Service d'authentification adaptative

Machine translated content

Disclaimer

Contents

Notes de publication

June 19, 2024

La note de mise à jour de l'authentification adaptative est un sous-ensemble des notes de publication de NetScaler. Les clients d'Adaptive Authentication doivent consulter les notes de version de NetScaler pour en savoir plus sur les améliorations, les problèmes résolus et les problèmes connus du service Adaptive Authentication.

> **Remarque :**
>
> La date indiquée dans ce document fait référence à la dernière date de mise à niveau du service.

16 Jan 2024

Nouveautés

- **Mise à niveau automatique des instances d'authentification adaptative**

Les instances d'authentification adaptative sont automatiquement mises à niveau vers les versions 14.1 à 12.35 et versions ultérieures, qui corrigent les vulnérabilités décrites dans le document CTX584986.

26 Sep 2023

Nouveautés

- **Mise à niveau automatique des instances d'authentification adaptative**

Les instances d'authentification adaptative sont automatiquement mises à niveau vers les versions 14.1 à 8.50 et versions ultérieures, qui corrigent les vulnérabilités décrites dans le document CTX579459.

18 juillet 2023

Nouveautés

- **Mise à niveau automatique des instances d'authentification adaptative**

Les instances d'authentification adaptative sont mises à niveau automatiquement vers les versions 13.1 à 49.101 et ultérieures qui corrigent les vulnérabilités de sécurité décrites dans le document CTX561482.

28 avril 2023

Nouveautés

- **Support LDAP et LDAPS avec équilibrage de charge**

  L'instance Citrix Adaptive Authentication fournit un support LDAP et LDAPS à l'aide d'un serveur virtuel d'équilibrage de charge. Pour plus de détails, voir Exemple de configuration d'équilibrage de charge LDAP et LDAPS.

  [AAUTH-2067]

- **Mappage des sous-réseaux du serveur principal AD ou RADIUS avec des emplacements de ressources**

  Les administrateurs peuvent choisir les connecteurs par lesquels les serveurs principaux AD et RADIUS doivent être accessibles. Pour plus de détails, consultez la section Provision d'une authentification adaptative.

Problèmes résolus

- Les stratégies d'accès intelligent et les stratégies d'authentification OAuth configurées pour l'authentification adaptative sont absentes de l'interface graphique de NetScaler.

  [AAUTH-68]

Problèmes connus

- Pour une instance d'authentification adaptative, lorsque vous utilisez l'option **Tester la connexion** dans le profil LDAP (interface graphique d'administration NetScaler) pour vérifier la connectivité, le serveur LDAP est affiché à tort comme étant accessible même s'il n'est pas accessible.

  [AAUTH-2111]

Configuration du service d'authentification adaptative

June 19, 2024

Les étapes de haut niveau suivantes sont nécessaires à la configuration du service d'authentification adaptative.

1. Provisionnez une authentification adaptative
2. Configuration des stratégies d'authentification adaptative
3. Activer l'authentification adaptative pour Workspace

Pré-requis

- Réservez un nom de domaine complet pour votre instance Adaptive Authentication. Par exemple `aauth.xyz.com`, en supposant que `xyz.com` c'est le domaine de votre entreprise. Ce nom de domaine complet est appelé nom de domaine complet du service d'authentification adaptative dans ce document et est utilisé lors du provisionnement de l'instance. Mappez le nom de domaine complet avec l'adresse IP publique du serveur virtuel IdP. Cette adresse IP est obtenue après le provisionnement à l'étape **Télécharger le certificat** .
- Procurez-vous un certificat pour aauth.xyz.com. Les certificats doivent contenir l'attribut SAN. Sinon, les certificats ne sont pas acceptés.
- L'interface utilisateur d'authentification adaptative ne prend pas en charge le téléchargement de lots de certificats. Pour lier un certificat intermédiaire, consultez la section Configurer des certificats intermédiaires.
- Choisissez votre type de connectivité pour la connectivité AD/RADIUS sur site. Les deux options suivantes sont disponibles. Si vous ne souhaitez pas que le centre de données soit accessible, utilisez le type de connectivité du connecteur.
  - **Citrix Cloud Connector** : pour plus de détails, consultez Citrix Cloud Connector.
  - **Azure VNet peering** : pour plus de détails, consultez Configuration de la connectivité aux serveurs d'authentification locaux à l'aide du peering AzureVNet.
- Configurez un serveur NTP (Network Time Protocol) pour éviter les décalages temporels. Pour plus de détails, consultez Comment synchroniser l'horloge système avec les serveurs du réseau.

Points à noter

- Citrix recommande de ne pas exécuter de configuration claire pour toute instance d'authentification adaptative ou de modifier toute configuration avec le préfixe AA (par exemple, AAuthAutoConfig), y compris les certificats. Cela perturbe la gestion de l'authentification adaptative et l'accès des utilisateurs est impacté. Le seul moyen de récupérer est le reprovisionnement.
- N'ajoutez pas SNIP ni aucune route supplémentaire sur l'instance Adaptive Authentication.
- L'authentification de l'utilisateur échoue si l'identifiant du client n'est pas entièrement en minuscules. Vous pouvez convertir votre identifiant en minuscules et le définir sur l'instance NetScaler à l'aide de la commande `set cloud parameter -customerID <all_lowercase_customerid>`.

- La configuration nFactor requise pour Citrix Workspace ou le service Citrix Secure Private Access est la seule configuration que les clients sont censés créer directement sur les instances. NetScaler ne contient actuellement aucun contrôle ou avertissement empêchant les administrateurs d'apporter ces modifications.
- Il est recommandé que toutes les configurations personnalisées soient effectuées dans l'interface utilisateur et non directement sur les instances d'authentification adaptative. En effet, les modifications apportées aux instances ne sont pas synchronisées automatiquement avec l'interface utilisateur et sont donc perdues.
- Ne mettez pas à niveau les instances Adaptive Authentication vers des versions RTM aléatoires. Toutes les mises à niveau sont gérées par Citrix Cloud.
- Seul un connecteur cloud basé sur Windows est pris en charge. L'appliance Connector n'est pas prise en charge dans cette version.
- Si vous êtes déjà client Citrix Cloud et que vous avez déjà configuré Azure AD (ou d'autres méthodes d'authentification), pour passer à l'authentification adaptative (par exemple, vérification de la posture de l'appareil), vous devez configurer l'authentification adaptative comme méthode d'authentification et configurer les stratégies d'authentification dans l'instance d'authentification adaptative. Pour plus de détails, consultez Connecter Citrix Cloud à Azure AD.
- Pour le déploiement du serveur RADIUS, ajoutez toutes les adresses IP privées du connecteur en tant que clients RADIUS sur le serveur RADIUS.
- Dans la version actuelle, l'agent ADM externe n'est pas autorisé et Citrix Analytics (CAS) n'est donc pas pris en charge.
- Le service NetScaler Application Delivery Management collecte la sauvegarde de votre instance d'authentification adaptative. Pour extraire la sauvegarde d'ADM, intégrez le service ADM. Pour plus de détails, voir Sauvegarde et restauration de la configuration. Citrix ne prend pas les sauvegardes explicitement à partir du service d'authentification adaptative. Les clients doivent effectuer la sauvegarde de leurs configurations à partir du service Application Delivery Management si nécessaire.
- Les instances d'authentification adaptative ne parviennent pas à établir le tunnel si un proxy est configuré dans la configuration du client. Par conséquent, il est recommandé de désactiver la configuration du proxy pour l'authentification adaptative.
- Si vous utilisez des services d'authentification tiers tels que SAML, l'authentification peut échouer si toutes les demandes ne sont pas trouvées. Par conséquent, il est recommandé aux clients d'ajouter un facteur supplémentaire tel que NOAUTH dans la configuration d'authentification multifactorielle pour répondre à toutes les demandes.
- Il est recommandé de garder le niveau du journal de débogage désactivé pendant les opérations normales et de ne l'activer que si nécessaire. Si le niveau du journal de débogage est toujours activé, cela entraîne une charge énorme sur le processeur de gestion. Cela peut entraîner des pannes du système lors de fortes charges de trafic. Pour plus d'informations, veuillez consulter l'article CTX222945.

Comment configurer le service d'authentification adaptative

Accéder à l'interface utilisateur Adaptive Authentication

Vous pouvez accéder à l'interface utilisateur Adaptive Authentication par l'une des méthodes suivantes.

- Saisissez manuellement l'URL https://adaptive-authentication.cloud.com.
- Connectez-vous à l'aide de vos informations d'identification et sélectionnez un client.

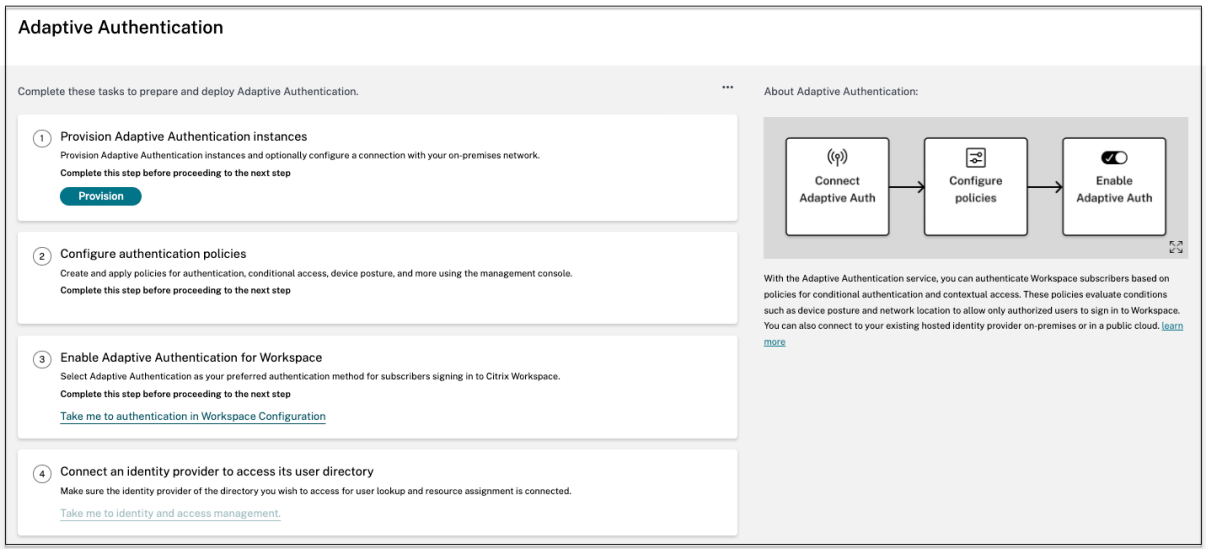
  Une fois que vous êtes authentifié avec succès, vous êtes redirigé vers l'interface utilisateur d'authentification adaptative.

OU

- Accédez à **Citrix Cloud > Gestion des identités et des accès**.
- Dans l'onglet Authentification, dans **Authentification adaptative**, cliquez sur le menu en ellipse et sélectionnez **Gérer**.

L'interface utilisateur Adaptive Authentication s'affiche.

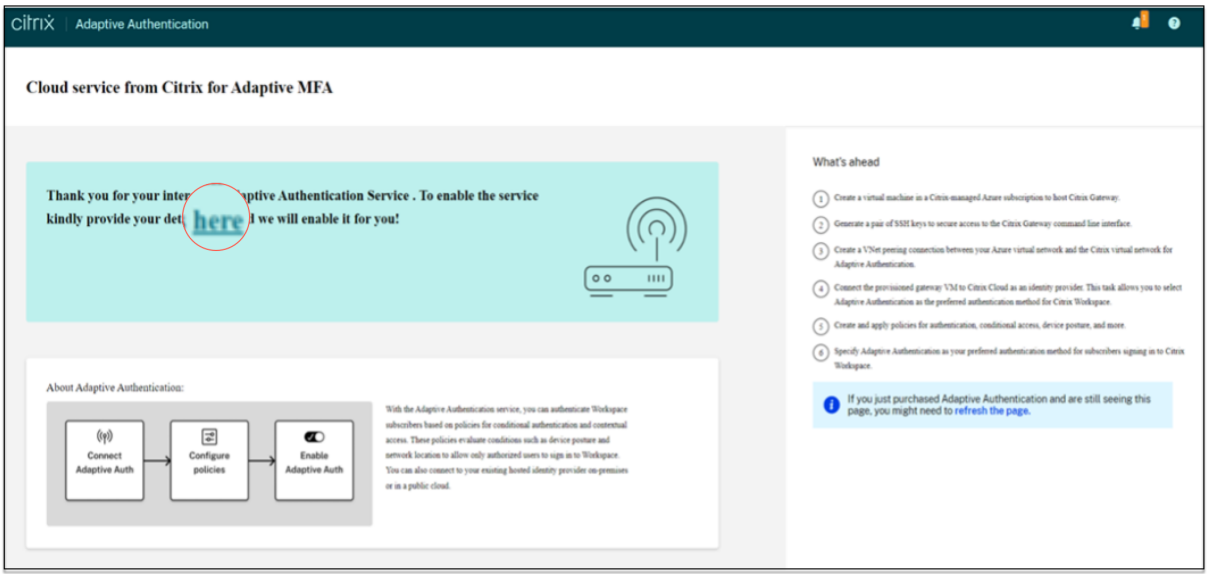
La figure suivante illustre les étapes de configuration de l'authentification adaptative.



Étape 1 : Provisionner l'authentification adaptative

> **Important :**
>
> les clients intéressés par le service d'authentification adaptative doivent cliquer sur le lien il-

> lustré dans la capture d'écran suivante et remplir le formulaire Podio. L'équipe Citrix Adaptive Authentication active ensuite le provisionnement des instances d'Authentification adaptative.



Procédez comme suit pour provisionner l'instance d'authentification adaptative :

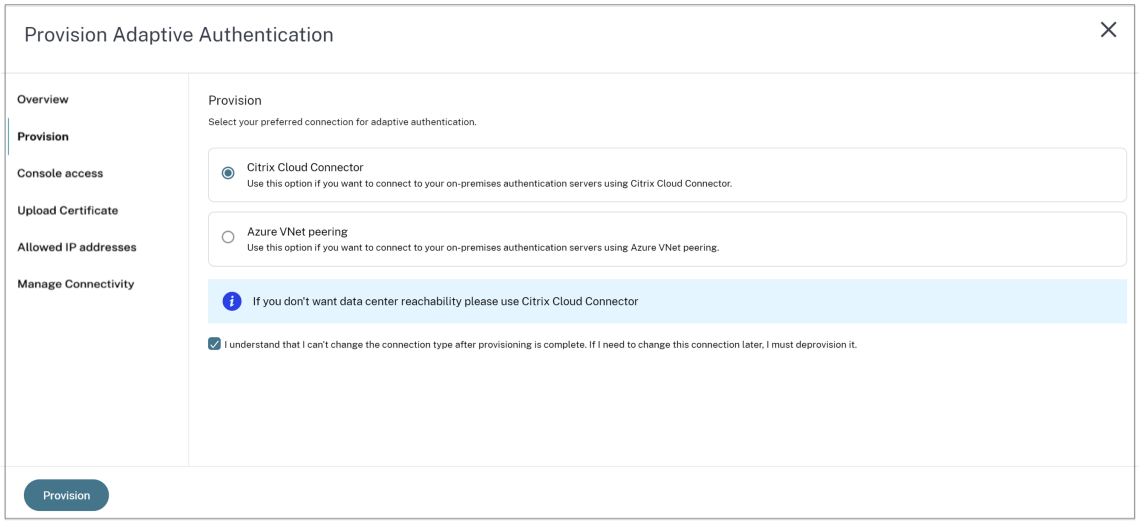
1. Dans l'interface utilisateur **d'authentification adaptative**, cliquez sur **Provisionner**
2. Sélectionnez la connexion préférée pour l'authentification adaptative.

    - **Citrix Cloud Connector :** pour ce type de connexion, vous devez configurer un connecteur sur votre réseau local. Citrix vous recommande de déployer au moins deux Citrix Cloud Connector dans votre environnement pour configurer la connexion à Citrix Gateway hébergé sur Azure. Vous devez autoriser votre Citrix Cloud Connector à accéder au domaine/URL que vous avez réservé à l'instance d'authentification adaptative. Par exemple, autorisez https://aauth.xyz.com/*.

      Pour plus de détails sur Citrix Cloud Connector, consultez Citrix Cloud Connector.

    - **Appairage de réseaux virtuels Azure** : vous devez configurer la connectivité entre les serveurs à l'aide de l'appairage de réseaux virtuels Azure.

        - Assurez-vous de disposer d'un compte d'abonnement Azure pour configurer la connectivité.
        - Le réseau virtuel du client qui est appairé doit déjà disposer d'une passerelle VPN Azure provisionnée. Pour plus de détails, consultez https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal.



Pour ajouter un Citrix Cloud Connector comme connexion préférée :

Effectuez les étapes suivantes.

- Sélectionnez l'option **Citrix Cloud Connector**, puis cochez la case du contrat utilisateur final.
- Cliquez sur **Provisionner**. La configuration du provisionnement peut prendre jusqu'à 30 minutes.

> **Remarque :**
>
> pour le type de connectivité du connecteur, assurez-vous que votre nom de domaine complet d'authentification adaptative est accessible depuis la machine virtuelle du connecteur après le provisionnement.

Pour configurer l'appairage de réseaux virtuels Azure :

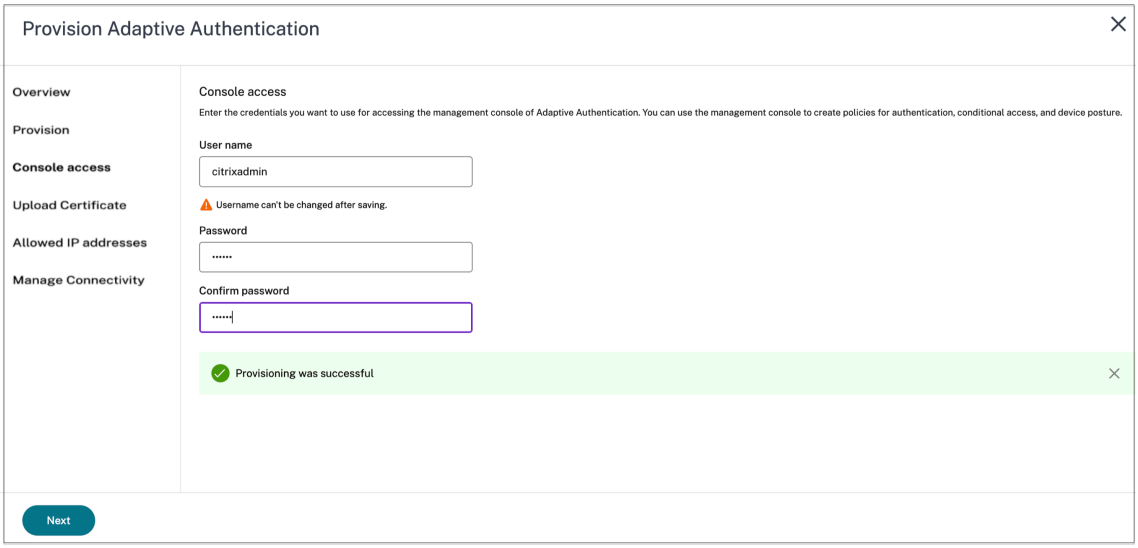
Si vous sélectionnez l'**appairage de réseau virtuel Azure** comme connexion, vous devez ajouter un bloc d'adresse CIDR de sous-réseau qui doit être utilisé pour provisionner l'instance Adaptive Authentication. Vous devez également vous assurer que le bloc d'adresse CIDR ne chevauche pas les autres plages réseau de votre organisation.

Pour plus de détails, consultez Configuration de la connectivité aux serveurs d'authentification locaux à l'aide de l'appairage de réseaux virtuels Azure.

3. Configurez les informations d'identification pour accéder aux instances que vous avez activées pour l'authentification adaptative. Vous avez besoin de l'accès à la console de gestion pour créer des stratégies d'authentification, d'accès conditionnel, etc.

   a) Dans l'écran **d'accès à la console**, entrez le nom d'utilisateur et le mot de passe.
   b) Cliquez sur **Suivant**.

> **Remarque :**
>
> Les utilisateurs créés à partir de l'écran d'**accès à la console** disposent de privilèges de « superutilisateur » qui ont accès au shell.



4. Ajoutez le nom de domaine complet du service Adaptive Authentication et chargez la paire de clés de certificat.
   Vous devez saisir le nom de domaine complet du service Adaptive Authentication de votre choix pour le serveur d'authentification accessible au public. Ce FQDN doit pouvoir être résolu publiquement.

   a) Dans l'écran **Télécharger le certificat**, entrez le nom de domaine complet que vous avez réservé pour l'authentification adaptative.

   b) Sélectionnez le type de certificat.

      - Le service d'authentification adaptative prend en charge les certificats de type PFX, PEM, DER pour le provisionnement des instances.
      - Le bundle de certificats n'est pris en charge que pour les certificats de type PEM. Pour les autres types de bundle, Citrix recommande d'installer les certificats racine et intermédiaire et de les lier au certificat du serveur.

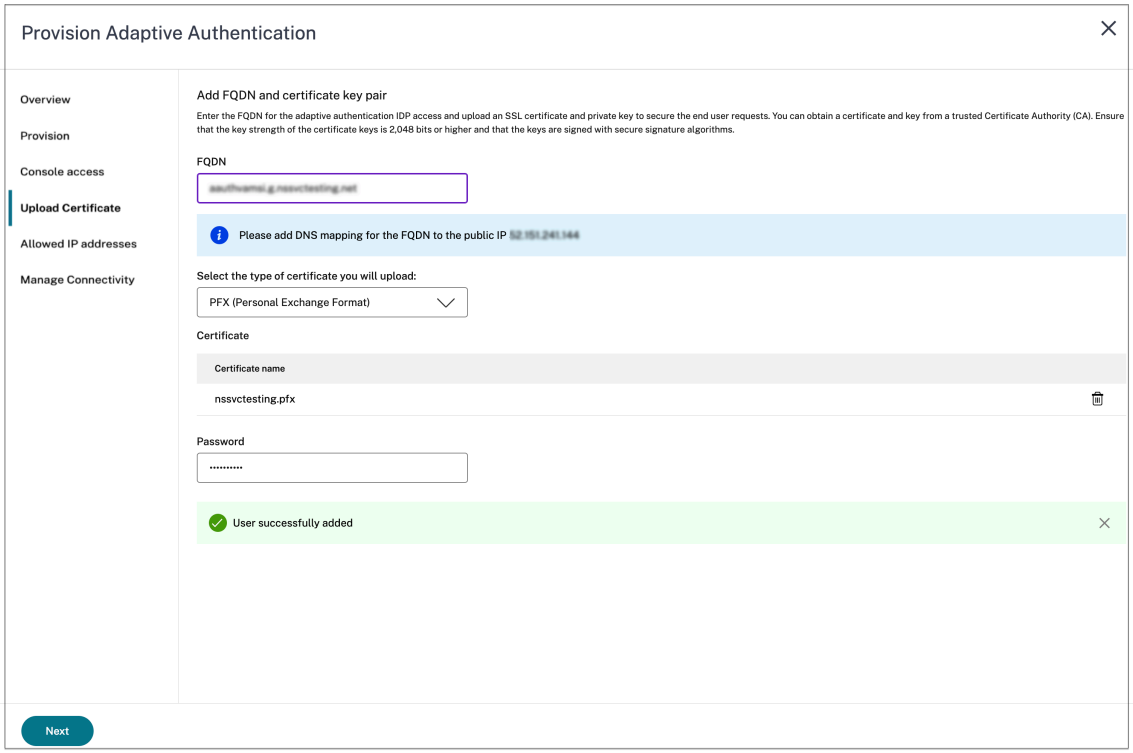
   c) Téléchargez le certificat et la clé.

> **Remarque :**
>
> - Installez votre certificat intermédiaire sur l'instance Adaptive Authentication et associez-le au certificat du serveur.
>
> ```
> 1. Connectez-vous à l'instance Adaptive Authentication. 1. Accédez à **Gestion du trafic > SSL**. Pour plus de dé
> ```



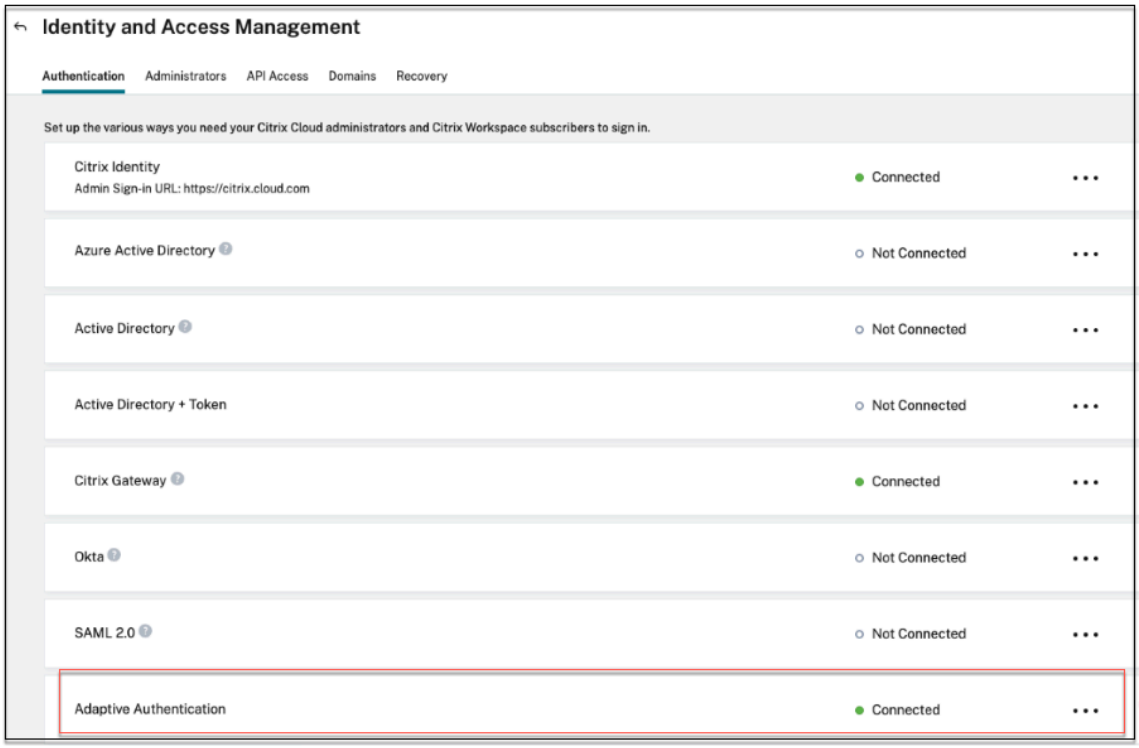
```
tails, consultez la section [Configuration des
certificats intermédiaires](/en-us/citrix-gateway/
current-release/install-citrix-gateway/certificate-
management-on-citrix-gateway/configure-intermediate-
certificate.html).
```

- Seuls les certificats publics sont acceptés. Les certificats signés par des autorités de certification privées ou inconnues ne sont pas acceptés.
- La configuration des certificats ou les mises à jour des certificats doivent être effectuées uniquement à l'aide de l'interface utilisateur d'authentification adaptative. Ne le modifiez pas directement sur l'instance car cela pourrait entraîner des incohérences.



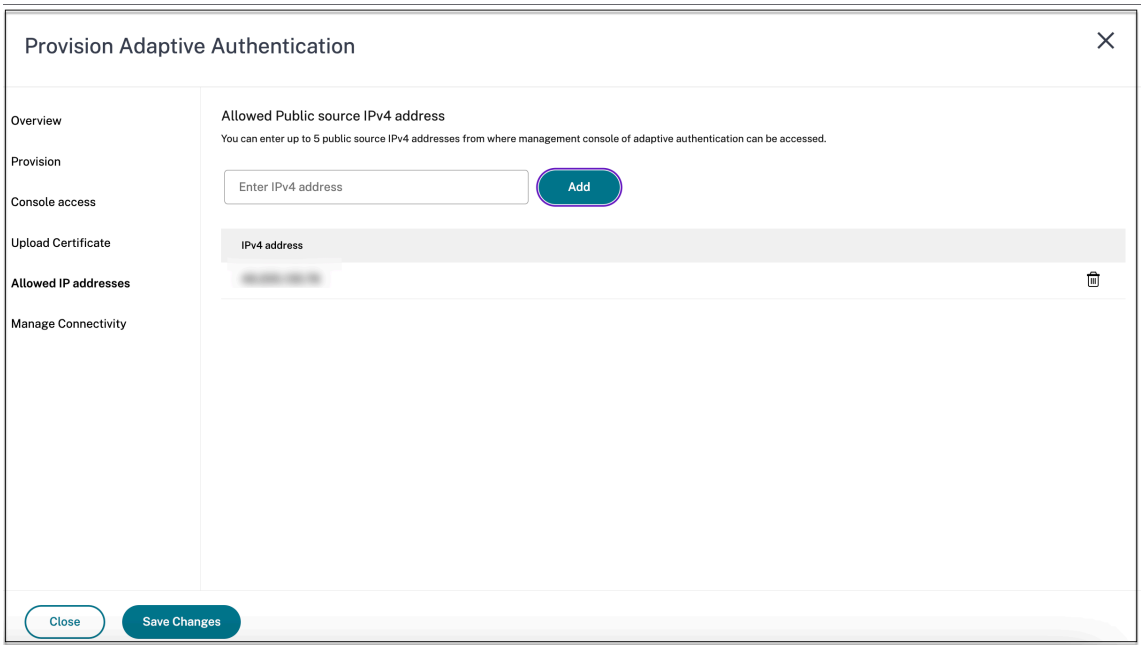
5. Téléchargez le certificat et la clé.

   L'instance Adaptive Authentication est désormais connectée au service Identity and Access Management. L'état de la méthode **d'authentification adaptative** s'affiche comme **Connecté**.



6. Configurez une adresse IP permettant d'accéder à la console de gestion de l'authentification adaptative.

    a) Dans l'écran **Adresses IP autorisées**, pour chaque instance, entrez une adresse IP publique comme adresse IP de gestion. Pour restreindre l'accès à l'adresse IP de gestion, vous pouvez ajouter plusieurs adresses IP autorisées à accéder à la console de gestion.
    b) Pour ajouter plusieurs adresses IP, vous devez cliquer sur **Ajouter**, saisir l'adresse IP, puis cliquer sur **Terminé**. Cela doit être fait pour chaque adresse IP. Si vous ne cliquez pas sur le bouton **OK**, les adresses IP ne sont pas ajoutées à la base de données mais uniquement dans l'interface utilisateur.



7. Si vous utilisez le type de connectivité du connecteur, spécifiez un ensemble d'emplacements de ressources (connecteurs) par lesquels les serveurs AD ou RADIUS sont accessibles. Si vous utilisez le type de connectivité d'appairage VNet, vous pouvez ignorer cette étape.

   Les administrateurs peuvent choisir les connecteurs par lesquels les serveurs principaux AD et RADIUS doivent être accessibles. Pour activer cette fonctionnalité, les clients peuvent configurer un mappage entre les sous-réseaux de leurs serveurs AD/RADIUS principaux de telle sorte que si le trafic d'authentification relève d'un sous-réseau spécifique, ce trafic soit dirigé vers l'emplacement de ressources spécifique. Toutefois, si un emplacement de ressources n'est pas mappé à un sous-réseau, les administrateurs peuvent spécifier d'utiliser l'emplacement de ressource générique pour ces sous-réseaux.

   Auparavant, le trafic d'authentification adaptative pour AD/RADIUS sur site était dirigé vers n'importe quel emplacement de ressources disponible à l'aide de la méthode circulaire. Cela a causé des problèmes aux clients disposant de plusieurs sites de ressources.

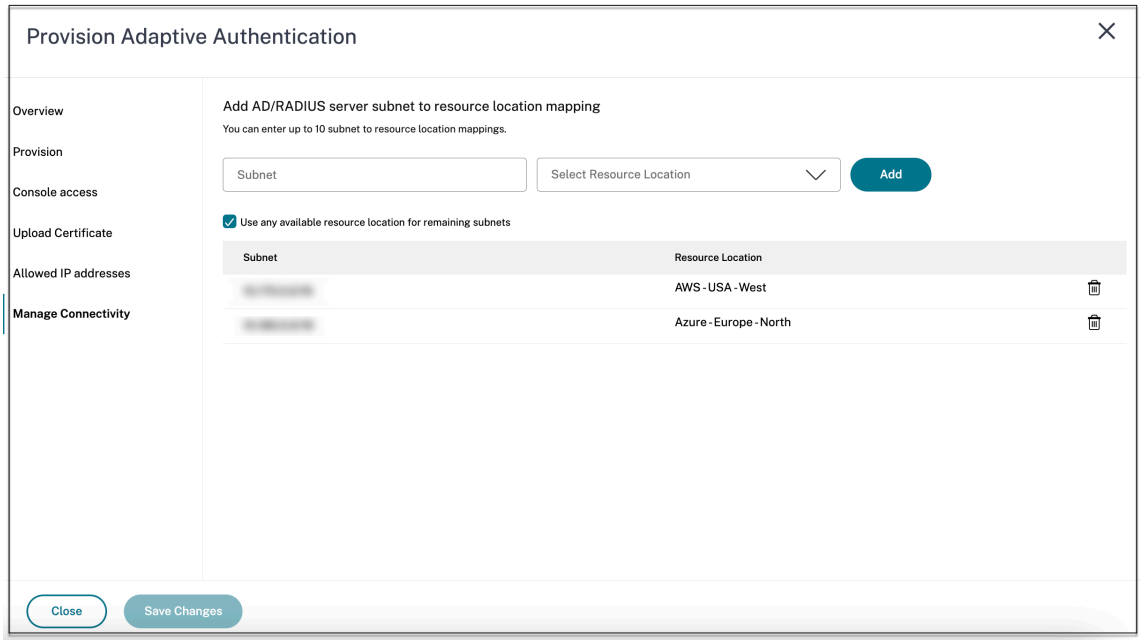
   a) Dans l'interface utilisateur de l'authentification adaptative, cliquez sur **Gérer la connectivité**.

   b) Entrez les détails du sous-réseau et sélectionnez l'emplacement de ressources correspondant.

      > **Remarque :**
      >
      > Si vous désactivez la case à cocher **Utiliser n'importe quel emplacement de ressource disponible pour les sous-réseaux restants**, seul le trafic dirigé vers les sous-réseaux configurés est tunnelisé.

c) Cliquez sur **Ajouter**, puis sur **Enregistrer les modifications**.

> **Remarque :**
>
> - Seuls les sous-réseaux d'adresses IP RFC1918 sont autorisés.
> - Le nombre de mappages de localisation des ressources du sous-réseau par client est limité à 10.
> - Plusieurs sous-réseaux peuvent être mappés vers un seul emplacement de ressources.
> - Les entrées dupliquées ne sont pas autorisées pour le même sous-réseau.
> - Pour mettre à jour l'entrée du sous-réseau, supprimez l'entrée existante, puis mettez-la à jour.
> - Si vous renommez ou supprimez l'emplacement des ressources, veillez à supprimer l'entrée de l'écran **Gérer la connectivité** de l'interface utilisateur d'authentification adaptative.
> - Toute modification apportée au mappage de l'emplacement des ressources à l'aide des commandes CLI suivantes est remplacée par les modifications apportées depuis l'interface utilisateur (**Adaptive Authentication Provisioning > Gérer**la connectivité).
>
> ```
> - set cloudtunnel parameter -subnetResourceLocationMappings
>
> - set policy expression aauth_allow_rfc1918_subnets
>   <>
> - set policy expression aauth_listen_policy_exp <>
> ```

> Provisioning de l'authentification adaptative est désormais terminé.

Étape 2 : Configuration des stratégies d'authentification adaptative

Comment se connecter à votre instance d'authentification adaptative :

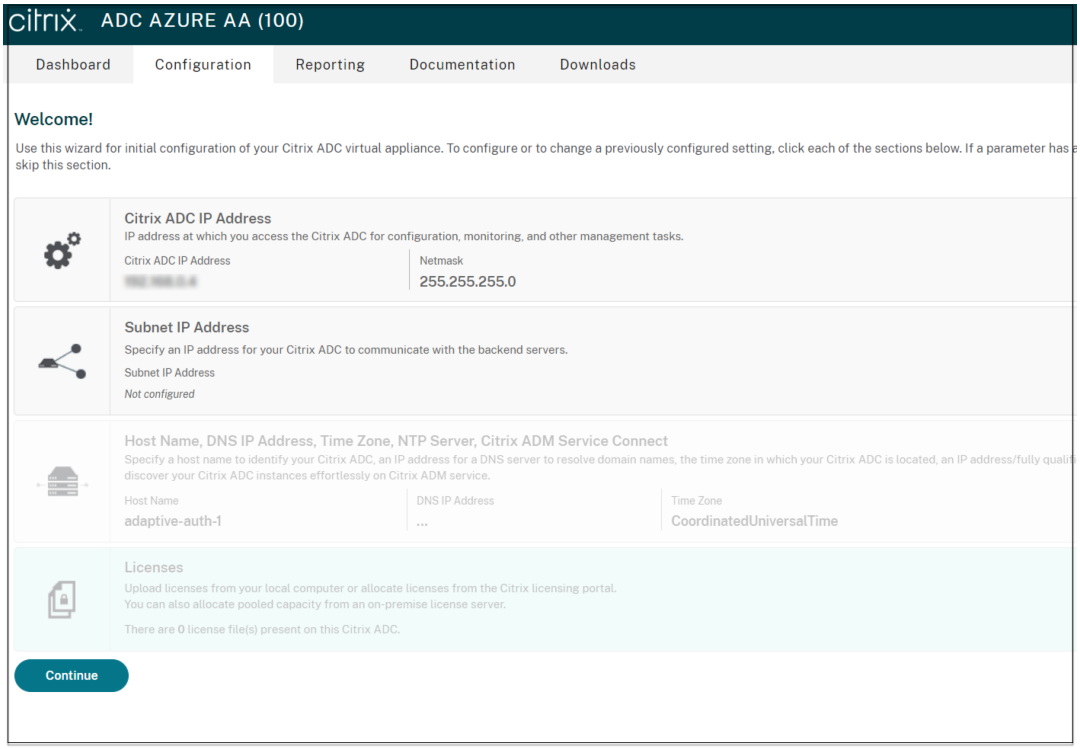
Après le provisionnement, vous pouvez accéder directement à l'adresse IP de gestion de l'authentification adaptative. Vous pouvez accéder à la console de gestion de l'authentification adaptative à l'aide du nom de domaine complet ou de votre adresse IP principale.

> **Important :**
>
> - Dans une configuration haute disponibilité, dans le cadre du processus de synchronisation, les certificats sont également synchronisés. Veillez donc à utiliser le certificat générique.
> - Si vous avez besoin d'un certificat unique pour chaque nœud, chargez les fichiers et les clés du certificat dans n'importe quel dossier qui n'est pas synchronisé (par exemple, créez un dossier distinct (nosync_cert) dans le répertoire NSConfig/SSL), puis chargez le certificat de manière unique sur chaque nœud.

Accédez à la console de gestion de l'authentification adaptative :

- Pour accéder à la console de gestion de l'authentification adaptative à l'aide du nom de domaine complet, voir Configurer SSL pour l'accès à l'interface utilisateur d'ADC Admin.
- Pour accéder à l'authentification adaptative à l'aide de votre adresse principale, procédez comme suit :

1. Copiez l'adresse IP principale depuis la section **Configurer les stratégies d'authentification** de l'interface graphique et accédez à l'adresse IP dans votre navigateur.
2. Connectez-vous à l'aide des informations d'identification que vous avez saisies lors de l'approvisionnement.
3. Cliquez sur **Continuer**.



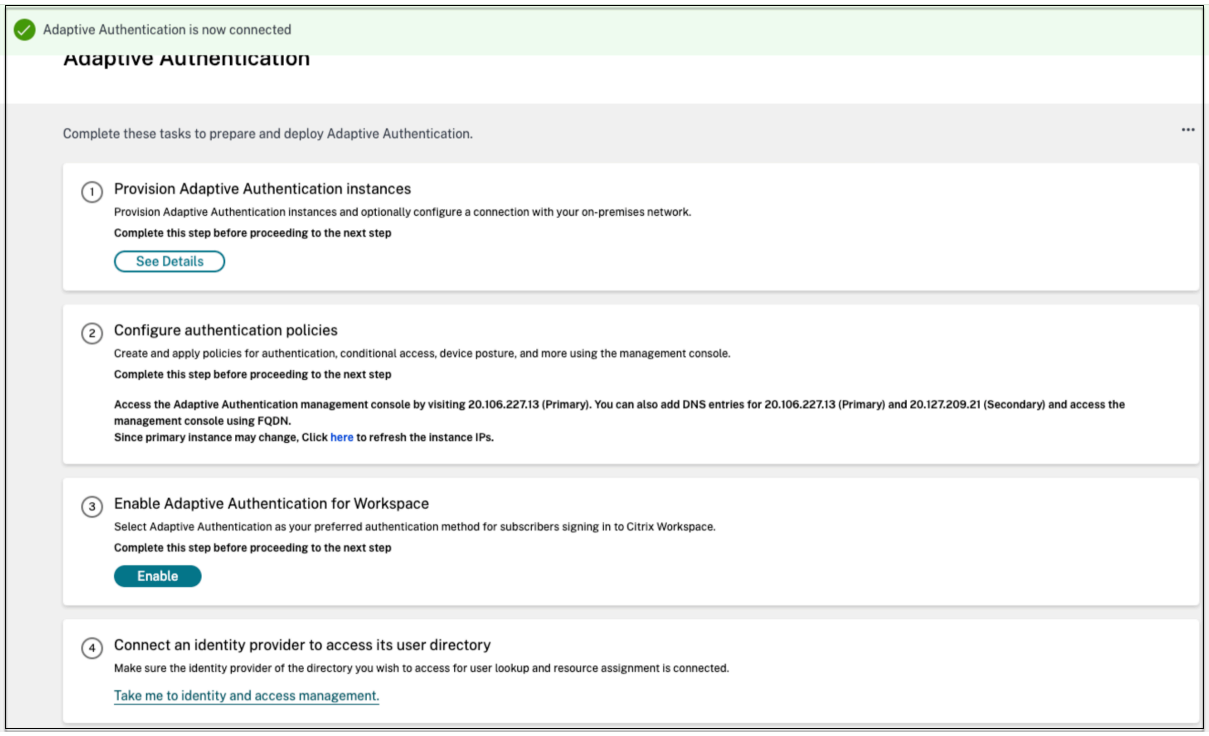
4. Accédez à **Configuration > Sécurité > AAA - Trafic des applications > Serveurs virtuels**.
5. Ajoutez les stratégies d'authentification. Pour différents cas d'utilisation, voir Exemples de configurations d'authentification.

> **Remarque :**
>
> l'accès à l'instance d'authentification adaptative à l'aide de l'adresse IP n'est pas fiable et de nombreux navigateurs bloquent l'accès par des avertissements. Nous vous recommandons d'accéder à la console de gestion de l'authentification adaptative avec le nom de domaine complet pour éviter toute barrière de sécurité. Vous devez réserver le nom de domaine complet pour la console de gestion Adaptive Authentication et le mapper avec l'adresse IP de gestion principale et secondaire.
>
> Par exemple, si l'adresse IP de votre instance d'authentification adaptative est 192.0.2.0 et secondaire : 192.2.2.2, alors ;

- primary.domain.com peut être mappé à 192.0.2.0
- secondary.domain.com peut être mappé à 192.2.2.2

Étape 3 : activer l'authentification adaptative pour Workspace

Une fois le provisionnement terminé, vous pouvez activer l'authentification pour Workspace en cliquant sur **Activer** dans la section **Activer l'authentification adaptative pour Workspace** .



Remarque :

La configuration de l'authentification adaptative est ainsi terminée. Lorsque vous accédez à l'URL de votre espace de travail, vous devez être redirigé vers le FQDN d'authentification adaptative.

Références connexes

- Modifier un nom de domaine complet
- Planifier la mise à niveau de vos instances d'authentification
- Déprovisionner vos instances Adaptive Authentication
- Permettre un accès sécurisé à la passerelle
- Configuration de la connectivité aux serveurs d'authentification locaux à l'aide de l'appairage de réseaux virtuels Azure
- URL personnalisée de l'espace de travail ou URL personnalisée

- Sauvegarde et restauration de configuration
- Exemple de configuration LDAPS à charge équilibrée
- Migrez votre méthode d'authentification vers l'authentification adaptative
- Exemples de configurations d'authentification

Configurations d'authentification adaptative associées

October 21, 2024

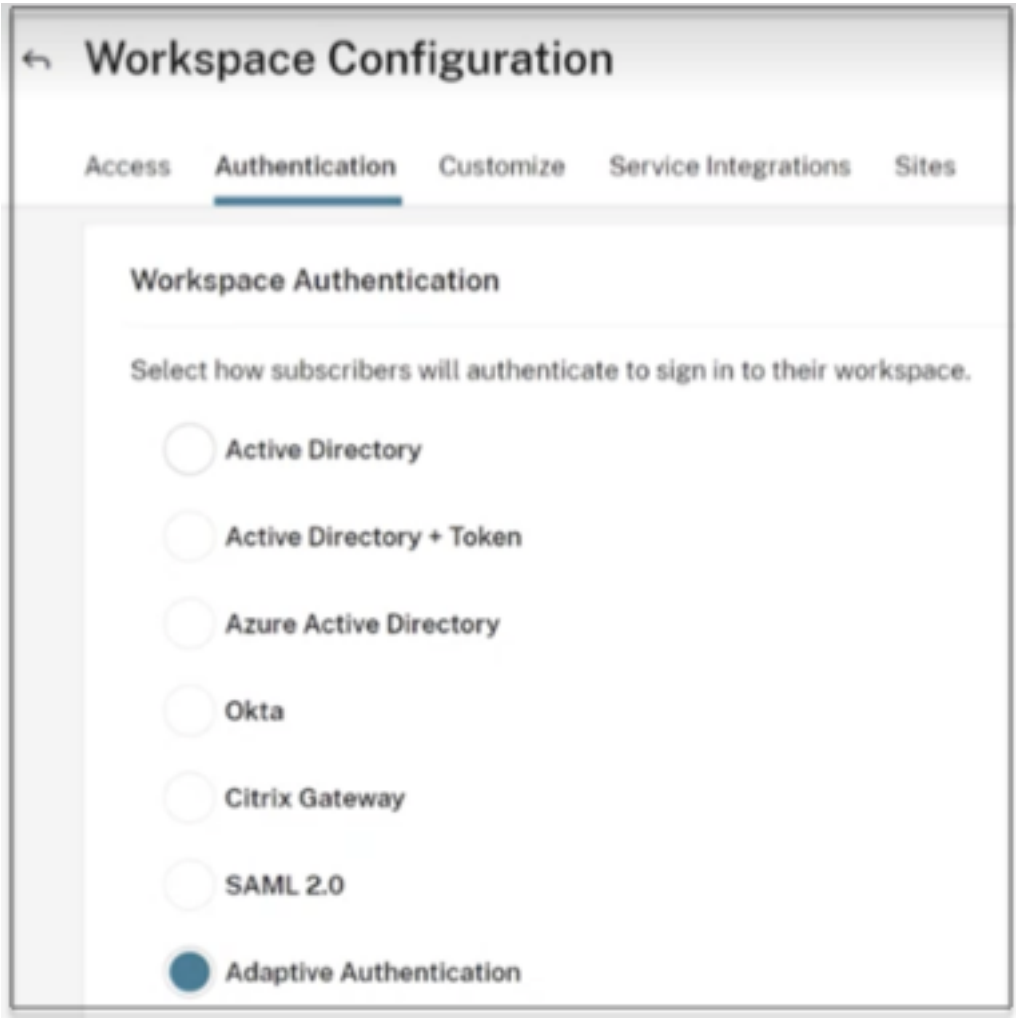
Modifier un FQDN

Vous ne pouvez pas modifier un FQDN si **Authentification adaptative** est sélectionné comme méthode d'authentification dans la configuration de l'espace de travail. Vous devez passer à une autre méthode d'authentification pour modifier le FQDN. Cependant, vous pouvez modifier le certificat si nécessaire.

> **Important :**
>
> - Avant de modifier le FQDN, assurez-vous que le nouveau FQDN est mappé à l'adresse IP publique du serveur virtuel IdP.
> - Les utilisateurs existants qui sont connectés à **Citrix Gateway** à l'aide de stratégies OAuth doivent migrer votre méthode d'authentification vers **Adaptive Authentication**. Pour plus de détails, voir Migrez votre méthode d'authentification vers l'authentification adaptative.

Pour modifier un FQDN, procédez comme suit :

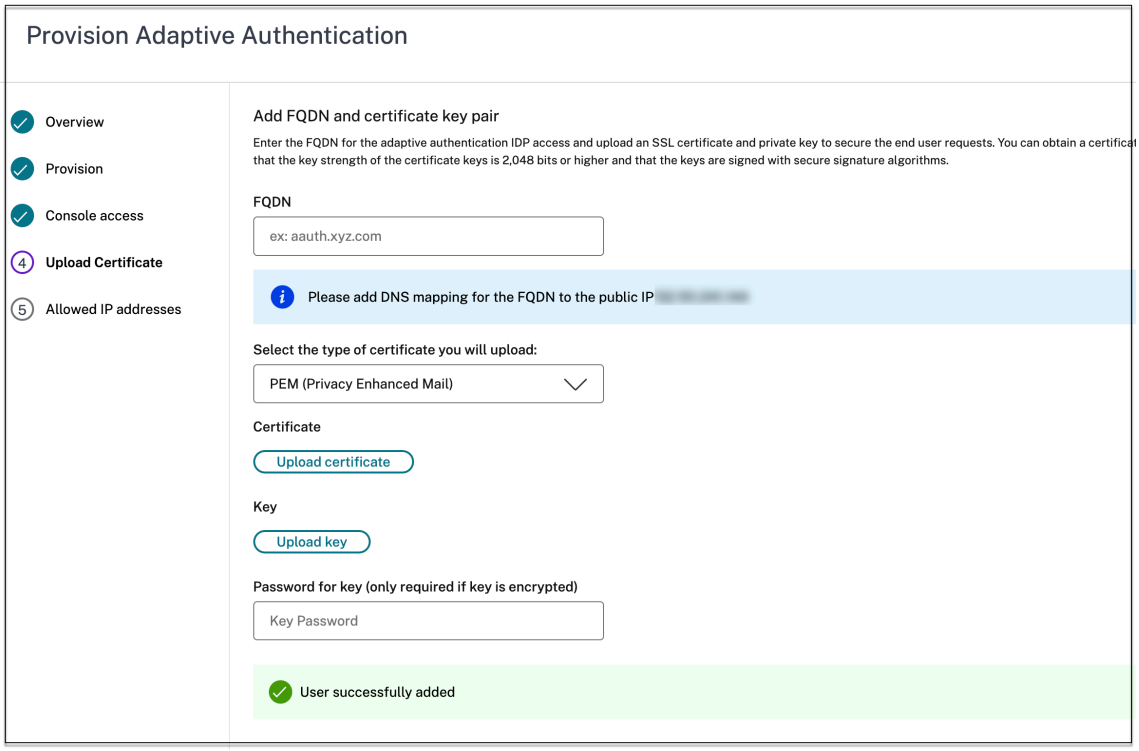
1. Passer à une méthode d'authentification différente de **Authentification adaptative**.



2. Sélectionnez **Je comprends l'impact sur l'expérience de l'abonné,** puis cliquez sur **Confirmer**.

   Lorsque vous cliquez sur **Confirmer**, la connexion à l'espace de travail des utilisateurs finaux est affectée et l'authentification adaptative n'est pas utilisée pour l'authentification jusqu'à ce que l'authentification adaptative soit à nouveau activée. Il est donc recommandé de modifier le FQDN pendant une fenêtre de maintenance.

3. Dans l'écran **Télécharger le certificat** , modifiez le FQDN.



4. Cliquez sur **Enregistrer les modifications**.

> **Important :**
>
> Si vous modifiez un FQDN, vous devez également télécharger à nouveau le certificat.

1. Réactivez la méthode d'authentification adaptative en cliquant sur **Activer** (étape 3) dans la page d'accueil de l'authentification adaptative.

2. Cliquez sur **Actualiser**.

URL d'espace de travail personnalisé ou URL personnalisée

Une URL d'espace de travail personnalisée vous permet d'utiliser un domaine de votre choix pour accéder à votre magasin Citrix Workspace. Les utilisateurs peuvent accéder à l'espace de travail à l'aide de l'URL de l'espace de travail par défaut ou de l'URL de l'espace de travail personnalisé ou des deux.

Pour configurer une URL d'espace de travail personnalisée ou une URL personnalisée, vous devez procéder comme suit :

1. Configurez votre domaine personnalisé. Pour plus de détails, voir Configuration de votre domaine personnalisé.
2. Configurez un nouveau profil OAuthIDP avec le même ID client, le même secret et la même audience que votre profil actuel ou par défaut (AAuthAutoConfig_oauthIdpProf) mais avec une URL de redirection différente. Pour plus de détails, voir Configuration des politiques et des profils OAuth.

   Exemple :

   Profil actuel :

   ```
   -add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf
    -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
   ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https
   ://accounts-internal.cloud.com/core/login-cip"-audience zzzz -
   sendPassword ON

   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol -
   rule true -action AAuthAutoConfig_oauthIdpProf

   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol
    -priority 100 -gotoPriorityExpression NEXT
   ```

   Nouveau profil:

   ```
   add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf_Custom1
    -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
   ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://
   custom_domain/core/login-cip"-audience zzzz -sendPassword ON

   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol_Custom1
    -rule true -action AAuthAutoConfig_oauthIdpProf_Custom1

   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol_Cu
    -priority 101 -gotoPriorityExpression NEXT
   ```

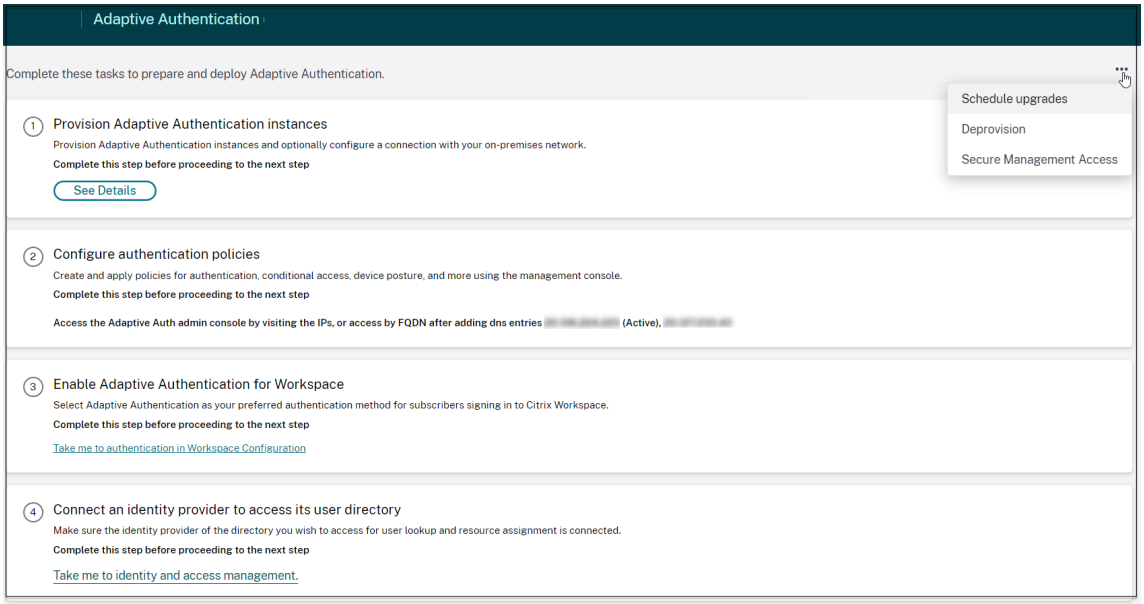
> **Important :**
>
> - La politique et le profil OAuth sont créés par le service d'authentification adaptative pendant la phase de provisionnement. Par conséquent, l'administrateur Citrix Cloud n'a pas accès au secret client non chiffré. Vous pouvez obtenir le secret chiffré à partir du fichier ns.conf. Pour créer un profil OAuth, vous devez utiliser le secret chiffré et créer le profil à l'aide uniquement des commandes CLI.
> - Vous ne pouvez pas créer de profil OAuth à l'aide de l'interface utilisateur NetScaler.

Planifiez la mise à niveau de vos instances d'authentification adaptative

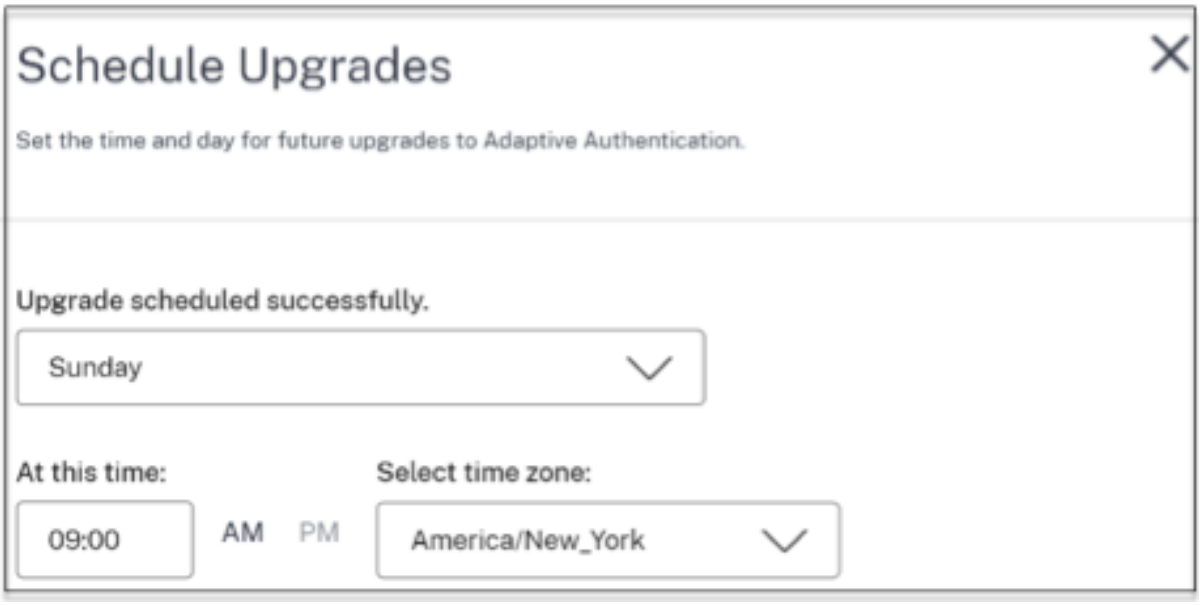
Pour le site ou le déploiement actuel, vous pouvez sélectionner la fenêtre de maintenance pour la mise à niveau.

> **Important :**
>
> Ne mettez pas à niveau les instances d'authentification adaptative vers des versions RTM aléatoires. Toutes les mises à niveau sont gérées par Citrix Cloud.

1. Dans l'interface utilisateur d'Authentification adaptative ** , dans la section **Provisionner les instances d'Authentification adaptative , cliquez sur le bouton points de suspension.



2. Cliquez sur **Planifier les mises à niveau**.
3. Sélectionnez le jour et l'heure de la mise à niveau.



Désapprovisionnez vos instances d'authentification adaptative

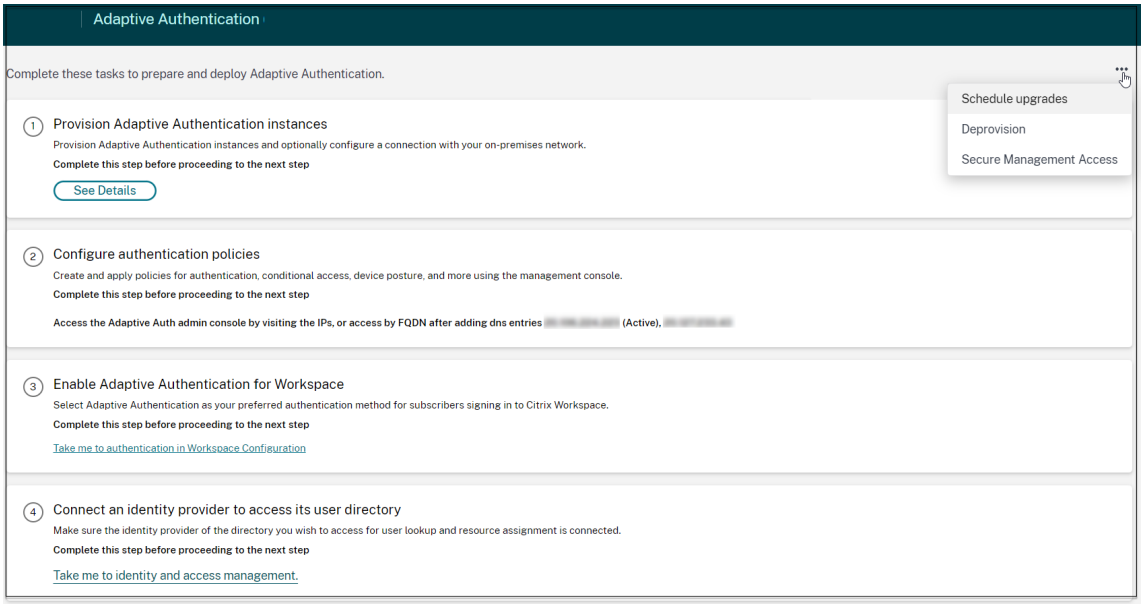
Les clients peuvent annuler la fourniture des instances d'authentification adaptative dans les cas suivants et conformément aux suggestions du support Citrix.

- Les instances d'authentification adaptative ne sont pas accessibles (en particulier après une mise à niveau planifiée), bien que ce scénario puisse ne pas se produire.
- Si le client doit passer du mode peering VNet au mode connecteur ou inversement.
- Si le client a sélectionné un sous-réseau incorrect au moment de la mise en service du mode de peering VNet (le sous-réseau est en conflit avec d'autres sous-réseaux de son centre de données ou de son réseau virtuel Azure).

> **Remarque**
>
> Le déprovisionnement supprime également la sauvegarde de configuration des instances. Vous devez donc télécharger les fichiers de sauvegarde et les enregistrer avant de déprovisionner vos instances Adaptive Authentication.

Pour annuler l'approvisionnement d'une instance d'Adaptive Authentication, procédez comme suit :

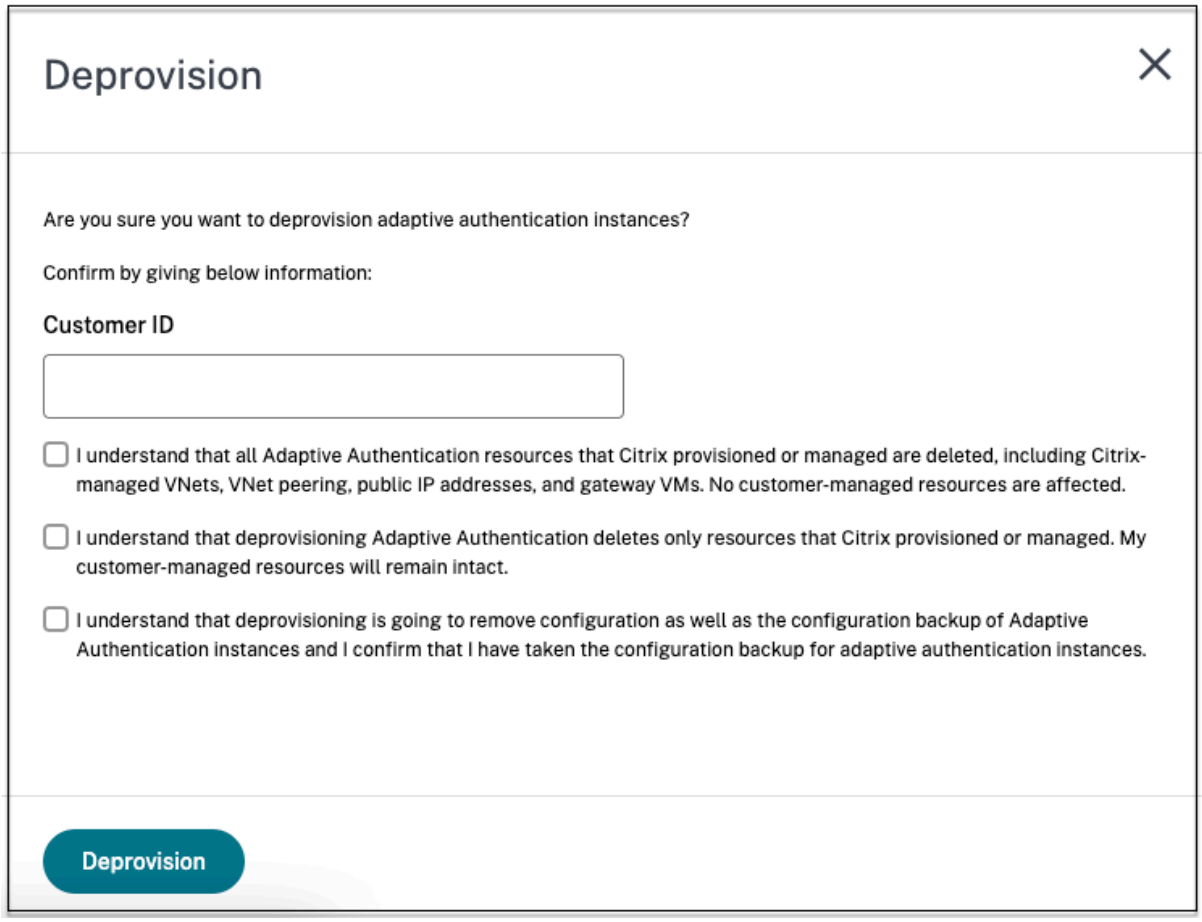
1. Dans l'interface utilisateur d'Authentification adaptative ** , dans la section **Provisionner les instances d'Authentification adaptative** , cliquez sur le bouton points de suspension.



2. Cliquez sur **Déprovisionner**.

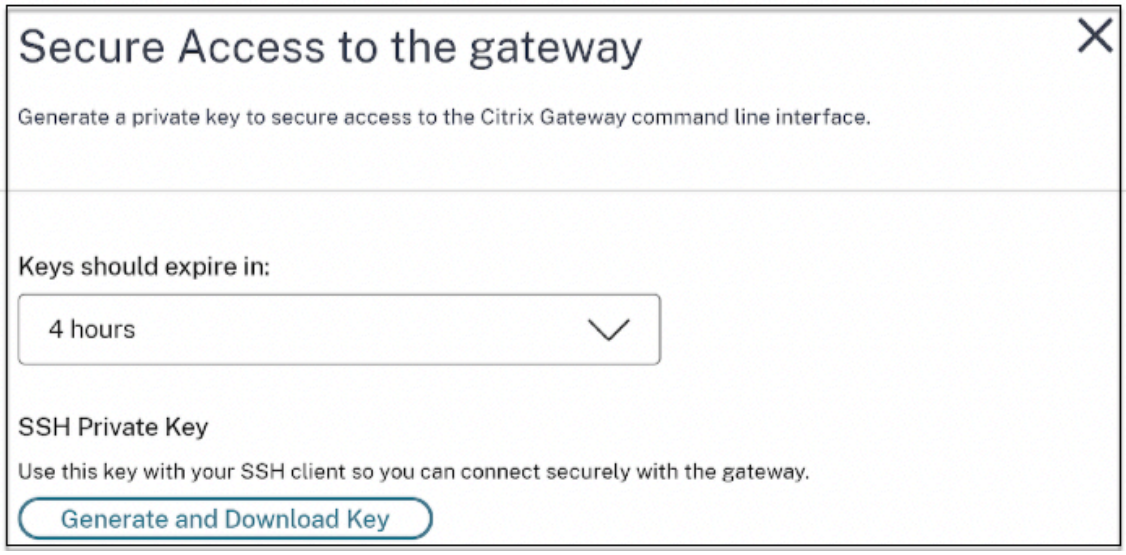
> **Remarque**
>
> Avant le déprovisionnement, vous devez déconnecter **Citrix Gateway** de la configuration de l'espace de travail.

1. Saisissez l'ID client pour annuler la fourniture des instances d'authentification adaptative.



Activer l'accès sécurisé à la passerelle

1. Dans l'interface utilisateur d'Authentification adaptative ** **, dans la section **Provisionner les instances d'Authentification adaptative** , cliquez sur le bouton points de suspension.
2. Cliquez sur **Accès à la gestion sécurisée**.



3. Dans **Les clés doivent expirer dans**, sélectionnez une durée d'expiration pour la nouvelle clé SSH.
4. Cliquez sur **Générer et télécharger les clés**. Copiez ou téléchargez la clé privée SSH pour une utilisation ultérieure car elle ne s'affiche pas après la fermeture de la page. Cette clé peut être utilisée pour se connecter aux instances d'authentification adaptative avec le nom d'utilisateur `authadmin`.

   Vous pouvez cliquer sur **Générer et télécharger les clés** pour créer une nouvelle paire de clés si la paire de clés précédente expire. Cependant, une seule paire de clés peut être active.
5. Cliquez sur **Terminé**.

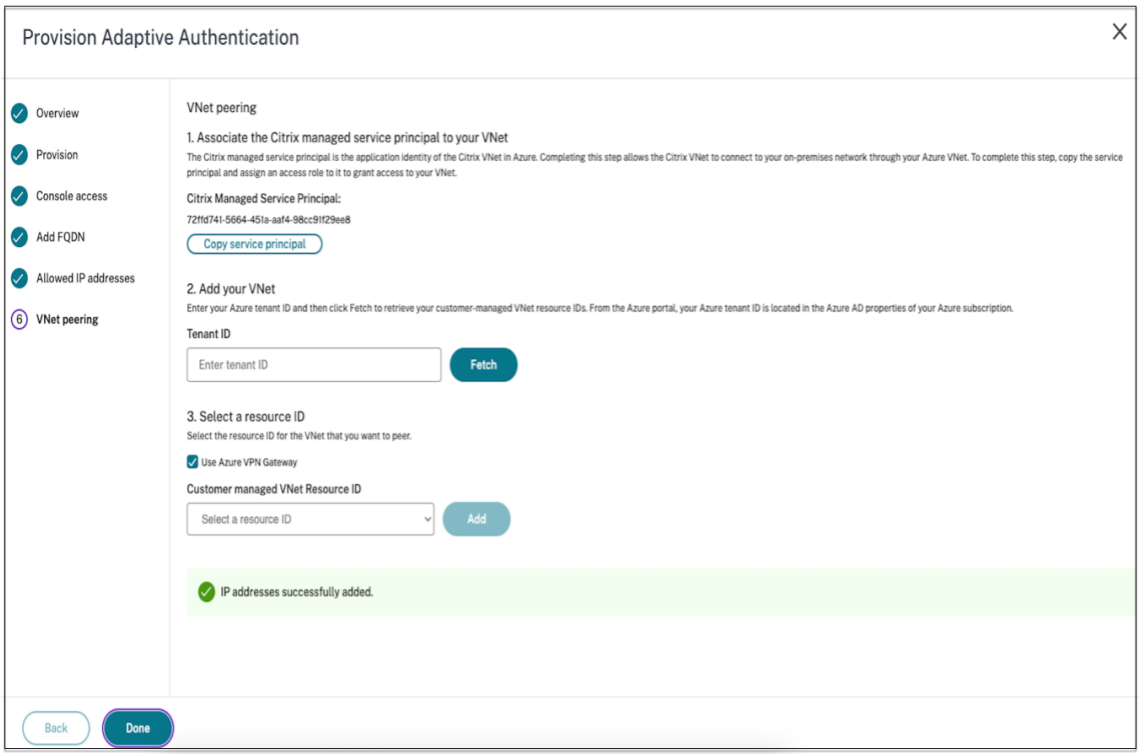
> **Important :**
>
> - Si vous utilisez PuTTY sous Windows pour vous connecter aux instances d'authentification adaptative, vous devez convertir la clé privée téléchargée en PEM. Pour plus de détails, consultez la section https://www.puttygen.com/convert-pem-to-ppk.
> - Il est recommandé d'utiliser la commande suivante pour se connecter aux instances d'authentification adaptative via le terminal à partir du MAC ou de l'invite de commande PowerShell/de Windows (version 10). `ssh -i <path-to-private-key> authadmin@<ip address of ADC>`
> - Si vous souhaitez que les utilisateurs AD accèdent à l'interface graphique d'authentification adaptative, vous devez les ajouter en tant que nouveaux administrateurs au groupe LDAP. Pour plus de détails, consultez https://support.citrix.com/article/CTX123782. Pour toutes les autres configurations, Citrix vous recommande d'utiliser l'interface graphique d'authentification adaptative et non les commandes CLI.

Configurer la connectivité aux serveurs d'authentification locaux à l'aide du peering Azure VNet

Vous devez configurer cette configuration uniquement si vous avez sélectionné le type de connectivité comme peering Azure VNet.

> **Remarque**
>
> Si vous utilisez des IDP tiers tels qu'Okta, Azure AD, Ping, cette étape n'est pas obligatoire.

1. Dans l'interface utilisateur Connect Adaptive Authentication, cliquez sur **Provision**, puis sur **Azure VNet Peering**.



Le champ **Citrix Managed Service Principal** contient l'ID d'application d'un principal de service Azure créé par Citrix pour votre client. Ce principal de service est requis pour permettre à Citrix d'ajouter un peering VNet à un VNet dans votre abonnement et votre locataire.

Pour permettre à ce principal de service de se connecter au locataire client, l'administrateur du site client (administrateur global du locataire) doit exécuter les commandes PowerShell suivantes pour ajouter le SPN au locataire. CloudShell peut également être utilisé. `Connect-AzureAD New-AzureADServicePrincipal -AppId $App_ID` Où `$App_ID` est un ID d'application SPN partagé par Citrix.

Remarque

- La commande mentionnée précédemment génère un nom de principal de service qui doit être utilisé pour les attributions de rôles.
- Pour permettre à ce principal de service d'ajouter un peering Azure VNet, l'administrateur du site client (non limité à l'administrateur global) doit ajouter un rôle « Contributeur réseau » au VNet qui doit être lié au VNet géré par Citrix.
- SPN est un identifiant unique utilisé pour associer le réseau virtuel Citrix dans Azure. L'association du SPN au VNet permet au réseau virtuel Citrix de se connecter au réseau local des clients via le VNet d'Azure.

1. Créer un peering VNet.

    - Saisissez l'ID du locataire pour lequel les étapes précédentes ont été exécutées et cliquez sur **Récupérer**.

    Cela renseigne l'ID de ressource VNet géré par le client avec les VNets candidats pour lesquels le rôle de contributeur réseau est ajouté pour le SPN. Si vous ne voyez pas votre VNet, assurez-vous que les étapes précédentes sont exécutées correctement ou répétez les étapes.

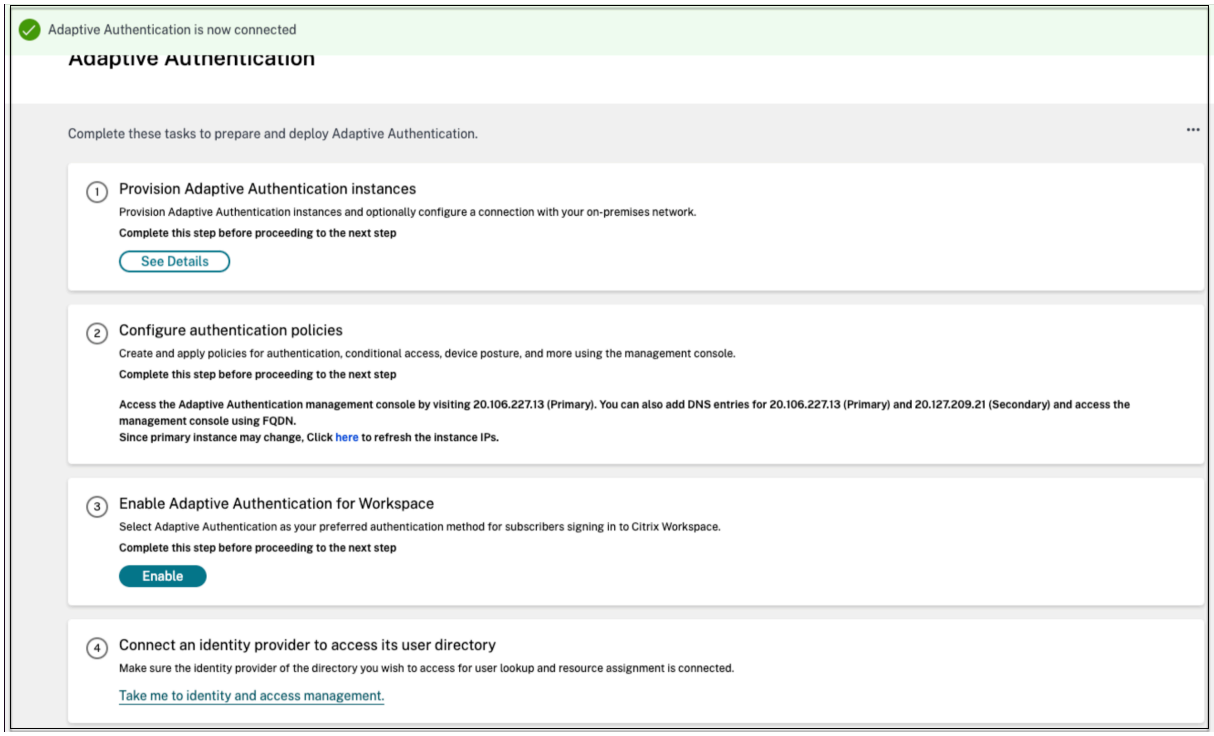
Remarque

Pour plus de détails sur la façon de trouver votre ID de locataire, consultez https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant.

1. Sélectionnez **Utiliser la passerelle VPN Azure** pour connecter vos réseaux locaux à Azure.
2. Dans **ID de ressource VNet géré par le client**, sélectionnez le VNet identifié pour le peering, puis cliquez sur **Ajouter**. Le VNet est ajouté au tableau avec le statut initialement **En cours**. Une fois le peering terminé avec succès, le statut passe à **Terminé**.
3. Cliquez sur **Terminé**.
4. Continuez avec la configuration, voir Étape 1 : Provisionner l'authentification adaptative.

Important :

- Pour que le trafic circule entre le réseau virtuel géré par Citrix et le réseau local, les règles de pare-feu et de routage peuvent être modifiées sur site pour diriger le trafic vers le réseau virtuel géré par Citrix.
- Vous ne pouvez ajouter qu'un seul homologue VNet à la fois. Les peerings VNet multiples ne sont actuellement pas autorisés. Vous pouvez supprimer un peering VNet ou en créer un selon vos besoins.



Sauvegarde et restauration de la configuration

Le service Application Delivery Management effectue la gestion des sauvegardes pour les instances d'authentification adaptative. Pour plus de détails, voir Sauvegarder et restaurer les instances NetScaler.

1. Dans la vignette Application Delivery Management, cliquez sur **Gérer**.
2. Accédez à **Infrastructure > Instances** et accédez aux sauvegardes.

> **Remarque**
>
> Si vous ne voyez pas le service intégré, intégrez le service Application Delivery Management. Pour plus de détails, voir Mise en route.

Exemple de configuration d'équilibrage de charge LDAP et LDAPS

L'instance Citrix Adaptive Authentication fournit la prise en charge LDAP/LDAPS à l'aide d'un serveur virtuel d'équilibrage de charge.

> **Remarque**
>
> - Si vous n'utilisez pas l'équilibrage de charge pour LDAP/LDAPS, évitez de créer un service ou un serveur pour un serveur LDAP car cela pourrait interrompre le tunnel d'authentifica-

> tion adaptative.
> - Si vous utilisez l'équilibrage de charge pour LDAP, créez un groupe de services et liez-le au service d'équilibrage de charge et non à un service autonome.
> - Lorsque vous utilisez un serveur virtuel d'équilibrage de charge pour l'authentification, assurez-vous d'ajouter l'adresse IP du serveur virtuel d'équilibrage de charge au lieu de l'adresse IP réelle du serveur LDAP dans l'action LDAP.
> - Par défaut, un moniteur TCP est lié au service que vous créez. Sur les instances NetScaler d'authentification adaptative, le service est marqué comme UP par défaut si un moniteur TCP est utilisé.
> - Pour la surveillance, il est recommandé d'utiliser des moniteurs personnalisés.

Prérequis

Adresse IP privée (adresse RFC1918) du serveur virtuel d'équilibrage de charge. Il peut s'agir d'une adresse IP factice car cette adresse est utilisée pour la configuration interne.

Équilibrage de charge des serveurs LDAP

Pour équilibrer la charge des serveurs LDAP, créez un groupe de services et liez-le au serveur virtuel d'équilibrage de charge. Ne créez pas de service pour équilibrer la charge des serveurs LDAP.

Configurer LDAP à l'aide de la CLI NetScaler :

Vous pouvez utiliser les commandes CLI suivantes comme référence pour configurer LDAP.

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>)<port>`
3. `ajouter lb vserver <name> <serviceType> <ip> <port>` - Le port doit être 389. Ce port est utilisé pour la communication interne et la connexion à un serveur local s'effectue via SSL en fonction du port configuré pour le groupe de services.
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
6. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
7. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Configurer LDAP à l'aide de l'interface graphique NetScaler :

1. Accédez à **Gestion du trafic > Équilibrage de charge** puis cliquez sur **Serveurs virtuels**.

2. Créez un serveur virtuel de type TCP et port 389.

   Ne créez pas de serveur virtuel d'équilibrage de charge de type SSL/SSL_TCP.

3. Accédez à **Gestion du trafic > Équilibrage de charge** puis cliquez sur **Groupes de services**.
4. Créez un groupe de services de type TCP et port 389.
5. Liez le groupe de services au serveur virtuel que vous avez créé à l'étape 1.

Pour plus de détails sur les procédures, voir Configuration de l'équilibrage de charge de base.

Équilibrage de charge des serveurs LDAPS

Pour équilibrer la charge des serveurs LDAPS, vous devez créer un serveur virtuel d'équilibrage de charge de type TCP pour éviter le chiffrement ou le déchiffrement SSL interne dans l'instance d'authentification adaptative. Dans ce cas, le serveur virtuel d'équilibrage de charge gère le cryptage/décryptage TLS. Ne créez pas de serveur virtuel d'équilibrage de charge de type SSL.

Configurer LDAPS à l'aide de la CLI NetScaler :

Vous pouvez utiliser les commandes CLI suivantes comme référence pour configurer LDAPS.

1. `ajouter lb vserver <name> <serviceType> <ip> <port>` - Le port doit être 636.
2. `bind lb vserver <name> <serviceGroupName>`
3. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
4. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
5. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Configurer LDAPS à l'aide de l'interface graphique NetScaler :

1. Accédez à **Gestion du trafic > Équilibrage de charge** puis cliquez sur **Serveurs virtuels**.
2. Créez un serveur virtuel de type TCP et port 636.

   Ne créez pas de serveur virtuel d'équilibrage de charge de type SSL/SSL_TCP.

3. Accédez à **Gestion du trafic > Équilibrage de charge** puis cliquez sur **Service**.
4. Créez un service de type SSL_TCP et port 636.
5. Liez le service au serveur virtuel que vous avez créé à l'étape 1.

Pour plus de détails sur les procédures, voir Configuration de l'équilibrage de charge de base.

Créer des moniteurs personnalisés

Créez des moniteurs personnalisés à l'aide de l'interface graphique NetScaler :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs** .
2. Créer un moniteur de type LDAP. Assurez-vous de définir l'intervalle de la sonde de surveillance sur 15 secondes et le délai de réponse sur 10 secondes.
3. Liez ce moniteur à votre service.

Pour plus de détails, voir Moniteurs personnalisés.

Possibilité d'ajouter jusqu'à 15 adresses IP d'administrateur

Le service d'authentification adaptative vous permet de saisir jusqu'à 15 sous-réseaux IP publics et adresses IP individuelles pour accéder à la console de gestion d'authentification adaptative.

Points à noter lors de la saisie des adresses IP/sous-réseaux :

- Assurez-vous que les CIDR des sous-réseaux IP publics sont compris entre /20 et /32.B.
- Assurez-vous qu'il n'y a pas de chevauchement entre les entrées.

Exemples :

- 192.0.2.0/24 et 192.0.2.8 ne sont pas acceptés car 192.0.2.8 se trouve dans 192.0.2.0/24.
- Sous-réseaux qui se chevauchent : 192.0.2.0/24 et 192.0.0.0/20 ne sont pas acceptés car les sous-réseaux se chevauchent.
- Lors de la saisie d'une valeur de sous-réseau réseau, saisissez l'adresse IP du réseau comme valeur d'adresse IP.

  Exemple :

  - 192.0.2.2/24 est incorrect, utilisez plutôt 191.0.2.0/24
  - 192.0.2.0/20 est incorrect, utilisez plutôt 192.0.0.0/20

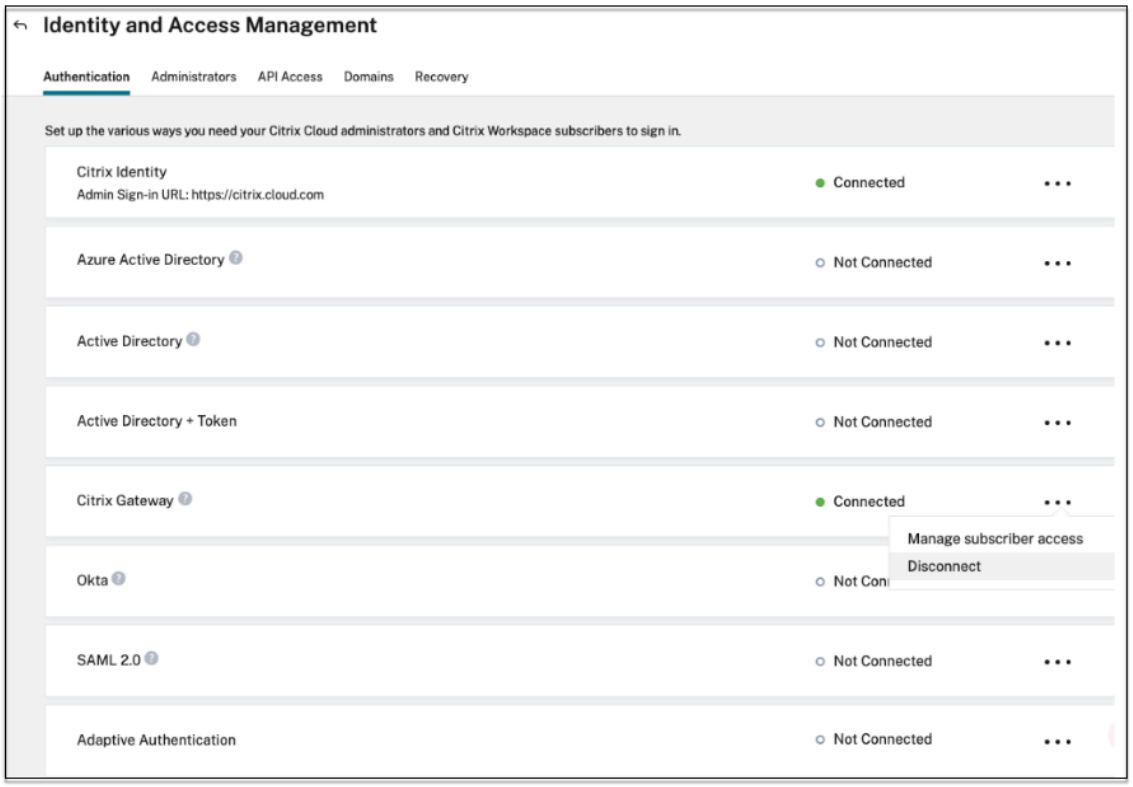
Pour activer cette fonctionnalité, contactez le support Citrix.

Migrez votre méthode d'authentification vers l'authentification adaptative

Les clients utilisant déjà Adaptive Authentication avec la méthode d'authentification **Citrix Gateway** doivent migrer **Adaptive Authentication** , puis supprimer la configuration OAuth de l'instance Adaptive Authentication.

1. Basculez vers une méthode d'authentification différente de Citrix Gateway.

2. Dans **Citrix Cloud > Identity and Access Management**, cliquez sur le bouton points de suspension correspondant à Citrix Gateway, puis cliquez sur **Déconnecter**.



3. Sélectionnez **Je comprends l'impact sur l'expérience de l'abonné**, puis cliquez sur **Confirmer**.

   Lorsque vous cliquez sur **Confirmer**, la connexion à l'espace de travail des utilisateurs finaux est affectée et l'authentification adaptative n'est pas utilisée pour l'authentification jusqu'à ce que l'authentification adaptative soit à nouveau activée.

4. Dans la console de gestion de l'instance Adaptive Authentication, supprimez la configuration associée à OAuth.

   En utilisant la CLI :

```
unbind authentication vs <authvsName> -policy <oauthIdpPolName>
rm authentication oauthIdpPolicy <oauthIdpPolName>
rm authentication oauthIdpProfile <oauthIdpProfName>
```

   En utilisant l'interface graphique :

   a) Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**.
   b) Libérer la politique OAuth.
   c) Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > OAuth IDP**.

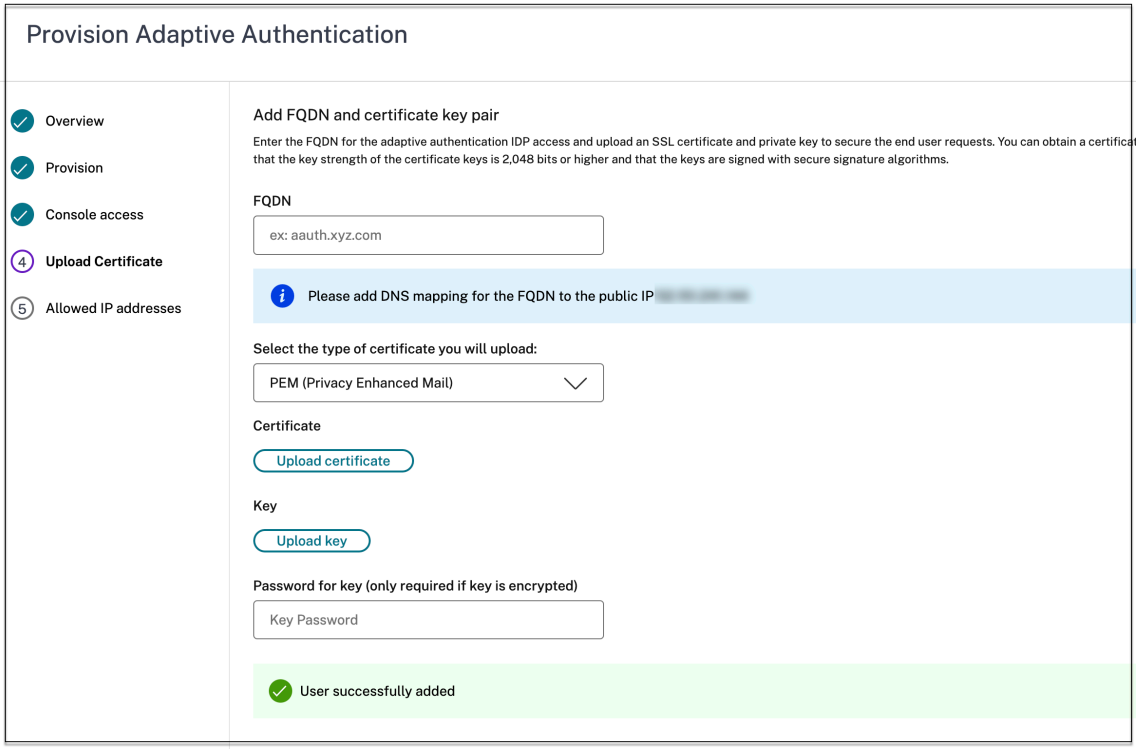
d) Supprimez la politique et le profil OAuth.

5. Accédez à **Citrix Cloud > Gestion des identités et des accès**. Dans l'onglet Authentification, dans Authentification adaptative, cliquez sur le menu à points de suspension et sélectionnez **Gérer**.

   OU accédez à https://adaptive-authentication.cloud.com

6. Cliquez sur **Voir les détails**.
7. Dans l'écran **Télécharger le certificat** , procédez comme suit :

   - Ajoutez le FQDN d'authentification adaptative.
   - Supprimez les certificats et les fichiers clés et téléchargez-les à nouveau.



Important :

Si vous modifiez un nom de domaine complet ou la paire certificat-clé directement sans migrer vers **Adaptive Authentication**, la connexion à Identity and Access Management échoue et les erreurs suivantes s'affichent. Vous devez migrer vers la méthode d'authentification adaptative pour corriger ces erreurs.

- La commande ADC a échoué avec une erreur. Une politique est déjà liée à la priorité spécifiée.
- La commande ADC a échoué avec une erreur. Impossible de dissocier une politique qui n'est pas liée.

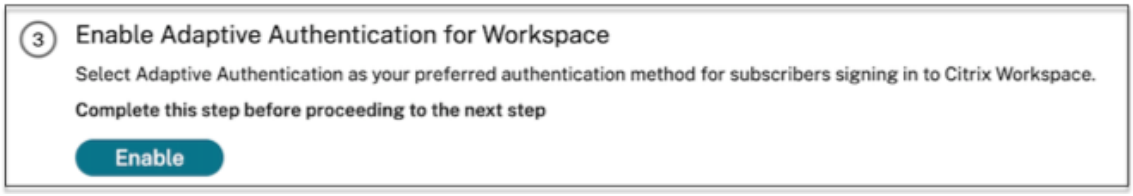
8. Cliquez sur **Enregistrer les modifications**.

   À ce stade, Identity and Access Management affiche **Adaptive Authentication** comme **Connecté** et l'instance Adaptive Authentication a le profil OAuth configuré automatiquement.

   Vous pouvez valider cela à partir de l'interface graphique.

   a) Accédez à votre instance d'authentification adaptative et connectez-vous avec vos informations d'identification.
   b) Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**. Vous devez voir que le profil IdP OAuth a été créé.
   c) Accédez à **Citrix Cloud > Gestion des identités et des accès**. L'authentification adaptative est dans le statut **Connecté** .

9. Réactivez la méthode d'authentification adaptative en cliquant sur **Activer** (étape 3) dans la page d'accueil de l'authentification adaptative.

   Cette étape active la méthode d'authentification en tant qu'authentification adaptative dans la configuration de votre espace de travail.

10. Cliquez sur le lien de l'espace de travail à l'étape 3 après avoir cliqué sur **Activer**. Vous devez voir que la méthode d'authentification est modifiée en authentification adaptative.

> **Remarque**
>
> Les nouveaux utilisateurs doivent suivre les mêmes étapes, à l'exception de l'étape de suppression de la configuration liée à OAuth.

Exemples de configurations d'authentification

Les clients peuvent configurer une politique d'authentification de leur choix et la lier au serveur virtuel d'authentification. Les liaisons de profil d'authentification ne sont pas requises pour le serveur virtuel d'authentification. Seules les politiques d'authentification peuvent être configurées. Voici certains des cas d'utilisation .

> **Important :**
>
> La configuration de l'authentification doit être effectuée sur les nœuds principaux uniquement.

Authentification multifactorielle avec authentification conditionnelle

- Authentification à double facteur avec LDAP et RADIUS à l'aide d'un schéma à double facteur (prenant la saisie de l'utilisateur une seule fois)
- Méthode de connexion à l'authentification selon les services de l'utilisateur (employé, partenaire, fournisseur) dans l'organisation avec menu déroulant pour sélectionner le service
- Méthode de connexion d'authentification selon les domaines d'utilisateur avec menu déroulant
- Configurer l'ID de messagerie (ou le nom d'utilisateur) comme premier facteur avec un accès conditionnel basé sur l'extraction de groupe avec l'ID de messagerie comme premier facteur et fournir un type de connexion différent pour chaque groupe
- Authentification multifacteur utilisant l'authentification par certificat pour les utilisateurs disposant de certificats utilisateur et l'enregistrement OTP natif pour les utilisateurs non certifiés
- Différents types d'authentification avec authentification conditionnelle en fonction des entrées du nom d'hôte de l'utilisateur
- Authentification à double facteur avec authentification OTP native
- Google Re-CAPTCHA

Intégration tierce avec authentification multifactorielle

- Configurer Azure AD comme IdP SAML (configurer le facteur suivant comme stratégie LDAP - NO_AUTH pour terminer la confiance OAuth)
- Authentification conditionnelle avec le premier facteur SAML, puis connexion personnalisée au certificat ou LDAP en fonction des attributs SAML
- Premier facteur comme connexion WebAuth suivie de LDAP

Scans de posture de l'appareil (EPA)

- Vérification de la posture de l'appareil pour la vérification de la version suivie d'une connexion personnalisée pour les utilisateurs conformes (RADIUS) et non conformes (LDAP)
- Authentification LDAP suivie d'une analyse obligatoire de la posture de l'appareil
- Vérification de la posture de l'appareil avant et après l'authentification AD - Pré et post-EPA comme facteur
- Le certificat de l'appareil comme facteur EPA

Scénarios divers

- Ajouter un CLUF avec authentification
- Personnaliser les étiquettes de politique nFactor, le schéma de connexion

Gestion de l'espace disque pour les instances

June 19, 2024

L'équipe d'authentification adaptative gère toutes les mises à niveau et la maintenance des instances d'authentification adaptative. Par conséquent, il est recommandé de ne pas mettre à niveau ou de rétrograder les instances d'authentification adaptative vers des versions RTM aléatoires. Citrix gère les instances d'authentification adaptative par défaut.

Pour les mises à niveau des instances, un minimum de 7 Go d'espace est requis dans le répertoire VAR. Par conséquent, l'équipe du service d'authentification adaptative libère de l'espace disque sur les instances avant d'appliquer les mises à niveau. Il est recommandé de ne conserver aucune information sensible, exclusive ou personnelle dans les répertoires suivants :

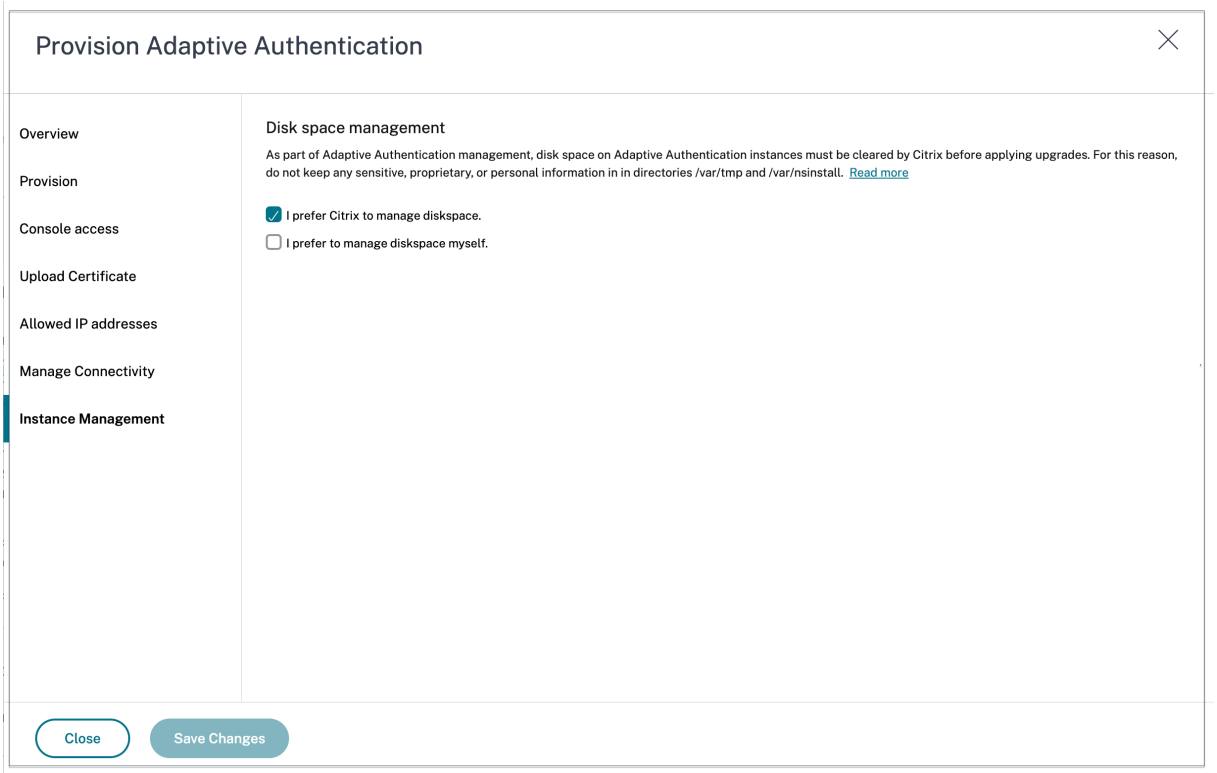
- /var/core
- /var/crash
- /var/tmp
- /var/nsinstall
- /var/nstrace
- /var/nslog

> **Remarque :**
>
> - Le répertoire /var/nsinstall est effacé en premier lors de la mise à niveau, puis le répertoire /var/tmp. Si l'espace minimum requis n'est toujours pas atteint, les autres répertoires (/var/core, /var/crash, /var/nstracem et /var/nslog) sont également effacés.
> - Le client est responsable de la gestion et de la maintenance de l'espace disque NetScaler et du nettoyage des disques.

Possibilité de gérer vous-même l'espace disque

Bien que Citrix gère les instances d'authentification adaptative, par défaut, vous pouvez préférer nettoyer vous-même l'espace disque sur les instances. Vous pouvez désactiver la méthode par défaut en procédant comme suit :

1. Dans le volet de navigation Adaptive Authentication, cliquez sur **Gestion des instances**.
2. Sélectionnez **Je préfère gérer moi-même l'espace disque**, puis cliquez sur **Confirmer** dans la boîte de dialogue du message de confirmation.
3. Cliquez sur **Enregistrer**.



> **Remarque :**
>
> vous pouvez également planifier les mises à niveau en fonction du trafic de vos clients. L'équipe Citrix Cloud met ensuite à niveau vos instances en conséquence.
> Pour plus d'informations sur la planification des mises à niveau, voir Planifier la mise à niveau de vos instances d'authentification adaptative.

Résoudre les problèmes d'authentification adaptative

June 19, 2024

Les problèmes sont classés en fonction des différentes étapes de la configuration :

- Provisioning
- Problème d'accessibilité des instances
- Problème de connectivité et d'authentification AD/Radius
- Problèmes d'authentification
- Problèmes liés à l'EPA/à l'état de sécurité de l'appareil
- Problèmes liés aux balises intelligentes
- Collecte de journaux

Vous pouvez également résoudre les problèmes à l'aide de l'interface de ligne de commande Adaptive Authentication. Pour vous connecter à l'interface de ligne de commande, procédez comme suit :

- Téléchargez le client SSH comme putty/securecrt sur votre machine.
- Accédez à l'instance Adaptive Authentication à l'aide de l'adresse IP de gestion (principale).
- Connectez-vous avec vos informations d'identification.

Pour plus de détails, consultez la section Accès à une appliance NetScaler.

Activer la journalisation des journaux d'authentification adaptatifs

Assurez-vous d'activer les niveaux de journalisation pour capturer les journaux d'authentification adaptatifs.

Activer les journaux à l'aide de la ligne de commande :

1. Connectez-vous à la CLI de l'instance Adaptive Authentication.
2. À l'aide de PuTTY, entrez les informations de gestion.
3. Exécutez la commande `set audit syslogParams logLevel ALL`

Activer les journaux via l'interface graphique :

1. Connectez-vous à l'instance d'authentification adaptative à l'aide d'un navigateur.
2. Accédez à **Configuration > Système > Audit**.
3. Sur la page Audit, sous **Paramètres**, cliquez sur **Modifier les paramètres du syslog d'audit**.
4. Dans **Log Levels**, sélectionnez **TOUT.**

Problèmes de provisionnement

- **Impossible d'accéder à l'interface utilisateur d'authentification adaptative**

  Vérifiez si le droit est activé pour votre numéro de client/locataire.

- **Bloqué dans la page d'approvisionnement pendant plus de 45 minutes**

  Collectez la capture d'écran de l'erreur, le cas échéant, puis contactez le support Citrix pour obtenir de l'aide.

- **Le pair de réseau virtuel est en panne**

  - Vérifiez s'il existe des alertes dans le portail Azure correspondant à cet appairage et prenez les mesures recommandées.
  - Supprimez l'appairage, ajoutez-le à nouveau depuis l'interface utilisateur d'authentification adaptative.

- **Le deprovisioning n'est pas terminé**

  Contactez l'assistance Citrix pour obtenir de l'aide.

Problème d'accessibilité des instances

- **L'adresse IP de gestion n'est pas accessible pour l'instance**
  - Vérifiez si l'adresse IP publique du client utilisée pour l'accès fait partie des adresses IP sources autorisées.
  - Vérifiez s'il existe un proxy qui modifie l'adresse IP source du client.
- **Impossible de se connecter à l'instance**

  Assurez-vous que l'accès administrateur fonctionne correctement avec les informations d'identification que vous avez saisies lors du provisionnement.
- **Les utilisateurs finaux ne disposent pas de tous les droits**

  Lors de l'ajout de l'utilisateur, assurez-vous d'avoir lié la stratégie de commande appropriée pour l'accès. Pour plus d'informations, consultez la section Utilisateur, groupes d'utilisateurs et stratégies de commande.

Problème de connectivité AD ou RADIUS

Problème avec le type de connectivité d'appairage de réseau virtuel Azure :

- Vérifiez si le réseau virtuel Azure géré par le client est accessible à partir des instances Adaptive Authentication.
- Vérifiez si la connectivité/l'accessibilité entre le réseau virtuel Azure géré par le client et AD fonctionne.
- Assurez-vous que des routes appropriées sont ajoutées pour diriger le trafic depuis les réseaux locaux vers les réseaux virtuels Azure.

Connecteur basé sur Windows :

- Tous les journaux sont disponibles dans le répertoire /var/log/ns.log et chaque journal est préfixé par [NS_AAUTH_TUNNEL].
- ConnectionId des journaux peut être utilisé pour corréler différentes transactions.
- Assurez-vous que l'adresse IP privée de la machine virtuelle du connecteur est ajoutée en tant que client RADIUS dans le serveur RADIUS, car cette adresse IP est l'adresse IP source du connecteur.

Pour chaque demande d'authentification, le tunnel est établi entre l'instance d'authentification adaptative (processus NS - AAAD) et le serveur d'authentification. Une fois le tunnel établi avec succès, l'authentification a lieu.

Assurez-vous que la machine virtuelle du connecteur peut résoudre le nom de domaine complet de l'authentification adaptative.

- Le connecteur est installé mais la connectivité sur site échoue.

  Validez si NSAUTH-TUNNEL est en cours d'établissement

  ```
  cat ns.log | grep -I "tunnel"
  ```

  Si l'exemple de journal suivant n'est pas imprimé dans le fichier ns.log pour la demande d'authentification, il peut y avoir un problème lors de l'établissement d'un tunnel ou un problème du côté du connecteur.

  ```
  1  LDAP:
  2  [NS_AAUTH_TUNNEL] Entering bitpump for
  3  Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636 ,
         Connection2 => Src : 10.106.103.70:2271, Dst :
        10.106.103.80:443"
  4  RADIUS:
  5  [NS_AAUTH_UDP_TUNNEL] MUX channel established"
  ```

  Vérifiez les détails du journal et prenez les mesures appropriées.

Détails du journal	Action corrective
Aucun journal avec préfixe `[NS_AAUTH_TUNNEL]` n'est inclus dans le fichier journal	Exécutez la commande `show cloudtunnel vserver`. Cette commande doit répertorier à la fois le serveur virtuel de tunnel cloud (TCP et UDP) avec l'état « UP ».
`[NS_AAUTH_TUNNEL] Waiting for outbound from connector` Pour ce journal, si la réponse suivante n'est pas reçue : `[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"`	Vérifiez si la machine du connecteur est en mesure d'accéder au nom de domaine complet de l'authentification adaptative **OU** vérifiez le pare-feu côté connecteur pour les connexions sortantes au nom de domaine complet de l'authentification adaptative.

Détails du journal	Action corrective
`[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0` et`[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"`	Contactez le support Citrix.

Aucune réponse du connecteur :

- Assurez-vous que le nom de domaine complet de l'authentification adaptative est accessible depuis la machine virtuelle du connecteur.
- Assurez-vous que vous disposez d'un certificat intermédiaire lié et lié au certificat du serveur sur l'instance Adaptive Authentication.

Paramètres LDAP/RADIUS incorrects :

Si l'adresse IP de votre serveur AD/RADIUS est une adresse IP publique, vous devez ajouter le sous-réseau ou l'adresse IP qui adresse les expressions dans NetScaler. Ne modifiez pas les plages existantes.

- Pour ajouter un sous-réseau ou une adresse IP à l'aide de l'interface de ligne de commande :

```
1  set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST
       .BETWEEN(10.0.0.0,10.255.255.255) || CLIENT.IP.DST.BETWEEN
       (172.16.0.0,172.31.255.255) || CLIENT.IP.DST.BETWEEN
       (192.168.0.0, 192.168.255.255) || CLIENT.IP.DST.BETWEEN
       (13.14.0.0, 13.14.255.255)||CLIENT.IP.DST.EQ(1.2.5.4))"
```

- Pour ajouter un sous-réseau ou une adresse IP à l'aide de l'interface graphique :

  1. Accédez à **AppExpert > Expressions**.
  2. Ajoutez l'expression **aauth_allow_rfc1918_subnets**.

Si le tunnel est établi mais que l'authentification échoue toujours, suivez les étapes suivantes pour résoudre le problème.

LDAP :

- Validez les détails du DN de liaison.
- Utilisez le test de connectivité pour confirmer l'erreur.
- Validez les erreurs à l'aide du débogage `aaad`.
- Connectez-vous à l'instance Adaptive Authentication à l'aide de la CLI.


```
shell
cd /tmp
cat aaad.debug
```

Erreurs LDAP courantes :

- Délai d'expiration du serveur : aucune réponse du connecteur pour la requête LDAP.
- Autres erreurs LDAP, reportez-vous à la section https://support.citrix.com/article/CTX138663.

Rayon :

- L'adresse IP du connecteur doit être ajoutée en tant qu'adresse IP source du client RADIUS dans la configuration du serveur RADIUS.

Problèmes d'authentification

- **Erreurs de post-assertion pour OAuth**
  - Assurez-vous que toutes les réclamations sont fournies par AD. Vous avez besoin de 7 demandes pour que cela aboutisse.
  - Validez les journaux dans le fichier /var/log/ns.log pour localiser l'erreur liée aux échecs OAuth.

```
cat /var/log/ns.log
```

  - Validez les paramètres du profil OAuth.

- **Authentification Azure AD bloquée lors de la post-assertion**

  Ajoutez l'authentification AD comme facteur suivant avec l'authentification désactivée. Cela permet d'obtenir toutes les revendications requises pour une authentification réussie.

Questions liées à l'EPA

- **Le plug-in est déjà présent mais l'utilisateur est invité à le télécharger.**

  Causes possibles : discordance de version ou fichiers corrompus

  - Exécutez les outils de développement et vérifiez si le fichier de liste des plug-ins contient la même version que celle de NetScaler et de votre machine cliente.
  - Assurez-vous que la version du client sur NetScaler est la même que sur l'ordinateur client.

    Mettez à jour le client sur NetScaler.

Sur l'instance Adaptive Authentication, accédez à **NetScaler Gateway > Paramètres généraux > Mettre à jour les bibliothèques clientes**.

La page des bibliothèques de plug-ins EPA sur les téléchargements Citrix vous fournit des informations détaillées.

- Parfois, la demande peut être mise en cache sur NetScaler même si la version est mise à jour.

  `show cache object` affiche les détails du plug-in mis en cache. Vous pouvez le supprimer à l'aide de la commande ;

  ```
  flush cache object -locator 0x00000023345600000007
  ```

Pour plus de détails sur la collecte des journaux EPA, reportez-vous à https://support.citrix.com/article/CTX209148.

- **Existe-t-il un moyen de rétablir les paramètres EPA (Toujours, Oui, Non) une fois que l'utilisateur a sélectionné une option.**

  Actuellement, la restauration des paramètres EPA est effectuée manuellement.

  - Sur la machine cliente, accédez à C:\Users <user_name>\ AppData \ Local \ Citrix \ AGEE.
  - Ouvrez le fichier `config.js` et définissez TrustAlways sur null - `"trustAlways": null`

Problèmes liés aux balises d'accès intelligentes

- **Après avoir configuré Smart Access, les applications ne sont pas disponibles**

  Assurez-vous que les balises sont définies à la fois sur l'instance Adaptive Authentication et sur les groupes de mise à disposition Citrix VDA.

  Vérifiez que les balises sont ajoutées au groupe de mise à disposition Workspace en majuscules.

  Vous pouvez récupérer le fichier ns.log et contacter le support Citrix si cela ne fonctionne pas.

Collecte de journaux générale pour l'instance d'authentification adaptative

- Offre groupée de support technique : pour plus de détails, consultez Comment collecter le pack de support technique auprès des appliances SDX et VPX pour une analyse approfondie.
- Fichiers de trace. Pour plus de détails, consultez Comment enregistrer une trace de paquets sur NetScaler.

Contactez le support Citrix pour obtenir des conseils.

Accès intelligent à l'aide de l'authentification adaptative

June 19, 2024

Les clients Citrix Cloud peuvent fournir un accès intelligent (accès adaptatif) aux ressources Citrix DaaS (applications et bureaux virtuels) ou au service Secure Private Access à l'aide de l'authentification adaptative en tant qu'IdP auprès de Citrix Workspace.

La fonctionnalité Smart Access permet au service d'authentification adaptative de transmettre toutes les informations de stratégie concernant l'utilisateur à Citrix Workspace ou Citrix DaaS. Le service d'authentification adaptative peut fournir la position de l'appareil (EPA), la localisation du réseau (à l'intérieur ou à l'extérieur du réseau de l'entreprise, géolocalisation), les attributs des utilisateurs tels que les groupes d'utilisateurs, l'heure de la journée ou une combinaison de ces paramètres dans le cadre des informations de stratégie. L'administrateur Citrix DaaS peut ensuite utiliser ces informations de stratégie pour configurer l'accès contextuel aux applications et bureaux virtuels. Les applications et bureaux virtuels peuvent être énumérés ou non en fonction des paramètres précédents (stratégie d'accès). Certaines actions de l'utilisateur, telles que l'accès au presse-papiers, la redirection de l'imprimante, le lecteur client ou le mappage USB, peuvent également être contrôlées.

Exemples de cas d'utilisation :

- L'administrateur peut configurer le groupe d'applications pour qu'elles soient affichées ou accessibles uniquement à partir d'emplacements réseau spécifiques tels que le réseau d'entreprise.
- L'administrateur peut configurer le groupe d'applications pour qu'elles soient affichées ou accessibles uniquement à partir des appareils gérés par l'entreprise. Par exemple, les analyses EPA peuvent vérifier si l'appareil est géré par l'entreprise ou s'il s'agit d'un appareil BYOD. Sur la base des résultats de l'analyse EPA, les applications pertinentes peuvent être énumérées pour l'utilisateur.

Conditions préalables

- L'authentification adaptative en tant que fournisseur d'identité doit être configurée pour Citrix Workspace. Pour plus de détails, voir Service d'authentification adaptative.
- Le service d'authentification adaptative avec Citrix DaaS est opérationnel.
- La fonctionnalité Adaptive Access est activée. Pour plus de détails, voir Activer l'accès adaptatif.

Comprendre le flux d'événements pour un accès intelligent

1. L'utilisateur se connecte à Citrix Workspace.

2. L'utilisateur est redirigé vers le service d'authentification adaptative configuré en tant qu'IdP.
3. L'utilisateur est invité à effectuer une pré-authentification (EPA) ou une authentification.
4. L'utilisateur est authentifié avec succès.
5. Les stratégies d'accès intelligentes sont évaluées en fonction de la configuration et des balises sont associées à la session utilisateur.
6. Le service d'authentification adaptative envoie les balises au service Citrix Graph. L'utilisateur est redirigé vers la page d'accueil de Citrix Workspace.
7. Citrix Workspace récupère les informations de stratégie pour cette session utilisateur, fait correspondre le filtre et évalue les applications ou les bureaux qui doivent être énumérés.
8. L'administrateur configure la stratégie d'accès sur Citrix DaaS afin de restreindre l'accès ICA aux utilisateurs.

Configuration des stratégies d'accès intelligentes sur les instances d'authentification adaptative

La configuration des stratégies d'accès intelligentes sur une instance d'authentification adaptative est un processus en deux étapes :

1. Définissez des stratégies d'accès intelligentes à l'aide de balises d'accès intelligentes sur les instances d'authentification adaptative. Par exemple, reportez-vous à *l'étape 1*.
2. Définissez les mêmes balises sur votre DAAS/Secure Private Access pour l'accès aux ressources. Par exemple, reportez-vous à *l'étape 2*.

Cas d'utilisation 1 : configurer une stratégie d'accès intelligente pour autoriser l'accès aux utilisateurs qui se connectent depuis le navigateur Chrome et leur bloquer l'accès au presse-papiers

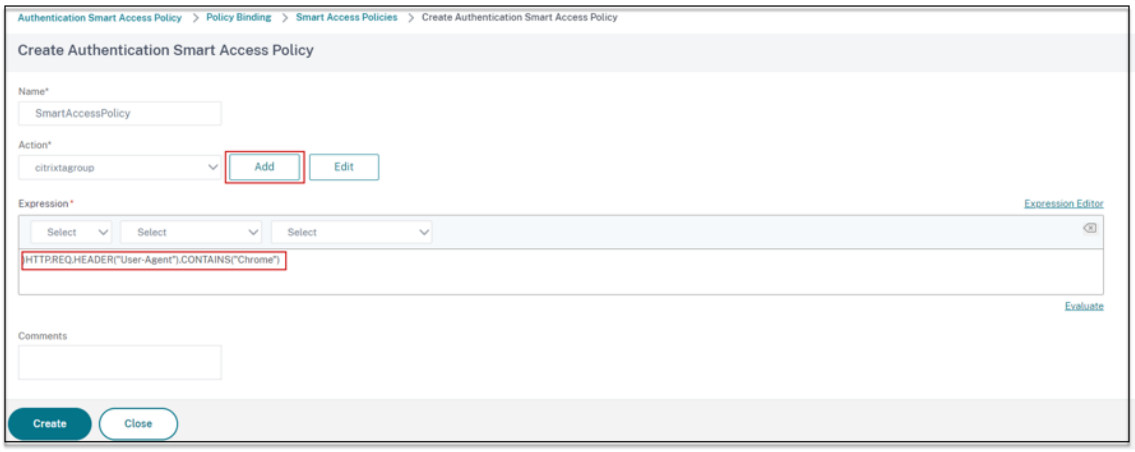
Étape 1 : configurer les stratégies d'accès intelligentes avec des balises actives sur l'instance d'authentification adaptative

1. Connectez-vous à l'instance Adaptive Authentication.
2. Accédez au serveur virtuel d'authentification adaptative (**Sécurité > AAA - Trafic des applications > Serveurs virtuels**).
3. Sélectionnez le serveur virtuel d'authentification, puis cliquez sur **Modifier**.
4. Cliquez sur **Stratégies d'accès intelligentes**.
5. Définissez l'expression de la stratégie en fonction de vos besoins.
    a) Cliquez sur **Add Binding**.
    b) Dans **Sélectionner une stratégie**, cliquez sur **Ajouter**.

c) Entrez un nom pour la stratégie d'accès intelligent.
d) Définissez l'expression.

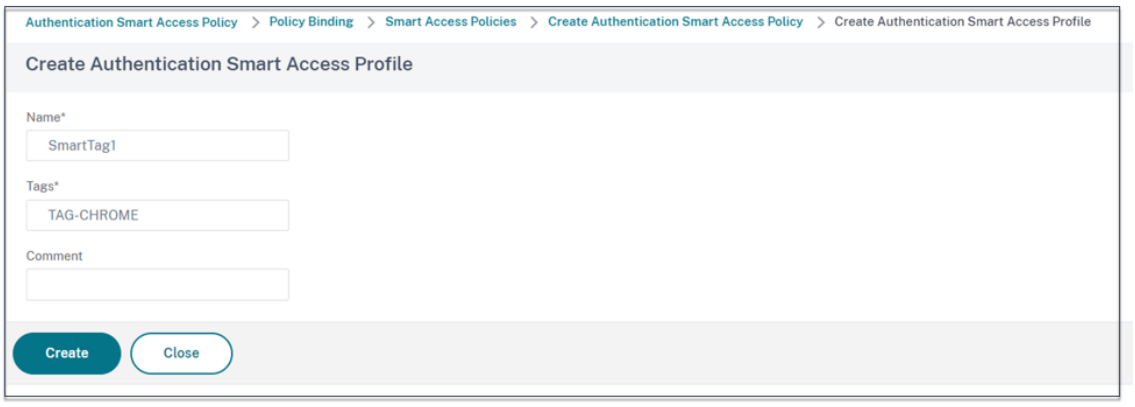
Pour donner l'exemple d'autoriser l'accès aux utilisateurs qui se connectent depuis un navigateur Chrome, entrez l'expression `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")`

De même, vous pouvez créer des expressions en fonction de l'heure, de la connexion utilisateur, du groupe d'authentification et d'autorisation, ainsi que d'autres options.

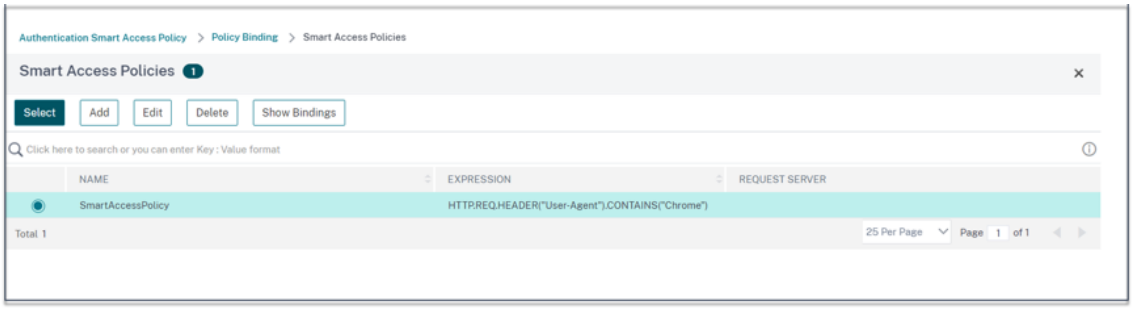


6. Créez maintenant des balises actives et liez ces balises à la stratégie d'accès intelligente.

a) Dans **Action**, cliquez sur **Ajouter**.
b) Dans **Nom**, tapez un nom pour le profil d'accès intelligent.
c) Dans **Tags**, définissez les balises d'accès intelligentes. Par exemple, TAG-CHROME.



a) Cliquez sur **Créer**.
b) Sélectionnez la stratégie d'accès intelligente et cliquez sur **Ajouter une liaison**.
c) Liez cette étiquette d'accès intelligent à la stratégie d'accès intelligente créée précédemment.



> **Remarque :**
>
> Vous pouvez également créer une stratégie d'accès intelligente dans **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Accès intelligent > Stratégies**, puis la lier au serveur virtuel d'authentification.

Étape 2 : définir des balises d'accès intelligentes dans DaaS Studio

1. Ajoutez les stratégies avec la balise intelligente « TAG-CHROME ». Pour plus de détails, consultez la section Définir des balises dans Citrix Studio.

Cas d'utilisation 2 : configurer des stratégies d'accès intelligentes en fonction des résultats de l'EPA, pour la post-authentification

Étape 1 : configurer les stratégies d'accès intelligentes avec des balises actives sur l'instance d'authentification adaptative Pour un accès intelligent basé sur des conditions telles que l'analyse des points finaux, configurez le flux nFactor, définissez une action EPA, puis ajoutez le groupe par défaut.

Pour configurer l'EPA en tant que facteur dans le flux nFactor, voir Configurer l'EPA en tant que facteur.

Flux logique

1. L'utilisateur accède à l'URL de l'espace de travail.
2. L'utilisateur est redirigé vers Adaptive Authentication for Authentication/EPA.
3. L'analyse du point final est effectuée sur l'utilisateur final et les résultats sont stockés en ajoutant l'utilisateur au groupe par défaut défini.
4. L'utilisateur est invité à passer au flux d'authentification suivant.
5. Les stratégies d'accès intelligent sont évaluées et les balises d'accès intelligentes sont attribuées à l'utilisateur.

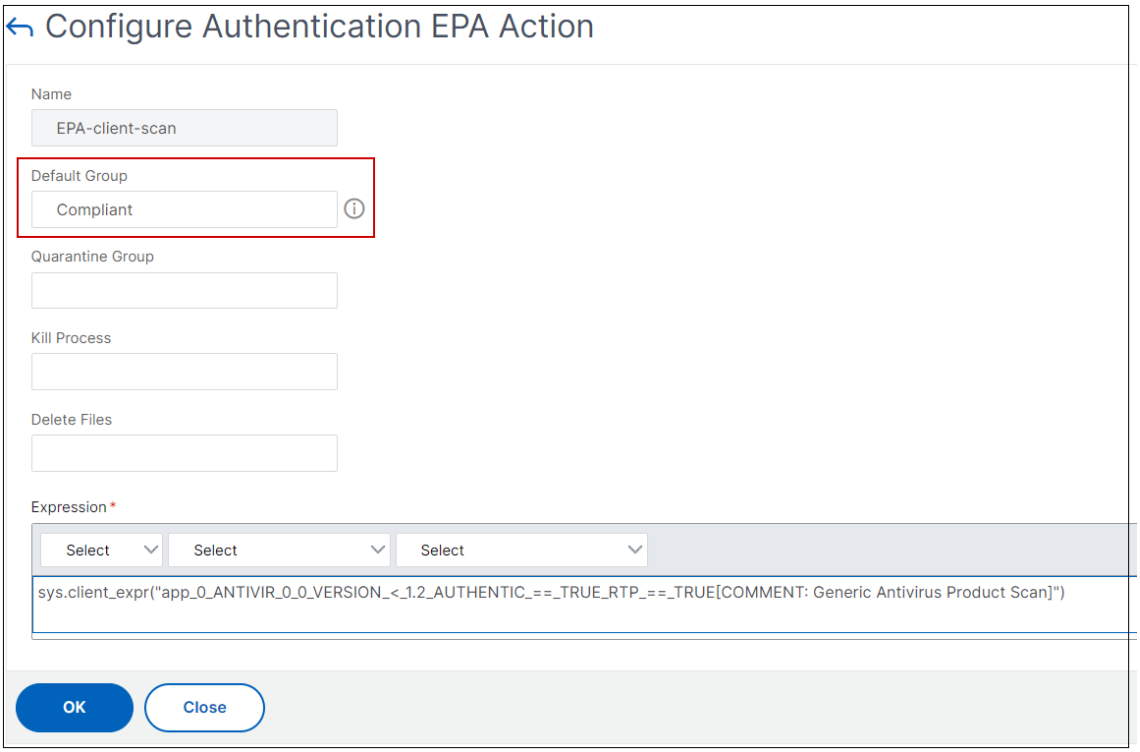
Configuration

Les utilisateurs accédant à partir d'une machine sur laquelle un antivirus est installé doivent être marqués comme conformes et bénéficier d'un accès complet. Toutefois, les machines utilisateur dépourvues d'antivirus doivent être marquées comme non conformes et bénéficier d'un accès limité.

1. Créez une stratégie nFactor pour l'EPA. Pour plus de détails, voir Configurer l'EPA en tant que facteur.

   Dans le flux nFactor, assurez-vous que le premier est un facteur d'authentification de l'utilisateur.

2. Sélectionnez l'expression EPA pour vérifier si l'antivirus est présent ou non.
3. Dans l'action EPA, définissez le groupe par défaut.



   L'utilisateur est ajouté à ce groupe par défaut si l'EPA s'exécute correctement.

4. Créez maintenant des stratégies d'accès intelligentes

   a) Connectez-vous à l'instance Adaptive Authentication.

   b) Accédez au serveur virtuel d'authentification adaptative (**Sécurité > AAA - Trafic des applications > Serveurs virtuels**).

   c) Sélectionnez le serveur virtuel d'authentification adaptative et cliquez sur **Modifier**.

d) Cliquez sur **Stratégies d'accès intelligentes**.

e) Créez deux stratégies d'accès intelligentes avec les expressions suivantes.

- AAA.USER.IS_MEMBER_OF (« Conforme ») - Pour la condition de réussite EPA de l'utilisateur
- ! AAA.USER.IS_MEMBER_OF (« Conforme ») —Conforme à la condition de défaillance EPA de l'utilisateur

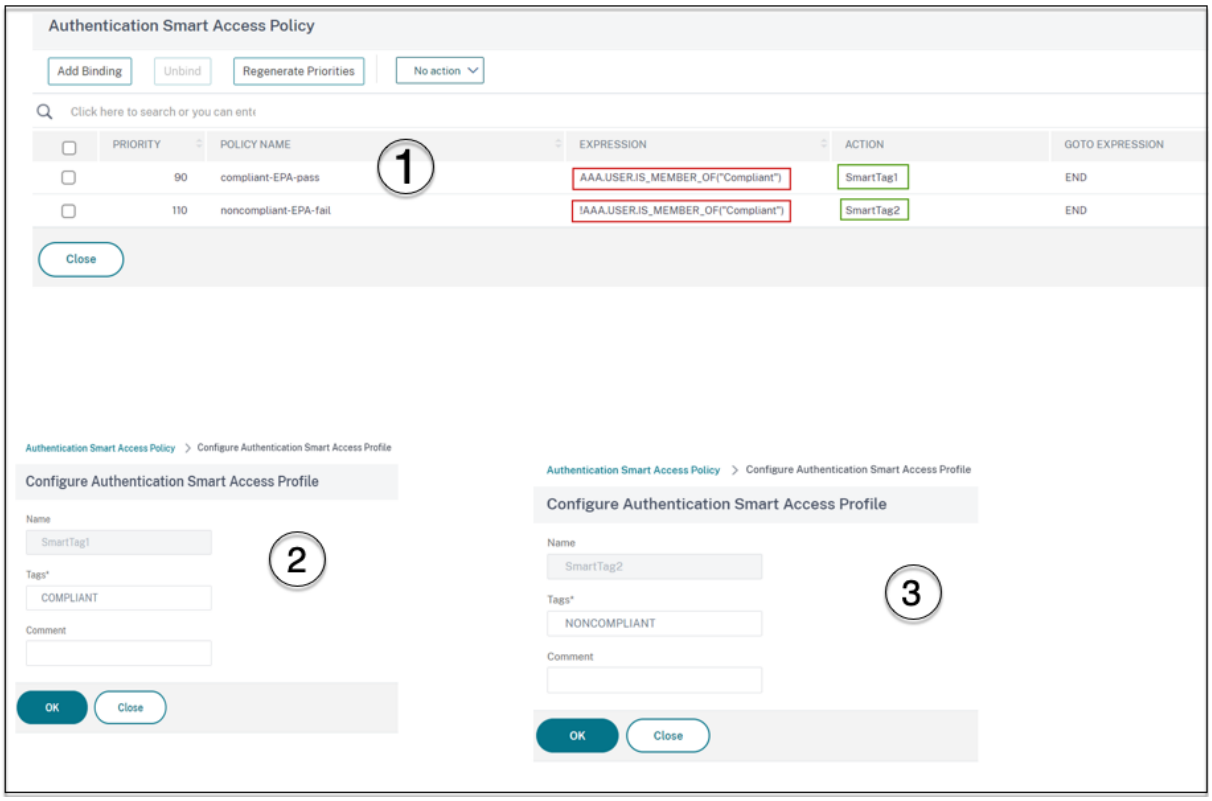
f) Définissez des balises d'accès intelligentes pour ces deux stratégies.

Exemple :

- Nom du tag `SmartTag1` avec le tag COMPLIANT pour `AAA.USER.IS_MEMBER_OF ("Compliant")`
- Nom du tag `SmartTag2` avec le tag NON CONFORME pour `!AAA.USER.IS_MEMBER_OF ("Compliant")`

La configuration de l'instance d'authentification adaptative avec des conditions telles que l'EPA pour l'accès intelligent est désormais terminée.

Vous pouvez configurer les balises et l'expression en fonction de vos besoins.



Étape 2 : configurer les balises d'accès intelligentes dans DaaS Studio Ajoutez les stratégies avec les balises intelligentes « CONFORME » et « NON CONFORME » dans les groupes de mise à disposition

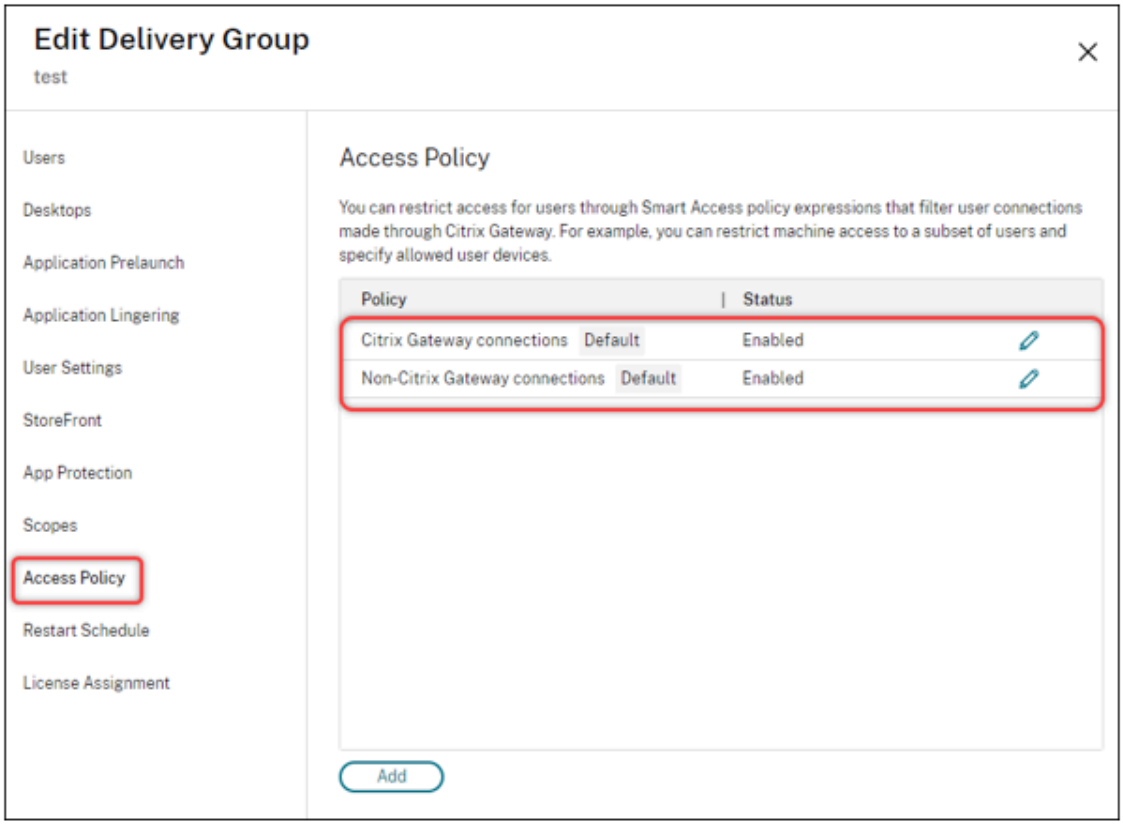
respectifs. Pour plus de détails, consultez la section Définir des balises dans Citrix Studio.

Définition de balises dans DaaS studio

Définissez des balises dans les groupes de mise à disposition afin de restreindre l'énumération des applications pour les utilisateurs.

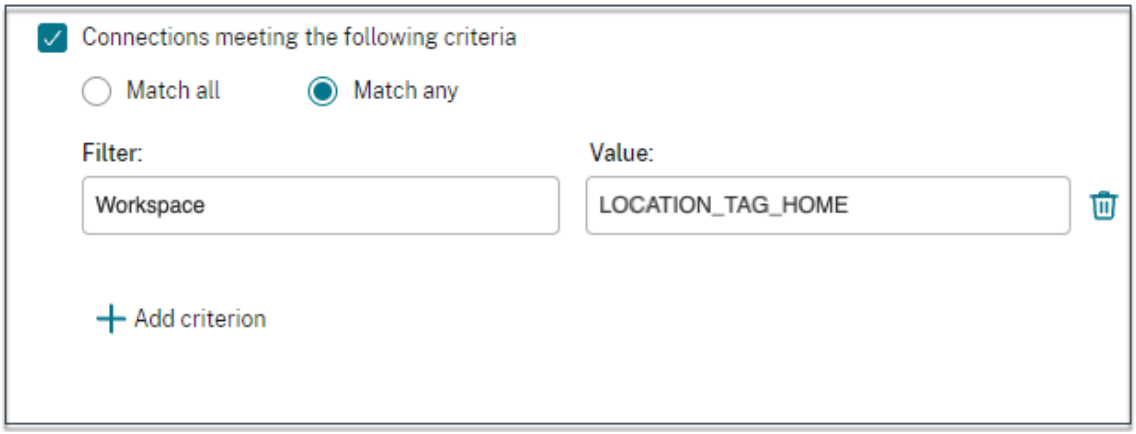
Exemple : les utilisateurs de BranchOffice doivent voir les applications du **groupe Adaptive Access Delivery** qui contient toutes les applications.
En revanche, les utilisateurs de WorkFromHome doivent voir les applications de **WFH**Delivery Group.

1. Connectez-vous à Citrix Cloud.
2. Sélectionnez **Mes services > DaaS**.
3. Cliquez sur **Manage**.
4. Créez des groupes de mise à disposition selon vos besoins. Pour de plus amples informations, consultez la section Créer des groupes de mise à disposition.
5. Sélectionnez le groupe de mise à disposition que vous avez créé et cliquez sur **Modifier le groupe de mise à disposition**.



6. Cliquez sur **Stratégie d'accès**.
7. Pour les clients qui utilisent l'accès adaptatif dans la plate-forme Citrix Workspace, procédez comme suit pour restreindre l'accès d'un groupe de mise à disposition aux réseaux internes uniquement :

   a) Cliquez avec le bouton droit sur le groupe de mise à disposition et sélectionnez **Modifier**.
   b) Sélectionnez la stratégie d'accès dans le panneau de gauche.
   c) Cliquez sur l'icône Modifier pour modifier la stratégie de connexion par défaut de Citrix Gateway.
   d) Sur la page Modifier la stratégie, sélectionnez **Connexions répondant aux critères** suivants , sélectionnez **Toutes les**connexions, puis ajoutez les critères.



   Pour les utilisateurs de WorkFromHome, entrez les valeurs suivantes dans le Delivery Controller correspondant.

   Batterie : espace de travail

   Filtre : LOCATION_TAG_HOME

   Pour les utilisateurs de BranchOffice, entrez les valeurs suivantes dans le Delivery Controller correspondant.

   Filtre : espace de travail

   Valeur: LOCATION_TAG_BRANCHOFFICE

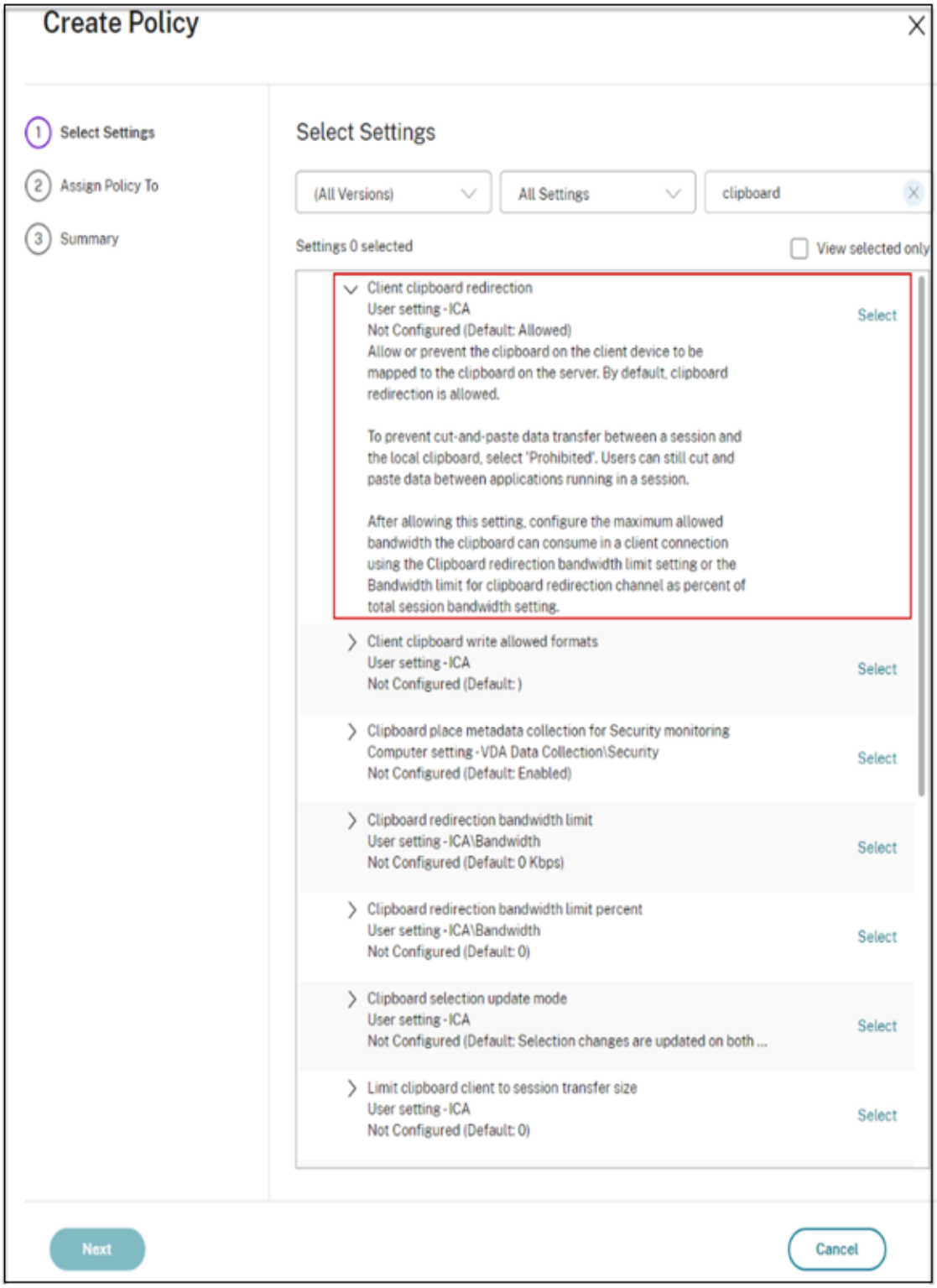
Vous pouvez désormais utiliser ces balises pour restreindre l'accès à vos applications.

Restreindre le type d'accès pour les applications fournies

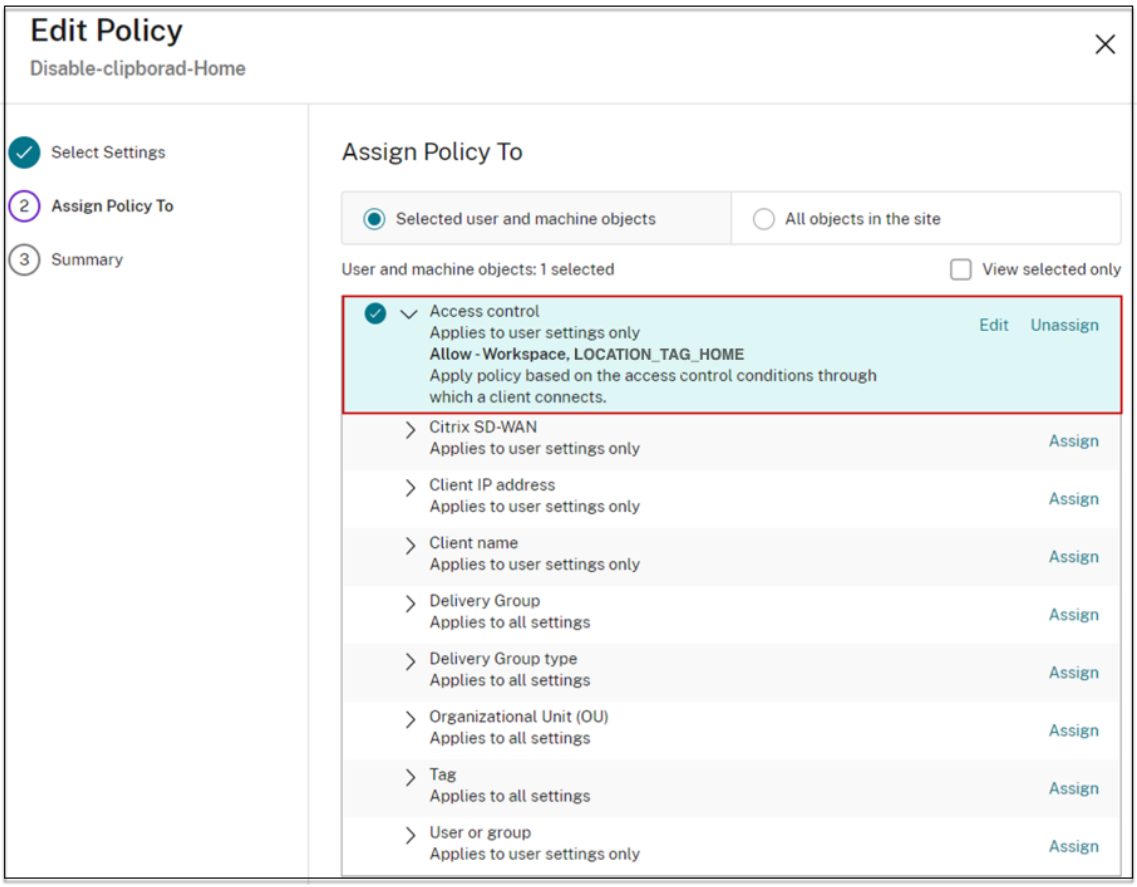
Exemple : les utilisateurs travaillant à domicile ne doivent pas disposer de droits sur le presse-papiers.

1. Dans DaaS Studio, accédez à **Stratégies** et cliquez sur **Créer une**stratégie.

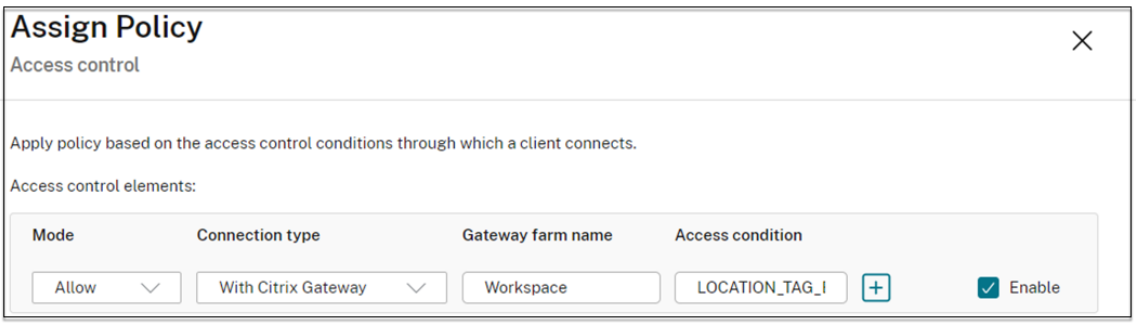
2. Sur la page **Créer une stratégie**, sélectionnez le paramètre pour lequel vous souhaitez autoriser ou interdire l'accès.
3. cliquez sur **Sélectionner**.



4. Sur la page **Modifier les paramètres**, cliquez sur **Autorisé** ou **Interdit**, puis sur **Enregistrer.**
5. Cliquez sur **Suivant**.
6. Sur la page **Attribuer une stratégie à**, sélectionnez **Contrôle d'accès**, puis cliquez sur **Suivant**.

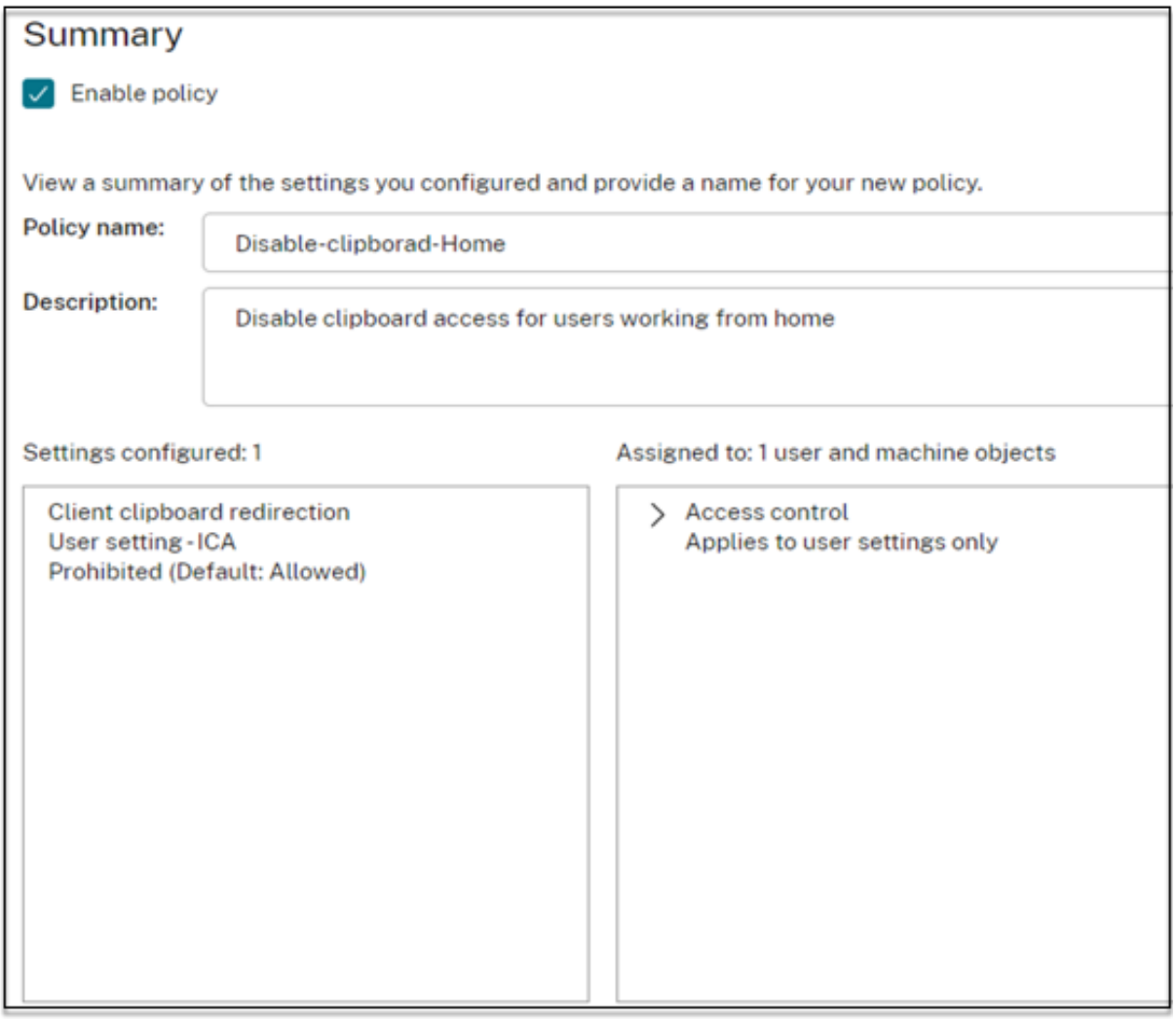


7. Définissez une stratégie avec les détails suivants :
   - **Mode** : - Autoriser
   - **Type de connexion** : - Avec Citrix Gateway
   - **Nom de la ferme** : - Workspace
   - **Condition d'accès** : LOCATION_TAG_HOME (en majuscules)



8. Cliquez sur **Suivant** et saisissez le nom de la stratégie.

9. Cliquez sur **Terminer**.



Vous êtes maintenant prêt à tester votre accès.

Résolution des erreurs courantes

- **Problème :** le message « Impossible de terminer votre demande » s'affiche.

  Résolution

  1. Assurez-vous que l'accès adaptatif est activé. Pour plus de détails, voir Activer l'accès adaptatif.
  2. Si la fonctionnalité n'est pas activée, contactez le support Citrix.

- **Problème :** aucune application ni aucun ordinateur de bureau n'est publié.

  Ce problème peut se produire si les balises actives ne sont pas transférées de l'authentification adaptative vers l'espace de travail ou ne sont pas reçues par le DaaS ou Secure Private Access.

Résolution :

- Vérifiez si les stratégies d'accès intelligentes sont touchées. Pour plus d'informations, consultez la section https://support.citrix.com/article/CTX138840.
- Vérifiez si l'instance Citrix Adaptive Authentication est capable de se connecter à `cas.citrix.com`.
- Consultez l'instance d'authentification adaptative pour plus de détails sur les balises intelligentes.
  * Assurez-vous que dans la commande `set audit syslogParams`, le paramètre LogLevel est défini sur `ALL` sur toutes les instances.
  * Connectez-vous à l'instance principale d'authentification adaptative à l'aide de Putty.

    Taper une commande shell

    ```
    cd /var/log
    ```

    ```
    cat ns.log | more or cat ns.log | grep -I “smartaccess”
    ```
- Si cela ne permet pas de résoudre le problème, contactez le support Citrix.

Changements de configuration pour une configuration à haute disponibilité

Il peut arriver que la synchronisation des fichiers soit retardée dans une configuration haute disponibilité dans les répertoires suivants. Par conséquent, les clés créées lors de l'enregistrement de Citrix ADM ne sont pas lues à temps.

- /var/mastools/conf/agent.conf
- /var/mastools/trust/.ssh/private.pem
- /var/mastools/trust/.ssh/public.pem

Pour résoudre le problème de synchronisation des fichiers, effectuez les étapes suivantes pour réexécuter la `set cloud` commande sur le périphérique secondaire.

```
1  > shell cat /var/mastools/conf/agent.conf
2  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3  <mps_agent>
4  <uuid>temp_str</uuid>
5  <url>fuji.agent.adm.cloud.com</url>
6  <customerid>customer_id</customerid>
7  <instanceid>instance_id</instanceid>
8  <servicename>MAS</servicename>
9  <download_service_url>download.citrixnetworkapistaging.net</
      download_service_url>
10 <abdp_url>fuji.agent.adm.cloud.com</abdp_url>
```



```
<msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>
</mps_agent> Done
> set cloud param -CustomerID customer_id -InstanceID instance_id -
    Deployment Production
```

Directives relatives au dimensionnement et aux performances

June 19, 2024

L'authentification adaptative permet aux clients d'accéder à leurs serveurs d'authentification locaux à l'aide de composants Cloud Connector déployés dans leurs centres de données ou d'Azure VNet Peering si l'accessibilité du centre de données est déjà établie à partir du réseau virtuel géré par le client. Cette rubrique contient des informations sur les performances des déploiements de Citrix Cloud Connector et d'Azure VNet Peering, ainsi que sur les configurations d'échelle et de taille recommandées pour les machines Citrix Cloud Connector.

Taux d'authentification des utilisateurs

Une machine virtuelle connecteur composée de processeurs virtuels de taille 2 et de 7 Go de RAM peut authentifier 14 utilisateurs/s.

Par défaut, le service du connecteur est configuré pour redémarrer automatiquement deux fois en cas de panne ou de crash. En cas de panne ou de crash ultérieur, le service s'arrête. De plus, actuellement, le service de connecteur échoue si le taux d'authentification augmente au-delà de 4 authentifications/s. Ce taux peut être atteint en configurant le service de connecteur pour qu'il redémarre après un certain nombre d'échecs (**Citrix Netscaler Cloud Gateway > Recovery > Redémarrer le service**). Si ce paramètre n'est pas configuré, le taux tombe à 4 authentifications/s.

Latence du trafic et taux d'authentification des utilisateurs lors de l'utilisation de composants Citrix Cloud Connector

Le tableau suivant indique la latence du trafic et le taux d'authentification des utilisateurs lors de l'utilisation de composants Citrix Cloud Connectors :

Type d'authentification	Latence d'authentification (p95) en ms	Taux d'authentification ou de connexion utilisateur par seconde
LDAP	5.99	14

Type d'authentification	Latence d'authentification (p95) en ms	Taux d'authentification ou de connexion utilisateur par seconde
RADIUS	3.17	14
LDAP+RADIUS	4.59	14
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

Latence du trafic et taux d'authentification des utilisateurs lors de l'utilisation d'Azure VNet Peering

Le tableau suivant affiche la latence du trafic et le taux d'authentification des utilisateurs lors de l'utilisation d'Azure VNet peering :

Type d'authentification	Latence des requêtes (p95) en ms	Taux d'authentification ou de connexion utilisateur par seconde
LDAP	6.95	17.54
LDAPS	7.19	16.98

Gouvernance des données

June 19, 2024

Cette rubrique fournit des informations concernant la collecte, le stockage et la conservation des journaux par le service Citrix Adaptive Authentication et les instances Adaptive Authentication. Tous les termes en majuscules non définis dans les définitions ont la signification spécifiée dans le contrat de services de l'utilisateur final Citrix.

- Services Adaptive Authentication : service Citrix Cloud auquel les administrateurs peuvent se connecter pour déployer et gérer les instances Adaptive Authentication.
- Instances d'authentification adaptative : machines virtuelles NetScaler déployées par le service Adaptive Authentication pour permettre aux administrateurs de gérer l'authentification des utilisateurs.

Résidence de données

Services d'authentification adaptative

Les données de contenu client du service Citrix Adaptive Authentication résident dans la région Azure Cloud Services East. Ils sont répliqués dans les régions Azure suivantes pour des raisons de disponibilité et de redondance :

- Ouest des États-Unis
- Europe du Nord

Vous trouverez ci-dessous les différentes destinations pour les journaux de configuration et d'exécution du service.

- Service Splunk pour la surveillance du système et les journaux de débogage, uniquement aux États-Unis et dans l'UE (Union européenne).
- Service NetScaler Application Delivery Management pour les journaux d'accès utilisateur agrégés. Pour plus de détails, consultez NetScaler ADM Data Governance.
- Service Citrix Cloud System Logs pour les journaux d'audit de l'administrateur. Pour plus de détails, consultez la section Gestion du contenu client et des journaux de Citrix Cloud Services et considérations géographiques.

instances d'authentification adaptative

Service NetScaler Application Delivery Management pour la sauvegarde de toutes les configurations et des artefacts spécifiques à une instance. Pour plus de détails, consultez NetScaler ADM Data Governance.

Collecte des données

Le service Citrix Adaptive Authentication permet aux administrateurs du client de configurer le service via l'interface utilisateur Adaptive Authentication et les appliances Connector associées via la console. Le contenu client suivant est collecté :

- Service d'authentification adaptative
  - FQDN (nom de domaine complet) et adresse IP du point de terminaison IdP (fournisseur d'identité).
  - Adresses/plages IP, ports et protocoles
  - Certificats utilisés pour accéder au serveur virtuel d'authentification IdP
  - Adresse IP publique du point de terminaison de gestion

  - Pour l'appairage de réseaux virtuels Azure, le principal de service avec le rôle de contributeur réseau. Pour plus de détails, consultez Configuration de la connectivité aux serveurs d'authentification locaux à l'aide de l'appairage de réseaux virtuels Azure.

- Identifiants utilisateur pour les droits d'accès aux applications
- Informations relatives à Citrix Cloud Connector. Pour plus de détails, voir Citrix Cloud Connector.

  - Adresses IP ou noms de domaine complets
  - Identifiants d'emplacement des utilisateurs, des appareils et des ressources
  - Configuration du proxy interne

Pour les journaux d'exécution collectés par les composants de service, les informations clés sont les suivantes :

- Adresse IP et port du client
- FQDN/adresse et port de destination
- Agent utilisateur client
- Chemin URL de l'application
- Durée et durée d'accès à l'application
- Nombre d'octets de demande
- Nombre d'octets de réponse
- ID de transaction HTTP
- Mode de déploiement (appairage Connector ou Azure VNet)
- Ressources Azure

  - Noms des groupes de ressources
  - Réseaux virtuels (adresses IP, CIDR)
  - Sous-réseaux (adresses IP, CIDR)
  - Noms des machines virtuelles

Transmission de données

Le service Citrix Adaptive Authentication envoie des journaux aux destinations (Splunk) protégées par la sécurité de la couche transport.

Contrôle des données

Le service Citrix Adaptive Authentication ne fournit actuellement aucune option permettant aux clients de désactiver l'envoi de journaux ou d'empêcher la réplication globale du contenu client.

Rétention des données

Sur la base de la stratégie de rétention des données de Citrix Cloud, les données de configuration du client sont purgées du service 90 jours (environ 3 mois) après l'expiration de l'abonnement.

Les destinations des journaux conservent leur stratégie de conservation des données spécifique au service.

- Pour les événements stockés dans Citrix Application Delivery Management. Consultez la section Gouvernance des données NetScaler ADM.
- Les journaux Splunk sont archivés et finalement supprimés après 90 jours (environ 3 mois).
- Les instances Adaptive Authentication sont désallouées 30 jours (environ quatre semaines et demie) après l'expiration de l'abonnement.

Exportation de données

Il existe différentes options d'exportation de données pour plusieurs types de journaux.

- Les journaux d'audit de l'administrateur sont accessibles depuis la console Citrix Cloud System Log.
- Les journaux Splunk ne sont pas destinés aux clients. Ces événements peuvent également être exportés depuis Splunk sous forme de fichier CSV.

Définitions

- Le contenu client désigne toutes les données téléchargées sur un compte client pour le stockage ou les données dans un environnement client auquel Citrix a accès pour fournir les services.
- Le journal désigne un enregistrement des événements liés aux services, y compris les enregistrements qui mesurent les performances, la stabilité, l'utilisation, la sécurité et le support.
- Services signifie que les services Citrix Cloud décrits précédemment dans le but de faciliter les cas d'utilisation des clients.