



Service d'authentification fédérée

Contents

| | |
|---|------------|
| Service d'authentification fédérée 2311 | 2 |
| Problèmes résolus | 2 |
| Problèmes connus | 2 |
| Avis de tiers | 3 |
| Configuration système requise | 3 |
| Installer et configurer | 4 |
| Configuration avancée | 27 |
| Activer le service d'authentification fédérée pour un client locataire | 27 |
| Authentification unique avec Azure Active Directory | 30 |
| Configuration de l'autorité de certification | 34 |
| Protection de clé privée | 40 |
| Configuration du réseau et de la sécurité | 60 |
| Compteurs de performances | 74 |
| Résoudre les problèmes d'ouverture de session Windows | 76 |
| Applets de commande PowerShell | 100 |
| Architectures de déploiement | 101 |
| Déploiement ADFS | 112 |
| Intégration d'Azure AD | 116 |

Service d'authentification fédérée 2311

June 5, 2024

Cette version du Service d'authentification fédérée inclut les nouvelles fonctionnalités suivantes :

- **Demande de certificat du Service d'authentification fédérée améliorée pour inclure le SID.**
La demande de certificat du FAS à l'autorité de certification a été améliorée pour inclure le paramètre SID. Pour les utilisateurs qui activent l'option **Fournir dans la demande** des propriétés du **nom du sujet** dans le modèle `Citrix_SmartcardLogon`, cet ajout permet à FAS de fonctionner avec les modifications d'authentification des certificats détaillées dans l'article [KB5014754](#). Ces modifications d'authentification sont déjà prises en charge pour les utilisateurs qui utilisent le paramètre par défaut **Créer à partir de ces informations Active Directory**.

Pour plus d'informations sur les corrections de bogues, consultez la section [Problèmes résolus](#).

Problèmes résolus

June 5, 2024

Il n'y a pas de problèmes résolus dans Service d'authentification fédérée 2311.

Problèmes connus

June 5, 2024

Il n'y a aucun problème connu dans Service d'authentification fédérée 2311.

L'avertissement suivant s'applique à toute solution qui suggère de modifier une entrée de registre :

Avertissement :

Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veuillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Avis de tiers

June 5, 2024

Cette version du Service d'authentification fédérée peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans les documents suivants :

- [Avis de tiers pour Citrix Virtual Apps and Desktops](#) (téléchargement PDF)
- [Divulgations de logiciels non commerciaux pour FlexNet Publisher 2017 \(11.15.0.0\)](#) (téléchargement PDF)
- [Supplément à la documentation FLEXnet Publisher Logiciels tiers et Open Source utilisés dans FlexNet Publisher 11.15.0](#) (Télécharger PDF)

Configuration système requise

June 5, 2024

- Le service d'authentification fédérée (FAS) est pris en charge sur les versions Windows Server suivantes :
 - Windows Server 2022, édition Standard et Datacenter
 - Windows Server 2019, éditions Standard et Datacenter, avec option Server Core
 - Windows Server 2016, éditions Standard et Datacenter, avec option Server Core
- Citrix vous recommande d'installer FAS sur un serveur qui ne présente aucun autre composant Citrix.
- Le serveur Windows doit être sécurisé car il a accès à un certificat d'autorité d'enregistrement et à une clé privée. Le certificat et la clé privée permettent au serveur d'émettre des certificats pour les utilisateurs du domaine. Le serveur a également accès aux certificats utilisateur de domaine et aux clés privées émis.
- Les [applets de commande PowerShell](#) de FAS nécessitent l'installation de Windows PowerShell 64 bits sur le serveur FAS.
- Une autorité de certification telle que Microsoft Enterprise ou toute autre autorité de certification validée dans le programme [Citrix Ready](#) est requise pour émettre des certificats utilisateur.
- Pour les autorités de certification autres que Microsoft, assurez-vous de ce qui suit :
 - L'autorité de certification (CA) est enregistrée dans Active Directory en tant que service d'inscription.

- Le certificat CA se trouve dans le magasin NTAAuth du contrôleur de domaine. Pour plus d'informations, consultez [Comment importer des certificats d'autorités de certification \(CA\) tierces dans le magasin Enterprise NTAAuth](#).

Dans le site Citrix Virtual Apps ou Citrix Virtual Desktops :

- Les Delivery Controller, les VDA et les serveurs StoreFront doivent tous être des versions prises en charge.
- Avant de créer le catalogue de machines, appliquez la configuration de la stratégie de groupe Service d'authentification fédérée aux VDA. Pour plus d'informations, consultez la section [Configurer la stratégie de groupe](#).

Lors de la planification de votre déploiement de ce service, veuillez consulter la section [Considérations de sécurité](#).

Installer et configurer

June 5, 2024

Séquence d'installation et de configuration

1. [Installer le Service d'authentification fédérée \(FAS\)](#)
2. [Activer le plug-in FAS sur des magasins StoreFront](#)
3. [Configurer le Delivery Controller](#)
4. [Configurer une stratégie de groupe](#)
5. Utiliser la console d'administration FAS pour :
 - a) [Déployer des modèles de certificat](#)
 - b) [Configurer les autorités de certification](#)
 - c) [Autoriser FAS de sorte qu'il utilise vos autorités de certification](#)
 - d) [Configurer des règles](#)
 - e) [Connecter FAS à Citrix Cloud](#) (facultatif)

Installer le Service d'authentification fédérée

Pour des raisons de sécurité, Citrix recommande d'installer le Service d'authentification fédérée (FAS) sur un serveur dédié. Ce serveur doit être sécurisé de la même manière qu'un contrôleur de domaine ou une autorité de certification. FAS peut être installé :

- depuis le programme d'installation Citrix Virtual Apps and Desktops (à partir du bouton **Service d'authentification fédérée** de l'écran de démarrage automatique lorsque l'ISO est inséré), ou
- depuis le fichier d'installation FAS autonome (disponible en tant que fichier MSI sur [Téléchargements de Citrix](#)).

Installent les composants suivants :

- Service d'authentification fédérée
- [Applets de commande du composant logiciel enfichable PowerShell](#) pour la configuration FAS avancée
- [Console d'administration FAS](#)
- Modèles de stratégie de groupe FAS (CitrixFederatedAuthenticationService.admx/adml)
- Fichiers de modèles de certificats
- [Compteurs de performances](#) et [journaux d'événements](#)

Mise à niveau de FAS

Vous pouvez mettre à niveau FAS vers une version plus récente à l'aide d'une mise à niveau sur place. Avant la mise à niveau, tenez compte des points suivants :

- Tous les paramètres du serveur FAS sont conservés lorsque vous effectuez une mise à niveau sur place.
- Assurez-vous de fermer la console d'administration FAS avant de mettre à niveau FAS.
- Assurez-vous qu'au moins un serveur FAS est toujours disponible. Si aucun serveur n'est accessible par un serveur StoreFront activé par le Service d'authentification fédérée, les utilisateurs ne peuvent pas se connecter ni démarrer d'applications.

Pour démarrer une mise à niveau, installez FAS à partir du programme d'installation Citrix Virtual Apps and Desktops ou du fichier d'installation FAS autonome.

Activer le plug-in FAS sur des magasins StoreFront

Remarque :

Cette étape n'est pas nécessaire si vous utilisez FAS uniquement avec Citrix Cloud.

Pour activer l'intégration de FAS sur un magasin StoreFront, exécutez les applets de commande PowerShell suivantes sous un compte d'administrateur. Si le magasin a un nom différent, modifiez `$StoreVirtualPath`.

```
1 Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2 $StoreVirtualPath = "/Citrix/Store"
3 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
```

```
4 $auth = Get-STFAuthenticationService -StoreService $store
5 Set-STFClaimsFactoryNames -AuthenticationService $auth -
  ClaimsFactoryName "FASClaimsFactory"
6 Set-STFStoreLaunchOptions -StoreService $store -
  VdaLogonDataProvider "FASLogonDataProvider"
7 <!--NeedCopy-->
```

Pour arrêter d'utiliser FAS, utilisez le script PowerShell suivant :

```
1 Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2 $StoreVirtualPath = "/Citrix/Store"
3 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4 $auth = Get-STFAuthenticationService -StoreService $store
5 Set-STFClaimsFactoryNames -AuthenticationService $auth -
  ClaimsFactoryName "standardClaimsFactory"
6 Set-STFStoreLaunchOptions -StoreService $store -
  VdaLogonDataProvider ""
7 <!--NeedCopy-->
```

Configurer le Delivery Controller

Remarque :

Cette étape n'est pas nécessaire si vous utilisez FAS uniquement avec Citrix Cloud.

Pour utiliser FAS, configurez le Delivery Controller Citrix Virtual Apps ou Citrix Virtual Desktops de manière à approuver les serveurs StoreFront qui s'y connectent : exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true**. Exécutez cette commande une seule fois par site, quel que soit le nombre de Delivery Controller présents sur le site.

Configurer une stratégie de groupe

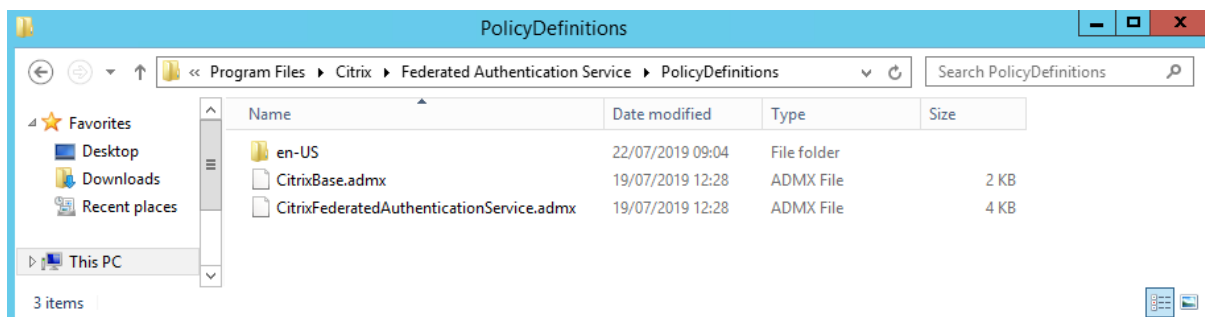
Après avoir installé FAS, utilisez les modèles de stratégie de groupe fournis dans le cadre de l'installation pour spécifier les noms de domaine complets des serveurs dans une stratégie de groupe.

Important :

Assurez-vous que les serveurs StoreFront qui demandent des tickets et les VDA (Virtual Delivery Agent) utilisant des tickets disposent de noms de domaine complets identiques, y compris l'attribution automatique de numéros appliquée aux serveurs par l'objet de stratégie de groupe.

À des fins de simplicité, les exemples suivants configurent une seule stratégie au niveau du domaine qui s'applique à toutes les machines. Cependant, cela n'est pas requis. FAS fonctionne tant que les serveurs StoreFront, les VDA, et la machine exécutant la console d'administration FAS voient la même liste de noms de domaine complets. Voir l'étape 6.

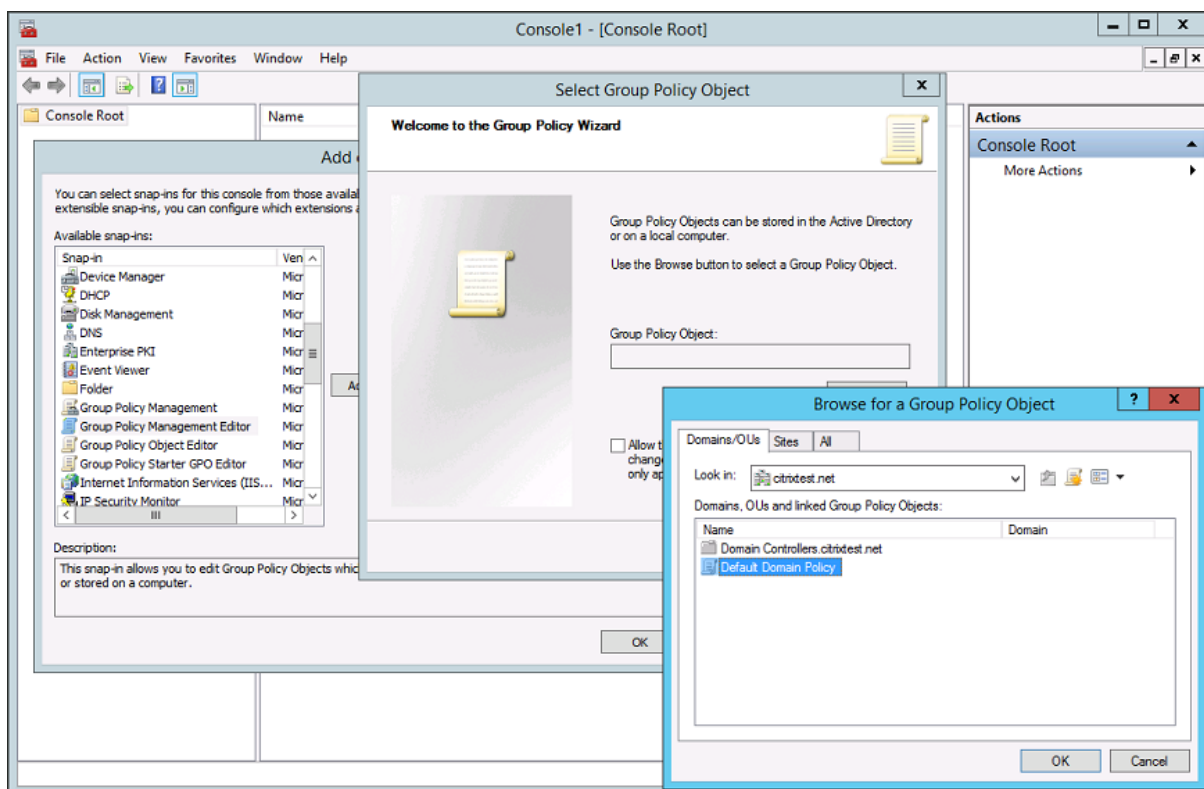
Étape 1. Sur le serveur sur lequel vous avez installé FAS, localisez les fichiers C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx et CitrixBase.admx, ainsi que le dossier en-US.



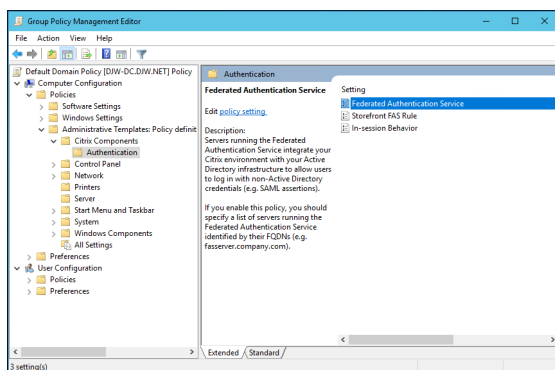
Étape 2. Copiez ces fichiers sur vos contrôleurs de domaine et placez-les dans C:\Windows\PolicyDefinitions et le sous-dossier en-US.

Étape 3. Exécutez la console Microsoft Management Console (mmc.exe à partir de la ligne de commande). À partir de la barre de menu, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**. Ajoutez l'**éditeur de gestion des stratégies de groupe**.

Lorsque vous y êtes invité par un objet de stratégie de groupe, sélectionnez **Parcourir**, puis sélectionnez la **stratégie de domaine par défaut**. Éventuellement, vous pouvez créer et sélectionner un objet de stratégie approprié pour votre environnement, à l'aide des outils de votre choix. La stratégie doit être appliquée à toutes les machines exécutant des logiciels Citrix affectés (VDA, serveurs StoreFront, outils d'administration).



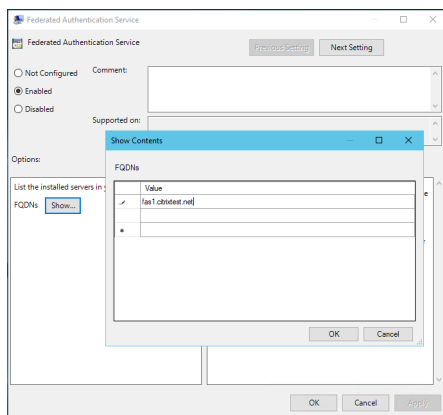
Étape 4. Accédez à la stratégie *Service d'authentification fédérée* dans Configuration ordinateur/S-tratégies/Modèles d'administration/Composants Citrix/Authentification.



Remarque :

Le paramètre de stratégie Service d'authentification fédérée est uniquement disponible sur un objet de stratégie de groupe du domaine lorsque vous ajoutez le fichier de modèle CitrixBase.admx/CitrixBase.adml au dossier PolicyDefinitions. Après l'étape 3, le paramètre de stratégie Service d'authentification fédérée est répertorié dans le dossier **Modèles d'administration > Composants Citrix > Authentification**.

Étape 5. Ouvrez la stratégie Service d'authentification fédérée et sélectionnez **Activé**. Cela vous permet de sélectionner le bouton **Afficher**, dans lequel vous pouvez configurer les noms de domaine complets de vos serveurs FAS.



Étape 6. Entrez les noms de domaine complets des serveurs FAS.

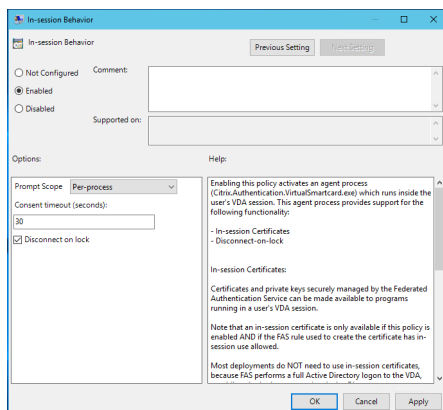
Important :

Si vous entrez plusieurs noms de domaine complets, l'ordre de la liste doit être cohérent pour les VDA, les serveurs StoreFront (le cas échéant) et les serveurs FAS. Consultez la section [Paramètres de stratégie de groupe](#).

Étape 7. Cliquez sur **OK** pour quitter l'assistant de stratégie de groupe et appliquer les modifications à la stratégie de groupe. Vous devrez peut-être redémarrer les machines (ou exécuter **gpupdate /force** à partir de la ligne de commandes) pour que les modifications soient appliquées.

Comportement en session

Cette stratégie active un processus d'agent dans la session VDA de l'utilisateur qui prend en charge les certificats en session, le consentement et la déconnexion au verrouillage. Les certificats en session ne sont disponibles que si cette stratégie est activée et si la règle FAS utilisée pour créer le certificat est autorisée. Reportez-vous à la section [Configurer des règles](#).



Activer active cette stratégie et permet à un processus d'agent FAS de s'exécuter dans la session VDA de l'utilisateur.

Désactiver désactive la stratégie et arrête l'exécution du processus d'agent FAS.

Prompt Scope Si cette stratégie est activée, **Prompt Scope** contrôle la manière dont les utilisateurs sont invités à consentir à autoriser une application à utiliser un certificat en cours de session. Il existe trois options :

- **No consent required** : cette option désactive l'invite de sécurité et les clés privées sont utilisées silencieusement.
- **Per-process consent** : chaque programme exécuté demande un consentement individuel.
- **Per-session consent** : une fois que l'utilisateur a cliqué sur **OK**, cette option s'applique à tous les programmes de la session.

Consent Timeout Si cette stratégie est activée, **Consent Timeout** contrôle la durée (en secondes) du consentement. Par exemple, si elle est réglée sur 300 secondes, les utilisateurs voient une invite toutes les cinq minutes. Une valeur de zéro invite les utilisateurs à donner leur consentement pour chaque opération de clé privée.

Déconnexion après verrouillage Si cette stratégie est activée, la session de l'utilisateur est automatiquement déconnectée lorsqu'il verrouille l'écran. Ce comportement est similaire à la stratégie de « déconnexion lors du retrait de la carte à puce ». Utilisez cette fonctionnalité lorsque les utilisateurs ne disposent pas d'informations d'identification de connexion Active Directory.

Remarque :

La stratégie de déconnexion après verrouillage s'applique à toutes les sessions sur le VDA.

Utiliser la console d'administration du Service d'authentification fédérée

Remarque :

Bien que la console d'administration FAS convienne à la plupart des déploiements, l'interface PowerShell offre des options plus avancées. Pour plus d'informations sur les applets de commande FAS PowerShell, consultez [Applets de commande PowerShell](#).

La console d'administration FAS est installée dans le cadre de FAS. Une icône (Service d'authentification fédérée de Citrix) est placée dans le menu Démarrer.

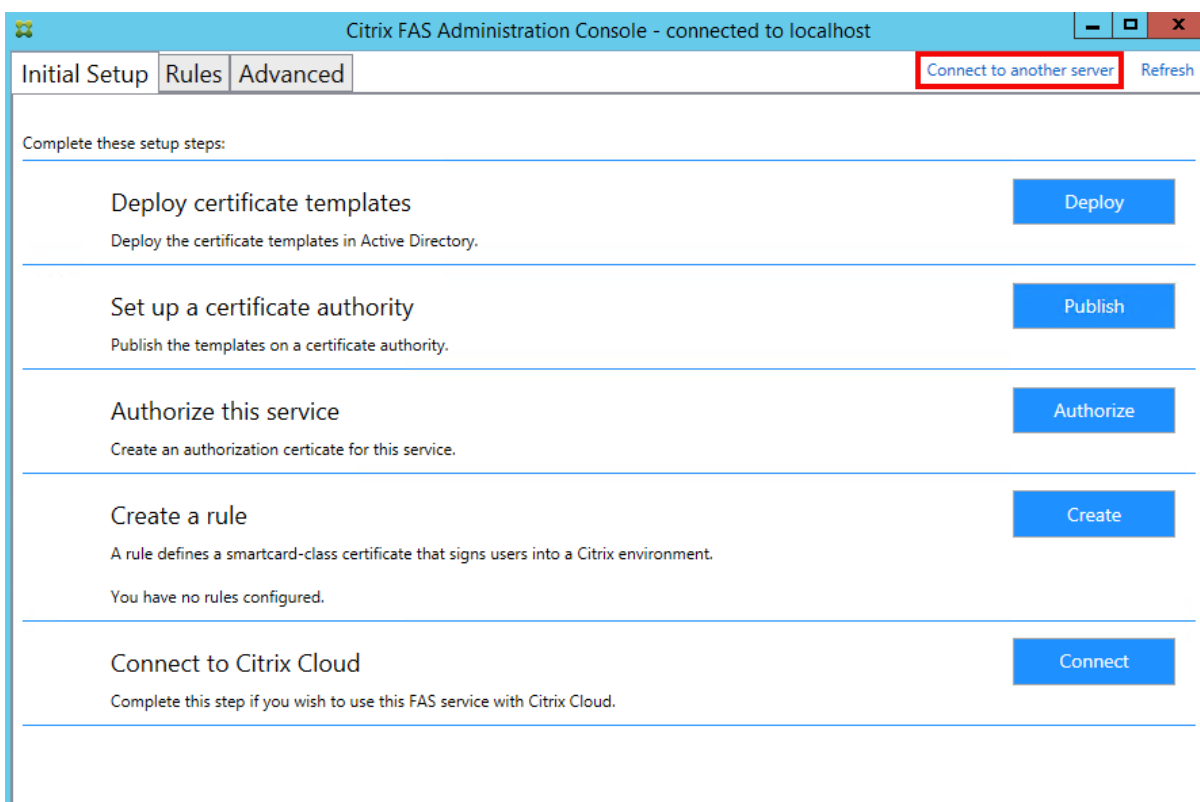
La première fois que vous utilisez la console d'administration, elle vous guide à travers les processus suivants pour :

- Déployez des modèles de certificat.
- Configurez l'autorité de certification.

- Autorisez FAS de sorte qu'il utilise l'autorité de certification.

Vous pouvez aussi utiliser les outils de configuration du système d'exploitation pour effectuer certaines étapes manuellement.

La console d'administration FAS effectue une connexion au service FAS local par défaut. Si nécessaire, vous pouvez vous connecter à un service distant à l'aide de **Se connecter à un autre serveur** en haut à droite de la console.

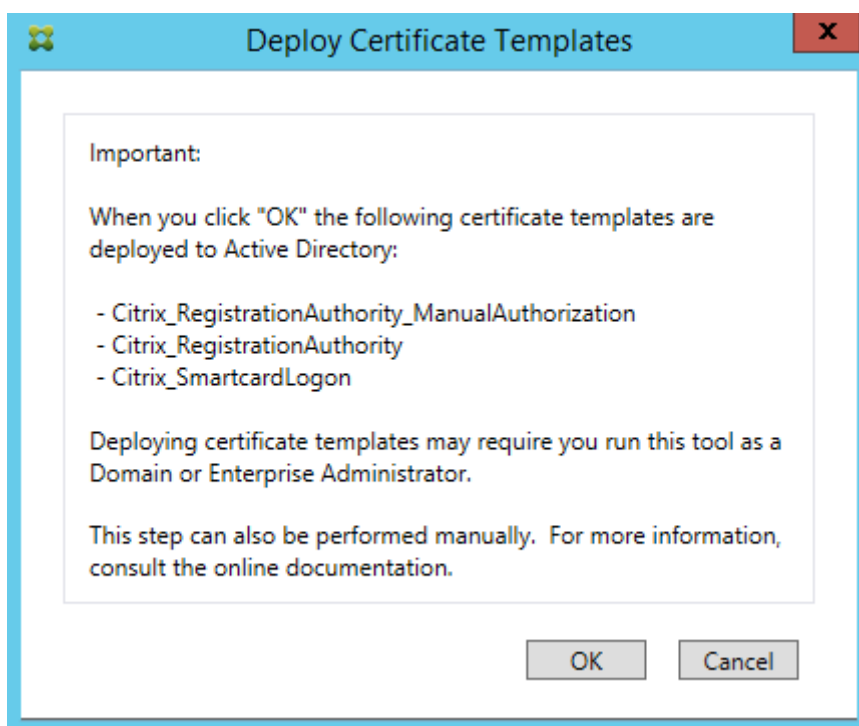


Déployer des modèles de certificat

Pour éviter des problèmes d'interopérabilité avec d'autres logiciels, FAS offre trois modèles de certificats Citrix pour son propre usage.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Ces modèles doivent être enregistrés auprès d'Active Directory. Cliquez sur le bouton **Déployer**, puis cliquez sur **OK**.



La configuration des modèles peut être trouvée dans les fichiers XML avec l'extension .certificatetemplate qui sont installés avec FAS dans :

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

| Name | Date modified | Type | Size |
|--|-------------------|-------------------|------|
| Citrix_RegistrationAuthority.certificatetemplate | 2/10/2020 5:23 AM | CERTIFICATETEMPL. | 6 KB |
| Citrix_RegistrationAuthority_ManualAuthorization.certificatetemplate | 2/10/2020 5:23 AM | CERTIFICATETEMPL. | 7 KB |
| Citrix_SmartcardLogon.certificatetemplate | 2/10/2020 5:23 AM | CERTIFICATETEMPL. | 5 KB |

Si vous ne disposez pas des autorisations nécessaires pour installer ces fichiers modèles, donnez-les à votre administrateur Active Directory.

Pour installer manuellement les modèles, vous pouvez exécuter les commandes PowerShell suivantes à partir du dossier contenant les modèles :

```

1   $template = [System.IO.File]::ReadAllBytes("$Pwd\
2       Citrix_SmartcardLogon.certificatetemplate")
3   $CertEnrol = New-Object -ComObject X509Enrollment.
4       CX509EnrollmentPolicyWebService
5   $CertEnrol.InitializeImport($template)
6   $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
7   $writabletemplate = New-Object -ComObject X509Enrollment.
8       CX509CertificateTemplateADWritable
9   $writabletemplate.Initialize($comtemplate)
10  $writabletemplate.Commit(1, $NULL)
11  <!--NeedCopy-->

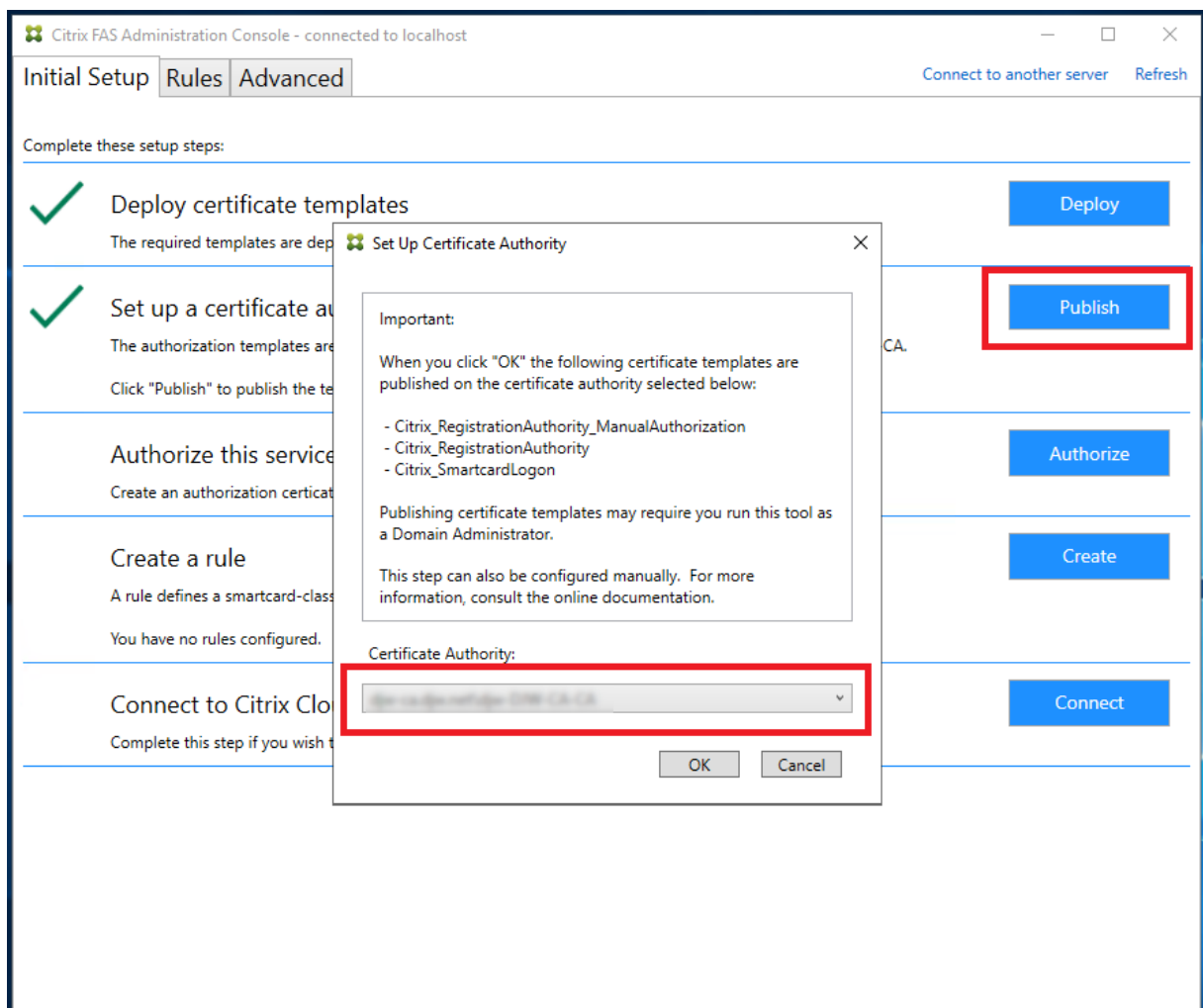
```

Configurer des services de certificats Active Directory

Après l'installation de modèles de certificats Citrix, ils doivent être publiés sur un ou plusieurs serveurs d'autorité de certification Microsoft Enterprise. Reportez-vous à la documentation Microsoft sur la manière de déployer des services de certificats Active Directory.

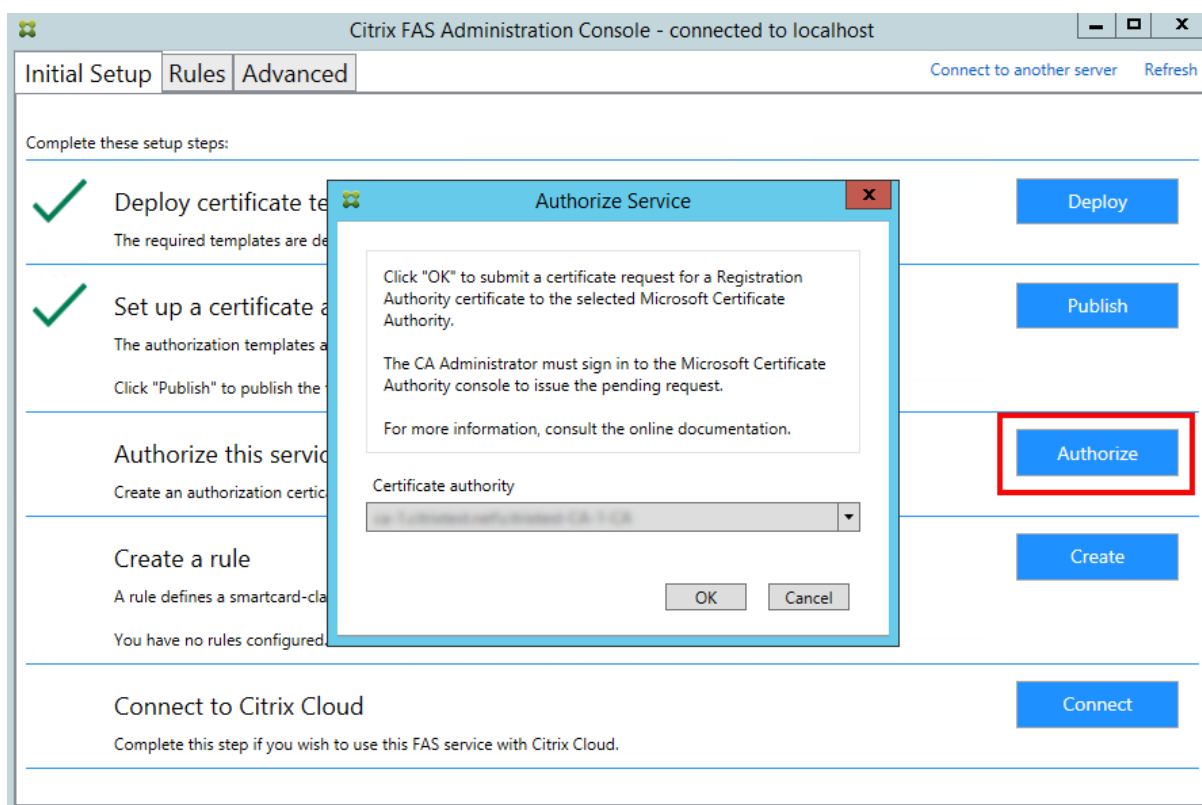
Un utilisateur autorisé à administrer l'autorité de certification doit publier les modèles sur au moins un serveur. Utilisez **Configurer une autorité de certification** pour les publier.

(Les modèles de certificats peuvent également être publiés à l'aide de la console Autorité de certification de Microsoft.)



Autoriser le Service d'authentification fédérée

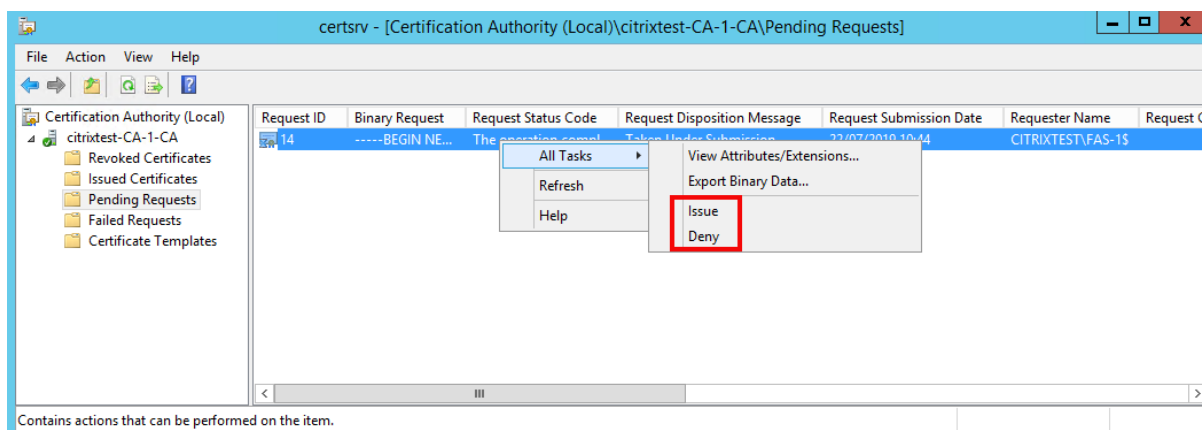
Cette étape initie l'autorisation de FAS. La console d'administration utilise le modèle Citrix_RegistrationAuthority_ManualAuthorization pour générer une requête de certificat, puis l'envoie à l'une des autorités de certification qui publient ce modèle.



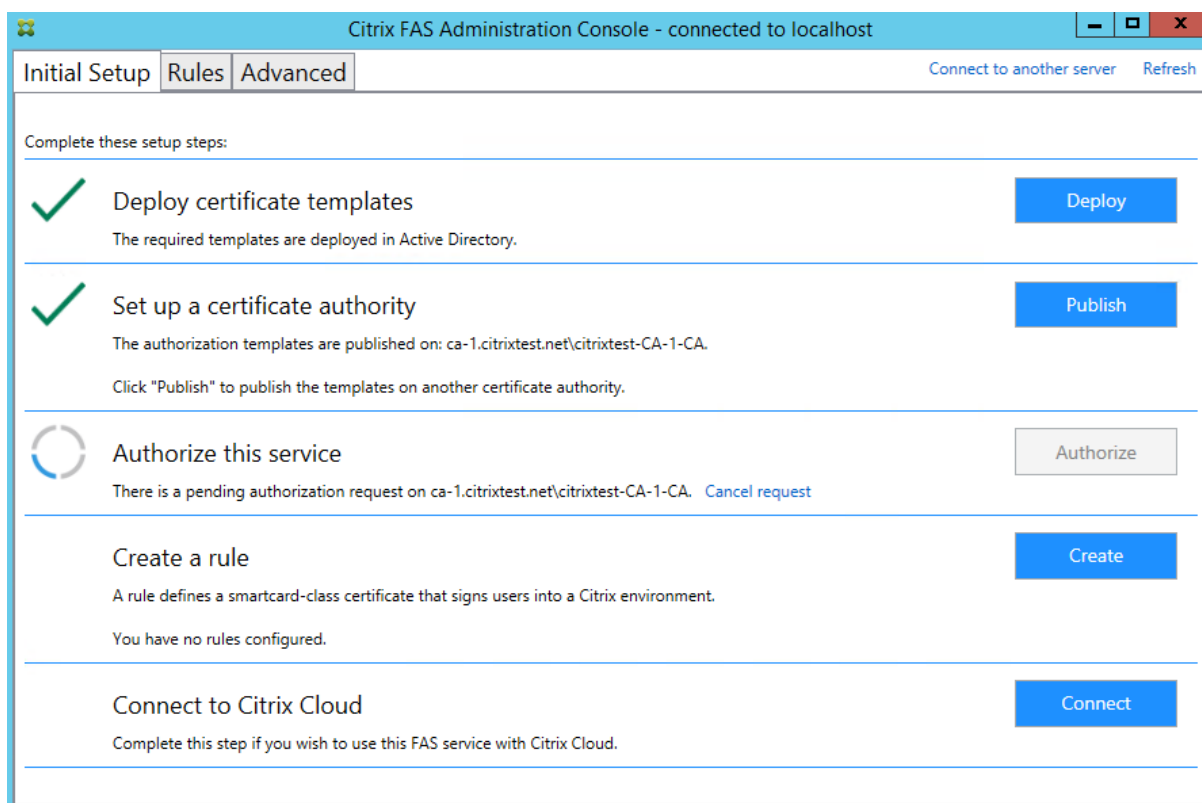
Une fois la requête envoyée, elle apparaît dans la liste **Demandes en attente** de la console Autorité de certification de Microsoft en tant que requête en attente du compte de machine FAS. L'administrateur de l'autorité de certification doit émettre ou rejeter la requête avant que la configuration de FAS puisse continuer.

La console d'administration FAS affiche un « compteur » jusqu'à ce que l'administrateur choisisse **Émettre** ou **Rejeter**.

Dans la console Autorité de certification Microsoft, cliquez avec le bouton droit sur **Toutes les tâches**, puis sélectionnez **Émettre** ou **Rejeter** pour la demande de certificat. Si vous choisissez **Émetteur**, la console d'administration FAS affiche le certificat d'autorisation. Si vous choisissez **Rejeter**, la console affiche un message d'erreur.



La console d'administration FAS détecte automatiquement lorsque ce processus est terminé. Cette opération peut prendre plusieurs minutes.



Configurer des règles

FAS utilise les règles pour autoriser l'émission de certificats pour l'ouverture de session sur des VDA et l'utilisation dans la session, conformément aux instructions de StoreFront.

Chaque règle précise les éléments suivants :

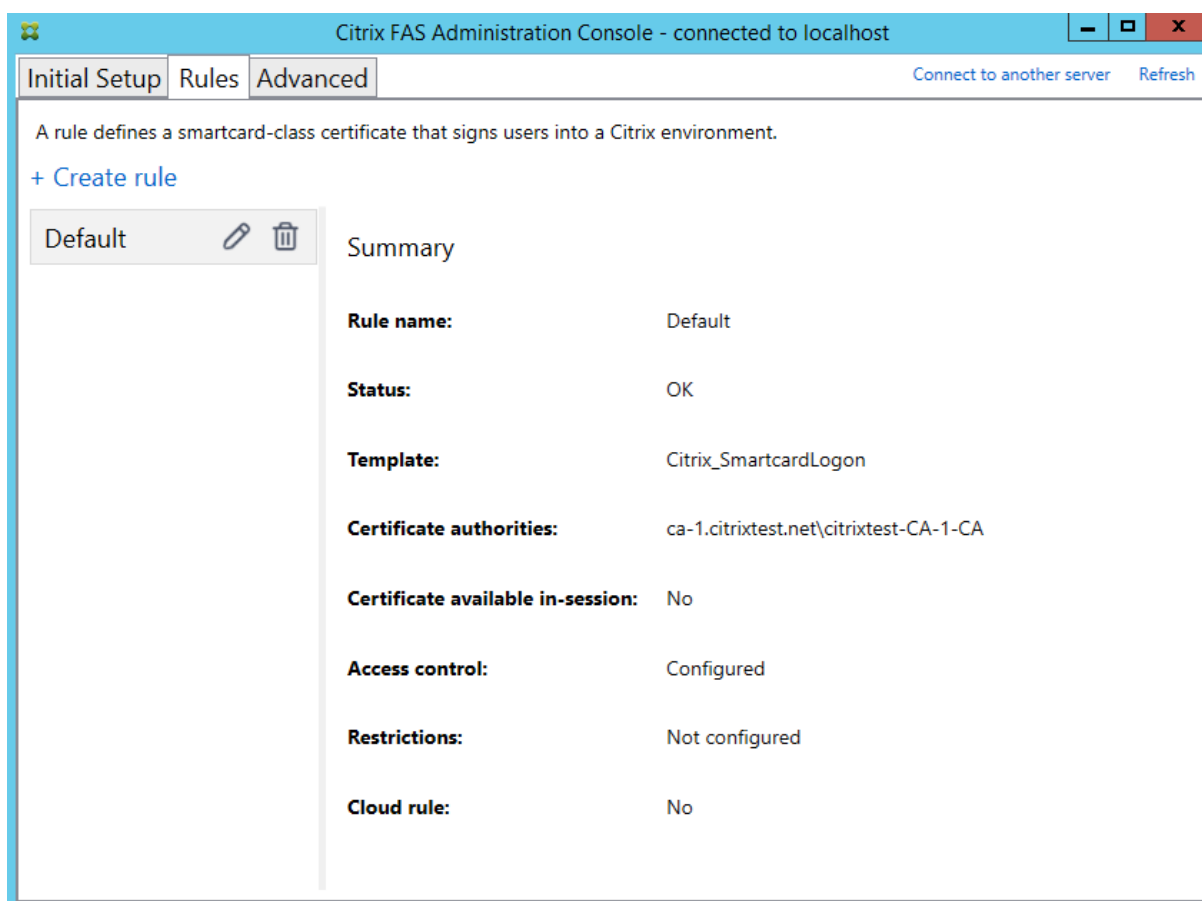
- Serveurs StoreFront fiables pour demander des certificats

- Ensemble d'utilisateurs pour lesquels les certificats sont demandés.
- Ensemble de machines VDA autorisées à utiliser les certificats.

Citrix recommande de créer une règle nommée « default », car StoreFront demande une règle du même nom lorsqu'il contacte FAS.

Vous pouvez créer des règles personnalisées supplémentaires pour référencer différents modèles de certificats et autorités de certification, et les configurer pour avoir des propriétés et des autorisations différentes. Ces règles peuvent être configurées pour être utilisées par différents serveurs StoreFront ou par Workspace. Configurez les serveurs StoreFront pour demander la règle personnalisée par nom à l'aide des options de configuration de stratégie de groupe.

Cliquez sur **Créer** (ou **Créer une règle** dans l'onglet « Règles ») pour démarrer l'assistant de création de règles qui recueille les informations nécessaires à la création de la règle. L'onglet « Règles » affiche un résumé de chaque règle.



L'assistant collecte les informations suivantes :

Template : modèle de certificat utilisé pour émettre des certificats utilisateur. Il doit s'agir du modèle Citrix_SmartcardLogon ou d'une copie modifiée de celui-ci (voir [Modèles de certificats](#)).

Autorité de certification : autorité de certification qui émet les certificats utilisateur et publie le mod-

èle. FAS prend en charge l'ajout de multiples autorités de certification à des fins de basculement et d'équilibrage de charge. Assurez-vous que le statut indique « Template available » (Modèle disponible) pour l'autorité de certification que vous choisissez. Consultez [Administration de l'autorité de certification](#).

In-Session Use : l'option **Allow in-session use** contrôle si un certificat peut être utilisé après l'ouverture de session sur le VDA.

- **Allow in-session use** non sélectionné (par défaut, *recommandé*) : le certificat est utilisé uniquement pour l'ouverture de session ou la reconnexion, et les utilisateurs n'ont pas accès au certificat après l'authentification.
- **Allow in-session use** sélectionné : les utilisateurs ont accès au certificat après l'authentification. La plupart des clients ne doivent pas sélectionner cette option. Les ressources accessibles depuis la session VDA, telles que les sites Web intranet ou les partages de fichiers, sont accessibles à l'aide de l'authentification unique Kerberos. Par conséquent, un certificat de session n'est pas requis.

Si vous sélectionnez **Allow in-session use**, la stratégie de groupe [Comportement en session](#) doit également être activée et appliquée au VDA. Les certificats sont alors placés dans le magasin de certificats personnel de l'utilisateur après l'ouverture de session afin que les applications puissent les utiliser. Par exemple, si vous exigez l'authentification TLS pour accéder aux serveurs Web dans la session VDA, Internet Explorer peut utiliser le certificat.

Access control : liste des serveurs StoreFront approuvés qui sont autorisés à demander des certificats pour l'ouverture de session ou la reconnexion des utilisateurs. Pour toutes ces autorisations, vous pouvez ajouter des objets ou des groupes AD individuels.

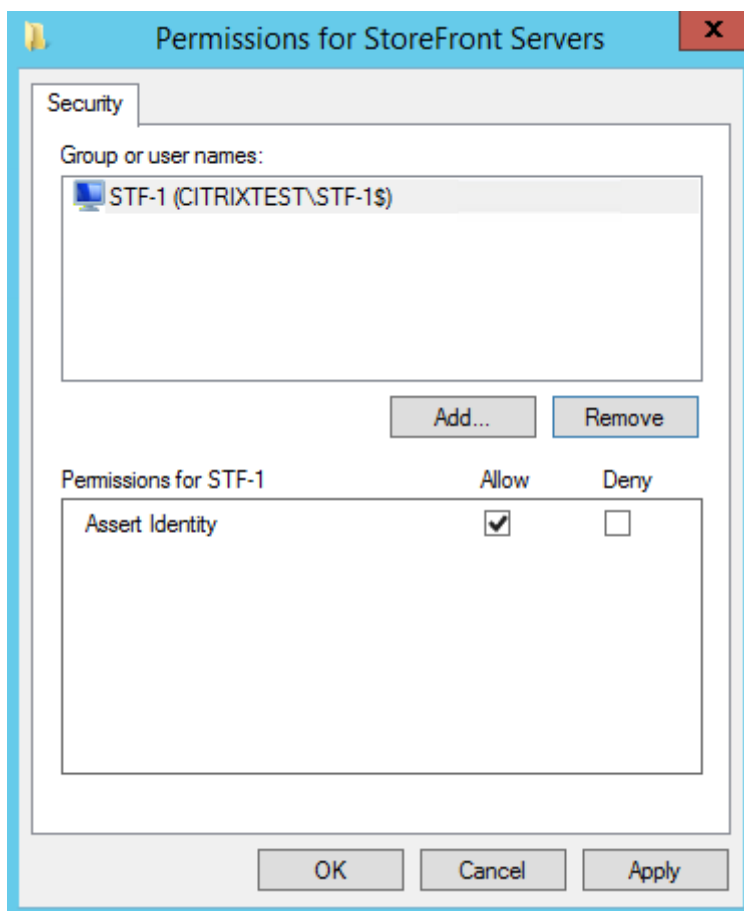
Important :

Notez que le paramètre **Access control** est critique à la sécurité et doit être géré avec soin.

Remarque :

Si vous utilisez le serveur FAS uniquement avec Citrix Cloud, vous n'avez pas besoin de configurer le contrôle d'accès. Lorsqu'une règle est utilisée par Citrix Cloud, les autorisations d'accès StoreFront sont ignorées. Vous pouvez utiliser la même règle avec Citrix Cloud et avec un déploiement StoreFront local. Les autorisations d'accès StoreFront sont toujours appliquées lorsque la règle est utilisée par un StoreFront local.

L'autorisation par défaut (« Assert Identity » autorisé) refuse tout. Par conséquent, vous devez autoriser explicitement vos serveurs StoreFront.

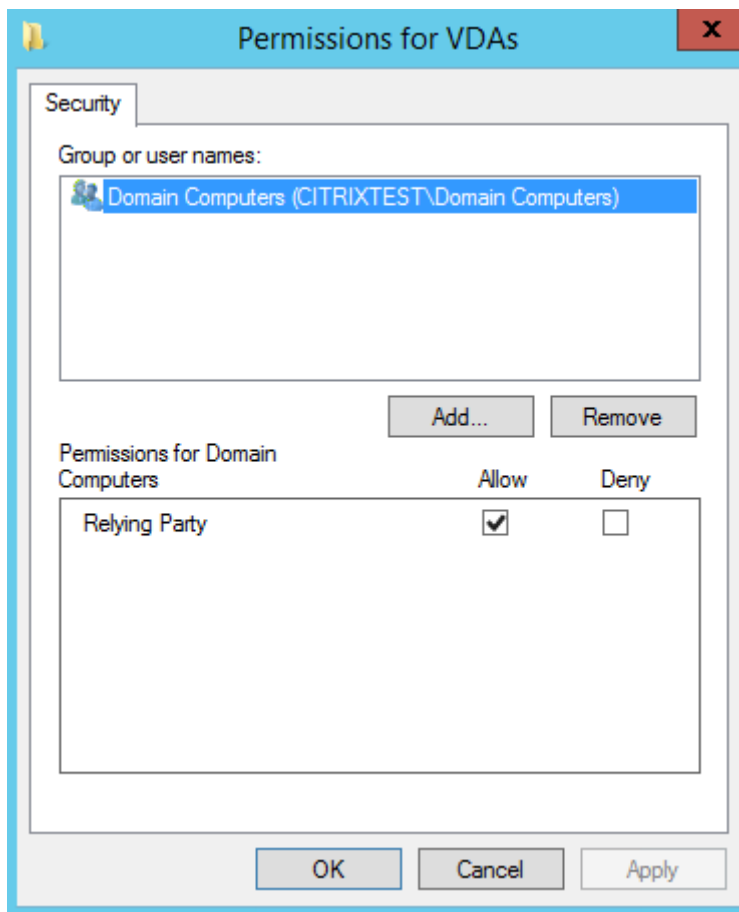


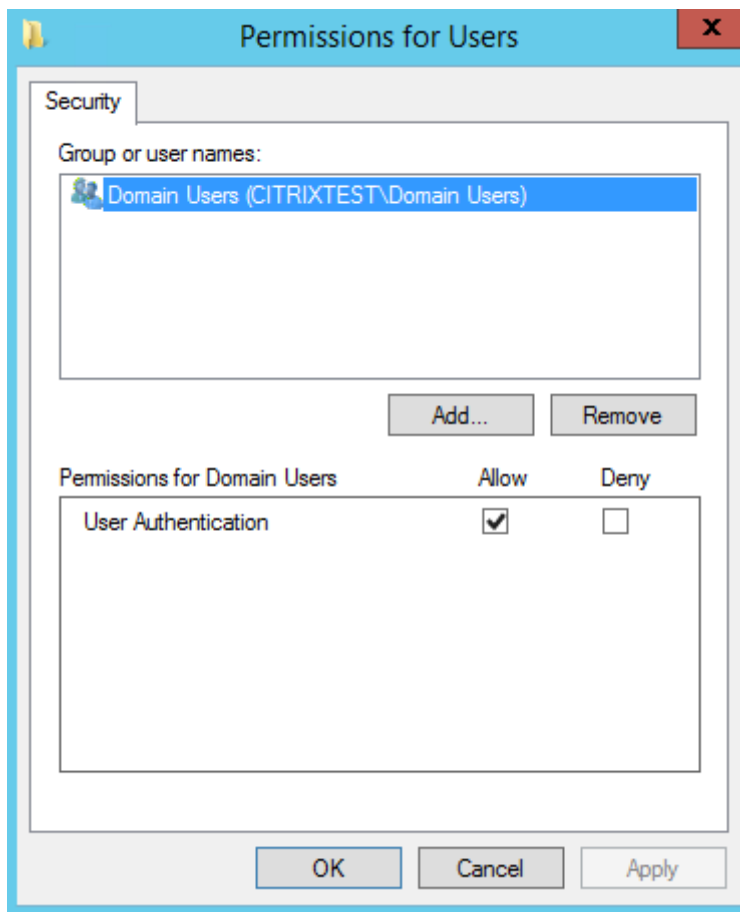
Restrictions : liste des machines VDA qui peuvent connecter les utilisateurs à l'aide de FAS et liste des utilisateurs auxquels des certificats peuvent être émis via FAS.

- **Manage VDA permissions** vous permet de spécifier quels VDA peuvent utiliser FAS pour connecter l'utilisateur. La liste des VDA est par défaut Domain Computers (Ordinateurs du domaine).
- **Manage user permissions** vous permet de spécifier quels utilisateurs peuvent utiliser FAS pour se connecter à un VDA. La liste des utilisateurs est par défaut Manage user permissions (Utilisateurs du domaine).

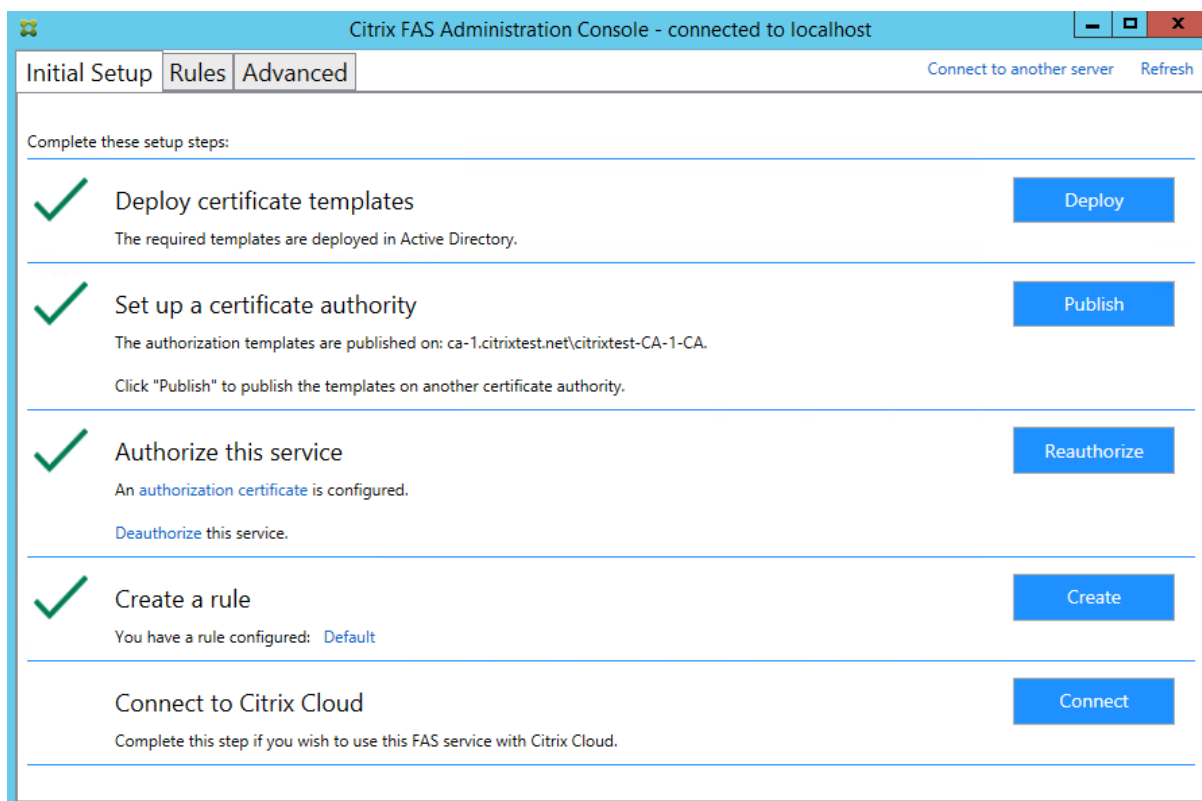
Remarque :

Si le domaine du serveur FAS est différent de celui des VDA et des utilisateurs, les restrictions par défaut doivent être modifiées.





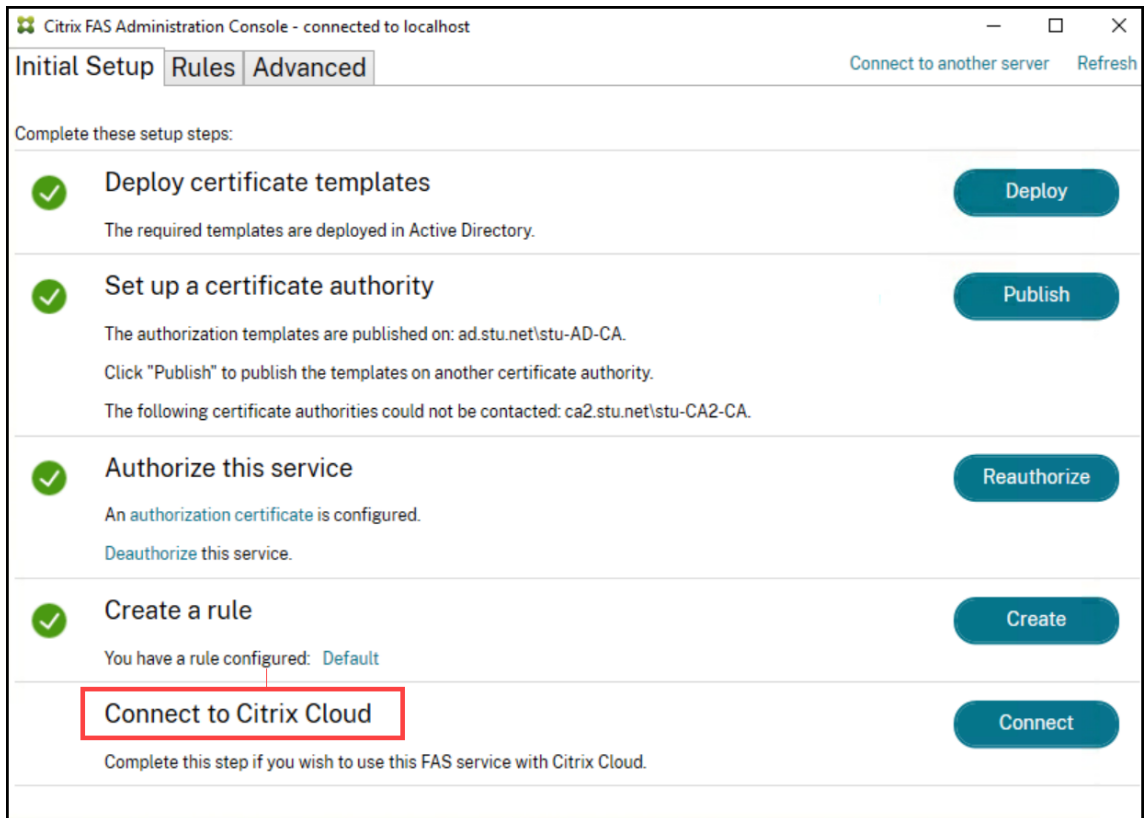
Cloud rule : indique si la règle est appliquée lorsque des assertions d'identité sont reçues à partir de Citrix Workspace. Lorsque vous vous connectez à Citrix Cloud, vous choisissez la règle à utiliser pour Citrix Cloud. Vous pouvez également modifier la règle après vous être connecté à Citrix Cloud à partir d'un lien dans la section **Connect to Citrix Cloud**.



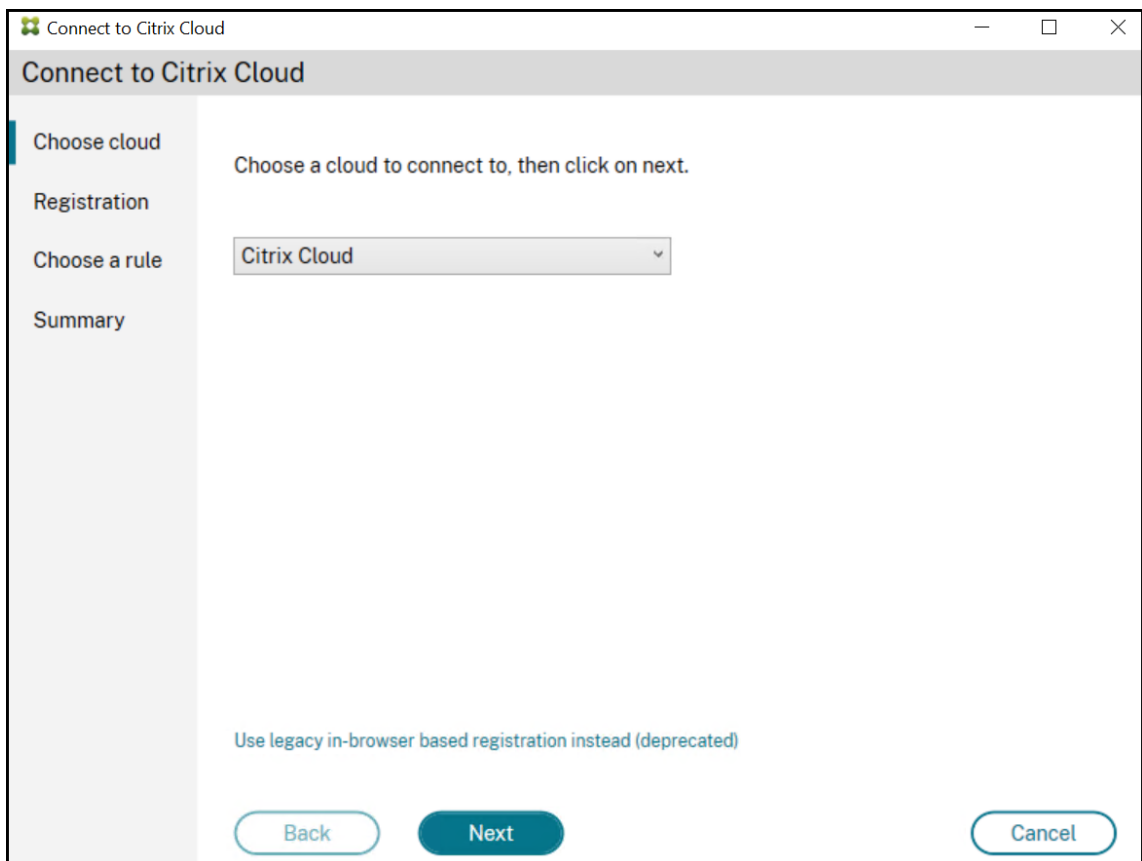
Se connecter à Citrix Cloud

Vous pouvez connecter le serveur FAS à Citrix Cloud avec Citrix Workspace. Consultez cet [article Citrix Workspace](#).

1. Dans l'onglet Initial Setup, pour **Connect to Citrix Cloud**, cliquez sur **Connect**.



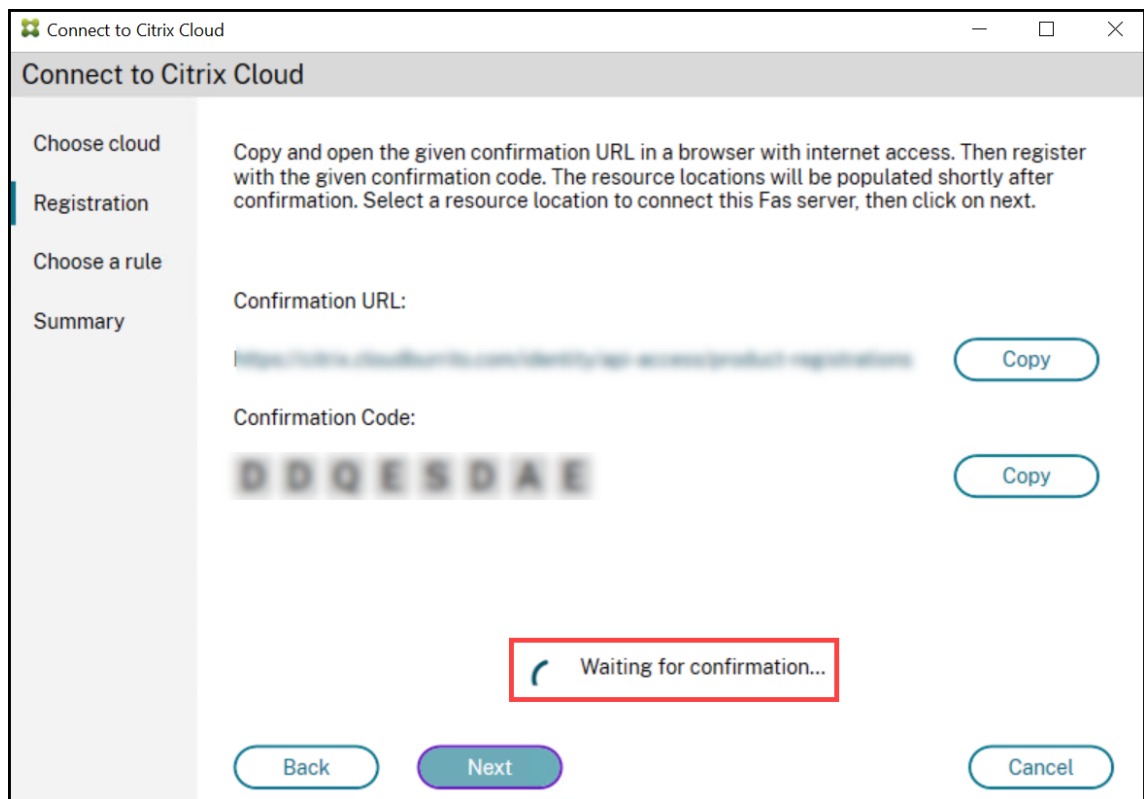
2. Sélectionnez le cloud auquel vous souhaitez vous connecter et cliquez sur **Next**.



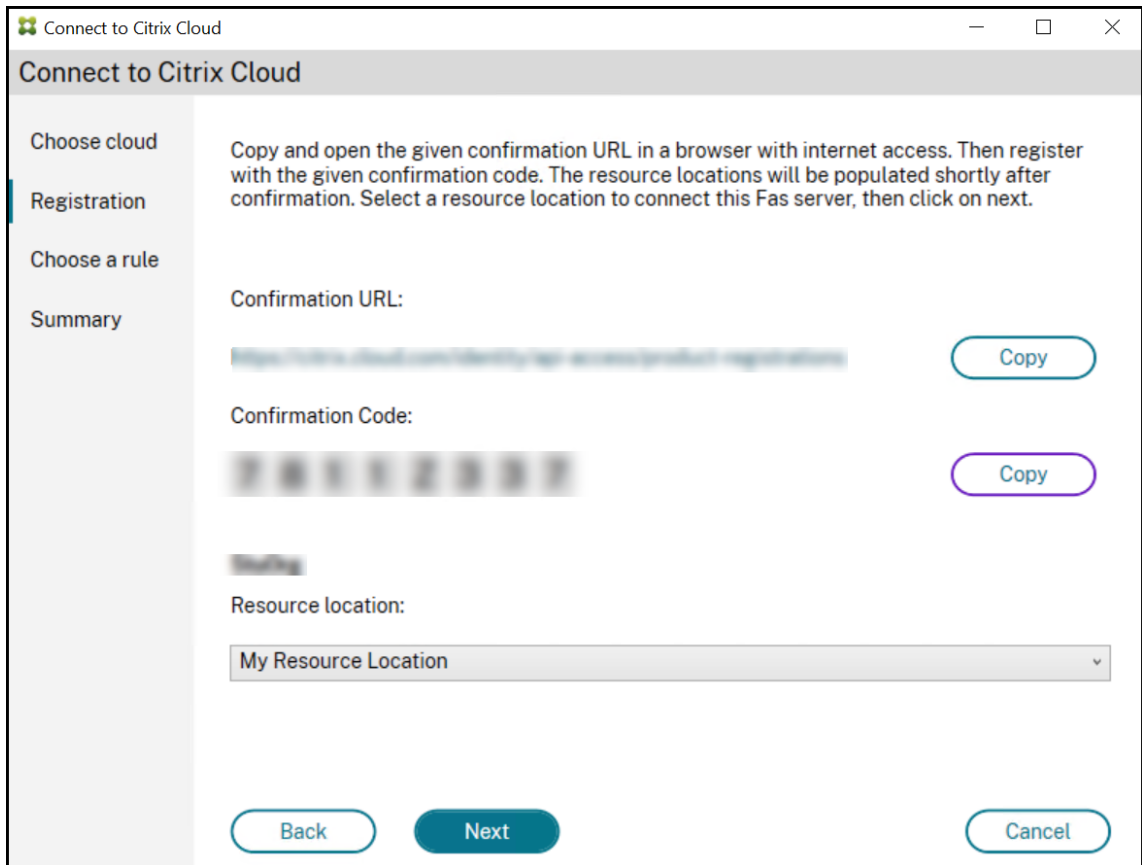
Remarque

Seul **Citrix Cloud** est disponible en Tech Preview.

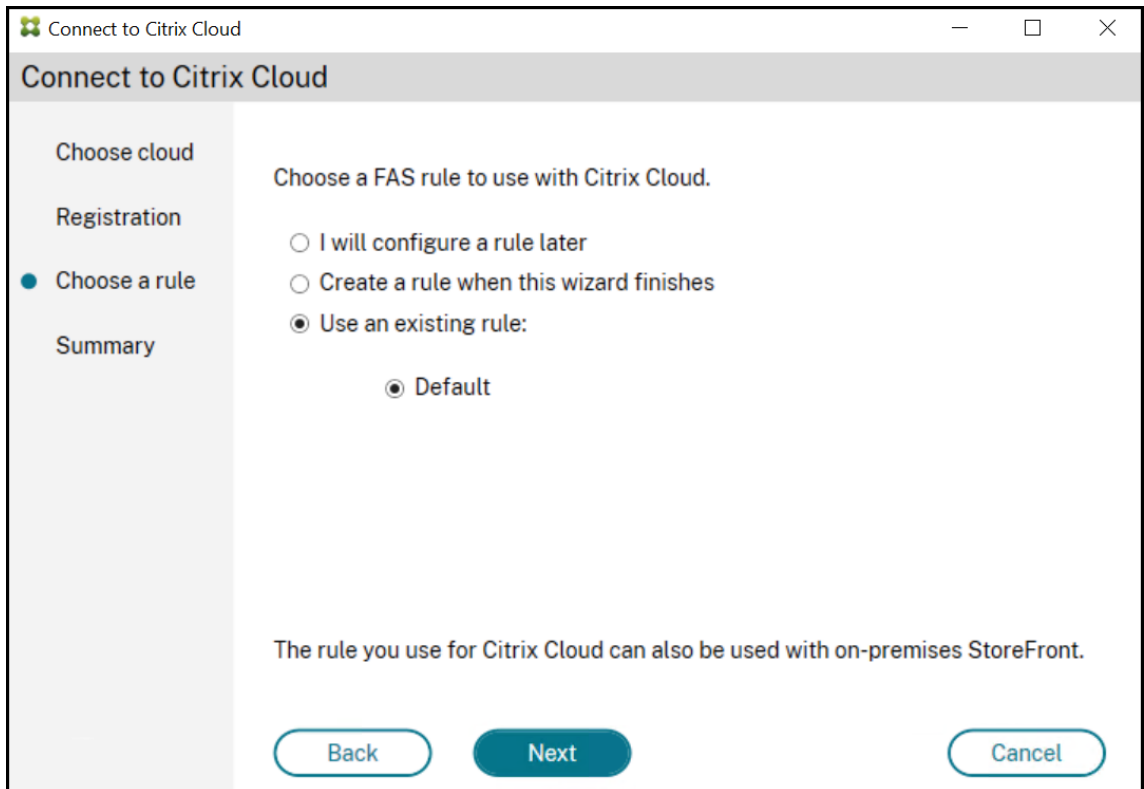
3. La fenêtre affiche un code d'enregistrement unique, qui doit être approuvé dans Citrix Cloud. Pour plus d'informations, consultez [Enregistrer des produits locaux avec Citrix Cloud](#).



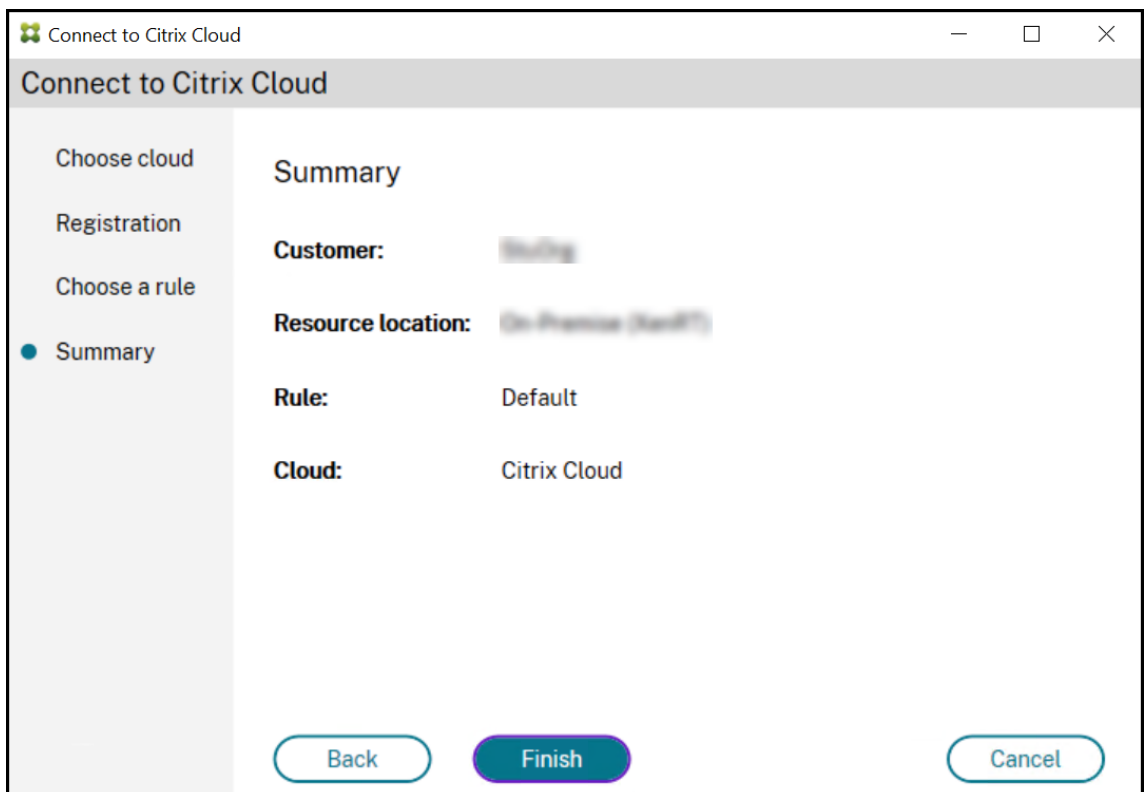
4. Une fois le code d'enregistrement validé, sélectionnez l'**emplacement de ressources** souhaité dans la liste déroulante.



5. Sélectionnez le compte client, le cas échéant, et sélectionnez l'emplacement de ressources où vous souhaitez connecter le serveur FAS. Cliquez sur **Continuer**, puis fermez la fenêtre de confirmation.
6. Dans la section **Choose a rule**, utilisez une règle existante ou créez-en une. Cliquez sur **Suivant**.



7. Dans la section **Summary**, cliquez sur **Finish** pour terminer la connexion à Citrix Cloud.



Citrix Cloud enregistre le serveur FAS et l'affiche sur la page Emplacements des ressources de votre compte Citrix Cloud.

Remarque

Un serveur FAS sur site peut émettre des certificats utilisateur pour autoriser l'accès à Citrix Cloud et à Citrix Virtual Apps and Desktops en même temps.

Déconnexion de Citrix Cloud

Après avoir supprimé le serveur FAS de votre emplacement de ressources Citrix Cloud, comme décrit dans cet [article Citrix Workspace](#), dans **Connect to Citrix Cloud**, sélectionnez **Disable**.

Configuration avancée

June 5, 2024

Les articles de cette section fournissent des informations de configuration et de gestion avancées pour le Service d'authentification fédérée (FAS).

Informations connexes

- L'article [Installer et configurer](#) est le document de référence principal pour obtenir des informations sur l'installation et la configuration de FAS.
- L'article [Architectures de déploiement](#) propose un résumé des principales architectures FAS, ainsi que des liens vers d'autres articles sur les architectures plus complexes.

Activer le service d'authentification fédérée pour un client locataire

June 5, 2024

Cet article décrit les étapes à suivre pour activer le service d'authentification fédérée (FAS) dans les environnements de fournisseur de services mobiles gérés (MSP). Pour plus d'informations, consultez [Architecture de référence : Citrix Service Provider DaaS](#).

Logiciels requis

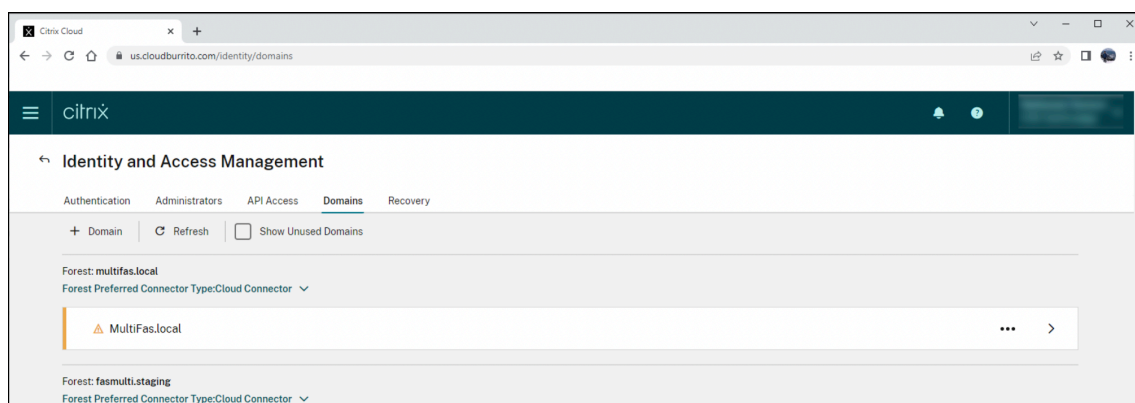
- Vous disposez d'un accès administrateur aux domaines et aux emplacements de ressources sur Citrix Cloud. Pour plus d'informations, consultez la section [Modifier les autorisations d'administrateur](#).
- Vous avez établi une relation locataire-MSP. Pour plus d'informations, consultez [Citrix DaaS pour les fournisseurs de services Citrix](#).

Configurer le client MSP

1. Utilisez un Cloud Connector pour mettre les domaines Active Directory à la disposition de Citrix Cloud.

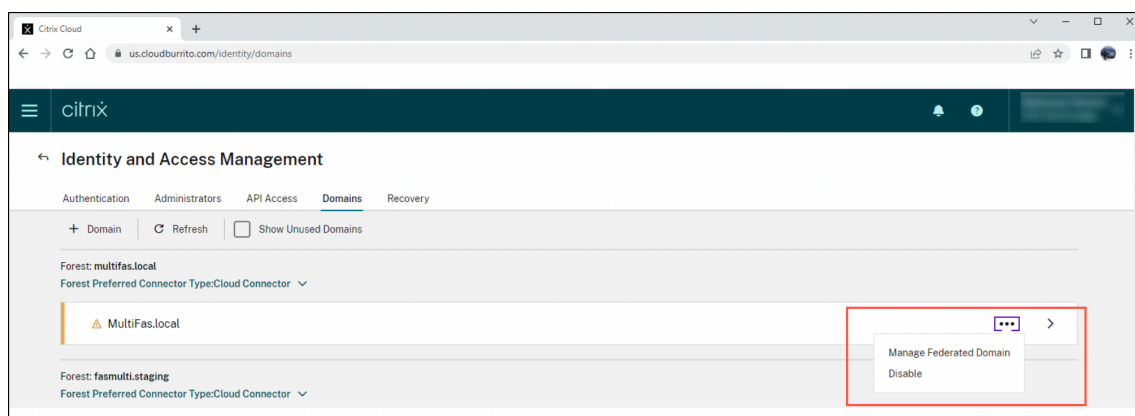
Connectez l'infrastructure locale à Citrix Cloud en [installant des Cloud Connector](#).

Vérifiez que les domaines associés au contrôleur de domaine local sont disponibles sous **Gestion des identités et des accès > Domaines**.

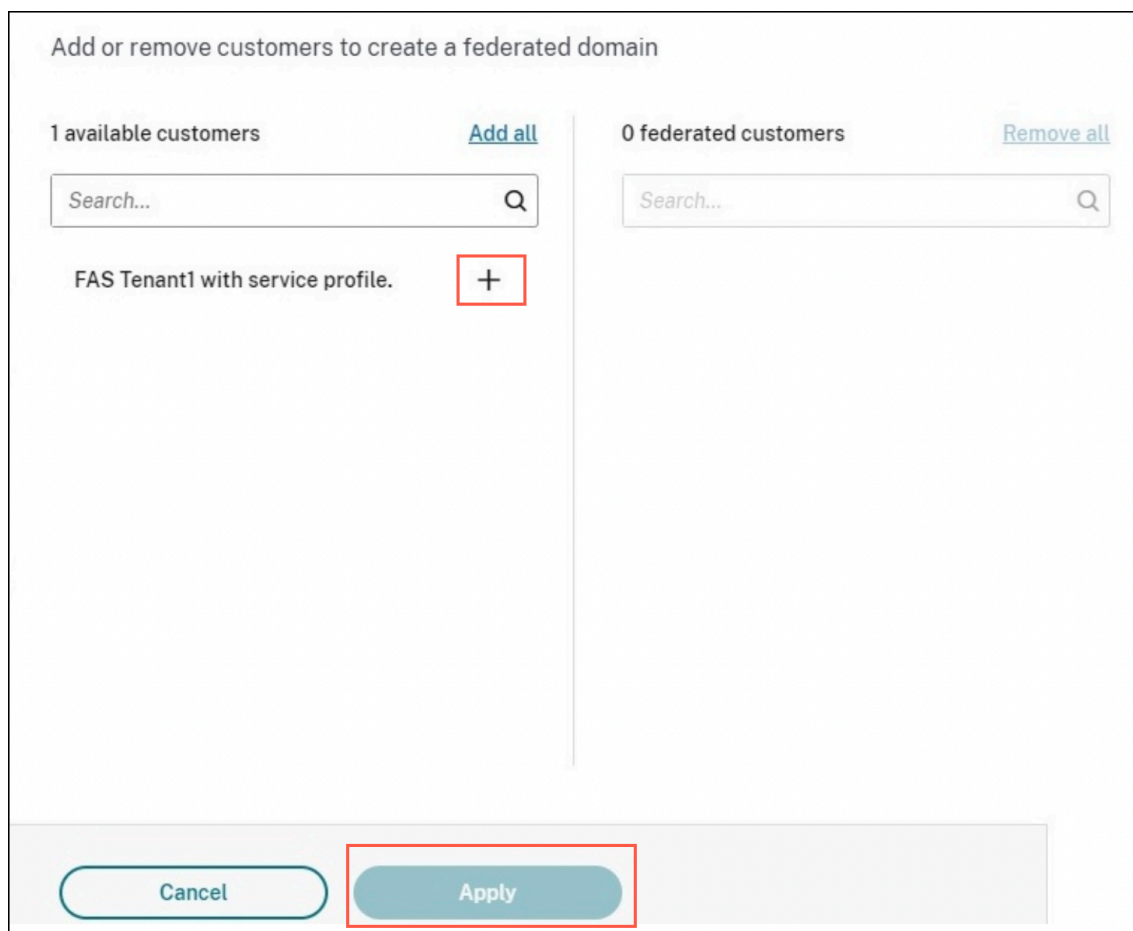


2. Fédérez le domaine au locataire.

Sélectionnez le domaine et cliquez sur le menu déroulant (...) et cliquez sur **Gérer les domaines fédérés**.

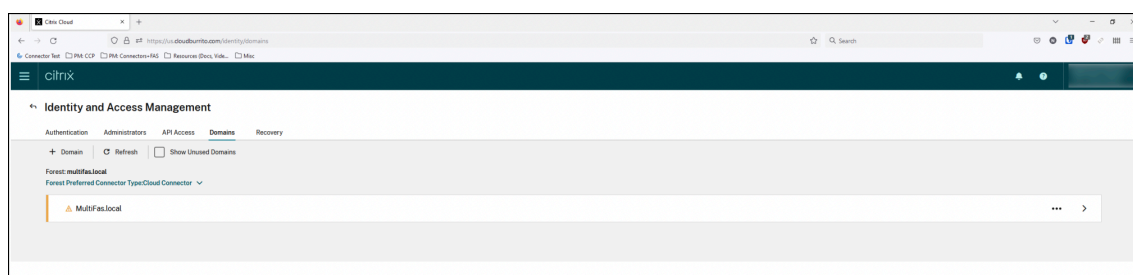


Recherchez le locataire et cliquez sur **+**. Cliquez ensuite sur **Appliquer**.



3. Vérifiez que les domaines associés sont présents dans le locataire.

Cette étape est facultative. Connectez-vous à la console des clients locataires et vérifiez que les domaines sont répertoriés sous **Gestion des identités et des accès > Domaines**.



Revenez au client MSP.

4. Installez et enregistrez un serveur FAS auprès de Citrix Cloud.

Installez FAS dans la forêt Active Directory (AD) où se trouvent les ressources Citrix Virtual Apps and Desktops du locataire. Connectez FAS à l'emplacement de ressources cloud associé à cette forêt AD. Pour installer un serveur FAS, consultez la section [Installer et configurer](#).

5. Configurez le client locataire

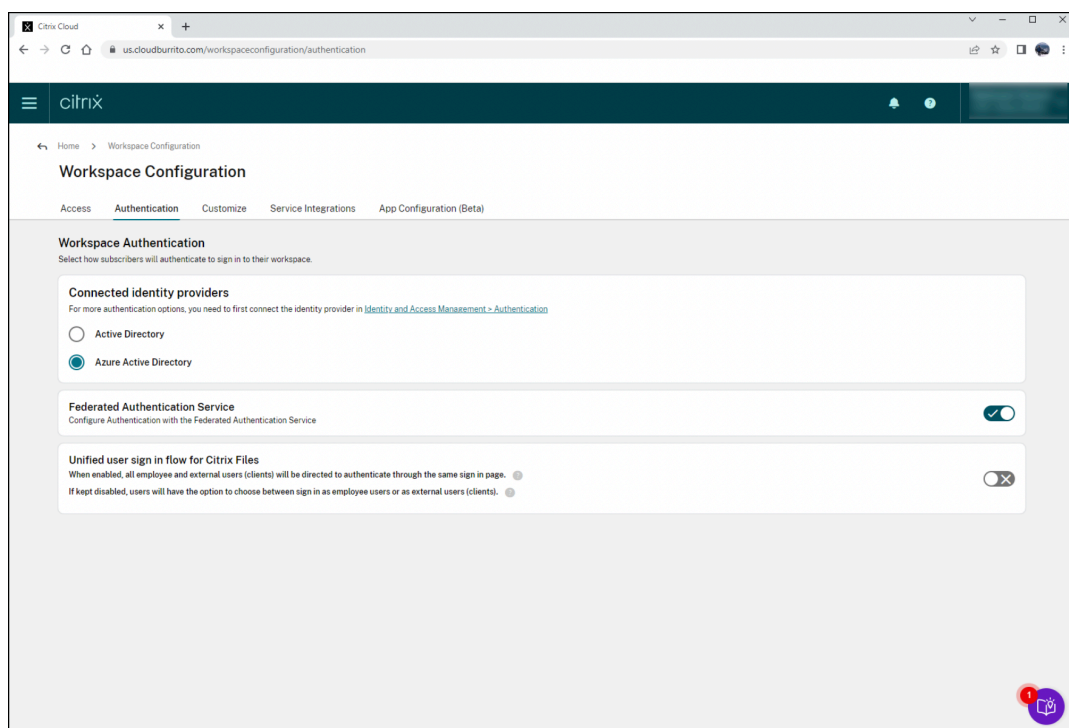
Activez FAS pour le client locataire

- Configurez votre fournisseur d'identité (IdP)

Passez au client locataire. Accédez à **Gestion des identités et des accès > Authentification**. Connectez-vous à votre IdP et assurez-vous qu'AD est synchronisé avec l'IdP.

- Activez FAS pour un locataire

Accédez à **Configuration de l'espace de travail > Authentification**. Sélectionnez l'authentification que vous avez configurée et activez FAS.



Problème connu

Il existe un problème connu lié à la suppression d'un domaine MSP avant de supprimer les domaines fédérés des locataires. Vous pouvez toujours activer FAS pour les locataires, mais FAS échoue car le domaine n'existe plus pour le MSP.

Authentification unique avec Azure Active Directory

June 5, 2024

Le service d'authentification fédérée (FAS) de Citrix fournit une authentification unique (SSO) aux Virtual Delivery Agents (VDA) joints à un domaine. FAS réalise l'authentification unique en fournissant au VDA un certificat utilisateur, que le VDA utilise pour authentifier l'utilisateur auprès d'Active Directory (AD). Une fois connecté à la session VDA, vous pouvez accéder aux ressources AD sans vous réauthentifier.

Il est courant d'implémenter Azure Active Directory (AAD) avec synchronisation entre votre AD et AAD, ce qui crée des identités hybrides pour les utilisateurs et les ordinateurs. Cet article décrit la configuration supplémentaire requise pour implémenter SSO sur AAD à partir de votre session VDA lors de l'utilisation de FAS, ce qui permet à l'utilisateur d'accéder à des applications protégées par AAD sans se réauthentifier.

Remarque :

- Aucune configuration spéciale n'est requise pour que FAS puisse utiliser SSO avec AAD.
- Vous n'avez pas besoin de certificats dans les sessions FAS.
- Vous pouvez utiliser n'importe quelle version de FAS.
- Vous pouvez utiliser n'importe quelle version de VDA qui prend en charge FAS.

Les techniques de SSO pour AAD sont résumées dans le tableau suivant :

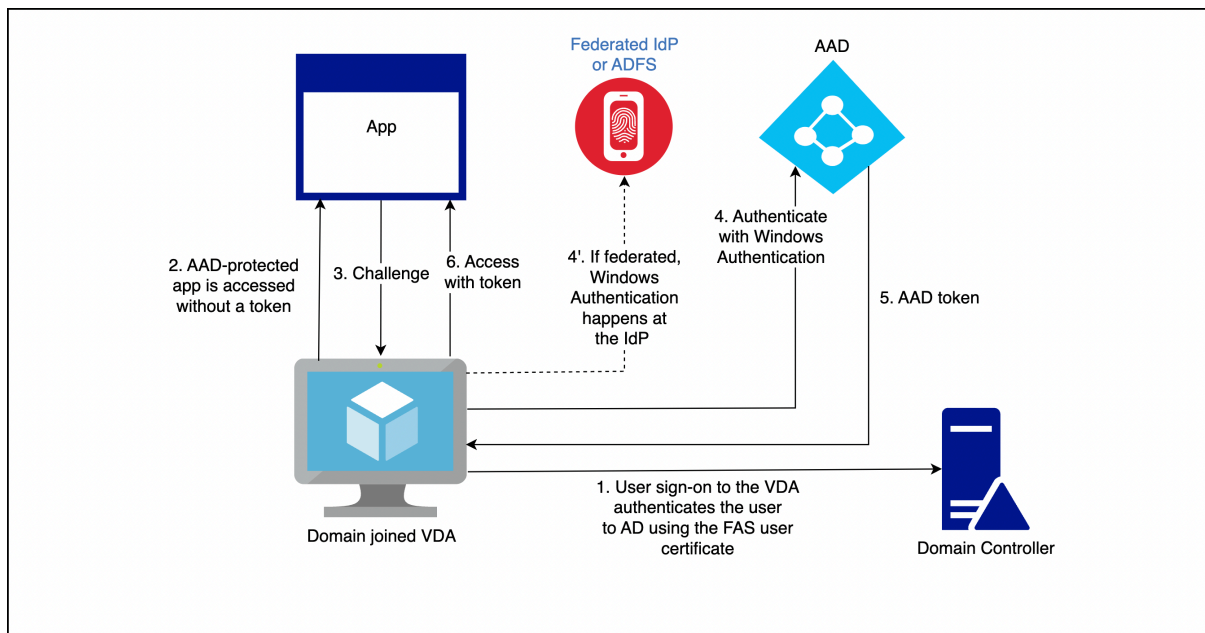
| Type d'authentification AAD | Le VDA est joint à un domaine | Le VDA est joint hybride |
|--|---|---|
| Géré | Utiliser SSO transparent AAD | Utiliser authentification basée sur certificat AAD |
| Fédérée vers Active Directory Federation Services (ADFS) | Activer l'authentification Windows sur ADFS | Assurez-vous que le point de terminaison <i>certificatemixedWS-Trust</i> est activé |
| Fédérée à un fournisseur d'identité tiers | Utiliser une solution tierce | Utiliser une solution tierce |

- Un domaine AAD géré est un domaine dans lequel l'authentification utilisateur s'effectue auprès d'AAD, parfois appelée authentification AAD native.
- Un domaine AAD fédéré est un domaine dans lequel AAD est configuré pour rediriger l'authentification ailleurs. Par exemple, à ADFS ou à un fournisseur d'identité tiers.
- Un VDA joint hybride est joint à AD et à AAD.

VDA joints à un domaine

Pour les VDA joints à un domaine, effectuez une authentification SSO vers AAD à l'aide de l'authentification Windows (traditionnellement appelée authentification Windows intégrée, ou Kerberos). L'

authentification auprès d'AAD se produit lorsque l'utilisateur accède à une application protégée par AAD depuis la session VDA. Le schéma suivant montre le processus d'authentification de haut niveau :



Les détails exacts varient selon que le domaine AAD est géré ou fédéré.

Pour plus d'informations sur la configuration du domaine AAD géré, consultez [Authentification unique transparente](#).

Pour un domaine AAD fédéré à ADFS, activez l'authentification Windows sur le serveur ADFS.

Pour un domaine AAD fédéré à un fournisseur d'identité tiers, une solution similaire existe. Contactez votre fournisseur d'identité pour obtenir de l'aide.

Remarque :

Vous pouvez également utiliser les solutions répertoriées pour les VDA joints à un domaine pour les VDA joints hybrides. Toutefois, aucun jeton d'actualisation principal (PRT) AAD n'est généré lors de l'utilisation de FAS.

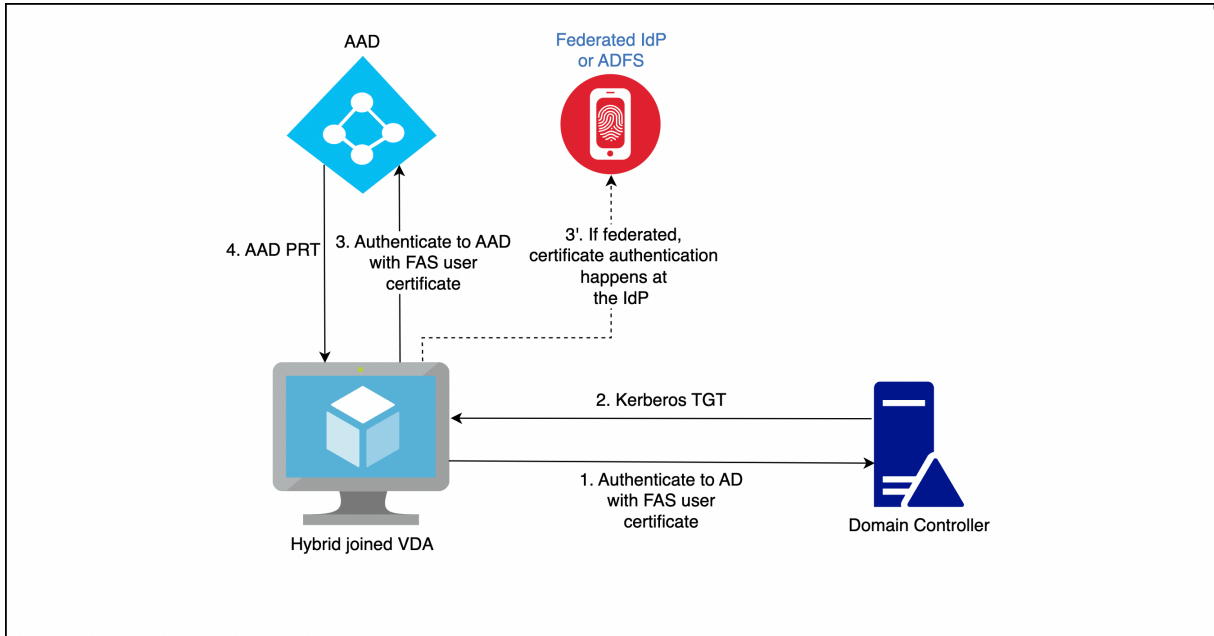
VDA joints hybrides

Les VDA joints hybrides sont joints à AD et à AAD en même temps. Lorsque l'utilisateur se connecte au VDA, les artefacts suivants sont créés :

- Un ticket TGT (Ticket Granting Ticket), pour s'authentifier auprès des ressources AD
- Un jeton d'actualisation principal (PRT), pour s'authentifier auprès des ressources AAD

Le PRT contient des informations à la fois sur l'utilisateur et sur l'ordinateur. Ces informations sont utilisées dans une stratégie d'accès conditionnel AAD si nécessaire.

Étant donné que FAS authentifie l'utilisateur en fournissant un certificat au VDA, un PRT ne peut être créé que si l'authentification basée sur des certificats pour AAD est implémentée. Le schéma suivant montre le processus d'authentification de haut niveau :



Les détails exacts varient selon que le domaine AAD est géré ou fédéré.

Pour un domaine AAD géré, configurez une CBA (Authentification basée sur les certificats) AAD. Pour plus d'informations, consultez la section [Présentation de l'authentification basée sur les certificats Azure AD](#). Le VDA utilise la CBA AAD pour authentifier l'utilisateur auprès d'AAD à l'aide du certificat FAS de l'utilisateur.

Remarque :

La documentation Microsoft décrit comment se connecter à l'aide d'un certificat de carte à puce, mais la technique sous-jacente s'applique lors de la connexion à l'aide d'un certificat utilisateur FAS.

Pour un domaine AAD fédéré vers ADFS, le VDA utilise le point de terminaison *certificatemixed* WS-Trust du serveur ADFS pour authentifier l'utilisateur auprès d'AAD à l'aide du certificat FAS de l'utilisateur. Ce point de terminaison est activé par défaut.

Pour un domaine AAD fédéré auprès d'un fournisseur d'identité tiers, une solution similaire peut exister. Le fournisseur d'identité doit implémenter un point de terminaison *certificatemixed* WS-Trust. Contactez votre fournisseur d'identité pour obtenir de l'aide.

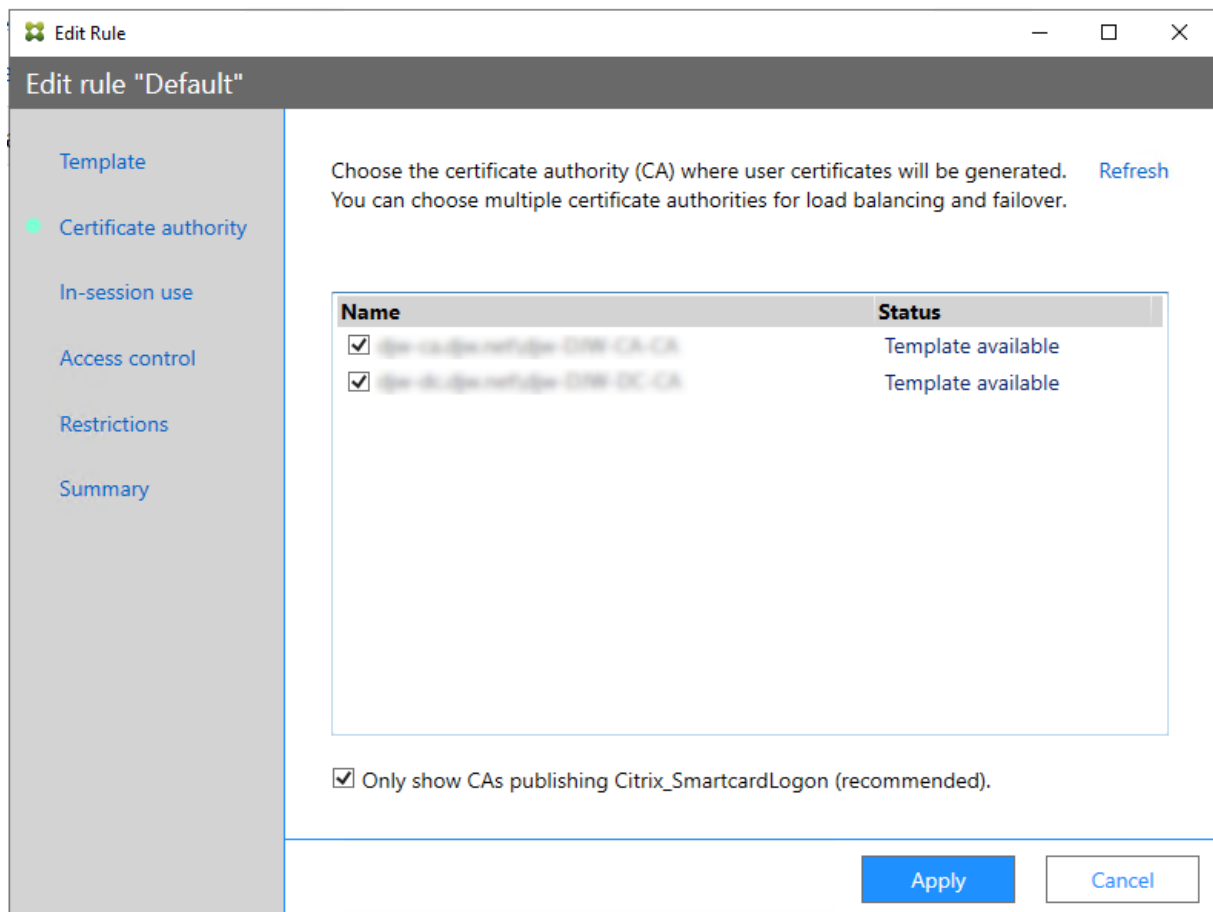
Configuration de l'autorité de certification

June 5, 2024

Cet article décrit la configuration avancée du Service d'authentification fédérée (FAS) pour l'intégration avec les serveurs d'autorité de certification (CA). La plupart de ces configurations ne sont pas prises en charge par la console d'administration FAS. Les instructions utilisent les API PowerShell fournies par FAS. Vous devez disposer de connaissances de base sur PowerShell avant d'exécuter les instructions de cet article.

Définir plusieurs serveurs d'autorité de certification à utiliser dans FAS

Vous pouvez utiliser la console d'administration FAS pour configurer FAS avec plusieurs autorités de certification lors de la création ou de la modification d'une règle :



Toutes les autorités de certification sélectionnées doivent publier le modèle de certificat Citrix_SmartcardLogon (ou le modèle que vous avez choisi dans votre règle).

Si l'une des autorités de certification que vous souhaitez utiliser ne publie pas le modèle souhaité, effectuez l'étape [Configurer une autorité de certification](#) pour l'autorité de certification.

Remarque :

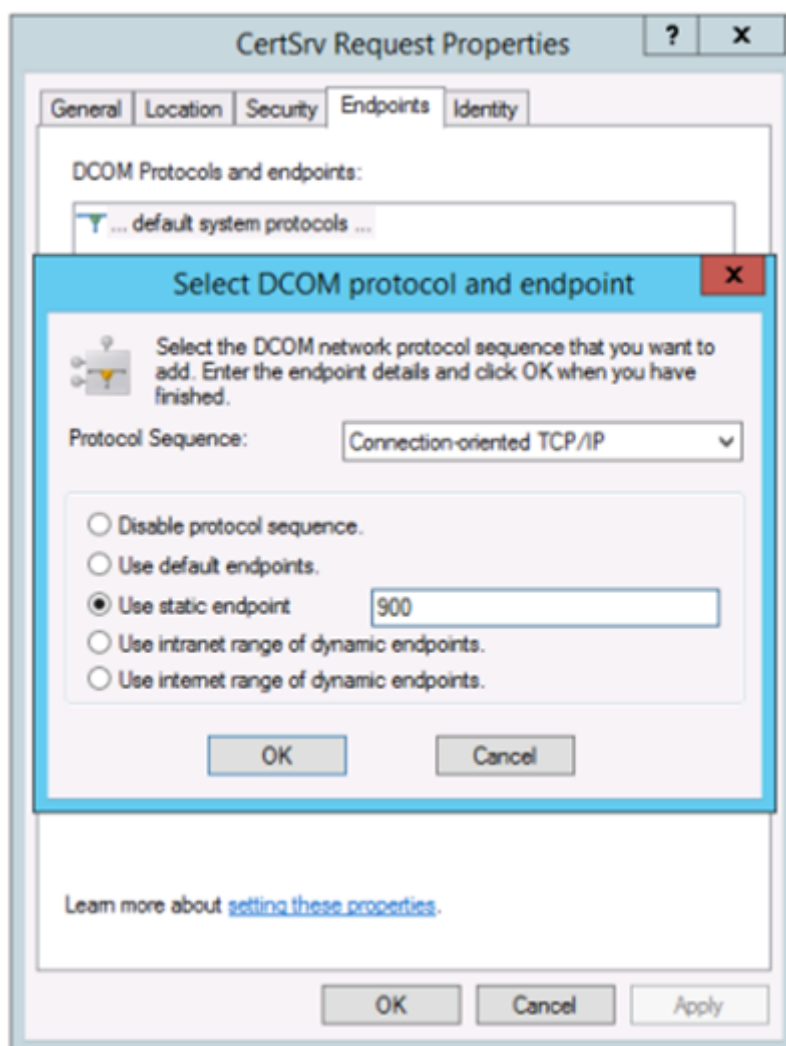
Vous n'avez pas besoin d'effectuer l'étape [Autoriser ce service](#) pour chaque autorité de certification, car le certificat d'autorisation configuré dans cette étape peut être utilisé dans n'importe laquelle de vos autorités de certification.

Changements de comportement attendus

Une fois que vous avez configuré le serveur FAS avec de multiples serveurs d'autorité de certification, la génération de certificat utilisateur est distribuée entre tous les serveurs d'autorité de certification configurés. De plus, si l'un des serveurs d'autorité de certification configurés échoue, le serveur FAS bascule vers un autre serveur d'autorité de certification disponible.

Configurer l'autorité de certification Microsoft pour l'accès TCP

Par défaut, l'autorité de certification Microsoft utilise DCOM pour l'accès. Cela peut compliquer la mise en place d'un pare-feu de sécurité, par conséquent Microsoft permet le basculement vers un port TCP statique. Sur l'autorité de certification Microsoft, utilisez **Démarrer>Exécuter>DCOMCNFG.exe** pour ouvrir le panneau de configuration DCOM, développez *Ordinateurs>Poste de travail>Configuration DCOM* pour afficher le nœud **Demande de CertSrv**, puis modifiez les propriétés de l'application DCOM de demande de CertSrv :



Modifiez les points de terminaison pour sélectionner un point de terminaison statique et spécifiez un numéro de port TCP (900 dans l'illustration ci-dessus).

Redémarrez l'autorité de certification Microsoft et envoyez une demande de certificat. Si vous exécutez `netstat -a -n -b`, vous verrez que `certsrv` écoute désormais le port 900 :

```
TCP 0.0.0.0:636 dc:0 LISTENING
[lsass.exe]
TCP 0.0.0.0:900 dc:0 LISTENING
[certsrv.exe]
TCP 0.0.0.0:3268 dc:0 LISTENING
[lsass.exe]
TCP 0.0.0.0:3269 dc:0 LISTENING
```

Il n'est pas nécessaire de configurer le serveur FAS (ou toute autre machine utilisant l'autorité de certification), car DCOM a une étape de négociation utilisant le port RPC. Lorsqu'un client doit utiliser DCOM, il se connecte au service DCOM RPC sur le serveur de certificats et demande l'accès à un serveur DCOM particulier. Cela déclenche l'ouverture du port 900 et le serveur DCOM indique au serveur FAS

comment se connecter.

Pré-générer les certificats utilisateur

La durée d'ouverture de session pour les utilisateurs peut nettement s'améliorer lorsque les certificats utilisateur sont pré-générés dans le serveur FAS. Les sections suivantes décrivent comment y procéder, pour un ou plusieurs serveurs FAS.

Obtenir une liste d'utilisateurs Active Directory

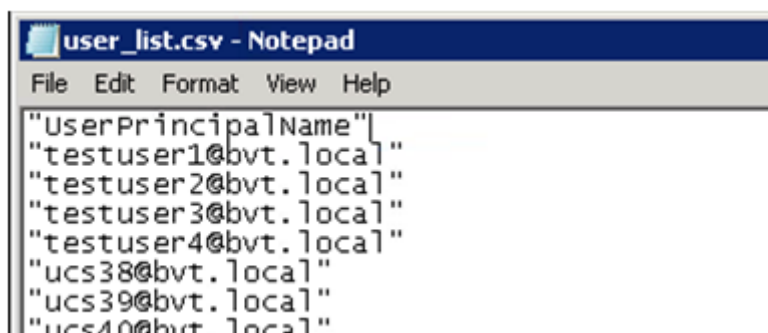
Vous pouvez améliorer la génération de certificat en interrogeant AD et en stockant la liste des utilisateurs dans un fichier (par exemple, un fichier .csv), comme illustré dans l'exemple suivant.

```
1 Import-Module ActiveDirectory
2
3 $searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for
   Users, leave it blank to search all
4 $filename = "user_list.csv" # Filename to save
5
6 if ($searchbase -ne ""){
7
8     Get-ADUser -Filter {
9     (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
10    -SearchBase $searchbase -Properties UserPrincipalName | Select
   UserPrincipalName | Export-Csv -NoTypeInfo -Encoding utf8 -
   delimiter "," $filename
11 }
12 else {
13
14     Get-ADUser -Filter {
15     (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
16    -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv
   -NoTypeInfo -Encoding utf8 -delimiter "," $filename
17 }
18
19 <!--NeedCopy-->
```

Get-ADUser est une applet de commande qui envoie une requête de liste d'utilisateurs. L'exemple ci-dessus contient un argument de filtre pour inclure uniquement les utilisateurs disposant d'un UserPrincipalName et avec un état de compte « activé ».

L'argument SearchBase spécifie la partie d'Active Directory dans laquelle rechercher des utilisateurs. Vous pouvez ignorer cette option si vous voulez inclure tous les utilisateurs présents dans Active Directory. Remarque : cette requête peut renvoyer un grand nombre d'utilisateurs.

Le fichier CSV ressemble à l'exemple ci-dessous :



```
user_list.csv - Notepad
File Edit Format View Help
"UserPrincipalName"
"testuser1@bvt.local"
"testuser2@bvt.local"
"testuser3@bvt.local"
"testuser4@bvt.local"
"ucs38@bvt.local"
"ucs39@bvt.local"
"ucs40@bvt.local"
```

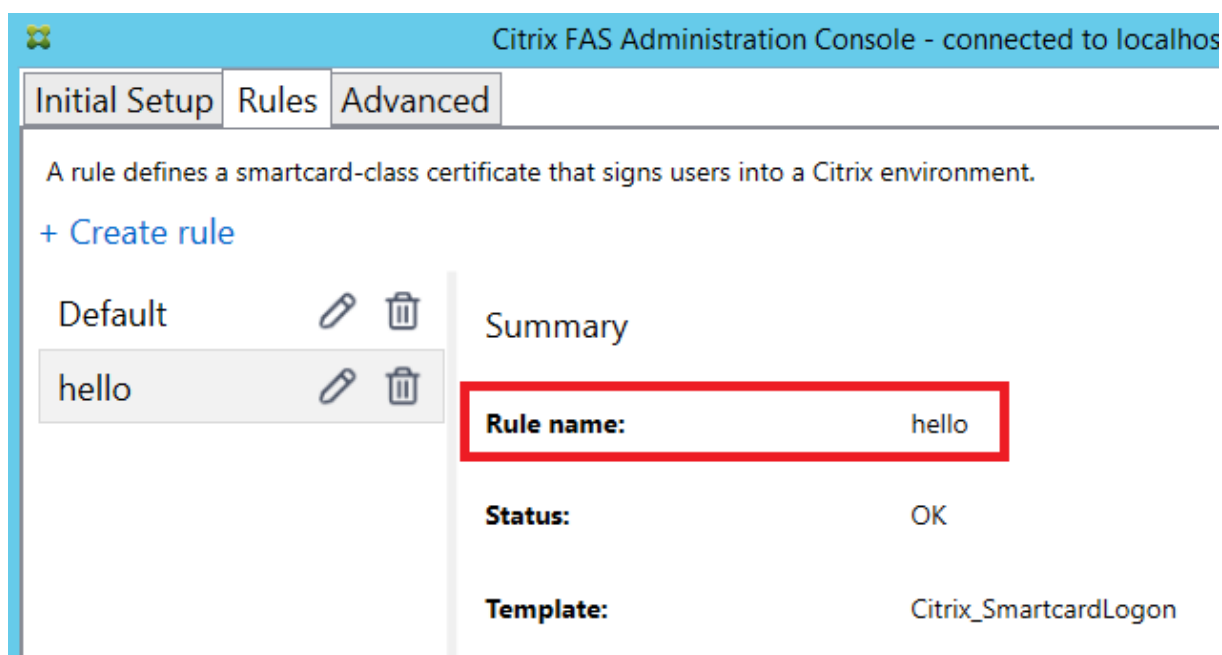
Serveur FAS

Le script PowerShell utilise la liste d'utilisateurs générée et crée une liste de certificats utilisateur.

```
1 Add-PSSnapin Citrix.A*
2 $csv = "user_list.csv"
3 $rule = "default" # rule/role in your admin console
4 $users = Import-Csv -encoding utf8 $csv
5 foreach ( $user in $users )
6 {
7
8     $server = Get-FasServerForUser -UserPrincipalNames $user.
        UserPrincipalName
9     if( $server.Server -ne $NULL) {
10
11         New-FasUserCertificate -Address $server.Server -
            UserPrincipalName $user.UserPrincipalName -
            CertificateDefinition $rule"_Definition" -Rule $rule
12     }
13
14     if( $server.Failover -ne $NULL) {
15
16         New-FasUserCertificate -Address $server.Failover -
            UserPrincipalName $user.UserPrincipalName -
            CertificateDefinition $rule"_Definition" -Rule $rule
17     }
18
19 }
20
21 <!--NeedCopy-->
```

Si vous disposez de plusieurs serveurs FAS, le certificat d'un utilisateur particulier est généré deux fois : une fois sur le serveur principal et une autre sur le serveur de basculement.

Le script ci-dessus inclut une règle « default ». Si votre règle porte un autre nom (par exemple, « hello »), il vous suffit de modifier la variable \$rule dans le script.

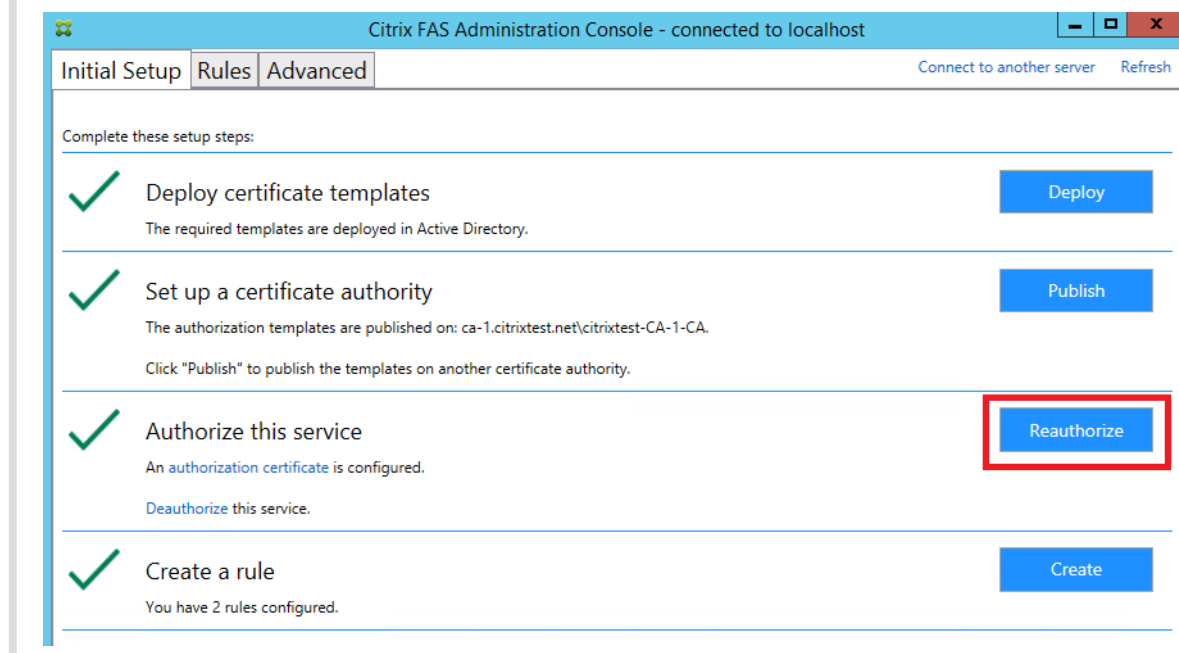


Renouveler les certificats d'autorité d'inscription

Si plusieurs serveurs FAS sont utilisés, vous pouvez renouveler un certificat d'autorisation FAS sans affecter les utilisateurs connectés.

Remarque :

Vous pouvez également utiliser l'interface graphique pour réautoriser FAS :



Effectuez la procédure suivante dans l'ordre indiqué :

1. Créer un nouveau certificat d'autorisation : `New-FasAuthorizationCertificate`
2. Noter le GUID du nouveau certificat d'autorisation, renvoyé par : `Get-FasAuthorizationCertificate`
3. Placer le serveur FAS en mode de maintenance : `Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. Changer le nouveau certificat d'autorisation : `Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
5. Retirer le serveur FAS du mode de maintenance : `Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. Supprimer l'ancien certificat d'autorisation : `Remove-FasAuthorizationCertificate`

Informations connexes

- L'article [Installer et configurer](#) est le document de référence principal pour obtenir des informations sur l'installation et la configuration de FAS.
- Les déploiements FAS (Service d'authentification fédérée) courants sont décrits dans l'article [Vue d'ensemble des architectures](#).
- D'autres informations pratiques sont disponibles dans l'article [Configuration avancée](#).

Protection de clé privée

June 5, 2024

Introduction

Les certificats sont stockés dans une base de données intégrée sur le serveur FAS. Les clés privées associées sont stockées par le biais du compte de service réseau du serveur FAS et marquées comme non-exportables par défaut.

Il existe deux types de clés privées:

- La clé privée associée au certificat de l'autorité d'inscription, à partir du modèle de certificat `Citrix_RegistrationAuthority`.
- Les clés privées associées aux certificats utilisateur, à partir du modèle de certificat `Citrix_SmartcardLogon`.

Il existe en fait deux certificats d'autorité d'inscription : Citrix_RegistrationAuthority_ManualAuthorization (valide pendant 24 heures par défaut) et Citrix_RegistrationAuthority (valide pendant deux ans par défaut).

Lors de l'étape 3 de la **configuration initiale** dans la console de gestion FAS, lorsque vous cliquez sur **Autoriser**, le serveur FAS génère une paire de clés et envoie une demande de signature de certificat à l'autorité de certification pour le certificat Citrix_RegistrationAuthority_ManualAuthorization. Il s'agit d'un certificat temporaire, valide pendant 24 heures par défaut. L'autorité de certification n'émet pas automatiquement ce certificat ; son émission doit être manuellement autorisée sur l'autorité de certification par un administrateur. Une fois que le certificat a été généré sur le serveur FAS, FAS utilise le certificat Citrix_RegistrationAuthority_ManualAuthorization pour obtenir automatiquement le certificat Citrix_RegistrationAuthority (valide pendant deux ans par défaut). Le serveur FAS supprime le certificat et la clé pour Citrix_RegistrationAuthority_ManualAuthorization dès qu'il obtient le certificat Citrix_RegistrationAuthority.

La clé privée associée au certificat d'autorité d'inscription est particulièrement sensible car la stratégie de certificat d'autorité d'inscription permet à toute personne qui dispose de la clé privée d'émettre des demandes de certificat pour le groupe d'utilisateurs configuré dans le modèle. En conséquence, toute personne qui contrôle cette clé peut se connecter à l'environnement en tant qu'utilisateur du groupe.

Vous pouvez configurer le serveur FAS pour protéger les clés privées selon les besoins de sécurité de votre organisation, à l'aide de l'une des configurations suivantes :

- Microsoft Enhanced RSA and AES Cryptographic Provider ou Microsoft Software Key Storage Provider pour le certificat d'autorité d'inscription et les clés privées des certificats utilisateur.
- Microsoft Platform Key Storage Provider avec une puce Trusted Platform Module (TPM) pour la clé privée du certificat d'autorité d'inscription et Microsoft Enhanced RSA and AES Cryptographic Provider ou Microsoft Software Key Storage Provider pour les clés privées des certificats utilisateur.
- Un fournisseur de service cryptographique ou un fournisseur de stockage de clés de module de sécurité matérielle (HSM) avec le périphérique HSM pour le certificat d'autorité d'inscription et les clés privées des certificats utilisateur.

Paramètres de configuration des clés privées

Configurez FAS pour utiliser l'une des trois options. Utilisez un éditeur de texte pour modifier le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config. L'emplacement par défaut du fichier est le dossier Program Files\Citrix\Federated Authentication Service sur le serveur FAS.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name. -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV_RSA_AES is 24 -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Suppress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value="" / -->
  </appSettings>
</startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

FAS lit le fichier de configuration uniquement lorsque le service démarre. Si des valeurs sont modifiées, FAS doit être redémarré avant qu'il reflète les nouveaux paramètres.

Définissez les valeurs appropriées dans le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config comme suit :

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (basculement entre API CAPI et CNG)

| Valeur | Commentaire |
|---------------------------|-----------------------|
| true | Utiliser les API CAPI |
| false (valeur par défaut) | Utiliser les API CNG |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (nom du fournisseur à utiliser)

| Valeur | Commentaire |
|--|-----------------------------|
| Microsoft Enhanced RSA and Cryptographic Provider | Fournisseur CAPI par défaut |
| Fournisseur de stockage des clés de logiciel Microsoft | Fournisseur CNG par défaut |

| Valeur | Commentaire |
|--|---|
| Fournisseur de stockage des clés de plateforme Microsoft | Fournisseur TPM par défaut Veuillez noter que TPM n'est pas recommandé pour les clés utilisateur. Utilisez le module de plateforme sécurisée (TPM) pour la clé d'autorité d'inscription uniquement. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur d'hyperviseur et de puce TPM si la virtualisation est prise en charge. |
| HSM_Vendor CSP/Fournisseur de stockage de clés | Fourni par le fournisseur HSM. La valeur diffère d'un fournisseur à l'autre. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur HSM si la virtualisation est prise en charge. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (requis uniquement avec API CAPI)

| Valeur | Commentaire |
|--------|---|
| 24 | Valeur par défaut. Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit être toujours 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM en décide autrement. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (lorsque FAS doit effectuer une opération de clé privée, il utilise la valeur spécifiée ici) Contrôle l'indicateur « exportable » des clés privées. Permet l'utilisation de stockage de clé TPM, s'il est pris en charge par le matériel.

| Valeur | Commentaire |
|--------------------------|---|
| NoProtection | La clé privée peut être exportée. |
| GenerateNonExportableKey | Valeur par défaut. La clé privée ne peut pas être exportée. |

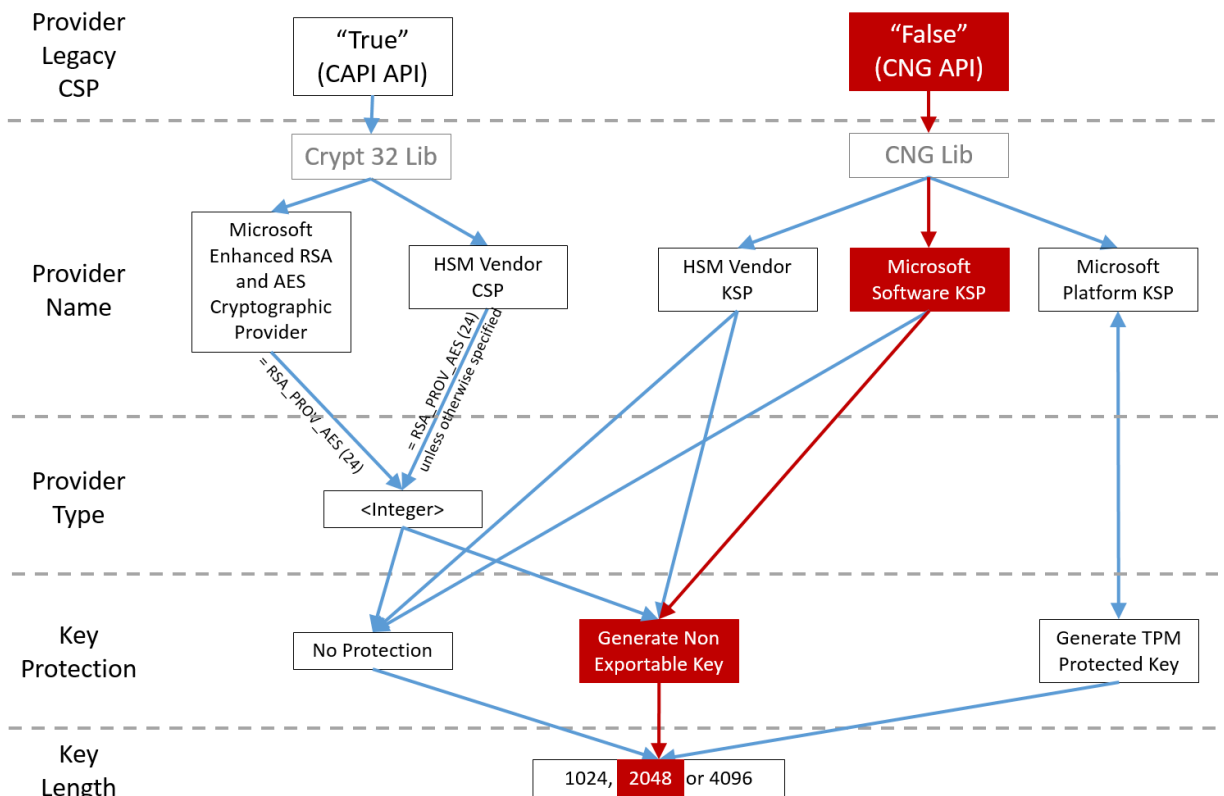
Service d'authentification fédérée

| Valeur | Commentaire |
|-------------------------|--|
| GenerateTPMProtectedKey | La clé privée sera gérée à l'aide de TPM. La clé privée est stockée via le nom de fournisseur que vous avez spécifié dans NomFournisseur (par exemple, Microsoft Platform Key Storage Provider). |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (spécifiez la taille de la clé privée en bits)

| Valeur | Commentaire |
|--------|--|
| 2048 | Default. 1024 ou 4096 peut également être utilisé. |

Les paramètres du fichier de configuration sont représentés sous forme de graphiques comme suit (les valeurs par défaut d'installation apparaissent en rouge) :



Exemples de scénario de configuration

Exemple 1

Cet exemple concerne la clé privée du certificat de l'autorité d'inscription et les clés privées des certificats utilisateur à l'aide de Microsoft Software Key Storage Provider

Il s'agit de la configuration post-installation par défaut. Aucune configuration de clé privée supplémentaire n'est requise.

Exemple 2

Cet exemple illustre la clé privée de certificat de l'autorité d'inscription stockée dans la puce TPM matérielle de la carte mère du serveur FAS via Microsoft Platform Key Storage Provider et les clés privées des certificats utilisateur stockées à l'aide de Microsoft Software Key Storage Provider.

Ce scénario part du principe que la puce TPM sur la carte mère de votre serveur FAS a été activée dans le BIOS selon la documentation du fabricant de la puce TPM et initialisée dans Windows ; consultez la section [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)).

Utilisation de la console d'administration FAS La console d'administration de FAS ne peut pas effectuer de requête de signature de certificat en mode déconnecté ; son utilisation n'est donc pas recommandée si votre organisation ne permet pas les requêtes de signature de certificat en mode connecté pour les certificats d'autorité d'inscription.

Lorsque vous effectuez la configuration initiale de FAS, après le déploiement des modèles de certificat et la configuration de l'autorité de certification, mais avant d'autoriser le service (étape 3 dans la séquence de configuration) :

Étape 1 : modifiez le fichier de configuration en modifiant la ligne suivante comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>
```

Le fichier doit maintenant s'afficher comme suit :

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name. -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV_RSA_AES is 24 -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Suppress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value="" / -->
  </appSettings>
</startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Certaines puces TPM limitent la longueur de clé. La valeur par défaut est une longueur de 2048 bits. Assurez-vous que vous spécifiez une longueur de clé prise en charge par votre matériel.

Étape 2 : redémarrez le Service d'authentification fédérée Citrix pour lire les valeurs à partir du fichier de configuration.

Étape 3 : autorisez le service.

Étape 4 : émettez manuellement la requête de certificat en attente depuis le serveur de l'autorité de certification. Une fois que le certificat d'autorité d'inscription a été obtenu, l'étape 3 dans la séquence d'installation de la console d'administration doit être indiquée en vert. À ce stade, la clé privée du certificat d'autorité d'inscription est générée dans la puce TPM. Le certificat sera valide pendant 2 ans par défaut.

Pour vérifier que la clé privée du certificat de l'autorité d'inscription est correctement stockée dans le module de plateforme sécurisée, utilisez les commandes PowerShell suivantes. Le champ `PrivateKeyProvider` sera défini sur *Microsoft Platform Crypto Provider* si la clé privée du certificat de l'autorité d'inscription est stockée dans le module de plateforme sécurisée :

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
2 Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
3 <!--NeedCopy-->
```

Étape 5 : modifiez le fichier de configuration comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

Remarque :

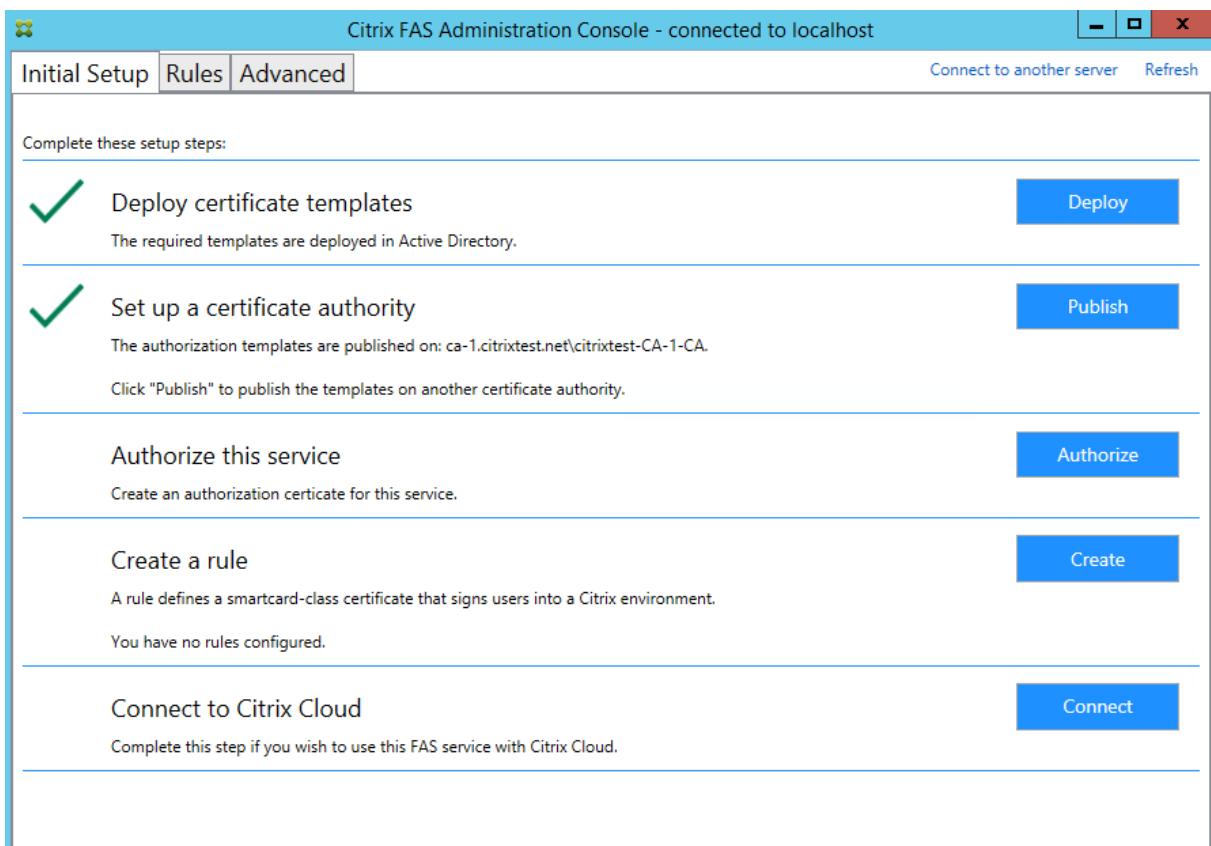
Bien que FAS puisse générer des certificats utilisateur avec des clés protégées TPM, le matériel TPM peut être trop lent pour les déploiements de grande envergure.

Étape 6 : redémarrez FAS. Cela oblige le service à relire le fichier de configuration et à refléter les valeurs modifiées. Les opérations de clé privée automatiques suivantes affecteront les clés de certificat utilisateur ; ces opérations ne stockeront pas les clés privées dans la puce TPM, mais utiliseront Microsoft Software Key Storage Provider.

Étape 7 : sélectionnez l'onglet **Rules** dans la console de gestion FAS et modifiez les paramètres décrits dans [Installer et configurer](#).

Utilisation de PowerShell Le certificat de l'autorité d'inscription peut être demandé hors connexion à l'aide de PowerShell. Cette option convient aux entreprises qui ne souhaitent pas que l'autorité de certification émette un certificat d'autorité d'inscription via une demande de signature de certificat en ligne. Vous ne pouvez pas effectuer de demande de signature de certificat d'autorité d'inscription hors connexion à l'aide de la console d'administration de FAS.

Étape 1 : lors de la configuration initiale de FAS à l'aide de la console de gestion, effectuez uniquement les deux premières étapes : « Déployer les modèles de certificat » et « Configurer une autorité de certification ».



Étape 2 : sur le serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC des modèles de certificat. Cliquez avec le bouton droit sur le modèle **Citrix_RegistrationAuthority_ManualAuthoriza** et sélectionnez **Dupliquer le modèle**.

Sélectionnez l'onglet **Général**. Modifiez le nom et la période de validité. Dans cet exemple, le nom est *Offline_RA* et la période de validité est de 2 ans :

Properties of New Template

| | | | | |
|----------------------|------------|-----------------------|--------------|-----------------|
| Subject Name | Server | Issuance Requirements | | |
| Superseded Templates | Extensions | Security | | |
| Compatibility | General | Request Handling | Cryptography | Key Attestation |

Template display name:
Offline_RA

Template name:
Offline_RA

Validity period: 2 years
Renewal period: 0 days

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

Étape 3 : sur votre serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC d'autorité de certification. Cliquez avec le bouton droit sur **Modèles de certificats**. Sélectionnez **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**. Choisissez le modèle que vous venez de créer.

Étape 4 : chargez les applets de commande PowerShell suivantes sur le serveur FAS :

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Étape 5 : générez la paire de clés RSA dans la puce TPM du serveur FAS et créez la demande de signature de certificat en entrant l'applet de commande PowerShell suivante sur le serveur FAS. **Remarque :** certaines puces TPM limitent la longueur de clé. La valeur par défaut est une longueur de 2048 bits. Veuillez à spécifier une longueur de clé prise en charge par votre matériel.

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of FAS Server>
```

Par exemple :

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

Les éléments suivants sont affichés :

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
MIICdCCAUACAQIwIzEhMB8GCgmSjomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
hkig9wDBAQEFAAOCQAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbhkhZU3wTnFR0XW
1hCMwi7X4YpTE7CbJtgIFY/9SEBa9StGeTUpeJi66gKozGdxyc2BwX6JNzrLi9hAf1bInFPgrz+
vbG3YjkuKtK35JpGqYwJUEdzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaN9MH0EFbepoSVOCAfunXW
snwIbX09Ic/fGyN/3f94P4fbNrjEIOHc+40y/WsPgPRgcq9XBWRjzpj0gQWRoJS9g220Y5PwD77
7f7vZvoQkRy5N8XXATJ+xxVEPLp9JujJaE1WXRJG+XP3SnG/oCCPit7iUIIc9Fj6a3qTUQIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAIJU9jR9XWHlvztjxPeJzAVU0srLp0sCfNdvYn9u+I7J8Gsr
4tuljuQ+An4Y2Rw7b6pZxEICU8rgd5Gy+wtPnUzoAf6eLg1Uht2RUfb6d7Ns6+Mc+F5bFegLHs8c
Y1ITN0tmcHFKt4Loz5D5E+tQw39MProej3p7GwF7Hr6Y+QsBFD38rbl19Z5cfHYyqMbsgyMgdR8F
3SmagQjN3C8lyqT8z1iF4132xlmQrP/4XQvr1F+TD15PMSFxi6PEKwopWTYZRGzSC1ufxevc0TK
+tTh9tQYJM6xw3+6TicFuWUjrd8RkJTdC5SMu7LJu1ajTNZ5Z+1eM61TAT03XG/AB7o=
-----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval

PS C:\Users\Administrator.AUTH> _
```




Remarques :

- L’ID GUID (dans cet exemple, « 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 ») est requis dans une étape suivante.
- Considérez cette applet de commande PowerShell comme un « remplacement » à usage unique, utilisé pour générer la clé privée pour le certificat d’autorité d’inscription.
- Lors de l’exécution de cette applet de commande, les valeurs qui sont lues à partir du fichier de configuration lorsque FAS démarre sont vérifiées pour déterminer la longueur de clé à utiliser (la valeur par défaut est de 2048).
- Étant donné que -UseTPM est défini sur \$true dans cette opération manuelle de clé privée de certificat d’autorité d’inscription initiée par PowerShell, le système ignore les valeurs du fichier qui ne correspondent pas aux paramètres requis pour utiliser une puce TPM.
- L’exécution de cette applet de commande ne modifie pas les paramètres du fichier de con-

figuration.

- Durant les opérations automatiques de clé privée de certificat utilisateur initiées par FAS, les valeurs qui ont été lues à partir du fichier lorsque FAS a démarré sont utilisées.
- Il est également possible de définir la valeur KeyProtection dans le fichier de configuration sur GenerateTPMProtectedKey lorsque le serveur FAS émet des certificats utilisateur pour générer des clés privées de certificat utilisateur protégées par la puce TPM.

Pour vérifier que la puce TPM a été utilisée pour générer la paire de clés, consultez le journal d'application dans l'observateur d'événements de Windows sur le serveur FAS, à l'heure où la paire de clés a été générée.

| | | | | | |
|---|-------------|---------------------|--|----|------|
|  | Information | 22/07/2019 12:59:42 | Citrix.Fas.PkiCore | 14 | None |
|  | Information | 22/07/2019 12:59:41 | Citrix.Fas.PkiCore | 16 | None |
|  | Information | 22/07/2019 12:59:41 | Citrix.Authentication.FederatedAuthenticationService | 15 | None |




Event 15, Citrix.Authentication.FederatedAuthenticationService

General Details

```
[S15] Administrator [CITRIXTEST\Administrator] creating certificate request [TPM: True] [correlation: e61a73d7-bb61-44af-8d21-1159d864d82e]
```

Remarque : “[TPM: True]”

Suivi de :

| Application | Number of events: 3 | | | | |
|---|---------------------|---------------------|--|-----------|------|
| Level | Date and Time | Source | Event ID | Task C... | |
|  | Information | 22/07/2019 12:59:42 | Citrix.Fas.PkiCore | 14 | None |
|  | Information | 22/07/2019 12:59:41 | Citrix.Fas.PkiCore | 16 | None |
|  | Information | 22/07/2019 12:59:41 | Citrix.Authentication.FederatedAuthenticationService | 15 | None |

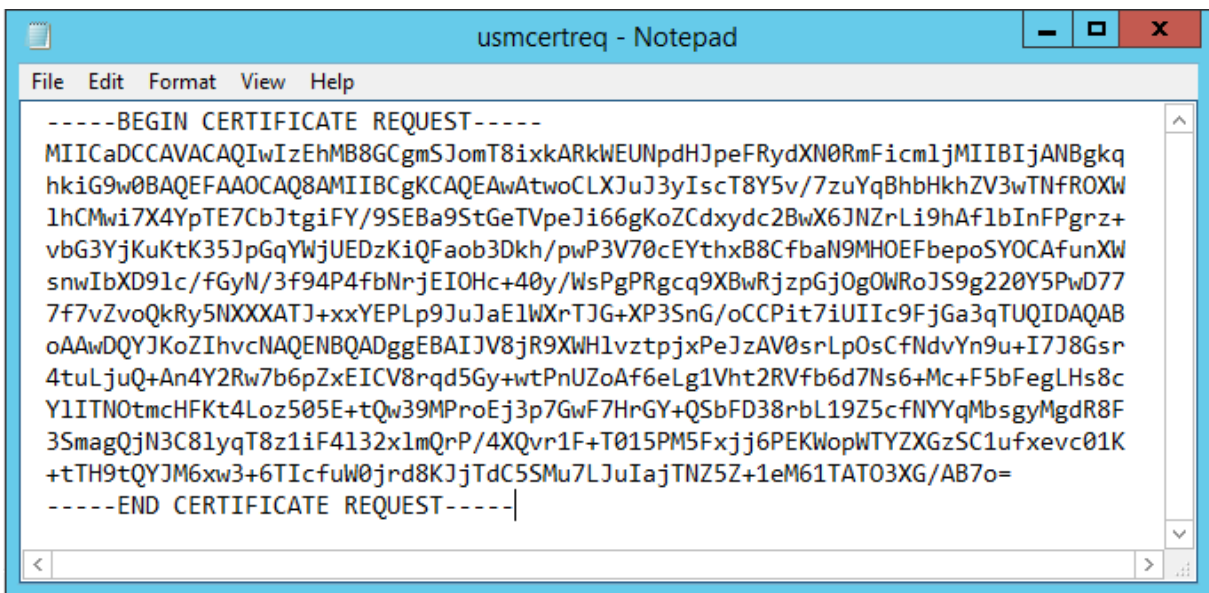
Event 16, Citrix.Fas.PkiCore

General Details

```
[S16] PrivateKey::Create [Identifier afae7c8d-53ff-4cf6-bd96-75fa3e606d3e_TWIN][MachineWide: False][Provider: [CNG] Microsoft Platform Crypto Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

Remarque : “Provider: [CNG] Microsoft Platform Crypto Provider”

Étape 6 : copiez la section de requête de certificat dans un éditeur de texte et enregistrez-la sur disque en tant que fichier texte.



```

-----BEGIN CERTIFICATE REQUEST-----
MIICaDCCAVACAQIwIzEhMB8GCGmSJomT8ixkARKWEUNpdHJpeFRydXN0RmFicm1jMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxyc2BwX6JNZrLi9hAflbInFPgrz+
vbG3YjKuKtK35JpGqYwJUEDzKiQFaob3Dkh/pwP3V70cEYthxB8CFbaN9MHOEFbepoSYOCAfunXW
snwIbXD91c/fGyN/3f94P4fbMrjEIOHc+40y/WsPgPRgcq9XBwRjzpGj0gOWRoJS9g220Y5PwD77
7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WxrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWH1vztpjxPeJzAV0srLp0sCfNdvYn9u+I7J8Gsr
4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZOaf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
YlITN0tmcHFkT4Loz505E+tQw39MPProEj3p7GwF7HrGY+QSbFD38rbL19Z5cFNYYqMbsgyMgdR8F
3SmagQjN3C81yqT8z1iF4132xlmQrP/4XQvr1F+T015PM5Fxfj6PEKWopWTYZXGzSC1ufxevc01K
+tTH9tQYJM6xw3+6TIcfuW0jrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TAT03XG/AB7o=
-----END CERTIFICATE REQUEST-----

```

Étape 7 : envoyez la demande de signature de certificat à l'autorité de certification en tapant les commandes suivantes dans PowerShell sur le serveur FAS :

```
certreq -submit -attrib "certificatetemplate:\<certificate template
from step 2>"\<certificate request file from step 6>
```

Par exemple :

```
certreq -submit -attrib "certificatetemplate:Offline_RA"C:\Users\
Administrator.AUTH\Desktop\usmcertreq.txt
```

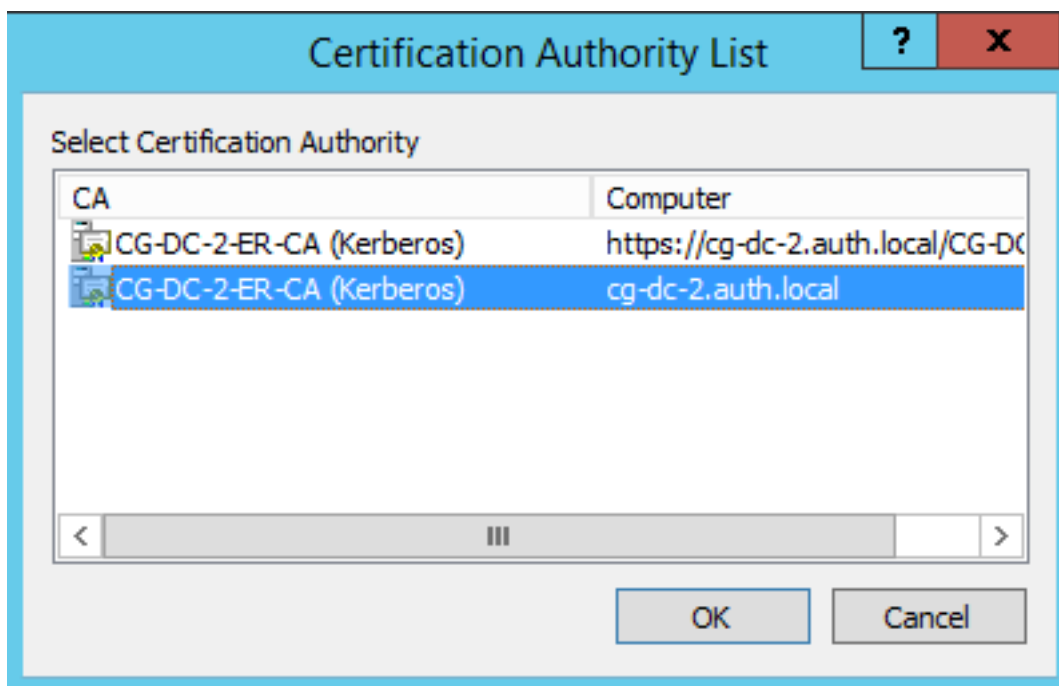
Les éléments suivants sont affichés :

```

PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0BDC-4D21-A4FD-2E29502177C2}
Idap:

```

À ce stade, une fenêtre contenant une liste d'autorités de certification peut s'afficher. Dans cet exemple, les inscriptions http (haut) et DCOM (bas) sont activées toutes les deux pour l'autorité de certification. Sélectionnez l'option DCOM, si elle est disponible :

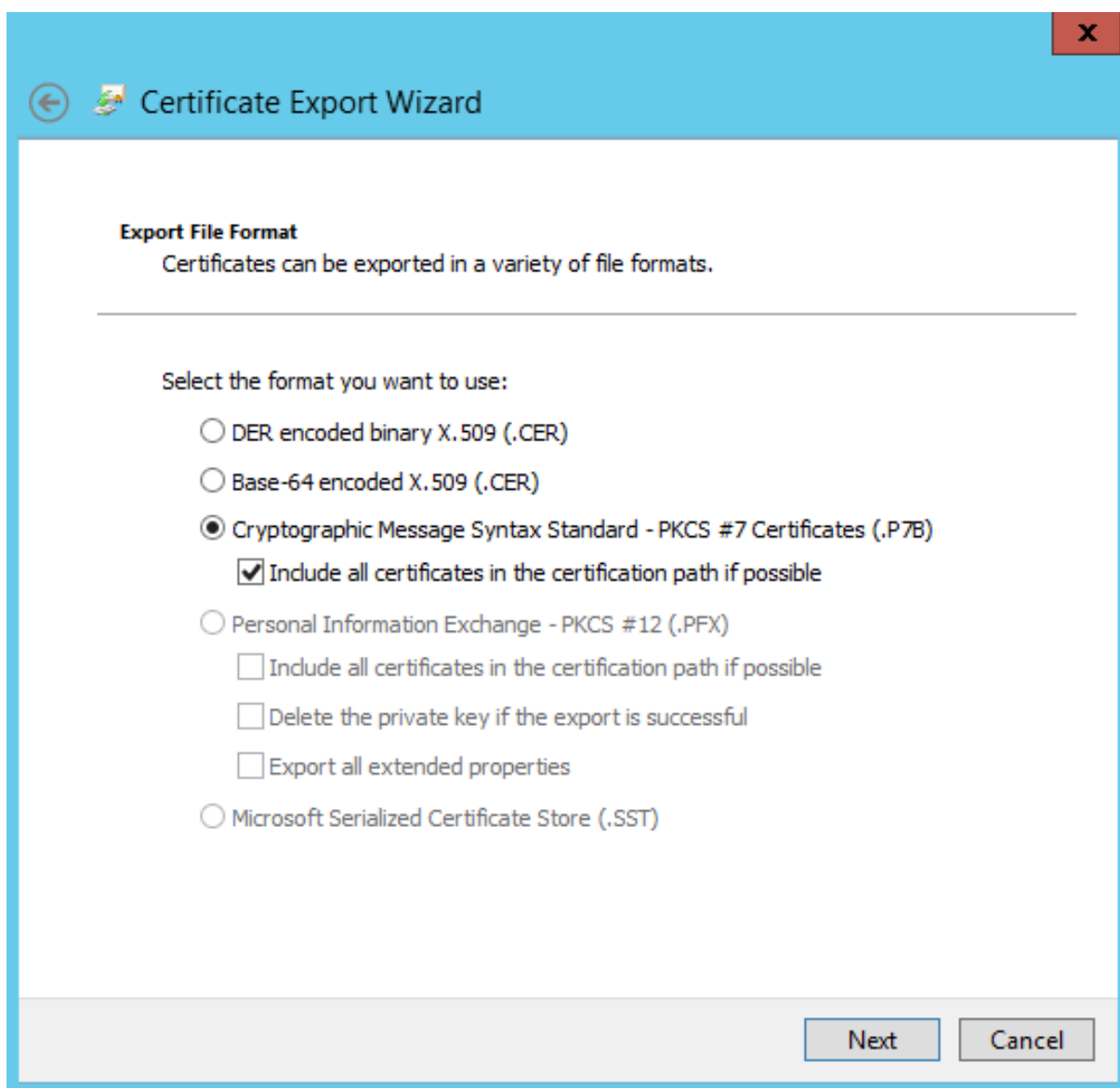


Après que l'autorité de certification a été spécifiée, PowerShell affiche la RequestID :

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_BA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0B0C-4D21-A4FD-2E29502177C2}
ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH> _
```

Étape 8 : sur le serveur de l'autorité de certification, dans le composant logiciel enfichable MMC d'autorité de certification, cliquez sur **Demandes en attente**. Notez l'ID de la demande, RequestID. Puis cliquez avec le bouton droit sur la demande et choisissez **Délivrer**.

Étape 9 : sélectionnez le nœud **Certificats délivrés**. Recherchez le certificat qui vient d'être émis (l'ID de demande doit correspondre). Cliquez deux fois pour ouvrir le certificat. Sélectionnez la page de l'onglet **Détails**. Cliquez sur **Copier dans un fichier**. L'Assistant d'exportation de certificat s'ouvre. Cliquez sur **Suivant**. Choisissez les options suivantes pour le format de fichier :



Le format doit être **Standard de syntaxe de message cryptographique –Certificate PKCS #7 (.P7B)** et **Inclure tous les certificats dans le chemin d'accès de certification, si possible** doit être sélectionné.

Étape 10 : copiez le fichier de certificat exporté sur le serveur FAS.

Étape 11 : importez le certificat d'autorité d'inscription dans le registre du serveur FAS en entrant l'applet de commande PowerShell suivante sur le serveur FAS :

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

Par exemple :

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

Les éléments suivants sont affichés :

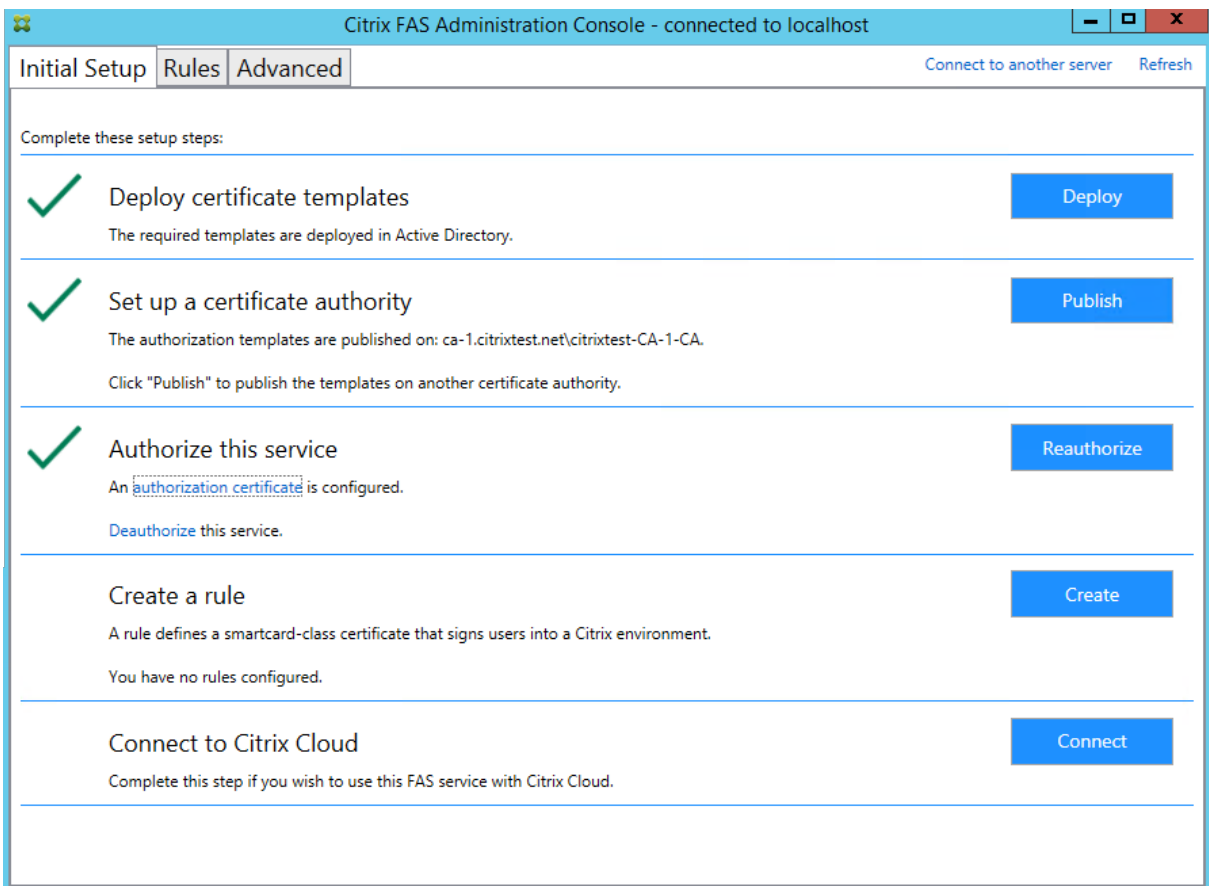
```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b

Id           : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address      : [Offline CSR]
TrustArea    : a5c27fcc-1dd7-4c2b-8963-16ec311020fc
CertificateRequest :
Status       : 0k
```

Pour vérifier que la clé privée du certificat de l'autorité d'inscription est correctement stockée dans le module de plateforme sécurisée, utilisez les commandes PowerShell suivantes. Le champ PrivateKeyProvider sera défini sur *Microsoft Platform Crypto Provider* si la clé privée du certificat de l'autorité d'inscription est stockée dans le module de plateforme sécurisée :

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
2 Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
3 <!--NeedCopy-->
```

Étape 12 : fermez la console de gestion FAS, puis redémarrez-la.



Remarque : l'étape « Autoriser ce service » comporte une coche verte.

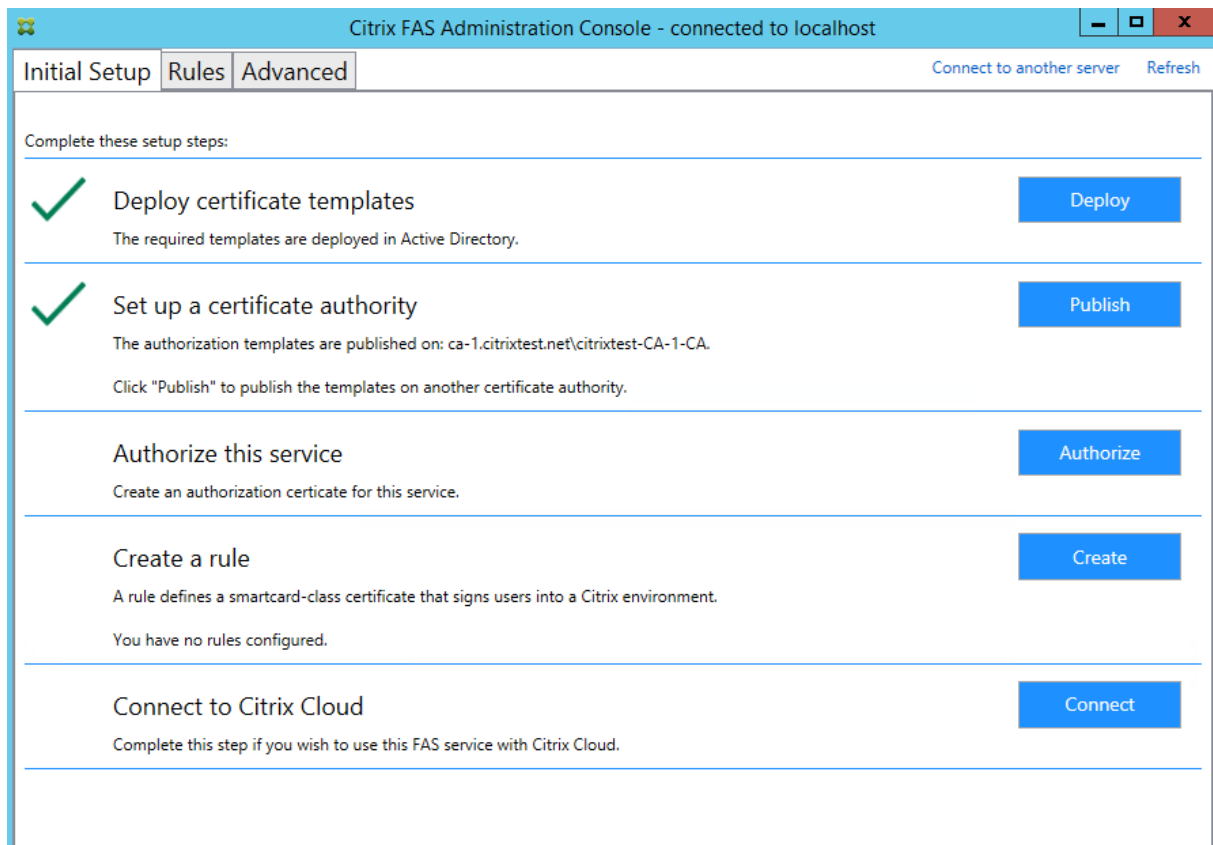
Étape 13 : sélectionnez l'onglet **Rules** dans la console de gestion FAS et modifiez les paramètres décrits dans [Installer et configurer](#).

Exemple 3

Cet exemple illustre une clé privée de certificat d'autorité d'inscription et les clés privées de certificats utilisateur stockées dans un HSM. Cet exemple suppose un HSM configuré. Votre HSM aura un nom de fournisseur, par exemple « HSM_Vendor's Key Storage Provider ».

Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur HSM si l'hyperviseur est pris en charge.

Étape 1. Lors de la configuration initiale de FAS à l'aide de la console de gestion, effectuez uniquement les deux premières étapes : « Déployer les modèles de certificat » et « Configurer une autorité de certification ».



Étape 2 : consultez la documentation de votre fournisseur HSM pour déterminer ce que doit être la valeur `ProviderName` de votre HSM. Si votre HSM utilise CAPI, le fournisseur peut être désigné dans la documentation comme fournisseur de service cryptographique (CSP). Si votre HSM utilise CNG, le fournisseur peut être désigné comme Key Storage Provider (KSP).

Étape 3 : modifiez le fichier de configuration comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>
```

Le fichier doit maintenant s'afficher comme suit :

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name. -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV_RSA_AES is 24 -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Suppress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value="" / -->
  </appSettings>
</startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Ce scénario part du principe que votre HSM utilise CNG de sorte que la valeur ProviderLegacyCsp est définie sur false. Si votre HSM utilise CAPI, la valeur ProviderLegacyCsp devrait être définie sur true. Consultez la documentation de votre fournisseur HSM pour déterminer si votre HSM utilise CAPI ou CNG. De plus, consultez la documentation de votre fournisseur HSM sur les longueurs de clé prises en charge pour la génération de clé asymétrique RSA. Dans cet exemple, la longueur de clé est définie sur la valeur par défaut de 2048 bits. Assurez-vous que la longueur de clé que vous avez spécifiée est prise en charge par votre matériel.

Étape 4 : redémarrez le Service d'authentification fédérée Citrix pour lire les valeurs à partir du fichier de configuration.

Étape 5 : générez la paire de clés RSA dans le HSM et créez la demande de signature de certificat en cliquant sur **Authorize** dans l'onglet **Initial Setup** de la console de gestion FAS.

Étape 6 : pour vérifier que la paire de clés a été générée dans le HSM, vérifiez les entrées d'application dans le journal d'événements Windows :

```
[S16] PrivateKey::Create [Identifiant e1608812-6693-4c54-a937-91a2e27df75b_TWAIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

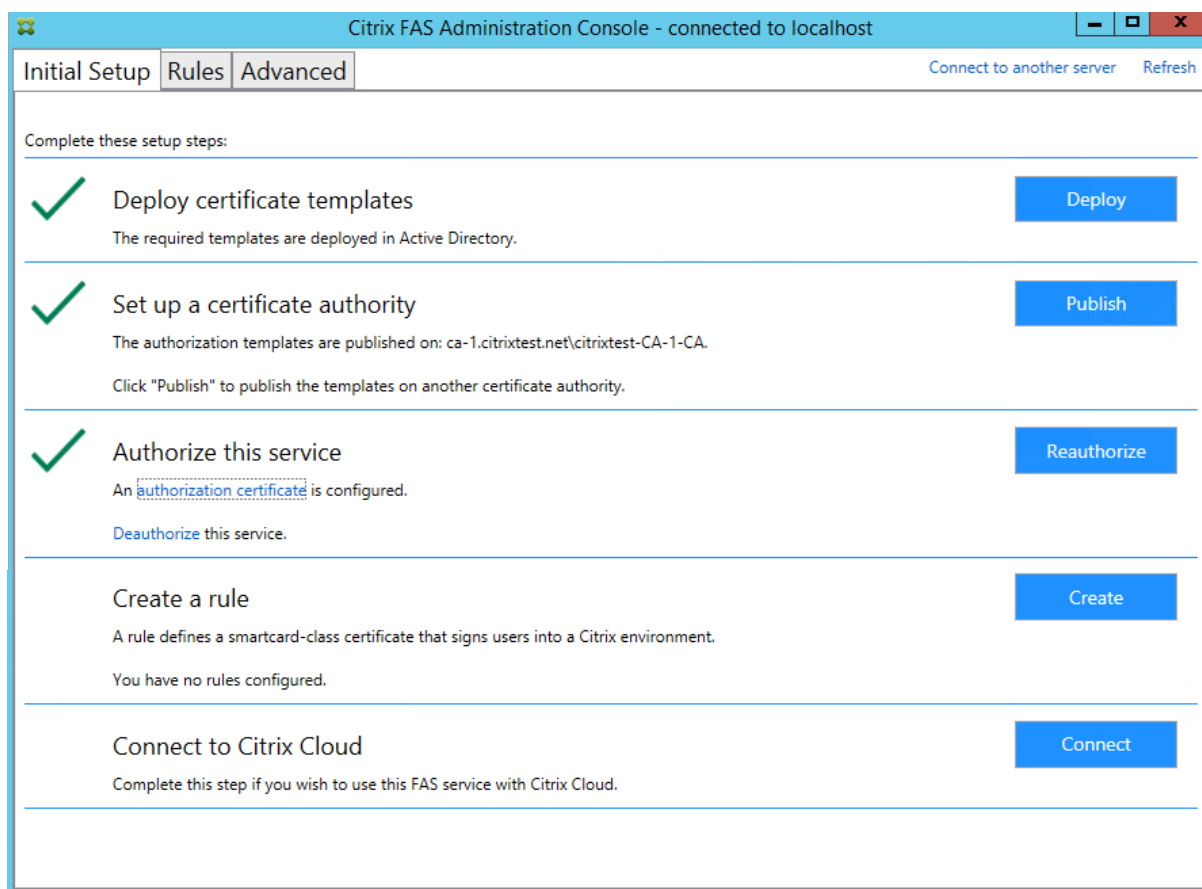
Remarque : [Provider: [CNG] HSM_Vendor's Key Storage Provider]

Étape 7 : sur le serveur de l'autorité de certification, dans la MMC d'autorité de certification, sélectionnez le nœud **Demandes en attente**.

| Request ID | Binary Request | Request Status Code | Request Disposition Message | Request Submission Date | Requester Name | Request Country/Region |
|------------|------------------|------------------------|-----------------------------|-------------------------|----------------|------------------------|
| 107 | -----BEGIN NE... | The operation compl... | Taken Under Submission | 07/04/2016 14:04 | AUTH\UCSHSMS | |

Cliquez avec le bouton droit sur la demande et choisissez **Délivrer**.

Remarque : l'étape « Autoriser ce service » comporte une coche verte.



Étape 8 : sélectionnez l'onglet **Rules** dans la console de gestion FAS et modifiez les paramètres décrits dans [Installer et configurer](#).

Stockage de certificats FAS

FAS n'utilise pas le magasin de certificats Microsoft sur le serveur FAS pour stocker ses certificats. Il utilise une base de données intégrée.

Pour déterminer le GUID du certificat d'autorité d'inscription, entrez les applets de commande PowerShell suivantes sur le serveur FAS :

```
Add-pssnapin Citrix.a\*
```

```
Get-FasAuthorizationCertificate -address \<FAS server FQDN>
```

Par exemple, **Get-FasAuthorizationCertificate -address cg-fas-2.auth.net :**

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local

Id                : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address           : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea         : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest :
Status            : MaintenanceDue

Id                : fcb185f9-5069-4e34-8625-a333ac126535
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
MIICaDCCAVACAQIwIzEhMB8GCgmSjomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAxyNzaiWX8DhUnOZMS2YV5Dhr36AV5BGeIYOGVCFKvZPe
Rmm/xOVM6cNKsLbew3dYlbo+vdglWg86DFRVxTORho1lV86iazDZy0iYGgxe9/s8YZzCspVWN1nB1
zX0UJfo1qo9UsmImYr7MR/dhGAtkfSfUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
ECz/CbXR00uiDhw+VWbjcsgklcavzvC/jR33F9dZ5XNgKRiGHgfD/lBb3eIZKA400oi90u64Q916
3ba9BnihqxIgvwWIL0myUfiJmCgbhLJV4TPBop0dKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgCJNJO/MU7/7X
bZB46drLpFzpzF88DkmFoCEg0x1bzFX9waaifS9CHC/AcEzb1N925y1gq1jsfC315TCKBAeLFoM1
PSEkfyMQU058YCuL1kFn1LXLSeQ3qJTz5vptYR0awFmUMQLffwLSR1v0u58DJ5rpa5rwdXJk3TOa
G10/xJo/NRM0wMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcw714JP+XIeFrE1TZmUL2skNIXEPNHc
H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiiy0MLGZ00aiER+z8=
-----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval
```

Pour obtenir une liste de certificats utilisateur, entrez :

```
Get-FasUserCertificate -address \<FAS server FQDN>
```

Par exemple, **Get-FasUserCertificate -address cg-fas-2.auth.net**

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local

ThumbPrint       : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName : walter@adfs.ext
Role              : default
CertificateDefinition : default_Definition
ExpiryDate        : 05/04/2016 12:02:13
```

Remarque :

Lorsque vous utilisez un HSM pour stocker des clés privées, les conteneurs HSM sont identifiés par un GUID. Le GUID de la clé privée dans le HSM peut être obtenu à l'aide de :

```
Get-FasUserCertificate -address \<FAS server FQDN> -KeyInfo $true
```

Par exemple :

```
Get-FasUserCertificate -address fas3.djwfas.net -KeyInfo $true
```

```
PS C:\Users\administrator> Get-FasUserCertificate -Address fas3.djwfas.net -KeyInfo $true

PrivateKeyIdentifier : 38405c4d-63af-43e4-9135-2412246b1112
PrivateKeyProvider   : Microsoft Software Key Storage Provider
PrivateKeyIsCng      : True
ThumbPrint           : AD2441F050A02966AA4DB190BA084976528DB667
UserPrincipalName    : joe@djwfas.net
Role                  : default
CertificateDefinition : default_Definition
SecurityContext       :
ExpiryDate            : 19/01/2018 09:18:48
```

Informations connexes

- L'article [Installer et configurer](#) est le document de référence principal pour obtenir des informations sur l'installation et la configuration de FAS.
- Les déploiements FAS courants sont décrits dans l'article [Vue d'ensemble des architectures du Service d'authentification fédérée](#).
- D'autres informations pratiques sont disponibles dans l'article [Configuration avancée](#).

Configuration du réseau et de la sécurité

June 5, 2024

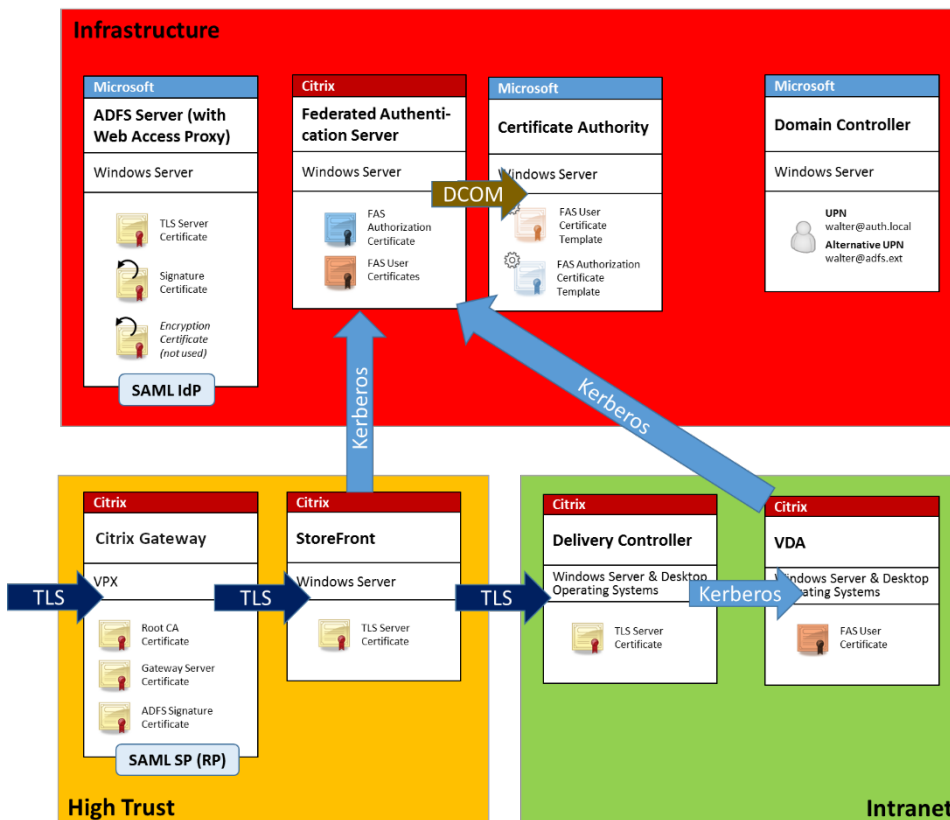
Le Service d'authentification fédérée (FAS) est étroitement intégré à Microsoft Active Directory et à l'autorité de certification Microsoft. Assurez-vous que le système est géré et sécurisé de manière appropriée, en développant une stratégie de sécurité comme vous le feriez pour un contrôleur de domaine ou toute autre infrastructure critique.

Ce document présente les problèmes de sécurité à prendre en compte lorsque vous déployez FAS. Il offre également une vue d'ensemble des fonctionnalités qui peuvent vous aider à sécuriser votre infrastructure.

Architecture réseau

Le diagramme suivant illustre les composants principaux et les limites de sécurité utilisés dans un déploiement FAS.

Le serveur FAS fait partie de l'infrastructure de sécurité, tout comme l'autorité de certification et le contrôleur de domaine. Dans un environnement fédéré, Citrix Gateway et Citrix StoreFront sont des composants qui permettent d'authentifier les utilisateurs. L'introduction de FAS n'affecte pas les autres composants Citrix Virtual Apps and Desktops.



Sécurité du réseau et pare-feu

Le protocole TLS sur le port 443 protège la communication entre les composants Citrix Gateway, StoreFront et Delivery Controller. Le serveur StoreFront se charge uniquement des connexions sortantes et Citrix Gateway accepte uniquement les connexions via Internet utilisant HTTPS sur le port 443.

Le serveur StoreFront contacte le serveur FAS sur le port 80 à l'aide de l'authentification mutuelle Kerberos. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS, et l'identité du compte de machine Kerberos du serveur StoreFront. Cette méthode d'authentification génère un « handle d'informations d'identification » à usage unique requis par le Citrix Virtual Delivery Agent (VDA) pour connecter l'utilisateur.

Lorsqu'une session HDX est connectée au VDA, le VDA contacte également le serveur FAS sur le port 80. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS, et l'identité de la machine Kerberos du VDA. De plus, le VDA doit fournir le « handle d'informations d'identification » pour accéder au certificat et à la clé privée.

L'autorité de certification Microsoft accepte les communications à l'aide du DCOM authentifié auprès de Kerberos, qui peut être configuré pour utiliser un port TCP fixe. L'autorité de certification requiert que le serveur FAS fournisse un paquet CMC signé par un certificat d'agent d'inscription approuvé.

| Serveur | Ports du pare-feu |
|-------------------------------------|---|
| Service d'authentification fédérée | [entrant] Kerberos via HTTP depuis StoreFront et VDA, [sortant] DCOM vers autorité de certification Microsoft |
| Citrix Gateway | [entrant] HTTPS depuis les machines clientes, [entrant/sortant] HTTPS depuis/vers un serveur StoreFront, [sortant] HDX vers VDA |
| StoreFront | [entrant] HTTPS depuis Citrix Gateway, [entrant/sortant] HTTPS vers Delivery Controller, [sortant] HTTP Kerberos vers FAS |
| Delivery Controller | [entrant] HTTPS depuis un serveur StoreFront, [entrant/sortant] Kerberos sur HTTP à partir de VDA |
| VDA | [entrant/sortant] Kerberos via HTTP depuis Delivery Controller, [entrant] HDX depuis Citrix Gateway, [sortant] Kerberos HTTP vers FAS |
| Autorité de certification Microsoft | [entrant] DCOM et signé depuis FAS |

Connexions entre Citrix Federated Authentication Service et Citrix Cloud

La console et FAS accèdent aux adresses suivantes à l'aide du compte de l'utilisateur et du compte de service réseau, respectivement.

- Console d'administration FAS, sous le compte utilisateur
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - Adresses requises par un fournisseur d'identité tiers, si elles sont utilisées dans votre environnement
- Service FAS, sous le compte de service réseau :
 - *.citrixworkspacesapi.net
 - *.citrixnetworkapi.net

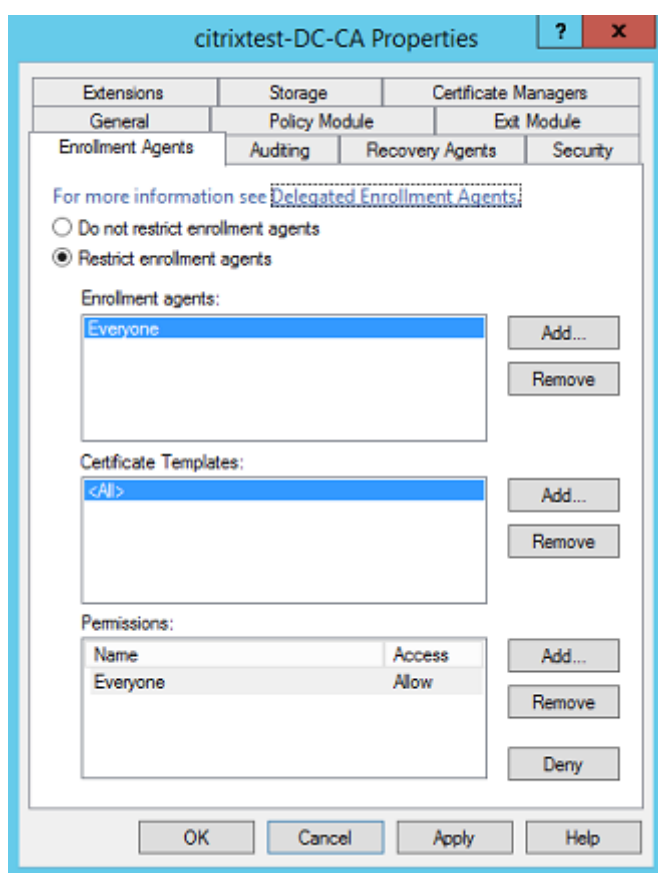
Si votre environnement inclut des serveurs proxy, configurez le proxy utilisateur avec les adresses de la console d'administration FAS. Assurez-vous également que l'adresse du compte de service réseau est configurée à l'aide de netsh ou d'un outil similaire.

Considérations de sécurité

FAS dispose d'un certificat d'autorité d'inscription qui lui permet d'émettre des certificats de manière autonome pour vos utilisateurs de domaine. Cela permet de développer et d'implémenter une stratégie de sécurité pour protéger les serveurs FAS et limiter leurs autorisations.

Agents d'inscription délégués

FAS émet des certificats utilisateur en agissant en tant qu'agent d'inscription. L'autorité de certification Microsoft vous permet de limiter les agents d'inscription, les modèles de certificats et les utilisateurs pour lesquels les agents d'inscription peuvent émettre des certificats.



Vous pouvez utiliser la boîte de dialogue indiquée pour vous assurer que :

- La liste *Agents d'inscription* ne contient que des serveurs FAS.
- La liste *Modèles de certificats* contient uniquement des modèles FAS.
- La liste *Autorisations* contient les utilisateurs autorisés à utiliser le FAS. Par exemple, il est déconseillé d'émettre des certificats pour un groupe d'administrateurs ou d'utilisateurs protégés.

Configuration de la liste de contrôle d'accès

Comme décrit dans la section [Configurer des règles](#), vous devez configurer une liste de serveurs StoreFront. Ces serveurs StoreFront certifient l'identité des utilisateurs auprès de FAS lors de l'émission de certificats. De même, vous pouvez restreindre les utilisateurs pour lesquels des certificats seront émis, et les machines VDA auprès desquelles ils peuvent s'authentifier. Cette fonctionnalité vient s'ajouter à toute autre fonctionnalité Active Directory standard ou de sécurité d'autorité de certification que vous configurez.

Paramètres de pare-feu

Toutes les communications avec les serveurs FAS utilisent des connexions réseau Kerberos WCF authentifiées mutuellement sur le port 80.

Analyse du journal des événements

FAS et le VDA écrivent des informations dans le journal d'événements Windows. Ce journal peut être utilisé pour à des fins de contrôle et d'audit d'informations. La section [Journaux d'événements](#) répertorie les entrées de journal d'événements qui peuvent être générées.

Modules matériels de sécurité

Toutes les clés privées, notamment celles des certificats utilisateur émis par FAS, sont stockées en tant que clés privées non exportables par le Compte de service réseau. FAS prend en charge l'utilisation d'un module matériel de sécurité cryptographique, si votre stratégie de sécurité l'exige.

Une configuration cryptographique de faible niveau est disponible dans le fichier FederatedAuthenticationService.exe.config. Ces paramètres s'appliquent lorsque les clés privées sont créées. Par conséquent, des paramètres différents peuvent être utilisés pour les clés privées d'autorité d'inscription (par exemple, 4 096 bits, Module de plateforme sécurisée protégé) et les certificats utilisateur d'exécution.

| Paramètre | Description |
|-------------------|---|
| ProviderLegacyCsp | Lorsque cette option est définie sur true, FAS utilise l'API CryptoAPI (CAPI) de Microsoft. Sinon, FAS utilise l'API Cryptography Next Generation (CNG) de Microsoft. |
| ProviderName | Nom du fournisseur CAPI ou CNG à utiliser. |

| Paramètre | Description |
|---------------|--|
| ProviderType | Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit toujours être 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM en décide autrement. |
| KeyProtection | Contrôle l'indicateur « Exportable » des clés privées. Permet également l'utilisation du stockage de clé TMP (Module de plateforme sécurisée), s'il est pris en charge par le matériel. |
| KeyLength | Longueur de clé des clés privées RSA. Les valeurs prises en charge sont 1024, 2048 et 4096 (valeur par défaut : 2048). |

Responsabilités en matière d'administration

L'administration de l'environnement peut être divisée dans les groupes suivants :

| Nom | Responsabilité |
|--|--|
| Administrateur d'entreprise | Installer et sécuriser les modèles de certificat dans la forêt |
| Administrateur de domaine | Configurer les paramètres de stratégie de groupe |
| Administrateur d'autorité de certification | Configurer l'autorité de certification |
| Administrateur FAS | Installer et configurer le serveur FAS |
| Administrateur StoreFront/Citrix Gateway | Configurer l'authentification utilisateur |
| Administrateur Citrix Virtual Desktops | Configurer les VDA et les Controller |

Chaque administrateur contrôle différents aspects du modèle de sécurité, ce qui assure une protection approfondie du système.

Paramètres de stratégie de groupe

Les machines FAS approuvées sont identifiées par une table de recherche « numéro d'index -> FQDN » configurée via la stratégie de groupe. Lors de la communication avec un serveur FAS, les clients vérifient l'identité Kerberos `HOST\<fqdn>` du serveur FAS. Tous les serveurs qui accèdent au serveur

FAS doivent posséder les mêmes configurations de nom domaine complet (FQDN) pour le même index ; dans le cas contraire, il est possible que StoreFront et les VDA contactent des serveurs FAS différents.

Citrix recommande d'appliquer une stratégie unique à toutes les machines de l'environnement afin d'éviter toute erreur de configuration. Soyez prudent lors de la modification de la liste des serveurs FAS, plus particulièrement lors de la suppression ou de la réorganisation d'entrées.

Le contrôle de cet objet de stratégie de groupe doit être limité aux administrateurs FAS (et/ou aux administrateurs de domaine) qui installent et désactivent des serveurs FAS. Prenez soin de ne pas réutiliser le nom de domaine complet (FQDN) d'une machine peu de temps après avoir désactivé un serveur FAS.

Modèles de certificats

Si vous ne souhaitez pas utiliser le modèle de certificat Citrix_SmartcardLogon fourni avec FAS, vous pouvez modifier une copie. Les modifications suivantes sont prises en charge.

Renommer un modèle de certificat

Si vous souhaitez renommer Citrix_SmartcardLogon pour qu'il corresponde aux conventions de nom de modèle de votre entreprise, vous devez :

- Créer une copie du modèle de certificat et le renommer pour qu'il corresponde aux conventions de nom de modèle de votre entreprise.
- Utiliser les commandes PowerShell FAS pour administrer FAS, plutôt que l'interface utilisateur d'administration. (L'interface utilisateur d'administration est conçue uniquement pour une utilisation avec les noms de modèle par défaut Citrix).
 - Utiliser le composant logiciel enfichable pour modèles de certificats MMC de Microsoft ou la commande Publish-FasMsTemplate pour publier votre modèle et
 - utiliser la commande New-FasCertificateDefinition pour configurer les FAS avec le nom de votre modèle.

Modifier les propriétés générales

Par défaut, la durée de vie d'un certificat utilisateur est de sept jours. Vous pouvez modifier la période de validité dans le modèle de certificat.

Ne modifiez pas la période de renouvellement. FAS ignore ce paramètre dans le modèle de certificat. FAS renouvelle automatiquement le certificat au cours de sa période de validité.

Modifier les propriétés de traitement de demande

Ne modifiez pas ces propriétés. FAS ignore ces paramètres dans le modèle de certificat. FAS désélectionne toujours **Autoriser l'exportation de la clé privée** et **Renouveler avec la même clé**.

Modifier les propriétés de cryptographie

Ne modifiez pas ces propriétés. FAS ignore ces paramètres dans le modèle de certificat.

Consultez [Protection des clés privées](#) pour connaître les paramètres équivalents fournis par FAS.

Modifier les propriétés d'attestation de clé

Ne modifiez pas ces propriétés. FAS ne gère pas l'attestation de clé.

Modifier les propriétés de modèles obsolètes

Ne modifiez pas ces propriétés. FAS ne gère pas les modèles obsolètes.

Modifier les propriétés d'extensions

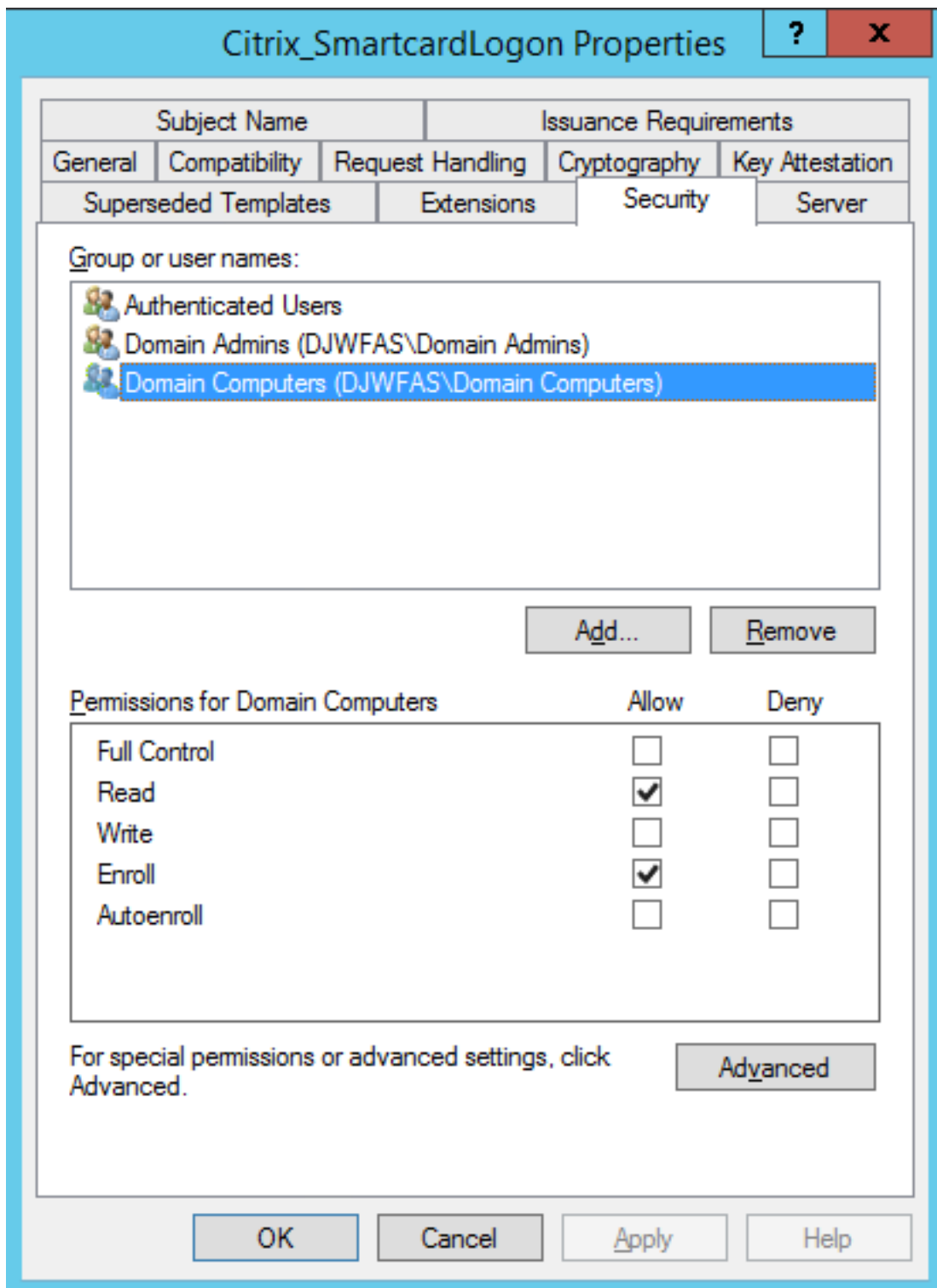
Vous pouvez modifier ces paramètres en fonction de la stratégie de votre organisation.

Remarque : des paramètres d'extension inappropriés peuvent entraîner des problèmes de sécurité ou aboutir à des certificats inutilisables.

Modifier les propriétés de sécurité

Citrix recommande de modifier ces paramètres pour accorder les autorisations **Lire** et **Inscription** aux comptes de machine des serveurs FAS uniquement. Le service FAS ne requiert aucune autre autorisation. Toutefois, comme pour d'autres modèles de certificat, vous pouvez :

- autoriser les administrateurs à lire ou écrire le modèle
- autoriser les utilisateurs authentifiés à lire le modèle



Modifier les propriétés de nom du sujet

Citrix vous recommande de ne pas modifier ces propriétés.

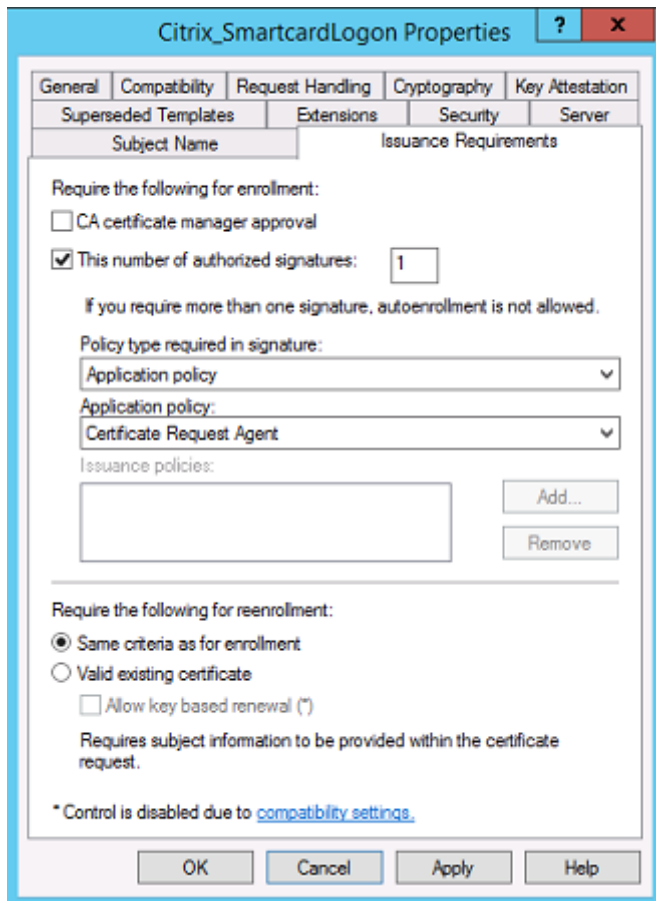
L'option *Build from this Active Directory information* est sélectionnée dans le modèle, obligeant l'autorité de certification à inclure le SID de l'utilisateur dans une extension de certificat, ce qui fournit un mappage solide avec le compte Active Directory de l'utilisateur.

Modifier les propriétés de serveur

Citrix ne le recommande pas, mais vous pouvez modifier ces paramètres en fonction de la stratégie de votre organisation, si nécessaire.

Modifier les propriétés de conditions d'émission

Ne modifiez pas ces paramètres. Ces paramètres doivent être définis comme suit :



Modifier les propriétés de compatibilité

Vous pouvez modifier ces paramètres. Le paramètre doit être au moins **Windows Server 2003 CAs** (version de schéma 2). Toutefois, FAS prend en charge uniquement Windows Server 2008 et les autorités de certification ultérieures. Comme expliqué ci-dessus, FAS ignore également les paramètres

supplémentaires disponibles si **Windows Server 2008 CAs** (version de schéma 3) ou **Windows Server 2012 CAs** est sélectionné (version de schéma 4).

Administration de l'autorité de certification

L'administrateur de l'autorité de certification est responsable de la configuration du serveur d'autorité de certification et de l'émission de la clé privée de certificat qu'il utilise.

Publication de modèles

Pour qu'une autorité de certification puisse émettre des certificats basés sur un modèle fourni par l'administrateur de l'entreprise, l'administrateur de l'autorité de certification doit choisir de publier ce modèle.

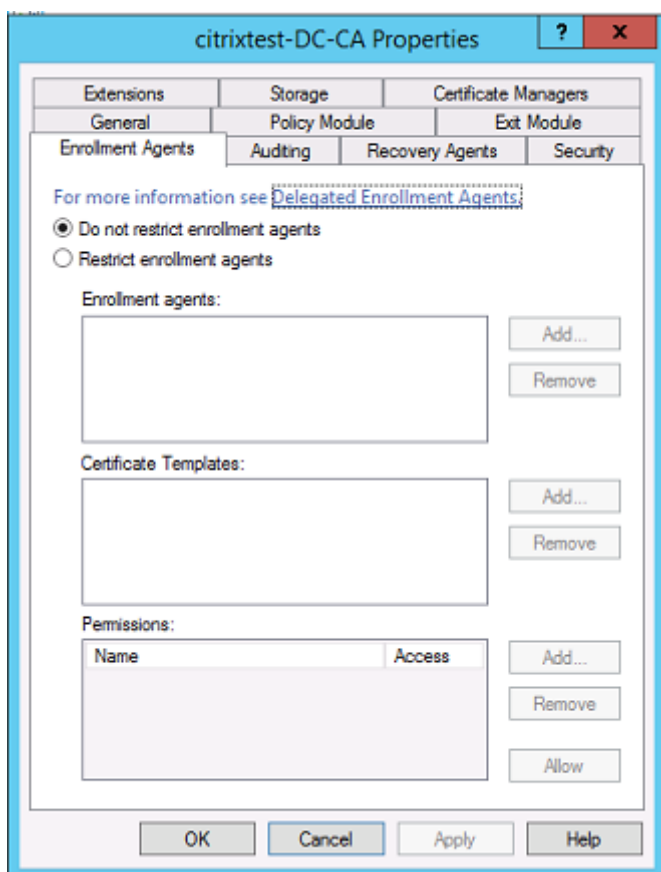
Une simple pratique de sécurité consiste à publier uniquement les modèles de certificat d'autorité d'inscription lorsque les serveurs FAS sont installés, ou d'opter pour un processus d'émission hors connexion. Dans les deux cas, l'administrateur d'autorité de certification doit conserver un contrôle total sur l'autorisation des demandes de certificat d'autorité d'inscription et disposer d'une stratégie pour autoriser les serveurs FAS.

Paramètres de pare-feu

L'administrateur de l'autorité de certification contrôle les paramètres de pare-feu réseau de l'autorité de certification, ce qui lui permet de contrôler les connexions entrantes. L'administrateur de l'autorité de certification peut configurer le protocole TCP de DCOM et des règles de pare-feu de manière à ce que seuls les serveurs FAS puissent demander des certificats.

Inscription restreinte

Par défaut, le détenteur d'un certificat d'autorité d'inscription peut émettre des certificats pour tous les utilisateurs, à l'aide d'un modèle de certificat autorisant l'accès. L'émission de certificats doit être restreinte à un groupe d'utilisateurs sans privilèges à l'aide de la propriété d'autorité de certification « Restreindre les agents d'inscription ».



Modules de stratégie et d'audit

Pour les déploiements avancés, des modules de sécurité personnalisés peuvent être utilisés pour assurer le suivi et interdire l'émission de certificats.

Administration de FAS

FAS possède plusieurs fonctions de sécurité.

Restreindre StoreFront, les utilisateurs et les VDA via une liste de contrôle d'accès

Au centre du modèle de sécurité de FAS figure le contrôle grâce auquel les comptes Kerberos peuvent accéder aux fonctionnalités :

| Vecteur d'accès | Description |
|-------------------------------------|---|
| StoreFront [fournisseur d'identité] | Ces comptes Kerberos sont approuvés pour déclarer qu'un utilisateur a été correctement authentifié. Si l'un de ces comptes est compromis, des certificats peuvent être créés et utilisés pour les utilisateurs autorisés par la configuration de FAS. |
| VDA [partie de confiance] | Il s'agit des machines qui sont autorisées à accéder aux certificats et aux clés privées. Un handle d'informations d'identification récupéré par le fournisseur d'identité est également nécessaire, de façon à limiter les possibilités d'attaque du système par un compte VDA compromis dans ce groupe. |
| Utilisateurs | Cette option contrôle les utilisateurs qui peuvent être certifiés par le fournisseur d'identité. Veuillez noter qu'il existe un chevauchement avec les options de configuration « Restreindre les agents d'inscription » de l'autorité de certification. En règle générale, il est conseillé d'inclure uniquement des comptes non privilégiés dans cette liste. Ceci empêche un compte StoreFront compromis de réaffecter des privilèges à un niveau administratif plus élevé. Particulièrement, les comptes d'administrateur de domaine ne doivent pas être autorisés par cette ACL. |

Configurer des règles

Les règles sont utiles si plusieurs déploiements Citrix Virtual Apps ou Citrix Virtual Desktops indépendants utilisent la même infrastructure de serveur FAS. Chaque règle dispose d'options de configuration distinctes ; en particulier, les listes de contrôle d'accès Kerberos (ACL) peuvent être configurées indépendamment.

Configurer l'autorité de certification et les modèles

Différents modèles de certificats et autorités de certification peuvent être configurés afin d'octroyer des droits d'accès différents. Des configurations avancées peuvent choisir d'utiliser plus ou moins de certificats puissants, en fonction de l'environnement. À titre d'exemple, les utilisateurs identifiés en tant que « externes » peuvent posséder un certificat avec moins de privilèges que les utilisateurs « internes ».

Certificats d'authentification et dans la session

L'administrateur FAS peut contrôler si le certificat utilisé pour l'authentification peut être utilisé dans la session de l'utilisateur.

Par exemple, un utilisateur peut uniquement disposer de certificats « de signature » dans la session, afin de réserver le certificat « d'ouverture de session » plus puissant uniquement pour l'ouverture de session.

Protection de clé privée et longueur de clé

L'administrateur FAS peut configurer FAS afin de stocker les clés privées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Citrix recommande de toujours stocker la clé privée du certificat de l'autorité d'inscription dans un TPM pour la protéger. FAS permet d'enregistrer la clé privée dans un TPM dans le cadre du processus de demande de certificat « en mode déconnecté ».

De même, les clés privées de certificat utilisateur peuvent être stockées dans un module TPM ou HSM. Toutes les clés doivent être générées comme « non exportables » et d'une longueur minimum de 2 048 bits.

Journaux d'événements

Le serveur FAS fournit des informations détaillées sur la configuration et des [journaux d'événements](#), qui peuvent être utilisés pour l'audit et la détection des intrusions.

Accès administratif et outils d'administration

FAS comprend des fonctionnalités d'administration à distance (authentification mutuelle Kerberos) ainsi que des outils. Les membres du « groupe Administrateurs local » exercent un contrôle total sur la configuration du FAS. La configuration FAS doit être correctement tenue à jour.

Administrateurs Citrix Virtual Apps, Citrix Virtual Desktops et VDA

L'utilisation de FAS ne modifie pas le modèle de sécurité des administrateurs Delivery Controller et VDA, car le « handle d'informations d'identification » de FAS remplace simplement le « mot de passe Active Directory ». Les groupes d'administration Controller et VDA doivent contenir uniquement des utilisateurs approuvés. Les journaux d'audit et d'événements doivent être tenus à jour.

Sécurité des serveurs Windows

Tous les correctifs doivent avoir été installés sur tous les serveurs, ainsi que des pare-feu et des logiciels antivirus. Les serveurs d'infrastructure dont la sécurité est critique doivent être conservés dans un endroit sûr, et un soin tout particulier doit être apporté aux options de cryptage de disque et de maintenance des machines virtuelles.

L'audit et les journaux d'événements doivent être stockés de manière sécurisée sur une machine distante.

L'accès RDP doit être limité aux administrateurs autorisés. Citrix recommande d'ouvrir les sessions des comptes utilisateur par carte à puce, notamment pour les comptes d'administrateur de domaine et d'autorité de certification.

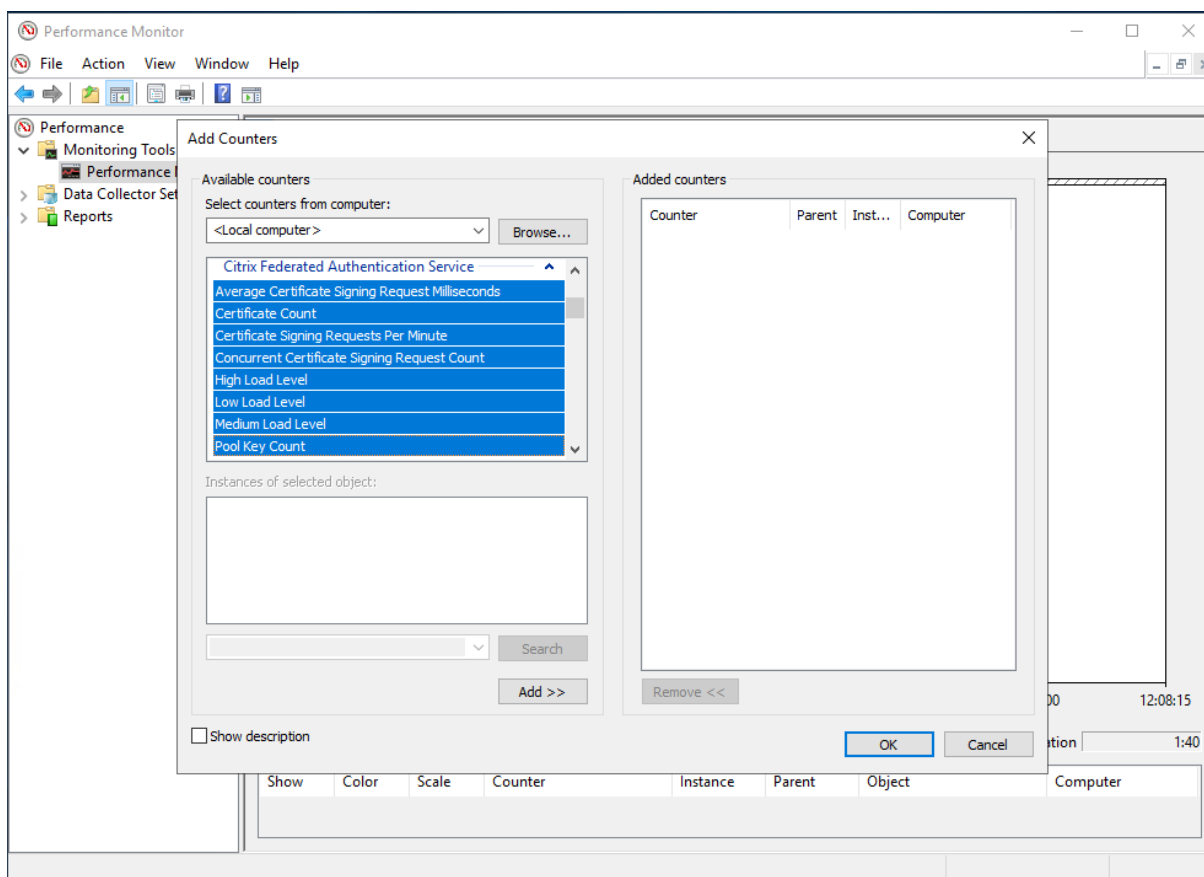
Informations connexes

- L'article [Installer et configurer](#) est le document de référence principal pour obtenir des informations sur l'installation et la configuration de FAS.
- Les architectures FAS sont présentées dans l'article [Architectures de déploiement](#).
- D'autres informations pratiques sont disponibles dans l'article [Configuration avancée](#).

Compteurs de performances

June 5, 2024

FAS inclut un jeu de compteurs de performances conçus pour surveiller la charge.



Le tableau suivant répertorie les compteurs disponibles. Sauf indication contraire, chaque compteur est mis à jour toutes les 10 secondes.

| Nom | Description |
|--|--|
| Average Certificate Signing Request Milliseconds | Durée moyenne (en millisecondes) des demandes de signature de certificat, calculée à l'aide des données de la minute précédente. |
| Certificate Count | Nombre de certificats gérés par le service d'authentification fédérée. |
| Certificate Signing Requests Per Minute | Nombre de demandes de signature de certificat émises par le service d'authentification fédérée par minute, calculé à l'aide des données de la minute précédente. |
| Concurrent Certificate Signing Request Count | Nombre de demandes de signature de certificats simultanées traitées par le service d'authentification fédérée. |

| Nom | Description |
|-----------------------------------|--|
| Pool Key Count | Nombre de paires de clés pré-générées dans le pool de clés pouvant être utilisées pour les demandes de signature de certificat. |
| Private Key Operations Per Minute | Nombre d'opérations de clé privée de certificat effectuées par le service d'authentification fédérée par minute, calculé à l'aide des données de la minute précédente. |
| Nombre de sessions | Nombre de sessions VDA suivies par le service d'authentification fédérée. |
| Low/Medium/High Load Level | Estimation de la charge que le service d'authentification fédérée peut accepter en termes de demandes de signature de certificat par minute. Les estimations sont mises à jour toutes les minutes, à l'aide des données de la minute précédente. Le dépassement du seuil « High Load » peut entraîner l'échec du lancement d'applications ou de postes de travail publiés. |

Résoudre les problèmes d'ouverture de session Windows

June 5, 2024

Cet article décrit les journaux et les messages d'erreur que Windows génère lorsqu'un utilisateur ouvre une session à l'aide de certificats ou de cartes à puce ou les deux. Ces journaux fournissent des informations que vous pouvez utiliser pour résoudre les échecs d'authentification.

Certificats et infrastructure de clé publique

Windows Active Directory propose plusieurs magasins de certificats qui gèrent les certificats pour les utilisateurs qui ouvrent une session.

- **Magasin de certificats NTAUTH** : pour s'authentifier auprès de Windows, l'autorité de certification émettant les certificats utilisateur (aucune chaîne n'est prise en charge) doit être placée dans le magasin NTAUTH. Pour voir ces certificats, dans le programme certutil, entrez :
`certutil -viewstore -enterprise NTAUTH`

- **Magasins de certificats racine et intermédiaires** : en règle générale, les systèmes d'ouverture de session par certificat peuvent fournir un seul certificat. Donc, si une chaîne est utilisée, le magasin de certificats intermédiaires sur toutes les machines doit inclure ces certificats. Le certificat racine doit être dans le magasin racine de confiance et l'avant-dernier certificat doit être dans le magasin NTAAuth.
- **Extensions de certificat d'ouverture de session et stratégie de groupe** : Windows peut être configuré pour appliquer la vérification des EKU et d'autres stratégies de certificat. Consultez la documentation Microsoft : [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)).

| Stratégie du Registre | Description |
|--|--|
| AllowCertificatesWithNoEKU | Lorsqu'elle est désactivée, les certificats doivent inclure l'Utilisation améliorée de la clé (EKU) pour l'ouverture de session avec carte à puce. |
| AllowSignatureOnlyKeys | Par défaut, Windows filtre les clés privées de certificats qui ne permettent pas le décryptage RSA. Cette option remplace ce filtre. |
| AllowTimeInvalidCertificates | Par défaut, Windows filtre les certificats expirés. Cette option remplace ce filtre. |
| EnumerateECCerts | Active l'authentification à courbe elliptique. |
| X509HintsNeeded | Si un certificat ne contient pas de nom d'utilisateur principal (UPN) unique, ou s'il est ambigu, cette option permet aux utilisateurs de spécifier manuellement leur compte d'ouverture de session Windows. |
| UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors | Désactive la vérification de la révocation des certificats (définie sur le contrôleur de domaine). |

- **Certificats du contrôleur de domaine** : pour authentifier les connexions Kerberos, tous les serveurs doivent avoir des certificats « Contrôleur de domaine » appropriés. Ils peuvent être demandés depuis le menu du composant logiciel enfichable MMC « Local Computer Certificate Personal Store » (magasin personnel de certificats de l'ordinateur local).

Nom UPN et mappage de certificat

Il est recommandé que les certificats utilisateur incluent un nom d'utilisateur principal (UPN) unique dans l'extension Nom de sujet alternatif.

Noms UPN dans Active Directory

Par défaut, chaque utilisateur d'Active Directory est associé à un UPN implicite, basé sur le modèle <NomUtilisateur_sam>@<NetBios_domaine> et <NomUtilisateur_sam>@<FQDN_domaine>. Les domaines disponibles et les noms de domaine complets sont inclus dans l'entrée RootDSE de la forêt. Un seul domaine peut disposer de plusieurs noms de domaine complets enregistrés dans RootDSE.

En outre, chaque utilisateur d'Active Directory a un nom UPN explicite et des altUserPrincipalNames. Ce sont des entrées LDAP qui spécifient le nom d'utilisateur principal (UPN) pour l'utilisateur.

Lors d'une recherche d'utilisateurs par UPN, Windows recherche d'abord dans le domaine courant (en fonction de l'identité du processus de recherche de l'UPN) les UPN explicites, puis les UPN alternatifs. S'il n'existe pas de correspondance, il recherche l'UPN implicite, qui peut se résoudre sur différents domaines de la forêt.

Service de mappage de certificat

Si un certificat ne contient pas d'UPN explicite, Active Directory peut stocker un certificat public exact pour chaque utilisation dans un attribut « x509certificate ». Pour résoudre un tel certificat pour un utilisateur, un ordinateur peut interroger cet attribut directement (par défaut, dans un seul domaine).

L'utilisateur peut spécifier un compte d'utilisateur qui accélère la recherche et permet également à cette fonctionnalité d'être utilisée dans un environnement inter-domaines.

S'il existe plusieurs domaines dans la forêt et que l'utilisateur ne spécifie pas explicitement un domaine, Active Directory rootDSE spécifie l'emplacement du service de mappage de certificat. Il est situé sur une machine de catalogue global et bénéficie d'une vue en cache de tous les attributs x509certificate de la forêt. Cet ordinateur peut être utilisé pour rechercher efficacement un compte utilisateur dans tout domaine, en se basant uniquement sur le certificat.

Sélection du contrôleur de domaine d'ouverture de session

Lorsqu'un environnement contient plusieurs contrôleurs de domaine, il est utile de voir et de restreindre le contrôleur de domaine qui est utilisé pour l'authentification, de façon à ce que les journaux puissent être activés et récupérés.

Contrôler la sélection du contrôleur de domaine

Pour forcer Windows à utiliser un contrôleur de domaine Windows spécifique pour l'ouverture de session, vous pouvez explicitement définir la liste des contrôleurs de domaine qu'une machine Windows utilise en configurant le fichier lmhosts : \Windows\System32\drivers\etc\lmhosts.

Il existe généralement un exemple de fichier nommé « lmhosts.sam » dans cet emplacement. Il vous suffit d'inclure une ligne :

1.2.3.4 dcnetbiosname #PRE #DOM:mondomaine

Où « 1.2.3.4 » est l'adresse IP du contrôleur de domaine nommé « dcnetbiosname » dans le domaine « mondomaine ».

Après un redémarrage, la machine Windows utilise ces informations pour ouvrir une session sur mon-domaine. Cette configuration doit être rétablie lors d'un débogage.

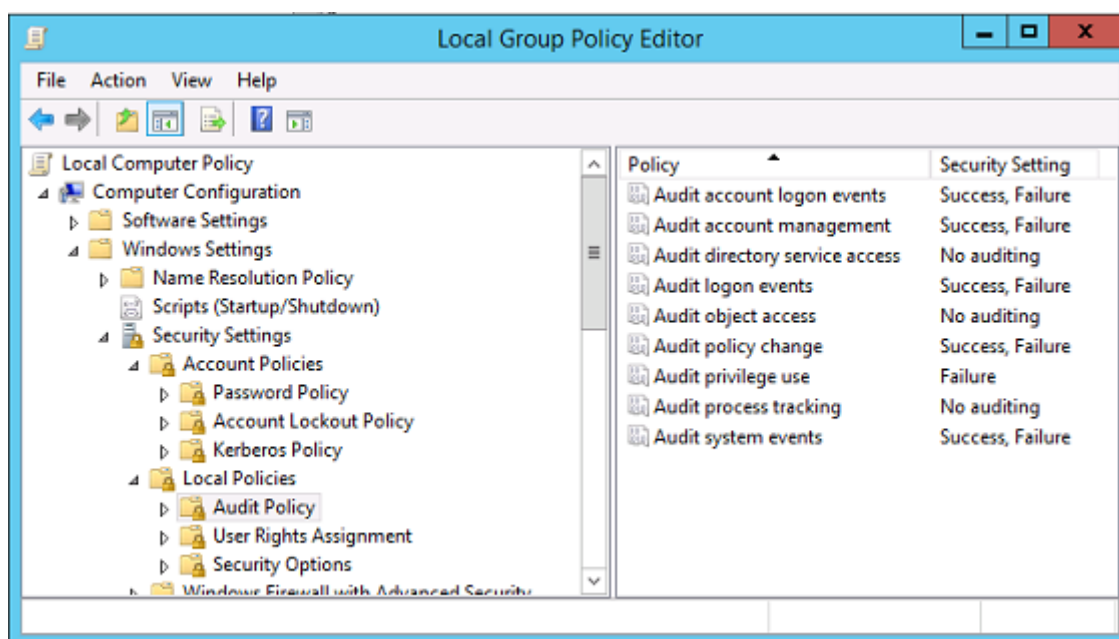
Identifier le contrôleur de domaine utilisé

À l'ouverture de session, Windows définit une variable d'environnement MSDOS avec le contrôleur de domaine qui a ouvert la session de l'utilisateur. Pour la voir, démarrez l'invite de commande avec la commande : **echo %LOGONSERVER%**.

Les journaux liés à l'authentification sont stockés sur l'ordinateur renvoyé par cette commande.

Activer les événements d'audit de compte

Par défaut, les contrôleurs de domaine Windows n'activent pas les journaux d'audit de compte complets. Ce réglage peut être contrôlé par le biais des stratégies d'audit dans les paramètres de sécurité dans l'éditeur de stratégie de groupe. Pour ouvrir l'éditeur de stratégie de groupe, exécutez `gpedit.msc` sur le contrôleur de domaine. Une fois les stratégies d'audit activées, le contrôleur de domaine génère des informations supplémentaires dans le journal de sécurité.



Journaux de validation de certificat

Vérifier la validité du certificat

Si un certificat de carte à puce est exporté en tant que certificat DER (sans clé privée), vous pouvez le valider avec la commande : `certutil -verify user.cer`

Activer la journalisation CAPI

Sur le contrôleur de domaine et les machines utilisateur, ouvrez l'observateur d'événements et activez la journalisation pour Microsoft/Windows/CAPI2/Operational Logs.

Sur le contrôleur de domaine et la machine VDA, ouvrez l'observateur d'événements et accédez à **Journaux des applications et des services > Microsoft > Windows > CAPI2 > Opérationnel**. Cliquez avec le bouton droit sur **Opérationnel** et sélectionnez **Activer le journal**.

En outre, affinez la journalisation CAPI à l'aide des valeurs de registre suivantes : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CAPI2\Operational`. Les valeurs suivantes n'existent pas par défaut, vous devez les créer. Supprimez les valeurs si vous souhaitez revenir aux paramètres de journalisation CAPI2 par défaut.

| Valeur | Description |
|-----------------------------|--|
| DiagLevel (DWORD) | Niveau de détail (0 à 5) |
| DiagMatchAnyMask (QUADWORD) | Filtre d'événements (utiliser 0xffffffff pour tout) |
| DiagProcessName (MULTI_SZ) | Filtre par nom du processus (par exemple, LSASS.exe) |

Journaux CAPI

| Message | Description |
|---------------------|---|
| Build Chain | CertGetCertificateChain appelé par LSA (comprend résultat) |
| Verify Revocation | CertVerifyRevocation appelé par LSA (comprend résultat) |
| X509 Objects | En mode détaillé, les certificats et les listes de révocation de certificats (CRL) sont placés dans <code>AppData\LocalLow\Microsoft\X509Objects</code> |
| Verify Chain Policy | CertVerifyChainPolicy appelé par LSA (comprend paramètres) |

Messages d'erreur

| Code d'erreur | Description |
|--|---|
| Certificat non approuvé | Le certificat de carte à puce n'a pas pu être créé à l'aide de certificats contenus dans les magasins de certificats racine approuvés et intermédiaires de l'ordinateur. |
| Erreur de vérification de la révocation de certificats | La liste de révocation de certificats pour la carte à puce n'a pas pu être téléchargée à partir de l'adresse spécifiée par le point de distribution de la liste de révocation de certificat. Si la vérification de la révocation des certificats est obligatoire, l'ouverture de session échoue. Consultez la section Certificats et infrastructure de clé publique . |
| Erreurs d'utilisation de certificat | Le certificat n'est pas approprié pour l'ouverture de session. Par exemple, il peut s'agir d'un certificat de serveur ou d'un certificat de signature. |

Journaux Kerberos

Pour activer la journalisation Kerberos, sur le contrôleur de domaine et la machine utilisateur, créez les valeurs de registre suivantes :

| Ruche | Nom de la valeur | Valeur [DWORD] |
|---|------------------|----------------|
| CurrentControlSet\Control\Lsa\Kerberos\Parameters | KrbtgtLevel | 0x1 |
| CurrentControlSet\Control\Lsa\Kerberos\Parameters | KrbtgtDebugLevel | 0xffffffff |
| CurrentControlSet\Services\Kdc | KdcDebugLevel | 0x1 |
| CurrentControlSet\Services\Kdc | KdcExtraLogLevel | 0x1f |

La journalisation Kerberos est écrite dans le journal d'événements système.

- Les messages tels que « certificat non approuvé » (untrusted certificate) devraient être faciles à diagnostiquer.
- Deux codes d'erreur sont des messages d'informations et peuvent être ignorés :

- KDC_ERR_PREAUTH_REQUIRED (utilisé pour la rétrocompatibilité avec les contrôleurs de domaine plus anciens)
- Erreur inconnue 0x4b

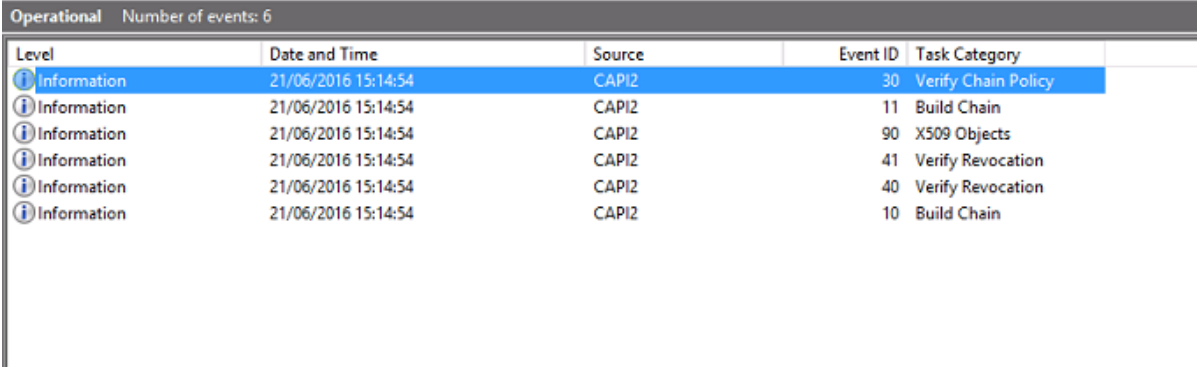
Journaux du contrôleur de domaine et de la station de travail

Cette section décrit les entrées de journal attendues sur le contrôleur de domaine et la station de travail lorsque l'utilisateur ouvre une session avec un certificat.

- Journal CAPI2 du contrôleur de domaine
- Journaux de sécurité du contrôleur de domaine
- Journal de sécurité Virtual Delivery Agent (VDA)
- Journal CAPI VDA
- Journal système VDA

Journal CAPI2 du contrôleur de domaine

Lors d'une ouverture de session, le contrôleur de domaine valide le certificat de l'appelant, produisant une séquence d'entrées de journal comme illustré ci-dessous.



| Level | Date and Time | Source | Event ID | Task Category |
|-------------|---------------------|--------|----------|---------------------|
| Information | 21/06/2016 15:14:54 | CAPI2 | 30 | Verify Chain Policy |
| Information | 21/06/2016 15:14:54 | CAPI2 | 11 | Build Chain |
| Information | 21/06/2016 15:14:54 | CAPI2 | 90 | X509 Objects |
| Information | 21/06/2016 15:14:54 | CAPI2 | 41 | Verify Revocation |
| Information | 21/06/2016 15:14:54 | CAPI2 | 40 | Verify Revocation |
| Information | 21/06/2016 15:14:54 | CAPI2 | 10 | Build Chain |

Le dernier message du journal d'événements indique que lsass.exe sur le contrôleur de domaine construit une chaîne en fonction du certificat fourni par le VDA et vérifie sa validité (y compris la révocation). Le résultat est « ERROR_SUCCESS ».

- **CertVerifyCertificateChainPolicy**
 - **Policy**
 - [type] CERT_CHAIN_POLICY_NT_AUTH
 - [constant] 6
 - **Certificate**
 - [fileRef] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
 - [subjectName] fred
 - **CertificateChain**
 - [chainRef] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
 - **Flags**
 - [value] 0
 - **Status**
 - [chainIndex] -1
 - [elementIndex] -1
 - **EventAuxInfo**
 - [ProcessName] lsass.exe
 - **CorrelationAuxInfo**
 - [TaskId] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
 - [SeqNumber] 1
 - **Result**
 - [value] 0
-

Journal de sécurité du contrôleur de domaine

Le contrôleur de domaine présente une séquence des événements d'ouverture de session, l'événement clé étant 4768, dans lequel le certificat est utilisé pour émettre le ticket Kerberos Ticket Granting (krbtgt).

Les messages précédents indiquent que le compte de machine du serveur s'authentifie auprès du contrôleur de domaine. Les messages suivants indiquent le compte d'utilisateur appartenant au nouveau krbtgt utilisé pour s'authentifier auprès du contrôleur de domaine.

| Keywords | Date and Time | Source | Event ID | Task Category |
|---------------|---------------------|-------------------|----------|------------------------------------|
| Audit Success | 21/06/2016 15:14:56 | Security-Auditing | 4624 | Logon |
| Audit Success | 21/06/2016 15:14:56 | Security-Auditing | 4624 | Logon |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4769 | Kerberos Service Ticket Operations |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4768 | Kerberos Authentication Service |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4769 | Kerberos Service Ticket Operations |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4634 | Logoff |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4624 | Logon |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4624 | Logon |

Event 4768, Security-Auditing

General Details

Friendly View XML View

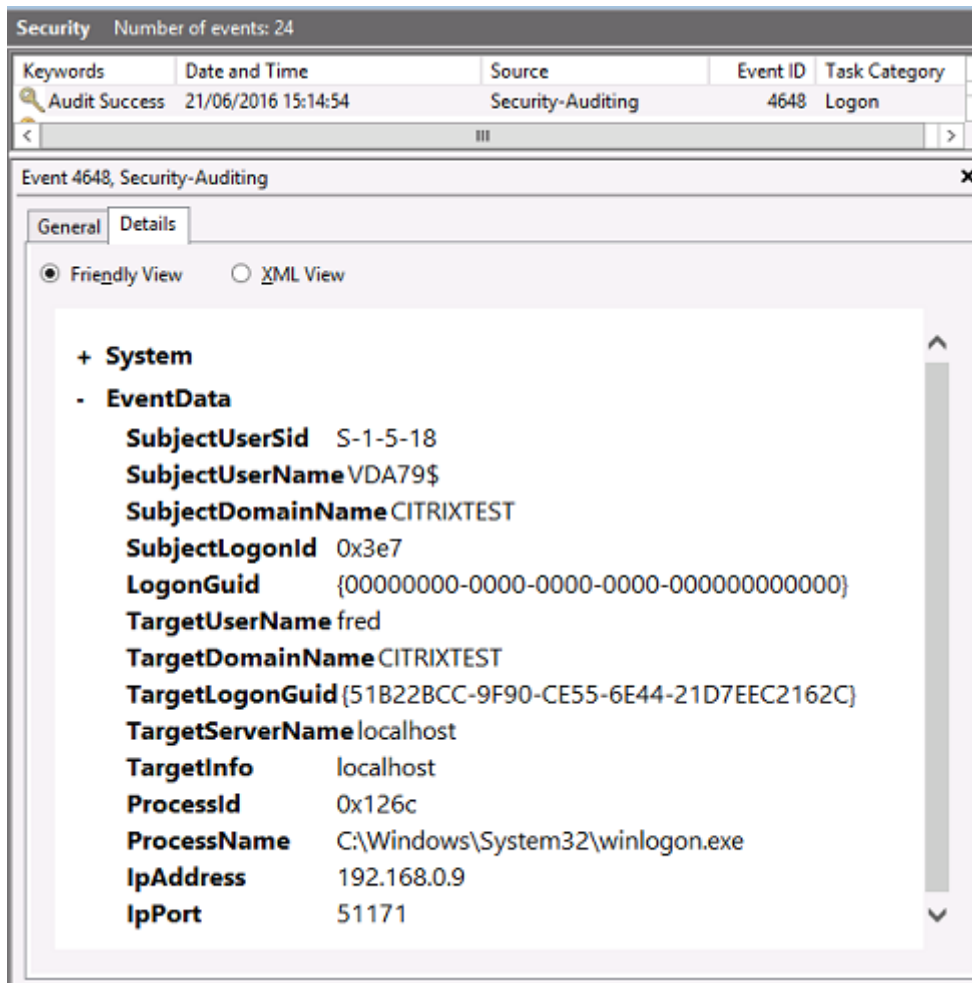
+ System

- EventData

- TargetUserName fred
- TargetDomainName CITRIXTEST.NET
- TargetSid S-1-5-21-390731715-1143989709-1377117006-1106
- ServiceName krbtgt
- ServiceSid S-1-5-21-390731715-1143989709-1377117006-502
- TicketOptions 0x40810010
- Status 0x0
- TicketEncryptionType 0x12
- PreAuthType 16
- IpAddress ::ffff:192.168.0.10
- IpPort 49348
- CertIssuerName citrixtest-DC-CA
- CertSerialNumber 5F0001D1FCA2AC30F36879CEEC00000001D1FC
- CertThumbprint 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

Journal de sécurité VDA

Les journaux d'audit de sécurité VDA correspondant à l'événement d'ouverture de session sont l'entrée avec l'ID 4648, provenant de winlogon.exe.



Journal CAPI VDA

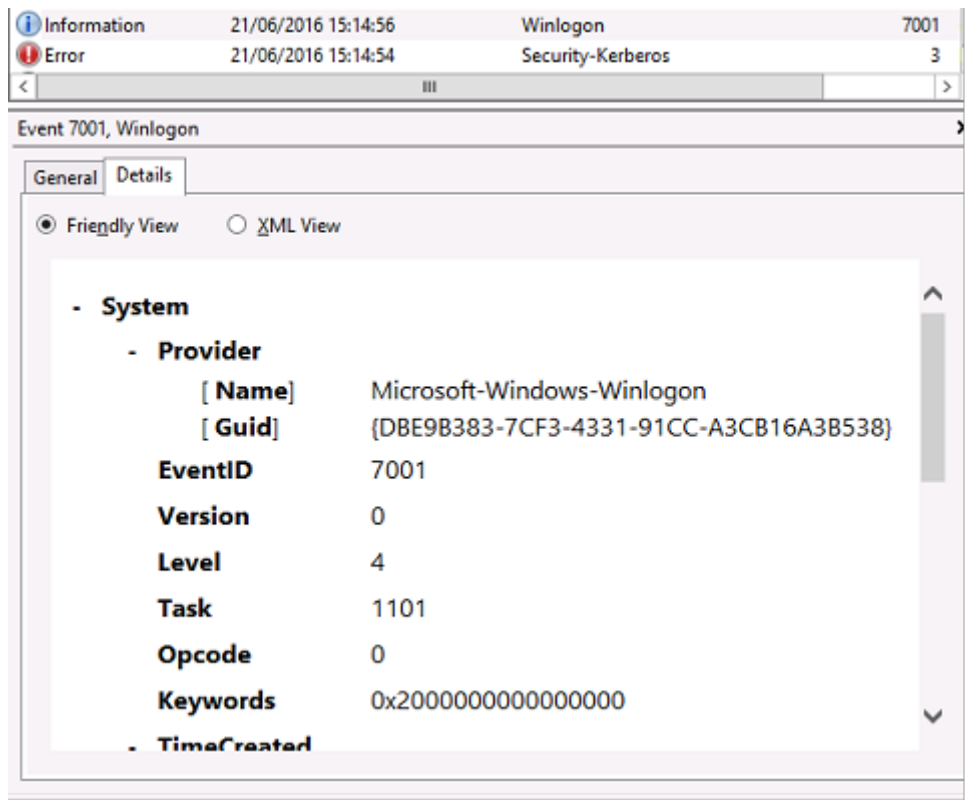
Cet exemple de journal CAPI VDA présente une séquence de création de chaîne et de vérification depuis lsass.exe, validant le certificat du contrôleur de domaine (dc.citrixtest.net).

| | | | | | |
|--|-------------|---------------------|-------|----|-------------------|
| | Information | 21/06/2016 15:14:54 | CAPI2 | 30 | Verify Chain P... |
| | Information | 21/06/2016 15:14:54 | CAPI2 | 11 | Build Chain |
| | Information | 21/06/2016 15:14:54 | CAPI2 | 90 | X509 Objects |
| | Information | 21/06/2016 15:14:54 | CAPI2 | 41 | Verify Revocat... |
| | Information | 21/06/2016 15:14:54 | CAPI2 | 40 | Verify Revocat... |
| | Information | 21/06/2016 15:14:54 | CAPI2 | 10 | Build Chain |

```
- UserData
  - CertVerifyCertificateChainPolicy
    - Policy
      [ type]      CERT_CHAIN_POLICY_NT_AUTH
      [ constant] 6
    - Certificate
      [ fileRef]   813C6D12E1E1800E61B8DB071E186EB912B7
      [ subjectName] dc.citrixtest.net
    - CertificateChain
      [ chainRef]  {84E0B3D1-A4D4-4AC7-BA99-5291415B343}
    - Flags
      [ value]     0
    - Status
      [ chainIndex] -1
```

Journal système VDA

Lorsque l'ouverture de session Kerberos est activée, le journal système affiche l'erreur KDC_ERR_PREAUTH_REQUIRED (qui peut être ignorée) et une entrée de Winlogon, indiquant que l'ouverture de session Kerberos a réussi.



Surveillance de FAS à l'aide du journal des événements Windows

Tous les événements de FAS sont consignés dans le journal des événements de l'application Windows. Vous pouvez utiliser des produits tels que System Center Operations Manager (SCOM) pour surveiller l'intégrité de votre service FAS à l'aide des processus et des événements décrits ici.

Le service FAS est-il en cours d'exécution ?

Pour déterminer si le service FAS est en cours d'exécution, surveillez le processus Citrix.Authentication.FederatedA

Seuls les événements les plus importants liés à la surveillance du service FAS sont décrits dans cette section. Pour obtenir la liste complète des codes d'événement de FAS, reportez-vous à la section [Journaux des événements de FAS](#).

Événements d'intégrité de FAS

Les événements suivants indiquent si votre service FAS fonctionne correctement.

Source de l'événement : **Citrix.Authentication.FederatedAuthenticationService**.

| Événement | Texte de l'événement | Explication | Remarques |
|-----------|---|---|---|
| [S003] | Administrator [{0}] setting Maintenance Mode to [{1}] | Le service FAS a été placé en mode de maintenance ou retiré de celui-ci. | En mode de maintenance, le serveur FAS n'est pas utilisable pour l' authentification unique. |
| [S022] | Administrator [{0}] setting Maintenance Mode to Off | Le service FAS a été retiré du mode de maintenance. | Disponible à partir de FAS 10.7/Citrix Virtual Apps and Desktops 2109. |
| [S023] | Administrator [{0}] setting Maintenance Mode to On | Le service FAS a été placé en mode de maintenance. | Disponible à partir de FAS 10.7/Citrix Virtual Apps and Desktops 2109. |

| Événement | Texte de l'événement | Explication | Remarques |
|-----------|---|--|--|
| [S123] | Failed to issue a certificate for [upn: {0} role: {1}] [exception: {2}] | Cet événement se produit après [S124] si aucune des autorités de certification de FAS n'est configurée avec un certificat utilisateur émis avec succès. L'authentification unique échouera pour cet utilisateur. | Cet événement indique qu'aucune des autorités de certification configurées ne fonctionne. Si FAS est configuré pour utiliser un HSM, cela peut également indiquer que le HSM ne fonctionne pas. |
| [S124] | Failed to issue a certificate for [upn: {0} role: {1}] at [certificate authority: {2}] [exception: {3}] | Un échec s'est produit lorsque FAS a tenté de demander un certificat utilisateur auprès de l'autorité de certification donnée. Si FAS est configuré avec plus d'une autorité de certification, FAS effectue une nouvelle demande auprès d'une autre autorité de certification. | Cet événement peut indiquer que l'autorité de certification ne fonctionne pas ou n'est pas joignable. Si FAS est configuré pour utiliser un HSM, cela peut également indiquer que le HSM ne fonctionne pas. L'exception peut être utilisée pour identifier la cause du problème. |

| Événement | Texte de l'événement | Explication | Remarques |
|-----------|--|---|--|
| [S413] | Authorization certificate expiring soon ({0} days left). Certificate details: {1} | Cet événement est généré périodiquement lorsque le certificat d'autorisation de FAS est sur le point d'expirer. Par défaut, l'événement est généré tous les jours si le certificat d'autorisation entre dans les 30 jours suivant l'expiration. | Les paramètres par défaut peuvent être ajustés à l'aide de l'applet de commande Set-FasRaCertificateMonitor ; voir Applets de commande PowerShell . |
| [S414] | Authorization certificate has expired. Certificate details: {0} | Cet événement est généré périodiquement lorsque le certificat d'autorisation de FAS a expiré. Par défaut, l'événement est généré tous les jours. | Une fois expiré, FAS ne peut pas générer de nouveaux certificats utilisateur et l'authentification unique commence à échouer. |

Événements FAS connectés au cloud

Si vous utilisez FAS avec Citrix Cloud, les événements suivants indiquent si votre service FAS fonctionne correctement.

La source de l'événement est **Citrix.Fas.Cloud**.

| Événement | Texte de l'événement | Explication | Remarques |
|-----------|---|---|--|
| [S012] | The FAS service is available for single sign-on from Citrix Cloud | Cet événement indique que l'authentification unique devrait fonctionner depuis Workspace (c'est-à-dire Citrix Cloud). | Avant d'émettre cet événement, FAS vérifie (1) qu'il est configuré, (2) qu'il n'est pas en mode de maintenance et (3) qu'il est connecté à Citrix Cloud. |
| [S013] | The FAS service is not available for single sign-on from Citrix Cloud. [0] Further details can be found in the admin console. | Cet événement indique que FAS n'est pas en mesure de fournir l'authentification unique à partir de Workspace (c'est-à-dire Citrix Cloud). Le message indique la raison pour laquelle l'authentification unique ne fonctionne pas. | FAS maintient une connexion permanente à Citrix Cloud. De temps en temps, cette connexion peut prendre fin pour diverses raisons (par exemple, un problème réseau ou une stratégie de durée de vie de connexion sur un serveur proxy). Lorsque cela se produit, le texte de l'événement contient « Service is not connected to the cloud ». Ce comportement est normal et FAS tente immédiatement de rétablir une connexion à Citrix Cloud. |

Événements de sécurité

Les événements suivants indiquent qu'une entité non autorisée a tenté d'utiliser FAS.

Source de l'événement : **Citrix.Authentication.FederatedAuthenticationService.**

| Événement | Texte de l'événement | Explication |
|-----------|--|--|
| [S001] | ACCESS DENIED: User [{0}] is not a member of the Administrators group | Une tentative d'affichage ou de modification de la configuration de FAS a été effectuée, mais l'appelant n'était pas un administrateur FAS. |
| [S002] | ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}] | Une tentative d'affichage ou de modification de la configuration d'une règle de FAS a été effectuée, mais l'appelant n'était pas un administrateur FAS. |
| [S101] | Server [{0}] is not authorized to assert identities in role [{1}] | Une tentative a été faite pour affirmer l'identité des utilisateurs, mais l'appelant n'est pas autorisé à effectuer une telle opération. Seuls les serveurs StoreFront qui y ont été autorisés dans la configuration de la règle FAS (et Workspace le cas échéant) peuvent affirmer des identités utilisateur. |
| [S104] | Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}]) | Une tentative a été faite pour affirmer l'identité d'un utilisateur, mais le compte de l'utilisateur n'y est pas autorisé conformément à la configuration de la règle FAS. |
| [S205] | Relying party access denied - the calling account [{0}] is not a permitted relying party of the rule [{1}] | Un VDA a tenté d'effectuer une authentification unique avec FAS, mais le VDA n'y est pas autorisé conformément à la configuration de la règle FAS. |

Journaux d'événements de FAS

Les tableaux suivants répertorient les entrées de journal d'événements générées par FAS.

Événements d'administration du [Service d'authentification fédérée]

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont consignés en réponse à une modification de la configuration du serveur FAS.

Codes de journal

[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group

[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]

[S003] Administrator [{0}] setting Maintenance Mode to [{1}]

[S004] Administrator [{0}] requesting authorization certificate from CA [{1}] using templates [{2}] and {3}]

[S005] Administrator [{0}] de-authorizing CA [{1}]

[S006] Administrator [{0}] creating Certificate Definition [{1}]

[S007] Administrator [{0}] updating Certificate Definition [{1}]

[S008] Administrator [{0}] deleting Certificate Definition [{1}]

[S009] Administrator [{0}] creating Rule [{1}]

[S010] Administrator [{0}] updating Rule [{1}]

[S011] Administrator [{0}] deleting Rule [{1}]

[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} rule: {3}]Certificate Definition: {4} Security Context: {5}]

[S013] Administrator [{0}] deleting certificates [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]

[S015] Administrator [{0}] creating certificate request [TPM: {1}]

[S016] Administrator [{0}] importing Authorization certificate [Reference: {1}]

[S022] Administrator [{0}] setting Maintenance Mode to Off

[S023] Administrator [{0}] setting Maintenance Mode to On

[S024] Administrator [{0}] setting system health monitor

[S025] Administrator [{0}] setting system health monitor

[S026] Administrator [{0}] setting RA Certificate Monitor

Codes de journal

[S027] Administrator [{0}] resetting RA certificate monitor

[S050] Administrator [{0}] creating cloud configuration: [{1}]

[S051] Administrator [{0}] updating cloud configuration: [{1}]

[S052] Administrator [{0}] removing cloud configuration

[S060] Administrator [{0}] Requesting Cloud Registration. Instance: {1}

[S060] Administrator [{0}] Requesting Direct Trust Cloud Registration. Instance: {1}
CloudServiceUrlFormat: {2}

[S061] Administrator [{0}] Completing Cloud Registration. Resource location: {1}, Rule name: {2}

[S062] Administrator [{0}] Completed Cloud Registration. Resource location: {1} ({2}), Rule name: {3},
Customer: {4} ({5})

[S063] A KRS error occurred during cloud registration. The exception was {0}

[S064] An unknown error occurred during cloud registration. The exception was {0}

Codes de journal

[S401] Performing configuration upgrade - [From version {0} to version {1}]

[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service
[currently running as: {0}]

[S404] Forcefully erasing the Citrix Federated Authentication Service database

[S405] An error occurred while migrating data from the registry to the database: [{0}]

[S406] Migration of data from registry to database is complete (note: user certificates are not
migrated)

[S407] Registry-based data was not migrated to a database since a database already existed

[S408] Cannot downgrade the configuration –[From version {0} to version {1}]

[S409] ThreadPool configuration succeeded - MinThreads adjusted from [workers: {0} completion:
{1}] to: [workers: {2} completion: {3}]

[S410] ThreadPool configuration failed - failed to adjust MinThreads from [workers: {0} completion:
{1}] to: [workers: {2} completion: {3}]; this may impact the scalability of the FAS server

[S411] Error starting the FAS service: [{0}]

[S412] Configuration upgrade complete –[From version {0} to version {1}]

[S413] Authorization certificate expiring soon ({0} days left). Certificate details: {1}

[S414] Authorization certificate has expired. Certificate details: {0}

Codes de journal

[S415] Authorization certificate checks completed. {0} issues were logged. Le prochain chèque est dû dans {1}

Création d'assertions d'identité [Service d'authentification fédérée]

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont journalisés au moment de l'exécution sur le serveur FAS lorsqu'un serveur approuvé assume l'ouverture de session d'un utilisateur.

Codes de journal

[S101] Server [{0}] is not authorized to assert identities in role [{1}]

[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})

[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}

[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])

[S105] Server [{0}] issued identity assertion [upn: {1}, role {2}, Security Context: [{3}]]

[S120] Issuing certificate to [upn: {0} role: {1}] Security Context: [{2}]]

[S121] Certificate issued to [upn: {0} role: {1}] by [certificate authority: {2}]

[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].

[S123] Failed to issue a certificate for [upn: {0} role: {1}] [exception: {2}]

[S124] Failed to issue a certificate for [upn: {0} role: {1}] at [certificate authority: {2}] [exception: {3}]

Agissant en tant que partie de confiance [Service d'authentification fédérée]

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont journalisés au moment de l'exécution sur le serveur FAS lorsqu'un VDA connecte un utilisateur.

Codes de journal

[S201] Relying party [{0}] does not have access to a password.

[S202] Relying party [{0}] does not have access to a certificate.

Codes de journal

[S203] Relying party [{0}] does not have access to the Logon CSP

[S204] Relying party [{0}] accessing the Logon CSP for [upn: {1}] in role: [{2}] [Operation: {3}] as authorized by [{4}]

[S205] Relying party access denied - the calling account [{0}] is not a permitted relying party of the rule [{1}]

[S206] Calling account [{0}] is not a relying party

[S208] Private Key operation failed [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].

Serveur de certificats dans la session [Service d'authentification fédérée]

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont journalisés sur le serveur FAS lorsqu'un utilisateur utilise un certificat dans la session.

Codes de journal

[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card

[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]

[S303] Access Denied: User [{0}] does not match Virtual Smart Card [upn: {1}]

[S304] User [{0}] running program [{1}] on computer [{2}] using Virtual Smart Card [upn: {3} role: {4} thumbprint: {5}] for private key operation [{6}]

[S305] Private Key operation failed [Operation: {0}] [upn: {1} role: {2} containerName {3} Error {4} {5}].

Plugin d'assertion FAS [Service d'authentification fédérée]

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont enregistrés par le plug-in d'assertion FAS.

Codes de journal

[S500] No FAS assertion plug-in is configured

[S501] The configured FAS assertion plug-in could not be loaded [exception:{0}]

Codes de journal

[S502] FAS assertion plug-in loaded [pluginId={0}] [assembly={1}] [location={2}]

[S503] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but the plug-in [{2}] does not support it)

[S504] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but there is no configured FAS plug-in)

[S505] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] rejected the logon evidence with status [{3}] and message [{4}])

[S506] The plug-in [{0}] accepted logon evidence from server [{1}] for UPN [{2}] with message [{3}]

[S507] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] threw exception [{3}] during method [{4}])

[S507] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] threw exception [{3}])

[S508] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but the plug-in [{2}] does not support it)

[S509] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but there is no configured FAS plugin)

[S510] Server [{0}] failed to assert UPN [{1}] (the access disposition was considered invalid by plug-in [{2}])

FAS activé pour Workspace [Service d'authentification fédérée]

[Source de l'événement : Citrix.Fas.Cloud]

Ces événements sont consignés lorsque FAS est utilisé avec Workspace.

Codes de journal

[S001] Rotated Citrix Cloud authorization key [fas id: {0}] [old key id:{1}] [new key id:{2}]

[S002] The cloud support module is starting. FasHub cloud service URL: {0}

[S003] FAS registered with the cloud [fas id: {0}] [transaction id: {1}]

[S004] FAS failed to register with the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S005] FAS sent its current configuration to the cloud [fas id: {0}] [transaction id: {1}]

[S006] FAS failed to send its current configuration to the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S007] FAS unregistered from the cloud [fas id: {0}] [transaction id: {1}]

[S009] FAS failed to unregister from the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]

Codes de journal

- [S010] The FAS service is connected to the cloud messaging URL: {0}
 - [S011] The FAS service is not connected to the cloud
 - [S012] The FAS service is available for single sign-on from Citrix Cloud
 - [S013] The FAS service is not available for single sign-on from Citrix Cloud. [{0}] Further details can be found in the admin console
 - [S014] A call to the cloud service <service name> failed [fas id: {0}] [transaction id: {1}]
[exception: {2}]
 - [S015] A message from Citrix Cloud was blocked because the caller is not permitted [message ID {0}]
[transaction ID {1}] [caller {2}]
 - [S016] A call to the cloud service <service name> succeeded [fas id: {0}] [transaction id: {1}]
 - [S019] FAS downloaded its configuration from the cloud [fas id: {0}] [transaction id: {1}]
 - [S020] FAS failed to download its configuration from the cloud [fas id: {0}] [transaction id: {1}]
[exception: {2}]
 - [S021] The cloud support module failed to start. Exception: {0}
 - [S022] The cloud support module is stopping
 - [S023] Failed to rotate Citrix Cloud authorization key [fas id: {0}] [current key id:{1}] [new key id:{2}]
[keys in cloud:{3}]
 - [S024] Initiating rotation of Citrix Cloud authorization key [fas id: {0}] [current key id:{1}] [new key id:{2}]
 - [S025] This service's authorization key is present in the Citrix Cloud [current key: {0}] [keys in cloud: {1}]
 - [S026] This service's authorization key is not present in the Citrix Cloud [current key: {0}] [keys in cloud: {1}]
 - [S027] Upgraded the Citrix Cloud authorization key storage format [fas id: {0}]
-

Ouverture de session [VDA]

[Source de l'événement : Citrix.Authentication.IdentityAssertion]

Ces événements sont journalisés sur le VDA durant la phase d'ouverture de session.

Codes de journal

- [S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
- [S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]

Codes de journal

[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}

[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0}
[Error: {1} {2}]

[S105] Identity Assertion Logon. Logging in [Username: {0} Domain: {1}]

[S106] Identity Assertion Logon.\n\nFederated Authentication Service: {0}\n\nLogging in [Certificate:
{1}]

[S107] Identity Assertion Logon failed. [Exception: {0}{1}]

[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

Certificats dans la session [VDA]

[Source de l'événement : Citrix.Authentication.IdentityAssertion]

Ces événements sont journalisés sur le VDA lorsqu'un utilisateur tente d'utiliser un certificat dans la session.

Codes de journal

[S201] Virtual smart card access authorized by [{0}] for [PID: {1} Program Name: {2}]Certificate
thumbprint: {3}]

[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}]

[S204] Virtual Smart Card Subsystem. Smart card support disabled

Demande de certificat et génération de paires de clés [Service d'authentification fédérée]

[Source de l'événement : Citrix.Fas.PkiCore]

Ces événements sont journalisés lorsque le serveur FAS effectue des opérations cryptographiques de bas niveau.

Codes de journal

[S001] TrustArea::TrustArea: Installed certificate [TrustArea: {0} Certificate
{1}TrustAreaJoinParameters {2}]

[S014] Pkcs10Request::Create: Created PKCS10 request [Distinguished Name {0}]

Codes de journal

[S016] PrivateKey::Create [Identifiant {0}MachineWide: {1} Provider: {2} ProviderType: {3} EllipticCurve: {4} KeyLength: {5} isExportable: {6}]
[S017] PrivateKey::Delete [CspName: {0}, Identifiant {1}]

Codes de journal

[S104] MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest Error submit response [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest Issued certificate [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

Messages d'erreur de l'utilisateur final

Cette section dresse la liste des messages d'erreur courants s'affichant sur la page d'ouverture de session Windows.

| Message d'erreur affiché | Description et référence |
|---|---|
| Nom d'utilisateur ou mot de passe non valide | L'ordinateur détecte que vous disposez d'un certificat et d'une clé privée valides, mais le contrôleur de domaine Kerberos a rejeté la connexion. Consultez la section Journaux Kerberos de cet article. |
| Le système n'a pas pu vous connecter. Impossible de vérifier les informations d'identification. / La requête n'est pas prise en charge. | Le Contrôleur de domaine ne peut pas être contacté ou le Contrôleur de domaine n'a pas été configuré avec un certificat prenant en charge l'authentification par carte à puce. Inscrivez les certificats de contrôleur de domaine pour « Authentification Kerberos », « Authentification du contrôleur de domaine » ou « Contrôleur de domaine ». Cette réinscription est recommandée, même lorsque le certificat existant semble valide. |

| Message d'erreur affiché | Description et référence |
|--|---|
| Il se peut que le système ne vous connecte pas. Le certificat de carte à puce utilisé pour l'authentification n'est pas approuvé. Demande incorrecte | Les certificats racine et intermédiaire ne sont pas installés sur l'ordinateur local. Consultez Certificats et infrastructure de clé publique . Ceci indique habituellement que les extensions sur le certificat ne sont pas définies correctement, ou que la clé RSA est trop courte (<2 048 bits). |

Informations connexes

- [Configuration d'un domaine pour ouverture de session par carte à puce](#)
- [\(Stratégies d'ouverture de session par carte à puce](#)
- [Activation de l'ouverture de session CAPI](#)
- [Activation de l'ouverture de session Kerberos](#)
- [Instructions pour activer l'ouverture de session par carte à puce avec des autorités de certification tierces](#)

Applets de commande PowerShell

June 5, 2024

Vous pouvez utiliser la console d'administration FAS (Service d'authentification fédérée) pour les déploiements simples ; toutefois l'interface PowerShell offre des options plus avancées. Si vous prévoyez d'utiliser des options qui ne sont pas disponibles dans la console, Citrix recommande d'utiliser uniquement PowerShell pour la configuration.

La commande suivante ajoute les applets de commande PowerShell FAS :

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Dans une fenêtre PowerShell, vous pouvez utiliser `Get-Help <nom cmdlet>` pour afficher l'aide de l'applet de commande.

Pour plus d'informations sur les applets de commande FAS PowerShell SDK, consultez <https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>.

Architectures de déploiement

June 5, 2024

Introduction

Le Service d'authentification fédérée (FAS) est un composant Citrix qui s'intègre avec votre autorité de certification Active Directory, qui permet aux utilisateurs d'être authentifiés dans un environnement Citrix. Ce document présente les différentes architectures d'authentification susceptibles d'être appropriées à votre déploiement.

Lorsqu'il est activé, FAS délègue l'authentification utilisateur aux serveurs StoreFront approuvés. StoreFront est doté d'un ensemble complet d'options d'authentification articulées autour de technologies Web modernes. En outre, il peut être étendu facilement grâce au SDK StoreFront ou à des plug-ins IIS tiers. L'objectif de base est que toute technologie d'authentification qui peut authentifier un utilisateur sur un site Web peut maintenant être utilisée pour la connexion à un déploiement Citrix Virtual Apps ou Citrix Virtual Desktops.

Ce document décrit certaines architectures de déploiement de haut niveau, par complexité croissante.

- [Déploiement interne](#)
- [Déploiement Citrix Gateway](#)
- [ADFS SAML](#)
- [Mappage de compte B2B](#)
- [Jonction à un domaine Azure AD \(Azure AD Join\) avec Windows 10](#)

Des liens vers les articles FAS sont fournis. Pour toutes les architectures, l'article [Installer et configurer](#) est le document de référence principal pour la configuration de FAS.

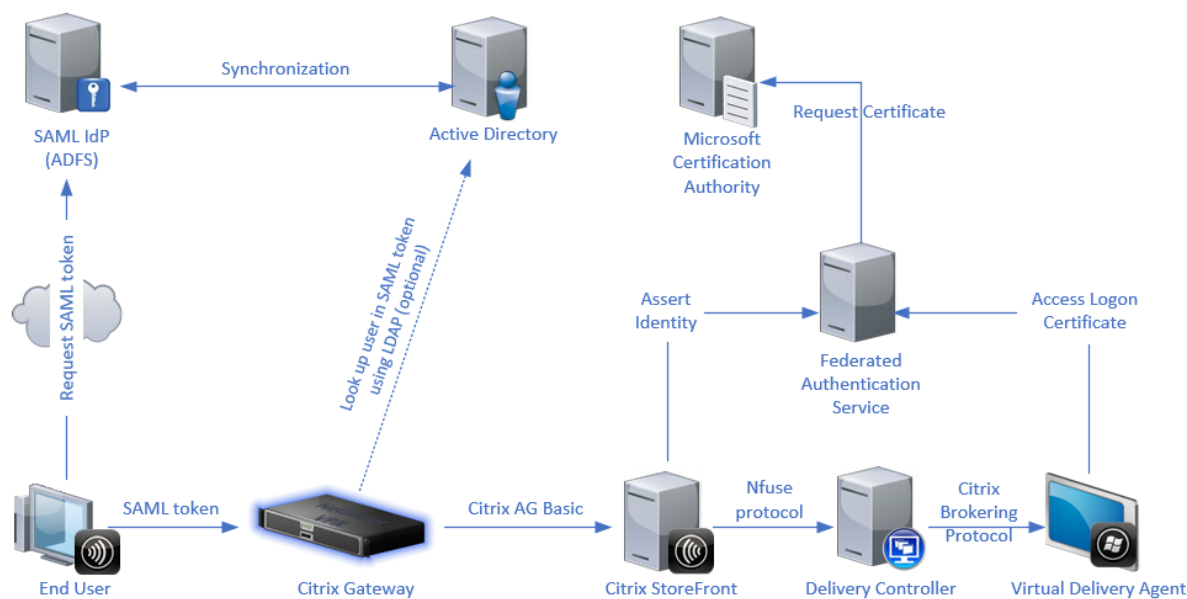
Aperçu de l'architecture

FAS est autorisé à émettre des certificats de classe de carte à puce automatiquement à la place des utilisateurs Active Directory qui sont authentifiés par StoreFront. Il utilise des API similaires aux outils qui permettent aux administrateurs de provisionner des cartes à puce physiques. Lorsqu'un utilisateur est connecté à un VDA Citrix Virtual Apps ou Citrix Virtual Desktops, le certificat est attaché à la machine, et le domaine Windows interprète l'ouverture de session en tant qu'authentification par carte à puce standard.

Les serveurs StoreFront de confiance contactent FAS lorsque les utilisateurs demandent accès à l'environnement Citrix. FAS accorde un ticket qui permet à une seule session Citrix Virtual Apps ou Citrix

Virtual Desktops de s'authentifier avec un certificat pour cette session. Lorsqu'un VDA doit authentifier un utilisateur, il se connecte à FAS utilise le ticket. Seul FAS a accès à la clé privée du certificat de l'utilisateur ; le VDA doit envoyer à FAS chaque opération de signature et de décryptage qu'il doit effectuer avec le certificat.

Le diagramme suivant illustre l'intégration de FAS avec une autorité de certification Microsoft, ainsi que la fourniture de services de support à StoreFront et aux VDA Citrix Virtual Apps and Desktops.



Déploiement interne

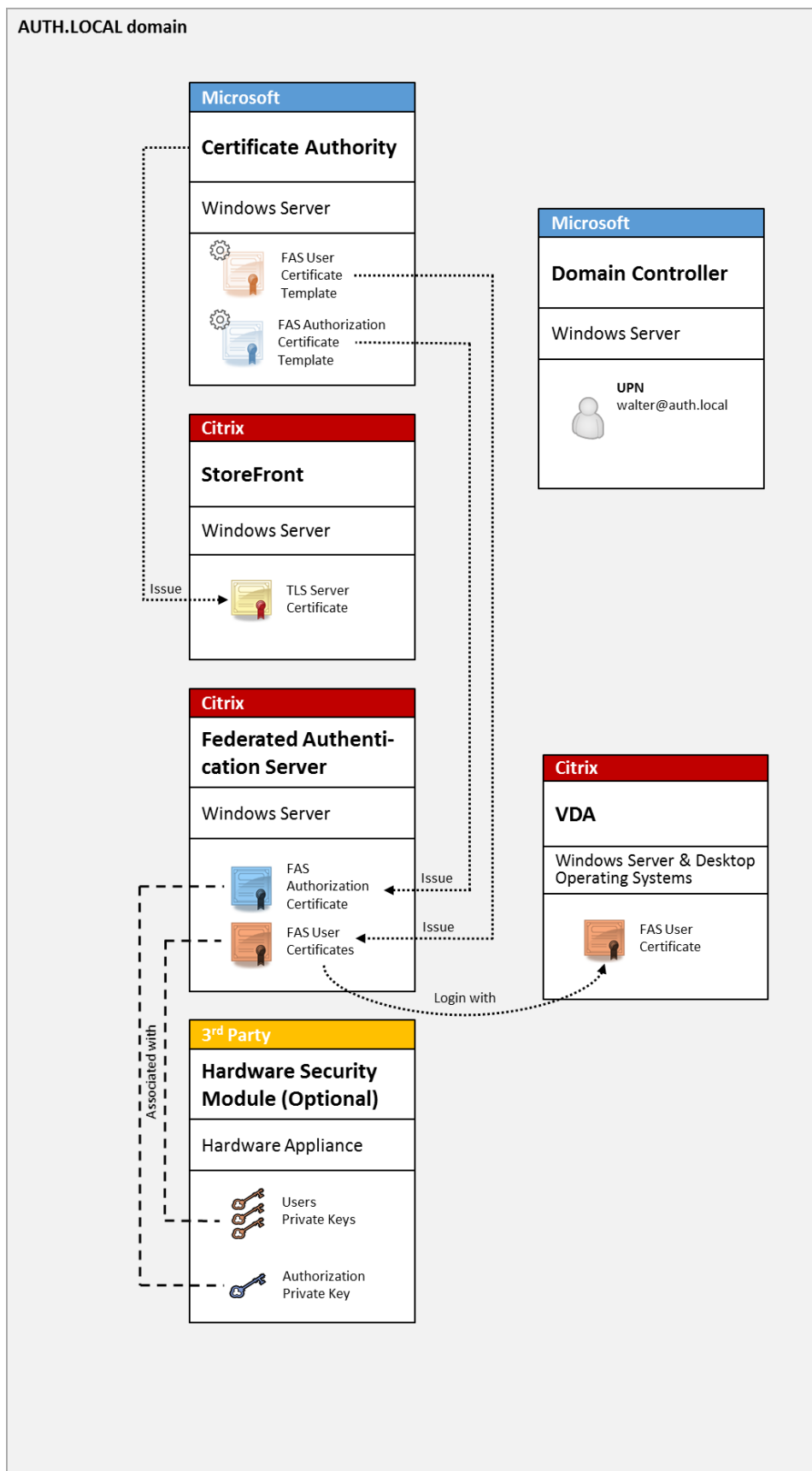
FAS permet aux utilisateurs de s'authentifier en toute sécurité auprès de StoreFront à l'aide de plusieurs options d'authentification (y compris l'authentification unique Kerberos) et de se connecter à une session Citrix HDX authentifiée.

Cela rend possible l'authentification Windows sans invite de saisie d'informations d'identification ou de codes PIN de carte à puce et sans l'utilisation de fonctionnalités de « gestion des mots de passe enregistrés » telles que le service Single Sign-On. Cela peut être utilisé pour remplacer les fonctionnalités d'ouverture de session de la délégation Kerberos contrainte disponibles dans les versions précédentes de Citrix Virtual Apps.

Tous les utilisateurs ont accès aux certificats PKI dans leur session, qu'ils se soient connectés ou non aux machines de point de terminaison avec une carte à puce. Ceci permet une migration fluide vers des modèles d'authentification à deux facteurs, et ce, même à partir de périphériques tels que des smartphones et tablettes qui ne disposent pas d'un lecteur de carte à puce.

Ce déploiement ajoute un nouveau serveur exécutant FAS, qui est autorisé à émettre des certificats de classe de carte à puce pour le compte d'utilisateurs. Ces certificats sont alors utilisés pour se con-

necter à des sessions utilisateur dans un environnement Citrix HDX comme si une ouverture de session par carte à puce était utilisée.



L'environnement Citrix Virtual Apps ou Citrix Virtual Desktops doit être configuré de la même manière que l'ouverture de session par carte à puce à, ce qui est décrit dans l'article [CTX206156](#).

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification Microsoft appartenant au domaine soit disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans l'article [CTX206156](#)).

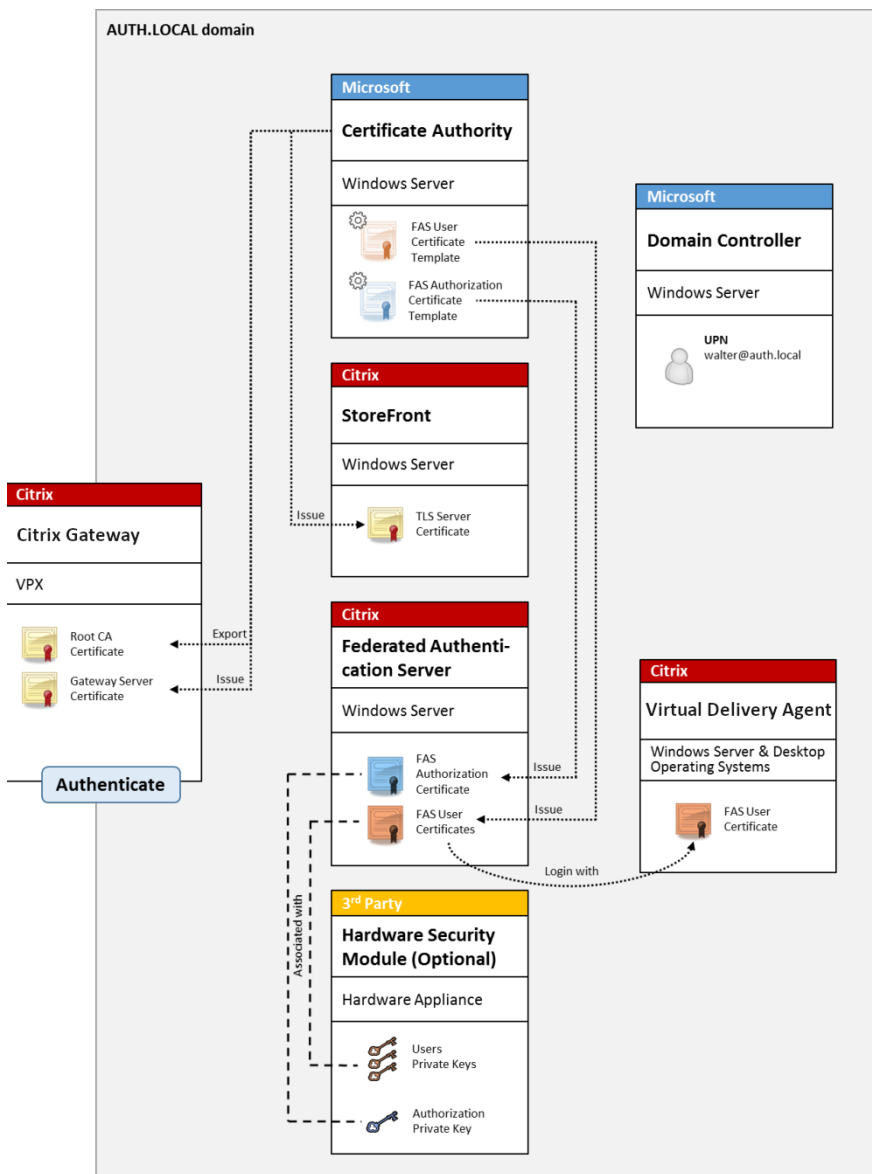
Informations connexes :

- Les clés peuvent être stockées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Pour de plus amples informations, consultez l'article [Protection de clé privée](#).
- L'article [Installer et configurer](#) décrit comment installer et configurer FAS.

Déploiement Citrix Gateway

Le déploiement Citrix Gateway est similaire au déploiement interne, mais ajoute Citrix Gateway couplé avec StoreFront, et déplace le point principal d'authentification sur Citrix Gateway. Citrix Gateway comprend des options d'authentification et d'autorisation avancées qui peuvent être utilisées pour sécuriser l'accès à distance aux sites Web d'une entreprise.

Ce déploiement peut être utilisé pour éviter l'affichage de plusieurs invites de saisie de code PIN qui se produisent lors de l'authentification auprès de Citrix Gateway, puis de la connexion à une session utilisateur. Il permet également d'utiliser les technologies d'authentification Citrix Gateway avancées sans nécessiter de mots de passe Active Directory ou de cartes à puce.



L'environnement Citrix Virtual Apps ou Citrix Virtual Desktops doit être configuré de la même manière que l'ouverture de session par carte à puce à, ce qui est décrit dans l'article [CTX206156](#).

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification Microsoft appartenant au domaine soit disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans l'article [CTX206156](#)).

Lors de la configuration de Citrix Gateway en tant que système d'authentification principal, assurez-vous que toutes les connexions entre Citrix Gateway et StoreFront sont sécurisées à l'aide du protocole TLS. En particulier, assurez-vous que l'URL de rappel est correctement configurée pour pointer

vers le serveur Citrix Gateway, car cela peut être utilisé pour authentifier le serveur Citrix Gateway dans ce déploiement.

The screenshot shows the 'Add NetScaler Gateway Appliance' configuration window. On the left, the 'StoreFront' sidebar is visible with 'Authentication Settings' selected. The main area is titled 'Authentication Settings' and contains the following fields:

- Version:** 10.0 (Build 69.4) or later
- VServer IP address (optional):** v10.0: SNIP or MIP, v10.1+: VIP
- Logon type:** Domain
- Smart card fallback:** None
- Callback URL (optional):** https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.aspx

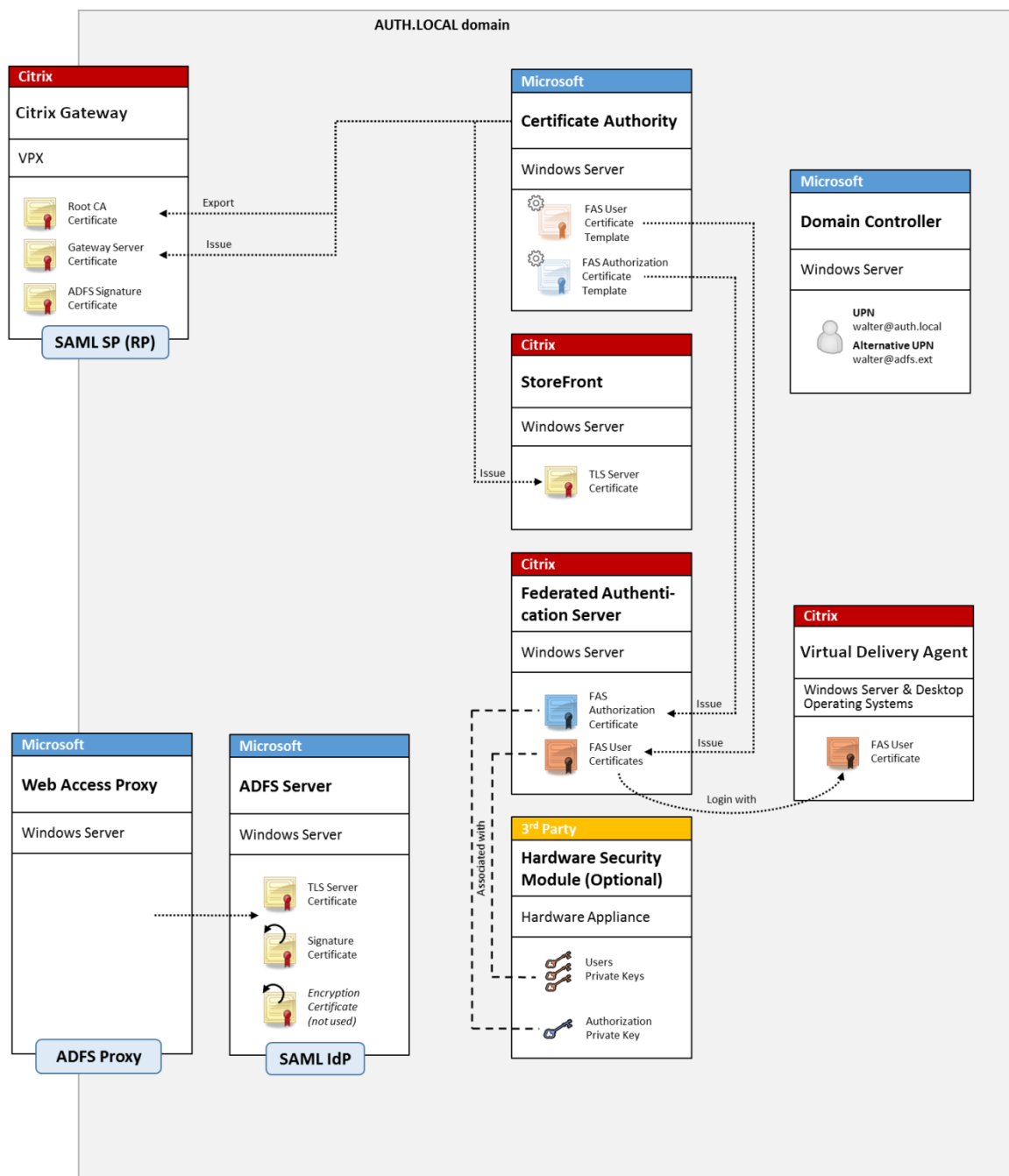
A warning message below the Callback URL field reads: 'When no Callback URL is specified, Smart Access is not available.' At the bottom right, there are three buttons: 'Back', 'Create', and 'Cancel'.

Informations connexes :

- Pour configurer Citrix Gateway, consultez la section [Comment configurer NetScaler Gateway 10.5 pour l'utiliser avec StoreFront 3.6 et Citrix Virtual Desktops 7.6](#).
- L'article [Installer et configurer](#) décrit comment installer et configurer FAS.

Déploiement SAML ADFS

Une technologie d'authentification Citrix Gateway clé permet l'intégration avec Microsoft ADFS, qui peut agir en tant que fournisseur d'identité SAML (IdP). Une assertion SAML est un bloc XML signé de manière cryptographique émis par un fournisseur d'identité approuvé qui autorise un utilisateur à ouvrir une session sur un ordinateur. Cela signifie que le serveur FAS permet de déléguer l'authentification d'un utilisateur au serveur Microsoft ADFS (ou d'autres fournisseurs d'identité SAML).



ADFS est généralement utilisé pour authentifier de manière sécurisée les utilisateurs auprès des ressources d'entreprise à distance via Internet ; par exemple, il est souvent utilisé pour l'intégration à Office 365.

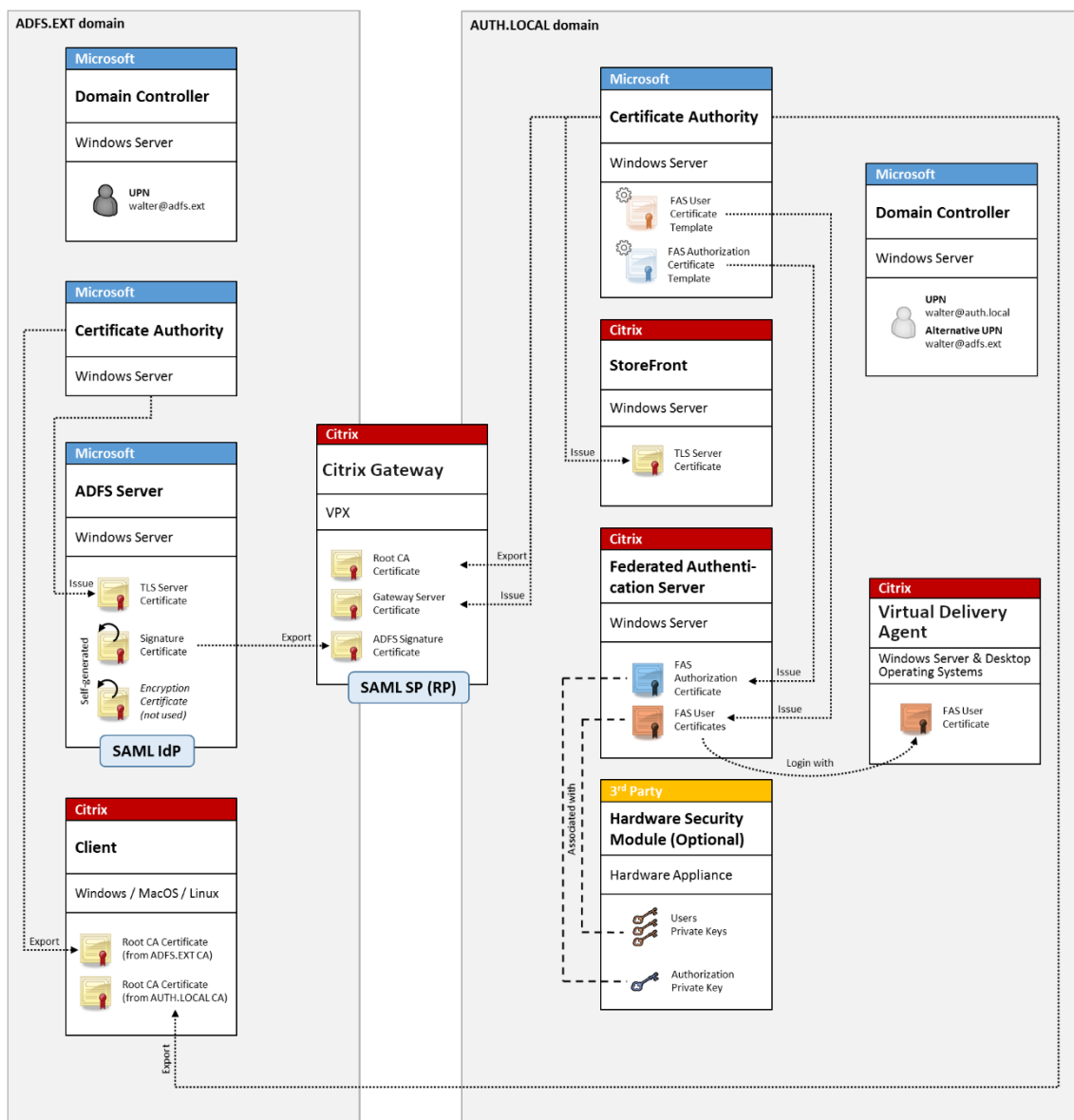
Informations connexes :

- L'article [Déploiement ADFS](#) contient des détails supplémentaires.
- L'article [Installer et configurer](#) décrit comment installer et configurer FAS.
- La section [Déploiement Citrix Gateway](#) dans cet article contient des recommandations en

matière de configuration.

Mappage de compte B2B

Si deux entreprises souhaitent utiliser réciproquement leurs systèmes informatiques, une option courante consiste à configurer un serveur Active Directory Federation Service (ADFS) avec une relation d'approbation. Cela permet aux utilisateurs d'une entreprise de s'authentifier en toute transparence auprès de l'environnement Active Directory (AD) d'une autre entreprise. Lors de l'ouverture de session, chaque utilisateur utilise ses propres informations d'identification d'ouverture de session d'entreprise ; ADFS mappe automatiquement ces dernières à un « compte fantôme » dans l'environnement Active Directory de l'entreprise homologue.

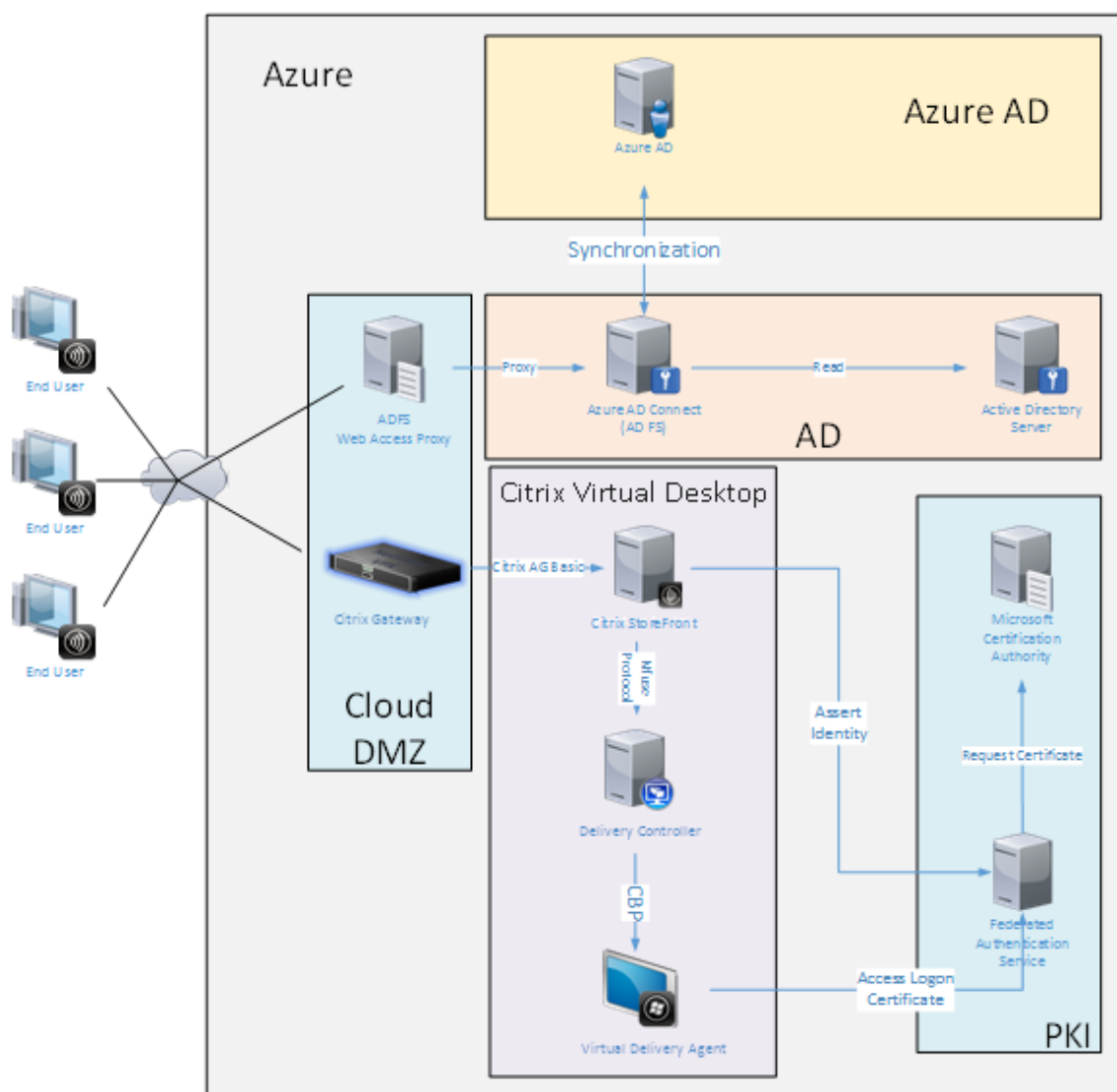


Informations connexes :

- L'article [Installer et configurer](#) décrit comment installer et configurer FAS.

Jonction à un domaine Azure AD (Azure AD Join) avec Windows 10

Windows 10 a introduit le concept de « Azure AD Join » (Jonction à un domaine Azure AD), qui est d'un point de vue conceptuel similaire à la jointure de domaine Windows traditionnelle mais ciblé pour les scénarios « via Internet ». Ce concept convient tout particulièrement aux ordinateurs portables et tablettes. Comme avec la jonction de domaine Windows traditionnelle, Azure AD est équipé de fonctionnalités permettant d'utiliser des modèles d'authentification unique pour la connexion aux sites Web et aux ressources de l'entreprise. Ces derniers sont tous « compatibles Internet », ils fonctionnent donc à partir de n'importe quel emplacement connecté à Internet, et pas seulement sur le réseau local du bureau.



Ce déploiement est un exemple dans lequel il n'existe pas de concept « utilisateurs au bureau. » Les ordinateurs portables sont inscrits et s'authentifient via Internet à l'aide des fonctionnalités modernes d'Azure AD.

Veuillez noter que l'infrastructure dans ce déploiement peut s'exécuter partout où une adresse IP est disponible : en interne, fournisseur hébergé, Azure ou un autre fournisseur de cloud. Le synchronisateur Azure AD Connect se connectera automatiquement à Azure AD. Le graphique utilise des VM Azure à des fins de simplicité.

Informations connexes :

- L'article [Installer et configurer](#) décrit comment installer et configurer FAS.
- L'article [Intégration d'Azure AD](#) contient des détails supplémentaires.

Déploiement ADFS

June 5, 2024

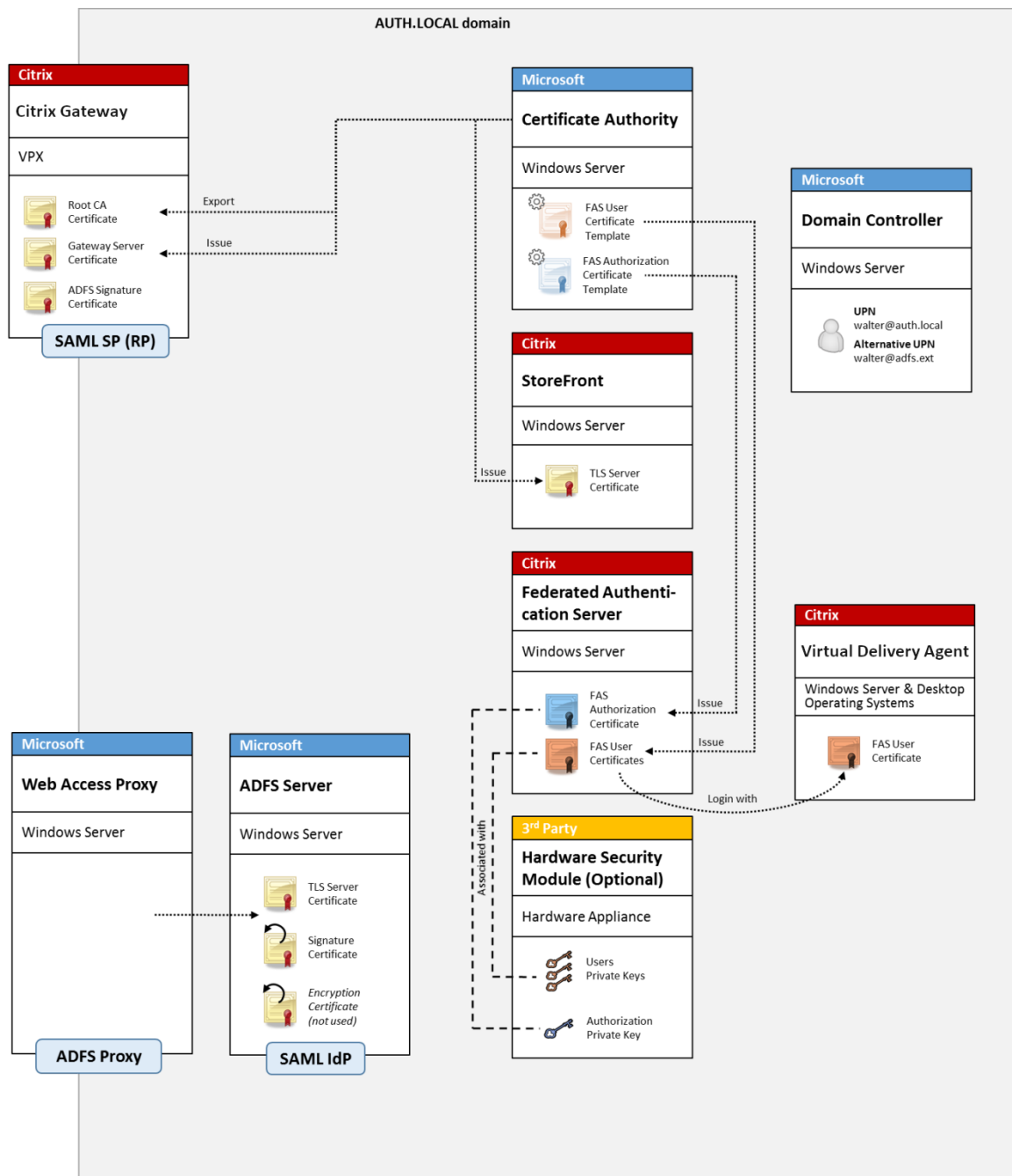
Introduction

Ce document décrit comment intégrer un environnement Citrix avec Microsoft ADFS.

De nombreuses organisations utilisent ADFS pour gérer l'accès sécurisé aux sites Web qui requièrent un seul point d'authentification. Par exemple, une entreprise peut disposer de contenu et de téléchargements supplémentaires disponibles pour les employés ; ces emplacements doivent être protégés avec des informations d'identification d'ouverture de session Windows standard.

Le Service d'authentification fédérée (FAS) permet également d'intégrer Citrix Gateway et Citrix Store-Front avec le système d'ouverture de session ADFS, ce qui réduit toute confusion potentielle pour les employés.

Ce déploiement intègre Citrix Gateway en tant que partie de confiance pour Microsoft ADFS.



Remarque :

Il n'y a aucune différence si la ressource principale est un VDA Windows ou un Linux VDA.

Présentation SAML

SAML (Security Assertion Markup Language) est un système d'ouverture de session sur navigateur Web de « redirection vers une page d'ouverture de session ». La configuration comprend les éléments

suivants :

URL de redirection [URL du service Single Sign-On]

Lorsque Citrix Gateway découvre qu'un utilisateur a besoin d'être authentifié, il indique au navigateur Web de l'utilisateur d'utiliser un HTTP POST vers une page Web d'ouverture de session SAML sur le serveur ADFS. C'est généralement une adresse <https://> au format : <https://adfs.mycompany.com/adfs/ls>.

Cette page Web POST comprend d'autres informations, notamment « l'adresse de retour » à laquelle ADFS renverra l'utilisateur lorsque l'ouverture de session est terminée.

Identificateur [Nom de l'émetteur/EntityID]

EntityId est un identificateur unique que Citrix Gateway inclut dans ses données POST à ADFS. Il renseigne ADFS sur le service auquel l'utilisateur tente de se connecter et applique différentes stratégies d'authentification le cas échéant. S'il est émis, le fichier XML d'authentification SAML pourra uniquement être utilisé pour ouvrir une session sur le service identifié par EntityId.

En règle générale, EntityID est l'adresse URL de la page d'ouverture de session du serveur Citrix Gateway, mais une quelconque autre adresse peut être utilisée, à condition que Citrix Gateway et ADFS l'acceptent : <https://ns.mycompany.com/application/logonpage>.

Adresse de retour [URL de réponse]

Si l'authentification réussit, ADFS indique au navigateur Web de l'utilisateur de publier un fichier ADFS d'authentification SAML sur l'une des URL de réponse qui sont configurées pour EntityId. Il s'agit généralement d'une adresse <https://> sur le serveur Citrix Gateway d'origine au format : <https://ns.mycompany.com/cgi/samlauth>.

S'il existe plusieurs URL de réponse configurées, Citrix Gateway peut en choisir une dans sa publication d'origine sur ADFS.

Certificat de signature [Certificat IDP]

ADFS signe de manière cryptographique les objets blob XML d'authentification SAML à l'aide de sa clé privée. Pour valider cette signature, Citrix Gateway doit être configuré pour vérifier ces signatures à l'aide de la clé publique incluse dans un fichier de certificat. Le fichier de certificat sera généralement un fichier texte obtenu à partir du serveur ADFS.

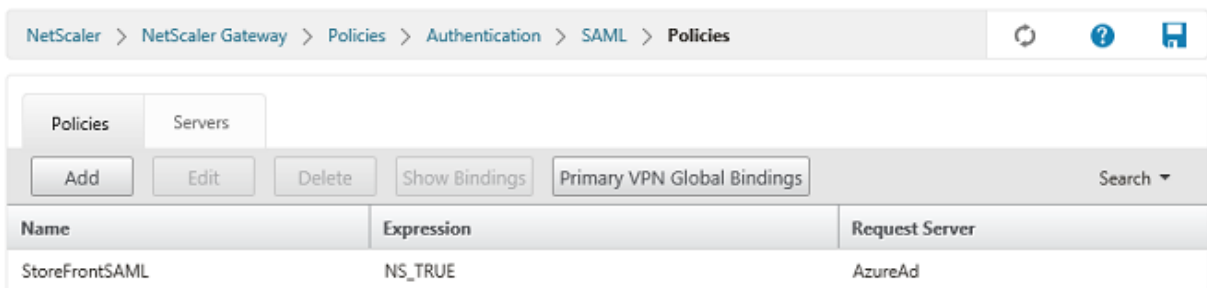
URL d'authentification unique [URL de déconnexion unique]

ADFS et Citrix Gateway prennent en charge un système de « déconnexion centrale ». Il s'agit d'une adresse URL que Citrix Gateway interroge parfois pour vérifier que l'objet blob XML d'authentification SAML représente toujours une session actuellement connectée.

Cette fonctionnalité est facultative et n'a pas besoin d'être configurée. C'est généralement une adresse <https://> au format <https://adfs.mycompany.com/adfs/logout>. (Notez que cette dernière peut être la même que l'URL d'ouverture de session unique).

Configuration

La section [Déploiement Citrix Gateway](#) explique comment configurer Citrix Gateway afin de gérer les options d'authentification LDAP standard. Une fois la configuration terminée, vous pouvez créer une nouvelle stratégie d'authentification sur Citrix Gateway qui autorise l'authentification SAML. Cela peut remplacer la stratégie LDAP par défaut utilisée par l'assistant Citrix Gateway.



The screenshot shows the Citrix Gateway management console interface. The breadcrumb navigation at the top reads: NetScaler > NetScaler Gateway > Policies > Authentication > SAML > Policies. Below the navigation, there are tabs for 'Policies' and 'Servers', with 'Policies' selected. A toolbar contains buttons for 'Add', 'Edit', 'Delete', 'Show Bindings', 'Primary VPN Global Bindings', and a 'Search' dropdown. Below the toolbar is a table with the following data:

| Name | Expression | Request Server |
|----------------|------------|----------------|
| StoreFrontSAML | NS_TRUE | AzureAd |

Renseigner la stratégie SAML

Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment dans la console de gestion ADFS. Lorsque cette stratégie est appliquée, Citrix Gateway redirige l'utilisateur vers ADFS pour l'ouverture de session, et accepte un jeton d'authentification SAML signé par ADFS.

Create Authentication SAML Server

Create Authentication SAML Server

Name*
AzureAd

Authentication Type
SAML

IDP Certificate Name*
AzureADSAML

Redirect URL*
29f-4c20-9826-14d5e484c62e/saml2

Single Logout URL
29f-4c20-9826-14d5e484c62e/saml2

User Field
userprincipalname

Signing Certificate Name

Issuer Name
https://ns.citrixsamldemo.net/Citrix/

Reject Unsigned Assertion*
ON

SAML Binding*
POST

Default Authentication Group

Skew Time(mins)
5

5

Two Factor
 ON OFF

Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*
Exact

Authentication Class Types
InternetProtocol
InternetProtocolPassword

Signature Algorithm*
 RSA-SHA1 RSA-SHA256

Digest Method*
 SHA1 SHA256

Send Thumbprint
 Enforce Username

Attribute 1
Attri

Attribute 3
Attri

Attribute 5
Attri

Attribute 7
Attri

Informations connexes

- L'article [Installer et configurer](#) est le document de référence principal pour obtenir des informations sur l'installation et la configuration de FAS.
- Les déploiements FAS courants sont décrits dans l'article [Vue d'ensemble des architectures](#).
- D'autres informations pratiques sont disponibles dans l'article [Configuration avancée](#).

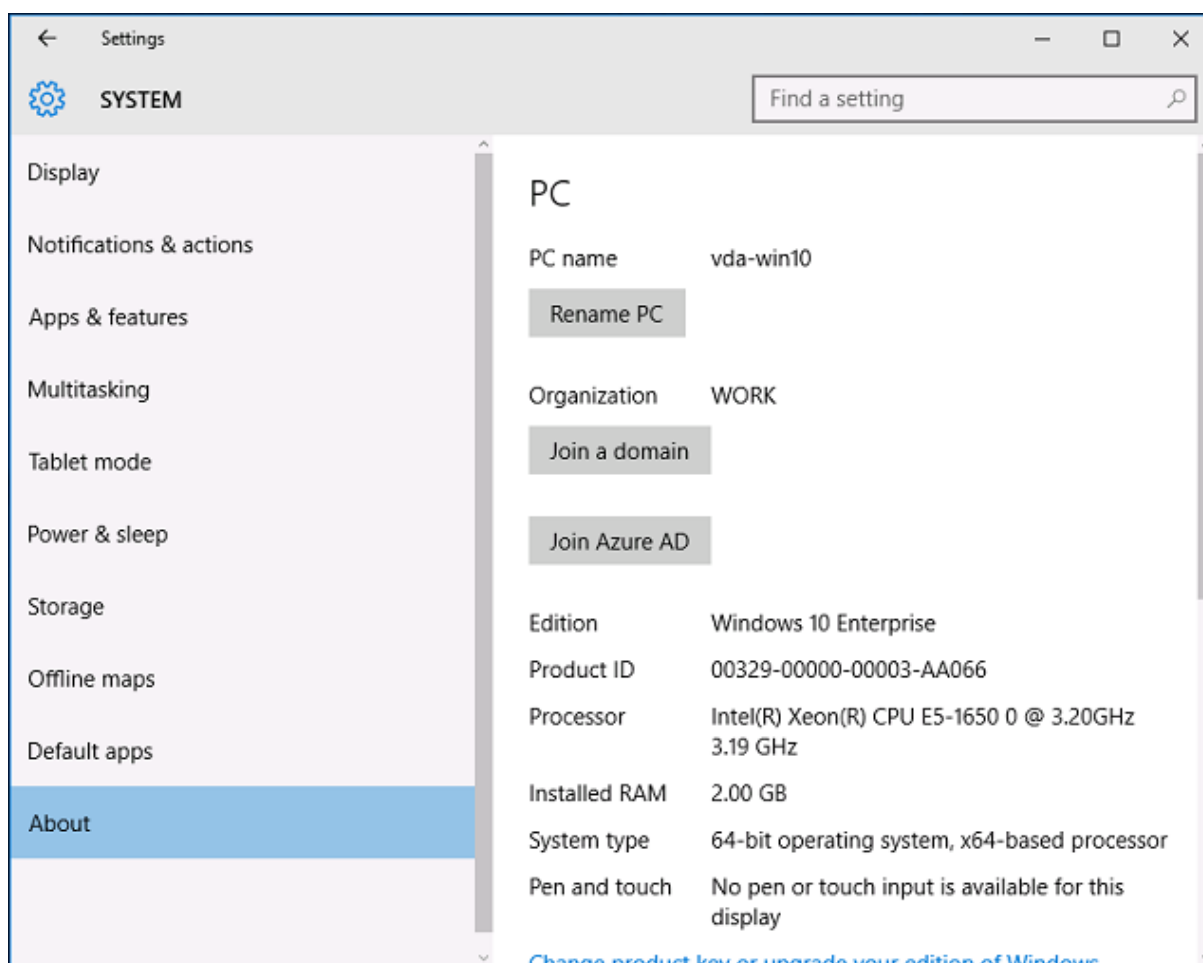
Intégration d'Azure AD

June 5, 2024

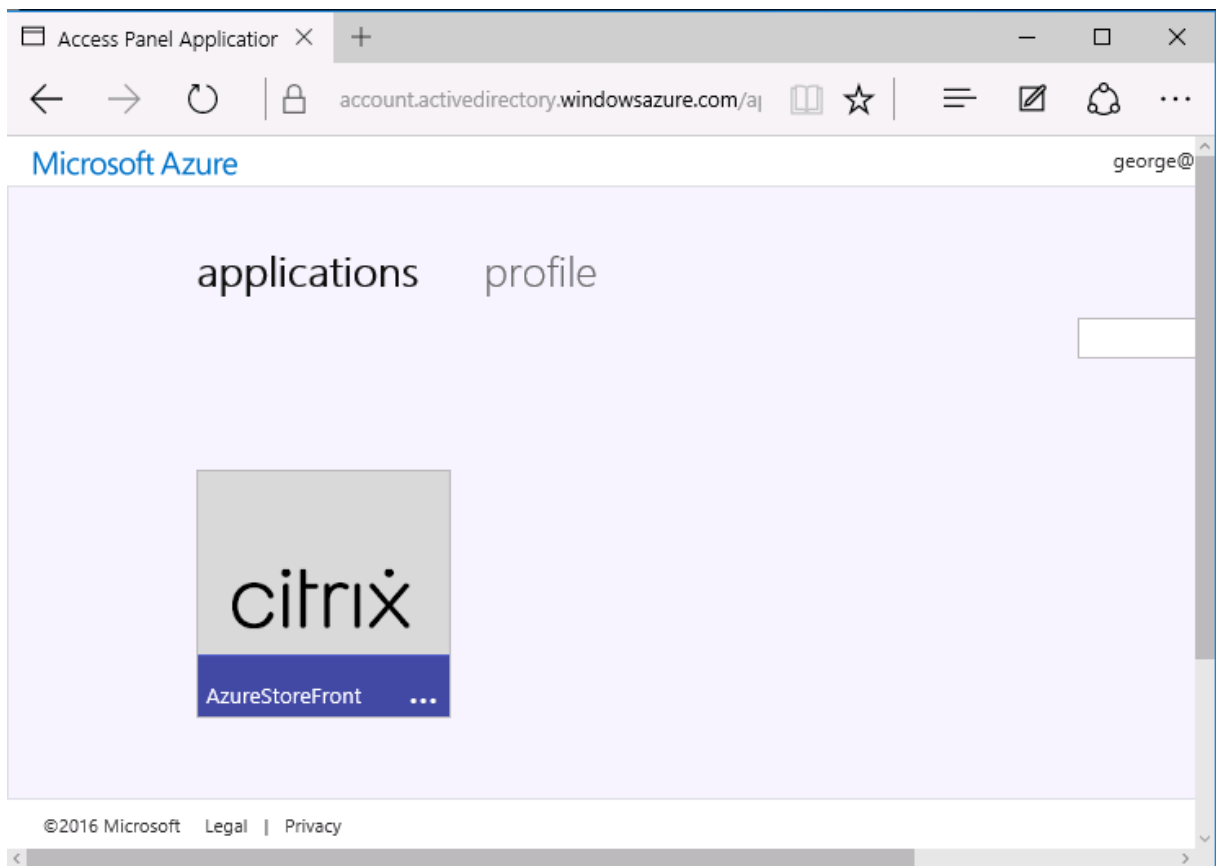
Introduction

Ce document décrit comment intégrer un environnement Citrix avec la fonctionnalité Azure AD de Windows 10. Windows 10 a introduit Azure AD, qui est un nouveau modèle de jonction de domaine dans lequel les ordinateurs portables itinérants peuvent être joints à un domaine d'entreprise via Internet à des fins de gestion et d'authentification unique.

L'exemple de déploiement dans ce document décrit un système dans lequel l'informatique fournit aux nouveaux utilisateurs une adresse de messagerie d'entreprise et un code d'inscription pour leurs ordinateurs portables Windows 10 personnels. Les utilisateurs accèdent à ce code via **Système > À propos de > Connecter à Azure AD** dans le volet **Paramètres**.



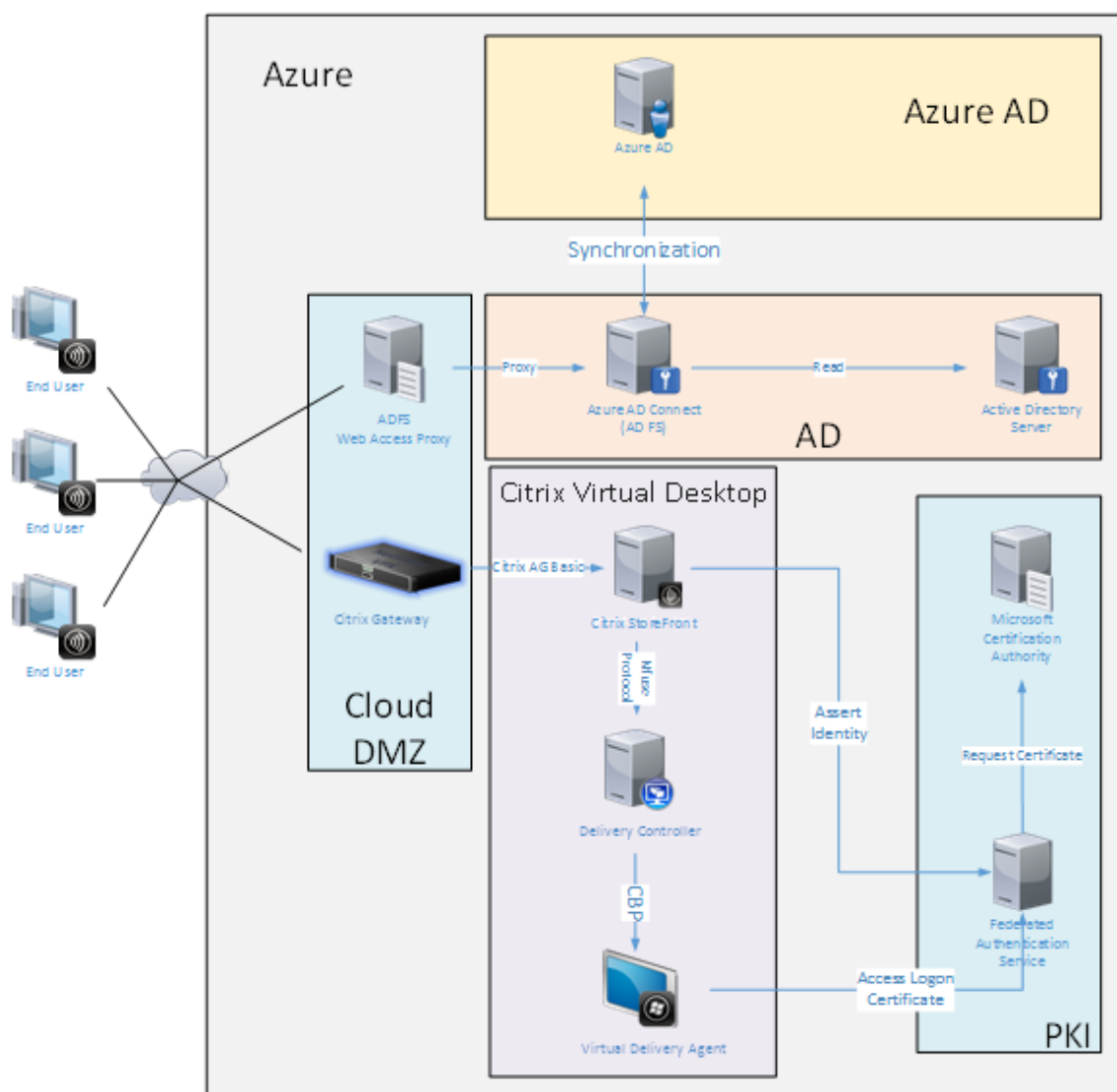
Une fois que l'ordinateur portable est inscrit, le navigateur Web Microsoft Edge se connecte automatiquement aux sites Web de l'entreprise et aux applications publiées Citrix via la page Web d'applications Azure SAAS, avec d'autres applications Azure telles que Microsoft Office 365.



Architecture

Cette architecture réplique un réseau d'entreprise traditionnel dans Azure, tout en intégrant des technologies de cloud modernes telles que Azure AD et Office 365. Les utilisateurs sont considérés comme des travailleurs distants, et la notion d'intranet n'a pas lieu.

Le modèle peut être appliqué aux entreprises disposant déjà de systèmes locaux, car le service de synchronisation Azure AD Connect peut établir un lien à Azure via Internet.



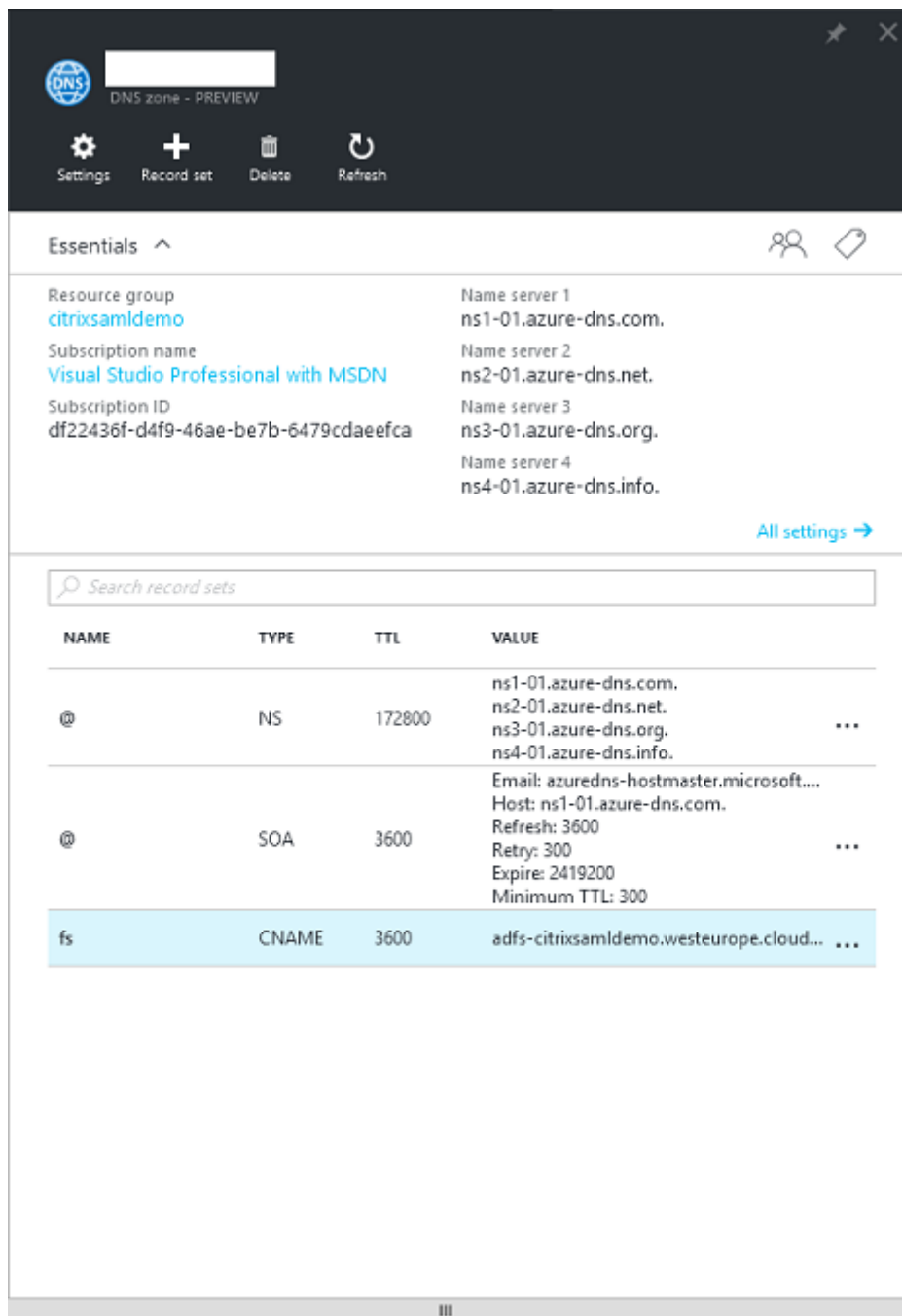
Les connexions sécurisées et l'authentification unique, qui sont traditionnellement derrière un pare-feu sur le LAN et l'authentification NTLM/ Kerberos, sont remplacées dans cette architecture par des connexions TLS à Azure et SAML. Des nouveaux services sont créés à mesure que des applications Azure sont jointes à Azure AD. Les applications existantes qui nécessitent Active Directory (telles qu'une base de données SQL Server) peuvent être exécutées à l'aide d'une VM de serveur Active Directory standard dans la partie IAAS du Azure Cloud Service.

Lorsqu'un utilisateur lance une application traditionnelle, elle est accessible à l'aide des applications publiées Citrix Virtual Apps and Desktops. Les différents types d'applications sont compilés via la page **Applications Azure** de l'utilisateur, à l'aide des fonctionnalités d'authentification unique de Microsoft Edge. Microsoft fournit également des applications Android et iOS qui peuvent énumérer et lancer des applications Azure.

Créer une zone DNS

Azure AD requiert que l'administrateur ait enregistré une adresse DNS publique et qu'il contrôle la zone de délégation pour le suffixe de nom de domaine. Pour ce faire, l'administrateur peut utiliser la fonctionnalité de zone DNS d'Azure.

Cet exemple utilise le nom de zone DNS *citrixsamldemo.net*.



La console affiche les noms des serveurs de noms DNS Azure. Ces derniers doivent être référencés

dans les entrées NS du bureau d'enregistrement DNS pour la zone (par exemple, citrixsaml-demo.net. NS n1-01.azure-dns.com)

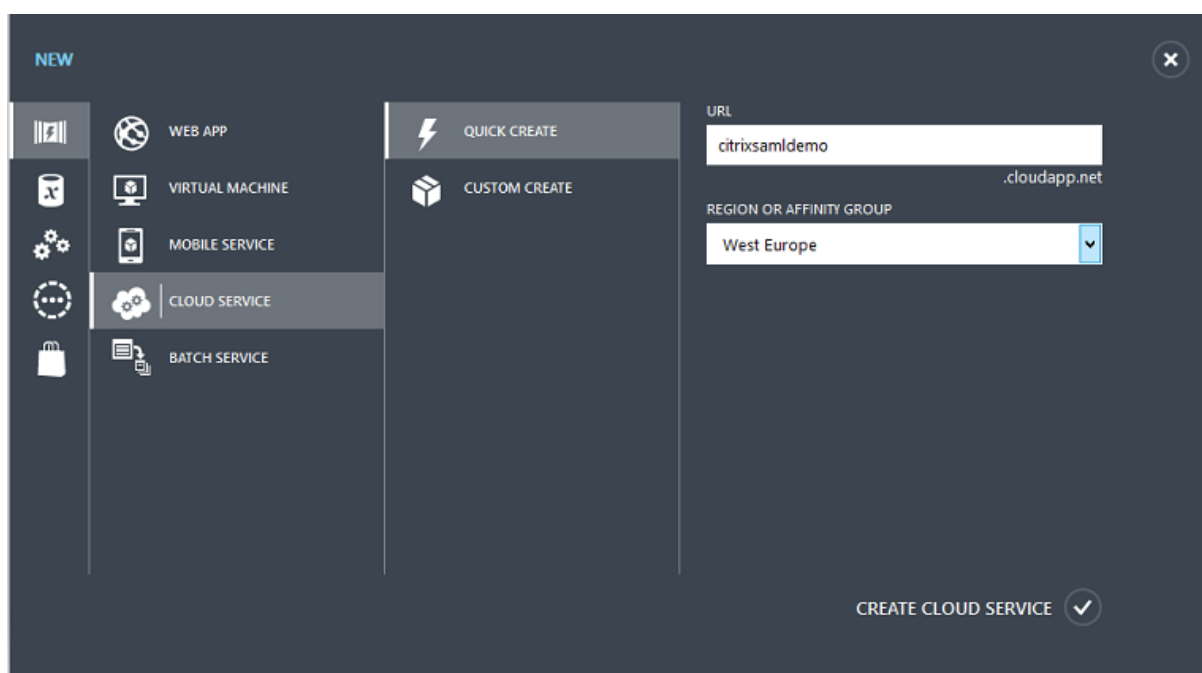
Lors de l'ajout de références aux VM exécutées dans Azure, il est plus facile d'utiliser un pointeur CNAME vers l'enregistrement DNS géré par Azure pour la VM. Si l'adresse IP de la VM change, vous n'aurez pas besoin de mettre à jour manuellement le fichier de la zone DNS.

Les suffixes des adresses DNS internes et externes correspondront pour ce déploiement. Le domaine est citrixsaml-demo.net, et utilise un split DNS (10.0.0.* en interne).

Ajoutez une entrée « fs.citrixsaml-demo.net » qui fait référence au serveur proxy d'application Web. Il s'agit du service de fédération pour cette zone.

Créer un service de cloud

Cet exemple configure un environnement Citrix comprenant un environnement Active Directory avec un serveur ADFS exécuté dans Azure. Un service de cloud appelé « [citrixsaml-demo](https://citrixsaml-demo.net) » est créé.

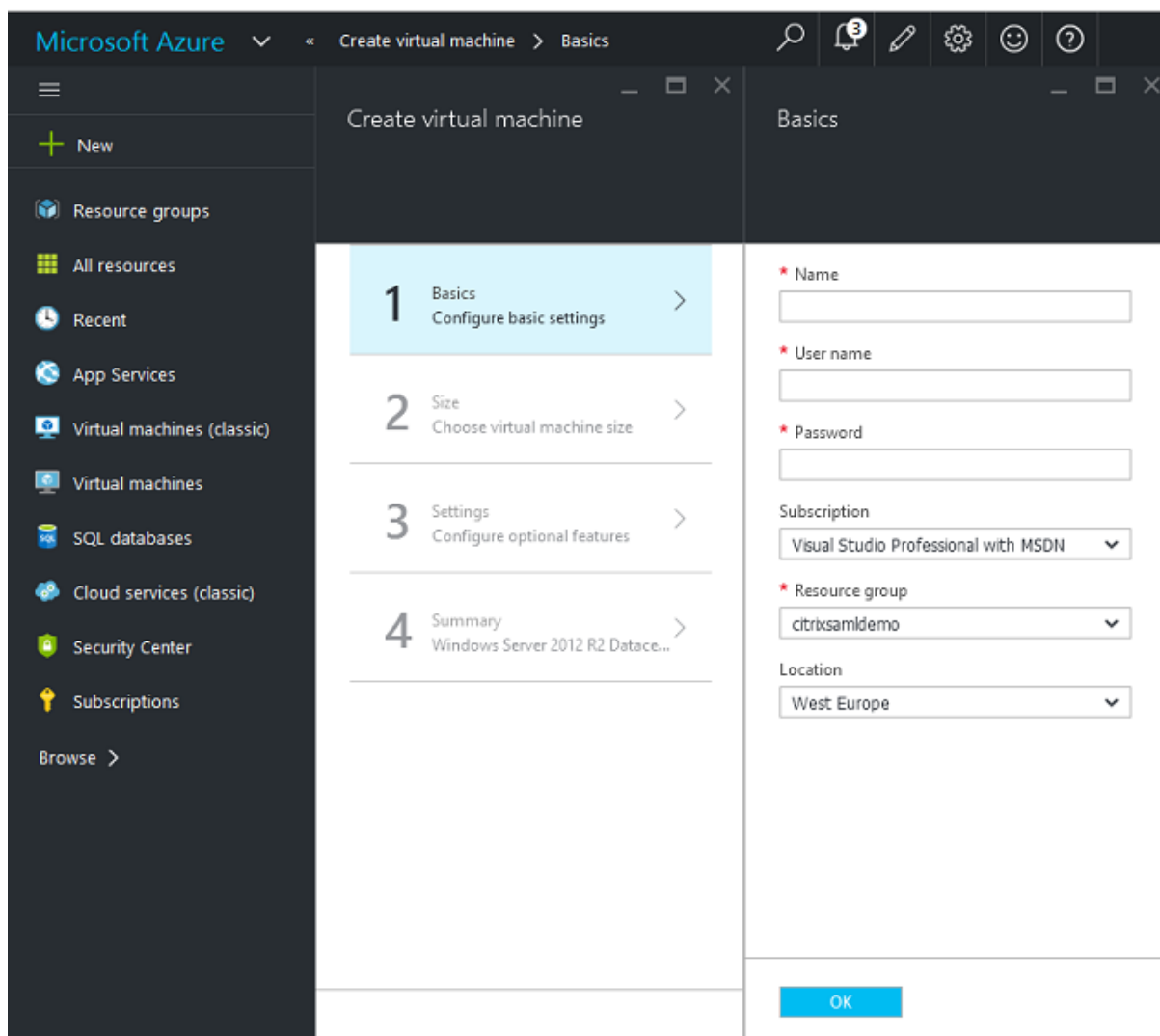


Créer des machines virtuelles Windows

Créez cinq VM Windows exécutées dans le service de cloud :

- Contrôleur de domaine (domaincontrol)
- Serveur ADFS Azure Connect (adfs)
- Proxy d'accès Web ADFS (proxy d'application Web, non joint à un domaine)

- Delivery Controller Citrix Virtual Apps and Desktops
- Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA)



Contrôleur de domaine

- Ajoutez les rôles **Serveur DNS** et **Services de domaine Active Directory** pour créer un déploiement Active Directory standard (dans cet exemple, citrixsamldemo.net). Une fois la promotion de domaine terminée, ajoutez le rôle **Services de certification Active Directory**.
- Créez un compte d'utilisateur normal pour le test (par exemple, George@citrixsamldemo.net).
- Étant donné que ce serveur exécutera le DNS interne, tous les serveurs doivent faire référence à ce serveur pour la résolution DNS. Cette opération peut être effectuée au travers de la page des **paramètres Azure DNS**. (Pour de plus amples informations, consultez la section Annexe dans ce document).

Contrôleur ADFS et serveur proxy d'application Web

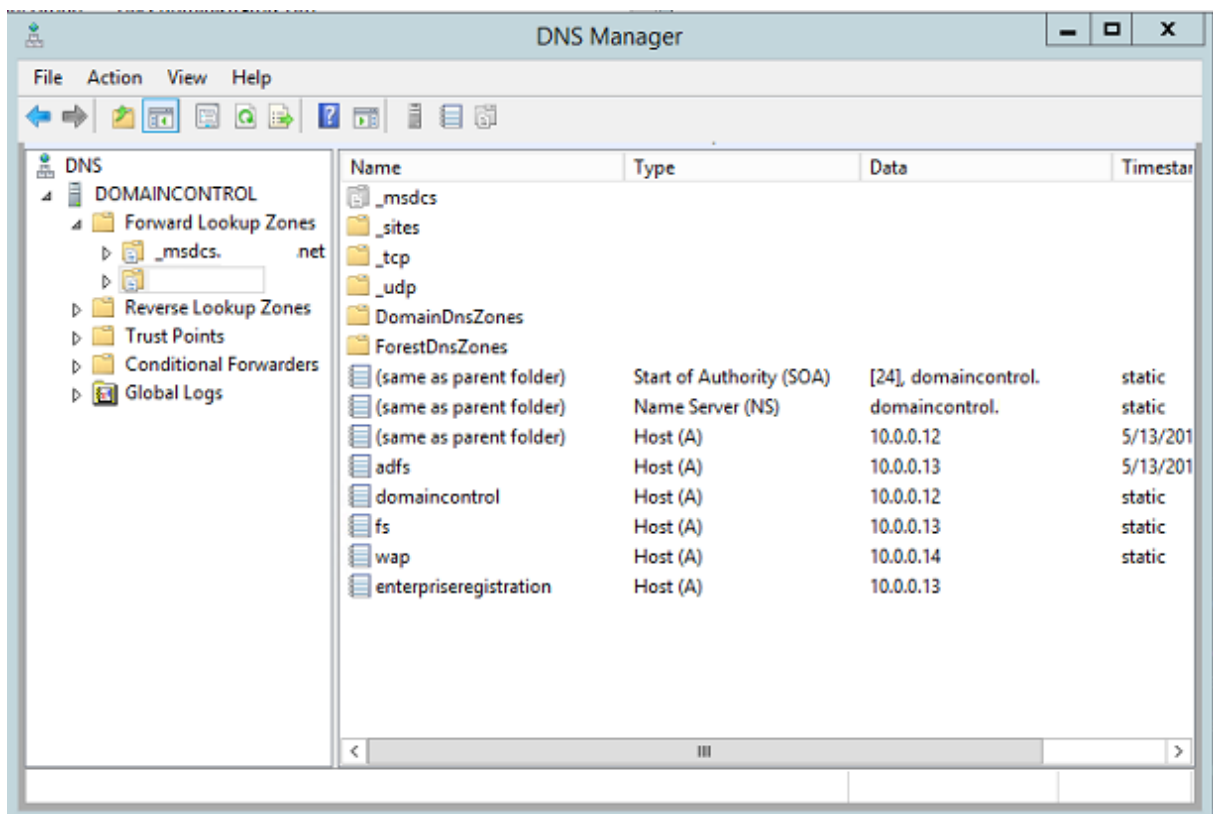
- Joignez le serveur ADFS au domaine citrixsamldemo. Le serveur proxy d'application Web doit rester dans un groupe de travail isolé, vous devez donc enregistrer une adresse DNS manuellement avec le DNS AD.
- Exécutez l'applet de commande **Enable-PSRemoting –Force** sur ces serveurs afin d'autoriser l'accès à distance PowerShell via les pare-feu depuis l'outil Azure AD Connect.

Citrix Virtual Desktops Delivery Controller et VDA

- Installez Citrix Virtual Apps ou Citrix Virtual Desktops Delivery Controller et le VDA sur les deux autres serveurs Windows joints à citrixsamldemo.

Configurer un DNS interne

Une fois le contrôleur de domaine installé, configurez le serveur DNS afin de gérer l'affichage interne de citrixsamldemo.net, et d'agir en tant que redirecteur vers un serveur DNS externe (par exemple : 8.8.8.8).

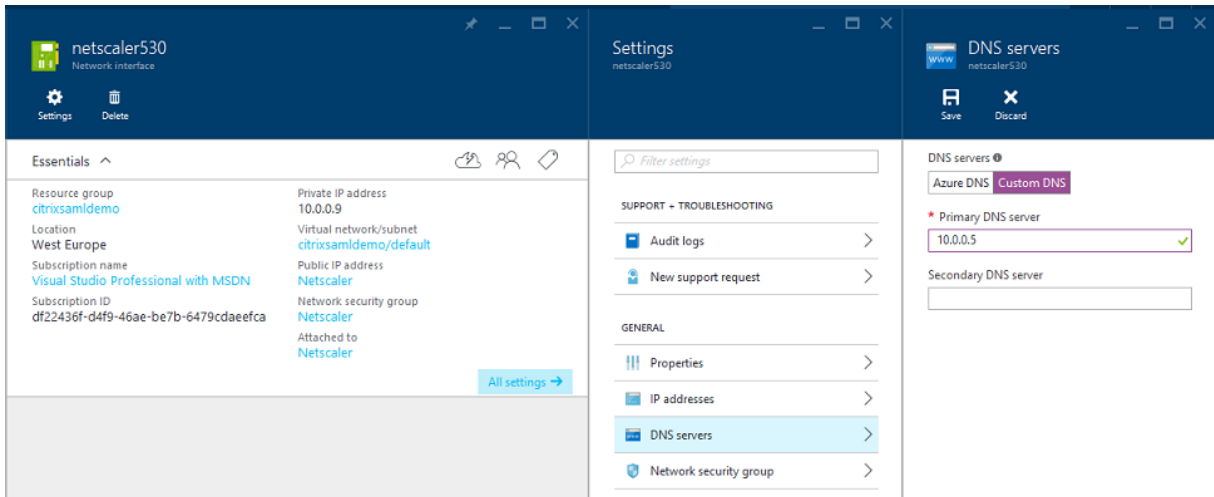


Ajoutez un enregistrement statique pour :

Service d'authentification fédérée

- wap.citrixsamldemo.net [la VM du proxy d'application Web ne sera pas jointe au domaine]
- fs.citrixsamldemo.net [adresse du serveur de fédération interne]
- enterpriseregistration.citrixsaml.net [identique à fs.citrixsamldemo.net]

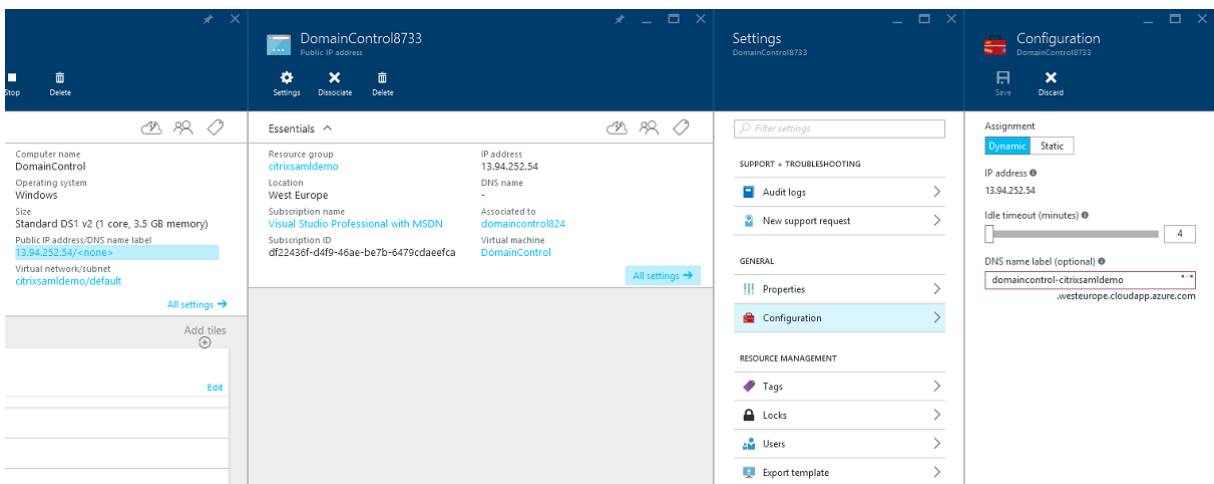
Toutes les VM exécutées dans Azure doivent être configurées pour utiliser uniquement ce serveur DNS. Vous pouvez effectuer cette opération à l'aide de l'interface réseau.



Par défaut, l'adresse IP interne (10.0.0.9) est attribuée de manière dynamique. Vous pouvez utiliser le paramètre d'adresses IP pour attribuer l'adresse IP de manière permanente. Ceci doit être effectué pour le serveur proxy d'application Web et le contrôleur de domaine.

Configurer une adresse DNS externe

Lorsqu'une VM est en cours d'exécution, Azure gère son propre serveur de zone DNS qui pointe vers l'adresse IP publique attribuée à la VM. Il est utile d'activer cette fonctionnalité car Azure attribue par défaut des adresses IP au démarrage de chaque VM.

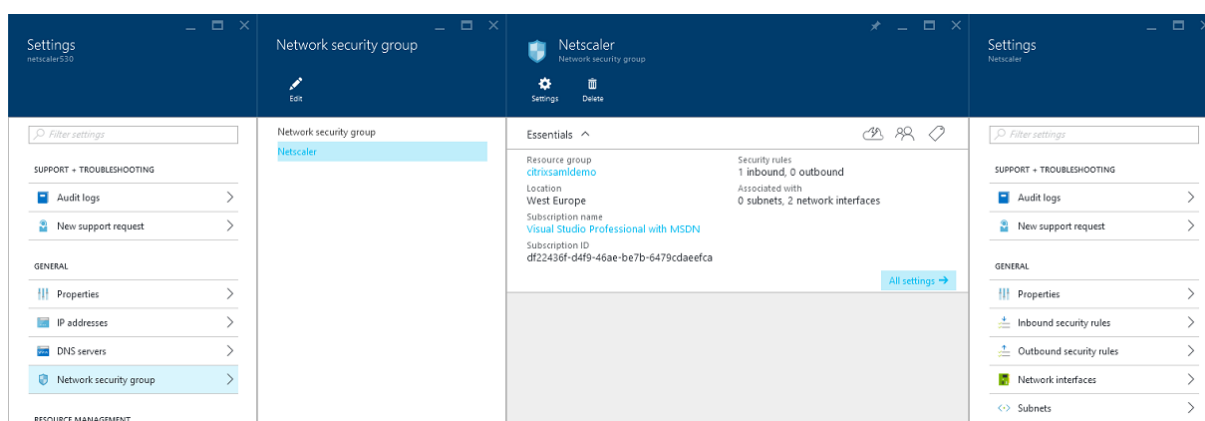


Cet exemple attribue l'adresse DNS `domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com` au contrôleur de domaine.

Notez que lorsque la configuration distante est terminée, seuls le proxy d'application Web et les VM Citrix Gateway doivent disposer d'adresses IP publiques. (Lors de la configuration, l'adresse IP publique est utilisée pour accéder à distance à l'environnement).

Configurer des groupes de sécurité

Le cloud Azure gère les règles de pare-feu pour l'accès TCP/UDP aux VM à partir d'Internet à l'aide de groupes de sécurité. Par défaut, toutes les VM autorisent l'accès RDP. Les serveurs Citrix Gateway et proxy d'application Web doivent également autoriser TLS sur le port 443.

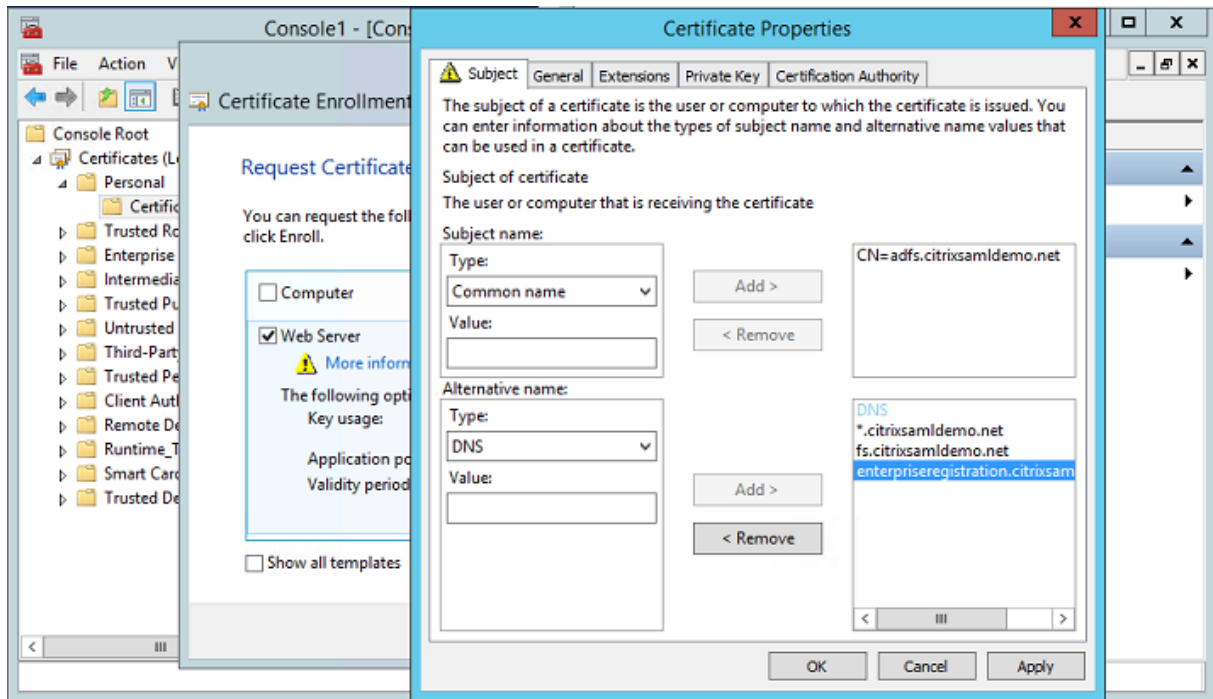


Créer un certificat d'ADFS

Activez le modèle de certificat **Serveur Web** sur l'autorité de certification Microsoft. Ceci permet la création d'un certificat avec des adresses DNS personnalisées qui peuvent être exportées (y compris la clé privée) sur un fichier pfx. Vous devez installer ce certificat sur les serveurs ADFS et proxy d'applications Web, par conséquent le fichier pfx est l'option préférée.

Émettez un certificat de serveur Web avec les noms de sujets suivants :

- Commonname:
 - `adfs.citrixsamldemo.net` [nom d'ordinateur]
- SubjectAltname:
 - `*.citrixsamldemo.net` [nom de zone]
 - `fs.citrixsamldemo.net` [entrée dans le DNS]
 - `enterpriseregistration.citrixsamldemo.net`



Exportez le certificat sur un fichier pfx, y compris une clé privée protégée par mot de passe.

Configurer Azure AD

Cette section décrit en détail la création d'une nouvelle instance Azure AD et la création d'identités utilisateur qui peuvent être utilisées pour joindre Windows 10 à Azure AD.

Créer un nouveau répertoire

Ouvrez une session sur le portail Azure et créez un nouveau répertoire.

Add directory

DIRECTORY ?
Create new directory

NAME ?
CitrixSAMLDemo

DOMAIN NAME ?
citrixsamldemo .onmicrosoft.com

COUNTRY OR REGION ?
United Kingdom

This is a B2C directory. ? **PREVIEW**

Une fois le répertoire créé, une page de résumé apparaît.

The screenshot shows the Citrix SAM Demo portal. At the top, the title 'citrixsamdemo' is displayed. Below it is a navigation menu with links for USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. A large banner features a blue geometric logo and the text: 'Your directory is ready to use. Here are a few options to get started.' Below the banner is a checkbox labeled 'Skip Quick Start the next time I visit'. Underneath, there is an 'I WANT TO' section with three buttons: 'Set Up Directory' (highlighted in blue), 'Manage Access', and 'Develop Applications'. The 'GET STARTED' section follows, listing three numbered steps:

- 1 Improve user sign-in experience**
Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.
[Add domain](#)
- 2 Integrate with your local directory**
Use the same user accounts and groups in the cloud that you already use on premises.
[Download Azure AD Connect](#)
- 3 Get Azure AD Premium**
Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.
[Try it now](#)

Créer un utilisateur administrateur global (AzureAdmin)

Créez un administrateur global dans Azure (dans cet exemple, `AzureAdmin@citrixsamdemo.onmicrosoft.com`) et ouvrez une session avec le nouveau compte pour définir un mot de passe.

ADD USER

user profile

FIRST NAME: Azure

LAST NAME: Admin

DISPLAY NAME: Azure Admin

ROLE: Global Admin

ALTERNATE EMAIL ADDRESS: [Red error icon]

MULTI-FACTOR AUTHENTICATION: Enable Multi-Factor Authentication

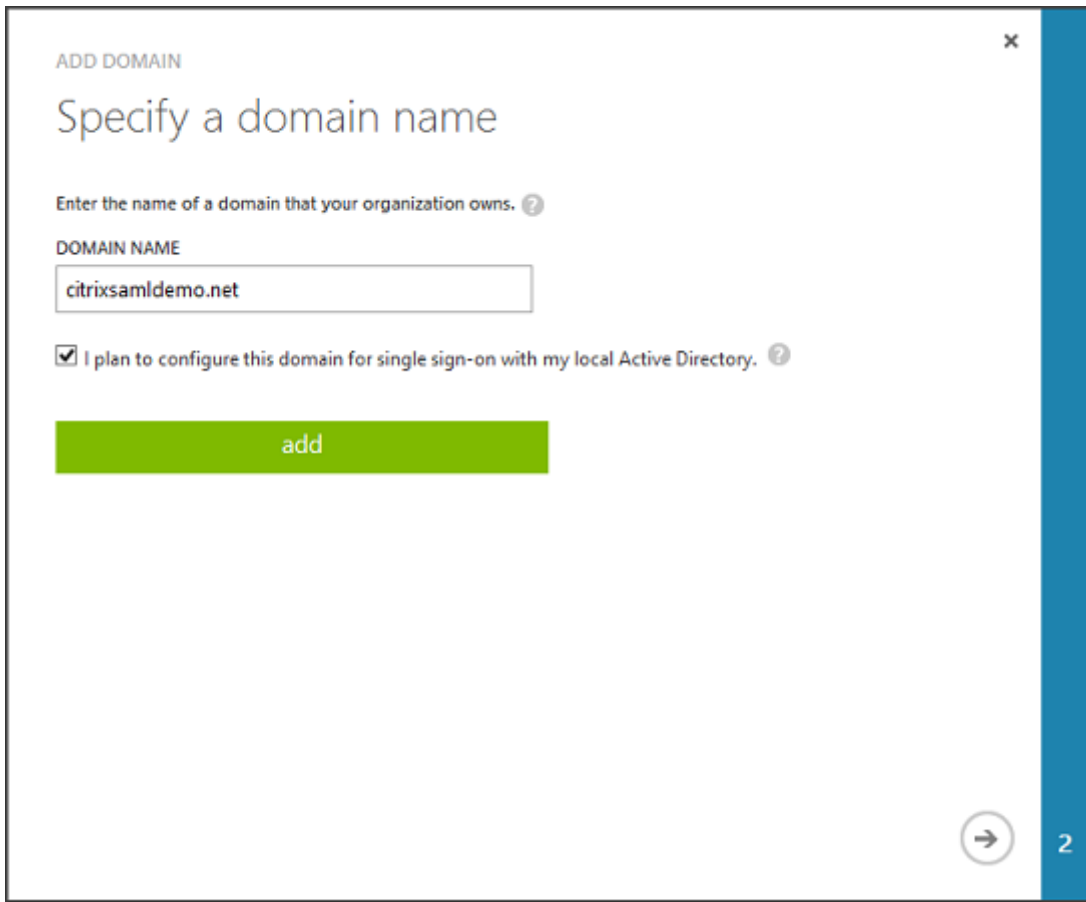
Enregistrer votre domaine avec Azure AD

Par défaut, les utilisateurs sont identifiés avec une adresse e-mail au format : `<user.name>@<company>.onmicrosoft.com`.

Bien que cela fonctionne sans configuration supplémentaire, une adresse e-mail au format standard est préférable, de préférence une qui correspond au compte de messagerie de l'utilisateur final : `<user.name>@<company>.com`.

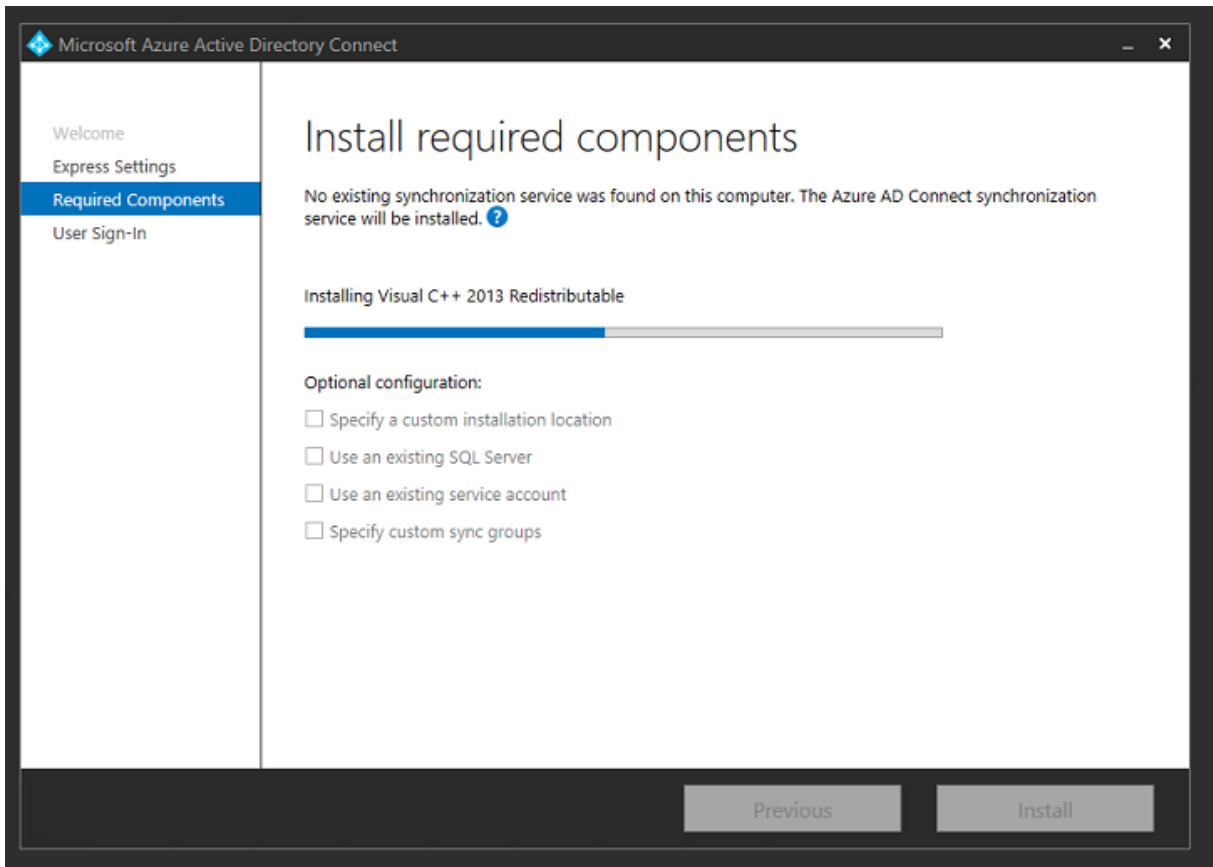
L'action **Ajouter un domaine** configure une redirection de votre domaine d'entreprise réel. L'exemple utilise `citrixsaml-demo.net`.

Si vous configurez ADFS pour l'authentification unique, activez la case à cocher.

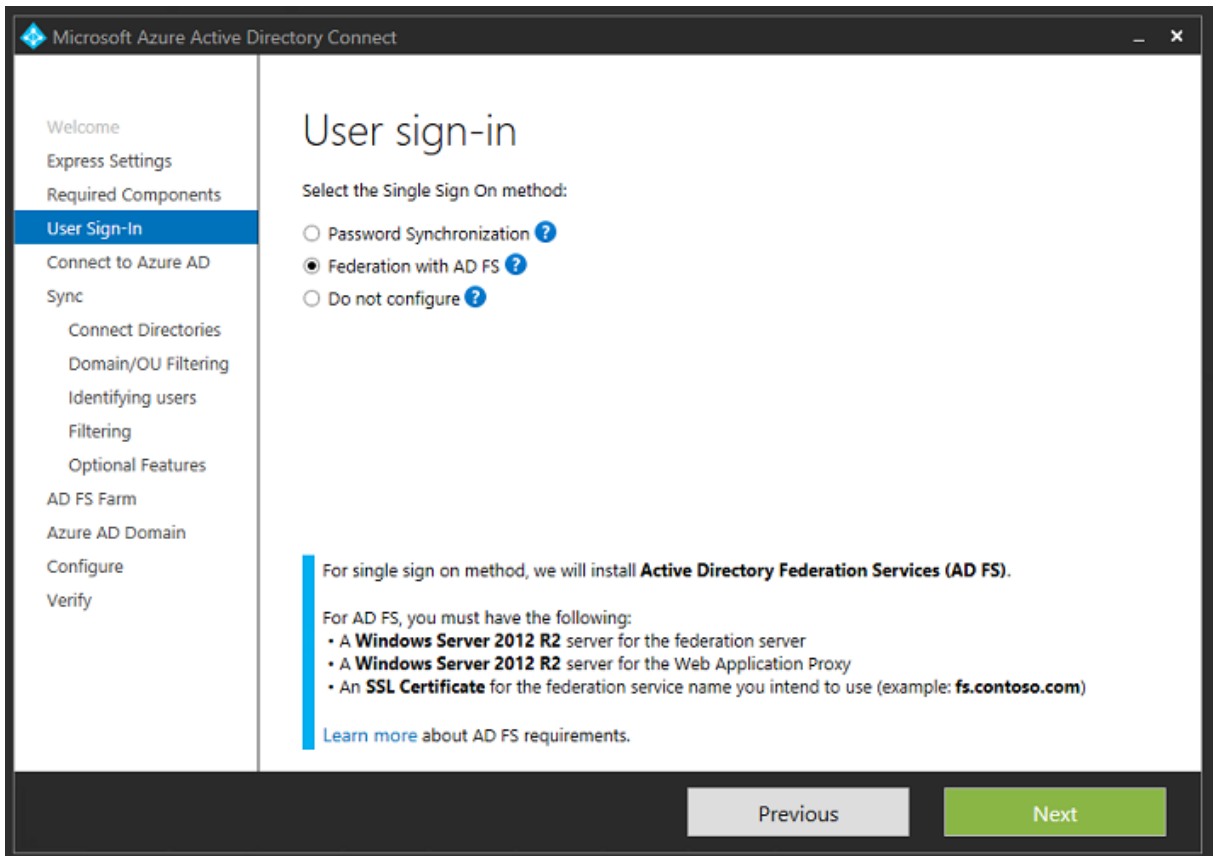


Installer Azure AD Connect

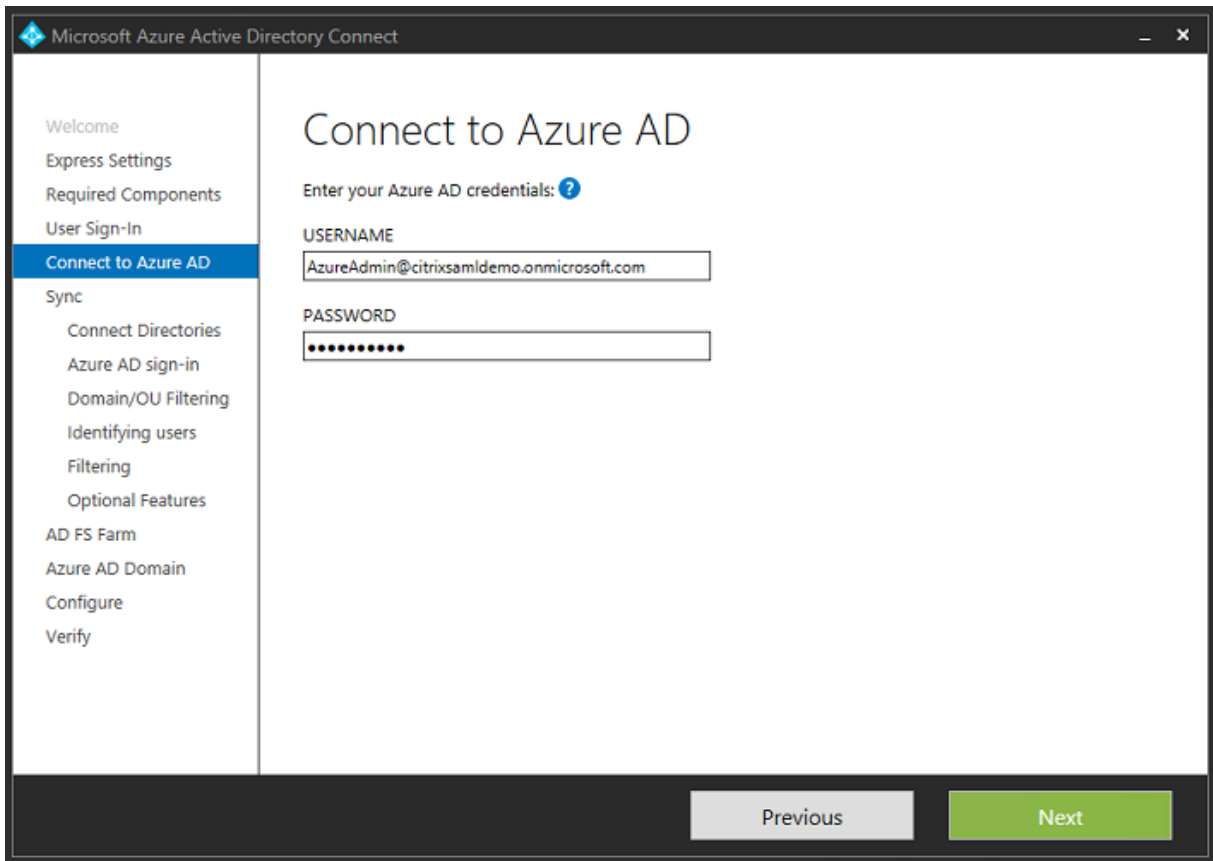
L'étape 2 de l'interface de configuration d'Azure AD redirige l'utilisateur vers la page de téléchargement Microsoft d'Azure AD Connect. Installez ce composant sur la VM ADFS. Utilisez **Installation personnalisée**, plutôt que **Configuration rapide** afin que les options ADFS soient disponibles.



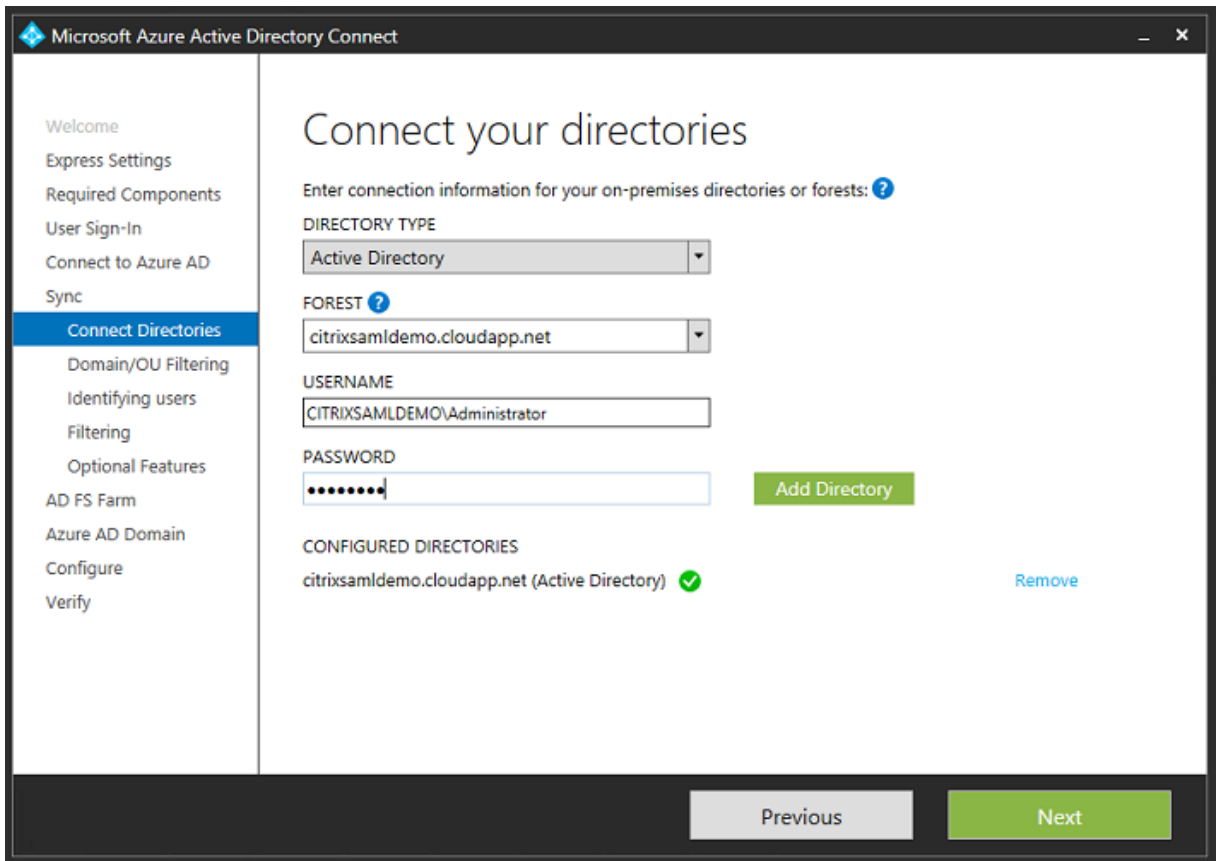
Sélectionnez l'option d'authentification unique **Fédération avec AD FS**.



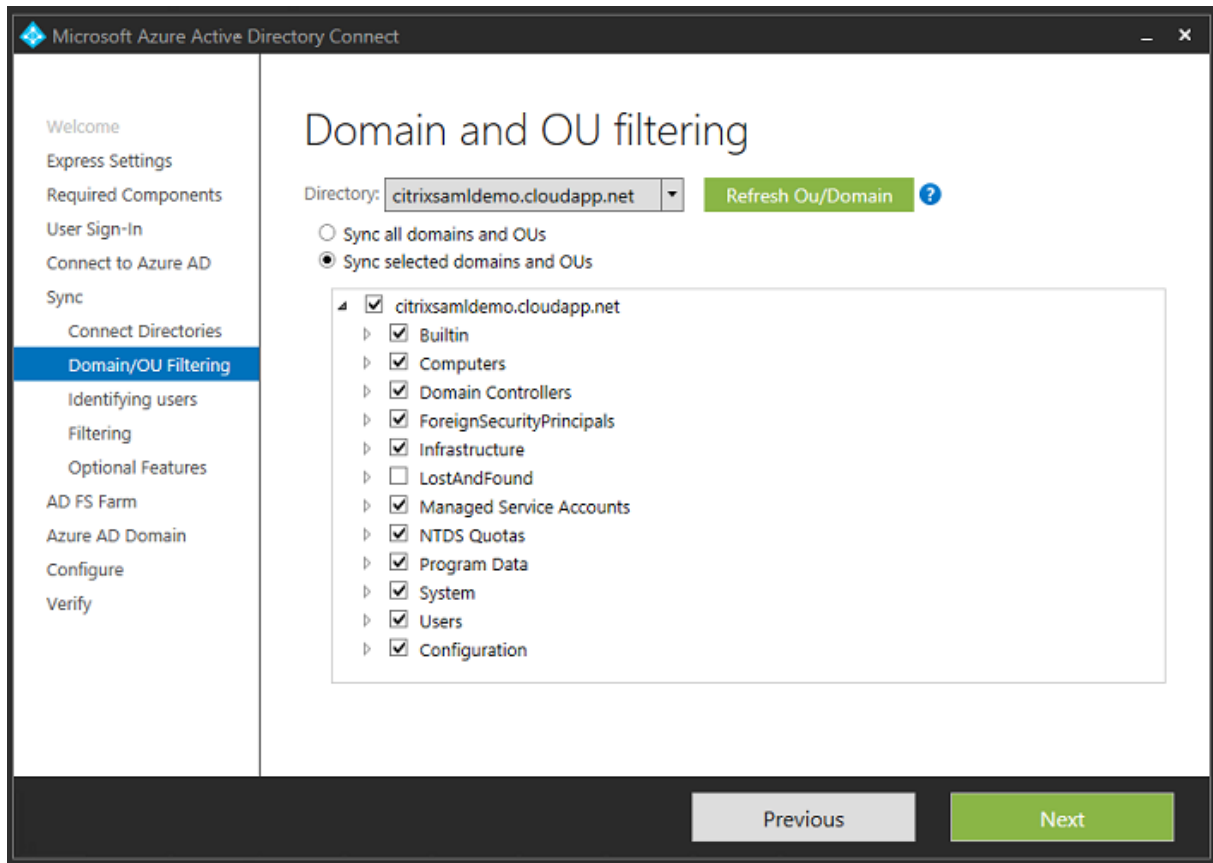
Connectez-vous à Azure avec le compte administrateur que vous avez créé précédemment.



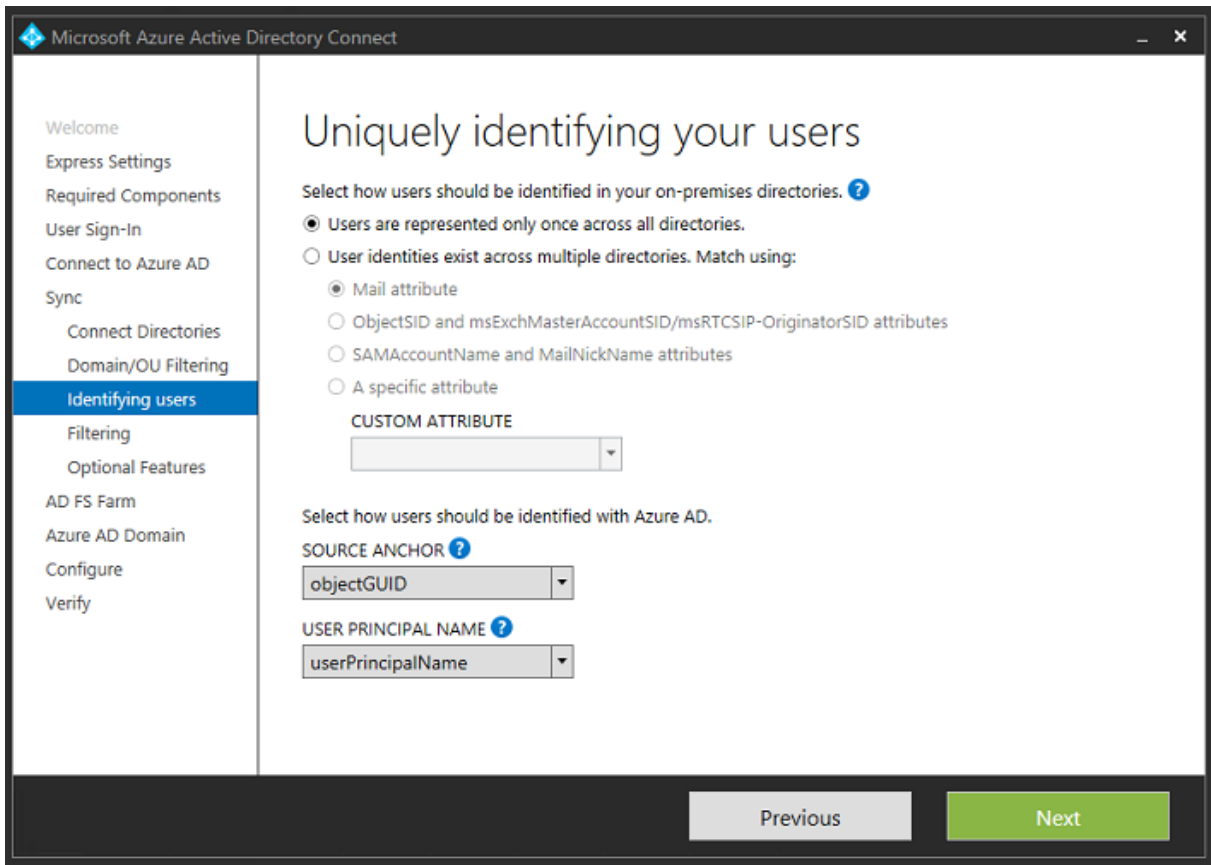
Sélectionnez la forêt AD interne.



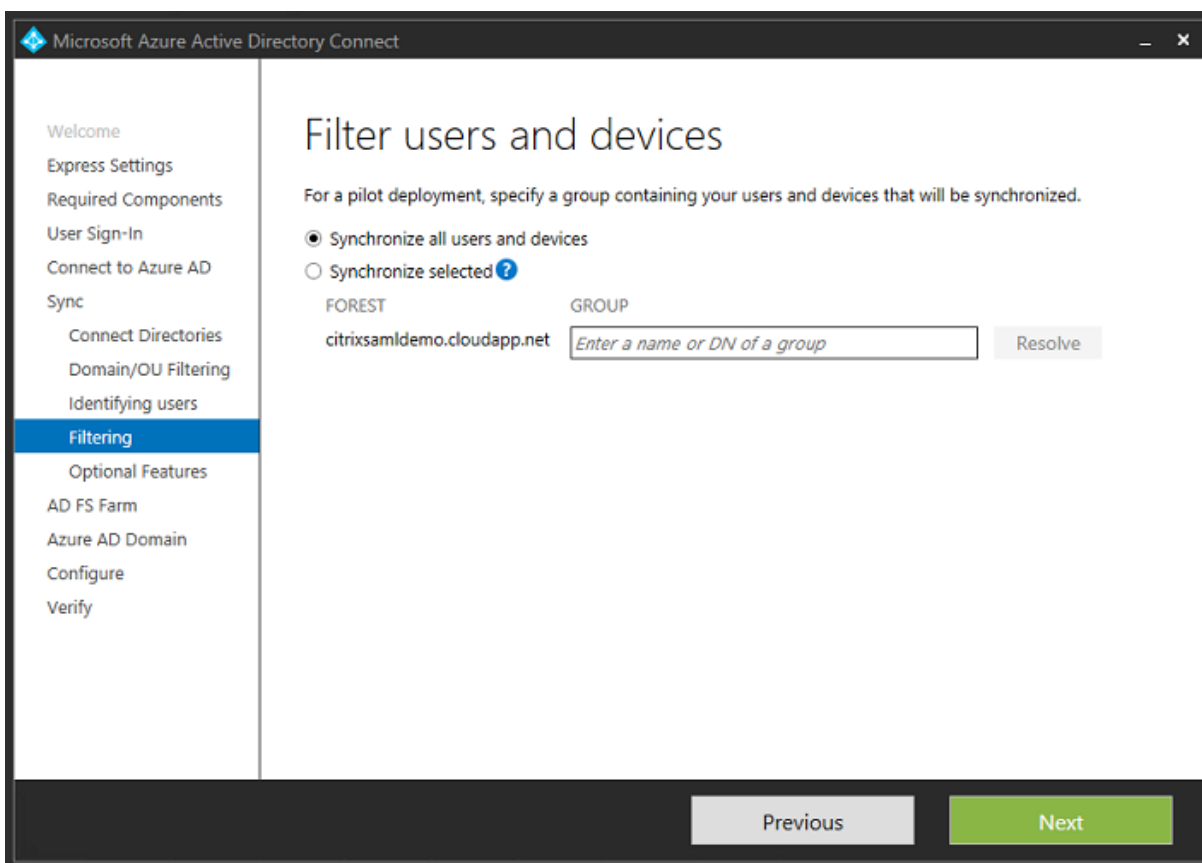
Synchronisez tous les anciens objets Active Directory avec Azure AD.



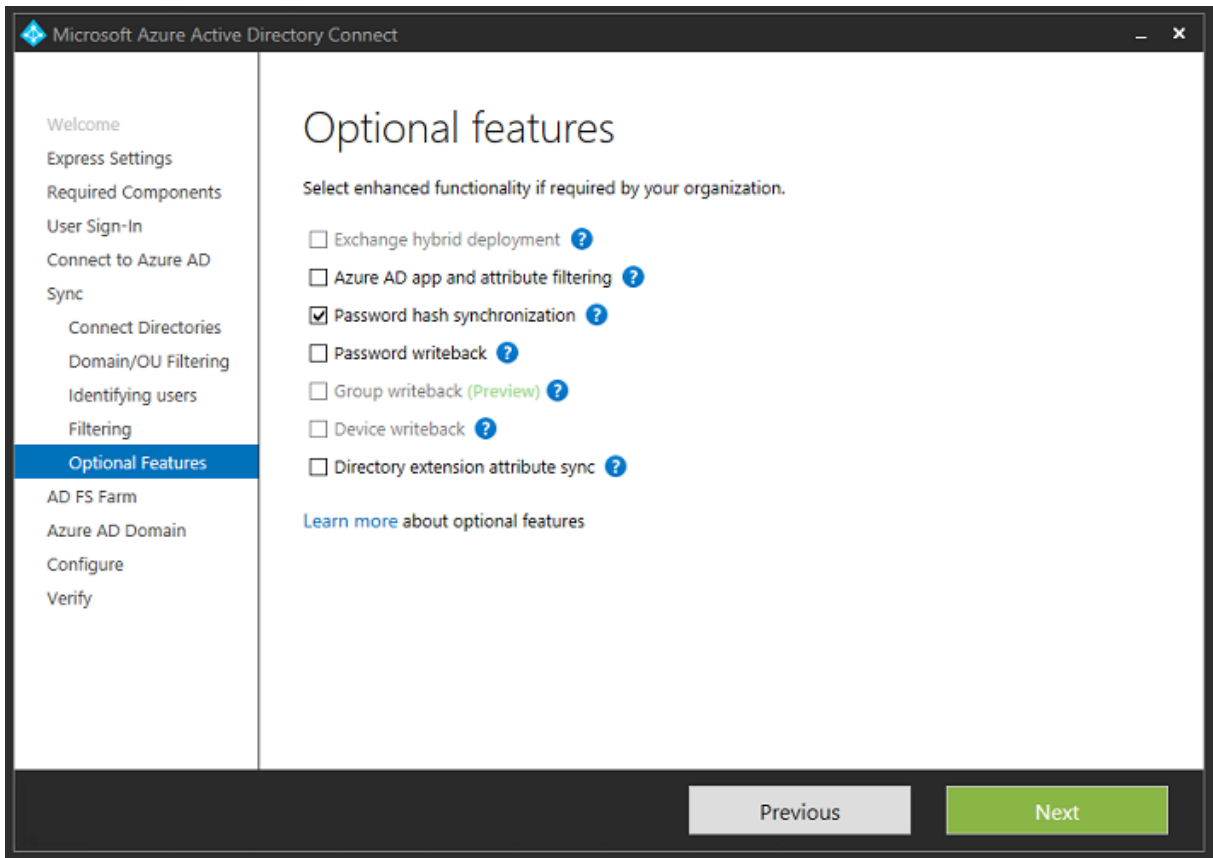
Si la structure de répertoire est simple, les noms d'utilisateur sont suffisamment uniques pour identifier un utilisateur qui ouvre une session.



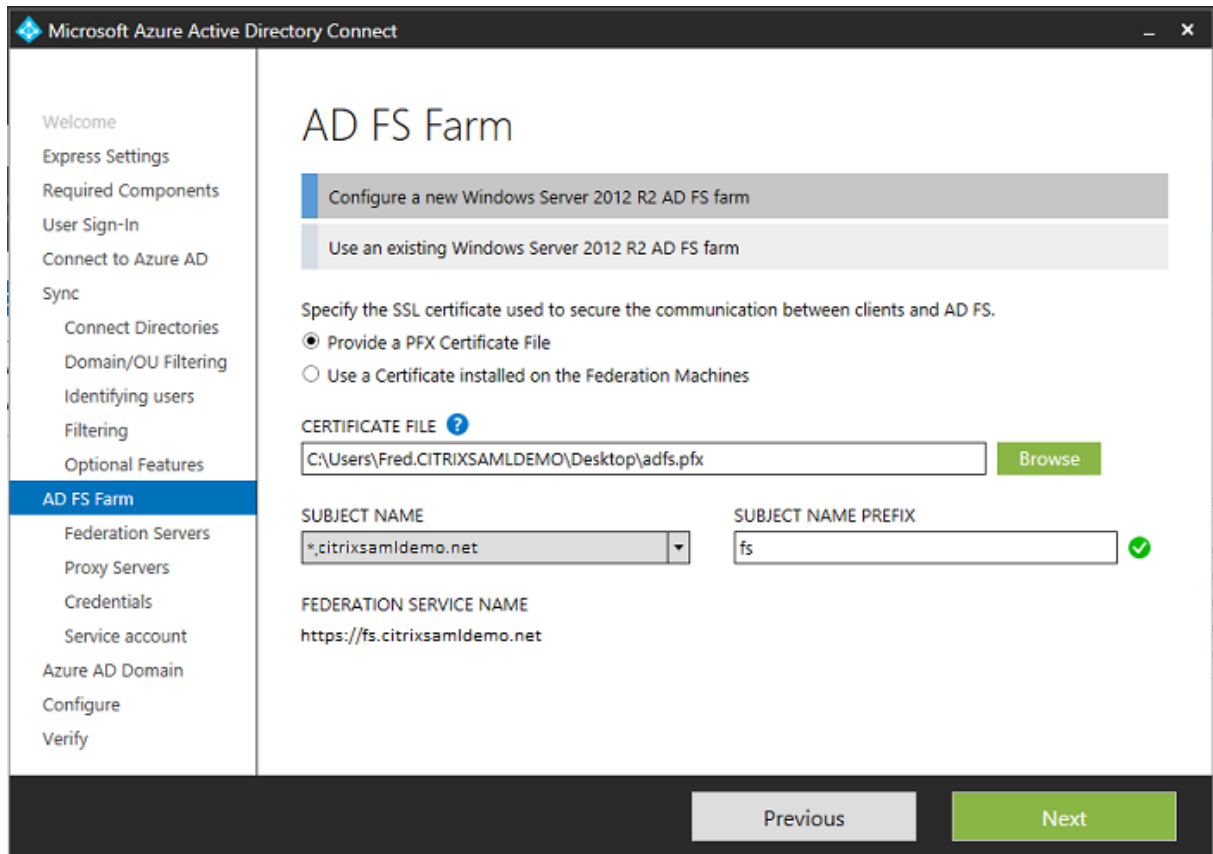
Acceptez les options de filtrage par défaut, ou limitez les utilisateurs et machines à un ensemble de groupes particulier.



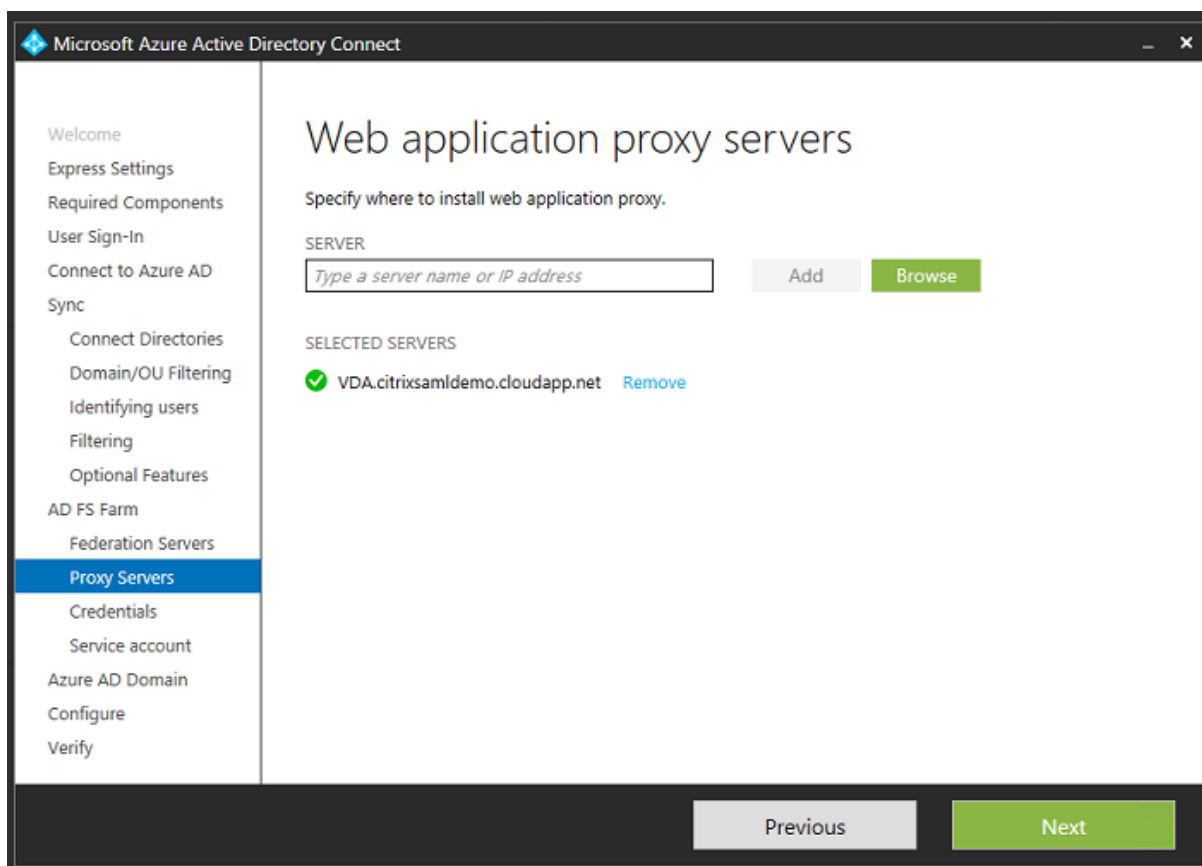
Si vous le souhaitez, vous pouvez synchroniser les mots de passe Azure AD avec Active Directory. Ceci n'est généralement pas nécessaire pour l'authentification ADFS.



Sélectionnez le fichier .pfx de certificat à utiliser dans ADFS, en spécifiant fs.citrixsamldemo.net en tant que nom DNS.



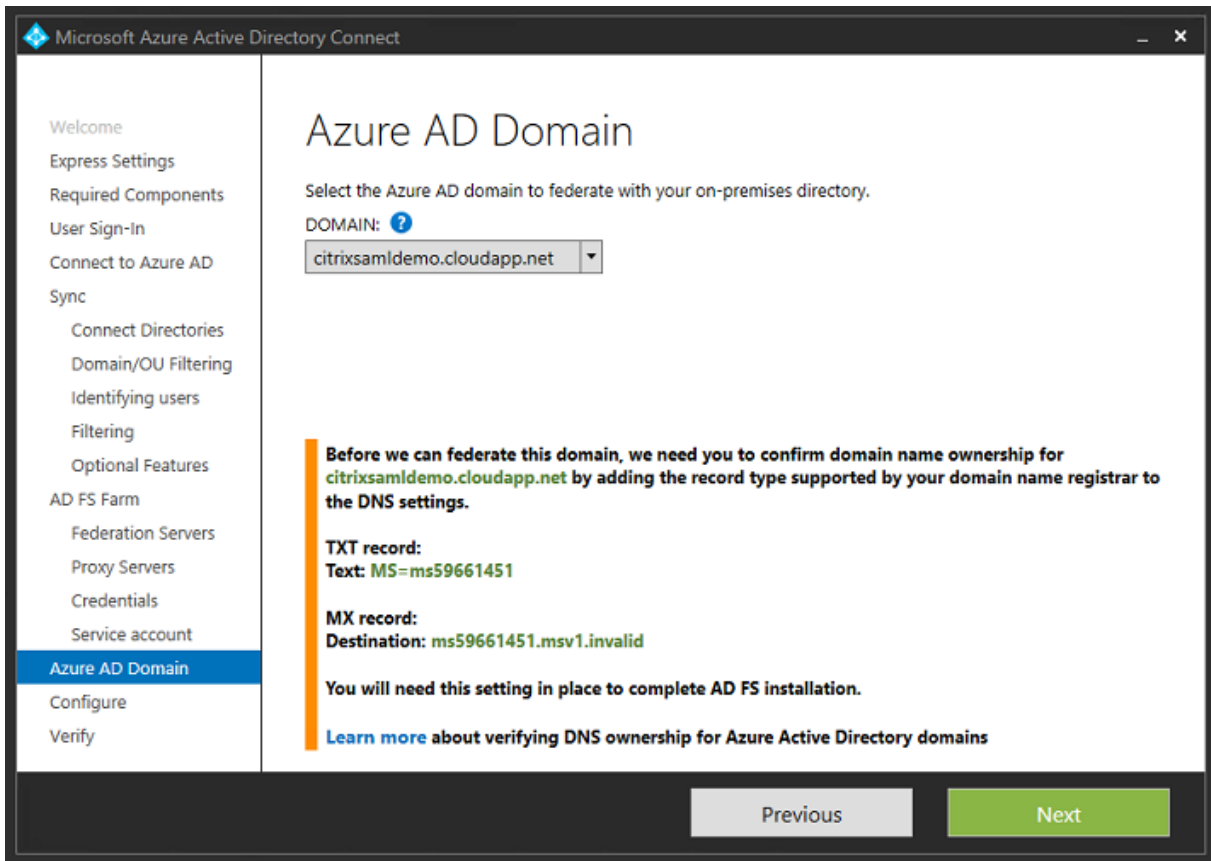
Lorsque vous êtes invité à sélectionner un serveur proxy, entrez l'adresse du serveur `wap.citrixsaml-demo.net`. Vous devrez peut-être exécuter l'applet de commande **Enable-PSRemoting -Force** en tant qu'administrateur sur le serveur proxy d'application Web, de façon à ce que Azure AD Connect puisse le configurer.



Remarque :

Si cette étape échoue en raison de problèmes de confiance avec PowerShell à distance, essayez de joindre le serveur proxy d'application Web au domaine.

Pour les étapes restantes de l'assistant, utilisez les mots de passe de l'administrateur et créez un compte de service pour ADFS. Azure AD Connect vous invitera alors à valider l'appartenance de la zone DNS.





Ajoutez les enregistrements TXT et MX aux enregistrements d'adresses DNS dans Azure.

| Search record sets | | | |
|--------------------|-------|--------|--|
| NAME | TYPE | TTL | VALUE |
| @ | NS | 172800 | ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info. ... |
| @ | SOA | 3600 | Email: azuredns-hostmaster.microsoft... Host: ns1-01.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 ... |
| @ | TXT | 3600 | ms70102213 ... |
| fs | CNAME | 3600 | adfs-citrixsaml-demo.westeurope.cloud... .. |

Cliquez sur **Vérier** dans la console de gestion Azure.

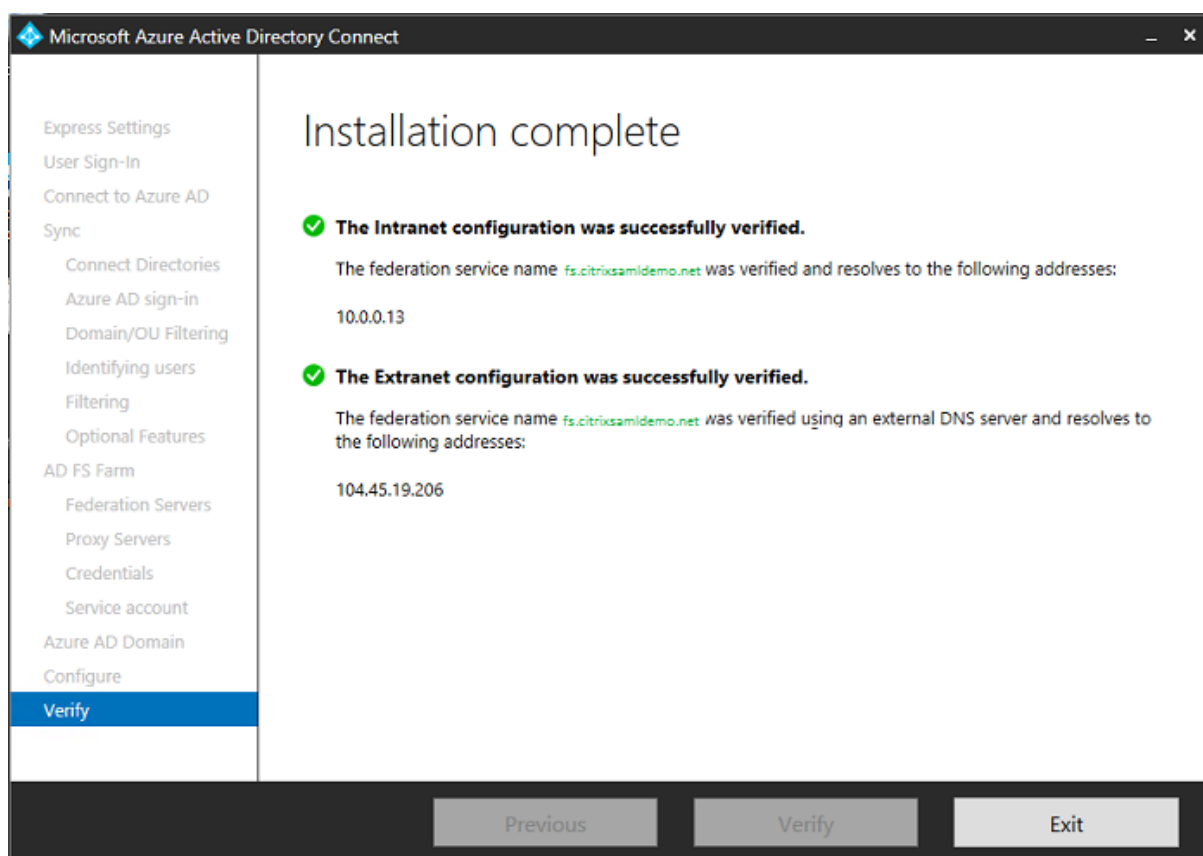
CitrixSamlDemo

|  | USERS | GROUPS | APPLICATIONS | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS | LICENSES |
|---|-----------------------|------------------------|------------------------------|----------------|---|---------------------------|-------------------------|--------------------------|
| DOMAIN NAME | TYPE | STATUS | SINGLE SIGN-ON | PRIMARY DOMAIN |  | | | |
| citrixsamldemo.onmicrosoft.com | Basic | ✓ Active | Not Available | Yes | | | | |
| citrixsamldemo.net | Custom | ⚠ Unverified | Not Configured | No | | | | |

Remarque :

Si cette étape échoue, vous pouvez vérifier le domaine avant d'exécuter Azure AD Connect.

Lorsque l'installation est terminée, l'adresse externe fs.citrixsamldemo.net est contactée sur le port 443.



Activer Azure AD Join (Jonction à un domaine Azure AD)

Lorsqu'un utilisateur entre une adresse e-mail afin que Windows 10 puisse réaliser la jonction Azure AD, le suffixe DNS est utilisé pour construire un enregistrement DNS CNAME qui doit pointer vers ADFS : enterpriseregistration.<suffixeupn>.

Dans l'exemple, c'est `fs.citrixsaml demo.net`.

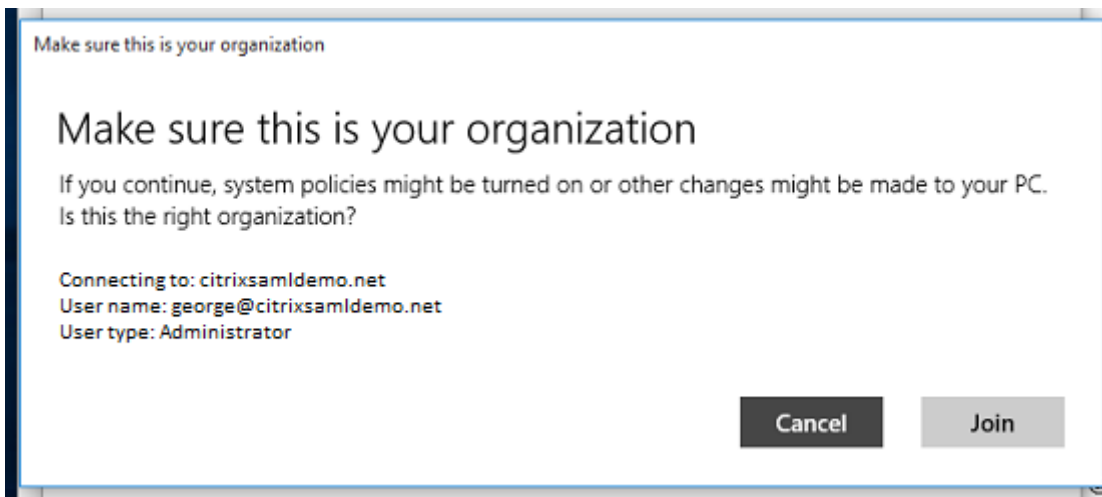
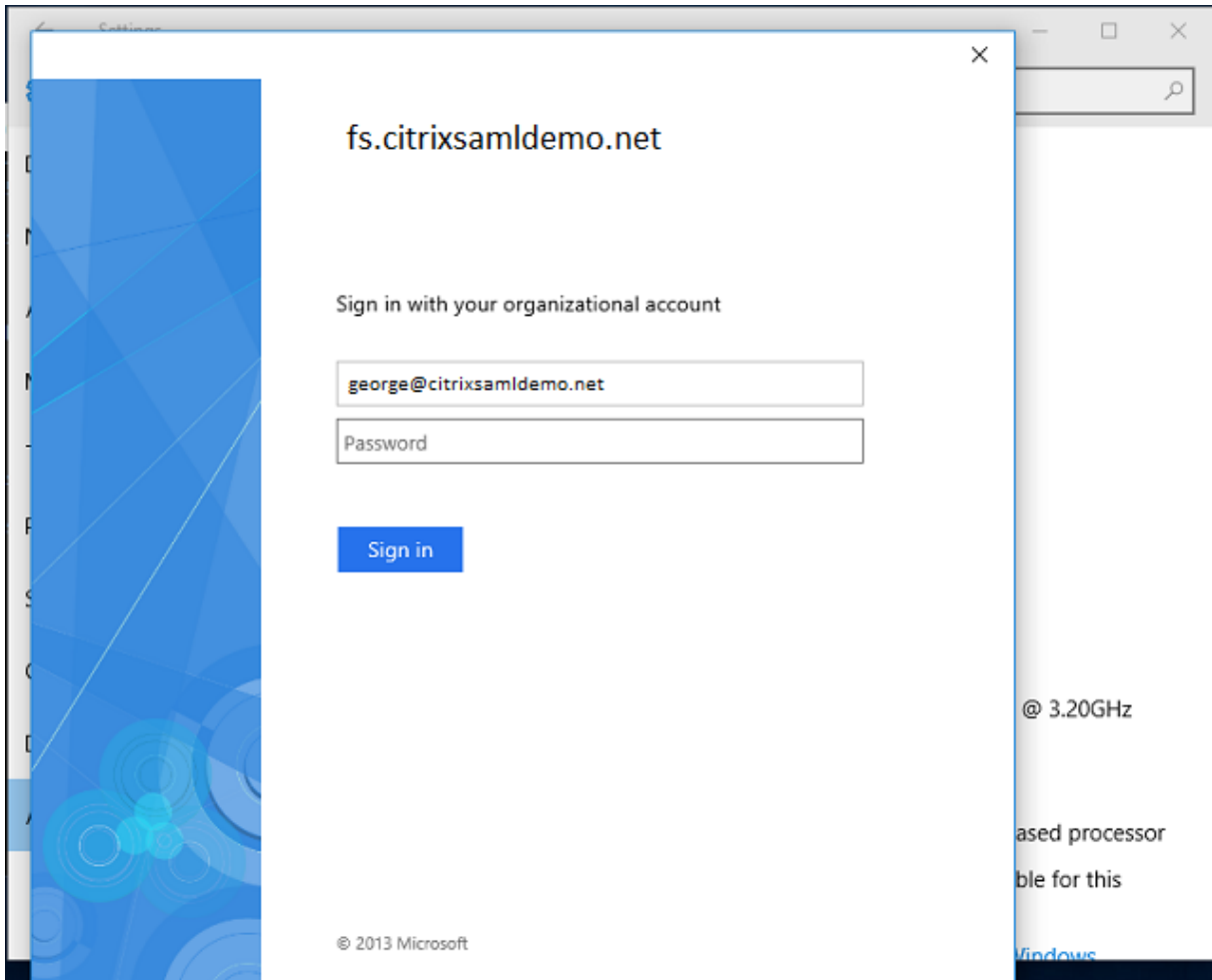
The screenshot shows a DNS record configuration interface. At the top, there is a text input field containing the domain `enterpriseregistration.citrixsaml demo.net` with a copy icon to its right. Below this, the record type is set to `CNAME`. The TTL is set to `1` with a green checkmark, and the TTL unit is set to `Minutes` with a dropdown arrow. The Alias field contains `fs.citrixsaml demo.net` with a green checkmark.

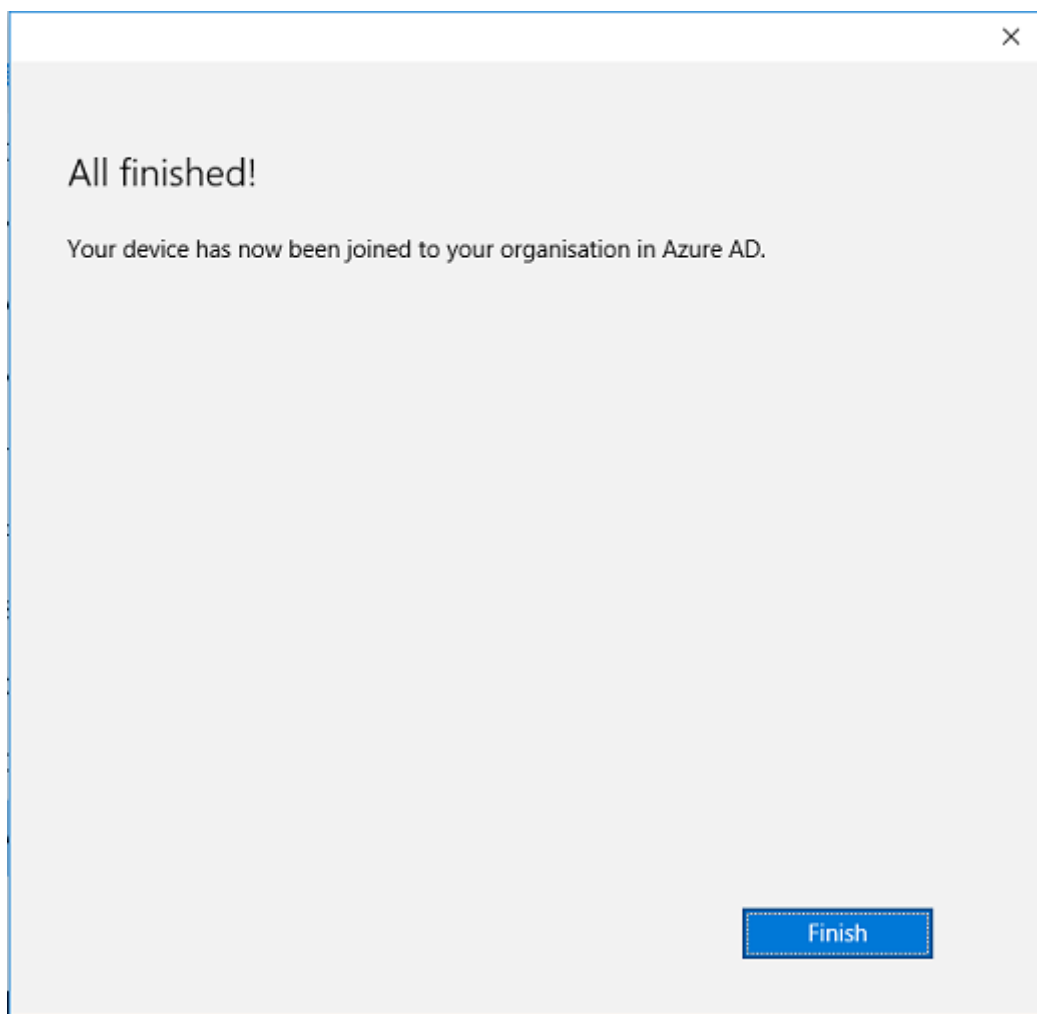
Si vous n'utilisez pas d'autorité de certification publique, assurez-vous que le certificat racine ADFS est installé sur l'ordinateur Windows 10 de façon à ce que Windows fasse confiance au serveur ADFS. Effectuez une jonction de domaine Azure AD à l'aide du compte utilisateur standard généré précédemment.

The screenshot shows a Windows login screen titled "Let's get you signed in". It is for a "Work or school account". The username field contains `George@citrixsaml demo.net` and the password field is labeled "Password". There is a link for "I forgot my password". Below the login fields, there is a section titled "Which account should I use?" with the text "Sign in with the username and password you use with Office 365 (or other business services from Microsoft)." and a link for "Privacy statement". At the bottom right, there are two buttons: "Sign in" (blue) and "Back" (grey).

Veuillez noter que le nom UPN doit correspondre au nom UPN reconnu par le contrôleur de domaine

ADFS.



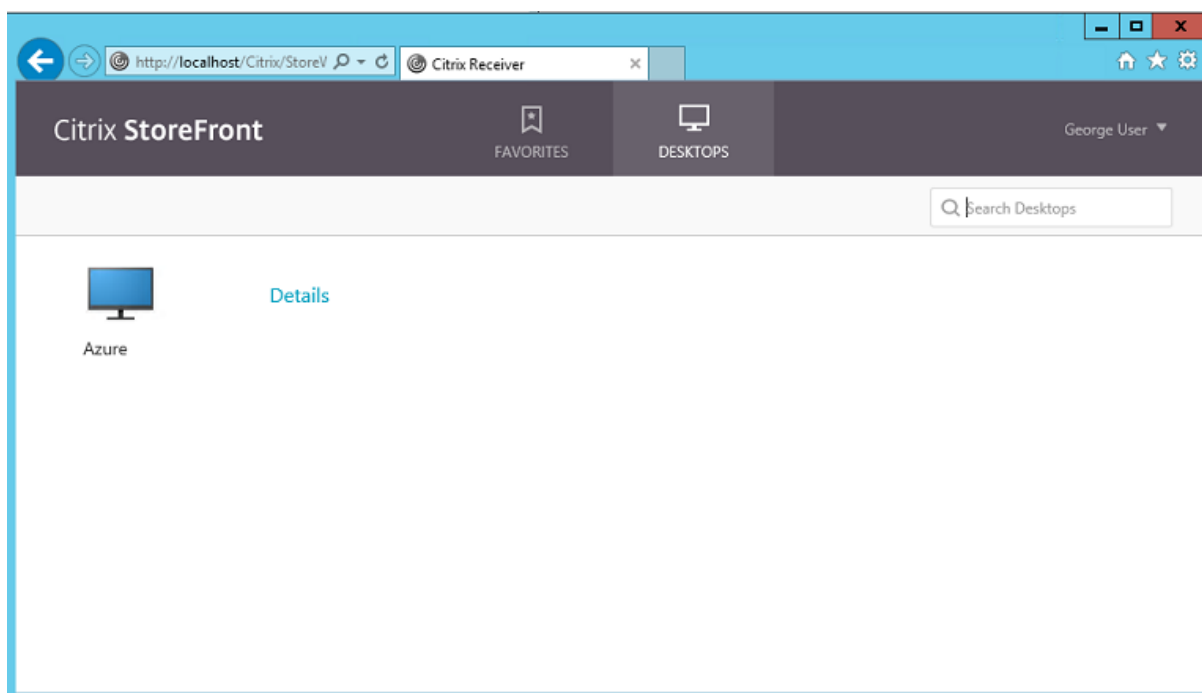


Vérifiez que la jonction Azure AD a réussi en redémarrant la machine et en ouvrant une session à l'aide de l'adresse e-mail de l'utilisateur. Une fois connecté, lancez Microsoft Edge et connectez-vous à <http://myapps.microsoft.com>. Le site Web doit utiliser l'authentification unique automatiquement.

Installer Citrix Virtual Apps ou Citrix Virtual Desktops

Vous pouvez installer le Delivery Controller et des machines virtuelles VDA dans Azure directement depuis l'ISO Citrix Virtual Apps ou Citrix Virtual Desktops de la manière habituelle.

Dans cet exemple, StoreFront est installé sur le même serveur que le Delivery Controller. Le VDA est installé en tant que travailleur RDS Windows 2012 R2 autonome, sans intégration avec Machine Creation Services (mais cela peut être configuré). Vérifiez que l'utilisateur `George@citrixsamldemo.net` peut s'authentifier avec un mot de passe avant de continuer.



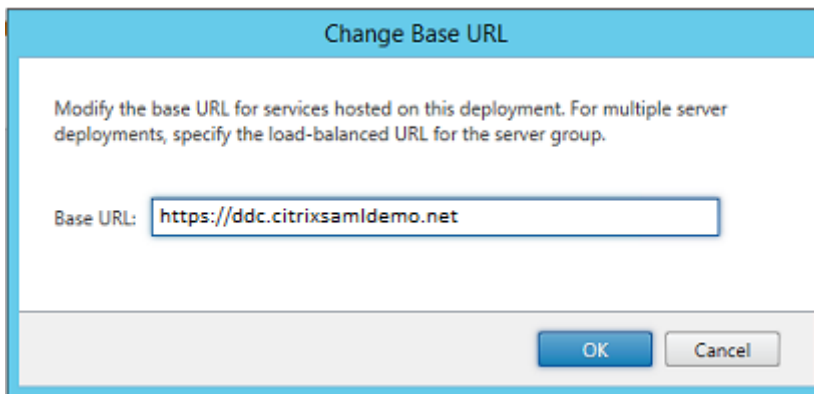
Exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** sur le Contrôleur pour permettre à StoreFront de s'authentifier sans les informations d'identification de l'utilisateur.

Installer le Service d'authentification fédérée

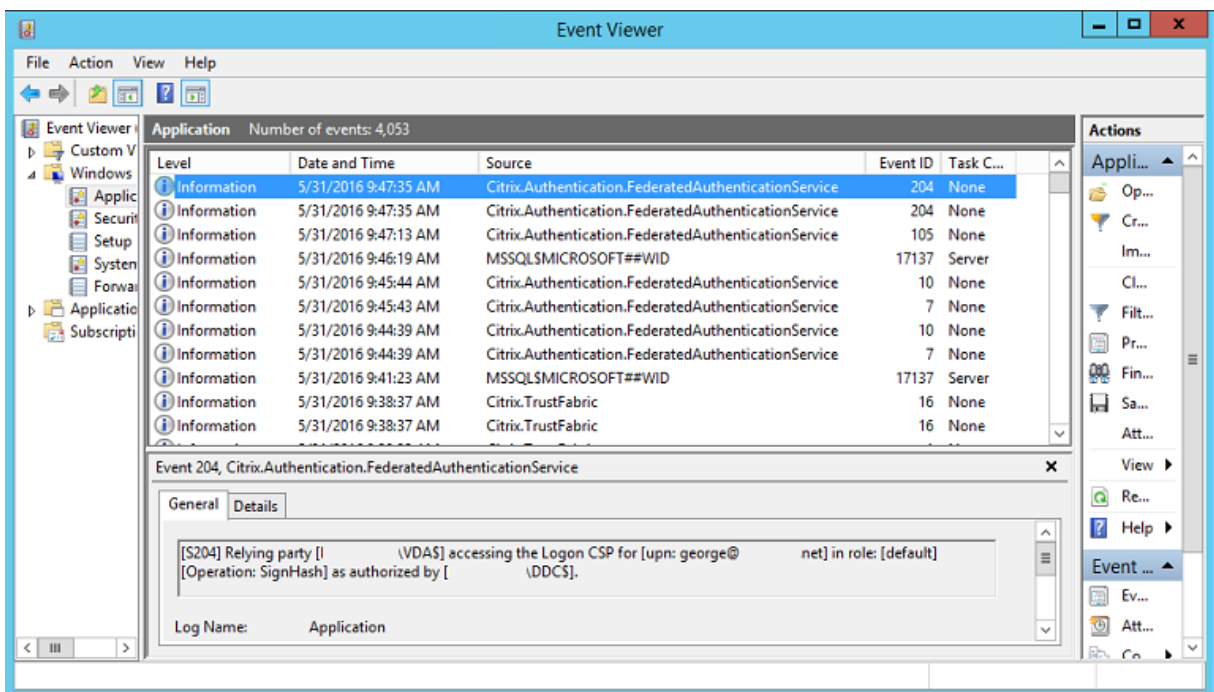
Installez FAS sur le serveur ADFS et configurez une règle pour faire en sorte que le Delivery Controller agisse en tant que StoreFront approuvé (dans cet exemple, StoreFront est installé sur la même VM que le Delivery Controller). Consultez [Installer et configurer](#).

Configurer StoreFront

Demandez un certificat d'ordinateur pour le Delivery Controller, et configurez IIS et StoreFront pour utiliser HTTPS en définissant une liaison IIS pour le port 443 et en modifiant l'adresse de base de StoreFront sur https:.

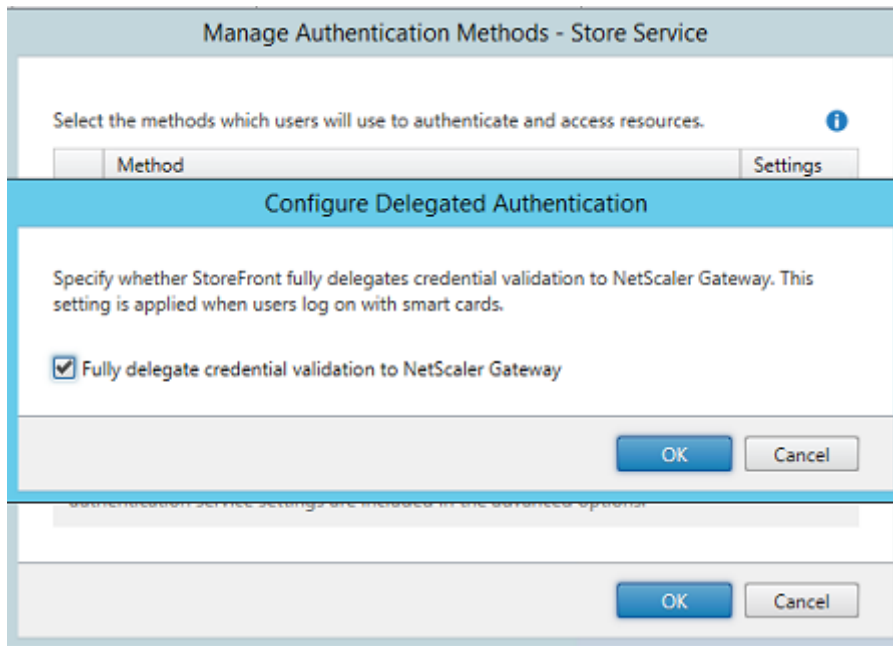


Configurez StoreFront pour utiliser le serveur FAS (utilisez le script PowerShell dans l'article [Installer et configurer](#)) et effectuez des tests en interne dans Azure, en vous assurant que l'ouverture de session utilise FAS en vérifiant l'observateur d'événements sur le serveur FAS.

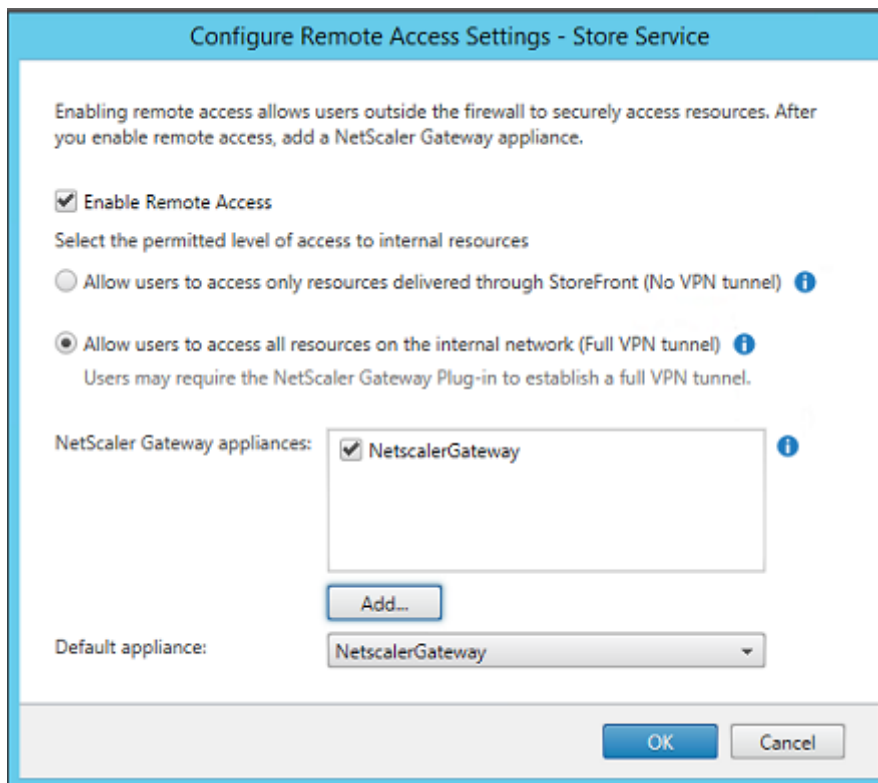


Configurer StoreFront pour utiliser Citrix Gateway

À l'aide de l'interface **Gérer les méthodes d'authentification** de la console de gestion StoreFront, configurez StoreFront de manière à ce qu'il utilise Citrix Gateway pour l'authentification.

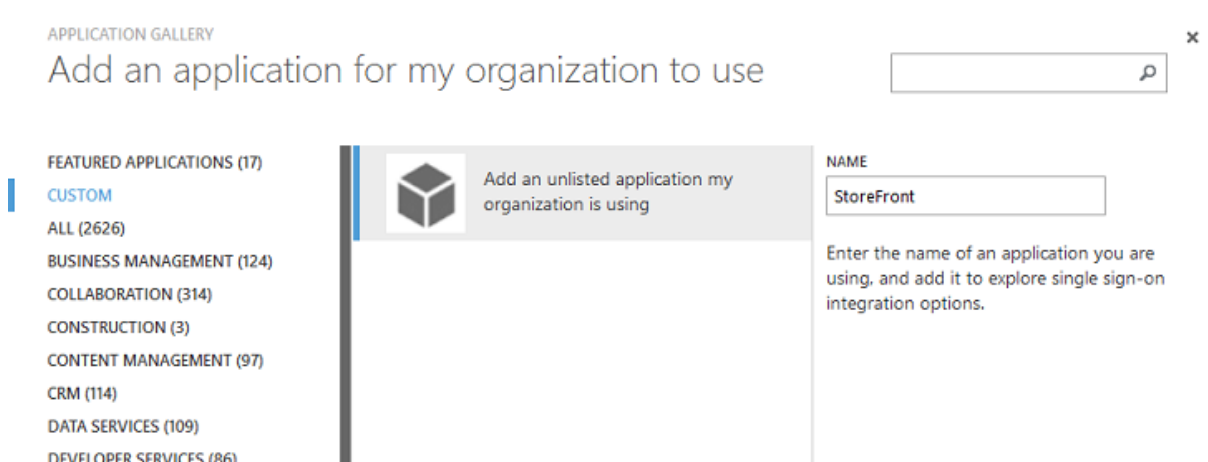


Pour intégrer les options d'authentification Citrix Gateway, configurez une STA (Secure Ticket Authority) et configurez l'adresse Citrix Gateway.



Configurer une nouvelle application Azure AD pour le Single Sign-On sur StoreFront

Cette section utilise les fonctionnalités d'authentification unique d'Azure AD SAML 2.0, qui requièrent un abonnement Azure Active Directory Premium. Dans l'outil de gestion Azure AD, sélectionnez **Nouvelle application** et **Ajouter une application à partir de la galerie**.



Sélectionnez **PERSONNALISER > Ajouter une application non répertoriée que mon organisation utilise** pour créer une nouvelle application personnalisée pour vos utilisateurs.

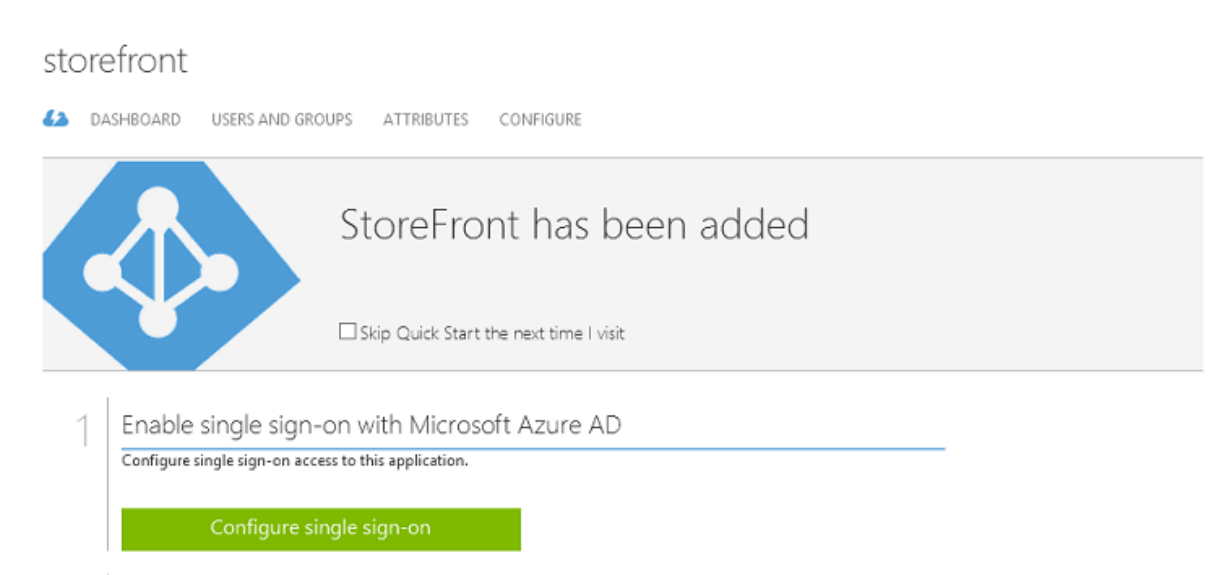
Configurer une icône

Créez une image de 215 x 215 pixels et chargez-la sur la page CONFIGURER pour l'utiliser comme icône pour l'application.

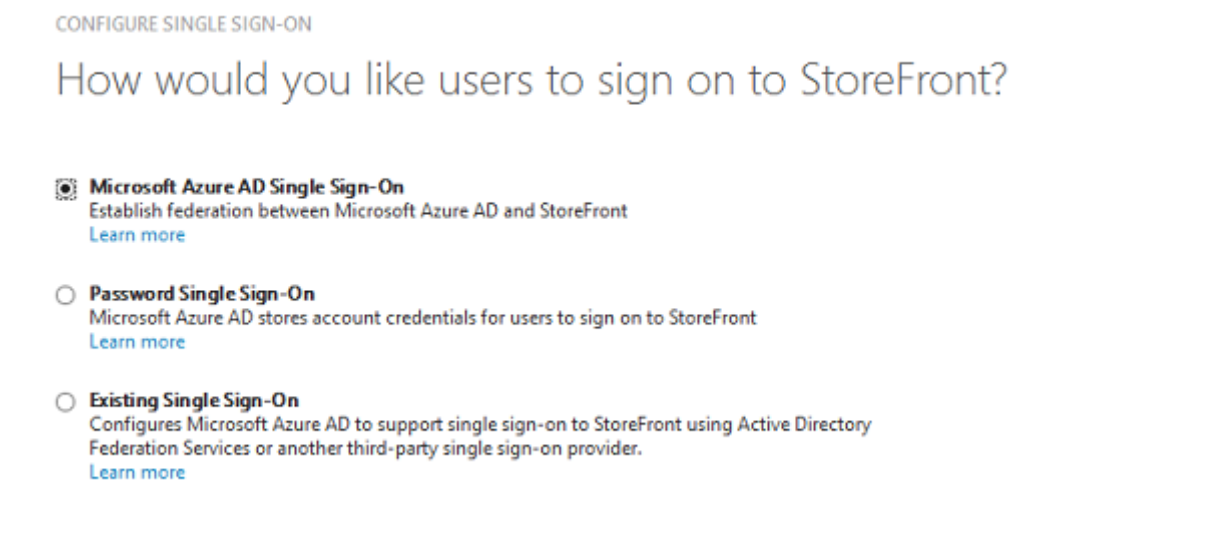


Configurer l'authentification SAML

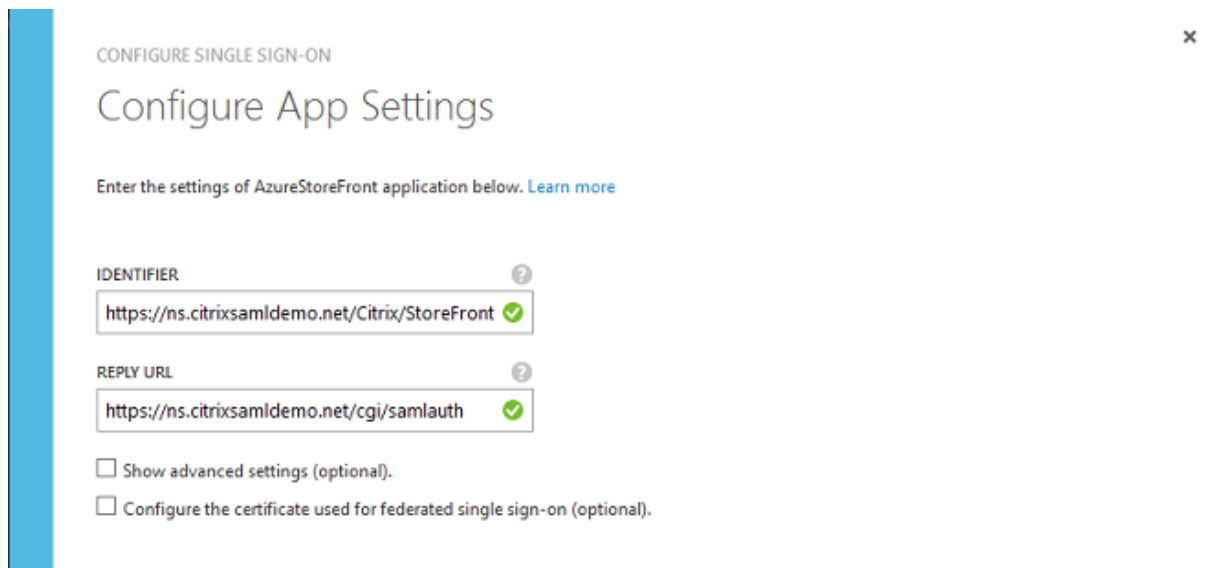
Retournez sur la page de tableau de bord de l'application et sélectionnez **Configurer l'authentification unique**.



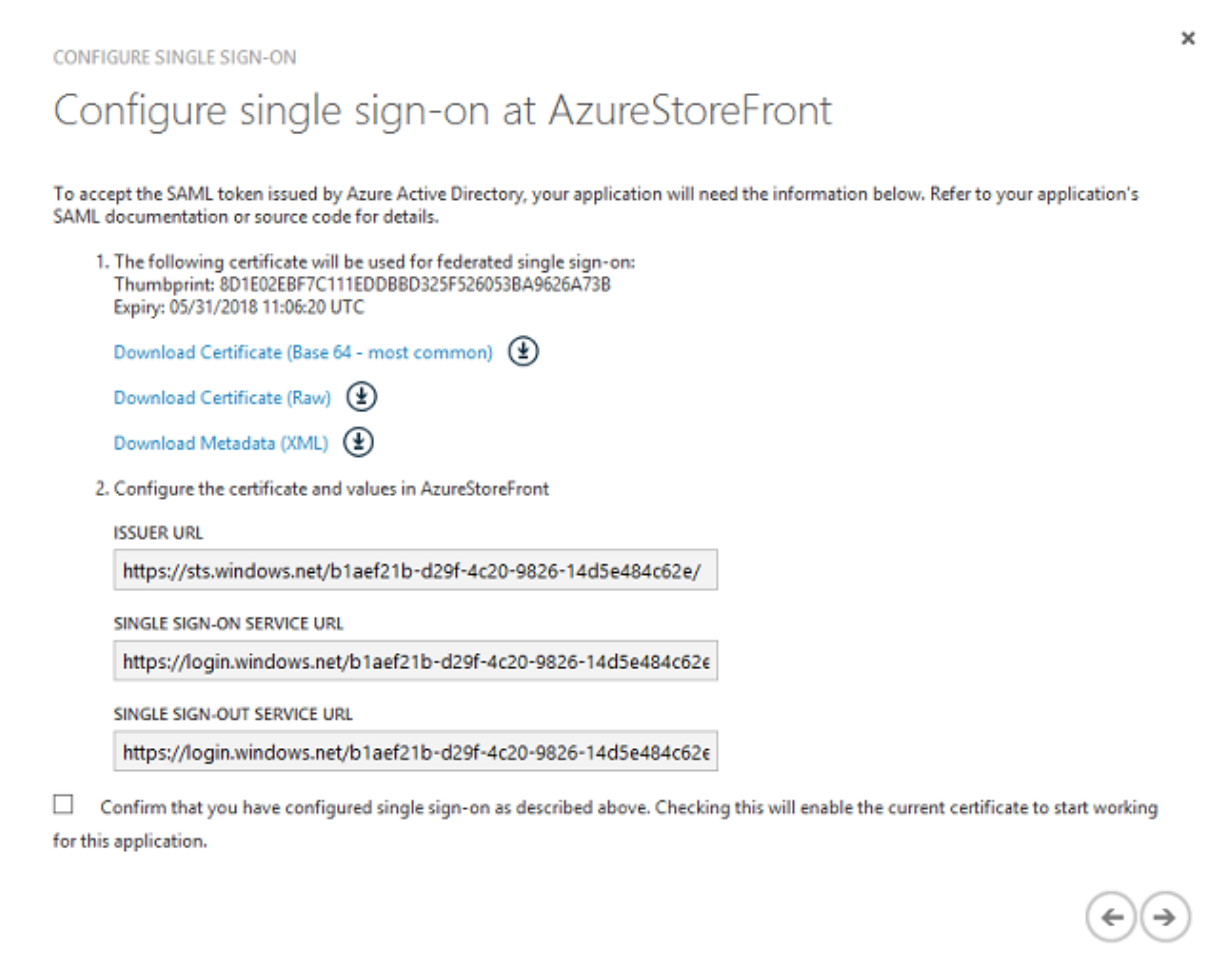
Ce déploiement utilise l'authentification SAML 2.0, qui correspond à **Authentification unique avec Microsoft Azure AD**.



L'**identificateur** peut être une chaîne arbitraire (doit correspondre à la configuration fournie à Citrix Gateway) ; dans cet exemple, l'**URL de réponse** est `/cgi/samlauth` sur le serveur Citrix Gateway.



La page suivante contient des informations qui sont utilisées pour configurer Citrix Gateway en tant que partie de confiance pour Azure AD.



Téléchargez le certificat de signature approuvé base 64 et copiez les URL de connexion et de décon-

nexion. Collez ces dernières dans les écrans de configuration de Citrix Gateway qui suivent.

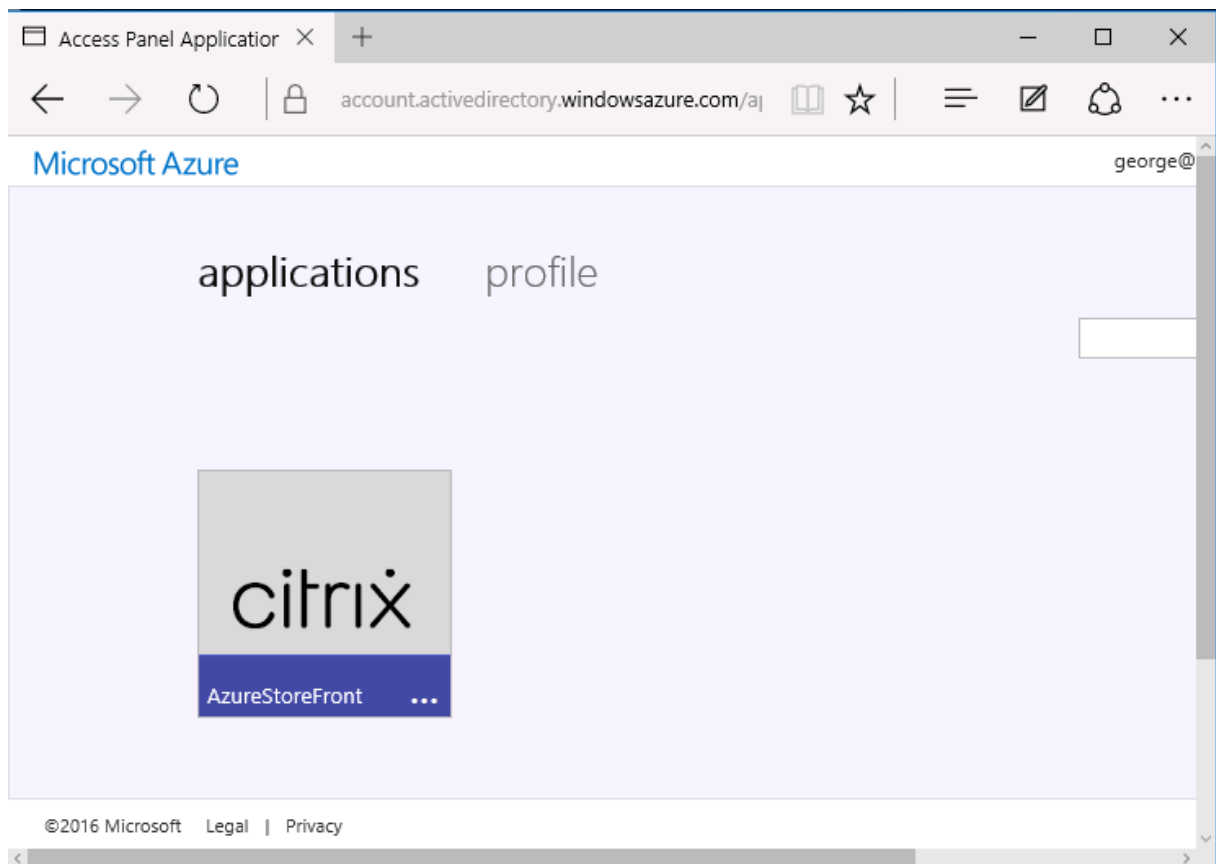
Attribuer l'application aux utilisateurs

La dernière étape consiste à activer l'application afin qu'elle apparaisse sur la page de contrôle "myapps.microsoft.com" des utilisateurs. Cette opération est réalisée sur la page UTILISATEURS ET GROUPEs. Attribuez l'accès aux comptes d'utilisateurs de domaine synchronisés par Azure AD Connect. D'autres comptes peuvent également être utilisés, mais ils doivent être explicitement mappés car ils ne sont pas conformes au format <utilisateur>@<domaine>.



Page MyApps

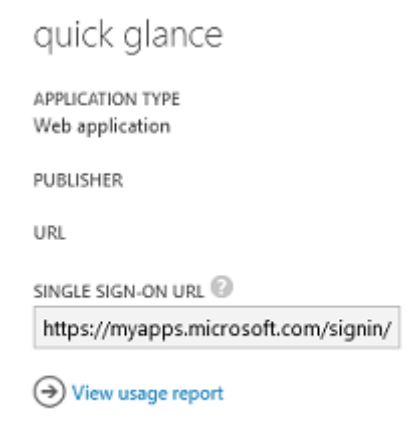
Lorsque l'application a été configurée, elle s'affiche dans les listes d'applications Azure des utilisateurs lorsqu'ils visitent <https://myapps.microsoft.com>.



Lorsqu'il est joint à Azure AD, Windows Azure 10 prend en charge l'authentification unique aux applications Azure pour l'utilisateur qui ouvre une session. Le fait de cliquer sur l'icône dirige le navigateur vers la page Web SAML `cgi/samlauth` qui a été configurée précédemment.

URL d'authentification unique

Retournez à l'application dans le tableau de bord Azure AD. Une adresse URL d'authentification unique est maintenant disponible pour l'application. Cette adresse URL est utilisée pour fournir des liens de navigateur Web ou pour créer des raccourcis du menu Démarrer qui dirigent les utilisateurs directement dans StoreFront.



Collez cette adresse URL dans un navigateur Web pour vous assurer que vous êtes redirigé par Azure AD sur la page Web Citrix Gateway `cgi/samlauth` configurée précédemment. Ceci fonctionne uniquement pour les utilisateurs qui ont été attribués, et fournira l'authentification unique uniquement aux sessions Windows 10 jointes à Azure AD. (Les autres utilisateurs seront invités à entrer des informations d'identification Azure AD).

Installer et configurer Citrix Gateway

Pour accéder à distance au déploiement, cet exemple utilise une VM distincte exécutant NetScaler (désormais appelé Citrix Gateway). Cela peut être acheté sur le Azure Store. Cet exemple utilise la version « BYOL » (avec apport de sa propre licence) de NetScaler 11.0.

Ouvrez une session sur la VM NetScaler en pointant un navigateur Web sur l'adresse IP interne et en entrant les informations d'identification spécifiées lorsque l'utilisateur s'est authentifié. Notez que vous devez modifier le mot de passe de l'utilisateur `nsroot` dans la VM Azure AD.

Ajoutez des licences en sélectionnant **redémarrer** après l'ajout de chaque fichier de licences, puis pointez la résolution DNS vers le contrôleur de domaine Microsoft.

Exécuter l'assistant de configuration Citrix Virtual Apps and Desktops

Cet exemple démarre en configurant une intégration StoreFront simple sans SAML. Une fois que le déploiement est opérationnel, il ajoute une stratégie d'ouverture de session SAML.

XenApp/XenDesktop Setup Wizard

What is your deployment



What is your Citrix Integration Point?

StoreFront

Continue

Cancel

Sélectionnez les paramètres Citrix Gateway StoreFront standard. À des fins d'utilisation dans Microsoft Azure, cet exemple configure le port 4433, plutôt que le port 443. Vous pouvez également transférer le port ou remapper le site Web d'administration Citrix Gateway.

NetScaler Gateway Settings

NetScaler Gateway IP Address*

10 . 0 . 0 . 18

Port*

4433

Virtual Server Name*

ns.citrixsaml demo.net

Redirect requests from port 80 to secure port

Continue

Cancel

À des fins de simplicité, l'exemple charge un certificat de serveur existant et la clé privée stockée dans un fichier.

Server Certificate

Certificate Format*
pem

Certificate File*
ns.citrixsamldemo.net

Private key is password protected

Private key password
●●●●●●

Configurer le contrôleur de domaine pour la gestion de comptes AD

Le contrôleur de domaine sera utilisé pour la résolution de compte, il convient donc d'ajouter son adresse IP dans la méthode d'authentification principale. Notez les formats attendus dans chaque champ de la boîte de dialogue.

Primary authentication method*
Active Directory/LDAP

IP Address*
10 . 0 . 0 . 12 IPv6

Load Balancing

Port*
389

Time out (seconds)*
3

Base DN*
CN=Users,DC= citrixsamldemo .DC

Service account*
CN=internaladmin,CN=Users,DC=

Group Extraction

Server Logon Name Attribute*
userPrincipalName

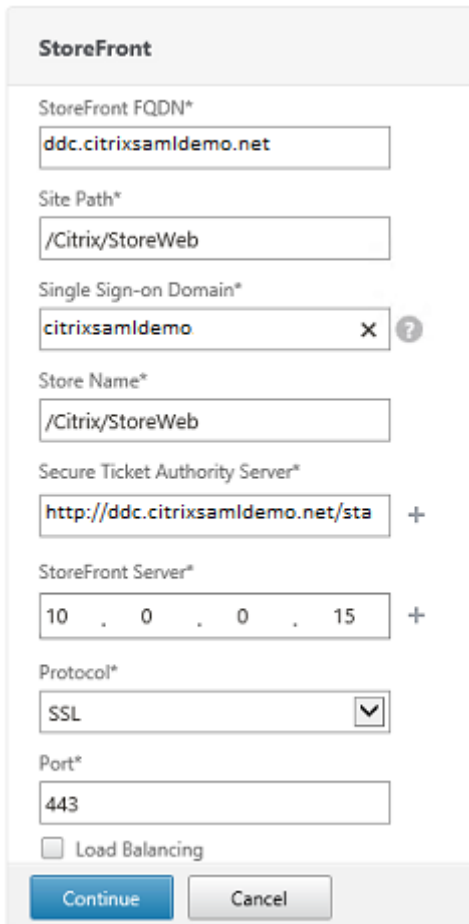
Password*
●●●●●●

Confirm Password*
●●●●●●

Secondary authentication method*
None

Configurer l'adresse de StoreFront

Dans cet exemple, StoreFront a été configuré avec HTTPS, vous devez donc sélectionner les options du protocole SSL.



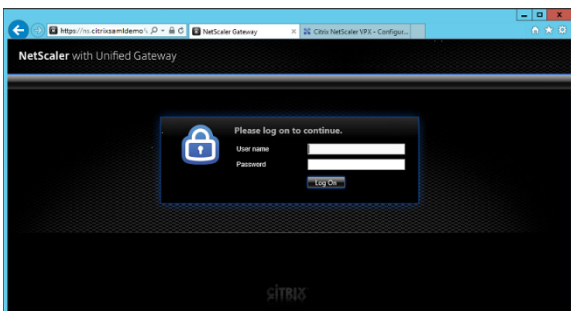
The screenshot shows a configuration window titled "StoreFront". It contains several input fields and a dropdown menu:

- StoreFront FQDN***: ddc.citrixsamldemo.net
- Site Path***: /Citrix/StoreWeb
- Single Sign-on Domain***: citrixsamldemo
- Store Name***: /Citrix/StoreWeb
- Secure Ticket Authority Server***: http://ddc.citrixsamldemo.net/sta
- StoreFront Server***: 10 . 0 . 0 . 15
- Protocol***: SSL (selected in a dropdown menu)
- Port***: 443
- Load Balancing

At the bottom, there are "Continue" and "Cancel" buttons.

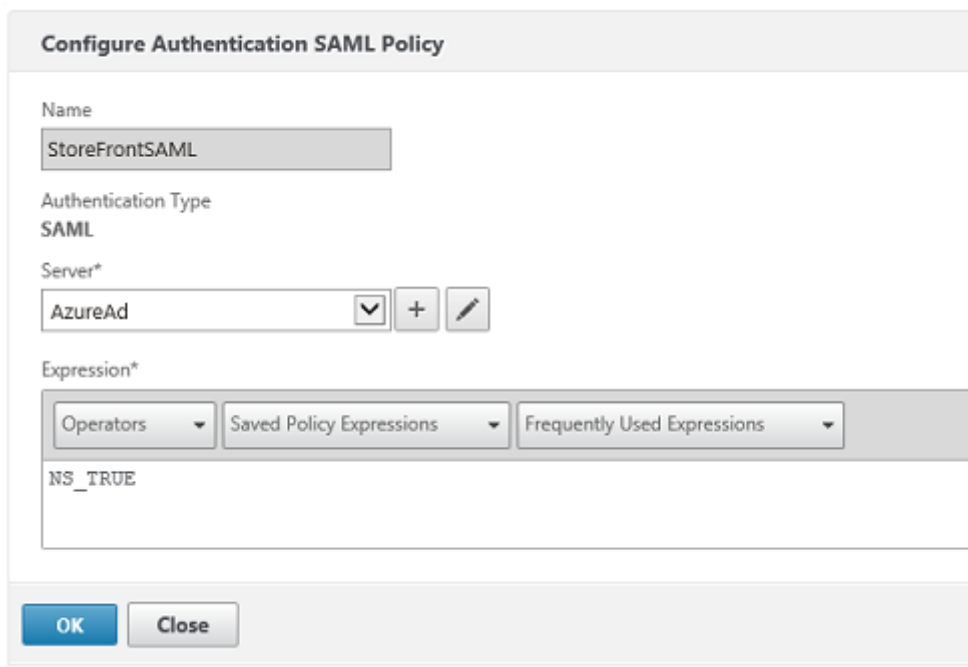
Vérifier le déploiement Citrix Gateway

Connectez-vous à Citrix Gateway et vérifiez le succès de l'authentification et du lancement avec le nom d'utilisateur et mot de passe.



Activer la prise en charge de l'authentification SAML Citrix Gateway

L'utilisation de SAML avec StoreFront est similaire à l'utilisation de SAML avec d'autres sites Web. Ajoutez une nouvelle stratégie SAML avec une expression **NS_TRUE**.



Configure Authentication SAML Policy

Name
StoreFrontSAML

Authentication Type
SAML

Server*
AzureAd

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
NS_TRUE

OK Close

Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment depuis Azure AD.

Create Authentication SAML Server

Create Authentication SAML Server

Name*
AzureAd

Authentication Type
SAML

IDP Certificate Name*
AzureADSAML

Redirect URL*
29f-4c20-9826-14d5e484c62e/saml2

Single Logout URL
29f-4c20-9826-14d5e484c62e/saml2

User Field
userprincipalname

Signing Certificate Name

Issuer Name
https://ns.citrixsaml demo.net/Citrix?

Reject Unsigned Assertion*
ON

SAML Binding*
POST

Default Authentication Group

Skew Time(mins)
5

Two Factor
 ON OFF

Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*
Exact

Authentication Class Types
InternetProtocol
InternetProtocolPassword

Signature Algorithm*
 RSA-SHA1 RSA-SHA256

Digest Method*
 SHA1 SHA256

Send Thumbprint
 Enforce Username

Attribute 1
Attri

Attribute 3
Attri

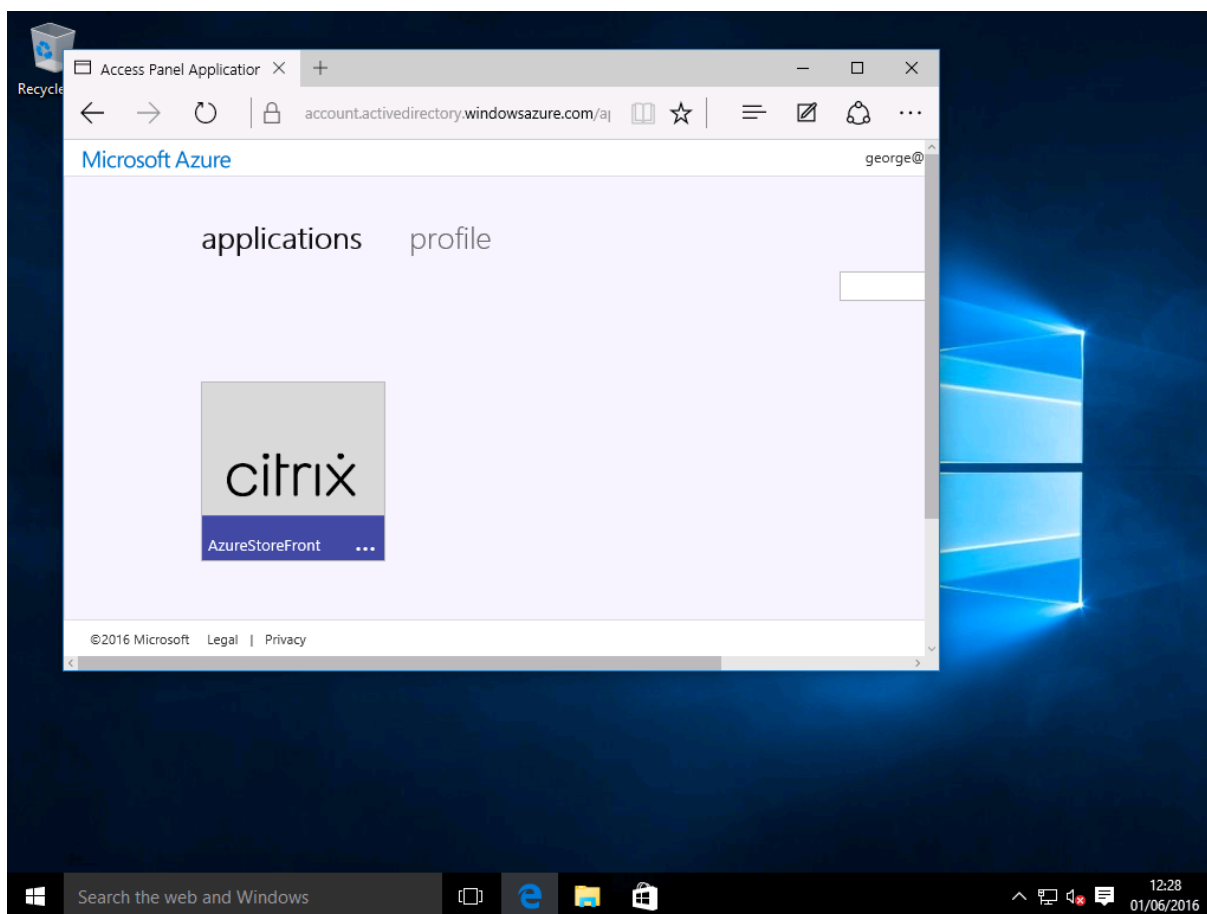
Attribute 5
Attri

Attribute 7
Attri

Vérifier le système de bout en bout

Ouvrez une session sur un bureau Windows 10 joint à Azure AD à l'aide d'un compte enregistré dans Azure AD. Lancez Microsoft Edge et connectez-vous à : <https://myapps.microsoft.com>.

Le navigateur Web devrait afficher les applications Azure AD de l'utilisateur.



Vérifiez qu'un clic sur l'icône vous redirige vers un serveur StoreFront authentifié.

De même, vérifiez que les connexions directes utilisant l'URL d'authentification unique et qu'une connexion directe au site Citrix Gateway vous redirigent vers Microsoft Azure et vice versa.

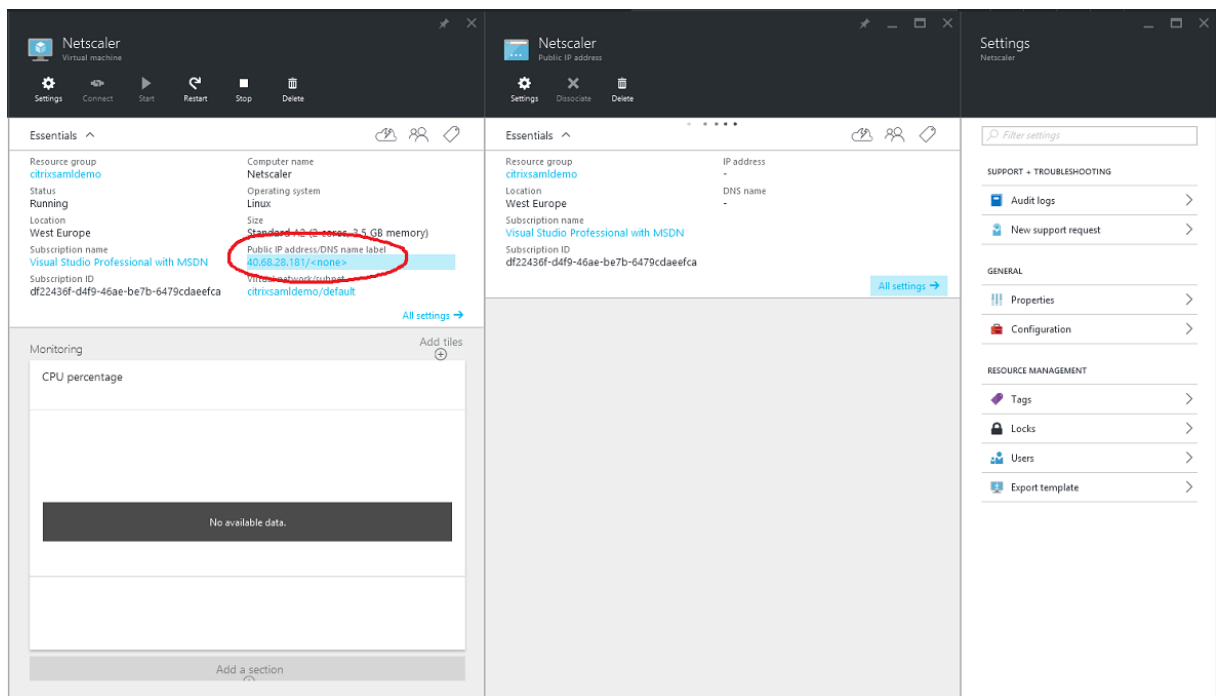
Enfin, vérifiez que les machines non jointes à Azure AD fonctionnent également avec les mêmes URL (bien qu'une authentification unique explicite à Azure AD sera utilisée pour la première connexion).

Annexe

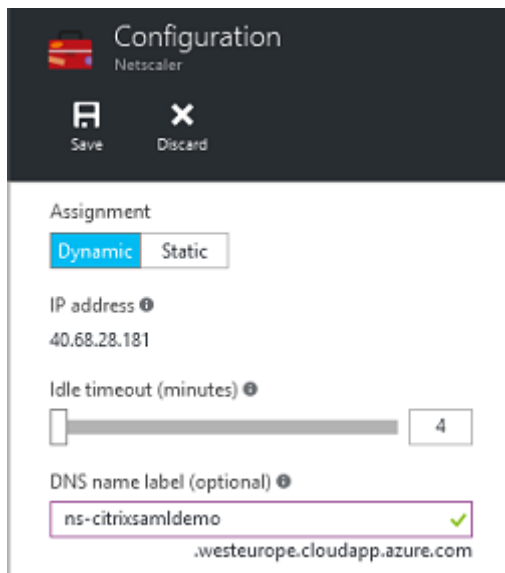
Vous devez configurer les options standard suivantes lorsque vous configurez une machine virtuelle dans Azure.

Fournir une adresse IP publique et une adresse DNS

Azure attribue à toutes les VM une adresse IP sur le sous-réseau interne (10.*.* dans cet exemple). Par défaut, une adresse IP publique est également fournie et cette dernière peut être référencée par un nom DNS mis à jour de manière dynamique.



Dans **Configuration**, sélectionnez **Public IP address/DNS name label**. Choisissez une adresse DNS publique pour la VM. Elle peut être utilisée pour les références CNAME dans d'autres fichiers de zone DNS, pour s'assurer que tous les enregistrements DNS pointent toujours vers la VM, même si l'adresse IP est réallouée.

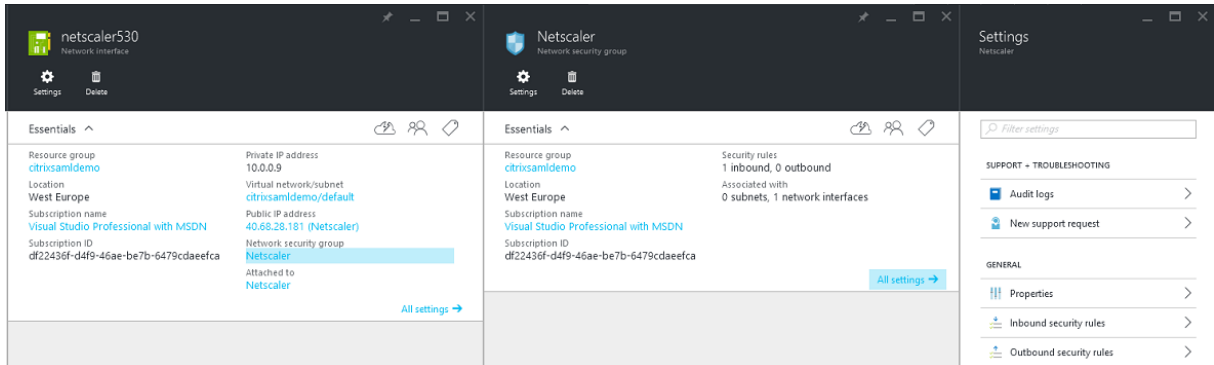


Configurer des règles de pare-feu (groupe de sécurité)

Chaque VM dans un cloud contient un ensemble de règles de pare-feu appliquées automatiquement, connues sous le nom de groupe de sécurité. Le groupe de sécurité contrôle le trafic transféré depuis

l'adresse publique vers l'adresse IP privée. Par défaut, Azure permet à RDP d'être transféré à toutes les VM. Les serveurs Citrix Gateway et ADFS doivent également transférer le trafic TLS (443).

Ouvrez **Network Interfaces** pour une VM et cliquez sur **Network Security Group**. Configurez l'option **Inbound security rules** pour autoriser le trafic réseau approprié.



Informations connexes

- L'article [Installer et configurer](#) est le document de référence principal pour obtenir des informations sur l'installation et la configuration de FAS.
- Les déploiements FAS courants sont décrits dans l'article [Vue d'ensemble des architectures](#).
- D'autres informations pratiques sont disponibles dans l'article [Configuration avancée](#).



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).