Citrix DaaS pour Azure

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Citrix DaaS Standard pour Azure

September 7, 2022

Introduction

Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure) est le moyen le plus simple et le plus rapide de fournir des applications et des postes Windows à partir de Microsoft Azure. Citrix DaaS pour Azure offre une gestion, un provisionnement et une capacité gérée basés sur le cloud pour fournir des applications et des postes virtuels sur n'importe quel appareil.

Cette solution comprend :

- Gestion et provisionnement basés sur le cloud pour la mise à disposition de bureaux virtuels Azure hébergés par Citrix et d'applications à partir de machines multi-sessions.
- Une expérience utilisateur haute définition à partir d'un large éventail d'appareils, à l'aide de l'application Citrix Workspace.
- Workflows simplifiés de création et de gestion d'images, ainsi que des images mono-session et multi-session Windows et Linux préparées par Citrix sur lesquelles le dernier Citrix Virtual Delivery Agent (VDA) est installé.
- Accès à distance sécurisé depuis n'importe quel appareil à l'aide des points de présence globaux du Citrix Gateway Service.
- Fonctionnalités avancées de surveillance et de gestion du service d'assistance.
- IaaS Azure géré, y compris le calcul, le stockage et la mise en réseau Azure pour la fourniture de postes de travail virtuels.

La fonctionnalité Citrix Remote PC Access permet aux utilisateurs d'utiliser à distance des machines physiques existantes situées dans le bureau. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir leur session PC de bureau.

Si vous connaissez d'autres produits Citrix DaaS, Citrix DaaS pour Azure simplifie le déploiement d'applications et de bureaux virtuels. Citrix peut gérer l'infrastructure d'hébergement de ces charges de travail.

Citrix DaaS pour Azure est un service Citrix Cloud. Citrix Cloud est la plateforme qui héberge et administre les services Citrix Cloud. En savoir plus sur Citrix Cloud.

Pour en savoir plus sur les composants, le flux de données et les considérations de sécurité, voir Présentation de la sécurité technique. Cet article décrit également les responsabilités des clients et de Citrix.

Comment les utilisateurs accèdent aux postes de travail et aux applications

Les utilisateurs (parfois appelés abonnés) accèdent à leurs bureaux et applications directement via leur navigateur, à l'aide du client Citrix HTML5. Les utilisateurs accèdent à une URL Citrix Workspace fournie par vous, leur administrateur. La plate-forme Citrix Workspace énumère et fournit les ressources numériques aux utilisateurs. Les utilisateurs démarrent un bureau ou une application depuis leur espace de travail.

Après avoir configuré un catalogue de machines qui fournissent des bureaux et des applications (ou un catalogue contenant des machines physiques pour Remote PC Access), Citrix DaaS pour Azure affiche l'URL de l'espace de travail. Vous devez ensuite informer vos utilisateurs d'accéder à cette URL pour démarrer leur bureau et leurs applications.

Au lieu d'accéder à Citrix Workspace pour accéder à leurs bureaux et applications, les utilisateurs peuvent installer une application Citrix Workspace sur leur appareil. Téléchargez l'application adaptée au système d'exploitation du terminal : https://www.citrix.com/downloads/workspace-app/.

Concepts et terminologie

Cette section présente certains éléments et termes utilisés par les administrateurs dans Citrix DaaS pour Azure :

- Catalogues
- Emplacements des ressources
- Images
- Abonnements Azure
- Connexions réseau
- Membre d'un domaine et non joint à un domaine

Catalogues

Un catalogue est un groupe de machines.

- Les bureaux et applications que Citrix DaaS pour Azure fournit à vos utilisateurs résident sur des machines virtuelles (VM). Ces machines virtuelles sont créées (provisionnées) dans le catalogue.

  Lorsque vous déployez des postes de travail, les machines du catalogue sont partagées avec les utilisateurs sélectionnés. Lorsque vous publiez des applications, les machines multi-sessions hébergent des applications qui sont partagées avec les utilisateurs sélectionnés.

- Pour Remote PC Access, un catalogue contient des machines physiques mono-session existantes. Un déploiement courant inclut les machines situées dans votre bureau. Vous contrôlez

l'accès des utilisateurs à ces machines par le biais de la méthode d'attribution des utilisateurs configurée et des utilisateurs sélectionnés.

Si vous connaissez d'autres produits Citrix DaaS, un catalogue dans Citrix DaaS est similaire à la combinaison d'un catalogue de machines et d'un groupe de mise à disposition.

Pour plus d'informations, consultez :

- Créez des catalogues pour les postes de travail et les applications publiés.
- Créez des catalogues pour Remote PC Access.
- Gérez les catalogues.
- Utilisateurs et authentification.

Emplacements des ressources

Les machines d'un catalogue se trouvent dans un emplacement de ressources. Un emplacement de ressources contient également deux ou plusieurs Cloud Connector.

- Lors de la publication de postes de travail ou d'applications, Citrix crée automatiquement l'emplacement des ressources et les Cloud Connector lorsque vous créez le premier catalogue.
- Pour Remote PC Access, l'administrateur crée l'emplacement des ressources et les Cloud Connector avant de créer un catalogue.

Lorsque vous créez plus de catalogues pour des postes de travail et des applications publiés, l'abonnement Azure, la région et le domaine déterminent si Citrix crée un autre emplacement de ressource. Si ces critères correspondent à un catalogue existant, Citrix essaie de réutiliser cet emplacement de ressource.

Pour plus d'informations, consultez :

- Spécifiez les informations d'emplacement des ressources lorsque vous créez un catalogue.
- Actions de localisation des ressources.

Images

Lorsque vous créez un catalogue pour les bureaux et les applications publiés, une image de machine est utilisée (avec d'autres paramètres) comme modèle pour créer les machines.

- Citrix DaaS pour Azure fournit plusieurs images préparées par Citrix :
  - Windows 10 Entreprise (session unique)
  - Windows 10 Enterprise Virtual Desktop (sessions multiples)
  - Windows 10 Enterprise Virtual Desktop (sessions multiples) avec Office 365 ProPlus
  - Windows Server 2012 R2

  - Windows Server 2016
  - Windows Server 2019
  - Linux

  Chaque image préparée par Citrix possède un VDA Citrix et des outils de dépannage installés. Le VDA est le mécanisme de communication entre les machines de vos utilisateurs et l'infrastructure Citrix Cloud qui gère Citrix DaaS pour Azure.

  Citrix met à jour les images préparées disponibles lors de la sortie d'une nouvelle version de VDA.

- Vous pouvez également importer et utiliser vos propres images depuis Azure. Vous devez installer un VDA (et d'autres logiciels) sur l'image avant de pouvoir l'utiliser pour créer un catalogue.

Le terme VDA fait souvent référence à la machine qui fournit des applications ou des postes de travail, et au composant logiciel installé sur cette machine.

Pour plus d'informations, consultez la section Images.

Abonnements Azure

Vous pouvez créer des catalogues pour mettre à disposition des bureaux et des applications, et créer/importer des images dans un abonnement Citrix Managed Azure ou dans votre propre abonnement Azure (géré par le client).

Si vous commandez uniquement Citrix DaaS pour Azure, vous devez importer (ajouter) et utiliser vos propres abonnements Azure. Si vous commandez également un fonds de consommation Citrix Azure, vous recevez un abonnement Citrix Managed Azure. Vous pouvez ensuite utiliser un abonnement Citrix Managed Azure ou l'un de vos abonnements Azure importés lors de la création d'un catalogue ou de la création d'une nouvelle image.

Pour plus d'informations, consultez :

- Lesscénarios de déploiement illustrent les manières d'utiliser les abonnements Azure avec Citrix DaaS pour Azure.
- Les abonnements Azure expliquent les différences entre Citrix Managed Azure et les abonnements Azure gérés par le client. Cet article explique également comment afficher, ajouter et supprimer des abonnements.
- L'aperçu technique de la sécurité décrit les différences de responsabilité entre Citrix Managed Azure et les abonnements Azure gérés par le client.

Connexions réseau

Lorsque vous créez un catalogue à l'aide d'un abonnement Citrix Managed Azure, vous indiquez si et comment les utilisateurs peuvent accéder aux emplacements et aux ressources de leur réseau local d'entreprise à partir de leurs bureaux et applications publiés. Les choix possibles sont l'absence de connectivité, l'appairage de réseaux virtuels Azure et Citrix SD-WAN.

Lorsque vous utilisez votre propre abonnement Azure, il n'est pas nécessaire de créer une connexion. Il vous suffit d'importer (ajouter) votre abonnement Azure au service.

Pour plus d'informations, consultez la section Connexions réseau.

Membre d'un domaine et non joint à un domaine

Plusieurs opérations et fonctionnalités de service diffèrent selon que les machines (VDA) sont jointes à un domaine ou non. L'appartenance au domaine affecte également les scénarios de déploiement disponibles.

- Les machines appartenant à un domaine et non jointes à un domaine prennent en charge toutes les méthodes d'authentification utilisateur disponibles dans l'espace de travail de l'utilisateur.
- Vous pouvez publier des bureaux, des applications ou les deux à partir de machines appartenant à un domaine ou non. Les machines des catalogues Remote PC Access doivent être jointes à un domaine.

Le tableau suivant répertorie plusieurs différences entre les machines non jointes au domaine et les machines jointes au domaine lors de la mise à disposition de bureaux et d'applications.

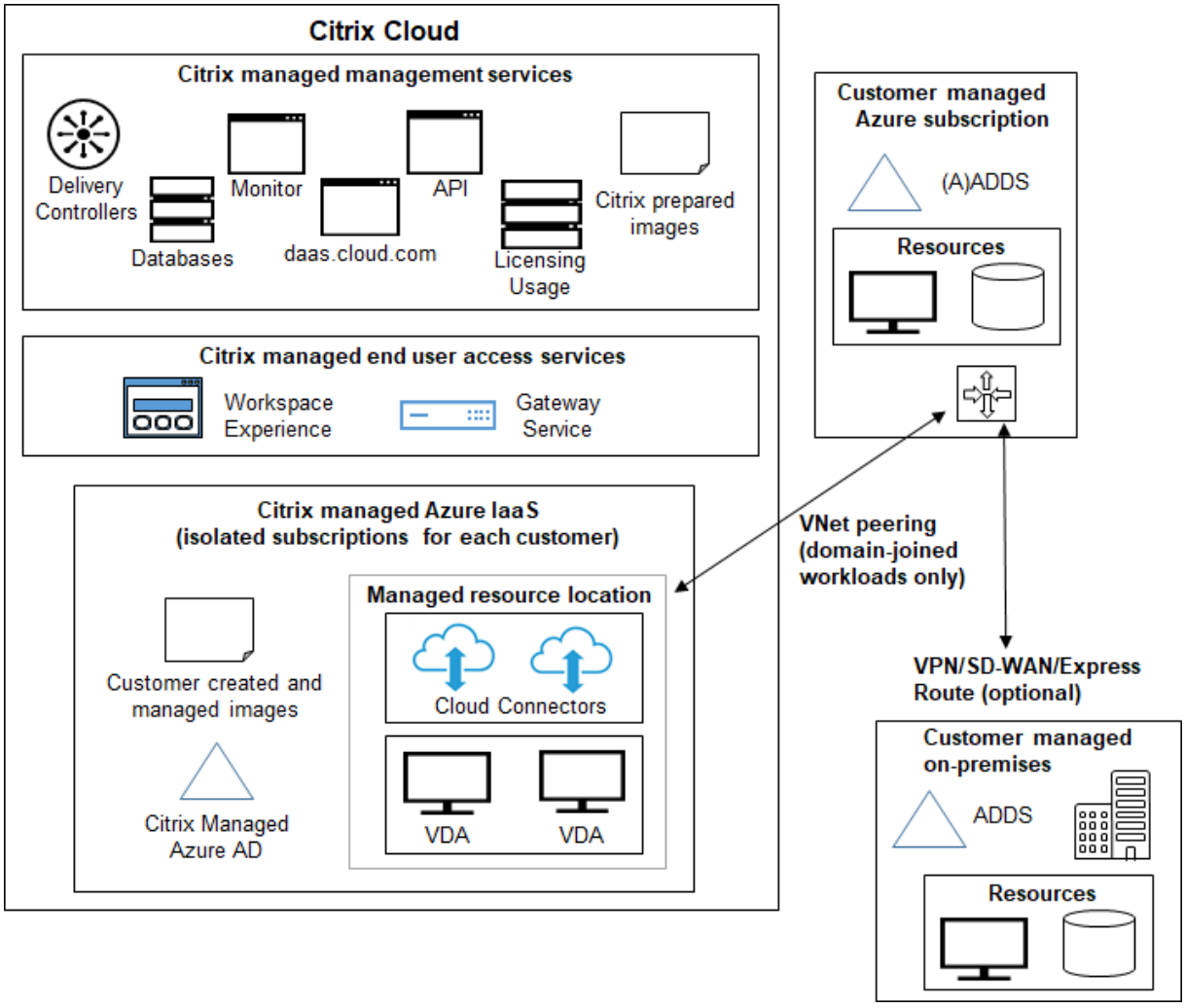
Non joint au domaine	Rejoint à un domaine
Active Directory n'est pas utilisé pour les machines. Les machines ne sont pas jointes à un domaine AD.	Active Directory est utilisé pour les machines. Les machines sont jointes à un domaine AD.
Les stratégies de groupe Active Directory ne peuvent pas être appliquées aux machines (VDA). (Vous pouvez appliquer un objet de stratégie de groupe local sur l'image utilisée pour créer un catalogue.)	Les VDA héritent des stratégies de groupe pour l'unité d'organisation AD spécifiée lors de la création du catalogue.

Non joint au domaine	Rejoint à un domaine
Les utilisateurs se connectent à l'aide de l'authentification unique.	Lorsque les utilisateurs se connectent à leur espace de travail à l'aide d'une méthode d'authentification autre qu'Active Directory, ils sont également invités à se connecter lors du lancement d'un poste de travail ou d'une application.
Vous n'avez pas besoin d'une connexion à un réseau local.	(Lors de l'utilisation d'un abonnement Citrix Managed Azure) Doit disposer d'une connexion pour accéder à un réseau local, à l'aide de Microsoft Azure VNet ou Citrix SD-WAN.
Vous devez utiliser un abonnement Citrix Managed Azure pour le provisionnement des VDA. (Impossible d'utiliser vos propres abonnements Azure pour le provisionnement de VDA. Toutefois, les utilisateurs peuvent être connectés depuis votre propre Azure AD.)	Vous pouvez utiliser un abonnement Citrix Managed Azure et vos propres abonnements Azure.
Impossible de résoudre les problèmes à l'aide d'une machine bastion ou d'un RDP direct.	Peut résoudre les problèmes à l'aide d'une machine à bastion ou d'un RDP direct.
Impossible d'utiliser Citrix Profile Management. (Recommandé : utilisez des catalogues persistants.)	Peut utiliser Citrix Profile Management ou FSLogix.

Scénarios de déploiement

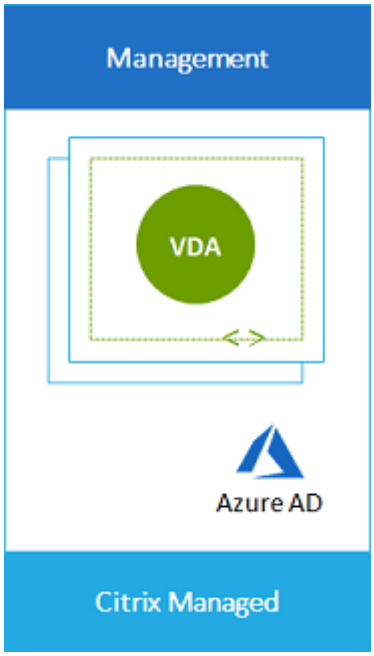
Les scénarios de déploiement pour les bureaux et les applications publiés diffèrent selon que vous utilisez un abonnement Citrix Managed Azure ou votre propre abonnement Azure géré par le client.

Déploiement dans un abonnement Citrix Managed Azure

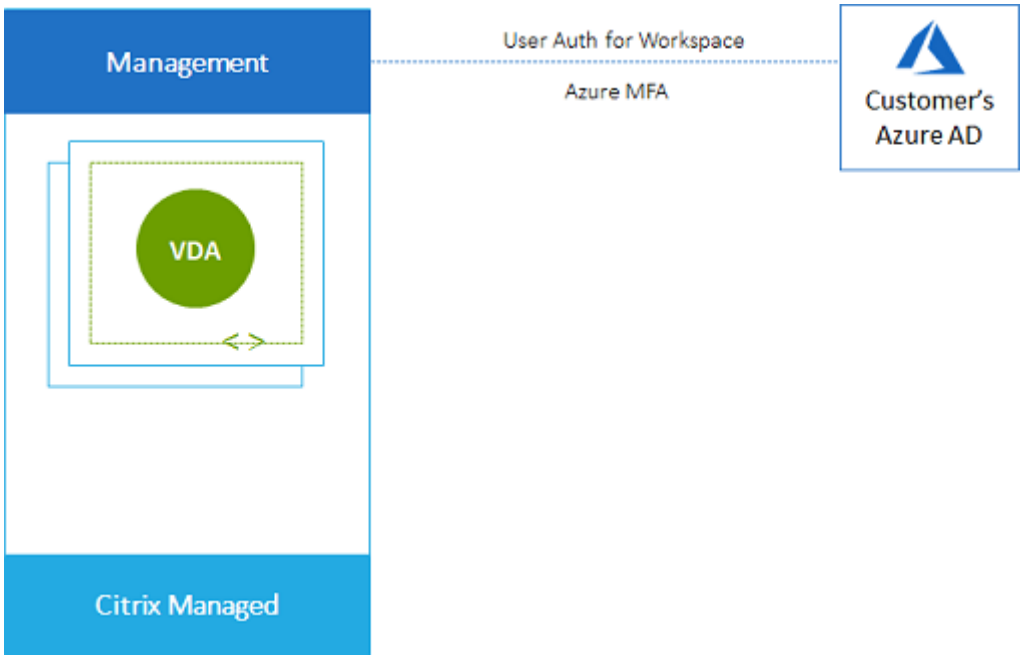


Citrix DaaS pour Azure prend en charge plusieurs scénarios de déploiement pour la connexion et l'authentification des utilisateurs.

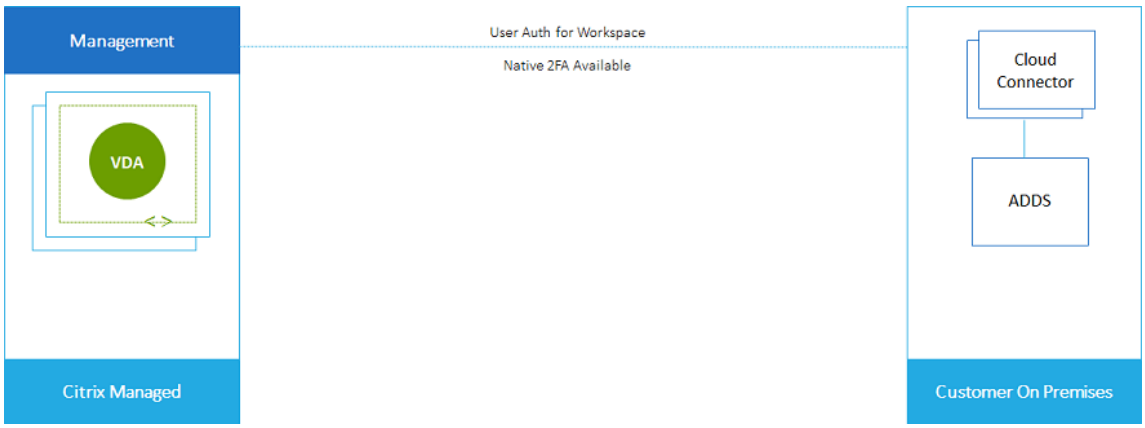
- **Azure AD géré :** il s'agit du déploiement le plus simple, avec des VDA non joints au domaine. Il est recommandé pour les preuves de concept. Vous utilisez Managed Azure AD (géré par Citrix) pour gérer les utilisateurs. Vos utilisateurs n'ont pas besoin d'accéder aux ressources de votre réseau local.



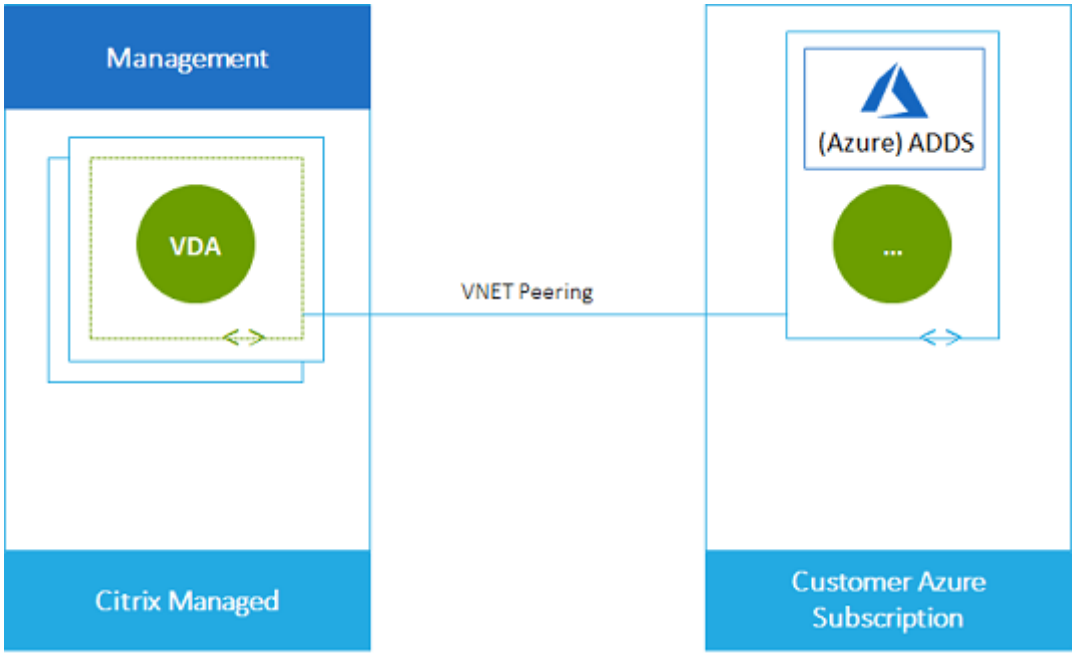
- **Azure Active Directory du client :** ce déploiement contient des VDA non joints à un domaine. Vous utilisez votre propre Active Directory ou Azure Active Directory (AAD) pour l'authentification de l'utilisateur final. Dans ce scénario, vos utilisateurs n'ont pas besoin d'accéder aux ressources de votre réseau local.



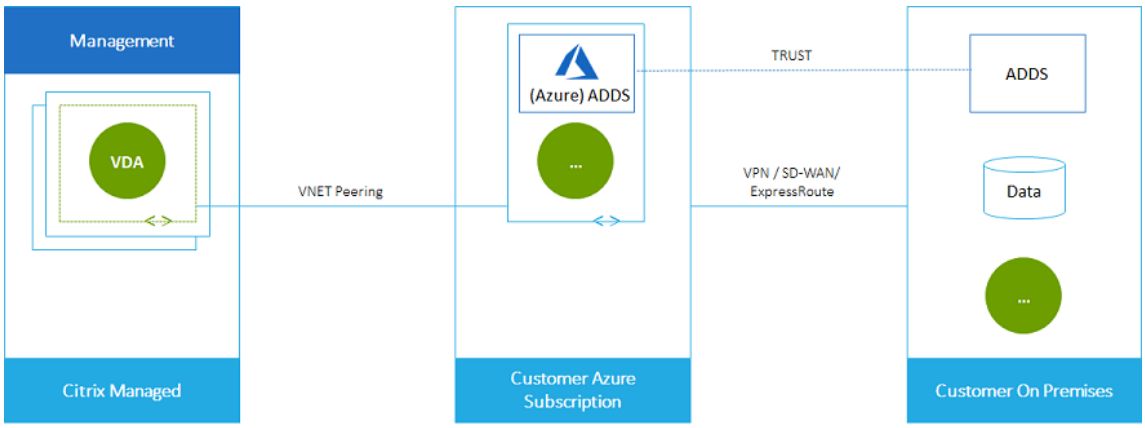
- **Azure Active Directory du client avec accès sur site :** ce déploiement contient des VDA non joints à un domaine. Vous utilisez votre propre AD ou AAD pour l'authentification de l'utilisateur final. Dans ce scénario, l'installation de Citrix Cloud Connector sur votre réseau local permet d'accéder aux ressources de ce réseau.



- **Services de domaine Azure Active Directory et appairage de réseaux virtuels du client :** si votre AD ou AAD réside dans votre propre abonnement Azure VNet et Azure, vous pouvez utiliser la fonctionnalité d'appairage de réseaux virtuels Microsoft Azure pour une connexion réseau et Azure Active Directory Domain Services (AADDS) pour l'authentification de l'utilisateur final. Les VDA sont joints à votre domaine.

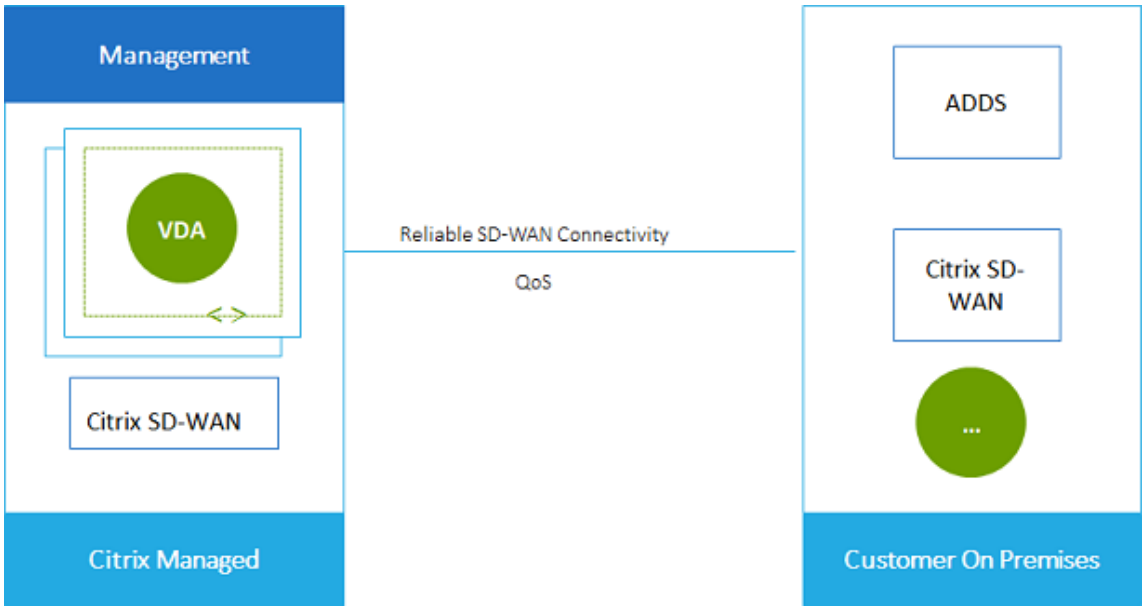


Pour permettre à vos utilisateurs d'accéder aux données stockées dans votre réseau local, vous pouvez utiliser votre connexion VPN depuis votre abonnement Azure vers l'emplacement sur site. L'appairage de réseaux virtuels Azure est utilisé pour la connectivité réseau. Les Active Directory Domain Services dans l'emplacement local sont utilisés pour l'authentification de l'utilisateur final.

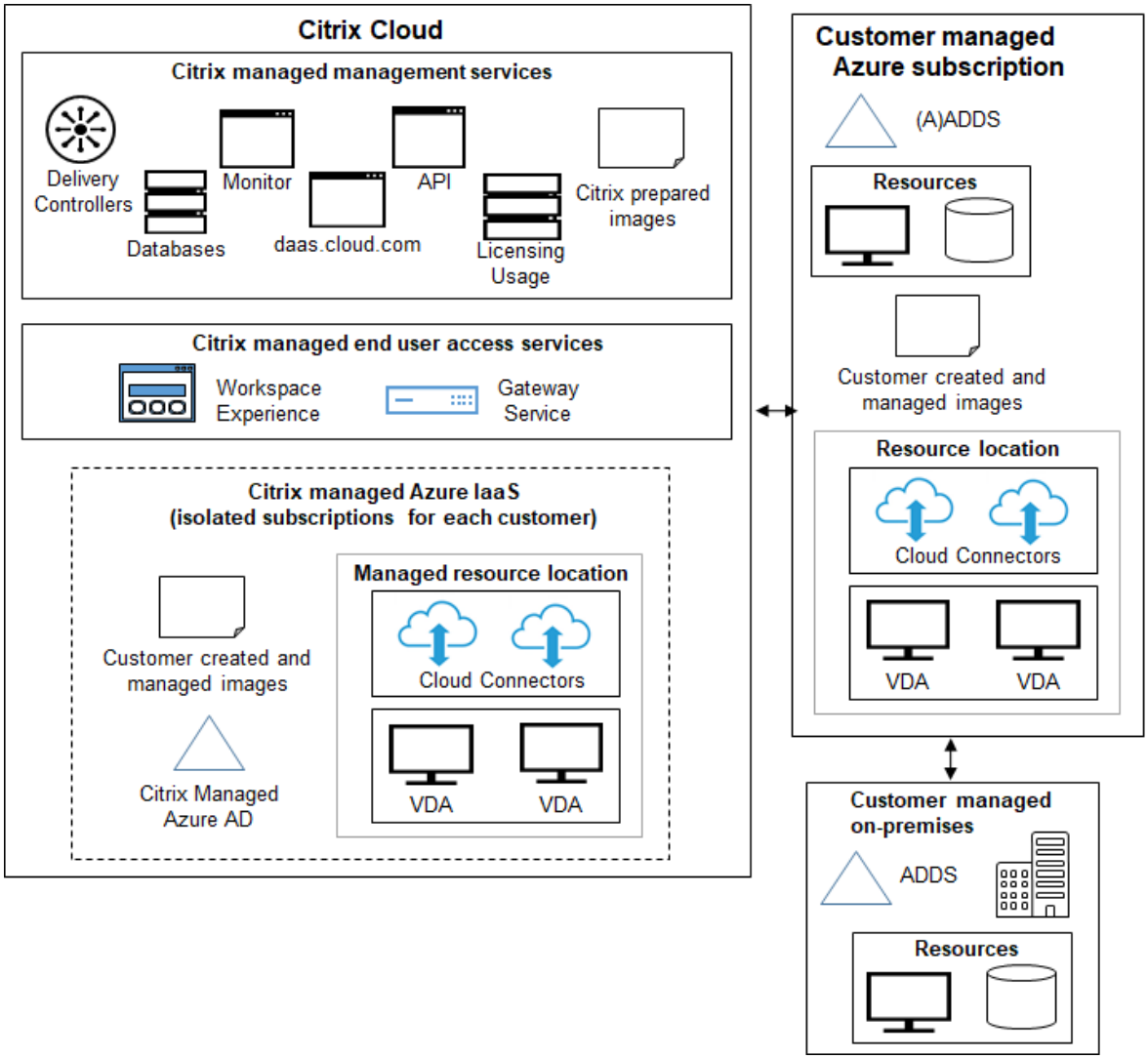


- **Active Directory et SD-WAN du client :** vous pouvez fournir aux utilisateurs un accès aux fichiers et à d'autres éléments à partir de vos réseaux SD-WAN sur site ou dans le cloud.

  Citrix SD-WAN optimise toutes les connexions réseau nécessaires à Citrix DaaS pour Azure. Travaillant de concert avec les technologies HDX, Citrix SD-WAN fournit une qualité de service et une fiabilité de connexion pour ICA et Citrix DaaS hors bande pour le trafic Azure.



Déploiement dans un abonnement Azure géré par le client



Le déploiement du graphique précédent utilise un abonnement Azure géré par le client. Toutefois, l'abonnement Citrix Managed Azure reste une option pour les autres catalogues et images, comme indiqué par le contour en pointillé.

Interfaces de gestion

Citrix DaaS pour Azure possède deux interfaces de gestion graphiques : Quick Deploy et Full Configuration.

- **Quick Deploy** vous permet de créer rapidement des catalogues et de commencer à fournir des bureaux et des applications à vos utilisateurs. (D'où le nom Quick Deploy.) Il s'agit de l'interface par défaut lorsque vous démarrez Citrix DaaS pour Azure. Vous pouvez également accéder à

cette interface en sélectionnant **Gérer > Déploiement rapide d'Azure**. Les instructions de cet ensemble de documentation produit supposent que vous utilisez Quick Deploy.

Si vous prévoyez d'utiliser un abonnement Citrix Managed Azure lors de la création d'un catalogue ou d'une image, vous devez utiliser Quick Deploy.

- **La configuration complète** offre des fonctionnalités avancées et des options de configuration pour personnaliser et gérer votre déploiement. Les catalogues que vous créez dans Quick Deploy apparaissent automatiquement dans Configuration complète. Pour passer du déploiement rapide à la configuration complète, sélectionnez **Gérer > Configuration complète**.

  Lorsque vous créez un catalogue dans Quick Deploy, un groupe de mise à disposition et une connexion hôte associés sont créés automatiquement dans Configuration complète.

  La configuration complète propose également son propre processus de création de catalogue qui inclut la création d'une connexion à l'hôte Azure, puis la création d'un catalogue et d'un groupe de mise à disposition. Ce processus n'est pris en charge que si vous utilisez votre propre abonnement Azure. Il est beaucoup plus facile de créer le catalogue dans Quick Deploy.

  La configuration complète prend en charge les processus liés à l'hyperviseur et aux hôtes de services cloud autres qu'Azure. Ils ne sont pas disponibles pour les clients Citrix DaaS pour Azure.

Gérer les catalogues créés dans l'interface Déploiement rapide

Après avoir créé un catalogue dans l'interface Déploiement rapide, vous pouvez continuer à gérer ce catalogue dans cette interface. Pour plus d'informations, consultez la section Gérer les catalogues. Vous pouvez également utiliser l'interface Configuration complète.

Lorsque vous créez un catalogue dans Déploiement rapide, ce catalogue (plus le groupe de mise à disposition et la connexion d'hébergement qui sont créés automatiquement en arrière-plan) se voient attribuer une étendue `Citrix managed object`. Les étendues sont utilisées dans l'administration déléguée pour regrouper des objets.

Les catalogues, les groupes de mise à disposition et les connexions avec l'étendue `Citrix managed object` sont interdits de certaines actions dans l'interface Configuration complète. (L'autorisation de ces actions dans Configuration complète peut nuire à la capacité du système à prendre en charge à la fois le déploiement rapide et la configuration complète, de sorte que ces actions sont désactivées.) Dans l'interface Configuration complète :

- **Catalogue :** La plupart des actions de gestion de catalogue ne sont pas disponibles. Vous ne pouvez pas supprimer un catalogue.
- **Groupe de mise à disposition :** La plupart des actions de gestion de groupe de mise à disposition sont disponibles. Vous ne pouvez pas supprimer le groupe de mise à disposition.

- **Connexion :** La plupart des actions de gestion de connexions ne sont pas disponibles. Vous ne pouvez pas supprimer une connexion. Vous ne pouvez pas créer de connexion basée sur une connexion avec l'étendue `Citrix managed object`.

Si vous créez un catalogue dans Déploiement rapide à l'aide de votre propre abonnement Azure (que vous avez ajouté à Déploiement rapide) et que vous souhaitez gérer le catalogue (ainsi que son groupe de mise à disposition et sa connexion) entièrement dans Configuration complète, vous pouvez *convertir* le catalogue.

- La conversion d'un catalogue limite sa gestion à l'interface Configuration complète uniquement. Une fois qu'un catalogue est converti, vous ne pouvez plus utiliser l'interface Déploiement rapide pour gérer ce catalogue.
- Une fois le catalogue converti, les actions qui étaient auparavant indisponibles dans Configuration complète peuvent être sélectionnées. (L'étendue `Citrix managed object` est supprimée du catalogue, du groupe de mise à disposition et de la connexion d'hébergement convertis.)
- Pour convertir un catalogue :

  Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, cliquez n'importe où dans l'entrée du catalogue. Dans l'onglet **Détails**, sous **Paramètres avancés**, sélectionnez **Convertir le catalogue**. Lorsque vous y êtes invité, confirmez la conversion.
- Vous ne pouvez pas convertir un catalogue créé dans Déploiement rapide à l'aide d'un abonnement Citrix Managed Azure.

Pour plus d'informations sur la façon de gérer les catalogues convertis en configuration complète, voir :

- Gérer les catalogues de machines (la configuration complète désigne les catalogues en tant que catalogues de machines)
- Gérer les groupes de mise à disposition

Informations supplémentaires

Pour des détails techniques, consultez :

- Architecture de référenceCitrix Tech Zone
- Fiche technique Citrix Tech Zone

Pour plus d'informations sur l'automatisation de vos déploiements, consultez l'aperçu de l'API publique des postes de travail gérés.

Une fois prêt, démarrez.

Nouveautés

December 28, 2023

L'un des objectifs de Citrix est de fournir de nouvelles fonctionnalités et des mises à jour de produits aux clients Citrix DaaS pour Azure dès qu'elles seront disponibles. Les nouvelles versions étant plus avantageuses, il est important que vous en profitiez le plus rapidement possible. Pour vous, administrateur client, ce processus est transparent.

Mises à jour d'images préparées Citrix

Les images préparées par Citrix ont un Citrix Virtual Delivery Agent (VDA) installé. En règle générale, les nouvelles versions de VDA sont publiées plusieurs fois par an et les images préparées par Citrix disponibles sont automatiquement mises à jour avec le dernier VDA. Pour en savoir plus sur les fonctionnalités nouvelles et améliorées de la version actuelle du VDA, voir :

- VDA Windows
- VDA Linux

Août 2022

- Cette fonctionnalité est globalement disponible : vous pouvez désormais créer des catalogues de machines jointes à votre Azure Active Directory. Consultez la section Création de catalogues.

Mai 2022

- Vous pouvez désormais créer des catalogues de machines associées à votre Azure Active Directory. Cette fonctionnalité est disponible dans la Tech Preview. Consultez la section Création de catalogues.
- Les fournisseurs de services Citrix peuvent désormais supprimer le service Citrix DaaS pour Azure des clients. Consultez Supprimer un service.

Avril 2022

- La création de connexion hôte pour Citrix Hypervisor, Microsoft SCVMM, VMware vSphere, Prism Central et Nutanix AHV est désormais disponible. Ainsi, vous pouvez désormais utiliser des hyperviseurs locaux en plus d'Azure.

- Le nom du produit est passé de Citrix Virtual Apps and Desktops Standard pour Azure à Citrix DaaS Standard pour Azure. Pour plus d'informations sur le changement de marque de toutes les offres Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), consultez What's New in Citrix DaaS. Apprenez-en plus sur les changements de nom lors de notre annonce sur notre blog.

Janvier 2022

- Lorsque vous créez des catalogues, vous pouvez désormais stocker vos machines sur un stockage SSD standard. Auparavant, seuls les disques standard (HDD) et les SSD haut de gamme étaient pris en charge.
- Prise en charge de ces nouvelles régions pour l'hébergement de charges de travail VDA : sud du Brésil, centre de l'Inde, Japon est, centre sud des États-Unis et sud du Royaume-Uni.
- Les instantanés et la restauration sont désormais disponibles pour les bureaux persistants hébergés sur Citrix Managed Azure et BYO Azure. Voir Instantané et restauration de VDA.
- Les adresses IP publiques statiques pour tout le trafic sortant des VDA hébergés sont désormais disponibles. Vous pouvez configurer une passerelle NAT Azure pour obtenir l'adresse IP. Consultez la section Création d'une adresse IP statique publique.
- Azure VPN est disponible en Tech Preview. Le VPN Azure vous permet de connecter Citrix Managed Azure directement aux centres de données locaux. Consultez la section Technical Preview d'Azure VPN.
- De nouvelles images Linux sont disponibles pour les images préparées par Citrix.

Novembre 2021

- Des essais de 7 jours approuvés automatiquement sont désormais disponibles (en plus des essais approuvés par les ventes).
- Les fournisseurs de services Citrix peuvent désormais gérer les utilisateurs à partir du tableau de bord **Gérer > Déploiement rapide d'Azure** du service ou de la console Citrix Cloud. Pour plus de détails, voir Accès des partenaires au fournisseur d'identité client.

Octobre 2021

- Nouvelles informations sur la gestion des catalogues créés dans Quick Deploy.

Septembre 2021

- Le contenu de preview de l'API est disponible.
- Prise en charge de Windows Server 2022 (nécessite un minimum de VDA 2106).

Juillet 2021

- L'interface de gestion de Web Studio a été renommée Configuration complète.

Juin 2021

- Prise en charge de deux interfaces de gestion : Quick Deploy et Web Studio.

May 2021

- Ce service prend en charge l'aperçu de la continuité du service.
- Lesimages préparées par Citrix incluent désormais des versions mono-session et multi-session Ubuntu.
- Lorsque vous ajoutez un Cloud Connector à un emplacement de ressources, à l'aide d'un abonnement Citrix Managed Azure, vous pouvez spécifier le type de performance de la machine Cloud Connector.
- Lors de la création d'un catalogue, les choix de performances de la machine incluent des options qui correspondent au type de génération (gen1 ou gen2) de l'image que vous avez sélectionnée. Vous pouvez mettre à jour un catalogue avec une image de type de génération différent, si les machines du catalogue prennent en charge ce type de génération.

Avril 2022

- Le nom du produit est passé de Citrix Virtual Apps and Desktops Standard pour Azure à Citrix DaaS Standard pour Azure.

Janvier 2021

- Prise en charge de l'aperçu pour afficher l'utilisation des engagementsde

Octobre 2020

- Vous pouvez utiliser la fonction Surveiller l'ombre pour afficher ou travailler sur la machine virtuelle ou la session d'un utilisateur.
- Prise en charge de la production pour Remote PC Access.
- Option de création de catalogue améliorée pour utiliser votre licence éligible Azure Virtual Desktop ou Azure Hybrid Benefit.
- Si une action de redémarrage sur une machine échoue, vous pouvez utiliser une action de redémarrage forcé.

Septembre 2020

- Les détails concernant les images sont réorganisés et développés. Par exemple, vous pouvez désormais ajouter et modifier des notes concernant les images que vous avez préparées ou importées. Vous pouvez également limiter l'accès aux seules adresses IP spécifiées.
- Lors de la création d'une connexion d'appairage de réseau virtuel Azure qui utilisera une passerelle réseau virtuelle Azure, vous pouvez désormais également activer la propagation de l'itinéraire de la passerelle réseau virtuelle.
- Le nom du produit passe de Citrix Managed Desktops à Citrix Virtual Apps and Desktops Standard pour Azure.

Août 2020

- Prise en charge de l'aperçu pour Remote PC Access.
- Une image Windows Server 2019 préparée par Citrix est désormais disponible.

Juillet 2020

- Lorsque vous ajoutez un Cloud Connector à un emplacement de ressources, à l'aide d'un abonnement Azure géré par le client, vous pouvez spécifier le type de performance et le groupe de ressources Azure de la machine Cloud Connector. Pour plus de détails, voir Actions d'emplacement des ressources.
- Lors de la création d'un catalogue, vous pouvez spécifier un schéma de dénomination de machine. Voir Créer un catalogue à l'aide de la création personnalisée.

Juin 2020

- Dans un environnement CSP, les connexions SD-WAN sont créées par locataire. Pour que l'option de connexion SD-WAN soit disponible pour l'administrateur CSP, le locataire doit disposer

d'un droit de service SD-WAN Orchestrator. Pour plus de détails, voir Filtrer les ressources par client (déploiements multilocataires).
- Support de production pour les VDA Linux lors de l'utilisation d'un abonnement Azure géré par le client.
- La limite de VDA par abonnement est désormais de 1 200.

Mai 2020

- Vous pouvez ajouter un autre abonnement Citrix Managed Azure lorsque vous avez besoin de plus de machines que la limite par abonnement Citrix Managed Azure.
- Informations supplémentaires sur les serveurs DNS.

Mars 2020

- Prise en charge de la production pour les connexions SD-WAN.

Février 2020

- Pour afficher les informations d'utilisation de vos licences Citrix, suivez les instructions de la section Surveillance des licences et de l'utilisation pour Citrix DaaS Standard pour Azure.
- Prise en charge de l'aperçu pour les catalogues contenant des machines Red Hat Enterprise Linux ou Ubuntu. Cette fonctionnalité n'est valide que lors de l'utilisation d'un abonnement Azure géré par le client et nécessite une image importée contenant un VDA Citrix Linux.
- Vous pouvez désormais configurer l'équilibrage de charge vertical ou horizontal pour toutes vos machines multi-sessions. (Auparavant, toutes les machines utilisaient un équilibrage de charge horizontal.) Cette sélection globale s'applique à tous les catalogues de votre déploiement. Voir Équilibrage de charge.
- Vous pouvez désormais ajouter un abonnement Azure si vous n'êtes pas un administrateur global.
- Une image préparée par Citrix est désormais disponible pour Windows 10 Enterprise Virtual Desktop (multi-session) avec Office 365 ProPlus.

Janvier 2020

- Ajout de la prise en charge des itinéraires personnalisés dans les connexions de peering de réseau virtuel.
- Mises à jour de l'article sur la sécurité pour améliorer les informations sur les ports et

Novembre 2019

- Prise en charge de l'aperçu pour les connexions SD-WAN.

Octobre 2019

- Dans Systèmes d'exploitation pris en charge, ajout d'entrées pour :
  - Windows 7 (prend uniquement en charge le VDA 7.15 avec la dernière mise à jour cumulative).
  - Windows Server 2019.
- Une image préparée pour Windows Server 2012 R2 Citrix est désormais disponible.
- Ajout d'informations sur les paramètres d'emplacement des ressources Pour plus de détails, voir Actions d'emplacement des ressources et Paramètres d'emplacement des ressources lors de la création d'un catalogue.

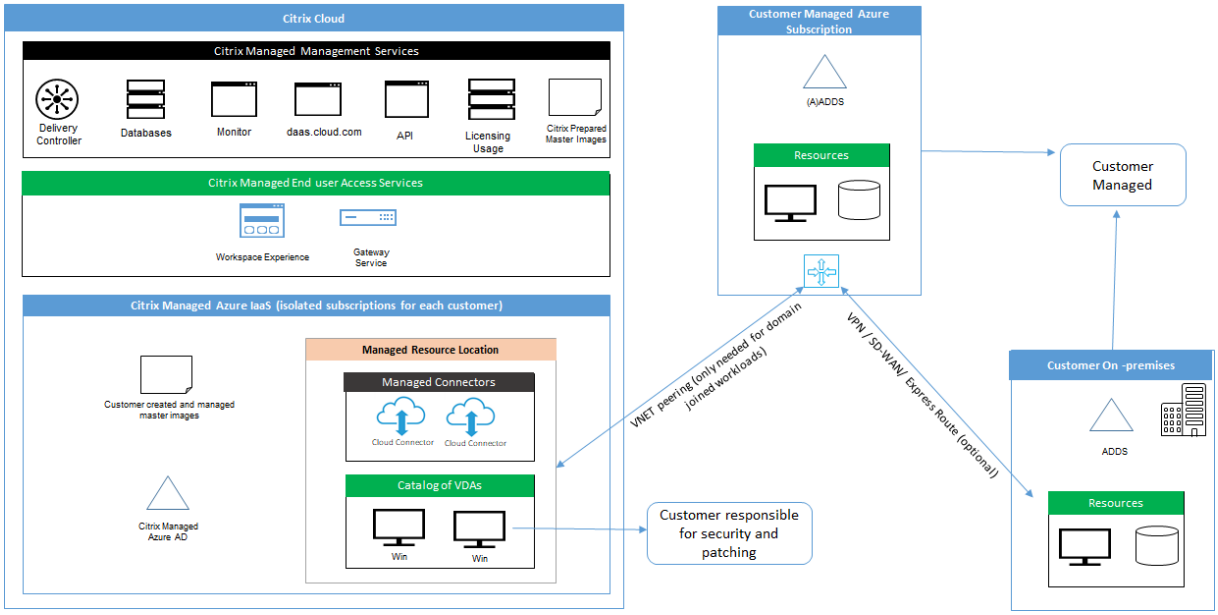
Septembre 2019

- Par défaut, les machines sont créées dans un abonnement Citrix Managed Azure. Vous pouvez désormais également créer des catalogues et des images dans votre propre abonnement Azure géré par le client.

Vue d'ensemble de la sécurité technique

May 16, 2022

Le diagramme suivant montre les composants d'un déploiement Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure). Cet exemple utilise une connexion d'appairage de réseaux virtuels.



Avec Citrix DaaS pour Azure, les Virtual Delivery Agents (VDA) du client qui fournissent des postes de travail et des applications, ainsi que des Citrix Cloud Connector, sont déployés dans un abonnement Azure et un locataire gérés par Citrix.

> **REMARQUE :**
>
> Cet article fournit une vue d'ensemble des exigences de sécurité pour les clients qui déploient Citrix DaaS pour Azure à l'aide d'un abonnement Azure géré par Citrix. Pour obtenir une présentation architecturale d'un déploiement de Citrix DaaS pour Azure à l'aide d'un abonnement Azure géré par le client, y compris des informations de sécurité, voir Architecture de référence : Virtual Apps and Desktops Service - Azure.

Conformité cloud de Citrix

L'utilisation de Citrix Managed Azure Capacity avec diverses éditions de Citrix DaaS et Workspace Premium Plus n'a pas été évaluée pour Citrix SOC 2 (Type 1 ou 2), ISO 27001, HIPAA ou d'autres exigences de conformité cloud. (Janvier 2021). Visitez le Citrix Trust Center pour en savoir plus sur les certifications Citrix Cloud et consultez-le fréquemment pour obtenir les informations les plus récentes.

Responsabilité de Citrix

Citrix Cloud Connector pour catalogues non joints à un domaine

Citrix DaaS pour Azure déploie au moins deux Cloud Connector dans chaque emplacement de ressources. Certains catalogues peuvent partager un emplacement de ressources s'ils se trouvent dans la même région que d'autres catalogues pour le même client.

Citrix est responsable des opérations de sécurité suivantes sur les Cloud Connector de catalogues non joints à un domaine :

- Installation des mises à jour du système d'exploitation et des correctifs
- Installation et maintenance d'un logiciel antivirus
- Installation des mises à jour logicielles des Cloud Connector

Les clients n'ont pas accès aux Cloud Connector. Citrix est donc entièrement responsable des performances des Cloud Connector de catalogues qui ne sont pas joints à un domaine.

Abonnement Azure et Azure Active Directory

Citrix est responsable de la sécurité de l'abonnement Azure et d'Azure Active Directory (AAD) créés pour le client. Citrix garantit l'isolation des locataires, de sorte que chaque client dispose de son propre abonnement Azure et AAD, et les échanges croisés entre différents locataires sont évités. Citrix restreint également l'accès à l'AAD au personnel d'exploitation Citrix DaaS pour Azure et Citrix uniquement. L'accès de Citrix à l'abonnement Azure de chaque client est vérifié.

Les clients utilisant des catalogues non joints à un domaine peuvent utiliser AAD géré par Citrix comme moyen d'authentification pour Citrix Workspace. Pour ces clients, Citrix crée des comptes utilisateurs à privilèges limités dans AAD géré par Citrix. Toutefois, ni les utilisateurs ni les administrateurs des clients ne peuvent exécuter d'actions sur AAD géré par Citrix. Si ces clients choisissent plutôt d'utiliser leur propre AAD, ils sont entièrement responsables de sa sécurité.

Infrastructure et réseaux virtuels

Au sein de l'abonnement Azure géré par Citrix du client, Citrix crée des réseaux virtuels pour isoler les emplacements de ressources. Au sein de ces réseaux, Citrix crée des machines virtuelles pour les VDA, les Cloud Connector et les machines de création d'images, en plus des comptes de stockage, des coffres de clés et d'autres ressources Azure. Citrix, en partenariat avec Microsoft, est responsable de la sécurité des réseaux virtuels, y compris des pare-feu de réseau virtuel.

Citrix garantit que la stratégie de pare-feu Azure par défaut (groupes de sécurité réseau) est configurée de façon à limiter l'accès aux interfaces réseau dans l'appairage de réseau virtuel et les connexions SD-WAN. En règle générale, cela contrôle le trafic entrant vers les VDA et Cloud Connector. Pour plus de détails, consultez :

- Stratégie de pare-feu pour les connexions d'appairage de réseaux virtuels Azure
- Stratégie de pare-feu pour les connexions SD-WAN

Les clients ne peuvent pas modifier cette stratégie de pare-feu par défaut, mais ils peuvent déployer des règles de pare-feu supplémentaires sur des machines VDA créées par Citrix. Par exemple, pour

limiter partiellement le trafic sortant. Les clients qui installent des clients de réseau privé virtuel, ou d'autres logiciels capables de contourner les règles de pare-feu, sur des machines VDA créées par Citrix sont responsables de tous les risques de sécurité pouvant en découler.

Lorsque vous utilisez le générateur d'image dans Citrix DaaS pour Azure pour créer et personnaliser une nouvelle image de machine, les ports 3389-3390 sont ouverts temporairement dans le réseau virtuel géré par Citrix, afin que le client puisse accéder au protocole RDP sur la machine contenant la nouvelle image de machine, afin de la personnaliser.

Responsabilité de Citrix lors de l'utilisation de connexions d'appairage de réseaux virtuels Azure

Pour que les VDA dans Citrix DaaS pour Azure puissent contacter des contrôleurs de domaine locaux, des partages de fichiers ou d'autres ressources intranet, Citrix DaaS pour Azure fournit un workflow d'appairage de réseau virtuel comme option de connectivité. Le réseau virtuel géré par Citrix du client est associé à un réseau virtuel Azure géré par le client. Le réseau virtuel géré par le client peut activer la connectivité avec les ressources sur site du client à l'aide de la solution de connectivité cloud vers site choisie par le client, telle que les tunnels Azure ExpressRoute ou IPSec.

La responsabilité de Citrix pour l'appairage de réseaux virtuels se limite à la prise en charge du flux de travail et de la configuration des ressources Azure associée pour établir une relation d'appairage entre Citrix et les réseaux virtuels gérés par le client.

Stratégie de pare-feu pour les connexions d'appairage de réseaux virtuels Azure Citrix ouvre ou ferme les ports suivants pour le trafic entrant et sortant qui utilise une connexion d'appairage de réseaux virtuels.

Réseau virtuel géré par Citrix avec des machines non jointes à un domaine

- Règles du trafic entrant
  - Autorisez les ports 80, 443, 1494 et 2598 entrants des VDA vers les Cloud Connector et des Cloud Connector vers les VDA.
  - Autorisez les ports 49152-65535 entrants vers les VDA à partir d'une plage IP utilisée par la fonction d'observation de Gérer. Consultez Ports de communication utilisés par les technologies Citrix.
  - Refusez tout autre trafic entrant. Cela inclut le trafic intra-réseau virtuel depuis VDA vers VDA et VDA vers Cloud Connector.
- Règles du trafic sortant
  - Autorisez tout le trafic sortant.

Réseau virtuel géré par Citrix avec des machines jointes à un domaine

- Règles du trafic entrant
  - Autorisez les ports 80, 443, 1494 et 2598 entrants des VDA vers les Cloud Connector et des Cloud Connector vers les VDA.
  - Autorisez les ports 49152-65535 entrants vers les VDA à partir d'une plage IP utilisée par la fonction d'observation de Gérer. Consultez Ports de communication utilisés par les technologies Citrix.
  - Refusez tout autre trafic entrant. Cela inclut le trafic intra-réseau virtuel depuis VDA vers VDA et VDA vers Cloud Connector.
- Règles du trafic sortant
  - Autorisez tout le trafic sortant.

Réseau virtuel géré par le client avec des machines jointes à un domaine

- Il appartient au client de configurer correctement son réseau virtuel. Cela inclut l'ouverture des ports suivants pour rejoindre un domaine.
- Règles du trafic entrant
  - Autorisez le trafic entrant sur 443, 1494 et 2598 à partir des adresses IP clientes pour les lancements internes.
  - Autorisez le trafic entrant sur 53, 88, 123, 135-139, 389, 445, 636 à partir de réseau virtuel Citrix (plage IP spécifiée par le client).
  - Autorisez le trafic entrant sur les ports ouverts avec une configuration proxy.
  - Autres règles créées par le client.
- Règles du trafic sortant
  - Autorisez le trafic entrant sur 443, 1494 et 2598 vers un réseau virtuel Citrix (plage IP spécifiée par le client) pour les lancements internes.
  - Autres règles créées par le client.

Responsabilité Citrix lors de l'utilisation de la connectivité SD-WAN

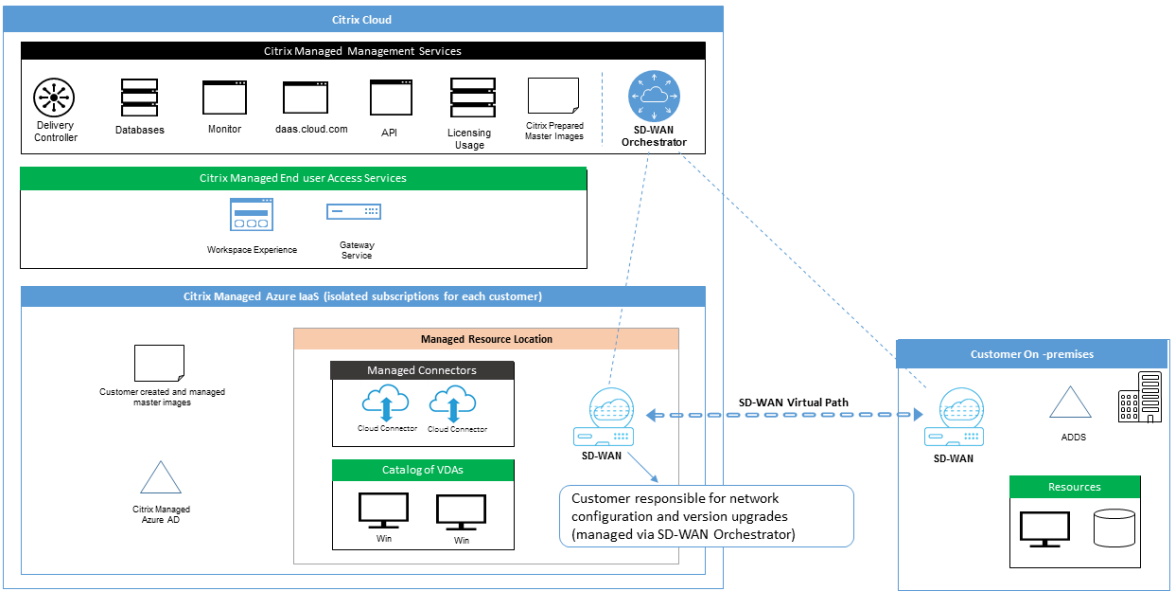
Citrix prend en charge une méthode entièrement automatisée de déploiement d'instances virtuelles Citrix SD-WAN afin d'activer la connectivité entre Citrix DaaS pour Azure et les ressources locales. La connectivité Citrix SD-WAN présente de nombreux avantages par rapport à l'appairage de réseaux virtuels, notamment :

Fiabilité et sécurité élevées des connexions VDA vers centre de données et VDA vers branche (ICA).

- Meilleure expérience utilisateur final pour les employés de bureau, avec des capacités QoS avancées et des optimisations VoIP.
- Possibilité intégrée d'inspecter, de hiérarchiser et de générer des rapports sur le trafic réseau Citrix HDX et l'utilisation d'autres applications.

Citrix demande aux clients qui souhaitent tirer parti de la connectivité SD-WAN pour Citrix DaaS pour Azure d'utiliser SD-WAN Orchestrator pour gérer leurs réseaux Citrix SD-WAN.

Le diagramme suivant montre les composants ajoutés dans un déploiement Citrix DaaS pour Azure à l'aide de la connectivité SD-WAN.



Le déploiement Citrix SD-WAN pour Citrix DaaS pour Azure est similaire à la configuration de déploiement Azure standard pour Citrix SD-WAN. Pour plus d'informations, consultez Déployer une instance Citrix SD-WAN Standard Edition sur Azure. Dans une configuration haute disponibilité, une paire d'instances SD-WAN active/en veille avec des équilibreurs de charge Azure est déployée en tant que passerelle entre le sous-réseau contenant des VDA et des Cloud Connector, et Internet. Dans une configuration sans haute disponibilité, seule une seule instance SD-WAN est déployée en tant que passerelle. Les interfaces réseau des appliances SD-WAN virtuelles se voient attribuer des adresses provenant d'une petite plage d'adresses distincte divisée en deux sous-réseaux.

Lors de la configuration de la connectivité SD-WAN, Citrix apporte quelques modifications à la configuration réseau des bureaux gérés décrite ci-dessus. En particulier, tout le trafic sortant du réseau virtuel, y compris le trafic vers des destinations Internet, est acheminé via l'instance Cloud SD-WAN. L'instance SD-WAN est également configurée pour être le serveur DNS du réseau virtuel géré par Citrix.

L'accès de gestion aux instances SD-WAN virtuelles nécessite un identifiant et un mot de passe admin-

istrateur. Chaque instance SD-WAN se voit attribuer un mot de passe sécurisé unique et aléatoire qui peut être utilisé par les administrateurs SD-WAN pour la connexion et le dépannage à distance via l'interface utilisateur SD-WAN Orchestrator, l'interface utilisateur de gestion des appliances virtuelles et l'interface de ligne de commande.

Tout comme les autres ressources spécifiques au locataire, les instances SD-WAN virtuelles déployées dans un réseau virtuel client spécifique sont complètement isolées de tous les autres réseaux virtuels.

Lorsque le client active la connectivité Citrix SD-WAN, Citrix automatise le déploiement initial des instances SD-WAN virtuelles utilisées avec Citrix DaaS pour Azure, conserve les ressources Azure sous-jacentes (machines virtuelles, équilibreurs de charge, etc.), fournit des valeurs par défaut prêtes à l'emploi sécurisées et efficaces pour le configuration d'instances virtuelles SD-WAN et permet une maintenance et un dépannage continus via SD-WAN Orchestrator. Citrix prend également des mesures raisonnables pour effectuer une validation automatique de la configuration réseau SD-WAN, vérifier les risques de sécurité connus et afficher les alertes correspondantes via SD-WAN Orchestrator.

Stratégie de pare-feu pour les connexions SD-WAN Citrix utilise des stratégies de pare-feu Azure (groupes de sécurité réseau) et l'attribution d'adresses IP publiques pour limiter l'accès aux interfaces réseau des appliances SD-WAN virtuelles :

- Seules les interfaces WAN et de gestion se voient attribuer des adresses IP publiques et permettent la connectivité sortante à Internet.
- Les interfaces LAN, agissant comme passerelles pour le réseau virtuel géré par Citrix, sont uniquement autorisées à échanger du trafic réseau avec des machines virtuelles sur le même réseau virtuel.
- Les interfaces WAN limitent le trafic entrant au port UDP 4980 (utilisé par Citrix SD-WAN pour la connectivité des chemins virtuels) et refusent le trafic sortant vers le réseau virtuel.
- Les ports de gestion autorisent le trafic entrant vers les ports 443 (HTTPS) et 22 (SSH).
- Les interfaces haute disponibilité ne sont autorisées qu'à échanger le trafic de contrôle entre elles.

Accès à l'infrastructure

Citrix peut accéder à l'infrastructure gérée par Citrix (Cloud Connector) du client pour effectuer certaines tâches administratives telles que la collecte des journaux (y compris l'Observateur d'événements Windows) et le redémarrage des services sans en avertir le client. Citrix est responsable de l'exécution de ces tâches en toute sécurité, avec un impact minimal sur le client. Citrix est également responsable de s'assurer que tous les fichiers journaux sont récupérés, transportés et traités en toute sécurité. Les VDA clients ne sont pas accessibles de cette façon.

Sauvegardes pour catalogues non joints à un domaine

Citrix n'est pas responsable des sauvegardes de catalogues non joints à un domaine.

Sauvegardes d'images de machine

Citrix est responsable de la sauvegarde de toutes les images de machines téléchargées sur Citrix DaaS pour Azure, y compris les images créées avec le générateur d'images. Citrix utilise un stockage redondant localement pour ces images.

Bastions pour catalogues non joints à un domaine

Le personnel des opérations Citrix a la capacité de créer un bastion, si nécessaire, pour accéder à l'abonnement Azure géré par Citrix du client pour diagnostiquer et réparer les problèmes des clients, potentiellement avant que le client ne soit conscient d'un problème. Citrix n'a pas besoin du consentement du client pour créer un bastion. Lorsque Citrix crée le bastion, Citrix crée un mot de passe fort généré aléatoirement pour le bastion et restreint l'accès RDP aux adresses IP NAT Citrix. Lorsque le bastion n'est plus nécessaire, Citrix le retire et le mot de passe n'est plus valide. Le bastion (et les règles d'accès RDP qui l'accompagnent) est retiré lorsque l'opération est terminée. Citrix peut accéder uniquement aux Cloud Connector non joints à un domaine du client avec le bastion. Citrix ne dispose pas du mot de passe nécessaire pour se connecter à des VDA non joints à un domaine ou à des Cloud Connector et VDA appartenant à un domaine.

Stratégie de pare-feu lors de l'utilisation d'outils de dépannage

Lorsqu'un client demande la création d'une machine bastion à des fins de dépannage, les modifications suivantes du groupe de sécurité sont apportées au réseau virtuel géré par Citrix :

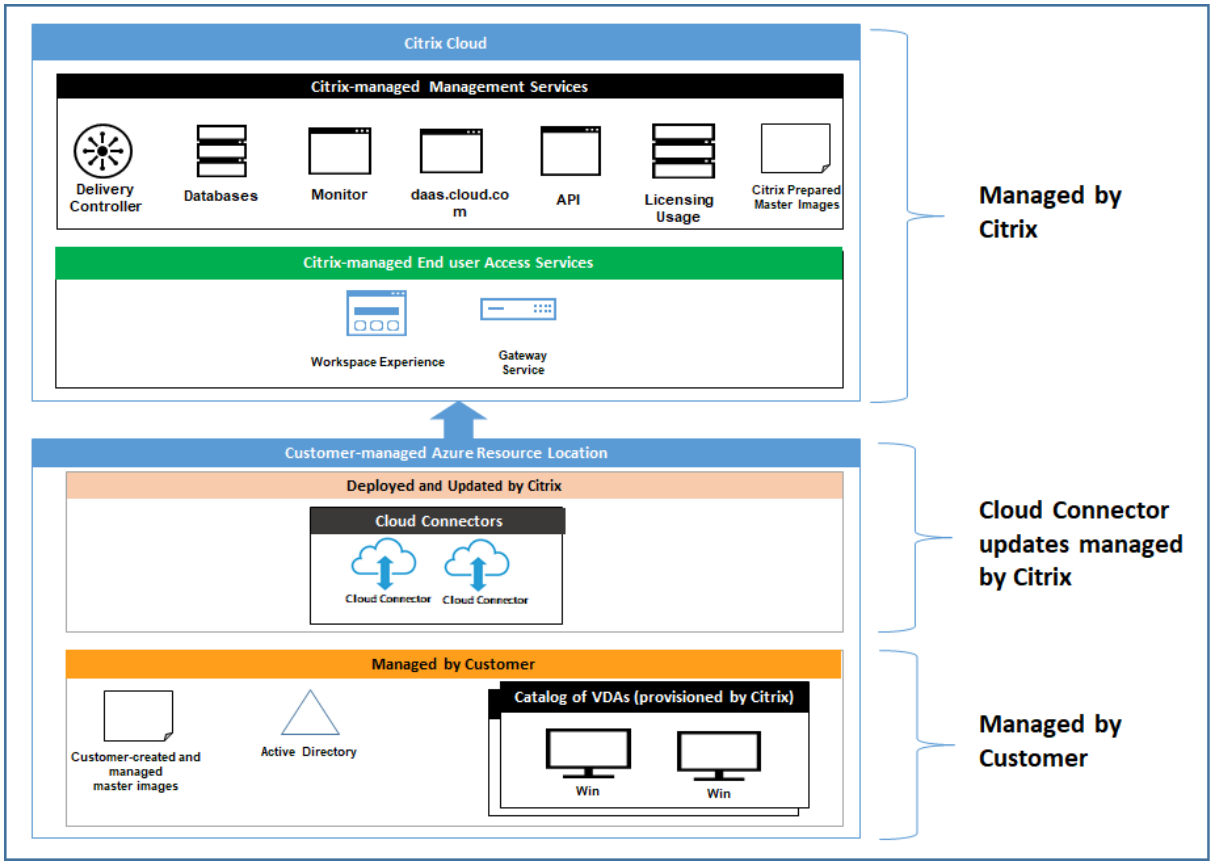
- Autorisez temporairement le trafic entrant 3389 de la plage IP spécifiée par le client vers le bastion.
- Autorisez temporairement le trafic entrant 3389 depuis l'adresse IP du bastion vers n'importe quelle adresse du réseau virtuel (VDA et Cloud Connector).
- Continuez à bloquer l'accès RDP entre les Cloud Connector, les VDA et les autres VDA.

Lorsqu'un client autorise l'accès RDP à des fins de dépannage, les modifications suivantes du groupe de sécurité sont apportées au réseau virtuel géré par Citrix :

- Autorisez temporairement le trafic entrant 3389 depuis la plage IP spécifiée par le client vers n'importe quelle adresse du réseau virtuel (VDA et Cloud Connector).
- Continuez à bloquer l'accès RDP entre les Cloud Connector, les VDA et les autres VDA.

Abonnements gérés par le client

Pour les abonnements gérés par le client, Citrix adhère aux responsabilités ci-dessus lors du déploiement des ressources Azure. Après le déploiement, tout ce qui précède relève de la responsabilité du client, car le client est propriétaire de l'abonnement Azure.



Responsabilité du client

VDA et images de machine

Le client est responsable de tous les aspects du logiciel installé sur les machines VDA, y compris :

- mises à jour du système d'exploitation et correctifs de sécurité
- antivirus et antimalware
- mises à jour logicielles VDA et correctifs de sécurité
- règles de pare-feu logiciel supplémentaires (en particulier le trafic sortant)
- suivre les considérations de sécurité et les meilleures pratiques Citrix

Citrix fournit une image préparée destinée à servir de point de départ. Les clients peuvent utiliser cette image à des fins de preuve de concept ou de démonstration ou comme base pour créer leur

propre image de machine. Citrix ne garantit pas la sécurité de cette image préparée. Citrix tentera de maintenir à jour le système d'exploitation et le logiciel VDA de l'image préparée et activera Windows Defender sur ces images.

Responsabilité du client lors de l'utilisation de l'appairage de réseaux virtuels

Le client doit ouvrir tous les ports spécifiés dans Réseau virtuel géré par le client avec des machines jointes à un domaine.

Lorsque l'appairage de réseaux virtuels est configuré, le client est responsable de la sécurité de son propre réseau virtuel et de sa connectivité à ses ressources locales. Le client est également responsable de la sécurité du trafic entrant provenant du réseau virtuel appairé géré par Citrix. Citrix ne prend aucune mesure pour bloquer le trafic entre le réseau virtuel géré par Citrix et les ressources locales du client.

Les clients disposent des options suivantes pour limiter le trafic entrant :

- Donnez au réseau virtuel géré par Citrix un bloc IP qui n'est pas utilisé ailleurs dans le réseau local du client ou dans le réseau virtuel connecté géré par le client. Ceci est nécessaire pour l'appairage de réseaux virtuels.
- Ajoutez des groupes de sécurité réseau Azure et des pare-feu au réseau virtuel du client et au réseau local pour bloquer ou restreindre le trafic provenant du bloc IP géré par Citrix.
- Déployez des mesures telles que des systèmes de prévention des intrusions, des pare-feu logiciels et des moteurs d'analyse comportementale dans le réseau virtuel du client et le réseau local, avec le bloc IP géré par Citrix comme cible.

Responsabilité du client lors de l'utilisation de la connectivité SD-WAN

Lorsque la connectivité SD-WAN est configurée, les clients disposent d'une flexibilité totale pour configurer les instances SD-WAN virtuelles utilisées avec Citrix DaaS pour Azure en fonction de leurs exigences réseau, à l'exception de quelques éléments requis pour garantir le bon fonctionnement du SD-WAN dans le réseau virtuel géré par Citrix. Responsabilités du client :

- Conception et configuration de règles de routage et de pare-feu, y compris les règles relatives à la rupture du trafic DNS et Internet
- Maintenance de la configuration réseau SD-WAN
- Surveillance de l'état opérationnel du réseau
- Déploiement rapide des mises à jour logicielles Citrix SD-WAN ou des correctifs de sécurité Étant donné que toutes les instances de Citrix SD-WAN sur un réseau client doivent exécuter la même version du logiciel SD-WAN, les déploiements de versions logicielles mises à jour vers les instances Citrix DaaS pour Azure SD-WAN doivent être gérés par les clients en fonction de leurs calendriers de maintenance réseau et de leurs contraintes.

Une configuration incorrecte des règles de routage et de pare-feu SD-WAN, ou une mauvaise gestion des mots de passe de gestion SD-WAN, peut entraîner des risques de sécurité à la fois pour les ressources virtuelles dans Citrix DaaS pour Azure et pour les ressources locales accessibles via les chemins virtuels Citrix SD-WAN. Un autre risque de sécurité possible provient de la non-mise à jour du logiciel Citrix SD-WAN vers la dernière version du correctif disponible. Bien que SD-WAN Orchestrator et d'autres services Citrix Cloud fournissent les moyens de faire face à ces risques, il incombe aux clients de s'assurer que les instances SD-WAN virtuelles sont configurées de manière appropriée.

Proxy

Le client peut choisir d'utiliser un proxy pour le trafic sortant du VDA. Si un proxy est utilisé, le client a les responsabilités suivantes :

- Configuration des paramètres proxy sur l'image de machine VDA ou, si le VDA est joint à un domaine, utilisation de la stratégie de groupe Active Directory
- Maintenance et sécurité du proxy

Les proxy ne peuvent pas être utilisés avec Citrix Cloud Connector ou une autre infrastructure gérée par Citrix.

Résilience du catalogue

Citrix fournit trois types de catalogues avec différents niveaux de résilience :

- **Statique :** chaque utilisateur est affecté à un seul VDA. Ce type de catalogue n'offre pas de haute disponibilité. Si le VDA d'un utilisateur tombe en panne, il devra être placé sur un nouveau VDA. Azure fournit un contrat de niveau de service de 99,5 % pour les machines virtuelles à instance unique. Le client peut toujours sauvegarder le profil utilisateur, mais toutes les personnalisations effectuées sur le VDA (telles que l'installation de programmes ou la configuration de Windows) seront perdues.
- **Aléatoire :** chaque utilisateur est affecté aléatoirement à un VDA serveur au moment du lancement. Ce type de catalogue offre une haute disponibilité via la redondance. Si un VDA tombe en panne, aucune information n'est perdue car le profil de l'utilisateur se trouve ailleurs.
- **Multisession Windows 10 :** ce type de catalogue fonctionne de la même manière que le type aléatoire, mais utilise des VDA de station de travail Windows 10 au lieu de VDA de serveur.

Sauvegardes pour catalogues joints à un domaine

Si le client utilise des catalogues joints à un domaine avec un appairage de réseaux virtuels, il est responsable de la sauvegarde de ses profils utilisateur. Citrix recommande aux clients de configurer

des partages de fichiers locaux et de définir des stratégies sur leur Active Directory ou leurs VDA pour extraire les profils utilisateur de ces partages de fichiers. Le client est responsable de la sauvegarde et de la disponibilité de ces partages de fichiers.

Récupération d'urgence

En cas de perte de données Azure, Citrix récupérera autant de ressources que possible dans l'abonnement Azure géré par Citrix. Citrix tentera de récupérer les Cloud Connector et les VDA. Si Citrix ne réussit pas à récupérer ces éléments, les clients sont responsables de la création d'un nouveau catalogue. Citrix suppose que les images machine sont sauvegardées et que les clients ont sauvegardé leurs profils utilisateur, ce qui permet de reconstruire le catalogue.

En cas de perte d'une région Azure complète, le client est responsable de la reconstruction de son réseau virtuel géré par le client dans une nouvelle région et de la création d'un nouvel appairage de réseau virtuel ou d'une nouvelle instance SD-WAN dans Citrix DaaS pour Azure.

Responsabilités partagées des clients et de Citrix

Citrix Cloud Connector pour catalogues joints à un domaine

Citrix DaaS pour Azure déploie au moins deux Cloud Connector dans chaque emplacement de ressources. Certains catalogues peuvent partager un emplacement de ressources s'ils se trouvent dans la même région, le même appairage de réseaux virtuels et le même domaine que d'autres catalogues pour le même client. Citrix configure les Cloud Connector du client joints à un domaine pour les paramètres de sécurité par défaut suivants sur l'image :

- mises à jour du système d'exploitation et correctifs de sécurité
- logiciel antivirus
- mises à jour logicielles des Cloud Connector

Les clients n'ont normalement pas accès aux Cloud Connector. Toutefois, ils peuvent obtenir un accès en utilisant les étapes de dépannage du catalogue et en se connectant à l'aide des informations d'identification du domaine. Le client est responsable des modifications qu'il apporte lors d'une connexion via le bastion.

Les clients ont également le contrôle sur les Cloud Connector joints à un domaine via la stratégie de groupe Active Directory. Il incombe au client de s'assurer que les stratégies de groupe qui s'appliquent au Cloud Connector sont sûres et raisonnables. Par exemple, si le client choisit de désactiver les mises à jour du système d'exploitation à l'aide de la stratégie de groupe, il doit effectuer les mises à jour du système d'exploitation sur les Cloud Connector. Le client peut également choisir d'utiliser la stratégie de groupe pour appliquer une sécurité plus stricte que les valeurs par défaut de Cloud

Connector, par exemple en installant un autre logiciel antivirus. En général, Citrix recommande aux clients de placer les Cloud Connector dans leur propre unité organisationnelle Active Directory sans stratégie, car cela garantit que les valeurs par défaut utilisées par Citrix peuvent être appliquées sans problème.

Résolution des problèmes

Si le client rencontre des problèmes avec le catalogue dans Citrix DaaS pour Azure, il existe deux options de dépannage : l'utilisation de bastions et l'activation de l'accès RDP. Les deux options présentent un risque de sécurité pour le client. Le client doit comprendre et accepter ce risque avant d'utiliser ces options.

Il incombe à Citrix d'ouvrir et de fermer les ports nécessaires pour effectuer des opérations de dépannage, et de limiter les machines accessibles pendant ces opérations.

Avec des bastions ou un accès RDP, l'utilisateur actif effectuant l'opération est responsable de la sécurité des machines auxquelles il accède. Si le client accède au VDA ou au Cloud Connector via RDP et contracte accidentellement un virus, le client est responsable. Si le personnel du support Citrix accède à ces machines, il incombe à ce personnel d'effectuer les opérations en toute sécurité. La responsabilité des vulnérabilités exposées par toute personne accédant au bastion ou à d'autres machines du déploiement (par exemple, la responsabilité du client d'ajouter des plages IP pour autoriser la liste, la responsabilité Citrix de mettre en œuvre correctement les plages IP) est traitée ailleurs dans ce document.

Dans les deux scénarios, Citrix est responsable de la création correcte d'exceptions de pare-feu pour autoriser le trafic RDP. Citrix est également responsable de la révocation de ces exceptions après que le client a supprimé le bastion ou a mis fin à l'accès RDP via Citrix DaaS pour Azure.

Bastions Citrix peut créer des bastions dans le réseau virtuel du client géré par Citrix au sein de l'abonnement du client géré par Citrix pour diagnostiquer et réparer les problèmes, soit de manière proactive (sans notification du client), soit en réponse à un problème signalé par le client. Le bastion est une machine à laquelle le client peut accéder via RDP, puis utiliser pour accéder aux VDA et (pour les catalogues joints à un domaine) Cloud Connector via RDP pour collecter des journaux, redémarrer les services ou effectuer d'autres tâches administratives. Par défaut, la création d'un bastion ouvre une règle de pare-feu externe pour autoriser le trafic RDP depuis une plage d'adresses IP spécifiée par le client vers la machine bastion. Il ouvre également une règle de pare-feu interne pour autoriser l'accès aux Cloud Connector et aux VDA via RDP. L'ouverture de ces règles pose un risque important pour la sécurité.

Le client est responsable de fournir un mot de passe fort utilisé pour le compte Windows local. Le client est également responsable de fournir une plage d'adresses IP externe qui permet un accès RDP

au bastion. Si le client choisit de ne pas fournir de plage IP (permettant à quiconque de tenter l'accès RDP), le client est responsable de toute tentative d'accès par des adresses IP malveillantes.

Le client est également responsable de la suppression du bastion une fois le dépannage terminé. L'hôte bastion exposant une surface d'attaque supplémentaire, Citrix arrête automatiquement la machine huit (8) heures après sa mise sous tension. Toutefois, Citrix ne supprime jamais automatiquement un bastion. Si le client choisit d'utiliser le bastion pendant une longue période, il est responsable de l'application des correctifs et des mises à jour. Citrix recommande qu'un bastion ne soit utilisé que pendant plusieurs jours avant sa suppression. Si le client souhaite utiliser un bastion à jour, il peut supprimer son bastion actuel, puis créer un nouveau bastion, qui fournira à une nouvelle machine les derniers correctifs de sécurité.

Accès RDP Pour les catalogues appartenant à un domaine, si l'appairage de réseaux virtuels du client est fonctionnel, le client peut activer l'accès RDP depuis son réseau virtuel appairé vers son réseau virtuel géré par Citrix. Si le client utilise cette option, il est responsable de l'accès aux VDA et aux Cloud Connector via l'appairage de réseaux virtuels. Des plages d'adresses IP source peuvent être spécifiées afin que l'accès RDP puisse être encore plus restreint, même au sein du réseau interne du client. Le client devra utiliser les informations d'identification du domaine pour se connecter à ces machines. Si le client travaille avec le support Citrix pour résoudre un problème, il peut être nécessaire de partager ces informations d'identification avec le personnel de support. Une fois le problème résolu, le client est responsable de la désactivation de l'accès RDP. Garder l'accès RDP ouvert à partir du réseau appairé ou local du client présente un risque de sécurité.

Informations d'identification du domaine

Si le client choisit d'utiliser un catalogue joint au domaine, il est responsable de fournir à Citrix DaaS pour Azure un compte de domaine (nom d'utilisateur et mot de passe) avec les autorisations nécessaires pour joindre des machines au domaine. Lorsqu'il fournit des informations d'identification de domaine, le client doit respecter les principes de sécurité suivants :

- **Auditable :** le compte doit être créé spécifiquement pour l'utilisation de Citrix DaaS pour Azure afin qu'il soit facile de vérifier à quoi sert le compte.
- **Étendue :** le compte nécessite uniquement des autorisations pour joindre des machines à un domaine. Il ne doit pas s'agir d'un administrateur de domaine complet.
- **Sécurité :** Un mot de passe fort doit être placé sur le compte.

Citrix est responsable du stockage sécurisé de ce compte de domaine dans un trousseau de clés Azure dans l'abonnement Azure du client géré par Citrix. Le compte est récupéré uniquement si une opération nécessite le mot de passe du compte de domaine.

Plus d'informations

Pour obtenir des informations connexes, voir :

- Guide de déploiement sécurisé pour la plate-forme Citrix Cloud : informations de sécurité pour la plateforme Citrix Cloud.
- Vue d'ensemble de la sécurité technique : informations de sécurité pour Citrix DaaS.
- Avis de tiers

Abonnez-vous à Citrix DaaS pour Azure

December 21, 2022

Introduction

Vous pouvez vous abonner à Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard for Azure service) et commander le Fonds de consommation Citrix Azure, via Citrix ou via Azure Marketplace. Vous pouvez évaluer Citrix DaaS pour Azure via Citrix.

Si vous êtes actuellement abonné à Citrix Virtual Apps Essentials ou Citrix Virtual Desktops Essentials, vous pouvez effectuer une mise à niveau vers Citrix DaaS Standard pour Azure.

Une commande complète comporte deux parties :

- **Citrix DaaS Standard pour Azure :** vous permet d'utiliser vos propres abonnements Azure (gérés par le client).
- **Fonds de consommation Citrix Azure :** en outre, vous permet d'utiliser un abonnement Citrix Managed Azure, en plus de vos propres abonnements Azure. L'utilisation d'un abonnement Citrix Managed Azure offre les avantages suivants :
  - Facturation unique de Citrix, plutôt que facturations de plusieurs entreprises.
  - Différences entre les fonctionnalités des abonnements Azure
  - Support Microsoft de haut niveau via Citrix.

Le fonds de consommation Citrix Azure n'est pas requis. Toutefois, si vous ne l'avez pas, vous êtes limité à l'utilisation de vos propres abonnements Azure et vous ne bénéficiez pas des autres avantages des fonctionnalités.

Le processus de commande diffère légèrement selon que vous commandez via Citrix ou Azure Marketplace :

- Lorsque vous commandez via Citrix, vous pouvez commander Citrix DaaS Standard pour Azure et le Fonds de consommation Citrix Azure en même temps.
- Lorsque vous commandez via Azure Marketplace, vous commandez d'abord Citrix DaaS Standard pour Azure. Ensuite, vous commandez le fonds de consommation Citrix Azure.

  Si vous décidez de ne commander que Citrix DaaS pour Azure, vous pouvez commander le Fonds de consommation Citrix Azure ultérieurement, soit via Azure Marketplace, soit par l'intermédiaire de votre représentant de compte Citrix.

Quel que soit l'endroit où vous commandez Citrix DaaS Standard pour Azure et le fonds de consommation, Citrix fournit une aide à l'intégration. Nous vérifierons également que Citrix DaaS Standard pour Azure est exécuté et configuré correctement.

Résumé de commande

Récapitulatif des étapes de commande :

1. Obtenez un compte Citrix Cloud.

   Si vous avez déjà un compte Citrix Cloud et que vous êtes actuellement abonné à Citrix DaaS, consultez Si vous êtes actuellement abonné à Citrix DaaS.

2. Commandez Citrix DaaS Standard pour Azure et un fonds de consommation via Azure Marketplace, ou commandez auprès de Citrix.

Essais

Citrix DaaS Standard pour Azure propose deux types d'évaluation :

- **Ventes approuvées :** dans le cadre d'un essai approuvé par les ventes, vous pouvez utiliser un abonnement Citrix Managed Azure pour créer des catalogues, des images et d'autres tâches. À partir de la période d'essai, vous pouvez passer à un abonnement de service payant et commander le fonds de consommation Citrix Managed Azure. Si vous n'achetez pas de consommation, toutes les ressources que vous avez créées à l'aide de l'abonnement Citrix Managed Azure sont supprimées automatiquement, ce qui peut affecter les utilisateurs.
- **Approuvé automatiquement :** dans le cadre d'une période d'essai approuvée automatiquement, vous pouvez utiliser votre propre abonnement Azure (géré par le client) pour créer des catalogues, des images et d'autres tâches. À partir de la période d'essai, vous pouvez passer à un abonnement payant. Pour plus d'informations, voir Essais de service approuvés automatiquement.

Pour plus d'informations sur les essais, consultez la section Essais des services Citrix Cloud.

Essais de service approuvés automatiquement

- Un essai approuvé automatiquement de Citrix DaaS Standard pour Azure dure 7 jours calendaires.
- Au cours d'un essai auto-approuvé, vous pouvez créer des catalogues à l'aide de votre abonnement Azure. Les catalogues contiennent les machines qui fournissent des bureaux ou des applications.
- Vous pouvez créer des catalogues à l'aide d'une image préparée par Citrix, d'une image que vous importez depuis Azure ou d'une image que vous créez dans Citrix DaaS Standard pour Azure.
- Les utilisateurs doivent être configurés dans un fournisseur d'identité pris en chargepar Citrix Workspace.
- Vous pouvez affecter jusqu'à 25 utilisateurs à des catalogues dans le cadre de votre déploiement d'essai. Bien que vous puissiez affecter un utilisateur à plusieurs catalogues, un total de 25 utilisateurs nommés uniques sont autorisés dans un déploiement d'essai.
- Vous devez disposer d'un compte d'utilisateur Microsoft Azure et d'au moins un abonnement Azure dans ce compte. (Les essais ne prennent en charge que les cas d'utilisation des abonnements Azure appartenant au client (apportez les vôtres).)

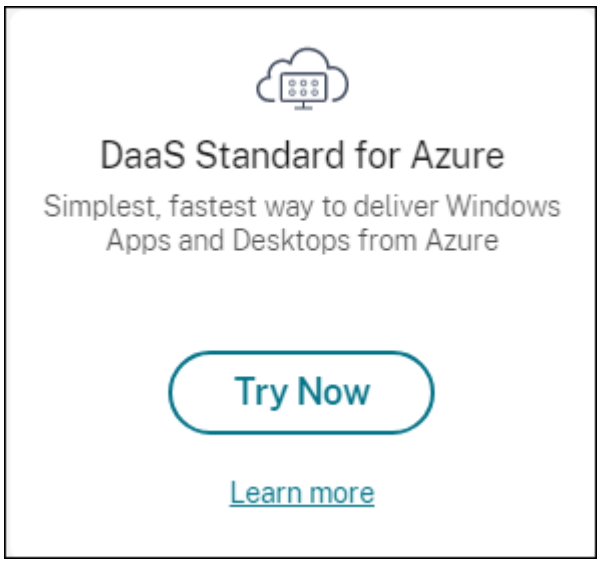
Demander et utiliser un essai de service approuvé automatiquement

1. Créez un compte Citrix Cloud (si vous n'en avez pas déjà un).

   a) Accédez à Citrix Cloud.
   b) Sélectionnez **Inscrivez-vous pour un essai gratuit**.
   c) Suivez les instructions à l'écran.

   Dans quelques instants, vous recevrez un e-mail concernant votre compte Citrix Cloud. Sélectionnez le lien de connexion dans l'e-mail.

2. Demandez un essai. Dans la console Citrix Cloud, sélectionnez **Essayer maintenant** sur la vignette **DaaS Standard pour Azure** .



Vous recevrez un e-mail lorsque votre essai de service sera activé et prêt (généralement environ deux heures après la demande d'essai).

3. Connectez-vous à Citrix Cloud.
4. Cliquez sur **Gérer** sur la vignette **DaaS Standard pour Azure** .
5. Configurez et configurez votre environnement d'essai. Au cours de la configuration, vous allez :

   a) Ajoutez votre abonnement Azure au service.
   b) Connectez votre fournisseur d'identité via la console Citrix Cloud.
   c) Créez un catalogue.
   d) Ajoutez des utilisateurs de votre fournisseur d'identité au catalogue.
   e) Informez vos utilisateurs de l'URL Citrix Workspace.

L'interface graphique vous guide tout au long du processus de configuration. Pour plus de détails, consultez la documentation du produit :

- Familiarisez-vous avec le produit et sa terminologie.
- Consultez les résumés et les détails de la configuration.

Obtenez un compte Citrix Cloud

Pour créer un compte Citrix Cloud et demander un essai, rendez-vous sur https://onboarding.cloud.com. Pour plus d'informations sur ce processus, consultez la section S'inscrire à Citrix Cloud. Votre compte possède un ID d'organisation (OrgID) qui apparaît toujours dans le coin supérieur droit de la console Citrix Cloud.

Prochaines étapes : Commandez Citrix DaaS Standard pour Azure via Citrix ou via Azure Marketplace.

Si vous êtes actuellement abonné à Citrix DaaS

Un compte Citrix Cloud (OrgID) vous permet de vous abonner à une seule édition de Citrix DaaS à la fois.

Vous pouvez effectuer une mise à niveau de Citrix DaaS Standard pour Azure vers l'une des éditions suivantes :

- Citrix DaaS Advanced Edition
- Édition Premium de Citrix DaaS.

Pour plus d'informations, contactez votre représentant Citrix.

Si vous êtes actuellement abonné à une édition Citrix DaaS autre que Advanced ou Premium (par exemple, Citrix Virtual Apps Essentials ou Citrix Virtual Desktops Essentials) et que vous souhaitez vous abonner à Citrix DaaS Standard pour Azure, vous devez soit :

- Abonnez-vous à Citrix DaaS Standard pour Azure à l'aide d'un autre compte Citrix Cloud (OrgID). Pour plus de détails, consultez la section Mettre à niveau vers Citrix DaaS Standard pour Azure.
- Mettez hors service le service dont vous disposez, puis commandez Citrix DaaS Standard pour Azure. Vous trouverez des instructions pour la désactivation dans CTX239027.

Vous pouvez utiliser un abonnement Citrix Managed Azure en achetant le Fonds de consommation Citrix Azure avec l'une des éditions de service suivantes :

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

Commander via Citrix

Vous pouvez commander Citrix DaaS Standard pour Azure (y compris le fonds de consommation) via Citrix Cloud ou auprès de votre représentant de compte Citrix.

Via Citrix Cloud :

1. Connectez-vous à Citrix Cloud. Cliquez sur **Essayer maintenant** sur la vignette **DaaS Standard pour Azure** . Renseignez les informations demandées. Le texte de la vignette devient **Essai demandé**.
2. Citrix vous contacte. Lorsque Citrix DaaS Standard pour Azure est disponible, le texte de la vignette devient **Gérer**.
3. Connectez-vous à Citrix Cloud. Sur la vignette **DaaS Standard pour Azure**, cliquez sur **Gérer**. La première fois que vous accédez à Citrix DaaS Standard pour Azure, vous êtes redirigé vers la page d'**accueil** de Quick Deploy.

Annulation d'un abonnement mensuel via Citrix

Les abonnements mensuels sont renouvelés automatiquement au début de chaque mois. Vous pouvez utiliser le tableau de bord Citrix DaaS Standard pour Azure pour annuler un abonnement mensuel que vous avez commandé via Citrix.

(Vous ne pouvez pas utiliser le tableau de bord Citrix DaaS Standard pour Azure pour annuler d'autres types d'abonnement que vous avez commandés via Citrix ou des commandes passées via Azure Marketplace.)

Pour annuler un abonnement mensuel :

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
3. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Général** sur la droite.
4. Cliquez sur **Annuler l'abonnement**.
5. Vos ressources actives sont répertoriées, telles que les catalogues, les images et les connexions. La page présente les actions entreprises par Citrix lors d'une annulation. Il vous informe également des mesures que vous devez prendre, le cas échéant. Indiquez pourquoi vous annulez le service. Si vous le souhaitez, fournissez plus de commentaires. Lorsque vous avez terminé, cliquez sur **Annuler l'abonnement**.
6. Confirmez que vous comprenez les conditions de l'annulation.

Une bannière sur le tableau de bord Citrix DaaS Standard pour Azure indique la réception de votre demande d'annulation.

Si vous annulez votre abonnement accidentellement, contactez votre représentant commercial Citrix ou votre partenaire Citrix avant la fin du mois pour réactiver Citrix DaaS Standard pour Azure.

Commander via Azure Marketplace

Commandez d'abord le Citrix DaaS Standard pour Azure, puis commandez le Fonds de consommation Citrix Azure.

Vous ne pouvez pas commander le fonds de consommation sauf si vous avez déjà acheté Citrix DaaS Standard pour Azure. Vous ne pouvez pas combiner Citrix DaaS Standard pour Azure et le fonds de consommation en une seule commande.

Citrix DaaS Standard pour Azure n'est pas proposé via le portail des fournisseurs de solutions cloud Azure. Si vous êtes un client d'assistance prioritaire ou si vous souhaitez bénéficier d'une assistance prioritaire, contactez votre représentant de compte Citrix.

Exigences :

- L'OrgID de votre compte Citrix Cloud.
  - Si vous possédez un compte Citrix Cloud, mais que vous ne connaissez pas l'OrgID, regardez dans le coin supérieur droit de la console Citrix Cloud. Vous pouvez également consulter l'e-mail que vous avez reçu lorsque vous avez créé le compte.
  - Si vous n'avez pas de compte Citrix Cloud, suivez les instructions de la section Obtenir un compte Citrix Cloud.
- Un compte Azure et au moins un abonnement Azure dans ce compte.

Commander Citrix DaaS Standard pour Azure via Azure Marketplace

1. Connectez-vous à Azure Marketplace à l'aide des informations d'identification de votre compte Azure.
2. Recherchez puis accédez à **Citrix DaaS Standard pour Azure**.
3. Cliquez sur **GET IT NOW**.
4. Dans le message **Encore une chose**, activez la case à cocher, puis cliquez sur **Continuer**.
5. Les onglets contiennent des informations sur le produit, les plans, les prix et l'utilisation. Lorsque vous êtes prêt, sélectionnez un plan (s'il y en a plusieurs disponibles), puis cliquez sur **Configurer + s'abonner**.
6. Dans l'onglet **Fonctions de base** :
   - **Abonnement** : indique le plan que vous avez sélectionné.
   - **Nom** : saisissez un nom pour votre commande d'abonnement.
   - La section **Plan** affiche le prix du plan sélectionné, sur la base de termes mensuels et pluriannuels (annuels).

     Pour modifier la durée du plan (mensuel ou annuel), sélectionnez **Modifier le plan**. Sélectionnez la durée souhaitée et cliquez sur **Modifier le plan**.
7. Dans l'onglet **Révision + abonnement** :
   - Consultez les informations de contact que vous avez fournies précédemment pour le profil de base Azure. Vous pouvez modifier votre adresse, votre numéro de téléphone ou les deux.
   - Cliquez sur **S'abonner**.
8. Sur la page **Abonnement en cours**, cliquez sur **Configurer le compte maintenant**. (Si le bouton est désactivé, patientez un moment.) Vous êtes redirigé vers une page d'activation Citrix.
9. Sur la page d'activation :

- Utilisez le **lien Connexion** pour vous connecter à Citrix Cloud. Une connexion réussie remplit automatiquement le champ **ID d'organisation**.
- **Quantité :** entrez le nombre d'utilisateurs. (Une commande initiale doit être d'au moins 25.) Un prix estimé est affiché.
- Acceptez les termes et conditions, puis cliquez sur **Activer la commande**.

Citrix vous envoie un e-mail lorsque votre service est provisionné. Le provisionnement peut prendre un certain temps. Si vous ne recevez pas l'e-mail le jour suivant, contactez l'assistance Citrix.

Lorsque vous recevez l'e-mail de Citrix, vous pouvez commencer à utiliser Citrix DaaS Standard pour Azure. N'oubliez pas : avec Citrix DaaS Standard pour Azure uniquement, vous ne pouvez utiliser que vos propres abonnements Azure.

Ne supprimez pas la ressource Citrix DaaS Standard pour Azure dans Azure. La suppression de cette ressource annule votre abonnement.

Commandez le fonds de consommation via Azure Marketplace

1. Connectez-vous à Azure Marketplace à l'aide des informations d'identification de votre compte Azure.
2. Recherchez et accédez à **Citrix Azure Consumption Fund**.
3. Cliquez sur **GET IT NOW**.
4. Cliquez sur **Configurer + s'abonner**.
5. Sur la page **S'abonner** :

   - Dans **Nom**, saisissez un nom facilement reconnaissable, tel que « Mes postes de travail gérés ». Vous pouvez utiliser ce nom ultérieurement, si vous souhaitez modifier l'abonnement au service.
   - Indiquez le nombre d'utilisateurs que vous souhaitez prendre en charge, compris entre 25 et 100 000.
   - Entrez votre adresse e-mail et votre numéro de téléphone.

   Lorsque vous avez terminé, cliquez sur **S'abonner**.
6. Sur la page **Progression de l'abonnement**, lorsque le bouton **Configurer le compte SaaS sur le site de l'éditeur** devient actif (bleu), cliquez dessus. Vous êtes automatiquement redirigé vers une page d'activation de commande Citrix.
7. Sur la page d'activation des commandes Citrix, saisissez votre Citrix Cloud OrgID. L'adresse e-mail que vous avez saisie précédemment s'affiche. Vous pouvez le modifier si nécessaire. Lorsque vous avez terminé, cliquez sur **Activer la commande**.

8. L'exécution de la commande du fonds de consommation ne prend pas beaucoup de temps. Lorsque Citrix est informé de la commande, une bannière apparaît dans la console Citrix DaaS pour Azure, indiquant qu'un abonnement Azure géré par Citrix est en cours de préparation pour vous.

   Le panneau **Abonnements Cloud** sur la droite du tableau de bord **Gérer > Déploiement rapide d'Azure** indique quand cet abonnement est prêt à être utilisé.

Augmentez ou diminuez les sièges utilisateur via Azure Marketplace

Si vous devez augmenter les sièges utilisateur, créez une nouvelle commande Azure Marketplace pour le nombre supplémentaire de postes que vous souhaitez.

Pour réduire le nombre de postes dont vous disposez, annulez Citrix DaaS Standard pour Azure sur Azure Marketplace, puis passez une commande pour le nombre de postes souhaité.

Annuler Citrix DaaS Standard pour Azure ou le fonds de consommation via Azure Marketplace

Pour annuler Citrix DaaS Standard pour Azure ou le fonds de consommation via Azure Marketplace :

1. Connectez-vous à Azure Marketplace.
2. Recherchez **DaaS**.
3. Sélectionnez **Nouveau > Afficher**.
4. Sélectionnez la ressource que vous souhaitez annuler.
5. Dans le menu représentant des points de suspension de la ressource, sélectionnez **Supprimer**.
6. Cliquez sur **Oui** dans la zone de confirmation pour confirmer que vous connaissez la politique de remboursement et que vous souhaitez annuler la ressource.

> **Important :**
>
> N'annulez pas le fonds de consommation Citrix Azure si vous utilisez des ressources gérées par Citrix, telles que des catalogues ou des images créés dans l'abonnement Citrix Managed Azure.

Quand votre commande est approuvée et traitée

Une fois votre essai ou service approuvé, plusieurs vignettes apparaissent sur la page d'accueil de Citrix Cloud :

- Citrix DaaS pour Azure
- Citrix DaaS
- Gateway

Citrix DaaS pour Azure est le seul service activé pour votre utilisation.

Pour commencer à utiliser Citrix DaaS Standard pour Azure, connectez-vous à Citrix Cloud. Accédez à Citrix DaaS Standard pour Azure à l'aide de l'une des méthodes suivantes :

- Sur la vignette **DaaS Standard pour Azure**, cliquez sur **Gérer**.
- Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.

Pour obtenir des conseils de configuration, voir Commencer.

Mise à niveau vers Citrix DaaS Standard pour Azure

Si vous êtes actuellement abonné au service Citrix Virtual Apps Essentials ou Citrix Virtual Desktops Essentials, effectuez la mise à niveau vers Citrix DaaS Standard pour Azure en effectuant les tâches suivantes.

1. Créez un nouvel ID d'organisation (OrgID) à utiliser avec la norme Citrix DaaS pour Azure sur https://onboarding.cloud.com/. (Comme décrit précédemment dans cet article, vous ne pouvez pas utiliser le même OrgID pour vous abonner à plusieurs éditions de Citrix DaaS.)
2. Contactez le service commercial Citrix pour acheter Citrix DaaS Standard pour Azure et le Fonds de consommation Citrix Azure, à l'aide du nouvel OrgID. (Vous n'êtes pas obligé de commander le fonds de consommation, mais sans celui-ci, vous ne pouvez pas accéder à toutes les fonctionnalités de Citrix DaaS Standard pour Azure.)
3. Connectez-vous à Citrix Cloud. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
4. Ajoutez au moins un de vos abonnements Azure à Citrix DaaS Standard pour Azure.
5. Importez une ou plusieurs images de vos abonnements Azure dans Citrix DaaS Standard pour Azure.
6. Créez des catalogues à l'aide des images que vous avez importées à partir de vos abonnements Azure.
7. Ajoutez des utilisateurs aux catalogues que vous avez créés.
8. Si vous souhaitez conserver la même URL d'espace de travail que celle utilisée avec Citrix Virtual Apps Essentials ou Citrix Virtual Desktops Essentials :

    a) Connectez-vous à Citrix Cloud à l'aide de l'OrgID que vous utilisez avec le service Essentials. Sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. Changez l'URL de votre espace de travail en une autre.

    b) Connectez-vous à Citrix Cloud à l'aide de l'OrgID que vous utilisez avec Citrix DaaS Standard pour Azure. Sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. Remplacez l'URL de l'espace de travail par celle que vous utilisiez auparavant pour le service Essentials.

9. Connectez-vous à Azure et supprimez toutes les ressources que vous avez utilisées avec le service Essentials. Pour obtenir des conseils, voir Annuler Virtual Apps Essentials. (La procédure est équivalente pour Citrix Virtual Desktops Essentials.)
10. Arrêtez votre service Essentials en supprimant votre ressource Azure Marketplace dans Azure.

Mise en route

September 7, 2022

Cet article résume les tâches de configuration pour la mise à disposition de postes de travail et d'applications à l'aide de Citrix Daas Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard for Azure service). Nous vous recommandons de consulter chaque procédure avant de la mettre en œuvre, afin que vous sachiez à quoi vous attendre.

Pour les tâches de configuration de Remote PC Access, reportez-vous Remote PC Access.

> **Important :**
>
> Pour être sûr d'obtenir les informations importantes sur Citrix Cloud et les services Citrix auxquels vous êtes abonné, vérifiez que vous pouvez recevoir toutes les notifications par e-mail. Par exemple, Citrix envoie des e-mails de notification informatifs mensuels détaillant votre consommation Azure (utilisation).
>
> Dans le coin supérieur droit de la console Citrix Cloud, développez le menu situé à droite des champs Nom du client et OrgID. Sélectionnez **Paramètres du compte**. Dans l'onglet **Mon profil**, sélectionnez toutes les entrées de la section **Notifications par e-mail**.

Résumé des tâches de configuration

Les sections suivantes de cet article vous guident dans les tâches de configuration :

1. Préparez-vous à la configuration.
2. Configurez un déploiement en suivant les instructions de l'un des éléments suivants :
    - Déploiement rapide de preuve de concept
    - Déploiement en production
3. Fournissez l'URL de l'espace de travail à vos utilisateurs.

Préparer

- Si vous n'êtes pas familier avec les catalogues, les images, les connexions réseau ou les abonnements Azure, consultez les concepts d'introduction et les informations terminologiques .
- Lisez la présentation de la sécurité pour savoir et comprendre ce dont vous (le client) et Citrix êtes responsables.
- Si vous ne possédez pas encore de compte Citrix Cloud pouvant être utilisé pour ce service, obtenez-en un, puis inscrivez-vous au service.
- Vérifiez la configuration système requise.
- Passez en revue les étapes de configuration : preuve de concept ou production.

Configurer un déploiement rapide de preuve de concept

Cette procédure nécessite un abonnement Azure géré par Citrix.

1. Créez un catalogue à l'aide de la création rapide.
2. Ajoutez vos utilisateurs à Managed Azure AD.
3. Ajoutez vos utilisateurs au catalogue.
4. Informez vos utilisateurs de l'URL Workspace.

Configurer un déploiement de production

1. Si vous utilisez votre propre Active Directory ou Azure Active Directory pour authentifier les utilisateurs, connectez-vous et définissez cette méthode dans Citrix Cloud.
2. Si vous utilisez des machines jointes à un domaine, vérifiez que vous disposez d'entrées de serveur DNS valides.
3. Si vous utilisez votre propre abonnement Azure (au lieu d'un abonnement Citrix Managed Azure), importez votre abonnement Azure.
4. Créez ou importez une image. Bien que vous puissiez utiliser l'une des images préparées par Citrix telle quelle dans un catalogue, elles sont principalement destinées à des déploiements de preuve de concept.
5. Si vous utilisez un abonnement Azure géré par Citrix et que vous souhaitez que vos utilisateurs puissent accéder à des éléments de votre réseau (tels que les serveurs de fichiers), configurez une connexion Peering de réseau virtuel Azure ou Citrix SD-WAN.
6. Créez un catalogue à l'aide de la création personnalisée.
7. Si vous créez un catalogue de machines à sessions multiples ajoutez des applications au catalogue, si nécessaire.
8. Si vous utilisez Azure géré par Citrix AD pour authentifier vos utilisateurs, ajoutez des utilisateurs à l'annuaire.
9. Ajoutez des utilisateurs au catalogue.

10. Informez vos utilisateurs de l'URL Workspace.

Après avoir configuré le déploiement, utilisez le tableau de bord **Surveiller** dans Citrix DaaS pour Azure pour voir l'utilisation des postesde travail, les sessionset les machines.

Configuration système requise

Pour tous les déploiements :

- **Citrix Cloud :** Ce service est fourni via Citrix Cloud et nécessite un compte Citrix Cloud pour terminer le processus d'intégration. Pour plus de détails, consultez la section Obtenir un compte Citrix Cloud.
- **Licences Windows :** assurez-vous de disposer d'une licence adaptée pour les Services Bureau à distance pour exécuter des charges de travail Windows Server ou Azure Virtual Desktop Licensing pour Windows 10.

Si vous utilisez un abonnement Citrix Managed Azure :

- **Abonnements Azure lors de l'utilisation de l'appairage de réseaux virtuels Azure (facultatif) :** si vous prévoyez d'accéder aux ressources (telles que AD et d'autres partages de fichiers) de votre propre réseau Azure à l'aide de connexions homologues Azure VNet, vous devez disposer d'un abonnement Azure.
- **Joindre des VDA à Azure Active Directory (facultatif) :** pour joindre des VDA à un domaine à l'aide de la stratégie de groupe Active Directory, vous devez être un administrateur autorisé à effectuer cette action dans Active Directory. Pour plus de détails, voir Responsabilité du client.

La configuration des connexions à votre réseau local d'entreprise comporte des exigences supplémentaires.

- Toute connexion (Azure VNet peering ou SD-WAN) : Exigences pour toutes les connexions.
- Connexions Azure VNet peering : Configuration requise et préparation pour Azure VNet peering.
- Connexions SD-WAN : Configuration requise et préparation de la connexion SD-WAN.

Si vous souhaitez utiliser vos propres images Azure lors de la création d'un catalogue, ces images doivent répondre à certaines exigences avant de les importer dans Citrix DaaS pour Azure.

Informations supplémentaires :

- Exigences en termes de connexion Internet :Configuration requise pour le système et la connectivité.
- Limites de ressources dans un déploiement de service : Limites.

Systèmes d'exploitation pris en charge

Lorsque vous utilisez un abonnement Citrix Managed Azure :

- Windows 7 (le VDA doit être 7.15 LTSR avec la dernière mise à jour cumulative)
- Windows 10 session unique
- Windows 10 sessions multiples
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (nécessite un VDA 2106 minimum)
- Red Hat Enterprise Linux et Ubuntu

Lorsque vous utilisez un abonnement Azure géré par le client :

- Windows 7 (le VDA doit être 7.15 LTSR avec la dernière mise à jour cumulative)
- Windows 10 Enterprise session unique
- Windows 10 Enterprise Virtual Desktop sessions multiples
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (nécessite un VDA 2106 minimum)
- Red Hat Enterprise Linux et Ubuntu

URL de l'espace de travail

Après avoir créé des catalogues et y avoir alloué des utilisateurs, indiquez aux utilisateurs où trouver leurs bureaux et applications : l'URL Workspace. L'URL Workspace est la même pour tous les catalogues et utilisateurs.

Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, affichez l'URL en développant **User Access & Authentication** sur la droite.

Vous pouvez modifier la première partie de l'URL de l'espace de travail dans Citrix Cloud. Pour obtenir des instructions, voir Personnaliser l'URL de l'espace de travail.

Obtenir de l'aide

Consultez l'article Dépannage .

Si vous rencontrez toujours des problèmes avec le service, ouvrez un ticket en suivant les instructions de la section Comment obtenir de l'aide.

Créer des catalogues

October 7, 2022

Lorsqu'il est utilisé pour des applications et des bureaux publiés, un catalogue est un groupe de machines virtuelles identiques. Lorsque vous déployez des postes de travail, les machines du catalogue sont partagées avec les utilisateurs sélectionnés. Lorsque vous publiez des applications, les machines multi-sessions hébergent des applications qui sont partagées avec les utilisateurs sélectionnés.

> **Remarque :**
>
> Pour plus d'informations sur la création de catalogues Remote PC Access, consultez Remote PC Access.

Types de machines

Un catalogue peut contenir l'un des types de machines suivants :

- **Statique :** le catalogue contient des machines statiques à session unique (également appelées bureaux personnels, dédiés ou persistants). Statique signifie que lorsqu'un utilisateur démarre un bureau, celui-ci « appartient » à cet utilisateur. Toute modification apportée par cet utilisateur au bureau est conservée lors de la fermeture de session. Plus tard, lorsque cet utilisateur revient sur Citrix Workspace et démarre un bureau, il s'agira du même bureau.
- **Aléatoire :** le catalogue contient des machines aléatoires à session unique (également appelées bureaux non persistants). Aléatoire signifie que lorsqu'un utilisateur démarre un bureau, toute modification apportée par cet utilisateur à ce bureau est supprimée après la fermeture de session. Plus tard, lorsque cet utilisateur revient sur Citrix Workspace et démarre un bureau, il peut s'agir ou non du même bureau.
- **Sessions multiples :** le catalogue contient des machines avec des applications et des bureaux. Plusieurs utilisateurs peuvent simultanément accéder à chacune de ces machines. Les utilisateurs peuvent lancer un bureau ou des applications depuis leur espace de travail. Les sessions d'application peuvent être partagées. Le partage de session n'est pas autorisé entre une application et un bureau.
  - Lorsque vous créez un catalogue à sessions multiples, vous sélectionnez la charge de travail : légère (par exemple saisie de données), moyenne (comme les applications bureautiques), lourde (comme l'ingénierie) ou personnalisée. Chaque option représente un nombre spécifique de machines et de sessions par machine, ce qui donne le nombre total de sessions prises en charge par le catalogue.

- Si vous sélectionnez la charge de travail personnalisée, vous sélectionnez l'une des combinaisons disponibles d'unités centrales, de RAM et de stockage. Tapez le nombre de machines et de sessions par machine, ce qui donne le nombre total de sessions prises en charge par le catalogue.

Lors du déploiement de bureaux, les types de machines statiques et aléatoires sont parfois appelés « types de bureau ».

Façons de créer un catalogue

Il existe plusieurs façons de créer et de configurer un catalogue :

- La **création rapide** est le moyen le plus rapide de démarrer. Vous fournissez un minimum d'informations, et Citrix DaaS pour Azure s'occupe du reste. Un catalogue à création rapide est idéal pour un environnement de test ou une preuve de concept.
- La **création personnalisée** permet plus de choix de configuration que la création rapide. Elle est plus adaptée à un environnement de production qu'un catalogue à création rapide.
- Les catalogues **Remote PC Access** contiennent des machines existantes (généralement physiques) auxquelles les utilisateurs accèdent à distance. Pour plus de détails et des instructions sur ces catalogues, consultez Remote PC Access.

Voici une comparaison entre la création rapide et la création personnalisée :

Création rapide	Création personnalisée
Moins d'informations à fournir.	Plus d'informations à fournir.
Moins de choix pour certaines fonctionnalités.	Plus de choix pour certaines fonctionnalités.
Authentification utilisateur Azure Active Directory gérée par Citrix.	Choix entre : Azure Active Directory géré par Citrix ou votre Active Directory/Azure Active Directory.
Aucune connexion à votre réseau local.	Choix entre : aucune connexion à votre réseau local, à Azure VNet peering et au SD-WAN.
Utilise une image Windows 10 préparée par Citrix. Cette image contient un VDA de bureau actuel.	Choix de : images préparées par Citrix, images que vous importez depuis Azure ou images que vous avez créées dans Citrix DaaS pour Azure à partir d'une image préparée ou importée par Citrix.
Chaque bureau dispose d'un stockage sur disque standard (HDD) Azure.	Plusieurs options de stockage sont disponibles.

Création rapide	Création personnalisée
Bureaux statiques uniquement.	Bureaux statiques, aléatoires ou à sessions multiples.
Un programme de gestion de l'alimentation ne peut pas être configuré pendant la création. La machine hébergeant le bureau s'éteint à la fin de la session. (Vous pouvez modifier ce paramètre ultérieurement.)	Un calendrier de gestion de l'alimentation peut être configuré lors de la création.
Vous devez utiliser un abonnement Azure géré par Citrix.	Vous pouvez utiliser Citrix Managed Azure ou votre propre abonnement Azure.

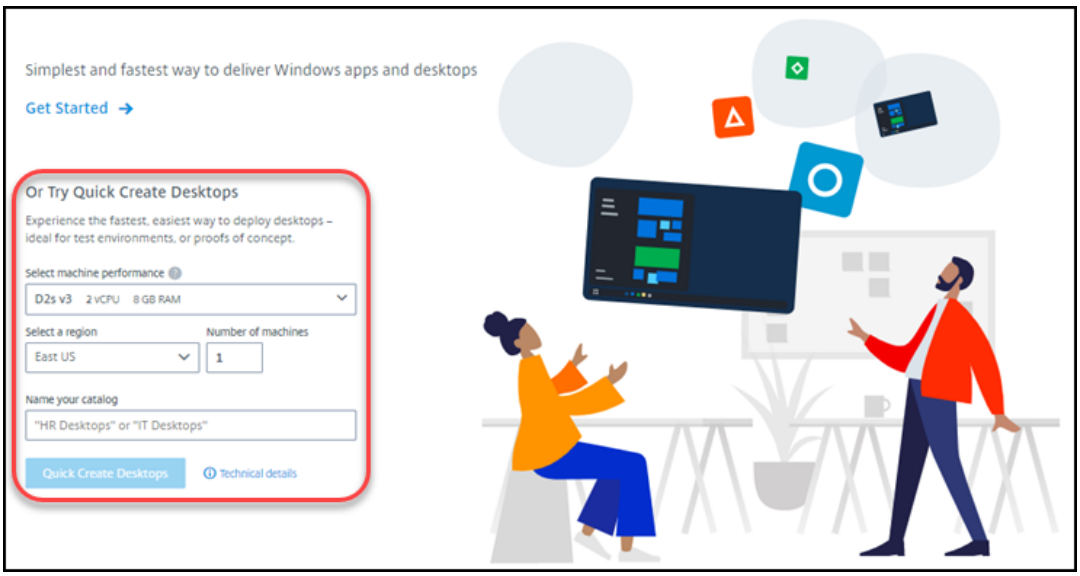
Pour plus de détails, consultez :

- Créer un catalogue à l'aide de la création rapide
- Créez un catalogue à l'aide de la création personnalisée

Créer un catalogue à l'aide de la création rapide

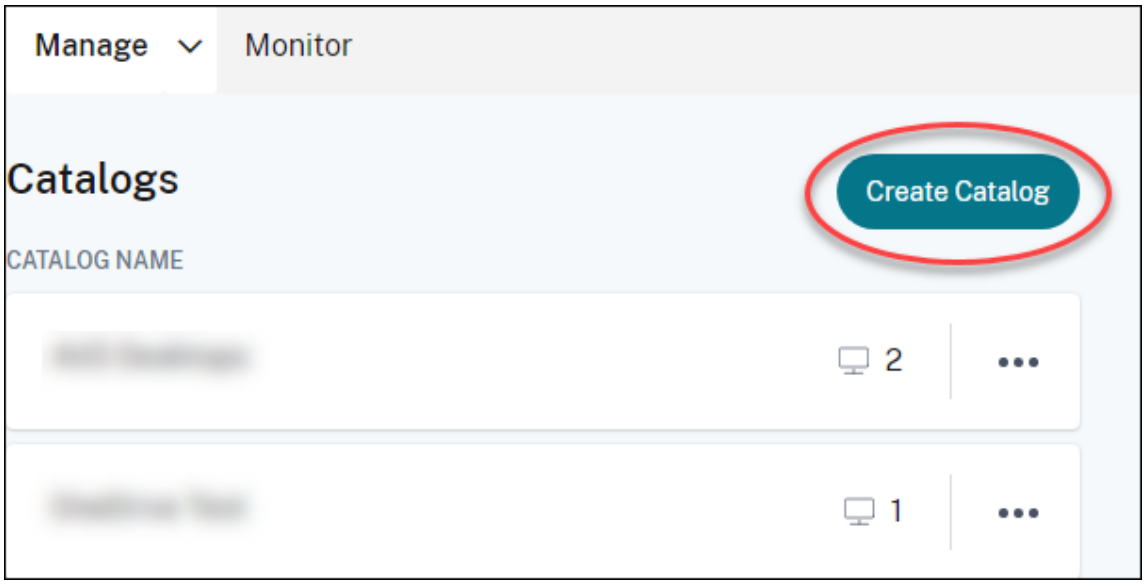
Cette méthode de création de catalogue utilise toujours un abonnement Citrix Managed Azure.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
3. Si aucun catalogue n'a encore été créé, vous accédez à la page d'**accueil** de Quick Deploy. Choisissez l'une des options suivantes :
    - Configurez le catalogue sur cette page. Passez aux étapes 6 à 10.

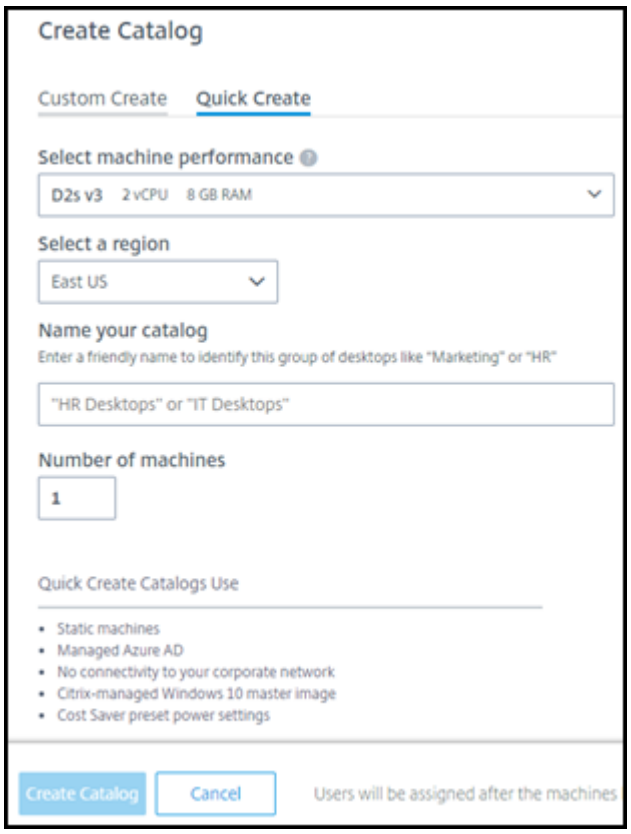


- Cliquez sur **Commencer**. Vous êtes redirigé vers le tableau de bord **Gérer > Déploiement rapide d'Azure** . Cliquez sur **Créer un catalogue**.

4. Si un catalogue a déjà été créé (et que vous en créez un autre), vous êtes redirigé vers le tableau de bord **Gérer > Déploiement rapide Azure** . Cliquez sur **Créer un catalogue**.



5. Cliquez sur **Création rapide** en haut de la page, s'il n'est pas déjà sélectionné.



- **Performances de la machine :** sélectionnez le type de machine. Chaque choix comprend une combinaison unique d'unités centrales, de RAM et de stockage. Les machines plus performantes ont des coûts mensuels plus élevés.
- **Région :** sélectionnez la région dans laquelle vous souhaitez créer les machines. Vous pouvez sélectionner une région proche de vos utilisateurs.
- **Nom :** saisissez un nom pour le catalogue. Ce champ est obligatoire et il n'y a pas de valeur par défaut.
- **Nombre de machines :** saisissez le nombre de machines souhaitées.

6. Lorsque vous avez terminé, cliquez sur **Créer un catalogue**. (Si vous créez le premier catalogue à partir de la page d'**accueil** de Quick Deploy, cliquez sur **Création rapide de bureaux**.)

Vous êtes automatiquement redirigé vers le tableau de bord **Gérer > Déploiement rapide d'Azure** . Pendant la création du catalogue, le nom du catalogue est ajouté à la liste des catalogues, ce qui indique l'avancement de la création.

Citrix DaaS pour Azure crée également automatiquement un emplacement de ressources et ajoute deux Cloud Connector.

Que faire ensuite :

- Si vous utilisez Citrix Managed Azure AD pour l'authentification des utilisateurs, vous pouvez ajouter des utilisateurs à l'annuaire lors de la création du catalogue.

- Quelle que soit la méthode d'authentification des utilisateurs que vous utilisez, une fois le catalogue créé, ajoutez des utilisateurs au catalogue.

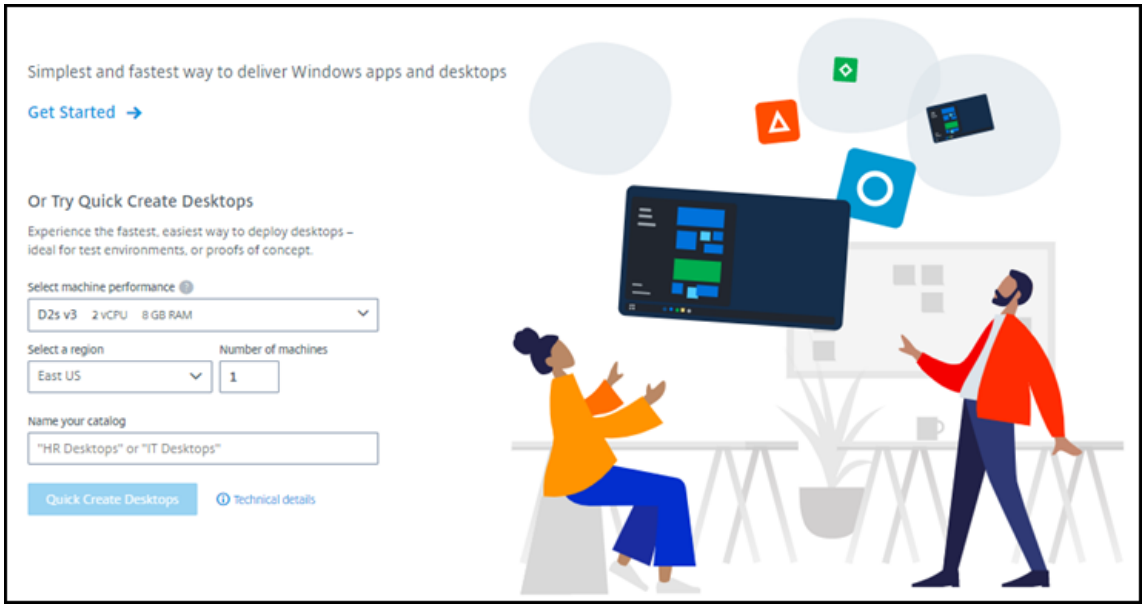
Créez un catalogue à l'aide de la création personnalisée

Si vous utilisez un abonnement Azure géré par Citrix et que vous prévoyez d'utiliser une connexion à vos ressources réseau locales, créez une connexion réseau avant de créer le catalogue. Pour permettre à vos utilisateurs d'accéder à vos ressources réseau locales ou à d'autres ressources réseau, vous devez également obtenir des informations Active Directory pour cet emplacement.

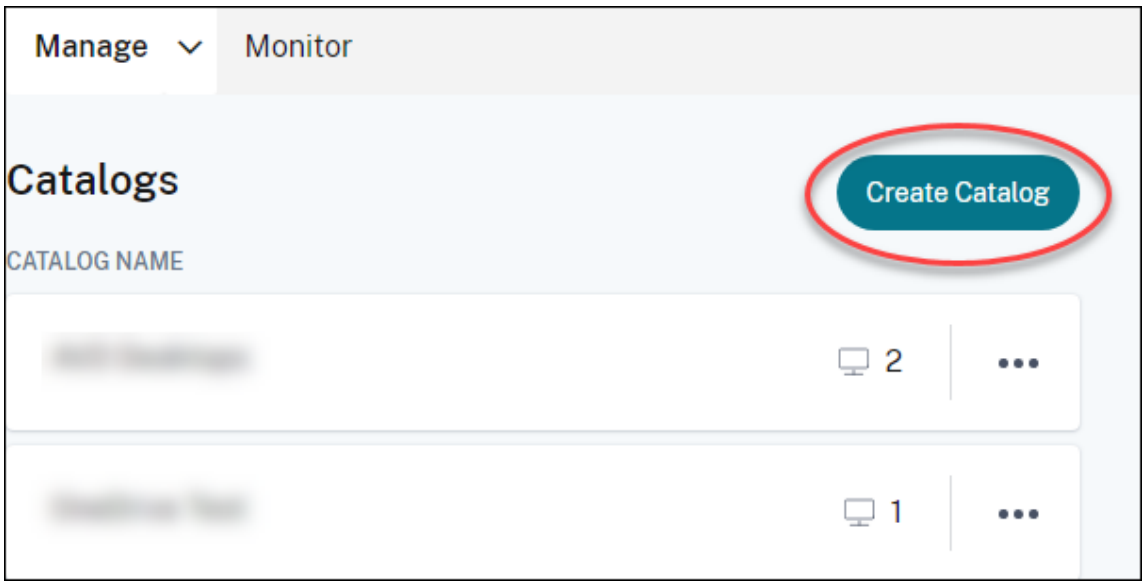
Si vous n'avez pas d'abonnement Azure géré par Citrix, vous devez importer (ajouter) au moins un de vos propres abonnements Azure à Citrix DaaS pour Azure avant de créer un catalogue.

Pour créer un catalogue :

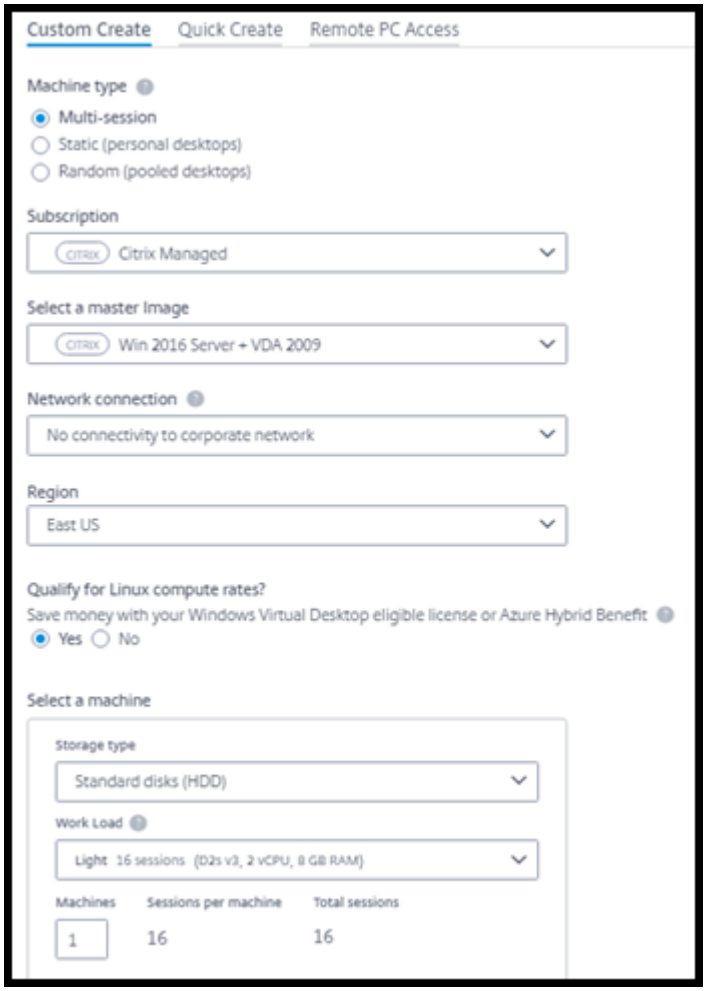
1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
3. Si aucun catalogue n'a encore été créé, vous accédez à la page d'**accueil** de Quick Deploy. Cliquez sur **Commencer**. À la fin de la page d'introduction, vous êtes redirigé vers le tableau de bord **Gérer > Déploiement rapide Azure** . Cliquez sur **Créer un catalogue**.



Si un catalogue a déjà été créé, vous êtes redirigé vers le tableau de bord **Gérer > Déploiement rapide Azure** . Cliquez sur **Créer un catalogue**.



4. Sélectionnez **Création personnalisée** en haut de la page, si ce n'est pas déjà fait.



5. Renseignez les champs suivants : (Certains champs sont valides uniquement pour certains

types de machines. L'ordre des champs peut différer.)

- **Type de machine** : sélectionnez un type de machine Pour plus d'informations, consultez la section Types de machines.
- **Abonnement** : Sélectionnez un abonnement Azure. Pour plus de détails, consultez Abonnements Azure.
- **Image principale :** sélectionnez une image du système d'exploitation. Pour plus de détails, voir Images.
- **Connexion réseau :** sélectionnez la connexion à utiliser pour accéder aux ressources de votre réseau. Pour plus de détails, consultez la section Connexions réseau.
  - Pour un abonnement Citrix Managed Azure, les choix sont les suivants :
    - **Aucune connectivité :** l'utilisateur ne peut pas accéder aux emplacements et aux ressources de votre réseau d'entreprise local.
    - *Connexions :* sélectionnez une connexion, telle qu'un appairage de réseaux virtuels ou une connexion SD-WAN.
  - Pour un abonnement Azure géré par le client, sélectionnez le groupe de ressources, le réseau virtuel et le sous-réseau appropriés.
- **Région :** (disponible uniquement si vous avez sélectionné **Aucune connectivité** dans **Connexion réseau**.) Sélectionnez la région dans laquelle vous souhaitez créer les bureaux. Vous pouvez sélectionner une région proche de vos utilisateurs.

  Si vous avez sélectionné un nom de connexion dans **Connexion réseau**, le catalogue utilise la région de ce réseau.
- **Êtes-vous éligible aux tarifs de calcul Linux ?** (Disponible uniquement si vous avez sélectionné une image Windows.) Vous pouvez économiser de l'argent lorsque vous utilisez votre licence éligible ou Azure Hybrid Benefit.

  Avantage du bureau virtuel Azure : licences Windows 10 ou Windows 7 par utilisateur éligibles pour :

  - Microsoft 365 E3/ES
  - Avantages d'utilisation de Microsoft 365 A3/AS/Student
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Entreprise E3/E5
  - Windows 10 Education A3/A5
  - VDA Windows 10 par utilisateur

  Licence d'accès client aux services Bureau à distance par utilisateur ou par appareil avec Software Assurance pour les charges de travail Windows Server.

Avantage Azure Hybrid : licences Windows Server avec Software Assurance active ou les licences d'abonnement éligibles équivalentes. Voir https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Machine :**
  - **Type de stockage**. Disque standard (HDD), SSD standard ou SSD haut de gamme.
  - **Performances de la machine** (pour types de machines **Statique** ou **Aléatoire**) ou **Charge de travail** (pour le type de machine à sessions multiples). Les choix comprennent uniquement les options correspondant au type de génération (gen1 ou gen2) de l'image que vous avez sélectionnée.

    Si vous sélectionnez la charge de travail personnalisée, saisissez le nombre de machines et de sessions par machine dans le champ **Performances des machines**.
  - **Machines**. Le nombre de machines que vous souhaitez dans ce catalogue.
- **Schéma de dénomination des machines :** voir Schéma de dénomination des machines.
- **Nom :** saisissez un nom pour le catalogue. Ce nom figure sur le tableau de bord **Gérer**.
- **Planification de l'alimentation :** par défaut, la case **Je configurerai cette option plus tard** est cochée. Pour plus de détails, voir Programmes de gestion de l'alimentation.

6. Lorsque vous avez terminé, cliquez sur **Créer un catalogue**.

Le tableau de bord **Gérer > Déploiement rapide d'Azure** indique quand votre catalogue est créé. Citrix DaaS pour Azure crée également automatiquement un emplacement de ressources et ajoute deux Cloud Connector.

Que faire ensuite :

- Si vous ne l'avez pas déjà fait, configurez la méthode d'authentification pour que vos utilisateurs s'authentifient sur Citrix Workspace.
- Une fois le catalogue créé, ajoutez des utilisateurs au catalogue.
- Si vous avez créé un catalogue à sessions multiples, ajoutez des applications (avant ou après l'ajout d'utilisateurs).

Création de catalogues de machines appartenant à un domaine Azure AD

Vous pouvez utiliser la création personnalisée pour créer des catalogues de machines jointes à votre Azure Active Directory.

Exigences

Votre déploiement doit inclure Citrix Cloud Connector. Machine Creation Services déploie vos Cloud Connectors en fonction des informations que vous fournissez sur votre domaine Azure AD lorsque vous créez un catalogue.

Ce type de catalogue ne peut être utilisé que pour approvisionner des machines statiques ou aléatoires. Le provisionnement de machines multisessions n'est pas pris en charge pour le moment.

Ne joignez pas l'image principale à Azure AD avant de créer un catalogue. Citrix MCS joint l'image principale à Azure AD lorsque le catalogue est créé.

Utilisez la version 2203 ou supérieure du VDA.

Dans le portail Azure, attribuez le rôle IAM Virtual Machine User Login aux machines virtuelles du catalogue. Vous pouvez le faire de plusieurs manières :

- Plus sécurisé : si vous créez des machines statiques, attribuez le rôle à l'utilisateur assigné à la machine.
- Autre méthode : Attribuez le rôle sur les groupes de ressources contenant les machines virtuelles à tous les utilisateurs ayant accès au catalogue.
- Le moins sécurisé : attribuez le rôle sur les abonnements à tous les utilisateurs ayant accès au catalogue.

Définissez l'authentification Workspace pour utiliser Azure AD que vous joignez aux machines du catalogue. Pour obtenir des instructions, consultez la section Configurer l'authentification utilisateur dans Citrix Cloud.

Pour plus d'informations sur les exigences, les problèmes connus et les considérations, consultez les informations sur les configurations de VDA joints à Azure AD pures dans la configuration de VDA joints à Azure Active Directory et non joints au domaine.

Pour créer un catalogue

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
3. Sélectionnez **Gérer > Déploiement rapide Azure**.
4. Si aucun catalogue n'a encore été créé, vous êtes redirigé vers la page d'**accueil** . Sélectionnez **Mise en route**. À la fin de la page d'introduction, vous êtes redirigé vers le tableau de bord **Gérer > Azure Quick Deploy** . Sélectionnez **Créer un catalogue**. Si un catalogue a déjà été créé, vous êtes redirigé vers le tableau de bord **Gérer > Déploiement rapide Azure** . Sélectionnez **Créer un catalogue**.
5. Sélectionnez **Création personnalisée** en haut de la page, si ce n'est pas déjà fait.
6. Renseignez les champs suivants :

- **Type de machine.** Sélectionnez **Statique (bureaux personnels)** ou **Aléatoire (bureaux regroupés)**.
- **Abonnement** : Sélectionnez votre abonnement Azure.
- **Image principale.** Sélectionnez l'image du système d'exploitation à utiliser pour les machines dans les catalogues.
- **Connexion réseau.** Sélectionnez le groupe de ressources, le réseau virtuel et le sous-réseau appropriés.
- **Configuration du domaine**. Sélectionnez **Azure Active Directory** comme type de domaine. Un avertissement peut s'afficher pour vous rappeler de définir l'authentification Workspace pour utiliser cet Azure AD.

7. Suivez les étapes restantes de l'assistant pour créer le catalogue.

Paramètres d'emplacement des ressources lors de la création d'un catalogue

Lors de la création d'un catalogue, vous pouvez éventuellement configurer plusieurs paramètres d'emplacement de ressources.

Lorsque vous cliquez sur **Paramètres avancés** dans la boîte de dialogue de création de catalogue Quick Deploy, Citrix DaaS pour Azure récupère les informations d'emplacement des ressources.

- Si vous disposez déjà d'un emplacement des ressources pour le domaine et la connexion réseau sélectionnés pour le catalogue, vous pouvez l'enregistrer pour qu'il soit utilisé par le catalogue que vous créez.

  Si cet emplacement des ressources ne possède qu'un seul Cloud Connector, un autre est installé automatiquement. Vous pouvez éventuellement spécifier des paramètres avancés pour le Cloud Connector que vous ajoutez.

- Si aucun emplacement de ressources n'est configuré pour le domaine et la connexion réseau sélectionnés pour le catalogue, vous êtes invité à en configurer un.

Configuration des paramètres avancés :

- (Obligatoire uniquement lorsque l'emplacement des ressources est déjà configuré.) Le nom de l'emplacement des ressources.
- Type de connectivité externe : via le service Citrix Gateway ou depuis votre réseau d'entreprise.
- Paramètres de Cloud Connector :
  - (Disponible uniquement en cas d'utilisation d'un abonnement Azure géré par le client) Performances de la machine. Cette sélection est utilisée pour les Cloud Connectors dans l'emplacement des ressources.
  - (Disponible uniquement lorsque vous utilisez un abonnement Azure géré par le client) Groupe de ressources Azure. Cette sélection est utilisée pour les Cloud Connectors dans l'

emplacement des ressources. La valeur par défaut est le groupe de ressources utilisé pour la dernière fois par l'emplacement des ressources (le cas échéant).
- l'unité d'organisation. La valeur par défaut est la dernière unité d'organisation utilisée par l'emplacement des ressources (le cas échéant).

Lorsque vous avez terminé avec les paramètres avancés, cliquez sur **Enregistrer** pour revenir à la boîte de dialogue de création de catalogue Quick Deploy.

Une fois que vous avez créé un catalogue, plusieurs actions d'emplacement des ressources sont disponibles. Pour plus de détails, voir Actions d'emplacement des ressources.

Schéma de dénomination de machines

Pour spécifier un schéma de résolution de noms de machine lors de la création d'un catalogue à l'aide de Déploiement rapide, sélectionnez **Spécifier le modèle de résolution de noms** Utilisez entre 1 et 4 caractères génériques (caractère hash) pour indiquer où des chiffres ou des lettres séquentiels apparaissent dans le nom. Règles :

- Le schéma de dénomination doit contenir entre un et quatre caractères génériques. Tous les caractères génériques doivent être regroupés.
- Le nom complet, y compris les caractères génériques, doit comporter entre 2 et 15 caractères.
- Un nom ne peut pas inclure des blancs (espaces), des barres obliques, des barres obliques inverses, des deux-points, des astérisques, des crochets, des pipe, des virgules, des tildes, des points d'exclamation, des signes de dollar, des signes de pourcentage, des carets, des parenthèses, des accolades ou des traits de soulignement.
- Un nom ne peut pas commencer par un point.
- Un nom ne peut contenir que des chiffres.
- N'utilisez pas les caractères suivantes à la fin d'un nom : `-GATEWAY`, `-GW`, et `-TAC`.

Indiquez si les valeurs séquentielles sont des chiffres (0-9) ou des lettres (A-Z).

Par exemple, un schéma de dénomination de `PC-Sales-##` (avec **0 à 9** sélectionné) donne lieu à des comptes d'ordinateur nommés `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03`, etc.

Laissez suffisamment de place pour d'éventuels autres éléments.

- Par exemple, un schéma de dénomination comportant 2 caractères génériques et 13 autres caractères (par exemple, `MachineSales-##`) utilise le nombre maximal de caractères (15).
- Une fois que le catalogue contient 99 machines, la création suivante échoue. Le service essaie de créer une machine à trois chiffres (100), mais cette opération générerait un nom de 16 caractères. Le maximum est de 15.
- Ainsi, dans cet exemple, un nom plus court (par exemple `PC-Sales-##`) permet d'aller au-delà de 99 machines.

Si vous ne spécifiez pas de schéma de dénomination de machine, Citrix DaaS pour Azure utilise le schéma de dénomination DAS%%%%%-**-### par défaut.

- %%%%% = cinq caractères alphanumériques aléatoires correspondant au préfixe d'emplacement des ressources
- ** = deux caractères alphanumériques aléatoires pour le catalogue
- ### = trois chiffres.

Informations connexes

- Machines appartenant à un domaine et non jointes à un domaine.
- Catalogues Remote PC Access.
- Créez un catalogue dans un réseau qui utilise un serveur proxy.
- Afficher les informations du catalogue.

Remote PC Access

May 9, 2023

Introduction

> **Remarque :**
>
> Cet article explique comment configurer Remote PC Access lors de l'utilisation de l'interface de gestion Quick Deploy dans Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard for Azure service). Pour plus d'informations sur la configuration de Remote PC Access lors de l'utilisation de l'interface de gestion de la configuration complète, voir Remote PC Access.

Citrix Remote PC Access permet aux utilisateurs d'utiliser à distance des machines physiques Windows ou Linux situées au bureau. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir leur session PC de bureau.

Remote PC Access prend en charge les machines jointes à un domaine.

Différences par rapport à la fourniture de bureaux et d'applications virtuels

La fonctionnalité Remote PC Access présente plusieurs différences avec la fourniture de bureaux et d'applications virtuels :

- Un catalogue Remote PC Access contient généralement des machines physiques existantes. Il n'est donc pas nécessaire de préparer une image ou de provisionner des machines pour utiliser Remote PC Access. La fourniture de bureaux et d'applications passe généralement par des machines virtuelles (MV), et une image est utilisée comme modèle pour provisionner les machines virtuelles.
- Lorsqu'une machine d'un catalogue de pool aléatoire Remote PC Access est mise hors tension, elle n'est pas réinitialisée à l'état d'origine de l'image.
- Pour les catalogues d'attribution d'utilisateur statiques Remote PC Access, l'attribution se produit après la connexion d'un utilisateur (soit sur la machine, soit via RDP). Lors de la livraison de bureaux et d'applications, un utilisateur est attribué si une machine est disponible.

Résumé de l'installation et de la configuration

Consultez cette section avant de commencer les tâches.

1. Avant de commencer :
    a) Consultez la configuration requise et les considérations.
    b) Effectuez les tâches de préparation.
2. À partir de Citrix Cloud :
    a) Configurez un compte Citrix Cloud et abonnez-vous au service Citrix DaaS Standard pour Azure.
    b) Configurez un emplacement des ressources qui peut accéder à vos ressources Active Directory. Installez au moins deux Cloud Connectors dans l'emplacement des ressources. Les Cloud Connectors communiquent avec Citrix Cloud.

    Suivez les instructions pour créer un emplacement de ressources et y installer des Cloud Connector. Ces informations incluent la configuration système requise, la préparation et les procédures.
    c) Connectez Active Directory à Citrix Cloud.
3. Installez un Citrix Virtual Delivery Agent (VDA) sur chaque machine à laquelle les utilisateurs accèderont à distance. Les VDA communiquent avec Citrix Cloud via les Cloud Connectors dans l'emplacement des ressources.
4. Depuis l'interface de gestion Citrix DaaS pour Déploiement rapide d'Azure :
    a) Créez un catalogue Remote PC Access. Dans cette procédure, vous indiquez l'emplacement de votre emplacement de ressources et sélectionnez la méthode d'attribution de l'utilisateur.

b) Ajoutez des abonnés (utilisateurs) au catalogue, si nécessaire. Ajoutez des utilisateurs à un catalogue si le catalogue utilise la méthode d'attribution d'utilisateurs automatique statique ou de pool aléatoire. Il n'est pas nécessaire d'ajouter des utilisateurs à un catalogue préattribué statique.

5. Envoyez l'URL de l'espace de travail aux utilisateurs. À partir de leur espace de travail, les utilisateurs peuvent se connecter à leurs machines au bureau.

Configuration requise et considérations

Les références aux machines dans cette section font référence aux machines auxquelles les utilisateurs accèdent à distance.

General:

- Les machines doivent exécuter un système d'exploitation à session unique Windows 10 ou Linux (Red Hat Enterprise Linux et Ubuntu).
- La machine doit être jointe à un domaine des services de domaine Active Directory.
- Si vous êtes familier avec Remote PC Access avec Citrix Virtual Apps and Desktops, la fonctionnalité Wake-On-LAN n'est pas disponible dans Citrix DaaS pour Azure.

Réseau :

- La machine doit disposer d'une connexion réseau active. Une connexion filaire est préférable pour plus de fiabilité et de bande passante.
- Si vous utilisez le Wi-Fi :
  - Définissez les paramètres d'alimentation pour laisser la carte sans fil allumée.
  - Configurez la carte sans fil et le profil réseau pour autoriser la connexion automatique au réseau sans fil avant que l'utilisateur ouvre une session. Sinon, le VDA ne s'enregistre pas tant que l'utilisateur ne se connecte pas. La machine n'est pas disponible pour un accès à distance tant qu'un utilisateur ne se connecte pas.
  - Assurez-vous que les Cloud Connectors sont accessibles depuis le réseau Wi-Fi.

Périphériques et périphériques :

- Les appareils suivants ne sont pas pris en charge :
  - Commutateurs KVM ou autres composants qui peuvent déconnecter une session.
  - PC hybride, y compris PC et ordinateurs portables tout en un et NVIDIA Optimus.
  - Machines à double démarrage.
- Connectez le clavier et la souris directement à la machine. La connexion au moniteur ou à d' autres composants qui peuvent être désactivés ou déconnectés peut rendre ces périphériques

indisponibles. Si vous devez connecter des périphériques d'entrée à des composants tels que des moniteurs, ne les éteignez pas.

- Pour les ordinateurs portables et les appareils Surface Pro : assurez-vous que l'ordinateur portable est connecté à une source d'alimentation au lieu de fonctionner sur batterie. Configurez les options d'alimentation de l'ordinateur portable pour qu'elles correspondent à un ordinateur de bureau. Par exemple :

  - Désactivez la fonctionnalité de veille prolongée.
  - Désactivez la fonctionnalité de veille.
  - Définissez l'action de fermeture de l'écran sur **Ne rien faire**.
  - Réglez l'action *Appuyez sur le bouton d'alimentation* sur **Arrêter**.
  - Désactivez les fonctionnalités d'économie d'énergie de la carte vidéo et de la carte réseau.

  Lorsque vous utilisez une station d'accueil, vous pouvez retirer et reconnecter les ordinateurs portables. Lorsque vous retirez l'ordinateur portable, le VDA se réenregistre auprès des Cloud Connectors via Wi-Fi. Toutefois, lorsque vous reconnectez l'ordinateur portable à la station d'accueil, le VDA ne passe pas à la connexion filaire tant que vous n'avez pas déconnecté l'adaptateur sans fil. Certains périphériques proposent des fonctionnalités intégrées pour déconnecter la carte sans fil lors de l'établissement d'une connexion filaire. D'autres périphériques nécessitent des solutions personnalisées ou des utilitaires tiers pour déconnecter la carte sans fil. Prenez en compte les considérations relatives au Wi-Fi mentionnées précédemment.

  Procédez comme suit pour activer l'ancrage et le retrait pour les périphériques Remote PC Access :

  - Dans **Démarrer > Paramètres > Système > Alimentation et veille**, réglez **Veille** sur **Jamais**.
  - Dans **Gestionnaire de périphériques > Cartes réseau > Carte Ethernet**, accédez à **Gestion de l'alimentation** et désactivez **Autoriser l'ordinateur à éteindre ce périphérique pour économiser de l'énergie**. Vérifiez que l'option **Autoriser ce périphérique à sortir l'ordinateur du mode veille** est sélectionnée.

Linux VDA :

- Utilisez le VDA Linux sur des machines physiques uniquement en mode non-3D. En raison des limitations du pilote NVIDIA, l'écran local du PC ne peut pas être masqué et affiche les activités de session lorsque le mode HDX 3D est activé. L'affichage de cet écran représente un risque pour la sécurité.
- Les catalogues avec des machines Linux doivent utiliser la méthode d'attribution des utilisateurs préattribuée statique. Les catalogues avec des machines Linux ne peuvent pas utiliser les méthodes d'attribution automatique statique ou de pool aléatoire.

Considérations concernant l'espace :

- Plusieurs utilisateurs avec l'accès au même PC de bureau voient la même icône dans Citrix Workspace. Lorsqu'un utilisateur se connecte à Citrix Workspace, cette machine apparaît indisponible si elle est déjà utilisée par un autre utilisateur.

Préparer

- Décidez comment installer le VDA sur les machines. Plusieurs méthodes sont possibles :
  - Installer manuellement le VDA sur chaque machine.
  - Pousser l'installation du VDA à l'aide de la stratégie de groupe en utilisant un script.
  - Pousser l'installation du VDA à l'aide d'un outil de distribution électronique de logiciels (ESD) tel que Microsoft System Center Configuration Manager (SCCM). Pour de plus amples informations, consultez Installer les VDA à l'aide de SCCM.
- Découvrez les méthodes d'attribution des utilisateurs et décidez de la méthode que vous allez utiliser. Vous spécifiez la méthode lors de la création d'un catalogue Remote PC Access.
- Décidez comment les machines (il s'agit en fait des VDA que vous installez sur les machines) vont s'enregistrer auprès de Citrix Cloud. Un VDA doit s'enregistrer pour établir des communications avec le session broker dans Citrix Cloud.

  Les VDA s'inscrivent via les Cloud Connectors dans l'emplacement des ressources. Vous pouvez spécifier des adresses Cloud Connector lorsque vous installez un VDA ou le faire ultérieurement.

  Pour le premier enregistrement (initial) d'un VDA, Citrix recommande d'utiliser un objet de stratégie de groupe ou LGPO basé sur des règles. Après l'enregistrement initial, Citrix recommande d'utiliser la mise à jour automatique, qui est activée par défaut. En savoir plus sur l'enregistrement VDA.

Installer un VDA

Téléchargez et installez un VDA sur chaque machine physique à laquelle les utilisateurs auront accès à distance.

Télécharger un VDA

- Pour télécharger un VDA Windows :
  1. À l'aide des informations d'identification de votre compte Citrix Cloud, accédez à la page de téléchargement Citrix DaaS.
  2. Téléchargez la dernière version du VDA. Deux types de packages d'installation sont disponibles. Les valeurs de l'année et du mois dans le titre VDA varient.

- Pour télécharger un VDA Linux pour Remote PC Access, suivez les instructions de la documentation du Linux VDA.

Types de packages d'installation VDA Windows Le site de téléchargement Citrix fournit deux types de package d'installation VDA Windows pouvant être utilisés pour les machines Remote PC Access :

- Installateur VDA principal à session unique (la*version* est au format *aamm*) : `VDAWorkstationCoreSetup.exe`

  Le programme d'installation VDA principal à session unique est spécialement conçu pour Remote PC Access. Il est léger et plus facile à déployer (que les autres installateurs de VDA) sur toutes les machines du réseau. Il n'inclut pas les composants qui ne sont généralement pas nécessaires dans ces déploiements, tels que Citrix Profile Management, Machine Identity Service et la couche de personnalisation des utilisateurs.

  Toutefois, si Citrix Profile Management n'est pas installé, les affichages de Citrix Analytics for Performance et certains détails de Surveiller ne sont pas disponibles. Pour plus d'informations sur ces limitations, consultez l'article de blog Surveillance et dépannage des machines Remote PC Access.

  Si vous souhaitez des écrans d'analyse et de surveillance complets, utilisez le programme d'installation VDA complet à session unique.

- Installateur VDA complet à session unique (*version* au format *aamm*) : `VDAWorkstationSetup_release.exe`

  Bien que le programme d'installation VDA complet à session unique soit un package plus volumineux que le programme d'installation VDA principal à session unique, vous pouvez l'adapter pour installer uniquement les composants dont vous avez besoin. Par exemple, vous pouvez installer les composants prenant en charge Profile Management.

Installer un VDA Windows pour Remote PC Access de manière interactive

1. Double-cliquez sur le fichier d'installation du VDA que vous avez téléchargé.
2. Sur la page **Environnement**, sélectionnez **Activer Remote PC Access**, puis cliquez sur **Suivant**.
3. Sur la page **Delivery Controller**, sélectionnez l'une des options suivantes :
   - Si vous connaissez les adresses de vos Cloud Connectors, sélectionnez **Effectuer manuellement**. Saisissez le nom de domaine complet d'un Cloud Connector, puis cliquez sur **Ajouter**. Répétez cette opération pour les autres Cloud Connectors de votre emplacement des ressources.

- Si vous savez où vous avez installé les Cloud Connectors dans votre structure Active Directory, sélectionnez **Choisir les emplacements d'Active Directory**, puis accédez à cet emplacement. Répétez cette opération pour les autres Cloud Connectors.
- Si vous souhaitez spécifier les adresses Cloud Connector dans la stratégie de groupe Citrix, sélectionnez **Le faire plus tard (Avancé)**, puis confirmez cette sélection lorsque vous y êtes invité.

Lorsque vous avez terminé, cliquez sur **Suivant**.

4. Si vous utilisez le programme d'installation VDA complet à session unique, sur la page **Composants supplémentaires**, sélectionnez les composants que vous souhaitez installer, tels que Profile Management. (Cette page n'apparaît pas si vous utilisez le programme d'installation VDA principal à session unique.)
5. Sur la page **Fonctionnalités**, cliquez sur **Suivant**.
6. Sur la page **Pare-feu**, sélectionnez **Automatiquement** (si ce n'est pas déjà le cas). Cliquez ensuite sur **Suivant**.
7. Sur la page **Résumé**, cliquez sur **Installer**.
8. Sur la page **Diagnostiquer**, cliquez sur **Connexion**. Assurez-vous que la case à cocher est activée. Lorsque vous y êtes invité, entrez vos informations d'identification de compte Citrix. Une fois vos informations d'identification validées, cliquez sur **Suivant**.
9. Sur la page **Terminer**, cliquez sur **Terminer**.

Pour plus d'informations sur l'installation, consultez la section Installer des VDA.

Installer un VDA Windows pour Remote PC Access à l'aide d'une ligne de commandes

- Si vous utilisez le programme d'installation VDA principal à session unique : exécutez `VDAWorkstationCoreSetup.exe` et incluez les options `/quiet`, `/enable_hdx_ports` et `/enable_hdx_udp_ports`. Pour spécifier des adresses Cloud Connector, utilisez l'option `/controllers`.

  Par exemple, la commande suivante installe un VDA principal à session unique. L'application Citrix Workspace et les autres services non fondamentaux ne sont pas installés. Les noms de domaine complets de deux Cloud Connectors sont spécifiés, et les ports du Service de pare-feu Windows seront automatiquement ouverts. L'administrateur doit gérer les redémarrages.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```


- Si vous utilisez le programme d'installation VDA complet à session unique et que vous souhaitez inclure Profile Management (ou d'autres composants facultatifs) : exécutez `VDAWorkstationSetup.exe` et incluez les options `/remotepc` et `/includeadditional` . L'option `/remotepc` empêche l'installation de la plupart des composants optionnels. L'option `/includeadditional` spécifie exactement les composants que vous souhaitez installer.

  Par exemple, la commande suivante empêche l'installation de tous les composants supplémentaires facultatifs, à l'exception de Profile Management.

  ```
  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
  ```

Pour plus d'informations, consultez les options de ligne de commande pour installer un VDA.

Installer un VDA Linux

Suivez les instructions de la documentation Linux pour installer un VDA Linux de manière interactive ou en utilisant la ligne de commandes.

Créez un catalogue Remote PC Access

Un emplacement des ressources contenant au moins deux Cloud Connectors doit exister avant de pouvoir créer un catalogue.

> **Important :**
>
> Une machine ne peut appartenir qu'à un seul catalogue à la fois. Cette restriction n'est pas appliquée lorsque vous spécifiez les machines à ajouter à un catalogue. Toutefois, ignorer la restriction peut entraîner des problèmes ultérieurement.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
3. Si vous n'avez pas encore créé de catalogues, cliquez sur **Commencer** sur la page d'**accueil** du déploiement rapide. Si vous avez créé un catalogue, cliquez sur **Créer un catalogue** dans le tableau de bord **Gérer > Déploiement rapide Azure** .
4. Dans l'onglet **Remote PC Access**, sélectionnez une méthode pour attribuer des utilisateurs à des machines.

5. Saisissez un nom pour le catalogue et sélectionnez l'emplacement des ressources que vous avez créé.
6. Ajoutez des machines.
7. Cliquez sur **Créer un catalogue**.
8. Sur la page **Votre catalogue Remote PC Access est en cours de création…**, cliquez sur **Terminé**.
9. Une entrée pour le nouveau catalogue apparaît dans le tableau de bord **Gérer**.

   Une fois le catalogue créé avec succès, cliquez sur l'un des liens pour ajouter des abonnés (utilisateurs) au catalogue. Cette étape s'applique si le catalogue utilise la méthode d'attribution d'utilisateurs automatique statique ou de pool aléatoire sans attribution.

Après avoir créé un catalogue et ajouté des utilisateurs (si nécessaire), envoyez l'URL Workspace à vos utilisateurs.

Méthodes d'attribution d'utilisateurs

La méthode d'attribution d'utilisateurs que vous choisissez lors de la création d'un catalogue indique comment les utilisateurs sont affectés aux machines.

- Attribution **automatique statique :** l'attribution d'un utilisateur se produit lorsque celui-ci se connecte à la machine (sans utiliser Citrix, par exemple, en personne ou via RDP), après l'installation d'un VDA sur la machine. Plus tard, si d'autres utilisateurs se connectent à cette machine (sans Citrix), ils sont également attribués. Un seul utilisateur peut utiliser la machine à la fois. Il s'agit d'une configuration typique pour les employés de bureau ou les employés travaillant en équipe qui partagent un ordinateur.

  Cette méthode est prise en charge pour les machines Windows. Elle ne peut pas être utilisée avec des machines Linux.

- **Préattribué statique :** les utilisateurs sont préattribués aux machines. (Cela est généralement configuré en téléchargeant un fichier CSV contenant le mappage de l'utilisateur à la machine.) Il n'est pas nécessaire d'ouvrir une session utilisateur pour établir une attribution après l'installation du VDA. Il n'est pas non plus nécessaire d'attribuer des utilisateurs au catalogue une fois qu'il a été créé. C'est la meilleure option pour les employés de bureau.

  Cette méthode est prise en charge pour les machines Windows et Linux.

- **Pool aléatoire sans attribution :** les utilisateurs sont attribués de façon aléatoire à une machine disponible. Un seul utilisateur peut utiliser la machine à la fois. C'est idéal pour les laboratoires informatiques en milieu scolaire.

Cette méthode est prise en charge pour les machines Windows. Elle ne peut pas être utilisée avec des machines Linux.

Méthodes d'ajout de machines à un catalogue

N'oubliez pas : un VDA doit être installé sur chaque machine.

Lorsque vous créez ou modifiez un catalogue, vous pouvez ajouter des machines à un catalogue de trois manières :

- Sélectionnez des comptes de machines un par un.
- Sélectionnez des unités d'organisation.
- Ajoutez en vrac à l'aide d'un fichier CSV. Vous pouvez utiliser un modèle pour le fichier CSV.

Ajouter des noms de machines

Cette méthode ajoute des comptes de machines un par un.

1. Sélectionnez votre domaine.
2. Recherchez le compte de machine.
3. Cliquez sur **Ajouter**.
4. Répétez l'opération pour ajouter d'autres machines.
5. Lorsque vous avez fini d'ajouter des machines, cliquez sur **Terminé**.

Ajouter des unités d'organisation

Cette méthode ajoute des comptes de machine en fonction de l'unité d'organisation où ils se trouvent.
Lorsque vous sélectionnez des unités d'organisation, choisissez des unités d'organisation de niveau inférieur pour une plus grande granularité. Si une telle granularité n'est pas requise, vous pouvez choisir des unités d'organisation de plus haut niveau.

Par exemple, dans le cas de `Bank`/`Officers`/`Tellers`, sélectionnez `Tellers` pour une plus grande granularité. Sinon, vous pouvez sélectionner `Officers` ou `Bank` en fonction des besoins.

Le déplacement ou la suppression d'unités d'organisation après leur attribution à un catalogue Remote PC Access affecte les associations de VDA et entraîne des problèmes avec les attributions futures. Assurez-vous que votre plan de modification Active Directory tient compte des mises à jour des affectations d'unité d'organisation pour les catalogues.

Pour ajouter des unités d'organisation :

1. Sélectionnez votre domaine.

2. Sélectionnez les unités d'organisation qui contiennent les comptes de machines que vous souhaitez ajouter.
3. Indiquez à l'aide de la case à cocher si vous souhaitez inclure des sous-dossiers dans vos sélections.
4. Lorsque vous avez fini de sélectionner des unités d'organisation, cliquez sur **Terminé**.

Ajouter en vrac

1. Cliquez sur **Télécharger le modèle CSV**.
2. Dans le modèle, ajoutez les informations du compte de machine (jusqu'à 100 entrées). Le fichier CSV peut également contenir les noms des utilisateurs attribués à chaque machine.
3. Enregistrez le fichier.
4. Faites glisser le fichier sur la page **Ajouter des machines en vrac** ou accédez au fichier.
5. Un aperçu du contenu du fichier s'affiche. Si ce n'est pas le fichier souhaité, vous pouvez créer un autre fichier, puis le faire glisser ou y accéder.
6. Lorsque vous avez terminé, cliquez sur **Terminé**.

Gérer les catalogues Remote PC Access

Pour afficher ou modifier les informations de configuration d'un catalogue Remote PC Access, sélectionnez le catalogue dans le tableau de bord **Gérer > Déploiement rapide d'Azure** (cliquez n'importe où dans son entrée).

- Dans l'onglet **Détails**, vous pouvez ajouter ou supprimer des machines.
- Dans l'onglet **Abonnés**, vous pouvez ajouter ou supprimer des utilisateurs.
- Dans l'onglet **Machines**, vous pouvez :
  - Ajouter ou supprimer des machines : bouton **Ajouter ou supprimer des machines**.
  - Modifier les attributions d'utilisateurs : icône de corbeille **Supprimer attribution**, **Modifier l'attribution de machine** dans le menu des points de suspension.
  - Vous voyez les machines enregistrées. Mettez les machines en mode de maintenance ou hors du mode de maintenance.

Abonnements Azure

December 28, 2023

Introduction

Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure service) prend en charge à la fois les abonnements Azure gérés par Citrix et vos propres abonnements Azure gérés par le client.

- Pour utiliser vos propres abonnements Azure, vous devez d'abord importer (ajouter) un ou plusieurs de ces abonnements dans Citrix DaaS pour Azure. Cette action permet à Citrix DaaS pour Azure d'accéder à vos abonnements Azure.
- L'utilisation d'un abonnement Azure géré par Citrix ne nécessite aucune configuration d'abonnement. Toutefois, pour avoir un abonnement Citrix Managed Azure disponible, vous devez avoir commandé le Fonds de consommation Citrix Azure (en plus de la norme Citrix DaaS pour Azure).

Lorsque vous créez un catalogue ou créez une image, vous choisissez parmi les abonnements Azure disponibles.

Certaines fonctionnalités de service diffèrent selon que les machines sont dans un abonnement Citrix Managed Azure ou dans votre propre abonnement Azure.

Abonnement Azure géré par Citrix	Votre propre abonnement Azure
Prend en charge les machines jointes au domaine ou n'appartenant pas au domaine.	Prend en charge uniquement les machines jointes au domaine.
Prend en charge les catalogues à création rapide et à création personnalisée.	Prend en charge uniquement les catalogues de création personnalisés.
Toujours disponible (et c'est la sélection d'abonnement par défaut) lors de la création de catalogues et d'images.	Vous devez ajouter l'abonnement Azure à Citrix DaaS pour Azure avant de créer un catalogue.
Pour l'authentification utilisateur, prend en charge Azure Active Directory géré par Citrix ou votre propre Active Directory.	Peut connecter votre propre Active Directory et Azure Active Directory.
Les options de connexion réseau incluent **Aucune connectivité**.	Les options de connexion réseau incluent uniquement vos propres réseaux virtuels.
Lorsque vous utilisez l'appairage de réseaux virtuels Azure pour vous connecter à vos ressources, vous devez créer une connexion homologue de réseau virtuel dans Citrix DaaS pour Azure.	Sélectionnez un réseau virtuel existant.

Abonnement Azure géré par Citrix	Votre propre abonnement Azure
Lorsque vous importez une image depuis Azure, vous spécifiez l'URI de l'image.	Lorsque vous importez une image, vous pouvez sélectionner un disque dur virtuel ou parcourir le stockage dans l'abonnement Azure.
Peut créer une machine bastion dans l'abonnement Azure du client pour résoudre les problèmes de machines.	Pas besoin de créer un bastion machine car vous pouvez déjà accéder aux machines de votre abonnement.

Afficher les abonnements

Pour afficher les détails de l'abonnement, dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Abonnements cloud** sur la droite. Cliquez ensuite sur une entrée d'abonnement.

- La page **Détails** inclut le nombre de machines, ainsi que les numéros et les noms des catalogues et des images de l'abonnement.
- La page **Emplacements des ressources** répertorie les emplacements de ressources où l'abonnement est utilisé.

Ajouter des abonnements Azure gérés par le client

Pour utiliser un abonnement Azure géré par le client, vous devez l'ajouter à Citrix DaaS Standard pour Azure avant de créer un catalogue ou une image qui utilise cet abonnement. Deux options s'offrent à vous lorsque vous ajoutez vos abonnements Azure :

- **Si vous êtes administrateur général de l'annuaire et que vous disposez des privilèges de propriétaire pour l'abonnement :** il vous suffit de vous authentifier auprès de votre compte Azure.
- **Si vous n'êtes pas administrateur général et que vous disposez de privilèges de propriétaire sur l'abonnement :** avant d'ajouter l'abonnement à Citrix DaaS pour Azure, créez une application Azure dans votre Azure AD, puis ajoutez-la en tant que contributeur de l'abonnement. Lorsque vous ajoutez cet abonnement à Citrix DaaS pour Azure, vous fournissez des informations pertinentes sur l'application.

Ajouter des abonnements Azure gérés par le client si vous êtes administrateur général

Cette tâche nécessite des privilèges d'administrateur global pour l'annuaire et des privilèges de propriétaire pour l'abonnement.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Abonnements cloud** sur la droite.
2. Cliquez sur **Ajouter un abonnement Azure**.
3. Sur la page **Ajouter des abonnements**, cliquez sur **Ajouter votre abonnement Azure**.
4. Sélectionnez le bouton qui permet à Citrix DaaS pour Azure d'accéder à vos abonnements Azure en votre nom.
5. Cliquez sur **Authentifier le compte Azure**. Vous accédez à la page de connexion Azure.
6. Saisissez vos informations d'identification Azure.
7. Vous êtes automatiquement redirigé vers Citrix DaaS pour Azure. La page **Ajouter un abonnement** répertorie les abonnements Azure découverts. Utilisez la zone de recherche pour filtrer la liste, si nécessaire. Sélectionnez un ou plusieurs abonnements. Lorsque vous avez terminé, cliquez sur **Ajouter des abonnements**.
8. Confirmez que vous souhaitez ajouter les abonnements sélectionnés.

Les abonnements Azure que vous avez sélectionnés sont répertoriés lorsque vous développez **Abonnements**. Les abonnements ajoutés peuvent être sélectionnés lors de la création d'un catalogue ou d'une image.

Ajoutez des abonnements Azure gérés par le client si vous n'êtes pas administrateur global

L'ajout d'un abonnement Azure lorsque vous n'êtes pas administrateur global est un processus en deux étapes :

- Avant d'ajouter un abonnement à Citrix DaaS pour Azure, créez une application dans Azure AD, puis ajoutez-la en tant que contributeur de l'abonnement.
- Ajoutez l'abonnement à Citrix DaaS pour Azure, en utilisant les informations relatives à l'application que vous avez créée dans Azure.

Créer une application dans Azure Active Directory et l'ajouter en tant que contributeur

1. Enregistrez une nouvelle application dans Azure Active Directory :

   a) À partir d'un navigateur, accédez à https://portal.azure.com.

   b) Dans le menu supérieur gauche, sélectionnez **Azure Active Directory**.

   c) Dans la liste **Gérer**, cliquez sur **Inscriptions d'applications**.

   d) Cliquez sur **+ Nouvelle inscription**.

   e) Sur la page **Enregistrer une application**, fournissez les informations suivantes :

      - **Nom :** saisissez le nom de la connexion
      - **Type d'application :** sélectionnez une **application Web/API**

- **URI de redirection :** laissez ce champ vide

f) Cliquez sur **Créer**.

2. Créez la clé d'accès secrète de l'application et ajoutez l'attribution de rôle :

a) Dans la procédure précédente, sélectionnez **Enregistrement de l'application** pour afficher les détails.

b) Notez l'**ID d'application** et l'**ID de répertoire**. Vous l'utiliserez ultérieurement lors de l'ajout de votre abonnement à Citrix DaaS pour Azure.

c) Sous **Gérer**, sélectionnez **Certificats et secrets**.

d) Sur la page **Clés secrètes clients**, sélectionnez **+ Nouvelle clé secrète client**.

e) Sur la page **Ajouter une clé secrète client**, fournissez une description et sélectionnez un intervalle d'expiration. Cliquez ensuite sur **Ajouter**.

f) Notez la valeur de la clé secrète client. Vous l'utiliserez ultérieurement lors de l'ajout de votre abonnement à Citrix DaaS pour Azure.

g) Sélectionnez l'abonnement Azure que vous souhaitez associer (ajouter) à Citrix DaaS pour Azure, puis cliquez sur **Contrôle d'accès (IAM)**.

h) Dans la zone **Ajouter une attribution de rôle**, cliquez sur **Ajouter**.

i) Dans l'onglet **Ajouter une attribution de rôle**, sélectionnez les éléments suivants :

- **Rôle :** contributeur
- **Attribuer l'accès à :** utilisateur, groupe ou principal du service Azure Active Directory
- **Sélectionnez :** nom de l'application Azure que vous avez créée précédemment.

j) Cliquez sur **Enregistrer**.

Ajoutez votre abonnement à Citrix DaaS pour Azure Vous aurez besoin de l'ID d'application, de l'ID d'annuaire et de la valeur secrète client de l'application que vous avez créée dans Azure AD.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Abonnements cloud** sur la droite.
2. Cliquez sur **Ajouter un abonnement Azure**.
3. Sur la page **Ajouter des abonnements**, cliquez sur **Ajouter vos abonnements Azure**.
4. Sélectionnez **J'ai une application Azure avec un rôle de contributeur pour l'abonnement**
5. Saisissez l'ID de locataire (ID de répertoire), l'ID client (ID d'application) et la clé secrète client de l'application que vous avez créée dans Azure.
6. Cliquez sur **Sélectionnez votre abonnement**, puis sélectionnez l'abonnement que vous souhaitez.

Plus tard, à partir de la page **Détails** de l'abonnement dans le tableau de bord Citrix DaaS pour Azure, vous pouvez mettre à jour le secret client ou remplacer l'application Azure à partir du menu de points de suspension.

Si Citrix DaaS pour Azure ne peut pas accéder à un abonnement Azure après son ajout, plusieurs fonctions de gestion de l'alimentation du catalogue et les actions individuelles de la machine ne sont pas autorisées. Un message permet d'ajouter à nouveau l'abonnement. Si l'abonnement a été initialement ajouté à l'aide d'une application Azure, vous pouvez remplacer l'application Azure.

Ajouter des abonnements Azure gérés par Citrix

Un abonnement Citrix Managed Azure prend en charge le nombre de machines indiqué dans Limites. (Dans ce contexte, les *machines* font référence aux machines virtuelles sur lesquelles un VDA Citrix est installé. Ces machines fournissent des applications et des bureaux aux utilisateurs. Il n'inclut pas d'autres machines dans un emplacement de ressources, telles que Cloud Connectors.)

Si votre abonnement Azure géré par Citrix est susceptible d'atteindre sa limite bientôt et que vous disposez de suffisamment de licences Citrix, vous pouvez demander un autre abonnement Azure géré par Citrix. Le tableau de bord contient une notification lorsque vous vous rapprochez de la limite.

Vous ne pouvez pas créer de catalogue (ou ajouter des machines à un catalogue) si le nombre total de machines pour tous les catalogues qui utilisent cet abonnement Citrix Managed Azure dépasse la valeur indiquée dans Limites.

Par exemple, supposons une limite hypothétique de 1 000 machines par abonnement Azure géré par Citrix.

- Supposons que vous ayez deux catalogues (`Cat1` et `Cat2`) qui utilisent le même abonnement Azure géré par Citrix. `Cat1` contient actuellement 500 machines et `Cat2` en contient 250.
- Au fur et à mesure que vous planifiez les besoins futurs en capacité, vous ajoutez 200 machines à `Cat2`. L'abonnement Azure géré par Citrix prend désormais en charge 950 machines (500 dans `Cat 1` et 450 dans `Cat 2`). Le tableau de bord indique que l'abonnement est proche de sa limite.
- Lorsque vous avez besoin de 75 machines supplémentaires, vous ne pouvez pas utiliser cet abonnement pour créer un catalogue avec 75 machines (ou ajouter 75 machines à un catalogue existant). Cela dépasserait la limite d'abonnement. Au lieu de cela, vous demandez un autre abonnement Azure géré par Citrix. Vous pouvez ensuite créer un catalogue en utilisant cet abonnement.

Lorsque vous disposez de plusieurs abonnements Azure gérés par Citrix :

- Rien n'est partagé entre ces abonnements.

- Chaque abonnement porte un nom unique.
- Vous pouvez choisir parmi les abonnements Azure gérés par Citrix (et tous les abonnements Azure gérés par le client que vous avez ajoutés) lorsque :
  - vous créez un catalogue ;
  - vous créez ou importez une image ;
  - vous créez un peering de réseau virtuel ou une connexion SD-WAN.

Exigence :

- Vous devez disposer de suffisamment de licences Citrix pour justifier l'ajout d'un autre abonnement Azure géré par Citrix. Pour reprendre l'exemple hypothétique précédent, si vous disposez de 2 000 licences Citrix en prévision du déploiement d'au moins 1 500 machines via des abonnements gérés par Citrix, vous pouvez ajouter un autre abonnement Azure géré par Citrix.

Pour ajouter un abonnement Azure géré par Citrix :

1. Contactez votre représentant Citrix pour demander un autre abonnement Azure géré par Citrix. Vous êtes averti lorsque vous pouvez continuer.
2. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Abonnements cloud** sur la droite.
3. Cliquez sur **Ajouter un abonnement Azure**.
4. Sur la page **Ajouter des abonnements**, cliquez sur **Ajouter un abonnement Citrix Managed Azure**.
5. Sur la page **Ajouter un abonnement géré Citrix**, cliquez sur **Ajouter un abonnement** en bas de la page.

Si vous êtes averti qu'une erreur s'est produite lors de la création d'un abonnement Azure géré par Citrix, contactez le support Citrix.

Supprimer les abonnements Azure

Pour supprimer un abonnement Azure, vous devez d'abord supprimer tous les catalogues et images qui l'utilisent.

Si vous possédez un ou plusieurs abonnements Azure gérés par Citrix, vous ne pouvez pas tous les supprimer. Vous devez en conserver au moins un.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Abonnements cloud** sur la droite.
2. Cliquez sur l'entrée d'abonnement.
3. Dans l'onglet **Détails**, cliquez sur **Supprimer l'abonnement**.
4. Cliquez sur **Authentifier le compte Azure**. Vous accédez à la page de connexion Azure.

5. Saisissez vos informations d'identification Azure.
6. Vous êtes automatiquement redirigé vers Citrix DaaS pour Azure. Confirmez la suppression dans les cases à cocher, puis cliquez sur **Oui, Supprimer l'abonnement**.

Connexions réseau

May 9, 2023

Introduction

Cet article fournit des informations sur plusieurs scénarios de déploiement lors de l'utilisation d'un abonnement Citrix Managed Azure.

Lors de la création d'un catalogue, vous indiquez si et comment les utilisateurs accèdent aux emplacements et aux ressources de leur réseau local d'entreprise à partir de leurs postes de travail et applications Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure).

Lorsque vous utilisez un abonnement Azure géré par Citrix, les choix sont les suivants :

- Aucune connectivité
- Peering de réseau virtuel Azure
- SD-WAN

Lorsque vous utilisez l'un de vos propres abonnements Azure gérés par le client, il n'est pas nécessaire de créer une connexion à Citrix DaaS pour Azure. Il vous suffit d'ajouter l'abonnement Azure à Citrix DaaS pour Azure.

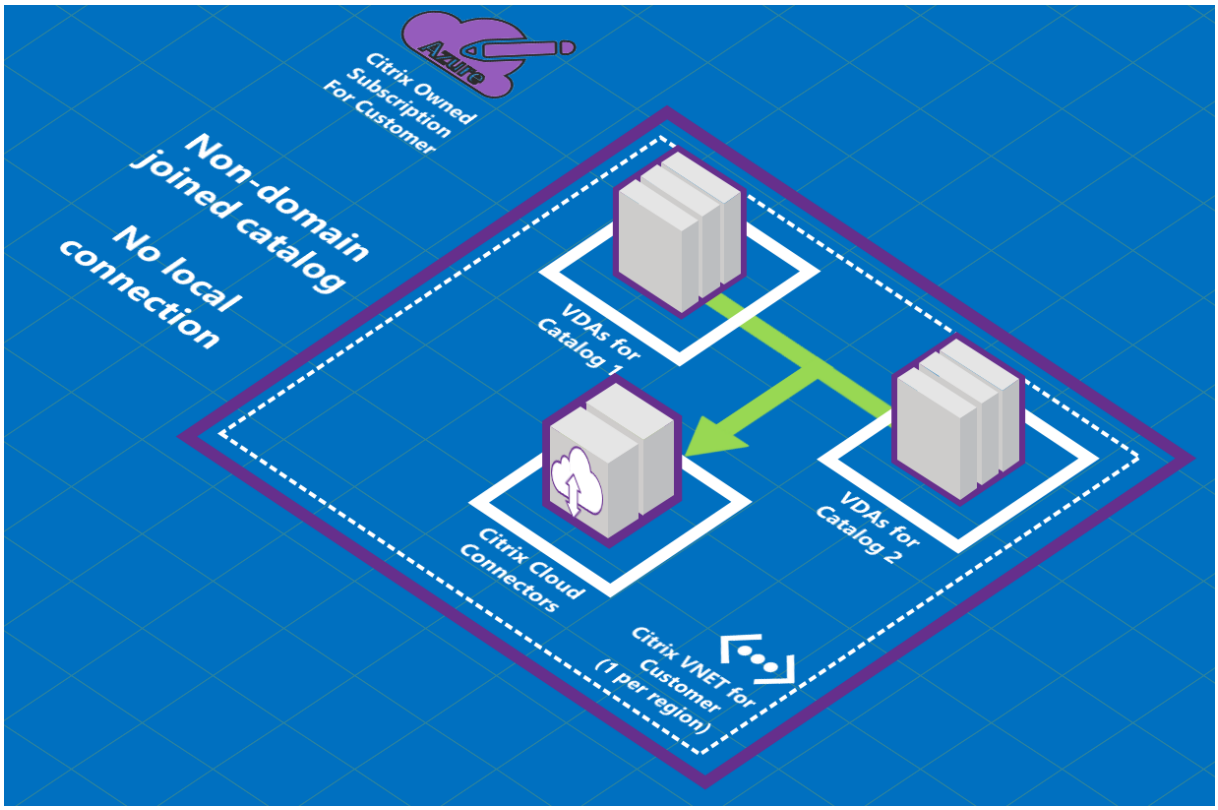
Vous ne pouvez pas modifier le type de connexion d'un catalogue une fois le catalogue créé.

Configuration requise pour toutes les connexions réseau

- Lors de la création d'une connexion, vous devez disposer d'entrées de serveur DNS valides.
- Lorsque vous utilisez Secure DNS ou un fournisseur DNS tiers, vous devez ajouter la plage d'adresses allouée pour une utilisation par Citrix DaaS pour Azure aux adresses IP du fournisseur DNS dans la liste verte. Cette plage d'adresses est spécifiée lorsque vous créez une connexion.
- Toutes les ressources de service qui utilisent la connexion (machines jointes à un domaine) doivent pouvoir atteindre votre serveur Network Time Protocol (NTP), afin d'assurer la synchronisation de l'heure.

Aucune connectivité

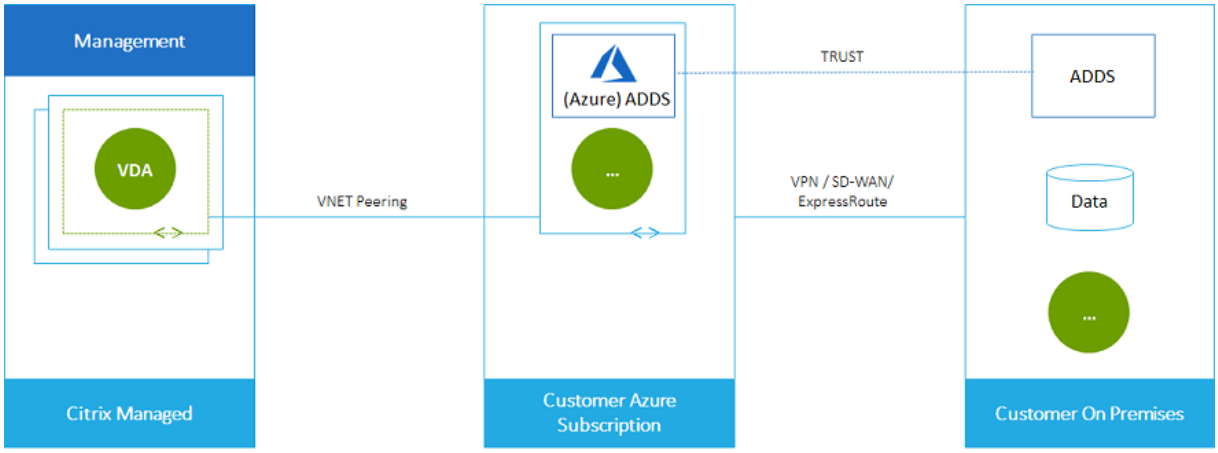
Lorsqu'un catalogue est configuré avec **Aucune connectivité**, l'utilisateur ne peut pas accéder aux ressources sur son réseau local ni sur d'autres réseaux. Il s'agit du seul choix lors de la création d'un catalogue à l'aide de la création rapide.



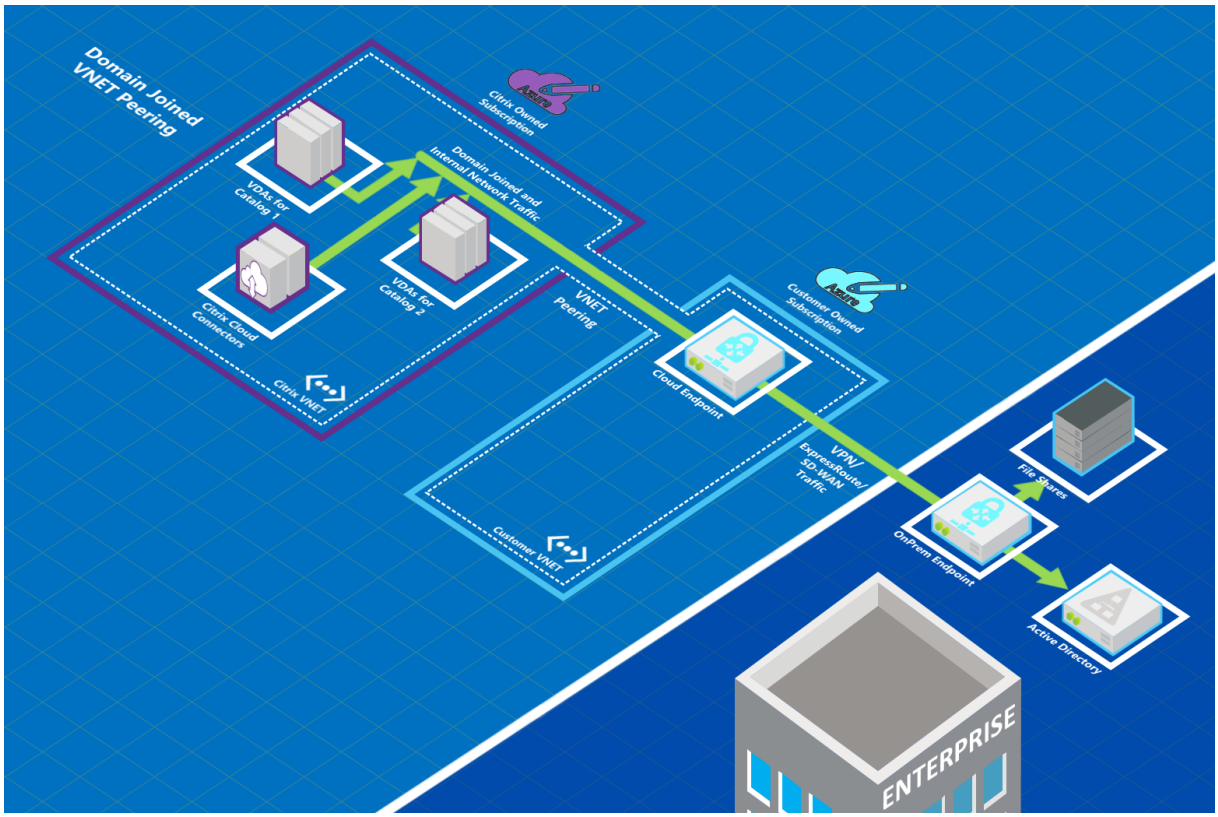
À propos des connexions de peering de réseau virtuel Azure

L'appairage de réseaux virtuels connecte de manière transparente deux réseaux virtuels Azure (VNET) : le vôtre et le réseau virtuel Citrix DaaS pour Azure. Le peering permet également aux utilisateurs d'accéder à des fichiers et autres éléments à partir de vos réseaux locaux.

Comme le montre le graphique suivant, vous créez une connexion à l'aide du peering de réseau virtuel Azure depuis l'abonnement Azure géré par Citrix vers le réseau virtuel dans l'abonnement Azure de votre entreprise.



Voici une autre illustration du peering de réseau virtuel.



Les utilisateurs peuvent accéder à leurs ressources réseau locales (telles que les serveurs de fichiers) en rejoignant le domaine local lorsque vous créez un catalogue. (C'est-à-dire que vous rejoignez le domaine AD qui contient les partages de fichiers et les autres ressources nécessaires.) Votre abonnement Azure se connecte à ces ressources (dans les graphiques, à l'aide d'un VPN ou d'Azure ExpressRoute). Lorsque vous créez le catalogue, vous fournissez les informations d'identification du domaine, de l'unité d'organisation et du compte.

> **Important :**
>
> - Découvrez l'appairage de réseaux virtuels avant de l'utiliser dans Citrix DaaS pour Azure.
> - Créez une connexion de peering de réseau virtuel avant de créer un catalogue qui l'utilise.

Itinéraires personnalisés de peering de réseau virtuel Azure

Les itinéraires personnalisés ou définis par l'utilisateur remplacent les itinéraires système par défaut d'Azure pour diriger le trafic entre les machines virtuelles dans un peering de réseau virtuel, les réseaux locaux et sur Internet. Vous pouvez utiliser des routes personnalisées s'il existe des réseaux auxquels les ressources Citrix DaaS pour Azure sont censées accéder mais qui ne sont pas directement connectées via l'appairage de réseaux virtuels. Par exemple, vous pouvez créer un itinéraire personnalisé qui force le trafic via une appliance réseau vers Internet ou vers un sous-réseau local.

Pour utiliser des itinéraires personnalisés :

- Vous devez disposer d'une passerelle réseau virtuelle Azure ou d'une appliance réseau telle que Citrix SD-WAN dans votre environnement Citrix DaaS pour Azure.
- Lorsque vous ajoutez des itinéraires personnalisés, vous devez mettre à jour les tables de routage de votre entreprise avec les informations du réseau virtuel de destination Citrix DaaS pour Azure afin de garantir une connectivité de bout en bout.
- Les itinéraires personnalisés sont affichés dans Citrix DaaS pour Azure dans l'ordre dans lequel ils sont entrés. Cet ordre d'affichage n'affecte pas l'ordre dans lequel Azure sélectionne les itinéraires.

Avant d'utiliser des itinéraires personnalisés, consultez l'article Microsoft Routage du trafic de réseau virtuel pour en savoir plus sur l'utilisation d'itinéraires personnalisés, les types de sauts suivants et la façon dont Azure sélectionne les itinéraires pour le trafic sortant.

Vous pouvez ajouter des itinéraires personnalisés lorsque vous créez une connexion d'appairage de réseau virtuel Azure ou à des connexions existantes dans votre environnement Citrix DaaS pour Azure. Lorsque vous êtes prêt à utiliser des itinéraires personnalisés avec votre peering de réseau virtuel, reportez-vous aux sections suivantes de cet article :

- Pour les itinéraires personnalisés avec de nouveaux peerings de réseaux virtuels Azure : créez une connexion de peering de réseau virtuel Azure
- Pour les itinéraires personnalisés avec des peerings de réseaux virtuels Azure existants : gérez des itinéraires personnalisés pour les connexions de peerings de réseaux virtuels Azure existantes

Configuration requise et préparation du peering de réseau virtuel Azure

- Informations d'identification pour le propriétaire d'un abonnement Azure Resource Manager. Il doit s'agir d'un compte Azure Active Directory. Citrix DaaS pour Azure ne prend pas en charge les autres types de comptes, tels que live.com ou les comptes Azure AD externes (dans un autre locataire).
- Un abonnement Azure, un groupe de ressources et un réseau virtuel.
- Configurez les itinéraires réseau Azure afin que les VDA de l'abonnement Azure géré par Citrix puissent communiquer avec vos emplacements réseau.
- Ouvrez les groupes de sécurité réseau Azure depuis votre réseau virtuel vers la plage IP spécifiée.
- **Active Directory :** dans les scénarios dans lesquels vous êtes joints à un domaine, nous vous recommandons d'utiliser un type de services Active Directory dans le réseau virtuel associé. Cela tire parti des caractéristiques de faible latence de la technologie de peering de réseau virtuel Azure.

  Par exemple, la configuration peut inclure Azure Active Directory Domain Services (AADDS), une machine virtuelle de contrôleur de domaine dans le réseau virtuel ou Azure AD Connect à votre Active Directory local.

  Après avoir activé AADDS, vous ne pouvez pas déplacer votre domaine géré vers un autre réseau virtuel sans supprimer le domaine géré. Il est donc important de sélectionner le réseau virtuel approprié pour activer votre domaine géré. Avant de continuer, consultez l'article Microsoft Considérations relatives à la conception du réseau virtuel et options de configuration pour Azure Active Directory Domain Services.
- **Plage IP du réseau virtuel :** lors de la création de la connexion, vous devez fournir un espace d'adressage de routage CIDR disponible (adresse IP et préfixe réseau) unique parmi les ressources réseau et les réseaux virtuels Azure connectés. Il s'agit de la plage d'adresses IP attribuée aux machines virtuelles au sein du réseau virtuel pair Citrix DaaS pour Azure.

  Assurez-vous de spécifier une plage IP qui ne chevauche aucune adresse que vous utilisez dans vos réseaux Azure et locaux.

  - Par exemple, si votre réseau virtuel Azure possède un espace d'adressage 10.0.0.0 /16, créez la connexion d'appairage de réseau virtuel dans Citrix DaaS pour Azure comme 192.168.0.0 /24.
  - Dans cet exemple, la création d'une connexion de peering avec une plage IP 10.0.0.0 /24 serait considérée comme une plage d'adresses qui se chevauchent.

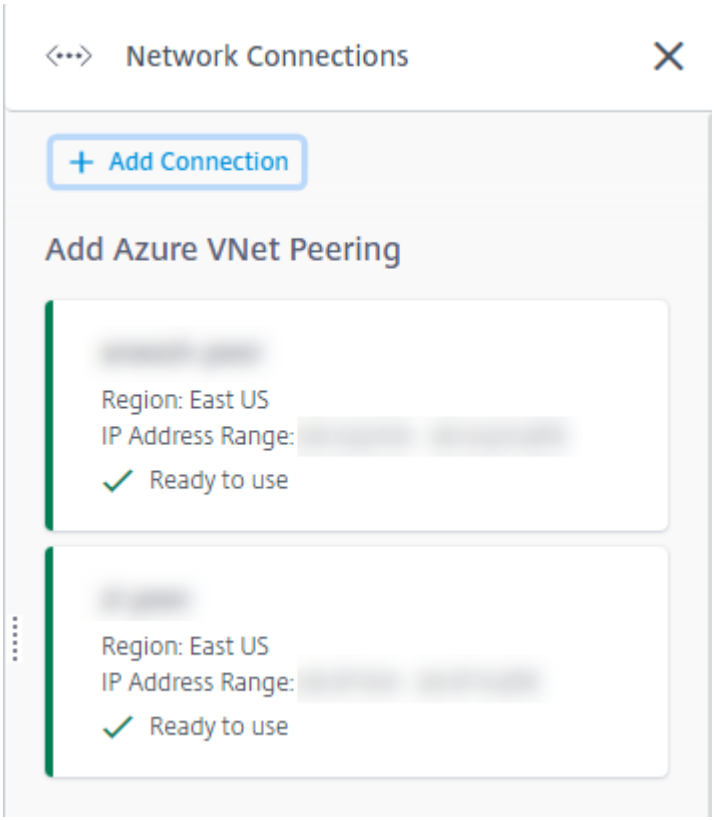
  Si les adresses se chevauchent, la connexion de peering de réseau virtuel est susceptible de ne pas être créée correctement. Cela ne fonctionne pas non plus correctement pour les tâches d'administration de site.

Pour en savoir plus sur le peering de réseau virtuel, consultez les articles Microsoft suivants.

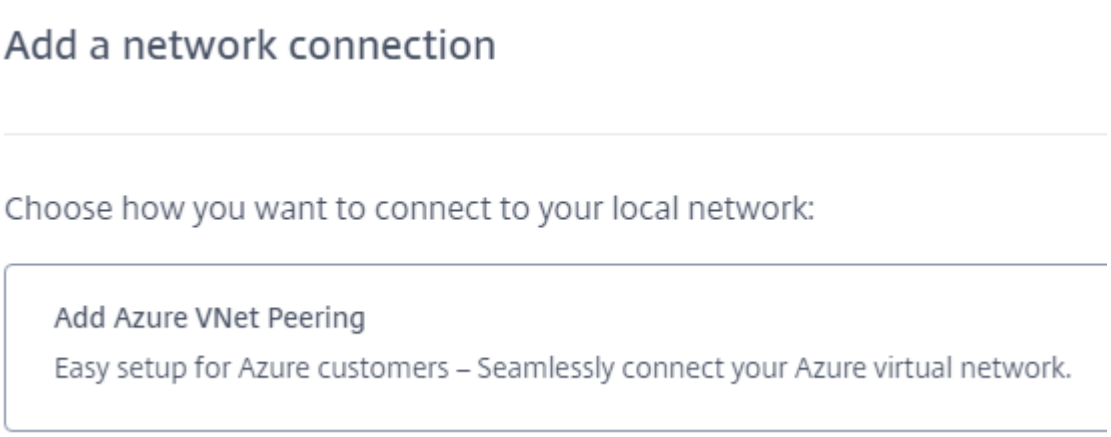
- Peering de réseau virtuel
- Passerelle VPN Azure
- Créer une connexion de site à site dans le portail Azure
- FAQ sur la passerelle VPN (recherchez « chevauchement »)

Création d'une connexion de peering de réseau virtuel Azure

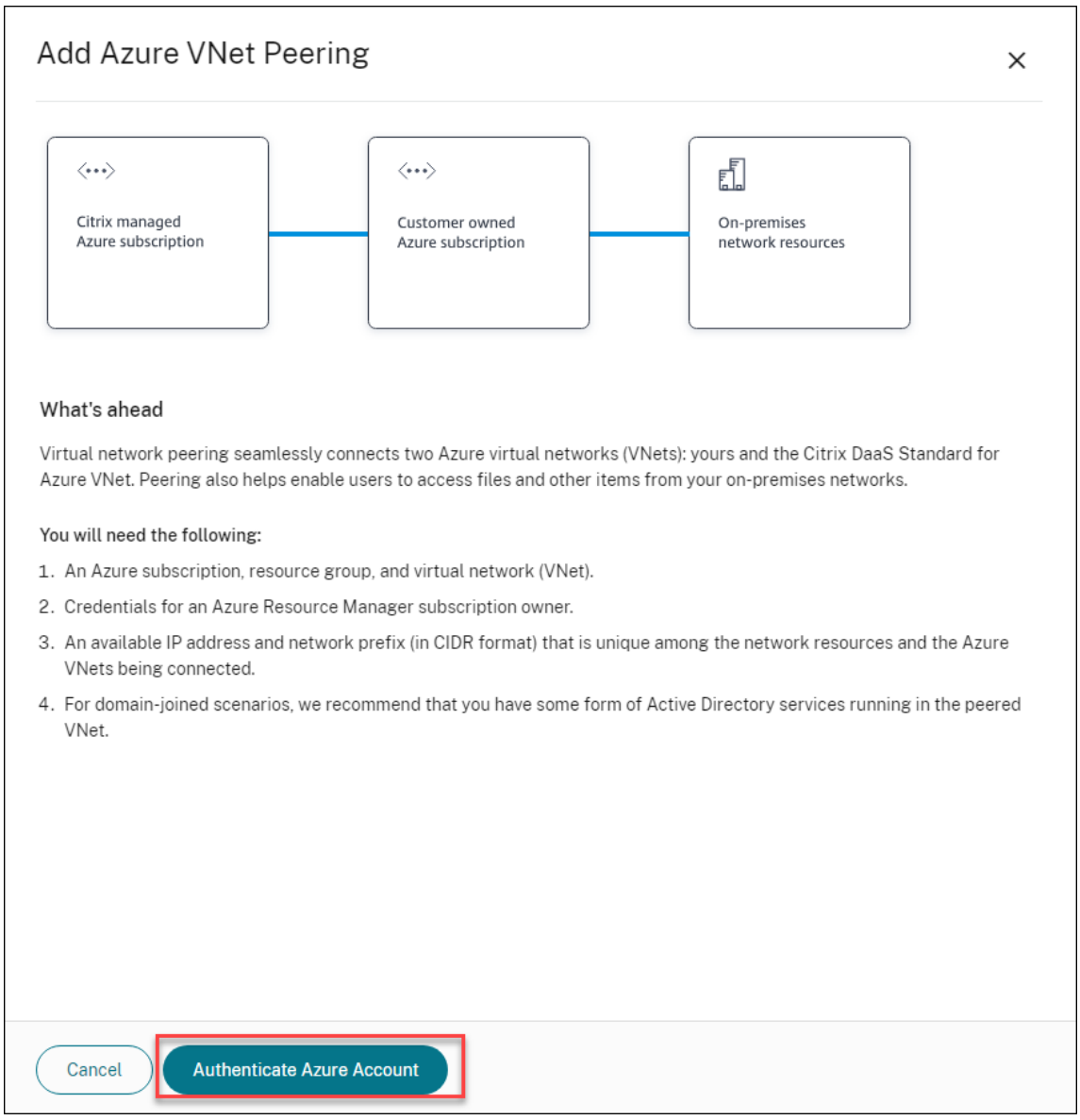
1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite. Si vous avez déjà configuré des connexions, elles sont répertoriées.



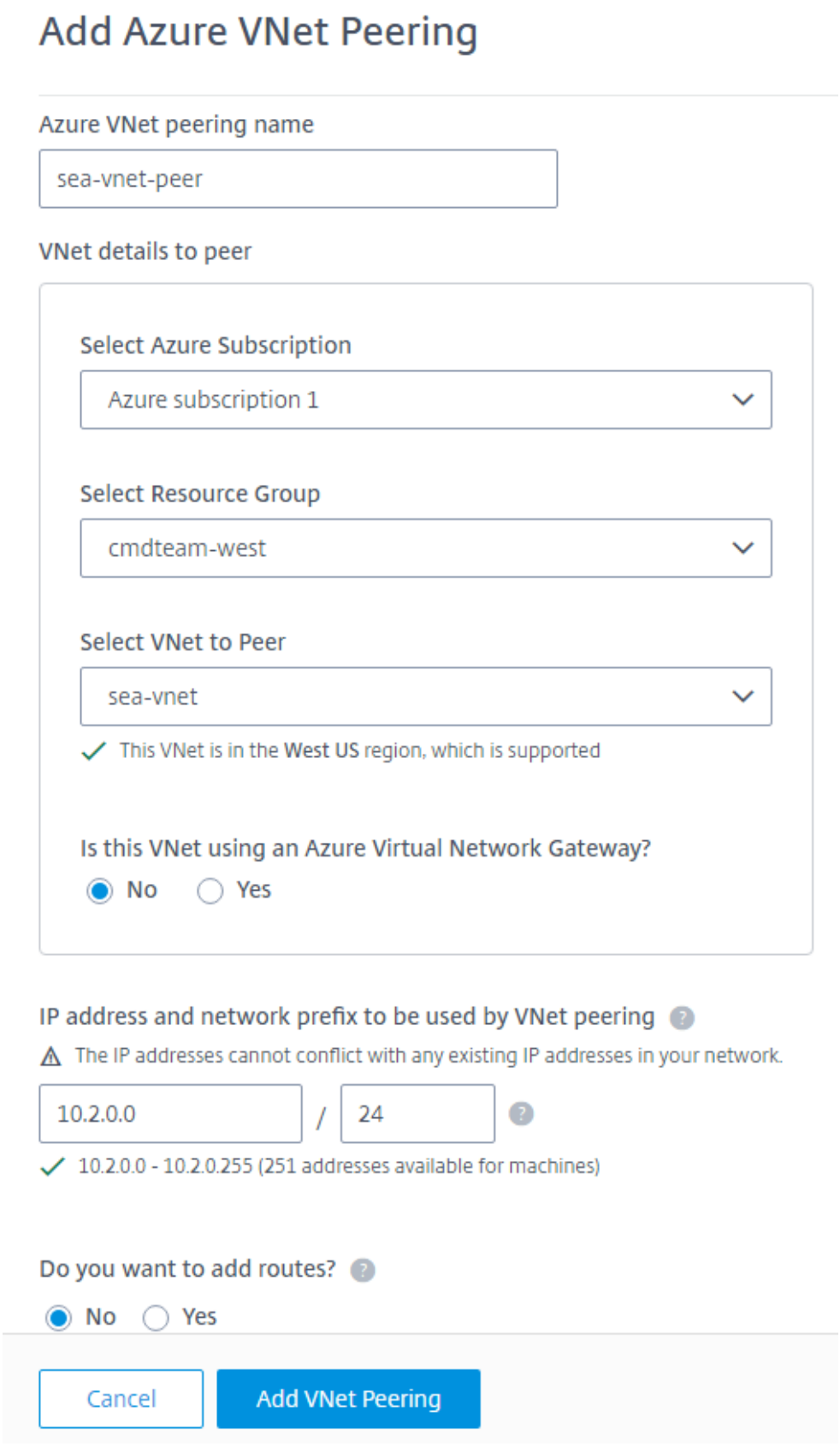
2. Cliquez sur **Ajouter une connexion**.
3. Cliquez n'importe où dans la zone **Ajouter peering de réseau virtuel Azure**.



4. Cliquez sur **Authentifier le compte Azure**.



5. Citrix DaaS pour Azure vous dirige automatiquement vers la page de connexion Azure pour authentifier vos abonnements Azure. Une fois que vous êtes connecté à Azure (avec les informations d'identification du compte administrateur général) et que vous avez accepté les termes, vous revenez à la boîte de dialogue des détails de création de connexion.



6. Saisissez un nom pour l'homologue de réseau virtuel Azure.
7. Sélectionnez l'abonnement Azure, le groupe de ressources et le réseau virtuel à homologue.
8. Indiquez si le réseau virtuel sélectionné utilise une passerelle réseau virtuel Azure. Pour plus d'informations, consultez l'article Microsoft Azure VPN Gateway.
9. Si vous avez répondu **Oui** à l'étape précédente (le réseau virtuel sélectionné utilise une passerelle réseau virtuel Azure), indiquez si vous souhaitez activer la propagation de l'itinéraire de la passerelle réseau virtuelle. Lorsque cette option est activée, Azure apprend (ajoute) automatiquement tous les itinéraires via la passerelle.

   Vous pouvez modifier ce paramètre ultérieurement sur la page **Détails** de la connexion. Toutefois, sa modification peut entraîner des changements de modèle de routage et des interruptions de trafic VDA. En outre, si vous le désactivez ultérieurement, vous devez ajouter manuellement des routes aux réseaux que les VDA utiliseront.
10. Saisissez une adresse IP et sélectionnez un masque réseau. La plage d'adresses à utiliser est affichée, ainsi que le nombre d'adresses prises en charge par la plage. Assurez-vous que la plage d'adresses IP ne chevauche pas les adresses que vous utilisez dans vos réseaux Azure et locaux.

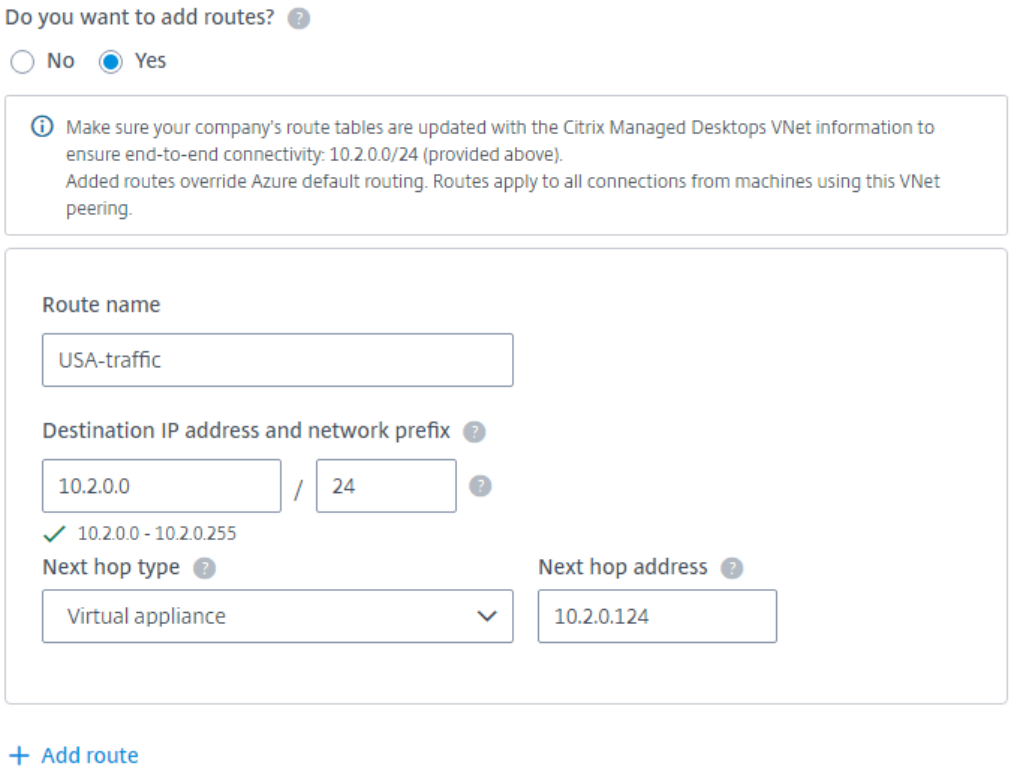
    - Par exemple, si votre réseau virtuel Azure possède un espace d'adressage de 10.0.0.0 /16, créez la connexion d'appairage de réseau virtuel dans Citrix Virtual Apps and Desktops Standard sous la forme de 192.168.0.0 /24.
    - Dans cet exemple, la création d'une connexion d'appairage de réseaux virtuels avec une plage d'adresses IP 10.0.0.0 /24 est considérée comme une plage d'adresses superposée.

    Si les adresses se chevauchent, la connexion de peering de réseau virtuel est susceptible de ne pas être créée correctement. Cela ne fonctionnera pas non plus correctement pour les tâches d'administration de site.
11. Indiquez si vous souhaitez ajouter des itinéraires personnalisés à la connexion de peering de réseau virtuel. Si vous sélectionnez **Oui**, saisissez les informations suivantes :

    a) Saisissez un nom convivial pour l'itinéraire personnalisé.

    b) Saisissez l'adresse IP de destination et le préfixe réseau. Le préfixe réseau doit être compris entre 16 et 24.

    c) Sélectionnez un type de saut suivant pour l'endroit où vous souhaitez acheminer le trafic. Si vous sélectionnez **Appliance virtuelle**, saisissez l'adresse IP interne de l'appliance.



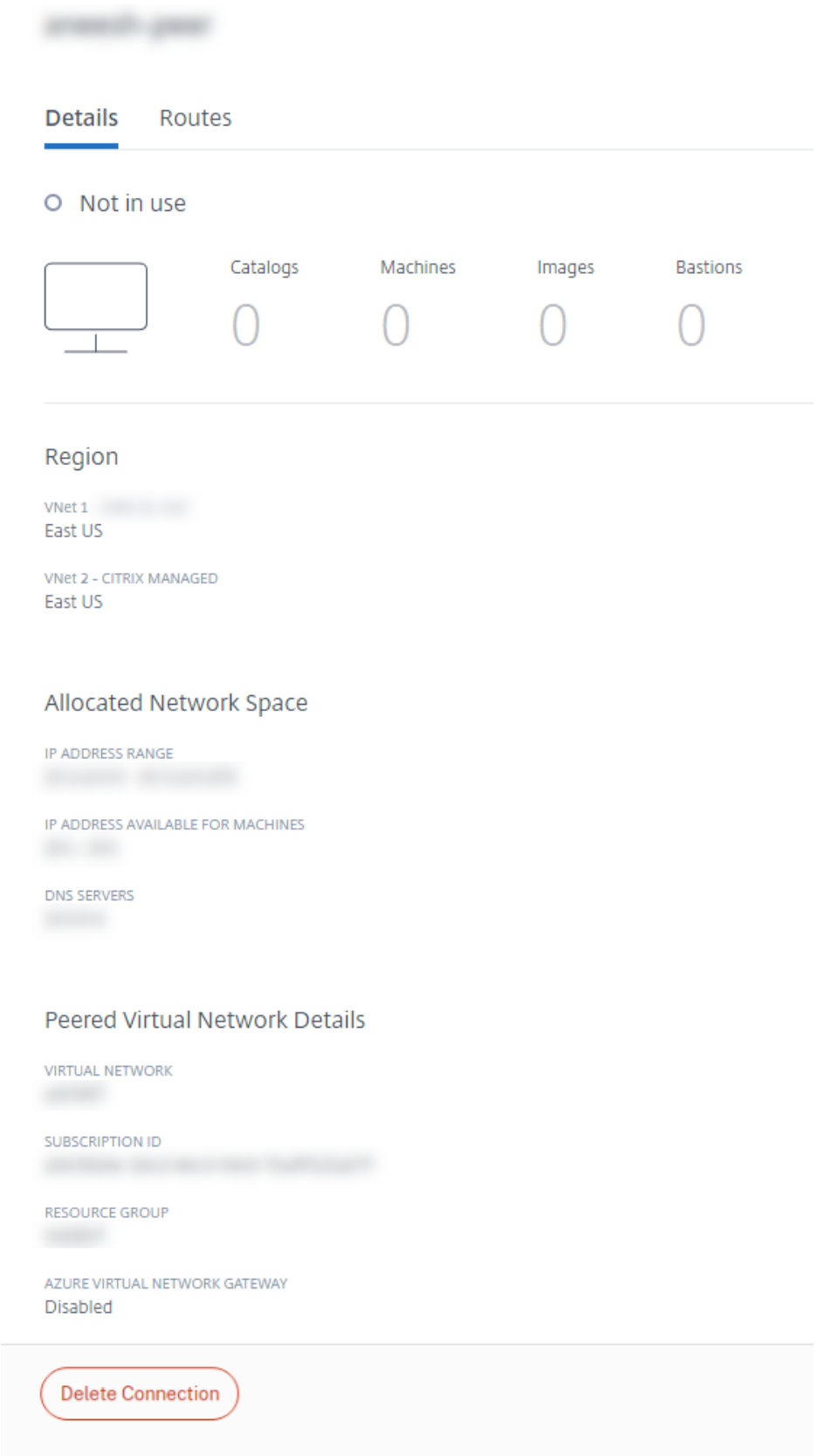
Pour plus d'informations sur les types de sauts suivants, voir Itinéraires personnalisés dans l'article Microsoft Routage du trafic réseau virtuel.

d) Cliquez sur **Ajouter un itinéraire** pour créer un autre itinéraire personnalisé pour la connexion.

12. Cliquez sur **Ajouter un appairage de réseaux virtuels**.

Une fois la connexion créée, elle est répertoriée sous **Connexions réseau > Azure VNet Peers** sur le côté droit du tableau de bord **Gérer > Déploiement rapide d'Azure** . Lorsque vous créez un catalogue, cette connexion est incluse dans la liste des connexions réseau disponibles.

Afficher les détails de la connexion de peering de réseau virtuel Azure



1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion de peering de réseau virtuel Azure que vous souhaitez afficher.

Les détails incluent :

- le nombre de catalogues, de machines, d'images et de bastions utilisant cette connexion ;
- la région, l'espace réseau alloué et les réseaux virtuels appairés ;
- les itinéraires actuellement configurés pour la connexion de peering de réseau virtuel.

Gérer les itinéraires personnalisés pour les connexions homologues de réseau virtuel Azure existantes

Vous pouvez ajouter de nouveaux itinéraires personnalisés à une connexion existante ou modifier des itinéraires personnalisés existants, y compris la désactivation ou la suppression d'itinéraires personnalisés.

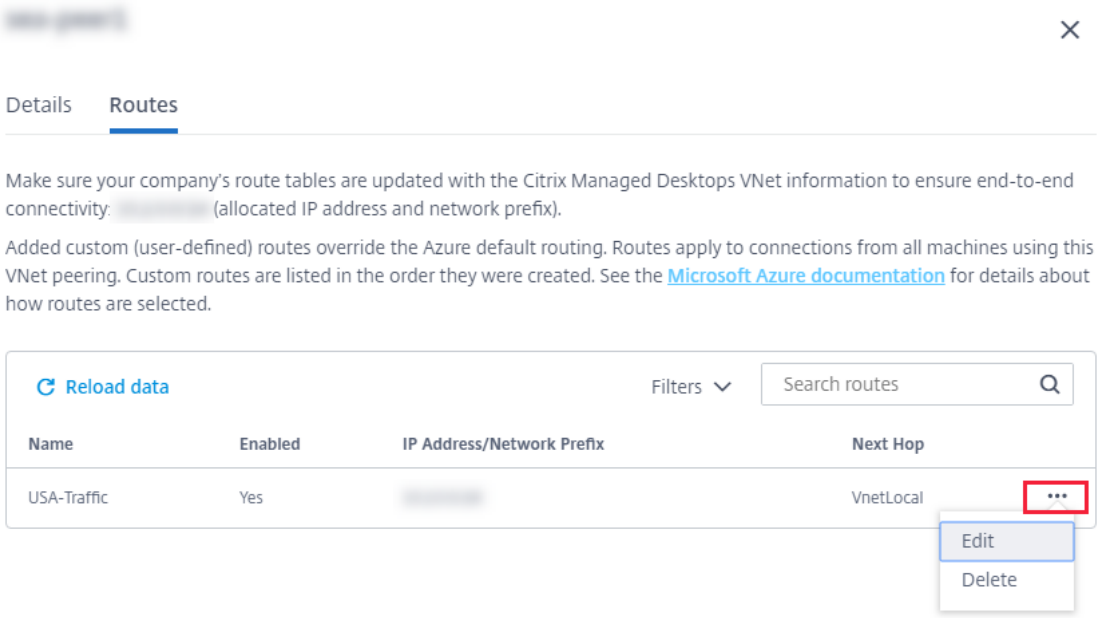
> **Important :**
>
> La modification, la désactivation ou la suppression d'itinéraires personnalisés modifient le flux de trafic de la connexion et peuvent perturber toutes les sessions utilisateur susceptibles d'être actives.

Pour ajouter un itinéraire personnalisé, procédez comme suit :

1. Dans les détails de la connexion d'appairage de réseaux virtuels, sélectionnez **Itinéraires**, puis cliquez sur **Ajouter un itinéraire**.
2. Saisissez un nom convivial, l'adresse IP de destination et le préfixe, ainsi que le type de saut suivant que vous souhaitez utiliser. Si vous sélectionnez **Appliance virtuelle** comme type de saut suivant, saisissez l'adresse IP interne de l'appliance.
3. Indiquez si vous souhaitez activer l'itinéraire personnalisé. Par défaut, l'itinéraire personnalisé est activé.
4. Cliquez sur **Ajouter un itinéraire**.

Pour modifier ou désactiver un itinéraire personnalisé, procédez comme suit :

1. Dans les détails de la connexion d'appairage de réseaux virtuels, sélectionnez **Itinéraires**, puis recherchez l'itinéraire personnalisé que vous souhaitez gérer.
2. Dans le menu des points de suspension, sélectionnez **Modifier**.



3. Apportez les modifications nécessaires à l'adresse IP de destination et au préfixe ou au type de saut suivant, le cas échéant.
4. Pour activer ou désactiver un itinéraire personnalisé, dans **Activer cet itinéraire ?**, sélectionnez **Oui** ou **Non**.
5. Cliquez sur **Enregistrer**.

Pour supprimer un itinéraire personnalisé, procédez comme suit :

1. Dans les détails de la connexion d'appairage de réseaux virtuels, sélectionnez **Itinéraires**, puis recherchez l'itinéraire personnalisé que vous souhaitez gérer.
2. Dans le menu des points de suspension, sélectionnez **Supprimer**.
3. Sélectionnez **Supprimer un itinéraire peut perturber les sessions actives** pour reconnaître l'impact de la suppression de l'itinéraire personnalisé.
4. Cliquez sur **Supprimer l'itinéraire**.

Supprimer une connexion de peering de réseau virtuel Azure

Avant de pouvoir supprimer un homologue de réseau virtuel Azure, supprimez tous les catalogues qui lui sont associés. Consultez la section Supprimer un catalogue.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez supprimer.
3. Dans les détails de la connexion, cliquez sur **Supprimer la connexion**.

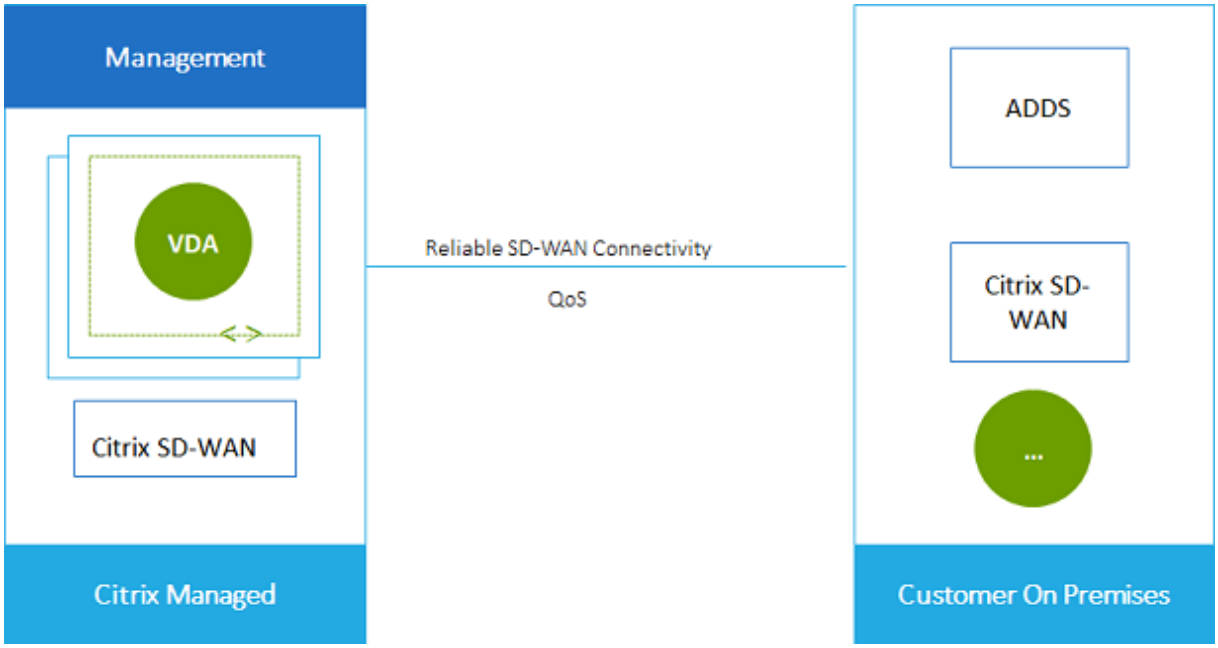
À propos des connexions SD-WAN

> **Important :**
>
> Citrix SD-WAN est devenu obsolète et tout le contenu associé sera supprimé de la documentation dans une prochaine version. Nous vous recommandons de passer à d'autres solutions réseau pour garantir un accès ininterrompu aux services Citrix.

Citrix SD-WAN optimise toutes les connexions réseau nécessaires à Citrix Virtual Apps and Desktops Standard pour Azure. Travaillant de concert avec les technologies HDX, Citrix SD-WAN fournit une qualité de service et une fiabilité de connexion pour le trafic ICA et hors bande Citrix Virtual Apps and Desktops Standard. Citrix SD-WAN prend en charge les connexions réseau suivantes :

- connexion ICA Multi-Stream entre les utilisateurs et leurs bureaux virtuels ;
- accès Internet depuis le bureau virtuel aux sites Web, aux applications SaaS et à d'autres propriétés Cloud :
- accès depuis le bureau virtuel à des ressources locales telles qu'Active Directory, serveurs de fichiers et serveurs de bases de données ;
- trafic interactif et en temps réel transporté par RTP depuis le moteur multimédia de l'application Workspace vers des services de communications unifiées hébergés dans le Cloud tels que Microsoft Teams ;
- récupération de vidéos côté client à partir de sites tels que YouTube et Vimeo.

Comme le montre le graphique suivant, vous créez une connexion SD-WAN à vos sites à partir de l'abonnement Azure géré par Citrix. Lors de la création de la connexion, les appliances VPX SD-WAN sont créées dans l'abonnement Azure géré par Citrix. Du point de vue du SD-WAN, cet emplacement est traité comme une succursale.



Configuration requise et préparation de la connexion SD-WAN

- Si les conditions suivantes ne sont pas remplies, l'option de connexion réseau SD-WAN n'est pas disponible.
  - Droits Citrix Cloud : Citrix Virtual Apps and Desktops Standard pour Azure et SD-WAN Orchestrator.
  - Déploiement SD-WAN installé et configuré. Le déploiement doit inclure un nœud de contrôle maître (MCN), que ce soit dans le Cloud ou local, et être géré avec SD-WAN Orchestrator.
- Plage IP vNet : fournir un espace d'adressage CIDR disponible (adresse IP et préfixe réseau) unique parmi les ressources réseau connectées. Il s'agit de la plage d'adresses IP attribuée aux machines virtuelles au sein du réseau virtuel Citrix Virtual Apps and Desktops Standard.

  Assurez-vous de spécifier une plage d'adresses IP qui ne chevauche pas les adresses que vous utilisez dans votre cloud et vos réseaux locaux.
  - Par exemple, si votre réseau possède un espace d'adressage de 10.0.0.0 /16, créez la connexion dans Citrix Virtual Apps and Desktops Standard comme 192.168.0.0 /24.
  - Dans cet exemple, la création d'une connexion avec une plage IP 10.0.0.0 /24 serait considérée comme une plage d'adresses qui se chevauche.

  Si les adresses se chevauchent, la connexion est susceptible de ne pas être créée correctement. Cela ne fonctionne pas non plus correctement pour les tâches d'administration de site.
- Le processus de configuration de la connexion inclut des tâches que vous (l'administrateur Citrix DaaS pour Azure) et l'administrateur SD-WAN Orchestrator devez effectuer. De plus, pour effectuer vos tâches, vous avez besoin d'informations fournies par l'administrateur SD-WAN Orchestrator.

  Avant de créer une connexion, nous vous recommandons de consulter à la fois les conseils de ce document, ainsi que la documentation SD-WAN.

Créer une connexion SD-WAN

> **Important :**
>
> Pour plus d'informations sur la configuration SD-WAN, consultez Configuration SD-WAN pour l'intégration Citrix Virtual Apps and Desktops Standard pour Azure.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Cliquez sur **Ajouter une connexion**.

3. Sur la page **Ajouter une connexion réseau**, cliquez n'importe où dans la zone SD-WAN.
4. La page suivante résume la suite. Lorsque vous avez terminé de lire, cliquez sur **Démarrer la configuration du SD-WAN**.
5. Sur la page **Configurer SD-WAN**, saisissez les informations fournies par votre administrateur SD-WAN Orchestrator.

    - **Mode de déploiement :** si vous sélectionnez **Haute disponibilité**, deux appliances VPX sont créées (recommandé pour les environnements de production). Si vous sélectionnez **Autonome**, une appliance est créée. Vous ne pouvez pas modifier ce paramètre ultérieurement. Pour passer au mode de déploiement, vous devez supprimer et recréer la succursale et tous les catalogues associés.
    - **Nom :** saisissez un nom pour le site SD-WAN.
    - **Débit et nombre de bureaux :** ces informations sont fournies par votre administrateur SD-WAN Orchestrator.
    - **Région :** région dans laquelle les appliances VPX seront créées.
    - **Sous-réseau VDA et sous-réseau SD-WAN :** ces informations sont fournies par votre administrateur SD-WAN Orchestrator. Consultez Exigences de connexion SD-WAN et préparation pour plus d'informations sur la façon d'éviter les conflits.

6. Lorsque vous avez terminé, cliquez sur **Créer une branche**.
7. La page suivante résume les éléments à rechercher dans le tableau de bord **Gérer > Déploiement rapide Azure** . Lorsque vous avez fini de lire, cliquez sur **J'ai compris**.
8. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, la nouvelle entrée SD-WAN sous **Connexions réseau** indique la progression du processus de configuration. Lorsque l'entrée devient orange avec le message **En attente d'activation par l'administrateur SD-WAN**, avertissez votre administrateur SD-WAN Orchestrator.
9. Pour les tâches d'administrateur SD-WAN Orchestrator, consultez la documentation produitSD-WAN Orchestrator.
10. Lorsque l'administrateur SD-WAN Orchestrator a terminé, l'entrée SD-WAN sous **Connexions réseau** devient verte, avec le message **Vous pouvez créer des catalogues à l'aide de cette connexion.**

Afficher les détails de la connexion SD-WAN

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez **SD-WAN** s'il ne s'agit pas de la seule sélection.
3. Cliquez sur la connexion que vous souhaitez afficher.

L'écran comprend :

- **Onglet Détails :** les informations que vous avez indiquées lors de la configuration de la connexion.
- **Onglet Connectivité des succursales :** nom, connectivité Cloud, disponibilité, niveau de bande passante, rôle et emplacement pour chaque succursale et MCN.

Supprimer une connexion SD-WAN

Avant de pouvoir supprimer une connexion SD-WAN, supprimez tous les catalogues qui y sont associés. Consultez la section Supprimer un catalogue.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez SD-WAN s'il ne s'agit pas de la seule sélection.
3. Cliquez sur la connexion que vous souhaitez supprimer pour développer ses informations.
4. Dans l'onglet **Détails**, cliquez sur **Supprimer la connexion**.
5. Confirmez la suppression.

Technical Preview d'Azure VPN

La fonctionnalité VPN Azure est disponible en Technical Preview.

À propos des connexions de passerelle VPN Azure

Une connexion de passerelle VPN Azure fournit un lien de communication entre vos VDA Azure gérés par Citrix (postes de travail et applications) et les ressources de votre entreprise, telles que les réseaux locaux ou les ressources d'autres emplacements cloud. Cela revient à configurer et à se connecter à une succursale distante.

La connectivité sécurisée utilise les protocoles standard de l'industrie Internet Protocol Security (IPsec) et Internet Key Exchange (IKE).

Au cours du processus de création de la connexion :

- Vous fournissez les informations que Citrix utilise pour créer la passerelle et la connexion.
- Citrix crée une passerelle VPN Azure basée sur des itinéraires de site à site. La passerelle VPN forme un tunnel IPsec (Internet Protocol Security) direct entre l'abonnement Azure géré par Citrix et le périphérique hôte de votre VPN.
- Une fois que Citrix a créé la passerelle et la connexion VPN Azure, vous mettez à jour la configuration, les règles de pare-feu et les tables de routage de votre VPN. Pour ce processus, vous

utilisez une adresse IP publique fournie par Citrix et une clé pré-partagée (PSK) que vous avez fournie pour créer la connexion.

Un exemple de connexion est illustré dans Créer une connexion de passerelle VPN Azure.

Vous n'avez pas besoin de votre propre abonnement Azure pour créer ce type de connexion.

Vous pouvez également utiliser des itinéraires personnalisés avec ce type de connexion.

Itinéraires personnalisés de la passerelle VPN Azure

Les itinéraires personnalisés ou définis par l'utilisateur remplacent les itinéraires système par défaut pour diriger le trafic entre les machines virtuelles de vos réseaux et Internet. Vous pouvez utiliser des itinéraires personnalisés s'il existe des réseaux auxquels les ressources Citrix Virtual Apps and Desktops Standard sont censées accéder mais ne sont pas directement connectés via une passerelle VPN Azure. Par exemple, vous pouvez créer un itinéraire personnalisé qui force le trafic via une appliance réseau vers Internet ou vers un sous-réseau local.

Lorsque vous ajoutez des itinéraires personnalisés à une connexion, ces itinéraires s'appliquent à toutes les machines qui utilisent cette connexion.

Pour utiliser des itinéraires personnalisés :

- Vous devez disposer d'une passerelle réseau virtuel existante ou d'une appliance réseau telle que Citrix SD-WAN dans votre environnement Citrix Virtual Apps and Desktops Standard.
- Lorsque vous ajoutez des itinéraires personnalisés, vous devez mettre à jour les tables de routage de votre entreprise avec les informations VPN de destination pour garantir une connectivité de bout en bout.
- Les itinéraires personnalisés sont affichés dans l'onglet **Connexion > Itinéraires** dans l'ordre dans lequel ils ont été saisis. Cet ordre d'affichage n'affecte pas l'ordre dans lequel les itinéraires sont sélectionnés.

Avant d'utiliser des itinéraires personnalisés, consultez l'article Microsoft Routage du trafic de réseau virtuel pour en savoir plus sur l'utilisation d'itinéraires personnalisés, les types de sauts suivants et la façon dont Azure sélectionne les itinéraires pour le trafic sortant.

Vous pouvez ajouter des itinéraires personnalisés lorsque vous créez une connexion de passerelle VPN Azure ou à des connexions existantes dans votre environnement de service.

Configuration requise et préparation de la passerelle VPN Azure

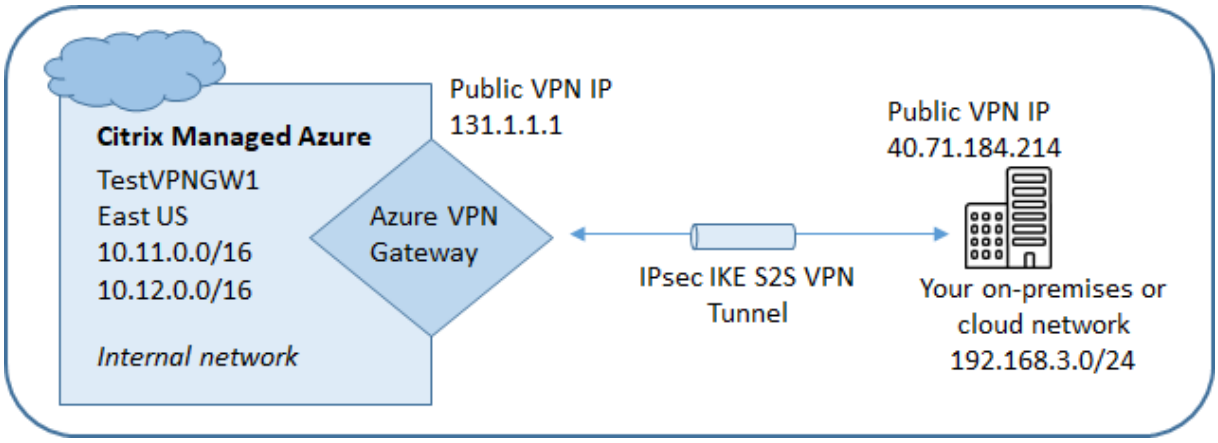
- Pour en savoir plus sur la passerelle VPN Azure, consultez l'article Microsoft Qu'est-ce que la passerelle VPN ?

- Consultez la configuration requise pour toutes les connexions réseau.
- Vous devez disposer d'un VPN configuré. Le réseau virtuel doit pouvoir envoyer et recevoir du trafic via la passerelle VPN. Un réseau virtuel ne peut pas être associé à plusieurs passerelles de réseau virtuel.
- Vous devez disposer d'un appareil IPsec doté d'une adresse IP publique. Pour en savoir plus sur les appareils VPN validés, consultez l'article Microsoft À propos des appareils VPN.
- Consultez la procédure Créer une connexion de passerelle VPN Azure avant de la démarrer réellement, afin de pouvoir collecter les informations dont vous avez besoin. Par exemple, vous aurez besoin d'adresses autorisées dans votre réseau, de plages d'adresses IP pour les VDA et la passerelle, du débit et du niveau de performance souhaités, ainsi que des adresses de serveur DNS.

Créer une connexion de passerelle VPN Azure

Assurez-vous de consulter cette procédure avant de la démarrer.

Le schéma suivant montre un exemple de configuration d'une connexion de passerelle VPN Azure. En règle générale, Citrix gère les ressources sur le côté gauche du diagramme et vous gérez les ressources sur le côté droit. Certaines descriptions de la procédure suivante incluent des références aux exemples du diagramme.



1. Depuis le tableau de bord **Gérer** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Cliquez sur **Ajouter une connexion**.
3. Cliquez n'importe où dans la zone **Passerelle VPN Azure** .
4. Consultez les informations sur la page **Ajouter une connexion VPN**, puis cliquez sur **Démarrer la configuration du VPN**.
5. Sur la page **Ajouter une connexion**, fournissez les informations suivantes.

- **Nom :** nom de la connexion. (Dans le diagramme, le nom est TestVPNGW1.)
- **Adresse IP VPN :** votre adresse IP publique.

  Dans le diagramme, l'adresse est 40.71.184.214.
- **Réseaux autorisés :** une ou plusieurs plages d'adresses auxquelles le service Citrix est autorisé à accéder sur votre réseau. En général, cette plage d'adresses contient les ressources auxquelles vos utilisateurs doivent accéder, telles que les serveurs de fichiers.

  Pour ajouter plusieurs plages, cliquez sur **Ajouter d'autres adresses IP** et entrez une valeur. Répétez l'opération au besoin.

  Dans le diagramme, la plage d'adresses est 192.168.3.0/24.
- **Clé pré-partagée :** valeur utilisée par les deux extrémités du VPN pour l'authentification (similaire à un mot de passe). C'est vous qui décidez quelle est cette valeur. N'oubliez pas de noter la valeur. Vous en aurez besoin plus tard lorsque vous configurerez votre VPN avec les informations de connexion.
- **Performances et débit :** niveau de bande passante à utiliser lorsque vos utilisateurs accèdent aux ressources de votre réseau.

  Tous les choix ne prennent pas nécessairement en charge le Border Gateway Protocol (BGP). Dans ce cas, les champs des **paramètres BCP** ne sont pas disponibles.
- **Région :** région Azure dans laquelle Citrix déploie des machines qui mettent à disposition des bureaux et des applications (VDA), lorsque vous créez des catalogues qui utilisent cette connexion. Vous ne pouvez pas modifier cette sélection après avoir créé la connexion. Si vous décidez ultérieurement d'utiliser une autre région, vous devez créer ou utiliser une autre connexion qui spécifie la région souhaitée.

  Dans le diagramme, la région est EastUS.
- **Mode actif-actif (haute disponibilité) :** indique si deux passerelles VPN sont créées pour une haute disponibilité. Lorsque ce mode est activé, une seule passerelle est active à la fois. Découvrez la passerelle VPN Azure active-active dans le document Microsoft Highly Available Cross-Premises Connectivity.
- **Paramètres BGP :** (Disponible uniquement si les **performances et le débit** sélectionnés prennent en charge le BGP.) Indique s'il faut utiliser le Border Gateway Protocol (BGP). Pour en savoir plus sur le BGP, consultez le document Microsoft : About BGP with Azure VPN Gateway. Si vous activez le protocole BGP, fournissez les informations suivantes :
  - **Numéro de système autonome (ASN) :** les passerelles de réseau virtuel Azure se voient attribuer un ASN par défaut de 65515. Une connexion compatible BGP entre deux passerelles réseau nécessite que leurs ASN soient différents. Si nécessaire, vous pouvez modifier l'ASN maintenant ou après la création de la passerelle.

  - **Adresse IP d'appairage IP BGP :** Azure prend en charge l'adresse IP BGP dans la plage 169.254.21.*x* à 169.254.22.*x*.

- **Sous-réseau VDA :** plage d'adresses dans laquelle les VDA Citrix (machines qui fournissent des bureaux et des applications) et Cloud Connector résideront lorsque vous créez un catalogue qui utilise cette connexion. Après avoir saisi une adresse IP et sélectionné un masque réseau, la plage d'adresses s'affiche, ainsi que le nombre d'adresses prises en charge par la plage.

  Bien que cette plage d'adresses soit gérée dans l'abonnement Azure géré par Citrix, elle fonctionne comme s'il s'agissait d'une extension de votre réseau.

  - La plage d'adresses IP ne doit pas chevaucher les adresses que vous utilisez sur vos réseaux locaux ou autres réseaux cloud. Si les adresses se chevauchent, la connexion est susceptible de ne pas être créée correctement. En outre, une adresse qui se chevauche ne fonctionnera pas correctement pour les tâches d'administration du site.
  - La plage de sous-réseau VDA doit être différente de l'adresse du sous-réseau de la passerelle.
  - Vous ne pouvez pas modifier cette valeur après avoir créé la connexion. Pour utiliser une valeur différente, créez une autre connexion.

  Dans le diagramme, le sous-réseau VDA est 10.11.0.0/16.

- **Sous-réseau de passerelle :** plage d'adresses dans laquelle la passerelle VPN Azure résidera lorsque vous créez un catalogue qui utilise cette connexion.

  - La plage d'adresses IP ne doit pas chevaucher les adresses que vous utilisez sur vos réseaux locaux ou autres réseaux cloud. Si les adresses se chevauchent, la connexion est susceptible de ne pas être créée correctement. En outre, une adresse qui se chevauche ne fonctionnera pas correctement pour les tâches d'administration du site.
  - La plage de sous-réseau de passerelle doit être différente de l'adresse de sous-réseau du VDA.
  - Vous ne pouvez pas modifier cette valeur après avoir créé la connexion. Pour utiliser une valeur différente, créez une autre connexion.

  Dans le diagramme, le sous-réseau de passerelle est 10.12.0.9/16.

- **Itinéraires :** indiquez si vous souhaitez ajouter des itinéraires personnalisés à la connexion. Si vous souhaitez ajouter des itinéraires personnalisés, fournissez les informations suivantes :

  - Saisissez un nom convivial pour l'itinéraire personnalisé.

- Saisissez l'adresse IP de destination et le préfixe réseau. Le préfixe réseau doit être compris entre 16 et 24.
- Sélectionnez un type de saut suivant pour l'endroit où vous souhaitez acheminer le trafic. Si vous sélectionnez **Appliance virtuelle, entrez l'adresse IP interne de l'appliance. Pour plus d'informations sur les types de sauts suivants, voir Itinéraires personnalisés dans l'article Microsoft Routage du trafic réseau virtuel.

Pour ajouter plusieurs itinéraires, cliquez sur **Ajouter un itinéraire** et saisissez les informations demandées.

- **Serveurs DNS :** entrez les adresses de vos serveurs DNS et indiquez le serveur préféré. Bien que vous puissiez modifier les entrées du serveur DNS ultérieurement, n'oubliez pas que leur modification peut entraîner des problèmes de connectivité pour les machines des catalogues qui utilisent cette connexion.

  Pour ajouter plus de deux adresses de serveur DNS, cliquez sur **Ajouter un autre DNS**, puis entrez les informations demandées.

6. Cliquez sur **Créer une connexion VPN**.

Une fois que Citrix a créé la connexion, elle est répertoriée sous **Connexions réseau > Passerelle VPN Azure** sur le tableau de bord **Gérer** dans Citrix DaaS pour Azure. La carte de connexion contient une adresse IP publique. (Dans le diagramme, l'adresse est 131.1.1.1.)

- Utilisez cette adresse (et la clé pré-partagée que vous avez spécifiée lors de la création de la connexion) pour configurer votre VPN et vos pare-feu. Si vous avez oublié votre clé pré-partagée, vous pouvez la modifier sur la page **Détails** de la connexion. Vous aurez besoin de la nouvelle clé pour configurer votre extrémité de passerelle VPN.

  Par exemple, autorisez les exceptions dans votre pare-feu pour les plages d'adresses IP du sous-réseau du VDA et de la passerelle que vous avez configurées.

- Mettez à jour les tables de routage de votre entreprise avec les informations de connexion de la passerelle VPN Azure pour garantir une connectivité de bout en bout.

  Dans le diagramme, de nouvelles routes sont requises pour le trafic allant de 192.168.3.0/24 à 10.11.0.0/16 et 10.12.0.9/16 (les sous-réseaux VDA et passerelle).

- Si vous avez configuré des itinéraires personnalisés, effectuez également les mises à jour appropriées pour eux.

Lorsque les deux extrémités de la connexion sont correctement configurées, l'entrée de la connexion dans **Connexions réseau > Passerelle VPN Azure** indique **Prêt à être utilisé**.

Afficher une connexion de passerelle VPN Azure

1. Depuis le tableau de bord **Gérer** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez afficher.

   Écrans :

- L'onglet **Détails** indique le nombre de catalogues, de machines, d'images et de bastions qui utilisent cette connexion. Il contient également la plupart des informations que vous avez configurées pour cette connexion.
- L'onglet **Itinéraires** répertorie les informations d'itinéraire personnalisées pour la connexion.

Gérer les itinéraires personnalisés pour une connexion de passerelle VPN Azure

Dans une connexion de passerelle VPN Azure existante, vous pouvez ajouter, modifier, désactiver et supprimer des itinéraires personnalisés.

Pour plus d'informations sur l'ajout d'itinéraires personnalisés lorsque vous créez une connexion, consultez Créer une connexion de passerelle VPN Azure.

> **Important :**
>
> La modification, la désactivation ou la suppression d'itinéraires personnalisés modifie le flux de trafic de la connexion et peut perturber les sessions utilisateur actives.

1. Depuis le tableau de bord **Gérer** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez afficher.
   - Pour ajouter un itinéraire personnalisé, procédez comme suit :
     a) Dans l'onglet **Itinéraires** de la connexion, cliquez sur **Ajouter un itinéraire**.
     b) Saisissez un nom convivial, l'adresse IP de destination et le préfixe, ainsi que le type de saut suivant que vous souhaitez utiliser. Si vous sélectionnez **Appliance virtuelle** comme type de saut suivant, saisissez l'adresse IP interne de l'appliance.
     c) Indiquez si vous souhaitez activer l'itinéraire personnalisé. Par défaut, l'itinéraire personnalisé est activé.
     d) Cliquez sur **Ajouter un itinéraire**.
   - Pour modifier ou activer/désactiver un itinéraire personnalisé :

a) Dans l'onglet **Itinéraires** de la connexion, recherchez l'itinéraire personnalisé que vous souhaitez gérer.

b) Dans le menu des points de suspension, sélectionnez **Modifier**.

c) Modifiez l'adresse IP et le préfixe de destination, ou le type de saut suivant, selon vos besoins.

d) Indiquez si vous souhaitez activer l'itinéraire.

e) Cliquez sur **Enregistrer**.

- Pour supprimer un itinéraire personnalisé, procédez comme suit :

a) Dans l'onglet **Itinéraires** de la connexion, recherchez l'itinéraire personnalisé que vous souhaitez gérer.

b) Dans le menu des points de suspension, sélectionnez **Supprimer**.

c) Sélectionnez **Supprimer un itinéraire peut perturber les sessions actives** pour reconnaître l'impact de la suppression de l'itinéraire personnalisé.

d) Cliquez sur **Supprimer l'itinéraire**.

Réinitialiser ou supprimer une connexion de passerelle VPN Azure

> **Important :**
>
> - La réinitialisation d'une connexion entraîne la perte de la connexion en cours et les deux extrémités doivent la rétablir. Une réinitialisation interrompt les sessions utilisateur actives.
> - Avant de pouvoir supprimer une connexion, supprimez tous les catalogues qui l'utilisent. Consultez la section Supprimer un catalogue.

Pour réinitialiser ou supprimer une connexion :

1. Depuis le tableau de bord **Gérer** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez réinitialiser ou supprimer.
3. Dans l'onglet **Détails** de la connexion :
   - Pour réinitialiser la connexion, cliquez sur **Réinitialiser la connexion**.
   - Pour supprimer la connexion, cliquez sur **Supprimer la connexion**.
4. Si vous y êtes invité, confirmez l'action.

Création d'une adresse IP statique publique

Si vous souhaitez que tous les VDA de machines sur une connexion utilisent une seule adresse IP statique publique sortante (passerelle) vers Internet, activez une passerelle NAT. Vous pouvez activer une passerelle NAT pour les connexions aux catalogues qui sont joints à un domaine ou qui ne sont pas joints à un domaine.

Pour activer une passerelle NAT pour une connexion :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Connexions réseau** sur la droite.
2. Sous **Connexions réseau**, sélectionnez une connexion sous **CITRIX MANAGED** ou **AZURE VNET PEERINGS**.
3. Dans la fiche de détails de connexion, cliquez sur **Activer la passerelle NAT**.
4. Sur la page Activer la passerelle NAT, déplacez le curseur sur **Oui** et configurez un temps d'inactivité.
5. Cliquez sur **Confirm Changes**.

Lorsque vous activez une passerelle NAT :

- Azure attribue automatiquement une adresse IP statique publique à la passerelle. (Vous ne pouvez pas spécifier cette adresse.) Tous les VDA de tous les catalogues qui utilisent cette connexion utiliseront cette adresse pour la connectivité sortante.
- Vous pouvez spécifier une valeur de délai d'inactivité. Cette valeur indique le nombre de minutes pendant lesquelles une connexion sortante ouverte via la passerelle NAT peut rester inactive avant la fermeture de la connexion.
- Vous devez autoriser l'adresse IP statique publique dans votre pare-feu.

Vous pouvez revenir à la fiche des détails de connexion pour activer ou désactiver la passerelle NAT et modifier la valeur du délai d'expiration.

Images

September 7, 2022

Lorsque vous créez un catalogue pour fournir des bureaux ou des applications, une image est utilisée (avec d'autres paramètres) comme modèle de création des machines.

Images préparées par Citrix

Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure) fournit plusieurs images préparées par Citrix :

- Windows 10 Entreprise (session unique)
- Windows 10 Enterprise Virtual Desktop (sessions multiples)
- Windows 10 Enterprise Virtual Desktop (sessions multiples) avec Office 365 ProPlus
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Linux Ubuntu (session unique et sessions multiples)

Les images préparées par Citrix sont dotées d'un agent Citrix Virtual Delivery Agent (VDA) actuel et d'outils de dépannage installés. Le VDA est le mécanisme de communication entre les machines de vos utilisateurs et l'infrastructure Citrix Cloud qui gère Citrix DaaS pour Azure. Les images fournies par Citrix sont notées **CITRIX**.

Vous pouvez également importer et utiliser votre propre image depuis Azure.

Façons d'utiliser les images

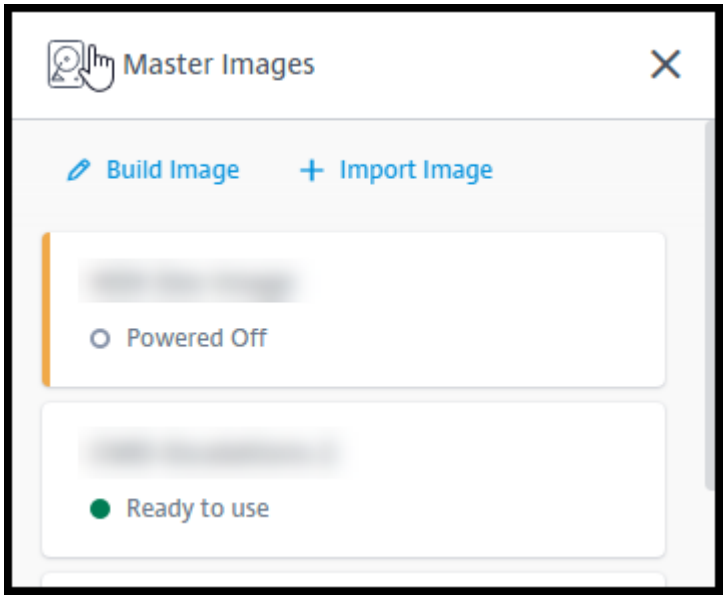
Vous pouvez :

- **Utiliser une image préparée par Citrix lors de la création d'un catalogue.** Ce choix est recommandé uniquement pour les déploiements de preuve de concept.
- **Utiliser une image préparée par Citrix pour créer une autre image.** Une fois la nouvelle image créée, vous la personnalisez en ajoutant des applications et d'autres logiciels dont vos utilisateurs ont besoin. Vous pouvez ensuite utiliser cette image personnalisée lors de la création d'un catalogue.
- **Importer une image depuis Azure.** Une fois que vous avez importé une image depuis Azure, vous pouvez ensuite utiliser cette image lors de la création d'un catalogue. Vous pouvez également utiliser cette image pour créer une nouvelle image, puis la personnaliser en ajoutant des applications. Vous pouvez ensuite utiliser cette image personnalisée lors de la création d'un catalogue.

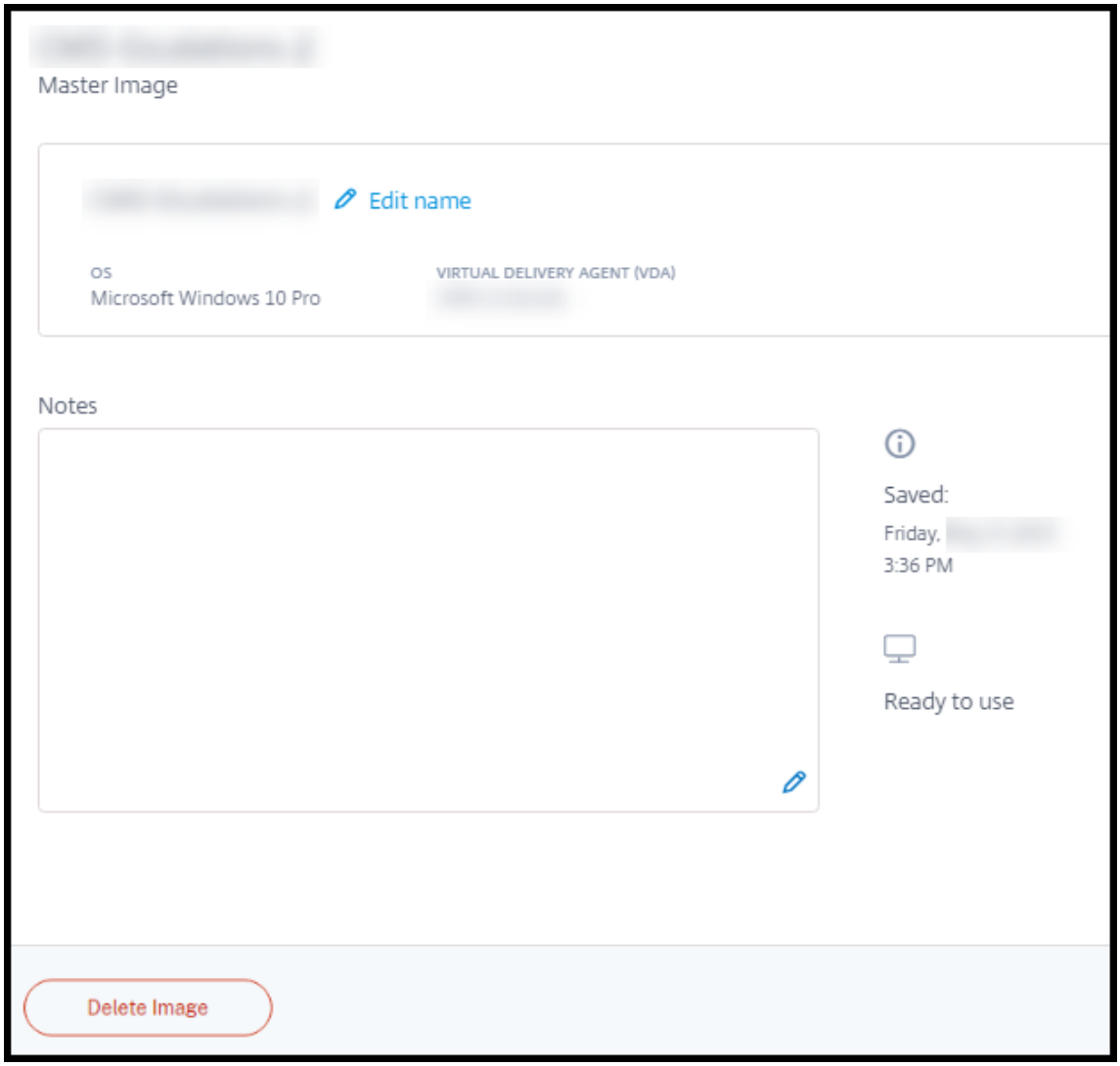
Lorsque vous créez un catalogue, Citrix DaaS pour Azure vérifie que l'image utilise un système d'exploitation valide et qu'un VDA Citrix et des outils de dépannage sont installés (ainsi que d'autres vérifications).

Afficher les informations sur l'image

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Images principales** sur la droite. L'affichage répertorie les images fournies par Citrix et les images que vous avez créées et importées.



2. Cliquez sur une image pour afficher ses détails.



À partir de la fiche de détails, vous pouvez :

- changer (modifier) le nom de l'image ;
- Ajouter et modifier des notes (disponible uniquement pour les images que vous avez préparées ou importées, et non pour les images fournies par Citrix).
- supprimer l'image.

Préparer une nouvelle image

La préparation d'une nouvelle image comprend la création de l'image, puis sa personnalisation. Lorsque vous créez une image, une machine virtuelle est créée pour charger la nouvelle image.

Exigences :

- Vous devez connaître les caractéristiques de performance dont les machines ont besoin. Par ex-

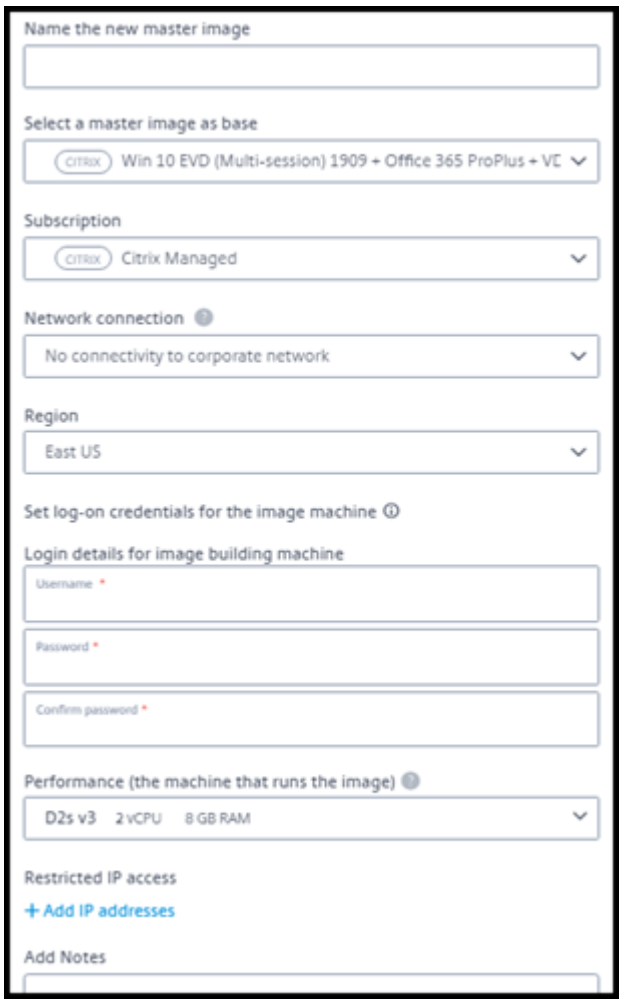
emple, l'exécution d'applications CAD peut nécessiter une unité centrale, une RAM et un stockage différents de ceux des autres applications bureautiques.
- Si vous envisagez d'utiliser une connexion à vos ressources locales, configurez cette connexion avant de créer l'image et le catalogue. Pour plus de détails, consultez la section Connexions réseau.

Lorsque vous utilisez une image Ubuntu préparée par Citrix pour créer une nouvelle image, un mot de passe racine est créé pour la nouvelle image. Vous pouvez modifier ce mot de passe racine, mais uniquement pendant le processus de création et de personnalisation de l'image. (Vous ne pouvez pas modifier le mot de passe racine après l'utilisation de l'image dans un catalogue.)

- Lorsque l'image est créée, le compte administrateur que vous avez spécifié (**Informations de connexion pour la machine de création d'image**) est ajouté au groupe `sudoers`.
- Une fois que vous êtes connecté via RDP à la machine contenant la nouvelle image, lancez l'application Terminal et tapez `sudo passwd root`. Lorsque vous y êtes invité, indiquez le mot de passe que vous avez spécifié lors de la création de l'image. Après vérification, vous êtes invité à entrer un nouveau mot de passe pour l'utilisateur racine.

Pour créer une image :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Images principales** sur la droite.
2. Cliquez sur **Créer image**.



3. Saisissez des valeurs dans les champs suivants :

   - **Nom :** saisissez un nom pour la nouvelle image.
   - **Image principale :** sélectionnez une image existante. Il s'agit de l'image de base utilisée pour créer la nouvelle image.
   - **Abonnement :** sélectionnez un abonnement Azure. Pour plus de détails, consultez Abonnements Azure.
   - **Connexion réseau :**
     - Si vous utilisez un abonnement Azure géré par Citrix, sélectionnez **Aucune connectivité** ou une connexion précédemment créée.
     - Si vous utilisez votre propre abonnement Azure géré par le client, sélectionnez votre groupe de ressources, votre réseau virtuel et votre sous-réseau. Ajoutez ensuite les détails du domaine : nom de domaine complet, unité d'organisation, nom de compte de service et informations d'identification.
   - **Configuration du domaine :** sélectionnez le type de domaine : Active Directory ou non

joint au domaine.

  - Si vous sélectionnez Active Directory, sélectionnez ou ajoutez un domaine. Spécifiez une unité d'organisation (facultatif), un nom de compte de service et un mot de passe.
  - Si vous sélectionnez une option n'appartenant pas à un domaine, aucune information supplémentaire n'est nécessaire.

- **Région :** (disponible uniquement pour **Aucune connectivité**.) Sélectionnez la région où vous souhaitez créer la machine contenant l'image.
- **Informations d'identification de connexion pour la machine à images :** vous utiliserez ces informations d'identification ultérieurement lorsque vous vous connecterez (RDP) à la machine contenant la nouvelle image, afin de pouvoir installer des applications et d'autres logiciels.
- **Performances de la machine :** il s'agit des informations relatives à l'unité centrale, à la RAM et au stockage de la machine qui exécute l'image. Sélectionnez une performance machine qui répond aux exigences de vos applications.
- **Accès IP restreint :** si vous souhaitez restreindre l'accès à des adresses spécifiques, sélectionnez **Ajouter des adresses IP**, puis saisissez une ou plusieurs adresses. Après avoir ajouté les adresses, cliquez sur **Terminé** pour revenir à la fiche **Image de création** .
- **Remarques :** vous pouvez ajouter jusqu'à 1 024 caractères de notes. Une fois l'image créée, vous pouvez mettre à jour les notes à partir de l'affichage des détails de l'image.
- **Jointure de domaine local :** indiquez si vous souhaitez rejoindre le domaine Active Directory local.

  - Si vous sélectionnez **Oui**, saisissez les informations Azure : nom de domaine complet, unité d'organisation, nom du compte de service et informations d'identification.
  - Si vous sélectionnez **Non**, saisissez les informations d'identification de la machine hôte.

4. Lorsque vous avez terminé, cliquez sur **Créer une image**.

La création d'une image peut prendre jusqu'à 30 minutes. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Images principales** sur la droite pour voir l'état actuel (tel que **Image du bâtiment** ou **Prêt à personnaliser**).

Que faire ensuite : connectez-vous à une nouvelle image et personnalisez-la.

Se connecter à une nouvelle image et la personnaliser

Après la création d'une nouvelle image, son nom est ajouté à la liste des images, avec le statut **Prêt à personnaliser** (ou un libellé similaire). Pour personnaliser cette image, vous devez d'abord

télécharger un fichier RDP. Lorsque vous utilisez ce fichier pour vous connecter à l'image, vous pouvez ensuite ajouter des applications et d'autres logiciels à l'image.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Images principales** sur la droite. Cliquez sur l'image à laquelle vous souhaitez vous connecter.
2. Cliquez sur **Télécharger le fichier RDP**. Un client RDP est téléchargé.

   La machine d'images peut s'éteindre si vous n'y ajoutez pas de fichier RDP peu de temps après sa création. Cela permet de réduire les coûts. Lorsque cela se produit, cliquez **sur Mettre sous tension**.
3. Double-cliquez sur le client RDP téléchargé. Il tente automatiquement de se connecter à l'adresse de la machine contenant la nouvelle image. Lorsque vous y êtes invité, saisissez les informations d'identification indiquées lors de la création de l'image.
4. Une fois que vous êtes connecté à la machine, ajoutez ou supprimez des applications, installez des mises à jour et terminez tout autre travail de personnalisation.

   N'effectuez **pas** de Sysprep de l'image.
5. Lorsque vous avez terminé de personnaliser la nouvelle image, retournez dans la zone **Images principales** et cliquez sur **Terminer la création**. La nouvelle image subit automatiquement des tests de validation.

Plus tard, lorsque vous créez un catalogue, la nouvelle image est incluse dans la liste des images que vous pouvez sélectionner.

Sur le tableau de bord **Gérer > Déploiement rapide**, les images affichées à droite indiquent le nombre de catalogues et de machines qui utilisent chaque image.

> **Remarque :**
>
> Une fois que vous avez finalisé une image, vous ne pouvez pas la modifier. Vous devez créer une nouvelle image (en utilisant l'image précédente comme point de départ), puis mettre à jour la nouvelle image.

Importer une image depuis Azure

Lorsque vous importez une image depuis Azure qui possède un VDA Citrix et des applications dont vos utilisateurs ont besoin, vous pouvez l'utiliser pour créer un catalogue ou remplacer l'image dans un catalogue existant.

Exigences relatives à l'image

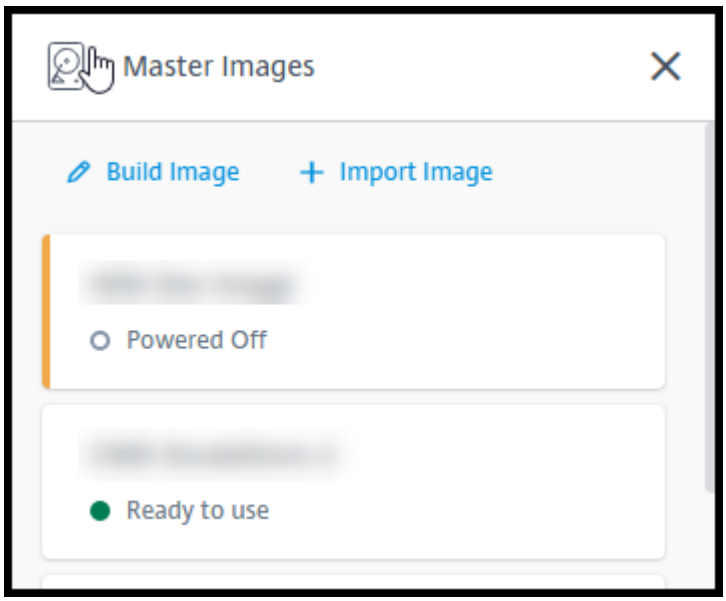
> **Remarque :**
>
> Citrix DaaS pour Azure ne prend pas en charge l'importation de disques associés aux machines virtuelles Azure de génération 2.

Citrix exécute des tests de validation sur l'image importée. Assurez-vous que les exigences suivantes sont respectées lorsque vous préparez l'image que vous allez importer dans Citrix DaaS pour Azure.

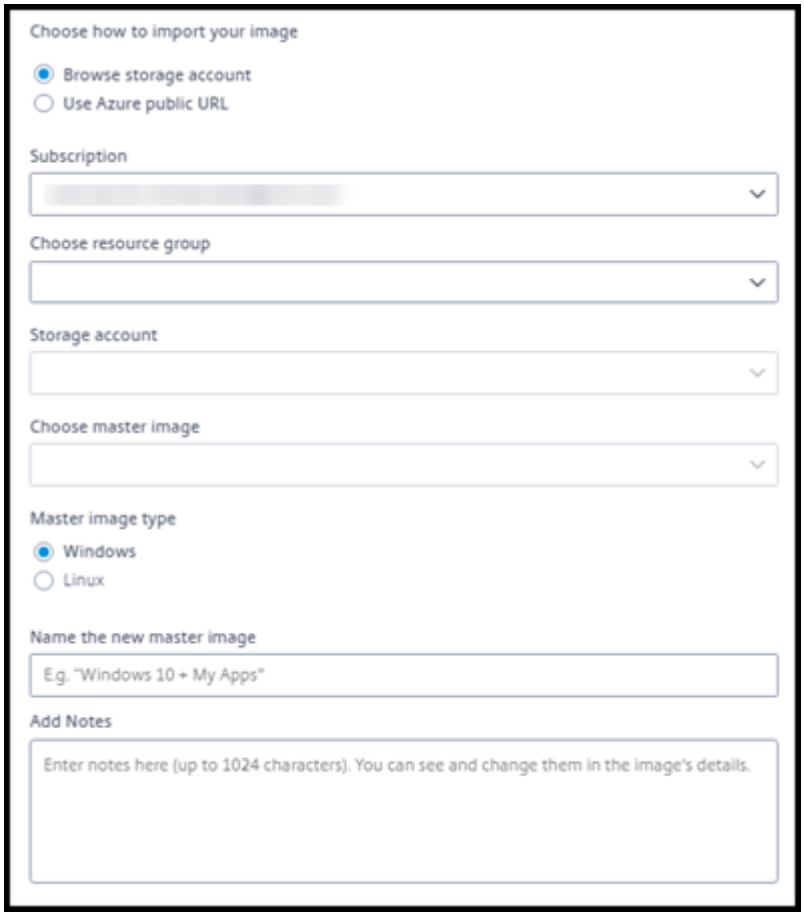
- **Système d'exploitation pris en charge :** l'image doit être un système d'exploitation pris en charge. Pour vérifier une version du système d'exploitation Windows, exécutez `Get-WmiObject Win32_OperatingSystem`.
- **Création prise en charge :** seules les machines virtuelles de génération 1 sont prises en charge.
- **Non généralisée :** l'image ne doit pas être généralisée.
- **Aucun Delivery Controller configuré :** assurez-vous qu'aucun Citrix Delivery Controller n'est configuré dans l'image. Assurez-vous que les clés de registre suivantes sont effacées.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Fichier Personality.ini :** le fichier `personality.ini` doit exister sur le lecteur système.
- **VDA valide :** un VDA Citrix plus récent que 7.11 doit être installé sur l'image.
  - Windows : pour vérifier, utilisez `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Pour obtenir des instructions d'installation, reportez-vous à la section Installer un VDA Windows sur une image.
  - Red Hat Enterprise Linux et Ubuntu : pour obtenir des conseils d'installation, reportez-vous à la documentation produit.
- **Agent de machine virtuelle Azure :** avant d'importer une image, assurez-vous que l'agent de machine virtuelle Azure est installé sur l'image. Pour plus d'informations, consultez l'article Microsoft Présentation d'Azure Virtual Machine Agent.

Importer l'image

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Images principales** sur la droite.



2. Cliquez sur **Importer une image**.



3. Choisissez comment importer l'image.

   - Pour les disques gérés, utilisez la fonctionnalité d'exportation pour générer une URL

Séquence d'avertissement sécurisée. Définissez le délai d'expiration à 7 200 secondes ou plus.

- Pour les disques durs virtuels d'un compte de stockage, choisissez l'une des options suivantes :
  - Générez une URL Séquence d'avertissement sécurisée pour le fichier VHD.
  - Mettez à jour le niveau d'accès d'un conteneur de stockage par blocs en blob ou en conteneur. Ensuite, récupérez l'URL du fichier.

4. Si vous avez sélectionné **Parcourir le compte de stockage** :

   a) Sélectionnez séquentiellement un abonnement > groupe de ressources > compte de stockage > image.
   b) Nommez l'image.

5. Si vous avez sélectionné l'**URL publique Azure** :

   a) Saisissez l'URL générée par Azure pour le disque dur virtuel. Pour obtenir des conseils, cliquez sur le lien vers le document Microsoft Télécharger un disque dur virtuel Windows à partir d'Azure.
   b) Sélectionnez un abonnement. (Une image Linux ne peut être importée que si vous sélectionnez un abonnement géré par le client.)
   c) Nommez l'image.

6. Lorsque vous avez terminé, cliquez sur **Importer une image**.

Mettre à jour un catalogue avec une nouvelle image

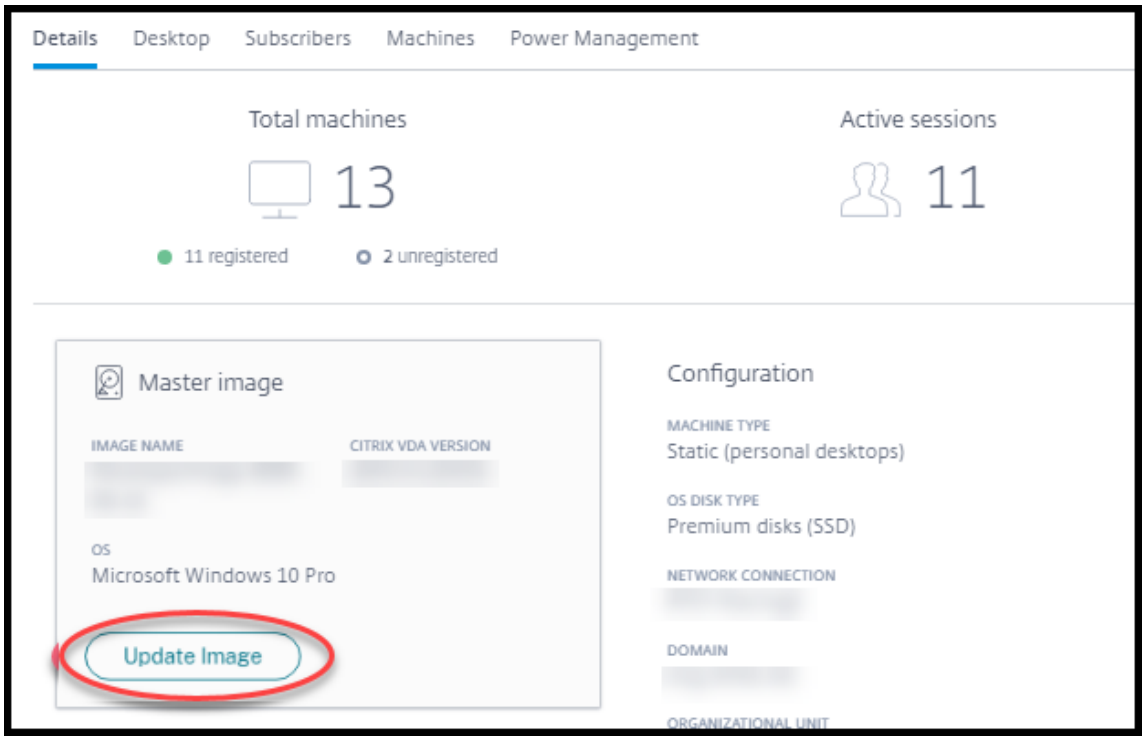
Le type de catalogue détermine quelles machines sont mises à jour lorsque vous mettez à jour le catalogue.

- Pour un catalogue aléatoire, toutes les machines actuellement dans le catalogue sont mises à jour avec la dernière image. Si vous ajoutez d'autres bureaux à ce catalogue, ceux-ci sont basés sur l'image la plus récente.
- Pour un catalogue statique, les machines actuellement dans le catalogue ne sont pas mises à jour avec la dernière image. Les machines actuellement dans le catalogue continuent d'utiliser l'image à partir de laquelle elles ont été créées. Toutefois, si vous ajoutez d'autres machines à ce catalogue, elles sont basées sur la dernière image.

Vous pouvez mettre à jour un catalogue contenant des machines avec des images de génération 1 avec une image de génération 2 si les machines du catalogue prennent en charge la génération 2. De même, vous pouvez mettre à jour un catalogue contenant des machines de génération 2 avec une image de génération 1 si les machines du catalogue prennent en charge la génération 1.

Pour mettre à jour un catalogue avec une nouvelle image :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Détails**, cliquez sur **Mettre à jour l'image**.



3. Sélectionnez une image.
4. Pour les catalogues aléatoires ou à sessions multiples : sélectionnez un intervalle de fermeture de session. Une fois que Citrix DaaS pour Azure a terminé le traitement d'image initial, les abonnés reçoivent un avertissement les invitant à enregistrer leur travail et à se déconnecter de leur bureau. L'intervalle de fermeture de session indique le temps dont disposent les abonnés après la réception du message jusqu'à ce que la session se termine automatiquement.
5. Cliquez sur **Update Image**.

Supprimer une image

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Images principales** sur la droite.
2. Cliquez sur l'image que vous souhaitez supprimer.
3. Cliquez sur **Supprimer l'image** en bas de la carte. Confirmez la suppression.

Installer un VDA Windows sur une image

Utilisez la procédure suivante lorsque vous préparez une image Windows que vous envisagez d'importer dans Citrix DaaS pour Azure. Pour obtenir des instructions d'installation de Linux VDA, consultez la documentation produit du Linux VDA.

1. Dans votre environnement Azure, connectez-vous à la machine virtuelle d'image (si vous n'êtes pas déjà connecté).
2. Vous pouvez télécharger un VDA à l'aide du lien **Téléchargements** sur la barre de navigation de Citrix Cloud. Vous pouvez également utiliser un navigateur pour accéder à la page de téléchargement de Citrix DaaS pour Azure.

   Téléchargez un VDA sur la machine virtuelle. Il existe des packages de téléchargement VDA distincts pour un système d'exploitation de bureau (à session unique) et un système d'exploitation serveur (à sessions multiples).
3. Lancez le programme d'installation de VDA en double-cliquant sur le fichier téléchargé. L'assistant d'installation démarre.
4. Sur la page **Environnement**, sélectionnez l'option permettant de créer une image à l'aide de MCS, puis cliquez sur **Suivant**.
5. Sur la page **Composants principaux**, cliquez sur **Suivant**.
6. Sur la page **Delivery Controller**, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**, puis cliquez sur **Suivant**.
7. Laissez les paramètres par défaut sur les pages **Composants supplémentaires**, **Fonctionnalités** et **Pare-feu**, sauf avis contraire de Citrix. Cliquez sur **Suivant** sur chaque page.
8. Sur la page **Résumé**, cliquez sur **Installer**. Les composants prérequis commencent à s'installer. Lorsque vous êtes invité à redémarrer, acceptez.
9. L'installation du VDA reprend automatiquement. L'installation des composants prérequis est terminée, puis les composants et les fonctionnalités sont installés. Sur la page **Call Home**, laissez le paramètre par défaut (sauf indication contraire de Citrix). Après vous être connecté, cliquez sur **Suivant**.
10. Cliquez sur **Terminer**. La machine redémarre automatiquement.
11. Pour vous assurer que la configuration est correcte, lancez une ou plusieurs des applications que vous avez installées sur la machine virtuelle.
12. Arrêtez la machine virtuelle. N'effectuez pas de Sysprep de l'image.

Pour plus d'informations sur l'installation de VDA, reportez-vous à la section Installer des VDA.

Utilisateurs et authentification

December 28, 2023

Méthodes d'authentification des utilisateurs

Les utilisateurs doivent s'authentifier lorsqu'ils se connectent à Citrix Workspace pour démarrer leur bureau ou leurs applications.

Citrix DaaS pour Azure prend en charge les méthodes d'authentification utilisateur suivantes :

- **Azure AD géré :** Azure AD géré est un Azure Active Directory (AAD) fourni et géré par Citrix. Vous n'avez pas besoin de fournir votre propre structure Active Directory. Il suffit d'ajouter vos utilisateurs au répertoire.
- **Votre fournisseur d'identité :** vous pouvez utiliser n'importe quelle méthode d'authentification disponible dans Citrix Cloud.

> **Remarque :**
>
> - Les déploiements Remote PC Access utilisent uniquement Active Directory. Pour plus d'informations, consultez la section Remote PC Access.
> - Si vous utilisez Azure AD Domain Services : les noms UPN de connexion à Workspace doivent contenir le nom de domaine qui a été spécifié lors de l'activation de Azure AD Domain Services. Les connexions ne peuvent pas utiliser les noms UPN d'un domaine personnalisé que vous créez, même si ce domaine personnalisé est désigné comme le domaine principal.

La configuration de l'authentification utilisateur inclut les procédures suivantes :

1. Configurez la méthode d'authentification utilisateur dans la configuration de l'espace de travail dans Citrix Cloud.
2. Si vous utilisez Azure géré par Citrix AD pour l'authentification de vos utilisateurs, ajoutez des utilisateurs à l'annuaire.
3. Ajoutez des utilisateurs à un catalogue.

Configurer l'authentification des utilisateurs dans Citrix Cloud

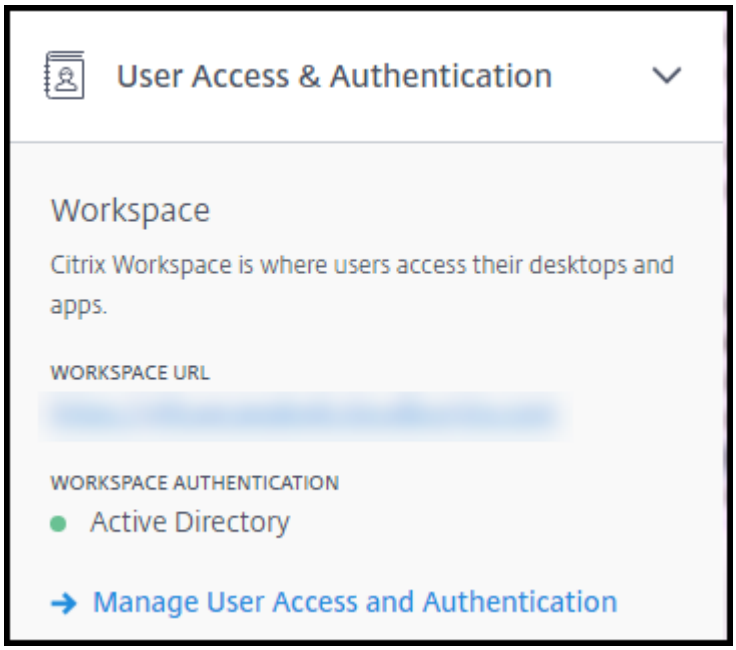
Pour configurer l'authentification des utilisateurs dans Citrix Cloud :

- Connectez-vous à la méthode d'authentification utilisateur que vous souhaitez utiliser. (Dans Citrix Cloud, vous vous « connectez » à une méthode d'authentification ou vous vous en « déconnectez ».)
- Dans Citrix Cloud, définissez l'authentification Workspace pour utiliser la méthode connectée.

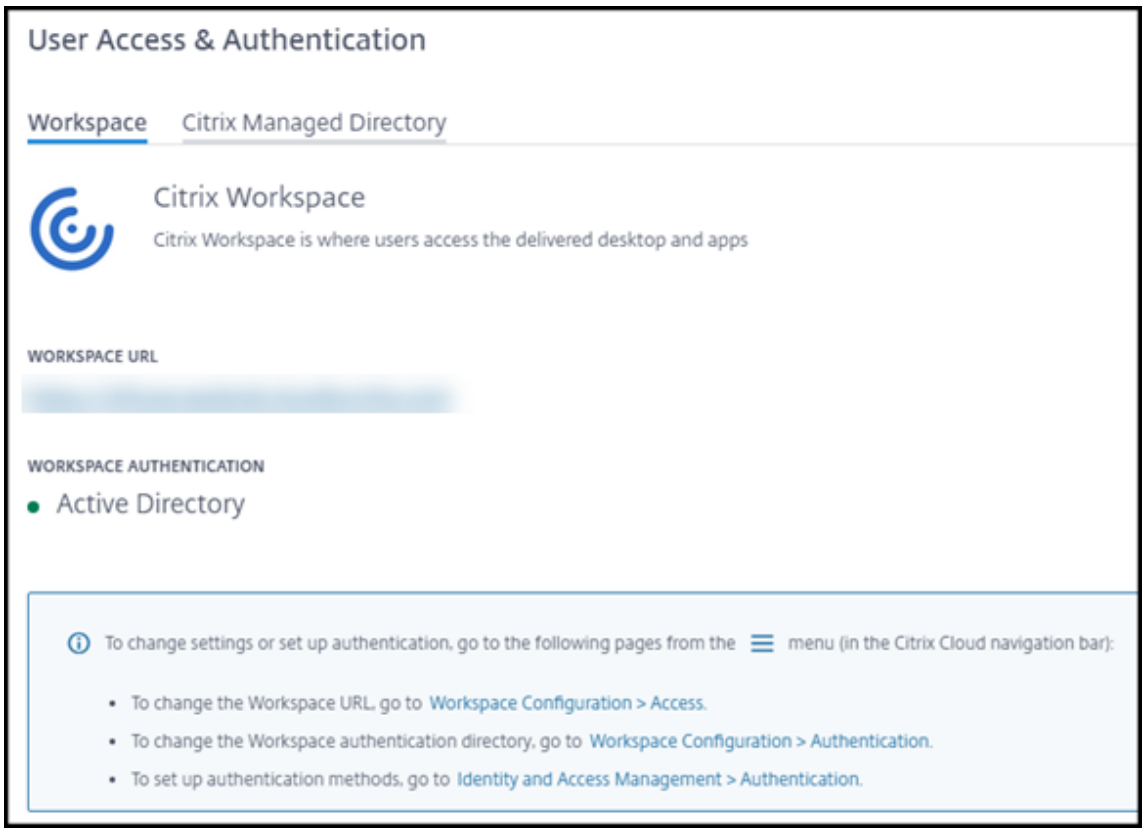
> **Remarque :**
>
> La méthode d'authentification Azure AD géré est configurée par défaut. C'est-à-dire qu'il est automatiquement connecté dans Citrix Cloud et que l'authentification Workspace est automatiquement définie pour utiliser Managed Azure AD pour Citrix DaaS pour Azure. Si vous souhaitez utiliser cette méthode (et que vous n'avez pas configuré d'autre méthode auparavant), continuez avec Ajouter et supprimer des utilisateurs dans Azure AD géré.
> Si Azure AD géré est déconnecté, l'authentification Workspace basculera vers Active Directory. Si vous souhaitez utiliser une autre méthode d'authentification, suivez les étapes ci-dessous.

Pour modifier la méthode d'authentification :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, cliquez sur **Accès utilisateur et authentification** sur la droite.



2. Cliquez sur **Gérer l'accès utilisateur et l'authentification**. Sélectionnez l'onglet **Workspace**, si ce n'est pas déjà fait. (L'autre onglet indique quelle méthode d'authentification utilisateur est actuellement configurée.)



3. Suivez le lien **Pour configurer les méthodes d'authentification**. Ce lien vous redirige vers Citrix Cloud. Sélectionnez **Connecter** dans le menu des points de suspension correspondant à la méthode souhaitée.
4. Lorsque vous êtes encore dans Citrix Cloud, sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. Dans l'onglet **Authentification**, sélectionnez la méthode souhaitée.

Que faire ensuite :

- Si vous utilisez Azure géré par Citrix AD, ajoutez des utilisateurs à l'annuaire.
- Pour toutes les méthodes d'authentification, ajoutez des utilisateurs au catalogue.

Ajouter et supprimer des utilisateurs dans Azure AD géré

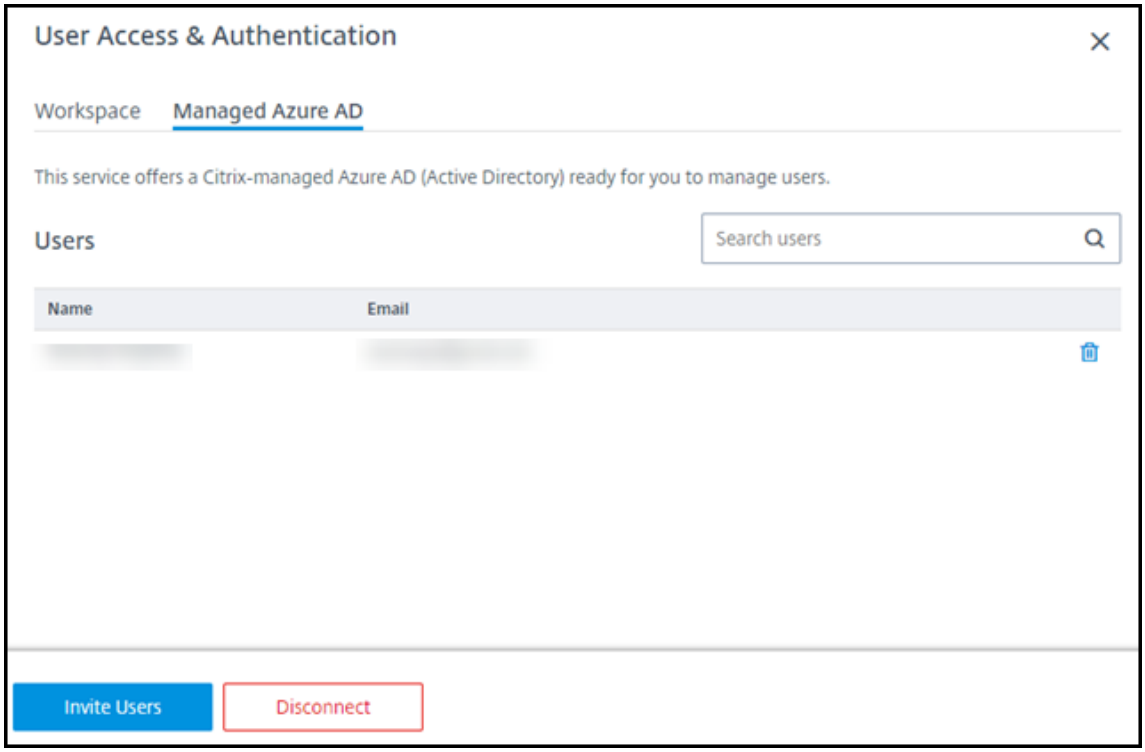
Effectuez cette procédure uniquement si vous utilisez Azure AD géré pour l'authentification des utilisateurs dans Citrix Workspace.

Vous indiquez le nom et les adresses e-mail de vos utilisateurs. Citrix leur envoie ensuite une invitation par e-mail. L'e-mail demande aux utilisateurs de cliquer sur un lien qui les relie à Citrix Managed Azure AD.

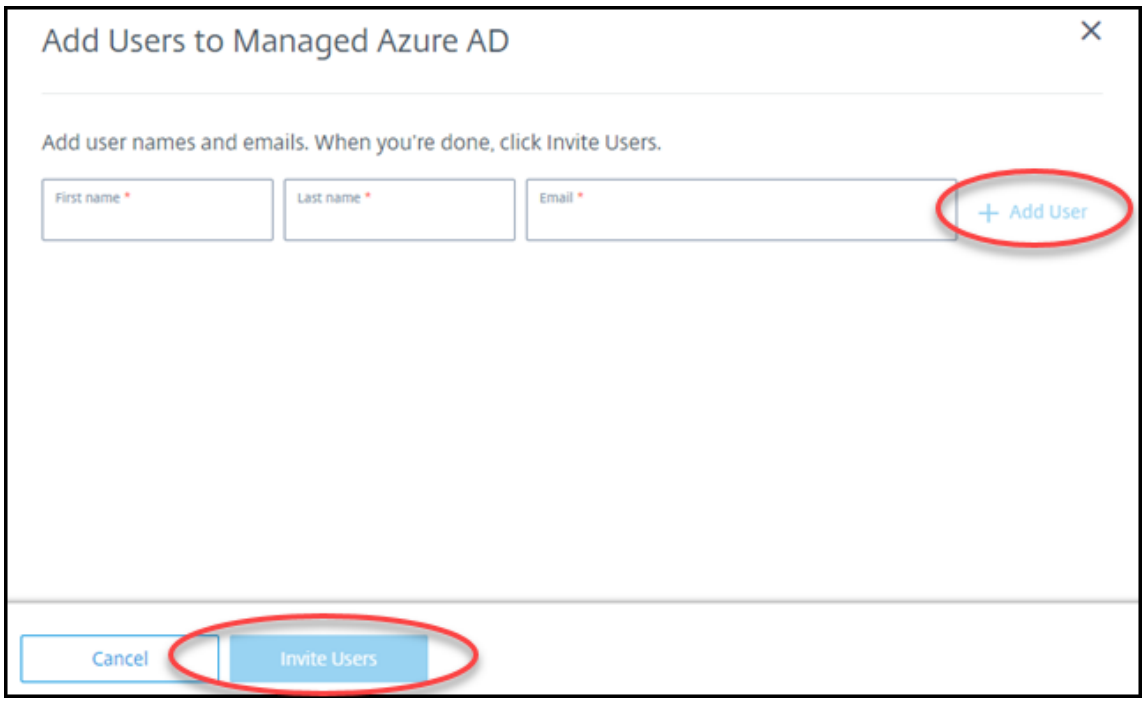
- Si l'utilisateur possède déjà un compte Microsoft associé à l'adresse e-mail que vous avez fournie, ce compte est utilisé.
- Si l'utilisateur ne possède pas de compte Microsoft avec cette adresse e-mail, Microsoft crée un compte.

Pour ajouter et inviter des utilisateurs à Azure AD géré, procédez comme suit :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **User Access & Authentication** sur la droite. Cliquez sur **Gérer l'accès utilisateur et l'authentification**.
2. Cliquez sur l'onglet **Managed Azure AD**.
3. Cliquez sur **Inviter des utilisateurs**.



4. Tapez le nom et l'adresse e-mail d'un utilisateur, puis cliquez sur **Ajouter un utilisateur**.



5. Répétez l'étape précédente pour ajouter d'autres utilisateurs.
6. Lorsque vous avez terminé d'ajouter des informations utilisateur, cliquez sur **Inviter des utilisateurs** au bas de la carte.

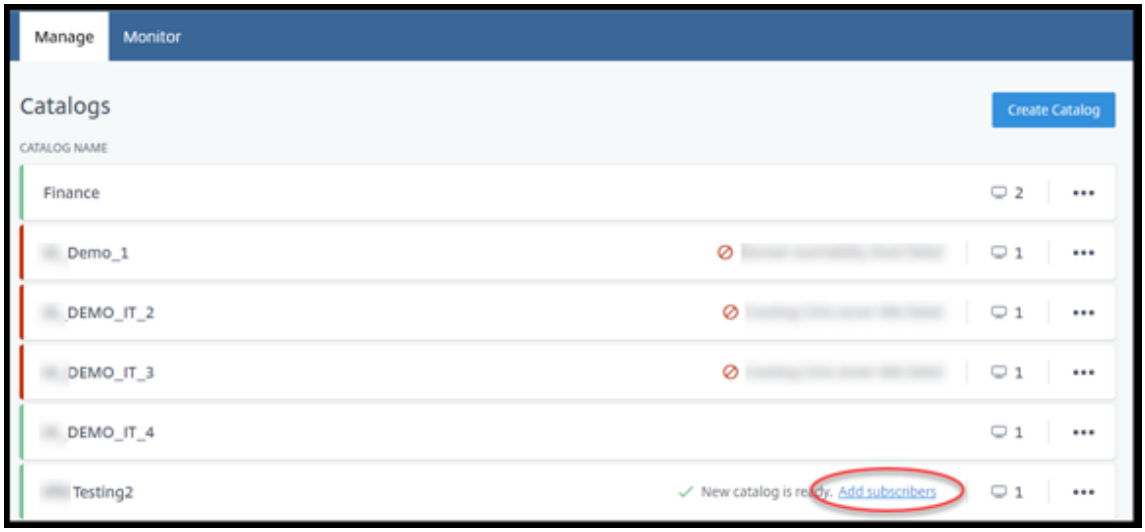
Pour supprimer un utilisateur de Managed Azure AD, cliquez sur l'icône de corbeille en regard du nom de l'utilisateur que vous souhaitez supprimer de l'annuaire. Confirmez la suppression.

Que faire ensuite : Ajouter des utilisateurs au catalogue

Ajouter ou supprimer des utilisateurs dans un catalogue

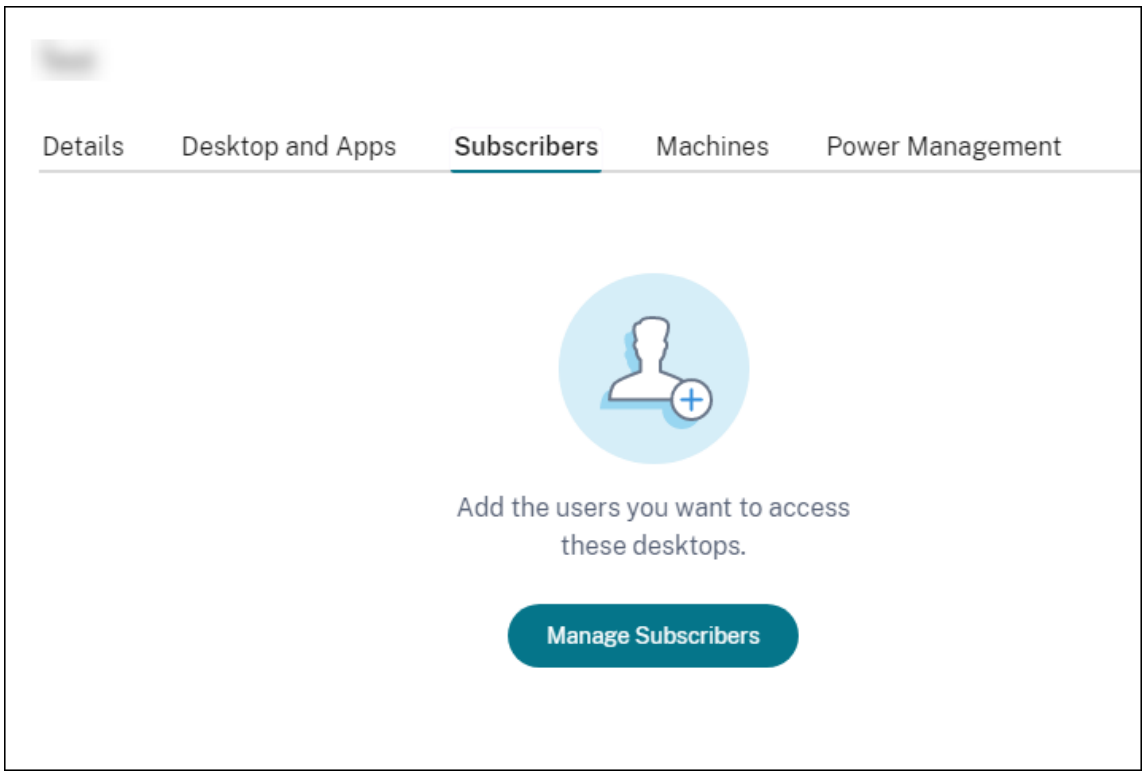
Effectuez cette procédure quelle que soit la méthode d'authentification que vous utilisez.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, si vous n'avez ajouté aucun utilisateur à un catalogue, cliquez sur **Ajouter des abonnés**.

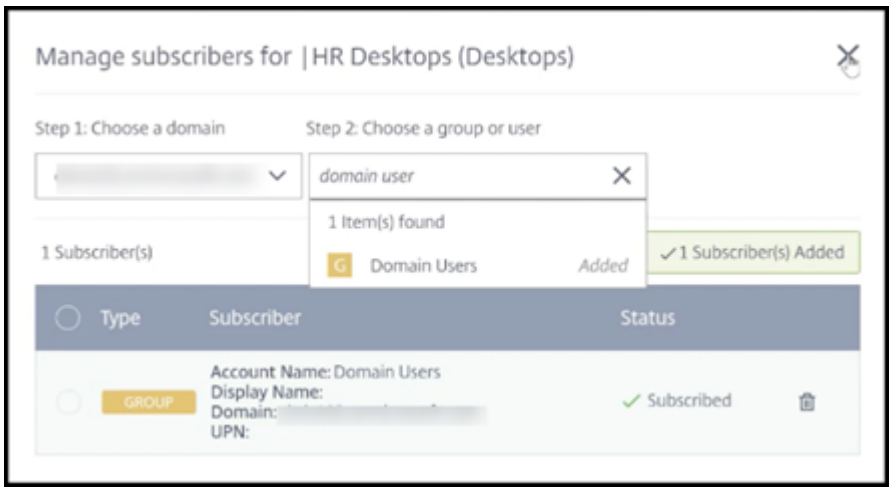


Pour ajouter des utilisateurs à un catalogue qui compte déjà des utilisateurs, cliquez n'importe où dans l'entrée du catalogue.

2. Dans l'onglet **Abonnés**, cliquez sur **Gérer les abonnés**.



3. Sélectionnez un domaine. (Si vous utilisez Azure AD géré pour l'authentification des utilisateurs, il n'y a qu'une seule entrée dans le champ de domaine.) Sélectionnez ensuite un utilisateur.



4. Sélectionnez d'autres utilisateurs, le cas échéant. Lorsque vous avez terminé, cliquez sur le **X** dans le coin supérieur droit.

Pour supprimer des utilisateurs d'un catalogue, suivez les étapes 1 et 2. À l'étape 3, cliquez sur l'icône de la corbeille en regard du nom que vous souhaitez supprimer (au lieu de sélectionner un domaine et un groupe/utilisateur). Cette action supprime l'utilisateur du catalogue, et non de la source (par exemple Azure AD géré ou votre propre AD ou AAD).

Que faire ensuite :

- Pour un catalogue avec des machines à sessions multiples, ajoutez des applications, si ce n'est déjà fait.
- Pour tous les catalogues, envoyez l'URL Citrix Workspace à vos utilisateurs.

Informations supplémentaires

Pour plus d'informations sur l'authentification dans Citrix Cloud, consultez Gestion des identités et des accès.

Gérer les catalogues

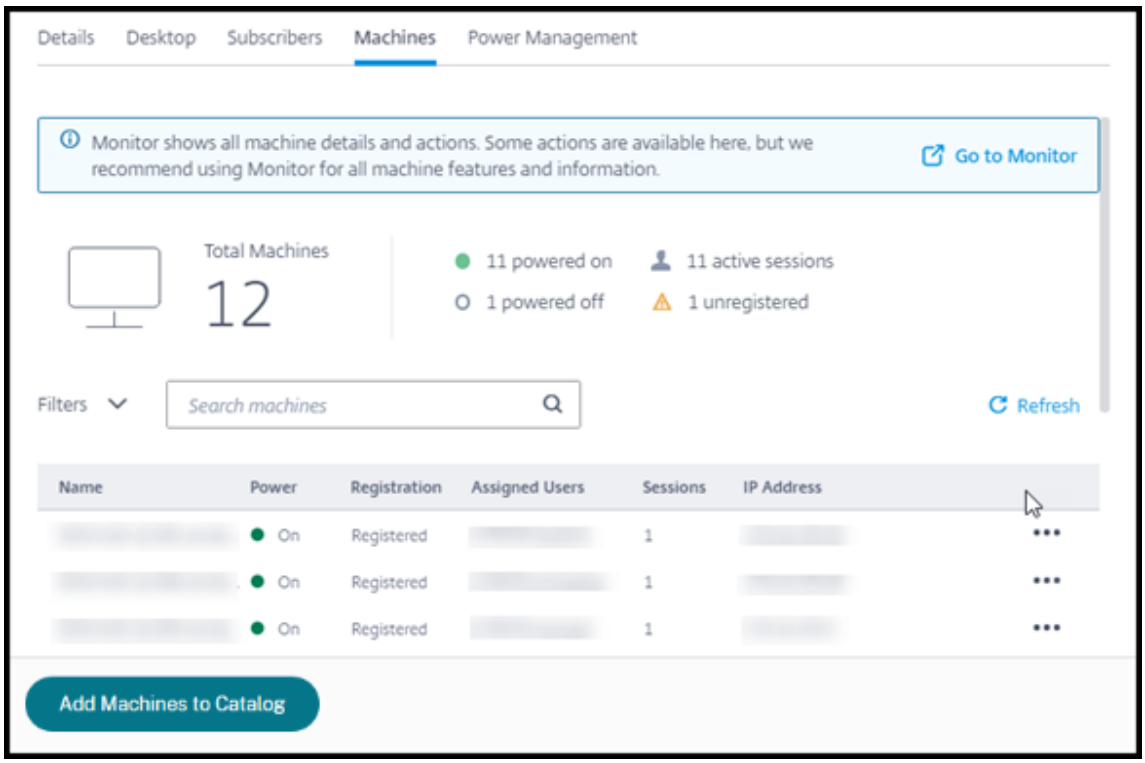
September 7, 2022

> **Remarque :**
>
> Cet article décrit les tâches que vous pouvez utiliser pour gérer les catalogues qui ont été créés dans l'interface de déploiement rapide. Pour plus d'informations sur la gestion des catalogues à l'aide de l'interface de gestion Configuration complète, voir Gérer les catalogues de machines.

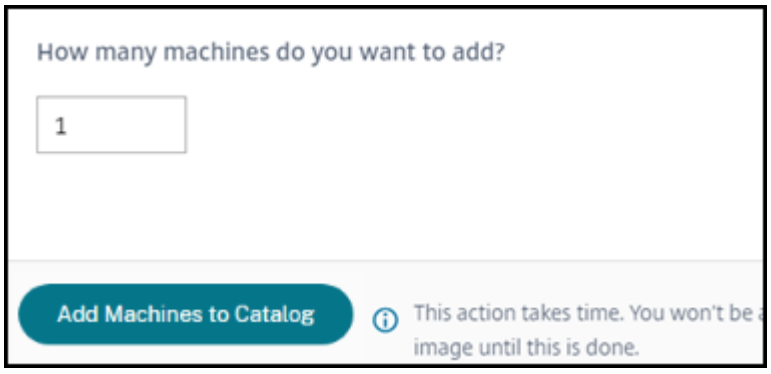
Ajouter des machines à un catalogue

Lorsque des machines sont ajoutées à un catalogue, vous ne pouvez pas apporter d'autres modifications à ce catalogue.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Machines**, cliquez sur **Ajouter des machines au catalogue**.



3. Saisissez le nombre de machines que vous souhaitez ajouter au catalogue.



4. (Valide uniquement si le catalogue est joint à un domaine.) Saisissez le nom d'utilisateur et le mot de passe du compte de service.
5. Cliquez sur **Ajouter des machines au catalogue**.

Vous ne pouvez pas réduire le nombre de machines pour un catalogue. Vous pouvez toutefois utiliser les paramètres de calendriers de gestion de l'alimentation pour contrôler le nombre de machines sous tension ou supprimer des machines individuelles depuis l'onglet **Machines**. Reportez-vous à la section Gérer les machines dans un catalogue pour plus d'informations sur la suppression de machines de l'onglet **Machines**.

Modifier le nombre de sessions par machine

La modification du nombre de sessions par machine à sessions multiples peut affecter l'expérience utilisateur. L'augmentation de cette valeur peut réduire les ressources de calcul allouées à des sessions simultanées. Recommandation : observez vos données d'utilisation pour déterminer l'équilibre approprié entre l'expérience utilisateur et le coût.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, sélectionnez un catalogue contenant des machines multi-sessions.
2. Sous l'onglet **Détails**, cliquez sur **Modifier** en regard de **Sessions par machine**.
3. Saisissez un nouveau nombre de sessions par machine.
4. Cliquez sur **Mettre à jour le nombre de sessions**.
5. Confirmez votre demande.

Cette modification n'affecte pas les sessions en cours. Lorsque vous modifiez le nombre maximum de sessions par une valeur inférieure à celle des sessions actuellement actives d'une machine, la nouvelle valeur est implémentée via l'attrition normale des sessions actives.

Si un échec survient avant le début du processus de mise à jour, l'affichage **Détails** du catalogue conserve le nombre correct de sessions. Si un échec survient pendant le processus de mise à jour, l'écran indique le nombre de sessions souhaitées.

Gérer les machines dans un catalogue

> **Remarque :**
>
> La plupart des actions disponibles dans le tableau de bord **Gérer > Déploiement rapide d'Azure** sont également disponibles à partir du tableau de bord **Surveiller** dans Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard for Azure service).

Pour sélectionner des actions dans le tableau de bord **Gérer > Déploiement rapide d'Azure** :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée d'un catalogue.
2. Dans l'onglet **Machines**, recherchez la machine que vous souhaitez gérer. Dans le menu des points de suspension de cette machine, sélectionnez l'action souhaitée :

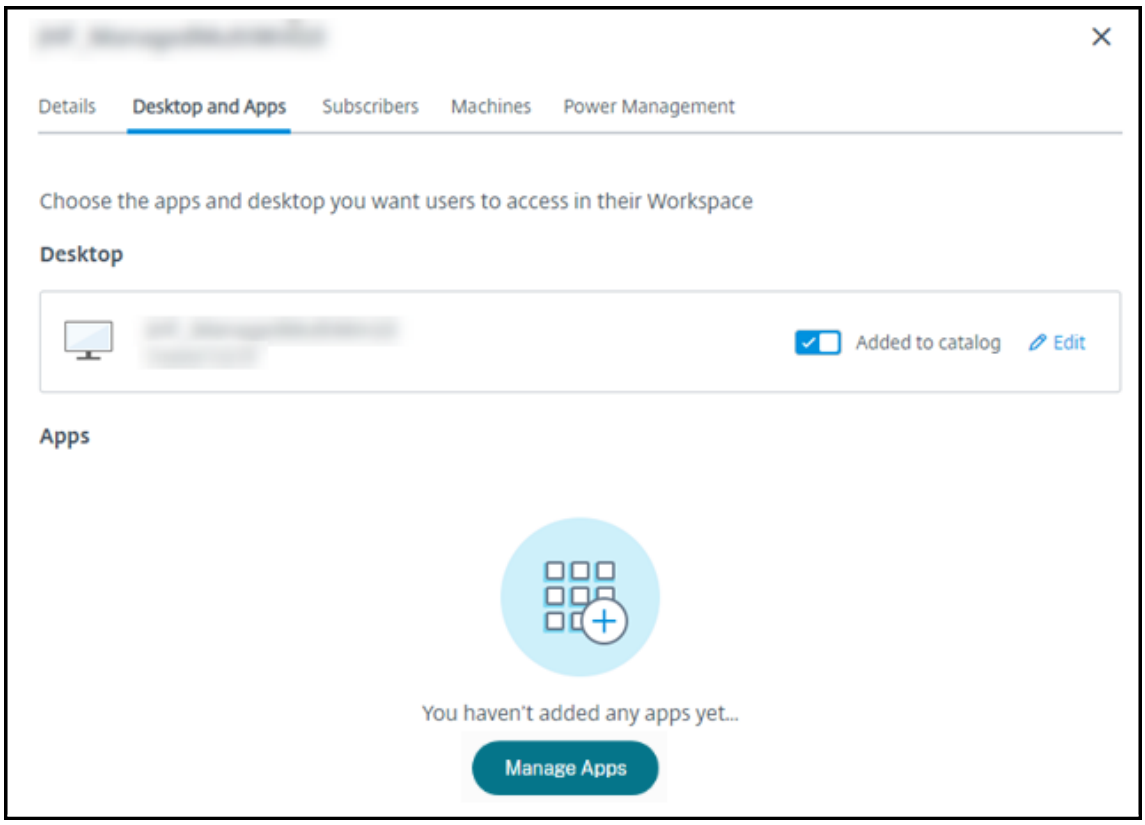
- **Redémarrer :** redémarrez la machine sélectionnée.
- **Démarrer :** démarrez la machine sélectionnée. Cette action n'est disponible que si la machine est hors tension.
- **Arrêt :** arrête la machine sélectionnée. Cette action n'est disponible que si la machine est sous tension.
- **Activer/désactiver le mode de maintenance :** Activez le mode de maintenance (s'il est désactivé) ou désactivez (s'il est activé) pour la machine sélectionnée.

  Par défaut, le mode de maintenance d'une machine est désactivé. L'activation du mode de maintenance pour une machine empêche l'établissement de nouvelles connexions à cette machine. L'utilisateur peut se connecter à des sessions existantes sur cette machine, mais ne peut pas démarrer de nouvelles sessions sur cette machine. Vous pouvez placer une machine en mode de maintenance avant d'appliquer des correctifs ou pour le dépannage.
- **Supprimer :** supprime la machine sélectionnée. Cette action est disponible uniquement lorsque le nombre de sessions de la machine est égal à zéro. Confirmez la suppression.

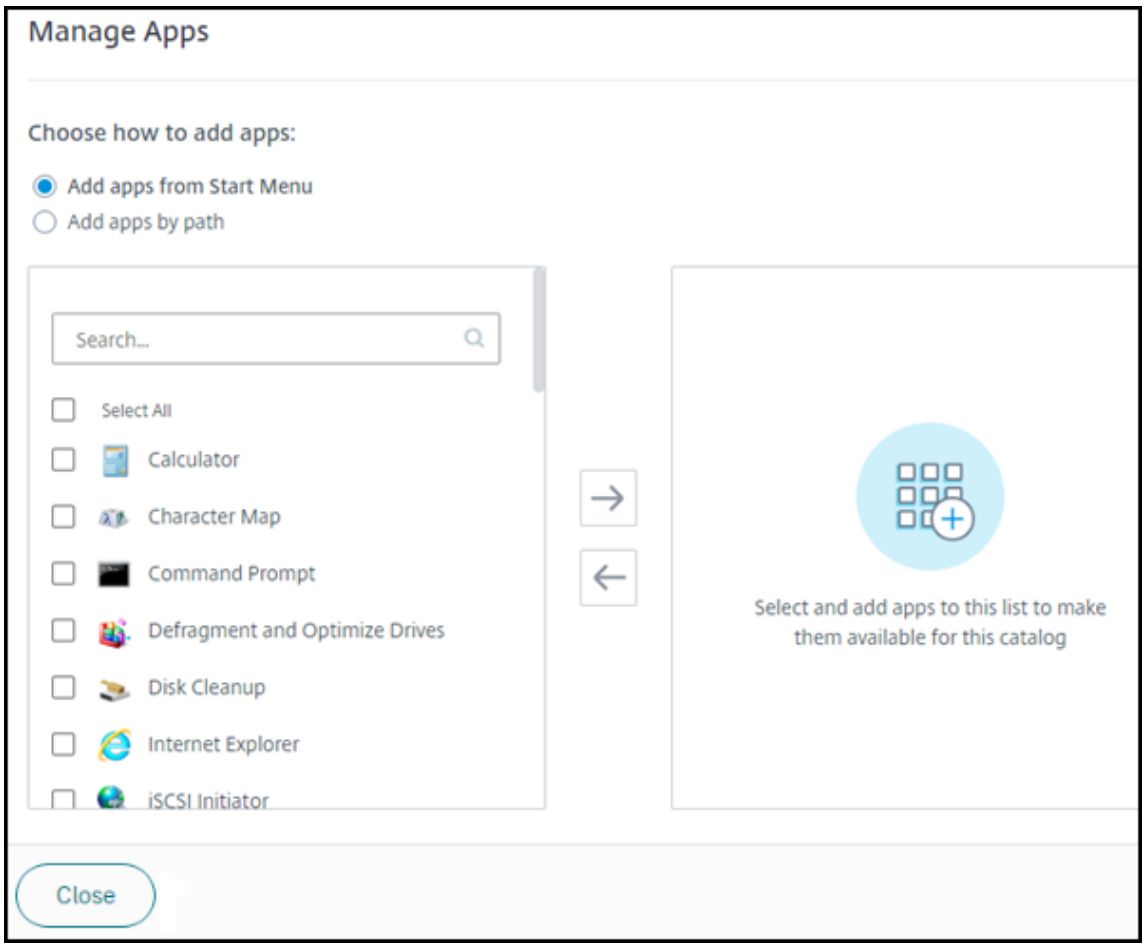
  Lorsqu'une machine est supprimée, toutes les données de la machine sont supprimées.
- **Forcer le redémarrage :** force le redémarrage de la machine sélectionnée. Sélectionnez cette action uniquement en cas d'échec d'une action de **redémarrage** de la machine.

Ajouter des applications à un catalogue

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Bureau et applications**, cliquez sur **Gérer les applications**.

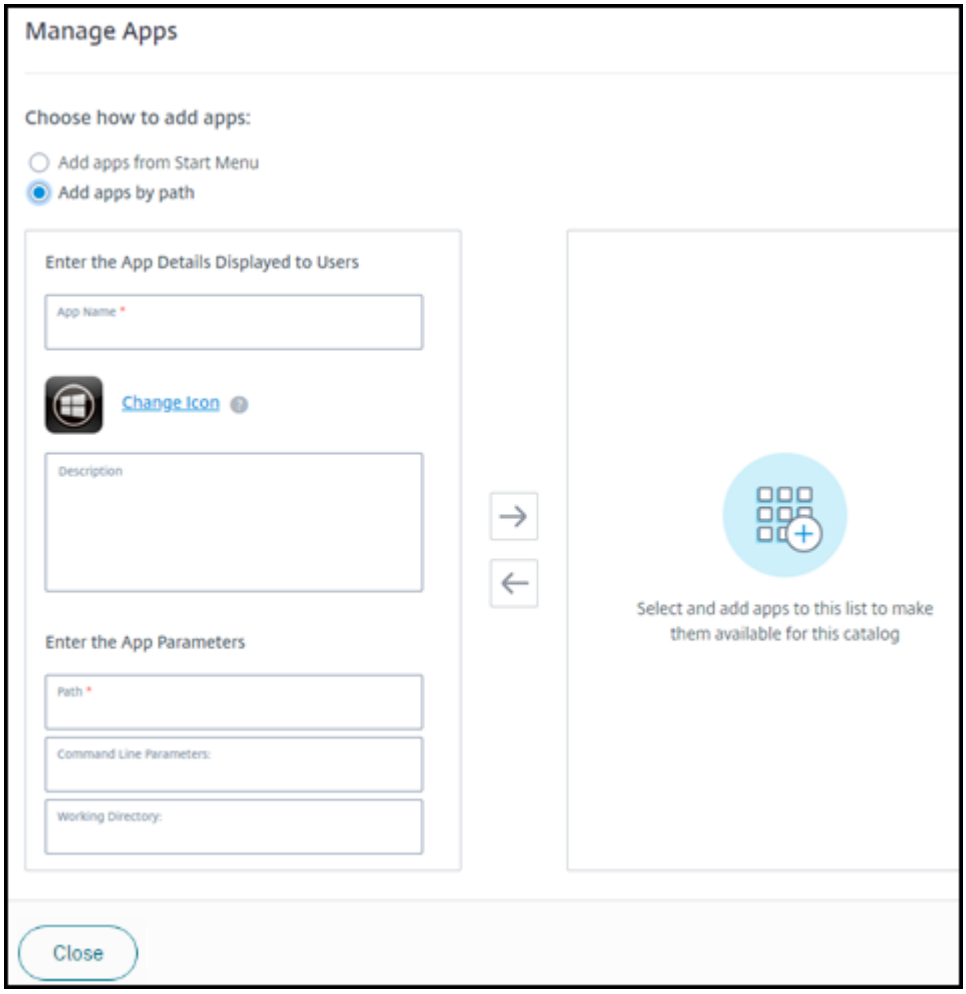


3. Sélectionnez la façon dont vous ajoutez des applications : dans le menu **Démarrer** des machines du catalogue ou à partir d'un autre chemin sur les machines.
4. Pour ajouter des applications à partir du menu **Démarrer** :



- Sélectionnez les applications disponibles dans la colonne de gauche. (Utilisez **la fonction de recherche** pour personnaliser la liste des applications.) Cliquez sur la flèche droite située entre les colonnes. Les applications sélectionnées se déplacent vers la colonne de droite.
- De même, pour supprimer des applications, sélectionnez-les dans la colonne de droite. Cliquez sur la flèche gauche entre les colonnes.
- Si le menu **Démarrer** contient plusieurs versions de la même application qui portent le même nom, vous ne pouvez en ajouter qu'une. Pour ajouter une autre version de cette application, modifiez le nom de cette version. Vous pourrez ensuite ajouter cette version de l'application.

5. Pour ajouter des applications par chemin d'accès :



- Saisissez le nom de l'application. Il s'agit du nom que les utilisateurs voient dans Citrix Workspace.
- L'icône affichée est l'icône que les utilisateurs voient dans Citrix Workspace. Pour sélectionner une autre icône, cliquez sur **Changer d'icône** et accédez à l'icône que vous souhaitez afficher.
- (Facultatif) Saisissez une description de l'application.
- Saisissez le chemin d'accès à l'application. Ce champ est obligatoire. Vous pouvez également ajouter des paramètres de ligne de commandes et le répertoire de travail. Pour plus d'informations sur les paramètres de ligne de commande, voir Transmettre des paramètres aux applications publiées.

6. Lorsque vous avez terminé, cliquez sur **Fermer**.

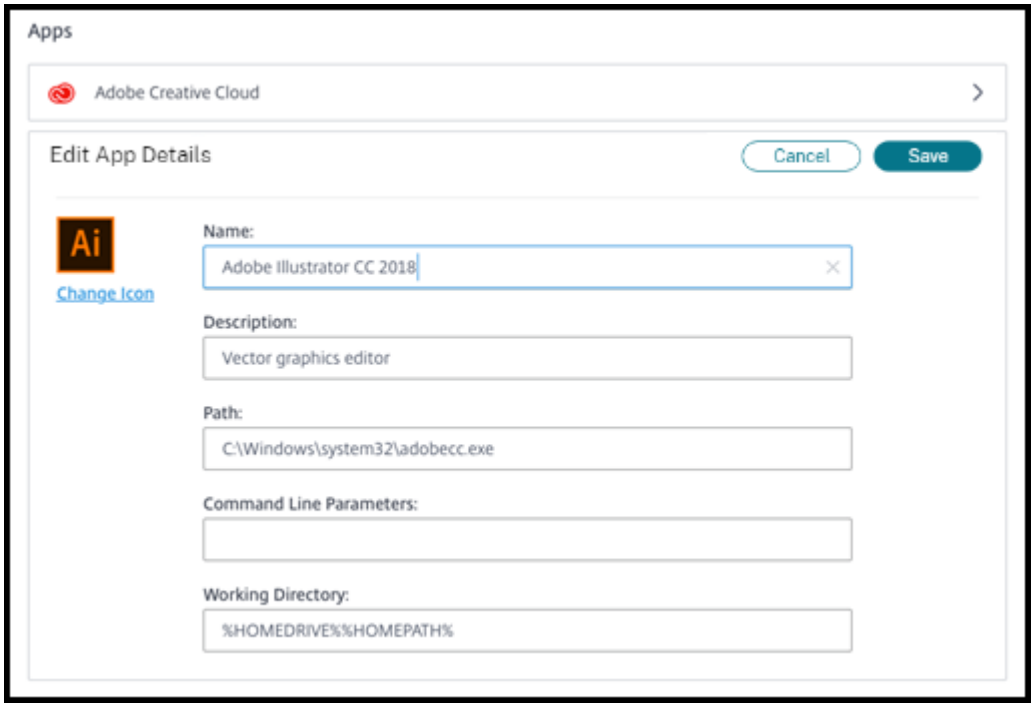
Que faire ensuite (si vous terminez le processus de création et de diffusion du catalogue) : envoyez l'URL Citrix Workspace à vos utilisateurs, si ce n'est déjà fait.

Sur les VDA Windows Server 2019, certaines icônes d'application peuvent ne pas apparaître correctement pendant la configuration et dans l'espace de travail des utilisateurs. Pour résoudre le problème,

une fois l'application publiée, modifiez l'application et utilisez la fonction **Changer d'icône** pour attribuer une autre icône qui s'affiche correctement.

Modifier une application dans un catalogue

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Bureau et applications**, cliquez n'importe où sur la ligne contenant l'application que vous souhaitez modifier.
3. Cliquez sur l'icône représentant un crayon .



4. Saisissez vos modifications dans l'un des champs suivants :
   - **Nom :** le nom que les utilisateurs voient dans Citrix Workspace.
   - **Description**
   - **Chemin :** chemin d'accès à l'exécutable.
   - **Paramètres de ligne de commande :** pour plus d'informations, voir Passer des paramètres aux applications publiées.
   - **Répertoire de travail**
5. Pour modifier l'icône que les utilisateurs voient dans leur Citrix Workspace, cliquez sur **Modifier l'icône** et accédez à l'icône que vous souhaitez afficher.
6. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Passer des paramètres aux applications publiées

Lorsque vous associez des types de fichier à une application publiée, les symboles pourcentage et astérisque (entre guillemets) sont ajoutés à la fin de la ligne de commandes de l'application. Ces symboles réservent l'emplacement des paramètres transmis aux machines utilisateur.

- Si une application publiée ne démarre pas, vérifiez que la ligne de commandes contient les symboles appropriés. Par défaut, les paramètres fournis par les machines utilisateur sont validés lorsque les symboles sont ajoutés.

  Pour les applications publiées qui utilisent des paramètres personnalisés fournis par la machine utilisateur, les symboles sont ajoutés à la ligne de commandes pour éviter la validation de ligne de commandes. Si ces symboles n'apparaissent pas dans la ligne de commande d'une application, vous pouvez les ajouter manuellement.

- Si le chemin d'accès du fichier exécutable comprend des noms de répertoire avec des espaces, (« C:\Program Files », par exemple), mettez la ligne de commande de l'application entre guillemets afin d'indiquer que l'espace fait partie de la ligne de commande. Pour ce faire, ajoutez des guillemets autour du chemin d'accès et des guillemets autour des symboles pourcentage et astérisque. Ajoutez une espace entre le guillemet de clôture du chemin et le guillemet d'ouverture pour les symboles de pourcentage et d'astérisque.

  Par exemple, la ligne de commandes pour l'application publiée Windows Media Player est : `“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”`

Supprimer des applications d'un catalogue

La suppression d'une application d'un catalogue ne la supprime pas des machines. Elle l'empêche simplement d'apparaître dans Citrix Workspace.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Bureau et applications**, cliquez sur l'icône de corbeille en regard des applications que vous souhaitez supprimer.

Supprimer un catalogue

Lorsque vous supprimez un catalogue, toutes les machines du catalogue sont définitivement détruites. La suppression d'un catalogue ne peut pas être annulée.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.

2. Sous l'onglet **Détails**, cliquez sur **Supprimer le catalogue** dans la partie inférieure de la fenêtre.
3. Confirmez la suppression en cochant les cases d'accusé de réception, puis en cliquant sur le bouton de confirmation.

Pour aider à identifier les comptes de machines Active Directory résiduels que vous devez supprimer, vous pouvez télécharger une liste de noms de machines et de Cloud Connector.

Gérer les calendriers de gestion de l'alimentation

Un calendrier de gestion de l'alimentation concerne toutes les machines d'un catalogue. Un calendrier assure :

- Une expérience utilisateur optimale : les machines sont disponibles pour les utilisateurs lorsqu'elles sont nécessaires.
- La sécurité : les sessions de bureau qui restent inactives pendant un intervalle spécifié sont déconnectées, ce qui oblige l'utilisateur à lancer une nouvelle session dans son espace de travail.
- La gestion des coûts et des économies d'énergie : les machines dont les bureaux restent inactifs sont mises hors tension. Les machines sont sous tension pour répondre à la demande planifiée et réelle.

Vous pouvez configurer un calendrier de gestion de l'alimentation lorsque vous créez un catalogue personnalisé ou le faire ultérieurement. Si aucun calendrier n'est sélectionné ou configuré, une machine s'éteint à la fin d'une session.

Vous ne pouvez pas sélectionner ou configurer un calendrier de gestion de l'alimentation lorsque vous créez un catalogue avec la création rapide. Par défaut, les catalogues créés à l'aide de la création rapide utilisent le calendrier prédéfini Économique. Vous pouvez sélectionner ou configurer un calendrier différent ultérieurement pour ce catalogue.

La gestion du calendrier comprend :

- connaître les informations contenues dans un calendrier ;
- créer un calendrier.

Informations contenues dans un calendrier

Le diagramme suivant illustre les paramètres de calendrier d'un catalogue contenant des machines à sessions multiples. Les paramètres d'un catalogue diffèrent légèrement s'il contient des machines à session unique (aléatoires ou statiques).

Un calendrier de gestion de l'alimentation contient les informations suivantes.

Calendriers prédéfinis Citrix DaaS pour Azure propose plusieurs planifications prédéfinies. Vous pouvez également configurer et enregistrer des calendriers personnalisés. Bien que vous puissiez supprimer des horaires prédéfinis personnalisés, vous ne pouvez pas supprimer les horaires prédéfinis fournis par Citrix.

Fuseau horaire Utilisé avec le réglage des machines sous tension pour établir les heures de travail et après les heures de travail, en fonction du fuseau horaire sélectionné.

Ce paramètre est valide pour tous les types de machines.

Machines sous tension : heures de travail et après les heures de travail Les jours de la semaine et les heures de début/fin de la journée qui constituent vos heures de travail. Ce paramètre indique généralement les intervalles où vous souhaitez que les machines soient sous tension. Tout moment en dehors de ces intervalles est considéré comme étant après les heures de travail. Plusieurs paramètres de calendrier vous permettent de saisir des valeurs distinctes pour les heures de travail et après les heures de travail. D'autres paramètres s'appliquent en permanence.

Ce paramètre est valide pour tous les types de machines.

Déconnecter les sessions de bureau en cas d'inactivité La durée d'inactivité d'un bureau (le temps où celui-ci n'est pas utilisé) avant que la session ne soit déconnectée. Une fois qu'une session est déconnectée, l'utilisateur doit accéder à Workspace et redémarrer un bureau. Il s'agit d'un paramètre de sécurité.

Ce paramètre est valide pour tous les types de machines. Un seul paramètre s'applique en permanence.

Éteindre les bureaux inactifs Il s'agit du temps qu'une machine peut rester déconnectée avant d'être mise hors tension. Une fois qu'une machine est mise hors tension, l'utilisateur doit se rendre dans Workspace et redémarrer un bureau. Il s'agit d'un paramètre d'économie d'énergie.

Par exemple, supposons que vous souhaitiez que les bureaux se déconnectent après avoir été inactifs pendant 10 minutes. Ensuite, mettez les machines hors tension si elles restent déconnectées pendant 15 minutes supplémentaires.

Si Tom cesse d'utiliser son bureau pour assister à une réunion d'une heure, le bureau sera déconnecté au bout de 10 minutes. Après 15 minutes supplémentaires, la machine sera mise hors tension (25 minutes au total).

Du point de vue de l'utilisateur, les deux paramètres d'inactivité (déconnexion et mise hors tension) ont le même effet. Si Tom s'éloigne de son bureau pendant 12 minutes ou une heure, il doit redémarrer un bureau depuis Workspace. La différence entre les deux horloges affecte l'état de la machine virtuelle fournissant le bureau.

Ce paramètre est valide pour les machines à session unique (statiques ou aléatoires). Vous pouvez saisir des valeurs pour les heures de travail et après les heures de travail.

Fermer les sessions déconnectées Il s'agit du temps qu'une machine peut rester déconnectée avant la fermeture de la session.

Ce paramètre est valide pour les machines à sessions multiples. Un seul paramètre s'applique en permanence.

Délai de mise hors tension Il s'agit de la durée minimale pendant laquelle une machine doit être mise sous tension avant d'être éligible à la mise hors tension (ainsi que d'autres critères). Ce paramètre empêche les machines de s'allumer et de s'éteindre sans cesse pendant les demandes de session volatiles.

Ce paramètre est valide pour les machines à sessions multiples et s'applique en permanence.

Nombre minimum de machines en fonctionnement Il s'agit du nombre de machines qui doivent rester sous tension, indépendamment de la durée pendant laquelle elles sont inactives ou déconnectées.

Ce paramètre est valide pour les machines aléatoires et à sessions multiples. Vous pouvez saisir des valeurs pour les heures de travail et après les heures de travail.

Tampon de capacité Un tampon de capacité permet de répondre aux pics soudains de la demande, en gardant un tampon de machines sous tension. Le tampon est indiqué en pourcentage de la demande de session actuelle. Par exemple, s'il y a 100 sessions actives et que le tampon de capacité est de 10 %, Citrix DaaS pour Azure fournit une capacité de 110 sessions. Un pic de demande peut survenir pendant les heures de travail ou l'ajout de nouvelles machines au catalogue.

Une valeur moindre diminue le coût. Une valeur supérieure contribue à assurer une expérience utilisateur optimisée. Lors du lancement de sessions, l'utilisateur n'a pas besoin d'attendre que des machines supplémentaires s'allument.

Lorsqu'un nombre plus que suffisant de machines est présent pour prendre en charge le nombre de machines sous tension nécessaires dans le catalogue (y compris le tampon de capacité), les machines supplémentaires sont mises hors tension. La mise hors tension peut se produire en raison d'une heure creuse, de fermetures de session ou d'un nombre réduit de machines dans le catalogue. La décision d'éteindre une machine doit répondre aux critères suivants :

- La machine est sous tension et n'est pas en mode de maintenance.
- La machine est enregistrée comme disponible ou attend de s'enregistrer après la mise sous tension.
- La machine n'a aucune session active. Toutes les sessions restantes sont terminées. (La machine était inactive pendant la période d'inactivité.)

- La machine est sous tension pendant au moins « X » minutes, où « X » correspond au délai de mise hors tension spécifié pour le catalogue.

  Dans un catalogue statique, une fois que toutes les machines du catalogue sont affectées, le tampon de capacité ne joue aucun rôle dans la mise sous tension ou hors tension des machines.

Ce paramètre est valide pour tous les types de machines. Vous pouvez saisir des valeurs pour les heures de travail et après les heures de travail.

Créer un calendrier de gestion de l'alimentation

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Gestion de l'alimentation**, déterminez si l'un des calendriers prédéfinis (dans le menu en haut) répondent à vos besoins. Sélectionnez un préréglage pour voir les valeurs qu'il utilise. Si vous souhaitez utiliser un préréglage, laissez-le sélectionné.
3. Si vous modifiez les valeurs de n'importe quel champ (par exemple, jours, heures ou intervalles), la sélection de préréglage passe automatiquement à **Personnalisé**. Un astérisque indique que les paramètres personnalisés n'ont pas été enregistrés.
4. Définissez les valeurs souhaitées pour le calendrier personnalisé.
5. Cliquez sur **Personnalisé** en haut et enregistrez les paramètres actuels en tant que nouveau préréglage. Entrez un nom pour le nouveau préréglage et cliquez sur la coche.
6. Lorsque vous avez terminé, cliquez sur **Enregistrer les modifications**.

Vous pourrez par la suite modifier ou supprimer un préréglage personnalisé à l'aide des icônes de crayon ou de corbeille du menu **Préréglages**. Vous ne pouvez pas modifier ou supprimer des préréglages courants.

Instantané et restauration du VDA

Les fonctionnalités de snapshot et de restauration de Citrix DaaS pour Azure permettent de récupérer des données après une perte de données imprévue ou d'autres défaillances dans les VDA qui fournissent des postes de travail et des applications. L'opération d'instantané prend et stocke un instantané de la machine. Ultérieurement, une opération de restauration utilise un instantané que vous sélectionnez.

- Vous pouvez configurer des programmes d'instantanés quotidiens et hebdomadaires pour toutes les machines d'un catalogue. Ces instantanés sont appelés *instantanés automatiques*. Un instantané est pris de chaque machine du catalogue. Il n'existe aucun programme d'instantanés par défaut.

- Vous pouvez sauvegarder un seul V dans un catalogue à la demande. C'est ce qu'on appelle un instantané manuel. Vous pouvez créer un *instantané manuel* d'une machine même si le catalogue auquel elle appartient contient des instantanés planifiés. (Toutefois, vous ne pouvez pas planifier d'instantanés sur une seule machine.)

> **Important :**
>
> Les fonctionnalités d'instantané et de restauration de Citrix DaaS pour Azure sont prises en charge uniquement pour les machines des catalogues statiques et attribuées aux utilisateurs.

Programmes d'instantanés

N'oubliez pas : les programmes d'instantanés s'appliquent à toutes les machines d'un catalogue.

Par défaut, il n'existe aucun programme d'instantanés.

Pour gérer les programmes d'instantanés :

1. Dans le tableau de bord **Gérer**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Détails**, cliquez sur **Planifier des instantanés**.
3. Sur la page **Planifier des instantanés**, configurez des planifications pour des instantanés automatiques hebdomadaires ou quotidiens, ou les deux :
    - Pour ajouter ou modifier des instantanés hebdomadaires, déplacez le curseur des **instantanés automatiques hebdomadaires** jusqu'à ce qu'une coche apparaisse. Sélectionnez le jour de la semaine et l'heure de début.
    - Pour ajouter ou modifier des instantanés quotidiens, déplacez le curseur des **instantanés automatiques quotidiens** jusqu'à ce qu'une coche apparaisse. Sélectionnez l'heure de début.
    - Pour supprimer des instantanés hebdomadaires, déplacez le curseur des **instantanés automatiques hebdomadaires** jusqu'à ce qu'un **X** apparaisse.
    - Pour supprimer des instantanés quotidiens, déplacez le curseur des **instantanés automatiques quotidiens** jusqu'à ce qu'un **X** apparaisse.
4. Lorsque vous avez terminé, cliquez sur **Enregistrer** en bas de la page.

Instantanés manuels

Un instantané manuel est destiné à une seule machine d'un catalogue. (Vous ne pouvez pas créer de planification pour prendre un instantané de machines individuelles.)

1. Dans le tableau de bord **Gérer**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Machines**, recherchez la machine dont vous souhaitez prendre un instantané. Sélectionnez **Instantanés** dans le menu des points de suspension de cette machine.

3. Sur la page **Snapshots for *VDA-Name***, cliquez sur **Create Manual Snapshot**.
4. Indiquez un nom pour l'instantané. Recommandé : Choisissez un nom que vous pourrez facilement identifier ultérieurement.
5. Confirmez votre demande.

Afficher et gérer les instantanés

1. Dans le tableau de bord **Gérer**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Machines**, recherchez la machine dont vous souhaitez prendre un instantané. Sélectionnez **Instantanés** dans le menu des points de suspension de cette machine.
3. Sur la page **Sauvegardes pour *VDA-Name*** :

    - S'il n'existe aucun instantané pour la machine, un message vous indique de créer un instantané manuel pour cette machine ou de créer des instantanés planifiés pour toutes les machines du catalogue contenant cette machine.
    - Vous pouvez sélectionner l'un des instantanés et restaurer la machine. Voir Restaurer.
    - Vous pouvez supprimer des instantanés. Activez les cases à cocher correspondant à un ou plusieurs clichés, puis cliquez sur **Supprimer** dans l'en-tête du tableau. Confirmez votre demande.

Conseil : lorsque vous supprimez un catalogue, tous les instantanés sont détruits.

Restaurer

Vous pouvez restaurer une machine à partir de n'importe quel instantané disponible pour cette machine.

Lors d'une restauration, la machine est mise hors tension. Aucune des actions du menu des points de suspension d'une machine n'est disponible pendant la restauration d'un instantané.

1. Dans le tableau de bord **Gérer**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Machines**, recherchez la machine dont vous souhaitez prendre un instantané. Sélectionnez **Instantanés** dans le menu des points de suspension de cette machine.
3. Sur la page **Snapshots for *VDA-name page**, cochez la case de l'instantané que vous souhaitez utiliser.
4. Cliquez sur **Restaurer** dans l'en-tête du tableau.
5. Confirmez la demande.

La colonne **État** de l'onglet **Machines** indique la progression et le résultat de l'opération de restauration.

Si un ordinateur ne parvient pas à restaurer un instantané, réessayez.

Informations connexes

- Mettre à jour un catalogue avec une nouvelle image
- Ajouter et supprimer des utilisateurs dans un catalogue
- Membre d'un domaine et non joint à un domaine

Surveiller

May 9, 2023

À partir du tableau de bord **Surveiller**, vous pouvez afficher l'utilisation du bureau, les sessions et les machines dans votre déploiement Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure). Vous pouvez également contrôler les sessions, gérer l'alimentation des machines et mettre fin aux applications et aux processus en cours d'exécution.

Pour accéder au tableau de bord **Surveiller** :

1. Connectez-vous à Citrix Cloud si vous ne l'avez pas déjà fait. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**.
2. Dans le tableau de bord **Gérer**, cliquez sur l'onglet **Surveiller** .

Surveiller l'utilisation du bureau

Les affichages sur cette page sont actualisés toutes les cinq minutes.

- **Vue d'ensemble de la machine et des sessions :** vous pouvez adapter l'affichage pour afficher des informations sur tous les catalogues (par défaut) ou sur un catalogue sélectionné. Vous pouvez également personnaliser la période : le dernier jour, la dernière semaine ou le dernier mois.

  Les chiffres en haut de l'écran indiquent le nombre total de machines, plus le nombre de machines sous tension et hors tension. Survolez une valeur pour afficher le nombre de machines en session unique et en sessions multiples.

  Le graphique situé sous les décomptes montre le nombre de machines sous tension et de sessions simultanées de pointe à intervalles réguliers pendant la période que vous avez sélectionnée. Survolez un point du graphique pour afficher les décompte à ce moment précis.

- **Top 10 :** pour personnaliser un affichage Top 10, sélectionnez une période : la dernière semaine (par défaut), le dernier mois ou les trois derniers mois. Vous pouvez également adapter l'affichage pour afficher uniquement des informations sur l'activité impliquant des machines à session unique, à sessions multiples ou des applications.
  - **Top 10 des utilisateurs actifs :** répertorie les utilisateurs qui ont démarré des bureaux le plus fréquemment pendant la période. Survoler une ligne affiche le nombre total de bureaux lancés.
  - **Top 10 des catalogues actifs :** répertorie les catalogues dont la durée est la plus longue pendant la période sélectionnée. La durée est la somme de toutes les sessions utilisateur de ce catalogue.

Rapport sur l'utilisation du bureau

Pour télécharger un rapport contenant des informations sur les lancements de machines au cours du dernier mois, cliquez sur **Launch Activity**. Un message indique que la demande est en cours de traitement. Le rapport est automatiquement téléchargé vers l'emplacement de téléchargement par défaut sur la machine locale.

Filtrer et rechercher pour surveiller les machines et les sessions

Lorsque vous surveillez les informations de session et de machine, toutes les machines ou sessions sont affichées par défaut. Vous pouvez :

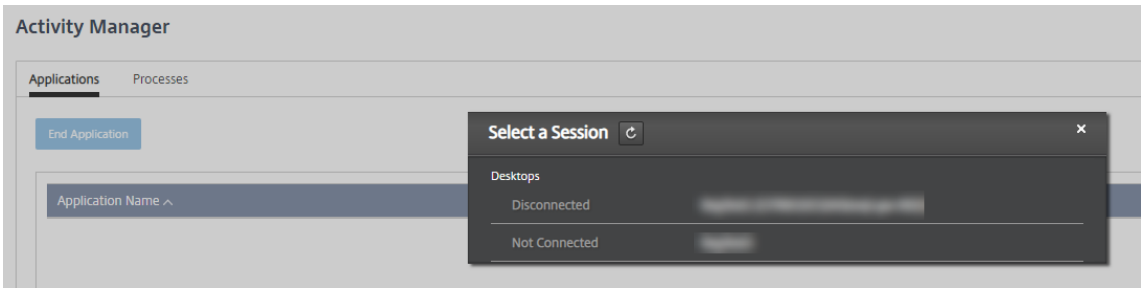
- filtrer l'affichage par machines, sessions, connexions ou applications ;
- affiner l'affichage des sessions ou des machines en choisissant les critères souhaités, en créant un filtre à l'aide d'expressions ;

- enregistrer les filtres que vous créez pour les réutiliser.

Contrôler les applications d'un utilisateur

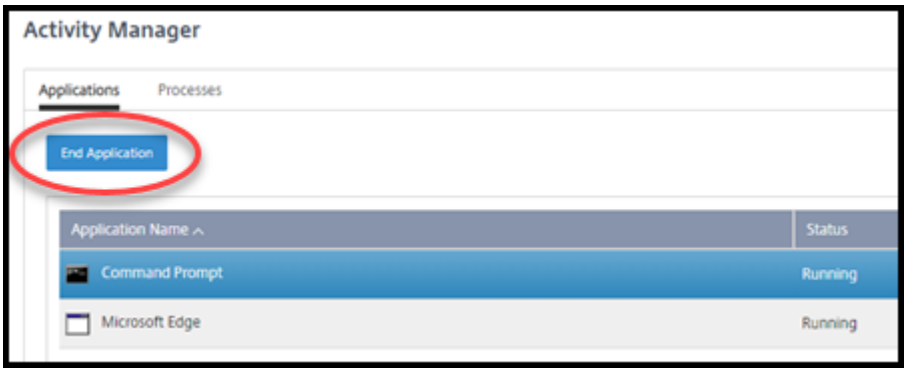
Vous pouvez afficher et gérer des applications et des processus pour un utilisateur disposant d'une session en cours d'exécution ou ayant un bureau attribué.

1. Dans le tableau de bord **Surveiller**, cliquez sur **Rechercher** et entrez le nom d'utilisateur (ou les premiers caractères du nom d'utilisateur), de la machine ou du point de terminaison. Dans les résultats de la recherche, sélectionnez l'article que vous recherchez. (Pour réduire la zone de recherche sans effectuer de recherche, cliquez à nouveau sur **Rechercher**.)
2. Sélectionnez une session.



   Le Gestionnaire d'activités répertorie les applications et les processus de la session de l'utilisateur.

3. Pour mettre fin à une application, sous l'onglet **Applications** du Gestionnaire d'activités, cliquez sur la ligne de l'application pour sélectionner cette application, puis cliquez sur Mettre **fin à l'application**.



4. Pour mettre fin à un processus, dans l'onglet **Processus** du Gestionnaire d'activités, cliquez sur la ligne du processus pour sélectionner ce processus, puis cliquez sur **Terminer le processus**.
5. Pour afficher les détails de la session, cliquez sur **Détails** dans l'angle supérieur droit. Pour revenir à l'affichage des applications et des processus, cliquez sur Gestionnaire d'activités dans l'angle supérieur droit.

6. Pour contrôler la session, cliquez sur **Contrôle de session > Déconnexion** ou **Contrôle de session > Déconnecter**.

Observer les utilisateurs

Utilisez la fonction d'observation pour afficher ou travailler directement sur la machine virtuelle ou la session d'un utilisateur. Vous pouvez observer des VDA Windows et Linux. L'utilisateur doit être connecté à la machine que vous souhaitez observer. Vérifiez ceci en examinant le nom de la machine dans la barre de titre `User`.

L'observation se lance dans un nouvel onglet de navigateur. Assurez-vous que votre navigateur autorise les fenêtres contextuelles à partir de l'URL Citrix Cloud.

Dans un abonnement Azure géré par Citrix, l'observation n'est prise en charge que pour les utilisateurs sur des machines jointes à un domaine. Pour observer une machine non jointe à un domaine dans le cadre d'un abonnement Azure géré par Citrix, vous devez configurer une machine bastion. Pour plus de détails, voir Accéder au Bastion.

L'observation doit être initiée à partir d'une machine sur le même réseau virtuel que les machines jointes au domaine, et répondre à toutes les exigences de port.

Activer l'observation

1. Dans le tableau de bord **Monitor**, accédez à la vue **Détails de l'utilisateur** .
2. Sélectionnez la session utilisateur, puis cliquez sur **Ombre** dans la vue **Gestionnaire d'activités** ou dans le panneau **Détails de la session** .

Observer les VDA Linux

L'observation est disponible pour les VDA Linux versions 7.16 ou ultérieures exécutant les distributions Linux RHEL7.3 ou Ubuntu version 16.04.

Surveiller utilise le nom de domaine complet pour se connecter au VDA Linux cible. Assurez-vous que le client du service de surveillance peut résoudre le nom de domaine complet du VDA Linux.

- Les paquets `python-websockify` et `x11vnc` doivent être installés sur le VDA.
- La connexion `noVNC` au VDA utilise le protocole WebSocket. Par défaut, le protocole WebSocket `ws://` est utilisé. Pour des raisons de sécurité, Citrix recommande que vous utilisiez le protocole `wss://` sécurisé. Installez des certificats SSL sur chaque client du service de surveillance et VDA Linux.

Suivez les instructions dans Observation de session pour configurer votre VDA Linux pour l'observation.

1. Une fois que vous avez activé l'observation, la connexion de l'observation démarre et une invite de confirmation s'affiche sur la machine utilisateur.
2. Demandez à l'utilisateur de cliquer sur **Oui** pour démarrer la machine ou le partage de session.
3. L'administrateur peut afficher uniquement la session observée.

Observer des VDA Windows

Les sessions de VDA Windows sont observées à l'aide de l'Assistance à distance Windows. Activez la fonctionnalité `Use Windows Remote Assistance` lors de l'installation du VDA.

1. Une fois que vous avez activé l'observation, la connexion d'observation démarre et une boîte de dialogue vous invite à ouvrir ou à enregistrer le fichier `.msrc incident`.
2. Ouvrez le fichier d'incident avec la visionneuse d'assistance à distance, si elle n'est pas déjà sélectionnée par défaut. Une invite de confirmation s'affiche sur la machine utilisateur.
3. Demandez à l'utilisateur de cliquer sur **Oui** pour démarrer la machine ou le partage de session.
4. Pour un contrôle supplémentaire, demandez à l'utilisateur de partager le contrôle du clavier et de la souris.

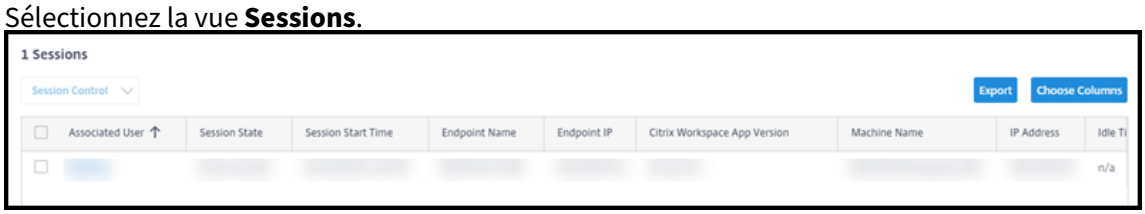
Surveillance et contrôle des sessions

Les écrans de session sont mis à jour chaque minute.

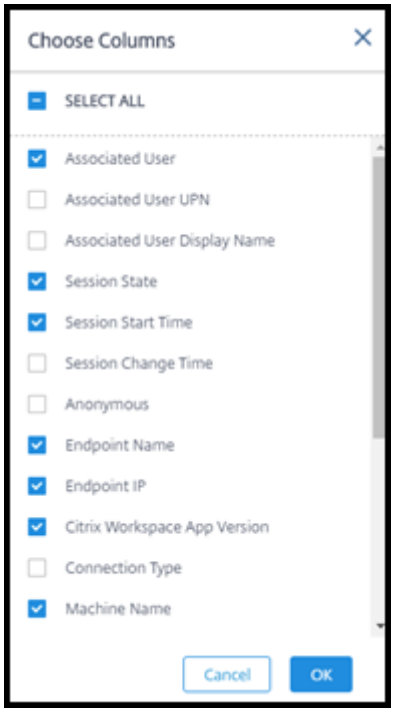
En plus de l'affichage des sessions, vous pouvez déconnecter une ou plusieurs sessions ou fermer la session des utilisateurs.

1. Dans le tableau de bord **Surveiller**, cliquez sur **Filtres**.

2. Sélectionnez la vue **Sessions**.



3. Pour personnaliser l'affichage, cliquez sur **Choisir des colonnes** et activez les cases à cocher des éléments à afficher. Lorsque vous avez terminé, cliquez sur **OK**. L'affichage des sessions est automatiquement actualisé.



4. Cochez la case située à gauche de chaque session que vous souhaitez contrôler.
5. Pour fermer ou déconnecter la session, sélectionnez **Contrôle de session > Fermer la session** ou **Contrôle de session > Déconnecter**.

N'oubliez pas que le programme de gestion de l'alimentation du catalogue peut également contrôler la déconnexion des sessions et la déconnexion des utilisateurs des sessions déconnectées.

Au lieu de suivre la procédure ci-dessus, vous pouvez également **rechercher** un utilisateur, sélectionner la session que vous souhaitez contrôler, puis afficher les détails de la session. Les options de fermeture de session et de déconnexion y sont également disponibles.

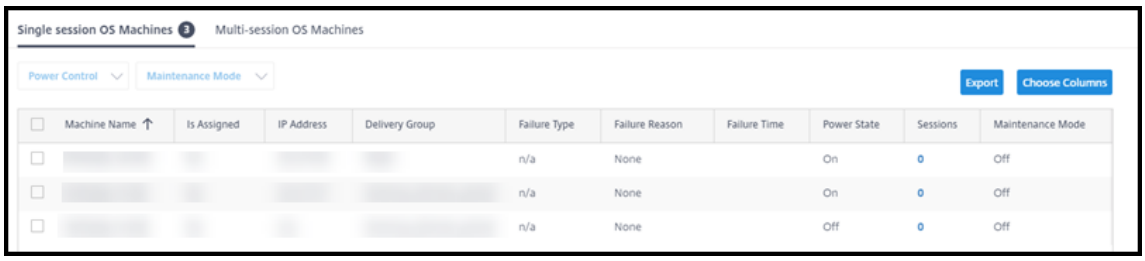
Rapport d'informations sur la session

Pour télécharger les informations de session, cliquez sur **Exporter** sur l'affichage des sessions. Un message indique que la demande est en cours de traitement. Le rapport est automatiquement téléchargé vers l'emplacement de téléchargement par défaut sur la machine locale.

Surveiller et contrôler l'alimentation des machines

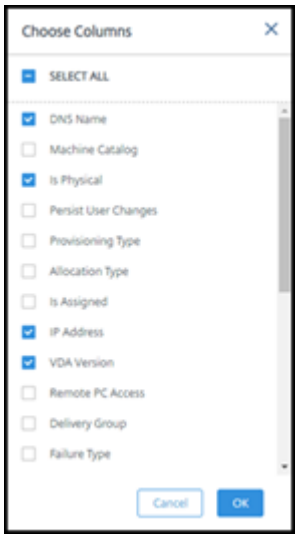
Les écrans des machines sont mis à jour toutes les minutes.

1. Dans le tableau de bord **Surveiller**, cliquez sur **Filtres**.
2. Sélectionnez la vue **Machines**.

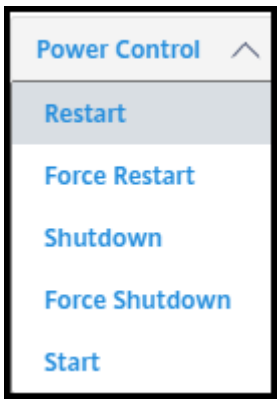


Par défaut, l'affichage répertorie les machines avec OS mono-session. Vous pouvez également afficher des machines à sessions multiples.

3. Pour personnaliser l'affichage, cliquez sur **Choisir des colonnes** et activez les cases à cocher des éléments à afficher. Lorsque vous avez terminé, cliquez sur **OK**. L'écran des machines est automatiquement actualisé.



4. Pour contrôler l'alimentation des machines ou les placer en mode maintenance ou en dehors, cochez la case située à gauche de chaque machine que vous souhaitez contrôler.
5. Pour contrôler l'alimentation des machines sélectionnées, cliquez sur **Contrôle de l'alimentation** et sélectionnez une action.



6. Pour placer les machines sélectionnées en mode de maintenance ou en dehors, cliquez sur Mode de **maintenance > Activé** ou **Mode de maintenance > Désactivé**.

Lorsque vous utilisez la fonction de recherche pour rechercher et sélectionner une machine, vous voyez les détails de la machine, son utilisation, son historique d'utilisation (au cours des sept derniers jours) et la moyenne des IOPS.

Rapport d'informations sur la machine

Pour télécharger les informations de session, cliquez sur **Exporter** sur l'affichage des machines. Un message indique que la demande est en cours de traitement. Le rapport est automatiquement téléchargé vers l'emplacement de téléchargement par défaut sur la machine locale.

Vérification de l'état des applications et du bureau

La vérification de l'intégrité automatise le processus de vérification de l'état des applications et des bureaux publiés. Les résultats de la vérification de l'intégrité sont disponibles via le tableau de bord **Surveiller**. Pour plus de détails, consultez :

- Analyse d'application
- Analyse de bureaux

Citrix DaaS pour Azure pour les fournisseurs de services Citrix

September 7, 2022

Cet article décrit comment les fournisseurs de services Citrix (CSP) peuvent configurer Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour le service Azure) pour les clients (locataires) dans Citrix Cloud.

Pour obtenir une vue d'ensemble des fonctionnalités disponibles pour Citrix Partners, reportez-vous à la section Citrix Cloud pour les partenaires.

Exigences

- Vous êtes un partenaire Citrix Service Provider.
- Vous disposez d'un compte Citrix Cloud.
- Vous avez un abonnement à Citrix DaaS pour Azure.

Limitations

- Les changements de nom de client peuvent prendre jusqu'à 24 heures pour s'appliquer à toutes les interfaces.
- Lors de la création d'un client, l'adresse e-mail doit être unique.

Problèmes connus

- Une fois que l'utilisateur d'un client est affecté à une ressource, vous ne pouvez pas le supprimer ou le désaffecter.
- La console de gestion n'applique pas la séparation des utilisateurs des clients. Vous êtes responsable de l'ajout d'utilisateurs aux catalogues et ressources appropriés.

Ajouter un client

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Cliquez sur **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord **du client**, cliquez sur **Inviter ou Ajouter**. Entrez les informations demandées.

   Si le client n'a pas de compte Citrix Cloud, l'ajout du client crée un compte. L'ajout du client vous ajoute automatiquement en tant qu'administrateur d'accès complet du compte de ce client.
3. Si le client dispose d'un compte Citrix Cloud :

   a) Une URL Citrix Cloud s'affiche, que vous copiez et envoyez au client. Pour plus de détails sur ce processus, consultez la section Inviter un client à se connecter.
   b) Le client doit vous ajouter en tant qu'administrateur d'accès complet à son compte. Voir Ajouter des administrateurs à un compte Citrix Cloud.

Vous pouvez ajouter d'autres administrateurs ultérieurement et contrôler les clients qu'ils peuvent voir sur les tableaux de bord Citrix DaaS pour Azure **Manage** and **Monitor** .

Ajouter Citrix DaaS pour Azure à un client

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Cliquez sur **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord du **client**, sélectionnez **Ajouter un service** dans le menu représentant des points de suspension pour le client.
3. Dans **Select a Service to Add**, cliquez sur **Citrix DaaS Standard pour Azure**.
4. Cliquez sur **Continuer**.

Une fois cette procédure terminée, le client est intégré à votre abonnement Citrix DaaS pour Azure.

Une fois l'intégration terminée, un nouveau client est automatiquement créé dans Citrix DaaS pour Azure. Le client est visible dans **Gérer > Déploiement rapide**.

Filtrer les ressources par client

Vous pouvez filtrer les ressources par client sur le tableau de bord Citrix DaaS pour Azure **Manage > Déploiement rapide d'Azure** . (Par défaut, toutes les ressources sont affichées.) Lorsque vous travaillez avec des ressources telles que des catalogues, des images de machines et des abonnements Azure, vous pouvez sélectionner des affichages clients spécifiques pour vous aider à organiser les ressources de vos locataires.

Les connexions SD-WAN sont créées par client. Le client doit disposer d'un droit de service SD-WAN Orchestrator.

- Pour créer une connexion SD-WAN pour un client, suivez les instructions de la zone Créer une connexion SD-WAN. Sur la page **Ajouter une connexion réseau**, sélectionnez le client. Vous pouvez sélectionner la zone Type de connexion SD-WAN uniquement si ce client possède un droit de service SD-WAN Orchestrator.
- Pour que la création de la connexion soit réussie, le client doit également disposer d'un nœud de contrôle principal (MCN) installé. Toutefois, seul le droit de service SD-WAN Orchestrator détermine si le type de connexion SD-WAN peut être sélectionné.

Créez des catalogues pour mettre à disposition des applications et des bureaux

Un catalogue est un groupe d'utilisateurs et la collection de machines virtuelles auxquelles ils ont accès. Lorsque vous créez un catalogue, une image est utilisée (avec d'autres paramètres) comme modèle pour créer les machines. Pour plus de détails, consultez la section Création de catalogues.

Domaines fédérés

Les domaines fédérés permettent aux utilisateurs d'utiliser les informations d'identification d'un domaine attaché à votre emplacement de ressources CSP pour se connecter à leur espace de travail. Vous pouvez fournir à vos clients des espaces de travail dédiés auxquels leurs utilisateurs peuvent accéder via une URL d'espace de travail personnalisée (par exemple, `customer.cloud.com`), tandis que l'emplacement des ressources reste sur votre compte Citrix Cloud.

Vous pouvez fournir des espaces de travail dédiés à côté de l'espace de travail partagé auquel les clients peuvent accéder à l'aide de l'URL de votre espace de travail CSP (par exemple, `csppartner.cloud.com`). Pour permettre aux clients d'accéder à leur espace de travail dédié, vous les ajoutez aux domaines appropriés que vous gérez.

Après avoir configuré l'espace de travail via Configurationde l'espace de travail, les utilisateurs des clients peuvent se connecter à leur espace de travail et accéder aux applications et bureaux que vous avez mis à disposition.

Ajouter un client à un domaine

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Cliquez sur **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord **client**, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
3. Sous l'onglet **Domaines**, sélectionnez **Gérer le domaine fédéré** dans le menu des points de suspension du domaine.
4. Sur la carte **Gérer le domaine fédéré**, dans la colonne **Clients disponibles**, sélectionnez un client que vous souhaitez ajouter au domaine. Cliquez sur le signe plus en regard du nom du client. Le client sélectionné apparaît désormais dans la colonne **Clients fédérés**. Répétez cette opération pour ajouter d'autres clients.
5. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Supprimer un client d'un domaine

Lorsque vous supprimez un client d'un domaine que vous gérez, les utilisateurs du client ne peuvent plus accéder à leurs espaces de travail à l'aide des informations d'identification de votre domaine.

1. Dans Citrix Cloud, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
2. Dans l'onglet **Domaines**, sélectionnez **Gérer le domaine fédéré** dans le menu représentant des points de suspension du domaine que vous souhaitez gérer.

3. Dans la liste des clients fédérés, recherchez ou recherchez les clients que vous souhaitez supprimer.

   - Cliquez sur **X** pour supprimer un client.
   - Pour supprimer tous les clients répertoriés du domaine, cliquez sur **Tout supprimer**.

   Les clients sélectionnés sont déplacés vers la liste des **clients disponibles**.

4. Cliquez sur **Appliquer**.
5. Passez en revue les clients que vous avez sélectionnés, puis cliquez sur **Supprimer des clients**.

Ajouter un administrateur avec accès restreint

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Cliquez sur **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord **client**, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
3. Sous l'onglet **Administrateurs**, cliquez sur **Ajouter adm. de**, puis sélectionnez **Identité Citrix**.
4. Tapez l'adresse e-mail de la personne que vous ajoutez en tant qu'administrateur, puis cliquez sur **Inviter**.
5. Configurez les autorisations d'accès appropriées de l'administrateur. Citrix recommande de sélectionner **Accès personnalisé**, sauf si vous souhaitez que l'administrateur puisse gérer Citrix Cloud et tous les services abonnés.
6. Sélectionnez une ou plusieurs paires de rôles et de portées pour Citrix DaaS pour Azure, selon vos besoins.
7. Lorsque vous avez terminé, cliquez sur **Envoyer une invitation**.

Lorsque l'administrateur accepte l'invitation, il dispose de l'accès que vous avez attribué.

Accès des partenaires au fournisseur d'identité client

Vous pouvez gérer les utilisateurs à partir du tableau de bord Citrix DaaS pour Azure **Manage > Déploiement rapide d'Azure** ou de la console Citrix Cloud.

Lorsque vous utilisez un fournisseur d'identité non AD pour les utilisateurs (tel que Citrix Managed Azure AD), vous devez être administrateur Citrix Cloud Identity et Workspace pour le client avant de pouvoir gérer les utilisateurs pour ce client. Si vous n'êtes pas administrateur pour un client, vous ne pouvez pas ajouter ou supprimer d'utilisateurs pour ce client.

Pour gérer les utilisateurs d'un client à partir du tableau de bord **Gérer > Déploiement rapide d'Azure**, sélectionnez le partenaire ou le client dans **Afficher les éléments pour**.

- **Exemple 1 :** sélectionnez le client A dans **Afficher les articles pour**. Le tableau de bord affiche désormais uniquement les éléments du client A. Lorsque vous sélectionnez un catalogue, seuls les utilisateurs du client A s'affichent dans l'onglet **Abonnés** . Vous pouvez ajouter ou supprimer des utilisateurs pour le client A (en supposant que vous êtes administrateur pour ce client).
- **Exemple 2 :** Vous sélectionnez l'entrée partenaire dans **Afficher les articles pour**. Le tableau de bord affiche désormais uniquement les éléments partenaires. Dans l'onglet **Abonnés**, seuls les utilisateurs créés pour le partenaire s'affichent. Aucune entrée client ne s'affiche. Vous pouvez ajouter ou supprimer des utilisateurs pour ce partenaire (en supposant que vous êtes administrateur de ce partenaire), mais vous ne pouvez pas gérer d'utilisateurs clients à partir de cet emplacement.

Pour gérer les utilisateurs d'un client à partir de la console Citrix Cloud, sélectionnez-le lorsque vous y êtes invité après la connexion (ou plus tard, en utilisant **Changer de client** dans la zone supérieure droite de la console Citrix Cloud). Lorsque vous utilisez la bibliothèque pour gérer les utilisateurs, le contexte d'affichage reflète le client sélectionné. Par exemple, si vous avez sélectionné le client A, la bibliothèque affiche uniquement les offres du client A.

Modifier les autorisations d'administration déléguée pour les administrateurs

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Cliquez sur **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord **client**, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
3. Sous l'onglet **Administrateurs**, sélectionnez **Modifier l'accès** dans le menu des points de suspension de l'administrateur.
4. Sélectionnez ou désactivez les paires de rôles et d'étendue pour Citrix DaaS pour Azure, selon vos besoins. Assurez-vous d'activer uniquement les entrées qui contiennent l'étendue unique créée pour le client.
5. Cliquez sur **Enregistrer**.

Accès et configuration des espaces de travail

Chaque client dispose de son propre espace de travail avec une URL `customer.cloud.com` unique. Cette URL est l'endroit où les utilisateurs du client accèdent à leurs applications et postes de travail publiés.

- **Depuis Citrix DaaS Standard for Azure : Dans** le tableau de bord **Gérer > Déploiement rapide d'Azure**, affichez l'URL en développant **User Access & Authentication** sur la droite.
- **Depuis Citrix Cloud :** dans le tableau de bord du **client**, sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. Affichez l'URL dans l'onglet **Accès**.

Vous pouvez modifier l'accès et l'authentification à un espace de travail. Vous pouvez également personnaliser l'apparence et les préférences de l'espace de travail. Pour de plus amples informations, consultez les articles suivants :

- Configurer les espaces de travail
- Espaces de travail sécurisés

Surveiller le service d'un client

Le tableau de bord Citrix Daas pour Azure **Monitor** dans un environnement CSP est essentiellement identique à un environnement non CSP. Voir Surveiller pour plus de détails.

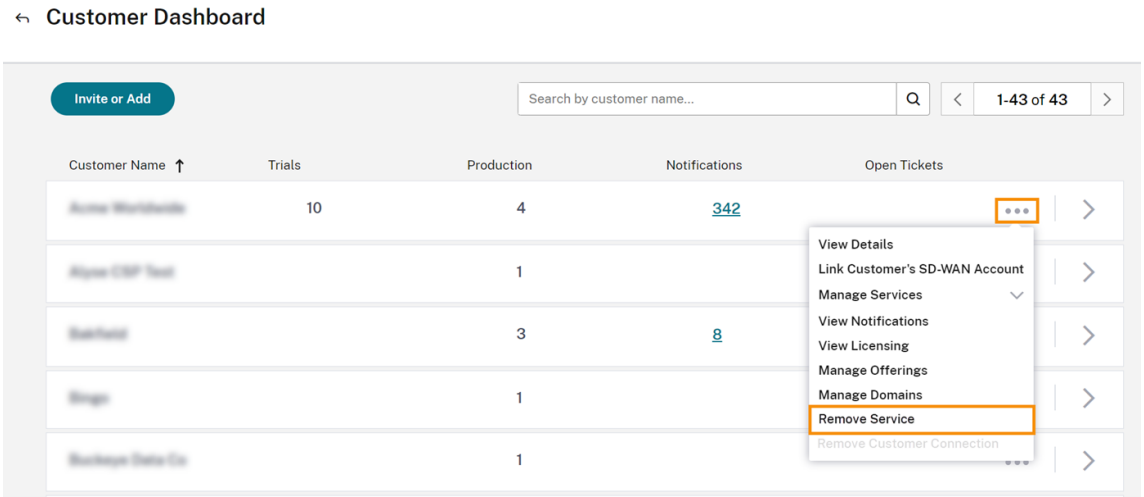
Par défaut, le tableau de bord **Surveiller** affiche des informations sur tous les clients. Pour afficher des informations sur un client, utilisez **Sélectionner un client**.

N'oubliez pas que la possibilité de voir les affichages du **moniteur** pour un client est contrôlée par l'accès configuré par l'administrateur.

Supprimer un service

Avant de commencer, assurez-vous que votre périmètre client n'est lié à aucun objet Citrix DaaS Standard pour Azure. S'ils sont liés, vous ne pouvez pas supprimer le service. Pour dissocier des étendues, accédez à **Citrix Studio > Administrateurs > Étendues** et modifiez l'étendue. Pour plus d'informations sur la dissociation des étendues, voir Création et gestion de la portée.

1. Connectez-vous à Citrix Cloud avec vos informations d'identification Citrix Service Provider.
2. Dans le tableau de bord **Client**, cliquez sur le menu de points de suspension (**...**) du client dont vous souhaitez supprimer un service et sélectionnez **Supprimer le service**.



La page **Sélectionnez un service à supprimer** s'affiche.

3. Cliquez sur **Supprimer** pour supprimer le service.

Dépanner

September 7, 2022

Introduction

Les emplacements de ressources contiennent les machines qui fournissent des bureaux et des applications. Ces machines sont créées dans des catalogues, de sorte que les catalogues sont considérés comme faisant partie de l'emplacement des ressources. Chaque emplacement de ressources contient également des Cloud Connectors. Les Cloud Connectors permettent à Citrix Cloud de communiquer avec l'emplacement des ressources. Citrix installe et met à jour les Cloud Connector.

Vous pouvez éventuellement lancer plusieurs actions Cloud Connector et d'emplacement des ressources. Voir :

- Actions d'emplacement des ressources
- Paramètres d'emplacement des ressources lors de la création d'un catalogue

Citrix DaaS pour Azure dispose d'outils de dépannage et de prise en charge qui peuvent aider à résoudre les problèmes de configuration et de communication avec les machines qui fournissent des postes de travail et des applications (les VDA). Par exemple, la création d'un catalogue peut échouer ou les utilisateurs peuvent ne pas être en mesure de démarrer leur bureau ou leurs applications.

Ce dépannage inclut l'accès à votre abonnement Azure géré par Citrix via une machine bastion ou un RDP direct. Après avoir accédé à l'abonnement, vous pouvez utiliser les outils de prise en charge Citrix pour localiser et résoudre les problèmes. Pour plus de détails, consultez :

- Dépannage VDA à l'aide d'un bastion ou d'un RDP direct
- Accéder au bastion
- Accès direct à RDP

Dépannage VDA à l'aide d'un bastion ou d'un RDP direct

Les fonctionnalités de prise en charge s'adressent aux personnes expérimentées dans le dépannage des problèmes Citrix. Parmi lesquelles :

- Les Citrix Service Providers (CSP) et d'autres personnes possédant les connaissances techniques et l'expérience de dépannage avec les produits Citrix DaaS.

- Les services de support technique Citrix.

Si vous ne connaissez pas ou n'êtes pas à l'aise avec le dépannage des composants Citrix, vous pouvez demander de l'aide au service de support Citrix. Les techniciens du support Citrix peuvent vous demander de configurer l'une des méthodes d'accès décrites dans cette section. Toutefois, ce sont les techniciens Citrix qui effectuent le dépannage à l'aide des outils et technologies Citrix.

> **Important :**
>
> Ces fonctionnalités de prise en charge ne concernent que les machines jointes à un domaine. Si les machines de vos catalogues ne sont pas jointes à un domaine, vous êtes guidé pour demander de l'aide au dépannage auprès du support Citrix.

Méthodes d'accès

Ces méthodes d'accès concernent uniquement l'abonnement Azure géré par Citrix. Pour plus d'informations, consultez Abonnements Azure.

Deux méthodes d'accès à la prise en charge sont fournies.

- Accédez à vos ressources via une machine bastion dans l'abonnement Azure géré par Citrix dédié du client. Le bastion est un point d'entrée unique qui permet d'accéder aux machines de l'abonnement. Il fournit une connexion sécurisée à ces ressources en autorisant le trafic distant à partir d'adresses IP dans une plage spécifiée.

  Les étapes de cette méthode sont les suivantes :

  - création de la machine bastion ;
  - téléchargement d'un agent RDP ;
  - RDP vers la machine bastion ;
  - établissement d'une connexion entre la machine bastion et les autres machines Citrix de votre abonnement.

  La machine bastion est destinée à une utilisation à court terme. Cette méthode est destinée aux problèmes liés à la création de catalogues ou de machines d'images.

- Accès RDP direct aux machines de l'abonnement Azure géré par Citrix dédié du client. Pour autoriser le trafic RDP, le port 3389 doit être défini dans le groupe de sécurité réseau.

  Cette méthode est destinée aux problèmes de catalogue autres que la création, tels que les utilisateurs qui ne peuvent pas démarrer leur bureau.

N'oubliez pas : pour remplacer ces deux méthodes d'accès, contactez le support Citrix pour obtenir de l'aide.

Accéder au bastion

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Dépannage et support** sur la droite.
2. Cliquez sur **Afficher les options de dépannage**.
3. Sur la page **Dépannage**, sélectionnez l'un des deux premiers types de problèmes, puis cliquez sur **Utiliser notre machine de dépannage**.
4. Sur la page **Dépannage avec machine bastion**, sélectionnez le catalogue.
   - Si les machines du catalogue sélectionné ne sont pas jointes au domaine, vous êtes invité à contacter le support Citrix.
   - Si une machine bastion a déjà été créée avec un accès RDP à la connexion réseau du catalogue sélectionné, passez à l'étape 8.
5. La plage d'accès RDP s'affiche. Si vous souhaitez limiter l'accès RDP à une plage inférieure à celle autorisée par la connexion réseau, sélectionnez la case à cocher **Restreindre l'accès RDP aux ordinateurs dans la plage d'adresses IP**, puis saisissez la plage souhaitée.
6. Saisissez un nom d'utilisateur et un mot de passe que vous utiliserez pour vous connecter lorsque vous effectuerez un RDP sur la machine bastion. Exigences de mot de passe.

   N'utilisez pas de caractères Unicode dans le nom d'utilisateur.
7. Cliquez sur **Créer une machine bastion**.

   Lorsque la machine bastion a été créée, le titre de la page devient **Bastion** —***connexion***.

   Si la création de la machine bastion échoue (ou si elle échoue pendant le fonctionnement), cliquez sur **Supprimer** au bas de la page de notification d'échec. Faites une nouvelle tentative de création de la machine bastion.

   Vous pouvez modifier la restriction de plage RDP après la création de la machine bastion. Cliquez sur **Modifier**. Saisissez la nouvelle valeur, puis cliquez sur la coche pour enregistrer la modification. (Cliquez sur **X** pour annuler la modification.)
8. Cliquez sur **Télécharger le fichier RDP**.
9. RDP vers le bastion, en utilisant les informations d'identification que vous avez spécifiées lors de la création du bastion. (L'adresse de la machine bastion est intégrée au fichier RDP que vous avez téléchargé.)
10. Connectez-vous à partir de la machine bastion aux autres machines Citrix de l'abonnement. Vous pouvez ensuite collecter des journaux et exécuter des diagnostics.

Les machines bastion sont sous tension lorsqu'elles sont créées. Pour réduire les coûts, les machines sont automatiquement mises hors tension si elles restent inactives après le démarrage. Les machines sont supprimées automatiquement après plusieurs heures.

Vous pouvez gérer l'alimentation d'une machine bastion ou la supprimer à l'aide des boutons situés en bas de la page. Si vous choisissez de supprimer une machine bastion, vous devez reconnaître que toutes les sessions actives sur la machine se termineront automatiquement. De plus, toutes les données et les fichiers enregistrés sur la machine seront supprimés.

Accès direct à RDP

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** dans Citrix DaaS pour Azure, développez **Dépannage et support** sur la droite.
2. Cliquez sur **Afficher les options de dépannage**.
3. Sur la page **Dépannage**, sélectionnez **Autre problème de catalogue**.
4. Sur la page **Dépanner l'accès RDP**, sélectionnez le catalogue.

   Si RDP a déjà été activé sur la connexion réseau du catalogue sélectionné, passez à l'étape 7.
5. La plage d'accès RDP s'affiche. Si vous souhaitez limiter l'accès RDP à une plage inférieure à celle autorisée par la connexion réseau, cochez la case **Restreindre l'accès RDP aux ordinateurs dans la plage d'adresses IP**, puis saisissez la plage souhaitée.
6. Cliquez sur **Activer l'accès RDP.**

   Lorsque l'accès RDP est activé, le titre de la page devient **Accès RDP** —***connexion***.

   Si l'accès RDP n'est pas activé correctement, cliquez sur **Réessayer d'activer RDP** au bas de la page de notification d'échec.
7. Connectez-vous à des machines en utilisant vos informations d'identification d'administrateur Active Directory. Vous pouvez ensuite collecter des journaux et exécuter des diagnostics.

Obtenir de l'aide

Si vous rencontrez toujours des problèmes, ouvrez un ticket en suivant les instructions de la section Comment obtenir de l'aide.

Limites

May 9, 2023

Cet article répertorie les limites des ressources dans un déploiement Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure service).

> **Remarque :**
>
> Ces limites sont recommandées par Citrix.

Limites de configuration

Ressource	Limite
Domaines Active Directory	25
Catalogues	100
Emplacements des ressources	25
VDA par abonnement	2,500

Limites d'emplacement des ressources

Le tableau suivant répertorie les limites pour chaque emplacement de ressources. Si vos exigences dépassent ces limites, Citrix vous recommande d'utiliser davantage d'emplacements de ressources.

Ressource	Limite
Domaines Active Directory	1
VDA mono-session	10,000
VDA multi-session	1,000

Les connecteurs Citrix Cloud sont affectés à des emplacements de ressources et relient les charges de travail à Citrix DaaS pour Azure. Pour plus d'informations sur les limites du Cloud Connector et pour obtenir des recommandations en matière de taille et d'échelle, consultez la section Considérations relatives à la taille et à l'échelle des Cloud Connector.

Limites de provisioning

Le tableau suivant répertorie les valeurs maximales recommandées pour un seul compte Citrix Cloud.

Pour les déploiements à plus grande échelle, Citrix recommande un modèle hub-and-spoke, dans lequel les VDA sont distribués sur plusieurs abonnements et connexions réseau.

Ressource	Limite
VDA multi-sessions par catalogue	500
VDA mono-session par catalogue	1,200
VDA par abonnement Microsoft Azure	2,500

Limites d'utilisation

Ressource	Limite
Administrateurs complets de Concurrent Monitor	5
Utilisateurs finaux simultanés	100,000
Ressources publiées pour un seul utilisateur	250
Lancements de session par minute	3,000

Limites d'essai

Le tableau suivant répertorie les limites pendant une période d'essai de Citrix DaaS pour Azure.

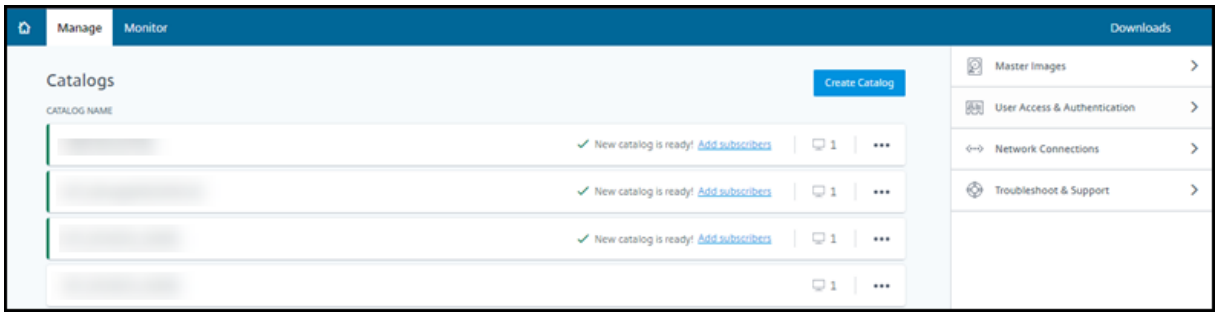
abonnement Azure	Ressource	Limite
Abonnement Azure géré par Citrix	Nombre maximum de catalogues	3
	Nombre maximum d'utilisateurs	25
	Nombre maximum de VDA par catalogue	3
Abonnement Azure géré par le client	Nombre maximum de catalogues	10
	Nombre maximum d'utilisateurs	25
	Nombre maximum de VDA par catalogue	10

Référence

September 7, 2022

Tableaux de bord

La plupart des activités d'administrateur pour Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard for Azure service) peuvent être saisies via les tableaux de bord **Gérer** et **surveiller**. Après avoir créé votre premier catalogue, le tableau de bord **Gérer** s'ouvre automatiquement lorsque vous vous connectez à Citrix Cloud et que vous sélectionnez Citrix DaaS pour Azure.



Vous pouvez accéder aux tableaux de bord une fois que votre demande d'essai ou d'achat est approuvée et terminée.

Pour accéder aux tableaux de bord :

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS Standard pour Azure**. (Vous pouvez également cliquer sur **Gérer** sur la vignette **DaaS Standard pour Azure** dans la zone principale de l'affichage.)
3. Si aucun catalogue n'a encore été créé, cliquez sur **Démarrer** dans la page d'**accueil**. Vous êtes redirigé vers le tableau de bord **Gérer > Déploiement rapide d'Azure** .
4. Si un catalogue a déjà été créé, vous êtes automatiquement redirigé vers le tableau de bord **Gérer > Déploiement rapide Azure** .
5. Pour accéder au tableau de bord **Monitor**, cliquez sur l'onglet **Monitor** .

Pour obtenir des conseils sur le produit à partir du tableau de bord, cliquez sur l'icône dans le coin inférieur droit.

Onglets Catalogue dans le tableau de bord Gérer

Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, cliquez n'importe où dans l'entrée du catalogue. Les onglets suivants contiennent des informations au sujet du catalogue :

- **Détails :** répertorie les informations spécifiées lors de la création du catalogue (ou de sa dernière modification). Cet onglet contient également des informations sur l'image utilisée pour créer le catalogue.

  Dans cet onglet, vous pouvez :

  - modifier l'image utilisée dans le catalogue ;
  - supprimer le catalogue ;
  - accéder à la page contenant les détails de l'emplacement des ressources utilisé par le catalogue.

- **Bureau :** disponible uniquement pour les catalogues contenant des machines à session unique (statiques ou aléatoires). Dans cet onglet, vous pouvez modifier le nom et la description du catalogue.

- **Bureau et applications :** l'onglet **Bureau et applications** est disponible uniquement pour les catalogues contenant des machines à sessions multiples. Dans cet onglet, vous pouvez :

  - ajouter, modifier, ou supprimer des applications auxquelles les utilisateurs du catalogue peuvent accéder dans Citrix Workspace ;
  - modifier le nom et la description du catalogue.

- **Abonnés :** répertorie tous les utilisateurs, y compris leur type (utilisateur ou groupe), leur nom de compte, leur nom d'affichage, ainsi que leur domaine Active Directory et leur nom d'utilisateur principal.

  Dans cet onglet, vous pouvez ajouter ou supprimer des utilisateurs d'un catalogue.

- **Machines :** affiche le nombre total de machines dans le catalogue, ainsi que le nombre de machines enregistrées, de machines non enregistrées et de machines sur lesquelles le mode de maintenance est activé.

  Pour chaque machine du catalogue, l'affichage inclut le nom de chaque machine, l'état d'alimentation (marche/arrêt), l'état d'enregistrement (enregistré ou non enregistré), les utilisateurs attribués, le nombre de sessions (0/1) et l'état du mode de maintenance (icône marche/arrêt).

  Dans cet onglet, vous pouvez :

  - ajouter ou supprimer une machine ;
  - démarrer, redémarrer, forcer le redémarrage ou arrêter une machine ;

  - activer ou désactiver le mode de maintenance d'une machine.

  Pour plus d'informations, consultez la section Gérer les catalogues. De nombreuses actions de la machine sont également disponibles sur le tableau de bord **Monitor** . Voir Surveiller et contrôler l'alimentation des machines.

- **Gestion de l'alimentation :** vous permet de gérer les moments où les machines du catalogue sont sous tension ou hors tension. Un programme d'alimentation indique également quand les machines inactives sont déconnectées.

  Vous pouvez configurer un programme d'alimentation lorsque vous créez un catalogue personnalisé ou ultérieurement. Si aucun programme d'alimentation n'est explicitement défini, une machine s'éteint à la fin d'une session.

  Lorsque vous créez un catalogue à l'aide de la création rapide, vous ne pouvez pas sélectionner ni configurer un programme d'alimentation. Par défaut, les catalogues créés à l'aide de la création rapide utilisent le calendrier prédéfini Économique. Toutefois, vous pouvez modifier ce catalogue ultérieurement et modifier la planification.

  Pour plus de détails, voir Gérer les calendriers de gestion de l'alimentation.

Serveurs DNS

Cette section s'applique à tous les déploiements qui contiennent des machines appartenant à un domaine. Vous pouvez ignorer cette section si vous utilisez uniquement des machines non jointes à un domaine.

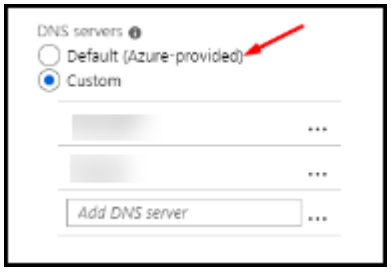
1. Avant de créer un catalogue joint à un domaine (ou une connexion, si vous utilisez un abonnement Azure géré par Citrix), vérifiez si des entrées de serveur DNS peuvent résoudre les noms de domaine publics et privés.

   Lorsque Citrix DaaS pour Azure crée un catalogue ou une connexion, il recherche au moins une entrée de serveur DNS valide. Si aucune entrée valide n'est trouvée, l'opération de création échoue.

   Où vérifier :

   - Si vous utilisez votre propre abonnement Azure, vérifiez l'entrée des **serveurs DNS** dans votre Azure.
   - Si vous utilisez un abonnement Azure géré par Citrix et que vous créez une connexion de peering de réseau virtuel Azure, vérifiez l'entrée des **serveurs DNS** dans le réseau virtuel Azure que vous êtes en train d'appairer.
   - Si vous utilisez un abonnement Azure géré par Citrix et que vous créez une connexion SD-WAN, vérifiez les entrées DNS dans le SD-WAN Orchestrator.

2. Dans Azure, le paramètre **Personnalisé** doit comporter au moins une entrée valide. Citrix DaaS pour Azure ne peut pas être utilisé avec le paramètre **par défaut (fourni par Azure)** .



   - Si **Défaut (fourni par Azure)** est activé, modifiez le paramètre sur **Personnalisé** et ajoutez au moins une entrée de serveur DNS.
   - Si vous avez déjà des entrées de serveur DNS sous **Custom**, vérifiez que les entrées que vous souhaitez utiliser avec Citrix DaaS pour Azure peuvent résoudre les noms IP de domaine public et privé.
   - Si vous ne disposez d'aucun serveur DNS capable de résoudre les noms de domaine, Citrix recommande d'ajouter un serveur DNS fourni par Azure doté de ces fonctionnalités.

3. Si vous modifiez des entrées de serveur DNS, redémarrez toutes les machines connectées au réseau virtuel. Le redémarrage attribue les nouveaux paramètres du serveur DNS. (Les machines virtuelles continuent d'utiliser leurs paramètres DNS actuels jusqu'au redémarrage.)

Si vous souhaitez modifier les adresses DNS ultérieurement, après la création d'une connexion :

- Lorsque vous utilisez votre propre abonnement Azure, vous pouvez les modifier dans Azure (comme décrit dans les étapes précédentes). Vous pouvez également les modifier dans Citrix DaaS pour Azure.
- Lorsque vous utilisez un abonnement Azure géré par Citrix, Citrix DaaS pour Azure ne synchronise pas les modifications d'adresse DNS que vous effectuez dans Azure. Toutefois, vous pouvez modifier les paramètres DNS de la connexion dans Citrix DaaS pour Azure.

N'oubliez pas que la modification des adresses des serveurs DNS peut potentiellement entraîner des problèmes de connectivité pour les machines des catalogues qui utilisent cette connexion.

Ajout de serveurs DNS via Citrix DaaS pour Azure

Avant d'ajouter une adresse de serveur DNS à une connexion, assurez-vous que le serveur DNS peut résoudre les noms de domaine publics et internes. Citrix recommande de tester la connectivité à un serveur DNS avant de l'ajouter.

1. Pour ajouter, modifier ou supprimer une adresse de serveur DNS lorsque vous créez une connexion, cliquez sur **Modifier les serveurs DNS** sur la page **Ajouter** un *type de connexion* . Ou,

si un message indique qu'aucune adresse de serveur DNS n'a été trouvée, cliquez sur **Ajouter des serveurs DNS**. Continuez avec l'étape 3.

2. Pour ajouter, modifier ou supprimer une adresse de serveur DNS pour une connexion existante, procédez comme suit :

   a) Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Connexions réseau** sur la droite.
   b) Sélectionnez la connexion que vous souhaitez modifier.
   c) Cliquez sur **Modifier les serveurs DNS**.

3. Ajoutez, modifiez ou supprimez des adresses.

   a) Pour ajouter une adresse, cliquez sur **Ajouter un serveur DNS**, puis saisissez l'adresse IP.
   b) Pour modifier une adresse, cliquez dans le champ d'adresse et modifiez les nombres.
   c) Pour supprimer une adresse, cliquez sur l'icône de la corbeille en regard de l'entrée d'adresse. Vous ne pouvez pas supprimer toutes les adresses de serveur DNS. La connexion doit en avoir au moins une.

4. Lorsque vous avez terminé, cliquez sur **Confirmer les modifications** en bas de la page.
5. Redémarrez toutes les machines qui utilisent cette connexion. Le redémarrage attribue les nouveaux paramètres du serveur DNS. (Les machines virtuelles continuent d'utiliser leurs paramètres DNS actuels jusqu'au redémarrage.)

Stratégies

Définir des stratégies de groupe pour les machines non jointes à un domaine

1. RDP vers la machine utilisée pour l'image.
2. Installez Citrix Gestion des stratégies de groupe :

   a) Accédez à CTX220345. Téléchargez la pièce jointe.
   b) Double-cliquez sur le fichier téléchargé. Dans le dossier `Group Policy Templates 1912 > Group Policy Management`, double-cliquez sur `CitrixGroupPolicyManagement.msi`.

3. Utilisez la commande **Exécuter** pour démarrer `gpedit.msc`, qui ouvre l'éditeur de stratégie de groupe.
4. Dans `User Configuration Citrix Policies > Unfiltered`, cliquez sur **Modifier la stratégie**.

   Si la console de gestion des stratégies de groupe échoue (comme décrit dans la section CTX225742), installez Microsoft Visual C++ 2015 Runtime (ou une version ultérieure de ce runtime).

5. Activez les paramètres de stratégie si nécessaire. Par exemple :

    - Lorsque vous travaillez dans **Configuration de l'ordinateur** ou **Configuration utilisateur** (en fonction de ce que vous souhaitez configurer) sous l'onglet **Paramètres** dans `Category > ICA / Printing`, sélectionnez **Créer automatiquement une imprimante universelle PDF** et définissez-la sur `Enabled`.
    - Si vous souhaitez que les utilisateurs connectés soient administrateurs de leur bureau, ajoutez le groupe **Utilisateurs interactifs** au groupe d'administrateurs intégré.

6. Lorsque vous avez terminé, enregistrez l'image.
7. Mettez à jour le catalogue existant ou créez un nouveau catalogue à l'aide de la nouvelle image.

Définir des stratégies de groupe pour les machines jointes à un domaine

1. Assurez-vous que la fonctionnalité de gestion des stratégies de groupe est installée.

    - Sur une machine Windows à sessions multiples, ajoutez la fonctionnalité de gestion des stratégies de groupe à l'aide de l'outil Windows pour ajouter des rôles et des fonctionnalités (tels que **Ajouter des rôles et fonctionnalités**).
    - Sur une machine Windows à session unique, installez les outils d'administration du serveur distant pour le système d'exploitation approprié. (Cette installation nécessite un compte administrateur de domaine.) Après cette installation, la console de gestion des stratégies de groupe est disponible dans le menu **Démarrer**.

2. Téléchargez et installez le package de gestion des stratégies de groupe Citrix à partir de la page de téléchargement Citrix, puis configurez les paramètres de stratégie si nécessaire. Suivez la procédure décrite dans Définir des stratégies de groupe pour les machines non jointes à un domaine, étape 2 jusqu'à la fin.

> **Remarque :**
>
> Bien que la console Citrix Studio ne soit pas disponible dans Citrix DaaS pour Azure, consultez les articles de référence sur les paramètres de stratégie pour en savoir plus sur ce qui est disponible.

Actions d'emplacement des ressources

Citrix crée automatiquement un emplacement des ressources et deux Cloud Connectors lorsque vous créez le premier catalogue de publication de bureaux et d'applications. Vous pouvez spécifier certaines informations liées à l'emplacement des ressources lorsque vous créez un catalogue. Voir Paramètres d'emplacement des ressources lors de la création d'un catalogue.

(Pour Remote PC Access, vous créez l'emplacement des ressources et les Cloud Connectors.)

Cette section décrit les actions disponibles après la création d'un emplacement des ressources.

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Abonnements Cloud** sur la droite.
2. Cliquez sur l'abonnement.

    - L'onglet **Détails** affiche le nombre et le nom des catalogues et des images de l'abonnement. Il indique également le nombre de machines pouvant fournir des bureaux ou des applications. Ce nombre n'inclut pas les machines utilisées à d'autres fins, telles que les images, les Cloud Connector ou les serveurs de licences RDS
    - L'onglet **Emplacements des ressources** répertorie chaque emplacement des ressources. Chaque entrée d'emplacement des ressources inclut le statut et l'adresse de chaque Cloud Connector dans l'emplacement des ressources.

Le menu des points de suspension de l'entrée d'un emplacement des ressources contient les actions suivantes.

Exécuter vérification de l'intégrité

La sélection de **Exécuter vérification de l'intégrité** démarre immédiatement le contrôle de connectivité. Si la vérification échoue, l'état du Cloud Connector est inconnu, car il ne communique pas avec Citrix Cloud. Essayez de redémarrer le Cloud Connector.

Redémarrer des connecteurs

Citrix recommande de ne redémarrer qu'un seul Cloud Connector à la fois. Le redémarrage met Cloud Connector hors ligne et perturbe l'accès des utilisateurs et la connectivité de la machine.

Cochez la case correspondant au Cloud Connector que vous souhaitez redémarrer. Cliquez sur **Redémarrer**.

Ajouter des connecteurs

L'ajout d'un Cloud Connector prend généralement 20 minutes.

Fournissez les informations suivantes :

- le nombre de Cloud Connectors à ajouter ;
- les informations d'identification du compte de service de domaine, qui permettent de joindre les machines Cloud Connector au domaine ;
- les performances de la machine ;

- le groupe de ressources Azure. La valeur par défaut est le dernier groupe de ressources utilisé par l'emplacement de ressources ;
- l'unité d'organisation. La valeur par défaut est la dernière unité d'organisation utilisée par l'emplacement de ressources ;
- si votre réseau a besoin d'un serveur proxy pour la connectivité Internet. Si vous indiquez **Oui**, précisez le nom de domaine complet ou l'adresse IP du serveur proxy, ainsi que le numéro de port.

Lorsque vous avez terminé, cliquez sur **Ajouter des connecteurs**.

Supprimer des connecteurs

Si un Cloud Connector ne peut pas communiquer avec Citrix Cloud et qu'un redémarrage ne résout pas le problème, le support Citrix peut recommander de supprimer ce Cloud Connector.

Cochez la case correspondant au Cloud Connector que vous souhaitez supprimer. Cliquez ensuite sur **Supprimer**. Lorsque vous y êtes invité, confirmez la suppression.

Vous pouvez également supprimer un Cloud Connector disponible. Toutefois, si la suppression de ce Cloud Connector entraînait la mise à disposition de moins de deux Cloud Connector dans l'emplacement des ressources, vous ne seriez pas autorisé à supprimer le Cloud Connector sélectionné.

Sélectionner l'heure de mise à jour

Citrix fournit automatiquement des mises à jour logicielles pour les Cloud Connectors. Lors d'une mise à jour, un Cloud Connector est mis hors ligne et mis à jour, tandis que les autres Cloud Connectors restent en service. Lorsque la première mise à jour est terminée, un autre Cloud Connector est mis hors ligne et mis à jour. Ce processus se poursuit jusqu'à ce que tous les Cloud Connectors de l'emplacement de ressources soient mis à jour. Le meilleur moment pour démarrer les mises à jour est généralement en dehors de vos heures de bureau habituelles.

Choisissez l'heure de début des mises à jour ou indiquez que vous souhaitez que les mises à jour démarrent lorsqu'une mise à jour est disponible. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Renommer

Saisissez le nouveau nom de l'emplacement des ressources. Cliquez sur **Enregistrer**.

Configurer la connectivité

Indiquez si les utilisateurs peuvent accéder aux bureaux et aux applications via Citrix Gateway Service, ou uniquement depuis le réseau de votre entreprise.

Profile Management

Profile Management veille à ce que les paramètres personnels soient appliqués à leurs applications virtuelles, indépendamment de l'emplacement de la machine utilisateur.

La configuration de Profile Management est facultative.

Vous pouvez activer Profile Management avec le service d'optimisation de profil. Ce service constitue un moyen fiable de gérer ces paramètres sous Windows. La gestion des profils assure une expérience cohérente grâce à un profil unique qui suit l'utilisateur. Il se consolide automatiquement et optimise les profils utilisateur afin de minimiser les besoins en gestion et en stockage. Le service d'optimisation de profil ne nécessite pas beaucoup d'administration, de support et d'infrastructure. En outre, l'optimisation des profils offre aux utilisateurs une meilleure expérience en matière de connexion et de déconnexion.

Le service d'optimisation des profils nécessite un partage de fichiers dans lequel tous les paramètres personnels sont conservés. Vous gérez les serveurs de fichiers. Nous recommandons de configurer la connectivité réseau pour autoriser l'accès à ces serveurs de fichiers. Vous devez spécifier le partage de fichiers en tant que chemin UNC. Le chemin peut contenir des variables d'environnement système, des attributs d'utilisateur Active Directory ou des variables Profile Management. Pour en savoir plus sur le format de la chaîne de texte UNC, voir Pour spécifier le chemin d'accès au magasin de l'utilisateur.

Lorsque vous activez Profile Management, vous pouvez envisager d'optimiser davantage le profil de l'utilisateur en configurant la redirection de dossiers afin de minimiser les effets de la taille de ce dernier. L'application de la redirection de dossiers vient compléter la solution Profile Management. Pour plus d'informations, consultez Redirection de dossiers Microsoft.

Configurer le serveur de licences Microsoft RDS pour les charges de travail Windows Server

Ce service accède aux fonctionnalités de session distante de Windows Server lors de la mise à disposition d'une charge de travail Windows Server, telle que Windows 2016. Cela nécessite généralement une licence d'accès client Services Bureau à distance (RDS CAL). La machine Windows sur laquelle le VDA Citrix est installé doit pouvoir contacter un serveur de licences RDS pour demander des licences RDS CAL. Installez et activez le serveur de licences. Pour plus d'informations, voir le document Microsoft Activer le serveur de licences Remote Desktop Services. Pour les environnements de validation technique, vous pouvez utiliser le délai de grâce fourni par Microsoft.

Avec cette méthode, vous pouvez faire en sorte que ce service applique les paramètres du serveur de licences. Vous pouvez configurer le serveur de licences et le mode par utilisateur dans la console RDS sur l'image. Vous pouvez également configurer le serveur de licences à l'aide des paramètres

de stratégie de groupe Microsoft. Pour plus d'informations, voir le document Microsoft Attribuer une licence à votre déploiement RDS avec des licences d'accès client (CAL).

Pour configurer le serveur de licences RDS à l'aide des paramètres de stratégie de groupe

1. Installez un serveur de licences Services Bureau à distance sur l'une des VM disponibles. La VM doit toujours être disponible. Les charges de travail du service Citrix doivent pouvoir atteindre ce serveur de licences.
2. Spécifiez l'adresse du serveur de licences et le mode de licence par utilisateur à l'aide de la stratégie de groupe Microsoft. Pour plus de détails, voir le document Microsoft Spécifier le mode de licence Bureau à distance pour un serveur hôte de session Bureau à distance.

Les charges de travail Windows 10 nécessitent l'activation d'une licence Windows 10 appropriée. Nous vous recommandons de suivre la documentation Microsoft pour activer les charges de travail Windows 10.

Utilisation de l'engagement de consommation

> **Remarque :**
>
> Il s'agit d'une version préliminaire de cette fonctionnalité.

Sur la fiche **Général** du tableau de bord **Gérer > Déploiement rapide d'Azure**, la valeur **Consommation** indique la quantité de consommation utilisée au cours du mois civil en cours. Cette valeur inclut les engagements mensuels et annuels.

Lorsque vous cliquez sur **Général**, l'onglet **Notifications** inclut :

- la consommation totale utilisée pour le mois (mensuelle et annuelle) ;
- le nombre d'unités d'engagement de consommation mensuel ;
- le pourcentage de l'engagement de consommation annuel.

Les valeurs et les barres de progression peuvent vous alerter en cas de dépassements d'utilisation potentiels ou réels.

Les données réelles peuvent prendre 24 heures avant d'apparaître. Les données d'utilisation et de facturation sont considérées comme définitives 72 heures après la fin d'un mois civil.

Pour plus d'informations sur l'utilisation, consultez Surveiller les licences et l'utilisation de Citrix DaaS Standard pour Azure.

Vous pouvez éventuellement demander que des notifications apparaissent dans le tableau de bord **Gérer** lorsque la consommation (pour les engagements mensuels, à terme ou les deux) atteint un niveau spécifié. Par défaut, les notifications sont désactivées.

1. Dans l'onglet **Notifications**, cliquez sur **Modifier les préférences de notification**.

2. Pour activer les notifications, cliquez sur le curseur pour que la coche apparaisse.
3. Saisissez une valeur. Répétez l'opération pour l'autre type de consommation, si nécessaire.
4. Cliquez sur **Enregistrer**.

Pour désactiver les notifications, cliquez sur le curseur afin que la coche ne s'affiche plus, puis cliquez sur **Enregistrer**.

Surveiller l'utilisation des licences Citrix

Pour afficher les informations d'utilisation de vos licences Citrix, suivez les instructions de la section Surveiller les licences et l'utilisation pour Citrix DaaS Standard for Azure. Vous pouvez consulter les éléments suivants :

- Résumé de l'option Système de licences
- Rapports d'utilisation
- Tendances d'utilisation et activité des licences
- Utilisateurs sous licence

Vous pouvez également libérer des licences.

Équilibrage de charge

L'équilibrage de charge s'applique aux machines à sessions multiples, et non aux machines à session unique.

> **Important :**
>
> La modification de la méthode d'équilibrage de charge affecte tous les catalogues de votre déploiement. Cela inclut tous les catalogues créés à l'aide de n'importe quel type d'hôte pris en charge, basé sur le Cloud et local, quelle que soit l'interface utilisée pour les créer (telle que Studio ou Déploiement rapide).
>
> Assurez-vous que les limites de session maximales sont configurées pour tous les catalogues avant de continuer.
>
> - Dans l'interface de gestion Quick Deploy pour Citrix DaaS pour Azure, ce paramètre se trouve dans l'onglet **Détails** de chaque catalogue.
> - Dans les autres services et éditions de Citrix DaaS, utilisez les paramètres de stratégie de gestion de la charge.

L'équilibrage de charge mesure la charge de la machine et détermine la machine à sessions multiples à sélectionner pour une session utilisateur entrante dans les conditions actuelles. Cette sélection est basée sur la méthode d'équilibrage de charge configurée.

Vous pouvez configurer l'une des deux méthodes d'équilibrage de charge : horizontale ou verticale. La méthode s'applique à tous les catalogues à sessions multiples (et donc à toutes les machines à sessions multiples) de votre déploiement de services.

- **Équilibrage de charge horizontal :** une session utilisateur entrante est attribuée à la machine sous tension la moins chargée disponible.

  Exemple simple : deux machines sont configurées pour 10 sessions chacune. La première machine gère cinq sessions simultanées. La deuxième machine en gère cinq.

  L'équilibrage de charge horizontal offre des performances utilisateur élevées, mais il peut augmenter les coûts à mesure que davantage de machines sont mises sous tension et utilisées.

  Cette méthode est activée par défaut.

- **Équilibrage de charge vertical :** une session utilisateur entrante est attribuée à la machine sous tension avec l'indice de charge le plus élevé. (Citrix DaaS pour Azure calcule puis attribue un indice de charge à chaque machine multisession. Le calcul prend en compte des facteurs tels que l'unité centrale, la mémoire et la concurrence.)

  Cette méthode sature les machines existantes avant de passer à de nouvelles machines. Lorsque les utilisateurs se déconnectent et libèrent de la capacité sur les machines existantes, une nouvelle charge est attribuée à ces machines.

  Exemple simple : deux machines sont configurées pour 10 sessions chacune. La première machine gère les 10 premières sessions simultanées. La deuxième machine s'occupe de la onzième session.

  Avec l'équilibrage de charge vertical, les sessions maximisent la capacité de la machine sous tension, ce qui peut réduire les coûts de la machine.

Pour configurer la méthode d'équilibrage de charge :

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, développez **Général** sur la droite.
2. Sous **Paramètres globaux**, cliquez sur **Afficher tout**.
3. Sur la page **Paramètres généraux**, sous **Équilibrage de charge de catalogues multi-session**, choisissez la méthode d'équilibrage de charge.
4. Cliquez sur **Confirmer**.

Créer un catalogue dans un réseau utilisant un serveur proxy

Suivez cette procédure si votre réseau nécessite un serveur proxy pour la connectivité Internet et que vous utilisez votre propre abonnement Azure. (L'utilisation d'un abonnement Azure géré par Citrix avec un réseau nécessitant un serveur proxy n'est pas prise en charge.)

1. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, lancez le processus de création du catalogue en fournissant les informations requises, puis en cliquant sur **Créer un catalogue** en bas de la page.
2. La création du catalogue échoue en raison de l'exigence de proxy. Toutefois, un emplacement de ressources est créé. Le nom de cet emplacement de ressources commence par « DAS », sauf si vous avez fourni un nom d'emplacement de ressources lors de la création du catalogue. Dans la console Citrix DaaS pour Azure, développez **Abonnements Cloud**. Dans l'onglet **Emplacements de ressources**, vérifiez si le nouvel emplacement des ressources créé contient des Cloud Connectors. Si c'est le cas, supprimez-les.
3. Dans Azure, créez deux machines virtuelles (voir Configuration système requise pour Cloud Connector). Joignez ces machines au domaine.
4. À partir de la console Citrix Cloud, installez un Cloud Connector sur chaque machine virtuelle. Assurez-vous que les Cloud Connector se trouvent dans le même emplacement de ressources que celui créé précédemment. Suivez les instructions décrites dans la section :
    - Configuration du pare-feu et du proxy d'un Cloud Connector
    - Configuration requise pour le système et la connectivité
5. Dans le tableau de bord **Gérer > Déploiement rapide d'Azure**, répétez le processus de création du catalogue. Lorsque le catalogue est créé, il utilise l'emplacement des ressources et les Cloud Connectors que vous avez créés lors des étapes précédentes.

Obtenir de l'aide

- Consultez la section Dépannage.
- Si vous avez besoin d'une assistance supplémentaire avec Citrix DaaS pour Azure, ouvrez un ticket d'assistance en suivant les instructions de la section How to Get Help and Support.