, weist der Brokerprinzipal den sekundären Broker an, die Prüfung auf Verbindungsinformationen einzustellen, und nimmt das Verbindungsbrokering wieder auf. Wenn ein VDA das nächste Mal mit dem Brokerprinzipal kommuniziert, wird eine Neuregistrierung ausgelöst. Der sekundäre

Broker entfernt alle verbleibenden VDA-Registrierungen aus dem vorherigen Ausfall. Der CSS nimmt die Synchronisierung von Informationen wieder auf, wenn er Konfigurationsänderungen in Citrix Cloud erkennt.

Im dem unwahrscheinlichen Fall, dass ein Ausfall während einer Synchronisierung beginnt, wird der aktuelle Import verworfen und die letzte bekannte Konfiguration verwendet.

Das Ereignisprotokoll enthält Informationen zu Synchronisierungen und Ausfällen.

Es gibt keine zeitliche Begrenzung für den Betrieb in Ausfallmodus.

Sie können einen Ausfall auch absichtlich auslösen. Informationen zu Zweck und Vorgehensweise finden Sie unter Erzwingen eines Ausfalls.

#### Ressourcenstandorte mit mehreren Cloud Connectors

Unter anderem hat der CSS die Aufgabe, den sekundären Broker regelmäßig mit Informationen zu allen Cloud Connectors am Ressourcenstandort zu versorgen. Anhand dieser Informationen sind die Sekundärbroker über alle anderen Sekundärbroker, die auf Cloud Connectors am Ressourcenstandort ausgeführt werden, unterrichtet.

Die sekundären Broker kommunizieren miteinander über einen anderen Kanal. Anhand einer alphabetischen Liste der FQDNs der Maschinen, auf denen sie ausgeführt werden, ermitteln (wählen) diese Broker, welcher sekundäre Broker bei einem Ausfall das Brokering in der Zone übernimmt. Bei einem Ausfall registrieren sich alle VDAs bei dem gewählten sekundären Broker neu. Die nicht gewählten sekundären Broker in der Zone weisen eingehende Verbindungs- und VDA-Registrierungsanfragen aktiv ab.

> **Wichtig:**
>
> Connectors innerhalb eines Ressourcenstandorts müssen in der Lage sein, einander über `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection` zu erreichen. Wenn Connectors unter dieser Adresse nicht kommunizieren können, werden möglicherweise mehrere Broker ausgewählt und während eines lokalen Hostcacheereignisses können zeitweise Startfehler auftreten.

Wenn ein gewählter sekundärer Broker während eines Ausfalls selbst ausfällt, wird stattdessen ein anderer sekundärer Broker gewählt und die VDAs registrieren sich bei diesem.

Wird bei einem Ausfall ein Cloud Connector neu gestartet, passiert Folgendes:

- Handelt es sich bei dem Cloud Connector nicht um den gewählten Broker, hat der Neustart keine Auswirkungen.
- Handelt es sich um den gewählten Broker, wird ein anderer Cloud Connector gewählt und somit werden die VDAs registriert. Wenn der Neustart des Cloud Connectors beendet ist, übernimmt

er automatisch das Brokering und somit werden die VDAs neu registriert. In diesem Szenario kann es während der Registrierungen zu Leistungseinbußen kommen.

Das Ereignisprotokoll enthält Informationen zu diesen Wahlen.

### Während eines Ausfalls nicht verfügbare Elemente und weitere Unterschiede

Es gibt keine zeitliche Begrenzung für den Betrieb in Ausfallmodus. Wenn der Ausfall jedoch auf einen Konnektivitätsverlust vom Ressourcenstandort zu Citrix Cloud zurückzuführen ist, empfiehlt Citrix die schnellstmögliche Wiederherstellung der Verbindung vom Ressourcenstandort.

Bei einem Ausfall:

- Während eines lokalen Hostcache-Ereignisses kann möglicherweise vorübergehend nicht auf die Benutzeroberfläche für die vollständige Konfiguration zugegriffen werden. Wenn auf die Benutzeroberfläche für die vollständige Konfiguration zugegriffen werden kann, werden VDAs an Ressourcenstandorten, die im HA-Modus arbeiten, in der Benutzeroberfläche für die vollständige Konfiguration als nicht registriert angezeigt. Auf diese VDAs kann weiterhin über den lokalen Hostcache zugegriffen werden.
- Sie haben eingeschränkten Zugriff auf das Remote PowerShell SDK.
  - Sie müssen zuerst Folgendes tun:
    * Fügen Sie einen Registrierungsschlüssel `EnableCssTestMode` mit dem Wert `1` hinzu: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Legen Sie die SDK-Authentifizierung auf `OnPrem` fest, damit der SDK-Proxy nicht versucht, die Cmdlet-Aufrufe umzuleiten: `$XDSDKAuth="OnPrem"`
    * Verwenden Sie Port 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - Nachdem Sie diese Befehle ausgeführt haben, können Sie auf Folgendes zugreifen:
    * Alle `Get-Broker*`-Cmdlets.
- Überwachungsdaten werden während eines Ausfalls nicht an Citrix Cloud gesendet. Daher enthalten die **Überwachungsfunktionen** keine Aktivität aus Ausfallintervallen.
- Hypervisor-Anmeldeinformationen können nicht vom Hostdienst abgerufen werden. Bei allen Maschinen ist der Energiezustand unbekannt, es können keine Energievorgänge ausgelöst werden. Auf dem Host eingeschaltete VMs können jedoch für Verbindungsanfragen verwendet werden.

- Zugewiesene Maschinen können nur verwendet werden, wenn die Zuweisung während des normalen Betriebs erfolgte. Neue Zuweisungen sind bei einem Ausfall nicht möglich.
- Die automatische Registrierung und Konfiguration von Remote-PC-Zugriff-Maschinen ist nicht möglich. Im normalen Betrieb registrierte und konfigurierte Maschinen können dagegen verwendet werden.
- Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt, wenn die Ressourcen in verschiedenen Zonen sind.
- Jede Zone agiert während eines LHC-Ereignisses unabhängig. Startvorgänge über Zonen hinweg (von einem Broker in einer Zone zu einem VDA in einer anderen Zone) werden während eines Ausfalls nicht unterstützt. Verwenden Sie die erweiterte Systemintegritätsprüfung von StoreFront, um Startanforderungen während eines LHC-Ereignisses an die entsprechende Zone weiterzuleiten.
- Fällt vor einem geplanten Neustart von VDAs in einer Bereitstellungsgruppe die Sitedatenbank aus, beginnt der Neustart erst nach Ende des Ausfalls. Dieses Szenario kann zu unbeabsichtigten Ergebnissen führen. Weitere Informationen finden Sie unter Verzögerung geplanter Neustarts aufgrund eines Datenbankausfalls.
- Die Zonenpräferenz kann nicht konfiguriert werden. Eventuell konfigurierte Präferenzen werden für den Sitzungsstart nicht berücksichtigt.
- Tagbeschränkungen, bei denen Tags zur Bezeichnung von Ressourcenstandorten verwendet werden, werden für Sitzungsstarts nicht unterstützt. Wenn solche Tagbeschränkungen konfiguriert sind und die Option Erweiterte Integritätsprüfung eines StoreFront-Stores aktiviert ist, können Sitzungen sporadisch evtl. nicht gestartet werden.

### StoreFront

Wenn Sie eine On-Premises-StoreFront-Bereitstellung verwenden, müssen Sie alle Cloud Connectors, bei denen VDAs registriert sind (oder sein können), zu StoreFront als Delivery Controller hinzufügen. Ein Cloud Connector, der nicht zu StoreFront hinzugefügt wird, kann nicht in den Ausfallmodus wechseln, was zu Startfehlern für Benutzer führen kann.

#### Ressourcenverfügbarkeit

Es gibt zwei Möglichkeiten, die Verfügbarkeit von Ressourcen (Apps und Desktops) während eines Ausfalls sicherzustellen:

- Veröffentlichen Sie die Ressourcen an jedem Ressourcenstandort in Ihrer Bereitstellung.

- Bei Verwendung von StoreFront 1912 CU4 oder höher veröffentlichen Sie die Ressourcen an mindestens einem Ressourcenstandort und aktivieren die erweiterte Integritätsprüfung auf allen StoreFront-Servern. Für Versionen vor StoreFront 2308 ist die erweiterte Integritätsprüfung standardmäßig deaktiviert und muss von einem Administrator aktiviert werden. Für StoreFront ab Version 2308 ist dieses Feature standardmäßig aktiviert. Weitere Informationen und Anweisungen zum Aktivieren der erweiterten Integritätsprüfung finden Sie unter Erweiterte Integritätsprüfung.

### Unterstützung für Anwendungen und Desktops

Der LHC unterstützt die folgenden Arten von VDAs und Bereitstellungsmodellen:

| VDA-Typ | Bereitstellungsmodell | VDA-Verfügbarkeit bei LHC-Ereignissen |
|---|---|---|
| Multisitzungs-OS | Anwendungen und Desktops | Immer verfügbar. |
| Einzelsitzungs-OS statisch (zugewiesen) | Desktops | Immer verfügbar. |
| Energieverwaltetes Einzelsitzungs-OS nach dem Zufallsprinzip (gepoolt) | Desktops | Standardmäßig nicht verfügbar. Alle Sitzungsstartversuche für energieverwaltete VDAs in gepoolten Bereitstellungsgruppen |

> **Hinweis:**
>
> Die Aktivierung des Zugriffs auf energieverwaltete Desktop-VDAs in gepoolten Bereitstellungsgruppen hat keinen Einfluss darauf, wie die konfigurierte Eigenschaft `ShutdownDesktopsAfterUse` im normalen Betrieb funktioniert. Wenn der Zugriff auf diese Desktops während LHC aktiviert ist, werden VDAs nach Abschluss des LHC-Ereignisses nicht automatisch neu gestartet. Energieverwaltete Desktop-VDAs in gepoolten Bereitstellungsgruppen können Daten aus früheren Sitzungen beibehalten, bis VDAs neu gestartet werden. Ein VDA-Neustart kann erfolgen, wenn sich ein Benutzer bei Nicht-LHC-Vorgängen vom VDA abmeldet oder Administratoren den VDA neu starten.

| | | Zugriffs auf gepoolte Einzelsitzungsmaschinen mit Energieverwaltung kann dazu führen, dass Daten und Änderungen aus früheren Benutzersitzungen in nachfolgenden Sitzungen wiedergegeben werden. |
|---|---|---|

#### LHC für gepoolte VDAs mit energieverwaltetem Einzelsitzungs-OS über die vollständige Konfiguration aktivieren

Mit der vollständigen Konfiguration können Sie diese Maschinen für neue Verbindungen während LHC-Ereignissen pro Bereitstellungsgruppe verfügbar machen:

- Informationen zum Aktivieren dieses Features bei der Erstellung von Bereitstellungsgruppen finden Sie unter Bereitstellungsgruppen erstellen.
- Informationen zum Aktivieren dieses Features für eine vorhandene Bereitstellungsgruppe finden Sie unter Bereitstellungsgruppen verwalten

> **Hinweis:**
>
> Diese Einstellung ist in der vollständigen Konfiguration nur für gepoolte Desktop-Bereitstellungsgruppen verfügbar, die energieverwaltete VDAs bereitstellen.

#### LHC für gepoolte VDAs für Einzelsitzungs-OS mit PowerShell aktivieren

Gehen Sie folgendermaßen vor, um LHC für VDAs in einer bestimmten Bereitstellungsgruppe zu aktivieren:

1. Aktivieren Sie dieses Feature auf Siteebene, indem Sie den folgenden Befehl ausführen:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. Aktivieren Sie LHC für eine Bereitstellungsgruppe, indem Sie diesen Befehl mit dem angegebenen Bereitstellungsgruppennamen ausführen:

   ```
   Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
    $true
   ```

Führen Sie den folgenden Befehl aus, um die LHC-Standardverfügbarkeit für neu erstellte gepoolte Bereitstellungsgruppen mit energieverwalteten VDAs zu ändern:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

### Funktionsprüfung des lokalen Hostcache

Erfahren Sie, wie Sie die Konfiguration des lokalen Hostcache überprüfen.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Überprüfung des lokalen Hostcache auf korrekte Einrichtung und fehlerfreien Betrieb:

- Wenn Sie StoreFront verwenden, stellen Sie sicher, dass die lokale StoreFront-Bereitstellung auf alle Cloud Connectors an dem Ressourcenstandort verweist.
- Vergewissern Sie sich, dass Synchronisierungsimporte erfolgreich abgeschlossen werden. Überprüfen Sie die Ereignisprotokolle.
- Stellen Sie sicher, dass die lokale Hostcachedatenbank auf jedem Cloud Connector erstellt wurde. Dadurch wird bestätigt, dass der Dienst für hohe Verfügbarkeit bei Bedarf übernehmen kann.

  - Navigieren Sie auf dem Cloud Connector-Server zu `c:\Windows\ServiceProfiles\NetworkService`.
  - Überprüfen Sie, ob `HaDatabaseName.mdf` und `HaDatabaseName_log.ldf` erstellt wurden.

- Erzwingen Sie einen Ausfall für alle Cloud Connectors am Ressourcenstandort. Vergessen Sie nicht, nach der Funktionsprüfung des lokalen Hostcache alle Cloud Connectors wieder in den normalen Modus zu versetzen. Dies kann ungefähr 15 Minuten dauern.

## Ereignisprotokolle

Ereignisprotokolle enthalten Informationen zu Synchronisierungen und Ausfällen. In Ereignisanzeige-Protokollen wird der Ausfallmodus als *HA mode*bezeichnet.

### Config Sync-Dienst

Im Normalbetrieb können die folgenden Ereignisse auftreten, wenn der CSS die Konfigurationsdaten mit dem lokalen Hostcachebrokers in die lokale Hostcachedatenbank importiert.

- 503: Der Citrix Config Sync-Dienst erhielt eine aktualisierte Konfiguration. Dieses Ereignis tritt jedes Mal auf, wenn eine aktualisierte Konfiguration von Citrix Cloud eintrifft. Es zeigt den Beginn des Synchronisationsprozesses an.
- 504: Der Citrix Config Sync-Dienst hat eine aktualisierte Konfiguration importiert. Der Konfigurationsimport wurde erfolgreich abgeschlossen.
- 505: Fehler bei einem Import in den Citrix Config Sync-Dienst. Der Konfigurationsimport wurde nicht erfolgreich abgeschlossen. Wenn eine frühere, erfolgreich importierte Konfiguration verfügbar ist, wird diese bei einem Ausfall verwendet. Sie ist jedoch im Vergleich zur aktuellen Konfiguration veraltet. Wenn keine vorherige Konfiguration vorliegt, kann sich der Dienst bei einem Ausfall nicht an der Sitzungsvermittlung beteiligen. Lesen Sie in diesem Fall den Abschnitt Fehlerbehebung und wenden Sie sich an den Citrix Support.
- 507: Der Citrix Config Sync Service hat einen Importvorgang abgebrochen, weil ein Systemausfall vorliegt und der lokale Hostcachebroker für die Vermittlung verwendet wird. Der Dienst hat eine neue Konfiguration erhalten, der Import wurde jedoch abgebrochen, da ein Ausfall aufgetreten ist. Dieses Verhalten wird erwartet.
- 510: Es wurden keine Konfigurationsdienst-Konfigurationsdaten vom primären Konfigurationsdienst empfangen.
- 517: Ein Problem ist bei der Kommunikation mit dem primären Broker aufgetreten.
- 518: Das Config Sync-Skript wurde abgebrochen, weil der sekundäre Broker (Hohe Verfügbarkeit) nicht ausgeführt wird.

### Dienst für hohe Verfügbarkeit

Dieser Dienst wird auch als lokaler Hostcachebroker bezeichnet.

- 3502: Ein Ausfall ist aufgetreten und der lokale Hostcachebroker führt Brokervorgänge durch.
- 3503: Ein Ausfall wurde behandelt und der Normalbetrieb wieder aufgenommen.
- 3504: Gibt an, welcher lokale Hostcachebroker gewählt wurde und welche anderen lokalen Hostcachebroker bei der Wahl beteiligt waren.
- 3507: Stellt alle 2 Minuten eine Statusaktualisierung des lokalen Hostcache bereit, die angibt, dass der Modus "Lokaler Hostcache"auf dem ausgewählten Broker aktiv ist. Enthält eine Zusammenfassung des Ausfalls, einschließlich Ausfalldauer, VDA-Registrierung und Sitzungsinformationen.
- 3508: Gibt an, dass der lokale Hostcache auf dem ausgewählten Broker nicht mehr aktiv ist und dass der normale Betrieb wiederhergestellt wurde. Enthält eine Zusammenfassung des Ausfalls, einschließlich Ausfalldauer, Anzahl der Maschinen, die während des lokalen Hostcache-Ereignisses registriert wurden, und der Anzahl erfolgreicher Starts während des lokalen Hostcache-Ereignisses.
- 3509: Gibt an, dass der lokale Hostcache auf dem bzw. den nicht ausgewählten Broker(n) aktiv ist. Liefert alle 2 Minuten Angaben zur Ausfalldauer und gibt den ausgewählten Broker an.
- 3510: Gibt an, dass der lokale Hostcache auf dem bzw. den nicht ausgewählten Broker(n) nicht mehr aktiv ist. Enthält die Ausfalldauer und gibt den ausgewählten Broker an.

### Remote Broker Provider

Dieser Dienst fungiert als Proxy zwischen Citrix Cloud und Ihren VDAs und Cloud Connectors.

- 3001: Prüft, ob Cloud Connectors in den HA-Modus wechseln müssen. Dieses Ereignis tritt nach einer einzigen fehlgeschlagenen Systemintegritätsprüfung des Cloud Connector auf. Schlägt eine zusätzliche Systemintegritätsprüfung nach 60 Sekunden fehl, wechselt der Cloud Connector in den HA-Modus.
- 3002: Benachrichtigt darüber, dass der Cloud Connector nicht in den HA-Modus wechseln kann. Der Grund dafür, dass der HA-Modus nicht aufgerufen wurde, ist in den Ereignisinformationen enthalten.
- 3003: Benachrichtigt darüber, dass der Cloud Connector verschiedene HA-Modusstatus durchläuft. Dieses Diagramm beschreibt die Status für das Aufrufen und Beenden des HA-Modus. Das Ereignis enthält Informationen zu:
  - dem Status, aus dem der Cloud Connector wechselt.
  - der Status, in den der Cloud Connector übergeht.
  - die Dauer des vorherigen Status.

> **Hinweis:**
>
> 3001-Ereignisse kommen für Cloud Connectors häufig vor. Diese Ereignisse können auf Netzwerkfehler zurückzuführen sein und geben keinen Anlass zur Sorge.

### Erzwingen eines Ausfalls

In folgenden Situationen kann das Erzwingen eines Ausfalls erforderlich sein:

- Die Netzwerkverbindung wird wiederholt unterbrochen. Durch das Erzwingen eines Ausfalls bis zum Beheben des Netzwerkproblems werden fortlaufende Übergänge zwischen normalem Modus und Ausfallmodus (und somit häufige VDA-Registrierungen) vermieden.
- Zum Testen eines Notfallwiederherstellungsplans
- Zur Prüfung des ordnungsgemäßen Betriebs des lokalen Hostcache

Ein Cloud Connector kann zwar während eines erzwungenen Ausfalls aktualisiert werden, dabei können jedoch unvorhergesehene Probleme auftreten. Wir empfehlen das Festlegen eines Zeitplans für Cloud Connector-Updates, durch den Zeiten erzwungener Ausfälle vermieden werden.

Zum Erzwingen eines Ausfalls bearbeiten Sie die Registrierung jedes Cloud Connector-Servers. Erstellen Sie für `HKLM\Software\Citrix\DesktopServer\LHC` `OutageModeForced` und legen Sie `REG_DWORD` auf `1` fest. Dadurch wird der lokale Hostcachebroker angewiesen, unabhängig vom Zustand der Verbindung mit Citrix Cloud in den Ausfallmodus zu wechseln. Wenn Sie den Wert auf `0` festlegen, wird der Ausfallmodus auf dem lokalen Hostcachebroker beendet.

Überprüfen Sie die Ereignisse in der Protokolldatei `Current_HighAvailabilityService` in `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAavailabilityService`.

### Problembehandlung

Mehrere Problembehandlungstools sind verfügbar, wenn ein Synchronisierungsimport in die lokale Hostcachedatenbank fehlschlägt und ein 505-Ereignis verzeichnet wird.

**Ablaufverfolgung mit CDF**: Enthält Optionen für die Module ConfigSyncServer und BrokerLHC. In Kombination mit anderen Brokermodulen kann mit diesen Optionen das Problem identifiziert werden.

**Bericht**: Wenn ein Synchronisierungsimport fehlschlägt, können Sie einen Bericht erstellen. Der Bericht endet mit dem Objekt, das den Fehler verursacht hat. Das Berichtsfeature wirkt sich auf die Synchronisierungsgeschwindigkeit aus. Deshalb empfiehlt Citrix, es zu deaktivieren, wenn es nicht verwendet wird.

Zum Aktivieren von CSS und Erstellen eines Ablaufverfolgungsberichts geben Sie folgenden Befehl ein:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Der HTML-Bericht wird unter `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html` veröffentlicht.

Wenn der Bericht generiert wurde, deaktivieren Sie das Berichtsfeature durch Eingabe des folgenden Befehls:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

#### PowerShell-Befehle für den lokalen Hostcache

Sie können den lokalen Hostcache auf Ihren Cloud Connectors mithilfe von PowerShell-Befehlen verwalten.

Das PowerShell-Modul ist auf den Cloud Connectors hier gespeichert:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Wichtig:**
>
> Führen Sie dieses Modul nur auf den Cloud Connectors aus.

**PowerShell-Modul importieren** Um das Modul zu importieren, führen Sie folgenden Befehl auf Ihrem Cloud Connector aus:

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-
Module .\HighAvailabilityServiceControl.psm1
```

**PowerShell-Befehle zur Verwaltung des lokalen Hostcache** Mit den folgenden Cmdlets können Sie den Modus “Lokaler Hostcache”(LHC) auf den Cloud Connectors aktivieren und verwalten.

| Cmdlets | Funktion |
| --- | --- |
| `Enable-LhcForcedOutageMode` | Versetzen Sie den Broker in den Modus “Lokaler Hostcache”. Datenbankdateien für den lokalen Hostcache müssen erfolgreich vom ConfigSync-Dienst erstellt worden sein, damit `Enable-LhcForcedOutageMode` ordnungsgemäß funktioniert. Dieses Cmdlet erzwingt den lokalen Hostcache nur auf dem Cloud Connector, auf dem es ausgeführt wurde. Um den lokalen Hostcache zu aktivieren, muss dieses Cmdlet auf allen Cloud Connectors innerhalb des Ressourcenstandorts ausgeführt werden. |
| `Disable-LhcForcedOutageMode` | Beendet den Modus “Lokaler Hostcache”auf dem Broker. Dieses Cmdlet deaktiviert den Modus “Lokaler Hostcache”nur auf dem Cloud Connector, auf dem es ausgeführt wurde. `Disable-LhcForcedOutageMode` muss auf allen Cloud Connectors innerhalb des Ressourcenstandorts ausgeführt werden. |
| `Set-LhcConfigSyncIntervalOverride` | Legt das Intervall fest, in dem Citrix Config Synchronizer Service (CSS) nach Konfigurationsänderungen innerhalb der Citrix DaaS-Site sucht. Das Zeitintervall kann zwischen 60 Sekunden (eine Minute) und 3600 Sekunden (eine Stunde) liegen. Diese Einstellung gilt nur für den Cloud Connector, auf dem sie ausgeführt wurde. Damit alle Cloud Connector übereinstimmen, sollten Sie das Cmdlet auf jedem Cloud Connector ausführen. Beispiel: `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |

| Cmdlets | Funktion |
| --- | --- |
| `Clear-LhcConfigSyncIntervalOverride` | Legt das Intervall fest, in dem Citrix Config Synchronizer Service (CSS) nach Konfigurationsänderungen innerhalb der Citrix DaaS-Site sucht. Standardwert 300 Sekunden (5 Minuten). Diese Einstellung gilt nur für den Cloud Connector, auf dem sie ausgeführt wurde. Damit alle Cloud Connector übereinstimmen, sollten Sie das Cmdlet auf jedem Cloud Connector ausführen. |
| `Enable-LhcHighAvailabilitySDK` | Ermöglicht den Zugriff auf jedes Cmdlet `Get-Broker*` innerhalb des Cloud Connectors, auf dem es ausgeführt wurde. |
| `Disable-LhcHighAvailabilitySDK` | Deaktiviert den Zugriff auf die Broker PowerShell-Befehle innerhalb des Cloud Connectors, auf dem er ausgeführt wurde. |

> **Hinweis:**
>
> - Verwenden Sie Port 89, wenn Sie die Cmdlets `Get-Broker*` auf dem Cloud Connector ausführen. Beispiel:
>   - `Get-BrokerMachine -AdminAddress localhost:89`
> - Wenn sich der Broker des lokalen Hostcache auf dem Cloud Connector nicht im Modus "Lokaler Hostcache"befindet, enthält er nur Konfigurationsinformationen.
> - Im Modus "Lokaler Hostcache"enthält der Broker des lokalen Hostcache auf dem ausgewählten Cloud Connector die folgenden Informationen:
>   - Ressourcenzustände
>   - Sitzungsdetails
>   - VDA-Registrierungen
>   - Konfigurationsangaben

### Weitere Informationen

Unter Überlegungen zur Skalierung und Größe für den lokalen Hostcache finden Sie Informationen zu:

- Testmethoden und -ergebnisse
- RAM-Größe

- CPU-Kern- und Socketkonfiguration
- Speicher

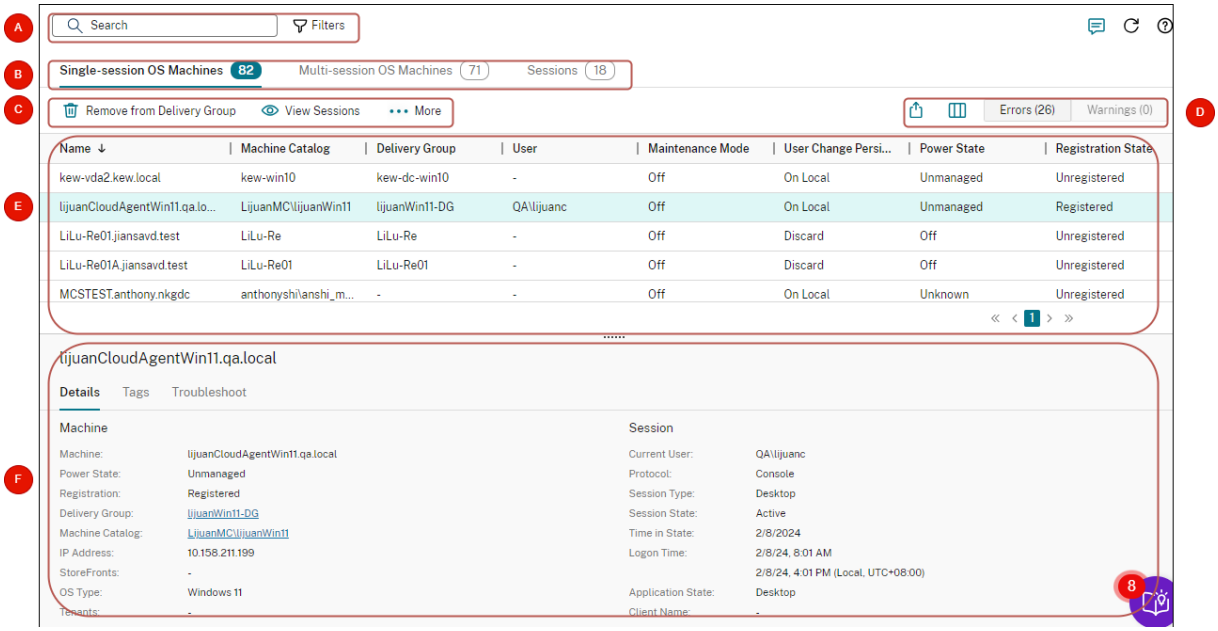
# Maschinen und Sitzungen mit der Suche überwachen und verwalten

June 12, 2024

In diesem Artikel erfahren Sie, wie Sie Maschinen und Sitzungen mit dem Knoten **Vollständige Konfiguration > Suchen** überwachen und verwalten.

## Weitere Informationen über den Knoten

Der Knoten **Suche** bietet einen zentralen Ort für die Überwachung und Verwaltung von Maschinen und Benutzersitzungen.




| Legende | Bereich | Beschreibung |
|---|---|---|
| A | Suchleiste | Bietet eine Schnellsuche und eine filterbasierte Suche, mit der Sie komplexe Suchkriterien definieren können. Weitere Informationen finden Sie unter Nach Instanzen suchen. |

| Legende | Bereich | Beschreibung |
| --- | --- | --- |
| B | Typ-Registerkarten | Zeigt Registerkarten an, auf denen Maschinen nach Typ oder alle Sitzungen aufgelistet werden. Die Anzahl der Instanzen wird in den Registerkartennamen angezeigt. |
| C | Aktionen auf Instanzebene | Zeigt Aktionen an, die Sie auf den *ausgewählten Instanzen* (Maschinen oder Sitzungen) ausführen können. Weitere Informationen finden Sie unter Maschinenaktionen und Sitzungsaktionen. |
| D | Aktionen auf Listenebene | Zeigt Aktionen an, die Sie für die aktuelle *Liste* ausführen können<br>**Exportsymbol**: Exportiert die Liste der in der Hauptansicht angezeigten Instanzen in eine CSV-Datei.<br>-Symbol für **anzuzeigende Spalte**: Passt die Hauptansicht für die Liste an.<br>**Fehlerlabel**: Aktivieren Sie dieses Label, um nur nicht registrierte Maschinen mit Fehlern in der Hauptansicht anzuzeigen. Um Problemdetails anzuzeigen, wechseln Sie im Bereich **Details** zur Registerkarte **Problembehandlung**.<br>**Warnlabel**: Aktivieren Sie dieses Label, um nur nicht registrierte Maschinen mit Warnungen in der Hauptansicht anzuzeigen. Um Problemdetails anzuzeigen, wechseln Sie im Bereich **Details** zur Registerkarte **Problembehandlung**. |
| E | Hauptansicht | Zeigt die Instanzen und ihre Eigenschaften an. Sie können die Hauptansicht anpassen, indem Sie das Symbol **Anzuzeigende Spalte** auswählen. Weitere Informationen zu den verfügbaren Spalten finden Sie unter Maschinenspalten und Sitzungsspalten. |
| F | Bereich “Details” | Zeigt die folgenden Details an<br>Details der ausgewählten Instanz (Maschine oder Sitzung)<br>Auf die ausgewählte Maschine angewendete Tags<br>Details zu Fehlern oder Warnungen mit der ausgewählten Maschine, einschließlich Problemen, möglichen Ursachen und Lösungsvorschlägen |

## Nach Instanzen suchen

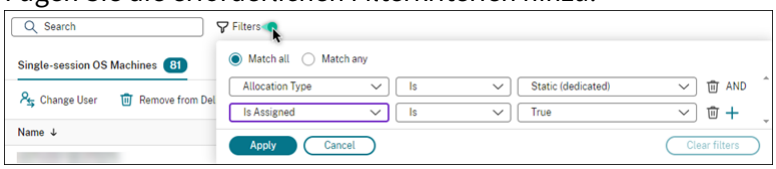
Verwenden Sie die Suchfunktion, um bestimmte Maschinen und Sitzungen zu finden:

- Mit Filtern suchen
- Aktuellen Filtersatz für eine schnelle Suche speichern
- Filterfeld in der Suchleiste fixieren
- Mit dem Schnellsuchfeld suchen
- Tipps zur Verbesserung der Suche

### Mit Filtern suchen

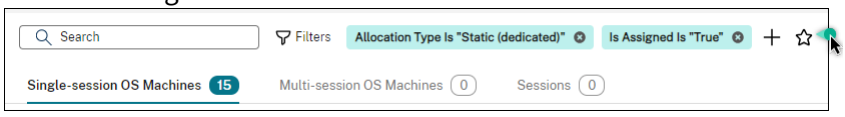
Beispiel: Gehen Sie wie folgt vor, um alle Maschinen mit Einzelsitzungs-OS zu finden, die *statisch* und *Benutzern zugewiesen* sind:

1. Klicken Sie auf der Registerkarte **Maschinen mit Einzelsitzungs-OS** auf das Symbol **Filter**. Das Fenster “Filter”wird angezeigt.
2. Fügen Sie die erforderlichen Filterkriterien hinzu.




3. Wählen Sie **Übereinstimmung mit allen** (AND-Operator), wenn die Suche Ergebnisse zurückgeben soll, die allen Filterkriterien entsprechen. Wählen Sie **Beliebige Übereinstimmung** (OR-Operator), wenn die Suche Ergebnisse zurückgeben soll, die einem der Filterkriterien entsprechen.
4. Klicken Sie auf **Anwenden**.

   In der gefilterten Liste werden alle Maschinen mit Einzelsitzungs-OS angezeigt, die statisch und Benutzern zugewiesen sind.




### Aktuellen Filtersatz für eine schnelle Suche speichern

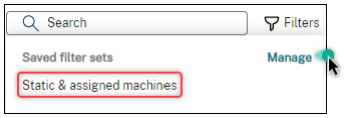
Gehen Sie beispielsweise folgendermaßen vor, um den Filtersatz für Maschinen mit Einzelsitzungs-OS zu speichern, die statisch und Benutzern für die zukünftige Verwendung zugewiesen sind:

1. Nachdem Sie eine filterbasierte Suche durchgeführt haben, klicken Sie in der Suchleiste auf das **Sternsymbol**, wie in der vorherigen Abbildung dargestellt.

2. Geben Sie auf der angezeigten Seite einen Namen für diesen Filtersatz ein (z. B. *Statische und zugewiesene Maschinen*).
3. Klicken Sie auf **Speichern**.

   Der gespeicherte Filtersatz wird in der Liste des Suchverlaufs angezeigt, wenn Sie auf das Suchfeld klicken.

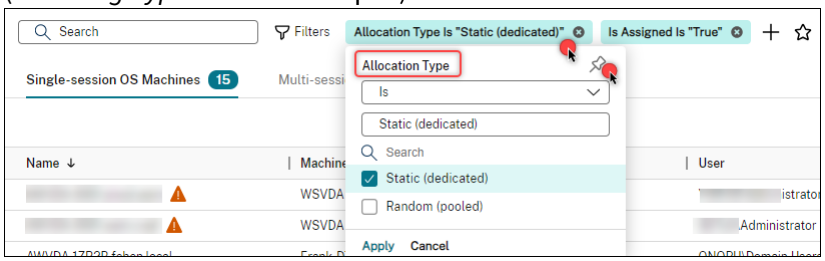



> **Hinweis:**
>
> Filtersätze werden pro Benutzerkonto gespeichert. Um gespeicherte Filtersätze zu verwalten, wählen Sie **Verwalten**.

### Filterfeld in der Suchleiste fixieren

Fixieren Sie häufig verwendete *Filterfelder* in der Suchleiste, um den Zugriff zu erleichtern. Beispiel: Nachdem Sie eine filterbasierte Suche durchgeführt haben, möchten Sie **Zuteilungstyp** in der Suchleiste fixieren. Führen Sie folgende Schritte aus:

1. Klicken Sie in der Suchleiste auf die *Filtereinstellung*.
2. Klicken Sie im daraufhin angezeigten Fenster auf das **Anheftsymbol**, um das Filterfeld (*Zuteilungstyp* für dieses Beispiel) in der Suchleiste zu fixieren.




### Mit dem Schnellsuchfeld suchen

Das Schnellsuchfeld bietet eine bequeme Möglichkeit, anhand namensbezogener Eigenschaften oder gespeicherter Filtersätze nach Instanzen zu suchen. Verfahren:

1. Klicken Sie auf das Suchfeld. Ihre letzten Suchanfragen und gespeicherten Filtersätze werden in der Dropdownliste angezeigt. Sie können auf eine vorherige Suche oder einen Filtersatz klicken, um eine Schnellsuche durchzuführen.
2. Um eine neue Suche zu starten, geben Sie einen vollständigen oder teilweisen Namen aus den folgenden Optionen ein:

- Maschinenname oder DNS-Name
- Maschinenkatalogname
- Bereitstellungsgruppenname
- Sitzungsbenutzername
- Name des Sitzungsclients
- Der vom Hypervisor verwendete Anzeigename der VM, die die Sitzung hostet.
- Hostingservername

**Tipps zur Verbesserung der Suche**

Beachten Sie bei der Verwendung der Suchfunktion die folgenden Tipps:

- Wählen Sie im Knoten **Suchen** eine beliebige Spalte, um Elemente zu sortieren.
- Um weitere Eigenschaften in die Anzeige zu integrieren, anhand derer Sie dann suchen und sortieren können, wählen Sie **Spalten auswählen** oder klicken Sie auf eine beliebige Spalte und wählen Sie **Spalten auswählen**. Aktivieren Sie im Fenster **Spalten auswählen** das Kontrollkästchen neben den anzuzeigenden Elementen, und wählen Sie **Speichern** zum Beenden.

  > **Hinweis:**
  >
  > Spalten, die die Leistung beeinträchtigen, sind mit **Beeinträchtigt die Leistung** gekennzeichnet.

- Wählen Sie zum Suchen eines mit einer Maschine verbundenen Benutzergeräts **Client (IP)** und **Ist** und geben Sie die IP-Adresse des Geräts ein.
- Wenn Sie aktive Sitzungen suchen, verwenden Sie **Sitzungszustand**, **Ist** und **Verbunden**.
- Um alle Maschinen in einer Bereitstellungsgruppe aufzulisten, wählen Sie im linken Bereich **Bereitstellungsgruppen**. Wählen Sie die Gruppe aus, und wählen Sie dann in der Aktionsleiste oder im Kontextmenü **Maschinen anzeigen**.

Beachten Sie bei Sortierungsvorgängen Folgendes:

- Wenn die Anzahl der Elemente 5000 nicht überschreitet, können Sie auf eine beliebige Spalte klicken, um die darin enthaltenen Elemente zu sortieren. Über 5000 Elemente können Sie nur nach Namen oder nach dem aktuellen Benutzer (je nach gerade geöffneter Registerkarte) sortieren. Filtern Sie die Elemente, um deren Anzahl auf maximal 5.000 zu reduzieren und die Sortierung zu ermöglichen.
- Bei einer Anzahl Elemente von 501 bis 5000 geschieht Folgendes:
  - Alle Daten werden lokal zwischengespeichert, um die Sortierleistung zu verbessern. Auf den Registerkarten **Maschinen mit Betriebssystemen für Einzelsitzungen** und **Maschinen mit Multisitzungs-OS** werden die Daten zwischengespeichert, wenn Sie zum ersten

Mal zum Sortieren auf eine Spalte klicken (mit Ausnahme der Spalte **Name**). Auf der Registerkarte **Sitzungen** werden die Daten zwischengespeichert, wenn Sie zum ersten Mal zum Sortieren auf eine Spalte klicken (mit Ausnahme der Spalte **Aktueller Benutzer**). Die Sortierung nimmt daher mehr Zeit in Anspruch. Sortieren Sie für eine schnellere Leistung nach dem Namen oder dem aktuellen Benutzer oder verwenden Sie Filter, um die Anzahl der Elemente zu reduzieren.

- Die folgende Meldung unterhalb der Tabelle weist darauf hin, dass die Daten zwischengespeichert wurden: Zuletzt aktualisiert: `<the time when you refreshed the table>`. In diesem Fall basiert die Sortierung auf den zuvor geladenen Elementen. Diese Elemente sind möglicherweise nicht auf dem neuesten Stand. Um sie auf den neuesten Stand zu bringen, klicken Sie auf das Aktualisierungssymbol.

### Anpassen der Spaltenanzeige

Erstellen Sie eine personalisierte Hauptansicht, um die Eigenschaften und Status anzuzeigen, die für Ihren täglichen Betrieb entscheidend sind. Verfahren:

1. Wählen Sie im Knoten **Suchen** nach Bedarf die Registerkarte **Maschine mit Multisitzungs-OS**, **Maschinen mit Einzelsitzungs-OS** oder **Sitzungen**.
2. Klicken Sie in der Aktionsleiste auf das Symbol **Anzuzeigende Spalten** und wählen Sie die Spalten aus.

   Weitere Informationen zu den verfügbaren Spalten und ihren Beschreibungen finden Sie unter Maschinenspalten und Sitzungsspalten.

Beim Auswählen der Spalten werden einige Spalten mit dem Hinweis **Beeinträchtigt die Leistung** ausgewiesen. Das Auswählen dieser Spalten kann die Leistung der Konsole beeinträchtigen. Beachten Sie diese Überlegungen:

- Nachdem Sie Ihre Anpassung abgeschlossen haben, wird die Tabelle aktualisiert, um die ausgewählten Spalten anzuzeigen. Ihr Vorhandensein kann zu Verzögerungen führen, wenn Sie die Tabelle aktualisieren.
- Nachdem Sie den Browser aktualisiert oder sich von der Konsole abgemeldet und dann angemeldet haben, wird eine Meldung angezeigt, in der Sie gefragt werden, ob diese Spalten beibehalten werden sollen. Wenn Sie sich dafür entscheiden, sie beizubehalten, können Sie die Tabelle nur einmal pro Minute aktualisieren, um eine optimale Konsolenleistung zu erzielen. Für häufigere Aktualisierungen entfernen Sie alle Spalten, die die Leistung beeinträchtigen.

## Maschinen und Sitzungen verwalten

Verwenden Sie Aktionen im Suchknoten, um Maschinen- und Sitzungsprobleme zu beheben oder Benutzeranfragen zu verarbeiten.

### Nützliche Info

Sie können Maschinen auf verschiedenen Ebenen verwalten:

- Auf der Ebene der einzelnen Maschinen. Verwenden Sie den **Suchknoten**, um Zielmaschinen zu finden und Aktionen auszuführen.
- Auf Maschinenkatalogebene, beispielsweise beim Ändern von Masterimages für einen Katalog, Löschen von Maschinen aus einem Katalog und Hinzufügen von Maschinen zu einem Katalog. Weitere Informationen finden Sie unter Verwalten von Maschinenkatalogen.
- Auf Bereitstellungsgruppenebene, beispielsweise beim Ein- oder Ausschalten des Wartungsmodus für Maschinen in einer Gruppe. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

Zusätzlich zur individuellen Sitzungsebene können Sie Sitzungen auch auf Bereitstellungsgruppenebene verwalten, indem Sie beispielsweise Sitzungsvorabstart und Sitzungsfortbestehen für eine Bereitstellungsgruppe konfigurieren. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

### Aktionen auf Maschinen oder Sitzungen ausführen

Gehen Sie folgendermaßen vor, um Maschinen oder Sitzungen auf der Ebene der einzelnen Instanzen zu verwalten:

1. Wählen Sie im Knoten **Suchen** die Registerkarte **Maschine mit Multisitzungs-OS**, **Maschinen mit Einzelsitzungs-OS** oder **Sitzungen**.
2. Wählen Sie je nach Bedarf eine oder mehrere Instanzen aus.
3. Wählen Sie in der Aktionsleiste oder im Rechtsklickmenü eine Aktion aus, die auf den Problemen basiert, die bei diesen Instanzen oder Benutzeranforderungen auftreten.

   Weitere Informationen zu den verfügbaren Aktionen und deren Beschreibungen finden Sie unter Maschinenaktionen und Sitzungsaktionen.

> **Hinweis:**

> Wenn Sie zwei oder mehr Instanzen auswählen, sind nur Aktionen verfügbar, die für alle Instanzen gelten.

### Maschinen- oder Sitzungsdaten in CSV-Dateien exportieren

Exportieren Sie die Liste der Instanzen (Maschinen oder Sitzungen), die auf einer Registerkarte angezeigt werden (bis zu 30.000 Elemente), in eine CSV-Datei. Verfahren:

1. Wählen Sie im Knoten **Suchen** nach Bedarf die Registerkarte **Maschine mit Multisitzungs-OS**, **Maschinen mit Einzelsitzungs-OS** oder **Sitzungen**.
2. Klicken Sie dazu auf das **Exportsymbol** in der oberen rechten Ecke.
3. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Weiter**.

   Es kann mehrere Minuten dauern, bis der Export abgeschlossen ist. Sie finden die Datei im Standard-Download-Ordner Ihres Browsers.

> **Hinweis:**
>
> Wenn bereits ein Export ausgeführt wird, können Sie auf einer Registerkarte des Knotens **Suchen** keinen weiteren Export ausführen.

## Maschinenaktionen und Spalten

June 12, 2024

In diesem Artikel werden Maschinenaktionen und Spalten mit Beschreibungen als Referenz aufgeführt.

### Aktionen

Sehen Sie sich die Aktionen an, die Sie an Maschinen ausführen können, und deren Beschreibungen.

| Aktion | Beschreibung | Gilt für |
| --- | --- | --- |
| Systemintegritätsprüfung ausführen | Nur für registrierte Windows VDAs Version 2019 und höher verfügbar. Systemintegritätsprüfung an einer Maschine durchführen. Weitere Informationen zu den Prüfinhalten finden Sie unter Über Systemprüfungen. | Einzelsitzung und Multisitzung |
| Aus Bereitstellungsgruppe entfernen | Eine Maschine aus der Bereitstellungsgruppe entfernen. | Einzelsitzung und Multisitzung |
| Zu Bereitstellungsgruppe hinzufügen | Fügen Sie einer Bereitstellungsgruppe eine Maschine hinzu. | Einzelsitzung und Multisitzung |
| Sitzungen anzeigen | Sehen Sie sich die Sitzungen an, die auf einer Maschine ausgeführt werden | Einzelsitzung und Multisitzung |
| Tags verwalten | Fügen Sie Tags für eine Maschine hinzu und verwalten Sie sie. Weitere Informationen zu typischen Anwendungsfällen von Tags finden Sie unter Tags. | Einzelsitzung und Multisitzung |
| Wartungsmodus einschalten | Es kann nötig sein, eine Maschine in den Wartungsmodus zu versetzen, bevor ein Patch angewendet oder ein Problem behandelt wird. Dieser Modus verhindert, dass neue Verbindungen zu dieser Maschine hergestellt werden. Die Benutzer können sich mit Sitzungen auf der Maschine verbinden, auf ihr aber keine neuen Sitzungen starten. | Einzelsitzung und Multisitzung |

| Aktion | Beschreibung | Gilt für |
| --- | --- | --- |
| Wartungsmodus ausschalten | Schalten Sie den Wartungsmodus für eine Maschine aus. | Einzelsitzung und Multisitzung |
| VDA aktualisieren | Aktualisieren Sie den VDA für eine Maschine. | Maschinen mit Einzelsitzungs- oder Multisitzungs-OS, die bestimmte Anforderungen erfüllen: Weitere Informationen. |
| Abmelden | Abmelden einer Maschine erzwingen | Einzelsitzung und Multisitzung |
| Löschen | Eine VM aus einem Maschinenkatalog löschen, während Sie sie auf dem Hypervisor oder Clouddienst intakt lassen. | Einzelsitzung und Multisitzung |
| Benutzer ändern | Weisen Sie eine Maschine einem bestimmten Benutzer zu. | *Statische* Einzelsitzungs-OS-Maschinen. |
| Starten | Eine Maschine starten. | Einzelsitzung und Multisitzung |
| Herunterfahren | Eine Maschine herunterfahren. | Einzelsitzung und Multisitzung |
| Neu starten | Maschine neu starten | Einzelsitzung und Multisitzung |
| Anhalten | Eine Maschine in den Ruhe- oder Anhaltezustand versetzen. Wenn Sie eine Maschine anhalten, speichert DaaS den Speicherinhalt der Maschine in einer Datei und fährt die Maschine dann herunter. | Maschinen mit Einzelsitzungs-OS |
| Fortsetzen | Eine angehaltene Maschine fortsetzen. Wenn Sie eine angehaltene Maschine fortsetzen, startet der DaaS die Maschine und versetzt sie in den vorherigen Zustand zurück. | Maschinen mit Einzelsitzungs-OS |
| Neustart erzwingen | Erzwingen Sie einen Neustart einer Maschine. | Maschinen mit Einzelsitzungs-OS |

| Aktion | Beschreibung | Gilt für |
| --- | --- | --- |
| Herunterfahren erzwingen | Damit können Sie das Herunterfahren einer Maschine erzwingen. | Maschinen mit Einzelsitzungs-OS |

## Spalten

Alle Maschinenspalten und ihre Beschreibungen nach Typ anzeigen:

- Maschine
- Maschinendetails
- Anwendungen
- Hosting
- Verbindung
- Registrierung
- Sitzungsdetails
- Sitzung

### Maschine

Spalten in der Kategorie **Maschine**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Name | Der DNS-Hostname der Maschine. | Einzelsitzung und Multisitzung |
| Maschinenkatalog | Der Name des Katalogs, zu dem die Maschine gehört. | Einzelsitzung und Multisitzung |
| Bereitstellungsgruppe | Der Name der Bereitstellungsgruppe, zu der die Maschine gehört. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Anzeigename für Benutzer | Die vollständigen Namen der Benutzer, die der Maschine zugewiesen sind (normalerweise in der Form `Firstname Lastname`). Zugewiesene Benutzer sind die aktuellen Benutzer für freigegebene Maschinen und die zugewiesenen Benutzer für dedizierte Maschinen. | Einzelsitzung und Multisitzung |
| Benutzer | Die Benutzernamen der Benutzer, die der Maschine zugewiesen sind (in der Form “domain\user”). Zugewiesene Benutzer sind die aktuellen Benutzer für freigegebene Maschinen und die zugewiesenen Benutzer für dedizierte Maschinen. | Einzelsitzung und Multisitzung |
| Benutzerprinzipalname | Die Benutzerprinzipalnamen der Benutzer, die der Maschine zugewiesen sind (in der Form “Benutzer@Domäne”). Zugewiesene Benutzer sind die aktuellen Benutzer für freigegebene Maschinen und die zugewiesenen Benutzer für dedizierte Maschinen. | Einzelsitzung und Multisitzung |
| Desktopanzeigename | Der veröffentlichte Name der Maschine, die ursprünglich zum Starten der Sitzung verwendet wurde. Dieser Name wird in der Citrix Workspace-App oder in StoreFront angezeigt. | Nur Einzelsitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| | **Hinweis:** Um die Anzeige eines Desktops zu ändern, benötigen Sie die Berechtigung **Maschinenupdate ausführen**, da das Ändern des Anzeigenamens eine Aktualisierung der Maschineneigenschaft mit sich bringt. | |
| Desktopbedingungen | Die Liste der ausstehenden Desktopbedingungen für die Maschine. Mögliche Werte: Unknown, CPU, ICALatency und UPMLogonTime. | Einzelsitzung und Multisitzung |
| Zuteilungstyp | Der Zuteilungstyp der Maschine: **Permanent**, wenn sie einem Benutzer dauerhaft zugeteilt ist. **Zufällig**, wenn zufällig zugeteilt. | Einzelsitzung und Multisitzung |
| Wartungsmodus | Zeigt an, ob sich die Maschine im Wartungsmodus befindet. | Einzelsitzung und Multisitzung |
| Windows-Verbindungseinstellung | Von Windows gemeldeter Anmeldemodus. Mögliche Werte: LogonEnabled, Draining, DrainingUntilRestart und LogonDisabled. | Nur Multisitzung |
| Ist zugewiesen | Gibt an, ob einem Benutzer oder einem Client ein dedizierter Desktop zugewiesen wurde (Name/Adresse). Benutzer können explizit oder durch Zuweisung bei der ersten Verwendung der Maschine zugewiesen werden. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Ist physisch | Zeigt an, ob es sich bei der Maschine um eine physische Maschine handelt. `True` gibt an, dass es sich um eine physische Maschine ohne Energieverwaltung durch DaaS handelt. `False` gibt an, dass dies nicht der Fall ist. | Einzelsitzung und Multisitzung |
| Provisioningtyp | Wie die Maschine bereitgestellt wurde. Mögliche Werte Manuell: Wird nicht mit PVS oder MCS bereitgestellt. PVS: Mit PVS bereitgestellt (physische, Blade- und virtuelle Maschinen) MCS: Mit MCS bereitgestellt (nur VMs) | Einzelsitzung und Multisitzung |
| Geplanter Neustart | Der Status aller geplanten Neustartvorgänge für die Maschine. Mögliche Werte Keiner: Es ist kein Neustart geplant. Ausstehend: Wartet auf den Neustart, kann aber verwendet werden. Draining: Wartet auf den Neustart und ist für neue Sitzungen nicht verfügbar. Wiederverbindungen zu bestehenden Verbindungen sind jedoch weiterhin zulässig. In Bearbeitung: Es wird gerade ein geplanter Neustart durchgeführt. Natürlich: Natürlicher Neustart ist im Gange. Die Maschine wartet auf einen Neustart. | Einzelsitzung und Multisitzung |
| Zone | Der Name der Zone, in der sich die Maschine befindet. | Einzelsitzung und Multisitzung |
| Status | Der Gesamtstatus der mit der Maschine verbundenen Desktops, der aus verschiedenen spezifischen Zuständen wie Sitzungsstatus, Registrierungszustand und Energiezustand abgeleitet wird. Mögliche Status: Aus, Nicht registriert, Verfügbar, Getrennt, InUse und In Vorbereitung. | Einzelsitzung und Multisitzung |
| Tags | Die Liste der Tags, die der Maschine zugeordnet sind. | Einzelsitzung und Multisitzung |
| VDA-Upgrade | Der Maschinenstatus für VDA-Paket-Upgrade-Aktionen. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| | Mögliche Werte: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate und Unknown. | |
| Anhalten-fähig | Zeigt an, ob die Maschine Stromversorgungsaktionen unterstützt (Anhalten und Fortfahren). | Einzelsitzung und Multisitzung |
| Lastindex | Der aktuelle Lastindex. Weitere Informationen finden Sie unter Weitere Informationen. | Nur Multisitzung |
| Drainingzustand | Zeigt an, ob sich die Maschine im Draining befindet und heruntergefahren wird, nachdem alle ihre Sitzungen beendet sind. True wird nur für energieverwaltete Maschinen mit mehreren Sitzungen angezeigt.<br>**Hinweis:** Die Maschine wird nicht heruntergefahren, wenn sie sich im Wartungsmodus befindet. Sie wird erst heruntergefahren, wenn der Wartungsmodus ausgeschaltet ist. | Nur Multisitzung |

**Maschinendetails**

Spalten in der Kategorie **Maschinendetails**.

| **Spalte** | **Beschreibung** | **Gilt für** |
| --- | --- | --- |
| Agentversion | Die Version von Citrix Virtual Delivery Agent (VDA), die auf der Maschine installiert ist. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| IP-Adresse | Die IP-Adresse der Maschine. | Einzelsitzung und Multisitzung |
| Ist zugewiesen | Gibt an, ob einem Benutzer oder einem Client ein dedizierter Desktop zugewiesen wurde (Name/Adresse). Benutzer können explizit oder durch Zuweisung bei der ersten Verwendung der Maschine zugewiesen werden. | Einzelsitzung und Multisitzung |
| Betriebssystemtyp | Der Typ des Betriebssystems, das auf der Maschine ausgeführt wird. | Nur Einzelsitzung |

**Anwendungen**

Spalten in der Kategorie **Anwendungen**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Anwendung wird verwendet | Die Liste der auf der Maschine verwendeten Anwendungen (als Browsernamen angezeigt). | Einzelsitzung und Multisitzung |
| Veröffentlichte Anwendungen | Die Liste der von der Maschine veröffentlichten Anwendungen (als Browsernamen angezeigt). | Einzelsitzung und Multisitzung |

**Verbindungen**

Spalten in der Kategorie **Verbindungen**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Client (IP) | Die IP-Adresse des Clients, der mit der Maschine verbunden ist. | Nur Einzelsitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Client | Der Hostname des Clients, der mit der Maschine verbunden ist. | Nur Einzelsitzung |
| Plug-In-Version | Die Version der Citrix Workspace-App auf dem verbundenen Client. | Nur Einzelsitzung |
| Verbunden durch | Der Hostname der eingehenden Verbindung, in der Regel ein Gateway, Router oder Client. | Nur Einzelsitzung |
| Verbunden durch (IP) | Die IP-Adresse der eingehenden Verbindung, in der Regel ein Gateway, Router oder Client. | Nur Einzelsitzung |
| Verbindungstyp | Das für die Sitzung verwendete Protokoll. Mögliche Werte: HDX, RDP und Console. Hinweis: Das Feld bleibt für Konsolensitzungen auf XenDesktop 5 VDAs leer. | Nur Einzelsitzung |
| Uhrzeit der letzten Verbindung (UTC) | Die Uhrzeit des letzten erkannten Verbindungsversuchs, der entweder fehlgeschlagen oder erfolgreich war. | Einzelsitzung und Multisitzung |
| Letzter Verbindungsbenutzer | Der SAM-Name (in der Form “DOMAIN\user”) des Benutzers, der zuletzt versucht hat, eine Verbindung mit der Maschine herzustellen. Wenn der SAM-Name nicht verfügbar ist, wird die SID verwendet. | Einzelsitzung und Multisitzung |
| Secure ICA aktiv | Gibt an, ob SecureICA in der aktuellen Sitzung aktiv ist. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |

### Hosting

Spalten in der Kategorie **Hosting**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| VM | Der vom Hypervisor verwendete Anzeigename einer gehosteten Maschine, auf der die Sitzung ausgeführt wird. Er stimmt nicht unbedingt mit dem DNS- oder AD-Namen der Maschine überein. | Einzelsitzung und Multisitzung |
| Hostingservername | Der DNS-Name des Hypervisors, der die Maschine hostet, sofern sie verwaltet wird. | Einzelsitzung und Multisitzung |
| Verbindung | Der Name der Hostverbindung, die der Maschine zugewiesen ist, die die Sitzung hostet. | Einzelsitzung und Multisitzung |
| Ausstehendes Update | Gibt an, ob das VM-Image für eine gehostete Maschine veraltet ist und beim nächsten Neustart der Maschine auf ein neues Image aktualisiert werden muss. | Einzelsitzung und Multisitzung |
| Benutzeränderungspersistenz | Wie Benutzeränderungen behandelt werden, wobei angegeben wird, ob die Änderungen persistent sind<br>On Local: Persistent.<br>Benutzeränderungen werden lokal gespeichert.<br>Virtuelle Maschine: Nicht persistent.<br>Benutzeränderungen werden beim Abmelden verworfen. | Einzelsitzung und Multisitzung |
| Ausstehende Energieaktion | Zeigt an, ob Energieaktionen für die Maschine ausstehen. | Einzelsitzung und Multisitzung |
| Energiezustand | Der Energiezustand der Maschine. Mögliche Werte: Nicht verwaltet, Unbekannt, Nicht verfügbar, Aus, Ein, Angehalten, Wird eingeschaltet, Wird ausgeschaltet, Wird angehalten und Wird fortgesetzt. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Wird nach Verwendung heruntergefahren | Gilt nur für Maschinen mit Energieverwaltung und Einzelsitzung. Zeigt an, ob die Maschine unsauber ist und heruntergefahren wird, wenn alle Sitzungen beendet sind. **Hinweis:** Die Maschine wird nicht heruntergefahren, wenn sie sich im Wartungsmodus befindet. Sie wird erst heruntergefahren, nachdem sie den Wartungsmodus verlassen hat. | Nur Einzelsitzung |

**Registrierung**

Spalten in der Kategorie **Registrierung**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Letzter Registrierungsfehler | Der Grund für die letzte Abmeldung der Maschine beim Broker. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| | Mögliche Werte sind: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError und BrokerRegistrationLimitReached. | |
| Zeitpunkt des letzten Registrierungsfehlers (UTC) | Der Zeitpunkt der letzten Registrierungsaufhebung der Maschine. | Einzelsitzung und Multisitzung |
| Registrierungszustand | Der Registrierungszustand der Maschine. Mögliche Werte: Unregistered, Initializing, Registered und AgentError. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Fehlerzustand | Der zusammenfassende Status aller aktuellen Fehlerzustände der Maschine. Mögliche Werte Keiner: Kein Fehler. Die Maschine ist fehlerfrei. FailedToStart: Der letzte Einschaltvorgang für die Maschine ist fehlgeschlagen. StuckOnBoot: Die Maschine konnte nach dem Einschalten nicht gestartet werden. Nicht registriert. Die Maschine konnte nicht innerhalb des erwarteten Zeitraums registriert werden oder ihre Registrierung wurde abgelehnt. Max. Kapazität. Die Maschine meldet sich selbst mit maximaler Kapazität. | Einzelsitzung und Multisitzung |

**Sitzungsdetails**

Spalten in der Kategorie **Sitzungsdetails**.

| **Spalte** | **Beschreibung** | **Gilt für** |
| --- | --- | --- |
| Gestartet über | Der Hostname des StoreFront-Servers, der zum Starten der aktuellen Brokersitzung verwendet wird. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |
| Gestartet über (IP) | Die IP-Adresse des StoreFront-Servers, der zum Starten der aktuellen Brokersitzung verwendet wird. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |
| Uhrzeit der Sitzungsänderung (UTC) | Die Uhrzeit der letzten Statusänderung der aktuellen Sitzung. | Nur Einzelsitzung |
| SmartAccess-Filter | Smart Access-Tags für die aktuelle Sitzung. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |

### Sitzung

Spalten in der Kategorie **Sitzung**.

| Spalte | Beschreibung | Gilt für |
|---|---|---|
| Sitzungszustand | Der Status der aktuellen Sitzung. Mögliche Werte: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession und Unknown. | Nur Einzelsitzung |
| Aktueller Benutzer | Der Name des Benutzers der aktuellen Sitzung (in der Form “DOMAIN\user”). | Nur Einzelsitzung |
| Startzeit (UTC) | Die Startzeit der aktuellen Sitzung. | Nur Einzelsitzung |
| Sitzungsanzahl | Die Anzahl der Sitzungen auf der Maschine. | Nur Multisitzung |

## Sitzungsaktionen und Spalten

June 12, 2024

In diesem Artikel werden Maschinenaktionen und Spalten mit Beschreibungen als Referenz aufgeführt.

### Aktionen

Sehen Sie sich die Aktionen an, die Sie an Sitzungen ausführen können, und deren Beschreibungen.

| Aktion | Beschreibung | Gilt für Sitzungen auf |
|---|---|---|
| Abmelden | Einen Benutzer von einer Sitzung abmelden. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |

| Aktion | Beschreibung | Gilt für Sitzungen auf |
|---|---|---|
| Nachricht senden | Eine Nachricht an den Benutzer einer Sitzung senden. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Maschinen anzeigen | Hostingmaschine für eine Sitzung anzeigen. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Trennen | Sitzung trennen. Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit dem DaaS. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Maschine herunterfahren | Die mit einer Sitzung verbundene Maschine herunterfahren. | Maschinen mit Einzelsitzungs-OS |
| Maschine neu starten | Neustart einer Maschine durchführen, die einer Sitzung zugeteilt ist. | Maschinen mit Einzelsitzungs-OS |

### Spalten

Sitzungsspalten und ihre Beschreibungen anzeigen.

| Spalte | Beschreibung |
|---|---|
| Aktueller Benutzer | Der Name des Benutzers; der Benutzerprinzipalname (User Principal Name, UPN). |
| Name | Der DNS-Hostname der Maschine, die die Sitzung hostet. |
| Bereitstellungsgruppe | Der Name der Bereitstellungsgruppe, die die Hostmaschine der Sitzung enthält. |
| Maschinenkatalog | Der Name des Maschinenkatalogs, der die Hostmaschine der Sitzung enthält. |

| Spalte | Beschreibung |
| --- | --- |
| Agentversion | Die Version des Citrix Virtual Delivery Agent (VDA), die auf der Maschine installiert ist, auf der die Sitzung gehostet wird. |
| Anwendung wird verwendet | Die Liste der in der Sitzung verwendeten Anwendungen, identifiziert durch ihre Administratornamen. |
| Autonom vermittelt | Ob es sich um eine HDX-Sitzung handelt, die über eine direkte Verbindung ohne Vermittlung eingerichtet wurde. |
| Brokerzeit (UTC) | Der Zeitpunkt, zu dem die Sitzung vermittelt wurde. |
| Vermittlungsbenutzername | Der Name des Vermittlungsbenutzers. |
| Client (IP) | Die IP-Adresse des Clients, der mit der Sitzung verbunden ist. |
| Client | Der Hostname des Clients, der mit der Sitzung verbunden ist. |
| Plug-In-Version | Die Version der Citrix Workspace-App, die auf dem mit der Sitzung verbundenen Client ausgeführt wird. |
| Verbunden durch | Der Hostname der eingehenden Verbindungen, in der Regel ein Gateway, Router oder Client. |
| Verbunden durch (IP) | Die IP-Adresse der eingehenden Verbindung, in der Regel ein Gateway, Router oder Client. |
| Zuteilungstyp | Ob die Sitzung geteilt oder dediziert ist. |
| Ausgeblendet | Ob die Sitzung vor dem Benutzer verborgen ist und nicht erneut verbunden werden soll. |
| VM | Der vom Hypervisor verwendete Anzeigename der VM, die die Sitzung hostet. Er stimmt nicht unbedingt mit dem DNS- oder AD-Namen der Maschine überein. |
| Hostingservername | Der DNS-Name des Hypervisors, der die Hostmaschine der Sitzung hostet. |
| Verbindung | Der Name der Hostverbindung, die der Maschine zugewiesen ist, die die Sitzung hostet. |

| Spalte | Beschreibung |
| --- | --- |
| Ausstehendes Update | Ob das VM-Image für eine gehostete Maschine veraltet ist und beim nächsten Neustart der Maschine auf ein neues Image aktualisiert werden muss. |
| Wartungsmodus | Ob sich die Maschine, die die Sitzung hostet, im Wartungsmodus befindet. |
| IP-Adresse | Die IP-Adresse der Maschine, die die Sitzung hostet. |
| Ist physisch | Ob es sich bei der Maschine, die die Sitzung hostet, um eine physische Maschine handelt. `True` gibt an, dass es sich um eine physische Maschine ohne Energieverwaltung durch DaaS handelt. `False` gibt an, dass dies nicht der Fall ist. |
| Gestartet über | Der Hostname des StoreFront-Servers, der zum Starten der Sitzung verwendet wird. Leer, wenn die Sitzung über Workspace gestartet wurde. |
| Gestartet über (IP) | Die IP-Adresse des StoreFront-Servers, der zum Starten der Sitzung verwendet wurde. Leer, wenn die Sitzung über Workspace gestartet wurde. |
| Betriebssystemtyp | Die Identifikationszeichenfolge des Betriebssystems, das die Sitzung hostet. |
| Benutzeränderungspersistenz | Wie Benutzeränderungen behandelt werden, wobei angegeben wird, ob die Änderungen persistent sind<br>OnLocal: Persistent. Benutzeränderungen werden lokal gespeichert.<br>Verworfen: Nicht persistent. Benutzeränderungen werden verworfen. |
| Verbindungstyp | Das für die Sitzung verwendete Protokoll, z. B. HDX, RDP oder Console. **Hinweis:** Das Feld ist leer für Konsolensitzungen auf XenDesktop 5 VDAs. |
| Provisioningtyp | Wie die Maschine, die die Sitzung hostet, bereitgestellt wurde<br>Manuell: Wird nicht mit PVS oder MCS bereitgestellt.<br>PVS: Wird von PVS bereitgestellt (physische Maschinen, Blade-Maschinen und virtuelle Maschinen).<br>MCS: Von MCS bereitgestellt (nur VMs). |
| Secure ICA aktiv | Ob SecureICA in der Sitzung aktiv ist. |

| Spalte | Beschreibung |
| --- | --- |
| Sitzungszustand | Der Status der Sitzung. Mögliche Werte: Verbunden, Aktiv oder Getrennt. Andere Zustände können für Sitzungen auf Maschinen mit Funktionsebenen vor L7 auftreten, z. B. PreparingSession, Reconnecting, NonBrokeredSession, Other und Unknown. |
| Uhrzeit der Sitzungsänderung | Die Uhrzeit der letzten Statusänderung für die Sitzung. |
| Anwendungszustand | Der Status der Anwendungen in der Sitzung. Mögliche Werte: PreLogon, PreLaunched, Active, Desktop, Lingering und NoApps. |
| Sitzungsunterstützung | Ob die Maschine, die die Sitzung hostet, mehrere oder einzelne Sitzungen unterstützt. |
| Zone | Name der Zone, in der sich die Maschine befindet, die die Sitzung hostet. |
| SmartAccess-Filter | Smart Access-Tags für die Sitzung. |
| Startzeit (UTC) | Wann die Sitzung gestartet wurde. |
| Status | Der zusammenfassende Status der Maschine. Mögliche Werte: Unregistered, Disconnected oder InUse. |
| Zeit in Zustand (UTC) | Wie lange sich die Sitzung in ihrem aktuellen Zustand befindet. |
| Delivery Controller | Der DNS-Hostname des Controllers, bei dem die Hostmaschine der Sitzung registriert ist. |
| Anzeigename für Benutzer | Der vollständige Name des Benutzers. |
| Desktopanzeigename | Der veröffentlichte Name der Maschine, die ursprünglich zum Starten der Sitzung verwendet wurde. Dieser Name wird in der Citrix Workspace-App oder in StoreFront angezeigt. Bei Anwendungssitzungen ist dies der Name der ersten Anwendung, die in der Sitzung gestartet wurde, auch wenn diese Anwendung inzwischen beendet wurde. Der Name bleibt unverändert, auch wenn die Ressource später umbenannt oder entfernt wird. |

# Sicherheitsschlüssel verwalten

April 14, 2023

> **Hinweis:**
>
> - Sie müssen dieses Feature in Kombination mit StoreFront 1912 LTSR CU2 oder höher verwenden.
> - Secure XML wird nur von Citrix ADC und Citrix Gateway ab Version 12.1 unterstützt.

Mit diesem Feature können nur genehmigte StoreFront- und Citrix Gateway-Maschinen mit Citrix Delivery Controllern kommunizieren. Nachdem Sie das Feature aktiviert haben, werden alle Anforderungen ohne Schlüssel blockiert. Verwenden Sie diese Funktion, um eine zusätzliche Sicherheitsebene zum Schutz vor Angriffen aus dem internen Netzwerk hinzuzufügen.

Ein allgemeiner Workflow zur Verwendung des Features ist folgender:

1. Sicherheitsschlüsseleinstellungen in der Schnittstelle für die vollständige Konfiguration anzeigen. (Verwenden Sie das Remote PowerShell SDK.)
2. Einstellungen für die Bereitstellung konfigurieren. (Verwenden Sie die Schnittstelle für die vollständige Konfiguration oder das Remote PowerShell SDK.)
3. Einstellungen in StoreFront konfigurieren. (Verwenden Sie PowerShell.)
4. Einstellungen in Citrix ADC konfigurieren.

## Sicherheitsschlüsseleinstellungen in der Schnittstelle für die vollständige Konfiguration anzeigen

Standardmäßig sind die Einstellungen für Sicherheitsschlüssel in der Schnittstelle für die vollständige Konfiguration ausgeblendet. Verwenden Sie das Remote PowerShell-SDK, um sie in dieser Schnittstelle anzuzeigen. Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.

Hier ist eine detaillierte Schrittfolge:

1. Führen Sie das Remote PowerShell SDK aus.
2. Führen Sie in einem Befehlsfenster die folgenden Befehle aus:
   - `Add-PSSnapIn Citrix*`. Mit diesem Befehl werden die Citrix Snap-Ins hinzugefügt.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

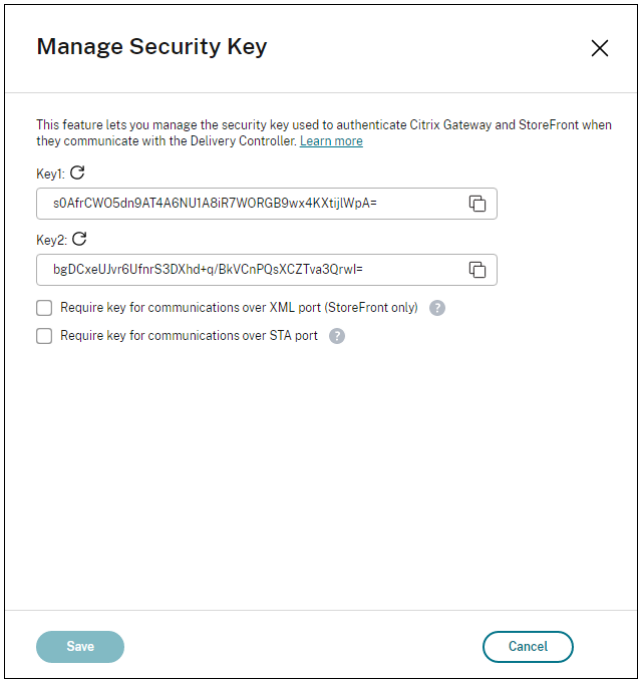
 

## Einstellungen für die Bereitstellung konfigurieren

Sie können die Einstellungen für Ihre Bereitstellung mithilfe der Schnittstelle für die vollständige Konfiguration oder mit PowerShell konfigurieren.

### Verwenden der Schnittstelle für die vollständige Konfiguration

Gehen Sie nach dem Aktivieren des Features zu **Vollständige Konfiguration> Einstellungen > Sicherheitsschlüssel verwalten** und klicken Sie auf **Bearbeiten**. Das Blatt **Sicherheitsschlüssel verwalten** wird angezeigt. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen und das Blatt zu schließen.




> **Wichtig:**
>
> - Es stehen zwei Schlüssel zur Verfügung. Sie können für die Kommunikation über den XML- und den STA-Port denselben oder verschiedene Schlüssel verwenden. Wir empfehlen, dass Sie jeweils nur einen Schlüssel verwenden. Der nicht verwendete Schlüssel dient nur zur Schlüsselrotation.
> - Klicken Sie nicht auf das Aktualisierungssymbol, um den bereits verwendeten Schlüssel zu aktualisieren. Dies führt zu einer Dienstunterbrechung.

Klicken Sie auf das Aktualisierungssymbol, um neue Schlüssel zu generieren

**Schlüssel für Kommunikation über XML-Port erforderlich (nur StoreFront).** Ist diese Option aktiviert, dann ist ein Schlüssel erforderlich, um die Kommunikation über den XML-Port zu authen-

tifizieren. StoreFront kommuniziert über diesen Port mit Citrix Cloud. Informationen zum Ändern des XML-Ports finden Sie im Knowledge Center-Artikel CTX127945.

**Schlüssel für die Kommunikation über den STA-Port erforderlich**. Ist diese Option aktiviert, dann ist ein Schlüssel erforderlich, um die Kommunikation über den STA-Port zu authentifizieren. Citrix Gateway und StoreFront kommunizieren über diesen Port mit Citrix Cloud. Informationen zum Ändern des STA-Ports finden Sie im Knowledge Center-Artikel CTX101988.

Nachdem Sie die Änderungen übernommen haben, klicken Sie auf **Schließen**, um das Blatt **Sicherheitsschlüssel verwalten** zu schließen.

#### Remote PowerShell-SDK verwenden

Nachfolgend werden die den in der Schnittstelle für die vollständige Konfiguration ausgeführten Schritten entsprechenden PowerShell-Schritte aufgeführt.

1. Führen Sie das Remote PowerShell SDK aus.
2. Führen Sie in einem Befehlsfenster folgenden Befehl aus:
   - `Add-PSSnapIn Citrix*`
3. Führen Sie die folgenden Befehle aus, um einen Schlüssel zu generieren und Key1 einzurichten:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Führen Sie die folgenden Befehle aus, um einen Schlüssel zu generieren und Key2 einzurichten:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Führen Sie einen oder beide der folgenden Befehle aus, um die Verwendung eines Schlüssels bei der Authentifizierung der Kommunikationen zu aktivieren:
   - Zum Authentifizieren der Kommunikation über den XML-Port:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Zum Authentifizieren der Kommunikation über den STA-Port:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Befehlen.

### Konfigurieren von Einstellungen in StoreFront

Nach Abschluss der Einstellungen für Ihre Bereitstellung müssen Sie relevante Einstellungen in StoreFront mit PowerShell konfigurieren.

Führen Sie auf dem StoreFront-Server die folgenden PowerShell-Befehle aus:

- Um den Schlüssel für die Kommunikation über den XML-Port zu konfigurieren, verwenden Sie die Befehle `Get-STFStoreServie` und `Set-STFStoreService`. Beispiel:

  - ```
    PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80
     -TransportType HTTP -Servers <domain name1, domain name2> -
    XMLValidationEnabled $true -XMLValidationSecret <the key you
    generated in Studio>
    ```

- Um den Schlüssel für die Kommunikation über den STA-Port zu konfigurieren, verwenden Sie den Befehl `New-STFSecureTicketAuthority`. Beispiel:

  - ```
    PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL
    > -StaValidationEnabled $true -StavalidationSecret <the key
    you generated in Studio>
    ```

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Befehlen.

### Konfigurieren der Einstellungen in Citrix ADC

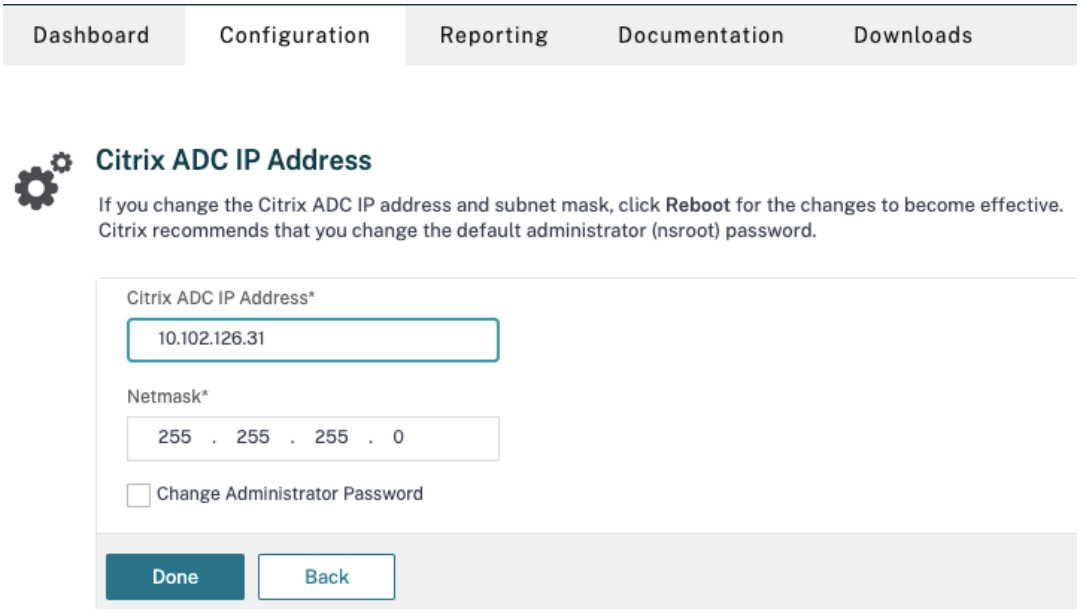
> **Hinweis:**
>
> Die Konfiguration dieses Features in Citrix ADC ist nur erforderlich, wenn Sie Citrix ADC als Gateway verwenden. Wenn Sie Citrix ADC verwenden, führen Sie die folgenden Schritte aus.

1. Vergewissern Sie sich, dass die erforderliche Konfiguration ausgeführt wurde:

   - Die folgenden IP-Adressen im Zusammenhang mit Citrix ADC wurden konfiguriert.

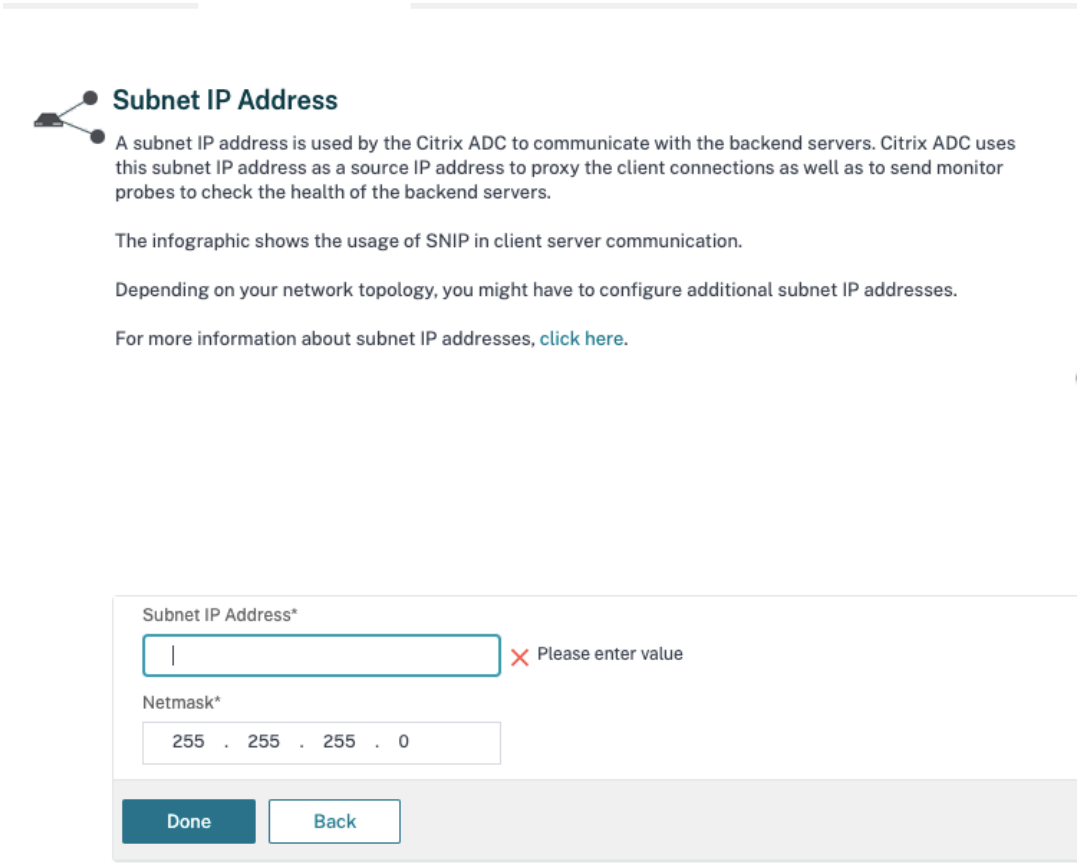
     - Citrix ADC Management-IP-Adresse (NSIP) für den Zugriff auf die Citrix ADC-Konsole. Weitere Informationen finden Sie unter Konfigurieren der NSIP-Adresse.



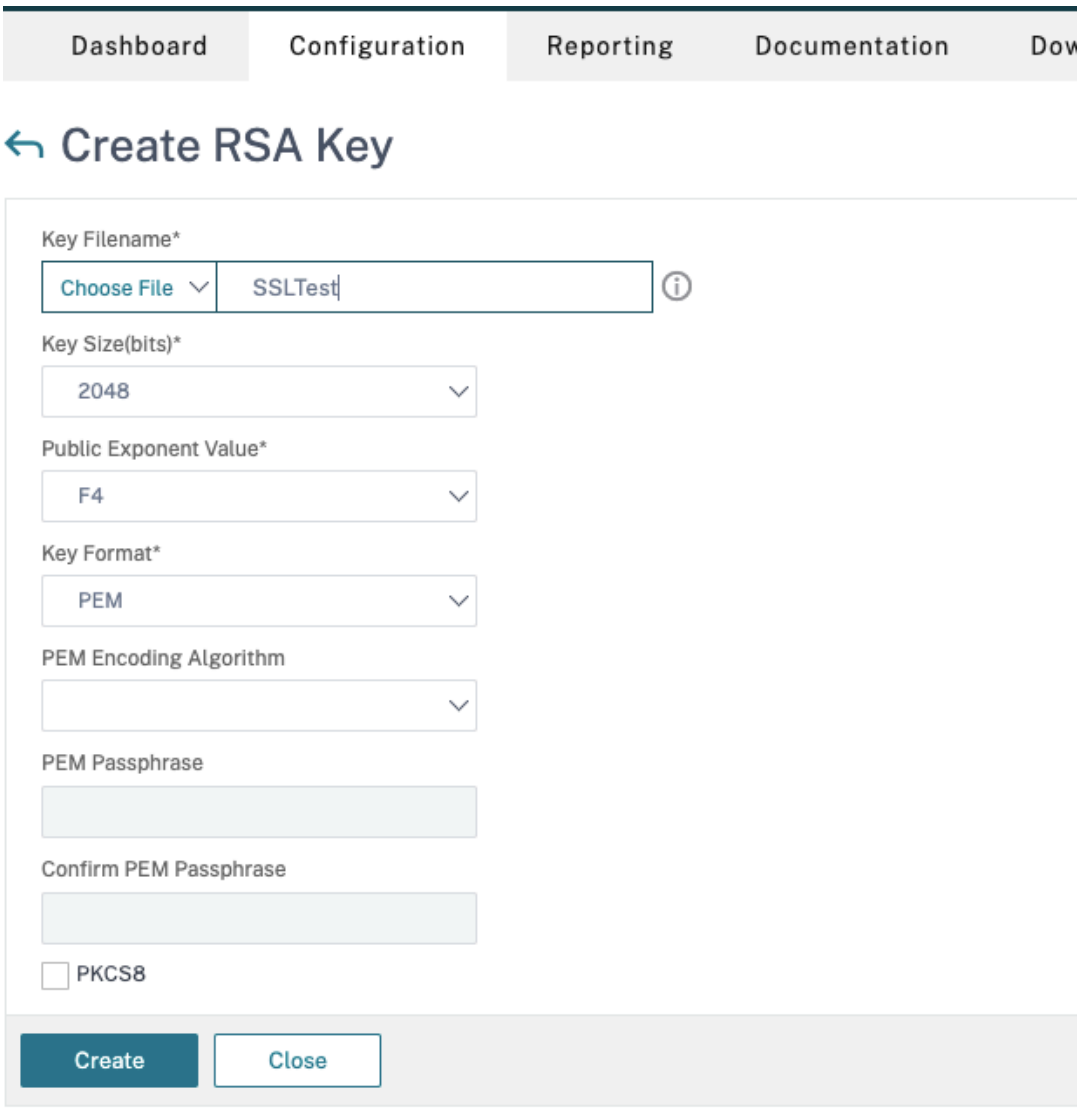

- Subnetz-IP-Adresse (SNIP) zur Kommunikation zwischen der Citrix ADC Appliance und den Back-End-Servern. Weitere Informationen finden Sie unter Konfigurieren von Subnetz-IP-Adressen.
- Virtuelle IP-Adresse von Citrix Gateway und des Load Balancers zur Anmeldung bei der ADC Appliance für den Sitzungsstart. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.



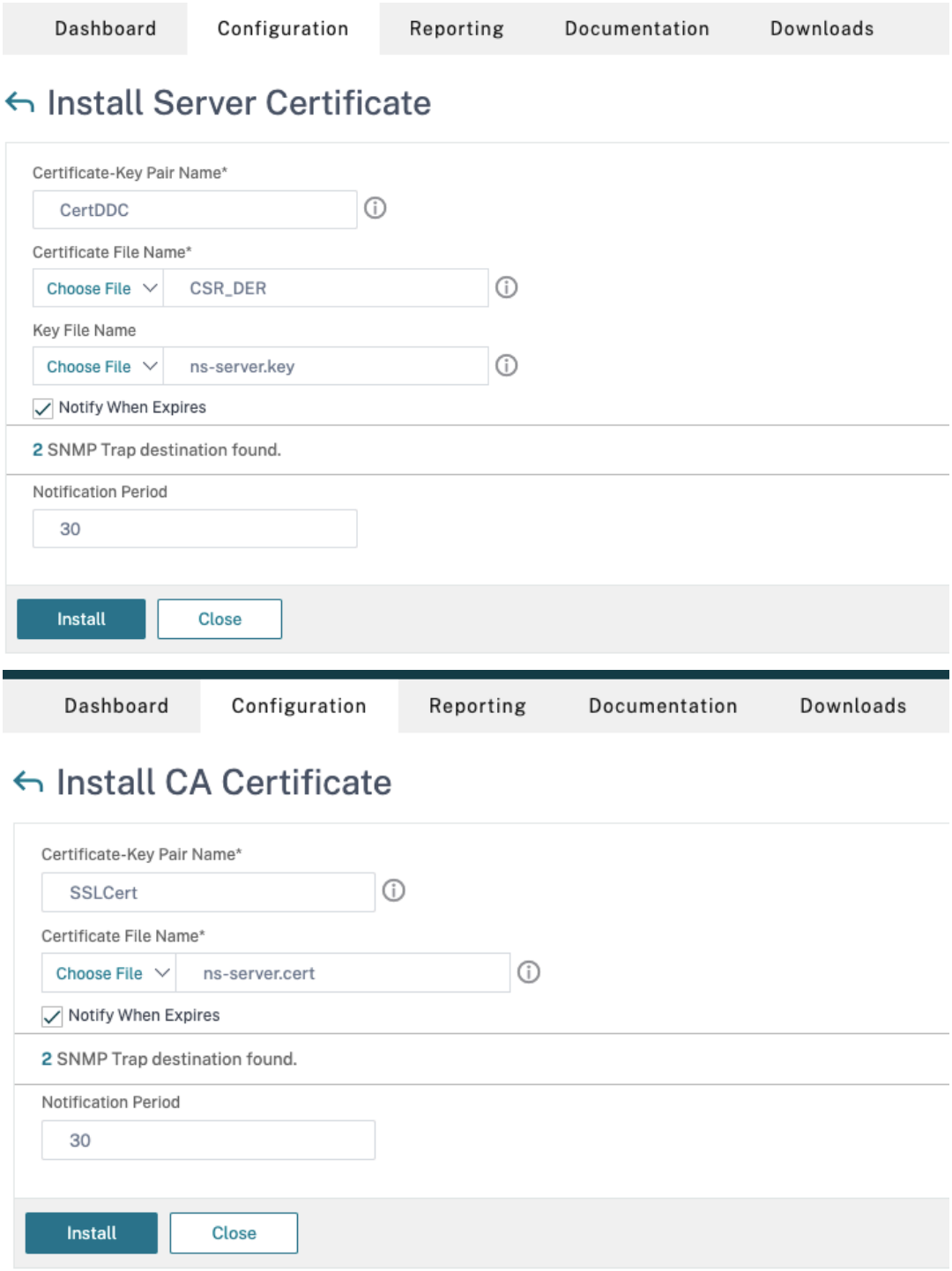

- Die erforderlichen Modi und Features in der Citrix ADC Appliance sind aktiviert.
  - Um die Modi zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Mode**.
  - Um die Features zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Basic Features**.
- Die Konfiguration für Zertifikate wurde ausgeführt.
  - Die Zertifikatsignieranforderung (CSR) wurde erstellt. Weitere Informationen finden Sie unter Erstellen eines Zertifikats.



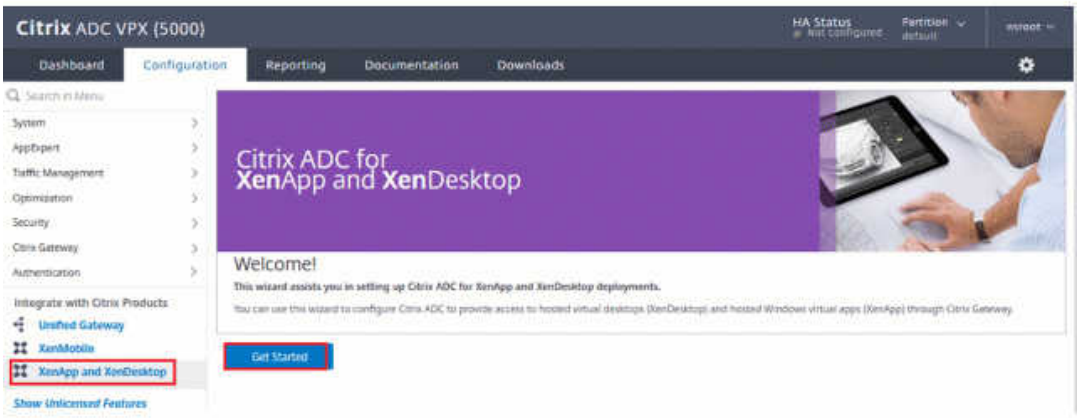

- Das Serverzertifikat, das ZS-Zertifikat und das Stammzertifikat wurden installiert. Weitere Informationen finden Sie unter Installieren, Links und Updates.



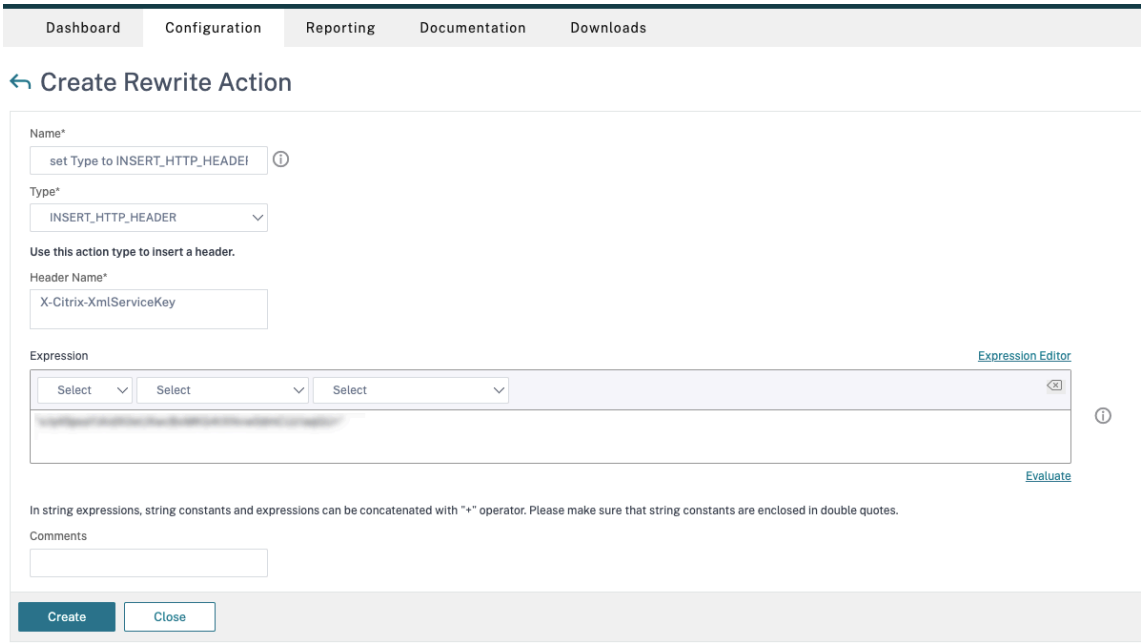

- Ein Citrix Gateway wurde für Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) erstellt. Testen Sie die Verbindung durch Klicken auf die Schaltfläche **Test STA Connectivity**, um sicherzustellen, dass die virtuellen Server online sind. Weitere Informationen finden Sie unter Einrichten von Citrix ADC für Citrix Virtual Apps and Desktops.




2. Fügen Sie eine Rewrite-Aktion hinzu. Weitere Informationen finden Sie unter Konfigurieren einer Rewrite-Aktion.

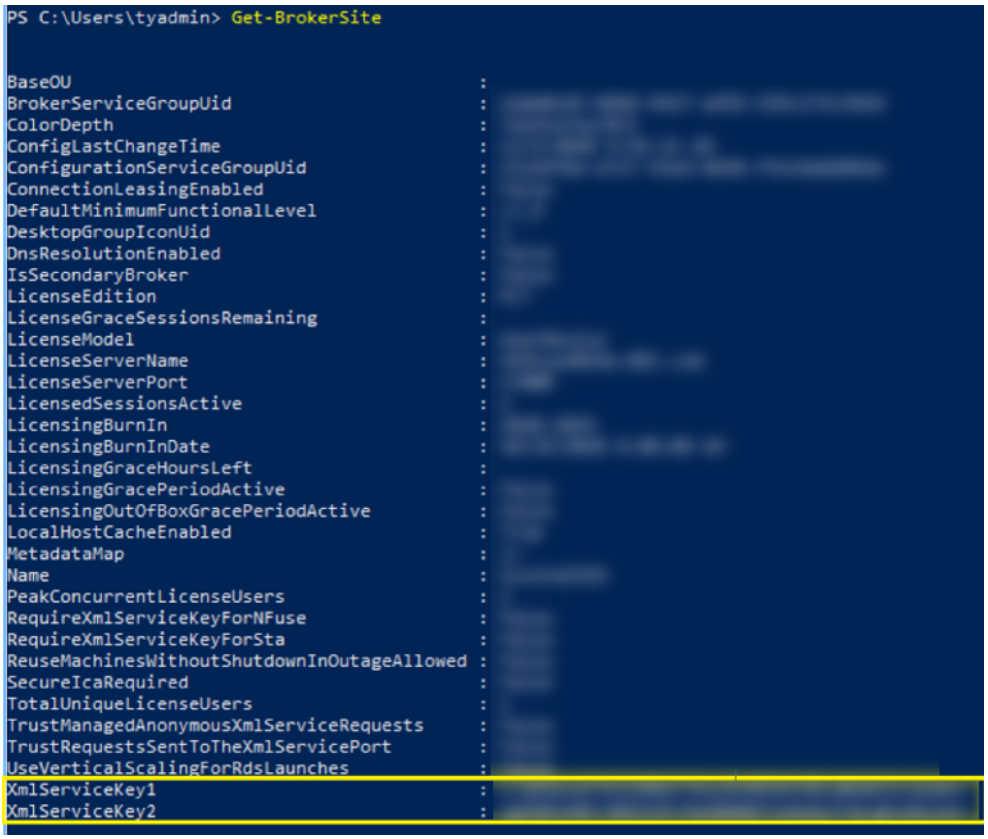
   a) Gehen Sie zu **AppExpert > Rewrite > Actions**.
   b) Klicken Sie auf **Hinzufügen**, um eine neue Rewrite-Aktion hinzuzufügen. Sie können die Aktion "set Type to INSERT_HTTP_HEADER"nennen.




   a) Wählen Sie unter **Type** die Option **INSERT_HTTP_HEADER**.
   b) Geben Sie im Feld **Header Name** "X-Citrix-XmlServiceKey"ein.
   c) Fügen Sie unter **Ausdruck** <XmlServiceKey1 value> mit Anführungszeichen hinzu.

Sie können den XmlServiceKey1-Wert aus der Desktop Delivery Controller-Konfiguration kopieren.

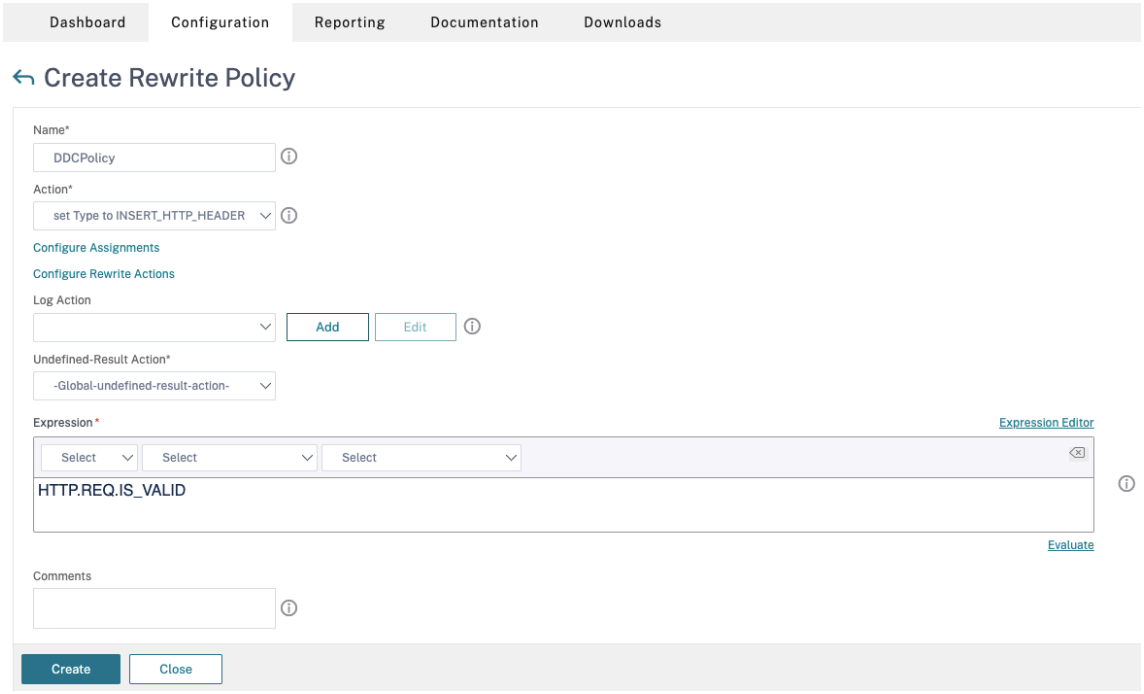



3. Fügen Sie eine Rewrite-Richtlinie hinzu. Weitere Informationen finden Sie unter Konfigurieren einer Rewrite-Richtlinie.

   a) Gehen Sie zu **AppExpert > Rewrite > Policies**.

   b) Klicken Sie auf **Add**, um eine neue Richtlinie hinzuzufügen.




a) Wählen Sie unter **Action** die im vorherigen Schritt erstellte Aktion aus.
b) Fügen Sie unter **Expression** “HTTP.REQ.IS_VALID”hinzu.
c) Klicken Sie auf **OK**.

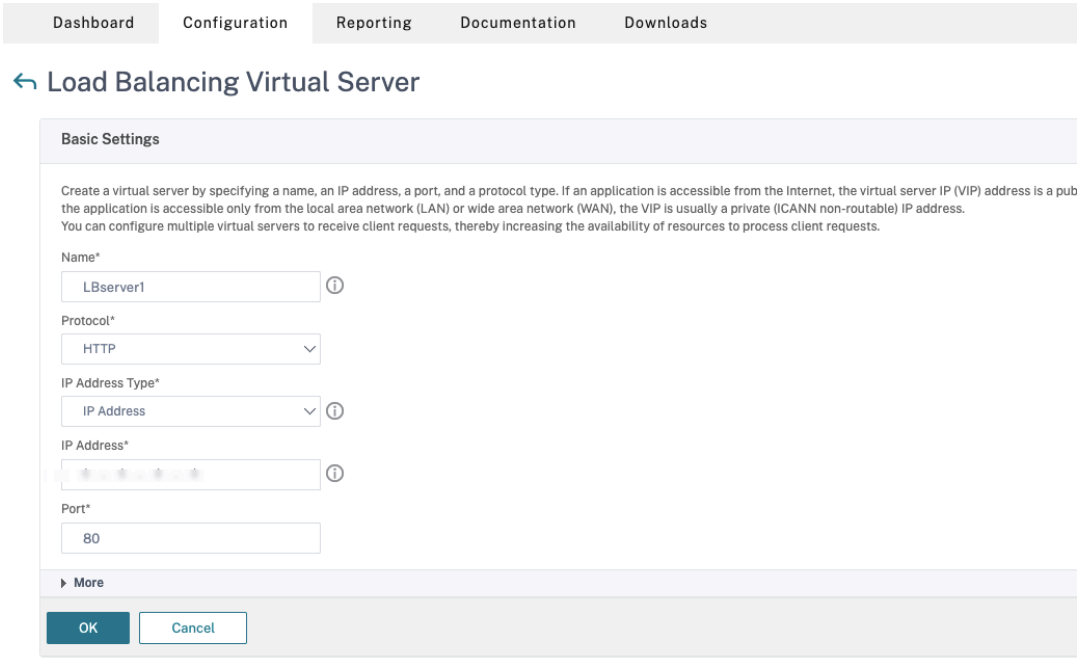
4. Richten Sie den Lastenausgleich ein. Sie müssen einen virtuellen Lastausgleichsserver pro STA-Server konfigurieren. Ansonsten können die Sitzungen nicht gestartet werden.

   Weitere Informationen finden Sie unter Einrichten des einfachen Lastenausgleichs.

   a) Erstellen Sie einen virtuellen Lastausgleichsserver.

      - Navigieren Sie zu **Traffic Management > Load Balancing > Servers**.
      - Klicken Sie auf der Seite **Virtual Servers** auf **Add**.

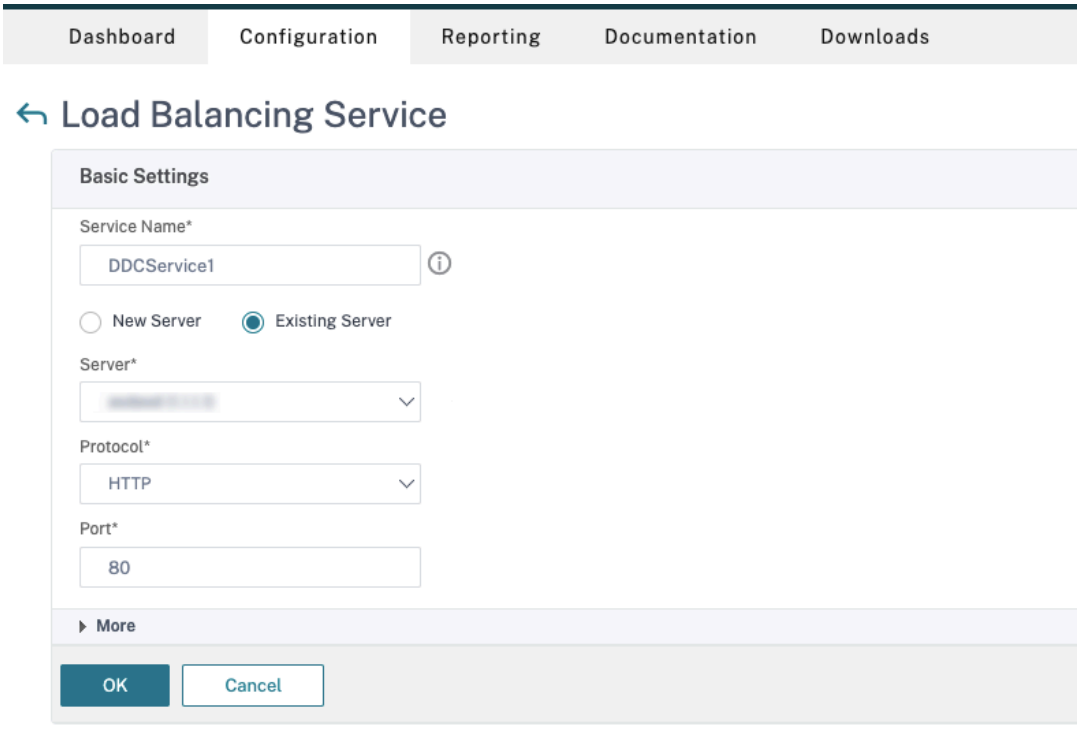
 




- Wählen Sie unter **Protocol** die Option **HTTP**.
- Geben Sie die IP-Adresse des virtuellen Lastausgleichsserver ein und wählen Sie für **Port** die Option **80**.
- Klicken Sie auf **OK**.

b) Erstellen Sie einen Lastausgleichsdienst.

- Navigieren Sie zu **Traffic Management > Load Balancing > Services**.

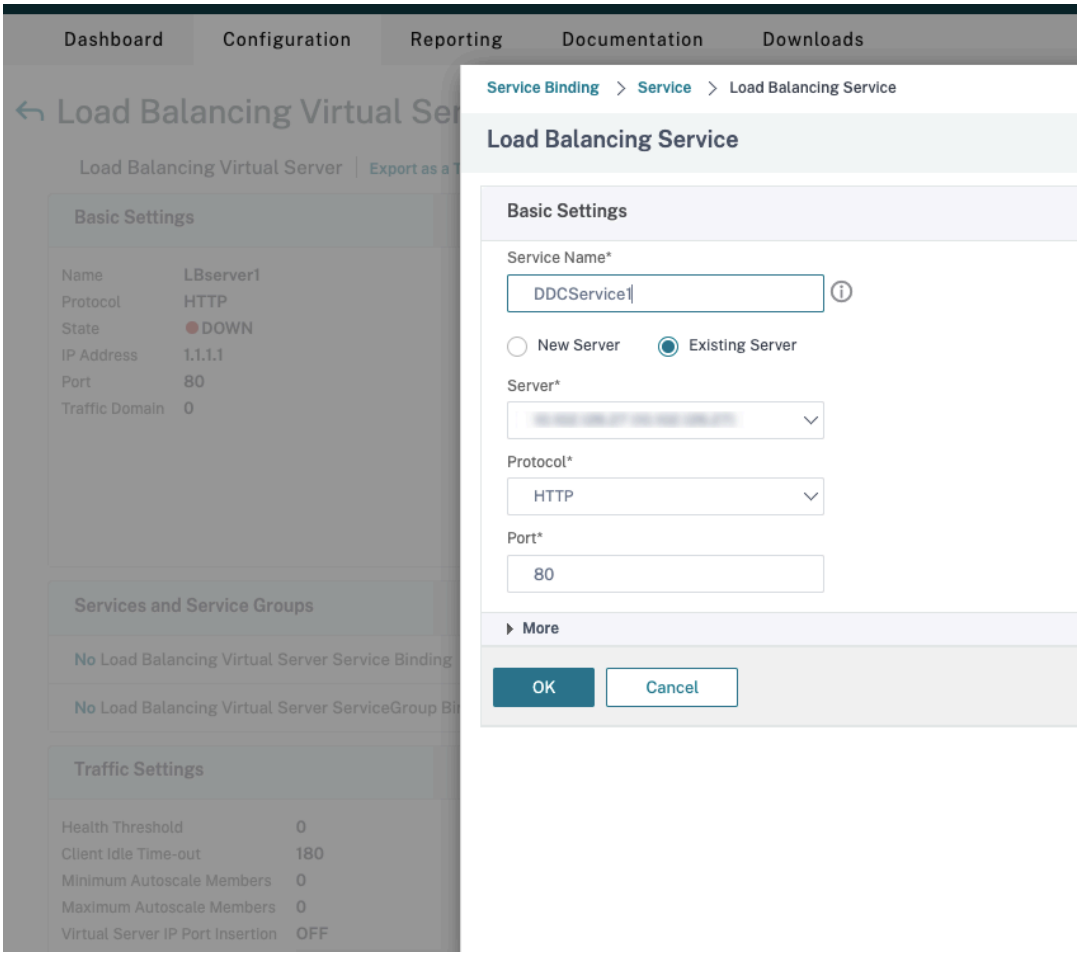


- Wählen Sie unter **Existing Server** den im vorherigen Schritt erstellten virtuellen Server aus.
- Wählen Sie für **Protocol** die Option **HTTP** und für **Port** die Option **80**.
- Klicken Sie auf **OK** und dann auf **Done**.

c) Binden Sie den Dienst an den virtuellen Server.

- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie in **Services and Service Groups** auf **No Load Balancing Virtual Server Service Group Binding**.

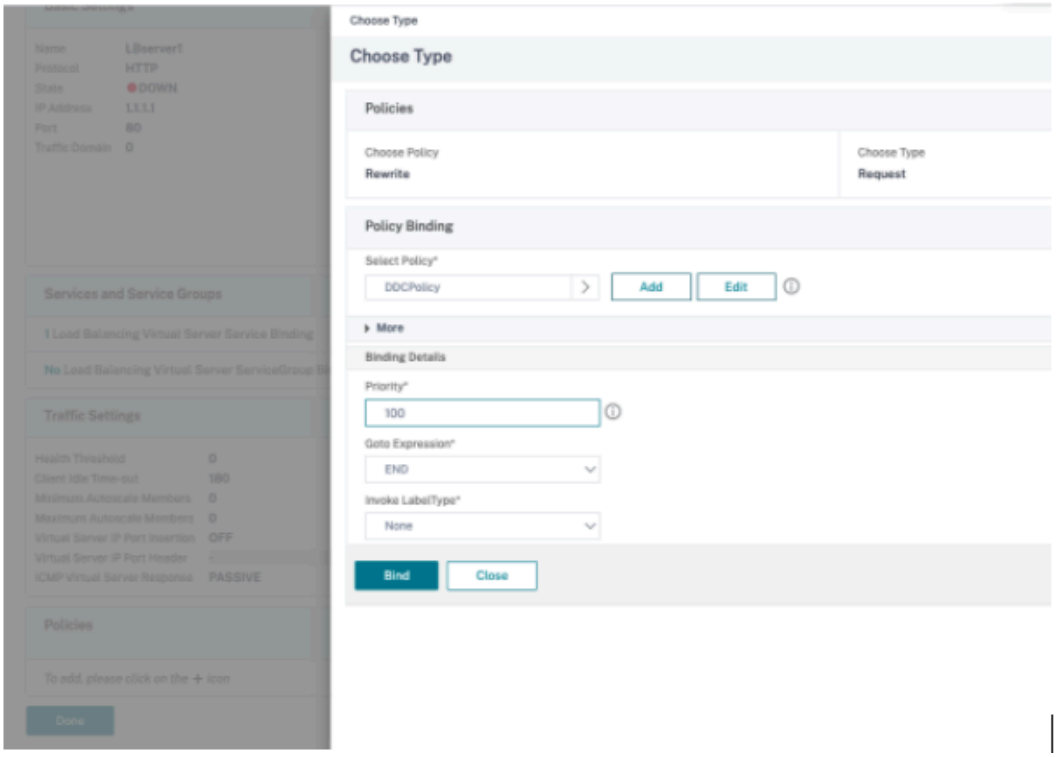



- Wählen Sie unter **Service Binding** das zuvor erstellte Citrix DaaS aus.
- Klicken Sie auf **Bind**.

d) Binden Sie die zuvor erstellte Rewrite-Richtlinie an den virtuellen Server.

- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie unter **Advanced Settings** auf **Policies** und im Bereich **Policies** auf **+**.

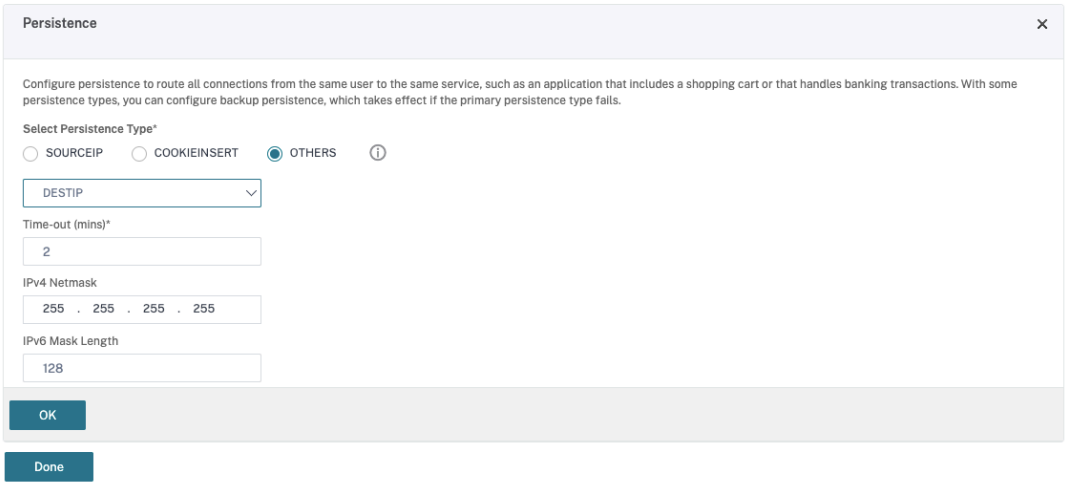
 




- Wählen Sie unter **Choose Policy** die Option **Rewrite** und für **Choose Type**, die Option **Request**.
- Klicken Sie auf **Weiter**.
- Wählen Sie unter **Select Policy** die zuvor erstellte Rewrite-Richtlinie aus.
- Klicken Sie auf **Bind**.
- Klicken Sie auf **Fertig**.

e) Legen Sie ggf. die Persistenz für den virtuellen Server fest.

- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie unter **Advanced Settings** auf **Persistence**.



- Wählen Sie als Persistenztyp **Others**.
- Wählen Sie **DESTIP**, um Persistenzsitzungen basierend auf der IP-Adresse des vom virtuellen Server ausgewählten Diensts (Ziel-IP-Adresse) zu erstellen
- Fügen Sie in **IPv4 Netmask** die Netzwerkmaske des DDC hinzu.
- Klicken Sie auf **OK**.

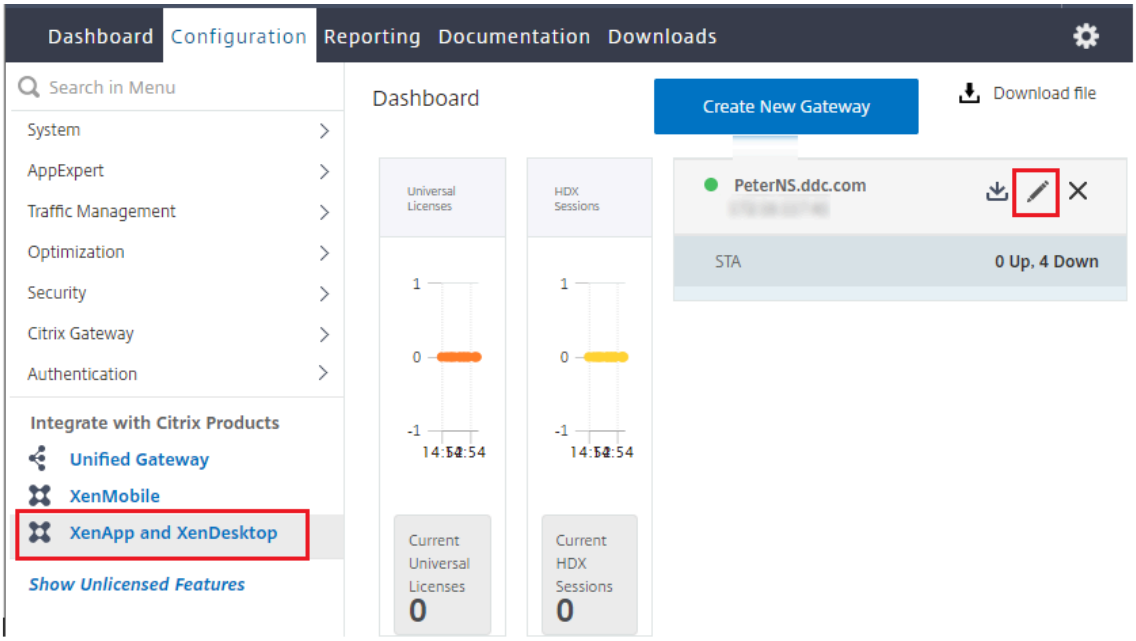
f) Wiederholen Sie diese Schritte für den anderen virtuellen Server.

**Konfigurationsänderungen bei bereits mit Citrix DaaS konfiguriertem Citrix ADC-Gerät**

Wenn das Citrix ADC-Gerät bereits mit Citrix DaaS konfiguriert ist, müssen Sie zur Verwendung von Secure XML die folgenden Konfigurationsänderungen vornehmen.

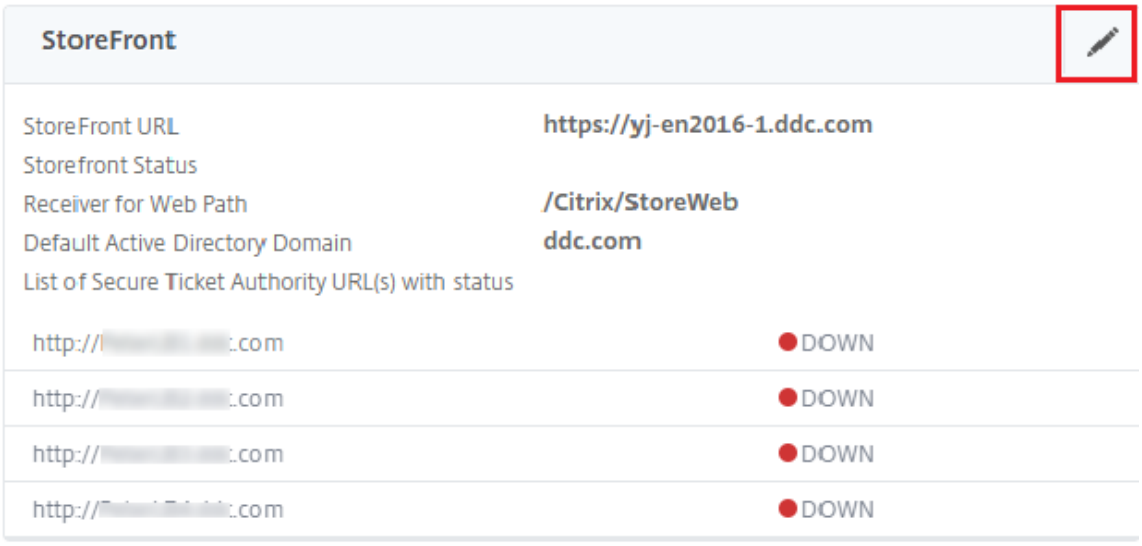
- Ändern Sie vor dem Start der Sitzung die **Secure Ticket Authority-URL** des Gateways, um die FQDNs der virtuellen Lastausgleichsserver zu verwenden.
- Stellen Sie sicher, dass der Parameter `TrustRequestsSentToTheXmlServicePort` auf "False"festgelegt ist. Standardmäßig ist der Parameter `TrustRequestsSentToTheXmlServicePort` auf "False"festgelegt. Wenn der Kunde jedoch Citrix ADC bereits für Citrix DaaS konfiguriert hat, ist `TrustRequestsSentToTheXmlServicePort` auf "True"festgelegt.

1. Gehen Sie in Citrix ADC zu **Configuration > Integrate with Citrix Products** und klicken Sie auf **XenApp and XenDesktop**.
2. Wählen Sie die Gateway-Instanz aus und klicken Sie auf das Bearbeitungssymbol




3. Klicken Sie im StoreFront-Bereich auf das Bearbeitungssymbol.

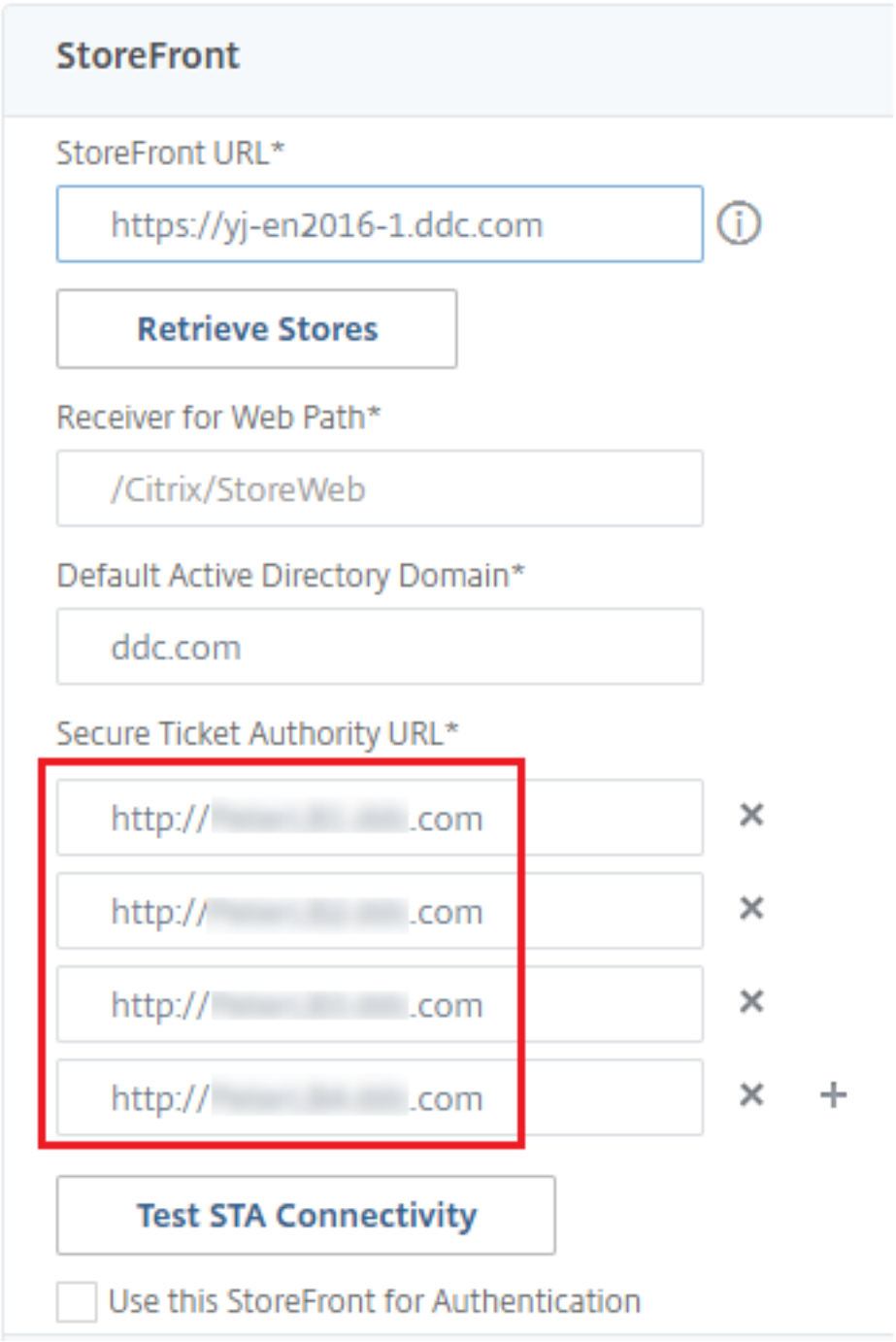
 




4. Fügen Sie die **Secure Ticket Authority-URL**hinzu.

   - Wenn Secure XML aktiviert ist, muss die STA-URL die URL des Lastausgleichsdiensts sein.
   - Wenn Secure XML deaktiviert ist, muss die STA-URL die URL der STA (Adresse des DDC) sein und der Parameter "TrustRequestsSentToTheXmlServicePort"des DDC muss auf "True"festgelegt sein.




## Resilienzeinstellungen für Sitzungen

March 30, 2024

Aufrechterhalten der Sitzungsaktivität ist wichtig für die beste Benutzererfahrung. Eine Unter-

brechung der Verbindung aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten kann zu Frustrationen bei den Benutzern führen. Ein schneller Wechsel zwischen Arbeitsstationen und Zugriff auf dieselben Anwendungen bei jeder Anmeldung ist eine Priorität für viele mobile Mitarbeiter, z. B. von Mitarbeitern in einem Krankenhaus.

Die hier beschriebenen Features dienen dazu, die Sitzungszuverlässigkeit zu optimieren, Unannehmlichkeiten, Ausfallzeiten und Produktivitätsverluste zu reduzieren, und mobilen Benutzern einen schnellen und einfachen Wechsel zwischen Geräten zu ermöglichen.

## Sitzungszuverlässigkeit

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Diese Funktion ist besonders für mobile Benutzer mit drahtlosen Verbindungen geeignet. Ein Benutzer mit einer drahtlosen Verbindung fährt z. B. in einen Tunnel und die Verbindung wird vorübergehend unterbrochen. Normalerweise würde die Sitzung getrennt und nicht mehr auf dem Bildschirm angezeigt. Der Benutzer müsste sich neu mit der getrennten Sitzung verbinden. Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf der Maschine aktiv. Auf dem Client friert der Bildschirm ein und der Mauszeiger wird als Sanduhr angezeigt, bis die Verbindung am Ende des Tunnels wiederhergestellt ist. Der Benutzer kann während der Unterbrechung weiterhin auf die Anzeige zugreifen und mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Citrix Workspace-App-Benutzer können die Controllereinstellung nicht außer Kraft setzen.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden. Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und Citrix Gateway gesendet werden.

Sie aktivieren und konfigurieren die Sitzungszuverlässigkeit mit den folgenden Einstellungen:

- Mit der Richtlinieneinstellung "Sitzungszuverlässigkeit - Verbindungen"können Sie die Sitzungszuverlässigkeit aktivieren oder deaktivieren.
- Der Standardwert für die Einstellung "Sitzungszuverlässigkeit - Timeout"ist 180 Sekunden (drei Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Benutzer nicht zu einer Neuauthentifizierung auffordert, um den Bedienungskomfort zu erhöhen. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.

- Eingehende Sitzungszuverlässigkeitsverbindungen verwenden Port 2598, es sei denn, die Portnummer wurde unter "Sitzungszuverlässigkeit - Portnummer"geändert.
- Verwenden Sie die Funktion zur automatischen Wiederverbindung von Clients, wenn Sie möchten, dass Benutzer eine Verbindung mit unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können. Sie können die Einstellung für die Citrix-Richtlinie Authentifizierung bei automatischer Wiederverbindung von Clients so konfigurieren, dass Benutzer aufgefordert werden, sich neu zu authentifizieren, wenn sie sich mit einer unterbrochenen Sitzung wieder verbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, sobald der mit der Option "Sitzungszuverlässigkeit - Timeout" festgelegte Zeitraum abläuft. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

### Automatische Wiederverbindung von Clients

Mit der automatischen Wiederverbindung von Clients kann die Citrix Workspace-App unabsichtlich getrennte ICA-Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden. Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können.

Bei Anwendungssitzungen versucht die Citrix Workspace-App, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Bei Desktopsitzungen versucht die Citrix Workspace-App eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist fünf Minuten. Um die Zeit zu ändern, bearbeiten Sie die Registrierung auf dem Benutzergerät:

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

wobei `seconds` die Zeit in Sekunden ist, nach der keine weiteren Versuche zur Wiederverbindung unternommen werden.

Sie aktivieren und konfigurieren die automatische Wiederverbindung von Clients mit den folgenden Einstellungen:

- **Automatische Wiederverbindung von Clients:** aktiviert oder deaktiviert die automatische Wiederverbindung derselben Citrix Workspace-App, nachdem die Verbindung unterbrochen wurde.

- **Authentifizierung bei automatischer Wiederverbindung von Clients:** aktiviert oder deaktiviert die erforderliche Benutzerauthentifizierung bei der automatischen Wiederverbindung
- **Protokollierung der automatischen Wiederverbindung von Clients:** aktiviert oder deaktiviert die Protokollierung von Wiederverbindungsereignissen im Ereignisprotokoll. Die Protokollierung ist standardmäßig deaktiviert. Wenn diese Einstellung aktiviert ist, werden Informationen zu erfolgreichen oder fehlgeschlagenen automatischen Wiederverbindungsereignissen im Systemprotokoll des Servers aufgezeichnet. Jeder Server speichert Informationen über Wiederverbindungsereignisse in seinem eigenen Systemprotokoll. Die Site stellt kein kombiniertes Protokoll zu Wiederverbindungsereignissen auf allen Servern zur Verfügung.

Bei der automatischen Wiederverbindung von Clients findet eine Authentifizierung mit verschlüsselten Anmeldeinformationen statt. Wenn sich ein Benutzer anmeldet, verschlüsselt und speichert der Server die Anmeldeinformationen und erstellt und sendet ein Cookie mit einem Verschlüsselungsschlüssel an die Citrix Workspace-App. Diese übermittelt den Schlüssel zur Wiederverbindung an den Server. Der Server entschlüsselt die Anmeldeinformationen und gibt sie an die Windows-Anmeldung für eine Authentifizierung weiter. Benutzer müssen sich beim Ablaufen von Cookies neu authentifizieren, um Sitzungen wiederherzustellen.

Cookies werden nicht verwendet, wenn Sie die Einstellung "Authentifizierung bei automatischer Wiederverbindung von Clients"aktivieren. Stattdessen wird der Benutzer in einem Dialogfeld zur Eingabe der Anmeldeinformationen aufgefordert, wenn die Citrix Workspace-App versucht, die Verbindung automatisch wiederherzustellen.

Zum maximalen Schutz der Anmeldeinformationen von Benutzern und von Sitzungen verwenden Sie die Verschlüsselung für die gesamte Kommunikation zwischen Clients und Site.

Sie deaktivieren die automatische Wiederverbindung in der Citrix Workspace-App für Windows über die Datei icaclient.adm. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Version der Citrix Workspace-App für Windows.

Einstellungen für Verbindungen wirken sich auch auf die automatische Wiederverbindung von Clients aus:

- In der Standardeinstellung wird die automatische Wiederverbindung von Clients durch Richtlinieneinstellungen auf der Siteebene aktiviert (siehe oben). Der Benutzer muss sich nicht authentifizieren. Wenn jedoch die ICA-TCP-Verbindung eines Servers so konfiguriert wurde, dass Sitzungen mit einer unterbrochenen Kommunikationsverbindung zurückgesetzt werden, findet die automatische Wiederverbindung nicht statt. Die automatische Wiederverbindung von Clients funktioniert nur, wenn der Server Sitzungen trennt, wenn eine unterbrochene Verbindung oder eine Verbindungstimeout vorliegt. In diesem Zusammenhang verweist "ICA-TCP-Verbindung"auf den virtuellen Serverport (nicht auf eine tatsächliche Netzwerkverbindung), der für Sitzungen in TCP/IP-Netzwerken verwendet wird.
- Standardmäßig ist die ICA-TCP-Verbindung auf einem Server so eingestellt, dass Sitzungen

mit unterbrochenen Verbindungen oder Verbindungen, die das Zeitlimit überschritten haben, getrennt werden. Getrennte Sitzungen bleiben im Systemspeicher intakt und stehen für eine Wiederverbindung durch die Citrix Workspace-App zur Verfügung.

- Die Verbindung kann so konfiguriert werden, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen mit Timeouts zurückgesetzt oder abgemeldet werden. Wenn eine Sitzung zurückgesetzt wird, startet der Wiederverbindungsversuch eine neue Sitzung. Die Umgebung des Benutzers wird in der verwendeten Anwendung nicht wiederhergestellt, sondern die Anwendung wird neu gestartet.
- Wenn der Server für das Zurücksetzen von Sitzungen konfiguriert ist, erstellt die automatische Wiederverbindung von Clients eine Sitzung. Benutzer müssen dann ihre Anmeldeinformationen eingeben, um sich am Server anzumelden.
- Die automatische Wiederverbindung kann fehlschlagen, wenn die Citrix Workspace-App oder das Plug-In falsche Authentifizierungsinformationen übergibt (dies kann während eines Angriffs passieren), oder wenn der Server feststellt, dass zu viel Zeit seit dem Erkennen der unterbrochenen Verbindung verstrichen ist.

### ICA-Keep-Alive

ICA-Keep-Alive verhindert, dass Sitzungen durch unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität erkennt (z. B. keine Zeitänderungen, Mausbewegungen oder Bildschirmaktualisierungen) wird verhindert, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Pakete, um zu erkennen, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt" gekennzeichnet.

> **Wichtig:**
>
> ICA-Keep-Alive funktioniert nur, wenn Sie die Sitzungszuverlässigkeit nicht verwenden. Die Sitzungszuverlässigkeit hat eigene Mechanismen für das Aufrechterhalten von Verbindungen. Konfigurieren Sie ICA-Keep-Alive nur für Verbindungen, die keine Sitzungszuverlässigkeit verwenden.

ICA-Keep-Alive-Einstellungen überschreiben Keep-Alive-Einstellungen, die in der Microsoft Windows-Gruppenrichtlinie konfiguriert wurden.

Sie aktivieren und konfigurieren ICA-Keep-Alive mit den folgenden Einstellungen:

- **ICA-Keep-Alive - Timeout:** gibt das Intervall (1–3600 Sekunden) für das Senden von ICA-Keep-Alive-Meldungen an. Konfigurieren Sie diese Option nicht, wenn die Netzwerksoftware inaktive Sitzungen schließen soll und unterbrochene Verbindungen in der Umgebung so selten sind, dass die Wiederverbindung mit Sitzungen nicht wichtig ist.

Die Standardeinstellung von 60 Sekunden bedeutet, dass alle 60 Sekunden ICA-Keep-Alive-Pakete an Benutzergeräte gesendet werden. Antwortet ein Benutzergerät nicht in 60 Sekunden, wird der Status der ICA-Verbindung auf "Getrennt"gesetzt.

- **ICA-Keep-Alives:** sendet oder verhindert das Senden von ICA-Keep-Alive-Meldungen.

### Workspace Control

Mit Workspace Control können Desktops und Anwendungen einem Benutzer von einem Gerät zum anderen folgen. Diese Roamingfähigkeit ermöglicht Benutzern den Zugriff auf alle Desktops oder offene Anwendungen von einem beliebigen Ort aus, ohne Neustart des Desktops oder der Anwendungen auf jedem einzelnen Gerät. Sie müssen sich lediglich anmelden. Mit Workspace Control kann das Pflegepersonal in einem Krankenhaus beispielsweise schnell an eine andere Arbeitsstation wechseln und nach der Anmeldung auf dieselben Anwendungen zugreifen. Bei entsprechender Konfiguration von Workspace Control können die Mitarbeiter die Verbindung zu mehreren Anwendungen auf einem Clientgerät trennen und die Verbindung zu denselben Anwendungen auf einem anderen Clientgerät wiederherstellen.

Workspace Control wirkt sich auf die folgenden Aktivitäten aus:

- **Anmelden:** Standardmäßig ermöglicht Workspace Control den Benutzern, die Verbindung mit allen ausgeführten Desktops und Anwendungen bei der Anmeldung automatisch wiederherzustellen, ohne sie erneut manuell zu öffnen. Mit Workspace Control können Benutzer getrennte Desktops oder Anwendungen öffnen sowie alle, die auf einem anderen Clientgerät aktiv sind. Beim Trennen der Verbindung mit einem Desktop bzw. einer Anwendung wird das Desktop bzw. die Anwendung weiterhin auf dem Server ausgeführt. Bei Benutzern im Roamingbetrieb, die einige Desktops oder Anwendungen auf einem Clientgerät ausführen müssen, während sie auf einem anderen Clientgerät eine Wiederverbindung zu einem Teil ihres Desktops bzw. ihrer Anwendungen durchführen möchten, können Sie das Wiederverbindungsverhalten bei der Anmeldung so konfigurieren, dass nur die Desktops bzw. Anwendungen geöffnet werden, die zuvor getrennt wurden.
- **Wiederverbinden:** Nach der Anmeldung am Server können die Benutzer eine Verbindung zu all ihren Desktops oder Anwendungen jederzeit wiederherstellen, indem Sie auf "Wiederverbinden"klicken. Beim Wiederverbinden werden standardmäßig sowohl getrennte Desktops oder Anwendungen geöffnet als auch alle aktiven Anwendungen, die derzeit auf einem anderen Clientgerät ausgeführt werden. Sie können die Wiederverbindung so konfigurieren, dass nur die Desktops oder Anwendungen geöffnet werden, deren Verbindung der Benutzer zuvor getrennt hat.
- **Abmelden:** Bei Benutzern, die Desktops oder Anwendungen über StoreFront öffnen, können Sie den Abmeldebefehl so konfigurieren, dass Benutzer entweder von StoreFront und allen aktiven Sitzungen gleichzeitig oder nur von StoreFront abgemeldet werden.

- **Verbindung wird getrennt:** Die Benutzer können die Verbindung mit allen ausgeführten Desktops und Anwendungen gleichzeitig trennen.

Workspace Control ist für Benutzer verfügbar, die über eine Citrix StoreFront-Verbindung oder über die Citrix Workspace-App auf Desktops und Anwendungen zugreifen. Workspace Control ist standardmäßig für virtuelle Desktopsitzungen deaktiviert und für gehostete Anwendungen aktiviert. Die Sitzungsfreigabe zwischen veröffentlichten Desktops und veröffentlichten Anwendungen in diesen Desktops erfolgt nicht standardmäßig.

Benutzerrichtlinien, Clientlaufwerkzuordnungen und Druckerkonfigurationen ändern sich entsprechend, wenn ein Benutzer ein neues Clientgerät verwendet. Diese Richtlinien und Zuordnungen werden auf dem Clientgerät angewendet, auf dem der Client bei der Sitzung angemeldet ist. Wenn sich Pflegepersonal z. B. von einem Clientgerät in der Notaufnahme des Krankenhauses abmeldet und dann bei einer Arbeitsstation in der Röntgenabteilung anmeldet, gelten für die Sitzung die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen der Röntgenabteilung.

Sie können die den Benutzern angezeigten Drucker je nach Standort anpassen. Außerdem können Sie steuern, ob Benutzer auf lokalen Druckern drucken können, wie viel Bandbreite bei einer Remoteverbindung verwendet wird sowie andere Aspekte des Druckens.

Weitere Informationen zur Aktivierung und Konfiguration von Workspace Control für Benutzer finden Sie in der StoreFront-Dokumentation.

### Sitzungsroaming

> **Hinweis:**
>
> Die folgende Anleitung zeigt Ihnen, wie Sie das Sitzungsroaming mit PowerShell konfigurieren. Sie können stattdessen auch die Verwaltungsoberfläche "Vollständige Konfiguration" verwenden. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

Standardmäßig wechseln Sitzungen zusammen mit dem Benutzer von Clientgerät zu Clientgerät. Wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet, wird die gleiche Sitzung verwendet und die Anwendungen stehen gleichzeitig auf beiden Geräten zur Verfügung. Sie können die Anwendungen auf mehreren Geräten anzeigen. Die Anwendungen folgen dem Benutzer unabhängig von dem Gerät und davon, ob aktuelle Sitzungen vorhanden sind. Oft folgen auch Drucker und andere Ressourcen, die einer Anwendung zugewiesen sind.

Dieses Standardverhalten bietet viele Vorteile, ist aber nicht in allen Fällen ideal. Sie können das Sitzungsroaming mit dem PowerShell-SDK verhindern.

Beispiel 1: Ein Mitarbeiter eines Krankenhauses verwendet beim Ausfüllen eines Versicherungsformulars einen Desktop-PC und ein Tablet zum Anzeigen von Patientendaten.

- Bei aktiviertem Sitzungsroaming werden beide Anwendungen auf beiden Geräten angezeigt (eine auf einem Gerät gestartete Anwendung ist auf allen Geräten zu sehen). Dies entspricht möglicherweise nicht den Sicherheitsanforderungen.
- Wenn das Sitzungsroaming deaktiviert ist, werden die Patientendaten nicht auf dem PC angezeigt und das Versicherungsformular nicht auf dem Tablet.

Beispiel 2: Ein Produktionsmanager startet eine Anwendung auf dem PC im Büro. Gerätename und Standort bestimmen, welche Drucker und anderen Ressourcen für die Sitzung verfügbar sind. Später nimmt er bei einer Besprechung in einem anderen Gebäude teil und muss etwas ausdrucken.

- Bei aktiviertem Sitzungsroaming kann er wahrscheinlich nicht auf die Drucker in der Nähe des Besprechungsraums zugreifen, da ihm durch den Anwendungsstart Drucker und Ressourcen für den Standort Büro zugewiesen wurden.
- Ist das Sitzungsroaming deaktiviert, wird bei der Anmeldung bei einem anderen Gerät (mit denselben Anmeldeinformationen) eine neue Sitzung gestartet und Drucker und Ressourcen in der Nähe sind verfügbar.

#### Sitzungsroaming konfigurieren

Zum Konfigurieren des Sitzungsroamings verwenden Sie die folgenden Anspruchsrichtlinienregel-Cmdlets mit der Eigenschaft "SessionReconnection". Optional können Sie auch die Eigenschaft "LeasingBehavior"angeben.

Desktopsitzungen:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Anwendungssitzungen:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Für `value` sind folgende Optionen möglich:

- **Always:** Das Sitzungsroaming ist immer aktiviert, unabhängig vom Clientgerät und davon, ob die Sitzung verbunden oder getrennt ist. Dies ist der Standardwert.
- **DisconnectedOnly:** Eine Wiederverbindung erfolgt nur bei Sitzungen, die bereits getrennt sind. Andernfalls wird eine neue Sitzung gestartet. (Sitzungen können zwischen Clientgeräten wechseln, indem sie zunächst getrennt werden oder das Roaming für sie explizit mit Workspace Control durchgeführt wird.) Eine aktive verbundene Sitzung von einem anderen Clientgerät wird nie verwendet. Stattdessen wird eine neue Sitzung gestartet.
- **SameEndpointOnly:** Der Benutzer erhält eine eigene Sitzung für jedes verwendete Clientgerät. Damit wird das Sitzungsroaming vollständig deaktiviert. Die Benutzer können eine Wiederverbindung nur auf dem Gerät vornehmen, das zuvor für die Sitzung verwendet wurde.

Die Eigenschaft “LeasingBehavior”wird weiter unten beschrieben.

**Auswirkungen anderer Einstellungen:**

Das in den Anwendungseigenschaften einer Bereitstellungsgruppe über “Nur eine Anwendungsinstanz pro Benutzer zulassen”festgelegte Anwendungslimit hat Auswirkungen auf die Deaktivierung des Sitzungsroamings.

- Wenn Sie das Sitzungsroaming deaktivieren, deaktivieren auch die Option “Nur eine Anwendungsinstanz pro Benutzer zulassen”.
- Wenn Sie die Option “Nur eine Anwendungsinstanz pro Benutzer zulassen”aktivieren, konfigurieren Sie keinen der beiden Werte, durch die neue Sitzungen auf neuen Geräten zugelassen werden.

### Anmeldeintervall

Wenn eine virtuelle Maschine mit einem Desktop-VDA geschlossen wird, bevor die Anmeldung abgeschlossen ist, können Sie dem Prozess mehr Zeit zuteilen. Die Standardeinstellung in Version 7.6 und höher ist 180 Sekunden (die Standardeinstellung für Version 7.0-7.5 ist 90 Sekunden).

Legen Sie auf der Maschine (oder dem im Maschinenkatalog verwendeten Masterimage) folgenden Registrierungsschlüssel fest:

Schlüssel: `HKLM\SOFTWARE\Citrix\PortICA`

- Wert: `AutoLogonTimeout`
- Typ: `DWORD`
- Geben Sie die Zeit als Dezimalwert in Sekunden ein, zulässig ist ein Wert von 0 bis 3600.

Wenn Sie das Masterimage ändern, müssen Sie das neue Image im Katalog bereitstellen. Weitere Informationen finden Sie unter Masterimage ändern.

Diese Einstellung gilt nur für VMs mit Einzelsitzungs-OS-VDAs. Microsoft steuert das Anmeldetimeout auf Maschinen mit Multisitzungs-OS-VDAs.

## Tags

November 16, 2023

### Einführung

Tags sind Zeichenfolgen zur Identifizierung von Elementen wie z. B. Maschinen, Anwendungen, Desktops, Bereitstellungsgruppen, Anwendungsgruppen und Richtlinien. Durch Erstellen und Hinzufügen

von Tags können Sie festlegen, dass bestimmte Vorgänge nur an Elementen stattfinden, die ein spezifisches Tag haben.

- Sie können die Suchanzeige in der Verwaltungsoberfläche "Vollständige Konfiguration" anpassen.

  Wenn Sie beispielsweise nur Anwendungen anzeigen möchten, die für Testzwecke optimiert wurden, erstellen Sie ein Tag mit dem Namen "Test"und fügen es den Anwendungen hinzu. Sie können dann die Suche nach dem Tag "Test"filtern.

- Veröffentlichen von Anwendungen aus einer Anwendungsgruppe oder von bestimmten Desktops aus einer Bereitstellungsgruppe unter ausschließlicher Berücksichtigung einer Teilmenge der Maschinen in den ausgewählten Bereitstellungsgruppen Dies wird als *Tagbeschränkung* bezeichnet.

  Mit Tagbeschränkungen können Sie Ihre vorhandenen Maschinen für mehrere Veröffentlichungstasks verwenden und sparen so die Kosten für die Bereitstellung und Verwaltung weiterer Maschinen. Die Verwendung von Tagbeschränkungen kann man sich als Unterteilung (oder Partitionierung) der Maschinen in einer Bereitstellungsgruppe vorstellen. Die Funktionsweise von Tagbeschränkungen ähnelt der von Workergruppen in XenApp-Releases vor 7.x, ist mit dieser jedoch nicht identisch.

  Anwendungsgruppen und Desktops mit Tagbeschränkungen können auch zur Isolierung von Maschinengruppen in einer Bereitstellungsgruppe zur Problembehandlung nützlich sein.

  Details zu und Beispiele für die Verwendung von Tagbeschränkungen werden weiter unten beschrieben.

- Planen regelmäßiger Neustarts für eine Teilmenge der Maschinen in einer Bereitstellungsgruppe

  Unter Einsatz einer Tagbeschränkung für Maschinen können Sie neue PowerShell-Cmdlets zum Konfigurieren mehrerer Neustart-Zeitpläne für Teilmengen von Maschinen in einer Bereitstellungsgruppe verwenden. Beispiele und weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen.

- Zielgerichtete Anwendung (Zuweisung) von Citrix Richtlinien auf Maschinen in Bereitstellungsgruppen, Bereitstellungsgruppentypen oder Organisationseinheiten, die ein bestimmtes Tag haben (oder nicht haben)

  Wenn Sie beispielsweise eine Citrix Richtlinie nur auf leistungsstarke Arbeitsstationen anwenden möchten, fügen Sie diesen Maschinen ein Tag mit dem Namen "Hohe Leistung" hinzu. Wählen Sie dann auf der Seite **Richtlinie zuweisen** des Assistenten zum Erstellen von Richtlinien dieses Tag und das Kontrollkästchen **Aktivieren**. Sie können auch einer Bereitstellungsgruppe ein Tag hinzufügen und eine Citrix Richtlinie auf die Gruppe anwenden. Einzelheiten finden Sie unter Erstellen von Richtlinien.

Sie können Tags auf Folgendes anwenden:

- Maschinen
- Anwendungen
- Maschinenkataloge
- Bereitstellungsgruppen
- Anwendungsgruppen

Sie können Tagbeschränkungen beim Erstellen und Bearbeiten der folgenden Elemente in der Schnittstelle für die vollständige Konfiguration konfigurieren:

- Desktops in einer freigegebenen Bereitstellungsgruppe
- Anwendungsgruppen

## Tagbeschränkungen für Desktops oder Anwendungsgruppen

Das Erstellen von Tagbeschränkungen umfasst mehrere Schritte:

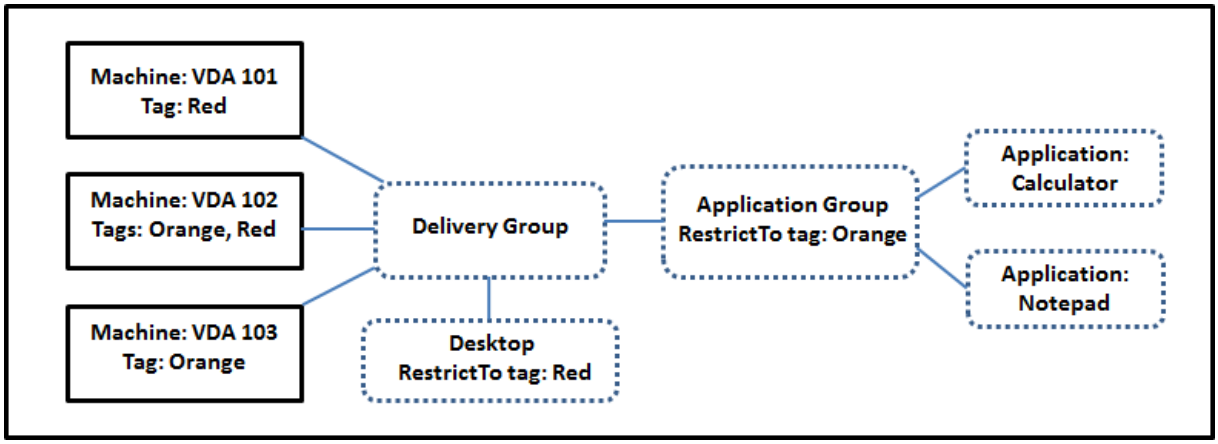
- Erstellen Sie das Tag und fügen Sie es Maschinen hinzu.
- Erstellen oder bearbeiten Sie eine Gruppe mit der Tagbeschränkung (d. h. beschränken Sie Starts auf Maschinen mit Tag *x*).

Tagbeschränkungen erweitern die Maschinenauswahl durch den Controller. Der Controller wählt Maschinen aus Bereitstellungsgruppen auf der Basis der Zugriffsrichtlinie, konfigurierten Benutzerlisten, der Zonenpräferenz, der Startbereitschaft und, falls vorhanden, der Tagbeschränkung aus. Bei Anwendungen berücksichtigt der Controller Bereitstellungsgruppen in der Reihenfolge der Priorität unter Anwendung der gleichen Maschinenauswahlregeln für jede Bereitstellungsgruppe.

### Beispiel 1: einfache Anordnung

Dieses Beispiel ist eine einfache Anordnung mit Tagbeschränkungen, die festlegen, welche Maschinen für bestimmte Desktop- und Anwendungsstarts in Betracht gezogen werden. Es gibt eine freigegebene Bereitstellungsgruppe, einen veröffentlichten Desktop und eine Anwendungsgruppe mit zwei Anwendungen.




- Allen drei Maschinen (VDA 101–103) wurden Tags hinzugefügt.
- Der Desktop in der Bereitstellungsgruppe wurde mit der Tagbeschränkung `Red` erstellt. Der Desktop kann daher nur auf Maschinen in dieser Bereitstellungsgruppe mit dem Tag `Red` (VDA 101 und 102) gestartet werden.
- Die Anwendungsgruppe wurde mit der Tagbeschränkung `Orange` erstellt. Die enthaltenen Anwendungen (`Calculator` und `Notepad`) werden daher nur auf Maschinen in dieser Bereitstellungsgruppe mit dem Tag `Orange`: VDA 102 und 103, gestartet.

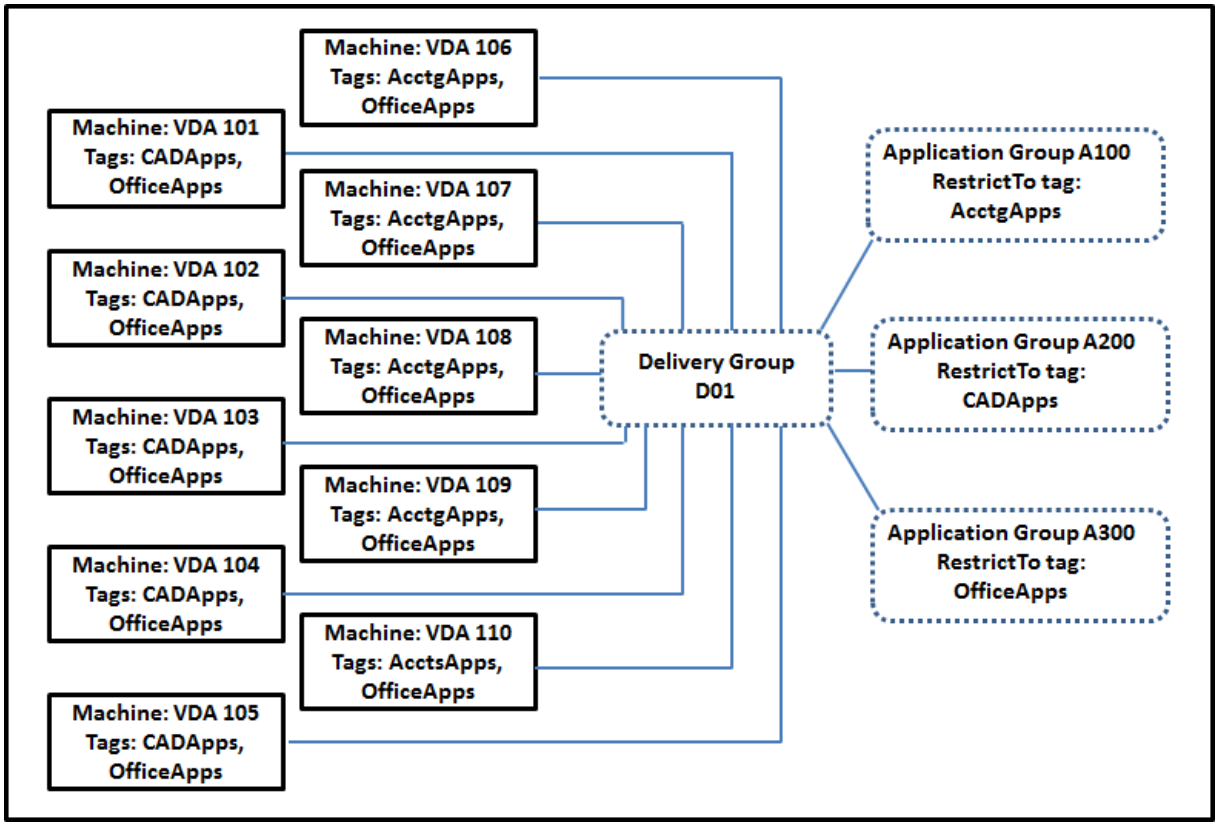
Maschine VDA 102 hat beide Tags (`Red` und `Orange`) und kann daher für das Starten von Anwendungen und Desktops verwendet werden.

#### Beispiel 2: komplexere Anordnung

Dieses Beispiel enthält mehrere Anwendungsgruppen mit Tagbeschränkungen. Auf diese Weise können mehr Anwendungen mit weniger Maschinen als bei bloßer Verwendung von Bereitstellungsgruppen bereitgestellt werden.

Unter Konfigurieren von Beispiel 2 werden die Schritte zum Erstellen und Anwenden der Tags und zum Konfigurieren der Tagbeschränkungen erläutert.




In diesem Beispiel hat die Umgebung 10 Maschinen (VDA 101–110), eine Bereitstellungsgruppe (`D01`) und drei Anwendungsgruppen (`A100`, `A200`, `A300`). Durch Anwenden von Tags auf jede Maschine und Festlegen von Tagbeschränkungen beim Erstellen jeder Anwendungsgruppe wird Folgendes erreicht:

- Die Benutzer der Gruppe "Accounting"können auf die benötigten Anwendungen auf fünf Maschinen (101–105) zugreifen.
- CAD-Designer können auf die benötigten Anwendungen auf fünf Maschinen (106–110) zugreifen.
- Benutzer, die Office-Anwendungen benötigen, können auf Office-Anwendungen auf 10 Maschinen (VDA 101–110) zugreifen.

Es werden nur 10 Maschine mit nur einer Bereitstellungsgruppe verwendet. Bei ausschließlicher Verwendung von Bereitstellungsgruppen ohne Anwendungsgruppen würden doppelt so viele Maschinen benötigt, da jede Maschine nur zu einer Bereitstellungsgruppe gehören kann.

### Verwalten von Tags und Tagbeschränkungen

Zum Erstellen, Hinzufügen (Anwenden), Bearbeiten und Löschen von Tags für ausgewählte Elemente wird die Aktion **Tags verwalten** in der Verwaltungsoberfläche "Vollständige Konfiguration"verwendet.

(Ausnahme: Tags für Richtlinienzuweisungen werden über die Aktion **Tags verwalten** erstellt, bearbeitet und gelöscht. Die Tags werden jedoch von Ihnen beim Erstellen der Richtlinie angewendet (zugewiesen). Weitere Informationen finden Sie unter Erstellen von Richtlinien.)

Tagbeschränkungen konfigurieren Sie beim Erstellen oder Bearbeiten von Desktops in Bereitstellungsgruppen und beim Erstellen und Bearbeiten von Anwendungsgruppen.

#### Verwenden des Features "Tags verwalten"

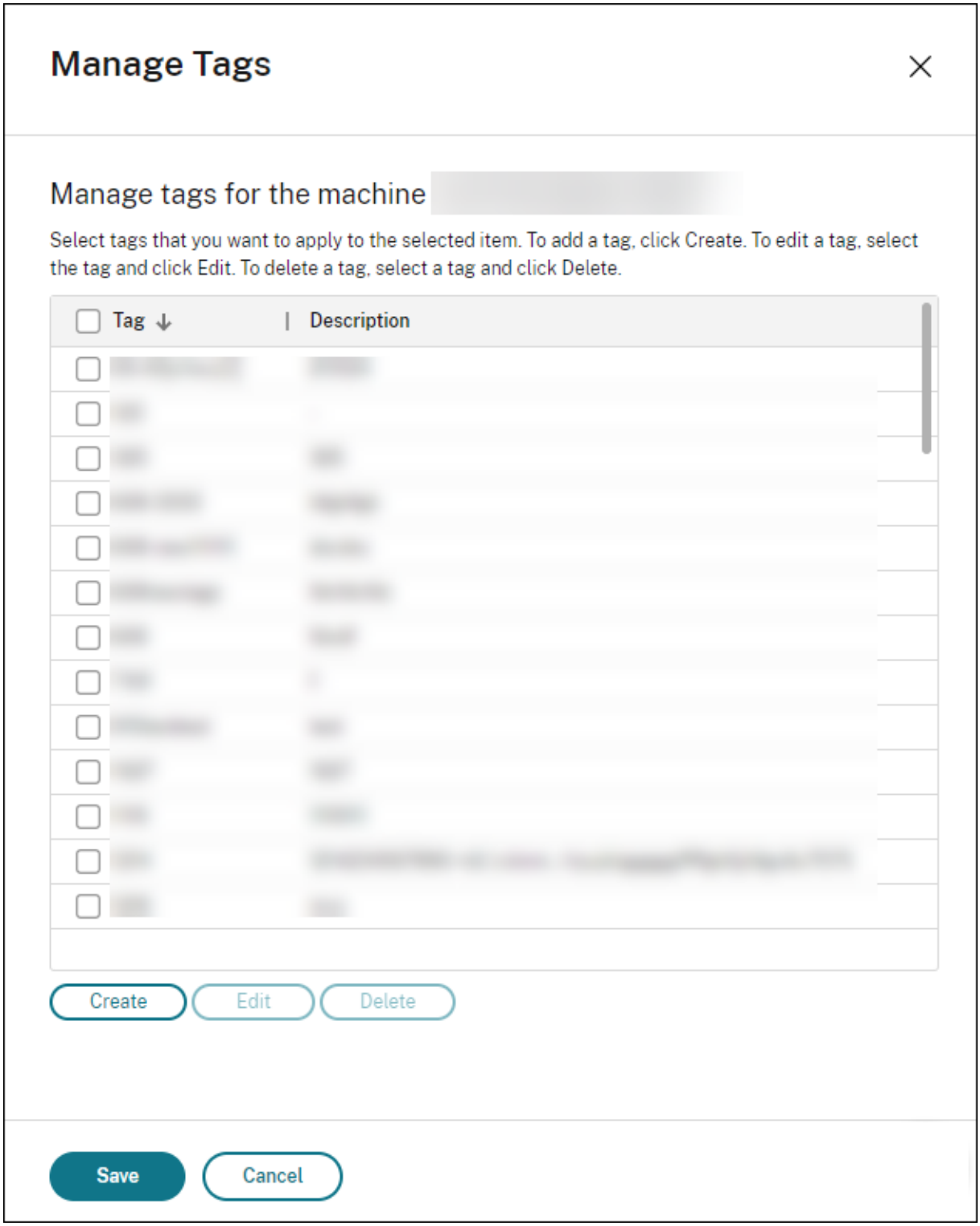
Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Elemente aus, auf die Sie ein Tag anwenden möchten. Dazu gehören:

- Eine oder mehrere Maschinen
- Eine oder mehrere Anwendungen
- Ein Desktop, eine Bereitstellungsgruppe oder eine Anwendungsgruppe
- Ein Maschinenkatalog

Wählen Sie dann in der Aktionsleiste **Tags verwalten**. Das Dialogfeld **Tags verwalten** zeigt alle vorhandenen Tags, nicht nur die Tags für die von Ihnen ausgewählten Elemente.

- Ist das Kontrollkästchen eines Tags aktiviert, wurde das Tag den ausgewählten Elementen bereits hinzugefügt. (In der Abbildung unten hat die ausgewählte Maschine das Tag "Tag1".)
- Wenn Sie mehrere Elemente auswählen, wird durch ein Kontrollkästchen mit einem Strich angezeigt, wenn das Tag einigen (aber nicht allen) Elementen hinzugefügt wurde.




Die folgenden Aktionen stehen im Dialogfeld **Tags verwalten** zur Verfügung. Konsultieren Sie den Artikel Hinweise zum Arbeiten mit Tags.

- **Tags erstellen:**

Wählen Sie **Erstellen**. Geben Sie einen Namen und eine Beschreibung ein. Tagnamen müssen eindeutig sein, die Groß- und Kleinschreibung spielt keine Rolle. Wählen Sie dann **Speichern**.

Durch das Erstellen eines Tags wird es nicht automatisch auf Elemente angewendet, die Sie ausgewählt haben. Verwenden Sie zum Anwenden die Kontrollkästchen.

- **Hinzufügen von Tags:**

  Aktivieren Sie die Kontrollkästchen neben den Tagnamen. Ein Kontrollkästchen mit einem Strich zeigt an, wenn das Tag auf einige (aber nicht alle) ausgewählten Elemente angewendet wurde. Wenn Sie mehrere Elemente auswählen und das Kontrollkästchen eines Tags einen Strich enthält, wirkt sich das Ändern in ein Häkchen auf alle ausgewählten Maschinen aus.

  Wenn Sie versuchen, ein als Einschränkung in einer Anwendungsgruppe verwendetes Tag Maschinen hinzuzufügen, werden Sie gewarnt, dass die Maschinen dadurch evtl. für Starts verfügbar gemacht werden. Wenn dies beabsichtigt ist, fahren Sie fort.

- **Entfernen von Tags:**

  Deaktivieren Sie die Kontrollkästchen neben den entsprechenden Tagnamen. Ein Kontrollkästchen mit einem Strich zeigt an, wenn das Tag auf einige (aber nicht alle) ausgewählten Elemente angewendet wurde. Wenn Sie mehrere Elemente auswählen und das Kontrollkästchen eines Tags einen Strich enthält, wird bei Deaktivieren des Kontrollkästchens das Tag von allen ausgewählten Maschinen entfernt.

  Wenn Sie versuchen, ein Tag von einer Maschine zu entfernen, werden Sie gewarnt, dass diese Aktion sich auf die für Starts infrage kommenden Maschinen auswirken kann. Wenn dies beabsichtigt ist, fahren Sie fort.

- **Bearbeiten von Tags:**

  Wählen Sie ein Tag und dann **Bearbeiten**. Geben Sie einen neuen Namen und/oder eine Beschreibung ein. Sie können immer nur ein Tag bearbeiten.

- **Löschen von Tags:**

  Wählen Sie die Tags und dann **Löschen**. Im Dialogfeld **Tag löschen** wird angezeigt, von wie vielen Elementen die ausgewählten Tags verwendet werden (z. B. "2 Maschinen"). Wählen Sie ein Element, um weitere Informationen anzuzeigen (z. B. die Namen der beiden Maschinen, auf die das Tag angewendet wurde). Bestätigen Sie, dass Sie die Tags löschen möchten.

  Sie können keine Tags löschen, die als Einschränkung verwendet werden. Bearbeiten Sie zuerst die Anwendungsgruppe entfernen Sie und die Tagbeschränkung oder wählen Sie ein anderes Tag.

Wenn Sie im Dialogfeld **Tags verwalten** fertig sind, wählen Sie **Speichern**.

Um festzustellen, ob auf eine Maschine Tags angewendet werden, gehen Sie folgendermaßen vor: Wählen Sie im linken Bereich **Bereitstellungsgruppen**. Wählen Sie eine Bereitstellungsgruppe und

wählen Sie dann in der Aktionsleiste **Maschinen anzeigen**. Wählen Sie eine Maschine und dann im Bereich **Details** die Registerkarte **Tags**.

#### Tagbeschränkungen verwalten

Das Verfahren zum Konfigurieren von Tagbeschränkungen besteht aus mehreren Schritten. Zunächst erstellen das Tag und wenden es auf Maschinen an. Anschließend fügen Sie der Anwendungsgruppe oder dem Desktop die Einschränkung hinzu.

- **Tag erstellen und anwenden:**

  Erstellen Sie mithilfe des Dialogfelds **Tags verwalten** das Tag und wenden Sie es dann auf die Maschinen an, für die die Beschränkung gelten soll.

- **Tagbeschränkung einer Anwendungsgruppe hinzufügen:**

  Erstellen oder bearbeiten Sie die Anwendungsgruppe. Wählen Sie auf der Seite **Bereitstellungsgruppen** die Option **Starts auf Maschinen mit Tag beschränken** und dann aus der Liste das Tag.

- **Tagbeschränkung für eine Anwendungsgruppe ändern/entfernen:**

  Bearbeiten Sie die Gruppe. Wählen Sie auf der Seite **Bereitstellungsgruppen** ein anderes Tag aus der Liste oder entfernen Sie die Tagbeschränkung vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

- **Tagbeschränkung einem Desktop hinzufügen:**

  Erstellen oder bearbeiten Sie eine Bereitstellungsgruppe. Wählen Sie auf der Seite **Desktops** entweder **Hinzufügen** oder **Bearbeiten**. Wählen Sie im Dialogfeld **Desktop hinzufügen** die Option **Starts auf Maschinen mit Tag beschränken** und dann aus dem Menü das Tag.

- **Ändern/Entfernen von Tagbeschränkung für eine Bereitstellungsgruppe:**

  Bearbeiten Sie die Gruppe. Wählen Sie **Bearbeiten** auf der Seite **Desktops**. Wählen Sie in dem Dialogfeld ein anderes Tag aus der Liste oder entfernen Sie die Tagbeschränkung vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

#### Hinweise zum Arbeiten mit Tags

Ein auf ein Element angewendetes Tag kann für verschiedene Zwecke verwendet werden. Das Hinzufügen, Entfernen und Löschen eines Tags kann ungewollte Auswirkungen haben. Sie können mit einem Tag Maschinenanzeigen sortieren, wenn Sie die Suche in der Verwaltungsoberfläche "Vollständige Konfiguration"verwenden. Sie können dasselbe Tag beim Konfigurieren einer Anwendungsgruppe oder eines Desktops als Einschränkung verwenden. Dadurch wird die Startauswahl auf Maschinen in den Bereitstellungsgruppen beschränkt, die das Tag haben.

Wenn Sie ein Tag einer Maschine hinzufügen, nachdem es als Tagbeschränkung für einen Desktop oder eine Anwendungsgruppe konfiguriert wurde, werden Sie gewarnt, dass die Maschinen durch das Hinzufügen des Tags zum Starten zusätzlicher Anwendungen oder Desktops verfügbar gemacht werden könnten. Wenn dies beabsichtigt ist, fahren Sie fort. Fall nicht, brechen Sie den Vorgang ab.

Angenommen, Sie erstellen eine Anwendungsgruppe mit der Tagbeschränkung Red. Später fügen Sie der von der Anwendungsgruppe verwendeten Bereitstellungsgruppe mehrere Maschinen hinzu. Wenn Sie versuchen, das Tag Red den Maschinen hinzuzufügen, wird folgende Meldung angezeigt: Das Tag Red dient als Beschränkung auf folgende Anwendungsgruppen. Durch das Hinzufügen des Tags werden die ausgewählten Maschinen möglicherweise für den Start von Anwendungen in dieser Anwendungsgruppe verfügbar gemacht. Sie können das Hinzufügen des Tags zu den zusätzlichen Maschinen dann bestätigen oder abbrechen.

Wenn ein Tag in einer Anwendungsgruppe zum Beschränken von Starts verwendet wird, können Sie das Tag erst löschen, wenn Sie es durch Bearbeiten der Gruppe als Beschränkung entfernt haben. (Wenn Sie das Tag löschen dürften, könnte das dazu führen, dass Anwendungen auf allen Maschinen in den der Anwendungsgruppe zugewiesenen Bereitstellungsgruppen gestartet werden könnten). Das Löschen ist auch nicht möglich, wenn ein Tag als Beschränkung für Desktopstarts verwendet wird. Sobald Sie die Tagbeschränkung von der Anwendungsgruppe oder dem Desktop in der Bereitstellungsgruppe entfernt haben, können Sie das Tag löschen.

Nicht alle Maschinen haben unbedingt den gleichen Satz Anwendungen. Ein Benutzer kann mehreren Anwendungsgruppen mit unterschiedlichen Tagbeschränkungen und verschiedenen oder einander überlagernden Maschinengruppen aus Bereitstellungsgruppen angehören. Die folgende Tabelle enthält Informationen dazu, welche Maschinen für einen Start berücksichtigt werden.

| **Anwendung gehört zu** | **Für Starts berücksichtigte Maschinen in den ausgewählten Bereitstellungsgruppen** |
|---|---|
| Einer Anwendungsgruppe ohne Tagbeschränkung | Beliebige Maschinen |
| Einer Anwendungsgruppe mit Tagbeschränkung A | Maschinen mit Tag A |
| Zwei Anwendungsgruppen, die eine mit Tagbeschränkung A, die zweite mit Tagbeschränkung B | Maschinen mit Tag A und B. Sind keine solchen verfügbar, Maschinen mit Tag A oder Tag B. |
| Zwei Anwendungsgruppen, die eine mit Tagbeschränkung A, die zweite ohne Tagbeschränkung | Maschinen mit Tag A; sind keine solchen verfügbar, beliebige Maschinen |

Wenn Sie eine Tagbeschränkung in einem Neustartzeitplan für Maschinen verwenden, treten Änderungen an der Anwendung von Tags bzw. an Tagbeschränkungen beim nächsten Neustartzyklus in

Kraft. Auf Neustartzyklen, die während der Durchführung von Änderungen laufen, haben diese keine Auswirkungen.

#### Konfigurieren von Beispiel 2

Nachfolgend wird erläutert, wie die im zweiten Beispiel gezeigten Tags erstellt und angewendet und die Tagbeschränkungen für die Anwendungsgruppen konfiguriert werden.

Die VDAs und Anwendungen wurden bereits auf den Maschinen installiert und die Bereitstellungsgruppe wurde erstellt.

Tags erstellen und auf Maschinen anwenden

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Bereitstellungsgruppen**. Wählen Sie Bereitstellungsgruppe `D01` und wählen Sie dann in der Aktionsleiste **Maschinen anzeigen**.
2. Wählen Sie die Maschinen VDA 101–105 und dann in der Aktionsleiste **Tags verwalten**.
3. Wählen Sie **Erstellen** im Dialogfeld **Tags verwalten**. Erstellen Sie ein Tag namens `CADApps`. Wählen Sie **OK**.
4. Wählen Sie erneut **Erstellen** und erstellen Sie ein Tag namens `OfficeApps`. Wählen Sie **OK**.
5. Fügen Sie die neu erstellten Tags den ausgewählten Maschinen hinzu, indem Sie die Kontrollkästchen neben den Tagnamen (`CADApps` und `OfficeApps`) aktivieren. Schließen Sie dann das Dialogfeld.
6. Wählen Sie die Bereitstellungsgruppe `D01`. Wählen Sie in der Aktionsleiste **Maschinen anzeigen**.
7. Wählen Sie die Maschinen VDA 106–110 und dann in der Aktionsleiste **Tags verwalten**.
8. Wählen Sie **Erstellen** im Dialogfeld **Tags verwalten**. Erstellen Sie ein Tag namens `AcctgApps`. Wählen Sie **OK**.
9. Fügen Sie die neu erstellten Tags `AcctgApps` und `OfficeApps` den ausgewählten Maschinen hinzu, indem Sie die Kontrollkästchen neben den Tagnamen aktivieren. Schließen Sie dann das Dialogfeld.

Anwendungsgruppen mit Tagbeschränkungen erstellen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Anwendungen**.
2. Wählen Sie in der Aktionsleiste **Anwendungsgruppe erstellen**. Der Assistent wird gestartet.
3. Wählen Sie auf der Seite **Bereitstellungsgruppen** die Bereitstellungsgruppe `D01` aus. Wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag `AcctgApps` aus der Liste aus.
4. Füllen Sie die restlichen Seiten des Assistenten unter Angabe der Benutzer und Anwendungen des Buchhaltungsteams aus. (Wählen Sie beim Hinzufügen der Anwendung als Quelle **Vom**

**Startmenü**, damit die Anwendung auf den Maschinen mit dem Tag `AcctgApps` gesucht wird.) Geben Sie auf der Seite **Zusammenfassung** als Namen für die Gruppe `A100` ein.

5. Wiederholen Sie diese Schritte zum Erstellen der Anwendungsgruppe `A200`, wobei Sie Maschinen mit dem Tag `CADApps` sowie die entsprechenden Benutzer und Anwendungen angeben.
6. Wiederholen Sie diese Schritte zum Erstellen der Anwendungsgruppe `A300`, wobei Sie Maschinen mit dem Tag `OfficeApps` sowie die entsprechenden Benutzer und Anwendungen angeben.

#### Anwenden von Tags auf Maschinenkataloge

Sie können Tags mit **Verwalten > Vollständige Konfiguration** oder PowerShell auf Maschinenkataloge anwenden.

- Die Verwendung der Verwaltungsschnittstelle ist unter Verwalten von Tags beschrieben. Die Kataloganzeigen lassen nicht erkennen, ob Tags angewendet wurden.
- Informationen zur Verwendung von PowerShell finden Sie unter Anwenden von Tags auf Kataloge mit PowerShell.

Beispiel für die Verwendung von Tags für Kataloge:

- Eine Bereitstellungsgruppe umfasst Maschinen aus mehreren Katalogen, aber Sie möchten einen Vorgang (z. B. einen Neustartzeitplan) nur auf Maschinen eines bestimmten Katalogs anwenden. Dies erreichen Sie durch Anwenden eines Tags auf diesen Katalog.

#### Anwenden von Tags auf Kataloge mit PowerShell

Die folgenden PowerShell-Cmdlets sind verfügbar:

- Sie können Katalogobjekte an Cmdlets wie `Add-BrokerTag` und `Remove-BrokerTag` übergeben.
- `Get-BrokerTagUsage` zeigt an, wie viele Kataloge Tags enthalten.
- `Get-BrokerCatalog` hat die Eigenschaft `Tags`.

Die folgenden Cmdlets fügen beispielsweise dem Katalog `acctg` ein zuvor erstelltes Tag namens `fy2018` hinzu: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`.

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Cmdlets.

### Automatische Tags (Preview)

Mit Auto-Tagging können Administratoren für verschiedene DaaS-Objekte automatische Tags benutzerdefiniert festlegen und entfernen. Dadurch entfällt die Notwendigkeit, periodisch ver-

schiedene Skripts zur Umgebungsoptimierung auszuführen und zu verwalten.

### Anwendungsfälle

Mit Auto-Tagging können Sie Regeln implementieren, die Ihren Geschäftsfaktoren entsprechen: z. B. Kostensenkung, Optimierung der Infrastruktur oder Verbrauchssteigerung. Im Folgenden sind einige der Anwendungsfälle aufgeführt:

- **Ungenutzte VDIs zurückfordern**: Freigabe dedizierter Workloads, die länger als eine vorkonfigurierte Anzahl von Tagen nicht genutzt wurden.
- **Übersichtlichere App-Anzeige**: Identifizieren von Anwendungen, die länger als eine vorkonfigurierte Anzahl von Tagen nicht verwendet wurden.
- **Bereitstellungsgruppen mit weniger als Funktionsebene X**: Anzeige von Bereitstellungsgruppen, die unter einer bestimmten Funktionsebene liegen.
- **Inaktive Benutzer**. Rückforderung der Ressourcen von Benutzern, die länger als eine vorkonfigurierte Anzahl von Tagen nicht angemeldet waren.

### PowerShell-Befehle

Sie können automatische Tags mithilfe von PowerShell-Befehlen erstellen. Nachdem eine Autotag-Regel erstellt wurde, wird sie alle 600 Sekunden ausgewertet. Weitere Informationen finden Sie unter New-BrokerAutoTagRule.

**Beispiele** `New-BrokerAutoTagRule` verwendet denselben Objekttyp und dieselben Filterparameter wie das Cmdlet `Get-BrokerMachine`. Weitere Informationen finden Sie unter GetBrokerMachine.

1. Taggen Sie dedizierte VDIs, die länger als 30 Tage nicht verwendet wurden, mit der ID 123:

   a) Definieren Sie ein Tag zum Kennzeichnen ungenutzter VDIs, zum Beispiel **Unused-VDI**.

      - Tagname: Unused-VDI
      - Tag-ID : 123

   b) Erstellen Sie die Autotag-Regel zum Kennzeichnen ungenutzter Maschinen. Definieren Sie die Regelparameter:

      - Name: Allgemeiner Name für die Regel.
      - Objekttyp: Maschine.
      - Regeltext: Statische, zugewiesene Maschinen, deren letzte Verbindungszeit länger als 30 Tage zurückliegt, oder keine Wertangabe.
      - Tag-UID: Die Tag-ID, die Sie zuordnen möchten: 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -
RuleText "-AllocationType Static -IsAssigned $true -Filter {
SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt '-30'
 -or LastConnectionTime -eq `$null )} " -TagUid 123
```

c) Überprüfen Sie die mit dem Tag **Unused-VDI** markierten Maschinen und geben Sie sie frei.

2. Kennzeichnen von Bereitstellungsgruppen, die unter Funktionsebene X liegen (mit **L7_20** als Schwellenwert für Funktionsebene):

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-
RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid
 123
```

3. Kennzeichnen von für Benutzer sichtbare Apps, die ohne Ordner veröffentlicht wurden:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-
TagUid 123
```

### Weitere Informationen

Blogbeitrag: How to assign desktops to specific servers.

## Zeitzonen einrichten

March 6, 2024

Passen Sie das Datums- und Uhrzeitformat in der Managementkonsole nach Ihren Wünschen an.

> **Hinweis:**
>
> Diese Einstellung ist für jedes Benutzerkonto spezifisch.

1. Gehen Sie zu **Vollständige Konfiguration > Einstellungen > Datum und Uhrzeit**.
2. Klicken Sie auf **Bearbeiten**, um die folgenden Einstellungen zu konfigurieren:
   - **Zeitformat:**
     - Wählen Sie diese Option, um die Uhrzeit im 12-Stunden-Format (z. B. 09:00 PM) oder im 24-Stunden-Format (z. B. 21:00 Uhr) anzuzeigen.

> **Hinweis:**
>
> Wählen Sie die Option **Wie lokale Einstellungen**, wenn das Format mit der Zeitzone Ihres Browsers übereinstimmen soll.

- **Datumsformat:**
  - Konfigurieren Sie das Datumsformat so, dass es Ihren Präferenzen entspricht, z. B. JJJJ/MM/TT.

> **Hinweis:**
>
> Wählen Sie die Option **Wie lokale Einstellungen**, wenn das Format mit der Zeitzone Ihres Browsers übereinstimmen soll.

- **Zeitzone:**
  - **UTC:** UTC für die Anzeige von Datum und Uhrzeit in der gesamten Benutzeroberfläche verwenden. Wenn Sie den Mauszeiger über das Feld führen, werden Datum und Uhrzeit Ihrer Zeitzone angezeigt.
  - **Lokale Zeitzone:** Lokale Zeitzone für Datum und Uhrzeit in der gesamten Benutzeroberfläche verwenden. Wenn Sie den Mauszeiger über das Feld führen, werden Datum und Uhrzeit in UTC angezeigt.

## Behandlung von Problemen bei der VDA-Registrierung und beim Sitzungsstart

April 1, 2022

Wir bieten eine Systemintegritätsprüfung, mit der Sie den Zustand von VDAs prüfen können. Mit diesem Feature können Sie Ursachen für häufige Probleme bei der VDA-Registrierung und beim Sitzungsstart über die Verwaltungsoberfläche “Vollständige Konfiguration”identifizieren.

Im Gegensatz zu Cloud Health Check, einem eigenständigen Tool zum Prüfen des Zustands und der Verfügbarkeit der Site und zugehöriger Komponenten, ist das Feature in Form der Aktion **Systemintegritätsprüfung ausführen** in Verwaltungsoberfläche “Vollständige Konfiguration”verfügbar.

Die Aktion **Systemintegritätsprüfung ausführen** kann für dieselben Prüfungen wie Cloud Health Check genutzt werden. Ausnahmen bilden:

- VDA-Registrierung:
  - Verfügbarkeit der VDA-Kommunikationsports

- Sitzungsstarts auf VDAs:
  - Verfügbarkeit der Sitzungsstart-Kommunikationsports
  - VDA-Anwendungsstartpfad

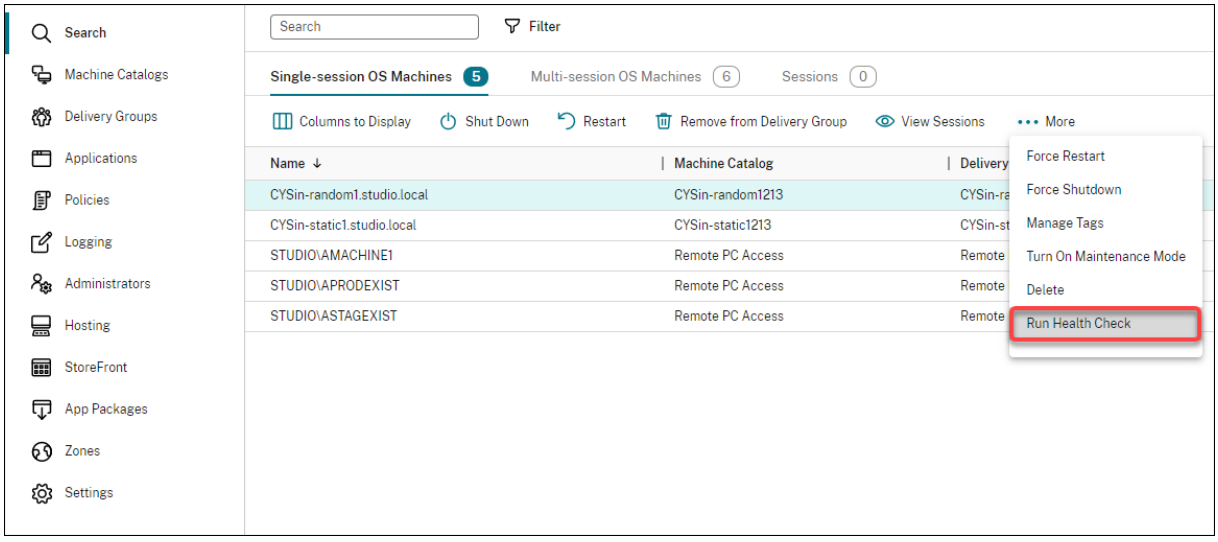
### Voraussetzungen

Bevor Sie das Feature verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Windows-VDAs
- VDA Version 2109 oder später
- VDAs sind registriert

### Durchführen von Integritätsprüfungen an VDAs

1. Rufen Sie in der Verwaltungsoberfläche "Vollständige Konfiguration"den Knoten **Suchen** auf.
2. Wählen Sie eine oder mehrere Maschinen und dann in der Aktionsleiste **Systemintegritätsprüfung ausführen**.




> **Hinweis:**
>
> Derzeit können Sie nur an registrierten VDAs Integritätsprüfungen ausführen. Die Aktion **Systemintegritätsprüfung ausführen** ist für nicht registrierte VDAs nicht verfügbar.

Nachdem Sie **Systemintegritätsprüfung ausführen** ausgewählt haben, wird der Fortschritt der Integritätsprüfungen in einem Fenster angezeigt. Warten Sie, bis die Prüfung abgeschlossen ist, oder

klicken Sie auf **Abbrechen**, um die Prüfung abzubrechen. Bei Bedarf können Sie das Fenster verschieben.

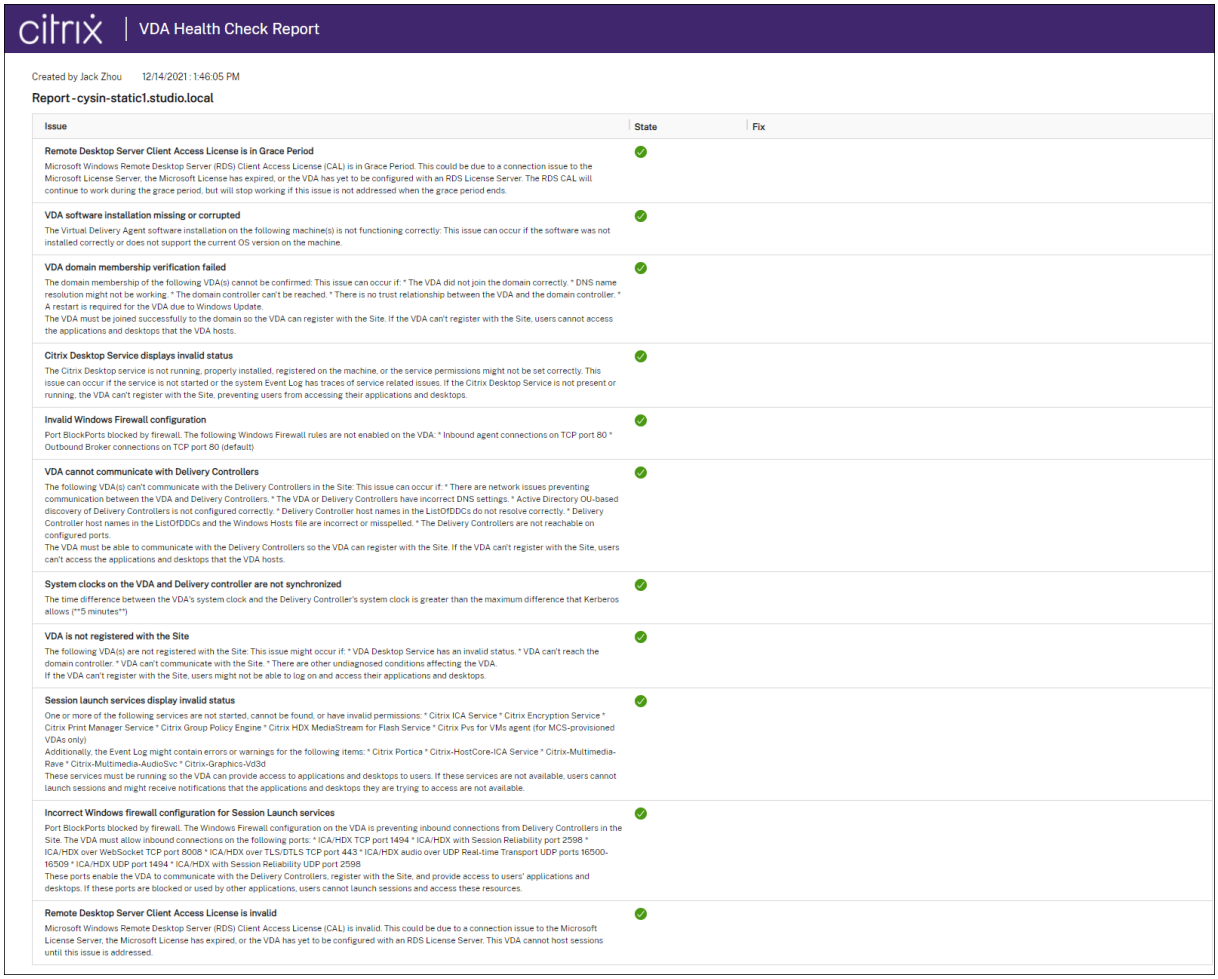

> **Hinweis:**
>
> Wird bereits ein Fenster mit dem Fortschritt einer Integritätsprüfungen angezeigt, können Sie keine weitere Integritätsprüfung ausführen, bis die laufende abgeschlossen ist.

Nach Abschluss der Integritätsprüfungen werden die folgenden beiden Schaltflächen angezeigt: **Bericht anzeigen** und **Schließen**. Um die Ergebnisse der Integritätsprüfung anzuzeigen, klicken Sie auf **Bericht anzeigen**.


Der Bericht wird in einer neuen Browserregisterkarte geöffnet. Der Bericht enthält folgende Elemente:

- Uhrzeit und Datum der Erstellung des Ergebnisberichts
- Ausführende Person
- Auf den Zielmaschinen ausgeführte Prüfungen
- Gefundene Probleme und Empfehlungen zur Fehlerbehebung



citrix | VDA Health Check Report

Created by Jack Zhou 12/14/2021 1:46:05 PM

Report - cysin-static1.studio.local

| Issue | State | Fix |
|---|---|---|
| **Remote Desktop Server Client Access License is in Grace Period**<br>Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends. | ✓ | |
| **VDA software installation missing or corrupted**<br>The Virtual Delivery Agent software installation on the following machine(s) is not functioning correctly: This issue can occur if the software was not installed correctly or does not support the current OS version on the machine. | ✓ | |
| **VDA domain membership verification failed**<br>The domain membership of the following VDA(s) cannot be confirmed: This issue can occur if: * The VDA did not join the domain correctly. * DNS name resolution might not be working. * The domain controller can't be reached. * There is no trust relationship between the VDA and the domain controller. * A restart is required for the VDA due to Windows Update.<br>The VDA must be joined successfully to the domain so the VDA can register with the Site. If the VDA can't register with the Site, users cannot access the applications and desktops that the VDA hosts. | ✓ | |
| **Citrix Desktop Service displays invalid status**<br>The Citrix Desktop service is not running, properly installed, registered on the machine, or the service permissions might not be set correctly. This issue can occur if the service is not started or the system Event Log has traces of service related issues. If the Citrix Desktop Service is not present or running, the VDA can't register with the Site, preventing users from accessing their applications and desktops. | ✓ | |
| **Invalid Windows Firewall configuration**<br>Port BlockPorts blocked by firewall. The following Windows Firewall rules are not enabled on the VDA: * Inbound agent connections on TCP port 80 * Outbound Broker connections on TCP port 80 (default) | ✓ | |
| **VDA cannot communicate with Delivery Controllers**<br>The following VDA(s) can't communicate with the Delivery Controllers in the Site: This issue can occur if: * There are network issues preventing communication between the VDA and Delivery Controllers. * The VDA or Delivery Controllers have incorrect DNS settings. * Active Directory OU-based discovery of Delivery Controllers is not configured correctly. * Delivery Controller host names in the ListOfDDCs do not resolve correctly. * Delivery Controller host names in the ListOfDDCs and the Windows Hosts file are incorrect or misspelled. * The Delivery Controllers are not reachable on configured ports.<br>The VDA must be able to communicate with the Delivery Controllers so the VDA can register with the Site. If the VDA can't register with the Site, users can't access the applications and desktops that the VDA hosts. | ✓ | |
| **System clocks on the VDA and Delivery controller are not synchronized**<br>The time difference between the VDA's system clock and the Delivery Controller's system clock is greater than the maximum difference that Kerberos allows (**5 minutes**) | ✓ | |
| **VDA is not registered with the Site**<br>The following VDA(s) are not registered with the Site: This issue might occur if: * VDA Desktop Service has an invalid status. * VDA can't reach the domain controller. * VDA can't communicate with the Site. * There are other undiagnosed conditions affecting the VDA.<br>If the VDA can't register with the Site, users might not be able to log on and access their applications and desktops. | ✓ | |
| **Session launch services display invalid status**<br>One or more of the following services are not started, cannot be found, or have invalid permissions: * Citrix ICA Service * Citrix Encryption Service * Citrix Print Manager Service * Citrix Group Policy Engine * Citrix HDX MediaStream for Flash Service * Citrix Pvs for VMs agent (for MCS-provisioned VDAs only)<br>Additionally, the Event Log might contain errors or warnings for the following items: * Citrix Portica * Citrix-HostCore-ICA Service * Citrix-Multimedia-Rave * Citrix-Multimedia-AudioSvc * Citrix-Graphics-Vd3d<br>These services must be running so the VDA can provide access to applications and desktops to users. If these services are not available, users cannot launch sessions and might receive notifications that the applications and desktops they are trying to access are not available. | ✓ | |
| **Incorrect Windows firewall configuration for Session Launch services**<br>Port BlockPorts blocked by firewall. The Windows Firewall configuration on the VDA is preventing inbound connections from Delivery Controllers in the Site. The VDA must allow inbound connections on the following ports: * ICA/HDX TCP port 1494 * ICA/HDX with Session Reliability port 2598 * ICA/HDX over WebSocket TCP port 8008 * ICA/HDX over TLS/DTLS TCP port 443 * ICA/HDX audio over UDP Real-time Transport UDP ports 16500-16509 * ICA/HDX UDP port 1494 * ICA/HDX with Session Reliability UDP port 2598<br>These ports enable the VDA to communicate with the Delivery Controllers, register with the Site, and provide access to users' applications and desktops. If these ports are blocked or used by other applications, users cannot launch sessions and access these resources. | ✓ | |
| **Remote Desktop Server Client Access License is invalid**<br>Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is invalid. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. This VDA cannot host sessions until this issue is addressed. | ✓ | |

Sie können Integritätsprüfungen einzeln und in Gruppen durchführen.

> **Hinweis:**
>
> Wenn Sie eine Systemintegritätsprüfung an mehreren Maschinen ausführen, wählen Sie nicht mehr als zehn Maschinen aus. Andernfalls ist die Aktion **Systemintegritätsprüfung ausführen** nicht verfügbar.

## Benutzerzugriff

April 26, 2023

Es gibt zwei primäre Komponenten für den Zugriff auf Anwendungen und Desktops in einer Bereitstellung von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service):

- **Citrix Workspace-Plattform**: Die Citrix Workspace-Plattform ist eine vollständige digitale Lösung, mit der Sie einen sicheren Zugriff auf Informationen bereitstellen, die für Personen in Ihrer

Organisation relevant sind. Benutzer abonnieren die Services, die Sie zur Verfügung stellen und können von überall und auf jedem Gerät darauf zugreifen. Die Citrix Workspace-Plattform unterstützt Sie bei der Organisation und Automatisierung aller notwendigen Details, damit Benutzer gut zusammenzuarbeiten, bessere Entscheidungen treffen und sich ganz auf ihre Arbeit konzentrieren.

Für die Bereitstellung von Citrix Workspace ist kein Aufwand erforderlich und die Bereitstellung wird von Citrix aktualisiert. Die Citrix Workspace-Plattform wird für neue und bestehende Kunden, Vorschauversionen (Previews) und Machbarkeitsstudien empfohlen.

- **On-Premises-StoreFront**: Kunden können auch ein bestehendes StoreFront verwenden, um Anwendungen und Desktops in Citrix Cloud zusammenzufassen. Dies erhöht die Sicherheit, da eine zweistufige Authentifizierung unterstützt wird und Benutzer ihr Kennwort nicht im Cloudservice eingeben. Kunden können zudem ihre Domänennamen und URLs anpassen. Dieser Bereitstellungstyp wird für Citrix Virtual Apps and Desktops-Kunden empfohlen, die StoreFront bereits bereitgestellt haben.

  Siehe auch Lokaler Hostcache und StoreFront.

Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in Citrix Cloud mit Citrix Gateway (früher "NetScaler Gateway") mit SSL gesichert werden. Citrix Gateway oder das virtuelle Citrix VPX-Gerät ist ein SSL-VPN-Gerät, das in der DMZ bereitgestellt wird. Es bietet einen sicheren Einzelzugangspunkt durch die Unternehmensfirewall.

### Verwenden von Citrix Workspace

Der Zugriff auf Workspace erfolgt über `https://<customername>.cloud.com`. Bei Bedarf können Sie den Teil `<customername>` der Workspace-URL anpassen. Anschließend können Sie die Konnektivität für jeden Ressourcenstandort konfigurieren, den Sie verwenden möchten, damit Endbenutzer auf die Ressourcen in ihrem Workspace zugreifen können. Endbenutzer greifen mit der neuesten Version der Citrix Workspace-App auf ihren Workspace zu.

Weitere Informationen zur Verwendung von Citrix Workspace finden Sie unter:

- Konfigurieren von Workspaces: Zum Konfigurieren von Zugriff und Anpassungen.
- Sichere Workspaces: Zum Konfigurieren der Authentifizierung.
- Verwalten der Workspace-Benutzeroberfläche: Beschreibung, wie Endbenutzer auf ihren Workspace zugreifen und wie er angezeigt wird.

Um Endbenutzern Remotezugriff über Citrix Workspace zu gewähren, können Sie entweder den Citrix Gateway Service oder Ihr eigenes Citrix Gateway verwenden.

- Verwenden von Citrix Gateway Service:

1. Wählen Sie unter **Citrix Cloud > Ressourcenstandorte** die Option **Gateway** für den Ressourcenstandort aus, den Sie verwenden möchten.
2. Wählen Sie **Gateway Service** und klicken Sie dann auf **Speichern**.
3. Gehen Sie unter **Citrix Cloud > Workspacekonfiguration > Serviceintegrationen** zum Gateway Service und wählen Sie im Ellipsenmenü die Option **Aktivieren**.

- Verwenden eines eigenen Citrix Gateways:

1. Richten Sie Citrix Gateway als ICA-Proxy ein (keine Authentifizierung oder Sitzungsrichtlinien erforderlich).
2. Konfigurieren Sie einen Ressourcenstandort für Citrix Gateway:
   a) Wählen Sie unter **Citrix Cloud > Ressourcenstandorte** die Option **Gateway** für den Ressourcenstandort aus, den Sie verwenden möchten.
   b) Wählen Sie **Traditionelles Gateway** und geben Sie den externen FQDN ein. Fügen Sie kein Protokoll hinzu. Ports sind optional. Eine Kombination aus Remote- und internem Zugriff wird in Citrix Workspace nicht unterstützt.
3. Binden Sie Citrix Cloud Connectors als STA-Server an Citrix Gateway. Einzelheiten finden Sie unter CTX232640.

> **Hinweis:**
>
> Nur Citrix Cloud Connector-Maschinen werden für die Verwendung als STA-Server mit Citrix Gateway unterstützt. Die Verwendung anderer Connectors als STA-Server, z. B. Connector Appliance, wird nicht unterstützt.

Weitere Informationen zu Citrix Gateway Service und Citrix Gateway finden Sie unter Citrix Gateway.

### Verwenden einer On-Premises-Installation von StoreFront

Informationen zum Konfigurieren einer On-Premises-Bereitstellung von StoreFront finden Sie in der StoreFront-Dokumentation.

Ein bestehendes StoreFront bietet beispielsweise den Vorteil, dass Benutzerkennwörter im Citrix Cloud Connector verschlüsselt werden. Der Cloud Connector verschlüsselt Anmeldeinformationen mit AES-256 und verwendet einen zufällig generierten Einmalschlüssel. Dieser Schlüssel wird direkt an die Citrix Workspace-App zurückgegeben und nie an die Cloud gesendet. Die Citrix Workspace-App stellt ihn beim Sitzungsstart dem VDA bereit, der damit die Anmeldeinformationen entschlüsselt und eine Windows-Anmeldung per Single Sign-On ermöglicht.

- Wählen Sie HTTP und Port 80 für den Datentransport. Die StoreFront-Maschine muss über den angegebenen FQDN direkt auf den Cloud Connector zugreifen können. Der Cloud Connector

muss die Cloud NFuse/STA-URL unter (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` und `ctxsta.dll`) erreichen können.
- Fügen Sie Cloud Connectors als Delivery Controller für hohe Verfügbarkeit hinzu.

Verwenden Sie die jeweils aktuelle Version von StoreFront.

#### Externer Zugriff

Führen Sie folgende Schritte aus, um den externen Zugriff über Citrix Gateway und On-Premises-StoreFront zu ermöglichen:

- Richten Sie Citrix Gateway wie gewöhnlich mit Authentifizierung und Sitzungsrichtlinien ein. Weitere Informationen finden Sie in der Dokumentation zu Citrix Gateway.
- Die Delivery Controller für den On-Premises-StoreFront-Store müssen auf die Citrix Cloud Connectors verweisen. Binden Sie Cloud Connectors als STA-Server an Citrix Gateway.
- Citrix Gateway muss die gleichen STA-URLs wie StoreFront verwenden. Wenn das Gateway nicht bereits für die Verwendung der Secure Ticket Authority (STA) einer vorhandenen Citrix Virtual Apps and Desktops-Umgebung konfiguriert ist, können auch Cloud Connectors als STA verwendet werden.

#### Interner Zugriff

Um internen Zugriff über ein On-Premises-StoreFront bereitzustellen, verweisen Sie die Delivery Controller des On-Premises-StoreFront-Stores auf die Citrix Cloud Connectors.

#### Externer und interner Zugriff

Führen Sie folgende Schritte aus, um den externen und internen Zugriff über Citrix Gateway und On-Premises-StoreFront zu ermöglichen:

- Richten Sie Citrix Gateway wie gewöhnlich mit Authentifizierung und Sitzungsrichtlinien ein. Weitere Informationen finden Sie in der Dokumentation zu Citrix Gateway.
- Binden Sie Cloud Connectors als STA-Server an Citrix Gateway.
- Die Delivery Controller für den On-Premises-StoreFront-Store müssen auf die Cloud Connectors verweisen.

### Lokaler Hostcache und StoreFront

Der lokale Hostcache ermöglicht das fortgesetzte Verbindungsbrokering in einer Citrix DaaS-Bereitstellung, wenn Cloud Connectors nicht mit Citrix Cloud kommunizieren können.

Der lokale Hostcache funktioniert nur bei Ressourcenstandorten mit einer vom Kunden bereitgestellten On-Premises-Installation von StoreFront. Lokaler Hostcache wird für die Verwendung mit Citrix Workspace nicht unterstützt.

Jeder Ressourcenstandort muss über eine vom Kunden bereitgestellte On-Premises-StoreFront-Instanz verfügen. Stellen Sie sicher, dass der Ressourcenstandort eine lokale StoreFront-Bereitstellung enthält, die auf alle Cloud Connectors an diesem Ressourcenstandort verweist.

Weitere Informationen finden Sie unter Lokaler Hostcache.

## Virtuelle IP und virtuelles Loopback

February 17, 2023

> **Wichtig:**
>
> Windows 10 Enterprise-Multisitzungs-OS unterstützt keine IP-Virtualisierung (virtuelle IP) für Remotedesktops und Citrix unterstützt weder virtuelle IPs noch virtuelles Loopback für Windows 10-Multisitzungs-OS.

Virtuelle IPs und virtuelles Loopback werden auf Windows Server 2016-Maschinen unterstützt. Die Features gelten nicht für Windows-Desktopbetriebssystemmaschinen.

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

Einige Anwendungen, z. B. CRM oder CTI, verwenden eine IP-Adresse für die Adressierung, Lizenzierung, Identifizierung und andere Zwecke und erfordern daher eine eindeutige IP-Adresse oder eine Loopbackadresse in Sitzungen. Andere Anwendungen binden sich möglicherweise an einen statischen Port an, sodass das Starten weitere Instanzen einer Anwendung in Mehrbenutzerumgebungen fehlschlägt, da der Port bereits verwendet wird. Damit solche Anwendungen in einer Citrix Virtual Apps-Umgebung richtig ausgeführt werden können, benötigen Sie für jedes Gerät eine eindeutige IP-Adresse.

Virtuelle IP-Adressen und virtuelles Loopback sind unabhängige Features. Sie können ein Feature oder beide wählen.

Zusammenfassung der Administratoraktion:

- Zur Verwendung von Microsoft virtuellen IPs aktivieren und konfigurieren Sie die Funktion auf dem Windows-Server. (Citrix-Richtlinieneinstellungen sind nicht erforderlich.)

- Für die Verwendung von virtuellem Loopback von Citrix konfigurieren Sie zwei Einstellungen in einer Citrix Richtlinie.

## Virtuelle IP

Wenn die virtuelle IP aktiviert und auf dem Windows-Server konfiguriert ist, scheint jede konfigurierte Anwendung, die in einer Sitzung ausgeführt wird, eine eindeutige Adresse zu haben. Benutzer greifen auf diese Anwendungen auf einem Citrix Virtual Apps-Server genauso wie auf andere veröffentlichte Anwendungen zu. Ein Prozess erfordert die virtuelle IP in den folgenden Fällen:

- Der Prozess verwendet eine hartcodierte TCP-Portnummer
- Der Prozess verwendet Windows Sockets und benötigt eine eindeutige IP-Adresse oder eine angegebene TCP-Portnummer

Ermitteln, ob eine Anwendung virtuelle IP-Adressen verwenden muss

1. Beziehen Sie das TCPView-Tool von Microsoft. Das Programm zeigt alle Anwendungen an, die an spezifische IP-Adressen und Ports binden.
2. Deaktivieren Sie das Auflösen von IP-Adressen, sodass statt der Adressen die Hostnamen angezeigt werden.
3. Starten Sie die Anwendung und ermitteln Sie mit TCPView, welche IP-Adressen und Ports von der Anwendung geöffnet werden und welche Prozesse diese Ports öffnen.
4. Konfigurieren Sie alle Prozesse, die die IP-Adresse des Servers, 0.0.0.0 oder 127.0.0.1, öffnen.
5. Starten Sie eine zusätzliche Instanz der Anwendung, um sicherzustellen, dass sie nicht dieselbe IP-Adresse auf einem anderen Port öffnet.

### Funktionsweise der IP-Virtualisierung von Microsoft-Remotedesktop

- Die virtuelle IP-Adressierung muss auf dem Microsoft Server aktiviert sein.

  Beispiel: In einer Umgebung mit Windows Server 2016 erweitern Sie im Server-Manager **Remotedesktopdienste > Remotedesktop-Sitzungshostverbindungen**, um das Remotedesktop-IP-Virtualisierungsfeature zu aktivieren, und konfigurieren Sie die Einstellungen so, dass IP-Adressen dynamisch mit dem DHCP-Server pro Sitzung oder pro Programm zugewiesen werden. Weitere Informationen finden Sie in der Microsoft Dokumentation.

- Nach der Aktivierung des Features fordert der Server beim Sitzungsstart dynamisch zugewiesene IP-Adressen vom DHCP-Server an.
- Das Remotedesktop-IP-Virtualisierungsfeature weist den Remotedesktopverbindungen die IP-Adressen pro Sitzung oder pro Programm zu. Wenn Sie IP-Adressen für mehrere Programme zuweisen, verwenden sie eine gemeine IP-Adresse pro Sitzung.

- Nachdem eine Adresse einer Sitzung zugewiesen wurde, verwendet die Sitzung bei jedem der folgenden Aufrufe die virtuelle Adresse anstelle der primären IP-Adresse für das System: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Wenn das IP-Virtualisierungsfeature von Microsoft in der Hostingkonfiguration der Remotedesktopsitzung verwendet wird, sind Anwendungen an bestimmte IP-Adressen gebunden, indem eine Filterkomponente zwischen die Anwendung und den Winsock-Funktionsaufrufen eingefügt wird. Die Anwendung erkennt dann nur die IP-Adresse, die sie verwenden soll. Sollte die Anwendung versuchen, TCP- oder UDP-Kommunikation abzuhören, wird sie automatisch an die zugewiesene virtuelle IP-Adresse (oder Loopbackadresse) gebunden und alle von der Anwendung geöffneten Ausgangsverbindungen gehen von der an die Anwendung gebundene IP-Adresse aus.

In Funktionen, die eine Adresse ausgeben (z. B. `GetAddrInfo()`, was über eine Windows-Richtlinie gesteuert wird), untersucht die virtuelle IP beim Abrufen der IP-Adresse des lokalen Hosts die zurückgegebene IP-Adresse und ändert sie in die virtuelle IP-Adresse der Sitzung. Anwendungen, die mit solchen Namensfunktionen versuchen, die IP-Adresse des lokalen Servers zu ermitteln, erhalten nur die eindeutige virtuelle IP-Adresse, die der Sitzung zugeordnet wurde. Diese IP-Adresse wird oft in späteren Socket-Aufrufen, wie "Bind"oder "Connect", verwendet. Weitere Informationen zu Windows-Richtlinien finden Sie unter RDS IP Virtualization in Windows Server.

Oft fordern Anwendungen eine Bindung an einen Port zum Abhören der Adresse 0.0.0.0. Wenn eine Anwendung dies versucht und einen statischen Port verwendet, können Sie höchstens eine Instanz der Anwendung starten. Das virtuelle IP-Adressfeature sucht in diesen Aufrufen nach 0.0.0.0 und ändert den Abruf so, dass die angegebene virtuelle IP-Adresse abgehört wird. Dies ermöglicht, dass mehrere Anwendungen denselben Port auf demselben Computer abhören, da sie auf verschiedenen Adressen abhören. Der Aufruf wird nur geändert, wenn er in einer ICA-Sitzungen erfolgt und virtuelle IP-Adressen aktiviert sind. Beispiel: Wenn zwei Instanzen einer Anwendung, die in unterschiedlichen Sitzungen ausgeführt werden, eine Bindung mit allen Schnittstellen (0.0.0.0) und einen bestimmten Port (z. B. 9000) versuchen, werden sie an VIPAddress1:9000 und VIPAddress2:9000 gebunden und es gibt keinen Konflikt.

### Virtuelles Loopback

Bei Aktivierung der Citrix Richtlinieneinstellungen für virtuelles Loopback kann jede Sitzung eine eigene Loopbackadresse für die Kommunikation haben. Wenn eine Anwendung die localhost-Adresse (Standard = 127.0.0.1) in einem Winsock-Aufruf verwendet, ersetzt das virtuelle Loopback einfach 127.0.0.1 durch 127.X.X.X, wobei X.X.X für die Sitzungs-ID + 1 steht. Wenn die Sitzungs-ID zum Beispiel 7 ist, ist die Adresse 127.0.0.8. Im unwahrscheinlichen Fall, dass die Sitzungs-ID größer ist, als im vierten Oktett zulässig (mehr als 255), wird beim nächsten Oktett weitergemacht (127.0.1.0)

bis zum Maximum von 127.255.255.255.

Ein Prozess erfordert das virtuelle Loopback in den folgenden Fällen:

- Der Prozess verwendet die Windows- Sockets-Loopbackadresse (localhost) (127.0.0.1)
- Der Prozess verwendet eine hartcodierte TCP-Portnummer

Verwenden Sie die Richtlinieneinstellungen für virtuelles Loopback für Anwendungen, die eine Loopbackadresse für prozessübergreifende Kommunikation verwenden. Eine zusätzliche Konfiguration ist nicht erforderlich. Virtuelles Loopback ist nicht von virtueller IP abhängig, sodass der Microsoft-Server nicht konfiguriert werden muss.

- Virtuelle IP - Loopbackunterstützung: Wenn diese Richtlinieneinstellung aktiviert ist, kann jede Sitzung eine eigene virtuelle Loopbackadresse haben. Diese Einstellung ist standardmäßig deaktiviert. Das Feature gilt nur für Anwendungen, die mit der Richtlinieneinstellung Virtuelle IP - Programme für virtuelles Loopback angegeben wurden.
- Virtuelle IP - Programme für virtuelles Loopback: Mit dieser Richtlinieneinstellung geben Sie die Anwendung an, die das Feature "Virtuelles IP-Loopback"verwenden. Diese Einstellung gilt nur, wenn die Richtlinieneinstellung Virtuelle IP - Loopbackunterstützung aktiviert ist.

**Verwandtes Feature**

Mit den folgenden Registrierungseinstellungen stellen Sie sicher, dass virtuelles Loopback den Vorrang vor virtuelle IP erhält; dies wird als bevorzugtes Loopback bezeichnet. Achten Sie jedoch auf Folgendes:

- Verwenden Sie bevorzugtes Loopback nur, wenn virtuellen IP-Adressen und das virtuelle Loopback aktiviert sind, sonst erhalten Sie u. U. unerwartete Ergebnisse.
- Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Führen Sie regedit auf den Servern aus, auf dem die Anwendungen installiert sind.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Name: PreferLoopback, Typ: REG_DWORD, Wert: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <Liste der Prozesse>

# Zonen

May 17, 2024

## Einführung

In Citrix DaaS-Bereitstellungen (ehemals Citrix Virtual Apps and Desktops Service), die weit auseinanderliegende Standorte in einem WAN verbinden, kann es zu Latenz- und Zuverlässigkeitsproblemen kommen. Mit Zonen können Benutzer an entfernten Standorten eine Verbindung mit Ressourcen herstellen, ohne dass die Verbindungen durch große WAN-Segmente laufen müssen. In der Citrix DaaS-Umgebung wird jeder Ressourcenstandort als Zone betrachtet.

Zonen können bei Bereitstellungen aller Größen nützlich sein. Mit Zonen können Sie Anwendungen und Desktops näher an den Benutzern ansiedeln und so die Leistung verbessern. Zonen können für die Notfallwiederherstellung, geografisch ferne Datencenter, Zweigstellen, eine Cloud oder eine Verfügbarkeitszone in einer Cloud verwendet werden.

In diesem Artikel bezieht sich der Begriff "lokal"auf die jeweils behandelte Zone. "Ein VDA registriert sich bei einem lokalen Cloud Connector"bedeutet beispielsweise, dass sich der VDA bei einem Cloud Connector in der Zone registriert, in der der VDA ist.

### Unterschiede zu Zonen in on-premises Citrix Virtual Apps and Desktops-Umgebungen

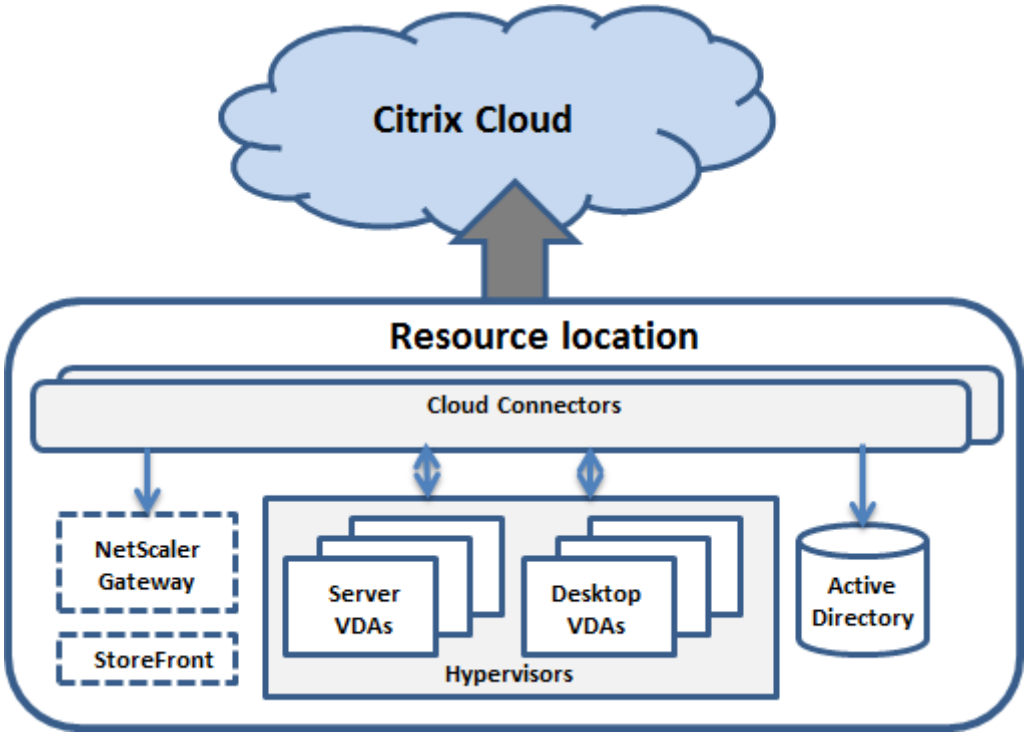
Zonen in einer Citrix DaaS-Umgebung ähneln Zonen in der On-Premises-Version Citrix Virtual Apps and Desktops, sie sind jedoch nicht mit ihnen identisch.

- Im Citrix DaaS werden Zonen automatisch erstellt, wenn Sie einen Ressourcenstandort erstellen und einen Cloud Connector hinzufügen. Im Gegensatz zu einer On-Premises-Bereitstellung werden Zonen in einer Citrix DaaS-Umgebung nicht als primäre Zonen oder Satellitenzonen klassifiziert.
- In XenApp Version 6.5 und früheren Versionen enthielten Zonen Datensammelpunkte. Citrix DaaS verwendet keine Datensammelpunkte für Zonen. Failover und bevorzugte Zonen funktionieren ebenfalls anders in diesem Release.

### Was ist in einer Zone

Eine Zone entspricht einem Ressourcenstandort. Wenn Sie einen Ressourcenstandort erstellen und einen Cloud Connector installieren, wird automatisch eine Zone für Sie erstellt. Jede Zone kann, basierend auf Ihren Anforderungen und Ihrer Umgebung, verschiedene Arten von Ressourcen enthalten.




In jeder Zone muss mindestens ein Cloud Connector installiert sein, für Redundanzzwecke am besten zwei oder mehr.

Sie können Maschinenkataloge, Hypervisors, Hostverbindungen, Benutzer und Anwendungen in eine Zone platzieren. Eine Zone kann auch Citrix Gateway- und StoreFront-Server enthalten. Um das lokale Hostcache-Feature zu verwenden, muss eine Zone über einen StoreFront-Server verfügen.

Zonen werden mit Citrix Workspace und Citrix Gateway Service unterstützt.

Wenn Sie Elemente in einer Zone platzieren, wirkt sich dies auf die Interaktion von Citrix DaaS mit diesen Elementen und den damit verbundenen Objekten aus.

- Wenn eine Hypervisorverbindung in einer Zone platziert wird, wird davon ausgegangen, dass alle über die Verbindung verwalteten Hypervisors in derselben Zone sind.
- Wenn ein Maschinenkatalog in einer Zone platziert wird, wird davon ausgegangen, dass alle VDAs des Katalogs in derselben Zone sind.
- Auch Citrix Gateway-Instanzen können Zonen hinzugefügt werden. Wenn Sie einen Ressourcenstandort erstellen, wird Ihnen die Option zum Hinzufügen eines Citrix Gateways angeboten. Wenn ein Citrix Gateway mit einer Zone verknüpft ist, wird es bevorzugt für Verbindungen mit VDAs in dieser Zone eingesetzt.
- Idealerweise sollte Citrix Gateway in einer Zone für Verbindungen mit Benutzern aus anderen Zonen oder externen Standorten verwendet werden. Es kann jedoch auch für zoneninterne Verbindungen verwendet werden.
- Nach dem Erstellen weiterer Ressourcenstandorte und der Installation von Cloud Connectors (wodurch automatisch weitere Zonen erstellt werden) können Sie Ressourcen zwischen den Zo-

nen verschieben. Diese Flexibilität birgt jedoch das Risiko der Trennung von Elementen, die am besten in unmittelbarer Nähe zueinander funktionieren. Das Verschieben eines Katalogs in eine andere Zone als die zugehörige Verbindung (Host), durch welche die Maschinen in dem Katalog erstellt werden, kann sich beispielsweise negativ auf die Leistung auswirken. Überlegen Sie daher vor dem Verschieben von Elementen zwischen Zonen, ob dies unerwünschte Auswirkungen haben könnte. Kataloge und zugehörige Hostverbindungen müssen in der gleichen Zone sein.

Wenn die Verbindung zwischen einer Zone und der Citrix Cloud ausfällt, kann ein Cloud Connector in der Zone mit dem lokalen Hostcache weiterhin Verbindungen zu VDAs in dieser Zone vermitteln. (In der Zone muss StoreFront installiert sein.) Dies ist beispielsweise an Standorten nützlich, an denen Mitarbeiter über die lokale StoreFront-Site auf ihre lokalen Ressourcen zugreifen, selbst wenn die WAN-Verbindung zwischen dem Standort und dem Unternehmensnetzwerk ausfällt. Weitere Informationen finden Sie unter Lokaler Hostcache.

### VDA-Registrierung

VDAs müssen mindestens die Version 7.7 haben, um die Zonenregistrierungsfunktionen zu verwenden:

- Ein VDA in einer Zone registriert sich bei einem lokalen Cloud Connector.
  - Solange der Cloud Connector mit Citrix Cloud kommunizieren kann, wird der normale Betrieb fortgesetzt.
  - Wenn dieser Cloud Connector funktionsfähig ist, aber nicht mit Citrix Cloud kommunizieren kann, tritt er in den lokalen Hostcache-Ausfallmodus (in der Zone muss eine lokale StoreFront-Bereitstellung sein).
  - Wenn ein Cloud Connector ausfällt, versuchen VDAs in dieser Zone, sich bei anderen lokalen Cloud Connectors zu registrieren. Ein VDA in einer Zone versucht nie, sich bei einem Cloud Connector in einer anderen Zone zu registrieren.
- Wenn Sie für eine Zone einen Cloud Connector hinzufügen oder entfernen (mit dem Citrix Cloud-Verwaltungskonsole) und die automatische Aktualisierung aktiviert ist, erhalten VDAs in dieser Zone aktualisierte Listen der für die Registrierung und für Verbindungen verfügbaren Cloud Connectors.
- Wenn Sie einen Maschinenkatalog (mit der Verwaltungsoberfläche "Vollständige Konfiguration") in eine andere Zone verschieben, registrieren sich die VDAs in diesem Katalog mit Cloud Connectors in der Zone, in die Sie den Katalog verschoben haben. Wenn Sie einen Katalog verschieben, müssen Sie auch alle zugehörigen Hostverbindungen in die gleiche Zone verschieben.
- Während eines Ausfalls (wenn Cloud Connectors in einer Zone nicht mit Citrix Cloud kommunizieren können) sind nur die Ressourcen verfügbar, die mit den in dieser Zone registrierten Maschinen verknüpft sind.

## Zonenpräferenz

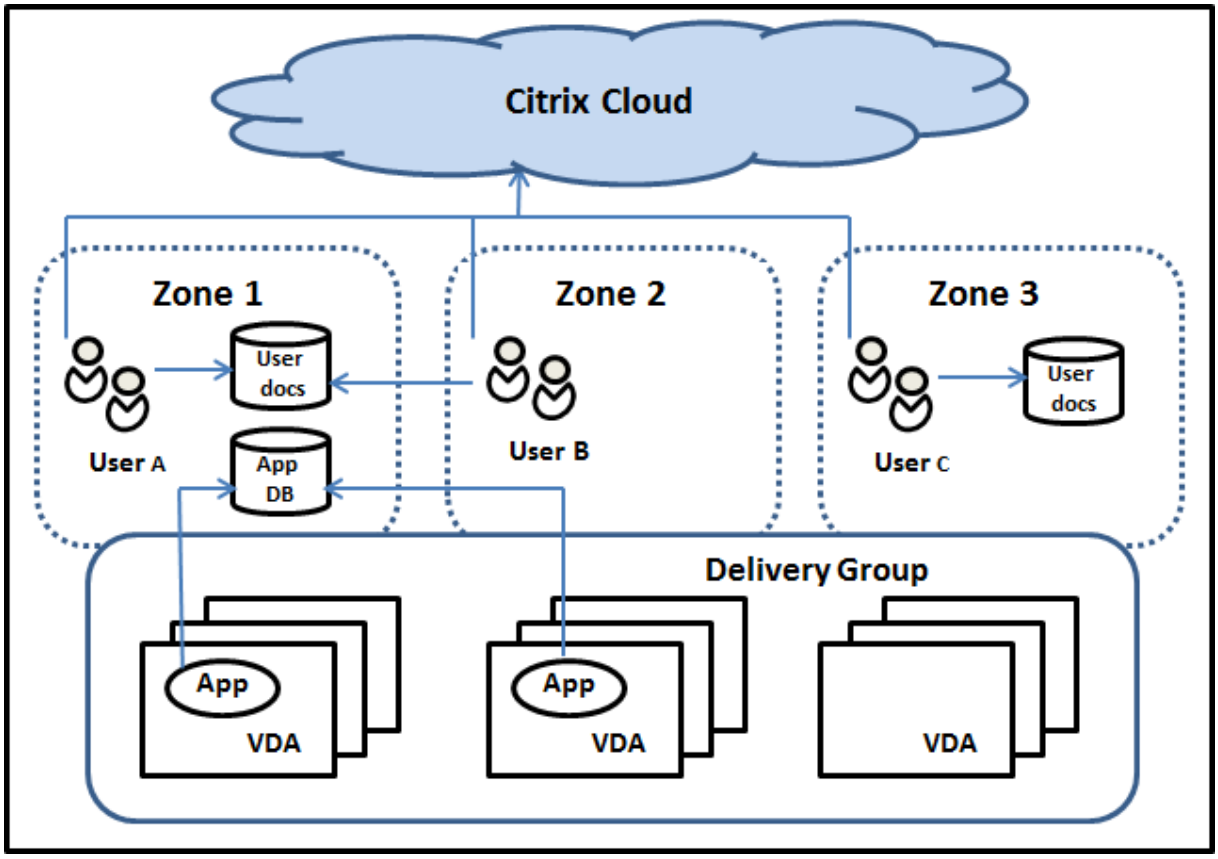
In einer Site mit mehreren Zonen bietet das Zonenpräferenz-Feature Administratoren mehr Flexibilität bei der Steuerung, welcher VDA zum Starten einer Anwendung oder eines Desktops verwendet werden soll.

### Funktionsweise der Zonenpräferenz

Es gibt drei Formen der Zonenpräferenz. Die Präferenz einer Zone zur Verwendung eines spezifischen VDAs kann auf folgenden Parametern basieren:

- Speicherort der Anwendungsdaten. Dies wird als "Anwendungshome"bezeichnet.
- Speicherort der Benutzerstammdaten (Profil oder Stammfreigabe). Dies wird als "Benutzer-home"bezeichnet.
- Aktueller Standort des Benutzers (auf dem die Citrix Workspace-App ausgeführt wird). Dies wird als "Benutzerstandort"bezeichnet. Der Benutzerstandort erfordert mindestens StoreFront 3.7 und Citrix Gateway (ehemals NetScaler Gateway) 11.0-65.x.

Die folgende Abbildung zeigt ein Beispiel für eine Konfiguration mit mehreren Zonen.



In diesem Beispiel sind die VDAs über drei Zonen verteilt, gehören jedoch zur gleichen Bereitstellungsgruppe. Daher hat der Citrix DaaS-Broker möglicherweise mehrere VDAs zur Auswahl für eine Startanforderung des Benutzers. Dieses Beispiel veranschaulicht, dass Benutzer ihre Citrix Workspace-App-Endpunkte an verschiedenen Standorten ausführen können. Benutzer A verwendet ein Gerät mit Citrix Workspace-App in Zone 1. Benutzer B verwendet ein Gerät in Zone 2. In ähnlicher Weise können die Dokumente eines Benutzers an verschiedenen Orten gespeichert sein. Benutzer A und B verwenden eine Freigabe in Zone 1. Benutzer C verwendet eine Freigabe in Zone 3. Für eine der veröffentlichten Anwendungen wird eine Datenbank in Zone 1 verwendet.

Zum Zuordnen eines Benutzers oder einer Anwendung zu einer Zone konfigurieren Sie eine Homezone für den Benutzer bzw. die Anwendung. Der Broker wählt dann anhand dieser Zuordnungen die Zone zum Start einer Sitzung, sofern Ressourcen verfügbar sind. Ihre Aufgaben:

- Sie konfigurieren die Homezone für einen Benutzer, indem Sie diesen einer Zone hinzufügen.
- Sie konfigurieren die Homezone für eine Anwendung durch Bearbeiten der Anwendungseigenschaften.

Ein Benutzer bzw. eine Anwendung kann jeweils nur eine Homezone haben. (Ausnahme sind ggf. Benutzer, die aufgrund von Gruppenmitgliedschaften zu mehreren Zonen gehören. Der Broker verwendet jedoch auch hier nur eine Homezone.)

Es können zwar Zonenpräferenzen für Benutzer und Anwendungen konfiguriert werden, der Broker wählt jedoch für einen Start nur eine bevorzugte Zone. Die Standardpriorität bei der Wahl der bevorzugten Zone ist Anwendungshome > Benutzerhome > Benutzerstandort. Ein Benutzer startet eine Anwendung:

- Wenn für die Anwendung eine Zonenzuordnung konfiguriert ist (= Anwendungshome), wird diese als bevorzugte Zone für die Anwendung verwendet.
- Wenn die Anwendung keine Zonenzuordnung hat, doch für den Benutzer wurde eine konfiguriert (= Benutzerhome), wird diese als bevorzugte Zone verwendet.
- Wenn weder Anwendung noch Benutzer eine Zonenzuordnung haben, wird als bevorzugte Zone diejenige verwendet, in der der Benutzer eine Citrix Workspace-App-Instanz ausführt (Benutzerstandort). Ist diese Zone nicht definiert, werden VDA und Zone nach dem Zufallsprinzip ausgewählt. Beim Lastausgleich werden alle VDAs in der bevorzugten Zone berücksichtigt. Gibt es keine bevorzugte Zone, werden beim Lastausgleich alle VDAs in der Bereitstellungsgruppe berücksichtigt.

#### Anpassen der Zonenpräferenz

Wenn Sie eine Homezone für einen Benutzer oder eine Anwendung konfigurieren oder entfernen, können Sie auch die Anwendung der Zonenpräferenz steuern.

- **Obligatorische Verwendung der Homezone des Benutzers:** In Bereitstellungsgruppen können Sie festlegen, dass Sitzungen in der Homezone von Benutzern (sofern eine existiert) gestartet werden und kein Failover auf andere Zonen erfolgt, wenn in der Homezone keine Ressourcen verfügbar sind. Dadurch können Sie verhindern, dass umfangreiche Profile oder große Datendateien von Zone zu Zone kopiert werden. In diesem Fall wird also eine Sitzung lieber gar nicht gestartet als in einer anderen Zone.
- **Obligatorische Verwendung der Homezone der Anwendung:** Wenn Sie eine Homezone für eine Anwendung konfigurieren, können Sie festlegen, dass die Anwendung nur in dieser Zone gestartet wird und kein Failover auf andere Zonen erfolgt, wenn in der Homezone der Anwendung keine Ressourcen verfügbar sind.
- **Keine Anwendungshomezone und konfigurierte Benutzerhomezone ignorieren:** Wenn Sie keine Homezone für eine Anwendung konfiguriert haben, können Sie auch festlegen, dass jegliche Benutzerhomezonen beim Starten der Anwendung nicht berücksichtigt werden. Verwenden Sie beispielsweise die Zonenpräferenz nach Benutzerstandort, wenn Benutzer eine bestimmte Anwendung auf einem VDA in der Nähe ihrer Maschine ausführen sollen, selbst wenn Benutzer eine andere Homezone haben.

#### Wie bevorzugte Zonen die Sitzungsverwendung beeinflussen

Wenn ein Benutzer eine Anwendung oder einen Desktop startet, bevorzugt der Broker die bevorzugte Zone anstelle der vorhandenen Sitzung.

Wenn ein Benutzer beim Starten einer Anwendung oder eines Desktops bereits eine Sitzung laufen hat, die sich für die gestartete Ressource eignet (die z. B. die Sitzungsfreigabe für eine Anwendung verwenden kann oder die die Ressource bereits ausführt), die Sitzung ist jedoch auf einem VDA in einer anderen als der bevorzugten Zone des Benutzers bzw. der Anwendung, kann eine neue Sitzung erstellt werden. Auf diese Weise erfolgt vorzugsweise der Start in der richtigen Zone (sofern dort Kapazität frei ist), vor der Wiederverbindung mit einer Sitzung in einer für die Sitzungsanforderungen des Benutzers weniger bevorzugten Zone.

Zur Vermeidung verwaister, nicht mehr erreichbarer Sitzungen ist eine Wiederverbindung mit vorhandenen getrennten Sitzungen zulässig, selbst wenn diese in einer nicht bevorzugten Zone sind.

Beim Start gilt für Sitzungen folgende Priorität:

1. Verbindung mit einer vorhandenen Sitzung in der bevorzugten Zone
2. Wiederverbinden mit einer vorhandenen getrennten Sitzung in einer anderen als der bevorzugten Zone.
3. Starten einer neuen Sitzung in der bevorzugten Zone
4. Wiederverbinden mit einer verbundenen Sitzung in einer anderen als der bevorzugten Zone
5. Starten einer neuen Sitzung in einer anderen als der bevorzugten Zone

#### Andere Überlegungen zur Zonenpräferenz

- Wenn Sie eine Homezone für eine Benutzergruppe konfigurieren (z. B. eine Sicherheitsgruppe), werden die (direkten und indirekten) Mitglieder der Gruppe dieser Zone zugeordnet. Da Benutzer jedoch mehreren Sicherheitsgruppen angehören können, können für sie über die Gruppenmitgliedschaft andere Homezonen konfiguriert sein. In solchen Fällen ist die Bestimmung der Homezone nicht eindeutig.

  Wenn für einen Benutzer eine Homezone konfiguriert und nicht per Gruppenmitgliedschaft zugewiesen wurde, so erhält diese Zone den Vorzug. Durch Gruppenmitgliedschaft entstandene Zonenzuordnungen werden dann ignoriert.

  Gibt es für einen Benutzer mehrere Zonenzuordnungen, die ausschließlich durch Gruppenmitgliedschaften entstanden sind, wählt der Broker die Zone nach dem Zufallsprinzip. Die einmal gewählte Zone wird so lange für nachfolgende Sitzungen verwendet, bis sich die Gruppenmitgliedschaft des Benutzers ändert.

- Für die Zonenpräferenz nach Benutzerstandort ist die Erkennung von der Citrix Workspace-App auf dem Endpunktgerät durch das Citrix Gateway erforderlich, über welches das Gerät eine Verbindung herstellt. Der Citrix Gateway muss so konfiguriert sein, dass IP-Adressbereiche bestimmten Zonen zugeordnet werden. Die ermittelte Zonenidentität muss über StoreFront an Citrix DaaS weitergegeben werden.

Der Blogbeitrag Zone Preference Internals enthält relevante technische Details, obwohl er für On-Premises-Zonen geschrieben wurde.

### Berechtigungen zum Verwalten von Zonen

Ein Volladministrator kann alle unterstützten Aufgaben der Zonenverwaltung ausführen. Das Verschieben von Elementen zwischen Zonen erfordert für die Zone selbst lediglich eine Leseberechtigung. Sie benötigen jedoch die Berechtigung zum Bearbeiten der Elemente, die Sie verschieben möchten. Zum Verschieben eines Maschinenkatalogs von einer Zone in eine andere brauchen Sie beispielsweise die Berechtigung zum Bearbeiten des Maschinenkatalogs.

**Mit Citrix Provisioning:** Die aktuelle Citrix Provisioning-Konsole erkennt keine Zonen. Citrix empfiehlt daher, die Oberfläche **Verwalten > Vollständige Konfiguration** zum Erstellen von Maschinenkatalogen zu verwenden, die Sie in bestimmten Zonen platzieren möchten. Nachdem Sie den Katalog erstellt haben, können Sie mit der Citrix Provisioning-Konsole Maschinen in diesem Katalog bereitstellen.

### Zonenerstellung

Wenn Sie in Citrix Cloud einen Ressourcenstandort erstellen und ihm dann einen Cloud Connector hinzufügen, wird in Citrix DaaS automatisch eine Zone erstellt und benannt. Sie können optional später eine Beschreibung hinzufügen.

Nachdem Sie mehrere Ressourcenstandorte (unter automatischer Erstellung der Zonen) erstellt haben, können Sie Ressourcen von einer Zone in eine andere verschieben.

Ressourcenstandorte und Zonen werden regelmäßig synchronisiert (normalerweise ca. alle fünf Minuten). Wenn Sie den Namen eines Ressourcenstandorts in Citrix Cloud ändern, wird diese Änderung innerhalb von fünf Minuten an die zugehörige Zone weitergegeben.

### Hinzufügen oder Ändern einer Zonenbeschreibung

Sie können zwar den Namen von Zonen nicht ändern, Sie können ihnen aber eine Beschreibung hinzufügen oder diese ändern.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Zonen**.
2. Wählen Sie im mittleren Bereich eine Zone und dann in der Aktionsleiste **Zone bearbeiten**.
3. Ändern Sie unter die Beschreibung oder fügen Sie eine hinzu.
4. Wählen Sie **OK** oder **Übernehmen**.

### Verschieben von Ressourcen zwischen Zonen

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Zonen**.
2. Wählen Sie im mittleren Bereich eine Zone und dann ein oder mehrere Elemente.
3. Ziehen Sie das Element in die Zielzone oder wählen Sie in der Aktionsleiste **Elemente verschieben** und geben Sie dann die gewünschte Zielzone an. (Sie können Cloud Connectors zwar auswählen, nicht aber in eine andere Zone verschieben.)

Durch eine Meldung mit einer Liste der ausgewählten Elemente werden Sie aufgefordert, das Verschieben zu bestätigen.

Nicht vergessen: Wenn ein Maschinenkatalog eine Hostverbindung zu einem Hypervisor oder Cloudservice verwendet, müssen Katalog und Verbindung in der gleichen Zone sein. Andernfalls kann die Leistung leiden. Wenn Sie eines dieser Elemente verschieben, verschieben Sie auch das andere.

### Löschen von Zonen

Sie können Zonen nicht löschen. Sie können jedoch einen Ressourcenstandort löschen (nachdem Sie die zugehörigen Cloud Connectors entfernt haben). Durch Löschen des Ressourcenstandorts wird die

Zone automatisch gelöscht.

- Wenn die Zone nichts enthält (z. B. Kataloge, Verbindungen, Anwendungen oder Benutzer), wird sie bei der nächsten Synchronisierung zwischen Zonen und Ressourcenstandorten gelöscht. Die Synchronisierung erfolgt alle fünf Minuten.
- Enthält die Zone Elemente, wird die Zone automatisch gelöscht, nachdem alle Elemente entfernt wurden.

### Hinzufügen einer Homezone für einen Benutzer

Das Konfigurieren einer Homezone für einen Benutzer wird als *Hinzufügen eines Benutzers zu einer Zone bezeichnet*.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Zonen**.
2. Wählen Sie im mittleren Bereich eine Zone und dann in der Aktionsleiste **Benutzer zur Zone hinzufügen**.
3. Wählen Sie **Hinzufügen** im Dialogfeld **Benutzer zur Zone hinzufügen** und wählen Sie dann die Benutzer und Gruppen, die der Zone hinzugefügt werden sollen. Wenn darunter Benutzer sind, die bereits eine Homezone haben, werden zwei Optionen angezeigt: Mit **Ja** werden nur die Benutzer hinzugefügt, die noch keine Homezone haben, bei Auswahl von **Nein** wird wieder das Dialogfeld zur Auswahl der Benutzer angezeigt.
4. Wählen Sie **OK**.

Für Benutzer mit einer Homezone können Sie festlegen, dass Sitzungen nur in der Homezone starten dürfen:

1. Erstellen oder bearbeiten Sie eine Bereitstellungsgruppe.
2. Aktivieren Sie auf der Seite **Benutzer** das Kontrollkästchen **Sitzungen müssen in der Homezone eines Benutzers starten, wenn eine konfiguriert wurde**.

Alle von Benutzern in der Bereitstellungsgruppe gestarteten Sitzungen müssen auf Maschinen in der Homezone des jeweiligen Benutzers gestartet werden. Wenn für einen Benutzer in der Bereitstellungsgruppe keine Homezone konfiguriert ist, hat diese Einstellung keine Auswirkung.

### Entfernen einer Homezone für einen Benutzer

Dieses Verfahren wird auch als Entfernen eines Benutzers aus einer Zone bezeichnet.

1. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Zonen**.
2. Wählen Sie im mittleren Bereich eine Zone und dann in der Aktionsleiste **Benutzer aus Zone entfernen**.

3. Wählen Sie **Entfernen** im Dialogfeld **Benutzer zur Zone hinzufügen**, und wählen Sie dann die Benutzer und Gruppen, die aus der Zone entfernt werden sollen. Mit dieser Aktion werden die Benutzer nur aus der Zone entfernt. Die Benutzer verbleiben in den Bereitstellungsgruppen, denen sie angehören.
4. Bestätigen Sie das Entfernen, wenn Sie dazu aufgefordert werden.

### Verwalten von Homezonen für Anwendungen

Das Konfigurieren einer Homezone für eine Anwendung wird als Hinzufügen einer Anwendung zu einer Zone bezeichnet. Standardmäßig haben Anwendungen in Umgebungen mit mehreren Zonen keine Homezone.

Die Homezone wird in den Anwendungseigenschaften festgelegt. Sie können die Eigenschaften von Anwendungen konfigurieren, wenn Sie die Anwendung einer Gruppe hinzufügen oder zu einem späteren Zeitpunkt.

- Wählen Sie beim Erstellen einer Bereitstellungsgruppe oder beim Hinzufügen von Anwendungen zu vorhandenen Gruppen die Option **Eigenschaften** auf der Seite **Anwendungen** des Assistenten.
- Zum Ändern der Eigenschaften einer Anwendung nach dem Hinzufügen wählen Sie im linken Bereich **Zonen**. Wählen Sie die Anwendung und dann in der Aktionsleiste **Eigenschaften**.

Auf der Seite **Zonen** in den Eigenschaften/Einstellungen der Anwendung:

- Wenn Sie eine Homezone für die Anwendung konfigurieren möchten:
  - Aktivieren Sie in das Optionsfeld **Durch ausgewählte Zone bestimmen, wo die Anwendung gestartet wird** und wählen Sie dann die Zone.
  - Wenn die Anwendung ausschließlich in der ausgewählten Zone gestartet werden soll, aktivieren Sie das Kontrollkästchen unter der Zonenauswahl.
- Wenn Sie keine Homezone für die Anwendung konfigurieren möchten:
  - Aktivieren Sie das Optionsfeld **Keine Homezone für diese Anwendung konfigurieren**.
  - Wenn der Broker beim Start dieser Anwendung keine für Benutzer konfigurierten Homezonen berücksichtigen soll, aktivieren Sie das Kontrollkästchen unterhalb des Optionsfelds. In diesem Fall werden weder für die Anwendung noch für Benutzer konfigurierte Homezonen bei der Wahl des Orts, an dem die Anwendung gestartet wird, berücksichtigt.

### Andere Aktionen, die eine Angabe von Zonen erfordern

Wenn Sie über mehr als eine Zone verfügen, können Sie beim Hinzufügen einer Hostverbindung oder beim Erstellen eines Katalogs eine Zone angeben. Zonen werden in Auswahllisten alphabetisch aufgelistet. Standardmäßig ist der erste Name ausgewählt.

## Problembehandlung

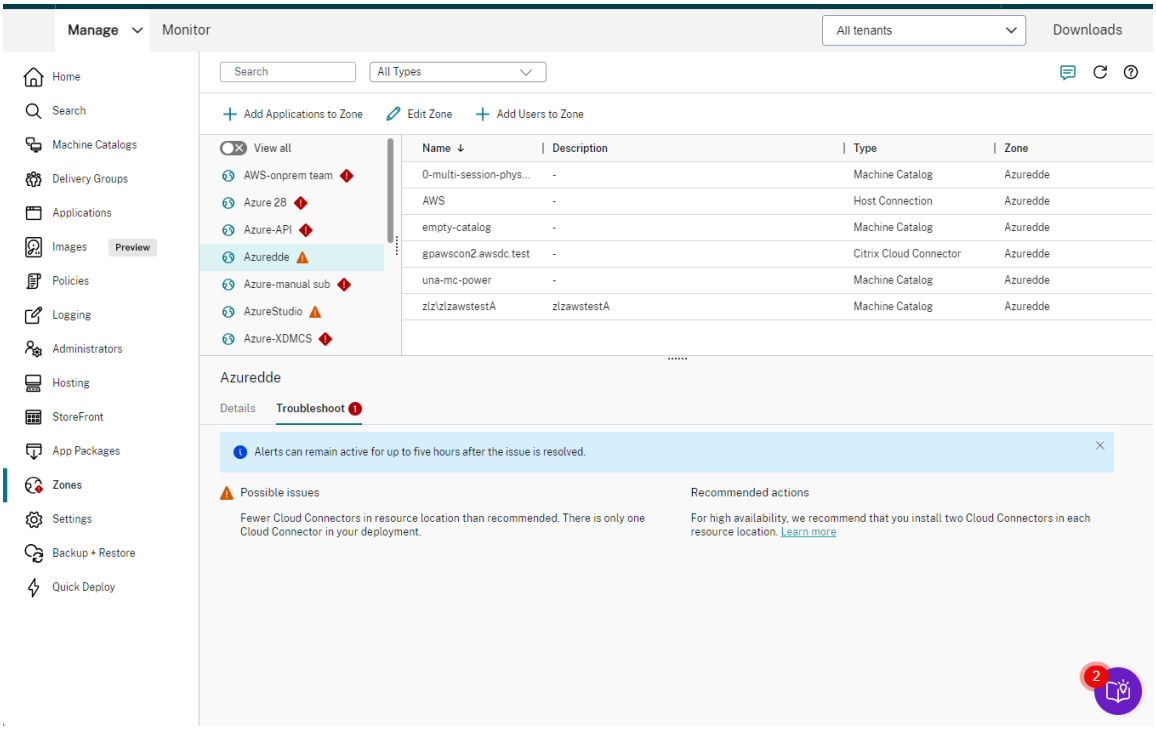
In “Vollständige Konfiguration”werden Sie proaktiv informiert, ob Ihr lokaler Hostcache und Ihre Zonen korrekt konfiguriert sind. Probleme lassen sich dadurch rechtzeitig beheben, bevor sich ein Ausfall auf Benutzer auswirkt. Dieses Feature unterstützt den kontinuierlichen Benutzerzugriff auf unternehmenskritische Workloads.

Für jede Zone mit Problemen wird eine Registerkarte **Problembehandlung** angezeigt.

Führen Sie folgende Schritte aus, um zonenbezogene Probleme zu überprüfen:

1. Navigieren Sie zu **Vollständige Konfiguration > Zonen** und klicken Sie auf die Zone mit dem Warnsymbol.
2. Wählen Sie im unteren Bereich die Registerkarte **Problembehandlung** und lesen Sie die angezeigten Informationen.

> **Hinweis:**
>
> Die Diagnosen werden stündlich aktualisiert.
>
> Beispiel für Hinweise zur Problembehandlung:




Die folgende Tabelle enthält eine Liste aller zonenbezogenen Warnhinweise und Fehlermeldungen:

| Schweregrad | Mögliche Probleme | Empfohlene Aktionen |
|---|---|---|
| Warnung | Der Ressourcenstandort enthält mehrere Domänen. Wenn die Vertrauensstellungen bei einem Ressourcenstandort mit mehreren Domänen nicht ordnungsgemäß konfiguriert sind, kann es länger dauern, bis VDAs registriert sind. Außerdem können VDAs möglicherweise nicht im Hochverfügbarkeitsmodus registriert werden. | Stellen Sie sicher, dass die Vertrauensstellungen zwischen den Domänen an diesem Ressourcenstandort ordnungsgemäß konfiguriert sind. Siehe Technische Daten zu Citrix Cloud Connector. |
| Warnung | Der Ressourcenstandort hat mehr als die empfohlenen Hostverbindungen. Das Überschreiten des Limits kann zu Leistungseinbußen führen und die Benutzererfahrung beeinträchtigen. | Reduzieren Sie die Anzahl der Hostverbindungen am Ressourcenstandort bis zur empfohlenen Obergrenze. Siehe Limits. |
| Warnung | Es sind weniger logische CPU-Prozessoren vorhanden als empfohlen. Im Hochverfügbarkeitsmodus kann es zu Leistungseinbußen kommen. | Stellen Sie sicher, dass die Mindestanforderungen für logische CPU-Prozessoren auf jedem Cloud Connector erfüllt werden. Siehe Lokaler Hostcache. |
| Warnung | Der Ressourcenstandort hat weniger Cloud Connectors als empfohlen. Es gibt nur einen Cloud Connector in Ihrer Bereitstellung. | Für eine hohe Verfügbarkeit empfehlen wir, an jedem Ressourcenstandort zwei Cloud Connectors zu installieren. Siehe Technische Daten zu Citrix Cloud Connector. |
| Warnung | Weniger RAM als empfohlen für mindestens einen Cloud Connector. Im Hochverfügbarkeitsmodus kann es zu Leistungseinbußen kommen. | Stellen Sie sicher, dass jeder Cloud Connector die Mindestanforderungen an den Arbeitsspeicher erfüllt. Siehe Überlegungen zur Skalierung und Größe für Cloud Connectors. |

| Schweregrad | Mögliche Probleme | Empfohlene Aktionen |
| --- | --- | --- |
| Fehler | Der Ressourcenstandort hat mehr als die empfohlenen VDAs. Im Hochverfügbarkeitsmodus lässt der lokale Hostcache nur 10.000 registrierte VDAs zu. Registrierungsversuche von zusätzlichen VDAs schlagen fehl. | Reduzieren Sie die Anzahl der VDAs am Ressourcenstandort bis zur empfohlenen Obergrenze. Siehe Limits. |
| Fehler | Cloud Connectors in der Zone sind nicht erreichbar. Keiner der Cloud Connectors in der Zone kann erreicht werden. VDAs an diesem Ressourcenstandort sind möglicherweise nicht verfügbar, es sei denn, der lokale Hostcache oder Servicekontinuität ist für Ihre Bereitstellung konfiguriert. | Überprüfen Sie die Konnektivität der Cloud Connectors in der Zone und überprüfen Sie in der Registrierung, ob der Modus “Lokaler Hostcache”(LHC) über die Registrierung erzwungen wird. Wenn die Registrierung LHC nicht erzwingt, sollten Sie evtl. das Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung ausführen. Wenn das Problem weiterhin besteht, öffnen Sie ein Support-Ticket. |

## Überwachung

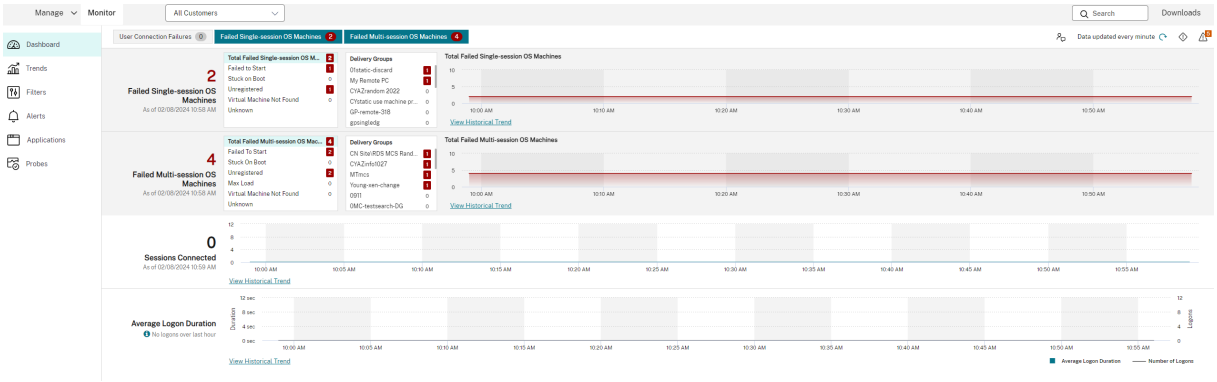
February 21, 2024

Administratoren und Helpdeskmitarbeiter können Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) über die Konsole **Überwachen** kontrollieren und Probleme beheben. Die Registerkarte **Überwachen** bietet ein Dashboard, um den Dienst zu überwachen, Fehler zu beheben und Supportaufgaben für Abonnenten auszuführen.

> **Hinweis:**
>
> Monitor ist als Director-Konsole verfügbar, um Citrix Virtual Apps and Desktops-Bereitstellungen (Aktuelles Release und LTSR) zu überwachen und zu warten.

Melden Sie sich bei **Citrix Cloud** an, um auf die Überwachung zuzugreifen. Wählen Sie im Menü oben links **Meine Dienste > DaaS**. Klicken Sie auf **Überwachen**.




> **Hinweis:**
>
> Die empfohlene optimale Bildschirmauflösung für die Anzeige von Citrix Monitor ist 1440 x 1024.

Monitor bietet folgende Funktionen:

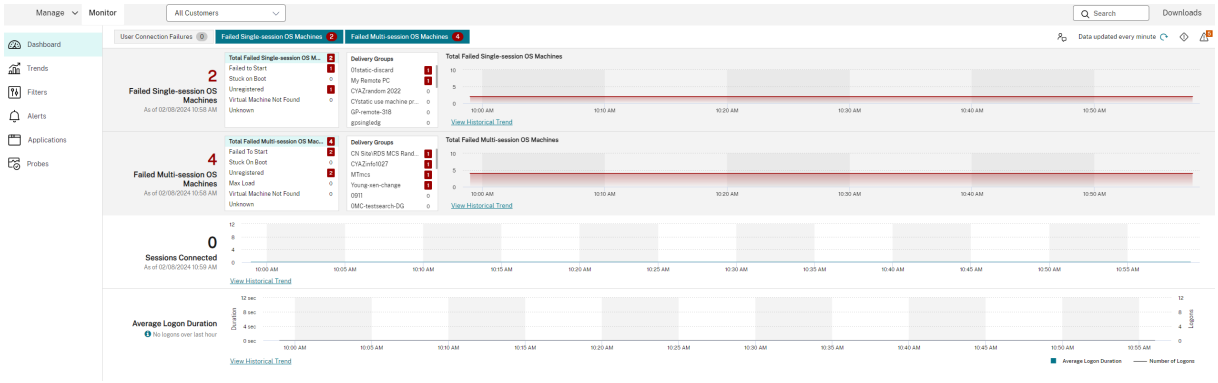
- Echtzeitdaten vom Brokeragent über eine einheitliche Konsole, die mit Analytics und Leistungsverwaltung integriert ist.
- Analytics umfasst eine Leistungsverwaltung zum Sicherstellen von Integrität und Kapazität, sowie historische Trends zum Identifizieren von Engpässen in der Citrix DaaS-Umgebung.
- In der Überwachungsdatenbank gespeicherte historische Daten für den Zugriff auf die Datenbank für die Konfigurationsprotokollierung.
- Übersicht über die Endbenutzererfahrung für virtuelle Anwendungen, Desktops und Benutzer für Citrix DaaS.
- Das Überwachungsdashboard zur Problembehandlung bietet ein Echtzeitmonitoring und historische Daten zur Integrität von Citrix DaaS. Mit diesem Feature können Sie Fehler in Echtzeit sehen und einen besseren Eindruck von der Endbenutzererfahrung erhalten.

## Siteanalyse

March 30, 2024

Das Überwachungsdashboard ermöglicht eine zentralisierte Überwachung der Integrität und Nutzung einer Site.




Wenn es zurzeit keine Fehler gibt und keine Fehler in den letzten 60 Minuten aufgetreten sind, bleiben die Bereiche ausgeblendet. Wenn Fehler auftreten, wird der zugehörige Fehlerbereich automatisch angezeigt.

| Bereich | Beschreibung |
| --- | --- |
| Benutzerverbindungsfehler | Verbindungsfehler während der letzten 60 Minuten. Klicken Sie auf die Kategorien neben der Gesamtzahl zum Anzeigen von Metriken für diesen Fehlertyp. In der nebenstehenden Tabelle wird diese Zahl anhand der einzelnen Bereitstellungsgruppen weiter kategorisiert. Verbindungsfehler umfassen auch solche, die aufgrund von Anwendungslimits auftreten. Weitere Informationen zu Anwendungslimits finden Sie unter Anwendungen. |
| Fehlgeschlagene Maschinen mit Einzelsitzungs-OS und fehlgeschlagene Maschinen mit Multisitzungs-OS | Gesamtzahl der Ausfälle in den letzten 60 Minuten, kategorisiert nach den einzelnen Bereitstellungsgruppen. Fehler unterteilt nach Typ, einschließlich “konnte nicht gestartet werden”, “beim Starten hängen geblieben”und “nicht registriert”. Bei Maschinen mit Multisitzungs-OS wird auch das Erreichen der maximalen Last angegeben. |
| Verbundene Sitzungen | Verbunden Sitzungen in allen Bereitstellungsgruppen in den letzten 60 Minuten. |

| Bereich | Beschreibung |
| --- | --- |
| Durchschnittliche Anmeldedauer | Anmeldedaten für die letzten 60 Minuten. Die große Zahl links ist die durchschnittliche Anmeldedauer während einer Stunde. Anmeldedaten für VDAs vor XenDesktop 7.0 sind nicht in diesem Durchschnitt enthalten. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen. |

> **Hinweis:**
>
> Wenn der von Ihnen verwendete Hosttyp keine bestimmte Metrik unterstützt, wird für diese bestimmte Metrik kein Symbol angezeigt. Beispiel: Für System Center Virtual Machine Manager-, AWS- und CloudStack-Hosts sind keine Integritätsdaten verfügbar.

Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe folgende Abschnitte) fort:

- Steuern der Energiezustände von Benutzermaschinen
- Verhindern von Verbindungen mit Maschinen

### Überwachen von Sitzungen

Wenn eine Sitzung getrennt wird, ist sie immer noch aktiv und ihre Anwendungen werden weiterhin ausgeführt. Das Benutzergerät kommuniziert jedoch nicht mehr mit dem Server.

| Aktion | Beschreibung |
| --- | --- |
| Anzeigen einer zurzeit verbundenen Maschine oder Sitzung des Benutzers | Mit den Ansichten Aktivitätsmanager und Benutzerdetails zeigen Sie die aktuell verbundene Maschine oder Sitzung des Benutzers an. Sehen Sie sich außerdem eine Liste aller Maschinen und Sitzungen an, auf die dieser Benutzer Zugriff hat. Klicken Sie auf das Symbol zum Sitzungswechsel in der Titelleiste des Benutzers, um auf diese Liste zuzugreifen. Weitere Informationen finden Sie unter Wiederherstellen von Sitzungen. |

| Aktion | Beschreibung |
| --- | --- |
| Anzeigen der Gesamtanzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen | Rufen Sie über das Dashboard im Bereich **Verbundene Sitzungen** die Gesamtzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen während der letzten 60 Minuten auf. Klicken Sie dann auf die große Gesamtzahl, wodurch die Filteransicht geöffnet wird. Hier können Sie die grafischen Sitzungsdaten basierend auf ausgewählten Bereitstellungsgruppen und Bereichen sowie der Nutzung von Bereitstellungsgruppen anzeigen. |
| Beenden von Sitzungen im Leerlauf | Die Filteransicht “Sitzungen”enthält Daten für alle aktiven Sitzungen. Sie können die Sitzungen basierend auf dem zugeordneten Benutzer, der Bereitstellungsgruppe, dem Sitzungszustand und der Überschreitung des Leerlauflimits filtern. Wählen Sie aus der gefilterten Liste Sitzungen zum Abmelden oder Trennen. Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen. |
| Anzeigen der Daten über einen längeren Zeitraum | Wählen Sie in der **Trendansicht** die Registerkarte **Sitzungen** aus, um einen Drilldown zu spezifischeren Nutzungsdaten durchzuführen. Sie können Daten für verbundene und getrennte Sitzungen über einen längeren Zeitraum aufschlüsseln. Sie können die Gesamtanzahl der Sitzungen aus einer Periode vor den letzten 60 Minuten einsehen. Klicken Sie zum Anzeigen dieser Informationen auf **Verlaufstrends anzeigen**. |

> **Hinweis:**
>
> Bedenken Sie, dass ein Benutzergerät auf einem älteren Virtual Delivery Agent (VDA) ausgeführt werden kann, z. B. auf einem VDA vor Version 7 oder einem Linux VDA. In diesem Fall kann Monitor keine vollständigen Informationen über die Sitzung anzeigen. Stattdessen wird gemeldet, dass die Informationen nicht verfügbar sind.

**Einschränkung für Desktopzuweisungsregeln:**

Die Verwaltungskonsole ermöglicht die Zuordnung mehrerer Desktopzuweisungsregeln für verschiedene Benutzer oder Benutzergruppen zu einem VDA in einer Bereitstellungsgruppe. In StoreFront wird der zugewiesene Desktop mit dem zugehörigen **Anzeigenamen** gemäß den Desktopzuordnungsregeln für den angemeldeten Benutzer angezeigt. Die Überwachung unterstützt keine Desktopzuordnungsregeln und zeigt den zugewiesenen Desktop unabhängig vom angemeldeten Benutzer unter dem Namen der Bereitstellungsgruppe an. Sie können daher einer Maschine unter "Überwachen"keinen bestimmten Desktop zuordnen.

Sie können den zugewiesenen Desktop, der in StoreFront angezeigt wird, dem Bereitstellungsgruppennamen zuordnen, der in Monitor angezeigt wird. Verwenden Sie für die Zuordnung den folgenden PowerShell-Befehl:

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

Führen Sie den vorgenannten PowerShell-Befehl mit dem Remote PowerShell-SDK aus (Anweisungen hierzu siehe Blog).

### Deaktivieren der Sichtbarkeit von ausgeführten Anwendungen im Aktivitätsmanager

Standardmäßig enthält der Aktivitätsmanager eine Liste aller in einer Benutzersitzung ausgeführten Anwendungen. Alle Administratoren, die Zugriff auf das Feature der Aktivitätsverwaltung haben, können diese Informationen einsehen. Bei delegierten Administratorrollen sind dies Volladministratoren, Bereitstellungsgruppenadministratoren und Helpdeskadministratoren.

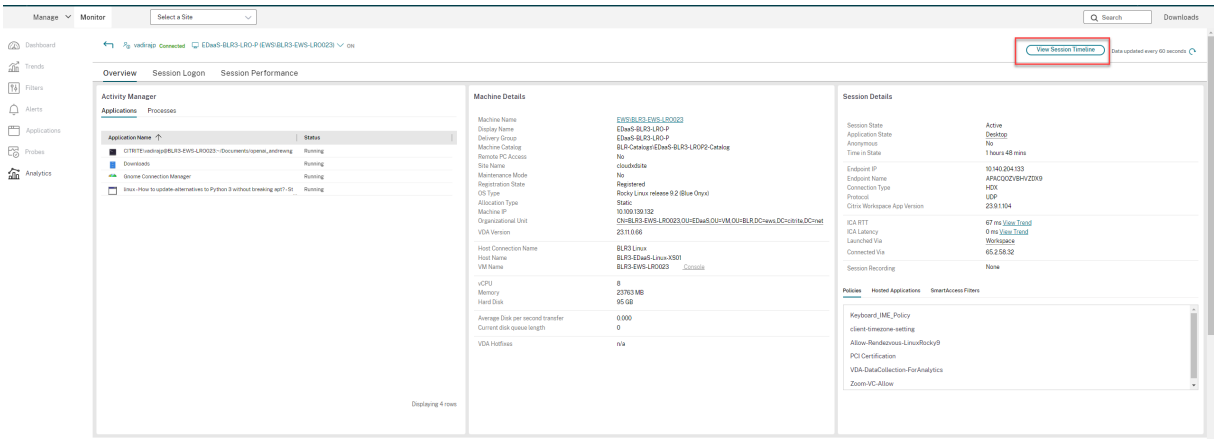
Um Daten zu Benutzern und ihren Anwendungen zu schützen, können Sie die Auflistung der ausgeführten Anwendungen auf der Registerkarte **Anwendungen** deaktivieren. Ändern Sie auf dem VDA den Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. Standardmäßig ist dieser Schlüssel auf 1 eingestellt. Ändern Sie den Wert auf 0, was bedeutet, dass die Informationen nicht auf dem VDA gesammelt und im Aktivitätsmanager angezeigt werden.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### Zugriff auf Sitzungsdetails aus Citrix Analytics für Leistung

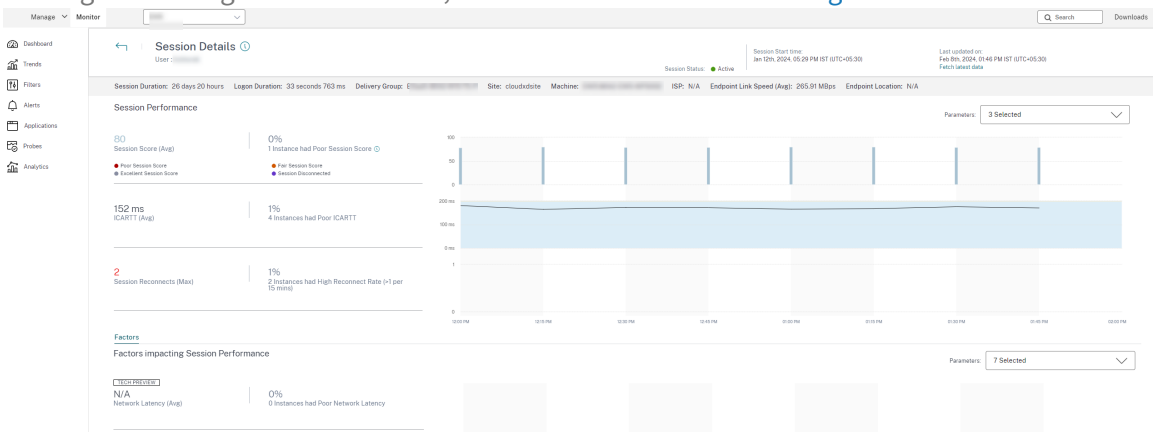
Die Seite “Sitzungsdetails”in Citrix Analytics für Leistung kann in “Überwachen”aufgerufen werden. Klicken Sie im Aktivitätsmanager unter **Sitzungsdetails** auf **Sitzungszeitachse anzeigen**. Die Seite mit den Sitzungsdetails aus “Citrix Analytics für Leistung”wird dann in “Überwachen”geöffnet.




**Hinweis:**

Für dieses Feature benötigen Sie einen gültigen Anspruch auf Citrix Analytics für Leistung.

Sitzungsdetails sind für Sitzungen verfügbar, die in Citrix Analytics für Leistung als “Ausgezeichnet”, “Ausreichend”oder “Schlecht”eingestuft sind. Weitere Informationen dazu, warum eine Sitzung nicht kategorisiert sein kann, finden Sie im Artikel Nicht kategorisiert.



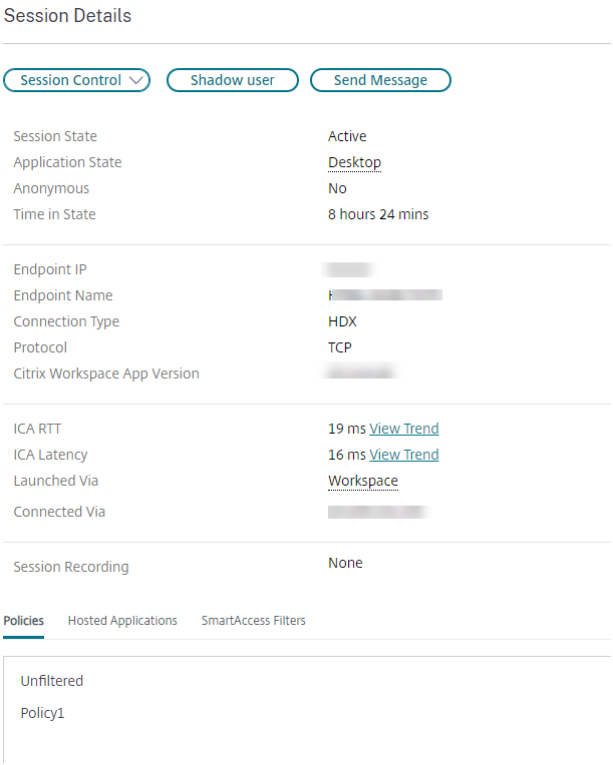

Sie können einen Trend der Sitzungserfahrung für die letzten drei Tage anzeigen. Diese Trendansicht beinhaltet auch die Faktoren, die zur Sitzungserfahrung beitragen. Diese Informationen ergänzen die in “Überwachen”verfügbaren Livedaten, die vom Helpdeskadministrator verwendet werden, um Probleme im Zusammenhang mit der Sitzungserfahrung zu beheben.

Weitere Informationen über die Seite “Sitzungsdetails”finden Sie unter Sitzungsdetails.

### Sitzungstransportprotokoll

Das Transportprotokoll für den HDX-Verbindungstyp der aktuellen Sitzung können Sie im Bereich **Sitzungsdetails** ansehen. Diese Informationen sind für Sitzungen verfügbar, die auf VDAs ab Version 7.13 gestartet wurden.




Verwenden Sie die Dropdownliste **Sitzungssteuerung** im Bereich **Sitzungsdetails**, um sich von einer Sitzung abzumelden oder diese zu trennen.

- **HDX**-Verbindungen:
  - Als Protokoll wird **UDP** angezeigt, wenn EDT für die HDX-Verbindung verwendet wird.
  - Als Protokoll wird **TCP** angezeigt, wenn TCP für die HDX-Verbindung verwendet wird.
- Für **RDP**-Verbindungen wird als Protokoll **Nicht zutreffend** angezeigt.

Wenn der adaptive Transport konfiguriert ist, wechselt das Sitzungstransportprotokoll basierend auf den Netzwerkbedingungen dynamisch zwischen EDT (über UDP) und TCP. Kann die HDX-Sitzung nicht über EDT hergestellt werden, erfolgt ein Fallback auf TCP.

Informationen zum adaptiven Transport und seiner Konfiguration finden Sie unter Adaptiver Transport.

## Exportieren von Berichten

Sie können Trenddaten zum Generieren normaler Auslastungs- und Kapazitätsverwaltungsberichte exportieren. Der Export kann als PDF-, Excel- und CSV-Datei erfolgen. Berichte in PDF- und Excel-Format enthalten Trenddaten in Diagramm- und Tabellenform. Berichte im CSV-Format enthalten tabellarische Daten, die Sie zum Generieren von Ansichten oder zum Archivieren verwenden können.

So exportieren Sie einen Bericht:

1. Rufen Sie die Registerkarte **Trends** auf.
2. Legen Sie Filterkriterien und Zeitraum fest und klicken Sie auf **Anwenden**. Das Trenddiagramm und die Tabelle werden mit Daten aufgefüllt.
3. Klicken Sie auf **Exportieren**, geben Sie einen Namen für den Bericht ein und wählen Sie das Format.

Die Überwachung generiert den Bericht basierend auf den von Ihnen gewählten Filterkriterien. Wenn Sie die Filterkriterien ändern, und klicken Sie auf **Anwenden** und erst dann auf **Exportieren**.

> **Hinweis:**
>
> Das Exportieren großer Datenmengen führt zu einer stark erhöhten CPU- und Speicherauslastung auf dem Überwachungsserver, dem Delivery Controller und den SQL Server-Computern. Die unterstützte Anzahl gleichzeitiger Exportvorgänge und die Menge der exportierbaren Daten sind auf Standardlimits festgelegt, um die optimale Leistung beim Exportieren zu erreichen.

### Unterstützte Limits beim Exportieren

Exportierte PDF- und Excel-Berichte enthalten vollständige Diagramme gemäß den ausgewählten Filterkriterien. Die Tabellendaten sind jedoch in allen Berichtsformaten auf das Standardtabellenzeilenlimit bzw. das Standarddatensatzlimit beschränkt. Die Standardlimits für die Zahl der Datensätze hängen jeweils vom Berichtformat ab.

| Berichtformat | Standardlimit für Datensätze |
|---|---|
| PDF | 500 |
| [Excel] | 100.000 |
| CSV | 100.000 (10.000.000 auf Registerkarte **Sitzungen**) |

#### Fehlerbehandlung

Folgende Fehler können während des Exportvorgangs auftreten:

- **In Director ist ein Timeout aufgetreten:** Dieser Fehler kann aufgrund von Netzwerkproblemen oder einer hohen Ressourcenauslastung auf dem Director-Server oder beim Überwachungsdienst auftreten.
- **Timeout in Überwachungsdienst:** Dieser Fehler kann aufgrund von Netzwerkproblemen oder einer hohen Ressourcenauslastung beim Überwachungsdienst oder auf dem SQL Server-Computer auftreten.
- **Maximum gleichzeitiger Export- oder Vorschauvorgänge in Verarbeitung:** Es kann nur eine Export- oder Vorschauinstanz zu einem bestimmten Zeitpunkt ausgeführt werden. Wenn gemeldet wird, dass das **Maximum gleichzeitiger Export- oder Vorschauvorgänge** überschritten wird, versuchen Sie es später noch einmal.

### Überwachen von Hotfixes

Zum Anzeigen der auf einem bestimmten Maschinen-VDA (physisch oder VM) installierten Hotfixes wählen Sie die Ansicht **Maschinendetails**.

### Steuern der Energiezustände von Benutzermaschinen

Steuern Sie den Zustand der im Überwachungsdienst ausgewählten Maschinen mit den Optionen für die Energieverwaltung. Diese Optionen sind für Maschinen mit Einzelsitzungs-OS verfügbar, aber möglicherweise nicht für Maschinen mit Multisitzungs-OS.

> **Hinweis:**
>
> Diese Funktionen stehen für physische Maschinen und Maschinen, die Remote-PC-Zugriff verwenden, nicht zur Verfügung.

| Befehl | Funktion |
| --- | --- |
| **Neu starten** | Die VM wird ordnungsgemäß heruntergefahren und alle ausgeführten Prozesse werden einzeln angehalten, bevor die VM neu gestartet wird. Wählen Sie diesen Befehl beispielsweise für den Neustart von Maschinen, die unter “Überwachen”mit “Konnten nicht gestartet werden”ausgewiesen werden. |
| **Neustart erzwingen** | Die VM wird neu gestartet, ohne dass sie heruntergefahren wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers und Neuanschließen und Einschalten des Servers. |
| **Herunterfahren** | Die VM wird ordnungsgemäß heruntergefahren Alle ausgeführten Prozesse werden einzeln angehalten. |
| **Herunterfahren erzwingen** | Die VM wird zwingend heruntergefahren, ohne dass das dafür vorgesehene Verfahren durchgeführt wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers. Es werden möglicherweise nicht immer alle ausgeführten Prozesse heruntergefahren, sodass bei diesem Verfahren die Gefahr von Datenverlust besteht. |
| **Anhalten** | Die laufende VM wird im aktuellen Zustand angehalten und dieser Zustand wird in einer Datei im Standardspeicherrepository gespeichert. Diese Option ermöglicht das Herunterfahren der VM auf dem Hostserver und später, nach einem Neustart, die Wiederaufnahme der VM mit dem ursprünglichen Ausführungsstatus. |
| **Fortsetzen** | Nimmt eine angehaltene VM wieder auf und stellt den ursprünglichen Ausführungsstatus wieder her. |
| **Starten** | Startet eine ausgeschaltete VM. |

Sollten die Energieverwaltungsaktionen fehlschlagen, zeigen Sie mit der Maus auf die Warnung und

es wird eine Meldung mit Details zum Fehler angezeigt.

### Verhindern von Verbindungen mit Maschinen

Verwenden Sie den Wartungsmodus, um vorübergehend neue Verbindungen zu verhindern, während der entsprechende Administrator Wartungsaufgaben am Image durchführt.

Wenn Sie den Wartungsmodus auf Maschinen aktivieren, werden keine neuen Verbindungen zugelassen, bis Sie ihn wieder deaktivieren. Wenn Benutzer momentan angemeldet sind, wird der Wartungsmodus erst wirksam, sobald alle Benutzer abgemeldet sind. Benutzer, die sich nicht abmelden, müssen Sie darüber benachrichtigen, dass die Maschine zu einem bestimmten Zeitpunkt heruntergefahren wird. Sie können die Energieverwaltung verwenden, um das Herunterfahren der Maschinen zu erzwingen.

1. Wählen Sie die Maschine aus, z. B. auf der Ansicht Benutzerdetails, oder eine Gruppe von Maschinen in der Ansicht Filter.
2. Klicken Sie auf **Wartungsmodus** und aktivieren Sie die Option.

Wenn ein Benutzer versucht, eine Verbindung zu einem zugewiesenen Desktop herzustellen, während er im Wartungsmodus ist, wird eine Meldung angezeigt, dass der Desktop nicht verfügbar ist. Es können keine neuen Verbindungen hergestellt werden, bis der Wartungsmodus deaktiviert wird.

### Anwendungsanalyse

Auf der Registerkarte **Anwendungen** werden konsolidierte Anwendungsdaten zur effizienten Analyse und Verwaltung der Anwendungsleistung angezeigt. Sie erhalten hier wertvolle Einblicke in die Integrität und Nutzung aller in der Site veröffentlichten Anwendungen. Metriken der folgenden Art werden angezeigt:

- Testergebnisse
- Anzahl der Instanzen pro Anwendung
- Störungen und Fehler im Zusammenhang mit den veröffentlichten Anwendungen

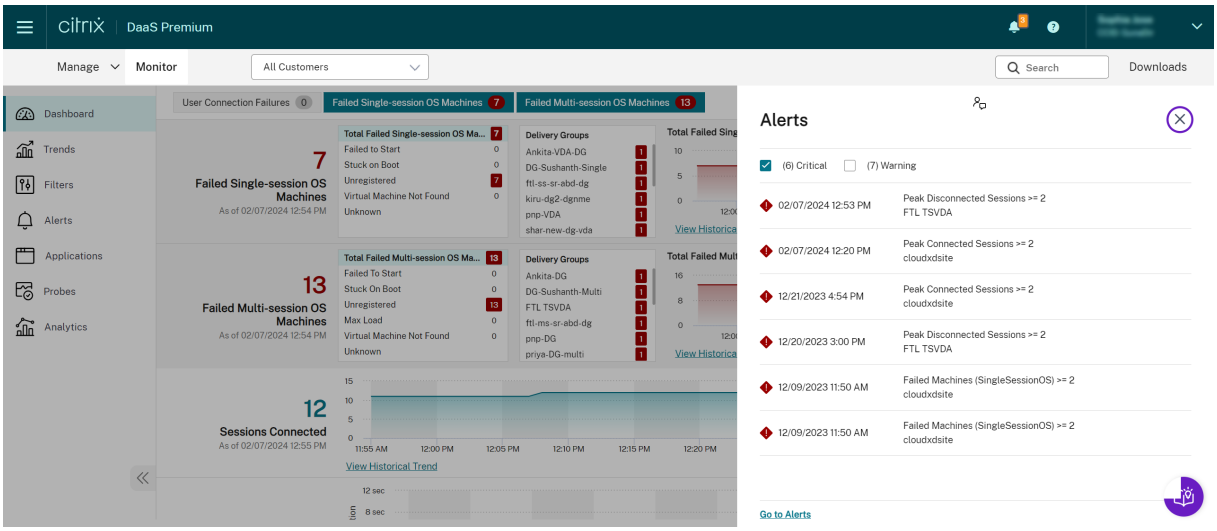
Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen im Abschnitt **Anwendungsanalyse**.

## Warnungen und Benachrichtigungen

February 21, 2024

Unter “Überwachen”werden im Dashboard und in anderen Ansichten der oberen Ebene Warnungen und kritische Warnungen mit entsprechenden Symbolen angezeigt. Die Anzeige von Warnungen wird jede Minute automatisch aktualisiert und kann bei Bedarf auch manuell aktualisiert werden.

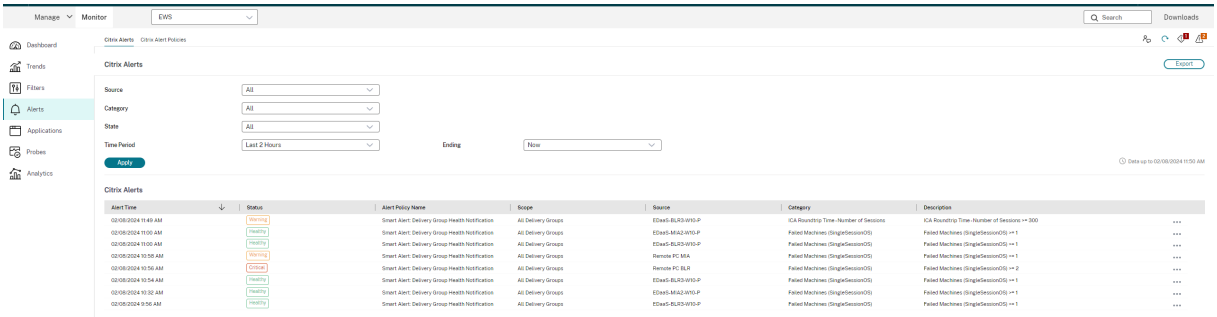



Eine Warnung (gelbes Dreieck) zeigt an, dass der Schwellenwert einer Bedingung erreicht oder überschritten wurde.

Eine kritische Warnung (roter Kreis) zeigt an, dass der kritische Schwellenwert einer Bedingung erreicht oder überschritten wurde.

Sie können detaillierte Informationen zu Warnungen anzeigen, indem Sie eine Warnung in der Seitenleiste auswählen und unten in der Seitenleiste auf **Warnungen** oder oben auf der Seite “Überwachen” auf **Warnungen** klicken.

In der Ansicht “Warnungen”können Sie Warnungen filtern und exportieren. Beispielsweise können Sie fehlerhafte Maschinen mit Multisitzungs-OS für eine bestimmte Bereitstellungsgruppe im vergangenen Monat oder alle Warnungen für einen bestimmten Benutzer anzeigen. Weitere Informationen finden Sie unter Exportieren von Berichten.



## Citrix Warnungen

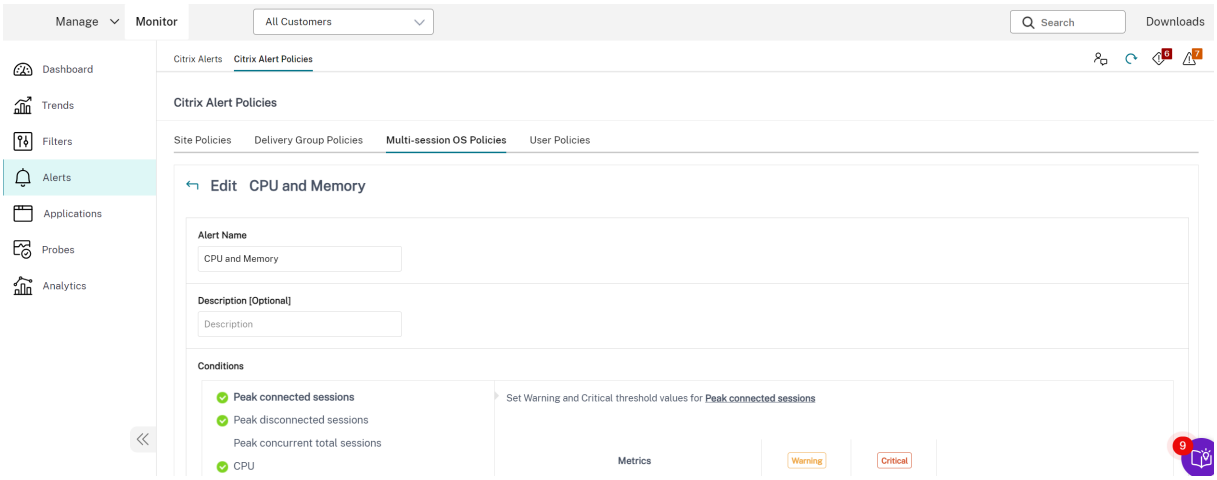
Citrix Warnungen stammen von Citrix Komponenten. Sie können Citrix Warnungen unter "Überwachen"über **Warnungen** > **Citrix Benachrichtigungsrichtlinie** konfigurieren. Im Rahmen der Konfiguration können Sie den Versand von Benachrichtigungen per E-Mail an Personen und Gruppen festlegen, wenn die Schwellenwerte überschritten werden. Weitere Informationen zum Einrichten von Citrix Warnungen finden Sie unter Erstellen von Benachrichtigungsrichtlinien.

## Intelligente Benachrichtigungsrichtlinien

Eine Reihe integrierter Benachrichtigungsrichtlinien mit vordefinierten Schwellenwerten ist für Bereitstellungsgruppen und Multisitzungs-OS-VDAs verfügbar. Sie können die Schwellenwertparameter der integrierten Benachrichtigungsrichtlinien unter **Warnungen** > **Citrix Benachrichtigungsrichtlinie** ändern.
Diese Richtlinien werden erstellt, wenn mindestens ein Warnungsziel –eine Bereitstellungsgruppe oder ein Multisitzungs-OS-VDA –in der Site vorhanden ist. Außerdem werden integrierte Benachrichtigungsrichtlinien automatisch neuen Bereitstellungsgruppen und Multisitzungs-OS-VDAs hinzugefügt.

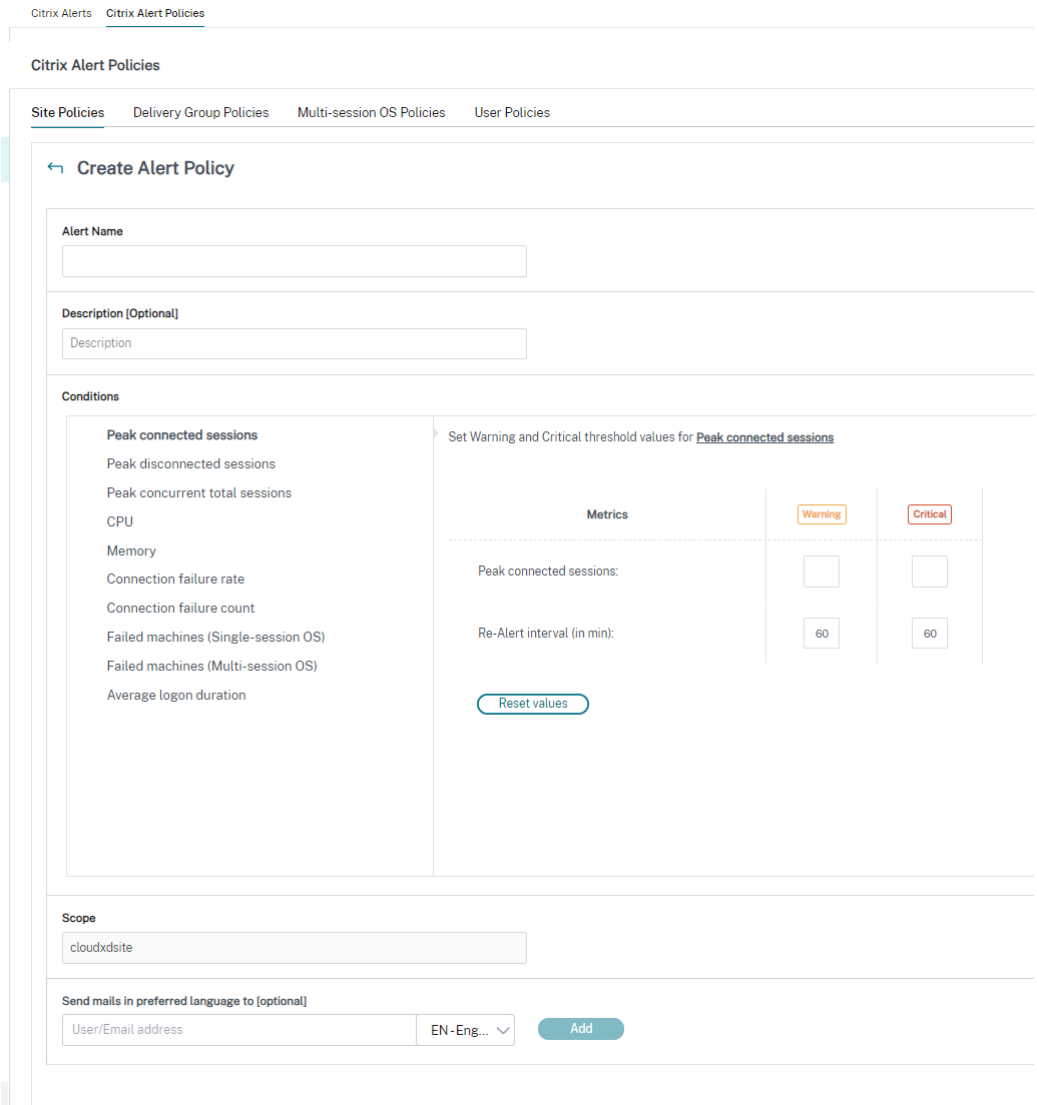
Integrierte Benachrichtigungsrichtlinien werden nur erstellt, wenn die Überwachungsdatenbank keine entsprechenden Warnmeldungsregeln enthält.

Informationen zu den Schwellenwerten der integrierten Benachrichtigungsrichtlinien finden Sie unter Bedingungen für Benachrichtigungsrichtlinien.



## Erstellen von Benachrichtigungsrichtlinien




Gehen Sie zum Erstellen einer Benachrichtigungsrichtlinie, z. B. zum Generieren einer Warnung bei Eintreten bestimmter Sitzungszahlbedingungen, folgendermaßen vor:

1. Gehen Sie zu **Warnungen**> **Citrix Benachrichtigungsrichtlinie** und wählen Sie beispielsweise “Multisitzungs-OS-Richtlinie”aus.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein und legen Sie die Bedingungen zum Auslösen der Warnung fest. Geben Sie beispielsweise für die Kategorie “Warnung” und “Kritisch”Werte für “Max. verbundener Sitzungen”, “Max. getrennter Sitzungen”und “Max. gleichzeitiger Sitzungen insgesamt”ein. Die Werte der Kategorie “Warnung”dürfen nicht größer sein als die der Kategorie “Kritisch”. Weitere Informationen finden Sie unter Bedingungen für Benachrichtigungsrichtlinien.

4. Legen Sie das Wiederholungsintervall fest. Wenn die Bedingungen für die Warnung weiterhin erfüllt sind, wird die Warnung nach diesem Zeitintervall neu ausgelöst und es wird, sofern dies in der Benachrichtigungsrichtlinie so festgelegt ist, eine E-Mail-Benachrichtigung generiert. Wird eine Warnung geschlossen, wird nach dem Warnmeldungsintervall keine E-Mail-Benachrichtigung generiert.
5. Legen Sie den Bereich fest. Wählen Sie beispielsweise eine Bereitstellungsgruppe.
6. Geben Sie in den Benachrichtigungseinstellungen an, wer per E-Mail benachrichtigt werden soll, wenn die Warnung ausgelöst wird. E-Mail-Benachrichtigungen werden über SendGrid gesendet. Stellen Sie sicher, dass die E-Mail-Adresse `donotreplynotifications@citrix.com` in Ihrer E-Mail-Bereitstellung auf der Positivliste steht.
7. Klicken Sie auf **Speichern**.

Wird eine Richtlinie mit einem Bereich von 20 oder mehr Bereitstellungsgruppen erstellt, kann es ca. 30 Sekunden dauern, bis die Konfiguration abgeschlossen ist. Während dieses Zeitraums wird ein Drehfeld angezeigt.

Wenn Sie mehr als 50 Richtlinien für bis zu 20 eindeutige Bereitstellungsgruppen (insgesamt 1000 Bereitstellungsgruppenziele) erstellen, nimmt die Reaktionszeit u. U. um mehr als 5 Sekunden zu.

Verschieben einer Maschine mit aktiven Sitzungen von einer Bereitstellungsgruppe in eine andere löst u. U. fälschlicherweise Bereitstellungsgruppenwarnungen aus, die mit Maschinenparametern definiert wurden.

> **Hinweis:**
> Wenn Sie eine Warnmeldungsrichtlinie löschen, kann es bis zu 30 Minuten dauern, bis die Richtlinie aufhört, Warnmeldungen zu generieren.

## Bedingungen für Benachrichtigungsrichtlinien

Nachfolgend werden die Warnmeldungskategorien, empfohlene Maßnahmen zur Problembehandlung und Bedingungen für integrierte Richtlinien (sofern definiert) aufgeführt. Die integrierten Benachrichtigungsrichtlinien sind für Warnungsintervalle von 60 Minuten definiert.

### Max. verbundener Sitzungen

- Prüfen Sie die Maximalzahl verbundener Sitzungen in der Trendansicht unter “Überwachen”.
- Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist.
- Fügen Sie, falls erforderlich, neue Maschinen hinzu.

### Max. getrennter Sitzungen

- Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht unter “Überwachen”.

- Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist.
- Fügen Sie neue Maschinen hinzu, falls erforderlich.
- Melden Sie getrennte Sitzungen, falls erforderlich, ab.

#### Max. gleichzeitiger Sitzungen insgesamt

- Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht unter "Überwachen".
- Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist.
- Fügen Sie neue Maschinen hinzu, falls erforderlich.
- Melden Sie getrennte Sitzungen, falls erforderlich, ab.

#### CPU

Der Prozentsatz der CPU-Auslastung umfasst die gesamte Auslastung auf dem VDA, einschließlich Prozesse. Detaillierte Informationen zur CPU-Auslastung durch einzelne Prozesse erhalten Sie auf der Seite **Maschinendetails** des jeweiligen VDAs.

- Rufen Sie hierzu **Maschinendetails > Historische Auslastung anzeigen > Top-10-Prozesse** auf. Die Prozessüberwachungsrichtlinie muss aktiviert sein, damit die Ressourcennutzung auf Prozessebene erfasst wird.
- Beenden Sie, falls erforderlich, den Prozess.
- Beim Beenden des Prozesses gehen nicht gespeicherte Daten verloren.
- Funktioniert alles erwartungsgemäß, fügen Sie zusätzliche CPU-Ressourcen künftig hinzu.

> **Hinweis:**
>
> Die Richtlinieneinstellung **Ressourcenüberwachung aktivieren** ist auf Maschinen mit VDAs standardmäßig zur Überwachung von CPU- und Arbeitsspeicherleistungsindikatoren zugelassen. Wenn diese Richtlinie deaktiviert wird, werden keine Warnungen über CPU- und Arbeitsspeicherbedingungen ausgelöst. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.

**Bedingungen für intelligente Benachrichtigungsrichtlinien:**

- **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
- **Schwellenwerte:** Warnung - 80 %, Kritisch - 90 %

#### Speicher

Der Prozentsatz der Speicherauslastung umfasst die gesamte Auslastung auf dem VDA, einschließlich Prozesse. Detaillierte Informationen zur Speicherauslastung durch einzelne Prozesse erhalten Sie auf

der Seite **Maschinendetails** des jeweiligen VDAs.

- Rufen Sie hierzu **Maschinendetails > Historische Auslastung anzeigen > Top-10-Prozesse** auf. Die Prozessüberwachungsrichtlinie muss aktiviert sein, damit die Ressourcennutzung auf Prozessebene erfasst wird.
- Beenden Sie, falls erforderlich, den Prozess.
- Beim Beenden des Prozesses gehen nicht gespeicherte Daten verloren.
- Funktioniert alles erwartungsgemäß, fügen Sie zusätzlichen Arbeitsspeicher künftig hinzu.

> **Hinweis:**
>
> Die Richtlinieneinstellung **Ressourcenüberwachung aktivieren** ist auf Maschinen mit VDAs standardmäßig zur Überwachung von CPU- und Arbeitsspeicherleistungsindikatoren zugelassen. Wenn diese Richtlinie deaktiviert wird, werden keine Warnungen über CPU- und Arbeitsspeicherbedingungen ausgelöst. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.

**Bedingungen für intelligente Benachrichtigungsrichtlinien:**

- **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
- **Schwellenwerte:** Warnung - 80 %, Kritisch - 90 %

#### Verbindungsfehlerrate

Verbindungsfehler während der letzten Stunde in Prozent.

- Verhältnis der Summe aller Fehler zur Summe aller Verbindungsversuche.
- Überprüfen Sie unter "Überwachen"die Trendansicht zu Verbindungsfehlern auf Ereignisse aus dem Konfigurationsprotokoll.
- Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind.

#### Anzahl Verbindungsfehler

Zahl der Verbindungsfehler während der letzten Stunde.

- Überprüfen Sie unter "Überwachen"die Trendansicht zu Verbindungsfehlern auf Ereignisse aus dem Konfigurationsprotokoll.
- Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind.

#### ICA RTT (Durchschnitt)

Durchschnittliche ICA-Roundtripzeit.

- Überprüfen Sie die Aufschlüsselung der ICA-Roundtripzeit in Citrix ADM, um die Ursache zu finden. Weitere Informationen finden Sie in der Dokumentation zu Citrix ADM.
- Wenn Citrix ADM nicht verfügbar ist, überprüfen Sie unter "Überwachen"die ICA-Roundtripzeit und die Latenz in der Ansicht "Benutzerdetails", um festzustellen, ob es sich um ein Netzwerkproblem oder ein Problem mit Anwendungen oder Desktops handelt.

#### ICA RTT (Anzahl an Sitzungen)

Anzahl der Sitzungen, die den Schwellenwert für die ICA-Roundtripzeit überschreiten

- Überprüfen Sie in Citrix ADM, wie viele Sitzungen eine hohe ICA-Roundtripzeit haben. Weitere Informationen finden Sie in der Dokumentation zu Citrix ADM.
- Wenn Citrix ADM nicht verfügbar ist, verständigen Sie zum Suchen der Ursache das Netzwerkteam.

  **Bedingungen für intelligente Benachrichtigungsrichtlinien:**

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 300 ms für 5 oder mehr Sitzungen, Kritisch - 400 ms für 10 oder mehr Sitzungen

#### ICA RTT (% der Sitzungen)

Prozentanteil der Sitzungen, die die durchschnittliche ICA-Roundtripzeit überschreiten

- Überprüfen Sie in Citrix ADM, wie viele Sitzungen eine hohe ICA-Roundtripzeit haben. Weitere Informationen finden Sie in der Dokumentation zu Citrix ADM.
- Wenn Citrix ADM nicht verfügbar ist, verständigen Sie zum Suchen der Ursache das Netzwerkteam.

#### ICA RTT (Benutzer)

ICA-Roundtripzeit für Sitzungen, die von dem angegebenen Benutzer gestartet werden Die Warnung wird ausgelöst, wenn die ICA-Roundtripzeit den Schwellenwert bei mindestens einer Sitzung überschreitet.

#### Fehlerhafte Maschinen (Einzelsitzungs-OS)

Anzahl fehlerhafter Maschinen mit Einzelsitzungs-OS. Fehler können verschiedene Ursachen haben, die im Überwachungsdashboard oder in gefilterten Ansichten angezeigt werden.

- Führen Sie eine Ursachendiagnose mit Citrix Scout durch. Weitere Informationen finden Sie unter Behandeln von Benutzerproblemen.

  **Bedingungen für intelligente Benachrichtigungsrichtlinien:**

  - **Bereich:** Bereitstellungsgruppe
  - **Schwellenwerte:** Warnung - 1, Kritisch - 2

#### Fehlerhafte Maschinen (Multisitzungs-OS)

Anzahl fehlerhafter Maschinen mit Multisitzungs-OS. Fehler können verschiedene Ursachen haben, die im Überwachungsdashboard oder in gefilterten Ansichten angezeigt werden.

- Führen Sie eine Ursachendiagnose mit Citrix Scout durch.

  **Bedingungen für intelligente Benachrichtigungsrichtlinien:**

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 1, Kritisch - 2

#### Fehlerhafte Maschinen (%)

Prozentsatz fehlerhafter Maschinen für Einzel- und Multisitzungs-OS in einer Bereitstellungsgruppe, basierend auf der Anzahl fehlerhafter Maschinen. Der Wert wird alle 30 Sekunden berechnet und erlaubt das Konfigurieren von Schwellenwerten für Warnungen als Prozentsatz fehlerhafter Maschinen in einer Bereitstellungsgruppe.
Fehler können aus verschiedenen Gründen auftreten und werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch. Weitere Informationen finden Sie unter Behandeln von Benutzerproblemen.

#### Durchschnittliche Anmeldedauer

Durchschnittliche Dauer der Anmeldungen in der letzten Stunde

- Überprüfen Sie im Überwachungsdashboard die aktuellen Daten zur Anmeldedauer. Melden sich viele Benutzer innerhalb kurzer Zeit an, kann die Anmeldung länger dauern.

- Überprüfen Sie Baseline und Aufschlüsselung der Anmeldungen zur Ursachenfindung. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

  **Bedingungen für intelligente Benachrichtigungsrichtlinien:**

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 45 Sekunden, Kritisch - 60 Sekunden

#### Anmeldedauer (Benutzer)

Dauer der Anmeldungen des angegebenen Benutzers in der letzten Stunde.

#### Lastauswertungsprogrammindex

Wert des Lastauswertungsprogrammindex der letzten 5 Minuten.

- Suchen Sie unter "Überwachen"nach Maschinen mit Multisitzungs-OS, die mit Spitzenlast ausgeführt werden. Zeigen Sie das Dashboard (Fehler) und die Trendansicht für den Lastauswertungsprogrammindex an.

  **Bedingungen für intelligente Benachrichtigungsrichtlinien:**

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 80 %, Kritisch - 90 %

### Überwachen von Hypervisorwarnungen

Unter "Überwachen"werden Warnungen zur Überwachung des Hypervisorstatus angezeigt. Warnungen von Citrix Hypervisor und VMware vSphere helfen bei der Überwachung von Hypervisorparametern und -zuständen. Der Hypervisor-Verbindungsstatus wird ebenfalls überwacht und eine Warnung generiert, wenn der Hostcluster bzw. -pool neu gestartet wird oder nicht verfügbar ist.

Um Hypervisorwarnungen zu erhalten, muss auf der Registerkarte "Verwalten"eine Hostingverbindung erstellt werden. Weitere Informationen finden Sie unter Verbindungen und Ressourcen. Nur diese Verbindungen werden auf Hypervisorwarnungen überwacht. In der folgenden Tabelle werden die verschiedenen Parameter und Zustände von Hypervisorwarnungen beschrieben.

| Warnung | Unterstützte Hypervisors | Ausgelöst durch | Bedingung | Konfiguration |
|---|---|---|---|---|
| CPU-Nutzung | Citrix Hypervisor, VMware vSphere | Hypervisor | Schwellenwert der CPU-Auslastung erreicht oder überschritten | Warnschwellenwerte müssen im Hypervisor konfiguriert werden. |
| Speichernutzung | Citrix Hypervisor, VMware vSphere | Hypervisor | Schwellenwert der Speicherauslastung erreicht oder überschritten | Warnschwellenwerte müssen im Hypervisor konfiguriert werden. |
| Netzwerknutzung | Citrix Hypervisor, VMware vSphere | Hypervisor | Schwellenwert der Netzwerkauslastung erreicht oder überschritten | Warnschwellenwerte müssen im Hypervisor konfiguriert werden. |
| Datenträgernutzung | VMware vSphere | Hypervisor | Schwellenwert der Datenträgerauslastung erreicht oder überschritten | Warnschwellenwerte müssen im Hypervisor konfiguriert werden. |
| Hostverbindung oder Energiezustand | VMware vSphere | Hypervisor | Hypervisorhost neu gestartet oder nicht verfügbar | In VMware vSphere sind die Warnungen vorkonfiguriert. Es ist keine zusätzliche Konfiguration erforderlich. |

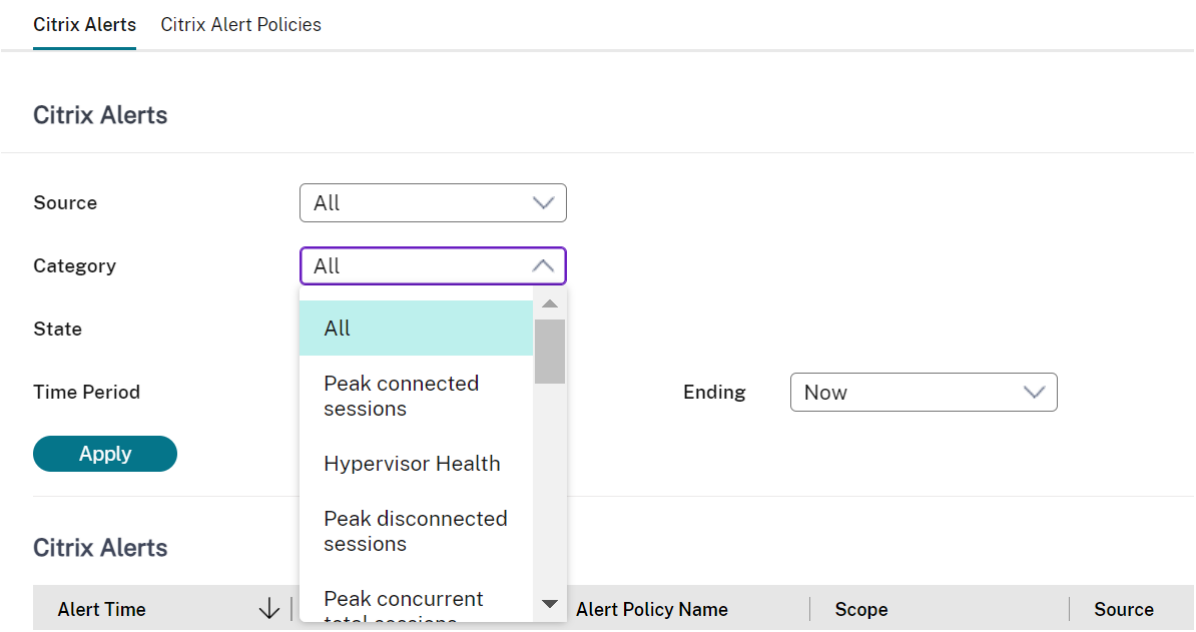
| Warnung | Unterstützte Hypervisors | Ausgelöst durch | Bedingung | Konfiguration |
|---|---|---|---|---|
| Hypervisorverbindung nicht verfügbar | Citrix Hypervisor, VMware vSphere | Delivery Controller | Die Verbindung mit dem Hypervisor (Pool oder Cluster) ist getrennt, heruntergefahren oder wird neu gestartet. Diese Warnung wird stündlich generiert, solange die Verbindung nicht verfügbar ist. | Warnungen für den Delivery Controller sind vorkonfiguriert. Es ist keine zusätzliche Konfiguration erforderlich. |

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren von Warnungen finden Sie unter Citrix XenCenter Alerts oder in der Dokumentation von VMware vCenter Alerts.

E-Mail-Benachrichtigungseinstellungen können unter **Citrix Benachrichtigungsrichtlinie > Siterichtlinie > Hypervisorzustand** konfiguriert werden. Die Schwellenwertbedingungen für Hypervisorwarnrichtlinien können nur im Hypervisor konfiguriert, bearbeitet, deaktiviert und gelöscht werden, nicht jedoch in der Überwachung. Die Konfiguration der E-Mail-Einstellungen und das Verwerfen von Warnungen ist jedoch unter "Überwachen"möglich.

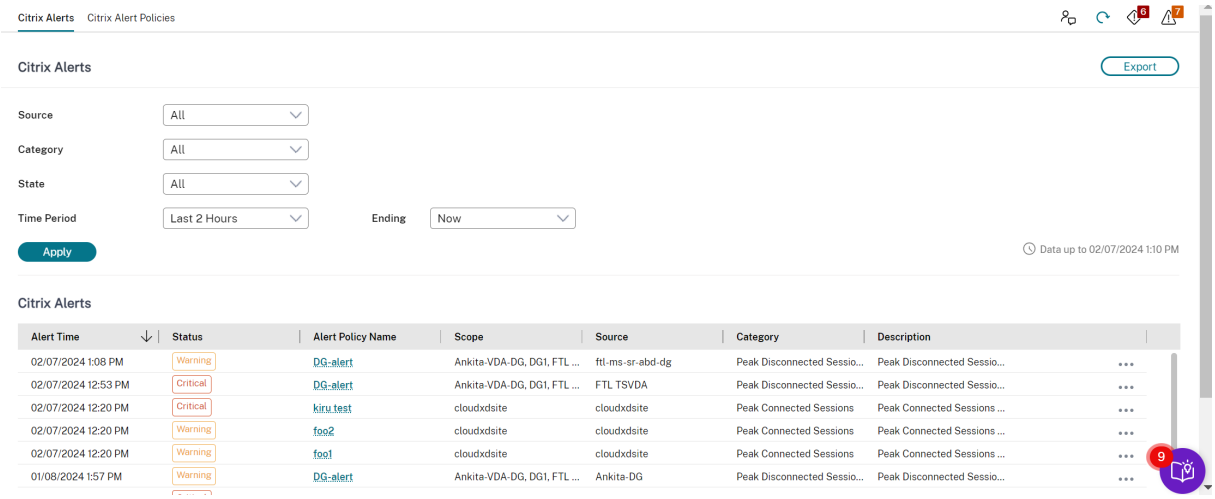
> **Wichtig:**
>
> - Alle Hypervisorwarnungen, die älter als ein Tag sind, werden automatisch verworfen.
> - Vom Hypervisor ausgelöste Warnungen werden abgerufen und unter "Überwachen" angezeigt. Änderungen im Lebenszyklus/Status der Hypervisorwarnungen werden jedoch nicht in der Überwachung wiedergegeben.
> - Warnungen, die fehlerfrei, verworfen oder in der Hypervisorkonsole deaktiviert sind, werden weiterhin unter "Überwachen"angezeigt und müssen explizit geschlossen werden.
> - Warnungen, die unter "Überwachen"geschlossen werden, werden nicht automatisch in der Hypervisorkonsole geschlossen.




Es gibt die neue Warnungskategorie **Hypervisorzustand**, mit der die Hypervisorwarnungen herausgefiltert werden können. Die Warnungen werden angezeigt, wenn die Schwellenwerte erreicht (oder überschritten) werden. Es gibt folgende Arten von Hypervisorwarnungen:

- Kritisch: Der kritische Schwellenwert der Hypervisorwarnungsrichtlinie wurde erreicht oder überschritten.
- Warnung: Der Warnschwellenwert der Hypervisorwarnungsrichtlinie wurde erreicht oder überschritten.
- Verworfen: Die Warnung wird nicht mehr als aktive Warnung angezeigt.



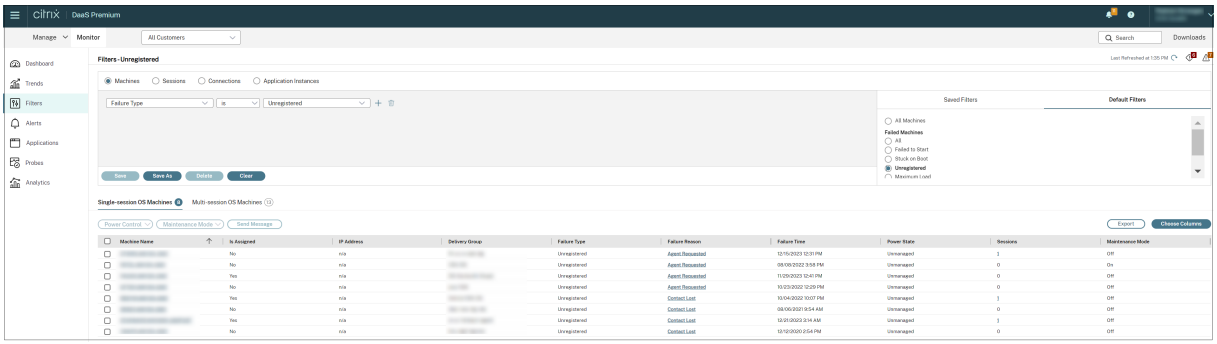

 

# Filtern von Daten zur Problembehandlung

August 18, 2023

Wenn Sie auf Zahlen im Dashboard klicken oder auf der Registerkarte **Filter** einen vordefinierten Standardfilter auswählen, wird die Ansicht "Filter"mit Daten für die ausgewählte Maschine oder den Fehlertyp geöffnet.

Sie können individuell gefilterte Ansichten von Maschinen, Verbindungen, Sitzungen und Anwendungsinstanzen für alle Bereitstellungsgruppen erstellen und das Suchergebnis speichern, um später darauf zuzugreifen. Sie können einen vordefinierten Filter bearbeiten und unter "Gespeicherte Filter" speichern.



1. Wählen Sie eine Ansicht aus:

    - **Maschinen**. Wählen Sie Einzelsitzungs-OS-Maschinen oder Multisitzungs-OS-Maschinen. Diese Ansicht zeigt die Anzahl der konfigurierten Computer. Die Registerkarte "Maschinen mit Multisitzungs-OS"enthält auch den Lastauswertungsindex, der die Verteilung der Leistungsindikatoren angibt, und Quickinfos zur Sitzungsanzahl, die Sie aufrufen können, wenn Sie mit der Maus auf den Link zeigen.
    - **Sitzungen**. Sie können die Sitzungsanzahl auch in der Ansicht "Sitzungen"anzeigen. Anhand der Leerlaufmessung können Sie Sitzungen suchen, die länger als der vorgegebene Schwellenwert im Leerlauf sind. Klicken Sie auf **Zugeordneter Benutzer**, um den Aktivitätsmanager für den Benutzer zu öffnen. Wenn Sie auf den **Endpunktnamen** klicken, wird der Aktivitätsmanager für den Endpunkt geöffnet. Wenn Sie auf **Details anzeigen** klicken, wird die Seite **Benutzerdetails** bzw. **Endpunktdetails** geöffnet. Weitere Informationen finden Sie unter Benutzerdetails.
    - **Verbindungen**. Filtern Sie Verbindungen nach verschiedenen Zeiträumen, u. a. die letzten 60 Minuten, die letzten 24 Stunden, oder die letzten 7 Tage.
    - **Anwendungsinstanzen**. Diese Ansicht zeigt die Eigenschaften aller Anwendungsinstanzen auf VDAs für Multisitzungs-OS und Einzelsitzungs-OS. Die Sitzungsleerlaufzeiten stehen für Anwendungsinstanzen auf Multisitzungs-OS-VDAs zur Verfügung.

2. Wählen Sie einen Filter aus den Listen “Gespeicherte Filter”oder “Standardfilter”aus.
3. Verwenden Sie die Dropdownlisten, um weitere Filterkriterien auszuwählen.
4. Wählen Sie zusätzliche Spalten bei Bedarf aus, um weitere Fehler zu beheben.
5. Speichern und benennen Sie den Filter.
6. Um den Filter später zu öffnen, wählen Sie in der Ansicht “Filter”die Ansicht (Maschinen, Sitzungen, Verbindungen oder Anwendungsinstanzen) und dann den gespeicherten Filter aus.
7. Klicken Sie auf **Exportieren**, um die Daten im CSV-Format zu exportieren. Daten von bis zu 100.000 Datensätzen können exportiert werden.
8. Verwenden Sie u. U. für die Ansichten **Maschinen** oder **Verbindungen** Energiesteuerelemente für alle in der gefilterten Liste ausgewählten Maschinen. Verwenden Sie in der Ansicht Sitzungen die Sitzungssteuerelemente oder die Option zum Senden von Nachrichten.
9. Klicken Sie in den Ansichten **Maschinen** und **Verbindungen** für fehlerhafte Maschinen oder Verbindungen auf **Fehlerursache**, um eine detaillierte Beschreibung des Fehlers und Empfehlungen zur Behebung aufzurufen. Informationen zu Ursachen von Maschinen- und Verbindungsfehlern sowie empfohlene Korrekturmaßnahmen finden Sie in dem Handbuch Citrix Director Failure Reasons Troubleshooting Guide.
10. Klicken Sie in der Ansicht **Maschinen** auf den Link mit dem Maschinennamen, um die zugehörige Seite **Maschinendetails** aufzurufen. Die Seite enthält Details zur Maschine, Optionen zur Energiesteuerung und Diagramme zur Überwachung von CPU, Arbeitsspeicher, Datenträgerüberwachung und GPU. Durch Klicken auf **Historische Auslastung anzeigen** können Sie Ressourcenauslastungstrends für die Maschine aufrufen. Weitere Informationen finden Sie unter Problembehandlung bei Maschinen.
11. In der Ansicht **Anwendungsinstanzen** können Sie die Instanzen basierend auf der **Leerlaufzeit**, die einen Schwellenwert überschreitet, sortieren und filtern. Wählen Sie die Anwendungsinstanzen im Leerlauf aus, die Sie beenden möchten. Durch Abmelden oder Trennen einer Anwendungsinstanz werden alle aktiven Anwendungsinstanzen in derselben Sitzung beendet. Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen. Die Seite zum Filtern von Anwendungsinstanzen und die Leerlaufzeitmessungen auf der Seite zum Filtern von Sitzungen stehen zur Verfügung, wenn VDAs in der Version 7.13 oder höher vorliegen.

> **Hinweis:**
>
> Die Verwaltungskonsole ermöglicht die Zuordnung mehrerer Desktopzuordnungsregeln (DAR) für verschiedene Benutzer oder Benutzergruppen zu einem VDA in einer Bereitstellungsgruppe. In StoreFront wird der zugewiesene Desktop mit dem zugehörigen Anzeigenamen gemäß den Desktopzuordnungsregeln für den angemeldeten Benutzer angezeigt. Die Überwachung unterstützt keine Desktopzuordnungsregeln und zeigt den zugewiesenen Desktop unabhängig

> vom angemeldeten Benutzer unter dem Namen der Bereitstellungsgruppe an. Sie können daher einer Maschine unter "Überwachen"keinen bestimmten Desktop zuordnen. Verwenden Sie folgenden PowerShell-Befehl, um den in StoreFront angezeigten, zugewiesenen Desktop dem unter "Überwachen"angezeigten Bereitstellungsgruppennamen zuzuordnen: Führen Sie den PowerShell-Befehl mit dem Remote PowerShell-SDK aus (Anweisungen hierzu siehe Blog).

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

## Siteübergreifendes Überwachen von Verlaufstrends

January 25, 2024

In der Ansicht "Trends"werden historische Trendinformationen der einzelnen Sites für die folgenden Parameter angezeigt:

- Sitzungen
- Verbindungsfehler
- Maschinenfehler
- Anmeldungsleistung
- Lastauswertung
- Kapazitätsverwaltung
- Maschinennutzung
- Ressourcenauslastung

Sie finden diese Informationen im Menü **Trends**.

Das Drilldownfeature ermöglicht das Navigieren durch Trenddiagramme, indem Sie bestimmte Zeiträume vergrößern (durch Klicken auf einen Datenpunkt im Diagramm) und die Detailinformationen zum Trend anzeigen. Durch dieses Feature können Sie die genauen Auswirkungen der angezeigten Trends besser verstehen.

Wenden Sie einen anderen Filter auf die Daten an, um den Standardgeltungsbereich der einzelnen Diagramme zu ändern.

> **Hinweis:**
>
> - Informationen zu Sitzungen, Fehlern und Anmeldungsleistungstrends stehen in Form von Diagrammen und Tabellen zur Verfügung, wenn Sie den Zeitraum auf den letzten Monat

> (**endet jetzt**) oder kürzer festlegen. Wenn Sie den Zeitraum auf "Letzter Monat"mit einem benutzerdefinierten Enddatum oder auf das letzte Jahr festlegen, werden die Trendinformationen nur in Form von Diagrammen angezeigt.
> - Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unterstützt die Aufbewahrung historischer Daten nur für 90 Tage. Daher enthalten Einjahrestrends und -berichte unter "Überwachen"die Daten der letzten 90 Tage.

### Verfügbare Trends

**Trends für Sitzungen anzeigen:** Wählen Sie auf der Registerkarte "Sitzungen"die Bereitstellungsgruppe und den Zeitraum aus, um weitere Informationen zur Anzahl gleichzeitiger Sitzungen anzuzeigen.

In der Spalte **Automatische Sitzungswiederverbindung** wird die Anzahl der automatischen Wiederverbindungen einer Sitzung angezeigt. Die automatische Wiederverbindung ist aktiviert, wenn die Richtlinie Sitzungszuverlässigkeit oder Client automatisch wieder verbinden aktiviert ist. Bei einer Netzwerkunterbrechung am Endpunkt werden die folgenden Richtlinien wirksam:

- Sitzungszuverlässigkeit wird (standardmäßig für 3 Minuten) wirksam und Citrix Receiver bzw. die Citrix Workspace-App versucht, eine Verbindung mit dem VDA herzustellen.
- Die automatische Wiederverbindung von Clients wird zwischen 3 und 5 Minuten wirksam und der Client versucht, eine Verbindung mit dem VDA herzustellen.

Beide Wiederverbindungen werden erfasst und dem Benutzer angezeigt. Diese Informationen werden maximal 5 Minuten nach der Wiederverbindung auf der Director-Benutzeroberfläche angezeigt.

Die Informationen zur automatischen Wiederverbindung ermöglichen die Anzeige und Problembehandlung von Netzwerkverbindungen mit Unterbrechungen und die Analyse von Netzwerken mit nahtloser Erfahrung. Sie können die Anzahl der Wiederverbindungen über Filter pro Bereitstellungsgruppe oder Zeitraum anzeigen.

Ein Drilldown bietet zusätzliche Informationen wie Sitzungszuverlässigkeit oder automatische Wiederverbindung von Clients, Zeitstempel, IP-Adresse und Name des Endpunkts, auf dem die Workspace-App installiert ist.

Standardmäßig werden Protokolle nach Zeitstempel in absteigender Reihenfolge sortiert. Das Feature ist für die Citrix Workspace-App für Windows, die Citrix Workspace-App für Mac, Citrix Receiver für Windows und Citrix Receiver für Mac verfügbar. Dieses Feature erfordert VDAs der Version 1906 oder höher.

Weitere Hinweise zur Wiederverbindung von Sitzungen finden Sie unter Sitzungen. Weitere Informationen zu Richtlinien finden Sie unter Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients" und Einstellungen der Richtlinie "Sitzungszuverlässigkeit".

Es kann vorkommen, dass die Daten für die automatische Wiederverbindung aus folgenden Gründen nicht in "Überwachen"angezeigt werden:

- Die Workspace-App sendet keine Daten zur automatischen Wiederverbindung an den VDA.
- Der VDA sendet keine Daten an den Überwachungsdienst.

> **Hinweis:**
>
> Es kann vorkommen, dass eine Client-IP-Adresse nicht richtig abgerufen wird, wenn bestimmte Citrix Gateway-Richtlinien festgelegt sind.

**Trends für Verbindungsfehler anzeigen:** Wählen Sie auf der Registerkarte "Fehler"die Verbindung, den Maschinentyp, den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Verbindungsfehler der Site anzuzeigen.

**Trends für Maschinenfehler anzeigen:** Wählen Sie auf der Registerkarte "Fehler"für Maschinen mit Einzelsitzungs-OS bzw. Multisitzungs-OS den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Maschinenfehler der Site anzuzeigen.

**Trends für die Anmeldeleistung anzeigen:** Wählen Sie auf der Registerkarte "Anmeldeleistung"die Bereitstellungsgruppe und den Zeitraum, um ein Diagramm mit ausführlichen Informationen über die Dauer der Benutzeranmeldungen bei der Site und wie sich die Anzahl der Anmeldungen auf die Leistung auswirkt, anzuzeigen. In dieser Ansicht wird auch die durchschnittliche Dauer der Anmeldephasen angezeigt, u. a. Vermittlungsdauer und VM-Startzeit.
Diese Daten beziehen sich speziell auf Benutzeranmeldungen und nicht auf Benutzer, die sich mit getrennten Sitzungen wieder verbinden.
Die Tabelle unterhalb des Diagramms zeigt die Anmeldedauer nach Benutzersitzung. Sie können die Spalten für die Anzeige auswählen und den Bericht nach einer beliebigen Spalte sortieren.
Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

**Trends für die Lastauswertung anzeigen:** Auf der Registerkarte Lastauswertungsindex können Sie ein Diagramm anzeigen, das ausführliche Informationen zur Last enthält, die auf die Multisitzungs-OS-Maschinen verteilt ist. Als Filteroptionen für dieses Diagramm stehen Bereitstellungsgruppe oder Multisitzungs-OS-Maschine in einer Bereitstellungsgruppe, Multisitzungs-OS-Maschine (nur wenn Multisitzungs-OS-Maschine in einer Bereitstellungsgruppe ausgewählt ist) und Bereich zur Verfügung. Der Lastauswertungsindex wird als Prozentsatz von CPU gesamt, Speicher, Datenträger oder Sitzungen im Vergleich zur Zahl der verbundenen Benutzer im letzten Intervall angezeigt.

**Anzeigen der Nutzung gehosteter Anwendungen:** Wählen Sie auf der Registerkarte "Kapazitätsverwaltung"die Registerkarte "Verwendung gehosteter Anwendungen"und dann die Bereitstellungsgruppe und den Zeitraum, um eine Kurve der höchsten gleichzeitigen Nutzung sowie eine Tabelle mit der anwendungsbasierten Verwendung anzuzeigen. In der Tabelle "Anwendungsbasierte Verwendung"können Sie eine bestimmte Anwendung auswählen, um Details und eine Liste der Benutzer anzuzeigen, die die Anwendung verwenden oder verwendet haben.

**Anzeigen der Nutzung von Einzelsitzungs-OS und Multisitzungs-OS:** In der Ansicht "Trends"wird die Einzelsitzungs-OS nach Site und Bereitstellungsgruppe angezeigt. Wenn Sie "Site"wählen, wird die Nutzung nach Bereitstellungsgruppe angezeigt. Wenn Sie "Bereitstellungsgruppe"wählen, wird die Nutzung nach Benutzer angezeigt.
In der Ansicht "Trends"wird außerdem die Nutzung von Multisitzungs-OS nach Site, Bereitstellungsgruppe und Maschine angezeigt. Wenn Sie "Site"wählen, wird die Nutzung nach Bereitstellungsgruppe angezeigt. Bei Auswahl von "Bereitstellungsgruppe"wird die Nutzung nach Maschine und nach Benutzer angezeigt. Wenn Sie "Maschine"wählen, wird die Nutzung nach Benutzer angezeigt.

**Anzeigen der Verwendung virtueller Maschinen:** Wählen Sie auf der Registerkarte "Maschinennutzung"die Option "Einzelsitzungs-OS"oder "Multisitzungs-OS", um einen Überblick über die Nutzung der VMs in Echtzeit zu erhalten. Auf der Seite wird die Zahl der mit Autoscale verwalteten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS angezeigt, die für eine ausgewählte Bereitstellungsgruppe und eine bestimmte Zeitdauer eingeschaltet sind. Außerdem werden die geschätzten, durch die Aktivierung von Autoscale erzielten Einsparungen angezeigt. Diese Prozentangabe wird anhand der Kosten pro Maschine berechnet.

Die Nutzungstrends der mit Autoscale verwalteten Maschinen repräsentieren die tatsächliche Nutzung, sodass Sie den Kapazitätsbedarf Ihrer Site schnell einschätzen können.

- Verfügbarkeit von Betriebssystemen für Einzelsitzungen: Zeigt den aktuellen Zustand von Maschinen mit Einzelsitzungs-OS (VDIs) nach Verfügbarkeit für die gesamte Site oder für eine bestimmte Bereitstellungsgruppe an.
- Verfügbarkeit von Betriebssystemen für mehrere Sitzungen: Zeigt den aktuellen Zustand von Maschinen mit Multisitzungs-OS nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an.

> **Hinweis:**
>
> Das Raster unterhalb des Diagramms enthält die Maschinennutzung pro Bereitstellungsgruppe in Echtzeit. Die Daten umfassen die Maschinenverfügbarkeit aller Maschinen unabhängig davon, ob sie mit Autoscale verwaltet werden. Unter "Verfügbar"werden auch Maschinen im Wartungsmodus angezeigt.

Die Konsolidierung der Überwachungsdaten hängt vom ausgewählten Zeitraum ab.

- Die Überwachungsdaten für die Zeiträume von einem Tag und einer Woche werden pro Stunde konsolidiert.
- Die Überwachungsdaten für den Zeitraum von einem Monat werden pro Tag konsolidiert.

Der Maschinenstatus wird zum Zeitpunkt der Konsolidierung erfasst, zwischenzeitliche Änderungen werden nicht berücksichtigt. Informationen zum Konsolidierungszeitraum finden Sie in der Dokumentation zur Überwachungs-API.

Weitere Informationen zur Überwachung der mit Autoscale verwalteten Maschinen finden Sie unter Autoscale.

**Anzeigen der Ressourcennutzung:** Zur Vereinfachung der Kapazitätsplanung wählen Sie auf der Registerkarte "Ressourcenauslastung"die Option "Maschinen mit Einzelsitzungs-OS"oder "Maschinen mit Multisitzungs-OS", um historische Trends zur CPU- und Arbeitsspeicherauslastung, IOPS und Datenträgerlatenz der einzelnen VDI-Maschine anzuzeigen.
Dieses Feature erfordert VDAs der **Version 7.11** oder höher.
Die Daten für die Parameter "Durchschnittliche CPU", "Speicherdurchschnitt", "Durchschnittliche IOPS", "Datenträgerlatenz"und "Max. gleichzeitiger Sitzungen"werden in Form von Diagrammen dargestellt. Sie können einen Drilldown für die einzelnen Maschinen ausführen, um Daten und Diagramme für die 10 Prozesse mit dem höchsten CPU-Verbrauch anzuzeigen. Filtern Sie die Anzeige nach Bereitstellungsgruppe und Zeitraum. Die Diagramme zu CPU, Speichernutzung und maximaler Zahl gleichzeitiger Sitzungen können für die letzten 2 Stunden, 24 Stunden, 7 Tage, den letzten Monat und das letzte Jahr angezeigt werden. Diagramme zu IOPS und Datenträgerlatenz sind für die letzten 24 Stunden, den letzten Monat und das letzte Jahr verfügbar.

> **Hinweis:**
>
> - Die Überwachungsrichtlinieneinstellung Prozessüberwachung aktivieren muss auf "Zugelassen"festgelegt sein, damit Daten für die Tabelle "Top-10-Prozesse"auf der Seite "Historische Maschinenauslastung"gesammelt und angezeigt werden können. Die Richtlinie ist standardmäßig auf "Nicht zugelassen"festgelegt. Standardmäßig werden alle Daten zur Ressourcenauslastung gesammelt. Diese Datensammlung kann über die Richtlinieneinstellung Ressourcenüberwachung aktivieren deaktiviert werden. Die Tabelle unterhalb der Diagrammen enthält die Ressourcenauslastung pro Maschine.
> - Für "Durchschnittliche IOPS"werden Tagesdurchschnittswerte angezeigt. Als maximale IOPS gilt der höchste IOPS-Durchschnittswert des ausgewählten Zeitraums. (Der IOPS-Durchschnittswert ist der Durchschnitt von IOPS im Zeitraum von einer Stunde auf dem VDA.)
> - Der Maschinendrilldown listet Prozesse mit durchschnittlicher CPU- oder Arbeitsspeichernutzung über 1 % auf, was bedeutet, dass manchmal weniger als 10 Prozesse aufgelistet werden.

**Anzeigen der Anwendungsstörungen:** Auf der Registerkarte "Anwendungsstörungen"werden Fehler bei den veröffentlichten Anwendungen auf den VDAs angezeigt.

Dieses Feature erfordert VDAs der **Version 7.15** oder höher. Einzelsitzungs-OS-VDAs unter Windows Vista und höher und Multisitzungs-OS-VDAs unter Windows Server 2008 und höher werden unterstützt.
Weitere Informationen finden Sie unter Überwachen historischer Anwendungsstörungen.

Standardmäßig werden nur Anwendungsausfälle von Multisitzungs-OS-VDAs angezeigt. Sie können

die Überwachung von Anwendungsstörungen über die Überwachungsrichtlinien steuern. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.

**Erstellen benutzerdefinierter Berichte:** Über die Registerkarte "Benutzerdefinierte Berichte"können benutzerdefinierte Berichte mit Echtzeit- und historischen Daten aus der Überwachungsdatenbank in tabellarischer Form erstellt werden.

Von der Liste der benutzerdefinierten Berichtsabfragen aus können Sie auf **Ausführen und herunterladen** klicken, um Berichte im CSV-Format zu exportieren. Darüber hinaus können Sie mit der Option **OData kopieren** die zugehörige OData-Abfrage kopieren und teilen und mit **Bearbeiten** die Abfrage bearbeiten.
Sie können eine Abfrage für benutzerdefinierte Berichte basierend auf Maschinen, Verbindungen, Sitzungen oder Anwendungsinstanzen erstellen. Filterbedingungen können Sie auf der Basis von Feldern (z. B. Maschine, Bereitstellungsgruppe oder Zeitraum) festlegen. Falls erforderlich, geben Sie weitere Spalten für den benutzerdefinierten Bericht an. In der Vorschau können Sie ein Beispiel für die Berichtsdaten anzeigen. Wenn Sie die benutzerdefinierte Berichtsabfrage speichern, wird sie der Liste der gespeicherten Abfragen hinzugefügt.

Sie können eine benutzerdefinierte Berichtsabfrage basierend auf einer kopierten OData-Abfrage erstellen. Wählen Sie hierfür die OData-Abfrageoption und fügen Sie die kopierte OData-Abfrage ein. Sie können die resultierende Abfrage für das Ausführen zu einem späteren Zeitpunkt speichern.

> **Hinweis:**
>
> Die Spaltennamen in der Vorschau und dem Exportbericht nach OData-Abfrage werden in Englisch angezeigt.

Die Flag-Symbole auf dem Diagramm weisen auf wichtige Ereignisse oder Aktionen für diesen Zeitraum hin. Bewegen Sie den Mauszeiger über das Flag und klicken Sie, um Ereignisse und Aktionen aufzulisten.

> **Hinweis:**
>
> - Anmeldedaten für HDX-Verbindungen werden für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.
> - Bereitstellungsgruppen, die in der Verwaltungskonsole gelöscht wurden, stehen in den Trendfiltern zur Auswahl, bis die zugehörigen Daten bereinigt werden. Wenn Sie eine gelöschte Bereitstellungsgruppe wählen, werden Diagramme für verfügbare Daten angezeigt. Die Tabellen zeigen jedoch keine Daten an.
> - Wenn eine Maschine mit aktiven Sitzungen von einer Bereitstellungsgruppe in eine andere verschoben wird, werden in den Tabellen **Ressourcenauslastung und Lastauswertungsprogrammindex** der neuen Bereitstellungsgruppe Metriken angezeigt, die aus den alten und neuen Bereitstellungsgruppen konsolidiert wurden.

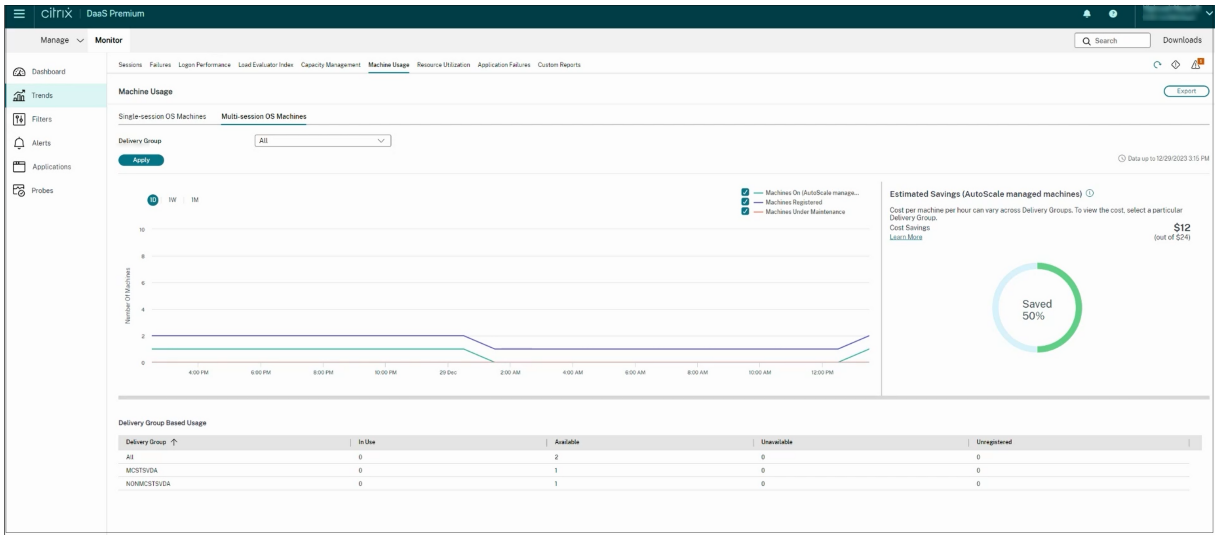
# Überwachen von mit Autoscale verwalteten Maschinen

April 1, 2022

Autoscale ermöglicht die proaktive Energieverwaltung aller registrierten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS in einer Bereitstellungsgruppe. Sie können Autoscale für eine ausgewählte Bereitstellungsgruppe auf der Registerkarte **Verwalten** konfigurieren. Weitere Informationen finden Sie unter Autoscale.
Sie können wichtige Kennzahlen mit Autoscale verwalteter Maschinen über die Registerkarte **Überwachen** überwachen.

## Maschinennutzung

Auf der Seite **Überwachung** > **Trends** > **Maschinennutzung** wird die Gesamtzahl der mit Autoscale verwalteten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS angezeigt, die für eine ausgewählte Bereitstellungsgruppe und eine bestimmte Zeitdauer eingeschaltet sind. Diese Kennzahl gibt die derzeitige Maschinennutzung in der Bereitstellungsgruppe an.
Wählen Sie auf der Registerkarte **Einzelsitzungs-OS-Maschinen**oder **Maschinen mit Multisitzungs-OS** die Bereitstellungsgruppe und den Zeitraum aus.




Im Diagramm werden folgende Kennzahlen dargestellt:

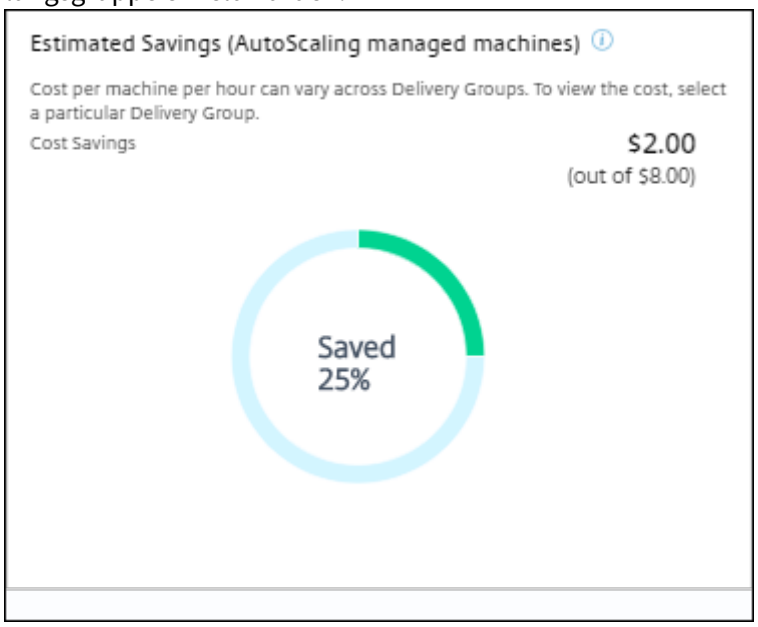
- **Eingeschaltete Maschinen** - Anzahl der mit Autoscale verwalteten Maschinen, die eingeschaltet sind
- **Registrierte Maschinen** - Anzahl der registrierten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS

- **Maschinen in Wartung** - Anzahl der Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS im Wartungsmodus.

### Geschätzte Einsparungen

Auf der Seite **Überwachung** > **Trends** > **Maschinenauslastung** werden auch die geschätzten Kosteneinsparungen angezeigt, die durch Aktivieren von Autoscale in der ausgewählten Bereitstellungsgruppe erzielt wurden.




Die Einsparungen werden als Prozentsatz der Einsparungen pro Maschine und Stunde (in US-Dollar) berechnet, die unter **Verwalten** > **Bereitstellungsgruppe bearbeiten** > **Autoscale** konfiguriert wurden. Weitere Informationen zum Konfigurieren der Einsparungen pro Maschine finden Sie unter Autoscale.

Wenn Sie alle Bereitstellungsgruppen auswählen, wird der Durchschnittswert der geschätzten Einsparungen für alle Bereitstellungsgruppen angezeigt.
Anhand der geschätzten Einsparungen können Administratoren die Infrastruktur konsolidieren und Kapazität mit dem Ziel maximaler Einsparungen und Auslastung planen.

### Warnmeldungsbenachrichtigungen für Maschinen und Sitzungen

Auf dem Überwachungsdashboard werden Warnmeldungen angezeigt, für die weitere Details aufgerufen werden können. Details zu Warnmeldungen werden auf der Seite **Überwachung** > **Warnungen** angezeigt.

- Um eine Warnrichtlinie für eine Bereitstellungsgruppe zu erstellen, gehen Sie zu **Überwachen** > **Warnungen** > **Citrix Benachrichtigungsrichtlinie** > **Bereitstellungsgruppenrichtlinie**.

- Hier können Sie die folgenden Warnungen und Schwellenwerte festlegen:
  - Fehlgeschlagene Maschinen (Einzelsitzungs-OS) und fehlgeschlagene Maschinen (Multisitzungs-OS),
  - Max. verbundener Sitzungen, max. getrennter Sitzungen und Max. gleichzeitiger Sitzungen insgesamt in der Bereitstellungsgruppe.
- Warnungen werden generiert, wenn der entsprechende Parameter in der Bereitstellungsgruppe den Schwellenwert erreicht.

For more details regarding the alert policy conditions and creation of new alert policies, see Alerts and notifications.

### Maschinenstatus

- Über **Überwachung** > **Filter** > **Maschinen** wird der Energiezustand aller Maschinen in einem tabellarischen Format angezeigt. Sie können die Anzeige nach Bereitstellungsgruppen filtern.
- Über **Überwachung** > **Filter** > **Sitzungen** werden die Maschinen zugeordneten Sitzungen und deren Echtzeitstatus angezeigt.
- Wählen Sie unter **Überwachung** > **Trends** > **Sitzungen** die Bereitstellungsgruppe und den Zeitraum aus, um den Trend der Sitzungen und die zugehörigen Kennzahlen anzuzeigen.

Weitere Informationen finden Sie unter Filtern von Daten bei der Problembehandlung.

### Lastauswertungstrends

Auf der Seite **Überwachung** > **Trends** > **Lastauswertung** wird ein Diagramm angezeigt, das ausführliche Informationen zu der auf die Multisitzungs-OS-Maschinen verteilten Last bietet. Als Filteroptionen für dieses Diagramm stehen Bereitstellungsgruppe oder Multisitzungs-OS-Maschine in einer Bereitstellungsgruppe, Multisitzungs-OS-Maschine (nur wenn Multisitzungs-OS-Maschine in einer Bereitstellungsgruppe ausgewählt ist) und Bereich zur Verfügung. Der Lastauswertungsindex wird als Prozentsatz von CPU gesamt, Speicher, Datenträger oder Sitzungen dargestellt und zwar im Vergleich mit der Zahl der verbundenen Benutzer im letzten Intervall.

## Problembehandlung bei Bereitstellungen

March 30, 2024

Als Helpdeskadministrator können Sie nach dem Benutzer suchen, der ein Problem gemeldet hat. Rufen Sie dann Details zu Sitzungen oder Anwendungen auf, die mit diesem Benutzer verbunden sind.

Sie können auch Maschinen und Endpunkte suchen, bei denen Probleme gemeldet wurden. Probleme können durch die Überwachung relevanter Metriken und das Ergreifen entsprechender Maßnahmen schnell gelöst werden.

Folgende Aktionen sind verfügbar:

- Beenden von Anwendung und Prozessen, die nicht mehr reagieren
- Spiegeln von Vorgängen auf Benutzermaschinen
- Abmelden nicht reagierender Sitzungen
- Neustarten von Maschinen
- Versetzen der Maschine in den Wartungsmodus
- Zurücksetzen des Benutzerprofils

## Problembehandlung bei Anwendungen

July 28, 2023

### Anwendungsanalyse

In der Ansicht **Anwendungen** werden konsolidierte Anwendungsdaten zur effizienten Analyse und Verwaltung der Anwendungsleistung angezeigt. Sie erhalten hier wertvolle Einblicke in die Integrität und Nutzung aller in der Site veröffentlichten Anwendungen. In der Standardansicht können die wichtigsten ausgeführten Anwendungen identifiziert werden.
Dieses Feature erfordert VDAs der Version 7.15 oder höher.


In der Spalte **Testergebnis** wird das Ergebnis der Anwendungstests der letzten 24 Stunden angezeigt. Klicken Sie auf einen Ergebnislink, um auf der Seite **Trends** > **Anwendungstestergebnisse** weitere Details aufzurufen. Weitere Informationen zum Konfigurieren von Anwendungstests finden Sie unter Anwendungs- und Desktoptests.

In der Spalte **Instanzen** wird die Verwendung der Anwendungen angezeigt. Sie zeigt die Zahl der aktuell ausgeführten Anwendungsinstanzen (verbundene und getrennte Instanzen). Zur weiteren

Problembehandlung klicken Sie auf das Feld **Instanzen**, um die entsprechende Filterseite **Anwendungsinstanzen** anzuzeigen. Hier können Sie Anwendungsinstanzen zum Abmelden oder Trennen der Verbindung auswählen.

> **Hinweis:**
>
> Anwendungsinstanzen, die unter "Anwendungsgruppen"erstellt wurden, werden für Administratoren mit benutzerdefiniertem Bereich unter "Überwachen"nicht angezeigt. Zur Anzeige aller Anwendungsinstanzen sind vollständige Administratorrechte erforderlich. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX256001.

Den Status veröffentlichter Anwendungen in der Site können Sie über die Spalten **Anwendungsausfälle** und **Anwendungsfehler** überwachen. In diesen Spalten wird die aggregierte Zahl der Fehler und Ausfälle beim Starten der jeweiligen Anwendung in der letzten Stunde angezeigt. Klicken Sie auf das Feld **Anwendungsausfälle** oder **Anwendungsfehler**, um auf der Seite **Trends** > **Anwendungsstörungen** Fehlerangaben für die ausgewählte Anwendung anzuzeigen.

Die Richtlinien für die Überwachung auf Anwendungsfehler bestimmen die Verfügbarkeit und Anzeige von Ausfällen und Fehlern. Weitere Informationen zu diesen Richtlinien und zu ihrer Bearbeitung finden Sie im Artikel "Einstellungen der Überwachungsrichtlinie"unter Richtlinien für die Überwachung auf Anwendungsfehler.

### Überwachen von Anwendungen in Echtzeit

Zur Problembehandlung bei Anwendungen und Sitzungen können Sie anhand von Leerlaufkennzahlen feststellen, welche Instanzen über ein bestimmtes Zeitlimit hinaus inaktiv bleiben.

Typische Einsatzbereiche für die Problembehandlung bei Anwendungen ist der Gesundheitssektor, wo Mitarbeiter Anwendungslizenzen gemeinsam verwenden. Sie müssen dort Sitzungen und Anwendungsinstanzen im Leerlauf beenden, um die Citrix Virtual Apps and Desktops-Umgebung zu bereinigen, Server mit schlechter Leistung neu zu konfigurieren oder Anwendungen zu warten oder zu aktualisieren.

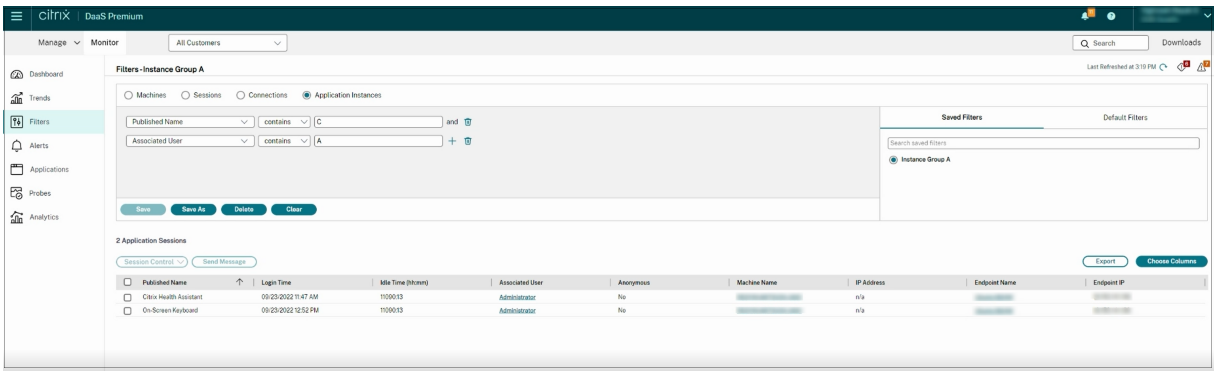
Die Filterseite **Anwendungsinstanzen** enthält alle Instanzen von Anwendungen auf VDAs für Multisitzungs-OS und Einzelsitzungs-OS. Die Leerlaufzeit wird für Anwendungsinstanzen auf Multisitzungs-OS-VDAs angezeigt, die mindestens 10 Minuten im Leerlauf sind.

> **Hinweis:**
>
> Die Kennzahlen für Anwendungsinstanzen stehen in Sites mit allen Lizenztypen zur Verfügung.

Anhand dieser Informationen können Sie Instanzen suchen, die länger als vorgegeben im Leerlauf sind und diese abmelden oder trennen. Wählen Sie hierfür **Filter > Anwendungsinstanzen** und wählen

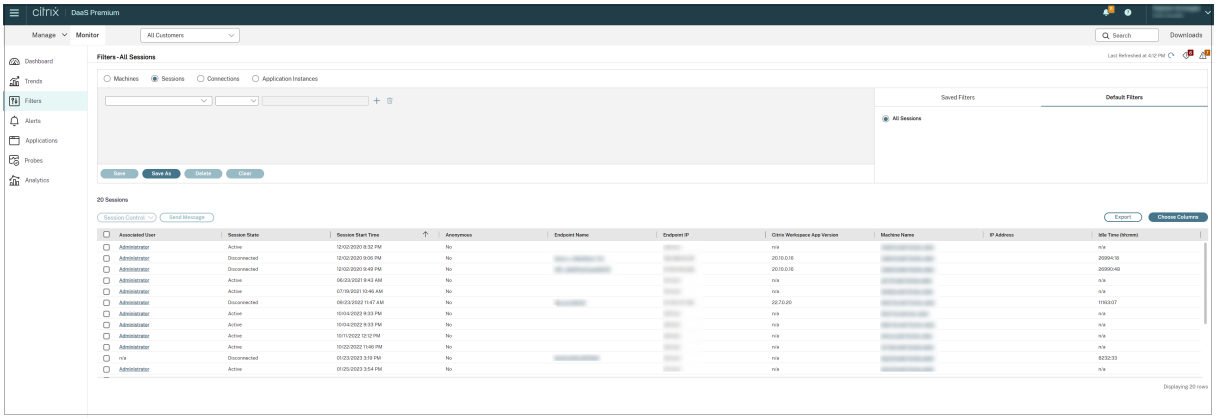
Sie einen vorhandenen Filter oder **Alle Anwendungsinstanzen** und erstellen Sie Ihren eigenen Filter.




Beispiel für einen Filter: Wählen Sie für **Filtern nach** die Kriterien **Veröffentlichter Name** (der Anwendung) und **Leerlaufzeit**. Legen Sie für **Leerlaufzeit** unter **größer als oder gleich** ein Zeitlimit fest und speichern Sie den Filter. Wählen Sie aus der gefilterten Liste die Anwendungsinstanzen aus. Wählen Sie die Option zum Senden von Nachrichten oder wählen Sie im Dropdownmenü **Sitzungssteuerung** den Befehl **Abmelden** oder **Trennen**, um die Instanzen zu beenden.

> **Hinweis:**
>
> Diese Aktion trennt die aktuelle Sitzung bzw. meldet sie ab und damit auch alle zu der Sitzung gehörenden Anwendungsinstanzen.

Sie können Sitzungen im Leerlauf auf der Filterseite **Sitzungen** über den Sitzungszustand und die Leerlaufkennzahl suchen. Sortieren Sie die Anzeige nach der Spalte **Leerlaufzeit** oder definieren Sie einen Filter, um Sitzungen zu identifizieren, die über eine bestimmte Zeitspanne hinaus inaktiv sind. Die Leerlaufzeit wird für Sitzungen auf Multisitzungs-OS-VDAs aufgelistet, die mindestens 10 Minuten im Leerlauf sind.




Für **Leerlaufzeit** wird **Nicht zutreffend** angezeigt, wenn die Sitzungs- oder Anwendungsinstanz

- erst bis zu 10 Minuten im Leerlauf ist
- auf einem Einzelsitzungs-OS-VDA gestartet wurde

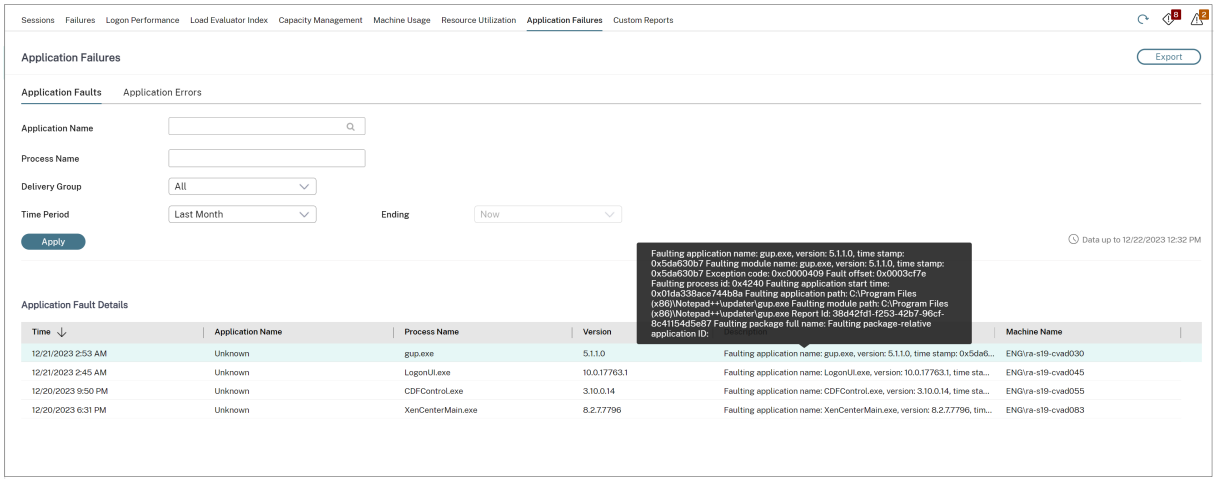
 

- oder auf einem VDA einer Version bis 7.12 ausgeführt wird

## Überwachen historischer Anwendungsstörungen

Auf der Registerkarte **Trends** > **Anwendungsstörungen** werden Fehler bei den veröffentlichten Anwendungen auf den VDAs angezeigt.

Weitere Informationen zur Verfügbarkeit der Anwendungsstörungstrends finden Sie im Artikel Datengranularität und -beibehaltung. Es werden Anwendungstörungen überwacht, die in der Ereignisanzeige mit der Quelle "Anwendungsfehler"protokolliert werden. Klicken Sie auf **Exportieren** zum Generieren von Berichten im CSV-, Excel- oder PDF-Format.




Anwendungsstörungen werden basierend auf dem Schweregrad als **Anwendungsausfall** oder als **Anwendungsfehler** klassifiziert. Auf der Registerkarte "Anwendungsausfälle"werden Fehler angezeigt, die zum Verlust von Funktionalität oder Daten führen. Anwendungsfehler sind Probleme ohne direkte Relevanz, die ggf. zukünftige Probleme verursachen können.

Zum Filtern der Störungen stehen folgende Optionen zur Verfügung: **Name der veröffentlichten Anwendung**, **Prozessname**, **Bereitstellungsgruppe** und **Zeitraum**. Die Tabelle enthält den Fehler bzw. Fehlercode und eine kurze Problembeschreibung. Detaillierte Fehlerbeschreibungen werden als QuickInfo angezeigt.

> **Hinweis:**
>
> Der Name der veröffentlichten Anwendung wird als "Unbekannt"angezeigt, wenn der zugehörige Anwendungsname nicht ermittelt werden kann. Das ist normalerweise der Fall, wenn bei einer gestarteten Anwendung in einer Desktopsitzung ein Fehler auftritt oder wenn ein Fehler die Folge einer unbehandelten, durch eine abhängige ausführbare Datei verursachten Ausnahme ist.

Standardmäßig werden nur Störungen von Anwendungen überwacht, die auf Multisitzungs-OS-VDAs gehostet werden. Sie können die Überwachungseinstellungen über die Überwachungsgrup-

penrichtlinien ändern: "Überwachung von Anwendungsausfällen aktivieren", "Überwachung von Ausfällen auf Einzelsitzungs-OS-VDAs"und "Von der Fehlerüberwachung ausgeschlossene Anwendungen". Weitere Informationen finden Sie unter Richtlinien für die Überwachung auf Anwendungsfehler im Artikel "Einstellungen der Überwachungsrichtlinie".

Auf der Seite **Trends** > **Anwendungstestergebnisse** werden die Ergebnisse der Anwendungtests der letzten 24 Stunden und der letzten 7 Tage angezeigt. Weitere Informationen zum Konfigurieren von Anwendungstests finden Sie unter Anwendungstests.

## Anwendungstests

January 17, 2023

Das Anwendungstestfeature automatisiert die Überprüfung der Integrität der in einer Site veröffentlichten Citrix Virtual Apps. Die Ergebnisse der Anwendungstests stehen auf der Registerkarte **Überwachen** von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) zur Verfügung. Citrix Probe Agent unterstützt Sites, die auf Steuerungsebenen für Citrix Cloud Japan und Citrix Cloud Government gehostet werden.

Stellen Sie sicher, dass Endpunktmaschinen mit Testagents Windows-Maschinen mit Citrix Receiver für Windows 4.8 oder höher oder der Citrix Workspace-App für Windows (früher Citrix Receiver für Windows) 1808 oder höher sind. Die Workspace-App für Unified Windows Platform (UWP) wird nicht unterstützt.

Anforderungen:

- Endpunktmaschinen mit Testagents sind Windows-Maschinen mit Citrix Receiver für Windows 4.8 oder höher oder der Citrix Workspace-App für Windows (früher Citrix Receiver für Windows) 1906 oder höher. Die Workspace-App für Unified Windows Platform (UWP) wird nicht unterstützt.
- Citrix Probe Agent unterstützt die formularbasierte Standardauthentifizierung, wie sie von Citrix WorkSpace unterstützt wird. Citrix Probe Agent unterstützt keine anderen Authentifizierungsmethoden wie Single Sign-On (SSO) oder Multifaktorauthentifizierung (MFA). Ähnlich funktioniert der Citrix Probe Agent nur, wenn kein Proxyserver oder Load Balancer wie Citrix Gateway oder Citrix ADC eingesetzt wird.
- Stellen Sie sicher, dass auf der Endpunktmaschine, auf der Sie den Probe Agent installieren möchten, Microsoft .NET Framework Version 4.7.2 oder höher installiert ist.
- Um den Testagent in der Steuerungsebene für Citrix Cloud Japan zu verwenden, wählen Sie im Pfad "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" den Registrierungswert 2. Um den Testagent in der Steuerungsebene für Citrix Cloud Govern-

ment zu verwenden, wählen Sie im Pfad "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeA den Registrierungswert 3.

Zum Ausführen von Anwendungstests erforderliche Benutzerkonten/Berechtigungen:

- Eindeutiger Workspace-Benutzer auf jeder Endpunktmaschine. Der Workspace-Benutzer muss kein Administrator sein.
- Benutzerkonten mit Windows-Administratorberechtigung zum Installieren und Konfigurieren von Citrix Probe Agent auf den Endpunktmaschinen
- Ein Volladministratorkonto mit den folgenden Berechtigungen. Die Wiederverwendung bestehender Benutzerkonten für Anwendungstests kann zur Abmeldung von deren aktiven Sitzungen führen.
  - Bereitstellungsgruppenberechtigungen:
    - Nur Lesen
  - Director-Berechtigungen:
    - Testkonfigurationen erstellen\bearbeiten\entfernen
    - Konfigurationsseite anzeigen
    - Trendseite anzeigen

### Konfigurieren von Anwendungstests

Sie können die Durchführung von Anwendungtests für außerhalb der Spitzenzeiten in mehreren Regionen planen. Die umfassenden Testergebnisse können helfen, Probleme bei Anwendungen, Hostcomputern oder Verbindung zu beheben, bevor sie sich bei den Benutzern bemerkbar machen.

Citrix Probe Agent Version 2103 unterstützt die Siteaggregation. Anwendungen und Desktops aggregierter Sites können angezeigt und gestartet werden. Wenn Sie den Probe Agent konfigurieren, wählen Sie die Option **Siteaggregation für Workspace (StoreFront) aktiviert**, um die Anzeige von Anwendungen und Desktops von aggregierten Sites zu ermöglichen. Die folgenden Sitekombinationen werden unterstützt:

- Mehrere On-Premises-Sites mit einer StoreFront-URL.
- On-Premises- und Cloudsites mit einer StoreFront-URL oder einer Workspace-URL.
- Mehrere Cloudsites mit einer Workspace-URL.

> **Hinweis:**
>
> Sie müssen separate Administratoren oder Benutzer erstellen, um Tests zu konfigurieren, die nur auf eine Site zugreifen können.

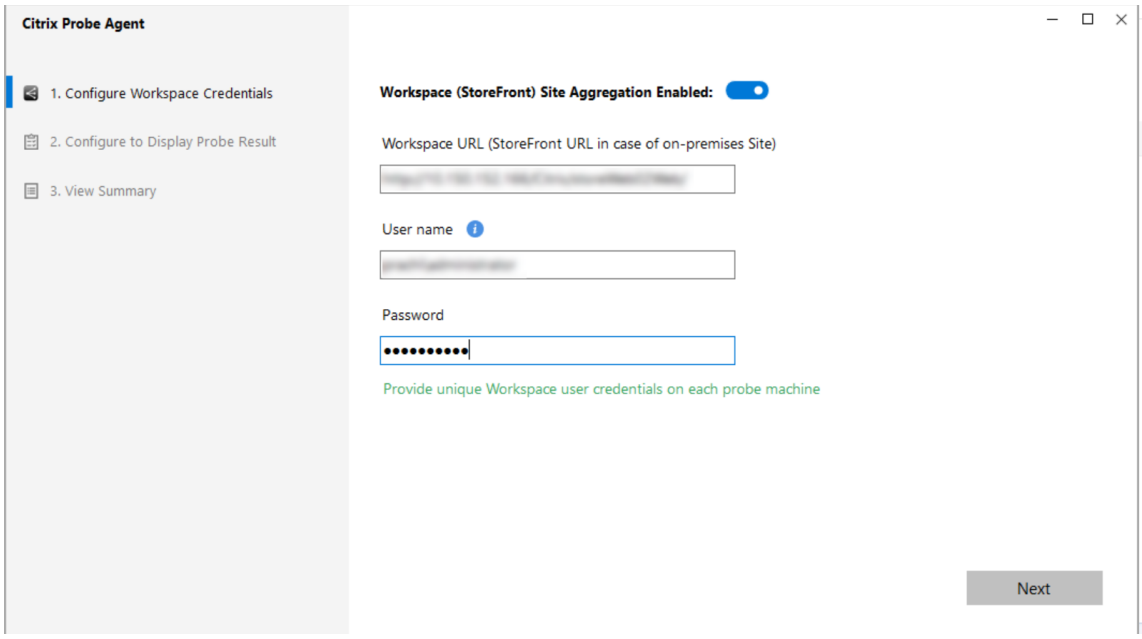
 

### Schritt 1: Installieren und Konfigurieren von Citrix Probe Agent

Citrix Probe Agent ist eine ausführbare Windows-Datei, die den Anwendungsstart durch einen Benutzer über Citrix Workspace simuliert. Der Agent testet Anwendungsstarts gemäß der Konfiguration unter "Überwachen"und meldet die Ergebnisse unter "Überwachen".

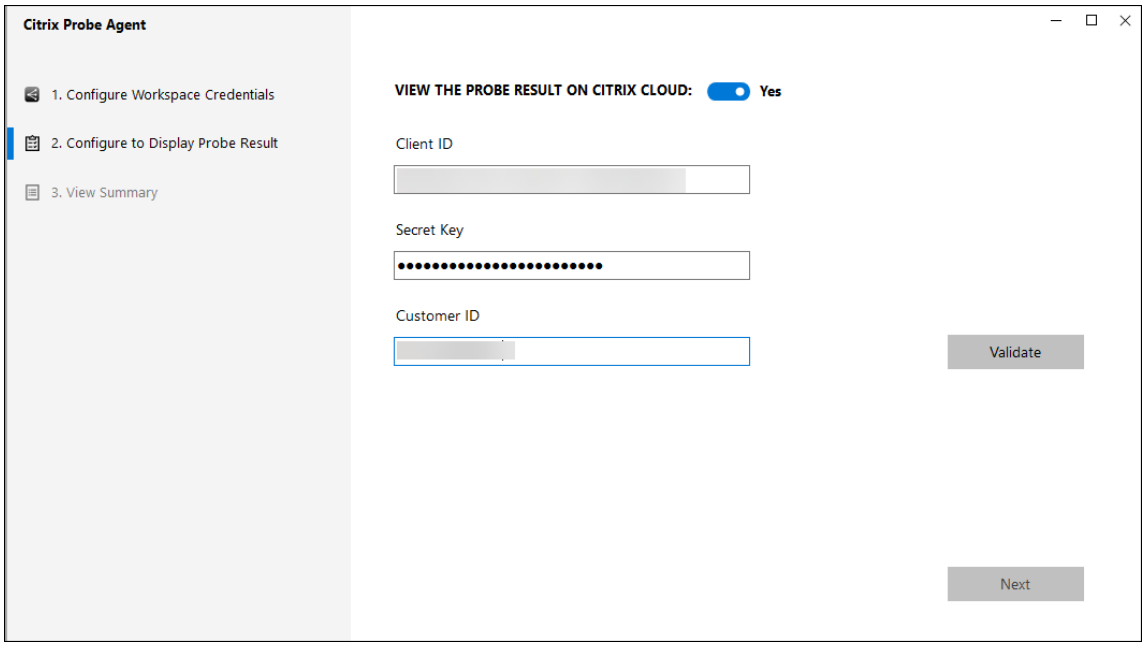
1. Identifizieren Sie die Endpunktmaschinen, auf denen Sie Anwendungtests ausführen möchten.
2. Benutzer mit Administratorberechtigung können Citrix Probe Agent auf den Endpunktmaschinen installieren und konfigurieren. Laden Sie die ausführbare Datei von Citrix Probe Agent von folgender Webseite herunter: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Starten Sie den Agent und konfigurieren Sie die Citrix Workspace- Anmeldeinformationen. Konfigurieren Sie einen eindeutigen Workspace-Benutzer auf jeder Endpunktmaschine. Die Anmeldeinformationen werden verschlüsselt und sicher gespeichert.

   > **Hinweise:**
   >
   > - Um auf die gewünschte Site von außerhalb des Netzwerks zuzugreifen, geben Sie in das Feld **Workspace-URL** die Login-URL für Citrix Gateway ein. Citrix Gateway leitet die Anforderung automatisch an die entsprechende Workspace-URL weiter.
   > - Verwenden Sie NetBIOS als Domänenname im Feld "Benutzername". Beispiel: NetBIOS/Benutzername.
   > - App-Tests unterstützen Citrix Content Collaboration mit Workspace-Authentifizierung (nur AD).



4. Geben Sie auf der Registerkarte **Anzeige der Testergebnisse konfigurieren** Ihre Anmeldeinformationen ein, um auf Citrix DaaS zuzugreifen. Kundennamen bzw. Kunden-ID, Client-ID und den geheimen Schlüssel finden Sie auf der API-Zugriffsseite der Citrix Cloud-Konsole.




**Schritt 2: Konfigurieren von Anwendungstests auf der Registerkarte "Überwachen"**

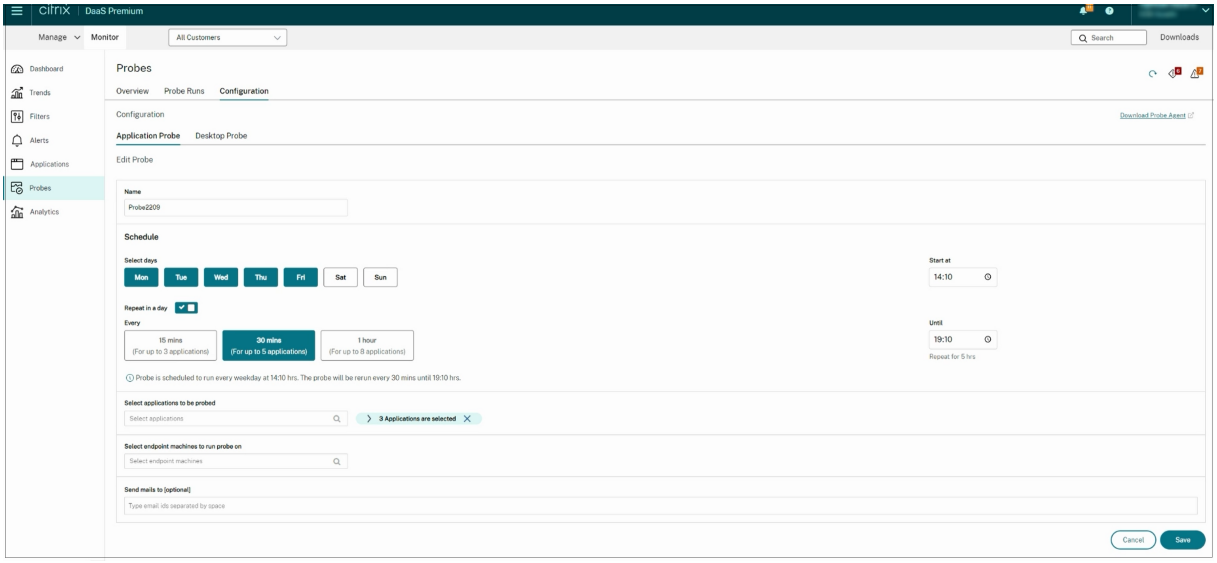
1. Gehen Sie in Citrix DaaS zu **Konfiguration** > **Testkonfiguration** > **Anwendungstest** und klicken Sie auf **Test erstellen**:
2. Geben Sie auf der Seite **Test erstellen** den Namen des Tests ein.
3. Wählen Sie den Zeitplan aus:

    a) Wählen Sie die Wochentage, an denen der Test ausgeführt werden soll.
    b) Geben Sie eine Startzeit für den Test ein.
    c) Sie können auch die Option **An einem Tag wiederholen** auswählen. Geben Sie die Endzeit ein und wie oft der Test innerhalb eines Tages wiederholt werden soll. In der folgenden Konfiguration können Anwendungstests beispielsweise jeden Montag, Mittwoch, Donnerstag und Sonntag von 12:08 Uhr bis 16:34 Uhr ausgeführt und alle 30 Minuten wiederholt werden.

4. Wählen Sie abhängig vom Intervall die empfohlene Anzahl von Anwendungen aus.
5. Wählen Sie die Endpunktmaschinen aus, auf denen der Test ausgeführt werden muss.
6. Geben Sie die E-Mail-Adressen ein, an die die Ergebnisse des Testmoduls gesendet werden und klicken Sie auf **Speichern**.

In dieser Konfiguration werden die Anwendungssitzungen jeden Montag, Mittwoch, Donnerstag und Sonntag um 12:08 Uhr, 12:38 Uhr, 13:08 Uhr usw. bis 16:08 Uhr gestartet.




**Hinweis:**

- Konfigurieren Sie Ihren E-Mail-Server unter **Warnungen** > **E-Mail-Server-Konfiguration**.
- Nach der Konfiguration auf der Registerkarte **Überwachen** führt der Agent konfigurierte Tests ab der nächsten Stunde aus.
- Tests, die vor Einführung der Option **An einem Tag wiederholen** eingerichtet wurden, werden weiterhin zur geplanten Zeit ausgeführt. Die Option **An einem Tag wiederholen** ist für diese Tests standardmäßig deaktiviert.

### Schritt 3: Ausführen des Tests

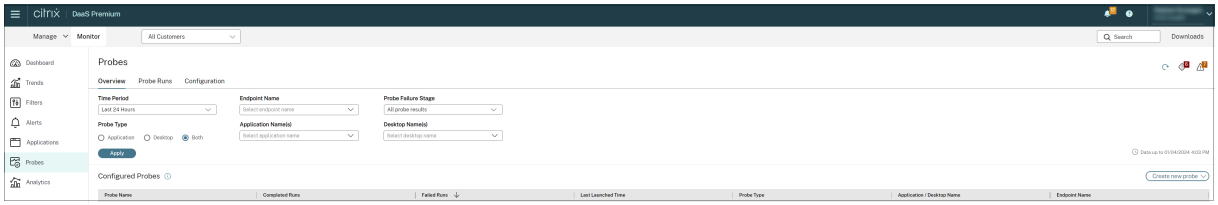
Der Agent führt Anwendungtests regelmäßig entsprechend der unter "Überwachen"abgerufenen Konfiguration aus. Er startet ausgewählte Anwendungen der Reihe nach über Workspace. Die Ergebnisse werden über die Überwachungsdatenbank gemeldet. Fehler werden für fünf spezifische Phasen gemeldet:

- **Workspaceerreichbarkeit:** Die konfigurierte Workspace-URL ist nicht erreichbar.
- **Workspaceauthentifizierung:** Die konfigurierten Workspace-Anmeldeinformationen sind ungültig.
- **Workspaceenumeration**: Die Liste der enumerierten Anwendungen in Workspace enthält die getestete Anwendung nicht.
- **ICA-Download**: Die ICA-Datei ist nicht verfügbar.
- **Anwendungsstart**: Die Anwendung konnte nicht gestartet werden.

### Schritt 4: Anzeigen der Testergebnisse

Sie können die neuesten Testergebnisse in Citrix DaaS auf der Seite **Anwendungen** anzeigen.




Zur weitergehenden Fehlerbehebung klicken Sie auf einen Ergebnislink, um auf der Seite **Trends** > **Anwendungstestergebnisse** weitere Details aufzurufen.

Auf dieser Seite werden die konsolidierten Ergebnisdaten für die letzten 24 Stunden oder die letzten 7 Tage angezeigt. Sie können die Phase sehen, in der ein Test fehlgeschlagen ist. Sie können die Tabelle nach Anwendungen, Fehlerphasen oder Endpunktmaschinen filtern.

## Desktoptests

February 14, 2023

Das Desktoptestfeature automatisiert die Überprüfung der Integrität der in einer Site veröffentlichten Citrix Virtual Desktops. Das Ergebnis der Desktoptests steht unter "Überwachen"zur Verfügung. Citrix Probe Agent unterstützt jetzt Sites, die auf den Steuerungsebenen für Citrix Cloud Japan und Citrix Cloud Government gehostet werden.

Konfigurieren Sie auf der Seite "Konfiguration"unter "Überwachen"die zu testenden Desktops, die Endpunktmaschinen zur Ausführung der Tests und die Testzeit. Der Agent testet den Start der ausgewählten Desktops mit Workspace und meldet das Ergebnis in "Überwachen". Die Testergebnisse werden in der Benutzeroberfläche von "Überwachen"angezeigt: die Daten der letzten 24 Stunden auf der Seite "Anwendungen"und die historischen Daten auf der Seite **Trends > Ergebnisse der Desktoptests**.

Hier sehen Sie die Phase, in der Fehler aufgetreten sind: Workspace-Erreichbarkeit, Workspace-Authentifizierung, Workspace-Enumeration, ICA-Download oder Desktopstart. Der Fehlerbericht wird per E-Mail an die konfigurierten Adressen gesendet.

Sie können die Durchführung von Desktoptests außerhalb der Spitzenzeiten in mehreren Regionen planen. Die umfassenden Testergebnisse können helfen, Probleme bei Desktops, Hostmaschinen oder Verbindungen zu beheben, bevor sie sich bei den Benutzern bemerkbar machen.

Für dieses Feature ist Probe Agent 1903 oder höher erforderlich.

Anforderungen:

- Endpunktmaschinen mit Testagents sind Windows-Maschinen mit Citrix Receiver für Windows 4.8 oder höher oder der Citrix Workspace-App für Windows (früher Citrix Receiver für Windows)

1906 oder höher. Die Workspace-App für Unified Windows Platform (UWP) wird nicht unterstützt.
- Citrix Probe Agent unterstützt die formularbasierte Standardauthentifizierung, wie sie von StoreFront und Citrix WorkSpace unterstützt wird. Citrix Probe Agent unterstützt keine anderen Authentifizierungsmethoden wie Single Sign-On (SSO) oder Multifaktorauthentifizierung (MFA). Ähnlich funktioniert der Citrix Probe Agent nur, wenn kein Proxyserver oder Load Balancer wie Citrix Gateway oder Citrix ADC eingesetzt wird.
- Stellen Sie sicher, dass auf der Endpunktmaschine, auf der Sie den Probe Agent installieren möchten, Microsoft .NET Framework Version 4.7.2 oder höher installiert ist.
- Um den Testagent in der Steuerungsebene für Citrix Cloud Japan zu verwenden, wählen Sie im Pfad "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" den Registrierungswert 2. Um den Testagent in der Steuerungsebene für Citrix Cloud Government zu verwenden, wählen Sie im Pfad "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeA den Registrierungswert 3.

Zum Ausführen von Desktoptests erforderliche Benutzerkonten bzw. Berechtigungen:

- Eindeutiger Workspace-Benutzer auf jeder Endpunktmaschine. Der Workspace-Benutzer muss kein Administrator sein; die Testmodule können in einem Nicht-Administratorkontext ausgeführt werden.
- Benutzerkonten mit Windows-Administratorberechtigung zum Installieren und Konfigurieren von Citrix Probe Agent auf den Endpunktmaschinen
- Ein Volladministratorkonto oder eine benutzerdefinierte Rolle mit den folgenden Berechtigungen. Die Wiederverwendung normaler Benutzerkonten für Desktoptests kann zur Abmeldung der Benutzer von den aktiven Sitzungen führen.
  - Bereitstellungsgruppenberechtigungen:
    - Nur Lesen
  - Überwachungsberechtigungen:
    - E-Mail-Serverkonfiguration erstellen, bearbeiten, entfernen (sofern der E-Mail-Server noch nicht konfiguriert ist)
    - Testkonfigurationen erstellen, bearbeiten, entfernen
    - Konfigurationsseite anzeigen
    - Trendseite anzeigen

### Desktoptests konfigurieren

Sie können die Durchführung von Desktoptests außerhalb der Spitzenzeiten in mehreren Regionen planen. Die umfassenden Testergebnisse können helfen, Probleme bei Desktops, Hostcomputern oder Verbindung zu beheben, bevor sie sich bei den Benutzern bemerkbar machen.

Citrix Probe Agent Version 2103 unterstützt die Siteaggregation. Anwendungen und Desktops aggregierter Sites können angezeigt und gestartet werden. Wenn Sie den Probe Agent konfigurieren, wählen Sie die Option **Siteaggregation für Workspace (StoreFront) aktiviert**, um die Anzeige von Anwendungen und Desktops von aggregierten Sites zu ermöglichen. Die folgenden Sitekombinationen werden unterstützt:

- Mehrere On-Premises-Sites mit einer StoreFront-URL.
- On-Premises- und Cloudsites mit einer StoreFront-URL oder einer Workspace-URL.
- Mehrere Cloudsites mit einer Workspace-URL.

> **Hinweis:**
>
> Sie müssen separate Administratoren oder Benutzer erstellen, um Tests zu konfigurieren, die nur auf eine Site zugreifen können.

#### Schritt 1: Installieren und Konfigurieren von Citrix Probe Agent

Citrix Probe Agent ist eine ausführbare Windows-Datei, die den Desktopstart durch einen Benutzer über Workspace simuliert. Der Agent testet Desktopstarts gemäß der Konfiguration unter "Überwachen"und meldet die Ergebnisse unter "Überwachen".

1. Identifizieren Sie die Endpunktmaschinen, auf denen Sie Desktoptests ausführen möchten.
2. Benutzer mit Administratorberechtigung können Citrix Probe Agent auf den Endpunktmaschinen installieren und konfigurieren. Laden Sie die ausführbare Datei von Citrix Probe Agent von folgender Webseite herunter: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Starten Sie den Agent und konfigurieren Sie Ihre Workspace-Anmeldeinformationen für Receiver für Web. Konfigurieren Sie einen eindeutigen Workspace-Benutzer auf jeder Endpunktmaschine. Die Anmeldeinformationen werden verschlüsselt und sicher gespeichert.

   > **Hinweise:**
   >
   > - Um auf die gewünschte Site von außerhalb des Netzwerks zuzugreifen, geben Sie in das Feld "Workspace-URL"die URL für Citrix Gateway-Anmeldeseite ein. Citrix Gateway leitet die Anforderung automatisch an die entsprechende Workspace-URL weiter. Das Feature ist ab Citrix Gateway-Version 12.1 verfügbar.
   > - Verwenden Sie NetBIOS als Domänenname im Feld "Benutzername". Beispiel: NetBIOS/Benutzername.
   > - Desktop-Tests unterstützen Citrix Content Collaboration mit Workspace-Authentifizierung (nur AD).
   > - Sie müssen die interaktive Anmeldung für den konfigurierten eindeutigen StoreFront-

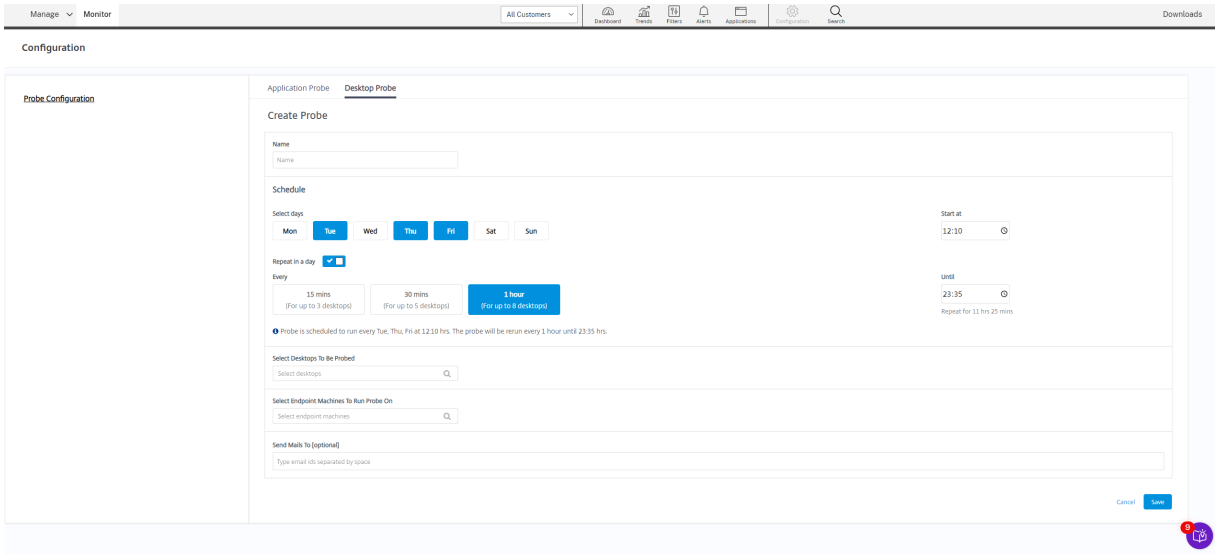
> Benutzer aktivieren.

4. Geben Sie auf der Registerkarte **Anzeige der Testergebnisse konfigurieren** Ihre Anmeldeinformationen für "Überwachen"ein. Kundennamen bzw. Kunden-ID, Client-ID und den geheimen Schlüssel finden Sie auf der API-Zugriffsseite der Citrix Cloud-Konsole.

### Schritt 2: Konfigurieren von Desktoptests in "Überwachen"

1. Gehen Sie in Citrix DaaS zu **Konfiguration** > **Testkonfiguration** > **Anwendungstest** und klicken Sie auf **Test erstellen**.
2. Geben Sie auf der Seite **Test erstellen** den Namen des Tests ein.
3. Wählen Sie den Zeitplan aus:
   a) Wählen Sie die Wochentage, an denen der Test ausgeführt werden soll.
   b) Geben Sie eine Startzeit für den Test ein.
   c) Sie können auch die Option **An einem Tag wiederholen** auswählen. Geben Sie die Endzeit ein und wie oft der Test innerhalb eines Tages wiederholt werden soll. In der folgenden Konfiguration können Desktoptests beispielsweise jeden Dienstag, Donnerstag und Freitag von 12:10 Uhr bis 23:35 Uhr ausgeführt und stündlich wiederholt werden.
4. Wählen Sie abhängig vom Intervall die empfohlene Anzahl von Desktops aus.
5. Wählen Sie die Endpunktmaschinen aus, auf denen der Test ausgeführt werden muss.
6. Geben Sie die E-Mail-Adressen ein, an die die Ergebnisse des Testmoduls gesendet werden und klicken Sie auf **Speichern**.

In dieser Konfiguration starten die Desktopsitzungen jeden Dienstag, Donnerstag und Freitag um 12:10 Uhr, 13:10 Uhr, 14:10 Uhr usw. bis 23:10 Uhr.



> **Hinweis:**
>
> - Konfigurieren Sie Ihren E-Mail-Server unter **Warnungen** > **E-Mail-Server-Konfiguration**.
> - Nach der Konfiguration des Desktoptests führt der Agent die konfigurierten Tests ab der nächsten Stunde aus.
> - Tests, die vor Einführung der Option **An einem Tag wiederholen** eingerichtet wurden, werden weiterhin zur geplanten Zeit ausgeführt. Die Option **An einem Tag wiederholen** ist für diese Tests standardmäßig deaktiviert.

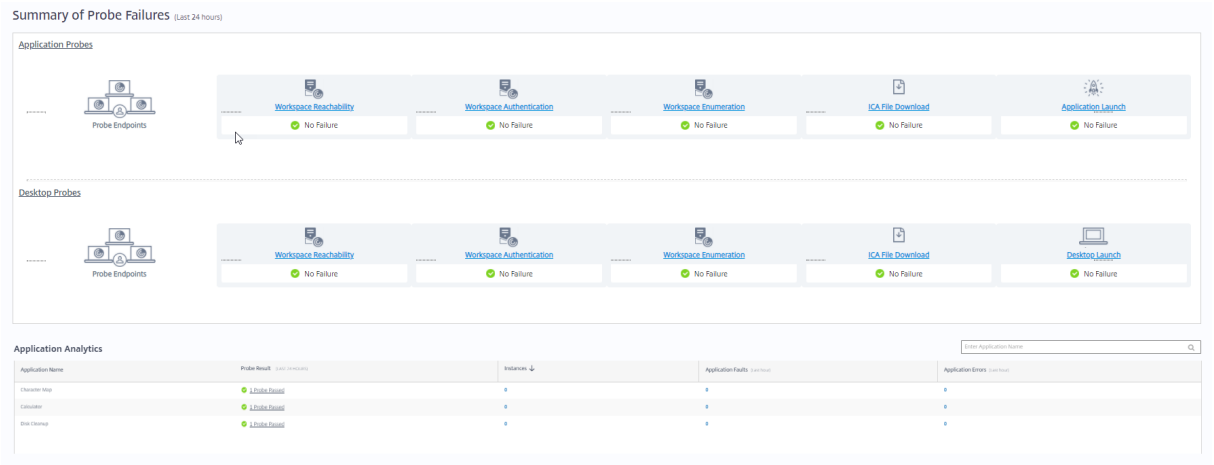
### Schritt 3: Ausführen des Tests

Der Agent führt Desktoptests regelmäßig entsprechend der von Monitor abgerufenen Konfiguration aus. Er startet ausgewählte Desktops der Reihe nach über Workspace. Die Ergebnisse werden über die Überwachungsdatenbank gemeldet. Fehler werden für fünf spezifische Phasen gemeldet:

- **Workspaceerreichbarkeit:** Die konfigurierte Workspace-URL ist nicht erreichbar.
- **Workspaceauthentifizierung:** Die konfigurierten Workspace-Anmeldeinformationen sind ungültig.
- **Workspaceenumeration**: Die Liste der enumerierten Desktops in Workspace enthält die getestete Desktops nicht.
- **ICA-Download**: Die ICA-Datei ist nicht verfügbar.
- **Desktopstart:** Der Desktop kann nicht gestartet werden.

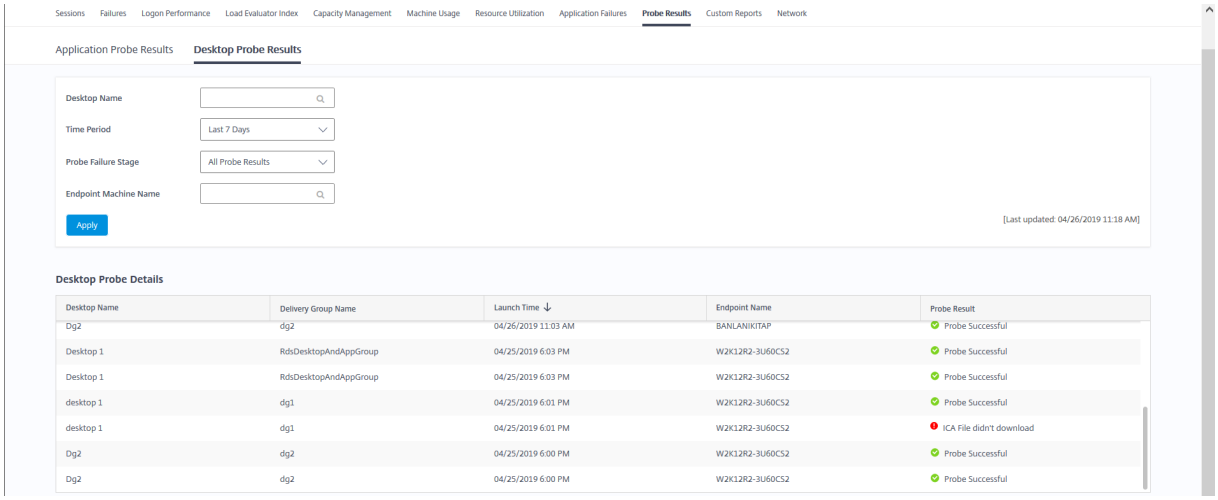
### Schritt 4: Anzeigen der Testergebnisse

Sie können die neuesten Testergebnisse auf der Seite **Desktops** anzeigen.




Zur weitergehenden Fehlerbehebung klicken Sie auf einen Ergebnislink, um auf der Seite **Trends** > **Testergebnisse** > **Desktoptestergebnisse** weitere Details aufzurufen.




Auf dieser Seite werden die konsolidierten Ergebnisdaten für die letzten 24 Stunden oder die letzten 7 Tage angezeigt. Sie können die Phase sehen, in der ein Test fehlgeschlagen ist. Sie können die Tabelle nach Desktops, Fehlerphasen oder Endpunktmaschinen filtern.

## Problembehandlung bei Maschinen

May 17, 2024

> **Hinweis:**
>
> **Citrix Health Assistant** ist ein Tool zum Beheben von Konfigurationsproblemen bei nicht registrierten VDAs. Durch verschiedene automatisierte Systemdiagnosen wird die mögliche Ursache von Konfigurationsproblemen bei der VDA-Registrierung, beim Sitzungsstart und bei der Zeitzonenumleitung gesucht. Der Knowledge Center-Artikel Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch enthält eine Downloadversion von **Citrix Health Assistant** und Anweisungen zu dessen Verwendung.

Die Ansicht **Filter > Maschinen** auf der Registerkarte “Überprüfen”zeigt die in der Site konfigurierten Maschinen an. Die Registerkarte “Maschinen mit Multisitzungs-OS”enthält den Lastauswertungsindex, der die Verteilung der Leistungsindikatoren angibt, und Quickinfos zur Sitzungsanzahl, die Sie aufrufen können, wenn Sie mit der Maus auf den Link zeigen.

Klicken Sie für fehlerhafte Maschinen auf die Spalte **Fehlerursache**, um eine detaillierte Beschreibung des Fehlers und Empfehlungen zur Behebung aufzurufen. Informationen zu Ursachen von Maschinen- und Verbindungsfehlern sowie empfohlene Korrekturmaßnahmen finden Sie in dem Handbuch Citrix Director Failure Reasons Troubleshooting Guide.

Klicken Sie auf Link mit dem Maschinennamen, um die Seite **Maschinendetails** aufzurufen.

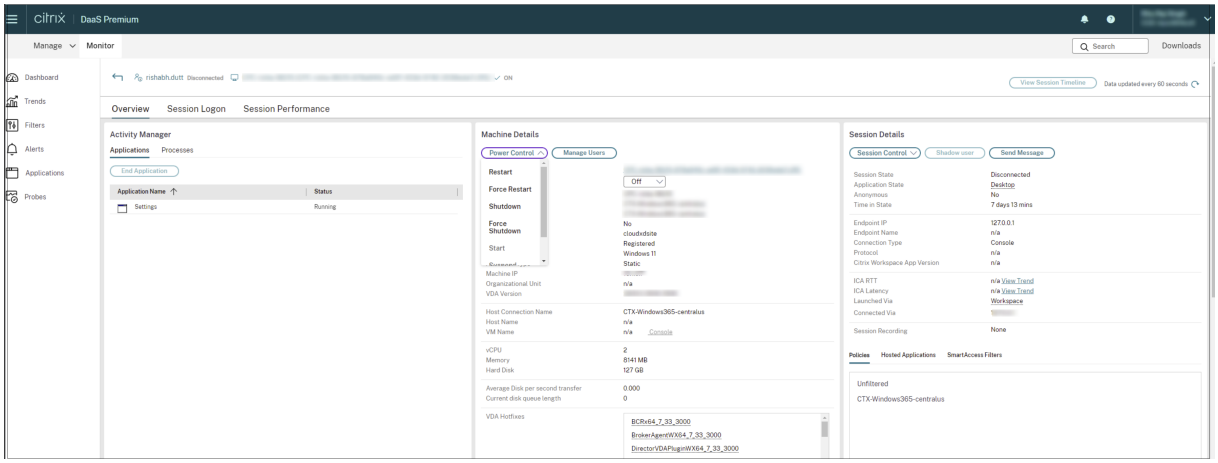
Die Seite “Maschinendetails”enthält die Einzelheiten zu der Maschine, der Infrastruktur und den auf die Maschine angewandten Hotfixes.

**Unterstützung für HDX Plus für Windows 365-Cloud-PCs und Azure Virtual Desktops:**

> **Hinweis:**
>
> Für HDX Plus für Windows 365-Cloud-PCs sind nur die Energieverwaltungsoptionen “Neustart” und “Neustart erzwingen”verfügbar. Für Azure Virtual Desktops (AVD) sind alle Energieverwaltungsoptionen verfügbar.

Sie können die verfügbaren Energieverwaltungsoptionen mit einer der folgenden Methoden anzeigen:

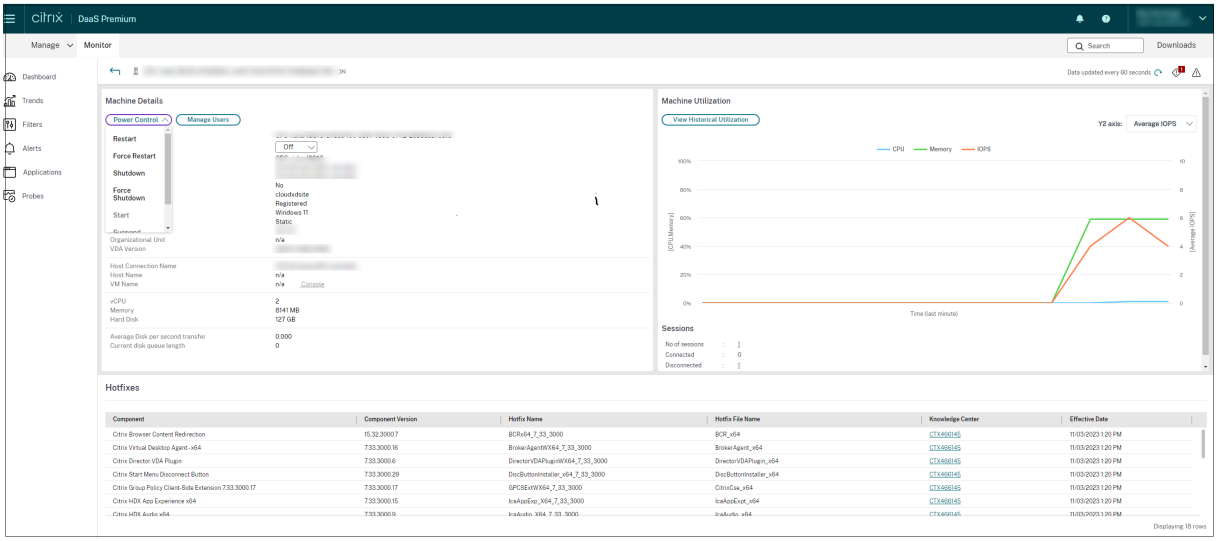
Klicken Sie auf **Filter** -> **Sitzungen** -> **Details anzeigen** -> **Maschinendetails** -> **Energieverwaltung** in der Dropdownliste und wählen Sie eine Option aus, um einer Maschine die erforderliche Energieverwaltungsoption zuzuweisen.




Oder

Klicken Sie auf **Filter** -> **Maschine** -> **Maschinendetails** -> **Energieverwaltung** in der Dropdownliste und wählen Sie eine Option aus, um einer Maschine die erforderliche Energieverwaltungsoption zuzuweisen.

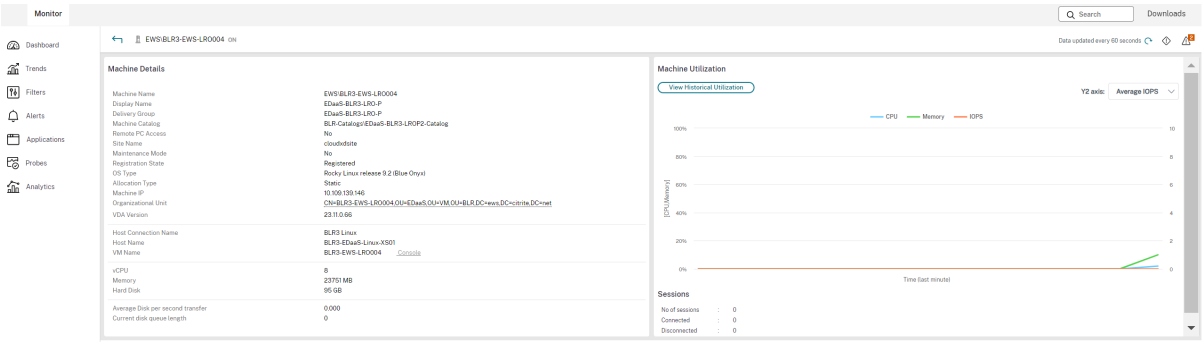
 




## Echtzeit-Ressourcennutzung auf Maschinen

Im Bereich **Maschinenauslastung** wird die Echtzeit-Auslastung von CPU und Speicher angezeigt. Darüber hinaus stehen für Sites mit VDAs ab Version 7.14 Diagramme zur Datenträger- und GPU-Überwachung zur Verfügung.

Datenträgerüberwachung, durchschnittliche IOPS und Datenträgerlatenz sind wichtige Kennzahlen für die Leistungsmessung, mit deren Hilfe Sie VDAs überwachen und Probleme bei VDA-Datenträgern beheben können. Das Diagramm der durchschnittlichen IOPS repräsentiert die durchschnittliche Zahl der Lese-/Schreibvorgänge auf einem Datenträger. Wählen Sie **Datenträgerlatenz**, um ein Diagramm der Verzögerung zwischen Datenanforderungen und Datenrückgabe vom Datenträger in Millisekunden anzuzeigen.




### GPU-Auslastung

Über **GPU-Auslastung** können Sie die prozentuale Auslastung von GPU, GPU-Speicher und Encoder sowie Decoder aufrufen und anhand dieser Informationen GPU-Probleme auf Multisitzungs-OS- oder Einzelsitzungs-OS-VDAs behandeln.

**Unterstützte GPU-Versionen:**

- NVIDIA Tesla M60-GPUs mit Display Driver Version 369.17 oder höher. Weitere Informationen finden Sie unter NVIDIA vGPU Software.
- AMD Radeon Instinct MI25-GPUs und AMD EPYC 7V12-CPUs (Rom). Weitere Informationen finden Sie unter AMD Drivers and Support.

**Treiber:**

Die entsprechenden Treiber oder Erweiterungen müssen auf den VDAs installiert sein.

- Installieren Sie für NVIDIA-GPUs die GRID-Treiber manuell oder über Erweiterungen. Weitere Informationen finden Sie unter NVIDIA vGPU Software.
  - Beachten Sie, dass für NVIDIA nur GRID-Treiber unterstützt werden. CUDA-Treiber funktionieren nicht mit der NVadsA10 v5-Serie und werden nicht unterstützt.
  - Ein Beispielverfahren für die Installation von Nvidia Grid GPU-Treibern über Erweiterungen auf Azure-basierten Maschinen finden Sie unter NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - Ein Beispielverfahren für die manuelle Installation von Nvidia Grid GPU-Treibern finden Sie unter Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Installieren Sie für AMD-GPUs AMD-Grafiktreiber manuell oder über Erweiterungen. Weitere Informationen finden Sie unter AMD Drivers and Support.
  - Ein Beispielverfahren für die Installation von AMD GPU-Treibern über Erweiterungen auf Azure-basierten Maschinen finden Sie unter AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - Ein Beispielverfahren für die manuelle Installation von AMD GPU-Treibern auf Azure-Maschinen finden Sie unter Install AMD GPU drivers on N-series VMs running Windows.

**Hinweise zur Verwendung:**

- Die GPU-Auslastungsdiagramme sind nur für VDAs verfügbar, auf denen 64-Bit-Windows ausgeführt wird.
- Die Diagramme zur AMD-GPU-Auslastung sind nur für VDAs verfügbar, auf denen Citrix Virtual Apps and Desktops 7 2212 oder höher ausgeführt wird.
- Auf den VDAs muss HDX 3D Pro für die GPU-Beschleunigung aktiviert sein. Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Einzelsitzungs-OS sowie GPU-Beschleunigung für Windows-Multisitzungs-OS.
- Wenn ein VDA auf mehrere GPUs greift, zeigt das Auslastungsdiagramm den Durchschnitt der bei den einzelnen GPUs gesammelten Kennzahlen. GPU-Kennzahlen werden für den gesamten VDA und nicht für einzelne Prozesse gesammelt.

- Für AMD werden Encoder und Decoder nicht getrennt unterstützt. Jede Codierungs- und Decodierungsworkload, die die GPU verwendet, wird als allgemeine 3D-Last der GPU-Workload gemeldet.
- Stellen Sie sicher, dass Sie NVIDIA WMI während der Installation installieren. Dieses Fenster ist nur während der manuellen Installation verfügbar.
- Wenn Treiber installiert sind, Director die GPU jedoch nicht erkennt
  - Sehen Sie im Task-Manager nach. Wenn die Treiber ordnungsgemäß installiert sind, sollte die GPU im Task-Manager angezeigt werden.
  - Prüfen Sie, ob die Maschine registriert ist. Manchmal kann es einige Zeit dauern, bis Maschinen als online erkannt werden.
- Wenn die GPU-Auslastung in Director keine Aktivität anzeigt, vergewissern Sie sich, dass die von Ihnen ausgeführte Workload die GPU verwendet. Für Grafikworkloads können Sie über "Einstellungen > System > Anzeige > Grafikeinstellungen > App auswählen"die Präferenz festlegen. Stellen Sie sicher, dass "High Performance"aktiviert ist. Manchmal verwendet Windows standardmäßig die CPU für Grafikworkloads, wenn auf der Grundlage anderer Einstellungen der Systemstandard oder Energiesparen eingestellt ist.
- Die Daten werden jede Minute aktualisiert und die Datenvisualisierung beginnt innerhalb einer Minute nach der Auswahl der **GPU-Auslastung**.

### Historische Ressourcennutzung auf Maschinen

Klicken Sie im Bereich **Maschinenauslastung** auf **Historische Auslastung anzeigen**, um die historische Auslastung der Ressourcen auf der ausgewählten Maschine anzuzeigen.
Die Auslastungsdiagramme enthalten wichtige Leistungsindikatoren für CPU, Speicher, maximale gleichzeitige Sitzungen, durchschnittliche IOPS und Datenträgerlatenz.

> **Hinweis:**
>
> Die Überwachungsrichtlinieneinstellung **Prozessüberwachung aktivieren** muss auf "Zugelassen"festgelegt sein, damit Daten für die Tabelle "Top-10-Prozesse"auf der Seite "Historische Maschinenauslastung"gesammelt und angezeigt werden können. Die Sammlung ist standardmäßig auf "Nicht zugelassen"festgelegt.

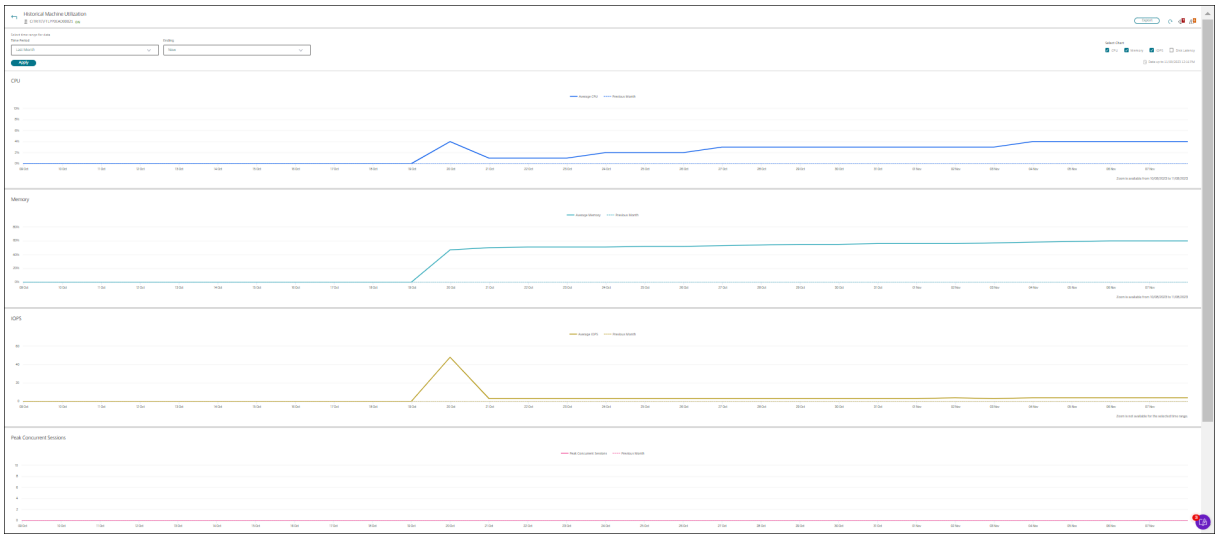
Daten zur CPU- und Arbeitsspeicherauslastung sowie IOPS und Datenträgerlatenz werden standardmäßig gesammelt. Die Datensammlung kann über die Richtlinieneinstellung **Ressourcenüberwachung aktivieren** deaktiviert werden.


1. Wählen Sie im Bereich **Maschinenauslastung** der Ansicht **Maschinendetails** die Option **Historische Auslastung anzeigen**.
2. Legen Sie auf der Seite **Historische Maschinenauslastung** die Option **Zeitraum** auf die letzten 2 oder 24 Stunden, auf die letzten 7 Tage, den letzten Monat oder das letzte Jahr fest.

   > **Hinweis:**
   >
   > IOPS-Durchschnitt und Datenträgerlatenz sind für die letzten 24 Stunden, den letzten Monat und das letzte Jahr verfügbar. Eine benutzerdefinierte Einstellung der Endzeit wird nicht unterstützt.

3. Klicken Sie auf **Anwenden** und wählen Sie die erforderlichen Diagramme aus.
4. Zeigen Sie auf die einzelnen Abschnitte des Diagramms, um weitere Informationen zu dem ausgewählten Zeitabschnitt einzublenden.



Wenn Sie beispielsweise **Letzte 2 Stunden** auswählen, gelten als Basiszeitraum die 2 Stunden vor dem ausgewählten Zeitraum. Angezeigt werden die Trends für CPU, Arbeitsspeicher und Sitzungen über die letzten 2 Stunden und die Grundlinienzeit. Wenn Sie **Letzten Monat** auswählen, gilt der Vormonat als Basiszeitraum. Wählen Sie die Anzeige der durchschnittlichen IOPS und Datenträgerlatenz im letzten Monat und den Basiszeitraum.

1. Klicken Sie auf **Exportieren**, um die Ressourcenauslastungsdaten für den gewählten Zeitraum zu exportieren. Weitere Informationen finden Sie unter "Überwachen von Bereitstellungen"im Abschnitt Exportieren von Berichten.
2. Unterhalb der Diagramme wird eine Tabelle mit den 10 Prozessen mit der höchsten CPU- bzw. Speicherauslastung angezeigt. Sie können diese nach einer beliebigen Spalte (Anwendungsname, Benutzername, Sitzungs-ID, CPU-Durchschnitt, CPU-Maximum, Speicherdurchschnitt und Speichermaximum) sortieren. Die Spalten für IOPS und Datenträgerlatenz können nicht sortiert werden.

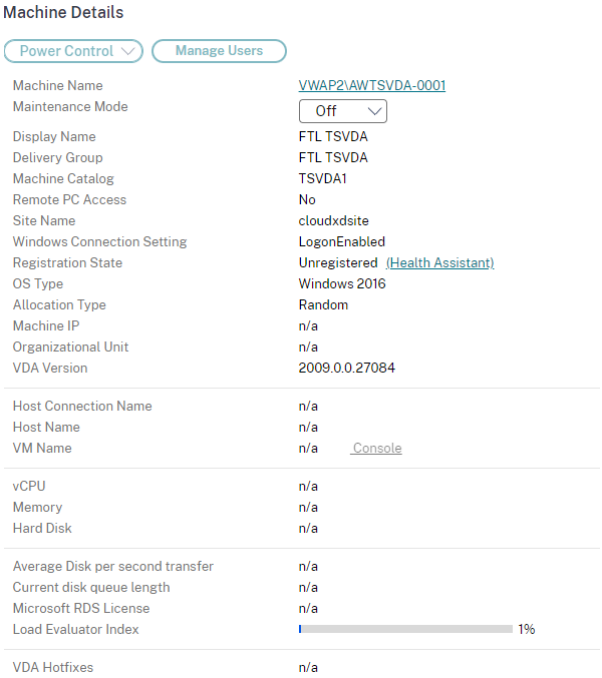
   > **Hinweis:**
   >
   > - Die Sitzungs-ID für Systemprozesse wird mit "0000"angegeben.
   > - Wenn eine zu Citrix Cloud Japan oder Citrix Cloud Government gehörende Site mehr als 5000 Maschinen enthält, sind Prozessdaten nur für bis zu 2000 Maschinen verfügbar. Die Prozessüberwachungsrichtlinie muss auf diesen Maschinen aktiviert sein.

3. Zum Anzeigen des historischen Trends für den Ressourcenverbrauch einzelner Prozesse können Sie einen Drilldown für jeden der aufgelisteten Top-10-Prozesse durchführen.

### Zugriff auf die Maschinenkonsole

Sie können auf die Konsolen von Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS, die unter XenServer ab Version 7.3 gehostet werden direkt über "Überwachen"zugreifen. XenCenter ist dann nicht zur Problembehandlung von auf XenServer gehosteten VDAs erforderlich. Damit dieses Feature verfügbar ist, muss der XenServer, der die Maschine hostet, in Version 7.3 oder höher vorliegen und über den Überwachungsdienst zugänglich sein.




Zur Problembehandlung auf einer Maschine klicken Sie im zugehörigen Bereich "Maschinendetails" auf den Link **Konsole**. Nach Authentifizierung der von Ihnen angegebenen Hostanmeldeinformationen wird die Maschinenkonsole mit dem webbasierten VNC-Client noVNC auf einer separaten Registerkarte geöffnet. Sie haben nun über Tastatur und Maus Zugriff auf die Konsole.

> **Hinweis:**
>
> - Das Feature wird unter Internet Explorer 11 nicht unterstützt.
> - Ist der Mauszeiger auf der Maschinenkonsole nicht korrekt ausgerichtet, finden Sie unter CTX230727 einen Fix.
> - Der Konsolenzugriff wird auf einer neuen Registerkarte gestartet. Vergewissern Sie sich daher, dass Ihre Browsereinstellungen Popups zulassen.
> - Citrix empfiehlt aus Sicherheitsgründen die Installation von SSL-Zertifikaten in Ihrem Browser.

### Maschinen mit kürzlich erfolgten Energieaktionen überprüfen

Sie können jetzt Maschinen mit erfolgreichen und fehlgeschlagenen Energieaktionen überprüfen. Mit diesem Feature können Sie Folgendes analysieren:

- Stromausfall, der Benutzerprobleme verursacht
- Fehler beim Abschalten, der die Kosten erhöht

> **Hinweis:**
>
> Daten sind nur für eine energieverwaltete Maschine verfügbar. Für die Energieaktionen, die vor der Unterstützung des Features ergriffen wurden, sind keine Daten verfügbar.

Sie können den Status der Energieaktionen auf Maschinen wie folgt anzeigen:

Über die Registerkarte **Filter** -> **Maschinen**. In diesem Fall sind standardmäßig die Spalten **Power Action Time** und **Power Action Result** sichtbar. Sie können auswählen, welche Spalten sichtbar sein sollen.

Auf der Registerkarte **Kostenoptimierung**. In diesem Fall ist der Standardfilter **Power Action Triggered by** auf *Autoscale* und das **Power Action Result** auf *Failed* gesetzt.

Mit diesem Feature können Sie die Details der Energieaktionsbefehle anzeigen. Sie können beispielsweise sehen, wer die Aktion ausgelöst hat, welche Aktion den Energiezustand geändert hat, den Grund für den Ausfall und den Zeitpunkt, zu dem die Aktion abgeschlossen ist. Sie können diese Details auch exportieren.

Die folgenden Filter wurden hinzugefügt, um den Status der Energieaktion anzuzeigen:

| Filter | Beschreibung |
| --- | --- |
| Ergebnis der Energieaktion | Zeigt das Ergebnis der Energieaktion an. Die möglichen Filterwerte sind “erfolgreich”und “fehlgeschlagen”. |
| Power Action Triggered By | Zeigt an, wer oder was die Energieaktion ausgelöst hat. Die möglichen Filterwerte sind<br>• Autoscale: Dieser Wert wird angezeigt, wenn eine Energieaktion durch folgende Umstände ausgelöst wird<br>• Wenn der Administrator eine VM herunterfährt, um den Betriebssystemdatenträger der VM wieder in den ursprünglichen Zustand zu versetzen<br>• Wenn eine VM aufgrund der festgelegten Richtlinien heruntergefahren oder angehalten wird<br>• Wenn eine VM basierend auf der Pool- oder Puffergrößenkonfiguration verfügbar gemacht wird |

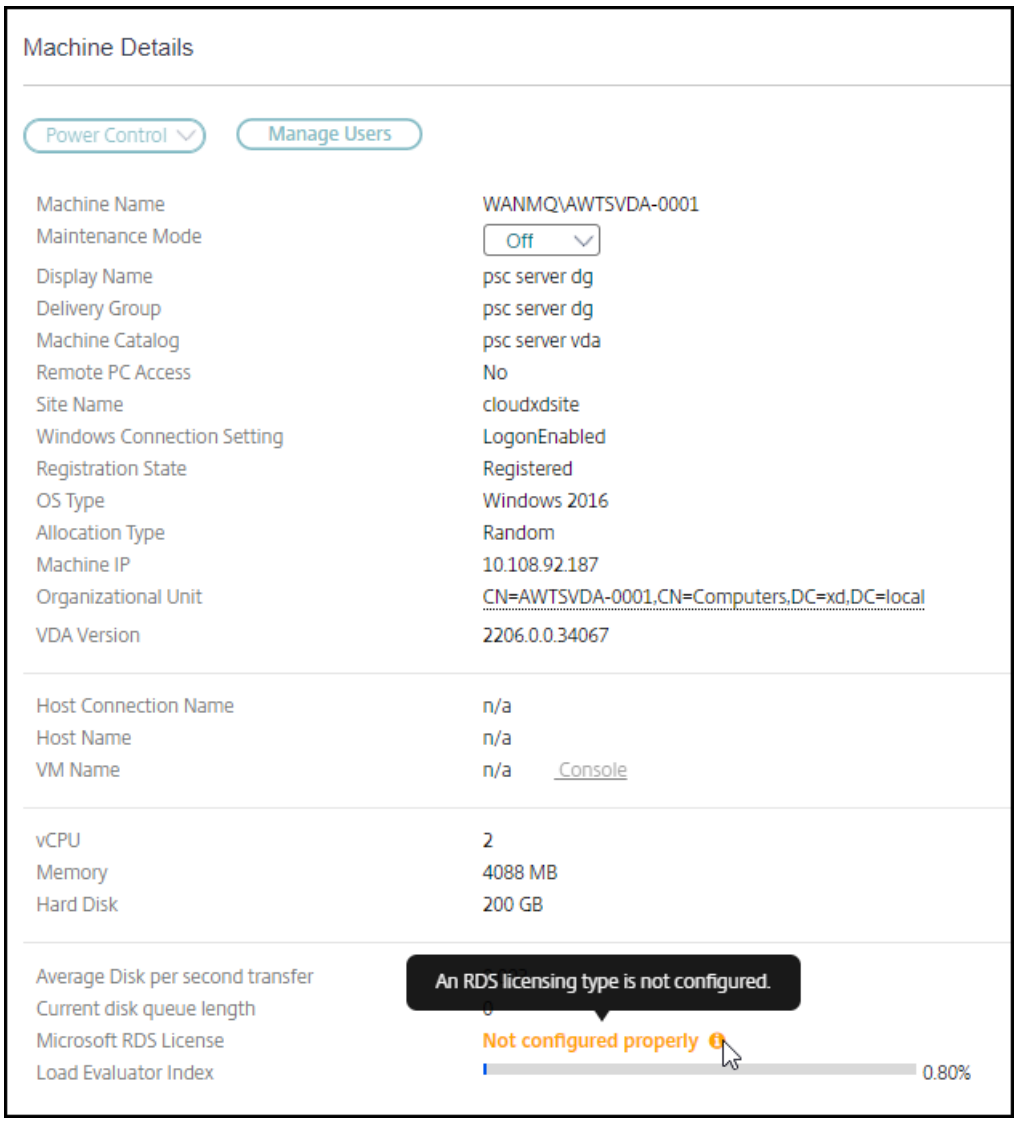
 

| Filter | Beschreibung |
| --- | --- |
| | • Administrator: Dieser Wert wird angezeigt, wenn eine Energieaktion von einem Administrator ausgelöst wird. Dies ist zum Beispiel der Fall, wenn der Administrator das Ausschalten, Einschalten, Anhalten, Wiederaufnehmen, Neustarten oder erneutes Hochfahren einer VM anfordert.<br>• Benutzer: Dieser Wert wird angezeigt, wenn eine Energieaktion von einem Benutzer ausgelöst wird. Dies ist zum Beispiel der Fall, wenn ein Benutzer die VM zurücksetzt, einschaltet oder die Arbeit an ihr wieder aufnimmt.<br>• Andere: Dieser Wert wird angezeigt, wenn die Stromzufuhr aus geplanten und unbekannten Gründen ausgelöst wird. |
| Last Power Action | Zeigt die genaue Aktion an, die an der Maschine stattgefunden hat, z. B. Einschalten, Ausschalten, Herunterfahren, Neustarten, Zurücksetzen, Wiederaufnehmen usw. |
| Power Action Time | Die Zeit, zu der die Energieaktion abgeschlossen ist. Gefiltert werden kann nach Letzte Minute, Letzte 5 Minuten, Letzte 30 Minuten, Letzte Stunde, Heute, Letzte 24 Stunden und Gestern. |
| Power Action Failure Reason | Zeigt den Grund für den Fehler an. Die möglichen Filterwerte sind: Vom Hypervisor gemeldeter Ausfall, Überschreitung der Hypervisorratenbegrenzung, unbekannter Fehler und keiner. Wenn eine Aktion erfolgreich ist, wird “Keiner”angezeigt. |

### Microsoft RDS-Lizenzstatus

Sie können den Status der Lizenz für Microsoft RDS (Remotedesktopdienste) im Fenster “Maschinendetails”auf den Seiten **Maschinendetails** und **Benutzerdetails** auf Maschinen mit Multisitzungs-OS anzeigen.




Eine der folgenden Meldungen wird angezeigt:

- Lizenz verfügbar
- Nicht richtig konfiguriert (Warnung)
- Lizenzfehler (Fehler)
- Nicht kompatible VDA-Version (Fehler)

> **Hinweis:**
>
> Der Status der RDS-Lizenz für Maschinen mit gültiger Lizenz im Kulanzzeitraum wird als **Lizenz verfügbar** in grün angezeigt. Erneuern Sie die Lizenzen, bevor sie ablaufen.

Zum Anzeigen von Warn- und Fehlermeldungen (siehe Tabelle unten) zeigen Sie mit der Maus auf das Infosymbol.

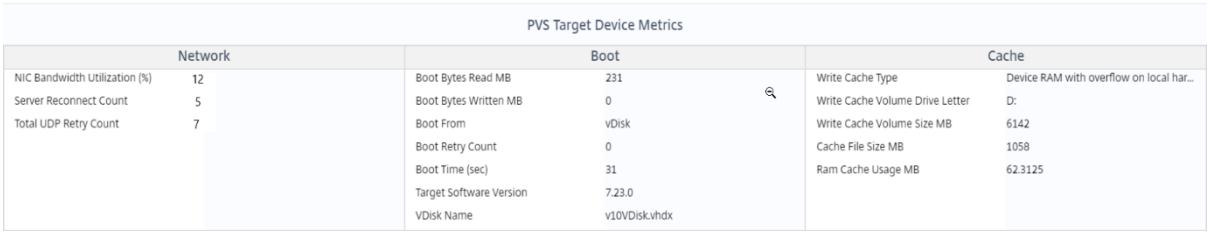
| Meldungstyp | Meldung in Überwachung |
|---|---|
| Fehler | Verfügbar ab VDA-Version 7.16 |
| Fehler | Neue RDS-Verbindungen sind nicht erlaubt. |
| Fehler | RDS-Lizenzierung hat den Kulanzzeitraum überschritten. |
| Fehler | Ein Lizenzserver ist nicht für die erforderliche Betriebssystemstufe mit dem Lizenztyp 'Pro Gerät-Clientzugriffslizenz'konfiguriert. |
| Fehler | Der konfigurierte Lizenzserver ist nicht kompatibel mit der RDS-Hostbetriebssystemstufe des Lizenztyps 'Pro Gerät-Clientzugriffslizenz'. |
| Warnung | 'Persönlicher Terminalserver'ist kein gültiger RDS-Lizenztyp in einer Citrix Virtual Apps and Desktops-Bereitstellung. |
| Warnung | 'Remotedesktop für Verwaltung'ist in einer Citrix Virtual Apps and Desktops-Bereitstellung kein gültiger Lizenztyp. |
| Warnung | Kein RDS-Lizenztyp konfiguriert. |
| Warnung | Mit dem Lizenztyp 'Per User Client Access RDS' ist der Domänencontroller oder Lizenzserver nicht erreichbar. |
| Warnung | Mit dem Lizenztyp 'Pro Gerät-Clientzugriffslizenz'konnte die Clientgerätelizenz nicht ermittelt werden, da der Lizenzserver für die erforderliche Betriebssystemstufe nicht erreichbar ist. |

> **Hinweis:**
>
> Diese Funktion gilt nur für Microsoft RDS-CAL (Client Access License).

### Metriken der PVS-Zielgeräte

Sie können den Status von PVS-Zielgeräten für Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS auf der Seite **Maschinendetails** in Monitor anzeigen. In diesem Bereich stehen Metriken für **Netzwerk**, **Start** und **Cache** zur Verfügung. Mit diesen Metriken können Sie PVS-Zielgeräte überwachen und Probleme beheben, um den ordnungsgemäßen Betrieb zu gewährleisten.




**Netzwerk:**

- NIC-Bandbreitenauslastung: Durchschnittliche Bandbreitenauslastung aller Netzwerkkarten.
- Anzahl der Serverneuverbindungen: Anzahl der Neuverbindungen, die der Server aufgrund von Netzwerkproblemen, einem Serverneuausgleich oder Herunterfahren und Neustarts des Citrix Provisioning-Streamdiensts ausgeführt hat.
- Anzahl der UDP-Wiederholungen insgesamt: Anzahl der Versuche des Provisioning-Zielgeräts, mithilfe von UDP die Verbindung zum Bereitstellungsserver wiederherzustellen. Diese Metrik lässt erkennen, ob beim Citrix Provisioning-Streamdienst Netzwerkprobleme vorliegen (z. B. fehlerhafte Switchkonfigurationen).

**Start:**

- Startbytelesen MB: Beim Starten gelesene Bytes.
- Startbyteschreiben MB: Beim Starten geschriebene Bytes.
- Starten von: Startmedium (vDisk, lokaler Datenträger usw.).
- Startwiederholungsanzahl: Anzahl der Versuche, die Maschine zu starten.
- Startzeit: Zeit in Sekunden, die zum Starten der Maschine benötigt wurde. Standardmäßig gibt es eine Verzögerung von 5 Sekunden zwischen Wiederholungen. Wenn diese Verzögerung in den zweistelligen Bereich ansteigt, erhöht sich die Startzeit erheblich. Überprüfen Sie Ihre Provisioning-Konfiguration, um dieses Problem zu beheben.
- Zielsoftwareversion: Version der Provisioning-Zielgerätesoftware.
- vDisk-Name: vDisk, von der das Provisioning-Zielgerät gestartet wird.

**Cache:**

- Schreibcachetyp: Die vDisk kann auf verschiedene Cachetypen festgelegt werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX119469.
- Schreibcache Volumelaufwerksbuchstabe: Laufwerksbuchstabe für Schreibcachetypen mit Laufwerken.
- Schreibcache Volumegröße MB: Konfigurierte Volumegesamtgröße für den Schreibcache.
- Cachedateigröße in MB: Aktuelle Cachedateigröße (Cache im Geräte-RAM mit Überlauf auf Festplatte).

- RAM-Cachenutzung in MB: Aktuelle RAM-Cachegröße (Cache im Geräte-RAM mit Überlauf auf Festplatte). Verwenden Sie den Überlauf auf die Festplatte nur bei Bedarf. Diese Metrik ist nützlich zum Festlegen bzw. Optimieren der geeigneten RAM-Cachegröße.

Weitere Informationen finden Sie unter Verwenden der Statusleiste auf einem Zielgerät.

Das Provisioning von Metriken der Zielgeräte ist nur verfügbar für:

- Provisioning von Maschinen.
- Provisioningzielgeräte ab Version 7.19.
- VDAs ab Version 2003.

> **Hinweis:**
>
> Die Anzahl der Serverneuverbindungen und die Anzahl der UDP-Wiederholungen sind nur für Provisioning-Zielgeräte ab Version 1912 CU2 verfügbar.

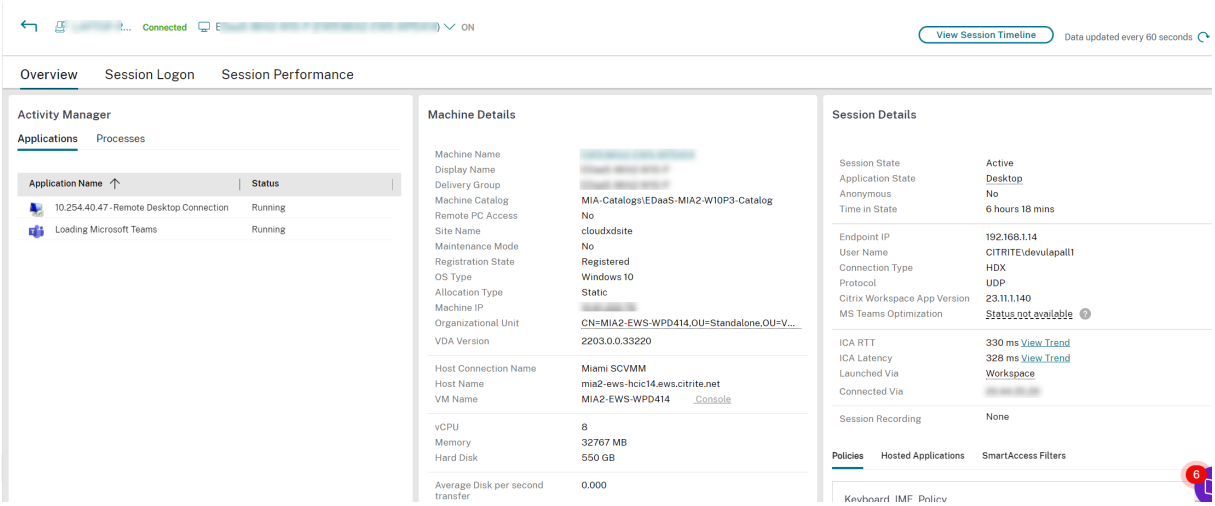
## Behandeln von Benutzerproblemen

May 17, 2024

Die Ansicht **Helpdesk** (Seite **Aktivitätsmanager**) des Überwachungsdiensts enthält Angaben zum Benutzer oder Endpunkt.


Wenn Sie im Aktivitätsmanager für Benutzer auf **Details anzeigen** klicken, wird die Seite **Benutzerdetails** geöffnet.
Wenn Sie im Aktivitätsmanager für Endpunkte auf **Details anzeigen** klicken, wird die Seite **Endpunktdetails** geöffnet.




Wenn der Benutzer mehrere Sitzungen gestartet hat, wird die Sitzungsauswahl angezeigt.


Wählen Sie eine Sitzung aus, um die Details anzuzeigen.

- Überprüfen Sie die Details zur Sitzung, zur Anmeldung des Benutzers, zum Sitzungsstart, zur Verbindung und zu den Anwendungen.
- Sie können die Maschine des Benutzers spiegeln.
- Behandeln Sie das Problem mit den in der folgenden Tabelle empfohlenen Aktionen und eskalieren Sie das Problem ggf. an den entsprechenden Administrator.

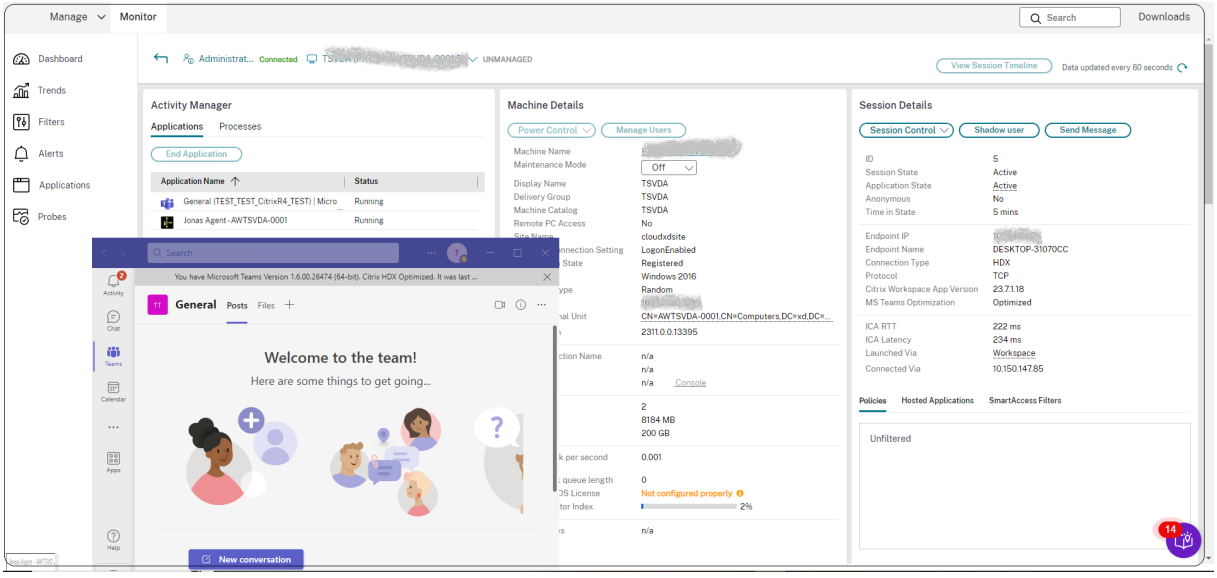
### Microsoft Teams-Optimierungsstatus

Citrix Monitor zeigt den Microsoft Teams-Optimierungsstatus für HDX-Sitzungen auf der Seite **Benutzerdetails** im Bereich **Sitzungsdetails** im Feld **MS Teams-Optimierung** an. Die Optimierung von Microsoft Teams ist entscheidend für eine bessere Benutzererfahrung, z. B. für klares Audio und Video. Aufgrund der Sichtbarkeit des Optimierungsstatus von Microsoft Teams kann der Zeitaufwand für die Lösung von Tickets reduziert werden und Administratoren können damit wichtige Kennzahlen bei der Problembehandlung identifizieren.

> **Hinweis:**
>
> Citrix Monitor unterstützt Microsoft Teams Version 2.1 oder früher.

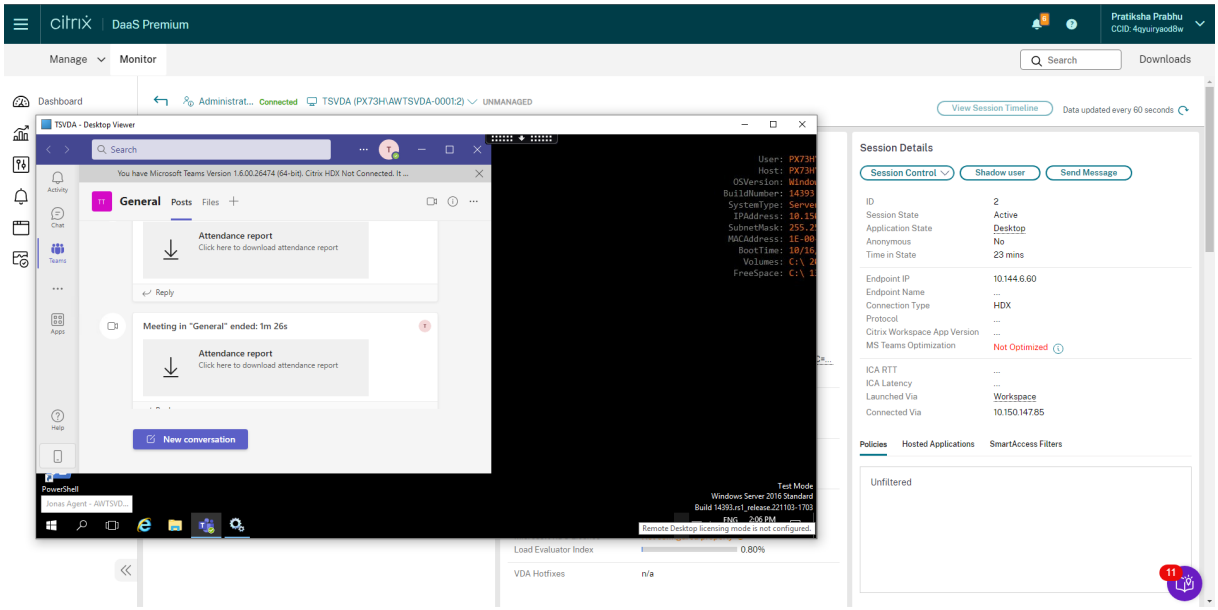
Voraussetzungen:

- Die unterstützten Versionen der Citrix Workspace-App sind unter Optimierung für Microsoft Teams aufgeführt.
- Microsoft Teams wird als veröffentlichte App oder auf einem veröffentlichten Desktop ausgeführt.
- Wichtige Dienste wie der Citrix HDX HTML5 Video Redirection Service werden ausgeführt.




Wenn Microsoft Teams nicht optimiert ist, enthält die QuickInfo einen Link zu einem externen Liveartikel zur Problembehandlung von HDX mit Tipps zur Optimierung von Microsoft Teams. Problembehandlung bei der HDX-Optimierung.




## Tipps zur Problembehandlung

| Benutzerproblem | Vorschläge |
|---|---|
| Anmeldung dauert lange oder schlägt periodisch oder wiederholt fehl | Diagnose von Benutzeranmeldeproblemen |
| Sitzungsstart dauert lange oder schlägt periodisch oder wiederholt fehl | Diagnose von Sitzungsstartproblemen |
| An Sitzungseinrichtung beteiligte Komponenten identifizieren | Sitzungstopologieansicht analysieren |
| Sitzung reagiert langsam oder gar nicht | Sitzungsleistungsprobleme diagnostizieren |
| Die Anwendung ist langsam oder reagiert nicht | Anwendungsstörungen beheben |
| Verbindung fehlgeschlagen | Desktopverbindungen wiederherstellen |
| Sitzung ist langsam oder reagiert nicht | Sitzungen wiederherstellen |
| Video ist langsam oder von schlechter Qualität | HDX-Kanalsystemberichte ausführen |

> **Hinweis:**
>
> Um sicherzustellen, dass die Maschine nicht im Wartungsmodus ist, überprüfen Sie in der Ansicht “Benutzerdetails”den Bereich “Maschinendetails”.

### Sitzungsleistung

Auf der Registerkarte **Sitzungsleistung** wurden die Workflows zur Fehlerbehebung verbessert, etwa durch die Möglichkeit, Echtzeitmetriken zur Identifizierung von Problemen in Benutzersitzungen zu korrelieren. Der Bereich **Sitzungstopologie** bietet eine visuelle Darstellung des sitzungsinternen Pfads für verbundene HDX-Sitzungen. Der Bereich **Leistungsmetriken** enthält Trends für Sitzungsmetriken wie ICARTT, ICA-Latenz, Frames pro Sekunde, verfügbare Ausgabebandbreite und verbrauchte Ausgabebandbreite, die Aufschluss darüber geben, wie sich diese Metriken im Zeitverlauf entwickelt haben. Weitere Informationen finden Sie unter Sitzungsleistungsprobleme diagnostizieren.

### Tipps zur Suche

Die Benutzernamensuche erfolgt in jedem konfigurierten Active Directory.

Wenn Sie den Namen einer Maschine, die von mehreren Benutzern verwendet wird, in ein Suchfeld eingeben, werden die Maschinendetails für die angegebene Maschine angezeigt.

Wenn Sie einen Endpunktnamen in ein Suchfeld eingeben, werden die nicht authentifizierten (anonymen) und die authentifizierten Sitzungen aufgelistet, die mit einem bestimmten Endpunkt verbunden sind. Diese Liste ermöglicht die Fehlerbehebung nicht authentifizierter Sitzungen. Vergewissern Sie sich, dass Endpunktnamen eindeutig sind, damit die Problembehandlung von nicht authentifizierten Sitzungen durchgeführt werden kann.

Die Suchergebnisse schließen auch Benutzer ein, die derzeit keine Maschine verwenden bzw. keiner Maschine zugewiesen sind.

- Bei der Suche wird die Groß- und Kleinschreibung nicht beachtet.
- Teileinträge ergeben eine Liste möglicher Übereinstimmungen.
- Nachdem Sie einige Buchstaben eines zweiteiligen Namens, getrennt durch ein Leerzeichen, eingegeben haben, enthalten die Ergebnisse Treffer für beide Zeichenfolgen. Die Beispiele für zweiteilige Namen sind Benutzername, Familienname und Vorname oder Anzeigename. Wenn Sie zum Beispiel “jo rob”eingeben, werden Zeichenfolgen wie “John Robertson”oder “Robert, Jones”als Ergebnisse angezeigt.

Klicken Sie auf die Registerkarte **Überwachen**, um zur Startseite zurückzukehren.

## Diagnose von Sitzungsstartproblemen

February 21, 2024

Zusätzlich zu den in Abschnitt Diagnose von Benutzeranmeldeproblemen genannten Anmeldeprozessphasen zeigt "Überwachen"die Dauer des Sitzungsstarts an. Die Dauer ist unterteilt in die Dauer des Workspace App-Sitzungsstarts und die des VDA-Sitzungsstarts auf den Seiten **Benutzerdetails** und **Endpunktdetails**. Diese beiden Prozesse sind ihrerseits in Phasen unterteilt, deren Dauer ebenfalls angezeigt wird. Anhand dieser Daten können Sie Verzögerungen beim Sitzungsstart auf den Grund gehen und beheben. Darüber hinaus lassen sich anhand der Angaben zur Zeitdauer der einzelnen Sitzungsstartphasen Probleme mit diesen Phasen gezielt beheben. Wenn beispielsweise die Dauer der Laufwerkzuordnung lang ist, können Sie überprüfen, ob alle gültigen Laufwerke im Gruppenrichtlinienobjekt oder Skript korrekt zugeordnet sind.

### Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, damit Daten zur Dauer des Sitzungsstarts angezeigt werden:

- VDA 1903 oder höher.
- Der Dienst Citrix End User Experience Monitoring (EUEM) wird auf dem VDA ausgeführt.

### Einschränkungen

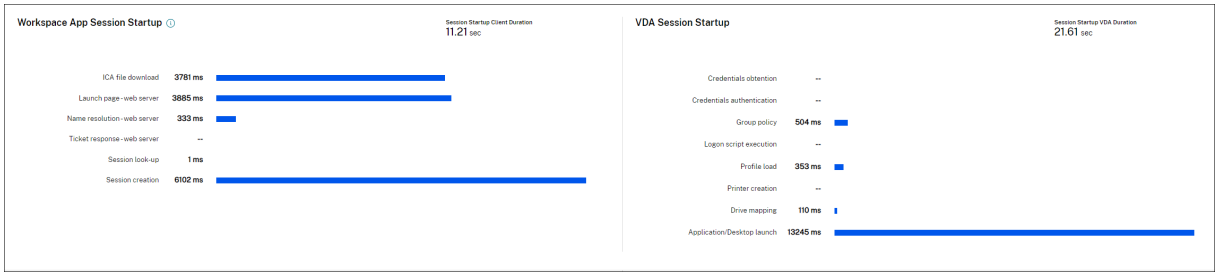
Die folgenden Einschränkungen gelten bei der Anzeige der Startdauerdaten unter "Überwachen".

- Die Sitzungsstartdauer ist nur für HDX-Sitzungen verfügbar.
- Für iOS- und Android OS-Sitzungsstarts ist nur die VDA-Startdauer verfügbar.
- Die IFDCD ist nur verfügbar, wenn die Workspace-App beim Starten von einem Browser erkannt wird.
- Für macOS-Sitzungsstarts ist die IFDCD nur ab Workspace-App-Version 1902 verfügbar.
- Für Windows OS-Sitzungsstarts ist die IFDCD für Workspace-App-Version ab 1902 verfügbar. In früheren Versionen wird die IFDCD nur für App-Starts aus einem Browser unter Erkennung der Workspace-App angezeigt.

> **Hinweise:**
>
> - Treten bei der Anzeige der Sitzungsstartdauer Probleme auf, obwohl die Voraussetzungen erfüllt sind, überprüfen Sie das Serverprotokoll und das VDA-Protokoll in "Überwachen" (siehe CTX130320).
>
>  Für gemeinsam genutzte Sitzungen (mehrere Anwendungen in einer Sitzung gestartet) werden die Workspace-App-Kennzahlen für die neueste Verbindung bzw. den letzten Anwendungsstart angezeigt.
> - Einige Kennzahlen des VDA-Sitzungsstarts gelten nicht bei Wiederverbindungen. In solchen

> Fällen wird eine Meldung angezeigt.




## Phasen des Workspace-App-Sitzungsstarts

### Sitzungsstartdauer auf Client (SSCD)

Ist der Wert hoch, deutet dies auf ein clientseitiges Problem hin, das eine lange Startdauer verursacht. Überprüfen Sie nachfolgende Kennzahlen, um die Ursache des Problems zu ermitteln. Die Sitzungsstartdauer auf dem Client beginnt möglichst nah am Zeitpunkt der Anforderung (Mausklick) und endet bei Herstellung der ICA-Verbindung zwischen dem Clientgerät und VDA. Bei einer gemeinsamen Sitzung ist diese Dauer viel geringer, da ein Großteil der mit der Erstellung einer neuen Verbindung zum Server verbundenen Einrichtung entfällt. Auf der nächsten Ebene darunter stehen mehrere detaillierte Kennzahlen zur Verfügung.

### Dauer des ICA-Dateidownloads (IFDCD)

IFDCD ist die Zeit, die das Herunterladen der ICA-Datei vom Server auf den Client in Anspruch nimmt. Der Gesamtprozess ist folgender:

1. Der Benutzer klickt in der Workspace-Anwendung auf eine Ressource (Anwendung oder Desktop).
2. Eine Anforderung wird über Citrix Gateway (falls konfiguriert) an StoreFront und von dort an den Delivery Controller gesendet.
3. Der Delivery Controller sucht eine verfügbare Maschine und sendet die Maschineninformationen und weitere Details an StoreFront. Außerdem fordert StoreFront ein einmaliges Ticket von der Secure Ticket Authority an.
4. StoreFront generiert eine ICA-Datei und sendet sie über Citrix Gateway (falls konfiguriert) an den Benutzer.

IFDCD entspricht der Zeit, die für den gesamten Prozess benötigt wird (Schritte 1–4). Die IFDCD-Dauer endet, wenn der Client die ICA-Datei empfängt.

LPWD ist der StoreFront-Teil des Prozesses.

Wenn IFDCD hoch und LPWD normal ist, war die serverseitige Verarbeitung des Starts erfolgreich, aber es gab Kommunikationsprobleme zwischen dem Clientgerät und StoreFront. Ursache sind Netzwerkprobleme zwischen den beiden Maschinen. Behandeln Sie in diesem Fall ggf. mögliche Netzwerkprobleme.

#### Dauer des Seitenstarts auf Webserver (LPWD)

Dies ist die Zeit für die Verarbeitung der Startseite (launch.aspx) in StoreFront. Ist der LPWD-Wert hoch, liegt bei StoreFront ggf. ein Engpass vor.

Mögliche Ursachen:

- Hohe Last in StoreFront. Suchen Sie die Ursache der Verzögerung in den Protokollen von IIS, Überwachungstools, Task-Manager, Systemmonitor usw.
- Kommunikationsprobleme zwischen StoreFront und anderen Komponenten, z. B. Delivery Controllern. Prüfen Sie, ob die Netzwerkverbindung zwischen StoreFront und Delivery Controllern langsam ist oder ob Delivery Controller ausgefallen oder überlastet sind.

#### Dauer der Namensauflösung auf Webserver (NRWD)

Dies ist die Zeit, die der Delivery Controller zum Auflösen des Namens einer veröffentlichten Anwendung/eines veröffentlichten Desktops in eine VDA-IP-Adresse braucht.

Ist der Wert hoch, bedeutet dies, dass der Delivery Controller lange braucht, um den Namen einer veröffentlichten Anwendung in eine IP-Adresse aufzulösen. Mögliche Ursachen:

- Problem auf dem Client
- Probleme mit dem Delivery Controller, z. B. Überlastung, oder ein Problem mit der Netzwerkverbindung zwischen den Maschinen.

#### Dauer der Antwort auf Tickets für Webserver (TRWD)

Dies ist die Zeit, die für den Abruf eines Tickets (falls erforderlich) vom Secure Ticket Authority-Server (STA) oder dem Delivery Controller benötigt wird. Ist der Wert hoch, deutet dies auf eine Überlastung des STA-Servers bzw. Delivery Controllers hin.

#### Sitzungslookupdauer auf Client (SLCD)

Dies ist die Zeit, die benötigt wird, um jede Sitzung zum Hosten der angeforderten veröffentlichten Anwendung abzufragen. Die Überprüfung wird auf dem Client durchgeführt, um festzustellen, ob eine bestehende Sitzung die Anforderung zum Starten der Anwendung verarbeiten kann. Die verwendete Methode hängt davon ab, ob die Sitzung neu ist oder gemeinsam genutzt wird.

#### Sitzungserstellungsdauer auf Client (SCD)

Dies ist die Zeit, die das Erstellen einer Sitzung ab dem Starten von wfica32.exe (oder einer äquivalenten Datei) bis zum Herstellen der Verbindung dauert.

### Phasen des VDA-Sitzungsstarts

#### Sitzungsstartdauer auf VDA (SSVD)

Diese serverseitige Kennzahl entspricht der Zeit, die der VDA für den gesamten Startvorgang benötigt. Ist der Wert hoch, deutet dies auf ein VDA-seitiges Problem hin, das eine lange Startdauer verursacht. Dies umfasst die Zeit, die der VDA für den gesamten Startprozess benötigt.

#### Dauer des Anmeldeinformationsabrufs auf VDA (COVD)

Die Zeit, die der VDA zum Abrufen der Benutzeranmeldeinformationen benötigt.

Die Dauer kann sich erhöhen, wenn ein Benutzer die Anmeldeinformationen nicht zügig eingibt, sie wird daher nicht in die VDA-Startdauer eingerechnet. Die Dauer ist in der Regel nur relevant, wenn eine manuelle Anmeldung verwendet wird und das serverseitige Anmeldedialogfeld angezeigt wird (oder wenn ein Rechtshinweis vor Beginn der Anmeldung angezeigt wird).

#### Dauer der Authentifizierung von Anmeldeinformationen auf VDA (CAVD)

Dies ist die Zeit, die der VDA für die Authentifizierung der Anmeldeinformationen des Benutzers anhand des Authentifizierungsanbieters benötigt (Kerberos, Active Directory oder ein SSPI).

#### Gruppenrichtliniendauer für VDA (GPVD)

Dies ist die Zeit, die für das Anwenden von Gruppenrichtlinienobjekten während der Anmeldung benötigt wird.

#### Anmeldeskriptdauer für VDA (LSVD)

Dies ist die Zeit, die der VDA zum Ausführen der Anmeldeskripts des Benutzers benötigt.

Sie können die Anmeldeskripts des Benutzers oder der Gruppe asynchron zu machen. Optimieren Sie Anwendungskompatibilitätsskripts oder verwenden Sie stattdessen Umgebungsvariablen.

**Profilladedauer für VDA (PLVD)**

Dies ist die Zeit, die der VDA zum Laden des Benutzerprofils in Anspruch nimmt.

Ist der Wert hoch, prüfen Sie die Benutzerprofilkonfiguration. Die Größe und der Speicherort von Roamingprofilen wirken sich auf die Dauer von Sitzungsstarts aus. Wenn ein Benutzer sich an einer Sitzung anmeldet, in der Terminaldienste-Roamingprofile und -Basisordner aktiviert sind, werden die Roamingprofilinhalte und der Zugriff auf diesen Ordner während der Anmeldung zugeordnet, wodurch zusätzliche Ressourcen benötigt werden. Dies kann zu einer erheblichen CPU-Auslastung führen. Verwenden Sie **Terminaldienste-Basisordner** mit umgeleiteten persönlichen Ordnern, um dieses Problem zu beheben. Verwenden Sie die Citrix Profilverwaltung für Benutzerprofile in Citrix Umgebungen. Wenn Sie die Citrix Profilverwaltung verwenden und die Anmeldedauer hoch ist, prüfen Sie, ob Ihre Antivirensoftware die Citrix Profilverwaltung blockiert.

**Dauer der Druckererstellung auf VDA (PCVD)**

Dies ist die Zeit, die der VDA benötigt, um die Clientdrucker des Benutzers synchron zuordnen. Ist die asynchrone Druckererstellung konfiguriert, wird kein PCVD-Wert aufgezeichnet, da sie sich nicht auf den Sitzungsstart auswirkt.

Ein hoher Zeitaufwand für die Zuordnung von Druckern wird oft von den Richtlinieneinstellungen für die automatische Druckererstellung verursacht. Die Anzahl der lokal auf den Clientgeräten der Benutzer hinzugefügten Drucker und die Druckkonfiguration können sich direkt auf die Sitzungsstartdauer auswirken. Beim Start einer Sitzung muss Citrix Virtual Apps and Desktops jeden lokal zugeordneten Drucker auf dem Clientgerät erstellen. Konfigurieren Sie die Druckrichtlinien neu, um die Anzahl der erstellten Drucker zu verringern, insbesondere wenn Benutzer viele lokale Drucker haben. Bearbeiten Sie hierzu die Richtlinie “Druckererstellung”auf dem Delivery Controller und in Citrix Virtual Apps and Desktops.

**Dauer der Laufwerkzuordnung auf VDA (DMVD)**

Dies ist die Zeit, die der VDA für die Zuordnung der Clientlaufwerke, -geräte und -ports des Benutzers in Anspruch nimmt.

Stellen Sie sicher, dass die Basisrichtlinien Einstellungen zum Deaktivieren nicht verwendeter virtueller Kanäle (z. B. Audio- oder COM-Portzuordnung) enthalten, um das ICA-Protokoll zu optimieren und die Gesamtsitzungsleistung zu verbessern.

**Startdauer von Anwendung/Desktop für VDA (ALVD/DLVD)**

Diese Phase ist die kombinierte aus UserInit- und Shell-Dauer. Wenn sich ein Benutzer bei einem Windows-Computer anmeldet, führt Winlogon userinit.exe aus. Usernit.exe führt Anmeldeskripts aus, stellt Netzwerkverbindungen wieder her und startet dann explorer.exe, die Windows-Benutzerschnittstelle. Userinit ist die Dauer zwischen dem Start von userinit.exe und dem Start der Benutzeroberfläche für den virtuellen Desktop oder die virtuelle Anwendung dar. Die Shell-Phase ist die Dauer zwischen der Initialisierung der Benutzeroberfläche und dem Zeitpunkt, zu dem der Benutzer die Kontrolle über Tastatur und Maus erhält.

**Dauer der Sitzungserstellung auf VDA (SCVD)**

Diese Zeit umfasst verschiedene Verzögerungen beim Erstellen der Sitzung auf dem VDA.

## Diagnose von Benutzeranmeldeproblemen

November 16, 2023

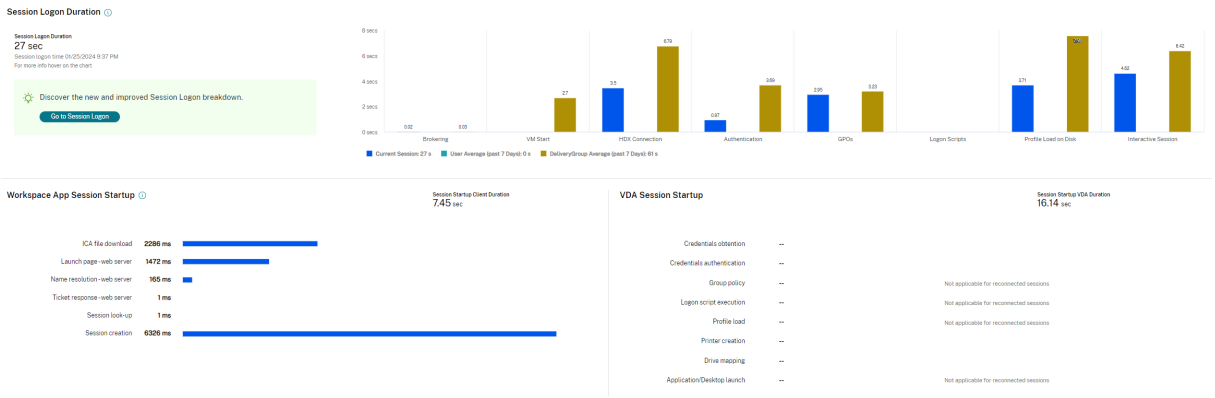
Mit den Anmeldedauerdaten können Sie Benutzeranmeldeprobleme beheben.

Die Anmeldedauer wird nur bei der ersten Verbindung mit einem Desktop oder einer App über HDX gemessen. Diese Daten umfassen keinen Verbindungsversuch über RDP oder die Wiederverbindung getrennter Sitzungen. Insbesondere wird die Anmeldedauer nicht gemessen, wenn ein Benutzer sich anfänglich mit einem anderen Protokoll als HDX verbindet und bei der Wiederverbindung HDX verwendet.

In der Ansicht ‘‘Benutzerdetails’’wird die Dauer als ein Zahlenwert angezeigt, darunter die Anmeldezeit und ein Diagramm der Phasen des Anmeldeprozesses.

Wenn Benutzer sich bei Citrix Virtual Apps and Desktops anmelden, verfolgt der Überwachungsdienst die Phasen des Anmeldeprozesses ab Herstellung der Verbindung über die Citrix Workspace-App bis zu dem Moment, in dem der Desktop einsatzbereit ist.




Die hohe Zahl auf der linken Seite repräsentiert die Gesamtdauer der Anmeldung. Sie errechnet sich aus der auf das Herstellen der Verbindung und das Abrufen eines Desktops vom Delivery Controller aufgewendeten Zeit plus der für Authentifizierung und Anmeldung bei einem virtuellen Desktop aufgewendeten Zeit. Die Dauer wird in Sekunden (oder Sekundenbruchteilen) angezeigt.

## Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, damit Daten zur Anmeldedauer und Drilldowns angezeigt werden:

1. Installieren Sie **Citrix User Profile Manager** und das **Citrix User Profile Manager-WMI-Plug-In** auf dem VDA.
2. Stellen Sie sicher, dass der Citrix Profilverwaltungsdienst ausgeführt wird.
3. Deaktivieren Sie die GPO-Einstellung **Herkömmliche Ausführungsliste nicht verarbeiten**, in XenApp und XenDesktop-Sites der Version bis einschließlich 7.15.
4. "Prozessverfolgung überwachen"muss für den Drilldown interaktiver Sitzungen aktiviert sein.
5. Erhöhen Sie für den GPO-Drilldown die Größe der Gruppenrichtlinien-Betriebsprotokolle.

> **Hinweis:**
>
> Die Anmeldedauer wird nur auf der Standard-Windows-Shell (explorer.exe) und nicht auf benutzerdefinierten Shells unterstützt.

## Beheben von Benutzeranmeldeproblemen

1. Überprüfen Sie in der Ansicht **Benutzerdetails** im Bereich "Anmeldedauer", welcher Anmeldezustand vorliegt.
    - Wenn Benutzer sich anmelden, wird der Anmeldeprozess in der Ansicht widergespiegelt.
    - Wenn der Benutzer angemeldet ist, wird im Bereich "Anmeldedauer"angezeigt, wie viel Zeit für die Anmeldung an der aktuellen Sitzung benötigt wurde.

2. Überprüfen Sie die Phasen des Anmeldeprozesses.

### Phasen des Anmeldeprozesses

#### Vermittlung

Zur Zuweisung des Desktops zum Benutzer benötigte Zeit.

#### VM-Start

Zum Starten einer virtuellen Maschine benötigte Zeit, wenn eine Sitzung den Start einer Maschine erforderte.

#### HDX-Verbindung

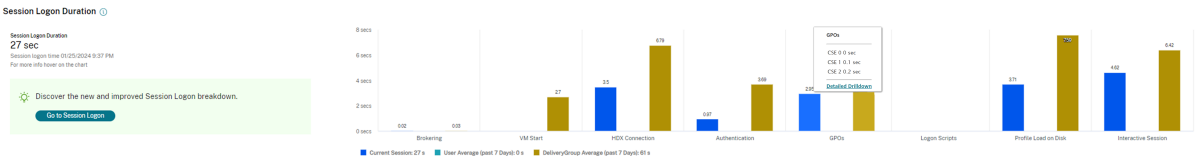
Zum Einrichten der HDX-Verbindung vom Client zur virtuellen Maschine benötigte Zeit.

#### Authentifizierung

Zum Abschließen der Authentifizierung bei der Remotesitzung benötigte Zeit.

#### Gruppenrichtlinienobjekte

Zum Anwenden von Gruppenrichtlinienobjekten benötigte Zeit, wenn bei der Anmeldung Gruppenrichtlinieneinstellungen auf den virtuellen Maschinen aktiviert sind. Die Aufschlüsselung der für die Anwendung der einzelnen Richtlinien gemäß CSE (clientsseitige Erweiterungen) benötigten Zeit wird als QuickInfo angezeigt, wenn mit der Maus auf die GPO-Leiste zeigen.




Klicken Sie auf **Detaillierter Drilldown**, um eine Tabelle mit dem Richtlinienstatus und dem entsprechenden GPO-Namen anzuzeigen. Die Zeitangaben im Drilldown repräsentieren nur die CSE-Verarbeitungszeit und nicht die gesamte GPO-Dauer. Sie können die Drilldowntabelle zur weiteren Fehlerbehebung oder zur Verwendung in Berichten kopieren. Die GPO-Zeit für die Richtlinien wird aus den Ereignisanzeigeprotokollen abgerufen. Die Protokolle können je nach dem für die Betriebsprotokolle zugewiesenen Speicher (Standardwert = 4 MB) überschrieben werden. Weitere Informationen zum Erhöhen der Größe der Betriebsprotokolle finden Sie im Microsoft TechNet-Artikel zum https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10).

### Anmeldeskripts

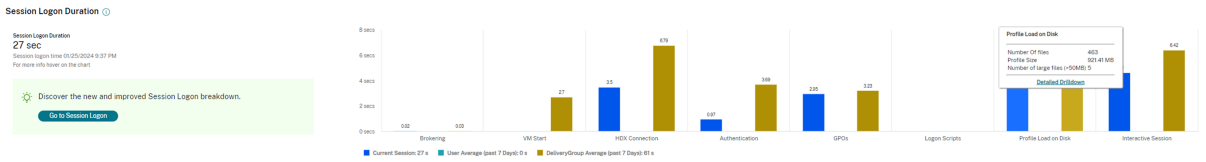
Zum Ausführen von Anmeldeskripts benötigte Zeit, wenn Anmeldeskripts für die Sitzung konfiguriert sind.

### Profilladezeit

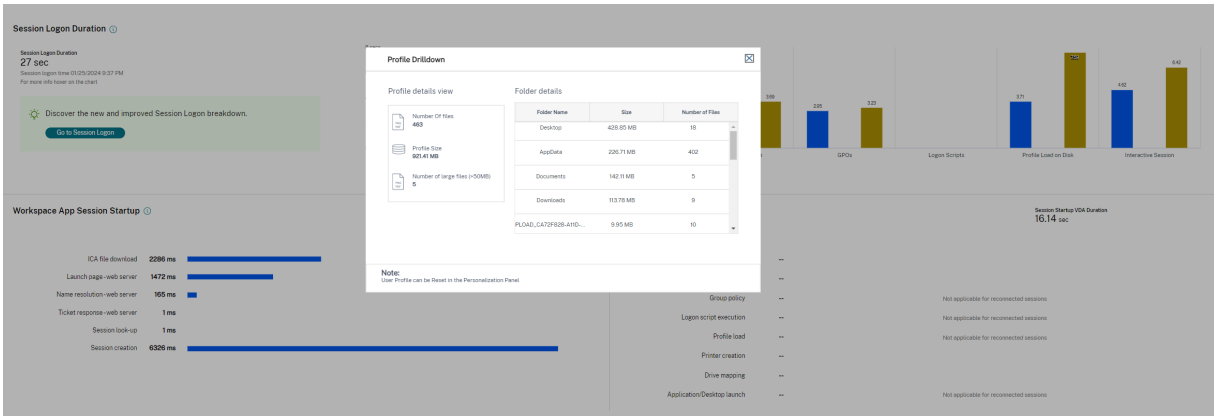
Zum Laden des Profils benötigte Zeit, wenn für den Benutzer Profileinstellungen auf der virtuellen Maschine konfiguriert sind.

Wenn die Citrix Profilverwaltung konfiguriert ist, wird die Dauer der Profilverarbeitung durch die Profilverwaltung im Balken “Profilladezeit”angezeigt. Anhand dieser Informationen ist eine gezieltere Problembehandlung bei langsamer Profilverarbeitung möglich. Wenn die Profilverwaltung konfiguriert ist, wird eine erhöhte Dauer im Balken “Profilladezeit”angezeigt. Der Anstieg der Dauer begründet sich durch diese Erweiterung und bedeutet keine Leistungseinbuße. Diese Erweiterung ist bei VDAs der Version 1903 und höher verfügbar.

Wenn Sie mit der Maus auf die Profilladezeitleiste zeigen, wird eine QuickInfo mit den Benutzerprofildetails der aktuellen Sitzung angezeigt. Diese zusätzlichen Informationen können bei der Behebung von Profilladeproblemen helfen.




Klicken Sie auf **Detaillierter Drilldown**, um Informationen zu den einzelnen Ordnern im Profilstammordner (z. B. C:/Users/username), dessen Größe und die Zahl der enthaltenen Dateien (einschließlich solcher in verschachtelten Ordnern) anzuzeigen.




Der Profildrilldown ist auf VDAs der Version 1811 und höher verfügbar. Anhand der Profildrilldown-Informationen können Sie Probleme lösen, die das Laden von Profilen verlangsamen. Sie haben folgende Möglichkeiten:

- Zurücksetzen des Benutzerprofils
- Optimieren des Profils durch Entfernen unerwünschter, großer Dateien
- Reduzieren der Anzahl Dateien zur Verringerung der Netzwerklast
- Verwenden von Profilstreaming

Standardmäßig werden alle Ordnernamen angezeigt. Um Ordnernamen auszublenden, bearbeiten Sie die Registrierungswerte auf der VDA-Maschine wie folgt:

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Fügen Sie auf dem VDA den Wert **ProfileFoldersNameHidden** für HKEY_LOCAL_MACHINE\Software\Citrix\Di hinzu.1. Legen Sie den Wert auf 1 fest. Der Wert muss ein DWORD-Wert (32-Bit) sein. Die Anzeige der Ordnernamen ist damit deaktiviert.
2. Um die Ordnernamen wieder einzublenden, legen Sie den Wert auf 0 fest.

> **Hinweis:**
>
> Sie können die Registrierungswertänderung mithilfe von GPO oder PowerShell auf mehreren Maschinen anwenden. Weitere Informationen zum Ändern von Registrierungswerten per GPO finden Sie in diesem Blog.

#### Weitere Informationen

- Beim Profildrilldown werden umgeleitete Ordner nicht berücksichtigt.
- NTUser.dat-Dateien im Stammordner sind für Endbenutzer möglicherweise nicht sichtbar. Sie sind jedoch im Profildrilldown enthalten und werden in der Liste der Dateien unter **Stammordner** angezeigt.
- Einige verborgene Dateien im Ordner "AppData"sind nicht im Profildrilldown enthalten.
- Die Anzahl der Dateien und Profilgrößendaten stimmen aufgrund bestimmter Windows-Einschränkungen möglicherweise nicht mit den Daten unter "Personalisierung"überein.

#### Interaktive Sitzung

Zum Übergeben von Tastatur- und Maussteuerung an den Benutzer benötigte Zeit, nachdem das Profil geladen wurde. Dies dauert normalerweise am längsten von allen Phasen des Anmeldeprozesses und wird wie folgt berechnet: **Dauer der interaktiven Sitzung = Zeitstempel des Ereignisses "Desktop**

**bereit"(Ereignis-ID 1000 auf VDA) - Zeitstempel des Ereignisses "Profilladezeit"(Ereignis-ID 2 auf VDA)**. Die interaktive Sitzung hat drei Teilphasen: Pre-Userinit, Userinit und Shell. Zeigen Sie auf die interaktive Sitzung, um eine QuickInfo mit Folgendem anzuzeigen:

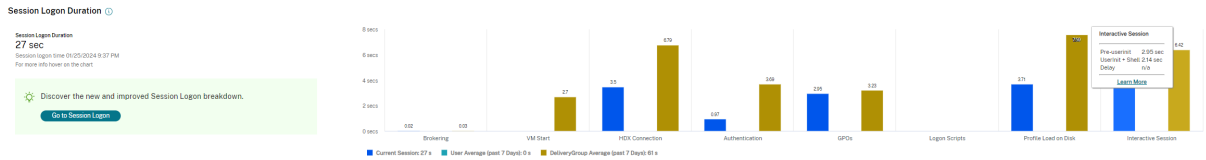
- Teilphasen
- für jede Teilphase aufgewendete Zeit
- gesamte kumulative Zeitverzögerung zwischen Teilphasen

> **Hinweis:**
>
> Dieses Feature ist ab VDA-Version 1811 verfügbar. Wenn Sie Sitzungen auf Sites vor Version 7.18 gestartet haben und dann ein Upgrade auf 7.18 durchführen, wird die Meldung "Drilldown aufgrund eines Serverfehlers nicht verfügbar"angezeigt. Wenn Sie hingegen Sitzungen nach einem Upgrade gestartet haben, wird keine Fehlermeldung angezeigt.

Um die Zeitdauer jeder Teilphase anzuzeigen, aktivieren Sie die Überwachung der Prozessverfolgung auf der VM (VDA). Wenn die Überwachung der Prozessverfolgung deaktiviert ist (Standardeinstellung), werden die Dauer der Teilphase Pre-Userinit und die kombinierte Dauer der Teilphasen Userinit und Shell angezeigt. Die Überwachung der Prozessverfolgung können Sie folgendermaßen über ein Gruppenrichtlinienobjekt aktivieren:

1. Erstellen Sie ein Gruppenrichtlinienobjekt, und bearbeiten Sie es mit dem Gruppenrichtlinienobjekt-Editor.
2. Rufen Sie **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Überwachungsrichtlinie** auf.
3. Doppelklicken Sie im rechten Fensterbereich auf **Prozessverfolgung überwachen**.
4. Wählen Sie **Erfolg** und klicken Sie auf "OK".
5. Wenden Sie das Gruppenrichtlinienobjekt auf die entsprechenden VDAs oder Gruppen an.

Weitere Informationen zur Überwachung der Prozessverfolgung und der Aktivierung bzw. Deaktivierung finden Sie unter https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10) in der Microsoft-Dokumentation.




Bereich "Anmeldedauer"in der Ansicht "Benutzerdetails"

- **Interaktive Sitzung –Pre-Userinit:** Dieser Teil der interaktiven Sitzung überschneidet sich mit Gruppenrichtlinienobjekten und Skripts. Die Teilphase kann durch Optimierung der GPOs und Skripts verkürzt werden.
- **Interaktive Sitzung –Userinit:** Wenn sich ein Benutzer bei einem Windows-Computer anmeldet, führt Winlogon userinit.exe aus. Userinit.exe führt Anmeldeskripts aus, stellt Netzw-

erkverbindungen wieder her und startet dann explorer.exe die Windows-Benutzeroberfläche. Diese Teilphase der interaktiven Sitzung repräsentiert die Dauer zwischen dem Start von userinit.exe bis zum Start der Benutzeroberfläche des virtuellen Desktops oder der Anwendung.

- **Interaktive Sitzung –Shell:** In der vorherigen Phase wurde von userinit die Initialisierung der Windows-Benutzeroberfläche begonnen. Die Shell-Teilphase erfasst die Dauer zwischen der Initialisierung der Benutzeroberfläche und dem Zeitpunkt, zu dem der Benutzer die Kontrolle über Tastatur und Maus erhält.
- **Verzögerung:** Dies ist die kumulative Verzögerung zwischen den Teilphasen **Pre-Userinit und Userinit** und den Teilphasen **Userinit und Shell**.

Die Gesamtanmeldedauer ist keine genaue Summe der einzelnen Phasen. Beispiel: Einige Phasen treten parallel auf und in anderen Phasen wird eine zusätzliche Verarbeitung durchgeführt, die zu einer längeren Anmeldedauer als die Summe der einzelnen Phasen führen kann.
Die Gesamtanmeldedauer umfasst nicht die ICA-Leerlaufzeit, d. h. die Zeit zwischen dem Herunterladen der ICA-Datei und dem Start der ICA-Datei für eine Anwendung.
Um das automatische Öffnen der ICA-Datei beim Start einer Anwendung zu ermöglichen, konfigurieren Sie den Browser so, dass ICA-Dateien nach dem Download automatisch gestartet werden. Weitere Informationen finden Sie unter CTX804493.

> **Hinweis:**
>
> Im Anmeldedauerdiagramm werden die Anmeldephasen in Sekunden angezeigt. Zeitwerte unter einer Sekunde werden als Sekundenbruchteile angezeigt. Werte, die größer sind als eine Sekunde, werden auf die nächste halbe Sekunde aufgerundet. Aufgrund des Diagrammdesigns kann ein Höchstwert von 200 Sekunden auf der Y-Achse angezeigt werden. Bei Werten über 200 Sekunden wird der tatsächliche Wert über dem Balken angezeigt.

### Tipps zur Problembehandlung

Um ungewöhnliche oder unerwartete Werte im Diagramm zu finden, vergleichen Sie die in jeder Phase der aktuellen Sitzung benötigte Zeit mit der durchschnittlichen Dauer für diesen Benutzer in den letzten sieben Tagen sowie mit der durchschnittlichen Dauer in den letzten sieben Tagen für alle Benutzer diese Bereitstellungsgruppe.

Eskalieren Sie wie erforderlich. Beispiel: Wenn der VM-Start langsam ist, liegt das Problem möglicherweise am Hypervisor, Sie können das Problem also an den Hypervisoradministrator eskalieren. Wenn die Vermittlungsdauer zu lang ist, können Sie das Problem dem Siteadministrator melden, damit der Lastausgleich auf dem Delivery Controller überprüft wird.

Überprüfen Sie ungewöhnliche Unterschiede, u. a.:

- Fehlende (aktuelle) Anmeldeleisten

- Große Abweichung zwischen der aktuellen und der durchschnittlichen Dauer für diesen Benutzer. Mögliche Ursachen:
  - Es wurde eine neue Anwendung installiert.
  - Das Betriebssystem wurde aktualisiert.
  - Es wurden Konfigurationsänderungen vorgenommen.
  - Das Profil des Benutzers ist sehr groß. In diesem Fall ist auch die Profilladezeit hoch.
- Große Abweichung zwischen den Anmeldewerten des Benutzers (aktuelle und durchschnittliche Dauer) und der durchschnittlichen Dauer der Bereitstellungsgruppe.

Klicken Sie ggf. auf **Neu starten**, um den Anmeldeprozess des Benutzers zu beobachten und Probleme zu beheben, z. B. VM-Start oder Brokering.

## Benutzer spiegeln

November 16, 2022

Mit dem Feature "Benutzer spiegeln"können Sie die virtuelle Maschine oder Sitzung eines Benutzers direkt anzeigen und darauf arbeiten. Sie können Windows- und Linux-VDAs spiegeln. Der Benutzer muss mit der zu spiegelnden Maschine verbunden sein. Wenn der Benutzer verbunden ist, wird der Name der verbundenen Maschine in der Titelleiste des Benutzers angezeigt.

Die Spiegelung wird in einer neuen Registerkarte gestartet. Aktualisieren Sie Ihre Browsereinstellungen dahingehend, dass Popups von der Citrix Cloud-URL zugelassen sind.

Das Feature "Spiegeln"über die Ansicht **Benutzerdetails** aufgerufen. Sie wählen die Benutzersitzung und klicken dann auf **Spiegeln** in der Aktivitätsmanageransicht oder im Bereich "Sitzungsdetails".

### Spiegeln von Linux-VDAs

Spiegeln ist bei Linux-VDAs ab Version 7.16 möglich, auf denen die Linux-Distribution RHEL7.3 oder Ubuntu Version 16.04 ausgeführt wird.

> **Hinweis:**
>
> - Der Überwachungsdienst verwendet den FQDN zum Herstellen einer Verbindung mit dem Linux-VDA. Vergewissern Sie sich, dass der Überwachungsclient den FQDN des Linux-VDAs auflösen kann.
> - Auf dem VDA müssen die Pakete "python-websockify"und "x11vnc"installiert sein.
> - Die noVNC-Verbindung zum VDA verwendet das WebSocket-Protokoll. Standardmäßig wird das WebSocket-Protokoll (**ws://**) verwendet. Aus Sicherheitsgründen empfiehlt

> Citrix, das **wss://**-Protokoll zu verwenden. Installieren Sie SSL-Zertifikate auf jedem Überwachungsclient und Linux-VDA.

Folgen Sie den Anweisungen unter Sitzungsspiegelung, um den VDA für die Spiegelung zu konfigurieren.

1. Nachdem Sie auf **Spiegeln** geklickt haben, wird die Spiegelungsverbindung initialisiert und auf dem Benutzergerät eine Bestätigungsaufforderung angezeigt.
2. Weisen Sie die Benutzer an, auf **Ja** zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.
3. Der Administrator kann nur die gespiegelte Sitzung anzeigen.

## Spiegeln von Windows-VDAs

Windows-VDA-Sitzungen werden mithilfe der Windows-Remoteunterstützung gespiegelt. Aktivieren Sie die Windows-Remoteunterstützung bei der VDA-Installation. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren von Features.

1. Wenn Sie auf **Spiegeln** klicken, wird die Verbindung initialisiert und es erscheint ein Dialogfeld mit der Aufforderung, die MSRC-Incidentdatei zu öffnen oder zu speichern.
2. Öffnen Sie die Vorfalldatei mit dem Remoteunterstützung-Viewer, wenn er nicht standardmäßig ausgewählt ist. Auf dem Benutzergerät wird eine Bestätigungsaufforderung angezeigt.
3. Weisen Sie die Benutzer an, auf **Ja** zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.
4. Fordern Sie den Benutzer auf, die Tastatur- und Maussteuerung freizugeben, damit Sie die Steuerung übernehmen können.

### Anpassen des Microsoft Internet Explorer-Browsers für das Spiegeln

Richten Sie den Microsoft Internet Explorer-Browser so ein, dass die heruntergeladene Datei zur Microsoft-Remoteunterstützung (.msra) automatisch mit dem Remoteunterstützungsclient geöffnet wird.

Hierzu müssen Sie die Einstellung Automatische Eingabeaufforderung für Dateidownloads im Gruppenrichtlinien-Editor aktivieren:

Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer > Internetsystemsteuerung > Sicherheitsseite > Internetzone > Automatische Eingabeaufforderung für Dateidownloads.

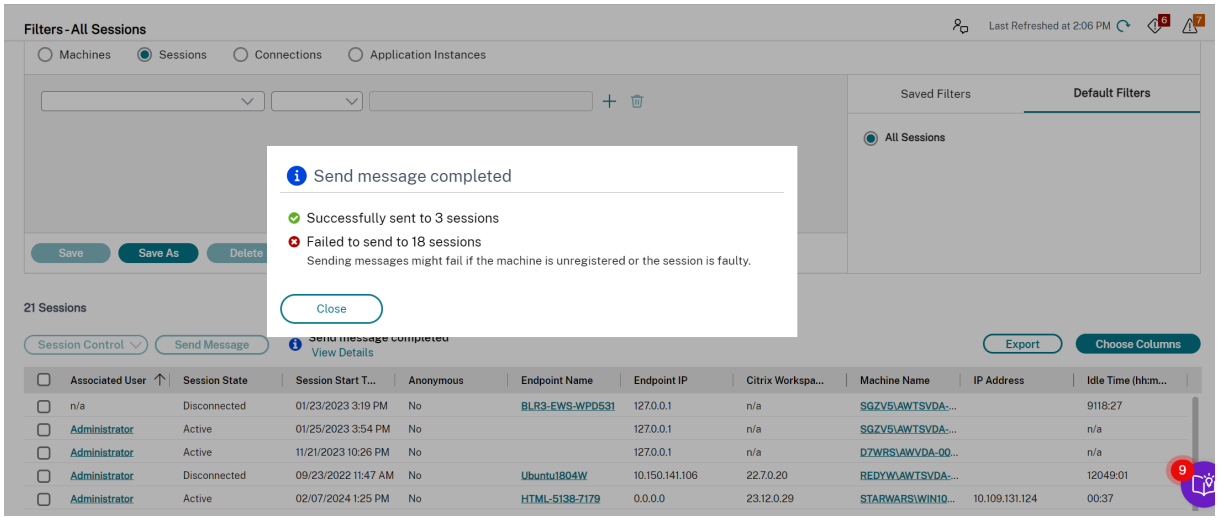
# Nachrichten an Benutzer senden

January 25, 2024

Sie können im Überwachungsdienst eine Nachricht an einen Benutzer senden, der mit einer oder mehreren Maschinen verbunden ist. Sie können beispielsweise mit dieser Funktion sofortige Benachrichtigungen über administrative Aktionen senden, wie bevorstehende Desktopwartung, Abmeldungen bzw. Neustarts von Maschinen und das Zurücksetzen von Profilen.

Gehen Sie folgendermaßen vor, um eine Nachricht an einen Benutzer zu senden:

1. Gehen Sie zu **Überwachen** > **Filter** > **Maschinen** > **Alle Maschinen**.
2. Wählen Sie die Maschine aus, an die Sie die Nachricht senden möchten, und klicken Sie auf **Nachricht senden**.
3. Geben Sie die Nachricht ein und klicken Sie auf **Senden**.




Das Senden von Nachrichten kann fehlschlagen, wenn die Maschinen nicht registriert oder die Sitzungen fehlerhaft sind.

Wenn die Nachricht gesendet wurde, wird eine Bestätigungsmeldung angezeigt. Wenn die Maschine des Benutzers verbunden ist, wird dort eine entsprechende Nachricht angezeigt.

Wenn die Nachricht nicht gesendet wurde, wird eine Fehlermeldung angezeigt. Gehen Sie bei der Problembehandlung gemäß der Anweisungen in der Fehlermeldung vor. Geben Sie abschließend den Betreff und Text der Nachricht neu ein und klicken Sie auf **Noch einmal versuchen**.

Wenn Sie Massennachrichten an alle verbundenen Sitzungen senden möchten, wird der Fortschritt des Vorgangs in Prozent angezeigt. Sobald der Vorgang abgeschlossen ist, werden die Anzahl der erfolgreich gesendeten Nachrichten und die Anzahl der fehlgeschlagenen Nachrichten angezeigt. Der

Status “Nachricht senden”ist besonders hilfreich, wenn Sie große Sites verwalten. Sie können damit erkennen, ob die Nachricht erneut an bestimmte Benutzer gesendet werden muss.

## Anwendungsstörungen beheben

February 14, 2023

Klicken Sie in der Ansicht **Aktivitätsmanager** auf die Registerkarte **Anwendungen**. Sie können alle Anwendungen auf allen Maschinen anzeigen, auf die dieser Benutzer zugreifen kann, einschließlich der lokalen und der gehosteten Anwendungen für die derzeit verbundene Maschine und den Status der einzelnen Maschine.

Die Liste enthält nur die Anwendungen, die in der Sitzung gestartet wurden.

Für Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS werden Anwendungen für jede getrennte Sitzung angezeigt. Wenn der Benutzer nicht verbunden ist, werden keine Anwendungen angezeigt.

| Aktion | Beschreibung |
| --- | --- |
| Beenden der Anwendung, die nicht reagiert | Wählen Sie die Anwendung aus, die nicht reagiert, und klicken Sie auf **Anwendung beenden**. Wenn die Anwendung beendet ist, fordern Sie den Benutzer auf, sie neu zu starten. |
| Beenden von Prozessen, die nicht reagieren | Wenn Sie die erforderlichen Berechtigungen haben, klicken Sie auf die Registerkarte **Prozesse**. Wählen Sie einen Prozess aus, der mit dieser Anwendung zusammenhängt oder der viele CPU-Ressourcen oder viel Speicher verbraucht, und klicken Sie auf **Prozess beenden**. Wenn Sie nicht die erforderlichen Berechtigungen zum Beenden des Prozesses haben, schlägt das Beenden fehl. |

| Aktion | Beschreibung |
| --- | --- |
| Neustarten der Maschine des Benutzers | Nur Maschinen mit Einzelsitzungs-OS: Klicken Sie für die ausgewählte Sitzung auf **Neu starten**. Sie können auch in der Ansicht "Maschinendetails"die Maschine mit den Energiesteuerelementen neu starten oder herunterfahren. Fordern Sie den Benutzer auf, sich neu anzumelden, sodass Sie die Anwendung überprüfen können. Für Maschinen mit Multisitzungs-OS steht die Option "Neu starten"nicht zur Verfügung. Melden Sie stattdessen den Benutzer ab und fordern Sie ihn auf, sich neu anzumelden. |
| Versetzen der Maschine in den Wartungsmodus | Wenn das Image einer Maschine gewartet werden muss, z. B. mit Patches oder anderen Updates, versetzen Sie die Maschine in den Wartungsmodus. Klicken Sie in der Ansicht "Maschinendetails"auf **Details** und aktivieren Sie die Option "Wartungsmodus". Eskalieren Sie an den entsprechenden Administrator. |

### Sichtbarkeit der ausgeführten Anwendungen deaktivieren

Standardmäßig enthält der Aktivitätsmanager eine Liste aller in einer Benutzersitzung ausgeführten Anwendungen. Diese Informationen können von allen Administratoren angezeigt werden, die Zugriff auf den Aktivitätsmanager haben. Bei delegierten Administratorrollen sind dies Volladministratoren, Bereitstellungsgruppenadministratoren und Helpdeskadministratoren.

Um Daten zu Benutzern und ihren Anwendungen zu schützen, können Sie die Auflistung der ausgeführten Anwendungen auf der Registerkarte "Anwendungen"deaktivieren. Ändern Sie auf dem VDA den Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. Standardmäßig ist dieser Schlüssel auf 1 eingestellt. Ändern Sie den Wert auf 0, was bedeutet, dass die Informationen nicht auf dem VDA gesammelt und im Aktivitätsmanager angezeigt werden.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des

> Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

## Wiederherstellen von Desktopverbindungen

April 1, 2022

Überprüfen Sie im Überwachungsdienst in der Titelleiste des Benutzers seinen Verbindungsstatus für die aktuelle Maschine.

Wenn die Desktopverbindung fehlgeschlagen ist, wird die Fehlerursache angezeigt, um Sie bei der Problembehandlung zu unterstützen.

| Aktion | Beschreibung |
| --- | --- |
| Stellen Sie sicher, dass die Maschine nicht im Wartungsmodus ist. | Achten Sie auf der Seite Benutzerdetails darauf, dass der Wartungsmodus deaktiviert ist. |
| Neustarten der Maschine des Benutzers | Wählen Sie die Maschine aus und klicken Sie auf **Neu starten**. Verwenden Sie diese Option, wenn die Maschine des Benutzers nicht mehr reagiert oder keine Verbindung herstellen kann, z. B. wenn die Maschine sehr viele CPU-Ressourcen verbraucht und dies die CPU unbrauchbar macht. |

## Wiederherstellen von Sitzungen

April 1, 2022

Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit dem Server.

Die Problembehandlung von Sitzungsfehlern erfolgt in der Ansicht “Benutzerdetails”im Bereich **Sitzungsdetails**. Sie können die Details der aktuellen Sitzung (durch die Sitzungs-ID gekennzeichnet) anzeigen.

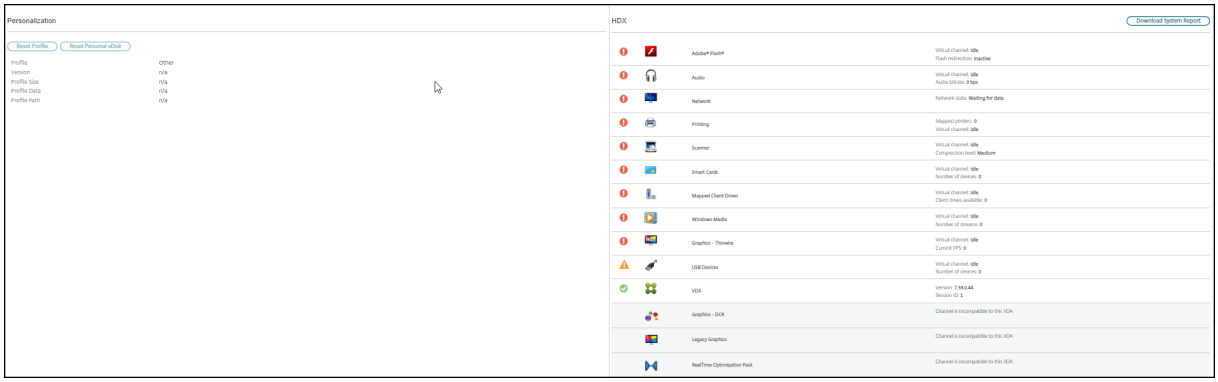
| Aktion | Beschreibung |
| --- | --- |
| Beenden von Anwendungen und Prozessen, die nicht reagieren | Klicken Sie auf die Registerkarte **Anwendungen**. Wählen Sie eine nicht reagierende Anwendung aus und klicken Sie auf **Anwendung beenden**. Sie können auch einen Prozess auswählen, der nicht reagiert, und auf **Prozess beenden** klicken. Beenden Sie auch Prozesse, die ungewöhnlich viel Speicher oder CPU-Ressourcen verbrauchen, da sie die CPU unbrauchbar machen können. |
| Trennen der Windows-Sitzung | Klicken Sie auf **Sitzungssteuerung** und wählen Sie dann **Trennen**. Diese Option steht nur für vermittelte Maschinen mit Multisitzungs-OS zur Verfügung. Für nicht vermittelte Sitzungen ist die Option deaktiviert. |
| Abmelden des Benutzers von der Sitzung | Klicken Sie auf **Sitzungssteuerung** und wählen Sie dann **Abmelden**. |

Zum Testen der Sitzung kann der Benutzer versuchen, sich neu anzumelden. Sie können den Benutzer auch spiegeln, um diese Sitzung genauer zu beobachten.

## HDX-Kanalsystemberichte ausführen

November 16, 2023

Prüfen Sie in der Ansicht **Benutzerdetails** im Bereich "HDX"den Status der HDX-Kanäle auf der Maschine des Benutzers. Dieser Bereich ist nur verfügbar, wenn die Maschine des Benutzers mit HDX verbunden ist.



Wenn eine Meldung angibt, dass die Informationen zurzeit nicht verfügbar sind, warten Sie eine Minute, bis die Seite aktualisiert ist, oder klicken Sie auf die Schaltfläche **Aktualisieren**. Die Aktualisierung von HDX-Daten kann etwas länger dauern als bei anderen Daten.

Klicken Sie zur Anzeige weiterer Informationen auf das Fehler- oder Warnsymbol.

> Tipp:
>
> Sie können Informationen über andere Kanäle in demselben Dialogfeld einblenden, indem Sie in der linken Ecke der Titelleiste auf den Pfeil nach links oder rechts klicken.

Systemberichte über die HDX-Kanäle werden hauptsächlich vom Citrix Support für die weitere Problembehandlung verwendet. Klicken Sie hierfür im Bereich HDX auf **Systembericht herunterladen**.

## Zurücksetzen eines Benutzerprofils

April 19, 2022

> **Achtung:**
>
> Wenn ein Profil zurückgesetzt wird, werden die Ordner und Dateien des Benutzers zwar gespeichert und in das neue Profil kopiert, aber die meisten Benutzerdaten werden gelöscht (z. B. wird die Registrierung zurückgesetzt und die Anwendungseinstellungen werden möglicherweise gelöscht).

1. Suchen Sie unter "Überwachen"den Benutzer, dessen Profil Sie zurücksetzen möchten, und wählen Sie seine Benutzersitzung aus.
2. Klicken Sie auf **Profil zurücksetzen**.
3. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
4. Fordern Sie den Benutzer auf, sich neu anzumelden. Der Ordner und Dateien, die aus dem Profil des Benutzers gespeichert wurden, werden in das neue Profil kopiert.

   > **Wichtig:**
   >
   > Wenn der Benutzer Profile auf mehreren Plattformen (z. B. Windows 8 und Windows 7) hat, fordern Sie ihn auf, sich zuerst bei dem gleichen Desktop oder bei der gleichen App anzumelden, bei dem bzw. der er Probleme hatte. Dies stellt sicher, dass das richtige Profil zurückgesetzt wird. Citrix Benutzerprofile sind zum Zeitpunkt der Benutzerdesktopanzeige bereits zurückgesetzt. Bei Microsoft-Roamingprofilen dauert die Ordnerwiederherstellung möglicherweise noch kurze Zeit an. Der Benutzer muss angemeldet bleiben, bis die Wiederherstellung abgeschlossen ist.

Bei den zuvor erläuterten Schritten wird davon ausgegangen, dass Sie Citrix Virtual Desktops (Desktop-VDA) verwenden. Wenn Sie Citrix Virtual Desktops (Server-VDA) verwenden, müssen Sie angemeldet sein, um das Profil zurückzusetzen. Der Benutzer muss sich dann abmelden und neu anmelden, um das Zurücksetzen des Profils abzuschließen.

Wenn das Profil nicht erfolgreich zurückgesetzt wird (z. B. der Benutzer kann sich nicht wieder anmelden oder einige der Dateien fehlen), müssen Sie das ursprüngliche Profil manuell wiederherstellen.

Die Ordner (und die Dateien) des Benutzerprofils werden gespeichert und in das neue Profil kopiert. Dabei gilt folgende Kopierreihenfolge:

- Desktop
- Cookies
- Favoriten
- Dokumente
- Bilder
- Musik
- Videos

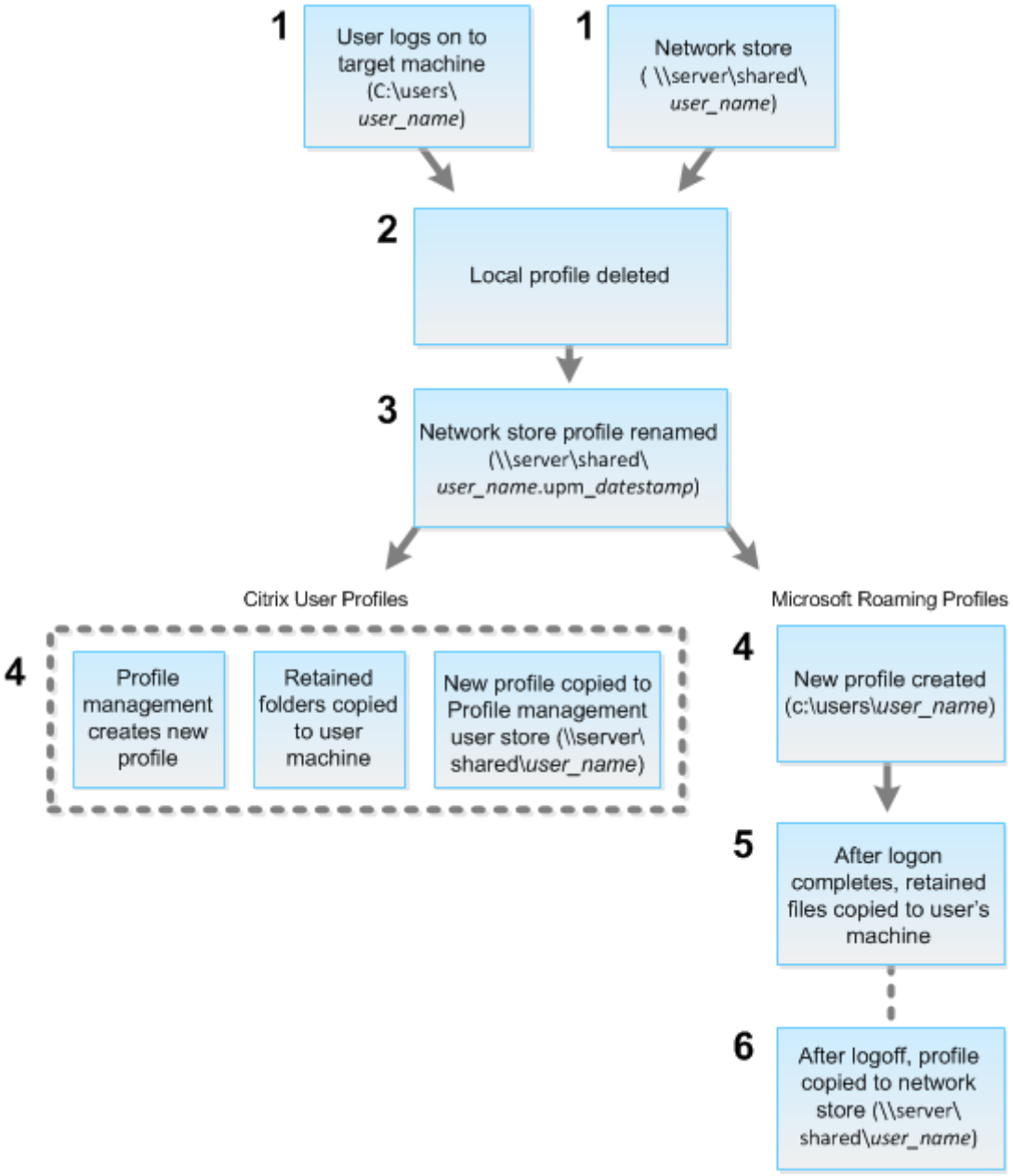
> **Hinweis:**
>
> In Windows 8 und höheren Versionen werden Cookies beim Zurücksetzen des Profils nicht kopiert.

### Verarbeiten von zurückgesetzten Profilen

Alle Citrix Benutzerprofile oder Microsoft Roamingprofile können zurückgesetzt werden. Wenn der Benutzer sich abmeldet und Sie den Befehl zum Zurücksetzen wählen (entweder unter "Überwachen" oder mit dem PowerShell SDK), wird das verwendete Benutzerprofil erst identifiziert und dann zurückgesetzt. Der Überwachungsdienst empfängt die Informationen (z. B. Daten zur Profilgröße, zum Typ und zu den Anmeldezeiten) über die Profilverwaltung.

Dieses Diagramm zeigt den Prozess, der auf die Benutzeranmeldung folgt, wenn ein Profil zurückgesetzt wird.




Der unter "Überwachen"erteilte Befehl zum Zurücksetzen gibt den Profiltyp an. Der Profilverwaltungsdienst versucht dann, ein Profil dieses Typs zurückzusetzen und sucht die entsprechende Netzwerkfreigabe (Benutzerspeicher). Wenn der Benutzer von der Profilverwaltung verarbeitet wird, aber einen Roamingprofilbefehl erhält, wird er abgelehnt (oder umgekehrt).

1. Wenn ein lokales Profil vorhanden ist, wird es gelöscht.
2. Das Netzwerkprofil wird umbenannt.
3. Die nächste Aktion hängt davon ab, ob es sich bei dem Profil, das zurückgesetzt wird, um ein Citrix Benutzerprofil oder ein Microsoft Roamingprofil handelt.

Für Citrix Benutzerprofile wird das neue Profil mit den Importregeln der Profilverwaltung erstellt, die Ordner werden in das Netzwerkprofil zurückkopiert und der Benutzer kann sich wie gewohnt anmelden. Wenn ein Roamingprofil für das Zurücksetzen verwendet wird, bleiben alle Registrierungseinstellungen im Roamingprofil im zurückgesetzten Profil gespeichert. Sie können in der Profilverwaltung konfigurieren, dass das Roamingprofil ggf. von einem Vorlagenprofil überschrieben wird.

Für Microsoft Roamingprofile wird ein neues Profil von Windows erstellt, und die Ordner werden bei Anmeldung des Benutzers auf das Benutzergerät zurückkopiert. Bei der nächsten Benutzerabmeldung wird das neue Profil in den Netzwerkspeicher kopiert.

### Manuelles Wiederherstellen eines Profils nach einer fehlgeschlagenen Zurücksetzung

1. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
2. Löschen Sie das lokale Profil, sofern vorhanden.
3. Suchen Sie den archivierten Ordner auf der Netzwerkfreigabe, bei dem das Datum und die Uhrzeit dem Ordnernamen angehängt wurden, also den Ordner mit der Erweiterung .upm_datumsstempel.
4. Löschen Sie den aktuellen Profilnamen. Das ist die Datei ohne die Erweiterung upm_datumsstempel.
5. Benennen Sie den archivierten Ordner unter Verwendung des ursprünglichen Profilnamens um. Das heißt, entfernen Sie die Datums- und Uhrzeit-Erweiterung. Sie haben das Profil auf den ursprünglichen Zustand zurückgesetzt.

## Sitzungen aufzeichnen

February 21, 2024

Sie können mit den Steuerelementen der Sitzungsaufzeichnung der Seiten **Benutzerdetails** und **Maschinendetails** in Monitor ICA-Sitzungen aufzeichnen. Dieses Feature steht bei Sites mit **Premium**-Lizenz zur Verfügung.

### Dynamische Sitzungsaufzeichnung

Sie können die aktuelle aktive Sitzung mithilfe der Steuerelemente für die Sitzungsaufzeichnung im Bildschirm **Benutzerdetails** aufzeichnen. Weitere Informationen zur dynamischen Sitzungsaufzeichnung finden Sie im Artikel zum Sitzungsaufzeichnungsdienst.

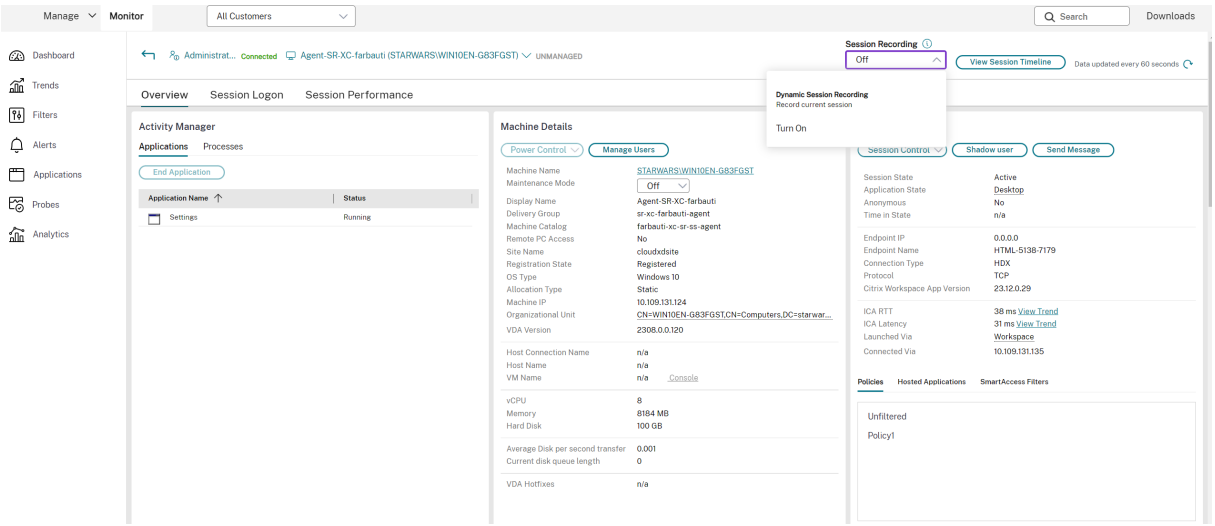
 

### Steuerelemente der Sitzungsaufzeichnung in Monitor

Sie können die Aktionen **Benutzerdetails** > **Sitzungsaufzeichnung** verwenden, um die aktuelle oder nachfolgende Sitzung aufzuzeichnen.

- Dynamische Sitzungsaufzeichnung einschalten: Die aktuelle Sitzung wird aufgezeichnet.
- Ausschalten: Die Aufzeichnung von Sitzungen wird für den Benutzer deaktiviert.

Im Bereich **Richtlinie** wird der Name der aktiven Sitzungsaufzeichnungsrichtlinie angezeigt.




Im Bereich **Maschinendetails** wird der Status der Sitzungsaufzeichnungsrichtlinie für die Maschine angezeigt.

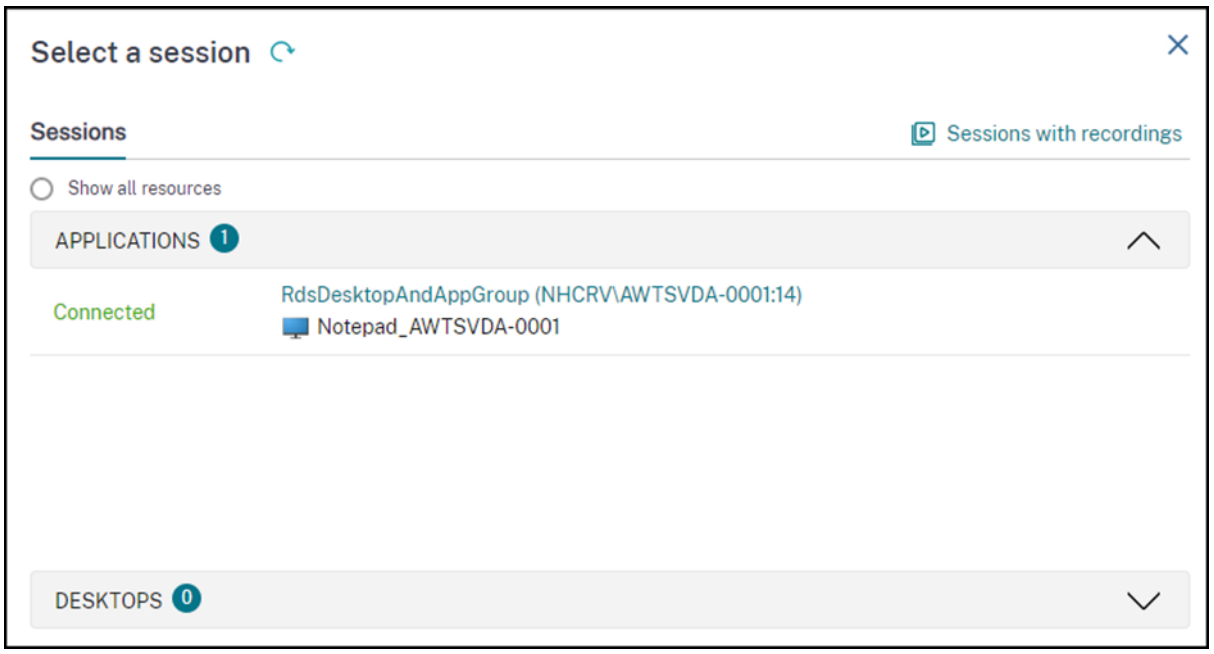
### Livesitzungen und aufgezeichnete Sitzungen wiedergeben

Sie können aufgezeichnete und Livebenutzersitzungen wiedergeben, um zu verstehen, auf welche Probleme der Benutzer gestoßen ist. Dank des direkten Zugriffs auf Aufzeichnungen und sitzungsbezogene Messwerte in der Monitor-Konsole müssen Sie nicht mehr auf mehreren Sitzungsaufzeichnungsservern nach den Aufzeichnungen suchen oder Apps von Drittanbietern aufrufen, um die Aufzeichnungen anzusehen. Die in den Aufzeichnungen festgestellten Probleme lassen sich so mit den Leistungskennzahlen verknüpfen.

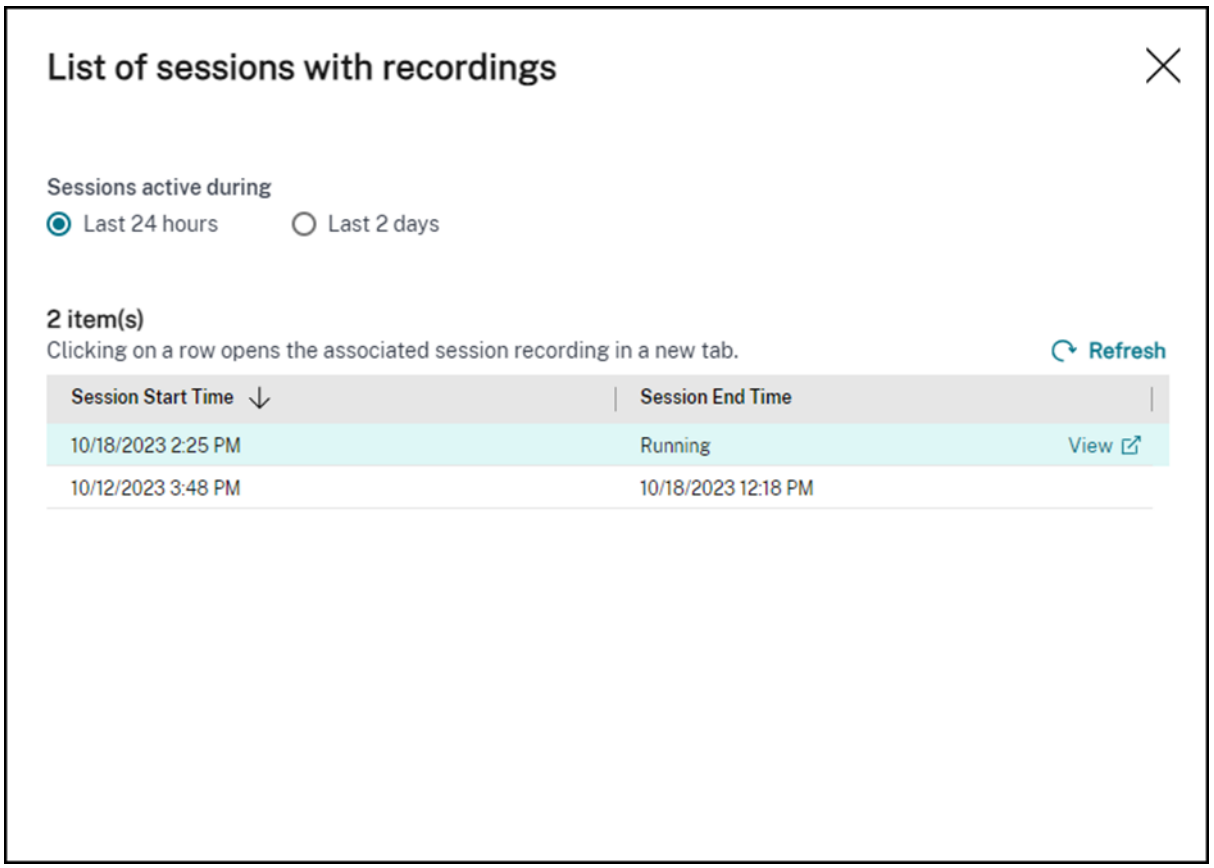
Für dieses Feature sind der VDA und die Sitzungsaufzeichnungsserver Version 2308 oder höher erforderlich.

Monitor speichert Sitzungsaufzeichnungen in einem zentralen Repository. Die Liste der Aufzeichnungen, die dem Benutzer gehören, wird angezeigt, wenn Sie auf das Modal **Sitzungsauswahl** > **Sitzungen mit Aufzeichnungen** klicken.




Sie können wählen, ob Sie Aufzeichnungen von Sitzungen anzeigen möchten, die in den letzten 24 Stunden oder in den letzten 2 Tagen aktiv waren. Liveaufzeichnungen von aktuell aktiven Sessions sind mit **Sitzungsende** als **Wird ausgeführt** gekennzeichnet.



Klicken Sie auf den Link **Anzeigen**, um die Aufzeichnung auf einer neuen Registerkarte mit dem Wiedergabeserver der Citrix Sitzungsaufzeichnung wiederzugeben.

## Featurekompatibilitätsmatrix

June 12, 2024

Citrix Monitor unterstützt drei Editionen von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service): **Premium**, **Citrix DaaS Advanced** und **Citrix DaaS Advanced Plus**. In der folgenden Tabelle sind Citrix Monitor-Features, VDA-Versionen, abhängige Komponenten mit den jeweiligen Editionen aufgeführt.

| Feature | Abhängigkeiten - erforderliche Mindestversion | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| GPU-Auslastung in Echtzeit für AMD-GPUs verfügbar | VDA 7 2212 unter 64-Bit-Windows | Ja | Ja | Ja |
| Zugriff auf Sitzungsdetails aus Citrix Analytics für Leistung | Anspruch auf Citrix Analytics für Leistung | Ja | Ja | Ja |
| Automatische Sitzungswiederverbindung | VDA 1906 | Ja | Ja | Ja |
| Sitzungsstartdauer | VDA 1903 | Ja | Ja | Ja |
| Desktoptests | Citrix Probe Agent 1903 | Ja | Nein | Nein |
| Citrix Profilverwaltung –Verarbeitungs-dauer | VDA 1903 | Ja | Ja | Ja |
| Profildrilldown | VDA 1811 | Ja | Ja | Ja |

| Feature | Abhängigkeiten - erforderliche Mindestversion | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Überwachen von Hypervisorwarnungen | Keine | Ja | Nein | Nein |
| Anwendungstests | Citrix Application Probe Agent 1811 | Ja | Nein | Nein |
| Microsoft RDS-Lizenzstatus | VDA 7.16 | Ja | Ja | Ja |
| Zugriff auf die Maschinenkonsole über die Überwachung | XenServer Hypervisor 7.3 | Ja | Ja | Ja |
| Export von Filterdaten | Keine | Ja | Ja | Ja |
| Drilldown für interaktive Sitzungen | VDA 1808 | Ja | Ja | Ja |
| GPO-Drilldown | VDA 1808 | Ja | Ja | Ja |
| Maschinendaten über OData-API verfügbar | Keine | Ja | Ja | Ja |
| Intelligente Benachrichtigungsrichtlinien | Keine | Ja | Nein | Nein |
| Health Assistant-Link | Keine | Ja | Ja | Ja |
| Drilldown für interaktive Sitzungen | Keine | Ja | Ja | Ja |
| Anwendungsanalyse | VDA 7.15 | Ja | Ja | Ja |
| OData API V.4 | Keine | Ja | Ja | Ja |

| Feature | Abhängigkeiten - erforderliche Mindestversion | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Spiegeln von Linux-VDA-Benutzersitzungen | VDA 7.16 | Ja | Ja | Ja |
| Zugriff auf die Maschinenkonsole | Keine | Ja | Ja | Ja |
| Überwachen von Anwendungsstörungen | VDA 7.15 | Ja | Ja | Ja |
| Anwendungszentrierte Problembehandlung | VDA 7.13 | Ja | Ja | Ja |
| Datenträgerüberwachung | VDA 7.14 | Ja | Ja | Ja |
| GPU-Überwachung | VDA 7.14 | Ja | Ja | Ja |
| Transportprotokoll in den Sitzungsdetails | VDA 7.13 | Ja | Ja | Ja |
| Benutzerfreundliche Beschreibung von Verbindungs- und Maschinenfehlern | VDA 7.x | Ja | Ja | Ja |
| Aufbewahrung historischer Daten | VDA 7.x | Ja | Nein | Nein |
| Benutzerdefinierte Berichte | VDA 7.x | Ja | Nein | Nein |
| Ressourcenauslastungsbericht | VDA 7.11 | Ja | Ja | Ja |

| Feature | Abhängigkeiten - erforderliche Mindestversion | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Warnungen erweitert auf CPU-, Speicher- und ICA-RTT-Bedingungen | VDA 7.11 | Ja | Nein | Nein |
| Verbesserungen am Berichtexport | VDA 7.x | Ja | Ja | Ja |
| Anmeldedauer | VDA 7.x | Ja | Ja | Ja |
| Proaktive Überwachung und Warnungen | VDA 7.x | Ja | Nein | Nein |
| Nutzung gehosteter Anwendungen | VDA 7.x | Ja | Nein | Nein |
| Nutzung von Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS | VDA 7.x | Ja | Nein | Nein |
| Unterstützung für Framehawk Virtual Channel | VDA 7.6 | Ja | Ja | Ja |

## Delegierte Administration und Überwachung

April 1, 2022

Bei der delegierten Administration werden drei Konzepte eingesetzt: Administratoren, Rollen und Geltungsbereiche. Berechtigungen richten sich nach der Administratorrolle und dem Geltungsbereich dieser Rolle. Beispiel: Einem Administrator wird die Helpdeskadministratorrolle zugewiesen, bei der der Geltungsbereich die Verantwortung für Endbenutzer an nur einer Site umfasst.

Die Berechtigungen eines Administrators definieren das Aussehen der Überwachungsoberfläche und legen fest, welche Aufgaben er ausführen kann. Mit Berechtigungen wird Folgendes festgelegt:

- Die Seiten, auf die der Administrator zugreifen kann, kollektiv als "Ansicht"bezeichnet
- Die Desktops, Maschinen und Sitzungen, die der Administrator anzeigen und verwenden kann
- Die Befehle, die der Administrator ausführen kann, z. B. das Spiegeln einer Benutzersitzung oder das Aktivieren des Wartungsmodus

Die Überwachung unterstützt jetzt auch Rollen delegierter Administratoren, mit denen Sie benutzerdefinierte oder integrierten Rollen Administratoren zuweisen können. Die Rolle definiert die verfügbaren Berechtigungen und legt damit fest, wie ein Administrator die Überwachung verwendet. Sie können auch den Geltungsbereich für diese Rollen definieren. Der Bereich bestimmt die Objekte, für die die Rolle verantwortlich ist.

Weitere Informationen über das Erstellen von delegierten Administratoren finden Sie unter Delegierte Administration.

Über die integrierten Rollen und Berechtigungen wird festgelegt, wie Administratoren den **Überwachungsdienst** verwenden:

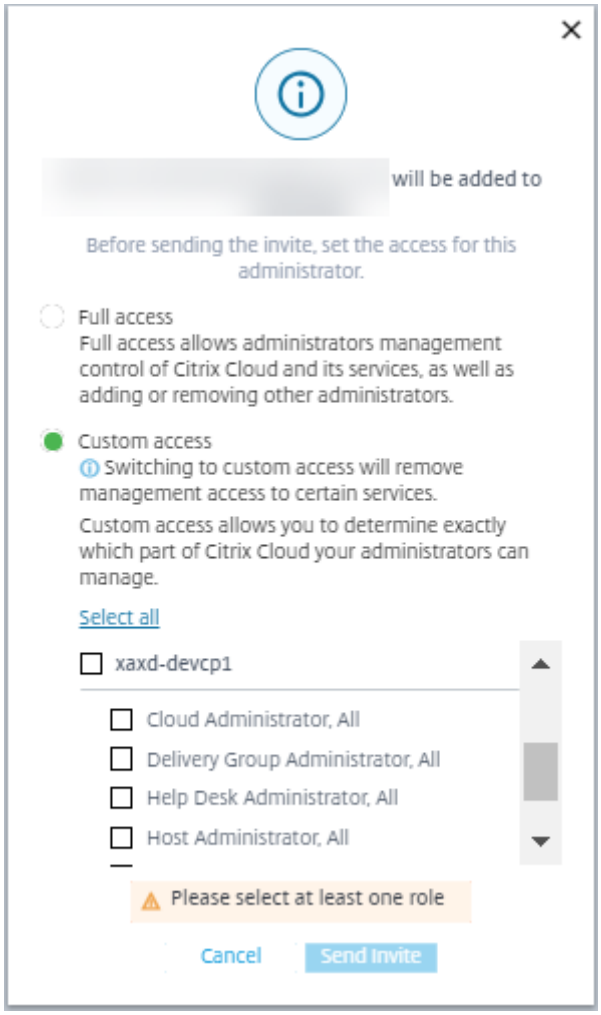
| Administratorrolle | Berechtigungen bei der Überwachung |
|---|---|
| Volladministrator | Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten. |
| Bereitstellungsgruppenadministrator | Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten. |
| Lesezugriffadministrator | Kann auf alle Ansichten zugreifen und alle Objekte in angegebenen Geltungsbereichen sowie globale Informationen anzeigen. Kann Berichte aus HDX-Kanälen herunterladen und Trenddaten mit der Exportoption in der Ansicht "Trends"exportieren. Kann keine anderen Befehle ausführen oder Daten in den Ansichten ändern. |

| Administratorrolle | Berechtigungen bei der Überwachung |
|---|---|
| Helpdeskadministrator | Kann nur auf die Ansichten “Helpdesk”und “Benutzerdetails”zugreifen und nur Objekte anzeigen, die dem Administrator zur Verwaltung übertragen wurden. Kann eine Benutzersitzung spiegeln und Befehle für diesen Benutzer ausführen. Kann Vorgänge im Wartungsmodus ausführen. Kann Energieoptionen auf Maschinen mit Einzelsitzungs-OS verwenden. Kann nicht auf das Dashboard, Trends, Warnungen oder Filteransichten zugreifen. Kann keine Energieoptionen auf Maschinen mit Multisitzungs-OS verwenden. |
| Maschinenkatalogadministrator | Kann nur auf die Seite “Maschinendetails” zugreifen (maschinenbasierte Suche). |
| Hostadministrator | Kein Zugriff. Dieser Administrator wird für die Überwachung nicht unterstützt und er kann keine Daten anzeigen. |
| Probe Agent-Administrator | Schreibgeschützter Zugriff auf die Seite “Anwendungen”, kann nicht auf eine andere Ansicht zugreifen. Zum Ausführen von Citrix Probe Agent auf Endpunktmaschinen gedacht. |
| Volladministrator für “Überwachen” | Hat vollen Zugriff auf alle Ansichten und Befehle auf der Registerkarte **Überwachen** |
| Sitzungsadministrator | Kann Bereitstellungsgruppen anzeigen und ihre zugeordneten Sitzungen und Maschinen auf der Seite **Filter** der Registerkarte **Überwachen** verwalten. |

Um einem Benutzer eine Rolle zuzuweisen (integriert oder benutzerdefiniert), wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** > **Administratoren**. Wenn Sie hier den Zugriff eines Administrators einrichten oder bearbeiten, können Sie **Benutzerdefinierter Zugriff** und dann eine der Rollen auswählen.

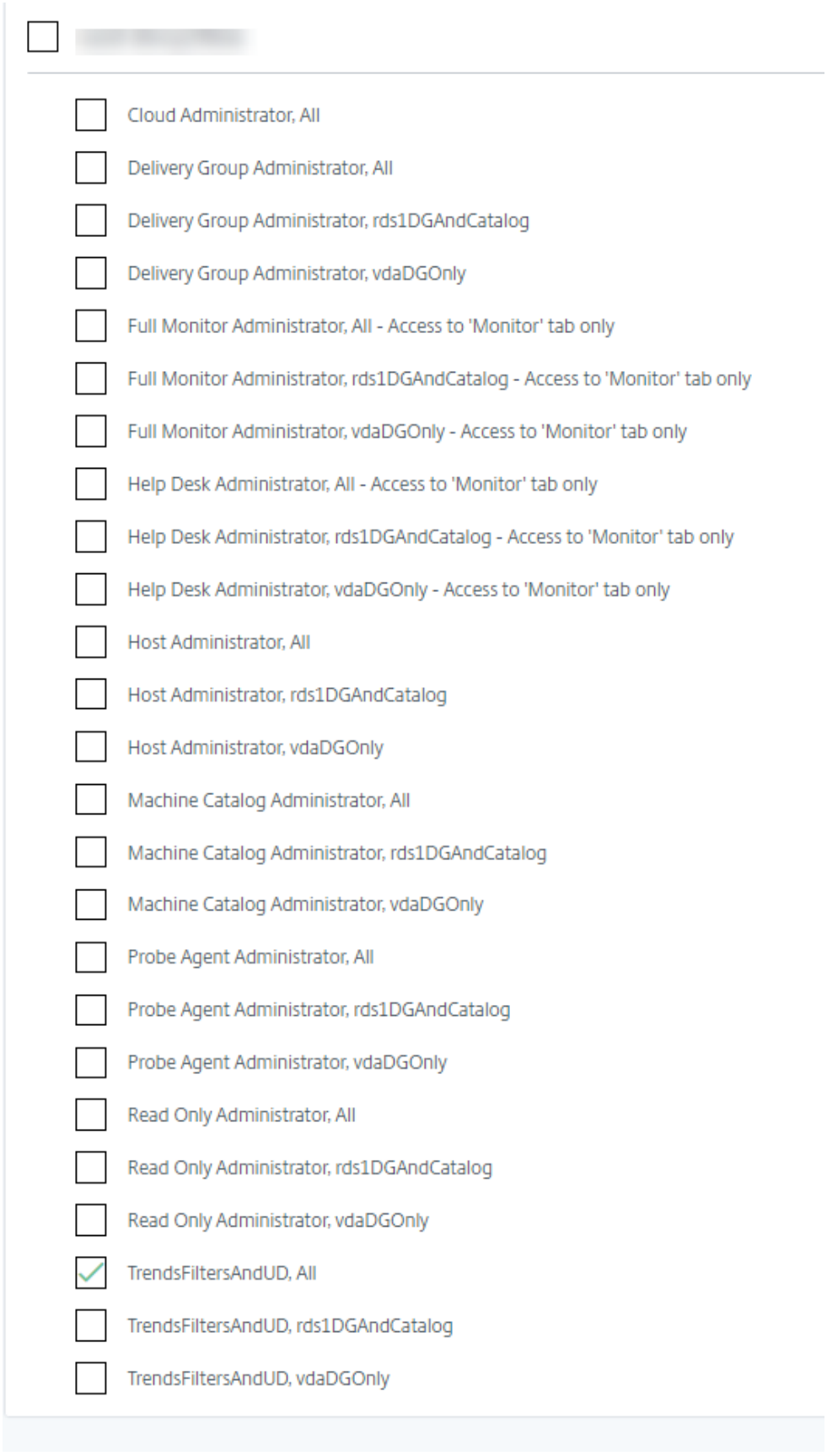
 




Sie können benutzerdefinierte Rollen und Bereiche unter **Vollständige Konfiguration > Administratoren > Administratoren** definieren.

Die integrierten und benutzerdefinierten Rollen werden zur Auswahl mit benutzerdefinierten Bereichen aufgelistet.



# Datengranularität und -beibehaltung

January 17, 2023

## Aggregation von Datenwerten

Der Überwachungsdienst erfasst diverse Daten über Benutzersitzungsnutzung, Benutzeranmeldeleistung, Sitzungslastausgleich und zu Fehlern bei Verbindungen und Maschinen. Die Daten werden je nach Kategorie unterschiedlich aggregiert. Zum Interpretieren der Daten sind Kenntnisse über die Aggregation der mit den OData-Methoden-APIs abgerufenen Datenwerte unverzichtbar. Beispiel:

- Fehler bei verbundenen Sitzungen und Maschinen treten über einen Zeitraum verteilt auf. Daher werden sie per Zeitraum als Höchstwerte angegeben.
- Die Anmeldedauer ist ein Zeitlängenwert und wird daher als Durchschnitt per Zeitraum angegeben.
- Die Anzahl der Anmeldungen und Verbindungsfehler repräsentieren eine Anzahl von Vorkommen in einem bestimmten Zeitraum und werden als Summen in einem Zeitraum gemacht.

## Gleichzeitigkeit von Daten

Sitzungen müssen sich überschneiden, um als gleichzeitig angesehen zu werden. Wenn das Zeitintervall jedoch 1 Minute beträgt, werden alle Sitzungen in dieser Minute (unabhängig davon, ob sie sich überlappen) als gleichzeitig behandelt. Das Intervall ist so klein, dass der Mehraufwand für die Berechnung der Genauigkeit sich nicht lohnt. Finden die Sitzungen in der gleichen Stunde, aber nicht in der gleichen Minute statt, werden sie als einander nicht überschneidend angesehen.

## Korrelation zwischen Zusammenfassungstabellen und Rohdaten

Das Datenmodell stellt Metriken auf zwei verschiedene Arten dar:

- Die Zusammenfassungstabellen zeigen aggregierte Ansichten der Metriken in Granularitäten pro Minute, Stunde und Tag an.
- Die Rohdaten stehen für einzelne Ereignisse oder den aktuellen Zustand, der bzw. die für eine Sitzung, Verbindung, Anwendung und andere Objekte protokolliert werden.

Wenn Sie versuchen, Daten über API-Aufrufe hinweg oder innerhalb des Datenmodells selbst zu korrelieren, sollten Sie die folgenden Konzepte und Einschränkungen kennen:

- **Keine Zusammenfassungsdaten für Teilintervalle:** Die Zusammenfassungen von Metriken erfüllen die Anforderungen von historischen Trends über lange Zeiträume. Diese Metriken werden

für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Für Teilintervalle am Anfang (die ältesten verfügbaren Daten) und am Ende der Datensammlung gibt es keine Zusammenfassungsdaten. Beim Anzeigen der Aggregation eines Tages (Intervall=1440) bedeutet dies, dass der erste Tag und der aktuelle unvollständige Tag keine Daten aufweisen. Obwohl für diese Teilintervalle u. U. Rohdaten vorhanden sind, werden sie nie zusammengefasst. Entnehmen Sie die Mindest- und Höchstwerte für "SummaryDate"aus einer bestimmten Zusammenfassungstabelle, um das früheste und letzte Aggregationsintervall für eine bestimmte Datengranularität zu bestimmen. Die Spalte "SummaryDate"stellt den Start des Intervalls dar. Die Spalte "Granularity"steht für die Länge des Intervalls der aggregierten Daten.

- **Korrelation nach Zeit:** Metriken werden, wie im vorigen Abschnitt beschrieben, für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Sie können für historische Trends verwendet werden, aber rohe Ereignisdaten stellen möglicherweise einen aktuelleren Zustand dar als die Zusammenfassung für die Trendanalyse. Bei zeitbasierten Vergleichen zwischen der Zusammenfassung und den Rohdaten muss beachtet werden, dass es keine Zusammenfassungsdaten für Teilintervalle gibt, die am Anfang und Ende des Zeitraums auftreten.
- **Verpasste und latente Ereignisse:** Wenn Ereignisse verpasst werden oder während des Aggregationszeitraums latent sind, sind die für die Zusammenfassungstabelle aggregierten Metriken möglicherweise ungenau. Obwohl der Überwachungsdienst versucht, einen genauen aktuellen Zustand zu erhalten, wird die Aggregation für verpasste oder latente Ereignisse nicht im Nachhinein neu für die Zusammenfassungstabellen berechnet.
- **Hochverfügbare Verbindungen:** Bei hoher Verfügbarkeit von Verbindungen entstehen in den Zusammenfassungsdaten für aktuelle Verbindungen Lücken, aber die Sitzungsinstanzen werden dennoch in den Rohdaten ausgeführt.
- **Beibehaltungszeitraum für Daten:** Daten werden in den Zusammenfassungstabellen basierend auf einem anderen Bereinigungszeitplan beibehalten als Rohdaten von Ereignissen. Daten fehlen möglicherweise, weil die Zusammenfassungstabellen oder die unformatierten Tabellen bereinigt wurde. Beibehaltungszeiträume können unterschiedliche Granularitäten für Zusammenfassungsdaten aufweisen. Daten basierend auf niedrigerer Granularität (Minuten) werden schneller bereinigt als Daten, die auf höherer Granularität (Tage) basieren. Wenn Daten bereinigt wurden und in einer Granularitätskategorie fehlen, sind sie möglicherweise in einer höheren Granularitätskategorie. API-Aufrufe geben nur Daten für die angeforderte Granularität zurück. Wenn für eine Granularität keine Daten zurückgegeben werden, sind möglicherweise für den gleichen Zeitraum Daten für eine höhere Granularität vorhanden.
- **Zeitzonen:** Metriken werden mit UTC-Zeitstempeln gespeichert. Zusammenfassungstabellen werden basierend auf stündlichen Zeitzonengrenzen aggregiert. Bei Zeitzonen, die nicht in diese stündlichen Grenzen fallen, gibt es möglicherweise Unstimmigkeiten beim Ort der Datenaggregation.

### Datengranularität und -beibehaltung

Die Granularität der aggregierten Daten, die vom Überwachungsdienst abgerufen werden, ist eine Funktion des angeforderten Zeitraums (T). Folgende Regeln gelten:

- 0 <T <=30 Tage: stundengenaue Granularität wird verwendet
- T > 31 Tage: tagesgenaue Granularität wird verwendet

Angeforderte Daten, die nicht von aggregierten Daten stammen, stammen von den rohen Sitzungs- und Verbindungsinformationen. Diese Menge dieser Daten nimmt schnell zu, daher haben sie eine eigene Bereinigungseinstellung. Bereinigung gewährleistet, dass nur relevante Daten langfristig gespeichert werden. Damit wird eine bessere Leistung sichergestellt, während die für die Berichterstellung erforderliche Granularität beibehalten werden kann.

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | Beibehaltungszeitraum für Sitzungs- und Verbindungsinformationen nach Beenden der Sitzung | 90 | 31 |
| 2 | GroomFailuresRetentionDays | Einträge für MachineFailureLog und ConnectionFailureLog | 90 | 31 |
| 3 | GroomLoadIndexesRetentionDays | Einträge für LoadIndex | 90 | 31 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 4 | GroomDeletedRetentionDays | MachineDays, Katalog-, Desktopgruppen- und Hypervisoren-titäten, die einen LifecycleState von “Deleted” haben. Dadurch werden auch zugehörige Einträge für Sitzung, Sitzungsde-tail, Zusammen-fassung, Fehler oder LoadIndex gelöscht. | 90 | 31 |
| 5 | GroomSummariesRetentionDays | Einträge für Desktop-GroupSum-mary, FailureLog-Summary und LoadIndex-Summary. Aggregierte Daten, tägliche Granularität | 365 | 31 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 6 | GroomMachineHotfixLogRetentionDays | Auf VDA- und Controller-maschinen angewendete Hotfixes | 90 | 31 |
| 7 | GroomHourlyRetentionDays | Aggregierte Daten - stun-dengenaue Granularität | 32 | 31 |
| 8 | GroomApplicationUsageRetentionDays | Anwendungsnutzung | 90 | Nicht zutreffend |
| 9 | GroomNotificationLogRetentionDays | Benachrichtigungsprotokolldaten | 90 | Nicht zutreffend |
| 10 | GroomResourceUsageRawDataRetentionDays | Rohdaten zur Ressource-nauslastung | 3 | 3 |
| 11 | GroomResourceUsageHourDataRetentionDays | Zusammengefasste Daten zur Ressource-nauslastung mit stunden-genauer Granularität | 30 | 30 |
| 12 | GroomResourceUsageDayDataRetentionDays | Zusammengefasste Daten zur Ressource-nauslastung mit tagesgenauer Granularität | 365 | 31 |
| 13 | GroomProcessUsageRawDataRetentionDays | Rohdaten zur Prozessauslas-tung | 1 | 1 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 14 | GroomProcessUsageHourDataRetentionDays | Zugehörige Daten zur Auslastung mit stundengenauer Granularität | 7 | 7 |
| 15 | GroomProcessUsageDayDataRetentionDays | Zugehörige Daten zur Auslastung mit tagesgenauer Granularität | 30 | 30 |
| 16 | GroomSessionMetricsDataRetentionDays | Daten zu Sitzungskennzahlen | 1 | 1 |
| 17 | GroomMachineMetricsDataRetentionDays | Daten zu Maschinenkennzahlen | 3 | 3 |
| 18 | GroomMachineMetricsSummarizedDataRetentionDays | Zusammengefasste Daten zu Maschinenkennzahlen | 395 | 31 |
| 19 | GroomApplicationErrorsRetentionDays | Anwendungsfehlerdaten | 1 | 1 |
| 20 | GroomApplicationUsageRetentionDays | Anwendungsnutzungsdaten | 1 | 1 |

> **Achtung:**
>
> Sie können die Werte in der Überwachungsdienstdatenbank nicht ändern.

Das Beibehalten von Daten über lange Zeiträume hinweg hat die folgenden Auswirkungen auf die Größe von Tabellen:

- **Stundengenaue Daten:** Wenn Sie stundengenaue Daten bis zu zwei Jahre lang in der Datenbank speichern, wächst die Datenbank einer Site mit 1000 Bereitstellungsgruppen ungefähr wie folgt an:

1000 Bereitstellungsgruppen x 24 Stunden/Tag x 365 Tage/Jahr x 2 Jahre = 17.520.000 Datenreihen. Diese große Datenmenge in den Aggregationstabellen hat beträchtliche Auswirkungen auf die Leistung. Wenn man bedenkt, dass die Dashboarddaten aus dieser Tabelle gezogen werden, sind die Anforderungen an den Datenbankserver möglicherweise riesig. Übermäßig viele Daten können dramatische Auswirkungen auf die Leistung haben.

- **Sitzungs- und Ereignisdaten:** Diese Daten werden jedes Mal gesammelt, wenn eine Sitzung gestartet und eine Verbindung/Wiederverbindung hergestellt wird. Bei einer großen Site (100.000 Benutzer) nimmt die Menge dieser Daten schnell zu. Beispielsweise entsprechen die über zwei Jahre gespeicherten Tabellen mehr als ein TB Daten und erfordern eine High-End-Unternehmensdatenbank.

## Sitzungsstartdiagnose

March 30, 2024

> **Hinweis:**
>
> Die Sitzungsstartdiagnose ist derzeit als Preview erhältlich.

Am Sitzungsstart sind mehrere Citrix Komponenten beteiligt. Untersuchen Sie Fehler beim Sitzungsstart mit Citrix Monitor (d. h. dem Citrix Director-Dienst), um präzise einzugrenzen, welche Komponente und Phase das Problem verursacht. Wenden Sie die empfohlenen Maßnahmen an, um das Problem zu beheben. Die Citrix Workspace-App generiert eine 32-stellige (8-4-4-4-12) Transaktions-ID, die zur Fehlerdiagnose beim Sitzungsstart verwendet werden kann.

> **Hinweis:**
>
> Dieses Feature ist nur für Cloud-Kunden in den Regionen USA, AP-S und EU verfügbar. In den Regionen “Japan”und “Government”ist es nicht verfügbar.

### Voraussetzungen

Wenn Sie Citrix DaaS verwenden, erfolgt das Onboarding automatisch. Cloud-Kunden, die On-Premises-StoreFront verwenden, müssen sicherstellen, dass eine unterstützte StoreFront-Version integriert ist.

- Wenn Sie Citrix Analytics für Leistung verwenden, konsultieren Sie Datenquellen für Anweisungen zum Integrieren von On-Premises-StoreFront.
- Wenn Sie nicht Citrix Analytics für Leistung verwenden:

1. Gehen Sie zu `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.
2. Klicken Sie auf **Verbinden mit StoreFront-Bereitstellung**, geben Sie die Details ein und laden Sie die Konfigurationsdatei herunter. Weitere Informationen finden Sie unter Onboarding on-premises sites using StoreFront.

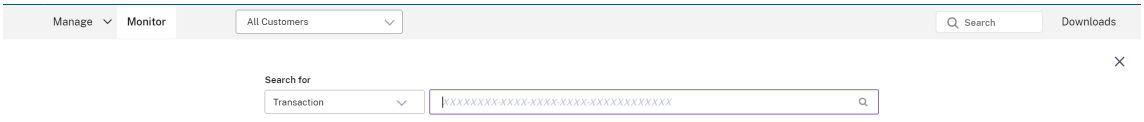
> **Hinweis:**
>
> Administratoren mit Cloud-Administratorrolle können StoreFront-Bereitstellungen integrieren, während Administratoren mit der Rolle "Volladministrator für Überwachen"diese nur anzeigen können.

Die unterstützten Mindestversionen anderer Komponenten sind wie folgt:

- Citrix Workspace-App für Windows 2109
- Citrix Workspace-App für Mac 2112
- Citrix Workspace-App für Linux 2112
- Citrix Workspace-App für HTML5 2110
- Citrix Workspace-App für Chrome 2110
- Citrix Workspace-App für Android 2110
- VDA-Version: Citrix Virtual Apps and Desktops 2112
- Citrix StoreFront 1912 LTSR CU4

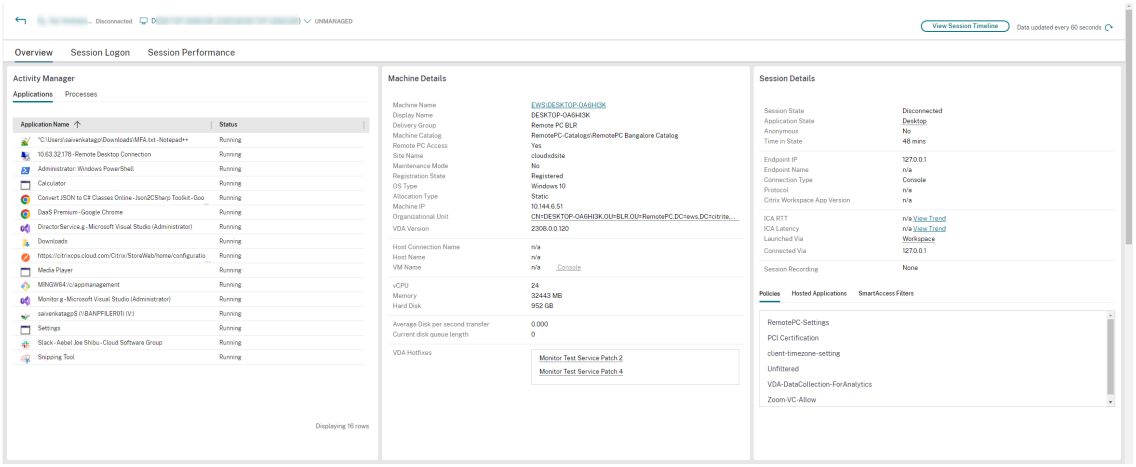
### Schritte zur Fehlerdiagnose beim Sitzungsstart

1. Kopieren Sie die Transaktions-ID des fehlgeschlagenen Sitzungsstarts aus der Citrix Workspace-App.
2. Suchen Sie in der Benutzeroberfläche "Überwachen"nach der 32-stelligen Transaktions-ID klicken Sie auf **Details**.

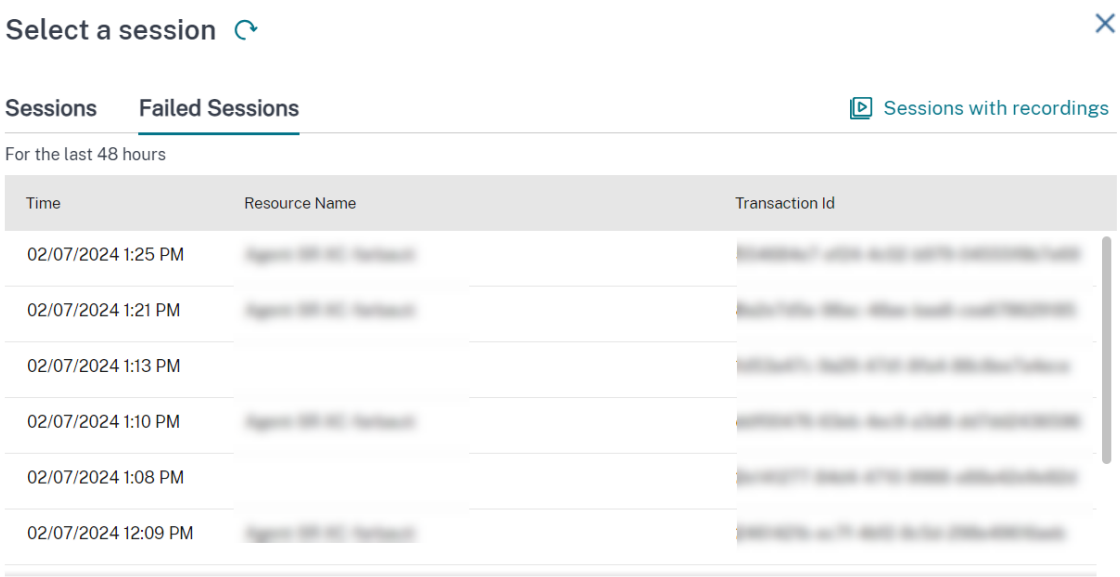



3. Bei nicht verfügbarer Transaktions-ID suchen Sie nach dem Benutzernamen. Der Aktivitätsmanager des Benutzers wird angezeigt.

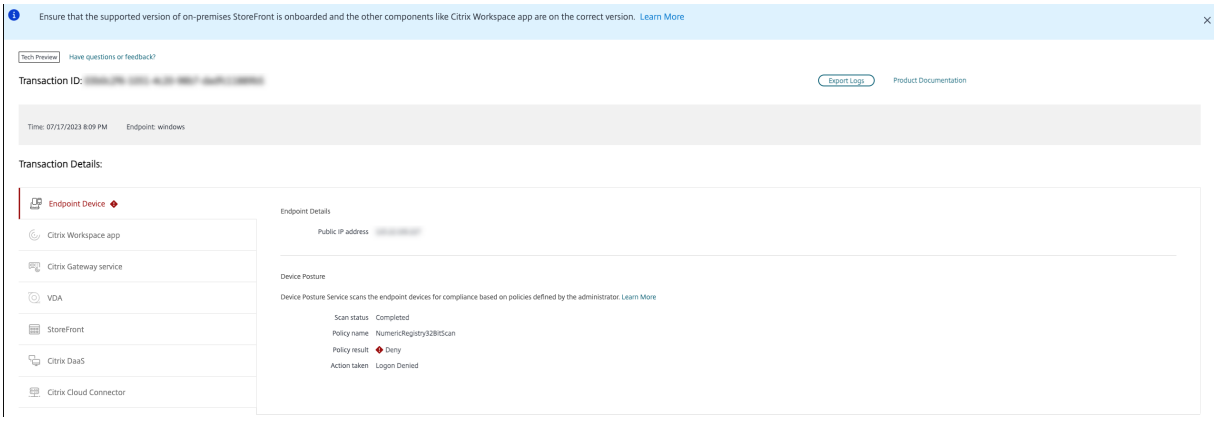



4. Klicken Sie auf die Sitzungsauswahl. Gehen Sie zur Registerkarte **Fehlgeschlagene Sitzungen**. Sie sehen eine Liste der Sitzungen, die in den letzten 48 Stunden fehlgeschlagen sind. Klicken Sie auf die ausgewählte Sitzung.




5. Die Citrix-Benutzeroberfläche “Überwachen”zeigt wichtige Informationen zur Transaktion an, z. B. den Benutzernamen, den Zeitstempel und die Anwendung oder den Desktop, wo der Fehler aufgetreten ist.
6. Der Bereich “Transaktionsdetails”enthält eine Liste der Komponenten und zeigt, wo ein Fehler aufgetreten ist.
7. Klicken Sie in der Liste der Komponenten auf **Endpoint Device**, um den Status der Device Posture-Überprüfung anzuzeigen. Der Device Posture-Dienst überprüft das Endgerät auf der Grundlage der vom Administrator definierten Richtlinien auf Richtlinientreue.

Seite 


Der Überprüfungsstatus, der Richtlinienname, das Richtlinienergebnis und die ausgeführte Aktion werden angezeigt. Stellen Sie sicher, dass der Device Posture-Dienst mit DaaS konfiguriert (siehe Device Posture). Eine Beschreibung der von Device Posture protokollierte Fehler finden Sie unter Device Posture Error Logs.

1. Durch Klicken auf die anderen Komponentennamen werden die Komponentendetails und die Details des letzten bekannten Fehlers angezeigt.
2. Der Fehlergrund und der Fehlercode werden angezeigt. Klicken Sie auf den Link **Weitere Infos über den Fehler**, um den spezifischen Fehlercode im Abschnitt Fehlercodes anzuzeigen, mit einer detaillierten Beschreibung und empfohlene Aktionen.
3. Sie können die Logs exportieren, um sie anzusehen. Die Protokolldatei listet die Schritte beim Sitzungsstart in chronologischer Reihenfolge auf und zeigt an, bei welcher Komponente und in welcher Phase der Fehler aufgetreten ist.
4. Falls mehrere Fehler in den Komponenten aufgetreten sind, werden nur die Details des letzten bekannten Fehlers auf der Transaktionsseite angezeigt. Die exportierten Logs enthalten die Details aller Fehler im Zusammenhang mit der Transaktion.

> **Hinweis:**
>
> Clientseitige Fehlercodes und Diagnoseinformationen sind nur verfügbar, wenn Citrix StoreFront integriert ist und Daten sendet. Weitere Informationen zum Integrieren von StoreFront finden Sie unter Voraussetzungen.

## Broker Agent

### bka.prepare.session.failure.validation

- Beschreibung: Fehler beim Validieren der Sitzungsvorbereitungsanforderung.
- Empfohlene Maßnahme: Wiederholen Sie die Aktion. Bei wiederholter Fehlermeldung überprüfen Sie, ob die Connectors funktionsfähig sind.

**bka.prepare.session.failure.rejected**

- Beschreibung: Der VDA kann die Startanforderung nicht annehmen.
- Empfohlene Maßnahme: Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

**bka.hdx.prepare.failure.general**

- Beschreibung: Fehler bei HDX-Vorbereitung.
- Empfohlene Maßnahme: Starten Sie den VDA neu.

**bka.hdx.validate.failure.ticket_not_found**

- Beschreibung: Referenziertes Ticket oder Start nicht im Startcache.
- Empfohlene Maßnahme: Gewährleisten Sie die Kommunikation zwischen VDA und Connector.

**bka.ticketing.validate.failure.unlicensed**

- Beschreibung: Lizenz für den Start kann nicht verifiziert werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**bka.ticketing.validate.failure.general**

- Beschreibung: Allgemeiner Fehler bei Ticketvalidierung.
- Empfohlene Maßnahme: Sammeln Sie Protokolle auf dem VDA und wenden Sie sich an den Citrix Support.

**bka.set.configuration.failure.policy**

- Beschreibung: Fehler beim Festlegen von Richtlinien.
- Empfohlene Maßnahme: Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

**bka.set.configuration.failure**

- Beschreibung: Fehler beim Festlegen der Konfiguration.
- Empfohlene Maßnahme: Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

## Broker

### brk.validate.credentials.failure.invalid

- Beschreibung: Fehler beim Validieren der Anmeldeinformationen aufgrund eines Problems. Die Fehlerursache kann im Meldungsparameter erweitert werden.
- Empfohlene Maßnahme: Wiederholen Sie die Aktion. Bei wiederholter Fehlermeldung überprüfen Sie, ob die Connectors funktionsfähig sind.

### brk.resolve.machine.failure.general

- Beschreibung: Worker kann nicht enumeriert oder aufgelöst werden. Die Fehlerursache kann im Meldungsparameter erweitert werden.
- Empfohlene Maßnahme: Stellen Sie sicher, dass Maschinen, die diese Anwendung starten können, beim Broker registriert sind. Stellen Sie sicher, dass alle verfügbaren Maschinen freie Kapazitäten besitzen.

### brk.license.check.failure.constraints

- Beschreibung: Fehler beim Sitzungsstart aufgrund von Lizenzeinschränkungen.
- Empfohlene Maßnahme: Stellen Sie sicher, dass Lizenzen für diese Art von Anwendung oder Desktop verfügbar sind.

### brk.resolve.machine.failure.timeout

- Beschreibung: Timeout des Brokers während des Datenbankzugriffs.
- Empfohlene Maßnahme: Probleme bei der Kommunikation mit der Site-Datenbank. Wenden Sie sich an den Citrix Support.

### brk.poweron.forlaunch.queued.failure.general

- Beschreibung: Fehler bei Energieaktion in Warteschlange.
- Empfohlene Maßnahme: Probleme bei der Kommunikation mit der Site-Datenbank. Wenden Sie sich an den Citrix Support.

### brk.set.configuration.failure.general

- Beschreibung: Unbekannter Fehler beim Festlegen der Konfiguration auf dem Ziel-VDA.

- Empfohlene Maßnahme: Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

**brk.prepare.session.failure.host_unreachable**

- Beschreibung: Fehler bei der Kommunikation mit dem VDA.
- Empfohlene Maßnahme: Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

**brk.prepare.session.failure.general**

- Beschreibung: Fehler bei der Sitzungsvorbereitung auf dem VDA, UnsupportedClientType- oder ConnectionRefused-Fehler.
- Empfohlene Maßnahme: Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

**brk.validate.ticket.failure.license**

- Beschreibung: Fehler beim Abrufen einer gültigen Lizenz für diese Sitzung.
- Empfohlene Maßnahme: Überprüfen Sie den Integritätsstatus der Site und stellen Sie sicher, dass alle Connectors und der Citrix DDC betriebsbereit sind.

**brk.validate.ticket.failure.general**

- Beschreibung: Ungültiger Ticketingaufruf.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**brk.reverse.prepare.failure.general**

- Beschreibung: Allgemeiner Fehler während des Sitzungsstarts.
- Empfohlene Maßnahme: Überprüfen Sie den Integritätsstatus der Site und stellen Sie sicher, dass alle Connectors und der Citrix DDC betriebsbereit sind.

**brk.reverse.prepare.failure.lease_revoked**

- Beschreibung: Lease für diese Sitzung wurde widerrufen.
- Empfohlene Maßnahme: Wiederholen Sie die Aktion. Wenn der Fehler sich wiederholt, überprüfen Sie die Funktionsfähigkeit der Connectors.

#### brk.reverse.prepare.failure.resource_unavailable

- Beschreibung: Die Ressource wird bereits verwendet oder ist vorübergehend nicht verfügbar.
- Empfohlene Maßnahme: Wiederholen Sie die Aktion. Wenn der Fehler sich wiederholt, überprüfen Sie die Funktionsfähigkeit der Connectors.

#### brk.reverse.prepare.failure.app_protection

- Beschreibung: App Protection fehlt und ist für diese Sitzung erforderlich.
- Empfohlene Maßnahme: Stellen Sie sicher, dass App Protection auf diesem VDA aktiviert ist, oder entfernen Sie die App Protection-Anforderung aus der Anwendung.

### HDX VDA Linux

#### VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Beschreibung: Wiederverbinden mit Sitzung im Vorabmeldezustand nicht zulässig.
- Empfohlene Maßnahme: Warten Sie und wiederholen Sie den Start später, damit ausreichend Zeit zum Abmelden der Sitzung bleibt.

#### VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Beschreibung: Wiederverbinden mit Sitzung, die nicht beendet wurde.
- Empfohlene Maßnahme: Versuchen Sie den Sitzungsstart später erneut. Wenn der Fehler erneut auftritt, wenden Sie sich an den Citrix Support.

#### VDA_LINUX_ERR_SAME_KEY

- Beschreibung: Verbindung wird vorbereitet, es liegt jedoch eine vorhandene Sitzung mit demselben Sitzungsschlüssel vor.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VDA_LINUX_ERR_GET_FQDN

- Beschreibung: Fehler beim Abrufen des FQDN für diesen VDA.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die DNS-Konfiguration auf dem VDA korrekt ist.

**VDA_LINUX_ERR_NO_CGP_LISTENER**

- Beschreibung: Es wird kein CGP-Listener ausgeführt.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die Richtlinie **Sitzungszuverlässigkeit - Verbindungen** aktiviert ist. Überprüfen Sie, ob der CGP-Listener den erwarteten Port im VDA überwacht (Standardport: 2598, kann über die Richtlinie **Sitzungszuverlässigkeit - Portnummer** geändert werden).

**VDA_LINUX_ERR_DTLS_CONNECT**

- Beschreibung: Fehler beim Herstellen einer DTLS-Verbindung zum Gateway Service.
- Empfohlene Maßnahme: Stellen Sie sicher, dass der FQDN des Gateway Service vom VDA erreicht werden kann. Prüfen Sie, ob der Pfad `/var/xdl/keystore/cacerts` im VDA vorhanden ist. Entfernen Sie `/var/xdl/keystore` und führen Sie `/var/xdl/split_ca_bundle.sh` aus, um ZS-Zertifikate neu zu generieren. Stellen Sie sicher, dass der FQDN des Gateway Service vom VDA als vertrauenswürdig eingestuft wird.

**VDA_LINUX_ERR_ACCEPT_EDT_CONNECT**

- Beschreibung: Fehler beim Akzeptieren des EDT-Handshake vom Client.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_TCP_CONNECT**

- Beschreibung: Fehler beim Herstellen einer TCP-Verbindung zum Gateway Service.
- Empfohlene Maßnahme: Stellen Sie sicher, dass der FQDN des Gateway Service vom VDA erreicht werden kann.

**VDA_LINUX_ERR_TLS_CONNECT**

- Beschreibung: Fehler beim Herstellen eines TLS-Handshake zum Gateway Service.
- Empfohlene Maßnahme: Überprüfen Sie, ob der Pfad `/var/xdl/keystore/cacerts` im VDA vorhanden ist. Entfernen Sie `/var/xdl/keystore` und führen Sie `/var/xdl/split_ca_bundle.sh` aus, um ZS-Zertifikate neu zu generieren. Stellen Sie sicher, dass der FQDN des Gateway Service vertrauenswürdig ist.

**VDA_LINUX_ERR_RDVZ_HANDSHAKE**

- Beschreibung: Fehler beim Herstellen eines Rendezvous-Handshake zum Gateway Service.

- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_ACCEPT_ICA_CONNECT**

- Beschreibung: Fehler beim Akzeptieren einer ICA-Verbindung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED**

- Beschreibung: Wiederverbinden mit anonymer Sitzung nicht zulässig.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_CONN_NOT_ALLOWED**

- Beschreibung: Verbindung ist nicht zulässig.
- Empfohlene Maßnahme: Wenn der Ergebniscode 3 vorliegt, stellen Sie sicher, dass die Lizenz nicht abgelaufen ist. Andernfalls versuchen Sie den Sitzungsstart später erneut. Wenn Sie das Problem nicht beheben können, wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_CONN_GENERAL**

- Beschreibung: Fehler beim Validieren der Verbindung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_USER_CANCELLED_LOGIN**

- Beschreibung: Der Endbenutzer hat die Anmeldung abgebrochen.
- Empfohlene Maßnahme: Dieser Fehler ist zu erwarten, wenn der Endbenutzer bei deaktiviertem Single Sign-On im Anmeldedialogfeld auf die Schaltfläche "Abbrechen"klickt. Andernfalls wenden Sie sich an den Citrix Support.

**VDA_LINUX_ERR_GET_TARGET**

- Beschreibung: Fehler beim Aufrufen der Zielsitzung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VDA_LINUX_ERR_START_LOGON_TIMERS

- Beschreibung: Fehler beim Start der Anmeldungstimer.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Beschreibung: Fehler beim Senden des Befehls an die Zielsitzung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Beschreibung: Fehler beim POST von Wiederverbindungsereignis.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Beschreibung: Timeout beim Wiederverbinden mit Benutzersitzung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### HDX VDA Windows

#### RENDEZVOUS_CONNECT_FAILED_TCP

- Beschreibung: Fehler beim Herstellen einer ausgehenden Rendezvous-Transportverbindung über TCP.
- Empfohlene Maßnahme: Ausfälle wegen schlechter Netzwerkbedingungen sind sporadisch möglich. Das ist zu erwarten. Falls das Problem häufiger auftritt, prüfen Sie die VDA-Konfiguration und wenden Sie sich an den Citrix Support.

#### RENDEZVOUS_CONNECT_FAILED_EDT

- Beschreibung: Fehler beim Herstellen einer ausgehenden Rendezvous-Transportverbindung über TCP.
- Empfohlene Maßnahme: Ausfälle wegen schlechter Netzwerkbedingungen sind sporadisch möglich. Das ist zu erwarten. Falls das Problem häufiger auftritt, prüfen Sie die VDA-Konfiguration und wenden Sie sich an den Citrix Support.

**RENDEZVOUS_CONNECT_FAILED_PROXY**

- Beschreibung: Fehler beim Herstellen einer ausgehenden Rendezvous-Transportverbindung aufgrund einer ungültigen Proxykonfiguration.
- Empfohlene Maßnahme: Prüfen Sie die Rendezvous-Proxy-Konfiguration, wenden Sie sich an den Citrix Support.

**RENDEZVOUS_CONNECT_FAILED_DTLS**

- Beschreibung: Fehler beim Herstellen einer ausgehenden Rendezvous-Transportverbindung aufgrund eines fehlgeschlagenen sicheren Transport-Handshake.
- Empfohlene Maßnahme: Überprüfen Sie die Rendezvous-Konfiguration und die Kryptographiekonfiguration. Wenden Sie sich an den Citrix Support.

**RENDEZVOUS_CONNECT_FAILED_TLS**

- Beschreibung: Fehler beim Herstellen einer ausgehenden Rendezvous-Transportverbindung aufgrund eines fehlgeschlagenen sicheren Transport-Handshake.
- Empfohlene Maßnahme: Überprüfen Sie die Rendezvous-Konfiguration und die Kryptographiekonfiguration und wenden Sie sich an den Citrix Support.

**RENDEZVOUS_CONNECT_FAILED_CGP**

- Beschreibung: Fehler beim Herstellen einer ausgehenden Rendezvous-Transportverbindung aufgrund einer fehlerhaften GCP-Konfiguration.
- Empfohlene Maßnahme: Vergewissern Sie sich, dass CGP (Sitzungszuverlässigkeit) aktiviert ist und die CGP-Ports überwacht werden, wenden Sie sich an den Citrix Support.

**CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT**

- Beschreibung: Netzwerkunterbrechung wurde wegen Timeout nicht behoben, Wiederverbinden durch Sitzungszuverlässigkeit nicht möglich.
- Empfohlene Maßnahme: Ausfälle wegen schlechter Netzwerkbedingungen sind sporadisch möglich. Das ist zu erwarten.

**CGP_SR_SUSPEND_RESUME_FAILED**

- Beschreibung: Netzwerkunterbrechung wurde wegen eines unerwarteten Fehlers nicht behoben, Wiederverbinden durch Sitzungszuverlässigkeit nicht möglich.

- Empfohlene Maßnahme: Ausfälle wegen schlechter Netzwerkbedingungen sind sporadisch möglich. Das ist zu erwarten.

#### PREPARE_RECONNECT_REJECTED

- Beschreibung: Die Wiederverbindungsanforderung einer eingehenden ICA-Verbindung wurde vom VDA aufgrund eines ungültigen Sitzungsschlüssels abgelehnt.
- Empfohlene Maßnahme: Prüfen Sie die VDA-Konfiguration, wenden Sie sich an den Citrix Support.

#### Fehler: PREPARE_REJECTED

- Beschreibung: Die Verbindungsanforderung einer eingehenden ICA-Verbindung wurde vom VDA aufgrund eines ungültigen Sitzungsschlüssels abgelehnt.
- Empfohlene Maßnahme: Prüfen Sie die VDA-Konfiguration, wenden Sie sich an den Citrix Support.

#### PREPARE_LISTENING_FAILED

- Beschreibung: VDA konnte die Listener für die eingehende ICA-Verbindung nicht starten.
- Empfohlene Maßnahme: Überprüfen Sie die Netzwerkkonfiguration, stellen Sie sicher, dass die Listener-Ports nicht von anderen Anwendungen verwendet werden, wenden Sie sich an den Citrix Support.

#### RENDEZVOUSCONNECTIONREQ_FAILED

- Beschreibung: VDA konnte den ICA-Stack nicht auffordern, eine ausgehende Rendezvous-Verbindung zu starten.
- Empfohlene Maßnahme: Prüfen Sie die Rendezvous-Konfiguration, die Rendezvous-Proxy-Konfiguration und die CGP-Konfiguration (Sitzungszuverlässigkeit), wenden Sie sich an den Citrix Support.

#### RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Beschreibung: VDA konnte ICA-Stack aufgrund einer fehlerhaften Proxykonfiguration nicht auffordern, eine ausgehende Rendezvous-Verbindung zu starten.
- Empfohlene Maßnahme: Prüfen Sie die Rendezvous-Proxy-Konfiguration, wenden Sie sich an den Citrix Support.

#### ESTABLISH_SESSION_FAILED

- Beschreibung: VDA konnte keine Sitzung für die eingehende ICA-Verbindung erstellen oder sich nicht mit einer vorhandenen Sitzung verbinden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### ICA_ESTABLISH_FAILED

- Beschreibung: Fehler beim Akzeptieren von ICA-Verbindungen oder von Handshake.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VALIDATE_FAILED

- Beschreibung: Broker konnte eine eingehende ICA-Verbindungsanforderung vom VDA nicht validieren.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### VALIDATE_TICKETING_FAILED

- Beschreibung: Broker konnte eine eingehende ICA-Verbindungsanforderung vom VDA aufgrund eines Ticketingproblems nicht validieren.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### MCS

#### brk.poweron.forlaunch.execution.generalfailure

- Beschreibung: Allgemeine Fehler.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### brk.poweron.forlaunch.execution.insufficientresourcefailure

- Beschreibung: Ein Hypervisor-Vorgang kann aufgrund unzureichender Ressourcen auf dem Hypervisor nicht abgeschlossen werden.
- Empfohlene Maßnahme: Prüfen Sie das Ressourcenkontingent im Hypervisor. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.nosuchmanagedmachine**

- Beschreibung: Eine Maschinen-ID ist nicht vorhanden.
- Empfohlene Maßnahme: Überprüfen Sie die Maschinen-ID im Hypervisor. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.hypervisorconnectionfailure**

- Beschreibung: Keine Verbindung zum Hypervisor möglich. Adresse der Hosting-Infrastruktur wurde beispielsweise nicht gefunden.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die Adresse der Hosting-Infrastruktur korrekt ist. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.invalidcredentialsfailure**

- Beschreibung: Ungültige Anmeldeinformationen.
- Empfohlene Maßnahme: Prüfen Sie die Anmeldeinformationen für die Hypervisorverbindung. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.authorizationfailure**

- Beschreibung: Unzureichende Berechtigungen oder Anmeldeinformationen.
- Empfohlene Maßnahme: Prüfen Sie die Berechtigungen, die den Anmeldeinformationen für die Hypervisorverbindung zugewiesen sind. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.sslcertauthfailure**

- Beschreibung: Verbindung kann aufgrund eines SSL-Authentifizierungsproblems nicht hergestellt werden.
- Empfohlene Maßnahme: Prüfen Sie das Verbindungszertifikat des Hypervisors. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.ratelimitedfailure**

- Beschreibung: Cloudverbindung meldet ein Ratenlimit.
- Empfohlene Maßnahme: Wiederholen Sie den Verbindungsaufbau später, falls die Anforderung durch das Ratenlimit des Hypervisors blockiert wurde. Wenn Sie keine Lösung finden, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.connectorconnectionfailure**

- Beschreibung: Vorhandene Fehler im Cloud Connector. Beispielsweise kommt es beim Verbindungsaufbau zum Timeout. Beim Erreichen des Timeouts wird der Cloud Connector getrennt.
- Empfohlene Maßnahme: Starten Sie den Cloud Connector neu. Falls der Vorgang fehlschlägt, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.remotehclserverconnectionfailure**

- Beschreibung: Fehler im HCL/Remote-Proxy-Plug-In oder Endpunkt beim Einrichten der Verbindung zum Plug-In nicht gefunden.
- Empfohlene Maßnahme: Starten Sie den Connector neu. Falls das nicht gelingt, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.expiredcredentialsfailure**

- Beschreibung: Die bereitgestellten Anmeldeinformationen sind abgelaufen.
- Empfohlene Maßnahme: Aktualisieren Sie die abgelaufenen Anmeldeinformationen, die von der Hypervisorverbindung verwendet werden.

**brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure**

- Beschreibung: Fehler beim Erstellen der Maschine.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.detachdiskfailed**

- Beschreibung: Fehler beim von der virtuellen Maschine verwendeten getrennten Datenträger.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.createclonefailed**

- Beschreibung: Fehler beim Erstellen eines geklonten Datenträgers im Hypervisor.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.provisionedvmnotfound**

- Beschreibung: Die bereitgestellte VM wurde nicht gefunden.
- Empfohlene Maßnahme: Entfernen Sie die bereitgestellte VM aus dem Katalog. Falls das nicht gelingt, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.invalidvmstate**

- Beschreibung: Der Vorgang kann aufgrund eines ungültigen VM-Zustands nicht fortgesetzt werden.
- Empfohlene Maßnahme: Starten Sie zuerst die VM neu und wiederholen Sie den Vorgang.

**brk.poweron.forlaunch.execution.insufficientresources**

- Beschreibung: Unzureichende Ressourcen während des Betriebs.
- Empfohlene Maßnahme: Prüfen Sie das vom Hypervisor verwendete Ressourcenkontingent.

**brk.poweron.forlaunch.execution.hypervisorinmaintenancemode**

- Beschreibung: Der Vorgang kann nicht fortgesetzt werden, da sich der Hypervisor im Wartungsmodus befindet.
- Empfohlene Maßnahme: Prüfen Sie, ob der Hypervisor im Wartungsmodus ist.

**brk.poweron.forlaunch.execution.delayed**

- Beschreibung: Der Vorgang befindet sich in der Warteschlange.
- Empfohlene Maßnahme: Warten Sie, bis der Vorgang abgeschlossen ist. Falls der Vorgang fehlschlägt, wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.recreatevmfailed**

- Beschreibung: Fehler beim Neuerstellen der VM.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**brk.poweron.forlaunch.execution.unknownvirtualmachine**

- Beschreibung: Unbekannte virtuelle Maschine.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### brk.poweron.forlaunch.execution.ratelimitexceed

- Beschreibung: Für die Cloudverbindung gilt ein Ratenlimit.
- Empfohlene Maßnahme: Wiederholen Sie den Verbindungsaufbau später, falls die Anforderung durch das Ratenlimit des Hypervisors blockiert wurde.

#### brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Beschreibung: Der virtuelle Datenträger wird nicht gespeichert.
- Empfohlene Maßnahme: Versuchen Sie es später erneut. Falls das nicht gelingt, wenden Sie sich an den Citrix Support.

### Profilverwaltung

#### xendesktop.upm.userprofile.error.failure

- Beschreibung: Die Citrix Profilverwaltung konnte das Benutzerprofil nicht verarbeiten. Verwenden Sie stattdessen ein temporäres Profil.
- Empfohlene Maßnahme: Dieser Fehler führt nicht zu einem Anmeldefehler. Die Citrix Profilverwaltung verwendet stattdessen ein temporäres Profil. Überprüfen Sie zur Problembehandlung die Windows-Ereignisprotokolle.

#### xendesktop.upm.userprofile.error.timeout

- Beschreibung: Die Citrix Profilverwaltung konnte das Benutzerprofil in der festgelegten Zeit nicht verarbeiten.
- Empfohlene Maßnahme: Dieser Fehler führt nicht zu einem Anmeldefehler. Die Citrix Profilverwaltung verarbeitet das Benutzerprofil weiter. Überprüfen Sie zur Problembehandlung die Protokolle der Citrix Profilverwaltung.

### WEM-Agent

#### wem.agent.userpolicy.error.failure

- Beschreibung: Der Workspace Environment Management (WEM)-Agent konnte keine Gruppenrichtlinien für den Benutzer verarbeiten. Die Benutzeranmeldung wird fortgesetzt.
- Empfohlene Maßnahme: Der Fehler führt nicht zu einem Anmeldefehler. Weitere Informationen finden Sie in der WEM-Produktdokumentation und in den WEM-Agent-Dienstprotokollen.

#### wem.agent.userpolicy.error.timeout

- Beschreibung: Der Workspace Environment Management (WEM)-Agent konnte in der vorgegebenen Zeit keine Gruppenrichtlinien für den Benutzer verarbeiten. Die Benutzeranmeldung wird fortgesetzt.
- Empfohlene Maßnahme: Der Fehler führt nicht zu einem Anmeldefehler. Weitere Informationen finden Sie in der WEM-Produktdokumentation und in den WEM-Agent-Dienstprotokollen.

### Android Postlaunch

#### SessionManager.Launch.EngineLoadFailed

- Beschreibung: Fehler beim Laden oder Initiieren der ICA Engine.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### SessionManager.Launch.ConnectionFailed

- Beschreibung: Engine vor dem Verbindungsaufbau beendet.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### SessionManager.Launch.LogonFailed

- Beschreibung: Sitzung vor Abschluss des Verbindungsaufbaus getrennt.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### SessionManager.LeaseResolution.Failed

- Beschreibung: Start der Lease nicht möglich.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### SessionManager.clxmtp.SoftDeny

- Beschreibung: Fehler bei CLXMTP-Aushandlung der Engine (Soft Deny).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### SessionManager.clxmtp.SoftDeny_Implicit

- Beschreibung: Fehler bei CLXMTP-Verbindung der Engine (Implicit Soft Deny).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### Transport.Connect.NoCGP_Fail

- Beschreibung: Fehler beim Verbindungsaufbau (CGP deaktiviert).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### Transport.Connect.FallbackFail

- Beschreibung: Fehler beim Verbindungsaufbau. ICA-Fallback versucht.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### Transport.Connect.Fail

- Beschreibung: Die Verbindung ist nicht verfügbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### Android Prelaunch

#### CWA-ICADOWNLOAD_ERR_00001

- Beschreibung: Inkorrekter Typ für das Senden der ICA-Anforderung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### CWA-ICADOWNLOAD_ERR_00002

- Beschreibung: ICA-Anforderung ist ungültig.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### CWA-ICADOWNLOAD_ERR_00003

- Beschreibung: Store für ICA-Anforderung ist null.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### CWA-ICADOWNLOAD_ERR_00004

- Beschreibung: Store-URL für ICA-Anforderung ist null.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00005**

- Beschreibung: Ressourcenparameter für ICA-Anforderung ist null.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00006**

- Beschreibung: Der für die ICA-Anforderung bereitgestellte Ressourcenparameter ist kein gültiger Ressourcentyp.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00007**

- Beschreibung: Der für die ICA-Anforderung bereitgestellte Ressourcenparameter ist null für die ICA-Start-URL.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00008**

- Beschreibung: Die ICA-Anfrage ist Null mit Authentifizierungsmanager-Parametern.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00009**

- Beschreibung: Textkörper der ICA-Anforderung ist null.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000010**

- Beschreibung: Fehler beim Erstellen einer HTTP-Entität aus dem Textkörper der ICA-Anforderung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000011**

- Beschreibung: Fehler beim Download der ICA-Datei aufgrund einer Ausnahme vom Erstellen der Authentifizierungsmanageranforderung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000012**

- Beschreibung: Fehler beim Download der ICA-Datei aufgrund einer Ausnahme vom Ausführen der Authentifizierungsmanageranforderung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000013**

- Beschreibung: Fehler beim Download der ICA-Datei aufgrund einer unerwarteten Antwort von der Authentifizierungsmanageranforderung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000014**

- Beschreibung: Fehler beim Download der ICA-Datei, wenn Sie inputStream aus der Authentifizierungsmanagerantwort kopieren.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000015**

- Beschreibung: Fehler beim Parsen des ICA-Dokuments, das inputStream aus der Authentifizierungsmanagerantwort verwendet.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000016**

- Beschreibung: Das heruntergeladene ICA-Dokument ist null ohne Ausnahme.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000017**

- Beschreibung: Fehler beim Download der ICA-Datei aufgrund einer fehlgeschlagenen Antwort.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000018**

- Beschreibung: Ressource ist nicht verfügbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000019**

- Beschreibung: Die zu startende Ressource ist entweder nicht vorhanden, nicht aktiviert oder für einen Benutzer nicht sichtbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000020**

- Beschreibung: Es gibt keine weiteren aktiven Sitzungen.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000021**

- Beschreibung: Server besitzt nicht die erforderliche Lizenz zum Ausführen der angeforderten Aktivität.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000022**

- Beschreibung: Es sind keine Arbeitsstationen verfügbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000023**

- Beschreibung: Verbindung zur Arbeitsstation nicht möglich. Der Server hat die Verbindung verweigert.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000024**

- Beschreibung: Die Arbeitsstation wird gewartet und kann nicht verwendet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000025**

- Beschreibung: Ressource kann aufgrund von Fehler `resourceerror` in der ICA-Datei nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000026**

- Beschreibung: Ressource kann aufgrund von Fehler `generalapplauncherror` in der ICA-Datei nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000027**

- Beschreibung: Ressource kann aufgrund eines unbekannten Fehlers in der ICA-Datei nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000028**

- Beschreibung: Ressource kann aufgrund eines Neustartfehlers in der ICA-Datei nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000029**

- Beschreibung: Ressource kann aufgrund eines Wiederaufnahmefehlers in der ICA-Datei nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000030**

- Beschreibung: Ressource kann aufgrund eines undefinierten Fehlers in der ICA-Datei nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_000031**

- Beschreibung: Fehler beim Download der ICA-Datei. Der Fehlercode wurde jedoch nicht in der definierten Zuordnung gefunden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

## Linux Postlaunch

### SessionManager.Launch.EngineLoadFailed

- Beschreibung: Fehler beim Laden der ICA Engine.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### SessionManager.Launch.Failed

- Beschreibung: Fehler beim Sitzungsstart.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### SessionManager.Launch.ConnectionFailed

- Beschreibung: Engine vor dem Verbindungsaufbau beendet.
- Empfohlene Maßnahme: Suchen Sie nach anderen Fehlern im Zusammenhang mit dem Startversuch.

### SessionManager.Launch.LogonFailed

- Beschreibung: Sitzung vor Abschluss des Verbindungsaufbaus getrennt.
- Empfohlene Maßnahme: Dieser Fehler weist auf einen Anmeldefehler hin. Möglicherweise wurden auch keine Anmeldeinformationen manuell vom Benutzer eingegeben. Untersuchen Sie, wie der Benutzer versucht hat, sich beim Remote-VDA anzumelden.

### SessionManager.LeaseResolution.Failed

- Beschreibung: Start der Lease nicht möglich.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die Leases mit dem Clientcomputer synchronisiert wurden und weiterhin gültig sind. Der Benutzer kann sich im Onlinemodus bei Citrix Workspace anmelden, um Leases (erneut) zu synchronisieren. Suchen Sie nach Fehlern, die vom Gateway oder Cloud Connector gesendet wurden. Diese Fehler können einen Hinweis auf die Fehlerursache geben.

### Transport.Connect.NoCGP_Fail

- Beschreibung: Fehler beim Verbindungsaufbau (CGP deaktiviert).
- Empfohlene Maßnahme: Untersuchen Sie, warum der Client sich nicht über TCP oder EDT mit einem VDA verbinden kann.

#### Transport.Connect.FallbackFail

- Beschreibung: Fehler beim Verbindungsaufbau. ICA-Fallback versucht.
- Empfohlene Maßnahme: Untersuchen Sie, warum der Client sich nicht über TCP oder EDT mit einem Gateway, Connector oder VDA verbinden kann.

#### Transport.Connect.Fail

- Beschreibung: Fehler beim Verbindungsaufbau über TCP, EDT oder UDP zwischen Citrix Workspace-App und Gateway, Connector oder VDA.
- Empfohlene Maßnahme: Untersuchen Sie, warum der Client sich nicht über TCP, EDT oder UDP mit dem Gateway, Connector oder VDA verbinden kann. Möglicherweise lässt die Firewall zwischen Client und Host die Protokolle (UDP/TCP) oder die erforderlichen Ports nicht zu.

#### SessionManager.clxmtp.SoftDeny

- Beschreibung: Fehler bei CLXMTP-Aushandlung der Engine (Soft Deny).
- Empfohlene Maßnahme: Dieser Fehler weist nicht auf einen zwangsläufigen Fehlstart hin. Er zeigt an, dass die Engine über einen bestimmten Netzwerkpfad nicht erfolgreich sein kann. Suchen Sie nach Fehlern, die vom Gateway oder Cloud Connector gesendet wurden. Diese Fehler können einen Hinweis auf die Fehlerursache geben.

#### SessionManager.clxmtp.SoftDeny_Implicit

- Beschreibung: Fehler bei CLXMTP-Verbindung der Engine (Implicit Soft Deny).
- Empfohlene Maßnahme: Dieser Fehler weist nicht auf einen zwangsläufigen Fehlstart hin. Er zeigt an, dass die Engine über einen bestimmten Netzwerkpfad nicht erfolgreich sein kann. Untersuchen Sie, warum der Client einen Connector oder Gateway nicht erreicht. Der Host könnte aufgrund der Netzwerktopologie oder wegen Firewalleinschränkungen nicht erreichbar sein.

### Linux Prelaunch

#### CWA-ICADOWNLOAD_ERR_00001

- Beschreibung: Verbindung zum Store nicht möglich, da keine Antwort von der Citrix Workspace-App empfangen wurde.
- Empfohlene Maßnahme: Überprüfen Sie, ob Citrix Workspace oder StoreFront ausgefallen sind. Überprüfen Sie außerdem die Internetverbindung.

**CWA-ICADOWNLOAD_ERR_00002**

- Beschreibung: Sitzungsstart wurde vom Benutzer abgebrochen.
- Empfohlene Maßnahme: Starten Sie die Sitzung nach einiger Zeit neu.

**CWA-ICADOWNLOAD_ERR_00003**

- Beschreibung: Verbindung zum Store nicht möglich. Stellen Sie sicher, dass die Serverzertifikate gültig sind.
- Empfohlene Maßnahme: Prüfen Sie, ob Serverzertifikate installiert und aktiv sind.

**CWA-ICADOWNLOAD_ERR_00004**

- Beschreibung: Die zu startende Ressource ist nicht vorhanden, nicht aktiviert oder für einen Benutzer nicht sichtbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00005**

- Beschreibung: Arbeitsstationen sind für diese Anforderung nicht verfügbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00006**

- Beschreibung: Server besitzt nicht die erforderliche Lizenz zum Ausführen der angeforderten Aktivität.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00007**

- Beschreibung: Server hat die Verbindung zur Arbeitsstation verweigert.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00008**

- Beschreibung: Die angeforderte Arbeitsstation wird gewartet und kann nicht verwendet werden.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### CWA-ICADOWNLOAD_ERR_00009

- Beschreibung: Das maximale Sitzungslimit wurde erreicht.
- Empfohlene Maßnahme: Das von einem Administrator konfigurierte maximale Sitzungslimit wurde erreicht. Starten Sie die Sitzung neu.

#### CWA-ICADOWNLOAD_ERR_000010

- Beschreibung: Allgemeiner Fehler, der nicht genauer festgelegt werden kann.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### Mac Postlaunch

#### Desktop konnte nicht gestartet werden

- Beschreibung: Der Desktop "Desktopname"konnte nicht gestartet werden. Transaktions-ID - "Transaktions-ID".
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

#### Viewer konnte nicht gestartet werden

- Beschreibung: Der Viewer konnte nicht gestartet werden. Transaktions-ID - "Transaktions-ID".
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

#### Desktop konnte nicht gestartet werden

- Beschreibung: Der Desktop "Desktopname"wird derzeit gewartet. Transaktions-ID - "Transaktions-ID".
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

#### Anwendung konnte nicht gestartet werden

- Beschreibung: "App-Name"konnte nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Anwendung konnte nicht gestartet werden**

- Beschreibung: “App-Name”konnte nicht gestartet werden. Transaktions-ID - “Transaktions-ID” .
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Desktop konnte nicht gestartet werden**

- Beschreibung: Der Desktop “Desktopname”konnte nicht gestartet werden.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Desktop konnte nicht gestartet werden**

- Beschreibung: Der Desktop “Desktopname”konnte nicht gestartet werden. Transaktions-ID - “Transaktions-ID”.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Viewer konnte nicht gestartet werden**

- Beschreibung: Der Viewer konnte “Anwendungsname”nicht öffnen. Transaktions-ID - “Transaktions-ID”.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Viewer konnte nicht gestartet werden**

- Beschreibung: Der Viewer konnte den Desktop “Desktopname”nicht öffnen. Transaktions-ID - “Transaktions-ID”.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Desktop konnte nicht gestartet werden**

- Beschreibung: Der Desktop “Desktopname”wird derzeit gewartet.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Desktop konnte nicht gestartet werden**

- Beschreibung: Der Desktop “Desktopname”wird derzeit gewartet. Transaktions-ID - “Transaktions-ID”.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

**Es kann keine Verbindung zum Desktop hergestellt werden**

- Beschreibung: Der Desktop "Desktopname"kann nicht erreicht werden. Transaktions-ID - "Transaktions-ID". Versuchen Sie es später.
- Empfohlene Maßnahme: Wenn das Problem weiterhin besteht, wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

## Mac Prelaunch

**CWA-ICADOWNLOAD_ERR_00001**

- Beschreibung: Die ICA-Datei ist ungültig.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00002**

- Beschreibung: Timeout der Startanforderung.
- Empfohlene Maßnahme: Überprüfen Sie die Internetverbindung oder wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00003**

- Beschreibung: Der Server hat nicht geantwortet.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00004**

- Beschreibung: Die zu startende Ressource ist entweder nicht vorhanden, nicht aktiviert oder für einen Benutzer nicht sichtbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00005**

- Beschreibung: Server ist nicht erreichbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00006**

- Beschreibung: Fehler beim Starten des Viewers.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00007**

- Beschreibung: Fehler beim Starten eines offenen Apple-Events.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00008**

- Beschreibung: Viewer-Pfad ist nicht erreichbar.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CWA-ICADOWNLOAD_ERR_00009**

- Beschreibung: Authentifizierung wurde vom Benutzer abgebrochen.
- Empfohlene Maßnahme: Bitten Sie den Benutzer, die Ressource neu zu starten.

**CWA-ICADOWNLOAD_ERR_000010**

- Beschreibung: LSI-Fenster wurde vom Benutzer abgebrochen.
- Empfohlene Maßnahme: Bitten Sie den Benutzer, die Ressource neu zu starten.

**CWA-ICADOWNLOAD_ERR_000011**

- Beschreibung: Die angeforderte Arbeitsstation wird gewartet und kann nicht verwendet werden.
- Empfohlene Maßnahme: Bitten Sie den Benutzer, es nach Abschluss der Wartung erneut zu versuchen, wenn die Arbeitsstation verfügbar ist.

**CWA-ICADOWNLOAD_ERR_000012**

- Beschreibung: Die Benutzeranmeldeinformationen müssen geändert werden.
- Empfohlene Maßnahme: Bitten Sie den Benutzer, die Anmeldeinformationen zu ändern.

#### CWA-ICADOWNLOAD_ERR_000013

- Beschreibung: Die mit der Ressource verbundene Sitzung ist nicht mehr aktiv.
- Empfohlene Maßnahme: Bitten Sie den Benutzer, es erneut zu versuchen, oder wenden Sie sich an den technischen Support von Citrix.

#### CWA-ICADOWNLOAD_ERR_000014

- Beschreibung: Fehler beim Download der ICA-Datei.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### Windows Postlaunch

#### SessionManager.Launch.EngineLoadFailed

- Beschreibung: Fehler beim Laden oder ordnungsgemäßen Initialisieren der Kernkomponenten für den Verbindungsaufbau zu einem Remotedesktop oder einer Remoteanwendung. Weitere Details könnten in der Fehlermeldung enthalten sein.
- Empfohlene Maßnahme: Die Citrix Workspace-App funktioniert nicht wie erwartet. Das Problem könnte durch eine Citrix-fremde DLL für den virtuellen Kanal oder eine andere Systemkomponente verursacht werden. Eventuell müssen CDF-Traces erfasst und übermittelt werden, um die Fehlerursache zu ermitteln.

#### SessionManager.Launch.ConnectionFailed

- Beschreibung: Dieser allgemeine Fehler gibt an, dass ein Startversuch fehlgeschlagen ist. Andere gesendete Fehlermeldungen könnten auf eine Ursache hinweisen.
- Empfohlene Maßnahme: Suchen Sie nach anderen Fehlern im Zusammenhang mit dem Startversuch.

#### SessionManager.Launch.LogonFailed

- Beschreibung: Dieser Fehler gibt an, dass eine Verbindung zu einem Remotedesktop oder einer Remoteanwendung hergestellt wurde. Die Sitzung wurde jedoch vor Abschluss der Anmeldung bei Windows (oder einem anderen Betriebssystem) getrennt.
- Empfohlene Maßnahme: Dieser Fehler weist auf einen Anmeldefehler hin. Möglicherweise wurden auch keine Anmeldeinformationen manuell vom Benutzer eingegeben. Untersuchen Sie, wie der Benutzer versucht hat, sich beim Remote-VDA anzumelden.

**SessionManager.Launch.Cancelled**

- Beschreibung: Der Verbindungsversuch der Citrix Engine wurde abgebrochen, wahrscheinlich durch eine Benutzeraktion.
- Empfohlene Maßnahme: Dieser Fehler zeigt an, warum der Verbindungsaufbau fehlgeschlagen ist, er verweist aber wahrscheinlich auf ein korrektes Verhalten.

**SessionManager.LeaseResolution.Failed**

- Beschreibung: Zeigt an, dass ein Offline-Start (auch "leasebasierter Start"genannt) fehlgeschlagen ist. Die Fehlerursache ist, dass eine gültige und erforderliche Lease für die Ressource auf dem Clientcomputer nicht gefunden wurde. Außerdem hat das Gateway oder der Cloud Connector die Startanforderung abgelehnt oder die Startanforderung war ungültig.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die Leases mit dem Clientcomputer synchronisiert wurden und weiterhin gültig sind. Der Benutzer kann sich im Onlinemodus bei Citrix Workspace anmelden, um Leases (erneut) zu synchronisieren. Suchen Sie nach Fehlern, die vom Gateway oder Cloud Connector gesendet wurden. Diese Fehler können einen Hinweis auf die Fehlerursache geben.

**SessionManager.clxmtp.SoftDeny**

- Beschreibung: Client erhält beim Versuch eines Leasestarts die Meldung, dass ein Connector oder Gateway den angeforderten Start nicht abschließen kann. Andere Connectors oder Gateways könnten jedoch beim Start behilflich sein.
- Empfohlene Maßnahme: Dieser Fehler weist nicht auf einen zwangsläufigen Fehlstart hin. Er zeigt an, dass die Engine über einen bestimmten Netzwerkpfad nicht erfolgreich sein kann. Suchen Sie nach Fehlern, die vom Gateway oder Cloud Connector gesendet wurden. Diese Fehler können einen Hinweis auf die Fehlerursache geben.

**SessionManager.clxmtp.SoftDeny_Implicit**

- Beschreibung: Beim Versuch eines Leasestarts war ein Connector oder Gateway nicht erreichbar. Andere Connectors oder Gateways könnten jedoch beim Start behilflich sein.
- Empfohlene Maßnahme: Dieser Fehler weist nicht auf einen zwangsläufigen Fehlstart hin. Er zeigt an, dass die Engine über einen bestimmten Netzwerkpfad nicht erfolgreich sein kann. Untersuchen Sie, warum der Client einen Connector oder Gateway nicht erreicht. Der Host könnte aufgrund der Netzwerktopologie oder wegen Firewalleinschränkungen nicht erreichbar sein.

#### Transport.Connect.NoCGP_Fail

- Beschreibung: Die (Engine)-Kernkomponenten der Citrix Workspace-App konnten sich nicht über das ICA-Protokoll (Port 1494) mit einem VDA-Host verbinden. Ein Verbindungsaufbau mit dem Gateway oder VDA über das CGP-Protokoll wurde nicht versucht, wenn dieses Ereignis gesendet wurde.
- Empfohlene Maßnahme: Untersuchen Sie, warum der Client sich nicht über TCP oder EDT mit einem VDA verbinden kann.

#### Transport.Connect.FallbackFail

- Beschreibung: Die (Engine)-Kernkomponenten der Citrix Workspace-App konnten sich nicht über das ICA-Protokoll (Port 1494) mit einem VDA-Host verbinden. Nach diesem Fehler kann die Citrix Workspace-App sich nicht über das CGP-Protokoll (Port 2598) mit einem Gateway oder VDA verbinden.
- Empfohlene Maßnahme: Untersuchen Sie, warum der Client sich nicht über TCP oder EDT mit einem Gateway, Connector oder VDA verbinden kann.

#### Transport.Connect.Fail

- Beschreibung: Die (Engine)-Kernkomponenten der Citrix Workspace-App konnten sich nicht über das GCP-Protokoll (Port 2598) mit einem Gateway oder VDA verbinden. Ein Verbindungsaufbau mit dem VDA über das ICA-Protokoll wurde nicht versucht, wenn dieses Ereignis gesendet wurde.
- Empfohlene Maßnahme: Untersuchen Sie, warum der Client sich nicht über TCP oder EDT mit einem Gateway, Connector oder VDA verbinden kann.

### Windows Prelaunch

#### CWA-ICADOWNLOAD_ERR_00001

- Beschreibung: Verbindung zum Store nicht möglich, da keine Antwort von der Citrix Workspace-App empfangen wurde.
- Empfohlene Maßnahme: Überprüfen Sie, ob Citrix Workspace oder StoreFront ausgefallen sind. Überprüfen Sie außerdem die Internetverbindung.

#### CWA-ICADOWNLOAD_ERR_00002

- Beschreibung: Sitzungsstart wurde vom Benutzer abgebrochen.

- Empfohlene Maßnahme: Starten Sie die Sitzung nach einiger Zeit neu.

**CWA-ICADOWNLOAD_ERR_00003**

- Beschreibung: Verbindung zum Store nicht möglich. Stellen Sie sicher, dass die Serverzertifikate gültig sind.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

**CWA-ICADOWNLOAD_ERR_00004**

- Beschreibung: Die zu startende Ressource ist nicht vorhanden, nicht aktiviert oder für einen Benutzer nicht sichtbar.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

**CWA-ICADOWNLOAD_ERR_00005**

- Beschreibung: Arbeitsstationen sind für diese Anforderung nicht verfügbar.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

**CWA-ICADOWNLOAD_ERR_00006**

- Beschreibung: Server besitzt nicht die erforderliche Lizenz zum Ausführen der angeforderten Aktivität.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

**CWA-ICADOWNLOAD_ERR_00007**

- Beschreibung: Server hat die Verbindung zur Arbeitsstation verweigert.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

**CWA-ICADOWNLOAD_ERR_00008**

- Beschreibung: Die angeforderte Arbeitsstation wird gewartet und kann nicht verwendet werden.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

#### CWA-ICADOWNLOAD_ERR_00009

- Beschreibung: Das maximale Sitzungslimit wurde erreicht.
- Empfohlene Maßnahme: Das von einem Administrator konfigurierte maximale Sitzungslimit wurde erreicht. Starten Sie die Sitzung neu.

#### CWA-ICADOWNLOAD_ERR_000010

- Beschreibung: Allgemeiner Fehler, der nicht genauer festgelegt werden kann.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren IT-Administrator.

### Workspace

#### StoreLaunchIcaEndpoint.LaunchFailed

- Beschreibung: Beim Start ist ein Fehler aufgetreten.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

#### StoreLaunchSessionEndpoint.BadRequest

- Beschreibung: Die Parameter der Startanforderung waren ungültig oder leer.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### StoreLaunchSessionEndpoint.FarmUnavailable

- Beschreibung: Für den Start waren keine Farmen verfügbar.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle.

#### StoreLaunchSessionEndpoint.Error

- Beschreibung: Beim Start ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### StoreGetIcaFileEndpoint.BadRequest

- Beschreibung: In der Anforderung wurde kein Startticket bereitgestellt.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed**

- Beschreibung: Workspace konnte die ICA-Datei nicht abrufen.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**StoreGetIcaFileEndpoint.Error**

- Beschreibung: Workspace konnte die ICA-Datei nicht abrufen.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**WebProxyGetLaunchStatusEndPoint.DSAuthFailure**

- Beschreibung: Es ist ein Authentifizierungsproblem aufgetreten.
- Empfohlene Maßnahme: Versuchen Sie, sich erneut zu authentifizieren. Wenden Sie sich an den Citrix Support.

**WebProxyGetLaunchStatusEndPoint.LaunchFailed**

- Beschreibung: Beim Start der Anwendung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**WebProxyGetLaunchStatusEndPoint.ResourceNotFound**

- Beschreibung: Der Start ist fehlgeschlagen, da die Anwendung nicht gefunden wurde.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle und die Anwendungskonfiguration.

**WebProxyLaunchIcaEndpoint.DSAuthFailure**

- Beschreibung: Es ist ein Authentifizierungsproblem aufgetreten.
- Empfohlene Maßnahme: Versuchen Sie, sich erneut zu authentifizieren. Wenden Sie sich an den Citrix Support.

**WebProxyLaunchIcaEndpoint.LaunchFailed**

- Beschreibung: Beim Start der Anwendung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**WebProxyLaunchIcaEndpoint.ResourceNotFound**

- Beschreibung: Der Start ist fehlgeschlagen, da die Anwendung nicht gefunden wurde.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle und die Anwendungskonfiguration.

**WebProxySessionsLaunchIcaEndpoint.SessionNotFound**

- Beschreibung: Workspace konnte die Verbindung mit der vorhandenen HDX-Sitzung nicht wiederherstellen. Ihre Sitzung wurde möglicherweise beendet.
- Empfohlene Maßnahme: Starten Sie die Anwendung neu.

**WebProxySessionsLaunchIcaEndpoint.DSAuthFailure**

- Beschreibung: Es ist ein Authentifizierungsproblem aufgetreten.
- Empfohlene Maßnahme: Versuchen Sie, sich erneut zu authentifizieren. Wenden Sie sich an den Citrix Support.

**WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed**

- Beschreibung: Workspace konnte die Verbindung mit der vorhandenen HDX-Sitzung nicht wiederherstellen. Ihre Sitzung wurde möglicherweise beendet.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**WebProxySessionsLaunchIcaEndpoint.Error**

- Beschreibung: Beim Wiederverbinden mit der Anwendung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure**

- Beschreibung: Es ist ein Authentifizierungsproblem aufgetreten.
- Empfohlene Maßnahme: Versuchen Sie, sich erneut zu authentifizieren. Wenden Sie sich an den Citrix Support.

**WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed**

- Beschreibung: Workspace konnte die Verbindung mit der HDX-Sitzung nicht wiederherstellen.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**WebProxySessionsGetLaunchStatusEndpoint.Error**

- Beschreibung: Beim Wiederverbinden mit der Anwendung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**DetermineGateway.Error**

- Beschreibung: Workspace konnte nicht ermitteln, mit welchem Gateway eine Verbindung hergestellt werden soll.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Gateway-Konfiguration. Wenden Sie sich an den Citrix Support.

**ConnectionRoutingProviderLaunch.Error**

- Beschreibung: Workspace konnte nicht ermitteln, mit welchem Gateway eine Verbindung hergestellt werden soll.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Gateway-Konfiguration. Wenden Sie sich an den Citrix Support.

**BrokerGetAddressCall.AnonymousPrelaunchNotSupported**

- Beschreibung: Workspace kann die Anwendung nicht starten, da die Farm keine anonymen Starts unterstützt.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**BrokerGetAddressCall.LeasingError**

- Beschreibung: Workspace hat einen Fehler vom Citrix Virtual Apps and Desktops-Broker erhalten.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**BrokerGetAddressCall.ServiceConnectionError**

- Beschreibung: Workspace konnte keinen Kontakt zu einem Citrix Virtual Apps and Desktops-Broker in der Farm herstellen.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**BrokerGetAddressCall.BrokerError**

- Beschreibung: Workspace hat eine Fehlermeldung von einem Citrix Virtual Apps and Desktops-Broker erhalten.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**BrokerGetAddressCall.LicensingError**

- Beschreibung: Workspace konnte die Anwendung aufgrund eines Lizenzfehlers nicht starten.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**BrokerGetAddressCall.Error**

- Beschreibung: Workspace kann keine VDA-Details vom Citrix Virtual Apps and Desktops-Broker abrufen.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**GetLaunchReference.NoAccessToken**

- Beschreibung: Workspace kann keine Verbindung zum VDA herstellen.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**GetLaunchReference.BrokerError**

- Beschreibung: Workspace kann keine Verbindung zum VDA herstellen.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**GetLaunchReference.Error**

- Beschreibung: Workspace kann keine Verbindung zum VDA herstellen.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**GenerateIcaFile.InvalidIcaSetting**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**StoreIcaFileAndGetTicket.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetFasVdaLogonTicket.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GenerateSTATicket.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetVdaAddress.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetTicket.NoAccessToken**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetTicket.BrokerError**

- Beschreibung: Der Citrix Virtual Apps and Desktops-Broker konnte die HDX-Sitzung nicht starten.
- Empfohlene Maßnahme: Prüfen Sie die ID in der Fehlermeldung und überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle.

**GetTicket.ServiceConnectionError**

- Beschreibung: Workspace kann keinen Kontakt zu einem Citrix Virtual Apps and Desktops-Broker herstellen.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetTicket.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetNetscalerConfigurationByCustomer.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**DiscoverMPSServerCapabilities.Error**

- Beschreibung: Beim Senden einer Anforderung an den Citrix Virtual Apps and Desktops-Broker ist ein Problem aufgetreten.
- Empfohlene Maßnahme: Überprüfen Sie Ihre Citrix Virtual Apps and Desktops-Protokolle. Wenden Sie sich an den Citrix Support.

**GetResourceLocationNetScalerConfig.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**GetCustomerResourceLocations.Error**

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### GetResourceLocationFromResourceProvider.Error

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### GetNetScalerGatewayInfo.Error

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### GetCustomerEntitlements.Error

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### GetResourceLocationForServerFeed.Error

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### GetResourceInformation.Error

- Beschreibung: Beim Herstellen einer HDX-Verbindung ist ein interner Fehler aufgetreten.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

### Citrix Gateway as a Service

#### CGS-ICASN_ERR_00001

- Beschreibung: Der Anwendungsstart ist aufgrund eines Fehlers beim Parsen der Anforderung fehlgeschlagen.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### CGS-ICASN_ERR_00002

- Beschreibung: Fehler beim Validieren eines Authentifizierungstickets.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS-ICASN_ERR_00003**

- Beschreibung: Fehler beim Validieren eines Authentifizierungstickets.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS-ICASN_ERR_00004**

- Beschreibung: Fehler beim Validieren eines Authentifizierungstickets.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS-ICASN_ERR_00005**

- Beschreibung: Verbindung zum Connector konnte nicht hergestellt werden.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00006**

- Beschreibung: Timeout bei Verbindungsanforderung an den Connector.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Prüfen Sie, ob der Datenverkehr zwischen Connector/VDA und NGS durch Proxy-Einstellungen blockiert wird. Überprüfen Sie die Konnektivität zwischen VDA und Connector. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00007**

- Beschreibung: Die Citrix Workspace-App hat die Verbindung getrennt.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die clientseitige Netzwerkkonnektivität stabil ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00008**

- Beschreibung: Das Back-End hat die Verbindung getrennt.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Überprüfen Sie die Netzwerkstabilität vom Connector/VDA zum öffentlichen Netzwerk (NGS). Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00009**

- Beschreibung: Fehler beim Verbindungsaufbau zwischen VDA und NGS (Rendezvous).
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Der VDA muss den Netscaler Gateway Service (NGS) erreichen können. Überprüfen Sie die Konnektivität zwischen VDA und Connector. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00010**

- Beschreibung: Fallback von EDT auf TCP. Überprüfen Sie die Voraussetzung für EDT.
- Empfohlene Maßnahme: Rendezvous muss aktiviert sein und der VDA muss den NetScaler Gateway Service (NGS) über UDP erreichen können. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00011**

- Beschreibung: Fehler im internen NetScaler Gateway Service (NGS).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00012**

- Beschreibung: Fehler im internen NetScaler Gateway Service (NGS).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00013**

- Beschreibung: Fehler bei der GCT-Validierung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00014**

- Beschreibung: Fehler bei der GCT-Validierung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00015**

- Beschreibung: Fehler im internen NetScaler Gateway Service (NGS).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00016**

- Beschreibung: Fehler im internen NetScaler Gateway Service (NGS).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00017**

- Beschreibung: Fehler im internen NetScaler Gateway Service (NGS).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00018**

- Beschreibung: Fehler beim Validieren eines Authentifizierungstickets.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00019**

- Beschreibung: Fehler beim Validieren eines Authentifizierungstickets.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00020**

- Beschreibung: Fehler bei der internen CGS-Lizenzierung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00021**

- Beschreibung: Rendezvous v2-Fallback aufgrund eines deaktivierten Feature-Flag.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00022**

- Beschreibung: Fehler im internen NetScaler Gateway Service (NGS).
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00023**

- Beschreibung: Timeout bei CLXMTP-Austausch.
- Empfohlene Maßnahme: Stellen Sie sicher, dass die Connectors funktionsfähig sind und vom NetScaler Gateway Service (NGS) erreicht werden können. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00024**

- Beschreibung: Fehler bei der CLXMTP-VSR-Validierung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00025**

- Beschreibung: Fehler bei der CLXMTP-VSR-Validierung.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00026**

- Beschreibung: Der Connector ist nicht in CLXMTP verfügbar.
- Empfohlene Maßnahme: Überprüfen Sie, ob der Connector funktionsfähig für den Ressourcenstandort ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00027**

- Beschreibung: Die CLXMTP-Umleitung zum Connector ist nach Erreichen der Höchstanzahl von Versuchen fehlgeschlagen.
- Empfohlene Maßnahme: Überprüfen Sie, ob der Connector funktionsfähig für den Ressourcenstandort ist. Stellen Sie sicher, dass der Dienst `Citrix ClxMtp Service` in allen Connectors ausgeführt wird. Wenden Sie sich an den Citrix Support.

**CGS_ICASN_ERR_00028**

- Beschreibung: Fehler bei der Kommunikation mit dem Controller.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

#### Erfolg: CGS_ICASN_SUCCESS_00001

- Beschreibung: Sitzungsstartanforderung wurde empfangen.
- Empfohlene Maßnahme: Nicht zutreffend

#### Erfolg: CGS_ICASN_SUCCESS_00002

- Beschreibung: Sitzungsstartanforderung wurde abgeschlossen.
- Empfohlene Maßnahme: Nicht zutreffend

### XAXD-Proxy

#### XDPXY_INF_00001

- Beschreibung: Broker fordert den VDA auf, sich auf eingehende Verbindungen vorzubereiten.
- Empfohlene Maßnahme: Nicht zutreffend

#### XDPXY_INF_00002

- Beschreibung: VDA bestätigt Verbindungsanforderung durch Broker.
- Empfohlene Maßnahme: Nicht zutreffend

#### XDPXY_ERR_00001

- Beschreibung: Fehler bei der Kommunikation mit dem VDA.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

#### XDPXY_ERR_00002

- Beschreibung: Ein Timeout ist aufgetreten, während XaxdProxy auf eine Antwort vom VDA wartete.

- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**XDPXY_ERR_00003**

- Beschreibung: Beim Versuch, eine Anforderung zu stellen, ist ein WCF-Fehler oder eine WCF-Ausnahme aufgetreten.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**XDPXY_INF_00003**

- Beschreibung: Die Anforderung zur Validierung einer eingehenden ICA- oder RDP-Verbindung wird vom Stapel aufgerufen.
- Empfohlene Maßnahme: Nicht zutreffend

**XDPXY_INF_00004**

- Beschreibung: Die Validierung der eingehenden ICA- oder RDP-Verbindung wurde hergestellt.
- Empfohlene Maßnahme: Nicht zutreffend

**XDPXY_ERR_00001**

- Beschreibung: Fehler bei der Kommunikation mit dem VDA-Proxy.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.

  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

#### XDPXY_ERR_00002

- Beschreibung: Ein Timeout ist aufgetreten, während XaxdProxy auf eine Antwort vom VDA-Proxy wartete.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

#### XDPXY_ERR_00003

- Beschreibung: Beim Versuch, eine Anforderung zu stellen, ist eine Ausnahme aufgetreten.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Starten Sie den Citrix Delivery Agent Service auf dem VDA neu oder starten Sie den VDA neu.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

#### XDPXY_INF_00005

- Beschreibung: Direkte Verbindung zwischen HDX-Sitzungsverkehr und VDA angefordert.
- Empfohlene Maßnahme: Nicht zutreffend

#### XDPXY_INF_00006

- Beschreibung: Der VDA stellt eine direkte Verbindung mit der Citrix Cloud-Steuerungsebene für den HDX-Sitzungsverkehr her.
- Empfohlene Maßnahme: Nicht zutreffend

**XDPXY_INF_00007**

- Beschreibung: Der Client sendet eine Verbindungsanforderung für eine Ressource an das On-Premises-StoreFront.
- Empfohlene Maßnahme: Nicht zutreffend

**XDPXY_INF_00008**

- Beschreibung: On-Premises-StoreFront akzeptiert Verbindungsanforderung vom Client für die Ressource.
- Empfohlene Maßnahme: Nicht zutreffend

**XDPXY_ERR_00004**

- Beschreibung: XaxdProxy hat beim versuchten Verbindungsaufbau eine HTTP-Fehlermeldung erhalten.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Überprüfen Sie die Netzwerkstabilität vom Connector zum öffentlichen Netzwerk.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**XDPXY_ERR_00006**

- Beschreibung: Die XML-Anforderung hat ein ungültiges Format.
- Empfohlene Maßnahme: Wenden Sie sich an den Citrix Support.

**XDPXY_ERR_00007**

- Beschreibung: Header und/oder Format der Anmeldeinformationen in der XML-Anforderung sind ungültig.
- Empfohlene Maßnahme: Melden Sie sich ab und erneut an und wiederholen Sie die Aktion. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

**XDPXY_INF_00011**

- Beschreibung: Der Start der Servicekontinuität wird vom Benutzer über WSA angefordert.
- Empfohlene Maßnahme: Nicht zutreffend

#### XDPXY_INF_00012

- Beschreibung: Der Start der Servicekontinuität wird vom Benutzer über WSA angefordert.
- Empfohlene Maßnahme: Nicht zutreffend

#### XDPXY_ERR_00004

- Beschreibung: Beim Verbindungsaufbau durch XaxdProxy ist ein HTTP-Fehler aufgetreten.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

#### XDPXY_ERR_00008

- Beschreibung: Fehler beim Start der Servicekontinuität aufgrund eines Timeouts, während XaxdProxy auf eine Antwort wartete.
- Empfohlene Maßnahme: Überprüfen Sie die Integrität des Connectors. Weitere Informationen finden Sie unter Citrix Cloud Connector und CTX224133.
  - Bei Verwendung eines Webproxys zwischen Connector und Broker muss dieser ordnungsgemäß konfiguriert sein.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

#### XDPXY_ERR_00009

- Beschreibung: Fehler beim Start der Servicekontinuität, da die Lease blockiert und/oder widerrufen wurde.
- Empfohlene Maßnahme: Wenden Sie sich mit den Fehlerdetails an Ihren Citrix Cloud-Administrator. Weitere Informationen finden Sie in der Dokumentation zur Servicekontinuität.
  - Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

## Citrix DaaS für Citrix Service Provider

February 14, 2024

In diesem Artikel wird beschrieben, wie **Citrix Service Provider (CSP)** Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) für Mandantenkunden in Citrix Cloud einrichten können. Eine Übersicht über die für Citrix Partner verfügbaren Features finden Sie unter Citrix Cloud for Partners.

## Anforderungen

- Sie sind Citrix Service Provider.
- Sie haben ein Citrix Cloud-Konto.
- Sie verfügen über ein Citrix DaaS-Abonnement.

## Einschränkungen und bekannte Probleme

### Einschränkungen

- Die Anwendung der Änderung eines Mandantennamens über alle Schnittstellen hinweg benötigt bis zu 24 Stunden.
- Beim Erstellen eines Mandanten muss die E-Mail-Adresse eindeutig sein.
- Die Filterung in **Verwalten > Vollständige Konfiguration** nach Geltungsbereich (ähnlich wie bei Überwachen) ist nicht verfügbar. Um die Ressourcen anzuzeigen, die einem Bereich zugeordnet sind, wählen Sie im linken Bereich die Option **Administratoren**. Wählen Sie den Geltungsbereich auf der Registerkarte **Geltungsbereiche** und wählen Sie **Geltungsbereich bearbeiten** im Aktionsbereich.

### Bekannte Probleme

- Wenn Bereiche einer Ressource zugewiesen wurden, können Sie diese nicht über die Verwaltungskonsole entfernen oder die Zuweisung aufheben. Diese Aufgaben sind nur über PowerShell möglich.
- **Verwalten > Vollständige Konfiguration** erzwingt keine Geltungsbereiche. Beim Erstellen von Maschinenkatalogen, Bereitstellungsgruppen und Anwendungsgruppen sind Sie für die Auswahl des richtigen Bereichs verantwortlich.
- Wenn mehr als 15 Bereiche erstellt wurden (automatisch oder benutzerdefiniert), werden die benutzerdefinierten Citrix Cloud-Zugriffsinformationen für einen Administrator (**Identitäts- und Zugriffsverwaltung > Administratoren**) nicht richtig angezeigt. Problemumgehung: Begrenzen Sie die Zahl der Bereiche auf maximal 15.

### Kunden hinzufügen

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Wählen Sie **Kunden** im Menü links oben.
2. Wählen Sie im Kundendashboard **Einladen oder hinzufügen**. Geben Sie die angeforderten Informationen an.
3. Wenn der Kunde kein Citrix Cloud-Konto hat, wird durch das Hinzufügen des Kunden eines erstellt. Wenn Sie den Kunden hinzufügen, werden Sie außerdem automatisch als Administrator mit Vollzugriff für das Konto dieses Kunden hinzugefügt.
4. Wenn der Kunde ein Citrix Cloud-Konto hat:

    a) wird eine Citrix Cloud-URL angezeigt, die Sie kopieren und an den Kunden senden. Einzelheiten zu diesem Vorgang finden Sie unter Senden einer Verbindungseinladung an einen Kunden.

    b) muss der Kunde Sie als Administrator mit Vollzugriff zu seinem Konto hinzufügen. Siehe Hinzufügen von Administratoren zu einem Citrix Cloud-Konto.

Sie können später über die Konsolen **Verwalten** und **Überwachen** weitere Administratoren hinzufügen und steuern, welche Kunden diesen Administratoren angezeigt werden.

### Hinzufügen von Citrix DaaS zu einem Kunden

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Wählen Sie **Kunden** im Menü links oben.
2. Wählen Sie im Kundendashboard im Menü mit den Auslassungspunkten für den Kunden die Option **Service hinzufügen**.
3. Wählen Sie unter **Service zum Hinzufügen auswählen** die Option **Virtual Apps and Desktops**.
4. Wählen Sie **Weiter**.

Wenn Sie dieses Verfahren abgeschlossen haben, wird der Kunde in Ihr Citrix DaaS-Abonnement aufgenommen.

Nach dem Onboarding wird automatisch ein neuer Kundenbereich in Citrix DaaS erstellt. Der Geltungsbereich ist in der Anzeige **Verwalten > Vollständige Konfiguration** sichtbar. Der Bereich gilt nur für diesen Kunden. Sie können den Bereich umbenennen, ihn jedoch nicht löschen.

Verwenden Sie diesen Bereich, um den Zugriff für andere Administratoren einzurichten. Beispiel: Sie haben zehn Kunden und zwei Administratoren. Mit einem eindeutigen Geltungsbereich können Sie den Zugriff eines Administrators auf nur drei dieser Kunden beschränken. Der andere Administrator erhält Zugriff auf einen dieser drei Kunden und auf zwei weitere Kunden. Einzelheiten finden Sie unter Steuern des Administratorzugriffs auf Kunden.

### Ressourcenstandort einrichten

Ein Ressourcenstandort enthält die Maschinen, die Apps und Desktops für Ihre Kunden bereitstellen, und Infrastrukturkomponenten wie Citrix Cloud Connectors. Einzelheiten finden Sie unter Herstellen einer Verbindung mit Citrix Cloud.

### Einrichten von Katalogen und Gruppen zum Bereitstellen von Apps und Desktops

> **Hinweis:**
>
> Um DaaS für einen Mandantenkunden zu verwalten, müssen Sie zum Konto des CSP-Kunden wechseln. Klicken Sie dazu im Menü oben rechts auf den Kundennamen und dann auf **Kunde ändern**.

Ein Katalog ist eine Gruppe identischer virtueller Maschinen. Wenn Sie einen Katalog erstellen, wird ein Image (mit anderen Einstellungen) als Vorlage zum Erstellen der Maschinen verwendet. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Die Bereitstellungsgruppe gibt an, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops für diese Benutzer verfügbar sein sollen. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.

Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden. Weitere Informationen finden Sie unter Anwendungsgruppen erstellen.

Achten Sie beim Konfigurieren von Gruppen auf Folgendes:

- Der Bereich der Bereitstellungsgruppe ist eine Teilmenge des Bereichs des Maschinenkatalogs. Angenommen, der Bereich des Katalogs ist A und B. Der Bereich der Bereitstellungsgruppe kann entweder A oder B oder A und B sein.
- Der Bereich der Anwendungsgruppe ist eine Teilmenge des Bereichs der Bereitstellungsgruppe. Angenommen, die einer Anwendungsgruppe zugeordneten Bereitstellungsgruppen haben den Bereich A und B. Der Bereich der Anwendungsgruppe kann entweder A oder B oder A und B sein.

### Verbunddomänen

Mithilfe von Verbunddomänen können sich die Benutzer des Kunden mit Anmeldeinformationen aus einer mit Ihrem Ressourcenstandort verknüpften Domäne bei ihrem Workspace anmelden. So können Sie Ihren Kunden dedizierte Arbeitsbereiche bereitstellen, auf die deren Benutzer mithilfe einer benutzerdefinierten Workspace-URL (z. B. customer.cloud.com) zugreifen können, während

sich der Ressourcenstandort weiterhin in Ihrem Citrix Cloud-Konto befindet. Sie können dedizierte Workspaces neben dem gemeinsam genutzten Workspace bereitstellen, auf den die Kunden über Ihre CSP-Workspace-URL zugreifen (z. B. csppartner.cloud.com).

Damit Kunden auf ihren dedizierten Workspace zugreifen können, fügen Sie sie den entsprechenden, von Ihnen verwalteten Domänen hinzu. Nachdem Sie den Workspace gemäß den Anweisungen unter Workspacekonfiguration konfiguriert haben, können sich die Benutzer des Kunden bei ihrem Workspace anmelden und auf die Apps und Desktops zugreifen, die Sie zur Verfügung gestellt haben.

#### Hinzufügen eines Kunden zu einer Domäne

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Wählen Sie **Kunden** im Menü links oben.
2. Wählen Sie im Kundendashboard im Menü links oben die Option **Identitäts- und Zugriffsverwaltung**.
3. Wählen Sie auf der Registerkarte **Domänen** im Menü der Domäne die Option **Verbunddomäne verwalten**.
4. Wählen Sie auf der Registerkarte **Verbunddomäne verwalten** in der Spalte **Verfügbare Kunden** den Kunden aus, den Sie der Domäne hinzufügen möchten. Wählen Sie das Pluszeichen neben dem Kundennamen. Der ausgewählte Kunde wird nun in der Spalte **Verbundkunden** angezeigt. Wiederholen Sie die Schritte, um weitere Kunden hinzuzufügen. Wenn Sie fertig sind, wählen Sie **Übernehmen**.

#### Entfernen eines Kunden aus einer Domäne

Wenn Sie einen Kunden aus einer von Ihnen verwalteten Domäne entfernen, können die Benutzer des Kunden nicht mehr mit Anmeldeinformationen aus Ihrer Domäne auf ihre Workspaces zugreifen.

1. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** und dann **Domänen**.
2. Suchen Sie die Domäne, die Sie verwalten möchten, und wählen Sie das Dreipunktmenü (…). Wählen Sie **Verbunddomäne verwalten**.
3. Suchen Sie in der Liste der Verbundkunden die Kunden, die Sie entfernen möchten, und wählen Sie das X. Wählen Sie **Alle entfernen**, um alle Kunden in der Liste aus der Domäne zu entfernen. Die ausgewählten Kunden werden in die Liste der verfügbaren Kunden verschoben.
4. Wählen Sie **Übernehmen**.
5. Überprüfen Sie die ausgewählten Kunden und wählen Sie **Kunden entfernen**.

## Steuern des Administratorzugriffs auf Kunden

Sie können den Administratorzugriff auf Kunden über den eindeutigen Bereich steuern, der beim Hinzufügen von Citrix DaaS zu dem Kunden erstellt wurde. Sie können den Zugriff beim Hinzufügen eines Administrators konfigurieren oder später.

Informationen zum Einschränken des Zugriffs mithilfe von Rollen und Bereichen in Citrix DaaS finden Sie unter Delegierte Administration.

### Hinzufügen eines Administrators mit eingeschränktem Zugriff

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Wählen Sie **Kunden** im Menü links oben.
2. Wählen Sie im Kundendashboard im Menü links oben die Option **Identitäts- und Zugriffsverwaltung**.
3. Wählen Sie auf der Registerkarte **Administratoren** zuerst **Administratoren hinzufügen von** und dann **Citrix-Identität**.
4. Geben Sie die E-Mail-Adresse der Person ein, die Sie als Administrator hinzufügen, und wählen Sie **Einladen**.
5. Konfigurieren Sie die Zugriffsberechtigungen für den Administrator. Citrix empfiehlt die Auswahl von **Benutzerdefinierter Zugriff**, es sei denn, der Administrator soll Citrix Cloud und alle abonnierte Services verwalten können.
6. Nach Auswahl von **Benutzerdefinierter Zugriff** wählen Sie nach Bedarf die Rollen-/Bereichspaare für Citrix DaaS aus. Achten Sie darauf, nur Einträge zu aktivieren, die den eindeutigen, für den Kunden erstellten Bereich enthalten.
7. Nach der Auswahl aller Rollen-/Bereichspaare wählen Sie **Einladung senden**.

Wenn der Administrator die Einladung annimmt, hat er den von Ihnen zugewiesenen Zugriff.

### Bearbeiten der Berechtigungen zur delegierten Administration für Administratoren

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Wählen Sie **Kunden** im Menü links oben.
2. Wählen Sie im Kundendashboard im Menü links oben die Option **Identitäts- und Zugriffsverwaltung**.
3. Wählen Sie auf der Registerkarte **Administratoren** im Menü für den Administrator die Option **Zugriff bearbeiten**.
4. Wählen Sie nach Bedarf die Rollen-/Bereichspaare für Citrix DaaS aus, bzw. heben Sie Zuweisungen auf. Achten Sie darauf, nur Einträge zu aktivieren, die den eindeutigen, für den Kunden erstellten Bereich enthalten.
5. Wählen Sie **Speichern**.

**Anzeigen von Kundenadministratoren und deren zugewiesenen Rollen und Bereichen**

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Wählen Sie **Kunden** im Menü links oben.
2. Wählen Sie im Kundendashboard im Menü links oben **Eigene Services > Citrix DaaS**.
3. Wählen Sie in Citrix DaaS **Verwalten > Vollständige Konfiguration**.
4. Wählen Sie im linken Bereich **Administratoren**.

Informationen stehen über drei Registerkarten zur Verfügung:

- Auf der Registerkarte **Administratoren** werden die erstellten Administratoren sowie deren Rollen und Bereiche aufgeführt.
- Auf der Registerkarte **Rollen** werden alle Rollen aufgelistet. Zum Anzeigen von Rollendetails wählen Sie die Rolle im mittleren Bereich aus. Im unteren Teil werden die Objekttypen und die zugehörigen Berechtigungen für die Rolle angezeigt. Klicken Sie auf die Registerkarte **Administratoren** im unteren Bereich, um eine Liste der Administratoren anzuzeigen, die derzeit diese Rolle haben.
- Auf der Registerkarte **Bereiche** werden alle Bereiche aufgelistet, einschließlich derer, die für Kunden von Citrix Partnern erstellt wurden.

## Workspace konfigurieren

Kunden haben einen eigenen Workspace mit einer eindeutigen `customer.cloud.com`-URL. Hier greifen die Benutzer der Kunden auf ihre veröffentlichten Apps und Desktops zu.

Die Workspace-URL wird an zwei Stellen angezeigt:

- Klicken Sie im Kundendashboard im Menü links oben auf **Workspacekonfiguration**.
- Auf dem **Begrüßungsbildschirm** von Citrix DaaS wird am unteren Seitenrand der Registerkarte **Übersicht** die Workspace-URL angezeigt.

Sie können Zugriff und Authentifizierung für Workspaces ändern. Sie können außerdem das Aussehen und die Voreinstellungen von Workspaces anpassen. Weitere Informationen finden Sie in den folgenden Artikeln:

- Workspace konfigurieren
- Sichere Workspaces

## Überwachung des Service für einen Kunden

Das Dashboard **Überwachen** in einer CSP-Umgebung entspricht im Wesentlichen dem in anderen Umgebungen. Einzelheiten finden Sie unter Überwachen.

Standardmäßig zeigt das Dashboard **Überwachen** Informationen über alle Kunden an. Um Informationen zu einem Kunden anzuzeigen, wählen Sie **Kunden auswählen**.

Bedenken Sie, dass die Anzeige der Überwachung für einen Kunden über die Zugriffskonfiguration des Administrators bestimmt wird. Der Zugriff muss ein Rollen-/Bereichspaar enthalten, das den eindeutigen Bereich des Kunden enthält.

Wenn Sie integrierte Rollen zum Konfigurieren des Zugriffs verwendet haben, bestimmen diese, ob ein Administrator die Registerkarten **Verwalten** und **Überwachen** sehen kann. Wenn Sie nur Rollen-/Kundenbereichspaare auswählen, die keine Anzeige der Registerkarte **Überwachen** enthalten, wird für den Administrator die Registerkarte **Überwachen** für keinen ausgewählten Kunden angezeigt. Wenn Sie beispielsweise einem Administrator **Lesezugriffadministrator, Kunde ABC** zuweisen, kann der Administrator die Registerkarte **Überwachen** für den Kunden ABC nicht sehen, da Lesezugriffadministratoren keinen Zugriff auf die Überwachungsanzeigen haben.

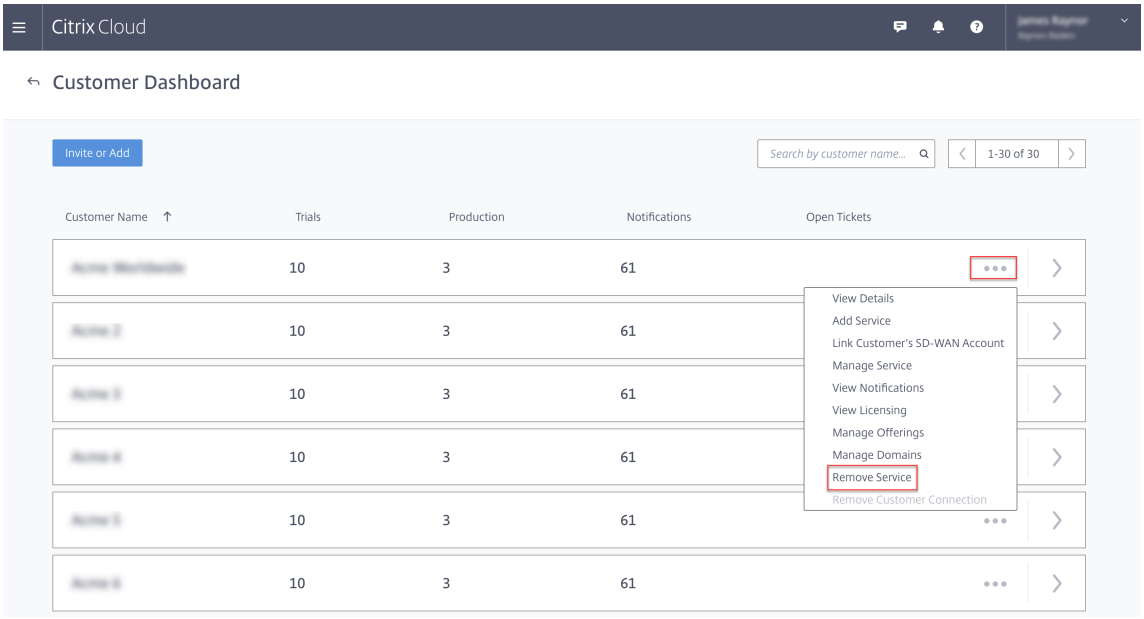
## Entfernen von Diensten

### Voraussetzungen

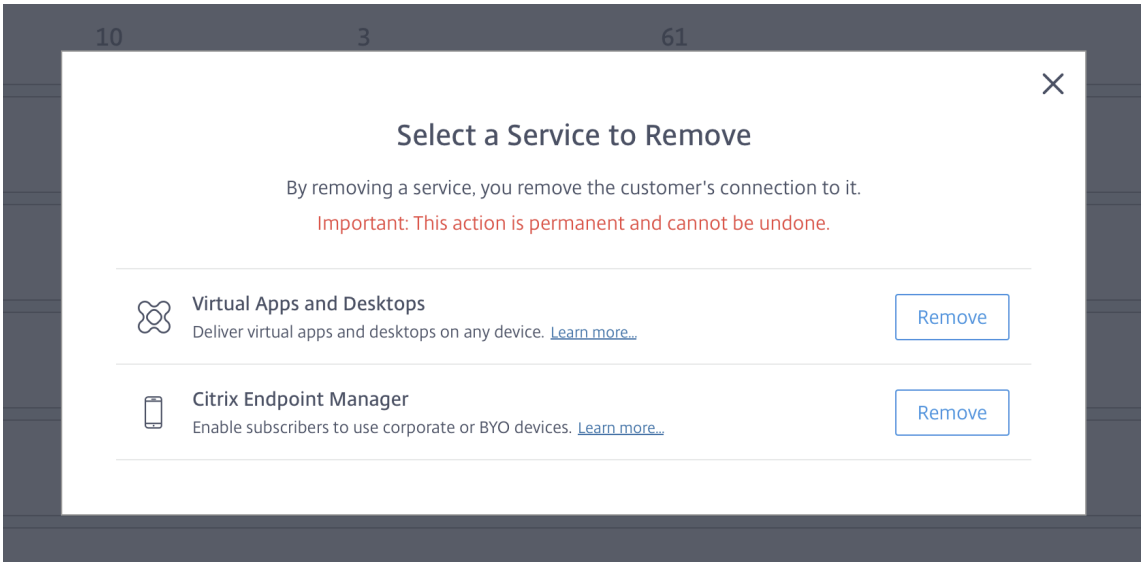
- Stellen Sie sicher, dass Ihr Kundenbereich nicht mit Citrix DaaS-Objekten verknüpft ist. Wenn eine Verknüpfung vorliegt, können Sie den Dienst nicht entfernen. Um die Verknüpfung von Bereichen aufzuheben, gehen Sie zu **Citrix Studio > Administratoren > Geltungsbereiche** und bearbeiten Sie den Bereich.
- Informationen zum Kundenbereich und seiner Verwaltung finden Sie unter Erstellen und Verwalten von Geltungsbereichen.

1. Melden Sie sich bei Citrix Cloud mit den Anmeldeinformationen für Ihren Citrix Service Provider an.
2. Klicken Sie im **Kundendashboard** auf das **Dreipunktmenü** (…) des Kunden, für den Sie einen Dienst entfernen möchten, und wählen Sie **Dienst entfernen**.

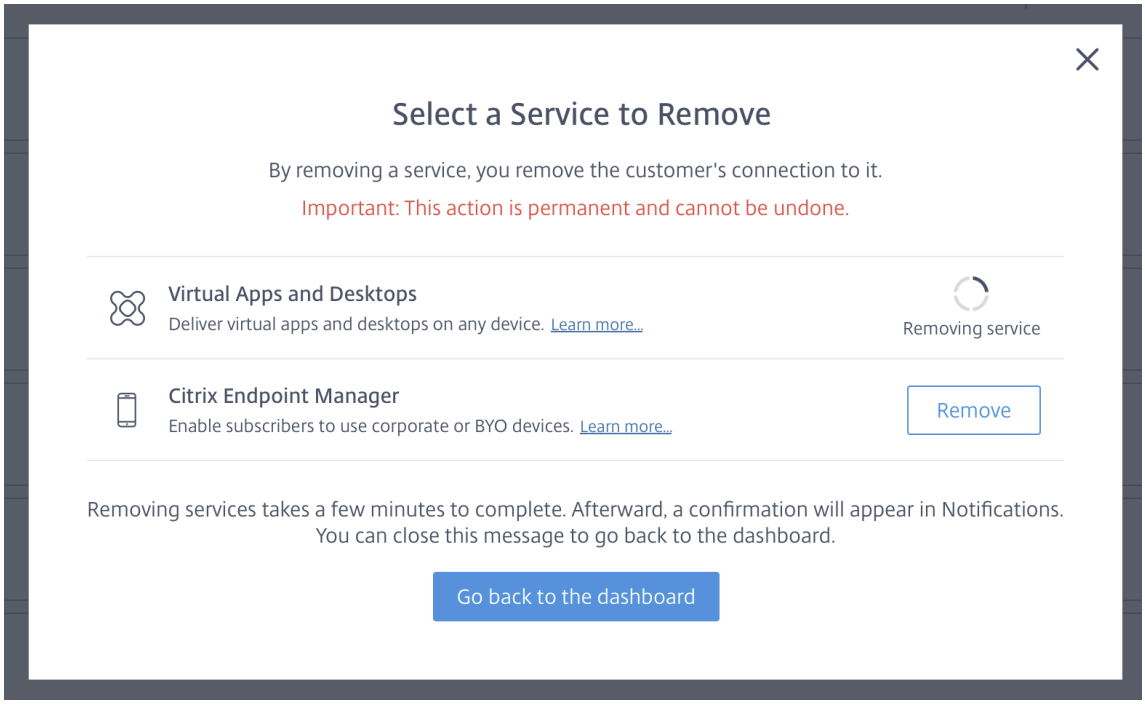



Die Seite **Dienst zum Entfernen auswählen** wird angezeigt.




3. Klicken Sie auf **Entfernen**, um den Dienst zu entfernen.




## Citrix Gateway Service

November 9, 2022

Citrix Gateway bietet Benutzern einen sicheren Zugriff auf Citrix DaaS-Anwendungen (ehemals Citrix Virtual Apps and Desktops Service).

Der Citrix Gateway-Service ermöglicht den sicheren Remotezugriff auf Anwendungen, ohne dass Sie Citrix Gateway in der DMZ bereitstellen oder Ihre Firewall neu konfigurieren müssen. Der Infrastrukturmehraufwand für die Verwendung von Citrix Gateway wird zu Citrix Cloud verlagert.

Weitere Informationen finden Sie in der Produktdokumentation zu Citrix Gateway Service. Sie enthält Informationen zum Aktivieren des Citrix Gateway-Service und bekannte Probleme der Version, die Sie verwenden.

Citrix ADC (Application Delivery Controller) analysiert den anwendungsspezifischen Datenverkehr, damit der Netzwerkdatenverkehr für L4–L7 (Layer 4 –Layer 7) für Webanwendungen intelligent verteilt, optimiert und gesichert werden kann. Das virtuelle Citrix ADC VPX-Gerät kann auf verschiedenen Virtualisierungs- und Cloud-Plattformen gehostet werden. Weitere Informationen finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz.

# SDKs und APIs

December 18, 2023

## Citrix DaaS Remote PowerShell-SDK

Das Remote PowerShell-SDK automatisiert komplexe und repetitive Aufgaben. Damit kann die Citrix DaaS-Umgebung (ehemals Citrix Virtual Apps and Desktops Service) ohne die Benutzeroberflächen unter **Verwalten** eingerichtet und verwaltet werden.

- Einzelheiten zu den Cmdlets finden Sie unter Citrix DaaS-SDK.
- Die unterstützten Module sind unter Unterstützung und Einschränkungen aufgeführt. Der Abschnitt enthält zudem eine Liste der in diesem SDK deaktivierten Cmdlets.
- Das Remote PowerShell SDK steht auf der Citrix-Website zum Download zur Verfügung.

Dieses Produkt unterstützt die PowerShell-Versionen 3 bis 5.

### Unterschiede zwischen diesem und dem SDK für kundenverwaltete Bereitstellungen

Bei von Administratoren des Kunden installierten und verwalteten Citrix Virtual Apps and Desktops-Bereitstellungen führen die Administratoren Cmdlets und Skripts in einer Site aus, die VDAs und Delivery Controller in einer gemeinsamen Domänenstruktur enthält. Bei Citrix DaaS sind die VDAs und Controller hingegen auf einen Ressourcenstandort und eine Steuerungsebene aufgeteilt. Aufgrund dieser Aufteilung funktioniert das ursprüngliche Citrix Virtual Apps and Desktops PowerShell SDK nicht in einer Citrix DaaS-Umgebung. Es kann die sichere Grenze vom Ressourcenstandort zur Steuerungsebene nicht überqueren.

Die Lösung ist das Citrix DaaS Remote PowerShell-SDK. Wenn das Remote PowerShell-SDK am Ressourcenstandort ausgeführt wird, greift es auf die Steuerungsebene zu als wäre es lokal. Die Funktionalität entspricht der einer einzelnen Citrix Virtual Apps and Desktops-Site. Es gibt nur die niedrigste, nicht sichtbare Kommunikationsschicht, die entweder für den Betrieb in einer einzelnen lokalen Site oder in der Cloudumgebung optimiert ist. Die Cmdlets sind die gleichen und die meisten bestehenden Skripts sind unverändert.

Das Cmdlet `Get-XdAuthentication` bietet die Berechtigung zum Passieren der Grenze zwischen sicherem Ressourcenstandort und Steuerungsebene. Standardmäßig fordert `Get-XdAuthentication` die Benutzer zur Eingabe von CAS-Anmeldeinformationen auf, was einmal pro PowerShell-Sitzung erforderlich ist. Alternativ können Benutzer Authentifizierungsprofile mit einem API Access Secure Client definieren, der in der Citrix Cloud-Konsole erstellt wurde. In beiden

Fällen bleiben die Sicherheitsinformationen für die Verwendung in nachfolgenden PowerShell-SDK-Aufrufen erhalten. Wenn das Cmdlet nicht explizit ausgeführt wird, wird es vom ersten PowerShell-SDK-Cmdlet aufgerufen.

#### Voraussetzungen

Um das Remote PowerShell-SDK von Citrix DaaS zu verwenden, setzen Sie die folgenden URLs auf die Positivliste:

#### Kommerziell

- `https://accounts.cloud.com`
- `https://[service].citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

#### Japan

- `https://accounts.citrixcloud.jp`
- `https://[service].citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

#### Behörden

- `https://accounts.cloud.us`
- `https://[service].citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

#### Installieren und Verwenden des Remote PowerShell SDKs

Anforderungen und Überlegungen:

> **Hinweis:**
>
> Installieren Sie das Remote PowerShell SDK nicht auf einer Citrix Cloud Connector-Maschine. Es kann auf jeder in der Domäne eingebundenen Maschine am gleichen Ressourcenstandort installiert werden.
>
> Citrix unterstützt die Ausführung der Cmdlets dieses SDK auf Cloud Connectors nicht. Am SDK-Betrieb sind die Cloud Connectors nicht beteiligt.
>
> Wenn Sie auch eine Bereitstellung von Citrix Virtual Apps and Desktops verwenden (zusätzlich zur Citrix DaaS-Bereitstellung), installieren Sie nicht das Remote PowerShell-SDK auf einer on-

> premises Delivery Controller-Maschine.

- Installieren Sie **Microsoft Edge WebView2**.
- Vergewissern Sie sich, dass auf der Maschine PowerShell 3.0, 4.0 oder 5.0 verfügbar ist.
- Das SDK-Installationsprogramm lädt .NET Framework 4.8 (oder eine spätere unterstützte Version) herunter und installiert es, sofern es noch nicht installiert ist.
- Wenn auf der Maschine das Citrix Virtual Apps and Desktops-SDK bereits installiert ist, entfernen Sie es (über Windows Programme und Funktionen), bevor Sie das Remote PowerShell-SDK installieren.
- Verwenden Sie für eine automatisierte Umgebung den Parameter `-quiet`, um das SDK ohne Benutzereingabe zu installieren.

Installieren des Remote PowerShell SDKs:

1. Laden Sie von der Downloadseite das Virtual Apps and Desktops Remote PowerShell SDK herunter.
2. Installieren Sie das SDK und führen Sie es aus.

Installationsprotokolle werden in `%TEMP%\CitrixLogs\CitrixPoshSdk` erstellt. Protokolle können beim Beheben von Installationsproblemen helfen.

Führen Sie das SDK auf einem Computer in der Domäne innerhalb des Ressourcenstandorts aus:

- Öffnen Sie eine PowerShell-Eingabeaufforderung. Das Programm muss nicht als Administrator ausgeführt werden.
- Um das Snap-In (und nicht das Modul) zu verwenden, fügen Sie das Snap-In über das Cmdlet `Add-PSSnapin` (oder `asnp`) hinzu.
- Sie können sich explizit über das Cmdlet `Get-XdAuthentication` authentifizieren. Führen Sie alternativ den ersten Remote PowerShell-SDK-Befehl aus, durch den Sie zur gleichen Authentifizierung wie bei `Get-XdAuthentication` aufgefordert werden. Wenn Sie einen Proxy verwenden, müssen Sie sich beim Proxy authentifizieren, um das Cmdlet `Get-XdAuthentication` verwenden zu können. Weitere Informationen finden Sie unter Remote PowerShell SDK mit einem Proxy verwenden.
- Zum Umgehen der Authentifizierungsaufforderung können Sie mit einem in der Citrix Cloud-Konsole erstellten Secure Client und dem Cmdlets `Set-XdCredentials` ein Standardauthentifizierungsprofil erstellen.
- Fahren Sie mit dem Ausführen von PowerShell-SDK-Cmdlets bzw. -Automatisierungsskripts fort. Sehen Sie ein Beispiel.

Um das Remote PowerShell-SDK zu deinstallieren, wählen Sie im Windows-Feature zum Entfernen oder Ändern von Programmen die Option **Citrix Virtual Apps and Desktops Remote PowerShell-SDK**. Klicken Sie mit der rechten Maustaste und wählen Sie **Deinstallieren**. Folgen Sie den Dialogfeldern.

**Remote PowerShell-SDK mit einem Proxy verwenden** Wenn Sie einen Proxy verwenden, können Sie das Cmdlet `Get-xdAuthentication` möglicherweise nicht verwenden, da der Proxy die HTTP-Anforderungen des Cmdlet blockiert.

Es gibt zwei Möglichkeiten, sich beim Proxy zu authentifizieren. Sie können den Parameter `ProxyUseDefault` oder die Parameter `ProxyUsername` und `ProxyPassword` verwenden:

- Der Parameter `ProxyUseDefault` ermöglicht die Authentifizierung beim Proxy mithilfe der Standard-Proxy-Anmeldeinformationen. Beispiel:

```
1 Get-XdAuthentication -ProxyUseDefault
2 <!--NeedCopy-->
```

- Die Parameter `ProxyUsername` und `ProxyPassword` ermöglichen die Authentifizierung beim Proxy innerhalb der PowerShell-Sitzung. Beispiel:

```
1 $secureString = ConvertTo-SecureString -String "password" -
      AsPlainText -Force
2
3 Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
      $secureString
4 <!--NeedCopy-->
```

### Beispielaktivitäten

Zu den häufigen Aktivitäten gehören das Einrichten von Maschinenkatalogen, Anwendungen und Benutzern. Siehe Beispielskript unten.

```
1     $users = "xd.local\Domain Users"
2
3     $TSVDACatalogName = "TSVDA"
4
5     $TSVDADGName = "TSVDA"
6
7     $TSVDAMachineName = "xd\ds-tsvda2"
8
9     #Create TSVDA Catalog
10
11    $brokerUsers = New-BrokerUser -Name $users
12
13    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
          AllocationType "Random" -Description $TSVDACatalogName -
          PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
          SessionSupport "MultiSession" -MachinesArePhysical $true
14
15    #Add TSVDA Machine to Catalog
16
17    $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
          -CatalogUid $catalog.uid
```

```
18
19      #Create new desktops & applications delivery group
20
21      $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
            $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
            " -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23      #Create notepad application
24
25      New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
            Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27      #Assign users to desktops and applications
28
29      New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
             $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31      New-BrokerAccessPolicyRule -Name $TSVDADGName -
            IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
            DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33      New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
            DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
             $TSVDADGName
34
35      #Add machine to delivery group
36
37      Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38  <!--NeedCopy-->
```

**Unterstützung und Einschränkungen**

Die folgenden Betriebssysteme werden vom Remote PowerShell SDK unterstützt:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Die folgenden PowerShell-Module von Citrix Virtual Apps and Desktops werden in diesem Release unterstützt:

- Broker
- Active Directory-Identität

- Maschinenerstellung
- Konfiguration
- Konfigurationsprotokollierung
- Host
- Delegierte Administration
- Analytics

Weitere Informationen zu Cmdlets finden Sie unter Citrix Virtual Apps and Desktops SDK.

Nach der Authentifizierung bleibt der Remotezugriff in der aktuellen PowerShell-Sitzung 24 Stunden lang gültig. Nach Ablauf dieser Zeit müssen Sie Ihre Anmeldeinformationen eingeben.

Das Remote PowerShell-SDK muss auf einem Computer im gleichen Ressourcenstandort ausgeführt werden.

Die folgenden Cmdlets sind bei Remotevorgängen deaktiviert, um die Integrität und Sicherheit der Citrix Cloudsteuerungsebene zu gewährleisten.

**Citrix.ADIdentity.Admin.V2:**

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

**Citrix.Analytics.Admin.V1:**

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite

- Set-AnalyticsDBConnection

**Citrix.DelegatedAdmin.Admin.V1:**

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

**Citrix.Broker.Admin.V2:**

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection

- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

**Citrix.Configuration.Admin.V2:**

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

**Citrix.Host.Admin.V2:**

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership

- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

**Citrix.ConfigurationLogging.Admin.V1:**

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

**Citrix.MachineCreation.Admin.V2:**

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

**Citrix.EnvTest.Admin.V1:**

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership

- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

**Citrix.Monitor.Admin.V1:**

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

**Citrix.Storefront.Admin.V1:**

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

## Citrix DaaS-Discoverymodul für App-V-Pakete und Server

Citrix DaaS kann Anwendungen in App-V-Paketen mit einer der folgenden Methoden für die Endpunkte bereitstellen:

- Methode der Einzelverwaltung (Zugriff auf Pakete von einer Netzwerkfreigabe)
- Methode der dualen Verwaltung (Zugriff auf Pakete von einem Microsoft App-V-Verwaltungsserver)

Das Registrieren von App-V-Paketen und Microsoft App-V-Verwaltungsservern und -Veröffentlichungsservern bei der Anwendungsbibliothek über Citrix DaaS unterscheidet sich geringfügig von der Registrierung über eine On-Premises-Bereitstellung. Das Zuweisen von Anwendungen für Benutzer und Starten auf dem Endpunkt eines Benutzers ist jedoch identisch.

Die Citrix DaaS-Verwaltungskonsole in Citrix Cloud kann keine Dateien an einem Ressourcenstandort anzeigen. Außerdem kann sie App-V-Pakete oder Microsoft App-V-Server in Ihrer Infrastruktur nicht direkt ermitteln. Das Discoverymodul bietet Funktionen, mit denen App-V-Paketinformationen in Ihrer On-Premises-Infrastruktur ermittelt und in Citrix DaaS hochgeladen werden. Dabei handelt es sich um App-V-Pakete, Microsoft App-V-Server und die Apps, die in den Paketen enthalten sind.

Das Discoverymodul verwendet das Virtual Apps and Desktops Remote PowerShell-SDK. Er kann Paketinformationen in einer Netzwerkfreigabe oder auf einem Microsoft App-V-Verwaltungsserver ermitteln. Sie verwenden das Discoverymodul auf einer Maschine an Ihrem Ressourcenstandort.

Voraussetzungen für die Verwendung des Discoverymoduls:

- Vergewissern Sie sich, dass auf der Maschine PowerShell 3.0 oder höher verfügbar ist.
- Vergewissern Sie sich, dass das Citrix Virtual Apps and Desktops Remote PowerShell SDK auf der Maschine installiert ist.
- Vergewissern Sie sich, dass Sie Lesezugriff auf die Netzwerkfreigabe mit den App-V-Paketen haben.
- Vergewissern Sie sich, dass Sie Zugriff auf den Server haben, auf dem die Citrix Cloud Connectors installiert sind und der Microsoft App-V-Verwaltungsserver gehostet wird.

#### Hinzufügen von App-V-Paketen zur Anwendungsbibliothek in der Citrix Cloud

Das folgende Verfahren gilt für das Hinzufügen von App-V-Paketen aus Netzwerkfreigaben (Einzelverwaltung) und für das Hinzufügen aller veröffentlichten App-V-Pakete vom Microsoft App-V-Verwaltungsserver (duale Verwaltung). Bei der dualen Verwaltung müssen Sie die hinzugefügten App-V-Pakete genauso verwalten, wie bei der Einzelverwaltung.

1. Laden Sie das Discoverymodul von der Citrix DaaS-Downloadseite https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html herunter. Extrahieren Sie die ZIP-Datei `Citrix.Cloud.AppLibrary.Admin.v1.psm1` in einen Ordner.

   > **Hinweis:**
   >
   > Die Datei ist im ISO-Image von Citrix Virtual Apps and Desktops unter `Support\Tools\Scripts`. Sie können sie lokal kopieren oder direkt vom CD-Laufwerk referenzieren.

2. Sicherstellen, dass das Citrix Virtual Apps and Desktops Remote PowerShell-SDK auf der Maschine installiert ist
3. Navigieren Sie zu dem Ordner mit dem Discoverymodul Geben Sie im PowerShell-Fenster den vollständigen Pfad des Ordners mit dem Discoverymodul ein und drücken Sie die **Eingabetaste**.
4. Importieren Sie das Discovery-Modul mit dem Befehl `Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1`.

5. Fügen Sie App-V-Pakete mit einer der folgenden Methoden zur Anwendungsbibliothek in der Citrix Cloud hinzu.

   - Um App-V-Pakete aus einer Netzwerkfreigabe hinzuzufügen, verwenden Sie das PowerShell-Cmdlet `Import-AppVPackageToCloud`.

     Beispiel: `Import-AppVPackageToCloud –PackagePath \\AppVSrv\share\Notepad++.appv`

     Geben Sie zum Aufrufen der Cmdlet-Hilfe `Get-Help Import-AppVPackageToCloud` ein.

   - Um App-V-Pakete von einem Microsoft App-V-Verwaltungsserver hinzuzufügen, führen Sie das PowerShell-Cmdlet `Import-AppVPackagesFromManagementServerToCloud` aus.

     Beispiel: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

     Geben Sie zum Aufrufen der Cmdlet-Hilfe `Get-Help Import-AppVPackagesFromManagement` ein.

     Mit diesem Befehl werden alle veröffentlichten App-V-Pakete vom Microsoft App-V-Verwaltungsserver in Citrix Cloud importiert.

     Wenn Sie die App-V-Pakete zu Citrix Cloud hinzugefügt haben, müssen Sie sie wie bei der Einzelverwaltungsmethode verwalten.

6. Melden Sie sich bei Citrix Cloud an. Wählen Sie den Zielkunden aus. Durch die Ausführung des Skripts werden die App-V-Pakete der Anwendungsbibliothek in Citrix Cloud hinzugefügt.

#### Allgemeine PowerShell-Funktionen

Das Modul enthält die folgenden High-Level-Funktionen, die Sie aus Ihrem eigenen PowerShell-Skript aufrufen können:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Discovery und Upload aller Informationen, die zum Veröffentlichen von Anwendungen aus einem einzigen App-V-Paket erforderlich sind, an Citrix DaaS.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Führt die Discovery der UNC-Pfade der Pakete durch, die vom Management Server veröffentlichten wurden. Anschließend wird **Import-AppVPackageToCloud** nacheinander für jedes Paket aufgerufen.

Auf diese Weise erkannte Pakete werden mit der Einzelverwaltungsmethode in Citrix DaaS geladen. Citrix DaaS kann keine Pakete mit der Dualverwaltungsmethode bereitstellen.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Erkennt Microsoft App-V-Verwaltungsserver und -Veröffentlichungsserver und importiert den Inhalt zur Anwendungsbibliothek. Mit diesem Cmdlet werden alle mit Microsoft App-V-Verwaltungsserver verwalteten Pakete sowie zugehörige Informationen importiert. Server können über PowerShell hinzugefügt und entfernt werden.

  Das Cmdlet fügt App-V-Pakete im Dualverwaltungsmodus hinzu. Es werden nur App-V-Pakete importiert, die auf dem Microsoft App-V-Verwaltungsserver veröffentlicht werden und denen AD-Gruppen hinzugefügt wurden. Wenn Sie Änderungen am Microsoft App-V-Verwaltungsserver vornehmen, führen Sie des Cmdlet erneut aus, um die Anwendungsbibliothek mit dem Microsoft App-V-Verwaltungsserver zu synchronisieren.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Entfernt die zur Anwendungsbibliothek hinzugefügten Microsoft App-V-Verwaltungsserver und -Veröffentlichungsserver.

  Mit diesem Cmdlet werden die angegebenen Microsoft App-V Verwaltungsserver und -Veröffentlichungsserver sowie alle zugehörigen App-V-Pakete entfernt.

Führen Sie das Discoverymodul für App-V-Pakete und Server auf einem Domänencomputer innerhalb des Ressourcenstandorts aus. Folgen Sie den Anweisungen unter Installieren und Verwenden des Remote PowerShell SDKs, um zu beginnen. Fahren Sie mit dem Ausführen von PowerShell-Cmdlets bzw. -Skripts fort. Siehe die folgenden Beispiele.

#### Beispielaktivitäten

Importieren Sie das App-V-Paketdiscoverymodul für Citrix DaaS.

```
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
<!--NeedCopy-->
```

Durchlaufen Sie das App-V-Paketspeicherverzeichnis und laden Sie jedes Paket hoch.

```
Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{

```

```
4      Import-AppVPackageToCloud -PackagePath $_.FullName
5   }
6
7   <!--NeedCopy-->
```

Führen Sie eine Discovery und einen Upload von Paketen aus, die bei einem Microsoft App-V-Verwaltungsserver registriert sind.

```
1  Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN
       AppVManagementServer.domain.net
2  <!--NeedCopy-->
```

Führen Sie eine Discovery von Microsoft App-V-Verwaltungsservern und -Veröffentlichungsservern aus und fügen Sie die Konfiguration zur Anwendungsbibliothek hinzu. Dabei werden auch alle vom Microsoft App-V-Verwaltungsserver verwalteten Pakete im Dualverwaltungsmodus importiert.

```
1  Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer
       .domain.net  – PublishingServerUrl http://AppVManagementServer.domain
       .net:8001
2  <!--NeedCopy-->
```

Lesen Sie die zum Modul gehörende PowerShell-Hilfedokumentation.

```
1  Get-Help Import-AppVPackageToCloud
2  <!--NeedCopy-->
```

#### Einschränkungen

- Die Discovery von App-V-Paketen in Ihrer Ressourcenstandortinfrastruktur kann nicht direkt über die Citrix DaaS-Verwaltungskonsole in Citrix Cloud erfolgen. Weitere Informationen zu Citrix Cloud finden Sie in der Dokumentation zu Citrix Cloud.
- Die Citrix DaaS-Verwaltungskonsole in Citrix Cloud hat keine Liveverbindung zum Microsoft App-V-Verwaltungsserver. Änderungen an Paketen und anderen Konfigurationen im Microsoft App-V-Verwaltungsserver werden erst in die Citrix DaaS-Verwaltungskonsole übernommen, wenn `Import-AppVDualAdminCloud` noch einmal ausgeführt wurde.

### Monitor Service OData API

Zusätzlich zur Anzeige von Verlaufsdaten über die Überwachungsfunktionen können Sie Daten mit der API des Überwachungsdiensts abfragen. Verwenden Sie die API für Folgendes:

- Analysieren historischer Trends für die Planung
- Durchführen einer eingehenden Problembehandlung bei Verbindungs- und Maschinenfehlern

- Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse, z. B. wenn PowerPivot-Tabellen in Microsoft Excel für die Anzeige von Daten auf verschiedene Weise verwendet werden
- Erstellen einer benutzerdefinierten Benutzeroberfläche auf der Basis der von der API bereitgestellten Daten

Weitere Informationen finden Sie unter Monitor Service OData API. Informationen zum Zugriff auf die Monitor Service API finden Sie unter Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

## Citrix DaaS APIs

Die APIs für Citrix DaaS stehen unter https://developer.cloud.com/citrixworkspace/citrix-daas zur Verfügung.

## Haftungsausschluss

Diese Software bzw. der Mustercode wird wie besehen und ohne Zusicherungen, Gewährleistungen und Bedingungen zur Verfügung gestellt. Verwendung, Modifizierung und Verteilung erfolgen auf eigene Gefahr. CITRIX SCHLIESST SÄMTLICHE AUSDRÜCKLICHEN, STILLSCHWEIGENDEN, GESETZLICHEN ODER ANDERWEITIGEN GEWÄHRLEISTUNGEN AUS. HIERZU ZÄHLEN U. A. DIE HAFTUNG FÜR RECHTSMÄNGEL, DIE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE RECHTSGEWÄHRLEISTUNG UND DIE GEWÄHRLEISTUNG DER NICHTVERLETZUNG. Unbeschadet der Allgemeingültigkeit des vorstehend Gesagten anerkennen Sie und erklären sich einverstanden, dass (a) die Software bzw. der Mustercode Fehler, Mängel oder andere Probleme aufweisen kann, die zu Datenverlusten oder Eigentumsbeschädigung führen können, (b) es ggf. nicht möglich ist, die Software bzw. den Mustercode vollfunktional zu verwenden und (c) Citrix ohne Ankündigung und oder Haftung die aktuelle Version und/oder zukünftige Versionen die Software bzw. des Mustercodes zurückziehen kann. Die Software bzw. der Mustercode darf unter keinen Umständen im Rahmen risikobehafteter Aktivitäten, zum Beispiel bei der Lebenserhaltung oder für Sprengungen, eingesetzt werden. CITRIX UND VON CITRIX ABHÄNGIGE UNTERNEHMEN SOWIE REPRÄSENTANTEN VON CITRIX ÜBERNEHMEN IM RAHMEN VERTRAGLICHER VERPFLICHTUNGEN ODER JEGLICHER ANDERER HAFTUNGSTHEORIE KEINERLEI HAFTUNG FÜR SCHÄDEN, DIE DURCH DIE VERWENDUNG DER SOFTWARE BZW. DES MUSTERCODES ENTSTEHEN. DAZU GEHÖREN DIREKTE UND SPEZIELLE SCHÄDEN, NEBENSCHÄDEN, SCHADENSERSATZ MIT STRAFWIRKUNG, FOLGESCHÄDEN UND ANDERE SCHÄDEN, SELBST WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. Sie erklären sich damit einverstanden, Citrix gegen jegliche Ansprüche, die aus einer Verwendung, Modifikation oder Verteilung des Codes durch Sie entstehen, zu verteidigen und schadlos zu halten.