



# StoreFront 1811

## Contents

<b>StoreFront 1811</b>	<b>3</b>
<b>Nouveautés</b>	<b>4</b>
<b>Problèmes résolus</b>	<b>8</b>
<b>Problèmes connus</b>	<b>8</b>
<b>Avis de tiers</b>	<b>9</b>
<b>Configuration système requise</b>	<b>10</b>
<b>Planifier votre déploiement StoreFront</b>	<b>18</b>
<b>Options d'accès utilisateur</b>	<b>24</b>
<b>Authentification utilisateur</b>	<b>35</b>
<b>Optimiser l'expérience utilisateur</b>	<b>48</b>
<b>Haute disponibilité et configuration multisite de StoreFront</b>	<b>53</b>
<b>Installer, configurer, mettre à niveau et désinstaller</b>	<b>58</b>
<b>Créer un nouveau déploiement</b>	<b>69</b>
<b>Joindre un groupe de serveurs existant</b>	<b>77</b>
<b>Migrer les fonctionnalités de l'Interface Web vers StoreFront</b>	<b>79</b>
<b>Configurer des groupes de serveurs</b>	<b>85</b>
<b>Configurer l'authentification et la délégation</b>	<b>88</b>
<b>Configurer le service d'authentification</b>	<b>90</b>
<b>Authentification basée sur le service XML</b>	<b>98</b>
<b>Configurer la délégation Kerberos contrainte pour XenApp 6.5</b>	<b>99</b>
<b>Configuration de l'authentification par carte à puce</b>	<b>103</b>
<b>Configurer la période de notification d'expiration du mot de passe</b>	<b>109</b>
<b>Configurer et gérer des magasins</b>	<b>110</b>

<b>Créer ou supprimer un magasin</b>	<b>111</b>
<b>Créer un magasin non authentifié</b>	<b>119</b>
<b>Exporter des fichiers de provisioning de magasin pour des utilisateurs</b>	<b>122</b>
<b>Publier et masquer des magasins pour les utilisateurs</b>	<b>123</b>
<b>Gérer les ressources mises à disposition dans les magasins</b>	<b>123</b>
<b>Gérer l'accès distant aux magasins via NetScaler Gateway</b>	<b>125</b>
<b>Intégrer des applications Citrix Online à des magasins</b>	<b>129</b>
<b>Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun</b>	<b>130</b>
<b>Paramètres de magasin avancés</b>	<b>132</b>
<b>Gérer un site Citrix Receiver pour Web</b>	<b>137</b>
<b>Créer un site Citrix Receiver pour Web</b>	<b>138</b>
<b>Configurer des sites Citrix Receiver pour Web</b>	<b>139</b>
<b>Prise en charge de l'expérience Citrix Receiver unifiée</b>	<b>146</b>
<b>Créer et gérer des applications recommandées</b>	<b>152</b>
<b>Configurer le contrôle de l'espace de travail</b>	<b>154</b>
<b>Configurer l'utilisation des onglets de navigateur par Citrix Receiver pour HTML5</b>	<b>155</b>
<b>Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion</b>	<b>156</b>
<b>Configurer l'accès utilisateur</b>	<b>158</b>
<b>Configurer StoreFront pour lancer les applications et les bureaux en mode fenêtré</b>	<b>167</b>
<b>Définir des magasins multisite à haute disponibilité</b>	<b>169</b>
<b>Forcer les connexions via Citrix Gateway à l'aide de la fonction Passerelle optimale de StoreFront</b>	<b>188</b>
<b>Intégrer avec Citrix Gateway et Citrix ADC</b>	<b>190</b>

<b>Ajouter une connexion NetScaler Gateway</b>	<b>192</b>
<b>Importer un boîtier NetScaler Gateway</b>	<b>195</b>
<b>Configurer les paramètres de connexion à NetScaler Gateway</b>	<b>205</b>
<b>Équilibrage de charge avec NetScaler</b>	<b>209</b>
<b>Configurer deux adresses URL pour le même NetScaler Gateway</b>	<b>229</b>
<b>Configurer l'authentification DFA entre NetScaler et StoreFront</b>	<b>239</b>
<b>Authentification à l'aide de domaines différents</b>	<b>242</b>
<b>Configurer des points balises</b>	<b>253</b>
<b>Configurations avancées</b>	<b>255</b>
<b>Configurer des sites Desktop Appliance</b>	<b>255</b>
<b>Créer un seul nom de domaine complet (FQDN) pour accéder à un magasin en interne et externe</b>	<b>259</b>
<b>Configurer le filtrage des ressources</b>	<b>279</b>
<b>Configurer des sites à l'aide des fichiers de configuration</b>	<b>280</b>
<b>Configurer StoreFront à l'aide des fichiers de configuration</b>	<b>281</b>
<b>Configurer des sites Citrix Receiver pour Web à l'aide des fichiers de configuration</b>	<b>286</b>
<b>Sécuriser votre déploiement StoreFront</b>	<b>288</b>
<b>Exporter et importer la configuration StoreFront</b>	<b>295</b>
<b>SDK StoreFront</b>	<b>307</b>
<b>Résolution des problèmes de StoreFront</b>	<b>323</b>

## StoreFront 1811

January 17, 2019

**StoreFront 1811** est la version Current Release la plus récente de StoreFront. Cette documentation reflète les fonctionnalités et les configurations de cette dernière version.

StoreFront est un magasin d'applications d'entreprise qui regroupe les applications et les bureaux des sites Citrix Virtual Apps and Desktops en un seul magasin facile à utiliser pour les utilisateurs. StoreFront fait partie intégrante de Citrix Virtual Apps and Desktops (anciennement XenApp et XenDesktop) mais peut être utilisé avec plusieurs versions de XenApp et XenDesktop.

### Versions précédentes

Pour accéder à la documentation des versions antérieures, consultez :

- [StoreFront 3.16](#)
- [StoreFront 3.15](#)
- [StoreFront 3.14](#)
- [StoreFront 3.13](#)
- [StoreFront 3.12](#)
- [StoreFront 3.11](#)
- [Versions antérieures de StoreFront](#)

La stratégie de cycle de vie du produit des versions Current Releases (CR) et Long Term Service Releases (LTSR) de Citrix Virtual Apps and Desktops est décrite dans [Étapes du cycle de vie](#). Pour de plus amples informations sur le cycle de vie de StoreFront, consultez l'article [CTX200356](#).

Remarque :

Les mises à niveau vers la version Current Release la plus récente de StoreFront à partir de versions non prises en charge ne sont pas prises en charge. Si vous utilisez des versions Current Release, vous devez vous assurer que vous utilisez une version Current Release de StoreFront prise en charge à tout moment.

### Modifications apportées aux noms et aux numéros de version des produits Citrix

Si vous êtes client ou partenaire Citrix depuis un certain temps, vous remarquerez de nouveaux noms dans nos produits et dans la documentation de ces produits. Si vous découvrez ce produit Citrix, vous pourrez parfois rencontrer des noms différents pour un produit ou un composant. Les nouveaux noms de produits et de composants représentent mieux le portefeuille toujours croissant de Citrix et sa stratégie cloud.

Pour savoir comment les changements de nom récents affectent StoreFront, consultez la section [Nouveaux noms de produits](#).

Dans cette version, les numéros de version des produits et des composants sont affichés dans un nouveau format. Pour savoir comment ces changements affectent StoreFront, consultez la section [Changements de numéros de version des produits et composants](#).

## Nouveautés

February 20, 2019

### StoreFront 1811

StoreFront 1811 comprend les nouvelles fonctionnalités suivantes. Pour plus d'informations sur les corrections de bogues, veuillez consulter la section [Problèmes résolus](#).

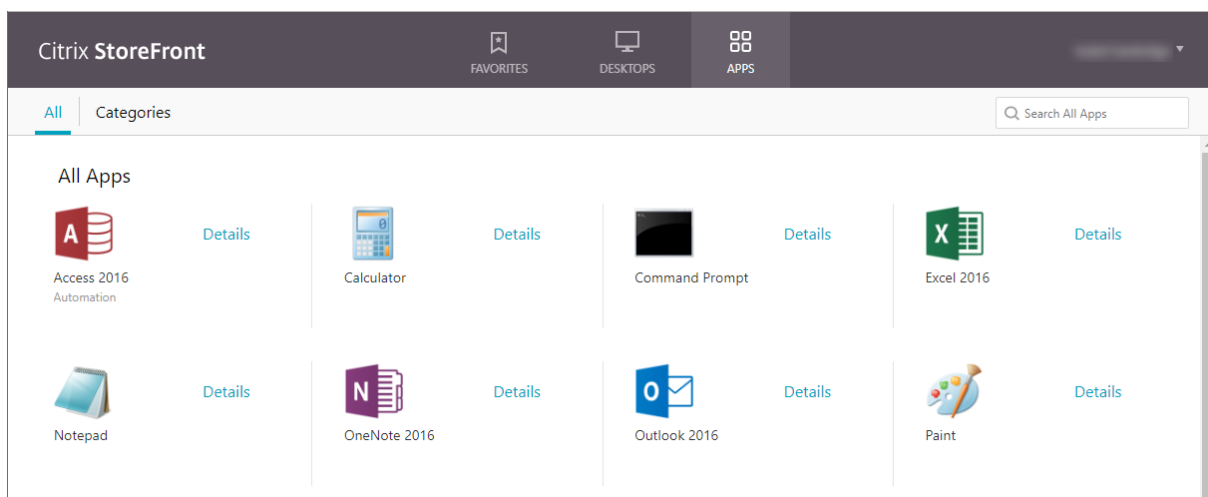
#### Expérience utilisateur unifiée

StoreFront prend en charge les expériences utilisateur *classique* et *unifiée*. Avec cette version, l'expérience utilisateur a été mise à jour pour mieux s'aligner avec Citrix Workspace et proposer une fonctionnalité plus étendue. Pour plus d'informations, consultez la section [Expérience utilisateur unifiée Citrix Receiver](#).

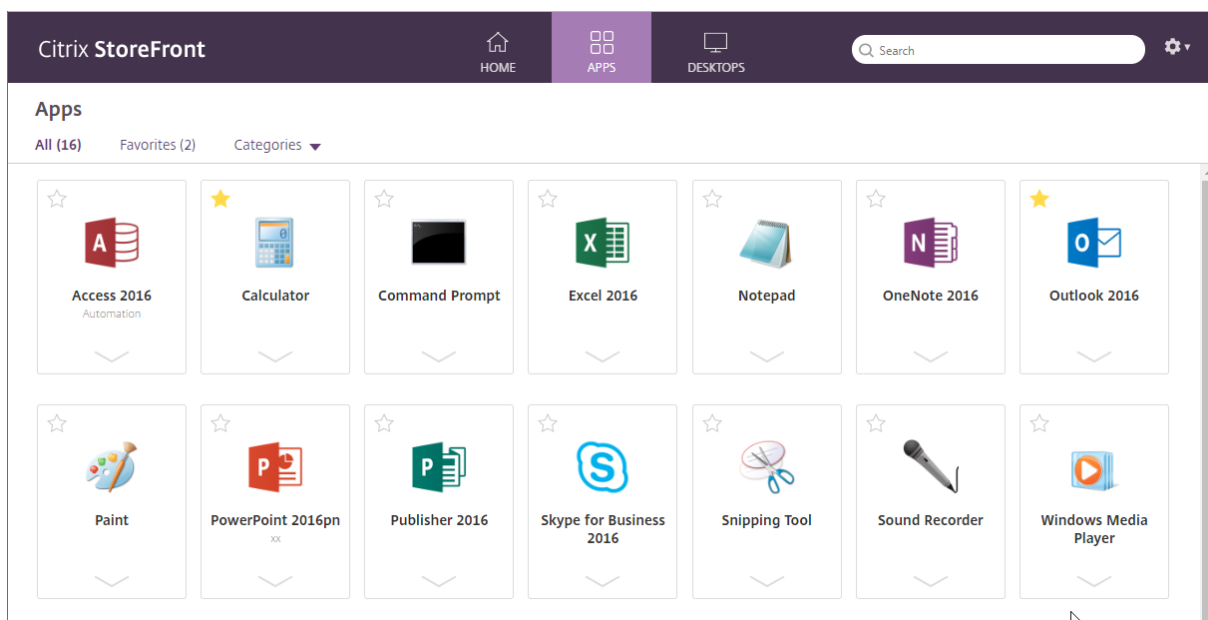
Remarque :

L'expérience unifiée n'est prise en charge que sur Internet Explorer 11. Consultez la section [Prise en charge d'Internet Explorer](#).

#### Avant



## Après



Si vous avez [personnalisé l'expérience unifiée](#), vos personnalisations sont préservées lorsque vous effectuez une mise à niveau vers cette version de StoreFront. Vérifiez que l'apparence de vos personnalisations est toujours adaptée à la nouvelle expérience unifiée. Nous vous recommandons d'informer les utilisateurs des changements de l'expérience unifiée apportés par cette mise à niveau, décrits dans [Expérience utilisateur unifiée Citrix Receiver](#).

## **Prise en charge des preuves de connexion du service et des données de disposition au lancement FAS**

StoreFront prend en charge la transmission au service d'authentification fédérée (FAS) des preuves de connexion du service et des données de disposition au lancement à des fins d'évaluation :

- StoreFront peut désormais capturer les preuves de connexion et les fournir au FAS à des fins de validation lorsque des utilisateurs essaient de lancer des VDA. Cela permet aux clients d'utiliser les plug-ins FAS pour vérifier que l'authentification a été effectuée auprès d'un fournisseur d'identité de confiance.
- StoreFront peut désormais fournir les données de disposition au lancement à FAS lorsque les VDA sont lancés. Cela permet aux clients de fournir des données de disposition à l'accès, quels plug-ins sur le serveur FAX peuvent être convertis en contexte de rôle et de sécurité à des fins d'évaluation d'identité.

Pour plus d'informations sur l'utilisation de ces fonctions, voir [Présentation des preuves de connexion du service d'authentification fédérée Citrix](#).

### **SDK d'authentification StoreFront**

Le SDK d'authentification StoreFront a été mis à jour pour prendre en charge les améliorations de collecte des preuves de connexion FAS.

La documentation du SDK d'authentification StoreFront est désormais disponible dans la documentation développeur Citrix <https://developer-docs.citrix.com/>.

### **SDK PowerShell StoreFront**

Le SDK PowerShell StoreFront a été mis à jour pour prendre en charge les améliorations de collecte des preuves de connexion FAS. L'objet représentant le service d'authentification, renvoyé par `Get-STFAuthenticationService`, contient une propriété « `AuthenticationOptions` ». Elle contient une nouvelle propriété « `CollectFasEvidence` » qui est définie sur `false` par défaut. Elle doit être activée pour utiliser la nouvelle fonction de preuve de connexion.

La documentation du SDK PowerShell StoreFront a été republiée sous la version 1811 dans la documentation développeur Citrix <https://developer-docs.citrix.com/>.

### **Nouveaux noms de produits**

Si vous êtes client ou partenaire Citrix depuis un certain temps, vous remarquerez de nouveaux noms dans nos produits et dans la documentation de ces produits. Si vous découvrez ce produit Citrix,



vous pourrez parfois rencontrer des noms différents pour un produit ou un composant. Les nouveaux noms de produits et de composants représentent mieux le portefeuille toujours croissant de Citrix et sa stratégie cloud.

L'implémentation de cette transition dans nos produits et leur documentation est en cours.

- Le contenu intégré au produit peut encore contenir les anciens noms. Par exemple, vous pouvez voir des instances des anciens noms dans le texte de la console, les messages et les noms de répertoire/fichier.
- Il est possible que certains éléments (tels que les commandes et les MSI) continuent à conserver leurs anciens noms pour éviter de casser les scripts clients existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.

Nous vous remercions de votre patience pendant cette transition. Pour plus de détails sur les nouveaux noms, voir <https://www.citrix.com/about/citrix-product-guide/>.

### **Nouveaux numéros de version des produits et composants**

Dans cette version, le numéro de version de StoreFront est affiché dans l'interface utilisateur de la console de gestion au même format numérique que Citrix Virtual App and Desktops (1811). La version de fichier utilise toujours le format 3.x (3.17). Pour une description complète de ce format, consultez la section [Nouveaux numéros de version des produits et composants](#).

### **Fin de prise en charge des versions TLS**

La fin de la prise en charge par StoreFront des protocoles TLS 1.0 et 1.1 a été annoncée pour StoreFront 3.14 et XenApp and XenDesktop 7.17, consultez la section [CTX23226](#).

Les clients peuvent désormais effectuer une mise à niveau vers l'application Citrix Workspace qui prend en charge le protocole TLS 1.2.

À compter de StoreFront 1811, Citrix recommande de désactiver la prise en charge de TLS 1.0 et 1.1 dans le serveur Web hébergeant StoreFront. Vous devriez appliquer cette désactivation via des objets de stratégie de groupe, qui créent les paramètres de registre nécessaires sur le serveur StoreFront pour désactiver les protocoles plus anciens comme TLS 1.0 et TLS 1.1. Consultez également la rubrique Microsoft [Paramètres TLS/SSL](#).

### **Prise en charge d'Internet Explorer**

Microsoft a supprimé la prise en charge des anciennes versions d'Internet Explorer. Consultez l'[avis de fin de prise en charge de Microsoft](#). Par conséquent, nous prenons uniquement en charge l'accès

aux magasins via les sites Citrix Receiver pour Web à l'aide d'Internet Explorer 11. Consultez la section [Configuration système requise](#).

## Problèmes résolus

February 20, 2019

Les problèmes suivants ont été résolus depuis la version 3.16 :

- Lorsque vous zoomez le navigateur à 125 %, le logo personnalisé peut disparaître. [LC9018]
- 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 ce message s'affiche :  
« Une erreur de protocole s'est produite lors de la communication avec le service d'authentification » . [LC9404]
- La session préliminaire peut ne pas fonctionner après la configuration de Filtrer les ressources par mots clés. [LC9642]
- Lorsque vous vous connectez à StoreFront et actualisez la page Citrix Receiver pour Web, la boîte de dialogue de délai d'expiration peut être supprimée. [LD0214]

## Problèmes connus

February 20, 2019

Les problèmes suivants sont connus dans cette version.

- La propagation des abonnements entre les membres d'un groupe de serveurs StoreFront échoue lorsque TLS 1.0 est désactivé dans Windows et que Windows Server utilise le serveur .NET 4.5 Framework. Par défaut, .NET 4.5 Framework utilise uniquement TLS 1.0. Une solution à ce problème consiste à mettre à niveau .NET Framework sur le serveur vers la version 4.7 ou ultérieure (qui utilise TLS 1.2 par défaut). [STF-2413]
- La jonction de groupes de serveurs ne fonctionne pas si TLS 1.0 est désactivé sur un serveur exécutant .NET Framework 4.6.1 ou version antérieure. Pour résoudre ce problème, effectuez une mise à niveau vers .NET 4.6.2 Framework ou version ultérieure. [STF-687]
- Il existe un problème de tiers connu avec l'authentification par carte à puce et Microsoft Edge. Pour résoudre ce problème, utilisez Internet Explorer. [DNA-47809]

- Le contrôle de l'espace de travail se reconnecte à une seule session d'application au lieu de toutes les applications dans l'espace de travail. Ce problème se produit si vous utilisez Chrome pour accéder au site Receiver pour Web. Pour résoudre ce problème, cliquez sur Connecter pour chaque application déconnectée. [DNA-25140, DNA-22561]
- Si une exception d'expiration du délai se produit pendant la mise à niveau de StoreFront à partir du programme d'installation de Citrix Virtual Apps and Desktops, procédez comme suit avant de redémarrer la mise à niveau :
  - Vérifiez que les [conditions matérielles requises pour Citrix Virtual Apps and Desktops](#) et la [configuration requise pour StoreFront](#) sont remplies.
  - Redémarrez la machine virtuelle hébergeant l'installation. [STF-3379]
- Lorsque StoreFront est désinstallé sur Windows Server 2019, la console PowerShell (PowerShell.exe) peut cesser de fonctionner sur le serveur. Les symptômes sont les suivants : PowerShell.exe s'ouvre brièvement, puis disparaît immédiatement et ne peut pas être utilisé. Powershell\_ISE.exe n'est pas affecté et peut toujours être utilisé pour exécuter des scripts Powershell.

**Ce problème se produit avec toutes les versions de StoreFront**, mais uniquement lorsque StoreFront est désinstallé sur Windows Server 2019.

Solution : pour que PowerShell.exe puisse fonctionner sur Windows Server 2019 après la désinstallation de StoreFront, ajoutez la ligne suivante :

```
<section name="uri" type="System.Configuration.UriSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
```

à la section de configuration des fichiers suivants :

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

Par exemple :

```
1 <configuration>
2   <configSections>
3     <section name="uri" type="System.Configuration.UriSection
      , System, Version=4.0.0.0, Culture=neutral,
      PublicKeyToken=b77a5c561934e089" />
```

[STF-2585]

## Avis de tiers

October 4, 2018

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

[Notices tierces StoreFront](#) (téléchargement PDF)

## Configuration système requise

February 20, 2019

Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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.

Remarque :

La mise à niveau vers la dernière version Current Release à partir d'une version Current Release plus ancienne qui est maintenant en fin de vie n'est pas prise en charge. Pour plus d'informations, voir [CTX200356](#).

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

- Windows Server 2019 éditions Standard et Datacenter
- Windows Server 2016 éditions Standard et Datacenter
- Windows Server 2012 R2 éditions Standard et Datacenter

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 ac-

tive 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
- 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 l'application Citrix Workspace pour HTML5 ou les versions Citrix Receiver prises en charge, 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.

- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp et XenDesktop 7.18
- XenApp et XenDesktop 7.17
- XenApp et XenDesktop 7.16
- XenApp et XenDesktop 7.15 LTSR
- XenApp et XenDesktop 7.14
- XenApp et XenDesktop 7.6 LTSR

### **Configuration requise pour Citrix Gateway**

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

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.x
- NetScaler Gateway 10.5

### **Configuration requise pour l'application Citrix Workspace pour HTML5**

Si vous souhaitez autoriser les utilisateurs à accéder aux bureaux et applications à l'aide de l'application Citrix Workspace pour HTML5 (anciennement Citrix Receiver for HTML5) exécutée sur les sites Receiver pour Web, les exigences supplémentaires suivantes s'appliquent.

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

- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp et XenDesktop 7.18
- XenApp et XenDesktop 7.17

- XenApp et XenDesktop 7.16
- XenApp et XenDesktop 7.15 LTSR
- XenApp et XenDesktop 7.14
- XenApp et XenDesktop 7.6 LTSR

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

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.x

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

- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp et XenDesktop 7.18
- XenApp et XenDesktop 7.17
- XenApp et XenDesktop 7.16
- XenApp et XenDesktop 7.15 LTSR
- XenApp et XenDesktop 7.14
- XenApp et XenDesktop 7.6 LTSR

## **Configuration requise pour la machine utilisateur**

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

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

#### **Application Citrix Workspace**

- [Application Citrix Workspace pour Android](#)
- [Application Citrix Workspace pour Chrome](#)
- [Application Citrix Workspace pour HTML5](#)
- [Application Citrix Workspace pour iOS](#)
- [Application Citrix Workspace pour Linux](#)
- [Application Citrix Workspace pour Mac](#)
- [Application Citrix Workspace pour Windows](#)
- [Application Citrix Workspace pour Windows \(Store\)](#)

#### **Citrix Receiver**

- [Citrix Receiver pour Android 3.13.x](#)
- [Citrix Receiver pour Chrome 2.x](#)
- [Citrix Receiver pour HTML5 2.x](#)
- [Citrix Receiver pour iOS 7.x](#)
- [Citrix Receiver pour Linux 13.x](#)
- [Citrix Receiver pour Mac 12.x](#)
- [Citrix Receiver pour Windows 4.x](#)

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

Les combinaisons application Citrix Workspace, 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 Citrix Gateway. Les connexions établies via Citrix Gateway peuvent être effectuées à l'aide de NetScaler Gateway Plug-in et de l'accès sans client.

Sauf indication contraire, les dernières versions de navigateur sont recommandées.

- Citrix Receiver pour Windows 4.9 et versions ultérieures, et application Citrix Workspace 1808 pour Windows et versions ultérieures
  - 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 11 (mode 32 bits)
    - \* Google Chrome
    - \* Mozilla Firefox
  - Windows 7 Service Pack 1 (éditions 32 et 64 bits)
    - \* Internet Explorer 11
    - \* Google Chrome
    - \* Mozilla Firefox
  - Windows Embedded Standard 7 Service Pack 1 ou Windows Thin PC
    - \* Internet Explorer 11
- Citrix Receiver pour Mac 12.0 et application Citrix Workspace 1808 pour Mac et versions ultérieures
  - Mac OS X 10.13 High Sierra
    - \* Safari 11
    - \* Google Chrome
    - \* Mozilla Firefox
  - Mac OS X 10.12 Sierra
    - \* Safari 11
    - \* Google Chrome
    - \* Mozilla Firefox
  - 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 13.x
  - Ubuntu 12.04 (32 bits) et 14.04 LTS (32 bits)
    - \* Google Chrome
    - \* Mozilla Firefox

### **Configuration requise pour l'accès aux bureaux et aux applications via l'application Citrix Workspace 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 l'application Citrix Workspace pour HTML5 exécutée sur des sites Receiver pour Web. Les connexions au réseau interne et les connexions via Citrix Gateway sont prises en charge. Toutefois, pour les connexions depuis le réseau interne, l'application Citrix Workspace pour HTML5 permet d'accéder uniquement aux ressources fournies par des produits spécifiques. En outre, des versions spécifiques de Citrix 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](#).

Sauf indication contraire, les dernières versions de navigateur sont recommandées.

- Navigateurs
  - Microsoft Edge
  - Internet Explorer 11
  - Safari 11
  - Google Chrome
  - Mozilla Firefox
- Systèmes d'exploitation
  - 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 10.13 High Sierra
  - Mac OS X 10.12 Sierra

- Mac OS X 10.10 Yosemite
- Mac OS X 10.9 Mavericks
- Mac OS X 10.8 Mountain Lion
- Google Chrome OS 48
- Google Chrome OS 47
- Ubuntu 16.04 (32 bits)
- Ubuntu 12.04 (32 bits)

### **Configuration requise pour accéder aux magasins via des sites Desktop Appliance**

Les combinaisons Citrix Receiver (appelé désormais application Citrix Workspace), 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 Citrix Gateway ne sont pas prises en charge.

- Citrix Receiver pour Windows 4.9 et versions ultérieures, et application Citrix Workspace 1808 pour Windows et versions ultérieures
  - 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)

### **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. Les connexions établies via Citrix 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, et l'application Citrix Workspace 1808 pour Windows et versions ultérieures, 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 Citrix Virtual Apps and Desktops et <http://www.citrix.com/ready>.

### **Configuration requise pour l'authentification via Citrix Gateway**

Les versions suivantes de Citrix 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.

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.x
- NetScaler Gateway 10.5

## **Planifier votre déploiement StoreFront**

February 26, 2019

### **Remarque :**

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

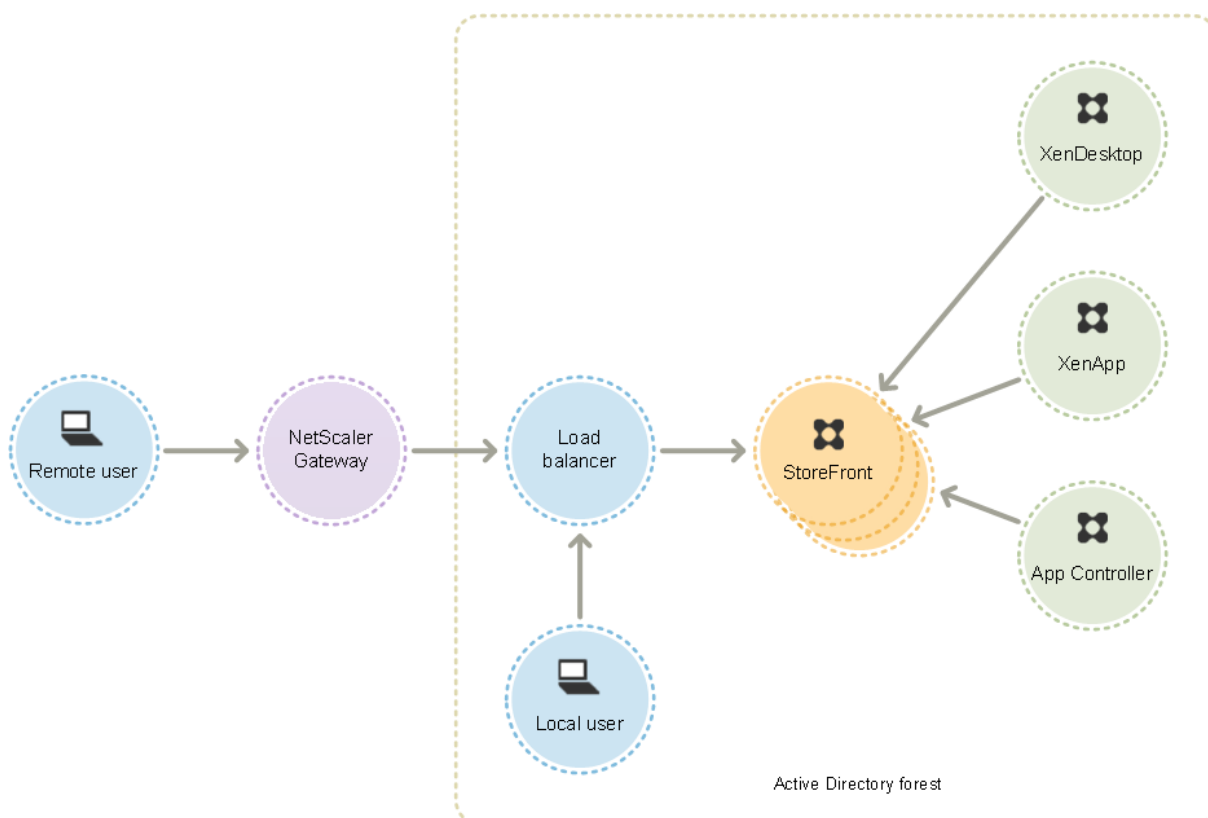
StoreFront fait appel à la technologie Microsoft .NET exécutée sur Microsoft Internet Information Services (IIS) pour fournir des magasins d'applications d'entreprise qui regroupent les ressources et les mettent à la disposition des utilisateurs. StoreFront s'intègre à vos déploiements XenDesktop, XenApp 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 présente un déploiement StoreFront classique.



## 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 <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 **Set-STFWebReceiverCommunication**.

Syntaxe :

```
1 Set-STFWebReceiverCommunication [-WebReceiverService] <
   WebReceiverService> [[-Loopback] <On | Off | OnUsingHttp>] [[-
```

```
LoopbackPortUsingHttp] <Int32>]
```

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 :

```
1 $wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
2 Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback
   OnUsingHttp -LoopbackPortUsingHttp 81
```

**Remarque :**

Désactivez 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 sites 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. Dans le cadre d'une activité simulée où les utilisateurs ouvrent une session, énumérez 100 applications publiées et démarrez une ressource ; un serveur StoreFront unique avec la spécification minimum recommandée de deux processeurs virtuels exécutés sur un serveur à double processeur Intel Xeon L5520 2.27 Ghz 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

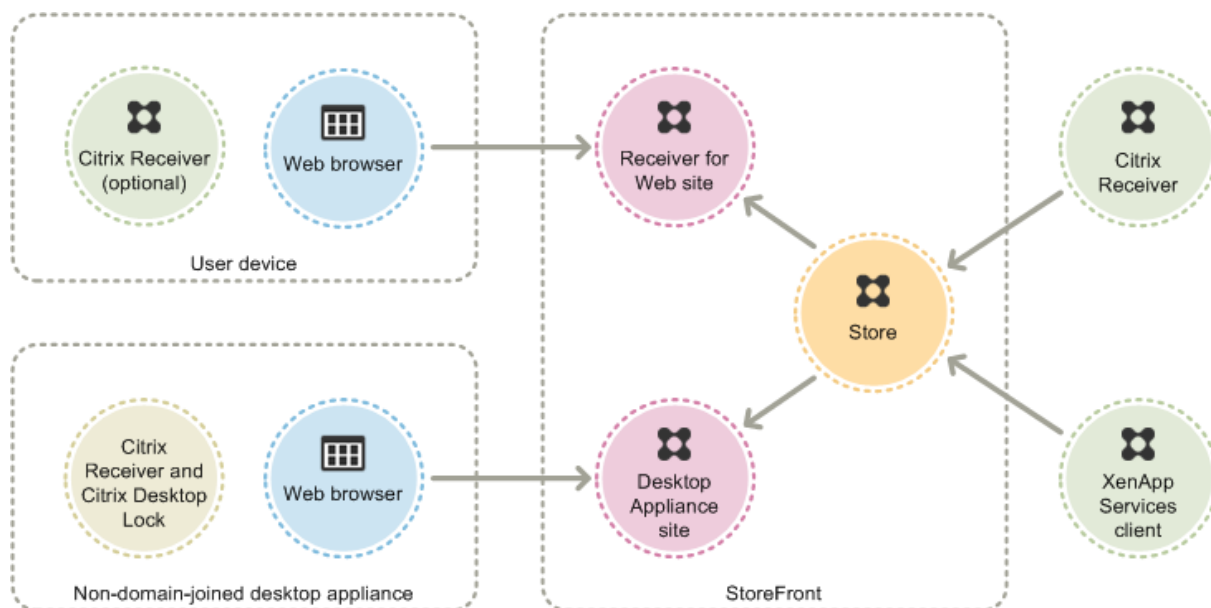
February 26, 2019

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 configu-

ration 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 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 plus d'informations, consultez la section [Exporter les 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. 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 ou 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 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. [\[ \]\(/en-us/netScaler-gateway/12-1/storefront-integration/ng-clg-session-policies-overview-con/ng-clg-storefront-policies-con/ng-clg-storefront-email-discovery-tsk.html\)](https://en-us/netScaler-gateway/12-1/storefront-integration/ng-clg-session-policies-overview-con/ng-clg-storefront-policies-con/ng-clg-storefront-email-discovery-tsk.html)

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**, 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 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 utilis-



teurs 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. Pour plus d'informations, veuillez consulter l'article <http://support.citrix.com/article/CTX123610>.

### **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 de 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]://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. 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

February 26, 2019

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.

Exigences :

- 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)
  - 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. Vous pouvez activer l'authentification pass-through au domaine 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 pour Internet Explorer, Edge, Mozilla Firefox et Google Chrome sur les machines client Windows jointes à un domaine.

### Pour activer l'authentification pass-through au domaine

1. Installez Citrix Receiver pour Windows ou Online Plug-in pour Windows sur les machines utilisateur. Assurez-vous que l'authentification pass-through est activée.
2. Dans le nœud du site Citrix Receiver pour Web dans la console d'administration, activez l'authentification pass-through au domaine.

3. Configurez SSON sur Citrix Receiver pour Windows, comme décrit dans [Configurer l'authentification pass-through au domaine](#). Citrix Receiver pour HTML5 ne prend pas en charge l'authentification pass-through au domaine.
4. Le comportement par défaut de Windows est « Connexion automatique uniquement dans la zone Intranet » Pour Internet Explorer, Mozilla Firefox et Google Chrome, configurez vos sites Citrix Receiver pour Web en tant que sites Intranet à l'aide des options Internet, ou activez la connexion automatique pour la zone approuvée. Pour Edge, vous devez configurer vos sites Citrix Receiver pour Web en tant que sites Intranet.
5. Pour Mozilla Firefox, modifiez les paramètres avancés du navigateur pour faire confiance à l'URI de Citrix Receiver pour Windows.

Attention :

la modification incorrecte des paramètres avancés peut entraîner de graves problèmes. Apportez des modifications à vos risques et périls.

- a) Démarrez Firefox, entrez **about:config** dans le champ d'adresse et sélectionnez « Je prends le risque ».
- b) Tapez **ntlm** dans la zone de recherche.
- c) Double-cliquez sur « network.automatic-ntlm-auth.trusted-uris » et tapez l'URL du site Citrix Receiver pour Windows dans le menu contextuel.
- d) Cliquez sur **OK**.

## 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 se connectent à NetScaler Gateway à l'aide de codes d'accès dérivés de codes de jetons générés par des jetons de sécurité combinés, dans certains cas, à 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 le type de connexion sur Domaine et jeton de sécurité. Pour plus d'informations, veuillez consulter <http://support.citrix.com/article/CTX125364>



Pour activer l'authentification multi-domaines via NetScaler Gateway vers StoreFront, définissez l'attribut de nom SSO 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 rationaliser le processus de connexion de vos utilisateurs tout en renforçant la sécurité de l'accès des utilisateurs à 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.

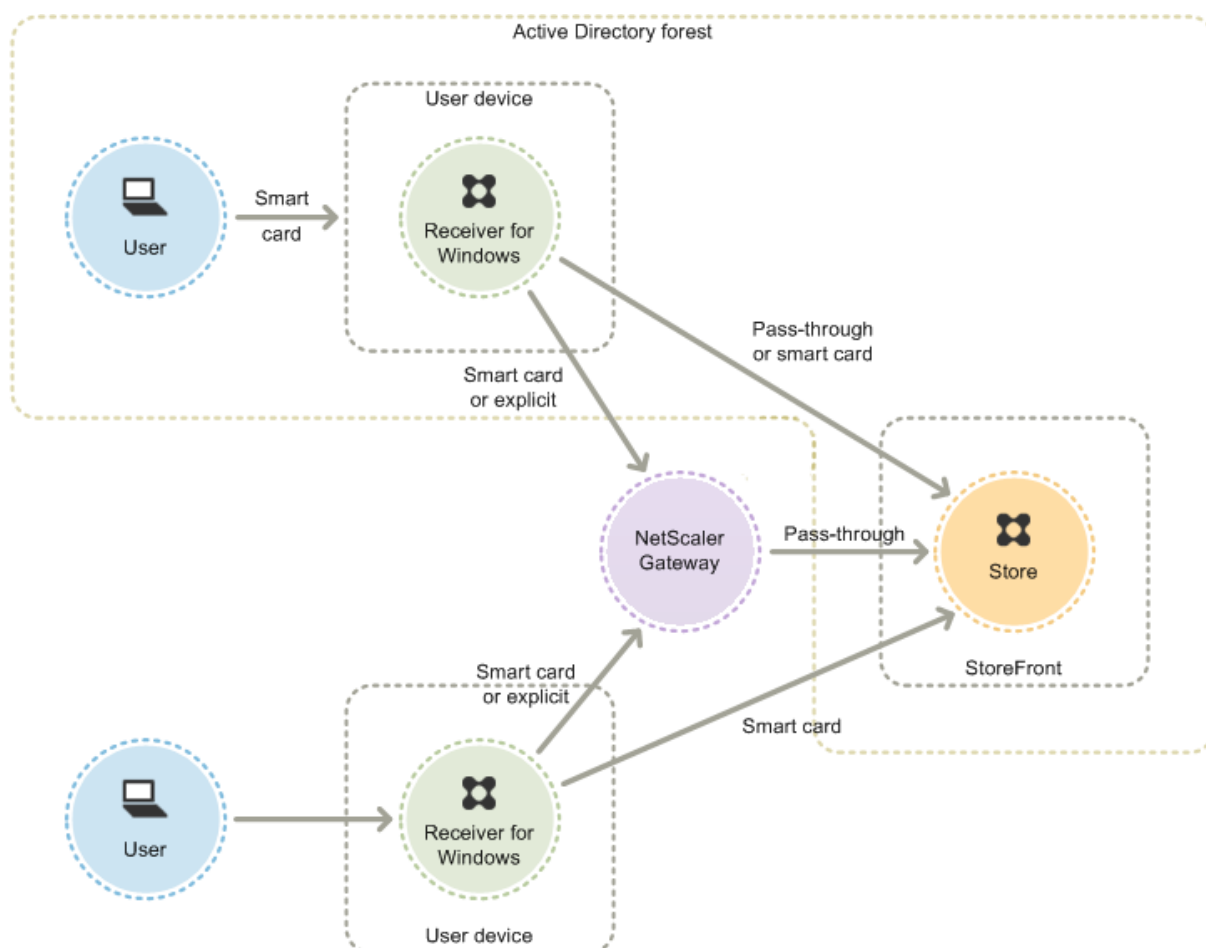
Pour activer l'authentification par carte à puce, les comptes des utilisateurs doivent être configurés au sein du domaine Microsoft Active Directory contenant les serveurs StoreFront ou au sein d'un domaine doté d'une relation d'approbation bidirectionnelle directe avec le domaine du serveur StoreFront. 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 :**

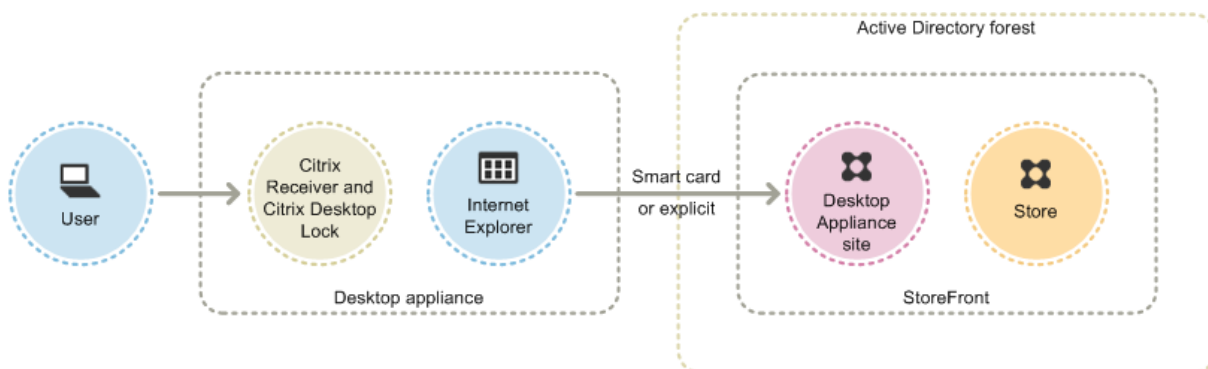
Si vous utilisez Citrix Receiver pour Windows 4.5 ou une version supérieure, vous pouvez configurer un autre vServer et utiliser la fonctionnalité de routage vers une passerelle optimale pour supprimer les invites de saisie du code PIN lors du démarrage d'applications et de bureaux.

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 l'authentification par carte à puce à partir d'un boîtier de bureau non lié à un domaine.



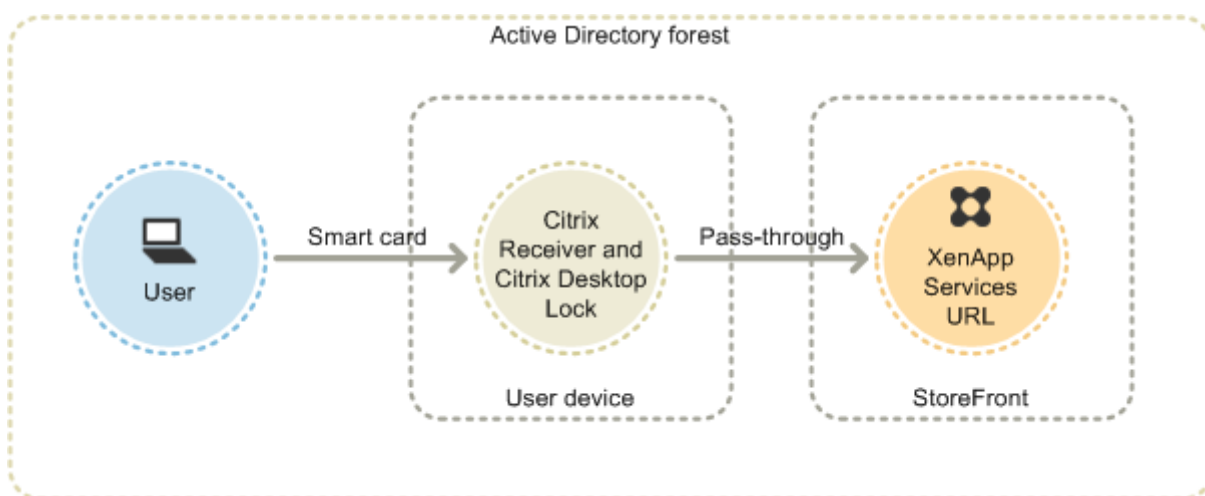
Lorsque les utilisateurs accèdent à leurs boîtiers de bureau, Internet Explorer démarre en mode plein écran et affiche l'écran de connexion d'un site Desktop Appliance. Les utilisateurs doivent s'authentifier sur le site à l'aide de leurs cartes à puce et codes PIN. Si le site Desktop Appliance est configuré 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 l'authentification par carte à puce à partir d'un périphérique lié 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 plus invités à entrer leur code PIN.

### 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.

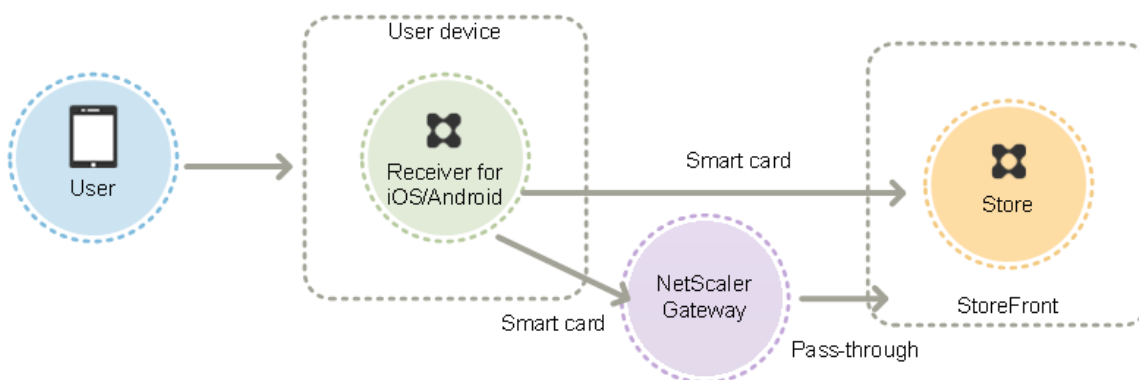
Si vous activez l'authentification pass-through avec carte à puce à XenDesktop et XenApp pour les utilisateurs Citrix Receiver pour Windows équipés de machines appartenant à un domaine qui n'accèdent pas aux magasins via NetScaler Gateway, ce paramètre s'applique à tous les utilisateurs du magasin. Pour 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'acquérir 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 [Configurer l'authentification par carte à puce](#) et pour obtenir des instructions sur l'utilisation des cartes à puce, consultez 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 util-

isateurs 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.

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

February 20, 2019

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 en fonction de leur type ou créer des dossiers pour différents rôles d'utilisateur dans 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, 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 [Configuration de la mise à disposition d'applications](#).
- Dans XenApp et XenDesktop 7.17, lorsque les utilisateurs lancent une application publiée depuis un bureau publié, les administrateurs peuvent contrôler si l'application est lancée dans cette session de bureau ou en tant qu'application publiée dans le même groupe de mise à disposi-

tion. Utilisez une applet de commande PowerShell sur le Broker Service et un paramètre de stratégie dans Citrix Receiver pour Windows (vPrefer) pour contrôler ce comportement. Cette fonctionnalité fonctionne uniquement avec les lancements d'applications publiées à partir de Citrix Receiver pour Windows. Elle ne peut pas être utilisée pour lancer une application localement si l'application publiée est lancée via le site StoreFront dans un navigateur Web. Dans les versions précédentes, le contrôle du lancement d'une application « double-hop » nécessitait l'utilisation de la balise `KEYWORDS:Prefer` dans Studio. La balise `KEYWORDS:Prefer` peut toujours être utilisée. Si les deux méthodes `KEYWORDS` et `vPrefer` ont été configurées, `vPrefer` a la priorité.

Pour plus d'informations, consultez l'article [CTX232210](#), l'article [Applications](#) dans XenApp et XenDesktop et la documentation de [Citrix Receiver pour Windows](#).

## Haute disponibilité et configuration multisite de StoreFront

October 4, 2018

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 multi-site 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

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

### 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.

### Important :

- 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 Framework, qui peut être téléchargé depuis Microsoft. Microsoft.NET 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](#).

- a) Assurez-vous que l'équilibrage de charge est activé sur votre boîtier NetScaler.
- b) 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.
- c) 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.

- d) Créez un serveur virtuel et liez les services au serveur virtuel.
- e) 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 > .NET Framework, ASP.NET

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

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 plus d'informations sur la création d'un certificat de serveur dans IIS, consultez [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637\(v=ws.11\)#create-certificate-wizard](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard). Pour plus d'informations sur l'ajout de la liaison HTTPS à un site IIS, consultez [https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11)).

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 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.

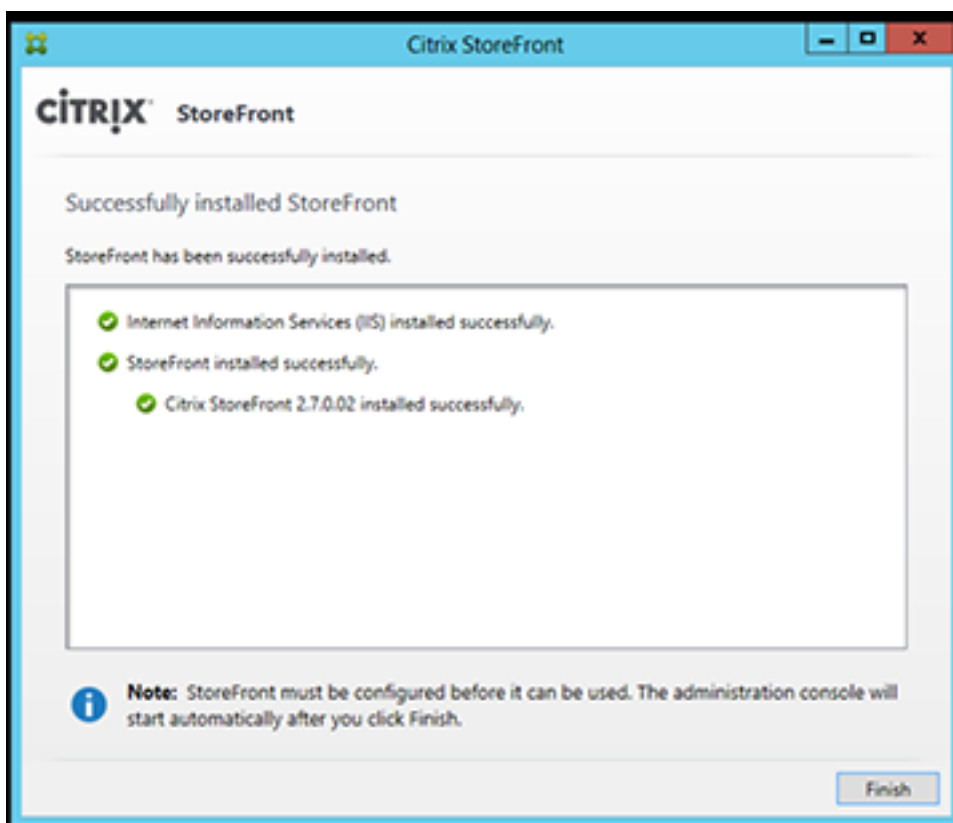
5. Lisez et acceptez le contrat de licence, puis cliquez sur Suivant.
6. Si la page Vérifier les composants requis s'affiche, cliquez sur Suivant.
7. Sur la page Prêt pour l'installation, vérifiez que les trois composants de StoreFront sont répertoriés pour l'installation et cliquez sur Installer.

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
- 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 > .NET Framework, ASP.NET
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 Citrix StoreFront, cliquez sur Créer un nouveau déploiement.
  - a) Spécifiez l'URL du serveur StoreFront dans la zone **URL de base**.
  - b) Sur la page **Nom du magasin**, spécifiez un nom pour votre magasin, puis cliquez sur Suivant.

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.

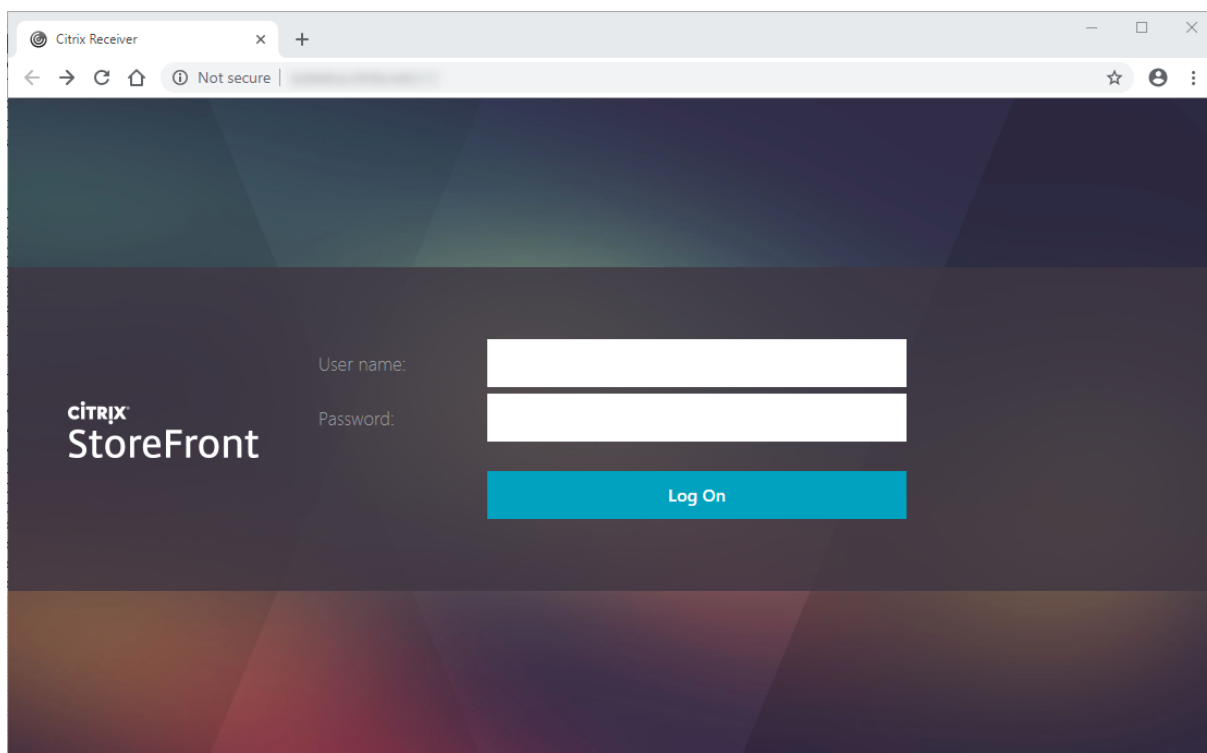
1. Définissez le **type de transport** et le **port**. Vous pouvez spécifier le protocole HTTP et le port 443 ; cliquez ensuite sur **OK**. Vous pouvez également copier les paramètres d'un déploiement existant de l'Interface Web ou de StoreFront.
2. Sur la page **Accès distant**, sélectionnez Aucun. Si vous utilisez NetScaler Gateway, sélectionnez Aucun tunnel VPN et entrez les détails de votre passerelle.
3. 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 Citrix Receiver pour Web du nouveau magasin s'affiche. Par exemple : [example.net/Citrix/MarketingWeb/](http://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) :

- 1 Emplacement : HKLM:\Software\Citrix\Telemetry\CEIP
- 2 Nom : Enabled
- 3 Type : REG\_DWORD
- 4 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 :

```
1 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'applique 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 ».

Données	Description
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

1. Ouvrez une session sur le serveur StoreFront en utilisant un compte disposant d'autorisations d'administrateur local.
2. Assurez-vous que toutes les exigences requises pour l'installation de StoreFront sont remplies avant d'installer StoreFront. Référez-vous à [Avant l'installation et la configuration](#) pour plus de détails.
3. Accédez à votre support d'installation ou votre package de téléchargement, recherchez CitrixStoreFront-x64.exe et copiez le fichier dans un emplacement temporaire sur le serveur.
4. Depuis une invite de commandes, accédez au dossier contenant le fichier d'installation, puis saisissez la commande suivante.

```
1 CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR  
installationlocation] [-WINDOWS_CLIENT filelocation\filename.  
exe] [-MAC_CLIENT filelocation\filename.dmg]
```

Utilisez l'argument **-silent** pour effectuer une installation silencieuse de StoreFront et de tous les logiciels requis. 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 OSX, 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 plus d'informations, consultez la section [Configurer la manière dont les ressources s'affichent auprès des utilisateurs](#).

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

### Remarque :

Si vous avez personnalisé l'expérience unifiée, vos personnalisations sont préservées lorsque vous effectuez une mise à niveau vers cette version de StoreFront. Vérifiez que l'apparence de vos personnalisations est toujours adaptée à la nouvelle expérience unifiée. Nous vous recommandons d'informer les utilisateurs des changements de l'expérience unifiée apportés par cette mise à niveau, décrits dans [Expérience utilisateur unifiée Citrix Receiver](#).

Pour mettre à niveau des déploiements 3.x vers cette version de StoreFront, exécutez le fichier d'installation pour cette version de StoreFront.

La mise à niveau vers la dernière version Current Release à partir d'une version Current Release plus ancienne qui est maintenant en fin de vie n'est pas prise en charge. Pour plus d'informations, voir [CTX200356](#).

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 :

- 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 3.x vers cette version de StoreFront**

1. 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.
2. Sauvegardez tous les serveurs dans le groupe de serveurs.
3. Retirez l'un des serveurs du groupe de serveurs existant.
4. Redémarrez le serveur que vous avez retiré.

Veillez 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.

**Remarque :**

- 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.
- Enregistrez les sauvegardes du fichier web.config dans un emplacement **différent** du répertoire IIS par défaut du magasin. N'enregistrez pas les sauvegardes dans l'emplacement `C:\inetpub\wwwroot\citrix\<storename>` par exemple. L'enregistrement des sauvegardes dans le même emplacement que le répertoire IIS par défaut du magasin peut interférer avec la mise à niveau de StoreFront.

## 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 la vignette **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 StoreFront**, cliquez sur **Oui**. Une fois la désinstallation terminée, cliquez sur **OK**.

## Créer un nouveau déploiement

February 20, 2019

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 volet de résultats de la console de gestion 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 les instructions décrites dans [Ajouter des ressources XenDesktop et XenApp au magasin](#). Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison des déploiements XenDesktop et XenApp. Répétez les procédures, si nécessaire, pour ajouter tous les déploiements fournissant des ressources 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 utilisateurs à accéder uniquement aux ressources délivrées via StoreFront (sans 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, suivez la procédure décrite dans [Fournir l'accès distant au magasin via un boîtier NetScaler Gateway](#). Répétez les procédures, si nécessaire, pour ajouter d'autres déploiements.
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 **Next**.
11. Sur la page **Méthodes d'authentification**, sélectionnez les méthodes que les utilisateurs utiliseront pour s'authentifier au magasin, puis 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 lors de sa création 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 une connexion HTTP sécurisée à l'aide du protocole 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. 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) pour 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.

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, 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 tokencode 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 tokencode 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 Next.

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 Next.

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 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

October 4, 2018

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 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 Citrix StoreFront, cliquez sur **Joindre un groupe de serveurs existant**.
3. Connectez-vous à 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 décon-



necté, vous pouvez de nouveau ajouter le serveur à un groupe de serveurs existant ou à un groupe différent de serveurs nouvellement créé.

1. Ouvrez la console d'administration StoreFront sur le serveur StoreFront principal que vous utilisez pour gérer l'ensemble de votre groupe de serveurs.
2. Sélectionnez le nœud du groupe de serveurs dans le volet gauche et choisissez un autre serveur à supprimer.
3. Supprimez le serveur sélectionné du groupe de serveurs.
4. Dans le volet Actions, propagez les modifications depuis le 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\Receiver StoreFront\Scripts\ImportModules.ps1 "
7. Exécutez la commande **Clear-DSCconfiguration**, qui restaure les paramètres par défaut du serveur.
8. Ouvrez la console d'administration StoreFront et le serveur déconnecté est réinitialisé et prêt à être ajouté à un autre groupe de serveurs.

## Migrer les fonctionnalités de l'Interface Web vers StoreFront

February 20, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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
<b>Personnalisation avec la console de gestion</b>	
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.
Activer la recherche, Désactiver la recherche	La recherche est activée par défaut. <b>Pour désactiver les zones de recherche sur le bureau ou l'interface Web</b> , ajoutez le style suivant au fichier style.css : <code>.search-container { display: none; }</code> . <b>Pour désactiver les zones de recherche sur l'interface utilisateur du téléphone</b> , ajoutez le style suivant au fichier style.css : <code>##searchBtnPhone { display: none; }</code> .
Activer l'actualisation	Activée par défaut (actualisation du navigateur).

Fonctionnalité de l'Interface Web	Équivalent StoreFront
Activer le retour au dernier dossier	<p>Non activé par défaut. Pour mémoriser le dossier actuel et y retourner au moment du chargement, ajoutez la ligne suivante au fichier <code>script.js</code> : <code>CTXS.Extensions</code>.</p> <pre>afterDisplayHomeScreen = function (){ //check if view was saved last time CTXS.ExtensionAPI. localStorage.getItem("view", function (view){ if (view){ // if view was saved, change to it CTXS. ExtensionAPI.changeView(view); } if (view == "store"){ // if view is store, see if folder was saved CTXS .ExtensionAPI.localStorage.getItem(" folder", function(folder){ if ( folder != ""){ // if folder was saved, change to it CTXS. ExtensionAPI.navigateToFolder( folder); } } ); } // set up monitoring of folder CTXS. Extensions.onFolderChange = function(folder){ CTXS.ExtensionAPI .localStorage.setItem("folder", folder); } ; // set up monitoring of view CTXS.Extensions. onViewChange = function(newview){ // don' t retain search or appinfo views // instead, remember parent view. if ((newview != "appinfo")&amp;&amp; (newview != "search")){ CTXS. ExtensionAPI.localStorage.setItem( " view", newview); } } ; } ); } ;</pre>
Activer les conseils	<p>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.</p>

Fonctionnalité de l'Interface Web	Équivalent StoreFront
Affichage Icônes, Affichage Arborescence, Affichage Détails, Affichage Liste, Affichage Groupe, Définir l'affichage par défaut, Affichage Icônes (Graphiques simplifiés), Affichage Liste (Graphiques simplifiés), Affichage par défaut (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 <a href="#">Spécifier différentes vues pour les applications et bureaux</a> .
Interface utilisateur à onglet unique, Interface utilisateur à plusieurs onglets (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 <b>Favori</b> (facultatif).
Logo d'en-tête, Couleur du texte, Couleur d'arrière-plan de l'en-tête, Image d'arrière-plan de l'en-tête	Équivalents pour les couleurs et logos à l'aide de la console d'administration StoreFront. Cliquez sur <b>Personnaliser l'apparence du site Web</b> dans le panneau <b>Actions</b> de la console d'administration StoreFront et apportez les modifications sur l'écran qui s'affiche. Vous pouvez définir une image d'arrière-plan pour l'en-tête en utilisant la personnalisation de style. Par exemple <pre>.theme-header-bgcolor { background-image: url('spirals.png'); }</pre>

---

**Fonctionnalité de l'Interface Web****Équivalent StoreFront**

---

Message de bienvenue de pré-ouverture de session (Pré-localisation) (Titre, Texte, Hyperlien, Libellé du bouton)

Par défaut, il n'existe aucun autre écran de pré-ouverture de session. Cet exemple de script ajoute une zone de message interactive :

```
var doneClickThrough = false; //
Before web login CTXS.Extensions.
beforeLogon = function (callback){
doneClickThrough = true; CTXS.
ExtensionAPI.showMessage({
messageTitle: "Welcome!",
messageText: "Only for \<a href="
http://www.WWc.com" target="_blank
">WWCo Employees", okButtonText: "
Accept", okAction: callback } ); }
; // Before main screen (for native
clients)CTXS.Extensions.
beforeDisplayHomeScreen = function
(callback){ if (!doneClickThrough){
CTXS.ExtensionAPI.showMessage({
messageTitle: "Welcome!",
messageText: "Only for WWCo
Employees", okButtonText: "Accept",
okAction: callback } ); } else {
callback(); } } ;
```

Fonctionnalité de l'Interface Web	Équivalent StoreFront
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: 16 px; } Exemple de script (contenu statique) : \\$(''.customAuthHeader'').html(" Welcome to ACME"); Exemple de script (contenu dynamique) : function setDynamicContent(txtFile, element) { CTXS.ExtensionAPI.proxyRequest({ url: "customweb/"+txtFile, success: function(txt){ \\$(element).html( txt); } } ); } setDynamicContent(" Message.txt", ".customAuthTop");</pre> <p><b>Remarque :</b> il ne faut pas explicitement inclure de contenu dynamique dans le script, ou le placer dans le répertoire <b>personnalisé</b>, car les modifications effectuées ici forcent les clients à recharger l'interface utilisateur. Placez le contenu dynamique dans le répertoire <b>customweb</b>.</p>
Message de bienvenue de l'écran d'application, Message système de l'écran d'application	<p>Consultez les exemples d'écran de bienvenue <b>CustomAuth</b> ci-dessus. Consultez les exemples de contenu dynamique ci-dessus. Utilisez <code>##customTop</code> plutôt que <code>.customAuthTop</code> 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; } ** Example <b>static</b> content using a script: **\\$(''.##customBottom''). html("Welcome to ACME");</pre>

---

Fonctionnalité de l'Interface Web	Équivalent StoreFront
-----------------------------------	-----------------------

---

### Fonctionnalités avec aucun équivalent direct

Écran d'ouverture de session sans en-têtes, Écran d'ouverture de session avec en-têtes (y compris des messages)	Il n'existe pas d'équivalent direct dans StoreFront. Toutefois, vous pouvez créer des en-têtes personnalisés. Consultez la section <i>Titre de l'écran d'ouverture de session</i> ci-dessus.
---	--

Paramètres utilisateur	Par défaut, il n'existe aucun paramètre utilisateur. Vous pouvez ajouter des menus et boutons JavaScript.
------------------------	---

Le contrôle de l'espace de travail	Fonctionnalité équivalente pour les paramètres d'administrateur. Les API d'extension permettent une plus grande flexibilité. Veuillez consulter la section <a href="http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html">http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html</a> .
------------------------------------	--

### Personnalisations avancées (code)

Hooks de génération du fichier ICA et autres personnalisations de routage d'appel	API équivalentes ou supérieures. <a href="http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html">http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html</a>
---	--

Personnalisations d'authentification	API équivalentes ou supérieures. <a href="http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html">http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html</a>
--------------------------------------	--

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

January 17, 2019

**Remarque :**

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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 plus d'informations sur la création d'un certificat de serveur dans IIS, consultez [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637\(v=ws.11\)#create-certificate-wizard](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard). Pour plus d'informations sur l'ajout de la liaison HTTPS à un site IIS, consultez [https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11)).

## 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** si 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**, puis 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 une heure, en minutes, pendant laquelle un Delivery Controller est considéré comme hors ligne après la défaillance de tous ses serveurs.
5. Sur la ligne **Durée de l'état hors ligne**, cliquez dans la deuxième colonne et entrez une heure, en minutes, pendant laquelle un seul serveur est considéré comme hors ligne après une défaillance.

## **Configurer l'authentification et la délégation**

September 21, 2018

**Remarque :**

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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.

---

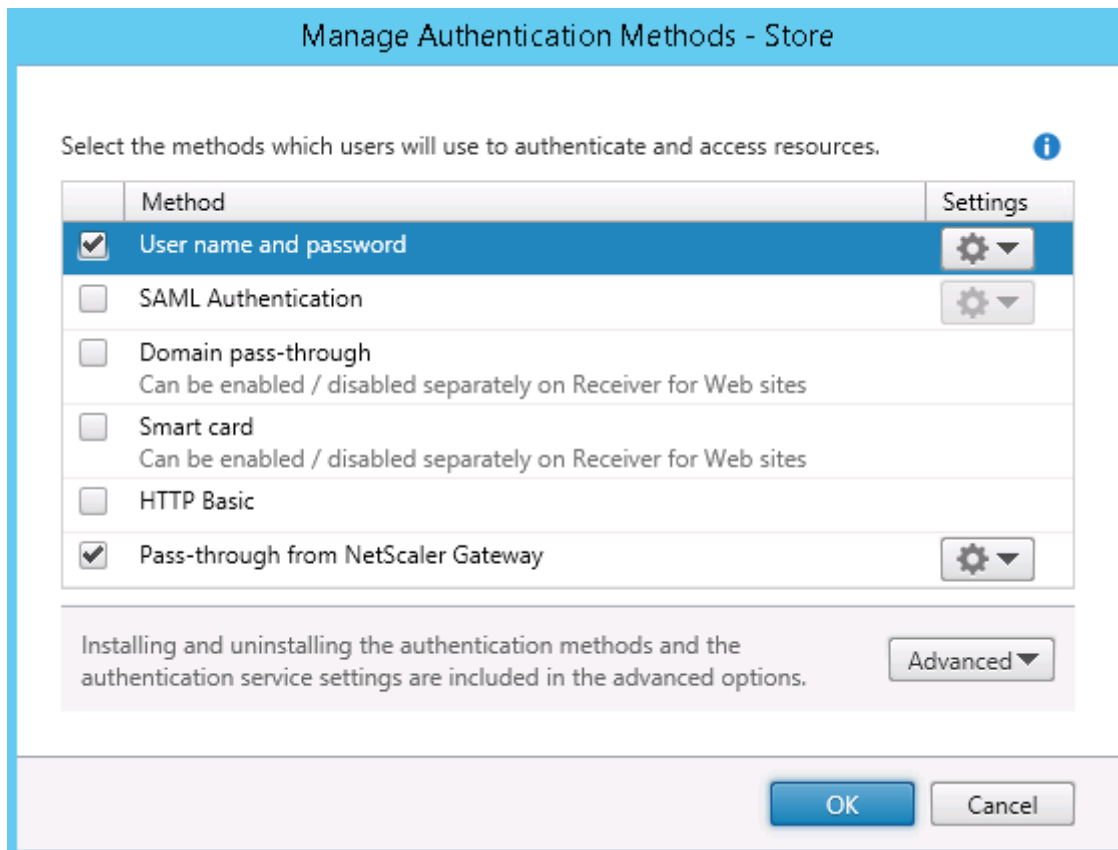
## Configurer le service d'authentification

February 26, 2019

### Gérer les 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 automa-

tiquement 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. Dans le panneau gauche de la console de gestion Citrix StoreFront, dans le panneau Actions, sélectionnez le nœud **Magasins** et 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 permettre aux utilisateurs de modifier leurs mots de passe uniquement lorsque les mots de passe ont déjà expiré, sélectionnez **À expiration uniquement**. Les utilisateurs qui ne peuvent pas se connecter car leurs mots de passe ont expiré sont redirigés vers la boîte de dialogue Modifier le mot de passe [ ] (/fr-fr/storefront/current-release/configure-authentication-and-delegation/password-expiry.html). Pris en charge pour les Citrix Receiver de bureau et Citrix Receiver pour Web.
  - Pour empêcher les utilisateurs de modifier leurs mots de passe, ne sélectionnez pas **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.

	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
Citrix Receiver			
Windows	Oui		
Mac	Oui		
Android			
iOS			
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 `username@domain.com`.

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

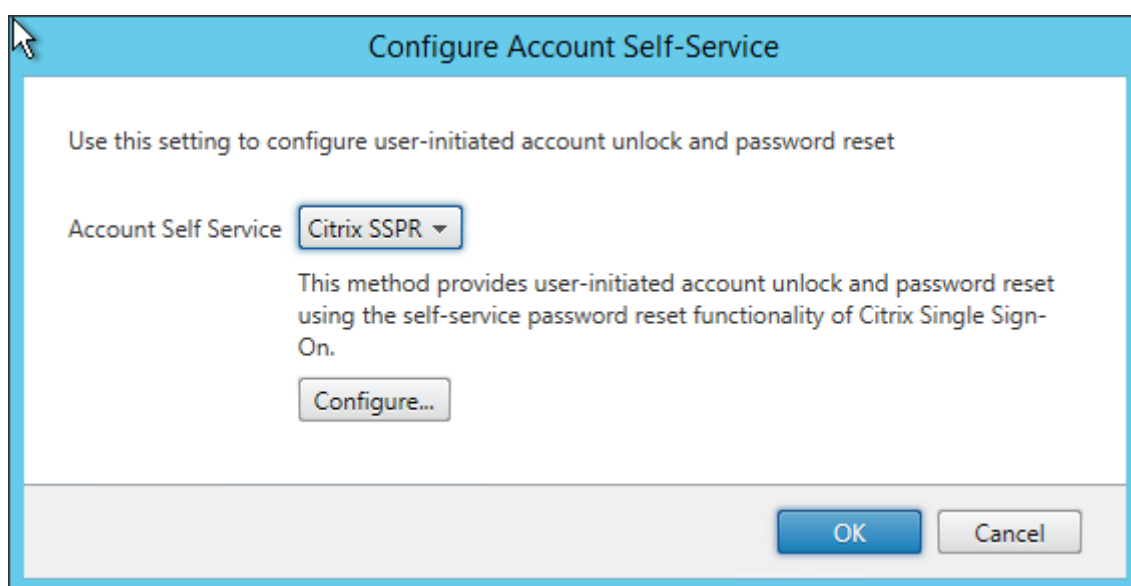
- Le magasin est configuré pour utiliser l'authentification par nom d'utilisateur et mot de passe.



- 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](#).

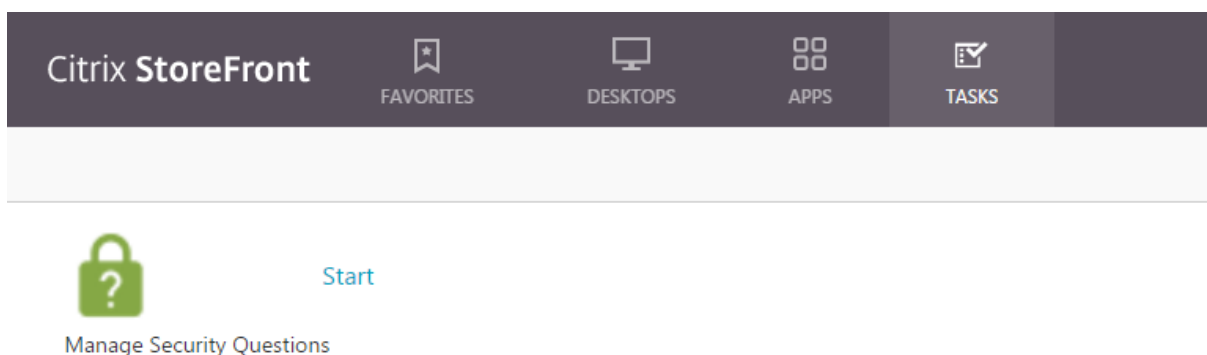
1. Activez la prise en charge de la fonction de réinitialisation en libre-service des mots de passe dans StoreFront en sélectionnant le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification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

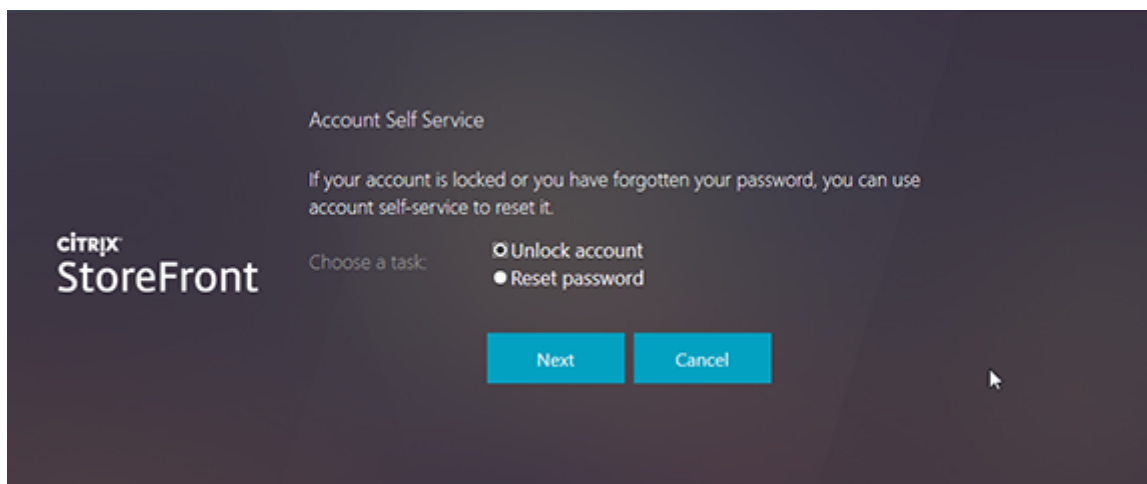


Une fois configurés dans StoreFront, les utilisateurs voient le lien **Compte en libre-service** sur l'écran de connexion Citrix Receiver pour Web (il s'affiche sous la forme d'un bouton dans d'autres Citrix Receiver).

En cliquant sur ce lien, l'utilisateur passe par une série de formulaires pour choisir d'abord entre **Déverrouiller le compte** et **Réinitialiser le mot de passe** (si les deux sont 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 `username@domain.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'y a pas de différence fonctionnelle 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

October 4, 2018

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

October 4, 2018

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 :

**Attention :**

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.

Pour les ordinateurs 32 bits : HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integra

Nom : SSONCheckEnabled

Type : REG\_SZ

Valeur : true ou false



Pour les ordinateurs 64 bits : HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerF  
Nom : SSONCheckEnabled  
Type : REG\_SZ  
Valeur : true ou false

## Configuration de l'authentification par carte à puce

February 26, 2019

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.

Le document [Configuration des cartes à puce pour les environnements Citrix](#) décrit comment configurer un déploiement Citrix pour les cartes à puce à l'aide d'un type de carte à puce spécifique. Des étapes similaires s'appliquent aux cartes à puce d'autres fournisseurs.

### 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.

- Sur votre boîtier NetScaler Gateway, installez 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 plus d'informations, voir [Configuration et liaison d'une stratégie d'authentification de 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 plus d'informations sur la création d'un certificat de serveur dans IIS, consultez [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637\(v=ws.11\)#create-certificate-wizard](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard). Pour plus d'informations sur l'ajout de la liaison HTTPS à un site IIS, consultez [https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11)).

- 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.

- 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 plus d'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 des stratégies de groupe pour importer le fichier de modèle d'objet de stratégie de groupe Receiver pour Windows, icaclient.adm, sur le contrôleur du 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 default.ica pour le magasin.

### 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 les modifications terminées, [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 default.ica du magasin, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\nommagasin\App\_Data\, où nommagasin désigne le nom attribué au magasin au moment de sa création.
2. Pour activer les informations d'identification des cartes à puce pour les utilisateurs qui accèdent aux 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 permettre la transmission des informations d'identification de la carte à puce pour les utilisateurs accédant aux magasins via NetScaler Gateway, ajoutez le paramètre suivant dans la section [Application].

`UseLocalUserAndPassword=0n`

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

October 4, 2018

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

September 21, 2018

**Remarque :**

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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.

---

<a href="#">Créer ou supprimer un magasin</a>	Permet de configurer autant de magasins supplémentaires que vous le souhaitez.
<a href="#">Créer un magasin non authentifié</a>	Permet de configurer des magasins non authentifiés supplémentaires afin de permettre l'accès des utilisateurs non authentifiés (anonymes).
<a href="#">Exporter des fichiers de provisioning de magasin pour des utilisateurs</a>	Permet de générer des fichiers contenant les détails de connexion aux magasins, y compris tout déploiement NetScaler Gateway et balise configurés pour les magasins.
<a href="#">Masquer et publier des magasins pour les utilisateurs</a>	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.
<a href="#">Gérer les ressources mises à disposition dans les magasins</a>	Permet d'ajouter et de supprimer des ressources de magasins.
<a href="#">Gérer l'accès distant aux magasins via NetScaler Gateway</a>	Permet de configurer l'accès aux magasins via NetScaler Gateway pour les utilisateurs se connectant depuis des réseaux publics.



<a href="#">Intégrer des applications Citrix Online à des magasins</a>	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.
<a href="#">Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun</a>	Permet de configurer deux magasins StoreFront pour partager une base de données d'abonnement commune.
<a href="#">Paramètres de magasin avancés</a>	Configurez les paramètres avancés du magasin.

---

## Créer ou supprimer un magasin

February 26, 2019

Utilisez la tâche Créer un magasin pour configurer des magasins supplémentaires. 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 permettant un magasin anonyme ou non authentifié. 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 les modifications terminées, [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 une connexion HTTP sécurisée à l'aide du protocole 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. 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 tokencode 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 tokencode 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.

11. 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.
12. 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.
13. 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]://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 à l'étape 3.

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

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 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 qu'utilisera StoreFront 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 votre serveur.
  - Pour envoyer des données via une connexion HTTP sécurisée à l'aide du protocole 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 **Créer**.
14. Sur la page **Configurer les méthodes d'authentification**, sélectionnez les méthodes par lesquelles les utilisateurs s'authentifieront et accéderont aux ressources, puis 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, cliquez sur **Suivant**.
16. Sur la page **URL XenApp Services**, configurez l'adresse URL pour les utilisateurs qui utilisent PNAgent pour accéder aux applications et 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 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.

## Créer un magasin non authentifié

February 26, 2019

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 les modifications terminées,

[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 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.
- 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 lors de sa création 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

February 20, 2019

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 les modifications terminées,

[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 **Enregistrer** pour enregistrer le fichier de provisioning avec une extension .cr sur un emplacement approprié de votre réseau.

## Publier et masquer des magasins pour les utilisateurs

February 20, 2019

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 les modifications terminées,

[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 le magasin**.
3. Sur la page **Publier le magasin**, sélectionnez **Publier le magasin** ou **Masquer le magasin**.

## Gérer les ressources mises à disposition dans les magasins

February 26, 2019

Utilisez la tâche Gérer les Contrôler 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 les modifications terminées,

[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 serveurs 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 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.

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

February 26, 2019

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 les modifications terminées,

[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 d'accès distant**.
3. Dans la boîte de dialogue **Configurer les 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, 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 tokencode 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 tokencode 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 sur un serveur Access Controller faisant 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 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 Next.

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 in-

terrompues 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

October 4, 2018

### Remarque :

À partir de StoreFront 3.12, cette fonctionnalité ne peut pas être configurée dans la console de gestion StoreFront. Si vous mettez à niveau vers StoreFront 3.12, vous pouvez continuer à utiliser cette fonctionnalité. Pour modifier votre configuration, utilisez l'applet de commande PowerShell, Update-DSGenericApplications.

Pour plus d'informations sur la configuration de cette fonctionnalité dans les versions antérieures de la console de gestion StoreFront, consultez l'article *Intégrer des applications Citrix Online à des magasins* de la [documentation de StoreFront 3.11](#).

## Update-DSGenericApplications

### Name

Update-DSGenericApplications

### Synopsis

Met à jour les paramètres d'application génériques pour un service de magasin.

### Syntaxe

---

```
1 Update-DSGenericApplications [[-StoreServiceSiteId] <Int64>] [[-  
    StoreServiceVirtualPath] <String>] [[-GoToMeetingEnabled] <Boolean>]  
    [[-GoToMeetingDeliveryOption] <String>] [[-GoToWebinarEnabled] <  
Boolean>] [[-GoToWebinarDeliveryOption] <String>] [[-  
GoToTrainingEnabled] <Boolean>] [[-GoToTrainingDeliveryOption] <  
String>] [<CommonParameters>]
```

## Description

Applet de commande utilisée pour mettre à jour la fonctionnalité générique (Citrix Online) du service de magasin.

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

October 4, 2018

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 le scénario par défaut impliquant deux magasins et leurs magasins de données d'abonnement correspondants, un utilisateur doit s'abonner deux fois à la même ressource. 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<nommagasin>.
- Chaque magasin web.config contient un point de terminaison client pour le Subscription Store Service.

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<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 :

```
1 <subscriptionsStoreClient enabled="true">
2 <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
  __Citrix_External" authenticationMode="windows" transferMode="
  Streamed">
3 <clientCertificate thumbprint="0" />
4 </clientEndpoint>
5 </subscriptionsStoreClient>
```

2. Modifiez le paramètre externe pour qu'il corresponde au point de terminaison du magasin interne :

```
1 <subscriptionsStoreClient enabled="true">
```

```
2 <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
   __Citrix_Internal" authenticationMode="windows" transferMode="
   Streamed">
3 <clientCertificate thumbprint="0" />
4 </clientEndpoint>
5 </subscriptionsStoreClient>
```

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

October 4, 2018

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

### 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 au serveur. La valeur par défaut est DnsPort. Dans le menu déroulant **Type de résolution d'adresse** sous **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 Activé.

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 Activé.

Utilisez la tâche **Paramètres avancés**, cochez la case **Autoriser la reconnexion de sessions**, puis cliquez sur **OK** pour activer la reconnexion de 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 les secondes à attendre pour établir 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 **Activé**.

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

### **Activer le regroupement de sockets**

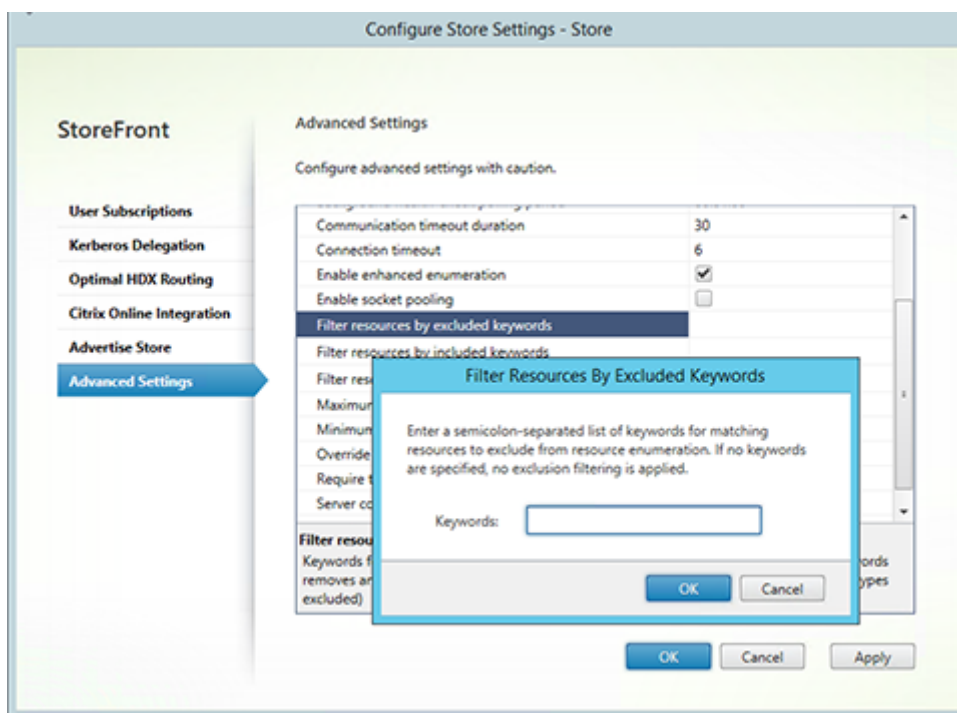
La mise en regroupement des sockets est désactivée par défaut dans les magasins. Lorsque le regroupement de sockets est activé, StoreFront conserve un groupe de sockets, au lieu de créer une socket chaque fois qu'elle en a besoin et de la renvoyer au système d'exploitation dès que la connexion est fermée. 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 Désactivé.

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 Activé.

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 Désactivé.

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

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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 :

Tâche	Détail
<a href="#">Créer un site Citrix Receiver pour Web</a>	Permet de créer des sites Receiver pour Web, ce qui permet aux utilisateurs d'accéder aux magasins via une page Web.
<a href="#">Configurer des sites Citrix Receiver pour Web</a>	Permet de modifier les paramètres de vos sites Receiver pour Web.

Tâche	Détail
<a href="#">Configurer la prise en charge de l'expérience Citrix Receiver unifiée</a>	StoreFront prend en charge les expériences utilisateur classique et unifiée. L'expérience unifiée offre une expérience utilisateur HTML5 gérée de façon centralisée.
<a href="#">Créer et gérer des applications recommandées</a>	Permet de créer des groupes d'applications recommandées pour des utilisateurs qui sont liés ou appartiennent à une certaine catégorie.
<a href="#">Configurer le contrôle de l'espace de travail</a>	Le contrôle de l'espace de travail permet aux applications de suivre les utilisateurs lorsqu'ils naviguent d'une machine à une autre.
<a href="#">Configurer l'utilisation des onglets de navigateur par Citrix Receiver pour HTML5</a>	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.
<a href="#">Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion</a>	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

February 26, 2019

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 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 les modifications terminées, [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 souhaitée dans la zone Chemin d'accès au 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

February 26, 2019

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 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 les modifications terminées, [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 **Magasins** 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 au-

tomatiquement 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 compat-

ible 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. Choisir **Déployer Citrix Receiver** et **Source pour Receiver**, puis accédez aux 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 vérifiez **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

February 20, 2019

Remarques :

- L'expérience unifiée n'est prise en charge que sur Internet Explorer 11. Consultez la section [Prise en charge d'Internet Explorer](#).
- StoreFront reste le nom utilisé pour le magasin d'applications d'entreprise qui regroupe les applications et les bureaux des sites Citrix Virtual Apps and Desktops en un seul magasin facile à utiliser pour les utilisateurs. La technologie Citrix Receiver fait désormais partie de l'application Citrix Workspace. La mise en œuvre de cette transition dans nos produits et notre documentation est toujours en cours. Les produits peuvent encore contenir d'anciens noms, par exemple l'expérience unifiée désigne « Citrix Receiver ». « Receiver pour Web » dans la console de gestion et dans la documentation continue de désigner l'accès Web sans client à StoreFront. Nous vous remercions de votre patience pendant cette transition. Pour plus d'informations sur les nouveaux noms, consultez la section <https://www.citrix.com/about/citrix-product-guide/>.

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. L'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 à 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. 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.

**Remarque :**

Si vous utilisez XenApp 6.x, les applications définies sur **Stream to client** ou **Streamed if possible, otherwise accessed from a server** ne sont pas prises en charge si 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.

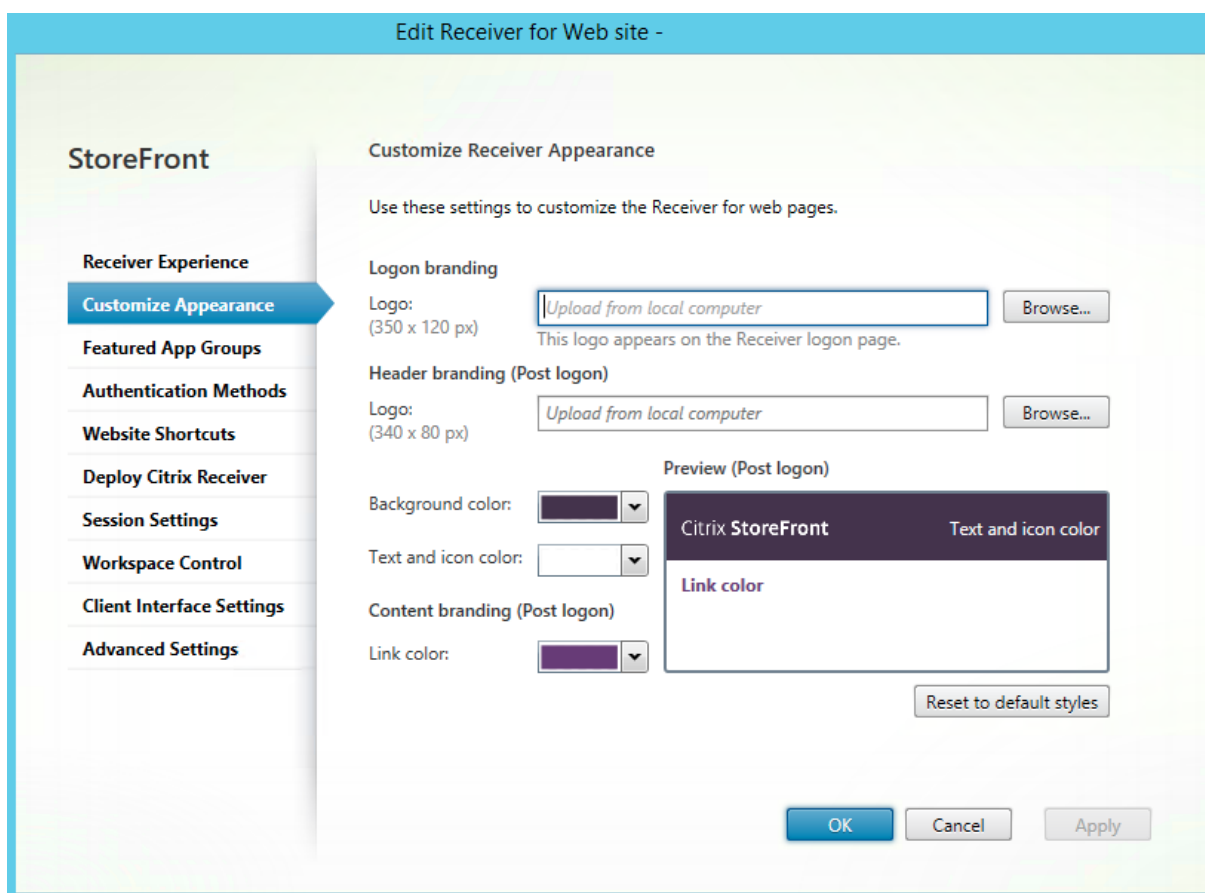
### Important :

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.



## Expérience utilisateur unifiée Citrix Receiver

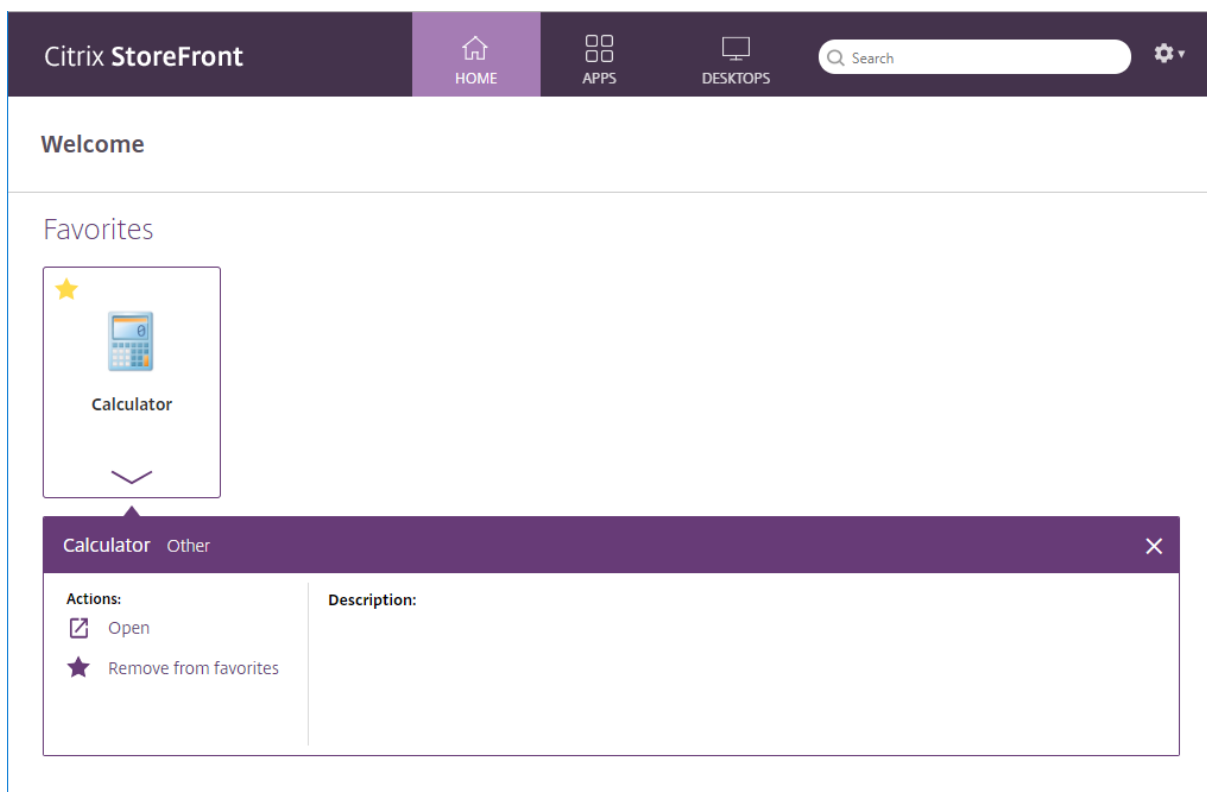
Cette section décrit les fonctionnalités et l'aspect de l'expérience unifiée.

### Disposition de la carte

Les applications du magasin sont représentées sous forme de cartes. Vous pouvez développer un panneau sous chaque carte pour afficher plus de détails et d'actions.

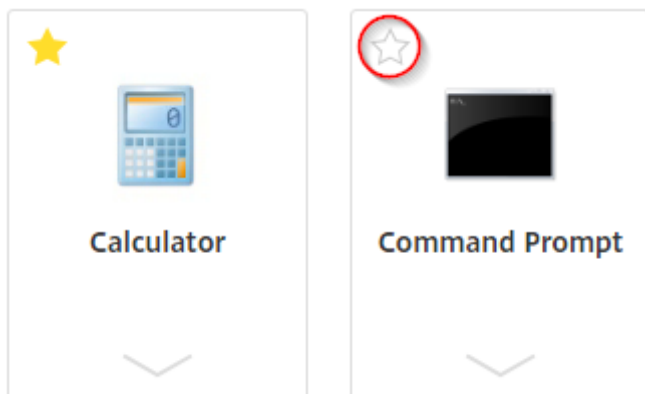
### Accueil

L'écran d'accueil affiche les favoris.



## Favoris

Cliquez ou appuyez sur l'étoile pour désigner un élément comme favori :



## Rechercher

Recherchez dans toutes les applications, tous les bureaux et toutes les catégories :



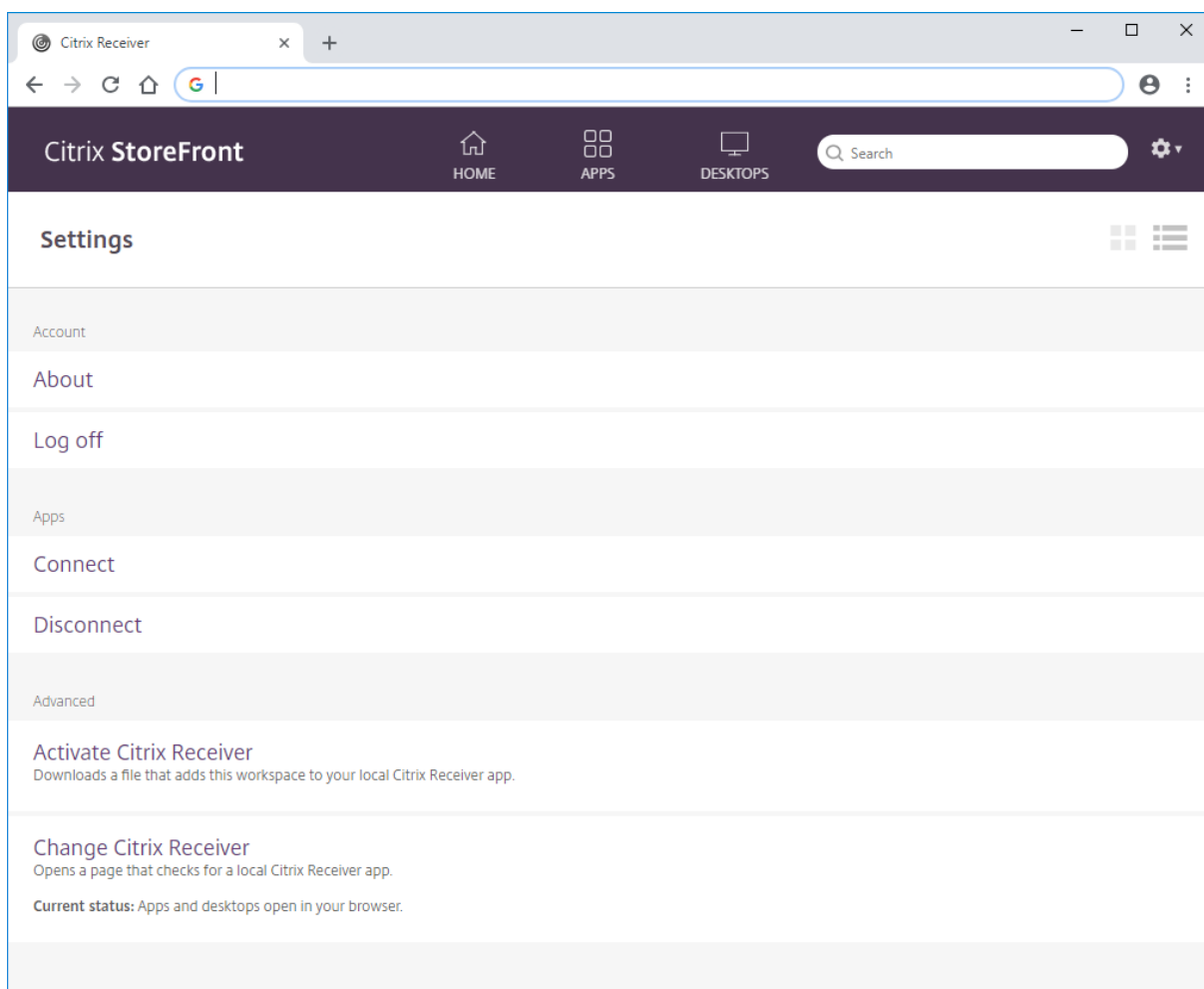


## Paramètres

Accédez aux paramètres depuis le menu déroulant :



Le menu affiche le nom d'utilisateur, qui provient du nom d'affichage Active Directory. Si le nom d'affichage est laissé vide (non recommandé), le domaine et le nom du compte s'affichent. Utilisez le menu pour ouvrir la page Paramètres, vérifier la version de Citrix Receiver ou vous déconnecter.



Les paramètres vous permettent de reprendre des sessions déconnectées ainsi que de déconnecter toutes vos sessions en cours et de vous déconnecter. Affichez la page Paramètres sous forme de cartes ou de liste :



**Connecter.** Reprend les sessions déconnectées.

**Déconnecter.** Déconnecte toutes vos sessions en cours et vous déconnecte.

**Activer Citrix Receiver.** Télécharge un fichier qui ajoute ce magasin à l'application Citrix Receiver locale.

**Changer Citrix Receiver.** Ouvre une page qui vérifie s'il existe une application Citrix Receiver locale. Elle permet aussi aux utilisateurs de passer du lancement de ressources en utilisant l'application Citrix Workspace (ou Citrix Receiver) à leur lancement dans un navigateur HTML5 et vice-versa.

## Créer et gérer des applications recommandées

February 20, 2019

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 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 les modifications terminées, [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 :

Cette fonctionnalité est disponible uniquement lorsque l'expérience classique est désactivée. Ceci est décrit dans [Personnaliser l'apparence de Citrix Receiver](#).

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

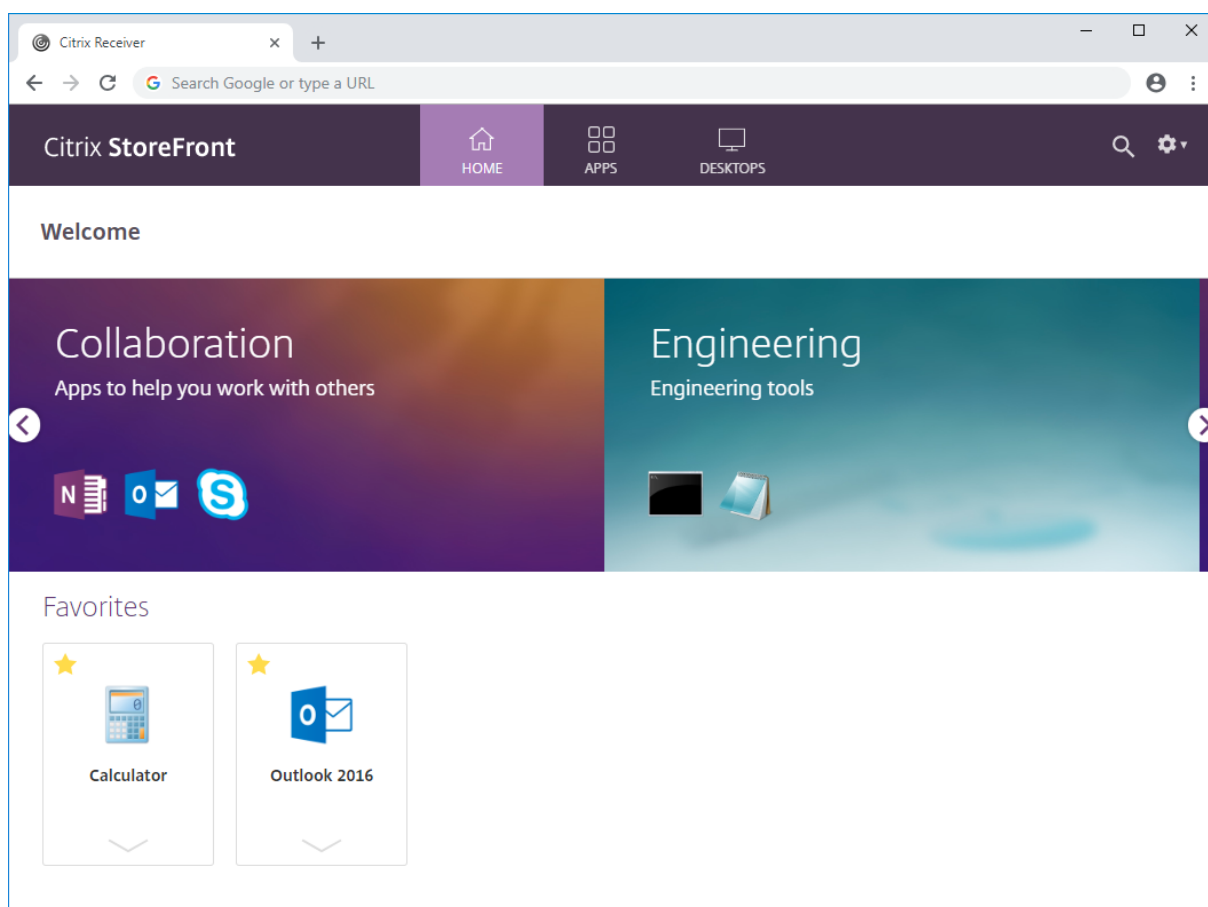
2. Sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Sélectionnez **Groupes d'applications recommandées**.
4. Dans la boîte de dialogue **Groupes 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	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. 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 <b>Exc</b> ne donne aucun résultat.

**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

October 4, 2018

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 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. 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

October 4, 2018

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 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. 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

February 20, 2019

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 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 **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.

## Configurer le délai d'expiration de session

Si le délai d'expiration de session n'est pas configuré correctement sur StoreFront, les utilisateurs peuvent voir le message suivant : « Votre session a expiré pour cause d'inactivité. » Vous pouvez réinitialiser le délai d'expiration de session pour augmenter le délai d'inactivité selon vos besoins.

Effectuez les étapes suivantes pour configurer le délai d'expiration de session sur StoreFront :

### Augmenter le délai d'expiration de session pour StoreFront

1. Sur StoreFront, accédez à `c:\inetpub\wwwroot\Citrix<StoreWeb>`.
2. Repérez l'entrée : `<sessionState timeout="20"/>` dans le fichier `web.config`.
3. Définissez `sessionState timeout` sur la valeur souhaitée, en minutes.

### Augmenter la durée de vie du jeton du service d'authentification

Si vous augmentez le délai d'expiration du jeton de Citrix Receiver pour Web et qu'il dépasse une heure, vous devez aussi augmenter la durée de vie maximale du jeton dans **Service d'authentification**.

### Augmenter le délai d'expiration de session pour le Citrix Receiver natif

1. Pour le Citrix Receiver natif installé sur le serveur StoreFront, accédez à **c:\inetpub\wwwroot\Citrix\Authent**
2. Dans le fichier `web.config`, repérez l'entrée : `<defaultLifetime="01:00:00"maxLifetime="01:00:00">`
3. Définissez `maxLifetime` sur la valeur souhaitée.

#### Remarque :

Pour le client Receiver natif (Windows/Linux), une fois que vous êtes déconnecté de la session actuelle, il se peut que Citrix Virtual Apps and Desktops soit visible en arrière-plan. Cependant, vous devez de nouveau entrer vos informations d'identification lorsque vous cliquez sur une application ou un bureau après l'expiration d'une session StoreFront.

### Augmenter la durée de vie du jeton d'authentification

Si la valeur du délai d'expiration est supérieure à huit heures, modifiez le fichier `web.config` sous Citrix Receiver pour Web pour augmenter la durée de vie du jeton d'authentification :

1. Sur StoreFront, accédez à **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Repérez l'entrée : `<authentication tokenLifeTime="08:00:00"method="Auto"/>`
3. Définissez `tokenLifeTime` sur la valeur souhaitée.

### Redémarrer IIS

- Exécutez la commande `iisreset` pour appliquer les modifications. L'exécution de cette commande déconnecte les utilisateurs de Citrix Receiver pour Web et n'a aucun impact sur leur session ICA actuelle.

#### Remarque :

Le format de la durée de vie est `.d.hh:mm:ss[.ff]`. La durée de vie maximale n'est pas limitée à 24 heures.

### Ressources supplémentaires

- [Blog Citrix - Idle timeout Receiver for Web](#)
- [Security Token Services API](#)

## Configurer l'accès utilisateur

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

## Configurer la prise en charge des connexions via les adresses URL des sites XenApp Services

Utilisez la tâche **Configurer la prise en charge des services XenApp** pour configurer l'accès à vos magasins via les adresses URL XenApp Services. 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. Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services est activée par défaut.

### 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 **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 la prise en charge de XenApp Services**.
3. Cochez ou décochez **Activer la prise en charge de XenApp Services** pour activer ou désactiver l'accès utilisateur au magasin via l'adresse URL XenApp Services affichée.

L'adresse URL XenApp Services d'un magasin s'affiche au format `http[s]://<serveraddress>/Citrix/<storename>/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.

4. Si vous activez XenApp Services Support, vous pouvez spécifier un magasin par défaut dans votre déploiement StoreFront pour les utilisateurs dotés de Citrix Online Plug-in.



Spécifiez un magasin par défaut afin que vos utilisateurs puissent configurer Citrix Online Plug-in avec l'adresse URL du serveur ou l'adresse URL à charge équilibrée du déploiement StoreFront, plutôt que l'adresse URL du site XenApp Services pour un magasin spécifique.

## Désactiver ou activer la reconnexion du contrôle de l'espace de travail pour tous les Citrix Receiver

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.

StoreFront contient une configuration pour empêcher le contrôle de l'espace de travail de se reconnecter dans le service de magasin pour tous les logiciels Citrix Receiver. Gérez cette fonctionnalité à l'aide de la console StoreFront ou PowerShell.

### Utiliser la console de gestion 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 **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Configurer les paramètres du magasin**.
3. Sélectionnez **Paramètres avancés** et cochez ou décochez **Autoriser la reconnexion de sessions**.

### Utiliser PowerShell

Fermez la console de gestion, puis exécutez l'extrait de code suivant pour importer les modules PowerShell de StoreFront :

```
1 $dsInstallProp = Get-ItemProperty '  
2 -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir  
3 $dsInstallDir = $dsInstallProp.InstallDir  
4 & $dsInstallDir\..\Scripts\ImportModules.ps1
```

Ensuite, la commande PowerShell **Set-DSAllowSessionReconnect** active ou désactive la reconnexion du contrôle de l'espace de travail.

Syntaxe

```
Set-DSAllowSessionReconnect [[-SiteId] <Int64>] [[-VirtualPath] <String> ]  
[[-IsAllowed] <Boolean>]
```

Par exemple, pour désactiver la reconnexion du contrôle de l'espace de travail pour un magasin dans */Citrix/Store*, la commande suivante configure le magasin :

```
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store -IsAllowed $false
```

## Configurer les abonnements des utilisateurs

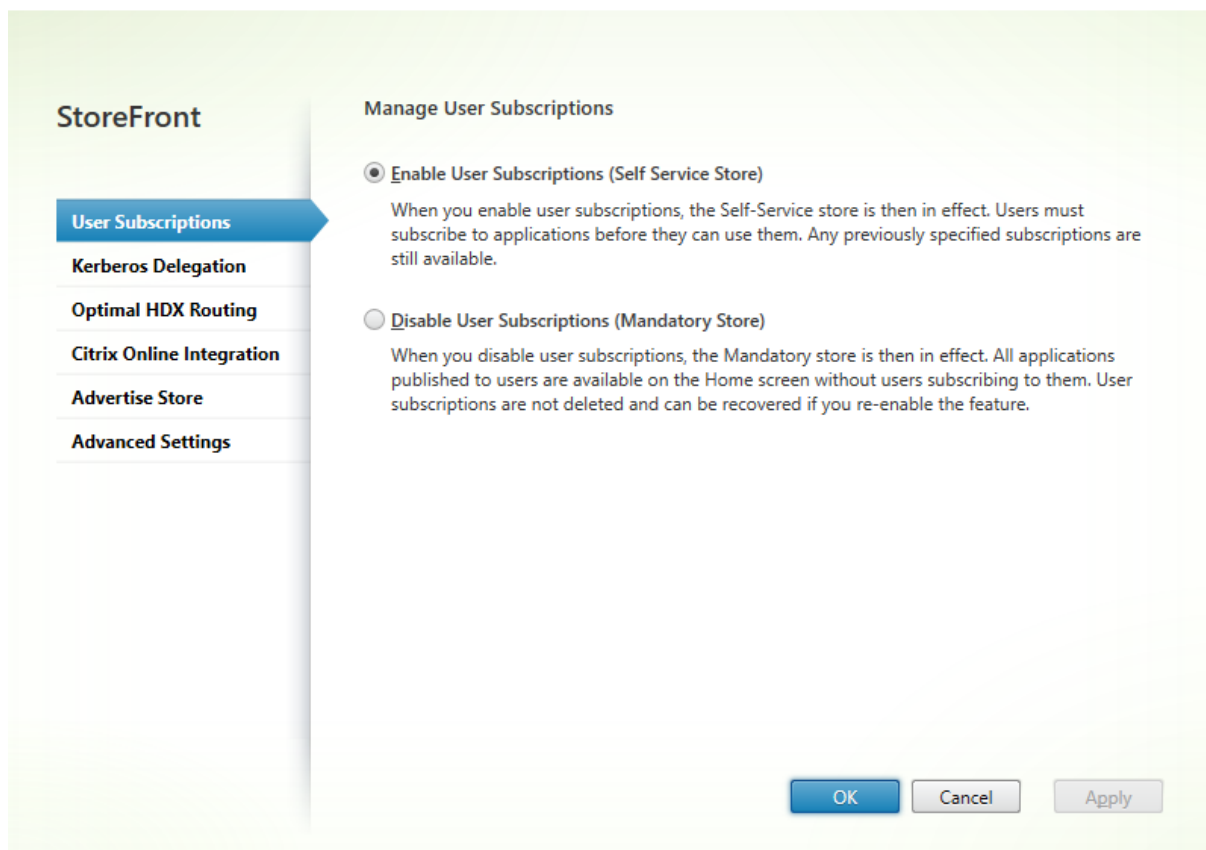
Utilisez la tâche Abonnements utilisateur pour sélectionner l'une des options suivantes :

- Demander aux utilisateurs de s'abonner à des applications avant de les utiliser (magasin en libre-service).
- Autoriser les utilisateurs à recevoir toutes les applications lorsqu'ils se connectent au magasin (magasin obligatoire).

La désactivation des abonnements utilisateur d'un magasin dans StoreFront empêche également l'affichage de l'onglet Favoris auprès des utilisateurs de Citrix Receiver. La désactivation des abonnements ne supprime pas les données d'abonnement du magasin. La réactivation des abonnements du magasin permettra à l'utilisateur de voir les applications auxquelles il est abonné dans les Favoris lors de la prochaine connexion.

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 > Abonnements utilisateur** pour activer/désactiver la fonctionnalité d'abonnements utilisateur.
3. Choisissez **Activer les abonnements utilisateur (Magasin en libre-service)** pour que les utilisateurs s'abonnent aux applications pour les utiliser. Tout abonnement précédemment spécifié est toujours disponible.
4. Choisissez **Désactiver les abonnements utilisateur (Magasin obligatoire)** pour que toutes les applications publiées pour les utilisateurs soient disponibles sur l'écran d'accueil, sans que les utilisateurs aient besoin de s'y abonner. Leurs abonnements ne sont pas supprimés, et ils peuvent les récupérer si vous réactivez la fonctionnalité.

Configure Store Settings - Store



Dans StoreFront 3.5 ou version ultérieure, vous pouvez utiliser le script PowerShell suivant pour configurer les abonnements utilisateur pour un magasin :

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
  votremagasin>"
2 Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
  Confirm:$False
```

Pour plus d'informations sur Get-STFStoreService, consultez <https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Get-STFStoreService/>

## Gérer les données d'abonnement d'un magasin

Gérer les données d'abonnement d'un magasin de données à l'aide d'applets de commande PowerShell.

### Remarque :

Utilisez la console de gestion StoreFront ou le PowerShell pour gérer StoreFront. N'utilisez pas les deux méthodes en même temps. Fermez toujours la console d'administration StoreFront

avant d'utiliser PowerShell pour modifier votre configuration StoreFront. Citrix vous recommande également d'effectuer une sauvegarde de vos données d'abonnement existantes avant d'apporter des modifications de façon à pouvoir restaurer l'état précédent.

### Effacer les données d'abonnement

Un dossier et un magasin de données contenant les données d'abonnement existent pour chaque magasin dans votre déploiement.

1. Arrêtez le service Citrix Subscriptions Store sur le serveur StoreFront. Si le service Citrix Subscriptions Store est en cours d'exécution, il n'est pas possible de supprimer les données d'abonnement de vos magasins.
2. Localisez le dossier du magasin d'abonnement sur le serveur StoreFront : `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. Supprimez le contenu du dossier du magasin d'abonnement, mais pas le dossier.
4. Redémarrez le service Citrix Subscriptions Store sur le serveur StoreFront.

Dans StoreFront 3.5 ou version ultérieure, vous pouvez utiliser le script PowerShell suivant pour effacer les données d'abonnements d'un magasin. Exécutez cette fonction PowerShell en tant qu'administrateur autorisé à arrêter ou démarrer des services et supprimer des fichiers. Cette fonction PowerShell donne le même résultat que les étapes manuelles décrites ci-dessus.

Pour exécuter les applets de commande avec succès, le service Citrix Subscriptions Store doit être exécuté sur le serveur.

```
1 function Remove-SubscriptionData
2
3 {
4
5     [CmdletBinding()]
6
7     [Parameter(Mandatory=$False)][String]$Store = "Store"
8
9     $SubsService = "Citrix Subscriptions Store"
10
11     # Path to Subscription Data in StoreFront version 2.6 or higher
12
13     $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
14                 Roaming\Citrix\SubscriptionsStore\1__Citrix_*$Store*"
15
16     Stop-Service -displayname $SubsService
17
18     Remove-Item $SubsPath -Force -Verbose
```

```
18
19     Start-Service -displayname $SubsService
20
21     Get-Service -displayname $SubsService
22 }
23
24
25     Remove-SubscriptionData -Store "YourStore"
```

### Exporter les données d'abonnement

Vous pouvez obtenir une copie de sauvegarde des données d'abonnement d'un magasin sous la forme d'un fichier .txt séparé par des onglets à l'aide de l'applet de commande PowerShell suivante.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
   votremagasin>"
2
3 Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
   :USERPROFILE\Desktop\Subscriptions.txt"
```

Si vous gérez un déploiement contenant plusieurs serveurs, vous pouvez exécuter cette applet de commande PowerShell sur n'importe quel serveur dans le groupe de serveurs StoreFront. Chaque serveur dans le groupe de serveurs conserve une copie synchronisée identique des données d'abonnement de ses homologues. Si vous pensez que vous rencontrez des problèmes avec la synchronisation des abonnements entre les serveurs StoreFront, exportez les données de tous les serveurs du groupe et comparez-les pour observer les différences.

### Restaurer les données d'abonnement

Utilisez `Restore-STFStoreSubscriptions` pour remplacer vos données d'abonnement existantes. Vous pouvez restaurer les données d'abonnement d'un magasin à l'aide du fichier .txt de sauvegarde séparé par des onglets que vous avez créé précédemment à l'aide de `Export-STFStoreSubscriptions`.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
   votremagasin>"
2
3 Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "
   $env:USERPROFILE\Desktop\Subscriptions.txt"
```

Pour plus d'informations sur `Restore-STFStoreSubscriptions`, consultez <https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Restore-STFStoreSubscriptions/>

### **Restaurer des données sur un serveur StoreFront unique**

Dans un déploiement ne contenant qu'un seul serveur, il n'est pas nécessaire d'arrêter le service Subscriptions Store. De même, il n'est pas nécessaire d'effacer les données d'abonnement existantes avant la restauration des données d'abonnement.

### **Restaurer des données sur un groupe de serveurs StoreFront**

Pour restaurer les données d'abonnement d'un groupe de serveurs, les étapes suivantes sont requises.

Exemple de déploiement d'un groupe de serveurs contenant trois serveurs StoreFront.

- StoreFrontA
  - StoreFrontB
  - StoreFrontC
1. Sauvegardez les données d'abonnement existantes de l'un des trois serveurs.
  2. Arrêtez le service Subscriptions Store sur les serveurs StoreFrontB et C. Cette action empêche les serveurs d'envoyer ou de recevoir des données d'abonnement lors de la mise à jour de StoreFrontA.
  3. Effacez les données d'abonnement des serveurs StoreFrontB et C. Cette action empêche toute incohérence entre les données d'abonnement restaurées.
  4. Restaurez les données sur StoreFrontA à l'aide de l'applet de commande **Restore-STFStoreSubscriptions**. Il n'est pas nécessaire d'arrêter le service Subscriptions Store, ou d'effacer les données d'abonnement sur StoreFrontA (elles sont remplacées lors de l'opération de restauration).
  5. Redémarrez le service Citrix Subscriptions Store sur les serveurs StoreFrontB et StoreFrontC. Les serveurs peuvent recevoir ensuite une copie des données de StoreFrontA.
  6. Attendez que les données soient synchronisées entre tous les serveurs. La durée de synchronisation dépend du nombre d'enregistrements sur StoreFrontA. Si tous les serveurs sont sur une connexion réseau locale, la synchronisation se produit généralement rapidement. La synchronisation des abonnements via une connexion WAN peut prendre plus de temps.
  7. Exportez les données à partir de StoreFrontB et C pour confirmer que la synchronisation est terminée, ou affichez les compteurs de Store Subscription.

### **Importer les données d'abonnement**

Utilisez **Import-STFStoreSubscriptions** lorsqu'il n'existe aucune donnée d'abonnement pour le magasin. Cette applet de commande permet également de transférer les données d'abonnement d'un magasin vers un autre ou si les données d'abonnement sont importées, vers les serveurs StoreFront nouvellement provisionnés.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
  votremagasin>"
2
3 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
  :USERPROFILE\Desktop\Subscriptions.txt"
```

Pour plus d'informations sur Import-STFStoreSubscriptions, consultez <https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Import-STFStoreSubscriptions/>

### Détails du fichier de données de l'abonnement

Le fichier de données d'abonnement est un fichier texte contenant une ligne par abonnement utilisateur. Chaque ligne est une séquence de valeurs séparées par des tabulations :

```
<user-identifiant> <resource-id> <subscription-id> <subscription-status> <
property-name> <property-value> <property-name> <property-value> ...
```

où :

- `<user-identifiant>` - Obligatoire. Séquence de caractères identifiant l'utilisateur. Il s'agit de l'identificateur de sécurité Windows de l'utilisateur.
- `<resource-id>` - Obligatoire. Séquence de caractères identifiant la ressource à laquelle vous avez souscrit.
- `<subscription-id>` - Obligatoire. Séquence de caractères identifiant de façon unique l'abonnement. Cette valeur n'est pas utilisée (mais, une valeur doit être présente dans le fichier de données).
- `<subscription-status>` - Obligatoire. État de l'abonnement : abonné ou non abonné.
- `<property-name>` et `<property-value>` - Facultatif. Séquence de zéro ou de plusieurs paires de nom/valeur de propriété. Ces dernières représentent les propriétés associées à l'abonnement par un client StoreFront (généralement Citrix Receiver). Propriété avec plusieurs valeurs qui est représentée par plusieurs paires de nom/valeur avec le même nom (par exemple, « ... MyProp A MyProp B ... » représente la propriété MyProp avec des valeurs A, B).

### Exemple

```
S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-
08002B30309D Subscribed dazzle:position 1
```

### Taille des données d'abonnement sur le disque du serveur StoreFront

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

#### Taille des fichiers .txt d'importation et d'exportation

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

#### Compteurs d'abonnement du magasin

Vous pouvez utiliser les compteurs de l'Analyseur de performances Microsoft Windows (**Démarrer > Exécuter > perfmon**) afin d'afficher, par exemple, le nombre total d'enregistrements d'abonnements sur le serveur ou le nombre d'enregistrements synchronisés entre les groupes de serveurs StoreFront.

#### Afficher les compteurs d'abonnements à l'aide de PowerShell



```
1 Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\
   Subscription Entries Count (including unpurged deleted records)"
2
3 Get-Counter -Counter "\Citrix Subscription Store Synchronization\
   Subscriptions Store Synchronizing"
4
5 Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
   Subscriptions Synchronized"
6
7 Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
   Subscriptions Transferred"
```

## Configurer StoreFront pour lancer les applications et les bureaux en mode fenêtré

February 20, 2019

Le lancement transparent des applications dépend de la disponibilité de StoreFront dans le déploiement. Si vous désactivez l'option transparente pour les applications et les bureaux, envisagez de lancer vos ressources en mode fenêtré.

Voici un exemple de Bloc-notes publié. Utilisez le nom de l'application publiée exactement comme il apparaît dans l'ensemble d'applications de la console Citrix Virtual Apps and Desktops.

### Remarque :

La plupart des paramètres des fichiers ICA ne sont pas sensibles à la casse sauf `DesiredHRES` et `DesiredVRES`. Lors de l'application de la version fenêtrée de l'application, utilisez le nom du navigateur pour référencer l'application dans le fichier `default.ica` sur le serveur StoreFront. Vérifiez le nom du navigateur de l'application en utilisant PowerShell sur Delivery Controller :

```
>>asnp citrix*
>>Get-BrokerApplication -ApplicationName
```

Pour configurer StoreFront

1. Modifiez le fichier `default.ica` situé sur le serveur StoreFront dans le répertoire `\inetpub\wwwroot\Citrix`
2. Dans le fichier `default.ica`, repérez les lignes suivantes: `[ApplicationServers] application=`.
3. Créez une ligne après `application=` et ajoutez les paramètres suivants :

```
1 [Notepad]
2 TWIMode=Off
```

```
3 DesiredHRES=1024
4 DesiredVRES=768
```

4. Enregistrez le fichier.

**Remarque :**

Remplacez **DesiredHRES=1024 DesiredVRES=768** par **ScreenPercent=90** pour utiliser le pourcentage d'écran plutôt que des résolutions d'écran spécifiques.

Pour les bureaux publiés depuis Citrix Virtual Apps and Desktops 7.x et StoreFront 3.x

1. Modifiez le fichier `web.config` situé sur le serveur StoreFront dans le répertoire `C:\inetpub\wwwroot\Citrix`.
2. Dans le fichier `web.config`, repérez la ligne suivante : **showDesktopViewer='true'**.
3. Modifiez la valeur de **True** et remplacez-la par **False**.
4. Sur le côté client ou depuis AD-GPMC, utilisez le fichier de modèle d'administration (`receiver.adm` ou `receiver.admx\receiver.adml`, selon le système d'exploitation) pour configurer la stratégie suivante :
  - **Configuration ordinateur > Composants Citrix > Citrix Receiver > Expérience utilisateur > Paramètres d'affichage du client : Activer**
  - **Fenêtres transparentes : False**
  - **Largeur de fenêtre : <As per requirement>, Hauteur de fenêtre : <As per requirement>**

## Ressources supplémentaires

`DesiredHRES` et `DesiredVRES` peuvent être définis sur n'importe quelle résolution souhaitée, telle que 800x600 ou 1024x768.

Si l'application doit s'exécuter dans un certain pourcentage de taille d'écran, après avoir défini `TWIMode=Off`, ajoutez la ligne `ScreenPercent=90` qui configure l'écran sur 90 %. Vous pouvez également effectuer cette procédure avec le site Services XenApp (anciennement le site Agent Program Neighborhood). Assurez-vous que le fichier correspondant sous le dossier `conf` de ce site (`Inetpub\wwwroot\Citrix\PNAgent\conf`) est modifié.

Si vous utilisez le client 10.x et modifiez le fichier `default.ica` ou `template.ica`, ajoutez seulement la ligne `TWIMode=Off`. Les paramètres `HRES` et `VRES` sont obtenus depuis les propriétés de l'application publiée. Sinon, une erreur s'affiche indiquant des entrées dupliquées dans le fichier ICA lorsqu'un utilisateur essaie de lancer l'application.

## Définir des magasins multisite à haute disponibilité

February 20, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Pour les magasins qui regroupent les ressources de plusieurs déploiements, plus particulièrement les déploiements répartis sur différents sites géographiques, vous pouvez configurer l'équilibrage de charge et le basculement entre les déploiements, le mappage des utilisateurs sur les déploiements, et des déploiements de récupération d'urgence spécifiques destinés à assurer un haut niveau de disponibilité des ressources. Si vous avez configuré des boîtiers NetScaler Gateway distincts pour vos déploiements, vous pouvez définir le boîtier optimal que les utilisateurs doivent utiliser pour accéder à chacun des déploiements.

Depuis StoreFront 3.5, la console de gestion StoreFront prend en charge les scénarios multisite courants. Citrix vous recommande d'utiliser la console de gestion lorsqu'elle répond à vos besoins.

### Configurer le mappage utilisateur et l'agrégation

La console de gestion StoreFront vous permet de :

- **Mapper des utilisateurs avec des déploiements :** sur la base de leur appartenance à un groupe Active Directory, vous pouvez restreindre les utilisateurs qui ont accès à certains déploiements.
- **Agréger les déploiements :** vous pouvez spécifier les déploiements qui ont des ressources à agréger. Les ressources correspondantes dans les déploiements regroupés sont présentées à l'utilisateur comme une seule ressource à haute disponibilité.
- **Associer une zone à un déploiement :** lorsque vous accédez à NetScaler Gateway dans une configuration d'équilibrage de charge globale, StoreFront hiérarchise les déploiements des zones correspondant à la zone de passerelle lors du lancement des ressources.

### 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. Vérifiez que vous avez configuré le magasin avec les détails de tous les déploiements XenDesktop et XenApp que vous voulez utiliser dans votre configuration. Pour de plus amples informations sur l'ajout de déploiements à des magasins, consultez la section [Gérer les ressources mises à disposition dans les magasins](#).

2. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette **Citrix StoreFront** et cliquez dessus.
3. 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**.
4. Si deux Controller ou plus sont définis, cliquez sur **Configuration du mappage utilisateur et de l'agrégation multisite > Configurer**.
5. Cliquez sur **Mapper des utilisateurs avec des Controller** et effectuez des sélections sur les écrans pour spécifier quels Delivery Controller sont disponibles pour quels utilisateurs.
6. Cliquez sur **Agréger les ressources**, sélectionnez les Controller et cliquez sur **Agréger** pour indiquer si les Delivery Controller sont regroupés. Si vous activez l'agrégation des Delivery Controller, les applications et les bureaux de ces Delivery Controller avec le même nom d'affichage et chemin d'accès sont présentés comme application/bureau unique dans Citrix Receiver.
7. Choisissez une ou les deux cases à cocher dans **Paramètres Controller agrégés**, puis cliquez sur **OK**.

**Les Controller publient des ressources identiques** : lorsque cette option est sélectionnée, StoreFront énumère les ressources à partir d'un seul des contrôleurs de l'agrégation. Lorsqu'elle est désactivée, StoreFront énumère les ressources depuis tous les contrôleurs de l'agrégation (pour cumuler l'ensemble des ressources disponibles de l'utilisateur). La sélection de cette option permet une amélioration des performances lors de l'énumération des ressources, mais nous ne la recommandons pas, sauf si vous êtes certain que la liste de ressources est identique sur tous les déploiements agrégés.

**Équilibrer la charge sur tous les Controller** : lorsque cette option est sélectionnée, les lancements sont distribués de manière équitable entre les contrôleurs. Lorsque cette option est désactivée, les lancements sont dirigés vers le premier contrôleur spécifié dans la boîte de dialogue de mappage utilisateur, basculant vers les autres contrôleurs si le lancement échoue.

## Configurations avancées

Bien que vous puissiez configurer la plupart des opérations multisite et de haute disponibilité courantes à l'aide de la console de gestion StoreFront, vous pouvez toujours configurer StoreFront à l'aide des fichiers de configuration de la même manière que dans les versions précédentes de StoreFront.

Fonctionnalités supplémentaires disponibles avec PowerShell ou en modifiant les fichiers de configuration de StoreFront :

- La possibilité de spécifier plusieurs groupes de déploiements pour l'agrégation.

- La console de gestion permet un seul regroupement de déploiements, ce qui est suffisant dans la plupart des cas.
- Pour les magasins avec de nombreux déploiements avec plusieurs ensembles distincts de ressources, l'utilisation de plusieurs groupes peut améliorer les performances.
- La possibilité de spécifier des ordres de préférence complexes pour les déploiements agrégés. La console de gestion permet d'équilibrer la charge des déploiements agrégés ou de les utiliser en tant que liste de basculement unique.
- La possibilité de définir des déploiements de récupération d'urgence (déploiements accessibles uniquement lorsque tous les autres déploiements ne sont pas disponibles).

**Avertissement :**

Après la configuration d'options multisite avancées avec la modification manuelle du fichier de configuration, certaines tâches deviennent indisponibles dans la console de gestion Citrix StoreFront pour empêcher une configuration incorrecte.

**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. Vérifiez que vous avez configuré le magasin avec les détails de tous les déploiements XenDesktop et XenApp que vous voulez utiliser dans votre configuration, y compris les déploiements de récupération d'urgence. Pour de plus amples informations sur l'ajout de déploiements à des magasins, consultez la section [Gérer les ressources mises à disposition dans les magasins](#).
2. Utilisez un éditeur de texte pour ouvrir le fichier web.config du magasin, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\nommagasin\, où nommagasin désigne le nom attribué au magasin au moment de sa création.
3. Recherchez la section suivante dans le fichier.

```
1 <resourcesWingConfigurations>
2 <resourcesWingConfiguration name="Default" wingName="Default" />
3 </resourcesWingConfigurations>
```

4. Spécifiez votre configuration comme illustré ci-dessous.

```
1 <resourcesWingConfigurations>
2 <resourcesWingConfiguration name="Default" wingName="Default">
3 <userFarmMappings>
4 <clear />
5 <userFarmMapping name="user_mapping">
```

```
6 <groups>
7 <group name="domain\usergroup" sid="securityidentif" />
8 <group ... />
9 ...
10 </groups>
11 <equivalentFarmSets>
12 <equivalentFarmSet name="setname" loadBalanceMode="{
13   LoadBalanced | Failover }
14   "
15   aggregationGroup="aggregationgroupname">
16   <primaryFarmRefs>
17     <farm name="primaryfarmname" />
18     <farm ... />
19     ...
20   </primaryFarmRefs>
21   <backupFarmRefs>
22     <farm name="backupfarmname" />
23     <farm ... />
24     ...
25   </backupFarmRefs>
26 </equivalentFarmSet>
27 <equivalentFarmSet ... >
28 ...
29 </equivalentFarmSet>
30 </equivalentFarmSets>
31 </userFarmMapping>
32 <userFarmMapping>
33 ...
34 </userFarmMapping>
35 </userFarmMappings>
36 </resourcesWingConfiguration>
37 </resourcesWingConfigurations>
```

Utilisez les éléments suivants pour définir votre configuration.

- **userFarmMapping** : spécifie les groupes de déploiements et définit le comportement de l'équilibrage de charge et du basculement entre ces déploiements. Identifie les déploiements à utiliser pour la récupération d'urgence. Contrôle l'accès utilisateur aux ressources en mappant les groupes d'utilisateurs Microsoft Active Directory aux groupes de déploiements spécifiés.
- **groups** : spécifie les noms et identificateurs de sécurité (SID) des groupes d'utilisateurs Active Directory auxquels le mappage associé s'applique. Les noms des groupes d'utilisateurs doivent être entrés au format *domaine\grouped'utilisateurs*. Lorsque plusieurs groupes sont indiqués, le mappage est appliqué uniquement aux utilisateurs qui sont membres de tous les groupes spécifiés. Pour activer l'accès de tous les comptes d'utilisateurs Active Directory, définissez le

nom du groupe et le SID sur **Tout le monde**.

- **equivalentFarmSet** : spécifie un groupe de déploiements équivalents offrant des ressources à agréger pour l'équilibrage de charge ou le basculement, ainsi qu'un groupe associé facultatif de déploiements de récupération d'urgence.

L'attribut **loadBalanceMode** détermine l'attribution d'utilisateurs aux déploiements. Définissez la valeur de l'attribut **loadBalanceMode** sur **LoadBalanced** pour attribuer de façon aléatoire des utilisateurs à des déploiements dans le jeu de déploiements équivalent, ce qui permet de répartir équitablement les utilisateurs sur tous les déploiements disponibles. Lorsque la valeur de l'attribut **loadBalanceMode** est définie sur **Failover**, les utilisateurs sont connectés au premier déploiement disponible dans l'ordre dans lequel ils sont répertoriés dans la configuration, ce qui réduit le nombre de déploiements utilisés à un moment donné. Spécifiez les noms des groupes d'agrégation pour identifier les jeux de déploiement équivalents qui fournissent les ressources à regrouper. Les ressources fournies par les jeux de déploiement équivalents qui appartiennent au même groupe d'agrégation sont regroupées. Pour indiquer que les déploiements définis dans un jeu de déploiements équivalent particulier ne doivent pas être agrégés à d'autres, définissez le nom du groupe d'agrégation sur "".

L'attribut **identical** accepte les valeurs **true** et **false**, et indique si tous les déploiements d'un ensemble de déploiement équivalent fournissent exactement la même série de ressources. Lorsque les déploiements sont identiques, StoreFront énumère les ressources de l'utilisateur à partir d'un seul déploiement principal de l'ensemble. Lorsque les déploiements fournissent des ressources qui se recoupent mais ne sont pas identiques, StoreFront effectue l'énumération depuis chaque déploiement pour obtenir l'ensemble complet de ressources disponibles pour un utilisateur. Un équilibrage de charge (au démarrage) peut se produire que les déploiements soient identiques ou non. La valeur par défaut pour l'attribut **identical** est **false**, mais il est défini sur **true** lorsque StoreFront est mis à niveau pour éviter de modifier le comportement pré-existant après une mise à niveau.

- **primaryFarmRefs** : spécifie un jeu de sites XenDesktop ou XenApp équivalents dans lequel certaines ou toutes les ressources correspondent. Entrez le nom des déploiements que vous avez déjà ajoutés au magasin. Les noms des déploiements spécifiés doivent correspondre exactement aux noms que vous avez entrés lorsque vous avez ajouté les déploiements au magasin.
- **optimalGatewayForFarms** : spécifie les groupes de déploiements et définit les boîtiers NetScaler Gateway que les utilisateurs doivent utiliser de préférence pour accéder aux ressources fournies par ces déploiements. En général, le boîtier optimal pour un déploiement figure dans le même emplacement géographique que ce déploiement. Vous ne devez définir les boîtiers NetScaler Gateway optimaux pour les déploiements uniquement lorsque le boîtier à partir duquel les utilisateurs accèdent à StoreFront n'est pas le boîtier optimal.

## Configurer la synchronisation des abonnements

Pour configurer la synchronisation régulière par envoi de données (pull) des applications auxquelles les utilisateurs ont souscrit avec les magasins dans différents déploiements StoreFront, exécutez des commandes Windows PowerShell.

**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.

**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 des groupes de serveurs](#) de façon à mettre à jour les autres serveurs dans le déploiement.

Lors de l'établissement de la synchronisation de votre abonnement, notez que les Delivery Controller configurés doivent être nommés de manière identique entre les magasins synchronisés et que les noms du Delivery Controller sont sensibles à la casse. Si les noms des Delivery Controller ne sont pas exactement les mêmes, les utilisateurs auront des abonnements différents dans les magasins synchronisés.

1. Utilisez un compte possédant des permissions d'administrateur local pour démarrer Windows PowerShell et, à l'invite de commande, tapez les commandes suivantes pour importer les modules StoreFront.

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

où *installationlocation* est le répertoire dans lequel StoreFront est installé, généralement C:\Program Files\Citrix\Receiver StoreFront.

2. Pour spécifier le déploiement StoreFront distant contenant le magasin à synchroniser, tapez la commande suivante.

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



où *deploymentname* est un nom qui vous aide à identifier le déploiement distant et est *deploymentaddress* l'adresse accessible en externe du serveur StoreFront ou d'un groupe de serveurs avec équilibrage de la charge pour le déploiement distant.

3. Pour spécifier le magasin distant avec lequel synchroniser les abonnements d'applications des utilisateurs, tapez la commande suivante.

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

où *deploymentname* est le nom que vous avez défini pour le déploiement distant à l'étape précédente et *storename* le nom spécifié lors de la création des magasins locaux et distants. Pour synchroniser les abonnements aux applications entre les magasins, les deux magasins doivent avoir le même nom dans leur déploiement StoreFront respectif.

4. Pour configurer la synchronisation à un moment donné chaque jour, tapez la commande suivante.

```
1 Add-DSSubscriptionsSyncSchedule -scheduleName synchronisationname  
-startTime hh:mm
```

où *synchronisationname* est un nom qui vous aidera à identifier la planification que vous créez. Utilisez le paramètre **-startTime** pour spécifier l'heure à laquelle vous souhaitez synchroniser les abonnements entre les magasins. Configurez plus de planifications pour spécifier des horaires de synchronisation supplémentaires au travers de la journée.

5. Vous pouvez également configurer la synchronisation régulière à un intervalle spécifique en tapant la commande suivante.

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

où *synchronisationname* est un nom qui vous aidera à identifier la planification que vous créez. Utilisez le paramètre **-startTime** pour spécifier l'heure à laquelle vous souhaitez démarrer la planification récurrente. Pour l'intervalle, spécifiez la durée (en minutes) entre chaque synchronisation.

6. Ajoutez les comptes de machine de domaine Microsoft Active Directory pour chaque serveur StoreFront du déploiement distant au groupe d'utilisateurs Windows local CitrixSubscriptionSyncUsers sur le serveur actuel.

Ceci permet aux serveurs dans le déploiement distant d'accéder au Subscription Store Service sur le déploiement local une fois que vous avez configuré une planification de synchronisation sur le déploiement distant. Le groupe CitrixSubscriptionSyncUsers est automatiquement créé lorsque vous importez le module de synchronisation d'abonnement à l'étape 1. Pour plus

d'informations sur la modification des groupes d'utilisateurs locaux, consultez <http://technet.microsoft.com/en-us/library/cc772524.aspx>.

7. Si votre déploiement StoreFront local se compose de plusieurs serveurs, utilisez la console de gestion Citrix StoreFront pour propager les modifications de configuration aux autres serveurs du groupe.

Pour de plus amples informations sur la propagation des modifications dans un déploiement StoreFront contenant de multiples serveurs, consultez la section [Configurer des groupes de serveurs](#).

8. Répétez les étapes 1 à 7 sur le déploiement StoreFront distant pour configurer un planning de synchronisation des abonnements complémentaire du déploiement distant vers le déploiement local.

Lors de la configuration des planifications de la synchronisation pour vos déploiements StoreFront, assurez-vous que les planifications ne débouchent pas sur une situation dans laquelle les déploiements tentent de synchroniser simultanément.

9. Pour démarrer la synchronisation des abonnements d'applications des utilisateurs entre les magasins, redémarrez le Subscription Store Service sur les déploiements local et distant. À partir d'une invite de commande Windows PowerShell sur un serveur dans chaque déploiement, entrez la commande suivante.

```
1 Restart-DSSubscriptionsStoreSubscriptionService
```

10. Pour supprimer une planification de synchronisation d'abonnement existante, tapez la commande suivante ; propagez ensuite les modifications apportées à la configuration aux autres serveurs StoreFront dans le déploiement et redémarrez le Subscription Store Service.

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

où *synchronizationname* est le nom que vous avez spécifié pour la planification lors de sa création.

11. Pour répertorier les planifications de synchronisation d'abonnement actuellement configurées pour votre déploiement StoreFront, tapez la commande suivante.

```
1 Get-DSSubscriptionsSyncScheduleSummary
```

## Configurer un routage HDX optimal pour un magasin

**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 les modifications terminées, [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.

**Différences entre une batterie et une zone lors de la définition de mappages de passerelles optimales pour un magasin**

Dans les versions de StoreFront antérieures à 3.5, vous pouviez mapper une passerelle optimale uniquement sur une ou des batteries. Le concept de zones vous permet de diviser un déploiement XenApp XenDesktop en zones en fonction du centre de données ou de l'emplacement géographique dans lequel les Controller XenApp ou XenDesktop et les ressources publiées résident. Définissez des zones dans XenApp ou XenDesktop Studio. StoreFront interagit avec XenApp XenDesktop ; par conséquent toute zone définie dans StoreFront doit correspondre en tout point aux noms de zones définis dans XenApp et XenDesktop.

StoreFront vous permet également de créer un mappage de passerelle optimale pour tous les Delivery Controller résidant dans la zone définie. La procédure de mappage d'une zone sur une passerelle optimale est presque identique à la création de mappages à l'aide de batteries, ce qui est une procédure que vous avez peut-être déjà eu l'occasion d'effectuer. La seule différence réside dans le fait que les zones représentent généralement des conteneurs beaucoup plus volumineux contenant de nombreux Delivery Controller. Vous n'avez pas besoin d'ajouter chaque Delivery Controller à un mappage de passerelle optimale. Pour placer les Controller dans la zone souhaitée, il vous suffit simplement d'ajouter un indicateur à chaque Delivery Controller dont le nom de zone correspond à une zone déjà définie dans XenApp ou XenDesktop. Vous pouvez mapper une passerelle optimale à plus d'une zone, mais il est généralement recommandé de n'utiliser qu'une seule zone. Une zone représente généralement un centre de données dans un emplacement géographique. Chaque zone doit disposer d'au moins une passerelle NetScaler Gateway optimale utilisée pour les connexions HDX aux ressources dans cette zone.

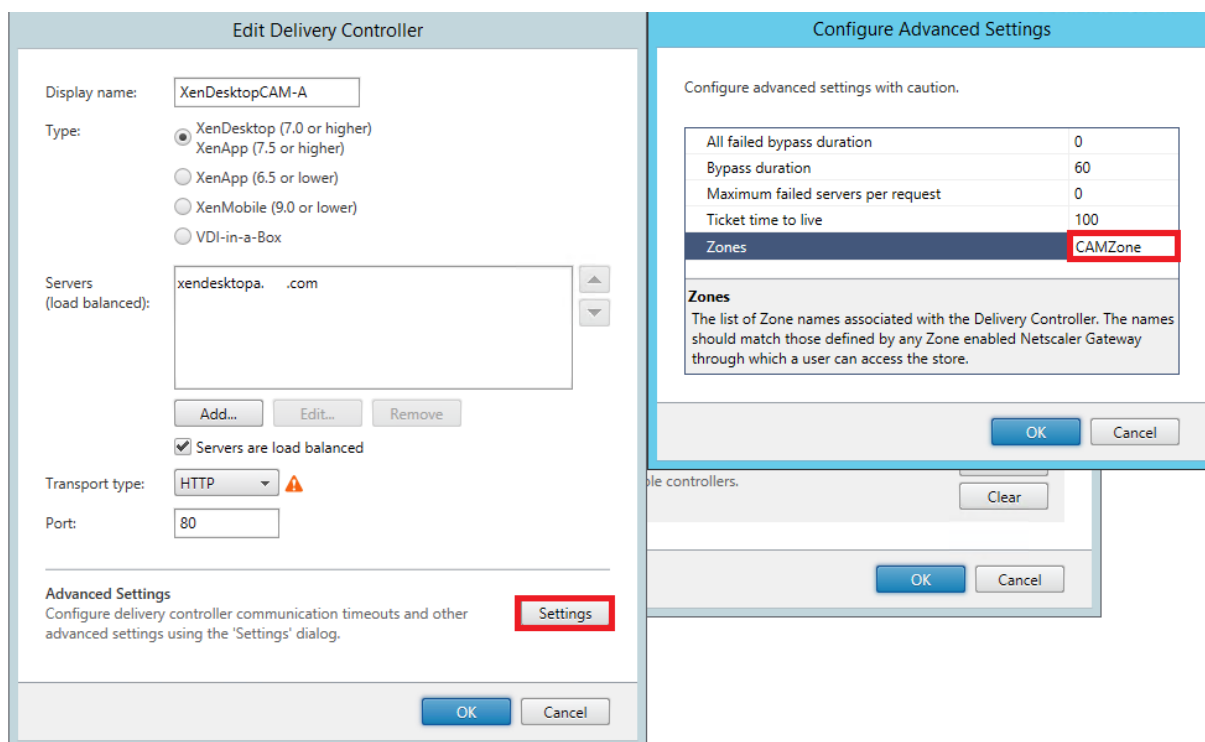
Pour de plus amples informations sur les zones, consultez la section [Zones](#).

**Placer un Delivery Controller dans une zone**

Définissez l'attribut de zone sur chaque Delivery Controller que vous voulez placer dans une zone.

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**, puis sur **Paramètres** dans l'écran **Modifier Delivery Controller**.
4. Sur la ligne **Zones**, cliquez dans la deuxième colonne.
5. Cliquez sur **Ajouter** dans l'écran **Noms de zone de Delivery Controller** et ajoutez un nom de zone.



Configurez un routage NetScaler Gateway optimal afin d'optimiser le traitement du routage de la connexion ICA depuis le moteur HDX vers des ressources publiées telles que des VDA XenDesktop ou des applications publiées XenApp ou XenDesktop à l'aide de StoreFront. En règle générale, la passerelle optimale pour un site est colocalisée dans le même emplacement géographique.

Vous ne devez définir des boîtiers NetScaler Gateway optimaux pour les déploiements que si le boîtier à partir duquel les utilisateurs accèdent à StoreFront n'est pas la passerelle optimale. Si les lancements doivent être redirigés via la passerelle à l'origine de la demande de lancement, StoreFront le fait automatiquement.

### Exemple de scénario avec des batteries

1 x passerelle FR → 1 x StoreFront FR

- Applications et bureaux locaux FR
- Applications et bureaux US utilisés uniquement pour le basculement FR

1 x passerelle US -> 1 x StoreFront US

- Applications et bureaux locaux US
- Applications et bureaux FR utilisés uniquement pour le basculement US

Une passerelle FR fournit un accès à distance aux ressources FR, telles que les applications et les bureaux utilisant un StoreFront FR.

Le StoreFront FR dispose à la fois d'un NetScaler Gateway FR et US, ainsi que de batteries de serveur FR et US dans sa liste de Delivery Controller. Les utilisateurs FR accèdent aux ressources à distance via leur passerelle, StoreFront et leurs batteries situés dans le même emplacement géographique. Si leurs ressources FR deviennent indisponibles, ils peuvent se connecter aux ressources US en tant qu'alternative de basculement temporaire.

Sans routage optimal de la passerelle, tous les lancements ICA passeraient par la passerelle FR qui a effectué la demande de lancement, quel que soit l'emplacement géographique des ressources. Par défaut, les passerelles utilisées pour initier des demandes de lancement sont identifiées dynamiquement par StoreFront lorsque la demande est faite. Le routage vers la passerelle optimale modifie ce comportement et force l'utilisation de connexions US via la passerelle la plus proche des batteries US qui fournissent les applications et bureaux.

**Remarque :**

Vous ne pouvez mapper qu'une passerelle optimale par site pour chaque magasin StoreFront.

**Exemple de scénario utilisant des zones**

1 x CAMZone -> 2 x StoreFront GB

- Cambridge, GB : Applications et bureaux
- Fort Lauderdale, États-Unis de l'Est : Applications et bureaux
- Bangalore, Inde : Applications et bureaux

1 x FTLZone -> 2 x StoreFront US

- Fort Lauderdale, États-Unis de l'Est : Applications et bureaux
- Cambridge, GB : Applications et bureaux
- Bangalore, Inde : Applications et bureaux

1 x BGLZone -> 2 x StoreFront IN

- Bangalore, Inde : Applications et bureaux
- Cambridge, GB : Applications et bureaux
- Fort Lauderdale, États-Unis de l'Est : Applications et bureaux

Figure 1. Routage vers la passerelle non optimal

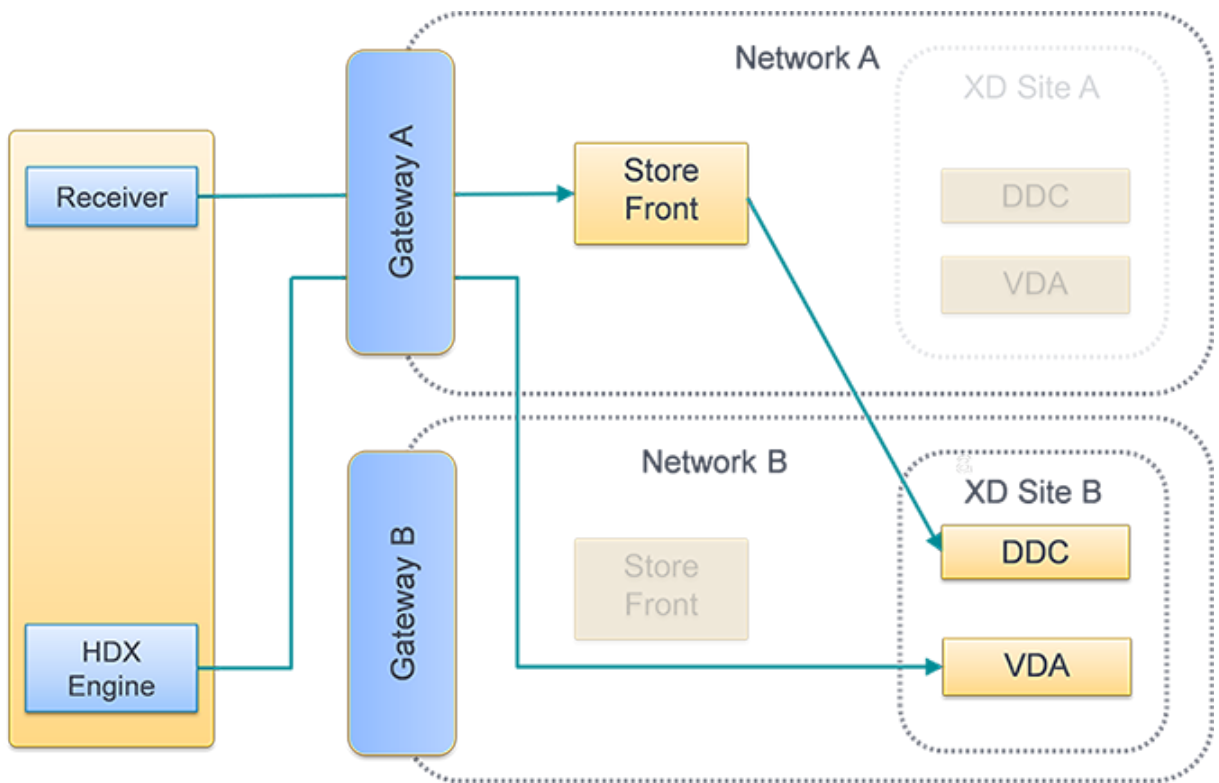
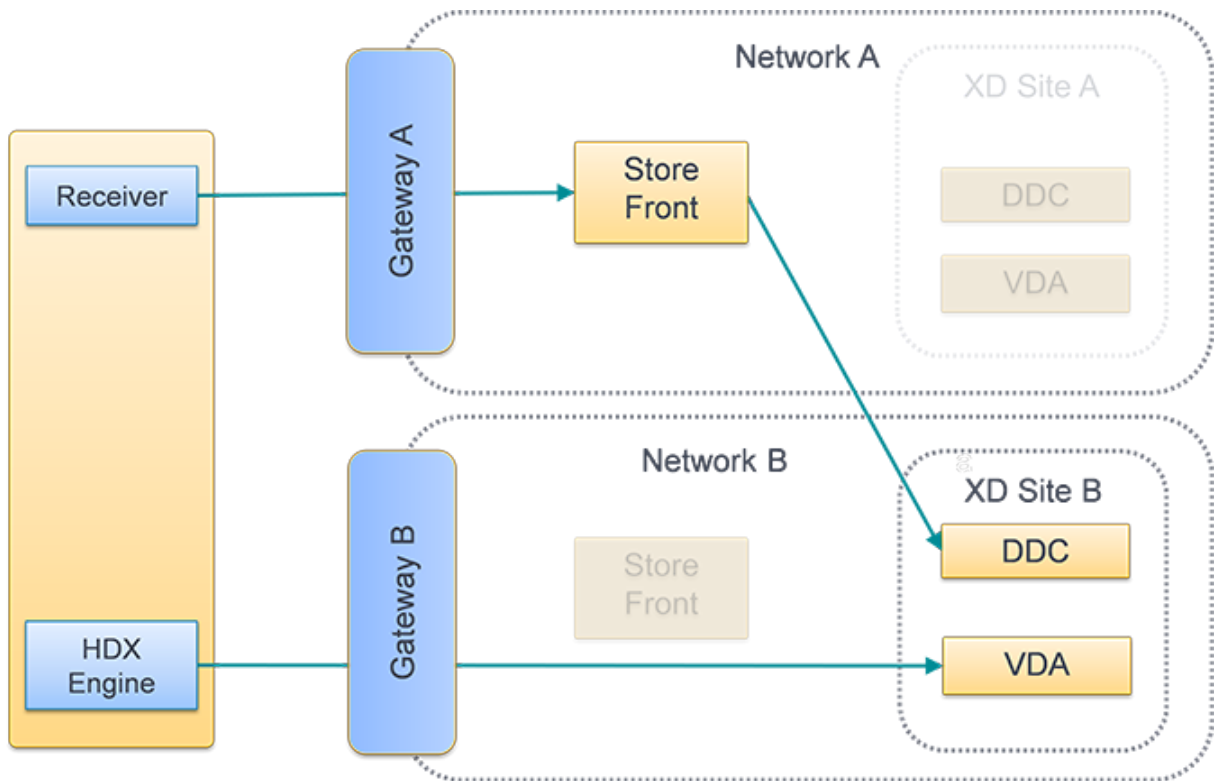


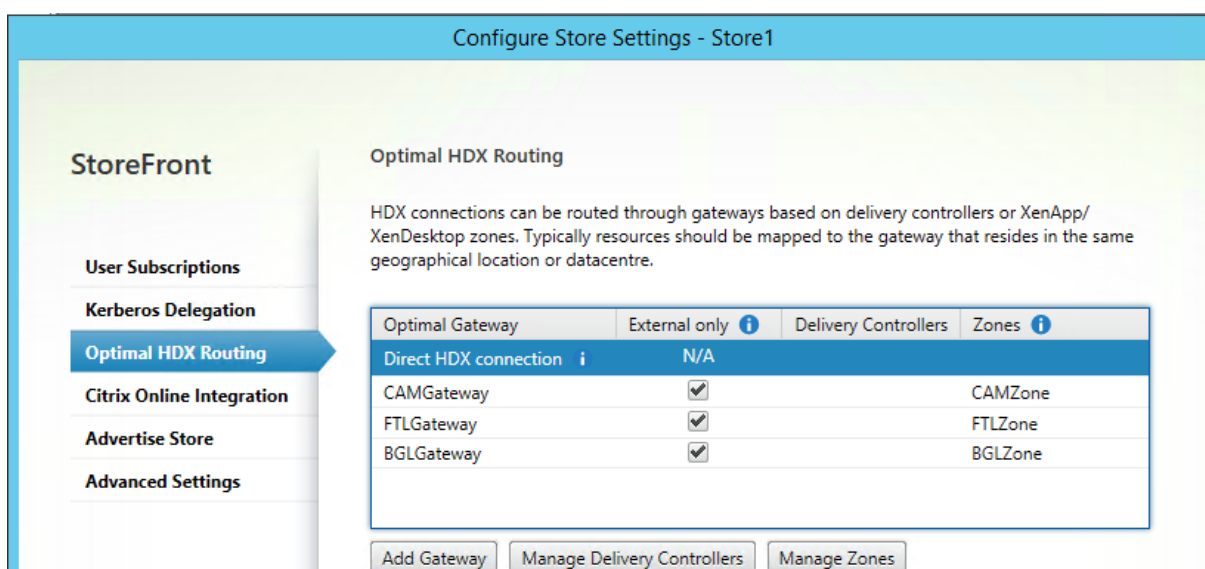
Figure 2. Routage vers la passerelle optimal



## Utilisation de la console de gestion Citrix StoreFront

Après avoir configuré des boîtiers NetScaler Gateway distincts pour vos déploiements, vous pouvez définir le boîtier optimal que les utilisateurs doivent utiliser pour accéder à chacun des déploiements.

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**.
3. Sur la page **Paramètres > Routage HDX optimal**, sélectionnez une passerelle.
4. Si vous sélectionnez la case à cocher **Externe uniquement**, cela correspond à **-enabledOnDirectAccess = false** ; l'option « Connexion HDX directe » correspond à **Set-DSFarmsWithNullOptimalGateway** pour des batteries ou des zones.



### Ajouter une nouvelle passerelle

L'une des options dans la procédure précédente consiste à **Ajouter une passerelle**. Après avoir choisi **Ajouter une passerelle**, l'écran Ajouter un boîtier NetScaler Gateway s'affiche.

1. Sur l'écran **Paramètres généraux**, définissez les paramètres Nom d'affichage, URL NetScaler Gateway et Utilisation ou rôle 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.
2. Sur l'écran **Secure Ticket Authority (STA)**, définissez les options affichées. 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.

3. Sur l'écran **Paramètres d'authentification**, entrez les paramètres spécifiant la manière dont l'utilisateur distant fournit des informations d'authentification.

## Utiliser PowerShell pour configurer un routage NetScaler Gateway optimal pour un magasin

### Paramètres de l'API PowerShell

**-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 (String)** — Chemin d'accès au magasin qui est configuré pour qu'une batterie utilise le mappage de passerelle optimale.

Exemple : « /Citrix/Store »

**-GatewayName (String)** — Nom donné pour identifier Netscaler Gateway dans StoreFront.

Exemple 1 : ExternalGateway

Exemple 2 : InternalGateway

**-Hostnames (String Array)** — Spécifie le nom de domaine complet (FQDN) et le port du boîtier NetScaler Gateway optimal.

Exemple 1 pour vServer standard port 443 : `gateway.example.com`

Exemple 2 pour vServer non standard port 500 : `gateway.example.com:500`

**-Farms (String Array)** — 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.

Vous pouvez configurer un site XenDesktop dans StoreFront sous des Delivery Controller en tant que « XenDesktop ». Cela représente une seule batterie. Peut contenir de multiples Delivery Controller dans sa liste de basculement.

Exemple : « XenDesktop »

`XenDesktop-A.example.com`

`XenDesktop-B.example.com`

`XenDesktop-C.example.com`

**-Zones (String Array)** — 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.



**-staUrls (String Array)** — 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 :

Exemple : `http://xenapp-a.example.com/scripts/ctxsta.dll,http://xendesktop-a.example.com/scripts/ctxsta.dll`

**-StasUseLoadBalancing (Boolean)** — 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. 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.

**-StasBypassDuration** — 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.

Exemple : 02:00:00

**-EnableSessionReliability (Boolean)** — Si cet attribut est défini sur **true** : garde les sessions déconnectées ouvertes lorsque 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.

**-UseTwoTickets (Boolean)** — 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. Si cet attribut est défini sur **false** : utilise un seul serveur STA.

**-EnabledOnDirectAccess (Boolean)** — 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. 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.

Lorsque les scripts PowerShell occupent plusieurs lignes comme illustré ci-dessous, chaque ligne doit se terminer avec le caractère de guillemet oblique (').

#### Conseil :

Citrix vous recommande de copier les exemples de code suivants dans l'environnement d'écriture de scripts intégré Windows PowerShell (ISE) pour valider le code PowerShell à l'aide du vérificateur de format avant de l'exécuter.

## Configurer une passerelle optimale pour une batterie

**Remarque :**

La configuration du routage HDX optimal avec l'ancienne applet de commande PowerShell, **Set-DSOptimalGatewayForFarms**, ne fonctionne pas.

Pour contourner ce problème :

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-DSSStoreOptimalGateway** 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-DSSStoreOptimalGateway -SiteId 1 -VirtualPath /Citrix/Store1 -GatewayId
2eba0524-af40-421e-9c5f-a1ccca80715f -Farms @"Controller"-EnabledOnDirectAccess
>true
```

**Exemple**

Créer ou remplacer les mappages de passerelle optimale de batteries pour le magasin **Internal**.

```
1 & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.
  ps1"
2
3 Set-DSOptimalGatewayForFarms -SiteId 1 \‘
4
5 -ResourcesVirtualPath /Citrix/Internal \‘
6 -GatewayName "gateway1" \‘
7 -Hostnames "gateway1.example.com:500" \‘
8 -Farms "XenApp","XenDesktop" \‘
9 -StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
  xendesktop.example.com/scripts/ctxsta.dll" \‘
10 -StasUseLoadBalancing:$false \‘
11 -StasBypassDuration 02:00:00 \‘
12 -EnableSessionReliability:$false \‘
13 -UseTwoTickets:$false \‘
14 -EnabledOnDirectAccess:$true
```

## Configurer une passerelle optimale pour une zone

### Exemple

Créer ou remplacer les mappages de passerelle optimale de batteries pour la zone **CAMZone**.

```
1 **& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules
   .ps1" **
2
3 **Set-DSOptimalGatewayForFarms -SiteId 1 \’**
4
5 **-ResourcesVirtualPath /Citrix/Internal \’
6 -GatewayName "gateway1" \’
7 -Hostnames "gateway1.example.com:500" \’
8 -Zones "CAMZone" \’
9 -StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
   xendesktop.example.com/scripts/ctxsta.dll" \’
10 -StasUseLoadBalancing:$false \’
11 -StasBypassDuration 02:00:00 \’
12 -EnableSessionReliability:$false \’
13 -UseTwoTickets:$false \’
14 -EnabledOnDirectAccess:$true **
```

### Exemple

Ce script renvoie tous les mappages de passerelle optimale de batteries pour le magasin appelé **Internal**.

```
Get-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```

### Exemple

Supprimer tous les mappages de passerelle optimale pour les batteries pour le magasin appelé **Internal**.

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```

Configure direct HDX connections **for** farms

**Exemple**

Ce script empêche tous les lancements ICA de transiter via une passerelle pour la liste des batteries spécifiées pour le magasin appelé **Internal**.

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/  
Store -Farms "Farm1","Farm2"
```

**Exemple**

Ce script renvoie toutes les batteries configurées pour empêcher les lancements ICA de transiter via une passerelle pour un magasin appelé **Internal**.

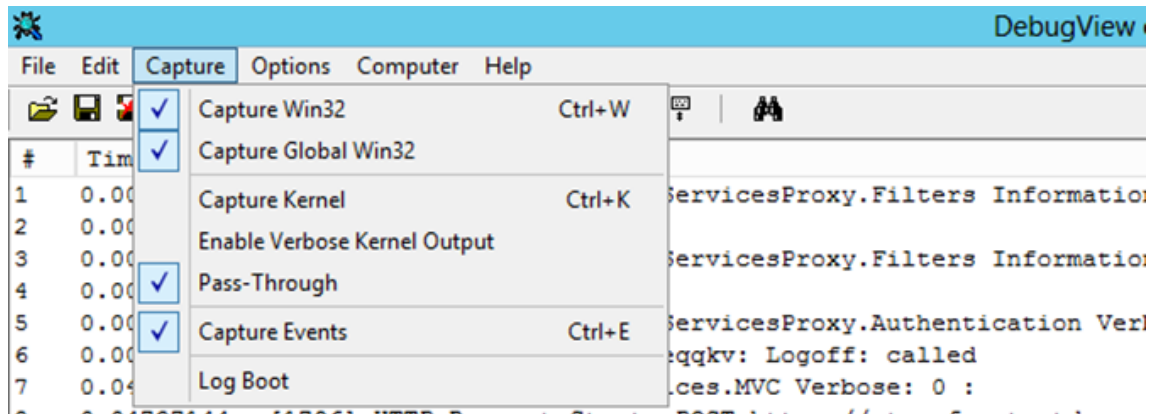
```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/  
Internal"
```

**Déterminer si vos mappages de passerelle optimale de batteries sont utilisés par StoreFront**

1. Activez le suivi StoreFront sur tous les nœuds de groupe de serveurs à l'aide de PowerShell en exécutant :

```
1 & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\  
   ImportModules.ps1" '  
2  
3 #Traces output is to c:\Program Files\Citrix\Receiver Storefront\  
   admin\trace\  
4 Set-DSTraceLevel -All -TraceLevel Verbose
```

2. Ouvrez l'outil DebugView sur le bureau d'un serveur StoreFront. Si vous utilisez un groupe de serveurs StoreFront, vous devrez peut être procéder de la sorte sur tous les nœuds pour vous assurer d'obtenir le suivi du nœud qui reçoit la demande de lancement.
3. Activez les événements Capture Global Win32.



4. Enregistrez la sortie du suivi en tant que fichier .log et ouvrez ce fichier avec Bloc-notes. Recherchez les entrées du journal affichées dans les exemples de scénarios ci-dessous.
5. Désactivez ensuite le suivi car il consomme beaucoup d'espace disque sur vos serveurs StoreFront.

```
Set-DSTraceLevel -All -TraceLevel Off
```

### Scénarios de passerelle optimale testés

```

1 - Un client externe se connecte à **Gateway1**. Le lancement est dirigé
   vers la passerelle optimale désignée **Gateway2** pour la batterie
   **Farm2**.
2
3 Set-DSOptimalGatewayForFarms -onDirectAccess=false
4
5 Farm2 est configurée pour utiliser la passerelle optimale Gateway2.
6
7 L'accès direct de Farm2 à la passerelle optimale est désactivé.
8
9 La passerelle optimale Gateway2 sera utilisée pour le lancement.
10
11 - Un client interne se connecte à l'aide de StoreFront. Le lancement
   est dirigé vers la passerelle optimale désignée Gateway1 pour la
   batterie Farm1.
12
13 'Set-DSOptimalGatewayForFarms -onDirectAccess=true'
14
15 Aucune passerelle identifiée dynamiquement dans la demande.
   StoreFront a été contacté directement.
16
17 Farm1 est configurée pour utiliser la passerelle optimale Gateway1.
18

```

```
19     L'accès direct de Farm1 à la passerelle optimale est activé.  
20  
21     La passerelle optimale Gateway1 sera utilisée pour le lancement.  
22  
23 -   Un client interne se connecte à l'aide de Gateway1. Le lancement de  
      ressources sur Farm1 ne peut transiter par aucune passerelle et  
      StoreFront est contacté directement.  
24  
25     'Set-DSFarmsWithNullOptimalGateway'  
26  
27     Passerelle identifiée dynamiquement dans la demande : Gateway1  
28  
29     Farm1 est configurée pour ne pas utiliser de passerelle. Aucune  
      passerelle ne sera utilisée pour le lancement.
```

## Forcer les connexions via Citrix Gateway à l'aide de la fonction Passerelle optimale de StoreFront

January 17, 2019

Le paramètre **Passerelle optimale**, disponible dans StoreFront, permet de forcer les applications à démarrer via Citrix Gateway. Il s'applique lors de l'accès à StoreFront via Citrix Receiver pour se connecter au serveur virtuel Citrix Gateway et lors du lancement de ressources à partir de Citrix Virtual Apps and Desktops à l'aide de l'authentification Single Sign-On.

Configuration système requise :

- 2 VPX Citrix Gateway
- 2 DDC XenDesktop 7.1
- 2 serveurs StoreFront séparés

Depuis un appareil joint à un domaine sur le réseau LAN/MPLS, les utilisateurs se connectent une seule fois avec les informations d'identification du domaine à l'invite de connexion Windows. Les utilisateurs doivent lancer leurs applications Citrix à l'aide d'un Receiver natif, via une connexion SLL protégée par Citrix ADC. Avant d'essayer d'utiliser cette fonctionnalité, vérifiez que les utilisateurs peuvent lancer des sessions directement avec StoreFront et avec Citrix ADC en mode proxy ICA. Assurez-vous également que vous avez déjà configuré NetScaler et StoreFront en utilisant [CTX139963](#) et Citrix Receiver avec authentification pass-through en utilisant [CTX133855](#).

## Configurer le routage Optimal Citrix Gateway

L'architecture Passerelle optimale vous permet de diriger l'authentification utilisateur vers le serveur StoreFront. Elle lance la session ICA via Citrix ADC pour garantir une connexion sécurisée. Le traitement des informations d'identification est sécurisé entre la machine Windows et les serveurs StoreFront. Avec la personnalisation de StoreFront, le ticket ICA dirige la connexion utilisateur via Citrix ADC.

Pour configurer le routage Optimal Citrix Gateway pour un magasin, modifiez le fichier `web.config` situé sur `C:\inetpub\wwwroot\Citrix\Store\web.config` pour instruire StoreFront de diriger les connexions utilisateur via Citrix Gateway.

Modifiez `enabledOnDirectAccess="true"` dans la clé `optimalGatewayForFarmsCollection`.

```
1 <optimalGatewayForFarmsCollection>
2   <optimalGatewayForFarms enabledOnDirectAccess="true">
3     <farms>
4       <farm name="farmname" />
5     </farms>
6     <optimalGateway key="_" name="deploymentname" stasUseLoadBalancing=
7       "{
8     true | false }
9     "
10    stasBypassDuration="hh:mm:ss" enableSessionReliability="{
11    true | false }
12    "
13    useTwoTickets="{
14    true | false }
15  ">
16    <hostnames>
17      <add hostname="appliancefqdn:port" />
18    </hostnames>
19    <staUrls>
20      <add staUrl="https://stapath/scripts/ctxsta.dll" />
21    </staUrls>
22  </optimalGateway>
23 </optimalGatewayForFarms>
24 <optimalGatewayForFarms>
25   ...
26 </optimalGatewayForFarms>
27 </optimalGatewayForFarmsCollection>
```

## Intégrer avec Citrix Gateway et Citrix ADC

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Utilisez Citrix Gateway avec StoreFront pour fournir un accès distant sécurisé aux utilisateurs en dehors du réseau d'entreprise et Citrix ADC pour fournir l'équilibrage de charge.

### Planifier l'utilisation des certificats de serveur et des passerelles

L'intégration de StoreFront avec Citrix ADC et Citrix Gateway requiert de planifier l'utilisation des certificats de serveur et des passerelles. Déterminez quels composants Citrix vont nécessiter des certificats de serveur dans votre déploiement :

- Planifiez d'obtenir des certificats auprès de serveurs connectés à Internet et des passerelles auprès d'autorités de certification externes. Il est possible que les machines clientes ne fassent pas automatiquement confiance aux certificats signés par une autorité de certification interne.
- Planifiez pour des deux noms de serveurs externes et internes. De nombreuses organisations ont des espaces de noms séparés pour une utilisation interne et externe, tels que `example.com` (externe) et `example.net` (interne). Un seul certificat peut contenir ces deux types de noms à l'aide de l'extension Autre nom de l'objet (SAN). Cela n'est généralement pas recommandé. Une autorité de certification publique émettra uniquement un certificat si le domaine de niveau supérieur (TLD) est enregistré auprès de l'IANA. Dans ce cas, certains noms de serveurs internes communément utilisés (tels que `exemple.local`) ne peuvent pas être utilisés et des certificats distincts pour les noms internes et externes sont requis.
- Utilisez des certificats distincts pour les serveurs externes et internes, lorsque cela est possible. Une passerelle peut prendre en charge plusieurs certificats en liant un certificat différent à chaque interface.
- Évitez de partager des certificats entre des serveurs accessibles via Internet et non accessibles via Internet. Ces certificats seront probablement différents, avec des périodes de validité différentes et des stratégies de révocation différentes de celles des certificats émis par vos autorités de certification internes.
- Partagez des certificats « génériques » uniquement entre des services équivalents. Évitez de partager un certificat entre des types de serveurs différents (par exemple les serveurs StoreFront et d'autres types de serveurs). Évitez de partager un certificat entre des serveurs se trouvant sous un contrôle administratif différent, ou qui ont des stratégies de sécurité différentes. Exemples typiques de serveurs qui fournissent un service équivalent :
  - Un groupe de serveurs StoreFront et le serveur chargé d'en équilibrer la charge.



- Un groupe de passerelles accessibles via Internet au sein du répartiteur GSLB.
- Un groupe de Controller XenApp et XenDesktop 7.x, qui fournissent des ressources équivalentes.
- Planifiez le stockage de la clé privée sur du matériel sécurisé. Les passerelles et les serveurs, y compris certains modèles de Citrix ADC, peuvent stocker la clé privée de manière sécurisée au sein d'un module de sécurité matériel (HSM) ou d'un module de plateforme sécurisée (TPM). Pour des raisons de sécurité, ces configurations ne sont généralement pas conçues pour prendre en charge le partage de certificats et de leurs clés privées ; consultez la documentation accompagnant le composant. Si vous mettez en place un répartiteur GSLB avec Citrix Gateway, cela peut nécessiter que chaque passerelle au sein du répartiteur GSLB dispose d'un certificat identique, contenant tous les noms de domaine complets que vous souhaitez utiliser.

Pour plus d'informations sur la sécurisation de votre déploiement Citrix, consultez l'article technique [End-To-End Encryption with Citrix Virtual Apps and Desktops](#) et la section [Sécuriser](#) dans la documentation Citrix Virtual Apps and Desktops.

## Configurer la connexion à StoreFront lorsque l'authentification est désactivée sur Citrix Gateway VIP

Connectez-vous à StoreFront lorsque l'authentification est désactivée sur Citrix Gateway VIP. Cette procédure fonctionne dans deux scénarios :

**Réseaux internes.** Le lancement d'application échoue depuis les emplacements distants car les STA ne peuvent pas être utilisées lorsque l'authentification est désactivée sur Citrix Gateway si l'en-tête X-Citrix-Gateway est transmis à StoreFront.

**Citrix Receiver pour Web.** Les clients Receiver ne s'authentifient pas si l'authentification n'est pas activée sur Citrix Gateway VIP.

### Changements sur le serveur StoreFront

1. Désactivez le champ **Exiger la cohérence des jetons** :
  - StoreFront 3.0
    - a) Modifiez le fichier `web.config` pour le site Web du magasin. Par exemple, si le nom d'un magasin StoreFront est `NoAuth`, le chemin d'accès au fichier `web.config` sur le serveur StoreFront est `inetpub\wwwroot\Citrix\NoAuth`.
    - a) Recherchez la ligne suivante dans le fichier `web.config` et définissez la valeur sur `true`.  
Avant  

```
<resourcesGateways requireTokenConsistency="true">
```

  
Après  

```
<resourcesGateways requireTokenConsistency="false">
```

**Remarque :**

Sur StoreFront 3.x, l'option **Exiger la cohérence des jetons** est une case à cocher dans l'interface graphique. Pour plus d'informations, consultez la section [Paramètres de magasin avancés](#).

- b) Enregistrez le fichier `web.config`, puis redémarrez le service IIS.
2. Ouvrez la **console de gestion Citrix StoreFront**.
3. Cliquez sur **Citrix StoreFront Receiver pour Web**.
4. Sélectionnez le Receiver correspondant pour le site Web, puis sélectionnez **Choisir les méthodes d'authentification**.
5. Assurez-vous que la case à cocher **Authentification pass-through via Citrix Gateway** n'est pas sélectionnée.

**Remarque :**

Nous supposons que Citrix Gateway et l'accès à distance sont configurés sur le serveur StoreFront.

## Changements sur Citrix Gateway

1. Ouvrez le serveur virtuel Citrix Gateway.
2. Cliquez sur l'onglet **Authentification** et assurez-vous que la case à cocher **Activer l'authentification** n'est pas sélectionnée.
3. Liez la stratégie de session correspondante au serveur virtuel Citrix Gateway.
4. Testez la connexion.

## Ajouter une connexion NetScaler Gateway

February 20, 2019

Utilisez la tâche Ajouter un boîtier NetScaler Gateway pour ajouter des déploiements NetScaler Gateway au travers desquels les utilisateurs peuvent accéder à vos magasins. Vous devez activer la méthode d'authentification pass-through de NetScaler Gateway avant de pouvoir configurer l'accès distant à vos magasins au travers de NetScaler Gateway. Pour de plus amples informations sur la configuration de NetScaler Gateway pour StoreFront, consultez la section [Utilisation de WebFront pour l'intégration avec StoreFront](#).

**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 les modifications terminées,

[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 NetScaler Gateway.
3. Cliquez sur **Ajouter** et sélectionnez Paramètres généraux, et donnez un nom au 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.

4. 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.

5. Si vous ajoutez un déploiement Access Gateway 5.0, passez à l'étape 7. 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.

6. Si vous ajoutez un boîtier exécutant NetScaler Gateway, 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 tokencode 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 tokencode 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 8.

7. 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. Si vous ajoutez un cluster, cliquez sur **Suivant** puis passez à l'étape 9.
8. Si vous configurez StoreFront pour NetScaler Gateway 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 11.

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.

9. 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**.
10. 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 **Next**.

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.

11. 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.

12. 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.

13. Cliquez sur **Créer** pour ajouter les détails de votre déploiement NetScaler Gateway. Une fois le déploiement ajouté, cliquez sur **Terminer**.

Pour de plus amples informations sur la mise à jour des détails de vos déploiements, consultez la section [Configurer les paramètres de connexion à NetScaler Gateway](#).

Pour fournir l'accès aux magasins via NetScaler Gateway, un point balise interne et au moins deux points balises externes sont requis. Citrix Receiver utilise des points balises pour déterminer si les utilisateurs sont connectés à des réseaux locaux ou publics, puis sélectionne la méthode d'accès appropriée. Par défaut, StoreFront utilise l'adresse URL du serveur ou l'URL à charge équilibrée de votre déploiement comme point balise interne. Les adresses URL du site Web de Citrix et du serveur virtuel ou du point d'ouverture de session utilisateur (pour Access Gateway 5.0) du premier déploiement NetScaler Gateway que vous ajoutez sont utilisées en tant que points balises externes par défaut. Pour plus d'informations sur la modification des points balises, consultez la section [Configurer des points balises](#).

Pour permettre aux utilisateurs d'accéder à vos magasins via NetScaler Gateway, assurez-vous de [configurer l'accès à distance des utilisateurs](#) pour ces magasins.

## Importer un boîtier NetScaler Gateway

February 26, 2019

Les paramètres de l'accès à distance configurés dans la console d'administration de NetScaler doivent être identiques à ceux configurés dans StoreFront. Cet article vous explique comment importer un boîtier NetScaler Gateway de façon à ce que NetScaler et StoreFront soient correctement configurés pour fonctionner ensemble.

## Exigences

- NetScaler 11.1.51.21 ou version ultérieure est requis pour exporter de multiples vServers de passerelle sur un fichier ZIP.

### Remarque :

NetScaler peut uniquement exporter des vServers de passerelle créés à l'aide de l'assistant de XenApp et XenDesktop.

- Il doit être possible de résoudre le DNS et pour StoreFront de contacter toutes les adresses URL de serveurs STA (Secure Ticket Authority) du fichier GatewayConfig.json dans le fichier ZIP généré par NetScaler.
- Le fichier GatewayConfig.json du fichier ZIP généré par NetScaler doit contenir l'adresse URL d'un site Citrix Receiver pour Web existant sur le serveur StoreFront. NetScaler 11.1 (et versions supérieures) se charge de cette tâche en contactant le serveur StoreFront et en énumérant tous les magasins et sites Citrix Receiver pour Web existants avant de générer le fichier ZIP pour l'exportation.
- StoreFront doit être en mesure de résoudre l'URL de rappel du DNS sur l'adresse IP du vServer VPN de passerelle pour garantir le succès de l'authentification à l'aide de la passerelle importée.

L'URL de rappel et de la combinaison de ports que vous utilisez sont généralement les mêmes que l'adresse URL et la combinaison de ports de la passerelle, à condition que StoreFront puisse résoudre cette adresse URL.

ou

L'URL de rappel et la combinaison de ports peuvent être différentes de l'adresse URL et de la combinaison de ports de la passerelle si vous utilisez des espaces de noms DNS externes et internes différents dans votre environnement. Si votre passerelle se trouve dans une zone démilitarisée (DMZ) et utilise une adresse URL `<example.com>` et que StoreFront est hébergé sur votre réseau d'entreprise privé et utilise une adresse URL `<example.local>`, vous pouvez utiliser une adresse URL de rappel `<example.local>` afin de pointer vers le vServer de passerelle dans la DMZ.

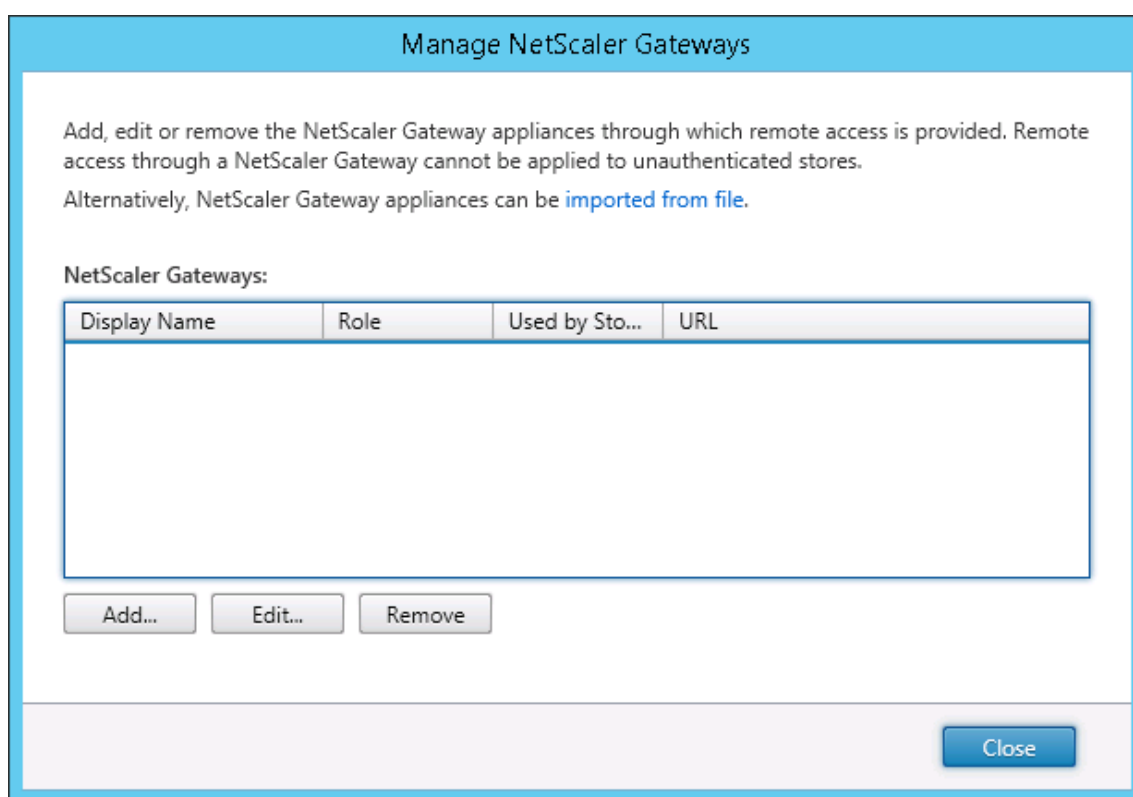
## Importer un boîtier NetScaler Gateway à l'aide de la console

Vous pouvez importer un ou plusieurs boîtiers NetScaler Gateway en important un fichier de configuration NetScaler.

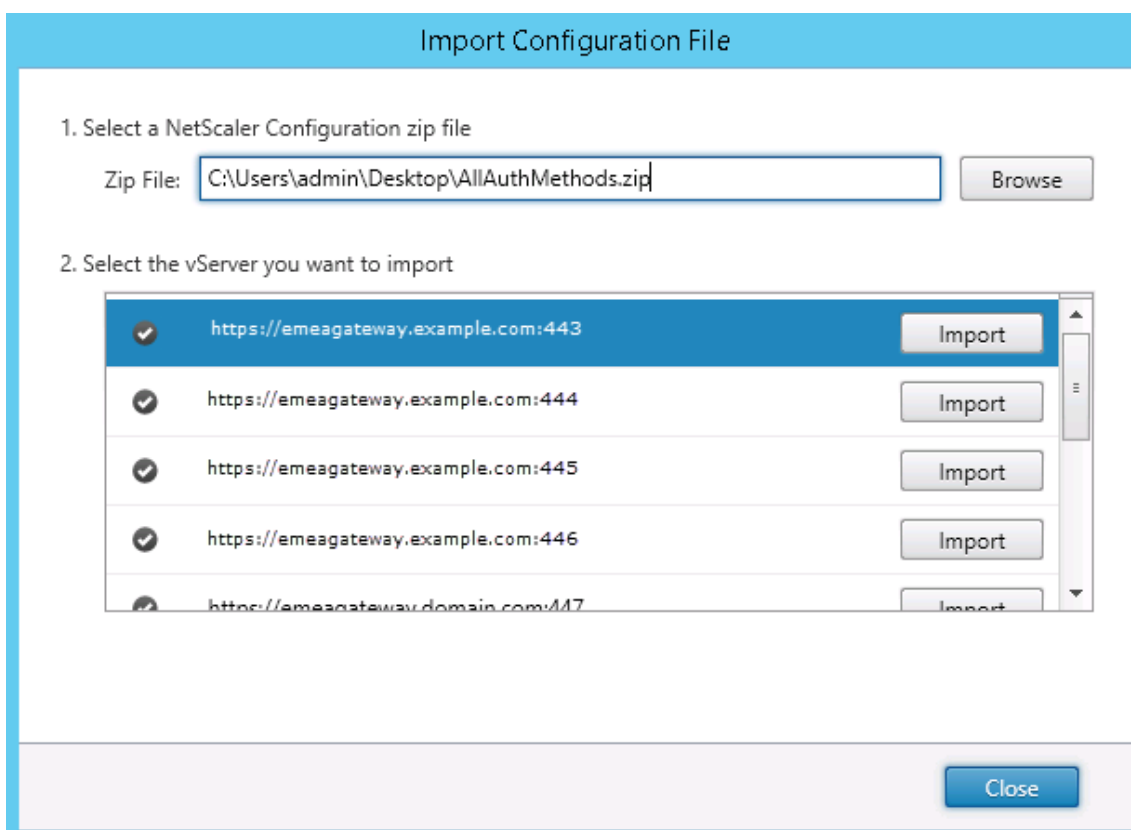
### Important :

Citrix ne prend pas en charge la modification manuelle du fichier de configuration exporté depuis NetScaler.

1. Sélectionnez **Magasin** dans le panneau de gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Gérer NetScaler Gateway**.
2. Sur l'écran Gérer NetScaler Gateway, cliquez sur le lien **importé à partir d'un fichier**.



3. Accédez au fichier zip de configuration de Netscaler.
4. Une liste des vServers de passerelle du fichier ZIP sélectionné s'affiche. Sélectionnez le vServer de passerelle que vous souhaitez importer et cliquez sur **Importer**. Si vous répétez l'importation d'un vServer, le bouton Importer est remplacé par un bouton de mise à jour. Si vous choisissez **Mettre à jour**, vous aurez la possibilité plus tard de remplacer ou créer une nouvelle passerelle.



5. Vérifiez le type d'ouverture de session pour la passerelle sélectionnée et spécifiez une adresse URL de rappel si nécessaire. Le type d'ouverture de session est la méthode d'authentification que vous avez configurée sur le boîtier NetScaler Gateway pour les utilisateurs de Citrix Receiver. Certains types d'ouverture de session nécessitent des adresses URL de rappel (voir le tableau).
  - Cliquez sur **Vérifier** pour vérifier que l'URL de rappel est valide et accessible depuis le serveur StoreFront.

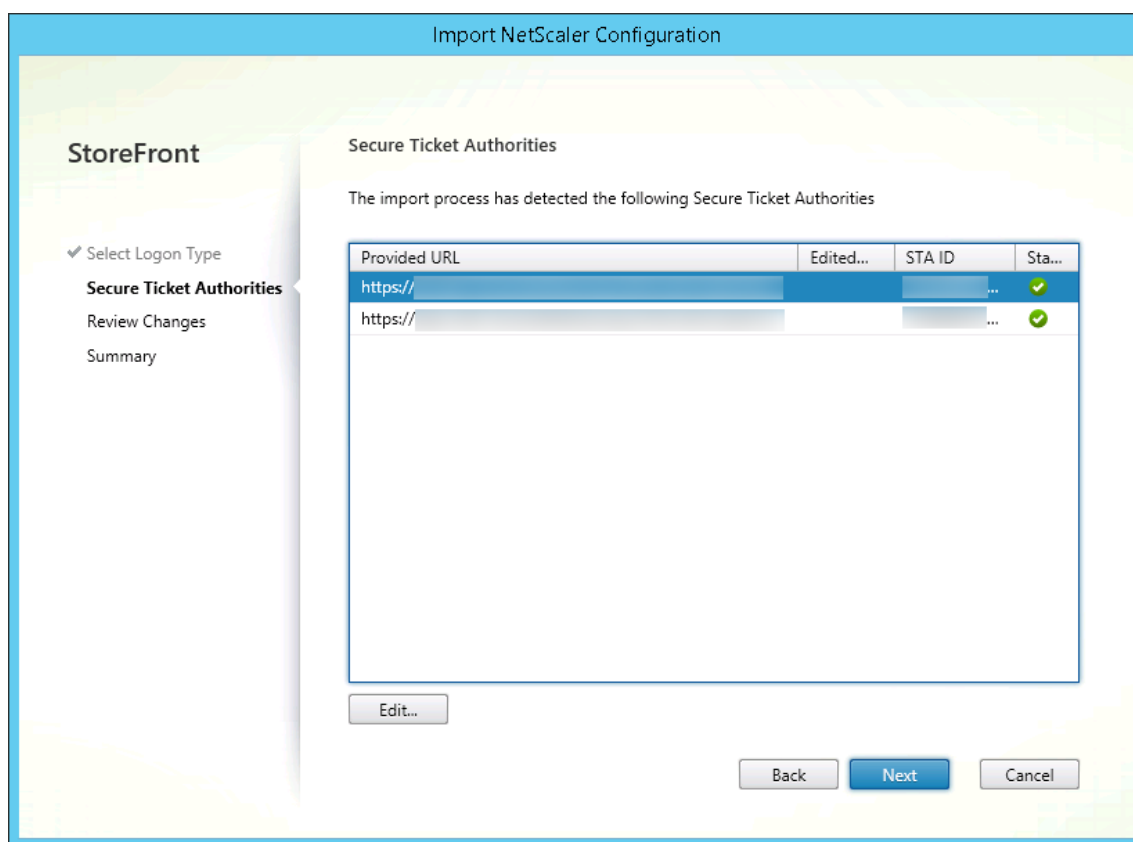


Type de connexion dans la console	LogonType dans le fichier JSON	URL de rappel requise
Domaine	Domaine	Non
Domaine et jeton de sécurité	DomainAndRSA	Non
Jeton de sécurité	RSA	Oui
Carte à puce - Sans solution alternative	SmartCard	Oui
Carte à puce - Domaine	SmartCardDomain	Oui
Carte à puce - Domaine et jeton de sécurité	SmartCardDomainAndRSA	Oui
Carte à puce - Jeton de sécurité	SmartCardRSA	Oui
Carte à puce - Authentification SMS	SmartCardSMS	Oui
Authentification SMS	SMS	Oui

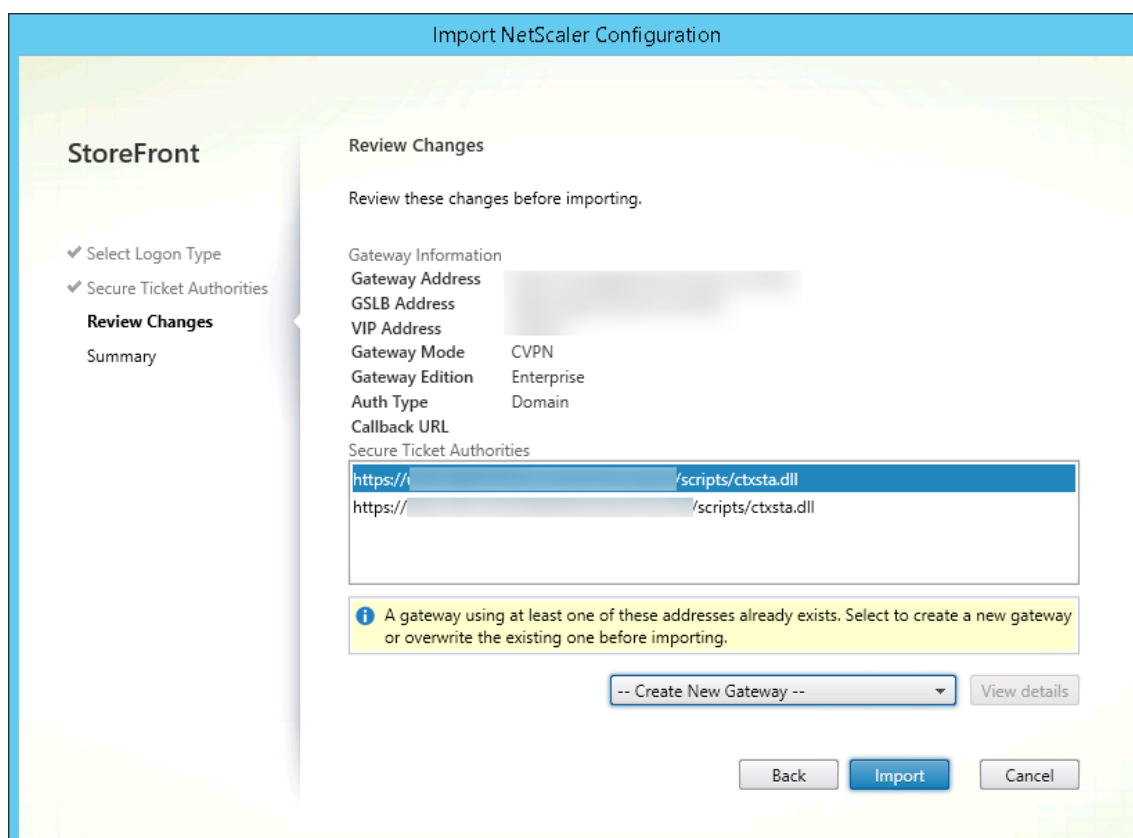
Si une URL de rappel est requise, StoreFront remplira automatiquement l'adresse URL de rappel en fonction de l'adresse URL de passerelle trouvée dans le fichier ZIP. Vous pouvez modifier cette adresse au profit de toute adresse URL valide qui pointe vers l'adresse IP du vServer NetScaler Gateway.

Si vous souhaitez utiliser [Smart Access](#), une adresse URL de rappel est requise.

6. Cliquez sur **Next**.
7. StoreFront contacte toutes les URL de serveurs STA (Secure Ticket Authorities) répertoriées dans le fichier ZIP à l'aide du DNS de façon à confirmer que les serveurs STA sont fonctionnels. L'importation ne se poursuivra pas si une ou plusieurs des URL STA ne sont pas valides.



8. Cliquez sur **Next**.
9. Vérifiez les détails de l'importation. Si une passerelle avec la même URL et combinaison de ports de passerelle (Gateway:port) existe déjà, utilisez le menu déroulant pour sélectionner une passerelle à remplacer ou créez une nouvelle passerelle.



StoreFront utilise la combinaison GatewayURL:port pour déterminer si une passerelle que vous essayez d'importer correspond à une passerelle existante que vous pourriez vouloir mettre à jour. Si une passerelle dispose d'une combinaison GatewayURL:port différente, StoreFront traite cette dernière comme une nouvelle passerelle. Ce tableau des paramètres de passerelle affiche les paramètres que vous pouvez mettre à jour.

Paramètre de passerelle	Peut être mis à jour
Combinaison Port :adresse URL de passerelle	Non
URL GSLB	Oui
Empreinte numérique et certificat de confiance Netscaler	Oui
URL de rappel	Oui
URL du site Receiver pour Web	Oui
Adresse de passerelle/VIP	Oui
URL et ID de la STA	Oui
Tous les Types d'ouverture de session	Oui

10. Cliquez sur **Importer**. Si le serveur StoreFront fait partie d'un groupe de serveurs, un message vous rappelle de propager les paramètres de passerelle importés aux autres serveurs du groupe.
11. Cliquez sur **Terminer**.

Pour importer une autre configuration vServer, répétez les étapes ci-dessus.

**Remarque :**

La passerelle par défaut d'un magasin est la passerelle à laquelle les Citrix Receiver natifs essaient de se connecter, sauf s'ils sont configurés pour utiliser une autre passerelle. Si aucune passerelle n'est configurée pour le magasin, la première passerelle importée à partir du fichier .zip deviendra la passerelle par défaut utilisée par les Citrix Receiver natifs. L'importation d'autres passerelles ne modifie pas la passerelle par défaut déjà définie pour le magasin.

## Importer plusieurs NetScaler Gateway à l'aide de PowerShell

### Read-STFNetScalerConfiguration

- Copiez le fichier ZIP sur le bureau de l'administrateur StoreFront actuellement connecté.
- Lisez le contenu du fichier ZIP de NetScaler en mémoire et examinez les trois passerelles qu'il contient à l'aide de leurs valeurs d'index.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
  USERPROFILE\desktop\GatewayConfig.zip"
```

Affichez les trois les objets passerelle en mémoire qui ont été lus dans le package d'importation ZIP de Netscaler à l'aide de l'applet de commande **Read-STFNetScalerConfiguration**.

```
1 $ImportedGateways.Document.Gateways[0]
2 $ImportedGateways.Document.Gateways[1]
3 $ImportedGateways.Document.Gateways[2]
4
5 GatewayMode           : CVPN
6 CallbackUrl           :
7 GslbAddressUri        : https://gslb.example.com/
8 AddressUri            : https://emeagateway.example.com/
9 Address               : https://emeagateway.example.com:443
10 GslbAddress           : https://gslb.example.com:443
11 VipAddress           : 10.0.0.1
12 Stas                 : {
13   STA298854503, STA909374257 }
14
15 StaLoadBalance        : True
```

```
16 CertificateThumbprints : {
17   F549AFAA29EBF61E8709F2316B3981AD503AF387 }
18
19 GatewayAuthType      : Domain
20 GatewayEdition       : Enterprise
21 ReceiverForWebSites  : {
22   Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
     ReceiverForWebSite }
23
24
25 GatewayMode          : CVPN
26 CallbackUrl         :
27 GslbAddressUri       : https://gslb.example.com/
28 AddressUri           : https://emeagateway.example.com/
29 Address              : https://emeagateway.example.com:444
30 GslbAddress          : https://gslb.example.com:443
31 VipAddress           : 10.0.0.2
32 Stas                 : {
33   STA298854503, STA909374257 }
34
35 StaLoadBalance       : True
36 CertificateThumbprints : {
37   F549AFAA29EBF61E8709F2316B3981AD503AF387 }
38
39 GatewayAuthType      : DomainAndRSA
40 GatewayEdition       : Enterprise
41 ReceiverForWebSites  : {
42   Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
     ReceiverForWebSite }
43
44
45 GatewayMode          : CVPN
46 CallbackUrl         : https://emeagateway.example.com:445
47 GslbAddressUri       : https://gslb.example.com/
48 AddressUri           : https://emeagateway.example.com/
49 Address              : https://emeagateway.example.com:445
50 GslbAddress          : https://gslb.example.com:443
51 VipAddress           : 10.0.0.2
52 Stas                 : {
53   STA298854503, STA909374257 }
54
55 StaLoadBalance       : True
56 CertificateThumbprints : {
57   F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
```

```

59 GatewayAuthType      : SmartCard
60 GatewayEdition       : Enterprise
61 ReceiverForWebSites  : {
62 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
   ReceiverForWebSite }

```

### Import-STFNetScalerConfiguration sans spécifier d'URL de rappel

Copiez le fichier ZIP sur le bureau de l'administrateur StoreFront actuellement connecté. Lisez le package d'importation ZIP de NetScaler en mémoire et examinez les trois passerelles qu'il contient à l'aide de leurs valeurs d'index.

```

1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
  USERPROFILE\desktop\GatewayConfig.zip"

```

Importez trois nouvelles passerelles dans StoreFront à l'aide de l'applet de commande **Import-STFNetScalerConfiguration** et spécifiez les index de passerelle dont vous avez besoin. L'utilisation du paramètre **-Confirm:\$False** empêche l'interface Powershell de vous inviter à autoriser chaque passerelle à importer. Supprimez cette option si vous souhaitez importer une passerelle à la fois.

```

1 ""
2 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 0 -Confirm:$False
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 1 -Confirm:$False
4 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 2 -Confirm:$False
5 ""

```

### Import-STFNetScalerConfiguration en spécifiant votre propre URL de rappel

Importez trois nouvelles passerelles dans StoreFront à l'aide de l'applet de commande **Import-STFNetScalerConfiguration** et spécifiez une URL de rappel de votre choix à l'aide du paramètre **-callbackURL**.

```

1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
  USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
  Confirm:$False
4

```

```
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
   GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -  
   Confirm:$False  
6  
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
   GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -  
   Confirm:$False
```

### Import-STFNetScalerConfiguration annule la méthode d'authentification stockée dans le fichier d'importation et spécifie votre propre URL de rappel

Importez trois nouvelles passerelles dans StoreFront à l'aide de l'applet de commande **Import-STFNetScalerConfiguration** et spécifiez une URL de rappel de votre choix à l'aide du paramètre `-callbackURL`.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:  
   USERPROFILE\desktop\GatewayConfig.zip"  
2  
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
   GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://  
   emeagatewaycb.example.com:443" -Confirm:$False  
4  
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
   GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://  
   emeagatewaycb.example.com:444" -Confirm:$False  
6  
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
   GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://  
   emeagatewaycb.example.com:445" -Confirm:$False
```

## Configurer les paramètres de connexion à NetScaler Gateway

February 20, 2019

Les tâches ci-dessous décrivent comment mettre à jour les détails des déploiements NetScaler Gateway par le biais desquels les utilisateurs accèdent à vos magasins. Pour de plus amples informations sur la configuration de NetScaler Gateway pour StoreFront, consultez la section [Utilisation de WebFront pour l'intégration avec StoreFront](#).

Si vous apportez des modifications à vos déploiements NetScaler Gateway, assurez-vous que les utilisateurs qui accèdent à des magasins via ces déploiements mettent à jour Citrix Receiver avec les

informations de connexion modifiées. Lorsqu'un site Citrix Receiver pour Web est configuré pour un magasin, les utilisateurs peuvent obtenir un fichier de provisioning Citrix Receiver mis à jour à partir du site. Sinon, vous pouvez [exporter un fichier de provisioning](#) pour le magasin et mettre ce fichier à la disposition de vos utilisateurs.

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 les modifications terminées,

[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.

## Modifier les paramètres NetScaler Gateway généraux

Utilisez la tâche Modifier les paramètres généraux pour modifier les noms de déploiement NetScaler Gateway affichés aux utilisateurs et mettre à jour StoreFront avec les modifications apportées au serveur virtuel ou à l'adresse URL du point d'ouverture de session, et le mode de déploiement de votre infrastructure 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 Magasins dans le panneau gauche de la console de gestion Citrix StoreFront, puis cliquez sur Gérer NetScaler Gateway.
3. Indiquez 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.

4. 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.

5. Si votre déploiement exécute Access Gateway 5.0, passez à l'étape 7. Sinon, spécifiez l'adresse IP de sous-réseau du boîtier NetScaler Gateway, si nécessaire.



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.

6. Si votre boîtier exécute NetScaler Gateway, 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 tokencode 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 tokencode 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**.

7. Si votre déploiement comprend NetScaler Gateway ou un seul boîtier Access Gateway 5.0, renseignez l'URL du service d'authentification NetScaler Gateway dans la case URL de rappel. 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.

## **Gérer les boîtiers Access Gateway 5.0**

Utilisez la tâche **Gérer les boîtiers** pour ajouter, modifier ou supprimer de StoreFront les adresses IP ou de noms de domaine complets des boîtiers de votre cluster Access Gateway 5.0.

## Activer l'authentification silencieuse de l'utilisateur via Access Controller

Utilisez la tâche Activer l'authentification silencieuse pour ajouter, modifier ou supprimer des adresses URL du service d'authentification exécuté sur les serveurs Access Controller dans votre cluster Access Gateway 5.0. Saisissez les adresses URL de plusieurs serveurs pour activer la tolérance aux pannes en dressant la liste des serveurs dans l'ordre de priorité pour définir la séquence de basculement. 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.

## Gérer les Secure Ticket Authorities

Utilisez la tâche Secure Ticket Authority pour mettre à jour la liste de STA (Secure Ticket Authorities) depuis laquelle StoreFront obtient des tickets de session utilisateur et pour configurer la fiabilité de session. 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.

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 des résultats, sélectionnez un déploiement NetScaler Gateway. Dans le panneau Actions, cliquez sur Gérer NetScaler Gateway.
3. Cliquez sur Ajouter pour entrer l'adresse URL d'un serveur exécutant la STA. Spécifiez les adresses URL de plusieurs STA pour activer la tolérance aux pannes en dressant la liste des serveurs dans l'ordre de priorité pour définir le basculement. Pour modifier une adresse URL, sélectionnez l'entrée correspondante dans la liste Adresses URL Secure Ticket Authority, puis cliquez sur Modifier. Sélectionnez une adresse URL dans la liste puis cliquez sur Supprimer pour empêcher StoreFront de se procurer des tickets de session auprès de cette STA.
4. 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.

## Supprimer des déploiements NetScaler Gateway

Dans le panneau **Actions**, utilisez la tâche Supprimer de **Gérer NetScaler Gateway** pour supprimer les détails d'un déploiement NetScaler Gateway de StoreFront. Une fois qu'un déploiement NetScaler Gateway a été supprimé, les utilisateurs ne peuvent plus accéder aux magasins au travers de ce déploiement.

## Équilibrage de charge avec NetScaler

February 20, 2019

Cet article contient les informations nécessaires à l'utilisation de NetScaler pour équilibrer la charge de deux serveurs StoreFront ou plus.

### Configurer un groupe de serveurs StoreFront et l'équilibrage de charge NetScaler

#### Planifier votre déploiement StoreFront avec équilibrage de charge

Cet article contient des instructions sur la manière de déployer un groupe de serveurs StoreFront contenant deux ou plusieurs serveurs StoreFront dans une configuration d'équilibrage de charge active. Cet article fournit des informations sur la manière de configurer un boîtier NetScaler pour l'équilibrage de charge des requêtes entrantes depuis Citrix Receiver et Citrix Receiver pour Web entre les nœuds StoreFront du groupe de serveurs. Cet article explique également comment configurer le nouveau moniteur StoreFront pour une utilisation avec un équilibrage de charge NetScaler ou tiers.

Pour des exemples de configuration d'équilibrage de charge, veuillez consulter les sections « Scénario 1 » et « Scénario 2 ».

#### Testé avec l'environnement suivant

- Quatre nœuds StoreFront 3.0 Windows Server 2012 R2 dans un seul groupe de serveurs.
- Un équilibrage de charge NetScaler 10.5 configuré pour l'équilibrage de charge « persistant » CookieInsert et Least Connection.
- Un client test Windows 8.1 avec Fiddler 4.0 et Citrix Receiver pour Windows 4.3 installés.

#### Certificat de serveur requis pour le déploiement avec charge équilibrée, si vous prévoyez d'utiliser le protocole HTTPS

Lisez la section [Planifier l'utilisation des certificats de serveur et des passerelles](#).

Tenez compte des options suivantes avant d'effectuer l'achat d'un certificat provenant d'une autorité de certification commerciale ou d'en émettre un à partir de votre autorité de certification d'entreprise.

- **Option 1** : permet d'utiliser un certificat générique *\*.exemple.com* sur le vServer d'équilibrage de charge NetScaler et sur les nœuds de groupe de serveurs StoreFront. Cela simplifie la configuration et vous permet d'ajouter des serveurs StoreFront supplémentaires dans le futur sans avoir à remplacer le certificat.
- **Option 2** : permet d'utiliser un certificat incluant des noms de sujet alternatifs sur le vServer d'équilibrage de charge NetScaler et sur les nœuds de groupe de serveurs StoreFront. Ajouter au certificat des SAN supplémentaires correspondant à tous les noms de domaine complets (FQDN) du serveur StoreFront est facultatif, mais recommandé, car cela permet une plus grande souplesse dans le déploiement StoreFront. Incluez un réseau SAN pour la découverte basée sur l'adresse e-mail `discoverReceiver.example.com`.

Pour plus de détails sur la configuration de la découverte basée sur l'adresse e-mail, voir <http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/>.

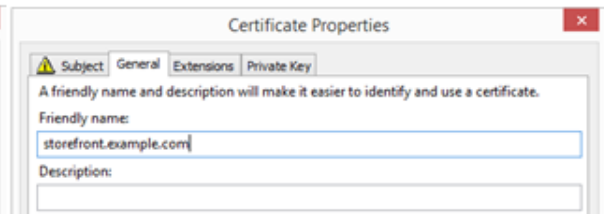
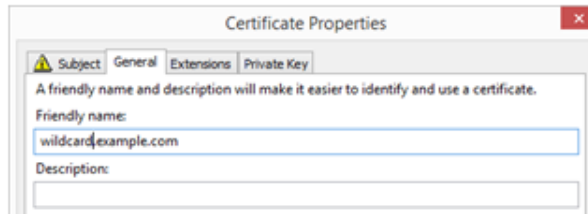
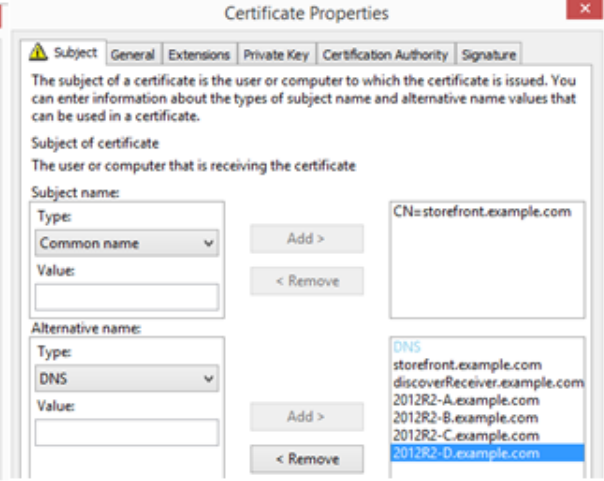
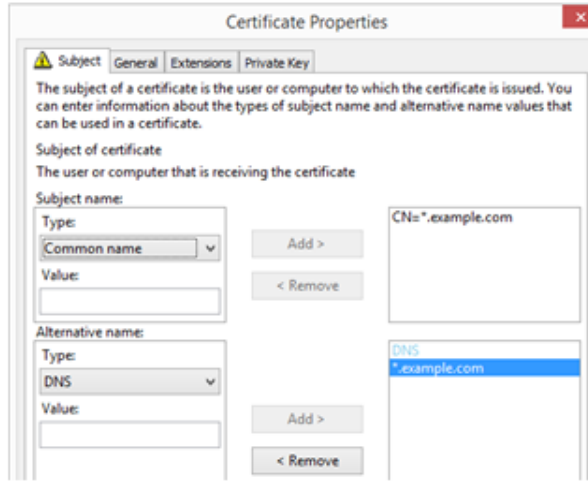
**Remarque :**

Lorsque l'exportation de la clé privée associée avec le certificat n'est pas possible, utilisez deux certificats distincts : un sur le vServer d'équilibrage de charge NetScaler et un autre certificat sur les nœuds de groupe de serveurs StoreFront. Les deux certificats doivent inclure des noms SAN.

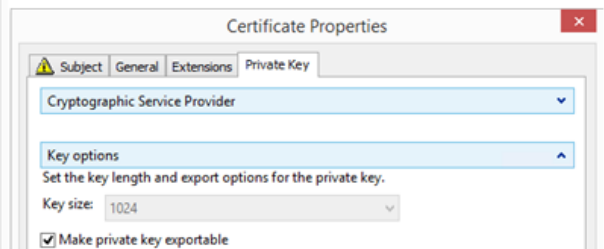
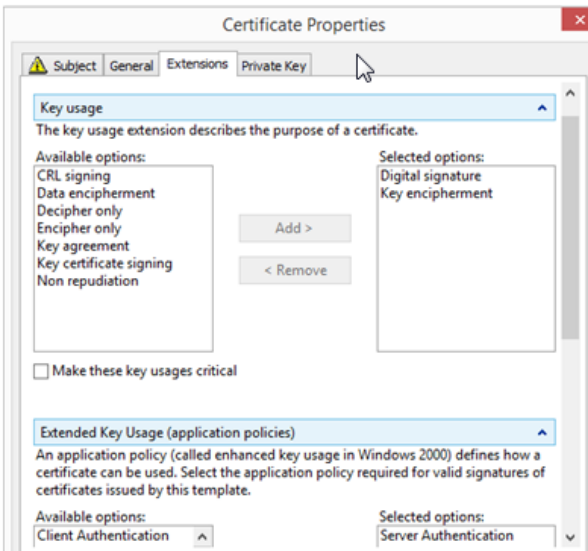
## Example Web server certificates

### Option 1: Wildcard certificate

### Option 2: SAN certificate with every StoreFront server



### Common Properties



## Créer un certificat SSL pour l'équilibrage de charge NetScaler et tous les serveurs StoreFront

### Importer un certificat émis par une autorité de certification Windows sur un boîtier NetScaler avec OpenSSL

- WinSCP est un outil tiers utile et gratuit pour déplacer des fichiers d'un ordinateur Windows sur un système de fichiers NetScaler. Copiez les certificats à importer sur le dossier `/nsconfig/ssl/` dans le système de fichiers NetScaler.
  - Vous pouvez aussi utiliser les outils OpenSSL de NetScaler pour extraire le certificat et la clé depuis un fichier `PKCS12/PFX` afin de créer deux fichiers `.CER` et `.KEY X.509` distincts au format PEM pouvant être utilisés par NetScaler.
1. Copiez le fichier PFX dans `/nsconfig/ssl/` sur le boîtier NetScaler ou VPX.
  2. Ouvrez l'interface de ligne de commande (CLI) de NetScaler.
  3. Tapez **Shell** pour quitter NetScaler CLI et basculer vers le shell FreeBSD.
  4. Changer de répertoire en utilisant `cd /nsconfig/ssl/`.
  5. Exécutez `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` et entrez le mot de passe PFX à l'invite correspondante.
  6. Exécutez `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key` et entrez le mot de passe du fichier PFX lorsque vous y êtes invité, puis définissez la phrase secrète au format PEM pour la clé privée pour protéger le fichier `.KEY`.
  7. Exécutez `ls -al` pour vérifier que les fichiers `.CER` et `.KEY` ont été créés avec succès dans `/nsconfig/ssl/`.
  8. Tapez **Exit** pour retourner à NetScaler CLI.

### Configurer le certificat de serveur sur NetScaler une fois qu'il a été importé

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez Traffic Management > SSL > SSL Certificates et cliquez sur Install.
3. Sur la page Install Certificate, entrez les noms de la paire de clés certificat et privée.
  - Sélectionnez le fichier de certificat `.cer` sur le système de fichiers NetScaler dans `/nsconfig/ssl/`.
  - Sélectionnez le fichier `.key` contenant la clé privée dans le même emplacement.

### Install Certificate

Certificate-Key Pair Name\*

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name\*

 Browse ▼ +

Key File Name

 Browse ▼ +

Certificate Format

PEM  DER

Password

Certificate Bundle  
 Notify When Expires

Notification Period

**Install** Close

## Créer des enregistrements DNS pour l'équilibrage de charge du groupe de serveurs StoreFront

Créez un enregistrement DNS A et PTR pour le nom de domaine complet (FQDN) partagé de votre choix. Les clients de votre réseau utilisent ce nom de domaine complet (FQDN) pour accéder au groupe de serveurs StoreFront utilisant l'équilibrage de charge NetScaler.

Exemple - **storefront.example.com** se résout sur l'adresse IP virtuelle (VIP) du vServer de l'équilibrage de charge.

### Scénario 1 : une connexion sécurisée HTTPS 443 de bout en bout entre le client et l'équilibrage de charge NetScaler et également entre l'équilibrage de charge et deux ou plusieurs serveurs StoreFront 3.0

Ce scénario utilise un moniteur StoreFront modifié utilisant le port 443.

#### Ajouter des nœuds de serveur StoreFront individuels à l'équilibrage de charge NetScaler

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Load Balancing > Servers > Add** et ajoutez chacun des quatre nœuds StoreFront à l'équilibrage de charge.

Exemple = 4 x nœuds 2012R2 StoreFront appelés 2012R2-A à -D

3. Utilisez la configuration de serveur basée sur l'adresse IP et entrez l'adresse IP du serveur pour chaque nœud StoreFront.

The screenshot shows the NetScaler management console. On the left is a navigation tree with 'Servers' selected under 'Load Balancing'. The main area shows a table of 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

#### Définir un moniteur StoreFront pour vérifier l'état de tous les nœuds StoreFront dans le groupe de serveurs

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Load Balancing > Monitors > Add**, ajoutez un nouveau moniteur appelé StoreFront et acceptez tous les paramètres par défaut.
3. Dans le menu déroulant **Type**, sélectionnez **StoreFront**.
4. Assurez-vous que la case **Secure** est cochée si vous utilisez des connexions SSL entre votre vServer d'équilibrage de charge et StoreFront ; sinon, laissez cette option désactivée.
5. Spécifiez le nom du magasin sous l'onglet Special Parameters.



6. Cochez la case **Check Backend Services** sous l'onglet Special Parameters. Cette option permet de contrôler les services exécutés sur le serveur StoreFront. Les services StoreFront sont contrôlés par interrogation d'un service Windows qui s'exécute sur le serveur StoreFront et qui renvoie l'état des services suivants :

- W3SVC (IIS)
- WAS (Service d'activation des processus Windows)
- CitrixCredentialWallet
- CitrixDefaultDomainService

#### Standard Parameters Tab

The 'Create Monitor' dialog box is shown with the 'Standard Parameters' tab selected. The 'Name' field contains 'StoreFront' and the 'Type' dropdown is set to 'STOREFRONT'. The 'Interval' is set to 5 seconds, 'Destination IP' is empty with an 'IPv6' checkbox, 'Response Time-out' is 2 seconds, 'Destination Port' is 'Bound Service', and 'Down Time' is 30 seconds. At the bottom, the 'Secure' checkbox is checked and highlighted with a red box.

#### Special Parameters Tab

The 'Configure Monitor' dialog box is shown with the 'Special Parameters' tab selected. The 'Name' field contains 'StoreFront' and the 'Type' dropdown is set to 'STOREFRONT'. The 'Store Name' field contains 'Store'. The 'Check Backend Services' checkbox is checked and highlighted with a red box. The 'OK' and 'Close' buttons are visible at the bottom.

### Créer un groupe de services HTTPS 443 contenant tous les serveurs StoreFront

1. Dans le groupe de services, sélectionnez l'option Members sur le côté droit et ajoutez tous les nœuds de serveurs StoreFront que vous avez définis précédemment dans la section Servers.
2. Définissez le port SSL et accordez à chaque nœud un ID de serveur unique lors de leur ajout.

### 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

1. Sur l'onglet Monitors, sélectionnez le moniteur StoreFront que vous avez créé précédemment.

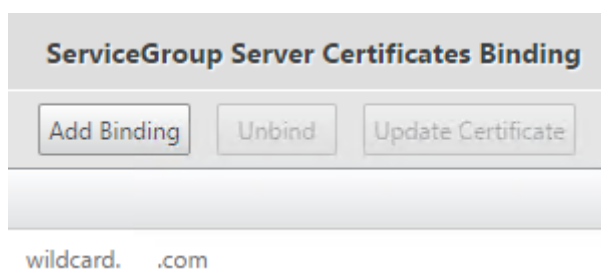
### Monitors

Add Binding Edit Binding Unbind Edit Monitor

Monitor Name	Weight	State
StoreFront	1	✓

Close

1. Sur l'onglet Certificates, liez le certificat SSL que vous avez importé préalablement.
2. Liez le certificat CA utilisé pour signer le certificat de serveur que vous avez importé préalablement et les autres autorités de certification faisant partie de la chaîne de confiance PKI.



### Créer un vServer d'équilibrage de charge pour le trafic utilisateur

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Load Balancing > Virtual Servers > Add** pour créer un nouveau vServer.
3. Sélectionnez la méthode d'équilibrage de charge pour le vServer. Les options courantes pour l'équilibrage de charge StoreFront sont **round robin** ou **least connection**.

1. Liez le **groupe de services** que vous avez créé précédemment au vServer d'équilibrage de charge.
2. Liez au vServer d'équilibrage de charge le même certificat de serveur et CA vous avez déjà lié au groupe de services.
3. Depuis le menu du vServer d'équilibrage de charge, sélectionnez **Persistence** sur le côté droit et définissez la méthode de persistance sur **CookieInsert**.
4. Attribuez un nom au cookie. Par exemple, **NSC\_SFPersistence**, car cela facilite l'identification dans les traces de Fiddler lors du débogage.
5. Définissez la persistance de sauvegarde sur **None**.

**Persistence** ×

Persistence\*

Time-out (mins)\*

Cookie Name

---

**Backup Persistence**

Backup Persistence

Backup Time-out

IPv4 Netmask

IPv6 Mask Length

## Scénario 2 : Arrêt HTTPS - Communication HTTPS 443 entre le client et l'équilibrage de charge NetScaler et connexions HTTP 80 entre l'équilibrage de charge et les serveurs StoreFront 3.0

Ce scénario utilise le moniteur StoreFront par défaut avec le port 8000.

### Ajouter des serveurs StoreFront individuels à l'équilibrage de charge NetScaler

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Load Balancing > Servers > Add** et ajoutez chacun des quatre serveurs StoreFront à l'équilibrage de charge.  
Exemple = 4 serveurs 2012R2 StoreFront appelés 2012R2-A à -D.
3. Utilisez la configuration de serveur basée sur l'adresse IP et entrez l'adresse IP du serveur pour chaque serveur StoreFront.

Name	State	IP Address / 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

### Définir un moniteur StoreFront HTTP 8000 pour vérifier l'état de tous les serveurs StoreFront du groupe de serveurs

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Monitors > Add** et ajoutez un nouveau moniteur appelé StoreFront.
3. Ajoutez un nom pour le nouveau moniteur et acceptez tous les paramètres par défaut.
4. Sélectionnez **Type** dans le menu déroulant et définissez-le sur **StoreFront**.
5. Spécifiez le nom du magasin sous l'onglet Special Parameters.
6. Entrez **8000** dans le port de destination, car il correspond à l'instance de moniteur par défaut créée sur chaque serveur StoreFront.
7. Cochez la case **Check Backend Services** sous l'onglet Special Parameters. Cette option permet de contrôler les services exécutés sur le serveur StoreFront. Les services StoreFront sont contrôlés par interrogation d'un service Windows qui s'exécute sur le serveur StoreFront et qui renvoie l'état des services suivants :
  - W3SVC (IIS)
  - WAS (Service d'activation des processus Windows)
  - CitrixCredentialWallet
  - CitrixDefaultDomainService

### Créer un groupe de services HTTP 80 contenant tous les serveurs StoreFront

1. Dans le groupe de services, sélectionnez l'option Members sur le côté droit et ajoutez tous les nœuds de serveurs StoreFront que vous avez définis précédemment dans la section Servers.
2. Définissez le port HTTP sur 80 et accordez à chaque serveur un ID de serveur unique lors de leur ajout.

3. Sur l'onglet Monitors, sélectionnez le moniteur StoreFront que vous avez créé précédemment.

### Créer un vServer d'équilibrage de charge d'arrêt HTTPS pour le trafic utilisateur

1. Sélectionnez **Traffic Management > Load Balancing > Virtual Servers > Add** pour créer un nouveau vServer.
2. Sélectionnez la méthode d'équilibrage de charge que le vServer utilisera. Les options courantes pour l'équilibrage de charge StoreFront sont **round robin** ou **least connection**.
3. Liez le **groupe de services** que vous avez créé précédemment au vServer d'équilibrage de charge.
4. Liez au vServer d'équilibrage de charge le même certificat de serveur et CA vous avez déjà lié au groupe de services.

**Remarque :**

Si le client n'est pas autorisé à stocker le cookie HTTP, les demandes ultérieures ne disposent pas du cookie HTTP et la **Persistence** n'est pas utilisé.

5. Depuis le menu du vServer d'équilibrage de charge, sélectionnez **Persistence** et définissez la méthode de persistance sur **CookieInsert**.
6. Attribuez un nom au cookie. Par exemple, **NSC\_SFPersistence**, car cela facilite l'identification dans les traces de Fiddler lors du débogage.
7. Définissez la persistance de sauvegarde sur **None**.

## 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

## Créer un équilibrage de charge vServer pour la synchronisation des abonnements entre les groupes de serveurs

Considérations à prendre en compte avant de créer un vServer d'équilibrage de charge :

- **Option 1 :** créez un seul vServer pour équilibrer la charge du trafic utilisateur uniquement. Cela suffit si vous effectuez uniquement des lancements ICA d'applications publiées et de bureaux. (obligatoire et généralement suffisant).
- **Option 2 :** créez une paire de vServers : un pour l'équilibrage de charge du trafic utilisateur pour effectuer des lancements ICA d'applications publiées et de bureaux et un autre pour l'équilibrage de charge des opérations de synchronisation de données d'abonnement. (nécessaire uniquement lors de la propagation de données d'abonnement entre plusieurs groupes de serveurs StoreFront dont la charge est équilibrée dans un grand déploiement multisite).

Si un déploiement multisite est constitué de plusieurs groupes de serveurs StoreFront se trouvant dans des emplacements géographiques différents, vous pouvez répliquer les données d'abonnement entre eux à l'aide d'une stratégie « pull » selon un planning récurrent. La réplication d'abonnement StoreFront utilise le port TCP 808, donc l'utilisation d'un vServer d'équilibrage de charge sur le port HTTP 80 ou HTTPS 443 échoue. Pour fournir une haute disponibilité pour ce service, vous devez créer

un deuxième vServer sur chaque NetScaler de votre déploiement pour équilibrer la charge du port TCP 808 pour chacun des groupes de serveurs StoreFront. Lors de la configuration du planning de réplication, spécifiez une adresse de groupe de services qui correspond à l'adresse IP virtuelle du vServer de synchronisation d'abonnement. Assurez-vous que l'adresse du groupe de serveurs est le nom de domaine complet de l'équilibrage de charge pour le groupe de serveurs à cet emplacement.

### Configurez un groupe de services pour la synchronisation d'abonnement

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Service Groups > Add** et ajoutez un nouveau groupe de services.
3. Définissez le protocole sur **TCP**.
4. Dans le groupe de services, sélectionnez l'option **Members** sur le côté droit et ajoutez tous les nœuds de serveurs StoreFront que vous avez définis précédemment dans la section Servers.
5. Sur l'onglet **Monitors**, sélectionnez le moniteur TCP.

Monitor Name	Weight	State	Passive
tcp	1	✓	✗

### Créer un équilibrage de charge vServer pour la synchronisation des abonnements entre les groupes de serveurs

1. Ouvrez une session sur la console de gestion de NetScaler.
2. Sélectionnez **Traffic Management > Service Groups > Add** et ajoutez un nouveau groupe de services.
3. Définissez la méthode d'équilibrage de charge sur **round robin**.
4. Définissez le protocole sur **TCP**.
5. Entrez **808** et NON **443** comme numéro de port.



## Load Balancing Virtual Server

### Basic Settings

Name\*

Protocol\*

IP Address Type\*

IP Address\*

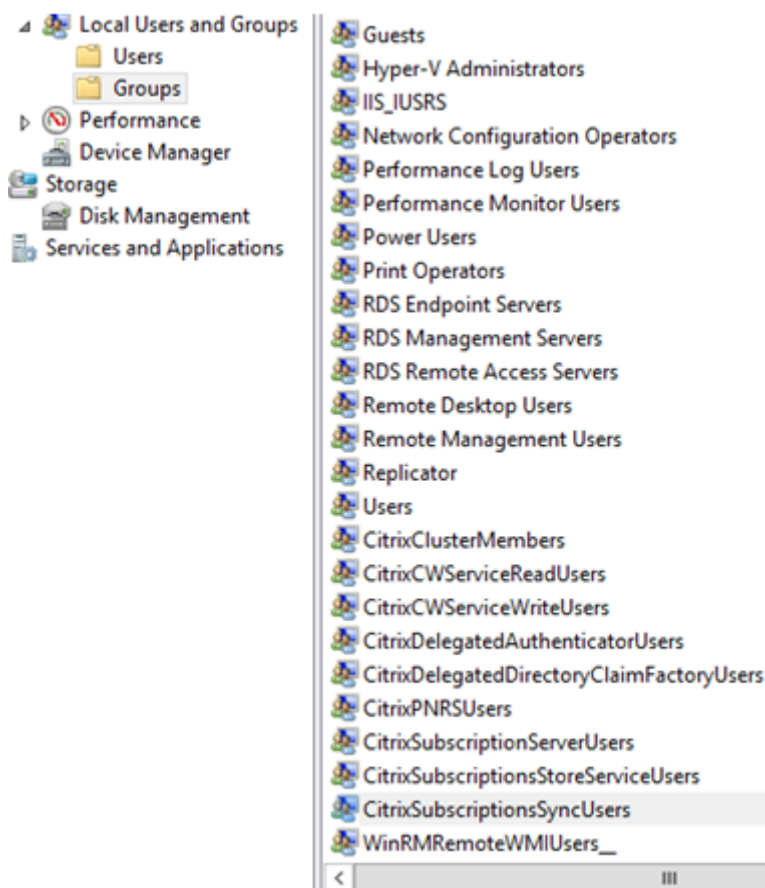
  IPv6

Port\*

 ?

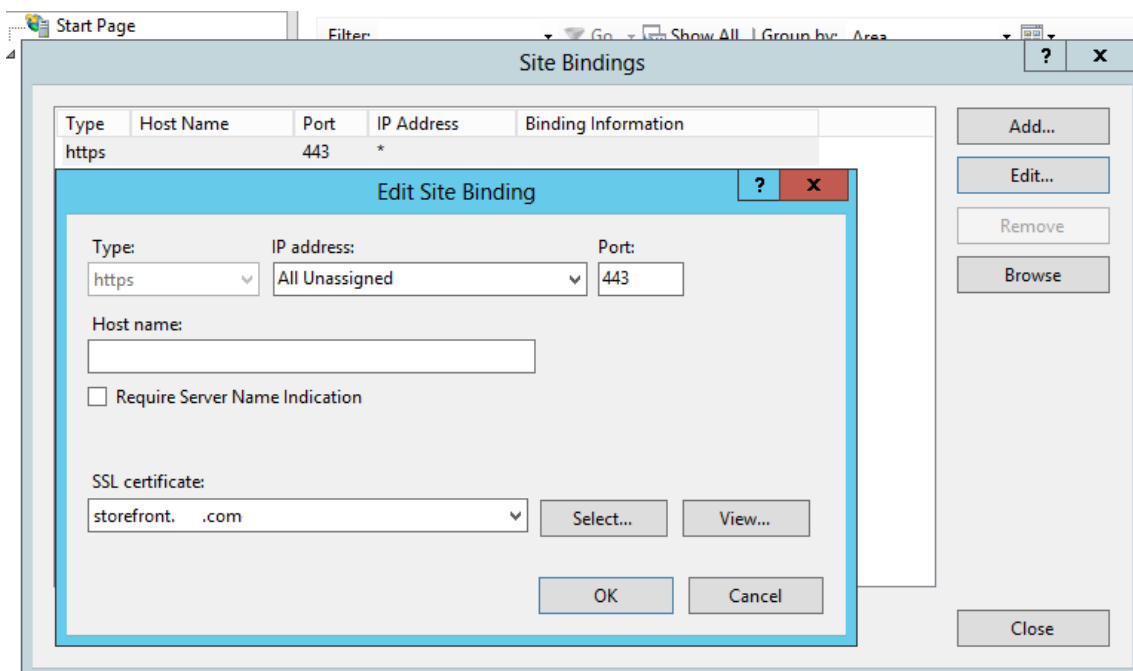
### Appartenance au groupe CitrixSubscriptionsSyncUsers

Pour que le **serveur StoreFront A** dans l'**emplacement A** demande et récupère des données d'abonnement à partir du **serveur B** à un emplacement différent, le serveur A doit être un membre du groupe de sécurité local **CitrixSubscriptionsSyncUsers** sur le serveur B. Le groupe local **CitrixSubscriptionsSyncUsers** contient une liste de contrôle d'accès de tous les serveurs StoreFront distants autorisés à extraire les données d'abonnement d'un serveur donné. Pour la synchronisation d'abonnement bidirectionnelle, le serveur B doit également être un membre du groupe de sécurité **CitrixSubscriptionsSyncUsers** sur le serveur A pour extraire les données d'abonnement à partir de ce dernier.



### **Configurer le groupe de serveurs StoreFront pour l'équilibrage de charge**

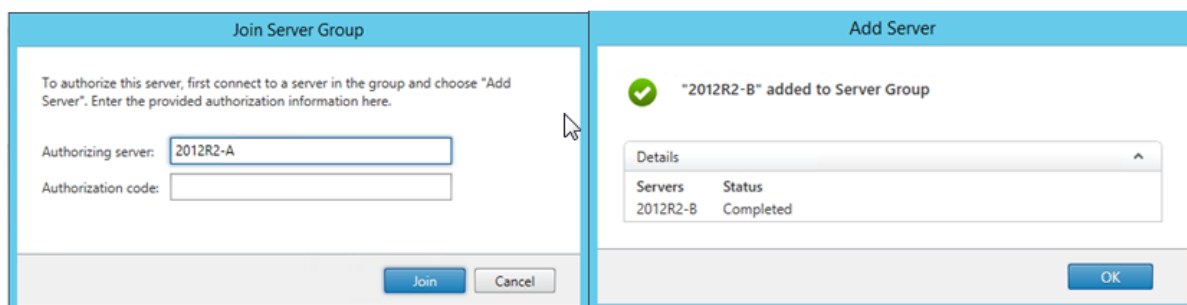
1. Importez la clé certificat et privée qui a été déployée sur le vServer d'équilibrage de charge NetScaler pour chaque nœud StoreFront du groupe de serveurs.
2. Créez une liaison HTTPS dans IIS sur chaque nœud StoreFront, puis liez le certificat que vous avez importé.



3. Installez StoreFront sur chaque nœud du groupe de serveurs.
4. Lors de l'installation de StoreFront, définissez l'URL de base de l'hôte sur le nœud principal qui sera le nom de domaine complet (FQDN) partagé utilisé par tous les membres du groupe de serveurs. Vous devez utiliser un certificat contenant le nom de domaine complet (FQDN) avec équilibrage de charge en tant que nom courant (CN) ou nom de sujet alternatif (SAN).

Consultez la section [Créer un certificat SSL pour l'équilibrage de charge NetScaler et les serveurs StoreFront](#).

5. Lorsque vous avez terminé la configuration initiale de StoreFront, associez tous les nœuds, l'un après l'autre, avec le groupe de serveurs à l'aide du nœud principal.
6. Sélectionnez **Server Group > Add Server > Copy the Authorization Code** pour le serveur à associer.



1. Propagez la configuration à partir du nœud principal vers tous les autres nœuds du groupe de serveurs.

2. Testez le groupe de serveurs avec équilibrage de charge à l'aide d'un client qui peut contacter et résoudre le nom de domaine complet partagé de l'équilibrage de charge.

### Moniteur de services Citrix

Pour activer la surveillance externe de l'état d'exécution des services Windows sur lesquels StoreFront s'appuie pour un fonctionnement correct, utilisez le service Windows **Citrix Service Monitor**. Ce service ne dépend d'aucun autre service et peut surveiller et signaler les échecs d'autres services essentiels de StoreFront. Le moniteur permet à d'autres composants Citrix, tels que NetScaler, de déterminer l'intégrité relative d'un déploiement de serveurs StoreFront en externe. Des logiciels tiers peuvent utiliser la réponse XML du moniteur StoreFront pour contrôler l'intégrité des services essentiels StoreFront.

Lorsque StoreFront est déployé, un moniteur par défaut qui utilise le protocole HTTP et le port 8000 est créé.

#### Remarque :

Une seule instance de moniteur peut exister dans un déploiement StoreFront.

Pour apporter des modifications au moniteur par défaut existant, telles que le réglage du protocole et du port sur HTTPS 443, utilisez les trois applets de commande PowerShell pour afficher ou reconfigurer l'URL de service du moniteur StoreFront.

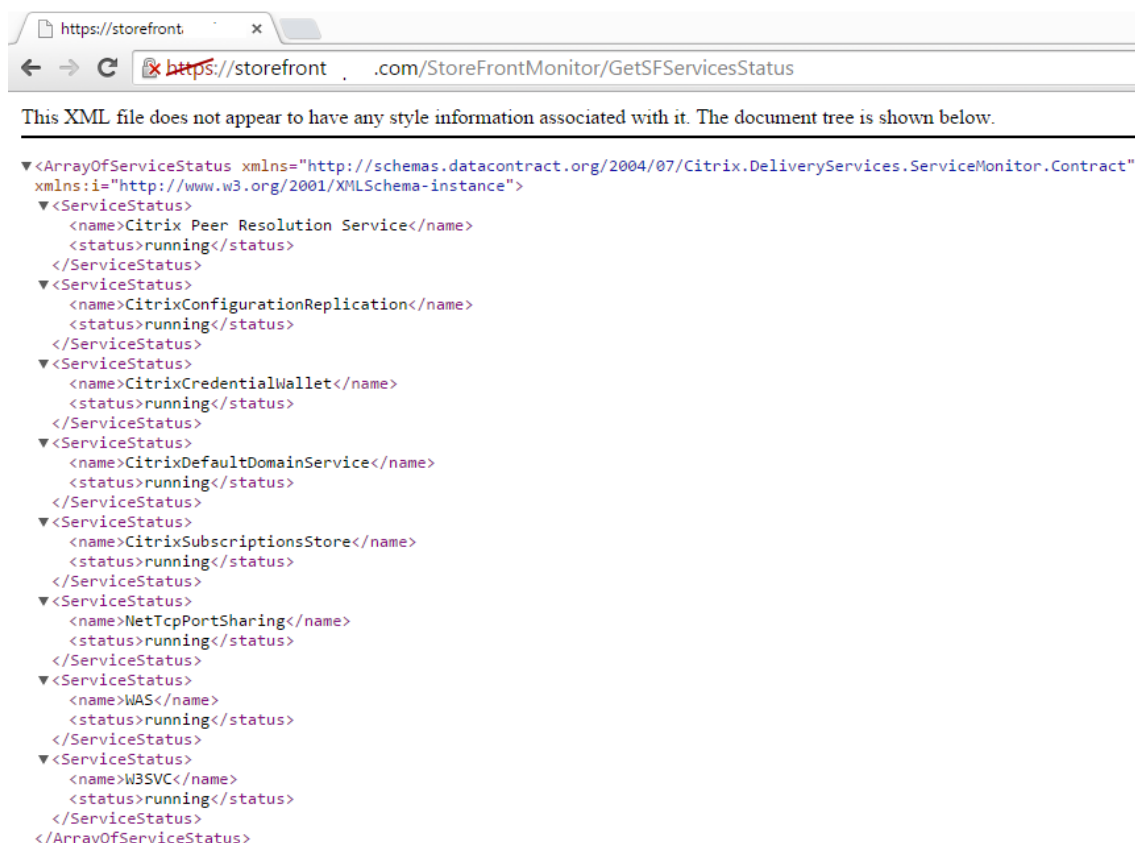
### Supprimer le moniteur de services par défaut et le remplacer par un moniteur qui utilise le protocole HTTPS et le port 443

1. Ouvrez la console PowerShell (ISE) sur le serveur StoreFront principal et exécutez les commandes suivantes pour modifier le moniteur par défaut sur HTTPS 443.

```
1 $ServiceUrl = "https://localhost:443/StorefrontMonitor"
2 Set-STFServiceMonitor -ServiceUrl $ServiceUrl
3 Get-STFServiceMonitor
```

2. Une fois terminé, propagez les modifications à tous les autres serveurs du groupe de serveurs StoreFront.
3. Pour effectuer un test rapide sur le nouveau moniteur, entrez l'adresse URL suivante dans le navigateur sur le serveur StoreFront ou toute autre machine avec accès réseau au serveur StoreFront. Le navigateur doit afficher un résumé XML de l'état de chaque service StoreFront.

<https://<loadbalancingFQDN>:443/StoreFrontMonitor/GetSFServicesStatus>



The screenshot shows a web browser window with the address bar containing `https://storefront.com/StoreFrontMonitor/GetSFServicesStatus`. Below the browser, a message states: "This XML file does not appear to have any style information associated with it. The document tree is shown below." The XML document tree is displayed as follows:

```
<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>
```

## vServers NetScaler Gateway et d'équilibrage de charge sur le même boîtier NetScaler

Si vous avez configuré le vServer NetScaler Gateway et le vServer d'équilibrage de charge sur le même boîtier NetScaler, les utilisateurs de domaine internes peuvent rencontrer des problèmes lors d'une tentative d'accès direct à l'URL de base de l'hôte avec équilibrage de charge StoreFront au lieu de passer par le vServer NetScaler Gateway.

Dans ce scénario, StoreFront suppose que l'utilisateur a déjà été authentifié sur NetScaler Gateway, car StoreFront associe l'adresse IP source de l'utilisateur entrant avec l'adresse IP de sous-réseau (SNIP) de NetScaler Gateway. StoreFront essaie alors d'utiliser le protocole AGBasic pour effectuer l'authentification silencieuse sur NetScaler Gateway, plutôt que d'inviter l'utilisateur à ouvrir une session à l'aide de ses informations d'identification de domaine. Pour éviter ce problème, ignorez l'adresse SNIP comme illustré ci-dessous afin que le nom d'utilisateur et le mot de passe d'authentification soient utilisés à la place d'AGBasic.

## Configurer un NetScaler Gateway sur le groupe de serveurs StoreFront

**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:

NetScaler Gateway URL:

Version:

Subnet IP address: (optional)

Logon type:

Smart card fallback:

Callback URL: (optional)  /CitrixAuthService/AuthService.asmx

### Options de bouclage lors de l'équilibrage de charge d'un groupe de serveurs StoreFront à l'aide de NetScaler

Dans les versions précédentes de StoreFront telles que 2.6 ou les versions plus anciennes, Citrix recommandait aux utilisateurs de modifier manuellement le fichier d'hôtes sur chaque serveur StoreFront pour mapper le nom de domaine complet (FQDN) de l'équilibrage de charge sur l'adresse de bouclage ou l'adresse IP du serveur StoreFront spécifique. Cela garantit que Receiver pour Web communique toujours avec les services StoreFront sur le même serveur dans un déploiement dont la charge est équilibrée. Ceci est nécessaire car une session HTTP est créée durant le processus de connexion explicite entre Receiver pour Web et le service d'authentification, et Receiver pour Web communique avec StoreFront Services à l'aide du nom de domaine complet (FQDN) de base. Si le nom de domaine complet (FQDN) de base parvenait à résoudre l'équilibrage de charge, l'équilibrage de charge pouvait potentiellement envoyer le trafic vers un autre serveur StoreFront dans le groupe, ce qui entraînait l'échec de l'authentification. L'équilibrage de charge n'est pas contourné, sauf lorsque Receiver pour Web tente de contacter le service de magasin qui réside sur le même serveur que lui-même.

Vous pouvez définir les options de bouclage à l'aide de PowerShell. L'activation du bouclage élimine le besoin de créer des entrées dans le fichier hôte sur chaque serveur StoreFront dans le groupe de serveurs.

### Exemple de fichier web.config Receiver pour Web

```
1 <communication attempts="2" timeout="00:01:00" loopback="On"
  loopbackPortUsingHttp="80">
```

### Exemple de commande PowerShell

```
1 & "c:\program files\Citrix\receiver storefront\scripts\ImportModules.
  ps1"
2 Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "
  OnUsingHttp" -LoopbackPortUsingHttp 81
```

Le paramètre **-Loopback** peut prendre trois valeurs possibles.

Valeur	Contexte
<b>On</b> : change l'hôte de l'adresse URL sur 127.0.0.1. Le schéma et le port (si spécifiés) ne sont pas modifiés.	Ne peut pas être utilisé si l'équilibrage de charge d'arrêt SSL est utilisé.
<b>OnUsingHttp</b> : change l'hôte sur 127.0.0.1 et le schéma sur HTTP et modifie la valeur du port configurée pour l'attribut <b>loopbackPortUsingHttp</b> .	À utiliser uniquement avec un équilibrage de charge d'arrêt SSL. Les communications entre l'équilibrage de charge et les serveurs StoreFront utilisent HTTP. Vous pouvez explicitement configurer le port HTTP à l'aide de l'attribut -loopbackPortUsingHttp.
<b>Off</b> : l'adresse URL de la requête n'est en aucun modifiée.	Utilisé pour résoudre les problèmes. Les outils tels que Fiddler ne peuvent pas enregistrer le trafic entre Receiver pour Web et StoreFront Services si le bouclage est défini sur <b>On</b> .

## Configurer deux adresses URL pour le même NetScaler Gateway

February 26, 2019

Dans StoreFront, vous pouvez ajouter une seule adresse URL NetScaler Gateway à partir de la console de gestion StoreFront dans Gérer NetScaler Gateway > Ajouter ou Modifier. Il est également possible d'ajouter une URL publique NetScaler Gateway et une URL GSLB (équilibrage de charge globale des serveurs) dans Gérer NetScaler Gateway > importé à partir d'un fichier.

Cet article vous explique comment utiliser les applets de commande PowerShell et le SDK PowerShell StoreFront pour utiliser un paramètre facultatif, - gslburl, pour définir l'attribut GslbLocation d'une

passerelle. Cette fonctionnalité simplifie l'administration de NetScaler Gateway dans StoreFront dans les cas d'utilisation suivants :

1. **Répartiteur GSLB avec plusieurs NetScaler Gateway.** Utilisez un répartiteur GSLB et plusieurs NetScaler Gateway pour équilibrer la charge des connexions à distance aux ressources publiées dans deux ou plusieurs emplacements dans un déploiement Citrix global à grande échelle.
2. **NetScaler Gateway unique avec adresse URL publique ou privée.** Utilisez le même NetScaler Gateway pour l'accès externe à l'aide d'une adresse URL publique et pour l'accès interne à l'aide d'une adresse URL privée.

Il s'agit d'une fonctionnalité avancée. Si vous n'êtes pas familier avec les concepts de répartiteur GSLB, veuillez consulter les liens Informations connexes à la fin de cet article.

Cette fonctionnalité offre les avantages suivants :

- Prise en charge des deux adresses URL simultanées pour un seul objet passerelle.
- Les utilisateurs peuvent basculer entre deux URL différentes pour accéder à NetScaler Gateway sans que l'administrateur ne soit obligé de reconfigurer l'objet passerelle de StoreFront afin qu'il corresponde à l'URL de la passerelle que l'utilisateur veut utiliser.
- Temps de préparation et durée des test plus courts pour valider la configuration de la passerelle StoreFront lors de l'utilisation de plusieurs passerelles GSLB.
- Possibilité d'utiliser le même objet NetScaler Gateway dans StoreFront au sein la DMZ pour l'accès externe et interne.
- Prend en charge les deux adresses URL pour un routage optimal de la passerelle. Pour de plus amples informations sur le routage optimal de la passerelle, consultez la section [Définir des magasins multisite à haute disponibilité](#).

## Considérations sur le déploiement lors de l'utilisation des deux adresses URL de passerelle

### Important :

Avant de configurer une deuxième adresse URL de passerelle à l'aide du paramètre - gslburl, Citrix vous recommande de vérifier les certificats de serveur en place et la manière dont votre entreprise effectue la résolution DNS. Les adresses URL que vous souhaitez utiliser dans votre déploiement NetScaler et StoreFront doivent être présentes dans vos certificats de serveur. Pour plus d'informations sur les certificats de serveur, veuillez consulter la section [Planifier l'utilisation des certificats de serveur et des passerelles](#).

## DNS

- **Split DNS.** Il est courant pour les grandes entreprises d'utiliser le split DNS. Le split DNS implique l'utilisation d'espaces de noms différents et de serveurs DNS différents pour la résolu-



tion DNS publique et privée. Vérifiez que l'infrastructure DNS dont vous disposez permettant de prendre en charge ce scénario.

- **URL unique pour l'accès externe et interne aux ressources publiées.** Décidez si vous souhaitez utiliser la même adresse URL pour accéder aux ressources publiées aussi bien à l'intérieur qu'à l'extérieur de votre réseau d'entreprise, ou si deux adresses URL différentes sont acceptables telles que `example.com` et `example.net`.

## Exemples de certificats de serveur

Cette section contient des exemples de déploiements de certificats de serveur lors de l'utilisation des deux adresses URL de passerelle.

### Exemple de certificat de serveur pour un déploiement StoreFront avec charge équilibrée

Un certificat de serveur générique signé de manière privée doit contenir le nom de domaine complet `*.storefront.example.net`.

Ou

Un certificat de serveur SAN signé de manière privée doit contenir tous les noms de domaine complets nécessaires pour équilibrer la charge de trois serveurs StoreFront.

```
1 loadbalancer.storefront.example.net
2 server1.storefront.example.net
3 server2.storefront.example.net
4 server3.storefront.example.net
```

Définissez l'URL de base d'hôte du groupe de serveurs StoreFront sur le nom de domaine complet partagé, qui est résolu sur l'adresse IP d'équilibrage de charge :

```
1 loadbalancer.storefront.example.net
```

### Exemple de certificat de serveur pour un groupe de Delivery Controller XenApp et XenDesktop 7.x

Un certificat de serveur générique signé de manière privée doit contenir le nom de domaine complet `*.xendesktop.example.net`.

Ou

Un certificat de serveur SAN signé de manière privée doit contenir toutes les noms de domaine complets du serveur nécessaires pour un site XenDesktop contenant quatre Controller.

```
1 XD1A. xendesktop.example.net
2 XD1B. xendesktop.example.net
3 XD2A. xendesktop.example.net
4 XD2B. xendesktop.example.net
```

### **Exemple de certificat de serveur pour un NetScaler Gateway accessible en externe et en interne à l'aide du split DNS**

Un certificat de serveur SAN signé publiquement pour l'accès externe et interne doit contenir les noms de domaine complets externes et internes.

```
1 gateway.example.com
2 gateway.example.net
```

### **Exemple de certificat de serveur pour toutes les passerelles GSLB accessibles en externe**

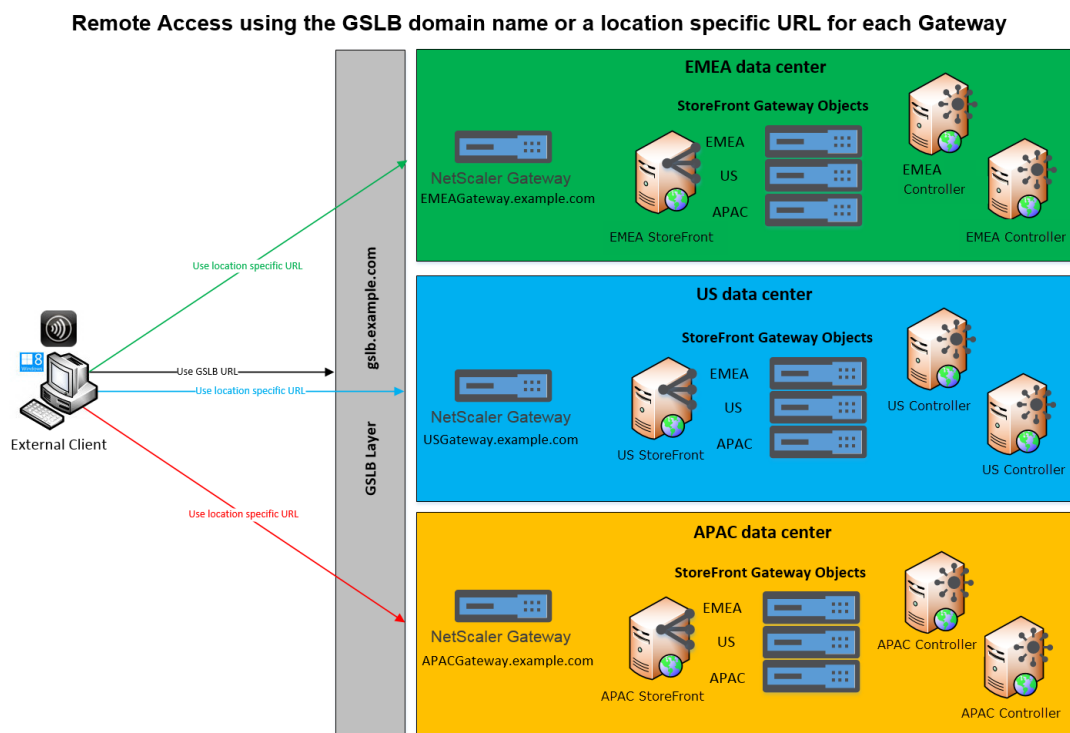
Un certificat de serveur SAN signé publiquement pour l'accès externe via un répartiteur GSLB doit contenir les noms de domaine complets.

```
1 gslbdomain.example.com
2 emeagateway.example.com
3 usgateway.example.com
4 apacgateway.example.com
```

Cela permet à l'utilisateur d'accéder à la passerelle la plus proche à l'aide du répartiteur GSLB ou de choisir une passerelle dans l'emplacement de son choix à l'aide de son nom de domaine complet unique.

### **Cas d'utilisation 1 : répartiteur GSLB avec plusieurs NetScaler Gateway**

L'administrateur utilise un répartiteur GSLB et plusieurs NetScaler Gateway pour équilibrer la charge des connexions à distance aux ressources publiées dans deux ou plusieurs emplacements dans un déploiement Citrix global à grande échelle.



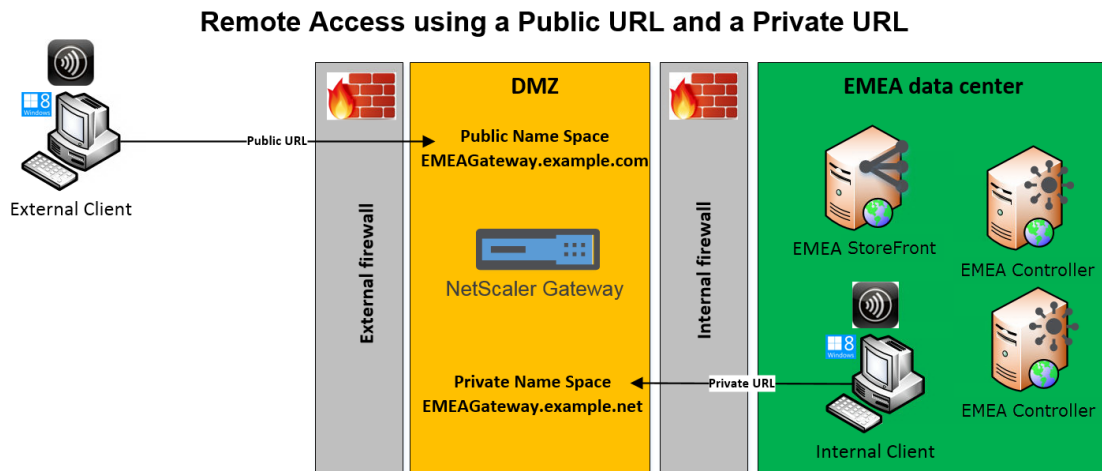
Dans cet exemple :

- Chaque emplacement ou data center contient au moins une passerelle, un ou plusieurs serveurs StoreFront et un ou plusieurs Controller XenApp et XenDesktop afin de fournir des ressources publiées pour cet emplacement.
- Chaque service GSLB configuré sur les Netscaler GSLB dans le déploiement global représente un vServer VPN de passerelle. Tous les serveurs StoreFront du déploiement doivent être configurés pour contenir tous les vServers NetScaler Gateway qui constituent la couche du répartiteur GSLB.
- Les GSLB NetScaler Gateway sont utilisés en mode actif/passif mais peuvent également fournir un basculement en cas de défaillance de la connexion réseau, du DNS, de la passerelle, du serveur StoreFront ou des Controller XenApp et XenDesktop sur un emplacement. Les utilisateurs sont dirigés automatiquement sur une autre passerelle au cas où un service GSLB n'est pas disponible.
- Les clients externes sont dirigés vers la passerelle la plus proche en fonction de l'algorithme d'équilibrage de charge GSLB configuré tel que la durée des boucles (RTT) ou la proximité statique lors de l'établissement de connexions à distance.
- L'adresse URL unique de chaque gateway permet aux utilisateurs de sélectionner manuellement le data center à partir duquel ils souhaitent lancer des ressources en choisissant l'URL spécifique à l'emplacement de la passerelle qu'ils veulent utiliser.
- Le répartiteur GSLB peut être ignoré lorsque GSLB ou une délégation DNS ne fonctionne pas comme prévu. Les utilisateurs peuvent continuer à accéder aux ressources à distance sur

n'importe quel data center à l'aide de l'adresse URL spécifique à l'emplacement jusqu'à ce que les problèmes liés au répartiteur GSLB sont résolus.

## Cas d'utilisation 2 : NetScaler Gateway unique avec adresse URL publique ou privée

L'administrateur utilise le même NetScaler Gateway pour l'accès externe à l'aide d'une adresse URL publique et pour l'accès interne à l'aide d'une adresse URL privée.



Dans cet exemple :

- L'administrateur souhaite que l'accès aux ressources publiées et que le trafic de lancement HDX transitent via un NetScaler Gateway, même si le client est interne.
- NetScaler est situé dans une zone démilitarisée (DMZ).
- Il existe deux itinéraires réseau différents vers NetScaler Gateway via les deux pare-feu des deux côtés de la DMZ.
- L'espace de noms externe public est différent de l'espace de noms interne.

## Exemples d'applets de commande PowerShell

Utilisez les applets de commande PowerShell **Add-STFRoamingGateway** et **Set-STFRoamingGateway** avec le paramètre - gslburl pour définir l'attribut **GslbLocation** sur l'objet passerelle de StoreFront. Par exemple :

```
1 Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
emeagateway.example.com" -GSLBurl "https://gslb.example.com" -
SubnetIPAddress "10.0.0.1" -CallbackUrl "https://emeagateway.example
.com" -LogonType "DomainAndRSA" -SmartCardFallbackLogonType "None" -
Version "Version10_0_69_4" -SecureTicketAuthorityUrls "https://emea-
controller.example.com/scripts/ctxsta.dll,https://us-controller.
```

```

example.com/scripts/ctxsta.dll,https://apac-controller.example.com/
scripts/ctxsta.dll"
2 Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
emeagateway.example.com" -GSLBurl "https://gslb.example.com"
3 Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA
gateway object)
4 Or
5 Get-STFRoamingGateway (returns all gateway object configured in
StoreFront)

```

Pour le cas d'utilisation 1, vous pouvez supprimer GSLBurl de « EMEAGateway » en définissant **GslbLocation** sur NULL. Le PowerShell suivant modifie l'objet de passerelle \$EMEAGateway stocké en mémoire. **Set-STFRoamingGateway** peut ensuite être transmis à \$EMEAGateway pour mettre à jour la configuration de StoreFront et supprimer l'attribut GSLBurl.

```

1 $EMEAGateway = Get-STFRoamingGateway
2 $EMEAGateway.GslbLocation = $Null
3 Set-STFRoamingGateway -Gateway $EMEAGateway

```

Pour le cas d'utilisation 1, les passerelles suivantes sont renvoyées à l'aide de **Get-STFRoamingGateway** :

```

1 Name: EMEAGateway
2 Location: https://emeagateway.example.com/ (Unique URL for the EMEA
Gateway)
3 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
gateways)
4
5 Name: USGateway
6 Location: https://USgateway.example.com/ (Unique URL for the US Gateway
)
7 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
gateways)
8
9 Name: APACGateway
10 Location: https://APACgateway.example.com/ (Unique URL for the APAC
Gateway)
11 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
gateways)

```

Pour le cas d'utilisation 2, les passerelles suivantes sont renvoyées à l'aide de **Get-STFRoamingGateway** :

```

1 Name: EMEAGateway
2 Location: https://emeagateway.example.com/ (Public URL for the Gateway)

```

```
3 GslbLocation: https://emeagateway.example.net/ (Private URL for the
   Gateway)
```

Pour le cas d'utilisation 1, le routage de passerelle optimal est renvoyé à l'aide de **Get-STFStoreRegisteredOptimal**

:

```
1 $StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<
   YourStore>"
2
3 Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject
4
5 Hostnames:      {
6   emeagateway.example.com, gslb.example.com }
7
8 Hostnames:      {
9   usgateway.example.com, gslb.example.com }
10
11 Hostnames:     {
12  apacgateway.example.com, gslb.example.com }
```

### L'URL GSLB ou l'URL interne de chaque passerelle est stockée dans le fichier web.config du service itinérant

StoreFront n'affiche pas l'adresse URL du répartiteur GSLB ni l'adresse URL interne de chaque passerelle dans la console de gestion StoreFront, toutefois, il est possible de voir le chemin d'accès GSLBLocation configuré pour toutes les passerelles GSLB en ouvrant le fichier Web.Config du service d'itinérance dans C:\inetpub\wwwroot\Citrix\Roaming\web.config sur le serveur StoreFront.

#### Cas d'utilisation n° 1 : Passerelles dans le fichier web.config en itinérance

```
1 <gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
   default="false" edition="Enterprise" version="Version10_0_69_1" auth
   ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.1" rwmode
   ="NONE" deployment="Appliance" callbackurl=https://emeagateway.
   example.com/CitrixAuthService/AuthService.asmx sessionreliability="
   true" requesttickettwesta="false" stasUseLoadBalancing="false"
   stasBypassDuration="01:00:00">
2 <location path="https://emeagateway.example.com/" /><gslbLocation path=
   "https://gslb.example.com/" /><clusternodes>
3 <clear />
4 </clusternodes>
5 <silentauthenticationurls>
```

```
6 <clear />
7 </silentauthenticationurls>
8 <secureticketauthorityurls>
9 <clear />
10 <location path="https://emea-controller.example.com/scripts/ctxsta.dll"
    />
11 <location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
12 <location path="https://apac-controller.example.com/scripts/ctxsta.dll"
    />
13 </secureticketauthorityurls>
14 </gateway>
15
16 <gateway id="b8ec720c-d85e-1889-8188-1cf08a2cf762" name="USGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.2" rwmode
    ="NONE" deployment="Appliance" callbackurl="https://usgateway.
    example.com/CitrixAuthService/AuthService.asmx" sessionreliability="
    true" requesttickettwesta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00"><location path="https://usgateway.
    example.com/" /><gslbLocation path="https://gslb.example.com/" /><
    clusternodes>
17 <clear />
18 </clusternodes>
19 <silentauthenticationurls>
20 <clear />
21 </silentauthenticationurls>
22 <secureticketauthorityurls>
23 <clear />
24 <location path="https://emea-controller.example.com/scripts/ctxsta.dll"
    />
25 <location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
26 <location path="https://apac-controller.example.com/scripts/ctxsta.dll"
    />
27 </secureticketauthorityurls>
28 </gateway>
29
30 <gateway id="c57117b5-e111-1eed-9117-a1ffa1c8100e" name="APACGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.3" rwmode
    ="NONE" deployment="Appliance" callbackurl="https://apacgateway.
    example.com/CitrixAuthService/AuthService.asmx" sessionreliability="
    true" requesttickettwesta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00"><location path="https://apacGateway.
```

```
    example.com/" /><gslbLocation path="https://gslb.example.com/" /><
    clusternodes>
31 <clear />
32 </clusternodes>
33 <silentauthenticationurls>
34 <clear />
35 </silentauthenticationurls>
36 <securicketauthorityurls>
37 <clear />
38 <location path="https://emea-controller.example.com/scripts/ctxsta.dll"
    />
39 <location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
40 <location path="https://apac-controller.example.com/scripts/ctxsta.dll"
    />
41 </securicketauthorityurls>
42 </gateway>
```

## Cas d'utilisation n ° 2 : Passerelles dans le fichier web.config en itinérance

```
1 <gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="Domain" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE
    " deployment="Appliance" callbackurl="https://emeagateway.example.
    com/CitrixAuthService/AuthService.asmx" sessionreliability="true"
    requesttickettwesta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
2 <location path="https://emeagateway.example.com/" />
3 <gslbLocation path=" https://emeagateway.example.net/" />
4 <clusternodes>
5 <clear />
6 </clusternodes>
7 <silentauthenticationurls>
8 <clear />
9 </silentauthenticationurls>
10 <securicketauthorityurls>
11 <clear />
12 <location path="https://emea-controller.example.net/scripts/ctxsta.dll"
    />
13 </securicketauthorityurls>
14 </gateway>
```



## Configurer l'authentification DFA entre NetScaler et StoreFront

February 26, 2019

L'authentification extensible fournit un seul point de personnalisation pour l'extension de l'authentification basée sur formulaires de StoreFront et NetScaler. Pour réaliser une solution d'authentification à l'aide du SDK Extensible Authentication, vous devez configurer l'authentification DFA entre NetScaler et StoreFront. Le protocole DFA permet de générer et de traiter les formulaires d'authentification, y compris la validation des informations d'identification, à déléguer à un autre composant. Par exemple, NetScaler délègue son authentification à StoreFront, qui interagit ensuite avec un serveur ou service d'authentification tiers.

La configuration de l'authentification DFA sur Citrix Gateway est décrite dans l'article [CTX200383](#).

### Recommandations d'installation

- Pour vous assurer que la communication entre NetScaler et StoreFront est protégée, utilisez le protocole HTTPS plutôt que le protocole HTTP.
- Pour un déploiement de cluster, assurez-vous que le même certificat de serveur est installé et configuré sur la liaison HTTPS IIS sur tous les nœuds avant de procéder aux étapes de configuration.
- Assurez-vous que l'émetteur du certificat de serveur de StoreFront Netscaler est une autorité de certification approuvée lorsque le protocole HTTPS est configuré dans StoreFront.

### Considérations relatives à l'installation de cluster StoreFront

- Installez un plug-in d'authentification tiers sur tous les nœuds avant de les associer.
- Configurez tous les paramètres associés à l'authentification DFA sur un nœud et propagez les modifications aux autres nœuds. Consultez la section « Activer l'authentification DFA ».

### Activer l'authentification DFA

Étant donné qu'il n'existe aucune interface utilisateur pour définir le paramètre de clé pré-partagée Citrix dans StoreFront, utilisez la console PowerShell pour installer l'authentification DFA.

1. Installez l'authentification DFA. Elle n'est pas installée par défaut et vous devez l'installer à l'aide de la console PowerShell.

```
1 PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
2 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
```

```
3 Adding snapins
4 Importing modules
5 Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
  DeliveryServices.ConfigurationProvider.dll'
6 Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
  DeliveryServices.ConfigurationProvider.dll'
7
8 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-
  DSDFAserver
9 Id : bf694fbc-ae0a-4d56-8749-
  c945559e897a
10 ClassType : e1eb3668-9c1c-4ad8-bbae-
  c08b2682c1bc
11 FrameworkController : Citrix.DeliveryServices.Framework
  .FileBased.FrameworkController
12 ParentInstance : 8dd182c7-f970-466c-ad4c-27
  a5980f716c
13 RootInstance : 5d0cdc75-1dee-4df7-8069-7375
  d79634b3
14 TenantId : 860e9401-39c8-4f2c-928d-34251102
  b840
15 Data : {
16 }
17
18 ReadOnlyData : {
19 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin
  , Citrix.DeliverySer
20 vices.Web.Commands], [Tenant, 860
  e9401-39c8-4f2c-928d-34251102
  b840] }
21
22 ParameterData : {
23 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [
  ParentInstanceId, 8dd182c7-f
24 970-466c-ad4c-27a5980f716c], [
  TenantId, 860e9401-39c8-4f2c
  -928d-34251102b840] }
25
26 AdditionalInstanceDependencies : {
27 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }
28
29 IsDeployed : True
30 FeatureClass : Citrix.DeliveryServices.Framework
  .Feature.FeatureClass
```

2. Ajoutez un client approuvé Citrix. Configurez la clé secrète partagée (phrase secrète) entre StoreFront et Netscaler. Votre phrase secrète et l'ID client doivent être identiques à ceux que vous avez configurés dans NetScaler.

```
1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
  DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -
  passphrase secret
```

3. Définissez la fabrique de conversation DFA afin d'acheminer tout le trafic vers le formulaire personnalisé. Pour trouver la fabrique de conversation, recherchez ConversationFactory dans C:\inetpub\wwwroot\Citrix\Authentication\web.config. Voici un exemple de ce que vous pourriez voir.

```
1 <example connectorURL="http://Example.connector.url:8080/adapters-
  sf-aaconnector-webapp">
2   <routeTable order="1000">
3     <routes>
4       <route name="StartExampleAuthentication" url="Example-
  Bridge-Forms/Start">
5         <defaults>
6           <add param="controller" value="
  ExplicitFormsAuthentication" />
7           <add param="action" value="AuthenticateStart" />
8           <add param="postbackAction" value="Authenticate" />
9           <add param="cancelAction" value="CancelAuthenticate"
  />
10          <add param="conversationFactory" value="
  ExampleBridgeAuthentication" />
11          <add param="changePasswordAction" value="
  StartChangePassword" />
12          <add param="changePasswordController" value="
  ChangePassword" />
13          <add param="protocol" value="CustomForms" />
14        </defaults>
15      </route>
```

4. Dans PowerShell, définissez la fabrique de conversation DFA. Dans cet exemple, sur ExampleBridgeAuthentication.

```
1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
  DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
```

Les arguments PowerShell ne sont pas sensibles à la casse : **-ConversationFactory** est identique à **-conversationfactory**.

## Désinstaller StoreFront

Avant de désinstaller StoreFront, désinstallez tout plug-in d'authentification tiers, car cela aura un impact sur les fonctionnalités de StoreFront.

## Authentification à l'aide de domaines différents

February 26, 2019

Certaines organisations adoptent des stratégies qui ne vous permettent pas d'accorder à des développeurs tiers ou des sous-traitants l'accès aux ressources publiées dans un environnement de production. Cet article vous explique comment accorder l'accès aux ressources publiées dans un environnement de test en vous authentifiant via NetScaler Gateway auprès d'un domaine. Vous pouvez utiliser un domaine différent pour vous authentifier auprès de StoreFront et du site Receiver pour Web. L'authentification via NetScaler Gateway décrite dans cet article est prise en charge pour les utilisateurs se connectant via le site Receiver pour Web. Cette méthode d'authentification n'est pas prise en charge pour les utilisateurs de bureaux natifs ou de Citrix Receiver mobiles.

### Configurer un environnement de test

Cet exemple utilise un domaine de production appelé `production.com` et un domaine de test appelé `development.com`.

#### **production.com** domaine

Le domaine `production.com` dans cet exemple est configuré comme suit :

- NetScaler Gateway avec la stratégie d'authentification LDAP `production.com` configurée.
- L'authentification via la passerelle se produit à l'aide d'un compte `production\testuser1` et d'un mot de passe.

#### **development.com** domaine

Le domaine `development.com` dans cet exemple est configuré comme suit :

- StoreFront, XenApp et XenDesktop 7.0 ou versions ultérieures et les VDA se trouvent tous sur le domaine `development.com`.
- L'authentification sur le site Citrix Receiver pour Web se produit à l'aide d'un compte `development\testuser1` et d'un mot de passe.
- Il n'existe aucune relation d'approbation entre les deux domaines.

## Configurer un NetScaler Gateway pour le magasin

Pour configurer un NetScaler Gateway pour le magasin :

1. Sélectionnez **Magasin** dans le panneau de gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Gérer NetScaler Gateway**.
2. Sur l'écran Gérer NetScaler Gateway, cliquez sur le bouton **Ajouter**.
3. Complétez les paramètres généraux, les paramètres Secure Ticket Authority et les paramètres d'authentification.

Add NetScaler Gateway Appliance

The screenshot shows the 'Add NetScaler Gateway Appliance' configuration window. On the left, a sidebar titled 'StoreFront' contains a menu with 'General Settings' selected, and other options: 'Secure Ticket Authority', 'Authentication Settings', and 'Summary'. The main area is titled 'General Settings' and contains the following text: 'Complete these settings to configure access to stores through NetScaler Gateway for users connecting from public networks. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores.' Below this text are three input fields: 'Display name:' with the value 'ProductionGateway', 'NetScaler Gateway URL:' with the value 'https://gateway.production.com', and 'Usage or role:' with a dropdown menu set to 'Authentication and HDX routing'. At the bottom right, there are two buttons: 'Next' (highlighted in blue) and 'Cancel'.

Add NetScaler Gateway Appliance

**StoreFront**

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

### Secure Ticket Authority (STA)

STA is hosted on XenDesktop, XenApp, and VDI-in-a-Box servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop, XenApp, and VDI-in-a-Box resources.

Secure Ticket Authority URLs: ⓘ

- https://sta1.development.com/scripts/cbxsta.dll
- https://sta2.development.com/scripts/cbxsta.dll

Buttons: Add... Edit... Remove

Load balance multiple STA servers

Bypass failed STA for: 1 hours 0 minutes 0 seconds

Enable session reliability ⓘ

Request tickets from two STAs, where available ⓘ

Buttons: Back Next Cancel

Edit NetScaler Gateway appliance - ProductionGateway

**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

VServer IP address: (optional)

Logon type: ⓘ Domain

Smart card fallback: None

Callback URL: ⓘ https://callback.production.com /CitrixAuthService/AuthService.asmx

Buttons: OK Cancel Apply

**Remarque :**




Il sera peut-être nécessaire d'ajouter des redirecteurs conditionnels DNS afin que les serveurs DNS utilisés sur les deux domaines puissent résoudre les noms de domaine complets sur l'autre domaine. NetScaler doit être en mesure de résoudre les noms de domaine complets du serveur STA sur le domaine `development.com` à l'aide de son serveur DNS `production.com`. StoreFront doit également être en mesure de résoudre l'URL de rappel sur le domaine `production.com` à l'aide de son serveur DNS `development.com`. Un nom de domaine complet `development.com` peut également être utilisé qui résout l'adresse IP virtuelle (VIP) du vServer NetScaler Gateway.

**Activer l'authentification pass-through depuis NetScaler Gateway**

1. Sélectionnez **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification**.
2. Sur l'écran Gérer les méthodes d'authentification, sélectionnez **Authentification pass-through via NetScaler Gateway**.
3. Cliquez sur **OK**.

**Manage Authentication Methods - Store**

Select the methods which users will use to authenticate and access resources. i

Method	Settings
<input checked="" type="checkbox"/> User name and password	
<input type="checkbox"/> SAML Authentication	
<input type="checkbox"/> Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
<input type="checkbox"/> Smart card Can be enabled / disabled separately on Receiver for Web sites	
<input type="checkbox"/> HTTP Basic	
<input checked="" type="checkbox"/> Pass-through from NetScaler Gateway	

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options. Advanced ▾

OK Cancel

## Configurer le magasin pour l'accès distant à l'aide de Netscaler Gateway

1. 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 d'accès distant**.
2. Sélectionnez **Activer l'accès à distance**.
3. Assurez-vous que vous avez enregistré le NetScaler Gateway auprès de votre magasin. Si vous n'enregistrez pas le NetScaler Gateway, la fonctionnalité de ticket STA ne fonctionnera pas.

### Configure Remote Access Settings - Store

Enabling remote access allows users outside the firewall to securely access resources. After you enable remote access, add a NetScaler Gateway appliance.

Enable Remote Access

Select the permitted level of access to internal resources

Allow users to access only resources delivered through StoreFront (No VPN tunnel) i

Allow users to access all resources on the internal network (Full VPN tunnel) i

Users may require the NetScaler Gateway Plug-in to establish a full VPN tunnel.

NetScaler Gateway appliances:

<input checked="" type="checkbox"/> ProductionGateway <span style="float: right;">i</span>

Add...

Default appliance:

ProductionGateway ▼

OK

Cancel

## Désactiver la cohérence des jetons

1. 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**.
2. Sur la page Configurer les paramètres du magasin, sélectionnez **Paramètres avancés**.
3. Décochez la case **Exiger la cohérence des jetons**. Pour plus d'informations, consultez la section [Paramètres de magasin avancés](#).



4. Cliquez sur **OK**.

Configure Store Settings - Store

**StoreFront**

**Advanced Settings**

Configure advanced settings with caution.

Communication timeout duration	30
Connection timeout	6
Enable enhanced enumeration	<input checked="" type="checkbox"/>
Enable socket pooling	<input type="checkbox"/>
Filter resources by excluded keywords	
Filter resources by included keywords	
Filter resources by type	
Maximum concurrent enumerations	0
Minimum farms for concurrent enumeration	3
Override ICA client name	<input type="checkbox"/>
<b>Require token consistency</b>	<input checked="" type="checkbox"/>
Server communication attempts	1
Show Desktop Viewer for legacy clients	<input type="checkbox"/>

**Require token consistency**  
When enabled, StoreFront enforces consistency between the gateway used to authenticate and the gateway used to access the store. When the values are inconsistent, users must reauthenticate. Must be enabled for Smart Access. Default: On

OK Cancel Apply

**Remarque**

Le paramètre Exiger la cohérence des jetons est sélectionné (activé) par défaut. Si vous désactivez ce paramètre, les fonctionnalités SmartAccess utilisées pour l'analyse de point de terminaison NetScaler Gateway (EPA) cessent de fonctionner. Pour plus d'informations sur SmartAccess, consultez l'article [CTX138110](#).

## Désactiver l'authentification pass-through depuis NetScaler Gateway pour le site Receiver pour Web

**Important :**

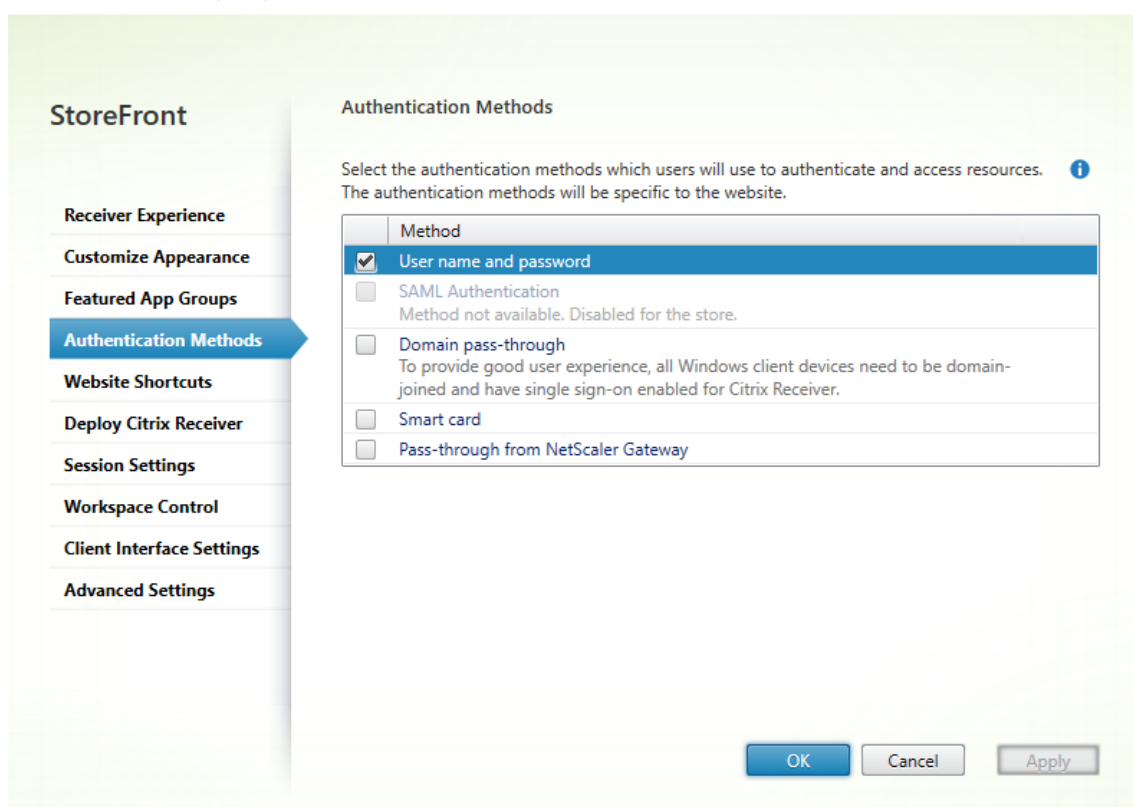
La désactivation de l'authentification pass-through depuis NetScaler Gateway empêche Receiver pour Web d'utiliser les informations d'identification incorrectes du domaine `production.com` transmises depuis NetScaler. Lorsque l'authentification pass-through est désactivée depuis NetScaler Gateway, Receiver pour Web invite l'utilisateur à entrer des informations d'identification. Ces informations d'identification sont différentes des informations d'identification utilisées pour se connecter via Netscaler Gateway.

1. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix Store-

Front.

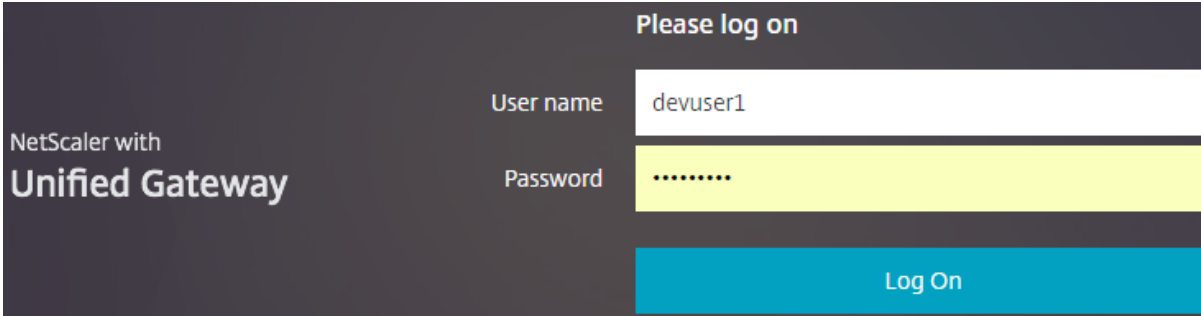
2. Sélectionnez le **magasin** que vous souhaitez modifier.
3. Dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web**.
4. Dans Méthodes d'authentification, désactivez l'authentification pass-through depuis la case NetScaler Gateway.
5. Cliquez sur **OK**.

Edit Receiver for Web site - /Citrix/StoreWeb

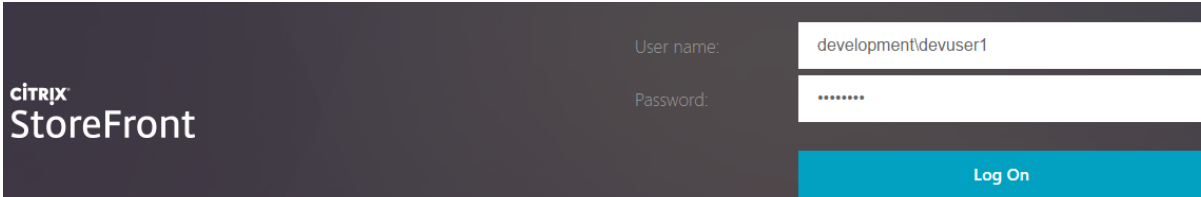


## Connexion à Netscaler Gateway à l'aide d'un utilisateur `production.com` et d'informations d'identification

Pour tester, connectez-vous à Netscaler Gateway à l'aide d'un utilisateur `production.com` et d'informations d'identification.



Après la connexion, l'utilisateur est invité à entrer des informations d'identification `development.com`.



### Ajouter une liste déroulante de domaine de confiance dans StoreFront (facultatif)

Ce paramètre est facultatif, mais il peut vous aider à empêcher l'utilisateur d'entrer accidentellement le domaine incorrect pour l'authentification via NetScaler Gateway.

Si le nom d'utilisateur est le même pour les deux domaines, il y a davantage de chances qu'un domaine incorrect soit entré. De nouveaux utilisateurs peuvent également être utilisés pour exclure le domaine lorsqu'ils se connectent via NetScaler Gateway. Il se peut que les utilisateurs oublient d'entrer le domaine\nnomd'utilisateur pour le second domaine lorsqu'ils sont invités à se connecter au site Receiver pour Web.

1. Sélectionnez **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Gérer les méthodes d'authentification**.
2. Sélectionnez la flèche déroulante à côté de **Nom d'utilisateur et mot de passe**.
3. Cliquez sur **Ajouter** pour ajouter `development.com` comme domaine de confiance et sélectionnez la case **Afficher la liste des domaines dans la page d'ouverture de session**.
4. Cliquez sur **OK**.

## Configure Trusted Domains

Allow users to log on from:  Any domain  
 Trusted domains only

Trusted domains:

Default domain:

Show domains list in logon page

OK

Cancel

**CITRIX**  
StoreFront

User name:

Password:

Domain:

**Remarque :**

La mise en cache du mot de passe de navigateur n'est pas recommandée dans ce scénario d'authentification. Si les utilisateurs disposent de mots de passe différents pour les deux comptes de domaine différents, la mise en cache du mot de passe peut entraîner une mauvaise expérience.

**Stratégie d'action de session VPN NetScaler sans client (CVPN)**

- Si le paramètre Authentification unique auprès des applications Web est activé dans votre stratégie de session NetScaler, les informations d'identification incorrectes envoyées par NetScaler à Receiver pour Web sont ignorées car vous avez désactivé la méthode d'authentification **Authentification pass-through via NetScaler Gateway** sur le site Receiver pour Web. Receiver pour Web vous invite à entrer les informations d'identification, quelle que soit la valeur de cette option.
- Le remplissage des entrées de Single Sign-on dans les onglets Client Experience et Published

App de NetScaler ne change pas le comportement décrit dans cet article.

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration	Client Experience	Security	Published Applications
Accounting Policy			
<input type="text"/>			
Override Global			
<input checked="" type="checkbox"/> Display Home Page			
Home Page			
<input type="text" value="https://sf.development.com/Citrix/S"/> <input checked="" type="checkbox"/>			
URL for Web-Based Email			
<input type="text"/> <input type="checkbox"/>			
Split Tunnel*			
<input type="text" value="OFF"/> <input type="checkbox"/>			
Session Time-out (mins)			
<input type="text" value="60"/> <input checked="" type="checkbox"/>			
Client Idle Time-out (mins)			
<input type="text"/> <input type="checkbox"/>			
Clientless Access*			
<input type="text" value="On"/> <input checked="" type="checkbox"/>			
Clientless Access URL Encoding*			
<input type="text" value="Clear"/> <input checked="" type="checkbox"/>			
Clientless Access Persistent Cookie*			
<input type="text" value="ALLOW"/> <input checked="" type="checkbox"/>			
Plug-in Type*			
<input type="text" value="Windows/MAC OS X"/> <input type="checkbox"/>			
Windows Plugin Upgrade			
<input type="text" value="Always"/> <input type="checkbox"/>			
Linux Plugin Upgrade			
<input type="text" value="Always"/> <input type="checkbox"/>			
MAC Plugin Upgrade			
<input type="text" value="Always"/> <input type="checkbox"/>			
AlwaysON Profile Name			
<input type="text"/> <input type="button" value="+"/> <input type="button" value="edit"/> <input type="checkbox"/>			
<input type="checkbox"/> Single Sign-on to Web Applications <input type="checkbox"/>			
Credential Index*			
<input type="text" value="PRIMARY"/> <input checked="" type="checkbox"/>			
KCD Account			
<input type="text"/> <input type="button" value="+"/> <input type="button" value="edit"/> <input type="checkbox"/> <input type="button" value="help"/>			
Single Sign-on with Windows*			
<input type="text" value="OFF"/> <input type="checkbox"/>			
Client Cleanup Prompt*			
<input type="text" value="ON"/> <input type="checkbox"/>			
<input type="checkbox"/> <a href="#">Advanced Settings</a>			

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration	Client Experience	Security	Published App
Override Global			
ICA Proxy*			
OFF			<input checked="" type="checkbox"/>
Web Interface Address			
https://sf.development.com/Citrix/S			<input checked="" type="checkbox"/>
Web Interface Address Type*			
IPV4			
Web Interface Portal Mode*			
NORMAL			<input type="checkbox"/>
Single Sign-on Domain			
			<input type="checkbox"/>
Citrix Receiver Home Page			
			<input type="checkbox"/>
Account Services Address			
			<input type="checkbox"/>

## Configurer des points balises

February 20, 2019

Utilisez la tâche Gérer les balises pour spécifier les adresses URL à l'intérieur et à l'extérieur de votre réseau interne à utiliser comme points balises. Citrix Receiver tente de contacter des points balises et utilise les réponses pour 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 garantit que les utilisateurs ne sont pas invités à rouvrir une

session lorsqu'ils accèdent à un bureau ou une application.

Par exemple, si le point balise interne est accessible, cela indique que l'utilisateur est connecté au réseau local. Toutefois, si Citrix Receiver ne parvient pas à contacter le point balise interne et reçoit les réponses à partir des points balises externes, cela signifie que l'utilisateur dispose d'une connexion Internet, mais qu'il se trouve en dehors du réseau de l'entreprise. Par conséquent, l'utilisateur doit se connecter aux bureaux et aux applications via NetScaler Gateway. Lorsque l'utilisateur accède à un bureau ou une application, le serveur qui fournit la ressource est averti qu'il doit fournir les détails relatifs que boîtier NetScaler Gateway par le biais duquel la connexion doit être routée. Cela signifie que l'utilisateur n'a pas besoin d'ouvrir une session sur le boîtier lors de l'accès au bureau ou à l'application.

Par défaut, StoreFront utilise l'adresse URL du serveur ou l'URL à charge équilibrée de votre déploiement comme point balise interne. Les adresses URL du site Web de Citrix et du serveur virtuel ou du point d'ouverture de session utilisateur (pour Access Gateway 5.0) du premier déploiement NetScaler Gateway que vous ajoutez sont utilisées en tant que points balises externes par défaut.

Si vous modifiez des points balises, assurez-vous que les utilisateurs mettent à jour Citrix Receiver à l'aide des informations modifiées sur les points balises. Lorsqu'un site Receiver pour Web est configuré pour un magasin, les utilisateurs peuvent obtenir un fichier de provisioning Citrix Receiver mis à jour à partir du site. Sinon, vous pouvez [exporter un fichier de provisioning](#) pour le magasin et mettre ce fichier à la disposition de vos utilisateurs.

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 les modifications terminées,

[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 balises**.
3. Spécifiez l'URL à utiliser comme point de balise interne.
  - Pour utiliser l'URL du serveur ou l'adresse URL à charge équilibrée de votre déploiement StoreFront, sélectionnez **Utiliser l'URL de service**.
  - Pour utiliser une autre URL, sélectionnez **Spécifier l'adresse de la balise** et entrez une adresse URL à haut niveau de disponibilité dans votre réseau interne.
4. Cliquez sur **Ajouter** pour entrer l'adresse l'URL d'un point balise externe. Pour modifier un point balise, sélectionnez l'URL dans la liste Balises externes et cliquez sur **Modifier**. Sélectionnez une



adresse URL dans la liste et cliquez sur **Supprimer** pour ne plus utiliser cette adresse comme point balise.

Vous devez spécifier au moins deux points balises externes hautement disponibles pouvant être résolus depuis des réseaux publics. Les URL de balises doivent être des noms de domaine complets (<http://example.com>) et non le nom NetBIOS abrégé (<http://example>). Ceci permet à Citrix Receiver de déterminer si les utilisateurs se trouvent derrière un Internet payant, comme dans un hôtel ou un cybercafé. Dans de tels cas, tous les points balises externes se connectent au même proxy.

## Configurations avancées

September 21, 2018

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Vous pouvez configurer les options avancées suivantes à l'aide de la console StoreFront, de PowerShell, de propriétés de certificat ou de fichiers de configuration.

---

#### Configurer des sites Desktop Appliance

Permet de créer, supprimer et modifier des sites Desktop Appliance.

#### Créer un seul nom de domaine complet (FQDN) pour accéder à un magasin en interne et externe

Permet de fournir un accès aux ressources depuis le réseau de votre entreprise et depuis Internet par le biais d'un NetScaler Gateway et de simplifier l'expérience utilisateur en créant un seul nom de domaine complet (FQDN) pour les clients externes itinérants et les clients internes.

#### Configurer le filtrage des ressources

Permet de filtrer les ressources d'énumération en fonction du type de ressource et de mots clés.

---

## Configurer des sites Desktop Appliance

February 20, 2019

Les tâches ci-dessous décrivent comment créer, supprimer et modifier des sites Desktop Appliance. Pour créer ou supprimer des sites, vous devez exécuter des commandes Windows PowerShell. Les modifications apportées aux paramètres d'un site Desktop Appliance sont effectuées en modifiant les fichiers de configuration de 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 les modifications terminées,

[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 :**

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.

## Pour créer ou supprimer des sites Desktop Appliance

Seul un magasin unique est accessible via chaque site Desktop Appliance. Vous pouvez créer un magasin contenant toutes les ressources que vous voulez mettre à la disposition des utilisateurs avec des boîtiers de bureau n'appartenant pas à un domaine. Vous pouvez également créer des magasins, chacun avec un site Desktop Appliance et configurer les boîtiers de bureau de vos utilisateurs pour qu'ils se connectent au site approprié.

1. Utilisez un compte possédant des permissions d'administrateur local pour démarrer Windows PowerShell et, à l'invite de commande, tapez la commande suivante pour importer les modules StoreFront.

```
1 & "installationlocation\Scripts\ImportModules.ps1"
```

Où **installationlocation** est le répertoire dans lequel StoreFront est installé, généralement C:\Program Files\Citrix\Receiver StoreFront\.

2. Pour créer un nouveau site Desktop Appliance, tapez la commande suivante.

```
1 Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid
2   -VirtualPath sitepath -UseHttps {
3     $False | $True }
4
5   -StoreUrl storeaddress [-EnableMultiDesktop {
6     $False | $True }
```

```
7 ]
8   [-EnableExplicit {
9     $True | $False }
10 ] [-EnableSmartCard {
11   $False | $True }
12 ]
13   [-EnableEmbeddedSmartCardSSO {
14     $False | $True }
15 ]
```

Où *sitename* est un nom qui vous aidera à identifier votre site Desktop Appliance. Pour *isid*, spécifiez l'ID numérique du site Microsoft Internet Information Services (IIS) hébergeant StoreFront, qui peut être obtenu à partir de la console Gestionnaire des services Internet (IIS). Remplacez *sitepath* avec le chemin d'accès relatif dans lequel le site doit être créé dans IIS, par exemple, /Citrix/DesktopAppliance. Notez que les adresses URL des sites Desktop Appliance sont sensibles à la casse.

Indiquez si StoreFront est configuré pour utiliser HTTPS en définissant **-UseHttps** sur la valeur appropriée.

Pour spécifier l'adresse URL absolue du service de magasin utilisée par le site Desktop Appliance Connector, utilisez **StoreUrl** *adressesmagasin*. Cette valeur est affichée dans le résumé du magasin sur la console d'administration.

Par défaut, lorsqu'un utilisateur ouvre une session sur un site Desktop Appliance, le premier bureau disponible pour l'utilisateur démarre automatiquement. Pour configurer votre nouveau site Desktop Appliance pour permettre aux utilisateurs de choisir entre plusieurs bureaux, si disponible, définissez **-EnableMultiDesktop** sur **\$True**.

L'authentification explicite est activée par défaut pour les nouveaux sites. Vous pouvez désactiver l'authentification explicite en définissant l'argument **-EnableExplicit** sur **\$False**. Activez l'authentification par carte à puce en définissant **-EnableSmartCard** sur **\$True**. Pour activer l'authentification pass-through par carte à puce, vous devez définir **-EnableSmartCard** et **-EnableEmbeddedSmartCardSSO** sur **\$True**. Si vous activez l'authentification explicite et l'authentification par carte à puce ou l'authentification pass-through par carte à puce, les utilisateurs sont initialement invités à ouvrir une session avec une carte à puce, mais ils peuvent revenir à l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce.

Les arguments facultatifs configurent des paramètres qui peuvent également être modifiés après la création du site Desktop Appliance en modifiant le fichier de configuration du site.

#### Exemple :

Créez un site Desktop Appliance Connector sur le chemin virtuel /Citrix/DesktopAppliance1 dans le site Web IIS par défaut.

```
1 Install-DSDesktopAppliance ‘
2 -FriendlyName DesktopAppliance1 ‘
3 -SiteId 1 ‘
4 -VirtualPath /Citrix/DesktopAppliance1 ‘
5 -UseHttps $false ‘
6 -StoreUrl https://serverName/Citrix/Store ‘
7 -EnableMultiDesktop $true ‘
8 -EnableExplicit $true ‘
9 -EnableSmartCard $true ‘
10 -EnableEmbeddedSmartCardSSO $false
```

3. Pour supprimer un site Desktop Appliance existant, tapez la commande suivante.

```
Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
```

où iisid est l’ID numérique du site IIS hébergeant StoreFront et sitepath est le chemin d’accès relatif au site Desktop Appliance dans IIS, par exemple, /Citrix/DesktopAppliance.

4. Pour répertorier les sites Desktop Appliance actuellement disponibles depuis votre déploiement StoreFront, tapez la commande suivante.

```
Get-DSDesktopAppliancesSummary
```

## Pour configurer l’authentification utilisateur

Les sites Desktop Appliance prennent en charge l’authentification explicite, l’authentification par carte à puce et l’authentification pass-through avec carte à puce. L’authentification explicite est activée par défaut. Si vous activez l’authentification explicite et l’authentification par carte à puce ou l’authentification pass-through par carte à puce, le comportement par défaut invite les utilisateurs à ouvrir une session à l’aide d’une carte à puce. Les utilisateurs qui rencontrent des problèmes avec leur carte à puce ont la possibilité de saisir des informations d’identification explicites. Si vous configurez IIS afin de demander des certificats client pour les connexions HTTPS à toutes les adresses URL de StoreFront, les utilisateurs ne peuvent pas revenir à l’authentification explicite s’ils rencontrent des problèmes avec leur carte à puce. Pour configurer les méthodes d’authentification pour un site Desktop Appliance, modifiez le fichier de configuration du site.

1. Utilisez un éditeur de texte pour ouvrir le fichier web.config du site Desktop Appliance, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance, où storename désigne le nom attribué au magasin au moment de sa création.
2. Recherchez l’élément suivant dans le fichier.

```
<explicitForms enabled="true"/>
```

3. Modifiez la valeur de l'attribut `enabled` sur `false` afin de désactiver l'authentification explicite pour le site.
4. Recherchez l'élément suivant dans le fichier.

```
<certificate enabled="false" useEmbeddedSmartcardSso="false" embeddedSmartcardSsoPinTimeout="00:00:20"/>
```

5. Définissez la valeur de l'attribut `enabled` sur `true` pour activer l'authentification par carte à puce. Pour activer l'authentification pass-through par carte à puce, vous devez également définir la valeur de l'attribut **`useEmbeddedSmartcardSso`** sur la valeur `true`. Utilisez l'attribut **`embeddedSmartcardSsoPinTimeout`** pour définir la durée en heures, minutes et secondes pendant laquelle l'écran de saisie du code PIN est affiché avant de disparaître. Lorsque l'écran de saisie du code PIN expire, les utilisateurs sont renvoyés à l'écran d'ouverture de session et doivent retirer et réinsérer leur carte à puce pour accéder de nouveau à l'écran de saisie du code PIN. Le délai d'attente est défini par défaut sur 20 secondes.

## Pour permettre aux utilisateurs de choisir entre plusieurs bureaux

Par défaut, lorsqu'un utilisateur ouvre une session sur un site Desktop Appliance, le premier bureau (par 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 modifier ces paramètres, modifiez le fichier de configuration du site.

1. Utilisez un éditeur de texte pour ouvrir le fichier `web.config` du site Desktop Appliance, qui se trouve en général dans le répertoire `C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance`, où `storename` désigne le nom attribué au magasin au moment de sa création.
2. Recherchez l'élément suivant dans le fichier.

```
<resources showMultiDesktop="false"/>
```

3. Modifiez la valeur de l'attribut `showMultiDesktop` sur `true` pour permettre aux utilisateurs d'afficher et de sélectionner parmi tous les bureaux disponibles dans le magasin lorsqu'ils ouvrent une session sur le site Desktop Appliance.

## Créer un seul nom de domaine complet (FQDN) pour accéder à un magasin en interne et externe

February 20, 2019

**Remarque :**

Pour utiliser cette fonctionnalité avec des Desktop Receiver natifs, les versions suivantes sont requises :

- Windows Receiver 4.2
- MAC Receiver 11.9

Vous pouvez fournir un accès aux ressources depuis le réseau de votre entreprise et depuis Internet par le biais d'un NetScaler Gateway et simplifier l'expérience utilisateur en créant un seul nom de domaine complet (FQDN) pour à la fois les clients externes itinérants et les clients internes.

La création d'un seul nom de domaine complet est utile pour les utilisateurs qui configurent l'un des logiciels Receiver natifs. Ils n'ont besoin de mémoriser qu'une seule adresse URL qu'ils soient connectés à un réseau interne ou public.

### **Balises StoreFront pour Receiver natifs**

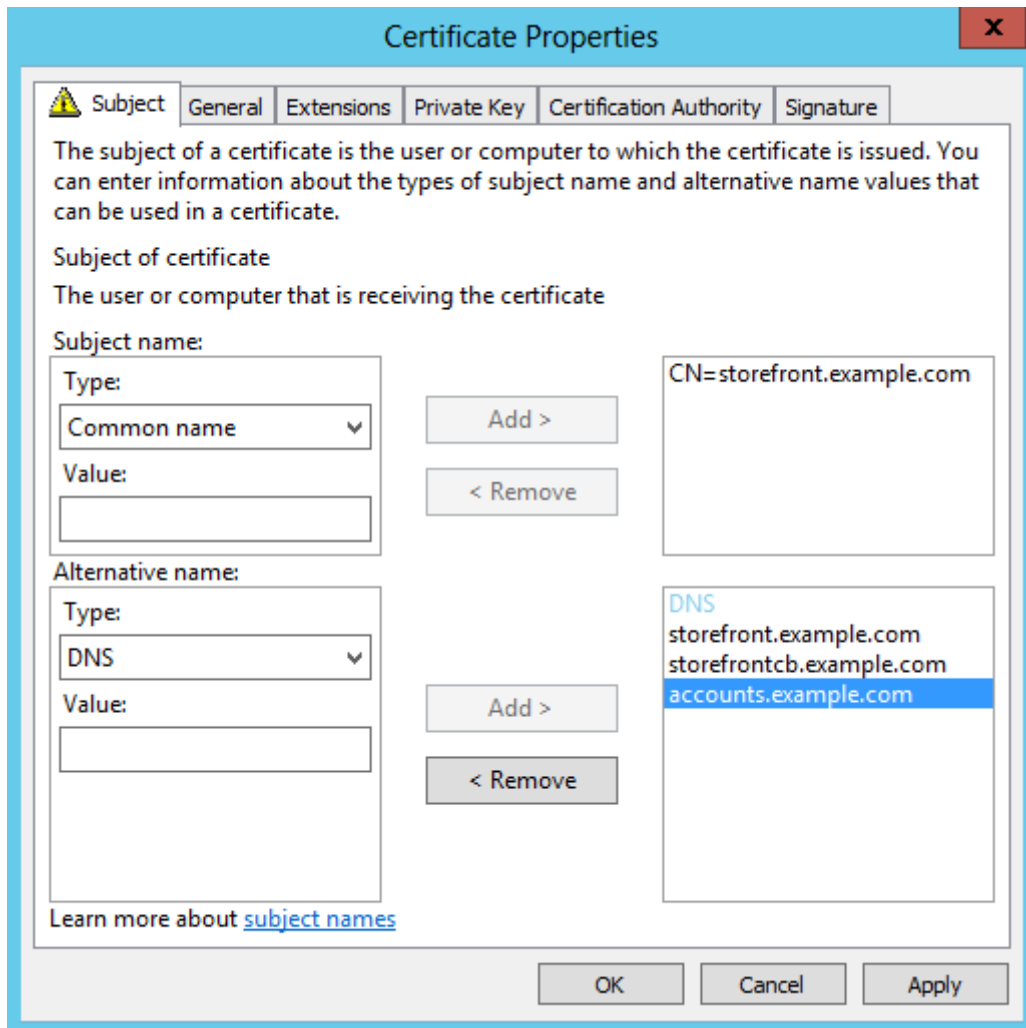
Citrix Receiver tente de contacter des points balises et utilise les réponses pour déterminer si les utilisateurs sont connectés à des réseaux locaux ou publics. Lorsqu'un utilisateur accède à un bureau ou une application, les informations d'emplacement sont transmises au serveur fournissant les ressources afin que les détails de connexion appropriés puissent être renvoyés à Citrix Receiver. Ceci garantit que les utilisateurs ne sont pas invités à rouvrir une session lorsqu'ils accèdent à un bureau ou une application. Pour plus d'informations sur la configuration des points balises, consultez la section [Configurer des points balises](#).

### **Configurez le vServer NetScaler Gateway et le certificat SSL**

Le nom de domaine complet (FQDN) partagé est résolu sur l'adresse IP de l'interface de routeur du pare-feu externe où sur l'adresse IP vServer NetScaler Gateway dans la zone démilitarisée (DMZ) lorsque les clients externes essaient d'accéder aux ressources en dehors du réseau d'entreprise. Assurez-vous que les champs Nom commun et Autre nom de l'objet du certificat SSL contiennent le nom de domaine complet partagé à utiliser pour accéder au magasin en externe. En utilisant une autorité de certification racine tierce telle que Verisign au lieu d'une autorité de certification d'entreprise pour signer le certificat de passerelle, tout client externe approuve automatiquement le certificat lié au vServer de passerelle. Si vous utilisez une autorité de certification racine tierce telle que Verisign, aucun certificat d'autorité de certification racine supplémentaire ne doit être importé sur des clients externes.

Pour déployer un seul certificat avec le nom commun du nom de domaine complet (FQDN) partagé sur le serveur NetScaler Gateway et le serveur StoreFront, vous devez décider si vous souhaitez prendre

en charge la découverte à distance. Si c'est le cas, vérifiez que le certificat est conforme à la spécification relative aux Autres noms de l'objet.



### Exemple de certificat NetScaler Gateway vServer : storefront.example.com

1. Assurez-vous que le nom de domaine complet partagé, l'URL de rappel et l'URL d'alias des comptes sont inclus dans le champ DNS en tant qu'Autre nom de l'objet (SAN).
2. Vérifiez que la clé privée est exportable de façon à ce que le certificat et la clé puissent être importés dans NetScaler Gateway.
3. Assurez-vous que Default Authorization est défini sur Allow.
4. Signez le certificat à l'aide d'une autorité de certification tierce telle que Verisign ou d'une autorité de certification racine d'entreprise pour votre organisation.

### Exemples d'autre nom de l'objet pour groupe de serveurs à deux nœuds

`storefront.example.com` (obligatoire)

`storefrontcb.example.com` (obligatoire)

`accounts.example.com` (obligatoire)

`storefrontserver1.example.com` (facultatif)

`storefrontserver2.example.com` (facultatif)

## **Signer le certificat SSL vServer Netscaler Gateway à l'aide d'une autorité de certification (CA)**

En fonction de vos besoins, vous disposez de deux options pour choisir le type de certificat signé par une autorité de certification.

- Option 1: certificat signé par une autorité de certification tierce. Si le certificat lié au vServer Netscaler Gateway est signé par un tiers de confiance, les clients externes n'auront probablement PAS besoin de copier les certificats d'autorité de certification racine dans leurs magasins de certificats d'autorité de certification racine de confiance. Les clients Windows sont livrés avec les certificats d'autorité de certification racine des agences de signature les plus courantes. Les autorités de certification tierces commerciales pouvant être utilisées comprennent DigiCert, Thawte et Verisign. Notez que les appareils mobiles tels que iPad, iPhone et tablettes et téléphones Android peuvent encore nécessiter la copie de l'autorité de certification racine sur l'appareil pour faire confiance au vServer NetScaler Gateway.
- Option 2 : certificat signé par une autorité de certification racine d'entreprise : si vous choisissez cette option, tous les clients externes nécessitent que le certificat d'autorité de certification racine d'entreprise soit copié sur leurs magasins d'autorité de certification racine de confiance. Si vous utilisez des appareils portables avec Receiver natif, tels que les iPhones et les iPad, créez un profil de sécurité sur ces appareils.

## **Importer le certificat racine sur des appareils mobiles**

- Les appareils iOS peuvent importer des fichiers de certificat .CER x.509 par le biais de pièces jointes, car l'accès au stockage local des appareils iOS n'est généralement pas possible.
- Les appareils Android requièrent le même format .CER x.509. Le certificat peut être importé à partir du stockage local de l'appareil ou des pièces jointes.

## **DNS externe : storefront.example.com**

Assurez-vous que la résolution DNS fournie par le fournisseur de services Internet de votre organisation est soit résolue sur l'adresse IP externe du routeur de pare-feu en périphérie extérieure de la zone



démilitarisée (DMZ), soit sur l'adresse IP virtuelle du vServer NetScaler Gateway.

## Split-view DNS

- Lorsque la vue split-view DNS est correctement configurée, l'adresse source de la requête DNS doit envoyer le client vers l'enregistrement DNS A correct.
- Lorsque les clients accèdent à des réseaux publics et réseaux d'entreprise, leur adresse IP doit s'adapter. En fonction du réseau auquel ils sont actuellement connectés, ils doivent recevoir l'enregistrement A correct lorsqu'ils interrogent storefront.exemple.com.

## Importer des certificats émis par une autorité de certification Windows sur NetScaler Gateway

WinSCP est un outil tiers utile pour déplacer des fichiers d'un ordinateur Windows sur un système de fichiers NetScaler Gateway. Copiez les certificats à importer sur le dossier `/nsconfig/ssl/` dans le système de fichiers NetScaler Gateway. Vous pouvez utiliser les outils OpenSSL de NetScaler Gateway pour extraire le certificat et la clé depuis un fichier PKCS12/PFX afin de créer deux fichiers `.CER` et `.KEY` X.509 distincts au format PEM pouvant être utilisés par NetScaler Gateway.

1. Copiez le fichier PFX dans `/nsconfig/ssl` sur le boîtier NetScaler Gateway ou VPX.
2. Ouvrez l'interface de ligne de commande NetScaler Gateway.
3. Pour basculer vers le shell FreeBSD, tapez **Shell** pour quitter l'interface de ligne de commande NetScaler Gateway.
4. Pour changer de répertoire, utilisez `cd /nsconfig/ssl`.
5. Exécutez `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` et entrez le mot de passe PFX à l'invite correspondante.
6. Exécutez `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key`
7. Entrez le mot de passe du fichier PFX lorsque vous y êtes invité, puis définissez une phrase secrète au format PEM pour la clé privée pour protéger le fichier `.KEY`.
8. Pour vous assurer que les fichiers `.CER` et `.KEY` ont été correctement créés dans `/nsconfig/ssl/`, exécutez `ls -al`.
9. Pour retourner à l'interface de ligne de commande NetScaler Gateway, tapez sur Exit.

## Stratégie de session de la passerelle Receiver Windows/Mac native

```
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS
```

## Stratégie de session de la passerelle Receiver pour Web

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

### Paramètres cVPN et Smart Access

Si vous utilisez SmartAccess, activez le mode Smart Access sur la page des propriétés de vServer NetScaler Gateway. Des licences universelles sont requises pour chaque utilisateur simultané qui accède à des ressources distantes.

### Profil Receiver

**Configure NetScaler Gateway Session Profile** ✕

Name\*

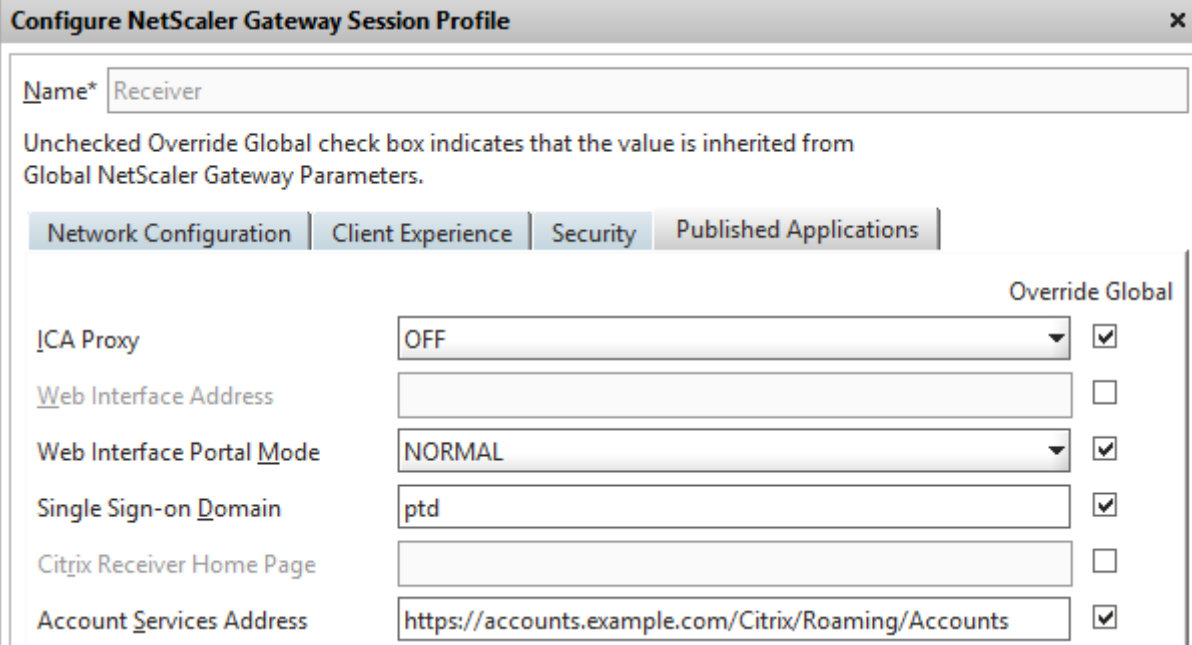
Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration
Client Experience
Security
Published Applications

		Override Global
Home Page	<input type="text" value="none"/> <input type="checkbox"/> Display Home Page	<input type="checkbox"/>
URL for Web-Based Email	<input type="text"/>	<input type="checkbox"/>
Split Tunnel	<input type="text" value="OFF"/>	<input type="checkbox"/>
Session Time-out (mins)	<input type="text" value="60"/>	<input checked="" type="checkbox"/>
Client Idle Time-out (mins)	<input type="text"/>	<input type="checkbox"/>
Clientless Access	<input type="text" value="On"/>	<input checked="" type="checkbox"/>
Clientless Access URL Encoding	<input type="text" value="Clear"/>	<input checked="" type="checkbox"/>
Clientless Access Persistent Co...	<input type="text" value="ALLOW"/>	<input checked="" type="checkbox"/>
Plug-in Type	<input type="text" value="Windows/Mac OS X"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Single Sign-on to Web Applications		<input checked="" type="checkbox"/>
Credential Index	<input type="text" value="PRIMARY"/>	<input type="checkbox"/>
KCD Account	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Single Sign-on with Windows		<input type="checkbox"/>
<input type="checkbox"/> Client Cleanup Prompt		<input type="checkbox"/>

[Advanced](#)

Configurez l'URL du service de comptes de profil de session sur <https://accounts.example.com/Citrix/Roaming/Accounts> et NON sur <https://storefront.example.com/Citrix/Roaming/Accounts>.



		Override Global
ICA Proxy	OFF	<input checked="" type="checkbox"/>
Web Interface Address		<input 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	<a href="https://accounts.example.com/Citrix/Roaming/Accounts">https://accounts.example.com/Citrix/Roaming/Accounts</a>	<input checked="" type="checkbox"/>

Ajoutez également cette URL en tant que <allowedAudiences> supplémentaire dans les fichiers de configuration d'authentification et d'itinérance web.config sur le serveur StoreFront. Pour de plus amples informations, consultez la section « Configurer l'URL de base de l'hôte serveur StoreFront, la passerelle et le certificat SSL » ci-dessous.

## Profil Receiver pour Web

**Configure NetScaler Gateway Session Profile**
✕

Name\*

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	<input type="text" value="none"/> <input type="checkbox"/> Display Home Page	<input type="checkbox"/>
URL for Web-Based Email	<input type="text"/>	<input type="checkbox"/>
Split Tunnel	<input type="text" value="OFF"/>	<input type="checkbox"/>
Session Time-out (mins)	<input type="text" value="60"/>	<input checked="" type="checkbox"/>
Client Idle Time-out (mins)	<input type="text"/>	<input type="checkbox"/>
Clientless Access	<input type="text" value="On"/>	<input checked="" type="checkbox"/>
Clientless Access URL Encoding	<input type="text" value="Clear"/>	<input checked="" type="checkbox"/>
Clientless Access Persistent Co...	<input type="text" value="ALLOW"/>	<input checked="" type="checkbox"/>
Plug-in Type	<input type="text" value="Windows/Mac OS X"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Single Sign-on to Web Applications		<input checked="" type="checkbox"/>
Credential Index	<input type="text" value="PRIMARY"/>	<input type="checkbox"/>
KCD Account	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Single Sign-on with Windows		<input type="checkbox"/>
<input type="checkbox"/> Client Cleanup Prompt		<input type="checkbox"/>

[Advanced](#)

**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

		Override Global
ICA Proxy	OFF	<input checked="" type="checkbox"/>
Web Interface Address	https://storefront.example.com/Citrix/StoreWeb	<input checked="" type="checkbox"/>
Web Interface Portal Mode	NORMAL	<input checked="" type="checkbox"/>
Single Sign-on Domain	example	<input checked="" type="checkbox"/>
Citrix Receiver Home Page		<input type="checkbox"/>
Account Services Address		<input type="checkbox"/>

### Paramètres ICA Proxy et du mode Basic

Si vous utilisez un serveur proxy ICA, activez le mode de base sur la page des propriétés de vServer NetScaler Gateway. Seule une licence de plate-forme Netscaler est requise.

## Profil Receiver

**Configure NetScaler Gateway Session Profile**
✕

Name\*

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	<input type="text" value="none"/> <input type="checkbox"/> Display Home Page	<input type="checkbox"/>
URL for Web-Based Email	<input type="text"/>	<input type="checkbox"/>
Split Tunnel	<input type="text" value="OFF"/>	<input type="checkbox"/>
Session Time-out (mins)	<input type="text" value="60"/>	<input checked="" type="checkbox"/>
Client Idle Time-out (mins)	<input type="text"/>	<input type="checkbox"/>
Clientless Access	<input type="text" value="Off"/>	<input checked="" type="checkbox"/>
Clientless Access URL Encoding	<input type="text" value="Clear"/>	<input checked="" type="checkbox"/>
Clientless Access Persistent Co...	<input type="text" value="DENY"/>	<input checked="" type="checkbox"/>
Plug-in Type	<input type="text" value="Java"/>	<input checked="" type="checkbox"/>

**Configure NetScaler Gateway Session Profile**
✕

Name\*

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	<input type="text" value="ON"/>	<input checked="" type="checkbox"/>
Web Interface Address	<input type="text" value="https://storefront.example.com"/>	<input checked="" type="checkbox"/>
Web Interface Portal Mode	<input type="text" value="NORMAL"/>	<input checked="" type="checkbox"/>
Single Sign-on Domain	<input type="text" value="ptd"/>	<input checked="" type="checkbox"/>
Citrix Receiver Home Page	<input type="text"/>	<input type="checkbox"/>
Account Services Address	<input type="text" value="https://storefront.example.com"/>	<input checked="" type="checkbox"/>

### Profil Receiver pour Web

**Configure NetScaler Gateway Session Profile** x

Name\*

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	<input type="text" value="https://storefront.ptd.com/Citrix/StoreWeb"/>	<input checked="" type="checkbox"/> Display Home Page <input checked="" type="checkbox"/>
URL for Web-Based Email	<input type="text"/>	<input type="checkbox"/>
Split Tunnel	<input type="text" value="OFF"/>	<input type="checkbox"/>
Session Time-out (mins)	<input type="text" value="60"/>	<input checked="" type="checkbox"/>
Client Idle Time-out (mins)	<input type="text"/>	<input type="checkbox"/>
Clientless Access	<input type="text" value="Off"/>	<input checked="" type="checkbox"/>
Clientless Access URL Encoding	<input type="text" value="Clear"/>	<input checked="" type="checkbox"/>
Clientless Access Persistent Co...	<input type="text" value="DENY"/>	<input checked="" type="checkbox"/>
Plug-in Type	<input type="text" value="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** x

Name\*

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	<input type="text" value="ON"/>	<input checked="" type="checkbox"/>
Web Interface Address	<input type="text" value="https://storefront.example.com/Citrix/StoreWeb"/>	<input checked="" type="checkbox"/>
Web Interface Portal Mode	<input type="text" value="NORMAL"/>	<input checked="" type="checkbox"/>
Single Sign-on Domain	<input type="text" value="ptd"/>	<input checked="" type="checkbox"/>
Citrix Receiver Home Page	<input type="text"/>	<input type="checkbox"/>
Account Services Address	<input type="text"/>	<input type="checkbox"/>

## Configurer l'URL de base de l'hôte serveur StoreFront, la passerelle et le certificat SSL

Le même nom de domaine complet (FQDN) partagé résolu sur le vServer NetScaler Gateway doit également être résolu directement sur l'équilibrage de la charge StoreFront, si un cluster StoreFront a été créé ou qu'une seule adresse IP StoreFront héberge le magasin.

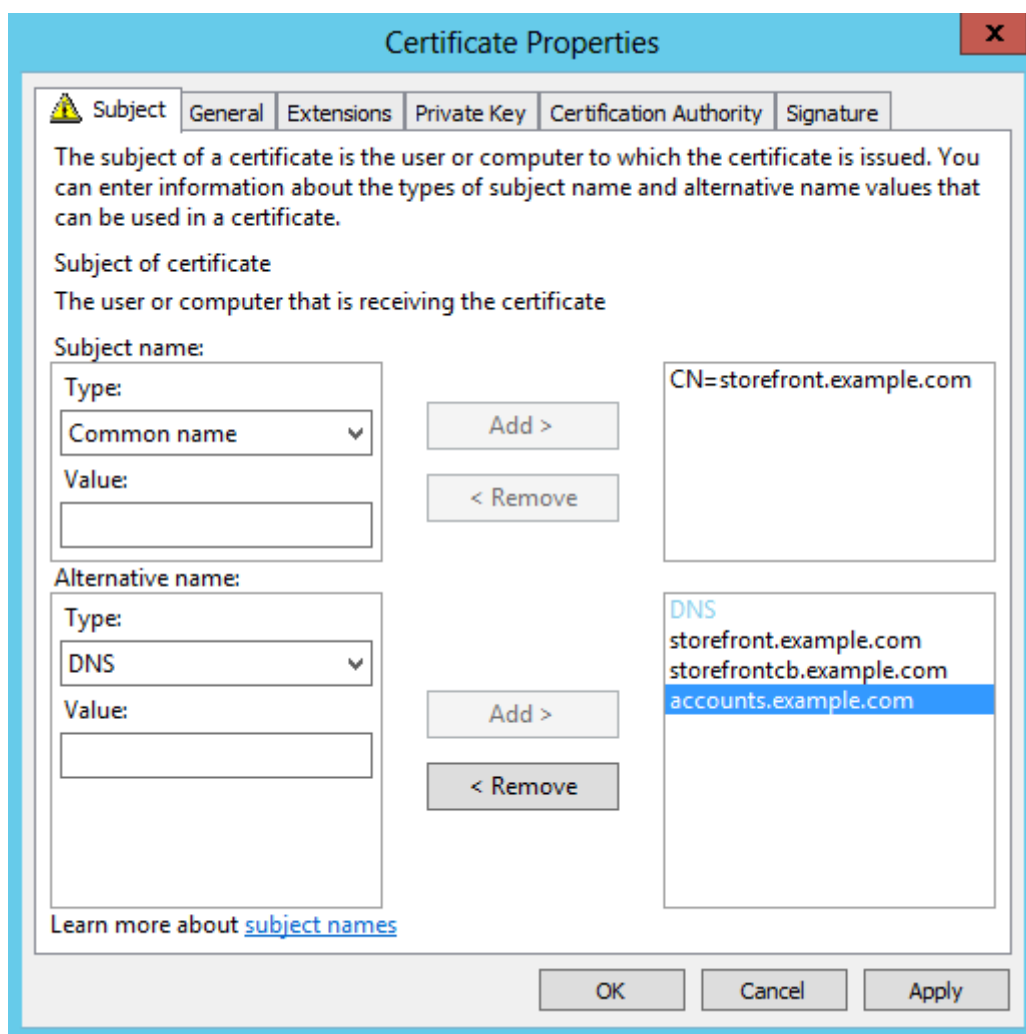
### DNS interne : créez trois enregistrements A DNS

- storefront.exemple.com doit être résolu sur l'équilibrage de charge StoreFront ou sur une adresse IP du serveur StoreFront.
- storefrontcb.exemple.com doit être résolu sur l'adresse IP virtuelle du vServer de la passerelle, par conséquent si un pare-feu est présent entre la DMZ et le réseau local d'entreprise, tenez-en compte.
- accounts.exemple.com : créez un alias DNS pour storefront.exemple.com. Cela permet également la résolution sur l'adresse IP d'équilibrage de charge pour le cluster StoreFront ou une adresse IP du serveur StoreFront.

### Exemple de certificat de serveur StoreFront : storefront.exemple.com

1. Créez un certificat approprié pour le serveur StoreFront ou groupe de serveurs avant l'installation de StoreFront.
2. Ajoutez le nom de domaine complet partagé aux champs Nom commun et DNS. Assurez-vous qu'ils correspondent au nom de domaine complet (FQDN) utilisé dans le certificat SSL lié au vServer NetScaler Gateway que vous avez créé précédemment ou utilisez le même certificat lié au vServer NetScaler Gateway.
3. Ajoutez l'alias de compte (`accounts.exemple.com`) comme un autre SAN au certificat. Notez que l'alias de compte utilisé dans le SAN est celui utilisé dans le profil de session de Netscaler Gateway dans la procédure précédente - **Stratégie et profil de session de passerelle Receiver natifs**.

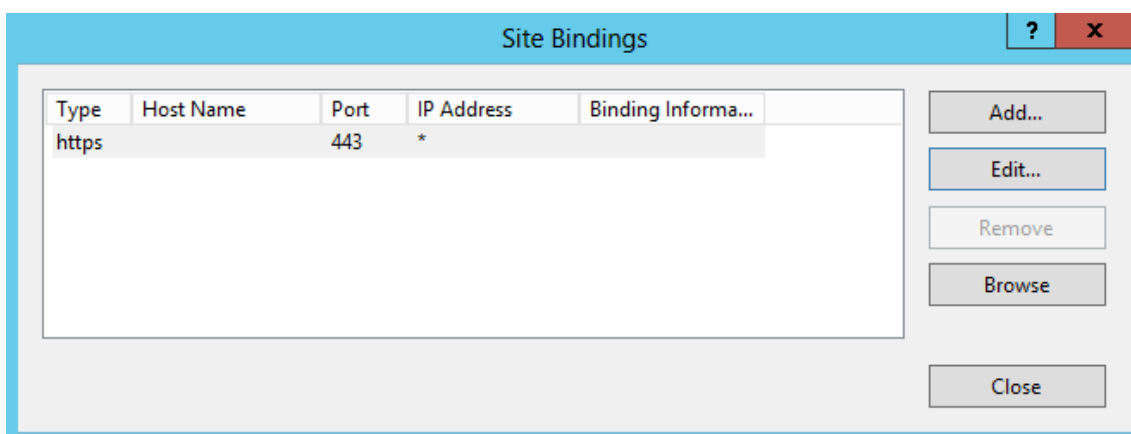




4. Vérifiez que la clé privée est exportable de façon à ce que le certificat puisse être transféré vers un autre serveur ou vers de multiples nœuds de groupe de serveurs StoreFront.

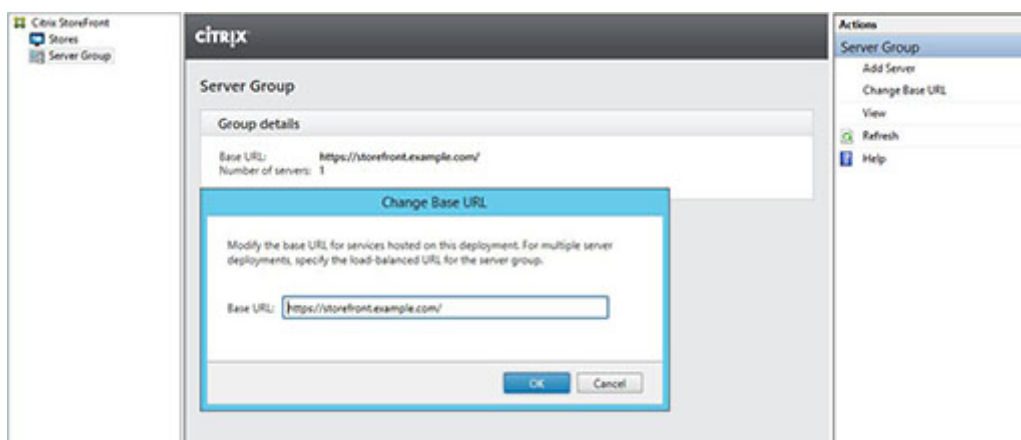


5. Signez le certificat à l'aide d'une autorité de certification tierce telle que Verisign, l'autorité de certification racine de votre entreprise ou une autorité de certification intermédiaire.
6. Exportez le certificat au format PFX y compris la clé privée.
7. Importez le certificat et la clé privée sur le serveur StoreFront. Si vous déployez un cluster StoreFront NLB Windows, importez le certificat sur chaque nœud. Si vous utilisez un autre équilibreur de charge, tel qu'un vServer LB Netscaler, importez le certificat sur ce dernier.
8. Créez une liaison HTTPS dans IIS sur le serveur StoreFront et liez-y le certificat SSL importé.



- Configurez l'adresse URL de l'hôte de base sur le serveur StoreFront pour correspondre au nom de domaine complet (FQDN) partagé déjà choisi.

**Remarque :** StoreFront sélectionne toujours automatiquement le dernier Autre nom de l'objet dans la liste des SAN dans le certificat. Il s'agit simplement d'une suggestion d'adresse URL de base de l'hôte destinée à aider les administrateurs StoreFront. Cette adresse est généralement correcte. Vous pouvez la définir manuellement sur toute adresse [HTTPS://<FQDN>](https://<FQDN>) valide à condition qu'elle existe dans le certificat en tant que SAN. Exemple : <https://storefront.example.com>.



### Modifier l'URL de base du serveur HTTP et la remplacer par HTTPS

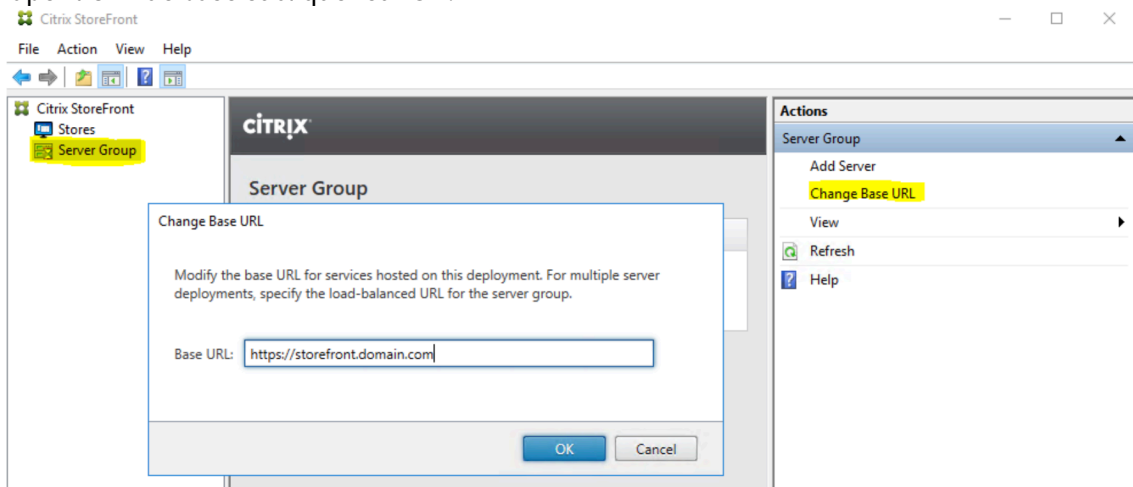
L'option d'URL de base de l'hôte est disponible lors de la configuration du déploiement d'un serveur unique ou d'un groupe de serveurs sur Citrix StoreFront. Cette option s'applique aux clients qui ont installé et configuré Citrix StoreFront sans certificat de serveur. Après avoir installé le certificat, assurez-vous que StoreFront et ses services utilisent une connexion sécurisée.

Remarque :

L'administrateur informatique doit générer et installer un certificat de serveur sur le serveur Citrix StoreFront avant d'exécuter cette procédure. En outre, une liaison IIS doit être créée via HTTPS (443) pour sécuriser toute nouvelle connexion.

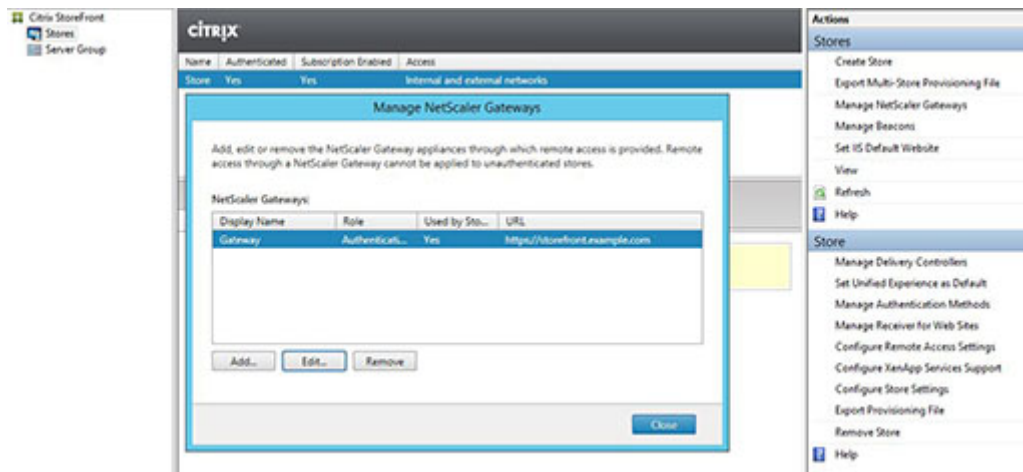
Procédez comme suit pour modifier l'URL de base sur StoreFront 3.x :

1. Dans StoreFront, cliquez sur **Groupe de serveurs** dans le panneau de gauche.
2. Cliquez sur **Changer l'URL de base** dans le panneau de droite.
3. Tapez l'URL de base et cliquez sur **OK**.



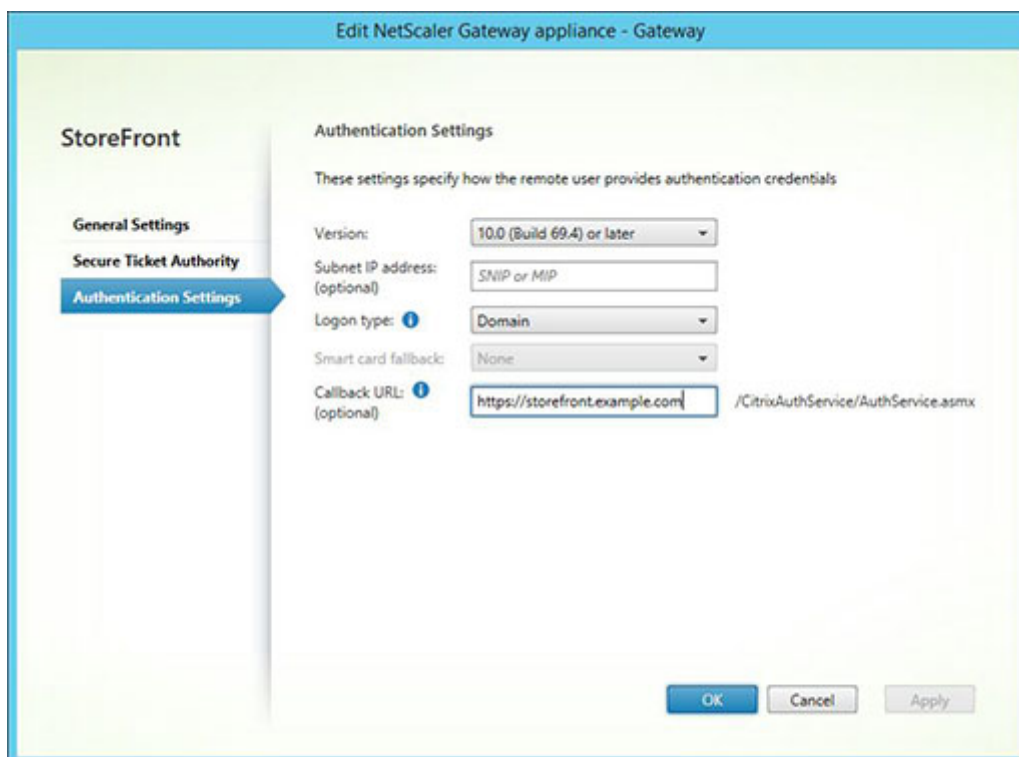
## Configurez la passerelle sur le serveur StoreFront : storefront.example.com

1. Dans le nœud **Magasins**, cliquez sur **Gérer NetScaler Gateway** dans le panneau **Actions**.
2. Sélectionnez la passerelle dans la liste **Passerelle** et cliquez sur **Modifier**.



1. Sur la page **Paramètres généraux**, indiquez le nom de domaine complet partagé dans le champ **URL NetScaler Gateway**.

2. Sélectionnez l'onglet **Paramètres d'authentification** et entrez le nom de domaine complet (FQDN) de rappel dans le champ d'adresse **URL de rappel**.



1. Sélectionnez l'onglet **Secure Ticket Authority** et vérifiez que les serveurs Secure Ticket Authority (STA) correspondent à la liste des Controller déjà configurés dans le nœud **Magasin**.
2. Activez l'accès à distance pour le magasin.
3. Définissez manuellement la balise interne sur les alias de compte (comptes.exemple.com) et elle ne doit pas pouvoir être résolue en dehors de la passerelle. Ce nom de domaine complet (FQDN) doit être différent de la balise externe qui est partagée par l'adresse URL de base de l'hôte StoreFront et le vServer NetScaler Gateway (storefront.exemple.com). N'utilisez PAS le nom de domaine complet (FQDN) partagé car cela crée une situation dans laquelle les balises internes et externes sont identiques.

**Remarque :**

que si vous souhaitez prendre en charge la découverte à l'aide de noms de domaine complets, suivez ces étapes. Si la configuration du fichier de provisioning est insuffisante ou si vous utilisez uniquement Receiver pour Web, vous pouvez ignorer les étapes suivantes.

Ajoutez une entrée `<allowedAudiences>` supplémentaire dans `C:\inetpub\wwwroot\Citrix\Authentication\web.config`. Il y a deux entrées `<allowedAudiences>` dans ce fichier. Seule la première entrée dans le fichier pour Authentication Token Producer nécessite que vous ajoutiez une autre entrée `<allowedAudience>`.

1. Trouvez la chaîne `<allowedAudiences>`. Recherchez la section `<service id>` suivante ci-dessous et ajoutez la ligne affichée en **gras**, enregistrez et fermez le fichier `web.config`.

```
<service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="Authentication Token Producer">
```

```
...
```

```
<allowedAudiences>
```

```
<add name="https-storefront.example.com" audience="https://storefront.example.com/" />
```

```
<add name="https-accounts.example.com" audience="https://accounts.example.com/" />
```

```
</allowedAudiences>
```

2. Dans `C:\inetpub\wwwroot\Citrix\Roaming\web.config`, recherchez la section `<tokenManager>` et ajoutez la ligne affichée en **gras**, enregistrez et fermez le fichier `web.config`.

```
<tokenManager>
```

```
<services>
```

```
<clear />
```

```
...
```

```
</trustedIssuers>
```

```
<allowedAudiences>
```

```
<add name="https-storefront.example.com" audience="https://storefront.example.com/" />
```

```
<add name="https-accounts.example.com" audience="https://accounts.example.com/" />
```

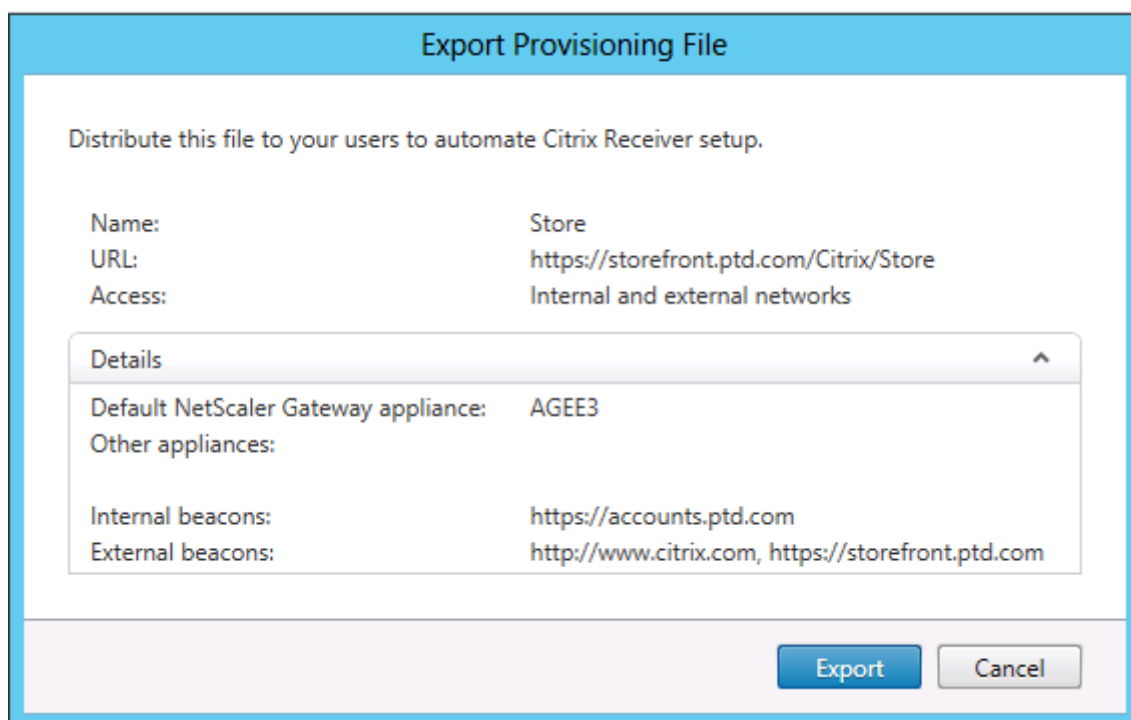
```
</allowedAudiences>
```

```
</service>
```

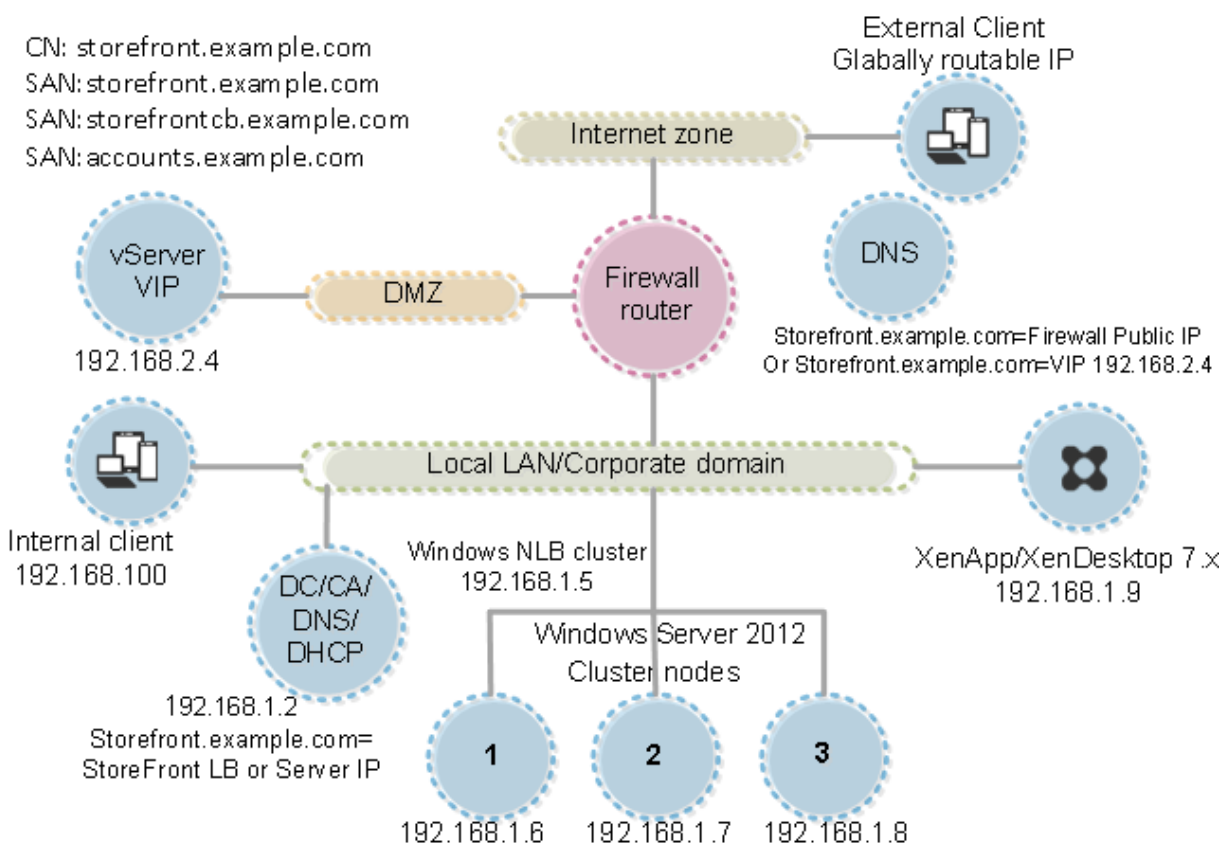
```
</services>
```

```
</tokenManager>
```

Il est également possible d'exporter le fichier de provisioning .CR Receiver natif pour le magasin. Cela élimine le besoin de configurer la première utilisation des Receiver natifs. Distribuez ce fichier à tous les clients Receiver Mac et Windows.



Si un Receiver est installé sur le client, le type de fichier .CR est reconnu et le fait de double-cliquer sur le fichier de provisioning déclenche son importation automatique.





## Configurer le filtrage des ressources

October 4, 2018

Cette rubrique explique comment filtrer les ressources d'énumération en fonction du type et de mots clés. Vous pouvez utiliser ce type de filtrage avec les personnalisations les plus avancées offertes par Store Customization SDK. À l'aide de ce SDK, vous pouvez contrôler les applications et bureaux qui seront affichés auprès des utilisateurs, modifier les conditions d'accès, et régler les paramètres de démarrage. Pour de plus amples informations, veuillez consulter Store Customization SDK.

### 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.

## Configurer le filtrage

Configurez le filtre à l'aide des applets de commande PowerShell définies dans StoresModule. Utilisez le fragment PowerShell suivants pour charger les modules requis :

```
1 $dsInstallProp = Get-ItemProperty '  
2 -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name  
   InstallDir  
3 $dsInstallDir = $dsInstallProp.InstallDir  
4 & $dsInstallDir..\Scripts\ImportModules.ps1
```

## Filtrer par type

Utilisez ce filtre pour l'énumération des ressources par type de ressource. Il s'agit d'un filtre inclusif, c'est-à-dire qu'il supprime toute ressource qui n'est pas du type spécifié dans les résultats de l'énumération des ressources. Utilisez les applets de commande suivants :

**Set-DSResourceFilterType:** configure le filtrage d'énumération basé sur les types de ressources.

**Get-DSResourceFilterType:** obtient la liste des types de ressources que Storefront est autorisé à retourner dans l'énumération.

Remarque : les types de ressources sont appliqués avant les mots-clés.

## Filtrer par mots-clés

Utilisez ceci pour filtrer les ressources en vous basant sur des mots-clés, tels que des ressources dérivées de XenDesktop ou XenApp. Les mots-clés sont générés depuis des annotations dans le champ de description de la ressource correspondante.

Le filtre peut opérer soit en mode inclusif soit en mode exclusif, mais pas les deux. Le filtre inclusif permet d'énumérer les ressources correspondant aux mots-clés configurés et supprime les ressources qui ne correspondent pas de l'énumération. Le filtre exclusif supprime les ressources correspondant aux mots-clés configurés de l'énumération. Utilisez les applets de commande suivants :

**Set-DSResourceFilterKeyword:** configure le filtrage d'énumération basé sur les mots-clés de ressources.

**Get-DSResourceFilterKeyword:** obtient la liste des mots-clés de filtre.

Les mots-clés suivants sont réservés et ne doivent pas être utilisés pour le filtrage :

- Automatique
- Obligatoire

Pour plus d'informations sur les mots-clés, consultez [Optimiser l'expérience utilisateur](#) et [Configurer la mise à disposition d'applications](#).

## Exemples

Cette commande définit le filtrage afin d'exclure les ressources de workflow de l'énumération :

```
1 Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -  
   ExcludeKeywords @"WFS")
```

Cet exemple définit les applications uniquement comme types de ressources autorisées :

```
1 Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -  
   IncludeTypes @"Applications")
```

## Configurer des sites à l'aide des fichiers de configuration

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Vous pouvez utiliser les fichiers de configuration pour configurer des paramètres supplémentaires pour Citrix StoreFront et Citrix Receiver pour Web qui ne peuvent pas être définis à l'aide de la console de gestion Citrix StoreFront.

Les paramètres de [Citrix StoreFront](#) que vous pouvez configurer sont les suivants :

- Activer la signature de fichier ICA
- Désactiver l'association de type de fichier
- Personnaliser la boîte de dialogue d'ouverture de session de Citrix Receiver
- Empêcher Receiver pour Windows de mettre les mots de passe et les noms d'utilisateur en cache

Les paramètres de [Citrix Receiver pour Web](#) que vous pouvez configurer sont les suivants :

- Manière dont les ressources s'affichent auprès des utilisateurs
- Désactiver l'affichage du dossier Mes applications

## Configurer StoreFront à l'aide des fichiers de configuration

February 20, 2019

Cet article décrit les tâches de configuration supplémentaires qui ne peuvent pas être effectuées à l'aide de la console de gestion Citrix StoreFront.

### Activer la signature de fichier ICA

StoreFront permet de signer numériquement les fichiers ICA afin que les versions de Citrix Receiver qui prennent en charge cette fonctionnalité puissent vérifier que le fichier provient d'une source approuvée. Lorsque la signature des fichiers est activée dans StoreFront, le fichier ICA généré quand un utilisateur lance une application est signé à l'aide d'un certificat provenant du magasin de certificats personnels du serveur StoreFront. Les fichiers ICA peuvent être signés en utilisant n'importe quel algorithme de hachage pris en charge par le système d'exploitation exécuté sur le serveur StoreFront. La signature numérique est ignorée par les clients qui ne prennent pas en charge cette fonctionnalité ou qui ne sont pas configurés pour la signature de fichier ICA. Si la procédure de signature échoue, le fichier ICA est généré sans signature numérique puis envoyé à Citrix Receiver, dont la configuration détermine si le fichier non signé sera accepté ou non.

Pour pouvoir être utilisés pour la signature de fichier ICA avec StoreFront, les certificats doivent inclure la clé privée et se situer dans la période de validité autorisée. Si le certificat contient une extension d'utilisation de la clé, celle-ci doit permettre l'utilisation de la clé pour les signatures numériques. Si une extension d'utilisation de la clé prolongée est incluse, elle doit être définie sur la signature de code ou l'authentification de serveur.

Pour la signature de fichier ICA, Citrix vous recommande d'utiliser un certificat de signature de code ou SSL que vous pouvez vous procurer auprès d'une autorité de certification publique ou de l'autorité de certification publique de votre organisation. Si vous ne parvenez pas à obtenir un certificat approprié auprès d'une autorité de certification, vous pouvez utiliser un certificat SSL existant, par exemple un certificat de serveur ou créer un nouveau certificat racine d'autorité de certification et le distribuer sur les périphériques des utilisateurs.

La signature de fichier ICA est désactivée par défaut dans les magasins. Pour activer la signature de fichier ICA, modifiez le fichier de configuration du magasin et exécutez les commandes Windows PowerShell. Pour plus d'informations sur l'activation de la signature de fichier ICA dans Citrix Receiver, reportez-vous à [Signature de fichier ICA pour se protéger contre le lancement d'applications ou de bureaux provenant de serveurs non approuvés](#).

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.

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 les modifications terminées, [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. Assurez-vous que le certificat que vous souhaitez utiliser pour signer les fichiers ICA est disponible dans le magasin de certificats Citrix Delivery Services du serveur StoreFront et non dans le magasin de certificats de l'utilisateur actuel.
2. Utilisez un éditeur de texte pour ouvrir le fichier web.config du magasin, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\nommagasin\, où nommagasin désigne le nom attribué au magasin au moment de sa création.
3. Recherchez la section suivante dans le fichier.

```
1 <certificateManager>
2   <certificates>
3     <clear />
4     <add ... />
5     ...
6   </certificates>
7 </certificateManager>
```

4. Incluez les détails du certificat à utiliser pour la signature.
-

```
1 <certificateManager>
2   <certificates>
3     <clear />
4     <add id="certificateid" thumb="certificatethumbprint" />
5     <add ... />
6     ...
7   </certificates>
8 </certificateManager>
```

où **certificateid** correspond à la valeur qui vous permet d'identifier le certificat dans le fichier de configuration du magasin et **certificatethumbprint** correspond au résumé (ou à l'empreinte numérique) des données du certificat produites par l'algorithme de hachage.

5. Recherchez l'élément suivant dans le fichier.

```
1 <icaFileSigning enabled="False" certificateId="" hashAlgorithm="
   sha1" />
```

6. Modifiez la valeur de l'attribut **enabled** sur **True** pour activer la signature de fichier ICA pour le magasin. Définissez la valeur de l'attribut **certificateid** sur l'ID que vous avez utilisé pour identifier le certificat, c'est-à-dire **certificateid** à l'étape 4.
7. Si vous souhaitez utiliser un algorithme de hachage autre que SHA-1, définissez la valeur de l'attribut **hashAlgorithm** sur **sha256**, **sha384** ou **sha512**, selon les besoins.
8. À l'aide d'un compte avec des autorisations d'administrateur local, démarrez Windows PowerShell et, à l'invite de commandes, tapez les commandes suivantes pour permettre au magasin d'accéder à la clé privée.

```
1 Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
2 $certificate = Get-DSCertificate "certificatethumbprint"
3 Add-DSCertificateKeyReadAccess -certificate $certificates[0] -
   accountName "IIS APPPOOL\Citrix Delivery Services Resources"
```

Où **certificatethumbprint** est le condensé des données de certificat produites par l'algorithme de hachage.

## Désactiver l'association de type de fichier

Par défaut, l'association de type de fichier est activée dans les magasins, afin que le contenu soit redirigé en toute transparence vers les applications auxquelles les utilisateurs se sont abonnés lorsqu'ils ouvrent des fichiers locaux des types appropriés. Pour désactiver l'association de type de fichier, modifiez le fichier de configuration du 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 les modifications terminées,

[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 web.config du magasin, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\nommagasin\, où nommagasin désigne le nom attribué au magasin au moment de sa création.
2. Recherchez l'élément suivant dans le fichier.

```
1 <farmset ... enableFileTypeAssociation="on" ... >
```

3. Réglez la valeur de l'attribut enableFileTypeAssociation sur off pour désactiver l'association de type de fichier pour le magasin.

### Personnaliser la boîte de dialogue d'ouverture de session de Citrix Receiver

Lorsque les utilisateurs Citrix Receiver se connectent à un magasin, aucun texte de titre ne s'affiche par défaut dans la boîte de dialogue de connexion. Vous pouvez afficher le texte par défaut « Please log on » ou composer votre propre message personnalisé. Pour afficher et personnaliser le texte du titre dans la boîte de dialogue de connexion Citrix Receiver, modifiez les fichiers 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 les modifications terminées,

[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 UsernamePassword.tfrm du serveur d'authentification, qui est généralement situé dans le répertoire C:\inetpub\wwwroot\Citrix\Authentication\.
2. Recherchez les lignes suivantes dans le fichier.

```
1 @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
```

3. Supprimez les marques de commentaire pour l'instruction en supprimant le début @\* et la fin \*@.

```
1 @Heading("ExplicitAuth:AuthenticateHeadingText")
```

Les utilisateurs Citrix Receiver voient le texte de titre par défaut s'afficher « Please log on », ou la version localisée appropriée de ce texte (Veuillez ouvrir une session), lorsqu'ils ouvrent une session sur les magasins qui utilisent ce service d'authentification.

4. Pour modifier le texte du titre, utilisez un éditeur de texte pour ouvrir le fichier *ExplicitFormsCommon.xx.resx* du service d'authentification, qui est généralement situé dans le répertoire `C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\`.
5. Recherchez les éléments suivants dans le fichier. Modifiez le texte compris entre l'élément `<value>` pour modifier le texte de titre que les utilisateurs verront sur la boîte de dialogue d'ouverture de session de Citrix Receiver lorsqu'ils accèdent aux magasins qui utilisent ce service d'authentification.

```
1 <data name="AuthenticateHeadingText" xml:space="preserve">
2     <value>My Company Name</value>
3 </data>
```

Pour modifier le texte de titre de la boîte de dialogue d'ouverture de session Citrix Receiver pour les utilisateurs d'autres paramètres régionaux, modifiez les fichiers localisés *ExplicitAuth.languagecode.resx*, où **languagecode** est l'identificateur de paramètres régionaux.

## Empêcher Citrix Receiver pour Windows de mettre les mots de passe et les noms d'utilisateur en cache

Par défaut, Citrix Receiver pour Windows stocke les mots de passe des utilisateurs lorsqu'ils se connectent à des magasins StoreFront. Pour empêcher Citrix Receiver pour Windows, mais pas Citrix Receiver pour Windows Enterprise, de mettre en cache les mots de passe des utilisateurs, modifiez les fichiers 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 les modifications terminées, [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 `inetpub\wwwroot\Citrix\Authentication\App_Data\Templat`
2. Recherchez la ligne suivante dans le fichier.

```
1 @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
```

3. Commentez l'instruction comme indiqué ci-dessous.

```
1 <!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),  
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",  
    initiallyChecked: ControlValue("SaveCredentials")) -->
```

Les utilisateurs de Citrix Receiver pour Windows doivent entrer leur mot de passe chaque fois qu'ils se connectent à des magasins utilisant ce service d'authentification. Ce paramètre ne s'applique pas à Citrix Receiver pour Windows Enterprise.

**Avertissement :**

Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Par défaut, Citrix Receiver pour Windows renseignait automatiquement le dernier nom d'utilisateur entré. Pour empêcher le champ du nom d'utilisateur d'être renseigné, modifiez le registre sur la machine utilisateur :

1. Créez une valeur HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Définissez sa valeur sur « false ».

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

February 20, 2019

Cet article décrit les tâches de configuration supplémentaires pour les sites Citrix Receiver pour Web qui ne peuvent pas être effectuées à l'aide de la console de gestion Citrix StoreFront.

### Configurer la manière dont les ressources s'affichent auprès des utilisateurs

Lorsque des bureaux et des applications sont disponibles depuis un site Citrix Receiver pour Web, les bureaux et applications sont affichés dans des vues distinctes. Les utilisateurs voient tout d'abord la vue de bureau lorsqu'ils ouvrent une session sur le site. Si un seul bureau est disponible pour un utilisateur, que les applications soient également disponibles ou non depuis un site, ce bureau démarre automatiquement lorsque l'utilisateur ouvre une session. Pour modifier ces paramètres, modifiez le fichier de configuration du site.



**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 les modifications terminées, [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 `web.config` du site Citrix Receiver pour Web, qui se trouve en général dans le répertoire `C:\inetpub\wwwroot\Citrix\nommagasinWeb\`, où `nommagasin` désigne le nom attribué au magasin au moment de sa création.
2. Recherchez l'élément suivant dans le fichier.

```
1 <uiViews showDesktopsView="true" showAppsView="true" defaultView="
  desktops" />
```

3. Réglez la valeur des attributs **showDesktopsView** et **showAppsView** sur **false** pour empêcher les bureaux et les applications, respectivement, d'être affichés pour les utilisateurs, même s'ils sont disponibles à partir du site. Lorsque les vues des bureaux et des applications sont activées, définissez la valeur de l'attribut `defaultView` sur `apps` pour afficher tout d'abord la vue d'application lorsque les utilisateurs ouvrent une session sur le site.
4. Recherchez l'élément suivant dans le fichier.

```
1 <userInterface ... autoLaunchDesktop="true">
```

5. Changez la valeur de l'attribut **autoLaunchDesktop** sur **false** pour empêcher les sites Citrix Receiver pour Web de démarrer automatiquement un bureau lorsqu'un utilisateur ouvre une session sur le site et qu'un seul bureau est disponible pour cet utilisateur.

Lorsque l'attribut **autoLaunchDesktop** est défini sur **true** et qu'un utilisateur pour lequel un seul bureau est disponible ouvre une session, les applications de cet utilisateur ne sont pas reconnectées, quelle que soit la configuration du contrôle de l'espace de travail.

**Remarque :**

Pour permettre aux sites Citrix Receiver pour Web de démarrer automatiquement leurs bureaux, les utilisateurs qui accèdent au site via Internet Explorer doivent ajouter le site à la zone Intranet local ou Sites de confiance.

## Désactiver l'affichage du dossier Mes applications

Par défaut, Citrix Receiver pour Web affiche le dossier Mes applications pour les magasins non authentifiés (accès des utilisateurs non authentifiés) et obligatoires (toutes les applications publiées sont disponibles dans l'écran d'accueil, sans que les utilisateurs aient besoin de s'y abonner). Cette vue affiche les applications dans une hiérarchie de dossiers et inclut un chemin de navigation.

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 les modifications terminées,

[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 web.config du site Citrix Receiver pour Web, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\nommagasinWeb\, où nommagasin désigne le nom attribué au magasin au moment de sa création.
2. Recherchez l'élément suivant dans le fichier.

```
1 <userInterface enableAppsFolderView="true">
```

3. Modifiez la valeur de l'attribut **enableAppsFolderView** sur **false** afin de désactiver l'affichage du dossier Mes applications dans Citrix Receiver pour Web.

## Sécuriser votre déploiement StoreFront

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Cet article dresse la liste des domaines susceptibles d'avoir un impact sur la sécurité du système lors du déploiement et de la configuration de StoreFront.

## Configurer Microsoft Internet Information Services (IIS)

Vous pouvez configurer Director avec une configuration IIS limitée. Veuillez noter qu'il ne s'agit pas de la configuration IIS par défaut.

## Extensions de nom de fichier

Vous pouvez interdire les extensions de nom de fichier non répertoriées.

StoreFront requiert les extensions de nom de fichier suivantes dans le Filtrage des demandes :

- . (extension vierge)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .gif
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

Si le téléchargement ou la mise à niveau de Citrix Receiver est activé(e) pour Citrix Receiver pour Web, StoreFront requiert également ces extensions de nom de fichier :

- .dmg
- .exe

Si Citrix Receiver pour HTML5 est activé, StoreFront requiert également ces extensions de nom de fichier :

- .eot
- .ttf
- .woff

## Types MIME

Vous pouvez supprimer les types MIME correspondant aux types de fichiers suivants :

- .exe
- .dll
- .com

- .bat
- .csh

### Filtrage des demandes

StoreFront requiert les verbes HTTP suivants dans le Filtrage des demandes : Vous pouvez interdire les verbes non répertoriés.

- GET
- POST
- HEAD

### Autres paramètres de Microsoft IIS

StoreFront ne nécessite pas :

- Filtres ISAPI
- Extensions ISAPI
- Programmes CGI
- Programmes FastCGI

#### Important :

- Ne configurez pas les règles d'autorisation IIS. StoreFront prend en charge l'authentification directement et n'utilise pas ou ne prend pas en charge l'authentification IIS.
- Ne sélectionnez pas **Certificats clients : Exiger** dans les paramètres SSL du site StoreFront. L'installation de StoreFront configure les pages appropriées du site StoreFront avec ce paramètre.
- StoreFront requiert l'activation des cookies. Le paramètre Utiliser les cookies doit être sélectionné. N'activez pas le paramètre Sans cookie/Utiliser URI.
- StoreFront requiert l'approbation Confiance totale. Ne définissez pas le niveau de confiance .NET global sur Élevé ou Moyen.
- StoreFront ne prend pas en charge un pool d'applications distinct pour chaque site. Ne modifiez pas ces paramètres de site. Toutefois, vous pouvez définir le délai d'inactivité du pool d'applications et la quantité de mémoire virtuelle qu'un pool d'applications utilise.

### Configurer les droits des utilisateurs

Remarque :

Microsoft IIS est activé dans le cadre de l'installation de StoreFront. Microsoft IIS accorde le droit de connexion **Ouvrir une session en tant que tâche** et le privilège **Emprunter l'identité d'un**

**client après l'authentification** au groupe IIS\_IUSRS intégré. Il s'agit d'un comportement normal d'installation de Microsoft IIS. Ne modifiez pas ces droits d'utilisateur. Reportez-vous à la documentation de Microsoft pour plus de détails.

Lorsque vous installez StoreFront, le droit d'ouverture de session **Ouvrir une session en tant que service** et les privilèges **Ajuster les quotas de mémoire pour un processus, Générer des audits de sécurité et Remplacer un jeton de niveau processus** sont accordés à ses pools d'applications. Il s'agit d'un comportement d'installation normal lorsque des pools d'applications sont créés. Les pools d'applications sont Citrix Configuration Api, Citrix Delivery Services Resources, Citrix Delivery Services Authentication et Citrix Receiver pour Web.

Vous n'avez pas besoin de changer ces droits d'utilisateur. Ces privilèges ne sont pas utilisés par StoreFront et sont automatiquement désactivés.

L'installation de StoreFront crée les services Windows suivants :

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)
- Citrix Peer Resolution (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Credential Wallet (NT SERVICE\CitrixCredentialWallet)
- Citrix Subscriptions Store (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Default Domain Services (NT SERVICE\CitrixDefaultDomainService)

Si vous configurez la délégation Kerberos StoreFront contrainte pour XenApp 6.5, le service Transition du protocole Citrix StoreFront est créé (NT SERVICE\SYSTEM). Ce service requiert un privilège qui n'est pas normalement accordé aux services Windows.

## Configurer les paramètres du service

Les services Windows StoreFront répertoriés ci-dessus dans la section « Configurer les droits des utilisateurs » sont configurés pour ouvrir une session avec l'identité NETWORK SERVICE. Le service de transition du protocole Citrix StoreFront ouvre une session en tant que SYSTEM. Ne modifiez pas cette configuration.

## Configurer l'appartenance aux groupes

Lorsque vous configurez un groupe de serveurs StoreFront, les services suivants sont ajoutés au groupe de sécurité Administrateurs :

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService). Ce service n'est visible que sur les serveurs qui font partie d'un groupe et ne s'exécute que lorsque la jointure est en cours.

Ces appartenances de groupe sont requises pour que StoreFront fonctionne correctement, pour :

- Créer, exporter, importer et supprimer des certificats et définir les autorisations d'accès
- Lire et écrire dans le registre Windows
- Ajouter et supprimer des assemblies Microsoft .NET Framework dans Global Assembly Cache (GAC)
- Accéder au dossier **Program Files\Citrix\<StoreFrontLocation>**
- Ajouter, modifier et supprimer des identités de pool d'applications IIS et des applications Web IIS
- Ajouter, modifier et supprimer des groupes de sécurité locaux et des règles de pare-feu
- Ajouter et supprimer des services Windows et des composants enfichables PowerShell
- Enregistrer des points de terminaison Microsoft Windows Communication Framework (WCF)

Dans les mises à jour de StoreFront, cette liste d'opérations peut être modifiée sans préavis.

L'installation de StoreFront crée également les groupes de sécurité locaux suivants :

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSUsers
- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront conserve l'appartenance de ces groupes de sécurité. Ils sont utilisés pour le contrôle d'accès dans StoreFront et ne sont pas appliqués aux ressources Windows, telles que les fichiers et les dossiers. Ne modifiez pas ces appartenances de groupe.

## Certificats dans StoreFront

### Certificats de serveur

Les certificats de serveur sont utilisés pour l'identification des machines et la sécurité du transport TLS dans StoreFront. Si vous choisissez d'activer la signature de fichier ICA, StoreFront peut également utiliser des certificats pour signer numériquement les fichiers ICA.

Pour activer la découverte de compte basée sur une adresse e-mail pour les utilisateurs qui installent Citrix Receiver sur un appareil pour la première fois, vous devez installer un certificat de serveur valide sur le serveur StoreFront. 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 Microsoft Active Directory

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 de plus amples informations, consultez la section [Configurer la découverte de compte basée sur une adresse e-mail](#).

Si vos utilisateurs configurent leurs comptes en entrant des adresses URL de magasin directement dans Citrix Receiver et n'utilisent pas la découverte de compte par e-mail, le certificat du serveur StoreFront doit uniquement être valide pour ce serveur et posséder une chaîne valide vers le certificat racine.

### **Certificats de gestion des jetons**

Les services d'authentification et les magasins requièrent chacun des certificats pour la gestion des jetons. StoreFront génère un certificat auto-signé lors de la création d'un service d'authentification ou d'un magasin. Les certificats auto-signés générés par StoreFront ne doivent pas être utilisés dans un quelconque autre but que ce soit.

### **Certificats Citrix Delivery Services**

StoreFront conserve un certain nombre de certificats dans un magasin de certificats Windows personnalisé (Citrix Delivery Services). Les services Citrix Configuration Replication Service, Citrix Credential Wallet Service et Citrix Subscriptions Store Service utilisent ces certificats. Chaque serveur StoreFront dans un cluster dispose d'une copie de ces certificats. Ces services ne dépendent pas de TLS pour sécuriser les communications et ces certificats ne sont pas utilisés comme certificats de serveur TLS. Ces certificats sont créés lorsqu'un magasin StoreFront est créé ou que StoreFront est installé. Ne modifiez pas le contenu de ce magasin de certificats Windows.

### **Certificats de signature de code**

StoreFront comprend un certain nombre de scripts PowerShell (.ps1) dans le dossier `<Répertoire d'installation>\Scripts`. L'installation de StoreFront par défaut ne peut pas utiliser ces scripts. Ils simplifient les étapes de configuration des tâches spécifiques ou non fréquentes. Ces scripts sont signés, ce qui permet à StoreFront de prendre en charge la stratégie d'exécution PowerShell. Nous recommandons la stratégie **AllSigned**. (La stratégie **Restreint** n'est pas prise en charge car elle empêche l'exécution des scripts PowerShell.) StoreFront ne modifie pas la stratégie d'exécution de PowerShell.

Bien que StoreFront n'installe pas de certificat de signature de code dans le magasin Éditeurs approuvés, Windows peut automatiquement y ajouter le certificat de signature de code. Cela se produit lorsque le script PowerShell est exécuté avec l'option **Toujours exécuter**. (Si vous sélectionnez l'option **Ne jamais exécuter**, le certificat est ajouté au magasin Certificats non autorisés, et les scripts PowerShell StoreFront ne seront pas exécutés.) Une fois que le certificat de code de signature a été ajouté au magasin Éditeurs approuvés, sa date d'expiration n'est plus vérifiée par Windows. Vous pouvez supprimer ce certificat du magasin Éditeurs approuvés après que les tâches StoreFront ont été effectuées.

## Communications StoreFront

Dans un environnement de production, Citrix vous recommande d'utiliser Internet Protocol Security (IPsec) ou le protocole HTTPS pour sécuriser le transfert des données entre StoreFront et vos serveurs. IPsec est un ensemble d'extensions standard du protocole Internet qui garantit des communications authentifiées et cryptées avec intégrité des données et protection contre la relecture. IPsec étant un ensemble de protocoles de couches réseau, les protocoles d'un niveau plus élevé peuvent l'utiliser sans modification. HTTPS utilise les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) pour fournir un chiffrement fort des données.

Le Relais SSL peut être utilisé pour sécuriser le trafic de données entre StoreFront et les serveurs XenApp. Le relais SSL est un composant par défaut de XenApp qui assure l'authentification hôte et le cryptage de données.

Citrix recommande de désactiver la prise en charge de TLS 1.0 et 1.1 dans le serveur Web hébergeant StoreFront. Vous devriez appliquer cette désactivation via des objets de stratégie de groupe, qui créent les paramètres de registre nécessaires sur le serveur StoreFront pour désactiver les protocoles plus anciens comme TLS 1.0 et TLS 1.1. Consultez également la rubrique Microsoft [Paramètres TLS/SSL](#).

Citrix vous recommande de sécuriser les communications entre StoreFront et les machines des utilisateurs à l'aide de NetScaler Gateway et du protocole HTTPS. Pour utiliser le protocole HTTPS, StoreFront requiert que l'instance Microsoft Internet Information Services (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. Citrix vous recommande de ne pas autoriser les connexions utilisateur non sécurisées à StoreFront dans un environnement de production.

## Séparation de la sécurité de StoreFront

Si vous déployez des applications Web dans le même domaine Web (nom de domaine et de port) en tant que StoreFront, tout risque ayant trait à la sécurité dans ces applications Web peut poten-



tiellement réduire la sécurité de votre déploiement StoreFront. Lorsqu'un degré plus important de séparation de la sécurité est nécessaire, Citrix recommande de déployer StoreFront dans un domaine Web distinct.

### **Signature de fichier ICA**

StoreFront permet de signer numériquement les fichiers ICA à l'aide d'un certificat spécifié sur le serveur, afin que les versions de Citrix Receiver qui prennent en charge cette fonctionnalité puissent vérifier que le fichier provient d'une source approuvée. Les fichiers ICA peuvent être signés en utilisant n'importe quel algorithme de hachage pris en charge par le système d'exploitation s'exécutant sur le serveur StoreFront, et notamment SHA-1 et SHA-256. Pour de plus amples informations, consultez la section [Activer la signature de fichier ICA](#).

### **Mot de passe modifié par l'utilisateur**

Vous pouvez autoriser les utilisateurs de sites Receiver pour Web qui ouvrent une session avec des informations d'identification de domaine Active Directory à modifier leurs mots de passe, à tout moment ou uniquement lorsqu'ils ont expiré. Toutefois, cela 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. Lorsque vous créez le service d'authentification, la configuration par défaut empêche les utilisateurs de sites Receiver pour Web de modifier leurs mots de passe, même s'ils ont expiré. Pour de plus amples informations, consultez la section [Optimiser l'expérience de l'utilisateur](#).

### **Personnalisations**

Pour renforcer la sécurité, n'écrivez pas de personnalisations destinées à charger du contenu ou des scripts depuis des serveurs n'étant pas sous votre contrôle. Copiez le contenu ou le script dans le dossier personnalisé du site Citrix Receiver pour Web sur lequel vous effectuez les personnalisations. Si StoreFront est configuré pour des connexions HTTPS, assurez-vous que les liens vers le contenu ou les scripts personnalisés utilisent également le protocole HTTPS.

## **Exporter et importer la configuration StoreFront**

February 26, 2019

**Remarque :**

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Vous pouvez exporter la configuration entière d'un déploiement StoreFront. Cela inclut aussi bien les déploiements ne contenant qu'un seul serveur que les configurations de groupe de serveurs. Si un déploiement existant est déjà présent sur le serveur d'importation, la configuration actuelle est supprimée et remplacée par la configuration contenue dans l'archive de sauvegarde. Si l'installation est effectuée sur un serveur vierge, un nouveau déploiement est créé à l'aide de la configuration importée stockée dans le fichier de sauvegarde. S'il est crypté, le fichier de sauvegarde de la configuration exportée est disponible au format .zip, ou au format .ctxzip si vous avez choisi de crypter le fichier de sauvegarde lors de sa création.

**Éléments à prendre en considération lors de l'exportation et de l'importation d'une configuration StoreFront**

- Voulez-vous utiliser l'URL de base de l'hôte contenue dans l'archive de sauvegarde ou spécifier une nouvelle URL de base de l'hôte à utiliser sur le serveur d'importation ?
- Utilisez-vous actuellement des exemples de SDK d'authentification publiés par Citrix, tels que l'authentification Magic Word ou des personnalisations d'authentification tierces ? Si c'est le cas, vous devez installer ces packages sur TOUS les serveurs d'importation AVANT d'importer une configuration contenant des méthodes d'authentification supplémentaires. L'importation de la configuration échoue si les packages du SDK d'authentification requis ne sont installés sur aucun des serveurs d'importation. Si vous importez une configuration dans un groupe de serveurs, installez les packages d'authentification sur tous les membres du groupe.
- Vous pouvez crypter ou décrypter vos fichiers de sauvegarde de configuration. Les applets de commande PowerShell d'exploration et d'importation prennent en charge les deux cas d'utilisation.
- Vous pouvez décrypter les fichiers de sauvegarde cryptés (.ctxzip) ultérieurement, mais StoreFront ne peut pas recrypter les fichiers de sauvegarde non cryptés (.zip). Si un fichier de sauvegarde crypté est requis, exportez de nouveau à l'aide d'un objet d'information d'identification PowerShell contenant un mot de passe de votre choix.
- Le SiteID du site Web IIS où StoreFront est actuellement installé (serveur d'exportation) doit correspondre au SiteID du site cible IIS (serveur d'importation) sur lequel vous voulez restaurer la sauvegarde de la configuration de StoreFront.

## Objets d'information d'identification PowerShell utilisés pour le cryptage et le décryptage des fichiers de sauvegarde de StoreFront

Un objet d'information d'identification PowerShell comprend un nom d'utilisateur et un mot de passe de compte Windows. Les objets d'information d'identification PowerShell garantissent la sécurité de votre mot de passe en mémoire.

### Remarque :

Pour configurer une archive de sauvegarde de la configuration, seul le mot de passe est requis pour effectuer des cryptages et décryptages. Le nom d'utilisateur stocké dans l'objet d'information d'identification n'est pas utilisé. Vous devez créer un objet d'information d'identification contenant le même mot de passe dans les sessions PowerShell que celui utilisé sur les **serveurs d'exportation et d'importation**. Vous pouvez spécifier un utilisateur quelconque dans l'objet d'information d'identification.

PowerShell nécessite que vous spécifiez un utilisateur lors de la création d'un nouvel objet d'information d'identification. Pour des raisons pratiques, cet exemple de code retourne uniquement l'utilisateur Windows connecté.

```
1 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
2 $Password = "Pa55w0rd"
3 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
4 $CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
```

## Applets de commande PowerShell

### Export-STFConfiguration

Paramètre	Description
-TargetFolder (chaîne)	Chemin d'accès d'exportation à l'archive de configuration. Exemple : "\$env:userprofile\desktop\"

Paramètre	Description
-Credential (Objet PSCredential)	Spécifiez un objet d'information d'identification pour créer une archive de sauvegarde cryptée .ctxzip durant l'exportation. L'objet d'information d'identification PowerShell doit contenir le mot de passe à utiliser pour le cryptage et le décryptage. N'utilisez pas <b>-Credential</b> conjointement avec le paramètre <b>-NoEncryption</b> . Exemple : \$CredObject
-NoEncryption (Commutateur)	Indique que l'archive de sauvegarde doit être un fichier .zip non crypté. N'utilisez pas <b>-NoEncryption</b> conjointement avec le paramètre <b>-Credential</b> .
-ZipFileName (chaîne)	Nom de l'archive de sauvegarde de la configuration de StoreFront. N'ajoutez pas d'extension de fichier, telle que .zip ou .ctxzip. L'extension de fichier est ajoutée automatiquement suivant que le paramètre <b>-Credential</b> ou <b>-NoEncryption</b> est spécifié durant l'exportation. Exemple : "backup"
-Force (Booléen)	Ce paramètre écrase automatiquement les archives de sauvegarde qui portent le même nom de fichier que les fichiers de sauvegarde existants déjà présents dans l'emplacement d'exportation spécifié.

**Important :**

Le paramètre **-SiteID** dans StoreFront 3.5 est obsolète dans la version 3.6. Il n'est plus nécessaire de spécifier le **SiteID** lors d'une importation, car le SiteID contenu dans l'archive de sauvegarde est toujours utilisé. Assurez-vous que le SiteID correspond au site Web de StoreFront déjà configuré dans IIS sur le serveur d'importation. Les importations de configuration de **SiteID 1** vers **SiteID 2** (et vice versa) ne sont pas prises en charge.

**Import-STFConfiguration**

Paramètre	Description
-ConfigurationZip (chaîne)	Chemin d'accès complet de l'archive de sauvegarde que vous voulez importer. Il doit également inclure l'extension de fichier. Utilisez l'extension .zip pour les archives de sauvegarde non cryptées et .ctxzip pour celles cryptées. Exemple : <code>\$env:userprofile\desktop\backup.ctxzip</code>
-Credential (Objet PSCredential)	Spécifiez un objet d'information d'identification pour décrypter un fichier de sauvegarde crypté durant l'importation. Exemple : <code>\$CredObject</code>
-HostBaseURL (chaîne)	Si ce paramètre est inclus, l'URL de base de l'hôte que vous spécifiez est utilisée à la place de l'URL de base de l'hôte du serveur d'exportation. Exemple : <code>https://&lt;importingserver&gt;.example.com</code>

### Unprotect-STFConfigurationBackup

Paramètre	Description
-TargetFolder (chaîne)	Chemin d'accès d'exportation à l'archive de configuration. Exemple : <code>\$env:userprofile\desktop\</code>
-Credential (Objet PSCredential)	Utilisez ce paramètre pour créer une copie non cryptée de l'archive de sauvegarde cryptée. Spécifiez l'objet d'information d'identification PowerShell contenant le mot de passe à utiliser pour le décryptage. Exemple : <code>\$CredObject</code>
-EncryptedConfigurationZip (chaîne)	Chemin d'accès complet de l'archive de sauvegarde cryptée que vous voulez décrypter. Vous devez spécifier l'extension de fichier .ctxzip. Exemple : <code>\$env:userprofile\desktop\backup.ctxzip</code>

Paramètre	Description
-OutputFolder (chaîne)	Chemin d'accès pour créer une copie non cryptée (.zip) de l'archive de sauvegarde cryptée (.ctxzip). La copie cryptée d'origine de la sauvegarde est conservée de façon à pouvoir être réutilisée. Ne spécifiez pas de nom de fichier ni d'extension de fichier pour la copie non cryptée. Exemple : <code>\$env:userprofile\desktop\</code>
-Force (Booléen)	Ce paramètre écrase automatiquement les archives de sauvegarde qui portent le même nom de fichier que les fichiers de sauvegarde existants déjà présents dans l'emplacement d'exportation spécifié.

## Exemples d'exportation et d'importation de configuration

### Importer le SDK StoreFront dans la session PowerShell en cours

Ouvrez la console PowerShell (ISE) sur le serveur StoreFront principal et exécutez :

```

1 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
   PowerShellSDK\Modules\Citrix.StoreFront'
2 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
3 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
   Authentication.psd1" -verbose
4 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
   verbose
5 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
   verbose
6 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
   psd1" -verbose
7 Import-Module "$SDKModules.SubscriptionsStore\Citrix.StoreFront.
   SubscriptionsStore.psd1" -verbose

```

### Scénarios impliquant un seul serveur

#### Créer une sauvegarde non cryptée d'une configuration existante sur un Serveur A et la restaurer sur le même déploiement

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
  zipFileName "backup" -NoEncryption
2 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
  backup.zip"
```

### Créer une sauvegarde cryptée d'une configuration existante sur un Serveur A et la restaurer sur le même déploiement

```
1 # Créez un objet d'information d'identification PowerShell
2 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
3 $Password = "Pa55w0rd"
4 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
5 $CredObject = New-Object System.Management.Automation.PSCredential(
  $User,$Password)
6 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
  zipFileName "backup" -Credential $CredObject
7 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
  backup.ctxzip" -Credential $CredObject
```

### Ôter la protection d'une archive de sauvegarde cryptée existante

```
1 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
2 $Password = "Pa55w0rd"
3 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
4 $CredObject = New-Object System.Management.Automation.PSCredential(
  $User,$Password)
5 Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
  userprofile\desktop\backup.ctxzip" -credential $CredObject -
  outputFolder "c:\StoreFrontBackups" -Force
```

### Sauvegarder une configuration existante sur le serveur A et la restaurer sur une *nouvelle installation par défaut* sur le serveur B

Le Serveur B est un nouveau déploiement conçu pour coexister avec le Serveur A. Spécifiez le paramètre **-HostBaseURL**. Le Serveur B est également une nouvelle installation de StoreFront.

1. Créez un objet d'information d'identification PowerShell et exportez une copie cryptée de la configuration du Serveur A.
2. Créez un objet d'information d'identification PowerShell le Serveur B à l'aide du même mot de passe que celui utilisé pour crypter le fichier de sauvegarde.

3. Décryptez et importez la configuration du Serveur A sur le Serveur B à l'aide du paramètre -**HostBaseURL**.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
backup.ctxzip"-Credential $CredObject -HostBaseURL "https://serverB.
example.com"
```

### **Sauvegarder une configuration existante sur le Serveur A et l'utiliser pour remplacer un déploiement existant sur le Serveur B**

Le Serveur B est un déploiement existant doté d'une configuration obsolète. Utilisez la configuration du Serveur A pour mettre à jour le Serveur B. Le serveur B est conçu pour coexister avec le Serveur A. Spécifiez le paramètre -**HostBaseURL**.

1. Créez un objet d'information d'identification PowerShell et exportez une copie cryptée de la configuration du Serveur A.
2. Créez un objet d'information d'identification PowerShell le Serveur B à l'aide du même mot de passe que celui utilisé pour crypter le fichier de sauvegarde.
3. Décryptez et importez la configuration du Serveur A sur le Serveur B à l'aide du paramètre -**HostBaseURL**.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
backup.ctxzip"-Credential $CredObject -HostBaseURL "https://serverB.
example.com"
```

### **Créer un clone d'un déploiement existant avec la même URL de base d'hôte, par exemple lors de la mise à niveau vers un nouveau système d'exploitation de serveur et de la mise hors service d'un déploiement StoreFront obsolète**

Le Serveur B 2012R2 est un nouveau déploiement conçu pour remplacer le Serveur A 2008R2 obsolète. Utilisez le paramètre HostBaseURL de l'archive de sauvegarde. N'utilisez pas le paramètre -**HostBaseURL** lors de l'importation. Le Serveur B est également une nouvelle installation de StoreFront.

1. Créez un objet d'information d'identification PowerShell et exportez une copie cryptée de la configuration du Serveur A 2008R2.
2. Créez un objet d'information d'identification PowerShell sur le Serveur B 2012R2 à l'aide du même mot de passe que celui utilisé pour crypter le fichier de sauvegarde.
3. Décryptez et importez la configuration du Serveur A 2008R2 sur le Serveur B 2012R2 sans utiliser le paramètre -**HostBaseURL**.



```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
backup.ctxzip"-Credential $CredObject
```

### StoreFront est déjà déployé sur un site Web personnalisé dans IIS. Restaurer la configuration sur un autre déploiement de site Web personnalisé

StoreFront est déployé sur un site Web personnalisé sur le Serveur A plutôt que sur le site Web par défaut habituel dans IIS. Le paramètre SiteID IIS pour le second site Web créé dans IIS est 2. Le chemin d'accès physique au site Web de StoreFront peut se trouver sur un lecteur autre que le lecteur système tel que d:\ ou sur le lecteur système par défaut c:\ mais doit utiliser un paramètre SiteID IIS supérieur à 1.

Un nouveau site Web appelé StoreFront a été configuré dans IIS, qui utilise **SiteID = 2**. StoreFront est déjà déployé sur le site Web personnalisé dans IIS et son chemin d'accès physique se trouve sur le lecteur d : \inetpub\wwwroot.

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

1. Créez un objet d'information d'identification PowerShell et exportez une copie cryptée de la configuration du Serveur A.
2. Sur le serveur B, configurez IIS avec un nouveau site Web appelé **StoreFront**, qui utilise également **SiteID 2**.
3. Créez un objet d'information d'identification PowerShell le Serveur B à l'aide du même mot de passe que celui utilisé pour crypter le fichier de sauvegarde.

4. Décryptez et importez la configuration du Serveur A sur le Serveur B à l'aide du paramètre - **HostBaseURL**. Le SiteID contenu dans la copie de sauvegarde est utilisé et doit correspondre au site Web cible sur lequel vous voulez importer la configuration de StoreFront.

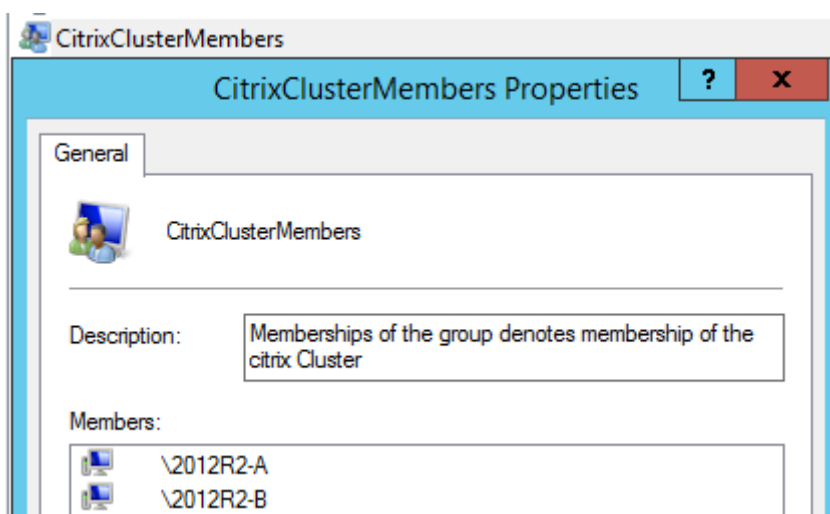
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\  
backup.ctxzip"-Credential $CredObject -HostBaseURL "https://serverB.  
example.com"
```

## Scénarios de groupe de serveurs

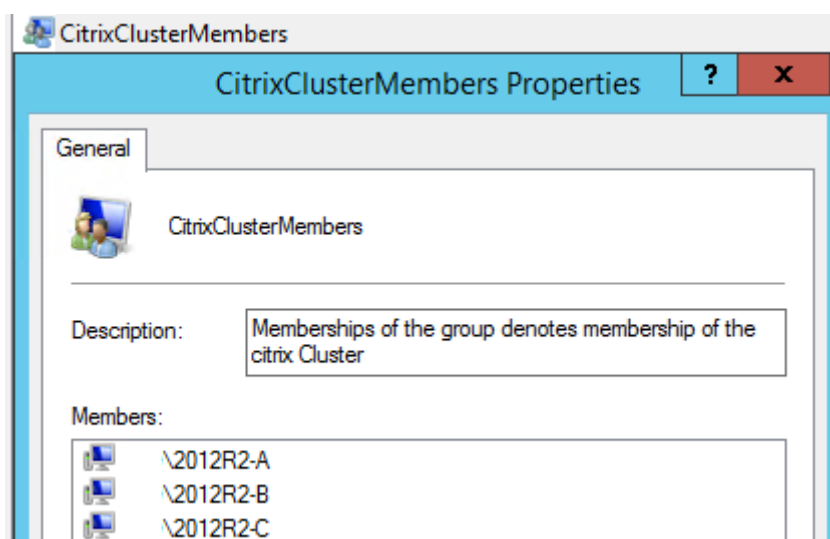
### Scénario 1 : sauvegarder une configuration de groupe de serveurs existante et la restaurer plus tard sur le même déploiement de groupe de serveurs

Une sauvegarde de configuration précédente a été effectuée lorsque seulement deux serveurs StoreFront, 2012R2-A et 2012R2-B, étaient membres du groupe de serveurs. L'archive de sauvegarde contient un enregistrement de **CitrixClusterMembership** correspondant au moment où la sauvegarde a été effectuée. Ce dernier contient uniquement les deux serveurs d'origine 2012R2-A et 2012R2-B. Depuis que la sauvegarde d'origine a été effectuée, le déploiement du groupe de serveurs a pris de l'ampleur afin de s'adapter à la demande croissante, c'est la raison pour laquelle le nœud 2012R2-C a été ajouté au groupe de serveurs. La configuration StoreFront sous-jacente du groupe de serveurs contenue dans la sauvegarde n'a pas été modifiée. Le CitrixClusterMembership actuel de trois serveurs doit être conservé même si une ancienne sauvegarde contenant uniquement les deux nœuds du groupe de serveurs d'origine est importée. Durant l'importation, l'appartenance au cluster actuel est conservée puis réécrite une fois que la configuration a été importée avec succès sur le serveur principal. L'importation préserve également le CitrixClusterMembership actuel si des nœuds de groupe de serveurs ont été supprimés du groupe de serveurs depuis que la sauvegarde d'origine a été effectuée.

1. Exportez la configuration du Groupe de serveurs 1 depuis 2012R2-A, qui est le serveur principal utilisé pour gérer le groupe de serveurs.



1. Ajoutez ensuite un serveur supplémentaire 2012R2-C au groupe de serveurs existant.



1. Restaurez la configuration du groupe de serveurs à un état fonctionnel antérieur. StoreFront sauvegarde le CitrixClusterMembership actuel de trois serveurs durant le processus d'importation, puis le restaure une fois l'importation terminée.
2. Réimportez la configuration du Groupe de serveurs 1 sur le nœud 2012R2-A.  

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip"-Credential $CredObject
```
3. Propagez la nouvelle configuration importée à tout le groupe de serveurs, de façon à ce que tous les serveurs disposent de la même configuration après l'importation.

**Scénario 2 : sauvegarder une configuration existante du Groupe de serveurs 1 et l'utiliser pour créer un nouveau groupe de serveurs sur une nouvelle installation différente. Vous pouvez ajouter d'autres membres du nouveau groupe de serveurs au nouveau serveur principal**

Le Groupe de serveurs 2 est créé avec deux nouveaux serveurs, 2012R2-C et 2012R2-D. La configuration du Groupe de serveurs 2 sera basée sur la configuration d'un déploiement existant, le Groupe de serveurs 1, qui contient également deux serveurs, 2012R2-A et 2012R2-B. Le CitrixClusterMembership contenu dans l'archive de sauvegarde n'est pas utilisé lors de la création d'un nouveau groupe de serveurs. Le CitrixClusterMembership actuel est toujours sauvegardé puis restauré une fois que l'importation est terminée. Lors de la création d'un nouveau déploiement à l'aide d'une configuration importée, le groupe de sécurité CitrixClusterMembership contient uniquement le serveur d'importation jusqu'à ce que des serveurs supplémentaires soient associés au nouveau groupe. Le Groupe de serveurs 2 est un nouveau déploiement conçu pour coexister avec le Groupe de serveurs 1. Spécifiez le paramètre -HostBaseURL. Le Groupe de serveurs 2 sera créé à l'aide d'une nouvelle l'installation de StoreFront par défaut.

1. Exportez la configuration du Groupe de serveurs 1 depuis 2012R2-A, qui est le serveur principal utilisé pour gérer le groupe de serveurs.
2. Importez la configuration du Groupe de serveurs 1 sur le nœud 2012R2-C, qui sera le serveur principal utilisé pour gérer le Groupe de serveurs 2 nouvellement créé.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\  
backup.ctxzip"-Credential $CredObject -HostBaseURL "https://servergroup2  
.example.com"
```

3. Ajoutez tout serveur supplémentaire qui fera partie du nouveau déploiement du Groupe de serveurs 2. La propagation de la configuration nouvellement importée du Groupe de serveurs 1 à tous les nouveaux membres du Groupe de serveurs 2 est automatique, car cela fait partie du processus d'association normal lorsqu'un nouveau serveur est ajouté.

### **Scénario 3 : sauvegarder une configuration existante du Groupe de serveurs A et l'utiliser pour remplacer la configuration existante du Groupe de serveurs B**

Le Groupe de serveurs 1 et le Groupe de serveurs 2 existent déjà dans deux centres de données distincts. La plupart des modifications de configuration StoreFront sont effectuées sur le Groupe de serveurs 1, que vous devez appliquer au Groupe de serveurs 2 dans l'autre centre de données. Vous pouvez porter les modifications du Groupe de serveurs 1 vers le Groupe de serveurs 2. N'utilisez pas le **CitrixClusterMembership** dans l'archive de sauvegarde sur le Groupe de serveurs 2. Spécifiez le paramètre **-HostBaseURL** durant l'importation, car l'URL de base de l'hôte du Groupe de serveurs 2 ne doit pas être modifiée sur le même nom de domaine complet que celui actuellement utilisé par le Groupe de serveurs 1. Le Groupe de serveurs 2 est un déploiement existant.

1. Exportez la configuration du Groupe de serveurs 1 depuis 2012R2-A, qui est le serveur principal utilisé pour gérer le groupe de serveurs.
2. Importez la configuration du Groupe de serveurs 1 sur la nouvelle installation par défaut sur le nœud 2012R2-C, qui sera le serveur principal du nouveau Groupe de serveurs 2.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\  
backup.ctxzip"-Credential $CredObject -HostBaseURL "https://servergroup2  
.example.com"
```

## SDK StoreFront

February 20, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

Citrix StoreFront fournit un kit de développement logiciel (SDK) basé sur un certain nombre de modules Microsoft Windows PowerShell version 3.0. Avec le kit de développement, vous pouvez effectuer les mêmes tâches qu'avec la console MMC StoreFront, ainsi que les tâches que vous ne pouvez pas effectuer avec la console uniquement.

Pour la référence SDK, consultez [SDK StoreFront](#).

### Différences clés entre le kit de développement StoreFront 3.0 et celui de la version actuelle de StoreFront

- **Exemples de SDK haut niveau** : cette version propose des scripts SDK de haut niveau qui vous permettent de créer un script et d'automatiser les déploiements StoreFront rapidement et facilement. Vous pouvez personnaliser les exemples de haut niveau selon vos besoins spécifiques, ce qui vous permet de créer un nouveau déploiement simplement par l'exécution d'un script.
- **Nouveau SDK de bas niveau** : Citrix offre un SDK StoreFront de bas niveau documenté permettant la configuration de déploiements, notamment des magasins, des méthodes d'authentification, des sites Citrix Receiver pour Web et Citrix Receiver unifié ainsi que l'accès distant avec NetScaler Gateway.
- **Rétrocompatibilité** : StoreFront 3.6 contient toujours les API de StoreFront 3.0 et versions antérieures, par conséquent les scripts existants peuvent être progressivement transférés vers le nouveau SDK.

### Important :

La rétrocompatibilité avec StoreFront 3.0 a été maintenue dans la mesure du possible. Toutefois, lors de l'écriture de scripts, Citrix recommande d'utiliser les nouveaux modules **Citrix.StoreFront.\***, car le kit de développement logiciel (SDK) StoreFront 3.0 est obsolète et sera supprimé.

## Utilisez le Kit de développement logiciel (SDK)

Le kit de développement logiciel comprend un certain nombre de composants logiciels enfichables PowerShell installés automatiquement par l'assistant d'installation lorsque vous installez différents composants StoreFront.

Pour accéder aux applets de commande et les exécuter :

1. Démarrez un shell dans PowerShell 3.0.

Vous devez exécuter le Shell ou le script en tant que membre du groupe d'administrateurs locaux sur le serveur StoreFront.

2. Pour utiliser les applets de commande du kit de développement dans des scripts, définissez la stratégie d'exécution dans PowerShell.

Pour plus d'informations sur la stratégie d'exécution PowerShell, veuillez consulter votre documentation Microsoft.

3. Ajoutez les modules dont vous avez besoin à l'environnement PowerShell en utilisant la commande **Add -Module** dans la console Windows PowerShell. Par exemple, entrez :

```
Import-Module Citrix.StoreFront
```

Pour importer toutes les applets de commande, entrez :

```
Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront")} | Import-Module
```

Après importation, vous avez accès aux applets de commande et à l'aide associée.

## Démarrage avec SDK

Pour créer un script, réalisez les étapes suivantes :

1. Utilisez un des exemples SDK fournis et installés par StoreFront dans le dossier **%Program-Files%\Citrix\Receiver StoreFront\PowerShellSDK\Examples**.
2. Pour vous aider à personnaliser votre propre script, consultez l'exemple de script pour comprendre la fonction de chaque partie. Pour plus d'informations, consultez l'exemple de cas d'utilisation qui décrit en détail les actions du script.
3. Convertissez et adaptez les exemples de script pour les changer en un script plus lisible. Pour ce faire :
  - Utilisez PowerShell ISE ou un outil similaire pour modifier le script.
  - Utilisez des variables pour affecter les valeurs à réutiliser ou modifier.
  - Supprimez toute commande qui n'est pas requise.
  - Notez que les applets de commande StoreFront peuvent être identifiées par le préfixe STF.

- Utilisez l'applet de commande **Get-Help** en fournissant le nom de la commande et le paramètre **-Full** pour de plus amples informations sur la commande.

## Exemples

### Remarque :

Lors de la création d'un script, pour vous assurer que vous obtiendrez toujours les dernières améliorations et derniers correctifs, Citrix vous recommande de suivre la procédure décrite ci-dessus, plutôt que de copier et de coller les scripts exemples.

Exemples	Description
Créer un déploiement simple	Script : crée un déploiement simple avec un contrôleur StoreFront configuré avec un seul serveur XenDesktop.
Créer un déploiement avec accès à distance	Script : basé sur le script précédent, ajoute l'accès à distance au déploiement.
Créer un déploiement avec accès à distance et passerelle de lancement optimale	Script : basé sur le script précédent, ajoute des passerelles de lancement optimales pour une meilleure expérience utilisateur.
Créer un déploiement avec un site Desktop Appliance	Script : crée un déploiement simple configuré avec un site Desktop Appliance.

### Exemple : Créer un déploiement simple

L'exemple suivant illustre comment créer un déploiement simple configuré avec un Controller XenDesktop.

Avant de commencer, suivez les étapes détaillées dans [Démarrage avec SDK](#). Cet exemple peut être personnalisé à l'aide des méthodes décrites pour produire un script qui automatise le déploiement StoreFront.

### Remarque :

Pour vous assurer que vous obtiendrez toujours les dernières améliorations et correctifs, Citrix vous recommande de suivre la procédure décrite dans ce document, plutôt que de copier et de coller le script exemple.

## Compréhension du script

Cette section décrit la fonction de chaque partie du script généré par StoreFront. Ceci vous aidera à la personnalisation de votre propre script.

- Définit la gestion des erreurs et importe les modules StoreFront requis. Les importations ne sont pas nécessaires dans des versions plus récentes de PowerShell.

```

1 Param(
2     [Parameter(Mandatory=$true)]
3     [Uri]$HostbaseUrl,
4     [long]$SiteId = 1,
5     [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
6         ")]
7     [string]$Farmtype = "XenDesktop",
8     [Parameter(Mandatory=$true)]
9     [string[]]$FarmServers,
10    [string]$StoreVirtualPath = "/Citrix/Store",
11    [bool]$LoadbalanceServers = $false,
12    [int]$Port = 80,
13    [int]$SSLRelayPort = 443,
14    [ValidateSet("HTTP","HTTPS","SSL")]
15    [string]$TransportType = "HTTP"
16 )
17 # Import StoreFront modules. Required for versions of
18 # PowerShell earlier than 3.0 that do not support
19 # autoloading
20 Import-Module Citrix.StoreFront
21 Import-Module Citrix.StoreFront.Stores
22 Import-Module Citrix.StoreFront.Authentication
23 Import-Module Citrix.StoreFront.WebReceiver

```

- Automatise le chemin d'accès virtuel de l'authentification et des services Citrix Receiver pour Web basé sur le paramètre **\$StoreIISPath** fourni.

```

1 # Determine the Authentication and Receiver virtual path to use
2 # based of the Store
3 $authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
4 $receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"

```

- Crée un nouveau déploiement, si ce n'est pas déjà fait, pour préparer l'ajout des services StoreFront requis. **-Confirm:\$false** supprime le besoin de confirmer que le déploiement peut se poursuivre.

```

1 # Determine if the deployment already exists
2 $existingDeployment = Get-STFDeployment
3 if(-not $existingDeployment)

```



```
4 {
5
6     # Install the required StoreFront components
7     Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
8 }
9
10 elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
11 {
12
13     # The deployment exists but it is configured to the desired
        hostbase url
14     Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
15 }
16
17 else
18 {
19
20     Write-Error "A deployment has already been created on this
        server with a different host base url."
21 }
```

- Crée un nouveau service d'authentification s'il n'en n'existe aucun dans le chemin d'accès virtuel spécifié. La méthode d'authentification par défaut, nom d'utilisateur et mot de passe, est activée.

```
1 # Determine if the authentication service at the specified
    virtual path exists
2 $authentication = Get-STFAuthenticationService -VirtualPath
    $authenticationVirtualPath
3 if(-not $authentication)
4 {
5
6     # Add an Authentication service using the IIS path of the
        Store appended with Auth
7     $authentication = Add-STFAuthenticationService
        $authenticationVirtualPath
8 }
9
10 else
11 {
12
13     Write-Output "An Authentication service already exists at the
        specified virtual path and will be used."
```

```
14 }
```

- Crée le nouveau service de magasin configuré avec un Controller XenDesktop avec les serveurs définis dans le tableau **\$XenDesktopServers** dans le chemin d'accès virtuel spécifié s'il n'en n'existe aucun.

```

1  # Determine if the store service at the specified virtual path
    exists
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  if(-not $store)
4  {
5
6  # Add a Store that uses the new Authentication service configured
    to publish resources from the supplied servers
7  $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
    AuthenticationService $authentication -FarmName $Farmtype -
    FarmType $Farmtype -Servers $FarmServers -LoadBalance
    $LoadbalanceServers '
8      -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
        $TransportType
9  }
10
11 else
12 {
13
14     Write-Output "A Store service already exists at the specified
        virtual path and will be used. Farm and servers will be
        appended to this store."
15     # Get the number of farms configured in the store
16     $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
        Count
17     # Append the farm to the store with a unique name
18     Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
        $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
        -LoadBalance $LoadbalanceServers -Port $Port '
19     -SSLRelayPort $SSLRelayPort -TransportType $TransportType
20 }
```

- Ajoute un service Citrix Receiver pour Web au chemin d'accès virtuel IIS spécifié pour accéder aux applications publiées dans le magasin créé ci-dessus.

```

1  # Determine if the receiver service at the specified virtual path
    exists
2  $receiver = Get-STFWebReceiverService -VirtualPath
    $receiverVirtualPath
```

```
3  if(-not $receiver)
4  {
5
6      # Add a Receiver for Web site so users can access the
          applications and desktops in the published in the Store
7      $receiver = Add-STFWebReceiverService -VirtualPath
          $receiverVirtualPath -StoreService $store
8  }
9
10 else
11 {
12
13     Write-Output "A Web Receiver service already exists at the
          specified virtual path and will be used."
14 }
```

- Active les services XenApp pour le magasin de sorte que les anciennes versions des clients de Citrix Receiver puissent se connecter aux applications publiées.

```
1  # Determine if PNA is configured for the Store service
2  $storePnaSettings = Get-STFStorePna -StoreService $store
3  if(-not $storePnaSettings.PnaEnabled)
4  {
5
6      # Enable XenApp services on the store and make it the default for
          this server
7      Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
          -DefaultPnaService
8  }
```

## Créer un déploiement avec accès à distance

L'exemple suivant est basé sur le script précédent et ajoute un déploiement avec accès à distance.

Avant de commencer, suivez les étapes détaillées dans [Démarrage avec SDK](#). Cet exemple peut être personnalisé à l'aide des méthodes décrites pour produire un script qui automatise le déploiement StoreFront.

### Remarque :

Pour vous assurer que vous obtiendrez toujours les dernières améliorations et correctifs, Citrix vous recommande de suivre la procédure décrite dans ce document, plutôt que de copier et de coller le script exemple.

## Compréhension du script

Cette section décrit la fonction de chaque partie du script généré par StoreFront. Ceci vous aidera à la personnalisation de votre propre script.

- Définit la gestion des erreurs et importe les modules StoreFront requis. Les importations ne sont pas nécessaires dans des versions plus récentes de PowerShell.

```
1 Param(
2     [Parameter(Mandatory=$true)]
3     [Uri]$HostbaseUrl,
4     [Parameter(Mandatory=$true)]
5     [long]$SiteId = 1,
6     [string]$Farmtype = "XenDesktop",
7     [Parameter(Mandatory=$true)]
8     [string[]]$FarmServers,
9     [string]$StoreVirtualPath = "/Citrix/Store",
10    [bool]$LoadbalanceServers = $false,
11    [int]$Port = 80,
12    [int]$SSLRelayPort = 443,
13    [ValidateSet("HTTP","HTTPS","SSL")]
14    [string]$TransportType = "HTTP",
15    [Parameter(Mandatory=$true)]
16    [Uri]$GatewayUrl,
17    [Parameter(Mandatory=$true)]
18    [Uri]$GatewayCallbackUrl,
19    [Parameter(Mandatory=$true)]
20    [string[]]$GatewaySTAUrls,
21    [string]$GatewaySubnetIP,
22    [Parameter(Mandatory=$true)]
23    [string]$GatewayName
24 )
25 Set-StrictMode -Version 2.0
26
27 # Any failure is a terminating failure.
28 $ErrorActionPreference = 'Stop'
29 $ReportErrorShowStackTrace = $true
30 $ReportErrorShowInnerException = $true
31 # Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
32 Import-Module Citrix.StoreFront
33 Import-Module Citrix.StoreFront.Stores
34 Import-Module Citrix.StoreFront.Roaming
```

- Créez un déploiement StoreFront avec accès en interne en appelant les exemples précédents de script. Le déploiement de base sera étendu pour prendre en charge l'accès distant.

```

1 # Create a simple deployment by invoking the SimpleDeployment
  example
2 $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
  Definition -Parent
3 $scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
4 & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
  FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
  Farmtype $Farmtype '
5   -LoadbalanceServers $LoadbalanceServers -Port $Port -
  SSLRelayPort $SSLRelayPort -TransportType $TransportType

```

- Obtient les services créés dans le déploiement simple car ils doivent être mis à jour pour prendre en charge le scénario d'accès à distance.

```

1 # Determine the Authentication and Receiver sites based on the
  Store
2 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3 $authentication = Get-STFAuthenticationService -StoreService
  $store
4 $receiverForWeb = Get-STFWebReceiverService -StoreService $store

```

- Active CitrixAGBasic sur le service Citrix Receiver pour Web requis pour l'accès à distance à l'aide de NetScaler Gateway. Obtenir la méthode d'authentification ExplicitForms et CitrixAGBasic de Citrix Receiver pour Web à partir des protocoles pris en charge.

```

1 # Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
  authentication method from the supported protocols
2 # Included for demonstration purposes as the protocol name can be
  used directly if known
3 $receiverMethods = Get-
  STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
4   $_ -match "Explicit" -or $_ -match "CitrixAG" }
5
6 # Enable CitrixAGBasic in Receiver for Web (required for remote
  access)
7 Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
  $receiverMethods

```

- Active CitrixAGBasic sur le service d'authentification. Requis pour l'accès distant.

```

1 # Get the CitrixAGBasic authentication method from the protocols
  installed.
2 # Included for demonstration purposes as the protocol name can be
  used directly if known

```

```

3  $CitrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
    Object {
4  $_ -match "CitrixAGBasic" }
5
6  # Enable CitrixAGBasic in the Authentication service (required
    for remote access)
7  Enable-STFAuthenticationServiceProtocol -AuthenticationService
    $authentication -Name $CitrixAGBasic

```

- Ajoute une passerelle d'accès à distance, en ajoutant l'adresse IP de sous-réseau facultative qui est fournie et en l'enregistrant auprès du magasin auquel accéder à distance.

```

1  # Add a new Gateway used to access the new store remotely
2  Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
3  -CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
4  # Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
5  $gateway = Get-STFRoamingGateway -Name $GatewayName
6  # If the gateway subnet was provided then set it on the gateway
    object
7  if($GatewaySubnetIP)
8  {
9
10     Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
11 }
12
13 # Register the Gateway with the new Store
14 Register-STFStoreGateway -Gateway $gateway -StoreService $store -
    DefaultGateway

```

### Exemple : Créer un déploiement avec accès à distance et passerelle de lancement optimale

L'exemple suivant est basé sur le script précédent et ajoute un déploiement avec accès à distance et passerelle de lancement optimale.

Avant de commencer, suivez les étapes détaillées dans [Démarrage avec SDK](#). Cet exemple peut être personnalisé à l'aide des méthodes décrites pour produire un script qui automatise le déploiement StoreFront.

**Remarque :**

Pour vous assurer que vous obtiendrez toujours les dernières améliorations et correctifs, Citrix vous recommande de suivre la procédure décrite dans ce document, plutôt que de copier et de coller le script exemple.

**Compréhension du script**

Cette section décrit la fonction de chaque partie du script généré par StoreFront. Ceci vous aidera à la personnalisation de votre propre script.

- Définit la gestion des erreurs et importe les modules StoreFront requis. Les importations ne sont pas nécessaires dans des versions plus récentes de PowerShell.

```
1 Param(
2     [Parameter(Mandatory=$true)]
3     [Uri]$HostbaseUrl,
4     [long]$SiteId = 1,
5     [string]$Farmtype = "XenDesktop",
6     [Parameter(Mandatory=$true)]
7     [string[]]$FarmServers,
8     [string]$StoreVirtualPath = "/Citrix/Store",
9     [bool]$LoadbalanceServers = $false,
10    [int]$Port = 80,
11    [int]$SSLRelayPort = 443,
12    [ValidateSet("HTTP","HTTPS","SSL")]
13    [string]$TransportType = "HTTP",
14    [Parameter(Mandatory=$true)]
15    [Uri]$GatewayUrl,
16    [Parameter(Mandatory=$true)]
17    [Uri]$GatewayCallbackUrl,
18    [Parameter(Mandatory=$true)]
19    [string[]]$GatewaySTAUrls,
20    [string]$GatewaySubnetIP,
21    [Parameter(Mandatory=$true)]
22    [string]$GatewayName,
23    [Parameter(Mandatory=$true)]
24    [Uri]$OptimalGatewayUrl,
25    [Parameter(Mandatory=$true)]
26    [string[]]$OptimalGatewaySTAUrls,
27    [Parameter(Mandatory=$true)]
28    [string]$OptimalGatewayName
29 )
30 Set-StrictMode -Version 2.0
31 # Any failure is a terminating failure.
```

```

32 $ErrorActionPreference = 'Stop'
33 $ReportErrorShowStackTrace = $true
34 $ReportErrorShowInnerException = $true
35 # Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
36 Import-Module Citrix.StoreFront
37 Import-Module Citrix.StoreFront.Stores
38 Import-Module Citrix.StoreFront.Roaming

```

- Appels dans le script de déploiement avec accès à distance pour configurer le déploiement de base et ajouter l'accès à distance.

```

1 # Create a remote access deployment
2 $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
3 $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
    ps1"
4 & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype '
5 -LoadbalanceServers $LoadbalanceServers -Port $Port -
    SSLRelayPort $SSLRelayPort -TransportType $TransportType '
6 -GatewayUrl $GatewayUrl -GatewayCallbackUrl
    $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
    GatewayName $GatewayName

```

- Ajoute la passerelle de lancement optimale préférée à partir de la liste de passerelles configurées.

```

1 # Add a new Gateway used for remote HDX access to desktops and
    apps
2 $gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -
    LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -
    SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru

```

- Oblige le service de magasin à utiliser la passerelle optimale, l'enregistrer, et l'attribuer aux lancements depuis la batterie désignée.

```

1 # Get the Store configured by SimpleDeployment.ps1
2 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3 # Register the Gateway with the new Store for launch against all
    of the farms (currently just one)
4 $farmNames = @($store.FarmsConfiguration.Farms | foreach {
5     $_.FarmName }
6 )

```



```
7 Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
  StoreService $store -FarmName $farmNames
```

### Exemple : Créer un déploiement avec un site Desktop Appliance

L'exemple suivant se base sur l'exemple de déploiement simple et ajoute un déploiement avec un site Desktop Appliance.

Avant de commencer, suivez les étapes détaillées dans [Démarrage avec SDK](#). Cet exemple peut être personnalisé à l'aide des méthodes décrites pour produire un script qui automatise le déploiement StoreFront.

#### Remarque :

Pour vous assurer que vous obtiendrez toujours les dernières améliorations et correctifs, Citrix vous recommande de suivre la procédure décrite dans ce document, plutôt que de copier et de coller le script exemple.

### Compréhension du script

Cette section décrit la fonction de chaque partie du script généré par StoreFront. Ceci vous aidera à la personnalisation de votre propre script.

- Définit la gestion des erreurs et importe les modules StoreFront requis. Les importations ne sont pas nécessaires dans des versions plus récentes de PowerShell.

```
1 Param(
2     [Parameter(Mandatory=$true)]
3     [Uri]$HostbaseUrl,
4     [long]$SiteId = 1,
5     [string]$Farmtype = "XenDesktop",
6     [Parameter(Mandatory=$true)]
7     [string[]]$FarmServers,
8     [string]$StoreVirtualPath = "/Citrix/Store",
9     [bool]$LoadbalanceServers = $false,
10    [int]$Port = 80,
11    [int]$SSLRelayPort = 443,
12    [ValidateSet("HTTP", "HTTPS", "SSL")]
13    [string]$TransportType = "HTTP",
14    [Parameter(Mandatory=$true)]
15    [Uri]$GatewayUrl,
16    [Parameter(Mandatory=$true)]
17    [Uri]$GatewayCallbackUrl,
18    [Parameter(Mandatory=$true)]
```

```

19     [string[]]$GatewaySTAUrls,
20     [string]$GatewaySubnetIP,
21     [Parameter(Mandatory=$true)]
22     [string]$GatewayName,
23     [Parameter(Mandatory=$true)]
24     [Uri]$OptimalGatewayUrl,
25     [Parameter(Mandatory=$true)]
26     [string[]]$OptimalGatewaySTAUrls,
27     [Parameter(Mandatory=$true)]
28     [string]$OptimalGatewayName
29 )
30 Set-StrictMode -Version 2.0
31 # Any failure is a terminating failure.
32 $ErrorActionPreference = 'Stop'
33 $ReportErrorShowStackTrace = $true
34 $ReportErrorShowInnerException = $true
35 # Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
36 Import-Module Citrix.StoreFront
37 Import-Module Citrix.StoreFront.Stores
38 Import-Module Citrix.StoreFront.Roaming

```

- Automatiser un chemin d'accès au boîtier de bureau basé sur celui de \$StoreVirtualPath.

```

1 $desktopApplianceVirtualPath = "$($StoreIISPath.TrimEnd('/'))
    Appliance"

```

- Appels dans le script de déploiement simple pour configurer un déploiement par défaut avec les services requis.

```

1 # Create a remote access deployment
2 $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
3 $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
    ps1"
4 & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype '
5     -LoadbalanceServers $LoadbalanceServers -Port $Port -
        SSLRelayPort $SSLRelayPort -TransportType $TransportType '
6     -GatewayUrl $GatewayUrl -GatewayCallbackUrl
        $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
        GatewayName $GatewayName

```

- Obtient le service de magasin de données à utiliser pour le site Desktop Appliance. Utilisez

l'applet de commande **Add-STFDesktopApplianceService** pour ajouter le nouveau site avec l'authentification MultiDesktop et l'authentification explicite par nom d'utilisateur et mot de passe.

```
1 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
2 # Create a new Desktop Appliance site using the desktops
  published by the Store Service
3 Add-STFDesktopApplianceService -VirtualPath
  $desktopApplianceVirtualPath -StoreService $store -
  EnableExplicit
```

### Exemple : échange des métadonnées entre le fournisseur d'identité et le fournisseur de services (StoreFront) pour l'authentification SAML

L'authentification SAML peut être configurée dans la console de gestion StoreFront (consultez [Configurer le service d'authentification](#)) ou à l'aide des applets de commande PowerShell suivantes :

- Export-STFSamlEncryptionCertificate
- Export-STFSamlSigningCertificate
- Import-STFSamlEncryptionCertificate
- Import-STFSamlSigningCertificate
- New-STFSamlEncryptionCertificate
- Nouveau-STFSamlIdPCertificate
- New-STFSamlSigningCertificate

Vous pouvez utiliser l'applet de commande, **Update-STFSamlIdPFromMetadata**, pour échanger des métadonnées (identificateurs, certificats, points de terminaison et autres configurations) entre le fournisseur d'identité et le fournisseur de services, qui est StoreFront dans ce cas.

Pour un magasin StoreFront, appelé « Store », avec son propre service d'authentification, le point de terminaison de métadonnées sera :

<https://<storefront host>/Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata>

Si votre fournisseur d'identité prend en charge l'importation de métadonnées, vous pouvez également le pointer sur l'adresse URL ci-dessus. **Remarque** : cette opération doit être effectuée sur HTTPS.

Pour que StoreFront utilise les métadonnées d'un fournisseur d'identité, vous pouvez utiliser le PowerShell suivant :

```
1 Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module
2
```

```

3 # Remember to change this with the virtual path of your Store.
4 $StoreVirtualPath = "/Citrix/Store"
5
6 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
7 $auth = Get-STFAuthenticationService -StoreService $store
8
9 # To read the metadata directly from the Identity Provider, use the
   following:
10 # Note again this is only allowed for https endpoints
11 Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https:
   //example.com/FederationMetadata/2007-06/FederationMetadata.xml
12
13 # If the metadata has already been download, use the following:
14 # Note: Ensure that the file is encoded as UTF-8
15 Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C
   :\Users\exampleusername\Downloads\FederationMetadata.xml"

```

### Exemple : répertorier les métadonnées et les points de terminaison ACS d'un magasin spécifié pour l'authentification SAML

Vous pouvez utiliser le script suivant pour répertorier les métadonnées et les points de terminaison ACS (service consommateur d'assertion) pour un magasin spécifié.

```

1 # Change this value for your Store
2 $storeVirtualPath = "/Citrix/Store"
3
4 $auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
   VirtualPath $storeVirtualPath)
5 $spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
   ServiceProvider.Uri.AbsoluteUri
6 $acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
   VirtualPath + "/SamlForms/AssertionConsumerService")
7 $md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
   VirtualPath + "/SamlForms/ServiceProvider/Metadata")
8 $samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
   VirtualPath + "/SamlTest")
9 Write-Host "SAML Service Provider information:
10 Service Provider ID: $spId
11 Assertion Consumer Service: $acs
12 Metadata: $md
13 Test Page: $samlTest"

```

Exemple de sortie :

```
1 SAML Service Provider information:  
2 Service Provider ID: https://storefront.example.com/Citrix/StoreAuth  
3 Assertion Consumer Service: https://storefront.example.com/Citrix/  
  StoreAuth/SamlForms/AssertionConsumerService  
4 Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/  
  ServiceProvider/Metadata  
5 Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
```

## Résolution des problèmes de StoreFront

February 26, 2019

### Remarque :

vous trouverez des informations sur les changements de nom de produit dans la section [Nouveautés](#).

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\StoreFront`. 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 les modifications terminées, [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\nommagasin` et `C:\inetpub\wwwroot\Citrix\nommagasinWeb\`, où *nommagasin* désigne le nom indiqué pour le magasin au moment de sa création.
2. Recherchez l'élément suivant dans le fichier.

```
<logger duplicateInterval="00:01:00"duplicateLimit="10">
```

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.

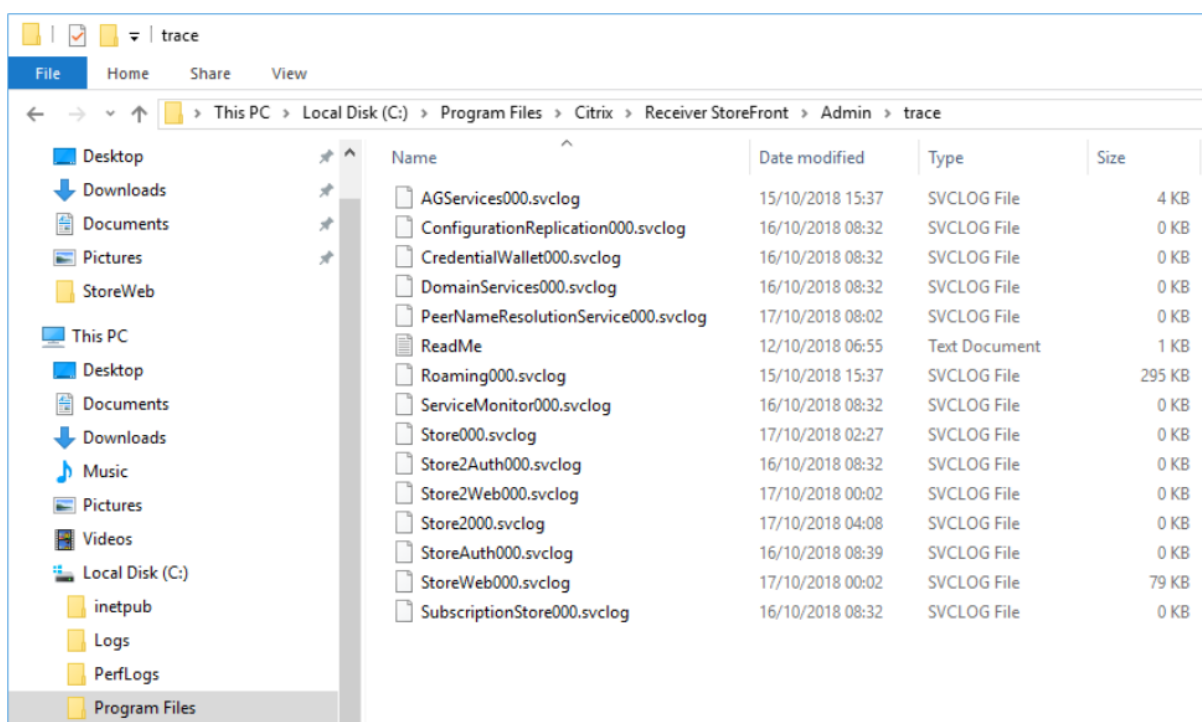
Lors du déclenchement de l'optimisation du journal, un message d'avertissement est journalisé pour indiquer que les autres entrées de journal identiques seront supprimées. Une fois la durée écoulée, la journalisation normale se poursuit et un message d'information est journalisé pour indiquer que les doublons d'entrées du journal ne sont plus supprimés.

### **Activer le suivi pour le débogage**

#### **Important :**

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 la console PowerShell avant d'ouvrir la console StoreFront.

L'emplacement des traces est `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`



#### Remarque :

Exécutez `Get-Help Set-STFDiagnostics -detailed` pour obtenir de l'aide pour PowerShell et des instructions sur l'utilisation de l'applet de commande `Set-STFDiagnostics`.

Utilisez un compte possédant des permissions d'administrateur local pour démarrer Windows PowerShell et, à l'invite de commande, spécifiez les paramètres obligatoires suivants pour activer ou désactiver le suivi.

- **-All.** Un indicateur signalant que le suivi doit être mis à jour pour toutes les instances et tous les services.
- **-TraceLevel.** Les valeurs autorisées pour `-TraceLevel` sont les suivantes (niveau de détail de suivi croissant) : Off (Désactivé), Error (Erreur), Warning (Avertissement), Info (Infos), Verbose (Détailé). En raison de la grande quantité de données pouvant être générées, le suivi peut avoir un impact significatif sur la performance de StoreFront. Les niveaux Info ou Verbose ne sont pas recommandés sauf s'ils sont requis spécifiquement à des fins de dépannage.

Paramètres facultatifs :

- **-FileSizeKb.** Taille du fichier de trace en Ko.
- **-FileCount.** Nombre de fichiers de trace à conserver sur un disque à la fois.
- **-confirm:\$False.** Supprime les invites Windows à autoriser l'applet de commande StoreFront à s'exécuter à chaque fois.

## Exemples

Pour activer le suivi de niveau Verbose pour tous les services à des fins de débogage :

```
1 Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
```

Pour désactiver le suivi de niveau Verbose et définir le niveau de suivi sur la valeur par défaut pour tous les services :

```
1 Set-STFDiagnostics -All -TraceLevel "Error" -confirm:$False
```

Pour plus d'informations sur l'applet de commande Set-STFDiagnostics, consultez la documentation [StoreFront PowerShell SDK](#).

## Pour autoriser la journalisation du fichier launch.ica

Enregistrez les informations dans le fichier launch.ica sur l'ordinateur client pour résoudre plusieurs problèmes. Le fichier launch.ica est généré par l'interface Web Citrix ou les serveurs Citrix StoreFront.

Pour autoriser la journalisation du fichier launch.ica, procédez comme suit :

1. Accédez à la clé de registre suivante en utilisant l'éditeur de registre :

  Systèmes 32 bits : HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\  
  Configuration\Advanced\Modules\Logging

  Systèmes 64 bits : HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\  
  \Engine\Configuration\Advanced\Modules\Logging

2. Définissez la valeur de chaîne suivante :

  LogFile=<chemin d'accès au fichier journal, utilisez le format suivant C:\ica\ica.log>  
  LogICAFile=true

## Ressources supplémentaires

Remarque :

L'utilisation d'un fichier ICA dans votre environnement pour autre chose qu'un dépannage est abordée dans [CTX200126](#).





**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).