Vue d'ensemble

Nouveautés de Citrix Cloud™ Government

Septembre 2023

La prise en charge d'Endpoint Management dans Citrix Cloud Government a été dépréciée puis supprimée. Pour plus d'informations, consultez Dépréciation dans la documentation du service Endpoint Management.

Août 2022

Interface de gestion des administrateurs améliorée : Citrix Cloud Government inclut désormais une interface améliorée pour l'ajout d'administrateurs individuels et de groupes d'administrateurs. Pour plus d'informations, consultez les articles suivants :

- Inviter des administrateurs individuels
- Ajouter des administrateurs à Citrix Cloud Government depuis AD

Aperçu de l'authentification SAML pour les administrateurs : Citrix Cloud Government prend désormais en charge l'utilisation de l'authentification SAML pour les groupes d'administrateurs dans AD. Pour plus d'informations, consultez Connecter SAML en tant que fournisseur d'identité à Citrix Cloud Government.

Mai 2022

Statut FedRAMP Moderate : Citrix DaaS et Citrix Cloud Government ont obtenu le statut FedRAMP Moderate. FedRAMP est un programme qui promeut les normes de sécurité pour les services cloud utilisés par les organisations gouvernementales américaines. Les organisations gouvernementales américaines peuvent déployer des applications et des bureaux virtuels dans Citrix Cloud Government avec Citrix DaaS sur Microsoft Azure Government, répondant ainsi aux exigences du statut FedRAMP Moderate. Pour plus d'informations, consultez Statut FedRAMP Moderate.

Mars 2022

Disponibilité générale du journal système : Le journal système est désormais généralement disponible. Le journal système affiche une liste horodatée des événements survenus dans Citrix Cloud Government. Affichez les événements des 90 derniers jours et exportez-les pour la conformité réglementaire ou l'analyse de sécurité. Pour plus d'informations, consultez Journal système.

Février 2022

SAML en tant que fournisseur d'identité : Citrix Cloud Government prend désormais en charge l'utilisation de SAML en tant que fournisseur d'identité pour authentifier les abonnés se connectant à leurs espaces de travail. Pour plus d'informations, consultez Connecter Okta en tant que fournisseur d'identité à Citrix Cloud Government.

Novembre 2021

Ajout d’administrateurs dans les groupes Microsoft Entra ID : Citrix Cloud Government prend désormais en charge l’ajout d’administrateurs à votre compte Citrix Cloud Government à l’aide de groupes Microsoft Entra ID. Pour plus d’informations, consultez Gérer les groupes d’administrateurs.

Septembre 2021

Okta en tant que fournisseur d’identité : Citrix Cloud Government prend désormais en charge l’utilisation d’Okta en tant que fournisseur d’identité pour authentifier les abonnés se connectant à leurs espaces de travail. Pour plus d’informations, consultez Connecter Okta en tant que fournisseur d’identité à Citrix Cloud Government.

Juillet 2021

Citrix Gateway en tant que fournisseur d’identité : Citrix Cloud Government prend désormais en charge l’utilisation d’un Citrix Gateway sur site en tant que fournisseur d’identité pour authentifier les abonnés se connectant à leurs espaces de travail. Pour plus d’informations, consultez Connecter un Citrix Gateway sur site en tant que fournisseur d’identité à Citrix Cloud Government.

Authentification multifacteur : Citrix Cloud Government exige désormais que les administrateurs se connectent à l’aide de l’authentification multifacteur. Pour plus d’informations, consultez S’inscrire à l’authentification multifacteur et Ajouter des administrateurs à un compte Citrix Cloud Government.

Juin 2021

Aperçu du journal système : Citrix Cloud Government inclut désormais la fonctionnalité d'aperçu du journal système qui affiche une liste horodatée des événements survenus dans Citrix Cloud Government. Affichez les événements des 90 derniers jours et exportez les événements pour répondre aux exigences de conformité réglementaire ou pour l'analyse de sécurité. Pour plus d'informations, consultez Journal système.

Octobre 2020

FedRAMP Ready : Citrix Workspace™ est FedRAMP Ready lorsqu'il est déployé dans Citrix Cloud Government. FedRAMP est un programme qui promeut les normes de sécurité pour les services cloud utilisés par les organisations gouvernementales américaines. Les organisations gouvernementales américaines qui exigent des services cloud FedRAMP Ready peuvent désormais utiliser Citrix Workspace et Citrix DaaS (anciennement le service Citrix Virtual Apps and Desktops™) pour fournir des applications et des bureaux virtuels.

Contrat de niveau de service

Date d'entrée en vigueur : 1er novembre 2024

Citrix Cloud™ Government est conçu en utilisant les meilleures pratiques de l'industrie pour atteindre un haut degré de disponibilité du service.

Ce Contrat de Niveau de Service (SLA) décrit l'engagement de Citrix concernant la disponibilité du service Citrix Cloud Government. Ce SLA fait partie du contrat de licence utilisateur final (CLUF) de Cloud Software Group pour les services couverts (« Services »).

L'engagement de service de Citrix (« Engagement de service ») est de maintenir une disponibilité mensuelle d'au moins 99,9 % (« Disponibilité mensuelle ») sur les Services. La Disponibilité mensuelle est calculée en soustrayant de 100 % le pourcentage de minutes, au cours d'un mois complet d'un Service, pendant lesquelles l'instance du Service était dans l'état « Indisponible ». Les Services et la mesure de disponibilité pour chacun sont définis dans le tableau ci-dessous. Les mesures du pourcentage de Disponibilité mensuelle excluent les temps d'arrêt résultant de :

- Fenêtres de maintenance planifiées régulièrement.
- Le non-respect par le client des exigences de configuration du Service telles que documentées dans la documentation produit Citrix, ou un comportement abusif, ou une saisie erronée.
- L'utilisation d'un Service par le client après que Citrix® a conseillé au client de modifier son utilisation du Service, si le client n'a pas modifié cette utilisation.

- Causé par tout composant non géré par Citrix, y compris, mais sans s'y limiter, les machines physiques et virtuelles contrôlées par le client, les systèmes d'exploitation installés et maintenus par le client, les logiciels installés et contrôlés par le client, les équipements réseau ou autre matériel ; les paramètres de sécurité, les stratégies de groupe et autres stratégies de configuration définis et contrôlés par le client ; les défaillances des fournisseurs de cloud public, les défaillances des fournisseurs de services Internet ; ou d'autres facteurs de support client échappant au contrôle de Citrix.
- Les employés, agents, sous-traitants ou fournisseurs du client, ou toute personne accédant au moyen des mots de passe ou de l'équipement du client, ou résultant autrement du non-respect par le client des pratiques de sécurité appropriées.
- Les tentatives du client d'effectuer des opérations qui dépassent les droits du Service.
- Interruption de service due à un cas de Force Majeure, y compris, mais sans s'y limiter, les catastrophes naturelles, la guerre ou les actes de terrorisme, ou les actions gouvernementales.

Aucun Engagement de service n'est offert pour les services d'essai, d'aperçu technologique, Labs ou Bêta de Citrix.

Citrix offre des Engagements de service aux clients qui :

- Ont acheté les Services via un abonnement à durée déterminée (période d'abonnement minimale d'un an).
- Avoir au moins un abonnement de 100 unités (1 000 minimum pour les fournisseurs de services Citrix), selon le modèle de licence applicable au Service, pendant la période de réclamation.

Mesures de disponibilité par service

Le tableau suivant répertorie les mesures de disponibilité dans les métriques SLA pour les différents services pris en charge dans Citrix Cloud Government :

SERVICE CITRIX CLOUD GOVERNMENT	MESURE DE LA DISPONIBILITÉ MENSUELLE
Service Citrix Gateway pour proxy HDX™	Temps pendant lequel les utilisateurs peuvent accéder à leur session d'application ou de bureau via le Service.
Citrix DaaS™	Temps pendant lequel les utilisateurs peuvent accéder à leur session d'application ou de bureau via le Service.

SERVICE CITRIX CLOUD GOVERNMENT	MESURE DE LA DISPONIBILITÉ MENSUELLE
Citrix Workspace™	Identique à ce qui précède pour les services composants, mais inclut la disponibilité pour chacun. Les crédits peuvent être calculés au prorata si une réclamation concerne moins de tous les composants.

Engagement de service et recours

Dans le cas où Citrix ne respecterait pas l'Engagement de service pendant au moins 3 mois sur 5 mois consécutifs à compter de la Date d'entrée en vigueur du SLA, le seul recours est un crédit de service de 10 % sur une base mensuelle, pour les mois où Citrix ne respecte pas l'Engagement de service, appliqué à la prochaine prolongation annuelle du Service du Client pendant la période de renouvellement immédiate pour le même Service et le même nombre d'unités impactées.

- Pourcentage de disponibilité mensuelle : > 99,9 %
- Crédit de service : 10 % de réduction pour les mois applicables (présenté au Client sous forme de bon)

Pour bénéficier du recours ci-dessus, le client doit être en conformité avec l'EULA et la défaillance doit être signalée par le client dans les trente (30) jours suivant la fin du dernier mois de la période consécutive de cinq mois pour laquelle une demande de crédit doit être faite. Pour obtenir des instructions sur la manière de signaler d'éventuelles violations de ce SLA, consultez CTX237141.

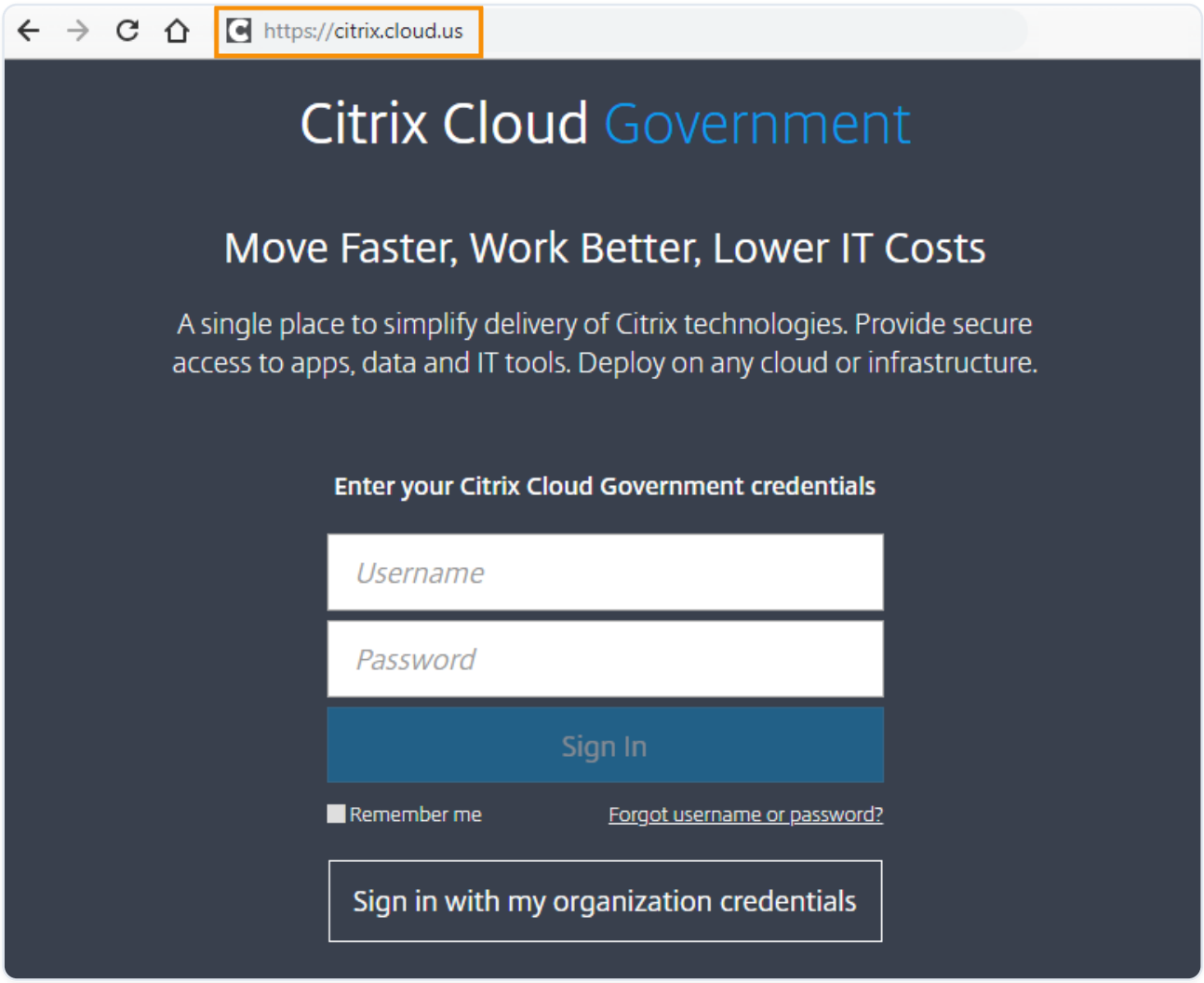
La demande doit identifier le(s) Service(s), définir les dates, heures et durées d'Indisponibilité, ainsi que les journaux ou enregistrements justificatifs qui corroborent l'Indisponibilité, et identifier les utilisateurs affectés et leurs emplacements, ainsi que tout support technique demandé ou toute mesure corrective mise en œuvre. Un seul crédit de service sera émis par Service, pour le nombre de mois applicable, avec un maximum d'un seul crédit de service de 10 % pour tous les mois de l'extension. Les clients doivent présenter le bon lors de l'achat de l'extension.

Si vous achetez l'extension par l'intermédiaire d'un revendeur, vous recevrez un crédit par l'intermédiaire du revendeur. Le crédit que nous appliquons pour un achat direct, ou que nous transmettons à votre revendeur pour un achat indirect, sera basé sur le prix de détail suggéré, pondéré et au prorata, de l'extension pour le même nombre d'unités. Citrix ne contrôle pas les prix de revente ni les crédits de revente. Les crédits n'incluent pas de droit de compensation sur les paiements dus à Citrix ou à un revendeur. Citrix mettra occasionnellement à jour ces conditions. Lorsque des mises à jour se produisent, Citrix révisera également la date de publication en haut du

Contrat de niveau de service. Toute modification s'applique uniquement à vos nouveaux achats de Services ou extensions de Services effectués à la date de publication actuelle ou après celle-ci.

Comment obtenir de l'aide et du support

Connexion à votre compte



Si vous rencontrez des difficultés pour vous connecter à votre compte Citrix Cloud™ Government :

- Vérifiez que vous vous connectez à https://citrix.cloud.us et que la page de connexion affiche le logo Citrix Cloud Government. L'URL de connexion de Citrix Cloud Government utilise le domaine de premier niveau `.us`, et non le domaine de premier niveau `.com`.
- Assurez-vous de vous connecter avec l'**adresse e-mail** que vous avez fournie lors de l'inscription à votre compte. Pour plus d'informations sur les adresses e-mail acceptées pour l'inscription au compte, consultez S'inscrire à Citrix Cloud Government.
- Si votre organisation permet aux utilisateurs de se connecter à Citrix Cloud Government en utilisant leurs informations d'identification d'organisation au lieu d'un compte Citrix Cloud

Government, cliquez sur **Se connecter avec les informations d'identification de mon organisation** et saisissez l'URL de connexion de votre organisation. Vous pourrez ensuite saisir vos informations d'identification d'organisation pour accéder au compte Citrix Cloud Government de votre organisation. Si vous ne connaissez pas l'URL de connexion de votre organisation, contactez l'administrateur de votre organisation pour obtenir de l'aide.

Remarque :

Vous pouvez vous connecter avec les informations d'identification de votre organisation si Microsoft Entra ID est activé en tant que fournisseur d'identité pour votre compte. Pour plus d'informations sur l'utilisation de Microsoft Entra ID comme fournisseur d'identité, consultez Connecter Microsoft Entra ID à Citrix Cloud Government.

Modification de votre mot de passe

Si vous avez oublié ou devez réinitialiser le mot de passe de votre compte Citrix Cloud Government, cliquez sur **Nom d'utilisateur ou mot de passe oublié ?** et vous pourrez saisir l'adresse e-mail de votre compte. Vous recevrez un e-mail pour réinitialiser votre mot de passe.

Citrix Cloud Government vous invite à réinitialiser votre mot de passe si votre mot de passe actuel a plus de 60 jours.

Le mot de passe que vous choisissez est sensible à la casse et doit respecter les exigences suivantes :

- Au moins 12 caractères
- Comprend au moins une lettre majuscule
- Comprend au moins une lettre minuscule
- Comprend au moins un chiffre
- Comprend au moins un caractère spécial : `! @ # $ % \^ * ? + = -`

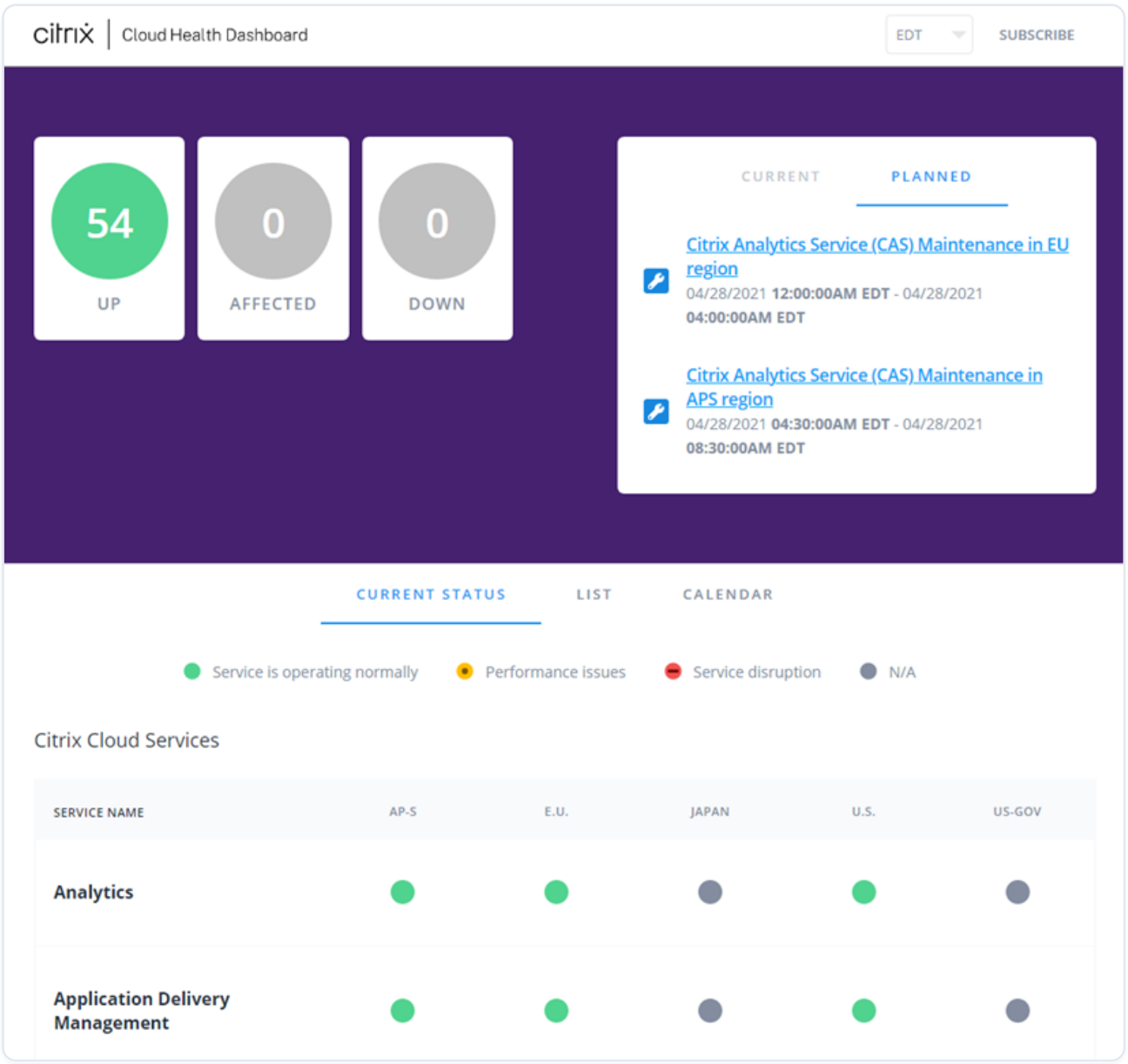
Important :

- Au moins un caractère de votre mot de passe doit être modifié. Vous ne pouvez pas utiliser votre mot de passe existant comme nouveau mot de passe.

- Vous ne pouvez pas réutiliser vos 24 mots de passe précédents.
- Votre nouveau mot de passe doit être actif pendant au moins un jour avant que vous puissiez le modifier à nouveau.

État du service cloud

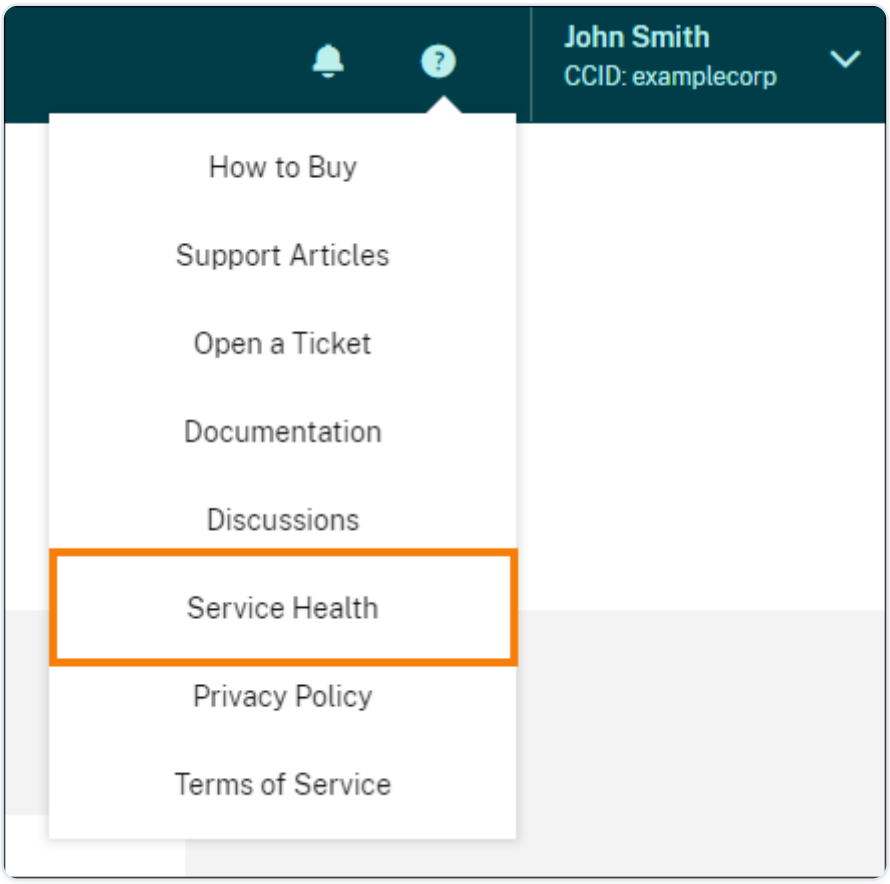
Le tableau de bord d'état de Citrix Cloud fournit un aperçu de la disponibilité en temps réel de la plateforme et des services Citrix Cloud dans chaque région géographique. Si vous rencontrez des problèmes avec Citrix Cloud, consultez le tableau de bord d'état du cloud pour vérifier que Citrix Cloud ou des services spécifiques fonctionnent normalement.



Vous pouvez accéder au tableau de bord d'état du cloud en utilisant les méthodes suivantes :

- Accédez à `<https://status.cloud.com>` via votre navigateur web.

- Sélectionnez **État du service** dans le menu Aide de Citrix Cloud.



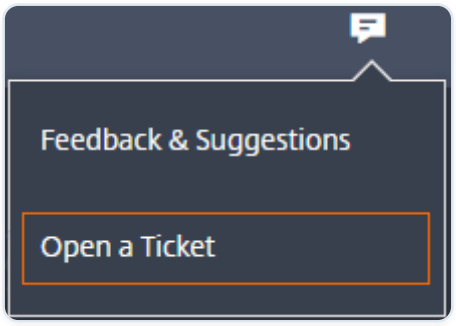
Utilisez le tableau de bord pour en savoir plus sur les conditions suivantes :

- L'état de santé actuel de tous les services Citrix Cloud, regroupés par région géographique
- L'historique de l'état de santé de chaque service pour les sept derniers jours
- Fenêtres de maintenance pour des services spécifiques

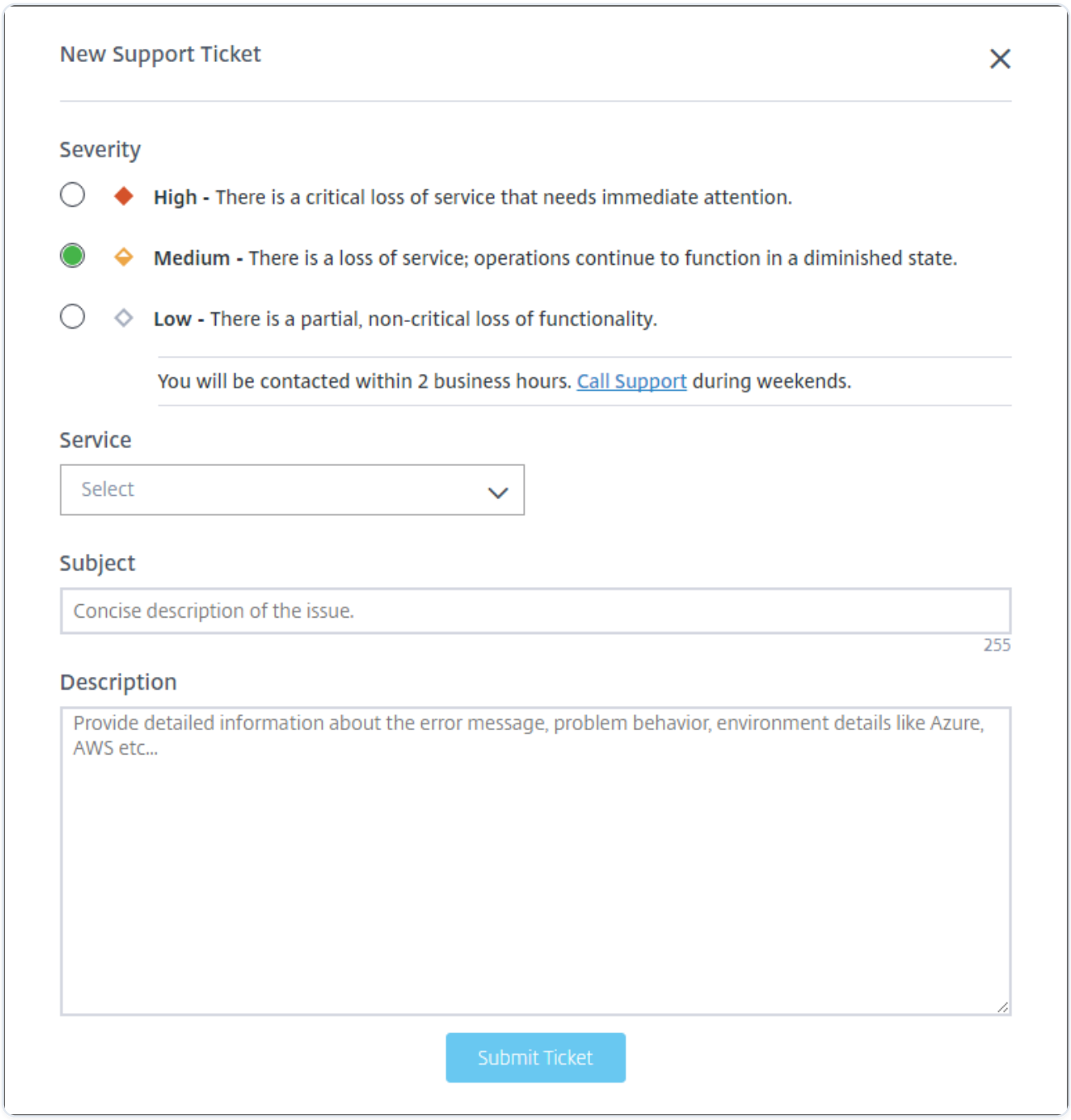
Vous pouvez également vous abonner aux notifications concernant des événements tels que les fenêtres de maintenance et les incidents de service. Pour plus d'informations sur l'état de santé des services Cloud, consultez (/fr-fr/citrix-cloud/overview/service-health.html).

Support technique

Si vous rencontrez un problème nécessitant une assistance technique, cliquez sur l'icône **Commentaires et support** en haut à droite de l'écran, puis sélectionnez **Ouvrir un ticket.**



Vous pouvez ensuite saisir les détails du problème dans le formulaire qui apparaît. Le support technique de Citrix vous contactera pour résoudre le problème.



Guide de déploiement sécurisé pour Citrix Cloud™ Government

Le Guide de déploiement sécurisé pour Citrix Cloud Government fournit un aperçu des meilleures pratiques de sécurité lors de l'utilisation de Citrix Cloud Government et décrit les informations que Citrix collecte et gère.

La Présentation technique de la sécurité de Citrix DaaS fournit des informations similaires pour Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops).

> **Remarque :**
>
> Dans cet article, le terme *client* fait référence aux agences gouvernementales et aux clients aux États-Unis qui utilisent Citrix Cloud Government.

Plan de contrôle

Conseils pour les administrateurs

- Utilisez des mots de passe forts et changez-les régulièrement.
- Tous les administrateurs d'un compte client peuvent ajouter et supprimer d'autres administrateurs. Assurez-vous que seuls les administrateurs de confiance ont accès à Citrix Cloud Government.
- Les administrateurs d'un client ont, par défaut, un accès complet à tous les services. Certains services offrent la possibilité de restreindre l'accès d'un administrateur. Consultez la documentation de chaque service pour plus d'informations.
- L'authentification à deux facteurs pour les administrateurs est réalisée grâce à l'intégration de Citrix Cloud Government avec Microsoft Entra ID.

Conformité des mots de passe

Citrix Cloud Government invite les administrateurs à modifier leur mot de passe si celui-ci a plus de 60 jours. Les nouveaux mots de passe doivent respecter tous les critères suivants :

- Au moins 12 caractères
- Inclure au moins une lettre majuscule et une lettre minuscule
- Inclure au moins un chiffre
- Inclure au moins un caractère spécial : `! @ # $ % \^ *? + = -`

Règles pour changer les mots de passe :

- Au moins un caractère du mot de passe actuel doit être modifié. Le mot de passe actuel ne peut pas être utilisé comme nouveau mot de passe.
- Les 24 mots de passe précédents ne peuvent pas être réutilisés.
- Le nouveau mot de passe doit être en vigueur pendant au moins un jour avant que Citrix Cloud Government n'autorise sa modification à nouveau.

Chiffrement et gestion des clés

Le plan de contrôle ne stocke pas d'informations client sensibles. Au lieu de cela, Citrix Cloud Government récupère les informations telles que les mots de passe administrateur à la demande (en les demandant explicitement à l'administrateur). Il n'y a pas de données au repos sensibles ou chiffrées. Par conséquent, vous n'avez pas besoin de gérer de clés.

Pour les données en transit, Citrix utilise la norme industrielle TLS 1.2 ou supérieure avec les suites de chiffrement les plus robustes. Les clients ne peuvent pas contrôler le certificat TLS utilisé, car Citrix Cloud Government est hébergé sur le domaine `cloud.us` appartenant à Citrix. Pour accéder à Citrix Cloud Government, les clients doivent utiliser un navigateur compatible avec TLS 1.2 ou supérieur et des suites de chiffrement robustes.

Les chiffrements robustes suivants sont recommandés :
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Pour plus d'informations sur le chiffrement et la gestion des clés au sein de chaque service cloud, consultez la documentation du service.

Souveraineté des données

Le plan de contrôle de Citrix Cloud Government est hébergé aux États-Unis. Les clients ne peuvent pas modifier l'emplacement d'hébergement.

Le client possède et gère les emplacements de ressources qu'il utilise avec Citrix Cloud Government. Un emplacement de ressource peut être créé dans n'importe quel centre de données, cloud, emplacement ou zone géographique souhaité par le client. Toutes les données commerciales critiques, telles que les documents, les feuilles de calcul, sont stockées dans les emplacements de ressources et sont sous le contrôle du client.

Audit et contrôle des modifications

Il n'y a pas d'audit ou de contrôle des modifications visible par le client disponible dans l'interface utilisateur ou les API de Citrix Cloud Government.

Citrix® dispose d'informations d'audit internes complètes. Si un client a une préoccupation, il est conseillé de contacter Citrix dans les 30 jours. Citrix examine les journaux d'audit pour déterminer l'administrateur qui a effectué une opération. Il examine également la date à laquelle elle a été effectuée et l'adresse IP associée à l'action.

Citrix Cloud Connector™

Installation

Pour des raisons de sécurité et de performances, Citrix recommande aux clients de ne pas installer le logiciel Cloud Connector sur un contrôleur de domaine.

De plus, les machines sur lesquelles le logiciel Cloud Connector est installé doivent se trouver à l'intérieur du réseau privé du client et non dans la DMZ. Pour connaître les exigences réseau et système et les instructions d'installation du Cloud Connector, consultez (/fr-fr/citrix-cloud-government/install-configure/create-resource-location.html).

Configuration

Le client est responsable de la mise à jour des machines sur lesquelles le Cloud Connector est installé avec les mises à jour de sécurité Windows.

Les clients peuvent utiliser un antivirus avec le Cloud Connector. Citrix effectue des tests avec McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8. Citrix prend en charge les clients qui utilisent d'autres produits antivirus standard de l'industrie.

Dans l'Active Directory (AD) du client, le compte machine du Cloud Connector doit être restreint à un accès en lecture seule. Dans Active Directory, c'est la configuration par défaut. De plus, le client peut activer la journalisation et l'audit AD sur le compte machine du Cloud Connector pour surveiller toute activité d'accès AD.

Connexion à la machine hébergeant le Cloud Connector

Le Cloud Connector contient des informations de sécurité sensibles telles que les mots de passe administratifs. Seuls les administrateurs les plus privilégiés peuvent se connecter aux machines hébergeant le Cloud Connector (par exemple, pour effectuer des opérations de maintenance). En

général, un administrateur n'a pas besoin de se connecter à ces machines pour gérer un produit Citrix. Le Cloud Connector est autonome à cet égard.

N'autorisez pas les utilisateurs finaux à se connecter aux machines hébergeant le Cloud Connector.

Installation de logiciels supplémentaires sur les machines Cloud Connector

Les clients peuvent installer un logiciel antivirus et des outils d'hyperviseur (s'ils sont installés sur une machine virtuelle) sur les machines où le Cloud Connector est installé. Cependant, Citrix recommande aux clients de ne pas installer d'autres logiciels sur ces machines. D'autres logiciels créent davantage de vecteurs d'attaque de sécurité possibles et pourraient réduire la sécurité de la solution Citrix Cloud Government globale.

Configuration des ports entrants et sortants

Le Cloud Connector nécessite que le port sortant 443 soit ouvert avec un accès à Internet. Le Cloud Connector n'a pas de ports entrants accessibles depuis Internet.

Les clients peuvent placer le Cloud Connector derrière un proxy web pour surveiller ses communications Internet sortantes. Cependant, le proxy web doit fonctionner avec des communications chiffrées SSL/TLS.

Le Cloud Connector peut avoir plus de ports sortants avec accès à Internet. Le Cloud Connector négocie sur une large gamme de ports pour optimiser la bande passante et les performances du réseau si plus de ports sont disponibles.

Le Cloud Connector doit avoir une large gamme de ports entrants et sortants ouverts au sein du réseau interne. Le tableau ci-dessous répertorie l'ensemble de base des ports ouverts requis.

PORTS CLIENTS	PORT SERVEUR	SERVICE
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	Mappeur de points de terminaison RPC
49152 -65535/TCP	464/TCP/UDP	Changement de mot de passe Kerberos
49152 -65535/TCP	49152-65535/TCP	RPC pour LSA, SAM, Netlogon (*)

PORTS CLIENTS	PORT SERVEUR	SERVICE
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB

Chacun des services utilisés dans Citrix Cloud Government étend la liste des ports ouverts requis. Pour plus d'informations, consultez Exigences de connectivité pour Citrix Cloud Government.

Surveillance des communications sortantes

Le Cloud Connector communique en sortie vers Internet sur le port 443, à la fois vers les serveurs Citrix Cloud Government et vers les serveurs Microsoft Azure Service Bus.

Le Cloud Connector communique avec les contrôleurs de domaine sur le réseau local qui se trouvent dans la forêt Active Directory où résident les machines hébergeant le Cloud Connector.

Pendant le fonctionnement normal, le Cloud Connector communique uniquement avec les contrôleurs de domaine dans les domaines qui sont répertoriés comme **Utiliser pour les abonnements** sur la page **Gestion des identités et des accès** dans l'interface utilisateur de Citrix Cloud Government.

Lors de la sélection des domaines à configurer comme **Utiliser pour les abonnements**, le Cloud Connector communique avec les contrôleurs de domaine dans tous les domaines de la forêt Active Directory où résident les machines hébergeant le Cloud Connector.

Chaque service au sein de Citrix Cloud Government étend la liste des serveurs et des ressources internes que le Cloud Connector pourrait contacter pendant les opérations normales. De plus, les clients ne peuvent pas contrôler les données que le Cloud Connector envoie à Citrix. Pour plus d'informations sur les ressources internes des services et les données envoyées à Citrix, consultez Exigences de connectivité.

Consultation des journaux du Cloud Connector

Toute information pertinente ou exploitable pour un administrateur est disponible dans le **Journal d'événements** Windows sur la machine Cloud Connector.

Consultez les journaux d'installation du Cloud Connector dans les répertoires suivants :

- %AppData%\\Local\\Temp\\CitrixLogs\\CloudServicesSetup
- %windir%\\Temp\\CitrixLogs\\CloudServicesSetup

Les journaux de ce que le Cloud Connector envoie au cloud se trouvent dans %ProgramData%\\Citrix\\WorkspaceCloud\\Logs.

Les journaux du répertoire WorkspaceCloud\\Logs sont supprimés lorsqu'ils dépassent un seuil de taille spécifié. L'administrateur peut contrôler ce seuil de taille en ajustant la valeur de la clé de registre pour `HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CloudServices\\AgentAdministration\\MaximumLogSpaceMegabytes`.

Configuration SSL/TLS

La configuration de base du Cloud Connector ne nécessite aucune configuration SSL/TLS spéciale.

Le Cloud Connector doit faire confiance à l'autorité de certification (CA) utilisée par les certificats SSL/TLS de Citrix Cloud Government et par les certificats SSL/TLS de Microsoft Azure Service Bus. Citrix et Microsoft pourraient modifier les certificats et les CA à l'avenir. Mais le Cloud Connector utilise toujours des CA qui font partie de la liste standard des éditeurs approuvés de Windows.

Chaque service au sein de Citrix Cloud Government a des exigences de configuration SSL différentes. Pour plus d'informations, consultez la présentation technique de la sécurité pour chaque service (énumérée au début de cet article).

Mises à jour du Connector

Lorsque des mises à jour logicielles Citrix sont disponibles, le Cloud Connector s'auto-gère. Ne désactivez pas les redémarrages et n'imposez pas d'autres restrictions au Cloud Connector. Ces actions empêchent le Cloud Connector de se mettre à jour en cas de mise à jour critique.

Le client n'est pas tenu de prendre d'autres mesures pour réagir aux problèmes de sécurité. Le Cloud Connector applique automatiquement les correctifs de sécurité et les mises à jour des logiciels Citrix.

Conseils pour la gestion des comptes compromis

- Vérifiez la liste des administrateurs dans Citrix Cloud Government et supprimez ceux qui ne sont pas fiables.
- Désactivez tous les comptes compromis au sein de l'Active Directory de votre entreprise.
- Contactez Citrix et demandez la rotation des secrets d'autorisation stockés pour tous les Cloud Connectors du client. En fonction de la gravité de la violation, prenez les mesures suivantes :
  - **Faible risque :** Citrix peut faire pivoter les secrets au fil du temps. Les Cloud Connectors continuent de fonctionner normalement. Les anciens secrets d'autorisation deviennent invalides en 2 à 4 semaines. Surveillez le Cloud Connector pendant cette période pour vous assurer qu'il n'y a pas d'opérations inattendues.
  - **Risque élevé continu :** Citrix peut révoquer tous les anciens secrets. Les Cloud Connectors existants ne fonctionneront plus. Pour reprendre un fonctionnement normal, le client doit désinstaller et réinstaller le Cloud Connector sur toutes les machines applicables.

Essais de service pour Citrix Cloud™ Government

Les essais pour les services individuels de Citrix Cloud Government sont fournis via la plateforme Citrix Cloud Government. La fonctionnalité d'un essai de service est la même que celle du service acheté, ils conviennent donc pour une preuve de concept (POC), un projet pilote ou une utilisation similaire.

L'accès aux essais de Citrix Cloud Government est géré par service. Pour personnaliser votre expérience et fournir les services les plus importants pour vos utilisateurs.

Lorsque vous êtes prêt à acheter des services, vous convertissez votre essai en un compte de production. Il n'est pas nécessaire de reconfigurer quoi que ce soit ou de créer un compte de production distinct.

En bref sur les essais de service

	ESSAI CITRIX CLOUD GOVERNMENT
Nombre d'abonnés autorisés	25
Durée maximale	60 jours calendaires. Vous ne pouvez demander un essai pour le service qu'une seule fois.

	ESSAI CITRIX CLOUD GOVERNMENT
Disponibilité	Disponibilité restreinte
Emplacement des ressources	Fourni et configuré par le client
Durée de la session utilisateur	Illimité
Intégration de Microsoft Active Directory local	Oui
Choix des emplacements de ressources	Oui
Déploiement sur site	Oui
Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops™)	Ensemble complet de fonctionnalités
Workspace	Ensemble complet de fonctionnalités
Personnalisable	Oui

Demander un essai de service

Pour demander un essai de service, vous devez contacter un représentant commercial Citrix® et fournir votre ID d'organisation (OrgID). Le représentant commercial s'assure que vous disposez de toutes les informations nécessaires pour commencer à utiliser le service.

Pour demander un essai et localiser votre OrgID, suivez les étapes suivantes :

1. Connectez-vous à votre compte Citrix Cloud Government.
2. Sous **Services disponibles**, localisez le service que vous souhaitez essayer et cliquez sur **Demander un essai**.
3. Notez l'OrgID affiché sur la notification qui apparaît.
4. Cliquez sur **Parler à un représentant commercial** pour enregistrer votre demande d'essai.

Lorsque votre essai est approuvé et prêt à être utilisé, vous recevez une notification par e-mail. Vous disposez de 60 jours pour effectuer l'essai.

> **Remarque :**

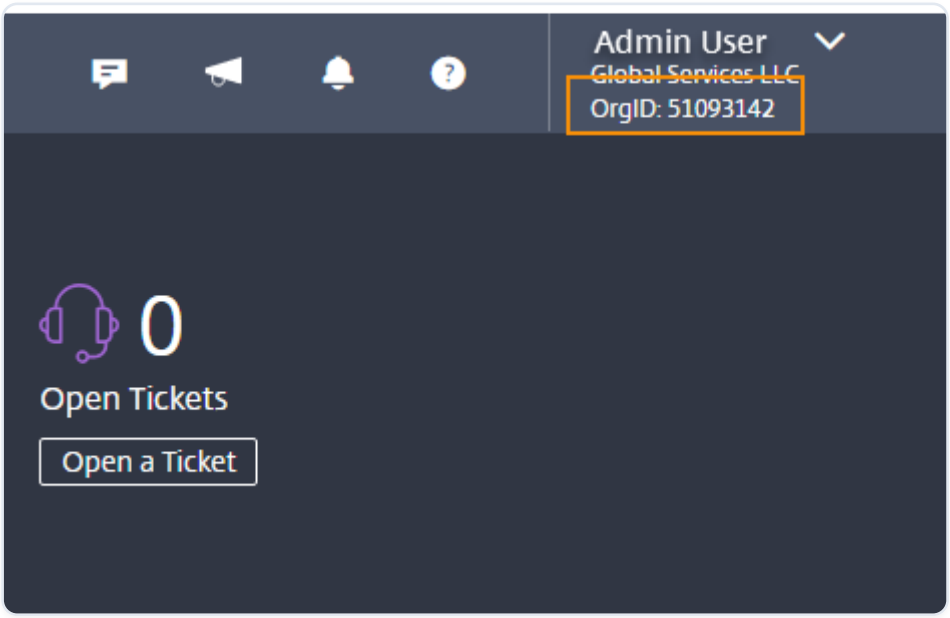
> Afin de garantir la meilleure expérience client, Citrix se réserve le droit de limiter les essais à certains participants à tout moment.

Acheter des services

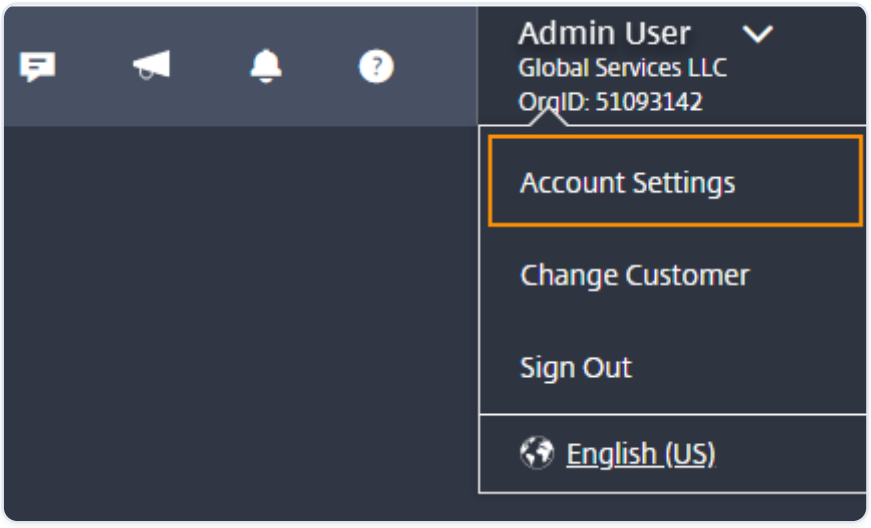
Lorsque vous êtes prêt à convertir votre essai en service de production, contactez un représentant commercial Citrix.

Pour finaliser l'achat, vous avez besoin de votre OrgID, disponible dans la console de gestion Citrix Cloud Government. Votre OrgID apparaît aux emplacements suivants :

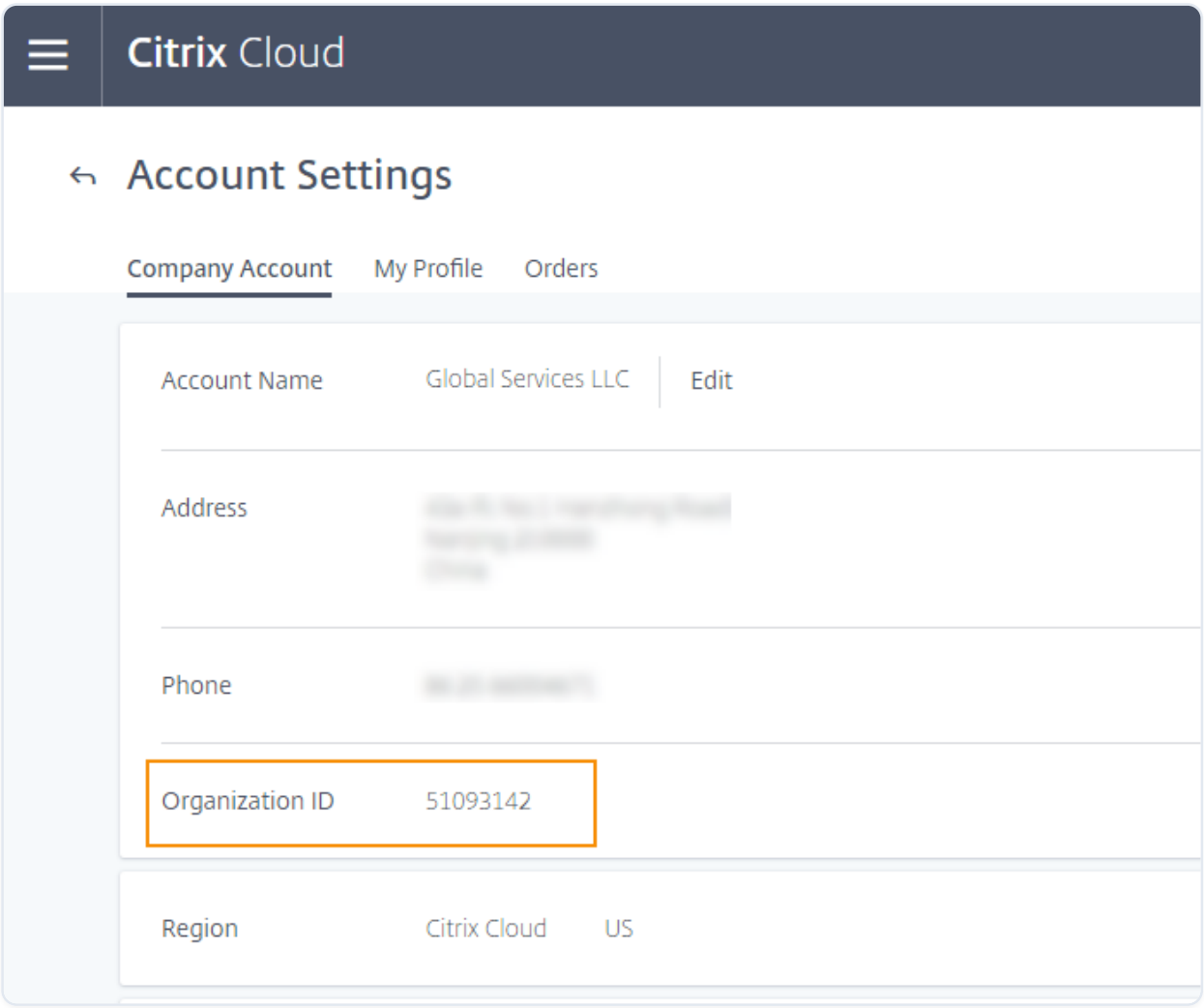
- Dans le coin supérieur droit de la console de gestion, votre OrgID est affiché sous le nom de votre compte.



- Dans le menu supérieur droit, cliquez sur **Paramètres du compte**.



Votre OrgID est affiché dans le champ ID d'organisation.



Important :

Si vous n'achetez pas avant la fin de votre essai de 60 jours, le service est résilié et Citrix archive toutes les données et tous les paramètres pendant 90 jours. Si vous achetez pendant la période de 90 jours, votre essai est réactivé et converti en service de production.

S’inscrire à Citrix Cloud™ Government

Cet article vous guide tout au long du processus d’inscription à Citrix Cloud Government et de l’exécution des tâches requises pour intégrer votre compte avec succès.

Qu’est-ce qu’un OrgID ?

Un OrgID est l’identifiant unique attribué à votre compte Citrix Cloud Government. Votre OrgID est associé à une adresse de site physique, généralement l’adresse commerciale de votre entreprise. Les organisations ont généralement un seul OrgID. Si vous avez différentes succursales ou

différents services qui gèrent vos actifs séparément, Citrix permet à une organisation d'avoir plusieurs OrgID.

Qu'est-ce qu'un compte Citrix Cloud Government ?

Un compte Citrix Cloud Government vous permet d'utiliser un ou plusieurs services Citrix Cloud Government pour fournir en toute sécurité vos applications et vos données. Citrix Cloud Government crée un compte OrgID identifié de manière unique. Il est important d'utiliser le bon compte Citrix Cloud Government, en fonction de la façon dont votre organisation a configuré les OrgID. Vos achats et l'accès administrateur peuvent se poursuivre sur les mêmes OrgID.

Exigences d'authentification multifacteur

Pour assurer la sécurité de votre compte Citrix Cloud Government, Citrix Cloud Government exige que tous les clients s'inscrivent à l'authentification multifacteur. Pour vous inscrire, vous avez besoin d'un appareil, tel qu'un ordinateur ou un appareil mobile. Avec une application d'authentification installée, telle que Citrix SSO, le compte est sûr et sécurisé.

Intégrer votre compte Citrix Cloud

- Si vous êtes un client Citrix existant et que vous n'avez pas de compte Citrix Cloud, veuillez intégrer le locataire cloud en visitant Mon organisation et en suivant les étapes de Gestion des comptes Citrix Cloud.
- Si vous êtes nouveau chez Citrix®, veuillez vous inscrire en contactant les représentants de compte pour faire créer votre OrgID.

Acheter Citrix Cloud Government

Commander Citrix Cloud Government

Pour commander Citrix Cloud Government pour votre organisation, contactez un représentant commercial Citrix. Une fois la commande terminée, vous recevez un e-mail de confirmation avec un lien pour configurer votre compte. Lors de la configuration de votre compte, vous créez le premier administrateur de compte en utilisant l'adresse e-mail de votre commande et un mot de passe que vous spécifiez.

Vérifier votre commande

Cliquez sur le lien dans votre e-mail de confirmation de commande. Une page de configuration de Citrix Cloud Government s'affiche dans une fenêtre de navigateur, affichant les détails de votre commande. Cliquez sur **Continuer**.

Créer un mot de passe

Saisissez et confirmez le mot de passe fort que vous souhaitez utiliser avec votre compte Citrix Cloud Government, puis cliquez sur **Continuer**. En tant que premier administrateur du compte, vous utilisez ce mot de passe avec l'adresse e-mail de votre commande pour vous connecter à Citrix Cloud Government.

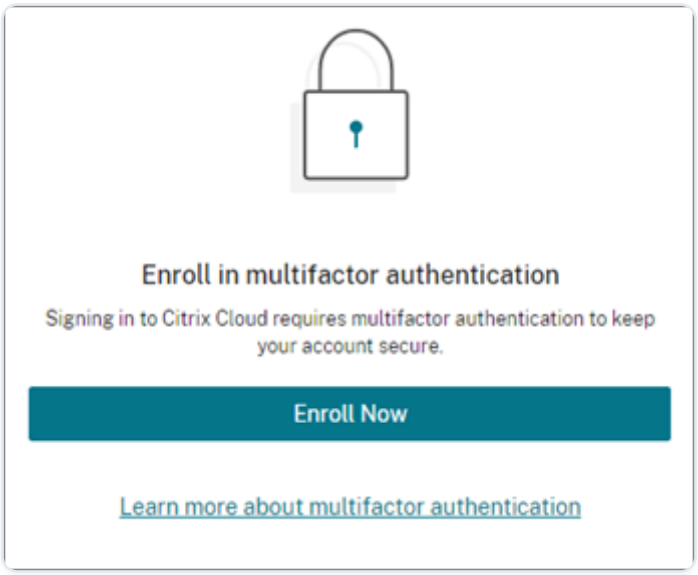
Connectez-vous avec vos informations d'identification Citrix Cloud Government

1. Connectez-vous à Citrix Cloud Government à l'adresse https://citrix.cloud.us en utilisant l'adresse e-mail que vous avez utilisée lors de votre commande et le mot de passe que vous avez choisi précédemment.
    - Citrix Cloud Government affiche votre région d'origine. Actuellement, Citrix Cloud Government inclut une seule région géographique des États-Unis, donc seule cette région apparaît.
2. Acceptez les Conditions d'utilisation, puis cliquez sur **Continuer**. La console de gestion Citrix Cloud Government apparaît.

S'inscrire à l'authentification multifacteur

Pour assurer la sécurité de votre compte administrateur, Citrix Cloud Government vous demande d'utiliser l'authentification multifacteur lorsque vous vous connectez. L'inscription à l'authentification multifacteur empêche l'accès non autorisé à votre compte administrateur et ne nécessite qu'un appareil, tel qu'un ordinateur ou un appareil mobile. Avec une application d'authentification installée qui suit la norme mot de passe à usage unique basé sur le temps, telle que Citrix SSO, le compte est sûr et sécurisé.

Si vous n'êtes pas inscrit à l'authentification multifacteur, Citrix Cloud Government vous invite à vous inscrire lorsque vous vous connectez.



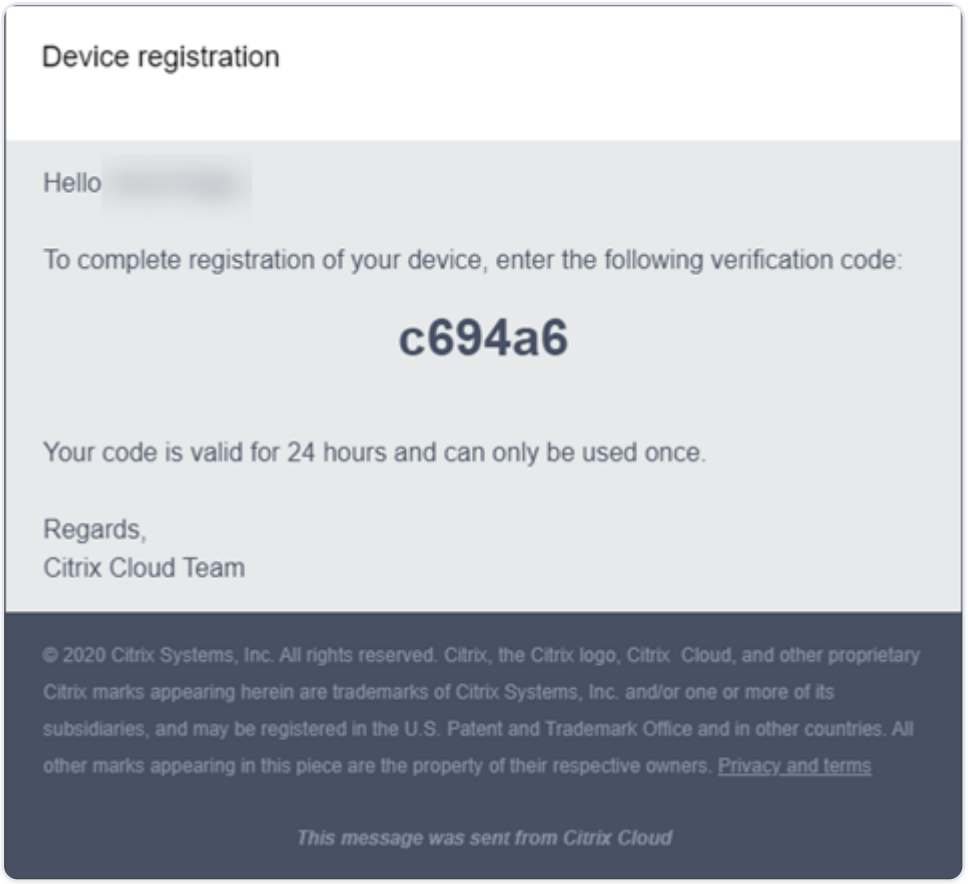
Lors de l'inscription, Citrix Cloud Government présente un code QR et une clé. Selon votre application d'authentification, vous scannez le code QR ou saisissez la clé pour enregistrer votre appareil. Pour un processus d'inscription fluide, Citrix recommande de télécharger et d'installer cette application sur votre appareil au préalable. Citrix Cloud Government génère également des codes de sauvegarde à usage unique. Les codes de sauvegarde sont utilisés pour accéder à votre compte si vous perdez votre appareil ou si vous ne pouvez pas utiliser votre application d'authentification.

Remarques :

- Lorsque vous vous connectez à Citrix Cloud Government, vérifiez que vous consultez la page de connexion de Citrix Cloud Government à l'adresse https://citrix.cloud.us. Si vous vous connectez à Citrix Cloud Government en utilisant une URL différente, l'inscription à l'authentification multifacteur échoue.
- Après votre inscription, l'authentification multifacteur est utilisée pour toutes les organisations clientes auxquelles vous appartenez dans Citrix Cloud Government. Vous ne pouvez pas désactiver l'authentification multifacteur après avoir terminé le processus d'inscription.
- Vous ne pouvez enregistrer qu'un seul appareil. Si vous enregistrez un autre appareil ultérieurement, Citrix Cloud Government supprime l'enregistrement de l'appareil actuel et le remplace par le nouvel appareil. Pour plus d'informations, consultez Modifier votre appareil pour l'authentification multifacteur.

Pour enregistrer votre appareil pour l'authentification multifacteur :

1. Accédez à Citrix Cloud Government à l'adresse https://citrix.cloud.us et vérifiez que l'URL redirige vers https://citrix.cloud.us. Connectez-vous à l'aide de vos informations d'identification Citrix Cloud Government. Citrix Cloud Government vous envoie un e-mail contenant un code de vérification.



Device registration

Hello

To complete registration of your device, enter the following verification code:

c694a6

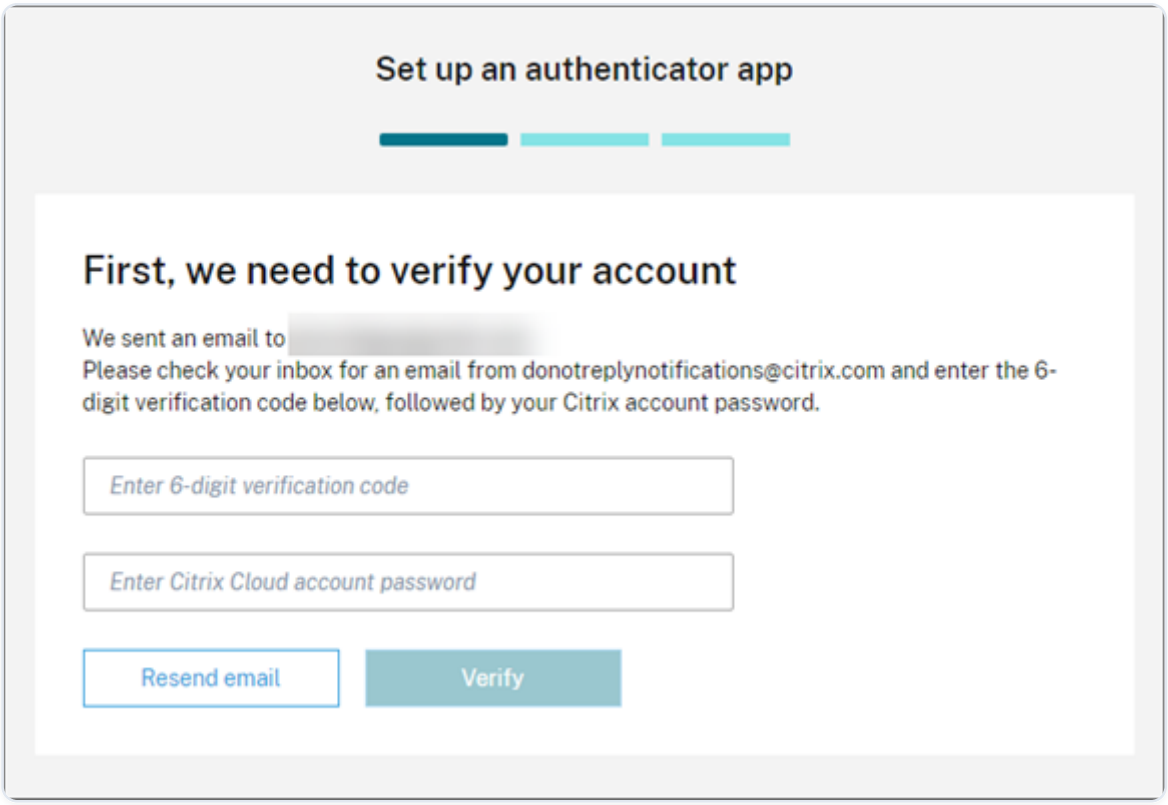
Your code is valid for 24 hours and can only be used once.

Regards,
Citrix Cloud Team

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners. Privacy and terms

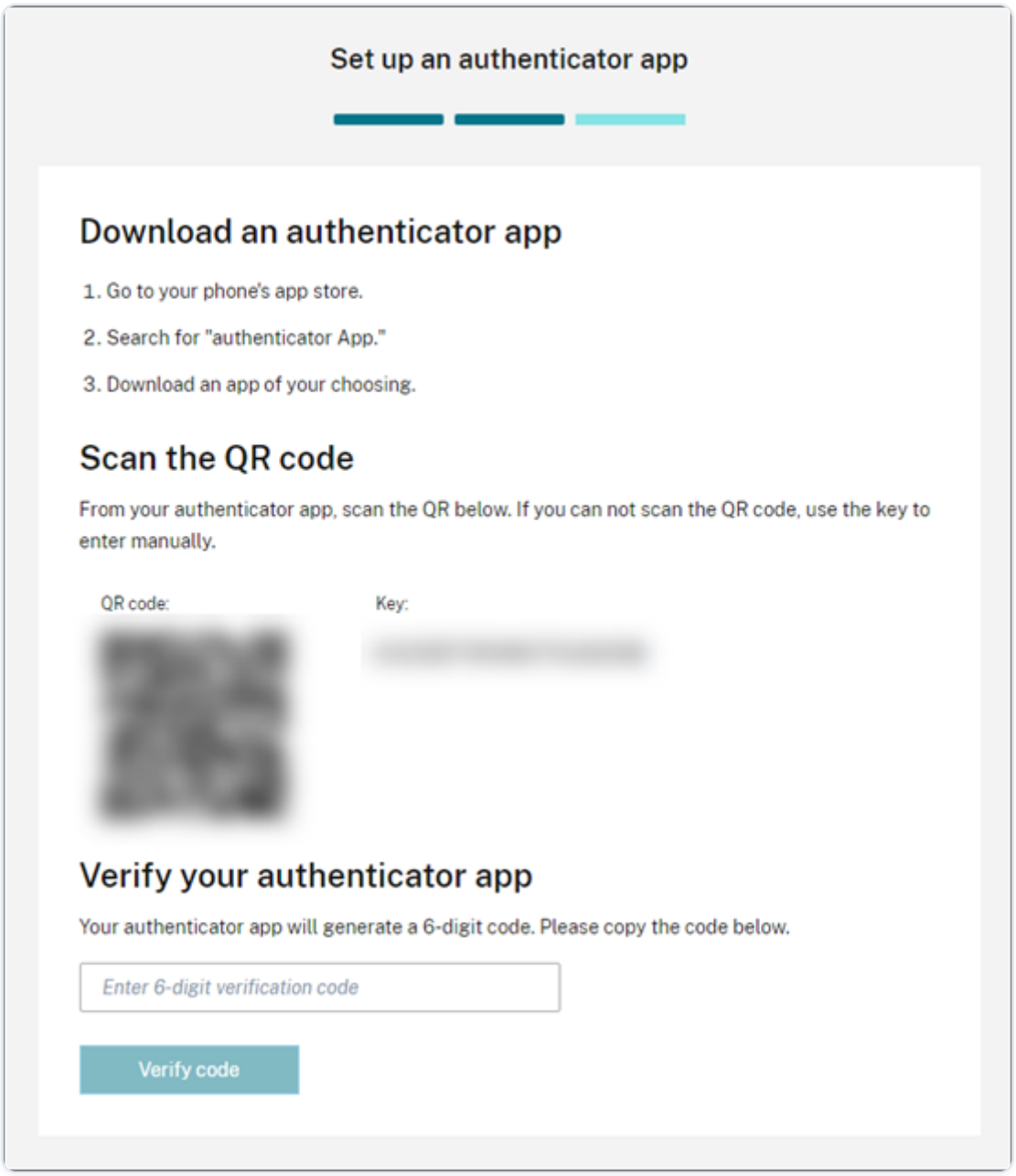
This message was sent from Citrix Cloud

2. Après avoir reçu l'e-mail, saisissez le code de vérification à 6 chiffres et votre mot de passe Citrix Cloud Government, puis sélectionnez **Vérifier**.



3. Depuis l'application d'authentification, scannez le code QR ou saisissez la clé manuellement. Votre application d'authentification affiche une entrée pour Citrix Cloud Government et génère

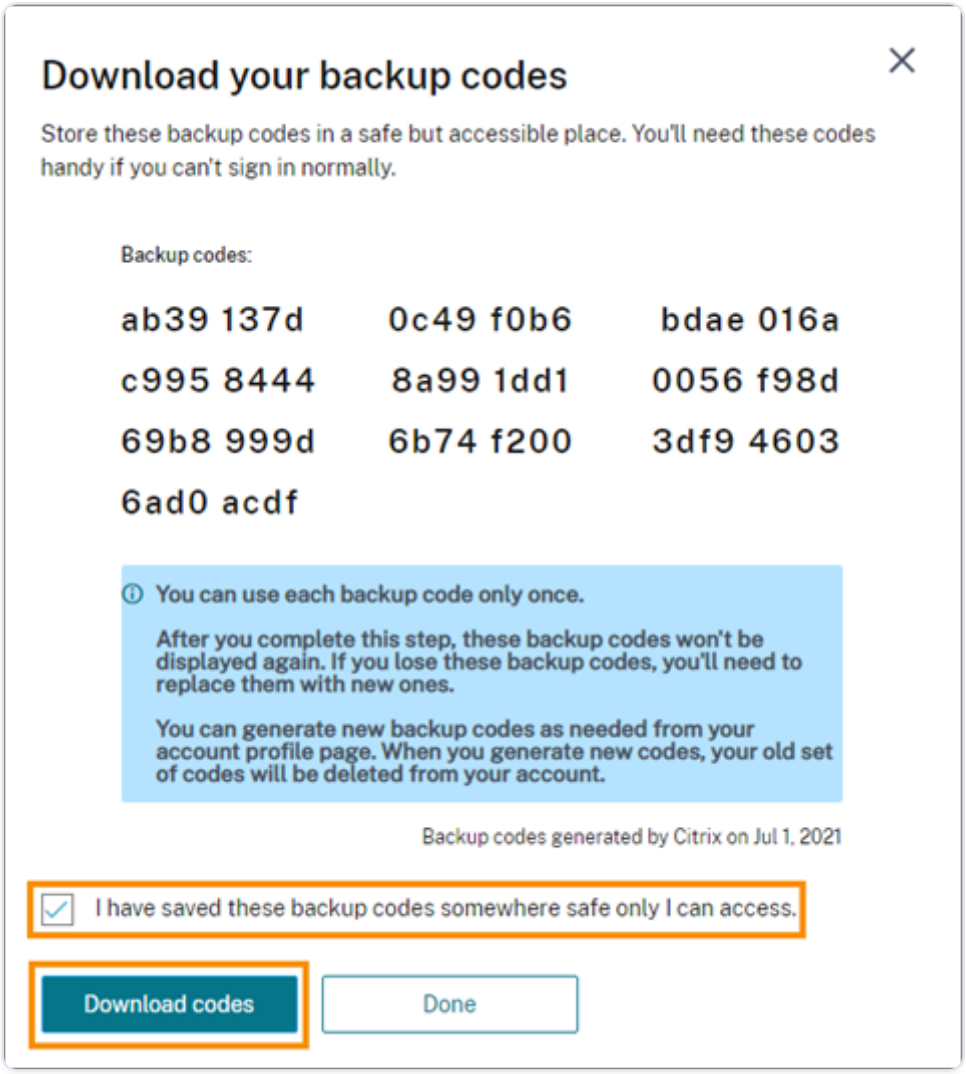
un code à 6 chiffres.



4. Sous **Vérifier votre application d'authentification**, saisissez le code de votre application d'authentification et sélectionnez **Vérifier le code**.
5. Configurez les méthodes de récupération de compte suivantes au cas où vous perdriez votre appareil ou ne pourriez pas utiliser votre application d'authentification :

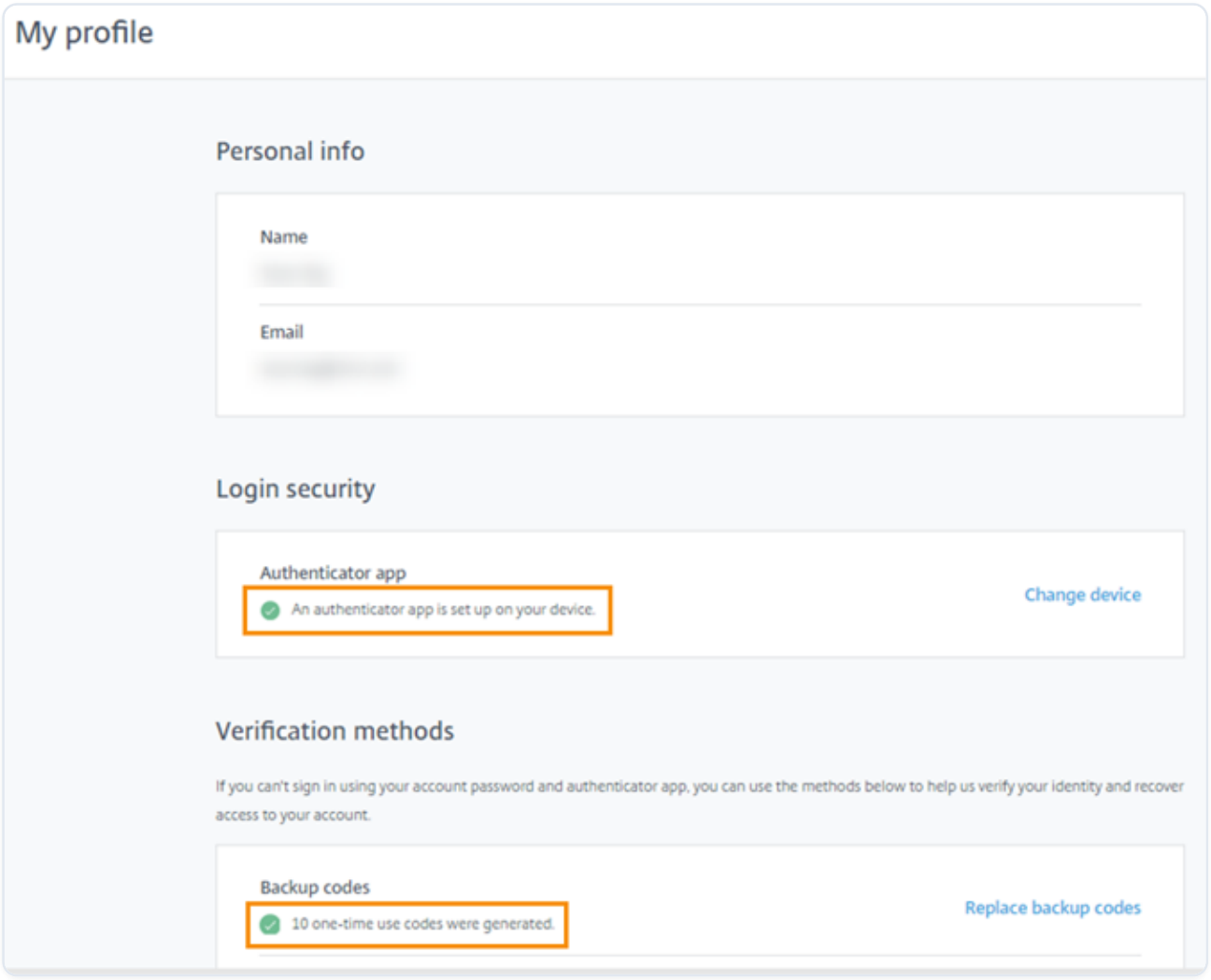
    - Téléphone de récupération (obligatoire) : Sélectionnez **Ajouter un téléphone de récupération** et saisissez un numéro de téléphone qu'un représentant du support Citrix peut utiliser pour vous appeler et vérifier votre identité. Le support Citrix utilise ce numéro de téléphone uniquement lorsque vous demandez de l'aide pour vous connecter. Citrix recommande d'utiliser un numéro de téléphone fixe.

- Codes de secours (obligatoire) : Sélectionnez **Générer des codes de secours** pour créer un ensemble de codes de secours à usage unique afin de vous aider à vous connecter si vous ne pouvez pas utiliser votre application d'authentification. Lorsque vous y êtes invité, sélectionnez **Télécharger les codes** pour télécharger votre code de secours sous forme de fichier texte. Ensuite, sélectionnez **J'ai enregistré ces codes** et sélectionnez **Fermer**.

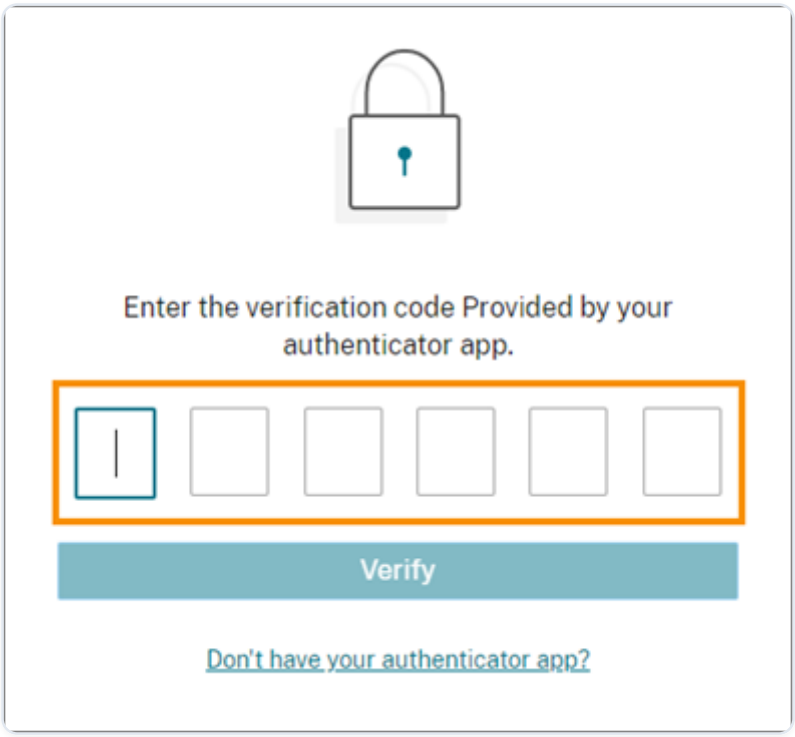


6. Sélectionnez **Terminer** pour finaliser l'enregistrement.

Une fois votre enregistrement terminé, la console Citrix Cloud apparaît. Dans le menu supérieur droit, sélectionnez **Mon profil**. Après un enregistrement réussi, la section **Application d'authentification** affiche une coche verte et la page Mon profil affiche vos méthodes de récupération configurées.



La prochaine fois que vous vous connecterez avec vos informations d'identification d'administrateur Citrix Cloud Government, Citrix Cloud Government vous demandera le code de vérification de votre application d'authentification.



Après vous être inscrit à l'authentification multifacteur, la connexion à votre compte Citrix Cloud Government vous amène à la page de la console Citrix Cloud. Si vous devez enregistrer un autre appareil, générez davantage de codes de secours. Mettez à jour votre numéro de téléphone de récupération ultérieurement, afin de pouvoir effectuer ces tâches depuis votre page Mon profil.

Pour plus d'instructions, consultez Gérer votre méthode MFA principale dans la documentation produit de Citrix Cloud.

Configuration système requise

Exigences de connectivité pour Citrix Cloud™ Government

Citrix Cloud Government fournit des fonctions administratives (via un navigateur web) et des requêtes opérationnelles (à partir d'autres composants installés) qui se connectent aux ressources au sein du déploiement d'un client. Ce document définit les exigences et les considérations relatives à l'établissement de la connectivité entre les ressources du client et Citrix Cloud Government.

La connexion à Internet depuis vos centres de données nécessite l'ouverture du port 443 pour les connexions sortantes. Cependant, pour fonctionner dans des environnements contenant un serveur proxy Internet ou des restrictions de pare-feu, une configuration supplémentaire pourrait être nécessaire.

Exigences relatives à la sécurité de la couche de transport

Citrix Cloud Government prend en charge Transport Layer Security (TLS) 1.2 pour les connexions basées sur TCP entre les composants. Citrix Cloud n'autorise pas la communication via TLS 1.0 ou TLS 1.1.

Pour accéder à Citrix Cloud Government, vous devez utiliser un navigateur qui prend en charge TLS 1.2 et avoir configuré des suites de chiffrement acceptées. Pour plus d'informations, consultez Chiffrement et gestion des clés.

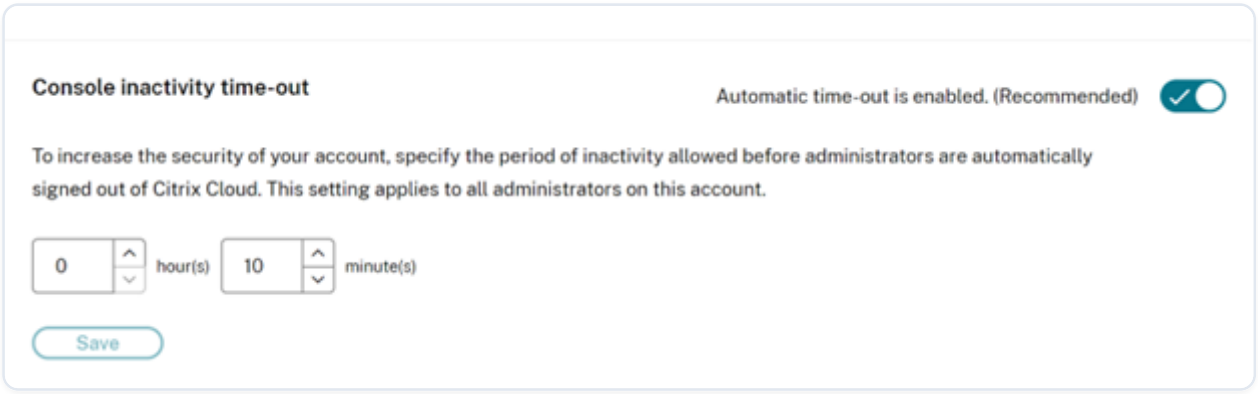
Console de gestion Citrix Cloud Government

La console de gestion Citrix Cloud Government est une console web à laquelle vous pouvez accéder après vous être connecté à https://citrix.cloud.us. Les pages web de la console nécessitent davantage de ressources Internet lors de la connexion ou de l'exécution d'opérations spécifiques.

Délai d'inactivité configurable pour la console

En tant qu'administrateur avec accès complet, vous pouvez configurer la durée d'inactivité sur la console Citrix Cloud avant que les administrateurs ne soient automatiquement déconnectés. Une

fois configurée, la période de délai d'expiration spécifiée sera appliquée à tous les administrateurs du compte Citrix Cloud.



Lorsque la fonctionnalité est activée, les administrateurs seront déconnectés après la période d'inactivité configurée, et le délai d'expiration de la session sera réinitialisé à chaque connexion ultérieure.

Lorsque la fonctionnalité est désactivée, il n'y a pas de minuteur d'inactivité, et les administrateurs ne seront déconnectés que lorsque la limite de session de 12 heures sera atteinte.

Remarque :

- Cette fonctionnalité est activée par défaut.
- Le délai d'inactivité configurable est de 10 minutes à 1 heure.
- Le délai d'inactivité par défaut est de 15 minutes.

Configuration du proxy

Si vous vous connectez via un serveur proxy, la console de gestion fonctionne en utilisant la même configuration que celle appliquée à votre navigateur web. La console fonctionne dans le contexte utilisateur, ce qui permet de configurer des serveurs proxy qui nécessitent une authentification utilisateur pour fonctionner comme prévu.

Configuration du pare-feu

Pour que la console de gestion fonctionne, le port 443 doit être ouvert pour les connexions sortantes. Vous pouvez tester la connectivité générale en naviguant dans la console.

Citrix Cloud Connector™

Le Citrix Cloud Connector est un package logiciel qui déploie un ensemble de services exécutés sur des serveurs Microsoft Windows. La machine hébergeant le Cloud Connector réside au sein du réseau où se trouvent les ressources que vous utilisez avec Citrix Cloud Government. Le Cloud Connector se connecte à Citrix Cloud Government, lui permettant d'opérer et de gérer vos ressources selon les besoins.

Pour connaître les exigences d'installation du Cloud Connector, consultez Exigences du Citrix Cloud Connector. Pour fonctionner, le Cloud Connector nécessite une connectivité sortante sur le port 443. Après l'installation, le Cloud Connector peut avoir des exigences d'accès supplémentaires en fonction du service Citrix Cloud Government avec lequel il est utilisé.

FQDN autorisés pour le Cloud Connector

Pour une liste complète des noms de domaine complets (FQDN) auxquels le Cloud Connector accède, reportez-vous au fichier JSON disponible à l'adresse `<https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-gov/allowlist.json>`. La liste est classée par produit et comprend un journal des modifications pour chaque groupe de FQDN.

Certains de ces FQDN sont spécifiques à un client et incluent des sections de modèle entre crochets angulaires. Ces sections de modèle doivent être remplacées par les valeurs réelles avant utilisation. Par exemple, pour `<CUSTOMER_ID>.xendesktop.net`, vous remplacez `<CUSTOMER_ID>` par l'ID client réel de votre compte Citrix Cloud. Vous trouverez l'ID client en haut de l'onglet **Accès API** dans **Gestion des identités et des accès**.

Connectivité du service Citrix DaaS™

Emplacement des ressources Citrix / Cloud Connector :

- `https://*.citrixworkspacesapi.us`
- `https://*.cloud.us`
- `https://*.apps.cloud.us`
- `https://*.blob.core.usgovcloudapi.net`
- `https://*.servicebus.usgovcloudapi.net`
- `https://*.xendesktop.us`

Console d'administration :

- `https://*.citrixworkspacesapi.us`

- `https://*.cloud.us`
- `https://*.blob.core.usgovcloudapi.net`
- `https://*.xendesktop.us`

SDK PowerShell distant Citrix DaaS

Pour utiliser le SDK PowerShell distant Citrix DaaS, ajoutez les URL suivantes à la liste blanche :

- `https://*.cloud.us`
- `https://*.citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

Exigences relatives à Citrix Cloud Connector™

Le Citrix Cloud™ Connector est un composant qui établit une connexion entre Citrix Cloud et vos emplacements de ressources. Cet article décrit les exigences et les scénarios de déploiement, la prise en charge d'Active Directory et de FIPS, ainsi que les options de dépannage.

Configuration système requise

Les machines hébergeant le Cloud Connector doivent satisfaire aux exigences suivantes. Citrix® recommande fortement d'installer au moins deux Cloud Connectors dans chaque emplacement de ressources afin d'assurer une haute disponibilité.

Consultez également nos recommandations de bonnes pratiques pour la configuration des machines Cloud Connector pour Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops) : Considérations relatives à la mise à l'échelle et à la taille des Cloud Connectors.

Systèmes d'exploitation

Les systèmes d'exploitation suivants sont pris en charge :

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Le Cloud Connector n'est pas pris en charge pour une utilisation avec Windows Server Core.

Exigences .NET

Microsoft .NET Framework 4.7.2 ou version ultérieure est requis.

Exigences du serveur

- Utilisez des machines dédiées pour héberger le Cloud Connector. N'installez aucun autre composant sur ces machines.
- Les machines ne sont **pas** configurées en tant que contrôleurs de domaine Active Directory. L'installation du Cloud Connector sur un contrôleur de domaine n'est pas prise en charge.
- L'horloge du serveur est réglée à l'heure UTC correcte.

Conseils pour Windows Update

Citrix recommande fortement d'activer Windows Update sur toutes les machines hébergeant le Citrix Cloud Connector. Le Citrix Cloud Connector effectue des vérifications régulières des redémarrages en attente, qui peuvent être déclenchés par divers facteurs, y compris les mises à jour Windows, toutes les cinq minutes. Tout redémarrage détecté est exécuté rapidement, indépendamment du calendrier de jours préféré défini sur l'emplacement des ressources. Cette approche proactive garantit que le Citrix Cloud Connector n'est pas laissé dans un état de mise à jour en attente pendant une période prolongée, maintenant ainsi la stabilité du système.

La plateforme Citrix Cloud gère les redémarrages pour maintenir la disponibilité, n'autorisant qu'un seul Citrix Cloud Connector à redémarrer à la fois. Lors de la configuration de Windows Update, assurez-vous que Windows est configuré pour télécharger et installer automatiquement les mises à jour en dehors des heures de bureau. Cependant, les redémarrages automatiques ne sont pas autorisés pendant au moins quatre heures afin de laisser au Citrix Cloud Connector suffisamment de temps pour gérer le processus de redémarrage. De plus, vous pouvez établir un mécanisme de redémarrage de secours à l'aide d'une stratégie de groupe ou d'un outil de gestion de système pour les situations où une machine doit être redémarrée après une mise à jour. Pour plus d'informations, consultez Gérer les redémarrages des appareils après les mises à jour.

> **Remarque :**
>
> - Si le client ne souhaite pas que son Citrix Cloud Connector redémarre pendant les heures de bureau, nous suggérons au client de planifier les mises à jour Windows en conséquence en dehors des heures de bureau.

- Chaque Citrix Cloud Connector nécessite environ 10 minutes pour redémarrer, ce qui inclut le temps nécessaire pour se synchroniser avec la plateforme Citrix Cloud afin de garantir qu'un seul Citrix Cloud Connector redémarre à un moment donné. Par conséquent, le délai minimum recommandé de quatre heures pour les redémarrages automatiques, comme mentionné précédemment, peut être ajusté en conséquence à une durée plus courte ou plus longue en fonction du nombre de Citrix Cloud Connectors dans le locataire.

Exigences de validation des certificats

Les binaires et les points de terminaison du Cloud Connector que le Cloud Connector contacte sont protégés par des certificats X.509 émis par des autorités de certification (CA) d'entreprise largement respectées. La vérification des certificats dans l'infrastructure à clé publique (PKI) inclut la liste de révocation de certificats (CRL).

Lorsqu'un client reçoit un certificat, il vérifie s'il fait confiance à l'autorité de certification qui a émis le certificat. Il vérifie également si le certificat figure sur une CRL. Si le certificat figure sur une CRL, il est révoqué et ne peut pas être considéré comme fiable, même s'il semble valide.

Les serveurs CRL utilisent HTTP sur le port 80 au lieu de HTTPS sur le port 443. Les composants du Cloud Connector, eux-mêmes, ne communiquent pas via le port externe 80. La nécessité du port externe 80 est un sous-produit du processus de vérification des certificats effectué par le système d'exploitation.

Les certificats X.509 sont vérifiés lors de l'installation du Cloud Connector. Par conséquent, toutes les machines Cloud Connector doivent être configurées pour faire confiance à ces certificats. Assurez-vous que le logiciel Cloud Connector peut être installé avec succès.

Les points de terminaison Citrix Cloud sont protégés par des certificats émis par DigiCert ou par l'une des autorités de certification racine utilisées par Azure. Pour plus d'informations sur les autorités de certification racine utilisées par Azure, consultez https://docs.microsoft.com/fr-fr/azure/security/fundamentals/tls-certificate-changes.

Pour valider les certificats, chaque machine Cloud Connector doit satisfaire aux exigences suivantes :

- Le port HTTP 80 est ouvert aux adresses suivantes. Ce port est utilisé lors de l’installation du Cloud Connector et lors des vérifications CRL périodiques. Pour plus d’informations sur la

façon de tester la connectivité CRL et OCSP, consultez https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm sur le site Web de DigiCert.

  - `http://cacerts.digicert.com/`
  - `http://dl.cacerts.digicert.com/`
  - `http://crl3.digicert.com`
  - `http://crl4.digicert.com`
  - `http://ocsp.digicert.com`
  - `http://www.d-trust.net`
  - `http://root-c3-ca2-2009.ocsp.d-trust.net`
  - `http://crl.microsoft.com`
  - `http://oneocsp.microsoft.com`
  - `http://ocsp.msocsp.com`

- La communication avec les adresses suivantes est activée :
  - `https://*.digicert.com`
- Les certificats racine suivants sont installés :
  - `https://cacerts.digicert.com/DigiCertGlobalRootG3.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootCA.crt`
  - `https://cacerts.digicert.com/DigiCertTrustedRootG4.crt`
  - `https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt`
  - `https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt`
  - `https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt`
  - `https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt`
  - `https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt`
- Les certificats intermédiaires suivants sont installés :

- `https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crt`

Si un certificat est manquant, l'installateur du Cloud Connector le télécharge depuis `http://cacerts.digicert.com`.

Pour des instructions complètes sur le téléchargement et l'installation des certificats, consultez CTX223828.

Exigences d'Active Directory

- Joint à un domaine Active Directory qui contient les ressources et les utilisateurs que vous utilisez pour créer des offres pour vos utilisateurs. Pour les environnements multi-domaines, consultez Scénarios de déploiement pour les Cloud Connectors dans Active Directory dans cet article.
- Chaque forêt Active Directory que vous prévoyez d'utiliser avec Citrix Cloud Government doit toujours être accessible par deux Cloud Connectors.
- Le Cloud Connector doit pouvoir atteindre les contrôleurs de domaine parents (racine) et les contrôleurs de domaine enfants dans l'infrastructure Active Directory, afin de compléter les workflows Active Directory dans lesquels le Cloud Connector est installé. Pour plus d'informations, consultez les articles de support Microsoft suivants :
  - Comment configurer les domaines et les approbations
  - Ports des services système

Exigences réseau

- Connecté à un réseau qui peut contacter les ressources que vous utilisez dans votre emplacement de ressources. Pour plus d'informations, consultez Configuration du proxy et du pare-feu du Cloud Connector.
- Connecté à Internet. Pour plus d'informations, consultez Exigences de connectivité Internet.

Niveaux fonctionnels Active Directory pris en charge

Le Citrix Cloud Connector prend en charge les niveaux fonctionnels de forêt et de domaine suivants dans Active Directory.

NIVEAU FONCTIONNEL DE LA FORÊT	NIVEAU FONCTIONNEL DU DOMAINE	CONTRÔLEURS DE DOMAINE PRIS EN CHARGE
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019, Windows Server 2022

Prise en charge de la norme FIPS (Federal Information Processing Standard)

Le Cloud Connector prend actuellement en charge les algorithmes cryptographiques validés FIPS qui sont utilisés sur les machines compatibles FIPS. Seule la dernière version du logiciel Cloud Connector disponible dans Citrix Cloud Government inclut cette prise en charge. Si vous disposez

de machines Cloud Connector existantes dans votre environnement (installées avant novembre 2018) et que vous souhaitez activer le mode FIPS sur ces machines, procédez comme suit :

1. Désinstallez le logiciel Cloud Connector sur chaque machine de votre emplacement de ressources.
2. Activer le mode FIPS sur chaque machine.
3. Installer la dernière version du Cloud Connector sur chaque machine compatible FIPS.

Important :

- N'essayez pas de mettre à niveau les installations existantes du Cloud Connector vers la dernière version. Désinstallez toujours l'ancien Cloud Connector en premier, puis installez le nouveau.
- N'activez pas le mode FIPS sur une machine hébergeant une version plus ancienne du Cloud Connector. Les Cloud Connectors antérieurs à la version 5.102 ne prennent pas en charge le mode FIPS. L'activation du mode FIPS sur une machine sur laquelle un Cloud Connector plus ancien est installé empêche Citrix Cloud Government d'effectuer les mises à jour de maintenance régulières pour le Cloud Connector.

Pour obtenir des instructions sur le téléchargement de la dernière version du Cloud Connector, consultez Tâche 3 : Installer les Cloud Connectors.

Scénarios de déploiement des Cloud Connectors dans Active Directory

Si vous avez un seul domaine dans une seule forêt, l'installation des Cloud Connectors dans ce domaine est tout ce dont vous avez besoin pour établir un emplacement de ressources. Cependant, si vous avez plusieurs domaines dans votre environnement, vous devez déterminer où installer les Cloud Connectors. Pour que les utilisateurs puissent accéder aux ressources que vous mettez à disposition via Citrix Cloud Government.

Remarque :

Les emplacements de ressources mentionnés constituent un modèle qui doit être répété dans d'autres emplacements physiques, en fonction de l'endroit où vos ressources sont hébergées.

Domaine unique dans une seule forêt avec un seul ensemble de Cloud Connectors

Dans ce scénario, un seul domaine contient tous les objets de ressources et d'utilisateurs (forest1.local). Un ensemble de Cloud Connectors est déployé au sein d'un seul emplacement de ressources et joint au domaine forest1.local.

- Relation d'approbation : Aucune - domaine unique
- Domaines répertoriés dans **Identity and Access Management** : forest1.local
- Ouvertures de session utilisateur sur Citrix Workspace™ : Pris en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront™ sur site : Pris en charge pour tous les utilisateurs

Domaines parent et enfant dans une seule forêt avec un seul ensemble de Cloud Connectors

Dans ce scénario, un domaine parent (forest1.local) et son domaine enfant (user.forest1.local) résident au sein d'une seule forêt. Le domaine parent agit comme domaine de ressources et le domaine enfant est le domaine utilisateur. Un ensemble de Cloud Connectors est déployé dans un seul emplacement de ressources et joint au domaine forest1.local.

- Relation d'approbation : Approbation de domaine parent/enfant
- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local, user.forest1.local
- Connexions utilisateur à Citrix Workspace : Pris en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront sur site : Pris en charge pour tous les utilisateurs

> **Remarque :**
>
> Vous devrez peut-être redémarrer les Cloud Connectors pour vous assurer que Citrix Cloud Government enregistre le domaine enfant.

Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un seul ensemble de Cloud Connectors

Dans ce scénario, une forêt (forest1.local) contient votre domaine de ressources et une forêt (forest2.local) contient votre domaine utilisateur. Une approbation existe entre ces forêts, ce qui

permet aux utilisateurs de se connecter aux ressources. Un ensemble de Cloud Connectors est déployé dans un seul emplacement de ressources et joint au domaine forest1.local.

- Relation d'approbation : Approbation de forêt
- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local
- Connexions utilisateur à Citrix Workspace : Pris en charge uniquement pour les utilisateurs de forest1.local
- Connexions utilisateur à un StoreFront sur site : Pris en charge pour tous les utilisateurs

> **Remarque :**

> La relation d'approbation entre les deux forêts doit permettre à l'utilisateur de la forêt d'utilisateurs de se connecter aux machines de la forêt de ressources.

> Étant donné que les Cloud Connectors ne peuvent pas traverser les approbations au niveau de la forêt, le domaine forest2.local n'est pas affiché sur la page **Gestion des identités et des accès** dans la console Citrix Cloud Government. La console présente les limitations suivantes :

- Les ressources sont publiées uniquement pour les utilisateurs et les groupes disponibles dans forest1.local dans Citrix Cloud Government. Cependant, les utilisateurs de forest2.local sont imbriqués dans des groupes de sécurité forest1.local pour atténuer ce problème.
- Citrix Workspace ne peut pas authentifier les utilisateurs du domaine forest2.local.

Pour contourner ces limitations, déployez les Cloud Connectors comme décrit dans Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un ensemble de Cloud Connectors dans chaque forêt.

Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un ensemble de Cloud Connectors dans chaque forêt

Dans ce scénario, une forêt (forest1.local) contient votre domaine de ressources et une forêt (forest2.local) contient votre domaine d'utilisateurs. Une approbation existe entre ces forêts qui permet aux utilisateurs de se connecter aux ressources. Un ensemble de Cloud Connectors est déployé dans le domaine forest1.local et un second ensemble est déployé dans le domaine forest2.local.

- Relation d'approbation : Approbation de forêt

- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local, forest2.local
- Connexions utilisateur à Citrix Workspace : Prise en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront sur site : Prise en charge pour tous les utilisateurs

Exigences d'installation

- Téléchargez le logiciel Cloud Connector uniquement depuis Citrix Cloud Government et installez-le sur des machines préparées. Par défaut, le programme d'installation de Cloud Connector tente de se connecter au plan de contrôle à partir duquel il a été téléchargé. Ainsi, si vous tentez d'installer le logiciel téléchargé depuis un compte Citrix Cloud commercial, le programme d'installation ne se connectera pas à Citrix Cloud Government.
- Étant donné que le logiciel Cloud Connector est téléchargé, votre navigateur doit autoriser le téléchargement de fichiers exécutables.

Considérations importantes relatives à l'utilisation

- Maintenez tous les Cloud Connectors sous tension en permanence pour garantir une connexion continue à Citrix Cloud Government.
- Ne mettez pas à niveau un Cloud Connector précédemment installé avec une version plus récente. Désinstallez plutôt l'ancien Cloud Connector, puis installez le nouveau.
- Citrix recommande fortement d'activer Windows Update sur toutes les machines hébergeant le Cloud Connector.
- Citrix recommande fortement d'installer au moins deux (2) Cloud Connectors dans chaque emplacement de ressources. En général, le nombre de Cloud Connectors à installer est N+1, où N est la capacité nécessaire pour prendre en charge l'infrastructure au sein de votre emplacement de ressources. Les deux connecteurs installés garantissent que la connexion entre Citrix Cloud Government et votre emplacement de ressources reste intacte au cas où un Cloud Connector deviendrait indisponible.
- Chaque forêt Active Directory que vous prévoyez d'utiliser avec Citrix Cloud Government doit être accessible en permanence par deux Cloud Connectors.
- Après l'installation, ne déplacez pas la machine hébergeant le Cloud Connector vers un autre domaine. Si la machine doit être jointe à un autre domaine, désinstallez le Cloud Connector. Réinstallez-le une fois que la machine est jointe à l'autre domaine.

Afficher l'état du Cloud Connector

La page Emplacements des ressources dans Citrix Cloud Government affiche l'état de santé de tous les Cloud Connectors de vos emplacements de ressources.

Dépanner le Cloud Connector

La première étape pour diagnostiquer tout problème avec le Cloud Connector consiste à vérifier les messages d'événement et les journaux d'événements. Si le Cloud Connector n'apparaît pas dans votre emplacement de ressources ou s'il n'est « pas en contact », les journaux d'événements fournissent des informations initiales.

Il semble y avoir un problème de connectivité entre Citrix Government et le Cloud Connector, car le statut est « déconnecté ». Bien que les journaux d'événements n'indiquent aucun problème de connectivité entre le Cloud Connector et Citrix Government, contactez le support pour obtenir de l'aide Contacter le support Citrix.

Si le Cloud Connector est en état d'« erreur », il peut y avoir un problème d'hébergement du Cloud Connector. Installez le Cloud Connector sur une nouvelle machine. Si le problème persiste, contactez le support Citrix.

Pour résoudre les problèmes courants liés à l'installation ou à l'utilisation du Cloud Connector, reportez-vous à CTX221535.

Messages d'événement

Le Cloud Connector génère certains messages d'événement que vous pouvez consulter dans l'**Observateur d'événements** Windows. Si vous souhaitez que votre logiciel de surveillance préféré recherche ces messages, vous pouvez les télécharger sous forme d'archive ZIP. L'archive ZIP inclut ces messages dans les fichiers XML suivants :

- Citrix.CloudServices.Agent.Core.dll.xml (Fournisseur d'agent de connecteur)
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (Fournisseur AgentWatchDog de connecteur)

Télécharger messages d'événement du Cloud Connector. (fichier ZIP)

Journaux d'événements

Par défaut, les journaux d'événements sont disponibles dans le répertoire C:\\ProgramData\\Citrix\\WorkspaceCloud\\Logs de la machine hébergeant le Cloud Connector.

Installer et configurer

Créer un emplacement de ressources

Après vous être inscrit à Citrix Cloud™ Government, continuez la configuration de votre compte en créant un emplacement de ressources.

Qu'est-ce qu'un emplacement de ressources ?

Un emplacement de ressources contient les ressources de calcul et de réseau nécessaires pour fournir des services à vos utilisateurs. Les ressources que contient votre emplacement de ressources dépendent des services que vous souhaitez fournir. Par exemple, si vous prévoyez de fournir des applications et des bureaux via Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops™), votre emplacement de ressources peut inclure les composants suivants :

- Un domaine Active Directory pour authentifier et autoriser les utilisateurs qui souhaitent accéder aux applications et aux bureaux.
- Un ou plusieurs Virtual Delivery Agents (VDA) pour gérer la connexion entre les machines qui hébergent les applications et les bureaux. Vous pourriez vouloir fournir les appareils utilisés pour accéder à ces ressources.
- Un hyperviseur ou un service cloud pris en charge, tel que Citrix XenServer® ou Microsoft Azure, pour provisionner les machines virtuelles qui fournissent les applications et les bureaux.
- Un Citrix Gateway pour permettre aux utilisateurs externes d'accéder aux applications et aux bureaux en toute sécurité.

Emplacements de ressources par défaut

Si vous n'avez aucun emplacement de ressources dans votre compte Citrix Cloud Government et que vous installez des Cloud Connectors dans votre domaine. L'emplacement de ressources créé par Citrix Cloud Government devient l'emplacement de ressources par défaut. Vous ne pouvez avoir qu'un seul emplacement de ressources par défaut dans votre compte. Si nécessaire, vous pouvez créer d'autres emplacements de ressources dans Citrix Cloud Government. Sélectionnez l'emplacement de ressources souhaité lorsque vous installez des Cloud Connectors dans d'autres domaines.

Vous pouvez également créer d'abord les emplacements de ressources dont vous avez besoin dans la console, avant d'installer les Cloud Connectors dans vos domaines. L'installateur du Cloud Connector vous invite à sélectionner l'emplacement de ressources souhaité pendant l'installation.

Tâche 1 : Préparer les machines

1. Consultez les exigences de Citrix Cloud Connector pour des considérations importantes, les niveaux fonctionnels Active Directory pris en charge et les informations de dépannage.
2. Préparez les machines qui répondent aux exigences de configuration.
3. Joignez les machines préparées à votre domaine.

Tâche 2 : Vérifier la connectivité

La connexion à Internet depuis vos centres de données nécessite l'ouverture du port 443 pour les connexions sortantes. Cependant, pour fonctionner dans des environnements contenant un serveur proxy Internet ou des restrictions de pare-feu, une configuration supplémentaire pourrait être nécessaire.

1. Consultez les Exigences de connectivité pour obtenir une liste des adresses contactables pour les services disponibles.
2. Assurez-vous que le port 443 (HTTPS) est ouvert pour les connexions sortantes.
3. Assurez-vous que les adresses requises peuvent être contactées afin de pouvoir exploiter et consommer les services Citrix Cloud Government.
4. Consultez la Configuration du proxy et du pare-feu du Citrix Cloud Connector pour obtenir des informations sur l'utilisation du Cloud Connector avec un proxy web.

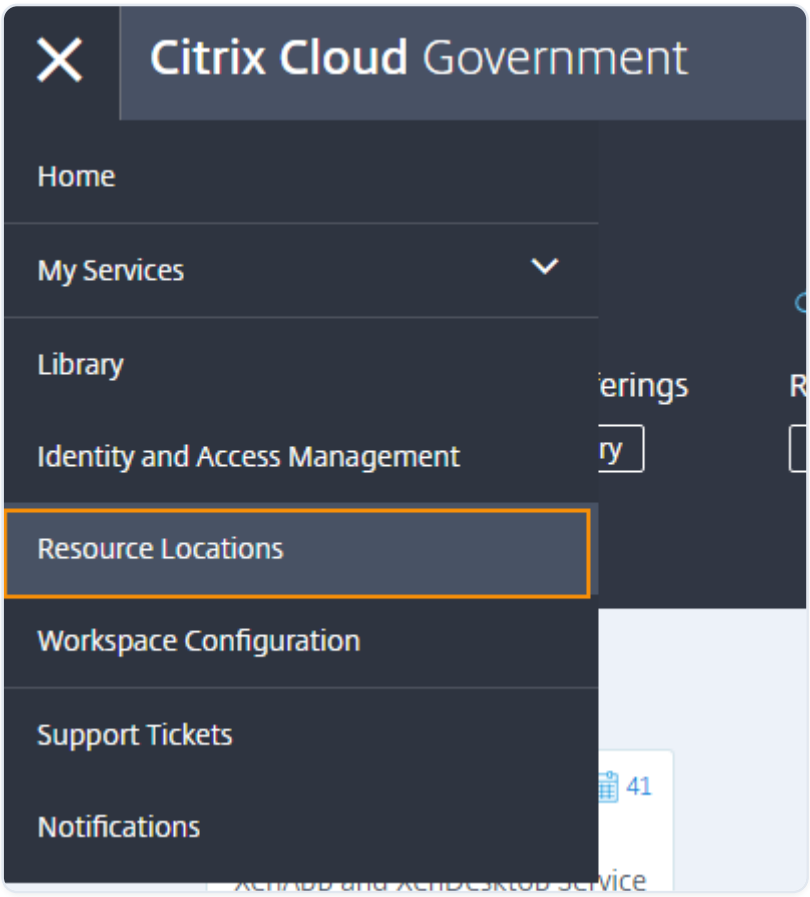
Tâche 3 : Installer les Cloud Connectors

> **Remarque :**

> L'appliance Connector n'est pas disponible pour Citrix Cloud Government.

> Pendant l'installation, le Cloud Connector nécessite un accès au cloud pour authentifier l'utilisateur afin d'effectuer l'installation. Il valide les autorisations de l'installateur, télécharge et configure les services fournis par le Cloud Connector. L'installation s'effectue avec les privilèges de l'utilisateur qui l'initie.

1. Dans le menu Citrix Cloud Government, sélectionnez **Emplacements des ressources**.



2. Cliquez sur **Télécharger** pour télécharger le programme d'installation du Cloud Connector.
3. Double-cliquez sur le programme d'installation. Citrix Cloud Government effectue une vérification initiale de la connectivité et vous invite à saisir votre nom d'utilisateur et votre mot de passe d'administrateur Citrix Cloud Government.
4. Suivez l'assistant pour installer et configurer le Cloud Connector. Une fois l'installation terminée, Citrix Cloud Government effectue une dernière vérification de la connectivité pour s'assurer que le Cloud Connector peut communiquer avec Citrix Cloud Government.

Après l'installation, Citrix Cloud enregistre votre domaine dans **Gestion des identités et des accès**.

> **Remarques :**

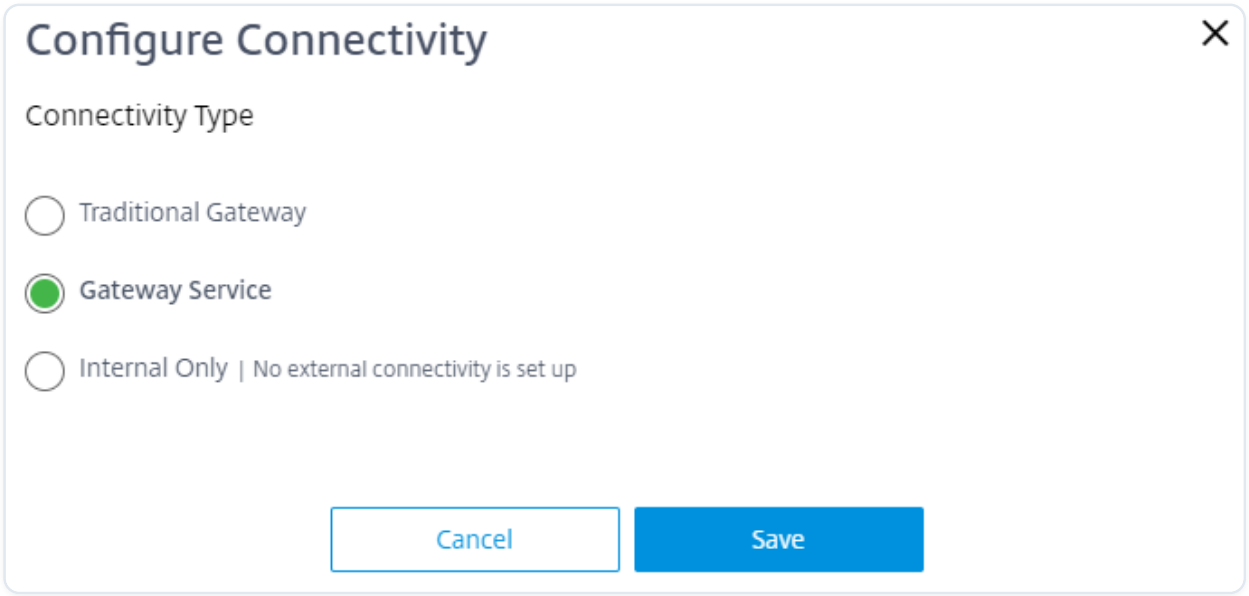
- Si vous êtes administrateur de plusieurs comptes d'organisation, Citrix Cloud Government vous invite à sélectionner le compte que vous souhaitez associer au Cloud Connector.

- L'utilisation du même programme d'installation du Cloud Connector pour des installations répétées sur une période donnée n'est pas recommandée.
- Téléchargez un nouveau Cloud Connector à partir de la page Emplacements des ressources dans la console Citrix Cloud Government.

Configurer la connectivité pour les utilisateurs

Fournissez un accès interne ou externe aux services que vous mettez à disposition dans l'emplacement des ressources. L'accès sécurisé pour les utilisateurs externes nécessite un Citrix Gateway existant dans votre environnement.

1. Sur la page **Emplacements des ressources**, localisez l'emplacement des ressources que vous souhaitez configurer et cliquez sur **Gateway**. La boîte de dialogue Configurer la connectivité apparaît.



2. Pour configurer un accès sécurisé pour les utilisateurs externes à l'aide d'un Gateway sur site :
   a. Sélectionnez **Gateway traditionnel**.
   b. Saisissez le nom de domaine complet externe du Citrix Gateway. Exemple : mynsg.my-domain.com
3. Pour utiliser le service Citrix Gateway afin de fournir un accès sécurisé aux applications et aux bureaux pour les utilisateurs externes, sélectionnez **Service Gateway**.
4. Pour configurer un accès interne uniquement, sélectionnez **Interne uniquement**.
5. Cliquez sur **Enregistrer**.

Créer d'autres emplacements de ressources

1. Depuis la console de gestion Citrix Cloud Government, cliquez sur le bouton de menu et sélectionnez **Emplacements des ressources**.
2. Cliquez sur **Emplacement des ressources** et saisissez un nom convivial.
3. Cliquez sur **Enregistrer**. Citrix Cloud Government affiche une vignette pour le nouvel emplacement des ressources.
4. Cliquez sur **Connecteurs Cloud**, puis cliquez sur **Télécharger** pour acquérir le logiciel Connecteur Cloud.
5. Sur chaque machine préparée, installez le logiciel Connecteur Cloud à l'aide de l'assistant d'installation ou de l'(/fr-fr/citrix-cloud-government/install-configure/connector-install-command.html)installation en ligne de commande. Citrix Cloud Government vous invite à sélectionner l'emplacement des ressources que vous souhaitez associer au Connecteur Cloud.

Journaux d'installation du Connecteur Cloud

Les journaux d'installation du Connecteur Cloud se trouvent à l'emplacement **%LOCALAPPDATA%\\Temp\\CitrixLogs\\CloudServicesSetup**.

De plus, les journaux sont ajoutés à **%ProgramData%\\Citrix\\WorkspaceCloud\\InstallLogs** après l'installation.

Installer les Cloud Connectors à partir de la ligne de commande

Vous pouvez installer le logiciel Citrix Cloud Connector™ de manière interactive ou en utilisant une installation silencieuse ou automatisée.

Pendant l'installation, le Cloud Connector nécessite un accès au cloud pour authentifier l'installation de l'utilisateur. Validez les autorisations de l'installateur, téléchargez et configurez les services fournis par le Cloud Connector. L'installation s'effectue avec les privilèges de l'utilisateur qui lance l'installation.

> **Important :**

> Il n'est pas recommandé d'utiliser le même programme d'installation pour des installations répétées sur une période donnée. Téléchargez un nouveau Cloud Connector depuis la page Emplacements des ressources dans la console Citrix Cloud™ Government.

Prérequis

Pour utiliser l'installation en ligne de commande avec Citrix Cloud Government, vous devez fournir les informations suivantes :

- L'ID client du compte Citrix Cloud Government pour lequel vous installez le Cloud Connector. Cet ID apparaît en haut de l'onglet **Accès API** dans **Gestion des identités et des accès**.
- L'ID client et le secret du client API sécurisé que vous souhaitez utiliser pour installer le Cloud Connector. Pour obtenir ces valeurs, vous devez d'abord créer un principal de service.
    - L'ID client et le secret garantissent que votre accès à l'API Citrix Cloud est sécurisé de manière appropriée. Lorsque vous créez un principal de service, le client fonctionne avec les mêmes autorisations d'administrateur que vous.
- Pour installer un Cloud Connector, vous devez utiliser un principal de service avec un administrateur à accès complet disposant également d'une autorisation d'accès complet.
- L'ID d'emplacement des ressources pour l'emplacement des ressources que vous souhaitez associer au Cloud Connector. Pour récupérer cette valeur, sélectionnez le bouton **ID** situé sous le nom de l'emplacement des ressources sur la page **Emplacements des ressources**. Si vous ne fournissez pas cette valeur, Citrix Cloud Government utilise l'ID de l'emplacement des ressources par défaut.

Créer un principal de service

Lors de la création d'un principal de service, Citrix Cloud Government génère un ID client et un secret uniques. Vous devez fournir ces valeurs lors des appels d'API via la ligne de commande.

1. Dans le menu Citrix Cloud Government, sélectionnez **Gestion des identités et des accès**, puis **Accès API**.
2. Dans l'onglet **principaux de service**, saisissez un nom pour votre client et sélectionnez **Créer un client**. Citrix Cloud Government génère et affiche un ID client et un secret pour le principal de service.
3. Sélectionnez **Télécharger** pour télécharger l'ID client et le secret sous forme de fichier CSV et stockez-le dans un emplacement sécurisé. Vous pouvez également sélectionner **Copier** pour acquérir manuellement chaque valeur. Une fois terminé, sélectionnez **Fermer** pour revenir à la console.

Paramètres pris en charge

Assurez la sécurité des détails du principal de service, un fichier de configuration JSON doit être fourni à l'installateur. Ce fichier doit être supprimé une fois l'installation terminée. Les valeurs prises en charge pour le fichier de configuration sont :

- **customerName** Obligatoire. L'ID client affiché sur la page Accès API dans la console Citrix Cloud Government.
- **clientId** Obligatoire. L'ID du principal de service qu'un administrateur peut créer, disponible sur la page Accès API.
- **clientSecret** Obligatoire. Le secret du principal de service qui peut être téléchargé après la création du principal de service. Disponible sur la page Accès API.
- **resourceLocationId** Recommandé. L'identifiant unique d'un emplacement de ressources existant. Sélectionnez le bouton ID pour récupérer l'ID de l'emplacement de ressources sur la page Emplacements de ressources dans la console Citrix Cloud. Si aucune valeur n'est spécifiée, Citrix Cloud utilise l'ID du premier emplacement de ressources du compte.
- **acceptTermsOfService** Obligatoire. Doit être défini sur **true**.

Exemple de fichier de configuration :

```
{

"customerName": "CustomerID",

"clientId": "ClientID",

"clientSecret": "ClientSecret",

"resourceLocationId": "ResourceLocationId",

"acceptTermsOfService": "true",

}
```

Exemple de ligne de commande qui installe à l'aide du fichier de paramètres :

```
CWCConnector.exe /q /ParametersFilePath:c:
\cwcconnector_install_params.json
```

Utilisez **Start /Wait CWCConnector.exe /ParametersFilePath:value** pour examiner un code d'erreur potentiel en cas d'échec. Vous pouvez utiliser le mécanisme standard d'exécution de **echo %ErrorLevel%** une fois l'installation terminée.

Dépannage

Journaux d'installation

Les journaux d'installation sont disponibles à l'adresse **%LOCALAPPDATA%\\Temp\\CitrixLogs\\CloudServicesSetup**.

De plus, les journaux sont ajoutés à **%ProgramData%\\Citrix\\WorkspaceCloud\\InstallLogs** après l'installation.

Codes de sortie

- 1603 - Une erreur inattendue s'est produite.
- 2 - Une vérification des prérequis a échoué.
- 0 - L'installation s'est terminée avec succès.

Considérations relatives aux machines clonées

Chaque machine hébergeant le Cloud Connector doit avoir un SID et un ID de connecteur uniques afin que Citrix Cloud Government puisse communiquer de manière fiable avec les machines de votre emplacement de ressources. L'installation du Cloud Connector sur un modèle de machine (avant le clonage) n'est pas prise en charge. Si vous clonez une machine avec le Cloud Connector installé, les services Cloud Connector ne s'exécutent pas et la machine ne peut pas se connecter à Citrix Cloud Government.

Si vous avez l'intention d'héberger le Cloud Connector sur plusieurs machines dans votre emplacement de ressources et que vous souhaitez utiliser des machines clonées, suivez les étapes suivantes :

1. Préparez le modèle de machine conformément aux exigences de votre environnement.
2. Provisionnez le nombre de machines que vous avez l'intention d'utiliser comme Cloud Connectors.
3. Installez le Cloud Connector sur chaque machine, soit manuellement, soit en utilisant le mode d'installation silencieuse.

Configuration du proxy et du pare-feu de Citrix Cloud Connector™

Port 443 utilisant le trafic HTTP, sortie uniquement. Pour plus de détails sur la connectivité, consultez Exigences de connectivité.

Configuration du Cloud Connector pour prendre en charge un proxy web

Le Cloud Connector prend en charge la connexion à Internet via un serveur proxy web. L'installateur et les services qu'il installe nécessitent des connexions à Citrix Cloud™ Government. L'accès à Internet doit être disponible à ces deux points.

> **Important :**
>
> L'activation du déchiffrement SSL sur certains proxys peut empêcher le Cloud Connector de se connecter correctement à Citrix Cloud Government. Pour plus d'informations sur la résolution de ce problème, consultez CTX221535.

Installateur

L'installateur utilise les paramètres configurés pour les connexions Internet. Si vous pouvez naviguer sur Internet depuis la machine, l'installateur fonctionne également.

Consultez Modification des paramètres du serveur proxy dans Internet Explorer pour plus de détails sur la configuration des paramètres du proxy.

Services en cours d'exécution

Le service d'exécution fonctionne dans le contexte d'un service local. Il n'utilise pas les paramètres définis pour l'utilisateur comme décrit précédemment. Vous devez importer le paramètre depuis le navigateur.

Pour configurer les paramètres du proxy pour le service d'exécution, ouvrez une fenêtre d'invite de commandes et utilisez **netsh** comme suit :

```
netsh winhttp import proxy source =ie
```

Après avoir exécuté la commande, redémarrez la machine hébergeant le Cloud Connector afin que les services démarrent avec ces paramètres de proxy.

Pour plus de détails, consultez Commandes Netsh pour le protocole de transfert hypertexte Windows (WinHTTP).

> **Remarque :**
>
> La détection automatique ou les scripts PAC ne sont pas pris en charge.

Configurer DaaS

Cet article fournit un aperçu des tâches requises pour configurer Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops). Pour une liste des fonctionnalités de service qui ne sont pas disponibles dans Citrix Cloud Government, consultez Citrix DaaS pour Citrix Cloud Government.

Demander un essai de service

Si vous n'avez pas d'abonnement à Citrix DaaS, vous pouvez demander un essai. Les essais de service durent 60 jours et offrent les mêmes fonctionnalités que le service de production. Pour demander un essai, suivez les étapes décrites dans Demander un essai de service.

Préparer une image principale et installer le VDA

Préparez une ou plusieurs machines virtuelles avec la configuration de bureau ou les applications que vous souhaitez fournir aux utilisateurs. Ensuite, installez le logiciel Virtual Delivery Agent (VDA) sur chaque machine. Joignez chaque machine à votre domaine avant d'installer le VDA.

Pour obtenir des instructions, consultez Installer les VDA

Configurer Citrix DaaS™

Pour configurer Citrix DaaS, effectuez les tâches suivantes :

- Créer une connexion d'hôte. Une connexion d'hôte permet à Citrix DaaS de provisionner et de gérer les machines dans votre hyperviseur ou environnement cloud.
- Créer des catalogues de machines. Les catalogues de machines sont des collections de machines configurées de manière identique qui sont créées à partir des VDA que vous avez préparés précédemment.
- Les utilisateurs accèdent aux applications ou aux bureaux sur ces machines via leurs espaces de travail.

- Créer des groupes de mise à disposition. Les groupes de mise à disposition vous permettent de définir quels utilisateurs ou groupes d'utilisateurs peuvent accéder à certaines applications ou certains bureaux.
    - Lorsque les utilisateurs accèdent à leur espace de travail, les groupes de mise à disposition régissent les applications ou les bureaux auxquels ces utilisateurs appartiennent.

Service Citrix Gateway

Le service Citrix Gateway est disponible pour Citrix DaaS. Le service Citrix Gateway est hébergé uniquement sur les clouds Citrix Cloud™ Government et est distinct des clouds commerciaux. Le service Citrix Gateway sur les clouds gouvernementaux est actuellement disponible aux États-Unis dans les trois régions suivantes.

- Arizona
- Texas
- Virginie

Configurer le service Citrix Gateway

La configuration du service Citrix Gateway pour Cloud Government est similaire à la configuration du service Citrix Gateway pour les clouds commerciaux. Vous devez activer le service Citrix Gateway pour configurer la connectivité pour les utilisateurs. Pour plus de détails, consultez Configurer la connectivité pour les utilisateurs.

Citrix Gateway

Citrix Gateway offre aux utilisateurs un accès sécurisé aux applications Citrix DaaS sur une gamme d'appareils. Si vous disposez d'une passerelle sur site existante, vous pouvez l'utiliser avec Citrix DaaS pour garantir que les utilisateurs externes peuvent accéder à leurs applications en toute sécurité. De plus, si vous devez créer un déploiement de passerelle à utiliser avec Citrix DaaS, reportez-vous à Déployer une instance Citrix ADC VPX.

Autres fonctionnalités

Pour en savoir plus sur l'utilisation des autres fonctionnalités de Citrix DaaS, consultez les articles suivants :

- Impression
- Technologies HDX
- Stratégies

- Gestion des ressources et des utilisateurs
- Surveillance

Étapes suivantes

Après avoir configuré Citrix DaaS, configurez les espaces de travail pour vos utilisateurs. Grâce aux espaces de travail, vos utilisateurs peuvent accéder aux applications et aux bureaux que vous mettez à leur disposition.

Configurer les espaces de travail pour les utilisateurs

L'espace de travail vous permet de fournir l'accès aux applications et aux bureaux depuis n'importe quel appareil. Les espaces de travail donnent accès aux ressources en fonction des groupes de mise à disposition que vous configurez dans Citrix DaaS (anciennement le service Citrix Virtual Apps and Desktops™).

Avant de configurer les espaces de travail pour vos utilisateurs, examinez les fonctionnalités qui ne sont pas disponibles dans Citrix Cloud Government. Consultez Service Workspace pour Citrix Cloud Government.

Lorsque vous êtes prêt à configurer les espaces de travail, consultez Configuration de l'espace de travail.

Mise en réseau Citrix

Pour fournir aux utilisateurs externes un accès sécurisé aux applications et aux bureaux, une appliance Citrix ADC, VPX ou MPX sur site est requise. L'utilisation de cartes à puce avec Citrix Gateway est un scénario d'accès courant pour les clients de Citrix Cloud™ Government.

Cet article décrit les recommandations de Citrix pour l'utilisation des cartes à puce avec Citrix Gateway.

1. Créez un serveur virtuel Gateway principal pour l'authentification des utilisateurs. Sélectionnez le paramètre **Authentification client** et définissez-le sur **Obligatoire**. L'option **Obligatoire** impose l'utilisation de cartes à puce en refusant toute négociation SSL qui n'inclut pas de certificat client.
2. Créez un serveur virtuel Gateway secondaire qui gère uniquement le proxy ICA®.

Cette passerelle n'est pas configurée pour demander l'authentification client. Ainsi, la connexion SSL ICA ne demande pas à nouveau un code PIN à l'utilisateur. Dans StoreFront™, utilisez ce serveur virtuel pour acheminer les connexions vers les ressources. Le serveur virtuel permet aux utilisateurs de se connecter à la passerelle principale, qui gère l'authentification initiale, et d'accéder aux ressources via la passerelle secondaire.

3. Créez un troisième serveur virtuel Gateway pour fournir l'URL de rappel pour StoreFront. Seul StoreFront utilise cette passerelle pour vérifier les requêtes provenant de l'appliance Gateway et n'a pas besoin d'être accessible publiquement. Ce serveur virtuel est requis lorsque l'authentification par certificat client est obligatoire. StoreFront ne peut pas présenter de certificat pour s'authentifier.

Informations supplémentaires

Pour plus d'informations sur la création de serveurs virtuels Citrix Gateway, consultez Création de serveurs virtuels.

Pour plus d'informations sur la configuration de l'authentification par carte à puce dans StoreFront, consultez Configurer l'authentification par carte à puce.

Service d'activation de licence

Le Service d'activation de licence (LAS) est une solution de gestion des licences moderne et basée sur le cloud pour les serveurs de licences Citrix sur site. Conçu comme une alternative simplifiée aux licences Citrix héritées traditionnelles, le LAS introduit de nouveaux modules pour l'activation des produits, garantissant une approche transparente de la gestion des licences.

Au lieu de gérer manuellement les cycles de vie des fichiers de licence, vous pouvez connecter votre serveur de licences à Citrix Cloud™ pour une activation en ligne. Une fois enregistré, le serveur de licences communique régulièrement avec le point de terminaison LAS pour s'assurer que les activations restent à jour et alignées avec la date d'expiration de votre droit ou la date de fin de votre contrat.

Pour plus d'informations, consultez Service d'activation de licence.

Identité

Gestion des identités et des accès pour Citrix Cloud™ Government

La gestion des identités et des accès inclut les fournisseurs d'identité et les comptes utilisés pour les administrateurs de Citrix Cloud Government et les abonnés à l'espace de travail.

Fournisseurs d'identité

Le fournisseur d'identité Citrix Cloud Government est le fournisseur d'identité par défaut. Les informations d'identité sont gérées pour tous les administrateurs dans le compte Citrix Cloud Government. Vous pouvez changer de fournisseur pour utiliser un autre fournisseur d'identité afin d'authentifier les administrateurs, les abonnés à l'espace de travail, ou les deux.

Citrix Cloud Government prend en charge les fournisseurs d'identité suivants :

- Microsoft Entra ID : Pour l'authentification des administrateurs Citrix Cloud Government et des abonnés à l'espace de travail.
- Active Directory : Pour l'authentification des abonnés à l'espace de travail.
- Citrix Gateway : Pour l'authentification des abonnés à l'espace de travail.
- Okta : Pour l'authentification des abonnés à l'espace de travail.
- SAML 2.0 : Pour l'authentification des administrateurs (préversion) et des abonnés à l'espace de travail.

Administrateurs

Les administrateurs utilisent leur identité pour accéder à Citrix Cloud Government, effectuer des activités de gestion et installer le Citrix Cloud Connector.

Le fournisseur d'identité Citrix Cloud Government authentifie les administrateurs à l'aide d'une adresse e-mail et d'un mot de passe. Les administrateurs peuvent également utiliser leurs informations d'identification My Citrix pour se connecter à Citrix Cloud Government.

Abonnés

L'identité d'un abonné définit les services auxquels il a accès dans Citrix Cloud Government. Cette identité provient des comptes de domaine Active Directory fournis par les domaines au sein de l'emplacement des ressources. L'attribution d'un abonné à une offre de bibliothèque l'autorise à accéder à cette offre.

Les administrateurs peuvent contrôler les domaines utilisés pour fournir ces identités dans l'onglet **Domaines**. Si vous prévoyez d'utiliser des domaines provenant de plusieurs forêts, installez au moins deux Cloud Connectors dans chaque forêt. Citrix® recommande au moins deux Cloud Connectors pour maintenir un environnement à haute disponibilité.

> **Remarque :**
>
> - La désactivation des domaines empêche uniquement la sélection de nouvelles identités. Elle n'empêche pas les abonnés d'utiliser les identités déjà attribuées.
> - Chaque Cloud Connector répertorie et utilise tous les domaines de la forêt unique dans laquelle il est installé.

> Pour plus d'informations, consultez les articles suivants dans la documentation produit Citrix Cloud :

- Attribuer des utilisateurs et des groupes à des offres de services à l'aide de la bibliothèque
- Scénarios de déploiement pour les Cloud Connectors dans Active Directory

Connecter Active Directory à Citrix Cloud™ Government

Par défaut, Citrix Cloud Government utilise le fournisseur d'identité Citrix Cloud Government pour gérer les informations d'identité de tous les utilisateurs de votre compte Citrix Cloud. Vous pouvez changer le fournisseur d'identité pour utiliser Active Directory (AD) à la place.

La connexion de votre Active Directory sur site à Citrix Cloud Government implique l'installation de Cloud Connectors dans votre domaine. Citrix recommande d'installer deux Cloud Connectors pour une haute disponibilité. Pour les exigences et les instructions, consultez Exigences relatives aux Citrix Cloud Connectors.

Pour connecter votre Active Directory à Citrix Cloud

1. Dans le menu Citrix Cloud Government, sélectionnez **Gestion des identités et des accès**.
2. Dans l'onglet **Authentification** de **Active Directory**, cliquez sur le menu d'options et sélectionnez **Connecter**.
3. Cliquez sur **Installer le connecteur** pour télécharger le logiciel Cloud Connector.
4. Lancez l'installateur Cloud Connector et suivez l'assistant d'installation.
5. Depuis la page **Connecter à Active Directory**, cliquez sur **Détecter**. Après vérification, Citrix Cloud affiche un message indiquant que votre Active Directory est connecté.
6. Cliquez sur **Retour à l'authentification**. L'entrée **Active Directory** est marquée **Activé** dans l'onglet **Authentification**.

Connecter Microsoft Entra ID à Citrix Cloud™ Government

Par défaut, Citrix Cloud Government utilise le fournisseur d'identité Citrix Cloud Government pour gérer les informations d'identité de tous les utilisateurs de votre compte Citrix Cloud Government. Vous pouvez modifier le fournisseur d'identité pour utiliser Microsoft Entra ID à la place.

En utilisant Microsoft Entra ID avec Citrix Cloud Government, vous pouvez :

- Utiliser votre propre Active Directory, afin de pouvoir contrôler l'audit, les politiques de mot de passe et désactiver facilement les comptes si nécessaire.
- Configurer l'authentification multifacteur pour un niveau de sécurité plus élevé contre la possibilité de vol d'identifiants de connexion.
- Utiliser une page de connexion personnalisée, afin que vos utilisateurs sachent qu'ils se connectent au bon endroit.
- Utiliser la fédération vers un fournisseur d'identité de votre choix, y compris ADFS, Okta et Ping, entre autres.

Préparer votre Active Directory et Microsoft Entra ID

Avant de pouvoir utiliser Microsoft Entra ID, assurez-vous de respecter les exigences suivantes :

- **Votre infrastructure Microsoft Entra ID est hébergée dans une instance Azure Government.** Vous ne pouvez pas fédérer Microsoft Entra ID hébergé dans une instance Azure commerciale vers Citrix Cloud Government. Si vous tentez d'utiliser Microsoft Entra ID dans une instance Azure commerciale avec Citrix Cloud Government, Microsoft Entra ID ne

fonctionnera pas. Si vous n'avez pas de compte Azure Government, inscrivez-vous à l'adresse https://azure.microsoft.com/fr-fr/global-infrastructure/government/request/.

- **Les comptes administrateur ont leur propriété « mail » configurée dans Microsoft Entra ID.** Pour configurer, vous pouvez synchroniser les comptes de votre Active Directory local vers Microsoft Entra ID à l'aide de l'outil Microsoft Entra ID Connect de Microsoft. Alternativement, vous pouvez configurer des comptes Microsoft Entra ID non synchronisés avec un e-mail Office 365.

Synchroniser les comptes avec Microsoft Entra ID Connect

1. Assurez-vous que les comptes Active Directory ont la propriété utilisateur Email configurée :
    a. Ouvrez Utilisateurs et ordinateurs Active Directory.
    b. Dans le dossier **Utilisateurs**, localisez le compte que vous souhaitez vérifier, cliquez avec le bouton droit et sélectionnez **Propriétés**. Sous l'onglet **Général**, vérifiez que le champ **E-mail** contient une entrée valide. Citrix Cloud exige que les administrateurs ajoutés à partir de Microsoft Entra ID aient des adresses e-mail différentes de celles des administrateurs qui se connectent à l'aide d'une identité hébergée par Citrix.
2. Installez et configurez Microsoft Entra ID Connect. Pour des instructions complètes, consultez Intégrer vos annuaires locaux avec Microsoft Entra ID sur le site web de Microsoft Azure.

Connecter Citrix Cloud Government à Microsoft Entra ID

Lors de la connexion de votre compte Citrix Cloud Government à votre Microsoft Entra ID, Citrix Cloud Government a besoin d'une autorisation pour accéder à votre profil utilisateur (ou au profil de l'utilisateur connecté). Ainsi qu'aux profils de base des utilisateurs de votre Microsoft Entra ID. Citrix demande cette autorisation afin de pouvoir obtenir votre nom et votre adresse e-mail (en tant qu'administrateur). Ou les utilisateurs peuvent être ajoutés en tant qu'administrateurs ultérieurement.

1. Connectez-vous à Citrix Cloud Government à l'adresse https://citrix.cloud.us.
2. Cliquez sur le bouton de menu dans le coin supérieur gauche de la page et sélectionnez **Gestion des identités et des accès**.
3. Localisez **Microsoft Entra ID**, cliquez sur le bouton des points de suspension, puis sélectionnez **Connecter**.
4. Lorsque vous y êtes invité, saisissez un identifiant court et convivial pour les URL pour votre entreprise, puis cliquez sur **Connecter**. L'identifiant que vous choisissez doit être globalement unique au sein de Citrix Cloud Government.

5. Lorsque vous y êtes invité, connectez-vous au compte Azure auquel vous souhaitez vous connecter. Azure vous montre les autorisations dont Citrix Cloud Government a besoin pour accéder au compte et acquérir les informations requises pour la connexion.
6. Cliquez sur **Accepter** pour accepter la demande d'autorisation.

Ajouter des administrateurs à Citrix Cloud Government depuis Microsoft Entra ID

1. Depuis la console de gestion Citrix Cloud Government, sur la page **Gestion des identités et des accès**, cliquez sur l'onglet **Administrateurs**.
2. Sélectionnez **Ajouter un administrateur/groupe**.
3. Dans **Détails de l'administrateur**, sélectionnez **Microsoft Entra ID**.
4. Saisissez le nom de l'utilisateur que vous souhaitez ajouter, puis cliquez sur **Suivant**.
    - L'invitation d'utilisateurs invités de Microsoft Entra ID n'est pas prise en charge.
5. Dans **Définir l'accès**, configurez les autorisations appropriées pour l'administrateur.
6. Vérifiez les détails de l'administrateur. Sélectionnez **Retour** pour apporter des modifications.
7. Sélectionnez **Envoyer l'invitation**. Citrix Cloud Government envoie une invitation à l'utilisateur que vous avez spécifié et ajoute l'administrateur à la liste.

Après avoir cliqué sur le lien de l'e-mail, vous pouvez vous connecter à l'ID Microsoft Entra de l'entreprise. Vous pouvez vérifier l'adresse e-mail de l'utilisateur et finaliser la connexion entre le compte utilisateur Microsoft Entra ID et Citrix Cloud Government.

Ajouter des groupes d'administrateurs Microsoft Entra ID à Citrix Cloud Government

Vous pouvez ajouter des administrateurs à votre compte Citrix Cloud Government à l'aide de groupes Microsoft Entra ID (AD). Vous pouvez ensuite gérer les autorisations d'accès aux services pour tous les administrateurs du groupe.

Cette fonctionnalité est prise en charge pour les utilisateurs uniquement avec Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops™). Les administrateurs du groupe n'ont pas accès à la gestion d'autres services dans le compte Citrix Cloud Government.

Pour plus d'informations, consultez Gérer les groupes d'administrateurs.

Se connecter à Citrix Cloud à l'aide de Microsoft Entra ID

Une fois les comptes utilisateur Microsoft Entra ID connectés, les utilisateurs peuvent se connecter à Citrix Cloud Government en utilisant l'une des méthodes suivantes :

- Accédez à l'URL de connexion de l'administrateur que vous avez configurée lors de la connexion initiale du fournisseur d'identité Microsoft Entra ID pour votre entreprise. Exemple : `https://citrix.cloud.us/go/myorganization`
- Depuis la page de connexion de Citrix Cloud Government, cliquez sur **Se connecter avec les informations d'identification de mon organisation**, saisissez l'identifiant que vous avez créé lors de la connexion initiale de Microsoft Entra ID, puis cliquez sur **Continuer**.

Activer les fonctionnalités avancées de Microsoft Entra ID

Microsoft Entra ID offre une authentification multifacteur avancée et des fonctionnalités de sécurité de pointe. Fédération à 20 fournisseurs d'identité différents. Changement et réinitialisation de mot de passe en libre-service, parmi de nombreuses autres fonctionnalités. L'activation de ces fonctionnalités pour vos utilisateurs Microsoft Entra ID permet à Citrix Cloud Government d'utiliser ces capacités automatiquement.

Connecter une passerelle Citrix Gateway sur site en tant que fournisseur d'identité à Citrix Cloud™ Government

Citrix Cloud Government prend en charge l'utilisation d'une passerelle Citrix Gateway sur site en tant que fournisseur d'identité pour authentifier les abonnés se connectant à leurs espaces de travail.

En utilisant l'authentification Citrix Gateway, vous pouvez :

- Continuer à authentifier les utilisateurs via votre Citrix Gateway existante afin qu'ils puissent accéder aux ressources de votre déploiement Citrix Virtual Apps and Desktops™ sur site via Citrix Workspace.
- Utiliser les fonctions d'authentification, d'autorisation et d'audit (AAA) de Citrix Gateway avec Citrix Workspace.
- Utiliser des fonctionnalités telles que l'authentification pass-through, les cartes à puce, les jetons sécurisés, les stratégies d'accès conditionnel et la fédération. De nombreuses autres fonctionnalités offrant à vos utilisateurs l'accès aux ressources dont ils ont besoin via Citrix Workspace.

Versions prises en charge

L'authentification Citrix Gateway est prise en charge pour les versions de produits sur site suivantes :

- Citrix Gateway 12.1 54.13 édition Advanced ou version ultérieure
- Citrix Gateway 13.0 41.20 édition Advanced ou version ultérieure

Conditions préalables

Cloud Connectors

Vous avez besoin d'au moins deux (2) serveurs sur lesquels installer le logiciel Citrix Cloud Connector™. Ces serveurs doivent répondre aux exigences suivantes :

- Répond aux exigences système décrites dans Détails techniques de Cloud Connector.
- Ne contient aucun autre composant Citrix installé, n'est pas un contrôleur de domaine Active Directory et n'est pas une machine critique pour l'infrastructure de votre emplacement de ressources.
- Joint au domaine où réside votre Site. Si les utilisateurs accèdent aux applications de votre Site dans de nombreux domaines, vous devez installer au moins deux Cloud Connectors dans chaque domaine.
- Connecté à un réseau pouvant contacter votre Site.
- Connecté à Internet. Pour plus d'informations, consultez les exigences de Citrix Cloud Connector.
- Citrix recommande deux serveurs pour la haute disponibilité du Cloud Connector. Après l'installation, les Cloud Connectors permettent à Citrix Cloud Government de localiser votre Site et de communiquer avec lui.

Pour plus d'informations sur l'installation du Cloud Connector, consultez Installer les Cloud Connectors à partir de la ligne de commande et Configuration du proxy et du pare-feu de Citrix Cloud Connector.

Active Directory

Avant d'activer l'authentification Citrix Gateway, effectuez les tâches suivantes :

- Vérifiez que les abonnés de votre espace de travail disposent de comptes utilisateur dans l'Active Directory (AD). Les abonnés disposant uniquement de comptes AD peuvent se connecter à leurs espaces de travail avec succès.

- Assurez-vous que les propriétés utilisateur des comptes AD de vos abonnés sont renseignées. Citrix Cloud Government a besoin de ces propriétés pour établir le contexte utilisateur lorsque les abonnés se connectent. Si ces propriétés ne sont pas renseignées, les abonnés ne peuvent pas se connecter à leur espace de travail. Ces propriétés incluent :
  - Adresse e-mail
  - Nom d'affichage
  - Nom commun
  - Nom de compte SAM
  - Nom d'utilisateur principal
  - OID
  - SID
- Connectez votre Active Directory (AD) à votre compte Citrix Cloud Government. Dans cette tâche, vous installez le logiciel Cloud Connector sur les serveurs que vous avez préparés, comme décrit dans la section Cloud Connectors. Les Cloud Connectors permettent à Citrix Cloud Government de communiquer avec votre environnement sur site. Pour obtenir des instructions, consultez Connecter Active Directory à Citrix Cloud Government.
- Si vous effectuez une fédération avec l'authentification Citrix Gateway, synchronisez vos utilisateurs AD avec le fournisseur de fédération. Citrix Cloud Government requiert les attributs utilisateur AD pour vos abonnés d'espace de travail afin qu'ils puissent se connecter avec succès.

Prérequis

Stratégies avancées Citrix Gateway

L'authentification Citrix Gateway requiert l'utilisation de stratégies avancées sur la passerelle sur site en raison de l'obsolescence des stratégies classiques. Les stratégies avancées prennent en charge l'authentification multifacteur pour Citrix Cloud Government, y compris des options telles que l'enchaînement des fournisseurs d'identité (Identity Provider Chaining). Si vous utilisez actuellement des stratégies classiques, vous devez créer de nouvelles stratégies avancées pour utiliser l'authentification Citrix Gateway dans Citrix Cloud Government. Vous pouvez réutiliser la partie Action de la stratégie classique lorsque vous créez la stratégie avancée.

Certificats pour la signature

Lors de la configuration de la passerelle pour authentifier les abonnés à Citrix Workspace, la passerelle agit comme un fournisseur OpenID Connect. Les messages entre Citrix Cloud Government et la passerelle sont conformes au protocole OIDC, qui implique la signature numérique des jetons. Vous devez configurer un certificat pour signer ces jetons. Ce certificat doit être émis par une autorité de certification (CA) publique. L'utilisation d'un certificat émis par une CA privée n'est prise en charge que pour fournir à Citrix Cloud Government le certificat de CA racine privé. Ainsi, la chaîne de confiance du certificat ne peut pas être établie. Si vous configurez plusieurs certificats pour la signature, ces clés sont alternées pour chaque message.

Les clés doivent être liées à **vpn global**. Sans ces clés, les abonnés ne peuvent pas accéder à leur espace de travail avec succès après s'être connectés.

Synchronisation de l'horloge

Étant donné que les messages signés numériquement dans OIDC comportent un horodatage, la passerelle doit être synchronisée avec l'heure NTP. Si l'horloge n'est pas synchronisée, Citrix Cloud Government suppose que les jetons sont périmés lors de la vérification de leur validité.

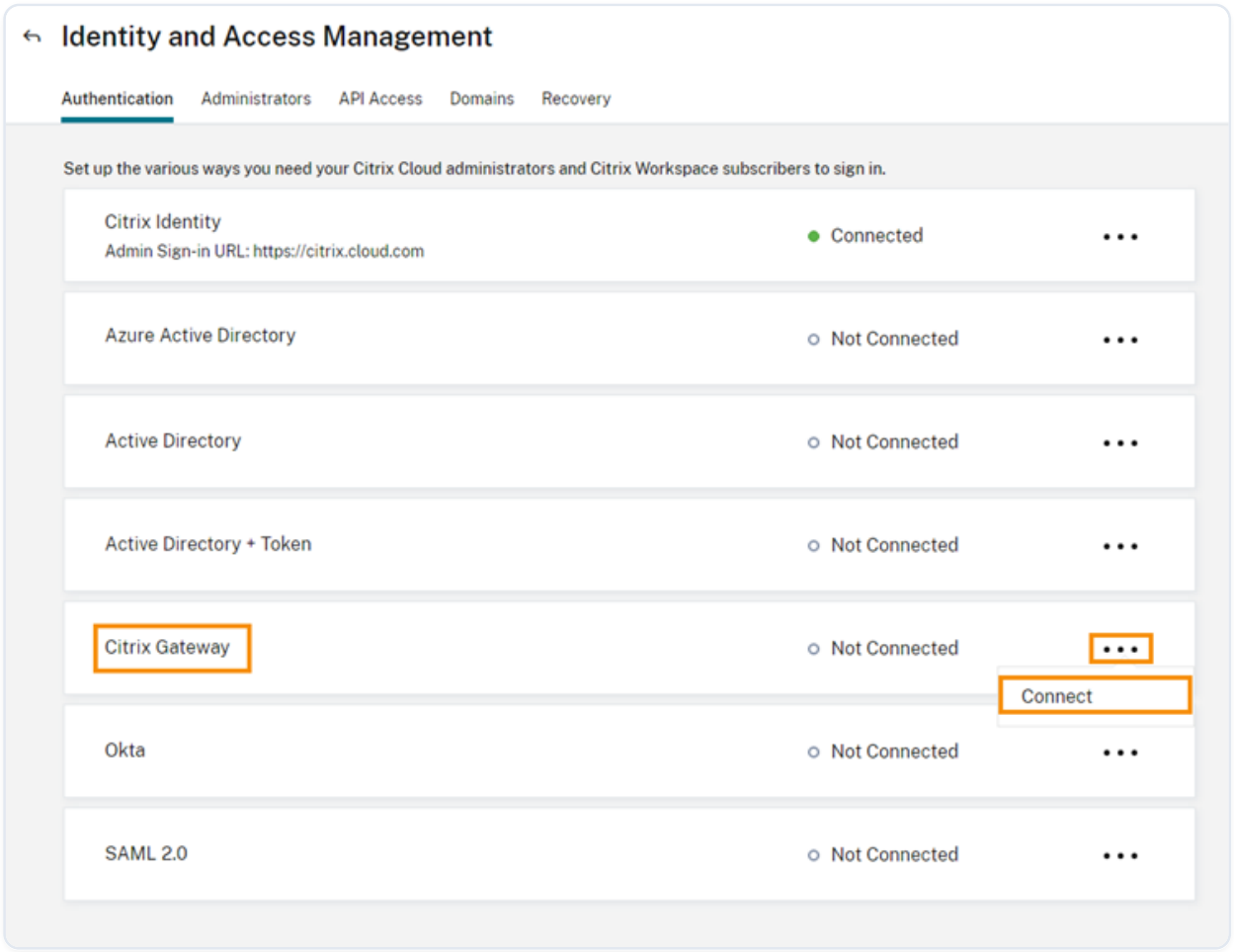
Présentation des tâches

Pour configurer l'authentification Citrix Gateway, vous effectuez les tâches suivantes :

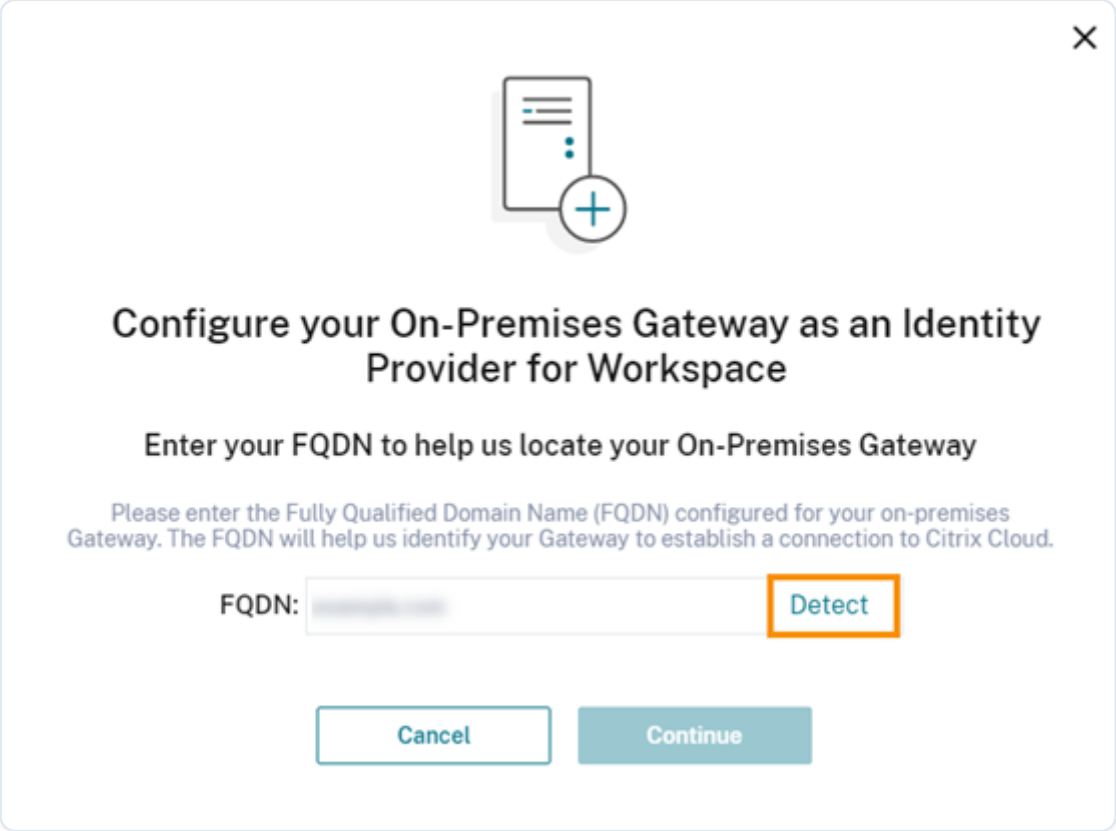
1. Dans **Gestion des identités et des accès**, commencez à configurer la connexion à votre passerelle. Au cours de cette étape, vous générez l'ID client, le secret et l'URL de redirection pour la passerelle.
2. Sur la passerelle, créez une stratégie avancée OAuth IdP à l'aide des informations générées par Citrix Cloud Government. La stratégie avancée OAuth IdP permet à Citrix Cloud Government de se connecter à votre passerelle sur site. Pour obtenir des instructions, consultez les articles suivants :
   - Citrix Gateway 12.1 : Utiliser un Citrix Gateway sur site comme fournisseur d'identité pour Citrix Cloud
   - Citrix Gateway 13.0 : Utiliser un Citrix Gateway sur site comme fournisseur d'identité pour Citrix Cloud
3. Dans **Workspace Configuration**, activez l'authentification Citrix Gateway pour les abonnés.

Pour activer l'authentification Citrix Gateway pour les abonnés de l'espace de travail

1. Dans le menu Citrix Cloud Government, sélectionnez **Identity and access management**.
2. Dans l'onglet **Authentication** de **Citrix Gateway**, cliquez sur le menu des points de suspension et sélectionnez **Connect**.



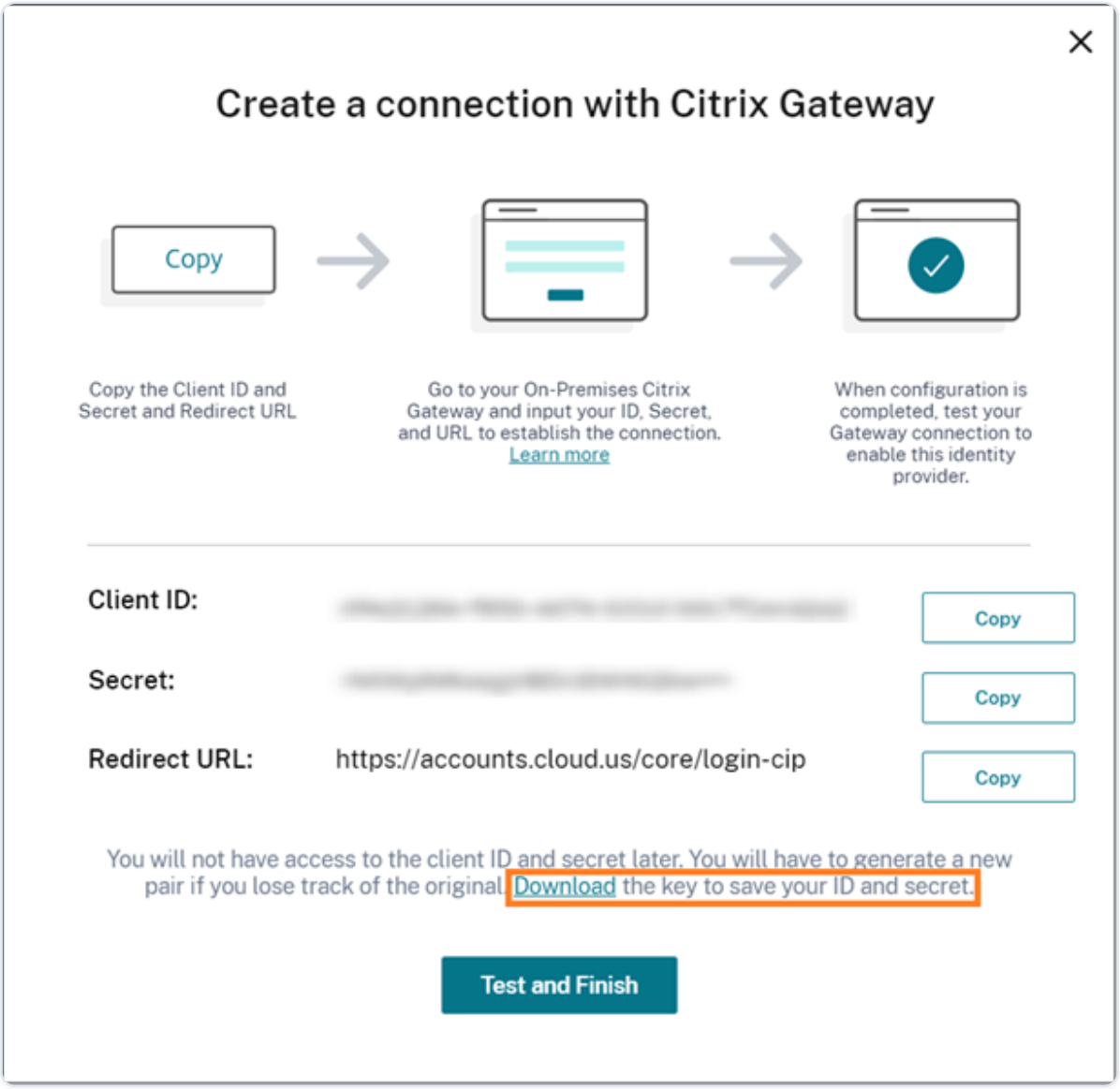
3. Saisissez le FQDN de votre Gateway sur site et cliquez sur **Detect**.



Une fois que Citrix Cloud Government l'a détecté avec succès, cliquez sur **Continue**.

4. Créez une connexion avec votre Gateway sur site :

a. Copiez l'ID client, le secret et l'URL de redirection affichés par Citrix Cloud Government.



De plus, téléchargez une copie de ces informations et enregistrez-les en toute sécurité hors ligne pour votre référence. Ces informations ne sont plus disponibles dans Citrix Cloud Government après leur génération.

b. Sur la Gateway, créez une stratégie avancée OAuth IdP à l'aide de l'ID client, du secret et de l'URL de redirection de Citrix Cloud Government. Pour obtenir des instructions, consultez les articles suivants :

- Pour Citrix Gateway 12.1 : Utiliser un Citrix Gateway sur site comme fournisseur d'identité pour Citrix Cloud
- Pour Citrix Gateway 13.0 : Utiliser un Citrix Gateway sur site comme fournisseur d'identité pour Citrix Cloud

c. Cliquez sur **Test and Finish**. Citrix Cloud Government vérifie que votre Gateway est accessible et configurée correctement.

5. Activez l'authentification Citrix Gateway pour les espaces de travail :

    a. Dans le menu Citrix Cloud Government, sélectionnez **Workspace Configuration**.

    b. Depuis l'onglet **Authentification**, sélectionnez **Citrix Gateway**.

    c. Sélectionnez **Je comprends l'impact sur l'expérience de l'abonné**, puis cliquez sur **Enregistrer**.

Dépannage

Dans un premier temps, consultez les sections Prérequis et Exigences de cet article. Vérifiez que vous disposez de tous les composants requis dans votre environnement sur site et que vous avez effectué toutes les configurations nécessaires. Si l'un de ces éléments est manquant ou mal configuré, l'authentification de l'espace de travail avec Citrix Gateway ne fonctionnera pas.

Si vous rencontrez un problème lors de l'établissement d'une connexion entre Citrix Cloud Government et votre Gateway sur site, vérifiez les points suivants :

- Le FQDN de la Gateway est accessible depuis Internet.
- Vous avez saisi correctement le FQDN de la Gateway dans Citrix Cloud Government.
- Vous avez saisi correctement l'URL de la Gateway dans le paramètre `-issuer` de la stratégie OAuth IdP. Exemple : `-issuer https://GatewayFQDN.com`. Le paramètre `issuer` est sensible à la casse.
- Les valeurs d'ID client, de secret et d'URL de redirection de Citrix Cloud Government sont correctement saisies dans les champs ID client, Secret client, URL de redirection et Audience de la stratégie OAuth IdP. Vérifiez que l'ID client correct a été saisi dans le champ Audience de la stratégie.
- La stratégie d'authentification OAuth IdP est configurée correctement. Pour obtenir des instructions, consultez les articles suivants :
    - Citrix Gateway 12.1 : Utiliser une Citrix Gateway sur site comme fournisseur d'identité pour Citrix Cloud
    - Citrix Gateway 13.0 : Utiliser une Citrix Gateway sur site comme fournisseur d'identité pour Citrix Cloud
- Vérifiez que la stratégie est correctement liée au serveur d'authentification AAA, comme décrit dans Liaison des stratégies d'authentification.

Serveurs de catalogue global

En plus de récupérer les détails des comptes utilisateur, Gateway récupère le nom de domaine des utilisateurs, le nom NETBIOS AD et le nom de domaine AD racine. Pour récupérer le nom NETBIOS AD, Gateway recherche l'AD où se trouvent les comptes utilisateur. Les noms NETBIOS ne sont pas répliqués sur les serveurs de catalogue global.

Si vous utilisez des serveurs de catalogue global dans votre environnement AD, les actions LDAP configurées sur ces serveurs ne fonctionnent pas avec Citrix Cloud Government. Au lieu de cela, vous devez configurer les AD individuels dans l'action LDAP. Si vous avez plusieurs domaines ou forêts, vous pouvez configurer plusieurs stratégies LDAP.

Recherche AD pour l'authentification unique avec Kerberos ou le chaînage IdP

Si vous utilisez Kerberos ou un fournisseur d'identité externe qui utilise les protocoles SAML ou OIDC pour la connexion des abonnés, vérifiez que la recherche AD est configurée. Gateway nécessite des recherches AD pour récupérer les propriétés utilisateur AD et les propriétés de configuration AD des abonnés.

Assurez-vous que des stratégies LDAP sont configurées, même si l'authentification est effectuée avec les serveurs tiers. Pour configurer ces stratégies, vous ajoutez un deuxième facteur d'authentification à votre profil de schéma de connexion existant en suivant les étapes suivantes :

1. Créez un serveur d'authentification LDAP qui effectue uniquement l'extraction d'attributs et de groupes à partir d'Active Directory.
2. Créez une stratégie d'authentification avancée LDAP.
3. Créez une étiquette de stratégie d'authentification.
4. Définissez l'étiquette de stratégie d'authentification comme facteur suivant, après le fournisseur d'identité principal.

Pour ajouter LDAP comme deuxième facteur d'authentification

1. Créez le serveur d'authentification LDAP :
    a. Sélectionnez **Système > Authentification > Stratégies de base > LDAP > Serveurs > Ajouter**.
    b. Sur la page **Créer un serveur LDAP d'authentification**, saisissez les informations suivantes :
        - Dans **Choisir le type de serveur**, sélectionnez **LDAP**.
        - Dans **Nom**, saisissez un nom convivial pour le serveur.

- Sélectionnez **Adresse IP du serveur**, puis saisissez l'adresse IP du serveur LDAP.
- Dans **Type de sécurité**, sélectionnez le type de sécurité LDAP requis.
- Dans **Type de serveur**, sélectionnez **AD**.
- Dans **Authentification**, ne cochez pas la case. Cette case doit être décochée car ce serveur d'authentification sert uniquement à extraire les attributs utilisateur et les groupes d'Active Directory, et non à l'authentification.

c. Sous **Autres paramètres**, saisissez les informations suivantes :

- Dans **Attribut de nom de connexion du serveur**, saisissez **UserPrincipalName**.
- Dans **Attribut de groupe**, sélectionnez **memberOf**.
- Dans **Nom du sous-attribut**, sélectionnez **cn**.

2. Créez la stratégie d'authentification avancée LDAP :

a. Sélectionnez **Sécurité > AAA - Trafic d'application > Stratégies > Authentification > Stratégies avancées > Stratégie > Ajouter**.

b. Sur la page **Créer une stratégie d'authentification**, saisissez les informations suivantes :

- Dans **Nom**, saisissez un nom convivial pour la stratégie.
- Dans **Type d'action**, sélectionnez **LDAP**.
- Dans **Action**, sélectionnez le serveur d'authentification LDAP que vous avez créé précédemment.
- Dans **Expression**, saisissez **TRUE**.

c. Cliquez sur **Créer** pour enregistrer la configuration.

3. Créer l'étiquette de stratégie d'authentification :

a. Sélectionnez **Sécurité > AAA – Trafic d'application > Stratégies > Authentification > Stratégies avancées > Étiquette de stratégie > Ajouter**.

b. Dans **Nom**, entrez un nom convivial pour l'étiquette de stratégie d'authentification.

c. Dans Schéma de connexion, sélectionnez **LSCHEMA_INT**.

d. Sous **Liaison de stratégie**, dans **Sélectionner la stratégie**, sélectionnez la stratégie d'authentification avancée LDAP que vous avez créée précédemment.

e. Dans **Expression GoTo**, sélectionnez **FIN**.

f. Cliquez sur **Lier** pour terminer la configuration.

4. Définissez l'étiquette de stratégie d'authentification LDAP comme facteur suivant, après le fournisseur d'identité principal :

    a. Sélectionnez **Système > Sécurité > AAA - Trafic d'application > Serveurs virtuels**.

    b. Sélectionnez le serveur virtuel qui a la liaison pour votre fournisseur d'identité principal et sélectionnez **Modifier**.

    c. Sous **Stratégies d'authentification avancées**, sélectionnez les liaisons de **Stratégie d'authentification** existantes.

    d. Sélectionnez la liaison pour votre fournisseur d'identité principal, puis sélectionnez **Modifier la liaison**.

    e. Sur la page **Liaison de stratégie**, dans **Sélectionner le facteur suivant**, sélectionnez l'étiquette de stratégie d'authentification LDAP que vous avez créée précédemment.

    f. Cliquez sur **Lier** pour enregistrer la configuration.

Mot de passe par défaut pour l'authentification multifacteur

Si vous utilisez l'authentification multifacteur pour les abonnés à l'espace de travail, Gateway utilise le mot de passe du dernier facteur comme mot de passe par défaut pour l'authentification unique. Ce mot de passe est envoyé à Citrix Cloud Government lorsque les abonnés se connectent à leur espace de travail. Si l'authentification LDAP est suivie d'un autre facteur dans votre environnement, vous devez configurer le mot de passe LDAP comme mot de passe par défaut envoyé à Citrix Cloud Government. Activez **SSOCredentials** sur le schéma de connexion correspondant au facteur LDAP.

Connecter Okta en tant que fournisseur d'identité à Citrix Cloud™ Government

Citrix Cloud Government prend en charge l'utilisation d'Okta comme fournisseur d'identité pour authentifier les abonnés se connectant à leurs espaces de travail. En connectant votre organisation Okta à Citrix Cloud Government, vous pouvez offrir une expérience de connexion commune à vos abonnés pour accéder aux ressources de Citrix Workspace.

Après avoir activé l'authentification Okta dans la configuration de l'espace de travail, les abonnés ont une expérience de connexion différente. La sélection de l'authentification Okta fournit une connexion fédérée, et non une authentification unique. Les abonnés se connectent aux espaces de travail à partir d'une page de connexion Okta. Ils pourraient devoir s'authentifier une deuxième fois lors de l'ouverture d'une application ou d'un bureau depuis Citrix DaaS (anciennement le service Citrix Virtual Apps and Desktops™).

Prérequis

Cloud Connectors

Vous avez besoin d'au moins deux (2) serveurs dans votre domaine Active Directory sur lesquels installer le logiciel Citrix Cloud Connector. Les Cloud Connectors sont nécessaires pour permettre la communication entre Citrix Cloud Government et votre emplacement de ressources. Citrix recommande deux serveurs pour la haute disponibilité des Cloud Connectors. Ces serveurs doivent répondre aux exigences suivantes :

- Répond aux exigences décrites dans Détails techniques du Cloud Connector.
- Ne doit pas avoir d'autres composants Citrix® installés et ne doit pas être un contrôleur de domaine Active Directory. Il ne s'agit pas d'une machine critique pour l'infrastructure de votre emplacement de ressources.
- Joint à votre domaine Active Directory (AD). Si les ressources et les utilisateurs de votre espace de travail se trouvent dans des domaines différents, vous devez installer au moins deux Cloud Connectors dans chaque domaine. Pour plus d'informations, consultez Scénarios de déploiement des Cloud Connectors dans Active Directory.
- Connecté à un réseau pouvant contacter les ressources auxquelles les utilisateurs accèdent via Citrix Workspace.
- Connecté à Internet. Pour plus d'informations, consultez Exigences relatives au Citrix Cloud Connector.

Pour plus d'informations sur l'installation des Cloud Connectors, consultez Installer les Cloud Connectors à partir de la ligne de commande et Configuration du proxy et du pare-feu du Citrix Cloud Connector.

Domaine Okta

Lors de la connexion d'Okta à Citrix Cloud Government, vous devez fournir le domaine Okta de votre organisation. Citrix prend en charge les domaines Okta suivants :

- okta.com
- okta-eu.com
- oktapreview.com

Vous pouvez également utiliser des domaines personnalisés Okta avec Citrix Cloud Government. Consultez les considérations importantes concernant l'utilisation de domaines personnalisés dans Personnaliser le domaine d'URL Okta sur le site Web d'Okta.

Pour plus d'informations sur la localisation du domaine personnalisé de votre organisation, consultez Rechercher votre domaine Okta sur le site Web d'Okta.

Application Web Okta OIDC

Pour utiliser Okta comme fournisseur d'identité, vous devez d'abord créer une application Web Okta OIDC avec des informations d'identification client que vous pouvez utiliser avec Citrix Cloud Government. Après avoir créé et configuré l'application, notez l'ID client et le secret client. Vous fournissez ces valeurs à Citrix Cloud Government lorsque vous connectez votre organisation Okta.

Pour créer et configurer cette application, consultez les sections suivantes de cet article :

- Créer une application Web Okta OIDC
- Configurer l'application Web Okta OIDC

URL de l'espace de travail

Lors de la création de l'application Okta, vous devez fournir l'URL de votre espace de travail depuis Citrix Cloud Government. Pour localiser l'URL de l'espace de travail, sélectionnez **Configuration de l'espace de travail** dans le menu Citrix Cloud Government. L'URL de l'espace de travail s'affiche dans l'onglet **Accès**.

> **Important :**

> Si vous modifiez l'URL de l'espace de travail ultérieurement, vous devez mettre à jour la configuration de l'application Okta avec la nouvelle URL. Dans le cas contraire, vos abonnés pourraient rencontrer des problèmes lors de la déconnexion de leur espace de travail.

Jeton d'API Okta

L'utilisation d'Okta comme fournisseur d'identité avec Citrix Cloud Government nécessite un jeton d'API pour votre organisation Okta. Créez ce jeton à l'aide d'un compte d'administrateur en lecture seule dans votre organisation Okta. Ce jeton peut lire les utilisateurs et les groupes de votre organisation Okta.

Pour créer le jeton d'API, consultez Créer un jeton d'API Okta dans cet article. Pour plus d'informations sur les jetons d'API, consultez Créer un jeton d'API sur le site Web d'Okta.

> **Important :**

> Lorsque vous créez le jeton d'API, notez la valeur du jeton (par exemple, copiez temporairement la valeur dans un document texte brut). Okta n'affiche cette valeur qu'une seule fois, vous pouvez donc créer le jeton juste avant d'effectuer les étapes de Connecter Citrix Cloud Government à votre organisation Okta.

Synchroniser les comptes avec l'agent Okta AD

Pour utiliser Okta comme fournisseur d'identité, vous devez d'abord intégrer votre AD sur site à Okta. Pour ce faire, vous installez l'agent Okta AD dans votre domaine et ajoutez votre AD à votre organisation Okta. Pour obtenir des conseils sur le déploiement de l'agent Okta AD, consultez Démarrer avec l'intégration Active Directory sur le site Web d'Okta.

Ensuite, vous importez vos utilisateurs et groupes AD dans Okta. Lors de l'importation, incluez les valeurs suivantes associées à vos comptes AD :

- E-mail
- SID
- UPN
- OID

> **Remarque :**

> Si vous utilisez le service Citrix Gateway avec Workspace, vous n'avez pas besoin de synchroniser vos comptes AD avec votre organisation Okta.

> Pour synchroniser vos utilisateurs et groupes AD avec votre organisation Okta :

1. Installez et configurez l'agent Okta AD. Pour des instructions complètes, reportez-vous aux articles suivants sur le site Web d'Okta :
   - Installer l'agent Okta Active Directory
   - Configurer l'importation Active Directory et les paramètres de compte
   - Configurer les paramètres de provisionnement d'Active Directory
2. Ajoutez vos utilisateurs et groupes AD à Okta en effectuant une importation manuelle ou une importation automatisée. Pour plus d'informations sur les méthodes et instructions

d'importation Okta, consultez Gérer les utilisateurs et les groupes Active Directory sur le site web d'Okta.

Créer une application web Okta OIDC

1. Depuis la console de gestion Okta, sous **Applications**, sélectionnez **Applications**.
2. Sélectionnez **Créer une intégration d'application**.
3. Dans **Méthode de connexion**, sélectionnez **OIDC - OpenID Connect**.
4. Dans **Type d'application**, sélectionnez **Application web**. Sélectionnez **Suivant**.
5. Dans **Nom de l'intégration d'application**, saisissez un nom convivial pour l'intégration d'application.
6. Dans **Type d'octroi**, sélectionnez les options suivantes :
   - Code d'autorisation
   - Implicite (Hybride)
7. Dans **URI de redirection de connexion**, saisissez `https://accounts.cloud.us/core/login-okta`.
8. Dans **URI de redirection de déconnexion**, saisissez l'URL de votre espace de travail depuis Citrix Cloud.
9. Sous **Attributions**, dans **Accès contrôlé**, sélectionnez si vous souhaitez attribuer l'intégration d'application à tous les membres de votre organisation, uniquement aux groupes que vous spécifiez, ou attribuer l'accès ultérieurement.
10. Sélectionnez **Enregistrer**. Après avoir enregistré l'intégration de l'application, la console affiche la page de configuration de l'application.
11. Dans la section **Informations d'identification du client**, copiez les valeurs **ID client** et **Secret client**. Vous utilisez ces valeurs lorsque vous (#connect-citrix-cloud-government-to-your-okta-organization) connectez Citrix Cloud Government à votre organisation Okta.

Configurer l'application web Okta OIDC

Dans cette étape, vous configurez votre application web Okta OIDC avec les paramètres requis pour Citrix Cloud Government. Citrix Cloud Government exige ces paramètres pour authentifier vos abonnés via Okta lorsqu'ils se connectent à leurs espaces de travail.

1. (Facultatif) Mettez à jour les autorisations client pour le type d'octroi implicite. Vous pouvez choisir d'effectuer cette étape si vous préférez accorder le moins de privilèges possible pour ce type d'octroi.

a. Depuis la page de configuration de l'application Okta, sous **Paramètres généraux**, sélectionnez **Modifier**.

b. Dans la section **Application**, sous **Client agissant au nom de l'utilisateur**, désactivez l'option **Autoriser le jeton d'accès avec le type d'octroi implicite**.

c. Sélectionnez **Enregistrer**.

2. Ajoutez des attributs d'application. Ces attributs sont sensibles à la casse.

a. Dans le menu de la console Okta, sélectionnez **Annuaire > Éditeur de profil**.

b. Sélectionnez le profil Okta **Utilisateur (par défaut)**. Okta affiche la page de profil **Utilisateur**.

c. Sous **Attributs**, sélectionnez **Ajouter un attribut**.

d. Saisissez les informations suivantes :

- Nom d'affichage : cip_email
- Nom de la variable : cip_email
- Description : E-mail de l'utilisateur AD
- Longueur de l'attribut : Supérieure à 1
- Attribut requis : Oui

e. Sélectionnez **Enregistrer et ajouter un autre**.

f. Saisissez les informations suivantes :

- Nom d'affichage : cip_sid
- Nom de la variable : cip_sid
- Description : Identificateur de sécurité de l'utilisateur AD
- Longueur de l'attribut : Supérieure à 1
- Attribut requis : Oui

g. Sélectionnez **Enregistrer et ajouter un autre**.

h. Saisissez les informations suivantes :

- Nom d'affichage : cip_upn
- Nom de la variable : cip_upn
- Description : Nom d'utilisateur principal AD
- Longueur de l'attribut : Supérieure à 1

- Attribut requis : Oui

i. Sélectionnez **Enregistrer et ajouter un autre**.

j. Saisissez les informations suivantes :

- Nom d'affichage : cip_oid
- Nom de la variable : cip_oid
- Description : GUID utilisateur AD
- Longueur de l'attribut : Supérieure à 1
- Attribut requis : Oui

k. Sélectionnez **Enregistrer**.

3. Modifiez les mappages d'attributs pour l'application :

a. Depuis la console Okta, sélectionnez **Répertoire > Éditeur de profil**.

b. Localisez le profil **active_directory** pour votre AD. Ce profil peut être étiqueté en utilisant le format `myDomain User`, où `myDomain` est le nom de votre domaine AD intégré.

c. Sélectionnez **Mappages**. La page Mappages de profils utilisateur pour votre domaine AD apparaît et l'onglet de mappage de votre AD à l'utilisateur Okta est sélectionné.

d. Dans la colonne **Profil utilisateur Okta**, localisez les attributs que vous avez créés à l'étape 2 et mappez-les comme suit :

- Pour `cip_email`, sélectionnez `email` dans la colonne Profil utilisateur de votre domaine. Une fois sélectionné, le mappage apparaît comme `appuser.email`.
- Pour `cip_sid`, sélectionnez `objectSid` dans la colonne Profil utilisateur de votre domaine. Une fois sélectionné, le mappage apparaît comme `appuser.objectSid`.
- Pour `cip_upn`, sélectionnez `userName` dans la colonne Profil utilisateur de votre domaine. Une fois sélectionné, le mappage apparaît comme `appuser.userName`.
- Pour `cip_oid`, sélectionnez `externalId` dans la colonne Profil utilisateur de votre domaine. Une fois sélectionné, le mappage apparaît comme `appuser.externalId`.

e. Sélectionnez **Enregistrer les mappages**.

f. Sélectionnez **Appliquer les mises à jour maintenant**. Okta démarre une tâche pour appliquer les mappages.

g. Synchronisez Okta avec votre AD.

i. Depuis la console Okta, sélectionnez **Directory > Directory Integrations**.

ii. Sélectionnez votre AD intégré.

iii. Sélectionnez l'onglet **Provisioning**.

iv. Sous **Settings**, sélectionnez **To Okta**.

v. Faites défiler jusqu'à la section **Okta Attribute Mappings**, puis sélectionnez **Force Sync**.

Créer un jeton d'API Okta

1. Connectez-vous à la console Okta à l'aide d'un compte d'administrateur en lecture seule.
2. Dans le menu de la console Okta, sélectionnez **Security > API**.
3. Sélectionnez l'onglet **Tokens**, puis sélectionnez **Create Token**.
4. Saisissez un nom pour le jeton.
5. Sélectionnez **Create Token**.
6. Copiez la valeur du jeton. Vous fournissez cette valeur lorsque vous connectez votre organisation Okta à Citrix Cloud.

Connecter Citrix Cloud Government à votre organisation Okta

1. Connectez-vous à Citrix Cloud Government à l'adresse https://citrix.cloud.us.
2. Dans le menu Citrix Cloud Government, sélectionnez **Identity and access management**.
3. Recherchez **Okta** et sélectionnez **Connect** dans le menu des ellipses.
4. Dans **Okta URL**, saisissez votre domaine Okta.
5. Dans **Okta API Token**, saisissez le jeton API de votre organisation Okta.
6. Dans **Client ID** et **Client Secret**, saisissez l'ID client et le secret de l'intégration d'application web OIDC que vous avez créée précédemment. Pour copier ces valeurs depuis la console Okta, sélectionnez **Applications** et localisez votre application Okta. Sous **Client Credentials**, utilisez le bouton **Copy to Clipboard** pour chaque valeur.
7. Cliquez sur **Test and Finish**. Citrix Cloud Government vérifie vos informations Okta et teste la connexion.

Une fois la connexion vérifiée avec succès, vous pouvez activer l'authentification Okta pour les abonnés de l'espace de travail.

Activer l'authentification Okta pour les espaces de travail

1. Dans le menu Citrix Cloud Government, sélectionnez **Workspace Configuration > Authentication**.
2. Sélectionnez **Okta**.
3. Lorsque vous y êtes invité, sélectionnez **Je comprends l'impact sur l'expérience de l'abonné**.
4. Sélectionnez **Enregistrer**.

Après être passé à l'authentification Okta, Citrix Cloud désactive temporairement les espaces de travail pendant quelques minutes. Lorsque les espaces de travail sont réactivés, vos abonnés peuvent se connecter à l'aide d'Okta.

Connecter SAML en tant que fournisseur d'identité à Citrix Cloud™ Government

Citrix Cloud Government prend en charge l'utilisation de SAML (Security Assertion Markup Language) en tant que fournisseur d'identité pour authentifier les administrateurs (aperçu) et les abonnés se connectant à leurs espaces de travail. Vous pouvez utiliser le fournisseur SAML 2.0 de votre choix avec votre Active Directory (AD) sur site.

Prérequis

L'utilisation de l'authentification SAML avec Citrix Cloud Government a les exigences suivantes :

- Fournisseur SAML qui prend en charge SAML 2.0
- Domaine AD sur site
- Deux Cloud Connectors déployés sur un emplacement de ressources et joints à votre domaine AD sur site. Les Cloud Connectors sont utilisés pour garantir que Citrix Cloud Government peut communiquer avec votre emplacement de ressources.
- Intégration AD avec votre fournisseur SAML.

Cloud Connectors

Vous avez besoin d'au moins deux (2) serveurs sur lesquels installer le logiciel Citrix Cloud Connector™. Citrix recommande au moins deux serveurs pour la haute disponibilité des Cloud Connectors. Ces serveurs doivent répondre aux exigences suivantes :

- Répond aux exigences système décrites dans Exigences de Citrix Cloud Connector.

- Ne doit pas avoir d'autres composants Citrix® installés, ne doit pas être un contrôleur de domaine AD, et ne doit pas être une machine critique pour l'infrastructure de votre emplacement de ressources.
- Joint au domaine où se trouvent vos ressources. Si les utilisateurs accèdent à des ressources dans de nombreux domaines, vous devez installer au moins deux Cloud Connectors dans chaque domaine.
- Connecté à un réseau pouvant contacter les ressources auxquelles les abonnés accèdent via Citrix Workspace.
- Connecté à Internet. Pour plus d'informations, consultez Exigences de connectivité pour Citrix Cloud Government.

Pour plus d'informations sur l'installation du Cloud Connector, consultez Tâche 3 : Installer les Cloud Connectors.

Active Directory

Avant de configurer l'authentification SAML, effectuez les tâches suivantes :

- Vérifiez que les abonnés de votre espace de travail disposent de comptes utilisateur dans Active Directory (AD). Les abonnés disposant uniquement de comptes AD ne peuvent pas se connecter à leurs espaces de travail si l'authentification SAML est configurée.
- Assurez-vous que les propriétés utilisateur des comptes AD de vos abonnés sont renseignées. Citrix Cloud Government a besoin de ces propriétés pour établir le contexte utilisateur lorsque les abonnés se connectent à Citrix Workspace. Si ces propriétés ne sont pas renseignées, les abonnés ne peuvent pas se connecter. Ces propriétés incluent :
  - Adresse e-mail
  - Nom d'affichage (facultatif)
  - Nom commun
  - Nom de compte SAM
  - Nom d'utilisateur principal
  - GUID d'objet
  - SID
- Connectez votre Active Directory (AD) à votre compte Citrix Cloud Government en déployant des Cloud Connectors dans votre AD sur site.

- Synchronisez vos utilisateurs AD avec le fournisseur SAML. Citrix Cloud Government requiert les attributs utilisateur AD pour les abonnés de votre espace de travail afin qu'ils puissent se connecter avec succès.

Intégration SAML avec Active Directory

Avant d'activer l'authentification SAML, vous devez intégrer votre AD sur site à votre fournisseur SAML. Cette intégration permet au fournisseur SAML de transmettre les attributs utilisateur AD requis suivants à Citrix Cloud dans l'assertion SAML :

- SecurityIDentifier (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (e-mail)

Bien que les étapes d'intégration précises varient selon les fournisseurs SAML, le processus d'intégration comprend généralement les tâches suivantes :

1. Installez un agent de synchronisation dans votre domaine AD pour établir une connexion entre votre domaine et votre fournisseur SAML.
2. Si vous ne disposez pas déjà d'attributs personnalisés qui correspondent aux attributs utilisateur AD décrits précédemment. Créez les attributs personnalisés et mappez-les à AD. À titre de référence, les étapes générales de cette tâche sont décrites dans Créer et mapper des attributs SAML personnalisés dans cet article.
3. Synchronisez vos utilisateurs AD avec votre fournisseur SAML.

> **Remarque :**

> Si vous avez déjà créé des attributs personnalisés qui correspondent aux attributs utilisateur AD requis répertoriés précédemment dans cette section. Vous n'avez pas besoin de créer et de mapper d'autres attributs personnalisés. Utilisez plutôt vos attributs personnalisés existants lorsque vous configurez les métadonnées de votre fournisseur SAML dans Citrix Cloud Government.

> Pour plus d'informations sur l'intégration de votre AD avec votre fournisseur SAML, consultez la documentation produit de votre fournisseur SAML.

Authentification de l'administrateur avec SAML 2.0

> **Remarque :**
>
> L'authentification SAML pour les administrateurs de Citrix Cloud Government est en préversion technique. Nous vous recommandons d'utiliser les fonctionnalités de préversion uniquement dans des environnements non-production.

Groupes AD

Vous pouvez ajouter des administrateurs à Citrix Cloud Government en utilisant uniquement des groupes AD. Vous ne pouvez pas ajouter d'administrateurs individuellement si vous utilisez l'authentification SAML.

URL de connexion

Lors de la configuration de l'authentification SAML, vous configurez une URL de connexion que les administrateurs peuvent utiliser pour se connecter à Citrix Cloud Government. Cette URL utilise le format `https://citrix.cloud.us/go/myorganization`, où **myorganization** est l'identifiant unique que vous choisissez pour votre organisation.

Après avoir ajouté des groupes AD, les administrateurs du groupe peuvent se connecter immédiatement à Citrix Cloud Government à l'aide de l'URL de connexion que vous avez spécifiée. Citrix n'envoie aucune notification pour informer les administrateurs qu'ils ont accès à Citrix Cloud Government.

Autorisations prises en charge

Seules les autorisations d'accès personnalisées sont prises en charge. Lorsque vous ajoutez un groupe AD, vous devez sélectionner les autorisations que vous souhaitez accorder aux administrateurs du groupe. Les autorisations d'accès complet ne sont pas prises en charge.

Vue d'ensemble des tâches

Pour configurer l'authentification SAML, vous effectuez les tâches suivantes :

1. Dans **Gestion des identités et des accès**, connectez votre AD local à Citrix Cloud Government comme décrit dans Connecter Active Directory à Citrix Cloud Government.
2. Intégrez votre fournisseur SAML à votre AD local comme décrit dans Intégration SAML avec Active Directory dans cet article.

3. Dans **Gestion des identités et des accès**, configurez l'authentification SAML dans Citrix Cloud Government. Cette tâche implique la configuration de votre fournisseur SAML avec les métadonnées SAML de Citrix Cloud Government. Ensuite, la configuration de Citrix Cloud Government avec les métadonnées de votre fournisseur SAML pour créer la connexion SAML.
4. Si vous utilisez SAML pour authentifier les administrateurs :
    a. Configurez l'URL de connexion que les administrateurs peuvent utiliser pour se connecter à Citrix Cloud Japan.
    b. Ajoutez des administrateurs à Citrix Cloud Government en spécifiant les groupes AD auxquels ils appartiennent.
5. Si vous utilisez SAML pour authentifier les abonnés de l'espace de travail, activez la méthode d'authentification SAML dans **Configuration de l'espace de travail**. Si vous utilisez SAML uniquement pour authentifier les administrateurs Citrix Cloud, vous n'avez pas besoin d'effectuer cette tâche.

Créer et mapper des attributs SAML personnalisés

Si vous avez déjà configuré des attributs personnalisés pour les attributs SID, UPN, OID et email dans votre fournisseur SAML, vous n'avez pas besoin d'effectuer cette tâche. Passez à Créer une application de connecteur SAML et utilisez vos attributs SAML personnalisés existants à l'étape 8.

> **Remarque :**
>
> Les étapes de cette section décrivent les actions que vous effectuez dans la console d'administration de votre fournisseur SAML. Les commandes spécifiques que vous utilisez pour effectuer ces actions peuvent varier par rapport aux commandes décrites dans cette section, en fonction du fournisseur SAML que vous avez choisi. Les commandes du fournisseur SAML dans cette section sont fournies à titre d'exemples uniquement. Reportez-vous à la documentation de votre fournisseur SAML pour plus d'informations sur les commandes correspondantes pour votre fournisseur SAML.

1. Connectez-vous à la console d'administration de votre fournisseur SAML et sélectionnez l'option de création d'attributs utilisateur personnalisés. Par exemple, selon la console de votre fournisseur SAML, vous pouvez sélectionner **Utilisateurs > Champs utilisateur personnalisés > Nouveau champ utilisateur**.
2. Ajoutez les attributs suivants :

- cip_sid
- cip_upn
- cip_oid
- cip_email

3. Sélectionnez l'AD que vous avez connecté à Citrix Cloud Government. Par exemple, selon la console de votre fournisseur SAML, vous pouvez sélectionner **Utilisateurs > Répertoires**.
4. Sélectionnez l'option d'ajout d'attributs de répertoire. Par exemple, selon la console de votre fournisseur SAML, vous pouvez sélectionner **Attributs de répertoire**.
5. Sélectionnez l'option d'ajout d'attributs et mappez les attributs AD suivants aux attributs utilisateur personnalisés que vous avez créés à l'étape 2 :
   - Sélectionnez `objectSid` et mappez-le à l'attribut `cip_sid`.
   - Sélectionnez `userPrincipalName` et mappez-le à l'attribut `cip_upn`.
   - Sélectionnez `ObjectGUID` et mappez-le à l'attribut `cip_oid`.
   - Sélectionnez `mail` et mappez-le à l'attribut `cip_email`.

Configurer l'URL de connexion de l'administrateur

1. Connectez-vous à Citrix Cloud à l'adresse https://citrix.cloud.us.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
3. Recherchez **SAML 2.0** et sélectionnez **Connecter** dans le menu des points de suspension.
4. Lorsque vous y êtes invité, entrez un identifiant court et convivial pour votre entreprise, puis sélectionnez **Enregistrer et continuer**. La page **Configurer SAML** apparaît.
5. Passez à la section suivante pour configurer la connexion SAML à Citrix Cloud Government.

Configurer les métadonnées du fournisseur SAML

Dans cette tâche, vous créez une application de connecteur à l'aide des métadonnées SAML de Citrix Cloud Government. Après avoir configuré l'application SAML, vous utilisez les métadonnées SAML de votre application de connecteur pour configurer la connexion SAML à Citrix Cloud Government.

> **Remarque :**

> Certaines étapes de cette section décrivent les actions que vous effectuez dans la console d'administration de votre fournisseur SAML. Les commandes spécifiques que vous utilisez pour effectuer ces actions peuvent varier des commandes décrites dans cette section, selon le fournisseur SAML que vous avez choisi. Les commandes du fournisseur SAML dans cette section sont fournies à titre d'exemples uniquement. Reportez-vous à la documentation de votre fournisseur SAML pour plus d'informations sur les commandes correspondantes pour votre fournisseur SAML.

Créer une application de connecteur SAML

1. Connectez-vous à Citrix Cloud Government à l'adresse https://citrix.cloud.us.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
3. Recherchez **SAML 2.0** et sélectionnez **Connecter** dans le menu des points de suspension. L'écran **Configurer SAML** s'affiche.
4. Depuis la console d'administration de votre fournisseur SAML, ajoutez une application pour un fournisseur d'identité avec des attributs et une réponse de signature. Par exemple, selon la console de votre fournisseur, vous pouvez sélectionner **Applications > Applications > Ajouter une application**, puis sélectionner **Connecteur de test SAML (IdP avec attributs et réponse de signature)**.
5. Le cas échéant, saisissez un nom d'affichage et enregistrez l'application.
6. Dans l'écran **Configurer SAML** de Citrix Cloud Government, sous **Métadonnées SAML**, sélectionnez **Télécharger**. Le fichier XML de métadonnées apparaît dans un autre onglet du navigateur.
7. Saisissez les détails suivants pour l'application de connecteur :
   - Dans le champ **Audience**, saisissez `https://saml.cloud.us`.
   - Dans le champ **Destinataire**, saisissez `https://saml.cloud.us/saml/acs`.
   - Dans le champ du validateur d'URL ACS, saisissez `https://saml.cloud.us/saml/acs`.
   - Dans le champ de l'URL ACS, saisissez `https://saml.cloud.us/saml/acs`.
   - Dans le champ de l'URL de déconnexion unique, saisissez `https://saml.cloud.us/saml/logout/callback`.
8. Ajoutez vos attributs SAML personnalisés en tant que valeurs de paramètre dans l'application :

CRÉER CE CHAMP	ATTRIBUER CET ATTRIBUT PERSONNALISÉ
cip_sid	cip_sid ou votre attribut SID existant
cip_upn	cip_upn ou votre attribut UPN existant
cip_oid	cip_oid ou votre attribut OID existant
cip_email	cip_email ou votre attribut d'e-mail existant

9. Ajoutez vos abonnés Workspace en tant qu'utilisateurs pour leur permettre d'accéder à l'application.

Ajouter les métadonnées du fournisseur SAML à Citrix Cloud™ Government

1. Acquérez les métadonnées SAML de votre fournisseur SAML. L'image suivante est un exemple de ce à quoi ce fichier pourrait ressembler :



2. Dans l'écran **Configurer SAML** de Citrix Cloud Government, entrez les valeurs suivantes à partir du fichier de métadonnées de votre fournisseur SAML :

   - Dans **ID d'entité**, entrez la valeur **entityID** de l'élément **EntityDescriptor** dans les métadonnées.

   - Dans **Signer la demande d'authentification**, sélectionnez **Oui** pour permettre à Citrix Cloud Government de signer les demandes d'authentification, certifiant qu'elles proviennent de Citrix Cloud Government et non d'un acteur malveillant. Sélectionnez **Non** si vous préférez ajouter l'URL ACS de Citrix à une liste d'autorisation que votre fournisseur SAML utilise pour publier les réponses SAML en toute sécurité.

   - Dans **URL du service SSO**, entrez l'URL du mécanisme de liaison que vous souhaitez utiliser. Vous pouvez utiliser la liaison HTTP-POST ou HTTP-Redirect. Dans le fichier de métadonnées, localisez les éléments **SingleSignOnService** avec des valeurs de liaison **HTTP-POST** ou **HTTP-Redirect**.

   - Dans **Mécanisme de liaison**, sélectionnez le mécanisme qui correspond à la liaison de l'URL du service SSO que vous avez choisie dans le fichier de métadonnées.

   - Dans **Réponse SAML**, sélectionnez la méthode de signature utilisée par votre fournisseur SAML pour la Réponse SAML et l'Assertion SAML. Par défaut, Citrix Cloud Government rejette toute réponse qui n'est pas signée comme spécifié dans ce champ.

3. Dans la console d'administration de votre fournisseur SAML, effectuez les actions suivantes :

   - Sélectionnez **SHA-256** pour l'algorithme de signature SAML.
   - Téléchargez le certificat X.509 en tant que fichier PEM.

4. Dans l'écran **Configurer SAML** de Citrix Cloud Government, sélectionnez **Charger un fichier** et sélectionnez le fichier PEM que vous avez téléchargé à l'étape précédente.
5. Sélectionnez **Continuer** pour terminer le chargement.
6. Dans **Contexte d'authentification**, sélectionnez le contexte que vous souhaitez utiliser et la rigueur avec laquelle vous souhaitez que Citrix Cloud applique ce contexte. Sélectionnez **Minimum** pour demander l'authentification dans le contexte sélectionné sans appliquer l'authentification dans ce contexte. Sélectionnez **Exact** pour demander l'authentification dans le contexte sélectionné et appliquer l'authentification uniquement dans ce contexte. Si votre

fournisseur SAML ne prend pas en charge les contextes d'authentification ou si vous choisissez de ne pas les utiliser, sélectionnez **Non spécifié** et **Minimum**.

7. Dans **URL de déconnexion**, localisez l'élément **SingleSignOnService** avec la liaison HTTP-Redirect dans le fichier de métadonnées de votre fournisseur SAML et saisissez l'URL.
8. Vérifiez que les valeurs d'attribut de nom par défaut suivantes dans Citrix Cloud Government correspondent aux valeurs d'attribut correspondantes dans la console d'administration de votre fournisseur SAML. Si votre fournisseur SAML a des valeurs différentes, vous pouvez modifier ces valeurs dans Citrix Cloud pour vous assurer qu'elles correspondent à celles de votre fournisseur SAML.

    - **Nom de l'attribut pour le nom d'affichage de l'utilisateur** : `displayName`
    - **Nom de l'attribut pour le prénom de l'utilisateur** : `givenName`
    - **Nom de l'attribut pour le nom de famille de l'utilisateur** : `familyName`

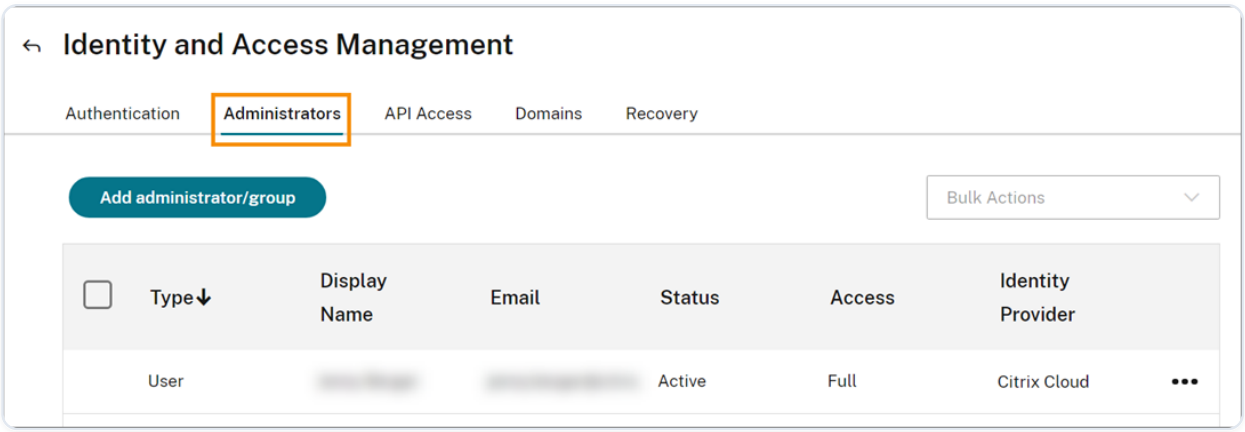
9. Dans Citrix Cloud, saisissez les attributs SAML personnalisés de votre fournisseur SAML :

    - Dans **Nom de l'attribut pour l'identificateur de sécurité (SID)**, saisissez le nom de votre attribut SID personnalisé. La valeur par défaut est `cip_sid`.
    - Dans **Nom de l'attribut pour le nom d'utilisateur principal (UPN)**, saisissez le nom de votre attribut UPN personnalisé. La valeur par défaut est `cip_upn`.
    - Dans **Nom d'attribut pour l'e-mail**, entrez le nom de votre attribut d'e-mail personnalisé. La valeur par défaut est `cip_email`.
    - Dans **Nom d'attribut pour l'identificateur d'objet AD (OID)**, entrez le nom de votre attribut OID personnalisé. La valeur par défaut est `cip_oid`.

10. Sélectionnez **Tester et terminer** pour vérifier que vous avez configuré la connexion avec succès.

Ajouter des administrateurs à Citrix Cloud Government depuis AD

1. Dans Citrix Cloud Government, depuis la page **Gestion des identités et des accès**, sélectionnez l'onglet **Administrateurs**.



2. Dans **Détails de l'administrateur**, sélectionnez **Active Directory**, puis sélectionnez le domaine que vous souhaitez utiliser.
3. Dans **Rechercher un groupe à ajouter**, commencez à taper le nom du groupe que vous souhaitez ajouter dans la zone de recherche. Lorsqu'il apparaît, cliquez sur le signe plus (+) pour sélectionner le groupe.
4. Sélectionnez **Suivant**.
5. Sélectionnez les autorisations d'accès personnalisées ou les rôles que vous souhaitez attribuer au groupe. Sélectionnez **Suivant**.
6. Vérifiez les détails de l'administrateur. Sélectionnez **Retour** pour apporter des modifications.
7. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

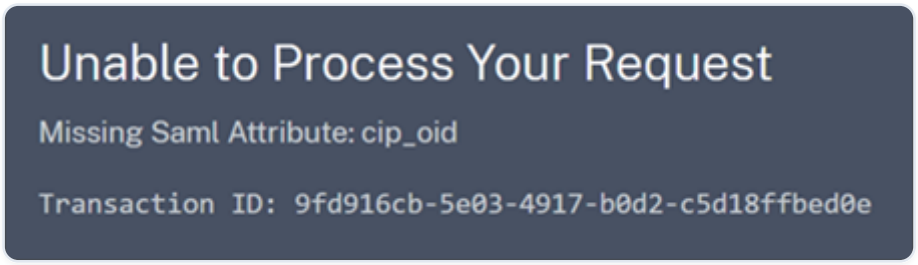
Activer l'authentification SAML pour les espaces de travail

1. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**.
2. Sélectionnez l'onglet **Authentification**
3. Sélectionnez **SAML 2.0**.

Dépannage

Erreurs d'attribut

Des erreurs d'attribut peuvent survenir si les attributs requis dans votre configuration SAML ne sont pas encodés correctement. Lorsqu'une erreur d'attribut se produit, Citrix Cloud Government affiche un message d'erreur qui inclut l'attribut défectueux.



Pour résoudre ce type d'erreur, assurez-vous que ces attributs sont encodés comme décrit dans le tableau suivant.

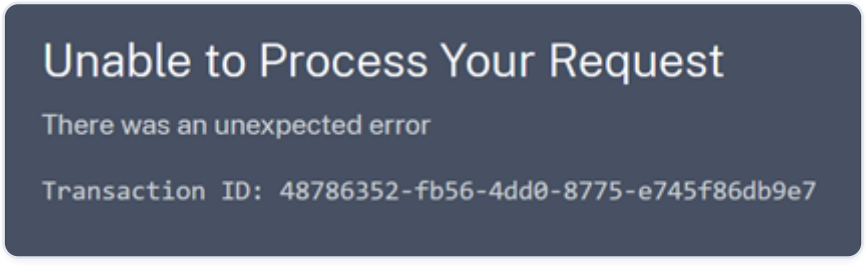
ATTRIBUT	ENCODAGE
cip_email	Doit être au format String (`user@domain`)
cip_oid	Doit être au format Base64 ou String
cip_sid	Doit être au format Base64 ou String
cip_upn	Doit être au format String (`user@domain`)

Erreurs inattendues

Citrix Cloud Government peut rencontrer une erreur inattendue lorsque :

- Un utilisateur démarre une requête SAML à l'aide d'un flux initié par l'IdP. Par exemple, la requête est effectuée en sélectionnant une vignette via le portail d'applications du fournisseur d'identité au lieu de naviguer directement vers l'URL de l'espace de travail (`customer.cloud.us`).
- Le certificat SAML est invalide ou a expiré.
- Le contexte d'authentification est invalide.
- L'assertion SAML et la signature de la réponse ne correspondent pas.

Lorsque cette erreur se produit, Citrix Cloud Government affiche un message d'erreur générique.



Si cette erreur résulte de la navigation vers Citrix Cloud Government via le portail d'applications d'un fournisseur d'identité, vous pouvez utiliser la solution de contournement suivante :

1. Créez une application de signet dans le portail d'applications du fournisseur d'identité qui référence l'URL de votre espace de travail (par exemple, `https://customer.cloud.us`).
2. Attribuez les utilisateurs à l'application SAML et à l'application de signet.
3. Modifiez les paramètres de visibilité de l'application SAML et de l'application de signet afin que l'application de signet soit visible et que l'application SAML soit masquée dans le portail d'applications.
4. Désactivez le paramètre Prompt=Login pour supprimer d'autres invites de mot de passe.

Gérer

Gérer Citrix Cloud™ Government

Citrix Cloud Government comprend les fonctionnalités d'administration suivantes :

- Inviter des administrateurs et déléguer l'accès aux services cloud
- Attribuer un emplacement de ressources principal
- Attribuer des utilisateurs aux offres de services dans la bibliothèque
- Surveiller les notifications de service
- Afficher le journal système des événements qui se sont produits dans Citrix Cloud Government

Administrateurs

Pendant le processus d'intégration du compte, un administrateur initial est créé. L'administrateur peut ensuite inviter d'autres administrateurs à rejoindre Citrix Cloud Government. Les nouveaux administrateurs utilisent leurs informations d'identification de compte Citrix Cloud Government existantes ou configurent un nouveau compte si nécessaire. Vous pouvez également affiner les autorisations d'accès des administrateurs que vous invitez. Les autorisations vous permettent de définir un accès aligné sur le rôle de l'administrateur dans votre organisation.

Ajouter des administrateurs et modifier les autorisations

Pour inviter d'autres administrateurs et affiner leur accès à Citrix Cloud Government, consultez Ajouter des administrateurs à un compte Citrix Cloud Government.

Supprimer des administrateurs

Vous pouvez supprimer des administrateurs de votre compte Citrix Cloud Government sous l'onglet **Administrateurs**. Lorsque vous supprimez un administrateur, il ne peut plus se connecter à Citrix Cloud Government. Si un administrateur est connecté au moment où vous supprimez le compte, l'administrateur reste actif pendant une minute. Finalement, l'accès à Citrix Cloud Government est refusé.

> **Remarque :**

- S'il n'y a qu'un seul administrateur dans le compte, vous ne pouvez pas le supprimer. Citrix Cloud Government exige au moins un administrateur pour chaque compte client.
- Les Cloud Connectors ne sont pas liés aux comptes administrateur. Ainsi, les Cloud Connectors continuent de fonctionner même si vous supprimez l'administrateur qui les a installés.

Abonnés

Vous pouvez ajouter des abonnés aux offres de la bibliothèque à l'aide de comptes individuels ou de groupes Active Directory. L'utilisation de groupes Active Directory ne nécessite pas de gestion via Citrix Cloud Government après avoir attribué le groupe à une offre.

Le processus d'attribution d'utilisateurs aux offres de la bibliothèque est le même pour Citrix Cloud Government et Citrix Cloud commercial. Pour obtenir des instructions, consultez Attribuer des utilisateurs et des groupes à des offres de service à l'aide de la bibliothèque.

Important :

Si vous utilisez un StoreFront local avec Citrix DaaS™, n'utilisez pas de bibliothèque pour attribuer des ressources lors de la création de groupes de mise à disposition. Utilisez plutôt Studio pour attribuer des ressources aux utilisateurs. Si vous utilisez une bibliothèque dans ce scénario, les ressources risquent de ne pas être énumérées aux utilisateurs.

Lorsque vous créez un groupe de mise à disposition dans Studio, sur la page Utilisateurs, ne sélectionnez pas **Laisser la gestion des utilisateurs à Citrix Cloud**. Sélectionnez plutôt une autre option (**Autoriser tous les utilisateurs authentifiés à utiliser ce groupe de mise à disposition** ou **Restreindre l'utilisation de ce groupe de mise à disposition aux utilisateurs suivants**).

Lorsqu'un administrateur supprime un abonné individuel ou un groupe d'abonnés d'une offre, ces abonnés ne peuvent plus accéder au service. Pour plus d'informations sur la suppression d'abonnés de services spécifiques, reportez-vous à la documentation du service sur le site Web Documentation produit Citrix.

Emplacements de ressources principaux

Un emplacement de ressources principal est un emplacement de ressources que vous choisissez comme « préféré » pour les communications entre votre domaine et Citrix Cloud Government. L'emplacement de ressources que vous sélectionnez comme « principal » contient des Cloud Connectors qui offrent les meilleures performances et la meilleure connectivité à votre domaine. L'emplacement de ressources permet à vos utilisateurs de se connecter rapidement à Citrix Cloud Government.

Le processus de sélection d'un emplacement de ressources principal est le même pour Citrix Cloud Government et Citrix Cloud commercial. Pour plus d'informations, consultez Sélectionner un emplacement de ressources principal.

Notifications

Les notifications fournissent des informations sur les problèmes ou les événements susceptibles d'intéresser les administrateurs, tels que les nouvelles fonctionnalités de Citrix Cloud Government. Les notifications fournissent également toute information sur les problèmes liés à une machine dans un emplacement de ressources. Les notifications peuvent provenir de n'importe quel service au sein de Citrix Cloud Government.

La gestion des notifications est la même dans Citrix Cloud Government et Citrix Cloud commercial. Pour plus d'informations sur les notifications, consultez Notifications.

Journal système

Le Journal système affiche une liste d'événements horodatés qui se sont produits dans Citrix Cloud Government. Vous pouvez exporter ces modifications sous forme de fichier CSV pour répondre aux exigences de conformité réglementaire de votre organisation ou pour soutenir l'analyse de sécurité.

Les fonctions du Journal système sont les mêmes dans Citrix Cloud Government et Citrix Cloud commercial, avec quelques limitations importantes. Pour plus d'informations, consultez Journal système

Gérer les administrateurs de Citrix Cloud™ Government

Les administrateurs sont gérés depuis la console Citrix Cloud Government. Selon le fournisseur d'identité que vous utilisez pour l'authentification, vous pouvez ajouter des administrateurs individuellement ou en utilisant des groupes.

Tous les administrateurs sont tenus d'utiliser des jetons comme deuxième facteur d'authentification lors de la connexion à Citrix Cloud. Après avoir ajouté un administrateur, celui-ci peut inscrire son appareil à l'authentification multifacteur. De plus, générez des jetons à l'aide de toute application qui suit la norme Time-Based One-Time Password, telle que Citrix SSO.

Par défaut, les nouveaux administrateurs disposent des autorisations d'accès complet à toutes les fonctions du compte Citrix Cloud Government. Consultez Configurer les autorisations d'administrateur dans cet article pour savoir comment déléguer l'administration du compte.

Ajouter de nouveaux administrateurs

Citrix Cloud prend en charge les fournisseurs d'identité suivants pour l'authentification des administrateurs :

- Fournisseur d'identité Citrix : Le fournisseur d'identité par défaut dans Citrix Cloud. Prend en charge l'ajout d'administrateurs individuels uniquement.
- Microsoft Entra ID : Prend en charge l'ajout d'administrateurs individuellement et via des groupes AAD. Les administrateurs des groupes AAD sont limités à l'accès à Citrix DaaS uniquement. Pour plus d'informations, consultez Gérer les groupes d'administrateurs.
- SAML 2.0 : Prend en charge l'ajout d'administrateurs via des groupes AD uniquement. Pour plus d'informations, consultez Connecter SAML en tant que fournisseur d'identité à Citrix Cloud.

L'ajout de nouveaux administrateurs utilise le flux de travail suivant :

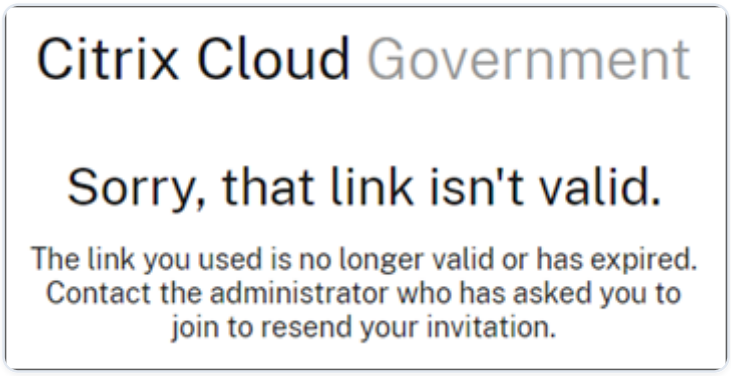
1. Sélectionnez le fournisseur d'identité que vous souhaitez utiliser pour l'authentification des administrateurs.
2. Selon le fournisseur d'identité, invitez des administrateurs individuels ou sélectionnez les groupes auxquels les administrateurs appartiennent.
3. Spécifiez les autorisations d'accès qui correspondent aux rôles des administrateurs dans votre organisation. Pour plus d'informations, consultez configurer les autorisations d'administrateur dans cet article.

Inviter des administrateurs individuels

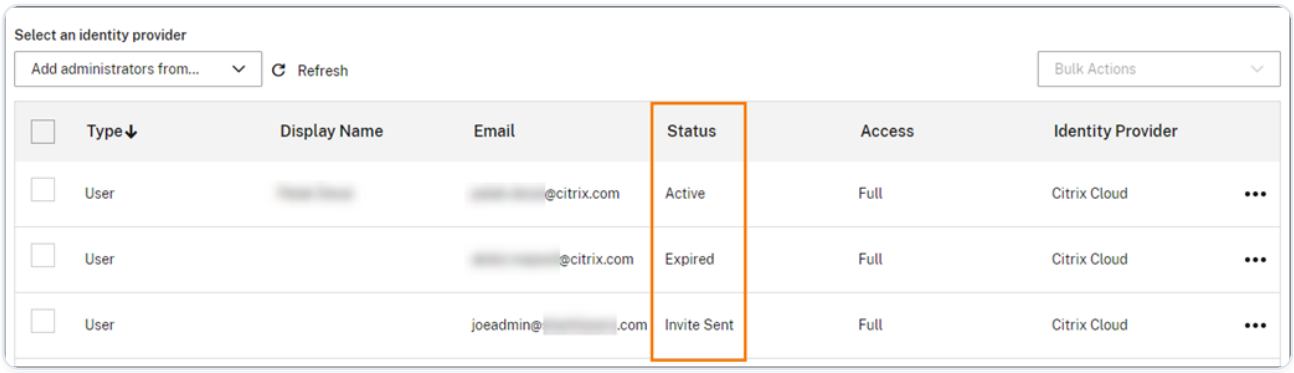
L'ajout d'administrateurs individuels implique de les inviter à rejoindre votre compte Citrix Cloud Government. Lorsque vous ajoutez un administrateur, Citrix lui envoie un e-mail d'invitation. Avant de pouvoir se connecter, l'administrateur doit accepter l'invitation. Les administrateurs que vous

ajoutez via des groupes ne reçoivent pas d'invitations et peuvent se connecter immédiatement après leur ajout.

Les e-mails d'invitation sont envoyés depuis `cloud@citrix.com` et expliquent comment accéder au compte. L'e-mail est valide pendant cinq jours consécutifs à compter du jour de l'envoi. Après cinq jours, le lien d'invitation expire. Si l'administrateur invité utilise le lien expiré, Citrix Cloud Government affiche un message indiquant que le lien n'est pas valide.



Citrix Cloud Government affiche également le statut de l'invitation afin que vous puissiez voir si l'administrateur l'a acceptée et s'est connecté.



Pour inviter un administrateur

1. Après vous être connecté à Citrix Cloud Government, sélectionnez **Gestion des identités et des accès** dans le menu.
2. Sur la page **Gestion des identités et des accès**, sélectionnez **Administrateurs**. La console affiche tous les administrateurs actuels du compte.
3. Sélectionnez **Ajouter un administrateur/groupe**.
4. Dans **Détails de l'administrateur**, sélectionnez le fournisseur d'identité que vous souhaitez utiliser. Si vous utilisez Microsoft Entra ID, Citrix Cloud peut vous inviter à vous connecter d'abord.
5. Si **Citrix Identity** est sélectionné, saisissez l'adresse e-mail de l'utilisateur, puis sélectionnez **Suivant**.

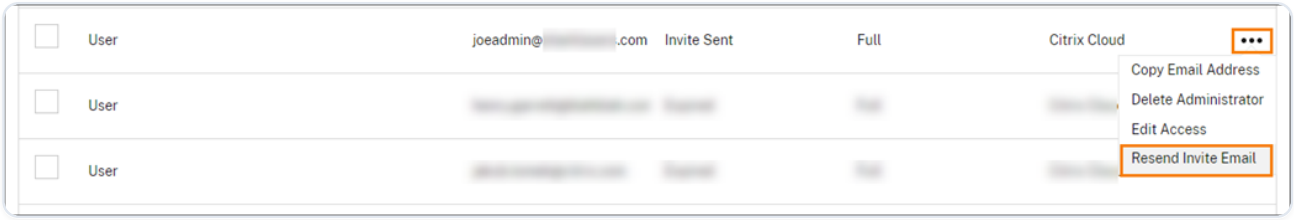
6. Si **Microsoft Entra ID** est sélectionné, saisissez le nom de l'utilisateur que vous souhaitez ajouter, puis cliquez sur **Suivant**. L'invitation d'utilisateurs invités de Microsoft Entra ID n'est pas prise en charge.
7. Dans **Définir l'accès**, configurez les autorisations appropriées pour l'administrateur. L'**accès complet** (sélectionné par défaut) permet de contrôler toutes les fonctions et services souscrits de Citrix Cloud Government. L'**accès personnalisé** permet de contrôler les fonctions et services que vous sélectionnez.
8. Vérifiez les détails de l'administrateur. Sélectionnez **Retour** pour apporter des modifications.
9. Sélectionnez **Envoyer l'invitation**. Citrix Cloud envoie une invitation à l'utilisateur que vous avez spécifié et ajoute l'administrateur à la liste.

Renvoyer une invitation

Pour renvoyer l'invitation, sélectionnez **Renvoyer l'e-mail d'invitation** dans le menu en forme de points de suspension situé à l'extrême droite de la console. Le renvoi d'une invitation n'affecte pas le délai de cinq jours avant l'expiration de l'invitation.

Renvoyer une invitation avec un nouveau lien de connexion

Si l'e-mail d'invitation original expire et que vous souhaitez en envoyer un nouveau à l'administrateur. Supprimez l'administrateur de Citrix Cloud Government, puis invitez-le à nouveau.



Accepter une invitation

Si vous êtes invité à un compte Citrix Cloud Government, Citrix Cloud Government vous envoie un e-mail qui inclut l'ID d'organisation et le nom du client du compte.

Pour accepter l'invitation, cliquez sur **Se connecter**. Ensuite, une fenêtre de navigateur s'ouvre. Si vous n'avez pas encore de compte Citrix Cloud Government, le navigateur affiche une page où vous pouvez créer votre mot de passe. Si vous avez déjà un compte, Citrix Cloud Government vous invite à utiliser votre mot de passe existant pour vous connecter.

Ajouter des groupes d'administrateurs

Vous pouvez ajouter des administrateurs à l'aide de groupes AD (pour l'authentification SAML) ou de groupes Microsoft Entra ID (pour l'authentification Microsoft Entra ID). Ces administrateurs ne peuvent gérer que Citrix DaaS (anciennement le service Citrix Virtual Apps and Desktops™). Pour plus d'informations, consultez les articles suivants :

- Gérer les groupes d'administrateurs
- Connecter SAML en tant que fournisseur d'identité à Citrix Cloud Government

Configurer les autorisations d'administrateur

Lorsque vous ajoutez des administrateurs à votre compte Citrix Cloud Government, vous devrez peut-être leur attribuer différents niveaux d'accès, tels que :

- Accès au support technique pour Citrix DaaS™
- Accès pour gérer un ou plusieurs services cloud spécifiques
- Accès pour gérer des fonctions spécifiques de Citrix Cloud Government, telles que la Bibliothèque ou les Emplacements de ressources.

Avec l'administration déléguée dans Citrix Cloud Government, vous pouvez configurer les autorisations d'accès pour tous vos administrateurs. Les autorisations sont définies en fonction de leur rôle dans votre organisation.

Autorisations de la console

Utilisez les autorisations suivantes pour configurer un accès personnalisé à la console de gestion Citrix Cloud Government :

- **Authentification :** Accorde l'accès à l'onglet **Gestion des identités et des accès > Authentification**. Les administrateurs peuvent créer et supprimer des connexions de fournisseurs d'identité et modifier l'URL de connexion de l'administrateur, le cas échéant. Pour gérer d'autres aspects des fournisseurs d'identité, tels que l'authentification de l'espace de travail, des autorisations supplémentaires sont requises.
- **Domaines :** Accorde l'accès à l'onglet **Gestion des identités et des accès > Domaines**. Les administrateurs peuvent ajouter un domaine Active Directory en téléchargeant le logiciel Citrix Cloud Connector™ à partir de cet onglet et en l'installant sur un serveur du domaine.
- **Bibliothèque :** Accorde l'accès à la page de la console **Bibliothèque**.
- **Notifications :** Accorde l'accès à la page de la console **Notifications**. Les administrateurs peuvent afficher et ignorer les notifications Citrix Cloud.

- **Emplacements de ressources :** Accorde l'accès à la page de la console **Emplacements de ressources**. Les administrateurs peuvent ajouter de nouveaux emplacements de ressources. Ils peuvent également ajouter des connecteurs et gérer les mises à jour des connecteurs.
- **Journal système :** Accorde l'accès à la page de la console **Journal système**. Les administrateurs peuvent afficher les événements du journal système et exporter les événements vers un fichier CSV.
- **Configuration de l'espace de travail :** Accorde l'accès à la page de la console **Configuration de l'espace de travail**. Les administrateurs peuvent modifier les méthodes d'authentification, personnaliser l'apparence et le comportement de l'espace de travail, activer et désactiver les services, et configurer l'agrégation de sites. Pour plus d'informations, consultez la documentation produit de Citrix Workspace.

Pour modifier les autorisations existantes

Seuls les administrateurs Citrix disposant d'un accès complet peuvent définir les autorisations d'accès pour les autres administrateurs.

1. Connectez-vous à Citrix Cloud Government à l'adresse https://citrix.cloud.us.
2. Cliquez sur le bouton de menu dans le coin supérieur gauche de la page et sélectionnez **Gestion des identités et des accès**.
3. Cliquez sur l'onglet **Administrateurs**.
4. Localisez l'administrateur que vous souhaitez gérer, cliquez sur le bouton des points de suspension, puis sélectionnez **Modifier l'accès**.
5. Sélectionnez **Accès personnalisé**.
6. Sélectionnez ou désélectionnez chaque autorisation selon les besoins.
7. Cliquez sur **Enregistrer**.

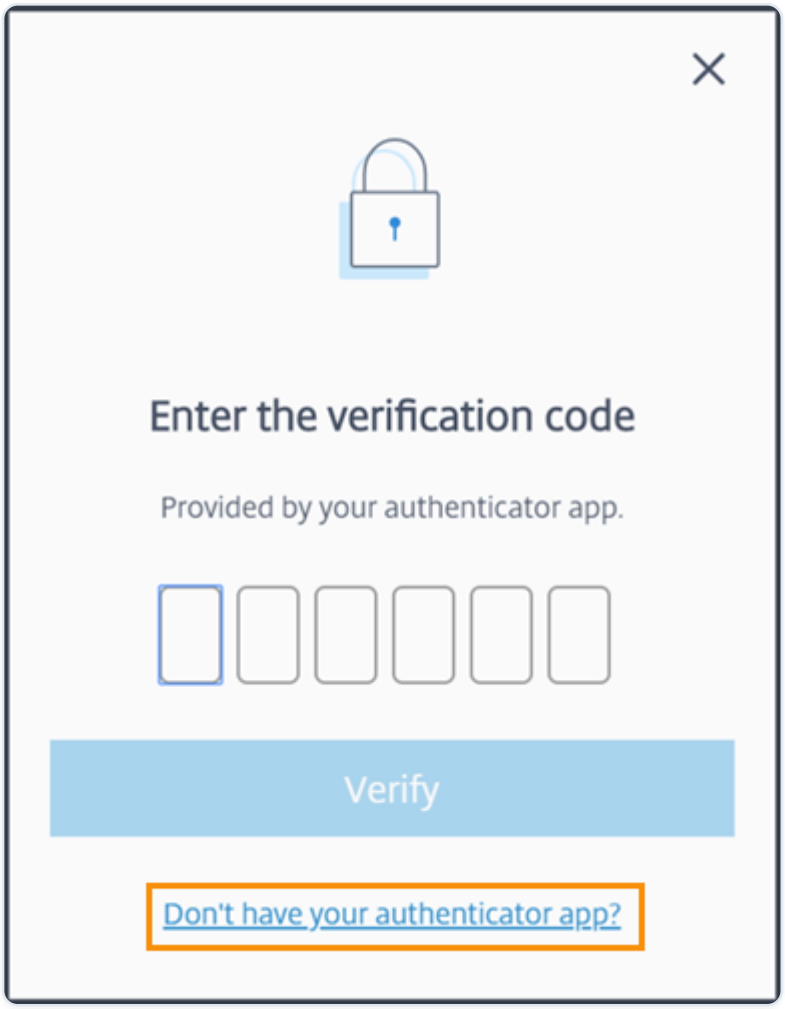
Changer votre appareil pour l'authentification multifacteur

Si vous perdez votre appareil enregistré, souhaitez utiliser un appareil différent avec Citrix Cloud Government. Réinitialisez votre application d'authentification, vous pouvez vous réinscrire à l'authentification multifacteur.

> **Remarques**

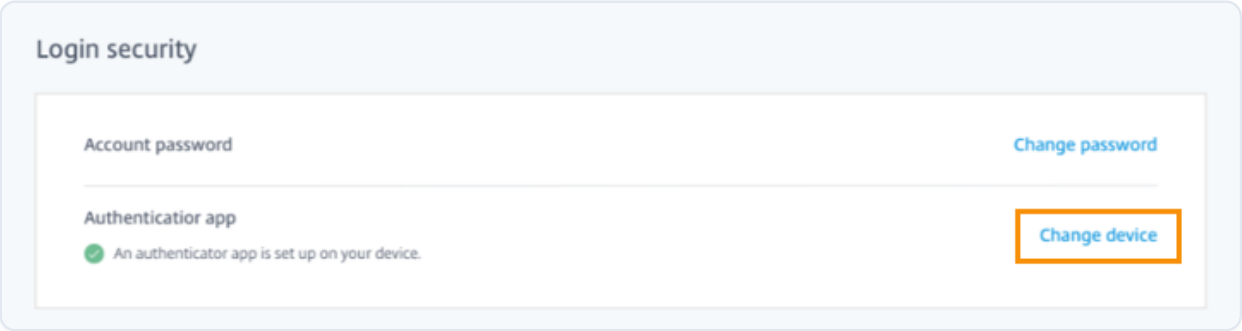
- Le changement de votre appareil supprime l'enregistrement actuel de l'appareil et génère une nouvelle clé d'application d'authentification.
- Si vous vous réinscrivez avec la même application d'authentification que lors de votre inscription initiale, supprimez l'entrée Citrix Cloud Government de votre application d'authentification avant de vous réinscrire. Les codes affichés dans cette entrée ne fonctionneront plus une fois la réinscription terminée. Si vous ne supprimez pas cette entrée avant ou après la réinscription, votre application d'authentification affichera deux entrées Citrix Cloud Government avec des codes différents. Ces entrées peuvent entraîner une confusion lors de la connexion à Citrix Cloud Government.
- Si vous vous réinscrivez avec un nouvel appareil et que vous n'avez pas d'application d'authentification, téléchargez-en et installez-en une depuis le magasin d'applications de votre appareil. Pour une expérience plus fluide, Citrix recommande d'installer une application d'authentification avant de réinscrire votre appareil.

1. Connectez-vous à Citrix Cloud Government et saisissez le code de votre application d'authentification.



Si vous n'avez pas votre application d'authentification, cliquez sur **Vous n'avez pas votre application d'authentification ?** et sélectionnez une méthode de récupération pour vous aider à vous connecter. Selon la méthode de récupération sélectionnée, saisissez le code de récupération que vous avez reçu ou un code de sauvegarde inutilisé, puis sélectionnez **Vérifier**.

2. Si vous êtes administrateur de plusieurs organisations clientes, sélectionnez n'importe quelle organisation cliente.
3. Dans le menu supérieur droit, sélectionnez **Mon profil**.
4. Dans **l'application d'authentification**, sélectionnez **Changer d'appareil**.

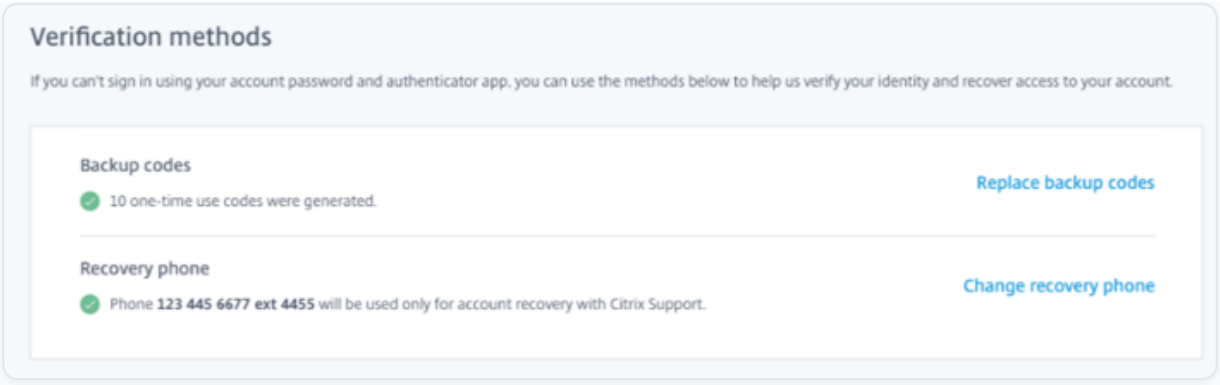


5. Lorsque vous êtes invité à confirmer le changement d'appareil, sélectionnez **Oui, changer d'appareil**.
6. Vérifiez votre identité en saisissant un code de vérification de votre application d'authentification. Si vous n'avez pas d'application d'authentification, sélectionnez **Vous n'avez pas votre application d'authentification ?** et sélectionnez une méthode de récupération. Selon la méthode de récupération que vous sélectionnez, saisissez le code de vérification ou le code de récupération que vous recevez, ou un code de sauvegarde inutilisé. Sélectionnez **Vérifier**.
7. Si vous utilisez l'appareil que vous avez initialement enregistré et votre application d'authentification d'origine, supprimez l'entrée Citrix Cloud Government existante de votre application d'authentification.
8. Si vous enregistrez un nouvel appareil et que vous n'avez pas d'application d'authentification, téléchargez-en une depuis la boutique d'applications de votre appareil.
9. Depuis votre application d'authentification, scannez le code QR avec votre appareil ou saisissez la clé manuellement.
10. Saisissez le code de vérification à 6 chiffres de votre application d'authentification et sélectionnez **Vérifier le code**.

Gérer vos méthodes de vérification

Important :

Pour garantir la sécurité de votre compte Citrix Cloud Government, maintenez vos méthodes de vérification à jour avec des informations précises. Si vous perdez l'accès à votre application d'authentification, ces méthodes de vérification sont le seul moyen de récupérer l'accès à votre compte.



Générer de nouveaux codes de sauvegarde

Si vous perdez ou avez besoin de générer davantage de codes de sauvegarde à usage unique, vous pouvez générer un nouvel ensemble de codes de sauvegarde à tout moment. Après avoir généré de nouveaux codes de sauvegarde, assurez-vous de les stocker dans un endroit sûr.

1. Connectez-vous à Citrix Cloud Government et saisissez le code de votre application d'authentification.
2. Si vous êtes administrateur de plusieurs organisations clientes, sélectionnez n'importe quelle organisation cliente.
3. Dans le menu en haut à droite, sélectionnez **Mon profil**.
4. Sous **Méthodes de vérification**, dans **Codes de secours**, sélectionnez **Remplacer les codes de secours**.
5. Vérifiez votre identité en saisissant un code de vérification depuis votre application d'authentification.
6. Lorsque vous êtes invité à remplacer votre code de secours, sélectionnez **Oui, remplacer**. Citrix Cloud Government génère et affiche un nouvel ensemble de codes de secours.
7. Sélectionnez **Télécharger les codes** pour télécharger vos nouveaux codes sous forme de fichier texte. Ensuite, sélectionnez **J'ai enregistré ces codes** et sélectionnez **Fermer**.

Modifier votre numéro de téléphone de récupération

1. Connectez-vous à Citrix Cloud Government et saisissez le code de votre application d'authentification.
2. Si vous êtes administrateur de plusieurs organisations clientes, sélectionnez l'organisation cliente à partir de laquelle vous vous êtes initialement inscrit à l'authentification multifacteur.
3. Dans le menu en haut à droite, sélectionnez **Mon profil**.
4. Sous **Méthodes de vérification**, dans **Téléphone de récupération**, sélectionnez **Modifier le téléphone de récupération**.
5. Saisissez le nouveau numéro de téléphone que vous souhaitez utiliser, puis sélectionnez **Enregistrer**.

Journal système

Le journal système affiche une liste horodatée des événements survenus dans Citrix Cloud™ Government. Vous pouvez exporter ces modifications sous forme de fichier CSV pour répondre aux exigences de conformité réglementaire de votre organisation ou pour prendre en charge l'analyse de sécurité.

Pour afficher le journal système, sélectionnez **Journal système** dans le menu Citrix Cloud Government.

Menu Citrix Cloud avec Journal système mis en surbrillance(/en-us/citrix-cloud-government/media/system-log-menu.png)

Pour plus d'informations sur la rétention des données du journal système, consultez Rétention des données dans cet article.

Limitations

Bien que le journal système fonctionne de la même manière dans Citrix Cloud Government et Citrix Cloud commercial, les éléments suivants ne sont pas disponibles pour une utilisation avec Citrix Cloud Government :

- API SystemLog
- Module complémentaire Splunk pour le journal système

Événements enregistrés

Le journal système capture les événements pour certaines opérations de la plate-forme Citrix Cloud Government et des services cloud. Pour une liste complète de ces événements et des descriptions des données capturées, consultez Référence des événements du journal système.

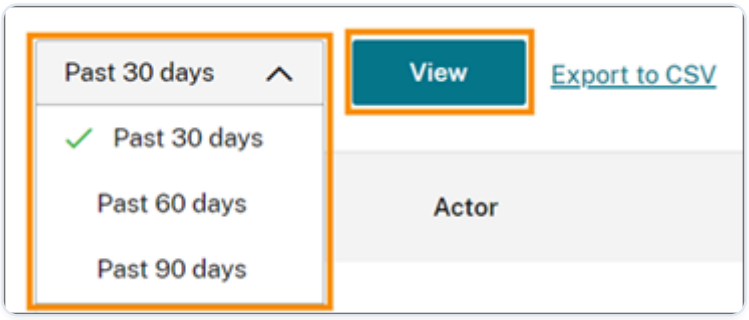
> **Remarque :**
>
> La Référence des événements du journal système inclut les événements liés à la plate-forme et aux services qui se produisent dans Citrix Cloud commercial. Les événements générés dans Citrix Cloud Government sont un sous-ensemble des événements générés dans Citrix Cloud commercial. Pour les notifications concernant les nouveaux événements pris en charge dans Citrix Cloud Government, consultez Nouveautés de Citrix Cloud Government.

> Le journal système affiche par défaut les événements survenus au cours des 30 derniers jours, jusqu'à un maximum de 90 jours. Les événements les plus récents sont affichés en premier. Journal système avec entrée développée(/en-us/citrix-cloud-government/media/system-log-list.png)

La liste affichée comprend les informations suivantes :

- Date et heure (UTC) de l'événement.
- Acteur qui a initié l'événement, tel qu'un administrateur ou un principal de service. Les entrées avec l'acteur **CwcSystem** indiquent que Citrix Cloud Government a effectué l'opération.
- Brève description de l'événement, telle que la modification d'un administrateur ou la création d'un nouveau principal de service.
- Cible de l'événement. La cible est l'objet système qui a été impacté ou modifié à la suite de l'événement. Par exemple, un utilisateur qui a été ajouté en tant qu'administrateur.

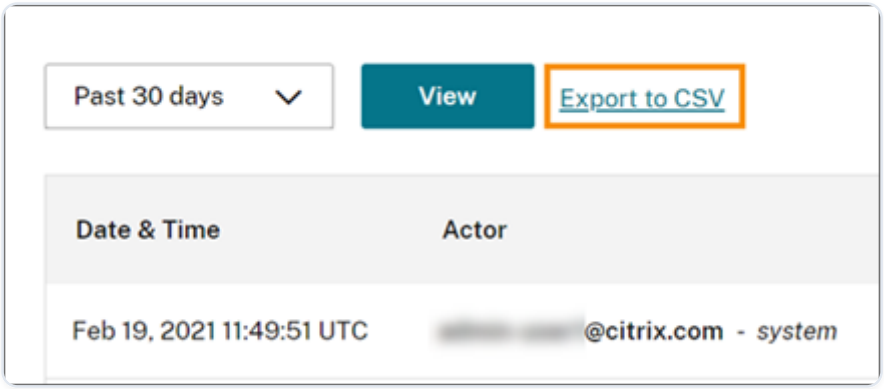
Pour afficher les événements survenus au cours des 90 derniers jours, filtrez la liste en sélectionnant la période que vous souhaitez afficher, puis sélectionnez **Afficher**.



Exporter les événements

Vous pouvez exporter un fichier CSV des événements du journal système survenus au cours des 90 derniers jours. Le nom du fichier téléchargé suit le format `SystemLog-CustomerName-OrgID-DateTimeStamp.csv`.

1. Dans le menu Citrix Cloud Government, sélectionnez **Journal système**.
2. Si nécessaire, filtrez la liste pour afficher la période pour laquelle vous souhaitez exporter les événements.
3. Sélectionnez **Exporter au format CSV** et enregistrez le fichier.



Le fichier CSV inclut les informations suivantes :

- Horodatage UTC de chaque événement
- Détails de l'acteur qui a initié l'événement, y compris le nom et l'ID de l'acteur.
- Détails de l'événement, tels que le type d'événement et le texte de l'événement
- Détails de la cible de l'événement, tels que l'ID de la cible, le nom de l'administrateur ou un principal de service.

Conservation des données

Citrix partage la responsabilité avec vous, le client, de la conservation des données du journal système que Citrix Cloud Government capture.

Citrix® conserve les enregistrements du journal système pendant 90 jours après l'enregistrement des événements.

Vous êtes responsable du téléchargement des enregistrements du journal système que vous souhaitez conserver pour répondre aux exigences de conformité de votre organisation et du stockage de ces enregistrements dans une solution de stockage à long terme.

Kits de développement logiciel (SDK)

Le **SDK PowerShell distant de Citrix DaaS™** automatise les tâches complexes et répétitives. Il fournit le mécanisme pour configurer et gérer l'environnement Citrix DaaS sans avoir à utiliser l'interface utilisateur de Studio.

Exigences

PowerShell 3.0 ou version ultérieure est disponible sur la machine.

Installer ou supprimer le SDK PowerShell distant

Pour installer le SDK PowerShell distant à utiliser avec Citrix Cloud™ Government :

1. Téléchargez le programme d'installation : https://download.apps.cloud.com/CitrixPoshSdk.exe.
2. Exécutez la commande `CitrixPoshSdk.exe EnvironmentName=USGovernment`. Cette commande permet au SDK de s'exécuter par défaut dans le contexte de Citrix Cloud Government.

> **Remarque :**
>
> Vous pouvez également exécuter le programme d'installation du SDK et suivre les boîtes de dialogue pour terminer l'installation. Cependant, vous devez spécifier l'environnement Citrix Cloud Government lorsque vous vous authentifiez à l'aide de la cmdlet Get-XdAuthentication. Consultez Pour exécuter le SDK PowerShell distant dans cet article.

Les journaux d'installation sont créés dans %TEMP%\CitrixLogs\CitrixPoshSdk. Les journaux peuvent aider à résoudre les problèmes d'installation.

Pour désinstaller le SDK PowerShell distant :

1. Dans la fonctionnalité Windows de suppression ou de modification de programmes, sélectionnez **Citrix DaaS Remote PowerShell SDK**.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Désinstaller**.
3. Suivez la boîte de dialogue.

Pour exécuter le SDK PowerShell distant

Exécutez le SDK PowerShell distant sur un ordinateur joint à un domaine au sein de cet emplacement de ressources :

1. Ouvrez une invite de commande PowerShell. Vous n'avez pas besoin de l'exécuter en tant qu'administrateur.
2. Ajoutez les snap-ins Citrix® : `asnp citrix.*`.
3. Vous pouvez vous authentifier explicitement en exécutant la commande `Get-XdAuthentication`. Vous pouvez également exécuter votre première commande SDK PowerShell distante, qui vous invite à la même authentification que Get-XdAuthentication.

    - Toutefois, si vous n'avez pas installé le SDK comme décrit dans Installer ou supprimer le SDK PowerShell distant plus tôt dans cet article, vous devez utiliser la commande `Get-XdAuthentication -EnvironmentName USGovernment` pour vous authentifier auprès de Citrix Cloud Government.

4. Continuez à exécuter les cmdlets du SDK PS ou les scripts d'automatisation du SDK PS. Pour un exemple de script, consultez Exemples d'activités dans la documentation Citrix DaaS.

> Remarques :
>
> - Une fois authentifié, l'accès à distance reste valide dans la session PowerShell actuelle pendant 24 heures. Passé ce délai, vous devez saisir vos informations d'identification.
> - Citrix vous recommande de ne pas exécuter les cmdlets de ce SDK sur les Cloud Connectors. Le fonctionnement du SDK n'implique pas les Cloud Connectors.

> Pour une liste complète des snap-ins pris en charge et désactivés, consultez Limitations dans la documentation Citrix DaaS.

Référence de service

Plateforme Citrix Cloud™ Government

La plateforme Citrix Cloud Government présente les différences suivantes par rapport à la plateforme Citrix Cloud (commerciale).

- Pour utiliser Microsoft Entra ID avec Citrix Cloud Government, votre infrastructure Microsoft Entra ID doit être hébergée dans une instance Azure Government. Les instances Microsoft Entra ID hébergées dans des instances Azure commerciales ne peuvent pas se fédérer à Citrix Cloud Government.
- Les guides en libre-service qui proposent des démonstrations de certains aspects de la plateforme ne sont pas disponibles.
- Les fonctions d'utilisation des licences cloud et les rapports d'utilisation active ne sont pas disponibles.
- L'API du journal système et l'Add-on du journal système Citrix pour Splunk ne sont pas disponibles pour une utilisation avec Citrix Cloud Government.

Citrix DaaS pour Citrix Cloud™ Government

Citrix DaaS (anciennement service Citrix Virtual Apps and Desktops™) est généralement disponible pour les clients de Citrix Cloud Government.

Service Workspace pour Citrix Cloud™ Government

L'expérience Workspace et l'agrégation de sites sont généralement disponibles pour les clients de Citrix Cloud Government.

Appliance Connector pour les services cloud

L'Appliance Connector est un composant Citrix hébergé dans votre hyperviseur. Elle sert de canal de communication entre Citrix Cloud™ et vos emplacements de ressources, permettant la gestion du cloud sans nécessiter de configuration réseau ou d'infrastructure complexe. L'Appliance Connector vous permet de gérer et de vous concentrer sur les ressources qui apportent de la valeur à vos utilisateurs.

Fonctions de l'Appliance Connector

- **La connexion d'Active Directory à Citrix Cloud** permet la gestion d'AD, autorisant l'utilisation de forêts et de domaines AD au sein de vos emplacements de ressources. Cela élimine le besoin d'ajouter des approbations AD supplémentaires. Pour plus d'informations, consultez Active Directory avec Appliance Connector.

D'autres services en préversion peuvent également dépendre de l'Appliance Connector.

La plateforme Appliance Connector fait partie de Citrix Cloud Platform et de Citrix Identity Platform et peut traiter des données, y compris les informations suivantes :

- Adresses IP ou FQDN
- Identifiants d'appareil, d'utilisateur et d'emplacement de ressource
- Horodatages
- Données d'événement
- Détails des utilisateurs et des groupes d'Active Directory (par exemple, utilisés pour l'authentification et la recherche d'utilisateurs et de groupes)

Les détails des informations spécifiques traitées par l'Appliance Connector sont disponibles dans le tableau *Données collectées par Citrix Cloud Platform* de l'Aperçu de la protection des données des services Citrix Cloud.

Disponibilité et gestion de la charge de l'Appliance Connector

Pour une disponibilité continue et pour gérer la charge, installez plusieurs Appliances Connector dans chacun de vos emplacements de ressources. Citrix recommande au moins deux Appliances Connector dans chaque emplacement de ressources. Si une Appliance Connector est indisponible pendant un certain temps, les autres Appliances Connector peuvent maintenir la connexion. Étant donné que chaque Appliance Connector est sans état, la charge peut être répartie sur toutes les Appliances Connector disponibles. Il n'est pas nécessaire de configurer cette fonction d'équilibrage de charge. Elle est automatisée. Si au moins une Appliance Connector est disponible, il n'y a aucune perte de communication avec Citrix Cloud.

Si vous n'avez qu'un seul connecteur configuré pour un emplacement de ressources, Citrix Cloud affiche un avertissement sur les pages **Emplacements de ressources** et **Connecteurs**.

Mises à jour de l'appliance Connector

L'appliance Connector est mise à jour automatiquement. Aucune action n'est requise de votre part pour mettre à jour votre connecteur.

Vous pouvez configurer votre emplacement de ressources pour appliquer les mises à jour soit immédiatement dès qu'elles sont disponibles, soit pendant une fenêtre de maintenance spécifique.

Pour plus d'informations sur la configuration des mises à jour, consultez Mises à jour du connecteur

Dans le cadre de la mise à jour, l'appliance Connector devient temporairement indisponible. Les mises à jour ne sont appliquées qu'à une seule appliance Connector par emplacement de ressources à la fois. Pour cette raison, enregistrez au moins deux appliances Connector dans chaque emplacement de ressources afin de garantir qu'au moins une appliance Connector est toujours disponible.

Communication de l'appliance Connector

L'appliance Connector authentifie et chiffre toutes les communications entre Citrix Cloud et vos emplacements de ressources. Une fois installée, l'appliance Connector initie la communication avec Citrix Cloud via une connexion sortante. Toutes les connexions sont établies de l'appliance Connector vers le cloud en utilisant le port HTTPS standard (443) et le protocole TCP. Aucune connexion entrante n'est autorisée.

Le tableau suivant répertorie les ports auxquels l'appliance Connector doit avoir accès :

SERVICE	PORT	PROTOCOLE DE DOMAINE PRIS EN CHARGE	DÉTAILS DE LA CONFIGURATION
DNS	53	TCP/UDP	Ce port doit être ouvert à la configuration locale
NTP	123	UDP	Ce port doit être ouvert à la configuration locale
HTTPS	443	TCP	Le Connector Appliance nécessite un accès sortant à ce port

Pour configurer le Connector Appliance, les administrateurs informatiques doivent pouvoir accéder à l'interface d'administration sur le port 443 (HTTPS) du Connector Appliance.

> **Remarque :**

> Vous devez inclure `https://` au début de l'adresse IP.

> Le Connector Appliance peut communiquer à la fois avec les systèmes sur site de votre emplacement de ressources et avec les systèmes externes. Si vous définissez un ou plusieurs proxys Web lors de l'enregistrement du Connector Appliance, seul le trafic du Connector Appliance vers les systèmes externes est acheminé via ce proxy Web. Si votre système sur site est situé dans un espace d'adressage privé, le trafic du Connector Appliance vers ce système n'est pas acheminé via le proxy Web.

Le Connector Appliance définit les espaces d'adressage privés comme les plages d'adresses IPv4 suivantes :

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Exigences de connectivité Internet

La connexion à Internet depuis vos centres de données nécessite l'ouverture du port 443 pour les connexions sortantes. Cependant, pour fonctionner dans des environnements contenant un serveur proxy Internet ou des restrictions de pare-feu, une configuration supplémentaire pourrait être nécessaire.

Pour fonctionner correctement et consommer les services Citrix Cloud, les adresses suivantes doivent être joignables avec des connexions HTTPS non modifiées :

- `https://*.cloud.us`
- `https://*.citrixworkspacesapi.us`
- `https://*.citrixnetworkapi.us`
- `https://*.nssvc.net`
    - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place :
        - `https://*.g.nssvc.net`
        - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`
- `https://ctxccopspacrconnappprodgov.azurecr.us`

Exigences réseau

Assurez-vous que votre environnement dispose de la configuration suivante :

- Soit le réseau permet au Connector Appliance d'utiliser le DHCP pour obtenir les serveurs DNS et NTP, une adresse IP, un nom d'hôte et un nom de domaine, soit vous pouvez définir manuellement les paramètres réseau dans la console du Connector Appliance.
- Le réseau n'est pas configuré pour utiliser les plages d'adresses IP locales 169.254.0.1/24, 169.254.64.0/18 ou 169.254.192.0/18, qui sont utilisées en interne par le Connector Appliance.
- Soit l'horloge de l'hyperviseur est réglée sur le temps universel coordonné (UTC) et est synchronisée avec un serveur de temps, soit le DHCP fournit les informations du serveur NTP au Connector Appliance.

- Si vous utilisez un proxy avec Connector Appliance, le proxy doit être non authentifié ou utiliser l'authentification de base.

Configuration système requise

Le Connector Appliance est pris en charge sur les hyperviseurs suivants :

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi version 7 mise à jour 2
- Hyper-V sur Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform
- XenServer® 9

Votre hyperviseur doit fournir les capacités minimales suivantes :

- Disque racine de 20 Go
- 2 vCPU
- 4 Go de mémoire
- Un réseau IPv4

Vous pouvez héberger plusieurs Connector Appliances sur le même hôte hyperviseur. Le nombre de Connector Appliances sur le même hôte est uniquement limité par l'hyperviseur et les limitations matérielles.

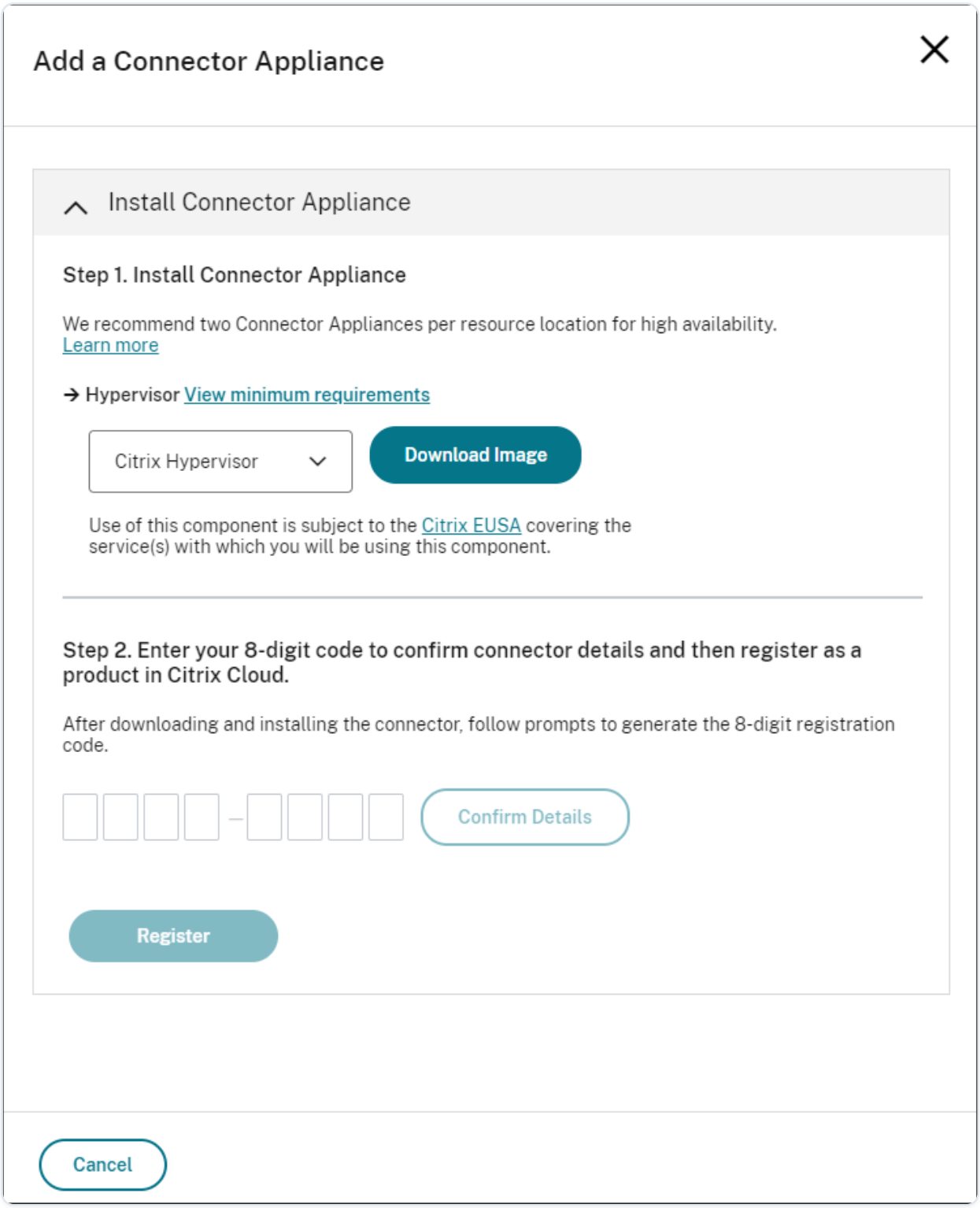
> **Remarque :**
>
> Le clonage, la suspension et la prise d'instantanés de la VM Connector Appliance ne sont pas pris en charge.

Obtenir le Connector Appliance

Téléchargez le logiciel Connector Appliance depuis Citrix Cloud.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu situé en haut à gauche de l'écran, sélectionnez **Emplacements des ressources**.
3. Si vous n'avez pas encore d'emplacement de ressources, cliquez sur l'icône plus (+) ou sélectionnez **Ajouter un emplacement de ressources**.
4. Dans l'emplacement de ressources où vous souhaitez enregistrer l'appliance Connector, cliquez sur l'icône plus (+) de **Connector Appliances**.

   La tâche **Ajouter une appliance Connector** s'ouvre.



5. Dans la liste **Hyperviseur** de l'**Étape 1**, choisissez le type d'hyperviseur ou de fournisseur de cloud que vous utilisez pour héberger votre appliance Connector.

   - Pour les hyperviseurs sur site et les environnements cloud, vous pouvez télécharger l'appliance Connector dans Citrix Cloud :

     a. Cliquez sur **Télécharger l'image**.

b. Consultez le Contrat de service utilisateur final de Citrix et, si vous êtes d'accord, sélectionnez **Accepter et continuer**.

c. Lorsque vous y êtes invité, enregistrez le fichier d'appliance Connector fourni.

L'extension de nom de fichier de l'appliance Connector dépend de l'hyperviseur que vous choisissez.

- Pour certains environnements cloud, vous pouvez obtenir l'appliance Connector depuis la place de marché :
  - AWS
  - Microsoft Azure
  - Google Cloud

6. Laissez la tâche **Installer l'appliance Connector** ouverte. Après avoir installé l'appliance Connector, vous saisissez votre code d'enregistrement dans l'**Étape 2**.

Vous pouvez également accéder à la tâche **Installer l'appliance Connector** depuis la page **Connecteurs**. Sélectionnez l'icône plus (+) pour ajouter un connecteur et choisissez d'ajouter une appliance Connector.

Installer Connector Appliance sur votre hyperviseur

- Citrix Hypervisor™
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

Cette section décrit comment importer le Connector Appliance sur un serveur Citrix Hypervisor à l'aide de XenCenter.

1. Connectez-vous à votre serveur ou pool Citrix Hypervisor à l'aide de XenCenter sur un système ayant accès au fichier XVA du Connector Appliance téléchargé.

2. Sélectionnez **Fichier** > **Importer**.
3. Spécifiez ou accédez au chemin où se trouve le fichier XVA du Connector Appliance. Cliquez sur **Suivant**.
4. Sélectionnez le serveur Citrix Hypervisor sur lequel vous souhaitez héberger le Connector Appliance. Vous pouvez également sélectionner le pool dans lequel héberger le Connector Appliance, et Citrix Hypervisor choisira un serveur disponible approprié. Cliquez sur **Suivant**.
5. Spécifiez le référentiel de stockage à utiliser pour votre Connector Appliance. Cliquez sur **Importer**.
6. Cliquez sur **Ajouter** pour ajouter une interface réseau virtuelle. Dans la liste **Réseau**, sélectionnez le réseau à utiliser pour le Connector Appliance. Cliquez sur **Suivant**.
7. Vérifiez les options à utiliser pour déployer le Connector Appliance. Si l'une d'elles est incorrecte, utilisez **Précédent** pour modifier ces options.
8. Assurez-vous que l'option **Démarrer automatiquement la ou les nouvelles machines virtuelles dès que l'importation est terminée** est sélectionnée. Cliquez sur **Terminer**.

Une fois le Connector Appliance déployé et démarré avec succès, sa console affiche une page d'accueil contenant l'adresse IP du Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration du Connector Appliance et terminer le processus d'enregistrement.

Par défaut, le Connector Appliance utilise le DHCP pour configurer son réseau. Si le DHCP n'est pas disponible dans votre environnement, vous devez configurer le réseau sur la console du Connector Appliance avant de pouvoir accéder à la console de gestion du Connector Appliance. Pour plus d'informations, consultez Configurer le réseau à l'aide de la console du Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

VMware ESXi

Cette section décrit comment déployer le Connector Appliance sur un hôte VMware ESXi à l'aide du client VMware vSphere.

1. Connectez-vous à votre hôte ESXi à l'aide du client vSphere sur un système ayant accès au fichier OVA du Connector Appliance téléchargé.
2. Sélectionnez **Fichier** > **Déployer un modèle OVF...**.
3. Spécifiez ou naviguez jusqu'au chemin où se trouve le fichier OVA du Connector Appliance. Cliquez sur **Suivant**.

4. Vérifiez les détails du modèle. Cliquez sur **Suivant**.
5. Vous pouvez spécifier un nom unique pour votre instance de Connector Appliance. Par défaut, le nom est défini sur **Connector Appliance**. Assurez-vous de choisir un nom qui distingue cette instance du Connector Appliance des autres instances hébergées sur cet hôte ESXi. Cliquez sur **Suivant**.
6. Spécifiez le stockage de destination pour votre Connector Appliance. Cliquez sur **Suivant**.
7. Choisissez le format de stockage des disques virtuels. Cliquez sur **Suivant**.
8. Passez en revue les options à utiliser pour déployer l'appliance de connecteur. Si l'une d'entre elles est incorrecte, utilisez **Retour** pour modifier ces options.
9. Sélectionnez **Mettre sous tension après le déploiement**. Cliquez sur **Terminer**.

Une fois l'appliance de connecteur déployée et démarrée avec succès, sa console affiche une page d'accueil qui contient l'adresse IP de l'appliance de connecteur. Utilisez cette adresse IP pour vous connecter à la page d'administration de l'appliance de connecteur et terminer le processus d'enregistrement.

Par défaut, l'appliance de connecteur utilise DHCP pour définir sa configuration réseau. Si DHCP n'est pas disponible dans votre environnement, vous devez définir la configuration réseau sur la console de l'appliance de connecteur avant de pouvoir accéder à l'interface utilisateur de l'appliance de connecteur. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de l'appliance de connecteur.

Étape suivante : Enregistrer votre appliance de connecteur auprès de Citrix Cloud.

Hyper-V

Cette section décrit comment déployer l'appliance de connecteur sur un hôte Hyper-V. Vous pouvez déployer la machine virtuelle à l'aide du Gestionnaire Hyper-V ou à l'aide du script PowerShell inclus.

Déployer l'appliance de connecteur à l'aide du Gestionnaire Hyper-V

1. Connectez-vous à votre hôte Hyper-V.
2. Copiez ou téléchargez le fichier ZIP de l'appliance de connecteur sur l'hôte Hyper-V.
3. Extrayez le contenu du fichier ZIP. Le fichier ZIP contient un script PowerShell et le fichier connector-appliance.vhdx.
4. Copiez le fichier VHDX à l'emplacement où vous souhaitez conserver vos disques de machine virtuelle. Par exemple, `C:\ConnectorApplianceVMs`.

5. Ouvrez le Gestionnaire Hyper-V.
6. Cliquez avec le bouton droit sur le nom de votre serveur et sélectionnez **Nouveau > Machine virtuelle**.
7. Dans l'**Assistant Nouvelle machine virtuelle**, dans le panneau **Spécifier le nom et l'emplacement**, entrez un nom unique pour identifier votre appliance de connecteur. Cliquez sur **Suivant**.
8. Dans le panneau **Spécifier la génération**, sélectionnez **Génération 1**. Cliquez sur **Suivant**.
9. Dans le panneau **Attribuer de la mémoire**, configurez les paramètres suivants, puis cliquez sur **Suivant** :
    a. Attribuez 4 Go de RAM.
    b. Désactivez la mémoire dynamique.
10. Dans le panneau **Configurer la mise en réseau**, sélectionnez un commutateur dans la liste (par exemple, Commutateur par défaut). Cliquez sur **Suivant**.
11. Dans le panneau **Connecter le disque dur virtuel**, sélectionnez **Utiliser un disque dur virtuel existant**.
12. Accédez à l'emplacement du fichier connector-appliance.vhdx et sélectionnez-le. Cliquez sur **Suivant**.
13. Dans le panneau **Résumé**, vérifiez les valeurs que vous avez choisies, puis cliquez sur **Terminer** pour créer la VM.
14. Dans le panneau **Machines virtuelles**, cliquez avec le bouton droit sur la VM Connector Appliance et sélectionnez **Paramètres**.
15. Dans la fenêtre **Paramètres**, sélectionnez **Matériel > Processeurs** et effectuez les actions suivantes :
    a. Dans **Nombre de processeurs virtuels**, modifiez la valeur sur **2**.
    b. Cliquez sur **Appliquer**.
    c. Cliquez sur **OK**.
16. Dans le panneau **Machines virtuelles**, cliquez avec le bouton droit sur la VM Connector Appliance et sélectionnez **Démarrer**.
17. Cliquez avec le bouton droit sur la VM Connector Appliance et sélectionnez **Connecter** pour ouvrir la console.

Après le déploiement et le démarrage réussi du Connector Appliance, connectez-vous à la console à l'aide du Gestionnaire Hyper-V. La console affiche une page d'accueil contenant l'adresse IP du Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration du Connector Appliance et terminer le processus d'enregistrement.

Par défaut, le Connector Appliance utilise le DHCP pour configurer son réseau. Si le DHCP n'est pas disponible dans votre environnement, vous devez configurer le réseau sur la console du Connector Appliance avant de pouvoir accéder à l'interface utilisateur du Connector Appliance. Pour plus d'informations, consultez Configurer la configuration réseau à l'aide de la console du Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Déployer le Connector Appliance à l'aide d'un script PowerShell

Le fichier connector-appliance.zip contient un script PowerShell qui crée et démarre une nouvelle machine virtuelle.

> **Remarque :**
>
> Pour exécuter ce script PowerShell non signé, vous devrez peut-être modifier les stratégies d'exécution sur le système Hyper-V. Pour plus d'informations, consultez `<https://go.microsoft.com/fwlink/?LinkID=135170>`. Vous pouvez également utiliser le script fourni comme base pour créer ou modifier votre propre script local.

1. Connectez-vous à votre hôte Hyper-V.
2. Copiez ou téléchargez le fichier ZIP du Connector Appliance sur l'hôte Hyper-V.
3. Extrayez le contenu du fichier ZIP : un script PowerShell et un fichier VHDX.
4. Dans une console PowerShell, changez le répertoire actuel pour l'emplacement du contenu du fichier ZIP et exécutez la commande suivante :

   ```
   .\connector-appliance-install.ps1
   ```

5. Lorsque vous y êtes invité, saisissez un nom pour votre machine virtuelle ou sélectionnez **Entrée** pour accepter la valeur par défaut **Connector Appliance**.
6. Lorsque vous y êtes invité, saisissez une destination pour le disque racine ou appuyez sur Entrée pour utiliser le répertoire système par défaut pour les VHD.

7. Lorsque vous y êtes invité, saisissez un nom de fichier pour le disque racine ou sélectionnez **Entrée** pour accepter la valeur par défaut connector-appliance.vhdx.
8. Lorsque vous y êtes invité, sélectionnez le commutateur à utiliser. Sélectionnez **Entrée**.
9. Vérifiez le résumé des informations d'importation de la VM. Si les informations sont correctes, sélectionnez **Entrée** pour continuer. Le script crée et démarre la VM Connector Appliance.

Une fois que le Connector Appliance est déployé et a démarré avec succès, sa console affiche une page d'accueil qui contient l'adresse IP du Connector Appliance. Utilisez cette adresse IP pour vous connecter au Connector Appliance et terminer le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Nutanix AHV

Cette section décrit comment déployer le Connector Appliance à partir du fichier `connector-appliance.vhdx` sur un hôte Nutanix AHV à l'aide de la console web Nutanix Prism.

1. Dans le menu principal de la console web Nutanix Prism, sélectionnez la vue **Stockage**.
2. Cliquez sur **+ Conteneur de stockage** pour créer un conteneur de stockage destiné à contenir le fichier image du Connector Appliance. Vous pouvez également utiliser un conteneur de stockage existant.
3. Chargez le fichier `connector-appliance.vhdx` dans votre conteneur de stockage.
    a. Dans le menu principal de la console web, sélectionnez **Paramètres**.
    b. Sélectionnez l'onglet **Configuration de l'image** et cliquez sur **+ Télécharger l'image**
    c. Dans **Créer une image**, spécifiez un **Nom** pour votre image.
    d. Dans la liste **Type d'image**, sélectionnez **DISQUE**.
    e. Dans la liste **Conteneur de stockage**, sélectionnez le conteneur de stockage que vous avez créé.
    f. Sélectionnez **Charger un fichier**.
    g. Cliquez sur **Choisir un fichier** et accédez au fichier `connector-appliance.vhdx` sur votre système local.
    h. Cliquez sur **Enregistrer**.
4. Attendez que l'image soit créée et que son état s'affiche comme **ACTIF** dans la page **Configuration de l'image**.
5. Sélectionnez l'onglet **Configuration réseau**.

6. Cliquez sur **+ Créer un réseau** pour créer un réseau à utiliser par le Connector Appliance.
7. Dans la page **Créer un réseau**, spécifiez les informations suivantes :
    - Le nom du réseau.
    - L'ID VLAN du réseau.
8. Dans le menu principal de la console web, sélectionnez la vue **VM**.
9. Cliquez sur **+ Créer une VM** pour créer une instance de Connector Appliance.
10. Dans **Créer une VM**, spécifiez les informations suivantes :
    - Le nom de la VM
    - Le nombre de vCPU
    - La quantité de mémoire en GiB
11. Sélectionnez d'utiliser le **BIOS hérité**.
12. Cliquez sur **+ Ajouter un nouveau disque** pour ajouter un disque à la VM.
13. Dans **Ajouter un disque**, complétez les informations suivantes :
    a. Pour **Type**, sélectionnez **DISK**.
    b. Pour **Opération**, sélectionnez **Cloner à partir du service d'image**.
    c. Pour **Type de bus**, sélectionnez **SCSI**
    d. Pour **Image**, sélectionnez l'image que vous avez créée lors du téléchargement du fichier Connector Appliance.
14. Cliquez sur **Ajouter** pour terminer l'ajout du disque.
15. Dans **Créer une VM**, cliquez sur **+ Ajouter une nouvelle carte réseau**.
16. Dans **Créer une carte réseau**, sélectionnez le réseau auquel ajouter la VM.
17. Pour **État de la connexion réseau**, sélectionnez **Connecté**.
18. Cliquez sur **Ajouter** pour terminer l'ajout de la carte réseau.
19. Cliquez sur **Enregistrer** pour créer la VM.

    Par défaut, la nouvelle VM est hors tension.
20. Dans la vue **VM**, sélectionnez la VM et cliquez sur **Mettre sous tension**.
21. Attendez que la VM démarre. Ce processus peut prendre plusieurs minutes.

Une fois que le Connector Appliance est déployé et a démarré avec succès, vous pouvez trouver l'adresse IP du Connector Appliance à l'un des emplacements suivants :

- Dans la vue **VM** de la console web Nutanix Prism.
- Dans la console du Connector Appliance.

Utilisez cette adresse IP pour vous connecter à la page d'administration du Connector Appliance et terminer le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Microsoft Azure

Cette section décrit comment déployer le Connector Appliance dans Microsoft Azure. Vous pouvez déployer le Connector Appliance à partir de la Place de marché Azure ou à partir de l'image disque téléchargée en utilisant le script PowerShell inclus.

Déployer le Connector Appliance à partir de la Place de marché Azure

Pour déployer le Connector Appliance à partir de la Place de marché Azure, suivez les étapes suivantes :

1. Accédez au Connector Appliance dans la Place de marché Azure. (Place de marché Azure)

   Vous pouvez également rechercher « Connector Appliance for Cloud Services » dans la recherche de la place de marché.
2. Cliquez sur **Obtenir maintenant**, puis sur **Créer**.
3. Sur la page **Créer un Citrix Connector™ Appliance pour les services cloud**, complétez les informations suivantes :

   - Sélectionnez l'**abonnement** à utiliser.
   - Sélectionnez le **groupe de ressources** à utiliser.
   - Sélectionnez la **région** dans laquelle localiser le Connector Appliance.
   - Spécifiez un **nom de VM**.
   - Sélectionnez un **réseau virtuel** pour y ajouter le Connector Appliance. Ce réseau est utilisé pour accéder à Citrix Cloud, aux ressources locales et à la page d'administration du Connector Appliance. Ce réseau ne peut pas être modifié ultérieurement.
   - Spécifiez une valeur pour **Sous-réseau**.

   Cliquez sur **Suivant : Balises >**.

4. Sous l'onglet **Balises**, ajoutez les balises requises si nécessaire.

   Cliquez sur **Suivant : Vérifier + créer >**.

5. Après avoir examiné les détails du déploiement, cliquez sur **Créer**.

Une fois le Connector Appliance déployé et démarré avec succès, sa console affiche une page d'accueil qui contient l'adresse IP du Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration du Connector Appliance et terminer le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Déployer la VM Connector Appliance à l'aide d'un script PowerShell

Le fichier `connector-appliance-azure.zip` contient un script PowerShell qui crée et démarre une nouvelle VM. Vous pouvez utiliser le script fourni comme base pour créer ou modifier votre propre script local.

Avant d'exécuter le script, assurez-vous de disposer des prérequis suivants :

- Installez le module Az PowerShell dans votre environnement PowerShell local.
- Exécutez le script PowerShell dans le répertoire où se trouve le fichier VHD.

Suivez les étapes suivantes :

1. Copiez ou téléchargez le fichier ZIP de l'appliance de connecteur sur votre système Windows.
2. Extrayez le contenu du fichier ZIP : un script PowerShell et un fichier VHD.
3. Ouvrez une console PowerShell en tant qu'administrateur.
4. Changez le répertoire actuel pour l'emplacement du contenu du fichier ZIP et exécutez la commande suivante :

   ```
   .\connector-appliance-upload-Azure.ps1
   ```

5. Une boîte de dialogue apparaît, vous invitant à vous connecter à Microsoft Azure. Saisissez vos informations d'identification.
6. Lorsque le script PowerShell vous y invite, sélectionnez l'abonnement à utiliser. Appuyez sur Entrée.
7. Suivez les invites du script, qui vous guident tout au long du processus de téléchargement de l'image et de création d'une machine virtuelle.

8. Après avoir créé la première machine virtuelle, le script vous demande si vous souhaitez créer une autre machine virtuelle à partir de l'image téléchargée.
    - Tapez `y` pour créer une autre machine virtuelle.
    - Tapez `n` pour quitter le script.

Une fois l'appliance de connecteur déployée et démarrée avec succès, sa console affiche une page d'accueil qui contient l'adresse IP de l'appliance de connecteur. Utilisez cette adresse IP pour vous connecter à la page d'administration de l'appliance de connecteur et terminer le processus d'enregistrement.

Étape suivante : Enregistrer votre appliance de connecteur auprès de Citrix Cloud.

AWS

Cette section décrit comment déployer l'appliance de connecteur dans AWS. L'appliance de connecteur est disponible en tant qu'AMI sur la place de marché AWS et nous vous recommandons d'installer l'appliance de connecteur à partir de l'AMI. Vous pouvez également déployer une image disque téléchargée en utilisant l'interface utilisateur AWS ou en utilisant le script PowerShell inclus.

Prérequis réseau

Pour déployer le Connector Appliance sur AWS, assurez-vous d'avoir accès à Citrix Cloud depuis le sous-réseau dans lequel le Connector Appliance est créé.

Nous recommandons d'utiliser une adresse IP privée pour l'appliance, ce qui nécessite une configuration spécifique pour fournir l'accès à Citrix Cloud. Pour réaliser cette configuration, suivez les étapes suivantes dans la **Console de gestion AWS** :

1. Créez la passerelle NAT.
    a. Dans la barre de navigation supérieure, sélectionnez **Services > VPC > Passerelles NAT**.
    b. En haut à droite, cliquez sur **Créer une passerelle NAT**. Saisissez les informations suivantes :
        - Saisissez le **Nom**.
        - Sélectionnez le **sous-réseau** dans la liste.
        - Définissez le **Type de connectivité** sur **Public**.

- Sélectionnez un **ID d'allocation d'IP élastique** dans la liste. S'il n'y a pas d'IP élastique disponible, cliquez sur **Allouer une IP élastique** et suivez les instructions pour en créer une.

c. Cliquez sur **Créer une passerelle NAT**.

2. Créez une entrée de table de routage incluant la passerelle NAT.

   a. Dans la barre de navigation supérieure, sélectionnez **Services > VPC > Tables de routage**.

   b. En haut à droite, cliquez sur **Créer une table de routage**. Saisissez les informations suivantes :

      - Saisissez le **Nom**.
      - Dans la liste, sélectionnez le VPC qui contient le sous-réseau que vous avez sélectionné lors de la création de la passerelle NAT.

   c. Cliquez sur **Créer une table de routage**.

   d. Dans l'onglet **Routes** de la table de routage que vous avez créée, cliquez sur **Modifier les routes > Ajouter une route**.

   e. Saisissez la **Destination** et la **Cible** pour la nouvelle entrée de route.

      - Définissez la destination sur 0.0.0.0/0.
      - Pour la cible, sélectionnez la **passerelle NAT** que vous avez créée dans la liste.

   f. Cliquez sur **Enregistrer la modification**.

3. Associez le sous-réseau à utiliser pour l'appliance Connector à cette table de routage.

   a. Dans la barre de navigation supérieure, **Sélectionner les services > VPC > Tables de routage**.

   b. Sélectionnez la table de routage qui contient la passerelle NAT.

   c. Sur la page d'affichage, accédez à l'onglet **Associations de sous-réseaux**.

   d. Cliquez sur **Modifier les associations de sous-réseaux**.

   e. Sélectionnez le ou les sous-réseaux à associer à la table de routage.

   f. Cliquez sur **Enregistrer les associations**.

Déployer l'appliance Connector depuis l'AWS Marketplace

Avant de commencer, assurez-vous de remplir les conditions préalables suivantes :

- Vous disposez des autorisations nécessaires pour exploiter les ressources EC2.
- Vous avez terminé la configuration dans Prérequis réseau.
- (Facultatif) Vous pouvez créer un groupe de sécurité qui restreint les adresses IP autorisées à accéder à votre Connector Appliance.

Suivez les étapes suivantes :

1. Connectez-vous à la **console de gestion AWS**.
2. Recherchez l'AMI du Connector Appliance sur la place de marché AWS. Vous pouvez le faire de l'une des manières suivantes :
    - Suivez le lien de la place de marché fourni dans Citrix Cloud. (AWS Marketplace)
    - Recherchez l'AMI dans la console de gestion AWS :
        a. Accédez à **Services > Compute > EC2 > AMIs**
        b. Assurez-vous que vous êtes dans la région USA Est (Ohio).
        c. Dans **Images publiques**, recherchez « Citrix Connector Appliance » ou l'ID AMI « ami-026eaf9b3b232577f ».
3. Vérifiez que vous avez la bonne AMI en contrôlant l'ID AMI (ami-026eaf9b3b232577f) et l'ID du propriétaire (414337923189).
4. Copiez l'AMI dans votre abonnement :
    a. Accédez à **Actions > Copier l'AMI**.
    b. Dans la boîte de dialogue **Copier l'AMI**, vous pouvez sélectionner la **Région de destination** dont vous avez besoin.
    c. Cliquez sur **Copy AMI**
5. Depuis la page de résumé de votre AMI copiée, cliquez sur **Launch instance from AMI**.
6. Dans la boîte de dialogue **Launch an instance**, suivez les étapes suivantes :
    a. Sélectionnez le nombre d'instances à créer. Pour la résilience, nous vous recommandons d'avoir au moins deux Connector Appliances dans chaque emplacement de ressources.
    b. Spécifiez un nom pour l'instance.
    c. Pour le **Type d'instance**, sélectionnez **t2.medium**. Le type d'instance doit avoir au moins 4 Go et 2 CPU.

d. Pour la **Paire de clés (connexion)**, sélectionnez **Proceed without a key pair**. La connexion SSH au Connector Appliance n'est pas autorisée, une paire de clés n'est donc pas nécessaire.

e. Pour les **Paramètres réseau**, dans la section **Pare-feu (groupe de sécurité)**, configurez les paramètres suivants :

   i. Choisissez si vous voulez **Create security group** ou **Select existing security group**.

   ii. Désélectionnez **Allow SSH traffic from the internet**

   iii. Sélectionnez **Allow HTTPs traffic from the internet**

   iv. Sélectionnez **Allow HTTP traffic from the internet**

Cliquez sur **Launch instance**.

7. Une fois l'instance créée, dans la section **Succès**, cliquez sur le lien de l'ID d'instance pour afficher votre instance Connector Appliance.

   Vous pouvez également cliquer sur le bouton **View All Instances** sur cette page ou accéder à **Services > EC2 >Instances** dans la console de gestion AWS pour afficher une liste de vos instances.

8. Lorsque l'**État de l'instance** est passé à **En cours d'exécution**, accédez aux détails de l'instance et utilisez l'**Adresse IPv4 privée** pour vous connecter à la page d'administration de l'appliance Connector et terminer le processus d'enregistrement.

Vous devrez peut-être utiliser un hôte bastion pour accéder à la page d'administration de l'appliance Connector à l'adresse IP interne depuis votre navigateur et terminer le processus d'enregistrement.

Par défaut, l'appliance Connector utilise le DHCP pour définir sa configuration réseau. Vous pouvez modifier cette configuration réseau à l'aide de l'interface web de l'appliance Connector. Pour plus d'informations, consultez Configuration des paramètres réseau sur la page d'administration de l'appliance Connector.

Étape suivante : Enregistrer votre appliance Connector auprès de Citrix Cloud.

Déployer l'appliance Connector à l'aide de l'interface utilisateur AWS

Avant de commencer, assurez-vous de satisfaire aux prérequis suivants :

- Vous disposez des autorisations nécessaires pour utiliser les ressources S3 et EC2.

- Vous avez créé un rôle de service et une stratégie disposant d'un accès à l'importation de VM. Pour plus d'informations, consultez `<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role>`.

  > **Remarque :**
  >
  > Pour créer un rôle de service, vous devez créer un compartiment S3. Lors de la création de la stratégie, définissez le compartiment S3 que vous avez créé avec un accès à l'importation de VM.

- Vous avez accès à AWS CloudShell. Il n'est disponible que dans certaines régions. Pour la liste des régions où AWS CloudShell est pris en charge, consultez `<https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html>`.
- Vous avez terminé la configuration dans Prérequis réseau.

Effectuez les étapes suivantes :

1. Sur votre système local, extrayez le contenu de `connector-appliance-aws.zip`.
2. Connectez-vous à la **console de gestion AWS**.
3. Créez un compartiment de stockage en suivant les étapes suivantes. (Vous pouvez également ignorer ces étapes et utiliser un compartiment de stockage existant.)
   a. Dans la barre de navigation supérieure, sélectionnez **Services** > **S3** > **Créer un compartiment**.
   b. Saisissez un nom unique pour votre compartiment. Pour les conventions de dénomination des compartiments dans Amazon S3, consultez `<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html>`.
   c. Sélectionnez la région de votre compartiment. Assurez-vous de choisir la même région que votre région AWS, car vous ne pourrez pas utiliser les fichiers du compartiment si ces régions sont différentes.
   d. Laissez les autres paramètres par défaut, puis cliquez sur **Créer un compartiment**.
4. Cliquez sur le nom du compartiment que vous avez créé. Cliquez sur **Télécharger** > **Ajouter des fichiers**, puis sélectionnez le fichier `connector-appliance.vhd`. Laissez les autres paramètres par défaut, puis cliquez sur **Télécharger**.
5. Cliquez sur le fichier que vous avez téléchargé. Cliquez sur **Copier l'URI S3**.

6. Cliquez sur l'**icône AWS CloudShell** dans la barre de navigation supérieure et exécutez les commandes suivantes :

   a. Créez une tâche pour convertir votre fichier VHD en instantané :

   ```
   aws ec2 import-snapshot --disk-container
   Format=VHD,Url="&lt;S3_URI>"
   ```

   Remplacez la valeur de l'espace réservé par votre URI S3 que vous avez copié à l'étape précédente. Par exemple, `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`.

   Cette commande est terminée lorsque la commande suivante renvoie une chaîne JSON contenant `"Status": "completed"`. Notez la valeur `ImportTaskId` dans la sortie JSON.

   b. Exécutez la commande suivante :

   ```
   aws ec2 describe-import-snapshot-tasks --import-task-ids
   &lt;ImportTaskId>
   ```

   Remplacez la valeur de l'espace réservé par le `ImportTaskId` copié à l'étape précédente. Par exemple, `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`.

7. Dans la **console de gestion AWS**, dans la barre de navigation supérieure, sélectionnez **Services** > **EC2**.
8. Dans le menu à gauche de l'écran, cliquez sur **Instantanés**.
9. Faites un clic droit sur l'instantané que vous avez créé et cliquez sur **Créer une image**.
10. Dans le volet qui s'ouvre, effectuez les étapes suivantes :

    a. Saisissez un nom pour votre AMI.

    b. Sélectionnez **Virtualisation assistée par le matériel**.

    Cliquez sur **Créer**.

11. Dans le menu à gauche de l'écran, cliquez sur **AMIs**.
12. Faites un clic droit sur l'AMI que vous avez créée et cliquez sur **Lancer**.
13. Dans le volet qui s'ouvre, effectuez les étapes suivantes :

a. Choisissez le type d'instance.

b. (Facultatif) Personnalisez le réseau sous l'onglet **Configurer l'instance**.

c. (Facultatif) Attachez un autre volume sous l'onglet **Ajouter du stockage**.

d. Définissez les règles du groupe de sécurité sous l'onglet **Configurer le groupe de sécurité**.

Après avoir examiné le lancement de l'instance, cliquez sur **Vérifier et lancer**.

Une fois que le Connector Appliance est déployé et a démarré avec succès, accédez à **Services** > **EC2** > **Instances** et sélectionnez l'instance que vous avez créée. Utilisez l'**adresse IPv4 privée** pour vous connecter à la page d'administration du Connector Appliance et terminer le processus d'enregistrement. Vous devrez peut-être utiliser un hôte bastion pour accéder à la page d'administration du Connector Appliance à l'adresse IP interne depuis votre navigateur afin de poursuivre le processus d'installation.

Par défaut, le Connector Appliance utilise le DHCP pour définir sa configuration réseau. Vous pouvez modifier cette configuration réseau à l'aide de l'interface web du Connector Appliance. Pour plus d'informations, consultez Configuration des paramètres réseau sur la page d'administration du Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Déployer le Connector Appliance à l’aide d’un script PowerShell

Le fichier `connector-appliance-aws.zip` contient un script PowerShell qui crée et démarre une nouvelle machine virtuelle. Avant d’exécuter le script, assurez-vous de disposer des prérequis suivants :

- Vous avez installé AWS.Tools, AWSPowerShell.NetCore ou AWSPowerShell sur votre système. Pour plus d’informations, consultez `<https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html>`.
- Vous avez créé un rôle de service et une stratégie disposant d’un accès à l’importation de machines virtuelles. Le rôle de service et la stratégie doivent être nommés `vmimport` pour que ce script PowerShell fonctionne. Pour plus d’informations, consultez `<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role>`.

> **Remarque :**

> Pour créer un rôle de service, vous devez créer un compartiment S3. Lors de la création de la stratégie, définissez le compartiment S3 que vous avez créé avec un accès à l'importation de machines virtuelles.

- Vous avez créé un groupe de sécurité Amazon EC2.
- Vous disposez des autorisations S3 et de l'accès API.
- Vous avez terminé la configuration dans Prérequis réseau.

Suivez les étapes suivantes :

1. Sur votre système local, extrayez le contenu de `connector-appliance-aws.zip` dans un dossier.
2. Dans PowerShell, exécutez les commandes suivantes :
   a. Pour pouvoir exécuter une cmdlet AWS dans votre environnement local, exécutez la commande suivante pour ajouter un nouveau profil au magasin AWS SDK :

      ```
      Set-AWSCredential -AccessKey <access_key_ID> -SecretKey
      <secret_key> -StoreAs MyProfile
      ```

      Remplacez les valeurs d'espace réservé par votre clé d'accès et votre clé secrète. Fournissez un nom de profil unique. Dans l'exemple que nous avons fourni, il s'agit de `MyProfile`.

   b. Définissez le profil par défaut :

      ```
      Initialize-AWSDefaultConfiguration -ProfileName MyProfile
      ```

   c. Accédez au dossier où se trouvent les fichiers extraits et exécutez la commande suivante :

      ```
      .\connector-appliance-upload-aws.ps1
      ```

3. Suivez les invites du script, qui vous guideront tout au long de la sélection de la région pour votre déploiement de Connector Appliance, du téléchargement de l'image vers le compartiment choisi et de la saisie d'un nom pour votre VM.
   - Vous devez utiliser le compartiment avec accès à l'importation de VM que vous avez créé précédemment.

- Lorsque vous êtes invité à sélectionner le VPC à utiliser, sélectionnez le VPC où la passerelle NAT et les tables de routage sont configurées.
- Lorsque vous êtes invité à sélectionner le sous-réseau à utiliser, sélectionnez le sous-réseau attaché à la table de routage contenant la passerelle NAT.

Pour plus d'informations, consultez Prérequis réseau.

Une fois le Connector Appliance déployé et démarré avec succès, le script affiche l'adresse IP privée du Connector Appliance. Vous devrez peut-être utiliser un hôte bastion pour accéder à la page d'administration du Connector Appliance à l'adresse IP interne depuis votre navigateur et terminer le processus d'enregistrement.

Par défaut, le Connector Appliance utilise le DHCP pour configurer son réseau. Vous pouvez modifier cette configuration réseau à l'aide de l'interface Web du Connector Appliance. Pour plus d'informations, consultez Configuration des paramètres réseau sur la page d'administration du Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Google Cloud Platform

Cette section décrit comment déployer Connector Appliance sur Google Cloud Platform. Vous pouvez installer le Connector Appliance depuis Google Cloud Marketplace. Vous pouvez également déployer une image disque téléchargée à l'aide de la console Google Cloud Platform ou à l'aide du script PowerShell inclus.

Le fichier `connector-appliance-gcp.zip` contient :

- `connector-appliance.tar.gz`, qui est une image disque du Connector Appliance
- `connector-appliance-upload-gcp.ps1`, qui est un script PowerShell pouvant être utilisé pour déployer automatiquement le Connector Appliance

Déployer le Connector Appliance depuis la place de marché Google Cloud

1. Connectez-vous à votre compte Google.
2. Suivez le lien de la place de marché fourni dans Citrix Cloud. (Google Cloud Marketplace)

   Vous pouvez également rechercher « Connector Appliance for Cloud Services » dans la recherche de la place de marché.
3. Cliquez sur **Lancer**.

4. Sur la page **Nouveau déploiement de Citrix Connector Appliance for Cloud Services**, renseignez les informations suivantes :

   - Spécifiez un **Nom de déploiement** pour la tâche de déploiement.
   - Sélectionnez la **Zone** dans laquelle localiser le Connector Appliance.
   - Sélectionnez la **Famille de machines**, la **Série** et le **Type de machine** à utiliser.
   - Sélectionnez le **Type de disque de démarrage** et la **Taille du disque de démarrage en Go** à utiliser.
   - Dans la section **Mise en réseau**, spécifiez l'interface réseau à utiliser par le Connector Appliance. Si vous souhaitez pouvoir vous connecter à la page d'administration depuis un réseau public, spécifiez une **Adresse IP externe**.

   Cliquez sur **Déployer**. Vous êtes redirigé vers la page **Gestionnaire de déploiement**.

   > **Remarque :**
   >
   > Une fois le Connector Appliance déployé et démarré avec succès, vous recevez un e-mail confirmant que le Connector Appliance est déployé sur Google Cloud Platform.

5. Sur la page **Gestionnaire de déploiement**, cliquez sur le nom de l'instance. Vous pouvez également rechercher l'instance de Connector Appliance que vous avez créée dans le **Compute Engine**.
6. Si vous avez précédemment spécifié une **adresse IP externe** lors de la configuration de l'interface réseau de votre Connector Appliance, copiez l'**adresse IP externe** dans la section **Interfaces réseau** de l'onglet **Détails**. Utilisez cette adresse IP pour vous connecter à la page d'administration du Connector Appliance et terminer le processus d'enregistrement. Vous pouvez également utiliser l'**adresse IP interne principale** pour visiter la page d'administration du Connector Appliance depuis une autre machine située dans le même sous-réseau que votre Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Déployer le Connector Appliance à l'aide de la console Google Cloud Platform

1. Sur votre système local, extrayez le contenu de `connector-appliance-gcp.zip`.
2. Dans votre projet Google Cloud Platform, créez un compartiment de stockage. (Vous pouvez également utiliser un compartiment de stockage existant.)

a. Dans le menu principal, sélectionnez **Cloud Storage**.

b. Dans le volet principal, sélectionnez **Créer un compartiment**.

c. Spécifiez un nom pour votre compartiment.

d. Configurez les paramètres de stockage et d'accès aux données dont vous avez besoin. Vous pouvez laisser ces paramètres par défaut.

e. Cliquez sur **Créer**.

3. Dans votre compartiment de stockage, sélectionnez **Importer des fichiers** et choisissez le fichier `connector-appliance.tar.gz`. Patientez pendant le téléchargement du fichier.
4. Sélectionnez le fichier téléchargé pour afficher ses détails. Copiez la valeur de **gsutil URI** dans le presse-papiers.
5. Ouvrez le Cloud Shell en cliquant sur l'icône **Activer Cloud Shell** dans la barre d'en-tête.
6. Dans votre Cloud Shell, exécutez la commande suivante pour créer une image :

```
gcloud compute images create "Image name" --guest-os-
features=MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded
connector-appliance.tar.gz file"
```

7. Dans le menu principal, sélectionnez **Compute Engine** > **Instances de VM**.
8. Sélectionnez **Créer une instance**. Dans le volet qui s’ouvre, spécifiez les informations suivantes :

a. Dans le champ **Nom**, spécifiez un nom pour l’instance de Connector Appliance.

b. Choisissez une région pour localiser le Connector Appliance.

c. Choisissez la configuration de la machine.

d. Dans la section **Disque de démarrage**, cliquez sur **Modifier**.

e. Dans la section qui s’ouvre, accédez à l’onglet **Images personnalisées**.

f. Dans la liste **Image**, sélectionnez l’image que vous avez créée.

g. Cliquez sur **Sélectionner**.

h. Dans la section **Pare-feu**, activez le trafic HTTPS pour autoriser l’accès à la page d’administration du Connector Appliance.

i. Spécifiez toute configuration supplémentaire requise. Par exemple, vous ne souhaitez peut-être pas utiliser la configuration réseau par défaut.

Cliquez sur **Créer**.

9. Dans la section **Instances de VM**, sélectionnez votre VM nouvellement créée pour afficher ses détails.

Une fois le Connector Appliance déployé et démarré avec succès, la section **Instances de VM** affiche les adresses IP du Connector Appliance.

Si le Connector Appliance possède une adresse IP externe, vous pouvez utiliser cette adresse IP pour accéder à la page d'administration du Connector Appliance depuis votre navigateur et terminer le processus d'enregistrement.

Si le Connector Appliance ne possède qu'une adresse IP interne, utilisez un hôte bastion pour accéder à la page d'administration du Connector Appliance depuis votre navigateur et terminer le processus d'enregistrement. Pour plus d'informations, consultez `<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>`.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Déployer le Connector Appliance à l'aide d'un script PowerShell

Pour utiliser le script PowerShell fourni afin de déployer le Connector Appliance, vous devez avoir le SDK Google Cloud installé sur votre système.

1. Sur votre système local, extrayez le contenu de `connector-appliance-gcp.zip` vers un dossier.
2. Dans PowerShell, changez le répertoire pour le dossier où se trouvent les fichiers extraits.
3. Exécutez la commande `.\connector-appliance-upload-GCP.ps1`.
4. Dans la fenêtre du navigateur qui s'ouvre, authentifiez-vous auprès du SDK Google Cloud avec un compte ayant accès au projet sur lequel vous souhaitez déployer le Connector Appliance.
5. Dans Google Cloud Tools pour PowerShell, lorsque le script PowerShell vous y invite, sélectionnez le projet à utiliser. Appuyez sur Entrée.
6. Suivez les invites du script, qui vous guident tout au long du processus de téléchargement du disque, de création d'une image et de création d'une machine virtuelle.
7. Après avoir créé la première VM, le script vous demande si vous souhaitez créer une autre VM à partir de l'image téléchargée.
    - Tapez `y` pour créer une autre VM.
    - Tapez `n` pour quitter le script.

Une fois le Connector Appliance déployé et démarré avec succès, le script affiche l'adresse IP interne du Connector Appliance. Vous pouvez également vous rendre sur la console Google Cloud Platform pour trouver l'adresse IP interne du Connector Appliance. La section **Compute Engine** > **Instances de VM** affiche l'adresse IP du Connector Appliance.

Utilisez un hôte bastion pour accéder à la page d'administration du Connector Appliance à l'adresse IP interne depuis votre navigateur et terminer le processus d'enregistrement. Pour plus d'informations, consultez `<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>`.

Étape suivante : Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Enregistrer votre Connector Appliance avec Citrix Cloud

Enregistrez un Connector Appliance avec Citrix Cloud pour fournir un canal de communication entre Citrix Cloud et vos emplacements de ressources.

Cette section décrit l'enregistrement du Connector Appliance à l'aide du code à huit chiffres du Key Registration Service (KRS).

Après avoir installé votre Connector Appliance sur l'hyperviseur et l'avoir démarré, la console affiche l'adresse IP du Connector Appliance. La console affiche également une empreinte SSL que vous pouvez utiliser pour valider votre connexion à l'interface utilisateur du Connector Appliance.



1. Copiez l'adresse IP du Connector Appliance dans la barre d'adresse de votre navigateur.

Remarque :

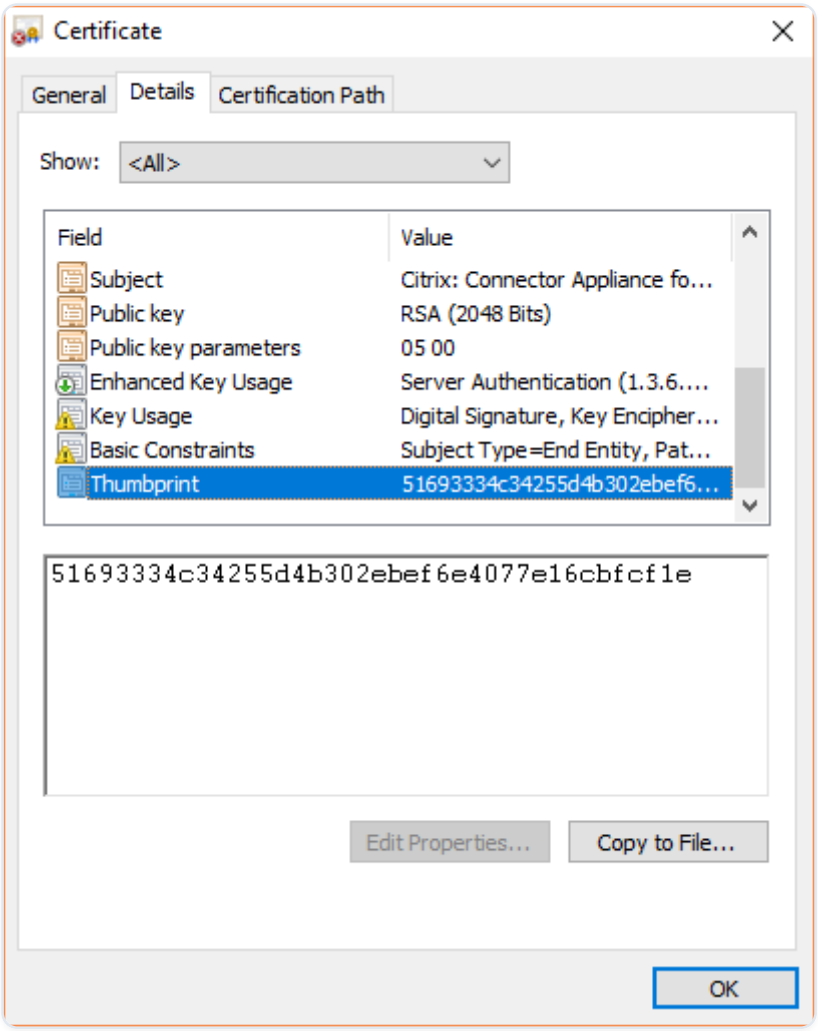
Vous devrez peut-être inclure `https://` au début de l'adresse IP. Pour Citrix Cloud Government, ajoutez `?deployment=productiongov` à la fin de l'adresse web.

L'interface utilisateur du Connector Appliance utilise un certificat auto-signé, qui est valide pendant cinq ans. Par conséquent, vous pourriez voir un message indiquant que la connexion n'est pas sécurisée. Pour vérifier la connexion à votre Connector Appliance, vous pouvez comparer l'empreinte SSL de la console avec l'empreinte que le navigateur reçoit de la page web.

Par exemple, dans le navigateur Google Chrome, suivez les étapes suivantes :

a. Cliquez sur le marqueur **Non sécurisé** à côté de la barre d'adresse.
b. Sélectionnez **Certificat**. La fenêtre **Certificat** s'ouvre.
c. Accédez à l'onglet **Détails** et recherchez le champ **Empreinte**.

   Si la valeur du champ **Empreinte** et l'empreinte SSL fournie dans la console correspondent, vous pouvez confirmer que votre navigateur se connecte directement à l'interface utilisateur du Connector Appliance.

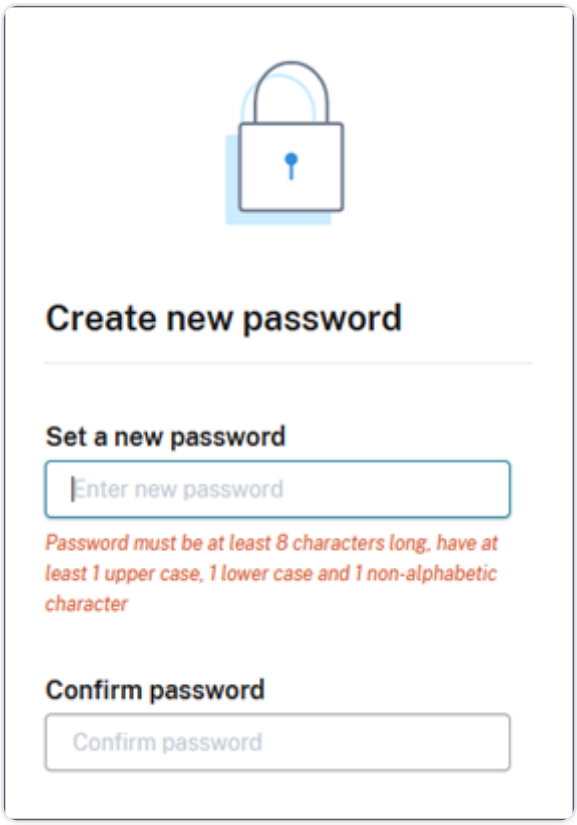


Vous pouvez remplacer ce certificat auto-signé par l'un des vôtres, signé par votre organisation ou généré à l'aide de la chaîne de confiance de votre organisation. Pour plus d'informations, consultez Gestion des certificats.

2. Si votre navigateur nécessite une étape supplémentaire pour confirmer que vous souhaitez continuer vers le site, effectuez cette étape maintenant.

   La page web **Créer un nouveau mot de passe** s'ouvre.

3. Créez un mot de passe pour l'interface utilisateur de votre Connector Appliance et cliquez sur **Définir le mot de passe**.

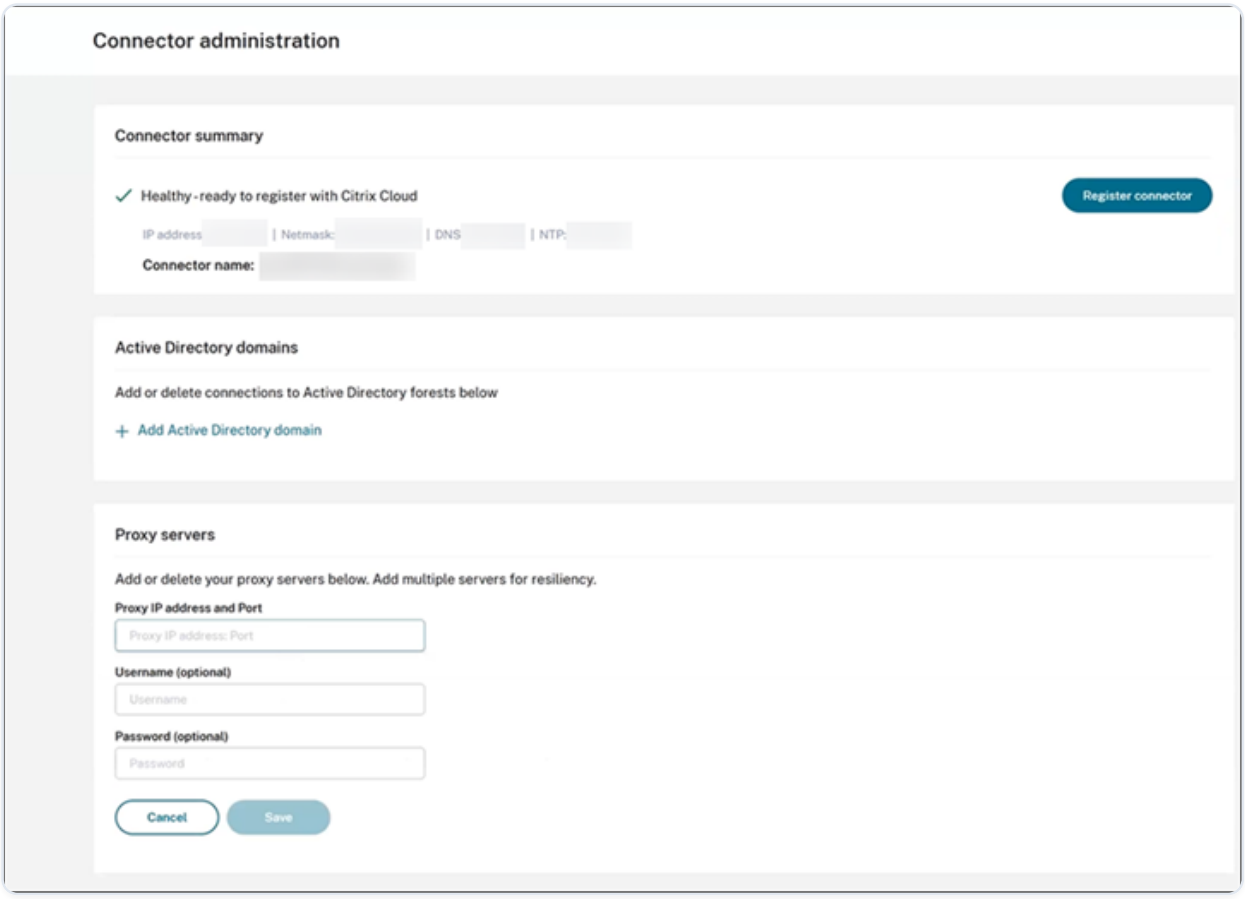


Le mot de passe que vous définissez doit répondre aux exigences suivantes :

- 8 caractères ou plus
- Contient des lettres majuscules et minuscules
- Contient au moins un caractère non alphabétique

Assurez-vous de stocker ce mot de passe dans un endroit sûr pour une utilisation future.

4. Connectez-vous avec le mot de passe que vous avez défini. La page **Administration du connecteur** s'ouvre.



5. (Facultatif) Si vous utilisez un ou plusieurs proxys web, vous pouvez ajouter les adresses des proxys dans la section **Serveurs proxy**. Les proxys non authentifiés et authentifiés sont pris en charge. Pour ajouter un proxy non authentifié, indiquez une **adresse IP et un port de proxy** valides. Pour ajouter un proxy authentifié, indiquez également un **nom d'utilisateur** et un **mot de passe** valides.

   > **Remarque :**
   >
   > Seule l'authentification proxy de base est prise en charge. Les autres formes d'authentification ne sont pas prises en charge.
   >
   > Seul le trafic vers les systèmes externes est acheminé via le proxy web. Pour plus d'informations, consultez Communication de l'appliance Connector.

6. (Facultatif) Si votre réseau utilise des proxys web intercepteurs TLS pour accéder à Internet, il peut être nécessaire que votre Connector fasse confiance à son autorité de certification racine pour communiquer avec succès avec le cloud.

   a. Sous **Autorités de certification racine**, sélectionnez **Ajouter un certificat**.

   b. Copiez le contenu du certificat au format PEM :

```
-----BEGIN CERTIFICATE-----

<certificate-base64-bytes>

-----END CERTIFICATE-----
```

c. Dans **Détails complets du certificat**, collez le contenu du certificat.

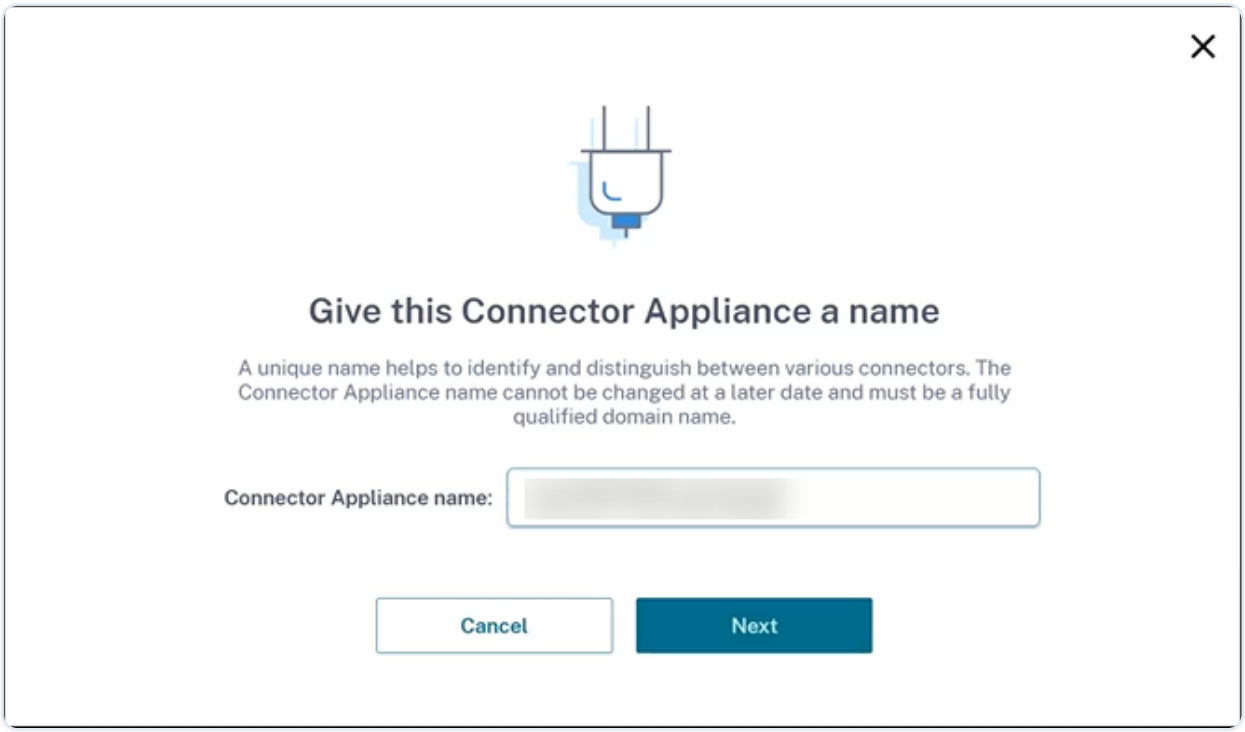
d. Sélectionnez **Ajouter un certificat**.

Pour ajouter une autorité de certification racine (RootCA) à l'aide des API de l'appliance Connector, consultez Gestion des autorités de certification racine dans la documentation Citrix Developer.

> **Remarque :**
>
> Les certificats expirés ou qui expireront dans les 30 prochains jours afficheront un avertissement.

7. Cliquez sur **Enregistrer le Connector** pour ouvrir la tâche d'enregistrement.
8. Choisissez un nom pour votre appliance Connector. Ce nom peut vous aider à distinguer les différentes appliances Connector qui existent dans votre emplacement de ressources. Une fois votre appliance Connector enregistrée, le nom ne peut pas être modifié.

   Saisissez le nom dans le champ **Nom de l'appliance Connector** et cliquez sur **Suivant**.

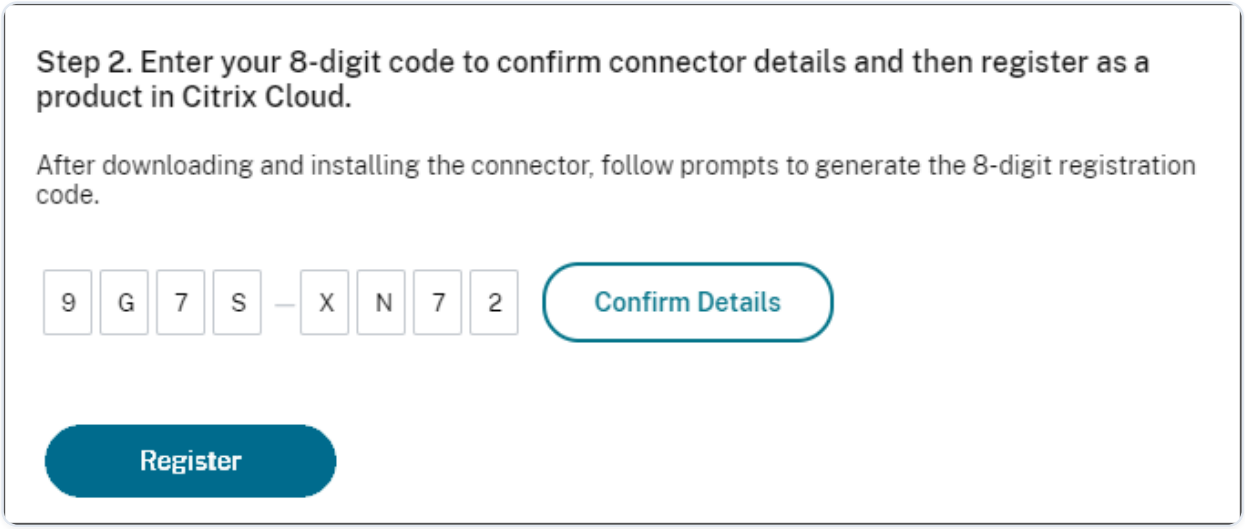


La page web fournit un code à utiliser pour s'enregistrer auprès de Citrix Cloud. Ce code expire dans 15 minutes.



9. Utilisez le bouton **Copier** pour copier le code dans le presse-papiers.
10. Retournez à la page web **Emplacements des ressources**.
11. Collez le code dans l'**Étape 2** de la tâche **Installer Connector Appliance**. Cliquez sur **Confirmer les détails**.

Citrix Cloud vérifie que le Connector Appliance est présent et peut être contacté. Si le code d'enregistrement a expiré, vous êtes invité à générer un nouveau code.



12. Cliquez sur **Enregistrer**.

    La page indique si l'enregistrement a réussi. Si l'enregistrement a échoué, vous êtes invité à réessayer.

13. Cliquez sur **Fermer**.

La **page d'administration du Connector Appliance** vous permet également de télécharger un rapport de diagnostic pour le Connector Appliance. Pour plus d'informations, consultez Génération d'un rapport de diagnostic.

Vous pouvez également enregistrer le Connector Appliance à l'aide d'un client sécurisé. Pour plus d'informations, consultez Enregistrement de votre Connector Appliance sans surveillance. Pour « deployment », saisissez « productiongov ».

Après l'enregistrement de votre Connector Appliance

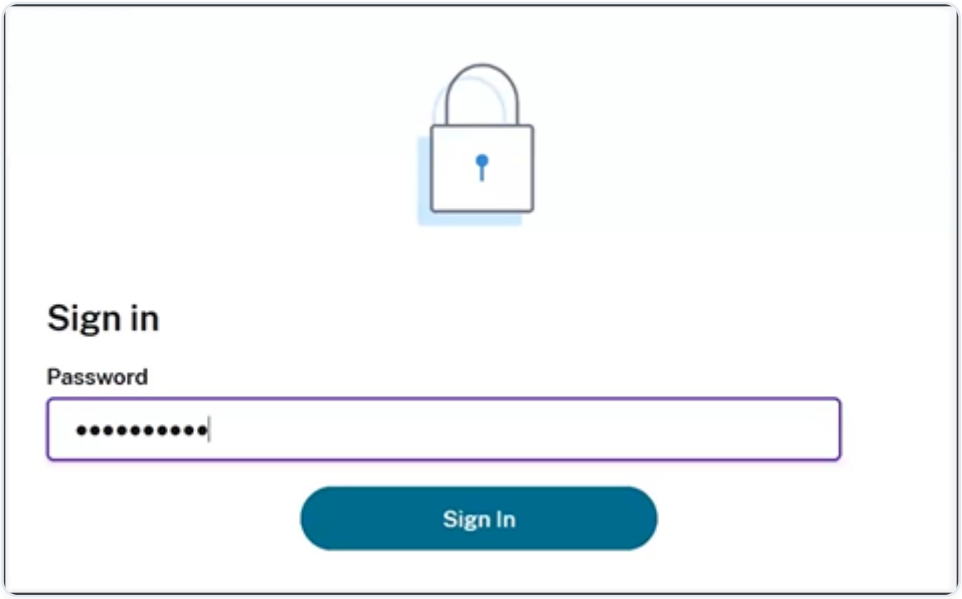
Pour chaque emplacement de ressources, nous vous conseillons d'installer et d'enregistrer au moins deux Connector Appliances. Cette configuration garantit une disponibilité continue et permet aux connecteurs d'équilibrer la charge.

Vous ne pouvez pas gérer directement votre Connector Appliance.

Le Connector Appliance est mis à jour automatiquement. Vous n'avez aucune action à effectuer pour mettre à jour votre connecteur. Vous pouvez spécifier l'heure et le jour auxquels vous souhaitez que les mises à jour du Connector Appliance soient appliquées dans votre emplacement de ressources. Pour plus d'informations, consultez Mises à jour du connecteur.

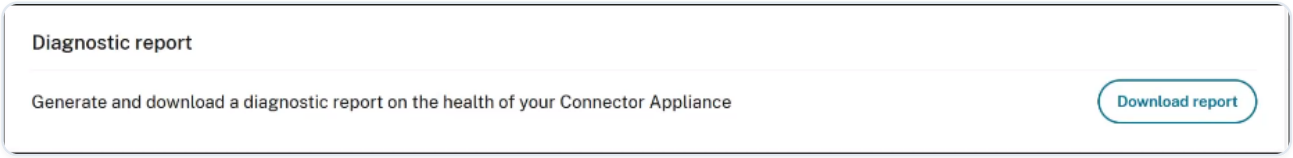
Ne clonez pas, ne suspendez pas et ne prenez pas d'instantané de vos machines virtuelles Connector Appliance. Ces actions ne sont pas prises en charge.

La page **Créer un nouveau mot de passe** ne s'affiche que la première fois que vous vous connectez à l'interface utilisateur du Connector Appliance. Assurez-vous de stocker ce mot de passe dans un endroit sûr pour une utilisation future. Ce mot de passe ne peut pas être réinitialisé. Si vous oubliez le mot de passe, vous devez réinstaller le Connector Appliance. Lors des connexions ultérieures à l'interface utilisateur, il vous sera demandé de saisir le mot de passe que vous avez défini lors de l'enregistrement du Connector Appliance.



Génération d'un rapport de diagnostic

Vous pouvez générer et télécharger un rapport de diagnostic depuis la **page d'administration du Connector Appliance**.



1. Depuis la console du Connector Appliance dans votre hyperviseur, copiez l'adresse IP dans la barre d'adresse de votre navigateur.
2. Saisissez le mot de passe que vous avez défini lors de l'enregistrement de votre Connector Appliance.
3. Dans la section **Rapport de diagnostic** de la page, cliquez sur **Télécharger le rapport**.

Les rapports de diagnostic sont fournis dans un fichier `.zip`.

Vérifier votre connexion réseau

Vous pouvez vérifier votre connexion réseau depuis la **page d'administration du Connector Appliance** en utilisant le contrôle de diagnostic **Capture TCP**.

1. Sur la **page d'administration du Connector Appliance**, cliquez sur le nom de votre compte dans la barre d'en-tête et sélectionnez **Diagnostics réseau**.
2. (Facultatif) Dans la section **Capture TCP**, saisissez l'adresse IP cible, le nom d'hôte ou le port pour restreindre la capture TCP.
3. Dans le menu **Durée de la trace**, sélectionnez la durée pendant laquelle vous souhaitez exécuter votre trace.
4. (Facultatif) Activez le **Traçage des paquets** pour capturer le contenu des paquets.

   Lorsque le traçage de paquets est désactivé, la fonctionnalité de capture TCP utilise une approche au mieux pour capturer les en-têtes à des fins de diagnostic. Cette approche au mieux capture les 512 premiers octets de chaque paquet. Cependant, comme les en-têtes n'ont pas une taille fixe, cette approche pourrait ne pas capturer l'intégralité de l'en-tête.
5. Cliquez sur **Démarrer le traçage**.
6. Attendez que le traçage soit terminé. Une fois le traçage terminé, vous pouvez télécharger un rapport de traçage ou démarrer un nouveau traçage.

   - Cliquez sur **Télécharger** pour télécharger le rapport de traçage. Le rapport de traçage est fourni dans un fichier `.pcap`.
   - Cliquez sur **Démarrer un nouveau traçage** pour lancer un autre traçage.

Connexion d'Active Directory à Citrix Cloud

Vous pouvez utiliser l'Appliance Connector pour connecter un emplacement de ressources à des forêts qui ne contiennent pas de ressources Citrix Virtual Apps and Desktops™. Par exemple, dans le cas de clients Citrix Secure Private Access ou de clients Citrix Virtual Apps and Desktops avec certaines forêts utilisées uniquement pour l'authentification des utilisateurs.

Pour plus d'informations, consultez Active Directory avec l'Appliance Connector.

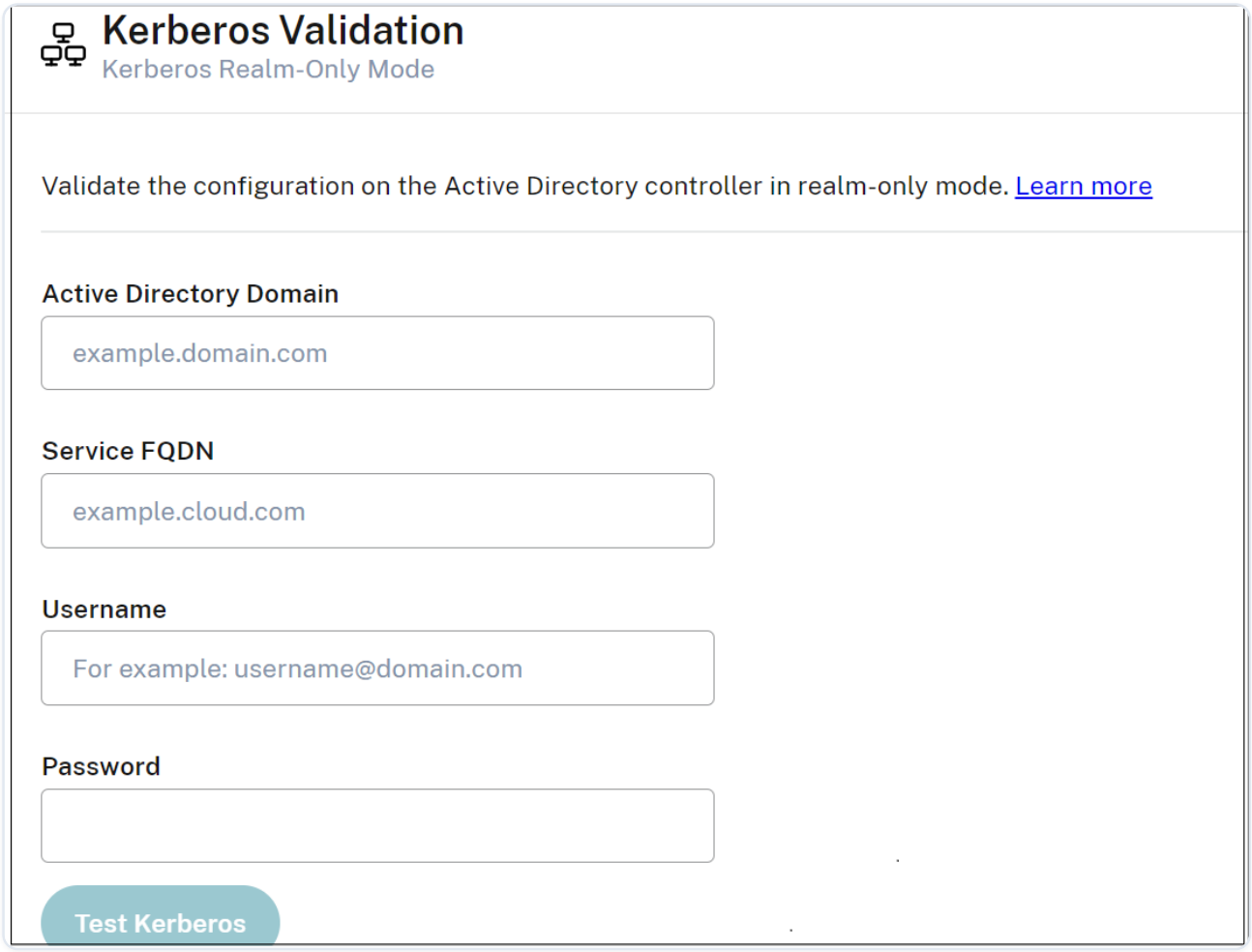
Validation de votre configuration Kerberos

Si vous utilisez Kerberos pour l'authentification unique, vous pouvez vérifier que la configuration de votre contrôleur Active Directory est correcte depuis la page d'**administration de l'Appliance Connector**. La fonctionnalité de **validation Kerberos** vous permet de valider une configuration en

mode Kerberos domaine uniquement ou une configuration en mode Délégation contrainte Kerberos (KCD).

Valider la configuration Kerberos domaine uniquement :

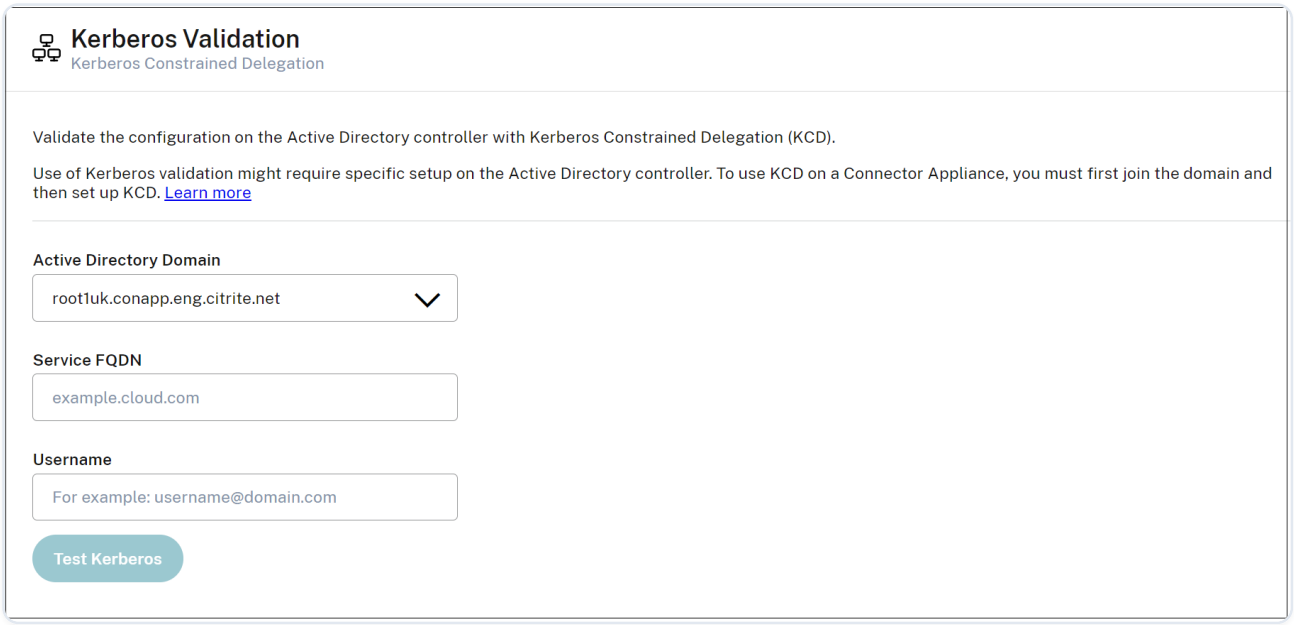
1. Accédez à la page d'**administration de l'Appliance Connector**.
2. Depuis la console de l'Appliance Connector dans votre hyperviseur, copiez l'adresse IP dans la barre d'adresse de votre navigateur.
3. Saisissez le mot de passe que vous avez défini lors de l'enregistrement de votre Appliance Connector.
4. Pour valider votre configuration Kerberos domaine uniquement, sélectionnez **Validation Kerberos domaine uniquement** dans la section **Domaines Active Directory**.
5. Spécifiez le **domaine Active Directory**.
    - Si vous validez une configuration en mode Kerberos realm-only, vous pouvez spécifier n'importe quel domaine Active Directory. Ce mode ne dépend pas de l'adhésion au domaine.
6. Spécifiez le **FQDN du service**. Le nom de service par défaut est supposé être « https ». Si vous spécifiez « computer.example.com », cette valeur est considérée comme identique à « `<https://computer.example.com>` ».
7. Spécifiez le **nom d'utilisateur**.
8. Spécifiez le **mot de passe**.
9. Cliquez sur **Tester Kerberos**.



Valider la configuration de la délégation contrainte Kerberos (KCD) :

1. Accédez à la page d'**administration de l'appliance Connector**.
2. Pour valider le mode **Délégation contrainte Kerberos (KCD)** pour les domaines auxquels l'appliance Connector a été jointe, sélectionnez **Validation Kerberos** dans le menu d'ellipse (…) du domaine concerné.
3. Spécifiez le **domaine Active Directory**.
    - Si vous validez une configuration de délégation contrainte Kerberos, vous devez sélectionner dans une liste de domaines joints.
4. Spécifiez le **FQDN du service**. Le nom de service par défaut est supposé être « https ». Par exemple, si vous spécifiez « computer.example.com », cette valeur est considérée comme identique à « `<https://computer.example.com”>` ».
5. Spécifiez le **nom d'utilisateur**.
    - Pour le mode Délégation contrainte Kerberos, vous pouvez également valider la configuration Kerberos à l'aide de comptes de service en sélectionnant l'onglet **Comptes de service**.

6. Cliquez sur **Tester Kerberos**.



Si la configuration Kerberos est correcte, le message "Configuration Kerberos validée avec succès" s'affiche. Si la configuration Kerberos n'est pas correcte, un message d'erreur s'affiche, fournissant des informations sur l'échec de la validation.

Pour plus d'informations sur Kerberos, consultez la documentation Microsoft.

Paramètres réseau de votre Connector Appliance

Par défaut, l'adresse IP et les paramètres réseau de votre Connector Appliance sont automatiquement attribués via DHCP.

Après avoir enregistré votre Connector Appliance via DHCP, vous pouvez modifier ses paramètres réseau dans la **page d'administration du Connector Appliance**.

Cependant, si DHCP n'est pas disponible dans votre environnement ou si vous n'avez pas accès à la **page d'administration du Connector Appliance**, vous pouvez configurer le réseau directement sur la console du Connector Appliance.

Configuration des paramètres réseau sur la page d'administration du Connector Appliance

Après avoir enregistré votre Connector Appliance via DHCP, vous pouvez modifier ses paramètres réseau dans la **page d'administration du Connector Appliance**.

Pour configurer manuellement vos paramètres réseau :

1. Dans la section **Résumé du connecteur**, sélectionnez **Modifier les paramètres réseau**.

2. Dans la boîte de dialogue **Paramètres réseau**, choisissez **Configurer vos propres paramètres réseau**.
3. Saisissez l'**adresse IP**, le **masque de sous-réseau** et la **passerelle par défaut**.
4. Ajoutez un ou plusieurs **serveurs DNS**.
5. Ajoutez un ou plusieurs **serveurs NTP**.
6. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez les modifications apportées à vos paramètres réseau, le Connector Appliance redémarre. Pendant le redémarrage, le Connector Appliance est temporairement indisponible. Vous êtes déconnecté de la **page d'administration du Connector Appliance** et l'URL de cette page change. Vous pouvez trouver la nouvelle URL dans la console du Connector Appliance ou en consultant les informations réseau de votre hyperviseur.

Pour modifier votre configuration réseau afin d'utiliser des valeurs attribuées automatiquement :

1. Dans la section **Résumé du connecteur**, sélectionnez **Modifier les paramètres réseau**.
2. Dans la boîte de dialogue **Paramètres réseau**, choisissez **Obtenir l'adresse IP automatiquement**.
3. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez les modifications apportées à vos paramètres réseau, le Connector Appliance redémarre. Pendant le redémarrage, le Connector Appliance est temporairement indisponible. Vous êtes déconnecté de la **page d'administration du Connector Appliance** et l'URL de cette page change. Vous pouvez trouver la nouvelle URL dans la console du Connector Appliance ou en consultant les informations réseau de votre hyperviseur.

Définir la configuration réseau à l'aide de la console du Connector Appliance

Par défaut, l'adresse IP et les paramètres réseau de votre Connector Appliance sont attribués automatiquement via DHCP. Cependant, si DHCP n'est pas disponible dans votre environnement ou si vous n'avez pas accès à la **page d'administration du Connector Appliance**, vous pouvez définir la configuration réseau directement sur la console du Connector Appliance.

Pour définir la configuration réseau :

1. Dans votre hyperviseur, redémarrez le Connector Appliance.
2. Pendant le démarrage du Connector Appliance, surveillez la console pour le message `Welcome to GRUB!`.
3. Lorsque vous voyez ce message, appuyez sur **Échap** pour accéder au menu GRUB.

4. Pour modifier les paramètres de démarrage, appuyez sur **e**.

   Vous voyez une vue qui ressemble à l'image suivante :



5. Modifiez la ligne qui commence par `linux` pour inclure la configuration réseau requise.

   - Pour spécifier la mise en réseau DHCP, ajoutez `network=dhcp` à la fin de la ligne.
   - Pour spécifier la mise en réseau statique, ajoutez les paramètres suivants à la fin de la ligne :

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route=<defau
     lt_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<ntp_server_1>,<nt
     p_server_2>
     ```

     Remplacez les valeurs d'espace réservé par les valeurs de votre configuration.

6. Appuyez sur **Ctrl+X** pour démarrer le Connector Appliance avec la nouvelle configuration.

Modifier le mot de passe de l'utilisateur administrateur pour le Connector Appliance

1. Dans le menu utilisateur en haut à droite de la console, sélectionnez **Changer le mot de passe**.

   La page de modification du mot de passe s'affiche.



2. Saisissez votre mot de passe actuel, puis saisissez et confirmez le nouveau mot de passe. Le nouveau mot de passe que vous définissez doit respecter les exigences suivantes :
    - 8 caractères ou plus
    - Contient des lettres majuscules et minuscules
    - Contient au moins un caractère non alphabétique
    - Ne doit pas être identique au mot de passe actuel
3. Sélectionnez **Changer le mot de passe** pour enregistrer vos modifications.

Citrix Cloud vous déconnecte automatiquement et vous redirige vers la page de connexion.

Active Directory avec Connector Appliance

Vous pouvez utiliser Connector Appliance pour connecter un emplacement de ressources à des forêts qui ne contiennent pas de ressources Citrix Virtual Apps and Desktops™. Par exemple, dans le cas de clients Citrix Secure Private Access ou de clients Citrix Virtual Apps and Desktops avec certaines forêts utilisées uniquement pour l'authentification des utilisateurs.

Lorsque vous utilisez Active Directory multi-domaine avec Connector Appliance, notez que Connector Appliance ne peut pas être utilisé à la place des Cloud Connectors dans les forêts qui contiennent des VDA.

Prérequis

Prérequis Active Directory

- Joint à un domaine Active Directory qui contient les ressources et les utilisateurs que vous utilisez pour créer des offres pour vos utilisateurs. Pour plus d'informations, consultez l'article (#deployment-scenarios-for-using-connector-appliance-with-active-directory) .
- Chaque forêt Active Directory que vous prévoyez d'utiliser avec Citrix Cloud™ doit toujours être accessible par deux Connector Appliances.
- Le Connector Appliance doit pouvoir atteindre les contrôleurs de domaine à la fois dans le domaine racine de la forêt et dans les domaines que vous avez l'intention d'utiliser avec Citrix Cloud. Pour plus d'informations, consultez les articles de support Microsoft suivants :
    - Comment configurer les domaines et les approbations

    - Section « Ports des services système » dans Vue d'ensemble des services et exigences en matière de ports réseau pour Windows

- Utilisez des groupes de sécurité universels au lieu de groupes de sécurité globaux. Cette configuration garantit que l'appartenance au groupe d'utilisateurs peut être obtenue à partir de n'importe quel contrôleur de domaine de la forêt.

Prérequis réseau

- Connecté à un réseau pouvant contacter les ressources que vous utilisez dans votre emplacement de ressources.
- Connecté à Internet. Pour plus d'informations, consultez Exigences système et de connectivité.

En plus des ports listés dans Communication du Connector Appliance, le Connector Appliance nécessite une connexion sortante vers le domaine Active Directory via ces ports :

SERVICE	PORT	PROTOCOLE DE DOMAINE PRIS EN CHARGE
Kerberos	88	TCP/UDP
Service de noms NetBIOS	137	UDP
Datagramme NetBIOS	138	UDP
Session NetBIOS	139	TCP
LDAP	389	TCP/UDP
SMB sur TCP	445	TCP
Kerberos mot de passe	464	TCP/UDP
Catalogue global	3268	TCP
Ports RPC dynamiques	49152–65535	TCP

Le Connector Appliance utilise la signature LDAP pour sécuriser les connexions au contrôleur de domaine. Cela signifie que le protocole LDAP sur SSL (LDAPS) n’est pas requis. Pour plus d’informations sur la signature LDAP, consultez Comment activer la signature LDAP dans Windows Server et Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Niveaux fonctionnels Active Directory pris en charge

Le Connector Appliance a été testé et est pris en charge avec les niveaux fonctionnels de forêt et de domaine suivants dans Active Directory.

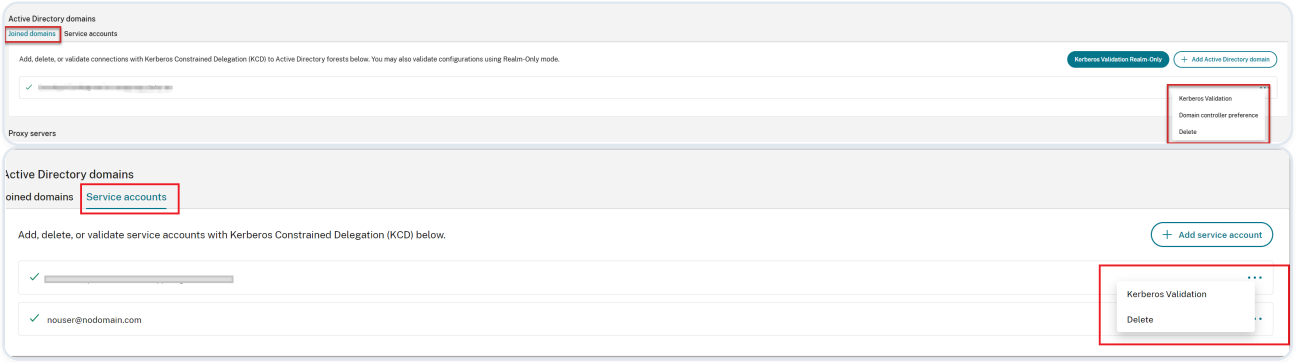
NIVEAU FONCTIONNEL DE LA FORÊT	NIVEAU FONCTIONNEL DU DOMAINE	CONTRÔLEURS DE DOMAINE PRIS EN CHARGE
Windows Server 2016	Windows Server 2016	Windows Server 2019

D’autres combinaisons de contrôleur de domaine, de niveau fonctionnel de forêt et de niveau fonctionnel de domaine n’ont pas été testées avec le Connector Appliance. Cependant, ces combinaisons devraient fonctionner et sont également prises en charge.

Connecter un domaine Active Directory à Citrix Cloud à l’aide de Connector Appliance

Lorsque vous vous connectez à la page web d’administration du Connector Appliance, la section des domaines Active Directory affiche deux onglets.

- **Domaines joints** – Utilisé pour joindre le Connector Appliance aux domaines AD en créant un compte d’ordinateur pour l’appliance dans le domaine. Kerberos peut être validé en cliquant sur le menu en forme de points de suspension sur le côté droit du domaine joint. La présence d’un compte d’ordinateur dans le domaine est requise.
- **Comptes de service** – Utilisé dans le cadre d’une solution Secure Private Access pour réaliser l’authentification unique Kerberos (SSO) à l’aide d’un compte de service au lieu du compte d’ordinateur créé en joignant le domaine. Kerberos peut être validé en cliquant sur le menu en forme de points de suspension sur le côté droit du compte de service. Il n’est pas obligatoire d’avoir un domaine spécifique associé à la machine. Cependant, même si le Connector Appliance n’est pas connecté au domaine, il peut toujours se connecter au contrôleur de domaine.



Pour configurer Active Directory afin de se connecter à Citrix Cloud via l'appliance de connecteur, suivez les étapes suivantes.

1. Installez une appliance de connecteur dans votre emplacement de ressources.

   Vous pouvez suivre les informations de la documentation produit de l'appliance de connecteur.
2. Connectez-vous à la page web d'administration de l'appliance de connecteur dans votre navigateur en utilisant l'adresse IP fournie dans la console de l'appliance de connecteur.
3. Dans la section **Domaines Active Directory**, accédez à l'onglet **Domaines joints**.
4. Cliquez sur **+ Ajouter un domaine Active Directory**, une nouvelle fenêtre contextuelle s'affiche pour saisir le nom de domaine.

   L'appliance de connecteur vérifie le domaine. Si la vérification est réussie, la boîte de dialogue **Joindre Active Directory** s'ouvre. Cette nouvelle fenêtre vous permet de saisir le nom d'utilisateur et le mot de passe pour joindre le domaine.
5. Cliquez sur **Ajouter**.
6. Fournissez le nom d'utilisateur et le mot de passe d'un utilisateur Active Directory disposant des autorisations de jonction pour le domaine.
7. L'appliance de connecteur suggère un nom de machine. Vous pouvez choisir de remplacer le nom suggéré et de fournir votre propre nom de machine, d'une longueur maximale de 15 caractères.

   Ce nom de machine est créé dans le domaine Active Directory lorsque l'appliance de connecteur le rejoint.
8. Cliquez sur **Joindre**.

   Le domaine est maintenant répertorié dans la section **Domaines Active Directory** de l'interface utilisateur de l'appliance de connecteur.
9. Pour ajouter d'autres **domaines Active Directory**, sélectionnez **+ Ajouter un domaine Active Directory** et répétez les étapes précédentes.
10. Accédez à la page des domaines dans **Citrix Cloud Console** et sélectionnez **Connector Appliance** pour gérer vos domaines.
11. Si vous n'avez pas encore enregistré votre Connector Appliance, poursuivez les étapes décrites dans Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Si vous recevez une erreur lors de la jonction au domaine, vérifiez que votre environnement répond aux exigences d'Active Directory et aux exigences réseau.

Et ensuite ?

- Vous pouvez ajouter d'autres domaines à ce Connector Appliance.

> **Remarque :**
>
> Le Connector Appliance est testé avec jusqu'à 10 forêts.

- Pour la résilience, ajoutez chaque domaine à plusieurs Connector Appliances dans chaque emplacement de ressources.

Affichage de votre configuration Active Directory

Vous pouvez afficher la configuration des domaines Active Directory et des Connector Appliances dans vos emplacements de ressources aux endroits suivants :

- Dans Citrix Cloud :
  a. Dans le menu, accédez à la page **Gestion des identités et des accès**.
  b. Accédez à l'onglet **Domaines**.

     Vos domaines Active Directory sont répertoriés avec les emplacements de ressources dont ils font partie.

- Dans la page web du Connector Appliance :
  a. Connectez-vous à la page web du Connector Appliance en utilisant l'adresse IP fournie dans la console du Connector Appliance.
  b. Connectez-vous avec le mot de passe que vous avez créé lors de votre première inscription.
  c. Dans la section **Domaines Active Directory** de la page, vous pouvez voir la liste des domaines Active Directory auxquels ce Connector Appliance est joint.

Suppression d'un domaine Active Directory d'un Connector Appliance

Pour quitter un domaine Active Directory, suivez les étapes suivantes :

1. Connectez-vous à la page web du Connector Appliance en utilisant l'adresse IP fournie dans la console du Connector Appliance.
2. Connectez-vous avec le mot de passe que vous avez créé lors de votre première inscription.

3. Dans la section **Domaines Active Directory** de la page, recherchez le domaine que vous souhaitez quitter dans la liste des domaines Active Directory joints.
4. Notez le nom du compte machine créé par votre Connector Appliance.
5. Cliquez sur l'icône de suppression (corbeille) à côté du domaine. Une boîte de dialogue de confirmation apparaît.
6. Cliquez sur **Continuer** pour confirmer l'action.
7. Accédez à votre contrôleur Active Directory.
8. Supprimez le compte machine créé par votre Connector Appliance du contrôleur.

Scénarios de déploiement pour l'utilisation de Connector Appliance avec Active Directory

Vous pouvez utiliser à la fois Cloud Connector et Connector Appliance pour vous connecter aux contrôleurs Active Directory. Le type de connecteur à utiliser dépend de votre déploiement.

Pour plus d'informations sur l'utilisation des Cloud Connectors avec Active Directory, consultez Scénarios de déploiement pour les Cloud Connectors dans Active Directory

Utilisez le Connector Appliance pour connecter votre emplacement de ressources à la forêt Active Directory dans les situations suivantes :

- Vous configurez Secure Private Access. Pour plus d'informations, consultez Secure Private Access avec Connector Appliance.
- Vous avez une ou plusieurs forêts qui sont uniquement utilisées pour l'authentification des utilisateurs
- Vous souhaitez réduire le nombre de connecteurs nécessaires pour prendre en charge plusieurs forêts
- Vous avez besoin d'un Connector Appliance pour d'autres cas d'utilisation

Uniquement des utilisateurs dans une ou plusieurs forêts avec un seul ensemble de Connector Appliances pour toutes les forêts

Ce scénario s'applique aux clients Workspace Standard ou aux clients utilisant Connector Appliance pour Secure Private Access.

Dans ce scénario, il existe plusieurs forêts qui ne contiennent que des objets utilisateur (`forest1.local`, `forest2.local`). Ces forêts ne contiennent pas de ressources. Un

ensemble de Connector Appliances est déployé au sein d'un emplacement de ressources et joint aux domaines de chacune de ces forêts.

- Relation d'approbation : Aucune
- Domaines répertoriés dans **Gestion des identités et des accès** : `forest1.local`, `forest2.local`
- Ouvertures de session utilisateur sur Citrix Workspace™ : Prises en charge pour tous les utilisateurs
- Ouvertures de session utilisateur sur un StoreFront™ sur site : Prises en charge pour tous les utilisateurs

Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un seul ensemble de Connector Appliances pour toutes les forêts

Ce scénario s'applique aux clients Citrix Virtual Apps and Desktops disposant de plusieurs forêts.

Dans ce scénario, certaines forêts (`resourceforest1.local`, `resourceforest2.local`) contiennent vos ressources (par exemple, des VDA) et certaines forêts (`userforest1.local`, `userforest2.local`) ne contiennent que vos utilisateurs. Une approbation existe entre ces forêts, ce qui permet aux utilisateurs de se connecter aux ressources.

Un ensemble de Cloud Connectors est déployé dans la forêt `resourceforest1.local`. Un ensemble distinct de Cloud Connectors est déployé dans la forêt `resourceforest2.local`.

Un ensemble de Connector Appliances est déployé dans la forêt `userforest1.local` et le même ensemble est déployé dans la forêt `userforest2.local`.

- Relation d'approbation : Approbation de forêt bidirectionnelle, ou approbation unidirectionnelle des forêts de ressources vers les forêts d'utilisateurs
- Domaines répertoriés dans **Gestion des identités et des accès** : `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.local`
- Connexions utilisateur à Citrix Workspace : Pris en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront sur site : Pris en charge pour tous les utilisateurs