

StoreFront 3.11

Jun 30, 2017

[À propos de StoreFront](#)

[Problèmes résolus](#)

[Problèmes connus](#)

[Avis de tiers](#)

[Configuration système requise](#)

[Planifier votre déploiement StoreFront](#)

[Options d'accès utilisateur](#)

[Authentification utilisateur](#)

[Optimiser l'expérience utilisateur](#)

[Haute disponibilité et configuration multisite de StoreFront](#)

[Installer, configurer, mettre à niveau et désinstaller](#)

[Créer un nouveau déploiement](#)

[Joindre un groupe de serveurs existant](#)

[Migrer les fonctionnalités de l'Interface Web vers StoreFront](#)

[Configurer des groupes de serveurs](#)

[Configurer l'authentification et la délégation](#)

[Configurer le service d'authentification](#)

[Authentification basée sur le service XML](#)

[Configurer la délégation Kerberos contrainte pour XenApp 6.5](#)

[Configuration de l'authentification par carte à puce](#)

[Configurer la période de notification d'expiration du mot de passe](#)

[Configurer et gérer des magasins](#)

[Créer ou supprimer un magasin](#)

[Créer un magasin non authentifié](#)

[Exporter des fichiers de provisioning de magasin pour des utilisateurs](#)

[Publier et masquer des magasins pour les utilisateurs](#)

- Gérer les ressources mises à disposition dans les magasins
- Gérer l'accès distant aux magasins via NetScaler Gateway
- Intégrer des applications Citrix Online à des magasins
- Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun
- Paramètres de magasin avancés

Gérer un site Citrix Receiver pour Web

- Créer un site Citrix Receiver pour Web
- Configurer des sites Citrix Receiver pour Web
- Prise en charge de l'expérience Citrix Receiver unifiée
- Créer et gérer des applications recommandées
- Configurer le contrôle de l'espace de travail
- Configurer l'utilisation des onglets de navigateur par Citrix Receiver pour HTML5
- Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion

Configurer l'accès utilisateur

Configurer la haute disponibilité pour les magasins

Intégration avec NetScaler et NetScaler Gateway

- Ajouter une connexion NetScaler Gateway
- Importer un boîtier NetScaler Gateway
- Configurer les paramètres de connexion à NetScaler Gateway
- Équilibrage de charge avec NetScaler
- Configurer deux adresses URL pour le même NetScaler Gateway
- Configurer NetScaler et StoreFront pour l'authentification DFA
- Configurer des points balises

Configurations avancées

- Configurer des sites Desktop Appliance
- Créer un seul nom de domaine complet (FQDN) pour accéder à un magasin en interne et externe
- Configurer le filtrage des ressources

Configurer des sites à l'aide des fichiers de configuration

- Configurer StoreFront à l'aide des fichiers de configuration
- Configurer des sites Citrix Receiver pour Web à l'aide des fichiers de configuration

[Sécuriser votre déploiement StoreFront](#)

[SDK StoreFront](#)

[Résolution des problèmes de StoreFront](#)

[Citrix SCOM Management Pack pour StoreFront](#)

[Citrix SCOM Management Pack pour Serveur de licences](#)

À propos de StoreFront

Jun 30, 2017

StoreFront gère la mise à disposition de bureaux et applications à partir de serveurs XenApp et XenDesktop, et de serveurs XenMobile dans le datacenter vers les périphériques des utilisateurs. StoreFront énumère et rassemble les bureaux et applications disponibles dans des magasins. Les utilisateurs accèdent aux magasins StoreFront via Citrix Receiver directement ou en accédant à un site Citrix Receiver pour Web ou Desktop Appliance. Ils peuvent également accéder à StoreFront à l'aide de clients légers et d'autres appareils compatibles via un site XenApp Services.

StoreFront conserve un enregistrement des applications de chaque utilisateur et met automatiquement à jour leurs périphériques. Cela garantit une expérience cohérente quelle que soit le périphérique que les utilisateurs utilisent, à savoir smartphones, tablettes, ordinateurs portables et ordinateurs de bureau. StoreFront fait partie intégrante de XenApp 7.x et XenDesktop 7.x mais il peut être utilisé avec plusieurs versions de XenApp et XenDesktop.

Nouveautés dans StoreFront

StoreFront 7.11 comprend un certain nombre de problèmes [résolus](#) et [connus](#).

Problèmes résolus

Jun 30, 2017

Les problèmes suivants ont été résolus depuis la version 3.9 :

- Si le service de l'Agent de Citrix SCOM Management Pack est installé sur le serveur StoreFront, StoreFront ne peut pas se mettre à niveau.

[#DNA-34792]

- Lors de la mise à niveau, StoreFront oublie le paramètre de site Web IIS par défaut. Ce problème s'applique aux mises à niveau depuis les versions 3.5, 3.6, 3.7 ou 3.8.

[#DNA-22721]

- La mise à niveau de StoreFront échoue avec une base de données d'abonnement importante (plus de 2 Go).

[#DNA-27194]

- Impossible de se connecter à un site Citrix Receiver pour Web à l'aide de l'authentification pass-through au domaine dans un environnement de service d'autorisation partagé. Si vous disposez de plusieurs magasins partageant un service d'autorisation et que vous créez un nouveau service d'authentification dédié pour l'un des magasins, il n'est pas possible de se connecter au site Citrix Receiver pour Web lors de l'utilisation de l'authentification pass-through au domaine.

[#DNA-34238]

- Les tentatives de lancement d'une session peuvent échouer avec le message d'erreur suivant :

« Le fichier ICA contient un paramètre non signé non valide. »

Avant de mettre à niveau ou remplacer le nouveau fichier ADMX, définissez la stratégie de signature de fichier ICA « Activer la signature de fichier ICA » sur « Non configuré ».

Remarque : la correction #LC5338 fonctionne avec la version 3.9 et les versions ultérieures de StoreFront.

[#LC5338]

- La couleur de l'icône de Citrix Receiver pour Windows ne change pas après la modification du thème de StoreFront.

[#LC6435]

- Après l'installation de StoreFront 3.0.1000 ou 3.0.2000, la console de gestion ne parvient pas à démarrer et le message d'erreur suivant s'affiche : « La console de gestion n'est pas disponible car il manque un certificat racine. Accédez à verisign et téléchargez le certificat "Verisign class primary CA - G5". Pour obtenir davantage d'informations, veuillez consulter l'article [CTX218815](#) du centre de connaissances.

[#LC6471]

- Lorsque vous sélectionnez un site configuré lors de la configuration de XenDesktop, il se peut qu'un magasin par défaut qui utilise le service d'authentification par défaut soit créé dans StoreFront. Si vous supprimez ce magasin, les utilisateurs

de Citrix Receiver pour Windows ne peuvent pas ajouter d'autres magasins et le message d'erreur suivant peut s'afficher :

« Une erreur de protocole s'est produite lors de la communication avec le service d'authentification ».

[#LC6664]

- La mise à niveau StoreFront vers la version 3.0.2000 à partir de la version 2.5 échoue avec l'erreur 1603. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX220411](#) du centre de connaissances.

[#LC6816]

- Les utilisateurs ne peuvent pas voir les applications et bureaux après s'être connectés lorsqu'un broker XML ne fonctionne pas correctement, même lorsque de nombreux autres brokers XML fonctionnent correctement. Le message d'erreur suivant s'affiche :

« Aucun bureau ni aucune application n'est disponible pour le moment. »

[#LC6928]

- Si vous configurez la réinitialisation en libre-service des mots de passe (SSPR) pour un magasin spécifique dans la console StoreFront, la configuration s'applique à tous les magasins et pas seulement au magasin spécifique que vous avez sélectionné.

[#LC6987]

- Les tentatives de propagation des modifications apportées à un groupe de serveurs en sélectionnant « Propager les modifications » sur la console StoreFront peuvent échouer et le message d'erreur suivant s'affiche :

« La propagation a échoué sur un ou plusieurs serveurs. »

[#LC7428]

Problèmes connus

Jun 30, 2017

Les problèmes suivants sont connus dans cette version.

- Les utilisateurs ne peuvent pas ouvrir de session sur Citrix Receiver pour Web si un formulaire d'authentification personnalisé contient un élément avec l'ID=confirmBtn. Les utilisateurs ne peuvent pas ouvrir de session sur Citrix Receiver pour Web si une extension d'authentification StoreFront génère un formulaire d'authentification personnalisé contenant un élément avec l'ID **confirmBtn**. Solution : l'extension d'authentification doit utiliser une valeur d'ID différente dans le formulaire personnalisé.

[# 603196, DNA-22593]

- La console Studio se bloque avec une erreur MMC lorsque vous cliquez sur le nœud StoreFront pour la première fois. Une fois que l'installation de XenDesktop est terminée, lorsque vous ouvrez la console Studio (et ne la refermez pas) et que vous cliquez sur le nœud StoreFront dans le panneau de gauche pour la première fois, le composant enfichable MMC peut se bloquer. Solution : rouvrez Studio.

[#655031, DNA-40366]

- La reconnexion des applications dans le navigateur Chrome peut échouer. Si vous utilisez le navigateur Chrome et que vous vous reconnectez à des applications publiées à partir de serveurs XenApp et XenDesktop, cliquer sur **Connecter** pour les applications peut reconnecter uniquement la première session lorsque plusieurs sessions sont en cours d'utilisation. Solution : cliquez sur **Connecter** pour reconnecter chaque session en cours d'utilisation.

[# 575364, DNA-22561]

- Applications dans AppController. Les applications publiées dans AppController peuvent ne pas démarrer. Solution : utilisez les commandes PowerShell StoreFront pour créer manuellement un magasin avec un service d'authentification situé sur **http://serveursf/Citrix/Authentication**.

[# 599292]

- La configuration du routage HDX optimal avec un ancien applet de commande PowerShell échoue. Lors de la tentative de configuration du routage HDX optimal avec l'ancien applet de commande PowerShell à l'aide de **Set-DSOptimalGatewayForFarms**, la commande échoue.

Solution :

1. Configurez une passerelle globale avec les paramètres souhaités pour le routage HDX optimal à l'aide de la commande **Add-DSGlobalV10Gateway** et fournissez les valeurs par défaut des paramètres d'authentification.
2. Utilisez la commande **Add-DSStoreOptimalGateway** pour ajouter la configuration de passerelle optimale.

Exemple :

```
Add-DSGlobalV10Gateway -Id 2eba0524-af40-421e-9c5f-a1ccca80715f -Name LondonGateway -Address "http://example" -Logon Domain -SecureTicketAuthorityUrls @("http://staur1", "http://staur2")
Add-DSStoreOptimalGateway -SiteId 1 -VirtualPath /Citrix/Store1 -GatewayId 2eba0524-af40-421e-9c5f-a1ccca80715f -Farms @("Controller") -EnabledOnDirectAccess $true
```

[# 624040]

- Problèmes avec le service d'authentification après la mise à niveau. Les mises à niveau de StoreFront 2.x vers 3.x suivies d'une propagation sur le groupe de serveurs peuvent entraîner l'ajout d'une entrée au fichier de configuration de l'authentification pour **pnaAuthenticationStartupModule**. Étant donné que les entrées peuvent uniquement être ajoutées aux services d'authentification qui ont été activés pour les services d'authentification PNA et la modification du mot de passe PNA, le service d'authentification ne peut pas démarrer car le module de démarrage nommé est absent. Solution : supprimez l'entrée du fichier de configuration de l'authentification. Le fichier de configuration réside par défaut sur **C:\inetpub\wwwroot\Citrix\web.config**.

[# 640644]

Avis de tiers

Jun 30, 2017

StoreFront peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans le document suivant :



[Avis de tiers StoreFront](#)

Configuration système requise

Jun 30, 2017

Lors de la planification de votre installation, Citrix vous recommande de prévoir au minimum 2 Go de RAM supplémentaire pour StoreFront en sus des exigences de tout autre produit installé sur le serveur. Le Citrix Subscriptions Store Service requiert un minimum de 5 Mo d'espace disque, plus environ 8 Mo pour chaque abonnement comprenant 1000 applications. Toutes les autres spécifications matérielles doivent remplir la configuration minimale requise pour le système d'exploitation installé.

Citrix a testé et fourni la prise en charge de l'installation de StoreFront sur les plates-formes suivantes :

- Windows Server 2016 éditions Standard et Datacenter
- Windows Server 2012 R2 éditions Standard et Datacenter
- Windows Server 2012 éditions Standard et Datacenter
- Windows Server 2008 R2 Service Pack 1 éditions Enterprise et Standard

La mise à niveau de la version du système d'exploitation sur un serveur exécutant StoreFront n'est pas prise en charge. Citrix vous recommande d'installer StoreFront sur une nouvelle installation du système d'exploitation. Tous les serveurs dans un déploiement sur plusieurs serveurs doivent exécuter la même version du système d'exploitation avec les mêmes paramètres régionaux. Les groupes de serveurs StoreFront contenant diverses versions de système d'exploitation et de paramètres régionaux ne sont pas pris en charge. Bien qu'un groupe de serveurs puisse contenir jusqu'à six serveurs, d'un point de vue de la capacité, les simulations ont démontré qu'aucun avantage ne découlait de l'utilisation de groupes de serveurs contenant plus de trois serveurs. Tous les serveurs dans un groupe de serveurs doivent résider dans le même emplacement.

Microsoft Internet Information Services (IIS) et Microsoft .NET Framework sont requis sur le serveur. Si l'un de ces composants est installé mais non activé, le programme d'installation de StoreFront les active avant de procéder à l'installation du produit. Windows PowerShell 2.0 et Microsoft Management Console 3.0, qui sont tous les deux des composants par défaut de Windows Server, doivent être installés sur le serveur Web avant de pouvoir installer StoreFront. Le chemin d'accès relatif à StoreFront dans IIS doit être identique sur tous les serveurs d'un groupe.

Le programme d'installation de StoreFront va installer les fonctionnalités IIS dont il a besoin. Si vous pré-installez ces fonctionnalités, ce qui suit est requis :

Sur toutes les plates-formes :

- Web-Static-Content
- Web-Default-Doc
- Web-Http-Errors
- Web-Http-Redirect
- Web-Http-Logging
- Web-Mgmt-Console
- Web-Scripting-Tools
- Web-Windows-Auth
- Web-Basic-Auth
- Web-AppInit

Sur Windows Server 2008 R2 :

- Web-Asp-Net
- As-Tcp-PortSharing

Sur Windows Server 2012 R2 :

- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

Sur Windows Server 2016

- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

StoreFront utilise les ports suivants pour les communications. Assurez-vous que votre pare-feu et autres périphériques réseau autorisent l'accès à ces ports.

- Les ports TCP 80 et 443 sont utilisés pour les communications HTTP et HTTPS, respectivement, et doivent être accessibles de l'intérieur et de l'extérieur du réseau de l'entreprise.
- Le port TCP 808 est utilisé pour les communications entre les serveurs StoreFront et doit être accessible de l'intérieur du réseau d'entreprise.
- Un port TCP sélectionné aléatoirement à partir de tous les ports non réservés est utilisé pour les communications entre les serveurs StoreFront dans un groupe de serveurs. Lorsque vous installez StoreFront, une règle du Pare-feu Windows est configurée pour activer l'accès à l'exécutable de StoreFront. Toutefois, étant donné que le port est attribué de manière aléatoire, vous devez vous assurer que tous les pare-feu ou autres périphériques sur votre réseau interne ne bloquent pas le trafic des ports TCP non attribués.
- Le port TCP 8008 est utilisé par Citrix Receiver pour HTML5, lorsque ce dernier est activé, pour les communications des utilisateurs locaux sur le réseau interne avec les serveurs fournissant leurs bureaux et applications.

StoreFront prend en charge les réseaux IPv6 et les environnements à double pile IPv4/IPv6.

Configuration requise pour l'infrastructure

Citrix a testé et fourni la prise en charge pour StoreFront lorsqu'il est utilisé avec les versions de produits Citrix suivants.

Configuration requise sur les serveurs Citrix

Les magasins StoreFront regroupent les bureaux et applications des produits suivants.

- XenDesktop
 - XenDesktop 7.14
 - XenDesktop 7.13
 - XenDesktop 7.12
 - XenDesktop 7.11
 - XenDesktop 7.9
 - XenDesktop 7.8
 - XenDesktop 7.7
 - XenDesktop 7.6
 - XenDesktop 7.5
 - XenDesktop 7.1
 - XenDesktop 7
 - XenDesktop 5.6 Feature Pack 1

- XenDesktop 5.6
- XenDesktop 5.5
- XenApp
 - XenApp 7.14
 - XenApp 7.13
 - XenApp 7.12
 - XenApp 7.11
 - XenApp 7.9
 - XenApp 7.8
 - XenApp 7.7
 - XenApp 7.6
 - XenApp 7.5
 - XenApp 6.5 Feature Pack 2
 - XenApp 6.5 Feature Pack 1 pour Windows Server 2008 R2
 - XenApp 6.5 pour Windows Server 2008 R2
 - XenApp 6.0 pour Windows Server 2008 R2
- XenMobile
 - XenMobile 9.0/App Controller 9.0

Configuration requise pour NetScaler Gateway.

Les versions suivantes de NetScaler Gateway peuvent être utilisées pour fournir l'accès à StoreFront aux utilisateurs de réseaux publics.

- NetScaler Gateway 11.x
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 build 69.4 (le numéro de version est affiché en haut de l'utilitaire de configuration)

Configuration requise pour Citrix Receiver pour HTML5

Si vous souhaitez autoriser les utilisateurs à accéder aux bureaux et applications à l'aide de Citrix Receiver pour HTML5 exécuté sur les sites Receiver pour Web, les exigences supplémentaires suivantes s'appliquent.

Pour les connexions au réseau interne, Citrix Receiver pour HTML5 permet d'accéder aux bureaux et applications fournis par les produits suivants.

- XenDesktop 7.14
- XenDesktop 7.13
- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7

- XenApp 7.14
- XenApp 7.13
- XenApp 7.12
- XenApp 7.11
- XenApp 7.9
- XenApp 7.8
- XenApp 7.7
- XenApp 7.6
- XenApp 7.5
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 pour Windows Server 2008 R2 (nécessite le correctif logiciel XA650R01W2K8R2X64051, qui est disponible sur <http://support.citrix.com/article/CTX135757>)

Pour les utilisateurs distants en dehors du réseau de l'entreprise, Citrix Receiver pour HTML5 permet d'accéder à des bureaux et des applications via les versions suivantes de NetScaler Gateway.

- NetScaler Gateway 11.x
- NetScaler Gateway 10.1
- Access Gateway 10 build 71.6014 (le numéro de version est affiché en haut de l'utilitaire de configuration)

Pour les utilisateurs qui se connectent via NetScaler Gateway, Citrix Receiver pour HTML5 permet d'accéder aux bureaux et applications fournis par les produits suivants.

- XenDesktop
 - XenDesktop 7.14
 - XenDesktop 7.13
 - XenDesktop 7.12
 - XenDesktop 7.11
 - XenDesktop 7.9
 - XenDesktop 7.8
 - XenDesktop 7.7
 - XenDesktop 7.6
 - XenDesktop 7.5
 - XenDesktop 7.1
 - XenDesktop 7
 - XenDesktop 5.6
 - XenDesktop 5.5
- XenApp
 - XenApp 7.14
 - XenApp 7.13
 - XenApp 7.12
 - XenApp 7.11
 - XenApp 7.9
 - XenApp 7.8
 - XenApp 7.7
 - XenApp 7.6
 - XenApp 7.5
 - XenApp 6.5 Feature Pack 2

- XenApp 6.5 Feature Pack 1 pour Windows Server 2008 R2
- XenApp 6.5 pour Windows Server 2008 R2
- XenApp 6.0 pour Windows Server 2008 R2

Configuration requise pour la machine utilisateur

Mise à jour : 22-02-2017

StoreFront fournit un certain nombre d'options permettant aux utilisateurs d'accéder à leurs bureaux et applications. Les utilisateurs Citrix Receiver peuvent accéder aux magasins via Citrix Receiver ou ils peuvent utiliser un navigateur Web pour ouvrir une session sur un site Citrix Receiver pour Web du magasin. Pour les utilisateurs qui ne peuvent pas installer Citrix Receiver, mais ont un navigateur Web compatible HTML5, vous pouvez fournir l'accès aux bureaux et applications directement dans le navigateur Web en activant Citrix Receiver pour HTML5 sur votre site Citrix Receiver pour Web.

Les utilisateurs équipés de boîtiers de bureau n'appartenant pas à un domaine accèdent à leurs bureaux au travers de leurs navigateurs Web, qui sont configurés pour accéder à des sites Desktop Appliance. Dans le cas de boîtiers de bureau appartenant à un domaine et de PC réaffectés exécutant Citrix Desktop Lock, ainsi que de clients Citrix plus anciens qui ne peuvent pas être mis à niveau, les utilisateurs doivent se connecter via l'adresse URL XenApp Services du magasin.

Si vous envisagez de proposer des applications en mode déconnecté aux utilisateurs, Offline Plug-in est requis en plus de Citrix Receiver pour Windows. Si vous envisagez de fournir aux utilisateurs des séquences Microsoft Application Virtualization (App-V), une version compatible de Microsoft Application Virtualization Desktop Client est également requise. Pour plus d'informations, veuillez consulter la section [Gestion des applications livrées en streaming](#). Les utilisateurs ne peuvent pas accéder aux applications en mode déconnecté ou aux séquences App-V via les sites Citrix Receiver pour Web.

Elle suppose que toutes les machines utilisateur répondent à la configuration matérielle minimale requise pour le système d'exploitation installé.

Configuration requise pour les magasins Citrix Receiver

Les versions suivantes de Citrix Receiver peuvent être utilisées pour accéder aux magasins StoreFront à partir du réseau interne et via NetScaler Gateway. Les connexions établies via NetScaler Gateway peuvent être effectuées à l'aide de NetScaler Gateway Plug-in et/ou de l'accès sans client. Citrix Receiver pour Windows 4.3 est la version minimale requise pour bénéficier de l'expérience unifiée StoreFront de Citrix Receiver. Consultez la section [Prise en charge de l'expérience Citrix Receiver unifiée](#).

- [Citrix Receiver pour Chrome 2.x](#)
- [Citrix Receiver pour HTML5 2.x](#)
- [Citrix Receiver pour Mac 12.x](#)
- [Citrix Receiver pour Windows 4.x](#)
- [Citrix Receiver pour Linux 13.x](#)

Configuration requise pour accéder aux magasins via les sites Citrix Receiver pour Web

Les combinaisons Citrix Receiver, système d'exploitation et navigateur Web suivantes sont recommandées pour les utilisateurs qui accèdent aux sites Citrix Receiver pour Web depuis le réseau interne et via NetScaler Gateway. Les connexions établies via NetScaler Gateway peuvent être effectuées à l'aide de NetScaler Gateway Plug-in et de l'accès sans client.

- Citrix Receiver for Windows 4.7, Citrix Receiver for Windows 4.6, Citrix Receiver pour Windows 4.5, Citrix Receiver pour Windows 4.4, Citrix Receiver pour Windows 4.3 et Citrix Receiver pour Windows 4.2.x
 - Windows 10 (éditions 32 et 64 bits)
 - Microsoft Edge
 - Internet Explorer 11
 - Google Chrome
 - Mozilla Firefox
 - Windows 8.1 (éditions 32 et 64 bits)
 - Internet Explorer 11 (mode 32 bits)
 - Google Chrome
 - Mozilla Firefox
 - Windows 8 (éditions 32 et 64 bits)
 - Internet Explorer 10 (mode 32 bits)
 - Google Chrome
 - Mozilla Firefox
 - Windows 7 Service Pack 1 (éditions 32 et 64 bits)
 - Internet Explorer 11, 10, 9
 - Google Chrome
 - Mozilla Firefox
 - Windows Embedded Standard 7 Service Pack 1 ou Windows Thin PC
 - Internet Explorer 11, 10, 9
- Citrix Receiver pour Windows 4.0 et Citrix Receiver pour Windows 3.4
 - Windows 8 (éditions 32 et 64 bits)
 - Internet Explorer 10 (mode 32 bits)
 - Google Chrome
 - Mozilla Firefox
 - Windows 7 Service Pack 1 (éditions 32 et 64 bits)
 - Internet Explorer 11, 10, 9
 - Google Chrome
 - Mozilla Firefox
 - Windows Embedded Standard 7 Service Pack 1 et Windows Thin PC
 - Internet Explorer 11, 10, 9
- Citrix Receiver pour Mac 12.0
 - Mac OS X 10.11 El Capitan
 - Safari 9
 - Google Chrome
 - Mozilla Firefox
 - Mac OS X 10.10 Yosemite
 - Safari 8
 - Google Chrome
 - Mozilla Firefox
 - Mac OS X 10.9 Mavericks
 - Safari 7
 - Google Chrome
 - Mozilla Firefox
- Citrix Receiver pour Linux 12.1 et Citrix Receiver pour Linux 13.x

- Ubuntu 12.04 (32 bits) et 14.04 LTS (32 bits)
 - Google Chrome
 - Mozilla Firefox

Configuration requise pour accéder aux bureaux et applications via Receiver pour HTML5

Les systèmes d'exploitation et les navigateurs Web suivants sont recommandés pour les utilisateurs qui accèdent aux bureaux et applications à l'aide de Receiver pour HTML5 exécuté sur des sites Receiver pour Web. Les connexions au réseau interne et les connexions via NetScaler Gateway sont prises en charge. Toutefois, pour les connexions depuis le réseau interne, Receiver pour HTML5 permet d'accéder uniquement aux ressources fournies par des produits spécifiques. En outre, des versions spécifiques de NetScaler Gateway sont requises pour autoriser les connexions extérieures au réseau d'entreprise. Pour plus d'informations, veuillez consulter la section [Configuration requise pour l'infrastructure](#).

- Navigateurs
 - Microsoft Edge
 - Internet Explorer 11 et 10 (connexions HTTP uniquement)
 - Safari 7
 - Safari 6
 - Google Chrome
 - Mozilla Firefox
- Systèmes d'exploitation
 - Windows RT
 - Windows 10 (éditions 32 et 64 bits)
 - Windows 8.1 (éditions 32 et 64 bits)
 - Windows 8 (éditions 32 et 64 bits)
 - Windows 7 Service Pack 1 (éditions 32 et 64 bits)
 - Windows Vista Service Pack 2 (éditions 32 et 64 bits)
 - Windows Embedded XP
 - Mac OS X 10.10 Yosemite
 - Mac OS X 10.9 Mavericks
 - Mac OS X 10.8 Mountain Lion
 - Mac OS X 10.7 Lion
 - Mac OS X 10.6 Snow Leopard
 - Google Chrome OS 48
 - Google Chrome OS 47
 - Ubuntu 12.04 (32 bits)

Configuration requise pour accéder aux magasins via des sites Desktop Appliance

Les combinaisons Citrix Receiver, système d'exploitation et navigateur Web suivantes sont recommandées pour les utilisateurs qui accèdent aux sites Desktop Appliance depuis le réseau interne. Les connexions via NetScaler Gateway ne sont pas prises en charge.

- Citrix Receiver pour Windows 4.5, Citrix Receiver pour Windows 4.4, Citrix Receiver pour Windows 4.3, Citrix Receiver pour Windows 4.2.x et Citrix Receiver pour Windows 4.1
 - Windows 8.1 (éditions 32 et 64 bits)

- Internet Explorer 11 (mode 32 bits)
- Windows 8 (éditions 32 et 64 bits)
 - Internet Explorer 10 (mode 32 bits)
- Windows 7 Service Pack 1 (éditions 32 bits et 64 bits), Windows Embedded Standard 7 Service Pack 1 ou Windows Thin PC
 - Internet Explorer 9 (mode 32 bits)
 - Internet Explorer 8 (mode 32 bits)
- Windows Embedded XP
 - Internet Explorer 8 (mode 32 bits)
- Citrix Receiver pour Windows 4.0 ou Citrix Receiver pour Windows 3.4
 - Windows 8 (éditions 32 et 64 bits)
 - Internet Explorer 10 (mode 32 bits)
 - Windows 7 Service Pack 1 (éditions 32 bits et 64 bits), Windows Embedded Standard 7 Service Pack 1 ou Windows Thin PC
 - Internet Explorer 9 (mode 32 bits)
 - Internet Explorer 8 (mode 32 bits)
 - Windows Embedded XP
 - Internet Explorer 8 (mode 32 bits)
- Citrix Receiver pour Windows Enterprise 3.4
 - Windows 7 Service Pack 1 (éditions 32 bits et 64 bits), Windows Embedded Standard 7 Service Pack 1 ou Windows Thin PC
 - Internet Explorer 9 (mode 32 bits)
 - Internet Explorer 8 (mode 32 bits)
 - Windows Embedded XP
 - Internet Explorer 8 (mode 32 bits)
- Citrix Receiver pour Linux 12.1
 - Ubuntu 12.04 (32 bits)
 - Mozilla Firefox 27

Configuration requise pour accéder aux magasins via les adresses URL XenApp Services

Toutes les versions de Citrix Receiver répertoriées ci-dessus peuvent être utilisées pour accéder aux magasins StoreFront avec fonctionnalités réduites via les adresses URL XenApp Services. En outre, vous pouvez utiliser l'ancien client qui ne prend pas en charge les autres méthodes d'accès, Citrix Receiver pour Linux 12.0 (connexions au réseau interne uniquement), pour accéder aux magasins via les adresses URL XenApp Services. Les connexions établies via NetScaler Gateway, lorsqu'elles sont prises en charge, peuvent être effectuées à l'aide de NetScaler Gateway Plug-in et de l'accès sans client.

Spécifications de la carte à puce

Configuration requise pour utiliser Citrix Receiver pour Windows 4.x avec des cartes à puce

Citrix teste la compatibilité des cartes avec des agences gouvernementales américaines telles le Government Common Access Card (CAC), le National Institute of Standards and Technology Personal Identity Verification (NIST PIV) et avec certains jetons de carte à puce USB. Vous pouvez utiliser des lecteurs de carte de contact conformes aux spécifications des lecteurs USB CCID qui sont classés par le German Zentraler Kreditausschuss (ZKA) en tant que lecteurs de carte à puce de classe 1. Les lecteurs de carte de contact de classe ZKA 1 exigent que les utilisateurs insèrent leur carte à puce dans le

lecteur. Les autres types de lecteurs de carte à puce, y compris les lecteurs de classe 2 (qui ont équipés de pavés numériques pour la saisie de codes PIN), les lecteurs sans contacts et les cartes à puce virtuelles basées sur les puces TPM, ne sont pas pris en charge.

Pour les machines Windows, la prise en charge des cartes à puce repose sur les spécifications standard PC/SC (Personal Computer/Smart Card) de Microsoft. En tant qu'exigence minimale, les cartes à puce et les lecteurs de carte doivent être pris en charge par le système d'exploitation et avoir obtenu la Certification matérielle Windows.

Pour de plus amples informations sur les cartes à puce et middleware compatibles avec Citrix, consultez la section [Cartes à puce](#) dans la documentation de XenDesktop et <http://www.citrix.com/ready>.

Configuration requise pour utiliser des sites Desktop Appliance avec des cartes à puce

Pour les utilisateurs dotés de boîtiers de bureau et de PC réaffectés exécutant Citrix Desktop Lock, Citrix Receiver pour Windows Enterprise 3.4 est requis pour l'authentification par carte à puce. Citrix Receiver pour Windows version 4.1 peut être utilisé sur toutes les autres machines Windows.

Configuration requise pour l'authentification via NetScaler Gateway

Les versions suivantes de NetScaler Gateway peuvent être utilisées pour fournir l'accès à StoreFront aux utilisateurs de réseaux publics qui s'authentifient à l'aide de cartes à puce.

- NetScaler Gateway 11.x
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 build 69.4 (le numéro de version est affiché en haut de l'utilitaire de configuration)

Planifier votre déploiement StoreFront

Jun 30, 2017

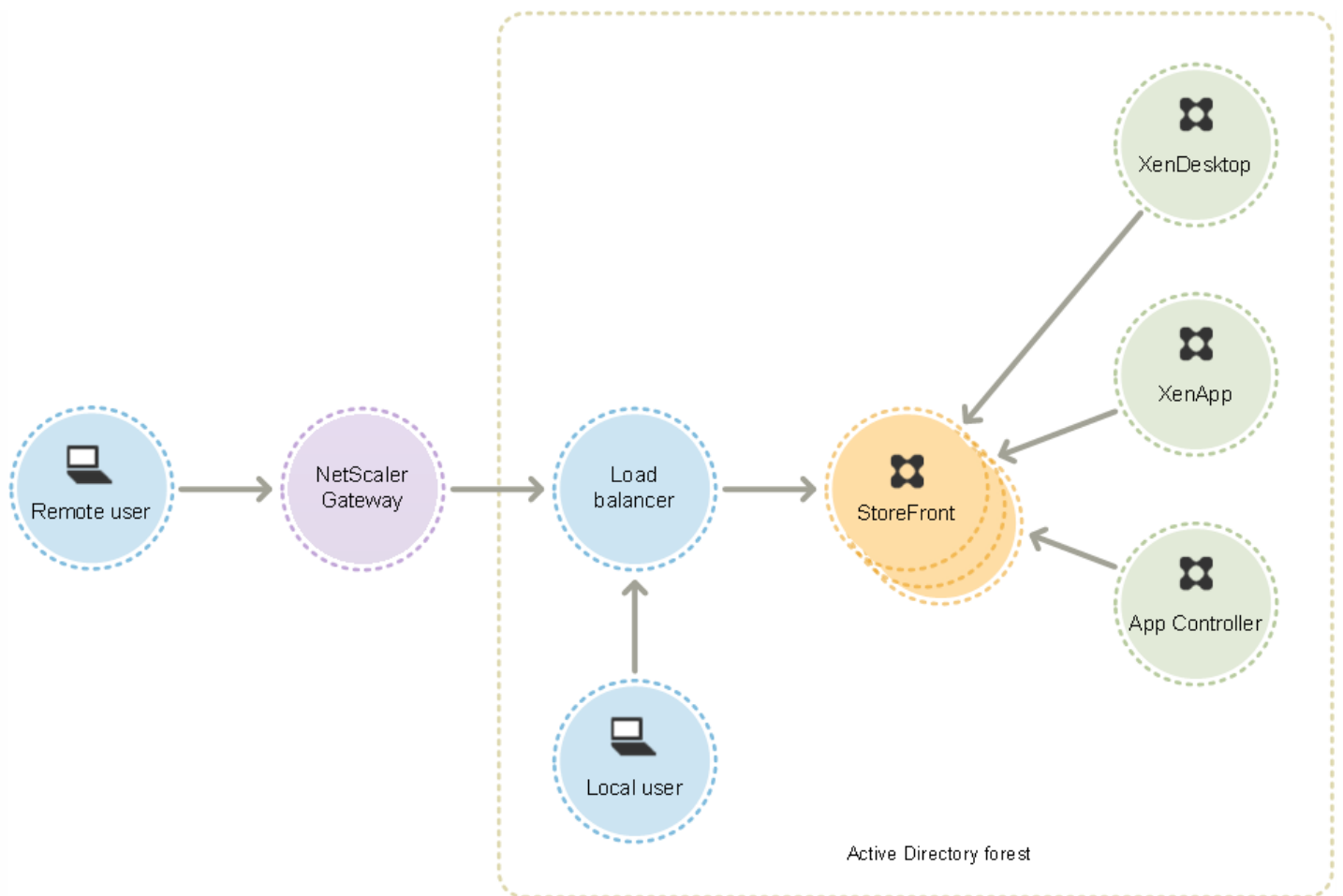
StoreFront fait appel à la technologie Microsoft .NET exécutée sur Microsoft Internet Information Services (IIS) pour fournir des magasins d'applications d'entreprise qui regroupent les ressources et les mettent à la disposition des utilisateurs. StoreFront s'intègre à vos déploiements XenDesktop, XenApp et App Controller pour offrir aux utilisateurs un point d'accès unique et en libre-service à leurs bureaux et applications.

StoreFront comprend les composants principaux suivants :

- Le service d'authentification authentifie les utilisateurs auprès de Microsoft Active Directory, si bien que les utilisateurs n'ont pas besoin de rouvrir une session pour accéder à leurs bureaux et applications. Pour plus d'informations, veuillez consulter la section [Authentification utilisateur](#).
- Les magasins énumèrent et regroupent les bureaux et les applications à partir de XenDesktop, XenApp et App Controller. Les utilisateurs accèdent aux magasins via Citrix Receiver, des sites Citrix Receiver pour Web, des sites Desktop Appliance et des adresses URL XenApp Services. Pour plus d'informations, veuillez consulter la section [Options d'accès utilisateur](#).
- Le Subscriptions Store Service enregistre les informations d'abonnement aux applications et met à jour les machines des utilisateurs afin de garantir une expérience d'itinérance cohérente. Pour de plus amples informations sur l'amélioration de l'expérience pour vos utilisateurs, consultez la section [Optimiser l'expérience utilisateur](#).

StoreFront peut être configuré sur un serveur unique ou sous forme de déploiement sur plusieurs serveurs. Les déploiements sur de multiples serveurs fournissent non seulement une capacité supplémentaire, mais aussi une plus grande disponibilité. L'architecture modulaire de StoreFront garantit que les informations de configuration et les détails des applications auxquelles les utilisateurs sont abonnés sont stockés et répliqués entre tous les serveurs dans un groupe de serveurs. Cela signifie que si un serveur StoreFront devient indisponible pour une raison quelconque, les utilisateurs peuvent continuer à accéder à leurs magasins à l'aide des serveurs restants. Dans le même temps, les données de configuration et d'abonnement sur le serveur défaillant sont automatiquement mises à jour lorsqu'il se reconnecte au groupe de serveurs. Les données d'abonnement sont mises à jour lorsque le serveur est de nouveau opérationnel, mais vous devez propager les modifications apportées à la configuration qui ont été ignorées par le serveur lorsqu'il était hors connexion. Dans le cas d'une défaillance matérielle nécessitant le remplacement du serveur, vous pouvez installer StoreFront sur un nouveau serveur et ajouter ce dernier au groupe de serveurs existant. Le nouveau serveur est automatiquement configuré et mis à jour avec les applications auxquelles les utilisateurs sont abonnés lorsqu'il est associé au groupe de serveurs.

La figure suivante illustre un déploiement StoreFront standard.



Équilibrage de charge

Pour les déploiements sur plusieurs serveurs, l'équilibrage de charge externe, par exemple, l'équilibrage de la charge réseau Windows ou NetScaler est requis. Configurez l'environnement d'équilibrage de charge pour le basculement entre les serveurs afin de fournir un déploiement tolérant aux pannes. Pour plus d'informations sur l'équilibrage de la charge avec NetScaler, consultez la section [Équilibrage de charge](#). Pour plus d'informations sur l'équilibrage de la charge réseau Windows, consultez l'article <http://technet.microsoft.com/en-us/library/hh831698.aspx>.

L'équilibrage de charge actif des demandes envoyées depuis StoreFront vers des sites XenDesktop et des batteries XenApp est recommandé pour les déploiements comprenant des milliers d'utilisateurs ou dans lesquels les charges sont élevées, par exemple lorsqu'un grand nombre d'utilisateurs ouvrent des sessions sur une courte période. Utilisez un équilibrage de charge avec analyses XML et persistance de session intégrés, tel que NetScaler.

Si vous déployez un équilibrage de charge d'arrêt SSL ou si vous avez besoin de résoudre des problèmes, vous pouvez utiliser l'applet de commande PowerShell **Set-STFWebReceiverCommunication**.

Syntaxe :

Set-STFWebReceiverCommunication [-WebReceiverService] [[-Loopback]] [[-LoopbackPortUsingHttp]]

Les valeurs valides sont :

- **On** : valeur par défaut pour les nouveaux sites Citrix Receiver pour Web. Citrix Receiver pour Web utilise le schéma (HTTPS

ou HTTP) et le numéro de port de l'adresse URL de base mais remplace l'hôte avec l'adresse IP de bouclage pour communiquer avec StoreFront Services. Cela fonctionne dans les déploiements ne contenant qu'un seul serveur et dans les déploiements ne contenant pas d'équilibrage de charge d'arrêt SSL.

- **OnUsingHttp** : Citrix Receiver pour Web utilise HTTP et l'adresse IP de bouclage pour communiquer avec StoreFront Services. Si vous utilisez un équilibrage de charge d'arrêt SSL, sélectionnez cette valeur. Vous devez également spécifier le port HTTP si le port par défaut 80 n'est pas utilisé.
- **Off** : cette option désactive le bouclage et Citrix Receiver pour Web utilise l'adresse URL de base StoreFront pour communiquer avec StoreFront Services. Si vous effectuez une mise à niveau sur place, il s'agit de la valeur par défaut pour éviter tout dysfonctionnement de votre déploiement existant.

À titre d'exemple, si vous utilisez un équilibrage de charge d'arrêt SSL, que votre IIS est configuré pour utiliser le port 81 pour HTTP, et que le chemin d'accès de votre site Citrix Receiver pour Web est /Citrix/StoreWeb, vous pouvez exécuter la commande suivante pour configurer le site Citrix Receiver pour Web :

```
$wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
```

```
Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback OnUsingHttp -LoopbackPortUsingHttp 81
```

Veuillez noter que vous devez désactiver le bouclage pour utiliser un outil de proxy Web tel que Fiddler pour capturer le trafic réseau entre Citrix Receiver pour Web et StoreFront Services.

Considérations relatives à Active Directory

Pour les déploiements sur un seul serveur, vous pouvez installer StoreFront sur un serveur n'appartenant pas à un domaine (mais certaines fonctionnalités ne seront pas disponibles) ; sinon, les serveurs StoreFront doivent résider dans le domaine Active Directory contenant les comptes de vos utilisateurs ou dans un domaine qui a une relation d'approbation avec le domaine des comptes utilisateur, sauf si vous activez la délégation d'authentification auprès des sites ou batteries XenApp et XenDesktop. Tous les serveurs StoreFront du groupe doivent résider sur le même domaine.

Connexions utilisateur

Dans un environnement de production, Citrix vous recommande d'utiliser le protocole HTTPS pour sécuriser les communications entre StoreFront et les machines des utilisateurs. Pour utiliser le protocole HTTPS, StoreFront requiert que l'instance IIS hébergeant le service d'authentification et les magasins associés soit configurée pour HTTPS. En l'absence de la configuration IIS appropriée, StoreFront utilise le protocole HTTP pour les communications. Vous pouvez passer de HTTP à HTTPS à tout moment, dans la mesure où la configuration IIS appropriée a été implémentée.

Si vous prévoyez d'activer l'accès à StoreFront en dehors du réseau d'entreprise, NetScaler Gateway est requis pour sécuriser les connexions des utilisateurs distants. Déployez NetScaler Gateway en dehors du réseau de l'entreprise, avec des pare-feu séparant NetScaler Gateway des réseaux internes et publics. Assurez-vous que NetScaler Gateway est en mesure d'accéder à la forêt Active Directory contenant les serveurs StoreFront.

Sites Web Internet Information Services (IIS) multiples

StoreFront vous permet de déployer différents magasins dans différents sites Web IIS par serveur Windows de façon à ce que chaque magasin puisse avoir une liaison de certificat et un nom d'hôte différents.

Commencez par créer deux sites Web, en plus du site Web par défaut. Après la création de plusieurs sites Web dans IIS, utilisez le kit de développement PowerShell pour créer un déploiement StoreFront dans chacun de ces sites Web IIS. Pour de plus amples informations sur la création de sites Web dans IIS, consultez la section [Comment configurer votre premier site Web IIS](#).

Remarque : les consoles StoreFront et PowerShell ne peuvent pas être ouvertes en même temps. Fermez toujours la console d'administration StoreFront avant d'utiliser la console PowerShell pour administrer votre configuration StoreFront. De même, fermez toutes les instances de PowerShell avant d'ouvrir la console StoreFront.

Exemple : pour créer deux déploiements de site Web IIS - un pour les applications et un pour le bureau.

1. Add-STFDeployment -SiteID 1 -HostBaseURL "https://www.storefront.app.com"
2. Add-STFDeployment -SiteID 2 -HostBaseURL "https://www.storefront.desktop.com"

StoreFront désactive la console de gestion lorsqu'il détecte de multiples sites et affiche un message à cet effet.

Pour de plus amples informations, consultez la section [Avant l'installation et la configuration](#).

Capacité à monter en charge

Le nombre d'utilisateurs Citrix Receiver pris en charge par un groupe de serveurs StoreFront dépend du matériel et du niveau d'activité utilisateur. D'après nos scénarios d'activités simulées au cours desquels les utilisateurs se connectent, énumèrent 100 applications publiées et démarrent une ressource, un seul serveur StoreFront doté de la spécification minimum recommandée de deux processeurs virtuels exécutés sur un serveur sous-jacent équipé de deux processeurs Intel Xeon L5520 2.27Ghz peut prendre en charge jusqu'à 30 000 connexions utilisateur par heure.

Un groupe de serveurs dotés de deux serveurs configurés à l'identique dans le groupe peut prendre en charge jusqu'à 60 000 connexions utilisateur par heure ; trois nœuds jusqu'à 90 000 connexions utilisateur par heure ; quatre nœuds jusqu'à 120 000 connexions utilisateur par heure ; cinq nœuds jusqu'à 150 000 connexions utilisateur par heure ; six nœuds jusqu'à 175 000 connexions utilisateur par heure.

La capacité d'un seul serveur StoreFront peut également être augmentée en attribuant plus de processeurs virtuels au système, sachant que quatre processeurs virtuels permettent de prendre en charge jusqu'à 55 000 connexions utilisateur par heure et que huit processeurs virtuels permettent de prendre en charge jusqu'à 80 000 connexions utilisateur par heure.

L'allocation de mémoire minimum recommandée pour chaque serveur est de 4 Go. Lors de l'utilisation de Citrix Receiver pour Web, attribuez 700 octets supplémentaires par ressource et par utilisateur en plus de l'allocation de mémoire de base. Comme c'est le cas lors de l'utilisation de Receiver pour Web, lors de l'utilisation de Citrix Receiver, prévoyez 700 octets supplémentaires par ressource lors de la création des environnements, par utilisateur en plus des 4 Go requis pour la mémoire pour cette version de StoreFront.

Étant donné que vos modes d'utilisation peuvent être différents de ces scénarios, il est possible que vos serveurs puissent prendre en charge plus ou moins de connexions utilisateur par heure.

Important : tous les serveurs dans un groupe de serveurs doivent résider dans le même emplacement. Les groupes de serveurs StoreFront contenant diverses versions de système d'exploitation et de paramètres régionaux ne sont pas pris en charge.

Considérations relatives au délai d'expiration

Des problèmes réseau ou d'autres problèmes peuvent parfois survenir entre un magasin StoreFront et les serveurs qu'il contacte, ce qui peut entraîner des retards ou des erreurs pour les utilisateurs. Vous pouvez utiliser les paramètres d'expiration d'un magasin pour adapter ce comportement. Si vous spécifiez un délai d'expiration court, StoreFront abandonne un serveur rapidement et en essaye un autre. Ceci est utile si, par exemple, vous avez configuré plusieurs serveurs à des fins de basculement.

Si vous spécifiez un délai d'expiration plus long, StoreFront accorde plus de temps à un serveur. Ceci est utile dans les

environnements dans lesquels la fiabilité du réseau ou du serveur est incertaine et dans lesquels les délais sont courants.

Citrix Receiver pour Web dispose également d'un paramètre d'expiration, qui contrôle la durée pendant laquelle un site Receiver pour Web attend une réponse du magasin. Définissez une valeur pour ce paramètre d'expiration au moins aussi longue que le délai d'expiration du magasin. Un paramètre de délai d'expiration plus important améliore la tolérance aux pannes, mais se traduit par des délais plus importants. Un paramètre de délai d'expiration plus court réduit les délais, mais en contrepartie les utilisateurs peuvent rencontrer plus d'erreurs.

Pour de plus amples informations sur la configuration des délais d'expiration, consultez les sections [Durée d'expiration des communications et nombre de tentatives de reconnexion au serveur](#) et [Durée d'expiration des communications et nombre de tentatives de reconnexion au serveur](#).

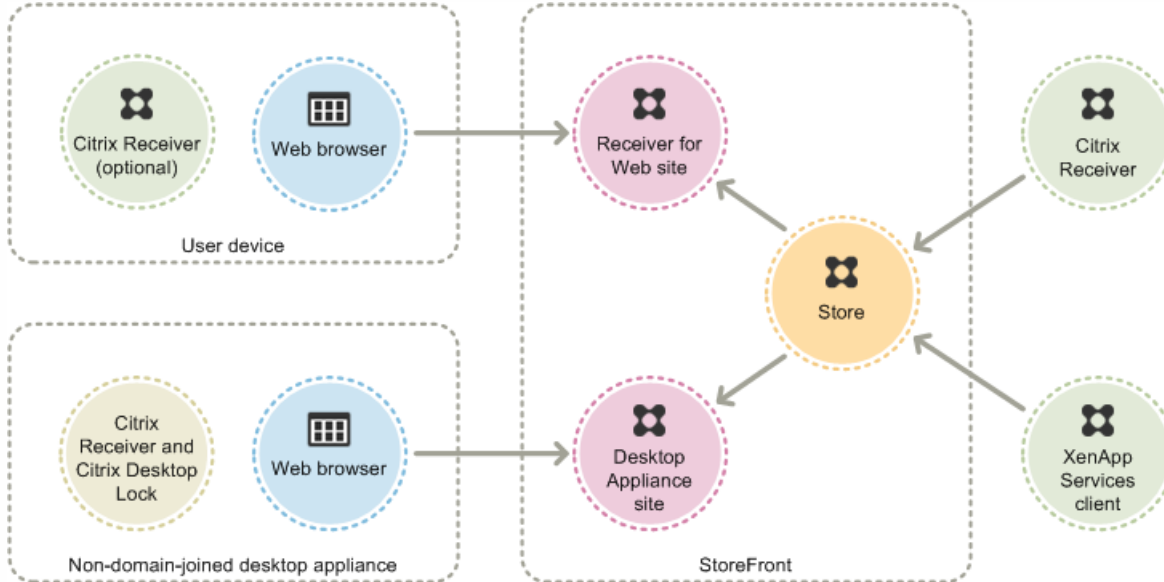
Options d'accès utilisateur

Jun 30, 2017

Quatre méthodes permettent aux utilisateurs d'accéder aux magasins StoreFront.

- **Citrix Receiver** : les utilisateurs disposant de versions compatibles de Citrix Receiver peuvent accéder aux magasins StoreFront depuis l'interface utilisateur de Citrix Receiver. L'accès aux magasins à partir de Citrix Receiver offre la meilleure expérience utilisateur et davantage de fonctionnalités.
- **Sites Citrix Receiver pour Web** : les utilisateurs dotés de navigateurs Web compatibles peuvent accéder aux magasins StoreFront en accédant aux sites Citrix Receiver pour Web. Par défaut, les utilisateurs doivent également disposer d'une version compatible de Citrix Receiver pour pouvoir accéder à leurs bureaux et applications. Toutefois, vous pouvez configurer des sites Citrix Receiver pour Web pour permettre aux utilisateurs dotés de navigateurs compatibles HTML5 d'accéder à leurs ressources sans installer Citrix Receiver. Lorsque vous créez un nouveau magasin, un site Citrix Receiver pour Web est créé pour le magasin par défaut.
- **Sites Desktop Appliance** : les utilisateurs équipés de boîtiers de bureau qui n'appartiennent pas à un domaine peuvent accéder à leurs bureaux via les navigateurs Web de leurs machines, qui sont configurés pour accéder à des sites Desktop Appliance en mode plein écran. Lorsque vous créez un nouveau magasin pour un déploiement XenDesktop à l'aide de Citrix Studio, un site Desktop Appliance est créé par défaut pour le magasin.
- **URL XenApp Services** : les utilisateurs équipés de boîtiers de bureau membres d'un domaine et de PC réaffectés qui exécutent Citrix Desktop Lock, ainsi que les utilisateurs disposant de clients Citrix plus anciens qui ne peuvent pas être mis à niveau, peuvent accéder aux magasins directement à l'aide de l'adresse URL XenApp Services du magasin. Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services est activée par défaut.

La figure illustre les différentes options permettant aux utilisateurs d'accéder aux magasins StoreFront :



Citrix Receiver

L'accès aux magasins à partir de l'interface utilisateur de Citrix Receiver offre la meilleure expérience utilisateur et davantage de fonctionnalités. Pour connaître les versions de Citrix Receiver qui peuvent être utilisées pour accéder aux magasins à l'aide de cette méthode, consultez la section [Configuration système requise](#).

Citrix Receiver utilise des adresses URL internes et externes en tant que points balises. En prenant contact avec ces points balises, Citrix Receiver peut déterminer si les utilisateurs sont connectés à des réseaux locaux ou publics. Lorsqu'un

utilisateur accède à un bureau ou une application, les informations d'emplacement sont transmises au serveur fournissant les ressources afin que les détails de connexion appropriés puissent être renvoyés à Citrix Receiver. Ceci permet à Citrix Receiver de s'assurer que les utilisateurs ne sont pas invités à ouvrir une nouvelle session lorsqu'ils accèdent à un bureau ou une application. Pour plus d'informations, veuillez consulter la section [Configurer des points balises](#).

Après l'installation, Citrix Receiver doit être configuré avec les détails de connexion aux magasins qui fournissent les bureaux et applications aux utilisateurs. Vous pouvez faciliter le processus de configuration pour vos utilisateurs en leur offrant les informations requises de l'une des manières suivantes.

Important : par défaut, Citrix Receiver requiert des connexions HTTPS pour les magasins. Si StoreFront n'est pas configuré pour le protocole HTTPS, les utilisateurs doivent effectuer des étapes de configuration supplémentaires pour utiliser les connexions HTTP. Citrix vous recommande de ne pas autoriser les connexions utilisateur non sécurisées à StoreFront dans un environnement de production. Pour de plus amples informations, référez-vous à la rubrique *Configuration et utilisation de Citrix Receiver pour Windows à l'aide de paramètres de ligne de commande* dans la documentation Citrix Receiver pour Windows.

Fichiers de provisioning

Vous pouvez fournir des fichiers de provisioning, aux utilisateurs, contenant des détails de connexion pour leurs magasins. Après l'installation de Citrix Receiver, les utilisateurs ouvrent le fichier .cr pour configurer automatiquement des comptes pour les magasins. Par défaut, les sites Citrix Receiver pour Web offrent aux utilisateurs un fichier de provisioning destiné au magasin pour lequel le site est configuré. Vous pouvez demander à vos utilisateurs d'accéder aux sites Receiver pour Web des magasins auxquels ils souhaitent accéder et télécharger les fichiers de provisioning à partir de ces sites. Éventuellement, pour un niveau de contrôle plus élevé, vous pouvez utiliser la console de gestion Citrix StoreFront pour générer des fichiers de provisioning contenant les détails de connexion à un ou plusieurs magasins. Vous pouvez distribuer ces fichiers après des utilisateurs appropriés. Pour de plus amples informations, reportez-vous à la section [Exporter des fichiers de provisioning de magasin pour des utilisateurs](#).

Adresses URL de configuration générées automatiquement

Pour les utilisateurs exécutant Mac OS, vous pouvez utiliser le générateur d'adresse URL de configuration Citrix Receiver pour Mac pour créer une adresse URL contenant les détails de connexion d'un magasin. Après l'installation de Citrix Receiver, les utilisateurs cliquent sur l'URL pour configurer un compte pour le magasin automatiquement. Entrez les détails de votre déploiement dans l'outil et générez une adresse URL que vous pouvez distribuer à vos utilisateurs.

Configuration manuelle

Les utilisateurs plus expérimentés peuvent créer de nouveaux comptes en entrant les adresses URL de magasins dans Citrix Receiver. Les utilisateurs distants qui accèdent à StoreFront via NetScaler Gateway 10.1 et Access Gateway 10 entrent l'adresse URL du boîtier. Citrix Receiver obtient les informations de configuration du compte requises lorsque la connexion est établie pour la première fois. Pour les connexions établies via Access Gateway 9.3, les utilisateurs ne peuvent pas créer de comptes manuellement et doivent utiliser l'une des autres méthodes ci-dessus. Pour de plus amples informations, veuillez consulter la documentation de Citrix Receiver.

Découverte de compte basée sur une adresse e-mail

Les utilisateurs qui installent Citrix Receiver sur un appareil pour la première fois peuvent créer des comptes en entrant leurs adresses e-mail, à condition qu'ils téléchargent Citrix Receiver à partir du site Web de Citrix ou d'une page de téléchargement Citrix Receiver hébergée au sein de votre réseau interne. Configurez des enregistrements de ressources de

localisation de l'emplacement du service (SRV) pour NetScaler Gateway ou StoreFront sur votre serveur DNS Microsoft Active Directory. Les utilisateurs n'ont pas à connaître les détails d'accès à leurs magasins, ils doivent seulement entrer leurs adresses e-mail lors de la configuration initiale de Citrix Receiver. Citrix Receiver contacte le serveur DNS pour le domaine spécifié dans l'adresse e-mail et obtient les détails que vous avez ajouté à l'enregistrement de ressources SRV. Les utilisateurs se voient alors présenter une liste de magasins auxquels ils peuvent accéder au travers de Citrix Receiver.

Configurer la découverte de compte basée sur une adresse e-mail

Configurez la découverte de compte basée sur une adresse e-mail pour permettre aux utilisateurs qui installent Citrix Receiver sur un appareil pour la première fois de configurer leurs comptes en entrant leurs adresses de messagerie. Dans la mesure où ils téléchargent Citrix Receiver à partir du site Web de Citrix où d'une page de téléchargement Citrix Receiver hébergée dans votre réseau interne, les utilisateurs n'ont pas besoin de connaître les détails d'accès à leurs magasins lorsqu'ils installent et configurent Citrix Receiver. La découverte de compte basée sur l'adresse e-mail est disponible si Citrix Receiver est téléchargé à partir d'un autre emplacement, tel qu'un site Receiver pour Web. Notez que les fichiers ReceiverWeb.exe ou ReceiverWeb.dmg téléchargés à partir de Citrix Receiver pour Web n'invitent pas les utilisateurs à configurer un magasin. Les utilisateurs peuvent toujours utiliser Ajouter un compte et entrer leur adresse e-mail.

Durant le processus de configuration initiale, Citrix Receiver invite les utilisateurs à entrer une adresse e-mail ou l'adresse URL d'un magasin. Lorsqu'un utilisateur entre une adresse e-mail, Citrix Receiver contacte le serveur DNS Microsoft Active Directory du domaine spécifié dans l'adresse e-mail pour obtenir une liste des magasins disponibles que l'utilisateur peut sélectionner.

Pour permettre à Citrix Receiver de localiser les magasins disponibles en fonction des adresses e-mail des utilisateurs, configurez des enregistrements de ressources de localisation de l'emplacement du service (SRV) pour NetScaler Gateway ou StoreFront sur votre serveur DNS. Vous pouvez également déployer StoreFront sur un serveur appelé « discoverReceiver.domaine », où domaine est le domaine contenant les comptes de messagerie de vos utilisateurs. Si aucun enregistrement SRV n'est détecté, Citrix Receiver recherche une machine appelée « discoverReceiver » afin d'identifier un serveur StoreFront.

Vous devez installer un certificat de serveur valide sur le boîtier Access Gateway ou le serveur StoreFront pour activer la découverte de compte par e-mail. La chaîne complète du certificat racine doit également être valide. Pour la meilleure expérience utilisateur possible, installez soit un certificat avec une entrée Objet ou Autre nom de l'objet de discoverReceiver.domaine, où domaine est le domaine contenant les comptes de messagerie de vos utilisateurs. Bien que vous puissiez utiliser un certificat générique pour le domaine contenant les comptes de messagerie de vos utilisateurs, vous devez d'abord vous assurer que le déploiement de tels certificats est autorisé par votre stratégie de sécurité d'entreprise. D'autres certificats pour le domaine contenant les comptes de courrier électronique de vos utilisateurs peuvent également être utilisés, mais les utilisateurs apercevront une boîte de dialogue d'avertissement de certificat lorsque Citrix Receiver se connecte d'abord au serveur StoreFront. La découverte de compte par e-mail ne peut pas être utilisée par d'autres identités de certificat.

Pour activer la découverte de compte par e-mail pour les utilisateurs se connectant depuis l'extérieur du réseau d'entreprise, vous devez également configurer NetScaler Gateway avec les détails de connexion à StoreFront. Pour plus d'informations, consultez la section [Connexion à StoreFront à l'aide de la découverte basée sur l'adresse e-mail](#).

Ajouter un enregistrement SRV à votre serveur DNS

1. Sur l'écran **Démarrer** de Windows, cliquez sur **Outils d'administration** et dans le dossier **Outils d'administration**, cliquez sur **DNS**.
2. Dans le panneau gauche du **Gestionnaire DNS**, sélectionnez votre domaine dans les zones de recherche inversées et

directes. Cliquez avec le bouton droit de la souris sur le domaine et sélectionnez **Nouveaux enregistrements**.

3. Dans la boîte de dialogue **Type d'enregistrement de ressource**, sélectionnez **Emplacement du service (SRV)** puis cliquez sur **Créer un enregistrement**.
4. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, entrez dans la zone **Service** la valeur d'hébergement **_citrixreceiver**.
5. Entrez dans la zone **Protocole** la valeur **_tcp**.
6. Dans la zone **Hôte offrant ce service**, spécifiez le nom de domaine complet (FQDN) et le port de votre boîtier Access Gateway (pour prendre en charge à la fois les utilisateurs locaux et distants) ou le serveur StoreFront (pour prendre en charge les utilisateurs du réseau local uniquement) au format *nomserveur.domaine:port*.
Si votre environnement comprend à la fois des serveurs DNS internes et externes, vous pouvez ajouter un enregistrement SRV spécifiant le nom de domaine complet du serveur StoreFront sur votre serveur DNS interne et un autre enregistrement sur votre serveur externe spécifiant le nom de domaine complet de NetScaler Gateway. Avec cette configuration, les utilisateurs du réseau local se voient offrir les détails StoreFront, tandis que les utilisateurs distants reçoivent des informations de connexion NetScaler Gateway.
7. Si vous avez configuré un enregistrement SRV pour votre boîtier NetScaler Gateway, ajoutez les détails de connexion StoreFront à NetScaler Gateway dans un profil de session ou un paramètre global.

Sites Citrix Receiver pour Web

Les utilisateurs dotés de navigateurs Web compatibles peuvent accéder aux magasins StoreFront en accédant aux sites Citrix Receiver pour Web. Lorsque vous créez un nouveau magasin, un site Citrix Receiver pour Web est automatiquement créé pour le magasin. La configuration par défaut des sites Citrix Receiver pour Web nécessite que les utilisateurs installent une version compatible de Citrix Receiver pour accéder à leurs bureaux et applications. Pour de plus amples informations sur les combinaisons Citrix Receiver et navigateur Web qui peuvent être utilisées pour accéder aux sites Citrix Receiver pour Web, consultez la section [Configuration requise pour la machine utilisateur](#).

Par défaut, lorsqu'un utilisateur accède à un site Citrix Receiver pour Web depuis un ordinateur exécutant Windows ou Mac OS X, le site tente de déterminer si Citrix Receiver est installé sur la machine de l'utilisateur. Si Citrix Receiver ne peut être détecté, l'utilisateur est invité à télécharger et installer la version appropriée de Citrix Receiver pour sa plate-forme. L'emplacement de téléchargement par défaut est le site Web de Citrix, mais vous pouvez également copier les fichiers d'installation sur le serveur StoreFront et fournir ces fichiers locaux aux utilisateurs. Le stockage des fichiers d'installation de Citrix Receiver localement vous permet de configurer le site afin d'offrir aux utilisateurs disposant de clients plus anciens la possibilité de mettre à niveau vers la version disponible sur le serveur. Pour de plus amples informations sur la configuration du déploiement de Citrix Receiver pour Windows et Citrix Receiver pour Mac, consultez la section [Configurer des sites Citrix Receiver pour Web](#).

Citrix Receiver pour HTML5

Citrix Receiver pour HTML5 est un composant de StoreFront qui est intégré par défaut aux sites Citrix Receiver pour Web. Vous pouvez activer Citrix Receiver pour HTML5 sur vos sites Citrix Receiver pour Web afin que les utilisateurs qui ne peuvent pas installer Citrix Receiver puissent quand même accéder à leurs ressources. Citrix Receiver pour HTML5 permet aux utilisateurs d'accéder aux bureaux et applications directement depuis des navigateurs Web compatibles HTML5 sans avoir à installer Citrix Receiver. Lorsqu'un site est créé, Citrix Receiver pour HTML5 est désactivé par défaut. Pour plus d'informations sur l'activation de Citrix Receiver pour HTML5, consultez [citrix-receiver-download-page-template.html](#).

Pour accéder à leurs bureaux et applications à l'aide de Citrix Receiver pour HTML5, les utilisateurs doivent accéder au site Citrix Receiver pour Web avec un navigateur compatible HTML5. Pour de plus amples informations sur les systèmes d'exploitation et les navigateurs Web qui peuvent être utilisés avec Citrix Receiver pour HTML5, consultez la section

Configuration requise pour la machine utilisateur.

Citrix Receiver pour HTML5 peut être utilisé par les utilisateurs sur le réseau interne et les utilisateurs distants se connectant via NetScaler Gateway. Pour les connexions depuis le réseau interne, Citrix Receiver pour HTML5 prend uniquement en charge l'accès aux bureaux et applications fournis par un sous-ensemble des produits pris en charge par les sites Citrix Receiver pour Web. Les utilisateurs qui se connectent via NetScaler Gateway peuvent accéder aux ressources fournies par une large gamme de produits si vous choisissez Citrix Receiver pour HTML5 comme option lors de la configuration de StoreFront. Des versions spécifiques de NetScaler Gateway sont requises pour l'utilisation avec Citrix Receiver pour HTML5. Pour plus d'informations, veuillez consulter la section [Configuration requise pour l'infrastructure](#).

Pour les utilisateurs du réseau interne, l'accès via Citrix Receiver pour HTML5 aux ressources fournies par XenDesktop et XenApp est désactivé par défaut. Pour activer l'accès local aux bureaux et applications à l'aide de Citrix Receiver pour HTML5, vous devez activer la stratégie Connexions WebSockets ICA sur vos serveurs XenDesktop et XenApp. Assurez-vous que vos pare-feu et autres périphériques réseau autorisent l'accès au port Citrix Receiver pour HTML5 spécifié dans la stratégie. Pour plus d'informations, veuillez consulter la section [Paramètres de stratégie WebSockets](#).

Par défaut, Citrix Receiver pour HTML5 démarre les bureaux et applications dans un nouvel onglet de navigateur. Toutefois, lorsque les utilisateurs démarrent des ressources à partir de raccourcis à l'aide de Citrix Receiver pour HTML5, le bureau ou l'application remplace le site Citrix Receiver pour Web dans l'onglet de navigateur existant plutôt que d'apparaître dans un nouvel onglet. Vous pouvez configurer Citrix Receiver pour HTML5 afin que les ressources soient toujours démarrées dans le même onglet que le site Receiver pour Web. Pour de plus amples informations, consultez la section [Configurer l'utilisation des onglets de navigateur par Citrix Receiver pour HTML5](#).

Raccourcis vers les ressources

Vous pouvez générer des URL qui fournissent un accès aux bureaux et applications disponibles via les sites Citrix Receiver pour Web. Intégrez ces liens aux sites Web hébergés sur le réseau interne pour fournir aux utilisateurs un accès rapide aux ressources. Les utilisateurs cliquent sur un lien et sont redirigés vers le site Receiver pour Web, où ils ouvrent une session si ce n'est pas déjà fait. Le site Citrix Receiver pour Web démarre automatiquement la ressource. Dans le cas des applications, les utilisateurs sont également abonnés aux applications s'ils ne se sont pas abonnés précédemment. Pour de plus amples informations sur la création des raccourcis vers les ressources, consultez la section [Configurer des sites Citrix Receiver pour Web](#).

Comme avec tous les bureaux et applications accessibles à partir des sites Citrix Receiver pour Web, les utilisateurs doivent avoir installé Citrix Receiver ou être en mesure d'utiliser Citrix Receiver pour HTML5 pour accéder aux ressources via les raccourcis. La méthode utilisée par un site Citrix Receiver pour Web dépend de la configuration du site, si Citrix Receiver peut être détecté sur les machines des utilisateurs et si un navigateur compatible HTML5 est utilisé. Pour des raisons de sécurité, les utilisateurs d'Internet Explorer peuvent être invités à confirmer qu'ils souhaitent démarrer les ressources accessibles via les raccourcis. Demandez à vos utilisateurs d'ajouter le site Receiver pour Web à la zone Intranet local ou Sites de confiance dans Internet Explorer pour éviter cette étape supplémentaire. Par défaut, le contrôle de l'espace de travail et le démarrage automatique des bureaux sont désactivés lorsque les utilisateurs accèdent à des sites Citrix Receiver pour Web via les raccourcis.

Lorsque vous créez un raccourci d'application, assurez-vous qu'aucune autre application disponible sur le site Citrix Receiver pour Web ne porte le même nom. Les raccourcis ne peuvent pas faire la distinction entre plusieurs instances d'une application avec le même nom. De même, si vous mettez à disposition plusieurs instances d'un bureau à partir d'un groupe de bureaux unique disponible depuis le site Citrix Receiver pour Web, vous ne pouvez pas créer de raccourcis distincts pour chaque instance. Les raccourcis ne peuvent pas transmettre les paramètres de ligne de commande aux applications.

Pour créer des raccourcis d'application, configurez StoreFront avec les adresses URL des sites Web internes qui hébergeront les raccourcis. Lorsqu'un utilisateur clique sur un raccourci d'application sur un site Web, StoreFront compare le site Web avec la liste des adresses URL que vous avez entrées pour s'assurer que la demande provient d'un site Web approuvé. Toutefois, pour les utilisateurs se connectant via NetScaler Gateway, les sites Web qui hébergent des raccourcis ne sont pas validés car les adresses URL ne sont pas transmises à StoreFront. Pour vous assurer que les utilisateurs distants peuvent uniquement accéder aux raccourcis d'applications sur des sites Web internes approuvés, configurez NetScaler Gateway afin de restreindre l'accès des utilisateurs uniquement à ces sites spécifiques. Consultez l'article <http://support.citrix.com/article/CTX123610> pour de plus amples informations.

Personnaliser vos sites

Les sites Citrix Receiver pour Web offrent un mécanisme qui permet de personnaliser l'interface utilisateur. Vous pouvez personnaliser les chaînes, la feuille de style en cascade (.css) et les fichiers JavaScript. Vous pouvez également ajouter un écran avant ou après l'ouverture de session ainsi que des packs de langue.

Remarques importantes

Les utilisateurs qui accèdent à des magasins via un site Citrix Receiver pour Web bénéficient des nombreuses fonctionnalités disponibles avec l'accès aux magasins via Citrix Receiver, telles que la synchronisation des applications. Lorsque vous déterminez si vous souhaitez utiliser des sites Citrix Receiver pour Web pour permettre aux utilisateurs d'accéder à vos magasins, tenez compte des restrictions suivantes.

- Seul un magasin unique est accessible via chaque site Citrix Receiver pour Web.
- Les sites Citrix Receiver pour Web ne peuvent initier des connexions VPN SSL. Les utilisateurs qui ouvrent une session via NetScaler Gateway sans connexion VPN ne peuvent pas accéder à des applications Web pour lesquelles App Controller exige qu'une connexion VPN soit utilisée.
- Les applications auxquelles les utilisateurs sont abonnés ne sont pas disponibles dans l'écran Démarrer de Windows lorsqu'ils accèdent à un magasin via un site Citrix Receiver pour Web.
- L'association des types de fichiers entre les documents locaux et les applications hébergées accessibles par le biais des sites Citrix Receiver pour Web n'est pas disponible.
- Les applications en mode hors connexion ne sont pas accessibles via les sites Citrix Receiver pour Web.
- Les sites Citrix Receiver pour Web ne prennent pas en charge les produits Citrix Online intégrés aux magasins. Les produits Citrix Online doivent être mis à disposition avec App Controller ou sous forme d'applications hébergées pour permettre l'accès via les sites Citrix Receiver pour Web.
- Citrix Receiver pour HTML5 peut être utilisé sur des connexions HTTPS si le VDA est XenApp 7.6 ou XenDesktop 7.6 sur lequel SSL est activé ou si l'utilisateur se connecte à l'aide de NetScaler Gateway.
- Pour utiliser Citrix Receiver pour HTML5 avec Mozilla Firefox via des connexions HTTPS, les utilisateurs doivent taper about:config dans la barre d'adresses de Firefox et définir la préférence network.websocket.allowInsecureFromHTTPS sur true.

Sites Desktop Appliance

Les utilisateurs équipés de boîtiers de bureau qui n'appartiennent pas à un domaine peuvent accéder à leurs bureaux via des sites Desktop Appliance. Dans ce contexte, les machines n'appartenant pas à un domaine sont des machines qui ne sont pas membres d'un domaine dans la forêt Active Directory contenant les serveurs StoreFront.

Lorsque vous créez un nouveau magasin pour un déploiement XenDesktop à l'aide de Citrix Studio, un site Desktop Appliance est créé par défaut pour le magasin. Les sites Desktop Appliance sont uniquement créés par défaut lorsque

StoreFront est installé et configuré dans le cadre d'une installation XenDesktop. Vous pouvez créer des sites Desktop Appliance manuellement à l'aide de commandes Windows PowerShell. Pour plus d'informations, consultez la section [Configurer des sites Desktop Appliance](#).

Les sites Desktop Appliance offrent une expérience utilisateur similaire à l'ouverture d'une session sur un bureau local. Les navigateurs Web qui équipent les boîtiers de bureau sont configurés pour démarrer en mode plein écran et afficher l'écran d'ouverture de session pour un site Desktop Appliance. Lorsqu'un utilisateur ouvre une session sur un site, par défaut, le premier bureau (dans l'ordre alphabétique) disponible pour l'utilisateur dans le magasin pour lequel le site est configuré démarre automatiquement. Si vous fournissez aux utilisateurs un accès à plusieurs bureaux dans un magasin, vous pouvez configurer le site Desktop Appliance pour afficher les bureaux disponibles de manière à ce que les utilisateurs puissent choisir celui auquel ils souhaitent accéder. Pour plus d'informations, consultez la section [Configurer des sites Desktop Appliance](#).

Lorsque le bureau d'un utilisateur démarre, il est affiché en mode plein écran et masque le navigateur Web. La session utilisateur au site Desktop Appliance est automatiquement fermée. Lorsque l'utilisateur ferme sa session sur le bureau, le navigateur Web qui affiche l'écran d'ouverture de session du site Desktop Appliance est de nouveau visible. Un message s'affiche lorsqu'un bureau est démarré. Ce dernier contient un lien qui permet à l'utilisateur de redémarrer le bureau s'il n'est pas accessible. Pour activer cette fonctionnalité, vous devez configurer le groupe de mise à disposition pour autoriser les utilisateurs à redémarrer leurs bureaux. Pour de plus amples informations, consultez la section [Groupes de mise à disposition](#).

Pour fournir l'accès aux bureaux, une version compatible de Citrix Receiver est requise sur le boîtier de bureau. En général, les fournisseurs de boîtiers compatibles avec XenDesktop intègrent Citrix Receiver dans leurs produits. Pour les boîtiers Windows, Citrix Desktop Lock doit également être installé et configuré avec l'adresse URL de votre site Desktop Appliance. Si Internet Explorer est utilisé, le site Desktop Appliance doit être ajouté à la zone Intranet local ou Sites de confiance. Pour de plus amples informations sur Citrix Desktop Lock, veuillez consulter la section [Empêcher l'utilisateur d'accéder au bureau local](#).

Remarques importantes

Les sites Desktop Appliance sont conçus pour les utilisateurs locaux du réseau interne qui accèdent aux bureaux à partir de boîtiers de bureau qui n'appartiennent pas au domaine. Lorsque vous déterminez si vous souhaitez utiliser des sites Desktop Appliance pour permettre aux utilisateurs d'accéder à vos magasins, tenez compte des restrictions suivantes.

- Si vous prévoyez de déployer des boîtiers de bureau qui appartiennent au domaine et des PC réaffectés, ne les configurez pas pour accéder aux magasins via des sites Desktop Appliance. Bien que vous puissiez configurer Citrix Receiver avec l'adresse URL du site XenApp Services pour le magasin, nous vous recommandons d'utiliser la nouvelle version de Desktop Lock aussi bien dans les environnements joints à un domaine que ceux non joints à un domaine. Pour de plus amples informations, consultez la section [Citrix Receiver Desktop Lock](#).
- Les sites Desktop Appliance ne prennent pas en charge les connexions des utilisateurs distants qui se trouvent en dehors du réseau de l'entreprise. Les utilisateurs qui ouvrent une session sur NetScaler Gateway ne peuvent pas accéder à des sites Desktop Appliance.

Adresses URL XenApp Services

Les utilisateurs équipés de clients Citrix plus anciens qui ne peuvent pas être mis à niveau peuvent accéder aux magasins en configurant leurs clients avec l'adresse URL du site XenApp Services pour un magasin. Vous pouvez également activer l'accès à vos magasins via les adresses URL XenApp Services à partir de boîtiers de bureau appartenant à un domaine et de PC réaffectés qui exécutent Citrix Desktop Lock. Dans ce contexte, les machines appartenant à un domaine sont des machines qui sont membres d'un domaine dans la forêt Active Directory contenant les serveurs StoreFront.

StoreFront prend en charge l'authentification pass-through avec des cartes de proximité via Citrix Receiver à des adresses URL XenApp Services. Les produits des partenaires Citrix Ready utilisent Citrix Fast Connect API pour simplifier les ouvertures de session des utilisateurs via Citrix Receiver pour Windows afin de se connecter aux magasins à l'aide de l'adresse URL d'un site XenApp Services. Les utilisateurs s'authentifient sur des stations de travail à l'aide de cartes de proximité et sont rapidement connectés aux bureaux et applications fournis par XenDesktop et XenApp. Pour plus d'informations, consultez la documentation [Citrix Receiver pour Windows](#) la plus récente.

Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services du magasin est activée par défaut. L'adresse URL XenApp Services d'un magasin s'affiche au format `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`, où `serveraddress` est le nom de domaine complet du serveur ou de l'environnement d'équilibrage de charge de votre déploiement StoreFront et `storename` le nom spécifié pour le magasin lors de sa création. Cela permet aux Citrix Receiver qui peuvent uniquement utiliser le protocole PNAgent de se connecter à StoreFront. Pour les clients qui peuvent être utilisés pour accéder aux magasins via des adresses URL XenApp Services, consultez la section [Configuration requise pour la machine utilisateur](#).

Remarques importantes

Les adresses URL XenApp Services sont conçues pour prendre en charge les utilisateurs qui ne peuvent pas mettre à niveau vers Citrix Receiver et pour les scénarios dans lesquels d'autres méthodes d'accès ne sont pas disponibles. Lorsque vous déterminez si vous souhaitez utiliser des adresses URL XenApp Services pour permettre aux utilisateurs d'accéder à vos magasins, tenez compte des restrictions suivantes.

- Vous ne pouvez pas modifier l'adresse URL du site XenApp Services pour un magasin.
- Vous ne pouvez pas modifier les paramètres de l'URL XenApp Services en modifiant le fichier de configuration, `config.xml`.
- Les adresses URL XenApp Services prennent en charge l'authentification explicite, l'authentification pass-through au domaine, l'authentification par carte à puce et l'authentification pass-through avec carte à puce. L'authentification explicite est activée par défaut. Une seule méthode d'authentification peut être configurée pour chaque adresse URL XenApp Services et une seule URL est disponible par magasin. Si vous devez activer plusieurs méthodes d'authentification, vous devez créer des magasins distincts, chacun avec une adresse URL XenApp Services, pour chaque méthode d'authentification. Les utilisateurs doivent ensuite se connecter au magasin approprié à leur méthode d'authentification. Pour plus d'informations, consultez la section [Authentification XML](#).
- Le contrôle de l'espace de travail est activé par défaut pour les adresses URL XenApp Services et ne peut pas être configuré ou désactivé.
- Les requêtes des utilisateurs pour modifier leur mot de passe sont directement transférées vers le contrôleur de domaine par le biais des serveurs XenDesktop et XenApp fournissant des bureaux et des applications au magasin, en contournant le service d'authentification de StoreFront.

Authentification utilisateur

Jun 30, 2017

StoreFront prend en charge plusieurs méthodes d'authentification pour les utilisateurs qui accèdent à des magasins, mais toutes ne sont pas disponibles selon la méthode d'accès et l'emplacement réseau des utilisateurs. Pour des raisons de sécurité, certaines méthodes d'authentification sont désactivées par défaut lorsque vous créez votre premier magasin. Pour plus d'informations sur les méthodes d'activation et de désactivation de l'authentification utilisateur, consultez la section [Créer et configurer le service d'authentification](#).

Nom d'utilisateur et mot de passe

Les utilisateurs saisissent leurs informations d'identification et sont authentifiés lorsqu'ils accèdent à leurs magasins. L'authentification explicite est activée par défaut. Toutes les méthodes d'accès utilisateur prennent en charge l'authentification explicite.

Lorsqu'un utilisateur utilise NetScaler Gateway pour accéder à Citrix Receiver pour Web, NetScaler Gateway gère la modification du nom de connexion et du mot de passe à l'expiration. Les utilisateurs peuvent modifier le mot de passe avec l'interface de Citrix Receiver pour Web. Après la modification d'un mot de passe, la session NetScaler Gateway prend fin et l'utilisateur doit de nouveau ouvrir une session. Les utilisateurs de Citrix Receiver pour Linux peuvent uniquement modifier les mots de passe qui ont expiré.

Authentification SAML

Les utilisateurs s'authentifient auprès d'un fournisseur d'identité SAML et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. StoreFront peut prendre en charge l'authentification SAML directement depuis le réseau d'entreprise, sans avoir besoin de passer par NetScaler.

SAML (Security Assertion Markup Language) est une norme ouverte utilisée par les produits d'identité et d'authentification tels que Microsoft ADFS (Active Directory Federation Services). Grâce à l'intégration de l'authentification SAML via StoreFront, les administrateurs peuvent autoriser les utilisateurs à, par exemple, se connecter une seule fois à leur réseau d'entreprise afin d'accéder à leurs applications publiées en SSO.

Configuration requise :

- Implémentation du [Service d'authentification fédérée de Citrix](#).
- Fournisseurs d'identité (IdP) compatibles avec SAML 2.0 :
 - Microsoft ADFS v4.0 (Windows Server 2016) à l'aide de liaisons SAML uniquement (et non des liaisons WS-Federation). Pour plus d'informations, consultez les articles [Microsoft AD FS 2016 Deployment](#) et [Microsoft AD 2016 FS Operations](#).
 - Microsoft ADFS v3.0 (Windows Server 2012 R2)
 - Microsoft ADFS v2.0 (Windows Server 2008 R2)
 - NetScaler Gateway (configuré en tant qu'IdP)
- Configurez l'authentification SAML dans StoreFront à l'aide de la console de gestion StoreFront dans un nouveau déploiement (Veuillez consulter la section [Créer un nouveau déploiement](#)), ou dans un déploiement existant (Veuillez consulter la section [Configurer le service d'authentification](#)). Vous pouvez également configurer l'authentification SAML à l'aide d'applets de commande PowerShell, consultez la section [SDK StoreFront](#) .
- Citrix Receiver pour Windows (4.6 et versions supérieures) ou Citrix Receiver pour Web.

L'utilisation de l'authentification SAML avec NetScaler est actuellement prise en charge avec les sites Receiver pour Web.

Authentification pass-through au domaine

Les utilisateurs s'authentifient sur leurs ordinateurs Windows membres d'un domaine et leurs informations d'identification sont utilisées pour ouvrir une session automatiquement lorsqu'ils accèdent à leurs magasins. Lorsque vous installez StoreFront, l'authentification pass-through au domaine est désactivée par défaut. L'authentification pass-through au domaine peut être activée pour les utilisateurs se connectant à des magasins via Citrix Receiver et des adresses URL XenApp Services. Les sites Citrix Receiver pour Web prennent en charge l'authentification pass-through au domaine uniquement pour Internet Explorer. L'activation de l'authentification pass-through au domaine dans le nœud du site Citrix Receiver pour Web dans la console d'administration requiert que vous configuriez SSON sur Citrix Receiver pour Windows. Citrix Receiver pour HTML5 ne prend pas en charge l'authentification pass-through au domaine. Pour utiliser l'authentification pass-through au domaine, les utilisateurs requièrent Citrix Receiver pour Windows ou Online Plug-in pour Windows. L'authentification pass-through doit être activée lorsque Citrix Receiver pour Windows ou Online Plug-in pour Windows est installé sur les machines des utilisateurs.

Authentification pass-through via NetScaler Gateway

Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. L'authentification pass-through via NetScaler Gateway est activée par défaut lorsque vous configurez l'accès distant à un magasin pour la première fois. Les utilisateurs peuvent se connecter via NetScaler Gateway aux magasins via Citrix Receiver ou des sites Citrix Receiver pour Web. Les sites Desktop Appliance ne prennent pas en charge les connexions via NetScaler Gateway. Pour plus d'informations sur la configuration de StoreFront pour NetScaler Gateway, veuillez consulter la section [Ajouter une connexion NetScaler Gateway](#).

StoreFront prend en charge l'authentification pass-through avec les méthodes d'authentification NetScaler Gateway suivantes.

- **Jeton de sécurité.** Les utilisateurs ouvrent une session sur NetScaler Gateway à l'aide de codes secrets provenant des codes de jeton générés par les jetons de sécurité combinés, dans certains cas, avec des numéros d'identification personnels. Si vous activez l'authentification pass-through par jeton de sécurité uniquement, assurez-vous que les ressources que vous mettez à disposition ne requièrent pas d'authentification supplémentaire ou d'autres méthodes d'authentification, telles que les informations d'identification de domaine Microsoft Active Directory.
- **Domaine et jeton de sécurité.** Les utilisateurs qui ouvrent une session sur NetScaler Gateway sont invités à entrer leurs informations d'identification de domaine et passcodes de jeton de sécurité.
- **Certificat client.** Les utilisateurs ouvrent une session sur NetScaler Gateway et sont authentifiés en fonction des attributs du certificat client présenté à NetScaler Gateway. Configurez l'authentification du certificat client pour permettre aux utilisateurs d'ouvrir une session sur NetScaler Gateway à l'aide de cartes à puce. L'authentification du certificat client peut également être utilisée avec d'autres types d'authentification afin de fournir une authentification double.

StoreFront utilise le service d'authentification de NetScaler Gateway pour fournir une authentification pass-through aux utilisateurs distants, afin qu'ils n'aient besoin de saisir leurs identifiants de connexion qu'une seule fois. Toutefois, par défaut, l'authentification pass-through est activée uniquement pour les utilisateurs ouvrant une session sur NetScaler Gateway avec un mot de passe. Pour configurer l'authentification pass-through via NetScaler Gateway à StoreFront pour les utilisateurs de carte à puce, déléguez la validation des informations d'identification à NetScaler Gateway. Pour plus d'informations, consultez [Créer et configurer le service d'authentification](#).

Les utilisateurs peuvent se connecter aux magasins dans Citrix Receiver avec l'authentification pass-through via un tunnel VPN SSL à l'aide de NetScaler Gateway Plug-in. Les utilisateurs distants qui ne peuvent pas installer NetScaler Gateway Plug-in peuvent utiliser un accès sans client pour se connecter aux magasins dans Citrix Receiver grâce à l'authentification

pass-through. Pour utiliser l'accès sans client pour se connecter aux magasins, les utilisateurs ont besoin d'une version de Citrix Receiver qui prend en charge l'accès sans client.

De plus, vous pouvez activer l'accès sans client avec l'authentification pass-through vers les sites Citrix Receiver pour Web. Pour ce faire, configurez NetScaler Gateway pour agir en tant que proxy distant sécurisé. Les utilisateurs ouvrent une session sur NetScaler Gateway directement et utilisent le site Citrix Receiver pour Web pour accéder à leurs applications sans avoir à s'authentifier de nouveau.

Les utilisateurs se connectant à l'aide d'un accès sans client aux ressources App Controller peuvent uniquement accéder des applications SaaS (software-as-a-service) externes. Pour accéder à des applications Web internes, les utilisateurs distants doivent utiliser NetScaler Gateway Plug-in.

Si vous configurez une authentification double à NetScaler Gateway pour les utilisateurs distants qui accèdent à des magasins dans Citrix Receiver, vous devez créer deux stratégies d'authentification sur NetScaler Gateway. Configurez RADIUS (Remote Authentication Dial-In User Service) en tant que méthode d'authentification principale et LDAP (Lightweight Directory Access Protocol) en tant que méthode secondaire. Modifiez l'index des informations d'identification afin d'utiliser la méthode d'authentification secondaire dans le profil de session afin que les informations d'identification LDAP soient transmises à StoreFront. Lorsque vous ajoutez le boîtier NetScaler Gateway à votre configuration StoreFront, définissez Type d'ouverture de session sur Domaine et jeton de sécurité. Pour de plus amples informations, veuillez consulter l'article <http://support.citrix.com/article/CTX125364>.

Pour activer l'authentification multidomaine via NetScaler Gateway à StoreFront, définissez SSO Name Attribute sur userPrincipalName dans la stratégie d'authentification LDAP NetScaler Gateway pour chaque domaine. Vous pouvez demander aux utilisateurs de spécifier un domaine sur la page d'ouverture de session de NetScaler Gateway de façon à ce que la stratégie LDAP appropriée à utiliser puisse être déterminée. Lorsque vous configurez les profils de session NetScaler Gateway pour les connexions à StoreFront, ne spécifiez pas de domaine à authentification pass-through. Vous devez configurer des relations d'approbation entre chaque domaine. Assurez-vous d'autoriser les utilisateurs à ouvrir une session à StoreFront à partir de n'importe quel domaine en prenant soin de ne pas limiter l'accès uniquement à des domaines approuvés de façon explicite.

Lorsque cela est pris en charge par votre déploiement NetScaler Gateway, vous pouvez utiliser SmartAccess pour contrôler l'accès utilisateur aux ressources XenDesktop et XenApp sur la base de stratégies de session NetScaler Gateway. Pour plus d'informations sur SmartAccess, consultez [How SmartAccess works for XenApp and XenDesktop](#).

Cartes à puce

Les utilisateurs doivent s'authentifier à l'aide de cartes à puce et de codes PIN lorsqu'ils accèdent à leurs magasins. Lorsque vous installez StoreFront, l'authentification par carte à puce est désactivée par défaut. L'authentification par carte à puce peut être activée pour les utilisateurs se connectant à des magasins via Citrix Receiver, Receiver pour Web, des sites Desktop Appliance et des adresses URL XenApp Services.

Utilisez l'authentification par carte à puce pour simplifier le processus d'ouverture de session pour vos utilisateurs tout en améliorant la sécurité de l'accès utilisateur dans votre infrastructure. L'accès au réseau d'entreprise interne est protégé par une authentification à deux facteurs basée sur certificat à l'aide d'une infrastructure à clé publique. Les clés privées sont protégées par des contrôles matériels et ne quittent jamais la carte à puce. Vos utilisateurs bénéficient d'un accès à leurs bureaux et applications à partir d'une large gamme de périphériques d'entreprise à l'aide de leurs cartes à puce et codes PIN.

Vous pouvez utiliser des cartes à puce pour l'authentification utilisateur via StoreFront aux bureaux et applications fournis par XenDesktop et XenApp. Les utilisateurs de carte à puce qui ouvrent une session sur StoreFront peuvent également accéder aux applications fournies par App Controller. Toutefois, les utilisateurs doivent s'authentifier à nouveau pour

accéder aux applications Web App Controller qui utilisent l'authentification du certificat client.

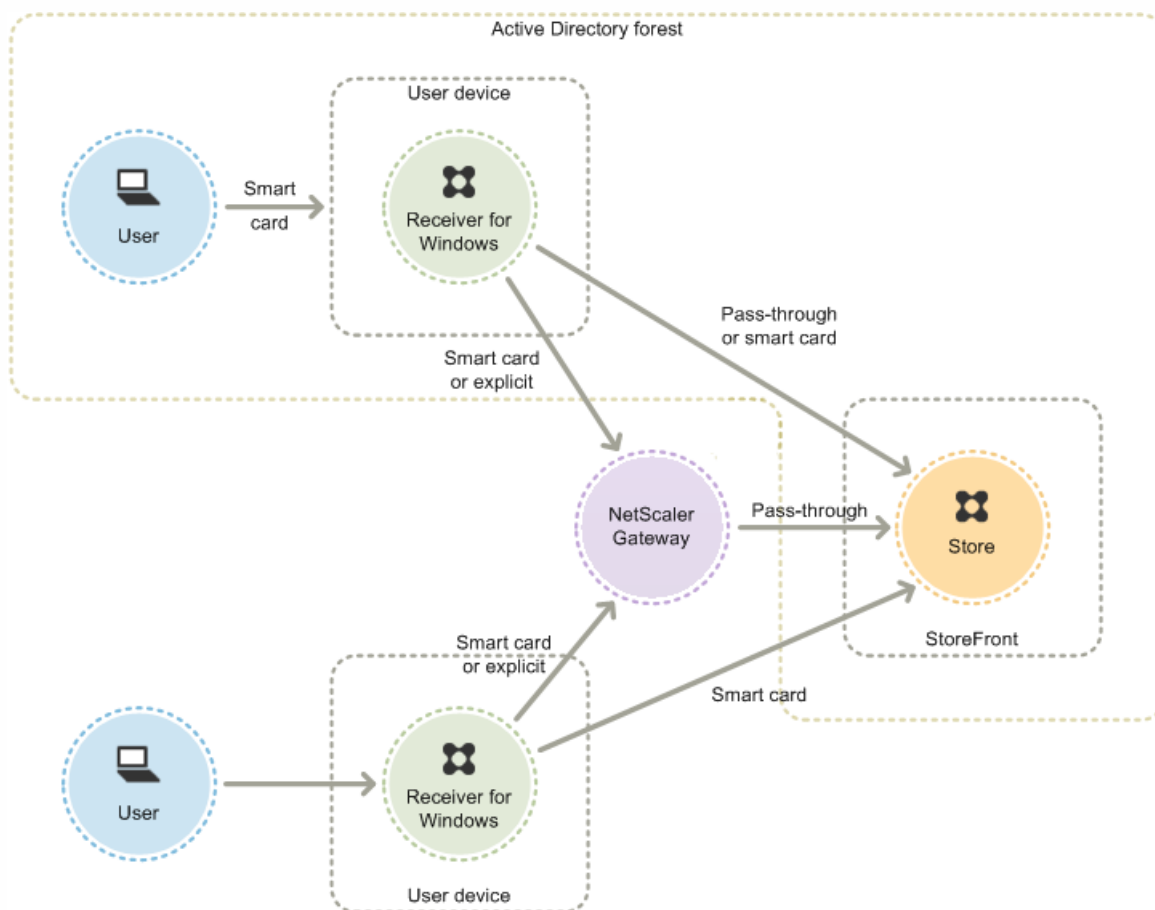
Pour activer l'authentification par carte à puce, les comptes des utilisateurs doivent être configurés au sein du domaine Microsoft Active Directory contenant les serveurs StoreFront ou au sein d'un domaine doté d'une relation d'approbation bidirectionnelle directe avec le domaine du serveur StoreFront. Les déploiements contenant de multiples forêts impliquant des approbations bidirectionnelles sont pris en charge.

La configuration de l'authentification par carte à puce avec StoreFront dépend des machines utilisateur, des clients installés, et de l'appartenance des machines à un domaine. Dans ce contexte, les machines appartenant à un domaine sont des machines qui sont membres d'un domaine dans la forêt Active Directory contenant les serveurs StoreFront.

Utiliser des cartes à puce avec Citrix Receiver pour Windows

Les utilisateurs équipés de machines exécutant Citrix Receiver pour Windows peuvent s'authentifier à l'aide de cartes à puce, soit directement, soit via NetScaler Gateway. Il est possible d'utiliser des machines appartenant ou non à un domaine, mais l'expérience utilisateur sera légèrement différente.

L'illustration affiche les options pour l'authentification par carte à puce via Citrix Receiver pour Windows.



Pour les utilisateurs locaux dotés de machines appartenant au domaine, vous pouvez configurer l'authentification par carte à puce de manière à ce que les utilisateurs ne soient invités à entrer leurs informations d'identification qu'une seule fois. Les utilisateurs ouvrent une session sur leurs machines à l'aide de leurs cartes à puces et codes PIN, et ne sont pas invités à entrer de nouveau leur code PIN lorsque la configuration appropriée est en place. Ils sont authentifiés de manière silencieuse auprès de StoreFront et de même lors de l'accès à leurs bureaux et applications. Pour ce faire, vous devez

configurer Citrix Receiver pour Windows pour l'authentification pass-through et activer l'authentification pass-through au domaine à StoreFront.

Les utilisateurs ouvrent une session sur leurs machines et s'authentifient auprès de Citrix Receiver pour Windows à l'aide de leur code PIN. Ils ne sont plus tenus d'entrer leur code PIN lorsqu'ils démarrent des applications et des bureaux

Étant donné que les utilisateurs de machines n'appartenant pas à un domaine ouvrent une session sur Citrix Receiver pour Windows directement, vous pouvez autoriser les utilisateurs à revenir à l'authentification explicite. Si vous configurez l'authentification par carte à puce et explicite, les utilisateurs sont initialement invités à ouvrir une session à l'aide de leurs cartes à puce et codes PIN mais ont la possibilité de sélectionner l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce.

Les utilisateurs qui se connectent via NetScaler Gateway doivent ouvrir une session à l'aide de leurs cartes à puce et codes PIN aux moins deux fois pour accéder à leurs bureaux et applications. Cela s'applique aussi bien aux machines appartenant à un domaine qu'à celles n'appartenant pas à un domaine. Les utilisateurs s'authentifient à l'aide de leurs cartes à puce et codes PIN, et lorsque la configuration appropriée est appliquée, ils ne sont invités à entrer que leur code PIN pour accéder à leurs bureaux et applications. Pour ce faire, vous devez activer l'authentification pass-through via NetScaler Gateway à StoreFront et déléguer la validation des informations d'identification à NetScaler Gateway. Créez ensuite un serveur virtuel NetScaler Gateway supplémentaire par le biais duquel router les connexions utilisateur vers les ressources. Pour ce qui est des machines n'appartenant pas à un domaine, vous devez également configurer Citrix Receiver pour Windows pour l'authentification pass-through.

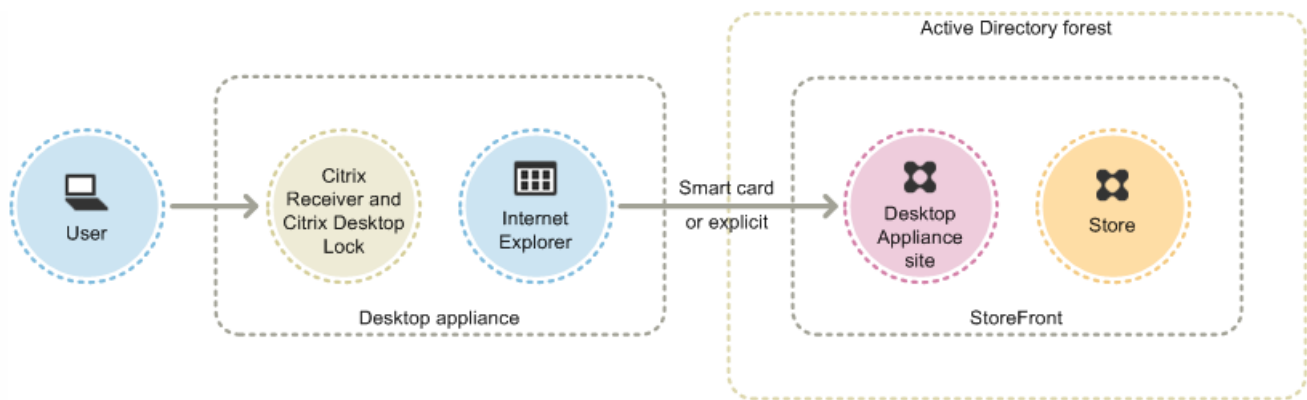
Remarque : si vous utilisez Citrix Receiver pour Windows 4.2 (la version actuelle), vous pouvez configurer un autre vServer et utiliser la fonctionnalité de routage vers une passerelle optimale pour supprimer les invites de saisie du code PIN lors du démarrage d'applications et de bureaux.

Les utilisateurs peuvent ouvrir une session sur NetScaler Gateway à l'aide de leurs cartes à puce et codes PIN, ou avec des informations d'identification explicites. Cela vous permet de fournir aux utilisateurs la possibilité de revenir à l'authentification explicite pour les ouvertures de session NetScaler Gateway. Configurez l'authentification pass-through via NetScaler Gateway à StoreFront et déléguez la validation des informations d'identification à NetScaler Gateway pour les utilisateurs de cartes à puce de façon à ce que les utilisateurs soient authentifiés auprès de StoreFront de manière silencieuse.

Utiliser des cartes à puce avec des sites Desktop Appliance

Les boîtiers de bureau Windows n'appartenant pas à un domaine peuvent être configurés pour autoriser les utilisateurs à ouvrir une session sur leurs bureaux à l'aide de cartes à puce. Citrix Desktop Lock est requis sur le boîtier et Internet Explorer doit être utilisé pour accéder au site Desktop Appliance.

La figure illustre une authentification par carte à puce à partir d'un boîtier de bureau n'appartenant pas à un domaine.



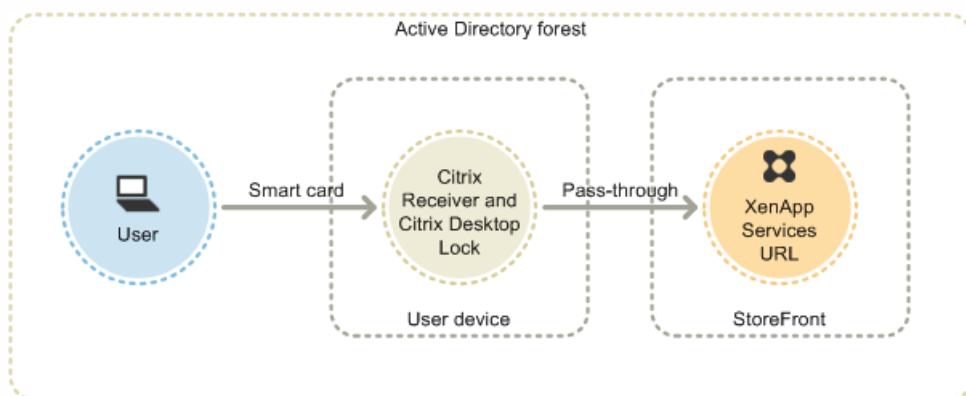
Lorsque les utilisateurs accèdent à leurs boîtiers de bureau, Internet Explorer démarre en mode plein écran et affiche l'écran d'ouverture de session pour un site Desktop Appliance. Les utilisateurs doivent s'authentifier sur le site à l'aide de leurs cartes à puce et codes PIN. Si le site Desktop Appliance est configuré pour l'authentification pass-through, les utilisateurs sont authentifiés automatiquement lorsqu'ils accèdent à leurs bureaux et applications. Les utilisateurs ne sont pas invités à entrer de nouveau leur code PIN. Sans l'authentification pass-through, les utilisateurs doivent entrer leur code PIN une seconde fois lorsqu'ils démarrent un bureau ou une application.

Vous pouvez autoriser les utilisateurs à revenir à l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce. Pour ce faire, vous devez configurer le site Desktop Appliance pour l'authentification carte à puce et explicite. Dans cette configuration, l'authentification par carte à puce est considérée comme la méthode d'accès principale donc les utilisateurs sont invités en premier à entrer leur code PIN. Toutefois, le site fournit également un lien qui permet aux utilisateurs d'ouvrir une session avec des informations d'identification explicites à la place.

Utiliser des cartes à puce avec des adresses URL XenApp Services

Les utilisateurs de boîtiers de bureau appartenant à un domaine et de PC réaffectés exécutant Citrix Desktop Lock peuvent s'authentifier à l'aide de cartes à puce. À l'inverse d'autres méthodes d'accès, l'authentification pass-through des informations d'identification de carte à puce est automatiquement activée lorsque l'authentification par carte à puce est configurée pour une adresse URL XenApp Services.

La figure illustre une authentification par carte à puce à partir d'une machine appartenant à un domaine exécutant Citrix Desktop Lock.



Les utilisateurs ouvrent une session sur leurs machines à l'aide de leurs cartes à puce et codes PIN. Citrix Desktop Lock authentifie ensuite de manière silencieuse les utilisateurs auprès de StoreFront via l'adresse URL XenApp Services. Les utilisateurs sont automatiquement authentifiés lorsqu'ils accèdent à leurs bureaux et applications, et ne sont pas invités à

entrer leur code PIN de nouveau.

Utiliser des cartes à puce avec Citrix Receiver pour Web

Vous pouvez activer l'authentification par carte à puce pour Citrix Receiver pour Web dans la console d'administration StoreFront.

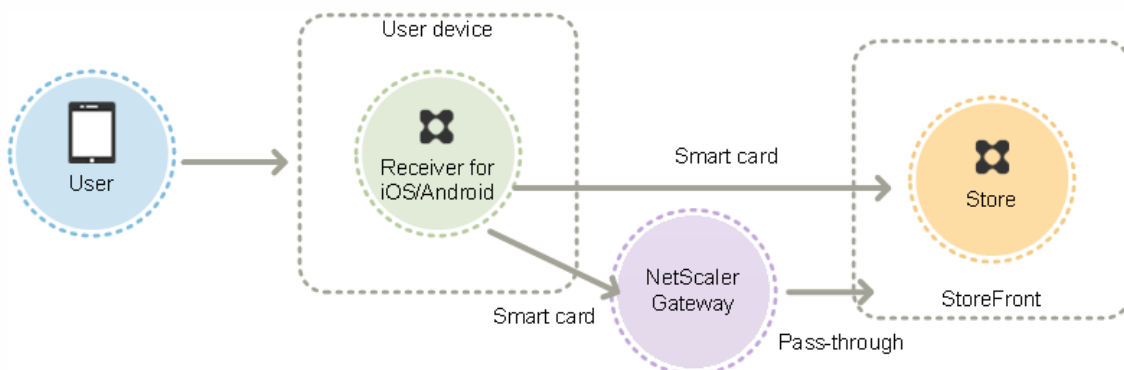
1. Sélectionnez le nœud Citrix Receiver pour Web dans le panneau de gauche.
2. Sélectionnez le site dans lequel vous voulez utiliser l'authentification par carte à puce.
3. Sélectionnez la tâche Choisir les méthodes d'authentification dans le panneau de droite.
4. Activez la case à cocher de la carte à puce dans la boîte de dialogue contextuelle et cliquez sur OK.

Si vous activez l'authentification pass-through avec carte à puce à XenDesktop et XenApp pour les utilisateurs Citrix Receiver pour Windows équipés de machines appartenant à un domaine qui n'accèdent pas aux magasins via NetScaler Gateway, ce paramètre s'applique à tous les utilisateurs du magasin. Pour activer l'authentification pass-through au domaine et l'authentification pass-through avec l'authentification par carte à puce à des bureaux et des applications, vous devez créer des magasins distincts pour chaque méthode d'authentification. Les utilisateurs doivent ensuite se connecter au magasin approprié à leur méthode d'authentification.

Si vous activez l'authentification pass-through avec carte à puce à XenDesktop et XenApp pour les utilisateurs Citrix Receiver pour Windows équipés de machines appartenant à un domaine qui accèdent aux magasins via NetScaler Gateway, ce paramètre s'applique à tous les utilisateurs du magasin. Pour activer l'authentification pass-through pour certains utilisateurs et exiger que d'autres ouvrent une session à leurs bureaux et applications, vous devez créer des magasins distincts pour chaque groupe d'utilisateurs. Ensuite, pointez vos utilisateurs vers le magasin approprié pour leur méthode d'authentification.

Utiliser des cartes à puce avec Citrix Receiver pour iOS et Android

Les utilisateurs équipés d'appareils exécutant Citrix Receiver pour iOS et Citrix Receiver pour Android peuvent s'authentifier à l'aide de cartes à puce, soit directement, soit via NetScaler Gateway. Il est possible d'utiliser des machines qui n'appartiennent pas à un domaine.



Dans le cas de machines sur le réseau local, le nombre minimal d'invites d'ouverture de session que les utilisateurs reçoivent est de deux. Lorsque les utilisateurs s'authentifient auprès de StoreFront ou qu'ils créent le magasin, ils sont invités à entrer le code PIN de la carte à puce. Lorsque la configuration appropriée est appliquée, les utilisateurs sont de nouveau invités à entrer leur code PIN uniquement lorsqu'ils accèdent à leurs bureaux et applications. Pour ce faire, vous devez activer l'authentification par carte à puce à StoreFront et installer les pilotes de carte à puce sur le VDA.

Avec ces Citrix Receiver, vous avez la possibilité de spécifier des cartes à puce ou des informations d'identification de domaine. Si vous avez créé un magasin pour utiliser les cartes à puce et que vous voulez vous connecter au même magasin à

l'aide d'informations d'identification de domaine, vous devez ajouter un magasin séparé sans activer les cartes à puce.

Les utilisateurs qui se connectent via NetScaler Gateway doivent ouvrir une session à l'aide de leurs cartes à puce et codes PIN aux moins deux fois pour accéder à leurs bureaux et applications. Les utilisateurs s'authentifient à l'aide de leurs cartes à puce et codes PIN, et lorsque la configuration appropriée est appliquée, ils ne sont invités à entrer que leur code PIN pour accéder à leurs bureaux et applications. Pour ce faire, vous devez activer l'authentification pass-through via NetScaler Gateway à StoreFront et déléguer la validation des informations d'identification à NetScaler Gateway. Créez ensuite un serveur virtuel NetScaler Gateway supplémentaire par le biais duquel router les connexions utilisateur vers les ressources.

Les utilisateurs peuvent ouvrir une session sur NetScaler Gateway à l'aide de leurs cartes à puce et codes PIN ou avec des informations d'identification explicites, en fonction de la façon dont vous avez spécifié l'authentification pour la connexion. Configurez l'authentification pass-through via NetScaler Gateway à StoreFront et déléguez la validation des informations d'identification à NetScaler Gateway pour les utilisateurs de cartes à puce de façon à ce que les utilisateurs soient authentifiés auprès de StoreFront de manière silencieuse. Si vous souhaitez modifier la méthode d'authentification, vous devez supprimer, puis recréer la connexion.

Utiliser des cartes à puce avec Citrix Receiver pour Linux

Les utilisateurs équipés de machines exécutant Citrix Receiver pour Linux peuvent s'authentifier à l'aide de cartes à puce de la même manière que des utilisateurs de machines Windows qui n'appartiennent pas au domaine. Même si l'utilisateur s'authentifie auprès de la machine Linux avec une carte à puce, Citrix Receiver pour Linux ne dispose d'aucun mécanisme lui permettant d'acquiescer ou réutiliser le code PIN entré.

Configurez les composants côté serveur pour les cartes à puce de la même manière que vous les configurez en vue de les utiliser avec Citrix Receiver pour Windows. Référez-vous à [Comment configurer StoreFront 2.x et l'authentification par carte à puce pour les utilisateurs internes à l'aide de magasins](#) et pour obtenir des instructions sur l'utilisation des cartes à puce, veuillez consulter la rubrique [Citrix Receiver pour Linux](#).

Le nombre minimal d'ouverture de session que les utilisateurs peuvent recevoir est de un. Les utilisateurs ouvrent une session sur leurs machines et s'authentifient auprès de Citrix Receiver pour Linux à l'aide de leurs cartes à puce et codes PIN. Les utilisateurs ne sont pas de nouveau invités à entrer leur code PIN lorsqu'ils accèdent à leurs bureaux et applications. Pour ce faire, vous devez activer l'authentification par carte à puce à StoreFront.

Étant donné que les utilisateurs ouvrent une session sur Citrix Receiver pour Linux directement, vous pouvez autoriser les utilisateurs à revenir à l'authentification explicite. Si vous configurez l'authentification par carte à puce et explicite, les utilisateurs sont initialement invités à ouvrir une session à l'aide de leurs cartes à puce et codes PIN mais ont la possibilité de sélectionner l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce.

Les utilisateurs qui se connectent via NetScaler Gateway doivent ouvrir une session à l'aide de leurs cartes à puce et codes PIN au moins une fois pour accéder à leurs bureaux et applications. Les utilisateurs s'authentifient à l'aide de leurs cartes à puce et codes PIN, et lorsque la configuration appropriée est appliquée, ils ne sont pas invités à entrer de nouveau leur code PIN pour accéder à leurs bureaux et applications. Pour ce faire, vous devez activer l'authentification pass-through via NetScaler Gateway à StoreFront et déléguer la validation des informations d'identification à NetScaler Gateway. Créez ensuite un serveur virtuel NetScaler Gateway supplémentaire par le biais duquel router les connexions utilisateur vers les ressources.

Les utilisateurs peuvent ouvrir une session sur NetScaler Gateway à l'aide de leurs cartes à puce et codes PIN, ou avec des informations d'identification explicites. Cela vous permet de fournir aux utilisateurs la possibilité de revenir à l'authentification explicite pour les ouvertures de session NetScaler Gateway. Configurez l'authentification pass-through via

NetScaler Gateway à StoreFront et délèguez la validation des informations d'identification à NetScaler Gateway pour les utilisateurs de cartes à puce de façon à ce que les utilisateurs soient authentifiés auprès de StoreFront de manière silencieuse.

Les cartes à puce pour Citrix Receiver pour Linux ne sont pas prises en charge avec les sites XenApp Services Support.

Une fois que la prise en charge des cartes à puce est activée à la fois sur le serveur et sur Citrix Receiver, à condition que la stratégie d'application des certificats de carte à puce le permette, vous pouvez utiliser des cartes à puce aux fins suivantes :

- Authentification d'ouverture de session par carte à puce. Servez-vous de cartes à puce pour authentifier les utilisateurs auprès des serveurs Citrix XenApp et XenDesktop.
- Prise en charge des applications recourant à une carte à puce. Autorisez les applications recourant à une carte à puce à accéder aux lecteurs de carte à puce locaux.

Utiliser des cartes à puce avec XenApp Services Support

Les utilisateurs qui ouvrent une session sur les sites XenApp Services Support pour démarrer des applications et des bureaux peuvent s'authentifier à l'aide de cartes à puce quels que soient le matériel, les systèmes d'exploitation et les logiciels Citrix Receiver utilisés. Lorsqu'un utilisateur accède à un site XenApp Services Support, qu'il insère une carte à puce et entre un code PIN, PNA détermine l'identité de l'utilisateur, authentifie l'utilisateur auprès de StoreFront et renvoie les ressources disponibles.

Pour que l'authentification pass-through et l'authentification par carte à puce fonctionnent, vous devez activer l'option Faire confiance aux requêtes envoyées au Service XML.

Utilisez un compte avec des autorisations d'administrateur local sur le Delivery Controller pour démarrer le Windows PowerShell et, à l'invite de commande, tapez les commandes suivantes pour que le Delivery Controller approuve les requêtes XML envoyées à partir de StoreFront. La procédure suivante s'applique à XenApp 7.5 à 7.8 et XenDesktop 7.0 à 7.8.

1. Chargez les applets de commande Citrix en tapant `asnp Citrix*`. (en incluant le point).
2. Tapez **Add-PSSnapin citrix.broker.admin.v2**.
3. Tapez **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$True**
4. Fermez PowerShell.

Pour de plus amples informations sur la configuration de la méthode d'authentification par carte à puce XenApp Services Support, veuillez consulter la section [Configurer l'authentification des adresses URL des sites XenApp Services](#).

Remarques importantes

L'utilisation de cartes à puce pour l'authentification utilisateur avec StoreFront est soumise aux conditions et restrictions suivantes.

- Pour utiliser des tunnels VPN avec l'authentification par carte à puce, les utilisateurs doivent installer NetScaler Gateway Plug-in et ouvrir une session via une page Web, et utiliser leurs cartes à puce et codes PIN pour s'authentifier à chaque étape. L'authentification pass-through à StoreFront avec NetScaler Gateway Plug-in n'est pas disponible pour les utilisateurs de cartes à puce.
- Plusieurs cartes à puce et plusieurs lecteurs peuvent être utilisés sur la même machine utilisateur, mais si vous activez l'authentification pass-through avec carte à puce, les utilisateurs doivent s'assurer qu'une seule carte à puce est insérée lors de l'accès à un bureau ou une application.
- Lorsqu'une carte à puce est utilisée dans une application, pour la signature numérique ou le cryptage, des messages

supplémentaires invitant l'utilisateur à insérer la carte à puce ou à saisir un code PIN peuvent s'afficher. Cela peut se produire si plusieurs cartes à puce sont insérées en même temps. Cela peut également être dû à des paramètres de configuration, tels que des paramètres de middleware comme la mise en cache du code PIN, qui sont généralement configurés à l'aide d'une stratégie de groupe. Les utilisateurs qui sont invités à insérer une carte à puce lorsque la carte à puce est déjà dans le lecteur doivent cliquer sur Annuler. Si les utilisateurs sont invités à entrer un code PIN, ils doivent entrer de nouveau ce code.

- Si vous activez l'authentification pass-through avec carte à puce à XenDesktop et XenApp pour les utilisateurs Citrix Receiver pour Windows équipés de machines appartenant à un domaine qui n'accèdent pas aux magasins via NetScaler Gateway, ce paramètre s'applique à tous les utilisateurs du magasin. Pour activer l'authentification pass-through au domaine et l'authentification pass-through avec l'authentification par carte à puce à des bureaux et des applications, vous devez créer des magasins distincts pour chaque méthode d'authentification. Les utilisateurs doivent ensuite se connecter au magasin approprié à leur méthode d'authentification.
- Si vous activez l'authentification pass-through avec carte à puce à XenDesktop et XenApp pour les utilisateurs Citrix Receiver pour Windows équipés de machines appartenant à un domaine qui accèdent aux magasins via NetScaler Gateway, ce paramètre s'applique à tous les utilisateurs du magasin. Pour activer l'authentification pass-through pour certains utilisateurs et exiger que d'autres ouvrent une session à leurs bureaux et applications, vous devez créer des magasins distincts pour chaque groupe d'utilisateurs. Ensuite, pointez vos utilisateurs vers le magasin approprié pour leur méthode d'authentification.
- Une seule méthode d'authentification peut être configurée pour chaque adresse URL XenApp Services et une seule URL est disponible par magasin. Si vous devez activer d'autres types d'authentification en plus de l'authentification par carte à puce, vous devez créer des magasins distincts, chacun avec une adresse URL XenApp Services pour chaque méthode d'authentification. Ensuite, pointez vos utilisateurs vers le magasin approprié pour leur méthode d'authentification.
- Lorsque StoreFront est installé, la configuration par défaut dans Microsoft Internet Information Services (IIS) requiert uniquement que les certificats clients soient présentés pour les connexions HTTPS à l'adresse URL d'authentification du certificat du service d'authentification de StoreFront. IIS ne demande de certificats clients pour aucune des autres adresses URL de StoreFront. Cette configuration vous permet de fournir aux utilisateurs de cartes à puce l'option de revenir à l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce. Sous réserve que les paramètres de stratégie Windows appropriés sont activés, les utilisateurs peuvent également retirer leur carte à puce sans avoir à s'authentifier de nouveau.

Si vous décidez de configurer IIS pour demander des certificats clients pour les connexions HTTPS à toutes les adresses URL de StoreFront, le service d'authentification et les magasins doit être colocalisés sur le même serveur. Vous devez utiliser un certificat client valide pour tous les magasins. Avec cette configuration de site IIS, les utilisateurs de carte à puce ne peuvent pas se connecter via NetScaler Gateway et ne peuvent pas revenir à l'authentification explicite. Les utilisateurs doivent ouvrir une nouvelle session s'ils retirent leur carte à puce de leur périphérique.

Optimiser l'expérience utilisateur

Jun 30, 2017

StoreFront comprend des fonctionnalités conçues pour améliorer l'expérience utilisateur. Ces fonctionnalités sont configurées par défaut lorsque vous créez de nouveaux magasins et leurs sites Citrix Receiver pour Web associés, des sites Desktop Appliance et des adresses URL XenApp Services.

Le contrôle de l'espace de travail

Le contrôle de l'espace de travail permet de s'assurer que les applications suivent les utilisateurs lorsqu'ils passent d'un périphérique à un autre. Les utilisateurs peuvent continuer à travailler avec les mêmes instances d'application sur plusieurs périphériques plutôt que d'avoir à redémarrer toutes leurs applications chaque fois qu'ils ouvrent une session sur un nouveau périphérique. Ceci permet, par exemple, aux médecins hospitaliers de gagner du temps lorsqu'ils passent d'un poste de travail à un autre pour accéder aux données de leurs patients.

Le contrôle de l'espace de travail est activé par défaut pour les sites Citrix Receiver pour Web et les connexions aux magasins via les adresses URL XenApp Services. Lorsque les utilisateurs ouvrent une session, ils sont automatiquement reconnectés à toutes les applications qu'ils ont laissées en cours d'exécution. Par exemple, un utilisateur ouvre une session sur un magasin, soit via le site Citrix Receiver pour Web ou l'adresse URL du site XenApp Services, et démarre certaines applications. Si l'utilisateur ouvre ensuite une session sur le même magasin en utilisant la même méthode d'accès mais sur un autre périphérique, les applications sont automatiquement transférées vers ce nouveau périphérique. Toutes les applications que l'utilisateur démarre depuis un magasin particulier sont automatiquement déconnectées, mais ne sont pas fermées, lorsque l'utilisateur ferme la session de ce magasin. Dans le cas des sites Citrix Receiver pour Web, le même navigateur doit être utilisé pour ouvrir une session, démarrer les applications et fermer la session.

Le contrôle de l'espace de travail pour les adresses URL XenApp Services ne peut pas être configuré ou désactivé. Pour plus d'informations sur la configuration du contrôle de l'espace de travail pour les sites Citrix Receiver pour Web, veuillez consulter la section [Configurer le contrôle de l'espace de travail](#).

L'utilisation du contrôle de l'espace de travail disponible sur les sites Citrix Receiver pour Web est soumise aux exigences et aux restrictions suivantes.

- Le contrôle de l'espace de travail n'est pas disponible lorsque les sites Citrix Receiver pour Web sont accessibles depuis des bureaux et des applications hébergés.
- Pour les utilisateurs qui accèdent à des sites Citrix Receiver pour Web à partir de périphériques Windows, le contrôle de l'espace de travail est uniquement activé si le site peut détecter que Citrix Receiver est installé sur les périphériques des utilisateurs ou si Citrix Receiver pour HTML5 est utilisé pour accéder aux ressources.
- Pour se reconnecter aux applications déconnectées, les utilisateurs accédant aux sites Citrix Receiver pour Web via Internet Explorer doivent ajouter le site à l'intranet local ou à des zones de sites approuvés.
- S'il n'existe qu'un seul bureau disponible pour un utilisateur sur un site Citrix Receiver pour Web configuré pour démarrer les bureaux automatiquement lorsque l'utilisateur ouvre une session, les applications de cet utilisateur ne sont pas reconnectées, quelle que soit la configuration du contrôle de l'espace de travail.
- Les utilisateurs doivent se déconnecter de leurs applications en utilisant le même navigateur que celui qu'ils ont utilisé pour leur exécution. Les ressources démarrées par le biais d'un autre navigateur ou localement depuis le bureau ou le menu Démarrer via Citrix Receiver ne peuvent pas être déconnectées ou arrêtées par les sites Citrix Receiver pour Web.

Redirection de contenu

Lorsque des utilisateurs se sont abonnés à l'application appropriée, la redirection de contenu permet aux fichiers locaux sur les machines des utilisateurs d'être ouverts à l'aide d'applications auxquelles ils se sont abonnés. Pour activer la redirection des fichiers locaux, associez l'application avec les types de fichiers requis dans XenDesktop ou XenApp. L'association de type de fichier est activée par défaut pour les nouveaux magasins. Pour plus d'informations, veuillez consulter la section [Désactiver l'association de type de fichier](#).

Mot de passe modifié par l'utilisateur

Vous pouvez permettre aux utilisateurs de sites Citrix Receiver pour Web qui ouvrent une session avec des informations d'identification de domaine Microsoft Active Directory de modifier leurs mots de passe à tout moment. Éventuellement, vous pouvez autoriser uniquement les utilisateurs dont les mots de passe ont expiré à les modifier. Cela permet de s'assurer que les utilisateurs ne se verront jamais refuser l'accès à leurs bureaux et applications en raison d'un mot de passe a expiré.

Si vous autorisez les utilisateurs de sites Citrix Receiver pour Web à modifier leurs mots de passe à tout moment, un avertissement s'affiche à l'attention des utilisateurs locaux dont les mots de passe sont sur le point d'expirer lorsqu'ils ouvrent une session. Par défaut, la période de notification pour un utilisateur est déterminée par le paramètre de stratégie Windows applicable. Les avertissements d'expiration du mot de passe s'affichent uniquement pour les utilisateurs se connectant depuis le réseau interne. Pour savoir comment autoriser les utilisateurs à modifier leurs mots de passe, consultez la section [Configurer le service d'authentification](#).

Les utilisateurs qui ouvrent une session sur des sites Desktop Appliance peuvent uniquement modifier leurs mots de passe expirés, même si vous autorisez les utilisateurs à modifier leurs mots de passe à tout moment. Les sites Desktop Appliance ne fournissent aucun contrôle permettant aux utilisateurs de modifier leurs mots de passe après l'ouverture d'une session.

Lorsque vous créez le service d'authentification, la configuration par défaut empêche les utilisateurs de sites Citrix Receiver pour Web de modifier leurs mots de passe, même si les mots de passe ont expiré. Si vous choisissez d'activer cette fonctionnalité, assurez-vous que les stratégies des domaines contenant vos serveurs n'empêchent pas les utilisateurs de modifier leurs mots de passe. StoreFront doit être en mesure de contacter le contrôleur de domaine pour modifier les mots de passe des utilisateurs.

L'activation de la fonctionnalité permettant aux utilisateurs de modifier leurs mots de passe expose des fonctions de sécurité sensibles à toute personne pouvant accéder aux magasins qui utilisent ce service d'authentification. Si votre organisation possède une stratégie de sécurité qui restreint les fonctions de modification des mots de passe utilisateur à un usage interne uniquement, vous devez vous assurer qu'aucun des magasins ne sont accessibles depuis l'extérieur de votre réseau interne.

Vues des applications et bureaux du site Citrix Receiver pour Web

Lorsque des bureaux et des applications sont disponibles depuis un site Citrix Receiver pour Web, le site affiche par défaut des vues distinctes des bureaux et des applications. Les utilisateurs voient tout d'abord la vue de bureau lorsqu'ils ouvrent une session sur le site. Que les applications soient disponibles ou non depuis un site Citrix Receiver pour Web, lorsqu'un seul bureau est disponible pour un utilisateur, le site démarre ce bureau automatiquement lorsque l'utilisateur ouvre une session. Vous pouvez configurer quelles vues s'affichent pour vos sites et empêcher les sites Citrix Receiver pour Web de démarrer automatiquement les bureaux des utilisateurs. Pour plus d'informations, consultez la section [Configurer la manière dont les ressources s'affichent auprès des utilisateurs](#).

Le comportement des vues sur les sites Citrix Receiver pour Web dépend des types de ressources mises à disposition. Par exemple, les utilisateurs doivent s'abonner aux applications avant qu'elles ne s'affichent dans la vue des applications, alors que tous les bureaux disponibles pour un utilisateur sont automatiquement affichés dans la vue des bureaux. Pour cette raison, les utilisateurs ne peuvent supprimer des bureaux de la vue des bureaux et ne peuvent pas les réorganiser en cliquant

sur les icônes et en les déplaçant. Lorsque les redémarrages de bureaux sont activés par l'administrateur XenDesktop, des commandes pour permettre aux utilisateurs de redémarrer leurs bureaux sont fournies dans la vue des bureaux. Si les utilisateurs possèdent un accès à plusieurs instances d'un bureau depuis un groupe de bureaux unique, les sites Citrix Receiver pour Web distinguent les bureaux des utilisateurs en ajoutant des suffixes numériques aux noms des bureaux.

Pour les utilisateurs se connectant à des magasins dans Citrix Receiver ou via les adresses URL XenApp Services, la manière dont les bureaux et applications sont affichés, et leur comportement, est déterminée par le client Citrix utilisé.

Recommandations supplémentaires

Lors de la mise à disposition d'applications avec XenDesktop et XenApp, envisagez les options suivantes pour améliorer l'expérience des utilisateurs qui accèdent à leurs applications par le biais de vos magasins. Pour plus d'informations sur la mise à disposition d'applications, consultez la section [Créer une application de groupe de mise à disposition](#).

- Organisez les applications dans des dossiers afin de permettre aux utilisateurs de trouver plus facilement ce dont ils ont besoin lorsqu'ils naviguent parmi les ressources mises à leur disposition. Les dossiers que vous créez dans XenDesktop et XenApp apparaissent sous forme de catégories dans Citrix Receiver. Vous pouvez, par exemple, regrouper les applications selon leur type ou bien créer des dossiers pour les différents rôles des utilisateurs au sein de votre organisation.
- Veillez à inclure des descriptions claires des applications que vous mettez à disposition, car ces descriptions sont consultées par les utilisateurs dans Citrix Receiver.
- Vous pouvez spécifier pour chaque utilisateur un ensemble d'applications de base qui ne peuvent pas être supprimées de l'écran d'accueil de Citrix Receiver en ajoutant la chaîne KEYWORDS:Mandatory à la description de l'application. Les utilisateurs peuvent toujours utiliser l'interface utilisateur en libre-service pour ajouter d'autres applications ou supprimer des applications qui ne sont pas nécessaires.
- Vous pouvez automatiquement abonner tous les utilisateurs d'un magasin à une application en ajoutant la chaîne KEYWORDS:Auto à la description que vous fournissez lorsque vous mettez l'application à disposition. Lorsque les utilisateurs ouvrent une session sur le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.
- Pour abonner automatiquement tous les utilisateurs d'un magasin à une application Web ou SaaS (software-as-a-service) gérée par App Controller, sélectionnez la case à cocher App is available in Citrix Receiver to all users automatically lorsque vous configurez les paramètres de l'application.
- Publiez des applications XenDesktop auprès des utilisateurs ou facilitez-leur la recherche des applications les plus couramment utilisées en les répertoriant dans la liste Sélection de Citrix Receiver. Pour ce faire, ajoutez la chaîne KEYWORDS:Featured à la description de l'application.

Remarque : les mots-clés multiples doivent uniquement être séparés par des espaces ; par exemple, KEYWORDS:Auto Featured.

- Par défaut, les bureaux partagés hébergés XenDesktop et XenApp sont traités comme tout autre bureau par les sites Citrix Receiver pour Web. Pour changer ce comportement, ajoutez la chaîne KEYWORDS:TreatAsApp à la description du bureau. Le bureau est affiché dans la vue des applications des sites Citrix Receiver pour Web plutôt que dans la vue des bureaux et les utilisateurs doivent s'abonner avant de pouvoir accéder au bureau. De plus, le bureau n'est pas automatiquement démarré lorsque l'utilisateur ouvre une session sur le site Citrix Receiver pour Web et qu'il n'est pas accédé à l'aide de Desktop Viewer, même si le site est configuré dans ce but pour d'autres bureaux.
- Pour les utilisateurs Windows, vous pouvez spécifier que la version d'une application installée localement doit être utilisée de préférence à l'instance équivalente mise à disposition si les deux sont disponibles. Pour ce faire, ajoutez la chaîne **KEYWORDS:prefer="application"** à la description de l'application, où application est un ou plusieurs mots complets dans le nom de l'application locale comme indiqué par le nom du fichier de raccourci, ou le chemin d'accès absolu, y compris le nom du fichier exécutable, vers l'application locale du dossier \Démarrer. Lorsqu'un utilisateur s'abonne à une application avec ce mot clé, Citrix Receiver recherche le nom ou chemin d'accès spécifié sur la machine utilisateur pour déterminer si

l'application est déjà installée localement. Si l'application est trouvée, Citrix Receiver abonne l'utilisateur à l'application mise à disposition, mais ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application mise à disposition à partir de Citrix Receiver, l'instance installée localement s'exécute à la place. Pour plus d'informations, veuillez consulter la section [Configurer la mise à disposition d'applications](#).

Haute disponibilité et configuration multisite de StoreFront

Jun 30, 2017

StoreFront comprend un certain nombre de fonctionnalités qui combinées permettent d'activer l'équilibrage de charge et le basculement entre les déploiements offrant des ressources aux magasins. Vous pouvez également spécifier des déploiements de récupération d'urgence dédiés afin d'augmenter la résilience. Ces fonctionnalités vous permettent de configurer des déploiements StoreFront répartis sur plusieurs sites afin de fournir une haute disponibilité pour vos magasins. Pour de plus amples informations, consultez la section [Définir des configurations multisite assurant une haute disponibilité des magasins](#).

Agrégation de ressources

Par défaut, StoreFront énumère tous les déploiements offrant des bureaux et des applications à un magasin et traite toutes ces ressources comme distinctes. Ceci signifie que si la même ressource est disponible à partir de plusieurs déploiements, les utilisateurs voient une icône pour chaque ressource, ce qui peut prêter à confusion si les ressources ont le même nom. Lorsque vous créez des configurations multisite à haut niveau de disponibilité, vous pouvez grouper les déploiements XenDesktop et XenApp qui délivrent le même bureau ou la même application afin que les ressources identiques puissent être agrégées pour les utilisateurs. Les déploiements groupés n'ont pas besoin d'être identiques, mais les ressources doivent avoir le même nom et le même chemin d'accès sur chaque serveur pour être regroupées.

Lorsqu'un bureau ou une application est disponible à partir de plusieurs déploiements XenDesktop et XenApp configurés pour un magasin spécifique, StoreFront regroupe toutes les instances de cette ressource et présente une seule icône aux utilisateurs. Les applications App Controller ne peuvent pas être regroupées. Lorsqu'un utilisateur démarre une ressource agrégée, StoreFront détermine l'instance de cette ressource la plus appropriée pour l'utilisateur sur la base de la disponibilité du serveur, si l'utilisateur a déjà une session active et l'ordre que vous avez spécifié dans la configuration.

StoreFront surveille dynamiquement les serveurs qui ne répondent pas aux requêtes parce qu'ils sont surchargés ou temporairement indisponibles. Les utilisateurs sont dirigés vers les instances de la ressource sur d'autres serveurs jusqu'à ce que les communications soient rétablies. Lorsque cela est pris en charge par les serveurs fournissant les ressources, StoreFront tente de réutiliser les sessions existantes pour mettre à disposition des ressources supplémentaires. Si un utilisateur a déjà une session active sur un déploiement qui fournit également la ressource demandée, StoreFront réutilise la session si elle est compatible avec cette ressource. La réduction du nombre de sessions par utilisateur permet de réduire le temps nécessaire au démarrage des bureaux ou applications supplémentaires et permet une utilisation plus efficace des licences des produits.

Après avoir vérifié la disponibilité et les sessions utilisateur existantes, StoreFront utilise l'ordre spécifié dans votre configuration pour déterminer le déploiement auquel l'utilisateur est connecté. Si plusieurs déploiements équivalents sont disponibles à l'utilisateur, vous pouvez spécifier que les utilisateurs sont connectés au premier déploiement disponible ou de manière aléatoire à tout déploiement dans la liste. Le fait de connecter les utilisateurs au premier déploiement disponible vous permet de réduire le nombre de déploiements utilisés pour le nombre actuel d'utilisateurs. Le fait de connecter les utilisateurs de manière aléatoire fournit une répartition plus équilibrée des utilisateurs sur tous les déploiements.

Vous pouvez remplacer l'ordre de déploiement spécifié pour les ressources XenDesktop et XenApp individuelles afin de définir les déploiements préférés auxquels les utilisateurs sont connectés lorsqu'ils accèdent à un bureau ou une application. Ceci vous permet, par exemple, de spécifier que les utilisateurs sont connectés à un déploiement spécialement conçu pour

mettre à disposition un bureau ou une application particulière, mais qu'ils utilisent d'autres déploiements pour d'autres ressources. Pour ce faire, ajoutez la chaîne KEYWORDS:Primary à la description de l'application ou bureau sur le déploiement préféré et la chaîne KEYWORDS:Secondary à la ressource sur d'autres déploiements. Dans la mesure du possible, les utilisateurs sont connectés au déploiement fournissant la ressource principale, quel que soit l'ordre de déploiement spécifié dans votre configuration. Les utilisateurs sont connectés aux déploiements fournissant les ressources secondaires lorsque le déploiement préféré n'est pas disponible.

Mapper les utilisateurs sur des ressources

Par défaut, les utilisateurs qui accèdent à un magasin voient un agrégat de toutes les ressources disponibles à partir de tous les déploiements configurés pour ce magasin. Pour fournir des ressources différentes pour des utilisateurs différents, vous pouvez configurer des magasins distincts ou même des déploiements StoreFront distincts. Toutefois, lorsque vous configurez des configurations multisite à haut niveau de disponibilité, vous pouvez fournir l'accès à certains déploiements en fonction de l'appartenance des utilisateurs à des groupes Microsoft Active Directory. Cela vous permet de configurer des expériences différentes pour différents groupes d'utilisateurs via un seul magasin.

Par exemple, vous pouvez grouper les ressources communes pour tous les utilisateurs sur un déploiement et les applications financières pour le département Comptes sur un autre déploiement. Dans cette configuration, un utilisateur qui n'est pas membre du groupe d'utilisateurs Comptes voit uniquement les ressources communes lors de l'accès au magasin. Un membre du groupe d'utilisateurs Comptes est présenté avec les ressources communes et les applications financières.

Éventuellement, vous pouvez créer un déploiement pour les utilisateurs avancés qui offre les mêmes ressources que vos autres déploiements, mais avec un matériel plus rapide et plus puissant. Cela vous permet de fournir une expérience améliorée pour les utilisateurs essentiels à l'entreprise, tels que votre équipe de direction. Tous les utilisateurs voient les mêmes bureaux et applications lorsqu'ils se connectent au magasin, mais les membres du groupe d'utilisateurs Direction sont connectés aux ressources fournies par le déploiement dédié aux utilisateurs avancés.

Synchronisation de l'abonnement

Si vous autorisez vos utilisateurs à accéder aux mêmes applications à partir de magasins similaires dans des déploiements StoreFront différents, les abonnements aux applications doivent être synchronisés entre les groupes de serveurs. Sinon, les utilisateurs qui s'abonnent à une application dans un magasin sur un déploiement StoreFront devront peut-être se réabonner à l'application lorsqu'ils se connectent à un groupe de serveurs différent. Pour offrir une expérience transparente aux utilisateurs qui utilisent plusieurs déploiements StoreFront, vous pouvez configurer la synchronisation régulière des abonnements aux applications entre les magasins dans différents groupes de serveurs. Choisissez entre une synchronisation régulière à intervalle spécifique ou programmez une synchronisation à certaines heures dans la journée. Pour plus d'informations, veuillez consulter la section [Configurer la synchronisation des abonnements](#).

Ressources de récupération d'urgence dédiées

Vous pouvez configurer des déploiements de récupération d'urgence spécifiques qui ne sont pas utilisés sauf si tous les autres déploiements ne sont pas disponibles. En général, les déploiements de récupération d'urgence ne sont pas colocalisés avec les déploiements principaux, ils fournissent uniquement un sous-ensemble des ressources qui sont normalement disponibles, et peuvent offrir une expérience utilisateur inférieure. Lorsque vous spécifiez un déploiement à utiliser pour la récupération d'urgence, ce dernier ne sera pas utilisé pour l'équilibrage de charge ou le basculement. Les utilisateurs ne peuvent pas accéder aux bureaux et applications fournis par les déploiements de récupération d'urgence, sauf si tous les autres déploiements pour lesquels les déploiements de récupération d'urgence sont configurés deviennent indisponibles.

Lorsque l'accès à un autre déploiement est rétabli, les utilisateurs ne peuvent pas démarrer d'autres ressources de récupération d'urgence, même s'ils utilisent déjà une telle ressource. Les utilisateurs exécutant des ressources de

récupération d'urgence ne sont pas déconnectés de ces ressources lorsque l'accès à d'autres déploiements est restauré. Toutefois, ils ne peuvent plus démarrer de ressources de récupération d'urgence une fois qu'ils ont quitté ces ressources. De même, StoreFront ne tente pas de réutiliser les sessions existantes avec les déploiements de récupération d'urgence si d'autres déploiements sont entre temps devenus disponibles.

Routage NetScaler Gateway optimal

Si vous avez configuré des boîtiers NetScaler Gateway distincts pour vos déploiements, StoreFront vous permet de définir le boîtier optimal que les utilisateurs doivent utiliser pour accéder à chacun des déploiements fournissant des ressources pour un magasin. Par exemple, si vous créez un magasin qui regroupe des ressources à partir de deux sites géographiques, chacun disposant d'un boîtier NetScaler Gateway, les utilisateurs se connectant via un boîtier dans un emplacement peuvent démarrer un bureau ou une application dans l'autre emplacement. Toutefois, par défaut, la connexion à la ressource est ensuite acheminée via le boîtier auquel l'utilisateur s'est connecté initialement et doit donc traverser le réseau étendu d'entreprise.

Pour améliorer l'expérience utilisateur et réduire le trafic réseau sur le réseau étendu, vous pouvez spécifier le boîtier NetScaler Gateway optimal pour chacun de vos déploiements. Avec cette configuration, les connexions utilisateur vers les ressources sont routées via le boîtier local pour le déploiement fournissant les ressources, quel que soit l'emplacement du boîtier par le biais duquel l'utilisateur accède au magasin.

Le routage NetScaler Gateway optimal peut également être utilisé dans le cas où les utilisateurs locaux sur le réseau interne doivent ouvrir une session sur NetScaler Gateway pour l'analyse de point de terminaison. Avec cette configuration, les utilisateurs se connectent au magasin via le boîtier NetScaler Gateway, mais il n'est pas nécessaire d'acheminer la connexion à la ressource via le boîtier car l'utilisateur est sur le réseau interne. Dans ce cas, vous devez activer le routage optimal, mais ne spécifiez pas de boîtier pour le déploiement, de façon à ce que les connexions utilisateur aux bureaux et applications soient acheminées directement et non via NetScaler Gateway. Notez que vous devez également configurer une adresse IP du serveur virtuel interne pour le boîtier NetScaler Gateway. En outre, spécifiez un point balise interne inaccessible afin que Citrix Receiver soit toujours invité à se connecter à NetScaler Gateway, quel que soit l'emplacement réseau de l'utilisateur.

Équilibrage de charge global des serveurs NetScaler Gateway

StoreFront prend en charge les déploiements NetScaler Gateway configurés pour l'équilibrage de charge des serveurs global avec de multiples boîtiers configurés avec un seul nom de domaine complet (FQDN). Pour pouvoir réaliser l'authentification utilisateur et acheminer les connexions utilisateur via le boîtier approprié, StoreFront doit être en mesure de faire la distinction entre les boîtiers. Étant donné que le nom de domaine complet du boîtier ne peut pas être utilisé comme identificateur unique dans une configuration d'équilibrage de charge des serveurs global, vous devez configurer StoreFront avec des adresses IP uniques pour chaque boîtier. En règle générale, il s'agit de l'adresse IP du serveur virtuel NetScaler Gateway.

Pour plus d'informations sur l'équilibrage de la charge, consultez la section [Équilibrage de charge avec NetScaler](#).

Remarques importantes

Lorsque vous décidez s'il convient de configurer des configurations multisite à haut niveau de disponibilité pour vos magasins, tenez compte des exigences et restrictions suivantes.

- Les bureaux et applications doivent avoir le même nom et chemin d'accès sur chaque serveur pour être agrégés. Par ailleurs, les propriétés des ressources agrégées, telles que les noms et les icônes, doivent être identiques. Si ce n'est pas le cas, les utilisateurs peuvent remarquer une modification des propriétés de leurs ressources lorsque Citrix Receiver

énumère les ressources disponibles.

- Les bureaux attribués, pré-attribués et attribués lors de la première utilisation, ne doivent pas être agrégés. Assurez-vous que les groupes de mise à disposition qui fournissent de tels bureaux ne possèdent pas le même nom ni le même chemin dans les sites que vous configurez pour l'agrégation.
- Les applications App Controller ne peuvent pas être regroupées.
- Si vous configurez la synchronisation des abonnements aux applications entre les magasins sur des déploiements StoreFront distincts, les magasins doivent avoir le même nom dans chaque groupe de serveurs. En outre, les deux groupes de serveurs doivent résider dans le domaine Active Directory contenant les comptes de vos utilisateurs ou dans un domaine qui a une relation d'approbation avec le domaine des comptes utilisateur.
- StoreFront fournit uniquement l'accès aux déploiements de secours pour la récupération d'urgence lorsque tous les sites principaux dans l'ensemble de déploiement équivalent ne sont pas disponibles. Si un déploiement de secours est partagé entre plusieurs ensembles de déploiements équivalents, tous les sites principaux dans chacun des ensembles doit être indisponible pour que les utilisateurs puissent accéder aux ressources de récupération d'urgence.

Installer, configurer, mettre à niveau et désinstaller

Jun 30, 2017

Avant l'installation et la configuration

Pour installer et configurer StoreFront, effectuez les étapes suivantes dans l'ordre :

1. Si vous prévoyez d'utiliser StoreFront pour fournir des ressources XenApp et XenDesktop aux utilisateurs, assurez-vous que le serveur StoreFront est membre du domaine Microsoft Active Directory contenant les comptes de vos utilisateurs ou d'un domaine qui a une relation d'approbation avec le domaine des comptes utilisateur.

Remarque :

- Pour les déploiements sur un seul serveur, vous pouvez installer StoreFront sur un serveur n'appartenant pas à un domaine.
- StoreFront ne peut pas être installé sur un contrôleur de domaine.

2. S'il n'est pas déjà installé, StoreFront requiert Microsoft.NET 4.5 Framework, qui peut être téléchargé depuis Microsoft. Microsoft.NET 4.5 doit être installé avant de pouvoir installer StoreFront.
3. Éventuellement, si vous prévoyez de configurer un déploiement StoreFront comprenant de multiples serveurs, configurez un environnement à équilibrage de charge pour vos serveurs StoreFront.

Pour utiliser NetScaler pour l'équilibrage de charge, définissez un serveur virtuel pour remplacer vos serveurs StoreFront. Pour de plus amples informations sur la configuration de NetScaler pour l'équilibrage de charge, consultez la section [Équilibrage de charge avec NetScaler](#).

1. Assurez-vous que l'équilibrage de charge est activé sur votre boîtier NetScaler.
2. Pour chaque serveur StoreFront, créez des services d'équilibrage de charge HTTP ou TLS individuels, selon les besoins, à l'aide du type de contrôle StoreFront.
3. Configurez les services de manière à insérer l'adresse IP du client dans l'en-tête HTTP X-Forwarded-For aux demandes transmises à StoreFront, ce qui remplace toute stratégie globale.

StoreFront requiert les adresses IP des utilisateurs pour établir des connexions à leurs ressources.

4. Créez un serveur virtuel et liez les services au serveur virtuel.
5. Sur le serveur virtuel, configurez la persistance à l'aide de la méthode d'insertion de cookies si vous avez installé la dernière version de Citrix Receiver sur toutes les plates-formes et que vous n'avez pas besoin de prendre en charge Android ; sinon, configurez la persistance en fonction de l'adresse IP source. Assurez-vous que la durée de vie (TTL) est suffisante pour permettre aux utilisateurs de rester connectés au serveur aussi longtemps que nécessaire.

La persistance garantit que seule la charge de la connexion utilisateur initiale est équilibrée, après quoi les demandes ultérieures de cet utilisateur sont redirigées vers le même serveur StoreFront.

4. Activez les fonctionnalités suivantes (facultatif).

- Fonctionnalités de .NET Framework 4.5 > .NET Framework 4.5 > ASP.NET 4.5

Si vous le souhaitez, vous pouvez activer les rôles suivants et leurs dépendances sur le serveur StoreFront.

- Serveur Web (IIS) > Serveur Web > Fonctionnalités HTTP communes > Document par défaut > Erreurs HTTP > Contenu statique > Redirection HTTP
- Serveur Web (IIS) > Serveur Web > État de santé et diagnostics > Journalisation HTTP
- Serveur Web (IIS) > Serveur Web > Sécurité > Filtrage des demandes > Authentification Windows
- Sur des serveurs Windows Server 2012 :

Serveur Web (IIS) > Serveur Web > Développement d'applications > Extensibilité .NET 4.5 > Initialisation d'application > ASP.NET 4.5 > Extensions ISAPI > Filtres ISAPI

Sur des serveurs Windows Server 2008 R2 :

Serveur Web (IIS) > Serveur Web > Développement d'applications > Extensibilité .NET > Initialisation d'application > ASP.NET > Extensions ISAPI > Filtres ISAPI

- Serveur Web (IIS) > Outils de gestion > Console de gestion IIS, Scripts et outils de gestion IIS

Le programme d'installation de StoreFront vérifie que toutes les fonctionnalités et tous les rôles de serveur ci-dessus sont activés.

5. [Installer StoreFront](#).

Si vous souhaitez que le serveur fasse partie d'un groupe de serveurs StoreFront, l'emplacement d'installation de StoreFront et les paramètres des sites Web IIS, tels que le chemin d'accès physique et les ID de site, doivent être identiques.

6. Vous pouvez éventuellement configurer Microsoft Internet Information Services (IIS) pour HTTPS si vous prévoyez d'utiliser le protocole HTTPS pour sécuriser les communications entre StoreFront et les machines des utilisateurs.

HTTPS est requis pour l'authentification par carte à puce. Par défaut, Citrix Receiver requiert des connexions HTTPS pour les magasins. Vous pouvez passer de HTTP à HTTPS à tout moment après l'installation de StoreFront, dans la mesure où la configuration IIS appropriée a été implémentée.

Pour configurer IIS pour HTTPS, utilisez la console Gestionnaire des services Internet (IIS) sur le serveur StoreFront pour créer un certificat de serveur signé par votre autorité de certification de domaine. Ensuite, ajoutez la liaison HTTPS au site Web par défaut. Pour de plus amples informations sur la création d'un certificat de serveur dans IIS, consultez l'article <http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate>. Pour plus d'informations sur l'ajout d'une liaison HTTPS à un site IIS, consultez l'article <http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding>.

7. Assurez-vous que votre pare-feu et autres périphériques réseau autorisent l'accès au port TCP 80 ou 443, aussi bien à l'intérieur qu'à l'extérieur du réseau d'entreprise. En outre, vérifiez que tous les pare-feu ou autres périphériques sur votre réseau interne ne bloquent pas le trafic des ports TCP non attribués.

Lorsque vous installez StoreFront, une règle pare-feu Windows est configurée pour activer l'accès à l'exécutable de StoreFront via un port TCP aléatoirement sélectionné à partir de

tous les ports non réservés. Ce port est utilisé pour les communications entre les serveurs StoreFront dans un groupe de serveurs.

8. Si vous prévoyez d'utiliser de multiples sites Web Internet Information Services (IIS), après la création des sites Web dans IIS, utilisez le SDK PowerShell pour créer un déploiement StoreFront dans chacun de ces sites Web IIS. Pour de plus amples informations, consultez la section [Sites Web Internet Information Services \(IIS\) multiples](#).

Remarque : StoreFront désactive la console de gestion lorsqu'il détecte de multiples sites et affiche un message à cet effet.

9. Utilisez la console de gestion Citrix StoreFront pour [configurer votre serveur](#).

Installer StoreFront

Important

Pour éviter des erreurs et la perte de données lors de l'installation de StoreFront, assurez-vous que toutes les applications sont fermées et qu'aucune autre tâche ou opération n'est en cours d'exécution sur le système cible.

1. Téléchargez le programme d'installation à partir de la page de téléchargement.
2. Ouvrez une session sur le serveur StoreFront en utilisant un compte disposant d'autorisations d'administrateur local.
3. Assurez-vous que le logiciel Microsoft .NET 4.5 Framework requis est installé sur le serveur.
4. Parcourez le pack de téléchargement, recherchez le fichier CitrixStoreFront-x64.exe, puis exécutez-le en tant qu'administrateur.
Remarque : sur les serveurs Windows Server 2008 R2, un message s'affiche indiquant que .NET sera activé. La fonctionnalité NET sera activée. Si ce message s'affiche, cliquez sur Oui.
5. Lisez et acceptez le contrat de licence, puis cliquez sur Suivant.
6. Si la page Vérifier les composants requis s'affiche, cliquez sur Suivant.
7. Sur la page Prêt pour l'installation, vérifiez que les trois composants de StoreFront sont répertoriés pour l'installation et cliquez sur Installer.
Avant l'installation des composants, les rôles suivants sont activés s'ils ne sont pas déjà configurés sur le serveur.

- Serveur Web (IIS) > Serveur Web > Fonctionnalités HTTP communes > Document par défaut > Erreurs HTTP > Contenu statique > Redirection HTTP
- Serveur Web (IIS) > Serveur Web > État de santé et diagnostics > Journalisation HTTP
- Serveur Web (IIS) > Serveur Web > Sécurité > Filtrage des demandes > Authentification Windows
- Sur des serveurs Windows Server 2012 :

Serveur Web (IIS) > Serveur Web > Développement d'applications > Extensibilité .NET 4.5 > Initialisation d'application > ASP.NET 4.5 > Extensions ISAPI > Filtres ISAPI

Sur des serveurs Windows Server 2008 R2 :

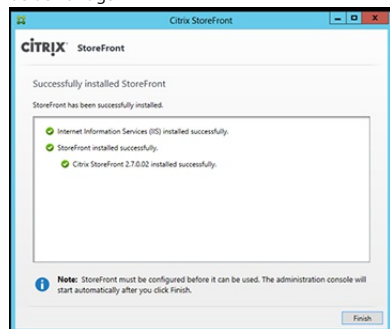
Serveur Web (IIS) > Serveur Web > Développement d'applications > Extensibilité .NET > Initialisation d'application > ASP.NET > Extensions ISAPI > Filtres ISAPI

- Serveur Web (IIS) > Outils de gestion > Console de gestion IIS, Scripts et outils de gestion IIS

Les fonctionnalités suivantes sont également activées si elles ne sont pas déjà configurées.

- Fonctionnalités de .NET Framework 4.5 > .NET Framework 4.5 > ASP.NET 4.5

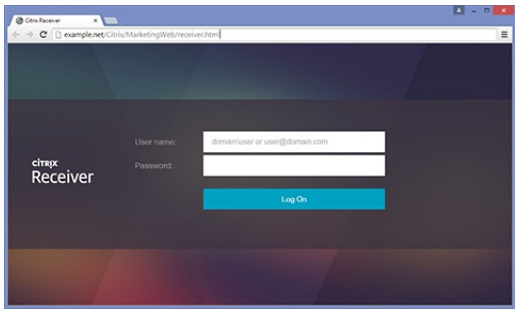
8. Une fois l'installation terminée, cliquez sur Terminer. La console de gestion Citrix StoreFront démarre automatiquement. Vous pouvez également accéder à StoreFront à partir de l'écran de démarrage.



9. Dans la console de gestion de Citrix StoreFront, cliquez sur **Créer un nouveau déploiement**.
 1. Spécifiez l'adresse URL du serveur StoreFront dans la case **URL de base**.
 2. Sur la page **Nom du magasin**, spécifiez un nom pour votre magasin, puis cliquez sur Suivant.
10. Sur la page **Delivery Controller**, indiquez l'infrastructure (les détails des services XenApp ou XenDesktop) qui fournit les ressources que vous souhaitez mettre à disposition dans le magasin. Vous pouvez entrer un serveur « fictif » ici ; cependant, aucune application ne s'affichera dans le magasin.
11. Définissez le **type de transport** et le **port**. Vous pouvez spécifier le protocole HTTP et le port 443 ; cliquez ensuite sur **OK**. Vous pouvez également copier les paramètres d'un déploiement existant de l'Interface Web ou de StoreFront.
12. Sur la page **Accès distant**, sélectionnez Aucun. Si vous utilisez NetScaler Gateway, sélectionnez Aucun tunnel VPN et entrez les détails de votre passerelle.
13. Sur la page **Accès distant**, sélectionnez Créer. Une fois que le magasin a été créé, cliquez sur Terminer.

Les utilisateurs peuvent désormais accéder au magasin via le site Citrix Receiver pour Web, ce qui leur permet d'accéder à leurs bureaux et applications via une page Web.

L'adresse URL permettant aux utilisateurs d'accéder au site Receiver pour Web du nouveau magasin s'affiche. For example : `example.net/Citrix/MarketingWeb/`. Ouvrez une session, vous verrez que vous avez accès à la nouvelle interface utilisateur de Citrix Receiver.



CEIP

Si vous choisissez de participer au Programme d'amélioration de l'expérience utilisateur (CEIP), des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour nous aider à améliorer la qualité et les performances des produits Citrix.

Par défaut, vous êtes automatiquement inscrit au programme CEIP lorsque vous installez StoreFront. Le premier chargement de données se produit approximativement sept jours après l'installation de StoreFront. Vous pouvez modifier cette valeur par défaut dans un paramètre de registre. Si vous modifiez le paramètre de registre avant d'installer StoreFront, cette valeur est utilisée. Si vous modifiez le paramètre de registre avant de mettre à niveau StoreFront, cette valeur est utilisée.

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 cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Paramètre de registre qui contrôle le chargement automatique des outils d'analyse (valeur par défaut=1) :

- Emplacement : HKLM:\Software\Citrix\Telemetry\CEIP
- Nom : Enabled
- Type : REG_DWORD
- Valeur : 0=désactivé, 1=activé

Par défaut, la propriété « Enabled » est masquée dans le registre. Si elle n'est pas spécifiée, la fonctionnalité de chargement automatique est activée.

L'applet de commande PowerShell suivante désactive l'inscription au programme CEIP :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0
```

Remarque : le paramètre de registre contrôle le chargement automatique des informations d'utilisation et des statistiques anonymes pour tous les composants sur le même serveur. Par exemple, si vous avez installé StoreFront sur le même serveur que le Delivery Controller et que vous décidez de ne pas prendre part au programme CEIP à l'aide du paramètre de Registre, ce choix s'appliquera aux deux composants.

Données CEIP collectées à partir de StoreFront

Le tableau suivant présente des exemples de types d'informations anonymes collectées. Les données ne contiennent aucun détail permettant d'identifier le client.

Données	Description
Version de StoreFront	Chaîne indiquant la version installée de StoreFront. Par exemple, « 3.8.0.0 »
Nombre de magasins	Compteur pour le nombre de magasins dans le déploiement.
Nombre de serveurs dans le groupe de serveurs	Compteur pour le nombre de serveurs dans le groupe de serveurs.
Nombre de Delivery Controller par magasin	Liste des valeurs numériques indiquant le nombre de Delivery Controller disponibles pour chaque magasin dans le déploiement.
HTTPS activé	Chaîne indiquant si le protocole https est activé pour le déploiement. « True » ou « False ».
Expérience classique activée pour Citrix Receiver	Liste des booléens indiquant si l'option « Expérience classique » est activée pour chaque Receiver pour Web. TRUE ou FALSE pour chaque Receiver pour Web.
Paramètre HTML5 pour Citrix Receiver	Liste des chaînes indiquant le paramètre de Receiver pour HTML5 pour chaque Receiver pour Web. « Always », « Fallback », « Off » pour chaque Receiver pour Web.

Contrôle de l'espace de travail activé pour Citrix Receiver	Liste des booléens indiquant si le « Contrôle de l'espace de travail » est activé pour chaque Receiver pour Web. TRUE ou FALSE pour chaque Receiver pour Web.
Accès à distance activé pour le magasin	Liste des chaînes indiquant si l'« Accès à distance » est activé pour chaque magasin du déploiement. « ENABLED » ou « DISABLED » pour chaque magasin.
Nombre de passerelles	Compteur du nombre de passerelles NetScaler Gateway configurées dans le déploiement.

Pour installer StoreFront à partir d'une invite de commandes

- Ouvrez une session sur le serveur StoreFront en utilisant un compte disposant d'autorisations d'administrateur local.
- Assurez-vous que toutes les conditions requises à l'installation de StoreFront sont remplies avant d'installer StoreFront. Référez-vous à [Avant l'installation et la configuration](#) pour plus de détails.
- En parcourant votre support d'installation ou après avoir téléchargé un pack, recherchez le fichier CitrixStoreFront-x64.exe, puis copiez-le à un emplacement temporaire du serveur.
- Depuis une invite de commandes, accédez au dossier contenant le fichier d'installation, puis saisissez la commande suivante.
`CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation] [-WINDOWS_CLIENT filelocationfilename.exe] [-MAC_CLIENT filelocationfilename.dmg]`
Utilisez l'argument `-silent` pour réaliser une installation silencieuse de StoreFront et de toutes les configurations requises. Par défaut, StoreFront est installé sur C:\Program Files\Citrix\Receiver StoreFront\. Toutefois, vous pouvez spécifier un autre emplacement d'installation à l'aide de l'argument `-INSTALLDIR`, où `installationlocation` est le répertoire dans lequel installer StoreFront. Veuillez noter que si vous souhaitez que le serveur fasse partie d'un groupe de serveurs StoreFront, l'emplacement d'installation de StoreFront et les paramètres des sites Web IIS, tels que le chemin d'accès physique et les ID de site, doivent être identiques.

Par défaut, si un site Citrix Receiver pour Web ne peut pas détecter Citrix Receiver sur une machine Windows ou Mac OS X, l'utilisateur est invité à télécharger et installer la version appropriée de Citrix Receiver pour sa plate-forme à partir du site Web de Citrix. Vous pouvez modifier ce comportement afin que les utilisateurs téléchargent les fichiers d'installation de Citrix Receiver à partir du serveur StoreFront plutôt que du site Web. Pour de plus amples informations, consultez la section [Mettre à disposition des fichiers d'installation Citrix Receiver sur le serveur](#).

Si vous envisagez de modifier cette configuration, spécifiez les arguments `-WINDOWS_CLIENT` et `-MAC_CLIENT` afin de copier les fichiers d'installation Citrix Receiver pour Windows et Citrix Receiver pour Mac, respectivement, sur l'emplacement approprié de votre déploiement StoreFront. Remplacez `filelocation` avec le répertoire contenant le fichier d'installation que vous voulez copier et `filename` avec le nom du fichier d'installation de Citrix Receiver. Les fichiers d'installation Citrix Receiver pour Windows et Citrix Receiver pour Mac sont inclus sur votre support d'installation StoreFront où le pack de téléchargement.

Mettre à niveau StoreFront

Pour mettre à niveau des déploiements de StoreFront 2.0 à StoreFront 3.0.x vers cette version de StoreFront, exécutez le fichier d'installation pour cette version de StoreFront. Les versions antérieures à StoreFront 2.0 ne peuvent pas être mises à niveau directement. Au lieu de cela, vous devez d'abord mettre à niveau StoreFront 1.2 vers StoreFront 2.0 avant de procéder à la mise à niveau vers cette version de StoreFront. Vous ne pouvez pas mettre à niveau StoreFront 1.1 vers cette version de StoreFront directement. Vous devez mettre à niveau StoreFront 1.1 vers StoreFront 1.2 puis vers StoreFront 2.0 avant de pouvoir mettre à niveau vers cette version de StoreFront.

Une fois le processus de mise à niveau démarré, il ne peut être annulé. Si la mise à niveau est interrompue ou ne peut pas être terminée, la configuration existante est supprimée, mais StoreFront n'est pas installé. Avant de commencer la mise à niveau, vous devez déconnecter les utilisateurs du déploiement StoreFront et empêcher les utilisateurs d'accéder aux serveurs durant la mise à niveau. Ceci garantit que tous les fichiers StoreFront sont accessibles par le programme d'installation lors de la mise à niveau. Si le programme d'installation ne peut pas accéder aux fichiers, ils ne peuvent pas être remplacés, ce qui entraîne l'échec de la mise à niveau et la suppression de la configuration de StoreFront. StoreFront ne prend pas en charge les déploiements sur plusieurs serveurs contenant différentes versions de produit, par conséquent tous les serveurs d'un groupe doivent être mis à jour vers la version mise à niveau avant de se voir accorder l'accès au déploiement. La mise à niveau simultanée n'est pas prise en charge pour les déploiements contenant de multiples serveurs ; les serveurs doivent être mis à niveau de manière séquentielle. Citrix vous recommande de sauvegarder vos données avant d'effectuer la mise à niveau.

La désinstallation de StoreFront supprime le service d'authentification, les magasins, les abonnements aux applications, les sites Citrix Receiver pour Web, les sites Desktop Appliance et les adresses URL des sites XenApp Services. Ceci signifie que si vous décidez de désinstaller StoreFront, vous devez recréer manuellement vos services, magasins et sites lorsque vous réinstallez StoreFront. La mise à niveau vous permet également de préserver votre configuration StoreFront ainsi que les données d'abonnement aux applications si bien que les utilisateurs n'ont pas besoin de se réabonner à toutes leurs applications.

La mise à niveau de la version du système d'exploitation sur un serveur exécutant StoreFront n'est pas prise en charge. Citrix vous recommande d'installer StoreFront sur une nouvelle installation du système d'exploitation.

Important

Avant de commencer la mise à niveau du groupe :

- Fermez toutes les autres applications sur le serveur StoreFront.
- Fermez toutes les lignes de commande et les fenêtres de PowerShell.

Pour mettre à niveau StoreFront version 2.0 à 3.0.x vers cette version de StoreFront

- Désactivez l'accès au déploiement via l'environnement d'équilibrage de charge. La désactivation de l'URL d'équilibrage de charge empêche les utilisateurs de se connecter au déploiement lors de la mise à niveau.
- Sauvegardez tous les serveurs dans le groupe de serveurs.
- Retirez l'un des serveurs du groupe de serveurs existant.
- Redémarrez le serveur que vous avez retiré.
Veuillez noter que vous pouvez utiliser un équilibrage de charge parallèle pour vérifier le nouveau groupe de serveurs à mesure que vous le créez. La variante qui permet de maximiser la disponibilité et de réduire les risques implique de retirer et de ne mettre à niveau qu'un seul serveur du groupe de serveurs d'origine. Vous pouvez ensuite créer le nouveau groupe à partir

de nouvelles machines plutôt que de machines provenant du groupe de serveurs d'origine.

5. Mettez à niveau le serveur que vous avez retiré à l'aide d'un compte d'administration n'exécutant aucune autre installation et un nombre minimum d'autres applications.
6. Vérifiez que le serveur que vous avez retiré a été mis à niveau avec succès.
7. Retirez de l'équilibrage de charge un autre des serveurs du groupe de serveurs existant.
8. Redémarrez le serveur que vous avez retiré pour les mêmes raisons que celles indiquées à l'étape 1.
9. Désinstallez la version actuellement installée de StoreFront et installez la nouvelle version de StoreFront.
10. Associez le serveur nouvellement installé à un nouveau groupe de serveurs composé de tous les serveurs mis à niveau et des serveurs récemment installés, et vérifiez qu'ils fonctionnent correctement.
11. Répétez les étapes 3 à 10 jusqu'à ce que la capacité du nouveau groupe de serveurs soit suffisante pour qu'il puisse remplacer l'ancien groupe de serveurs, pointez l'équilibrage de charge vers le nouveau groupe de serveurs et vérifiez qu'il fonctionne correctement.
12. Répétez les étapes 3 à 10 pour les serveurs restants, en les ajoutant un à un à l'équilibrage de charge après chaque mise à niveau réussie.

Conseil

- Si vous souhaitez maximiser la disponibilité, vous pouvez maintenir l'accès au groupe de serveurs d'origine durant le processus de mise à niveau jusqu'à ce que le nouveau groupe de serveurs soit disponible. Pour ce faire :
 1. Ignorez l'étape 1.
 2. Modifiez l'étape 11 pour désactiver l'accès au groupe de serveurs d'origine à l'aide de l'équilibrage de charge. Exportez les données d'abonnement du groupe de serveurs d'origine et importez-les dans le nouveau groupe de serveurs. Activez l'accès au nouveau groupe de serveurs à l'aide de l'équilibrage de la charge.

Cela garantit que les modifications apportées à l'abonnement par les utilisateurs après l'étape 3 et avant l'étape 11 sont disponibles dans le nouveau groupe de serveurs.

- Vous pouvez maximiser davantage la disponibilité en ne retirant qu'un seul serveur du groupe de serveurs d'origine et en le mettant à niveau, puis en créant le nouveau groupe de serveurs à l'aide de nouveaux serveurs plutôt que de serveurs retirés du groupe de serveurs d'origine. Une fois le nouveau groupe de serveurs en production, vous pouvez retirer les anciens serveurs.

Configurer StoreFront

Lors du premier démarrage de la console de gestion Citrix StoreFront, deux options sont disponibles.

- **Créer un nouveau déploiement.** Configurez le premier serveur StoreFront dans un nouveau déploiement StoreFront. Les déploiements sur un seul serveur sont particulièrement adaptés à l'évaluation de StoreFront ou aux déploiements de production de petite taille. Une fois que vous avez configuré votre premier serveur StoreFront, vous pouvez ajouter plus de serveurs au groupe à tout moment pour augmenter la capacité de votre déploiement.
- **Joindre un groupe de serveurs existant.** Ajoutez un autre serveur à un déploiement StoreFront. Sélectionnez cette option pour augmenter rapidement la capacité de votre déploiement StoreFront. L'équilibrage de charge externe est requis pour les déploiements comprenant plusieurs serveurs. Pour ajouter un nouveau serveur, vous devez pouvoir accéder à un serveur existant du déploiement.

Désinstaller StoreFront

En plus du produit lui-même, la désinstallation de StoreFront supprime le service d'authentification, les magasins, les sites Citrix Receiver pour Web, les sites Desktop Appliance et les adresses URL XenApp Services ainsi que les configurations associées à ces composants. Le Subscription Store Service contenant les données d'abonnement des applications est également supprimé. Dans les déploiements sur un serveur unique, cela signifie que les détails des abonnements aux applications sont perdus. Toutefois, dans les déploiements contenant de multiples serveurs, ces données sont conservées sur les autres serveurs dans le groupe. Les composants activés par le programme d'installation de StoreFront, tels que les fonctionnalités .NET Framework et les services de rôle de serveur Web (IIS), ne sont pas supprimés du serveur lors de la désinstallation de StoreFront.

1. Ouvrez une session sur le serveur StoreFront en utilisant un compte disposant d'autorisations d'administrateur local.
2. Sur l'écran **Démarrer** de Windows ou l'écran Applications, accédez à **Citrix StoreFront**. Cliquez avec le bouton droit sur la vignette et cliquez sur **Désinstaller**.
3. Dans la boîte de dialogue **Programmes et fonctionnalités**, sélectionnez **Citrix StoreFront** et cliquez sur **Désinstaller** pour supprimer tous les composants StoreFront du serveur.
4. Dans la boîte de dialogue **Désinstaller Citrix StoreFront**, cliquez sur **Oui**. Une fois la désinstallation terminée, cliquez sur **OK**.

Créer un nouveau déploiement

Jun 30, 2017

1. Si la console de gestion Citrix StoreFront n'est pas déjà ouverte après installation de StoreFront, sur l'écran Démarrer de Windows où l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Dans le panneau des résultats de la console de gestion de Citrix StoreFront, cliquez sur Créer un nouveau déploiement.
3. Spécifiez l'URL du serveur StoreFront ou de l'environnement d'équilibrage de charge pour un déploiement comprenant de multiples serveurs dans la case URL de base.

Si vous n'avez pas encore configuré votre environnement d'équilibrage de charge, entrez l'adresse URL du serveur. Vous pouvez modifier l'URL de base de votre déploiement à tout moment.

Vous pouvez passer de HTTP à HTTPS à tout moment à l'aide de la tâche Changer l'URL de base dans la console de gestion StoreFront, à condition que Microsoft Internet Information Services (IIS) soit configuré pour HTTPS.

4. Cliquez sur Suivant pour configurer le service d'authentification, qui permet d'authentifier les utilisateurs sur Microsoft Active Directory.

Pour utiliser le protocole HTTPS de manière à sécuriser les communications entre StoreFront et les machines des utilisateurs, vous devez configurer Microsoft Internet Information Services (IIS) pour HTTPS. En l'absence de la configuration IIS appropriée, StoreFront utilise le protocole HTTP pour les communications.

Par défaut, Citrix Receiver requiert des connexions HTTPS pour les magasins. Si StoreFront n'est pas configuré pour le protocole HTTPS, les utilisateurs doivent effectuer des étapes de configuration supplémentaires pour utiliser les connexions HTTP. HTTPS est requis pour l'authentification par carte à puce. Vous pouvez passer de HTTP à HTTPS à tout moment après la configuration de StoreFront, dans la mesure où la configuration IIS appropriée a été implémentée. Pour plus d'informations, veuillez consulter la section [Configurer des groupes de serveurs](#).

Vous pouvez passer de HTTP à HTTPS à tout moment à l'aide de la tâche **Changer l'URL de base** dans la console de gestion StoreFront, à condition que Microsoft Internet Information Services (IIS) soit configuré pour HTTPS.

5. Sur la page Nom du magasin, spécifiez un nom pour votre magasin, indiquez si vous voulez autoriser uniquement des utilisateurs non authentifiés (anonymes) à accéder au magasin, puis cliquez sur Suivant.
Les magasins StoreFront regroupent les bureaux et les applications pour les mettre à disposition des utilisateurs. Les noms des magasins s'affichent dans Citrix Receiver sous les comptes des utilisateurs, c'est la raison pour laquelle vous devez choisir un nom qui permette aux utilisateurs d'identifier le contenu du magasin.
6. Sur la page Controller, indiquez l'infrastructure fournissant les ressources que vous souhaitez mettre à disposition dans le magasin. Pour ajouter des bureaux et des applications au magasin, suivez la procédure appropriée ci-dessous. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop, XenApp et XenMobile (App Controller). Répétez les procédures, si nécessaire, pour ajouter tous les déploiements fournissant des ressources au magasin.
 - [Ajouter des ressources XenDesktop et XenApp au magasin](#)
 - [Ajouter des applications App Controller au magasin](#)
7. Une fois que vous avez ajouté toutes les ressources requises pour le magasin, sur la page Controller, cliquez sur Suivant.
8. Sur la page Accès distant, spécifiez si les utilisateurs se connectant depuis des réseaux publics (et la manière dont ils se connectent) peuvent accéder aux ressources internes.
 - Pour mettre le magasin à la disposition des utilisateurs sur des réseaux publics, sélectionnez la case à cocher **Activer l'accès à distance**. Si vous laissez cette case désactivée, seuls les utilisateurs locaux sur le réseau interne peuvent

accéder au magasin.

- Pour ne mettre à disposition que les ressources disponibles au travers du magasin via NetScaler Gateway, sélectionnez **Autoriser les utilisateurs à accéder uniquement aux ressources mises à disposition via StoreFront (Aucun tunnel VPN)**.
- Pour mettre le magasin et les autres ressources du réseau interne à disposition via un tunnel de réseau privé virtuel SSL (VPN), sélectionnez **Autoriser les utilisateurs à accéder à toutes les ressources du réseau interne (Tunnel VPN complet)**. Les utilisateurs peuvent avoir besoin de NetScaler Gateway Plug-in pour établir le tunnel VPN.

Si vous configurez l'accès distant au magasin au travers de NetScaler Gateway, la méthode d'authentification pass-through via depuis NetScaler Gateway est automatiquement activée. Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

9. Si vous avez activé l'accès à distance, répertoriez les déploiements NetScaler Gateway au travers desquels les utilisateurs peuvent accéder au magasin. Pour ajouter un déploiement NetScaler Gateway approprié, suivez la procédure ci-dessous. Répétez les procédures, si nécessaire, pour ajouter d'autres déploiements.
 - [Fournir l'accès distant au magasin via un boîtier NetScaler Gateway](#)
 - [Fournir l'accès distant au magasin via un cluster Access Gateway 5.0](#)
10. Une fois que vous avez ajouté tous vos déploiements NetScaler Gateway, sélectionnez dans la liste Boîtiers NetScaler Gateway les déploiements par le biais desquels les utilisateurs peuvent accéder au magasin. Si vous activez l'accès au travers de plusieurs déploiements, spécifiez le déploiement par défaut à utiliser pour accéder au magasin. Cliquez sur **Suivant**.
11. Sur la page **Méthodes d'authentification**, sélectionnez les méthodes que vos utilisateurs peuvent utiliser pour s'authentifier auprès du magasin et cliquez sur **Suivant**. Vous pouvez sélectionner l'une des méthodes suivantes :
 - **Nom d'utilisateur et mot de passe** : les utilisateurs saisissent leurs informations d'identification et sont authentifiés lorsqu'ils accèdent à leurs magasins.
 - **Authentification SAML** : les utilisateurs s'authentifient auprès d'un fournisseur d'identité et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.
 - **Authentification pass-through au domaine** : les utilisateurs s'authentifient sur leurs ordinateurs Windows membres d'un domaine et leurs informations d'identification sont utilisées pour ouvrir une session automatiquement lorsqu'ils accèdent à leurs magasins.
 - **Carte à puce** : les utilisateurs doivent s'authentifier à l'aide de cartes à puce et de codes PIN lorsqu'ils accèdent à leurs magasins.
 - **HTTP basique** : les utilisateurs s'authentifient avec le serveur Web IIS du serveur StoreFront.
 - **Authentification pass-through via NetScaler Gateway** : les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Cette option est automatiquement activée lorsque l'accès distant est activé.

12. Sur la page **URL XenApp Services**, configurez l'adresse URL XenApp Services pour les utilisateurs qui utilisent PNAgent pour accéder aux applications et bureaux.

13. Après avoir créé le magasin, d'autres options vous sont alors proposées via la console de gestion de Citrix StoreFront. Pour plus d'informations, consultez les [différents articles sur la gestion](#).

Les utilisateurs peuvent désormais accéder à votre magasin avec Citrix Receiver, qui doit être configuré avec les détails d'accès au magasin. Il existe plusieurs méthodes vous permettant de fournir ces détails aux utilisateurs afin de faciliter le processus de configuration. Pour plus d'informations, veuillez consulter la section [Options d'accès utilisateur](#).

Éventuellement, les utilisateurs peuvent accéder au magasin via le site Citrix Receiver pour Web, ce qui leur permet d'accéder

à leurs bureaux et applications via une page Web. L'adresse URL permettant aux utilisateurs d'accéder au site Citrix Receiver pour Web du nouveau magasin s'affiche lorsque vous créez le magasin.

Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services est activée par défaut. Les utilisateurs équipés de boîtiers de bureau membres du domaine et de PC réaffectés qui exécutent Citrix Desktop Lock, ainsi que les utilisateurs disposant de clients Citrix plus anciens qui ne peuvent pas être mis à niveau, peuvent accéder aux magasins directement à l'aide de l'adresse URL XenApp Services du magasin. L'adresse URL XenApp Services s'affiche au format `http[s]://adresseserveur/Citrix/nomdumagasin/PNAgent/config.xml`, où `adresseserveur` est le nom de domaine complet du serveur ou de l'environnement d'équilibrage de charge de votre déploiement StoreFront et `nomdumagasin` le nom spécifié pour le magasin à l'étape 5.

Vous pouvez rapidement ajouter d'autres serveurs à votre déploiement en sélectionnant l'option permettant de [rejoindre un groupe de serveurs existant](#) lors de l'installation d'autres instances de StoreFront.

Ajouter des ressources XenDesktop et XenApp au magasin

Suivez les étapes suivantes pour mettre des bureaux et applications fournis par XenApp et XenDesktop à disposition dans le magasin que vous créez dans le cadre de la configuration initiale de votre serveur StoreFront. Vous êtes supposé avoir effectué les étapes 1 à 6 de la procédure « Créer un nouveau déploiement » en haut de cet article.

1. Sur la page Controller de l'assistant Créer un magasin, cliquez sur Ajouter.
2. Dans la boîte de dialogue Ajouter Delivery Controller, spécifiez un nom qui vous aidera à identifier le déploiement et indiquez si les ressources que vous souhaitez mettre à disposition dans le magasin sont fournies par XenDesktop, XenApp ou XenMobile.
3. Ajoutez les noms ou les adresses IP de vos serveurs à la liste Serveurs. Spécifiez plusieurs serveurs pour activer la tolérance aux pannes en dressant la liste des entrées par ordre de priorité pour définir le basculement. Pour les sites XenDesktop, spécifiez les détails des Controller. Dans le cas de batteries XenApp, dressez la liste des serveurs exécutant le service XML Citrix.
4. Sélectionnez dans la liste Type de transport, le type de connexion que StoreFront utilisera pour les communications avec les serveurs.
 - Pour envoyer des données via des connexions non cryptées, sélectionnez HTTP. Si vous sélectionnez cette option, vous devez prendre vos propres dispositions pour sécuriser les connexions entre StoreFront et vos serveurs.
 - Pour envoyer des données via des connexions HTTP sécurisées à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security), sélectionnez HTTPS. Si vous sélectionnez cette option pour les serveurs XenDesktop et XenApp, vérifiez que le service XML Citrix est configuré pour partager son port avec les services Microsoft Internet Information Services (IIS) et que ces derniers sont configurés pour prendre en charge le protocole HTTPS.
 - Pour envoyer des données via des connexions sécurisées sur les serveurs XenApp à l'aide du Relais SSL pour effectuer une authentification hôte et le cryptage de données, sélectionnez Relais SSL.

Remarque : si vous utilisez le protocole HTTPS ou le Relais SSL pour sécuriser les connexions entre StoreFront et vos serveurs, vérifiez que les noms que vous spécifiez dans la liste Serveurs correspondent exactement (casse comprise) aux noms figurant sur les certificats de ces serveurs.

5. Spécifiez le port StoreFront à utiliser pour les connexions aux serveurs. Le port par défaut est 80 pour les connexions utilisant le protocole HTTP et le Relais SSL, et 443 pour les connexions HTTPS. Dans le cas de serveurs XenDesktop et XenApp, le port spécifié doit être le port utilisé par le service XML Citrix.
6. Si vous utilisez le Relais SSL pour sécuriser les connexions entre StoreFront et des serveurs XenApp, indiquez le port TCP du Relais SSL dans la zone Port du Relais SSL. Le port par défaut est le port 443. Assurez-vous que tous les serveurs exécutant le Relais SSL sont configurés pour surveiller le même port.

Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements

XenDesktop, XenApp et XenMobile. Pour ajouter d'autres sites XenDesktop ou batteries XenApp, répétez la procédure ci-dessus. Pour mettre des applications gérées par App Controller à disposition dans le magasin, suivez les étapes de la section [Ajouter des applications App Controller au magasin](#). Après avoir ajouté toutes les ressources requises au magasin, retournez à l'étape 7 de la procédure « Créer un nouveau déploiement » en haut de cet article.

Ajouter des applications App Controller au magasin

Effectuez les étapes suivantes pour mettre à disposition des applications gérées par App Controller dans le magasin que vous créez dans le cadre de la configuration initiale de votre serveur StoreFront. Vous êtes supposé avoir effectué les étapes 1 à 6 de la procédure « Créer un nouveau déploiement » en haut de cet article.

1. Sur la page Delivery Controller de l'assistant Créer un magasin, cliquez sur Ajouter.
2. Dans la boîte de dialogue Ajouter Delivery Controller, spécifiez un nom qui vous aidera à identifier le boîtier virtuel App Controller qui gère les applications que vous souhaitez mettre à disposition dans le magasin. Assurez-vous que le nom ne contienne pas d'espaces. Sélectionnez AppController.
3. Entrez le nom ou l'adresse IP du boîtier virtuel App Controller dans la boîte de dialogue Serveur et spécifiez le port StoreFront à utiliser pour les connexions à App Controller. Le port par défaut est le port 443.

Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop, XenApp et App Controller. Pour ajouter des applications gérées par d'autres boîtiers virtuels App Controller, répétez la procédure ci-dessus. Pour mettre à disposition des bureaux et applications fournis par XenDesktop et XenApp dans le magasin, suivez les étapes de la section [Ajouter des ressources XenDesktop et XenApp au magasin](#). Après avoir ajouté toutes les ressources requises au magasin, retournez à l'étape 7 de la procédure « Créer un nouveau déploiement » en haut de cet article.

Fournir l'accès distant au magasin via un boîtier NetScaler Gateway

Effectuez les étapes suivantes pour configurer l'accès distant via un boîtier NetScaler Gateway au magasin que vous créez dans le cadre de la configuration initiale de votre serveur StoreFront. Vous êtes supposé avoir effectué les étapes 1 à 9 de la procédure « Créer un nouveau déploiement » en haut de cet article.

1. Sur la page Accès distant de l'interface Créer un magasin de la console StoreFront, cliquez sur Ajouter.
2. Dans la boîte de dialogue Ajouter un boîtier NetScaler Gateway, spécifiez un nom pour le boîtier qui permettra aux utilisateurs de l'identifier.
Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans Citrix Receiver. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser ce boîtier. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements NetScaler Gateway pour permettre aux utilisateurs d'identifier facilement le déploiement le plus pratique en fonction de leur situation.
3. Entrez l'URL du serveur virtuel ou le point d'ouverture de session utilisateur (pour Access Gateway 5.0) de votre boîtier. Spécifiez la version du produit utilisé dans votre déploiement.
Pour de plus amples informations sur la création d'un seul nom de domaine complet (FQDN) pour accéder à un magasin en interne et externe, consultez la section [Créer un seul nom de domaine complet \(FQDN\) pour accéder à un magasin en interne et externe](#).
4. Si vous ajoutez un boîtier Access Gateway 5.0, sélectionnez Boîtier dans la liste Mode de déploiement. Sinon, spécifiez l'adresse IP de sous-réseau du boîtier NetScaler Gateway, si nécessaire. Une adresse IP de sous-réseau est requise pour les boîtiers Access Gateway 9.3, mais facultative pour les versions plus récentes du produit.
L'adresse de sous-réseau correspond à l'adresse IP que NetScaler Gateway utilise pour représenter la machine utilisateur

dans les communications avec les serveurs sur le réseau interne. Il peut également s'agir de l'adresse IP mappée du boîtier NetScaler Gateway. Lorsque cela est spécifié, StoreFront utilise l'adresse IP du sous-réseau pour vérifier que les requêtes entrantes proviennent d'une machine approuvée.

5. Si vous ajoutez un boîtier exécutant NetScaler Gateway 10.1, Access Gateway 10 ou Access Gateway 9.3, sélectionnez dans la liste Type d'ouverture de session la méthode d'authentification que vous avez configurée sur le boîtier pour les utilisateurs de Citrix Receiver.

Les informations que vous fournissez sur la configuration de votre boîtier NetScaler Gateway sont ajoutées au fichier de provisioning pour le magasin. Ceci permet à Citrix Receiver d'envoyer une demande de connexion appropriée lorsque vous contactez le boîtier pour la première fois.

- Si les utilisateurs sont tenus de saisir leurs informations d'identification de domaine Microsoft Active Directory, sélectionnez Domaine.
- Si les utilisateurs sont tenus de saisir un code de jeton obtenu à partir d'un jeton de sécurité, sélectionnez Jeton de sécurité.
- Si les utilisateurs sont tenus de saisir leurs identifiants de domaine et un code de jeton obtenu à partir d'un jeton de sécurité, sélectionnez Domaine et jeton de sécurité.
- Si les utilisateurs sont tenus de saisir un mot de passe ponctuel envoyé par SMS, sélectionnez Authentification SMS.
- Si les utilisateurs sont tenus de présenter une carte à puce et d'entrer un code PIN, sélectionnez Carte à puce.

Si vous configurez l'authentification avec carte à puce avec une méthode d'authentification secondaire sur laquelle les utilisateurs peuvent se rabattre s'ils rencontrent des problèmes avec leur carte à puce, sélectionnez la méthode d'authentification secondaire dans la liste Carte à puce de remplacement.

6. Renseignez l'adresse URL du service d'authentification de NetScaler Gateway dans la case URL de rappel. StoreFront ajoute automatiquement la partie standard de l'URL. Cliquez sur Suivant.

Entrez l'adresse URL du boîtier accessible en interne. StoreFront contacte le service d'authentification NetScaler Gateway pour vérifier que les requêtes reçues de NetScaler Gateway proviennent de ce boîtier.

7. Si vous mettez les ressources fournies par XenDesktop ou XenApp à disposition dans le magasin, répertoriez les adresses URL des serveurs qui exécutent la STA sur la page Secure Ticket Authority (STA). Saisissez les adresses URL de plusieurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs par ordre de priorité pour définir la séquence de basculement.

La STA est hébergée sur les serveurs XenDesktop et XenApp, et émet des tickets de session en réponse à des demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources XenDesktop et XenApp.

8. Si vous souhaitez que XenDesktop et XenApp laissent les sessions déconnectées ouvertes lorsque Citrix Receiver tente de se reconnecter automatiquement, cochez la case Activer la fiabilité de session. Si vous avez configuré plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, cochez la case Demander des tickets de deux STA, si possible.

Lorsque la case Demander des tickets de deux STA, si possible est cochée, StoreFront obtient des tickets de deux STA différentes de façon à ce que les sessions utilisateur ne soient pas interrompues si l'une des STA devenait indisponible au cours de la session. Si pour une raison quelconque, StoreFront ne parvient pas à contacter deux STA, il en utilise une seule.

9. Cliquez sur Créer pour ajouter votre déploiement NetScaler Gateway à la liste sur la page Accès distant.

Pour ajouter d'autres déploiements, répétez la procédure ci-dessus. Pour configurer l'accès distant au magasin via un cluster Access Gateway 5.0, suivez les étapes de la section [Fournir l'accès distant au magasin via un cluster Access Gateway 5.0](#).

Après avoir ajouté tous vos déploiements NetScaler Gateway, retournez à l'étape 10 de la procédure « Créer un nouveau déploiement » en haut de cet article.

Fournir l'accès distant au magasin via un cluster Access Gateway 5.0

Effectuez les étapes suivantes pour configurer l'accès distant via un cluster Access Gateway 5.0 au magasin que vous créez dans le cadre de la configuration initiale de votre serveur StoreFront. Vous êtes supposé avoir effectué les étapes 1 à 9 de la procédure « Créer un nouveau déploiement » en haut de cet article.

1. Sur la page Accès distant de l'interface Créer un magasin de la console StoreFront, cliquez sur Ajouter.
2. Dans la boîte de dialogue Ajouter un boîtier NetScaler Gateway, spécifiez un nom pour le cluster qui permettra aux utilisateurs de l'identifier.
Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans Citrix Receiver. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser ce cluster. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements NetScaler Gateway pour permettre aux utilisateurs d'identifier facilement le déploiement le plus pratique en fonction de leur situation.
3. Entrez l'adresse URL du point d'ouverture de session de l'utilisateur pour votre cluster et sélectionnez dans la liste la Version 5.x.
4. À partir de la liste Mode de déploiement, sélectionnez Access Controller et cliquez sur Suivant.
5. Sur la page Boîtiers, dressez la liste des adresses IP ou des noms de domaine complets des boîtiers dans le cluster et cliquez sur Suivant.
6. Sur la page Activer l'authentification silencieuse, dressez la liste des adresses URL du service d'authentification exécuté sur les serveurs Access Controller. Ajoutez les adresses URL de plusieurs serveurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs par ordre de priorité pour définir la séquence de basculement. Cliquez sur Suivant.
StoreFront utilise le service d'authentification pour authentifier les utilisateurs distants afin de leur éviter de ressaisir leurs informations d'identification lorsqu'ils accèdent aux magasins.
7. Si vous mettez les ressources fournies par XenDesktop et XenApp à disposition dans le magasin, répertoriez les adresses URL des serveurs qui exécutent la STA sur la page Secure Ticket Authority (STA). Saisissez les adresses URL de plusieurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs par ordre de priorité pour définir la séquence de basculement.
La STA est hébergée sur les serveurs XenDesktop et XenApp, et émet des tickets de session en réponse à des demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources XenDesktop et XenApp.
8. Si vous souhaitez que XenDesktop et XenApp laissent les sessions déconnectées ouvertes lorsque Citrix Receiver tente de se reconnecter automatiquement, cochez la case Activer la fiabilité de session. Si vous avez configuré plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, cochez la case Demander des tickets de deux STA, si possible.
Lorsque la case Demander des tickets de deux STA, si possible est cochée, StoreFront obtient des tickets de deux STA différentes de façon à ce que les sessions utilisateur ne soient pas interrompues si l'une des STA devenait indisponible au cours de la session. Si pour une raison quelconque, StoreFront ne parvient pas à contacter deux STA, il en utilise une seule.
9. Cliquez sur Créer pour ajouter votre déploiement NetScaler Gateway à la liste sur la page Accès distant.

Pour ajouter d'autres clusters, répétez la procédure ci-dessus. Pour configurer l'accès distant au magasin via NetScaler

Gateway 10.1, Access Gateway 10, Access Gateway 9.3, ou un seul boîtier Access Gateway 5.0, suivez les étapes de l'étape de la section [Fournir l'accès distant au magasin via un boîtier NetScaler Gateway](#). Après avoir ajouté tous vos déploiements NetScaler Gateway, retournez à l'étape 10 de la procédure « Créer un nouveau déploiement » en haut de cet article.

Joindre un groupe de serveurs existant

Jun 30, 2017

Avant d'installer StoreFront, assurez-vous que le serveur que vous ajoutez au groupe exécute la même version du système d'exploitation avec les mêmes paramètres régionaux que les autres serveurs du groupe. Les groupes de serveurs StoreFront contenant diverses versions de système d'exploitation et de paramètres régionaux ne sont pas pris en charge. Bien qu'un groupe de serveurs puisse contenir jusqu'à cinq serveurs, d'un point de vue de la capacité, les simulations ont démontré qu'aucun avantage ne découlait de l'utilisation de groupes de serveurs contenant plus de trois serveurs. En outre, vérifiez que le chemin d'accès relatif à StoreFront dans IIS sur le serveur que ajoutez est le même que sur les autres serveurs du groupe.

Important

lorsque vous ajoutez un nouveau serveur à un groupe de serveurs, les comptes de service StoreFront sont ajoutés en tant que membres du groupe d'administrateurs locaux sur le nouveau serveur. Ces services requièrent des autorisations d'administrateur local pour devenir membre et se synchroniser avec le groupe de serveurs. Si vous utilisez une stratégie de groupe pour empêcher l'ajout de nouveaux membres au groupe d'administrateurs locaux ou que vous limitez les autorisations du groupe d'administrateurs locaux sur vos serveurs, StoreFront ne peut pas s'associer à un groupe de serveurs.

1. Si la console de gestion Citrix StoreFront n'est pas ouverte après l'installation de StoreFront, sur l'écran Démarrer de Windows où l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Dans le panneau des résultats de la console de gestion Citrix StoreFront, cliquez sur Joindre un groupe de serveurs existant.
3. Ouvrez une session sur un serveur du déploiement StoreFront que vous souhaitez rejoindre et ouvrez la console de gestion Citrix StoreFront. Sélectionnez le nœud Groupe de serveurs dans le panneau gauche de la console puis, dans le panneau Actions, cliquez sur Ajouter un serveur. Notez le code d'autorisation qui s'affiche.
4. Retournez sur le nouveau serveur et, dans la boîte de dialogue Joindre groupe de serveurs, spécifiez le nom du serveur existant dans la zone Serveur d'autorisation. Saisissez le code d'autorisation que vous avez obtenu auprès de ce serveur, puis cliquez sur Joindre.
Une fois joint au groupe, la configuration du nouveau serveur est mise à jour pour correspondre à la configuration du serveur existant. Tous les autres serveurs du groupe sont mis à jour avec les détails du nouveau serveur.

Pour gérer un déploiement contenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Toutes les modifications de configuration que vous effectuez doivent être propagées aux autres serveurs du groupe pour garantir une configuration homogène sur l'ensemble du déploiement.

Supprimer un serveur d'un groupe de serveurs

Si un serveur StoreFront était membre d'un groupe de serveurs et a été supprimé, vous devez exécuter l'applet de commande PowerShell Clear-DSCConfiguration pour restaurer l'état par défaut du serveur StoreFront. Après avoir exécuté l'applet de commande Clear-DSCConfiguration sur le serveur déconnecté, vous pouvez de nouveau ajouter le serveur à un groupe de serveurs existant ou à un différent groupe de serveurs nouvellement créé.

1. Ouvrez la console d'administration StoreFront sur le serveur StoreFront principal que vous utilisez pour gérer votre groupe de serveurs entier.

2. Sélectionnez le nœud du groupe de serveurs sur le panneau de gauche et choisissez un autre serveur à supprimer.
3. Supprimez le serveur sélectionné du groupe de serveurs.
4. Dans le panneau Actions, propagez les modifications à partir du serveur que vous avez utilisé pour déconnecter l'un des membres de votre groupe de serveurs. Tous les autres membres du groupe de serveurs savent maintenant qu'un serveur a été supprimé du groupe. Tant que vous ne restaurez pas l'état par défaut du serveur déconnecté, ce dernier ne sait pas qu'il n'est plus membre du groupe.
5. Fermez la console d'administration sur le serveur déconnecté.
6. Ouvrez une session PowerShell sur votre serveur déconnecté après qu'il ait été supprimé du groupe et importez les modules PowerShell StoreFront à l'aide de :&
`"$Env:PROGRAMFILES\Citrix\ReceiverStoreFront\Scripts\ImportModules.ps1"`
7. Exécutez la commande Clear-DSConfiguration, qui restaure les paramètres par défaut du serveur.
8. Ouvrez la console d'administration StoreFront et le serveur déconnecté est restauré et prêt à être ajouté à un autre groupe de serveurs.

Migrer les fonctionnalités de l'Interface Web vers StoreFront

Jun 30, 2017

La plupart des personnalisations de l'Interface Web ont des équivalents dans StoreFront par le biais d'ajustements JavaScript, d'API publiées par Citrix ou de la console de gestion StoreFront.

Ce tableau contient une vue d'ensemble des personnalisations et des informations de base sur la manière de les réaliser.

Emplacements des dossiers

- Pour les personnalisations de script, ajoutez les exemples au fichier script.js qui se trouve dans

C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- Pour la personnalisation de style, ajoutez l'exemple au fichier style.css qui se trouve dans

C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- Pour le contenu dynamique, ajoutez le contexte dynamique à un fichier texte dans

C:\inetpub\wwwroot\Citrix\StoreNameWeb\customweb

- Si vous disposez d'un déploiement à plusieurs serveurs, vous pouvez répliquer les modifications vers d'autres serveurs depuis la console d'administration StoreFront ou à l'aide de PowerShell.

Remarque : l'Interface Web permettait aux utilisateurs de personnaliser plusieurs paramètres. Actuellement, StoreFront ne propose pas cette capacité, et s'il est possible d'ajouter des personnalisations plus importantes pour prendre en charge cette fonctionnalité, il ne s'agit pas de l'objet de cet article.

Fonctionnalité de l'Interface Web	Équivalent StoreFront
Personnalisation avec la console de gestion	
<ul style="list-style-type: none">• Disposition-Graphiques simplifiés• Disposition-Graphiques avancés• Autoriser les utilisateurs à choisir	Sans objet. StoreFront détecte automatiquement et adapte l'interface utilisateur à l'écran de l'appareil.
<ul style="list-style-type: none">• Activer la recherche• Désactiver la recherche	<ul style="list-style-type: none">• La recherche est activée par défaut.• Désactiver. Pour masquer les zones de recherche sur le bureau ou l'interface Web, ajoutez le style suivant au fichier style.css : .search-container { display: none;

	<pre> } Pour masquer les zones de recherche sur l'interface utilisateur du téléphone, ajoutez : #searchBtnPhone { display: none; } </pre>
Activer l'actualisation	Activée par défaut (actualisation du navigateur).
Activer le retour au dernier dossier	<p>Non activé par défaut.</p> <p>Activer le retour au dernier dossier - Pour mémoriser le dossier actuel et y retourner au moment du chargement, ajoutez la ligne suivante au fichier script.js :</p> <pre> CTXS.Extensions.afterDisplayHomeScreen = function () { // vérifier si la vue a été enregistrée la dernière fois CTXS.ExtensionAPI.localStorageGetItem("view", function (view) { if (view) { // si la vue a été enregistrée, y retourner CTXS.ExtensionAPI.changeView(view); } if (view == "store") { // si la vue est magasin, vérifier si dossier a été enregistré CTXS.ExtensionAPI.localStorageGetItem("folder", function(folder) { if (folder != "") { // si le dossier a été enregistré, y retourner CTXS.ExtensionAPI.navigateToFolder(folder); } } } } } </pre>

```

    );
}

// configurer le contrôle de dossier
CTXS.Extensions.onFolderChange = function(folder) {

    CTXS.ExtensionAPI.localStorageSetItem("folder",

        folder);

};

// configurer le contrôle de la vue
CTXS.Extensions.onViewChange = function(newview) {

    // ne pas conserver les vues de recherche ou d'informations
    d'application

    // au lieu de cela, mémoriser la vue parent .

    if ((newview != "appinfo") &&

        (newview != "search")) {

        CTXS.ExtensionAPI.localStorageSetItem(

            "view", newview);

        }

    };

});

};

```

Activer les conseils

Citrix Receiver utilise très peu les info-bulles, car il cible les appareils tactiles et non tactiles. Vous pouvez ajouter des info-bulles à l'aide d'un script personnalisé.

- Affichage Icônes
- Affichage Arborescence
- Affichage Détails
- Affichage Liste
- Affichage Groupe
- Définir l'affichage par défaut
- Affichage Icônes (Graphiques simplifiés)
- Affichage Liste (Graphiques simplifiés)

L'interface utilisateur de Citrix Receiver est différente, donc ces options ne s'appliquent pas. Vous pouvez utiliser la console de gestion StoreFront pour configurer des vues. Pour de plus amples informations, consultez la section [Spécifier différentes vues pour les applications et bureaux](#).

Affichage par défaut (Graphiques simplifiés)	
<ul style="list-style-type: none"> • Interface utilisateur à onglet unique • Interface utilisateur à plusieurs onglets <ul style="list-style-type: none"> • Onglet Application • Onglet Bureau • Onglet Contenu • (Ordre des onglets) 	L'interface utilisateur de Citrix Receiver contient des onglets par défaut, avec applications et contenu dans un onglet et bureaux dans l'autre. Il existe également un onglet Favori (facultatif).
<ul style="list-style-type: none"> • Logo d'en-tête • Couleur du texte • Couleur d'arrière-plan de l'en-tête • Image d'arrière-plan de l'en-tête 	<p>Équivalents pour les couleurs et logos à l'aide de la console d'administration StoreFront. Cliquez sur Personnaliser l'apparence du site Web dans le panneau Actions de la console d'administration StoreFront et apportez les modifications sur l'écran qui s'affiche.</p> <p>Vous pouvez définir une image d'arrière-plan pour l'en-tête en utilisant la personnalisation de style. Par exemple</p> <pre>.theme-header-bgcolor { background-image: url('spirals.png'); }</pre>
<ul style="list-style-type: none"> • Message de bienvenue de pré-ouverture de session (Pré-localisation) <ul style="list-style-type: none"> • Titre • Texte • Hyperlien • Libellé du bouton 	<p>Par défaut, il n'existe aucun autre écran de pré-ouverture de session.</p> <p>Cet exemple de script ajoute une zone de message interactive :</p> <pre>var doneClickThrough = false; // Avant l'ouverture de session Web CTXS.Extensions.beforeLogon = function (callback) { doneClickThrough = true; CTXS.ExtensionAPI.showMessage({ messageTitle: "Bienvenue !", messageText: "Réservé uniquement aux employés de WWCo", okButtonText: "Accepter", okAction: callback }); };</pre>

	<pre>// Avant l'écran principal (pour les clients natifs) CTXS.Extensions.beforeDisplayHomeScreen = function (callback) { if (!doneClickThrough) { CTXS.ExtensionAPI.showMessage({ messageTitle: "Bienvenue !", messageText: "Réservé uniquement aux employés de WWCo", okButtonText: "Accepter", okAction: callback }); } else { callback(); } };</pre>
<ul style="list-style-type: none"> • Titre de l'écran d'ouverture de session • Message de l'écran d'ouverture de session • Message système de l'écran d'ouverture de session 	<p>Il existe quatre zones de personnalisation sur l'écran d'ouverture de session. Haut et bas de l'écran (en-tête et bas de page) et haut et bas de la boîte de dialogue d'ouverture de session.</p> <pre>.customAuthHeader, .customAuthFooter .customAuthTop, .customAuthBottom { text-align: center; color: white; font-size: 16px; }</pre> <p>Exemple de script (contenu statique)</p> <pre>\$('#.customAuthHeader').html("Welcome to ACME");</pre> <p>Exemple de script (contenu dynamique)</p>

	<pre>function setDynamicContent(txtFile, element) { CTXS.ExtensionAPI.proxyRequest({ url: "customweb/"+txtFile, success: function(txt) {\$(element).html(txt);}); } setDynamicContent("Message.txt", ".customAuthTop");</pre> <p>Remarque : il ne faut pas explicitement inclure de contenu dynamique dans le script, ou le placer dans le répertoire personnalisé, car les modifications effectuées ici forcent les clients à recharger l'interface utilisateur. Placez le contenu dynamique dans le répertoire customweb.</p>
<ul style="list-style-type: none"> • Message de bienvenue de l'écran d'application • Message système de l'écran d'application 	<p>Consultez les exemples d'écran de bienvenue CustomAuth ci-dessus.</p> <p>Consultez les exemples de contenu dynamique ci-dessus. Utilisez #customTop plutôt que .customAuthTop pour placer du contenu sur l'écran d'accueil.</p>
Texte de bas de page (tous les écrans)	<p>Exemple de script :</p> <pre>#customBottom { text-align: center; color: white; font-size: 16px; }</pre> <p>Exemple de contenu statique à l'aide d'un script :</p> <pre>\$('#customBottom').html("Welcome to ACME");</pre>
Fonctionnalités avec aucun équivalent direct	
<ul style="list-style-type: none"> • Écran d'ouverture de session sans en-têtes • Écran d'ouverture de session avec en-têtes (y compris des messages) 	<p>Il n'existe pas d'équivalent direct dans StoreFront. Toutefois, vous pouvez créer des en-têtes personnalisés. Consultez la section « Titre de l'écran d'ouverture de session » ci-dessus.</p>

Paramètres utilisateur	Par défaut, il n'existe aucun paramètre utilisateur. Vous pouvez ajouter des menus et boutons JavaScript.
Contrôle de l'espace de travail	Fonctionnalité équivalente pour les paramètres d'administrateur. Les API d'extension permettent une plus grande flexibilité. Voir http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html .
Personnalisations avancées (code)	
Hooks de génération du fichier ICA et autres personnalisations de routage d'appel.	API équivalentes ou supérieures. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
Personnalisations d'authentification	API équivalentes ou supérieures. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
Accès source JSP/ASP	Il n'existe pas d'API équivalente sur StoreFront, car l'interface utilisateur n'est pas restituée de la même manière. Il existe de nombreuses API JavaScript permettant la personnalisation de l'interface utilisateur.

Configurer des groupes de serveurs

Jun 30, 2017

Les tâches décrites ci-dessous vous permettent de modifier les paramètres de déploiements StoreFront comprenant de multiples serveurs. Pour gérer un déploiement contenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Toutes les modifications de configuration que vous effectuez doivent être propagées aux autres serveurs du groupe pour garantir une configuration homogène sur l'ensemble du déploiement.

Vous devez configurer des serveurs comprenant un groupe de serveurs StoreFront de manière identique en termes d'emplacement d'installation de StoreFront et des paramètres des sites Web IIS, tels que le chemin d'accès physique et les ID de site.

Ajouter un serveur à un groupe de serveurs

Utilisez la tâche Ajouter un serveur pour obtenir un code d'autorisation qui vous permet d'associer un serveur StoreFront récemment installé à votre déploiement existant. Pour plus d'informations sur l'ajout de nouveaux serveurs aux déploiements StoreFront existants, reportez-vous à la section [Joindre un groupe de serveurs existant](#). Veuillez consulter la section *Capacité à monter en charge* de [Planifier votre déploiement StoreFront](#) pour évaluer le nombre de serveurs dont vous avez besoin dans votre groupe.

Supprimer des serveurs d'un groupe de serveurs

Utilisez la tâche Supprimer le serveur pour supprimer des serveurs d'un déploiement StoreFront comprenant de multiples serveurs. Vous pouvez supprimer n'importe quel serveur du groupe, excepté celui sur lequel vous êtes en train d'exécuter la tâche. Avant de supprimer un serveur d'un déploiement sur plusieurs serveurs, supprimez d'abord le serveur de l'environnement d'équilibrage de charge.

Propager les modifications locales à un groupe de serveurs

Utilisez la tâche Propager les modifications pour mettre à jour la configuration de tous les autres serveurs dans un déploiement StoreFront contenant de multiples serveurs, afin qu'elle corresponde à celle du serveur actuel. Toutes les modifications effectuées sur les autres serveurs du groupe sont abandonnées. Lors de l'exécution de cette tâche, il n'est pas possible d'effectuer d'autres modifications tant que tous les serveurs du groupe n'ont pas été mis à jour.

Important : si vous actualisez la configuration d'un serveur sans propager les modifications aux autres serveurs du groupe, il est possible que vous perdiez ces mises à jour si vous propagez ensuite des modifications à partir d'un autre serveur du déploiement.

Modifier l'URL de base d'un déploiement

Utilisez la tâche Changer l'URL de base pour modifier l'adresse URL utilisée comme racine des URL des magasins et autres services StoreFront hébergés sur un déploiement. Pour les déploiements contenant de multiples serveurs, spécifiez l'adresse URL à charge équilibrée. Vous pouvez utiliser cette tâche pour passer de HTTP à HTTPS à tout moment, à condition que Microsoft Internet Information Services (IIS) soit configuré pour HTTPS.

Pour configurer IIS pour HTTPS, utilisez la console Gestionnaire des services Internet (IIS) sur le serveur StoreFront pour créer un certificat de serveur signé par votre autorité de certification de domaine Microsoft Active Directory. Ensuite, ajoutez la liaison HTTPS au site Web par défaut. Pour de plus amples informations sur la création d'un certificat de serveur dans IIS, consultez l'article <http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate>. Pour plus

d'informations sur l'ajout d'une liaison HTTPS à un site IIS, consultez l'article <http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding>.

Configurer le comportement de contournement de serveur

Pour améliorer les performances lorsque certains des serveurs qui fournissent des ressources deviennent indisponibles, StoreFront ignore temporairement les serveurs qui ne répondent pas. Lorsqu'un serveur est contourné, StoreFront ignore ce serveur et ne l'utilise pas pour accéder aux ressources. Utilisez ces paramètres pour spécifier la durée du comportement de contournement :

- **Durée de l'état hors ligne en cas d'échec de tous les serveurs** spécifie une durée réduite en minutes que StoreFront utilise à la place de **Durée de l'état hors ligne** lorsque tous les serveurs d'un Delivery Controller particulier sont ignorés. La valeur par défaut est 0 minutes.
- **Durée de l'état hors ligne** spécifie la durée en minutes pendant laquelle StoreFront ignore un serveur individuel après un échec de tentative de contact de ce serveur. La durée par défaut est de 60 minutes.

Considérations à prendre en compte lors de la définition de l'option **Durée de l'état hors ligne en cas d'échec de tous les serveurs**

La définition d'une valeur **Durée de l'état hors ligne en cas d'échec de tous les serveurs** plus importante réduit l'impact de l'indisponibilité d'un Delivery Controller particulier ; cependant, cela a des répercussions négatives dans la mesure où les ressources dans ce Delivery Controller ne sont pas disponibles pour les utilisateurs pendant la durée spécifiée après une panne réseau ou une indisponibilité du serveur temporaire. Envisagez d'utiliser des valeurs **Durée de l'état hors ligne en cas d'échec de tous les serveurs** plus importantes lorsque plusieurs Delivery Controller ont été configurés pour un magasin, plus particulièrement pour des Delivery Controller non stratégiques.

La définition d'une valeur **Durée de l'état hors ligne en cas d'échec de tous les serveurs** plus faible augmente la disponibilité des ressources mises à disposition par Delivery Controller, mais augmente la possibilité d'interruptions du côté client si de nombreux Delivery Controller sont configurés pour un magasin et que plusieurs d'entre eux deviennent indisponibles. Il est préférable de conserver la valeur par défaut de 0-minute lorsqu'un nombre faible de batteries est configuré et pour les Delivery Controller stratégiques.

Pour modifier les paramètres de contournement pour un magasin

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Ceci terminé, [propagez les modifications que vous avez apportées au groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront et cliquez sur **Gérer les Delivery Controller** dans le volet **Actions**.
3. Sélectionnez un Controller, cliquez sur **Modifier**, et cliquez sur **Paramètres** dans l'écran **Modifier Delivery Controller**.
4. Sur la ligne **Durée de l'état hors ligne en cas d'échec de tous les serveurs**, cliquez dans la deuxième colonne et entrez la durée, en minutes, pendant laquelle un Delivery Controller est considéré comme étant hors ligne lorsque aucun de ses serveurs ne répond.
5. Sur la ligne **Durée de l'état hors ligne**, cliquez dans la deuxième colonne et entrez la durée, en minutes, pendant laquelle un serveur est considéré comme étant hors ligne lorsqu'il ne répond pas.

Configurer l'authentification et la délégation

Jun 30, 2017

En fonction de vos besoins, il existe plusieurs méthodes d'authentification et de délégation.

Configurer le service d'authentification	Le service d'authentification authentifie les utilisateurs auprès de Microsoft Active Directory, si bien que les utilisateurs n'ont pas besoin de rouvrir une session pour accéder à leurs bureaux et applications.
Authentification basée sur le service XML	Lorsque StoreFront ne se trouve pas dans le même domaine que XenApp ou XenDesktop, et qu'il n'est pas possible de mettre des approbations Active Directory en place, vous pouvez configurer StoreFront pour que le service XML XenApp et XenDesktop soit utilisé pour l'authentification des noms d'utilisateur et mots de passe.
Délégation Kerberos contrainte pour XenApp 6.5	Utilisez la tâche Configurer la délégation Kerberos pour spécifier si StoreFront utilise la délégation Kerberos contrainte pour domaine unique pour s'authentifier auprès des Delivery Controller.
Authentification par carte à puce	Configurez l'authentification par carte à puce pour tous les composants d'un déploiement StoreFront typique.
Période de notification d'expiration du mot de passe	Si vous autorisez les utilisateurs de sites Citrix Receiver pour Web à modifier leurs mots de passe à tout moment, un avertissement s'affiche à l'attention des utilisateurs locaux dont les mots de passe sont sur le point d'expirer lorsqu'ils ouvrent une session.

Configurer le service d'authentification

Jun 30, 2017

[Gestion des méthodes d'authentification](#)

[Configurer des domaines utilisateur approuvés](#)

[Autoriser les utilisateurs à modifier leurs mots de passe](#)

[Réinitialisation en libre-service des mots de passe](#)

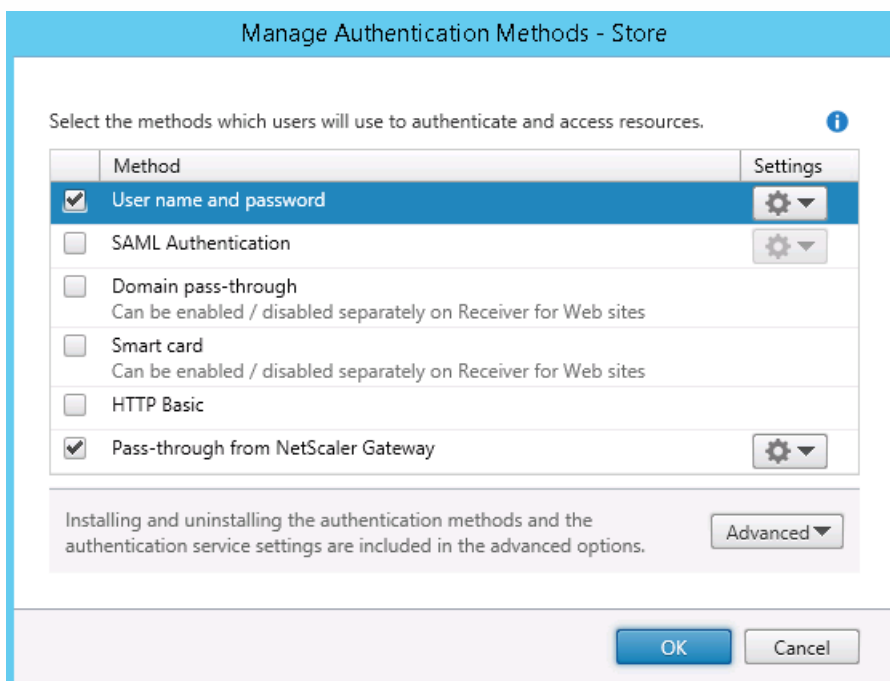
[Paramètres du service d'authentification partagé](#)

[Déléguer la validation des informations d'identification à NetScaler Gateway](#)

Gestion des méthodes d'authentification

Vous pouvez activer ou désactiver la configuration des méthodes d'authentification des utilisateurs lorsque le service d'authentification a été créé en sélectionnant une méthode d'authentification dans le panneau des résultats de la console de gestion Citrix StoreFront, et dans le panneau Actions, en cliquant sur **Gérer les méthodes d'authentification**.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix **StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification**.
3. Indiquez les méthodes d'accès que vous souhaitez activer pour vos utilisateurs.



- Cochez la case **Nom d'utilisateur et mot de passe** pour activer l'authentification explicite. Les utilisateurs saisissent leurs informations d'identification lorsqu'ils accèdent à leurs magasins.
- Sélectionnez la case **Authentification SAML** pour activer l'intégration avec un fournisseur d'identité SAML. Les utilisateurs s'authentifient sur Access Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Depuis le menu déroulant Paramètres :

- Sélectionnez **Fournisseur d'identité** pour configurer l'approbation du fournisseur d'identité.
- Sélectionnez **Fournisseur de services** pour configurer l'approbation du fournisseur de services. Cette information est requise par le fournisseur d'identité.
- Sélectionnez la case à cocher **Authentification pass-through au domaine**. Cette dernière permet d'autoriser l'authentification pass-through des informations d'identification de domaine Active Directory à partir des machines des utilisateurs. Les utilisateurs doivent s'authentifier sur leur ordinateur Windows membre d'un domaine et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Pour pouvoir utiliser cette option, l'authentification pass-through doit être activée lorsque Citrix Receiver pour Windows est installé sur les machines utilisateur.
- Sélectionnez la case **Carte à puce** pour activer l'authentification par carte à puce. Les utilisateurs doivent s'authentifier à l'aide de cartes à puce et de codes PIN lorsqu'ils accèdent à leurs magasins.
- Sélectionnez la case à cocher **HTTP Basique** pour activer l'authentification HTTP de base. Les utilisateurs s'authentifient avec le serveur Web IIS du serveur StoreFront.
- Sélectionnez la case **Authentification pass-through via NetScaler Gateway** pour activer l'authentification pass-through à partir de NetScaler Gateway. Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

Pour activer l'authentification pass-through par carte à puce pour les utilisateurs qui accèdent à des magasins via NetScaler Gateway, utilisez la tâche **Configurer l'authentification déléguée**.

Configurer des domaines utilisateur approuvés

Utilisez la tâche **Domaines approuvés** pour restreindre l'accès aux magasins des utilisateurs qui ouvrent une session avec des informations d'identification de domaine explicites, soit directement, soit à l'aide de l'authentification pass-through de NetScaler Gateway.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau des résultats, sélectionnez la méthode d'authentification appropriée. Dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification**.
3. Dans le menu déroulant **Nom d'utilisateur et mot de passe (explicite) > Paramètres**, sélectionnez **Configurer Domaines approuvés**.
4. Sélectionnez **Domaines approuvés uniquement**, cliquez sur **Ajouter** pour entrer le nom d'un domaine approuvé. Les utilisateurs disposant de comptes dans ce domaine pourront se connecter à tous les magasins qui utilisent ce service d'authentification. Pour modifier un nom de domaine, sélectionnez l'entrée correspondante dans la liste **Domaines approuvés**, puis cliquez sur **Modifier**. Sélectionnez un domaine dans la liste et cliquez sur **Supprimer** pour interrompre l'accès aux magasins des comptes utilisateur dans ce domaine.

La manière dont vous spécifiez le nom de domaine détermine le format auquel les utilisateurs devront saisir leurs informations d'identification. Si vous souhaitez que les utilisateurs saisissent leurs informations d'identification au format de nom d'utilisateur de domaine, ajoutez le nom **NetBIOS** à la liste. Pour exiger que les utilisateurs saisissent leurs informations d'identification au format de nom principal d'utilisateur, ajoutez le nom de domaine complet à la liste. Si vous souhaitez que les utilisateurs saisissent leurs informations d'identification aux formats de nom d'utilisateur de domaine et de nom principal d'utilisateur, vous devez ajouter le nom **NetBIOS** et le nom de domaine complet à la liste.

5. Si vous configurez plusieurs domaines approuvés, sélectionnez dans la liste **Domaine par défaut** le domaine sélectionné par défaut lorsque les utilisateurs ouvrent une session.
6. Si vous voulez dresser la liste des domaines approuvés sur la page d'ouverture de session, sélectionnez la case **Afficher une liste de domaines sur la page d'ouverture de session**.

Autoriser les utilisateurs à modifier leurs mots de passe

Utilisez la tâche **Gérer les options de mot de passe** pour permettre aux utilisateurs de Receiver de bureau et de sites Receiver pour Web qui ouvrent une session avec des informations d'identification de domaine de modifier leurs mots de

passe. Lorsque vous créez le service d'authentification, la configuration par défaut empêche les utilisateurs de Citrix Receiver et de sites Citrix Receiver pour Web de modifier leurs mots de passe, même si les mots de passe ont expiré. Si vous choisissez d'activer cette fonctionnalité, assurez-vous que les stratégies des domaines contenant vos serveurs n'empêchent pas les utilisateurs de modifier leurs mots de passe. L'activation de la fonctionnalité permettant aux utilisateurs de modifier leurs mots de passe expose des fonctions de sécurité sensibles à toute personne pouvant accéder aux magasins qui utilisent ce service d'authentification. Si votre organisation possède une stratégie de sécurité qui restreint les fonctions de modification des mots de passe utilisateur à un usage interne uniquement, vous devez vous assurer qu'aucun des magasins ne sont accessibles depuis l'extérieur de votre réseau interne.

1. Citrix Receiver pour Web prend en charge la modification des mots de passe sur expiration, ainsi que la modification élective de mot de passe. Tous les Citrix Receiver de bureau prennent en charge la modification de mot de passe via NetScaler Gateway sur expiration uniquement. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur Gérer les méthodes d'authentification.
3. À partir du menu déroulant **Nom d'utilisateur et mot de passe > Paramètres**, sélectionnez **Gérer les options de mot de passe**, indiquez sous quelles conditions les utilisateurs de sites Citrix Receiver pour Web qui ouvrent une session à l'aide d'informations d'identification de domaine sont en mesure de modifier leurs mots de passe.
 - Pour autoriser les utilisateurs à modifier leurs mots de passe quand ils souhaitent, sélectionnez À tout moment. Un avertissement s'affiche lorsque les utilisateurs locaux dont les mots de passe sont sur le point d'expirer ouvrent une session. Les avertissements d'expiration du mot de passe s'affichent uniquement pour les utilisateurs se connectant depuis le réseau interne. Par défaut, la période de notification pour un utilisateur est déterminée par le paramètre de stratégie Windows applicable. Pour de plus amples informations sur la configuration de périodes de notification personnalisées, consultez la section [Configurer la période de notification d'expiration du mot de passe](#). Pris en charge uniquement avec Citrix Receiver pour Web.
 - Pour autoriser les utilisateurs à modifier leurs mots de passe uniquement lorsqu'ils ont expiré, sélectionnez Après expiration. Les utilisateurs qui ne peuvent pas ouvrir de session car leurs mots de passe ont expiré sont redirigés vers la boîte de dialogue Modifier le mot de passe. Pris en charge avec Citrix Receiver pour bureau et Citrix Receiver pour Web.
 - Pour empêcher les utilisateurs de modifier leurs mots de passe, ne sélectionnez pas l'option **Autoriser les utilisateurs à modifier les mots de passe**. Si vous ne sélectionnez pas cette option, vous devez prendre vos propres dispositions pour prendre en charge les utilisateurs qui ne peuvent pas accéder à leurs bureaux et applications car leurs mots de passe ont expiré.

Si vous autorisez les utilisateurs de sites Citrix Receiver pour Web à modifier leurs mots de passe à tout moment, assurez-vous que l'espace disque est suffisant sur vos serveurs StoreFront pour stocker les profils de tous vos utilisateurs. Pour vérifier si le mot de passe d'un utilisateur est sur le point d'expirer, StoreFront crée un profil local pour cet utilisateur sur le serveur. StoreFront doit être en mesure de contacter le contrôleur de domaine pour modifier les mots de passe des utilisateurs.

Citrix Receiver	L'utilisateur peut modifier un mot de passe expiré si cette option est activée sur StoreFront	L'utilisateur est notifié que le mot de passe va expirer	L'utilisateur peut modifier un mot de passe avant expiration si cette option est activée sur StoreFront
Windows	Oui		
Mac	Oui		

Android Citrix Receiver iOS	L'utilisateur peut modifier un mot de passe expiré si cette option est activée sur StoreFront	L'utilisateur est notifié que le mot de passe va expirer	L'utilisateur peut modifier un mot de passe avant expiration si cette option est activée sur StoreFront
Linux	Oui		
Web	Oui	Oui	Oui

Questions de sécurité de la réinitialisation en libre-service des mots de passe

La réinitialisation en libre-service des mots de passe confère aux utilisateurs un plus grand contrôle sur leurs comptes d'utilisateur. Une fois la réinitialisation en libre-service des mots de passe configurée, si les utilisateurs rencontrent des problèmes lors de l'ouverture de session sur leurs systèmes, ils peuvent déverrouiller leurs comptes ou réinitialiser leurs mots de passe en répondant correctement à plusieurs questions de sécurité.

Lors de la configuration de la réinitialisation en libre-service des mots de passe, vous indiquez quels utilisateurs sont autorisés à réinitialiser leur mot de passe et à déverrouiller leur compte à l'aide de la console de gestion. Si vous activez ces fonctionnalités pour StoreFront, il se peut que les utilisateurs ne soient pas autorisés à réaliser ces tâches en fonction des paramètres configurés dans la console Configuration de la réinitialisation en libre-service des mots de passe.

Seuls les utilisateurs qui accèdent à StoreFront à l'aide de connexions HTTPS peuvent utiliser la réinitialisation en libre-service des mots de passe. Ils ne peuvent pas accéder à StoreFront à l'aide d'une connexion HTTP alors que la réinitialisation en libre-service des mots de passe est disponible. La réinitialisation en libre-service des mots de passe est disponible uniquement lors de l'authentification directe à StoreFront avec un nom d'utilisateur et un mot de passe.

La réinitialisation en libre-service des mots de passe ne prend pas en charge l'ouverture de session à l'aide d'un nom UPN, tel que nomd'utilisateur@domaine.com.

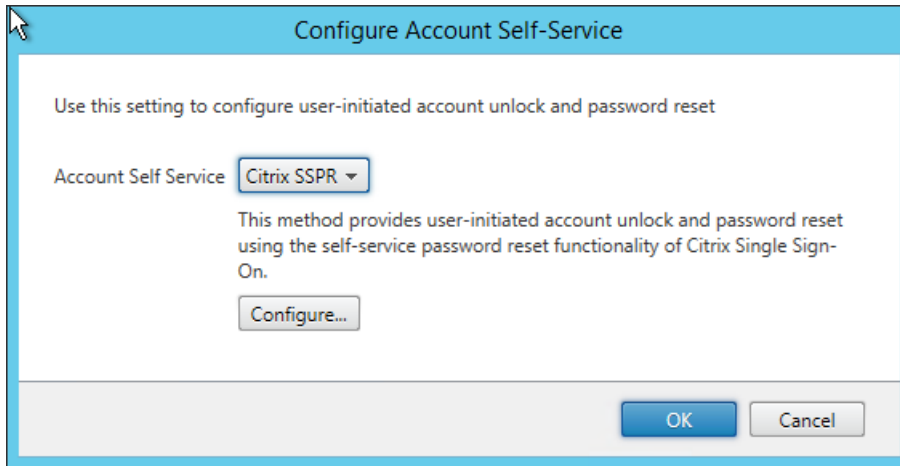
Avant de configurer la réinitialisation en libre-service des mots de passe pour un magasin, vous devez vous assurer que :

- Le magasin est configuré pour utiliser l'authentification par nom d'utilisateur et mot de passe.
- Le magasin est configuré pour utiliser uniquement la réinitialisation en libre-service des mots de passe. Si StoreFront est configuré pour utiliser de nombreuses batteries au sein d'un même domaine ou de plusieurs domaines de confiance, vous devez configurer la réinitialisation en libre-service des mots de passe pour accepter les informations d'identification de tous ces domaines.
- Le magasin est configuré pour permettre aux utilisateurs de changer leur mot de passe à n'importe quel moment, dans le cas où vous activez la fonctionnalité de réinitialisation du mot de passe.
- Vous devez associer un magasin StoreFront avec un site Receiver pour Web, et configurer ce site pour qu'il utilise l'expérience unifiée.

Avant de pouvoir utiliser la réinitialisation en libre-service des mots de passe, vous devez l'installer et la configurer. Elle est disponible sur le support pour XenApp et XenDesktop. Pour de plus amples informations, consultez la documentation [Réinitialisation en libre-service des mots de passe](#).

1. Activez la prise en charge de la fonction de réinitialisation en libre-service des mots de passe dans StoreFront en sélectionnant le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification > Nom d'utilisateur et mot de passe** et choisissez **Gérer les options de mot de passe** dans le menu déroulant.

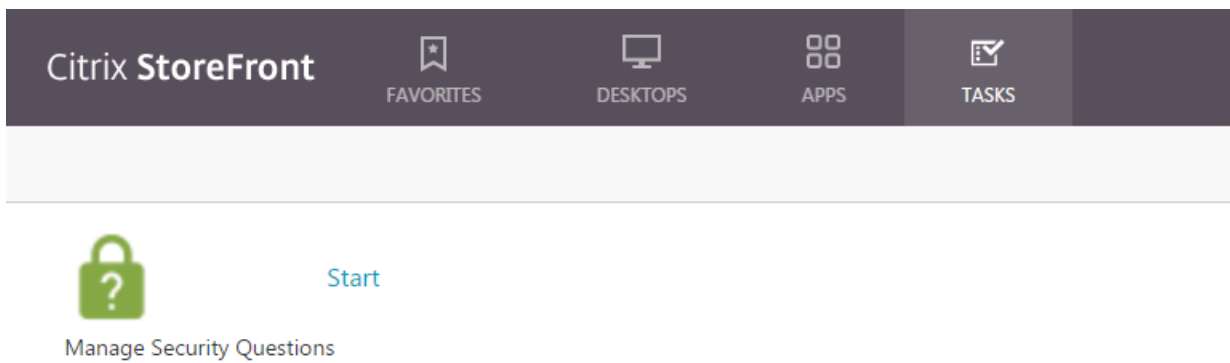
2. Choisissez si vous voulez autoriser les utilisateurs à modifier les mots de passe et cliquez sur **OK**.
3. À partir du menu déroulant **Nom d'utilisateur et mot de passe**, choisissez **Configurer libre-service de compte**, sélectionnez **Citrix SSPR** dans le menu déroulant, puis cliquez sur **OK**.
4. Spécifiez si les utilisateurs sont autorisés à réinitialiser leurs mots de passe et à déverrouiller leurs comptes avec la réinitialisation en libre-service des mots de passe, ajoutez l'URL du compte du service de réinitialisation des mots de passe et cliquez deux fois sur **OK**.



Cette option est disponible uniquement lorsque l'adresse URL de base de StoreFront est HTTPS (non HTTP) et l'option **Activer la réinitialisation du mot de passe** est uniquement disponible après que vous ayez utilisé **Gérer les options de mot de passe** pour permettre aux utilisateurs de modifier les mots de passe à tout moment.



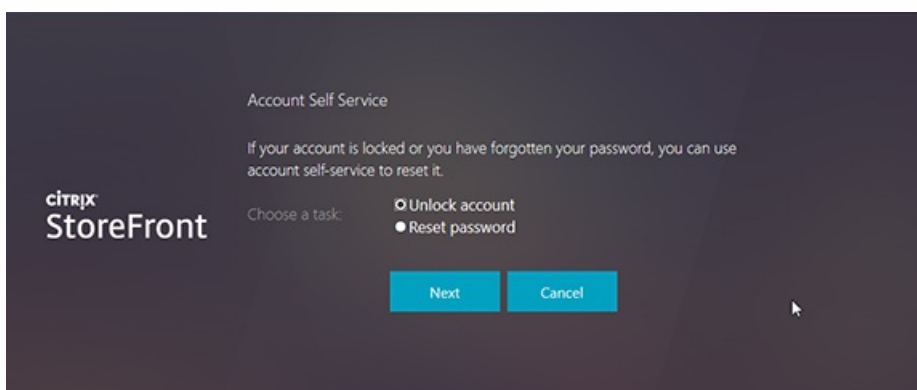
La prochaine fois que l'utilisateur ouvre une session sur Citrix Receiver ou Citrix Receiver pour Web, l'enregistrement de questions de sécurité est disponible. Après avoir cliqué sur **Démarrer**, les questions sont affichées et l'utilisateur doit fournir des réponses.



Une fois configurés dans StoreFront, les utilisateurs voient le lien **Compte en libre-service** sur l'écran d'ouverture de session de Citrix Receiver pour Web (il s'affiche sous forme d'un bouton dans les autres logiciels Citrix Receiver).

Lorsque l'utilisateur clique sur ce lien, il est guidé à travers une série de formulaires à sélectionner entre **Déverrouiller compte** et **Réinitialiser le mot de passe** (s'ils sont tous deux disponibles).

Après avoir choisi un bouton radio et cliqué sur **Suivant**, l'écran suivant vous invite à entrer un domaine et un nom d'utilisateur (*domaine\utilisateur*), si ces informations n'ont pas été entrées dans le formulaire d'ouverture de session. Veuillez noter que le libre-service de compte ne prend pas en charge les ouvertures de session UPN, telles que *nomd'utilisateur@domaine.com*.



Ils doivent répondre aux questions de sécurité. Si les réponses correspondent à celles fournies par l'utilisateur, l'opération demandée (déverrouiller ou réinitialiser) est exécutée et l'utilisateur est notifié de la réussite.

Paramètres du service d'authentification partagé

Utilisez la tâche Paramètres du service d'authentification partagé pour spécifier les magasins qui partageront le service d'authentification activant l'authentification pass-through entre eux.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification**.

3. Dans le menu déroulant **Avancé**, sélectionnez **Paramètres du service d'authentification partagé**.
4. Cliquez sur la case **Utiliser un service d'authentification partagé** et sélectionnez un magasin dans le menu déroulant **Magasin**.

Remarque : il n'existe pas de différence opérationnelle entre un service d'authentification partagé et dédié. Un service d'authentification partagé par plus de deux magasins est traité comme un service d'authentification partagé et les modifications apportées à la configuration affectent l'accès à tous les magasins qui utilisent ce service d'authentification partagé.

Déléguer la validation des informations d'identification à NetScaler Gateway

Utilisez la tâche Configurer l'authentification déléguée pour activer l'authentification pass-through pour les utilisateurs de cartes à puce qui accèdent aux magasins via NetScaler Gateway. Cette tâche est uniquement disponible lorsque Authentification pass-through via NetScaler Gateway est activée et sélectionnée dans le panneau des résultats.

Lorsque la validation des informations d'identification est déléguée à NetScaler Gateway, les utilisateurs s'authentifient sur NetScaler Gateway à l'aide de leurs cartes à puce et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Ce paramètre est désactivé par défaut lorsque vous activez l'authentification pass-through via NetScaler Gateway, afin que l'authentification pass-through ne soit appliquée que lorsque les utilisateurs ouvrent une session sur NetScaler Gateway avec un mot de passe.

Authentification basée sur le service XML

Jun 30, 2017

Lorsque StoreFront ne se trouve pas dans le même domaine que XenApp ou XenDesktop, et qu'il n'est pas possible de mettre des approbations Active Directory en place, vous pouvez configurer StoreFront pour que le service XML XenApp et XenDesktop soit utilisé pour l'authentification des noms d'utilisateur et mots de passe.

Activer l'authentification basée sur le service XML

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les méthodes d'authentification**.
3. Sur la page **Gérer les méthodes d'authentification**, à partir du menu déroulant **Nom d'utilisateur et mot de passe > Paramètres**, sélectionnez **Configurer la validation du mot de passe**.
4. À partir du menu déroulant **Valider les mots de passe via**, sélectionnez **Delivery Controller**, puis cliquez sur **Configurer**.
5. Suivez les écrans **Configurer Delivery Controller** pour ajouter un ou plusieurs **Delivery Controller** pour la validation des informations d'identification de l'utilisateur et cliquez sur **OK**.

Désactiver l'authentification basée sur le service XML

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les méthodes d'authentification**.
3. Sur la page **Gérer les méthodes d'authentification**, à partir du menu déroulant **Nom d'utilisateur et mot de passe > Paramètres**, sélectionnez **Configurer la validation du mot de passe**.
4. À partir du menu déroulant **Valider les mots de passe via**, sélectionnez **Active Directory**, puis cliquez sur **OK**.

Configurer la délégation Kerberos contrainte pour XenApp 6.5

Jun 30, 2017

Utilisez la tâche **Configurer les paramètres du magasin > Délégation Kerberos** pour spécifier si StoreFront utilise la délégation Kerberos contrainte pour domaine unique pour s'authentifier auprès des Delivery Controller.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Ceci terminé, propagez les modifications que vous avez apportées au groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau Actions, cliquez sur **Configurer les paramètres du magasin**, puis sur Délégation Kerberos.
3. Choisissez d'activer ou de désactiver Utiliser la délégation Kerberos pour authentifier les Delivery Controller pour activer ou désactiver la délégation Kerberos contrainte.

Configurer le serveur StoreFront pour la délégation

Suivez cette procédure lorsque StoreFront n'est pas installé sur la même machine que XenApp.

1. Sur le contrôleur de domaine, ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.
2. Sur le menu Affichage, cliquez sur Fonctionnalités avancées.
3. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs sous le nom de domaine et sélectionnez le serveur StoreFront.
4. Dans le panneau Actions, cliquez sur Propriétés.
5. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser n'importe quel protocole d'authentification, puis cliquez sur Ajouter.
6. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.
7. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom du serveur exécutant le service XML Citrix (XenApp) dans la zone de texte Entrez le nom de l'objet à sélectionner, puis cliquez sur OK.
8. Sélectionnez le type de service HTTP dans la liste et cliquez sur OK.
9. Appliquez les modifications et fermez la boîte de dialogue.

Configurer le serveur XenApp pour la délégation

Configurez la délégation approuvée Active Directory pour chaque serveur XenApp.

1. Sur le contrôleur de domaine, ouvrez le composant logiciel enfichable **MMC Utilisateurs et ordinateurs Active Directory**.
2. Dans le panneau de gauche, cliquez sur le nœud **Ordinateurs** sous le nom de domaine et sélectionnez le serveur exécutant le service XML Citrix (XenApp) que StoreFront est configuré pour contacter.
3. Dans le panneau **Actions**, cliquez sur **Propriétés**.
4. Sur l'onglet **Délégation**, cliquez sur **Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement** et **Utiliser n'importe quel protocole d'authentification**, puis cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Ajouter des services**, cliquez sur **Utilisateurs ou ordinateurs**.

6. Dans la boîte de dialogue **Sélectionnez utilisateurs ou ordinateurs**, tapez le nom du serveur exécutant le service XML Citrix (XenApp) dans la zone de texte **Entrez le nom de l'objet à sélectionner**, puis cliquez sur **OK**.
7. Sélectionnez le type de service HOST dans la liste, cliquez sur **OK** et ensuite sur **Ajouter**.
8. Dans la boîte de dialogue **Sélectionnez utilisateurs ou ordinateurs**, tapez le nom du contrôleur de domaine dans la case **Entrez les noms des objets à sélectionner** et cliquez sur **OK**.
9. Sélectionnez les types de service **cifs** et **ldap** dans la liste et cliquez sur **OK**. Remarque : si vous avez deux possibilités pour le service ldap, sélectionnez celui qui correspond au FQDN du contrôleur de domaine.
10. Appliquez les modifications et fermez la boîte de dialogue.

Remarques importantes

Lorsque vous déterminez si vous souhaitez utiliser la délégation Kerberos contrainte, tenez compte des points suivants.

- Points clés :
 - Vous n'avez pas besoin de ssonsvr.exe sauf si l'authentification pass-through (ou authentification pass-through par carte à puce) est effectuée sans la délégation Kerberos contrainte.
- Authentification pass-through au domaine StoreFront et Citrix Receiver pour Web :
 - Vous n'avez pas besoin de ssonsvr.exe sur le client.
 - Vous pouvez définir un nom d'utilisateur et un mot de passe locaux quelconques dans le modèle icaclient.adm Citrix (contrôle la fonction ssonsvr.exe).
 - Le paramètre Kerberos du modèle icaclient.adm est requis.
 - Ajoutez le nom de domaine complet (FQDN) de StoreFront à la liste des sites de confiance d'Internet Explorer. Cochez la case Utiliser le nom de l'utilisateur local dans les paramètres de sécurité d'Internet Explorer pour la zone de confiance.
 - Le client doit figurer dans un domaine.
 - Activez la méthode d'authentification Authentification pass-through au domaine sur le serveur StoreFront et Citrix Receiver pour Web.
- StoreFront, Citrix Receiver pour Web et authentification par carte à puce avec invite de saisie du code PIN :
 - Vous n'avez pas besoin de ssonsvr.exe sur le client.
 - L'authentification par carte à puce a été configurée.
 - Vous pouvez définir un nom d'utilisateur et un mot de passe locaux quelconques dans le modèle icaclient.adm Citrix (contrôle la fonction ssonsvr.exe).
 - Le paramètre Kerberos du modèle icaclient.adm est requis.
 - Activez la méthode d'authentification Carte à puce sur le serveur StoreFront et Citrix Receiver pour Web.
 - Pour vous assurer que l'authentification par carte à puce est choisie, ne cochez pas la case Utiliser le nom de l'utilisateur local dans les paramètres de sécurité d'Internet Explorer pour le site StoreFront.
 - Le client doit figurer dans un domaine.
- NetScaler Gateway, StoreFront, Citrix Receiver pour Web et authentification par carte à puce avec invite de saisie du code PIN :
 - Vous n'avez pas besoin de ssonsvr.exe sur le client.
 - L'authentification par carte à puce a été configurée.
 - Vous pouvez définir un nom d'utilisateur et un mot de passe locaux quelconques dans le modèle icaclient.adm Citrix (contrôle la fonction ssonsvr.exe).
 - Le paramètre Kerberos du modèle icaclient.adm est requis.
 - Activez la méthode d'authentification Authentification pass-through via NetScaler Gateway sur le serveur StoreFront et Citrix Receiver pour Web.
 - Pour vous assurer que l'authentification par carte à puce est choisie, ne cochez pas la case Utiliser le nom de l'utilisateur local dans les paramètres de sécurité d'Internet Explorer pour le site StoreFront.
 - Le client doit figurer dans un domaine.
 - Configurez NetScaler Gateway pour l'authentification par carte à puce et configurez le lancement d'un autre vServer à l'aide du routage StoreFront HDX afin d'acheminer le trafic ICA via le vServer NetScaler Gateway non authentifié.
- Citrix Receiver pour Windows (AuthManager), authentification par carte à puce avec invite de saisie du code PIN et StoreFront :
 - Vous n'avez pas besoin de ssonsvr.exe sur le client.
 - Vous pouvez définir un nom d'utilisateur et un mot de passe locaux quelconques dans le modèle icaclient.adm Citrix (contrôle la fonction ssonsvr.exe).
 - Le paramètre Kerberos du modèle icaclient.adm est requis.
 - Le client doit figurer dans un domaine.
 - Activez la méthode d'authentification Carte à puce sur le serveur StoreFront.
- Citrix Receiver pour Windows (AuthManager), Kerberos et StoreFront :
 - Vous n'avez pas besoin de ssonsvr.exe sur le client.
 - Vous pouvez définir un nom d'utilisateur et un mot de passe locaux quelconques dans le modèle icaclient.adm Citrix (contrôle la fonction

ssonsvr.exe).

- Le paramètre Kerberos du modèle icaclient.adm est requis.
- Cochez la case Utiliser le nom de l'utilisateur local dans les paramètres de sécurité d'Internet Explorer pour la zone de confiance.
- Le client doit figurer dans un domaine.
- Activez la méthode d'authentification Authentification pass-through au domaine sur le serveur StoreFront.
- Assurez-vous que cette clé de registre est définie :

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 cet outil. Veuillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour les ordinateurs 32 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindows

Nom : SSONCheckEnabled

Type : REG_SZ

Valeur : true ou false

Pour les ordinateurs 64 bits :

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\integratedwindows

Nom : SSONCheckEnabled

Type : REG_SZ

Valeur : true ou false

Configuration de l'authentification par carte à puce

Jun 30, 2017

Cet article fournit une vue d'ensemble des tâches comprises dans la configuration de l'authentification par carte à puce pour tous les composants dans un déploiement StoreFront. Pour plus d'informations et des instructions détaillées sur la configuration, consultez la documentation des produits individuels.



Configuration de carte à puce pour environnements Citrix

This overview for configuring a Citrix deployment for smart cards uses a specific smart card type. Note that similar steps apply to smart cards from other vendors.

Conditions préalables

- Assurez-vous que les comptes de tous les utilisateurs sont configurés au sein du domaine Microsoft Active Directory dans lequel vous prévoyez de déployer vos serveurs StoreFront ou au sein d'un domaine doté d'une relation d'approbation bidirectionnelle directe avec le domaine du serveur StoreFront.
- Si vous prévoyez d'activer l'authentification pass-through par carte à puce, vérifiez que votre lecteur de carte à puce, votre middleware, votre configuration et la stratégie de mise en cache du code PIN du middleware prennent en charge l'authentification pass-through.
- Installez le middleware de carte à puce de votre fournisseur sur les machines physiques ou virtuelles exécutant le Virtual Delivery Agent qui fournit les bureaux et applications des utilisateurs. Pour de plus amples informations sur l'utilisation de cartes à puce avec XenDesktop, consultez la section [Cartes à puce](#).
- Avant de continuer, vérifiez que votre infrastructure de clé publique est configurée correctement. Vérifiez que le mappage du certificat sur le compte est correctement configuré pour votre environnement Active Directory et que la validation du certificat utilisateur peut être effectuée avec succès.

Configurer NetScaler Gateway

- Sur votre boîtier NetScaler Gateway, installez un certificat de serveur signé par une autorité de certification. Pour de plus amples informations, consultez la section [Installation et gestion des certificats](#).
- Installez sur votre boîtier le certificat racine de l'autorité de certification émettant les certificats utilisateur de votre carte à puce. Pour de plus amples informations, consultez la section [Pour installer un certificat racine sur NetScaler Gateway](#).
- Créez et configurez un serveur virtuel pour l'authentification du certificat client. Créez une stratégie d'authentification de certificat, en spécifiant SubjectAltName:PrincipalName pour l'extraction du nom d'utilisateur à partir du certificat. Ensuite, liez la stratégie au serveur virtuel et configurez le serveur virtuel pour demander des certificats clients. Pour de plus amples informations, consultez la section [Configuration et liaison d'une stratégie d'authentification du certificat client](#).
- Liez le certificat racine d'autorité de certification au serveur virtuel. Pour de plus amples informations, consultez la section [Pour ajouter un certificat racine à un serveur virtuel](#).
- Pour vous assurer que les utilisateurs ne reçoivent pas de demande d'informations d'identification supplémentaire sur le serveur virtuel lorsque les connexions à leurs ressources sont établies, créez un second serveur virtuel. Lorsque vous créez le serveur virtuel, désactivez l'authentification du client dans les paramètres Secure Sockets Layer (SSL). Pour plus d'informations, veuillez consulter la section [Configuration de l'authentification par carte à puce](#).

Vous devez également configurer StoreFront afin d'acheminer les connexions utilisateur aux ressources via ce serveur virtuel supplémentaire. Les utilisateurs ouvrent une session sur le premier serveur virtuel et le second serveur virtuel est utilisé pour les connexions à leurs ressources. Lorsque la connexion est établie, les utilisateurs n'ont pas besoin de

s'authentifier auprès de NetScaler Gateway mais ils doivent entrer leur code PIN pour ouvrir des sessions à leurs bureaux et applications. La configuration d'un serveur virtuel pour les connexions utilisateur aux ressources est facultative sauf si vous voulez autoriser les utilisateurs à revenir à l'authentification explicite au cas où ils rencontrent des problèmes avec leurs cartes à puce.

- Créez des stratégies de session et des profils pour les connexions depuis NetScaler Gateway vers StoreFront et liez-les au serveur virtuel approprié. Pour de plus amples informations, consultez la section [Accéder à StoreFront via NetScaler Gateway](#).
- Si vous avez configuré le serveur virtuel utilisé pour les connexions à StoreFront pour demander l'authentification du certificat client pour toutes les communications, vous devez créer un autre serveur virtuel pour fournir l'adresse URL de rappel pour StoreFront. Ce serveur virtuel est uniquement utilisé par StoreFront pour vérifier les demandes du boîtier NetScaler Gateway et n'a pas besoin d'être publiquement accessible. Un autre serveur virtuel est requis lorsque l'authentification du certificat client est obligatoire, car StoreFront ne peut pas présenter de certificat à authentifier. Pour plus d'informations, veuillez consulter la section [Création de serveurs virtuels](#).

Configurer StoreFront

- Vous devez utiliser le protocole HTTPS pour les communications entre StoreFront et les machines des utilisateurs pour activer l'authentification par carte à puce. Configurez Microsoft Internet Information Services (IIS) pour HTTPS en obtenant un certificat SSL dans IIS puis en ajoutant une liaison HTTPS au site Web par défaut. Pour de plus amples informations sur la création d'un certificat de serveur dans IIS, consultez l'article <http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate>. Pour plus d'informations sur l'ajout d'une liaison HTTPS à un site IIS, consultez l'article <http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding>.
- Si vous souhaitez demander que les certificats clients soient présentés pour les connexions HTTPS à toutes les adresses URL de StoreFront, configurez IIS sur le serveur StoreFront.
Lorsque StoreFront est installé, la configuration par défaut dans IIS requiert uniquement que les certificats clients soient présentés pour les connexions HTTPS à l'adresse URL d'authentification du certificat du service d'authentification de StoreFront. Cette configuration est nécessaire pour offrir aux utilisateurs de cartes à puce la possibilité de revenir à l'authentification explicite et, en fonction des paramètres de stratégie Windows appropriés, autoriser les utilisateurs à retirer leur carte à puce sans avoir à s'authentifier de nouveau.

Lorsque IIS est configuré pour demander des certificats clients pour les connexions HTTPS à toutes les adresses URL de StoreFront, les utilisateurs de carte à puce ne peuvent pas se connecter via NetScaler Gateway et ne peuvent pas revenir à l'authentification explicite. Les utilisateurs doivent ouvrir une nouvelle session s'ils retirent leur carte à puce de leur périphérique. Pour activer cette configuration de site IIS, le service d'authentification et les magasins doivent être colocalisés sur le même serveur, et un certificat client valide pour tous les magasins doit être utilisé. De plus, cette configuration dans laquelle IIS requiert des certificats clients pour les connexions HTTPS à toutes les adresses URL StoreFront entrera en conflit avec l'authentification des clients Citrix Receiver pour Web. Pour cette raison, cette configuration doit être utilisée lorsque l'accès au client Citrix Receiver pour Web n'est pas requis.

Si vous installez StoreFront sur Windows Server 2012, veuillez noter que les certificats non auto-signés installés dans le magasin de certificats Autorités de certification racines de confiance sur le serveur ne sont pas approuvés lorsque IIS est configuré pour utiliser SSL et l'authentification du certificat client. Pour de plus amples informations sur ce problème, veuillez consulter l'article <http://support.microsoft.com/kb/2802568>.

- Installez et configurez StoreFront. Créez le service d'authentification et ajoutez vos magasins, si nécessaire. Si vous configurez l'accès distant via NetScaler Gateway, n'activez pas l'intégration de réseau privé virtuel (VPN). Pour de plus amples informations, consultez la section [Installer et configurer StoreFront](#).
- Activez l'authentification par carte à puce à StoreFront pour les utilisateurs locaux sur le réseau interne. Pour les

utilisateurs de cartes à puce qui accèdent à des magasins via NetScaler Gateway, activez la méthode d'authentification pass-through avec NetScaler Gateway et assurez-vous que StoreFront est configuré pour déléguer la validation des informations d'identification à NetScaler Gateway. Si vous prévoyez d'activer l'authentification pass-through lorsque vous installez Citrix Receiver pour Windows sur des machines utilisateur appartenant au domaine, activez l'authentification pass-through au domaine. Pour de plus amples informations, consultez la section [Configurer le service d'authentification](#).

Pour autoriser l'authentification du client Citrix Receiver pour Web avec des cartes à puce, vous devez activer la méthode d'authentification pour chaque site Citrix Receiver pour Web. Pour de plus amples informations, reportez-vous aux instructions de la section [Configurer des sites Citrix Receiver pour Web](#).

Si vous souhaitez que les utilisateurs de cartes à puce aient la possibilité de revenir à l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce, ne désactivez pas la méthode d'authentification avec nom d'utilisateur et mot de passe.

- Si vous prévoyez d'activer l'authentification pass-through lorsque vous installez Citrix Receiver pour Windows sur des machines utilisateur appartenant au domaine, modifiez le fichier default.ica pour le magasin afin d'activer l'authentification pass-through des informations d'identification de carte à puce des utilisateurs lorsqu'ils accèdent à leurs bureaux et applications. Pour plus d'informations, consultez la section [Activer l'authentification pass-through par carte à puce pour Citrix Receiver pour Windows](#).
- Si vous avez créé un serveur virtuel NetScaler Gateway supplémentaire à utiliser uniquement pour les connexions utilisateur aux ressources, configurez le routage NetScaler Gateway optimal via ce serveur virtuel pour les connexions aux déploiements fournissant des bureaux et des applications au magasin. Pour plus d'informations, consultez la section [Configurer un routage HDX optimal pour un magasin](#).
- Pour permettre aux utilisateurs de boîtiers de bureau Windows qui n'appartiennent pas au domaine d'ouvrir une session à leurs bureaux à l'aide de cartes à puce, activez l'authentification par carte à puce à vos sites Desktop Appliance. Pour plus d'informations, consultez la section [Configurer des sites Desktop Appliance](#).

Configurez le site Desktop Appliance pour l'authentification par carte à puce et explicite pour permettre aux utilisateurs d'ouvrir une session avec des informations d'identification explicites s'ils rencontrent des problèmes avec leurs cartes à puce.

- Pour permettre aux utilisateurs de boîtiers de bureau appartenant à un domaine et aux PC réaffectés exécutant Citrix Desktop Lock de s'authentifier à l'aide de cartes à puce, activez l'authentification pass-through avec carte à puce à vos adresses URL XenApp Services. Pour plus d'informations, consultez la section [Configurer l'authentification des adresses URL des sites XenApp Services](#).

Configurer les machines utilisateur

- Assurez-vous que le middleware de votre fournisseur de carte à puce est installé sur toutes les machines utilisateur.
- Pour les utilisateurs équipés de boîtiers de bureau Windows qui n'appartiennent pas au domaine, installez Receiver pour Windows Enterprise à l'aide d'un compte doté d'autorisations d'administrateur. Configurez Internet Explorer pour qu'il démarre en mode plein écran et affiche le site Desktop Appliance lorsque le périphérique est mis sous tension. Notez que les adresses URL des sites Desktop Appliance sont sensibles à la casse. Ajoutez le site Desktop Appliance à la zone Intranet local ou Sites de confiance dans Internet Explorer. Une fois que vous avez confirmé que vous pouvez ouvrir une session sur le site Desktop Appliance avec une carte à puce et accéder aux ressources à partir du magasin, installez Citrix Desktop Lock. Pour de plus amples informations, consultez la section [Pour installer Desktop Lock](#).
- Pour les utilisateurs équipés de boîtiers de bureau qui appartiennent au domaine et de PC réaffectés, installez Receiver pour Windows Enterprise à l'aide d'un compte doté d'autorisations d'administrateur. Configurez Receiver pour Windows

avec l'adresse URL XenApp Services du magasin approprié. Une fois que vous avez confirmé que vous pouvez ouvrir une session sur la machine avec une carte à puce et accéder aux ressources à partir du magasin, installez Citrix Desktop Lock. Pour de plus amples informations, consultez la section [Pour installer Desktop Lock](#).

- Pour tous les autres utilisateurs, installez la version appropriée de Citrix Receiver sur la machine utilisateur. Pour activer l'authentification unique des informations d'identification de la carte à puce sur XenDesktop et XenApp pour les utilisateurs dont les machines appartiennent au domaine, utilisez un compte avec des autorisations d'administrateur pour installer Receiver pour Windows à partir d'une invite de commandes avec l'option /includeSSON. Pour de plus amples informations, consultez la section [Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande](#).

Assurez-vous que Receiver pour Windows est configuré pour l'authentification par carte à puce, soit par le biais d'une stratégie de domaine ou d'une stratégie d'ordinateur local. Pour une stratégie de domaine, utilisez la console de gestion de stratégie de groupe pour importer le fichier de modèle d'objet de stratégie de groupe Receiver pour Windows, icaclient.adm, sur le contrôleur de domaine pour le domaine contenant les comptes de vos utilisateurs. Pour configurer une machine individuelle, utilisez l'Éditeur d'objet de stratégie de groupe sur cette machine pour configurer le modèle. Pour de plus amples informations, consultez la section [Configurer Receiver avec le modèle d'objet de stratégie de groupe](#).

Activez la stratégie Authentification par carte à puce. Pour activer l'authentification unique des informations d'identification de carte à puce des utilisateurs, sélectionnez Utiliser l'authentification pass-through pour le code PIN. Puis, pour transmettre les informations d'identification de carte à puce des utilisateurs à XenDesktop et XenApp, activez la stratégie Nom d'utilisateur et mot de passe locaux et sélectionnez Autoriser l'authentification pass-through pour toutes les connexions ICA. Pour de plus amples informations, consultez la section [Référence des paramètres ICA](#).

Si vous avez activé l'authentification pass-through des informations d'identification de carte à puce à XenDesktop et XenApp pour les utilisateurs équipés de machines appartenant au domaine, ajoutez l'adresse URL du magasin à la zone Intranet local ou Sites de confiance dans Internet Explorer. Assurez-vous que Connexion automatique avec le nom d'utilisateur et le mot de passe est sélectionnée dans les paramètres de sécurité de la zone.

- Si nécessaire, vous devez fournir aux utilisateurs les détails de connexion pour le magasin (pour les utilisateurs sur le réseau interne) ou le boîtier NetScaler Gateway (pour les utilisateurs distants) à l'aide d'une méthode appropriée. Pour de plus amples informations sur la communication des informations de configuration à vos utilisateurs, consultez la section [Citrix Receiver](#).

Activer l'authentification pass-through par carte à puce pour Receiver pour Windows

Vous pouvez activer l'authentification pass-through lorsque vous installez Receiver pour Windows sur des machines utilisateur appartenant au domaine. Pour activer l'authentification unique des informations d'identification de carte à puce des utilisateurs lorsqu'ils accèdent à des applications et bureaux hébergés par XenDesktop et XenApp, vous devez modifier le fichier ica pour le magasin.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Utilisez un éditeur de texte pour ouvrir le fichier ica du magasin, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\storename\App_Data\, où storenamedésigne le nom attribué au magasin au moment de sa création.
2. Pour activer l'authentification pass-through des informations d'identification de carte à puce pour les utilisateurs qui accèdent à des magasins sans NetScaler Gateway, ajoutez le paramètre suivant dans la section [Application].
DisableCtrlAltDel=Off

Ce paramètre s'applique à tous les utilisateurs du magasin. Pour activer l'authentification pass-through au domaine et l'authentification pass-through avec l'authentification par carte à puce à des bureaux et des applications, vous devez créer des magasins distincts pour chaque méthode d'authentification. Ensuite, pointez vos utilisateurs vers le magasin approprié pour leur méthode d'authentification.

3. Pour activer l'authentification pass-through des informations d'identification de carte à puce pour les utilisateurs qui accèdent à des magasins via NetScaler Gateway, ajoutez le paramètre suivant dans la section [Application].

UseLocalUserAndPassword=On

Ce paramètre s'applique à tous les utilisateurs du magasin. Pour activer l'authentification pass-through pour certains utilisateurs et exiger que d'autres ouvrent une session pour accéder à leurs bureaux et applications, vous devez créer des magasins distincts pour chaque groupe d'utilisateurs. Ensuite, pointez vos utilisateurs vers le magasin approprié pour leur méthode d'authentification.

Configurer la période de notification d'expiration du mot de passe

Jun 30, 2017

Si vous autorisez les utilisateurs de sites Citrix Receiver pour Web à modifier leurs mots de passe à tout moment, un avertissement s'affiche à l'attention des utilisateurs locaux dont les mots de passe sont sur le point d'expirer lorsqu'ils ouvrent une session. Par défaut, la période de notification pour un utilisateur est déterminée par le paramètre de stratégie Windows applicable. Pour définir une période de notification personnalisée pour tous les utilisateurs, modifiez le fichier de configuration du service d'authentification.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les méthodes d'authentification**.
3. Sur la page **Gérer les méthodes d'authentification**, à partir du menu déroulant **Nom d'utilisateur et mot de passe > Paramètres**, sélectionnez **Gérer les options de mot de passe**, et cochez la case **Autoriser les utilisateurs à modifier les mots de passe**.
4. Sélectionnez **À tout moment...** et faites un choix dans **Envoyer un rappel aux utilisateurs avant que leur mot de passe expire**.

Remarque : StoreFront ne prend pas en charge les stratégies de mot de passe affinées dans Active Directory.

Configurer et gérer des magasins

Jun 30, 2017

Dans Citrix StoreFront, vous pouvez créer et gérer des magasins qui regroupent des bureaux et applications de XenApp et XenDesktop en offrant aux utilisateurs un accès en libre-service et à la demande aux ressources.

Créer ou supprimer un magasin	Permet de configurer autant de magasins supplémentaires que vous le souhaitez.
Créer un magasin non authentifié	Permet de configurer des magasins non authentifiés supplémentaires afin de permettre l'accès des utilisateurs non authentifiés (anonymes).
Exporter des fichiers de provisioning de magasin pour des utilisateurs	Permet de générer des fichiers contenant les détails de connexion aux magasins, y compris tout déploiement NetScaler Gateway et balise configurés pour les magasins.
Masquer et publier des magasins pour les utilisateurs	Permet d'empêcher les utilisateurs d'ajouter des magasins à leurs comptes lorsqu'ils configurent Citrix Receiver via la découverte de compte basée sur une adresse e-mail ou un nom de domaine complet.
Gérer les ressources mises à disposition dans les magasins	Permet d'ajouter et de supprimer des ressources de magasins.
Gérer l'accès distant aux magasins via NetScaler Gateway	Permet de configurer l'accès aux magasins via NetScaler Gateway pour les utilisateurs se connectant depuis des réseaux publics.
Intégrer des applications Citrix Online à des magasins	Permet de sélectionner les applications Citrix Online que vous souhaitez inclure dans le magasin et d'indiquer l'action que Citrix Receiver entreprend lorsque les utilisateurs s'abonnent à une application Citrix Online.
Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun	Permet de configurer deux magasins StoreFront pour partager une base de données d'abonnement commune.
Paramètres de magasin avancés	Configurez les paramètres avancés du magasin.

Créer ou supprimer un magasin

Jun 30, 2017

Utilisez la tâche Créer un magasin pour configurer d'autres magasins. Vous pouvez créer autant de magasins que vous le souhaitez. Par exemple, vous pouvez créer un magasin pour un groupe particulier d'utilisateurs ou regrouper un ensemble spécifique de ressources. Vous pouvez également créer un magasin non authentifié pour l'accès anonyme. Pour créer ce type de magasin, reportez-vous aux instructions de la section [Créer un magasin non authentifié](#).

Pour créer un magasin, identifiez et configurez les communications avec les serveurs fournissant les ressources que vous souhaitez mettre à disposition dans le magasin. Si vous le souhaitez, vous pouvez également configurer l'accès distant au magasin via NetScaler Gateway.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Ajouter des bureaux et des applications au magasin

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau Actions, cliquez sur Créer un magasin.
3. Sur la page Nom du magasin, spécifiez un nom pour votre magasin, puis cliquez sur Suivant.
Les noms des magasins s'affichent dans Citrix Receiver sous les comptes des utilisateurs, c'est la raison pour laquelle vous devez choisir un nom qui permette aux utilisateurs d'identifier le contenu du magasin.
4. Sur la page Delivery Controller, indiquez l'infrastructure fournissant les ressources que vous souhaitez mettre à disposition dans le magasin. Cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter Delivery Controller, spécifiez un nom qui vous aidera à identifier le déploiement et indiquez si les ressources que vous souhaitez mettre à disposition dans le magasin sont fournies par XenDesktop, XenApp ou AppController. Pour les déploiements App Controller, assurez-vous que le nom que vous avez spécifié ne contient pas d'espaces.
6. Si vous ajoutez les détails de serveurs XenDesktop ou XenApp, passez à l'étape 7. Pour mettre des applications gérées par App Controller à disposition dans le magasin, entrez le nom ou l'adresse IP d'un boîtier virtuel App Controller dans la boîte de dialogue Serveur et spécifiez le port StoreFront à utiliser pour les connexions à App Controller. Le port par défaut est le port 443. Passez à l'étape 11.
7. Pour mettre des bureaux et applications fournis par XenDesktop ou XenApp à disposition dans le magasin, ajoutez les noms ou les adresses IP de vos serveurs dans la liste Serveurs. Spécifiez plusieurs serveurs pour activer la tolérance aux pannes en dressant la liste des entrées par ordre de priorité pour définir le basculement. Pour les sites XenDesktop, spécifiez les détails des Delivery Controller. Dans le cas de batteries XenApp, dressez la liste des serveurs exécutant le service XML Citrix.
8. Sélectionnez dans la liste Type de transport, le type de connexion que StoreFront utilisera pour les communications avec les serveurs.
 - Pour envoyer des données via des connexions non cryptées, sélectionnez HTTP. Si vous sélectionnez cette option, vous devez prendre vos propres dispositions pour sécuriser les connexions entre StoreFront et vos serveurs.
 - Pour envoyer des données via des connexions HTTP sécurisées à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security), sélectionnez HTTPS. Si vous sélectionnez cette option pour les serveurs XenDesktop et XenApp, vérifiez que le service XML Citrix est configuré pour partager son port avec les services Microsoft Internet

Information Services (IIS) et que ces derniers sont configurés pour prendre en charge le protocole HTTPS.

- Pour envoyer des données via des connexions sécurisées sur les serveurs XenApp à l'aide du Relais SSL pour effectuer une authentification hôte et le cryptage de données, sélectionnez Relais SSL.

Remarque : si vous utilisez le protocole HTTPS ou le Relais SSL pour sécuriser les connexions entre StoreFront et vos serveurs, vérifiez que les noms que vous spécifiez dans la liste Serveurs correspondent exactement (casse comprise) aux noms figurant sur les certificats de ces serveurs.

9. Spécifiez le port StoreFront à utiliser pour les connexions aux serveurs. Le port par défaut est 80 pour les connexions utilisant le protocole HTTP et le Relais SSL, et 443 pour les connexions HTTPS. Dans le cas de serveurs XenDesktop et XenApp, le port spécifié doit être le port utilisé par le service XML Citrix.
10. Si vous utilisez le Relais SSL pour sécuriser les connexions entre StoreFront et des serveurs XenApp, indiquez le port TCP du Relais SSL dans la zone Port du Relais SSL. Le port par défaut est le port 443. Assurez-vous que tous les serveurs exécutant le Relais SSL sont configurés pour surveiller le même port.
11. Cliquez sur OK. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop, XenApp et App Controller. Répétez les étapes 4 à 11, si nécessaire, pour répertorier les déploiements supplémentaires qui fournissent des ressources au magasin. Une fois que vous avez ajouté toutes les ressources requises au magasin, cliquez sur Suivant.
12. Sur la page Accès distant, spécifiez si les utilisateurs se connectant depuis des réseaux publics (et la manière dont ils se connectent) peuvent accéder au magasin au travers de NetScaler Gateway.
 - Pour ne pas mettre le magasin à la disposition des utilisateurs sur des réseaux publics, ne sélectionnez pas la case à cocher **Activer l'accès à distance**. Seuls les utilisateurs locaux du réseau interne pourront accéder au magasin.
 - Pour activer l'accès à distance, cochez la case **Activer l'accès à distance**.
 - Pour ne mettre à disposition que les ressources disponibles au travers du magasin via NetScaler Gateway, sélectionnez Aucun tunnel VPN. Les utilisateurs ouvrent une session directement sur NetScaler Gateway et n'ont pas besoin d'utiliser NetScaler Gateway Plug-in.
 - Pour mettre le magasin et les autres ressources du réseau interne à disposition via un tunnel de réseau privé virtuel SSL (VPN), sélectionnez Tunnel VPN complet. Les utilisateurs requièrent NetScaler Gateway Plug-in pour établir le tunnel VPN.

Si elle n'est pas déjà activée, la méthode d'authentification pass-through via NetScaler Gateway est automatiquement activée lorsque vous configurez l'accès distant au magasin. Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

13. Si vous avez activé l'accès à distance, passez à la procédure suivante pour spécifier les déploiements NetScaler Gateway au travers desquels les utilisateurs peuvent accéder au magasin. Sinon, sur la page Accès distant, cliquez sur Créer. Une fois que le magasin a été créé, cliquez sur Terminer.

Fournir l'accès distant au magasin via NetScaler Gateway

Effectuez les étapes suivantes pour configurer l'accès distant via NetScaler Gateway au magasin que vous avez créé dans la procédure précédente. Vous êtes supposé avoir effectué toutes les étapes précédentes.

1. Sur la page **Accès distant** de l'assistant **Créer un magasin**, sélectionnez dans la liste **Boîtiers NetScaler Gateway** les déploiements par le biais desquels les utilisateurs peuvent accéder au magasin. Tout déploiement que vous avez configuré précédemment pour d'autres magasins est disponible pour sélection dans la liste. Si vous souhaitez ajouter un déploiement supplémentaire à la liste, cliquez sur Ajouter. Sinon, passez à l'étape 12.
2. Sur la page **Ajouter un boîtier NetScaler Gateway > Paramètres généraux**, spécifiez un nom pour le déploiement NetScaler Gateway qui permettra aux utilisateurs de l'identifier.
Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans Citrix Receiver. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser le déploiement. Par

exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements NetScaler Gateway pour permettre aux utilisateurs d'identifier facilement le déploiement le plus pratique en fonction de leur situation.

3. Entrez l'URL du serveur virtuel ou le point d'ouverture de session utilisateur pour votre déploiement. Spécifiez la version du produit utilisé dans votre déploiement.

Le nom de domaine complet (FQDN) de votre déploiement StoreFront doit être unique et différent du nom de domaine complet du serveur virtuel NetScaler Gateway. L'utilisation d'un même nom de domaine complet pour StoreFront et le serveur virtuel NetScaler Gateway n'est pas prise en charge.

4. Sélectionnez l'utilisation de NetScaler Gateway dans les options disponibles.
 - + **Authentification et routage HDX** : NetScaler Gateway sera utilisé pour l'authentification, ainsi que pour le routage des sessions HDX.
 - + **Authentification uniquement** : NetScaler Gateway sera utilisé pour l'authentification mais pas pour le routage des sessions HDX.
 - + **Routage HDX uniquement** : NetScaler Gateway sera utilisé pour le routage des sessions HDX mais pas pour l'authentification.
5. Sur la page Secure Ticket Authority (STA), si vous mettez les ressources fournies par XenDesktop ou XenApp à disposition dans le magasin, répertoriez toutes les adresses URL des serveurs qui exécutent la STA sur la page Secure Ticket Authority. Saisissez les adresses URL de plusieurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs par ordre de priorité pour définir la séquence de basculement.

La STA est hébergée sur les serveurs XenDesktop et XenApp, et émet des tickets de session en réponse à des demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources XenDesktop et XenApp.

6. Choisissez d'équilibrer la charge de la Secure Ticket Authority. Vous pouvez également spécifier l'intervalle de temps après lequel les STA qui ne répondent pas sont ignorées.
7. Si vous souhaitez que XenDesktop et XenApp laissent les sessions déconnectées ouvertes lorsque Citrix Receiver tente de se reconnecter automatiquement, cochez la case **Activer la fiabilité de session**. Si vous avez configuré plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, cochez la case **Demander des tickets de deux STA, si possible**. StoreFront obtient des tickets de deux STA différentes de façon à ce que les sessions utilisateur ne soient pas interrompues si l'une des STA devenait indisponible au cours de la session. Si pour une raison quelconque, StoreFront ne parvient pas à contacter deux STA, il en utilise une seule.
8. Sur la page Paramètres d'authentification, sélectionnez la version de NetScaler Gateway que vous souhaitez configurer.
9. Spécifiez l'adresse IP VServer du boîtier NetScaler Gateway, si nécessaire. Une adresse IP VServer est requise pour les boîtiers Access Gateway 9.x, mais facultative pour les versions plus récentes du produit. L'adresse IP correspond à l'adresse IP VServer que NetScaler Gateway utilise pour représenter la machine utilisateur dans les communications avec les serveurs sur le réseau interne. Il peut également s'agir de l'adresse IP mappée du boîtier NetScaler Gateway. Lorsque cela est spécifié, StoreFront utilise l'adresse IP VServer pour vérifier que les requêtes entrantes proviennent d'une machine approuvée.
10. Sélectionnez dans la liste Type d'ouverture de session la méthode d'authentification que vous avez configurée sur le boîtier pour les utilisateurs de Citrix Receiver. Les informations que vous fournissez sur la configuration de votre boîtier NetScaler Gateway sont ajoutées au fichier de provisioning pour le magasin. Ceci permet à Citrix Receiver d'envoyer une demande de connexion appropriée lorsque vous contactez le boîtier pour la première fois.
 - Si les utilisateurs sont tenus de saisir leurs informations d'identification de domaine Microsoft Active Directory, sélectionnez Domaine.

- Si les utilisateurs doivent saisir un code de jeton obtenu à partir d'un jeton de sécurité, sélectionnez Jeton de sécurité.
- Si les utilisateurs sont tenus de saisir leurs identifiants de domaine et un code de jeton obtenu à partir d'un jeton de sécurité, sélectionnez Domaine et jeton de sécurité.
- Si les utilisateurs sont tenus de saisir un mot de passe ponctuel envoyé par SMS, sélectionnez Authentification SMS.
- Si les utilisateurs sont tenus de présenter une carte à puce et d'entrer un code PIN, sélectionnez Carte à puce.

Si vous configurez l'authentification avec carte à puce avec une méthode d'authentification secondaire à laquelle les utilisateurs peuvent revenir s'ils rencontrent des problèmes avec leur carte à puce, sélectionnez la méthode d'authentification secondaire dans la liste Carte à puce de remplacement.

- Entrez l'adresse URL du service d'authentification de NetScaler Gateway dans la case URL de rappel. Il s'agit d'un champ facultatif. StoreFront ajoute automatiquement la partie standard de l'URL. Entrez l'adresse URL du boîtier accessible en interne. StoreFront contacte le service d'authentification NetScaler Gateway pour vérifier que les requêtes reçues de NetScaler Gateway proviennent de ce boîtier.
- Cliquez sur **Créer** pour ajouter votre déploiement NetScaler Gateway à la liste sur la page Accès distant. Répétez les étapes 1 à 11, si nécessaire, pour ajouter plus de déploiements NetScaler Gateway à la liste Boîtiers NetScaler Gateway. Si vous activez l'accès au travers de plusieurs déploiements en sélectionnant plus d'une entrée dans la liste, spécifiez le déploiement par défaut à utiliser pour accéder au magasin.
- Sur la page Accès distant, cliquez sur **Créer**. Une fois que le magasin a été créé, cliquez sur **Terminer**.

Les utilisateurs peuvent désormais accéder à votre magasin avec Citrix Receiver, qui doit être configuré avec les détails d'accès au magasin. Il existe plusieurs méthodes vous permettant de fournir ces détails aux utilisateurs afin de faciliter le processus de configuration. Pour plus d'informations, veuillez consulter la section [Options d'accès utilisateur](#).

Éventuellement, les utilisateurs peuvent accéder au magasin via le site Receiver pour Web, ce qui leur permet d'accéder à leurs bureaux et applications via une page Web. L'adresse URL permettant aux utilisateurs d'accéder au site Receiver pour Web du nouveau magasin s'affiche lorsque vous créez le magasin.

Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services est activée par défaut. Les utilisateurs équipés de boîtiers de bureau membres du domaine et de PC réaffectés qui exécutent Citrix Desktop Lock, ainsi que les utilisateurs disposant de clients Citrix plus anciens qui ne peuvent pas être mis à niveau, peuvent accéder aux magasins directement à l'aide de l'adresse URL XenApp Services du magasin. L'adresse URL XenApp Services s'affiche au format `http[s]://adresseserveur/Citrix/nomdumagasin/PNAgent/config.xml`, où `adresseserveur` est le nom de domaine complet du serveur ou de l'environnement d'équilibrage de charge de votre déploiement StoreFront et `nomdumagasin` le nom spécifié pour le magasin lors de sa création à l'étape 3.

Créer un magasin pour les déploiements à un seul serveur sur un serveur n'appartenant pas à un domaine

- Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
- Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Créer un magasin**.
- Sur la page **Nom du magasin**, spécifiez un nom pour votre magasin, puis cliquez sur **Suivant**.
Les noms des magasins s'affichent dans Citrix Receiver sous les comptes des utilisateurs, c'est la raison pour laquelle vous devez choisir un nom qui permette aux utilisateurs d'identifier le contenu du magasin.
- Sur la page **Delivery Controller**, indiquez l'infrastructure fournissant les ressources que vous souhaitez mettre à disposition dans le magasin. Cliquez sur **Ajouter**.
- Dans la boîte de dialogue **Ajouter Delivery Controller**, spécifiez un nom qui vous aidera à identifier le déploiement et indiquez si les ressources que vous souhaitez mettre à disposition dans le magasin sont fournies par XenDesktop, XenApp

ou XenMobile AppController. Pour les déploiements App Controller, assurez-vous que le nom que vous avez spécifié ne contient pas d'espaces.

6. Si vous ajoutez les détails de serveurs XenDesktop ou XenApp, passez à l'étape 7. Pour mettre des applications gérées par App Controller à disposition dans le magasin, entrez le nom ou l'adresse IP d'un boîtier virtuel App Controller dans la boîte de dialogue Serveur et spécifiez le port StoreFront à utiliser pour les connexions à App Controller. Le port par défaut est le port 443. Passez à l'étape 11.
7. Pour mettre des bureaux et applications fournis par XenDesktop ou XenApp à disposition dans le magasin, ajoutez les noms ou les adresses IP de vos serveurs dans la liste **Serveurs**. Pour les sites XenDesktop, spécifiez les détails des Delivery Controller. Dans le cas de batteries XenApp, répertoriez le serveur exécutant le service XML Citrix.
8. Sélectionnez dans la liste **Type de transport**, le type de connexion que StoreFront utilisera pour les communications avec le serveur.
 - Pour envoyer des données via des connexions non cryptées, sélectionnez HTTP. Si vous sélectionnez cette option, vous devez prendre vos propres dispositions pour sécuriser les connexions entre StoreFront et votre serveur.
 - Pour envoyer des données via une connexion HTTP sécurisée à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security), sélectionnez HTTPS. Si vous sélectionnez cette option pour les serveurs XenDesktop et XenApp, vérifiez que le service XML Citrix est configuré pour partager son port avec les services Microsoft Internet Information Services (IIS) et que ces derniers sont configurés pour prendre en charge le protocole HTTPS.
 - Pour envoyer des données via des connexions sécurisées sur les serveurs XenApp à l'aide du Relais SSL pour effectuer une authentification hôte et le cryptage de données, sélectionnez Relais SSL.

Remarque : si vous utilisez le protocole HTTPS ou le Relais SSL pour sécuriser les connexions entre StoreFront et vos serveurs, vérifiez que les noms que vous spécifiez dans la liste **Serveurs** correspondent exactement (casse comprise) aux noms figurant sur les certificats de ces serveurs.

9. Spécifiez le port StoreFront à utiliser pour les connexions au serveur. Le port par défaut est 80 pour les connexions utilisant le protocole HTTP et le Relais SSL, et 443 pour les connexions HTTPS. Dans le cas de serveurs XenDesktop et XenApp, le port spécifié doit être le port utilisé par le service XML Citrix.
10. Si vous utilisez le Relais SSL pour sécuriser les connexions entre StoreFront et une batterie XenApp, indiquez le port TCP du Relais SSL dans la zone Port du Relais SSL. Le port par défaut est le port 443. Assurez-vous que tous les serveurs exécutant le Relais SSL sont configurés pour surveiller le même port.
11. Cliquez sur **OK**. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop, XenApp et App Controller. Répétez les étapes 4 à 11, si nécessaire, pour répertorier les déploiements supplémentaires qui fournissent des ressources au magasin. Une fois que vous avez ajouté toutes les ressources requises au magasin, cliquez sur Suivant.
12. Sur la page **Accès distant**, spécifiez si les utilisateurs se connectant depuis des réseaux publics (et la manière dont ils se connectent) peuvent accéder au magasin au travers de NetScaler Gateway.
 - Pour rendre le magasin non disponible auprès des utilisateurs sur les réseaux publics, sélectionnez **Aucun**. Seuls les utilisateurs locaux du réseau interne pourront accéder au magasin.
 - Pour ne mettre à disposition que les ressources disponibles au travers du magasin via NetScaler Gateway, sélectionnez **Aucun tunnel VPN**. Les utilisateurs ouvrent une session directement sur NetScaler Gateway et n'ont pas besoin d'utiliser NetScaler Gateway Plug-in.
 - Pour mettre le magasin et les autres ressources du réseau interne à disposition via un tunnel de réseau privé virtuel SSL (VPN), sélectionnez **Tunnel VPN complet**. Les utilisateurs requièrent NetScaler Gateway Plug-in pour établir le tunnel VPN.

Si elle n'est pas déjà activée, la méthode d'authentification pass-through via NetScaler Gateway est

automatiquement activée lorsque vous configurez l'accès distant au magasin. Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

13. Si vous avez activé l'accès à distance, passez à la procédure [Fournir l'accès distant au magasin via NetScaler Gateway](#) pour spécifier les déploiements NetScaler Gateway au travers desquels les utilisateurs peuvent accéder au magasin. Sinon, sur la page **Accès distant**, cliquez sur **Suivant**.
14. Sur la page **Configurer les méthodes d'authentification**, sélectionnez les méthodes que vos utilisateurs peuvent utiliser pour s'authentifier et accéder aux ressources et cliquez sur **Suivant**.
15. Sur la page **Configurer la validation du mot de passe**, sélectionnez les Delivery Controller qui fourniront la validation du mot de passe et cliquez sur **Suivant**.
16. Sur la page **URL XenApp Services**, configurez l'adresse URL pour les utilisateurs qui utilisent PNAgent pour accéder à l'application et aux bureaux et cliquez sur **Créer**.

Les panneaux **Nœud Groupe de serveurs** et **Action** sont remplacés par **Changer l'URL de base**. La seule option disponible est la modification de l'adresse URL de base, car les groupes de serveurs ne sont pas disponibles dans des serveurs n'appartenant pas à un domaine.

Supprimer un magasin

Utilisez la tâche Supprimer le magasin pour supprimer un magasin. Lorsque vous supprimez un magasin, les sites Receiver pour Web, les sites Desktop Appliance et les adresses URL XenApp Services associés sont également supprimés.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Créer un magasin non authentifié

Jun 30, 2017

Utilisez la tâche Créer un magasin pour configurer des magasins non authentifiés supplémentaires afin de prendre en charge les utilisateurs (anonymes) non authentifiés. Vous pouvez créer autant de magasins non authentifiés que vous le souhaitez. Par exemple, vous pouvez créer un magasin non authentifié pour un groupe particulier d'utilisateurs ou regrouper un ensemble spécifique de ressources.

L'accès distant via NetScaler Gateway ne peut pas être appliqué à des magasins non authentifiés.

Pour créer un magasin non authentifié, identifiez et configurez les communications avec les serveurs fournissant les ressources que vous souhaitez mettre à disposition dans le magasin.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Ajouter des bureaux et des applications au magasin

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau Actions, cliquez sur Créer un magasin.
3. Sur la page Nom du magasin, spécifiez un nom pour votre magasin, sélectionnez **Autoriser uniquement les utilisateurs non authentifiés (anonymes) à accéder à ce magasin**, puis cliquez sur Suivant.
Les noms des magasins s'affichent dans Citrix Receiver sous les comptes des utilisateurs, c'est la raison pour laquelle vous devez choisir un nom qui permette aux utilisateurs d'identifier le contenu du magasin.
4. Sur la page **Delivery** Controller, indiquez l'infrastructure fournissant les ressources que vous souhaitez mettre à disposition dans le magasin. Cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter Delivery Controller, spécifiez un nom qui vous aidera à identifier le déploiement et indiquez si les ressources que vous souhaitez mettre à disposition dans le magasin sont fournies par XenApp ou XenMobile (AppController). Pour les déploiements XenMobile (App Controller), assurez-vous que le nom que vous avez spécifié ne contient pas d'espaces. Lorsque vous attribuez des Controller, veillez à n'utiliser que ceux qui prennent en charge la fonctionnalité d'applications anonymes. Si vous configurez votre magasin non authentifié avec des Controller qui ne prennent pas en charge cette fonctionnalité, il est possible qu'aucune application anonyme ne soit disponible dans le magasin.
6. Si vous ajoutez les détails de serveurs XenApp, passez à l'étape 7. Pour mettre des applications gérées par XenMobile (AppController) à disposition dans le magasin, entrez le nom ou l'adresse XenMobile (App Controller) d'un boîtier virtuel App Controller dans la boîte de dialogue Serveur et spécifiez le port IP à utiliser pour les connexions à XenMobile (App Controller). Le port par défaut est le port 443. Passez à l'étape 10.
7. Pour mettre des bureaux et applications fournis par XenApp à disposition dans le magasin, ajoutez les noms ou les adresses IP de vos serveurs dans la liste Serveurs. Spécifiez plusieurs serveurs pour activer la tolérance aux pannes en dressant la liste des entrées par ordre de priorité pour définir le basculement. Pour les sites XenDesktop, spécifiez les détails des Controller. Dans le cas de batteries XenApp, dressez la liste des serveurs exécutant le service XML Citrix.
8. Sélectionnez dans la liste Type de transport, le type de connexion que StoreFront utilisera pour les communications avec les serveurs.
 - Pour envoyer des données via des connexions non cryptées, sélectionnez HTTP. Si vous sélectionnez cette option, vous devez prendre vos propres dispositions pour sécuriser les connexions entre StoreFront et vos serveurs.

- Pour envoyer des données via des connexions HTTP sécurisées à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security), sélectionnez HTTPS. Si vous sélectionnez cette option pour les serveurs XenDesktop et XenApp, vérifiez que le service XML Citrix est configuré pour partager son port avec les services Microsoft Internet Information Services (IIS) et que ces derniers sont configurés pour prendre en charge le protocole HTTPS.

Remarque : si vous utilisez le protocole HTTPS pour sécuriser les connexions entre StoreFront et vos serveurs, vérifiez que les noms que vous spécifiez dans la liste Serveurs correspondent exactement (casse comprise) aux noms figurant sur les certificats de ces serveurs.

9. Spécifiez le port StoreFront à utiliser pour les connexions aux serveurs. Le port par défaut est 80 pour les connexions utilisant le protocole HTTP et 443 pour les connexions HTTPS. Dans le cas de serveurs XenDesktop et XenApp, le port spécifié doit être le port utilisé par le service XML Citrix.
10. Cliquez sur OK. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop, XenApp et App Controller. Répétez les étapes 4 à 10, si nécessaire, pour répertorier les déploiements supplémentaires qui fournissent des ressources au magasin. Une fois que vous avez ajouté toutes les ressources requises au magasin, cliquez sur Créer.

Votre magasin non authentifié est maintenant disponible. Pour permettre aux utilisateurs d'accéder au nouveau magasin, Citrix Receiver doit être configuré avec les détails d'accès au magasin. Il existe plusieurs méthodes vous permettant de fournir ces détails aux utilisateurs afin de faciliter le processus de configuration. Pour plus d'informations, veuillez consulter la section [Options d'accès utilisateur](#).

Éventuellement, les utilisateurs peuvent accéder au magasin via le site Receiver pour Web, ce qui leur permet d'accéder à leurs bureaux et applications via une page Web. Par défaut avec les magasins non authentifiés, Receiver pour Web affiche les applications dans une hiérarchie de dossiers qui comprend un chemin de navigation. L'adresse URL permettant aux utilisateurs d'accéder au site Receiver pour Web du nouveau magasin s'affiche lorsque vous créez le magasin.

Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services est activée par défaut. Les utilisateurs équipés de boîtiers de bureau membres du domaine et de PC réaffectés qui exécutent Citrix Desktop Lock, ainsi que les utilisateurs disposant de clients Citrix plus anciens qui ne peuvent pas être mis à niveau, peuvent accéder aux magasins directement à l'aide de l'adresse URL XenApp Services du magasin. L'adresse URL XenApp Services s'affiche au format `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`, où `serveraddress` est le nom de domaine complet du serveur ou de l'environnement d'équilibrage de charge de votre déploiement StoreFront et `storename` le nom spécifié pour le magasin à l'étape 3.

Remarque : dans les configurations StoreFront dans lesquelles le fichier `web.config` a été configuré avec le paramètre `LogoffAction="terminate"`, les sessions Citrix Receiver pour Web qui accèdent à ce magasin non authentifié ne se ferment pas. Le fichier `web.config` se trouve généralement dans `C:\inetpub\wwwroot\Citrix\storename\`, où `storename` est le nom spécifié pour le magasin lors de sa création. Pour vous assurer que ces sessions sont correctement fermées, l'option d'approbation des requêtes XML doit être activée sur le serveur XenApp utilisé par ce magasin comme indiqué dans la section *Configuration du port et de l'approbation du Service XML Citrix* dans la documentation XenApp et XenDesktop.

Exporter des fichiers de provisioning de magasin pour des utilisateurs

Jun 30, 2017

Utilisez les tâches Exporter le fichier de provisioning multi-magasins et Exporter le fichier de provisioning pour générer des fichiers contenant les détails de connexion des magasins, y compris les déploiements NetScaler Gateway et les balises configurées pour les magasins. Mettez ces fichiers à la disposition des utilisateurs pour leur permettre de configurer Citrix Receiver automatiquement avec les détails relatifs aux magasins. Les utilisateurs peuvent également obtenir les fichiers de provisioning Citrix Receiver à partir de sites Receiver pour Web.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront.
2. Pour générer un fichier de provisioning contenant les détails relatifs à plusieurs magasins, dans le panneau Actions, cliquez sur Exporter le fichier de provisioning multi-magasins, puis sélectionnez les magasins que vous souhaitez inclure dans ce fichier.
3. Cliquez sur Exporter et enregistrez le fichier de provisioning avec une extension .cr vers un emplacement approprié de votre réseau.

Publier et masquer des magasins pour les utilisateurs

Jun 30, 2017

Utilisez la tâche Masquer le magasin pour empêcher les utilisateurs d'ajouter des magasins à leurs comptes lorsqu'ils configurent Citrix Receiver via la découverte de compte basée sur une adresse e-mail ou un nom de domaine complet. Par défaut, lorsque vous créez un magasin, les utilisateurs ont la possibilité de l'ajouter dans Citrix Receiver lorsqu'ils découvrent le déploiement StoreFront hébergeant le magasin. Le fait de masquer un magasin ne le rend pas inaccessible, mais les utilisateurs doivent configurer Citrix Receiver avec les informations de connexion au magasin, manuellement, à l'aide d'une adresse URL de configuration ou avec un fichier de provisioning. Pour reprendre la publication d'un magasin masqué, utilisez la tâche Publier magasin.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Configurer les paramètres du magasin > Publier magasin**.
3. Sur la page **Publier magasin**, sélectionnez **Publier magasin** ou **Masquer le magasin**.

Gérer les ressources mises à disposition dans les magasins

Jun 30, 2017

Utilisez la tâche Gérer les Delivery Controller pour ajouter et supprimer, des magasins, des ressources fournies par XenDesktop, XenApp et App Controller, et pour modifier les détails des serveurs offrant ces ressources.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau Actions, cliquez sur Gérer les Delivery Controller.
3. Dans la boîte de dialogue Gérer les Delivery Controller, cliquez sur Ajouter pour inclure les bureaux et applications provenant d'un autre déploiement XenDesktop, XenApp ou App Controller au magasin. Pour modifier les paramètres d'un déploiement, sélectionnez l'entrée dans la liste Delivery Controller et cliquez sur Modifier. Sélectionnez une entrée dans la liste, puis cliquez sur Supprimer pour empêcher les ressources fournies par le déploiement d'être disponibles dans le magasin.
4. Dans la boîte de dialogue Ajouter Controller ou Modifier Controller, spécifiez un nom qui vous aidera à identifier le déploiement et indiquez si les ressources que vous souhaitez mettre à disposition dans le magasin sont fournies par XenDesktop, XenApp ou AppController. Pour les déploiements App Controller, assurez-vous que le nom que vous avez spécifié ne contient pas d'espaces.
5. Si vous ajoutez les détails de serveurs XenDesktop ou XenApp, passez à l'étape 6. Pour mettre des applications gérées par App Controller à disposition dans le magasin, entrez le nom ou l'adresse IP d'un boîtier virtuel App Controller dans la boîte de dialogue Serveur et spécifiez le port StoreFront à utiliser pour les connexions à App Controller. Le port par défaut est le port 443. Passez à l'étape 10.
6. Pour mettre des bureaux et applications fournis par XenDesktop ou XenApp à disposition dans le magasin, cliquez sur Ajouter pour entrer le nom ou l'adresse IP d'un serveur. En fonction de la façon dont le fichier web.config est configuré, la spécification de multiples serveurs active soit l'équilibrage de charge, soit le basculement, comme indiqué dans la boîte de dialogue. L'équilibrage de charge est configuré par défaut. Si le basculement est configuré, dressez la liste des serveurs par ordre de priorité pour définir le basculement. Pour les sites XenDesktop, spécifiez les détails des Delivery Controller. Dans le cas de batteries XenApp, dressez la liste des serveurs exécutant le service XML Citrix. Pour modifier le nom ou l'adresse IP d'un serveur, sélectionnez l'entrée dans la liste Serveurs, puis cliquez sur Modifier. Sélectionnez une entrée dans la liste puis cliquez sur Supprimer pour empêcher StoreFront de contacter le serveur pour énumérer les ressources disponibles auprès de l'utilisateur.
7. Sélectionnez dans la liste Type de transport, le type de connexion que StoreFront utilisera pour les communications avec les serveurs.
 - Pour envoyer des données via des connexions non cryptées, sélectionnez HTTP. Si vous sélectionnez cette option, vous devez prendre vos propres dispositions pour sécuriser les connexions entre StoreFront et vos serveurs.
 - Pour envoyer des données via des connexions HTTP sécurisées à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security), sélectionnez HTTPS. Si vous sélectionnez cette option pour les serveurs XenDesktop et XenApp, vérifiez que le service XML Citrix est configuré pour partager son port avec les services Microsoft Internet Information Services (IIS) et que ces derniers sont configurés pour prendre en charge le protocole HTTPS.
 - Pour envoyer des données via des connexions sécurisées sur les serveurs XenApp à l'aide du Relais SSL pour effectuer

une authentification hôte et le cryptage de données, sélectionnez Relais SSL.

Remarque : si vous utilisez le protocole HTTPS ou le Relais SSL pour sécuriser les connexions entre StoreFront et vos serveurs, vérifiez que les noms que vous spécifiez dans la liste Serveurs correspondent exactement (casse comprise) aux noms figurant sur les certificats de ces serveurs.

8. Spécifiez le port StoreFront à utiliser pour les connexions aux serveurs. Le port par défaut est 80 pour les connexions utilisant le protocole HTTP et le Relais SSL, et 443 pour les connexions HTTPS. Dans le cas de serveurs XenDesktop et XenApp, le port spécifié doit être le port utilisé par le service XML Citrix.
9. Si vous utilisez le Relais SSL pour sécuriser les connexions entre StoreFront et des serveurs XenApp, indiquez le port TCP du Relais SSL dans la zone Port du Relais SSL. Le port par défaut est le port 443. Assurez-vous que tous les serveurs exécutant le Relais SSL sont configurés pour surveiller le même port.
10. Cliquez sur OK. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop, XenApp et App Controller. Répétez les étapes 3 à 10, si nécessaire, pour ajouter des déploiements supplémentaires ou les modifier dans la liste Delivery Controller.

Gérer l'accès distant aux magasins via NetScaler Gateway

Jun 30, 2017

Utilisez la tâche Paramètres d'accès distant pour configurer l'accès aux magasins via NetScaler Gateway pour les utilisateurs se connectant depuis des réseaux publics. L'accès distant via NetScaler Gateway ne peut pas être appliqué à des magasins non authentifiés.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau Actions, cliquez sur **Configurer** Paramètres d'accès distant.
3. Dans la boîte de dialogue **Configurer** Paramètres d'accès distant, spécifiez si les utilisateurs se connectant depuis des réseaux publics (et la manière dont ils se connectent) peuvent accéder au magasin via NetScaler Gateway.
 - Pour ne pas mettre le magasin à la disposition des utilisateurs sur des réseaux publics, ne sélectionnez pas la case à cocher **Activer l'accès à distance**. Seuls les utilisateurs locaux du réseau interne pourront accéder au magasin.
 - Pour activer l'accès à distance, cochez la case **Activer l'accès à distance**.
 - Pour ne mettre à disposition que les ressources disponibles au travers du magasin via NetScaler Gateway, sélectionnez Aucun tunnel VPN. Les utilisateurs ouvrent une session directement sur NetScaler Gateway et n'ont pas besoin d'utiliser NetScaler Gateway Plug-in.
 - Pour mettre le magasin et les autres ressources du réseau interne à disposition via un tunnel VPN SSL, sélectionnez Tunnel VPN complet. Les utilisateurs requièrent NetScaler Gateway Plug-in pour établir le tunnel VPN.

Si elle n'est pas déjà activée, la méthode d'authentification pass-through via NetScaler Gateway est automatiquement activée lorsque vous configurez l'accès distant au magasin. Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

4. Si vous avez activé l'accès à distance, sélectionnez dans la liste Boîtiers NetScaler Gateway les déploiements par le biais desquels les utilisateurs accèdent au magasin. Les déploiements que vous avez configurés précédemment pour ce magasin et d'autres magasins sont disponibles pour sélection dans la liste. Si vous souhaitez ajouter un déploiement supplémentaire à la liste, cliquez sur Ajouter. Sinon, passez à l'étape 16.
5. Sur la page Paramètres généraux, indiquez le nom pour le déploiement NetScaler Gateway qui permettra aux utilisateurs de l'identifier.

Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans Citrix Receiver. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser le déploiement. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements NetScaler Gateway pour permettre aux utilisateurs d'identifier facilement le déploiement le plus pratique en fonction de leur situation.
6. Entrez l'URL du serveur virtuel ou le point d'ouverture de session utilisateur (pour Access Gateway 5.0) pour votre déploiement. Spécifiez la version du produit utilisé dans votre déploiement.

Le nom de domaine complet (FQDN) de votre déploiement StoreFront doit être unique et différent du nom de domaine complet du serveur virtuel NetScaler Gateway. L'utilisation d'un même nom de domaine complet pour StoreFront et le

serveur virtuel NetScaler Gateway n'est pas prise en charge.

7. Si vous ajoutez un déploiement Access Gateway 5.0, passez à l'étape 9. Sinon, spécifiez l'adresse IP de sous-réseau du boîtier NetScaler Gateway, si nécessaire. Une adresse IP de sous-réseau est requise pour les boîtiers Access Gateway 9.3, mais facultative pour les versions plus récentes du produit.
L'adresse de sous-réseau correspond à l'adresse IP que NetScaler Gateway utilise pour représenter la machine utilisateur dans les communications avec les serveurs sur le réseau interne. Il peut également s'agir de l'adresse IP mappée du boîtier NetScaler Gateway. Lorsque cela est spécifié, StoreFront utilise l'adresse IP du sous-réseau pour vérifier que les requêtes entrantes proviennent d'une machine approuvée.
8. Si vous ajoutez un boîtier exécutant NetScaler Gateway 11, NetScaler Gateway 10.1, Access Gateway 10 ou Access Gateway 9.3, sélectionnez dans la liste Type d'ouverture de session la méthode d'authentification que vous avez configurée sur le boîtier pour les utilisateurs de Citrix Receiver.
Les informations que vous fournissez sur la configuration de votre boîtier NetScaler Gateway sont ajoutées au fichier de provisioning pour le magasin. Ceci permet à Citrix Receiver d'envoyer une demande de connexion appropriée lorsque vous contactez le boîtier pour la première fois.
 - Si les utilisateurs sont tenus de saisir leurs informations d'identification de domaine Microsoft Active Directory, sélectionnez Domaine.
 - Si les utilisateurs sont tenus de saisir un code de jeton obtenu à partir d'un jeton de sécurité, sélectionnez Jeton de sécurité.
 - Si les utilisateurs sont tenus de saisir leurs identifiants de domaine et un code de jeton obtenu à partir d'un jeton de sécurité, sélectionnez Domaine et jeton de sécurité.
 - Si les utilisateurs sont tenus de saisir un mot de passe ponctuel envoyé par SMS, sélectionnez Authentification SMS.
 - Si les utilisateurs sont tenus de présenter une carte à puce et d'entrer un code PIN, sélectionnez Carte à puce.Si vous configurez l'authentification avec carte à puce avec une méthode d'authentification secondaire sur laquelle les utilisateurs peuvent se rabattre s'ils rencontrent des problèmes avec leur carte à puce, sélectionnez la méthode d'authentification secondaire dans la liste Carte à puce de remplacement. Passez à l'étape 10.
9. Pour ajouter un déploiement Access Gateway 5.0, indiquez si le point d'ouverture de session de l'utilisateur est hébergé sur un boîtier autonome ou un serveur Access Controller qui fait partie d'un cluster. Si vous ajoutez un cluster, cliquez sur Suivant puis passez à l'étape 11.
10. Si vous configurez StoreFront pour NetScaler Gateway 11, NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3, ou un seul boîtier Access Gateway 5.0, entrez l'adresse URL du service d'authentification NetScaler Gateway dans la case URL de rappel. StoreFront ajoute automatiquement la partie standard de l'URL. Cliquez sur Suivant et passez à l'étape 13.
Entrez l'adresse URL du boîtier accessible en interne. StoreFront contacte le service d'authentification NetScaler Gateway pour vérifier que les requêtes reçues de NetScaler Gateway proviennent de ce boîtier.
11. Pour configurer StoreFront pour un cluster Access Gateway 5.0, indiquez sur la page Boîtiers la liste des adresses IP ou des noms de domaine complets des boîtiers dans le cluster et cliquez sur Suivant.
12. Sur la page Activer l'authentification silencieuse, dressez la liste des adresses URL du service d'authentification exécuté sur les serveurs Access Controller. Ajoutez les adresses URL de plusieurs serveurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs par ordre de priorité pour définir la séquence de basculement. Cliquez sur Suivant.
StoreFront utilise le service d'authentification pour authentifier les utilisateurs distants afin de leur éviter de ressaisir leurs informations d'identification lorsqu'ils accèdent aux magasins.
13. Pour tous les déploiements, si vous mettez les ressources fournies par XenDesktop ou XenApp à disposition dans le

magasin, répertoriez les adresses URL des serveurs qui exécutent la STA sur la page Secure Ticket Authority (STA). Saisissez les adresses URL de plusieurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs par ordre de priorité pour définir la séquence de basculement. La STA est hébergée sur les serveurs XenDesktop et XenApp, et émet des tickets de session en réponse à des demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources XenDesktop et XenApp.

14. Si vous souhaitez que XenDesktop et XenApp laissent les sessions déconnectées ouvertes lorsque Citrix Receiver tente de se reconnecter automatiquement, cochez la case Activer la fiabilité de session. Si vous avez configuré plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, cochez la case Demander des tickets de deux STA, si possible.
Lorsque la case Demander des tickets de deux STA, si possible est cochée, StoreFront obtient des tickets de deux STA différentes de façon à ce que les sessions utilisateur ne soient pas interrompues si l'une des STA devenait indisponible au cours de la session. Si pour une raison quelconque, StoreFront ne parvient pas à contacter deux STA, il en utilise une seule.
15. Cliquez sur Créer pour ajouter votre déploiement NetScaler Gateway à la liste dans la boîte de dialogue Paramètres d'accès distant.
16. Répétez les étapes 4 à 15, si nécessaire, pour ajouter plus de déploiements NetScaler Gateway à la liste Boîtiers NetScaler Gateway. Si vous activez l'accès au travers de plusieurs déploiements en sélectionnant plus d'une entrée dans la liste, spécifiez le déploiement par défaut à utiliser pour accéder au magasin.

Intégrer des applications Citrix Online à des magasins

Jun 30, 2017

Exécutez la tâche Citrix Online Integration pour sélectionner les applications Citrix Online à inclure dans un magasin, et indiquer l'action que Citrix Receiver devra mettre en place lorsque les utilisateurs s'abonnent à une application Citrix Online.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau Actions, cliquez sur **Configurer les paramètres du magasin >** Citrix Online Integration.
3. Sélectionnez les applications Citrix Online que vous souhaitez inclure dans le magasin et indiquez l'action que Citrix Receiver devra mettre en place lorsque les utilisateurs s'abonnent à une application Citrix Online.
 - Si vous souhaitez autoriser les utilisateurs ne possédant pas de compte pour les applications sélectionnées à visiter le site Web de Citrix et créer des comptes d'évaluation personnels, sélectionnez Aider les utilisateurs à créer un compte d'évaluation, si besoin est.
 - Si vous souhaitez inviter les utilisateurs à contacter l'administrateur système pour obtenir un compte pour les applications sélectionnées, sélectionnez Demander aux utilisateurs de contacter leur service d'assistance.
 - Si les comptes de tous les utilisateurs sont déjà en place pour les applications sélectionnées, choisissez Ajouter l'application immédiatement.

Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun

Jun 30, 2017

À compter de la version 2.0, StoreFront n'utilise plus de base de données SQL pour stocker ses données d'abonnement. Citrix a remplacé la base de données SQL par un magasin de données Windows qui ne requiert aucune configuration supplémentaire lorsque StoreFront est installé en premier. Le programme d'installation installe le magasin de données Windows localement sur chaque serveur StoreFront. Dans les environnements de groupes de serveurs StoreFront, chaque serveur stocke également une copie des données d'abonnement utilisées par le magasin. Ces données sont propagées sur les autres serveurs afin de garder à jour les abonnements utilisateur sur l'ensemble du groupe. Par défaut, StoreFront crée un seul magasin de données pour chaque magasin. Chaque magasin de données d'abonnement est mis à jour indépendamment de chaque magasin.

Lorsque des paramètres de configuration différents sont requis, il est pratique courante chez les administrateurs de configurer StoreFront avec deux magasins distincts ; un pour l'accès externe aux ressources à l'aide d'un Netscaler Gateway et un autre pour l'accès interne à l'aide du réseau local d'entreprise. Vous pouvez configurer deux magasins « externe » et « interne » pour partager un magasin de données d'abonnement commun en effectuant une simple modification au fichier web.config du magasin.

Dans les scénarios impliquant deux magasins et leurs magasins de données d'abonnement correspondant, un utilisateur doit s'abonner à la même ressource deux fois. La configuration de deux magasins afin de partager une base de données d'abonnement commune améliore et simplifie l'expérience d'itinérance lorsque les utilisateurs accèdent à la même ressource à l'intérieur ou à l'extérieur du réseau de l'entreprise. Avec un magasin de données d'abonnement partagé, il importe peu que les utilisateurs utilisent le magasin « externe » ou « interne » lorsqu'ils s'abonnent à une ressource.

- Chaque magasin dispose d'un fichier web.config dans C:\inetpub\wwwroot\citrix\<storename>.
- Chaque magasin web.config contient un point de terminaison client pour le Subscription Store Service.

```
StoreName>" authenticationMode="windows" transferMode="Streamed">
```

Les données d'abonnement pour chaque magasin de données se trouvent dans :

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
```

Pour que deux magasins puissent partager un magasin de données d'abonnement, il suffit de pointer un magasin vers le point de terminaison du service d'abonnement de l'autre magasin. Dans le cas d'un déploiement de groupes de serveurs, tous les serveurs ont des paires identiques de magasins définies et des copies identiques du magasin de données partagé qu'ils partagent.

Remarque : les Controller XenApp, XenDesktop et AppC configurés sur chaque magasin doivent correspondre exactement ; si ce n'est pas le cas, il est possible que les ressources ne soient pas les mêmes sur les magasins. Le partage d'un magasin de données est uniquement pris en charge lorsque les deux magasins résident sur le même serveur StoreFront ou déploiement de groupes de serveurs.

Points de terminaison de magasins de données d'abonnement StoreFront

1. Dans un déploiement StoreFront unique, ouvrez le fichier web.config du magasin externe à l'aide du Bloc-notes, puis recherchez le clientEndpoint. Par exemple :

```
External" authenticationMode="windows" transferMode="Streamed">
```
2. Modifiez le point de terminaisonexternal pour qu'il corresponde au point de terminaisoninternal du magasin :

```
Internal" authenticationMode="windows" transferMode="Streamed">
```
3. Si vous utilisez un groupe de serveurs StoreFront, propagez toutes les modifications apportées au fichier web.config du nœud principal à tous les autres nœuds.

Les deux magasins sont maintenant configurés pour partager le magasin de données d'abonnement interne.

Paramètres de magasin avancés

Jun 30, 2017

Vous pouvez configurer des propriétés avancées pour un magasin en utilisant les paramètres avancés dans la page Configurer les paramètres du magasin.

Type de résolution d'adresses

Activer le lissage des polices

Autoriser la reconnexion de sessions

Autoriser la redirection de dossiers spéciaux

Période d'interrogation de la vérification de l'intégrité en arrière-plan

Délai d'expiration des communications

Délai d'expiration de la connexion

Activer l'énumération améliorée

Activer le regroupement de sockets

Filtrer les ressources par mots clés exclus

Filtrer les ressources par mots clés inclus

Filtrer les ressources par type

Nombre maximal d'énumérations simultanées

Nombre minimal de batteries pour les énumérations simultanées

Remplacer le nom du client ICA

Exiger la cohérence des jetons

Tentatives de communication avec le serveur

Afficher Desktop Viewer pour les clients d'ancienne génération

Important

Dans les déploiements faisant appel à de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront, sélectionnez un magasin dans le panneau du milieu, et, dans le panneau Action, sélectionnez **Configurer les paramètres du magasin**.
3. Sur la page **Configurer les paramètres du magasin**, sélectionnez **Paramètres avancés**, sélectionnez l'option que vous souhaitez configurer, apportez les modifications nécessaires, puis cliquez sur **OK**.

Type de résolution d'adresses

Utilisez la tâche **Paramètres avancés** pour spécifier le type d'adresse à demander auprès du serveur. La valeur par défaut est DnsPort. Dans le menu déroulant **Type de résolution d'adresses** sur **Paramètres avancés**, sélectionnez l'une des options suivantes :

- Dns
- DnsPort
- IPV4
- IPV4Port
- Point
- DotPort
- Uri
- NoChange

Activer le lissage des polices

Vous pouvez spécifier si vous souhaitez activer le lissage de polices pour les sessions HDX. La valeur par défaut est On.

Utilisez la tâche **Paramètres avancés**, cochez la case **Activer le lissage des polices**, puis cliquez sur **OK**.

Autoriser la reconnexion de sessions

Vous pouvez spécifier si vous souhaitez que les sessions HDX soient reconnectées. La valeur par défaut est On.

Utilisez la tâche **Paramètres avancés**, cochez la case **Autoriser la reconnexion de sessions**, puis cliquez sur **OK** pour activer la reconnexion aux sessions.

Autoriser la redirection de dossiers spéciaux

Utilisez la tâche **Paramètres avancés** pour activer ou désactiver la redirection de dossiers spéciaux. Lorsque la redirection de dossiers spéciaux est configurée, les utilisateurs peuvent mapper des dossiers spéciaux Windows pour le serveur vers ceux de leurs ordinateurs locaux. Le terme dossiers spéciaux fait référence aux dossiers Windows standard, tels que \Documents et \Bureau, qui s'affichent toujours de la même façon quel que soit le système d'exploitation.

Utilisez la tâche **Paramètres avancés**, cochez ou décochez la case **Autoriser la redirection de dossiers spéciaux** pour activer ou désactiver la redirection de dossiers spéciaux, puis cliquez sur **OK**.

Période d'interrogation de la vérification de l'intégrité en arrière-plan

StoreFront exécute des vérifications de l'intégrité périodiques sur chaque broker XenDesktop et serveur XenApp pour réduire l'impact d'une disponibilité intermittente des serveurs. La valeur par défaut est toutes les minutes (00:01:00). Utilisez la tâche **Paramètres avancés**, spécifiez une durée pour la **Période d'interrogation de la vérification de l'intégrité en arrière-plan**, puis cliquez sur **OK** pour contrôler la fréquence de vérification de l'intégrité.

Délai d'expiration des communications

Par défaut, les demandes envoyées par StoreFront à un serveur fournissant les ressources pour un magasin expirent après 30 secondes. Le serveur est considéré comme indisponible après une tentative de communication infructueuse. Utilisez la tâche **Paramètres avancés**, apportez les modifications voulues aux valeurs par défaut, puis cliquez sur **OK** pour modifier ces paramètres.

Délai d'expiration de la connexion

Vous pouvez spécifier le délai d'attente (en secondes) à observer lors de l'établissement d'une connexion initiale à un Delivery Controller. La valeur par défaut est 6.

Utilisez la tâche **Paramètres avancés**, spécifiez le délai d'attente (en secondes) à observer lors de l'établissement de la connexion initiale, puis cliquez sur **OK**.

Activer l'énumération améliorée

Vous pouvez activer (ou désactiver) la communication parallèle avec les Delivery Controller. La valeur par défaut est On.

Utilisez la tâche **Paramètres avancés**, cochez (ou décochez) la case **Activer l'énumération améliorée**, puis cliquez sur **OK**.

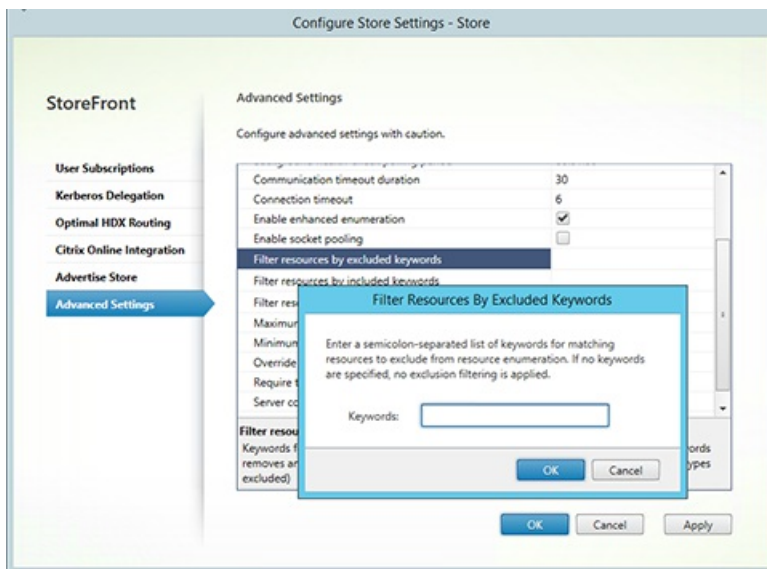
Activer le regroupement de sockets

La mise en regroupement des sockets est désactivée par défaut dans les magasins. Lorsque le regroupement de sockets est activé, StoreFront conserve un groupe de sockets, au lieu de créer une socket chaque fois qu'elle en a besoin et de la renvoyer au système d'exploitation dès que la connexion est fermée. L'activation du regroupement des sockets améliore les performances, plus particulièrement pour les connexions SSL (Secure Sockets Layer). Pour activer le regroupement des sockets, modifiez le fichier de configuration du magasin. Utilisez la tâche **Paramètres avancés**, cochez la case **Activer le regroupement de sockets**, puis cliquez sur **OK** pour activer le regroupement de sockets.

Filtrer les ressources par mots clés exclus

Vous pouvez filtrer les ressources par mots clés exclus. La spécification de mots clés à exclure supprime tous les mots clés à inclure préalablement configurés. La valeur par défaut est Aucun filtrage (aucun type de ressources n'est exclu).

Utilisez la tâche **Paramètres avancés**, sélectionnez **Filtrer les ressources par mots clés exclus**, cliquez à droite de cette option, entrez une liste séparée par des points-virgules de mots clés dans la zone appropriée, puis cliquez sur **OK**.



Filtrer les ressources par mots clés inclus

Vous pouvez filtrer les ressources par mots clés inclus. La spécification de mots clés à inclure supprime tous les mots clés à exclure préalablement configurés. La valeur par défaut est Aucun filtrage (aucun type de ressources n'est exclu).

Utilisez la tâche **Paramètres avancés**, sélectionnez **Filtrer les ressources par mots clés inclus**, cliquez à droite de cette option, entrez une liste séparée par des points-virgules de mots clés dans la zone appropriée, puis cliquez sur **OK**.

Filtrer les ressources par type

Sélectionnez les types de ressources à inclure dans l'énumération des ressources. La valeur par défaut est Aucun filtrage (tous les types de ressources sont inclus).

Utilisez la tâche **Paramètres avancés**, sélectionnez **Filtrer les ressources par type**, cliquez à droite de cette option, sélectionnez les types de ressources à inclure dans l'énumération, puis cliquez sur **OK**.

Nombre maximal d'énumérations simultanées

Spécifiez le nombre maximal de demandes simultanées à envoyer à des Delivery Controller différents. La valeur par défaut est 0 (pas limite).

Utilisez la tâche **Paramètres avancés**, sélectionnez **Nombre maximal d'énumérations simultanées**, entrez un chiffre, puis cliquez sur **OK**.

Nombre minimal de batteries pour les énumérations simultanées

Spécifiez le nombre minimum de Delivery Controller avant que les énumérations ne se produisent en parallèle. La valeur par défaut est 3.

Utilisez la tâche **Paramètres avancés**, sélectionnez **Nombre minimal de batteries pour les énumérations simultanées**, entrez un chiffre, puis cliquez sur **OK**.

Remplacer le nom du client ICA

Remplace le paramètre de nom du client dans le fichier de lancement .ica avec un identificateur généré par Citrix Receiver

pour Web. Lorsque cette option est désactivée, Citrix Receiver spécifie le nom du client. La valeur par défaut est Off.

Utilisez la tâche **Paramètres avancés**, cochez la case **Remplacer le nom du client ICA** et cliquez sur **OK**.

Exiger la cohérence des jetons

Lorsque cette option est activée, StoreFront assure la cohérence entre la passerelle utilisée pour l'authentification et la passerelle utilisée pour l'accès au magasin. Lorsque les valeurs sont incohérentes, les utilisateurs doivent s'authentifier de nouveau. Vous devez activer cette option pour Smart Access. La valeur par défaut est On.

Utilisez la tâche **Paramètres avancés**, cochez la case **Exiger la cohérence des jetons**, puis cliquez sur **OK**.

Tentatives de communication avec le serveur

Spécifiez le nombre de tentatives de communication avec les Delivery Controller avant de les marquer comme indisponibles. La valeur par défaut est 1.

Utilisez la tâche **Paramètres avancés**, sélectionnez **Tentatives de communication avec le serveur**, entrez un chiffre, puis cliquez sur **OK**.

Afficher Desktop Viewer pour les clients d'ancienne génération

Spécifiez si vous souhaitez afficher la fenêtre Citrix Desktop Viewer et la barre d'outils lorsque les utilisateurs accèdent à leur poste de travail à partir de clients d'ancienne génération. La valeur par défaut est Off.

Utilisez la tâche **Paramètres avancés**, cochez la case **Afficher Desktop Viewer pour les clients d'ancienne génération** et cliquez sur **OK**.

Gérer un site Citrix Receiver pour Web

Jun 30, 2017

Citrix Receiver pour Web permet d'accéder à des applications, données et bureaux de manière simple et sécurisée à partir d'un large éventail d'appareils. Utilisez StoreFront pour configurer la sélection des applications Citrix Receiver pour Web pour Citrix Receiver pour Web.

Utilisez la console de gestion StoreFront pour effectuer les tâches liées à Citrix Receiver pour Web suivantes :

Créer un site Citrix Receiver pour Web	Permet de créer des sites Receiver pour Web, ce qui permet aux utilisateurs d'accéder aux magasins via une page Web.
Configurer des sites Citrix Receiver pour Web	Permet de modifier les paramètres de vos sites Receiver pour Web.
Configurer la prise en charge de l'expérience Citrix Receiver unifiée	StoreFront prend en charge les expériences utilisateur classique et unifiée. L'expérience unifiée offre une expérience utilisateur HTML5 gérée de façon centralisée.
Créer et gérer des applications recommandées	Permet de créer des groupes d'applications recommandées pour des utilisateurs qui sont liés ou appartiennent à une certaine catégorie.
Configurer le contrôle de l'espace de travail	Le contrôle de l'espace de travail permet aux applications de suivre les utilisateurs lorsqu'ils naviguent d'une machine à une autre.
Configurer l'utilisation des onglets de navigateur par Citrix Receiver pour HTML5	Lorsque les utilisateurs démarrent des ressources à partir de raccourcis à l'aide de Citrix Receiver pour HTML5, spécifiez si le bureau ou l'application remplace le site Citrix Receiver pour Web dans l'onglet de navigateur existant plutôt que d'apparaître dans un nouvel onglet.
Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion	Par défaut, les demandes effectuées par un site Citrix Receiver pour Web auprès du magasin associé expirent au bout de trois minutes. Le serveur est considéré comme indisponible après une tentative de communication infructueuse. Vous pouvez modifier les paramètres par défaut.

Créer un site Citrix Receiver pour Web

Jun 30, 2017

Utilisez la tâche Créer un site Web pour ajouter des sites Receiver pour Web, qui permettent aux utilisateurs d'accéder aux magasins via une page Web.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront, sélectionnez le magasin pour lequel vous souhaitez créer le site Receiver pour Web, et dans le panneau Actions, cliquez sur Gérer les sites Receiver pour Web.
3. Cliquez sur **Ajouter** pour créer un nouveau site Citrix Receiver pour Web. Spécifiez l'adresse URL dans la zone Chemin du site Web et cliquez sur **Suivant**.
4. Sélectionnez l'expérience Citrix Receiver et cliquez sur **Suivant**.
5. Choisissez une méthode d'authentification, cliquez sur Créer, puis, une fois le site créé, cliquez sur Terminer.
L'adresse URL permettant aux utilisateurs d'accéder au site Citrix Receiver pour Web s'affiche. Pour plus d'informations sur la modification des paramètres des sites Citrix Receiver pour Web, reportez-vous à la section [Configurer des sites Citrix Receiver pour Web](#).

Par défaut, lorsqu'un utilisateur accède à un site Receiver pour Web depuis un ordinateur exécutant Windows ou Mac OS X, le site tente de déterminer si Citrix Receiver est installé sur la machine de l'utilisateur. Si Citrix Receiver ne peut être détecté, l'utilisateur est invité à télécharger et installer la version appropriée de Citrix Receiver pour sa plate-forme à partir du site Web de Citrix. Pour de plus amples informations sur la modification de ce comportement, consultez la section [Désactiver la détection et le déploiement de Citrix Receiver](#).

La configuration par défaut des sites Receiver pour Web nécessite que les utilisateurs installent une version compatible de Citrix Receiver pour accéder à leurs bureaux et applications. Toutefois, vous pouvez activer Receiver pour HTML5 sur vos sites Receiver pour Web afin que les utilisateurs qui ne peuvent pas installer Citrix Receiver puissent quand même accéder aux ressources. Pour de plus amples informations, reportez-vous aux instructions de la section [Configurer des sites Citrix Receiver pour Web](#).

Configurer des sites Citrix Receiver pour Web

Jun 30, 2017

Les sites Citrix Receiver pour Web permettent aux utilisateurs d'accéder aux magasins via une page Web. Les tâches décrites ci-dessous vous permettent de modifier les paramètres de vos sites Citrix Receiver pour Web. Certains paramètres avancés peuvent uniquement être modifiés par le biais d'une modification des fichiers de configuration des sites. Pour plus d'informations, reportez-vous à [Configuration de sites Receiver pour Web à l'aide des fichiers de configuration](#).

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Choisir les méthodes d'authentification

Utilisez la tâche Choisir les méthodes d'authentification afin d'attribuer des méthodes d'authentification aux utilisateurs qui se connectent au site Citrix Receiver pour Web. Cela vous permet de spécifier un sous-ensemble de méthodes d'authentification pour chaque site Receiver pour Web.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront et sélectionnez le magasin que vous voulez modifier dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur **Configurer** et sélectionnez **Méthodes d'authentification** pour spécifier les méthodes d'accès que vous voulez activer pour vos utilisateurs.
 - Cochez la case Nom d'utilisateur et mot de passe pour activer l'authentification explicite. Les utilisateurs saisissent leurs informations d'identification lorsqu'ils accèdent à leurs magasins.
 - Sélectionnez la case **Authentification SAML** pour activer l'intégration avec un fournisseur d'identité SAML. Les utilisateurs s'authentifient auprès d'un fournisseur d'identité et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Depuis le menu déroulant Paramètres :
 - Sélectionnez **Fournisseur d'identité** pour configurer l'approbation du fournisseur d'identité.
 - Sélectionnez **Fournisseur de services** pour configurer l'approbation du fournisseur de services. Cette information est requise par le fournisseur d'identité.
 - Sélectionnez la case à cocher Authentification pass-through au domaine. Cette dernière permet d'autoriser l'authentification pass-through des informations d'identification de domaine Active Directory à partir des machines des utilisateurs. Les utilisateurs doivent s'authentifier sur leur ordinateur Windows membre d'un domaine et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Pour pouvoir utiliser cette option, l'authentification pass-through doit être activée lorsque Citrix Receiver pour Windows est installé sur les machines utilisateur. Veuillez noter que l'authentification pass-through au domaine pour Citrix Receiver pour Web est limitée aux systèmes d'exploitation Windows utilisant Chrome, Firefox, Internet Explorer et Edge.
 - Sélectionnez la case Carte à puce pour activer l'authentification par carte à puce. Les utilisateurs doivent s'authentifier à l'aide de cartes à puce et de codes PIN lorsqu'ils accèdent à leurs magasins.
 - Sélectionnez la case Authentification pass-through via NetScaler Gateway pour activer l'authentification pass-through à partir de NetScaler Gateway. Les utilisateurs s'authentifient sur NetScaler Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.
4. Une fois la méthode d'authentification sélectionnée, cliquez sur OK.

Pour plus d'informations sur la modification des paramètres relatifs aux méthodes d'authentification, reportez-vous à la section [Configurer le service d'authentification](#).

Ajouter des raccourcis vers les ressources à d'autres sites Web

Utilisez la tâche Ajouter des raccourcis aux sites Web pour fournir aux utilisateurs un accès rapide aux bureaux et aux applications à partir de sites Web hébergés sur le réseau interne. Générez des adresses URL pour les ressources disponibles via le site Citrix Receiver pour Web et incorporez ces liens à vos sites Web. Les utilisateurs cliquent sur un lien et sont redirigés vers le site Receiver pour Web, où ils ouvrent une session si ce n'est pas déjà fait. Le site Receiver pour Web démarre automatiquement la ressource. Dans le cas des applications, les utilisateurs sont également abonnés aux applications s'ils ne se sont pas abonnés précédemment.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez le site.
3. Dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur **Configurer**, et sélectionnez **Raccourcis de site Web**.
4. Cliquez sur **Ajouter** pour entrer l'adresse URL d'un site Web sur lequel vous planifiez d'héberger les raccourcis. Les adresses URL doivent être spécifiées au format `http[s]://hostname[:port]`, où `hostname` est le nom de domaine complet de l'hôte de site Web et `port` est le port utilisé pour la communication avec l'hôte si le port par défaut du protocole n'est pas disponible. Les chemins d'accès aux pages spécifiques du site Web ne sont pas requis. Pour modifier une adresse URL, sélectionnez l'entrée dans la liste Sites Web, puis cliquez sur Modifier. Sélectionnez une entrée dans la liste et cliquez sur Supprimer pour supprimer l'URL d'un site Web sur lequel vous ne voulez plus héberger des raccourcis vers les ressources disponibles via le site Citrix Receiver pour Web.
5. Cliquez sur Obtenir les raccourcis, puis sur Enregistrer lorsque vous êtes invité à enregistrer les modifications apportées à la configuration.
6. Ouvrez une session sur le site Citrix Receiver pour Web et copiez les URL dont vous avez besoin sur votre site Web.

Définir un délai d'expiration de session

Par défaut, les sessions des utilisateurs sur les sites Citrix Receiver pour Web expirent au bout de 20 minutes d'inactivité. Lors de l'expiration d'une session, les utilisateurs peuvent continuer à utiliser des bureaux ou applications en cours d'exécution, mais ils devront ouvrir une nouvelle session pour accéder aux fonctions des sites Citrix Receiver pour Web telles que l'abonnement aux applications.

Utilisez la tâche Expiration de session dans **Gérer les sites Receiver pour Web** pour modifier la valeur du délai d'expiration de session.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau de gauche, et dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur **Configurer**, puis choisissez **Paramètres de session**. Vous pouvez spécifier **Expiration de session** en minutes et en heures. La valeur minimale pour tous les intervalles de temps est 1. La valeur maximale correspond à 1 an pour chaque intervalle de temps.

Spécifier différentes vues pour les applications et bureaux

Utilisez la tâche **Affichage des applications et des bureaux sur Receiver pour Web** dans **Gérer les sites Receiver pour Web** pour modifier la valeur du délai d'expiration de session.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau de gauche, et dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur Configurer, puis choisissez **Paramètres de l'interface du client**.
3. Dans les menus déroulants **Sélectionner l'affichage** et **Affichage par défaut**, sélectionnez les vues à afficher.

Pour activer l'affichage des dossiers :

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau de gauche, et dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Paramètres avancés** et cochez la case **Activer l'affichage des dossiers**.

Arrêter de fournir des fichiers de provisioning aux utilisateurs

Par défaut, les sites Citrix Receiver pour Web offrent des fichiers de provisioning qui permettent aux utilisateurs de configurer Citrix Receiver automatiquement pour le magasin associé. Les fichiers de provisioning contiennent les détails de connexion du magasin qui fournit les ressources sur le site, y compris les détails des déploiements NetScaler Gateway et des balises configurés pour le magasin.

Utilisez la tâche **Activer la configuration de Receiver** dans **Gérer les sites Receiver pour Web** pour modifier la valeur du délai d'expiration de session.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau de gauche, et dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur **Configurer**, puis choisissez **Paramètres de l'interface du client**.
3. Sélectionnez **Activer la configuration de Receiver**.

Configurer le comportement du site des utilisateurs ne disposant pas de Citrix Receiver

Utilisez la tâche **Déployer Citrix Receiver** pour configurer le comportement d'un site Citrix Receiver pour Web lorsqu'un utilisateur Windows ou Mac OS X sans Citrix Receiver accède au site. Par défaut, les sites Citrix Receiver pour Web tentent automatiquement de déterminer si Citrix Receiver est installé lors de l'accès à partir d'ordinateurs exécutant Windows ou Mac OS X.

Si Citrix Receiver ne peut être détecté, l'utilisateur est invité à télécharger et installer la version appropriée de Citrix Receiver pour sa plate-forme. L'emplacement de téléchargement par défaut est le site Web de Citrix, mais vous pouvez également copier les fichiers d'installation sur le serveur StoreFront et fournir ces fichiers locaux aux utilisateurs.

Pour les utilisateurs qui ne peuvent pas installer Citrix Receiver, vous pouvez activer Citrix Receiver pour HTML5 sur vos sites Citrix Receiver pour Web. Citrix Receiver pour HTML5 permet aux utilisateurs d'accéder aux bureaux et applications directement depuis des navigateurs Web compatibles HTML5 sans avoir à installer Citrix Receiver. Les connexions au réseau interne et les connexions via NetScaler Gateway sont prises en charge. Toutefois, pour les connexions depuis le réseau interne, Citrix Receiver pour HTML5 permet d'accéder uniquement aux ressources fournies par des produits spécifiques. En outre, des versions spécifiques de NetScaler Gateway sont requises pour autoriser les connexions extérieures au réseau d'entreprise. Pour plus d'informations, veuillez consulter la section [Configuration requise pour l'infrastructure](#).

Pour les utilisateurs du réseau interne, l'accès via Citrix Receiver pour HTML5 aux ressources fournies par XenDesktop et XenApp est désactivé par défaut. Pour activer l'accès local aux bureaux et applications à l'aide de Citrix Receiver pour HTML5, vous devez activer la stratégie Connexions WebSockets ICA sur vos serveurs XenDesktop et XenApp. XenDesktop et XenApp utilisent le port 8008 pour les connexions à Citrix Receiver pour HTML5. Assurez-vous que votre pare-feu et autres périphériques réseau autorisent l'accès à ce port. Pour plus d'informations, veuillez consulter la section [Paramètres de stratégie WebSockets](#).

Citrix Receiver pour HTML5 peut uniquement être utilisé avec Internet Explorer via des connexions HTTP. Pour utiliser Citrix Receiver pour HTML5 avec Mozilla Firefox via des connexions HTTPS, les utilisateurs doivent taper **about:config** dans la

barre d'adresses de Firefox et définir la préférence **network.websocket.allowInsecureFromHTTPS** sur **true**.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
 2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un site. Dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
 3. Choisissez **Déployer Citrix Receiver** et spécifiez la réponse du site Citrix Receiver pour Web au cas où Citrix Receiver ne peut pas être détecté sur une machine utilisateur.
- Si vous voulez que le site invite l'utilisateur à télécharger et installer la version appropriée de Citrix Receiver pour sa plate-forme, sélectionnez **Installer localement**. Les utilisateurs doivent installer Citrix Receiver pour accéder aux bureaux et applications via le site.
 - Si vous sélectionnez **Autoriser les utilisateurs à télécharger le moteur HDX (plug-in)**, Citrix Receiver pour Web permet à l'utilisateur de télécharger et d'installer Citrix Receiver sur le client de l'utilisateur final si Citrix Receiver n'est pas disponible.
 - Si vous sélectionnez **Mettre le plug-in à niveau à l'ouverture de session**, Citrix Receiver pour Web met à niveau le client Citrix Receiver lorsque l'utilisateur ouvre une session. Pour activer cette fonctionnalité, assurez-vous que les fichiers de Citrix Receiver sont disponibles sur le serveur StoreFront.
 - Sélectionnez une source dans la liste déroulante.
 - Si vous voulez que le site invite l'utilisateur à télécharger et installer Citrix Receiver mais qu'il se replie sur Citrix Receiver pour HTML5 dans le cas où Citrix Receiver ne peut pas être installé, sélectionnez **Utiliser Receiver pour HTML5 si une installation Receiver locale n'est pas disponible**. Les utilisateurs sans Citrix Receiver sont invités à télécharger et installer Citrix Receiver chaque fois qu'ils ouvrent une session sur le site.
 - Si vous souhaitez que le site autorise l'accès aux ressources via Citrix Receiver pour HTML5 sans inviter l'utilisateur à télécharger et installer Citrix Receiver, sélectionnez **Toujours utiliser Receiver pour HTML5**. Lorsque cette option est sélectionnée, les utilisateurs accèdent toujours aux bureaux et applications sur le site via Citrix Receiver pour HTML5, à condition qu'ils utilisent un navigateur compatible HTML5. Les utilisateurs qui ne disposent pas d'un navigateur compatible HTML5 doivent installer le Citrix Receiver natif.

Mettre à disposition des fichiers d'installation Citrix Receiver sur le serveur

Par défaut, lorsqu'un utilisateur accède à un site Citrix Receiver pour Web depuis un ordinateur exécutant Windows ou Mac OS X, le site tente de déterminer si Citrix Receiver est installé sur la machine de l'utilisateur. Si Citrix Receiver ne peut être détecté, l'utilisateur est invité à télécharger et installer la version appropriée de Citrix Receiver pour sa plate-forme à partir du site Web de Citrix.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un site. Dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Choisissez **Déployer Citrix Receiver** et **Source pour Receiver**, puis recherchez les fichiers d'installation.

Exécuter l'invite à installer Citrix Receiver après l'ouverture de session

Avant d'ouvrir une session sur StoreFront, Citrix Receiver pour Web invite l'utilisateur à installer la dernière version de Citrix Receiver si Citrix Receiver n'est pas déjà installé sur l'ordinateur de l'utilisateur (pour utilisateurs Internet Explorer, Firefox et Safari) ou la première fois qu'un utilisateur visite le site (pour utilisateurs Chrome). En fonction de la configuration, l'invite peut également s'afficher si l'installation de Citrix Receiver de l'utilisateur peut être mise à niveau.

Vous pouvez configurer Citrix Receiver pour Web pour afficher l'invite après l'ouverture d'une session sur StoreFront.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez le site.
3. Dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
4. Sélectionnez **Paramètres avancés** et cochez la case **Inviter à installer Citrix Receiver après la connexion**.

Supprimer des sites Citrix Receiver pour Web

Utilisez l'option **Gérer les sites Receiver pour Web** dans le panneau **Actions** pour supprimer un site Citrix Receiver pour Web. Lorsque vous supprimez un site, les utilisateurs ne peuvent plus utiliser cette page Web pour accéder au magasin.

Prise en charge de l'expérience Citrix Receiver unifiée

Jun 30, 2017

StoreFront prend en charge les expériences utilisateur **classique** et **unifiée**. Avec l'expérience classique, chaque plate-forme Citrix Receiver est responsable de la mise à disposition de sa propre expérience utilisateur. La nouvelle expérience unifiée offre une expérience utilisateur HTML5 gérée de façon centralisée pour tous les Receiver Web et natifs. Elle prend en charge la personnalisation et la gestion des groupes d'applications recommandées.

Les magasins créés à l'aide de cette version de StoreFront utilisent l'expérience unifiée par défaut, mais pour les mises à niveau, Citrix conserve l'expérience classique par défaut. Pour prendre en charge l'expérience unifiée, vous devez associer un magasin StoreFront avec un site Receiver pour Web, et ce site doit être configuré pour utiliser l'expérience unifiée.

Important : l'expérience unifiée n'est pas prise en charge si le site Receiver pour Web est ajouté à la zone restreinte. Si vous devez ajouter le site Receiver pour Web à la zone restreinte, configurez votre magasin pour utiliser l'expérience classique.

Utilisez la console de gestion StoreFront pour effectuer les tâches liées à Citrix Receiver pour Web suivantes :

- Créer un site Citrix Receiver pour Web
- Modifier l'expérience d'un site Citrix Receiver pour Web.
- Sélectionner un site Citrix Receiver pour Web unifié à associer avec le magasin
- Personnaliser l'apparence de Receiver.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

Remarque

Si vous utilisez XenApp 6.x, les applications définies sur **Livrée en streaming sur la machine cliente** ou **Livrée en streaming si possible, sinon, accès depuis un serveur, sinon, accès depuis un serveur** ne sont pas prises en charge lorsque l'expérience unifiée est activée.

Créer un site Web Citrix Receiver pour Web

Un site Citrix Receiver pour Web est créé automatiquement chaque fois que vous créez un magasin. Vous pouvez également créer des sites Receiver pour Web à l'aide de cette procédure.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur Gérer les sites Receiver pour Web > Ajouter et suivez l'assistant.

Modifier l'expérience Citrix Receiver

Vous pouvez spécifier si un site Web Citrix Receiver pour Web propose l'expérience **classique** ou **unifiée**. Veuillez noter que l'activation de l'expérience classique désactive les fonctionnalités de personnalisation avancée et la gestion des groupes d'applications recommandées.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.

2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront, sélectionnez le magasin que vous voulez modifier dans le panneau central, cliquez sur **Gérer les sites Receiver pour Web** dans le panneau Actions, et cliquez sur **Configurer**.
3. Sélectionnez **Expérience Receiver** et choisissez **Désactiver l'expérience classique** ou **Activer l'expérience classique**.

Sélectionner un site Citrix Receiver pour Web unifié à associer avec le magasin

Lorsqu'un nouveau magasin de données est créé à l'aide de StoreFront, un site Citrix Receiver pour Web est créé automatiquement en mode unifié et associé au magasin. Toutefois, si vous mettez à niveau une version précédente de StoreFront, la valeur par défaut est l'expérience classique.

Pour sélectionner un site Citrix Receiver pour Web afin de proposer l'expérience unifiée pour un magasin, au moins un site Citrix Receiver pour Web doit avoir été créé avec l'expérience classique désactivée.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront, sélectionnez un magasin dans le panneau du milieu, puis cliquez sur **Configurer l'expérience unifiée** dans le volet **Actions**. Seuls les sites Web qui prennent en charge l'expérience unifiée (expérience classique désactivée) peuvent être définis comme défaut pour le magasin. Si vous ne disposez pas d'un site Web Citrix Receiver pour Web, un message s'affiche, avec un lien vers l'assistant de création d'un nouveau site Receiver pour Web. Vous pouvez également modifier un site Receiver pour Web en site Web Receiver pour Web. Consultez la section [Modifier l'expérience Citrix Receiver](#).
3. Lorsque vous disposez d'un site Citrix Receiver pour Web, choisissez **Configurer l'expérience unifiée** pour ce magasin et choisissez le site Web spécifique.

Important

Si vous basculez de l'expérience unifiée vers l'expérience classique sur un site Receiver pour Web, cela peut affecter les clients Citrix Receiver natifs. Revenir à l'expérience unifiée sur ce site Receiver pour Web ne met pas à jour l'expérience pour les clients Citrix Receiver natifs. Vous devez réinitialiser l'expérience unifiée dans le nœud Magasins dans la console de gestion.

Personnaliser l'apparence de Citrix Receiver

Pour personnaliser l'apparence de Citrix Receiver, l'expérience Receiver classique doit être désactivée sur votre site Web Citrix Receiver pour Web.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Expérience Receiver** > **Désactiver l'expérience classique**.
4. Sélectionnez **Personnaliser l'apparence** et effectuez des sélections pour personnaliser la manière dont le site Web s'affiche après avoir ouvert une session.

Edit Receiver for Web site -

StoreFront

Receiver Experience

Customize Appearance

Featured App Groups

Authentication Methods

Website Shortcuts

Deploy Citrix Receiver

Session Settings

Workspace Control

Client Interface Settings

Advanced Settings

Customize Receiver Appearance

Use these settings to customize the Receiver for web pages.

Logon branding

Logo:
(350 x 120 px)
This logo appears on the Receiver logon page.

Upload from local computer

Browse...

Header branding (Post logon)

Logo:
(340 x 80 px)

Upload from local computer

Browse...

Preview (Post logon)

Background color:

Text and icon color:

Content branding (Post logon)

Link color:

Citrix StoreFront

Text and icon color

Link color

Reset to default styles

OK

Cancel

Apply

Créer et gérer des applications recommandées

Jun 30, 2017

Vous pouvez créer des groupes d'applications recommandées pour des utilisateurs qui sont liés ou appartiennent à une certaine catégorie. Par exemple, vous pouvez créer un groupe d'applications recommandées Service commercial contenant des applications qui sont utilisées par ce département. Vous pouvez définir les applications recommandées dans la console d'administration StoreFront à l'aide de leurs noms ou à l'aide de mots clés ou de catégories d'applications qui ont été définis dans la console Studio.

Utilisez la tâche Groupes d'applications recommandées pour ajouter, modifier ou supprimer des groupes d'applications recommandées.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Notez que cette fonctionnalité est disponible uniquement lorsque l'expérience classique est désactivée.

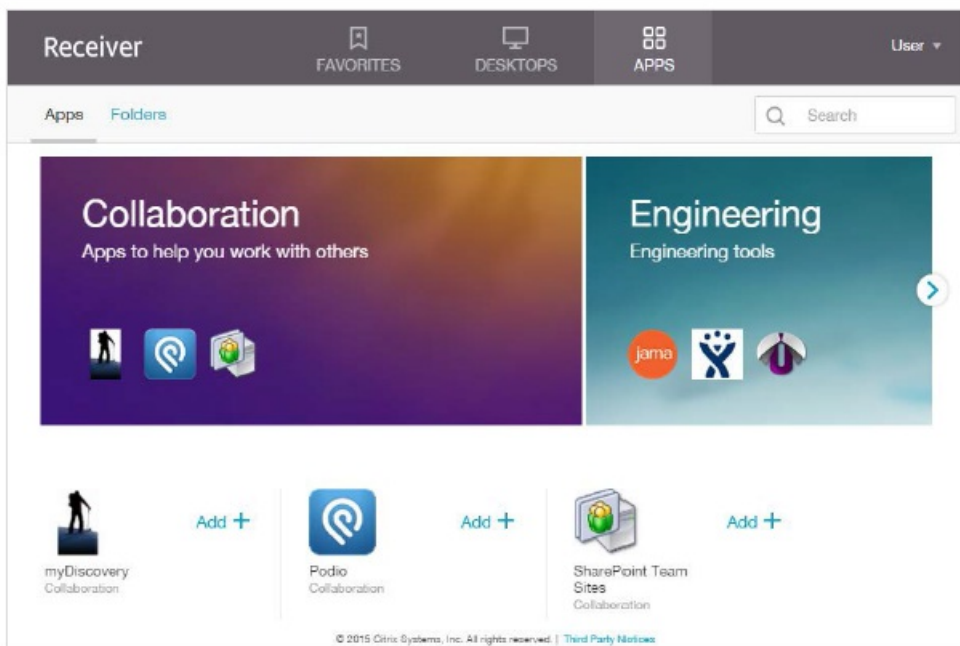
1. Sur l'écran **Démarrer** de Windows ou l'écran Applications, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Groupes d'applications recommandées**.
4. Dans la boîte de dialogue **Groupes d'applications recommandées**, cliquez sur **Créer** pour définir un nouveau groupe d'applications recommandées.
5. Dans la boîte de dialogue **Créer un groupe d'applications recommandées**, spécifiez le nom, la description (facultatif) et l'arrière-plan du groupe d'applications ainsi que la méthode utilisée pour définir les groupes d'applications recommandées. Choisissez des mots clés, les noms des applications ou une catégorie d'applications, puis cliquez sur **OK**.

Option	Description
Mots clés	Définissez les mots clés dans Studio.
Catégorie d'application	Définissez la catégorie d'applications dans Studio.
Noms d'applications	<p>Utilisez le nom des applications pour définir le groupe d'applications recommandées. Tous les noms d'applications qui correspondent au nom inclus dans l'écran Créer un groupe d'applications recommandées sont inclus dans le groupe d'applications recommandées.</p> <p>StoreFront ne prend pas en charge les caractères génériques dans les noms d'application. La correspondance n'est pas sensible à la casse, mais reconnaît les mots entiers uniquement. Par exemple, si vous entrez Excel, StoreFront renvoie l'application publiée Microsoft Excel 2013, alors que Exc ne donne aucun résultat.</p>

Exemple :

Nous avons créé deux groupes d'applications recommandées :

- Collaboration : créé en associant des applications dans la catégorie **Collaboration** de Studio.
- Engineering : créé en donnant un nom au groupe d'applications et en spécifiant une collection de noms d'applications.



Configurer le contrôle de l'espace de travail

Jun 30, 2017

Le contrôle de l'espace de travail permet aux applications de suivre les utilisateurs lorsqu'ils naviguent d'une machine à une autre. Ceci permet, par exemple, aux médecins hospitaliers de passer d'un poste de travail à un autre sans avoir à redémarrer leurs applications sur chaque machine. Le contrôle de l'espace de travail est activé par défaut pour les sites Citrix Receiver pour Web. Pour désactiver ou configurer le contrôle de l'espace de travail, modifiez le fichier de configuration du site.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran **Démarrer de Windows** ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Dans le panneau de gauche, sélectionnez **Magasins**, et dans le panneau Action, sélectionnez **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Contrôle de l'espace de travail**.
4. Configurez les paramètres par défaut du contrôle de l'espace de travail, ce qui comprend :

Activation du contrôle de l'espace de travail

Configuration des options de reconnexion à la session

Définition des actions de fermeture de session

Configurer l'utilisation des onglets de navigateur par Citrix Receiver pour HTML5

Jun 30, 2017

Par défaut, Citrix Receiver pour HTML5 démarre les bureaux et applications dans un nouvel onglet de navigateur. Toutefois, lorsque les utilisateurs démarrent des ressources à partir de raccourcis à l'aide de Citrix Receiver pour HTML5, le bureau ou l'application remplace le site Citrix Receiver pour Web dans l'onglet de navigateur existant plutôt que d'apparaître dans un nouvel onglet.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran **Démarrer de Windows** ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Dans le panneau de gauche, sélectionnez **Magasins**, et dans le panneau Action, sélectionnez **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Déployer Citrix Receiver**.
4. Sélectionnez **Toujours utiliser Receiver pour HTML5** dans le menu déroulant **Options de déploiement** et, selon l'onglet dans lequel vous souhaitez démarrer les applications, sélectionnez ou désélectionnez **Lancer les applications dans le même onglet que Receiver pour Web**.

Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion

Jun 30, 2017

Par défaut, les demandes effectuées par un site Citrix Receiver pour Web auprès du magasin associé expirent au bout de trois minutes. Le serveur est considéré comme indisponible après une tentative de communication infructueuse. Utilisez la tâche **Paramètres de session** pour modifier les paramètres par défaut.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront, sélectionnez un magasin dans le panneau du milieu, et, dans le panneau **Action**, sélectionnez **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Paramètres de session**, effectuez vos modifications, puis cliquez sur **OK** ou **Appliquer** pour enregistrer les modifications.

•
•

The screenshot shows the 'StoreFront' configuration interface. On the left is a navigation pane with the following items: 'User Subscriptions' (highlighted with a blue arrow), 'Kerberos Delegation', 'Optimal HDX Routing', 'Citrix Online Integration', 'Advertise Store', and 'Advanced Settings'. The main content area is titled 'Manage User Subscriptions' and contains two radio button options. The first option, 'Enable User Subscriptions (Self Service Store)', is selected and includes a descriptive paragraph. The second option, 'Disable User Subscriptions (Mandatory Store)', is unselected and also includes a descriptive paragraph. At the bottom right of the main area are three buttons: 'OK', 'Cancel', and 'Apply'.

StoreFront

- User Subscriptions
- Kerberos Delegation
- Optimal HDX Routing
- Citrix Online Integration
- Advertise Store
- Advanced Settings

Manage User Subscriptions

☒ **Enable User Subscriptions (Self Service Store)**

When you enable user subscriptions, the Self-Service store is then in effect. Users must subscribe to applications before they can use them. Any previously specified subscriptions are still available.

☐ **Disable User Subscriptions (Mandatory Store)**

When you disable user subscriptions, the Mandatory store is then in effect. All applications published to users are available on the Home screen without users subscribing to them. User subscriptions are not deleted and can be recovered if you re-enable the feature.

OK Cancel Apply


```
function Remove-SubscriptionData
```

```
{
```

```
[CmdletBinding()]
```

```
[Parameter(Mandatory=$False)][String]$Store = "Store"
```

```
$SubsService = "Citrix Subscriptions Store"
```

```
# Path to Subscription Data in StoreFront version 2.6 or higher
```

```
$SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store\*"
```

```
Stop-Service -displayname $SubsService
```

```
Remove-Item $SubsPath -Force -Verbose
```

```
Start-Service -displayname $SubsService
```

```
Get-Service -displayname $SubsService
```

```
}
```

```
Remove-SubscriptionData -Store "YourStore"
```

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"
```

```
Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"
```

```
Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"
```

```
Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

-
-
-
-

Subscription Datastore Size	
No of Records	Size MB
0	6.02
1000	7.02
10000	40.00
100000	219.00
200000	358.00
500000	784.00
800000	1213.02
1000000	1497.15
1300000	1919.15
1500000	2205.15
1700000	2487.15
2000000	2915.15

Subscriptions Import/Export.txt	
No of Records	Size MB
0	0.00
1000	0.13
10000	1.30
100000	12.80
200000	25.60
500000	64.10
800000	102.00
1000000	128.00
1300000	166.00
1500000	192.00
1700000	218.00
2000000	256.00

Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\Subscription Entries Count (including unpurged deleted records)"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Subscriptions Store Synchronizing"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number Subscriptions Synchronized"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number Subscriptions Transferred"

-
-
-

-
-
-
-
-

-
-
-

-
-

```
Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1" Import-Module "installationlocation\Management\Cmdlets\SubscriptionSyncModule.psm1"
```

```
Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname -clusterAddress deploymentaddress
```

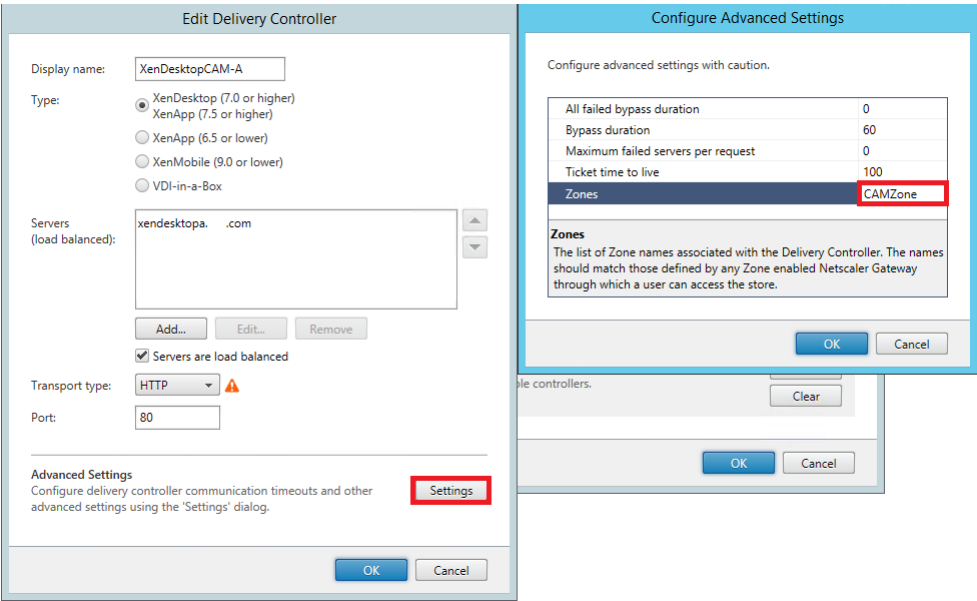
```
Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname -storeName storename
```

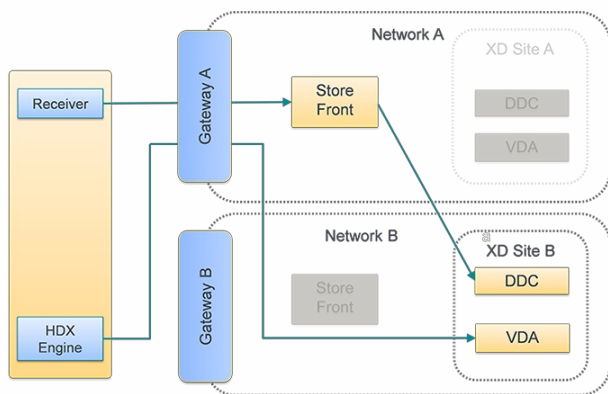
```
Add-DSSubscriptionsSyncSchedule -scheduleName synchronizationname -startTime hh:mm
```

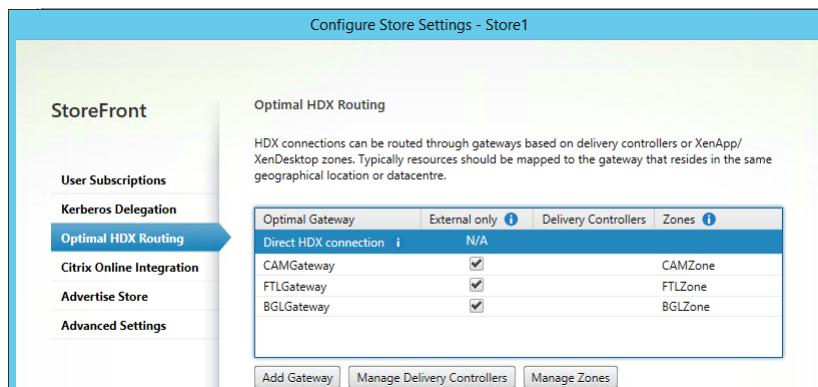
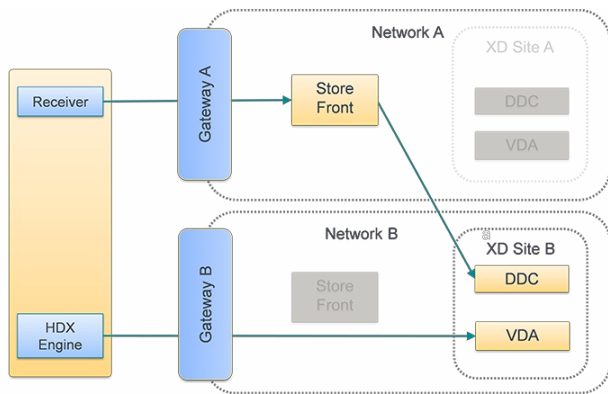
```
Add-DSSubscriptionsSyncReoccurringSchedule -scheduleName synchronizationname -startTime hh:mm:ss -repeatMinutes interval
```

```
Restart-DSSubscriptionsStoreSubscriptionService
```

```
Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
```



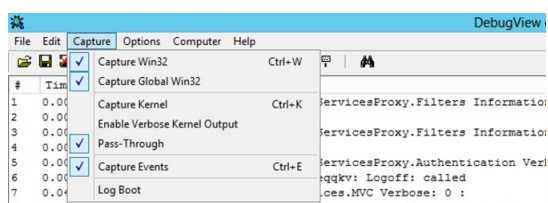




Paramètres de l'API PowerShell

Paramètre	Description
-SiteId (Int)	ID du site dans IIS. Il s'agit généralement de 1 pour le site dans IIS où StoreFront est installé par défaut.
-ResourcesVirtualPath (chaîne)	Chemin d'accès au magasin qui est configuré pour qu'une batterie utilise le mappage de passerelle optimale. Exemple : « /Citrix/Store »
-GatewayName (chaîne)	Nom donné pour identifier Netscaler Gateway dans StoreFront. Exemple 1 : ExternalGateway Exemple 2 : InternalGateway

-Hostnames (tableau de chaînes)	<p>Spécifie le nom de domaine complet (FQDN) et le port du boîtier NetScaler Gateway optimal.</p> <p>Exemple 1 pour vServer standard port 443 : passerelle.exemple.com</p> <p>Exemple 2 pour vServer non standard port 500 : passerelle.exemple.com:500</p>
-Farms (tableau de chaînes)	<p>Spécifie un jeu de déploiements XenDesktop, XenApp et App Controller, généralement colocalisés, qui partagent un boîtier NetScaler Gateway optimal commun. Une batterie peut contenir un seul ou plusieurs Delivery Controller qui fournissent des ressources publiées.</p> <p>Vous pouvez configurer un site XenDesktop dans StoreFront sous des Delivery Controller en tant que « XenDesktop ». Cela représente une seule batterie.</p> <p>Peut contenir de multiples Delivery Controller dans sa liste de basculement :</p> <p>Exemple : « XenDesktop »</p> <p>XenDesktop-A.exemple.com</p> <p>XenDesktop-B.exemple.com</p> <p>XenDesktop-C.exemple.com</p>
-Zones (tableau de chaînes)	<p>Spécifie un ou des centres de données contenant de nombreux Delivery Controller. Cela nécessite que vous ajoutiez un indicateur aux objets Delivery Controller dans StoreFront avec la zone appropriée à laquelle vous voulez les allouer.</p>
-staUrls (tableau de chaînes)	<p>Spécifie les adresses URL des serveurs XenDesktop ou XenApp exécutant la Secure Ticket Authority (STA). Si vous utilisez plusieurs batteries, répertoriez les serveurs STA sur chaque batterie à l'aide d'une liste séparée par des virgules :</p> <p>Exemple : "http://xenapp-a.exemple.com/scripts/ctxsta.dll","http://xendesktop-a.exemple.com/scripts/ctxsta.dll"</p>
-StasUseLoadBalancing (booléen)	<p>Si cet attribut est défini sur true : obtient de manière aléatoire des tickets de session auprès de toutes les STA, ce qui permet de distribuer équitablement les demandes sur toutes les STA.</p> <p>Si cet attribut est défini sur false : les utilisateurs sont connectés à la première STA disponible dans l'ordre dans lequel elles sont répertoriées dans la configuration, ce qui réduit le nombre de STA.</p>
-StasBypassDuration	<p>Permet de définir la période de temps, en heures, minutes et secondes pendant laquelle une STA est considérée comme indisponible après un échec de la demande.</p> <p>Exemple : 02:00:00</p>
- EnableSessionReliability (booléen)	<p>Si cet attribut est défini sur true : garde les sessions déconnectées ouvertes lorsque Citrix Receiver tente de se reconnecter automatiquement. Si vous avez configuré plusieurs STA et que vous voulez vous assurer que la fiabilité de session est toujours disponible, définissez la valeur de l'attribut useTwoTickets sur true pour obtenir des tickets de deux STA différentes dans le cas où l'une des STA deviendrait indisponible au cours de la session.</p>
-UseTwoTickets (booléen)	<p>Si cet attribut est défini sur true : obtient des tickets de deux STA différentes dans le cas où l'une des STA deviendrait indisponible au cours de la session.</p> <p>Si cet attribut est défini sur false : utilise un seul serveur STA.</p>
- EnabledOnDirectAccess (booléen)	<p>Si cet attribut est défini sur true : garantit que lorsque les utilisateurs locaux du réseau interne se connectent directement à StoreFront, les connexions à leurs ressources sont toujours routées via le boîtier optimal défini pour la batterie.</p> <p>Si cet attribut est défini sur false : les connexions aux ressources ne sont pas routées via le boîtier optimal pour la batterie sauf si les utilisateurs accèdent à StoreFront via NetScaler Gateway.</p>



.

-

-

-

-

-

-
-
-
-

-
-
-
-
-

-
-
-
-

Manage NetScaler Gateways

Add, edit or remove the NetScaler Gateway appliances through which remote access is provided. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores.

Alternatively, NetScaler Gateway appliances can be [imported from file](#).

NetScaler Gateways:

Display Name	Role	Used by Sto...	URL
--------------	------	----------------	-----

Add...

Edit...

Remove

Close

Import Configuration File

1. Select a NetScaler Configuration zip file

Zip File: C:\Users\admin\Desktop\AllAuthMethods.zip

Browse

2. Select the vServer you want to import

<input checked="" type="checkbox"/>	https://emeagateway.example.com:443	Import
<input checked="" type="checkbox"/>	https://emeagateway.example.com:444	Import
<input checked="" type="checkbox"/>	https://emeagateway.example.com:445	Import
<input checked="" type="checkbox"/>	https://emeagateway.example.com:446	Import
<input checked="" type="checkbox"/>	https://emeagateway.domain.com:447	Import

Close

•

Import NetScaler Configuration

StoreFront

Select Logon Type

Secure Ticket Authorities

Review Changes

Summary

Select Logon Type

Review the logon type for the gateway you wish to import. Smartcard logon types include a smartcard fallback option.

Logon type: ⓘ

Domain

Callback URL (Optional):

https://NetScalerGatewayFQDN

/CitrixAuthService/AuthService.asmx

Verify

ⓘ This is the internally accessible URL of the appliance. This is used to verify that requests received from NetScaler Gateway originate from that appliance.

Next

Cancel

<https://docs.citrix.com>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

p.154

Import NetScaler Configuration

StoreFront

✓ Select Logon Type

Secure Ticket Authorities

Review Changes

Summary

Secure Ticket Authorities

The import process has detected the following Secure Ticket Authorities

Provided URL	Edited...	STA ID	Sta...
https://		...	✓
https://		...	✓

Edit...

Back

Next

Cancel

Import NetScaler Configuration

StoreFront

✓ Select Logon Type

✓ Secure Ticket Authorities

Review Changes

Summary

Review Changes

Review these changes before importing.

Gateway Information

Gateway Address

GSLB Address

VIP Address

Gateway Mode

Gateway Edition

Auth Type

Callback URL

CVPN

Enterprise

Domain

Secure Ticket Authorities

https://

/scripts/ctxsta.dll

https://

/scripts/ctxsta.dll

A gateway using at least one of these addresses already exists. Select to create a new gateway or overwrite the existing one before importing.

-- Create New Gateway --

View details

Back

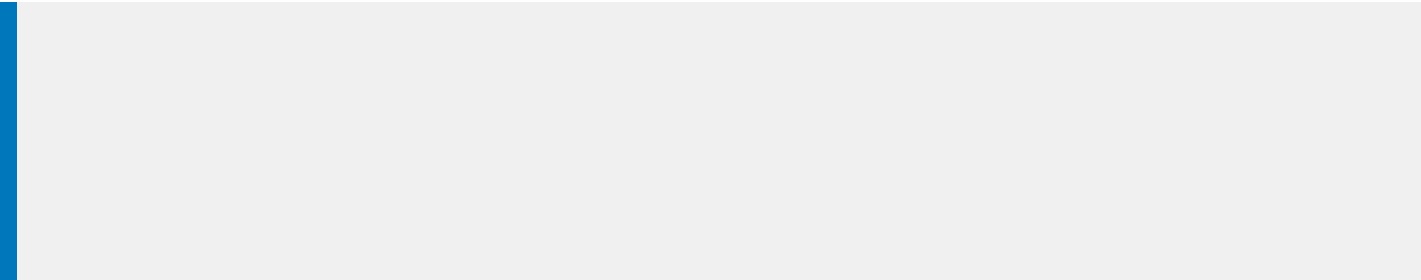
Import

Cancel

<https://docs.citrix.com>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

p.157



-
-

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

```
$ImportedGateways.Document.Gateways[0]  
  
$ImportedGateways.Document.Gateways[1]  
  
$ImportedGateways.Document.Gateways[2]
```

```
$importedGateways.Document.Gateways[2]
```

GatewayMode : CVPN

CallbackUrl :

GslbAddressUri : https://gslb.example.com/

AddressUri : https://emeagateway.example.com/

Address : https://emeagateway.example.com:443

GslbAddress : https://gslb.example.com:443

VipAddress : 10.0.0.1

Stas : {STA298854503, STA909374257}

StaLoadBalance : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType : Domain

GatewayEdition : Enterprise

ReceiverForWebSites : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}

GatewayMode : CVPN

CallbackUrl :

GslbAddressUri : https://gslb.example.com/

AddressUri : https://emeagateway.example.com/

Address : https://emeagateway.example.com:444

GslbAddress : https://gslb.example.com:443

VipAddress : 10.0.0.2

Stas : {STA298854503, STA909374257}

StaLoadBalance : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType : DomainAndRSA

GatewayEdition : Enterprise

ReceiverForWebSites : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}

GatewayMode : CVPN

CallbackUrl : https://emeagateway.example.com:445

GslbAddressUri : https://gslb.example.com/

AddressUri : https://emeagateway.example.com/

Address : https://emeagateway.example.com:445

GslbAddress : https://gslb.example.com:443

VipAddress : 10.0.0.2

Stas : {STA298854503, STA909374257}

StaLoadBalance : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType :SmartCard

GatewayEdition : Enterprise

ReceiverForWebSites : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -Confirm:$False
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -Confirm:$False
```

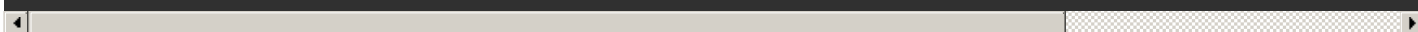
```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -Confirm:$False
```

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -CallbackUrl "https://emeagatewayc
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewayc
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewayc
```



•



```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -LogonType "SmartCard" -CallbackUr
```

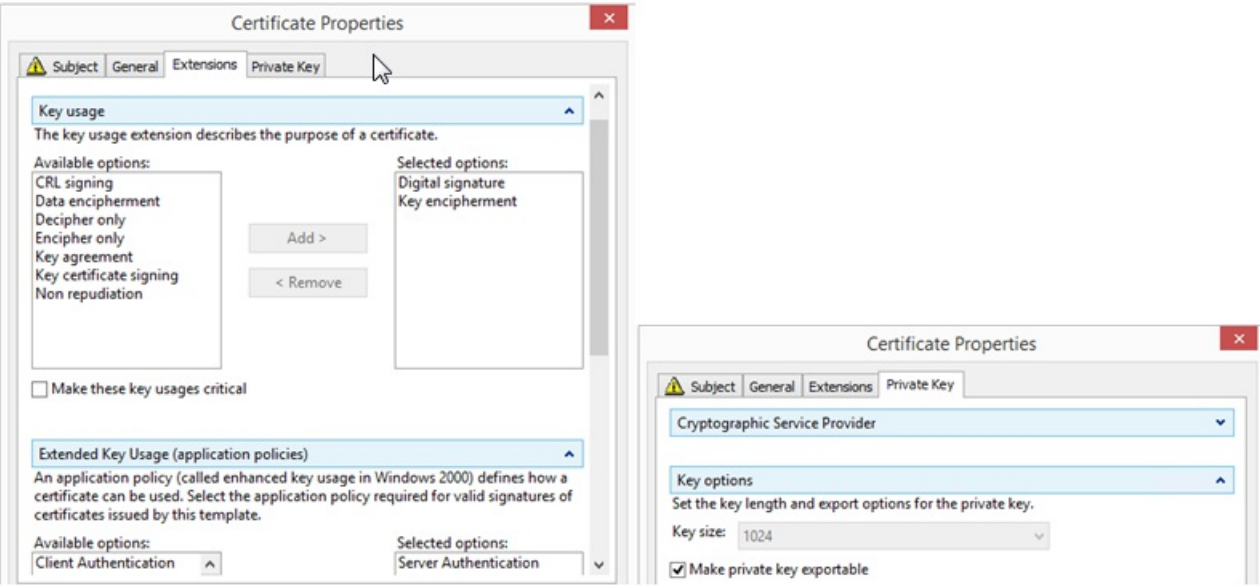
```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -LogonType "SmartCard" -CallbackUr
```

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -LogonType "SmartCard" -CallbackUr
```


-
-
-
-
-

-
-
-

Common Properties|



-
-

-
-

Install Certificate

Certificate-Key Pair Name*

wildcard.example.com

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*

wildcard.example.com.cer

Browse ▼ +

Key File Name

wildcard.example.com.key

Browse ▼ +

Certificate Format

☒ PEM ☐ DER

Password

☐ Certificate Bundle

☒ Notify When Expires

Notification Period

30

Install Close


+ System


+ AppExpert

— Traffic Management





— Load Balancing

- Virtual Servers
- Services
- Service Groups
- Monitors
- Metric Tables
- Servers**
- Persistence Groups

+ Content Switching 

+ Cache Redirection 

NetScaler > Traffic Management > Load Balancing > Servers

Name	State	IPAddress / Domain
▶ 2012R2-A	 Enabled	172.27.44.90
▶ 2012R2-B	 Enabled	172.27.44.91
▶ 2012R2-C	 Enabled	172.27.44.92
▶ 2012R2-D	 Enabled	172.27.44.93

Standard Parameters Tab

Create Monitor

Name*

StoreFront

Type*

STOREFRONT

Standard Parameters

Special Parameters

Interval

5

Second

Destination IP

☐ IPv6

Response Time-out

2

Second

Destination Port

Bound Service

Down Time

30

Second

☒ Enabled

☐ Reverse

☐ Transparent

☒ LRTM (Least Response Time using Monitoring)

☒ Secure

Special Parameters Tab

← Back

Configure Monitor

Name

StoreFront

Type

STOREFRONT

Standard Parameters

Special Parameters

Store Name

Store

☐ Storefront Account Service

☒ Check Backend Services

OK

Close

Create Service Group Member

☐ IP Based ☒ Server Based

Select Server*

2012R2-A, 2012R2-B, 2012R2-C, ... > + 

Port*

443

Weight

1

Server Id

1

Hash Id

☒ State

Create

Close

Monitors

Add Binding

Edit Binding

Unbind

Edit Monitor

Monitor Name	Weight	State
StoreFront	1	✓

Close

ServiceGroup Server Certificates Binding

Add Binding

Unbind

Update Certificate

wildcard, .com

Method

×

Load Balancing Method*

LEASTCONNECTION ▾

New Service Startup Request Rate

New Service Request unit*

PER_SECOND ▾

Increment Interval

OK

Persistence

Persistence*

COOKIEINSERT

Time-out (mins)*

20

Cookie Name

NSC_SFPersistence

Backup Persistence

Backup Persistence

NONE

Backup Time-out

2

IPv4 Netmask

255 . 255 . 255 . 255

IPv6 Mask Length

128



OK

<https://docs.citrix.com>

© 1999-2017 Citrix Systems, Inc. All rights reserved.





p.175

NetScaler configuration tree:

- + System
- + AppExpert
- Traffic Management
 - Load Balancing
 - Virtual Servers
 - Services
 - Service Groups
 - Monitors
 - Metric Tables
 - Servers**
 - Persistency Groups
- + Content Switching 
- + Cache Redirection 

NetScaler > Traffic Management > Load Balancing > Servers

Buttons: Add, Edit, Delete, Action (dropdown)

Name	State	IPAddress / Domain
▶ 2012R2-A	 Enabled	172.27.44.90
▶ 2012R2-B	 Enabled	172.27.44.91
▶ 2012R2-C	 Enabled	172.27.44.92
▶ 2012R2-D	 Enabled	172.27.44.93

Standard Parameters Tab

Create Monitor

Name*

StoreFront

Type*

STOREFRONT

Standard Parameters

Special Parameters

Interval

5

Second

Destination IP

.

.

.

☐ IPv6

Response Time-out

2

Second

Destination Port

Bound Service

Down Time

30

Second

☒ Enabled

☐ Reverse

☐ Transparent

☒ LRTM (Least Response Time using Monitoring)

☒ Secure

Special Parameters Tab

← Back

Configure Monitor

Name

StoreFront

Type

STOREFRONT

Standard Parameters

Special Parameters

Store Name

Store

☐ Storefront Account Service

☒ Check Backend Services

OK

Close

Monitors

Add Binding

Edit Binding

Unbind

Edit Monitor

Monitor Name	Weight	State	Passive
tcp	1	✓	✗

Close

Load Balancing Virtual Server

Basic Settings

Name*

2012R2A-D-Synch

Protocol*

TCP

IP Address Type*

IP Address

IP Address*

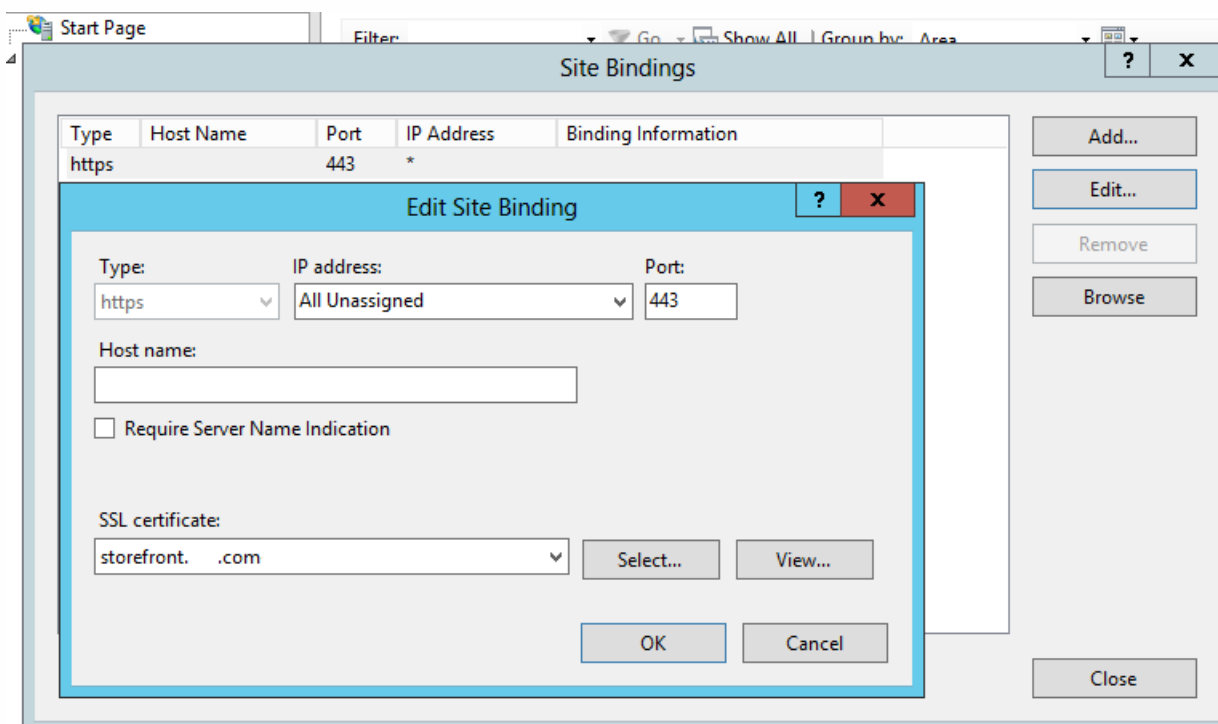
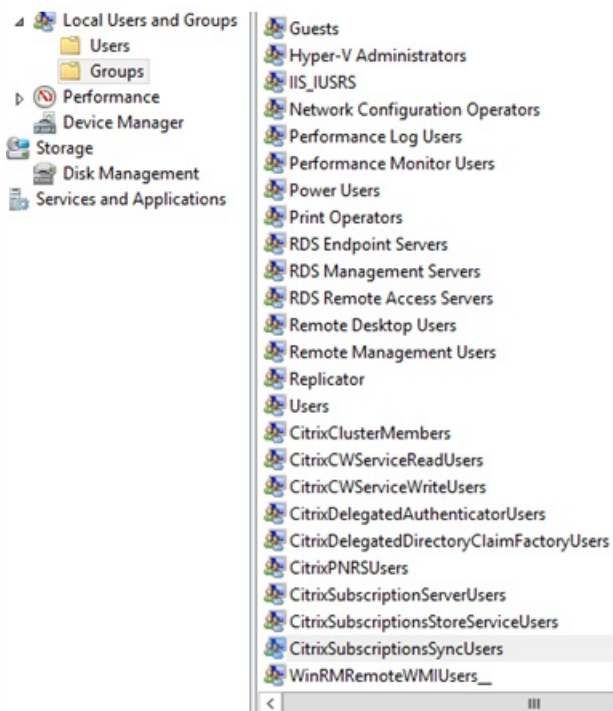
172 . 27 . 44 . 179

☐ IPv6

Port*

808





Join Server Group

To authorize this server, first connect to a server in the group and choose "Add Server". Enter the provided authorization information here.


Authorizing server:

Authorization code:

Join

Cancel

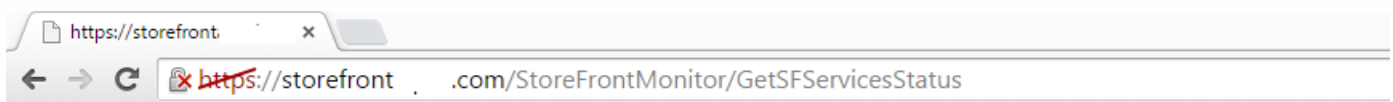
Add Server

 "2012R2-B" added to Server Group

Details

Servers	Status
2012R2-B	Completed

OK



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<ArrayOfServiceStatus xmlns="http://schemas.datacontract.org/2004/07/Citrix.DeliveryServices.ServiceMonitor.Contract"
  xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  <ServiceStatus>
    <name>Citrix Peer Resolution Service</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>CitrixConfigurationReplication</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>CitrixCredentialWallet</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>CitrixDefaultDomainService</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>CitrixSubscriptionsStore</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>NetTcpPortSharing</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>WAS</name>
    <status>running</status>
  </ServiceStatus>
  <ServiceStatus>
    <name>W3SVC</name>
    <status>running</status>
  </ServiceStatus>
</ArrayOfServiceStatus>
```

Add NetScaler Gateway Appliance

StoreFront

General Settings

Secure Ticket Authority

General Settings

The display name is visible to users in Citrix Receiver preferences.

Display name:	<input type="text" value="AGEE"/>
NetScaler Gateway URL:	<input type="text" value="https://storefront.example.com"/>
Version:	<input type="text" value="10.0 (Build 69.4) or later"/>
Subnet IP address: (optional)	<input type="text" value="SNIP or MIP"/>
Logon type:	<input type="text" value="Domain"/>
Smart card fallback:	<input type="text" value="None"/>
Callback URL: ⓘ (optional)	<input type="text" value="https://storecb.example.com"/> /CitrixAuthService/AuthService.asmx

-
-
-
-
-



-

-

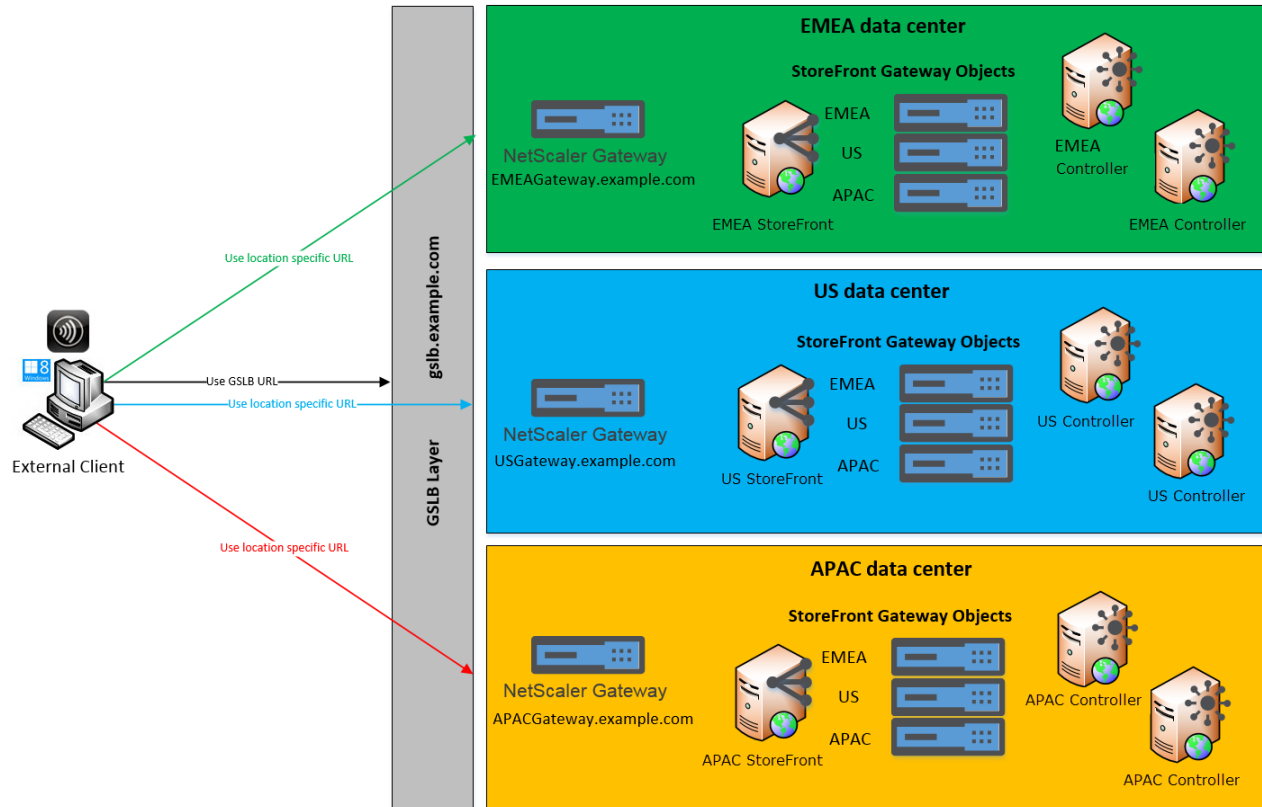
-

-

-

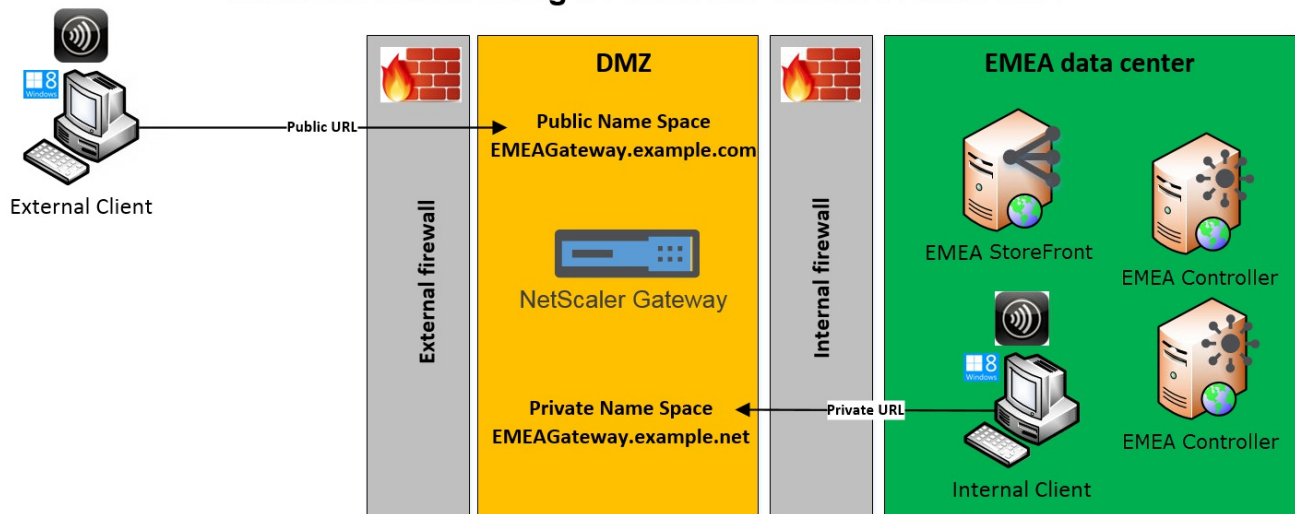
-

Remote Access using the GSLB domain name or a location specific URL for each Gateway



-
-
-
-
-
-

Remote Access using a Public URL and a Private URL



-
-
-
-

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.e
```

```
Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.e
```

```
Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA gateway object)
```

Or

```
Get-STFRoamingGateway (returns all gateway object configured in StoreFront)
```

Name: **EMEAGateway**

Location: **https://emeagateway.example.com/** (Unique URL for the EMEA Gateway)

GslbLocation: **https://gslb.example.com/** (GSLB URL for all three gateways)

Name: **USGateway**

Location: **https://USgateway.example.com/** (Unique URL for the US Gateway)

GslbLocation: **https://gslb.example.com/** (GSLB URL for all three gateways)

Name: **APACGateway**

Location: **https://APACgateway.example.com/** (Unique URL for the APAC Gateway)

GslbLocation: **https://gslb.example.com/** (GSLB URL for all three gateways)

Name: **EMEAGateway**

Location: **https://emeagateway.example.com/** (Public URL for the Gateway)

GslbLocation: **https://emeagateway.example.net/** (Private URL for the Gateway)

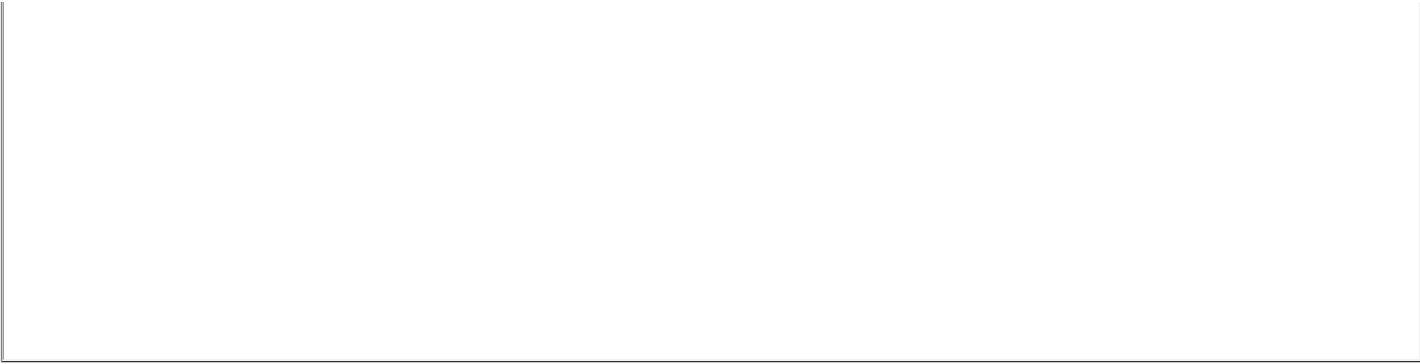
```
$StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<YourStore>"
```

```
Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject
```

Hostnames: **{emeagateway.example.com, gslb.example.com}**

Hostnames: **{usgateway.example.com, gslb.example.com}**

Hostnames: **{apacgateway.example.com, gslb.example.com}**



-
-
-
-
-

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts' PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
```

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
```

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
```

-

-




```
& "installationlocation\Scripts\ImportModules.ps1"
```

```
Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid -VirtualPath sitepath -UseHttps {$False | $True} -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}]
```

```
Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
```

```
Get-DSDesktopAppliancesSummary
```



-
-

Certificate Properties

Subject

General

Extensions

Private Key

Certification Authority

Signature

Subject

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type:

Common name

Add >

< Remove

CN=storefront.example.com

Alternative name:

Type:

DNS

Add >

< Remove

DNS

storefront.example.com

storefrontcb.example.com

accounts.example.com

Learn more about [subject names](#)

OK

Cancel

Apply

-

-

-

-

-

Configure NetScaler Gateway Session Profile

Name* Receiver

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration

Client Experience

Security

Published Applications

Home Page

none

Display Home Page

URL for Web-Based Email

Split Tunnel

OFF

Session Time-out (mins)

60

Client Idle Time-out (mins)

Clientless Access

On

Clientless Access URL Encoding

Clear

Clientless Access Persistent Co...

ALLOW

Plug-in Type

Windows/Mac OS X

Single Sign-on to Web Applications

Credential Index

PRIMARY

ICD Account

Single Sign-on with Windows

Client Cleanup Prompt

Override Global

Advanced

Configure NetScaler Gateway Session Profile

Name* Receiver

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration

Client Experience

Security

Published Applications

ICA Proxy

OFF

Override Global

Web Interface Address

Web Interface Portal Mode

NORMAL

Single Sign-on Domain

ptd

Citrix Receiver Home Page

Account Services Address

https://accounts.example.com/Citrix/Roaming/Accounts

Configure NetScaler Gateway Session Profile x

Name* Receiver ICAProxy

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Override Global

Home Page	none	<input type="checkbox"/> Display Home Page	<input type="checkbox"/>
URL for Web-Based Email			<input type="checkbox"/>
Split Tunnel	OFF		<input type="checkbox"/>
Session Time-out (mins)	60		<input checked="" type="checkbox"/>
Client Idle Time-out (mins)			<input type="checkbox"/>
Clientless Access	Off		<input checked="" type="checkbox"/>
Clientless Access URL Encoding	Clear		<input checked="" type="checkbox"/>
Clientless Access Persistent Co...	DENY		<input checked="" type="checkbox"/>
Plug-in Type	Java		<input checked="" type="checkbox"/>

Configure NetScaler Gateway Session Profile x

Name* Receiver ICAProxy

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Override Global

ICA Proxy	ON		<input checked="" type="checkbox"/>
Web Interface Address	https://storefront.example.com		<input checked="" type="checkbox"/>
Web Interface Portal Mode	NORMAL		<input checked="" type="checkbox"/>
Single Sign-on Domain	ptd		<input checked="" type="checkbox"/>
Citrix Receiver Home Page			<input type="checkbox"/>
Account Services Address	https://storefront.example.com		<input checked="" type="checkbox"/>

Configure NetScaler Gateway Session Profile x

Name* WebReceiver ICA Proxy

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Override Global

Home Page	https://storefront.ptd.com/Citrix/StoreWeb	<input checked="" type="checkbox"/> Display Home Page	<input checked="" type="checkbox"/>
URL for Web-Based Email			<input type="checkbox"/>
Split Tunnel	OFF		<input type="checkbox"/>
Session Time-out (mins)	60		<input checked="" type="checkbox"/>
Client Idle Time-out (mins)			<input type="checkbox"/>
Clientless Access	Off		<input checked="" type="checkbox"/>
Clientless Access URL Encoding	Clear		<input checked="" type="checkbox"/>
Clientless Access Persistent Co...	DENY		<input checked="" type="checkbox"/>
Plug-in Type	Windows/Mac OS X		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Single Sign-on to Web Applications			<input checked="" type="checkbox"/>

Configure NetScaler Gateway Session Profile

Name*WebReceiver

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration

Client Experience

Security

Published Applications

ICA Proxy

Web Interface Address

Web Interface Portal Mode

Single Sign-on Domain

Citrix Receiver Home Page

Account Services Address

ON

https://storefront.example.com/Citrix/StoreWeb

NORMAL

ptd

Override Global

☒

☒

☒

☒

☐

☐

-
-
-

Certificate Properties [X]

Subject | General | Extensions | Private Key | Certification Authority | Signature

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type: Common name ▼

Value:

Add > < Remove

CN=storefront.example.com

Alternative name:

Type: DNS ▼

Value:

Add > < Remove

DNS
storefront.example.com
storefrontcb.example.com
accounts.example.com

Learn more about [subject names](#)

OK Cancel Apply

Certificate Properties [X]

Subject | General | Extensions | Private Key | Certification Authority | Signature

Cryptographic Service Provider ▼

Key options ^

Set the key length and export options for the private key.

Key size: 1024 ▼

☒ Make private key exportable

☐ Allow private key to be archived

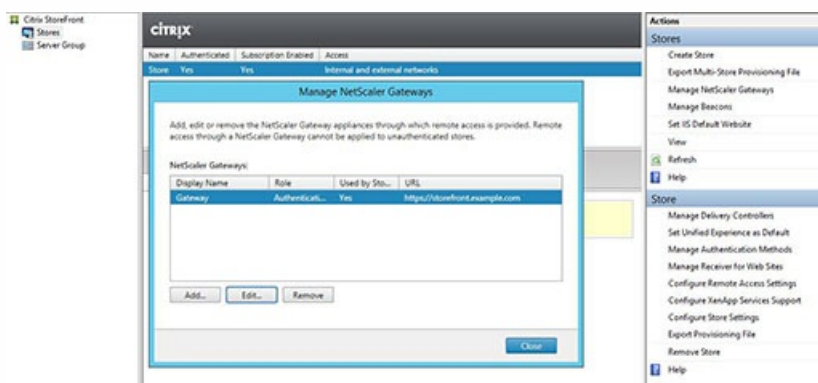
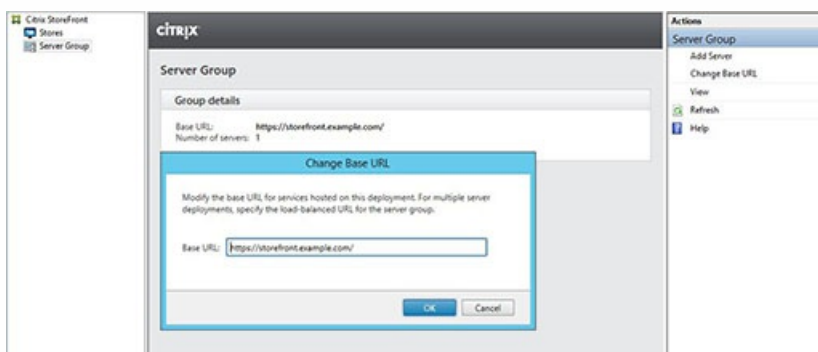
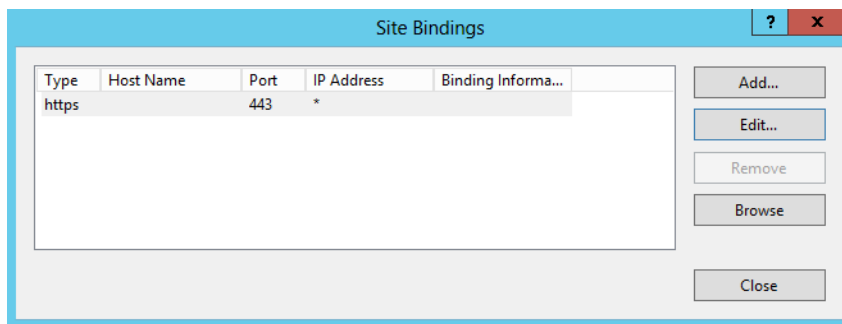
☐ Strong private key protection

Key type ▼

Key permissions ▼

Learn more about [private keys](#)

OK Cancel Apply



Edit NetScaler Gateway appliance - Gateway

StoreFront

General Settings

Secure Ticket Authority

Authentication Settings

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

Subnet IP address: (optional) SNIP or MIP

Logon type: 1 Domain

Smart card fallback: None

Callback URL: 1 (optional) https://storefront.example.com /CitrixAuthService/AuthService.asmx

OK Cancel Apply

Manage Beacons

Beacon points are used to determine whether users are connecting from internal or external networks. Two external addresses that can be resolved from the Internet are required.

Internal beacon: ☐ Use the service URL ☒ Specify beacon address: https://accounts.example.com

External beacons: http://www.citrix.com https://storefront.example.com

Add... Edit... Remove

OK Cancel

Export Provisioning File

Distribute this file to your users to automate Citrix Receiver setup.

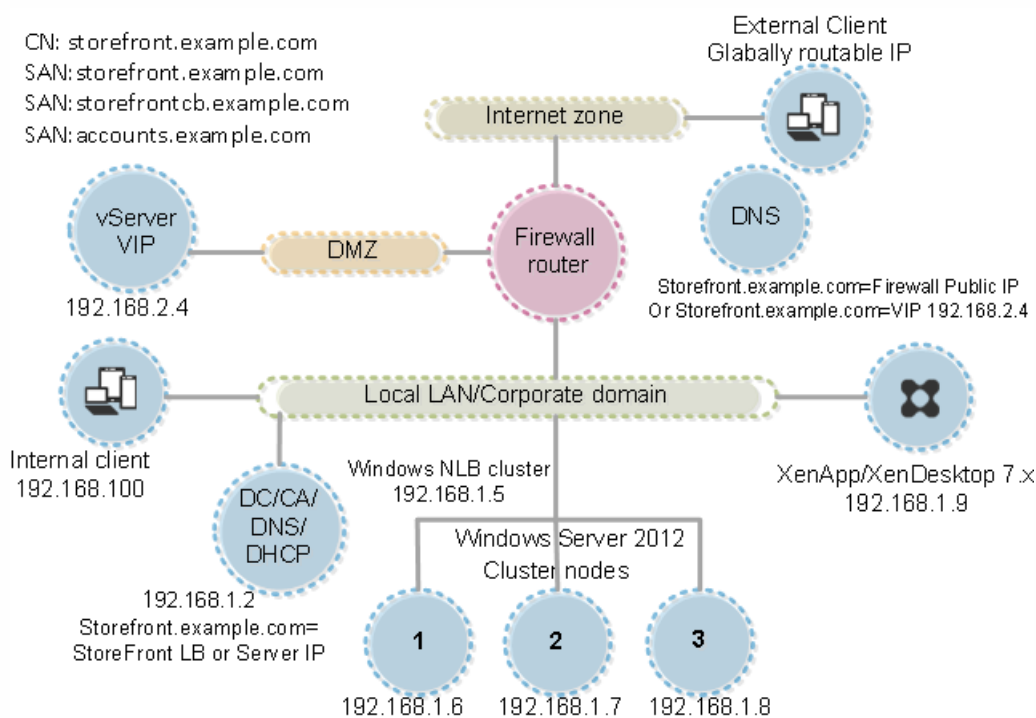
Name: Store
 URL: https://storefront.ptd.com/Citrix/Store
 Access: Internal and external networks

Details

Default NetScaler Gateway appliance: AGEE3
 Other appliances:

Internal beacons: https://accounts.ptd.com
 External beacons: http://www.citrix.com, https://storefront.ptd.com

Export Cancel



```
$dsInstallProp = Get-ItemProperty ` -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir $dsInstallDir = $dsInstallProp.InstallDir & $dsInstallDi
```

```
•  
•
```

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

```
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -IncludeTypes @("Applications")
```

-
-
-
-

-
-

...

```
certificateid" thumb="certificatethumbprint" /> ...
```

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands $certificate = Get-DSCertificate "certificatethumbprint" Add-DSCertificateKeyReadAccess -certificate $cert
```

@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@

@Heading("ExplicitAuth:AuthenticateHeadingText")

My Company Name

@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

-
-

-
-
-

-
-
-

-
-
-
-

-
-

-
-
-
-
-
-

-
-

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-

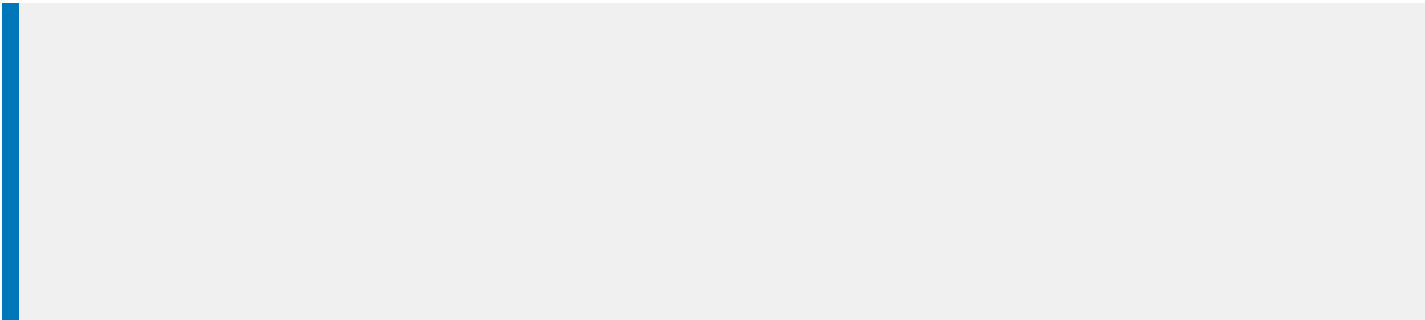
-

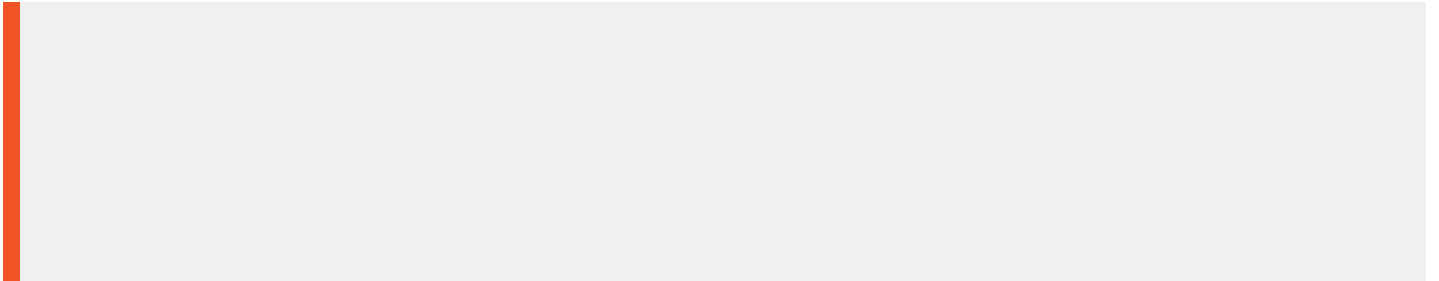
-

-

-

-





Add Website

Site name:

Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type:

IP address:

Port:

Host name:

☐ Require Server Name Indication

SSL certificate:

☒ Start Website immediately

Browse For Folder

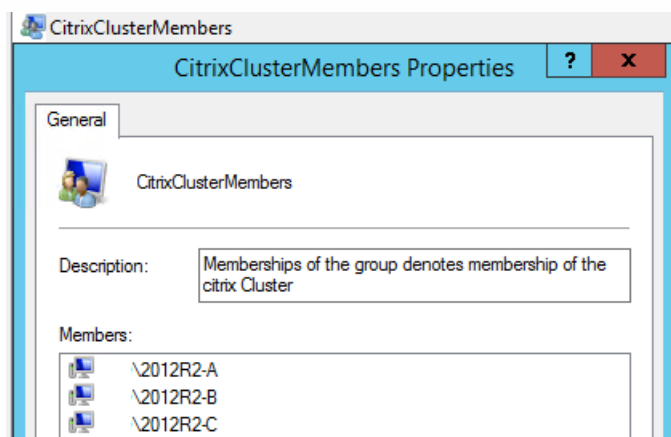
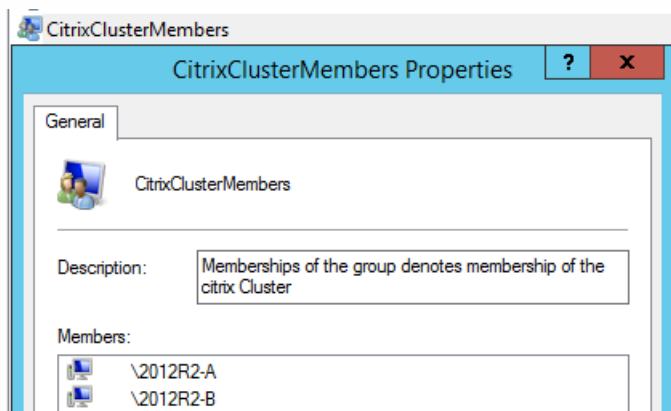
Select a directory for the application.

- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- New Volume (D:)
 - Inetpub
 - wwwroot
- CD Drive (E:)

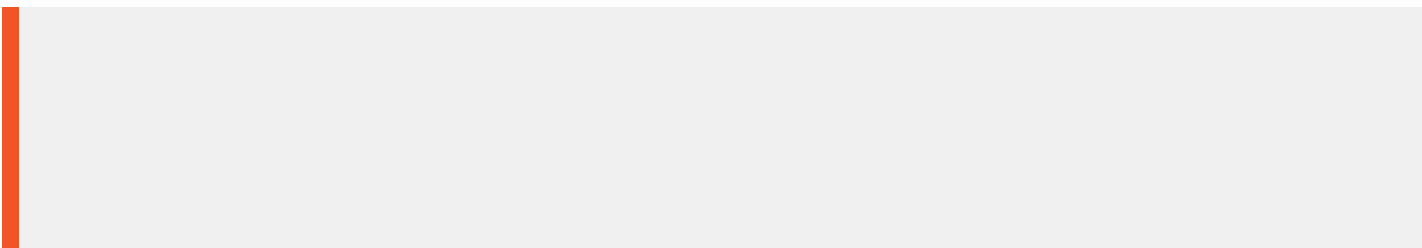
Application Pools

- Sites
 - Default Web Site
 - Storefront

Name	ID	Status	Binding	Path
Default Web Site	1	Started (http)	*:80 (http)	%SystemDrive%\inetpub\wwwroot
Storefront	2	Started (http)	*:443 (https)	D:\inetpub\wwwroot



-
-
-



```
Import-Module Citrix.StoreFront
```

```
Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront") } | Import-Module
```

-
-
-
-
-

•

-

-

•

•

•

•

•

•

-

-

-

•

•

•

•

•

-

-

-


```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module
```

```
# Remember to change this with the virtual path of your Store.
```

```
$StoreVirtualPath = "/Citrix/Store"
```

```
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
```

```
$auth = Get-STFAuthenticationService -StoreService $store
```

```
# To read the metadata directly from the Identity Provider, use the following:
```

```
# Note again this is only allowed for https endpoints
```

```
Update-STFSamlIDPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMetadata.xml
```

```
# If the metadata has already been download, use the following:
```

```
# Note: Ensure that the file is encoded as UTF-8
```

```
Update-STFSamlIDPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.xml"
```

Change this value for your Store

```
$storeVirtualPath = "/Citrix/Store"
```

```
$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -VirtualPath $storeVirtualPath)
```

```
$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.ServiceProvider.Uri.AbsoluteUri
```

```
$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlForms/AssertionConsumerService")
```

```
$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlForms/ServiceProvider/Metadata")
```

```
$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlTest")
```

Write-Host "SAML Service Provider information:

Service Provider ID: \$spId

Assertion Consumer Service: \$acs

Metadata: \$md

Test Page: \$samlTest"

SAML Service Provider information:

Service Provider ID: <https://storefront.example.com/Citrix/StoreAuth>

Assertion Consumer Service: <https://storefront.example.com/Citrix/StoreAuth/SamlForms/AssertionConsumerService>

Metadata: <https://storefront.example.com/Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata>

Test Page: <https://storefront.example.com/Citrix/StoreAuth/SamlTest>

Résolution des problèmes de StoreFront

Jun 30, 2017

Lorsque StoreFront est installé ou désinstallé, les fichiers journaux suivants sont créés par le programme d'installation de StoreFront dans le répertoire C:\Windows\Temp\. Les noms des fichiers reflètent les composants qui les ont créés et incluent des horodatages.

- Citrix-DeliveryServicesRoleManager-*.log : créé lorsque StoreFront est installé de manière interactive.
- Citrix-DeliveryServicesSetupConsole-*.log : créé lorsque StoreFront est installé en mode silencieux et lorsque StoreFront est désinstallé de manière interactive ou silencieuse.
- CitrixMsi-CitrixStoreFront-x64-*.log : créé lorsque StoreFront est installé et désinstallé, de manière interactive ou silencieuse.

StoreFront prend en charge la journalisation d'événements Windows pour le service d'authentification, les magasins et les sites Receiver pour Web. Tous les événements générés sont journalisés dans le journal des applications de StoreFront, qui peut être consulté à l'aide de l'Observateur d'événements accessible dans Journaux des applications et des services > Citrix Delivery Services ou dans Journaux Windows > Application. Vous pouvez contrôler le nombre des doublons d'entrées du journal pour un événement unique en modifiant les fichiers de configuration du service d'authentification, des magasins et des sites Receiver pour Web.

La console de gestion Citrix StoreFront enregistre automatiquement les informations de suivi. Par défaut, le suivi d'autres opérations est désactivé et doit être activé manuellement. Les journaux créés par les commandes Windows PowerShell sont stockés dans le répertoire \Admin\logs\ de l'installation StoreFront, généralement situé sur C:\Program Files\Citrix\Receiver StoreFront\. Le nom du fichier journal contient les actions de commande et les objets, ainsi que les informations de date qui peuvent être utilisés pour différencier les séquences de commande.

Important : dans les déploiements comprenant de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, [propagez les modifications que vous avez apportées à la configuration du groupe de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Pour configurer l'optimisation du journal

1. Utilisez un éditeur de texte pour ouvrir le fichier web.config du service d'authentification, du magasin ou du site Receiver pour Web, qui se trouve en général dans les répertoires C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\, et C:\inetpub\wwwroot\Citrix\storenameWeb\, où storename désigne le nom indiqué pour le magasin au moment de sa création.
2. Recherchez l'élément suivant dans le fichier.
Par défaut, StoreFront est configuré pour limiter le nombre de doublons d'entrées du journal à 10 par minute.
3. Modifiez la valeur de l'attribut duplicateInterval sur la durée définie en heures, minutes et secondes pendant laquelle les doublons d'entrées du journal seront analysés. Utilisez l'attribut duplicateLimit pour définir le nombre de doublons d'entrées devant être consignés dans l'intervalle spécifié, afin de déclencher l'optimisation du journal.

Lors du déclenchement de l'optimisation du journal, un message d'avertissement est journalisé pour indiquer que les autres entrées de journal identiques seront supprimées. Une fois la durée écoulée, la journalisation normale se poursuit et un message d'information est journalisé pour indiquer que les doublons d'entrées du journal ne sont plus supprimés.

Pour activer le suivi

Avertissement : les consoles StoreFront et PowerShell ne peuvent pas être ouvertes en même temps. Fermez toujours la console d'administration StoreFront avant d'utiliser la console PowerShell pour administrer votre configuration StoreFront. De même, fermez toutes les instances de PowerShell avant d'ouvrir la console StoreFront.

1. Utilisez un compte possédant des permissions d'administrateur local pour démarrer Windows PowerShell et, à l'invite de commande, tapez les commandes suivantes et redémarrez le serveur pour activer le traçage.

`Add-PSSnapin Citrix.DeliveryServices.Framework.Commands Set-DSTraceLevel -All -TraceLevel Verbose`
Valeurs autorisées pour -TraceLevel sont, niveau de détail de suivi : Off, Error, Warning, Info, Verbose.

StoreFront capture automatiquement les messages de trace d'erreur. Compte tenu du volume important de données qui peut être potentiellement généré, le suivi peut affecter de manière considérable les performances de StoreFront, il est donc recommandé de ne pas utiliser les niveaux Info ou Verbose à moins que cela ne soit nécessaire à des fins de dépannage.

Les arguments facultatifs de l'applet de commande Set-DSTraceLevel sont :

-FileCount : spécifie le nombre de fichiers de trace (valeur par défaut = 3)

-FileSizeKb : spécifie la taille maximale de chaque fichier de trace (valeur par défaut = 1000)

-ConfigFile : alternative à -All qui permet de mettre à jour un fichier de configuration spécifique plutôt que tous les fichiers. Par exemple, une valeur -ConfigFile value of c:\inetpub\wwwroot\Citrix\web.config définirait le traçage pour le magasin appelé .

2. Pour désactiver le suivi, tapez les commandes suivantes et redémarrez le serveur.

`Add-PSSnapin Citrix.DeliveryServices.Framework.Commands Set-DSTraceLevel -All -TraceLevel Off`

Lorsque le suivi est activé, les informations de suivi sont journalisées dans le répertoire d'installation de StoreFront (\Admin\Trace\), qui se trouve sur l'emplacement C:\Program Files\Citrix\Receiver StoreFront\.