



Service d'authentification fédérée 1912

Contents

Service d'authentification fédérée 1912	3
Service d'authentification fédérée 1912	4
Problèmes résolus	4
Problèmes connus	5
Avis de tiers	5
Configuration système requise	5
Installer et configurer	6
Architectures de déploiement	32
Déploiement ADFS	41
Intégration d'Azure AD	45
Configuration avancée	92
Configuration de l'autorité de certification	93
Protection de clé privée	99
Configuration du réseau et de la sécurité	117
Résoudre les problèmes d'ouverture de session Windows	128
Applets de commande PowerShell	140

Service d'authentification fédérée 1912

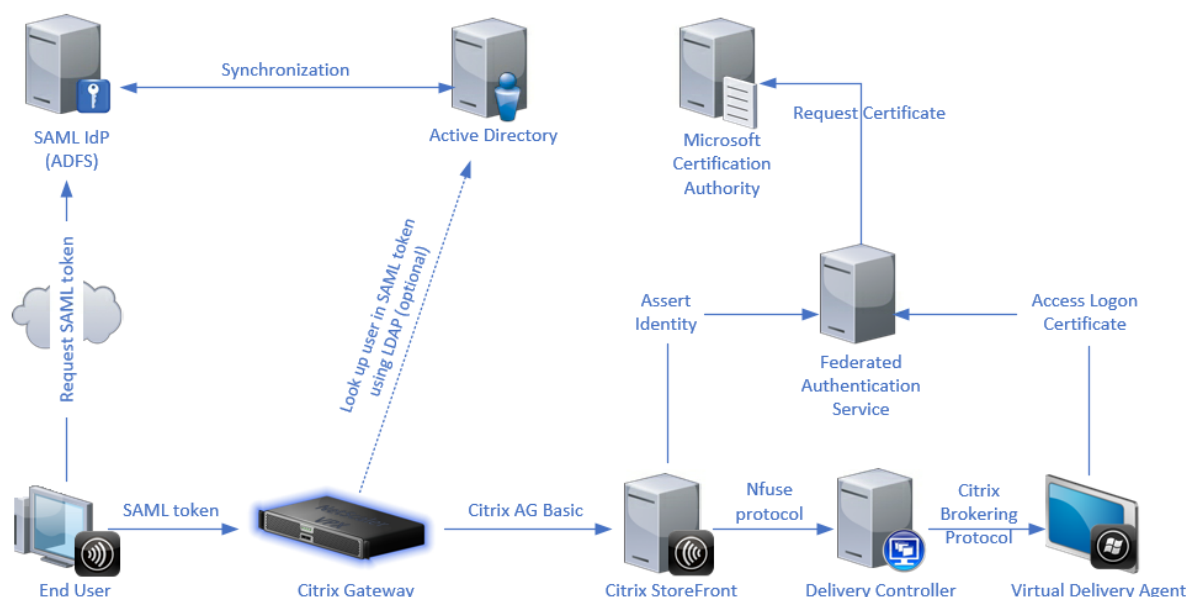
September 30, 2020

Remarque :

Cette documentation prend en charge **Federated Authentication Service 1912**, qui est un composant de base de Citrix Virtual Apps and Desktops 7 1912 LTSR. Pour obtenir le contenu le plus récent, consultez la [documentation de la version actuelle](#) du Service d'authentification fédérée. La stratégie de cycle de vie du produit des versions Current Releases (CR) et Long Term Service Releases (LTSR) est décrite dans [Étapes du cycle de vie](#).

Le Service d'authentification fédérée (FAS) est un composant doté de privilèges conçu pour s'intégrer avec les Services de certificats Active Directory. Il émet des certificats pour les utilisateurs de manière dynamique, ce qui leur permet de se connecter à un environnement Active Directory comme s'ils avaient une carte à puce. Cela permet à StoreFront d'utiliser un éventail plus large d'options d'authentification, telles que les assertions SAML (Security Assertion Markup Language). SAML est généralement utilisé comme une alternative aux comptes utilisateur Windows traditionnels sur Internet.

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.



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.

Références

- Services de certificats Active Directory [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11))
- Configuration de Windows pour l'ouverture de session par certificat <http://support.citrix.com/article/CTX206156>

Service d'authentification fédérée 1912

September 30, 2020

Le service d'authentification fédérée 1912 ne comprend aucune nouvelle fonctionnalité. Pour plus d'informations sur les corrections de bogues, veuillez consulter la section [Problèmes résolus](#).

Problèmes résolus

June 18, 2020

Problèmes résolus dans la version 1912

Comparaison avec : Federated Authentication Service 1909

Federated Authentication Service 1912 contient les correctifs suivants :

- Dans les propriétés du modèle de certificat Citrix_SmartcardLogon, la description de l'extension Utilisation de la clé doit contenir uniquement 'Signature numérique' et 'Chiffrement de la clé', mais répertorie des éléments supplémentaires. Toutefois, les certificats émis à l'aide de ce modèle sont corrects. [CVADHELP-14040]
- Lorsque la console d'administration FAS est utilisée pour déployer des modèles de certificats dans Active Directory, les autorisations de sécurité des modèles ne comprennent plus l'autorisation « inscription automatique ». Cette autorisation n'est pas nécessaire pour le bon fonctionnement de FAS et provoque des tentatives d'inscription indésirables par les ordinateurs de domaine dans certains déploiements clients. [AUTH-224]

Problèmes connus

September 30, 2020

Le Service d'authentification fédérée 1912 ne contient aucun problème connu.

Cet avertissement 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

September 30, 2020

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 \(PDF\)](#)
- [Divulgations de logiciels non commerciaux pour FlexNet Publisher 2017 \(11.15.0.0\) \(PDF\)](#)
- [Supplément à la documentation FlexNet Publisher Logiciels tiers et Open Source utilisés dans FlexNet Publisher 11.15.0 \(PDF\)](#)

Configuration système requise

September 30, 2020

Le Service d'authentification fédérée (FAS) est pris en charge sur toutes les versions de Windows Server actuellement prises en charge. Pour plus d'informations, consultez la [Configuration système requise](#) de Citrix Virtual Apps ou Citrix Virtual Desktops

- Citrix vous recommande d'installer FAS sur un serveur qui ne contient pas d'autres composants Citrix.

- Le serveur Windows doit être sécurisé. Il aura accès à un certificat d'autorité d'inscription et à une clé privée qui lui permettent d'émettre automatiquement des certificats pour les utilisateurs du domaine, et il aura accès à ces certificats utilisateur et clés privées.
- Les [Applets de commande PowerShell](#) de FAS nécessitent l'installation de Windows PowerShell 64 bits sur le serveur FAS.
- Une autorité de certification Microsoft Enterprise est requise pour émettre des certificats utilisateur.

Dans le site Citrix Virtual Apps ou Citrix Virtual Desktops :

- Les Delivery Controller, Virtual Delivery Agent (VDA) et le serveur StoreFront doivent tous être des versions actuellement prises en charge. Pour plus d'informations, consultez la [Configuration système requise](#) de Citrix Virtual Apps ou Citrix Virtual Desktops.

Remarque :

FAS n'est pas pris en charge sur XenApp et XenDesktop 7.6 version Long Term Service Release (LTSR).

- Avant de créer le catalogue de machines, la configuration de la stratégie de groupe Service d'authentification fédérée doit être appliquée correctement aux VDA. Consultez la section [Configurer une stratégie de groupe](#) pour plus de détails.

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

Installer et configurer

September 30, 2020

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 une stratégie de groupe](#)
4. Utiliser la console d'administration FAS pour : (a) [Déployer les modèles fournis](#), (b) [Configurer les autorités de certification](#) et (c) [Autoriser FAS de sorte qu'il utilise votre autorité de certification](#)
5. [Configurer des règles d'utilisateur](#)

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 qui est sécurisé de la même manière qu'un contrôleur de domaine ou une autorité de certification. FAS peut être installé à partir du bouton **Service d'authentification fédérée** sur l'écran de démarrage autorun lorsque l'ISO est inséré.

Les composants suivants sont installés :

- Service d'authentification fédérée
- [Applets de commande du composant logiciel enfichable PowerShell](#) pour configurer FAS à distance
- [Console d'administration FAS](#)
- Modèles de stratégie de groupe FAS (CitrixFederatedAuthenticationService.admx/adml)
- Fichiers de modèle de certificat pour la configuration de l'autorité de certification
- [Compteurs de performances](#) et [journaux d'événements](#)

Activer le plug-in FAS sur des magasins StoreFront

Pour activer l'intégration de FAS sur un magasin StoreFront, exécutez les applets de commande PowerShell suivantes sous un compte d'administrateur. Si vous disposez de plus d'un magasin, ou si le magasin a un autre nom, le texte du chemin d'accès ci-dessous peut différer.

```
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"
```

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 ""
```

Configurer le Delivery Controller

Pour utiliser FAS, configurez le Delivery Controller Citrix Virtual Apps ou Citrix Virtual Desktops de manière à approuver les serveurs StoreFront qui peuvent s'y connecter : exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true**.

Configurer une stratégie de groupe

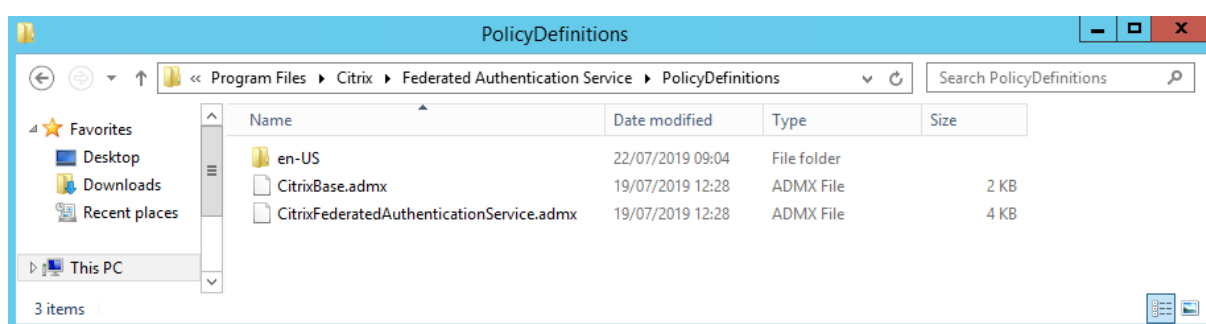
Après avoir installé FAS, vous devez spécifier les adresses DNS complètes des serveurs FAS dans une stratégie de groupe à l'aide des modèles de stratégie de groupe fournis dans le cadre de l'installation.

Important :

Assurez-vous que les serveurs StoreFront qui demandent des tickets et les VDA (Virtual Delivery Agent) utilisant des tickets disposent d'adresses DNS 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 fonctionnera tant que les serveurs StoreFront, les VDA, et la machine exécutant la console d'administration FAS voient la même liste d'adresses DNS. Veuillez noter que l'objet de stratégie de groupe ajoute un numéro d'index pour chaque entrée, qui doit également correspondre si plusieurs objets sont utilisés.

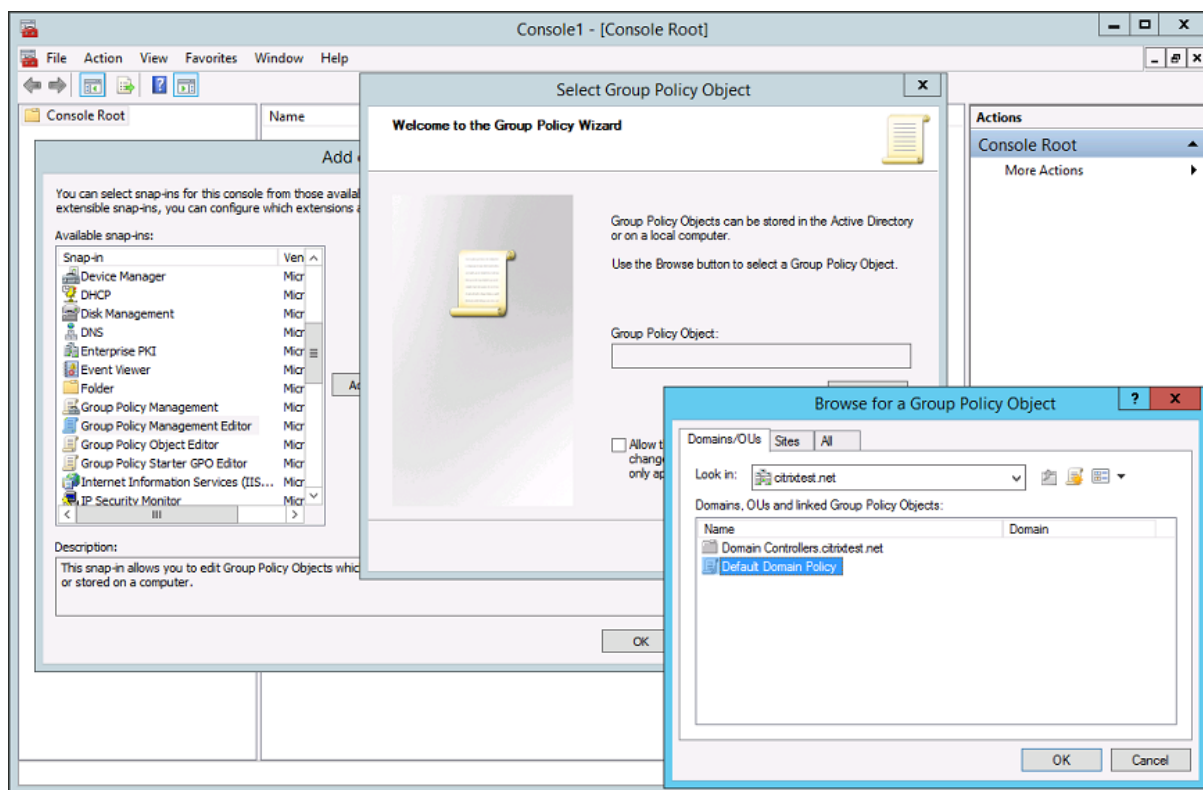
Étape 1. Sur le serveur sur lequel vous avez installé FAS, localisez les fichiers C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx et CitrixBase.admx, ainsi que le dossier en-US.



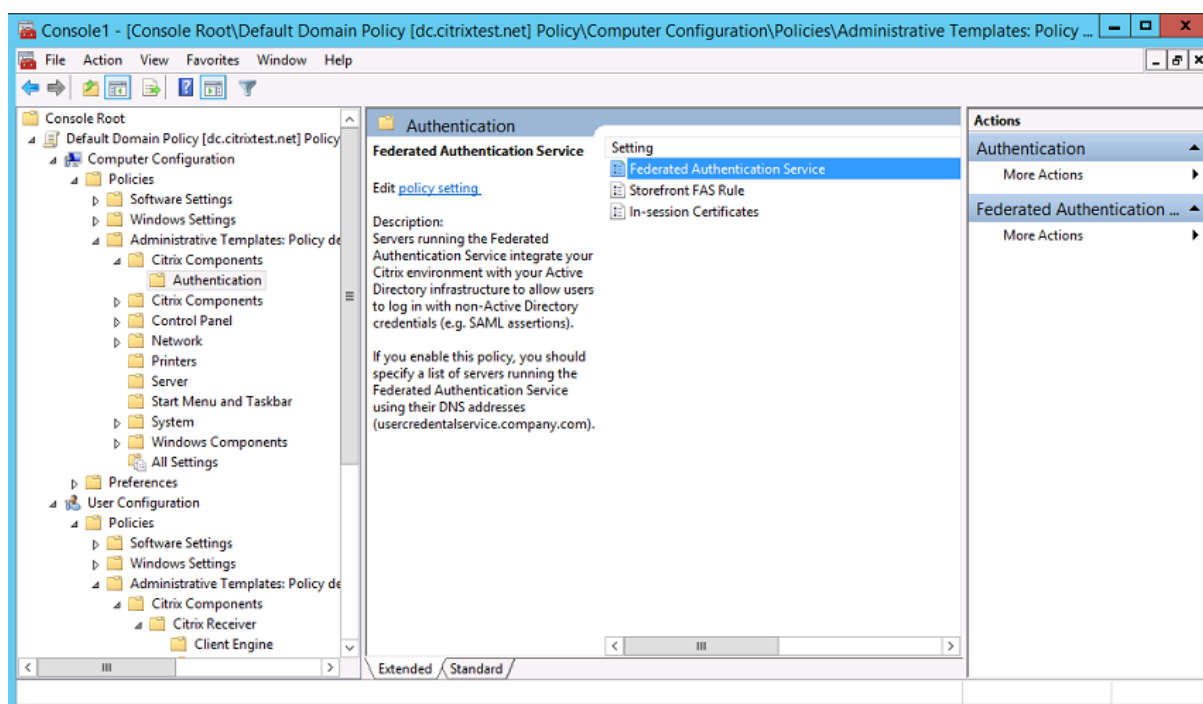
Étape 2. Copiez ces derniers sur votre contrôleur de domaine et placez-les dans C:\Windows\PolicyDefinitions et le sous-dossier en-US.

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 **Éditeur d'objets de stratégie 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).



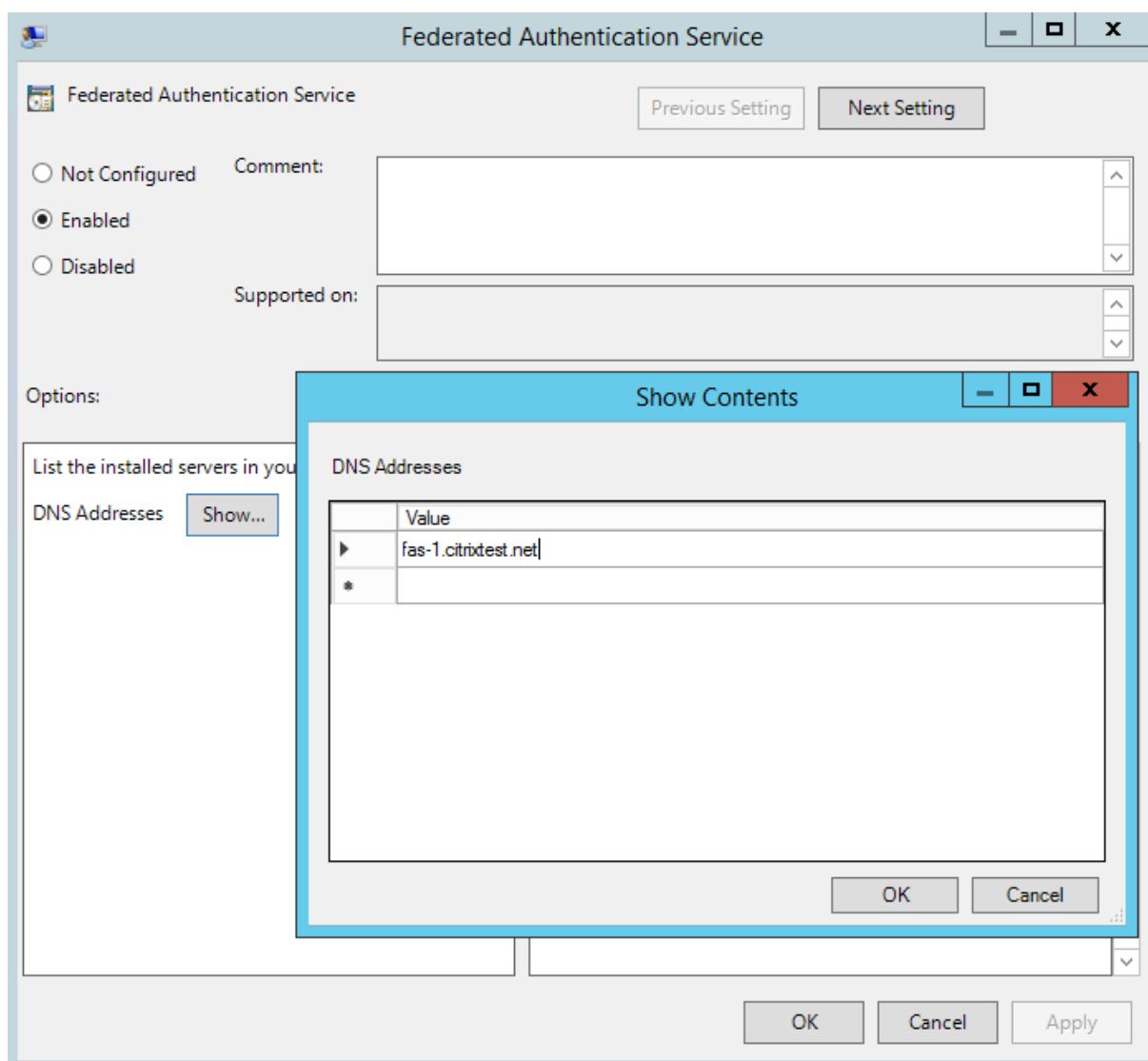
Étape 4. Accédez à la stratégie *Service d'authentification fédérée* située dans Configuration ordinateur/Stratégies/Modèles d'administration/Composants Citrix/Authentification.



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. Le paramètre de stratégie Service d'authentification fédérée est ensuite 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 adresses DNS de vos serveurs FAS.



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

Rappel : si vous entrez plusieurs noms de domaine complets, l'ordre de la liste doit être cohérent entre les serveurs StoreFront et les VDA. Cela comprend des entrées vides ou non utilisées.

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 commande) pour que les modifications prennent effet.

Prise en charge des certificats dans la session et déconnexion après verrouillage

In-session Certificates

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on:

Options:

Prompt Scope: Per-process

Consent timeout (seconds): 30

☒ Disconnect on lock

Help:

Certificates and private keys securely managed by the Federated Authentication Service can be made available to programs running in users' sessions. If this policy is disabled, this feature will be unavailable.

If this policy is enabled, the Prompt Scope setting will control how users are prompted for consent. There are three options:

- No consent required -- This option disables the security prompt and private keys are used silently.
- Per-process consent -- Each running program will individually prompt for consent.
- Per-session consent -- Once the user has clicked ok, this will apply to all programs in the session

If this policy is enabled, the Consent Timeout will control how long (in seconds) the consent lasts. So for example, if set to 300 seconds the user will see a prompt every five minutes. A value of zero will prompt the user for every private key operation.

If this policy is enabled, it is also possible to automatically disconnect a user's session rather than display the logon prompt. This functionality provides similar behaviour to the "disconnect on smart card removal" policy, and is useful for situations where users do not have Active Directory logon credentials.

OK Cancel Apply

Prise en charge des certificats dans la session

Par défaut, les VDA n'autorisent pas l'accès aux certificats après l'ouverture de session. Si nécessaire, vous pouvez utiliser le modèle de stratégie de groupe pour configurer le système pour les certificats de la session. Ceci place les certificats 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, le certificat peut être utilisé par Internet Explorer.

Déconnexion après verrouillage

Si cette stratégie est activée, la session de l'utilisateur est automatiquement déconnectée lorsqu'il verrouille l'écran. Cette fonctionnalité fournit un comportement similaire à la stratégie de « déconnexion lors du retrait de la carte à puce ». Elle est utile dans les situations où les utilisateurs ne disposent pas d'informations d'identification d'ouverture de session Active Directory.

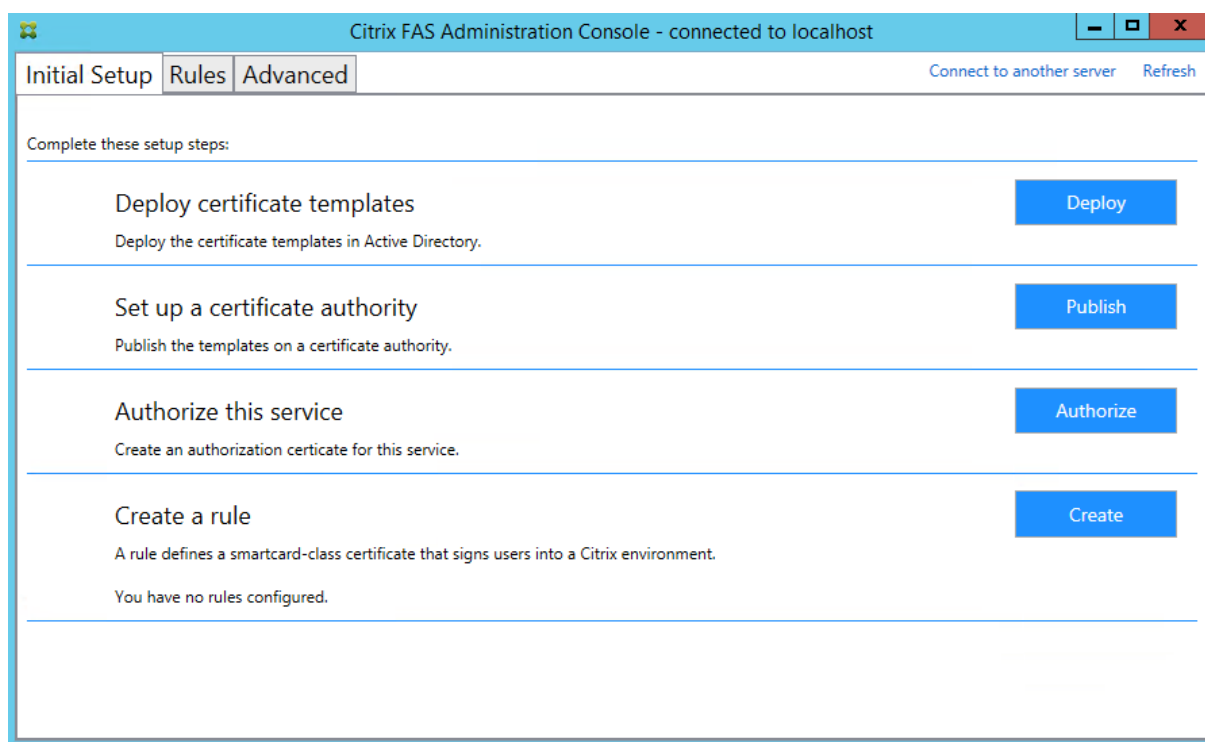
Remarque :

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

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 la console d'administration est utilisée, elle vous guide au travers d'un processus qui déploie les modèles de certificat, configure l'autorité de certification et autorise FAS à utiliser l'autorité de certification. Certaines des étapes peuvent également être effectuées manuellement à l'aide des outils de configuration du système d'exploitation.



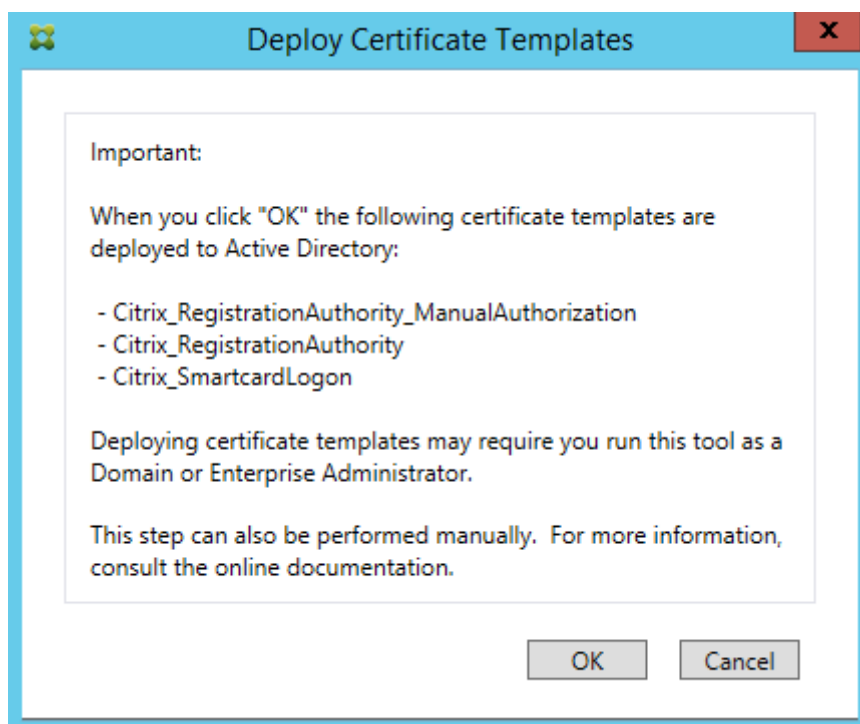
Déployer des modèles de certificat

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. Si la console ne peut pas les trouver, l'outil **Déployer des modèles de certificat** peut les installer. Cet outil doit être exécuté sous un compte disposant des autorisations nécessaires pour gérer votre forêt d'entreprise.



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

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 utiliser les commandes PowerShell suivantes :

```
1 $template = [System.IO.File]::ReadAllBytes("$Pwd\  
Citrix_SmartcardLogon.certificatetemplate")  
2 $CertEnrol = New-Object -ComObject X509Enrollment.  
CX509EnrollmentPolicyWebService  
3 $CertEnrol.InitializeImport($template)  
4 $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)  
5 $writabletemplate = New-Object -ComObject X509Enrollment.  
CX509CertificateTemplateADWritable
```

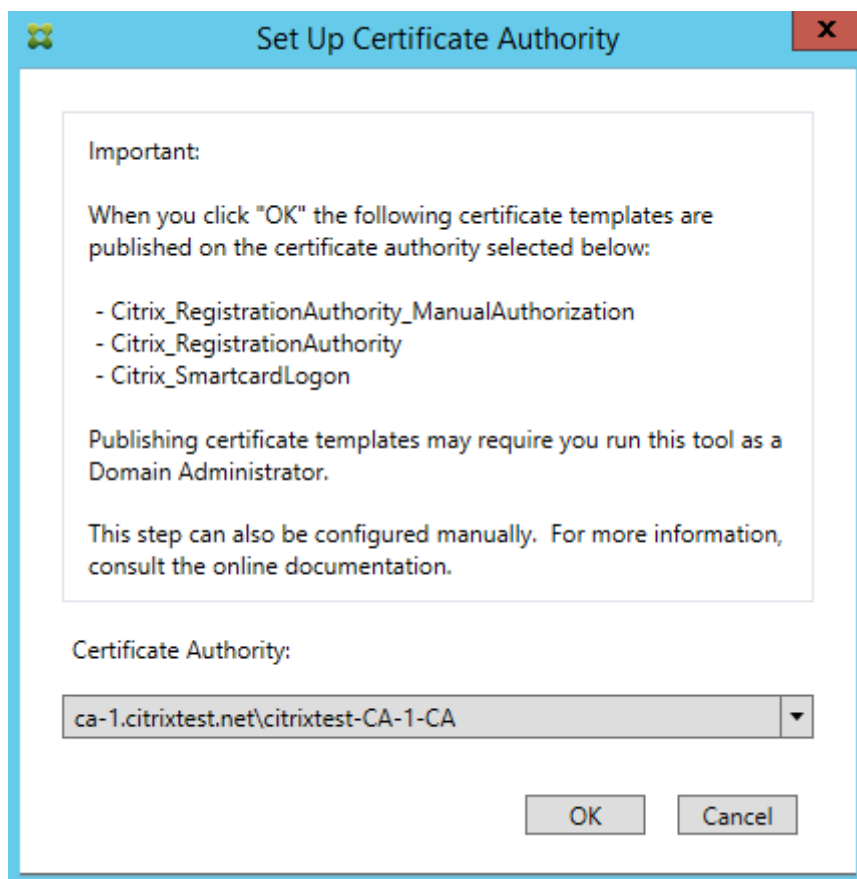
```
6 $writabletemplate.Initialize($comtemplate)
7 $writabletemplate.Commit(1, $NULL)
```

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. Reportez-vous à la documentation Microsoft sur la manière de déployer des services de certificats Active Directory.

Si les modèles ne sont pas publiés sur au moins un serveur, l'outil **Configurer une autorité de certification** permet de les publier. Vous devez exécuter cet outil en tant qu'utilisateur disposant d'autorisations suffisantes pour gérer l'autorité de certification.

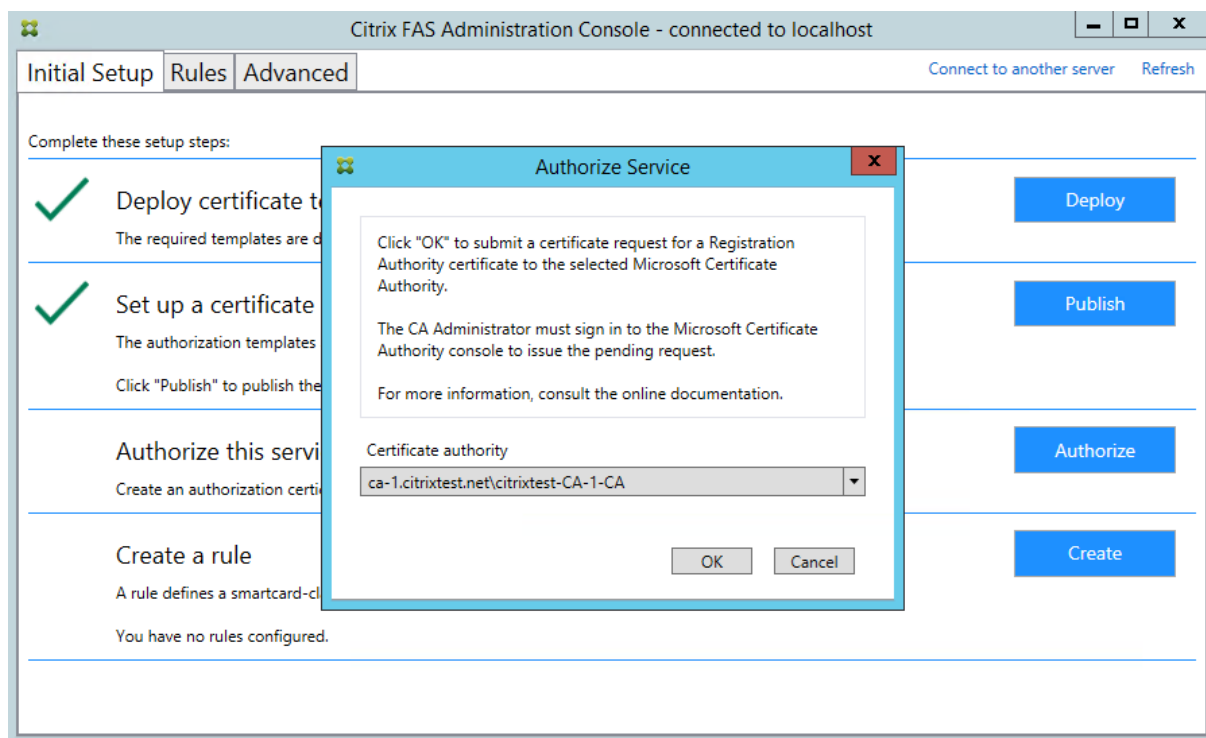
(Les modèles de certificats peuvent également être publiés à l'aide de la console Autorité de certification de Microsoft.)



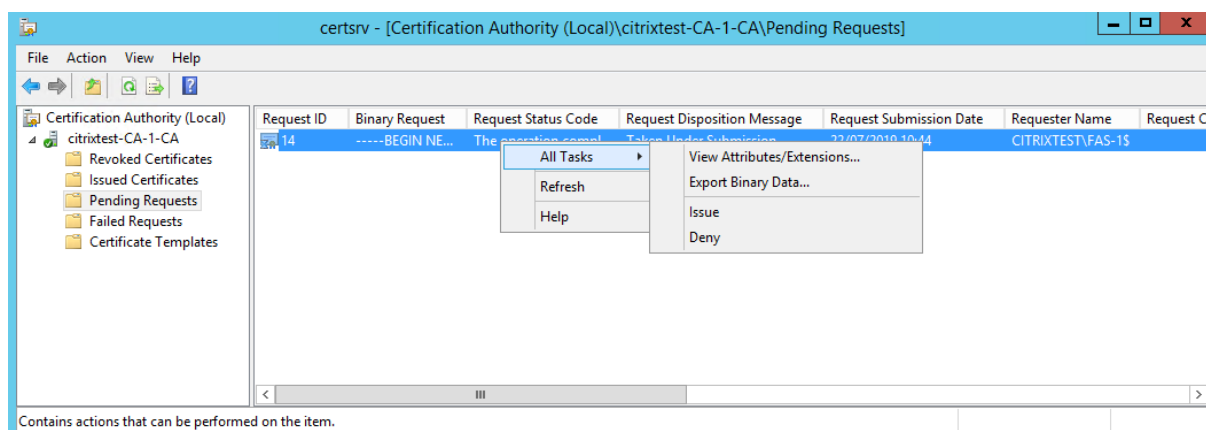
Autoriser le Service d'authentification fédérée

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

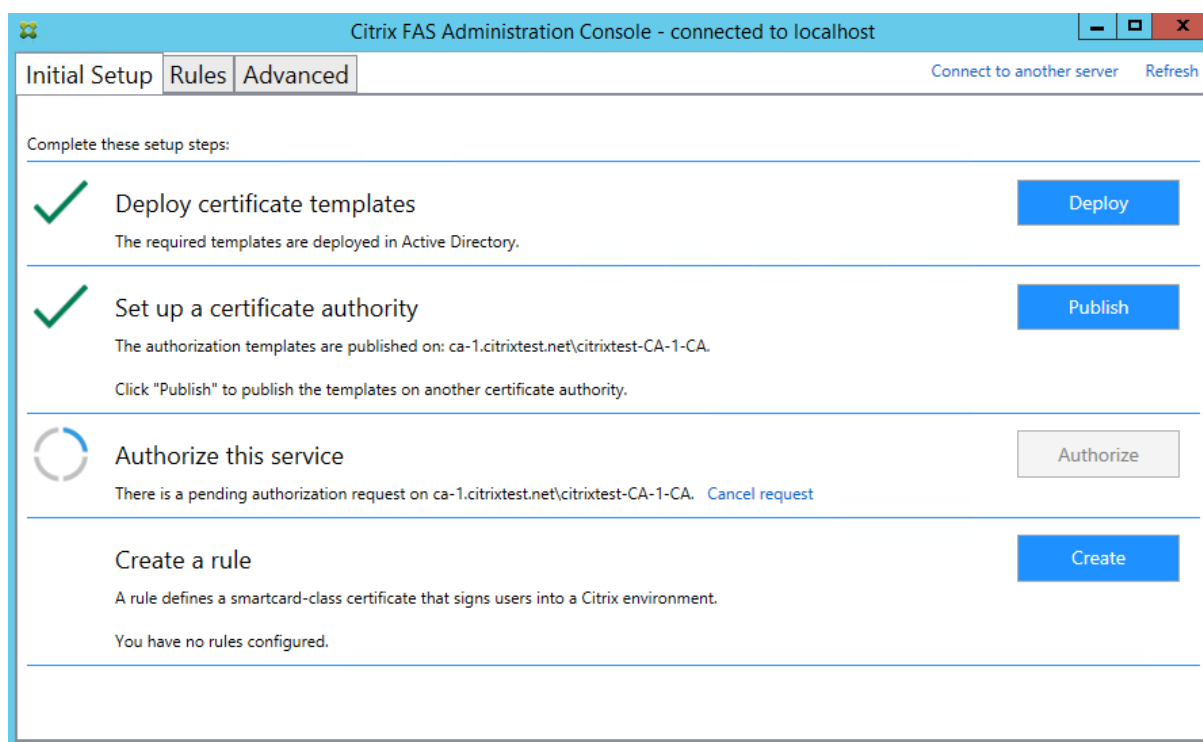
à l'une des autorités de certification qui publient ce modèle.



Une fois la requête envoyée, elle apparaît dans la liste **Demandes en attente** de la console Autorité de certification de Microsoft. L'administrateur de l'autorité de certification doit choisir d'**émettre** ou de **rejeter** la requête avant que la configuration de FAS puisse continuer. Veuillez noter que la demande d'autorisation s'affiche en tant que **Demande en attente** depuis le compte de la machine FAS.



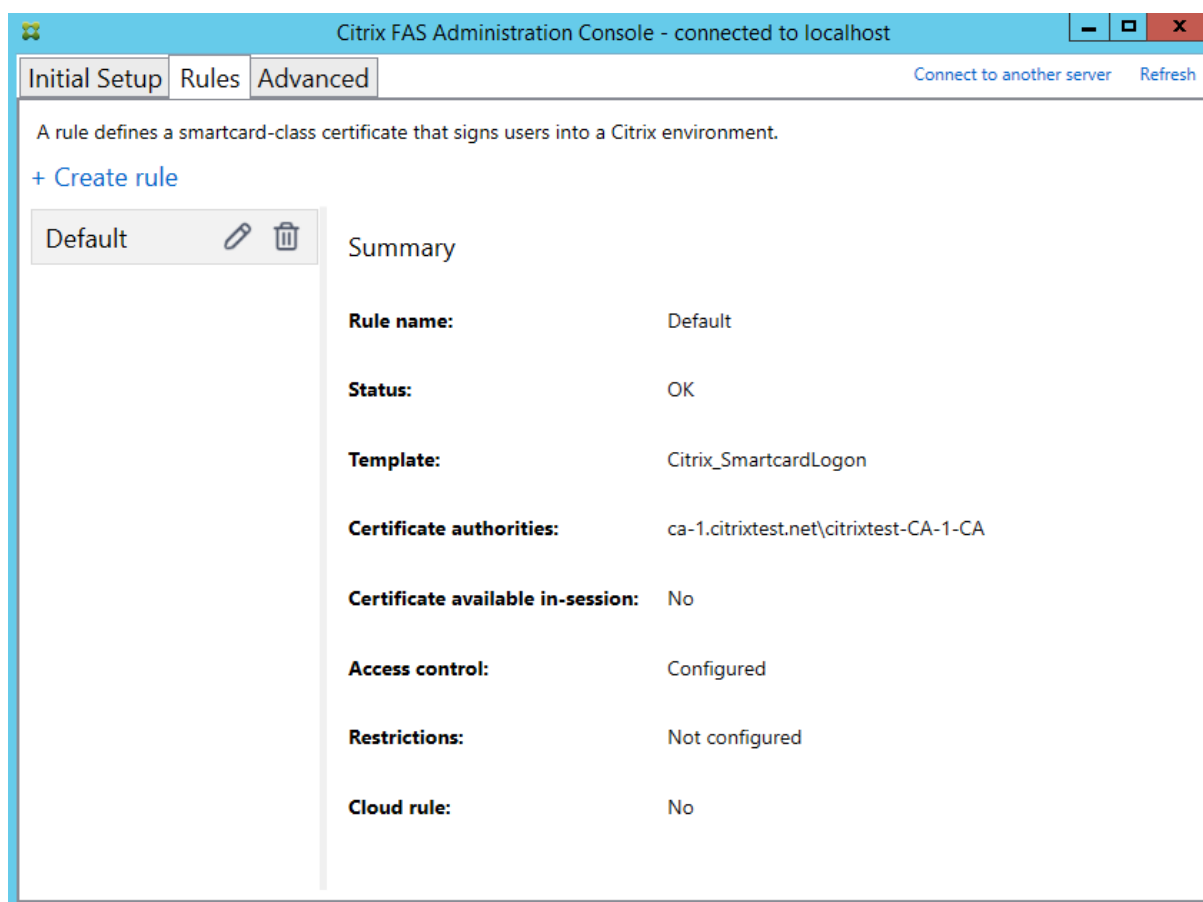
Cliquez avec le bouton droit sur **Toutes les tâches**, puis sélectionnez **Émettre** ou **Rejeter** pour la demande de certificat. La console d'administration FAS détecte automatiquement lorsque ce processus est terminé. Cette opération peut prendre plusieurs minutes.



Configurer des règles d'utilisateur

Une règle d'utilisateur autorise 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 spécifie les serveurs StoreFront qui sont approuvés pour demander des certificats, les utilisateurs pour lesquels ils peuvent être demandés, et les VDA autorisés à les utiliser.

Pour terminer la configuration FAS, vous devez définir la règle par défaut. Cliquez sur **Create** pour créer une règle ou accédez à l'onglet Rules et cliquez sur **Create rule**. L'assistant rassemble les informations nécessaires à la définition d'une règle.



Les informations suivantes sont collectées par l'assistant :

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.

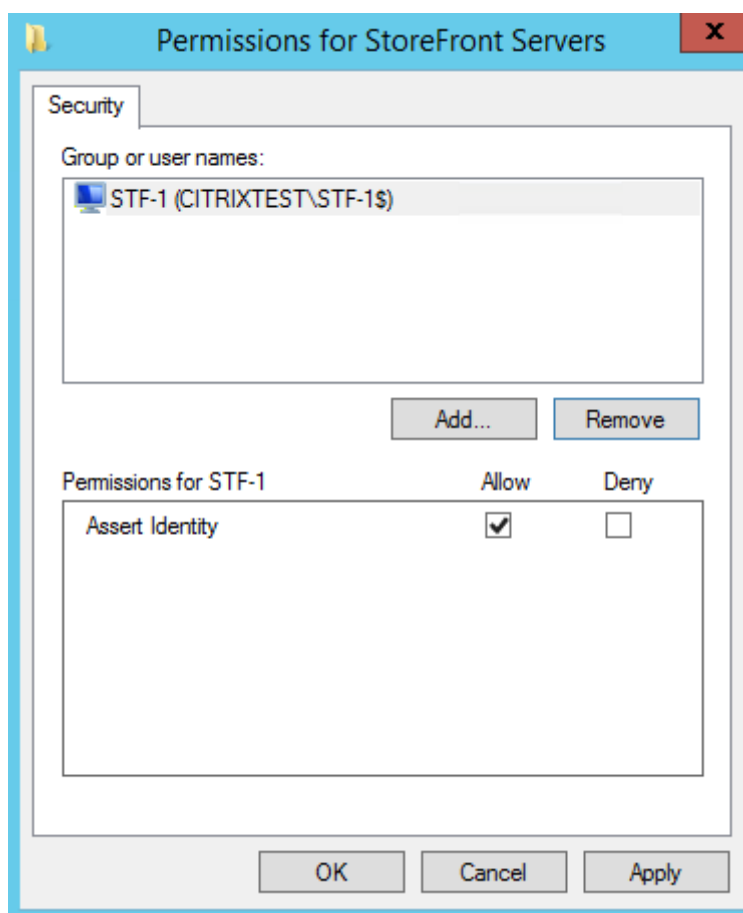
Certificate Authority : autorité de certification qui émet des certificats utilisateur. Le modèle doit être publié par l'autorité de certification. FAS prend en charge l'ajout de multiples autorités de certification à des fins de basculement et d'équilibrage de charge.

In-Session Use : l'option **Allow in-session use** contrôle si un certificat peut être utilisé après l'ouverture de session sur le VDA. Sélectionnez cette option uniquement si vous souhaitez que les utilisateurs aient accès au certificat après l'authentification. Si cette option n'est pas sélectionnée, 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.

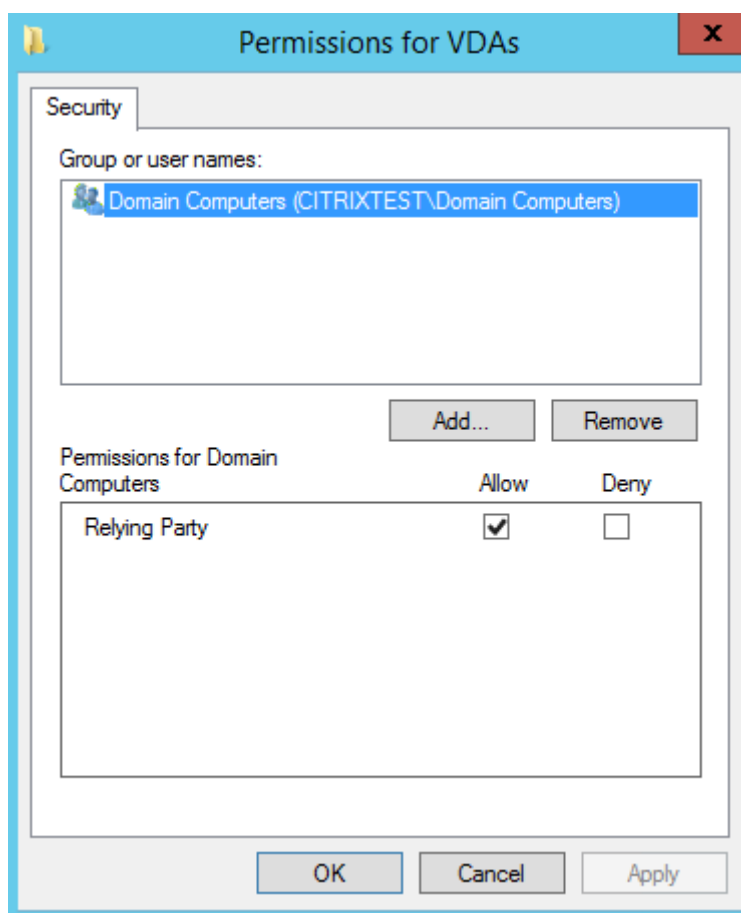
Access control : liste des serveurs StoreFront approuvés qui sont autorisés à demander des certificats pour l'ouverture de session ou la reconnexion des utilisateurs.

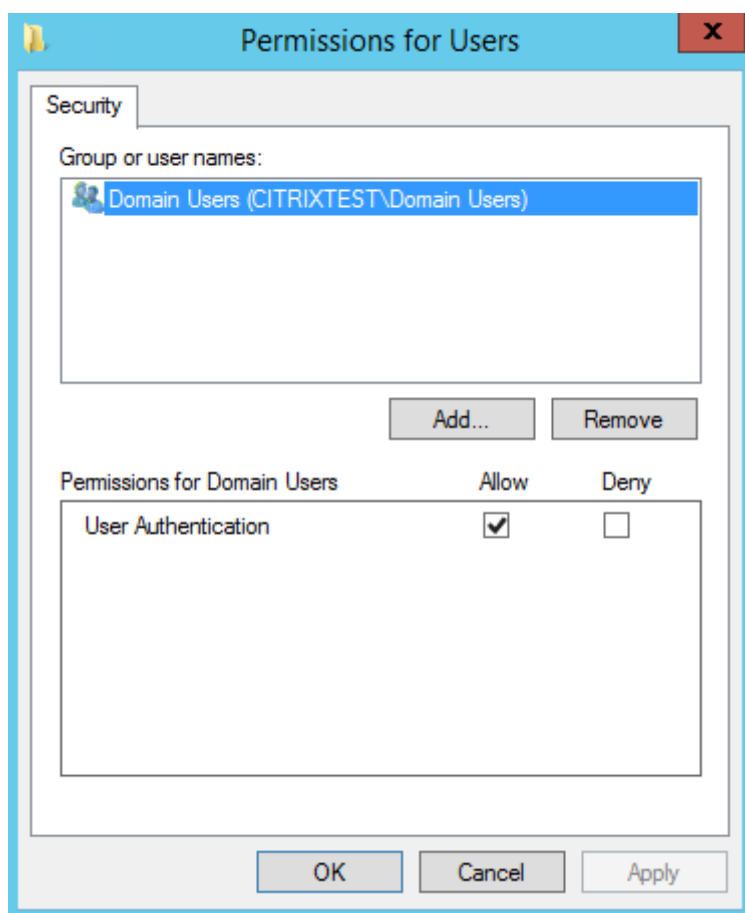
Important :

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



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. La liste des VDA est par défaut Ordinateurs du domaine et la liste des utilisateurs est par défaut Utilisateurs du domaine ; ces informations peuvent être modifiées si les valeurs par défaut ne sont pas appropriées.





Cloud rule : règle actuellement non prise en charge.

Utilisation avancée

Vous pouvez créer des règles supplémentaires pour référencer des autorités et des modèles de certificat différents, qui peuvent être configurés pour avoir des propriétés et des autorisations différentes. Ces règles peuvent être configurées pour être utilisées par différents serveurs StoreFront, qui devront être configurés pour demander la nouvelle règle par nom. Par défaut, StoreFront requiert les **valeurs par défaut** lors du contact de FAS. Cela peut être modifié à l'aide des options de configuration de la stratégie de groupe.

Pour créer un nouveau modèle de certificat, dupliquez le modèle Citrix_SmartcardLogon dans la console Autorité de certification de Microsoft, renommez-le (par exemple, Citrix_SmartcardLogon2) et modifiez-le si nécessaire. Créez une nouvelle règle d'utilisateur en cliquant sur **Add** afin de référencer le nouveau modèle de certificat.

Notions importantes sur la mise à niveau

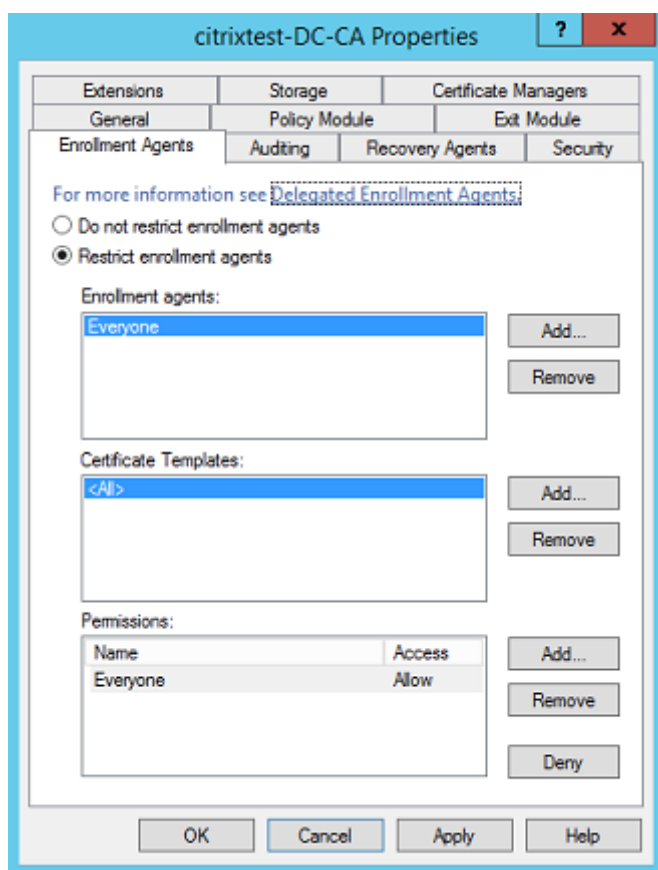
- Tous les paramètres du serveur FAS sont conservés lorsque vous effectuez une mise à niveau sur place.
- Mettez à niveau FAS en exécutant le programme d'installation du produit complet de Virtual Apps and Desktops.
- Avant de mettre à niveau FAS, mettez à niveau le contrôleur et les VDA (et autres composants principaux) vers la version requise.
- Assurez-vous que la console d'administration FAS est fermée avant de mettre à niveau FAS.
- Assurez-vous qu'au moins un serveur FAS est disponible à tout moment. 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.

Considérations de sécurité

FAS dispose d'un certificat d'autorité d'inscription qui lui permet d'émettre des certificats de manière autonome de la part de vos utilisateurs de domaine. C'est la raison pour laquelle il est important de développer et d'appliquer 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 permet de contrôler les modèles que le serveur FAS peut utiliser, ainsi que de limiter les utilisateurs pour lesquels le serveur FAS peut émettre des certificats.



Citrix recommande fortement de configurer ces options de façon à ce que FAS puisse uniquement émettre des certificats pour les utilisateurs visés. Par exemple, il est conseillé d'empêcher FAS d'émettre des certificats aux utilisateurs d'un groupe d'utilisateurs protégés ou d'un groupe d'administration.

Configuration de la liste de contrôle d'accès

Comme indiqué dans la section [Configurer des règles d'utilisateur](#), vous devez configurer une liste de serveurs StoreFront autorisés à assumer des identités utilisateur sur FAS lorsque des certificats sont émis. De même, vous pouvez restreindre les utilisateurs pour lesquels des certificats seront émis, et les machines VDA auprès desquelles ils peuvent s'authentifier. Cela vient s'ajouter à tout Active Directory standard ou toute fonctionnalité 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. Ces informations peuvent être utilisées à des fins de contrôle et d'audit. La section [Journaux d'événements](#) dresse la liste des entrées de journal d'événements qui peuvent être générées.

Modules matériels de sécurité

Toutes les clés privées, y compris 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.
ProviderType	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.
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).

SDK PowerShell

Bien que la console d'administration FAS convienne aux déploiements simples, l'interface PowerShell offre des options plus avancées. Lorsque vous utilisez 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 :

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

Utilisez **Get-Help** <nom cmdlet> pour afficher l'aide de l'applet de commande. Le tableau suivant dresse la liste de plusieurs commandes où * représente un verbe PowerShell standard (comme New, Get, Set, Remove).

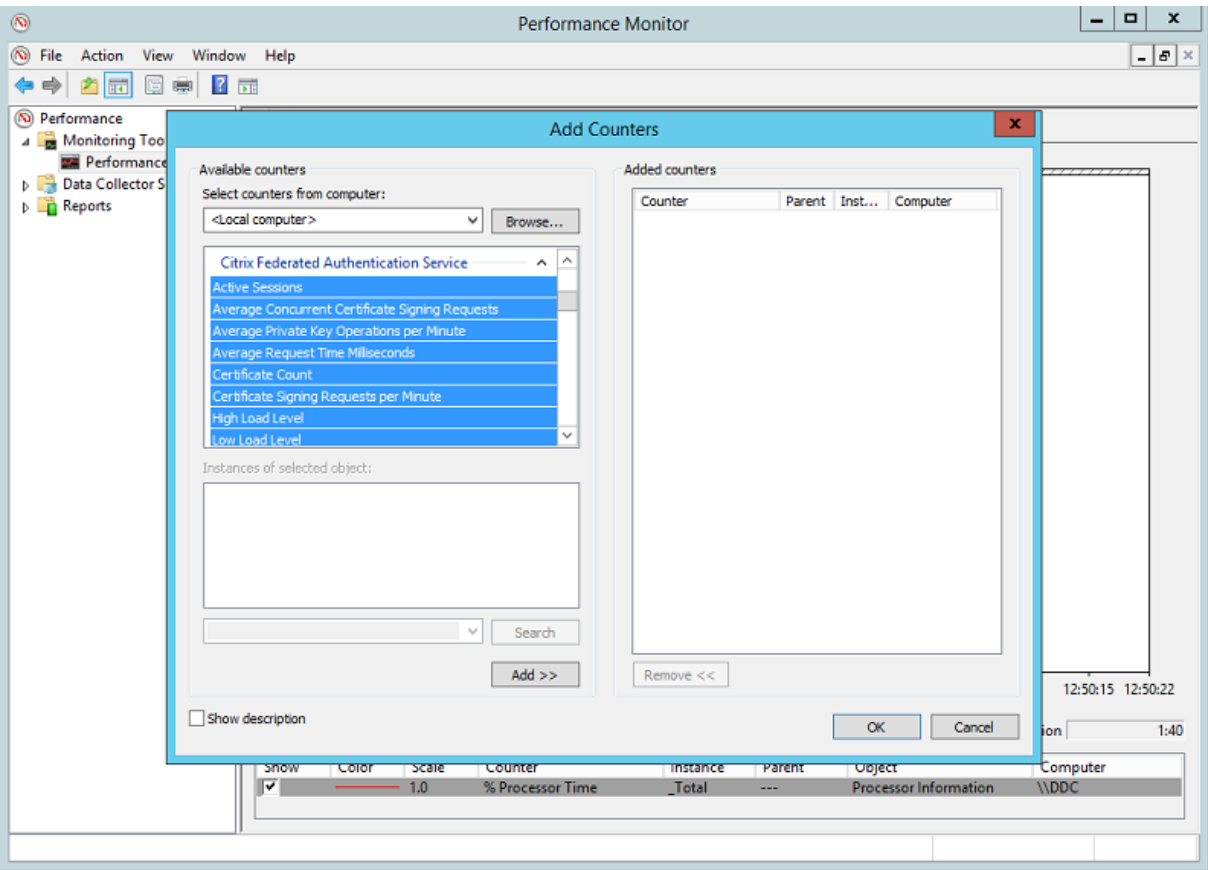
Commandes	Généralités
*-FasServer	Dresse la liste des serveurs FAS et les reconfigure dans l'environnement actuel.
*-FasAuthorizationCertificate	Gère le certificat d'autorité d'inscription.
*-FasCertificateDefinition	Contrôle les paramètres que FAS utilise pour générer des certificats.
*-FasRule	Gère les règles utilisateur configurées sur FAS.
*-FasUserCertificate	Répertorie et gère les certificats mis en cache par FAS.

Des applets de commande PowerShell peuvent être utilisées à distance en spécifiant l'adresse d'un serveur FAS.

Pour plus d'informations sur les applets de commande FAS PowerShell, consultez [Applets de commande PowerShell](#).

Compteurs de performances

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



Le tableau suivant répertorie les compteurs disponibles. La plupart des compteurs sont des moyennes mobiles de cinq minutes.

Nom	Description
Active Sessions	Nombre de connexions suivies par FAS.
Concurrent CSRs	Nombre de demandes de certificat traitées simultanément.
Private Key ops	Nombre d'opérations de clé privée effectuées par minute.
Request time	Durée requise pour générer et signer un certificat.
Certificate Count	Nombre de certificats mis en cache dans FAS.
CSR per minute	Nombre de demandes de signature de certificat traitées par minute.

Nom	Description
Low/Medium/High	Estimations de la charge que FAS peut accepter en termes de « demandes CSR par minute ». Le dépassement du seuil « High Load » peut entraîner l'échec du lancement de sessions.

Journaux d'événements

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}] enrolling with CA [{1}] templates [{2} et {3}]

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

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

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

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

[S009] Administrator [{0}] creating new Role [{1}]

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

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

[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} role: {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}]

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 MinThreads adjusted from [workers: {0} completion: {1}] to: [workers: {2}
completion: {3}]

[S410] Failed to adjust ThreadPool MinThreads from [workers: {0} completion: {1}] to: [workers:
{2} completion: {3}]

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.

[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] Calling account [{0}] is not a relying party in role [{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}].

FAS assertion plugin [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 plugin is configured

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

[S502] FAS assertion plugin loaded [pluginId={0}] [assembly={1}] [location={2}]

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

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

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

[S506] The plugin [{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}])

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

[S508] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but the plugin [{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 deemed invalid by plugin [{2}])

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}]

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

Codes de journal

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

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

[S106] Identity Assertion Logon. Connexion [Certificate: {0}]

[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. Accès refusé [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]

[Event Source: 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}]

[S016] PrivateKey::Create [Identifier {0}][MachineWide: {1}][Provider: {2}][ProviderType: {3}][EllipticCurve: {4}][KeyLength: {5}][isExportable: {6}]

[S017] PrivateKey::Delete [CspName: {0}, Identifier {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}]

Informations connexes

- Les déploiements FAS courants sont décrits dans l'article [Architectures de déploiement](#).
- Des informations pratiques sont disponibles dans l'article [Configuration avancée](#).

Architectures de déploiement

September 30, 2020

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.

Fonctionnement

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.

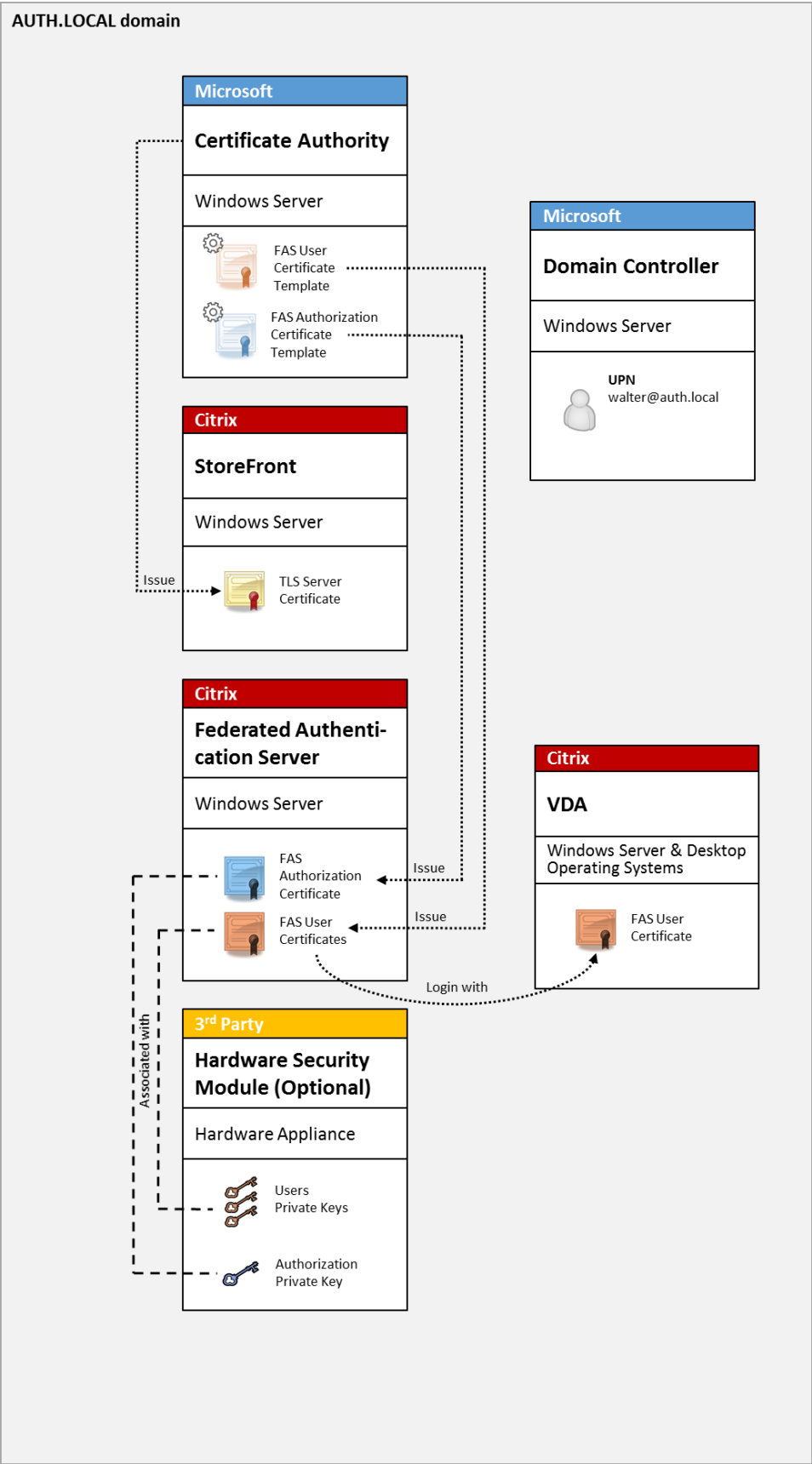
Déploiement interne

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 connecter 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).

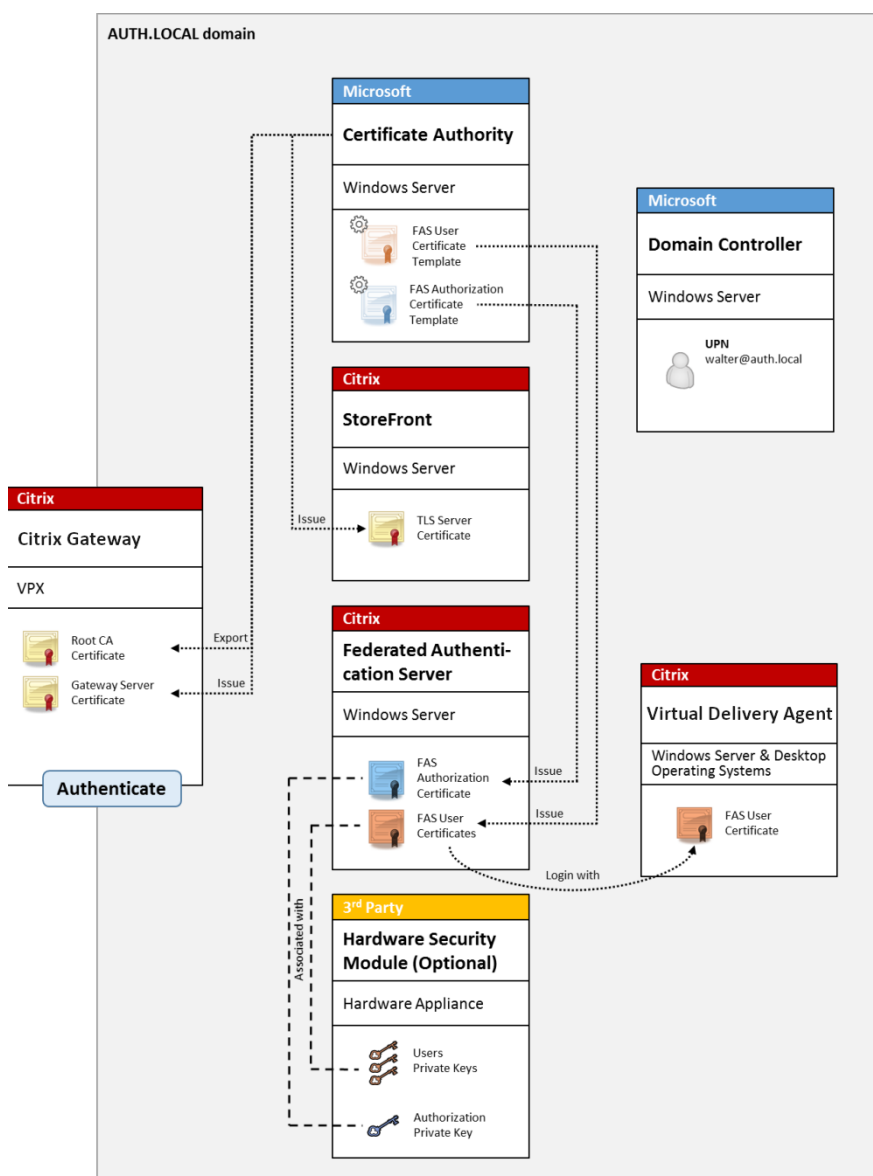
Informations connexes :

- Les clés peuvent être stockées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Pour de plus amples informations, veuillez consulter 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.

Add NetScaler Gateway Appliance

StoreFront

- ✓ General Settings
- ✓ Secure Ticket Authority
- Authentication Settings**
- Summary

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

Callback URL: https://NetScalerGatewayFQDN/CitrixAuthService/AuthService.aspx

When no Callback URL is specified, Smart Access is not available.

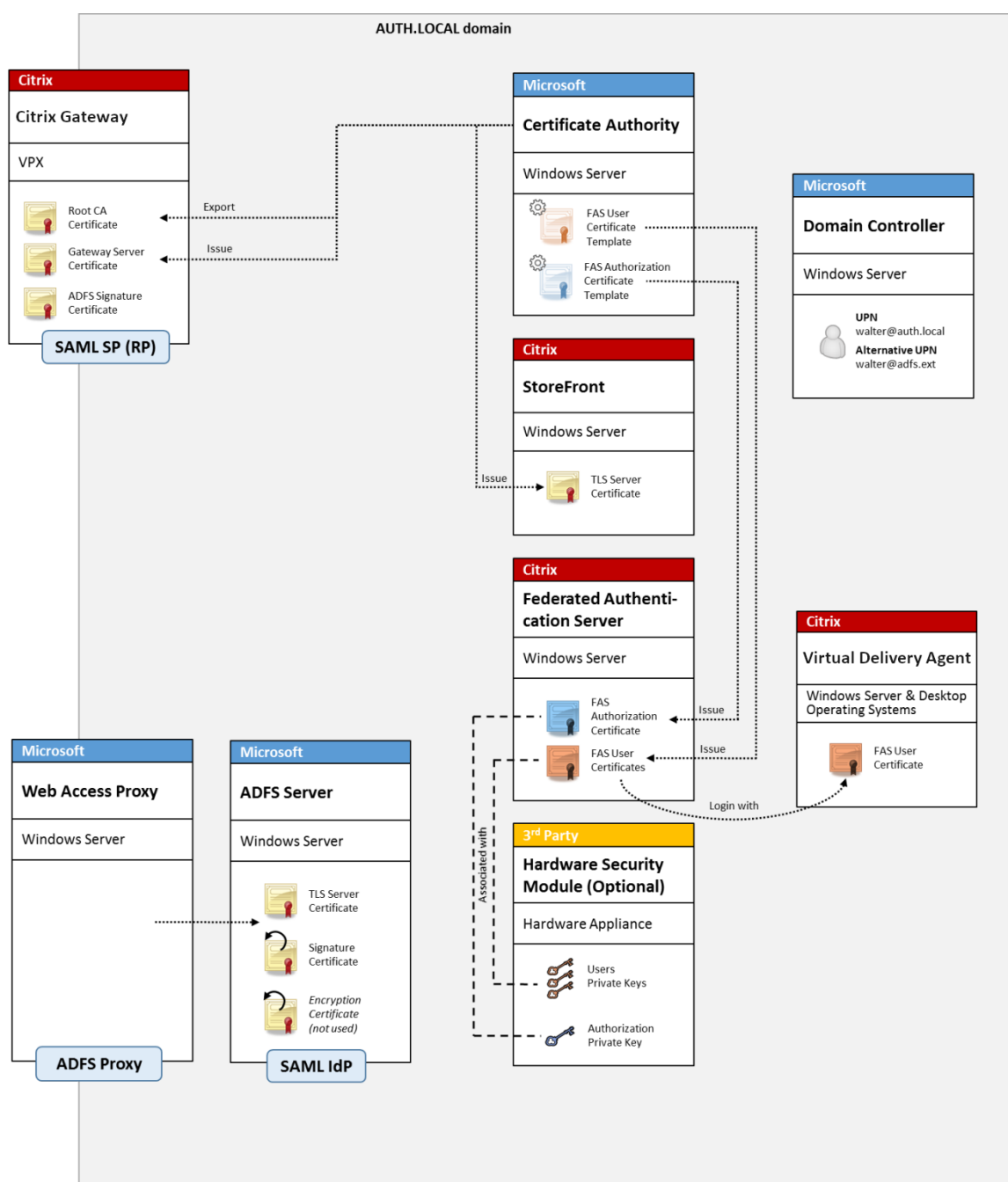
Back Create Cancel

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.

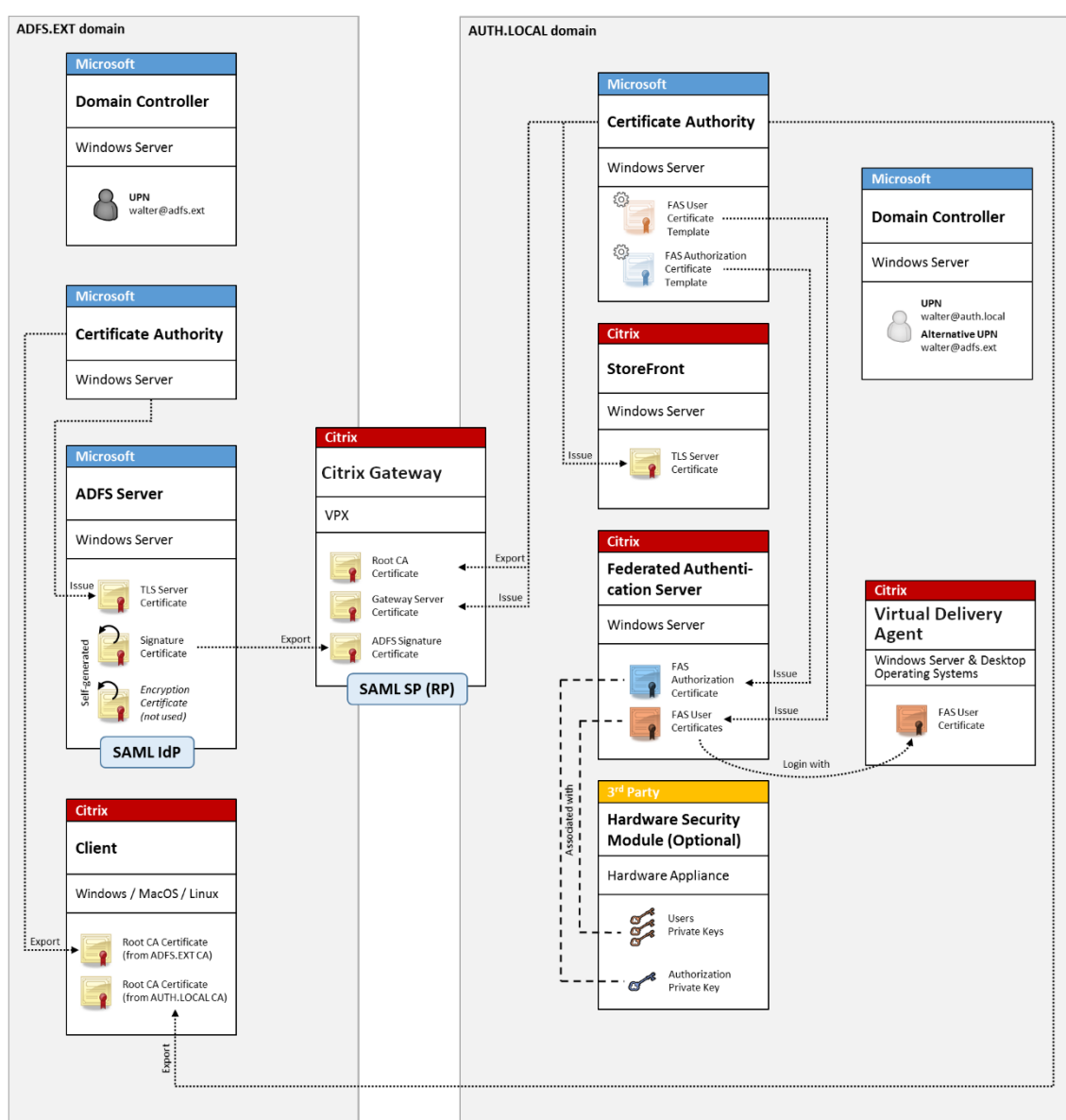
Informations connexes :

- L'article [Déploiement ADFS](#) contient des détails.
- 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.

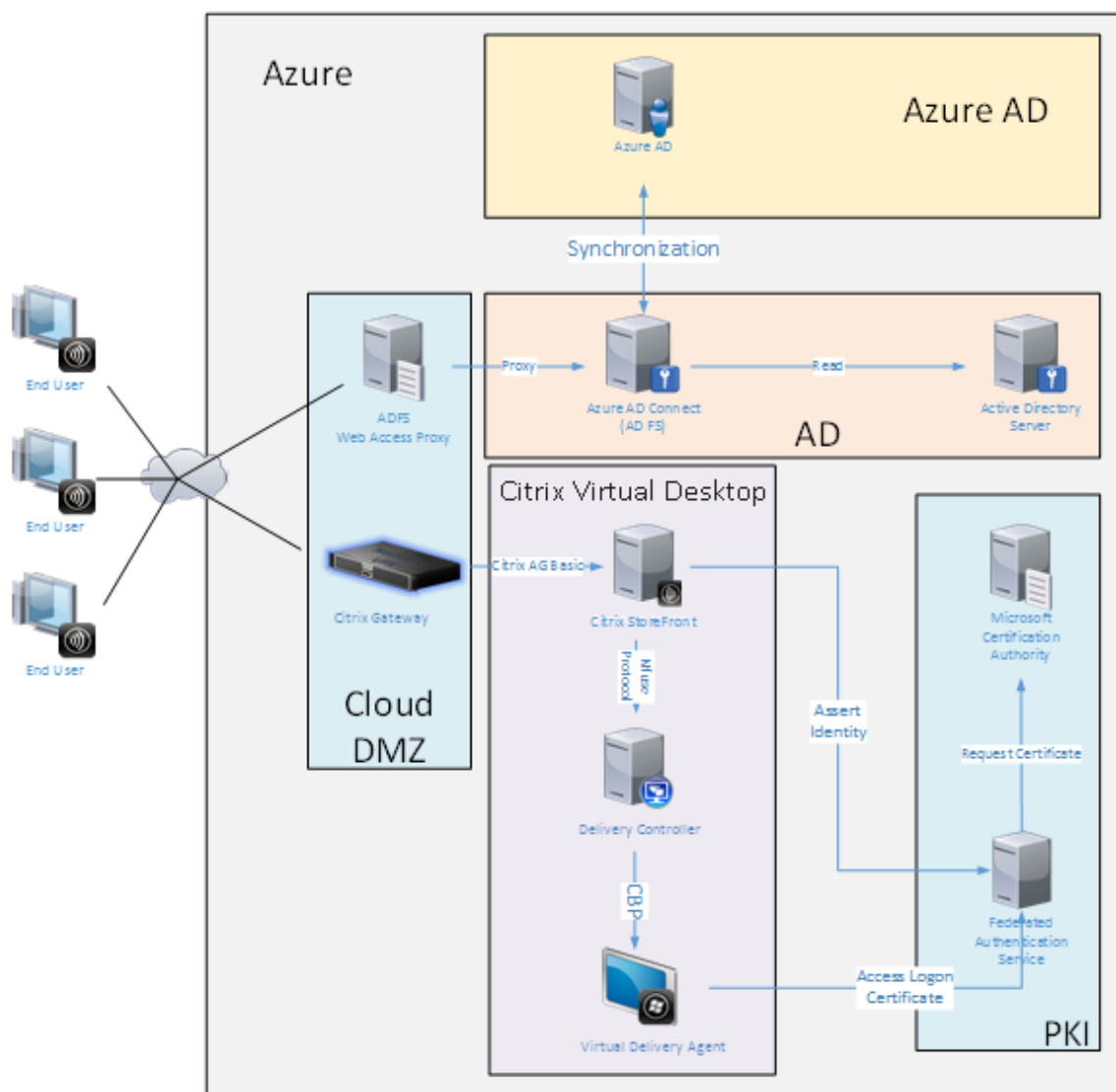


Informations connexes :

- 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.

Veillez 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.

Déploiement ADFS

April 2, 2020

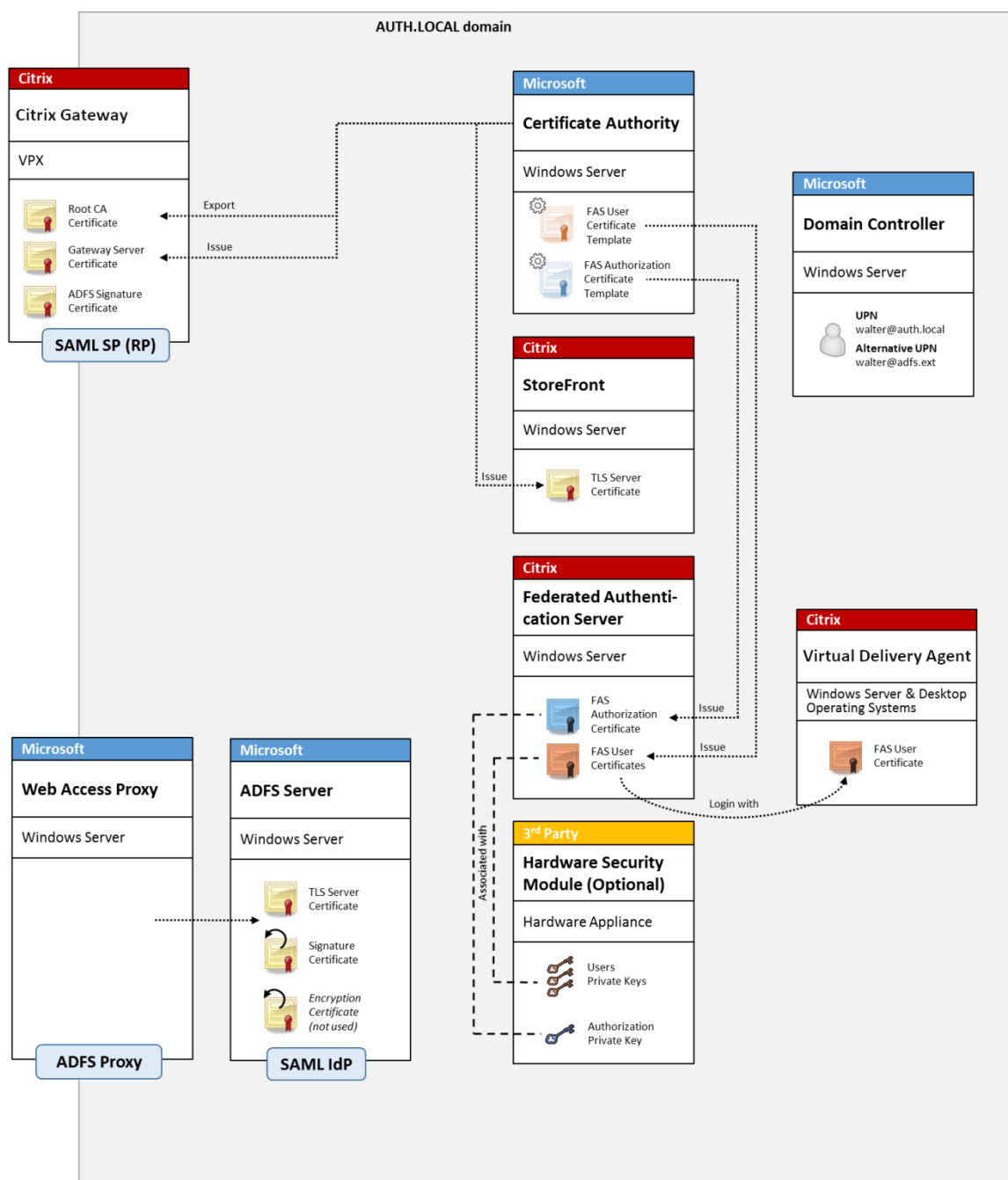
Introduction

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 le personnel de l'entreprise.

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



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/loginpage>.

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.

NetScaler > NetScaler Gateway > Policies > Authentication > SAML > Policies

Policies

Servers

Add

Edit

Delete

Show Bindings

Primary VPN Global Bindings

Search

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*

Authentication Type

SAML

IDP Certificate Name*

Redirect URL*

Single Logout URL

User Field

Signing Certificate Name

Issuer Name

Reject Unsigned Assertion*

SAML Binding*

Default Authentication Group

Skew Time(mins)

5

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

Attribute Consuming Service Index

Requested Authentication Context*

Authentication Class Types

Signature Algorithm*

☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method*

☐ SHA1 ☒ SHA256

☐ Send Thumbprint

☒ Enforce Username

Attribute 1

Attribute 3

Attribute 5

Attribute 7

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 [Architectures de déploiement](#).
- Des informations pratiques sont disponibles dans l'article [Configuration avancée](#).

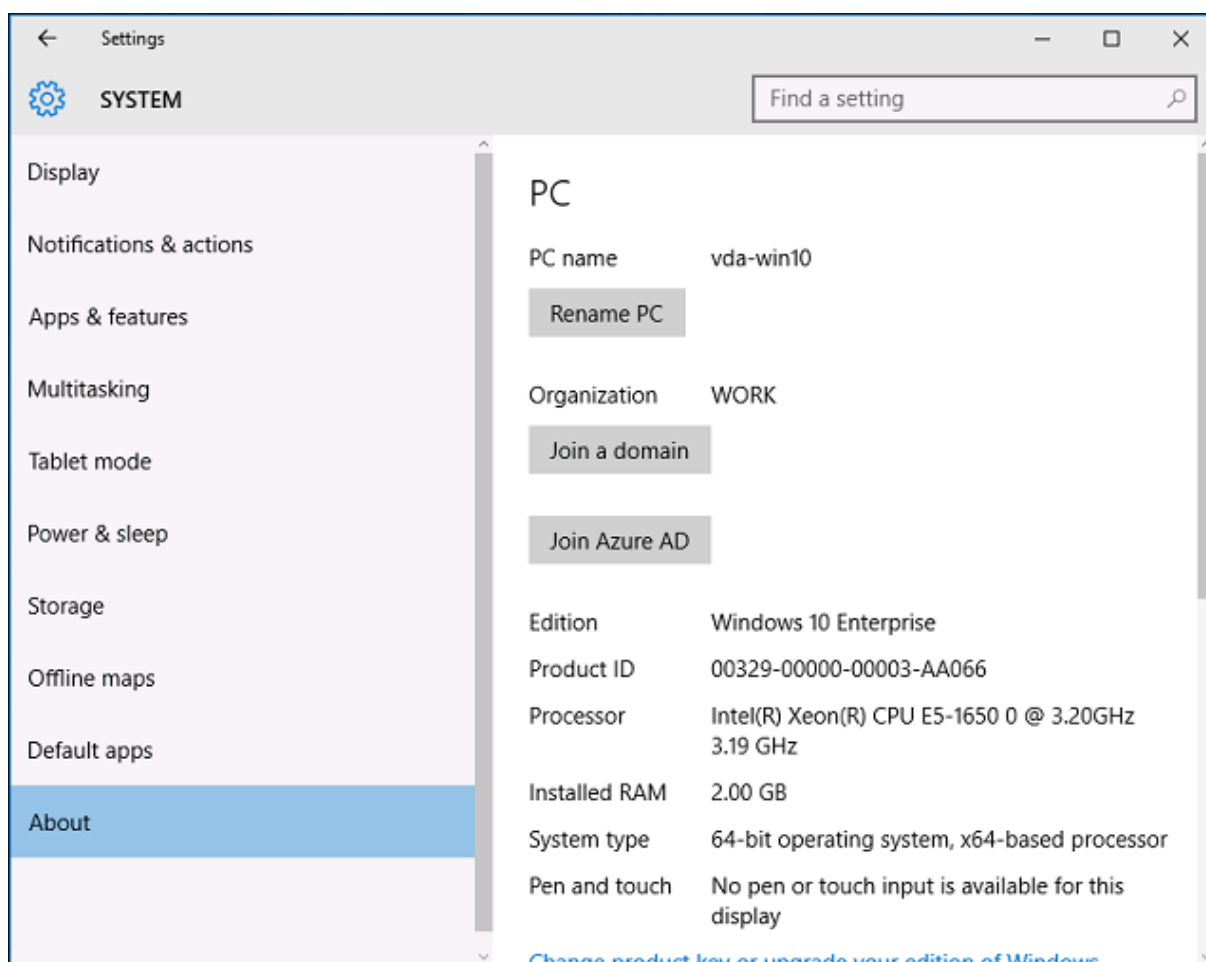
Intégration d'Azure AD

April 2, 2020

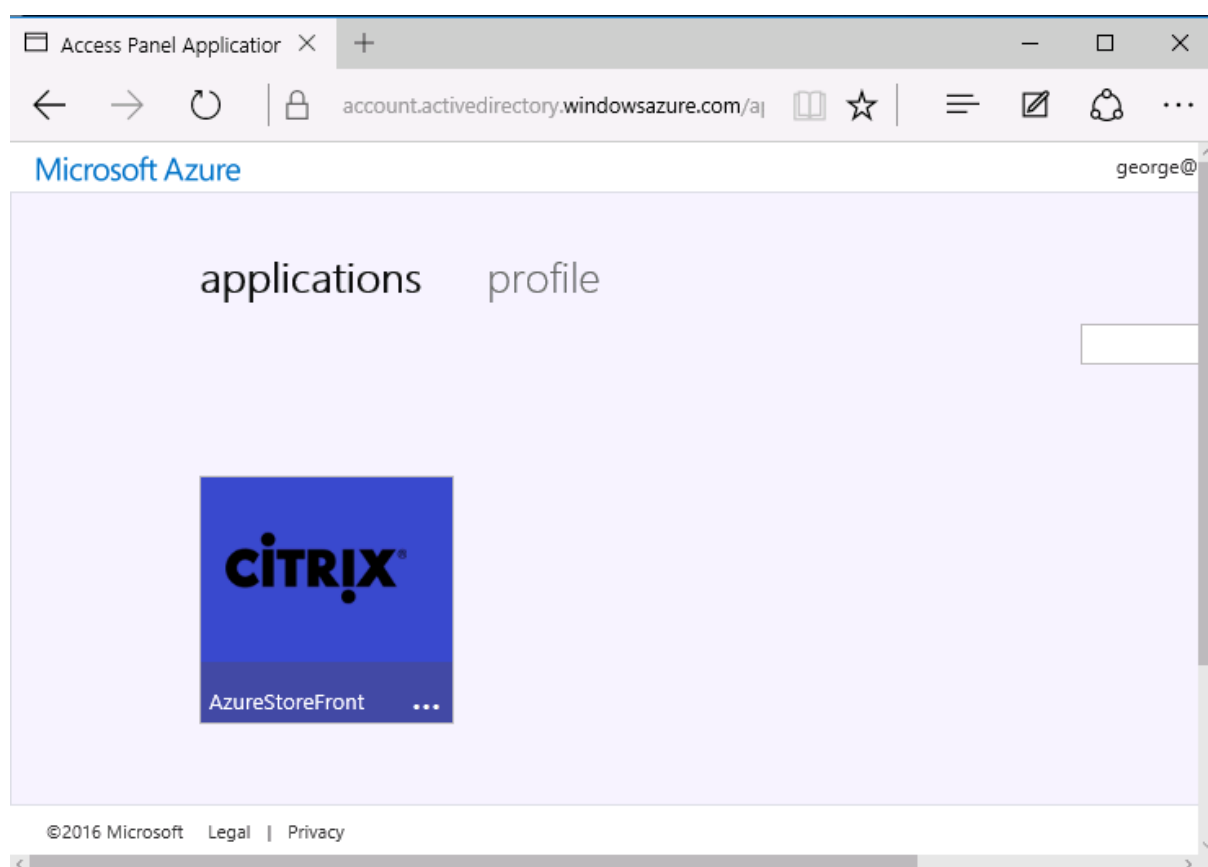
Introduction

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**.



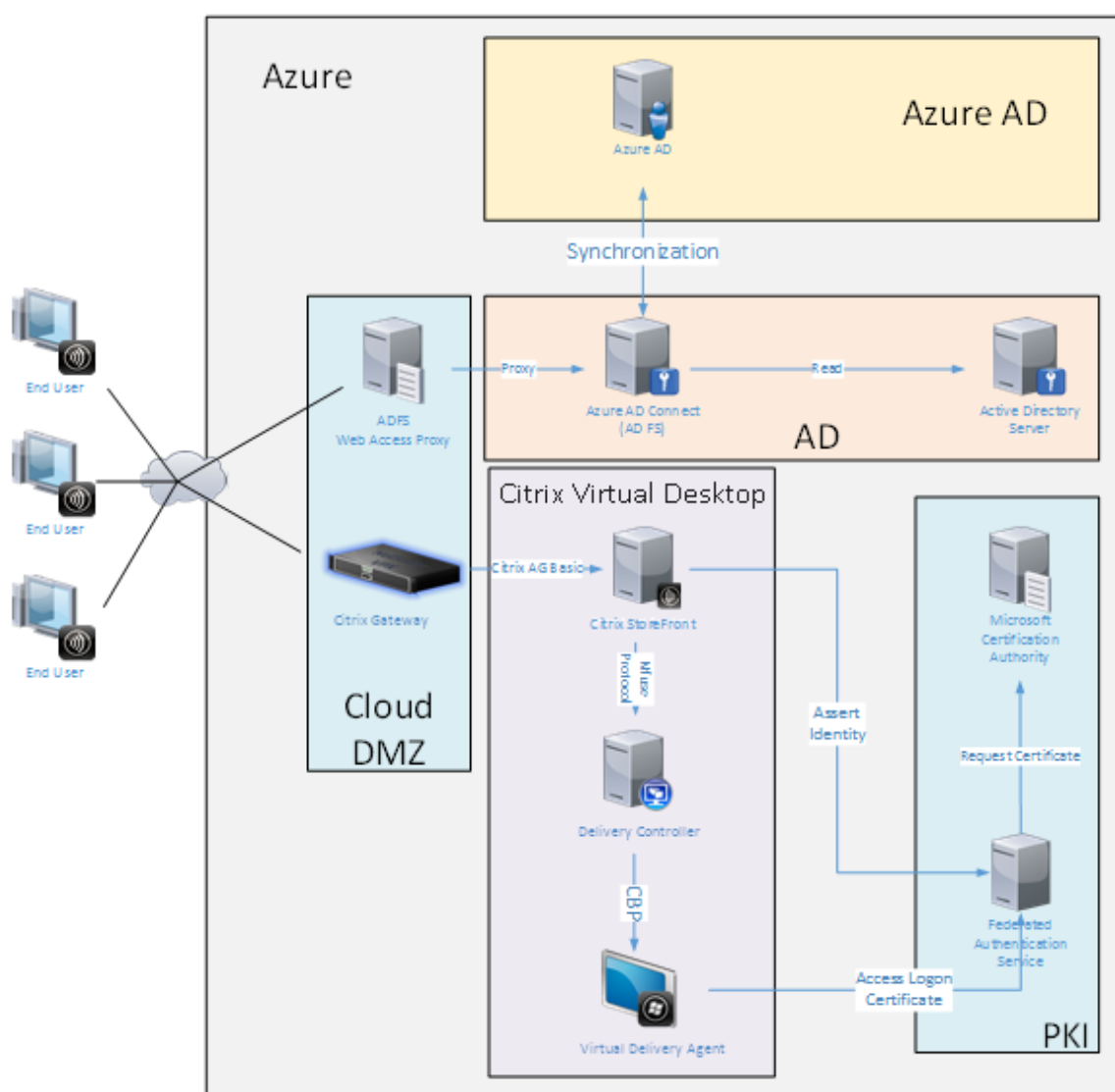
Une fois que l'ordinateur portable est inscrit, le navigateur Web Microsoft Edge se connecte automatiquement aux sites Web de l'entreprise et aux applications publiées Citrix via la page Web d'applications Azure SAAS, avec d'autres applications Azure telles que Microsoft Office 365.



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*.

The screenshot shows the 'DNS zone - PREVIEW' interface in Azure. The top bar includes a search icon, a close icon, and a toolbar with 'Settings', 'Record set', 'Delete', and 'Refresh' buttons. Below the toolbar, the 'Essentials' section displays the resource group 'citrixsamldemo', subscription name 'Visual Studio Professional with MSDN', and subscription ID 'df22436f-d4f9-46ae-be7b-6479cdaeefca'. To the right, it lists four name servers: ns1-01.azure-dns.com, ns2-01.azure-dns.net, ns3-01.azure-dns.org, and ns4-01.azure-dns.info. A link for 'All settings' is provided. Below this, a search bar for 'Search record sets' is present. The main table displays the following 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 ...
fs	CNAME	3600	adfs-citrixsamldemo.westeurope.cloud... ...

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, *citrixsamldemo*).

net. NS n1-01.azure-dns.com)

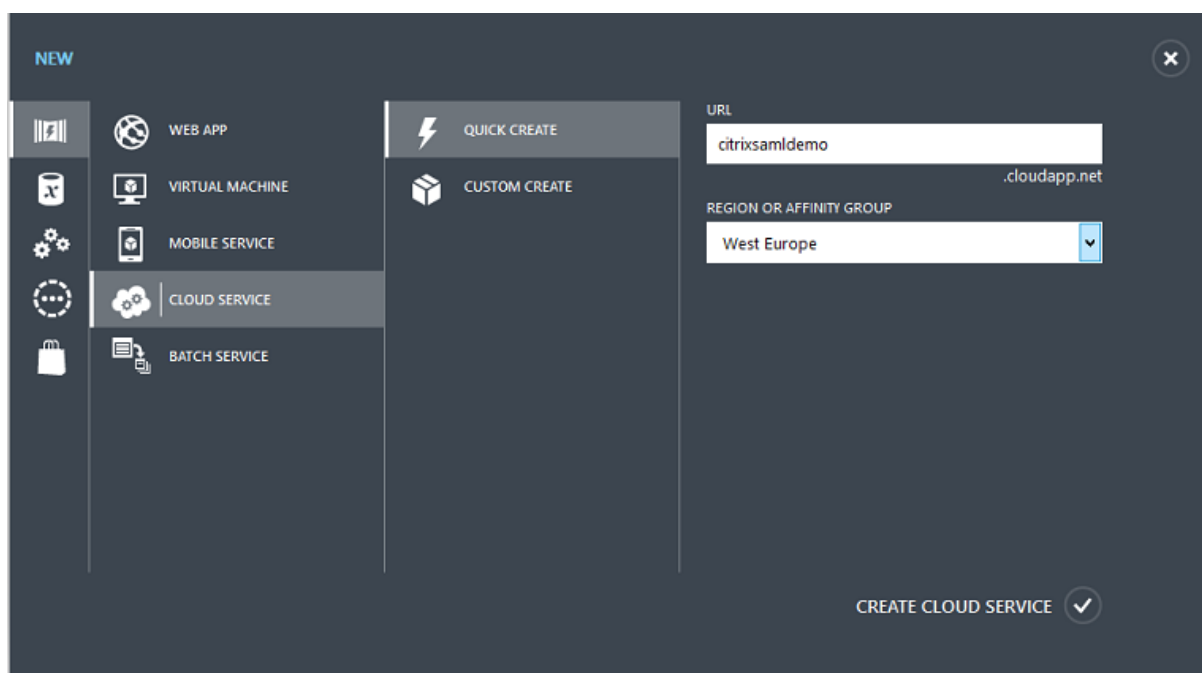
Lors de l'ajout de références aux VM exécutées dans Azure, il est plus facile d'utiliser un pointeur CNAME vers l'enregistrement DNS géré par Azure pour la VM. Si l'adresse IP de la VM change, vous n'aurez pas besoin de mettre à jour manuellement le fichier de la zone DNS.

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

Ajoutez une entrée « fs.citrixsamldemo.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 « citrixsamldemo » 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)
- Citrix Virtual Apps and Desktops Delivery Controller
- Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA)

Microsoft Azure

Create virtual machine > Basics

Create virtual machine

Basics

- 1 Basics
Configure basic settings
- 2 Size
Choose virtual machine size
- 3 Settings
Configure optional features
- 4 Summary
Windows Server 2012 R2 Datacenter

* Name

* User name

* Password

Subscription
Visual Studio Professional with MSDN

* Resource group
citrixsamldemo

Location
West Europe

OK

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

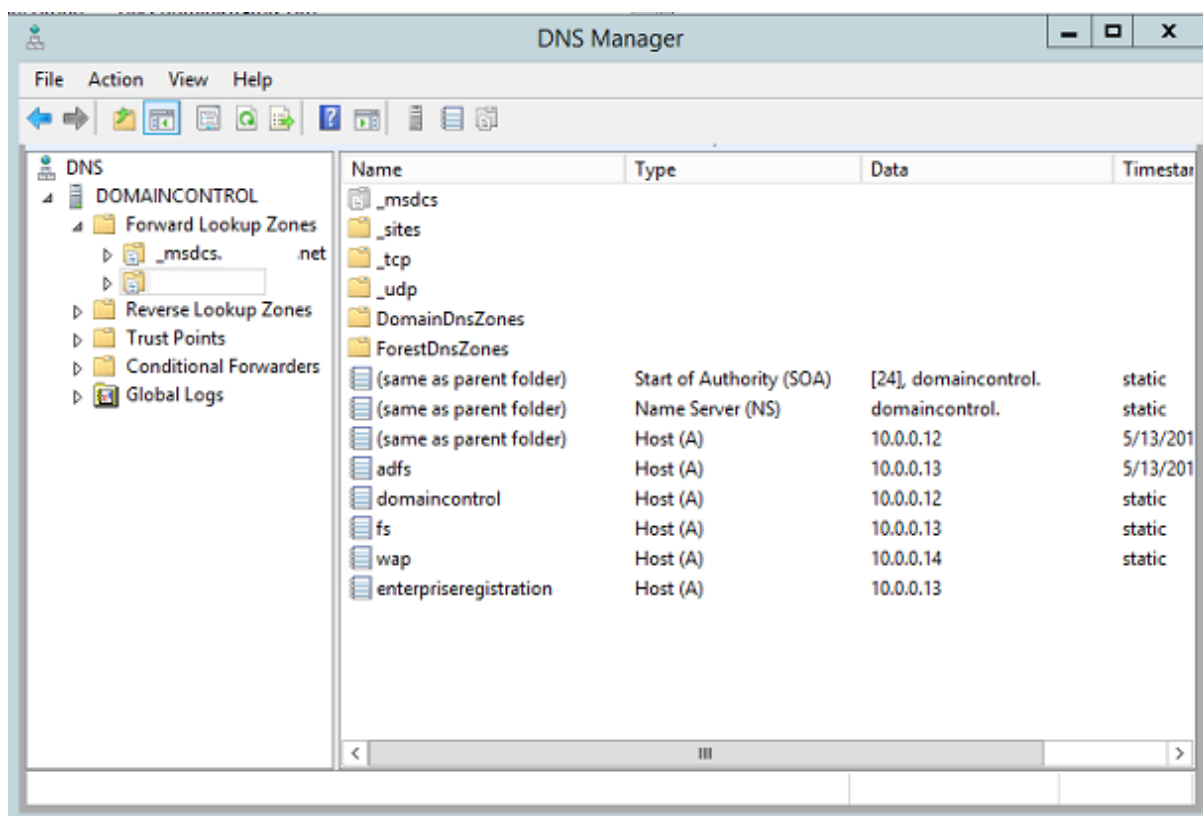
- Joignez le serveur ADFS au domaine citrixsamldemo. Le serveur proxy d'application Web doit rester dans un groupe de travail isolé, vous devez donc enregistrer une adresse DNS manuellement avec le DNS AD.
- Exécutez l'applet de commande **Enable-PSRemoting -Force** sur ces serveurs afin d'autoriser 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).

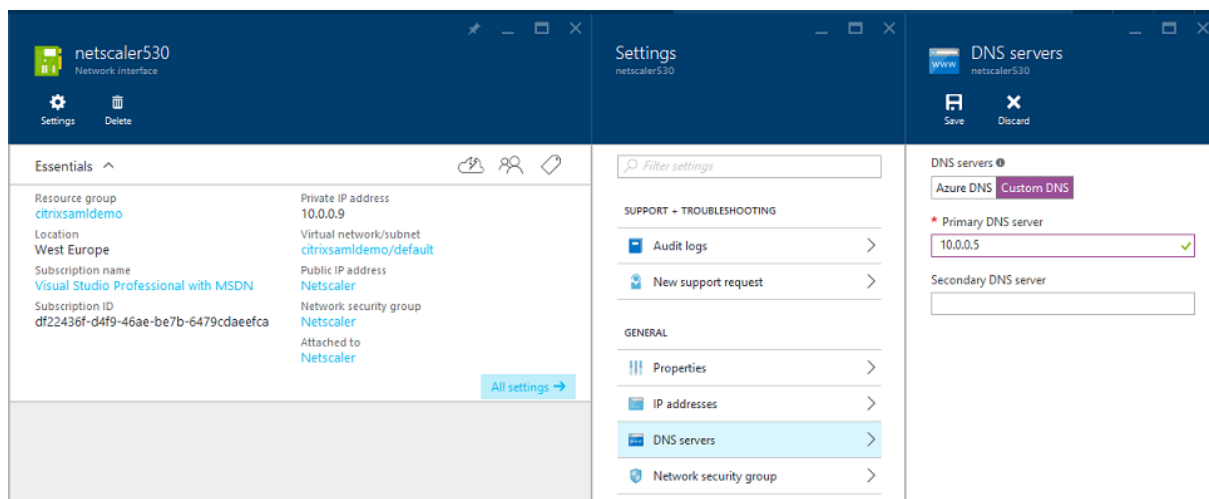


Ajoutez un enregistrement statique pour :

- wap.citrixsamldemo.net [la VM du proxy d'application Web ne sera pas jointe au domaine]

- fs.citrixsaml demo.net [adresse du serveur de fédération interne]
- enterpriseregistration.citrixsaml.net [identique à fs.citrixsaml demo.net]

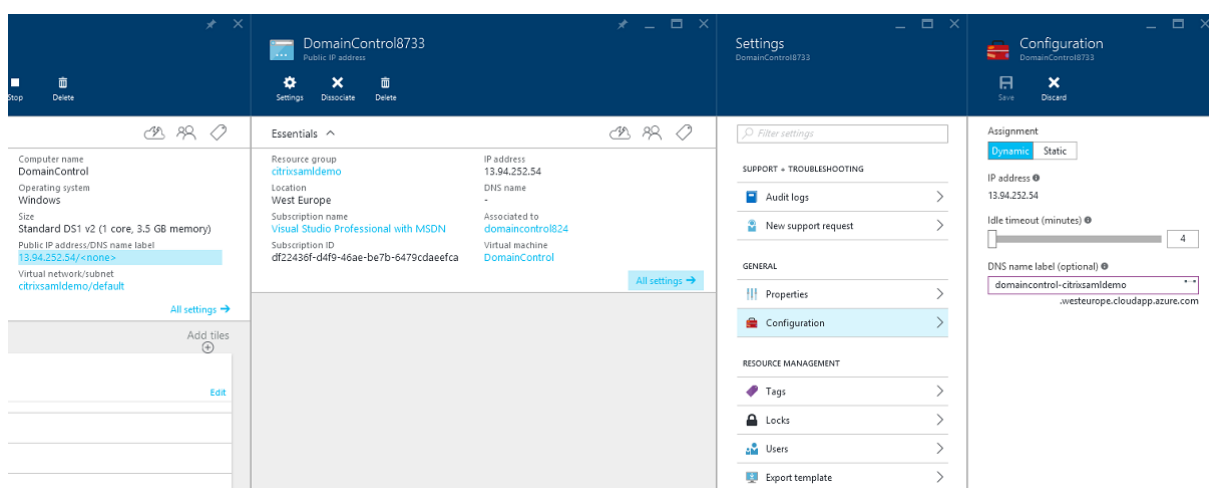
Toutes les VM exécutées dans Azure doivent être configurées pour utiliser uniquement ce serveur DNS. Vous pouvez effectuer cette opération à l'aide de l'interface réseau.



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.

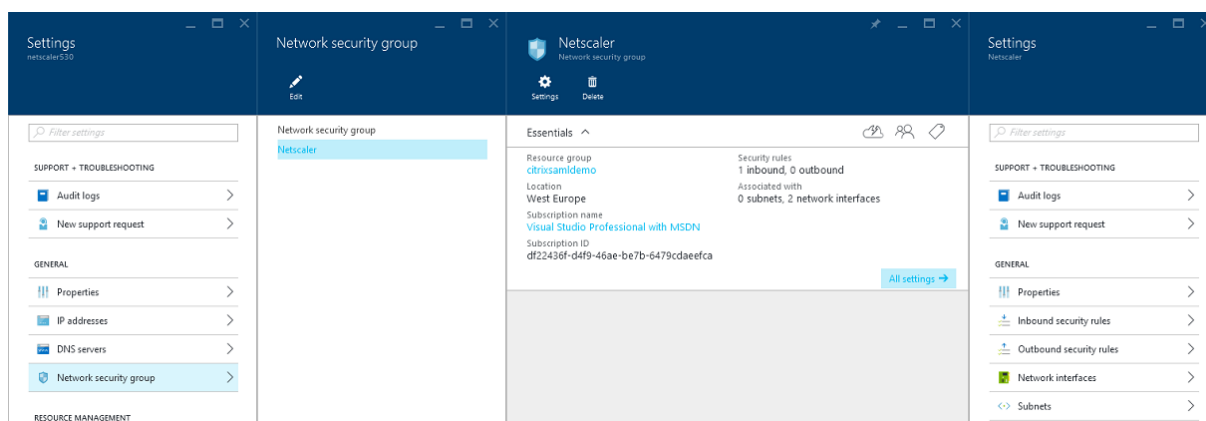


Cet exemple attribue l'adresse DNS domaincontrol-citrixsaml demo.westeurope.cloudapp.azure.com au contrôleur de domaine.

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.

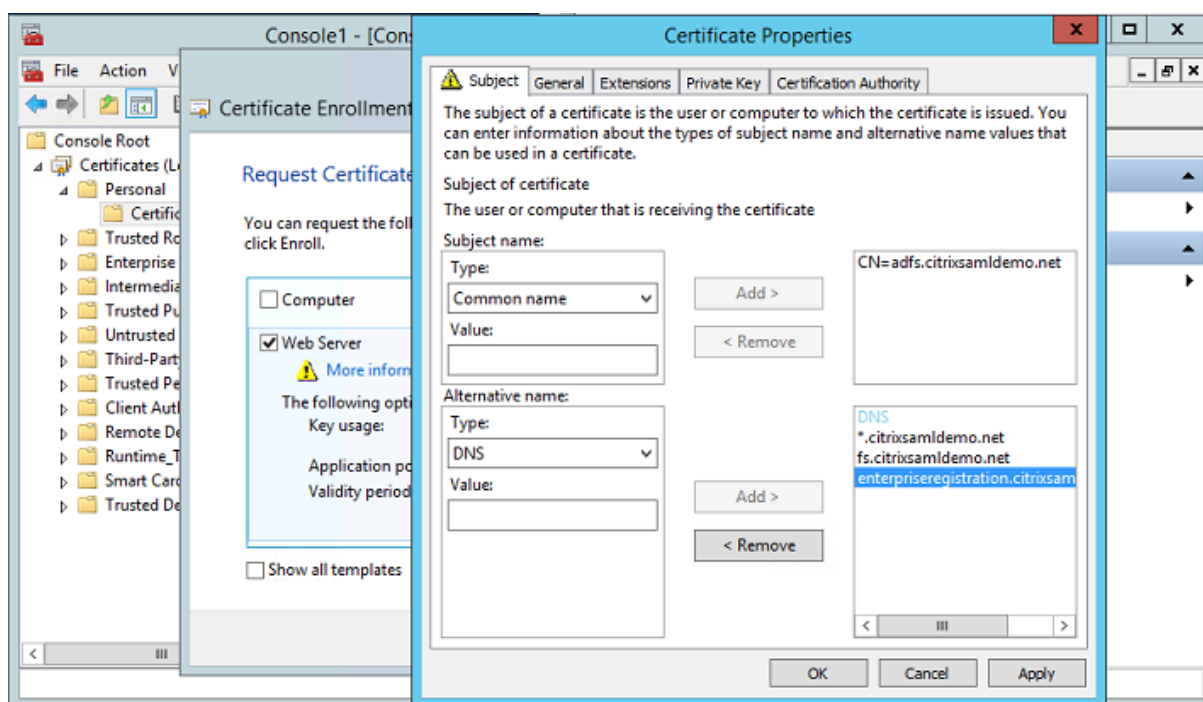


Créer un certificat d'ADFS

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.citrixsaml-demo.net [nom de l'ordinateur]
- SubjectAltname:
 - *.citrixsaml-demo.net [nom de la zone]
 - fs.citrixsaml-demo.net [entrée dans le DNS]
 - enterpriseregistration.citrixsaml-demo.net



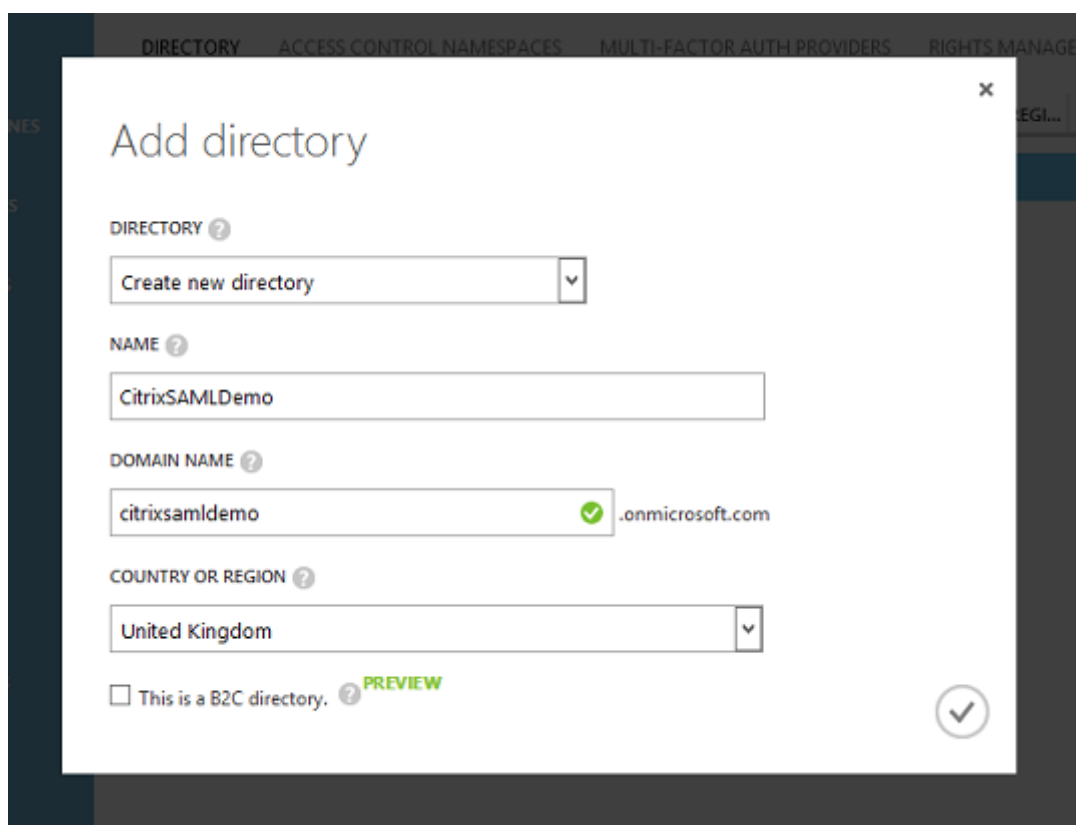
Exportez le certificat sur un fichier pfx, y compris une clé privée protégée par mot de passe.

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.



The screenshot shows the 'Add directory' dialog box in the Azure AD portal. The dialog has a title bar with a close button (X). The main content area is titled 'Add directory'. Below the title, there are several fields and a checkbox:

- DIRECTORY** (with a help icon ?): A dropdown menu showing 'Create new directory'.
- NAME** (with a help icon ?): A text input field containing 'CitrixSAMLdemo'.
- DOMAIN NAME** (with a help icon ?): A text input field containing 'citrixsaml demo', followed by a green checkmark icon and the text '.onmicrosoft.com'.
- COUNTRY OR REGION** (with a help icon ?): A dropdown menu showing 'United Kingdom'.
- Checkbox**: A checkbox labeled 'This is a B2C directory.' (with a help icon ?) and a green 'PREVIEW' label.

A large green checkmark icon is located in the bottom right corner of the dialog box.

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

citrixsamldemo

 [USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#)
[LICENSES](#)



Your directory is ready to use.

Here are a few options to get started.

☐ Skip Quick Start the next time I visit

I WANT TO [Set Up Directory](#) [Manage Access](#) [Develop Applications](#)

GET STARTED

- #### 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 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@citrixsamldemo.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

MULTI-FACTOR AUTHENTICATION ?
☐ Enable Multi-Factor Authentication

1 3

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.

ADD DOMAIN

Specify a domain name

Enter the name of a domain that your organization owns. ?

DOMAIN NAME

citrixsamldemo.net

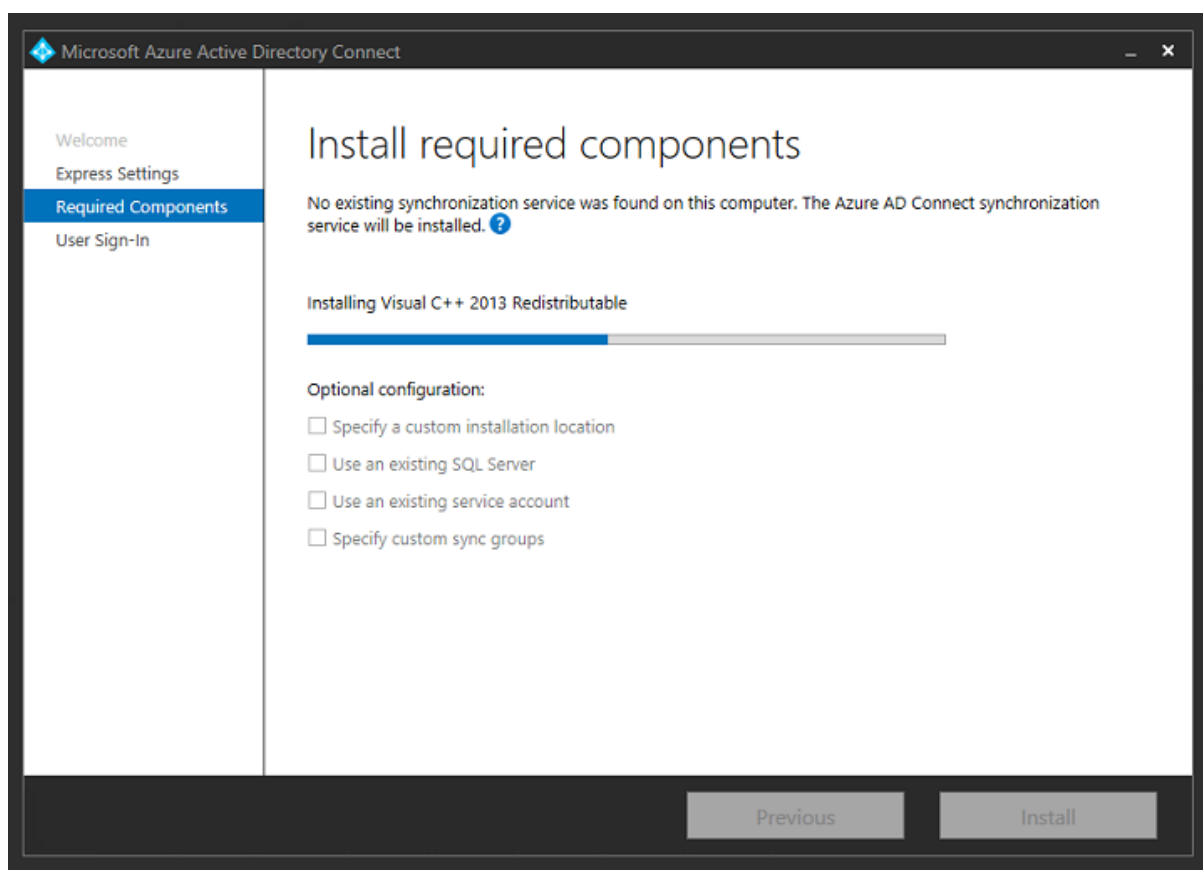
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

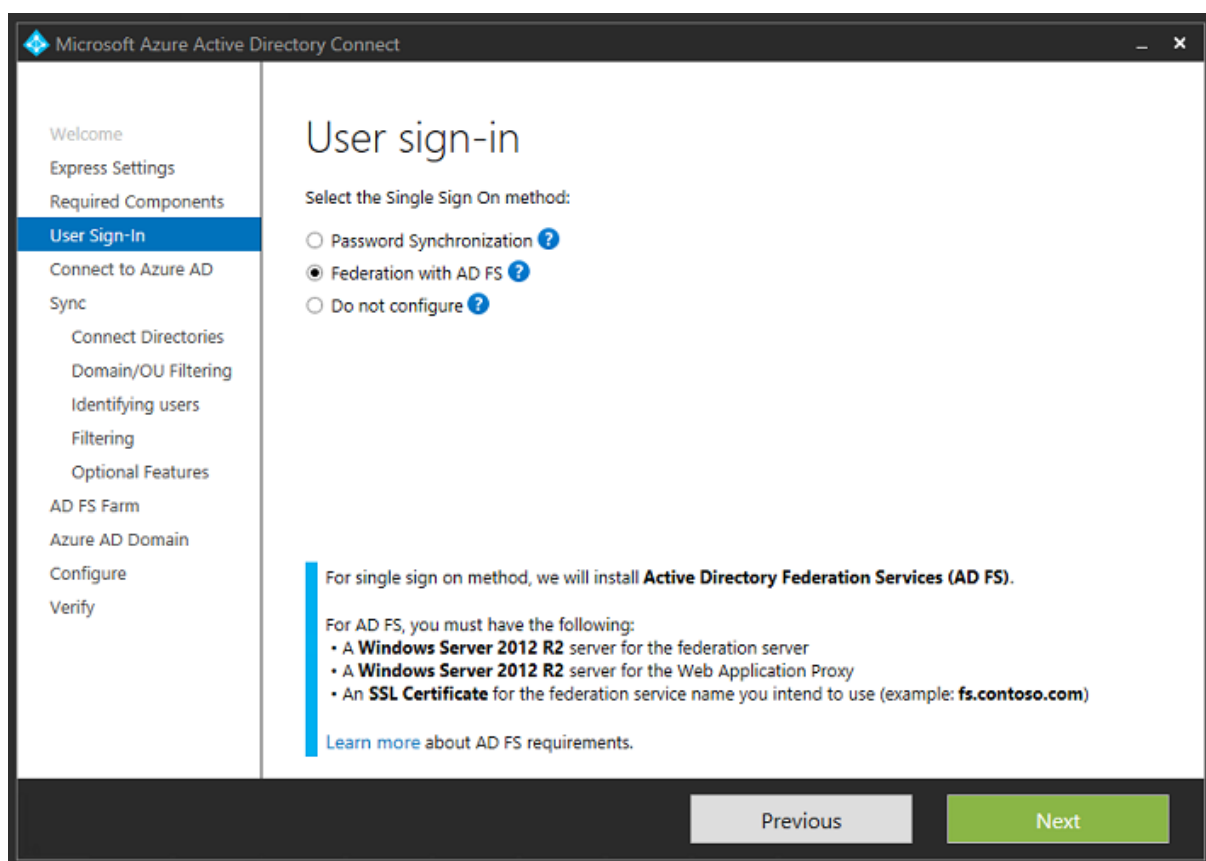
2

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.

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

Domain/OU Filtering

Identifying users

Filtering

Optional Features

AD FS Farm

Azure AD Domain

Configure

Verify

Connect to Azure AD

Enter your Azure AD credentials: ?

USERNAME

AzureAdmin@citrixsaml demo.onmicrosoft.com

PASSWORD

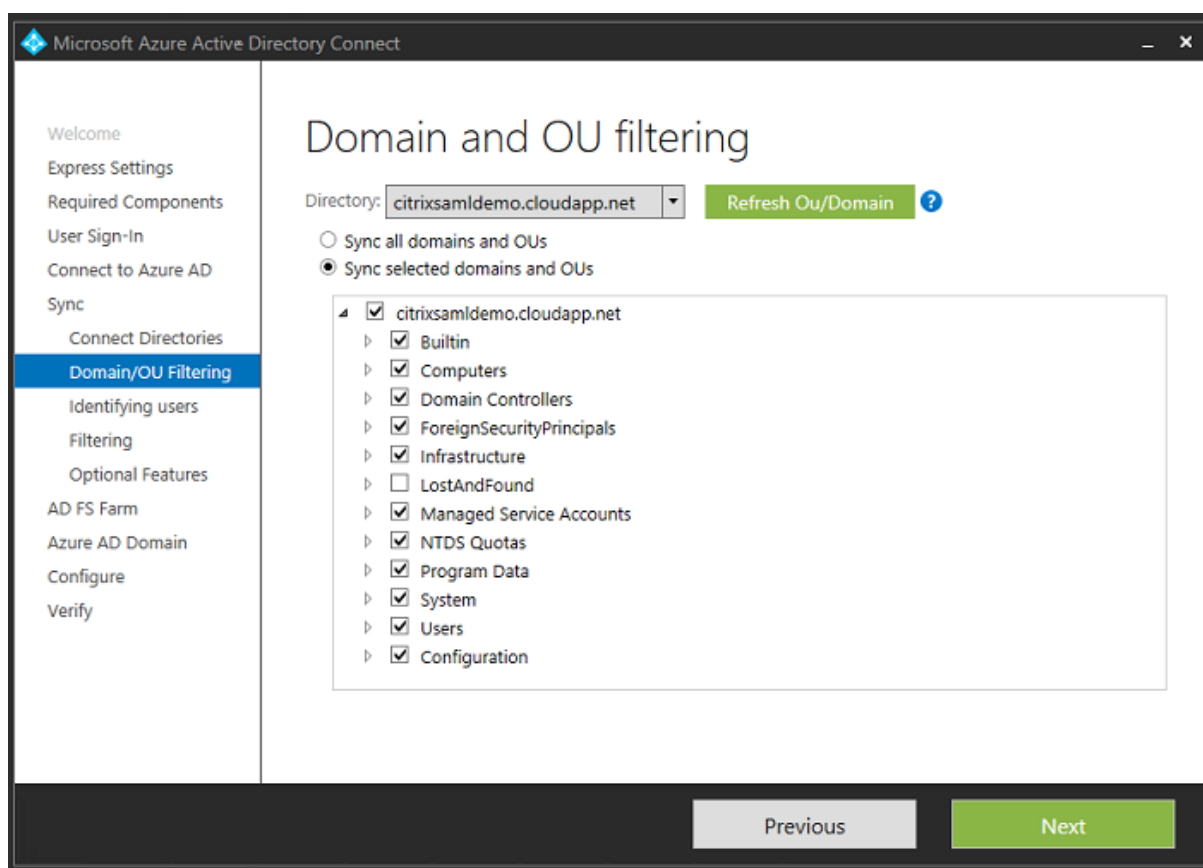
.....

Previous Next

Sélectionnez la forêt AD interne.

The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar includes the Microsoft logo and the text 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with the following items: 'Welcome', 'Express Settings', 'Required Components', 'User Sign-In', 'Connect to Azure AD', 'Sync', 'Connect Directories' (highlighted in blue), 'Domain/OU Filtering', 'Identifying users', 'Filtering', 'Optional Features', 'AD FS Farm', 'Azure AD Domain', 'Configure', and 'Verify'. The main area is titled 'Connect your directories' and contains the instruction 'Enter connection information for your on-premises directories or forests: ?'. Below this are four input fields: 'DIRECTORY TYPE' (a dropdown menu showing 'Active Directory'), 'FOREST ?' (a dropdown menu showing 'citrixsaml-demo.cloudapp.net'), 'USERNAME' (a text box containing 'CITRIXSAMLDEMO\Administrator'), and 'PASSWORD' (a masked text box with dots). To the right of the password field is a green 'Add Directory' button. Below these fields is a section titled 'CONFIGURED DIRECTORIES' which lists 'citrixsaml-demo.cloudapp.net (Active Directory)' with a green checkmark icon. To the right of this entry is a blue 'Remove' link. At the bottom of the window are two buttons: 'Previous' (disabled) and 'Next' (active).

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.

The screenshot shows the 'Identifying users' step in the Microsoft Azure Active Directory Connect wizard. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering, Identifying users (highlighted), Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Uniquely identifying your users' and contains the following options:

Select how users should be identified in your on-premises directories. ?

- ☒ Users are represented only once across all directories.
- ☐ User identities exist across multiple directories. Match using:
 - ☒ Mail attribute
 - ☐ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
 - ☐ SAMAccountName and MailNickName attributes
 - ☐ A specific attribute

CUSTOM ATTRIBUTE

Select how users should be identified with Azure AD.

SOURCE ANCHOR ?

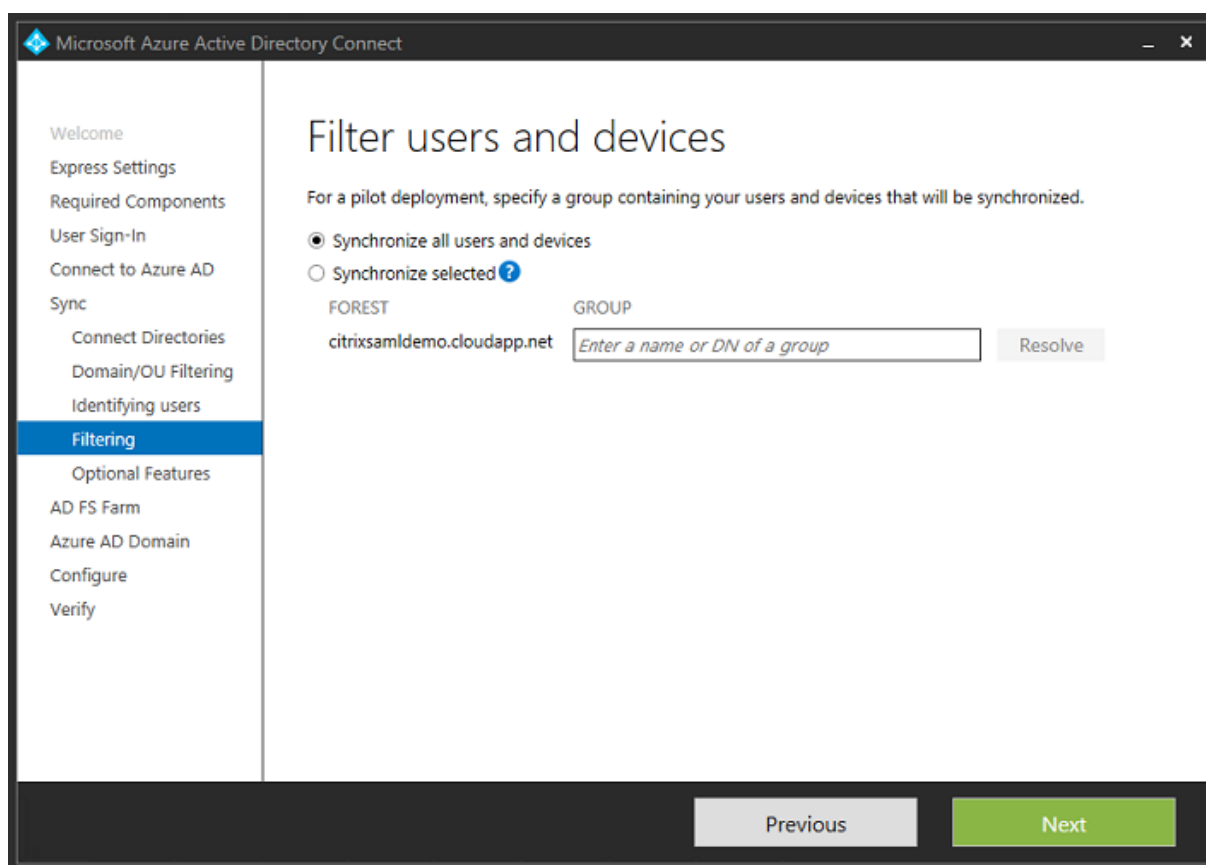
objectGUID

USER PRINCIPAL NAME ?

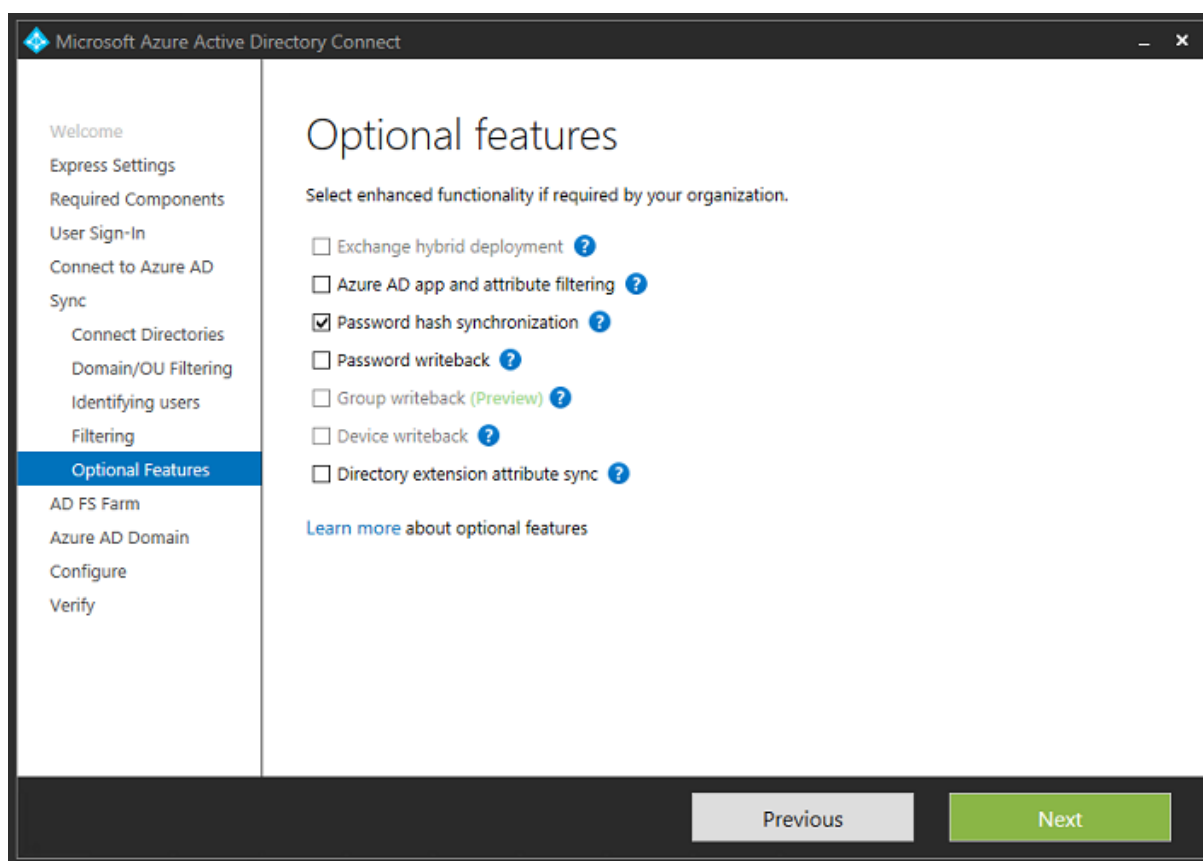
userPrincipalName

At the bottom of the window, there are two buttons: 'Previous' and 'Next'.

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.

Microsoft Azure Active Directory Connect

AD FS Farm

Configure a new Windows Server 2012 R2 AD FS farm

Use an existing Windows Server 2012 R2 AD FS farm

Specify the SSL certificate used to secure the communication between clients and AD FS.

☒ Provide a PFX Certificate File

☐ Use a Certificate installed on the Federation Machines

CERTIFICATE FILE ?

C:\Users\Fred.CITRIXSAMLDEMO\Desktop\adfs.pfx Browse

SUBJECT NAME

*.citrixsaml demo.net

SUBJECT NAME PREFIX

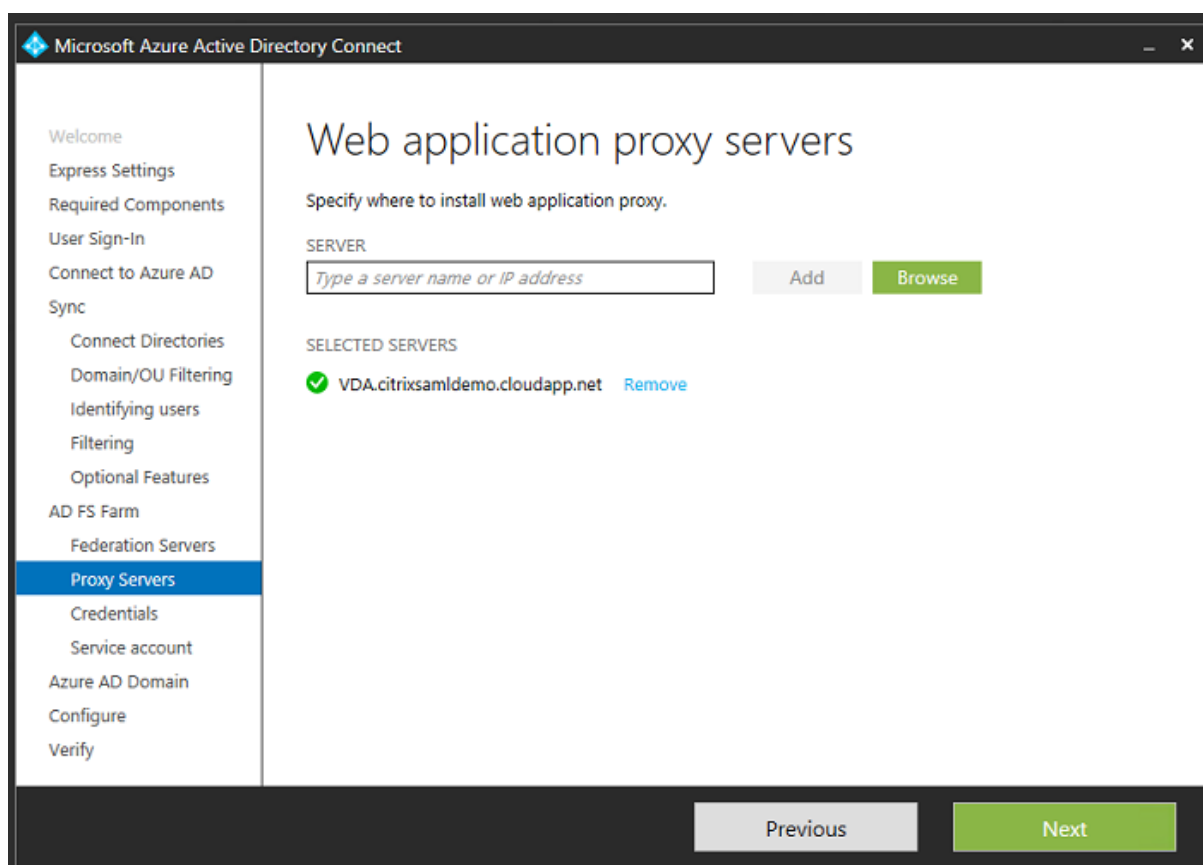
fs ✓

FEDERATION SERVICE NAME

https://fs.citrixsaml demo.net

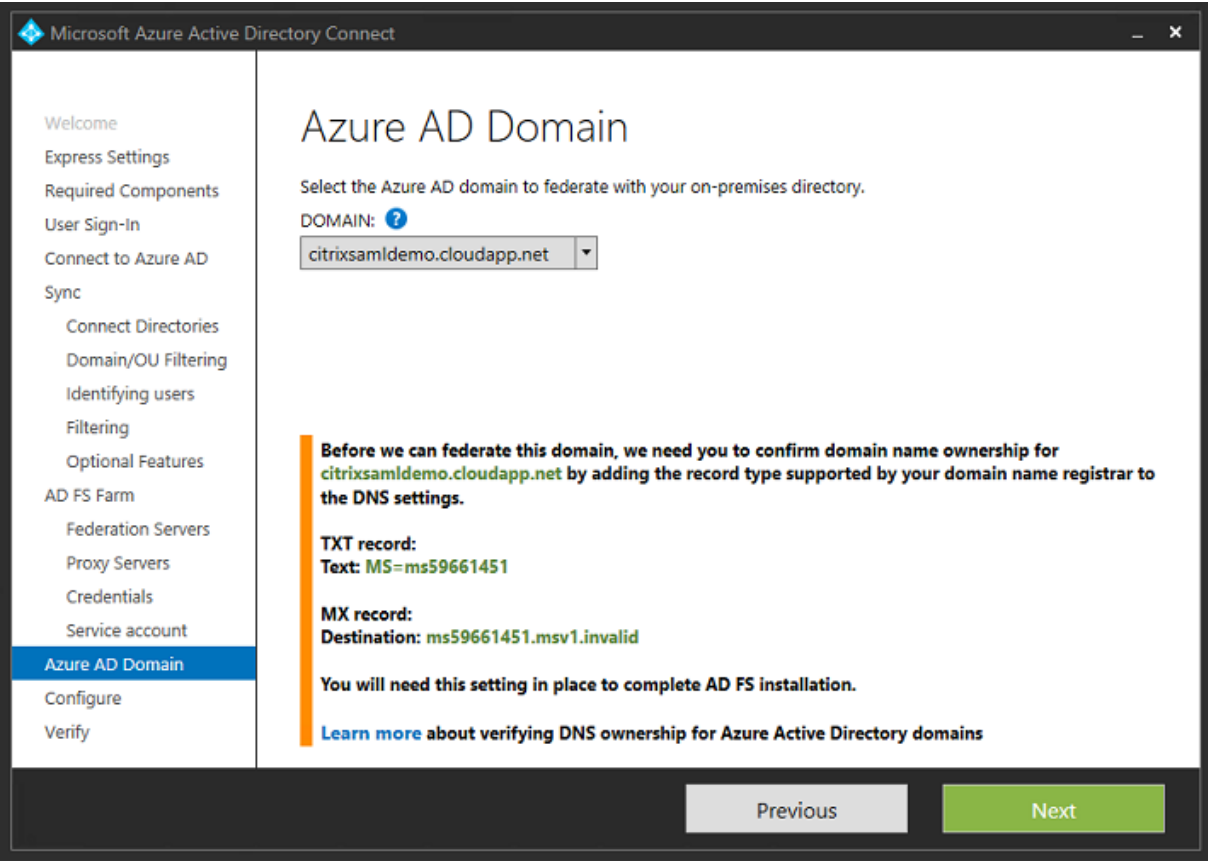
Previous Next

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.com. 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.cloudapp.azure.com ...

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

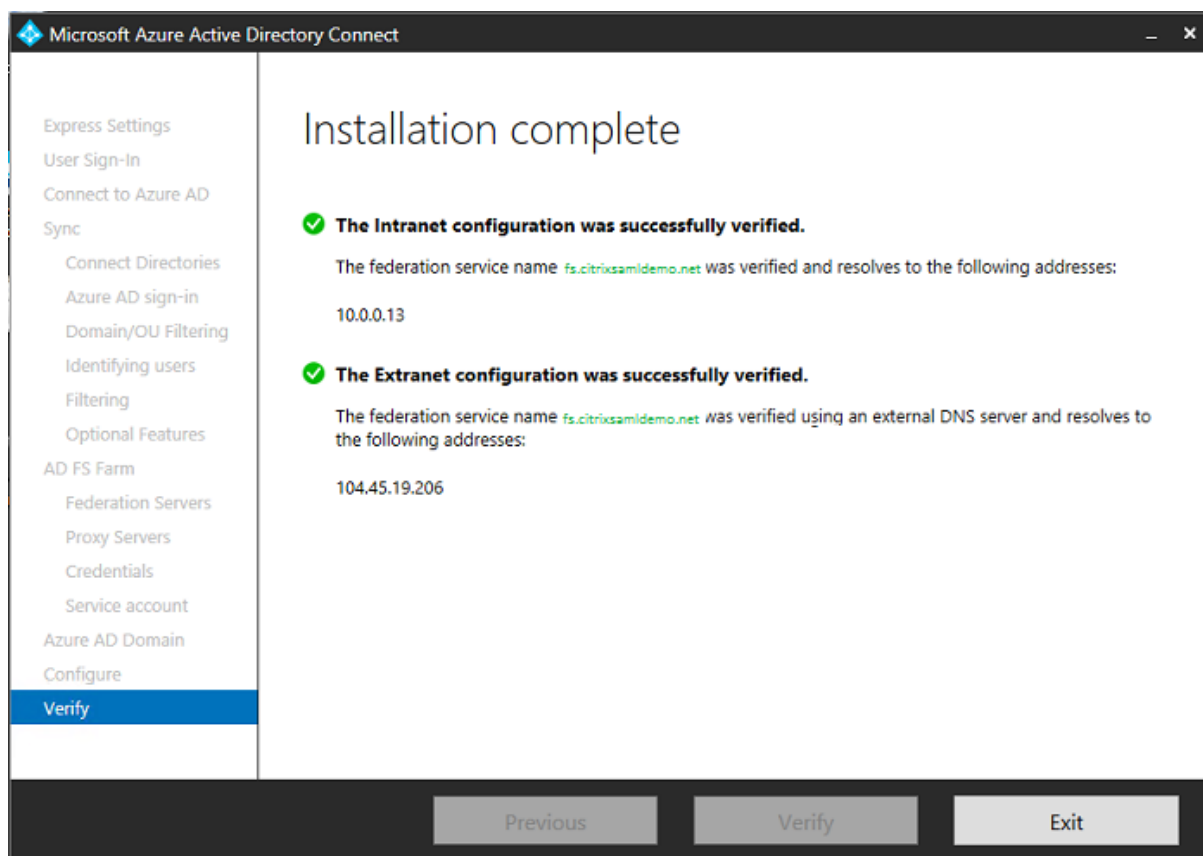
CitrixSamlDemo

DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY DOMAIN	
citrixsaml-demo.onmicrosoft.com	Basic	✓ Active	Not Available	Yes	
citrixsaml-demo.net	Custom	⚠ Unverified	Not Configured	No	

Remarque :

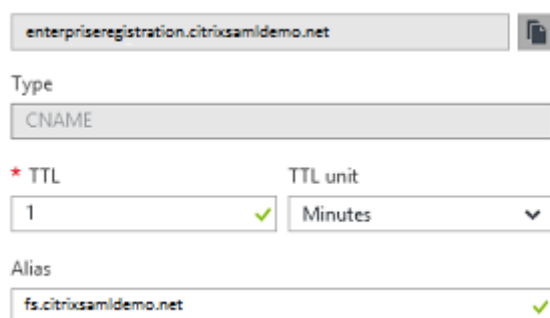
Si cette étape échoue, vous pouvez vérifier le domaine avant d'exécuter Azure AD Connect.

Lorsque l'installation est terminée, l'adresse externe fs.citrixsaml-demo.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.



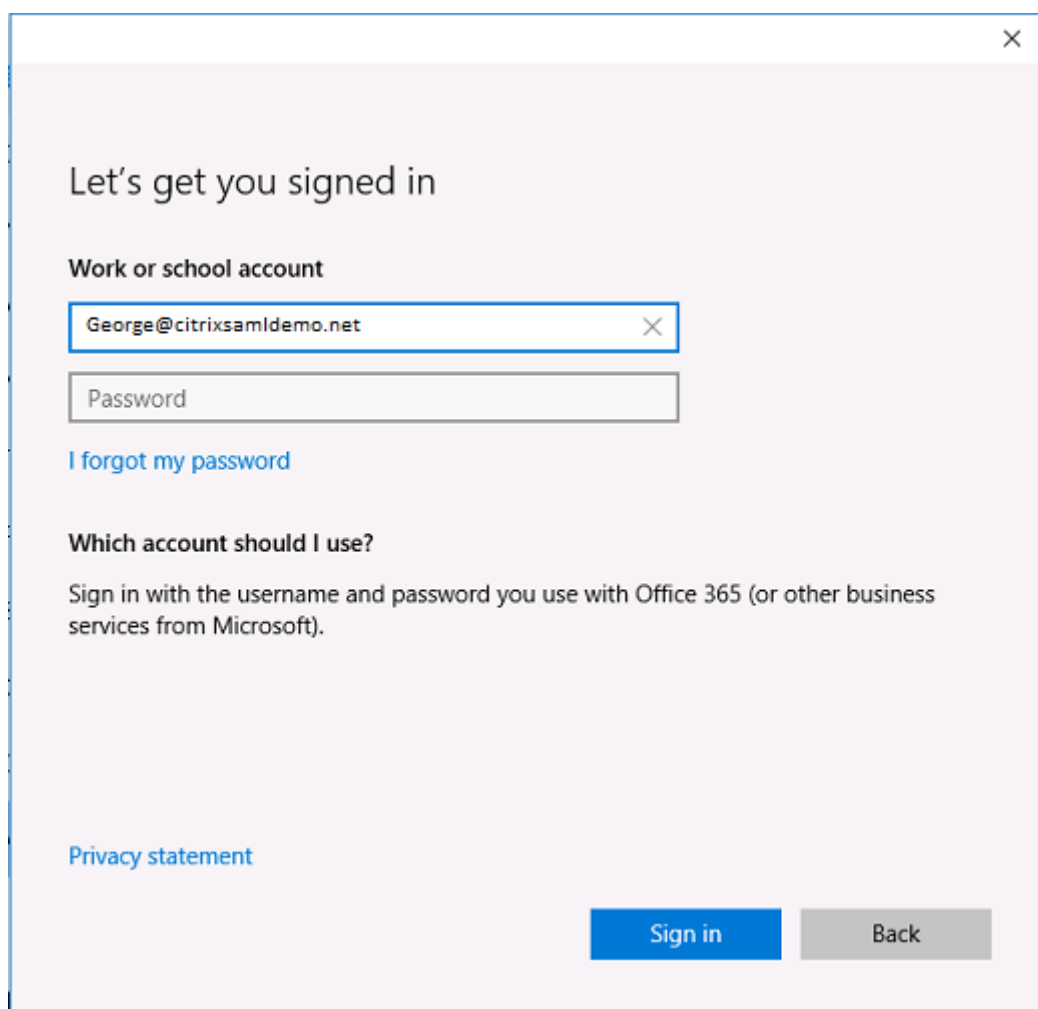
enterpriseregistration.citrixsaml demo.net

Type
CNAME

* TTL TTL unit
1 Minutes

Alias
fs.citrixsaml demo.net

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.



Let's get you signed in

Work or school account

George@citrixsaml demo.net

Password

[I forgot my password](#)

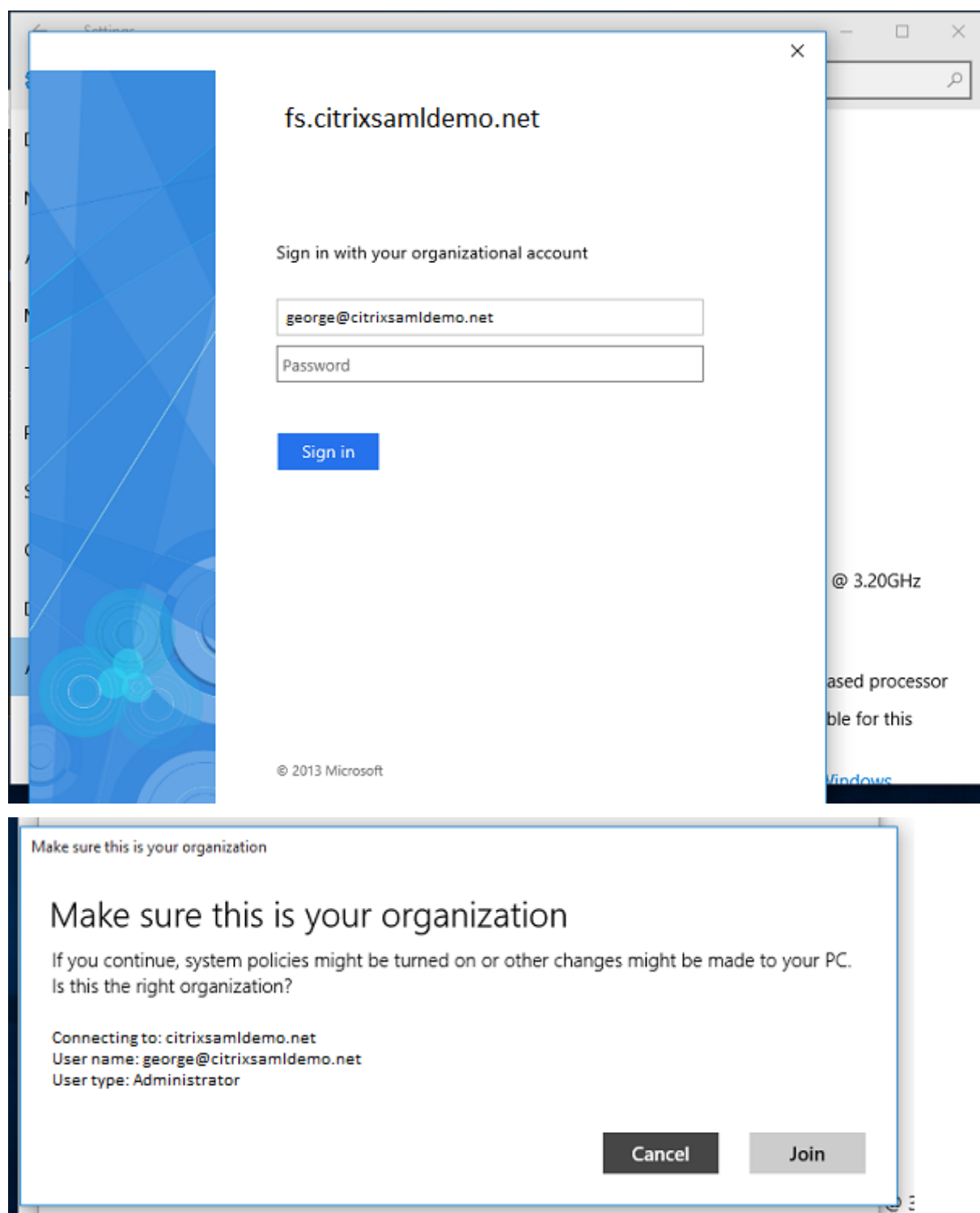
Which account should I use?

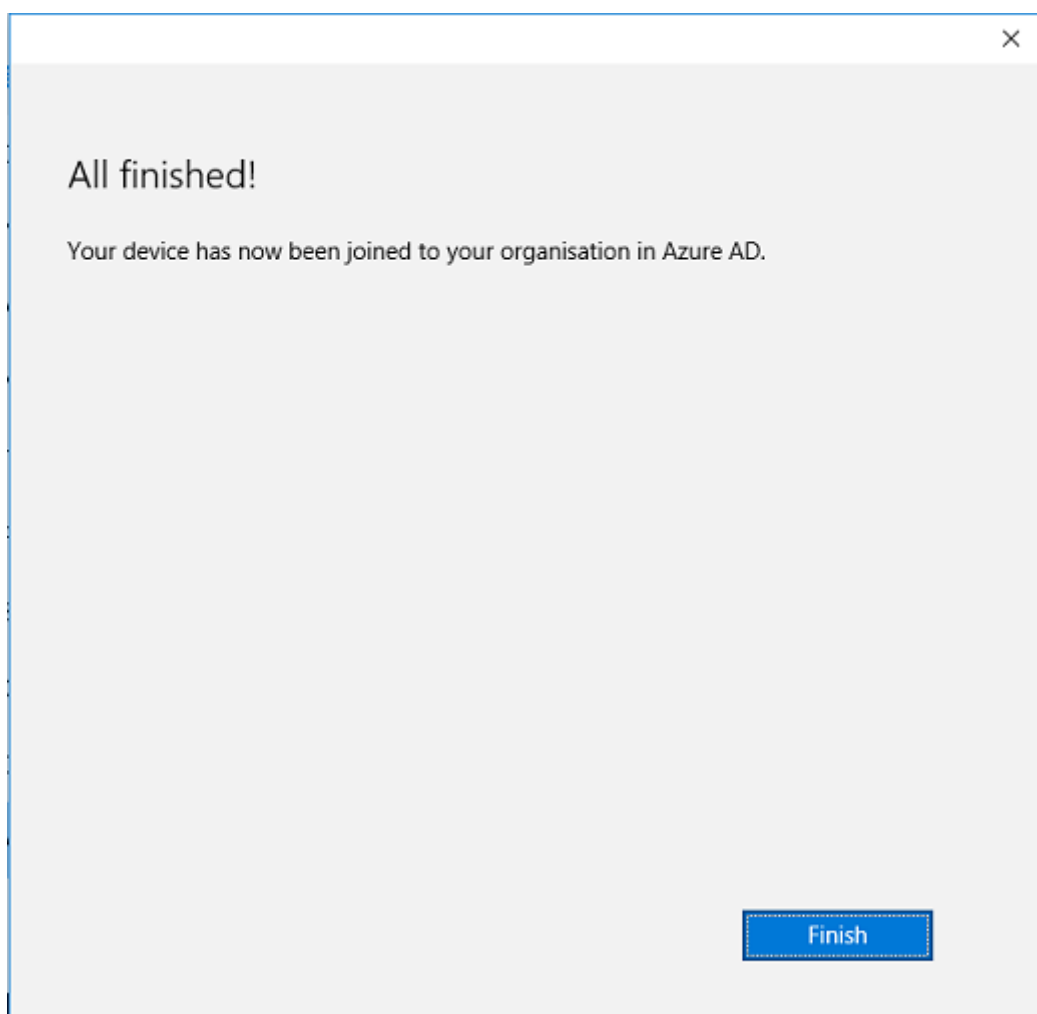
Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[Privacy statement](#)

Sign in Back

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



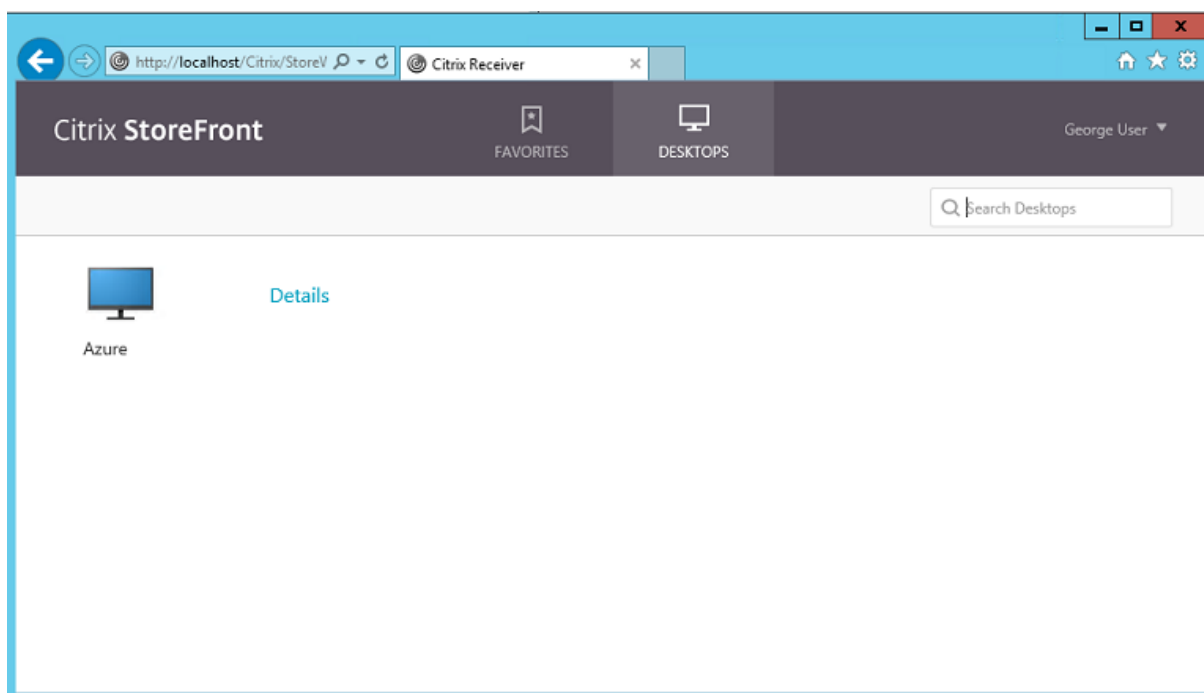


Vérifiez que la jonction Azure AD a réussi en redémarrant la machine et en ouvrant une session à l'aide de l'adresse e-mail de l'utilisateur. Une fois connecté, lancez Microsoft Edge et connectez-vous à <http://myapps.microsoft.com>. Le site Web doit utiliser l'authentification unique automatiquement.

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.



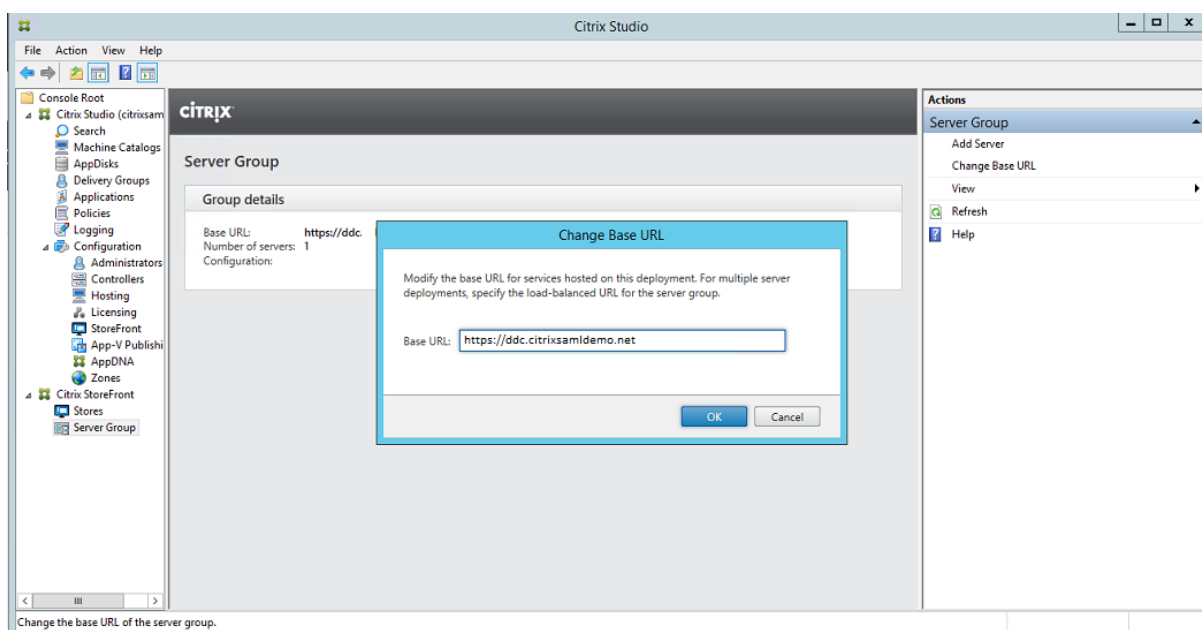
Exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** sur le Controller pour permettre à StoreFront de s'authentifier sans les informations d'identification de l'utilisateur.

Installer le Service d'authentification fédérée

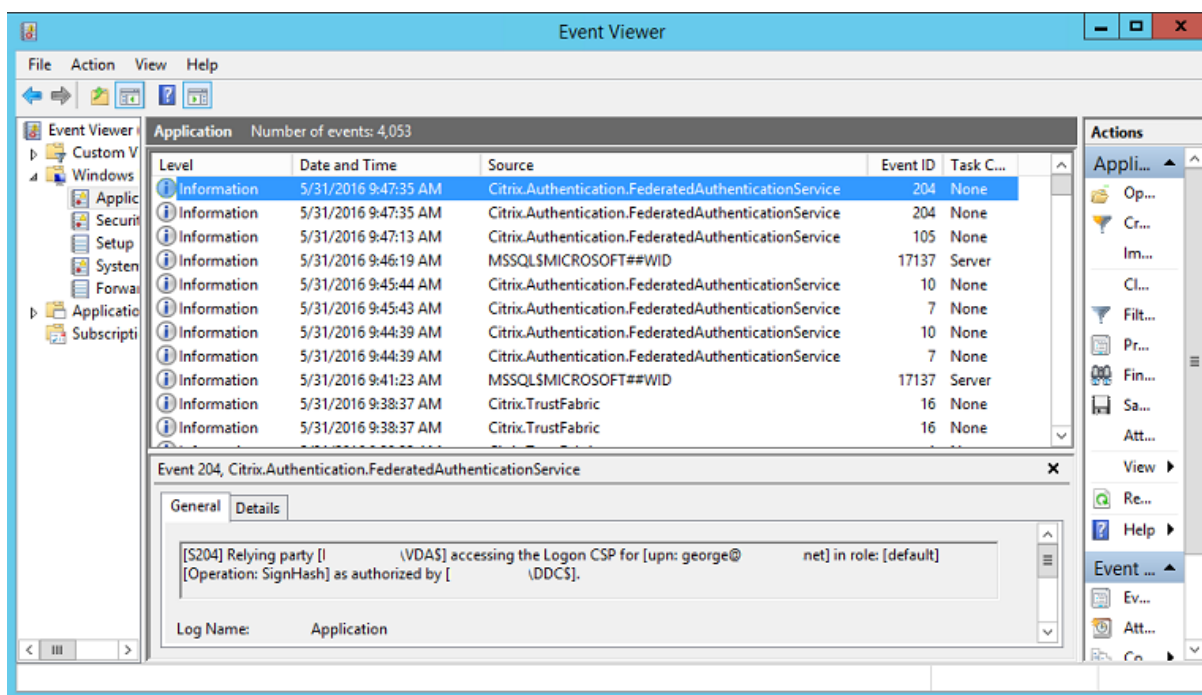
Installez FAS sur le serveur ADFS et configurez une règle pour faire en sorte que le Delivery Controller agisse en tant que StoreFront approuvé (dans cet exemple, StoreFront est installé sur la même VM que le Delivery Controller). Consultez la section [Installer et configurer](#).

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:.

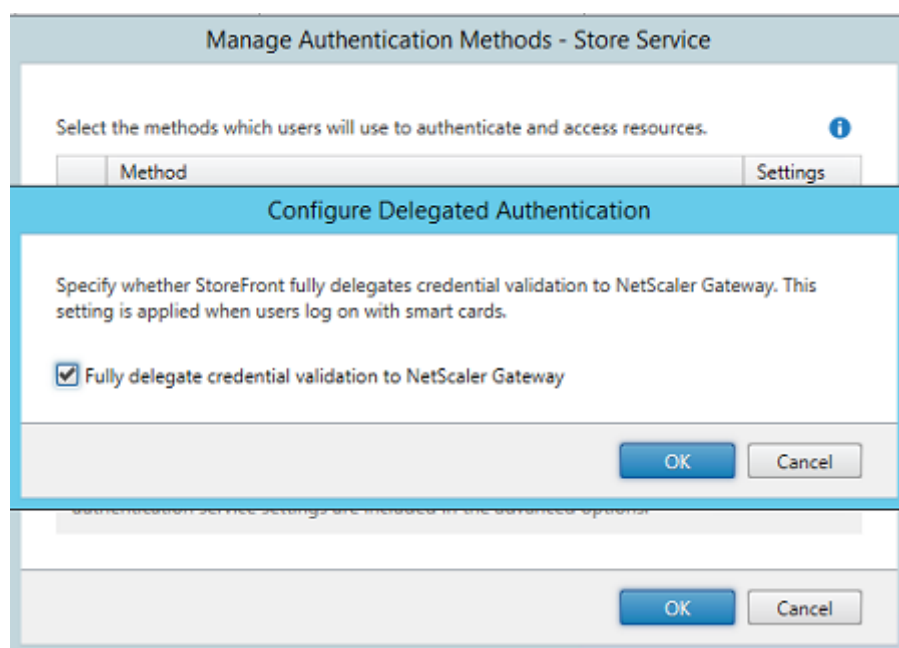


Configurez StoreFront pour utiliser le serveur FAS (utilisez le script PowerShell dans l'article [Installer et configurer](#)) et effectuez des tests en interne dans Azure, en vous assurant que l'ouverture de session utilise FAS en vérifiant l'observateur d'événements sur le serveur FAS.

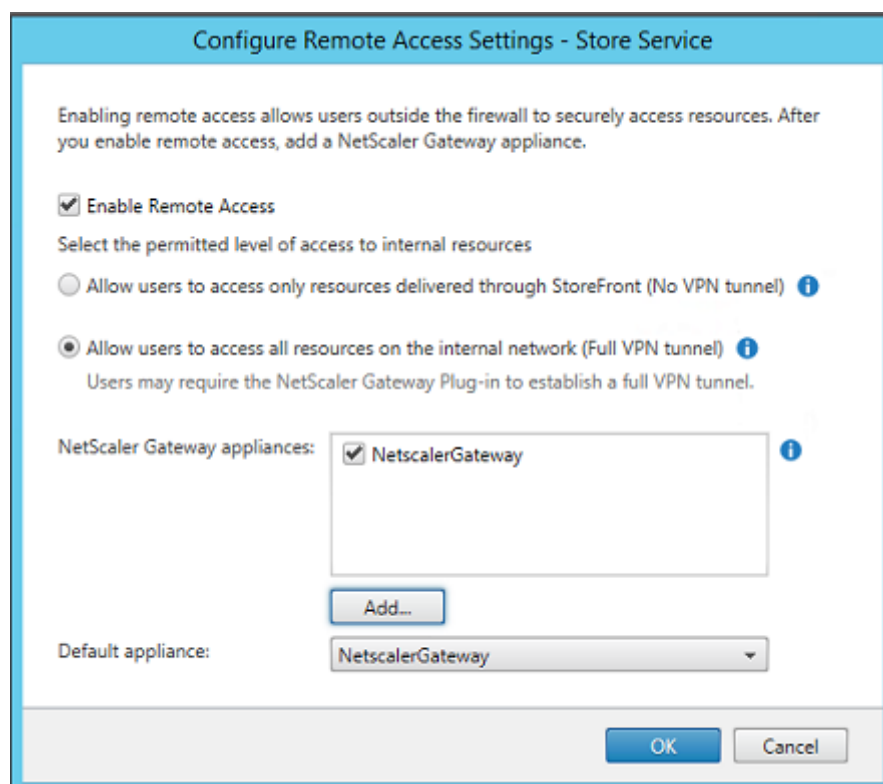


Configurer StoreFront pour utiliser Citrix Gateway

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.

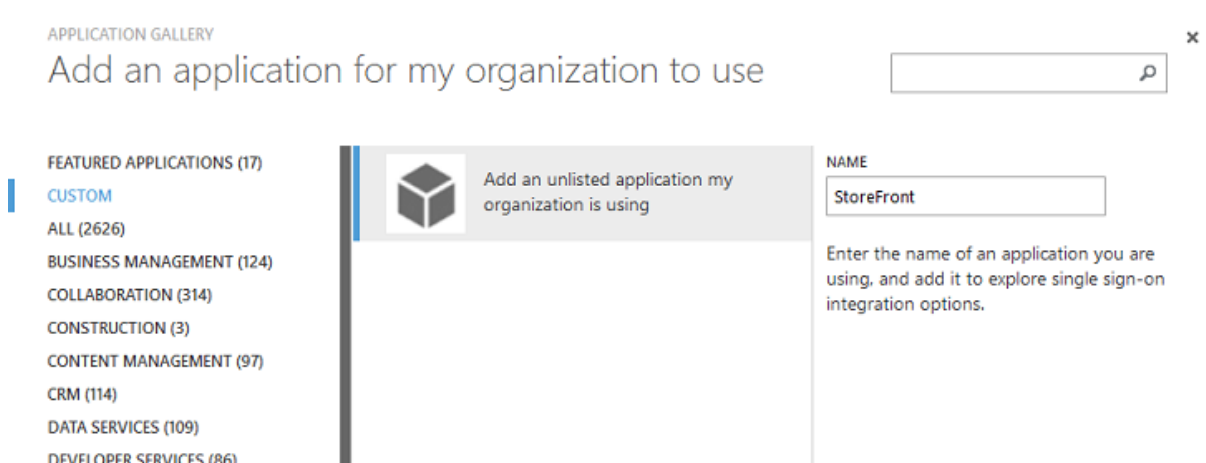


Pour intégrer les options d'authentification Citrix Gateway, configurez une STA (Secure Ticket Authority) et configurez l'adresse Citrix Gateway.



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.

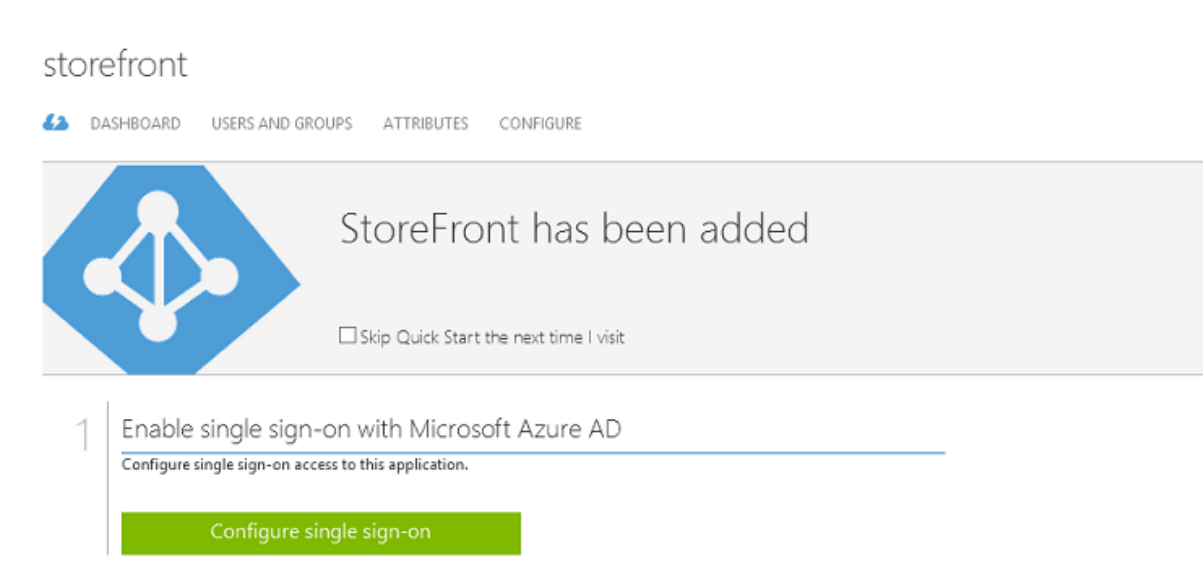
Configurer une icône

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

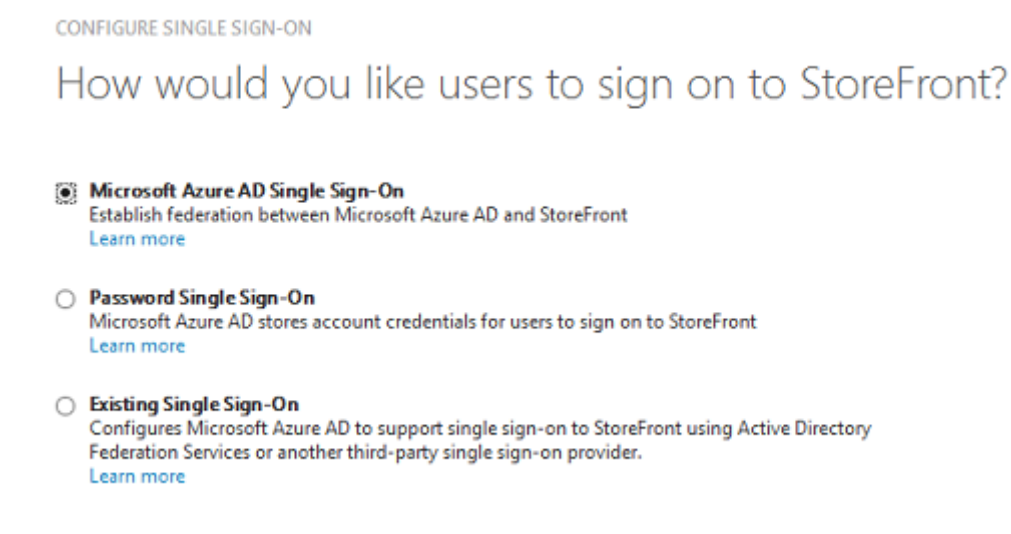


Configurer l'authentification SAML

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.

CONFIGURE SINGLE SIGN-ON

Configure App Settings

Enter the settings of AzureStoreFront application below. [Learn more](#)

IDENTIFIER 



REPLY URL 



☐ Show advanced settings (optional).

☐ Configure the certificate used for federated single sign-on (optional).

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

CONFIGURE SINGLE SIGN-ON

Configure single sign-on at AzureStoreFront

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

- The following certificate will be used for federated single sign-on:
Thumbprint: 8D1E02EBF7C111EDDBBD325F526053BA9626A73B
Expiry: 05/31/2018 11:06:20 UTC

[Download Certificate \(Base 64 - most common\)](#) 

[Download Certificate \(Raw\)](#) 

[Download Metadata \(XML\)](#) 

- Configure the certificate and values in AzureStoreFront

ISSUER URL

SINGLE SIGN-ON SERVICE URL

SINGLE SIGN-OUT SERVICE URL

☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.

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 GROUPE. 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>.

storefront

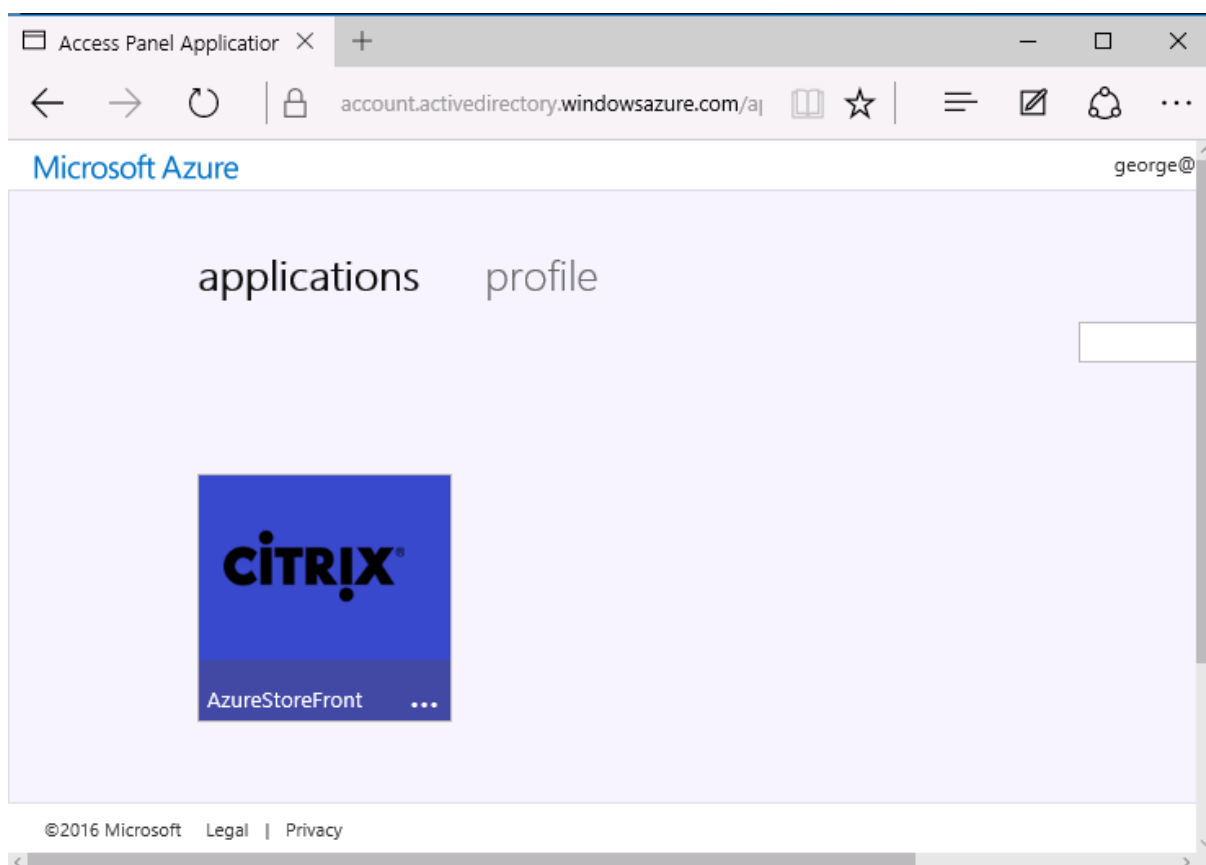
 DASHBOARD USERS AND GROUPS ATTRIBUTES CONFIGURE

SHOW 

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Azure Admin	AzureAdmin@citrixsaml..			No	Unassigned	
George User	george@citrixsaml..demo.net			No	Unassigned	
On-Premises Directory Sy...	Sync_ADFS_21a7e8060dcf...			No	Unassigned	

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.

quick glance

APPLICATION TYPE
Web application

PUBLISHER

URL

SINGLE SIGN-ON URL ?

➔ [View usage report](#)

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.



Bring Your Own License enabled.

Citrix NetScaler is an all-in-one web application delivery controller that makes applications run five times better, reduces web application ownership costs, optimizes the user experience, and makes sure that applications are always available by using advanced L4-7 load balancing and traffic management; proven application acceleration such as HTTP compression and caching; an integrated application firewall for application security; and server offloading to significantly reduce costs and consolidate servers. As an undisputed leader of service and application delivery, Citrix NetScaler solutions are deployed in thousands of networks around the globe to optimize, secure and control the delivery of all enterprise and cloud services. Deployed directly in front of web and database servers, NetScaler solutions combine high-speed load balancing and content switching, http compression, content caching, SSL acceleration, application flow visibility and a powerful application firewall into an integrated, easy-to-use platform. Meeting SLAs is greatly simplified with end-to-end monitoring that transforms network data into actionable business intelligence. Policies are defined and managed using a simple declarative policy engine, with no programming expertise required. BYOL is available for customers with NetScaler Gateway VPX or NetScaler VPX 10, VPX 200 and VPX 1000 licenses purchased via other channels from Citrix.

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)

PUBLISHER Citrix Systems

USEFUL LINKS [NetScaler VPX on Azure Guide](#)
[Deploying NetScaler VPX with XenApp and XenDesktop in Azure](#)

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*

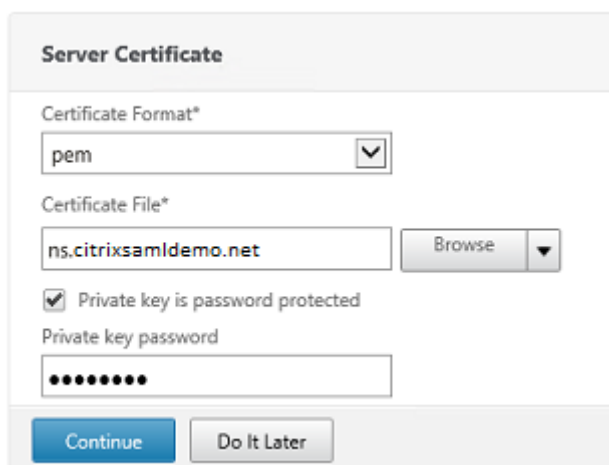
ns.citrixsamldemo.net

☐ 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 Browse

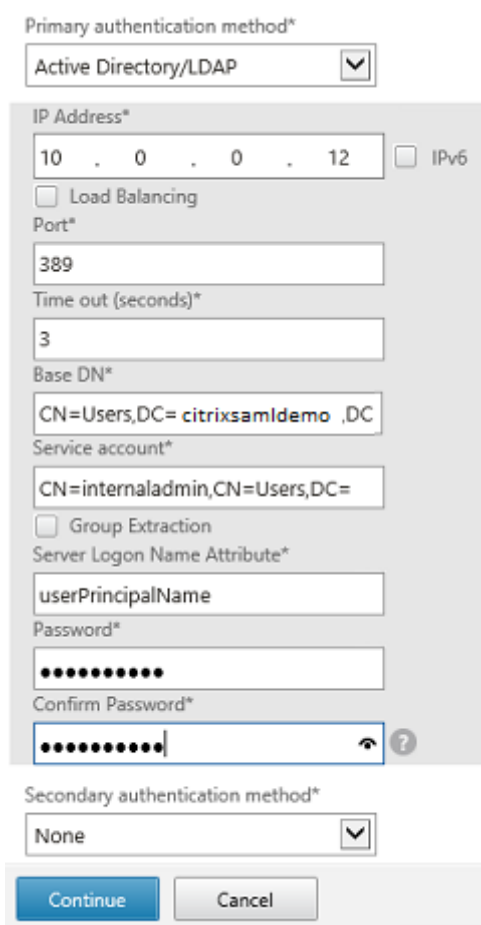
☒ Private key is password protected

Private key password
••••••••

Continue Do It Later

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*
••••••••

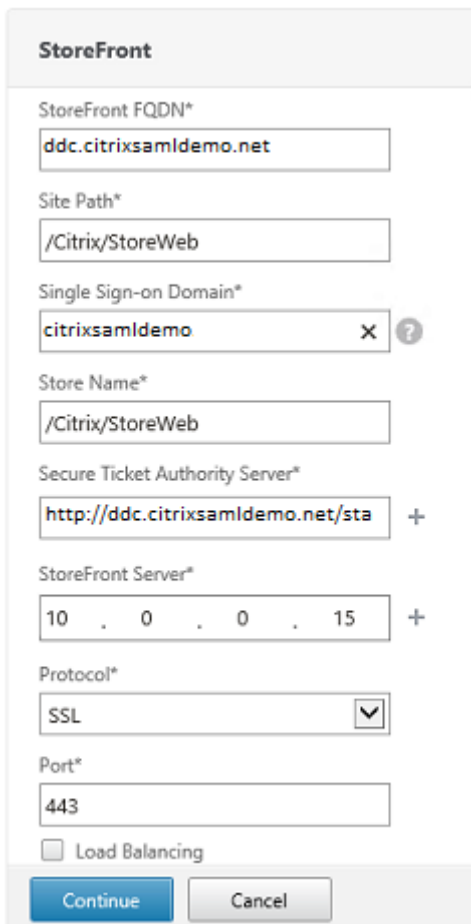
Confirm Password*
••••••••

Secondary authentication method*
None

Continue Cancel

Configurer l'adresse de StoreFront

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

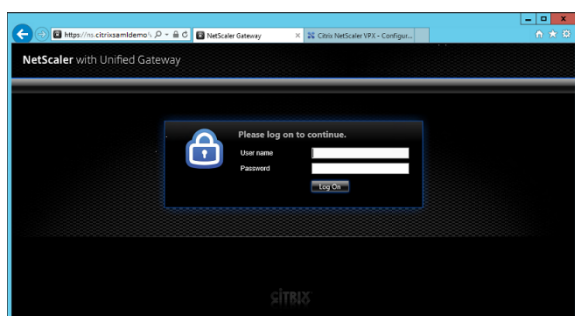


The screenshot shows the 'StoreFront' configuration window. It contains the following fields and controls:

- StoreFront FQDN***: Text box containing 'ddc.citrixsamldemo.net'.
- Site Path***: Text box containing '/Citrix/StoreWeb'.
- Single Sign-on Domain***: Text box containing 'citrixsamldemo' with a clear (X) and help (?) button.
- Store Name***: Text box containing '/Citrix/StoreWeb'.
- Secure Ticket Authority Server***: Text box containing 'http://ddc.citrixsamldemo.net/sta' with a plus (+) button.
- StoreFront Server***: Text box containing '10 . 0 . 0 . 15' with a plus (+) button.
- Protocol***: Dropdown menu set to 'SSL'.
- Port***: Text box containing '443'.
- Load Balancing**: An unchecked checkbox.
- Buttons**: 'Continue' and 'Cancel' buttons at the bottom.

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

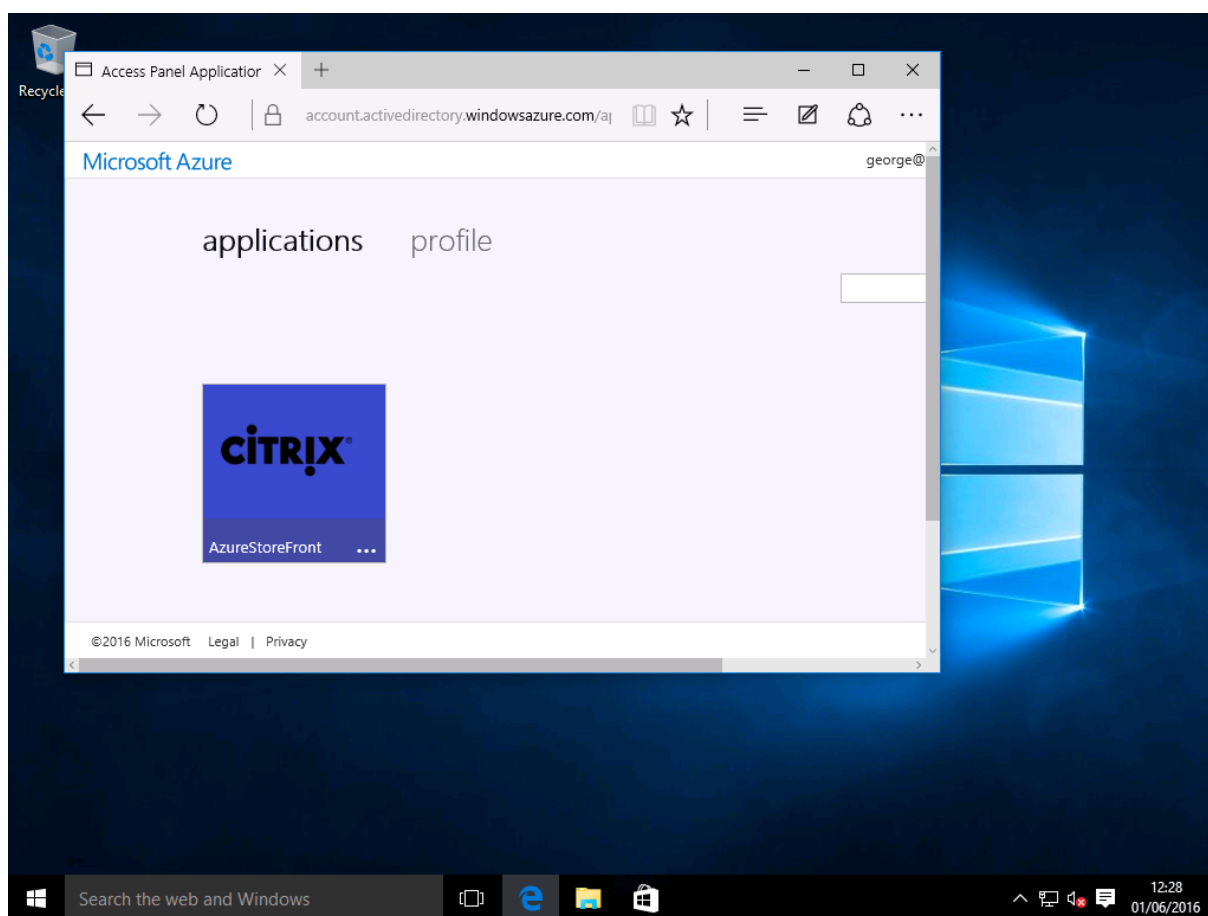
Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment depuis Azure AD.

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
	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.

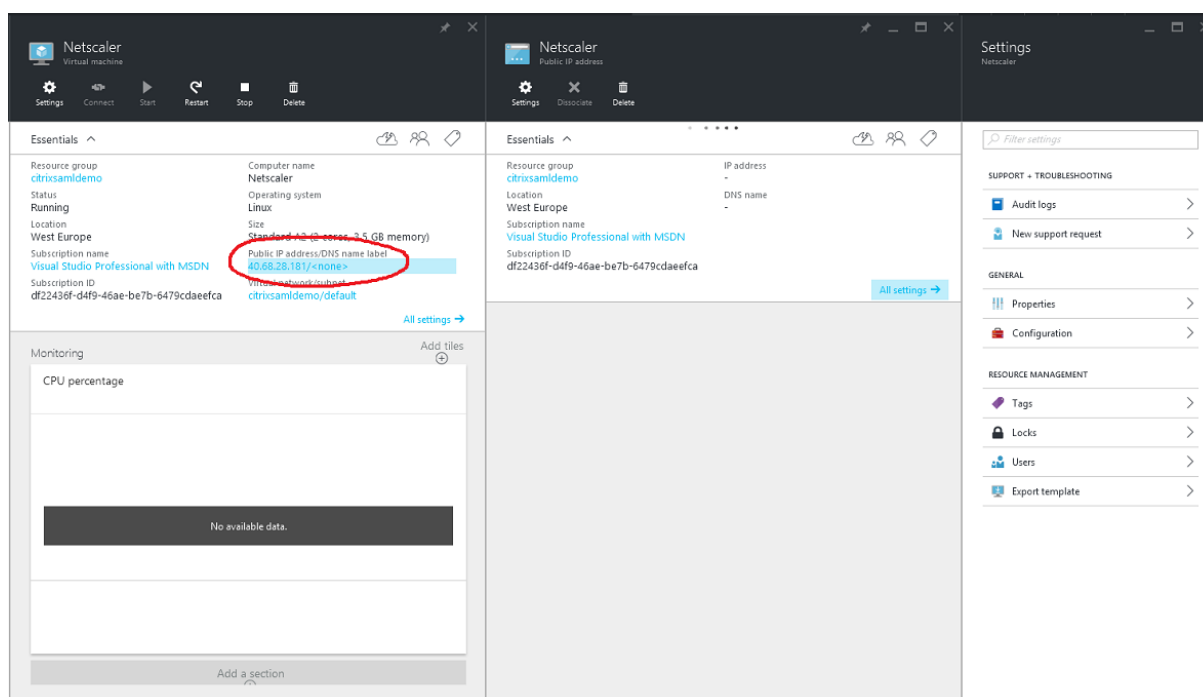
Enfin, vérifiez que les machines non jointes à Azure AD fonctionnent également avec les mêmes URL (bien qu'une authentification unique explicite à Azure AD sera utilisée pour la première connexion).

Annexe

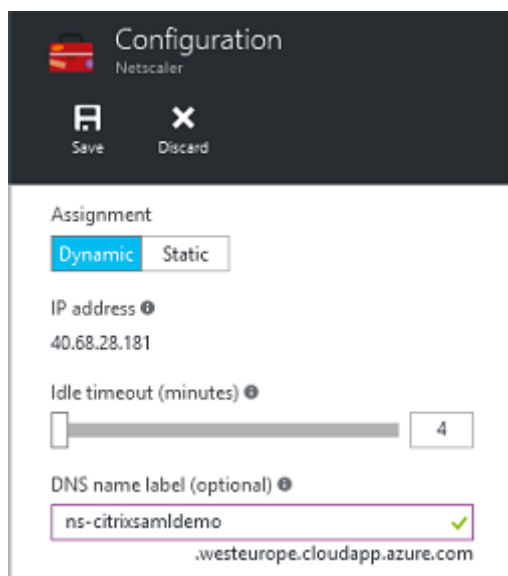
Vous devez configurer les options standard suivantes lorsque vous configurez une machine virtuelle dans Azure.

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.

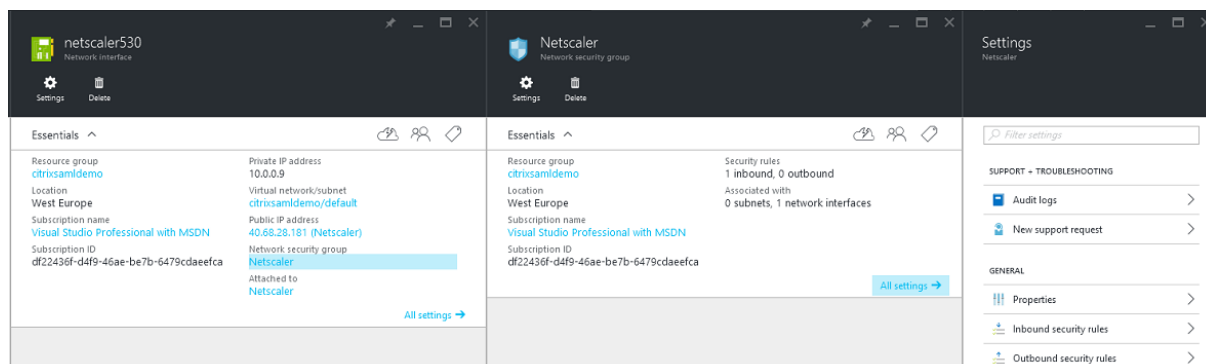


Configurer des règles de pare-feu (groupe de sécurité)

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 [Architectures de déploiement](#).
- Des informations pratiques sont disponibles dans l'article [Configuration avancée](#).

Configuration avancée

September 30, 2020

Les guides pratiques 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.

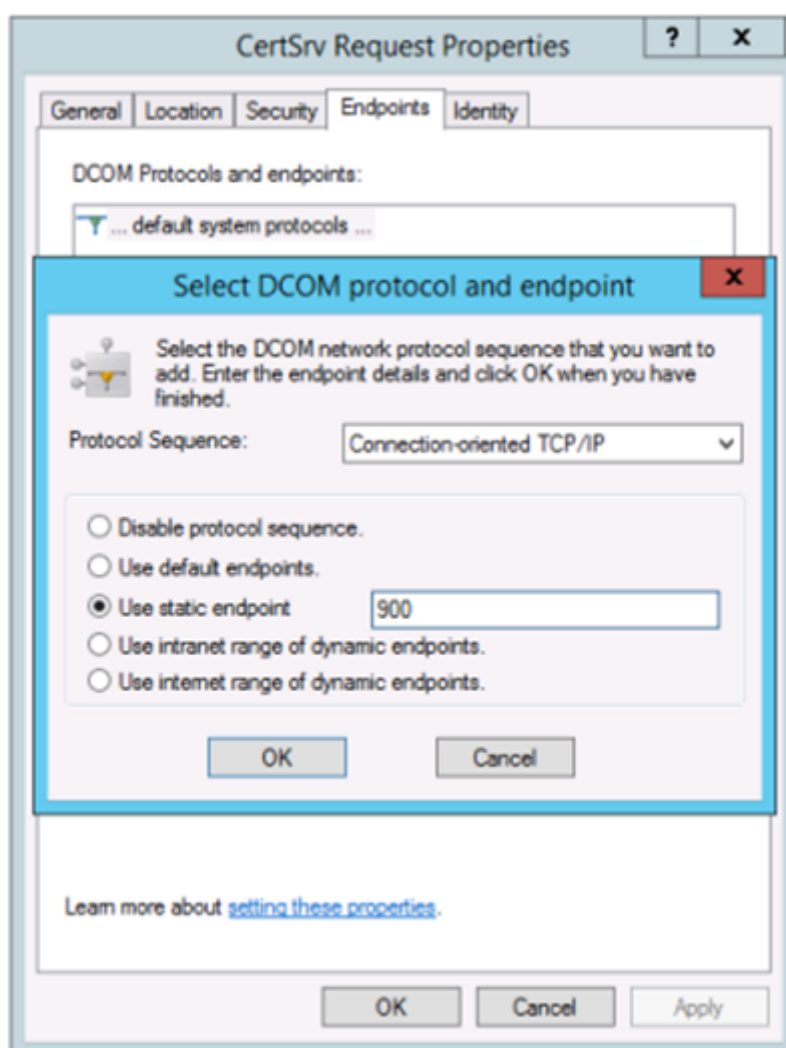
Configuration de l'autorité de certification

April 2, 2020

Cet article décrit la configuration avancée du Service d'authentification fédérée (FAS) pour l'intégration avec les serveurs d'autorité de certification qui ne sont pas pris en charge par la console de gestion 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.

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, ouvrez le panneau de configuration de DCOM et modifiez les propriétés de l'application « CertSrv DCOM » :



Modifiez les points de terminaison (endpoints) 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

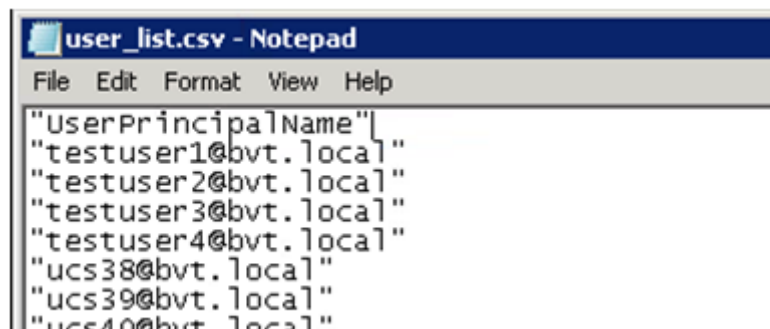
Vous pouvez améliorer la génération de certificat en interrogeant AD et en stockant la liste des utilisateurs dans un fichier (par exemple, un fichier .csv), comme illustré dans l'exemple suivant.

```
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 -NoTypeInfoation -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
        -NoTypeInfoation -Encoding utf8 -delimiter "," $filename
17 }
```

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 :



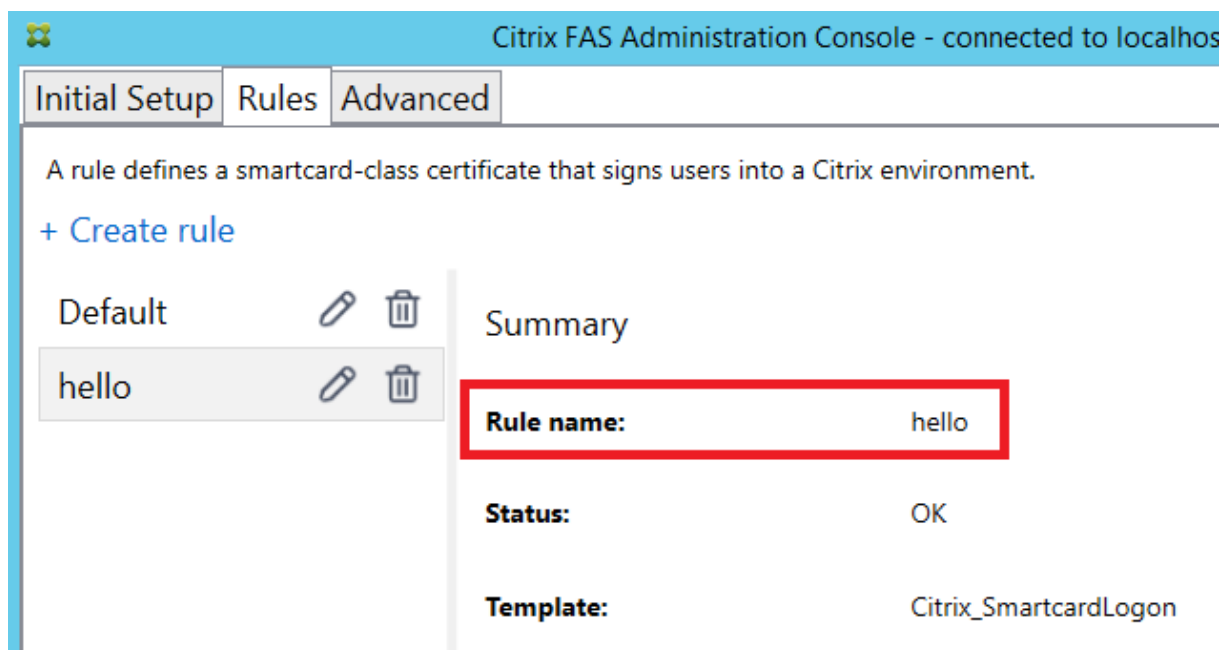
Serveur FAS

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 }
```

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.

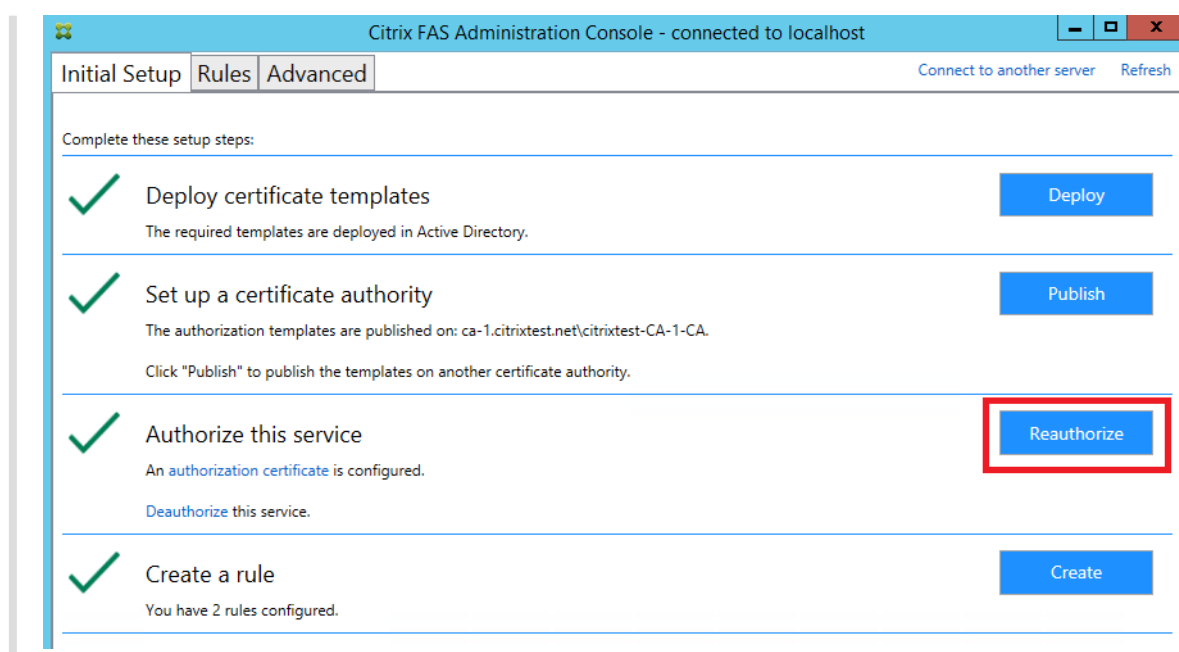


Renouveler les certificats d'autorité d'inscription

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 courants sont décrits dans l'article [Architectures de déploiement](#).
- D'autres articles « pratiques » sont disponibles dans l'article [Configuration avancée](#).

Protection de clé privée

September 30, 2020

Introduction

Les clés privées sont stockées par le biais du compte de service réseau 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>
</configuration>
<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)

Value	Commentaires
true	Utiliser les API CAPI
false (valeur par défaut)	Utiliser les API CNG

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

Value	Commentaires
Microsoft Enhanced RSA and Cryptographic Provider	Fournisseur CAPI par défaut
Fournisseur de stockage des clés de logiciel Microsoft	Fournisseur CNG par défaut
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)

Value	Commentaires
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

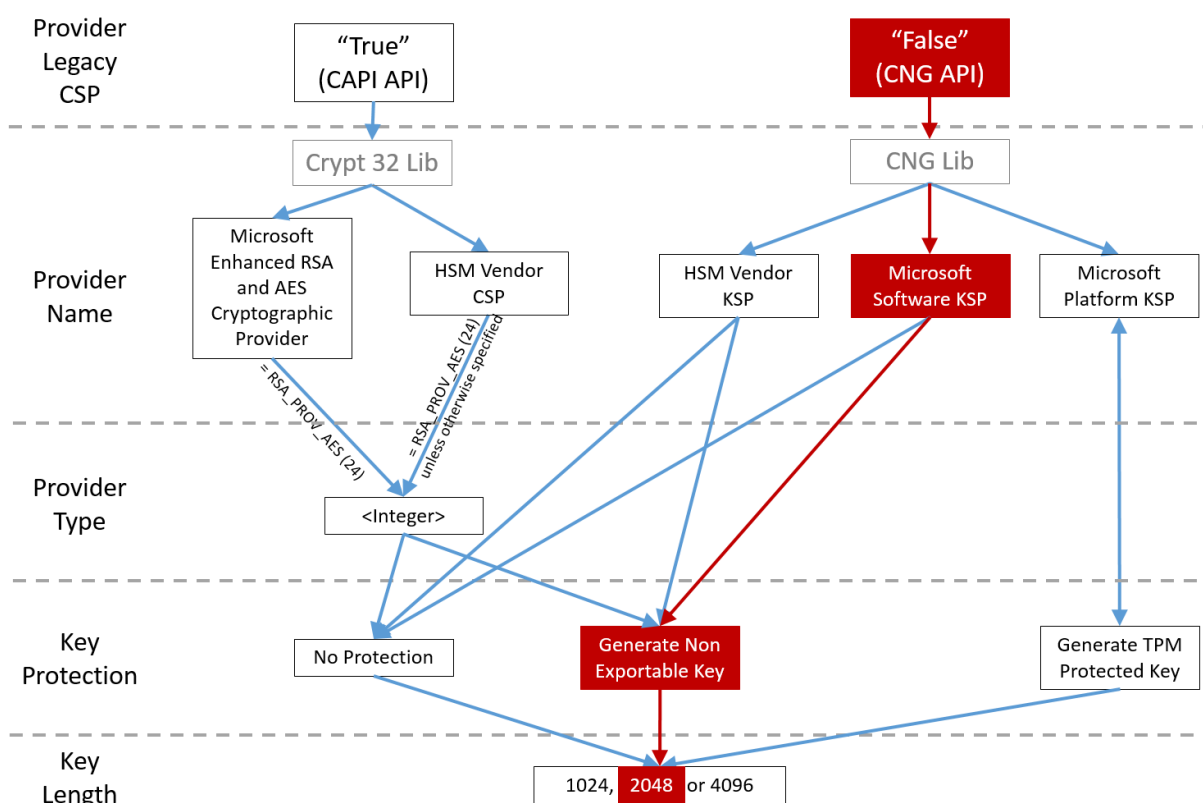
privées. Permet l'utilisation de stockage de clé TPM, s'il est pris en charge par le matériel.

Value	Commentaires
NoProtection	La clé privée peut être exportée.
GenerateNonExportableKey	Valeur par défaut. La clé privée ne peut pas être exportée.
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)

Value	Commentaires
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

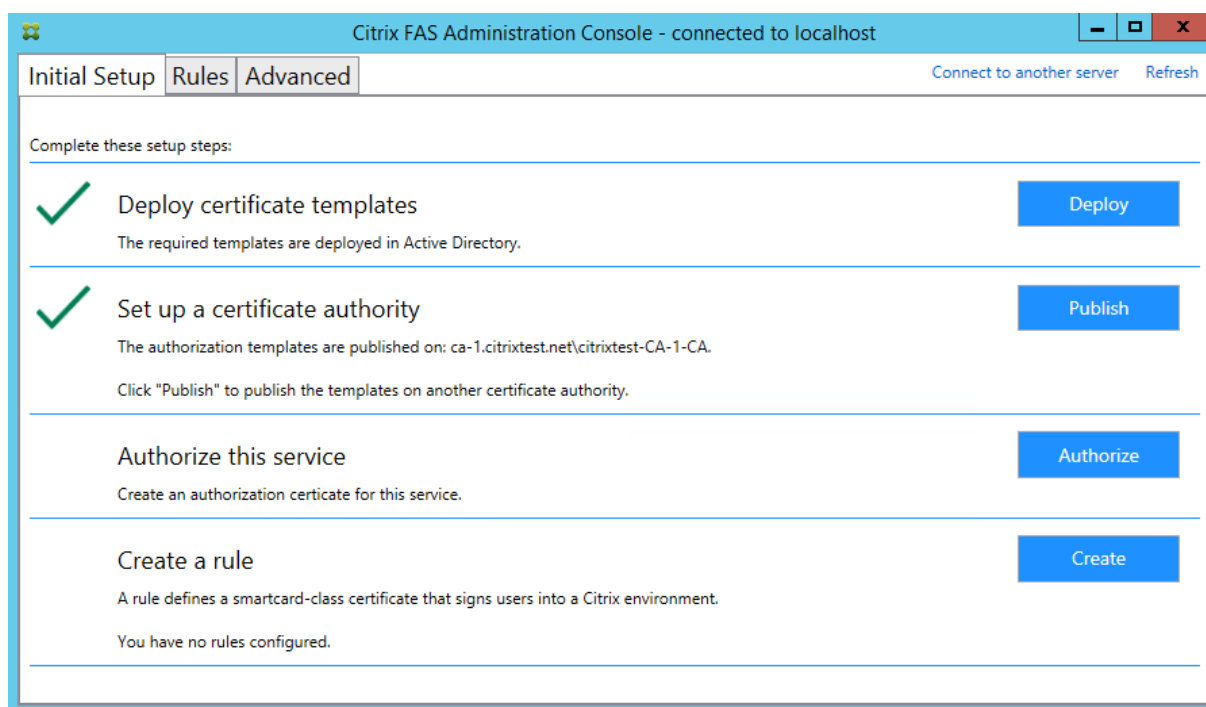
Cet exemple illustre la clé privée de certificat de l'autorité d'inscription stockée dans la puce TPM matérielle de la carte mère du serveur FAS via Microsoft Platform Key Storage Provider et les clés privées des certificats utilisateur stockées à l'aide de Microsoft Software Key Storage Provider.

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 PowerShell (recommandé)

Le certificat de l'autorité d'inscription peut être demandé hors connexion à l'aide de PowerShell. Cette option est recommandée pour les 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. Une demande de signature de certificat d'autorité d'inscription hors connexion ne peut pas être effectuée à l'aide de la console de gestion 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 l'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_ManualAuthorization** 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 :

```
1 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. Veillez à spécifier une longueur de clé prise en charge par votre matériel.

```
1 New-FasAuthorizationCertificateRequest -UseTPM $true -address \<nom de
  domaine complet du serveur FAS>
```

Par exemple :

```
1 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-----
MIICADCCAVACAQIwIzEhMB8GCgmSjomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
hkIG9wDBAQEFAA0CAQ8AMIIBCAQEAAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZU3wTnFR0XW
1hCMwi7X4YpTE7CbJtgY/9SEBa9StGeTVpeJi66gkoZCdxyc2BwX6JNZrLi9hAf1bInFPgrz+
vbG3YjKuKtK35JpGqYwJUEDzKiQFaob3Dkh/pwP3U70cEYthxB8CfbaN9MH0EFbepoSY0CAfunXW
snwIbX091c/fGyN/3f94P4fbNrjEIOHc+40y/WsPgPRgcq9XBwRjzpGj0g0WRoJS9g220Y5PwD77
7f7vZvo0kRy5MXXATJ+xxYEPLp9JuJaE1WZrTJG+XP3Sn6/oCCPit7iUIIc9Fj6a3gTUQIDAQAQ
oAAwDQYJKoZIhvcNAQENBQADggEBAIJU8jR9XVHlvztjpxPeJzAV0srLp0ScfNdvYn9u+I7J8Gsr
4tuljuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUzoAf6eLg1Vht2RUVfb6d7Ns6+Mc+F5bFegLHs8c
Y1ITN0tmcHFkt4Loz50SE+tQw39MPProEj3p7GwF7Hr6Y+QsbfD38rbL19Z5cfHYVqMbsgyMgdR8F
3SmagQjN3C8lyqT8z1iF4132xlmQrP/4XQvr1F+T015PM5Fzjj6PEKWopWTYZXGzSC1ufxevcD1K
+tTH9tQYJM6xw3+6TicfuWQjrd8KJjTdC5SMu7LJuIajTNZ5Z+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 configuration.
- 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]

Notez : “[TPM : True]”

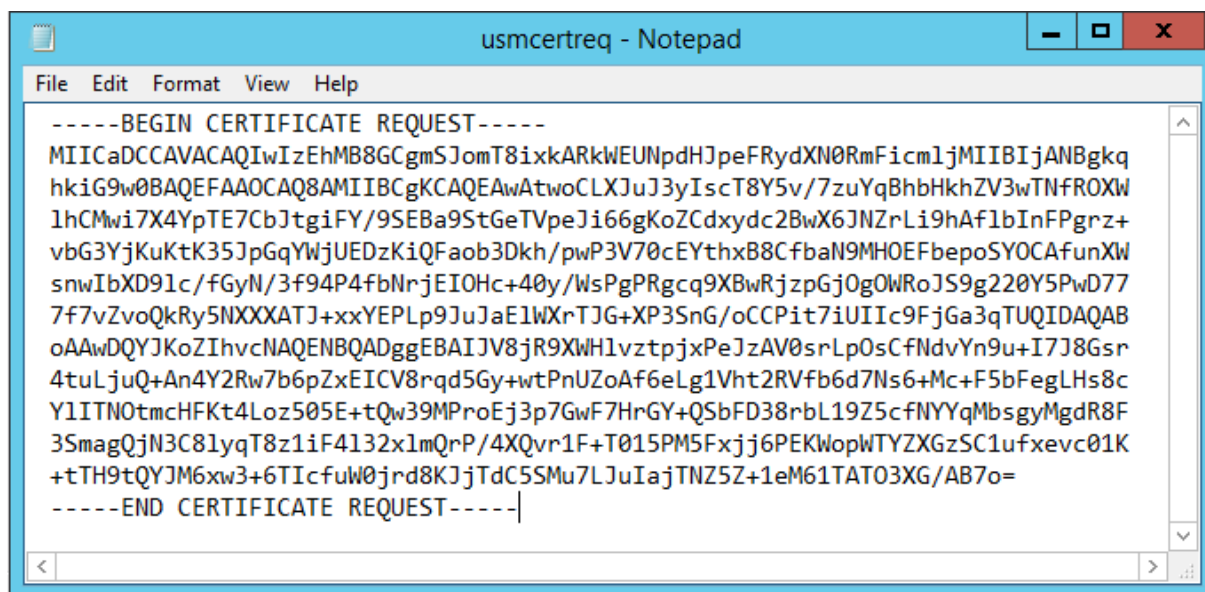
Suivi de :

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]					

Notez : “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.



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 :

```
1 certreq -submit -attrib "certificatetemplate:<modèle de certificat de l'étape 2>" \<fichier de demande de certificat de l'étape 6>
```

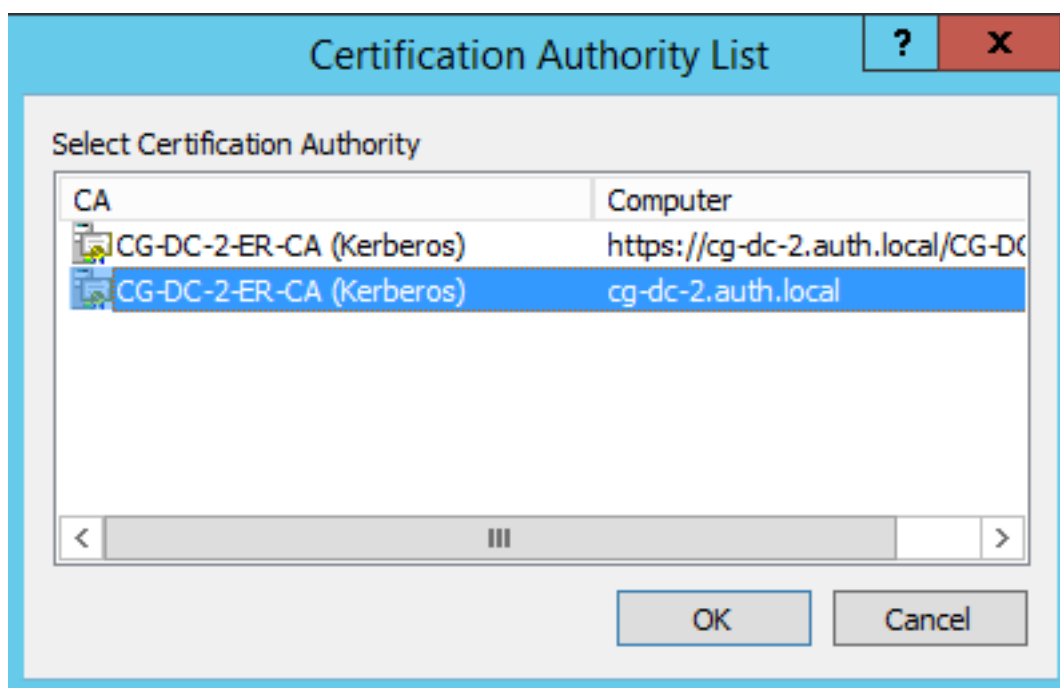
Par exemple :

```
1 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-0B0C-4D21-A4FD-2E29502177C2}
ldap:
```

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 :

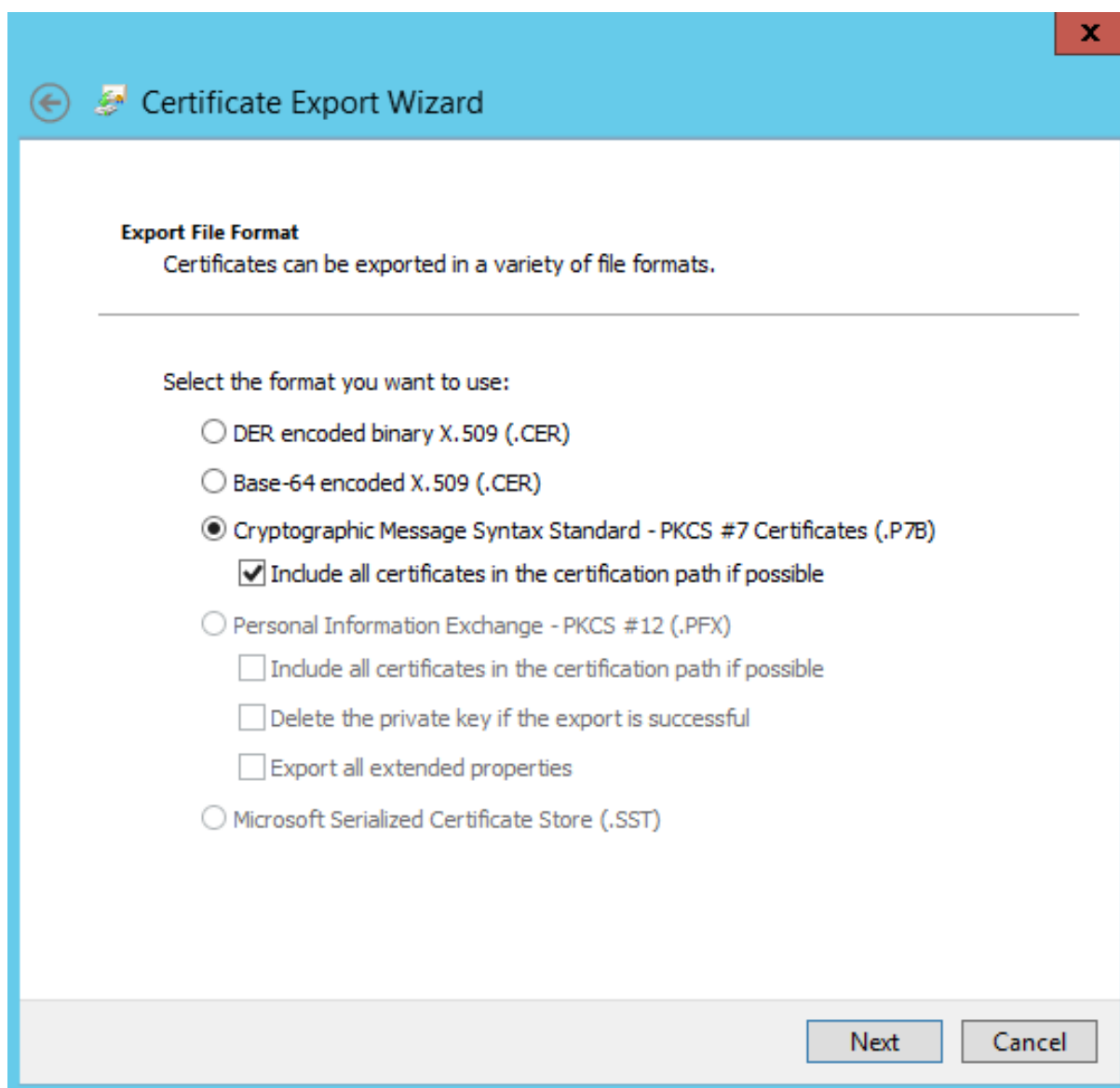


Après que l'autorité de certification a été spécifiée, PowerShell affiche la RequestID :

```
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 :

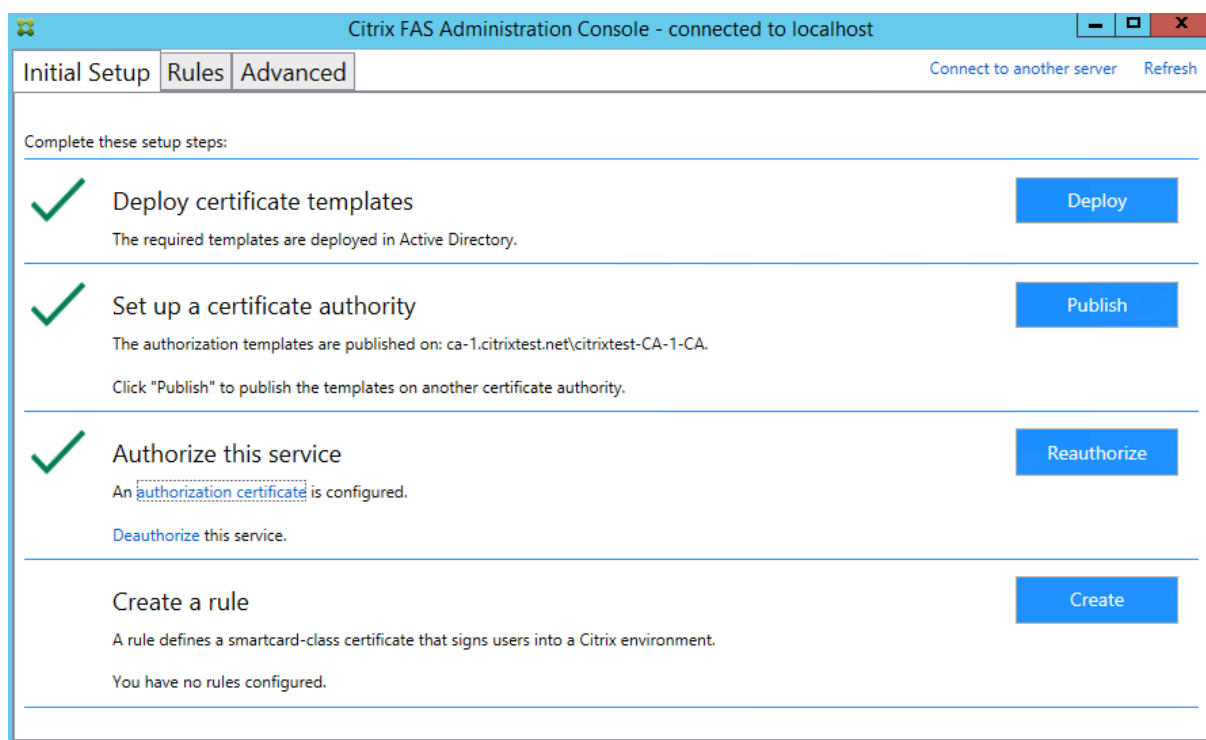
```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

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
```

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](#).

Utilisation de la console de gestion FAS

La console de gestion 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>
</configuration>
<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 : autorisez le service.

Étape 3 : 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 de gestion 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.

Étape 4 : 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 5 : 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.

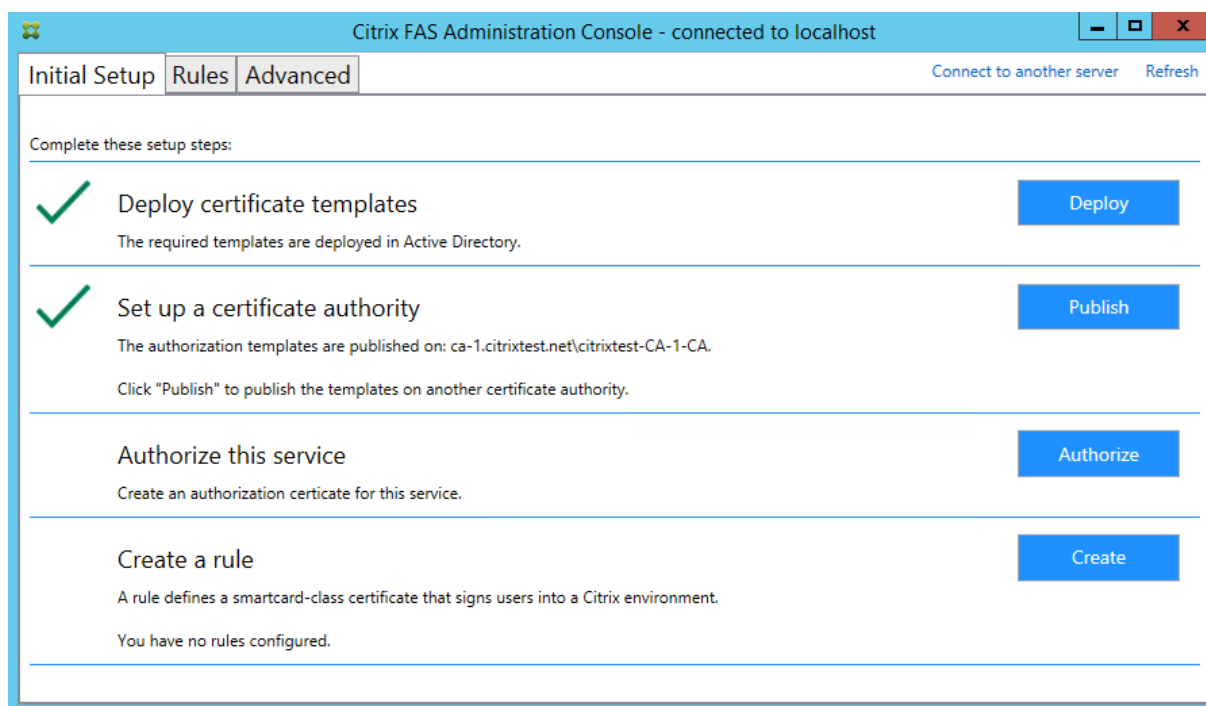
Étape 6 : sélectionnez l'onglet **Rules** dans la console de gestion FAS et modifiez les paramètres décrits dans [Installer et configurer](#).

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 l'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"/></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 [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWAIN][MachineWide: False][Provider: [CNG]
HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

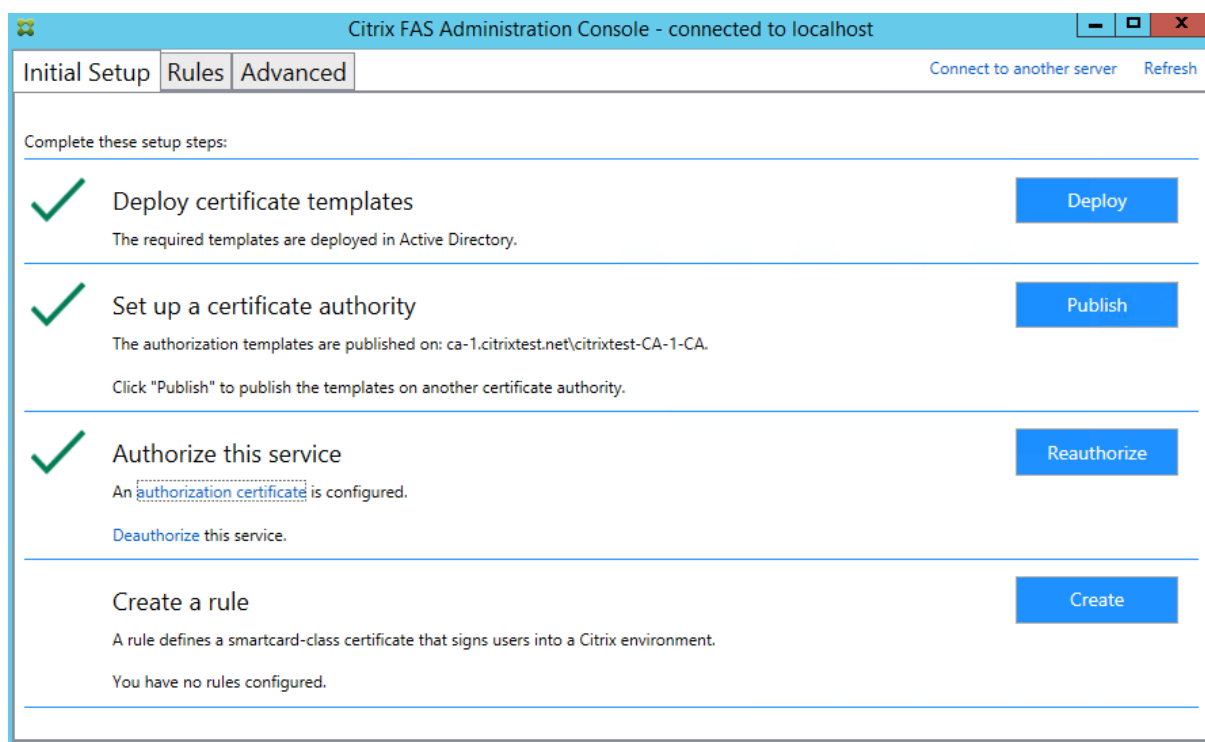
Notez : [Fournisseur : [CNG] HSM_Vendor's Key Storage Provider]

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\UCSHSM\$	

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 :

```
1 Add-psnapin Citrix.a\*
2 Get-FasAuthorizationCertificate - address \<nom de domaine complet du
  serveur FAS>
```

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/xOVM6cNKsLbew3dY1bo+vdgwG86DFRVxTORho11V86iazDZy0iYGgxe9/s8YZzCspVWN1nB1
zX0UJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
ECz/CbXR00uiDhw+VWbjcsgk1cavzvC/jR33F9dZSXNgKRiGHgfd/1Bb3e1ZKA400oi90u64Q916
3ba98nihqxIgvwWIL0myUfiJmCgbhLJV4TPBop0dKz/axZEIO5p5XYVjCcpXqhL7Ppn1wIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKggcJNJO/MU7/7X
bZB46drLPFzpzF88DkmFoCEg0x1bzFX9waaiFs9CHC/AcEzb1N925y1gq1jsfC315TCKBAeLFoM1
PSEkfYMQU05BYCuL1kFn1LXLSeQ3qJTz5vptYR0awFmUMQLffwLSR1v0u58DJ5rpASrwdXJk3TOa
G10/xJo/NRM0wMH+AvGbBsgp3l+jnDjXED5RudqARfGvGcW714JP+XIeFrE1TZmUL2skNIXEPNHC
H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZ00aiER+z8=
-----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval
```

Pour obtenir une liste de certificats utilisateur, entrez :

```
1 Get-FasUserCertificate - address \

```

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 :

```
1 Get-FasUserCertificate - address \

```

Par exemple :

```
1 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 des Services d'authentification fédérée](#).
- D'autres articles « pratiques » sont disponibles dans l'article [Configuration avancée](#).

Configuration du réseau et de la sécurité

April 2, 2020

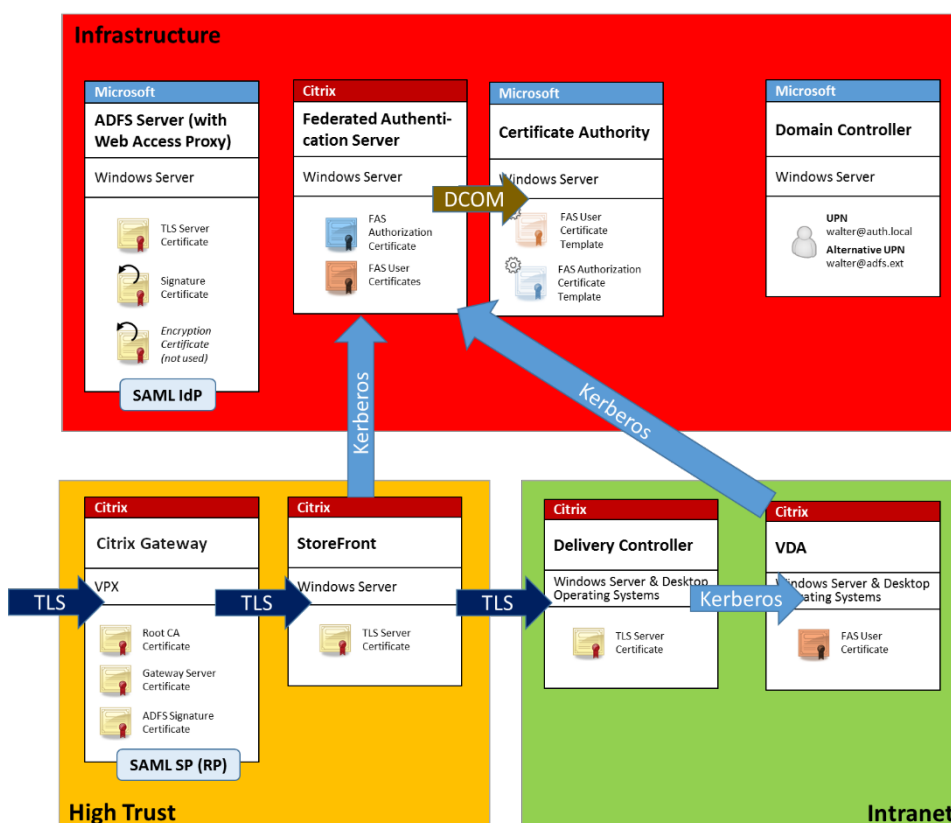
Le Service d'authentification fédérée (FAS) est étroitement intégré à Microsoft Active Directory et à l'autorité de certification Microsoft. Il est essentiel de vous assurer que le système est géré et sécurisé de manière appropriée, en développant une stratégie de sécurité comme vous le feriez pour un 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 doit être considéré comme faisant 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 approuvés pour authentifier les utilisateurs ; les autres composants de Citrix Virtual Apps and Desktops ne sont pas affectés par l'introduction de FAS.



Sécurité du réseau et pare-feu

Les communications entre les composants Citrix Gateway, StoreFront et Delivery Controller doivent être protégées par TLS sur le port 443. Le serveur StoreFront se charge uniquement des connexions sortantes, et Citrix Gateway doit uniquement accepter 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. Ceci 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. En outre, 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 également 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	[dans] Kerberos via HTTP depuis StoreFront et VDA, [sortant] DCOM vers autorité de certification Microsoft
Citrix Gateway	[dans] HTTPS depuis les machines clientes, [entrant/sortant] HTTPS depuis/vers un serveur StoreFront, [sortant] HDX vers VDA
StoreFront	[dans] HTTPS depuis Citrix Gateway, [sortant] HTTPS vers Delivery Controller, [sortant] HTTP Kerberos vers FAS
Delivery Controller	[dans] HTTPS depuis un serveur StoreFront, [entrant/sortant] Kerberos sur HTTP à partir de VDA
VDA	[entrant/sortant] Kerberos via HTTP depuis Delivery Controller, [dans] HDX depuis Citrix Gateway, [sortant] Kerberos HTTP vers FAS
Autorité de certification Microsoft	[dans] DCOM et signé depuis FAS

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.

Pour éviter toute erreur de configuration, Citrix recommande d'appliquer une seule stratégie à toutes les machines dans l'environnement. 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

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.

Reportez-vous à la section [Protection de clé privée](#) pour connaître les paramètres équivalents que FAS fournit.

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

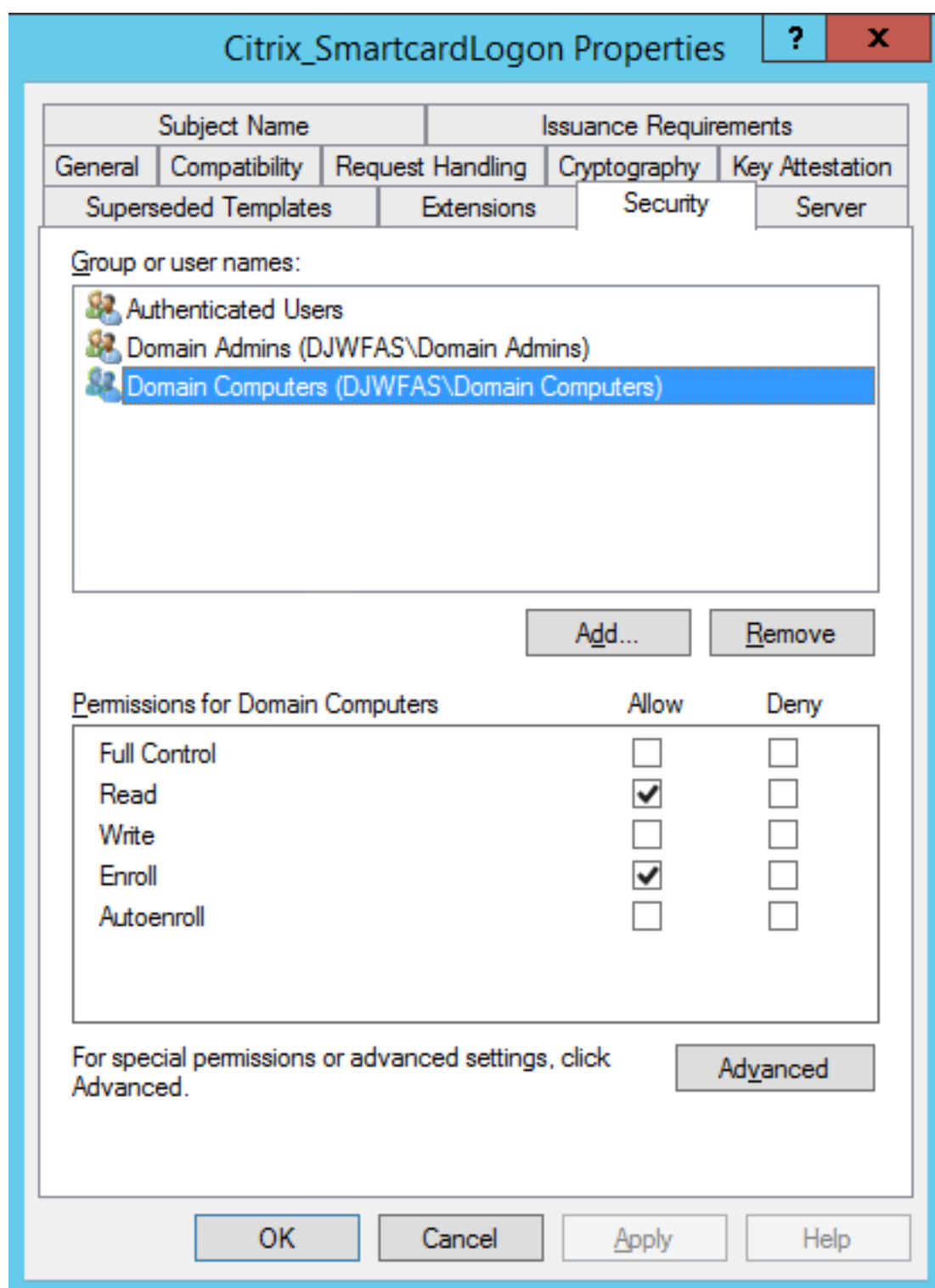
Vous pouvez modifier ces paramètres en fonction de la stratégie de votre organisation.

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 d'ordinateur des serveurs FAS uniquement. Aucune autre autorisation n'est requise par le service FAS. 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

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

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 comme indiqué :

The screenshot shows the 'Citrix_SmartcardLogin Properties' dialog box with the 'Issuance Requirements' tab selected. The 'General' tab is also visible. The 'Issuance Requirements' section includes the following settings:

- Subject Name:** Issuance Requirements
- Require the following for enrollment:**
 - ☐ CA certificate manager approval
 - ☒ This number of authorized signatures: 1
- If you require more than one signature, autoenrollment is not allowed.**
- Policy type required in signature:** Application policy (dropdown)
- Application policy:** Certificate Request Agent (dropdown)
- Issuance policies:** (empty list box with 'Add...' and 'Remove' buttons)
- Require the following for reenrollment:**
 - ☒ Same criteria as for enrollment
 - ☐ Valid existing certificate
 - ☐ Allow key based renewal (*)
- Requires subject information to be provided within the certificate request.**
- * Control is disabled due to [compatibility settings](#).**

At the bottom of the dialog are buttons for OK, Cancel, Apply, and Help.

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.

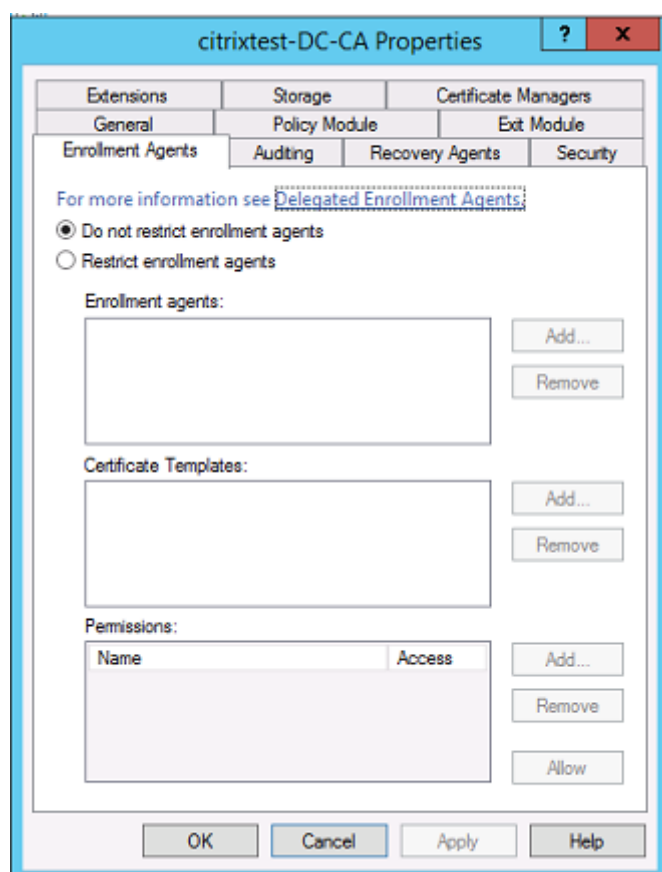
Une simple pratique de sécurité consiste à publier uniquement les modèles de certificat d'autorité d'inscription lorsque les serveurs FAS sont installés, ou d'opter pour un processus d'émission hors connexion. Dans les deux cas, l'administrateur d'autorité de certification doit conserver un contrôle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

En général, l'administrateur de l'autorité de certification contrôlera également les paramètres de pare-feu réseau de l'autorité de certification, ce qui 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 quelconque modèle de certificat autorisant l'accès. Ceci devrait être restreint à un groupe d'utilisateurs non privilégiés 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	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. En particulier, 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 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, ceci peut être utilisé pour mettre uniquement à disposition des 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 protéger au moins une clé privée de certificat d'autorité d'inscription en la stockant dans un TPM ; cette option est fournie dans le cadre du processus de demande de certificat « hors connexion ».

De même, les clés privées de certificat utilisateur peuvent être stockées dans un module TPM ou HSM. Toutes les clés doivent être générées en tant que « 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. Cette liste doit être soigneusement tenue à jour.

Administrateurs Citrix Virtual Apps, Citrix Virtual Desktops et VDA

En général, 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. L'audit et les journaux d'événements doivent être tenus à jour.

Sécurité des serveurs Windows

Tous les correctifs doivent avoir été installés sur tous les serveurs, de même que des pare-feu et des logiciels antivirus. Les serveurs d'infrastructure critiques à la sécurité doivent être conservés dans un endroit sécurisé, et un soin tout particulier doit être apporté au cryptage du disque et aux options 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. Dans la mesure du possible, les comptes utilisateur doivent demander une ouverture de session par carte à puce, plus particulièrement 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 articles « pratiques » sont disponibles dans l'article [Configuration avancée](#).

Résoudre les problèmes d'ouverture de session Windows

September 30, 2020

Cet article décrit les journaux et les messages d'erreur Windows lorsqu'un utilisateur ouvre une session à l'aide de certificats et/ou de cartes à puce. 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 afficher ces certificats, depuis 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 NTAUTH.

- **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 peut être 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 (généralement 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. Veuillez noter qu'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 généralement 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. Notez que cette configuration doit être rétablie lors d'un débogage.

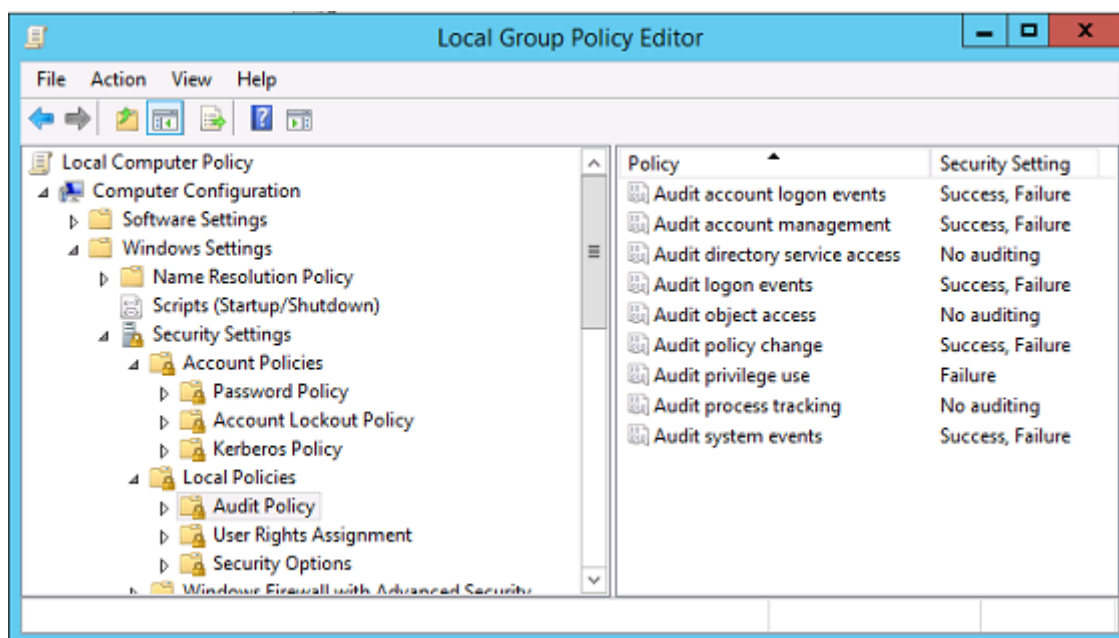
Identifier le contrôleur de domaine utilisé

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. Une fois qu'ils sont activés, le contrôleur de domaine génère des informations supplémentaires dans le journal d'événements 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.

Vous pouvez contrôler la journalisation CAPI avec les clés de registre dans : `CurrentControlSet\Services\crypt32`.

Value	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. Voir 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\	LogLevel	0x1
CurrentControlSet\Control\Lsa\	Krb5DesCiphers	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

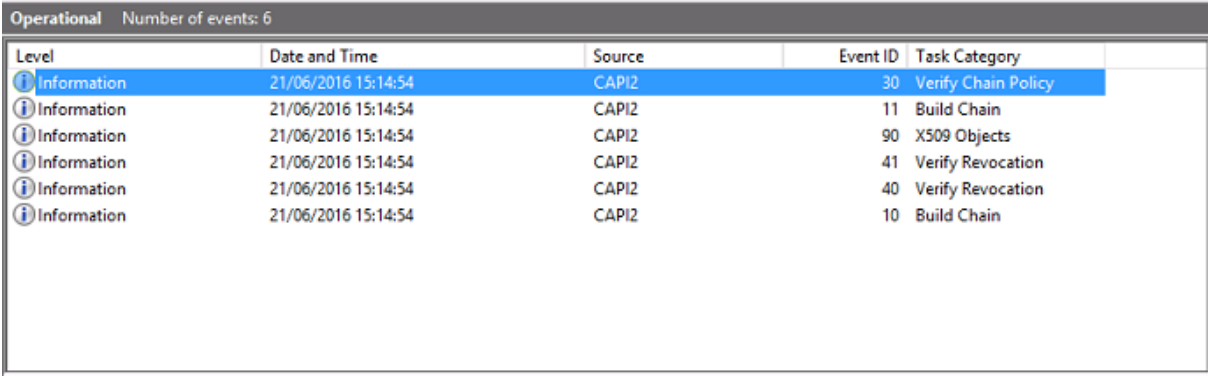
Messages des journaux d'événements

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.



Operational Number of events: 6				
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

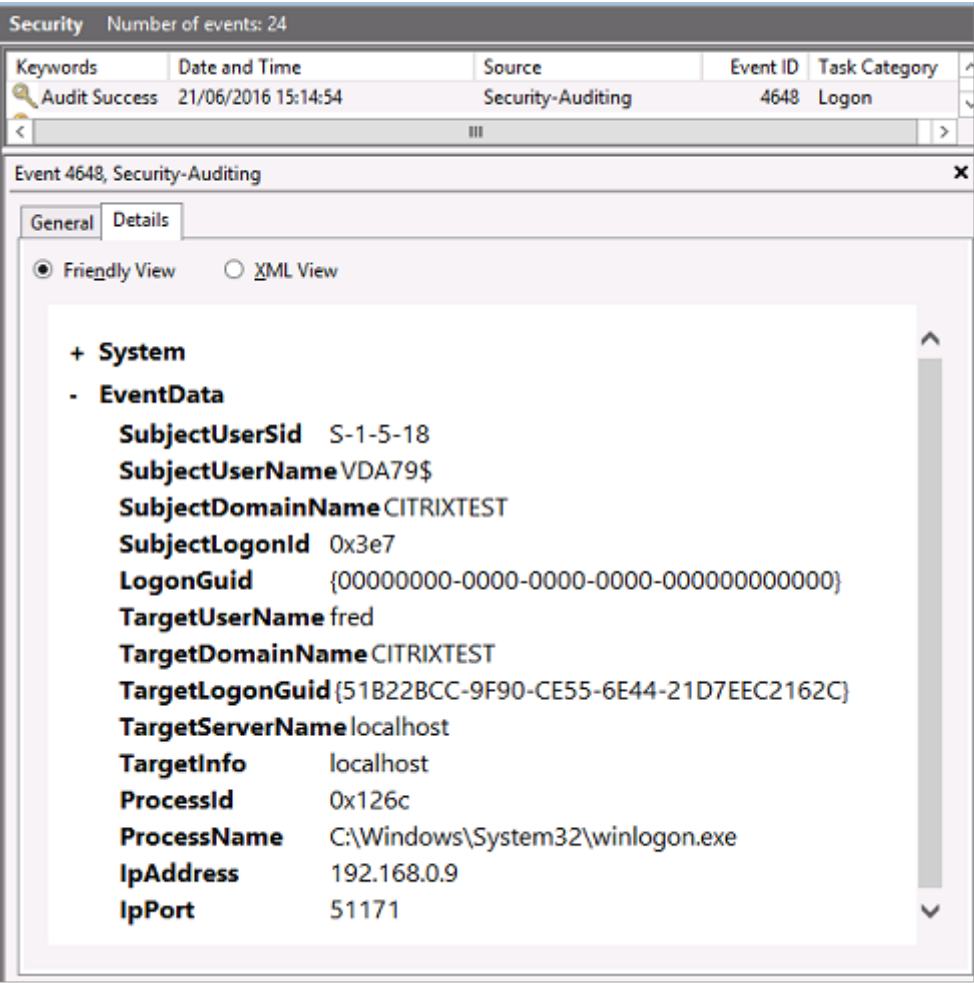
☒ Friendly View ☐ XML View

```

+ 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

Le journal d'audit de sécurité VDA correspondant à l'événement d'ouverture de session est 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

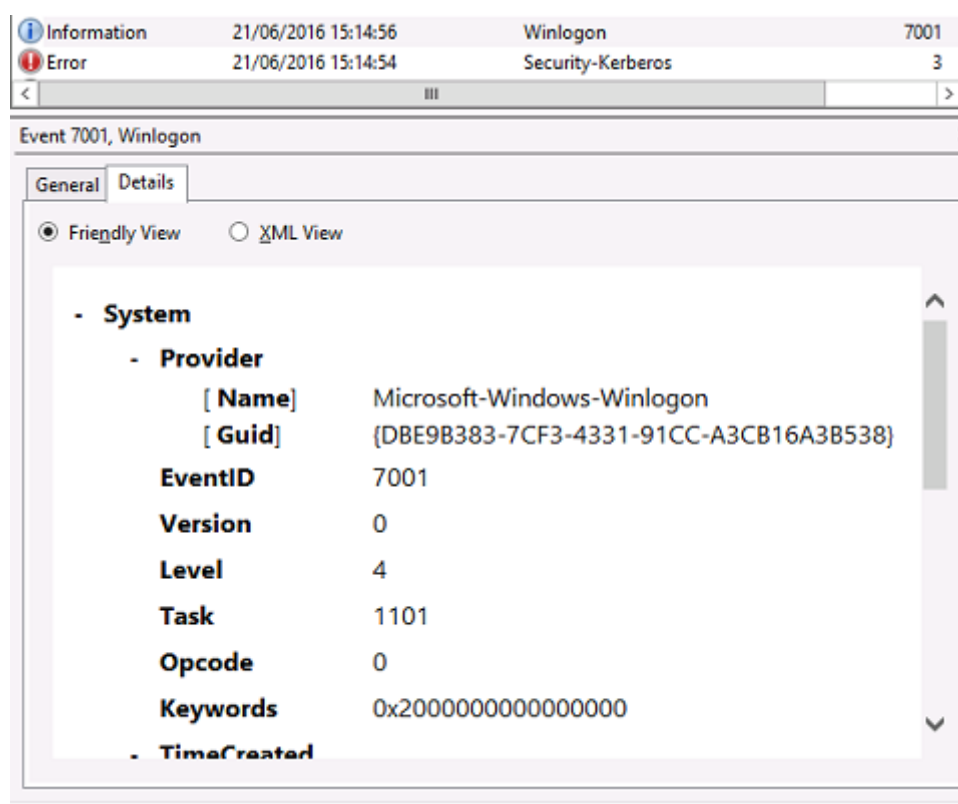
```

- 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.



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 <i>Journaux Kerberos</i> 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.
Le système n'a pas pu vous connecter. Le certificat de carte à puce utilisé pour l'authentification n'est pas approuvé.	Les certificats racine et intermédiaire ne sont pas installés sur l'ordinateur local. Consultez Certificats et infrastructure de clé publique .
Demande incorrecte	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 : <http://support.citrix.com/article/CTX206156>
- Stratégies d'ouverture de session par carte à puce : [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))
- Activation de l'ouverture de session CAPI : <http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx>
- Activation de l'ouverture de session Kerberos : <https://support.microsoft.com/en-us/kb/>

[262177](#)

- Instructions pour activer l'ouverture de session par carte à puce avec des autorités de certification tierces : <https://support.microsoft.com/en-us/kb/281245>

Applets de commande PowerShell

April 1, 2020

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/>.



Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, 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).