Citrix DaaS für Azure

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Citrix DaaS Standard für Azure

September 7, 2022

Einführung

Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure) ist der einfachste und schnellste Weg, Windows-Apps und Desktops von Microsoft Azure bereitzustellen. Citrix DaaS für Azure bietet cloudbasierte Verwaltung, Bereitstellung und verwaltete Kapazität für die Bereitstellung virtueller Apps und Desktops auf jedem Gerät.

Diese Lösung umfasst:

- Cloud-basierte Verwaltung und Bereitstellung für die Bereitstellung von Citrix gehosteten Azure Virtual Desktops und Apps von Multi-Session-Computern.
- Eine hochauflösende Benutzererfahrung von einer Vielzahl von Geräten unter Verwendung der Citrix Workspace-App.
- Vereinfachte Workflows zur Image-Erstellung und Verwaltung sowie Citrix vorbereitete Windows- und Linux-Images für Einzelsitzungen und mehrere Sitzungen, auf denen der neueste Citrix Virtual Delivery Agent (VDA) installiert ist.
- Sichern Sie den Remotezugriff von jedem Gerät aus mit globalen Präsenzpunkten des Citrix Gateway Service Gateway-Dienstes.
- Erweiterte Überwachungs- und Helpdesk-Verwaltungsfunktionen
- Verwaltete Azure IaaS, einschließlich Azure-Rechen-, Speicher- und Netzwerkfunktionen für die Bereitstellung virtueller Desktops.

Mit der Citrix Remote-PC-Zugriffsfunktion können Benutzer vorhandene physische Computer im Büro remote verwenden. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Sitzungen verwenden.

Wenn Sie mit anderen Citrix DaaS-Produkten vertraut sind, vereinfacht Citrix DaaS für Azure die Bereitstellung virtueller Apps und Desktops. Citrix kann die Infrastruktur für das Hosten dieser Workloads verwalten.

Citrix DaaS für Azure ist ein Citrix Cloud-Dienst. Citrix Cloud ist die Plattform, die Citrix Cloud-Dienste hostet und verwaltet. Erfahren Sie mehr über Citrix Cloud.

Weitere Informationen zu Komponenten, Datenfluss und Sicherheitsaspekten finden Sie unter Technische Sicherheitsübersicht. In diesem Artikel werden auch die Verantwortlichkeiten von Kunden und Citrix beschrieben.

Wie Benutzer auf Desktops und Apps zugreifen

Benutzer (manchmal als Abonnenten bezeichnet) greifen mit dem Citrix HTML5-Client direkt über ihren Browser auf ihre Desktops und Apps zu. Benutzer navigieren zu einer Citrix Workspace-URL, die von Ihnen, ihrem Administrator, bereitgestellt wird. Die Citrix Workspace-Plattform zählt und liefert die digitalen Ressourcen an Benutzer. Benutzer starten einen Desktop oder eine Anwendung von ihrem Workspace aus.

Nachdem Sie einen Maschinenkatalog konfiguriert haben, der Desktops und Apps bereitstellt (oder einen Katalog mit physischen Maschinen für Remote-PC-Zugriff), zeigt Citrix DaaS für Azure die Workspace-URL an. Anschließend benachrichtigen Sie Ihre Benutzer, zu dieser URL zu gehen, um ihren Desktop und ihre Apps zu starten.

Alternativ zum Navigieren zu Citrix Workspace, um auf ihre Desktops und Apps zuzugreifen, können Benutzer eine Citrix Workspace-App auf ihrem Gerät installieren. Laden Sie die App herunter, die für das Betriebssystem des Endpunktgeräts geeignet ist: https://www.citrix.com/downloads/workspace-app/.

Konzepte und Terminologie

In diesem Abschnitt werden einige Elemente und Begriffe vorgestellt, die Administratoren in Citrix DaaS für Azure verwenden:

- Kataloge
- Ressourcenstandorte
- Images
- Azure-Abonnements
- Netzwerkverbindungen
- Domänenbeitritt und nicht in die Domäne eingebunden

Kataloge

Ein Katalog ist eine Gruppe von Maschinen.

- Die Desktops und Apps, die Citrix DaaS für Azure Ihren Benutzern bereitstellt, befinden sich auf virtuellen Maschinen (VMs). Diese VMs werden im Katalog erstellt (bereitgestellt).

  Wenn Sie Desktops bereitstellen, werden die Computer im Katalog für ausgewählte Benutzer freigegeben. Wenn Sie Anwendungen veröffentlichen, hosten mehrere Sitzungsmaschinen Anwendungen, die für ausgewählte Benutzer freigegeben werden.

- Für Remote-PC-Zugriff enthält ein Katalog vorhandene physische Einzelsitzungscomputer. Eine gemeinsame Bereitstellung umfasst Maschinen in Ihrem Büro. Sie steuern den Benutzerzugriff

auf diese Computer über die konfigurierte Benutzerzuweisungsmethode und ausgewählte Benutzer.

Wenn Sie mit anderen Citrix DaaS-Produkten vertraut sind, ähnelt ein Katalog in Citrix DaaS dem Kombinieren eines Maschinenkatalogs und einer Bereitstellungsgruppe.

Weitere Informationen:

- Erstellen Sie Kataloge für veröffentlichte Desktops und Apps.
- Erstellen Sie Kataloge für Remote-PC-Zugriff.
- Verwalten Sie Kataloge.
- Benutzer und Authentifizierung.

Ressourcenstandorte

Die Maschinen eines Katalogs befinden sich an einem Ressourcenstandort. Ein Ressourcenstandort enthält auch zwei oder mehr Cloud Connectors.

- Beim Veröffentlichen von Desktops oder Apps erstellt Citrix automatisch den Ressourcenstandort und die Cloud Connectors, wenn Sie den ersten Katalog erstellen.
- Für Remote-PC-Zugriff erstellt der Administrator den Ressourcenstandort und die Cloud Connectors, bevor er einen Katalog erstellt.

Wenn Sie weitere Kataloge für veröffentlichte Desktops und Apps erstellen, bestimmen das Azure-Abonnement, die Region und die Domäne, ob Citrix einen anderen Ressourcenstandort erstellt. Wenn diese Kriterien einem vorhandenen Katalog entsprechen, versucht Citrix, diesen Ressourcenstandort wiederzuverwenden.

Weitere Informationen:

- Geben Sie beim Erstellen eines Katalogs Informationen zum Ressourcenstandort an.
- Aktionen für den Standort von Ressourcen.

Images

Wenn Sie einen Katalog für veröffentlichte Desktops und Apps erstellen, wird ein Maschinenimage (mit anderen Einstellungen) als Vorlage zum Erstellen der Computer verwendet.

- Citrix DaaS für Azure stellt mehrere von Citrix vorbereitete Images bereit:
  - Windows 10 Enterprise (Einzelsitzung)
  - Virtueller Windows 10 Enterprise-Desktop (Multisitzung)
  - Virtueller Windows 10 Enterprise-Desktop (Multisitzung) mit Office 365 ProPlus
  - Windows Server 2012 R2

  - Windows Server 2016
  - Windows Server 2019
  - Linux

  Auf jedem von Citrix vorbereiteten Image ist ein Citrix VDA und Tools zur Fehlerbehebung installiert. Der VDA ist der Kommunikationsmechanismus zwischen den Computern Ihrer Benutzer und der Citrix Cloud-Infrastruktur, die Citrix DaaS für Azure verwaltet.

  Citrix aktualisiert die verfügbaren vorbereiteten Images, wenn eine neue VDA-Version veröffentlicht wird.

- Sie können auch Ihre eigenen Images aus Azure importieren und verwenden. Sie müssen einen VDA (und eine andere Software) auf dem Image installieren, bevor er zum Erstellen eines Katalogs verwendet werden kann.

Der Begriff VDA bezieht sich häufig auf den Computer, der Apps oder Desktops bereitstellt, und auf die auf diesem Computer installierte Softwarekomponente.

Weitere Informationen finden Sie unter Images.

Azure-Abonnements

Sie können Kataloge für die Bereitstellung von Desktops und Apps erstellen und Images entweder in einem Citrix Managed Azure-Abonnement oder in Ihrem eigenen (vom Kunden verwalteten) Azure-Abonnement erstellen/importieren.

Wenn Sie nur Citrix DaaS für Azure bestellen, müssen Sie Ihre eigenen Azure-Abonnements importieren (hinzufügen) und verwenden. Wenn Sie auch einen Citrix Azure-Verbrauchsfonds bestellen, erhalten Sie ein Citrix Managed Azure-Abonnement. Sie können dann entweder ein Citrix Managed Azure-Abonnement oder eines Ihrer importierten Azure-Abonnements verwenden, wenn Sie einen Katalog erstellen oder ein neues Image erstellen.

Weitere Informationen:

- Bereitstellungsszenarien veranschaulichen die Verwendung von Azure-Abonnements mit Citrix DaaS für Azure.
- Azure-Abonnements erläutern die Unterschiede zwischen Citrix Managed Azure und kundenverwalteten Azure-Abonnements. In diesem Artikel wird auch beschrieben, wie Abonnements angezeigt, hinzugefügt und entfernt werden.
- Technische Sicherheitsübersicht beschreibt die Unterschiede in der Verantwortung bei Citrix Managed Azure und kundenverwalteten Azure-Abonnements.

Netzwerkverbindungen

Wenn Sie einen Katalog mit einem Citrix Managed Azure-Abonnement erstellen, geben Sie an, ob und wie Benutzer von ihren veröffentlichten Desktops und Apps aus auf Standorte und Ressourcen in ihrem on-premises Unternehmensnetzwerk zugreifen können. Die Auswahl ist keine Konnektivität, Azure VNet Peering und Citrix SD-WAN.

Wenn Sie Ihr eigenes Azure-Abonnement verwenden, müssen Sie keine Verbindung herstellen. Sie müssen nur Ihr Azure-Abonnement in den Dienst importieren (hinzufügen).

Weitere Informationen finden Sie unter Netzwerkverbindungen.

Domänenbeitritt und nicht in die Domäne eingebunden

Mehrere Dienstvorgänge und Funktionen unterscheiden sich, je nachdem, ob die Maschinen (VDAs) in Domäne eingebunden oder nicht in die Domäne eingebunden sind. Die Domänenmitgliedschaft beeinflusst auch die verfügbaren Bereitstellungsszenarien

- Sowohl in Domäne eingebundene als auch nicht in der Domäne verbundene Computer unterstützen eine der im Workspace des Benutzers verfügbaren Benutzerauthentifizierungsmethoden.
- Sie können Desktops, Apps oder beides von in die Domäne eingebundenen und nicht in die Domäne eingebundenen Computern veröffentlichen. Computer in Remote-PC-Zugriffskatalogen müssen in die Domäne eingebunden sein.

In der folgenden Tabelle sind mehrere Unterschiede zwischen nicht in der Domäne verbundenen und in Domäne verbundenen Computern bei der Bereitstellung von Desktops und Apps aufgeführt.

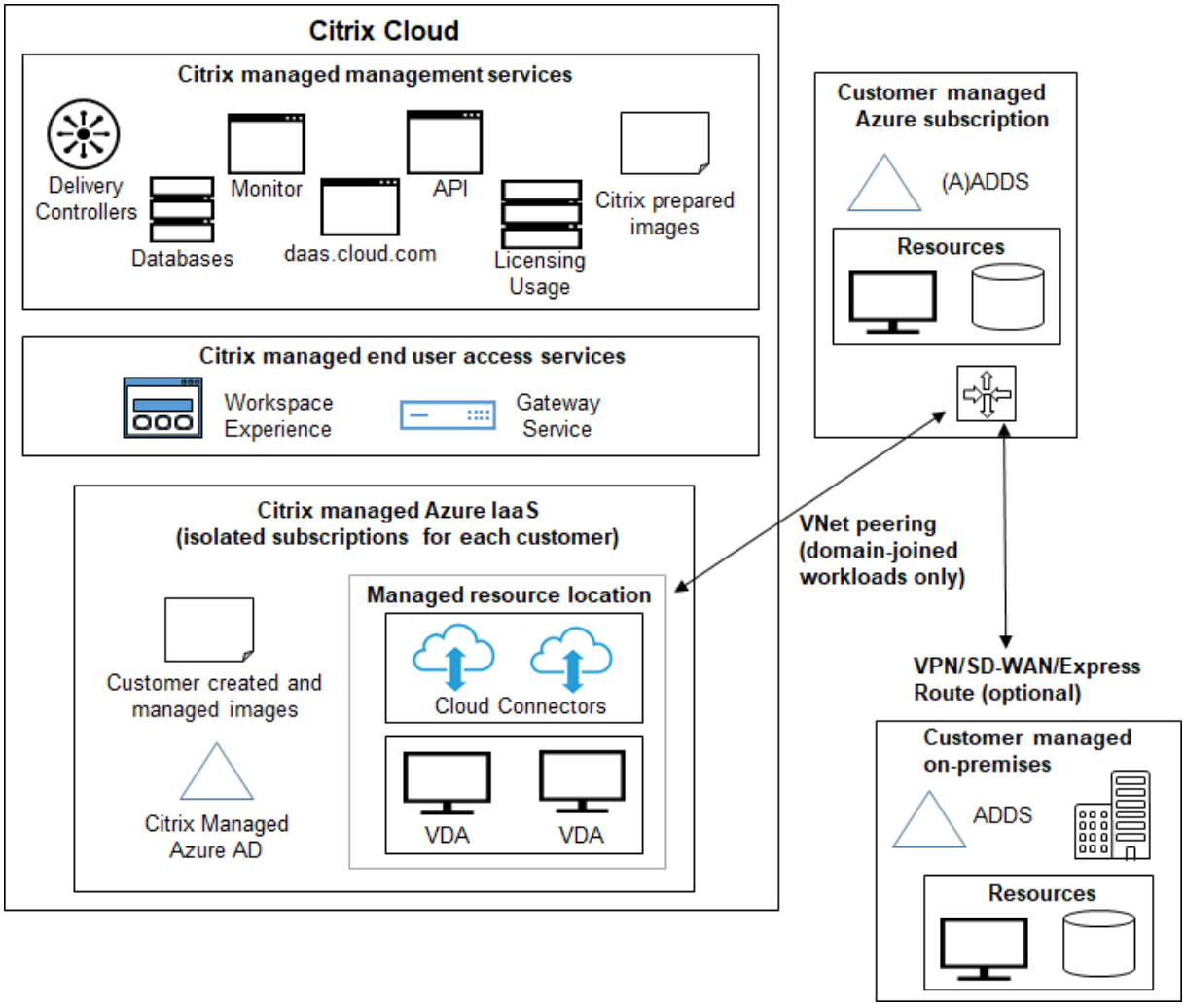
Nicht in die Domäne eingetreten	Domäne beigetreten
Active Directory wird nicht für Computer verwendet. Computer sind nicht mit einer AD-Domäne verbunden.	Active Directory wird für Computer verwendet. Computer sind mit einer AD-Domäne verbunden.
Active Directory-Gruppenrichtlinien können nicht auf Maschinen (VDAs) angewendet werden. (Sie können lokales Gruppenrichtlinienobjekt auf das Image anwenden, das zum Erstellen eines Katalogs verwendet wird.)	VDAs erben Gruppenrichtlinien für die AD-Organisationseinheit, die bei der Katalogerstellung angegeben wurde.

Nicht in die Domäne eingetreten	Domäne beigetreten
Benutzer melden sich mit Single Sign-On an.	Wenn Benutzer sich mit einer anderen Authentifizierungsmethode als Active Directory bei ihrem Workspace anmelden, werden sie auch aufgefordert, sich anzumelden, wenn ein Desktop oder eine App gestartet wird.
Benötigen Sie keine Verbindung zu einem On-Premises-Netzwerk.	(Bei Verwendung eines Citrix Managed Azure-Abonnements) Muss über eine Verbindung verfügen, um mit Microsoft Azure VNet oder Citrix SD-WAN auf ein lokales Netzwerk zugreifen zu können.
Muss ein Citrix Managed Azure-Abonnement für die Bereitstellung von VDAs verwenden. (Ihre eigenen Azure-Abonnements können nicht für die Bereitstellung von VDAs verwendet werden. Benutzer können jedoch von Ihrem eigenen Azure AD aus verbunden werden.)	Kann ein Citrix Managed Azure-Abonnement und Ihre eigenen Azure-Abonnements verwenden.
Fehler bei der Verwendung einer Bastionsmaschine oder direktem RDP können nicht behoben werden.	Kann Probleme mit einer Bastionsmaschine oder direktem RDP beheben.
Die Citrix Profilverwaltung kann nicht verwendet werden. (Empfehlen: Verwenden Sie persistente Kataloge.)	Kann Citrix Profilverwaltung oder FSLogix verwenden.

Bereitstellungsszenarios

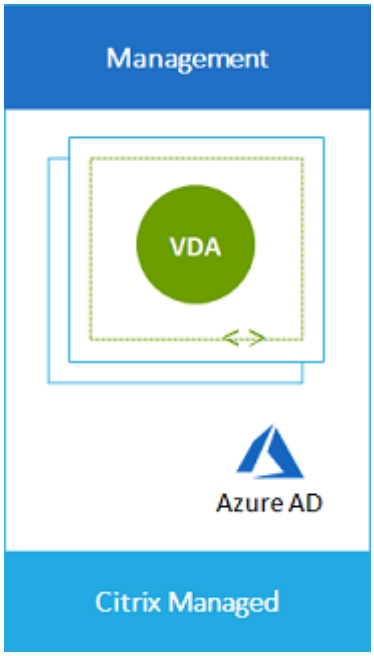
Bereitstellungsszenarien für veröffentlichte Desktops und Apps unterscheiden sich, je nachdem, ob Sie ein Citrix Managed Azure-Abonnement oder Ihr eigenes vom Kunden verwaltetes Azure-Abonnement verwenden.

Bereitstellen in einem Citrix Managed Azure-Abonnement

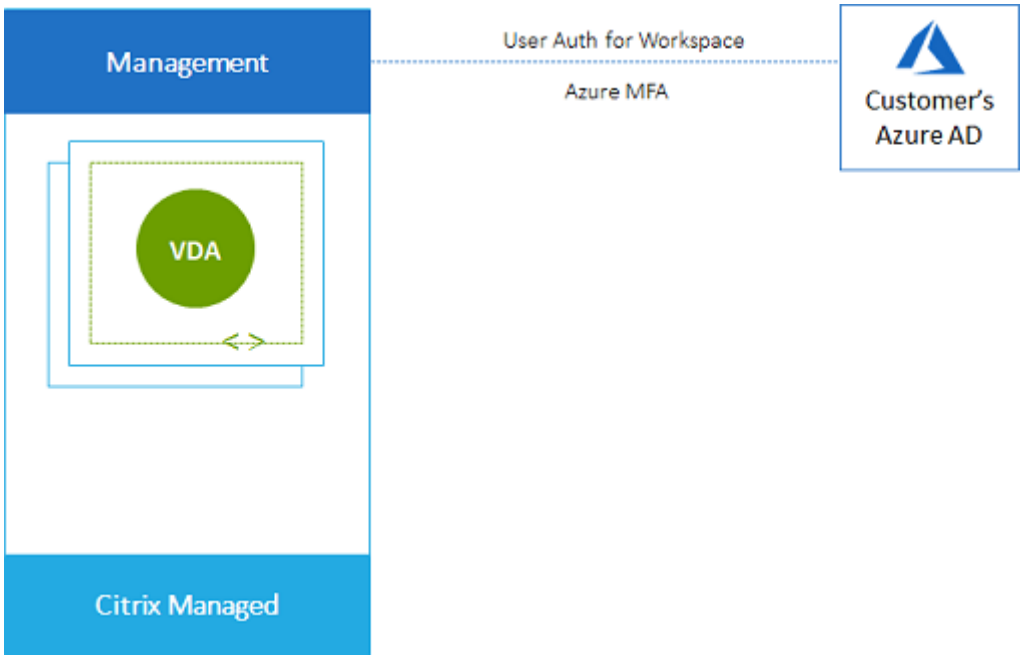


Citrix DaaS für Azure unterstützt verschiedene Bereitstellungsszenarien für Verbindungs- und Benutzerauthentifizierung.

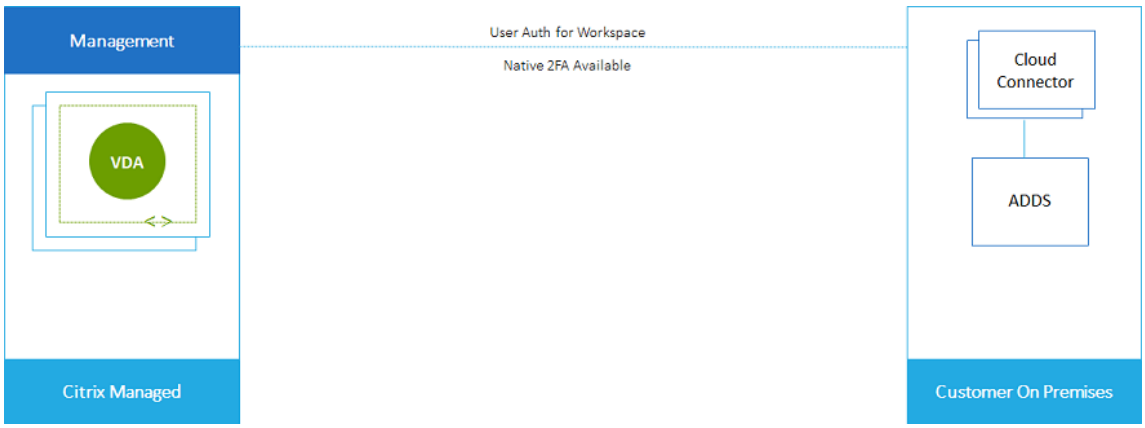
- **Managed Azure AD:** Dies ist die einfachste Bereitstellung mit nicht in die Domäne eingebundenen VDAs. Es wird für Konzeptnachweise empfohlen. Sie verwenden das Managed Azure AD (das Citrix verwaltet), um Benutzer zu verwalten. Ihre Benutzer müssen nicht auf Ressourcen in Ihrem On-Premises-Netzwerk zugreifen.



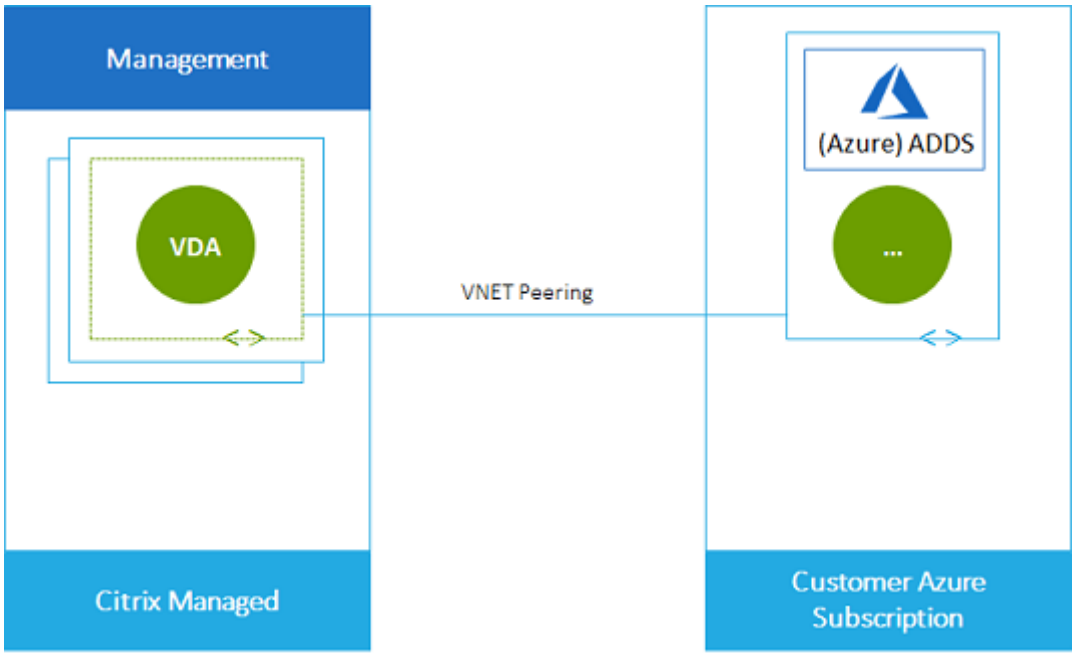
- **Azure Active Directory des Kunden:** Diese Bereitstellung enthält VDAs, die nicht in die Domäne eingebunden sind. Sie verwenden Ihr eigenes Active Directory oder Azure Active Directory (AAD) für die Endbenutzerauthentifizierung. In diesem Szenario müssen Ihre Benutzer nicht auf Ressourcen in Ihrem On-Premises-Netzwerk zugreifen.



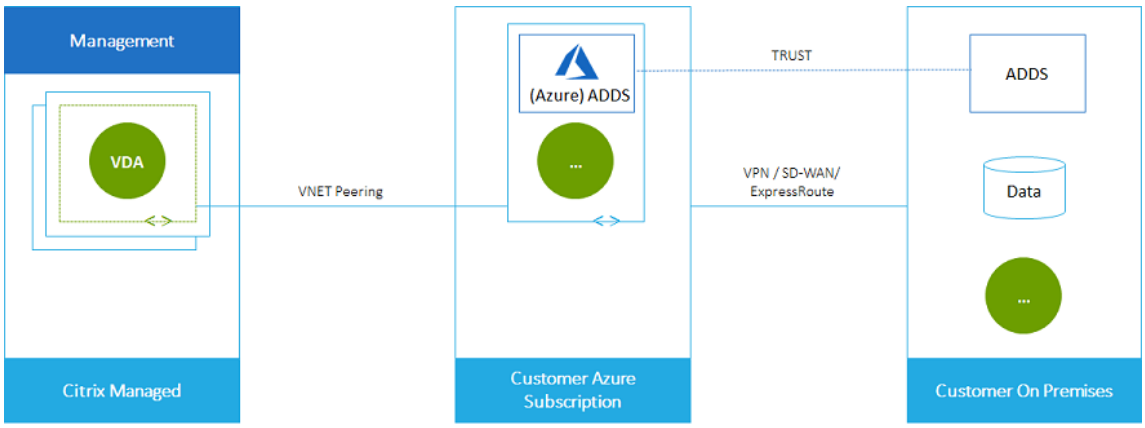
- **Azure Active Directory des Kunden mit lokalem Zugriff:** Diese Bereitstellung enthält nicht in Domäne verbundene VDAs. Sie verwenden Ihr eigenes AD oder AAD für die Endbenutzerauthentifizierung. In diesem Szenario ermöglicht die Installation von Citrix Cloud Connectors in Ihrem On-Premises-Netzwerk den Zugriff auf Ressourcen in diesem Netzwerk.



- **Azure Active Directory Domain Services Directory-Domänendienste und VNet-Peering des Kunden:** Wenn sich Ihr AD oder AAD in Ihrem eigenen Azure VNet- und Azure-Abonnement befindet, können Sie die Microsoft Azure VNet-Peering-Funktion für eine Netzwerkverbindung und Azure Active Directory Domain Services Directory-Domänendienste (AADDS) für die Endbenutzerauthentifizierung verwenden. Die VDAs sind Ihrer Domain beigetreten.

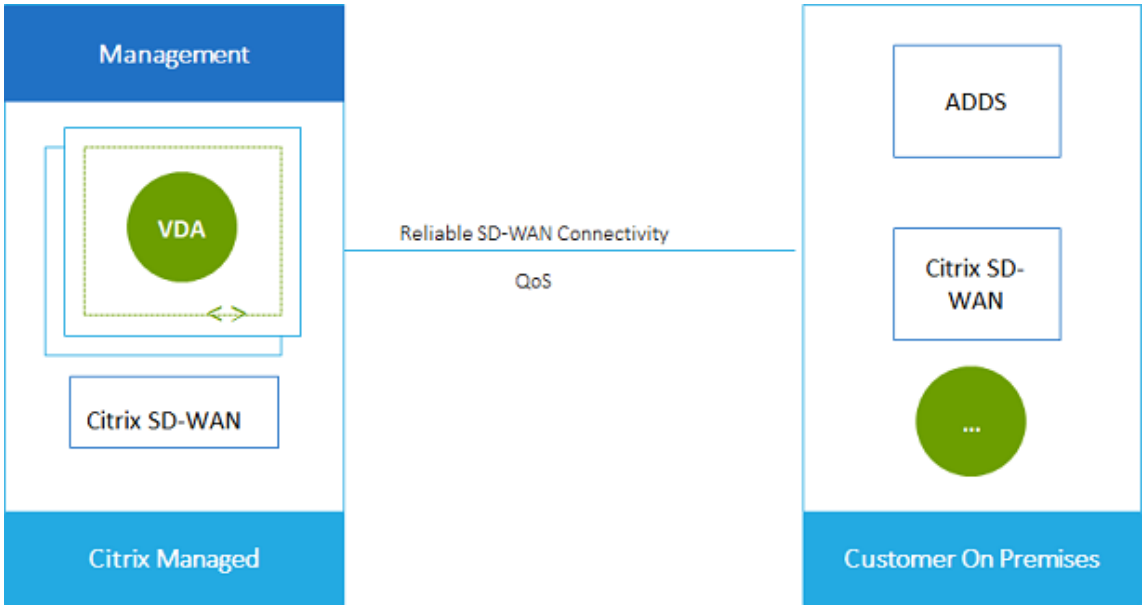


Um Ihren Benutzern den Zugriff auf Daten zu ermöglichen, die in Ihrem On-Premises-Netzwerk gespeichert sind, können Sie Ihre VPN-Verbindung von Ihrem Azure-Abonnement zum on-premises Standort verwenden. Azure VNet Peering wird für die Netzwerkkonnektivität verwendet. Active Directory Domain Services on-premises Speicherort werden für die Endbenutzerauthentifizierung verwendet.

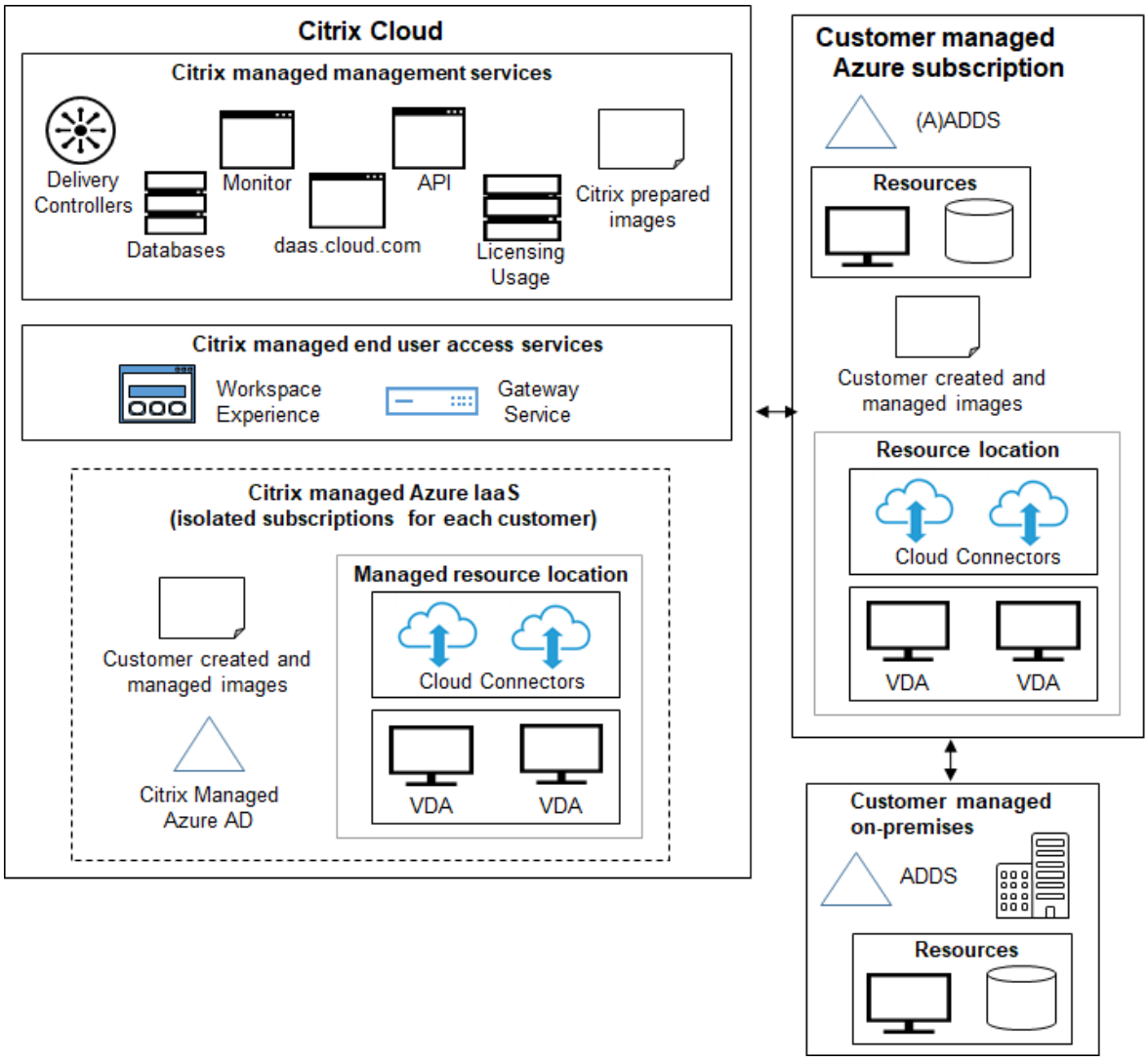


- **Active Directory und SD-WAN des Kunden:** Sie können Benutzern Zugriff auf Dateien und andere Elemente aus Ihren on-premises oder Cloud-SD-WAN-Netzwerken gewähren.

  Citrix SD-WAN optimiert alle Netzwerkverbindungen, die von Citrix DaaS für Azure benötigt werden. In Zusammenarbeit mit den HDX-Technologien bietet Citrix SD-WAN Servicequalität und Verbindungszuverlässigkeit für ICA- und Out-of-Band-Citrix DaaS für Azure-Datenverkehr.



Bereitstellen in einem vom Kunden verwalteten Azure-Abonnement



Die Bereitstellung in der vorhergehenden Grafik verwendet ein vom Kunden verwaltetes Azure-Abonnement. Das Citrix Managed Azure-Abonnement bleibt jedoch eine Option für andere Kataloge und Images, wie durch die gepunktete Gliederung angegeben.

Managementschnittstellen

Citrix DaaS für Azure verfügt über zwei grafische Verwaltungsschnittstellen: Quick Deploy und Full Configuration.

- Mit**Quick Deploy** können Sie schnell Kataloge erstellen und Ihren Benutzern Desktops und Apps bereitstellen. (Daher der Name Quick Deploy.) Dies ist die Standardschnittstelle, wenn Sie Citrix DaaS für Azure starten. Sie können diese Schnittstelle auch aufrufen, indem Sie **Verwalten > Azure Quick Deploy**auswählen. Die Anweisungen in diesem Produktdokumentationssatz

gehen davon aus, dass Sie Quick Deploy verwenden.

Wenn Sie vorhaben, beim Erstellen eines Katalogs oder Images ein Citrix Managed Azure-Abonnement zu verwenden, müssen Sie Quick Deploy verwenden.

- **Vollständige Konfiguration** bietet erweiterte Funktionen und Konfigurationsoptionen zur Anpassung und Verwaltung Ihrer Bereitstellung. Kataloge, die Sie in Quick Deploy erstellen, werden automatisch in Vollkonfiguration angezeigt. Um von Quick Deploy zu Vollkonfiguration zu wechseln, wählen Sie **Verwalten > Vollständige Konfiguration**.

  Wenn Sie in Quick Deploy einen Katalog erstellen, werden eine zugehörige Bereitstellungsgruppe und eine Host-Verbindung automatisch in Vollkonfiguration erstellt.

  Vollständige Konfiguration bietet auch einen eigenen Katalogerstellungsprozess, der das Herstellen einer Verbindung zum Azure-Host und das anschließenden Erstellen eines Katalogs und einer Bereitstellungsgruppe umfasst. Dieser Prozess wird nur unterstützt, wenn Sie Ihr eigenes Azure-Abonnement verwenden. Es ist viel einfacher, den Katalog in Quick Deploy zu erstellen.

  Die vollständige Konfiguration unterstützt Prozesse im Zusammenhang mit anderen Hypervisor- und Cloud-Service-Hosts als Azure. Diese stehen Kunden von Citrix DaaS für Azure nicht zur Verfügung.

Verwalten von mit Quick Deploy erstellten Katalogen

Wenn Sie einen Katalog in der Quick Deploy-Schnittstelle erstellen, können Sie ihn dort auch weiterhin verwalten. Einzelheiten finden Sie unter Verwalten von Katalogen. 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 im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure auf eine beliebige Stelle im Katalogeintrag. 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.

Informationen zum Verwalten von konvertierten Katalogen in Vollkonfiguration finden Sie unter:

- Verwalten von Maschinenkatalogen (Vollkonfiguration bezeichnet Kataloge als Maschinenkataloge)
- Verwalten von Bereitstellungsgruppen

Weitere Informationen

Technische Details finden Sie in folgenden Artikeln:

- Citrix Tech Zone Referenzarchitektur
- Tech Briefs von Citrix Tech Zone

Informationen zur Automatisierung Ihrer Bereitstellungen finden Sie in der öffentlichen API-Vorschau für verwaltete Desktops.

Wenn Sie bereit sind, fangen Sie an.

Was ist neu

December 28, 2023

Ein Ziel von Citrix ist es, neue Funktionen und Produktupdates für Citrix DaaS für Azure-Kunden bereitzustellen, sobald diese verfügbar sind. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern. Für Sie, den Kundenadministrator, ist dieser Prozess transparent.

Citrix hat Image-Updates vorbereitet

Auf den von Citrix vorbereiteten Images ist ein aktueller Citrix Virtual Delivery Agent (VDA) installiert. Im Allgemeinen werden mehrmals im Jahr neue VDA-Versionen veröffentlicht, und die verfügbaren von Citrix vorbereiteten Images werden automatisch mit dem neuesten VDA aktualisiert. Weitere Informationen zu neuen und erweiterten Funktionen in der aktuellen Version des VDA finden Sie unter:

- Windows-VDAs
- Linux VDAs

August 2022

- Diese Funktion ist allgemein verfügbar: Sie können jetzt Kataloge von Maschinen erstellen, die mit Ihrem Azure Active Directory verknüpft sind. Siehe Erstellen von Katalogen.

Mai 2022

- Sie können jetzt Kataloge von Maschinen erstellen, die mit Ihrem Azure Active Directory verknüpft sind. Dieses Feature ist als Preview verfügbar. Siehe Erstellen von Katalogen.
- Citrix Service Provider können jetzt den Citrix DaaS für Azure-Dienst von Kunden entfernen. Weitere Informationen finden Sie unter Service entfernen.

April 2022

- Die Erstellung von Hostverbindungen für Citrix Hypervisor, Microsoft SCVMM, VMware vSphere, Prism Central und Nutanix AHV ist jetzt verfügbar. Daher können Sie jetzt zusätzlich zu Azure auch on-premises Hypervisoren verwenden.

- Der Produktname wurde von Citrix Virtual Apps and Desktops Standard for Azure zu Citrix DaaS Standard für Azure geändert. Weitere Informationen zum Rebranding aller Citrix DaaS-Angebote (ehemals Citrix Virtual Apps and Desktops Service) finden Sie unter Neue Features in Citrix DaaS. Erfahren Sie mehr über die Namensänderungen in unserer Ankündigung in unserem Blog.

Januar 2022

- Wenn Sie Kataloge erstellen, können Sie Ihre Maschinen jetzt auf Standard-SSD-Speicher speichern. Bisher wurden nur Standarddatenträger (HDD) und Premium-SSD unterstützt.
- Unterstützung für diese neuen Regionen beim Hosten von VDA-Workloads: Brasilien, Süden; Zentralindien; Japan, Osten; USA, Mitte Süd; Großbritannien, Süden.
- Snapshots und Wiederherstellungen sind jetzt für persistente Desktops verfügbar, die auf Citrix Managed Azure und BYO Azure gehostet werden. Siehe VDA-Snapshot und -Wiederherstellung.
- Statische öffentliche IP-Adressen für den gesamten ausgehenden Datenverkehr von gehosteten VDAs sind jetzt verfügbar. Sie können ein Azure NAT-Gateway konfigurieren, um die IP-Adresse abzurufen. Weitere Informationen finden Sie unter Erstellen einer öffentlichen statischen IP-Adresse.
- Azure VPN ist für die technische Vorschau verfügbar. Mit Azure VPN können Sie Citrix Managed Azure direkt mit on-premises Rechenzentren verbinden. Siehe Technische Vorschau für Azure VPN.
- Für von Citrix vorbereitete Images sind neue Linux-Images verfügbar.

November 2021

- Automatisch genehmigte 7-Tage-Studien sind jetzt verfügbar (zusätzlich zu den vom Vertrieb genehmigten Studien).
- Citrix Service Provider können Benutzer jetzt über das Dashboard **Verwalten > Azure Quick Deploy** des Dienstes oder über die Citrix Cloud-Konsole verwalten. Einzelheiten finden Sie unter Partnerzugriff auf Kundenidentitätsanbieter.

Oktober 2021

- Neue Informationen zum Verwalten von Katalogen, die in Quick Deploy

Mai 2021

- Vorschau-API-Inhalt ist verfügbar.
- Unterstützung für Windows Server 2022 (erfordert mindestens VDA 2106).

Juli 2021

- Die Web Studio-Verwaltungsschnittstelle wurde in Vollkonfiguration umbenannt.

Juni 2021

- Unterstützung für zwei Verwaltungsschnittstellen: Quick Deploy und Web Studio.

Mai 2021

- Dieser Dienst unterstützt die Vorschau der Service Continuity.
- Citrix vorbereitete Images enthalten jetzt Ubuntu Single-Sitzungs- und Multi-Session-Versionen.
- Wenn Sie einen Cloud Connector zu einem Ressourcenstandort mithilfe eines Citrix Managed Azure-Abonnements hinzufügen, können Sie den Leistungstyp der Cloud Connector-Maschine angeben.
- Beim Erstellen eines Katalogs enthalten die Optionen für die Maschinenleistung Optionen, die dem Erzeugungstyp (gen1 oder gen2) des ausgewählten Images entsprechen. Sie können einen Katalog mit einem Image eines anderen Generationstyps aktualisieren, wenn die Maschinen des Katalogs diesen Generationstyp unterstützen.

April 2022

- Der Produktname wurde von Citrix Virtual Apps and Desktops Standard for Azure zu Citrix DaaS Standard für Azure geändert.

Januar 2021

- Vorschau der Unterstützung für die Anzeige von Konsumverpflichtungen.

Oktober 2020

- Sie können die Monitor-Shadow-Funktion verwenden, um die VM oder Sitzung eines Benutzers anzuzeigen oder daran zu arbeiten.
- Produktionsunterstützung für Remote-PC-Zugriff.
- Erweiterte Option zur Katalogerstellung zur Verwendung Ihrer Azure Virtual Desktop-Lizenz oder Azure Hybrid Benefit.
- Wenn eine Neustartaktion auf einer Maschine nicht erfolgreich ist, können Sie eine Neustartaktion erzwingenverwenden.

September 2020

- Details zu Images werden neu organisiert und erweitert. Beispielsweise können Sie jetzt Notizen zu Images hinzufügen und bearbeiten, die Sie vorbereitet oder importiert haben. Sie können den Zugriff auch auf bestimmte IP-Adressen beschränken.
- Beim Erstellen einer Azure VNet-Peering-Verbindung, die ein virtuelles Azure-Netzwerk-Gateway verwendet, können Sie jetzt auch die Routenverbreitung des virtuellen Netzwerk-Gateways aktivieren.
- Der Produktname ändert sich von Citrix Managed Desktops zu Citrix Virtual Apps and Desktops Standard für Azure.

August 2020

- Vorschau-Unterstützung für Remote-PC-Zugriff.
- Ein von Citrix vorbereitetes Windows Server 2019-Image ist jetzt verfügbar.

Juli 2020

- Wenn Sie einen Cloud Connector zu einem Ressourcenstandort mit einem vom Kunden verwalteten Azure-Abonnement hinzufügen, können Sie den Leistungstyp des Cloud Connector-Computers und die Azure-Ressourcengruppe angeben. Einzelheiten finden Sie unter Aktionen für Ressourcenstandorte.
- Beim Erstellen eines Katalogs können Sie ein Benennungsschema für die Maschine angeben. Siehe Erstellen eines Katalogs mithilfe von benutzerdefinierter Erstellung.

Juni 2020

- In einer CSP-Umgebung werden SD-WAN-Verbindungen auf Mandantenbasis erstellt. Damit die SD-WAN-Verbindungsoption dem CSP-Administrator zur Verfügung steht, muss der Mandant

über eine SD-WAN Orchestrator-Serviceberechtigung verfügen. Einzelheiten finden Sie unter Filtern von Ressourcen nach Kunden (Mehrmandantenbereitstellungen).
- Produktionsunterstützung für Linux VDAs bei Verwendung eines kundenverwalteten Azure-Abonnements.
- Das Limit von VDAs pro Abonnement liegt jetzt bei 1.200.

May 2020

- Sie können ein weiteres Citrix Managed Azure-Abonnement hinzufügen, wenn Sie mehr Maschinen als das Limit pro Citrix Managed Azure-Abonnement benötigen.
- Zusätzliche Informationen zu DNS-Servern.

März 2020

- Produktionsunterstützung für SD-WAN-Verbindungen.

Februar 2020

- Um Informationen zur Citrix-Lizenznutzung anzuzeigen, befolgen Sie die Anweisungen unter Überwachen der Lizenz- und Nutzungsüberwachung für Citrix DaaS Standard für Azure.
- Vorschau der Unterstützung für Kataloge, die Red Hat Enterprise Linux- oder Ubuntu-Maschinen enthalten. Diese Funktion ist nur gültig, wenn ein vom Kunden verwaltetes Azure-Abonnement verwendet wird und erfordert ein importiertes Image, das einen Citrix Linux VDA enthält.
- Sie können jetzt entweder den vertikalen oder horizontalen Lastenausgleich für alle Ihre Multi-Session-Computer konfigurieren. (Bisher verwendeten alle Maschinen den horizontalen Lastenausgleich.) Diese globale Auswahl gilt für alle Kataloge in Ihrer Bereitstellung. Siehe Lastenausgleich.
- Sie können jetzt ein Azure-Abonnement hinzufügen, wenn Sie kein globaler Administrator sind.
- Ein von Citrix vorbereitetes Image ist jetzt für Windows 10 Enterprise Virtual Desktop (Multisession) mit Office 365 ProPlus verfügbar.

Januar 2020

- Fügen Sie Unterstützung für benutzerdefinierte Routen in VNet-Peering-Verbindungen hinzu.
- Aktualisierungen des Sicherheitsbeitrags zur Verbesserung der Port- und Regelinformationen.

Dezember 2019

- Vorschau der Unterstützung für SD-WAN-Verbindungen.

Oktober 2019

- In Unterstützte Betriebssysteme wurden Einträge hinzugefügt für:
  - Windows 7 (unterstützt nur VDA 7.15 mit dem neuesten kumulativen Update).
  - Windows Server 2019.
- Ein von Windows Server 2012 R2 Citrix vorbereitetes Image ist jetzt verfügbar.
- Informationen zu den Ressourcenstandorteinstellungen wurden hinzugefügt. Einzelheiten finden Sie unter Aktionen für Ressourcenstandorte und Einstellungen für Ressourcenstandorte beim Erstellen eines Katalogs.

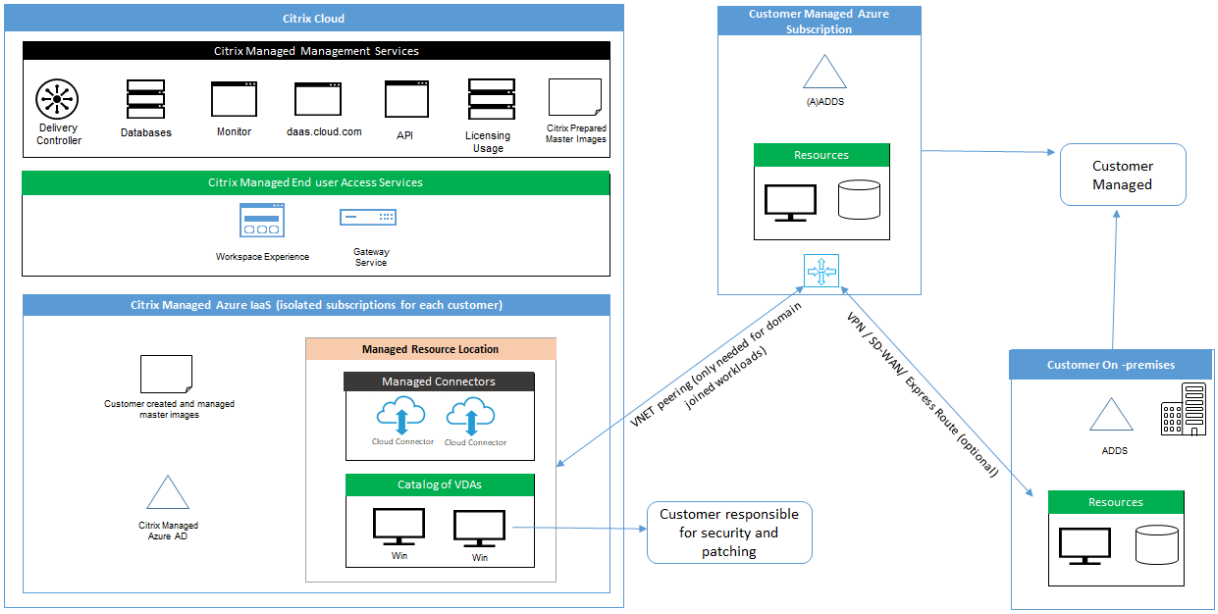
September 2019

- Standardmäßig werden Computer in einem Citrix Managed Azure-Abonnement erstellt. Jetzt können Sie auch Kataloge und Images in Ihrem eigenen kundenverwalteten Azure-Abonnement erstellen.

Technische Sicherheit

May 13, 2022

Das folgende Diagramm zeigt die Komponenten in einer Bereitstellung von Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure). In diesem Beispiel wird eine VNet-Peering-Verbindung verwendet.



Mit Citrix DaaS für Azure werden die Virtual Delivery Agents (VDAs) des Kunden, die Desktops und Apps bereitstellen, sowie Citrix Cloud Connectors in einem Azure-Abonnement und -Mandanten bereitgestellt, das von Citrix verwaltet wird.

> **HINWEIS:**
>
> Dieser Artikel bietet einen Überblick über die Sicherheitsanforderungen für Kunden, die Citrix DaaS für Azure mithilfe eines Citrix Managed Azure-Abonnements bereitstellen. Einen Überblick über die Architektur einer Bereitstellung von Citrix DaaS für Azure mithilfe eines vom Kunden verwalteten Azure-Abonnement, einschließlich Sicherheitsinformationen, finden Sie unter Referenzarchitektur: Virtual Apps and Desktops Service - Azure.

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

Citrix DaaS für Azure stellt 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. Citrix beschränkt den Zugriff auf den AAD auch nur auf das Citrix DaaS für Azure- 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 für Azure verwenden, um ein neues Maschinenimage zu erstellen und anzupassen, werden die Ports 3389-3390 vorübergehend im von Citrix verwalteten VNet geöffnet, sodass der Kunde eine RDP an die Maschine senden kann, die das neue Maschinenimage enthält, um es anzupassen.

Verantwortungsbereich von Citrix bei Verwendung von Azure VNet-Peering-Verbindungen

Damit VDAs in Citrix DaaS für Azure on-premises Domänencontroller, Dateifreigaben oder andere Intranetressourcen kontaktieren können, bietet Citrix DaaS für Azure einen VNet-Peering-Workflow

als Konnektivitätsoption. 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 die Konnektivität mit den lokalen Ressourcen des Kunden mithilfe der Cloud-zu-lokalen Konnektivitätslösung nach Wahl des Kunden ermöglichen, z. B. Azure ExpressRoute oder IPsec-Tunnel.

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

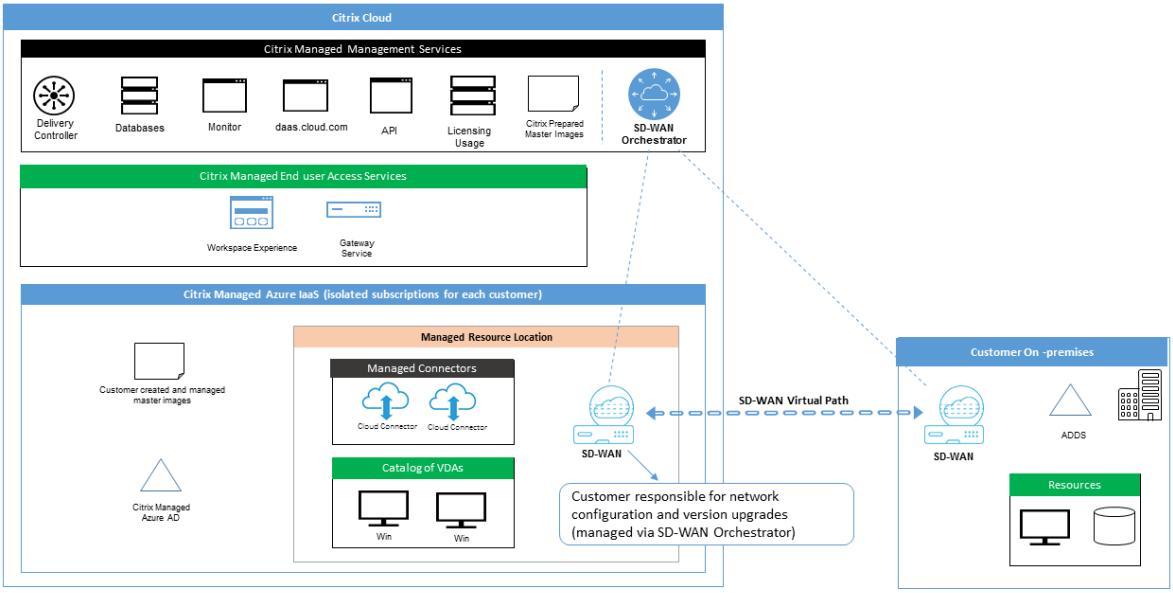
Citrix unterstützt eine vollautomatische Methode zur Bereitstellung virtueller Citrix SD-WAN-Instanzen, um die Konnektivität zwischen Citrix DaaS für Azure und on-premises Ressourcen zu ermöglichen. Die Citrix SD-WAN-Konnektivität hat eine Reihe von Vorteilen im Vergleich zum VNet-Peering, darunter:

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.

Für Citrix müssen Kunden, die die SD-WAN-Konnektivität für Citrix DaaS für Azure nutzen möchten, SD-WAN Orchestrator für die Verwaltung ihrer Citrix SD-WAN-Netzwerke verwenden.

Das folgende Diagramm zeigt die hinzugefügten Komponenten in einer Citrix DaaS für Azure-Bereitstellung mithilfe von SD-WAN-Konnektivität.



Die Citrix SD-WAN-Bereitstellung für Citrix DaaS für Azure ähnelt der standardmäßigen Azure-Bereitstellungskonfiguration 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 zu Internetzielen, 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 der Kunde die Citrix SD-WAN-Konnektivität aktiviert, automatisiert Citrix die anfängliche Bereitstellung virtueller SD-WAN-Instanzen, die mit Citrix DaaS für Azure verwendet werden, verwaltet die zugrunde liegenden Azure-Ressourcen (virtuelle Maschinen, Load Balancer usw.) und bietet sichere

und effiziente Standardwerte für die anfängliche Konfiguration virtueller SD-WAN-Instanzen und ermöglicht die laufende Wartung und Fehlerbehebung über den 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 auf Citrix DaaS für Azure hochgeladenen Maschinenimages verantwortlich, einschließlich Images, 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:

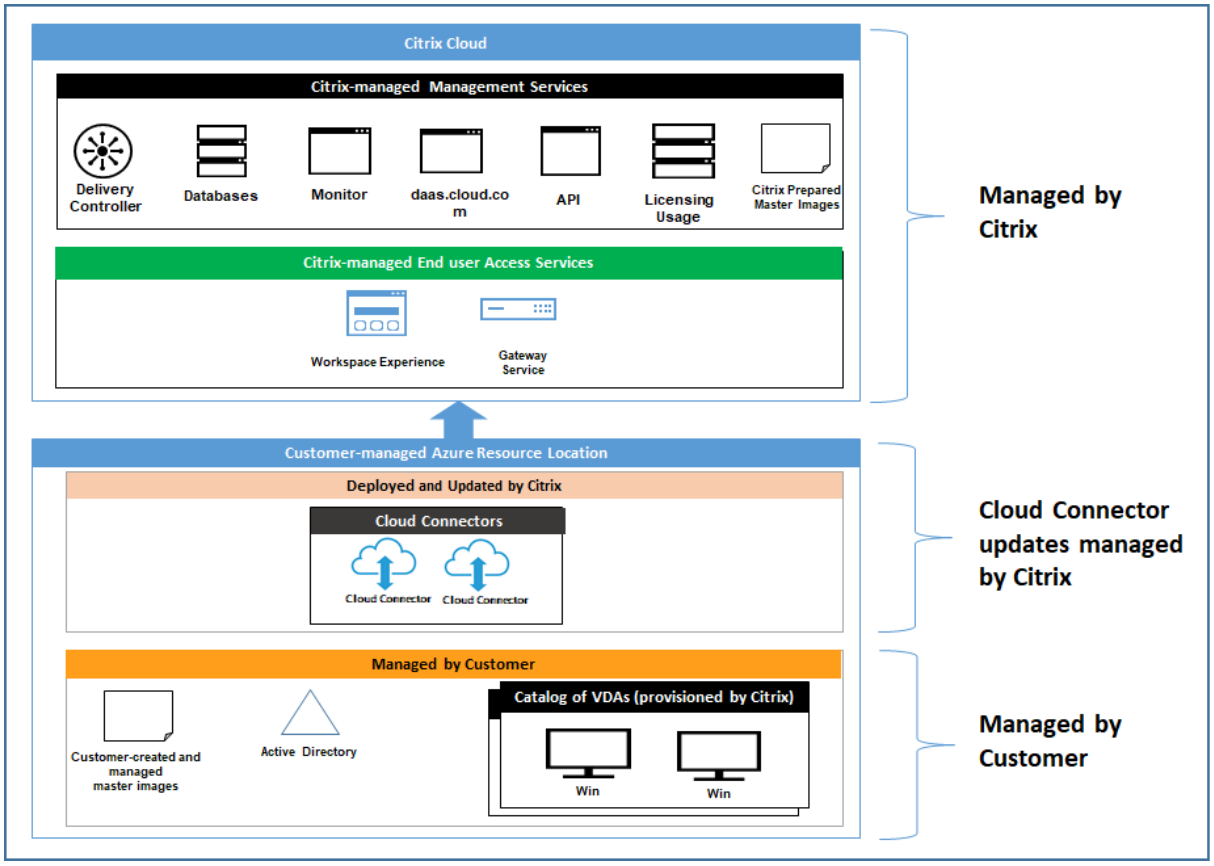
- Vorübergehend wird über Port 3389 eingehender Datenverkehr von dem vom Kunden angegebenen IP-Bereich an die Bastion zugelassen.
- Vorübergehend wird über Port 3389 eingehender Datenverkehr von der IP-Adresse der Bastion an beliebige Adressen im VNet (VDAs und Cloud Connectors) zugelassen.
- RDP-Zugriff 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

Wenn die SD-WAN-Konnektivität konfiguriert ist, haben Kunden die volle Flexibilität, virtuelle SD-WAN-Instanzen, die mit Citrix DaaS für Azure verwendet werden, gemäß ihren Netzwerkanforderungen zu konfigurieren, mit Ausnahme einiger Elemente, die für den ordnungsgemäßen Betrieb von SD-WAN im von 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 Instanzen von Citrix SD-WAN in einem Kundennetzwerk dieselbe Version der SD-WAN-Software ausführen müssen, müssen Bereitstellungen aktualisierter Softwareversionen für Citrix DaaS für Azure SD-WAN-Instanzen von Kunden gemäß ihren Netzwerkwartungsplänen und -beschränkungen verwaltet werden.

Eine falsche Konfiguration von SD-WAN-Routing- und Firewallregeln oder die Missverwaltung von SD-WAN-Verwaltungskennwörtern kann zu Sicherheitsrisiken sowohl für virtuelle Ressourcen in Citrix

DaaS für Azure als auch für on-premises Ressourcen führen, die über virtuelle Citrix SD-WAN-Pfade erreichbar sind. 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.

Im Falle des Verlusts einer gesamten Azure-Region ist der Kunde dafür verantwortlich, sein vom Kunden verwaltetes virtuelles Netzwerk in einer neuen Region wieder aufzubauen und ein neues VNet-Peering oder eine neue SD-WAN-Instanz innerhalb von Citrix DaaS für Azure zu erstellen.

Gemeinsamer Verantwortungsbereich von Citrix und Kunden

Citrix Cloud Connector für domänengebundene Kataloge

Citrix DaaS für Azure stellt mindestens zwei Cloud Connectors an jedem Ressourcenstandort bereit. 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

Falls der Kunde Probleme mit dem Katalog in Citrix DaaS für Azure hat, gibt es zwei Möglichkeiten zur Fehlerbehebung: Verwenden von Bastionen und Aktivieren des RDP-Zugriffs. 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 dafür verantwortlich, diese Ausnahmen zu widerrufen, nachdem der Kunde die Bastion entsorgt oder den RDP-Zugriff über Citrix DaaS für Azure 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

Wenn sich der Kunde für die Verwendung eines in die Domäne eingebundenen Katalogs entscheidet, ist der Kunde dafür verantwortlich, Citrix DaaS für Azure ein Domänenkonto (Benutzername und Kennwort) mit Berechtigungen zum Beitritt von Computern zur Domäne bereitzustellen. Bei der Bereitstellung von Domänenanmeldeinformationen muss folgende Sicherheitsprinzipien einhalten:

- **Überprüfbar:** Das Konto sollte speziell für die Verwendung von Citrix DaaS für Azure erstellt werden, damit leicht überprüft werden kann, wofür das Konto 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

Abonnieren von Citrix DaaS für Azure

December 21, 2022

Einführung

Sie können Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) abonnieren und den Citrix Azure Consumption Fund über Citrix oder Azure Marketplace bestellen. Sie können Citrix DaaS für Azure über Citrix auswerten.

Wenn Sie derzeit Citrix Virtual Apps Essentials oder Citrix Virtual Desktops Essentials abonnieren, können Sie ein Upgrade auf Citrix DaaS Standard für Azure durchführen.

Eine umfassende Bestellung besteht aus zwei Teilen:

- **Citrix DaaS Standard für Azure:** Ermöglicht Ihnen die Verwendung Ihrer eigenen (vom Kunden verwalteten) Azure-Abonnements.
- **Citrix Azure Consume Fund:** Darüber hinaus können Sie zusätzlich zu Ihren eigenen Azure-Abonnements ein Citrix Managed Azure-Abonnement verwenden. Die Verwendung eines Citrix Managed Azure-Abonnements bietet folgende Vorteile:
  - Einzelne Abrechnung von Citrix statt Abrechnungen mehrerer Unternehmen.
  - Unterschiede bei den Azure-Abonnementfunktionen.
  - Microsoft-Unterstützung auf Premiumebene durch Citrix.

Der Citrix Azure Consum-Fonds ist nicht erforderlich. Wenn Sie es jedoch nicht haben, können Sie nur Ihre eigenen Azure-Abonnements verwenden, und Sie erhalten keine anderen Feature-Vorteile.

Der Bestellvorgang unterscheidet sich geringfügig, je nachdem, ob Sie über Citrix oder Azure Marketplace bestellen:

- Wenn Sie über Citrix bestellen, können Sie Citrix DaaS Standard für Azure und den Citrix Azure Consumption Fund gleichzeitig bestellen.
- Wenn Sie über Azure Marketplace bestellen, bestellen Sie zuerst Citrix DaaS Standard für Azure. Dann bestellen Sie den Citrix Azure Consume Fund.

  Wenn Sie sich entscheiden, nur Citrix DaaS für Azure zu bestellen, können Sie den Citrix Azure Consumption Fund später entweder über Azure Marketplace oder über Ihren Citrix Kundenbetreuer bestellen.

Unabhängig davon, wo Sie Citrix DaaS Standard für Azure und den Konsumentenfonds bestellen, bietet Citrix Onboarding-Hilfe. Wir überprüfen auch, ob Citrix DaaS Standard für Azure ordnungsgemäß ausgeführt und konfiguriert ist.

Zusammenfassung der Bestellung

Zusammenfassung der Bestellschritte:

1. Holen Sie sich ein Citrix Cloud-Konto.

   Wenn Sie bereits ein Citrix Cloud-Konto haben und derzeit Citrix DaaS abonnieren, finden Sie weitere Informationen unter Wenn Sie derzeit Citrix DaaS abonnieren.

2. Bestellen Sie Citrix DaaS Standard für Azure und Konsumfonds über Azure Marketplaceoder bestellen Sie über Citrix.

Prüfungen

Citrix DaaS Standard für Azure bietet zwei Arten von Testversionen:

- **Verkaufsgenehmigung:** In einer vom Vertrieb genehmigten Testversion können Sie ein Citrix Managed Azure-Abonnement verwenden, um Kataloge, Images und andere Aufgaben zu erstellen. In der Testversion können Sie in ein kostenpflichtiges Service-Abonnement umwandeln und den Citrix Managed Azure Consumption Fund bestellen. Wenn Sie keinen Verbrauch kaufen, werden alle Ressourcen, die Sie mit dem Citrix Managed Azure-Abonnement erstellt haben, automatisch gelöscht, was sich auf Benutzer auswirken kann.
- **Automatisch genehmigt:** In einer automatisch genehmigten Testversion können Sie Ihr eigenes (vom Kunden verwaltetes) Azure-Abonnement verwenden, um Kataloge, Images und andere Aufgaben zu erstellen. Aus der Testversion können Sie in ein kostenpflichtiges Abonnement umwandeln. Weitere Informationen finden Sie unter Automatisch genehmigte Service-Testversionen.

Weitere Informationen zu Testversionen finden Sie unter Testversionen von Citrix Cloud-Diensten.

Automatisch genehmigte Serviceversionen

- Eine automatisch genehmigte Testversion von Citrix DaaS Standard für Azure dauert 7 Kalendertage.
- Während einer automatisch genehmigten Testversion können Sie Kataloge mit Ihrem Azure-Abonnement erstellen. Kataloge enthalten die Maschinen, die Desktops oder Anwendungen liefern.
- Sie können Kataloge mit einem von Citrix vorbereiteten Image, einem Image, das Sie aus Azure importieren, oder einem Image erstellen, das Sie in Citrix DaaS Standard für Azure erstellen.
- Benutzer müssen in einem Identitätsanbieter konfiguriert sein, den Citrix Workspace unterstützt.

- Sie können Katalogen in Ihrer Testbereitstellung bis zu 25 Benutzer zuweisen. Sie können einen Benutzer zwar mehr als einem Katalog zuweisen, jedoch sind insgesamt 25 eindeutige benannte Benutzer in einer Testbereitstellung zulässig.
- Sie müssen über ein Microsoft Azure-Benutzerkonto und mindestens ein Azure-Abonnement in diesem Konto verfügen. (Testversionen unterstützen nur Anwendungsfälle für Azure-Abonnements im Besitz von Kunden (bringen Sie Ihr eigenes mit).)

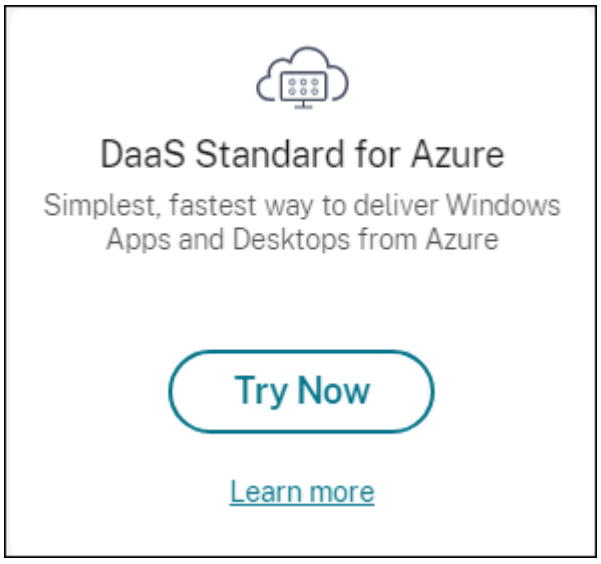
Fordern Sie eine automatisch genehmigte Testversion an und nutzen Sie

1. Eröffnen Sie ein Citrix Cloud-Konto (falls Sie noch keines haben).

   a) Navigieren Sie zu Citrix Cloud.
   b) Wählen Sie **Anmelden und probieren Sie es kostenlos**aus.
   c) Folgen Sie den Anweisungen auf dem Bildschirm.

   In wenigen Augenblicken erhalten Sie eine E-Mail über Ihr Citrix Cloud-Konto. Wählen Sie in der E-Mail den Anmeldelink aus.

2. Fordern Sie eine Studie an. Wählen Sie in der Citrix Cloud-Konsole auf der Kachel **DaaS Standard für Azure** die Option **Jetzt testen** aus.

   Sie erhalten eine E-Mail, wenn Ihre Testversion aktiviert und bereit ist (in der Regel etwa zwei Stunden nachdem Sie die Testversion angefordert haben).

3. Melden Sie sich bei Citrix Cloud an.
4. Klicken Sie auf der Kachel **DaaS Standard für Azure** auf **Verwalten**.
5. Richten Sie Ihre Testumgebung ein und konfigurieren sie. Während der Einrichtung werden Sie:

   a) Fügen Sie dem Dienst Ihr Azure-Abonnement hinzu.

b) Verbinden Sie Ihren Identitätsanbieter über die Citrix Cloud-Konsole.
c) Erstellen Sie einen Katalog.
d) Fügen Sie Benutzer Ihres Identitätsanbieters zum Katalog hinzu.
e) Informieren Sie Ihre Benutzer über die Citrix Workspace-URL.

Die grafische Oberfläche führt Sie durch den Einrichtungsprozess. Einzelheiten finden Sie in der Produktdokumentation:

- Machen Sie sich mit dem Produkt und seiner Terminologie vertraut.
- Überprüfen Sie die Zusammenfassungen und Details der Einrichtung.

Holen Sie sich ein Citrix Cloud-Konto

Um sich für ein Citrix Cloud-Konto anzumelden und eine Testversion anzufordern, gehen Sie zu https://onboarding.cloud.com. Einzelheiten zu diesem Vorgang finden Sie unter Anmelden für Citrix Cloud. Ihr Konto verfügt über eine Organisations-ID (OrgID), die immer in der oberen rechten Ecke der Citrix Cloud-Konsole angezeigt wird.

Nächste Schritte: Bestellen Sie Citrix DaaS Standard für Azure über Citrix oder Azure Marketplace.

Wenn Sie derzeit Citrix DaaS abonnieren

Mit einem Citrix Cloud-Konto (OrgID) können Sie jeweils nur eine Edition des Citrix DaaS abonnieren.

Sie können ein Upgrade von Citrix DaaS Standard für Azure auf eine der folgenden Editionen durchführen:

- Citrix DaaS Advanced Edition
- Citrix DaaS Premium Edition.

Wenden Sie sich für weitere Informationen an Ihren Citrix Vertreter.

Wenn Sie derzeit eine andere Citrix DaaS Edition als Advanced oder Premium abonnieren (z. B. Citrix Virtual Apps Essentials oder Citrix Virtual Desktops Essentials) und Citrix DaaS Standard für Azure abonnieren möchten, müssen Sie entweder:

- Abonnieren Sie Citrix DaaS Standard für Azure mit einem anderen Citrix Cloud-Konto (OrgID). Einzelheiten finden Sie unter Upgrade auf Citrix DaaS Standard für Azure.
- Nehmen Sie den Dienst außer Betrieb, den Sie haben, und bestellen Sie dann Citrix DaaS Standard für Azure. Anweisungen zur Außerbetriebnahme von Diensten finden Sie unter CTX239027.

Sie können ein Citrix Managed Azure-Abonnement verwenden, indem Sie den Citrix Azure Consumption Fund mit einer der folgenden Service-Editionen erwerben:

- Citrix DaaS Standard für Azure
- Citrix DaaS Advanced
- Citrix DaaS Advanced Plus
- Citrix DaaS Premium

Bestellen über Citrix

Sie können Citrix DaaS Standard für Azure (einschließlich des Konsumfonds) über die Citrix Cloud oder über Ihren Citrix Kundenbetreuer bestellen.

Über Citrix Cloud:

1. Melden Sie sich bei Citrix Cloud an. Klicken Sie auf der Kachel **DaaS Standard für Azure** auf **Jetzt testen** . Füllen Sie die angeforderten Informationen aus. Der Text auf der Kachel ändert sich zu **Testversion angefordert**.
2. Citrix kontaktiert Sie. Wenn Citrix DaaS Standard für Azure für Sie verfügbar ist, ändert sich der Text auf der Kachel in **Verwalten**.
3. Melden Sie sich bei Citrix Cloud an. Klicken Sie auf der Kachel **DaaS Standard für Azure** auf **Verwalten**. Wenn Sie zum ersten Mal auf Citrix DaaS Standard für Azure zugreifen, werden Sie zur **Willkommensseite** von Quick Deploy weitergeleitet.

Kündigen Sie ein monatliches Abonnement über Citrix

Monatliche Abonnements verlängern sich zu Beginn eines jeden Monats automatisch. Sie können das Dashboard "Citrix DaaS Standard für Azure"verwenden, um ein monatliches Abonnement zu kündigen, das Sie über Citrix bestellt haben.

(Sie können das Dashboard Citrix DaaS Standard für Azure nicht verwenden, um andere Abonnementtypen zu kündigen, die Sie über Citrix bestellt haben, oder Bestellungen, die über Azure Marketplace aufgegeben wurden.)

So kündigen Sie ein monatliches Abonnement:

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.
3. Erweitern Sie im Dashboard **Verwalten > Azure Quick Deploy** rechts **Allgemein** .
4. Klicken Sie auf **Abonnement kündigen**.
5. Ihre aktiven Ressourcen werden aufgeführt, wie Kataloge, Images und Verbindungen. Die Seite beschreibt die Aktionen, die Citrix während einer Stornierung durchführt. Es informiert Sie auch über Maßnahmen, die Sie gegebenenfalls ergreifen müssen. Geben Sie an, warum Sie den Dienst kündigen. Geben Sie optional mehr Feedback. Wenn Sie fertig sind, klicken Sie auf **Abonnement kündigen**.

6. Bestätigen Sie, dass Sie die Bedingungen der Stornierung verstanden haben.

Ein Banner auf dem Dashboard von Citrix DaaS Standard für Azure zeigt den Eingang Ihrer Stornierungsanfrage an.

Wenn Sie Ihr Abonnement versehentlich kündigen, wenden Sie sich vor Ende des Monats an Ihren Citrix Vertriebsmitarbeiter oder Citrix Partner, um Citrix DaaS Standard für Azure zu reaktivieren.

Bestellen über Azure Marketplace

Bestellen Sie zuerst den Citrix DaaS Standard für Azure und bestellen Sie dann den Citrix Azure Consumption Fund.

Sie können den Konsumfonds nur bestellen, wenn Sie zuvor Citrix DaaS Standard für Azure gekauft haben. Sie können Citrix DaaS Standard für Azure und den Konsumentenfonds nicht in einer Reihenfolge kombinieren.

Citrix DaaS Standard für Azure wird nicht über das Azure Cloud Solutions Provider-Portal angeboten. Wenn Sie ein vorrangiger Support-Kunde sind oder an vorrangigen Support interessiert sind, wenden Sie sich an Ihren Citrix Kundenbetreuer.

Anforderungen:

- Die OrgID von Ihrem Citrix Cloud-Konto.
  - 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 kein Citrix Cloud-Konto haben, befolgen Sie die Anweisungen unter Citrix Cloud-Konto einrichten.
- Ein Azure-Konto und mindestens ein Azure-Abonnement in diesem Konto.

Citrix DaaS Standard für Azure über Azure Marketplace bestellen

1. Melden Sie sich bei Azure Marketplace mit den Anmeldeinformationen Ihres Azure-Kontos an.
2. Suchen Sie nach **Citrix DaaS Standard für Azure**, und navigieren Sie dann zu Citrix.
3. Klicken Sie auf **JETZT HOLEN**.
4. Aktivieren Sie in der Nachricht **Eine weitere Sache** das Kontrollkästchen und klicken Sie dann auf **Weiter**.
5. Die Registerkarten enthalten Informationen über das Produkt, die Pläne, die Preise und die Verwendung. Wenn Sie bereit sind, wählen Sie einen Plan aus (falls mehr als einer verfügbar ist) und klicken Sie dann auf **Einrichten+ abonnieren**.

6. Auf der Registerkarte **Basics**:
    - **Abonnement**: Gibt den Plan an, den Sie ausgewählt haben.
    - **Name**: Geben Sie einen Namen für Ihre Abonnementbestellung ein.
    - Der Abschnitt **Plan** zeigt den Preis für den ausgewählten Plan basierend auf monatlichen und mehrjährigen (jährlichen) Bedingungen.

      Um die Planlaufzeit (monatlich oder jährlich) zu ändern, wählen Sie **Plan ändern**aus. Wählen Sie den gewünschten Begriff aus und klicken Sie auf **Plan ändern**.
7. Auf der Registerkarte **Review + abonnieren** :
    - Überprüfen Sie die Kontaktdaten, die Sie zuvor für das Azure-Basisprofil angegeben haben. Sie können Ihre Adresse, Telefonnummer oder beides ändern.
    - Klicken Sie auf **Abonnieren**.
8. Klicken Sie auf der Seite **"Abonnement** "auf **Konto jetzt konfigurieren**. (Wenn die Schaltfläche deaktiviert ist, warten Sie einen Moment.) Sie werden zu einer Citrix Aktivierungsseite weitergeleitet.
9. Auf der Aktivierungsseite:
    - Verwenden Sie den Link **Anmelden in**, 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 Allgemeinen Geschäftsbedingungen zu und klicken Sie dann auf **Bestellung aktivieren**.

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.

Wenn Sie die E-Mail von Citrix erhalten, können Sie Citrix DaaS Standard für Azure verwenden. Denken Sie daran: Nur mit Citrix DaaS Standard für Azure können Sie nur Ihre eigenen Azure-Abonnements verwenden.

Löschen Sie nicht die Citrix DaaS Standard für Azure-Ressource in Azure. Durch das Löschen dieser Ressource wird Ihr Abonnement gekündigt.

Bestellen Sie den Konsumfonds über Azure Marketplace

1. Melden Sie sich bei Azure Marketplace mit den Anmeldeinformationen Ihres Azure-Kontos an.
2. Suchen Sie nach **Citrix Azure Consume Fund und navigieren Sie dann zu diesem**.

3. Klicken Sie auf **JETZT HOLEN**.
4. Klicken Sie auf **Einrichten + abonnieren**.
5. Auf der **Abonnieren-Seite** :

   - Geben Sie **unter Name**einen leicht erkennbaren Namen ein, z. B. "Meine verwalteten Desktops". Sie können diesen Namen später verwenden, wenn Sie das Dienstabonnement ändern möchten.
   - Geben Sie an, wie viele Benutzer Sie unterstützen möchten, im Bereich von 25 bis 100000.
   - Geben Sie Ihre E-Mail-Adresse und Telefonnummer ein.

   Wenn Sie fertig sind, klicken Sie auf **Abonnieren**.
6. Wenn auf der Seite **Fortschritt des Abonnements** die Schaltfläche **SaaS-Konto auf der Website des Herausgebers konfigurieren** aktiviert (blau) wird, klicken Sie darauf. Sie werden automatisch zu einer Citrix Auftragsaktivierungsseite weitergeleitet.
7. Geben Sie auf der Seite zur Aktivierung von Citrix Bestellungen Ihre Citrix Cloud OrgID ein. Die zuvor eingegebene E-Mail-Adresse wird angezeigt. Sie können es bei Bedarf ändern. Wenn Sie fertig sind, klicken Sie auf **Bestellung aktivieren**.
8. Die Erfüllung der Bestellung des Verbrauchsfonds nimmt nicht viel Zeit in Anspruch. Wenn Citrix über die Bestellung informiert wird, wird in der Citrix DaaS für Azure-Konsole ein Banner angezeigt, das darauf hinweist, dass ein Citrix Managed Azure-Abonnement für Sie vorbereitet wird.

   Im Bereich **Cloud-Abonnements** auf der rechten Seite des Dashboards **Verwalten > Azure Quick Deploy** wird angezeigt, wann das Abonnement einsatzbereit ist.

Erhöhen oder verringern Sie Benutzersitze durch Azure Marketplace

Wenn Sie Benutzersitze erhöhen müssen, erstellen Sie eine neue Azure Marketplace-Bestellung für die gewünschte zusätzliche Anzahl von Sitzplätzen.

Um die Anzahl Ihrer Arbeitsplätze zu reduzieren, kündigen Sie Citrix DaaS Standard für Azure im Azure Marketplace und bestellen Sie dann die gewünschte Anzahl von Arbeitsplätzen.

Kündigen Sie Citrix DaaS Standard für Azure oder Konsumfonds über Azure Marketplace

So kündigen Sie Citrix DaaS Standard für Azure oder den Konsumfonds über Azure Marketplace:

1. Melden Sie sich beim Azure Marketplace an.
2. Suchen Sie nach **DaaS**.

3. Wählen Sie **Neu > Ansicht**.
4. Wählen Sie die Ressource aus, die Sie abbrechen möchten.
5. Wählen Sie im Auslassungsmenü der Ressource die Option **Löschen**aus.
6. Klicken Sie im Bestätigungsfeld auf **Ja**, um zu bestätigen, dass Sie die Rückerstattungsrichtlinie kennen und die Ressource stornieren möchten.

> **Wichtig:**
>
> Kündigen Sie den Citrix Azure Consume Fund nicht, wenn Sie von Citrix verwaltete Ressourcen wie Kataloge oder Images verwenden, die im Citrix Managed Azure-Abonnement erstellt wurden.

Wenn Ihre Bestellung genehmigt und bearbeitet wurde

Nachdem Ihre Testversion oder Ihr Dienst genehmigt wurde, werden auf der Citrix Cloud-Homepage mehrere Kacheln angezeigt:

- Citrix DaaS für Azure
- Citrix DaaS
- Gateway

Citrix DaaS für Azure ist der einzige Dienst, der für Ihre Verwendung aktiviert ist.

Melden Sie sich bei Citrix Cloud an, um mit Citrix DaaS Standard für Azure zu beginnen. Greifen Sie mit einer der folgenden Methoden auf Citrix DaaS Standard für Azure zu:

- Klicken Sie auf der Kachel **DaaS Standard für Azure** auf **Verwalten**.
- Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.

Eine Anleitung zur Einrichtung finden Sie unter Erste Schritte.

Upgrade auf Citrix DaaS Standard für Azure

Wenn Sie derzeit den Dienst Citrix Virtual Apps Essentials oder Citrix Virtual Desktops Essentials abonnieren, führen Sie ein Upgrade auf Citrix DaaS Standard für Azure durch, indem Sie die folgenden Aufgaben ausführen.

1. Erstellen Sie eine neue Organisations-ID (OrgID) zur Verwendung mit dem Citrix DaaS Standard für Azure unter https://onboarding.cloud.com/. (Wie bereits in diesem Artikelbeschrieben, können Sie dieselbe OrgID nicht verwenden, um mehr als eine Citrix DaaS-Edition zu abonnieren.)
2. Wenden Sie sich an den Citrix Vertrieb, um Citrix DaaS Standard für Azure und den Citrix Azure Consumption Fund mit der neuen OrgID zu erwerben. (Sie müssen den Konsumfonds nicht bestellen, aber ohne ihn können Sie nicht auf alle Funktionen von Citrix DaaS Standard für Azure zugreifen.)

3. Melden Sie sich bei Citrix Cloud an. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.
4. Fügen Sie mindestens eines Ihrer Azure-Abonnements für Citrix DaaS Standard für Azure hinzu.
5. Importieren Sie ein oder mehrere Images aus Ihren Azure-Abonnements in Citrix DaaS Standard für Azure.
6. Erstellen Sie Kataloge mit den Images, die Sie aus Ihren Azure-Abonnements importiert haben.
7. Fügen Sie Benutzer zu den von Ihnen erstellten Katalogen hinzu.
8. Wenn Sie dieselbe Workspace-URL beibehalten möchten, die Sie mit Citrix Virtual Apps Essentials oder Citrix Virtual Desktops Essentials verwendet haben:

    a) Melden Sie sich bei Citrix Cloud mit der OrgID an, die Sie mit dem Essentials-Dienst verwenden. Wählen Sie im Menü oben links die Option **Workspace-Konfiguration** aus. Ändern Sie Ihre Workspace-URL in etwas anderes.

    b) Melden Sie sich mit der OrgID, die Sie mit dem Citrix DaaS Standard für Azure verwenden, bei Citrix Cloud an. Wählen Sie im Menü oben links die Option **Workspace-Konfiguration** aus. Ändern Sie die Workspace-URL in die URL, die Sie früher für den Essentials-Dienst verwendet haben.

9. Melden Sie sich bei Azure an und löschen Sie alle Ressourcen, die Sie mit dem Essentials-Dienst verwendet haben. Anleitungen finden Sie unter Stornieren von Virtual Apps Essentials. (Das Verfahren ist für Citrix Virtual Desktops Essentials identisch.)
10. Beenden Sie Ihren Essentials-Service, indem Sie Ihre Azure Marketplace-Ressource in Azure löschen.

Erste Schritte

September 7, 2022

In diesem Artikel werden die Setup-Aufgaben für die Bereitstellung von Desktops und Apps mit Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) zusammengefasst. Wir empfehlen, jedes Verfahren vor der Ausführung durchzulesen, damit Sie gut vorbereitet sind.

Informationen zur Einrichtung von Remote-PC-Zugriff finden Sie unter Remote-PC-Zugriff.

> **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.

Überblick über die Einrichtungsaufgaben

Die folgenden Abschnitte dieses Artikels enthalten Informationen zu den Einrichtungsaufgaben:

1. Bereiten Sie sich auf die Einrichtung vor
2. Richten Sie eine Bereitstellung ein und folgen Sie den Anweisungen in einer von:
    - Schneller Nachweis der Konzeptbereitstellung
    - Bereitstellung in der Produktion
3. Stellen Sie Ihren Benutzern die Workspace-URL zur Verfügung.

Vorbereiten

- Wenn Sie mit Katalogen, Images, Netzwerkverbindungen oder Azure-Abonnements nicht vertraut sind, lesen Sie die einführenden Konzepte und Terminologieinformationen .
- Lesen Sie die Sicherheitsübersicht, um zu erfahren und zu verstehen, wofür Sie (der Kunde) und Citrix verantwortlich sind.
- Wenn Sie noch kein Citrix Cloud-Konto haben, das für diesen Dienst verwendet werden kann, holen Sie sich eines und melden Sie sich dann für den Dienst an.
- Überprüfen Sie die Systemanforderungen.
- Überprüfen Sie die Einrichtungsschritte: Machbarkeitsnachweis oder Produktion.

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 die Domäne eingebundene Maschinen verwenden, vergewissern Sie sich, dass Sie über gültige DNS-Servereinträge verfügen.
3. Wenn Sie Ihr eigenes Azure-Abonnement verwenden (anstelle eines Citrix Managed Azure-Abonnements), importieren Sie Ihr Azure-Abonnement.
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.

Nachdem Sie die Bereitstellung eingerichtet haben, verwenden Sie das **Monitor-Dashboard** in Citrix DaaS für Azure, um die Desktopnutzung, Sitzungenund Maschinenanzuzeigen.

Systemanforderungen

Für alle Bereitstellungen:

- **Citrix Cloud:** Dieser Dienst wird über die Citrix Cloud bereitgestellt und benötigt ein Citrix Cloud-Konto, um den Onboarding-Prozess abzuschließen. Einzelheiten finden Sie unter Holen Sie sich ein Citrix Cloud-Konto.
- **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.

Wenn Sie ein Citrix Managed Azure-Abonnement verwenden:

- **Azure-Abonnements bei Verwendung von Azure VNet Peering (optional):** Wenn Sie planen, über Azure VNet-Peer-Verbindungen auf Ressourcen (wie AD und andere Dateifreigaben) in Ihrem eigenen Azure-Netzwerk zuzugreifen, müssen Sie über ein Azure-Abonnement verfügen.
- **Verbinden von VDAs mit Azure Active Directory (optional):** Um VDAs mithilfe der Active Directory-Gruppenrichtlinie mit einer Domäne zu verbinden, müssen Sie ein Administrator sein, der die Berechtigung zum Ausführen dieser Aktion in Active Directory hat. Einzelheiten 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, bevor Sie sie in Citrix DaaS für Azure importieren.

Zusätzliche Informationen:

- Anforderungen an die Internetverbindung: System- und Konnektivitätsanforderungen.
- Ressourcenlimits in einer Service-Bereitstellung: Limits.

Unterstützte Betriebssysteme

Bei Verwendung eines Citrix Managed Azure-Abonnements:

- Windows 7 (VDA: 7.15 LTSR mit dem neuesten kumulativen Update)
- Windows 10 (Einzelsitzungs-OS)
- Windows 10 (Multisitzungs-OS)
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (erfordert mindestens VDA 2106)
- Red Hat Enterprise Linux und Ubuntu

Bei Verwendung eines vom Kunden verwalteten Azure-Abonnements:

- Windows 7 (VDA: 7.15 LTSR mit dem neuesten kumulativen Update)
- 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
- Windows Server 2022 (erfordert mindestens VDA 2106)
- Red Hat Enterprise Linux und Ubuntu

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.

Zeigen Sie im Dashboard **Verwalten > Azure Quick Deploy** die URL an, indem Sie auf der rechten Seite **Benutzerzugriff und Authentifizierung** erweitern.

Sie können den ersten Teil der Workspace-URL in Citrix Cloud ändern. Anweisungen finden Sie unter Anpassen der Arbeitsbereich-URL.

Hilfe und Unterstützung

Lesen Sie den Artikel Problembehandlung.

Können Probleme mit dem Service nicht gelöst werden, erstellen Sie ein Supportticket. Folgen Sie hierfür den Anweisungen unter Hilfe und Support.

Kataloge erstellen

October 7, 2022

Bei Verwendung für veröffentlichte Desktops und Apps ist ein Katalog eine Gruppe identischer virtueller Maschinen. Wenn Sie Desktops bereitstellen, werden die Computer im Katalog für ausgewählte Benutzer freigegeben. Wenn Sie Anwendungen veröffentlichen, hosten mehrere Sitzungsmaschinen Anwendungen, die für ausgewählte Benutzer freigegeben werden.

> **Hinweis:**
>
> Informationen zum Erstellen von Remote-PC-Zugriffskatalogen finden Sie unter Remote-PC-Zugriff.

Maschinentypen

Ein 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 Maschinentypen manchmal als "Desktop-Typ"bezeichnet.

Möglichkeiten zum Erstellen eines Katalogs

Es gibt mehrere Möglichkeiten, einen Katalog zu erstellen und zu konfigurieren:

- Die **Schnellerstellung** ist der schnellste Einstieg. Sie stellen nur minimale Informationen zur Verfügung, und Citrix DaaS für Azure 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 aus: Von Citrix vorbereitete Images, Ihre Images, die Sie aus Azure importieren, oder Images, die Sie in Citrix DaaS für Azure aus einem von Citrix vorbereiteten 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.
Muss ein Citrix Managed Azure-Abonnement verwenden.	Kann das Citrix Managed Azure oder Ihr eigenes Azure-Abonnement verwenden.

Einzelheiten finden Sie in den folgenden Abschnitten:

- Erstellen Sie einen Katalog mit Quick Create
- Erstellen eines benutzerdefinierten Katalogs

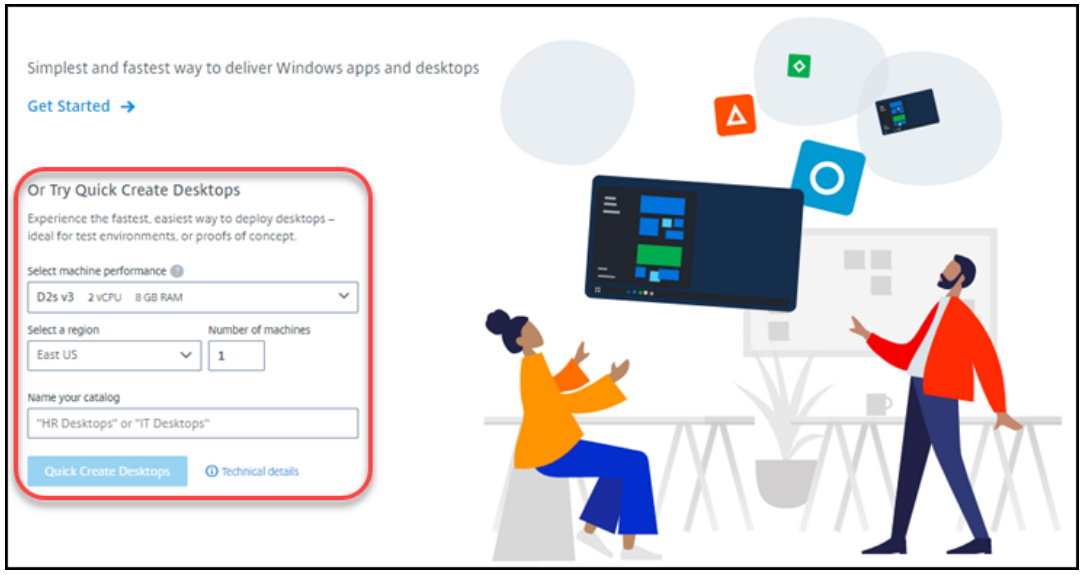
Erstellen Sie einen Katalog mit Quick Create

Diese Katalogerstellungsmethode verwendet immer ein Citrix Managed Azure-Abonnement.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.

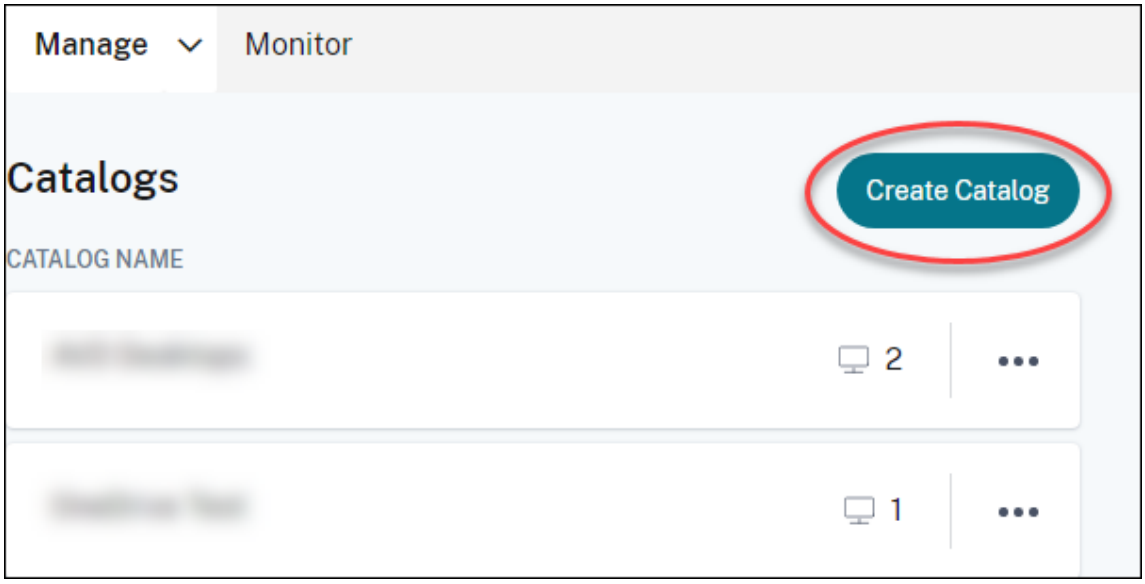
3. Wenn noch kein Katalog erstellt wurde, werden Sie zur **Willkommensseite** für die Quick Deploy weitergeleitet. Treffen Sie eine Auswahl:

   - Konfigurieren Sie den Katalog auf dieser Seite. Fahren Sie mit den Schritten 6 bis 10 fort.

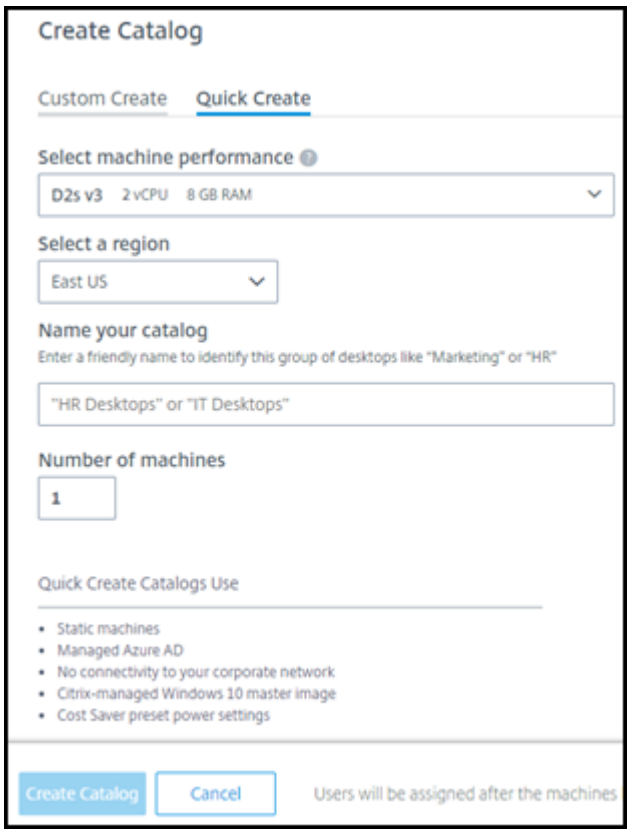


   - Klicken Sie auf **Erste Schritte**. Sie werden zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet. Klicken Sie auf **Katalog erstellen**.

4. Wenn bereits ein Katalog erstellt wurde (und Sie einen anderen erstellen), werden Sie zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet. Klicken Sie auf **Katalog erstellen**.



5. Klicken Sie oben auf der Seite auf **Quick Create**, falls diese 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 können 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.

6. Wenn Sie fertig sind, klicken Sie auf **Katalog erstellen**. (Wenn Sie den ersten Katalog auf der **Willkommensseite** “Quick Deploy”**erstellen, klicken Sie auf Desktops schnell erstellen**.)

Sie werden automatisch zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet. Während der Katalog erstellt wird, wird sein Name zur Liste der Kataloge hinzugefügt, was den Fortschritt seiner Erstellung anzeigt.

Citrix DaaS für Azure erstellt außerdem automatisch einen Ressourcenstandort und fügt zwei Cloud Connectors hinzu.

Nachfolgende Schritte:

- Wenn Sie Citrix Managed Azure AD für die Benutzerauthentifizierung verwenden, können Sie dem Verzeichnis Benutzer hinzufügen, während der Katalog erstellt wird.

- Unabhängig davon, welche Benutzerauthentifizierungsmethode Sie verwenden, fügen Sie nach der Erstellung des Katalogs Benutzer zum Katalog hinzu.

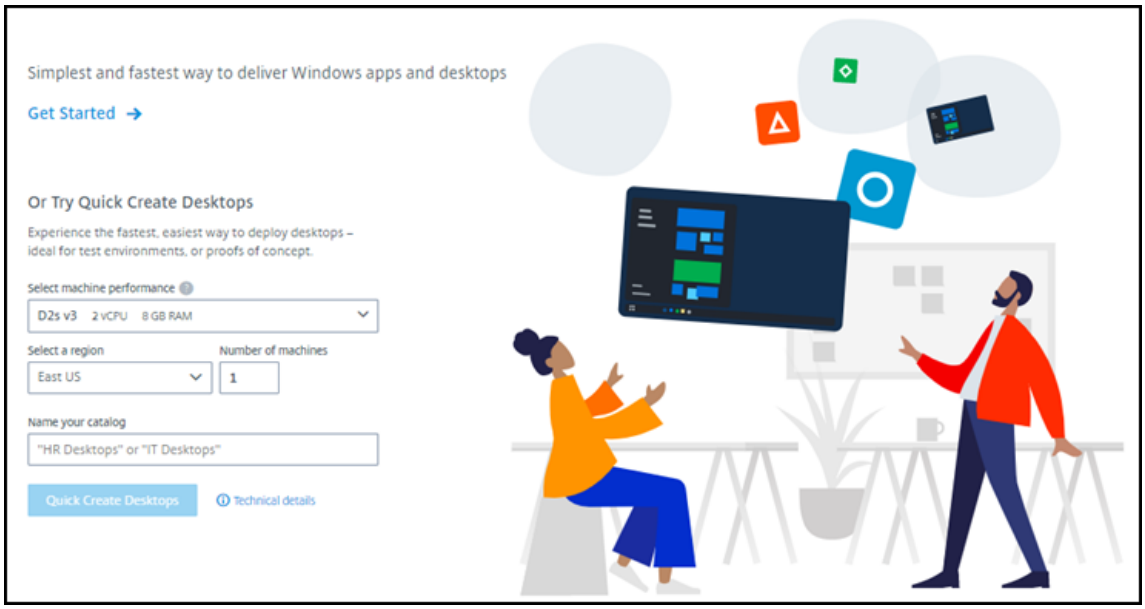
Erstellen eines benutzerdefinierten Katalogs

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.

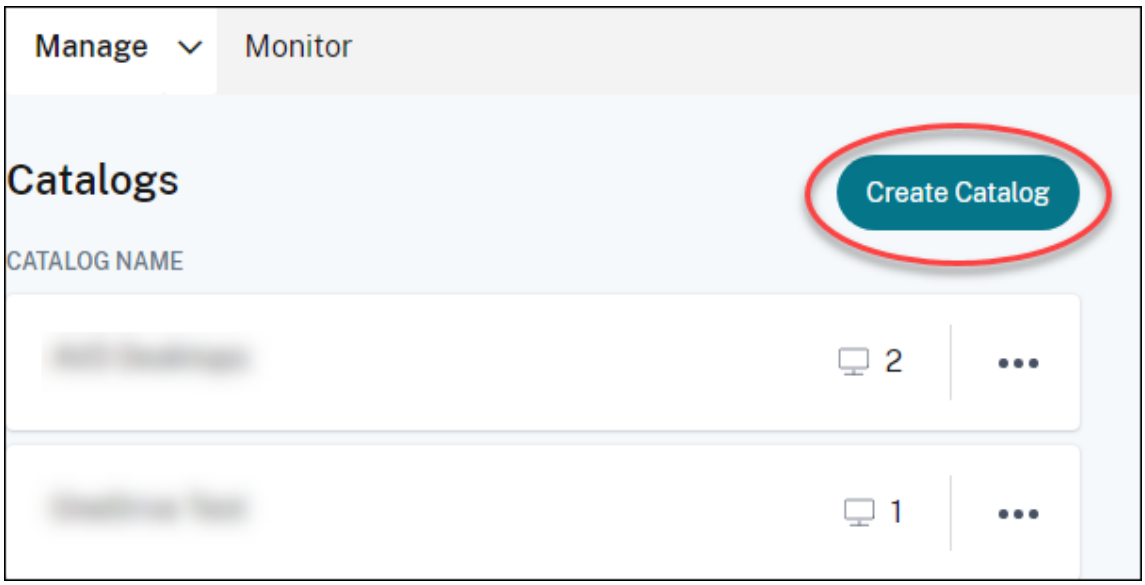
Wenn Sie kein Citrix Managed Azure-Abonnement haben, müssen Sie mindestens eines Ihrer eigenen Azure-Abonnements in Citrix DaaS für Azure importieren (hinzufügen), bevor Sie einen Katalog erstellen.

Gehen Sie zum Erstellen eines Katalogs wie folgt vor:

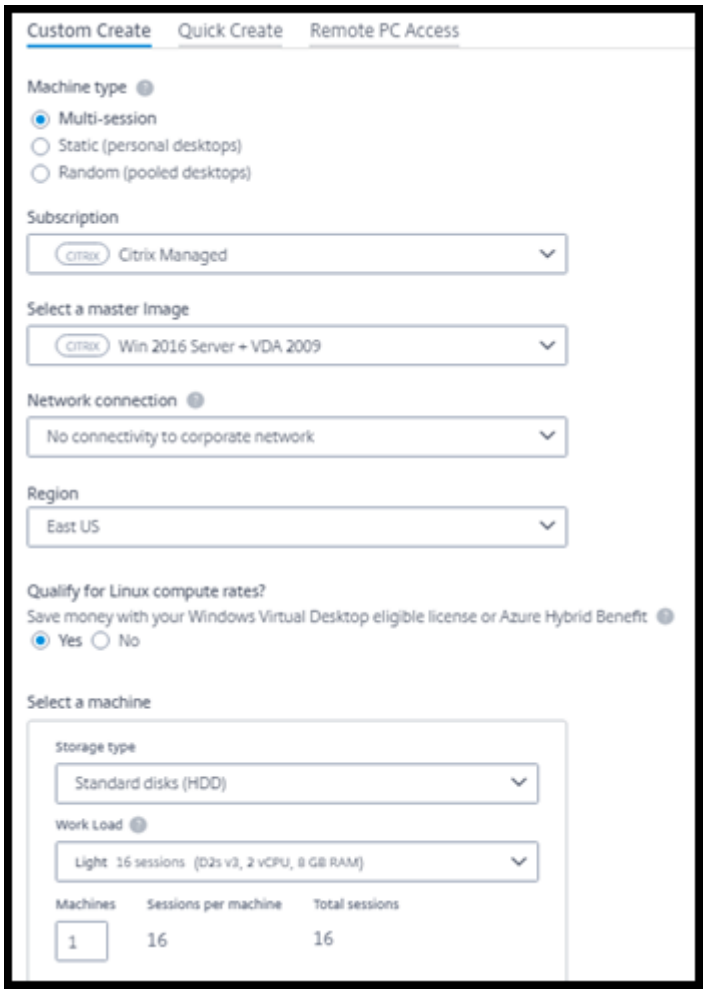
1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.
3. Wenn noch kein Katalog erstellt wurde, werden Sie zur **Willkommensseite** für die Quick Deploy weitergeleitet. Klicken Sie auf **Erste Schritte**. Am Ende der Einführungsseite gelangen Sie zum Dashboard **Verwalten > Azure Quick Deploy** . Klicken Sie auf **Katalog erstellen**.



Wenn bereits ein Katalog erstellt wurde, werden Sie zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet. Klicken Sie auf **Katalog erstellen**.



4. Wählen Sie oben auf der Seite **Benutzerdefinierte Erstellung** (falls die Option noch nicht ausgewählt ist).



5. 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 aus. Einzelheiten finden Sie unter Azure-Abonnements.
   - **Masterimage:** Wählen Sie ein Betriebssystemimage aus. Einzelheiten finden Sie unter Images.
   - **Netzwerkverbindung:** Wählen Sie die Verbindung aus, die für den Zugriff auf Ressourcen in Ihrem Netzwerk verwendet werden soll. Einzelheiten finden Sie unter Netzwerkverbindungen.
     - Für ein Citrix Managed Azure-Abonnement sind folgende Optionen:
       * **Keine Verbindung:** Die Benutzer können nicht auf Standorte und Ressourcen in Ihrem On-Premises-Unternehmensnetzwerk zugreifen.
       * *Verbindungen:* Wählen Sie eine Verbindung aus, z. B. ein VNet-Peering oder eine SD-WAN-Verbindung.
     - Wählen Sie für ein vom Kunden verwaltetes Azure-Abonnement die entsprechende 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 in der **Netzwerkverbindung**einen Verbindungsnamen 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.

     Vorteil von Azure Virtual Desktop: Berechtigte Windows 10 oder Windows 7 pro 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:** Standarddatenträger (HDD), Standard-SSD oder Premium-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.
- **Benennungsschema für Maschinen:** siehe Benennungsschema für Maschinen.
- **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.

6. Wenn Sie fertig sind, klicken Sie auf **Katalog erstellen**.

Das Dashboard **Verwalten > Azure Quick Deploy** zeigt an, wann Ihr Katalog erstellt wurde Citrix DaaS für Azure erstellt außerdem automatisch einen Ressourcenstandort und fügt zwei Cloud Connectors hinzu.

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).

Erstellen von Katalogen von mit der Azure AD-Domäne verbundenen Maschinen

Sie können benutzerdefinierte Erstellung verwenden, um Kataloge von Maschinen zu erstellen, die mit Ihrem Azure Active Directory verknüpft sind.

Anforderungen

Ihre Bereitstellung muss Citrix Cloud Connectors enthalten. Machine Creation Services stellt Ihre Cloud Connectors basierend auf den Informationen bereit, die Sie beim Erstellen eines Katalogs über Ihre Azure AD-Domäne bereitstellen.

Diese Art von Katalog kann nur zum Provisioning statischer oder zufälliger Maschinen verwendet werden. Provisioning von Maschinen mit mehreren Sitzungen wird derzeit nicht unterstützt.

Verbinden Sie das Masterimage nicht mit Azure AD, bevor Sie einen Katalog erstellen. Citrix MCS verbindet das Masterimage mit Azure AD, wenn der Katalog erstellt wird.

Verwenden Sie VDA-Version 2203 oder höher.

Weisen Sie im Azure-Portal den virtuellen Maschinen im Katalog die IAM-Rolle "Benutzeranmeldung für virtuelle Maschinen"zu. Sie können dies auf verschiedene Arten tun:

- Am sichersten: Wenn Sie statische Maschinen erstellen, weisen Sie die Rolle dem Benutzer zu, der der Maschine zugewiesen ist.
- Alternative Methode: Weisen Sie die Rolle in den Ressourcengruppen, die die virtuellen Maschinen enthalten, allen Benutzern mit Zugriff auf den Katalog zu.
- Am wenigsten sicher: Weisen Sie die Rolle in den Abonnements allen Benutzern mit Zugriff auf den Katalog zu.

Legen Sie die Workspace-Authentifizierung so fest, dass das Azure AD verwendet wird, das Sie mit den Maschinen im Katalog verbinden. Anweisungen finden Sie unter Konfigurieren der Benutzerauthentifizierung in Citrix Cloud.

Weitere Informationen zu Anforderungen, bekannten Problemen und Überlegungen finden Sie in den Informationen zu reinen Azure-AD-verbundenen VDA-Konfigurationen in der Konfiguration eines mit Azure Active Directory verbundenen und einer nicht domänenverbundenen VDA-Konfiguration.

So erstellen Sie einen Katalog

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.
3. Wählen Sie **Verwalten > Azure Quick Deploy**.
4. Wenn noch kein Katalog erstellt wurde, werden Sie zur **Willkommensseite** weitergeleitet. Wählen Sie **Erste Schritte** aus. Am Ende der Einführungsseite werden Sie zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet. Wählen Sie **Katalog erstellen**. Wenn bereits ein Katalog erstellt wurde, werden Sie zum Dashboard **Verwalten > Azure 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.

    - **Typ der Maschine.** Wählen Sie **Statisch (persönliche Desktops)** oder **Zufällig (gepoolte Desktops) aus**.
    - **Abonnement:** Wählen Sie Ihr Azure-Abonnement aus.
    - **Masterimage.** Wählen Sie ein Betriebssystemimage aus, das für die Maschinen in den Katalogen verwendet werden soll.
    - **Netzwerkverbindung.** Wählen Sie die entsprechende Ressourcengruppe, das virtuelle Netzwerk und das Subnetz aus.
    - **Domain-Konfiguration**. Wählen Sie **Azure Active Directory** als Ihren Domänentyp aus. Möglicherweise wird eine Warnung angezeigt, die Sie daran erinnert, die Workspace-Authentifizierung für dieses Azure AD festzulegen.

7. Vervollständigen Sie den Rest des Assistenten, um den Katalog zu erstellen.

Einstellungen für den Ressourcenstandort beim Erstellen eines Katalogs

Beim Erstellen eines Katalogs können Sie optional mehrere Ressourcenstandorteinstellungen konfigurieren.

Wenn Sie im Dialogfeld Quick Deploy-Katalogerstellung auf **Erweiterte Einstellungen** klicken, ruft Citrix DaaS für Azure 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 mit den erweiterten Einstellungen fertig sind, klicken Sie auf **Speichern**, um zum Dialogfeld zur Katalogerstellung Quick Deploy 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 mit Schnellbereitstellung 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. Es wird 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 für Azure das Standardbenennungsschema DAS%%%%%-**-###.

- %%%%% = fünf zufällige alphanumerische Zeichen, die dem Präfix des Ressourcenstandorts entsprechen
- ** = zwei zufällige alphanumerische Zeichen für den Katalog
- ### = drei Ziffern.

Verwandte Informationen

- Domaingebundene und nicht domänengebundene Maschinen.
- Kataloge für Remote-PC-Zugriff.
- Erstellen Sie einen Katalog in einem Netzwerk, das einen Proxyserver verwendet.
- Zeigt Kataloginformationenan.

Remote-PC-Zugriff

September 7, 2022

Einführung

> **Hinweis:**
>
> In diesem Artikel wird beschrieben, wie Sie Remote-PC-Zugriff konfigurieren, wenn Sie die Quick Deploy-Verwaltungsschnittstelle in Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) verwenden. Informationen zum Konfigurieren von Remote-PC-Zugriff bei Verwendung der Vollkonfigurationsverwaltungsoberfläche finden Sie unter Remote-PC-Zugriff.

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.

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 den Dienst Citrix DaaS Standard für Azure.

   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. Über die Citrix DaaS für Azure Quick Deploy-Verwaltungsschnittstelle

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.

Allgemein:

- 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.
- Wenn Sie an den Remote-PC-Zugriff mit Citrix Virtual Apps and Desktops gewohnt sind: Die Wake-on-LAN-Funktion ist in Citrix DaaS für Azure 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.
  - Dual-Boot-Maschinen.

- 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.
  - Stellen *Sie die Aktion zum Drücken der Ein-/Aus-Taste* auf **Herunterfahren**.
  - 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 jedoch erneut andocken, wechselt der VDA erst, um die Kabelverbindung zu verwenden, wenn Sie den drahtlosen Adapter trennen. 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 geschwärzt werden und zeigt Sitzungsaktivitäten 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.

Überlegungen zum Arbeitsplatz:

- 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 optionalen Komponenten. Die Option `/includeadditional` gibt genau an, welche Komponenten Sie installieren möchten.

  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 oben links **Meine Services > DaaS Standard für Azure** aus.
3. Wenn Sie noch keine Kataloge erstellt haben, klicken Sie auf der **Willkommensseite** für die Quick Deploy auf **Erste Schritte**. Wenn Sie einen Katalog erstellt haben, klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** auf **Katalog erstellen**.
4. Wählen Sie auf der Registerkarte **Remote-PC-Zugriff** eine Methode zum Zuweisen von Benutzern zu Maschinen.
5. Geben Sie einen Namen für den Katalog ein und wählen Sie den von Ihnen erstellten Ressourcenstandort aus.

6. Fügen Sie Maschinen hinzu.
7. Klicken Sie auf **Katalog erstellen**.
8. Klicken Sie auf der Seite **Ihr Remote-PC-Zugriff-Katalog wird erstellt** auf **Fertig**.
9. Ein Eintrag für den neuen Katalog wird im **Manage** Dashboard 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 Konfigurationsinformationen eines Remote-PC-Access-Katalogs anzuzeigen oder zu ändern, wählen Sie den Katalog im Dashboard **Verwalten > Azure Quick Deploy** aus (klicken Sie auf eine beliebige Stelle im Eintrag).

- 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.

Azure-Abonnements

December 28, 2023

Einführung

Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) unterstützt sowohl Citrix Managed Azure-Abonnements als auch Ihre eigenen, vom Kunden verwalteten Azure-Abonnements.

- Um Ihre eigenen Azure-Abonnements zu verwenden, importieren (fügen) Sie zunächst eines oder mehrere dieser Abonnements in Citrix DaaS für Azure hinzu. Diese Aktion ermöglicht es Citrix DaaS für Azure, auf Ihre Azure-Abonnements zuzugreifen.
- Die Verwendung eines Citrix Managed Azure-Abonnements erfordert keine Abonnementkonfiguration. Um jedoch ein Citrix Managed Azure-Abonnement verfügbar zu haben, müssen Sie den Citrix Azure Consumption Fund bestellt haben (zusätzlich zum Citrix DaaS Standard für Azure).

Wenn Sie einen Katalog erstellen oder ein Image erstellen, wählen Sie zwischen den verfügbaren Azure-Abonnements aus.

Einige Dienstfunktionen unterscheiden sich je nachdem, ob sich die Computer in einem Citrix Managed Azure-Abonnement oder in Ihrem eigenen Azure-Abonnement befinden.

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 (und ist die Standardabonnementauswahl) beim Erstellen von Katalogen und Images.	Sie müssen das Azure-Abonnement für Citrix DaaS für Azure hinzufügen, bevor Sie einen Katalog erstellen.
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 verwenden, um eine Verbindung zu Ihren Ressourcen herzustellen, müssen Sie in Citrix DaaS für Azure eine VNet-Peer-Verbindung 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.

Abonnements anzeigen

Um Abonnementdetails anzuzeigen, blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure die Option **Cloud-Abonnements** auf der rechten Seite ein. Klicken Sie dann auf einen Abonnementeintrag.

- Die Seite **Details** enthält die Anzahl der Maschinen sowie die Nummern und Namen der Kataloge und Images im Abonnement.
- 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 Standard für Azure hinzufügen, bevor Sie einen Katalog oder ein Image erstellen, das dieses Abonnement verwendet. Sie haben zwei Möglichkeiten, wenn Sie Ihre Azure-Abonnements hinzufügen:

- **Wenn Sie ein globaler Administrator für das Verzeichnis sind und Besitzerrechte für das Abonnement haben:** Authentifizieren Sie sich einfach bei Ihrem Azure-Konto.
- **Wenn Sie kein globaler Administrator sind und über Besitzerrechte für das Abonnement verfügen:** Bevor Sie das Abonnement zu Citrix DaaS für Azure hinzufügen, erstellen Sie eine Azure-App in Ihrem Azure AD und fügen Sie diese App dann als Mitwirkender zum Abonnement hinzu. Wenn Sie dieses Abonnement zu Citrix DaaS für Azure hinzufügen, geben Sie relevante App-Informationen an.

Hinzufügen kundenverwalteter Azure-Abonnements als globaler Administrator

Für diese Aufgabe sind globale Administratorrechte für das Verzeichnis und Besitzerrechte für das Abonnement erforderlich.

1. Erweitern Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure die Option **Cloud-Abonnements** auf der rechten Seite.
2. Klicken Sie auf **Azure-Abonnement hinzufügen**.
3. Klicken Sie auf der Seite **Abonnements hinzufügenauf Azure-Abonnement**hinzufügen.
4. Wählen Sie die Schaltfläche, über die Citrix DaaS für Azure in Ihrem Namen auf Ihre Azure-Abonnements zugreifen kann.
5. Klicken Sie auf **Azure-Konto authentifizieren**. Sie werden zur Azure-Anmeldeseite weitergeleitet.
6. Geben Sie Ihre Azure-Anmeldeinformationen ein.

7. Sie kehren automatisch zu Citrix DaaS für Azure zurück. 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, klicken Sie auf **Abonnements hinzufügen**.
8. Bestätigen Sie, dass Sie die ausgewählten Abonnements hinzufügen möchten.

Die von Ihnen ausgewählten Azure-Abonnements werden aufgeführt, wenn Sie **Abonnements** erweitern. Beim Erstellen eines Katalogs oder Images stehen hinzugefügte Abonnements zur Auswahl.

Hinzufügen kundenverwalteter Azure-Abonnements ohne Konto des globalen Administrators

Das Hinzufügen eines Azure-Abonnements, wenn Sie kein globaler Administrator sind, ist ein zweiteiliger Prozess:

- Bevor Sie ein Abonnement für Citrix DaaS für Azure hinzufügen, erstellen Sie eine App in Azure AD und fügen Sie diese App dann als Mitwirkenden des Abonnementshinzu.
- Fügen Sie das Abonnement für Citrix DaaS für Azurehinzu, indem Sie Informationen zur App verwenden, 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) Klicken Sie in der Liste **Verwalten** auf **App-Registrierungen**.
   d) Klicken Sie auf **+ Neue Registrierung**.
   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) Klicken Sie auf **Erstellen**.
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 werden dies später verwenden, wenn Sie Ihr Abonnement für Citrix DaaS für Azure 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. Klicken Sie dann auf **Hinzufügen**.

f) Notieren Sie sich den geheimen Clientschlüssel. Sie werden dies später verwenden, wenn Sie Ihr Abonnement für Citrix DaaS für Azure hinzufügen.

g) Wählen Sie das Azure-Abonnement aus, das Sie mit Citrix DaaS für Azure verknüpfen (hinzufügen) möchten, und klicken Sie dann auf **Zugriffssteuerung (IAM)**.

h) Klicken Sie im Feld **Rollenzuweisung hinzufügen** auf **Hinzufügen**.

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) Klicken Sie auf **Speichern**.

Fügen Sie Ihr Abonnement für Citrix DaaS für Azure hinzu Sie benötigen die Anwendungs-ID, die Verzeichniskennung und den geheimen Wert des Clients von der App, die Sie in Azure AD erstellt haben.

1. Erweitern Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure die Option **Cloud-Abonnements** auf der rechten Seite.
2. Klicken Sie auf **Azure-Abonnement hinzufügen**.
3. Klicken Sie auf der Seite **Abonnements hinzufügenauf Azure-Abonnements**hinzufügen.
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.

Später können Sie auf der **Detailseite** des Abonnements im Citrix DaaS für Azure-Dashboard das Client-Geheimnis aktualisieren oder die Azure-App über das Auslassungsmenü ersetzen.

Wenn Citrix DaaS für Azure nach dem Hinzufügen nicht auf ein Azure-Abonnement zugreifen kann, sind mehrere Katalogenergieverwaltungen und einzelne Maschinenaktionen 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 die in Limits angegebene Anzahl von Computern. (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 (oder Maschinen zu einem Katalog hinzufügen), wenn die Gesamtzahl der Maschinen für alle Kataloge, die dieses Citrix Managed Azure-Abonnement verwenden, den in Limits angegebenen Wert 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 im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure die Option **Cloud-Abonnements** auf der rechten Seite.
3. Klicken Sie auf **Azure-Abonnement hinzufügen**.
4. Wählen Sie auf der Seite **Abonnements hinzufügen** die Option **Von Citrix verwaltetes Azure-Abonnement hinzufügen**.
5. Klicken **Sie auf der Seite Verwaltetes Citrix Abonnementhinzufügen** unten auf der Seite auf 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

Um ein Azure-Abonnement zu entfernen, müssen Sie zuerst 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 im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure die Option **Cloud-Abonnements** auf der rechten Seite.
2. Klicken Sie auf den Abonnementeintrag.
3. Klicken Sie auf der Registerkarte **Details** auf **Abonnement entfernen**.
4. Klicken Sie auf **Azure-Konto authentifizieren**. Sie werden zur Azure-Anmeldeseite weitergeleitet.
5. Geben Sie Ihre Azure-Anmeldeinformationen ein.
6. Sie kehren automatisch zu Citrix DaaS für Azure zurück. Bestätigen Sie die Löschung in den Kontrollkästchen, und klicken Sie dann auf **Ja, Abonnement löschen**.

Netzwerkverbindungen

May 9, 2023

Einführung

Dieser Artikel enthält Details zu verschiedenen Bereitstellungsszenarien bei Verwendung eines Citrix Managed Azure-Abonnements.

Beim Erstellen eines Katalogs geben Sie an, ob und wie Benutzer über ihre Desktops und Apps Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure) auf Standorte und Ressourcen in ihrem on-premises Unternehmensnetzwerk zugreifen.

Wenn Sie ein Citrix Managed Azure-Abonnement verwenden, gibt es folgende Optionen:

- Keine Konnektivität
- Azure VNet-Peering
- SD-WAN

Wenn Sie eines Ihrer eigenen, vom Kunden verwalteten Azure-Abonnements verwenden, müssen Sie keine Verbindung zu Citrix DaaS für Azure herstellen. Sie fügen einfach das Azure-Abonnement zu Citrix DaaS für Azurehinzu.

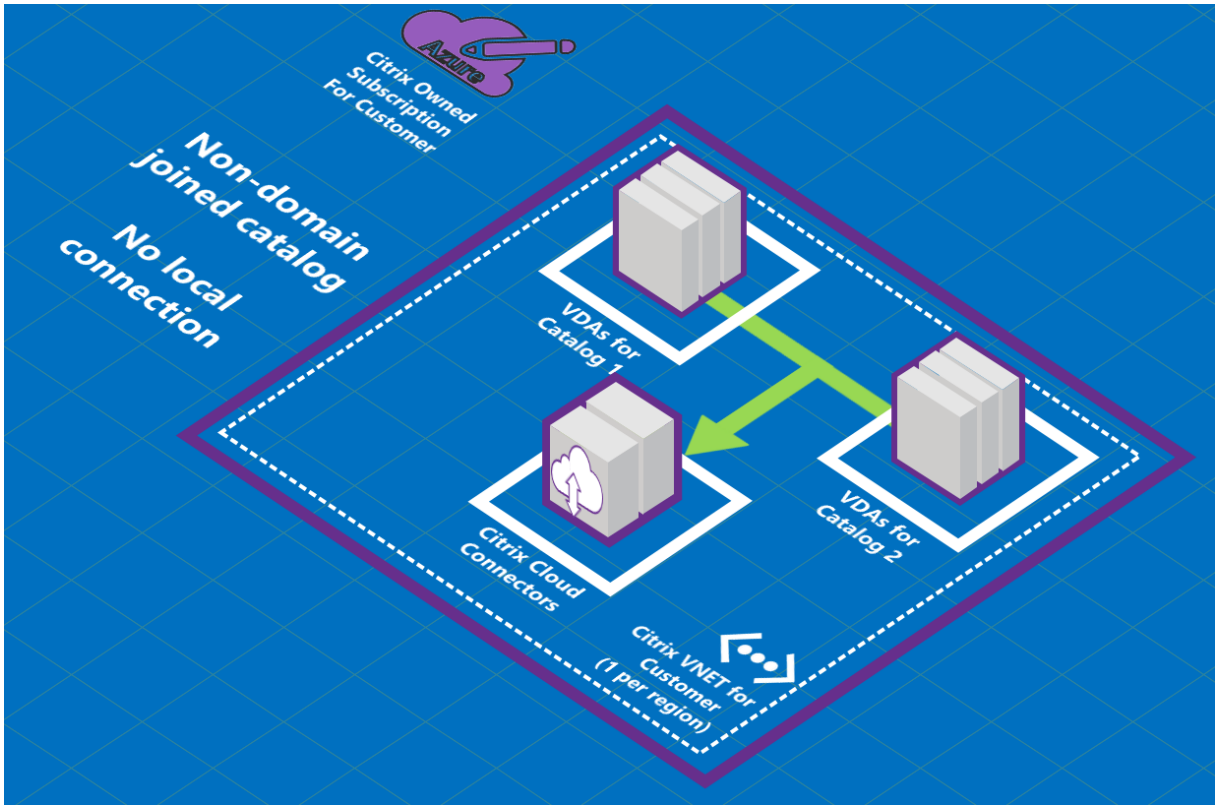
Sie können den Verbindungstyp eines Katalogs nach dessen Erstellung nicht mehr ändern.

Anforderungen für alle Netzwerkverbindungen

- Beim Erstellen einer Verbindung müssen Sie über gültige DNS-Servereinträge verfügen.
- Wenn Sie Secure DNS oder einen DNS-Drittanbieter verwenden, müssen Sie den Adressbereich, der für die Verwendung durch Citrix DaaS für Azure zugewiesen ist, den IP-Adressen des DNS-Anbieters in der Zulassungsliste hinzufügen. Dieser Adressbereich wird beim Erstellen einer Verbindung angegeben.
- Alle Dienstressourcen, die die Verbindung verwenden (in die Domäne verbundene Computer), müssen in der Lage sein, Ihren Network Time Protocol (NTP) -Server zu erreichen, um die Zeitsynchronisierung sicherzustellen.

Keine Konnektivität

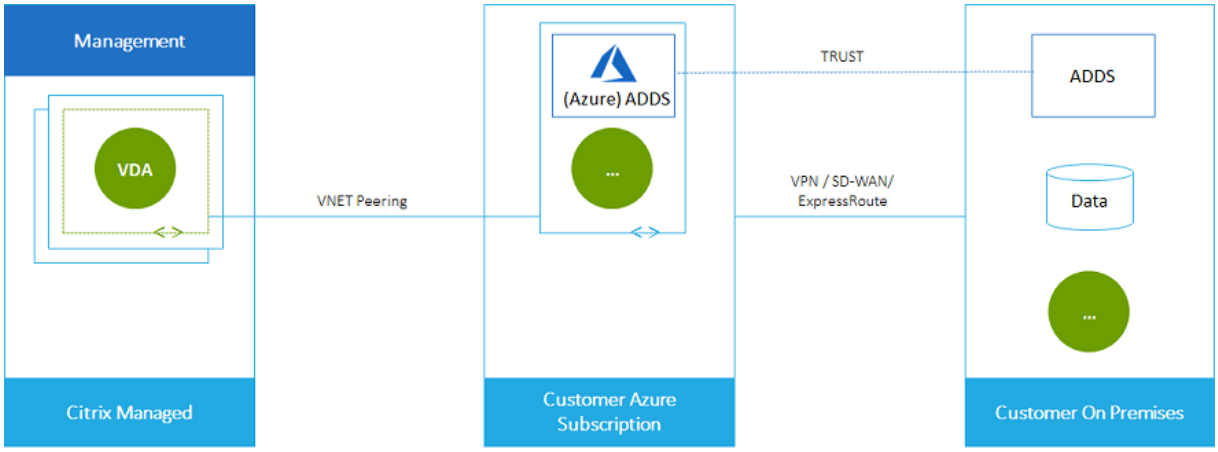
Wenn ein Katalog mit **Keine Konnektivität**konfiguriert ist, können Benutzer nicht auf Ressourcen in ihren on-premises oder anderen Netzwerken zugreifen. Dies ist die einzige Wahl, wenn Sie einen Katalog mit Quick Create erstellen.



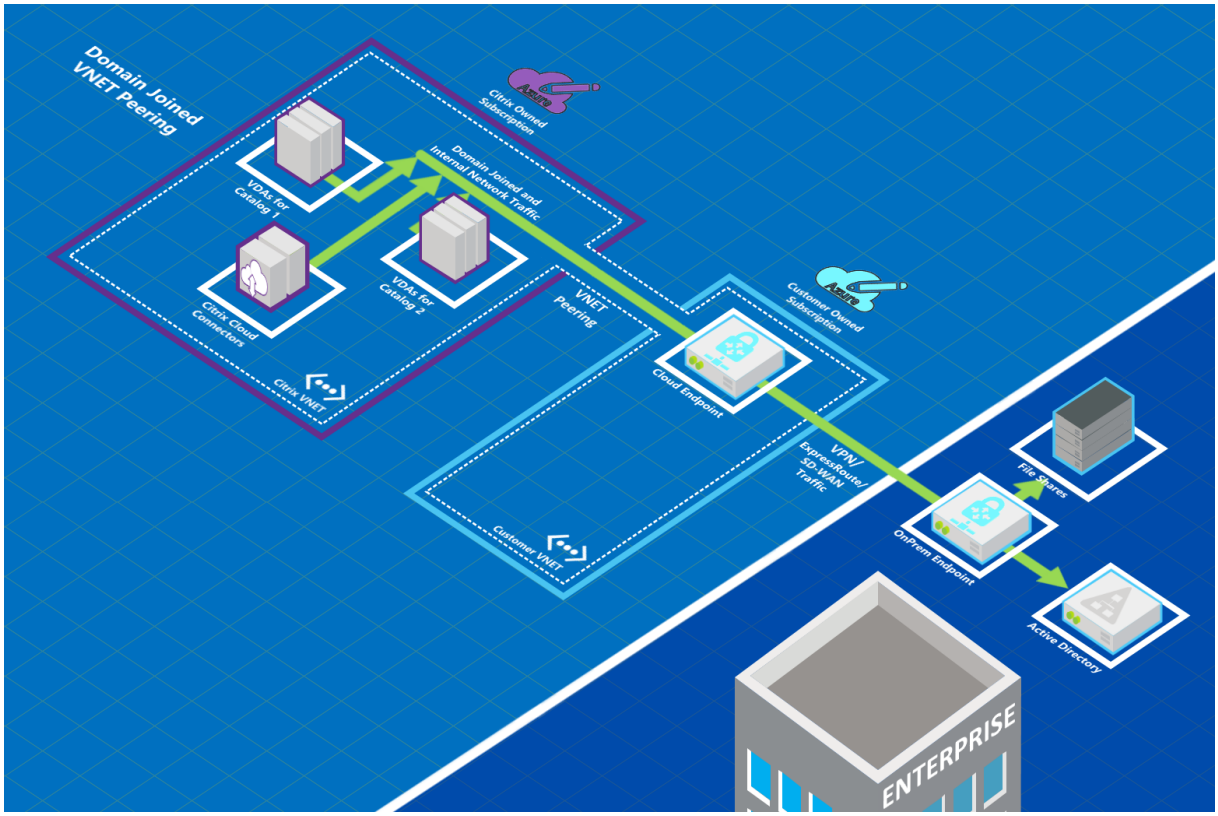
Informationen zu Azure VNet-Peering-Verbindungen

Das Peering eines virtuellen Netzwerks verbindet nahtlos zwei virtuelle Azure-Netzwerke (VNets): Ihres und das Citrix DaaS für Azure VNet. 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 mit Azure VNet Peering aus dem Citrix Managed Azure-Abonnement für das VNet im Azure-Abonnement Ihres Unternehmens.



Hier ist eine weitere Illustration des VNet-Peering.



Benutzer können auf ihre On-Premises-Netzwerkressourcen (z. B. Dateiserver) zugreifen, indem sie beim Erstellen eines Katalogs der lokalen Domäne beitreten. (Das heißt, Sie treten der AD-Domäne bei, in der sich Dateifreigaben und andere benötigte Ressourcen befinden.) Ihr Azure-Abonnement stellt eine Verbindung zu diesen Ressourcen her (in der Grafik unter Verwendung eines VPN oder Azure ExpressRoute). Beim Erstellen des Katalogs geben Sie die Anmeldeinformationen für die Domäne, die Organisationseinheit und das Konto an.

> **Wichtig:**
>
> - Erfahren Sie mehr über VNet-Peering, bevor Sie es in Citrix DaaS für Azure verwenden.
> - Erstellen Sie die VNet-Peering-Verbindung vor dem Katalog, der sie verwenden soll.

Azure VNet Peering-benutzerdefinierte 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. Sie können benutzerdefinierte Routen verwenden, wenn es Netzwerke gibt, auf die Citrix DaaS für Azure-Ressourcen voraussichtlich zugreifen, die jedoch nicht direkt über 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:

- Sie müssen über ein vorhandenes virtuelles Azure-Netzwerkgateway oder eine Netzwerk-Appliance wie Citrix SD-WAN in Ihrer Citrix DaaS für Azure-Umgebung verfügen.
- Wenn Sie benutzerdefinierte Routen hinzufügen, müssen Sie die Routing-Tabellen Ihres Unternehmens mit den Citrix DaaS für Azure-Ziel-VNet-Informationen aktualisieren, um eine End-to-End-Konnektivität sicherzustellen.
- Benutzerdefinierte Routen werden in Citrix DaaS für Azure in der Reihenfolge angezeigt, in der sie eingegeben wurden. 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 hinzufügen, wenn Sie eine Azure VNet-Peering-Verbindung erstellen, oder zu vorhandenen Routen in Ihrer Citrix DaaS für Azure-Umgebung. Wenn Sie alle Vorbereitungen für benutzerdefinierte Routen mit Ihrem VNet-Peering getroffen haben, lesen Sie die folgenden Abschnitte in diesem Artikel:

- Für benutzerdefinierte Routen mit neuen Azure VNet-Peerings: Erstellen einer Azure VNet-Peering-Verbindung
- Für benutzerdefinierte Routen mit vorhandenen Azure VNet-Peerings: Verwalten Sie benutzerdefinierte Routen für bestehende Azure VNet-Peer-Verbindungen

Anforderungen und Vorbereitung von Azure VNet Peering-Anforderungen

- Anmeldeinformationen für einen Besitzer eines Azure Resource Manager-Abonnements Dies muss ein Azure Active Directory-Konto sein. Citrix DaaS für Azure unterstützt keine anderen Kontotypen wie live.com oder externe Azure AD-Konten (in einem anderen Mandanten).
- 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 bis zum angegebenen IP-Bereich.
- **Active Directory:** Für in Domäne verbundene Szenarien empfehlen wir, dass Sie eine Form von Active Directory-Diensten im Peered-VNet ausführen. Dies nutzt die Eigenschaften der Azure VNet-Peering-Technologie mit geringer Latenz.

Die Konfiguration könnte beispielsweise Azure Active Directory Domain Services 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 die verwaltete Domäne zu löschen. Daher ist es wichtig, das richtige VNet auszuwählen, um Ihre verwaltete Domain zu aktivieren. Bevor Sie fortfahren, lesen Sie den Microsoft-Artikel Überlegungen zum Netzwerk für Azure AD-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 innerhalb des Citrix DaaS für Azure Peered-VNet zugewiesen wird.

  Stellen Sie sicher, dass Sie einen IP-Bereich ohne Überschneidung mit Adressen angeben, die Sie in Ihrem Azure- oder On-Premises-Netzwerk verwenden.

  - Wenn Ihr Azure VNet beispielsweise einen Adressraum von 10.0.0.0 /16 hat, erstellen Sie die VNet-Peering-Verbindung in Citrix DaaS für Azure als etwas wie 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.

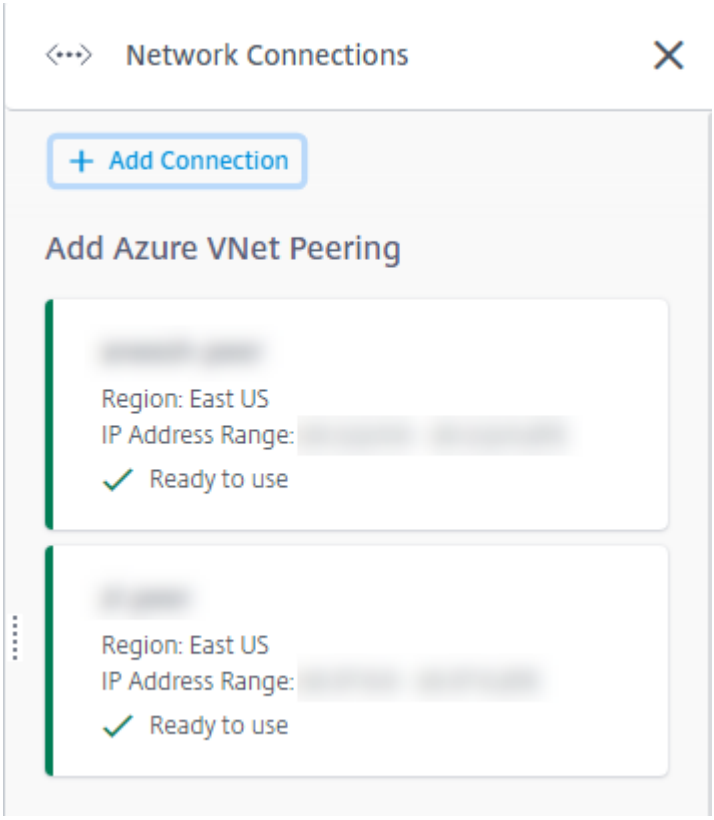
  Wenn sich Adressen überschneiden, wird die VNet-Peering-Verbindung möglicherweise nicht erfolgreich erstellt. Sie funktioniert außerdem nicht einwandfrei für Site-Verwaltungsaufgaben.

Weitere Informationen zu VNet-Peering finden Sie in den folgenden Microsoft-Artikeln.

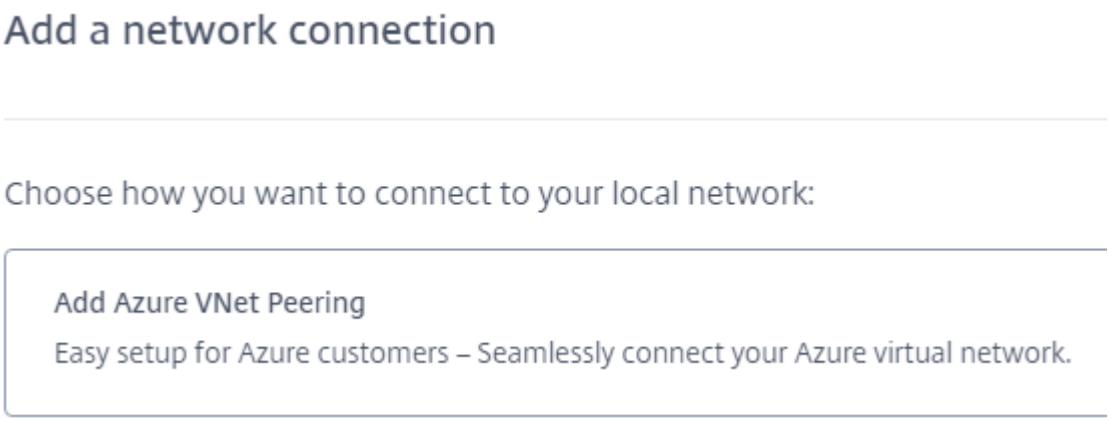
- Peering in virtuellen Netzwerken
- Azure-VPN-Gateway
- Erstellen Sie eine Site-to-Site-Verbindung im Azure-Portal
- VPN Gateway FAQ (Suche nach “Überlappung”)

Erstellen einer Azure VNet-Peering-Verbindung

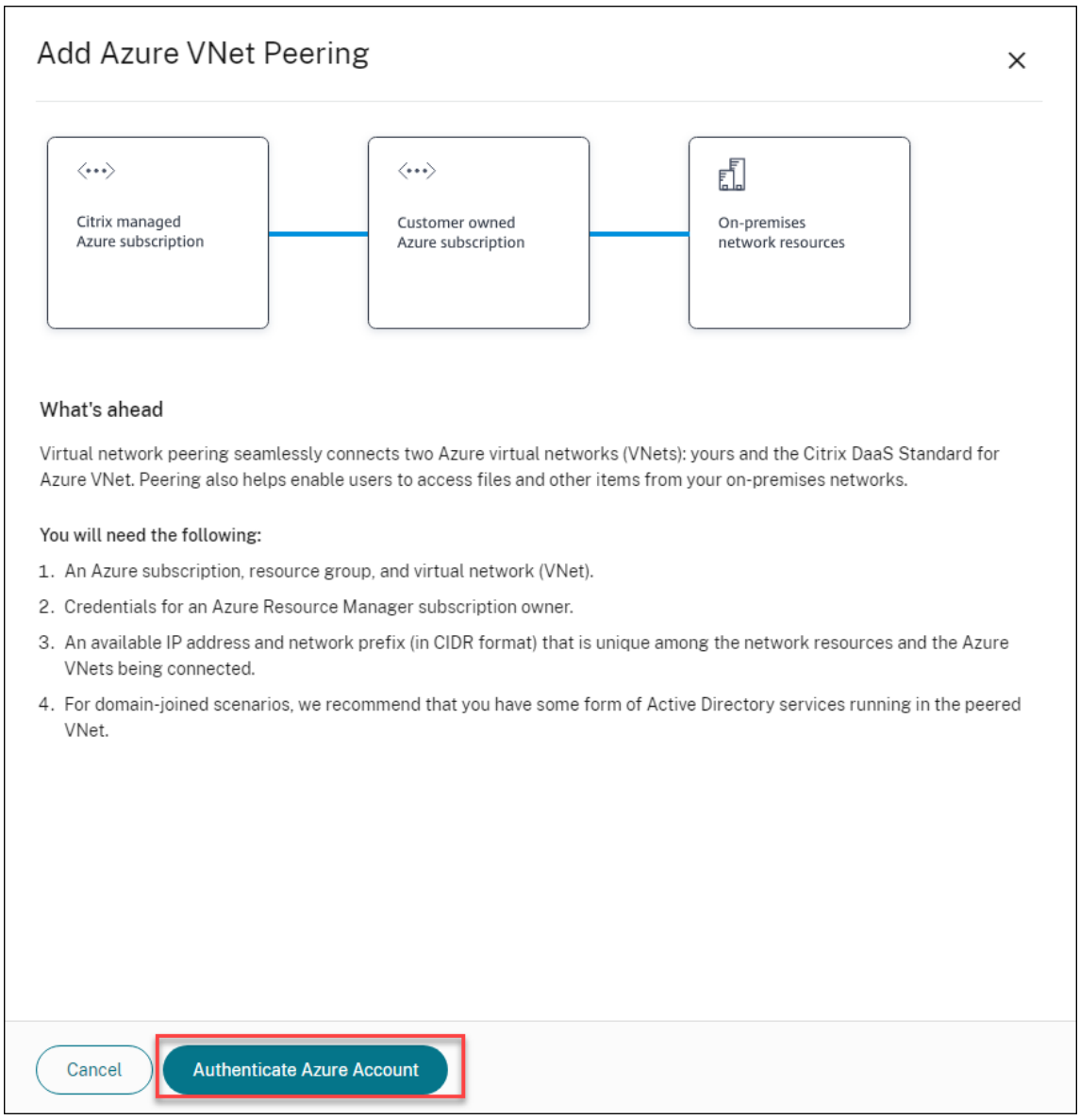
1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein. Wenn Sie bereits Verbindungen eingerichtet haben, werden diese aufgeführt.



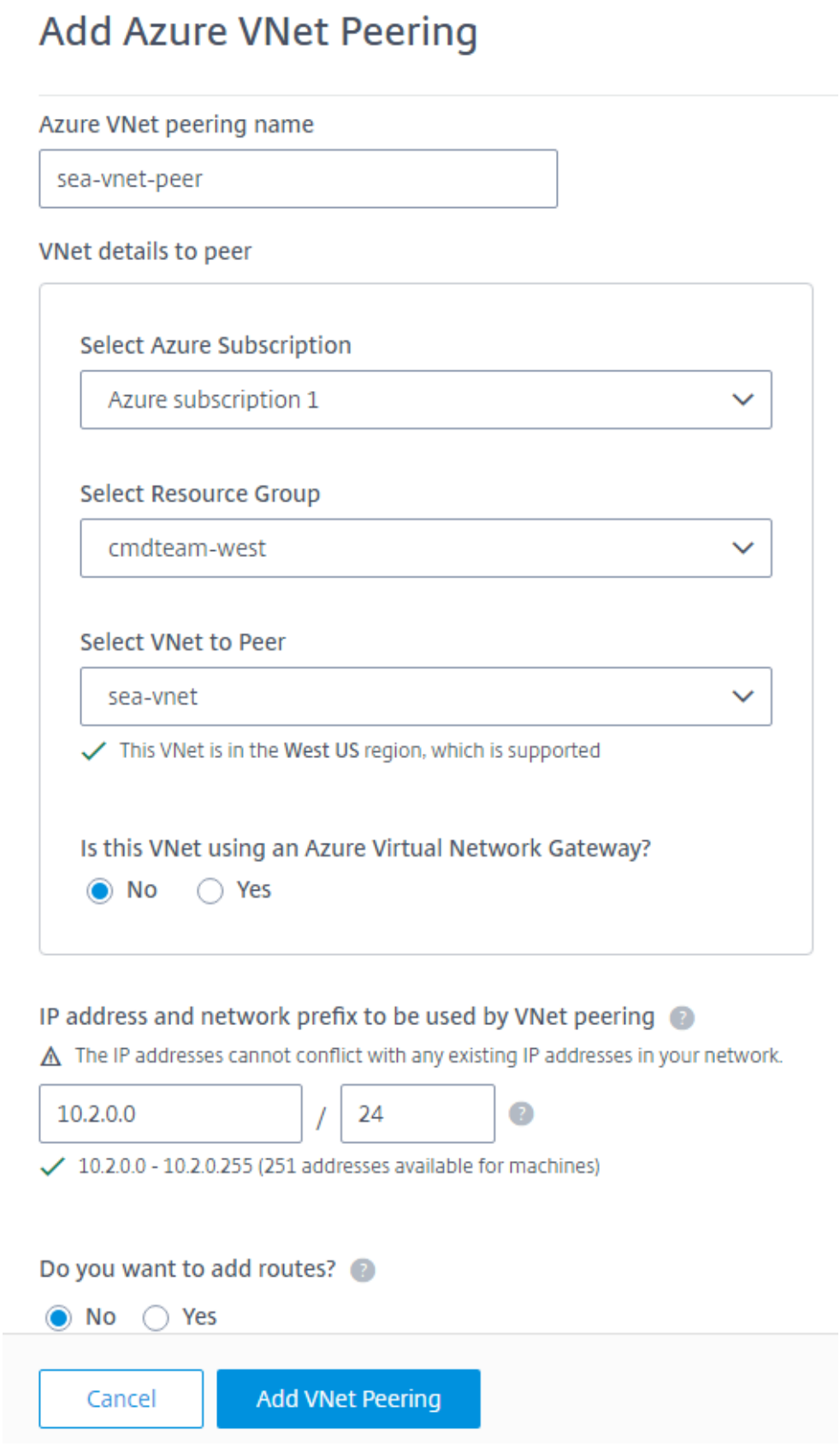
2. Klicken Sie auf **Verbindung hinzufügen**.
3. Klicken Sie auf eine beliebige Stelle im Feld **Azure VNet Peering hinzufügen** .



4. Klicken Sie auf **Azure-Konto authentifizieren**.



5. Citrix DaaS für Azure führt Sie automatisch zur Azure-Anmeldeseite, 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 zu peer aus.
8. Geben Sie an, ob das ausgewählte VNet ein Azure Virtual Network Gateway verwendet. Weitere Informationen finden Sie im Microsoft-Artikel Azure VPN Gateway.
9. Wenn Sie im vorherigen Schritt mit **Ja** beantwortet haben (das ausgewählte VNet verwendet ein virtuelles Azure-Netzwerkgateway), geben Sie an, ob Sie die Routenpropagierung des virtuellen Netzwerkgateways aktivieren möchten. Wenn diese Option aktiviert ist, lernt (fügt) Azure automatisch alle Routen durch das Gateway ein.

   Sie können diese Einstellung später auf der **Detailseite** der Verbindung ändern. Eine Änderung kann jedoch zu Änderungen des Routenmusters und zu Unterbrechungen des VDA-Datenverkehrs führen. Wenn Sie es später deaktivieren, müssen Sie außerdem manuell Routen zu Netzwerken hinzufügen, die VDAs verwenden.
10. Geben Sie eine IP-Adresse ein und wählen Sie eine Netzwerkmaske aus. Der zu verwendende Adressbereich wird angezeigt und wie viele Adressen der Bereich unterstützt. Stellen Sie sicher, dass der IP-Bereich keine Adressen überlappt, die Sie in Ihren Azure- und On-Premises-Netzwerken verwenden.

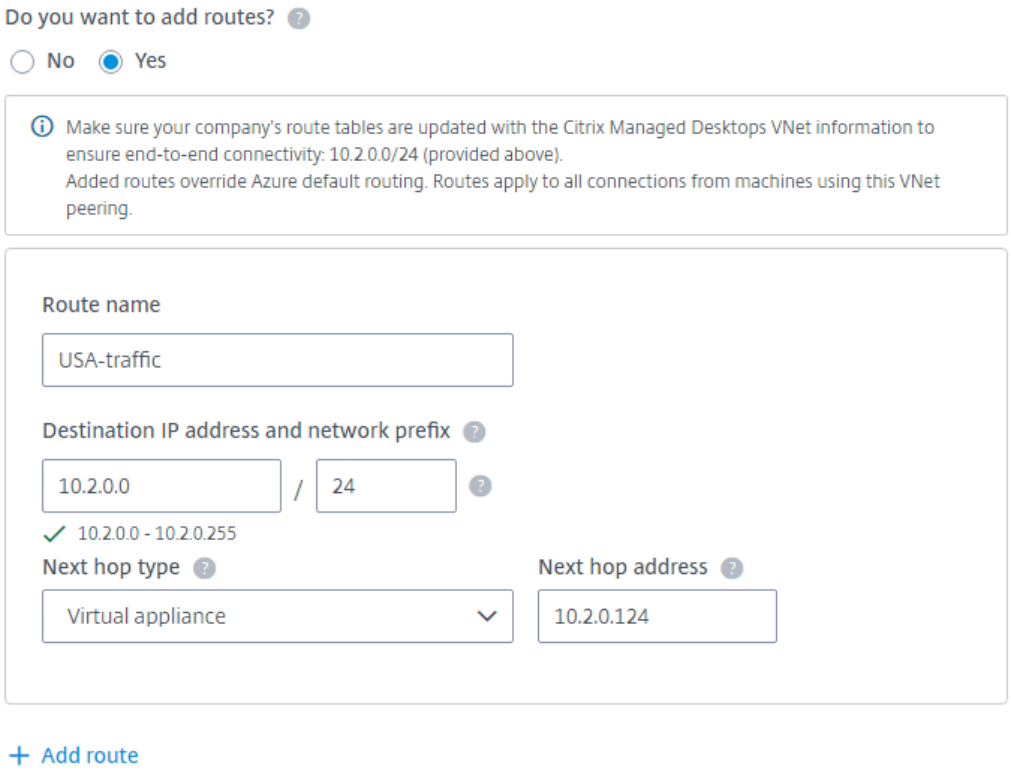
    - Wenn Ihr Azure VNet beispielsweise einen Adressraum von 10.0.0.0 /16 hat, erstellen Sie die VNet-Peering-Verbindung in Citrix Virtual Apps and Desktops Standard wie 192.168.0.0 /24.
    - In diesem Beispiel würde das Erstellen einer VNet-Peering-Verbindung mit einem IP-Bereich von 10.0.0.0 /24 als überlappender Adressbereich angesehen.

    Wenn sich Adressen überschneiden, wird die VNet-Peering-Verbindung möglicherweise nicht erfolgreich erstellt. Es funktioniert auch nicht richtig für Site-Administrationsaufgaben.
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 nächsten Hop-Typ für den Ort aus, an dem der Datenverkehr weitergeleitet werden soll. Wenn Sie **Virtuelle Appliance** auswählen, geben Sie die interne IP-Adresse der Appliance ein.



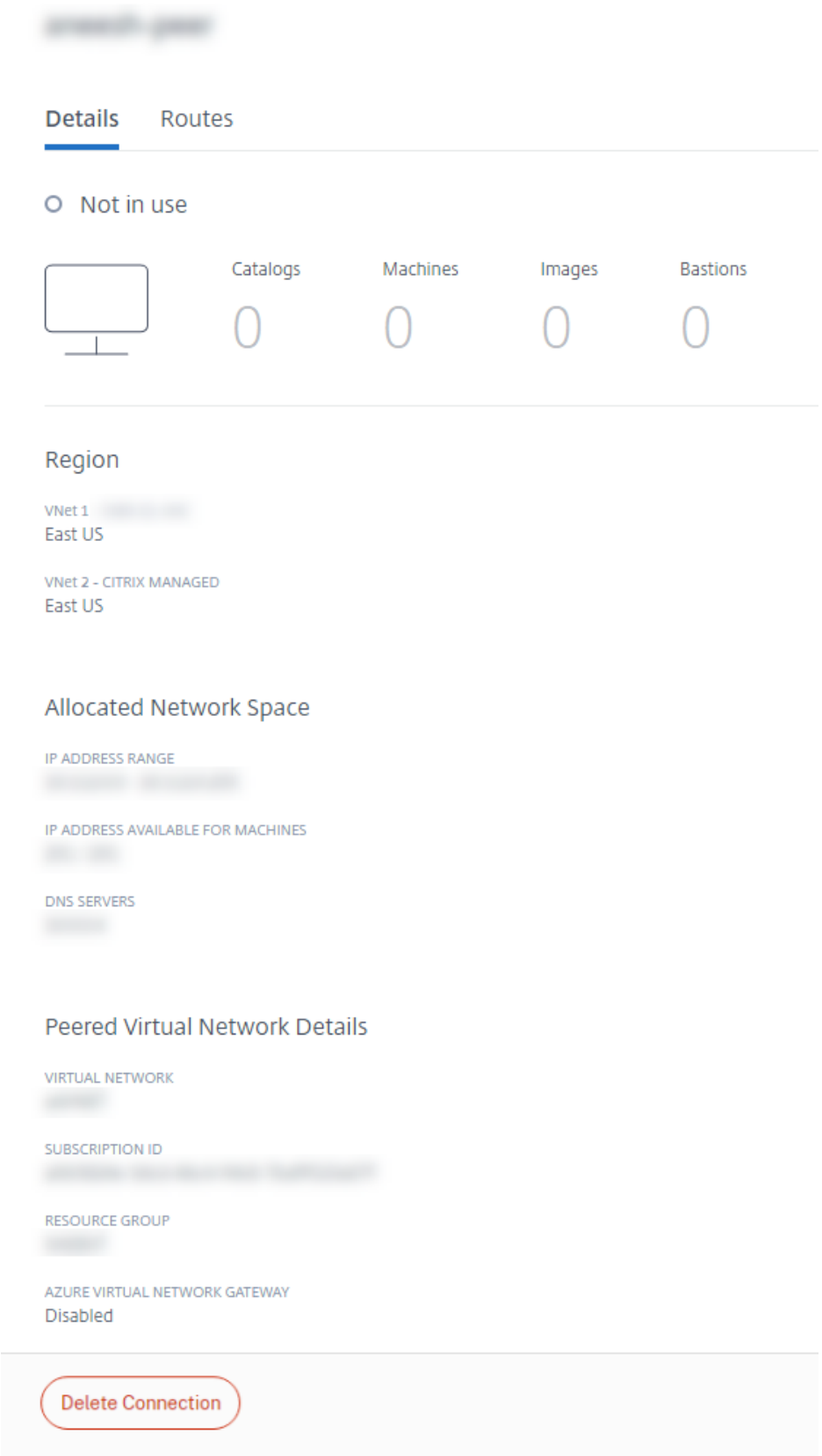
Weitere Informationen zu Next-Hop-Typen finden Sie unter Benutzerdefinierte Routen im Microsoft-Artikel Routing des virtuellen Netzwerkverkehrs.

d) Klicken Sie auf **Route hinzufügen**, um eine weitere benutzerdefinierte Route für die Verbindung zu erstellen.

12. Klicken Sie auf **VNet Peering hinzufügen**.

Nachdem die Verbindung erstellt wurde, wird sie unter **Netzwerkverbindungen > Azure VNet Peers** auf der rechten Seite des Dashboards **Verwalten > Azure 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. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein.
2. Wählen Sie die gewünschte Azure VNet-Peering-Verbindung aus.

Zu den Einzelheiten gehören:

- Die Anzahl der Kataloge, Maschinen, Images und Bastionen, die diese Verbindung verwenden.
- Die Region, der zugewiesene Netzwerkspeicher und Peered-VNets.
- Die derzeit für die VNet-Peering-Verbindung konfigurierten Routen.

Verwalten Sie benutzerdefinierte Routen für vorhandene Azure VNet Peer-Verbindungen

Sie können einer vorhandenen Verbindung neue benutzerdefinierte Routen hinzufügen oder vorhandene benutzerdefinierte Routen ändern, einschließlich des Deaktivierens oder Löschens benutzerdefinierter Routen.

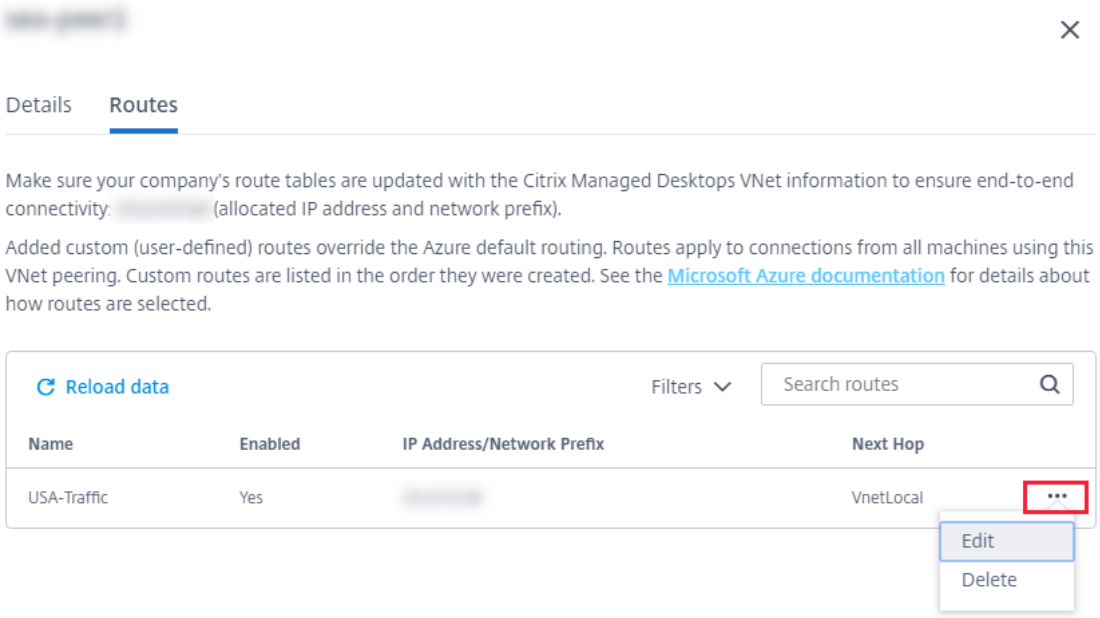
> **Wichtig:**
>
> Das Ändern, Deaktivieren oder Löschen benutzerdefinierter Routen ändert den Datenverkehrsfluss der Verbindung und stört möglicherweise alle Benutzersitzungen, die möglicherweise aktiv sind.

Gehen Sie zum Hinzufügen einer benutzerdefinierten Route folgendermaßen vor:

1. Wählen Sie in den VNet-Peering-Verbindungsdetails die Option **Routen** aus, und klicken Sie dann auf **Route hinzufügen**.
2. Geben Sie einen Anzeigenamen, die Ziel-IP-Adresse und das Präfix sowie den Typ des nächsten Hops ein. Wenn Sie **Virtual Appliance** als nächsten Hop-Typ auswählen, geben Sie die interne IP-Adresse der Appliance ein.
3. Geben Sie an, ob Sie die benutzerdefinierte Route aktivieren möchten. Standardmäßig ist die benutzerdefinierte Route aktiviert.
4. Klicken Sie auf **Route hinzufügen**.

So ändern oder deaktivieren Sie eine benutzerdefinierte Route:

1. Wählen Sie in den VNet-Peering-Verbindungsdetails **Routen** aus, und suchen Sie dann die benutzerdefinierte Route, die Sie verwalten möchten.
2. Wählen Sie im Menü die Option **Bearbeiten**.



3. Nehmen Sie bei Bedarf alle erforderlichen Änderungen an der Ziel-IP-Adresse und dem Präfix oder dem nächsten Hop-Typ vor.
4. Um eine benutzerdefinierte Route zu aktivieren oder zu deaktivieren, finden Sie unter **Diese Route aktivieren?**, wählen Sie **Ja** oder **Nein**aus.
5. Klicken Sie auf **Speichern**.

Gehen Sie zum Löschen einer benutzerdefinierten Route folgendermaßen vor:

1. Wählen Sie in den VNet-Peering-Verbindungsdetails **Routen** aus, und suchen Sie dann die benutzerdefinierte Route, die Sie verwalten möchten.
2. Wählen Sie im Menü die Option **Löschen**.
3. Wählen Sie **Das Löschen einer Route kann aktive Sitzungen unterbrechen**, um die Auswirkungen des Löschens der benutzerdefinierten Route zu bestätigen.
4. Klicken Sie auf **Route löschen**.

Löschen einer Azure VNet-Peering-Verbindung

Bevor Sie einen Azure VNet-Peer löschen können, entfernen Sie alle damit verbundenen Kataloge. Siehe Löschen eines Katalogs.

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein.
2. Wählen Sie die gewünschte Verbindung aus.
3. Klicken Sie in den Verbindungsdetails auf **Verbindung löschen**.

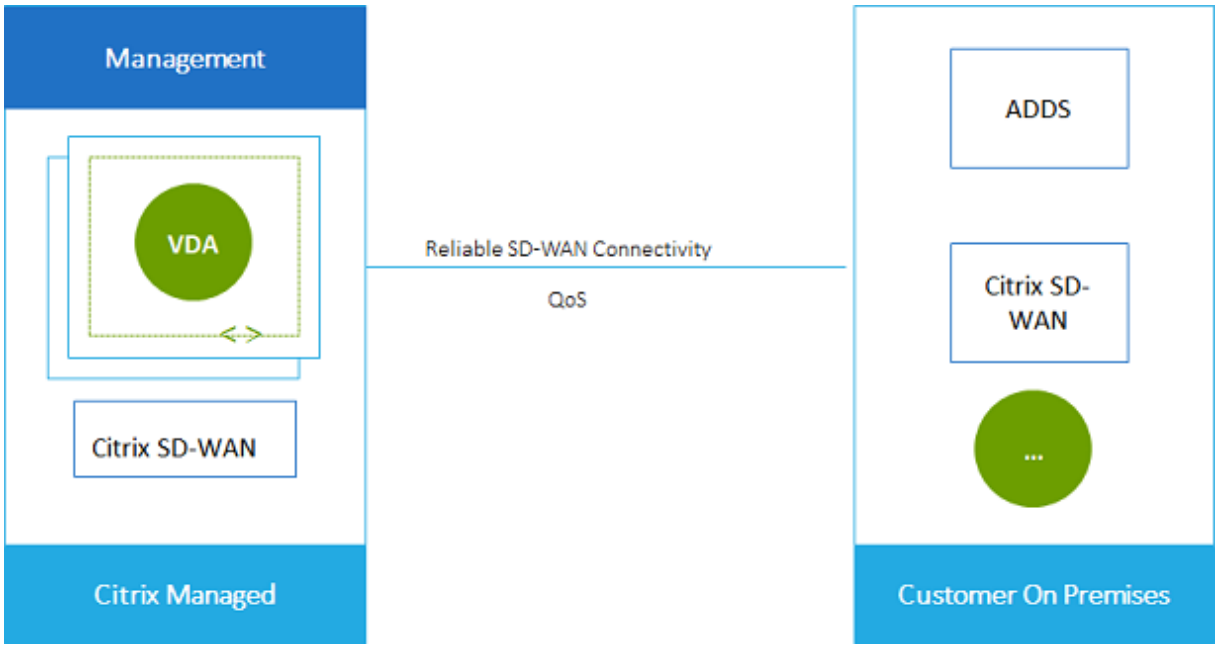
Informationen zu SD-WAN-Verbindungen

> **Wichtig:**
>
> Citrix SD-WAN ist veraltet und alle zugehörigen Inhalte werden in einer zukünftigen Version aus der Dokumentation entfernt. Wir empfehlen, auf alternative Netzwerklösungen umzusteigen, um einen unterbrechungsfreien Zugriff auf die Citrix-Dienste zu gewährleisten.

Citrix SD-WAN optimiert alle Netzwerkverbindungen, die von Citrix Virtual Apps and Desktops Standard for Azure benötigt werden. In Zusammenarbeit mit den HDX-Technologien bietet Citrix SD-WAN Servicequalität und Verbindungszuverlässigkeit für ICA- und Out-of-Band Citrix Virtual Apps and Desktops Standardverkehr. Citrix SD-WAN unterstützt die folgenden Netzwerkverbindungen:

- Multistream-ICA-Verbindung zwischen Benutzern und ihren virtuellen Desktops
- Internetzugriff vom virtuellen Desktop auf Websites, SaaS-Apps und andere Cloud-Eigenschaften
- Zugriff vom virtuellen Desktop zurück auf on-premises Ressourcen wie Active Directory, Dateiserver und Datenbankserver
- Echtzeit-/interaktiver Datenverkehr übertrug RTP von der Medien-Engine in der Workspace-App auf Cloud-gehostete Unified Communications-Dienste wie Microsoft Teams
- Clientseitiges Abrufen von Videos von Websites wie YouTube und Vimeo

Wie in der folgenden Grafik gezeigt, erstellen Sie eine SD-WAN-Verbindung aus dem Citrix Managed Azure-Abonnement für Ihre Sites. Während der Verbindungserstellung werden SD-WAN VPX-Appliances im Citrix Managed Azure-Abonnement erstellt. Aus der SD-WAN-Perspektive wird dieser Standort als Zweig behandelt.



Anforderungen und Vorbereitung der SD-WAN-Verbindung

- Wenn die folgenden Anforderungen nicht erfüllt sind, ist die SD-WAN-Netzwerkverbindungsoption nicht verfügbar.
  - Citrix Cloud-Berechtigungen: Citrix Virtual Apps and Desktops Standard für Azure und SD-WAN Orchestrator.
  - Eine installierte und konfigurierte SD-WAN-Bereitstellung. Die Bereitstellung muss einen Master Control Node (MCN) enthalten, sei es in der Cloud oder on-premises, 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 innerhalb der Citrix Virtual Apps and Desktops Standard VNet zugewiesen ist.

  Stellen Sie sicher, dass Sie einen IP-Bereich angeben, der keine Adressen überlappt, die Sie in Ihrer Cloud- und On-Premises-Netzwerken verwenden.
  - Wenn Ihr Netzwerk beispielsweise einen Adressraum von 10.0.0.0 /16 hat, erstellen Sie die Verbindung in Citrix Virtual Apps and Desktops Standard wie 192.168.0.0 /24.
  - In diesem Beispiel würde das Erstellen einer Verbindung mit einem IP-Bereich 10.0.0.0 /24 als überlappender Adressbereich angesehen.

  Wenn sich Adressbereiche überschneiden, wird die Verbindung möglicherweise nicht erfolgreich erstellt. Sie funktioniert außerdem nicht einwandfrei für Site-Verwaltungsaufgaben.
- Der Verbindungskonfigurationsprozess umfasst Aufgaben, die Sie (der Citrix DaaS für Azure-Administrator) und der SD-WAN Orchestrator-Administrator ausführen müssen. Um Ihre Aufgaben zu erledigen, benötigen Sie außerdem Informationen vom SD-WAN Orchestrator-Administrator.

  Wir empfehlen Ihnen, sowohl die Leitlinien in diesem Dokument als auch die SD-WAN-Dokumentation zu überprüfen, bevor Sie tatsächlich eine Verbindung herstellen.

Erstellen einer SD-WAN-Verbindung

> **Wichtig:**
>
> Einzelheiten zur SD-WAN-Konfiguration finden Sie unter SD-WAN-Konfiguration für Citrix Virtual Apps and Desktops Standard für Azure-Integration.

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein.
2. Klicken Sie auf **Verbindung hinzufügen**.

3. Klicken Sie auf der Seite **Netzwerkverbindung hinzufügen auf eine** beliebige Stelle im Feld SD-WAN.
4. Die nächste Seite fasst zusammen, was vor uns liegt. Wenn Sie mit dem Lesen fertig sind, klicken **Sie auf SD-WAN konfigurieren**.
5. Geben Sie auf der Seite **SD-WAN konfigurieren** die Informationen ein, die von Ihrem SD-WAN Orchestrator-Administrator bereitgestellt wurden.

    - **Bereitstellungsmodus:** Wenn Sie **Hochverfügbarkeit**auswählen, werden zwei VPX-Appliances erstellt (empfohlen für Produktionsumgebungen). Wenn Sie **Standalone**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 die SD-WAN-Site ein.
    - **Durchsatz und Anzahl der Büros:** Diese Informationen werden von Ihrem SD-WAN Orchestrator-Administrator bereitgestellt.
    - **Region:** Die Region, in der die VPX-Appliances erstellt werden.
    - **VDA-Subnetz und SD-WAN-Subnetz:** Diese Informationen werden von Ihrem SD-WAN Orchestrator-Administrator bereitgestellt. Informationen zur Vermeidung von Konflikten finden Sie unter SD-WAN-Verbindungsanforderungen und Vorbereitung .
6. Wenn Sie fertig sind, klicken Sie auf **Zweig erstellen**.
7. Auf der nächsten Seite wird zusammengefasst, worauf Sie im Dashboard **Verwalten > Azure Quick Deploy** achten müssen. Wenn Site mit dem Lesen fertig bist, klicken Sie auf **Verstanden**.
8. Im Dashboard **Verwalten > Azure Quick Deploy** zeigt der neue SD-WAN-Eintrag unter **Netzwerkverbindungen** den Fortschritt des Konfigurationsprozesses an. Wenn der Eintrag mit der Meldung **Auf Aktivierung durch den SD-WAN-Administrator** orange wird, benachrichtigen Sie Ihren SD-WAN Orchestrator-Administrator.
9. Informationen zu SD-WAN Orchestrator-Administratoraufgaben finden Sie in der SD-WAN Orchestrator-Produktdokumentation.
10. Wenn der SD-WAN Orchestrator-Administrator abgeschlossen ist, wird der SD-WAN-Eintrag unter **Netzwerkverbindungen** grün, mit der Meldung **Sie können Kataloge mit dieser Verbindung erstellen.**

Anzeigen der Details der SD-WAN-Verbindung

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein.
2. Wählen Sie **SD-WAN**, falls es mehrere Auswahlmöglichkeiten gibt.

3. Klicken Sie auf die Verbindung, die Sie anzeigen möchten.

Das Display beinhaltet:

- **Registerkarte "Details":** Informationen, die Sie beim Konfigurieren der Verbindung angegeben haben.
- **Registerkarte Zweigkonnektivität:** Name, Cloud-Konnektivität, 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 damit verbundenen Kataloge. Siehe Löschen eines Katalogs.

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein.
2. Wählen Sie SD-WAN, falls es mehrere Auswahlmöglichkeiten gibt.
3. Klicken Sie auf die Verbindung, die Sie löschen möchten, um ihre Details zu erweitern.
4. Klicken Sie auf der Registerkarte **Details** auf **Verbindung löschen**.
5. Bestätigen Sie die Löschung.

Technische Vorschau für Azure VPN

Die Azure VPN-Funktion ist für die technische Vorschau verfügbar.

Informationen zu Azure VPN-Gate

Eine Azure VPN-Gateway-Verbindung stellt eine Kommunikationsverbindung zwischen Ihren von Citrix verwalteten Azure VDAs (Desktops und Apps) und den Ressourcen Ihres Unternehmens bereit, z. B. on-premises Netzwerke oder Ressourcen an anderen Cloud-Standorten. Dies entspricht dem Einrichten und Verbinden mit einer Remote-Zweigstelle.

Für die sichere Konnektivität werden die branchenüblichen Protokolle Internet Protocol Security (IPSec) und Internet Key Exchange (IKE) verwendet.

Während des Erstellungsprozesses der Verbindung:

- Sie geben Informationen an, die Citrix zum Erstellen des Gateway und der Verbindung verwendet.
- Citrix erstellt ein routenbasiertes Site-to-Site-VPN-Gateway für Azure. Das VPN-Gateway bildet einen direkten Internet Protocol Security (IPsec) -Tunnel zwischen dem von Citrix verwalteten Azure-Abonnement und dem Host-Gerät Ihres VPN.

- Nachdem Citrix das Azure VPN-Gateway und die Verbindung erstellt hat, aktualisieren Sie die Konfiguration Ihres VPN, die Firewallregeln und Routing-Tabellen. Für diesen Vorgang verwenden Sie eine öffentliche IP-Adresse, die Citrix bereitstellt, und einen vorab freigegebenen Schlüssel (PSK), den Sie zum Erstellen der Verbindung angegeben haben.

Ein Beispiel für eine Verbindung ist in Erstellen einer Azure VPN-Gatewayverbindungdargestellt.

Sie benötigen kein eigenes Azure-Abonnement, um diese Art von Verbindung herzustellen.

Sie können optional auch benutzerdefinierte Routen mit diesem Verbindungstyp verwenden.

Benutzerdefinierte Azure VPN-Gateways

Benutzerdefinierte oder benutzerdefinierte Routen überschreiben Standardsystemrouten für die Umleitung des Datenverkehrs zwischen virtuellen Maschinen in Ihren Netzwerken und dem Internet. Sie können benutzerdefinierte Routen verwenden, wenn es Netzwerke gibt, auf die Citrix Virtual Apps and Desktops Standard-Ressourcen voraussichtlich zugreifen, die jedoch nicht direkt über ein Azure VPN-Gateway 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.

Wenn Sie einer Verbindung benutzerdefinierte Routen hinzufügen, gelten diese Routen für alle Computer, die diese Verbindung verwenden.

Für benutzerdefinierte Routen gilt Folgendes:

- Sie müssen über ein vorhandenes virtuelles Netzwerk-Gateway oder ein Netzwerkgerät wie Citrix SD-WAN in Ihrer Citrix Virtual Apps and Desktops Standardumgebung verfügen.
- Wenn Sie benutzerdefinierte Routen hinzufügen, müssen Sie die Routentabellen Ihres Unternehmens mit den Ziel-VPN-Informationen aktualisieren, um eine durchgängige Konnektivität zu gewährleisten.
- Benutzerdefinierte Routen werden auf der Registerkarte **Verbindung > Routen** in der Reihenfolge angezeigt, in der sie eingegeben wurden. Diese Anzeigereihenfolge hat keinen Einfluss auf die Reihenfolge, in der die Routen ausgewählt werden.

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 hinzufügen, wenn Sie eine Azure VPN-Gateway-Verbindung oder zu vorhandenen Verbindungen in Ihrer Serviceumgebung erstellen.

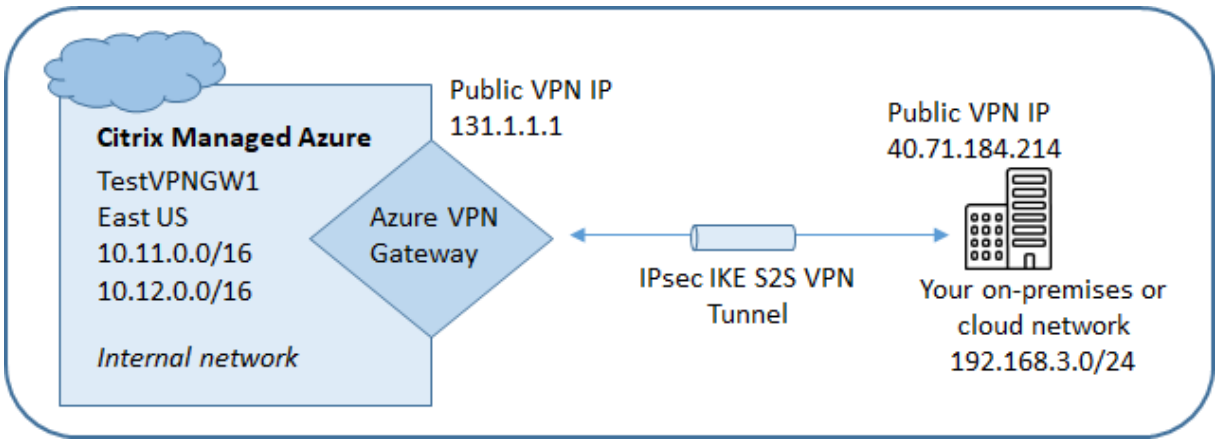
Anforderungen und Vorbereitung der Azure VPN-Gateway

- Weitere Informationen zu Azure VPN Gateway finden Sie im Microsoft-Artikel Was ist VPN-Gateway?
- Prüfen Sie die Anforderungen für alle Netzwerkverbindungen.
- Sie müssen ein konfiguriertes VPN haben. Das virtuelle Netzwerk muss in der Lage sein, Datenverkehr über das VPN-Gateway zu senden und zu empfangen. Ein virtuelles Netzwerk kann nicht mit mehr als einem virtuellen Netzwerk-Gateway verknüpft werden.
- Sie müssen über ein IPSec-Gerät mit einer öffentlichen IP-Adresse verfügen. Weitere Informationen zu validierten VPN-Geräten finden Sie im Microsoft-Artikel Über VPN-Geräte.
- Lesen Sie das Verfahren Erstellen einer Azure VPN-Gateway-Verbindung, bevor Sie es tatsächlich starten, damit Sie die benötigten Informationen sammeln können. Sie benötigen beispielsweise zulässige Adressen in Ihrem Netzwerk, IP-Bereiche für die VDAs und das Gateway, den gewünschten Durchsatz und das Leistungsniveau sowie DNS-Serveradressen.

Erstellen einer Azure VPN-Gateway

Überprüfen Sie dieses Verfahren unbedingt, bevor Sie es tatsächlich starten.

Das folgende Diagramm zeigt ein Beispiel für die Konfiguration einer Azure VPN-Gateway-Verbindung. Im Allgemeinen verwaltet Citrix Ressourcen auf der linken Seite des Diagramms, und Sie verwalten Ressourcen auf der rechten Seite. Einige Beschreibungen im folgenden Verfahren enthalten Verweise auf die Beispiele des Diagramms.



1. Erweitern Sie im Dashboard **“Verwalten** “in Citrix DaaS für Azure auf der rechten Seite **Netzwerkverbindungen** .
2. Klicken Sie auf **Verbindung hinzufügen**.
3. Klicken Sie auf eine beliebige Stelle im Feld **Azure VPN Gateway** .

4. Prüfen Sie die Informationen auf der Seite **VPN-Verbindung hinzufügen**, und klicken Sie dann auf **VPN-Konfiguration starten**.
5. Geben Sie auf der Seite **Verbindung hinzufügen die folgenden Informationen ein** .

    - **Name:** Ein Name für die Verbindung. (Im Diagramm lautet der Name TestVPNGW1.)
    - **VPN-IP-Adresse:** Ihre öffentlich zugängliche IP-Adresse.

      Im Diagramm lautet die Adresse 40.71.184.214.
    - **Zulässige Netzwerke:** Ein oder mehrere Adressbereiche, auf die der Citrix Dienst in Ihrem Netzwerk zugreifen darf. In der Regel enthält dieser Adressbereich die Ressourcen, auf die Ihre Benutzer zugreifen müssen, z. B.

      Um mehr als einen Bereich hinzuzufügen, klicken Sie auf **Weitere IP-Adressen hinzufügen** und geben Sie einen Wert ein. Wiederholen Sie dies nach Bedarf.

      Im Diagramm ist der Adressbereich 192.168.3.0/24.
    - **Vorab freigegebener Schlüssel:** Ein Wert, der von beiden Enden des VPN für die Authentifizierung verwendet wird (ähnlich einem Kennwort). Sie entscheiden, wie hoch dieser Wert ist. Achten Sie darauf, den Wert zu notieren. Sie benötigen es später, wenn Sie Ihr VPN mit den Verbindungsinformationen konfigurieren.
    - **Leistung und Durchsatz:** Die Bandbreite, die verwendet werden soll, wenn Ihre Benutzer auf Ressourcen in Ihrem Netzwerk zugreifen.

      Alle Auswahlmöglichkeiten unterstützen nicht unbedingt das Border Gateway Protocol (BGP). In diesen Fällen sind die **BCP-Einstellungsfelder** nicht verfügbar.
    - **Region:** Azure-Region, in der Citrix Maschinen bereitstellt, die Desktops und Apps (VDAs) bereitstellen, wenn Sie Kataloge erstellen, die diese Verbindung verwenden. Sie können diese Auswahl nicht ändern, nachdem Sie die Verbindung hergestellt haben. Wenn Sie später eine andere Region verwenden möchten, müssen Sie eine andere Verbindung erstellen oder verwenden, die die gewünschte Region angibt.

      In der Abbildung ist die Region EastUS.
    - **Active-Active-Modus (Hochverfügbarkeit):** Ob zwei VPN-Gateways für Hochverfügbarkeit erstellt wurden. Wenn dieser Modus aktiviert ist, ist immer nur ein Gateway aktiv. Weitere Informationen zum aktiv-aktiven Azure VPN-Gateway finden Sie im Microsoft-Dokument Hochverfügbare Cross-Premises-Konnektivität.
    - **BGP-Einstellungen:** (Nur verfügbar, wenn die ausgewählte **Leistung und der Durchsatz** BGP unterstützen.) Ob das Border Gateway Protocol (BGP) verwendet werden soll. Erfahren Sie mehr über BGP im Microsoft-Dokument: Über BGP mit Azure VPN Gateway. Wenn Sie BGP aktivieren, geben Sie die folgenden Informationen an:

  - **Autonomous System Number (ASN):** Azure-Gateways für virtuelle Netzwerke wird eine Standard-ASN von 65515 zugewiesen. Eine BGP-fähige Verbindung zwischen zwei Netzwerk-Gateways setzt voraus, dass ihre ASNs unterschiedlich sind. Bei Bedarf können Sie die ASN jetzt oder nach der Erstellung des Gateway ändern.
  - **BGP-IP-Peering-IP-Adresse:** Azure unterstützt BGP-IP im Bereich 169.254.21.*x* auf 169.254.22.*x*.

- **VDA-Subnetz:** Der Adressbereich, in dem sich Citrix VDAs (Maschinen, die Desktops und Apps bereitstellen) und Cloud Connectors befinden, wenn Sie einen Katalog erstellen, der diese Verbindung verwendet. Nachdem Sie eine IP-Adresse eingegeben und eine Netzwerkmaske ausgewählt haben, wird der Adressbereich sowie die Anzahl der Adressen angezeigt, die der Bereich unterstützt.

  Obwohl dieser Adressbereich im von Citrix verwalteten Azure-Abonnement beibehalten wird, funktioniert er so, als ob er eine Erweiterung Ihres Netzwerks wäre.

  - Der IP-Bereich darf sich nicht mit Adressen überschneiden, die Sie in Ihren on-premises oder anderen Cloud-Netzwerken verwenden. Wenn sich Adressbereiche überschneiden, wird die Verbindung möglicherweise nicht erfolgreich erstellt. Außerdem funktioniert eine überlappende Adresse bei Site-Verwaltungsaufgaben nicht richtig.
  - Der VDA-Subnetzbereich muss sich von der Gateway-Subnetzadresse unterscheiden.
  - Sie können diesen Wert nicht ändern, nachdem Sie die Verbindung erstellt haben. Um einen anderen Wert zu verwenden, erstellen Sie eine weitere Verbindung.

  In dem Diagramm ist das VDA-Subnetz 10.11.0.0/16.

- **Gateway-Subnetz:** Der Adressbereich, in dem sich das Azure VPN-Gateway befindet, wenn Sie einen Katalog erstellen, der diese Verbindung verwendet.

  - Der IP-Bereich darf sich nicht mit Adressen überschneiden, die Sie in Ihren on-premises oder anderen Cloud-Netzwerken verwenden. Wenn sich Adressbereiche überschneiden, wird die Verbindung möglicherweise nicht erfolgreich erstellt. Außerdem funktioniert eine überlappende Adresse bei Site-Verwaltungsaufgaben nicht richtig.
  - Der Gateway-Subnetzbereich muss sich von der VDA-Subnetzadresse unterscheiden.
  - Sie können diesen Wert nicht ändern, nachdem Sie die Verbindung erstellt haben. Um einen anderen Wert zu verwenden, erstellen Sie eine weitere Verbindung.

  Im Diagramm ist das Gateway-Subnetz 10.12.0.9/16.

- **Routen:** Geben Sie an, ob Sie der Verbindung benutzerdefinierte Routen hinzufügen möchten. Wenn Sie benutzerdefinierte Routen hinzufügen möchten, geben Sie die

folgenden Informationen an:

- Geben Sie einen Anzeigenamen für die benutzerdefinierte Route ein.
- Geben Sie die Ziel-IP-Adresse und das Netzwerkpräfix ein. Das Netzwerkpräfix muss zwischen 16 und 24 liegen.
- Wählen Sie einen nächsten Hop-Typ für den Ort aus, an dem der Datenverkehr weitergeleitet werden soll. Wenn Sie **Virtuelle Appliance auswählen, geben Sie die interne IP-Adresse der Appliance ein. Weitere Informationen zu Next-Hop-Typen finden Sie unter Benutzerdefinierte Routen im Microsoft-Artikel Routing des virtuellen Netzwerkverkehrs.

Um mehr als eine Route hinzuzufügen, klicken Sie auf **Route hinzufügen** und geben Sie die angeforderten Informationen ein.

- **DNS-Server:** Geben Sie Adressen für Ihre DNS-Server ein und geben Sie den bevorzugten Server an. Sie können die DNS-Servereinträge zwar später ändern, aber denken Sie daran, dass eine Änderung möglicherweise zu Konnektivitätsproblemen für die Maschinen in Katalogen führen kann, die diese Verbindung verwenden.

  Um mehr als zwei DNS-Serveradressen hinzuzufügen, klicken Sie auf **Alternatives DNS hinzufügen** und geben dann die angeforderten Informationen ein.

6. Klicken Sie auf **VPN-Verbindung erstellen**.

Nachdem Citrix die Verbindung erstellt hat, wird sie im **Verwaltungs-Dashboard** in Citrix DaaS für Azure**unter Netzwerkverbindungen > Azure VPN Gateway** aufgeführt. Die Verbindungskarte enthält eine öffentliche IP-Adresse. (Im Diagramm lautet die Adresse 131.1.1.1.)

- Verwenden Sie diese Adresse (und den vorab freigegebenen Schlüssel, den Sie beim Herstellen der Verbindung angegeben haben), um Ihr VPN und Ihre Firewalls zu konfigurieren. Wenn Sie Ihren vorab freigegebenen Schlüssel vergessen haben, können Sie ihn auf der **Detailseite** der Verbindung ändern. Sie benötigen den neuen Schlüssel, um Ihr Ende des VPN-Gateways zu konfigurieren.

  Lassen Sie beispielsweise in Ihrer Firewall Ausnahmen für die von Ihnen konfigurierten VDA- und Gateway-Subnetz-IP-Adressbereiche zu.

- Aktualisieren Sie die Routing-Tabellen Ihres Unternehmens mit den Azure VPN-Gateway-Verbindungsinformationen, um eine durchgängige Konnektivität sicherzustellen.

  Im Diagramm sind neue Routen für den Verkehr von 192.168.3.0/24 auf 10.11.0.0/16 und 10.12.0.9/16 (die VDA- und Gateway-Subnetze) erforderlich.

- Wenn Sie benutzerdefinierte Routen konfiguriert haben, nehmen Sie auch die entsprechenden Aktualisierungen für diese vor.

Wenn beide Enden der Verbindung erfolgreich konfiguriert wurden, zeigt der Eintrag der Verbindung unter **Netzwerkverbindungen > Azure VPN Gateway** an **Bereit zur Verwendung**.

Eine Azure VPN-Gatewayverbindung

1. Erweitern Sie im Dashboard **"Verwalten** "in Citrix DaaS für Azure auf der rechten Seite **Netzwerkverbindungen** .
2. Wählen Sie die gewünschte Verbindung aus.

   Zeigt:

- Auf der Registerkarte **Details** wird die Anzahl der Kataloge, Maschinen, Images und Bastions angezeigt, die diese Verbindung verwenden. Es enthält auch die meisten Informationen, die Sie für diese Verbindung konfiguriert haben.
- Auf der Registerkarte **Routen** werden benutzerdefinierte Routeninformationen für die Verbindung aufgeführt.

Verwalten von benutzerdefinierten Routen für eine Azure VPN-Gate

In einer vorhandenen Azure VPN-Gateway-Verbindung können Sie benutzerdefinierte Routen hinzufügen, ändern, deaktivieren und löschen.

Informationen zum Hinzufügen von benutzerdefinierten Routen beim Erstellen einer Verbindung finden Sie unter Erstellen einer Azure VPN-Gateway-Verbindung.

> **Wichtig:**
>
> Das Ändern, Deaktivieren oder Löschen von benutzerdefinierten Routen ändert den Verkehrsfluss der Verbindung und kann aktive Benutzersitzungen unterbrechen.

1. Erweitern Sie im Dashboard **"Verwalten** "in Citrix DaaS für Azure auf der rechten Seite **Netzwerkverbindungen** .
2. Wählen Sie die gewünschte Verbindung aus.
   - Gehen Sie zum Hinzufügen einer benutzerdefinierten Route folgendermaßen vor:
     a) Klicken Sie auf der Registerkarte **Routen** der Verbindung auf **Route hinzufügen**.
     b) Geben Sie einen Anzeigenamen, die Ziel-IP-Adresse und das Präfix sowie den Typ des nächsten Hops ein. Wenn Sie **Virtual Appliance** als nächsten Hop-Typ auswählen, geben Sie die interne IP-Adresse der Appliance ein.
     c) Geben Sie an, ob Sie die benutzerdefinierte Route aktivieren möchten. Standardmäßig ist die benutzerdefinierte Route aktiviert.

d) Klicken Sie auf **Route hinzufügen**.

- So ändern oder aktivieren/deaktivieren Sie eine benutzerdefinierte Route:

  a) Suchen Sie auf der Registerkarte **Routen** der Verbindung die benutzerdefinierte Route, die Sie verwalten möchten.

  b) Wählen Sie im Menü die Option **Bearbeiten**.

  c) Ändern Sie die Ziel-IP-Adresse und das Präfix oder den nächsten Hop-Typ nach Bedarf.

  d) Geben Sie an, ob Sie die Route aktivieren möchten.

  e) Klicken Sie auf **Speichern**.

- Gehen Sie zum Löschen einer benutzerdefinierten Route folgendermaßen vor:

  a) Suchen Sie auf der Registerkarte **Routen** der Verbindung die benutzerdefinierte Route, die Sie verwalten möchten.

  b) Wählen Sie im Menü die Option **Löschen**.

  c) Wählen Sie **Das Löschen einer Route kann aktive Sitzungen unterbrechen**, um die Auswirkungen des Löschens der benutzerdefinierten Route zu bestätigen.

  d) Klicken Sie auf **Route löschen**.

Zurücksetzen oder Löschen einer Azure VPN-Gatewayverbindung

> **Wichtig:**
>
> - Durch das Zurücksetzen einer Verbindung geht die aktuelle Verbindung verloren und beide Enden müssen sie wieder herstellen. Ein Reset unterbricht aktive Benutzersitzungen.
> - Bevor Sie eine Verbindung löschen können, löschen Sie alle Kataloge, die sie verwenden. Siehe Löschen eines Katalogs.

So setzen Sie eine Verbindung zurück oder löschen sie:

1. Erweitern Sie im Dashboard **“Verwalten** “in Citrix DaaS für Azure auf der rechten Seite **Netzwerkverbindungen** .
2. Wählen Sie die Verbindung aus, die Sie zurücksetzen oder löschen möchten.
3. Auf der Registerkarte “**Details** “der Verbindung:
   - Um die Verbindung zurückzusetzen, klicken Sie auf **Verbindung zurücksetzen**.
   - Um die Verbindung zu löschen, klicken Sie auf **Verbindung löschen**.
4. Wenn Sie dazu aufgefordert werden, bestätigen Sie die Aktion.

Erstellen einer öffentlichen statischen IP-Adresse

Wenn Sie möchten, dass alle Maschinen-VDAs auf einer Verbindung eine einzelne ausgehende öffentliche statische IP-Adresse (Gateway) zum Internet verwenden, aktivieren Sie ein NAT-Gateway. Sie können ein NAT-Gateway für Verbindungen zu Katalogen aktivieren, die mit einer Domäne verbunden oder nicht mit einer Domäne verbunden sind.

So aktivieren Sie ein NAT-Gateway für eine Verbindung:

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Netzwerkverbindungen** ein.
2. Wählen Sie unter **Netzwerkverbindungen**eine Verbindung unter **CITRIX MANAGED** oder **AZURE VNET PEERINGS**aus.
3. Klicken Sie auf der Karte mit den Verbindungsdetails auf **NAT-Gateway aktivieren**.
4. Bewegen Sie auf der Seite NAT-Gateway aktivieren den Schieberegler auf **Ja** und stellen Sie eine Leerlaufzeit ein.
5. Klicken Sie auf **Änderungen bestätigen**.

Wenn Sie ein NAT-Gateway aktivieren:

- Azure weist dem Gateway automatisch eine öffentliche statische IP-Adresse zu. (Sie können diese Adresse nicht angeben.) Alle VDAs in allen Katalogen, die diese Verbindung verwenden, verwenden diese Adresse für ausgehende Konnektivität.
- Sie können einen Timeout-Wert für den Leerlauf angeben. Dieser Wert gibt an, wie viele Minuten eine offene ausgehende Verbindung über das NAT-Gateway im Leerlauf verbleiben kann, bevor die Verbindung geschlossen wird.
- Sie müssen die öffentliche statische IP-Adresse in Ihrer Firewall zulassen.

Sie können zur Karte mit den Verbindungsdetails zurückkehren, um das NAT-Gateway zu aktivieren oder zu deaktivieren und den Timeout-Wert zu ändern.

Images

September 7, 2022

Wenn Sie einen Katalog zur Bereitstellung von Desktops oder Apps erstellen, wird ein Image (mit anderen Einstellungen) als Vorlage zum Erstellen der Maschinen verwendet.

Von Citrix vorbereitete Images

Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure) bietet mehrere von Citrix vorbereitete Images:

- Windows 10 Enterprise (Einzelsitzung)
- Virtueller Windows 10 Enterprise-Desktop (Multisitzung)
- Virtueller Windows 10 Enterprise-Desktop (Multisitzung) mit Office 365 ProPlus
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Linux Ubuntu (Einzel- und 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 Computern Ihrer Benutzer und der Citrix Cloud-Infrastruktur, die Citrix DaaS für Azure verwaltet. Von Citrix bereitgestellte Images werden als **CITRIX** notiert.

Sie können auch eigene Images aus Azure importieren und verwenden.

Möglichkeiten, Images zu verwenden

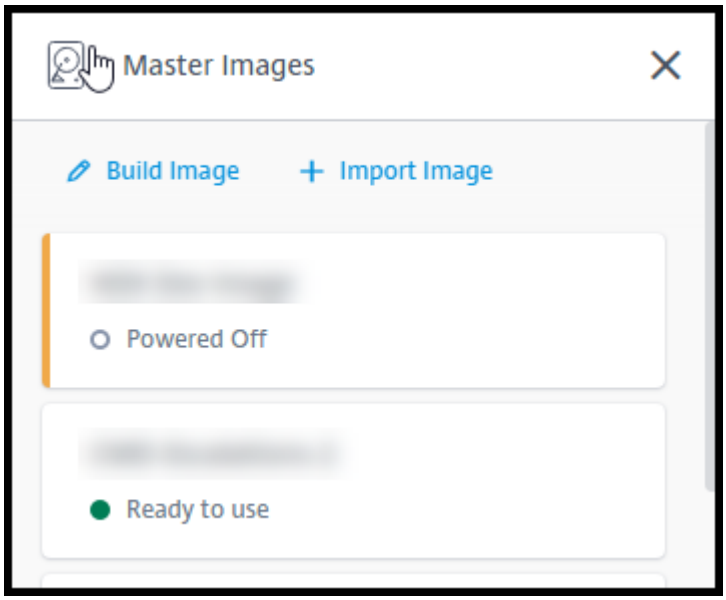
Sie haben folgende Möglichkeiten:

- **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.

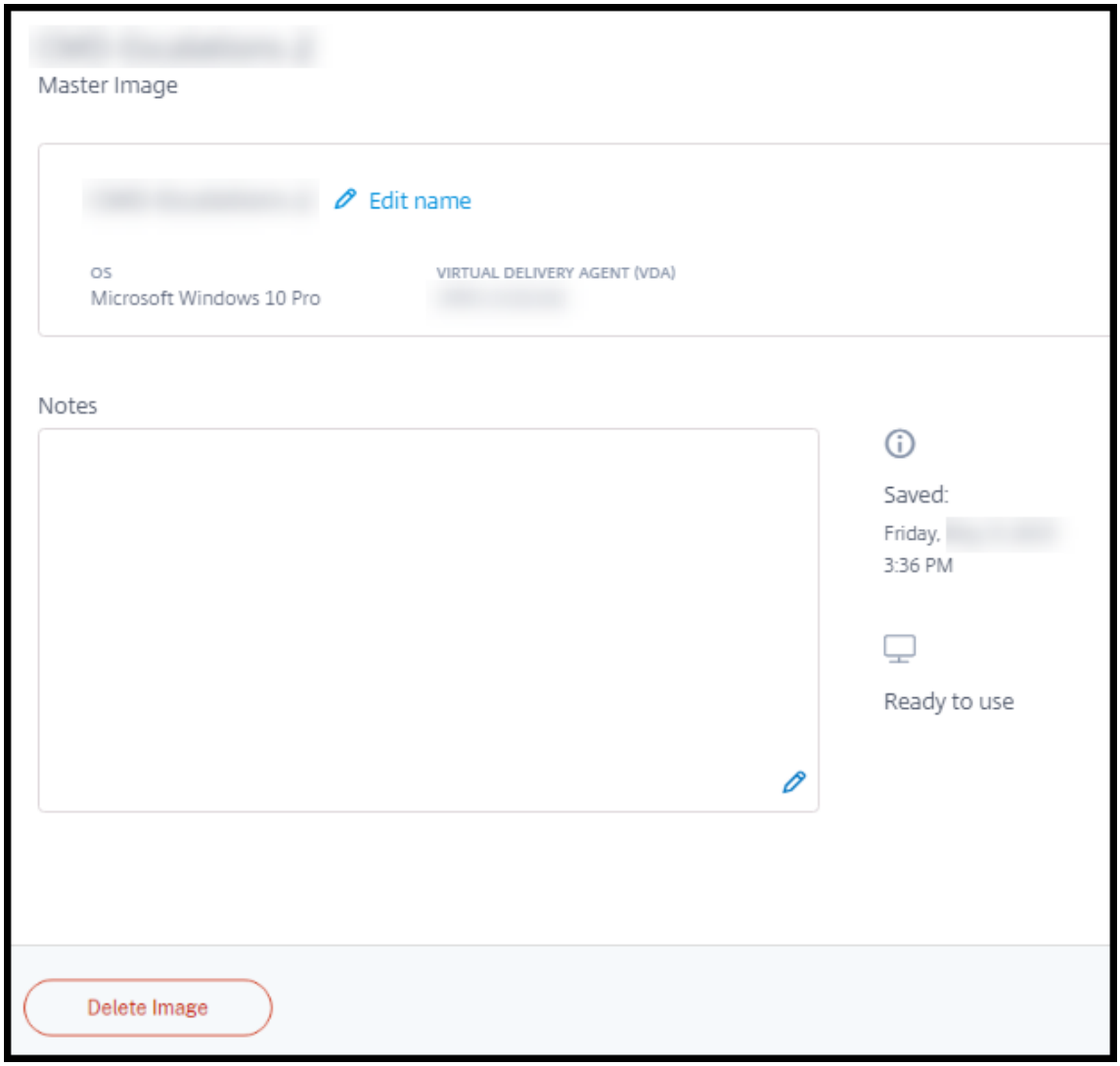
Wenn Sie einen Katalog erstellen, überprüft Citrix DaaS für Azure, ob das Image ein gültiges Betriebssystem verwendet und dass ein Citrix VDA und Tools zur Fehlerbehebung installiert sind (zusammen mit anderen Prüfungen).

Anzeigen von Imageinformationen

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** auf der rechten Seite **Masterimages** ein. Die Anzeige listet die von Citrix bereitgestellten Images sowie die von Ihnen erstellten und importierten Images auf.



2. Klicken Sie auf ein Image, um seine Details anzuzeigen.



In den Details können Sie folgende Schritte ausführen:

- Image ändern (bearbeiten).
- Notizen hinzufügen und bearbeiten (Nur für Images verfügbar, die Sie vorbereitet oder importiert haben, nicht von Citrix bereitgestellte Images).
- 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.

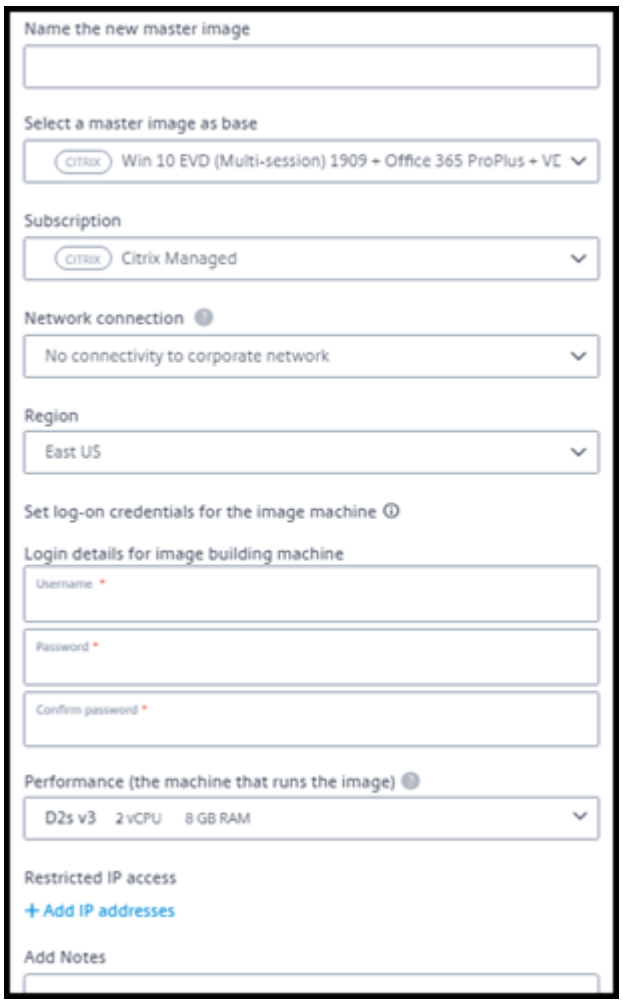
- Wenn Sie eine Verbindung zu Ihren On-Premises-Ressourcen verwenden möchten, richten Sie diese ein, bevor Sie das Image und den Katalog erstellen. Weitere Details finden Sie unter Netzwerkverbindungen.

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. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** auf der rechten Seite **Masterimages** ein.
2. Klicken Sie auf **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. Einzelheiten finden Sie unter Azure-Abonnements.
   - **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, OU, Dienstkontoname und Anmeldeinformationen.
   - **Domänenkonfiguration:** Wählen Sie den Domänentyp aus: Active Directory oder nicht domänengebunden.

  - Wenn Sie Active Directory auswählen, wählen Sie eine Domäne aus oder fügen Sie sie hinzu. Geben Sie eine OU (optional), einen Dienstkontonamen und ein Kennwort an.
  - Wenn Sie Nicht-Domain-Joined auswählen, sind keine zusätzlichen Informationen erforderlich.

- **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. Klicken Sie nach dem Hinzufügen der Adressen auf **Fertig**, um zur **Image-Karte erstellen** zurückzukehren.
- **Notizen:** 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 die Azure-Informationen ein: FQDN, OU, Dienstkontoname und Anmeldeinformationen.
  - Wenn Sie **Nein** auswählen, geben Sie die Anmeldeinformationen für die Hostmaschine ein.

4. Wenn Sie fertig sind, klicken Sie auf **Image erstellen**.

Das Erstellen eines Images kann bis zu 30 Minuten dauern. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** rechts **MasteriImages** ein, um den aktuellen Status anzuzeigen (z. B. **Image erstellen** oder **Bereit zum Anpassen**).

Nächste Schritte: Verbinden mit einem neuen Image und Anpassen des Images.

Verbinden Sie sich mit einem neuen Image und passen Sie es an

Nachdem ein neues Image erstellt wurde, wird sein Name zur Image-Liste mit dem Status **Bereit zum Anpassen** (oder einem ähnlichen Wortlaut) hinzugefügt. 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. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** auf der rechten Seite **Masterimages** ein. Klicken Sie auf das Image, mit dem Sie eine Verbindung herstellen möchten.
2. Klicken Sie auf **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. Klicken Sie in diesem Fall auf **Einschalten**.
3. Doppelklicken Sie auf den heruntergeladenen RDP 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 mit dem Anpassen des neuen Images fertig sind, kehren Sie zum Feld **Master-Images** zurück und klicken Sie auf **Build beenden**. 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.

Auf dem Dashboard **Verwalten > Schnellbereitstellung** zeigt die Images auf der rechten Seite an, wie viele Kataloge und Maschinen jedes Image verwenden.

> **Hinweis:**
>
> Nachdem Sie ein Image fertiggestellt haben, können Sie es nicht bearbeiten. Sie müssen ein neues Image erstellen (indem Sie das vorherige Image als Ausgangspunkt verwenden) und dann das neue Image 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

> **Hinweis:**

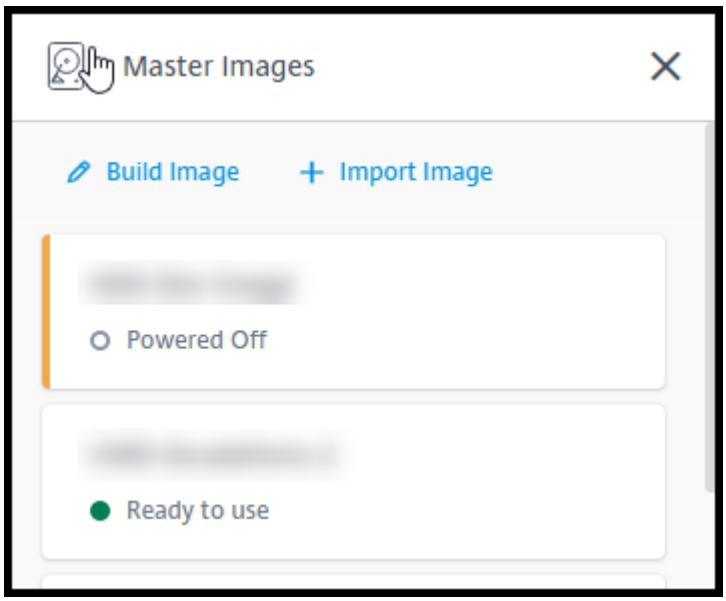
> Citrix DaaS für Azure unterstützt den Import von Datenträgern nicht, die mit VMs der Azure-Generation 2 verknüpft sind.

Citrix führt eine Validierung importierter Images aus. Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, wenn Sie das Image vorbereiten, das Sie in Citrix DaaS für Azure importieren.

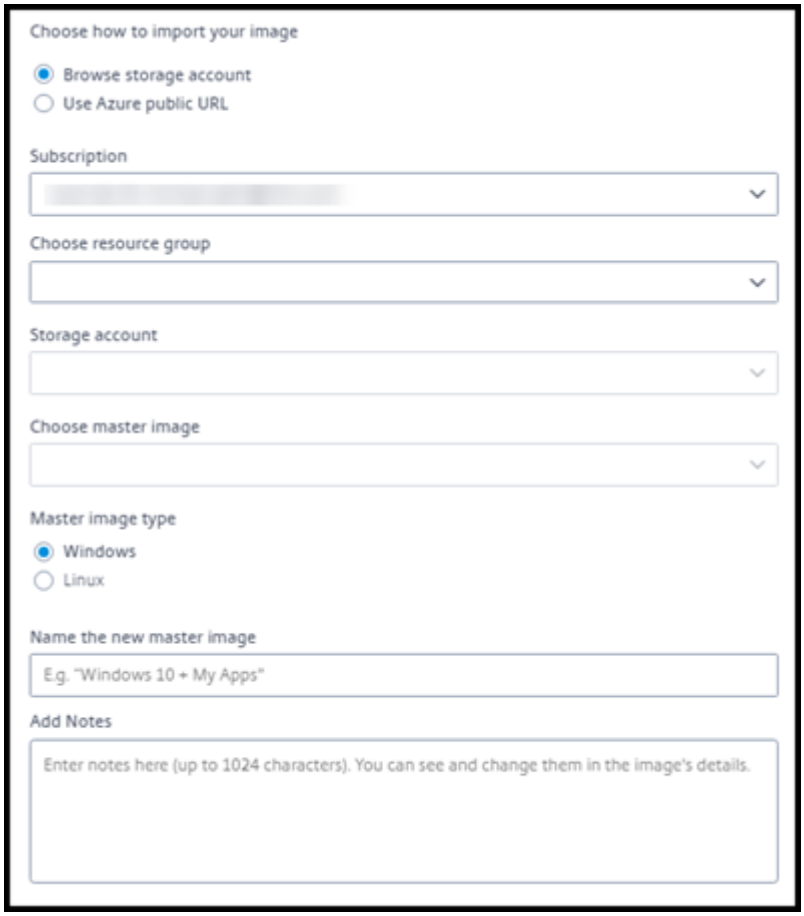
- **Unterstütztes Betriebssystem:** Das Image muss ein unterstütztes OS enthalten. Um die Windows-Betriebssystemversion zu überprüfen, führen Sie `Get-WmiObject Win32_OperatingSyste` aus.
- **Unterstützte Generation:** Es werden nur Gen1-VMs unterstützt.
- **Nicht generalisiert:** Das Image darf kein 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 Azure Virtual Machine Agent —Übersicht.

Importieren Sie das Image

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** auf der rechten Seite **Masterimages** ein.



2. Klicken Sie auf **Image importieren**.



3. Wählen Sie aus, wie das Image importiert werden soll.

   - Verwenden Sie für verwaltete Datenträger die Exportfunktion, um eine SAS-URL zu gener-

ieren. 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. Klicken Sie zur Orientierung auf den Link zum Microsoft-Dokument Laden Sie eine Windows VHD von Azure herunter.
   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, klicken Sie auf **Image importieren**.

Aktualisieren eines Katalogs mit einem neuen Image

Der Katalogtyp bestimmt, welche Maschinen aktualisiert werden, wenn Sie den Katalog aktualisieren.

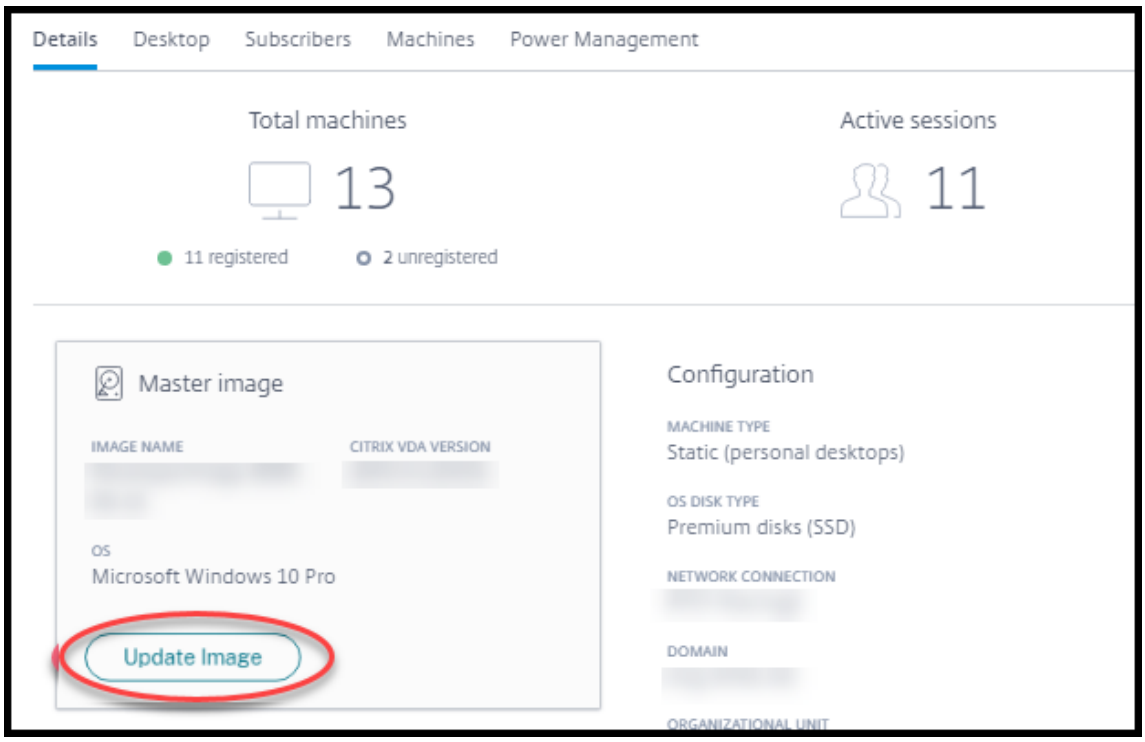
- Bei einem zufälligen Katalog werden alle Maschinen im Katalog mit dem neuesten Image aktualisiert. Wenn Sie dem Katalog weitere Desktops hinzufügen, verwenden diese das neueste Image.
- Bei statischen Katalogen werden die im Katalog befindlichen Maschinen nicht mit dem neuesten Image aktualisiert. 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 im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.

2. Klicken Sie auf der Registerkarte **Details** auf **Image aktualisieren**.



3. Wählen Sie ein Image aus.
4. Zufällige/Mehrsitzungskataloge: Wählen Sie ein Abmeldeintervall aus. Nachdem Citrix DaaS für Azure die anfängliche Image-Verarbeitung abgeschlossen hat, erhalten Abonnenten eine Warnung, 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. Klicken Sie auf **Image aktualisieren**.

Löschen Sie ein Image

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** auf der rechten Seite **Masterimages** ein.
2. Klicken Sie auf das Image, das Sie löschen möchten.
3. Klicken Sie unten auf der Karte auf **Image löschen** . Bestätigen Sie die Löschung.

Installieren eines Windows-VDAs auf einem Image

Gehen Sie wie folgt vor, wenn Sie ein Windows-Image vorbereiten, das Sie in Citrix DaaS für Azure importieren möchten. 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 verwenden Sie einen Browser, um zur Downloadseite von Citrix DaaS für Azure zu navigieren.

   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 aus, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite **Kernkomponenten** auf **Weiter**.
6. Wählen Sie auf der Seite **Delivery Controller** die Option **Automatische Erstellung durch Maschinenerstellungsdienste** und klicken Sie auf **Weiter**.
7. Verwenden Sie die Standardeinstellungen auf den Seiten **Zusätzliche Komponenten**, **Features** und **Firewall** (sofern Sie keine anderslautende Anweisung von Citrix erhalten). Klicken Sie auf jeder Seite auf **Weiter**.
8. Klicken Sie auf der Seite **Zusammenfassung** auf **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 Sie eine Verbindung hergestellt haben, klicken Sie auf **Weiter**.
10. Klicken Sie auf **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.

Benutzer und Authentifizierung

December 28, 2023

Methoden der Benutzerauthentifizierung

Die Benutzer müssen sich authentifizieren, wenn sie sich bei Citrix Workspace anmelden, um ihren Desktop oder ihre Apps zu starten.

Citrix DaaS für Azure 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:

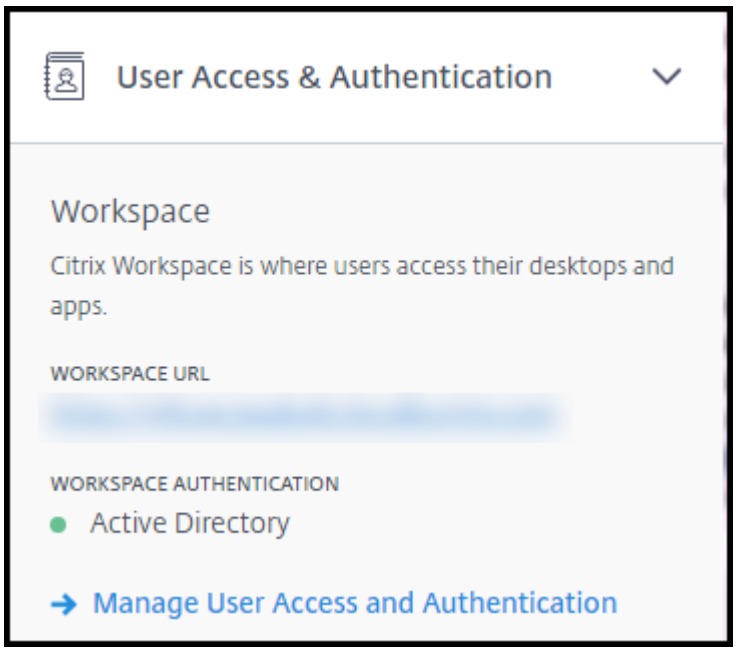
- Stellen Sie eine Verbindung mit der Benutzerauthentifizierungsmethode her, die Sie verwenden möchten. (In Citrix Cloud wird eine "Verbindung"mit einer Authentifizierungsmethode hergestellt bzw. getrennt.)
- Legen Sie in Citrix Cloud die Workspace-Authentifizierung auf die verbundene Methode fest.

> **Hinweis:**
>
> Die Managed Azure AD-Authentifizierungsmethode ist standardmäßig konfiguriert. Das heißt, es wird automatisch in Citrix Cloud verbunden, und die Workspace-Authentifizierung wird automa-

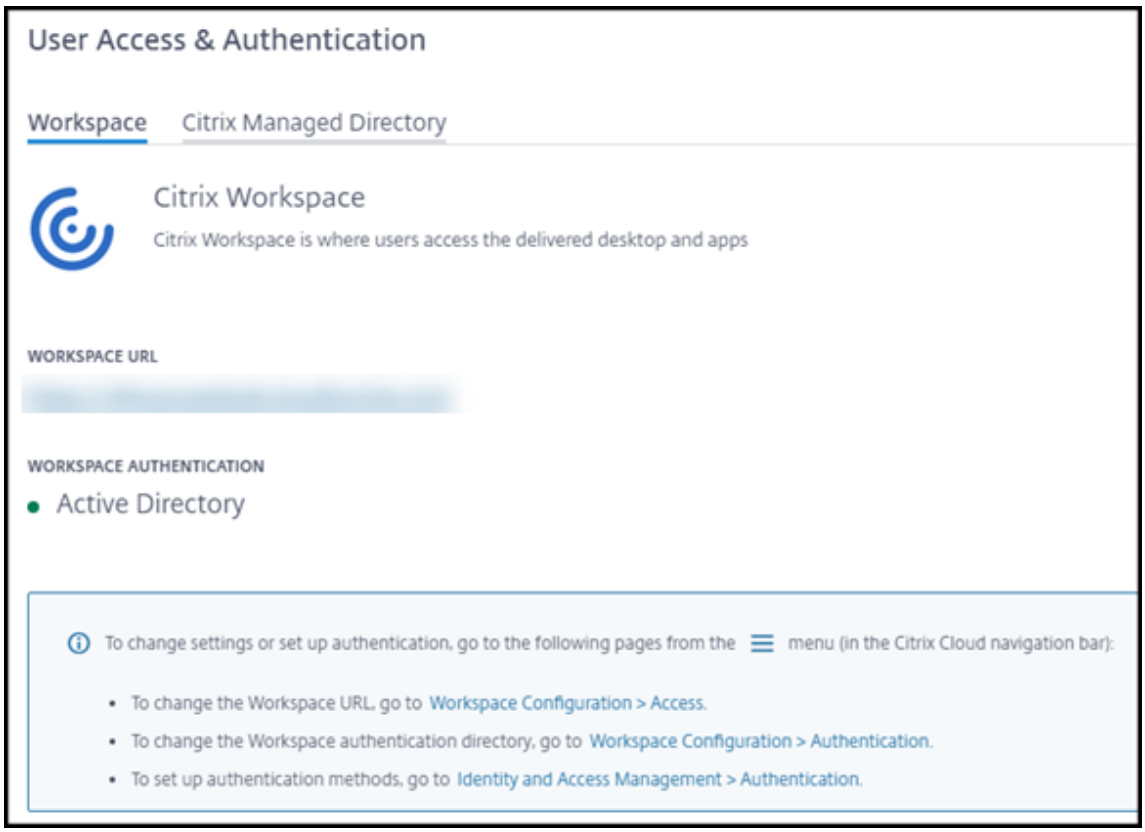
> tisch auf die Verwendung von Managed Azure AD for Citrix DaaS für Azure eingestellt. Wenn Sie diese Methode verwenden möchten und zuvor keine andere Methode konfiguriert haben, fahren Sie mit den Anweisungen unter Hinzufügen und Löschen von Benutzern in Managed Azure AD fort.
> Wenn Managed Azure AD 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. Klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure auf der rechten Seite auf **Benutzerzugriff und Authentifizierung** .



2. Klicken Sie auf **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.

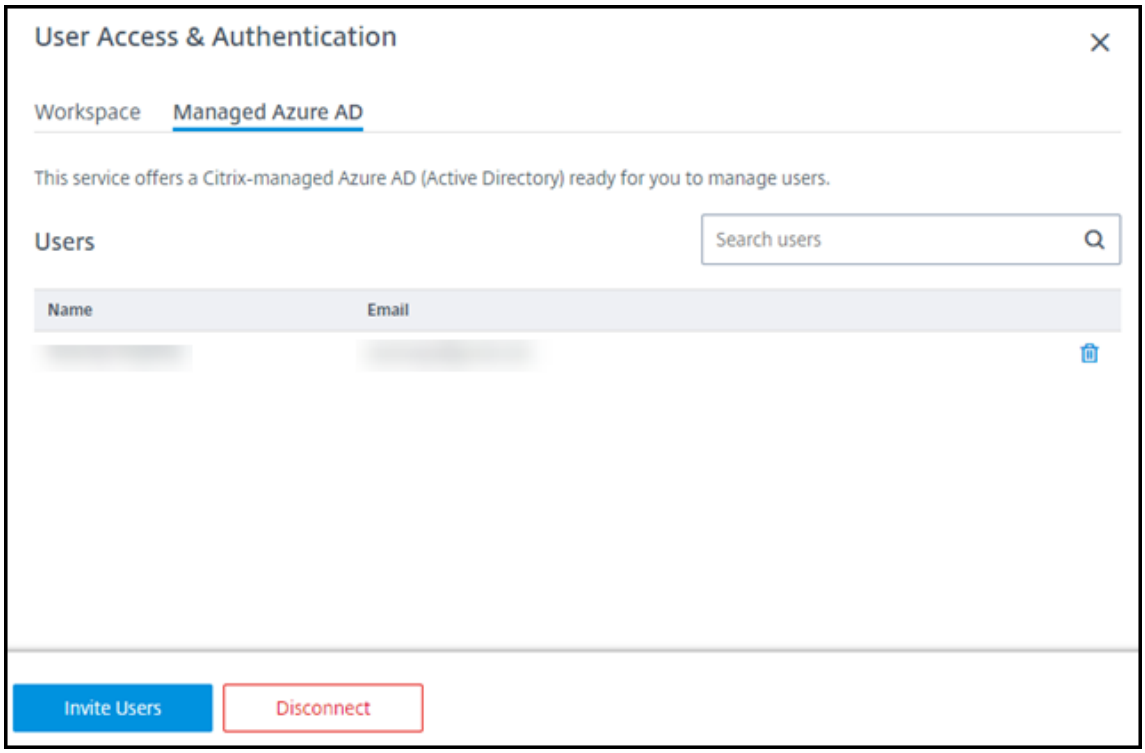
Sie geben die Namen und E-Mail-Adressen der Benutzer an. Citrix sendet dann an jeden per E-Mail eine Einladung. Die E-Mail weist Benutzer an, auf einen Link zu klicken, der sie mit dem Citrix Managed Azure AD verbindet.

- Hat ein Benutzer bereits ein Microsoft-Konto mit der von Ihnen angegebenen E-Mail-Adresse, wird dieses verwendet.

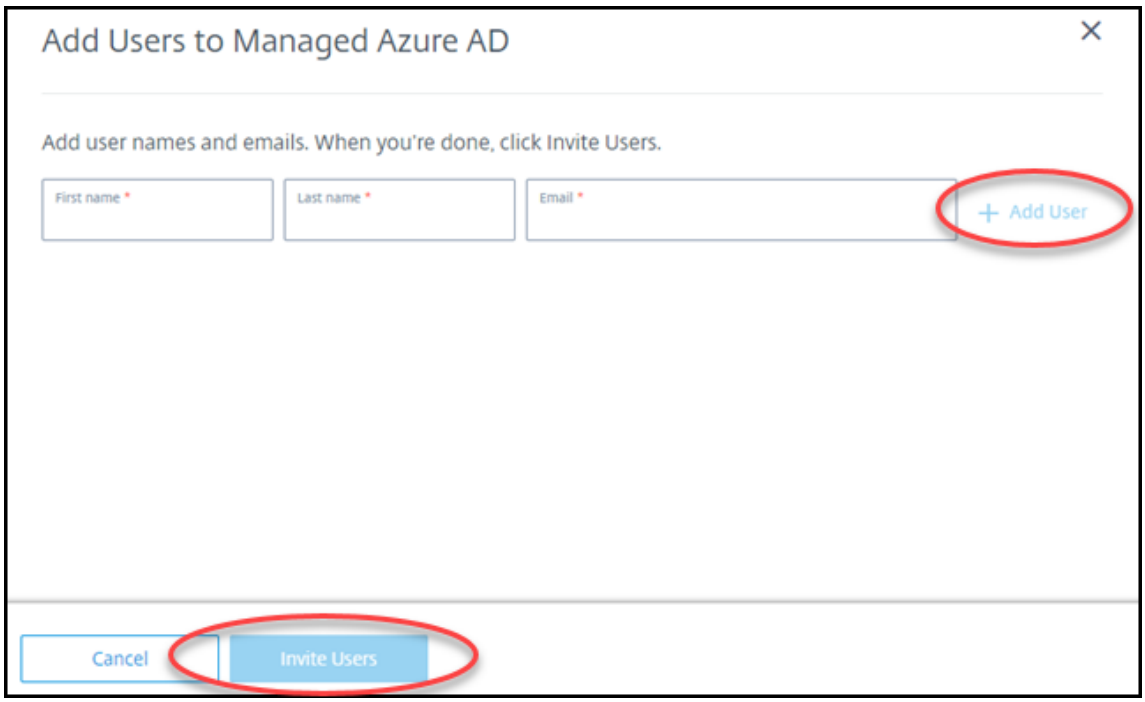
- Hat er kein Microsoft-Konto mit der E-Mail-Adresse, erstellt Microsoft ein Konto.

Gehen Sie zum Hinzufügen und Einladen von Benutzern zu Managed Azure AD folgendermaßen vor:

1. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Benutzerzugriff und Authentifizierung** ein. Klicken Sie auf **Benutzerzugriff und Authentifizierung verwalten**.
2. Klicken Sie auf die Registerkarte **Managed Azure AD** .
3. Klicken Sie auf **Benutzer einladen**.



4. Geben Sie den Namen und die E-Mail-Adresse eines Benutzers ein, und klicken Sie dann auf **Benutzer hinzufügen**.



5. Wiederholen Sie den vorherigen Schritt, um weitere Benutzer hinzuzufügen.
6. Wenn Sie mit dem Hinzufügen von Benutzerinformationen fertig sind, klicken Sie unten auf der Karte auf **Benutzer einladen** .

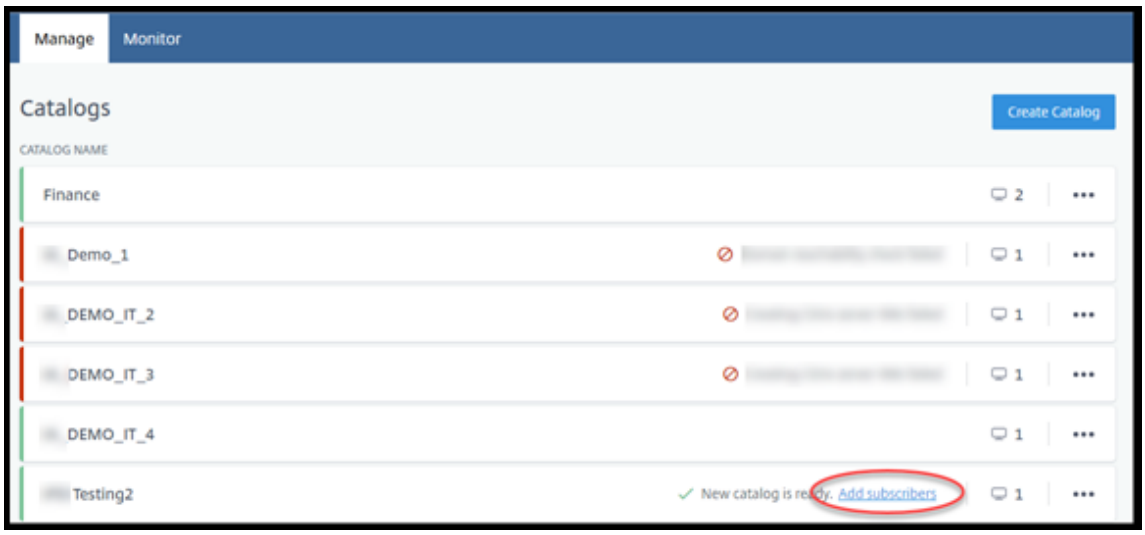
Um einen Benutzer aus Managed Azure AD zu löschen, klicken Sie auf das Papierkorbsymbol neben dem Namen des Benutzers, den Sie aus dem Verzeichnis löschen möchten. Bestätigen Sie die Löschung.

Nachfolgende Schritte: Benutzer zum Katalog hinzufügen

Hinzufügen oder Entfernen von Benutzern in einem Katalog

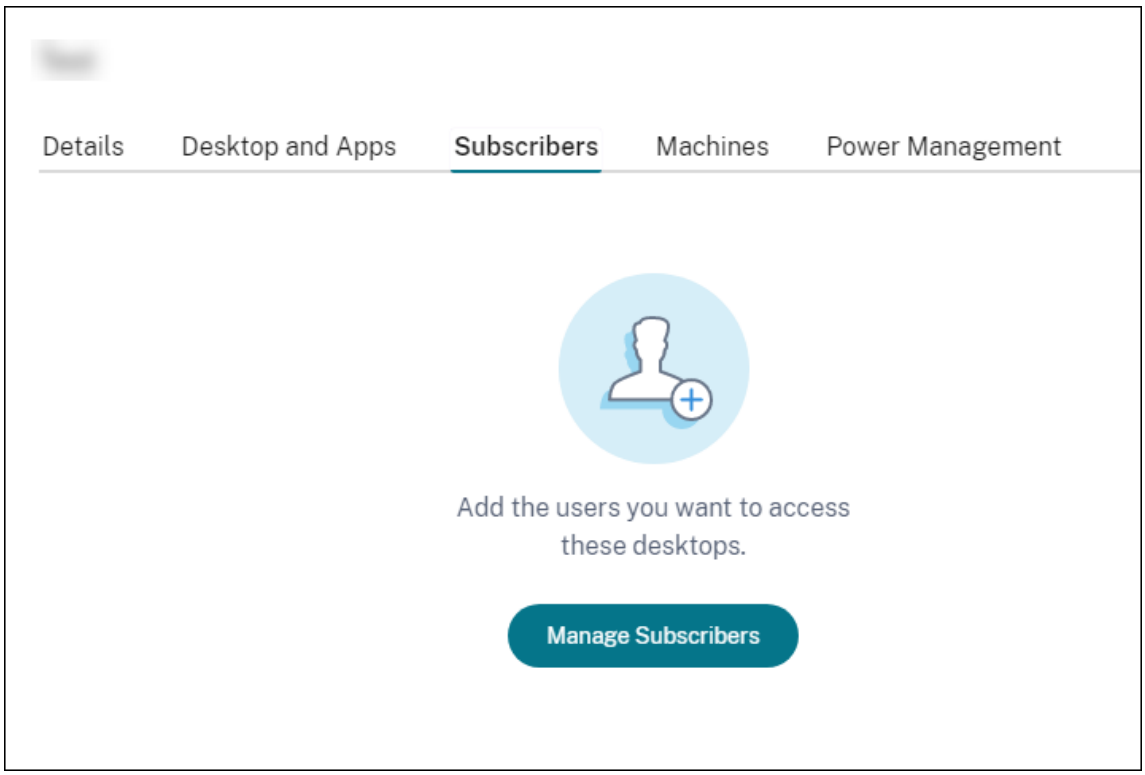
Dieses Verfahren gilt für alle Authentifizierungsmethoden.

1. Wenn Sie keine Benutzer zu einem Katalog hinzugefügt haben, klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure auf **Abonnenten hinzufügen**.

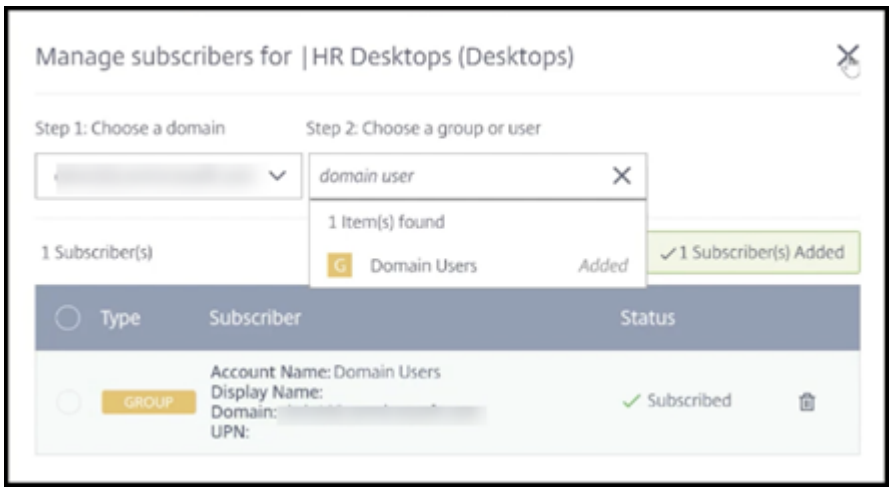


Sollen Benutzer zu einem Katalog hinzugefügt werden, der bereits Benutzer enthält, klicken Sie auf eine beliebige Stelle im Katalogeintrag.

2. Klicken Sie auf der Registerkarte **Abonnenten** auf **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, klicken Sie auf das **X** in der oberen rechten Ecke.

Zum Entfernen von Benutzern aus einem Katalog führen Sie die Schritte 1 und 2 aus. Klicken Sie in Schritt 3 auf das Papierkorbsymbol neben dem Namen, den Sie löschen möchten (anstatt eine Domäne und eine Gruppe/einen Benutzer auszuwählen). 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.
- Senden Sie für alle Kataloge die Citrix Workspace-URL an Ihre Benutzer.

Weitere Informationen

Weitere Informationen zur Authentifizierung in Citrix Cloud finden Sie unter Identitäts- und Zugriffsverwaltung.

Verwalten von Katalogen

September 7, 2022

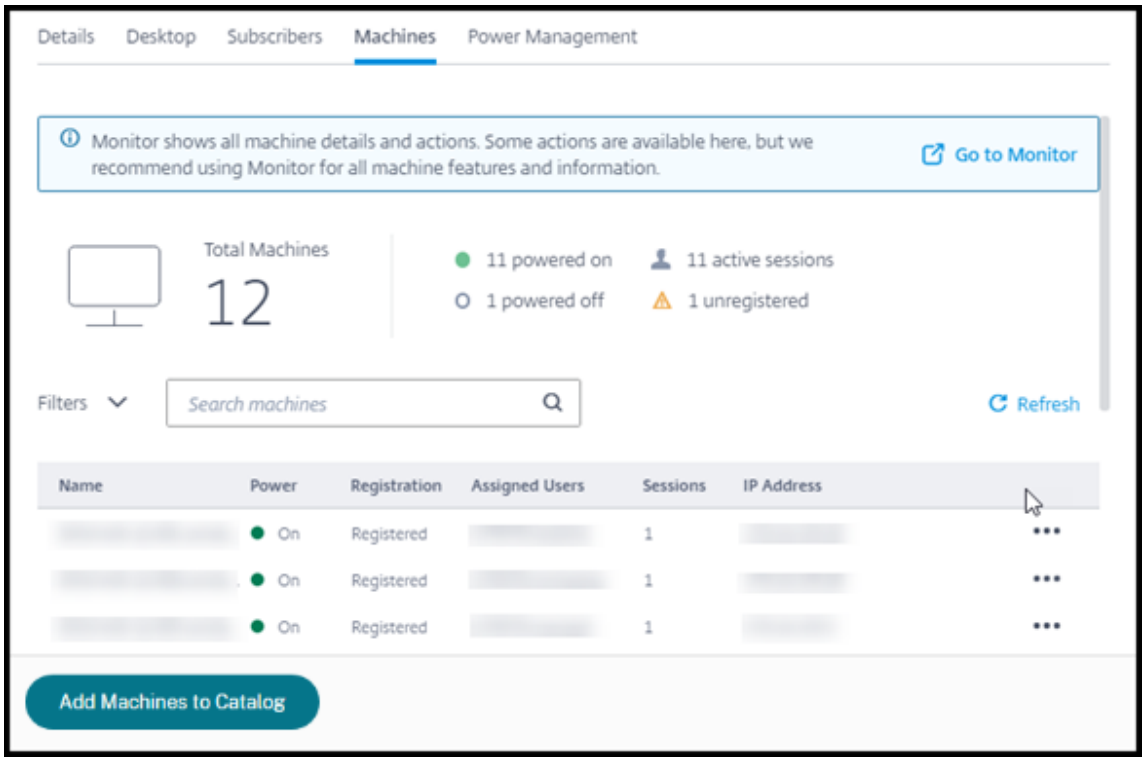
> **Hinweis:**
>
> In diesem Artikel werden die Aufgaben beschrieben, mit denen Sie Kataloge verwalten können, die in der Schnellbereitstellungsschnittstelle erstellt wurden. Informationen zur Katalogverwaltung mit der Verwaltungsschnittstelle für vollständige Konfiguration finden Sie unter Verwalten

> von Maschinenkatalogen.

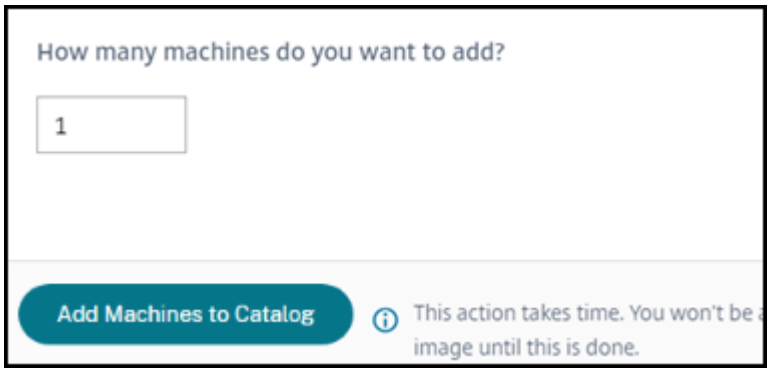
Hinzufügen von Maschinen zum Maschinenkatalog

Während Maschinen zu einem Katalog hinzugefügt werden, können Sie keine weiteren Änderungen an diesem Katalog vornehmen.

1. Klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.
2. Klicken Sie auf der Registerkarte **Computer** auf **Computer zum 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 Service-Konto ein.
5. Klicken Sie auf **Maschinen zum 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 im Dashboard **Verwalten > Azure Quick Deploy** einen Katalog aus, der Maschinen mit mehreren Sitzungen enthält
2. Klicken Sie auf der Registerkarte **Details** neben **Sitzungen pro Computer** auf **Bearbeiten**.
3. Geben Sie eine neue Anzahl an Sitzungen pro Maschine ein.
4. Klicken Sie auf **Anzahl der 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 Aktionen, die über das Dashboard **Verwalten > Azure Quick Deploy** verfügbar sind, sind auch über das **Monitor-Dashboard** in Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) verfügbar.

So wählen Sie Aktionen im Dashboard **Verwalten > Azure Quick Deploy** aus

1. Klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag eines Katalogs.
2. Suchen Sie auf der Registerkarte **Maschinen** die Maschine, die Sie verwalten möchten. Wählen Sie im Menü für die Maschine die gewünschte Aktion aus:

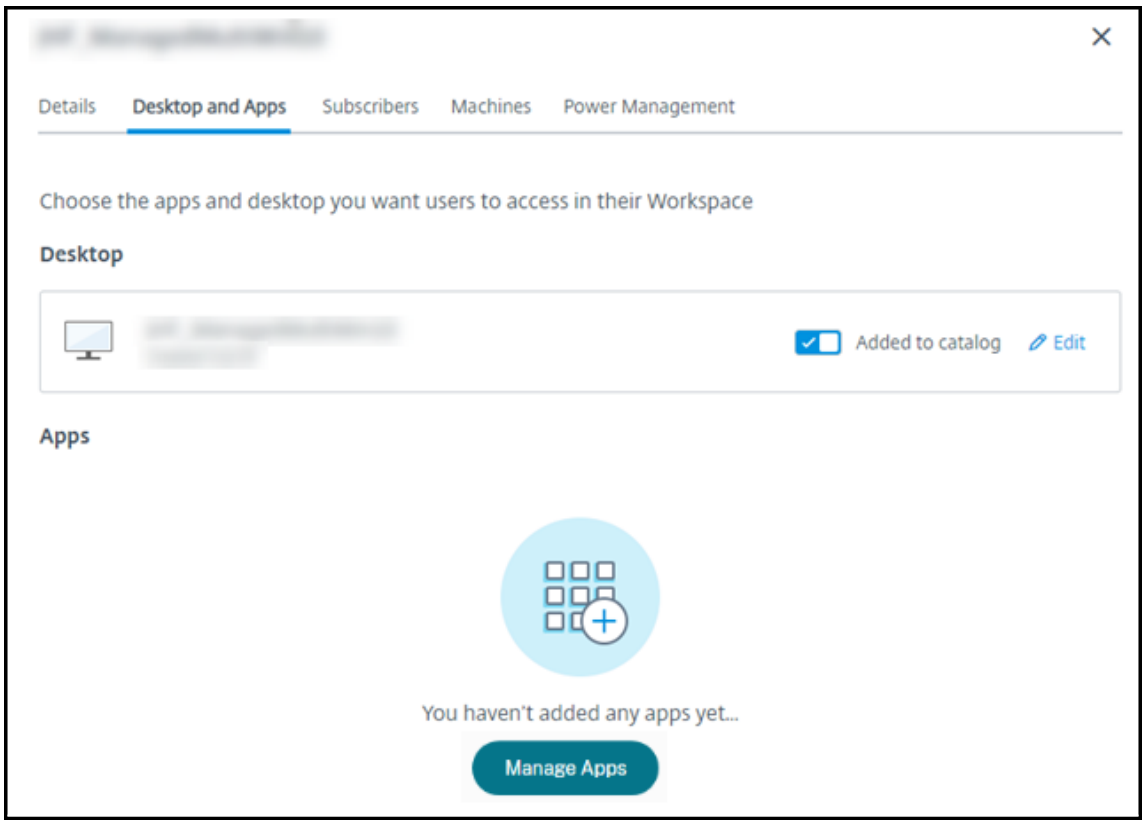
   - **Neustart:** Starten Sie den ausgewählten Computer neu.
   - **Start:** Starten Sie den ausgewählten Computer. Diese Aktion ist nur verfügbar, wenn die Maschine ausgeschaltet ist.
   - **Herunterfahren:** Fährt die Maschine herunter. Diese Aktion ist nur verfügbar, wenn die Maschine eingeschaltet ist.
   - **Wartungsmodus ein-/ausschalten:** Schalten Sie den Wartungsmodus für die ausgewählte Maschine ein (falls ausgeschaltet) oder aus (falls er eingeschaltet ist).

     Standardmäßig ist der Wartungsmodus ausgeschaltet. Das Einschalten des Wartungsmodus für eine Maschine 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. Möglicherweise möchten Sie eine Maschine in den Wartungsmodus versetzen, bevor Sie einen Patch anwenden oder ein Problem behandeln.
   - **Löschen:** Löscht den ausgewählten Computer. Diese Aktion ist nur verfügbar, wenn die Sitzungsanzahl Null ist. Bestätigen Sie die Löschung.

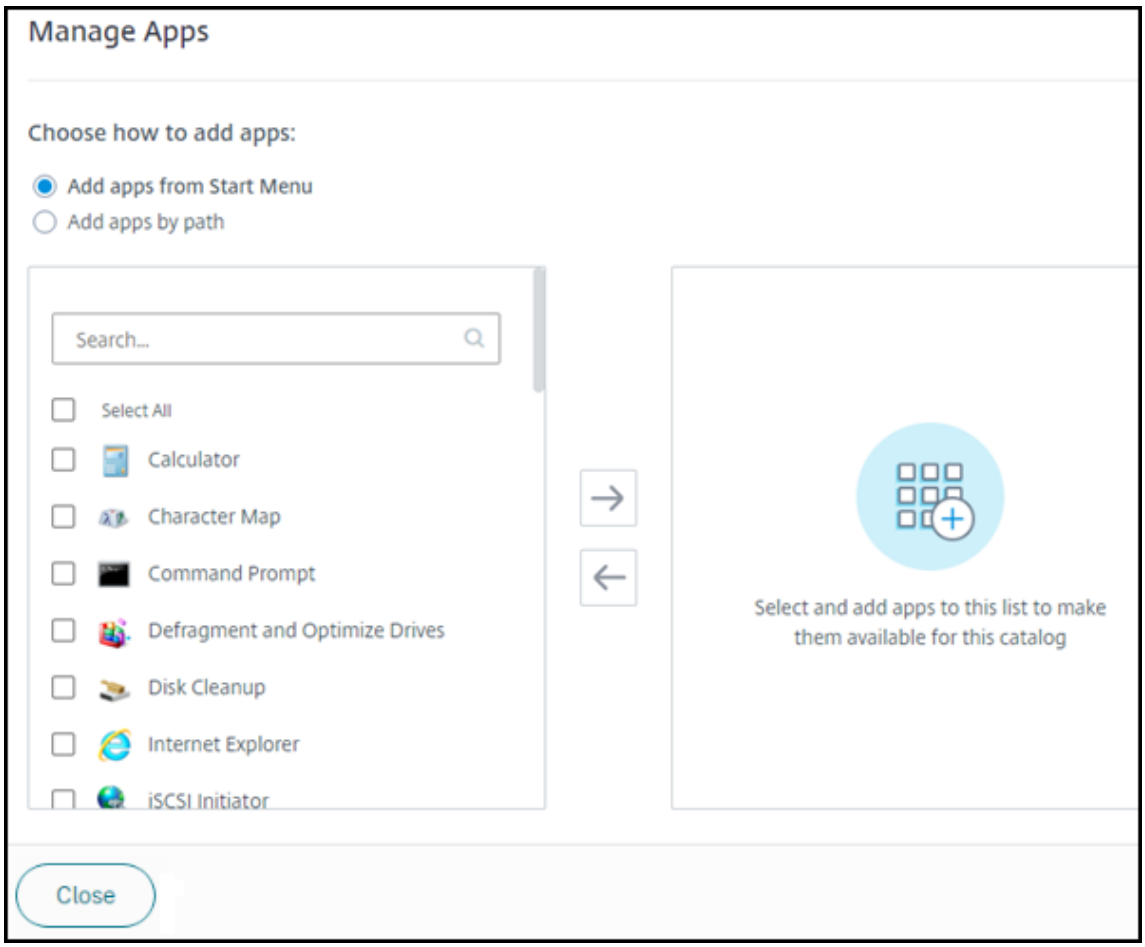
     Wenn eine Maschine gelöscht wird, werden alle Daten auf ihr entfernt.
   - **Neustart erzwingen:** Erzwingen Sie einen Neustart des ausgewählten Rechners. Wählen Sie diese Aktion nur aus, wenn eine **Neustartaktion** für den Computer fehlgeschlagen ist.

Hinzufügen von Apps zu einem Katalog

1. Klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.
2. Klicken Sie auf der Registerkarte **Desktop und Apps** auf **Apps verwalten**.

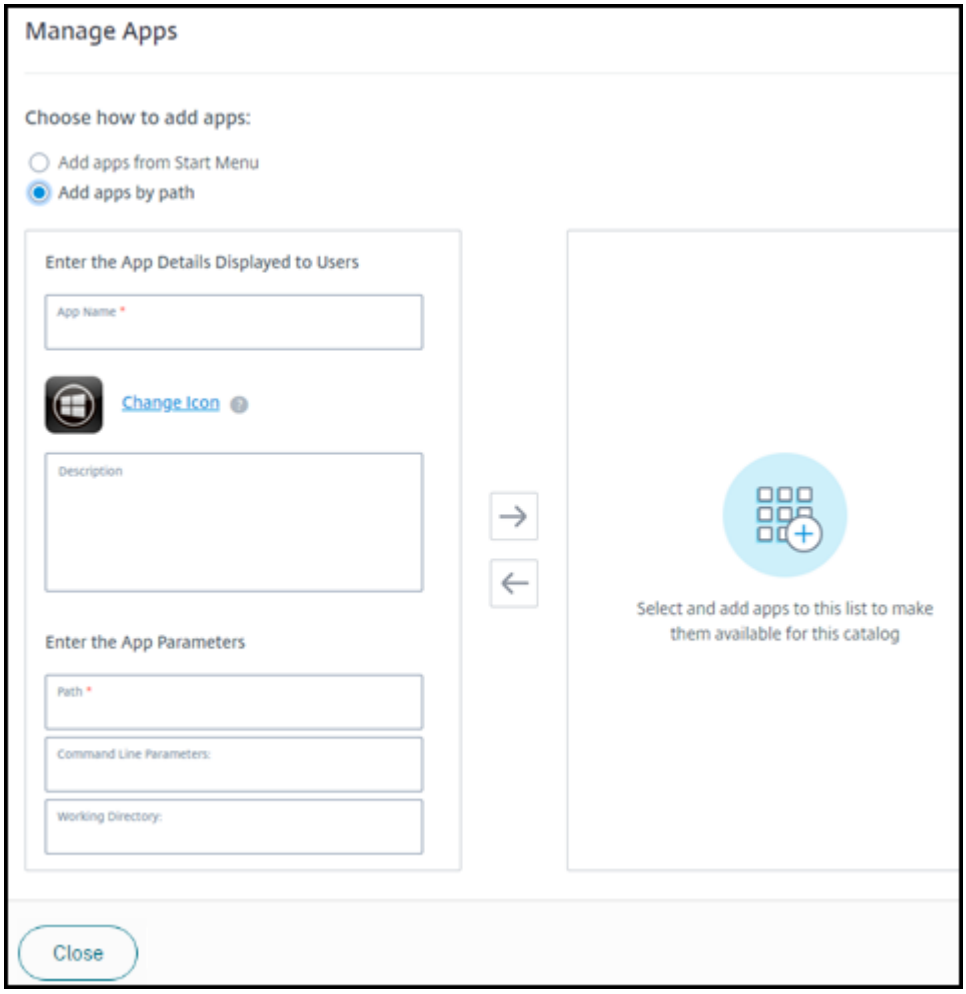


3. Wählen Sie aus, wie Sie Apps hinzufügen möchten: Über das Menü **Start** der Maschinen im Katalog oder aus einem anderen Pfad auf den Maschinen.
4. So fügen Sie Apps über das **Startmenü** hinzu:



- Wählen Sie in der linken Spalte verfügbare Apps aus. (Verwenden Sie die **Suche**, um die App-Liste anzupassen.) Klicken Sie auf 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. Klicken Sie auf 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, klicken Sie auf **Symbol ändern** und navigieren Sie zu dem Symbol, das Sie anzeigen möchten.
- 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. Einzelheiten zu Befehlszeilenparametern finden Sie unter Übergeben von Parametern an veröffentlichte Anwendungen.

6. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

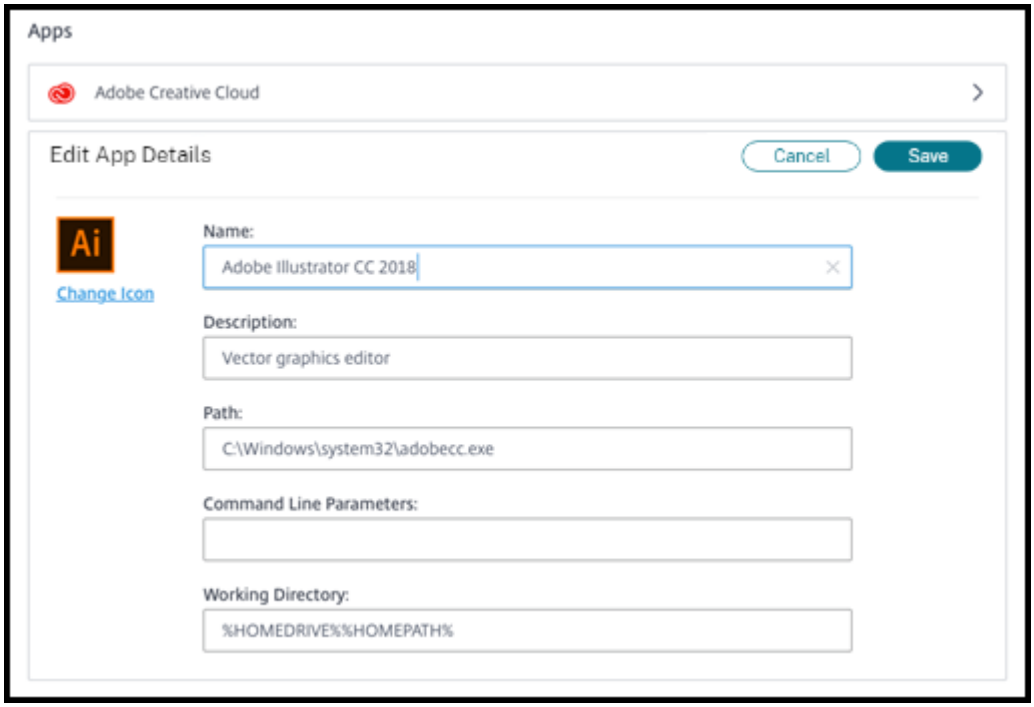
Was als Nächstes zu tun ist (wenn Sie den Ablauf zur Katalogerstellung und -bereitstellung abschließen): Senden Sie die Citrix Workspace-URL an Ihre Benutzer, falls Sie dies noch nicht getan haben.

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 im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.
2. Klicken Sie auf der Registerkarte **Desktop und Apps** auf eine beliebige Stelle in der Zeile mit der App, die Sie bearbeiten möchten.
3. Klicken Sie auf das Stiftsymbol .



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 zu ändern, das Benutzer in ihrem Citrix Workspace sehen, klicken Sie auf **Symbol ändern** und navigieren Sie zu dem Symbol, das Sie anzeigen möchten.
6. Klicken Sie zum Abschluss auf **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 im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.
2. Klicken Sie auf der Registerkarte **Desktop und Apps** auf das Papierkorbsymbol neben den Apps, 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 im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.

2. Klicken Sie auf der Registerkarte **Details** im unteren Bereich des Fensters auf **Katalog löschen**.
3. Bestätigen Sie das Löschen, indem Sie die Kontrollkästchen für die Bestätigung aktivieren und dann auf die Bestätigungsschaltfläche klicken.

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 für Azure 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. Wenn beispielsweise 100 aktive Sitzungen vorhanden sind und der Kapazitätspuffer 10% beträgt, bietet Citrix DaaS für Azure Kapazität für 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 im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs.
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. Klicken Sie oben auf **Benutzerdefiniert** und speichern Sie die aktuellen Einstellungen als neue Voreinstellung. Geben Sie einen Namen für das neue Preset ein und klicken Sie auf das Häkchen.
6. Wenn Sie fertig sind, klicken Sie auf **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.

VDA-Snapshot und -Wiederherstellung

Die Snapshot- und Wiederherstellungsfunktionen von Citrix DaaS für Azure bieten eine Möglichkeit zur Wiederherstellung nach ungeplantem Datenverlust oder anderen Ausfällen in VDAs, die Desktops und Apps bereitstellen. Der Snapshot-Vorgang nimmt einen Snapshot der Maschine auf und speichert ihn. Später verwendet ein Wiederherstellungsvorgang einen ausgewählten Snapshot.

- Sie können tägliche und wöchentliche Snapshot-Zeitpläne für alle Maschinen in einem Katalog konfigurieren. Diese Schnappschüsse werden als *automatische Snapshots*bezeichnet. Von jeder Maschine im Katalog wird ein Snapshot erstellt. Es gibt keine standardmäßigen Snapshot-Zeitpläne.
- Sie können bei Bedarf ein einzelnes V in einem Katalog sichern. Dies wird als manueller Snapshot bezeichnet. Sie können einen *manuellen Snapshot* einer Maschine erstellen, auch wenn der Katalog, zu dem sie gehört, geplante Snapshots enthält. (Sie können jedoch keine Einzelmaschinen-Snapshots planen.)

> **Wichtig:**
>
> Die Snapshot- und Wiederherstellungsfunktionen von Citrix DaaS für Azure werden nur für Maschinen in statischen Katalogen unterstützt und Benutzern zugewiesen.

Snapshot-Fahrpläne

Denken Sie daran: Snapshot-Zeitpläne gelten für alle Maschinen in einem Katalog.

Standardmäßig gibt es keine Snapshot-Zeitpläne.

So verwalten Sie Snapshot-Pläne:

1. Klicken Sie im Dashboard **Verwalten** auf eine beliebige Stelle im Katalogeintrag.
2. Klicken Sie auf der Registerkarte **Details** auf **Snapshots planen**.
3. Konfigurieren Sie auf der Seite **Snapshots planen** Zeitpläne für wöchentliche oder tägliche automatische Snapshots oder beides:
    - Um wöchentliche Snapshots hinzuzufügen oder zu ändern, verschieben Sie den Schieberegler für **wöchentliche automatische Schnappschüsse**, bis ein Häkchen angezeigt wird. Wählen Sie den Wochentag und die Startzeit aus.
    - Um tägliche Schnappschüsse hinzuzufügen oder zu ändern, bewegen Sie den Schieberegler für **tägliche automatische Schnappschüsse**, bis ein Häkchen angezeigt wird. Wählen Sie die Startzeit aus.
    - Um wöchentliche Snapshots zu entfernen, bewegen Sie den Schieberegler für **wöchentliche automatische Snapshots**, bis ein **X** angezeigt wird.
    - Um tägliche Schnappschüsse zu entfernen, bewegen Sie den Schieberegler für **tägliche automatische Schnappschüsse**, bis ein **X** angezeigt wird.
4. Wenn Sie fertig sind, klicken **Sie unten auf der Seite auf Speichern** .

Manuelle Schnappschüsse

Ein manueller Snapshot bezieht sich auf eine einzelne Maschine in einem Katalog. (Sie können keinen Zeitplan erstellen, um einen Snapshot einzelner Computer zu erstellen.)

1. Klicken Sie im Dashboard **Verwalten** auf eine beliebige Stelle im Katalogeintrag.
2. Suchen Sie auf der Registerkarte **Maschinen** den Computer, von dem Sie einen Snapshot erstellen möchten. Wählen Sie im Ellipsenmenü für dieses Gerät **Snapshots** aus.
3. Klicken Sie auf der Seite **Snapshots für *VDA-Name*** auf **Manuellen Snapshot erstellen**.
4. Geben Sie einen Namen für den Snapshot an. Empfehlung: Wählen Sie einen Namen, den Sie später leicht identifizieren können.
5. Bestätigen Sie Ihre Anforderung.

Snapshots anzeigen und verwalten

1. Klicken Sie im Dashboard **Verwalten** auf eine beliebige Stelle im Katalogeintrag.

2. Suchen Sie auf der Registerkarte **Maschinen** den Computer, von dem Sie einen Snapshot erstellen möchten. Wählen Sie im Ellipsenmenü für dieses Gerät **Snapshots** aus.
3. Auf der Seite **Backups für*VDA-Name***:

    - Wenn keine Snapshots für die Maschine vorhanden sind, werden Sie in einer Meldung entweder zum Erstellen eines manuellen Snapshots für diesen Computer oder zum Erstellen geplanter Snapshots für alle Maschinen im Katalog mit diesem Computer weitergeleitet.
    - Sie können einen der Snapshots auswählen und den Computer wiederherstellen. Siehe Wiederherstellen.
    - Sie können Schnappschüsse löschen. Markieren Sie die Kontrollkästchen für einen oder mehrere Snapshots und klicken Sie dann im Tabellenkopf auf **Löschen** . Bestätigen Sie Ihre Anforderung.

Tipp: Wenn Sie einen Katalog löschen, werden alle Snapshots zerstört.

Wiederherstellen

Sie können eine Maschine aus jedem verfügbaren Snapshot für diesen Computer wiederherstellen.

Während einer Wiederherstellung wird das Gerät ausgeschaltet. Keine der Aktionen im Ellipsenmenü eines Computers ist verfügbar, während ein Snapshot wiederhergestellt wird.

1. Klicken Sie im Dashboard **Verwalten** auf eine beliebige Stelle im Katalogeintrag.
2. Suchen Sie auf der Registerkarte **Maschinen** den Computer, von dem Sie einen Snapshot erstellen möchten. Wählen Sie im Ellipsenmenü für dieses Gerät **Snapshots** aus.
3. Aktivieren Sie auf der Seite **Snapshots für *VDA-Name*** das Kontrollkästchen des Snapshots, den Sie verwenden möchten.
4. Klicken Sie im Tabellenkopf auf **Wiederherstellen** .
5. Bestätigen Sie die Anfrage.

Die Spalte **Status** auf der Registerkarte **Maschinen** zeigt den Fortschritt und das Ergebnis des Wiederherstellungsvorgangs an.

Wenn ein Computer einen Snapshot nicht wiederherstellen kann, versuchen Sie es erneut.

Verwandte Informationen

- Aktualisieren eines Katalogs mit einem neuen Image
- Hinzufügen und Entfernen von Benutzern in einem Katalog
- Domänenbeitritt und nicht in die Domäne eingebunden

Überwachung

May 9, 2023

Im **Monitor-Dashboard** können Sie die Desktop-Nutzung, Sitzungen und Maschinen in Ihrer Bereitstellung von Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure) anzeigen. Sie können außerdem Sitzungen steuern, die Energieverwaltung von Maschinen einrichten und laufende Anwendungen sowie laufende Prozesse beenden.

So greifen Sie auf das **Monitor** Dashboard zu

1. Melden Sie sich bei Citrix Cloud an, falls Sie es noch nicht getan haben. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus.
2. Klicken Sie im Dashboard zum **Verwalten** auf die Registerkarte **Überwachen**.

Überwachen der Desktopnutzung

Wird auf dieser Seite alle fünf Minuten aktualisiert.

- **Überblick über Maschinen und Sitzungen:** Sie können die Anzeige so anpassen, dass Informationen zu allen Katalogen (Standard) oder einem ausgewählten Katalog angezeigt werden. Sie können auch den Zeitraum anpassen: den letzten Tag, die letzte Woche oder den letzten Monat.

  Zählungen oben auf dem Display geben die Gesamtzahl der Maschinen sowie die Anzahl der ein- und ausgeschalteten Maschinen an. 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 10s:** Um eine Top-10-Anzeige anzupassen, wählen Sie einen Zeitraum aus: die letzte Woche (Standard), Monat oder drei Monate. Sie können die Anzeige auch so anpassen, dass nur Informationen über Aktivitäten mit Einzelsitzungsmaschinen, Mehrsitzungsmaschinen oder Anwendungen angezeigt werden.
  - **Top 10 aktive Benutzer:** Listet die Benutzer auf, die Desktops während des Zeitraums am häufigsten gestartet haben. Indem Sie auf einer Linie schweben, werden die gesamten Starts angezeigt.
  - **Top 10 aktive Kataloge:** Listet die Kataloge mit der längsten Dauer während des ausgewählten Zeitraums auf. Dauer ist die Summe aller Benutzersitzungen aus diesem Katalog.

Bericht über die Desktop-Nutzung

Um einen Bericht mit Informationen zu Computerstarts im letzten Monat herunterzuladen, klicken Sie auf **Aktivität starten**. Eine Meldung zeigt an, dass die Anforderung verarbeitet wird. Der Bericht wird automatisch an den standardmäßigen Downloadspeicherort auf dem lokalen Computer heruntergeladen.

Filtern und suchen, um Maschinen und Sitzungen zu überwachen

Wenn Sie Sitzungs- und Maschineninformationen überwachen, werden standardmäßig alle Computer oder Sitzungen angezeigt. Sie haben folgende Möglichkeiten:

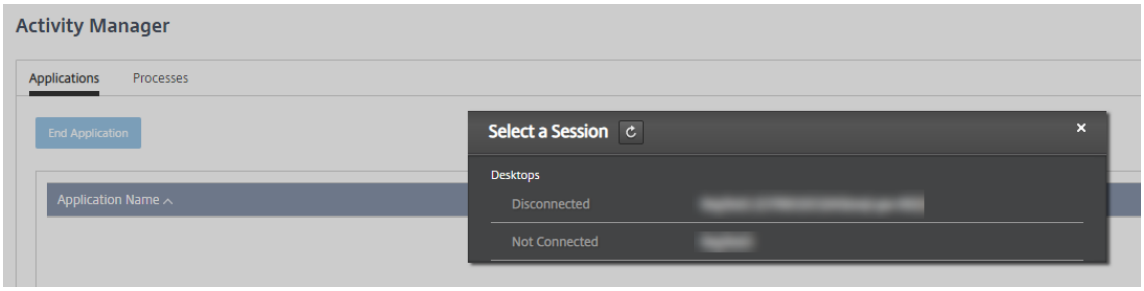
- Filtern Sie die Anzeige nach Computern, Sitzungen, Verbindungen oder Anwendungen.
- Verfeinern Sie die Anzeige von Sitzungen oder Computern, indem Sie die gewünschten Kriterien auswählen und einen Filter mithilfe von Ausdrücken erstellen.

- Speichern Sie die Filter, die Sie erstellen, zur Wiederverwendung.

Steuern Sie die Anwendungen eines Benutzers

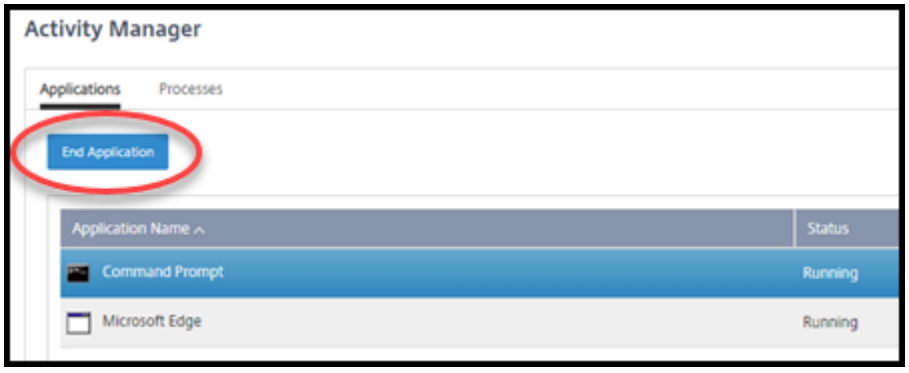
Sie können Anwendungen und Prozesse für einen Benutzer anzeigen und verwalten, der eine laufende Sitzung oder einen zugewiesenen Desktop hat.

1. Klicken Sie im **Überwachungs-Dashboard** auf **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 Suche auszublenden, klicken Sie erneut auf **Suchen**.)
2. Wählen Sie eine Sitzung.



   Der Activity Manager listet die Anwendungen und Prozesse für die Sitzung des Benutzers auf.

3. Um eine Anwendung zu beenden, klicken Sie auf der Registerkarte **Anwendungen** im Aktivitätsmanager in die Zeile der Anwendung, um diese Anwendung auszuwählen, und klicken Sie dann auf **Anwendung beenden**.



4. Um einen Prozess zu beenden, klicken Sie auf der Registerkarte **Prozesse** im Aktivitätsmanager in die Zeile des Prozesses, um diesen Prozess auszuwählen, und klicken Sie dann auf **Prozess beenden**.
5. Um Sitzungsdetails anzuzeigen, klicken Sie oben rechts auf **Details** . Um zur Anzeige von Anwendungen und Prozessen zurückzukehren, klicken Sie oben rechts auf Aktivitätsmanager.

6. Um die Sitzung zu steuern, klicken Sie auf **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 darin 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 `User`-Titelleiste angezeigt.

Das Spiegeln wird in einer neuen Browserregisterkarte gestartet. Stellen Sie sicher, dass Ihr Browser Popups der Citrix Cloud-URL zulässt.

In einem Citrix Managed Azure-Abonnement wird das Spiegeln nur für Benutzer domänengebundener Maschinen unterstützt. Um eine nicht domänengebundene Maschine in einem Citrix Managed Azure-Abonnement 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.

Spiegeln aktivieren

1. Wechseln Sie im **Überwachungs-Dashboard** zur Ansicht **Benutzerdetails**.
2. Wählen Sie die Benutzersitzung aus und klicken Sie dann in der Ansicht des **Aktivitäts-Managers** oder im Fenster **Sitzungsdetails** auf **Spiegeln**.

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.

Monitor verwendet den FQDN, um eine Verbindung zum Linux-Ziel-VDA herzustellen. Vergewissern Sie sich, dass der Überwachungsclient den FQDN des Linux-VDAs auflösen kann.

- Der VDA muss die Pakete `python-websockify` und `x11vnc` installiert haben.
- Die `noVNC`-Verbindung zum VDA verwendet das WebSocket-Protokoll. Standardmäßig wird das `ws://` WebSocket-Protokoll verwendet. Aus Sicherheitsgründen empfiehlt Citrix, das sichere `wss://` Protokoll 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, 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 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, 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.

Überwachen und Steuern von Sitzungen

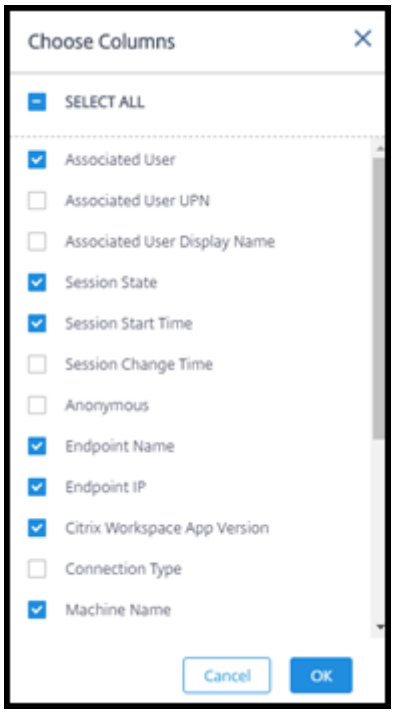
Sitzungsanzeigen werden jede Minute aktualisiert.

Neben dem Anzeigen von Sitzungen können Sie Sitzungen trennen und Benutzer von Sitzungen abmelden.

1. Klicken Sie im **Überwachungsdashboard** auf **Filter**.

2. Wählen Sie die Ansicht **Sitzungen** aus.

3. Um die Anzeige anzupassen, klicken Sie auf **Spalten auswählen** und aktivieren Sie die Kontrollkästchen der Elemente, die angezeigt werden sollen. Wenn Sie fertig sind, klicken Sie auf **OK**. Die Sitzungsanzeige wird automatisch aktualisiert.



4. Klicken Sie auf das Kontrollkästchen links neben jeder Sitzung, die Sie steuern möchten.
5. Um die Sitzung abzumelden oder zu trennen, wählen Sie entweder "**Sitzungssteuerung**"> "**Abmelden**" oder "**Sitzungssteuerung**"> "**Trennen**".

Denken Sie daran, dass der Energieverwaltungszeitplan für den Katalog auch das Trennen von Sitzungen und das Abmelden von Benutzern von getrennten Sitzungen steuern kann.

Alternativ zum obigen Verfahren können Sie auch **nach einem Benutzer suchen**, die Sitzung auswählen, die Sie steuern möchten, und dann Sitzungsdetails anzeigen. Die Optionen zum Abmelden und Trennen sind dort ebenfalls verfügbar.

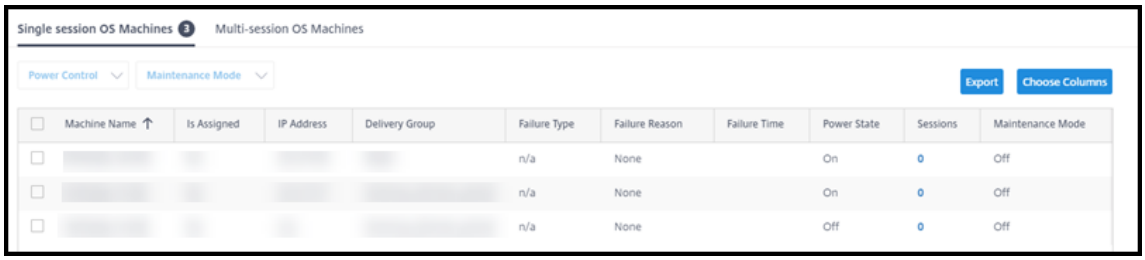
Bericht über Sitzungsinformationen

Um Sitzungsinformationen herunterzuladen, klicken Sie in der Sitzungsanzeige auf **Exportieren** . Eine Meldung zeigt an, dass die Anforderung verarbeitet wird. Der Bericht wird automatisch an den standardmäßigen Downloadspeicherort auf dem lokalen Computer heruntergeladen.

Monitor- und Leistungssteuerungsmaschinen

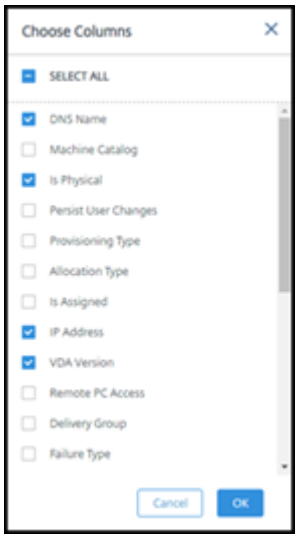
Die Anzeige der Maschinen wird jede Minute aktualisiert.

1. Klicken Sie im **Überwachungsdashboard** auf **Filter**.
2. Wählen Sie die Ansicht **Maschinen**.

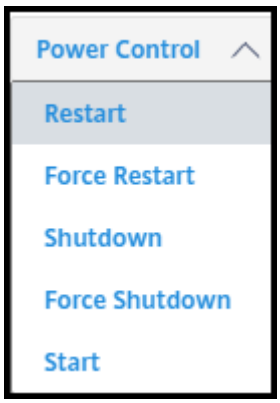


   Standardmäßig listet die Anzeige Betriebssystemmaschinen für Einzelsitzungen auf. Alternativ können Sie Multi-Session-Maschinen anzeigen.

3. Um die Anzeige anzupassen, klicken Sie auf **Spalten auswählen** und aktivieren Sie die Kontrollkästchen der Elemente, die angezeigt werden sollen. Wenn Sie fertig sind, klicken Sie auf **OK**. Die Anzeige des Rechners wird automatisch aktualisiert.



4. Um Maschinen mit Strom zu steuern oder sie in den Wartungsmodus zu versetzen oder zu verlassen, aktivieren Sie das Kontrollkästchen links neben jedem Computer, den Sie steuern möchten.
5. Um die ausgewählten Computer mit Strom zu steuern, klicken Sie auf **Power Control** und wählen Sie eine Aktion aus.



6. Um die ausgewählten Maschinen in den Wartungsmodus oder aus dem Wartungsmodus zu versetzen, klicken Sie auf **Wartungsmodus > EIN** oder **Wartungsmodus > AUS**.

Wenn Sie die Suchfunktion verwenden, um eine Maschine zu suchen und auszuwählen, sehen Sie Maschinendetails, Auslastung, historische Auslastung (der letzten sieben Tage) und durchschnittliche IOPS.

Bericht über Maschineninformationen

Um Sitzungsinformationen herunterzuladen, klicken Sie auf der Computeranzeige auf **Exportieren**. Eine Meldung zeigt an, dass die Anforderung verarbeitet wird. Der Bericht wird automatisch an den standardmäßigen Downloadspeicherort auf dem lokalen Computer heruntergeladen.

Überprüfen der Integrität von Apps und Desktops

Probing automatisiert den Prozess der Überprüfung des Zustands veröffentlichter Apps und Desktops. Die Ergebnisse der Integritätsprüfung sind über das **Monitor-Dashboard** verfügbar. Einzelheiten finden Sie in den folgenden Abschnitten:

- Anwendungstests
- Desktoptests

Citrix DaaS für Azure für Citrix Service Provider

September 7, 2022

In diesem Artikel wird beschrieben, wie Citrix Service Provider (CSPs) Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure Service) für Kunden (Mandanten) 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 haben ein Abonnement für Citrix DaaS für Azure.

Einschränkungen

- Es kann bis zu 24 Stunden dauern, bis Änderungen des Kundennamens auf allen Schnittstellen angewendet werden.
- Beim Erstellen eines Kunden muss die E-Mail-Adresse eindeutig sein.

Bekannte Probleme

- Nachdem der Benutzer eines Kunden einer Ressource zugewiesen wurde, können Sie ihn nicht entfernen oder die Zuweisung aufheben.
- Die Verwaltungskonsole erzwingt keine Trennung von Kundenbenutzern. Sie sind dafür verantwortlich, Benutzer zu den entsprechenden Katalogen und Ressourcen hinzuzufügen.

Kunden hinzufügen

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Klicken Sie in dem Menü oben links auf **Kunden**.
2. Klicken Sie im **Kunden-Dashboard** auf **Einladen oder Hinzufügen**. Geben Sie die angeforderten Informationen an.

   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.
3. 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 weitere Administratoren hinzufügen und steuern, welche Kunden sie in den Citrix DaaS für Azure **Manage** and **Monitor-Dashboards** sehen können.

Hinzufügen von Citrix DaaS für Azure zu einem Kunden

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Klicken Sie in dem Menü oben links auf **Kunden**.
2. Wählen Sie im **Kunden-Dashboard** im Auslassungsmenü den Befehl **Service hinzufügen** für den Kunden aus.
3. Klicken **Sie unter Wählen Sie einen hinzuzufügenden Dienst**aus auf **Citrix DaaS Standard für Azure**.
4. Klicken Sie auf **Weiter**.

Nachdem Sie dieses Verfahren abgeschlossen haben, wird der Kunde in Ihr Citrix DaaS für Azure-Abonnement integriert.

Wenn das Onboarding abgeschlossen ist, wird automatisch ein neuer Kunde in Citrix DaaS für Azure erstellt. Der Kunde ist unter **Verwalten > Quick Deploy**sichtbar.

Ressourcen nach Kunden filtern

Sie können Ressourcen im Dashboard Citrix DaaS für Azure **Verwalten > Azure Quick Deploy** nach Kunden filtern. (Standardmäßig werden alle Ressourcen angezeigt.) Wenn Sie mit Ressourcen wie Katalogen, Maschinenimages und Azure-Abonnements arbeiten, können Sie bestimmte Kundenanzeigen auswählen, um die Ressourcen Ihrer Mandanten zu organisieren.

SD-WAN-Verbindungen werden auf Kundenbasis hergestellt. Der Kunde muss über eine SD-WAN Orchestrator Service Orchestrator-Serviceberechtigung verfügen.

- Um eine SD-WAN-Verbindung für einen Kunden herzustellen, befolgen Sie die Anweisungen unter Erstellen einer SD-WAN-Verbindung. Wählen Sie auf der Seite **Netzwerkverbindung hinzufügen** den Kunden aus. Sie können das Feld SD-WAN-Verbindungstyp nur auswählen, wenn dieser Kunde über eine SD-WAN Orchestrator Service Orchestrator-Dienstberechtigung verfügt.
- Damit der Verbindungsaufbau erfolgreich ist, muss der Kunde auch über einen installierten Master Control Node (MCN) verfügen. Nur die SD-WAN Orchestrator-Dienstberechtigung bestimmt jedoch, ob der SD-WAN-Verbindungstyp ausgewählt werden kann.

Erstellen Sie Kataloge zur Bereitstellung von Apps und Desktops

Ein Katalog ist eine Gruppe von Benutzern und die Sammlung virtueller Maschinen, auf die sie Zugriff haben. Wenn Sie einen Katalog erstellen, wird ein Image (mit anderen Einstellungen) als Vorlage zum

Erstellen der Maschinen verwendet. Einzelheiten finden Sie unter Erstellen von Katalogen.

Verbunddomänen

Mithilfe von Verbunddomänen können sich die Benutzer des Kunden mit Anmeldeinformationen aus einer mit Ihrem Ressourcenstandort verknüpften Domäne bei ihrem Workspace anmelden. Sie können Ihren Kunden dedizierte Arbeitsbereiche bereitstellen, auf die ihre Benutzer über eine benutzerdefinierte Workspace-URL zugreifen können (z. B. `customer.cloud.com`), während der Ressourcenstandort in Ihrem Citrix Cloud-Konto verbleibt.

Sie können neben dem freigegebenen Workspace dedizierte Arbeitsbereiche bereitstellen, auf die Kunden beispielsweise über Ihre CSP-Workspace-URL zugreifen können. `csppartner.cloud.com` Um den Kundenzugriff auf seinen dedizierten Workspace zu ermöglichen, fügen Sie sie den entsprechenden Domänen hinzu, die Sie verwalten.

Nach der Konfiguration des Arbeitsbereichs über Workspace Configurationkönnen sich die Benutzer der 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. Klicken Sie in dem Menü oben links auf **Kunden**.
2. Wählen Sie im **Kunden-Dashboard** im Menü oben links die Option **Identitäts- und Zugriffsverwaltung** aus.
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. Klicken Sie auf das Pluszeichen neben dem Kundennamen. Der ausgewählte Kunde wird nun in der Spalte **Verbundkunden** angezeigt. Wiederholen Sie die Schritte, um weitere Kunden hinzuzufügen.
5. Wenn Sie fertig sind, klicken Sie auf **Anwenden**.

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 in Citrix Cloud im Menü oben links die Option **Identitäts- und Zugriffsverwaltung** aus.

2. Wählen Sie auf der Registerkarte **Domänen** im **Auslassungsmenü für die Domäne, die Sie verwalten** möchten, die Sie verwalten möchten.
3. Suchen oder suchen Sie aus der Liste der Verbundkunden nach den Kunden, die Sie entfernen möchten.

   - Klicken Sie auf **X**, um einen Kunden zu entfernen.
   - Um alle aufgelisteten Kunden aus der Domäne zu entfernen, klicken Sie auf **Alle entfernen**.

   Die ausgewählten Kunden wechseln zur Liste der **verfügbaren Kunden**.
4. Klicken Sie auf **Anwenden**.
5. Überprüfen Sie die von Ihnen ausgewählten Kunden, und klicken Sie dann auf **Kunden entfernen**.

Hinzufügen eines Administrators mit eingeschränktem Zugriff

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Klicken Sie in dem Menü oben links auf **Kunden**.
2. Wählen Sie im **Kunden-Dashboard** im Menü oben links die Option **Identitäts- und Zugriffsverwaltung** aus.
3. Klicken Sie auf der Registerkarte **Administratoren** auf **Administratoren hinzufügen von** und wählen Sie **Citrix-Identität**.
4. Geben Sie die E-Mail-Adresse der Person ein, die Sie als Administrator hinzufügen, und klicken Sie auf **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. Wählen Sie bei Bedarf ein oder mehrere Rollen- und Geltungsbereichspaare für Citrix DaaS für Azure aus.
7. Wenn Sie fertig sind, klicken Sie auf **Einladung senden**.

Wenn der Administrator die Einladung annimmt, hat er den von Ihnen zugewiesenen Zugriff.

Partnerzugriff auf Kundenidentitätsanbieter

Sie können Benutzer über das Dashboard Citrix DaaS für Azure **Manage > Azure Quick Deploy** oder die Citrix Cloud-Konsole verwalten.

Wenn Sie einen Nicht-AD-Identitätsanbieter für Benutzer verwenden (z. B. Citrix Managed Azure AD), müssen Sie Citrix Cloud Identity and Workspace-Administrator für den Kunden sein, bevor Sie Be-

nutzer für diesen Kunden verwalten können. Wenn Sie kein Administrator für einen Kunden sind, können Sie keine Benutzer für diesen Kunden hinzufügen oder löschen.

Um Benutzer für einen Kunden über das Dashboard **Verwalten > Azure Quick Deploy** zu verwalten, wählen Sie den Partner oder Kunden unter **Elemente anzeigen für**aus.

- **Beispiel 1:** Wählen Sie unter **Artikel anzeigen für** Kunde A aus. Das Dashboard zeigt jetzt nur die Artikel für Kunde A. Wenn Sie einen Katalog auswählen, sehen Sie nur die Benutzer von Kunde A auf der Registerkarte **Abonnenten** . Sie können Benutzer für Kunde A hinzufügen oder entfernen (vorausgesetzt, Sie sind Administrator für diesen Kunden).
- **Beispiel 2:** Sie wählen den Partnereintrag unter **Artikel anzeigen für**aus. Das Dashboard zeigt jetzt nur Partnerartikel an. Auf der Registerkarte **Abonnenten** sehen Sie nur Benutzer, die für den Partner erstellt wurden. Es werden keine Kundeneinträge angezeigt. Sie können Benutzer für diesen Partner hinzufügen oder entfernen (vorausgesetzt, Sie sind Administrator dieses Partners), aber Sie können von diesem Standort aus keine Kundenbenutzer verwalten.

Um Benutzer für einen Kunden über die Citrix Cloud-Konsole zu verwalten, wählen Sie den Kunden aus, wenn Sie nach der Anmeldung dazu aufgefordert werden (oder später mit **Kunden ändern** im oberen rechten Bereich der Citrix Cloud-Konsole). Wenn Sie die Bibliothek zur Verwaltung von Benutzern verwenden, spiegelt der Anzeigekontext den ausgewählten Kunden wider. Wenn Sie beispielsweise Kunde A ausgewählt haben, zeigt die Bibliothek nur die Angebote von Kunde A an.

Bearbeiten der Berechtigungen zur delegierten Administration für Administratoren

1. Melden Sie sich mit Ihren CSP-Anmeldeinformationen bei Citrix Cloud an. Klicken Sie in dem Menü oben links auf **Kunden**.
2. Wählen Sie im **Kunden-Dashboard** im Menü oben links die Option **Identitäts- und Zugriffsverwaltung** aus.
3. Wählen Sie auf der Registerkarte **Administratoren** im Menü für den Administrator die Option **Zugriff bearbeiten**.
4. Wählen oder löschen Sie die Rollen- und Geltungsbereichspaare für Citrix DaaS für Azure nach Bedarf. Achten Sie darauf, nur Einträge zu aktivieren, die den eindeutigen, für den Kunden erstellten Bereich enthalten.
5. Klicken Sie auf **Speichern**.

Zugreifen und Konfigurieren von Arbeitsbereichen

Jeder Kunde erhält seinen eigenen Workspace mit einer eindeutigen URL `customer.cloud.com`. Diese URL ist der Ort, an dem die Benutzer des Kunden auf ihre veröffentlichten Apps und Desktops zugreifen.

- **In Citrix DaaS Standard für Azure:** Zeigen Sie im Dashboard **Verwalten > Azure Quick Deploy** die URL an, indem Sie auf der rechten Seite **Benutzerzugriff und Authentifizierung** erweitern.
- **Aus Citrix Cloud:** Wählen Sie im **Kunden-Dashboard** im Menü oben links die Option **Workspace-Konfiguration** aus. Zeigen Sie die URL auf der Registerkarte **Zugriff** an.

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:

- Konfigurieren von Workspaces
- Sichere Workspaces

Überwachung des Service für einen Kunden

Das Dashboard von Citrix DaaS für Azure **Monitor** in einer CSP-Umgebung entspricht im Wesentlichen einer Nicht-CSP-Umgebung. Einzelheiten finden Sie unter Überwachen.

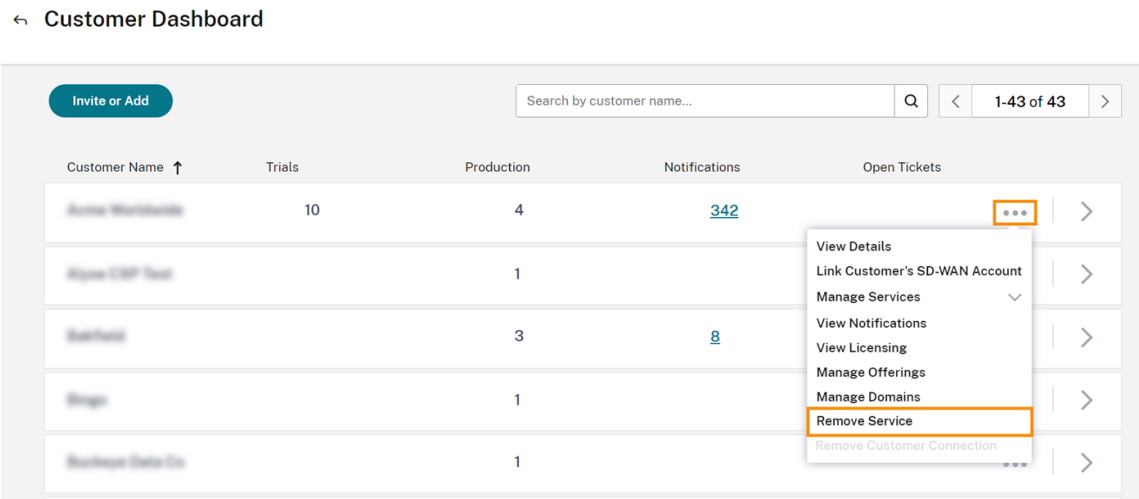
Standardmäßig zeigt das Dashboard **Überwachen** Informationen über alle Kunden an. Um Informationen zu einem Kunden anzuzeigen, wählen Sie **Kunden auswählen**.

Beachten Sie, dass die Möglichkeit, **Monitoranzeigen** für einen Kunden anzuzeigen, durch den konfigurierten Zugriff des Administrators gesteuert wird.

Entfernen von Diensten

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Kundenbereich nicht mit Objekten des Citrix DaaS Standard für Azure 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. Weitere Informationen zum Aufheben der Verknüpfung von Bereichen 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 **Kunden-Dashboard** auf das Ellipsenmenü (**...**) des Kunden, von dem Sie einen Dienst entfernen möchten, und wählen Sie **Service entfernen**aus.



Die Seite **Dienst zum Entfernen auswählen** wird angezeigt.

3. Klicken Sie auf **Entfernen**, um den Dienst zu entfernen.

Problembehandlung

September 7, 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. Citrix installiert und aktualisiert die Cloud Connectors.

Optional können Sie verschiedene Aktionen an Cloud Connectors und Ressourcenstandorten ausführen. Siehe:

- Aktionen für Ressourcenstandorte
- Ressourcenstandorteinstellungen beim Erstellen eines Katalogs

Citrix DaaS für Azure verfügt über Tools zur Fehlerbehebung und Unterstützbarkeit, mit denen Sie Konfigurations- und Kommunikationsprobleme mit den Maschinen lösen können, die Desktops und Apps (die VDAs) bereitstellen. 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. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Troubleshoot & Support** ein.
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. Blenden Sie im Dashboard **Verwalten > Azure Quick Deploy** in Citrix DaaS für Azure rechts **Troubleshoot & Support** ein.
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.

Limits

May 9, 2023

In diesem Artikel werden die Beschränkungen für Ressourcen in einer Bereitstellung von Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) aufgeführt.

> **Hinweis:**
>
> Die Grenzwerte sind Empfehlungen von Citrix.

Konfigurationslimits

Ressource	Limit
Active Directory-Domänen	25
Kataloge	100
Ressourcenstandorte	25
VDAs pro Abonnement	2.500

Limits für Ressourcenstandorte

Die folgende Tabelle enthält die Limits für Ressourcen auf Ressourcenstandortebene. Wenn Ihre Anforderungen diese Grenzwerte überschreiten, empfiehlt Citrix, mehr Ressourcenstandorte zu verwenden.

Ressource	Limit
Active Directory-Domänen	1
Einzelsitzungs-VDAs	10.000
Multisitzungs-VDAs	1.000

Citrix Cloud Connectors werden Ressourcenstandorten zugewiesen und verknüpfen Workloads mit Citrix DaaS für Azure. Informationen zu den Cloud Connector-Beschränkungen sowie Größen- und Skalierungsempfehlungen finden Sie unter Überlegungen zu Größe und Skalierung für Cloud Connectors.

Provisioning-Limits

In der folgenden Tabelle sind die empfohlenen Maximen für ein einzelnes Citrix Cloud-Konto aufgeführt.

Für größere Bereitstellungen empfiehlt Citrix ein Hub-and-Spoke-Modell, bei dem VDAs über mehrere Abonnements und Netzwerkverbindungen verteilt sind.

Ressource	Limit
Multi-Session-VDAs pro Katalog	500
VDAs für Einzelsitzungen pro Katalog	1,200
VDAs pro Microsoft Azure-Abonnement	2,500

Nutzungslimits

Ressource	Limit
Concurrent Monitor Volladministratoren	5
Gleichzeitige Endbenutzer	100,000
Für einen Benutzer veröffentlichte Ressourcen	250
Sitzungsstarts pro Minute	3,000

Grenzwerte für Studien

In der folgenden Tabelle sind die Grenzwerte während einer Testversion von Citrix DaaS für Azure aufgeführt.

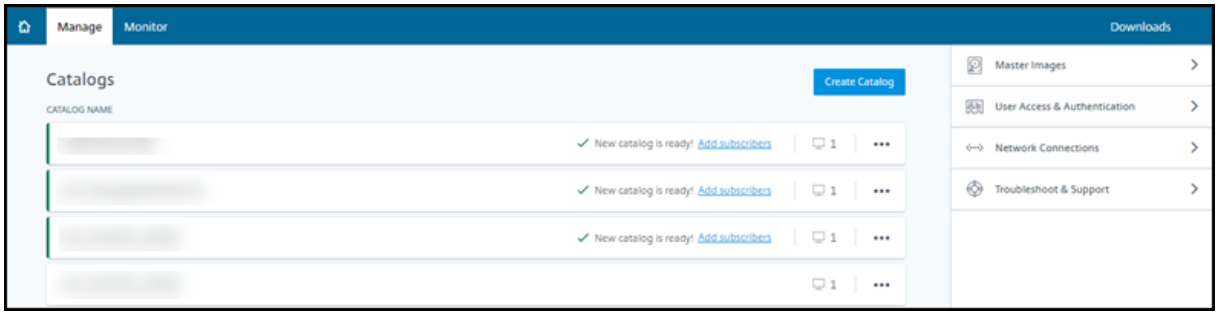
Azure-Abonnement	Ressource	Limit
Citrix Managed Azure-Abonnement	Maximale Anzahl von Katalogen	3
	Maximale Anzahl von Benutzern	25
	Maximale Anzahl von VDAs pro Katalog	3
Kundenverwaltetes Azure-Abonnement	Maximale Anzahl von Katalogen	10
	Maximale Anzahl von Benutzern	25
	Maximale Anzahl von VDAs pro Katalog	10

Referenz

September 7, 2022

Dashboards

Die meisten Administratoraktivitäten für Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard for Azure-Dienst) können über die **Verwalten**- und **Überwachen**-Dashboards eingegeben werden. Nachdem Sie Ihren ersten Katalog erstellt haben, wird das **Verwalten**-Dashboard automatisch gestartet, wenn Sie sich bei Citrix Cloud anmelden und Citrix DaaS für Azure auswählen.



Sie können auf die Dashboards zugreifen, nachdem Ihre Anfrage für eine Testversion oder einen Kauf genehmigt und abgeschlossen wurde.

So greifen Sie auf die Dashboards zu:

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Services > DaaS Standard für Azure** aus. (Alternativ können Sie auf der Kachel **DaaS Standard für Azure** im Hauptbereich der Anzeige auf **Verwalten** klicken.)
3. Wenn noch kein Katalog erstellt wurde, klicken Sie auf der **Willkommensseite** auf **Erste Schritte**. Sie werden zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet.
4. Wenn bereits ein Katalog erstellt wurde, werden Sie automatisch zum Dashboard **Verwalten > Azure Quick Deploy** weitergeleitet.
5. Um auf das **Überwachen**-Dashboard zuzugreifen, klicken Sie auf die Registerkarte **Überwachen**.

Klicken Sie auf das Symbol in der unteren rechten Ecke, um im Produkt eine Anleitung über das Dashboard zu erhalten.

Katalog-Registerkarten im Dashboard verwalten

Klicken Sie im Dashboard **Verwalten > Azure Quick Deploy** auf eine beliebige Stelle im Eintrag des Katalogs. 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 der Maschinenaktionen sind auch über das **Monitor-Dashboard** verfügbar. Siehe Überwachungs- und Leistungssteuerungsmaschinen.
- **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, die in die Domäne eingebundene Maschinenenthalten. Sie können ihn ignorieren, wenn Sie nur nicht domänengebundene Maschinen verwenden.

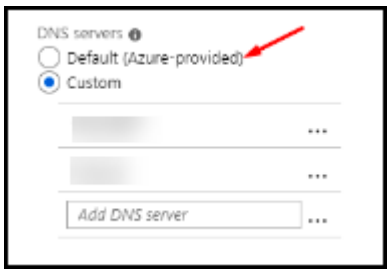
1. Bevor Sie einen domänengebundenen Katalog erstellen (oder, im Fall eines Citrix Managed Azure-Abonnements eine Verbindung), prüfen Sie, ob Sie DNS-Servereinträge haben, die öffentliche und private Domänennamen auflösen können.

   Wenn Citrix DaaS für Azure einen Katalog oder eine Verbindung erstellt, sucht es nach mindestens einem gültigen DNS-Servereintrag. 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. Citrix DaaS für Azure kann nicht mit der **Standardeinstellung (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 die Einträge, die Sie mit Citrix DaaS für Azure 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.). Sie können sie auch in Citrix DaaS für Azure ändern.
- Wenn Sie ein Citrix Managed Azure-Abonnement verwenden, synchronisiert Citrix DaaS für Azure keine DNS-Adressänderungen, die Sie in Azure vornehmen. Sie können jedoch die DNS-Einstellungen für die Verbindung in Citrix DaaS für Azure ändern.

Denken Sie daran, dass das Ändern von DNS-Serveradressen zu Verbindungsproblemen für Maschinen in Katalogen führen kann, die diese Verbindung verwenden.

DNS-Server über Citrix DaaS für Azure hinzufügen

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, klicken Sie auf der Seite *Verbindungstyp***hinzufügen** auf **DNS-Server bearbeiten** . Wenn eine Meldung darauf hinweist, dass keine DNS-Serveradressen gefunden wurden, klicken Sie auf **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 im Dashboard **Verwalten > Azure Quick Deploy** die Option **Netzwerkverbindungen** auf der rechten Seite.
    b) Wählen Sie die gewünschte Verbindung.
    c) Klicken Sie auf **DNS-Server bearbeiten**.
3. Fügen Sie Adressen hinzu, bzw. ändern oder entfernen Sie Adressen.
    a) Um eine Adresse hinzuzufügen, klicken Sie auf **DNS-Server hinzufügen** und geben Sie dann 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, klicken Sie auf das Papierkorbsymbol neben dem Adresseintrag. Sie können nicht alle DNS-Serveradressen entfernen. Die Verbindung benötigt mindestens eine Adresse.
4. Wenn Sie fertig sind, klicken Sie unten auf der Seite auf **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`, dadurch wird der Gruppenrichtlinien-Editor geöffnet.
4. Klicken Sie in `User Configuration Citrix Policies` > `Unfiltered` auf **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. Befolgen Sie das Verfahren unter Festlegen von Gruppenrichtlinien für nicht in die Domäne eingebundene Maschinen, Schritt 2 bis zum Ende.

> **Hinweis:**
>
> Obwohl die Citrix Studio-Konsole in Citrix DaaS für Azure nicht verfügbar ist, lesen Sie die Referenzartikel zu Richtlinieneinstellungen, um zu erfahren, was verfügbar ist.

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 Ressourcenstandorteinstellungen beim Erstellen eines Katalogs.

(Für 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 im Dashboard **Verwalten > Azure Quick Deploy** die Option **Cloud-Abonnements** auf der rechten Seite.
2. Klicken Sie auf 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 Anzahl umfasst keine Maschinen, die für andere Zwecke wie Images, Cloud Connectors oder RDS-Lizenzserver verwendet werden
   - 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. Klicken Sie auf **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, klicken Sie auf **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. Klicken Sie dann auf **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. Klicken Sie zum Abschluss auf **Speichern**.

Umbenennen

Geben Sie den neuen Namen für den Ressourcenstandort ein. Klicken Sie auf **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 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 Gruppenrichtlinieneinstellungen

1. Installieren Sie einen Lizenzserver für die Remotedesktopdienste auf einer der verfügbaren VMs. 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 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.

Auf der Karte **Allgemein** im Dashboard **Verwalten > Azure Quick Deploy** gibt der Wert **Verbrauch** an, wie viel Verbrauch im aktuellen Kalendermonat verbraucht wurde. Der Wert beinhaltet die monatliche und die Laufzeitverbrauchsverpflichtung.

Wenn Sie auf **Allgemein**klicken, enthält die Registerkarte **Benachrichtigungen** :

- 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 Verwendung finden Sie unter Überwachen von Lizenzen und Verwendung für Citrix DaaS Standard für Azure.

Sie können optional verlangen, dass Benachrichtigungen im Dashboard **verwalten** angezeigt werden, wenn die Verbrauchsnutzung (für monatliche, Laufzeiten oder beide Verpflichtungen) ein bestimmtes Niveau erreicht. Standardmäßig sind diese Benachrichtigungen deaktiviert.

1. Klicken Sie auf der Registerkarte **Benachrichtigungen** auf **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. Klicken Sie auf **Speichern**.

Um Benachrichtigungen zu deaktivieren, klicken Sie auf den Schieberegler, damit das Häkchen nicht mehr angezeigt wird, und klicken Sie dann auf **Speichern**.

Überwachen der Citrix Lizenznutzung

Um Informationen zur Citrix-Lizenznutzung anzuzeigen, befolgen Sie die Anweisungen unter Überwachen von Lizenzen und Verwendung für Citrix DaaS Standard für Azure. 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. Studio, Quick Deploy).
>
> Stellen Sie sicher, dass die maximalen Sitzungslimits für alle Kataloge konfiguriert wurden, bevor Sie fortfahren.
>
> - In der Quick Deploy-Verwaltungsoberfläche für Citrix DaaS für Azure befindet sich diese Einstellung auf der Registerkarte **Details** jedes Katalogs.
> - Verwenden Sie in anderen Citrix DaaS-Diensten und -Editionen die Einstellungen für die Lastenverwaltungsrichtlinie.

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 Service-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 für Azure berechnet und weist dann

für jede Maschine mit mehreren Sitzungen einen Lastindex 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 im Dashboard **Verwalten > Azure Quick Deploy** rechts **Allgemein** .
2. Klicken Sie unter **Globale Einstellungen**auf **Alle anzeigen**.
3. Wählen Sie auf der Seite **Globale Einstellungen** unter **Lastausgleich für Multisitzungskataloge** die Lastausgleichsmethode.
4. Klicken Sie auf **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. Starten Sie im Dashboard **Verwalten > Azure Quick Deploy** die Katalogerstellung, indem Sie die erforderlichen Informationen angeben und dann unten auf der Seite auf **Katalog erstellen** klicken.
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 in der Citrix DaaS für Azure-Konsole **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 von der Citrix Cloud-Konsole aus einen Cloud Connector auf jeder VM. Stellen Sie sicher, dass sich die Cloud Connectors am selben Ressourcenstandort befinden, der zuvor erstellt wurde. Folgen Sie den Anweisungen in folgenden Artikeln:

- Konfiguration von Cloud Connector-Proxy und Firewall
- Anforderungen an System und Konnektivität

5. Wiederholen **Sie im Dashboard Verwalten > Azure Quick Deploy** den Prozess der 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 mit Citrix DaaS für Azure benötigen, öffnen Sie ein Support-Ticket, indem Sie den Anweisungen unter How to Get Help and Supportfolgen.