CITRIX

StoreFront 1912

Contents

StoreFront 1912 3

Nouveautés 4

Problèmes résolus 5

Problèmes connus 6

Avis de tiers 7

Configuration système requise 7

Planifier votre déploiement StoreFront 14

Options d'accès utilisateur 20

Authentification utilisateur 30

Optimiser l'expérience utilisateur 42

Haute disponibilité et configuration multisite de StoreFront 47

Installer, configurer, mettre à niveau et désinstaller 52

Créer un nouveau déploiement 76

Joindre un groupe de serveurs existant 83

Réinitialiser les paramètres d'usine du serveur 84

Migrer les fonctionnalités de l'Interface Web vers StoreFront 86

Configurer des groupes de serveurs 92

Configurer l'authentification et la délégation 96

Configurer le service d'authentification 97

Authentification basée sur le service XML 105

Configurer la délégation Kerberos contrainte pour XenApp 6.5 108

Configuration de l'authentification par carte à puce 112

Configurer la période de notification d'expiration du mot de passe 118

Configurer et gérer des magasins 119

Créer ou supprimer un magasin 120

Créer un magasin non authentifié 127

Exporter des fichiers de provisioning de magasin pour des utilisateurs 130

Publier et masquer des magasins pour les utilisateurs 131

Gérer les ressources mises à disposition dans les magasins 131

Gérer l'accès distant aux magasins via Citrix Gateway 133

Vérification des listes de révocation de certificats (CRL) 137

Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun 148

Gérer les données d'abonnement d'un magasin 149

stocker les données d'abonnement à l'aide de Microsoft SQL Server 155

Paramètres de magasin avancés 177

Gérer un site Citrix Receiver pour Web 182

Créer un site Citrix Receiver pour Web 183

Configurer des sites Citrix Receiver pour Web 184

Prise en charge de l'expérience utilisateur unifiée 192

Créer et gérer des applications recommandées 214

Configurer le contrôle de l'espace de travail 216

Configurer l'utilisation des onglets de navigateur par l'application Citrix Workspace pour HTML5 217

Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion 218

Configurer l'accès utilisateur 220

Configurer StoreFront pour lancer les applications et les bureaux en mode fenêtré 223

Définir des magasins multisite à haute disponibilité 225

Intégrer avec Citrix Gateway et Citrix ADC 244

Ajouter une connexion Citrix Gateway 247

Importer un appliance Citrix Gateway 250

Configurer les paramètres de connexion Citrix Gateway 260

Équilibrage de charge avec l'appliance Citrix ADC 264

Configurer deux adresses URL pour la même instance Citrix Gateway 282

Configurer Citrix ADC et StoreFront pour l'authentification DFA 294

Authentification à l'aide de domaines différents 297

Configurer des points balises 308

Créer un seul nom de domaine complet (FQDN) pour accéder à un magasin en interne et externe 310

Configurations avancées 329

Configurer le filtrage des ressources 330

Configurer des sites à l'aide des fichiers de configuration 331

Configurer StoreFront à l'aide des fichiers de configuration 332

Configurer des sites Citrix Receiver pour Web à l'aide des fichiers de configuration 337

Sécuriser votre déploiement StoreFront 338

Exporter et importer la configuration StoreFront 348

SDK StoreFront 358

Résolution des problèmes de StoreFront 372

StoreFront 1912

January 30, 2020

StoreFront 1912 est la version actuelle 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 et peut être utilisé avec plusieurs versions de Virtual Apps and Desktops.

Les utilisateurs peuvent utiliser l'application Citrix Workspace ou les versions prises en charge de Citrix Receiver pour accéder aux magasins StoreFront. Si une version spécifique se comporte différemment, ou si le texte de l'interface utilisateur fait référence aux deux, cela est spécifié de manière appropriée. Sinon, la documentation fait référence à « application Citrix Workspace ».

Versions précédentes

Pour accéder à la documentation des versions antérieures, consultez :

- StoreFront 1909
- StoreFront 1906
- StoreFront 1903
- StoreFront 1811
- StoreFront 3.16
- StoreFront 3.12
- StoreFront 3.0
- Versions antérieures de StoreFront

La stratégie de cycle de vie du produit des version CR (Current Releases) et LTSR (Long Term Service Releases) de Citrix Virtual Apps and Desktops est décrite dans la section 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 actuelle (Current Release) de StoreFront à partir de versions plus anciennes non prises en charge ne sont pas gérées. Si vous utilisez une version actuelle (Current Release), vous devez vous assurer que vous utilisez une version actuelle de StoreFront prise en charge à tout moment.

Nouveautés

January 30, 2020

StoreFront 1912

StoreFront 1912 comprend les nouvelles fonctionnalités suivantes. Pour plus d'informations sur les corrections de bogues, veuillez consulter la section Problèmes résolus.

Prise en charge des appareils Chrome avec l'application Workspace pour Android par le gestionnaire de protocoles StoreFront

Lorsque les utilisateurs d'appareils Chrome ouvrent un site Citrix Receiver pour Web et que l'application Citrix Workspace pour Android 1912 ou version ultérieure est installée, le navigateur ouvre automatiquement les fichiers ICA à l'aide de l'application Citrix Workspace pour Android lors du lancement.

Le workflow de détection client pour Android, qui détermine si l'application Citrix Workspace pour Android est installée, est désormais identique à l'application Citrix Workspace pour Windows et l'application Citrix Workspace pour MAC lorsque le navigateur Chrome est utilisé sur des appareils Chrome. Dans les versions précédentes, les utilisateurs d'appareils Chrome devaient d'abord ouvrir manuellement un fichier ICA téléchargé.

Prise en charge des stratégies de protection des applications

StoreFront 1912 prend en charge les stratégies de protection des applications pour améliorer la sécurité lorsque d'autres composants Citrix, tels que l'application Citrix Workspace et les Delivery Controller Citrix Virtual Apps and Desktops, prennent également en charge la fonctionnalité de protection des applications. Les stratégies de protection des applications sont définies au niveau du groupe de mise à disposition et Citrix Virtual Apps and Desktops détermine si les stratégies de protection des applications sont utilisées. Vous devez activer manuellement la fonctionnalité de protection des applications dans StoreFront. Lorsque StoreFront reçoit des requêtes contenant l'en-tête « X-Citrix-AppProtection-Capable » à partir d'une application Citrix Workspace qui prend en charge les stratégies de protection des applications, StoreFront envoie automatiquement une balise Smart Access à Citrix Virtual Apps and Desktops indiquant que les stratégies de protection des applications sont prises en charge. Pour plus d'informations sur la configuration des groupes de mise à disposition avec des stratégies de protection des applications, consultez la section Protection des applications.

Pour activer la protection des applications sur un serveur StoreFront, exécutez la commande PowerShell suivante sur le serveur StoreFront : `Add-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control" -IsEnabled $True`. (Dans un déploiement StoreFront avec plusieurs serveurs, vous devez propager manuellement ces modifications à tous les autres serveurs du groupe de serveurs. Voir Propager les modifications locales à un groupe de serveurs.)

Pour vérifier que la fonctionnalité est activée sur un serveur StoreFront, utilisez la commande PowerShell suivante :
`Get-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control`.

Fin de la prise en charge des sites Desktop Appliance

La fin de la prise en charge StoreFront permettant aux utilisateurs d'accéder aux bureaux sur les sites Desktop Appliance a été annoncée dans Citrix Virtual Apps and Desktops 7 1811. Dans cette version, les sites Desktop Appliance ne sont plus pris en charge. Nous vous recommandons donc d'utiliser l'application Citrix Workspace Verrouillage du bureau pour tous les cas d'utilisation n'appartenant pas au domaine.

> **Avertissement :**
>
> Lorsque vous effectuez une mise à niveau vers StoreFront 1912, tous les sites Desktop Appliance de votre déploiement sont automatiquement supprimés. Voir Mettre à niveau StoreFront.

SDK PowerShell StoreFront

Le SDK PowerShell StoreFront a été republié en tant que version 1912. Vous ne pouvez plus créer ou gérer des sites Desktop Appliance à l'aide de PowerShell.

Problèmes résolus

January 30, 2020

Les problèmes suivants ont été résolus depuis la version 1909 :

- Une instance StoreFront locale ne peut pas ajouter de passerelle de lancement pour les liens Web dans MMC. [WSP-4368]
- LCM-6351 : les anciennes clés de registre CitrixPrivilegedService_x64.msi n'ont pas été supprimées après la mise à niveau DDC. [WSP-4785]

- Si VMware VMTools v10.3.x est installé sur votre serveur StoreFront lorsque vous tentez de mettre à niveau StoreFront vers la version 1906 à l'aide du metainstaller Citrix Virtual Apps and Desktops 7 1906, la mise à niveau échoue. StoreFront est mis à niveau par le programme d'installation autonome de StoreFront 1906, mais StoreFront 1906 n'est pas ajouté à la liste Ajout/Suppression de programmes Windows. [WSP-4895]
- La personnalisation pour tronquer les noms d'applications longs ne fonctionne plus dans l'interface utilisateur X1.1 Purple. [WSP-4899]
- Les mises à niveau qui incluent 2.6, 3.0.1, 3.5 et 3.8 dans leur historique de mise à niveau vers 3.12 CU* et versions ultérieures peuvent échouer si le service KCD est en état Arrêté. [WSP-5160]
- La page `http://downloadplugins.citrix.com` a été mise à jour pour mettre à disposition l'application Citrix Workspace au lieu des composants Citrix Receiver qui sont en fin de vie. [WSP-5303]

Problèmes connus

January 8, 2020

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]
- 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 contourner ce problème, cliquez sur Connecter pour chaque application déconnectée. [DNA-25140, DNA-22561]
- Lorsque StoreFront est installé sur Windows Server 2012 R2, il peut ne pas s'inscrire auprès du service Citrix Analytics (CAS). Cela se produit lorsque les composants logiciels C++ Runtime ne sont pas déjà installés. Le programme d'installation autonome StoreFront n'installe pas ces composants. Une simple solution consiste à installer C++ Runtime avant ou après l'installation de StoreFront. [WSP-4412]

Avis de tiers

January 8, 2020

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

Avis de tiers StoreFront (PDF)

Configuration système requise

January 30, 2020

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 version actuelle (Current Release) à partir d'une version plus ancienne qui est maintenant en fin de vie n'est pas prise en charge. Pour plus d'informations, consultez 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. Les groupes de serveurs StoreFront peuvent contenir un maximum de six serveurs. Cependant, 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. Idéalement, tous les serveurs d'un groupe de serveurs doivent résider au même

emplacement (centre de données, zone de disponibilité), mais les groupes de serveurs peuvent couvrir des emplacements dans la même région à condition que les liens entre les serveurs du groupe répondent aux critères minimaux de latence. Voir Capacité à monter en charge.

Avant de pouvoir installer StoreFront, Windows PowerShell (version 4.0 ou ultérieure) et Microsoft Management Console (version 3.0 ou ultérieure) doivent être installés sur le serveur Web. Il s'agit des deux composants par défaut de Windows Server.

Le programme d'installation StoreFront vérifie que les composants requis suivants sont installés et activés avant d'installer StoreFront. Par défaut, ces composants requis sont fournis en tant que packages de fonctionnalités par le système d'exploitation. Si le programme d'installation StoreFront détecte que l'un de ces composants requis est absent ou désactivé, ils sont automatiquement installés et activés :

- Microsoft .NET Framework (version 4.5.1 ou ultérieure)
- Microsoft ASP.NET (version 4.5 ou ultérieure)
- Microsoft Visual C++ VC141 x64 Runtime
- Microsoft Internet Information Services (IIS)

  IIS est ajouté par le rôle « Windows Server » du serveur Web, sa version dépendant du système d'exploitation choisi. Pour référence, le programme d'installation StoreFront ajoute les rôles IIS suivants :

  - 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

  Le chemin d'accès relatif à StoreFront dans IIS doit être identique sur tous les serveurs d'un groupe de serveurs.

StoreFront utilise les ports suivants pour la communication. 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 donc être accessible.
- 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 de Citrix Receiver et de l'application Citrix Workspace 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.

Stockage des données d'abonnement à l'aide de Microsoft SQL Server

Vous pouvez éventuellement stocker les données d'abonnement à l'aide de Microsoft SQL Server. StoreFront prend en charge les mêmes versions de Microsoft SQL Server que Citrix Virtual Apps and Desktops pour les bases de données. Dans la configuration système requise pour Citrix Virtual Apps and Desktops, reportez-vous à la section Bases de données.

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 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp et XenDesktop 7.15 LTSR *
- XenApp et XenDesktop 7.6 LTSR *

* Pour plus d'informations sur l'utilisation de cette version actuelle (CR) dans un environnement Long Term Service (LTSR) et d'autres questions fréquemment posées, consultez article du Centre de connaissances Citrix.

Configuration requise pour Citrix Gateway

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

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Configuration requise pour l'application Citrix Workspace pour HTML5

Pour autoriser les utilisateurs à accéder aux bureaux et applications à l'aide de l'application Citrix Workspace pour 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 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp et XenDesktop 7.15 LTSR
- XenApp et XenDesktop 7.6 LTSR

> **Remarque :**
>
> L'application Citrix Workspace pour HTML5 lance uniquement des bureaux et des applications à l'aide de connexions réseau internes lorsque des connexions sécurisées aux VDA hébergeant ces ressources ont été configurées. Vous ne pouvez pas utiliser de connexions HTTP aux VDA qui hébergent les applications et les bureaux.

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 et NetScaler Gateway.

- Citrix Gateway 13.0

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

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 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp et XenDesktop 7.15 LTSR
- 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 de PC exécutant Citrix Desktop Lock, ainsi que les clients Citrix plus anciens qui ne peuvent pas être mis à niveau, doivent se connecter via l'adresse URL XenApp Services du magasin.

Pour fournir aux utilisateurs des séquences Microsoft Application Virtualization (App-V), une version compatible de Microsoft Application Virtualization Desktop Client est également requise. Pour de plus amples informations, consultez 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.

Utiliser l'application Citrix Workspace pour accéder aux magasins StoreFront

Vous pouvez utiliser toutes les versions de l'application Citrix Workspace prises en charge pour accéder aux magasins StoreFront à partir de connexions au réseau interne et via Citrix Gateway. Pour plus d'informations sur l'application Citrix Workspace et les dates de cycle de vie de Citrix Receiver, consultez la page https://www.citrix.com/support/product-lifecycle/milestones/receiver.html.

Vous pouvez vous connecter aux magasins StoreFront via Citrix Gateway à l'aide de Citrix Gateway Plug-in, du proxy ICA ou du VPN sans client (cVPN). Voir Expérience utilisateur unifiée.

Accéder aux magasins via les sites Citrix Receiver pour Web

Pour accéder aux sites Citrix Receiver pour Web à partir de connexions au réseau internes et via Citrix Gateway, utilisez la dernière version des navigateurs suivants :

Sous Windows

- Internet Explorer 11
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Sous Mac

- Safari
- Google Chrome
- Mozilla Firefox

Sous Linux

- Google Chrome
- Mozilla Firefox

Les connexions établies via Citrix Gateway peuvent être effectuées à l'aide de Citrix Gateway Plug-in, du proxy ICA ou du VPN sans client (cVPN). En outre, des versions spécifiques de Citrix Gateway sont requises pour autoriser les connexions extérieures au réseau d'entreprise. Pour de plus amples informations, consultez la section Configuration requise pour l'infrastructure.

Lancer des ressources via les sites Citrix Receiver pour Web

Les sites Citrix Receiver pour Web prennent en charge les lancements via une application Citrix Workspace installée en mode natif ou via l'application Citrix Workspace pour HTML5. Tous les navigateurs répertoriés ci-dessus sont conformes à HTML5 et prennent en charge les lancements de ressources HTML5. Selon votre configuration Receiver pour Web, les utilisateurs peuvent basculer entre les deux méthodes de lancement.

Accéder aux magasins via les adresses URL XenApp Services

Vous pouvez utiliser les adresses URL XenApp Services pour accéder aux magasins StoreFront avec des fonctionnalités réduites. Les adresses URL XenApp Services fournissent une prise en charge d'anciennes versions rétrocompatible pour les connexions établies par Citrix Receiver 3.4 Enterprise et les clients plus anciens qui ne prennent en charge que les connexions via PNAgent. Les connexions établies via Citrix Gateway, lorsqu'elles sont prises en charge, peuvent être effectuées à l'aide de Citrix 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 ou 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 la page http://www.citrix.com/ready.

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 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Configuration requise pour Citrix Analytics Service

Vous pouvez configurer Citrix StoreFront afin que l'application Citrix Workspace puisse envoyer des données à Citrix Analytics Service. Les détails de configuration sont décrits dans la section Citrix Analytics Service. Cette fonctionnalité est prise en charge pour les scénarios suivants :

- Magasins accessibles à partir des sites Citrix Receiver pour Web dans des navigateurs compatibles HTML5. Les données Citrix Analytics Service sont fournies lors du lancement de ressources à l'aide de l'application Citrix Workspace native ou HTML5.
- Magasins accessibles à partir de l'application Citrix Workspace 1903 pour Windows ou version ultérieure.
- Magasins accessibles à partir de l'application Citrix Workspace 1901 pour Linux ou version ultérieure.

Planifier votre déploiement StoreFront

January 8, 2020

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 Citrix Virtual Apps and Desktops pour offrir aux utilisateurs un point d'accès unique et en libre-service à leurs bureaux et applications.

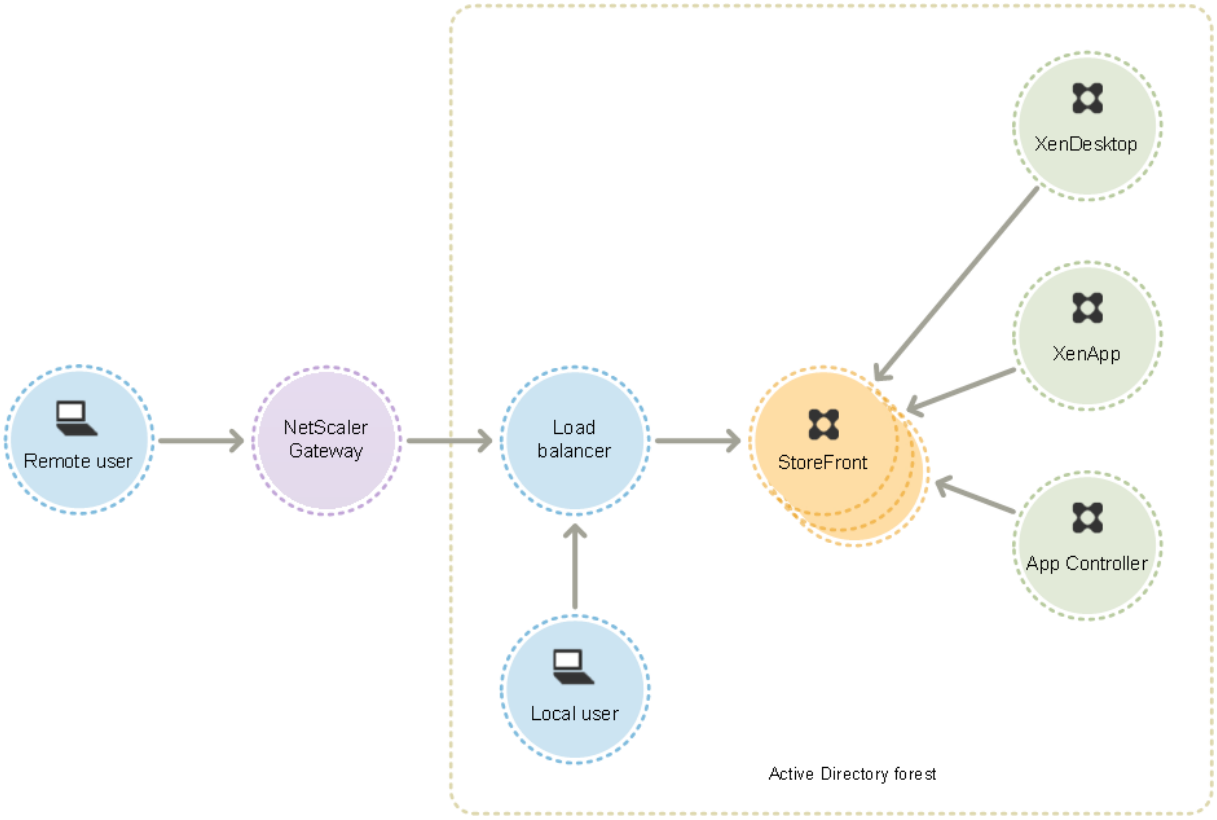
StoreFront comprend les composants principaux suivants :

- 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 de plus amples informations, consultez la section Authentification utilisateur.
- Les magasins énumèrent et regroupent les bureaux et les applications à partir de Citrix Virtual Apps and Desktops. Les utilisateurs accèdent aux magasins via l'application Citrix Workspace, des sites Citrix Receiver pour Web et des adresses URL XenApp Services. Pour de plus amples informations, consultez 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 supplé-

mentaire, 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 Citrix ADC 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 charge avec Citrix ADC, 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 Citrix Virtual Desktops et des batteries Citrix Virtual Apps 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 Citrix ADC.

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

Syntaxe :

```
Set-STFWebReceiverCommunication [-WebReceiverService] <
    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 :

```
$wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
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 Citrix Virtual Apps and Desktops. 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, Citrix Gateway est requis pour sécuriser les connexions des utilisateurs distants. Déployez Citrix Gateway en dehors du réseau de l'entreprise, avec des pare-feu séparant Citrix Gateway des réseaux internes et publics. Assurez-vous que Citrix 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 de l'application Citrix Workspace 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 Citrix Receiver pour Web, lors de l'utilisation de l'application Citrix Workspace, 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 :**
>
> Les déploiements de groupes de serveurs StoreFront ne sont pris en charge que lorsque les liens entre les serveurs d'un groupe de serveurs ont une latence inférieure à 40 ms (avec les abonnements désactivés) ou inférieure à 3 ms (avec les abonnements activés). Idéalement, tous les serveurs d'un groupe de serveurs doivent résider au même emplacement (centre de données, zone de disponibilité), mais les groupes de serveurs peuvent couvrir des emplacements dans la même région à condition que les liens entre les serveurs du groupe répondent à ces critères de latence, comme par exemple, les groupes de serveurs couvrant des zones de disponibilité au sein d'une région du cloud ou des centres de données de zone métropolitaine. Notez que la latence entre les zones varie selon le fournisseur de cloud. Citrix ne recommande pas d'étendre les emplacements en tant que configuration de récupération d'urgence, mais cette méthode peut convenir à une configuration haute disponibilité.
>
> Les groupes de serveurs StoreFront contenant diverses versions de système d'exploitation, différentes langues de système d'exploitation ou différentes configurations 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 plus d'informations sur la définition 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.

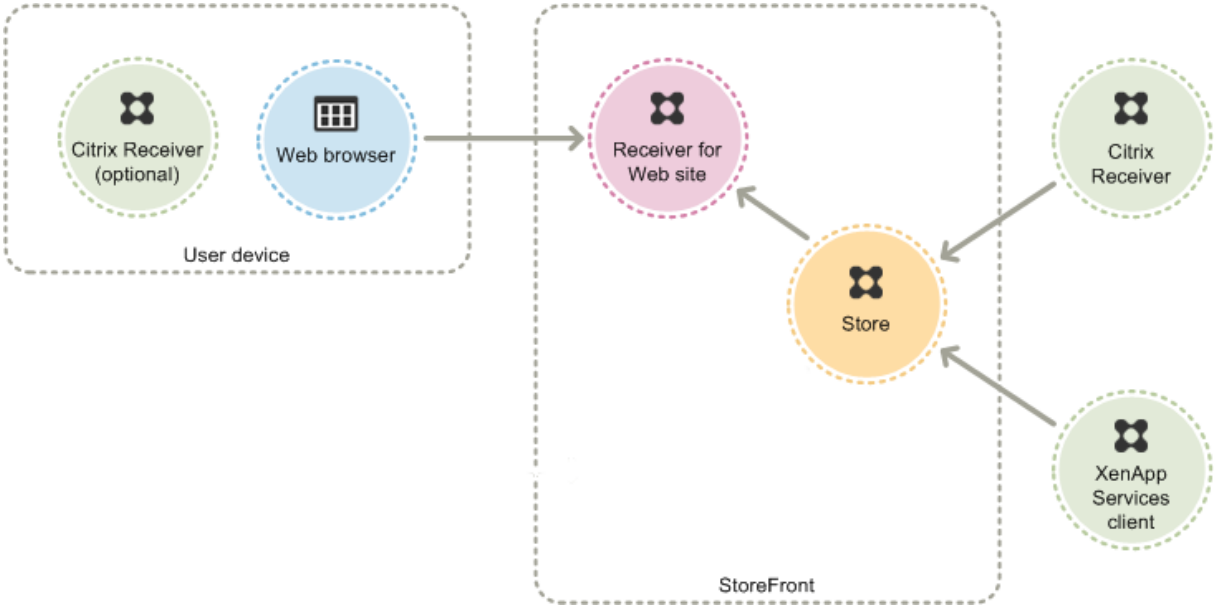
Options d'accès utilisateur

December 23, 2019

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

- Citrix Receiver ou application Citrix Workspace : les utilisateurs disposant de versions compatibles de Citrix Receiver ou de l'application Citrix Workspace peuvent accéder aux magasins StoreFront depuis l'interface utilisateur de Citrix Receiver ou de l'application Citrix Workspace. Cet accès 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 ou de l'application Citrix Workspace 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 ou l'application Citrix Workspace. Lorsque vous créez un magasin, un site Citrix Receiver pour Web est créé pour le magasin par défaut.
- Adresses URL XenApp Services : les utilisateurs équipés d'appliances 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 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 ou application Citrix Workspace

L'accès aux magasins à partir de l'interface utilisateur de Citrix Receiver ou de l'application Citrix Workspace offre la meilleure expérience utilisateur et davantage de fonctionnalités. Pour connaître les versions de Citrix Receiver ou de l'application Citrix Workspace qui peuvent être utilisées pour accéder aux magasins à l'aide de cette méthode, consultez la section Configuration système requise. Dans cet article, les mentions de « Application Citrix Workspace » représentent également les versions prises en charge de Citrix Receiver, sauf indication contraire.

L'application Citrix Workspace utilise des adresses URL internes et externes en tant que points balises. En prenant contact avec ces points balises, l'application Citrix Workspace 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 l'application Citrix Workspace. Cela permet à l'application Citrix Workspace de garantir que les utilisateurs ne sont pas invités à rouvrir une session lorsqu'ils accèdent à un bureau ou une application. Pour de plus amples informations, consultez la section Configurer des points balises.

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

> **Important :**
>
> Par défaut, l'application Citrix Workspace nécessite des connexions HTTPS aux 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 plus d'informations, consultez la section Configurer et installer à l'aide de paramètres de ligne de commande de la documentation de Citrix Receiver pour Windows ou de l'application Citrix Workspace 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 l'application Citrix Workspace, les utilisateurs ouvrent le fichier .cr pour configurer automatiquement des comptes pour les magasins. Par défaut, les sites Citrix Receiver pour Web offrent aux utilisateurs un fichier de provisioning destiné au magasin pour lequel le site est configuré. Vous pouvez demander à vos utilisateurs d'accéder aux sites Receiver pour Web des magasins auxquels ils souhaitent accéder et télécharger les fichiers de provisioning à partir de ces sites. Éventuellement, pour un niveau de contrôle plus élevé, vous pouvez utiliser la console de gestion Citrix StoreFront pour générer des fichiers de provisioning contenant les détails de connexion à un ou plusieurs magasins. Vous pouvez distribuer ces fichiers après des utilisateurs appropriés. Pour de plus amples informations, consultez la section Exporter des fichiers de provisioning de magasin pour des utilisateurs.

Adresses URL de configuration générées automatiquement

Pour les utilisateurs exécutant Mac OS, vous pouvez utiliser le générateur d'adresse URL de configuration de Citrix Receiver pour Mac ou de l'application Citrix Workspace pour Mac pour créer une adresse URL contenant les détails de connexion d'un magasin. Après l'installation de l'application Citrix Workspace, 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 avancés peuvent créer des comptes en entrant les adresses URL de magasin dans l'application Citrix Workspace. Pour plus d'informations, consultez la documentation de l'application Citrix Workspace.

Découverte de compte basée sur une adresse e-mail

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

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 l'application Citrix Workspace sur un appareil pour la première fois de configurer leurs comptes en entrant leurs adresses e-mail. S'ils téléchargent l'application Citrix Workspace à partir du site Web Citrix ou d'une page de téléchargement de l'application Citrix Workspace hébergée ai sein de votre réseau interne, les utilisateurs n'ont pas besoin de connaître les détails d'accès de leurs magasins lorsqu'ils installent et configurent l'application Citrix Workspace. La découverte de compte basée sur une adresse e-mail est disponible si l'application Citrix Workspace est téléchargée 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, l'application Citrix Workspace invite les utilisateurs à entrer une adresse e-mail ou l'adresse URL d'un magasin. Lorsqu'un utilisateur entre une adresse e-mail, l'application Citrix Workspace 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 l'application Citrix Workspace 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 Citrix 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, l'application Citrix Workspace recherche une machine appelée « discoverReceiver » afin d'identifier un serveur StoreFront.

Vous devez installer un certificat de serveur valide sur l'appliance Citrix 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 messagerie de vos utilisateurs peuvent également être utilisés, mais les utilisateurs apercevront une boîte de dialogue d'avertissement de certificat lorsque l'application Citrix Workspace 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)

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 Citrix Gateway avec les détails de connexion à StoreFront. Pour de plus amples 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 appliance Citrix 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 Citrix 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 Citrix Gateway.

7. Si vous avez configuré un enregistrement SRV pour votre appliance Citrix Gateway, ajoutez les détails de connexion StoreFront à Citrix 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 l'application Citrix Workspace pour accéder à leurs bureaux et applications. Pour de plus amples informations sur les combinaisons application Citrix Workspace 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 l'application Citrix Workspace est installée sur la machine de l'utilisateur. Si l'application Citrix Workspace ne peut être détectée, l'utilisateur est invité à télécharger et à installer la version appropriée 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 l'application Citrix Workspace 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 ou de l'application Citrix Workspace pour Windows et de Citrix Receiver pour Mac ou de l'application Citrix Workspace pour Mac, consultez la section Configurer des sites Citrix Receiver pour Web.

Application Citrix Workspace pour HTML5

L'application Citrix Workspace pour HTML5 est un composant de StoreFront qui est intégré par défaut aux sites Citrix Receiver pour Web. Vous pouvez activer l'application Citrix Workspace pour HTML5 sur vos sites Citrix Receiver pour Web afin que les utilisateurs qui ne peuvent pas installer l'application Citrix Workspace puissent quand même accéder à leurs ressources. Avec l'application Citrix Workspace pour HTML5, les utilisateurs peuvent accéder directement aux bureaux et aux applications dans des navigateurs Web compatibles HTML5 sans avoir besoin d'installer l'application

Citrix Workspace. Lorsqu'un site est créé, l'application Citrix Workspace pour HTML5 est désactivée par défaut. Pour plus d'informations sur l'activation de l'application Citrix Workspace pour HTML5, consultez citrix-receiver-download-page-template.html.

Pour accéder à leurs bureaux et applications à l'aide de l'application Citrix Workspace 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 l'application Citrix Workspace pour HTML5, consultez la section Configuration requise pour la machine utilisateur.

L'application Citrix Workspace pour HTML5 peut être utilisée par les utilisateurs sur le réseau interne et les utilisateurs distants se connectant via Citrix Gateway. Pour les connexions depuis le réseau interne, l'application Citrix Workspace 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 Citrix Gateway peuvent accéder aux ressources fournies par une large gamme de produits si vous choisissez l'application Citrix Workspace pour HTML5 comme option lors de la configuration de StoreFront. Des versions spécifiques de Citrix Gateway sont requises pour l'utilisation avec l'application Citrix Workspace pour HTML5. Pour de plus amples informations, consultez la section Configuration requise pour l'infrastructure.

Pour les utilisateurs du réseau interne, l'accès via l'application Citrix Workspace pour HTML5 aux ressources fournies par Citrix Virtual Apps and Desktops est désactivé par défaut. Pour activer l'accès local aux bureaux et applications à l'aide de l'application Citrix Workspace pour HTML5, vous devez activer la stratégie Connexions WebSockets ICA sur vos serveurs Citrix Virtual Apps and Desktops. Assurez-vous que vos pare-feu et autres périphériques réseau autorisent l'accès au port de l'application Citrix Workspace pour HTML5 spécifié dans la stratégie. Pour de plus amples informations, consultez la section Paramètres de stratégie WebSockets.

Par défaut, l'application Citrix Workspace 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 l'application Citrix Workspace 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 l'application Citrix Workspace 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 l'application Citrix Workspace 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 l'application Citrix Workspace ou être en mesure d'utiliser l'application Citrix Workspace 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 l'application Citrix Workspace peut être détectée sur les machines des utilisateurs et si un navigateur compatible HTML5 est utilisé. Pour des raisons de sécurité, les utilisateurs d'Internet Explorer peuvent être invités à confirmer qu'ils souhaitent démarrer les ressources accessibles via les raccourcis. Demandez à vos utilisateurs d'ajouter le site Receiver pour Web à la zone Intranet local ou Sites de confiance dans Internet Explorer pour éviter cette étape supplémentaire. Par défaut, le contrôle de l'espace de travail et le démarrage automatique des bureaux sont désactivés lorsque les utilisateurs accèdent à des sites Citrix Receiver pour Web via les raccourcis.

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

Pour créer des raccourcis d'application, configurez StoreFront avec les adresses URL des sites Web internes qui hébergeront les raccourcis. Lorsqu'un utilisateur clique sur un raccourci d'application sur un site Web, StoreFront compare le site Web avec la liste des adresses URL que vous avez entrées pour s'assurer que la demande provient d'un site Web approuvé. Toutefois, pour les utilisateurs se connectant via Citrix 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 Citrix Gateway afin de restreindre l'accès des utilisateurs uniquement à ces sites spécifiques. Pour de plus amples informations, consultez la section 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 des nombreuses fonctionnalités disponibles avec l'accès aux magasins via l'application Citrix Workspace, 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 Citrix 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.
- L'application Citrix Workspace pour HTML5 peut être utilisée 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 Citrix Gateway.
- Pour utiliser l'application Citrix Workspace pour HTML5 avec Mozilla Firefox via des connexions HTTPS, les utilisateurs doivent saisir `about:config` dans la barre d'adresses de Firefox et définir la préférence `network.websocket.allowInsecureFromHTTPS` sur true.

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 d'appliances 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 l'application Citrix Workspace 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 ou l'application Citrix Workspace 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 postes de travail à l'aide de cartes de proximité et sont rapidement connectés aux bureaux et applications fournis par Citrix Virtual Apps and Desktops. Pour de plus amples 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 applications Citrix Workspace 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 l'application Citrix Workspace 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 de plus amples 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 Citrix Virtual Apps and Desktops fournissant

des bureaux et des applications au magasin, en contournant le service d'authentification de StoreFront.

Authentification utilisateur

December 23, 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 entrent 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 Citrix Gateway pour accéder à Citrix Receiver pour Web, Citrix 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 Citrix Gateway prend fin et l'utilisateur doit de nouveau ouvrir une session. Les utilisateurs de Citrix Receiver pour Linux ou de l'application Citrix Workspace 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 Citrix Gateway.

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, veuillez consulter Déploiement AD FS 2016 Microsoft et Opérations AD FS 2016 Microsoft.
  - Microsoft ADFS v3.0 (Windows Server 2012 R2)
  - Citrix Gateway (configurée en tant qu'IdP)
- Configurez l'authentification SAML dans StoreFront à l'aide de la console de gestion StoreFront dans un nouveau déploiement (voir la section Créer un nouveau déploiement) ou dans un déploiement existant (voir 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 (4.6 et versions supérieures), l'application Citrix Workspace pour Windows ou Citrix Receiver pour Web.

L'utilisation de l'authentification SAML avec Citrix Gateway 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 l'application Citrix Workspace et des adresses URL XenApp Services. Les sites Citrix Receiver pour Web prennent en charge l'authentification pass-through pour Internet Explorer, Microsoft Edge, Mozilla Firefox et Google Chrome sur les machines client Windows appartenant à un domaine.

Pour activer l'authentification pass-through au domaine

1. Installez Citrix Receiver pour Windows, l'application Citrix Workspace pour Windows ou Citrix 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 ou l'application Citrix Workspace pour Windows, comme indiqué dans la section Configurer l'authentification pass-through au domaine. L'application Citrix Workspace 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 Microsoft 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 ou de l'application Citrix Workspace pour Windows.

   > Avertissement :
   >
   > 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) Cliquez deux fois sur « network.automatic-ntlm-auth.trusted-uris » et tapez l'URL du site Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Windows dans le menu contextuel.
   d) Cliquez sur **OK**.

Authentification pass-through via Citrix Gateway

Les utilisateurs s'authentifient sur Citrix Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. L'authentification pass-through via Citrix Gateway est activée par défaut lorsque vous configurez l'accès distant à un magasin pour la première fois. Les utilisateurs peuvent se connecter via Citrix Gateway aux magasins via l'application Citrix Workspace ou des sites Citrix Receiver pour Web. Pour plus d'informations sur la configuration de StoreFront pour Citrix Gateway, consultez la section Ajouter une connexion Citrix Gateway.

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

- **Jeton de sécurité.** Les utilisateurs se connectent à Citrix 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 Citrix Gateway sont invités à entrer leurs informations d'identification de domaine et codes d'accès de jeton de sécurité.
- **Certificat client.** Les utilisateurs ouvrent une session sur Citrix Gateway et sont authentifiés en fonction des attributs du certificat client présenté à Citrix Gateway. Configurez l'authentification du certificat client pour permettre aux utilisateurs d'ouvrir une session sur Citrix 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 Citrix Gateway pour fournir une authentification pass-through aux utilisateurs distants, afin qu'ils n'aient besoin de saisir leurs informations d'identification qu'une seule fois. Toutefois, par défaut, l'authentification pass-through est activée uniquement pour les utilisateurs ouvrant une session sur Citrix Gateway avec un mot de passe. Pour configurer l'authentification pass-through via Citrix Gateway à StoreFront pour les utilisateurs de carte à puce, déléguez la validation des informations d'identification à Citrix Gateway. Pour de plus amples informations, consultez la section Créer et configurer le service d'authentification.

Les utilisateurs peuvent se connecter aux magasins dans l'application Citrix Workspace avec l'authentification pass-through via un tunnel VPN SSL à l'aide de Citrix Gateway Plug-in. Les utilisateurs distants qui ne peuvent pas installer Citrix Gateway Plug-in peuvent utiliser un accès sans client pour se connecter aux magasins dans l'application Citrix Workspace 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 l'application Citrix Workspace 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 Citrix Gateway pour agir en tant que proxy distant sécurisé. Les utilisateurs ouvrent une session sur Citrix 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 Citrix Gateway Plug-in.

Si vous configurez une authentification double à Citrix Gateway pour les utilisateurs distants qui accèdent à des magasins dans l'application Citrix Workspace, vous devez créer deux stratégies d'authentification sur Citrix 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 l'appliance Citrix Gateway à votre configuration StoreFront, définissez le type de connexion sur Domaine et jeton de sécurité.

Pour de plus amples informations, consultez http://support.citrix.com/article/CTX125364

Pour activer l'authentification multi-domaines via Citrix Gateway vers StoreFront, définissez l'attribut de nom SSO sur userPrincipalName dans la stratégie d'authentification LDAP Citrix Gateway pour chaque domaine. Vous pouvez demander aux utilisateurs de spécifier un domaine sur la page d'ouverture de session de Citrix Gateway de façon à ce que la stratégie LDAP appropriée à utiliser puisse être déterminée. Lorsque vous configurez les profils de session Citrix 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 Citrix Gateway, vous pouvez utiliser SmartAccess pour contrôler l'accès utilisateur aux ressources Citrix Virtual Apps and Desktops sur la base de stratégies de session Citrix Gateway. Pour plus d'informations sur SmartAccess, consultez l'article How SmartAccess works for Citrix Virtual Apps and Desktops.

Cartes à puce

Les utilisateurs s'authentifient 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 l'application Citrix Workspace, Citrix Receiver pour Web 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 Citrix Virtual Apps and Desktops. 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.

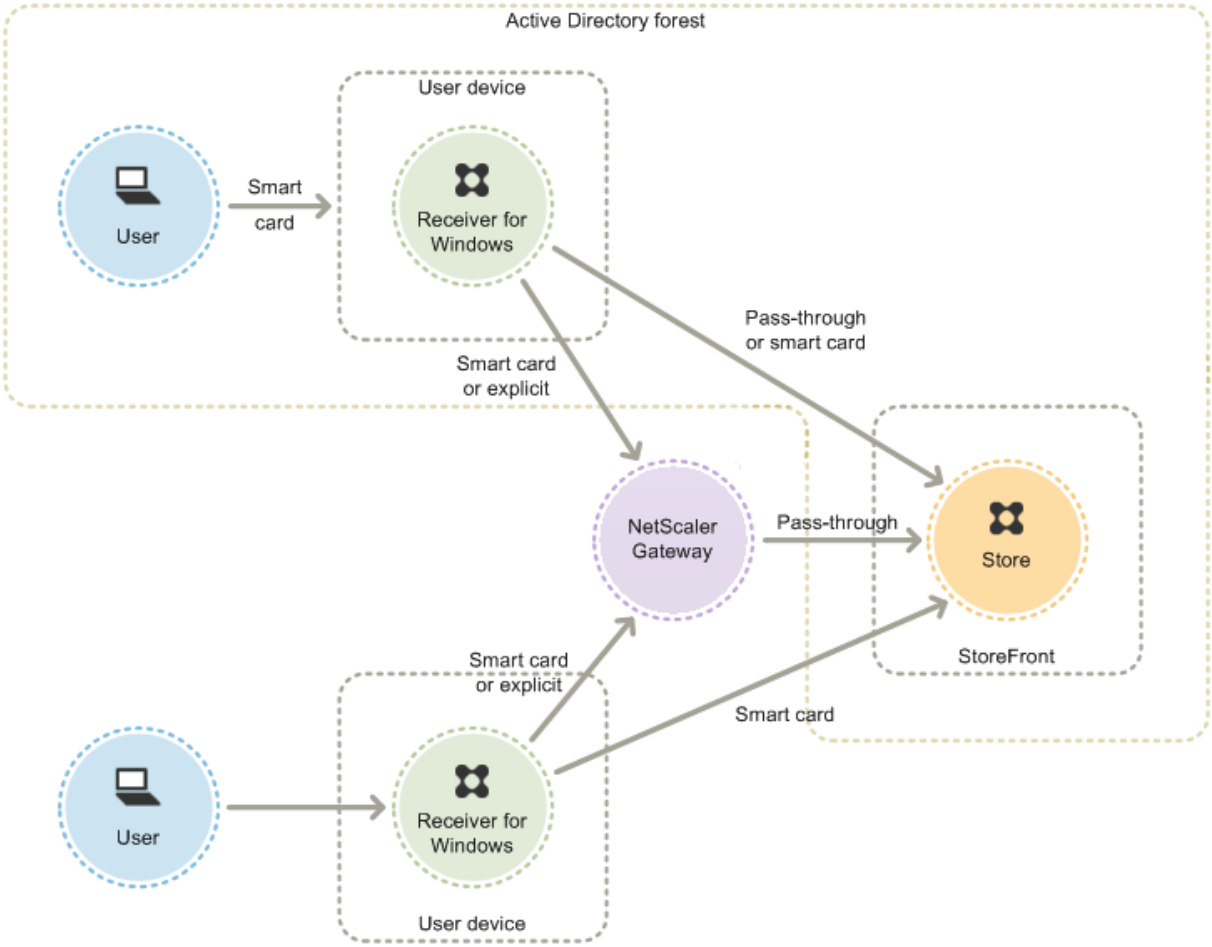
Pour activer l'authentification par carte à puce, les comptes des utilisateurs doivent être configurés au sein du domaine Microsoft Active Directory contenant les serveurs StoreFront ou au sein d'un domaine doté d'une relation d'approbation bidirectionnelle directe avec le domaine du serveur StoreFront.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

Les utilisateurs équipés de machines exécutant Citrix Receiver pour Windows ou l'application Citrix Workspace pour Windows peuvent s'authentifier à l'aide de cartes à puce, soit directement, soit via Citrix 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 ou l'application Citrix Workspace 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 ou l'application Citrix Workspace 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 ou de l'application Citrix Workspace 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 ou sur l'application Citrix Workspace 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 Citrix 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 Citrix Gateway à StoreFront et déléguer la validation des informations d'identification à Citrix Gateway. Créez ensuite un serveur virtuel Citrix 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 ou l'application Citrix Workspace pour Windows pour l'authentification pass-through.

> **Remarque :**
>
> Si vous utilisez Citrix Receiver pour Windows ou l'application Citrix Workspace pour Windows, 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.

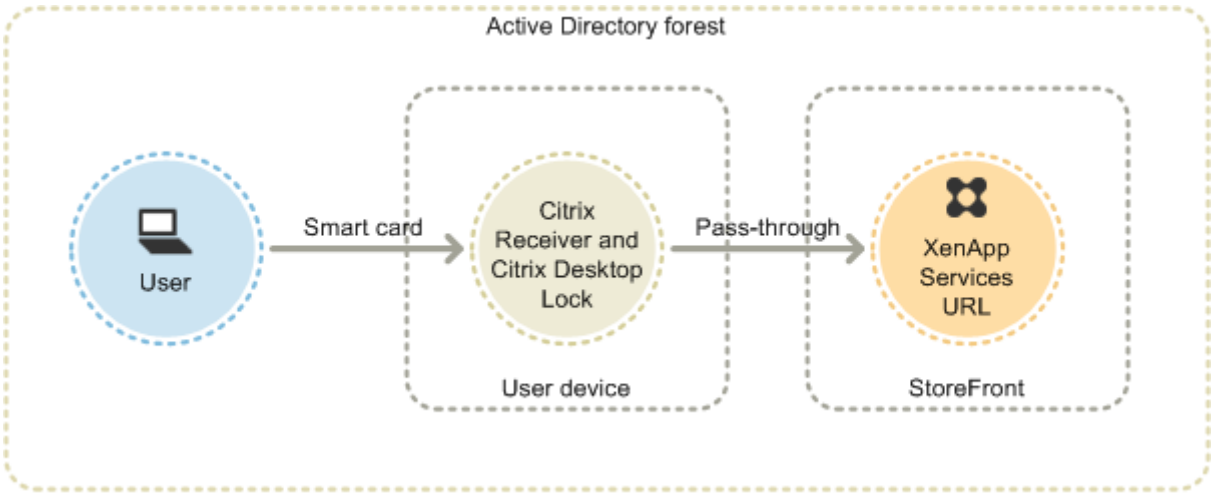
Les utilisateurs peuvent ouvrir une session sur Citrix Gateway à l'aide de leurs cartes à puce et codes PIN, ou avec des informations d'identification explicites. Cela vous permet de fournir aux utilisateurs la possibilité de revenir à l'authentification explicite pour les ouvertures de session Citrix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

Les utilisateurs de PC 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.

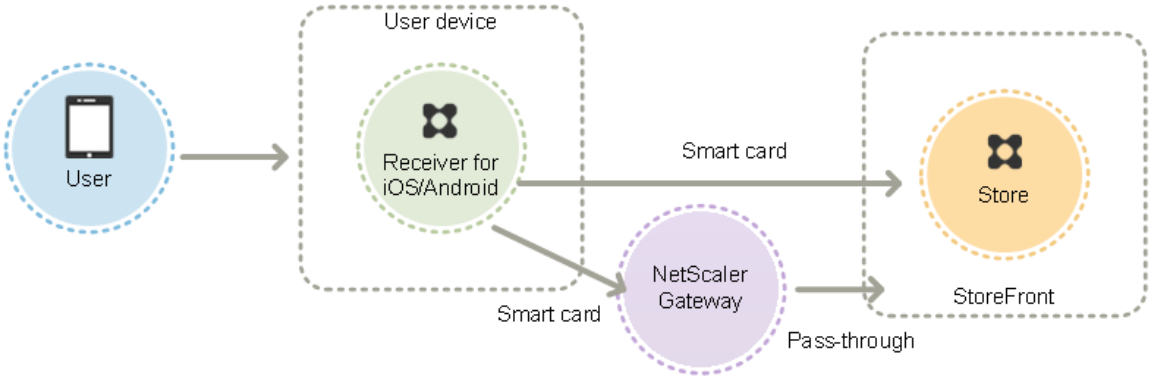
Si vous activez l'authentification pass-through avec carte à puce à Citrix Virtual Apps and Desktops pour les utilisateurs de Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Win-

dows équipés de machines appartenant à un domaine qui n'accèdent pas aux magasins via Citrix 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 Citrix Virtual Apps and Desktops pour les utilisateurs de Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Windows équipés de machines appartenant à un domaine qui accèdent aux magasins via Citrix 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 l'application Citrix Workspace pour iOS et Android

Les utilisateurs équipés de machines exécutant l'application Citrix Workspace pour iOS et Android peuvent s'authentifier à l'aide de cartes à puce, soit directement, soit via Citrix 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 applications Citrix Workspace, 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 Citrix 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 Citrix Gateway à StoreFront et déléguer la validation des informations d'identification à Citrix Gateway. Créez ensuite un serveur virtuel Citrix Gateway supplémentaire par le biais duquel router les connexions utilisateur vers les ressources.

Les utilisateurs peuvent ouvrir une session sur Citrix 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 Citrix Gateway à StoreFront et déléguez la validation des informations d'identification à Citrix 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 ou l'application Citrix Workspace pour Linux

Les utilisateurs équipés de machines exécutant Citrix Receiver pour Linux ou l'application Citrix Workspace 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 ou l'application Citrix Workspace 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 ou l'application Citrix Workspace pour Windows. Consultez la section Configuration de l'authentification par carte à puce et pour obtenir des instructions sur l'utilisation des cartes à puce, consultez la section 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 ou l'application Citrix Workspace 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 ou l'application Citrix Workspace 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 Citrix Gateway doivent ouvrir une session à l'aide de leurs cartes à puce et codes PIN aux 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 pas sont 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 Citrix Gateway à StoreFront et déléguer la validation des informations d'identification à Citrix Gateway. Créez ensuite un serveur virtuel Citrix Gateway supplémentaire par le biais duquel router les connexions utilisateur vers les ressources.

Les utilisateurs peuvent ouvrir une session sur Citrix 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 Citrix Gateway. Configurez l'authentification pass-through via Citrix Gateway à StoreFront et déléguez la validation des informations d'identification à Citrix 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 ou pour l'application Citrix Workspace 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 l'application Citrix Workspace, 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 Virtual Apps and Desktops.
- 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 applications Citrix Workspace 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, consultez 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 Citrix Gateway Plug-in et ouvrir une session via une page Web à l'aide de leurs cartes à puce et codes PIN pour s'authentifier à chaque étape. L'authentification pass-through à StoreFront avec Citrix 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 Citrix Virtual Apps and Desktops pour les utilisateurs de Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Windows équipés de machines appartenant à un domaine qui n'accèdent pas aux magasins via Citrix 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 Citrix Virtual Apps and Desktops pour les utilisateurs de Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Windows équipés de machines appartenant à un domaine qui accèdent aux magasins via Citrix 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 Citrix 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

January 8, 2020

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, ainsi que 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, consultez 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 d'appareils Windows, le contrôle de l'espace de travail est uniquement activé si le site peut détecter que l'application Citrix Workspace est installée sur les appareils des utilisateurs ou si l'application Citrix Workspace pour HTML5 est utilisée 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 l'application Citrix Workspace 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 Citrix Virtual Apps and Desktops. L'association de type de fichier est activée par défaut pour les nouveaux magasins. Pour de plus amples informations, consultez 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.

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 de plus amples 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 Citrix Virtual Desktops, 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 l'application Citrix Workspace 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 Citrix Virtual Apps and Desktops, 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 un groupe de mise à disposition d'application.

- 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 Citrix Virtual Apps and Desktops apparaissent sous forme

de catégories dans l'application Citrix Workspace. 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 l'application Citrix Workspace.
- Vous pouvez spécifier pour chaque utilisateur un ensemble d'applications de base qui ne peuvent pas être supprimées de l'écran d'accueil de l'application Citrix Workspace 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 or Citrix Workspace app to all users automatically** lorsque vous configurez les paramètres de l'application.
- Pour publier des applications Citrix Virtual Apps and Desktops auprès des utilisateurs ou pour faciliter la recherche des applications fréquemment utilisées en les répertoriant dans la liste Sélection de l'application Citrix Workspace, 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 Citrix Virtual Apps and Desktops 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, l'application Citrix Workspace 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, l'application Citrix Workspace abonne l'utilisateur à l'application, mais ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application mise à disposition à partir de l'application Citrix Workspace, l'instance installée localement s'exécute à la place. Pour de plus amples informations, consultez la section Configuration de la mise à disposition d'applications.

- Dans Citrix Virtual Apps and Desktops, 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 disposition. 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 ou de l'application Citrix Workspace 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 de plus amples informations, consultez CTX232210, l'article Applications : dans la documentation Citrix Virtual Apps and Desktops et la documentation Citrix Receiver pour Windows.

Haute disponibilité et configuration multisite de StoreFront

August 28, 2019

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 Citrix Virtual Apps and Desktops qui mettent à disposition 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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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 de plus amples informations, consultez 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 Citrix Gateway optimal

Si vous avez configuré des appliances Citrix Gateway distinctes pour vos déploiements, StoreFront vous permet de définir l'appliance optimale 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'une appliance Citrix Gateway, les utilisateurs se connectant via une appliance 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 l'appliance à laquelle 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 l'appliance Citrix Gateway optimale pour chacun de vos déploiements. Avec cette configuration, les connexions utilisateur vers les ressources sont routées via l'appliance locale pour le déploiement fournissant les ressources, quel que soit l'emplacement de l'appliance par le biais duquel l'utilisateur accède au magasin.

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

Équilibrage de charge globale des serveurs Citrix Gateway

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

Pour plus d'informations sur l'équilibrage de charge, consultez la section Équilibrage de charge avec Citrix ADC.

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 l'application Citrix Workspace 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

January 30, 2020

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 Citrix Virtual Apps and Desktops 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 Citrix ADC pour l'équilibrage de charge, définissez un serveur virtuel pour remplacer vos serveurs StoreFront. Pour plus d'informations sur la configuration de Citrix ADC pour l'équilibrage de charge, consultez la section Équilibrage de charge avec Citrix ADC.

a) Assurez-vous que l'équilibrage de charge est activé sur votre appliance Citrix ADC.

b) Pour chaque serveur StoreFront, créez des services d'équilibrage de charge HTTP ou SSL 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 l'**adresse IP du client** ou de la méthode **Cookie Insert**. 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, l'application Citrix Workspace nécessite des connexions HTTPS aux magasins. Pour configurer IIS afin de pouvoir utiliser une adresse URL de base HTTPS dans StoreFront, créez une liaison HTTPS au site Web par défaut et associez-la au certificat de serveur StoreFront. Pour plus d'informations sur l'ajout de liaison HTTPS à un site IIS, consultez Sécuriser votre déploiement StoreFront.

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. 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 prérequis et les composants StoreFront sont répertoriés pour l'installation et cliquez sur **Installer**.

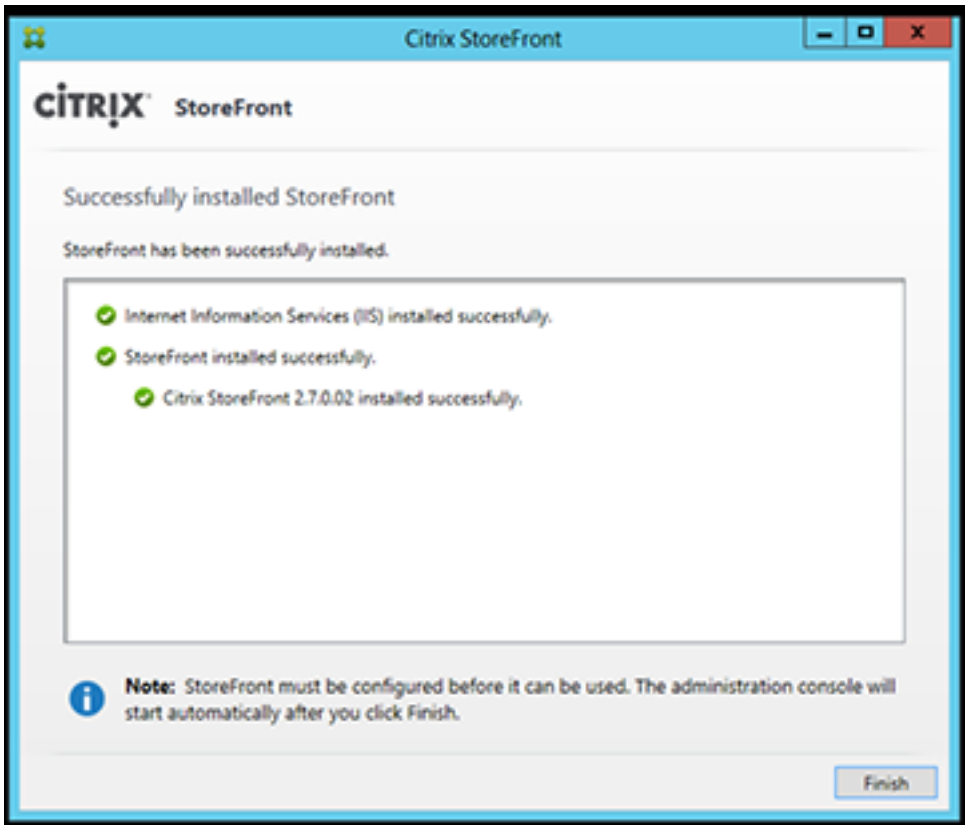
   Avant l'installation des composants, les rôles suivants sont activés s'ils ne sont pas déjà configurés sur le serveur.

   - 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**.

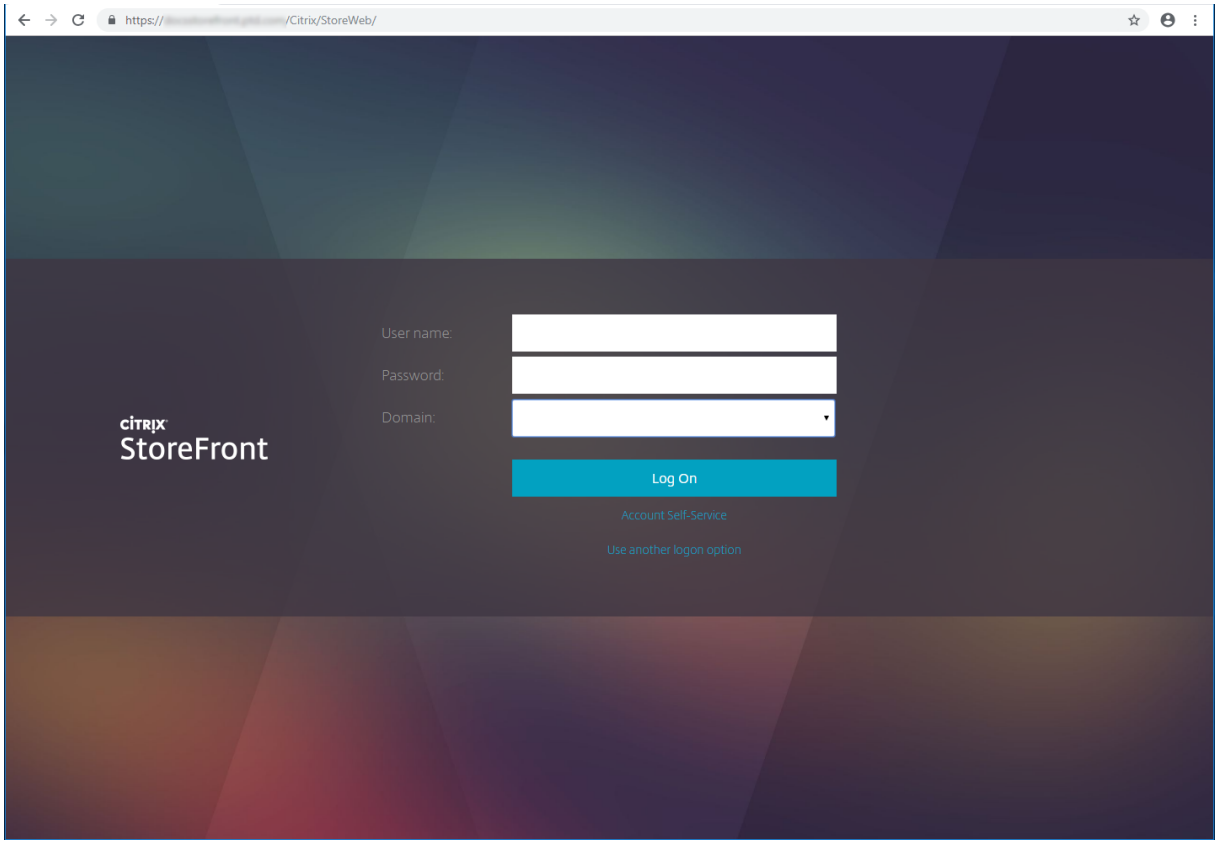
a) Spécifiez l'URL du serveur StoreFront dans la zone **URL de base**.
b) Sur la page **Nom du magasin**, spécifiez un nom pour votre magasin, puis cliquez sur **Suivant**.

Sur la page **Delivery Controller**, entrez les détails des déploiements Citrix Virtual Apps and Desktops qui fournissent les ressources que vous souhaitez mettre à disposition dans le magasin.

1. Définissez les champs **Type de transport** et **Port**, tels que HTTP et port 80, ou HTTPS et port 443, puis cliquez sur **OK**.
2. Sur la page **Accès distant**, sélectionnez Aucun. Si vous utilisez Citrix 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/StoreWeb/`. Ouvrez une session at accédez à la nouvelle interface utilisateur de l'application Citrix Workspace.



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. Consultez la section 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.

```
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. 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 l'application Citrix Workspace sur une machine Windows ou Mac OS X, l'utilisateur est invité à télécharger et installer la version appropriée de l'application Citrix Workspace 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 l'application Citrix Workspace à partir du serveur StoreFront plutôt que du site Web. Pour de plus amples 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 de Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Windows et de Citrix Receiver pour Mac ou de l'application Citrix Workspace pour Mac, respectivement, sur l'emplacement approprié de votre déploiement StoreFront. Remplacez *filelocation* par le répertoire contenant le fichier d'installation que vous voulez copier et *filename* par le nom du fichier d'installation. Les fichiers d'installation de Citrix Receiver pour Windows ou de l'application Citrix Workspace pour Windows et de Citrix Receiver pour Mac ou de l'application Citrix Workspace pour Mac sont inclus dans votre support d'installation Citrix Virtual Apps and Desktops.

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 l'Éditeur du Registre. 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) :

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Type: REG_DWORD
Value: 0 = disabled, 1 = enabled
```

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

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

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

> **Remarque :**
>
> Le paramètre de registre contrôle le chargement automatique des informations d'utilisation et des statistiques anonymes pour tous les composants sur le même serveur. Par exemple, si vous avez installé StoreFront sur le même serveur que le Delivery Controller et que vous décidez de ne pas prendre part au programme CEIP à l'aide du paramètre de Registre, ce choix s'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 »).
Paramètre HTML5 pour Citrix Receiver pour Web	Liste des chaînes indiquant le paramètre de Receiver pour HTML5 pour chaque site Receiver pour Web (« Always », « Fallback », or « Off »).
Contrôle de l'espace de travail activé pour l'application Citrix Workspace/Citrix Receiver	Liste des booléens indiquant si le « Contrôle de l'espace de travail » est activé pour chaque site Receiver pour Web (« True » ou « False »).
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 »).
Nombre de passerelles	Compteur du nombre de passerelles Citrix Gateway configurées dans le déploiement.

Citrix Analytics Service

Si vous êtes un client Citrix Cloud et que vous disposez d'un déploiement StoreFront local, vous pouvez configurer StoreFront de manière à ce que les données soient envoyées à Citrix Analytics Service dans Citrix Cloud. Une fois la configuration effectuée, l'application Citrix Workspace et les sites Citrix Receiver pour Web accessibles à partir de navigateurs compatibles HTML5 envoient des événements

relatifs à l'utilisateur à Citrix Analytics pour traitement. Citrix Analytics regroupe des mesures sur les utilisateurs, les applications, les points de terminaison, les réseaux et les données pour fournir des informations complètes sur le comportement des utilisateurs. Pour en savoir plus sur cette fonctionnalité, consultez la section Intégrer des sites Virtual Apps and Desktops à l'aide de StoreFront dans la documentation Citrix Analytics.

Pour configurer ce comportement, procédez comme suit :

- Téléchargez un fichier de configuration à partir de Citrix Analytics.
- Importez les données Citrix Analytics dans votre déploiement StoreFront local à l'aide de PowerShell.

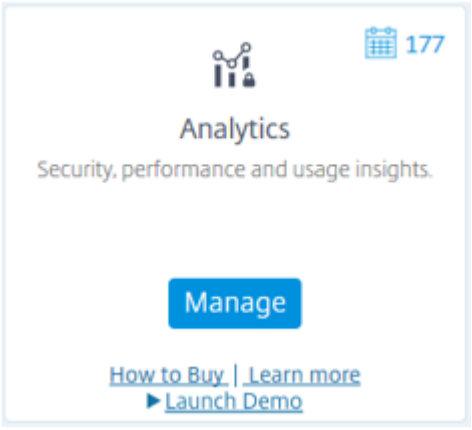
Une fois StoreFront configuré, l'application Citrix Workspace peut envoyer des données à partir des magasins StoreFront lorsque Citrix Analytics Service le demande.

> **Important :**
>
> Votre déploiement StoreFront doit pouvoir contacter les adresses suivantes sur le port 443 pour que cette fonctionnalité fonctionne correctement et utilise les services Citrix Cloud :
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

Télécharger le fichier de configuration à partir de Citrix Analytics

> **Important :**
>
> Un fichier de configuration contenant des informations sensibles est requis pour la configuration initiale. Conservez le fichier en toute sécurité après le téléchargement. Ne partagez pas ce fichier avec quiconque en dehors de votre organisation. Après la configuration, vous pouvez supprimer ce fichier. Si vous devez réappliquer la configuration sur une autre machine, vous pouvez télécharger à nouveau le fichier à partir de la console de gestion de Citrix Analytics Service.

1. Connectez-vous à Citrix Cloud (`https://citrix.cloud.com/`) à l'aide d'un compte d'administrateur.
2. Sélectionnez un client Citrix Cloud.
3. Cliquez sur **Gérer** pour ouvrir la console de gestion de Citrix Analytics Service.



4. Dans la console de gestion de Citrix Analytics Service, sélectionnez **Settings > Data Sources**.
5. Dans la carte Virtual Apps and Desktops, sélectionnez l'icône de menu (⋮), puis sélectionnez **Connect StoreFront deployment**.
6. Sur la page Connect StoreFront Deployment, sélectionnez **Download File** pour télécharger le fichier *StoreFrontConfigurationFile.json*.

Exemple de fichier de configuration

```
{

  "customerId": "<yourcloudcustomer>",
  "enablementService": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata",
  "cwsServiceKey": "PFJTPn …… .. T4=",
  "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/storefront/config",
  "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
  "name": "CASSingleTenant"
 }
```

où

customerId est l'ID unique du client Citrix Cloud actuel.

cwsServiceKey est une clé unique identifiant le compte client Citrix Cloud actuel.

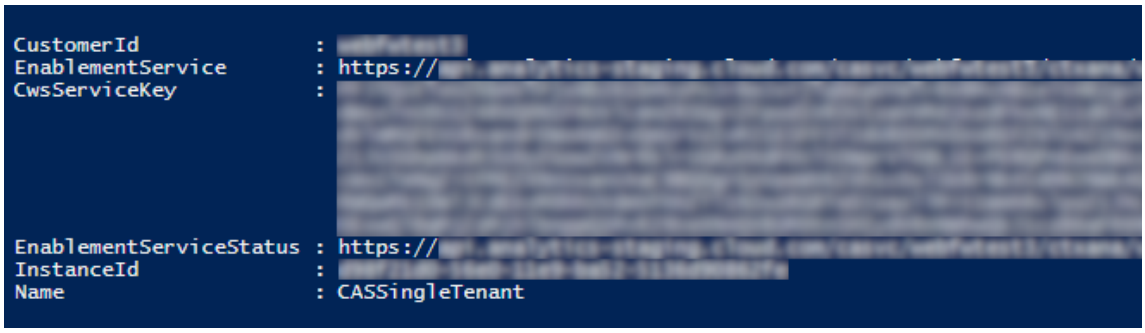
instanceID est un ID généré utilisé pour signer des requêtes (sécurisées) effectuées à partir de l'application Citrix Workspace vers Citrix Analytics. Si vous enregistrez plusieurs serveurs StoreFront ou groupes de serveurs avec Citrix Cloud, chacun possède un ID instanceID unique.

Importer les données Citrix Analytics dans votre déploiement StoreFront

1. Copiez le fichier *StoreFrontConfigurationFile.json* dans un dossier approprié sur le serveur StoreFront local (ou un serveur dans un groupe de serveurs StoreFront). Les commandes suivantes supposent que le fichier est enregistré sur le bureau.
2. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.
3. Exécutez les commandes suivantes :

```
1 Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
     StoreFrontConfigurationFile.json"
2 Get-STFCasConfiguration
```

4. Cette commande renvoie une copie des données importées et l'affiche dans la console PowerShell.



> **Remarque :**
>
> Les serveurs StoreFront locaux, qui sont installés sur Windows Server 2012 R2, peuvent nécessiter l'installation manuelle des composants logiciels C++ Runtime, afin qu'ils puissent s'inscrire auprès de CAS. Si StoreFront est installé lors de l'installation de Citrix Virtual Apps and Desktops, cette étape n'est pas requise, car le métainstaller CVAD installe déjà les composants C++ Runtime. Si StoreFront est installé en utilisant uniquement le métainstaller CitrixStoreFront-x64.exe sans C++ Runtime, il peut ne pas réussir à s'inscrire auprès de Citrix Cloud après l'importation du fichier de configuration CAS.

Propager les données Citrix Analytics vers un groupe de serveurs StoreFront

Si vous effectuez ces actions sur un groupe de serveurs StoreFront, vous devez propager les données Citrix Analytics importées à tous les membres du groupe de serveurs. Cette étape n'est pas nécessaire dans un déploiement de serveur StoreFront unique.

Pour propager les données, utilisez l'une des approches suivantes :

- Utilisez la console de gestion StoreFront.
- Utilisez l'applet de commande PowerShell **Publish-STFServerGroupConfiguration**.

Vérifier l'ID du groupe de serveurs StoreFront

Pour vérifier si votre déploiement s'est correctement enregistré auprès de Citrix Analytics Service, vous pouvez utiliser PowerShell pour afficher l'ID ServerGroupID de votre déploiement.

1. Connectez-vous à votre serveur StoreFront ou à un serveur StoreFront dans le groupe de serveurs.
2. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.
3. Exécutez les commandes suivantes :

```
$WebConfigPath = "C:\Program Files\Citrix\Receiver StoreFront\
    Framework\FrameworkData\Framework.xml"
$XMLObject = (Get-Content $WebConfigPath) -as [Xml]
$XMLObject.framework.properties.property
```

Par exemple, ces commandes génèrent une sortie comme suit :

```
name value
---- -----
ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
HostBaseUrl https://storefront.example.com/
SelectedIISWebSiteId 1
AdminConsoleOperationMode Full
```

Arrêter d'envoyer des données à Citrix Analytics à partir de StoreFront

1. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.
2. Exécutez les commandes suivantes :

```
Remove-STFCasConfiguration
```

```
Get-STFCasConfiguration
```

Get-STFCasConfiguration ne renvoie aucune valeur si les données Citrix Analytics précédemment importées ont été supprimées.

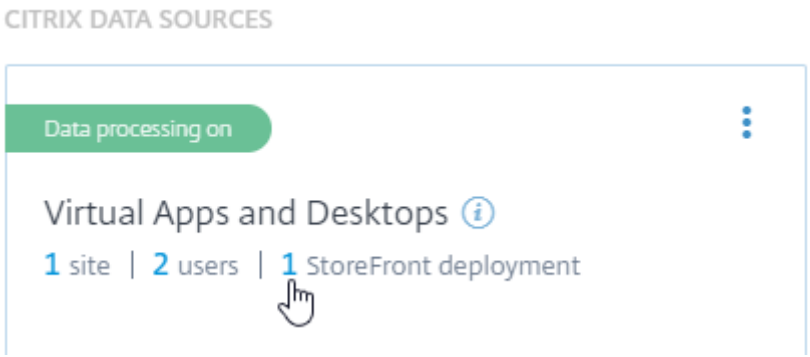
3. Si vous effectuez ces actions sur un groupe de serveurs StoreFront, propagez la modification et supprimez les données Citrix Analytics importées de tous les membres du groupe de serveurs. Sur un serveur du groupe de serveurs, exécutez la commande suivante :

```
Publish-STFServerGroupConfiguration
```

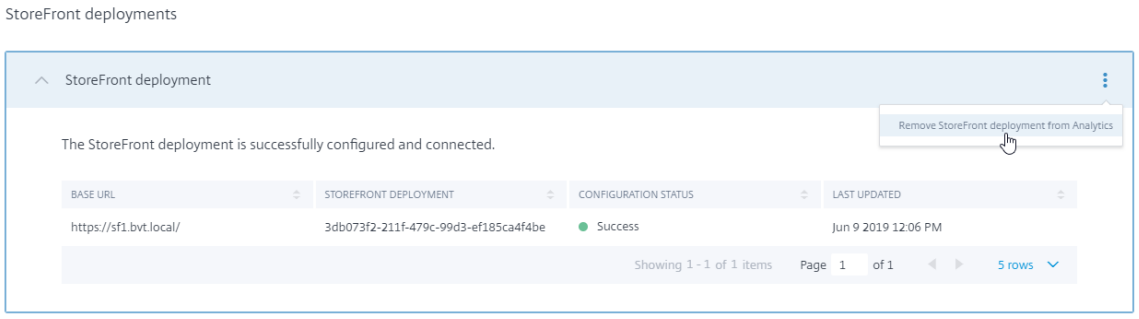
4. Sur tous les autres membres du groupe de serveurs, exécutez la commande suivante pour confirmer que la configuration de Citrix Analytics a bien été supprimée de tous les serveurs du groupe :


```
Get-STFCasConfiguration
```

5. Connectez-vous à Citrix Cloud (`https://citrix.cloud.com/`) à l'aide d'un compte d'administrateur.
6. Sélectionnez un client Citrix Cloud.
7. Cliquez sur **Gérer** pour ouvrir la console de gestion de Citrix Analytics Service.
8. Dans la console de gestion de Citrix Analytics Service, sélectionnez **Settings > Data Sources**.
9. Dans la carte Virtual App and Desktops, sélectionnez le nombre de StoreFront deployment :



10. Identifiez le déploiement StoreFront que vous souhaitez supprimer en faisant référence à son URL de base de l'hôte et son ID ServerGroupID.
11. Dans le menu (⋮), sélectionnez **Remove StoreFront deployment from Analytics**.



> **Remarque :**
>
> Si vous supprimez la configuration côté serveur, mais pas à partir de Citrix Analytics, l'entrée StoreFront deployment reste dans Citrix Analytics, mais ne reçoit aucune donnée de StoreFront. Si vous supprimez la configuration de Citrix Analytics uniquement, l'entrée StoreFront deployment est de nouveau ajoutée lors du prochain recyclage du pool d'applications (effectué lors d'une réinitialisation IIS ou automatiquement toutes les 24 heures).

Configurer StoreFront pour utiliser un proxy Web pour contacter Citrix Cloud et s'enregistrer auprès de Citrix Analytics

Si StoreFront est placé sur un serveur Web hôte derrière un proxy Web, l'enregistrement auprès de Citrix Analytics échoue. Si les administrateurs StoreFront utilisent un proxy HTTP dans leur déploiement Citrix, le trafic StoreFront lié à Internet doit passer par le proxy Web avant d'atteindre Citrix Analytics dans le cloud. StoreFront n'utilise pas automatiquement les paramètres proxy du système d'exploitation d'hébergement ; une configuration supplémentaire est requise pour demander au magasin d'envoyer le trafic sortant via le proxy Web. Vous pouvez définir une configuration de proxy `<system.net>` en ajoutant une nouvelle section au fichier web.config du magasin. Effectuez cette opération pour chaque magasin sur le serveur StoreFront qui est utilisé pour envoyer des données à Citrix Analytics.

Méthode 1 – Définir la configuration du proxy de magasin via Powershell pour un ou plusieurs magasins (recommandé)

L'exécution du script Powershell Config-StoreProxy.ps1 automatise ce processus pour un ou plusieurs magasins et insère automatiquement le fichier XML valide pour configurer `<system.net>`. Le script sauvegarde également le fichier web.config store sur le bureau de l'utilisateur actuel, ce qui permet de restaurer le fichier web.config non modifié si nécessaire.

> **Remarque :**
>
> L'exécution répétée du script peut entraîner l'ajout de plusieurs copies du fichier XML `<system.net>`. Chaque magasin ne devrait avoir qu'une seule entrée pour `<system.net>`. L'ajout de plusieurs copies empêche la configuration du proxy de magasin de fonctionner correctement.

1. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.
2. Définissez `$Stores = @("Store","Store2")` pour inclure les magasins que vous souhaitez configurer avec un proxy Web.
3. Spécifiez :
   - une adresse IP OU
   - un nom de domaine complet pour le proxy Web
4. Exécutez les applets de commande PowerShell suivants :

```
$Stores = @("Store","Store2")
$ProxyIP = "10.0.0.1"
$ProxyFQDN = "proxyserver.example.com"
$ProxyPort = 8888

# Set this for every Store using Stores array
function Set-StoreProxyServer() # Tested with both IP and FQDN
```



```
8  {
9
10     [CmdletBinding()]
11     param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
           Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
           array]$Stores,
12         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
              string]$ProxyIP,
13         [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
              string]$ProxyFQDN,
14         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
              Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
              ][int]$ProxyPort)
15
16     foreach($Store in $Stores)
17     {
18
19         Write-Host "Backing up the Store web.config file for store
               $Store before making changes..." -ForegroundColor "
              Yellow"
20         Write-Host "`n"
21
22         if(!(Test-Path "$env:UserProfile\desktop$Store"))
23         {
24
25             Write-Host "Creating $env:UserProfile\desktop$Store\
                  directory for backup..." -ForegroundColor "Yellow"
26             New-Item -Path "$env:UserProfile\desktop$Store" -
                  ItemType "Directory" | Out-Null
27             Write-Host "`n"
28          }
29
30
31         Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
              config to $env:UserProfile\desktop$Store..." -
              ForegroundColor "Yellow"
32         Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
              config" -Destination "$env:UserProfile\desktop$Store" -
              Force | Out-Null
33
34         if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35         {
36
37             Write-Host "$env:UserProfile\desktop$Store\web.config
                  file backed up" -ForegroundColor "Green"
```



```
38          }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file NOT found!" -ForegroundColor "Red"
44          }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
                Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
                config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58          }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64          }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                "")
71          $DefaultProxy = $XMLObject.CreateNode("element","
                defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
```

```
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host "Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
                net'.defaultProxy.proxy.proxyaddress | Out-Null
87          Write-Host ("Configured proxy server for Store $Store"+":
                "+ $ConfiguredProxyServer) -ForegroundColor "Green"
88          Write-Host "`n"
89       }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93   }
94
95
96  Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
       ProxyPort $ProxyPort
97  # OR
98  Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
       $ProxyPort
```

5. Vérifiez que C:\inetpub\wwwroot\Citrix<magasin>\web.config contient maintenant une nouvelle section `<system.net>` à la fin du fichier web.config.

```
1           </dependentAssembly>
2       </assemblyBinding>
3   </runtime>
4   <system.net>
5       <defaultProxy>
6       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
            bypassonlocal="true" />
7       </defaultProxy>
8   </system.net>
9   </configuration>
```

6. Importez les données Citrix Analytics comme décrit à la section Importer les données Citrix Analytics dans votre déploiement StoreFront.

Méthode 2 – Ajouter manuellement une section `<system.net>` au fichier web.config du magasin

Cette opération doit être effectuée pour chaque magasin sur le serveur StoreFront qui est utilisé pour envoyer des données à Citrix Analytics.

1. Sauvegardez le fichier web.config du magasin et copiez-le vers un autre emplacement en dehors de C:\inetpub\wwwroot\Citrix<magasin>\web.config.
2. Modifiez le fichier XML suivant avec vos paramètres de proxy à l'aide d'une combinaison Nom de domaine complet + Port ou d'une combinaison Adresse IP + Port.

   Par exemple, à l'aide d'une combinaison Nom de domaine complet + Port, utilisez l'élément `<system.net>` suivant :

   ```
   <system.net>
       <defaultProxy>
       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
          bypassonlocal="true" />
       </defaultProxy>
   </system.net>
   ```

   Par exemple, à l'aide d'une combinaison Adresse IP + Port, utilisez l'élément `<system.net>` suivant :

   ```
   <system.net>
       <defaultProxy>
       <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
          " />
       </defaultProxy>
   </system.net>
   ```

3. À la fin du fichier web.config du magasin, insérez l'élément `<system.net>` approprié comme indiqué ici :

   ```
   <runtime>
   <gcServer enabled="true" />
   <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
       <dependentAssembly>
       <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
          BF3856AD364E35" culture="neutral" />
       <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
          5.0.0.0" />
       </dependentAssembly>
       <dependentAssembly>
       <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
          ad4fe6b2a6aeed" culture="neutral" />
   ```



```
10      <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
            9.0.0.0" />
11      </dependentAssembly>
12  </assemblyBinding>
13  </runtime>
14
15  Insert the <system.net> element here
16
17  </configuration>
```

4. Importez les données Citrix Analytics comme décrit à la section Importer les données Citrix Analytics dans votre déploiement StoreFront.

Mettre à niveau StoreFront

> **Avertissement :**
>
> Lorsque vous effectuez une mise à niveau vers StoreFront 1912, tous les sites Desktop Appliance de votre déploiement sont automatiquement supprimés. Si vous devez conserver vos sites Desktop Appliance, n'effectuez pas de mise à niveau. Comme alternative, Citrix recommande d'utiliser Citrix Workspace Desktop Lock pour tous les cas d'utilisation n'appartenant pas au domaine.

La mise à niveau 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. En revanche, la désinstallation de StoreFront supprime StoreFront et les services, les sites et les données d'abonnement aux applications (sur des serveurs autonomes) associés, ainsi que la configuration associée.

À noter

- 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.
- La mise à niveau vers la version actuelle de StoreFront (Current Release) à partir d'une version plus ancienne qui est maintenant en fin de vie n'est pas prise en charge. Pour plus d'informations, consultez CTX200356.
- 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 niveau vers la même version avant de se voir accorder l'accès au déploiement.
- StoreFront ne prend pas en charge les déploiements sur plusieurs serveurs contenant différents systèmes d'exploitation de serveur ; par conséquent tous les serveurs d'un groupe doivent être

sur le même système d'exploitation Windows Server.

- 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.
- Tous les magasins qui utilisent l'expérience utilisateur classique sont mis à jour pour utiliser l'expérience unifiée lors de la mise à niveau vers cette version de StoreFront. Nous vous recommandons d'informer les utilisateurs des changements de la nouvelle expérience apportés par cette mise à niveau, décrits dans la section Expérience utilisateur unifiée. 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.
- Avant que la mise à niveau StoreFront ne s'exécute, elle effectue des vérifications préalables à la mise à niveau. Si une vérification préalable à la mise à niveau échoue, la mise à niveau ne démarre pas et vous êtes averti des échecs. Votre installation StoreFront reste inchangée. Après avoir corrigé les erreurs, réexécutez la mise à niveau.
- Si la mise à niveau de StoreFront échoue, votre installation StoreFront existante risque de perdre sa configuration initiale. Restaurez votre installation StoreFront à un état fonctionnel, puis réexécutez la mise à niveau. Pour restaurer StoreFront à un état fonctionnel, tenez compte des approches suivantes :
  - Restaurer l'instantané de la VM que vous avez créé avant la mise à niveau
  - Importer la configuration StoreFront que vous avez exportée avant la mise à niveau (voir Exporter et importer la configuration StoreFront)
  - Effectuer les conseils de dépannage décrits dans la section Résolution des problèmes de mise à niveau de StoreFront
- Tous les échecs de mise à niveau de StoreFront qui se produisent à partir du metainstaller Citrix Virtual Apps and Desktops sont signalés dans une boîte de dialogue contenant un lien vers le journal des échecs correspondant.

Se préparer à la mise à niveau

Avant de démarrer la mise à niveau, nous vous recommandons d'effectuer les étapes suivantes afin d'éviter l'échec de la mise à niveau :

- Planifiez votre stratégie de sauvegarde avant la mise à niveau.
- Fermez toutes les autres applications sur le serveur StoreFront.
- Fermez la console de gestion StoreFront.
- Fermez toutes les lignes de commande et les fenêtres de PowerShell.
- Fermez tous les dossiers liés à StoreFront tels que C:\inetpub\wwwroot\Citrix\Store et C:\inetpub\wwwroot\Citrix\StoreWeb. Cela empêche l'Explorateur Windows d'appliquer un verrou exclusif sur ces dossiers.
- Avant de procéder à la mise à niveau d'un serveur, redémarrez-le pour vous assurer qu'aucun

verrou exclusif n'existe sur les fichiers ou dossiers StoreFront. (Le redémarrage du processus de l'Explorateur, par exemple en fermant toutes les instances de l'Explorateur Windows, *n'est pas* suffisant).
- Exécutez la mise à niveau immédiatement sans démarrer d'autres programmes sur le serveur.
- Mettez à niveau le serveur à l'aide d'un compte d'administration n'exécutant aucune autre installation et un nombre minimum d'autres applications.

Mettre à niveau un serveur StoreFront autonome

1. Déconnectez les utilisateurs du déploiement StoreFront pour les empêcher 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.
2. Sauvegardez le serveur en créant un instantané de la VM.
3. Exportez la configuration StoreFront existante (recommandé).
4. Exécutez le fichier d'installation de cette version de StoreFront.

Mettre à niveau un groupe de serveurs StoreFront

La mise à niveau de groupes de serveurs StoreFront implique l'utilisation d'un des serveurs pour supprimer les autres serveurs du groupe. Les serveurs supprimés conservent la configuration liée au groupe, ce qui peut les empêcher d'être associés à un nouveau groupe de serveurs. Avant de pouvoir être réutilisés pour créer de nouveaux groupes de serveurs ou en tant que serveurs StoreFront autonomes, ils doivent être réinitialisés aux paramètres d'usine ou réinstallés sur StoreFront.

Avant de procéder à la mise à niveau d'un groupe de serveurs, procédez comme suit :

- Sauvegardez tous les serveurs du groupe en créant des instantanés de VM. Cela vous permet de revenir rapidement à un groupe opérationnel de serveurs à trois nœuds si la mise à niveau ne se déroule pas comme prévu.
- Exportez la configuration StoreFront existante (recommandé). Exportez uniquement la configuration du groupe de serveurs à partir d'un serveur. Si vous avez propagé toutes les modifications sur les serveurs, tous les serveurs d'un groupe de serveurs conservent des copies identiques de la configuration. Cette sauvegarde vous permet de créer facilement un nouveau groupe de serveurs.

Exemple 1 – Mettre à niveau un groupe de serveurs StoreFront à trois nœuds lors d'un temps d'arrêt planifié réservé à la maintenance

Cette procédure décrit la mise à niveau d'un groupe de serveurs StoreFront composé de trois serveurs A, B et C, pendant des temps d'arrêt planifiés.

1. Désactivez l'accès utilisateur au groupe de serveurs en désactivant l'URL d'équilibrage de charge. Cela empêche les utilisateurs de se connecter au déploiement lors de la mise à niveau.
2. Utilisez le serveur A pour supprimer les serveurs B et C du groupe.

   Les serveurs B et C sont désormais « orphelins » au sein du groupe de serveurs.
3. Mettez à niveau le serveur A en exécutant le fichier d'installation de cette version de StoreFront.
4. Assurez-vous que le serveur A a bien été mis à niveau.
5. Sur les serveurs B et C, désinstallez la version actuellement installée de StoreFront, puis installez la nouvelle version de StoreFront.
6. Associez les serveurs B et C au serveur A mis à niveau pour créer un groupe de serveurs mis à niveau. Ce groupe de serveurs se compose d'un serveur mis à niveau (A) et de deux serveurs récemment installés (B et C).

   Ce processus (Joindre un groupe de serveurs existant) propage automatiquement toutes les données de configuration et d'abonnement aux nouveaux serveurs B et C.
7. Vérifiez que tous les serveurs fonctionnent correctement.
8. Activez l'accès de l'utilisateur au groupe de serveurs mis à niveau en activant l'URL d'équilibrage de charge.

Exemple 2 – Mettre à niveau un groupe de serveurs StoreFront à trois nœuds sans temps d'arrêt planifié

Cette procédure décrit la mise à niveau d'un groupe de serveurs StoreFront composé de trois serveurs A, B et C, sans temps d'arrêt planifié.

Avant de procéder à la mise à niveau d'un groupe de serveurs, procédez comme suit :

1. Exportez les données d'abonnement à partir du serveur A à l'aide de la commande **Export-STFStoreSubscriptions**. Cette sauvegarde est nécessaire car les serveurs sont réinitialisés aux paramètres d'usine plus tard dans le processus, ce qui supprime les données d'abonnement et de configuration. Voir Gérer les données d'abonnement d'un magasin.
2. Désactivez l'accès de l'utilisateur au serveur C en désactivant le service d'équilibrage de charge qui représente le serveur C. Cela empêche les utilisateurs de se connecter au serveur C pendant le processus de mise à niveau. Maintenez le service d'équilibrage de charge représentant les serveurs A et B activés, afin que vos utilisateurs puissent continuer à les utiliser.
3. Utilisez le serveur A pour supprimer le serveur C du groupe.
   Les serveurs A et B continuent de fournir un accès aux ressources de vos utilisateurs. Le serveur

C est désormais « orphelin » au sein du groupe de serveurs et est réinitialisé aux paramètres d'usine.

4. Réinitialisez les paramètres d'usine du serveur C orphelin à l'aide de la commande **Clear-STFDeployment**.
5. Importez la configuration StoreFront que vous avez précédemment exportée vers le serveur C à l'aide de la commande **Import-STFConfiguration**.
6. Mettez à niveau le serveur C en exécutant le fichier d'installation de cette version de StoreFront. Le serveur C a désormais une configuration identique à l'ancien groupe de serveurs et est mis à niveau vers une nouvelle version de StoreFront.
7. Importez les données d'abonnement que vous avez précédemment exportées vers le serveur C. Il *n'est pas* nécessaire de répéter cette étape plus tard. Un seul serveur a besoin d'une copie des données d'abonnement pour les propager sur les autres serveurs qui sont associés au groupe.
8. Répétez les étapes 2 à 6 à l'aide du serveur B. Pendant ce temps, seul le serveur A fournit aux utilisateurs un accès aux ressources. Il est donc préférable d'effectuer cette étape pendant les périodes de travail plus calmes, où la charge sur le groupe de serveurs StoreFront devrait être minime.
9. Associez le serveur B au serveur C à l'aide du processus Joindre un groupe de serveurs existant. Cela permet d'obtenir un déploiement de serveur unique sur la version actuelle de StoreFront (serveur A) et un nouveau groupe de serveurs à deux nœuds sur la nouvelle version de StoreFront (serveurs B et C).
10. Activez les services d'équilibrage de charge sur les serveurs B et C afin qu'ils puissent prendre la place du serveur A.
11. Désactivez le service d'équilibrage de charge sur le serveur A afin que les utilisateurs soient dirigés vers les serveurs B et C récemment mis à niveau.
12. Répétez les étapes 2 à 6 à l'aide du serveur A.
    Le processus de mise à niveau du groupe de serveurs est maintenant terminé. Les données de configuration et d'abonnement des serveurs A, B et C sont identiques à celles du groupe d'origine.

> **Remarque :**
>
> Pendant la brève période où le serveur A est le seul serveur accessible, les abonnements peuvent être perdus (étape 9). En effet, le nouveau groupe de serveurs peut disposer d'une copie légèrement obsolète de la base de données d'abonnement après la mise à niveau et tout nouvel enregistrement d'abonnement peut être perdu.
>
> Cela n'a aucun impact fonctionnel car les données d'abonnement ne sont pas essentielles pour permettre aux utilisateurs de se connecter et de lancer des ressources. Les utilisateurs devront

> cependant s'abonner à nouveau à une ressource une fois le serveur A réinitialisé aux paramètres d'usine et associé au groupe récemment mis à niveau. Bien qu'il soit peu probable que plus de quelques enregistrements d'abonnement soient perdus, il s'agit d'une conséquence possible de la mise à niveau d'un environnement de production StoreFront actif sans temps d'arrêt planifié.

Configurer StoreFront

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

- Créer un 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 serveur, vous devez pouvoir accéder à un serveur existant du déploiement. Citrix vous recommande de ne pas ajouter plus de 6 serveurs à un groupe de serveurs.

Désinstallez StoreFront

En plus du produit lui-même, la désinstallation de StoreFront supprime le service d'authentification, les magasins, les sites Citrix Receiver pour Web 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, les détails des abonnements utilisateur aux applications sont par conséquent 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. Fermez la console d'administration StoreFront si elle est ouverte.
3. Fermez toutes les sessions PowerShell qui ont pu être utilisées pour gérer StoreFront via son SDK PowerShell.
4. 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**.

5. Dans la boîte de dialogue **Programmes et fonctionnalités**, sélectionnez **Citrix StoreFront** et cliquez sur **Désinstaller** pour supprimer tous les composants StoreFront du serveur.
6. Dans la boîte de dialogue **Désinstaller Citrix StoreFront**, cliquez sur **Oui**. Une fois la désinstallation terminée, cliquez sur **OK**.

Créer un nouveau déploiement

December 23, 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.
4. Cliquez sur **Suivant** pour configurer le service d'authentification, qui authentifie les utilisateurs auprès de 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, l'application Citrix Workspace nécessite des connexions HTTPS aux 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 de plus amples informations, consultez la section Configurer des groupes de serveurs.

   Vous pouvez utiliser la tâche **Changer l'URL de base** dans la console de gestion StoreFront pour passer de HTTP à HTTPS à tout moment, 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 l'application Citrix Workspace 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 **Delivery 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 Citrix Virtual Apps and Desktops au magasin. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison de déploiements Citrix Virtual Apps and Desktops. 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 **Delivery 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 Citrix Gateway, sélectionnez **Autoriser utilisateurs à accéder uniquement aux ressources délivrées via StoreFront (sans tunnel VPN)**. Les utilisateurs ouvrent une session à l'aide d'ICAProxy ou d'un VPN sans client (CVPN) à Citrix Gateway et n'ont pas besoin d'utiliser Citrix Gateway Plug-in pour établir un VPN complet.
   - 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 requièrent Citrix Gateway Plug-in pour établir le tunnel VPN.

   Lorsque vous activez l'accès à distance au magasin, la méthode d'authentification **Authentification pass-through via Citrix Gateway** est automatiquement activée. Les utilisateurs s'authentifient sur Citrix Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

9. Si vous avez activé l'accès à distance, **Appliances Citrix Gateway** dresse la liste des déploiements par le biais desquels les utilisateurs peuvent accéder au magasin. Pour ajouter un déploiement Citrix Gateway à cette liste, suivez la procédure appropriée décrite dans la section

Fournir l'accès distant au magasin via une appliance Citrix Gateway. Répétez les procédures, si nécessaire, pour ajouter d'autres déploiements.

10. Dans la liste **Appliances Citrix Gateway**, sélectionnez les déploiements par le biais desquels les utilisateurs peuvent accéder au magasin. Si vous activez l'accès au travers de plusieurs déploiements, spécifiez l'**appliance par défaut** à utiliser pour accéder au magasin. Cliquez sur **Suivant**.

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 Citrix Gateway :** les utilisateurs s'authentifient sur Citrix Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Cette option est automatiquement activée lorsque l'accès distant est activé.1. Sur la page **Configurer la validation du mot de passe**, sélectionnez les Delivery Controller qui fourniront la validation du mot de passe et cliquez sur **Suivant**.

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. Une fois le magasin créé, d'autres options vous sont alors proposées via la console de gestion de Citrix StoreFront. Pour de plus amples informations, consultez la section Configurer et gérer des magasins.

Les utilisateurs peuvent désormais accéder à votre magasin avec l'application Citrix Workspace, 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 de plus amples informations, consultez 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 d'appliances 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 https[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.

Pour ajouter rapidement d'autres serveurs à votre déploiement, sélectionnez l'option Joindre un groupe de serveurs existant lors de l'installation d'autres instances de StoreFront.

Ajouter des ressources Citrix Virtual Apps and Desktops au magasin

Suivez les étapes suivantes pour mettre des bureaux et applications fournis par Citrix Virtual Apps and Desktops 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 **Delivery Controller**, indiquez l'infrastructure fournissant les ressources que vous souhaitez mettre à disposition dans le magasin. Cliquez sur **Ajouter**.
2. Dans la boîte de dialogue Ajouter un Delivery Controller, spécifiez un **nom d'affichage** qui vous aidera à identifier le déploiement et sélectionnez un **type** pour indiquer comment les ressources mises à disposition dans le magasin sont fournies. Tapez les valeurs par défaut sur Citrix Virtual Apps and Desktops. XenApp 6.5 est disponible en tant que Type, mais il a atteint sa fin de vie en juin 2018 et est désormais couvert par le Programme de support étendu.
3. Pour mettre des bureaux et applications fournis par Citrix Virtual Apps and Desktops et XenApp 6.5 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 Citrix Virtual Apps and Desktops, spécifiez les détails des Delivery Controller. Dans le cas de batteries XenApp 6.5, dressez la liste des serveurs exécutant le service XML Citrix.
4. Dans la liste **Type de transport**, sélectionnez 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 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 Citrix Virtual Apps and Desktops, 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 6.5 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 Citrix Virtual Apps and Desktops, 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 6.5, indiquez le port TCP du Relais SSL dans **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.
7. Cliquez sur **OK**. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison de déploiements Citrix Virtual Apps and Desktops. Pour ajouter d'autres sites Citrix Virtual Desktops ou des batteries Citrix Virtual Apps, 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 une appliance Citrix Gateway

Effectuez les étapes suivantes pour configurer l'accès distant via une appliance Citrix 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 une appliance Citrix Gateway, sur la page **Paramètres généraux**, spécifiez un **nom d'affichage** pour l'appliance Citrix Gateway qui permettra aux

utilisateurs de l'identifier.

Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans l'application Citrix Workspace. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser cette passerelle. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements Citrix Gateway pour permettre aux utilisateurs d'identifier facilement la passerelle la plus pratique ou la plus proche en fonction de leur situation.

3. Pour **URL de Citrix Gateway**, tapez la combinaison URL:port du serveur virtuel Citrix Gateway pour votre déploiement. Si aucun port n'est spécifié, alors le port par défaut `https://` de 443 est utilisé. Il n'est pas nécessaire de spécifier le port 443 dans l'URL.

   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. Sélectionnez **Utilisation ou rôle** de Citrix Gateway dans les options disponibles.

   - **Authentification et routage HDX :** Citrix Gateway sera utilisé pour l'authentification, ainsi que pour le routage des sessions HDX.
   - **Authentification uniquement :** Citrix Gateway sera utilisé pour l'authentification mais pas pour le routage des sessions HDX.
   - **Routage HDX uniquement :** Citrix Gateway sera utilisé pour le routage des sessions HDX mais pas pour l'authentification.

5. Pour tous les déploiements sur lesquels vous mettez les ressources fournies par Citrix Virtual Apps and Desktops ou XenApp 6.5 à disposition dans le magasin, sur la page **Secure Ticket Authority (STA)**, ajoutez les **adresses URL STA** des serveurs qui exécutent la 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 Citrix Virtual Apps and Desktops ou XenApp 6.5, et émet des tickets de session en réponse aux demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources Citrix Virtual Apps and Desktops ou XenApp 6.5. Utilisez l'URL STA correcte (telle que `HTTPS://` ou `HTTP://`) en fonction de la configuration de vos Delivery Controller. L'URL STA doit également être identique à celle configurée dans Citrix Gateway sur votre serveur virtuel.

6. Pour vous assurer que Citrix Virtual Apps and Desktops ou XenApp 6.5 maintiennent les sessions déconnectées ouvertes pendant que l'application Citrix Workspace tente de se reconnecter automatiquement, sélectionnez **Activer la fiabilité de session**.

7. Si vous configurez plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, sélectionnez **Demander des tickets de deux STA, si possible**. StoreFront

obtient des tickets de deux STA différentes et les sessions utilisateur ne sont pas interrompues si l'une des STA devient 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. Dans la page **Paramètres d'authentification**, tapez l'**Adresse IP de vServer** de l'appliance Citrix Gateway.

   Utilisez l'adresse IP privée du serveur virtuel Citrix Gateway plutôt que l'adresse IP publique qui est routée vers l'adresse IP privée. Les passerelles sont généralement identifiées par StoreFront via leurs URL. Si vous utilisez l'équilibrage de charge globale du serveur (GSLB), vous devez ajouter le VIP à chaque passerelle. Cela permet à StoreFront d'identifier plusieurs passerelles qui utilisent toutes la même URL (nom de domaine GSLB) comme des passerelles distinctes. Par exemple, trois passerelles peuvent être configurées pour le magasin avec la même URL telle que `https://gslb.domain.com` mais elles auraient chacune des VIP uniques configurées telles que 10.0.0.1, 10.0.0.2 et 10.0.0.3.

9. Si vous ajoutez une appliance exécutant Citrix Gateway, sélectionnez dans la liste **Type d'ouverture de session** la méthode d'authentification que vous avez configurée sur l'appliance pour les utilisateurs de l'application Citrix Workspace.

   - 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 parmi 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**.

10. Si vous configurez StoreFront pour Citrix Gateway et que vous souhaitez utiliser Smart Access, vous devez taper une **URL de rappel**. StoreFront ajoute automatiquement la partie standard de l'URL. Entrez l'adresse URL de l'appliance accessible en interne. StoreFront contacte le service d'authentification Citrix Gateway pour vérifier que les requêtes reçues de Citrix Gateway proviennent de cette appliance.

    Lorsque vous utilisez GSLB, nous vous recommandons de configurer des URL de rappel uniques pour chacune de vos passerelles GSLB. StoreFront doit être capable de faire correspondre cha-

cune des URL de rappel uniques avec les VIP privés configurés pour chacun des serveurs virtuels de passerelle GSLB. Par exemple, `emeagateway.domain.com`, `usgateway.domain.com` et `apacgateway.domain.com` devraient correspondre à la passerelle VIP correcte.

11. Cliquez sur **Créer** pour ajouter votre appliance Citrix Gateway à la liste dans la boîte de dialogue **Paramètres d'accès à distance**.

    Les informations sur la configuration de vos appliances Citrix Gateway sont enregistrées dans le fichier de provisioning .cr du magasin. Ceci permet à l'application Citrix Workspace d'envoyer une demande de connexion appropriée lorsque vous contactez les appliances pour la première fois.

12. Retournez à l'étape 10 de la procédure « Créer un nouveau déploiement » en haut de cet article.

Joindre un groupe de serveurs existant

August 28, 2019

Un groupe de serveurs peut contenir un maximum de cinq serveurs. Toutefois, 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.

Avant d'installer StoreFront sur un serveur que vous ajoutez au groupe, vérifiez les éléments suivants :

- Le serveur que vous ajoutez 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.
- Le chemin d'accès relatif à StoreFront dans IIS sur le serveur que vous ajoutez est le même que sur les autres serveurs du groupe.

Si le serveur StoreFront que vous avez ajouté précédemment appartenait à un groupe de serveurs et a été supprimé, avant qu'il puisse être ajouté à nouveau, vous devez réinitialiser les paramètres d'usine du serveur sur le même groupe de serveurs ou sur un autre groupe de serveurs. Voir Réinitialiser les paramètres d'usine du serveur

> **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 em-

> pêcher 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.

Réinitialiser les paramètres d'usine du serveur

June 13, 2019

Dans certains cas, il est nécessaire de réinitialiser une installation StoreFront à son état d'installation initial, par exemple, avant de pouvoir ajouter à nouveau un serveur StoreFront à un groupe de serveurs.

Une désinstallation et une réinstallation manuelles peuvent être effectuées, mais cela prend plus de temps et peut causer d'autres problèmes imprévus. Au lieu de cela, vous pouvez exécuter l'applet de commande PowerShell **Clear-STFDeployment** pour réinitialiser les paramètres d'usine d'un serveur StoreFront.

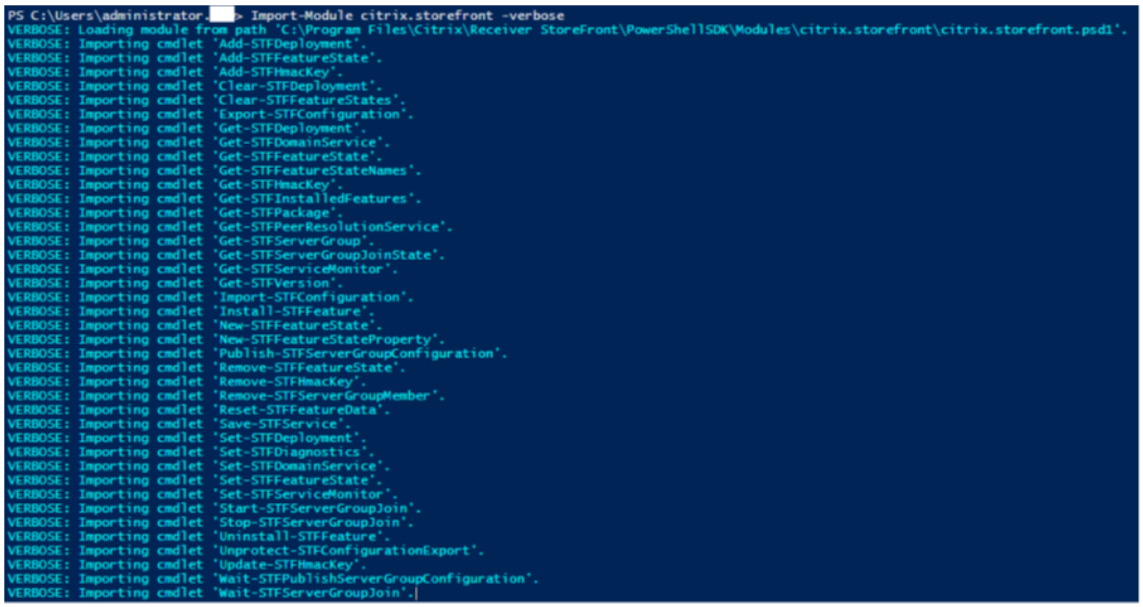
1. Assurez-vous que la console de gestion StoreFront est fermée.

2. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.
3. Définissez le chemin d'accès PowerShell :

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('
    PSModulePath','Machine')
```

4. Importez le module Citrix StoreFront.

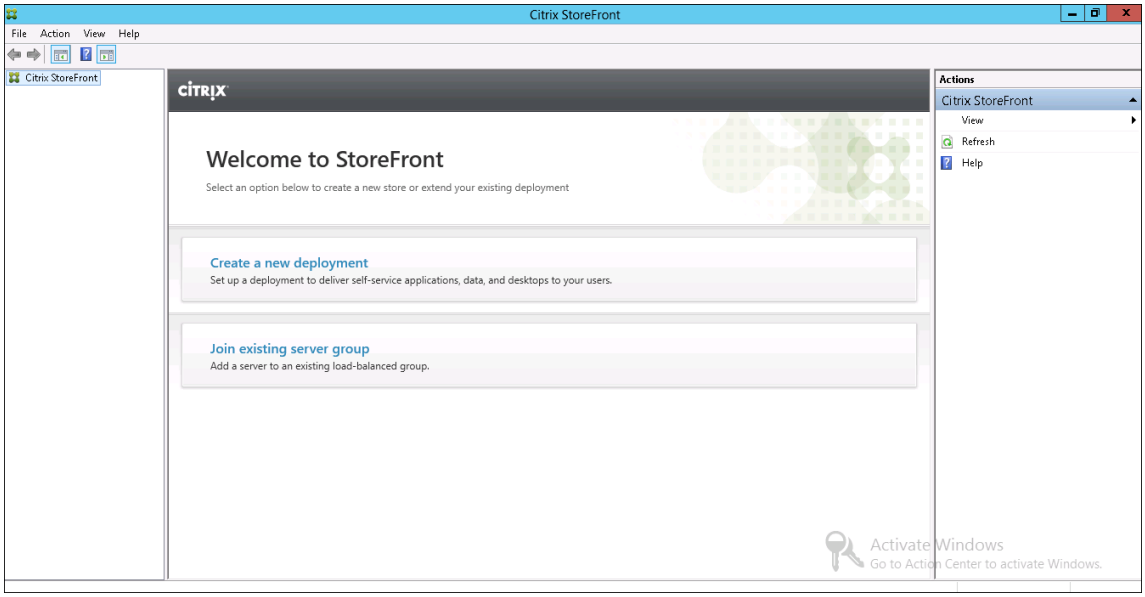
```
Import-Module citrix.storefront -verbose
```



5. Une fois le module importé, exécutez la commande **Clear-STFDeployment** pour réinitialiser les paramètres par défaut du serveur StoreFront :

```
Clear-STFDeployment -Confirm $False
```

6. Une fois la commande terminée, ouvrez la console de gestion StoreFront et vérifiez que tous les paramètres sont réinitialisés. Les options **Créer un nouveau déploiement** ou **Joindre un groupe de serveurs existant** sont disponibles.



Migrer les fonctionnalités de l'Interface Web vers StoreFront

January 8, 2020

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

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

Emplacements des dossiers

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

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom
- Pour la personnalisation de style, ajoutez l'exemple au fichier style.css qui se trouve dans

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom
- Pour le contenu dynamique, ajoutez le contexte dynamique à un fichier texte dans

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\customweb
- Si vous disposez d'un déploiement à plusieurs serveurs, vous pouvez répliquer les modifications vers d'autres serveurs depuis la console d'administration StoreFront ou à l'aide de PowerShell.

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

Fonctionnalité de l'Interface Web	Équivalent StoreFront
Personnalisation avec la console de gestion	
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. **Pour désactiver les zones de recherche sur le bureau ou l'interface Web**, ajoutez le style suivant au fichier style.css : `.search-container { display: none; }` . **Pour désactiver les zones de recherche sur l'interface utilisateur du téléphone**, ajoutez le style suivant au fichier style.css : `## searchBtnPhone { display: none; }` .
Activer l'actualisation	Activée par défaut (actualisation du navigateur).

Fonctionnalité de l'Interface Web	Équivalent StoreFront
Activer le retour au dernier dossier	Non activé par défaut. Pour mémoriser le dossier actuel et y retourner au moment du chargement, ajoutez la ligne suivante au fichier script.js : `CTXS.Extensions.afterDisplayHomeScreen = function(){ //check if view was saved last time CTXS.ExtensionAPI.localStorageGetItem("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.localStorageGetItem("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.localStorageSetItem("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")&&(newview != "search")){ CTXS.ExtensionAPI.localStorageSetItem("view", newview); } } ; }); } ;`
Activer les conseils	L'application Citrix Workspace utilise très peu les info-bulles, car elle cible les appareils tactiles et non tactiles. Vous pouvez ajouter des info-bulles à l'aide d'un script personnalisé.

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 l'application Citrix Workspace est différente, donc ces options ne s'appliquent pas. Vous pouvez utiliser la console de gestion StoreFront pour configurer des vues. Pour plus d'informations, veuillez consulter la section Spécifier différentes vues pour les applications et bureaux.
Interface utilisateur à onglet unique, Interface utilisateur à plusieurs onglets (Onglet Application, Onglet Bureau, Onglet Contenu, (Ordre des onglets))	L'interface utilisateur de l'application Citrix Workspace contient des onglets par défaut, avec applications et contenu dans un onglet et bureaux dans l'autre. Il existe également un onglet **Favori** (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 **Personnaliser l'apparence du site Web** dans le panneau **Actions** de la console d'administration StoreFront et apportez les modifications sur l'écran qui s'affiche. Vous pouvez définir une image d'arrière-plan pour l'en-tête en utilisant la personnalisation de style. Par exemple `.theme-header-bgcolor { background-image: url('spirals.png'); }`

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	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 : `.customAuthHeader, .customAuthFooter .customAuthTop, .customAuthBottom { text-align: center; color: white; font-size: 16px; }` 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");` **Remarque :** il ne faut pas explicitement inclure de contenu dynamique dans le script, ou le placer dans le répertoire **personnalisé**, car les modifications effectuées ici forcent les clients à recharger l'interface utilisateur. Placez le contenu dynamique dans le répertoire **customweb**.
Message de bienvenue de l'écran d'application, Message système de l'écran d'application	Consultez les exemples d'écran de bienvenue **CustomAuth** ci-dessus. Consultez les exemples de contenu dynamique ci-dessus. Utilisez `##customTop` plutôt que `.customAuthTop` pour placer du contenu sur l'écran d'accueil.
Texte de bas de page (tous les écrans)	Exemple de script : `##customBottom { text-align: center; color: white; font-size: 16px; } ** Example static content using a script: **\$('\##customBottom').html("Welcome to ACME");`

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 *Titre de l'écran d'ouverture de session* 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. Voir http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html.
Personnalisations avancées (code)	
Hooks de génération du fichier ICA et autres personnalisations de routage d'appel	API équivalentes ou supérieures. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
Personnalisations d'authentification	API équivalentes ou supérieures. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
Accès source JSP/ASP	Il n'existe pas d'API équivalente sur StoreFront, car l'interface utilisateur n'est pas restituée de la même manière. Il existe de nombreuses API JavaScript permettant la personnalisation de l'interface utilisateur.

Configurer des groupes de serveurs

March 3, 2020

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. Consultez la section *Évolutivité* 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.

Avant qu'un serveur StoreFront supprimé puisse être ajouté à nouveau, vous devez réinitialiser les paramètres d'usine du serveur sur le même groupe de serveurs ou sur un autre groupe de serveurs. Voir Réinitialiser les paramètres d'usine du serveur

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. La propagation des informations de configuration est lancée manuellement. Vous conservez ainsi le contrôle de l'heure de la mise à jour des serveurs du groupe avec des modifications de configuration. 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 :**
>
> Toutes les modifications effectuées sur les autres serveurs du groupe sont abandonnées lors de la propagation. Si vous actualisez la configuration d'un serveur, propagez les modifications aux autres serveurs du groupe pour éviter de perdre ces modifications si vous les propagez ensuite à partir d'un autre serveur du déploiement.

Les informations propagées entre les serveurs du groupe sont les suivantes :

- Contenu de tous les fichiers web.config qui incluent la configuration StoreFront
- Contenu de `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, tels que `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` et `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`
- Contenu de `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`
- Contenu de `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, tels que les images copiées et les fichiers customisation.js
- Contenu du magasin de certificats Citrix Delivery Services, à l'exception des listes de révocation de certificats importées manuellement. Pour plus de détails sur la distribution des listes de révocation de certificats locales, consultez la section Vérification des listes de révocation de certificats (CRL).

> **Remarque :**
>
> Les données d'abonnement sont synchronisées avec les autres serveurs indépendamment du mécanisme Propager les modifications. Cette opération se produit automatiquement sans que la tâche Propager les modifications soit lancée.

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 et que vous ajoutiez une liaison HTTPS au site Web par défaut. Pour de plus amples informations, consultez la section Sécuriser votre déploiement StoreFront.

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 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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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. Dans Paramètres avancés, cliquez sur **Paramètres**.
5. Dans la boîte de dialogue Configurer les paramètres avancés :
   a) 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.
   b) 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

January 8, 2020

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

Méthode	Détail
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 Citrix Virtual Apps and Desktops, et qu'il n'est pas possible de mettre des approbations Active Directory en place, vous pouvez configurer StoreFront pour que le Citrix Virtual Apps and Desktops XML Service 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.

Méthode	Détail
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.

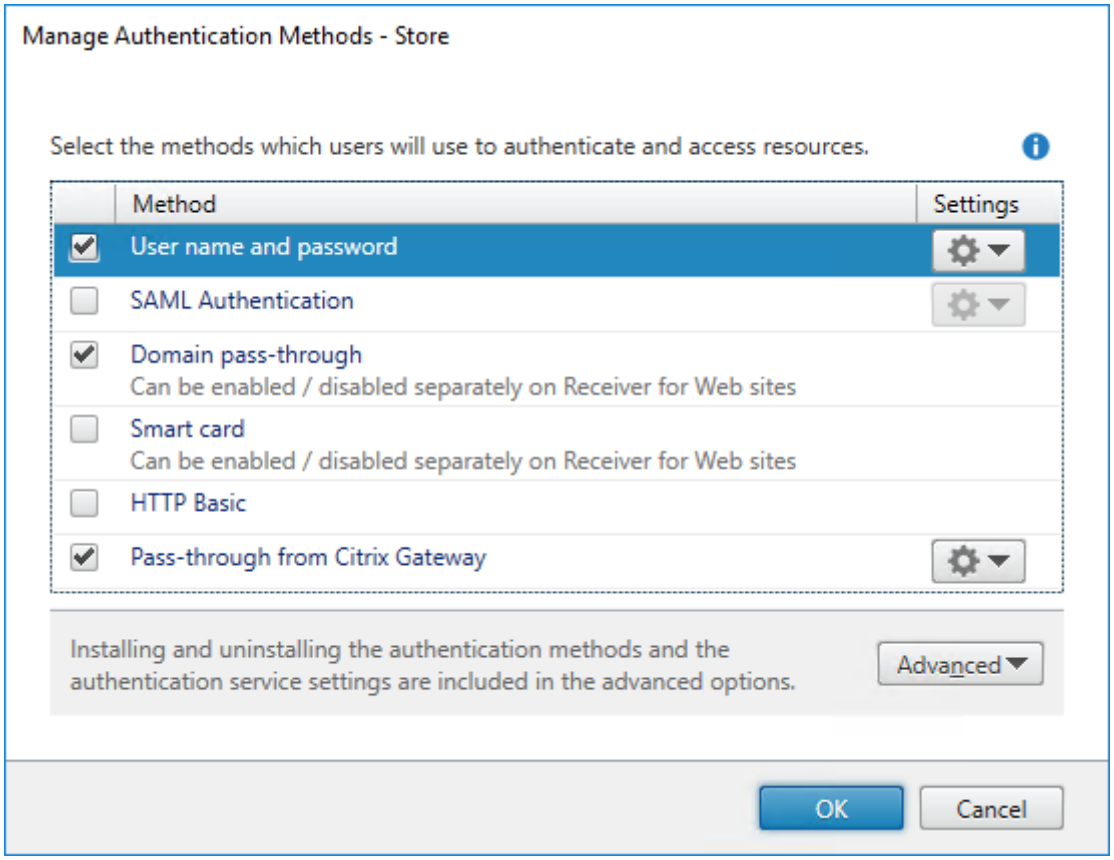
Configurer le service d'authentification

March 3, 2020

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 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 **Authentification pass-through au domaine** pour 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 ou l'application Citrix Workspace pour Windows est installé sur les machines utilisateur.
- Sélectionnez **Carte à puce** pour activer l'authentification par carte à puce. Les utilisateurs s'authentifient à l'aide de cartes à puce et de codes PIN lorsqu'ils accèdent à leurs magasins.

- Sélectionnez **HTTP Basique** pour activer l'authentification HTTP de base. Les utilisateurs s'authentifient avec le serveur Web IIS du serveur StoreFront.
- Sélectionnez **Authentification pass-through via Citrix Gateway** pour activer l'authentification pass-through à partir de Citrix Gateway. Les utilisateurs s'authentifient sur Citrix 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 Citrix 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 Citrix 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 > 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 l'application Citrix Workspace 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 l'application Citrix Workspace 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. Toutes les applications Citrix Workspace de bureau prennent en charge la modification de mot de passe via Citrix Gateway après 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 ouvrir de session car leurs mots de passe ont expiré sont redirigés vers la boîte de dialogue Changer le mot de passe. Ceci est pris en charge pour les applications Citrix Workspace et Citrix Receiver pour Web.

  > Remarque :
  >
  > 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.

- 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.

- 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.

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

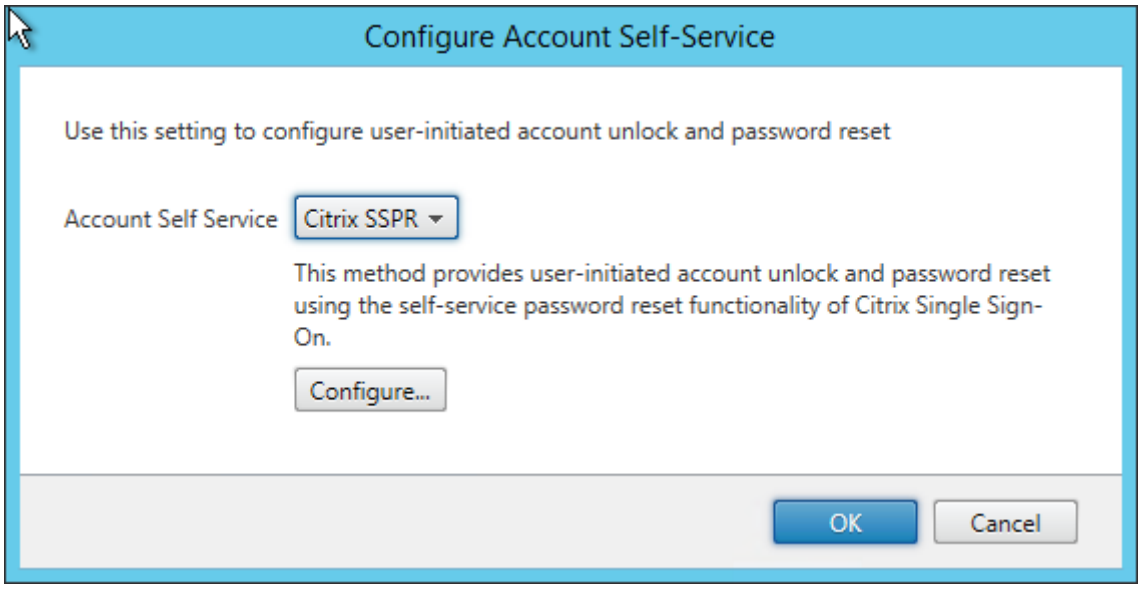
- Le magasin est configuré pour utiliser l'authentification par nom d'utilisateur et mot de passe.
- Le magasin est configuré pour utiliser uniquement la réinitialisation en libre-service des mots de passe. Si StoreFront est configuré pour utiliser de nombreuses batteries au sein d'un même domaine ou 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 à un site Receiver pour Web.

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 de Citrix Virtual Apps and Desktops. Pour de plus amples informations, consultez la documentation de Réinitialisation en libre-service des mots de passe

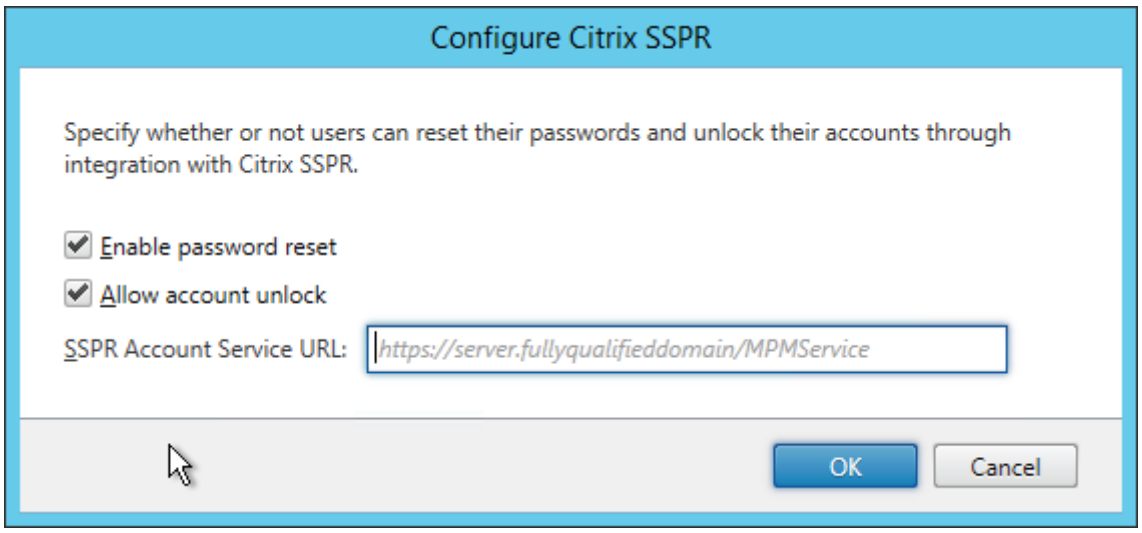
1. Activez la prise en charge de la fonction de réinitialisation en libre-service des mots de passe dans StoreFront en sélectionnant le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Gérer les méthodes**

d'authentification > Nom d'utilisateur et mot de passe et choisissez **Gérer les options de mot de passe** dans le menu déroulant.

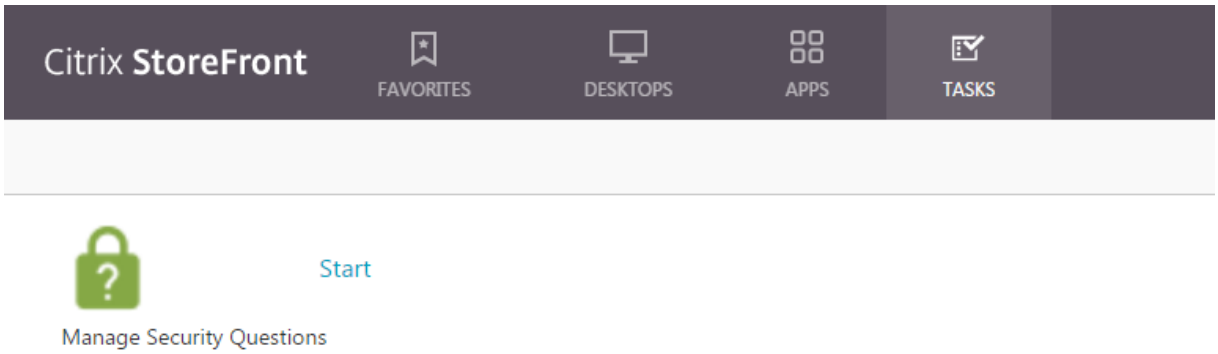
2. Choisissez si vous voulez autoriser les utilisateurs à modifier les mots de passe et cliquez sur **OK**.
3. À partir du menu déroulant **Nom d'utilisateur et mot de passe**, choisissez **Configurer libre-service de compte**, sélectionnez **Citrix SSPR** dans le menu déroulant, puis cliquez sur **OK**.
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.



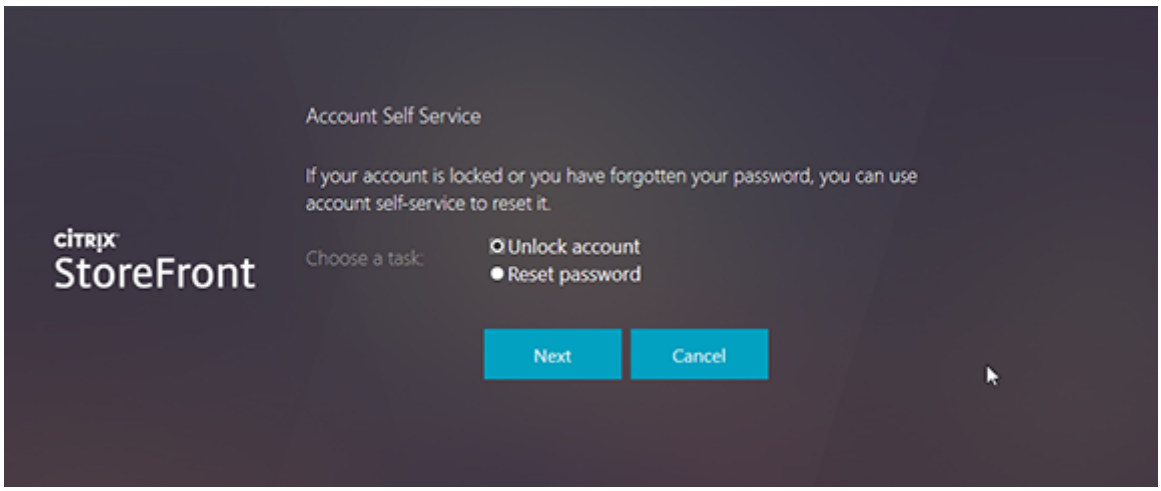
La prochaine fois que l'utilisateur se connecte à l'application Citrix Workspace ou Citrix Receiver pour Web, l'enregistrement de questions de sécurité est disponible. Après avoir cliqué sur **Démarrer**, les questions sont affichées et l'utilisateur doit fournir des réponses.



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 applications Citrix Workspace).

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 Citrix Gateway

Pour activer l'authentification pass-through par carte à puce pour les utilisateurs qui accèdent à des magasins via Citrix Gateway, utilisez la tâche Configurer l'authentification déléguée. Cette tâche est uniquement disponible lorsque Authentification pass-through via Citrix Gateway est activée et sélectionnée dans le panneau des résultats.

Lorsque la validation des informations d'identification est déléguée à Citrix Gateway, les utilisateurs s'authentifient sur Citrix 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 Citrix Gateway, afin que l'authentification pass-through ne soit appliquée que lorsque les utilisateurs ouvrent une session sur Citrix Gateway avec un mot de passe.

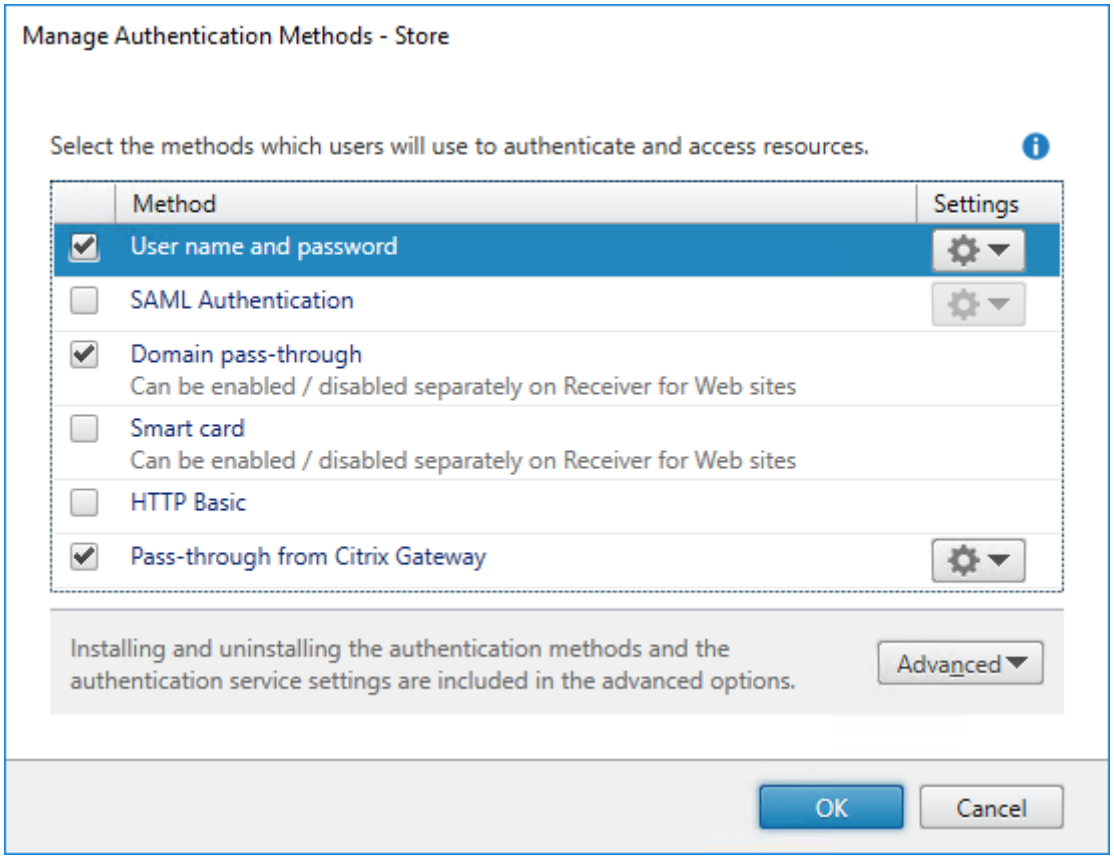
Authentification basée sur le service XML

August 28, 2019

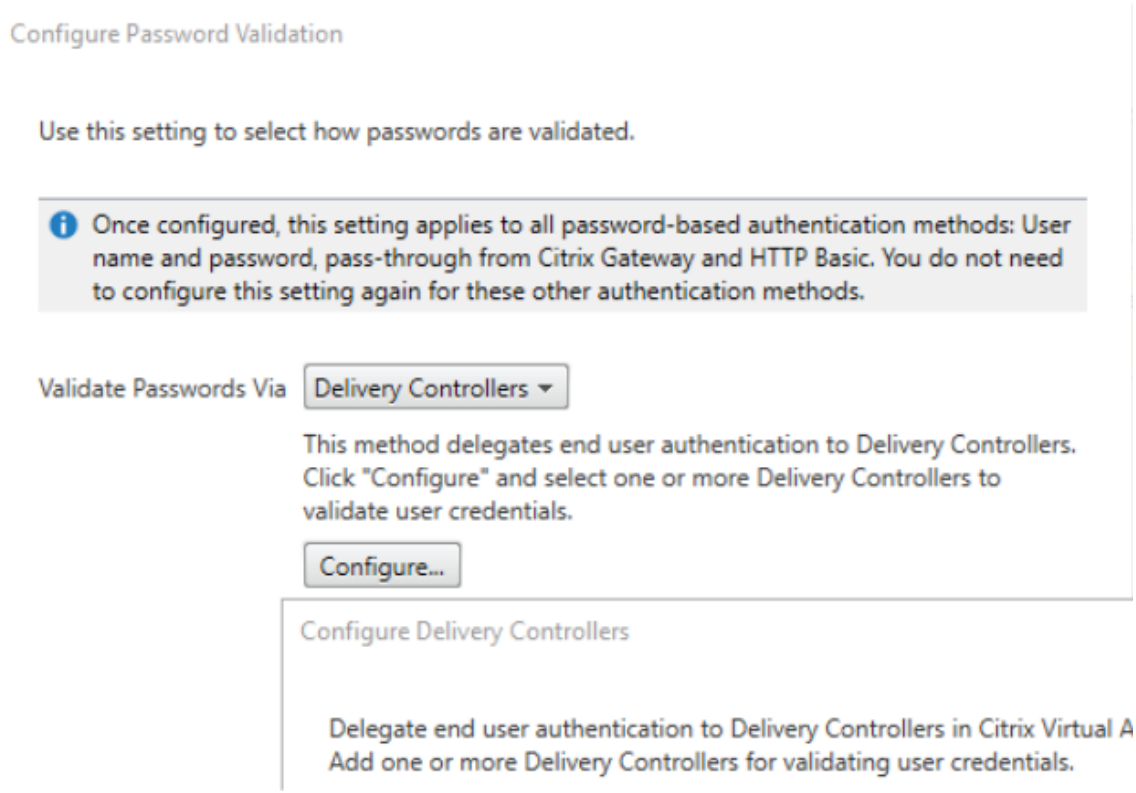
Lorsque StoreFront ne se trouve pas dans le même domaine que Citrix Virtual Apps and Desktops, et qu'il n'est pas possible de mettre des approbations Active Directory en place, vous pouvez configurer StoreFront pour que le Citrix Virtual Apps and Desktops XML Service soit utilisé pour l'authentification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

Activer l'authentification basée sur le service XML

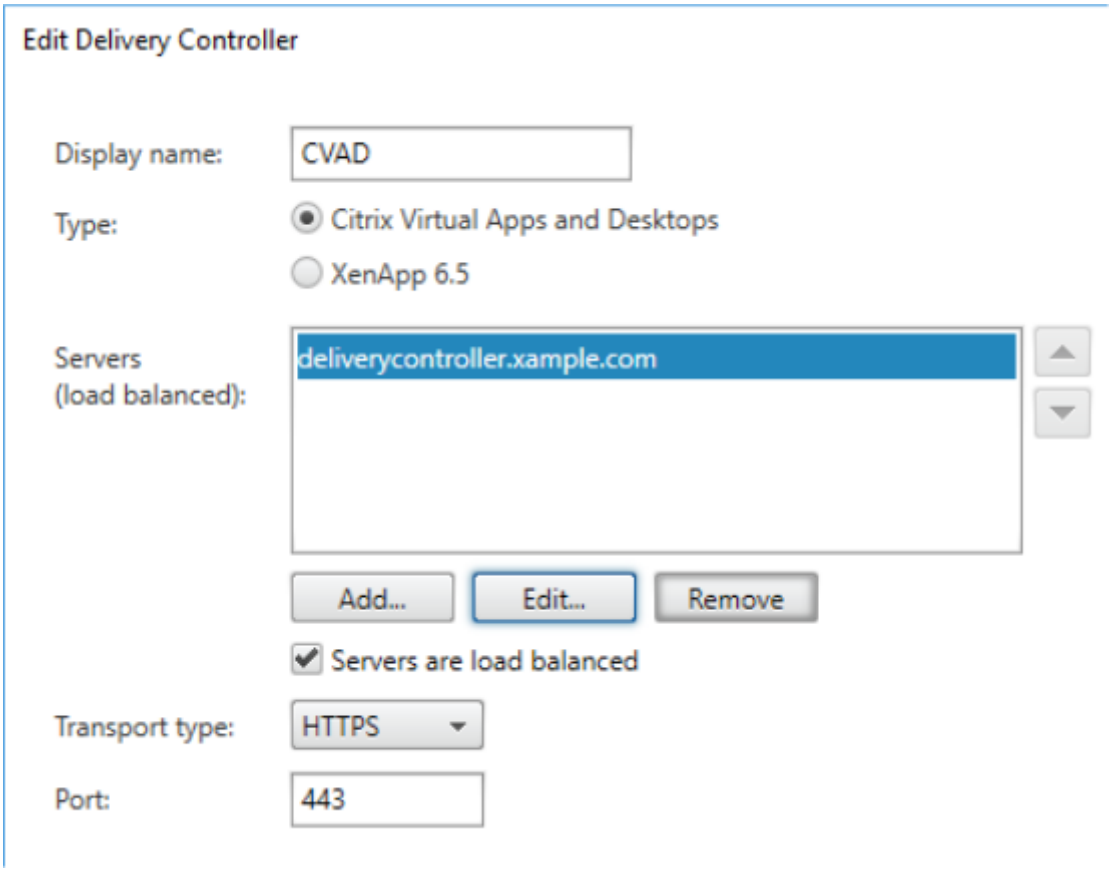
1. Sur l'écran **Démarrer** de Windows ou l'écran **Applications**, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau Actions, cliquez sur **Gérer les méthodes d'authentification**.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

March 3, 2020

> Remarque :
>
> XenApp 6.5 a atteint la fin de vie (EOL) et est désormais couvert par le programme de support étendu.

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. Une fois ce processus terminé, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

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

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 Citrix Virtual Apps and Desktops XML Service 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 Citrix Virtual Apps pour la délégation

Configurez la délégation approuvée Active Directory pour chaque serveur Citrix Virtual Apps.

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 Citrix Virtual Apps and Desktops XML Service 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 Citrix Virtual Apps and Desktops XML Service 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.
- Citrix 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 Citrix 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 Citrix 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 serveur virtuel Citrix Gateway non authentifié.
- Citrix Receiver pour Windows ou l'application Citrix Workspace 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 ou l'application Citrix Workspace pour Windows (AuthManager), Kerberos et StoreFront :
  - Vous n'avez pas besoin de ssonsvr.exe sur le client.
  - Vous pouvez définir un nom d'utilisateur et un mot de passe locaux quelconques dans le modèle icaclient.adm Citrix (contrôle la fonction ssonsvr.exe).
  - Le paramètre Kerberos du modèle icaclient.adm est requis.
  - Cochez la case Utiliser le nom de l'utilisateur local dans les paramètres de sécurité d'Internet Explorer pour la zone de confiance.
  - Le client doit figurer dans un domaine.
  - Activez la méthode d'authentification Authentification pass-through au domaine sur le serveur StoreFront.
  - Assurez-vous que cette clé de registre est définie :

    > **Avertissement :**
    > Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. 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\AuthManagerP
    Nom : SSONCheckEnabled
    Type : REG_SZ
    Valeur : true ou false

Configuration de l'authentification par carte à puce

March 3, 2020

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.

> Remarque :
>
> Dans cet article, les mentions de « Application Citrix Workspace » représentent également les versions prises en charge de Citrix Receiver, sauf indication contraire.

Composants requis

- 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 Citrix Virtual Desktops, 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 Citrix Gateway

- Sur votre appliance Citrix 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 appliance Citrix 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 Citrix Gateway.

- Créez et configurez un serveur virtuel pour l'authentification du certificat client. Créez une stratégie d'authentification de certificat, en spécifiant SubjectAltName:PrincipalName pour l'extraction du nom d'utilisateur à partir du certificat. Ensuite, liez la stratégie au serveur virtuel et configurez le serveur virtuel pour demander des certificats clients. Pour de plus amples informations, consultez la section Configuration et liaison d'une stratégie d'authentification 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 de plus amples informations, consultez 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 Citrix 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 Citrix Gateway vers StoreFront et liez-les au serveur virtuel approprié. Pour de plus amples informations, consultez la section Accès à StoreFront via Citrix 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 de l'appliance Citrix 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 de plus amples informations, consultez 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. Pour plus d'informations sur l'ajout de liaison HTTPS à un site IIS, consultez 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 Citrix 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 Citrix 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 Citrix Gateway, activez la méthode d'authentification pass-through avec Citrix Gateway et assurez-vous que StoreFront est configuré pour déléguer la validation des informations d'identification à Citrix Gateway. Si vous prévoyez d'activer l'authentification pass-through lorsque vous installez Citrix Receiver pour Windows ou l'application Citrix Workspace 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 ou l'application Citrix Workspace 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 de plus amples informations, consultez la section Activer l'authentification pass-through par carte à puce pour Citrix Receiver pour Windows ou l'application Citrix Workspace pour Windows.
- Si vous avez créé un serveur virtuel Citrix Gateway supplémentaire à utiliser uniquement pour les connexions utilisateur aux ressources, configurez le routage Citrix Gateway optimal via ce serveur virtuel pour les connexions aux déploiements fournissant des bureaux et des applications au magasin. Pour de plus amples informations, consultez la section Configurer un routage HDX optimal pour un magasin.
- Pour permettre aux utilisateurs de PC exécutant Citrix Desktop Lock de s'authentifier à l'aide de cartes à puce, activez l'authentification pass-through avec carte à puce sur vos adresses URL XenApp Services. Pour de plus amples 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 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 Workspace sur la machine utilisateur. Pour activer l'authentification unique des informations d'identification de la carte à puce sur Citrix Virtual Apps and Desktops pour les utilisateurs dont les machines appartiennent au domaine, utilisez un compte avec des autorisations d'administrateur pour installer l'application Citrix Workspace pour Windows à partir d'une invite de commandes avec

l'option **/includeSSON**. Pour de plus amples informations, consultez la section Utilisation des paramètres de ligne de commande.

Assurez-vous que l'application Citrix Workspace pour Windows est configurée 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 de l'application Citrix Workspace 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 Carte à puce.

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 Citrix Virtual Apps and Desktops, 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 Citrix Virtual Apps and Desktops 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 l'appliance Citrix 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 Référence des paramètres ICA.

Activer l'authentification pass-through par carte à puce pour Receiver pour Windows ou l'application Citrix Workspace 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 Citrix Virtual Apps and Desktops, 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 Citrix 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 Citrix Gateway, ajoutez le paramètre suivant dans la section [Application].

   ```
   UseLocalUserAndPassword=On
   ```

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

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

March 3, 2020

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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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

January 8, 2020

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

Tâche	Détail
Créer ou supprimer un magasin	Permet de configurer autant de magasins supplémentaires que vous le souhaitez.
Créer un magasin non authentifié	Permet de configurer des magasins non authentifiés supplémentaires afin de permettre l'accès des utilisateurs non authentifiés (anonymes).

Tâche	Détail
Exporter des fichiers de provisioning de magasin pour des utilisateurs	Permet de générer des fichiers contenant les détails de connexion aux magasins, y compris tout déploiement Citrix Gateway et balise configurés pour les magasins.
Masquer et publier des magasins pour les utilisateurs	Empêchez les utilisateurs d'ajouter des magasins à leurs comptes lorsqu'ils configurent l'application Citrix Workspace via la découverte de compte basée sur une adresse e-mail ou un nom de domaine complet.
Gérer les ressources mises à disposition dans les magasins	Permet d'ajouter et de supprimer des ressources de magasins.
Gérer l'accès distant aux magasins via Citrix Gateway	Permet de configurer l'accès aux magasins via Citrix Gateway pour les utilisateurs se connectant depuis des réseaux publics.
Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun	Permet de configurer deux magasins StoreFront pour partager une base de données d'abonnement commune.
Paramètres de magasin avancés	Configurez les paramètres avancés du magasin.

Créer ou supprimer un magasin

March 3, 2020

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.

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 Citrix Gateway.

Sur la page Nom du magasin, lorsque vous sélectionnez **Autoriser uniquement les utilisateurs non authentifiés à accéder à ce magasin**, vous pouvez créer un magasin non authentifié, qui est anonyme (ou non authentifié). Lorsque vous créez un magasin non authentifié, les pages **Méthodes d'authentification** et **Accès distant** ne sont pas disponibles ; les panneaux de gauche **Nœud Groupe**

de serveurs et Action sont remplacés par **Changer l'URL de base**. (Il s'agit de la seule option disponible, car les groupes de serveurs ne sont pas disponibles dans des serveurs n'appartenant pas à un domaine.)

> 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 l'application Citrix Workspace 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 d'affichage** qui vous aidera à identifier le déploiement. Spécifiez le **Type** pour indiquer comment les ressources mises à disposition dans le magasin sont fournies. Tapez les valeurs par défaut sur Citrix Virtual Apps and Desktops. XenApp 6.5 est disponible en tant que Type, mais il a atteint sa fin de vie en juin 2018 et est désormais couvert par le Programme de support étendu.
6. Pour mettre des bureaux et applications fournis par Citrix Virtual Apps and Desktops et XenApp 6.5 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 Citrix Virtual Apps and Desktops, spécifiez les détails des Delivery Controller. Dans le cas de batteries XenApp 6.5, dressez la liste des serveurs exécutant le service XML Citrix.
7. Dans la liste **Type de transport**, sélectionnez 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 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 Citrix Virtual Apps and Desktops, 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 6.5 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 Citrix Virtual Apps and Desktops, 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 6.5, indiquez le port TCP du Relais SSL dans **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 de déploiements Citrix Virtual Apps and Desktops. 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 **Suivant**.
11. 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 Citrix 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, sélectionnez **Activer l'accès à distance**.

- Pour ne mettre à disposition que les ressources disponibles au travers du magasin via Citrix Gateway, sélectionnez **Aucun tunnel VPN**. Les utilisateurs ouvrent une session à l'aide d'ICAProxy ou d'un VPN sans client (CVPN) à Citrix Gateway et n'ont pas besoin d'utiliser Citrix Gateway Plug-in pour établir un VPN complet.
- 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 Citrix Gateway Plug-in pour établir le tunnel VPN.

Lorsque vous activez l'accès à distance au magasin, la méthode d'authentification **Authentification pass-through via Citrix Gateway** est automatiquement activée. Les utilisateurs s'authentifient sur Citrix Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

12. Si vous avez activé l'accès à distance, sélectionnez dans la liste **Appliances Citrix Gateway**, sélectionnez les appliances (déploiements) par le biais desquels les utilisateurs peuvent accéder 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 activez l'accès au travers de plusieurs appliances en sélectionnant plus d'une entrée dans la liste, spécifiez l'**appliance par défaut** à utiliser pour accéder au magasin. Pour ajouter d'autres appliances à la liste, suivez la procédure décrite dans la section Fournir l'accès distant au magasin via Citrix Gateway.

13. 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 Citrix Gateway :** les utilisateurs s'authentifient sur Citrix Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Cette option est automatiquement activée lorsque l'accès distant est activé.1. Sur la page **Configurer la validation du mot de passe**, sélectionnez les Delivery Controller qui fourniront la validation du mot de passe et cliquez sur **Suivant**.

14. 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**.
15. Une fois que le magasin a été créé, cliquez sur **Terminer**.

Accès au magasin

Les utilisateurs peuvent désormais accéder à votre magasin avec l'application Citrix Workspace, 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 de plus amples informations, consultez 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 PC 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.

Fournir l'accès distant au magasin via Citrix Gateway

Effectuez les étapes suivantes pour configurer l'accès distant via Citrix 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**, cliquez sur **Ajouter**.
2. Sur la page **Ajouter une appliance Citrix Gateway**, sur la page **Paramètres généraux**, spécifiez un **nom d'affichage** pour l'appliance Citrix Gateway qui permettra aux utilisateurs de l'identifier.

   Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans l'application Citrix Workspace. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser cette passerelle. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements

Citrix Gateway pour permettre aux utilisateurs d'identifier facilement la passerelle la plus pratique ou la plus proche en fonction de leur situation.

3. Pour **URL de Citrix Gateway**, tapez la combinaison URL:port du serveur virtuel Citrix Gateway pour votre déploiement. Si aucun port n'est spécifié, alors le port par défaut `https://` de 443 est utilisé. Il n'est pas nécessaire de spécifier le port 443 dans l'URL.

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

4. Sélectionnez **Utilisation ou rôle** de Citrix Gateway dans les options disponibles.

   - **Authentification et routage HDX :** Citrix Gateway sera utilisé pour l'authentification, ainsi que pour le routage des sessions HDX.
   - **Authentification uniquement :** Citrix Gateway sera utilisé pour l'authentification mais pas pour le routage des sessions HDX.
   - **Routage HDX uniquement :** Citrix Gateway sera utilisé pour le routage des sessions HDX mais pas pour l'authentification.

5. Pour tous les déploiements sur lesquels vous mettez les ressources fournies par Citrix Virtual Apps and Desktops ou XenApp 6.5 à disposition dans le magasin, sur la page **Secure Ticket Authority** (STA), répertoriez les adresses URL STA des serveurs qui exécutent la 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 Citrix Virtual Apps and Desktops ou XenApp 6.5, et émet des tickets de session en réponse aux demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources Citrix Virtual Apps and Desktops ou XenApp 6.5. Utilisez l'URL STA correcte (telle que `HTTPS://` ou `HTTP://`) en fonction de la configuration de vos Delivery Controller. L'URL STA doit également être identique à celle configurée dans Citrix Gateway sur votre serveur virtuel.

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. Pour vous assurer que Citrix Virtual Apps and Desktops ou XenApp 6.5 maintiennent les sessions déconnectées ouvertes pendant que l'application Citrix Workspace tente de se reconnecter automatiquement, sélectionnez **Activer la fiabilité de session**.

8. Si vous configurez plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, sélectionnez **Demander des tickets de deux STA, si possible**. StoreFront obtient des tickets de deux STA différentes et les sessions utilisateur ne sont pas interrompues si l'une des STA devient 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. Dans la page **Paramètres d'authentification**, tapez l'**Adresse IP de vServer** de l'appliance Citrix Gateway.

   Utilisez l'adresse IP privée du serveur virtuel Citrix Gateway plutôt que l'adresse IP publique qui est routée vers l'adresse IP privée. Les passerelles sont généralement identifiées par StoreFront via leurs URL. Si vous utilisez l'équilibrage de charge globale du serveur (GSLB), vous devez ajouter le VIP à chaque passerelle. Cela permet à StoreFront d'identifier plusieurs passerelles qui utilisent toutes la même URL (nom de domaine GSLB) comme des passerelles distinctes. Par exemple, trois passerelles peuvent être configurées pour le magasin avec la même URL telle que `https://gslb.domain.com` mais elles auraient chacune des VIP uniques configurées telles que 10.0.0.1, 10.0.0.2 et 10.0.0.3.

10. Si vous ajoutez une appliance exécutant Citrix Gateway, sélectionnez dans la liste **Type d'ouverture de session** la méthode d'authentification que vous avez configurée sur l'appliance pour les utilisateurs de l'application Citrix Workspace.

    - 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 parmi 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**.

11. Si vous configurez StoreFront pour Citrix Gateway et que vous souhaitez utiliser Smart Access, vous devez taper une **URL de rappel**. StoreFront ajoute automatiquement la partie standard de l'URL. Entrez l'adresse URL de l'appliance accessible en interne. StoreFront contacte le service d'authentification Citrix Gateway pour vérifier que les requêtes reçues de Citrix Gateway proviennent de cette appliance.

    Lorsque vous utilisez GSLB, nous vous recommandons de configurer des URL de rappel uniques pour chacune de vos passerelles GSLB. StoreFront doit être capable de faire correspondre chacune des URL de rappel uniques avec les VIP privés configurés pour chacun des serveurs virtuels de passerelle GSLB. Par exemple, `emeagateway.domain.com`, `usgateway.domain.com` et `apacgateway.domain.com` devraient correspondre à la passerelle VIP correcte.

12. Cliquez sur **Créer** pour ajouter votre appliance Citrix Gateway à la liste dans la boîte de dialogue **Paramètres d'accès à distance**.

    Les informations sur la configuration de vos appliances Citrix Gateway sont enregistrées dans le fichier de provisioning .cr du magasin. Ceci permet à l'application Citrix Workspace d'envoyer une demande de connexion appropriée lorsque vous contactez les appliances pour la première fois.

Supprimer un magasin

Utilisez la tâche Supprimer le magasin pour supprimer un magasin. Lorsque vous supprimez un magasin, les sites Receiver pour Web 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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

Créer un magasin non authentifié

March 3, 2020

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 Citrix 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 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 ce processus terminé,

> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 Citrix Virtual Apps and Desktops ou par XenApp 6.5. (Notez que XenApp 6.5 a atteint la fin de son cycle de vie et est désormais couvert par le programme de support étendu.) Lorsque vous attribuez des Delivery 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.

   Pour mettre des bureaux et des applications fournis par des batteries XenApp 6.5 à disposition dans le magasin, ajoutez les noms de chaque serveur individuel de la batterie 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 Citrix Virtual Desktops, spécifiez les détails des Controller. Pour les batteries XenApp 6.5, dressez la liste des serveurs exécutant le service XML Citrix.
6. Dans la liste Type de transport, sélectionnez 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 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 Citrix Virtual Apps and Desktops, 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.

7. 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 Citrix Virtual Apps and Desktops, le port spécifié doit être le port utilisé par le service XML Citrix.
8. Cliquez sur **OK**. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison de déploiements Citrix Virtual Apps and Desktops. Répétez les étapes 4 à 9, 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, l'application Citrix Workspace doit être configurée 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 de plus amples informations, consultez 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 d'appliances 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 Store-

Front 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.

Exporter des fichiers de provisioning de magasin pour des utilisateurs

March 3, 2020

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 Citrix Gateway et les balises configurées pour les magasins. Mettez ces fichiers à la disposition des utilisateurs pour leur permettre de configurer l'application Citrix Workspace automatiquement avec les détails relatifs aux magasins. Les utilisateurs peuvent également obtenir les fichiers de provisioning de l'application Citrix Workspace à partir de sites Receiver pour 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus. Sélectionnez le nœud Magasins dans le volet 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

March 3, 2020

Utilisez la tâche Masquer le magasin pour empêcher les utilisateurs d'ajouter des magasins à leurs comptes lorsqu'ils configurent l'application Citrix Workspace 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 l'application Citrix Workspace 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 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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

March 3, 2020

Utilisez la tâche **Gérer les Delivery Controller** pour ajouter et supprimer, des magasins, des ressources fournies par Citrix Virtual Apps and Desktops, et pour modifier les détails des serveurs offrant ces 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Sélectionnez le nœud Magasin dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau Actions, cliquez sur **Gérer les Delivery Controller**.
3. Dans la boîte de dialogue Gérer les Delivery Controller :
   a) cliquez sur **Ajouter** pour inclure des bureaux et applications provenant d'un autre déploiement Citrix Virtual Apps and Desktops dans le magasin.
   b) cliquez sur **Modifier** pour modifier les paramètres d'un déploiement.
   c) Sélectionnez une entrée dans la liste des Delivery Controller, 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 un Controller ou Modifier le Controller, spécifiez un **nom d'affichage** qui vous aidera à identifier le déploiement.
5. Pour mettre des bureaux et applications fournis par Citrix Virtual Apps and Desktops 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 Citrix Virtual Desktops, spécifiez les détails des Delivery Controller. Dans le cas de batteries Citrix Virtual Apps, 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 et 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.
6. Dans la liste **Type de transport**, sélectionnez 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 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 Citrix Virtual Apps and Desktops, 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 Citrix Virtual Apps 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.

7. 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 Citrix Virtual Apps and Desktops, le port spécifié doit être le port utilisé par le service XML Citrix.
8. Si vous utilisez le Relais SSL pour sécuriser les connexions entre StoreFront et des serveurs Citrix Virtual Apps, 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.
9. Cliquez sur **OK**. Vous pouvez configurer les magasins pour fournir des ressources à partir de n'importe quelle combinaison de déploiements Citrix Virtual Apps and Desktops. Répétez les étapes 3 à 9, si nécessaire, pour ajouter des déploiements supplémentaires ou les modifier dans la liste Delivery Controller.

Gérer l'accès distant aux magasins via Citrix Gateway

March 3, 2020

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

> 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 droit 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 Citrix Gateway.

   - Pour ne pas mettre le magasin à la disposition des utilisateurs sur des réseaux publics, ne sélectionnez pas **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 mettre à disposition les ressources disponibles dans le magasin via Citrix Gateway, sélectionnez **Aucun tunnel VPN**. Les utilisateurs ouvrent une session à l'aide d'ICAProxy ou d'un VPN sans client (CVPN) à Citrix Gateway et n'ont pas besoin d'utiliser Citrix Gateway Plug-in pour établir un VPN complet.
     - 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 Citrix Gateway Plug-in pour établir le tunnel VPN.

   Lorsque vous activez l'accès à distance au magasin, la méthode d'authentification **Authentification pass-through via Citrix Gateway** est automatiquement activée. Les utilisateurs s'authentifient sur Citrix 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 **Appliances Citrix 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 14.
5. Sur la page Paramètres généraux, spécifiez un **nom d'affichage** pour l'appliance Citrix Gateway qui permettra aux utilisateurs de l'identifier.

   Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans l'application Citrix Workspace. Par conséquent, il est important d'inclure des informations utiles dans le nom pour aider les utilisateurs à se décider ou non à utiliser cette passerelle. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms affichés de vos déploiements Citrix Gateway pour permettre aux utilisateurs d'identifier facilement la passerelle la plus pratique ou la plus proche en fonction de leur situation.

6. Pour **URL de Citrix Gateway**, tapez la combinaison URL:port du serveur virtuel Citrix Gateway pour votre déploiement. Si aucun port n'est spécifié, alors le port par défaut `https://` de 443 est utilisé. Il n'est pas nécessaire de spécifier le port 443 dans l'URL.
7. Sélectionnez l'utilisation de Citrix Gateway dans les options disponibles.
   - **Authentification et routage HDX :** Citrix Gateway sera utilisé pour l'authentification, ainsi que pour le routage des sessions HDX.
   - **Authentification uniquement :** Citrix Gateway sera utilisé pour l'authentification mais pas pour le routage des sessions HDX.
   - **Routage HDX uniquement :** Citrix Gateway sera utilisé pour le routage des sessions HDX mais pas pour l'authentification.
8. Pour tous les déploiements sur lesquels vous mettez les ressources fournies par Citrix Virtual Apps and Desktops ou XenApp 6.5 à disposition dans le magasin, sur la page **Secure Ticket Authority (STA)**, répertoriez les adresses URL STA des serveurs qui exécutent la 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 Citrix Virtual Apps and Desktops ou XenApp 6.5, et émet des tickets de session en réponse aux demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources Citrix Virtual Apps and Desktops ou XenApp 6.5. Utilisez l'URL STA correcte (telle que `HTTPS://` ou `HTTP://`) en fonction de la configuration de vos Delivery Controller. L'URL STA doit également être identique à celle configurée dans Citrix Gateway sur votre serveur virtuel.
9. 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.
10. Pour vous assurer que Citrix Virtual Apps and Desktops ou XenApp 6.5 maintiennent les sessions déconnectées ouvertes pendant que l'application Citrix Workspace tente de se reconnecter automatiquement, sélectionnez **Activer la fiabilité de session**.
11. Si vous configurez plusieurs STA et si vous voulez vous assurer que la fiabilité de session est toujours disponible, sélectionnez **Demander des tickets de deux STA, si possible**. StoreFront obtient des tickets de deux STA différentes et les sessions utilisateur ne sont pas interrompues si l'une des STA devient indisponible au cours de la session. Si pour une raison quelconque, StoreFront ne parvient pas à contacter deux STA, il en utilise une seule.
12. Dans la page **Paramètres d'authentification**, tapez l'**Adresse IP de vServer** de l'appliance Citrix Gateway.

    Utilisez l'adresse IP privée du serveur virtuel Citrix Gateway plutôt que l'adresse IP publique qui est routée vers l'adresse IP privée. Les passerelles sont généralement identifiées par StoreFront via leurs URL. Si vous utilisez l'équilibrage de charge globale du serveur (GSLB), vous devez

ajouter le VIP à chaque passerelle. Cela permet à StoreFront d'identifier plusieurs passerelles qui utilisent toutes la même URL (nom de domaine GSLB) comme des passerelles distinctes. Par exemple, trois passerelles peuvent être configurées pour le magasin avec la même URL telle que `https://gslb.domain.com` mais elles auraient chacune des VIP uniques configurées telles que 10.0.0.1, 10.0.0.2 et 10.0.0.3.

13. Si vous ajoutez une appliance exécutant Citrix Gateway, sélectionnez dans la liste **Type d'ouverture de session** la méthode d'authentification que vous avez configurée sur l'appliance pour les utilisateurs de l'application Citrix Workspace.

    - 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 parmi 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**.

14. Si vous configurez StoreFront pour Citrix Gateway et que vous souhaitez utiliser Smart Access, vous devez taper une **URL de rappel**. StoreFront ajoute automatiquement la partie standard de l'URL. Entrez l'adresse URL de l'appliance accessible en interne. StoreFront contacte le service d'authentification Citrix Gateway pour vérifier que les requêtes reçues de Citrix Gateway proviennent de cette appliance.

    Lorsque vous utilisez GSLB, nous vous recommandons de configurer des URL de rappel uniques pour chacune de vos passerelles GSLB. StoreFront doit être capable de faire correspondre chacune des URL de rappel uniques avec les VIP privés configurés pour chacun des serveurs virtuels de passerelle GSLB. Par exemple, `emeagateway.domain.com`, `usgateway.domain.com` et `apacgateway.domain.com` devraient correspondre à la passerelle VIP correcte.

15. Cliquez sur **Créer** pour ajouter votre appliance Citrix Gateway à la liste dans la boîte de dialogue **Paramètres d'accès à distance**.

    Les informations sur la configuration de vos appliances Citrix Gateway sont enregistrées dans le fichier de provisioning .cr du magasin. Ceci permet à l'application Citrix Workspace d'envoyer une demande de connexion appropriée lorsque vous contactez les appliances pour la première

fois.

16. Répétez les étapes 4 à 13, si nécessaire, pour ajouter d'autres appliances Citrix Gateway à la liste des appliances Citrix Gateway. Si vous activez l'accès au travers de plusieurs appliances en sélectionnant plus d'une entrée dans la liste, spécifiez l'**appliance par défaut** à utiliser pour accéder au magasin.
17. Cliquez sur **OK** pour enregistrer la configuration et fermer la boîte de dialogue Configurer l'accès distant.

Vérification des listes de révocation de certificats (CRL)

March 3, 2020

Introduction

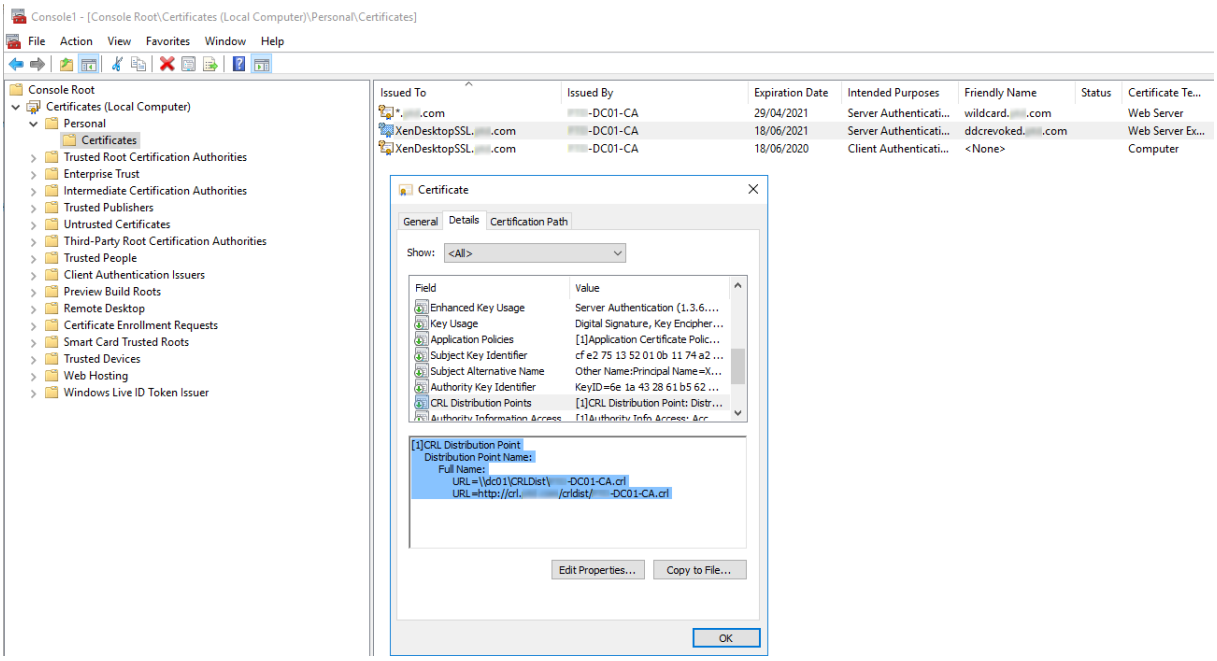
Vous pouvez configurer StoreFront pour vérifier l'état des certificats TLS utilisés par les Delivery Controller CVAD à l'aide d'une liste de révocation de certificats (CRL) publiée.
Il peut être nécessaire de révoquer l'accès à un certificat si :

- vous pensez que la clé privée a été compromise
- l'autorité de certification est compromise
- l'affiliation a été modifiée
- le certificat a été remplacé

> **Remarque :**
>
> Cette rubrique ne s'applique que lorsque des connexions HTTPS entre StoreFront et Citrix Virtual Apps and Desktops sont utilisées. Les connexions HTTP aux Delivery Controller ne nécessitant pas de certificat, le paramètre -CertRevocationPolicy pour le magasin, décrit ici, n'a aucun effet.
>
> StoreFront prend en charge la vérification de la révocation de certificats à l'aide d'extensions de certificats de points de distribution de CRL (CDP) et de listes de révocation de certificats (CRL) installées localement. StoreFront prend uniquement en charge les listes de révocation de certificats complètes : les listes delta ne sont pas prises en charge.

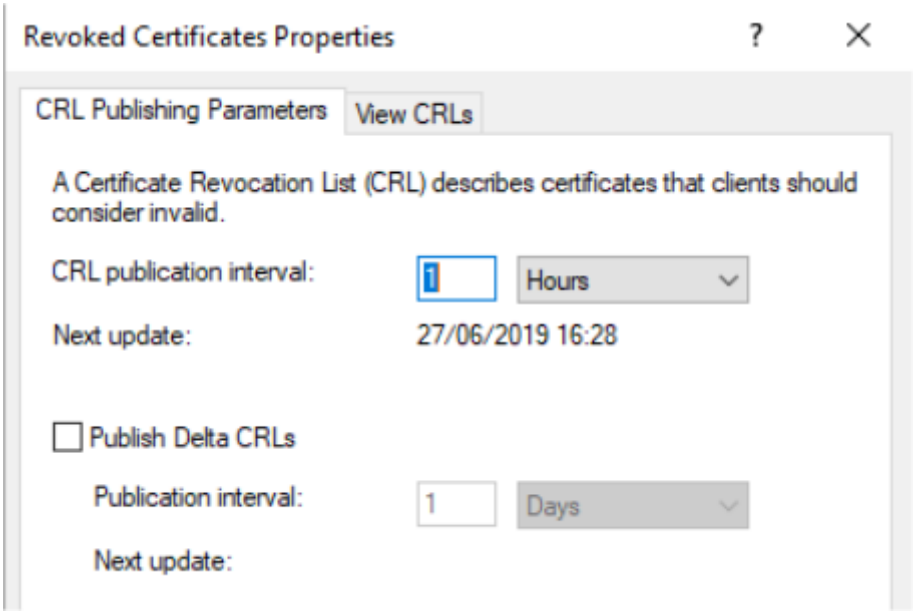
Extensions de points de distribution de CRL (CDP)

StoreFront n'énumère pas les ressources des Delivery Controller
Citrix Virtual Apps and Desktops qui utilisent des certificats révoqués dont les numéros de série sont répertoriés dans la liste de révocation de certificats publiée. Pour détecter les certificats révoqués,
StoreFront doit pouvoir accéder à la liste de révocation de certificats publiée à l'aide de l'une des URL définies dans les extensions de certificats CDP.



Intervalle de publication de CRL

Pour que StoreFront détecte plus
rapidement les certificats révoqués sur le Delivery Controller, réduisez l'intervalle de publication de la liste de révocation de certificats sur l'autorité de certification. Modifiez les propriétés de l'extension de points de distribution CLR pour définir une
valeur d'intervalle de publication CLR inférieure appropriée à votre infrastructure de clé publique.



Mise en cache de la liste de révocation de certificats client

Le client d'infrastructure de clé publique Windows met en cache les listes de révocation de certificats localement. Une nouvelle liste de révocation de
certificats n'est pas téléchargée tant que la liste de révocation de certificats mise en cache localement n'a pas expiré.

Accès de StoreFront aux listes de révocation de certificats (CRL)

La vérification de la révocation de certificats repose sur la capacité de StoreFront à accéder aux listes de révocation de certificats.
Veillez à prendre en compte la façon dont StoreFront contacte le serveur Web ou
l'autorité de certification qui publie la liste de révocation de certificats et la façon dont StoreFront reçoit les mises à jour des listes de révocation de certificats.

Autorités de certification internes d'entreprise et certificats privés sur les Delivery Controller

Pour utiliser des autorités de certification et des certificats privés, StoreFront nécessite
une autorité de certification d'entreprise correctement configurée et une liste de révocation de certificats publiée à laquelle il peut accéder au sein de votre organisation
et du réseau interne. Reportez-vous à la documentation Microsoft pour plus d'informations sur la configuration de l'autorité de certification d'entreprise pour publier des extensions CDP. Il peut être nécessaire d'émettre de nouveau tous les certificats de
vos Delivery Controller, qui existaient avant la configuration de l'autorité de certification pour inclure

des extensions
CDP.

Les serveurs StoreFront et Citrix Virtual Apps and Desktops se trouvent souvent
dans des réseaux privés isolés sans accès à Internet. Dans ce scénario, des autorités de certification privées devraient être utilisées.

Autorités de certification publiques externes et certificats publics sur les Delivery Controller

Les serveurs StoreFront et les Delivery Controller Citrix Virtual Apps and Desktops peuvent
utiliser des certificats émis par des autorités de certification publiques. StoreFront doit pouvoir contacter le serveur Web de l'autorité de certification
publique via Internet, en utilisant l'URL référencée dans les
extensions CDP. Si StoreFront ne peut pas télécharger une copie de la liste de révocation de certificats à l'aide d'une URL CDP
après la révocation d'un certificat public, StoreFront ne peut pas effectuer la vérification de la liste de révocation de certificats.

paramètres de stratégie de révocation de certificats

Utilisez les applets de commande PowerShell de Citrix StoreFront **Get-STFStoreFarmConfiguration** et **Set-STFStoreFarmConfiguration** pour définir la stratégie de révocation de certificats
pour un magasin. L'exécution de **Get-Help Set-STFStoreFarmConfiguration -detailed**
affiche l'aide de PowerShell et des exemples contenant l'option
-CertRevocationPolicy. Pour plus d'informations sur ces applets de commande PowerShell de StoreFront,
reportez-vous à la section Citrix StoreFront SDK PowerShell Modules.

L'option **-CertRevocationPolicy** peut être définie sur les valeurs suivantes :

Paramètre	Description
NoCheck	StoreFront ne vérifie pas l'état de révocation du certificat sur le Delivery Controller. StoreFront énumère les ressources des Delivery Controller qui utilisent des certificats révoqués. C'est le réglage par défaut.

Paramètre	Description
MustCheck	C'est l'option la plus sûre. StoreFront tente d'obtenir une liste de révocation de certificats en contactant les URL référencées dans les extensions CDP du certificat sur le Delivery Controller. StoreFront ne parvient pas à énumérer à partir du Delivery Controller si la liste de révocation de certificats n'est pas disponible ou si le certificat utilisé sur le Delivery Controller a été révoqué. L'URL peut pointer vers un serveur Web interne si le certificat est privé, ou vers un serveur Web Internet public si le certificat est émis par une autorité de certification publique.
FullCheck	StoreFront tente de contacter les URL publiées dans les extensions CDP du certificat de Delivery Controller. Si StoreFront ne parvient pas à obtenir une copie de la liste de révocation de certificats à partir des URL, il permet toujours l'énumération des ressources à partir du Delivery Controller. Si StoreFront obtient avec succès la liste de révocation de certificats et que le certificat du Delivery Controller a été révoqué, StoreFront n'énumère pas les ressources. L'URL peut pointer vers un serveur Web interne si le certificat est privé, ou vers un serveur Web Internet public si le certificat est émis par une autorité de certification publique.

Paramètre	Description
NoNetworkAccess	Seules les listes de révocation de certificats importées localement dans le magasin de certificats de Citrix Delivery Services sur le serveur StoreFront sont vérifiées. StoreFront ne tente pas de contacter l'une des URL spécifiées dans les extensions CDP. Si StoreFront ne parvient pas à obtenir une copie locale de la liste de révocation de certificats, il permet quand même l'énumération des ressources à partir du Delivery Controller. Si StoreFront obtient avec succès une copie locale de la liste de révocation de certificats à partir du magasin de certificats de Citrix Delivery Services et que le certificat du Delivery Controller a été révoqué, StoreFront n'énumère pas les ressources.

Configurer un magasin pour la vérification de la révocation de certificats

Pour définir la stratégie de révocation de certificats pour un magasin, ouvrez PowerShell ISE avec **Exécuter en tant qu'administrateur**, puis exécutez les applets de commande PowerShell suivantes. Si vous avez
plusieurs magasins, répétez cette procédure sur tous les magasins. -CertRevocationPolicy est un paramètre de
niveau magasin qui affecte tous les Delivery Controller configurés pour le
magasin spécifié dans $StoreVirtualPath.

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy
"MustCheck"
```

Pour vérifier que le paramètre a été correctement appliqué ou pour afficher la configuration -CertRevocationPolicy actuelle, exécutez la commande suivante :


```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
   CertRevocationPolicy
```

Utilisation de listes de révocation de certificats importées localement sur le serveur StoreFront

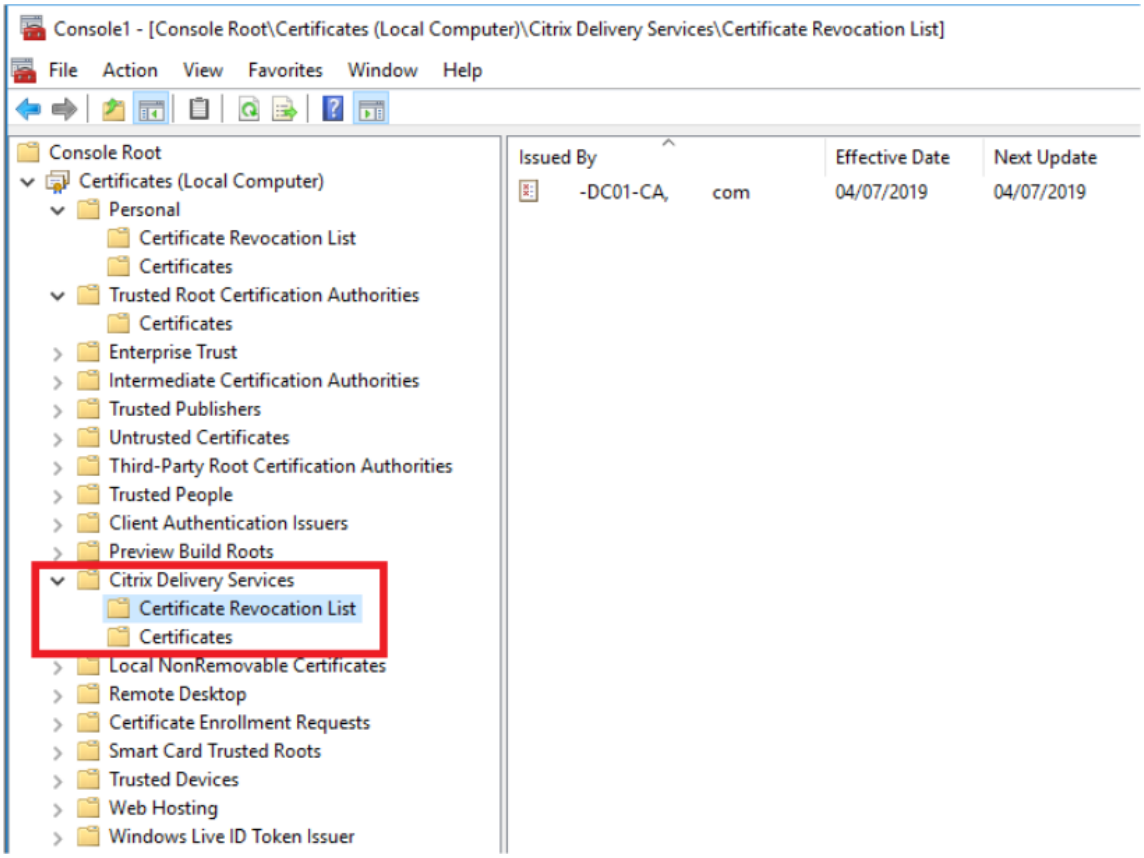
L'utilisation de listes de révocation de certificats importées localement est prise en charge, mais Citrix ne le recommande pas
car :

- Elles sont difficiles à gérer et à mettre à jour dans les déploiements de grandes entreprises, où plusieurs groupes de serveurs StoreFront peuvent être impliqués.
- La mise à jour manuelle de listes de révocation de certificats sur chaque serveur StoreFront, chaque fois qu'un certificat est révoqué, est beaucoup moins efficace que l'utilisation d'extensions CDP et de
  listes de révocation de certificats publiées sur l'ensemble du domaine Active Directory.

L'utilisation de listes de révocation de certificats mises à jour ou installées localement est possible si -CertRevocationPolicy est
défini sur "NoNetworkAccess" et que vous avez les moyens de distribuer
efficacement la liste de révocation de certificats à tous les serveurs StoreFront.

Pour utiliser des listes de révocation de certificats importées localement

1. Copiez la liste de révocation de certificats sur le bureau du serveur StoreFront. Si le serveur StoreFront fait
   partie d'un groupe de serveurs, copiez-le sur tous les serveurs StoreFront du groupe.
2. Ouvrez le composant logiciel enfichable MMC et sélectionnez **File > Add/remove Snapins > Certificates > Computer Account > Citrix Delivery Services certificate store**.
3. Cliquez avec le bouton droit de la souris et sélectionnez **All Tasks > Import**, puis accédez au fichier .CRL
   et choisissez **Select All Files > Open > Place all certificates in the following Store > Citrix Delivery Services**.



Pour ajouter la liste de révocation de certificats au magasin de certificats de Citrix Delivery Services via PowerShell ou la ligne de commande

1. Connectez-vous à StoreFront et copiez le fichier .CRL sur le bureau de l'utilisateur actuel.
2. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.
3. Exécutez la commande suivante :

```
certutil -addstore "Citrix Delivery Services" "$env:UserProfile\
    Desktop\Example-DC01-CA.crl"
```

En cas de succès, les informations suivantes sont renvoyées :

```
Citrix Delivery Services
CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.
CertUtil: -addstore command completed successfully.
```

Vous pouvez utiliser cette commande comme exemple pour distribuer automatiquement la liste de révocation de certificats à tous les serveurs StoreFront de votre déploiement via des scripts.

Authentification XML à l'aide de Delivery Controller

Vous pouvez configurer StoreFront pour déléguer l'authentification utilisateur aux Delivery Controller Citrix Virtual Apps and Desktops. Les utilisateurs ne peuvent pas se connecter à StoreFront si le certificat du Delivery Controller a été révoqué. Ce comportement est souhaitable car les utilisateurs Active Directory ne devraient pas être en mesure de se connecter à StoreFront si le certificat sur le Delivery Controller Citrix Virtual Apps and Desktops, responsable de leur authentification, a été révoqué.

Pour déléguer l'authentification utilisateur aux Delivery Controller

1. Configurez le magasin pour la révocation des certificats comme décrit dans la section précédenteConfigurer un magasin pour la vérification de la révocation de certificats.
2. Configurez le Delivery Controller pour qu'il utilise HTTPS, en suivant la procédure décrite à la section Authentification basée sur le service XML.

Configurer un service d'authentification XML pour la vérification de la révocation de certificats

Ces étapes ne sont requises que si vous utilisez l'authentification XML dans votre déploiement.

> **Remarque :**
>
> StoreFront prend en charge deux modèles de mappage des magasins vers un service d'authentification. L'approche recommandée est un mappage un-à-un entre le magasin et le service d'authentification. Dans ce cas, vous devez effectuer les étapes de cette section sur tous les magasins et leurs services d'authentification respectifs.
>
> Assurez-vous que le mode de révocation de certificat est défini sur la même valeur pour le magasin et le service d'authentification. Sinon, si la configuration d'authentification est identique pour tous les magasins, plusieurs magasins peuvent être configurés pour partager un service d'authentification unique.

Les applets de commande PowerShell du service d'authentification n'ont pas d'équivalent à **Set-STFStoreFarmConfiguration**, donc une approche PowerShell légèrement différente est requise. Utilisez les paramètres de stratégie de révocation de certificats décrits dans la section précédente.

1. Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.


```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$AuthVirtualPath = "/Citrix/StoreAuth"
```

2. Sélectionnez le service de magasin, le service d'authentification et le Delivery Controller à utiliser pour l'authentification XML. Assurez-vous que le Delivery Controller est déjà configuré pour le magasin.

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName "CVAD"
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
```

3. Modifiez directement la propriété CertRevocationPolicy du service d'authentification.

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
```

4. Vérifiez que vous avez défini le mode de révocation de certificat correct.

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
```

Erreurs de l'Observateur d'événements Windows

Lorsque la vérification des listes de révocation de certificats est activée, des erreurs sont signalées dans l'Observateur d'événements Windows sur le serveur StoreFront.

Pour ouvrir l'Observateur d'événements :

- Sur le serveur StoreFront, tapez **Run**.
- Tapez **eventvwr**, puis appuyez sur Entrée.
- Dans Applications et services, recherchez les événements Citrix Delivery Services.

Exemple d'erreur : le magasin ne peut pas contacter un Delivery Controller avec un certificat révoqué

```
Une connexion SSL n'a pas pu être établie : une erreur s'est produite
    lors de la cryptographie SSL :
l'accés est refusé.

Ce message a été signalé à partir du service XML Citrix à l'adresse
https://deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.

Le service XML Citrix spécifié n'a pas pu être contacté et a été
    temporairement
supprimé de la liste des services actifs.
```

Exemple d'erreur : depuis Receiver pour Web, si l'utilisateur ne peut pas se connecter en raison de l'échec de l'authentification XML

```
Une réponse inattendue a été reçue durant le processus d'
    authentification.

Citrix.DeliveryServicesClients.Authentication.Exceptions.
    ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

Échec général de l'authentification

ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
    LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
    GetExplicitAuthResult(ActionType
type, Dictionary`2 postParams)
```


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

April 5, 2019

Le processus d'installation de StoreFront installe un magasin de données Windows localement sur chaque serveur StoreFront pour stocker ses données d'abonnement. 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 Citrix 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 Citrix Virtual Apps and Desktops 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 :

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

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

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

Gérer les données d'abonnement d'un magasin

June 13, 2019

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.

```
function Remove-SubscriptionData

{

        [CmdletBinding()]

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

        $SubsService = "Citrix Subscriptions Store"

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



```
12
13          $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
                Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store*"
14
15          Stop-Service -displayname $SubsService
16
17          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-identifier> <resource-id> <subscription-id> <subscription-status> <property-name> <property-value> <property-name> <property-value> ...`

où :

- `<user-identifier>` - 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 une application Citrix Workspace). 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

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

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

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

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

stocker les données d'abonnement à l'aide de Microsoft SQL Server

March 3, 2020

> **Remarque :**
>
> Ce document part du principe que vous disposez d'une connaissance de base des requêtes MS SQL Server et T-SQL. Les administrateurs doivent savoir comment configurer, utiliser et gérer SQL Server avant de tenter de suivre ce document.

Introduction

ESENT est un moteur de base de données transactionnel intégré que Windows peut utiliser. Toutes les versions de StoreFront prennent en charge l'utilisation d'une base de données ESENT intégrée par défaut. Elles peuvent également se connecter à une instance Microsoft SQL Server si le magasin est configuré pour utiliser une chaîne de connexion SQL.

Le principal avantage d'utiliser StoreFront avec SQL au lieu d'ESENT est que les instructions de mise à jour T-SQL vous permettent de gérer, de modifier ou de supprimer des enregistrements d'abonnement. Si vous utilisez SQL, vous n'avez pas besoin d'exporter, de modifier et de réimporter

l'intégralité des données d'abonnement ESENT chaque fois que des modifications mineures sont apportées à ces données.

Pour migrer les données d'abonnement existantes ESENT vers Microsoft SQL Server, les données ESENT plates exportées depuis StoreFront doivent être converties en un format SQL convivial pour une importation en bloc. Pour les nouveaux déploiements sans nouvelles données d'abonnement, cette étape n'est pas requise. L'étape de transformation des données n'est nécessaire qu'une seule fois. Cet article décrit la configuration prise en charge qui peut être utilisée dans toutes les versions de StoreFront à partir de la version 3.5, qui a introduit le SDK -STF PowerShell référencé dans l'article.

> **Remarque :**
>
> Les échecs de connexion à l'instance SQL Server utilisée par StoreFront pour stocker les données d'abonnement en raison de pannes réseau ne rendent pas le déploiement StoreFront inutilisable. Les pannes entraînent uniquement une expérience utilisateur temporairement dégradée ; les utilisateurs ne peuvent pas ajouter, supprimer ou afficher leurs ressources préférées tant que la connexion à l'instance SQL Server n'est pas restaurée. Les ressources peuvent toujours être énumérées et lancées pendant la panne. Le comportement attendu est le même que si le service Citrix Subscription Store devait s'arrêter lors de l'utilisation d'ESENT.
>
> **Conseil :**
>
> Les ressources configurées avec la chaîne KEYWORDS:Auto ou KEYWORDS:Mandatory se comportent de la même manière lorsque vous utilisez ESENT ou SQL. Les nouveaux enregistrements d'abonnement SQL sont créés automatiquement lorsqu'un utilisateur ouvre une session pour la première fois si l'une des chaînes KEYWORD est inclue dans les ressources de l'utilisateur.

Avantages de ESENT et SQL Server

ESENT	SQL
Par défaut et ne nécessite aucune configuration supplémentaire pour utiliser une instance StoreFront prête à l'emploi.	Beaucoup plus facile à gérer ; les données d'abonnement peuvent être manipulées ou mises à jour facilement à l'aide de requêtes T-SQL. Permet la suppression ou la mise à jour des enregistrements par utilisateur. Facilite le comptage des enregistrements par application, Delivery Controller ou utilisateur. Facilite la suppression des données utilisateur inutiles pour les employés qui ont quitté l'entreprise/l'organisation. Facilite la mise à jour des références du Delivery Controller, par exemple lorsque l'administrateur passe à l'utilisation de l'agrégation ou lorsque de nouveaux Delivery Controller sont provisionnés.
Facilite la configuration de réplication entre différents groupes de serveurs à l'aide de la synchronisation des abonnements et des planifications d'extraction. Voir Configurer la synchronisation des abonnements	Déconnecté de StoreFront ; vous n'avez pas besoin de sauvegarder les données d'abonnement avant la mise à niveau de StoreFront car les données sont conservées sur une instance SQL Server distincte. La sauvegarde des abonnements est indépendante de StoreFront et utilise des stratégies et des mécanismes de sauvegarde SQL.
SQL est inutile lorsque la gestion des abonnements n'est pas requise. Si les données d'abonnement n'ont jamais besoin d'être mises à jour, ESENT répondra probablement aux besoins des clients.	Copie unique des données d'abonnement partagée par tous les membres du groupe de serveurs, ce qui réduit les risques de différences de données entre les serveurs ou les problèmes de synchronisation des données.

Inconvénients de ESENT et SQL Server

ESENT	SQL
Les données d'abonnement ne peuvent pas être gérées facilement et de manière granulaire. Exige que les manipulations d'abonnement soient effectuées dans les fichiers .txt exportés. La base de données d'abonnement dans son intégralité doit être exportée et réimportée. Des milliers d'enregistrements auront peut-être besoin d'être modifiés à l'aide de techniques de recherche et de remplacement, ce qui nécessite un travail intense et est susceptible d'entraîner des erreurs.	Nécessite une expertise et une infrastructure SQL de base. Peut nécessiter l'achat d'une licence SQL, ce qui augmente le coût total de possession du déploiement StoreFront. Cependant, une instance de base de données Citrix Virtual Apps and Desktops peut également être partagée avec StoreFront pour réduire les coûts.
Une copie de la base de données ESENT doit être conservée sur chaque serveur StoreFront dans un groupe de serveurs. Dans de rares cas, cette base de données peut être désynchronisée dans un groupe de serveurs ou entre différents groupes de serveurs.	La réplication des données d'abonnement entre les groupes de serveurs n'est pas une tâche de déploiement aisée. Elle nécessite plusieurs instances SQL et une réplication de transactions entre chaque instance par data center. Cette opération nécessite une expertise spécialisée dans MS SQL.
	Exige la migration des données depuis ESENT et leur transformation dans un format SQL convivial. Ce processus n'est requis qu'une seule fois.
	Des serveurs Windows et des licences supplémentaires peuvent être nécessaires.
	Étapes supplémentaires pour déployer StoreFront.

Scénarios de déploiement

> **Remarque :**
>
> Chaque magasin configuré dans StoreFront nécessite soit une base de données ESENT, soit une base de données Microsoft SQL si vous souhaitez prendre en charge les abonnements utilisateur. La méthode de stockage des données d'abonnement est définie au niveau du magasin dans StoreFront.

Citrix recommande que toutes les bases de données de magasin résident sur la même instance de

Microsoft SQL Server afin de réduire la complexité de gestion et les risques de mauvaise configuration.

Plusieurs magasins peuvent partager la même base de données, à condition qu'ils soient tous configurés pour utiliser la même chaîne de connexion. Peu importe s'ils utilisent différents Delivery Controller. L'inconvénient de plusieurs magasins partageant une base de données est qu'il n'y a aucun moyen de savoir à quel magasin correspond chaque enregistrement d'abonnement.

Une combinaison des deux méthodes de stockage de données est techniquement possible sur un déploiement StoreFront unique avec plusieurs magasins. Il est possible de configurer un magasin pour utiliser ESENT et un autre pour utiliser SQL. Cependant, cette méthode n'est pas recommandée en raison de la complexité accrue de gestion et la possibilité d'une mauvaise configuration.

Vous pouvez utiliser quatre scénarios pour stocker des données d'abonnement dans SQL Server :

Scénario 1 – Serveur StoreFront unique ou groupe de serveurs utilisant ESENT (par défaut)

Par défaut, toutes les versions de StoreFront depuis la version 2.0 utilisent une base de données ESENT plate pour stocker et répliquer les données d'abonnement entre les membres d'un groupe de serveurs. Chaque membre du groupe de serveurs conserve une copie identique de la base de données d'abonnement ; celle-ci est synchronisée avec tous les autres membres du groupe de serveurs. Ce scénario ne nécessite aucune étape supplémentaire de configuration. Ce scénario convient à la plupart des clients qui ne s'attendent pas à des modifications fréquentes des noms de Delivery Controller ou qui n'ont pas besoin d'effectuer des tâches de gestion fréquentes sur leurs données d'abonnement, telles que la suppression ou la mise à jour d'anciens abonnements utilisateur.

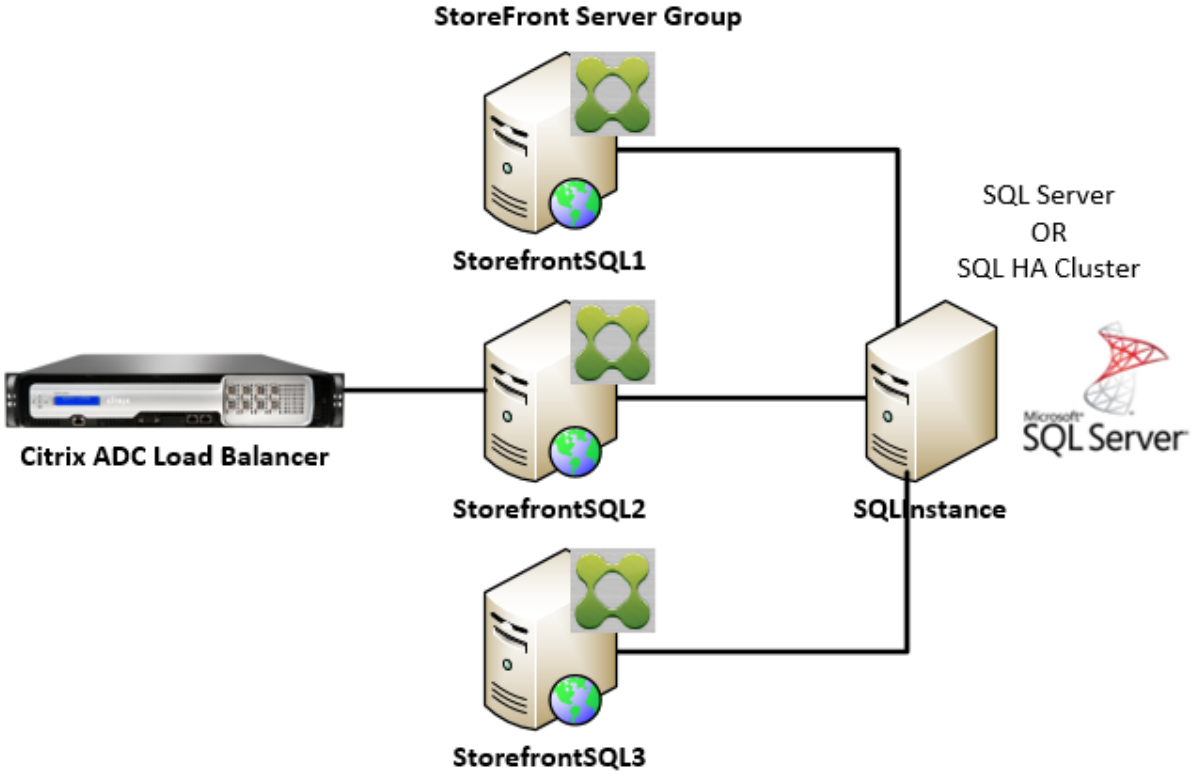
Scénario 2 – Serveur StoreFront unique et instance locale de Microsoft SQL Server installée

StoreFront utilise une instance SQL Server installée localement et les deux composants résident sur le même serveur. Ce scénario convient à un déploiement simple de StoreFront où les clients peuvent avoir besoin de modifier fréquemment les noms de Delivery Controller ou d'effectuer des tâches de gestion fréquentes sur leurs données d'abonnement, telles que la suppression ou la mise à jour d'anciens abonnements utilisateur. Cependant, dans ce scénario, les clients n'ont pas besoin d'un déploiement StoreFront haute disponibilité. Citrix ne recommande pas ce scénario pour les groupes de serveurs car il crée un point de défaillance unique sur le membre du groupe de serveurs qui héberge l'instance de base de données Microsoft SQL. Ce scénario ne convient pas aux déploiements de grande taille.

Scénario 3 – Groupe de serveurs StoreFront et instance Microsoft SQL Server dédiée configurés pour une haute disponibilité (recommandé)

Tous les membres du groupe de serveurs StoreFront se connectent à la même instance Microsoft SQL Server dédiée ou au même cluster de basculement SQL. Il s'agit du modèle le plus approprié

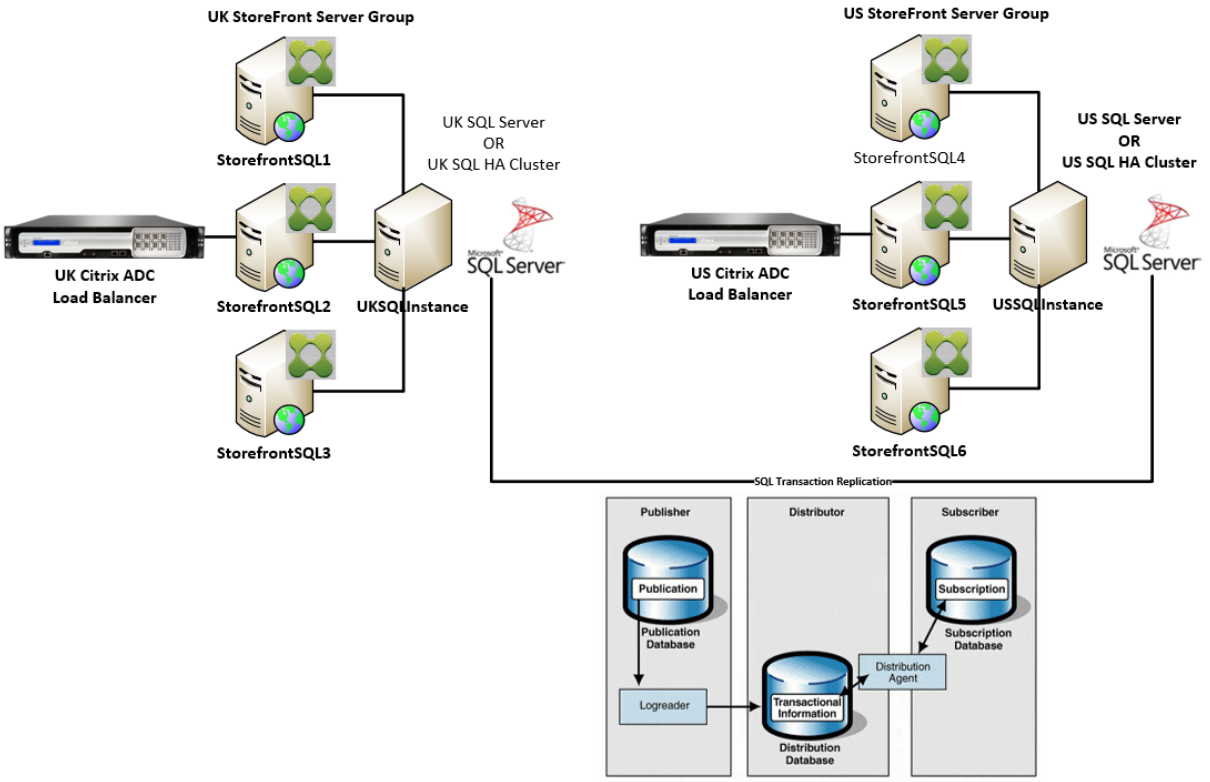
pour les déploiements de grande taille où les administrateurs Citrix souhaitent modifier fréquemment les noms de Delivery Controller ou effectuer des tâches de gestion fréquentes sur leurs données d'abonnement, telles que la suppression ou la mise à jour d'anciens abonnements utilisateur, tout en nécessitant une haute disponibilité.



Scénario 4 – Plusieurs groupes de serveurs StoreFront et instance Microsoft SQL Server dédiée dans chaque data center par groupe de serveurs

> **Remarque :**
>
> Il s'agit d'une configuration avancée. Utilisez ce scénario uniquement si vous êtes un administrateur SQL Server expérimenté connaissant bien la réplication des transactions et que vous disposez des compétences nécessaires pour déployer cette configuration.

Il s'agit de la même configuration que le scénario 3, mais ce scénario s'applique également aux situations où plusieurs groupes de serveurs StoreFront sont requis dans différents data centers distants. Les administrateurs Citrix peuvent choisir de synchroniser les données d'abonnement entre différents groupes de serveurs dans le même data center ou dans des data centers différents. Chaque groupe de serveurs du centre de données se connecte à sa propre instance Microsoft SQL Server dédiée pour la redondance, le basculement et les performances. Ce scénario nécessite une configuration et une infrastructure Microsoft SQL Server supplémentaires considérables. Il s'appuie entièrement sur la technologie Microsoft SQL pour répliquer les données d'abonnement et les transactions SQL.



Ressources

Vous pouvez télécharger les scripts suivants à partir de https://github.com/citrix/sample-scripts/tree/master/storefront pour vous aider :

Scripts de configuration

- **Set-STFDatabase.ps1** : définit la chaîne de connexion MS SQL pour chaque magasin. Exécutez ce script sur le serveur StoreFront.
- **Add-LocalAppPoolAccounts.ps1** : accorde aux pools d'applications du serveur StoreFront local un accès en lecture et en écriture à la base de données SQL. Exécutez ce script pour le scénario 2 sur l'instance SQL Server.
- **Add-RemoteSFAccounts.ps1** : accorde à tous les serveurs StoreFront d'un groupe de serveurs un accès en lecture et en écriture à la base de données SQL. Exécutez ce script pour le scénario 3 sur l'instance SQL Server.
- **Create-StoreSubscriptionsDB-2016.sql** : crée la base de données et le schéma SQL. Exécutez ce script sur l'instance SQL Server.

Scripts de transformation et d'importation de données

- **Transform-SubscriptionDataForStore.ps1** : exporte et convertit les données d'abonnement existantes dans ESENT en un format SQL convivial pour l'importation.
- **Create-ImportSubscriptionDataSP.sql** : crée une procédure stockée pour importer les données converties par le script Transform-SubscriptionDataForStore.ps1. Exécutez ce script une fois sur l'instance SQL Server après avoir créé le schéma de base de données à l'aide du script Create-StoreSubscriptionsDB-2016.sql.

Configurer le groupe de sécurité local du serveur StoreFront sur SQL Server

Scénario 2 – Serveur StoreFront unique et instance locale de Microsoft SQL Server installée

Créez un groupe de sécurité local appelé `<SQLServer>\StoreFrontServers` sur Microsoft SQL Server et ajoutez les comptes virtuels pour `IIS APPPOOL\DefaultAppPool` et `IIS APPPOOL\Citrix Receiver for Web` pour accorder au serveur StoreFront installé localement un accès en lecture et en écriture à SQL. Ce groupe de sécurité est référencé dans le script .SQL qui crée le schéma de base de données d'abonnement au magasin. Assurez-vous donc que les noms de groupe correspondent.

Vous pouvez télécharger le script Add-LocalAppPoolAccounts.ps1 pour vous aider.

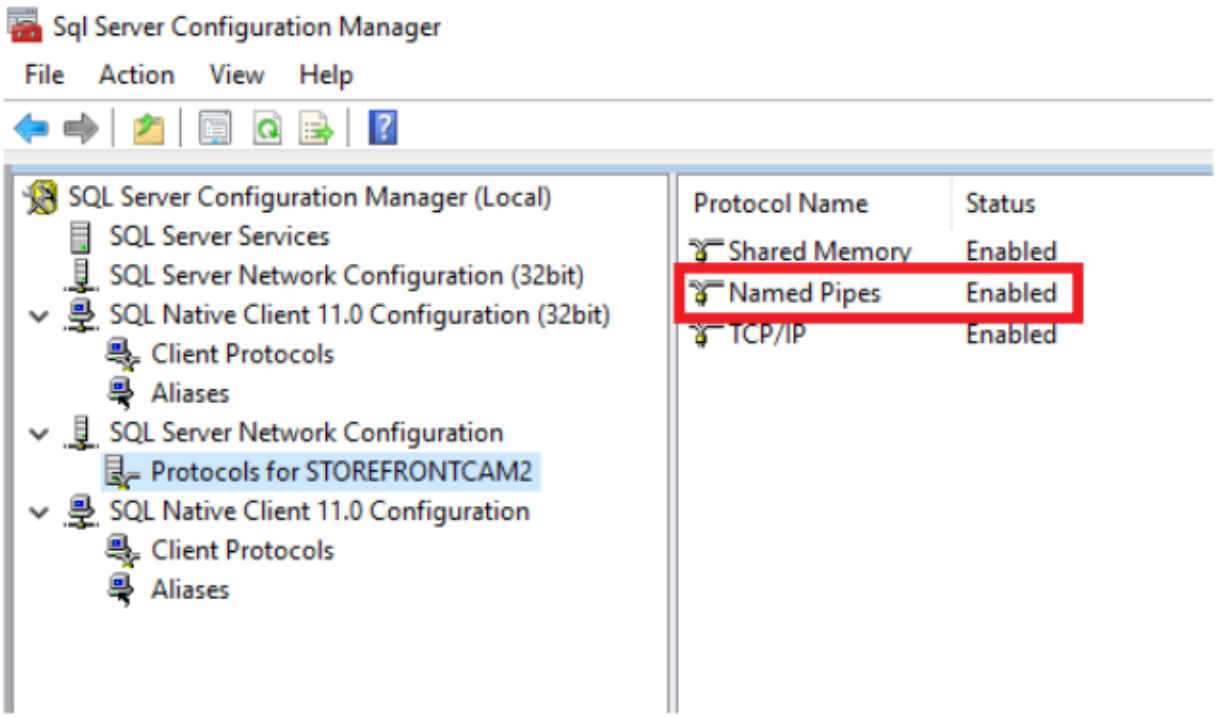
Installez StoreFront avant d'exécuter le script *Add-LocalAppPoolAccounts.ps1*. Le script dépend de la capacité de localiser le compte IIS virtuel `IIS APPPOOL\Citrix Receiver for Web`, qui n'existe pas tant que StoreFront n'a pas été installé et configuré. `IIS APPPOOL\DefaultAppPool` est créé automatiquement en installant le rôle de serveur Web IIS.

```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

# Check whether the Local Group Exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
 }

else
{

Write-Host "Creating $LocalGroupName local security group" -
    ForegroundColor "Yellow"
```



```
16
17 # Create Local User Group
18 $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
19 $LocalGroup = $Computer.Create("group",$LocalGroupName)
20 $LocalGroup.setinfo()
21 $LocalGroup.description = $Description
22 $Localgroup.SetInfo()
23 Write-Host "$LocalGroupName local security group created" -
       ForegroundColor "Green"
24  }
25
26 $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
27
28 # Add IIS APPPOOL\DefaultAppPool
29 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
       APPPOOL\DefaultAppPool")
30 $StrSID = $objAccount.Translate([System.Security.Principal.
       SecurityIdentifier])
31 $DefaultSID = $StrSID.Value
32
33 $Account = [ADSI]"WinNT://$DefaultSID"
34 $Group.Add($Account.Path)
35
36 # Add IIS APPPOOL\Citrix Receiver for Web
37 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
       APPPOOL\Citrix Receiver for Web")
38 $StrSID = $objAccount.Translate([System.Security.Principal.
       SecurityIdentifier])
39 $WebRSID = $StrSID.Value
40
41 $Account = [ADSI]"WinNT://$WebRSID"
42 $Group.Add($Account.Path)
43
44 Write-Host "AppPools added to $LocalGroupName local group" -
       ForegroundColor "Green"
```

Activez les canaux nommés dans votre instance SQL locale à l'aide du Gestionnaire de configuration SQL Server. Les canaux nommés sont requis pour la communication entre les processus entre StoreFront et SQL Server.

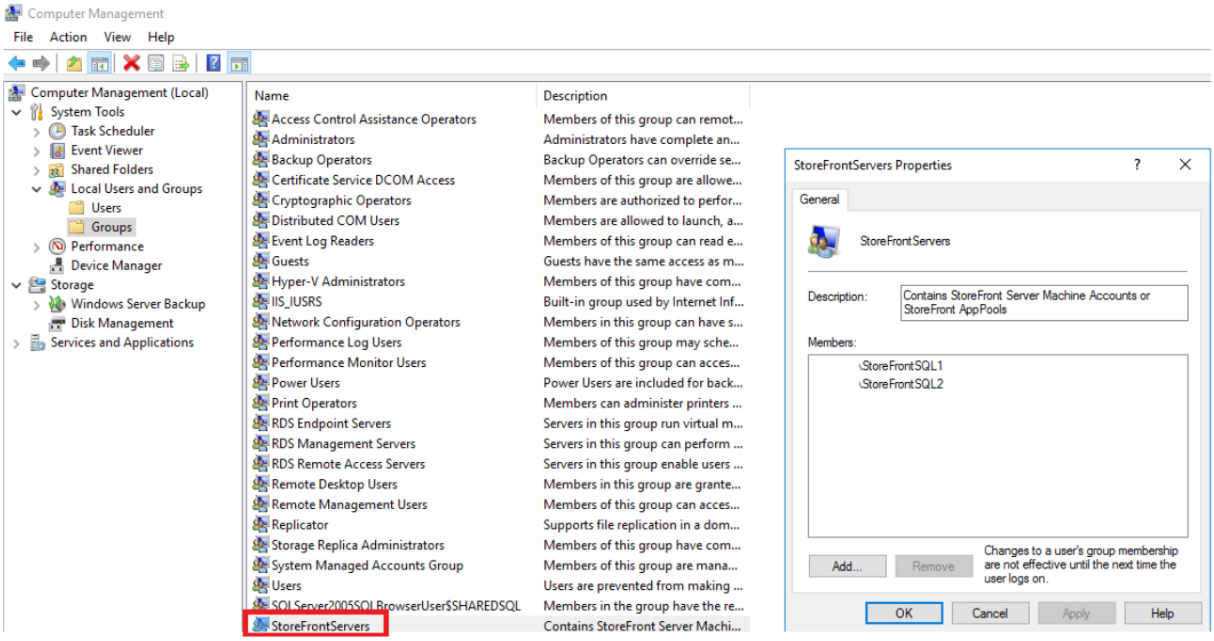


Vérifiez que les règles de pare-feu Windows sont correctement configurées pour autoriser les connexions SQL Server à l'aide d'un port spécifique ou de ports dynamiques. Reportez-vous à la documentation Microsoft pour savoir comment procéder dans votre environnement.

> **Conseil :**
>
> Si la connexion à l'instance SQL locale échoue, vérifiez que localhost ou `<hostname>` utilisé dans la chaîne de connexion est résolu correctement sur l'adresse IPv4. Windows peut essayer d'utiliser IPv6 au lieu d'IPv4, et la résolution DNS de localhost peut renvoyer ::1 au lieu de l'adresse IPv4 correcte de StoreFront et de SQL Server. La désactivation complète de la pile réseau IPv6 sur le serveur hôte peut être nécessaire pour résoudre ce problème.

Scénario 3 – Groupe de serveurs StoreFront et instance Microsoft SQL Server dédiée

Créez un groupe de sécurité local appelé `<SQLServer>\StoreFrontServers` sur l'instance Microsoft SQL Server et ajoutez tous les membres du groupe de serveurs StoreFront. Ce groupe de sécurité est référencé ultérieurement dans le script **Create-StoreSubscriptionsDB-2016.sql** qui crée le schéma de base de données d'abonnement dans SQL.



Ajoutez tous les comptes d'ordinateurs de domaine de groupe de serveurs StoreFront au groupe `<SQLServer>\StoreFrontServers`. Seuls les comptes d'ordinateurs de domaine du serveur StoreFront répertoriés dans le groupe peuvent accéder en lecture et en écriture aux enregistrements d'abonnement dans SQL si l'authentification Windows est utilisée par SQL Server. La fonction PowerShell suivante, fournie dans le script Add-RemoteSFAccounts.ps1, crée le groupe de sécurité local et y ajoute deux serveurs StoreFront nommés StoreFrontSQL1 et StoreFrontSQL2.

```
function Add-RemoteSTFMachineAccounts
{

[CmdletBinding()]
param([Parameter(Mandatory=$True)][string]$Domain,
[Parameter(Mandatory=$True)][array]$StoreFrontServers)

# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts"

# Check whether the Local Security Group already exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
 }

```



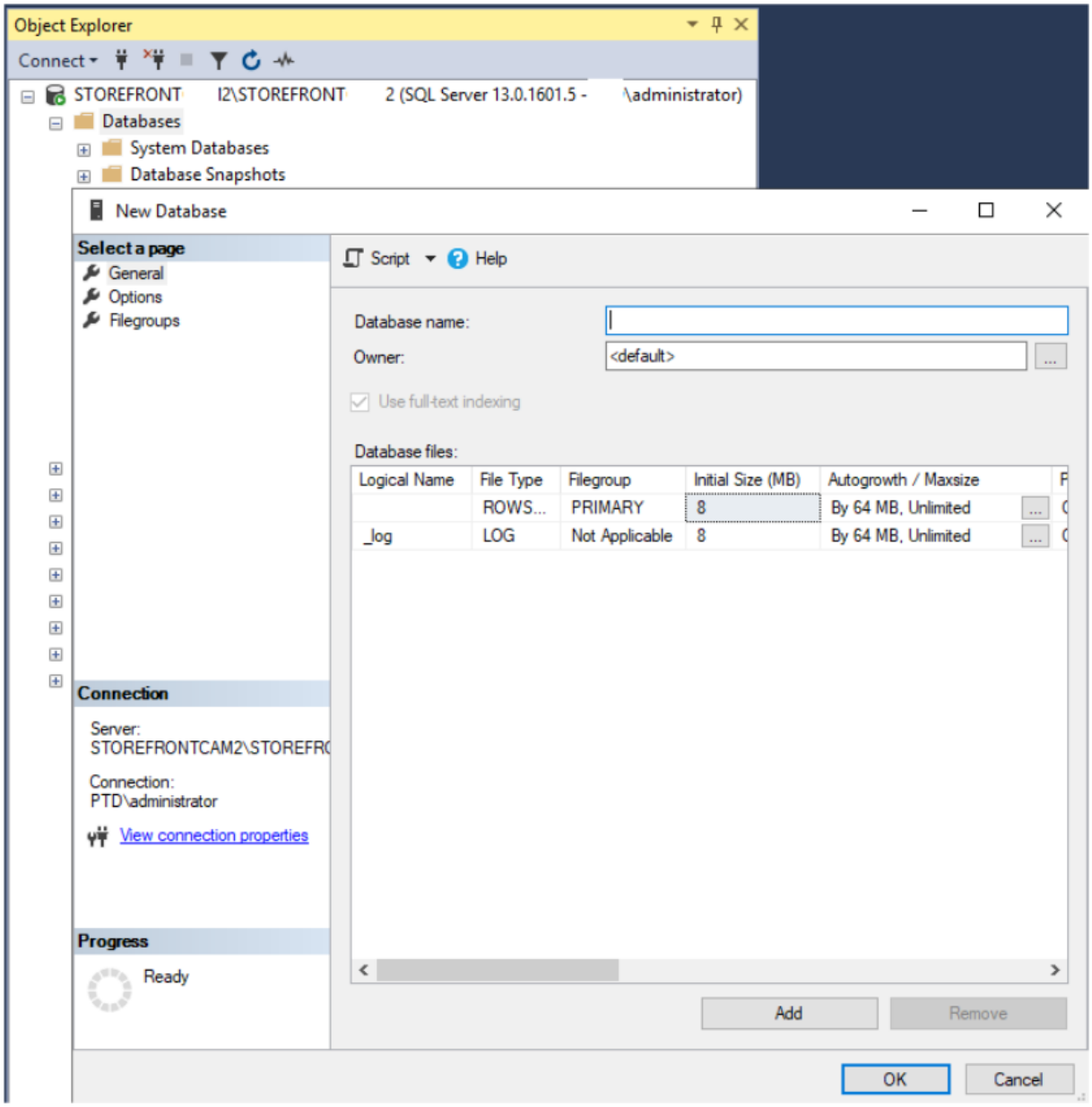
```
19 else
20 {
21
22     Write-Host ”Creating $LocalGroupName local group” -ForegroundColor
       ”Yellow”
23
24     # Create Local Security Group
25     $Computer = [ADSI]”WinNT://$env:ComputerName,Computer”
26     $LocalGroup = $Computer.Create(”group”,$LocalGroupName)
27     $LocalGroup.setinfo()
28     $LocalGroup.description = $Description
29     $Localgroup.SetInfo()
30 Write-Host ”$LocalGroupName local group created” -ForegroundColor ”
       Green”
31  }
32
33 Write-Host ”Adding $StoreFrontServers to $LocalGroupName local group” -
       ForegroundColor ”Yellow”
34
35 foreach ($StoreFrontServer in $StoreFrontServers)
36 {
37
38     $Group = [ADSI]”WinNT://$env:ComputerName/$LocalGroupName,group”
39     $Computer = [ADSI]”WinNT://$Domain/$StoreFrontServer$”
40     $Group.Add($Computer.Path)
41  }
42
43 Write-Host ”$StoreFrontServers added to $LocalGroupName” -
       ForegroundColor ”Green”
44  }
45
46 Add-RemoteSTFMachineAccounts -Domain ”example” -StoreFrontServers @(”
       StoreFrontSQL1”,”StoreFrontSQL2”)
```

Configurer le schéma de base de données d’abonnement dans Microsoft SQL Server pour chaque magasin

Créez une instance nommée sur votre instance Microsoft SQL Server à utiliser par StoreFront. Définissez le chemin d’accès dans le script .SQL pour qu’il corresponde à l’emplacement où votre version de SQL est installée ou l’emplacement où les fichiers de base de données sont stockés. L’exemple de script Create-StoreSubscriptionsDB-2016.sql utilise SQL Server 2016 Enterprise.

Créez une base de données vide à l’aide de SQL Server Management Studio (SSMS) en cliquant avec

le bouton droit de la souris sur **Bases de données**, puis en sélectionnant **Nouvelle base de données**.



Tapez un **nom de base de données** correspondant à votre magasin ou choisissez un autre nom, tel que *STFSubscriptions*.

Avant d'exécuter le script, pour chaque magasin de votre déploiement StoreFront, modifiez les références de l'exemple de script pour qu'elles correspondent à vos déploiements StoreFront et SQL. Par exemple, modifiez :

- Nommez chaque base de données que vous créez pour qu'elle corresponde au nom du magasin dans StoreFront dans `USE [STFSubscriptions]`.
- Définissez le chemin d'accès aux fichiers .mdf et .ldf de la base de données sur l'emplacement

où vous souhaitez stocker la base de données.

```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.mdf
```

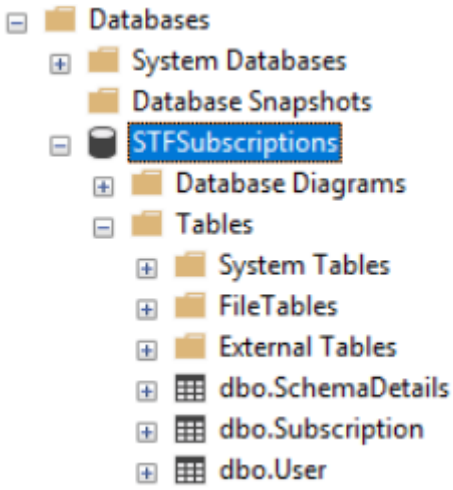
```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.ldf
```

- Définissez la référence sur le nom de votre instance SQL Server dans le script :

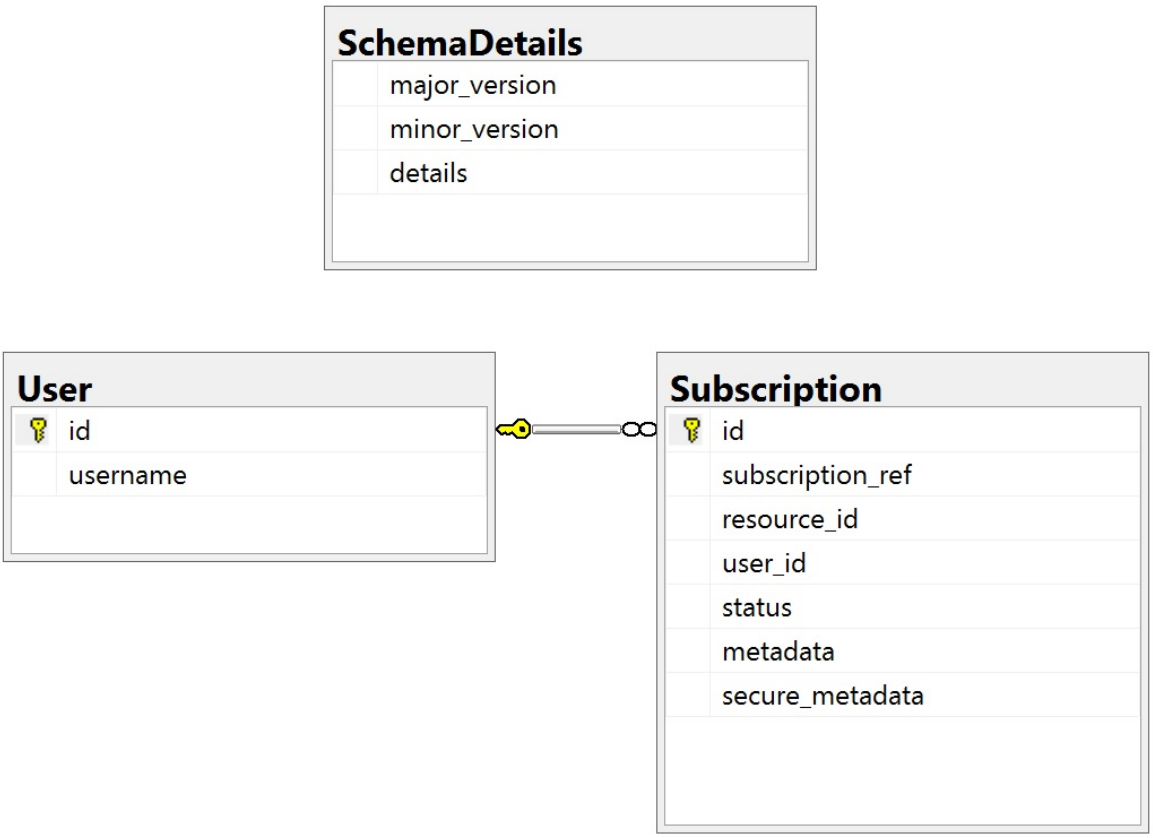
```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;
```

```
ALTER LOGIN [SQL2016\StoreFrontServers]
```

Exécutez le script. Une fois la configuration réussie du schéma, trois tables de base de données sont créées : *SchemaDetails*, *Subscription* et *User*.



Le diagramme suivant montre le schéma de base de données d'abonnement créé par le script *Create-StoreSubscriptionsDB-2016.sql* :



Configurer la chaîne de connexion SQL Server pour chaque magasin StoreFront

Scénario 1

> **Conseil :**
>
> Les données d'abonnement d'origine stockées sur le disque dans la base de données ESENT ne sont ni détruites ni supprimées. Si vous décidez d'utiliser ESENT au lieu de Microsoft SQL Server, il est possible de supprimer la chaîne de connexion du magasin et de revenir simplement à l'utilisation des données d'origine. Tous les abonnements supplémentaires qui ont été créés pendant l'utilisation de SQL pour le magasin n'existeront pas dans ESENT et les utilisateurs ne verront pas ces nouveaux enregistrements d'abonnement. Tous les enregistrements d'abonnement d'origine seront toujours présents.

Réactiver les abonnements ESENT sur un magasin

Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.

Utilisez l'option **-UseLocalStorage** pour spécifier le magasin sur lequel vous souhaitez réactiver les abonnements ESENT :


```
$SiteID = 1
$StoreVirtualPath = ”/Citrix/Store1”

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $StoreVirtualPath

# Removes the SQL DB Connection string and reverts back to using ESENT
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

Scénarios 2, 3 et 4

Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu’administrateur**.

Spécifiez le magasin pour lequel vous souhaitez définir une chaîne de connexion pour l’utilisation de **$StoreVirtualPath**

```
$SiteID = 1
$VirtualPath= ”/Citrix/Store1”
$DBName = ”Store1”
$DBServer = ”SQL2016Ent”
$DBLocalServer = ”localhost”
$DBInstance = ”StoreFrontInstance”

# For a remote database instance
$ConnectionString = ”Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;” Database=$DBName;Trusted_Connection=True;”
```

OU

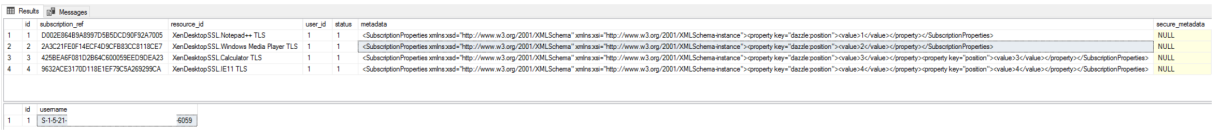
```
# For a locally installed database instance
$ConnectionString = ”$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;”

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath ”/
    Citrix/Store”
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```


Répétez le processus pour chaque magasin de votre déploiement si vous souhaitez tous les configurer pour utiliser une chaîne de connexion SQL.

Migrer des données existantes depuis ESENT vers Microsoft SQL Server

Pour migrer vos données ESENT existantes vers SQL, vous devez utiliser un processus de transformation des données en deux étapes. Deux scripts sont fournis pour vous aider à effectuer cette opération ponctuelle. Si la chaîne de connexion dans StoreFront et l'instance SQL sont correctement configurées, tous les nouveaux abonnements sont créés automatiquement dans SQL au format correct. Après la migration, les données d'abonnement ESENT historiques sont converties en format SQL et les utilisateurs peuvent également afficher les ressources auxquelles ils sont déjà abonnés.

Exemple : quatre abonnements SQL pour le même utilisateur de domaine



Étape 1 – Utiliser le script Transform-SubscriptionDataForStore.ps1 pour convertir les données ESENT en un format SQL convivial pour l'importation en bloc

Connectez-vous au serveur StoreFront à partir duquel vous souhaitez convertir les données ESENT.

Cette opération est possible pour tous les membres d'un groupe de serveurs à condition qu'ils contiennent tous le même nombre d'enregistrements d'abonnement.

Ouvrez PowerShell ISE et sélectionnez **Exécuter en tant qu'administrateur**.

Exécutez le script Transform-SubscriptionDataForStore.ps1 qui exporte un fichier `<StoreName>.txt` de la base de données ESENT vers le bureau de l'utilisateur actuel.

Le script PowerShell fournit des commentaires détaillés sur chaque ligne d'abonnement traitée pour faciliter le débogage et vous aider à évaluer la réussite de l'opération. Le script peut prendre du temps.

Les données converties sont écrites dans le fichier `<StoreName>SQL.txt` sur le bureau de l'utilisateur actif une fois le script terminé. Le script répertorie le nombre d'enregistrements utilisateur uniques et le nombre total d'abonnements traités.

Répétez ce processus pour chaque magasin que vous souhaitez migrer vers SQL Server.

Étape 2 – Utiliser une procédure stockée T-SQL pour importer en bloc les données converties dans SQL

Les données de chaque magasin doivent être importées un magasin à la fois.

Copiez le fichier `<StoreName>SQL.txt` créé à l'étape 1 à partir du bureau du serveur StoreFront `C:\` sur l'instance Microsoft SQL Server et renommez-le SubscriptionsSQL.txt.

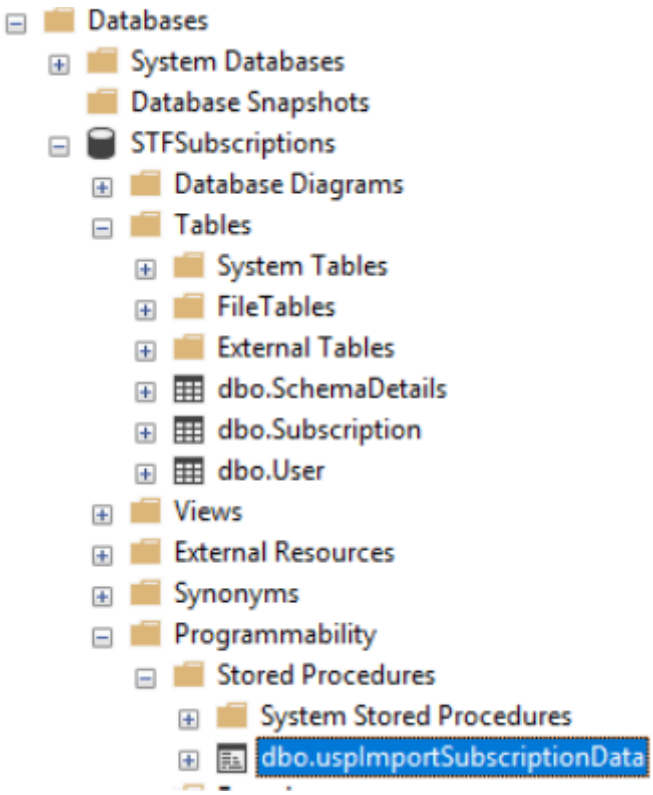
Le script Create-ImportSubscriptionDataSP.sql crée une procédure stockée T-SQL pour importer en bloc les données d'abonnement. Il supprime les entrées en double pour chaque utilisateur unique afin que les données SQL résultantes soient correctement normalisées et divisées en tables correctes.

Avant d'exécuter *Create-ImportSubscriptionDataSP.sql*, modifiez `USE [STFSubscriptions]` pour que cet élément corresponde à la base de données sous laquelle vous souhaitez créer la procédure stockée.

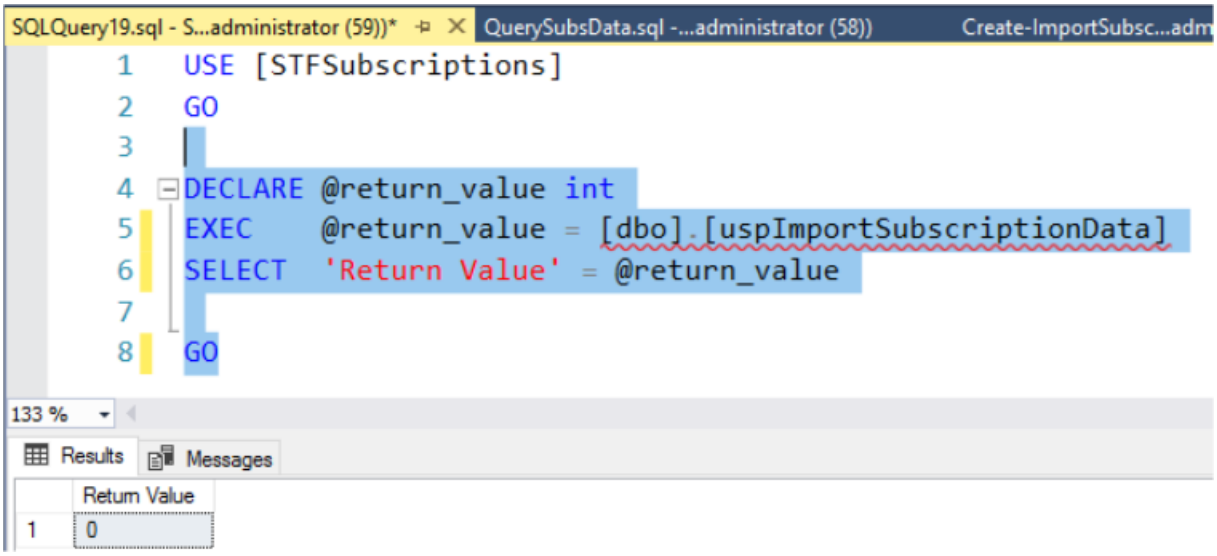
Ouvrez le fichier *Create-ImportSubscriptionDataSP.sql* à l'aide de SQL Server Management Studio et exécutez le code qui s'y trouve. Ce script ajoute la procédure stockée *ImportSubscriptionDataSP* à la base de données que vous avez créée précédemment.

Après la création réussie de la procédure stockée, le message suivant s'affiche dans la console SQL et la procédure stockée ImportSubscriptionDataSP est ajoutée à la base de données :

```
Commands completed successfully.
```



Pour exécuter la procédure stockée, cliquez dessus avec le bouton droit de la souris, sélectionnez **Exécuter la procédure stockée**, puis cliquez sur **OK**.



La valeur de retour 0 indique que toutes les données ont été correctement importées. Tout problème lors de l'importation est enregistré dans la console SQL. Une fois la procédure stockée exécutée, comparez le nombre total d'enregistrements d'abonnement et d'utilisateurs uniques fourni par le script Transform-SubscriptionDataForStore.ps1 avec le résultat des deux requêtes SQL ci-dessous. Les deux chiffres devraient correspondre.

Le nombre total d'abonnements fourni par le script de transformation doit correspondre au nombre total signalé par SQL :

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
```

Le nombre d'utilisateurs uniques fourni par le script de transformation doit correspondre au nombre d'enregistrements de la table User signalé par SQL :

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
```

Si le script de transformation affiche 100 utilisateurs uniques et 1 000 enregistrements d'abonnement, SQL doit afficher les mêmes chiffres une fois la migration effectuée.

Connectez-vous à StoreFront pour vérifier si les utilisateurs existants peuvent afficher leurs données d'abonnement. Les enregistrements d'abonnement existants sont mis à jour dans SQL lorsque les utilisateurs abonnent ou désabonnent leurs ressources. De nouveaux utilisateurs et enregistrements d'abonnement sont également créés dans SQL.

Étape 3 – Exécuter des requêtes T-SQL sur vos données importées

> **Remarque :**
>
> Tous les noms de Delivery Controller sont sensibles à la casse et doivent correspondre exactement aux noms utilisés dans StoreFront.

```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

-- Get total number of Subscription records for a particular user SID
Use [STFSubscriptions]
SELECT COUNT(Subscription.id)
FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
```

```
-- Get all subscription records for a particular delivery controller
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
```


Mettre à jour ou supprimer des enregistrements d'abonnement existants à l'aide de T-SQL

> **Clause d'exclusion de responsabilité :**
>
> Tous les exemples d'instructions SQL de mise à jour et de suppression sont utilisés entièrement à vos propres risques. Citrix n'est pas responsable de toute perte ou altération accidentelle de vos données d'abonnement par une utilisation incorrecte des exemples fournis. Les instructions T-SQL suivantes sont fournies à titre indicatif pour permettre l'exécution de mises à jour simples. Sauvegardez toutes les données d'abonnement dans les sauvegardes complètes de base de données SQL avant de tenter de mettre à jour vos abonnements ou de supprimer des enregistrements obsolètes. Si vous n'effectuez pas les sauvegardes nécessaires, vous risquez de perdre ou de corrompre les données. Avant d'exécuter vos propres instructions T-SQL de mise à jour (UPDATE) ou de suppression (DELETE) sur la base de données de production, testez-les sur des données fictives ou sur une copie redondante des données de production à l'extérieur de la base de données de production active.
>
> **Remarque :**
>
> Tous les noms de Delivery Controller sont sensibles à la casse et doivent correspondre exactement aux noms utilisés dans StoreFront.

```
-- Update the delivery controller used in all subscriptions.
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    NewDeliveryController.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- Delete all subscription records for a particular Delivery Controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
```

```
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Delete all subscription records for a particular application
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE '%.Application'

-- Delete all subscription records for an application published via a specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
```

```
-- Delete all subscription records for a particular user SID
Use [STFSubscriptions]
DELETE FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'

Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
```

```
-- Delete ALL subscription data from a particular database and reset the primary key clustered index to start numbering from 0.
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a clean database.

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
DBCC CHECKIDENT ([User], RESEED, 0)
```

Paramètres de magasin avancés

March 3, 2020

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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 page **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 Citrix Virtual Desktops et serveur Citrix Virtual Apps 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**.

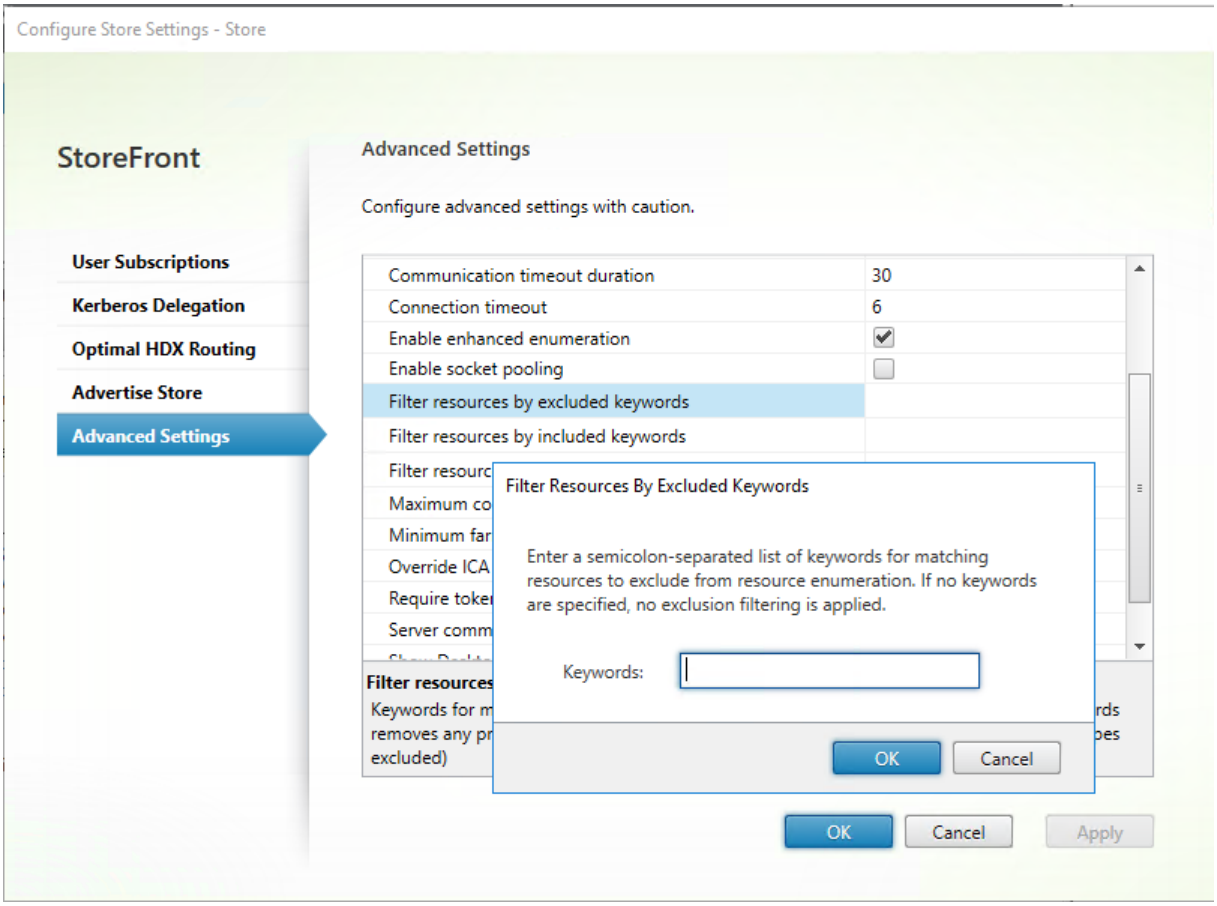
Activer le regroupement de sockets

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, l'application Citrix Workspace 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

January 30, 2020

Un site *Citrix Receiver pour Web* est un site Web utilisé comme un magasin d'applications. Les utilisateurs peuvent ouvrir le site dans un navigateur et accéder en toute sécurité aux applications, données et bureaux publiés pour eux via Citrix Virtual Apps and Desktops.

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

Tâche	Détail
Créer un site Citrix Receiver pour Web	Permet de créer des sites Citrix Receiver pour Web, ce qui permet aux utilisateurs d'accéder aux magasins via une page Web.
Configurer des sites Citrix Receiver pour Web	Permet de modifier les paramètres de vos sites Receiver pour Web.
Expérience utilisateur unifiée	StoreFront prend en charge l'expérience utilisateur unifiée. L'expérience unifiée offre une expérience utilisateur HTML5 gérée de façon centralisée.
Créer et gérer des applications recommandées	Permet de créer des groupes d'applications recommandées pour des utilisateurs qui sont liés ou appartiennent à une certaine catégorie.
Configurer le contrôle de l'espace de travail	Le contrôle de l'espace de travail permet aux applications de suivre les utilisateurs lorsqu'ils naviguent d'une machine à une autre.

Tâche	Détail
Configurer l'utilisation des onglets de navigateur par l'application Citrix Workspace pour HTML5	Lorsque les utilisateurs démarrent des ressources à partir de raccourcis à l'aide de Citrix Receiver pour HTML5 ou l'application Citrix Workspace pour HTML5, spécifiez si le bureau ou l'application remplace le site Citrix Receiver pour Web dans l'onglet de navigateur existant plutôt que d'apparaître dans un nouvel onglet.
Configurer la durée d'expiration des communications et le nombre de tentatives de reconnexion	Par défaut, les demandes effectuées par un site Citrix Receiver pour Web auprès du magasin associé expirent au bout de trois minutes. Le serveur est considéré comme indisponible après une tentative de communication infructueuse. Vous pouvez modifier les paramètres par défaut.

Créer un site Citrix Receiver pour Web

March 3, 2020

Lorsque vous créez un magasin, un site Citrix Receiver pour Web est automatiquement créé pour ce magasin. Vous pouvez ajouter des sites Citrix Receiver pour Web supplémentaires aux magasins existants.

> 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 Citrix 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. Saisissez le **chemin d'accès au site Web** souhaité et cliquez sur **Suivant**.
4. Sélectionnez l'expérience Citrix Receiver et cliquez sur **Suivant**.
5. Sélectionnez des méthodes 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 l'application Citrix Workspace est installée sur la machine de l'utilisateur. Si l'application Citrix Workspace ne peut être détectée, l'utilisateur est invité à télécharger et à installer la version appropriée pour sa plate-forme à partir du site Web de Citrix. Pour plus d'informations sur la modification de ce comportement, reportez-vous à la section Configurer le comportement du site des utilisateurs ne disposant pas de l'application Citrix Workspace.

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

Configurer des sites Citrix Receiver pour Web

March 3, 2020

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 de plus amples informations, consultez la section Configurer des sites Citrix 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 ce processus terminé,

> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

Choisir les méthodes d'authentification

Utilisez la tâche Gérer 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 Magasins.
3. Dans le panneau Magasins, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur **Configurer** et sélectionnez **Méthodes d'authentification** pour spécifier les méthodes d'accès que vous souhaitez activer pour vos utilisateurs.
    - Sélectionnez **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 **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 **Authentification pass-through au domaine** pour 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 ou l'application Citrix Workspace pour Windows est installé sur les machines utilisateur.

      > Remarque :

> L'authentification pass-through au domaine pour Citrix Receiver pour Web est limitée aux systèmes d'exploitation Windows utilisant Chrome, Firefox et Internet Explorer.

- Sélectionnez **Carte à puce** pour activer l'authentification par carte à puce. Les utilisateurs s'authentifient à l'aide de cartes à puce et de codes PIN lorsqu'ils accèdent à leurs magasins.
- Sélectionnez **Authentification pass-through via Citrix Gateway** pour activer l'authentification pass-through à partir de Citrix Gateway. Les utilisateurs s'authentifient sur Citrix 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.

Avant de pouvoir créer des raccourcis vers les ressources, vous devez ajouter les adresses URL des sites Web hôtes à la liste des « adresses URL approuvées » à l'aide de la console de gestion Citrix StoreFront ou à l'aide de PowerShell. Les adresses URL approuvées sont répertoriées dans la section `<trustedUrls>` du fichier web.config pour le site Citrix Receiver pour Web. web.config se trouve généralement dans le répertoire `C:\inetpub\wwwroot\Citrix\storenameWeb\`, où *storename* désigne le nom attribué au magasin au moment de sa création.

Par défaut, StoreFront avertit les utilisateurs s'ils tentent de lancer des raccourcis vers les ressources à partir de sites Web non approuvés ; les utilisateurs peuvent quand même choisir de lancer la ressource. Pour arrêter l'affichage de ces avertissements, dans le panneau Magasins, cliquez sur **Gérer les sites Receiver pour Web**, cliquez sur **Configurer**, choisissez **Paramètres avancés** et désactivez l'option **Invite pour les raccourcis non approuvés**.

Ajouter des sites Web approuvés à l'aide de la console de gestion

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.

Ajouter des sites Web approuvés à l'aide de PowerShell

Vous pouvez ajouter des adresses URL approuvées à l'aide de l'applet de commande PowerShell **Set-STFWebReceiverApplicationShortcuts** décrite à la section https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Citrix.StoreFront.SubscriptionsStore/.

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 ou l'application Citrix Workspace 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 Citrix Gateway et des balises configurés pour le magasin. Dans cet article, les mentions de « Application Citrix Workspace » représentent également les versions prises en charge de Citrix Receiver, sauf indication contraire.

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 l'application Workspace/Receiver**.

Configurer le comportement du site des utilisateurs ne disposant pas de l'application Citrix Workspace

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

Si l'application Citrix Workspace ne peut être détectée, l'utilisateur est invité à télécharger et à installer la version appropriée pour sa plate-forme. L'emplacement de téléchargement par défaut est le site Web Citrix, mais vous pouvez également copier les programmes d'installation de l'application Citrix Workspace sur le serveur StoreFront et autoriser les utilisateurs à en télécharger des copies directement à partir du serveur StoreFront.

Pour les utilisateurs qui ne peuvent pas installer l'application Citrix Workspace, vous pouvez activer l'application Citrix Workspace pour HTML5 sur vos sites Citrix Receiver pour Web. L'application Citrix Workspace pour HTML5 permet aux utilisateurs d'accéder directement aux bureaux et aux applications dans des navigateurs Web compatibles HTML5 sans avoir à installer l'application Citrix Workspace. Les connexions réseau internes 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 de plus amples informations, consultez la section Configuration requise pour l'infrastructure.

Pour les utilisateurs du réseau interne, l'accès via l'application Citrix Workspace pour HTML5 aux ressources fournies par Citrix Virtual Apps and Desktops est désactivé par défaut. Pour activer l'accès local aux bureaux et applications à l'aide de l'application Citrix Workspace pour HTML5, vous devez activer la stratégie Connexions WebSockets ICA sur vos serveurs Citrix Virtual Apps and Desktops. Le composant Citrix Virtual Apps and Desktops utilise le port 8008 pour l'application Citrix Workspace pour les connexions HTML5. Assurez-vous que votre pare-feu et autres périphériques réseau autorisent l'accès à ce port. Pour de plus amples informations, consultez la section Paramètres de stratégie WebSockets.

Pour que les lancements de ressources Citrix Virtual Apps and Desktops réussissent à utiliser l'application Citrix Workspace pour HTML5 lors de la connexion directe à StoreFront, les connexions

TLS aux VDA qui hébergent les applications et les bureaux doivent être configurées. Les connexions à distance via Citrix Gateway peuvent lancer des ressources à l'aide de l'application Citrix Workspace pour HTML5 sans nécessiter la configuration des connexions TLS au VDA.

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. Sélectionnez **Déployer l'application Workspace/Citrix Receiver** et spécifiez une **Option de déploiement**.
    - Sélectionnez **Toujours utiliser Receiver pour HTML5** si vous souhaitez que le site accède toujours aux ressources via un navigateur compatible HTML5 sans inviter l'utilisateur à télécharger et à installer l'application Citrix Workspace. Lorsque cette option est sélectionnée, les utilisateurs accèdent toujours aux bureaux et aux applications du site via l'application Citrix Workspace pour HTML5, à condition qu'ils utilisent un navigateur compatible HTML5. Les utilisateurs sans navigateur compatible HTML5 ne peuvent pas accéder aux ressources. L'accès via n'importe quelle application Citrix Workspace installée localement est désactivé.
    - Sélectionnez **Utiliser Receiver pour HTML5 si une installation Receiver locale n'est pas disponible** si vous souhaitez que le site invite l'utilisateur à télécharger et à installer l'application Citrix Workspace mais qu'il se replie sur l'application Citrix Workspace pour HTML5 dans le cas où l'application Citrix Workspace ne peut pas être installée. Les utilisateurs sans application Citrix Workspace sont invités à la télécharger et à l'installer chaque fois qu'ils ouvrent une session sur le site.
    - Sélectionnez **Installer localement** si vous souhaitez que le site accède toujours aux ressources via une application Citrix Workspace installée localement. Les utilisateurs sont invités à télécharger et installer l'application Citrix Workspace appropriée pour leur plate-forme. L'accès via les navigateurs compatibles HTML5 est désactivé.
        - 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 l'application Citrix Workspace sur le client de l'utilisateur final si l'application Citrix Workspace n'est pas disponible.
        - Si vous sélectionnez **Mettre le plug-in à niveau à l'ouverture de session**, Citrix Receiver pour Web offre aux utilisateurs l'option de mettre à niveau l'application Citrix Workspace lorsqu'ils ouvrent une session. Les utilisateurs peuvent choisir d'ignorer la mise à niveau et ne seront pas invités à effectuer une nouvelle mise à niveau à moins que les cookies du navigateur Citrix Receiver pour Web ne soient effacés. Pour activer cette fonctionnalité, assurez-vous que les fichiers de l'application Citrix Workspace

sont disponibles sur le serveur StoreFront.
- Sélectionnez une source dans la liste déroulante.

Mettre à disposition des fichiers d'installation de l'application Citrix Workspace 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 l'application Citrix Workspace est installée sur la machine de l'utilisateur. Si l'application Citrix Workspace ne peut pas être détectée, l'utilisateur est invité à la télécharger et à l'installer pour sa plate-forme à partir du site Web Citrix ou en téléchargeant le programme d'installation approprié à partir du serveur 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 un site. Dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web** et cliquez sur **Configurer**.
3. Choisissez **Déployer l'application Workspace/Citrix Receiver** et **Source de l'application Workspace/Receiver**, puis accédez aux fichiers d'installation.

Exécuter l'invite d'installation de l'application Citrix Workspace après l'ouverture de session

Avant de se connecter à StoreFront, Citrix Receiver pour Web invite l'utilisateur à installer l'application Citrix Workspace la plus récente si elle n'est pas déjà installée sur l'ordinateur de l'utilisateur. En fonction de la configuration, l'invite peut également s'afficher si l'installation de l'application Citrix Workspace de l'utilisateur peut être mise à niveau.

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

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

March 3, 2020

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

StoreFront prend en charge l'expérience utilisateur *unifiée*. L'expérience unifiée offre une expérience utilisateur HTML5 gérée de façon centralisée pour toutes les applications Citrix Workspace Web et natives. 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.

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.

Utiliser Javascript et CSS pour personnaliser les pages Citrix Receiver pour Web.

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 ce processus terminé, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

> Remarque :
>
> Si vous utilisez XenApp 6.x, les applications définies sur **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.

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

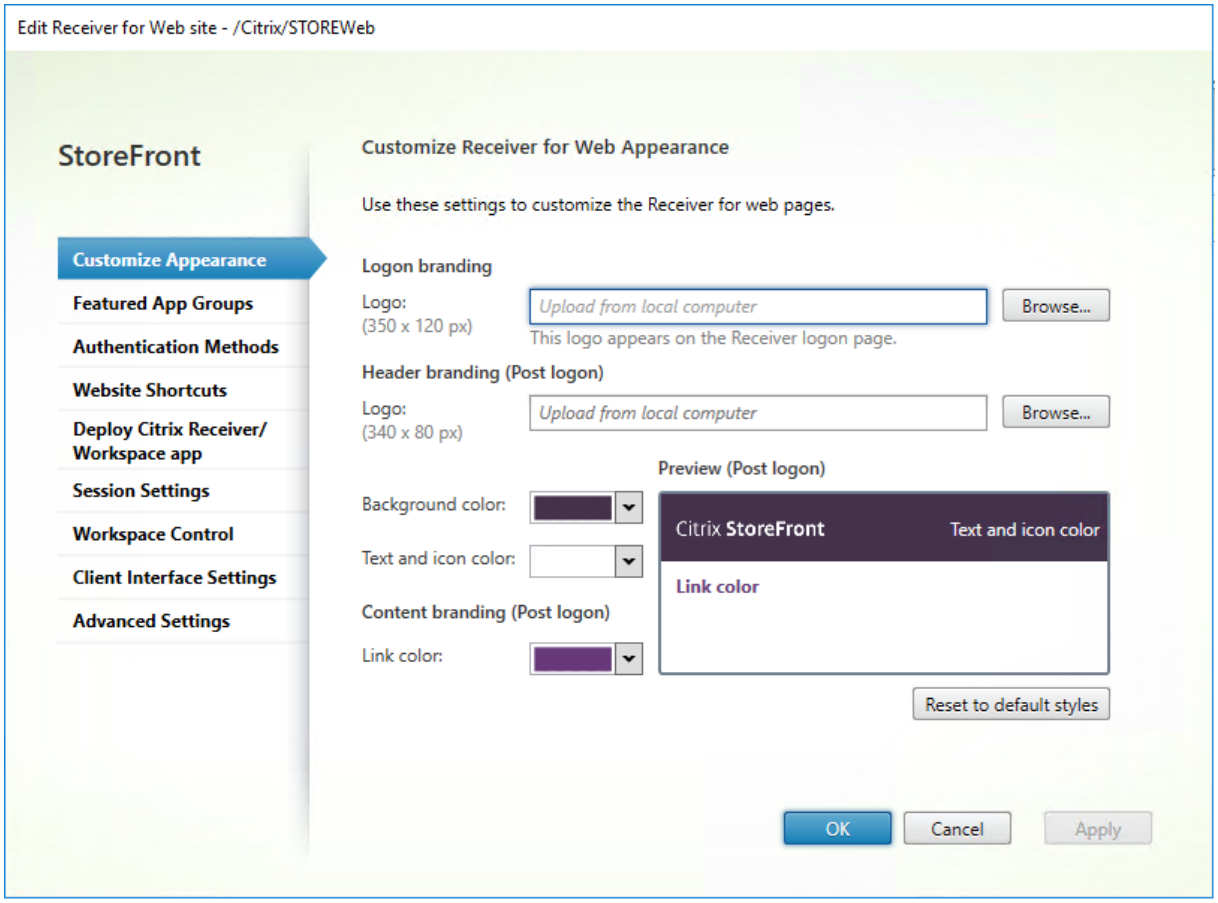
Lorsqu'un nouveau magasin de données est créé à l'aide de StoreFront, un site Citrix Receiver pour Web est créé automatiquement et associé au magasin. Les sites Citrix Receiver pour Web utilisent l'expérience unifiée. Lorsqu'un magasin possède plusieurs sites Receiver pour Web, vous devez sélectionner le site Receiver pour Web qui s'affiche lorsque les utilisateurs accèdent au magasin à l'aide de l'application Citrix Workspace.

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**. Si vous ne disposez pas d'un site Web Citrix Receiver pour Web, un message s'affiche, avec un lien vers l'assistant Ajouter un site Receiver pour Web.
3. Sélectionnez le site Receiver pour Web par défaut que les clients d'application Citrix Workspace affichent lorsque les utilisateurs accèdent à ce magasin.
4. Cliquez sur **OK**.

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 **Personnaliser l'apparence** et effectuez des sélections pour personnaliser la manière dont le site Web s'affiche après avoir ouvert une session.



Personnalisation supplémentaire à l'aide de Javascript et CSS

> Remarque :
>
> Dans les exemples de cette section, ajoutez Javascript au fichier *script.js* (par exemple dans C:\inetpub\wwwroot\Citrix\StoreWeb\custom) et ajoutez CSS au fichier *style.css* dans le même répertoire.

Ajouter un en-tête statique à la page de connexion dans Receiver pour Web

Ici, « en-tête statique » signifie un texte fixe comme un message de bienvenue ou un nom d'entreprise. Pour tout élément changeant, tel qu'un message d'information ou l'état du serveur, consultez la section Ajouter un en-tête dynamique à la page de connexion dans Receiver pour Web.

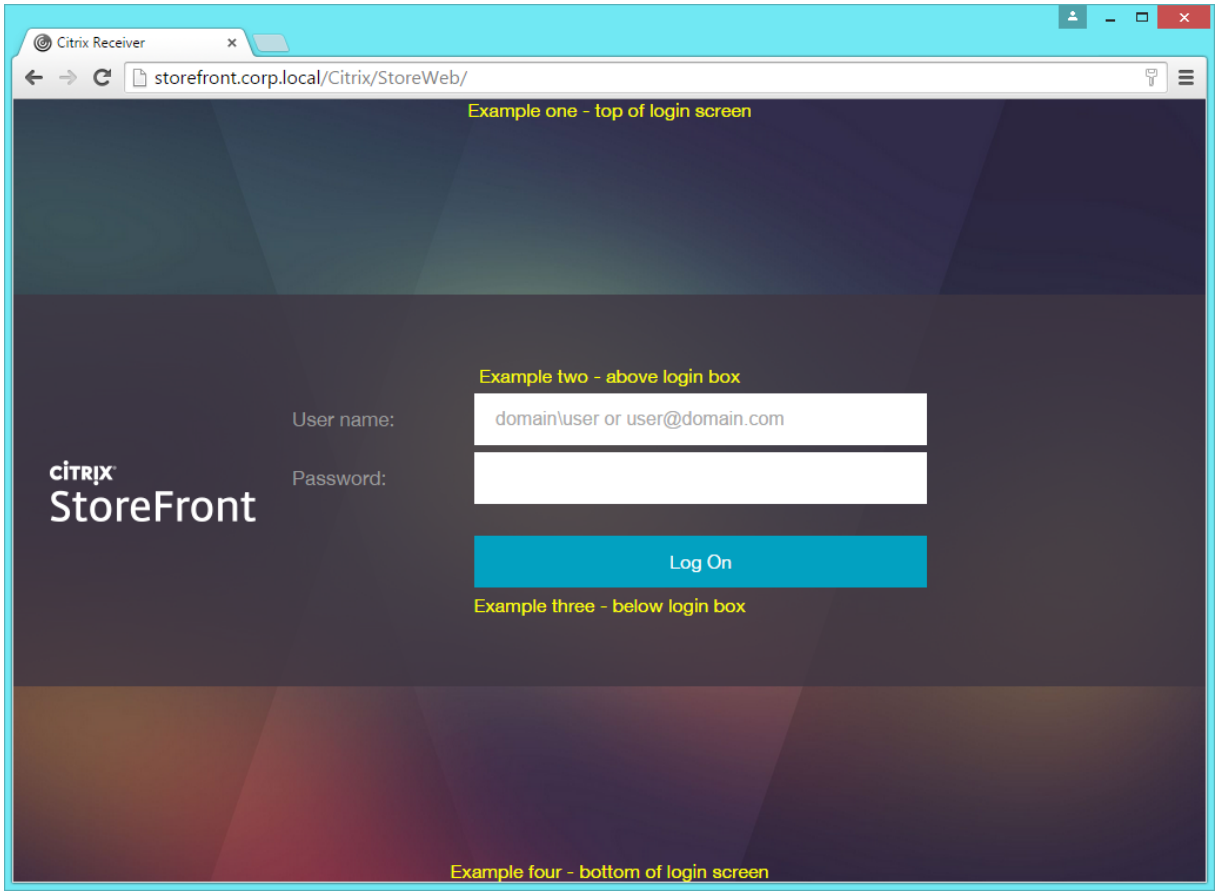
Vous pouvez ajouter du texte statique sur quatre positions en utilisant les lignes suivantes de javascript :

```
$('.customAuthHeader').html("Example one - top of login screen");
$('.customAuthTop').html("Example two - above login box");
$('.customAuthBottom').html("Example three - below login box");
$('.customAuthFooter').html("Example four - bottom of login screen");
```

Pour mettre le texte en évidence, ajoutez le style suivant à custom.css :

```
.customAuthHeader,
.customAuthFooter,
.customAuthTop,
.customAuthBottom
{

 font-size:16px;
 color:yellow;
 text-align: center;
 }
```

Le résultat ressemble à ce qui suit :



Pour utiliser le formatage HTML, remplacez les quatre lignes de javascript par ce qui suit :

```
$('.customAuthHeader').html("<b>Example one</b> - top of login screen");
$('.customAuthTop').html("<div style='background:black'>Example two - above login box</div>");
$('.customAuthBottom').html("<i>Example three - below login box</i>");
$('.customAuthFooter').html("<img src='logo.png'>Example four - bottom of login screen");
```

> Remarque :
>
> La quatrième ligne d'exemple attend une image nommée *logo.png* dans le répertoire \custom.

Ajouter un en-tête dynamique à la page de connexion dans Receiver pour Web

Ici, « en-tête dynamique » signifie que certains contenus sont chargés et affichés à chaque fois, plutôt que d'être mis en cache. Les navigateurs Web mettent souvent en cache des éléments lorsqu'ils le peuvent. L'application Citrix Workspace, quant à elle, met toujours en cache l'interface utilisateur et charge toujours l'interface utilisateur précédemment mise en cache. Cela signifie que si vous utilisez

l'exemple précédent pour afficher l'état du service, vous n'obtenez pas le résultat attendu.

Au lieu de cela, vous devez effectuer un appel Ajax pour charger dynamiquement le contenu et l'insérer sur la page. Pour ce faire :

1. Définissez une fonction utilitaire qui récupère le contenu d'une page du répertoire *\customweb* sur le serveur et l'ajoute à la page. Il s'agit de l'équivalent des exemples .html ci-dessus ; la page personnalisée peut contenir du texte ou un extrait HTML. Utilisez le répertoire *\customweb* car il est copié sur tous les serveurs d'un groupe de serveurs StoreFront (tout comme le répertoire \custom), mais il n'est pas téléchargé et mis en cache.
2. Faites de sorte que cette fonction soit appelée à un moment approprié. Si la fonction est appelée trop tôt, des problèmes peuvent se produire dans l'application Citrix Workspace, car le script s'exécute avant que la configuration n'ait été complètement chargée. Un moment approprié pour ce type d'action est **beforeDisplayHomeScreen** (si vous souhaitez afficher du contenu sur la page de connexion, utilisez plutôt **beforeLogin**). Le code suivant gère les deux cas et convient aux clients web et natifs.

Le script complet est le suivant :

```
function setDynamicContent(txtFile, element) {

   CTXS.ExtensionAPI.proxyRequest({

      url: "customweb/"+txtFile,
      success: function(txt) {
 $(element).html(txt); }
  }
 );
 }


var fetchedContent=false;
function doFetchContent(callback)
{

  if(!fetchedContent) {

    fetchedContent = true;
    setDynamicContent("ReadMe.txt", "#customScrollTop");
   }

  callback();
 }


```



```
CTXS.Extensions.beforeDisplayHomeScreen = doFetchContent;
CTXS.Extensions.beforeLogon = doFetchContent;
```

Ce script permet de charger le contenu de *\customweb\readme.txt* qui, par défaut, contient des informations non pertinentes. Ajoutez votre propre fichier (*status.txt*) et modifiez le script d'appel pour obtenir des résultats plus utiles.

Afficher une clause d'exclusion de responsabilité interactive avant ou après la connexion

L'exemple suivant est déjà fourni dans le fichier *script.js* à titre d'exemple, mais ses marques de commentaire doivent être supprimées. Il existe deux versions de ce code : la première est effectuée avant la connexion pour les navigateurs Web, et la seconde avant l'affichage de l'interface utilisateur principale pour les clients natifs. Si vous souhaitez afficher uniquement un message après la connexion, supprimez la première fonction. Cependant, l'utilisation d'un message avant la connexion uniquement n'est pas recommandée, car le flux de connexion n'est visible que sur les navigateurs Web (et non sur les clients natifs). Le flux de connexion est donc masqué lors de l'accès utilisateur à partir de Citrix Gateway.

```
var doneClickThrough = false;

// Before web login
CTXS.Extensions.beforeLogon = function (callback) {

  doneClickThrough = true;
  CTXS.ExtensionAPI.showMessage({

    messageTitle: "Welcome!",
    messageText: "Only for WWCo Employees",
    okButtonText: "Accept",
    okAction: callback
   }
 );
 }
 ;

// Before main screen (both web and native)
CTXS.Extensions.beforeDisplayHomeScreen = function (callback) {

  if (!doneClickThrough) {

    CTXS.ExtensionAPI.showMessage({

      messageTitle: "Welcome!",
```



```
26        messageText: "Only for WWCo Employees",
27        okButtonText: "Accept",
28        okAction: callback
29       }
30  );
31    }
32   else {
33
34     callback();
35    }
36
37  }
38  ;
```

Élargir la zone de la clause d'exclusion de responsabilité interactive

La zone de message utilisée pour **CTXS.ExtensionAPI.showMessage()** est déjà mise en forme. Vous pouvez modifier ce style en l'élargissant pour qu'il convienne aux autres messages. Ajoutez l'exemple de fonction suivant à script.js pour réduire à nouveau le style ultérieurement. Appelez **showLargeMessage()** au lieu de **CTXS.ExtensionAPI.showMessage()** lorsque vous souhaitez élargir la zone.

```
1  function mkLargeMessageExitFn(origfn)
2  {
3
4    if(origfn) {
5
6      return function() {
7
8        origfn();
9        window.setTimeout(function() {
10  $('body').removeClass('largeMessage'); }
11  ,500);
12       }
13  ;
14    }
15
16  }
17
18
19  function showLargeMessage(details)
20  {
21
```



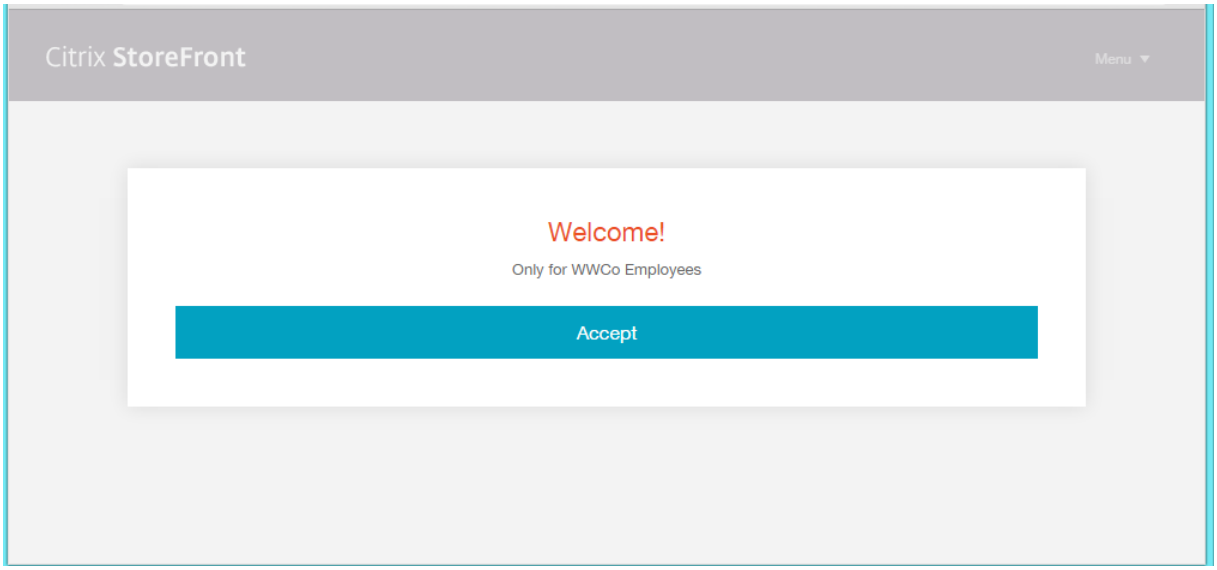
```
22    $('body').addClass('largeMessage');
23    details.cancelAction = mkLargeMessageExitFn(details.cancelAction);
24    details.okAction = mkLargeMessageExitFn(details.okAction);
25    CTXS.ExtensionAPI.showMessage(details);
26   }
27   ;
```

Cela permet d'ajouter une classe de marqueur lorsque le message volumineux est affiché. Lorsque la zone est fermée, la classe de marqueur est supprimée après un bref délai (nécessaire pour éviter un saut indésirable).

Ajoutez CSS pour modifier la taille de cette zone en fonction de la présence de cette classe de marqueur. Par exemple, essayez ce qui suit dans custom\style.css :

```
1  .largeTiles .largeMessage .messageBoxPopup
2  {
3
4    width:800px;
5   }
```

Ainsi, lorsqu'un message de type « messageBoxPopup » est affiché sur une interface utilisateur de grande taille et que l'indicateur « largeMessage » est défini, la largeur est de 800 pixels. Le code existant garantit qu'il est centré. (Sur une interface utilisateur de petite taille, comme un téléphone mobile, la zone de message par défaut est déjà définie sur une pleine largeur).



Pour insérer davantage de texte, vous pouvez réduire la taille de la police en ajoutant ce qui suit à custom\style.css, ou bien envisager d'ajouter une zone de défilement.

```
1  .largeTiles .largeMessage .messageBoxText
2  {
```



```
3
4    font-size:10px;
5   }
```

Ajouter une zone de défilement à la zone de la clause d'exclusion de responsabilité interactive

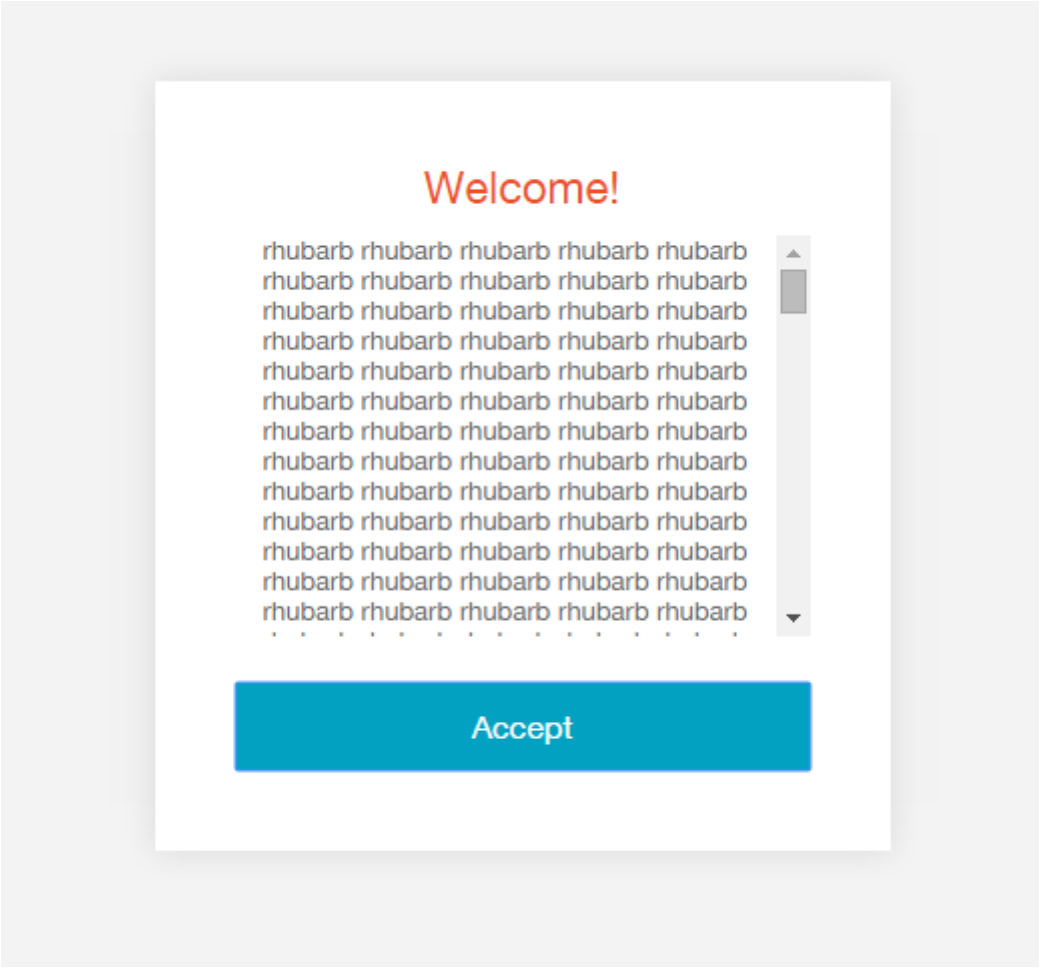
Lorsque vous appelez **showMessage**, vous pouvez transmettre du code HTML, plutôt que simplement une chaîne, pour ajouter du style. Pour ce faire, remplacez messageText, dans l'un des appels précédents à showMessage, par ce qui suit :

```
1      CTXS.ExtensionAPI.showMessage({
2
3            messageTitle: "Welcome!",
4            messageText: "&lt;div class='disclaimer'&gt;rhubarb rhubarb
                 rhubarb ... rhubarb rhubarb&lt;/div&gt;",
5            okButtonText: "Accept",
6            okAction: callback  }
7   );
```

Ajoutez ensuite ce qui suit à style.css :

```
1   .disclaimer {
2
3      height: 200px;
4      overflow-y: auto;
5   }
```

Le résultat ressemble à ce qui suit :



Ajouter un pied de page à chaque page

Il existe une autre zone personnalisée destinée à cette fonction. Vous pouvez ajouter la ligne suivante de Javascript pour définir son contenu :

```
$('#customBottom').html("For ACME Employees Only");
```

Définissez le style dans style.css. Définissez `position:static` pour vous assurer que la zone de défilement fonctionne comme prévu.

```
#customBottom
{

 text-align:center;
 font-size:30px;
 position:static;
 }
```


> Remarque :
>
> Si vous redimensionnez dynamiquement cette zone à l'aide d'un script, vous devez appeler la commande **CTXS.ExtensionAPI.resize()** pour informer l'application Citrix Workspace qu'une modification a été apportée.

Rendre l'affichage des dossiers la valeur par défaut lorsque les utilisateurs accèdent à l'onglet Applications

Pour ce faire, surveillez l'événement « view change ». Si l'affichage du magasin (nom interne utilisé pour l'affichage des applications) est modifié, accédez au dossier racine. Attention :

- Lorsque l'événement **onViewChange** se déclenche, l'affichage du magasin n'est pas encore dessiné pour indiquer qu'il est en train de changer. Par conséquent, si vous accédez au dossier immédiatement, le code d'initialisation de l'affichage du magasin annule votre travail, car il s'exécute après votre code. Pour éviter cela, ajoutez un délai de 1 ms pour vous assurer que le code s'exécute après le déroulement de la pile actuelle.
- Les trois lignes contenant le mot « whitespace » garantissent que l'interface utilisateur initiale de Toutes les applications est dessinée hors de l'écran en plaçant une zone volumineuse personnalisée au-dessus de celle-ci. Cela permet d'arrêter l'effet de scintillement de l'affichage de Toutes les applications avant l'apparition des dossiers.

Ajoutez le code suivant à script.js comme d'habitude :

```
$('#customScrollTop').append('&lt;div class="whitespace"&gt;&lt;/div&gt
    ;');

CTXS.Extensions.onViewChange = function(view) {

  if (view == "store") {

    $('.whitespace').height(5000);
    window.setTimeout(function() {

      CTXS.ExtensionAPI.navigateToFolder("/");
      $('.whitespace').height(0);
     }
 , 1);
   }

 }
 ;
```


Masquer les applications de l'onglet Toutes les applications si elles apparaissent également dans une sélection de catégorie

Vous pouvez utiliser le code suivant pour y parvenir. Commencez par répertorier chaque application d'un bundle, puis supprimez-les de la liste « All Apps display ».

```
var bundleApps = [];

CTXS.Extensions.sortBundleAppList = function(apps,bundle, defaultfn) {

  for (var i = 0; i &lt; apps.length; i++) {

    bundleApps.push(apps[i]);
   }

  defaultfn();
 }
 ;

CTXS.Extensions.filterAllAppsDisplay = function(allapps) {

  for (var i = 0; i &lt; allapps.length; i++) {

    if ($.inArray(allapps[i], bundleApps) != -1) {

       allapps.splice(i, 1);
       i--;
     }

   }

 }
 ;
```

Si vous utilisez cette personnalisation, il est conseillé de remplacer la chaîne de texte « All Apps » (Toutes les applications) par « Other Apps » (Autres applications) par souci de clarté. Pour ce faire, modifiez le fichier *strings.en.js* dans le répertoire \custom, puis ajoutez une balise pour **AllAppsTitle**. Par exemple, les changements seront indiqués ici en jaune :

```
(function ($) {

  $.localization.customStringBundle("en", {

   <span style="background-color: yellow;">AllAppsTitle: "Other Apps"
      ,</span>
```

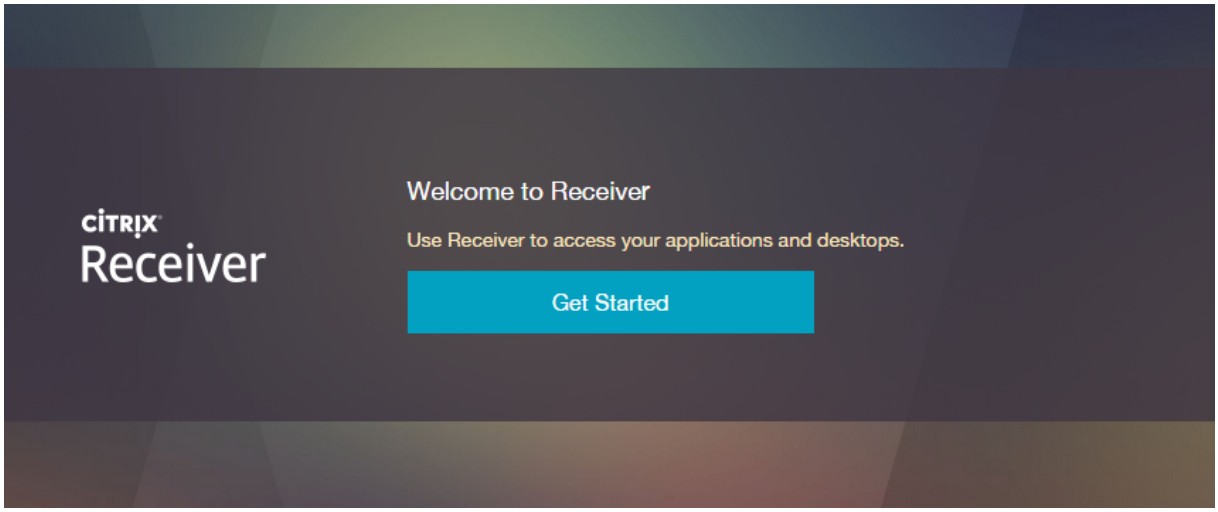


```
    Example1: ”This is an example”,
    Example2: ”This is another example”
  }
  );
  }
  )(jQuery);
```

Modifier le texte de l’interface utilisateur par défaut

Vous pouvez modifier n’importe quel texte utilisé dans l’interface utilisateur si vous connaissez son libellé. Par exemple, pour remplacer l’écran « Install » (Installer) utilisé dans Receiver pour Web sur Google Chrome par « Get Started » (Démarrer), ajoutez une chaîne personnalisée comme suit :

```
(function ($) {

  $.localization.customStringBundle(”en”, {

    <span style=”background-color: yellow;”>Install: ”Get Started”,</
       span>
    Example1: ”This is an example”,
    Example2: ”This is another example”
  }
  );
  }
  )(jQuery);
```



Pour afficher le nom du libellé à modifier, procédez comme suit :

1. Sur le serveur StoreFront, accédez au répertoire C:\inetpub\wwwroot\citrix\StoreWeb\receiver\js\localizatio
   (en supposant que votre magasin est appelé « Store »).

2. Ouvrez le fichier *ctxs.strings_something.js* dans Bloc-notes.
3. Recherchez la chaîne que vous souhaitez modifier. **Remarque** : au lieu de modifier ce fichier directement, créez des valeurs de remplacement dans le répertoire \custom comme pour l'exemple « install ».

Modifier les images d'arrière-plan pour la sélection de catégories

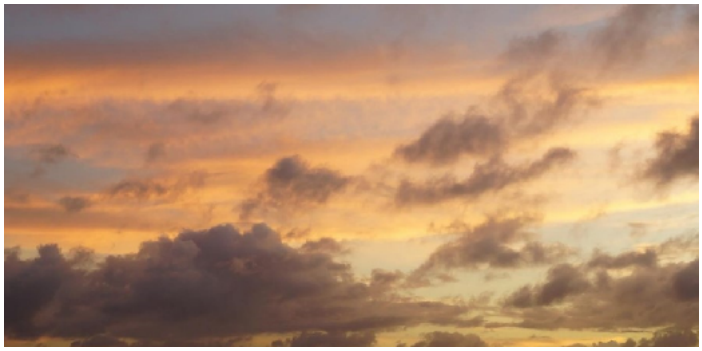
> Important :
>
> N'essayez pas de remplacer les images sur le serveur. Cela peut induire en erreur les clients qui ont déjà téléchargé les images, car ils ne savent pas qu'elles ont été modifiées. Cela rend également la mise à niveau difficile, voire impossible.

Vous pouvez ajouter vos propres images au répertoire *custom* et ajouter CSS pour les référencer. Chaque sélection de catégorie (appelée « bundles » en interne) utilise deux images :

- La première image est utilisée comme une mosaïque dans le carrousel.
- La deuxième image est utilisée comme image d'arrière-plan derrière l'en-tête de la page des détails. Cette image est étirée pour remplir la largeur de l'écran, et un flou est ajouté à son bord inférieur.

Vous pouvez utiliser différentes images pour chaque écran. Envisagez d'utiliser la même image, mais doubler sa hauteur d'arrière-plan dans la page des détails, de sorte que seule la moitié supérieure de l'image est affichée. Étant donné que l'image est étirée sur la page des détails, utilisez une image qui apparaisse de manière satisfaisante même si elle est déformée.

La classe du premier bundle est « appBundle1 », celle du deuxième bundle « appBundle2 », et ainsi de suite jusqu'à « appBundle8 ». L'exemple suivant utilise l'image « clouds.png » que vous pouvez télécharger en cliquant avec le bouton droit sur l'image suivante :



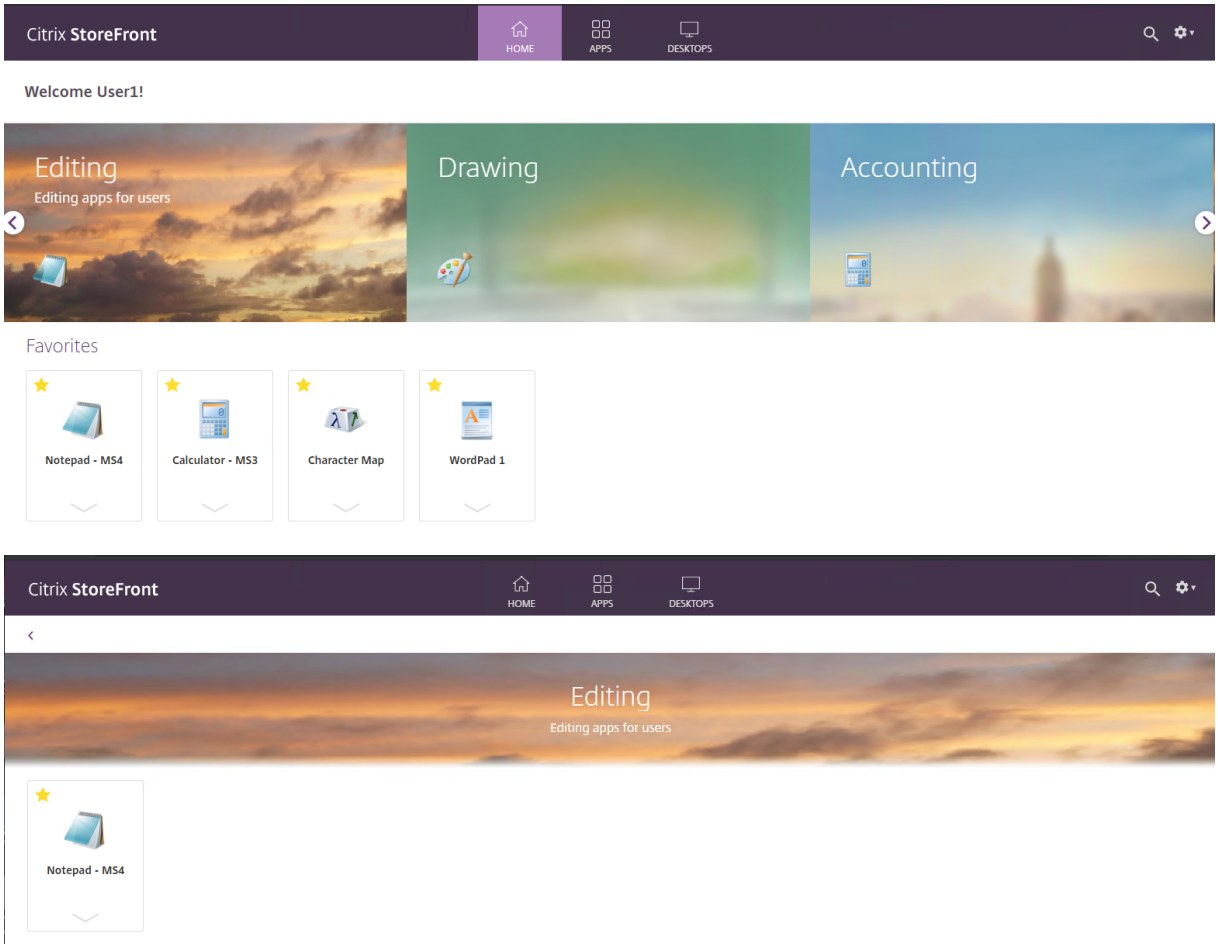
1. Enregistrez l'image dans le répertoire *custom*. La taille de l'image doit être d'environ 520 × 256 pixels pour être cohérente avec les autres (mais elle est mise à l'échelle au besoin).
2. Ajoutez ce qui suit à style.css :

```
1 .appBundle1 {
2
```



```
  background-image: url('clouds.png');
 }


.bundleDetail.appBundle1 {

  background-image: url('clouds.png');
  background-size: 100% 200%;
 }
```

Le résultat ressemble à ce qui suit :



Empêcher le logo d'une entreprise d'avoir l'air flou

Receiver for Web doit gérer correctement à la fois les écrans standard (DPI faible) et les écrans haute résolution plus récents (DPI élevé) qui ont un nombre plus élevé de pixels par pouce carré. Par exemple, la résolution des écrans Apple Retina est deux fois plus élevée que celle d'écrans non-Retina. Sur les ordinateurs portables, les écrans ont généralement une fois et demie (x1.5), deux fois (x2) ou même

trois fois (x3) le nombre « normal » de pixels pour leur taille. La résolution x2 étant la plus courante et la plus utile, la plupart des ressources d'images de l'application Citrix Workspace possèdent deux résolutions. Une image dont la résolution est de 100 × 100 pixels sur un écran normal a également une version dont la résolution est deux fois plus élevée (200 × 200 pixels).

Lorsque vous téléchargez des images de logo à partir de la console de gestion StoreFront, assurez-vous qu'il s'agit d'images avec une résolution x2. En d'autres termes, elles représentent environ le double de la largeur et de la hauteur de l'« espace » sur un écran régulier. (Les images téléchargées avec la résolution x1 ne sont pas agrandies avec la résolution x2.) L'« espace » sur un écran normal est de 170 × 40 pixels ; ainsi l'image du logo que vous téléchargez doit être d'environ 340 × 80 pixels.

StoreFront crée une copie du logo et le met à l'échelle à la moitié de la taille. Cette image est utilisée sur les écrans à faible résolution.

Parfois, cela se traduit par une image floue car la moitié des détails de l'image ont été ignorés. Ce phénomène est cependant rare car les logos ont tendance à être vifs et simples. Si votre logo rencontre ce problème, utilisez la solution suivante :

1. Créez deux versions de votre logo, une à la résolution x1 et une autre à la résolution x2, et enregistrez-les dans le répertoire *\custom*.
2. Modifiez le fichier *custom\style.css* afin qu'il fasse référence aux deux images différentes. Le résultat ressemble à ce qui suit :

```
<span style="color: green;">/* The following section of the file is
   reserved for use by StoreFront. \*/</span>
<span style="color: green;">/\* CITRIX DISCLAIMER: START OF MANAGED
   SECTION. PLEASE DO NOT EDIT ANY STYLE IN THIS SECTION \*/</span>
<span style="color: green;">/\* CITRIX DISCLAIMER: END OF MANAGED
   SECTION. \*/</span>
<span style="color: green;">/\* You may add custom styles below this
   line. */</span>

.logo-container {

    background-image: url('mylogo_x1.png');
    background-size: 169px 21px;
 }


.highdpi .logo-container {

    background-image: url('mylogo_x2.png');
    background-size: 169px 21px;
 }
```


> Remarque :
>
> - Assurez-vous que ces styles personnalisés n'apparaissent pas dans la zone « managed section ». Si c'est le cas, ils sont remplacés ou ils induisent la console de gestion StoreFront en erreur.
> - Les deux styles spécifient la même taille d'arrière-plan. En effet, la taille est spécifiée dans les unités « logiques » et pour l'image x2, la taille de l'arrière-plan est la moitié de la largeur et de la hauteur du logo réel.

Définir une image d'arrière-plan

> Remarque :
>
> L'expérience unifiée est conçue pour un arrière-plan blanc simple. Les images d'arrière-plan ont tendance à avoir un effet distrayant. Si vous ajoutez une image d'arrière-plan, essayez d'utiliser une image claire et simple. Si nécessaire, modifiez les polices pour qu'elles continuent de fonctionner avec cette image.

Exemple 1 : référence CSS à une image téléchargée

Modifiez custom.css comme suit :

```
.storeViewSection {

   background: url('images/background.jpg') no-repeat center center
      fixed;
   background-size: cover;
 }
```

> Remarque :
>
> L'instruction « background-size:cover; » ne fonctionne pas dans certains anciens navigateurs.

Exemple 2 : référence CSS à une image existante avec des réglages

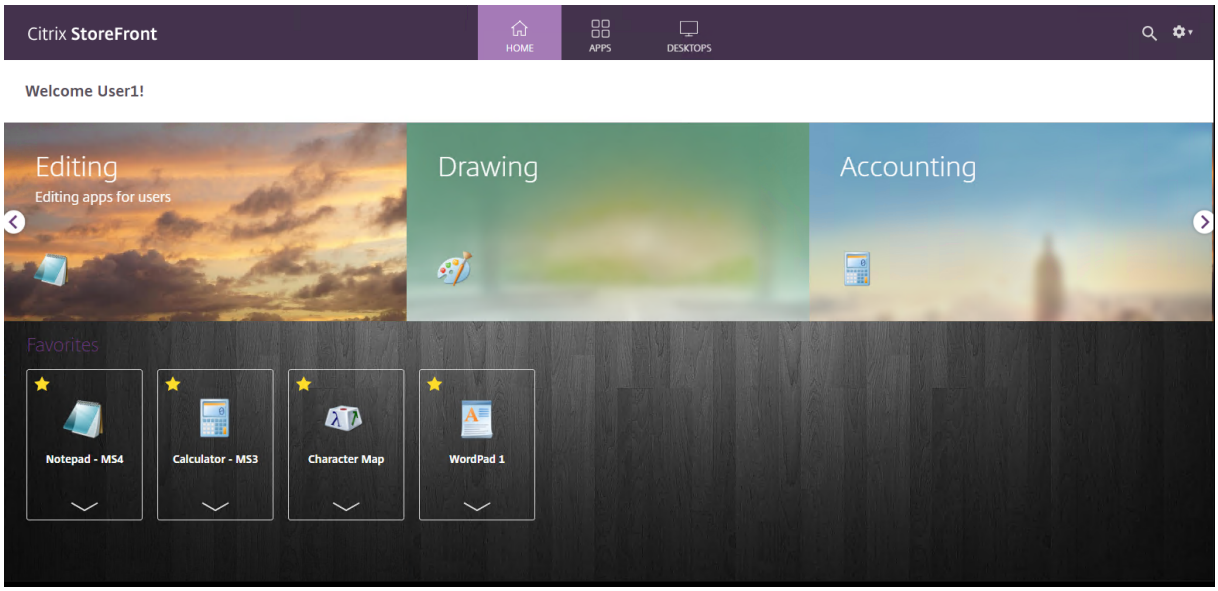
Modifiez custom.css comme suit :

```
.storeViewSection {

   background: url('../media/bg_bubbles.jpg') no-repeat center center
      fixed;
    background-size: cover;
    color: white;
 }
```



```
7
8
9  // Tweak fonts
10 .smallTiles .storeapp .storeapp-name,
11 .largeTiles .storeapp .storeapp-name {
12
13     color: white;
14  }
15
16
17 // Tweak bundle area so it doesn't clash as badly
18 .largeTiles .applicationBundleContainer {
19
20     background-color: rgba(255, 255, 255, 0.4);
21     margin-top: 0;
22     padding-top: 25px;
23  }
24
25
26 .smallTiles .applicationBundleContainer {
27
28     background-color: rgba(255, 255, 255, 0.4);
29     margin-top: 0;
30     padding-top: 14px;
31  }
```

Le résultat ressemble à ce qui suit :



Détecter les erreurs dans votre code

Il y a plusieurs façons d'effectuer un débogage. Essayez toujours d'utiliser d'abord un navigateur. Il s'agit d'une approche beaucoup plus facile que le débogage des personnalisations dans l'application Citrix Workspace. Vous pouvez ajouter les arguments suivants après « ? » ou « # » dans l'URL de la page, et vous pouvez associer plusieurs chaînes. Par exemple :

```
1 http://storefront.wwco.net/Citrix/StoreWeb/#-tr-nocustom
```

-errors : nous essayons généralement de supprimer toutes les erreurs qui pourraient se produire dans le code, mais vous pouvez les surligner à la place. Cet argument affiche un message d'alerte lorsqu'une erreur se produit.

-debug : cet argument désactive toute gestion des exceptions pour le code de personnalisation. Cet argument utile peut être utilisé avec les outils de développement intégrés aux navigateurs modernes (comme F12 dans Google Chrome ou Internet Explorer), et vous permet de déboguer vous-même les exceptions.

-nocustom : cet argument désactive votre script et vos personnalisations CSS. Il s'agit d'un argument utile si l'application Citrix Workspace ne fonctionne pas et que vous souhaitez savoir si cela est causé par une erreur que vous avez introduite.

-tr : cet argument fournit le suivi du code de l'interface utilisateur de l'application Citrix Workspace dans un onglet de navigateur séparé, y compris le suivi que vous ajoutez avec les appels à **CTXS.ExtensionAPI.trace()**.

Expérience utilisateur unifiée

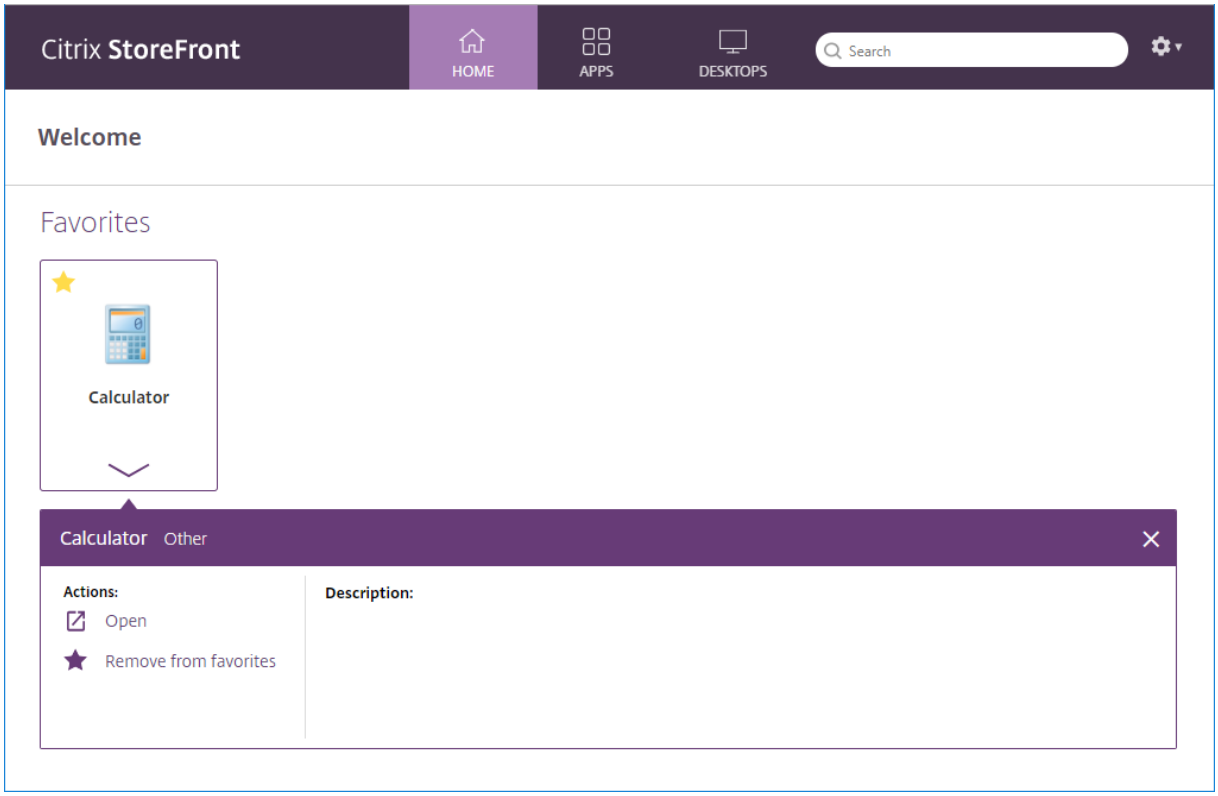
Cette section décrit les fonctionnalités et l'aspect de l'expérience unifiée.

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.

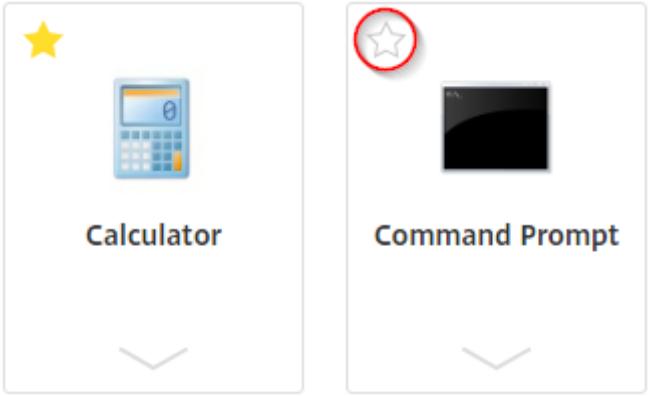
Accueil

L'écran d'accueil affiche les favoris.



Favoris

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



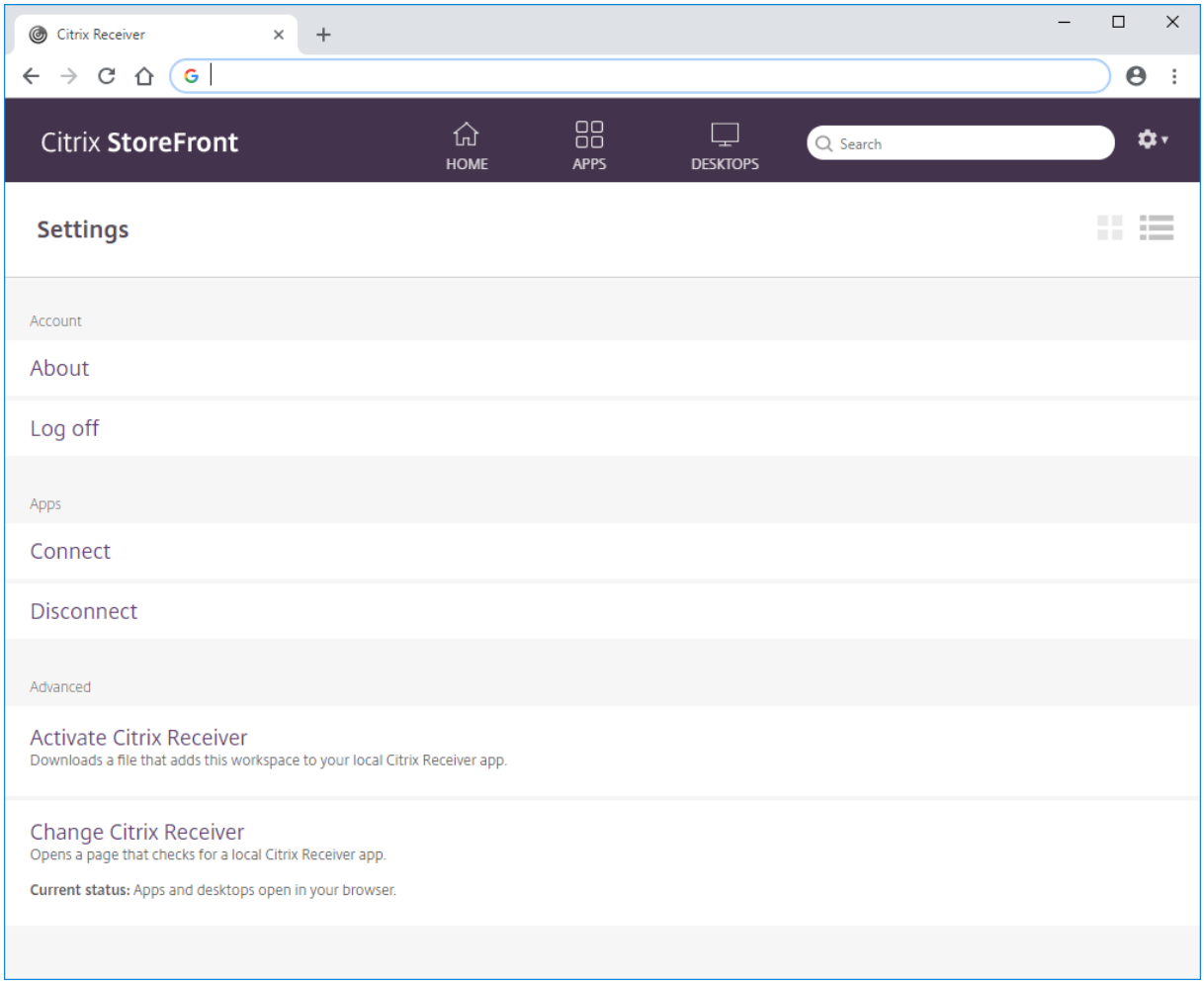
Rechercher

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 l'application Citrix Workspace 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 Workspace locale.

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

Créer et gérer des applications recommandées

March 3, 2020

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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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**.

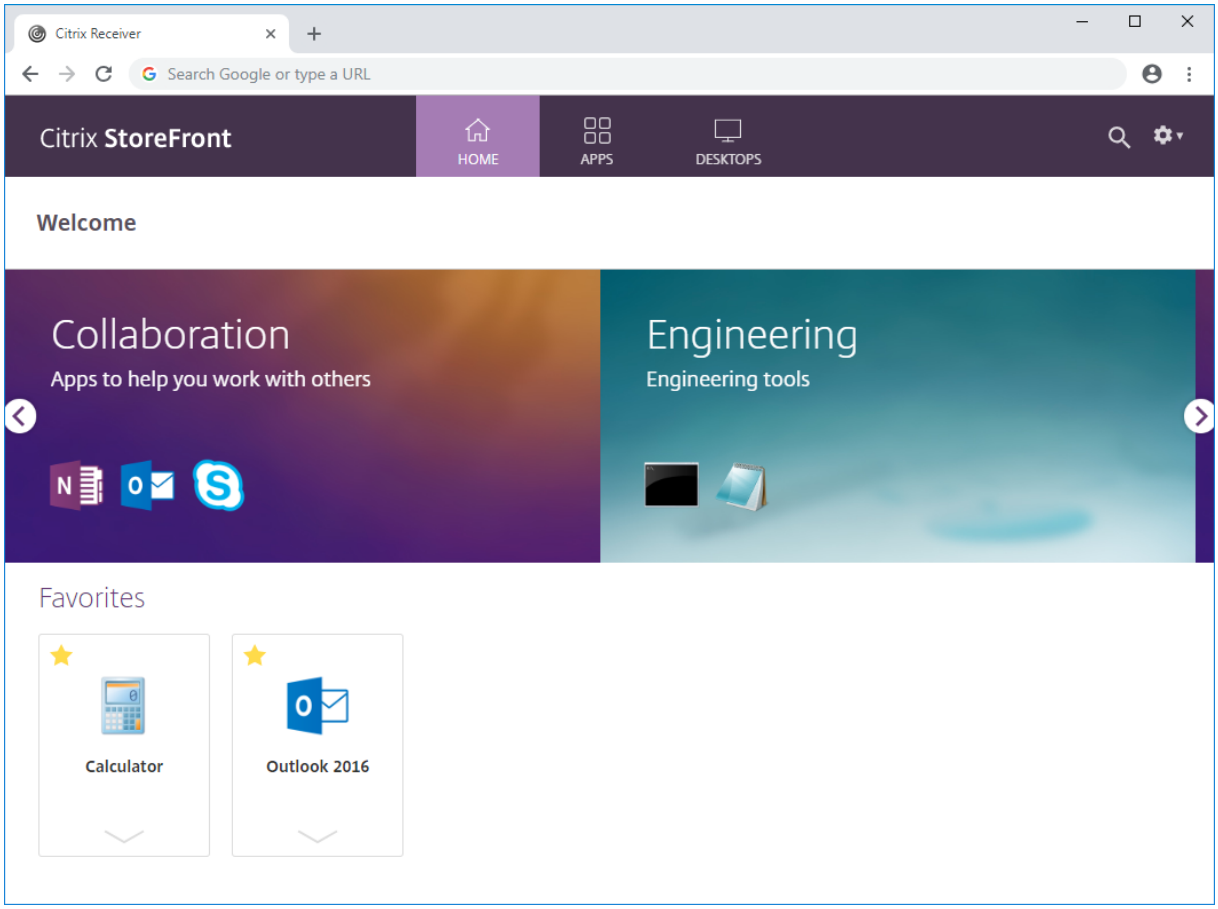
3. Sélectionnez **Groupes d'applications recommandées**.
4. Dans la boîte de dialogue **Groupes d'applications recommandées**, cliquez sur **Créer** pour définir un nouveau groupe d'applications recommandées.
5. Dans la boîte de dialogue **Créer un groupe d'applications recommandées**, spécifiez le nom, 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 `Exc` 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

March 3, 2020

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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 l'application Citrix Workspace pour HTML5

March 3, 2020

Par défaut, l'application Citrix Workspace 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 l'application Citrix Workspace 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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 l'application Workspace/Citrix Receiver**.
4. À partir de la liste **Options de déploiement**, sélectionnez **Toujours utiliser Receiver pour HTML5** 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

March 3, 2020

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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 l'application Citrix Workspace

1. Pour l'application Citrix Workspace installée sur StoreFront Server, accédez au chemin d'accès du service d'authentification de votre magasin. Dans les versions récentes de StoreFront, ce chemin correspond à **c:\inetpub\wwwroot\Citrix\<Store>Auth**(qui peut être l'un des nombreux services d'authentification en fonction du nombre de magasins que vous possédez).

   Dans les anciennes versions de StoreFront, le chemin d'accès correspond à **c:\inetpub\wwwroot\Citrix\Authentication**(qui peut être partagé entre les services d'authentification ou être le seul sur le serveur).

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 :
>
> Application Citrix Workspace pour Windows et application Citrix Workspace pour 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

March 3, 2020

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 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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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

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 l'application Citrix Workspace. 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 :

```
$dsInstallProp = Get-ItemProperty '
-Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $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
```

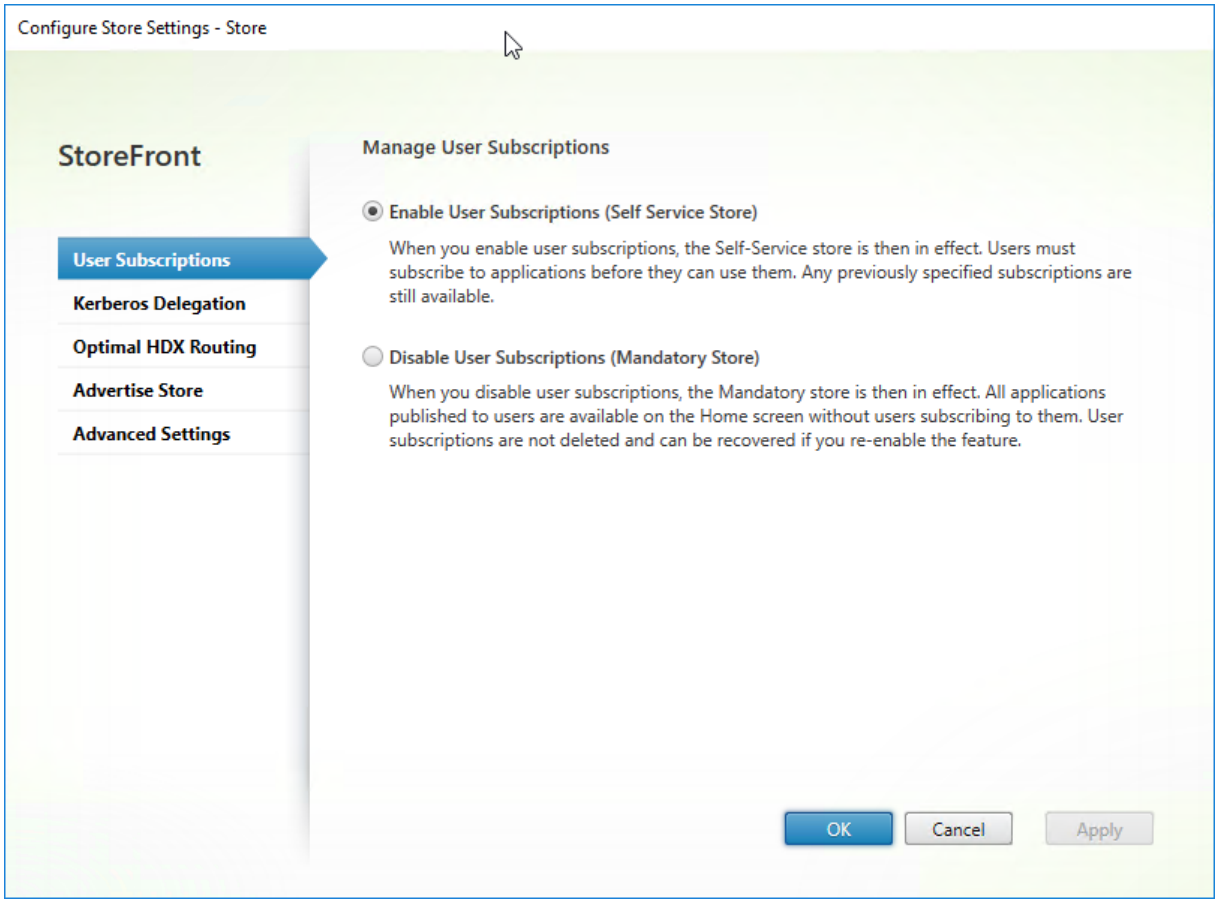
Configurer les abonnements des utilisateurs

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 l'application Citrix Workspace. 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.



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/

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

June 13, 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 sur le serveur StoreFront dans le répertoire `\inetpub\wwwroot\Citrix\StoreName\App_Data`.
2. Dans le fichier default.ica, recherchez les lignes : `[ApplicationServers] application=`.
3. Créez une ligne après `application=` et ajoutez les paramètres suivants :

   ```
   [Notepad]
   TWIMode=Off
   DesiredHRES=1024
   DesiredVRES=768
   ```

4. Enregistrez le fichier.

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

1. Modifiez le fichier *web.config* sur le serveur StoreFront dans le répertoire `C:\inetpub\wwwroot\Citrix\storeWeb`.
2. Dans le fichier web.config, recherchez 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>**

Remarques

`DeisredHRES` 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 XenApp Services. 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

March 3, 2020

> **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 ce processus terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 appliances Citrix Gateway distinctes pour vos déploiements, vous pouvez définir l'appliance optimale que les utilisateurs doivent utiliser pour accéder à chacun des déploiements.

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 Citrix 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.

1. Vérifiez que vous avez configuré le magasin avec les détails de tous les déploiements Citrix Virtual Apps and Desktops que vous souhaitez 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** pour agréger les ressources de plusieurs déploiements. Lorsque les Delivery Controller sont agrégés, 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 l'application Citrix Workspace.

   a) Pour agréger les Delivery Controller, sélectionnez plusieurs contrôleurs et cliquez sur **Agréger**.

   b) Sélectionnez les options **Paramètres Controller agrégés** :

      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.

7. Dans la boîte de dialogue Configuration du mappage utilisateur et de l'agrégation multisite, cliquez sur **OK**.
8. Dans la boîte de dialogue Gérer les Delivery Controller, cliquez sur **OK**.

Configurations avancées

Vous pouvez configurer la plupart des opérations multisite et de haute disponibilité courantes à l'aide de la console de gestion StoreFront. Vous pouvez également configurer StoreFront à l'aide de PowerShell ou en modifiant les fichiers de configuration StoreFront, ce qui fournit les fonctionnalités supplémentaires suivantes :

- 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.
- 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.
- 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.

1. Vérifiez que vous avez configuré le magasin avec les détails de tous les déploiements Citrix Virtual Apps and Desktops que vous souhaitez 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>
```



```
<resourcesWingConfiguration name="Default" wingName="Default" />
</resourcesWingConfigurations>
```

4. Spécifiez votre configuration comme illustré ci-dessous.

```
<resourcesWingConfigurations>
<resourcesWingConfiguration name="Default" wingName="Default">
<userFarmMappings>
<clear />
<userFarmMapping name="user_mapping">
<groups>
<group name="domain\usergroup" sid="securityidentifier" />
<group ... />
...
</groups>
<equivalentFarmSets>
<equivalentFarmSet name="setname" loadBalanceMode="{
 LoadBalanced | Failover }
 "
aggregationGroup="aggregationgroupname">
<primaryFarmRefs>
<farm name="primaryfarmname" />
<farm ... />
...
</primaryFarmRefs>
<backupFarmRefs>
<farm name="backupfarmname" />
<farm ... />
...
</backupFarmRefs>
</equivalentFarmSet>
<equivalentFarmSet ... >
...
</equivalentFarmSet>
</equivalentFarmSets>
</userFarmMapping>
<userFarmMapping>
...
</userFarmMapping>
</userFarmMappings>
</resourcesWingConfiguration>
</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 l'ensemble 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 ensembles de déploiement équivalents qui fournissent les ressources à regrouper. Les ressources fournies par les ensembles de déploiement équivalents qui appartiennent au même groupe d'agrégation sont regroupées. Pour indiquer que les déploiements définis dans un ensemble 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 ensemble de sites Citrix Virtual Apps and Desktops 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 corre-

spondre exactement aux noms que vous avez entrés lorsque vous avez ajouté les déploiements au magasin.

- **optimalGatewayForFarms** : spécifie les groupes de déploiements et définit les appliances Citrix Gateway optimales que les utilisateurs doivent utiliser pour accéder aux ressources fournies par ces déploiements. En général, l'appliance optimale pour un déploiement figure dans le même emplacement géographique que ce déploiement. Vous ne devez définir les appliances Citrix Gateway optimales pour les déploiements uniquement lorsque l'appliance à partir de laquelle les utilisateurs accèdent à StoreFront n'est pas l'appliance optimale.

Configurer la synchronisation des abonnements

Pour configurer la synchronisation régulière par envoi de données (pull) des abonnements des utilisateurs 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.

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. Si vous synchronisez des abonnements à partir de ressources agrégées, le nom des groupes d'agrégation utilisés par les deux magasins doit également correspondre. Les noms des Delivery Controller et les noms des groupes d'agrégation sont sensibles à la casse ; par exemple, *XenDesktop7* ne correspond pas à *Xendesktop7*.

1. Utilisez un compte disposant des autorisations d'administrateur local pour démarrer Windows PowerShell ISE.
2. Pour configurer la synchronisation à un moment donné chaque jour, exécutez la commande suivante.

```
$RepeatMinutes = 30
Add-STFSubscriptionSynchronizationSchedule -StartTime (Get-Date -
    Format t) -RepeatMinutes $RepeatMinutes
```

Utilisez **-StartTime** pour spécifier quand la planification de synchronisation démarre.

L'utilisation de **(Get-Date -Format t)** démarre immédiatement la planification de synchronisation, tandis que la spécification *10:00* démarre la planification récurrente à l'heure spécifiée.

-RepeatMinutes définit la fréquence à laquelle la planification s'exécute. Par exemple, *30* exécute la planification toutes les demi-heures et *180* toutes les 3 heures. Nous vous recommandons de décaler les planifications d'extraction pour éviter que deux groupes de serveurs ne tentent d'extraire les données d'abonnement les uns des autres en même temps. Par exemple, une planification pour extraire des données de chaque groupe de serveurs toutes les 60 minutes est configurée comme suit. Le Groupe de serveurs 1 extrait les données du Groupe de serveurs 2 à 01:00, 02:00, 03:00 et ainsi de suite. Le Groupe de serveurs 2 extrait les données du Groupe de serveurs 1 à 01h30, 02h30, 03h30 et ainsi de suite.

3. Pour spécifier le déploiement StoreFront distant contenant le magasin à synchroniser, tapez la commande suivante. Vous devez configurer cette planification pour chaque data center où réside un groupe de serveurs StoreFront afin qu'il puisse extraire les données d'abonnement d'autres data centers distants. Vous trouverez ci-dessous des exemples de data centers aux États-Unis et au Royaume-Uni :

   - Exécutez cette commande sur les serveurs StoreFront du data center aux États-Unis pour extraire les données des serveurs du data center au Royaume-Uni :

   ```
   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
       Citrix/Store"
   Add-STFSubscriptionSynchronizationSource -FriendlyName "
       SyncFromUKStore" -StoreService $StoreObject -
       RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
       com"
   ```

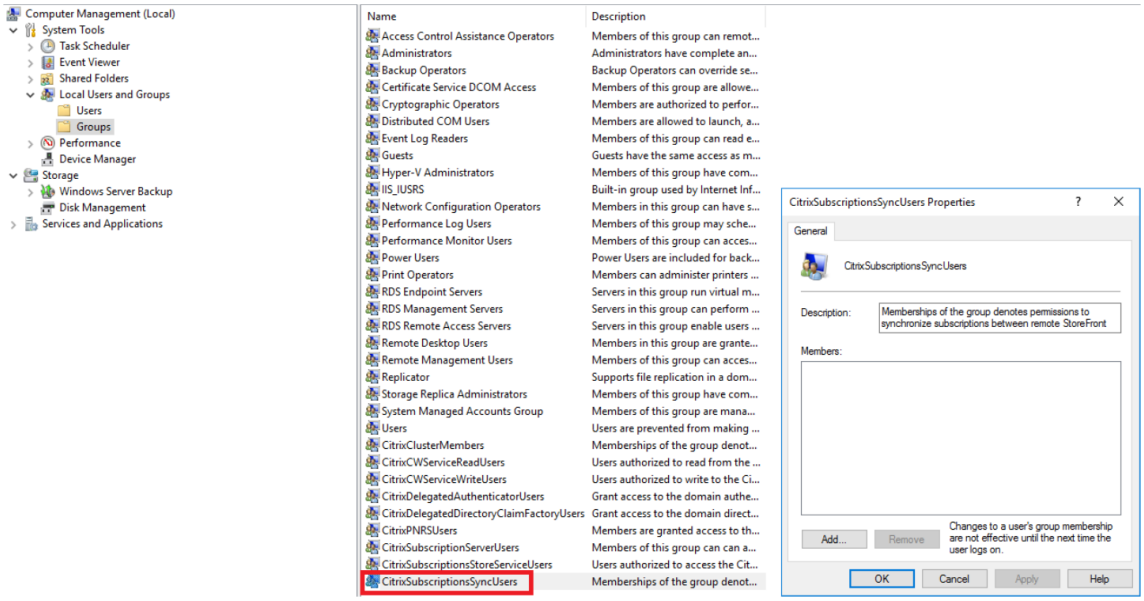
   - Exécutez cette commande sur les serveurs StoreFront du data center au Royaume-Uni pour extraire les données des serveurs du data center aux États-Unis :

   ```
   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
       Citrix/Store"
   Add-STFSubscriptionSynchronizationSource -FriendlyName "
       SyncFromUSStore" -StoreService $StoreObject -
       RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
       com"
   ```

   où *FriendlyName* est un nom qui vous aide à identifier le déploiement distant et *RemoteStoreFrontAddress* est le nom de domaine complet du serveur StoreFront ou d'un groupe de serveurs avec équilibrage de la charge pour le déploiement distant. Pour synchroniser les abonnements aux applications entre deux ou plusieurs magasins, tous les magasins qui doivent être synchronisés doivent porter le même nom dans leur déploiement StoreFront respectif.

4. 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.

   Cela permet aux serveurs actuels d'extraire de nouvelles données d'abonnement ou des données d'abonnement mises à jour à partir des serveurs distants répertoriés dans le groupe CitrixSubscriptionSyncUsers une fois que vous avez configuré une planification de synchronisation. Pour plus d'informations sur la modification des groupes d'utilisateurs locaux, consultez http://technet.microsoft.com/en-us/library/cc772524.aspx.



5. Une fois la planification configurée, utilisez la console de gestion Citrix StoreFront ou Powershell ci-dessous pour propager les planifications et les sources de synchronisation des abonnements à tous les autres serveurs du groupe.

```
1 Publish-STFServerGroupConfiguration
```

   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.

6. Pour supprimer une planification de synchronisation d'abonnement existante, exécutez la commande suivante ; propagez ensuite les modifications apportées à la configuration aux autres serveurs StoreFront dans le déploiement.

```
1 Clear-STFSubscriptionSynchronizationSchedule
```

7. Pour supprimer une source de synchronisation d'abonnement spécifique, exécutez la commande suivante ; propagez ensuite les modifications apportées à la configuration aux autres serveurs StoreFront dans le déploiement.


```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
```

8. Pour supprimer toutes les sources de synchronisation d'abonnement existantes, exécutez la commande suivante ; propagez ensuite les modifications apportées à la configuration aux autres serveurs StoreFront dans le déploiement.

```
Clear-STFSubscriptionSynchronizationSource
```

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

```
Get-STFSubscriptionSynchronizationSchedule
```

10. Pour répertorier les sources de synchronisation d'abonnement actuellement configurées pour votre déploiement StoreFront, exécutez la commande suivante.

```
Get-STFSubscriptionSynchronizationSource
```

Configurer un routage HDX optimal pour un magasin

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 Citrix Virtual Apps and Desktops en zones en fonction du centre de données ou de l'emplacement géographique dans lequel les Controller Citrix Virtual Apps and Desktops et les ressources publiées résident. Définissez des zones dans Citrix Virtual Apps and Desktops Studio. StoreFront interagit avec Citrix Virtual Apps and Desktops ; par conséquent toute zone définie dans StoreFront doit correspondre en tout point aux noms de zones définis dans Citrix Virtual Apps and Desktops.

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 Citrix Virtual Apps and Desktops. Vous pouvez mapper une passerelle optimale à

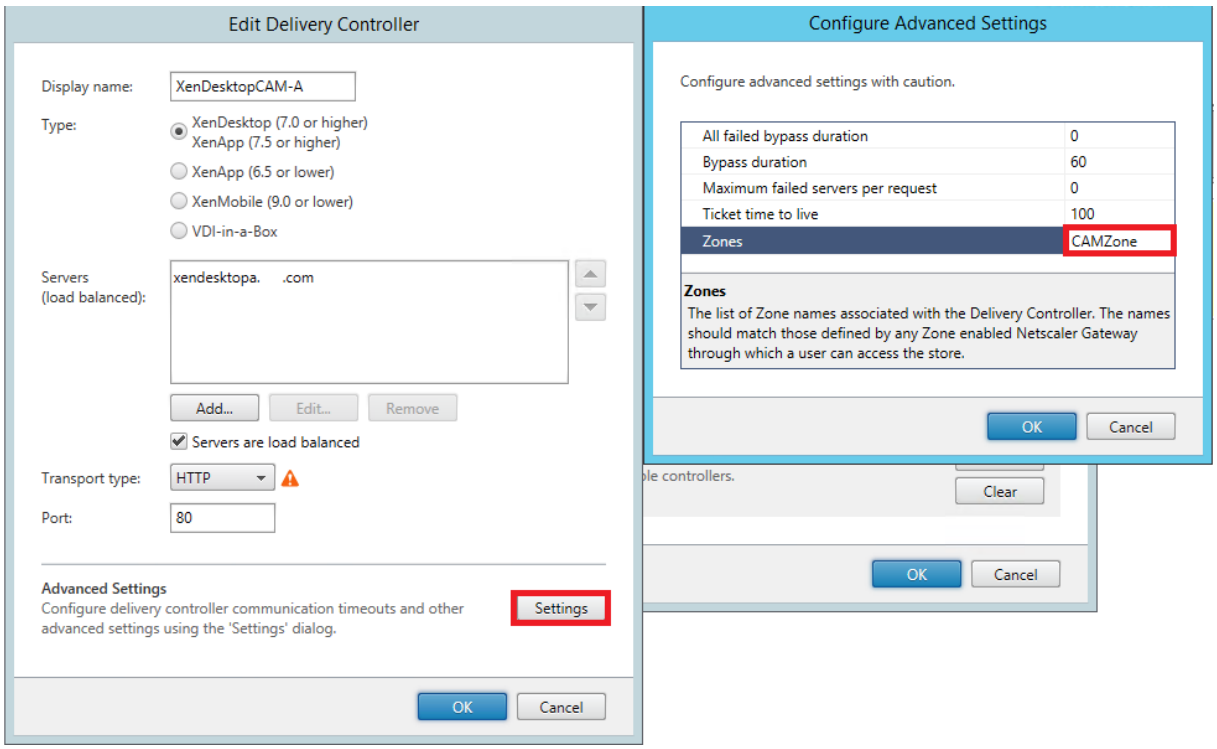
plus d'une zone, mais il est généralement recommandé de n'utiliser qu'une seule zone. Une zone représente généralement un centre de données dans un emplacement géographique. Chaque zone doit disposer d'au moins une passerelle Citrix Gateway optimale utilisée pour les connexions HDX aux ressources dans 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 souhaitez 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 Citrix 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 Citrix Virtual Apps and Desktops 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 les appliances Citrix Gateway optimales pour les déploiements uniquement lorsque l'appliance à partir de laquelle 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 Citrix Gateway FR et US, ainsi que de contrôleurs 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

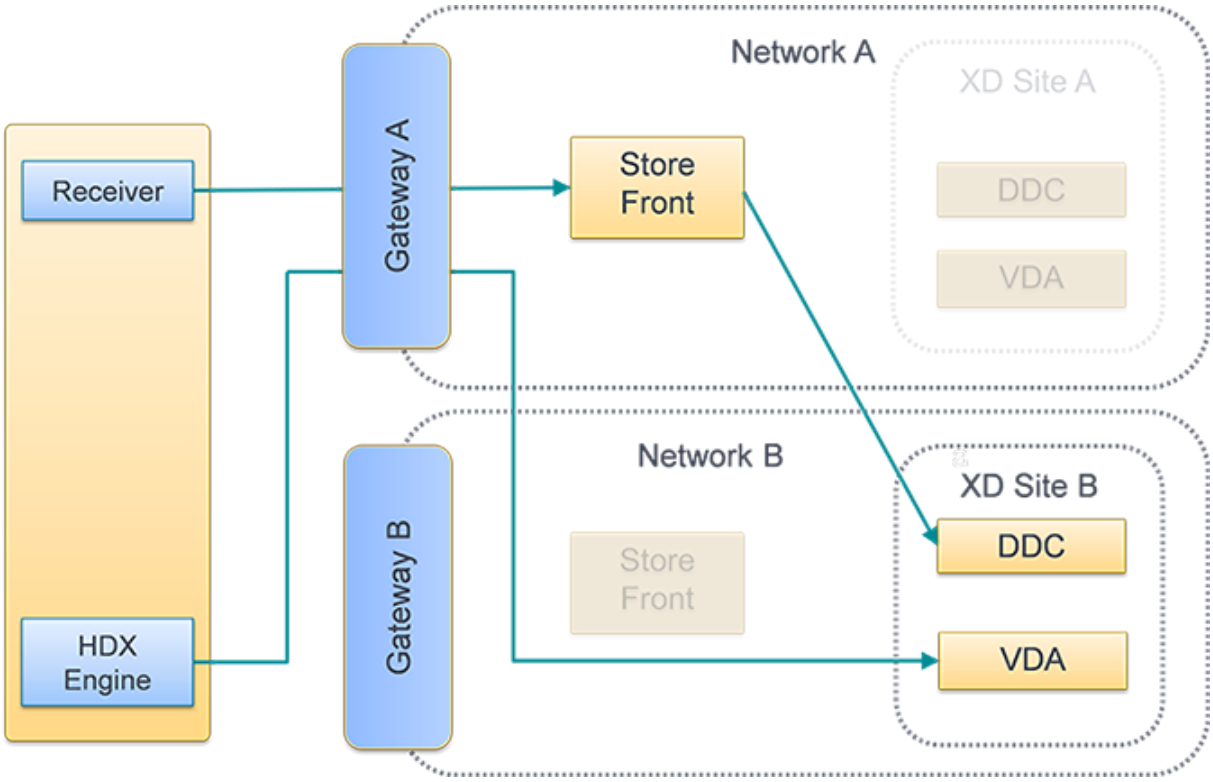
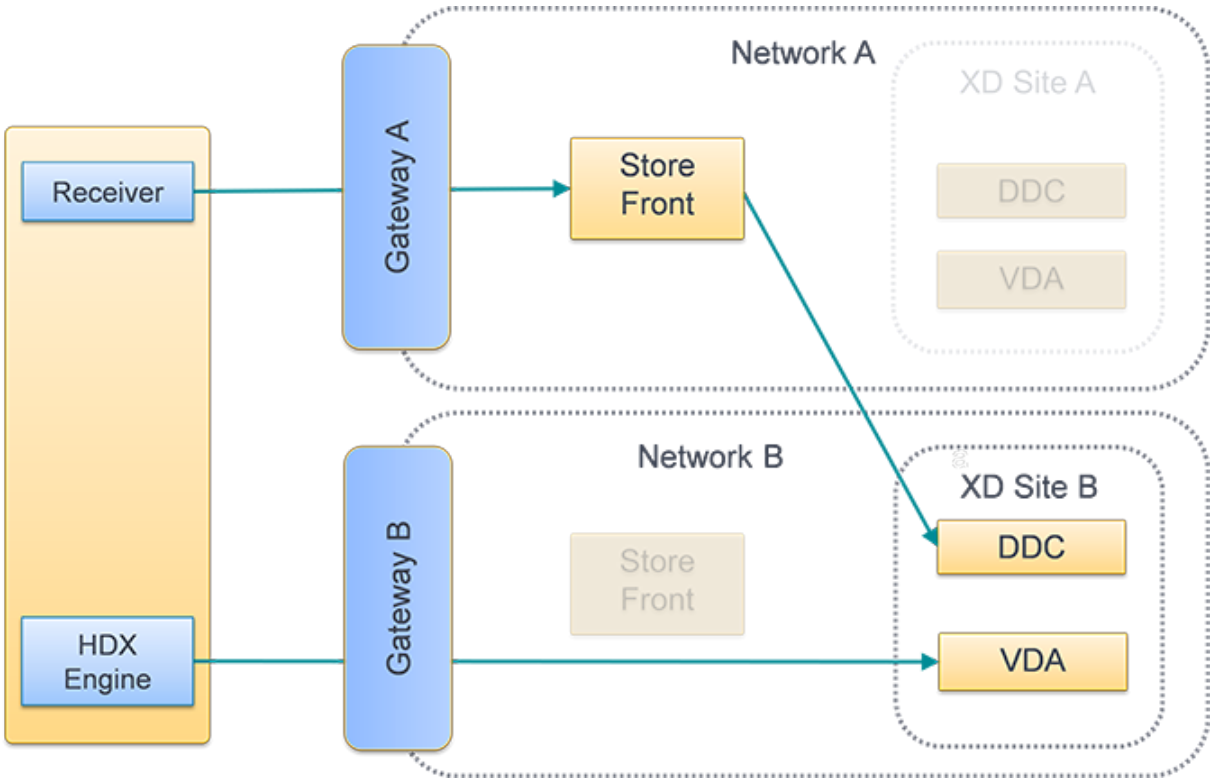


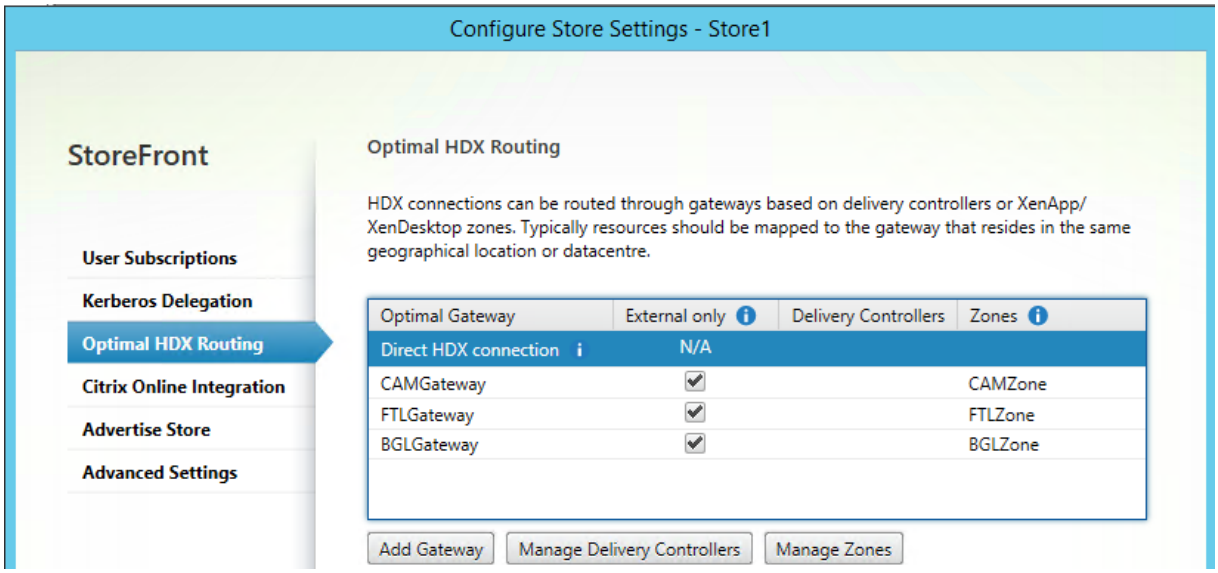
Figure 2. Routage vers la passerelle optimal



Utilisation de la console de gestion Citrix StoreFront

Après avoir configuré des appliances Citrix Gateway distinctes pour vos déploiements, vous pouvez définir l'appliance optimale 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 une appliance Citrix Gateway s'affiche.

1. Sur l'écran **Paramètres généraux**, définissez les paramètres Nom d'affichage, URL Citrix Gateway et Utilisation ou rôle pour configurer l'accès aux magasins via Citrix Gateway pour les utilisateurs se connectant depuis des réseaux publics. L'accès distant via Citrix 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 Citrix Virtual Apps and Desktops et émet des tickets de session en réponse aux demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources Citrix Virtual Apps and Desktops.
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 Citrix 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 Citrix Gateway dans StoreFront.

Exemple 1 : ExternalGateway

Exemple 2 : InternalGateway

-Hostnames (String Array) — Spécifie le nom de domaine complet (FQDN) et le port de l'appliance Citrix Gateway optimale.

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 ensemble de déploiements Citrix Virtual Apps and Desktops (généralement colocalisés) qui partagent une appliance Citrix Gateway optimale commune. Une batterie de serveurs peut contenir un ou plusieurs Delivery Controller qui fournissent des ressources publiées.

Vous pouvez configurer un site Citrix Virtual Desktops 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 souhaitez les allouer.

-staUrls (String Array) — Spécifie les adresses URL des serveurs Citrix Virtual Apps and Desktops 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 souhaitez 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 l'appliance optimale définie pour la batterie. Si cet attribut est défini sur **false** : les connexions aux ressources ne sont pas routées via l'appliance optimale pour la batterie sauf si les utilisateurs accèdent à StoreFront via Citrix 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-DSStoreOptimalGateway** pour ajouter la configuration de passerelle optimale.
>
> Exemple :
>
> ```
> Add-DSGlobalV10Gateway -Id 2eba0524-af40-421e-9c5f-a1ccca80715f -Name
> LondonGateway -Address ”http://example”-Logon Domain -SecureTicketAuthorityUrls
> ```



```
 @("http://staurl1", "http://staurl2")
Add-DSStoreOptimalGateway -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**.

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.
    ps1"

Set-DSOptimalGatewayForFarms -SiteId 1 ‘

-ResourcesVirtualPath /Citrix/Internal ‘
-GatewayName "gateway1" ‘
-Hostnames "gateway1.example.com:500" ‘
-Farms "XenApp","XenDesktop" ‘
-StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
    xendesktop.example.com/scripts/ctxsta.dll" ‘
-StasUseLoadBalancing:$false ‘
-StasBypassDuration 02:00:00 ‘
-EnableSessionReliability:$false ‘
-UseTwoTickets:$false ‘
-EnabledOnDirectAccess:$true
```

Configurer une passerelle optimale pour une zone

Exemple

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

```
**& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules
    .ps1" **

\*\*Set-DSOptimalGatewayForFarms -SiteId 1 ‘\*\*

**-ResourcesVirtualPath /Citrix/Internal ‘
-GatewayName "gateway1" ‘
-Hostnames "gateway1.example.com:500" ‘
-Zones "CAMZone" ‘
```



```
-StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
    xendesktop.example.com/scripts/ctxsta.dll" ‘
-StasUseLoadBalancing:$false ‘
-StasBypassDuration 02:00:00 ‘
-EnableSessionReliability:$false ‘
-UseTwoTickets:$false ‘
-EnabledOnDirectAccess:$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"
```

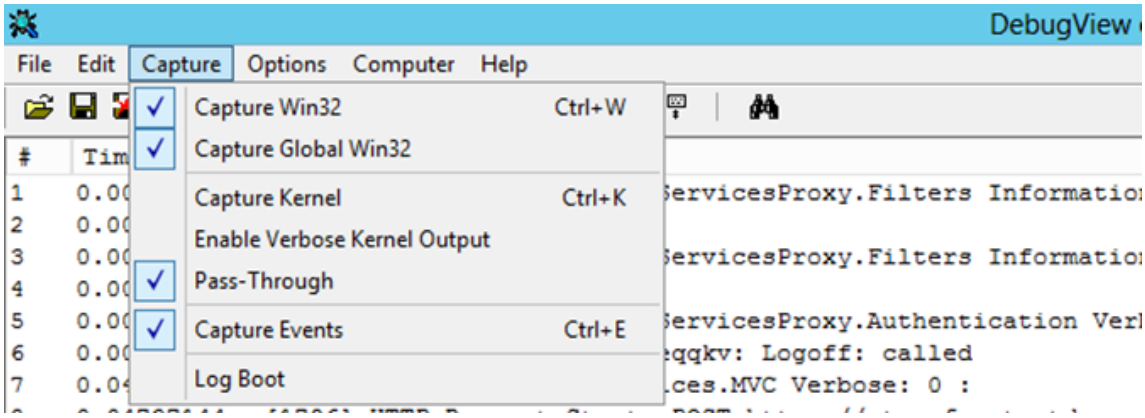

Déterminer si vos mappages de passerelle optimale de batteries sont utilisés par StoreFront

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

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\
    ImportModules.ps1"‘

#Traces output is to c:\Program Files\Citrix\Receiver Storefront\
    admin\trace\
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

```
- Un client externe se connecte à **Gateway1**. Le lancement est dirig
    é vers la passerelle optimale désignée **Gateway2** pour la batterie
     **Farm2**.

    Set-DSOptimalGatewayForFarms -onDirectAccess=false
```



```
4
5       Farm2 est configurée pour utiliser la passerelle optimale Gateway2.
6
7       L'accés 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'accés 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.
```

Intégrer avec Citrix Gateway et Citrix ADC

January 8, 2020

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 contrôleurs Citrix Virtual Apps and Desktops 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 Chiffrement de bout en bout avec 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 de plus amples 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 **Gérer les sites Receiver pour Web** pour le Web.

4. Sélectionnez le site Citrix Receiver pour Web correspondant, cliquez sur **Configurer**, puis sélectionnez **Méthodes d'authentification**.
5. Assurez-vous que l'option **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 Citrix Gateway

March 3, 2020

Utilisez la tâche Ajouter une appliance Citrix Gateway pour ajouter des déploiements Citrix Gateway au travers desquels les utilisateurs peuvent accéder à vos magasins. Vous devez activer la méthode d'authentification pass-through de Citrix Gateway avant de pouvoir configurer l'accès distant à vos magasins au travers de Citrix Gateway. Pour plus d'informations sur la configuration de Citrix 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 Citrix Gateway**.
3. Cliquez sur **Ajouter**, sélectionnez Paramètres généraux et spécifiez un **nom d'affichage** pour le déploiement Citrix 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 d'affichage de vos déploiements Citrix 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 Citrix Gateway. L'utilisation d'un même nom de domaine complet pour StoreFront et le serveur virtuel Citrix 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 de l'appliance Citrix Gateway, si nécessaire. Une adresse IP de sous-réseau est requise pour les appliances Access Gateway 9.3, mais facultative pour les versions plus récentes du produit.

   L'adresse de sous-réseau correspond à l'adresse IP que Citrix 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 de l'appliance Citrix 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 une appliance exécutant Citrix Gateway, sélectionnez dans la liste Type d'ouverture de session la méthode d'authentification que vous avez configurée sur l'appliance pour les utilisateurs de l'application Citrix Workspace.

   Les informations que vous fournissez sur la configuration de votre appliance Citrix Gateway sont ajoutées au fichier de provisioning pour le magasin. Ceci permet à l'application Citrix Workspace d'envoyer une demande de connexion appropriée lorsque vous contactez l'appliance 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 parmi 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 Citrix Gateway ou une seule appliance Access Gateway 5.0, entrez l'adresse URL du service d'authentification Citrix 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 de l'appliance accessible en interne. StoreFront contacte le service d'authentification Citrix Gateway pour vérifier que les requêtes reçues de Citrix Gateway proviennent de cette appliance.
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 Suivant.

    StoreFront utilise le service d'authentification pour authentifier les utilisateurs distants afin de leur éviter de ressaisir leurs informations d'identification lorsqu'ils accèdent aux magasins.
11. Pour tous les déploiements, si vous mettez les ressources fournies par Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops et émet des tickets de session en réponse aux demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources Citrix Virtual Apps and Desktops.

12. Si vous souhaitez que Citrix Virtual Apps and Desktops maintienne les sessions déconnectées ouvertes pendant que l'application Citrix Workspace tente de se reconnecter automatiquement, sélectionnez la case à cocher 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 Citrix 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 Citrix Gateway.

Pour fournir l'accès aux magasins via Citrix Gateway, un point balise interne et au moins deux points balises externes sont requis. L'application Citrix Workspace 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 Citrix 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 Citrix Gateway, assurez-vous de configurer l'accès à distance des utilisateurs pour ces magasins.

Importer un appliance Citrix Gateway

July 9, 2019

Les paramètres de l'accès à distance configurés dans la console d'administration de Citrix Gateway doivent être identiques à ceux configurés dans StoreFront. Cet article vous explique comment importer les détails d'un serveur virtuel Citrix Gateway de façon à ce que Citrix Gateway 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 :**
  >
  > Les appliances Citrix ADC peuvent uniquement exporter les vServers de passerelle créés à l'aide de l'assistant Citrix Virtual Apps and Desktops.

- 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 l'appliance Citrix ADC.
- Le fichier GatewayConfig.json du fichier ZIP généré par l'appliance Citrix ADC doit contenir l'adresse URL d'un site Citrix Receiver pour Web existant sur le serveur StoreFront. Citrix ADC 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

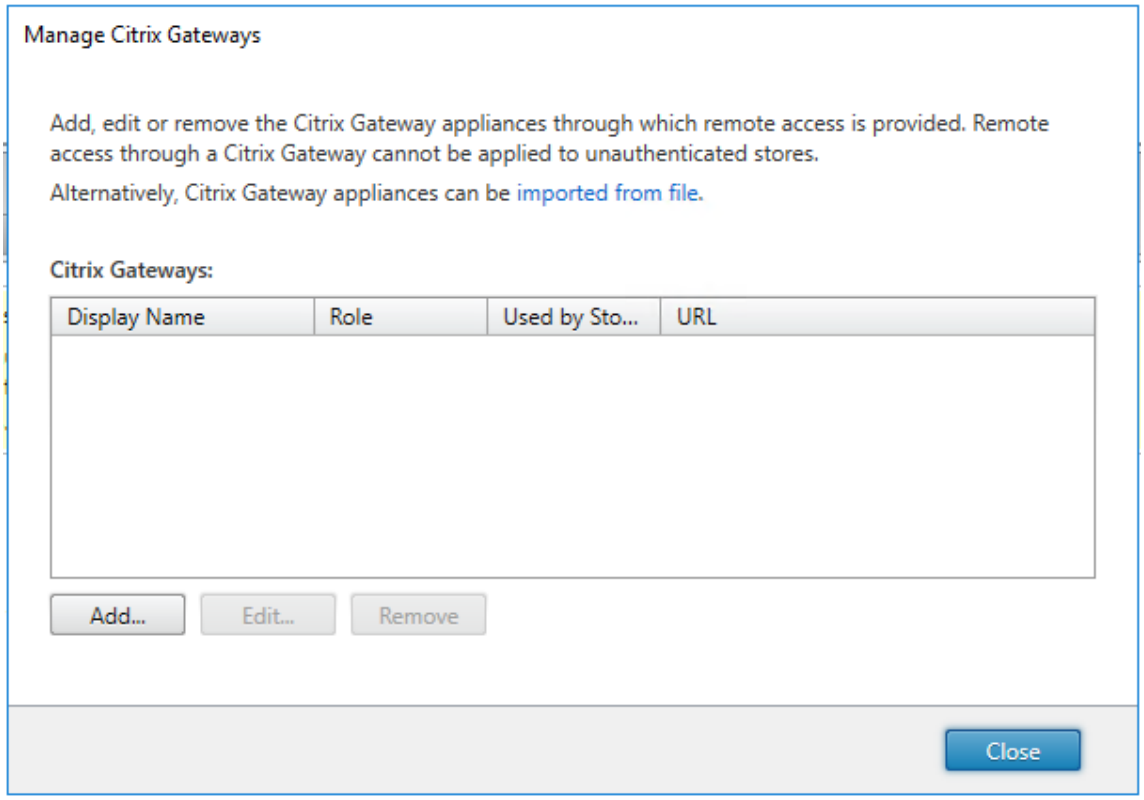
  L'URL de rappel et la combinaison de ports peuvent être différentes de l'adresse URL et de la combinaison de ports de la passerelle si vous utilisez des espaces de noms DNS externes et internes différents dans votre environnement. Si votre passerelle se trouve dans une zone démilitarisée (DMZ) et utilise 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 une appliance Citrix Gateway à l'aide de la console

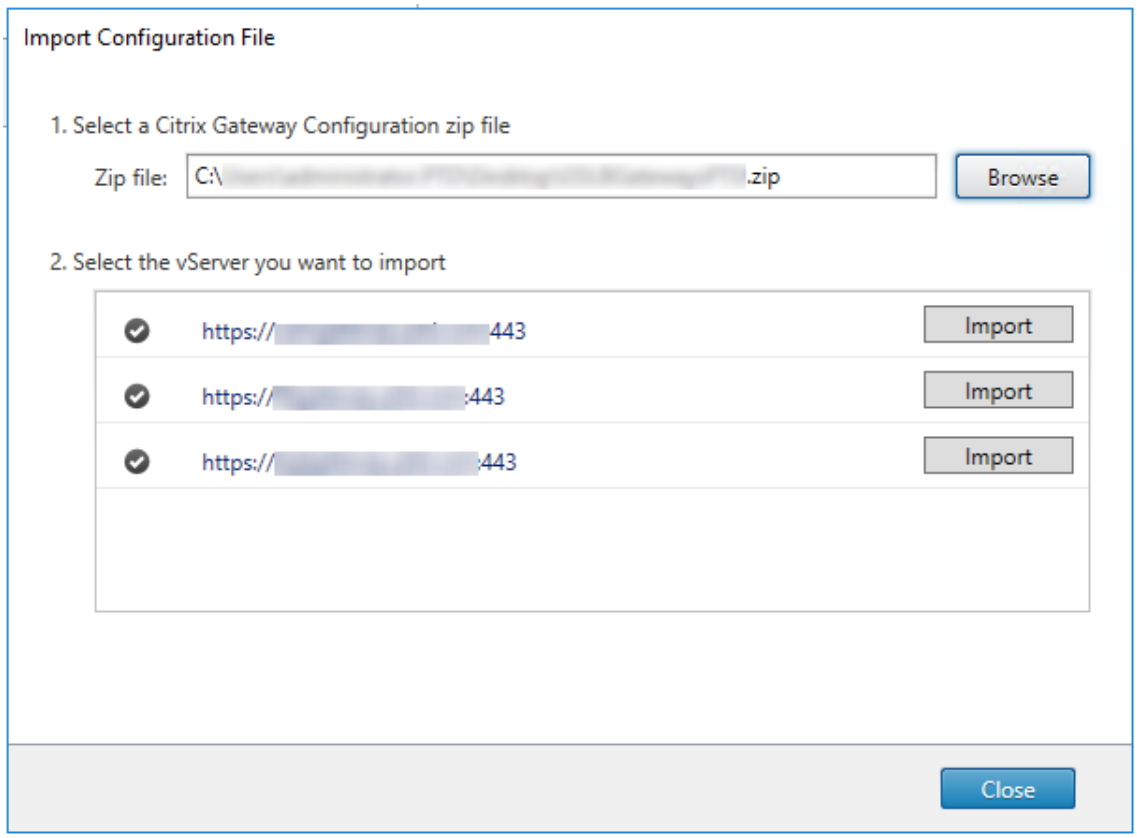
Vous pouvez importer une ou plusieurs configurations de serveur virtuel Citrix Gateway à l'aide du même fichier d'importation. Si vous disposez de plusieurs serveurs virtuels de passerelle provenant de différentes appliances Citrix ADC, vous devez utiliser plusieurs fichiers d'importation.

> Important :
>
> Citrix ne prend pas en charge la modification manuelle du fichier de configuration exporté depuis Citrix Gateway.

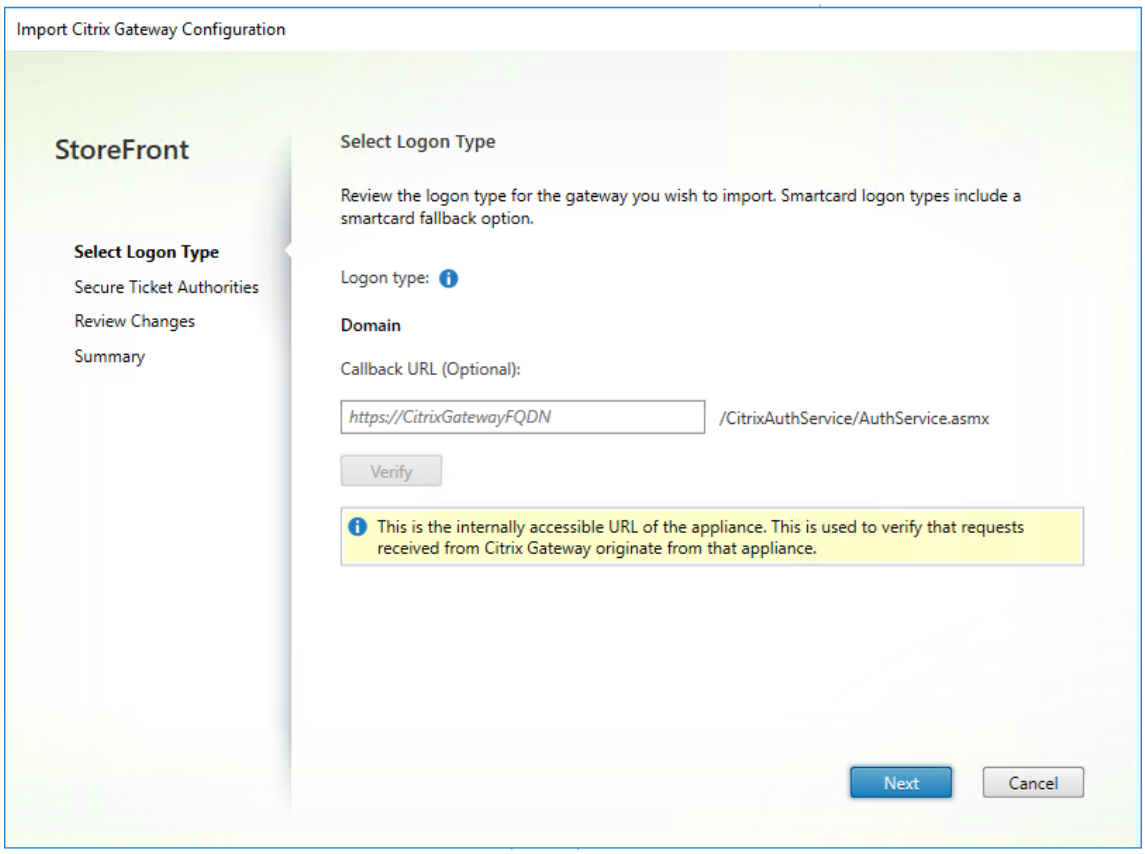
1. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Gérer Citrix Gateway**.
2. Sur l'écran Gérer Citrix Gateway, cliquez sur le lien **importé à partir d'un fichier**.



3. Accédez au fichier de configuration du serveur virtuel Citrix Gateway.
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 l'appliance Citrix Gateway pour les utilisateurs de l'application Citrix Workspace. 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.

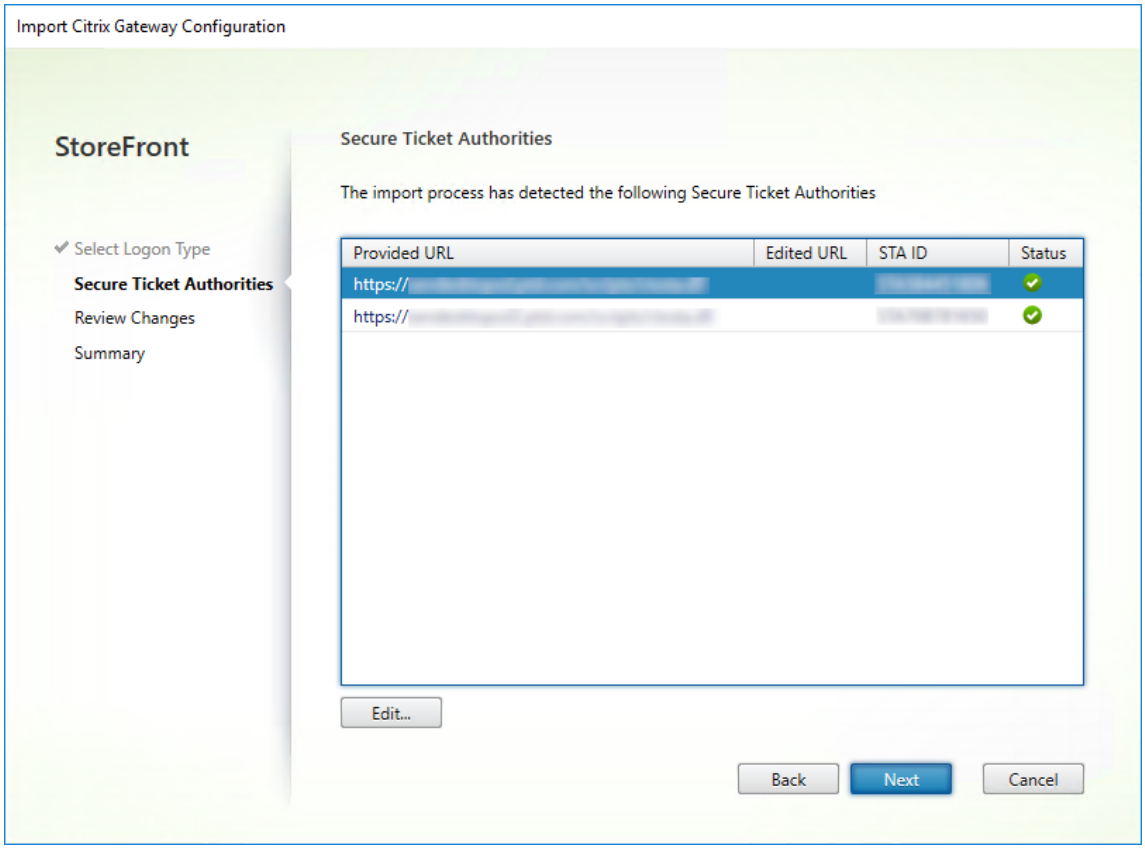


Type de connexion dans la console	LogonType dans le fichier JSON	URL de rappel requise
Domaine	Domaine	Non
Domaine et jeton de sécurité	DomainAndRSA	Non
Jeton de sécurité	RSA	Oui
Carte à puce - Sans solution alternative	SmartCard	Oui
Carte à puce - Domaine	SmartCardDomain	Oui
Carte à puce - Domaine et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

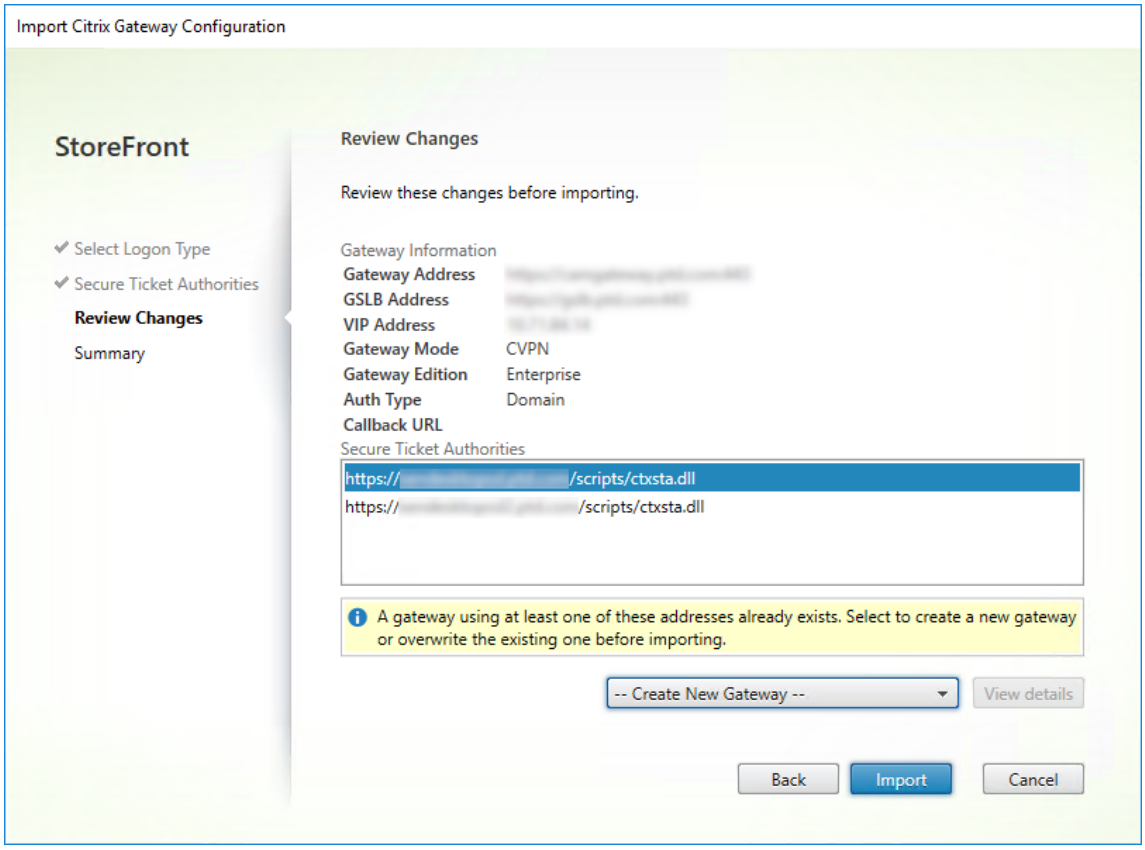
Si une URL de rappel est requise, StoreFront remplira automatiquement l'adresse URL de rappel en fonction de l'adresse URL de passerelle trouvée dans le fichier ZIP. Vous pouvez modifier cette adresse au profit de toute adresse URL valide qui pointe vers l'adresse IP virtuelle de Citrix Gateway. Pour les passerelles GSLB, des URL de rappel uniques sont requises pour chacune des passerelles que vous importez.

Pour utiliser Smart Access, une URL de rappel est requise.

6. Cliquez sur **Suivant**.
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 **Suivant**.
9. Vérifiez les détails de l'importation. Si une passerelle avec la même URL et combinaison de ports de passerelle (GatewayURL: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 qui 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 GatewayURL:port	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 rappel 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 applications Citrix Workspace essayent de se connecter, sauf si elles sont configurées pour utiliser une autre passerelle. Si aucune passerelle n'est configurée pour le magasin, la première passerelle importée à partir du fichier ZIP devient la passerelle par défaut utilisée par les applications Citrix Workspace. L'importation d'autres passerelles ne modifie pas la passerelle par défaut déjà définie pour le magasin.

Importer plusieurs appliances Citrix 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 configuration du serveur virtuel Citrix Gateway en mémoire et examinez les trois passerelles qu'il contient à l'aide de leurs valeurs d'index.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$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**.

```
$ImportedGateways.Document.Gateways[0]
$ImportedGateways.Document.Gateways[1]
$ImportedGateways.Document.Gateways[2]

GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:443
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.1
Stas                   : {
STA298854503, STA909374257 }

```



```
StaLoadBalance          : True
CertificateThumbprints : {
F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         : Domain
GatewayEdition          : Enterprise
ReceiverForWebSites     : {
Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
   ReceiverForWebSite }


GatewayMode             : CVPN
CallbackUrl             :
GslbAddressUri          : https://gslb.example.com/
AddressUri              : https://emeagateway.example.com/
Address                 : https://emeagateway.example.com:444
GslbAddress             : https://gslb.example.com:443
VipAddress              : 10.0.0.2
Stas                    : {
STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints : {
F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         : DomainAndRSA
GatewayEdition          : Enterprise
ReceiverForWebSites     : {
Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
   ReceiverForWebSite }


GatewayMode             : CVPN
CallbackUrl             : https://emeagateway.example.com:445
GslbAddressUri          : https://gslb.example.com/
AddressUri              : https://emeagateway.example.com/
Address                 : https://emeagateway.example.com:445
GslbAddress             : https://gslb.example.com:443
VipAddress              : 10.0.0.2
Stas                    : {
STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints : {
F549AFAA29EBF61E8709F2316B3981AD503AF387 }
```



```
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 Citrix Gateway 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 Citrix Gateway

March 3, 2020

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

Si vous apportez des modifications à vos déploiements Citrix Gateway, assurez-vous que les utilisateurs qui accèdent à des magasins via ces déploiements mettent à jour l'application Citrix Workspace 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 de l'application Citrix Workspace 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 ce processus terminé,
propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

Modifier les paramètres Citrix Gateway généraux

Utilisez la tâche Modifier les paramètres généraux pour modifier les noms de déploiement Citrix 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 Citrix 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, dans le panneau Actions, cliquez sur Gérer Citrix Gateway.
3. Indiquez un nom pour le déploiement Citrix Gateway qui permettra aux utilisateurs de l'identifier.

   Les utilisateurs verront alors s'afficher le nom que vous avez saisi dans l'application Citrix Workspace. 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 déploiement. Par exemple, vous pouvez indiquer l'emplacement géographique dans les noms d'affichage de vos déploiements Citrix 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 Citrix Gateway. L'utilisation d'un même nom de domaine complet pour StoreFront et le serveur virtuel Citrix 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 de l'appliance Citrix Gateway, si nécessaire.

   L'adresse de sous-réseau correspond à l'adresse IP que Citrix 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 de l'appliance Citrix 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 appliance exécute Citrix Gateway, sélectionnez dans la liste Type d'ouverture de session la méthode d'authentification que vous avez configurée sur l'appliance pour les utilisateurs de l'application Citrix Workspace.

   Les informations que vous fournissez sur la configuration de votre appliance Citrix Gateway sont ajoutées au fichier de provisioning pour le magasin. Ceci permet à l'application Citrix Workspace d'envoyer une demande de connexion appropriée lorsque vous contactez l'appliance 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 parmi 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 Citrix Gateway ou une seule appliance Access Gateway 5.0, renseignez l'URL du service d'authentification Citrix Gateway dans la case URL de rappel. StoreFront ajoute automatiquement la partie standard de l'URL.

   Entrez l'adresse URL de l'appliance accessible en interne. StoreFront contacte le service d'authentification Citrix Gateway pour vérifier que les requêtes reçues de Citrix Gateway proviennent de cette appliance.

Gérer les appliances Access Gateway 5.0

Utilisez la tâche Gérer les appliances pour ajouter, modifier ou supprimer de StoreFront les adresses IP ou de noms de domaine complets des appliances 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 Citrix Virtual Apps and Desktops et émet des tickets de session en réponse aux demandes de connexion. Ces tickets de session constituent la base de l'authentification et de l'autorisation d'accès aux ressources Citrix Virtual Apps and Desktops.

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 Citrix Gateway. Dans le panneau Actions, cliquez sur Gérer Citrix 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 Citrix Virtual Apps and Desktops maintienne les sessions déconnectées ouvertes pendant que l'application Citrix Workspace tente de se reconnecter automatiquement, sélectionnez la case à cocher 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 Citrix Gateway

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

Équilibrage de charge avec l'appliance Citrix ADC

March 3, 2020

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 une appliance Citrix ADC pour l'équilibrage de charge des requêtes entrantes depuis l'application Citrix Workspace et Citrix Receiver pour Web entre les nœuds StoreFront du groupe de serveurs. Cet article explique également comment configurer StoreFront Monitor pour une utilisation avec une appliance Citrix ADC.

Les exemples de cette section ont été testés dans l'environnement suivant :

- Quatre nœuds StoreFront 3.x Windows Server 2012 R2 dans un seul groupe de serveurs.
- Un équilibrage de charge de l'appliance Citrix ADC 12.1 configuré pour l'équilibrage de charge persistant CookieInsert et Least Connection.
- Un client de test Windows 10 avec l'application Citrix Workspace installée.

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

Passez en revue 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 de l'appliance Citrix ADC 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.

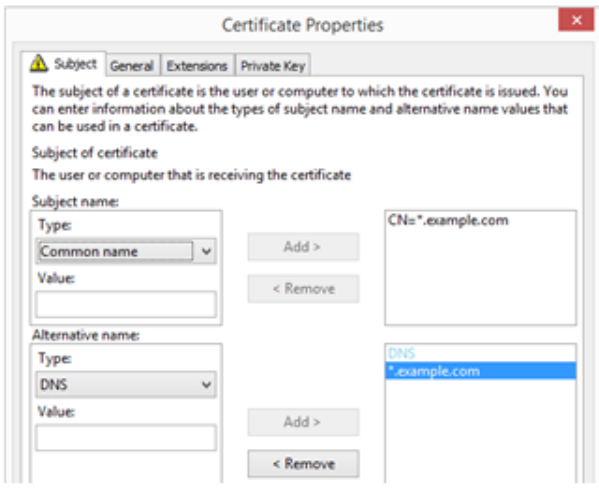
- **Option 2 :** permet d'utiliser un certificat incluant des noms de sujet alternatifs sur le vServer d'équilibrage de charge de l'appliance Citrix ADC et sur les nœuds de groupe de serveurs StoreFront. L'ajout des SAN supplémentaires au certificat qui correspondent à tous les noms de domaine complets (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/.

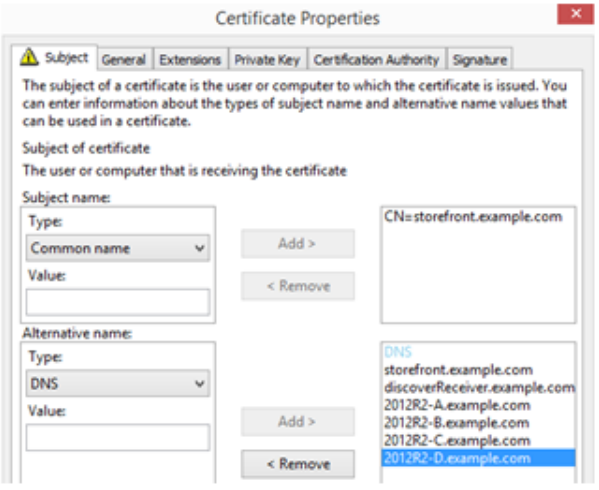
> **Remarque :**
>
> Lorsque l'exportation de la clé privée associée avec le certificat n'est pas possible, utilisez deux certificats distincts : un sur le vServer d'équilibrage de charge de l'appliance Citrix ADC et un autre certificat sur les nœuds de groupe de serveurs StoreFront. Les deux certificats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

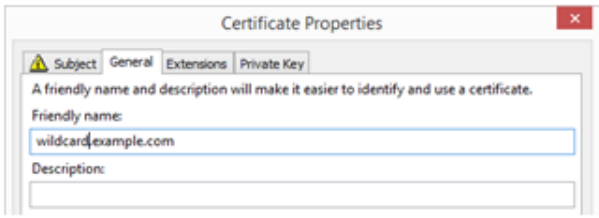
Example Web server certificates

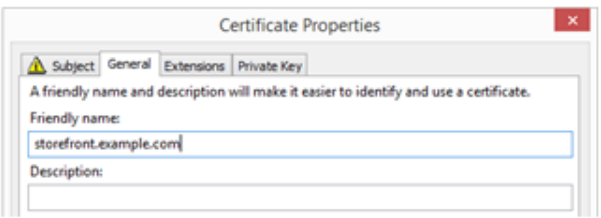
Option 1: Wildcard certificate



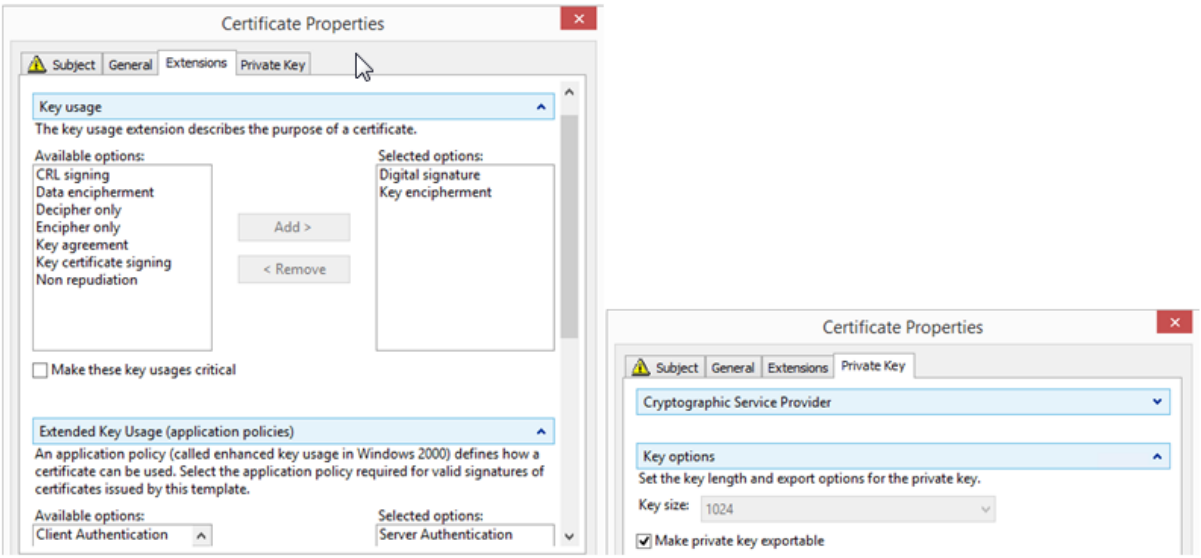
Option 2: SAN certificate with every StoreFront server







Common Properties



Créer un certificat de serveur pour l'équilibrage de charge de l'appliance Citrix ADC et tous les serveurs StoreFront

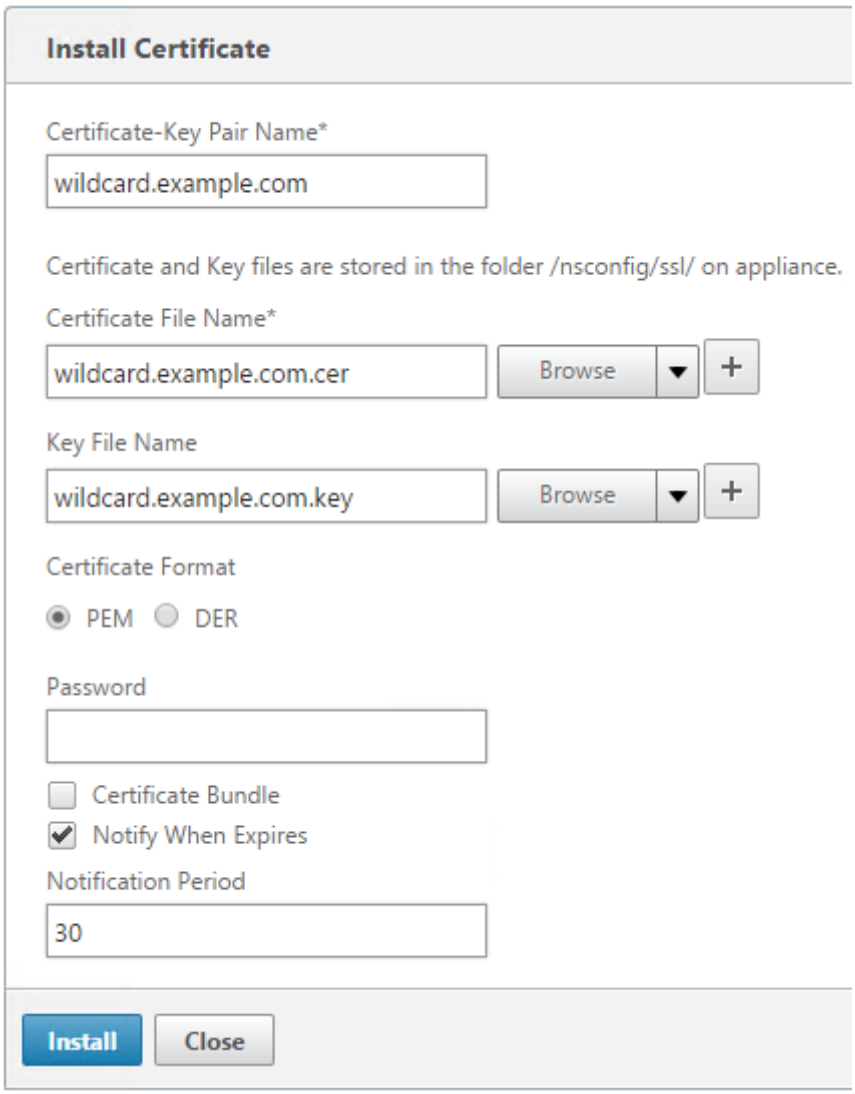
Importer un certificat émis par une autorité de certification Windows sur une appliance Citrix ADC

- WinSCP est un outil tiers utile et gratuit pour déplacer des fichiers d'un ordinateur Windows sur un système de fichiers d'appliance Citrix ADC. Copiez les certificats à importer sur le dossier */nsconfig/ssl/* dans le système de fichiers de l'appliance Citrix ADC.
- Vous pouvez aussi utiliser les outils OpenSSL de l'appliance Citrix ADC 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 Citrix ADC.

1. Copiez le fichier PFX dans */nsconfig/ssl* sur l'appliance Citrix ADC ou VPX.
2. Ouvrez l'interface de ligne de commande (CLI) de l'appliance Citrix ADC.
3. Tapez **Shell** pour quitter la CLI de l'appliance Citrix ADC 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 revenir à l'interface de ligne de commande de l'appliance Citrix ADC.

Configurer le certificat de serveur de l'appliance Citrix ADC une fois qu'il a été importé

1. Ouvrez une session sur la console de gestion de l'appliance Citrix ADC.
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 de l'appliance Citrix ADC dans /nsconfig/ssl/.
    - Sélectionnez le fichier .key contenant la clé privée dans le même emplacement.



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 de l'appliance Citrix ADC.

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

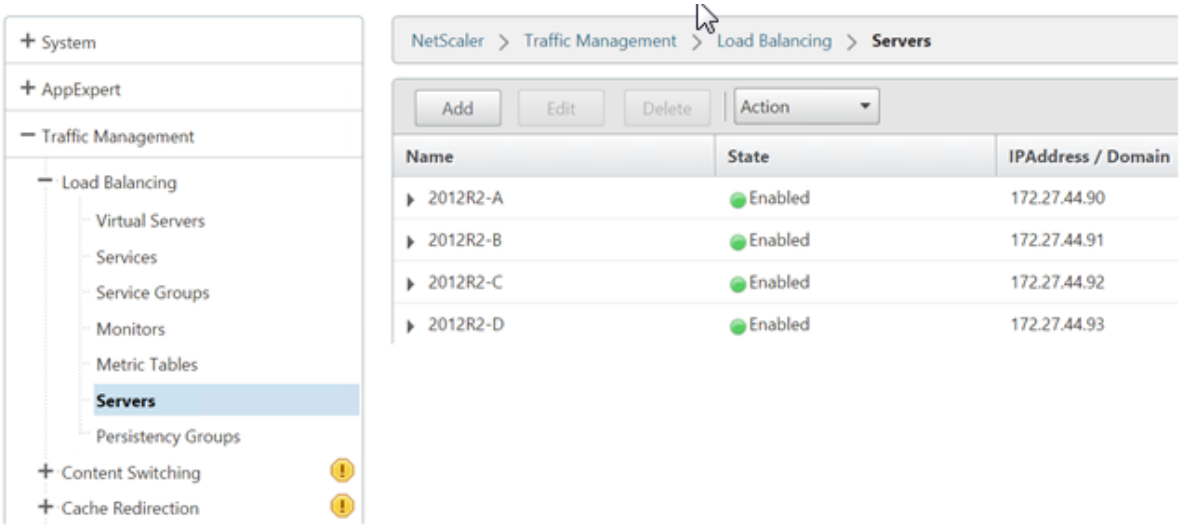
Scénario 1 – Connexion sécurisée HTTPS 443 de bout en bout entre le client et l'équilibrage de charge de l'appliance Citrix ADC, et entre l'équilibrage de charge et plusieurs serveurs StoreFront 3.x

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

Ajouter des nœuds de serveur StoreFront individuels à l'équilibrage de charge de l'appliance Citrix ADC

1. Ouvrez une session sur la console de gestion de l'appliance Citrix ADC.
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.

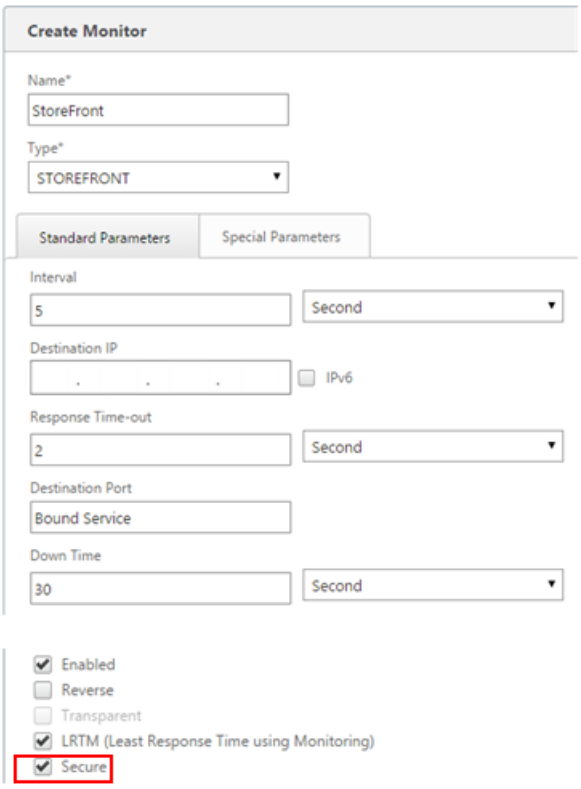


Définir un moniteur StoreFront pour vérifier l'état de tous les nœuds StoreFront dans le groupe de serveurs

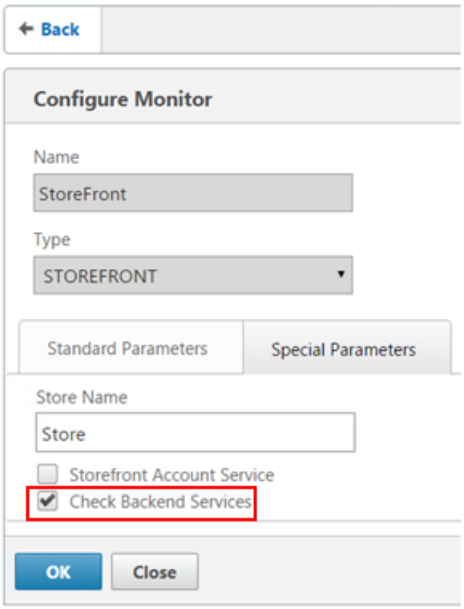
1. Ouvrez une session sur la console de gestion Citrix ADC.

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 HTTPS entre votre vServer d'équilibrage de charge et StoreFront ; sinon, laissez cette option désactivée.
5. Dans l'onglet **Special Parameters**, saisissez le nom du magasin sous **Store Name**.
6. Dans l'onglet **Special Parameters**, sélectionnez l'option **VCheck Backend Services**. 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

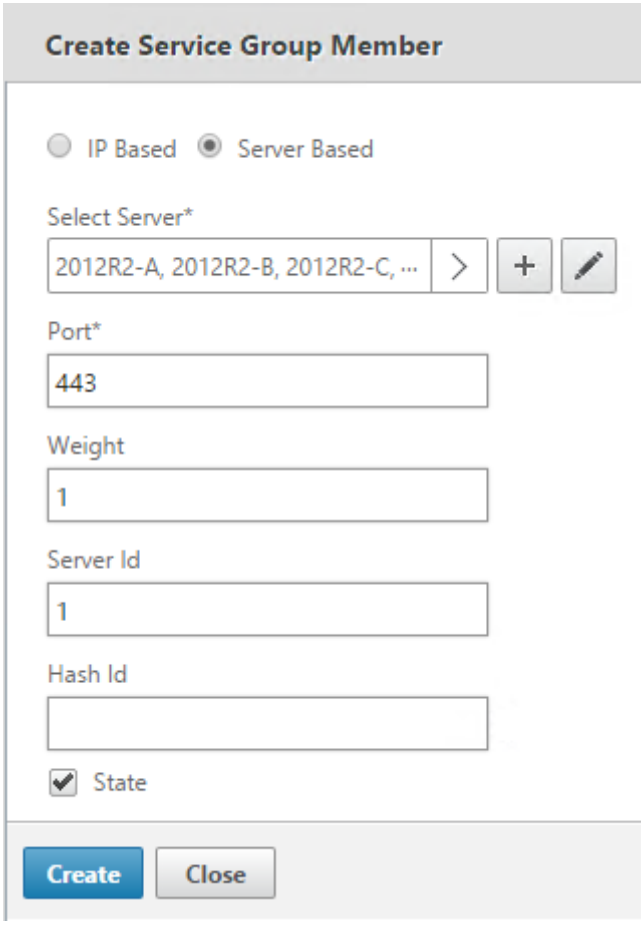


Special Parameters Tab

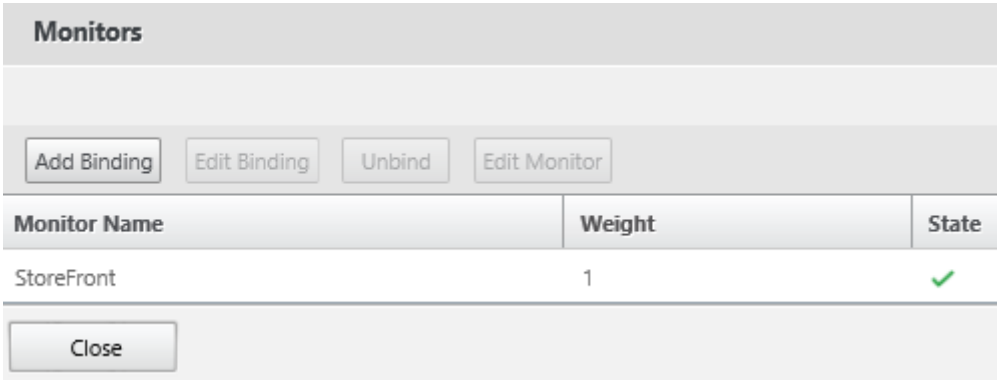


Créer un groupe de services HTTPS 443 contenant tous les serveurs StoreFront

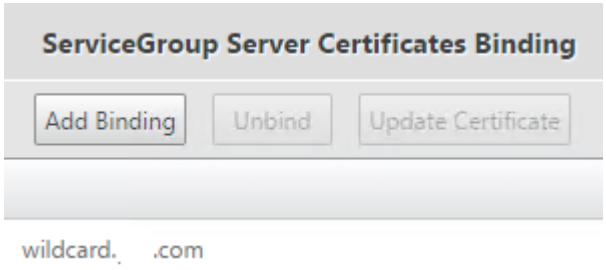
1. Dans le groupe de services, sélectionnez l'option **Members** sur le côté droit et ajoutez tous les nœuds de serveurs StoreFront que vous avez définis précédemment dans la section Servers.
2. Définissez le port TLS et accordez à chaque nœud un ID de serveur unique lors de leur ajout.



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

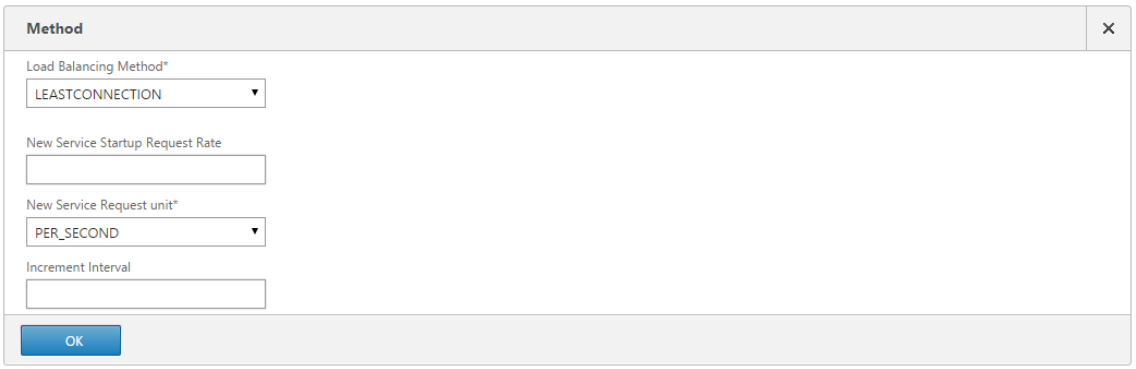


4. Sur l'onglet **Certificates**, liez le certificat SSL que vous avez importé préalablement.
5. Liez le certificat CA utilisé pour signer le certificat de serveur que vous avez importé précédemment et les autres autorités de certification faisant partie de la chaîne de confiance PKI.

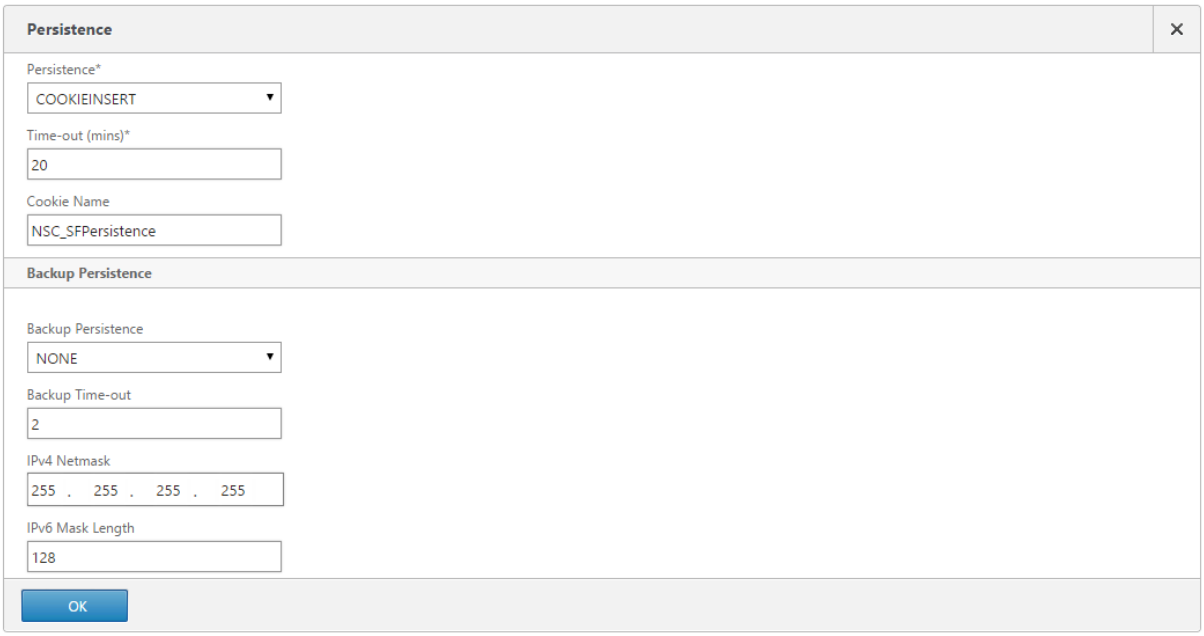


Créer un vServer d'équilibrage de charge pour le trafic utilisateur

1. Ouvrez une session sur la console de gestion de l'appliance Citrix ADC.
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**.



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



Scénario 2 – Arrêt HTTPS/Communication HTTPS 443 entre le client et l'équilibrage de charge Citrix ADC, et connexions HTTP 80 entre l'équilibrage de charge et les serveurs StoreFront 3.x

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

Ajouter des serveurs StoreFront individuels à l'équilibrage de charge Citrix ADC

1. Ouvrez une session sur la console de gestion Citrix ADC.
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.
3. Utilisez la configuration de serveur basée sur l'adresse IP et entrez l'adresse IP du serveur pour chaque serveur StoreFront.

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 Citrix ADC.
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. Dans la liste **Type**, sélectionnez **StoreFront** .
5. Dans l'onglet **Special Parameters**, saisissez le nom du magasin sous **Store Name**.

6. Saisissez 8000 dans le champ **Destination Port**. Cela correspond à l'instance de moniteur par défaut créée sur chaque serveur StoreFront.
7. Dans l'onglet **Special Parameters**, sélectionnez l'option **VCheck Backend Services**. 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 de tous les services StoreFront en cours d'exécution.

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 persistance n'est pas utilisée.

5. Depuis le menu du vServer d'équilibrage de charge, sélectionnez **Persistence** sur le côté droit 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**.

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

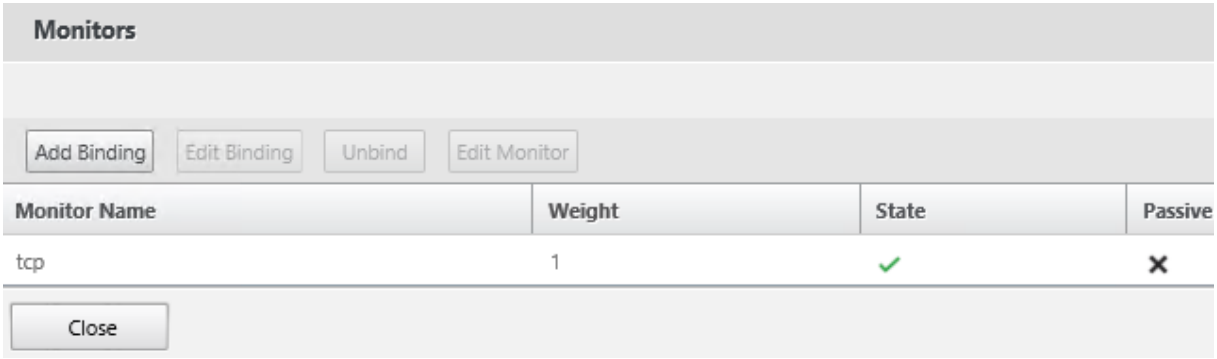
Considérations à prendre en compte avant de créer un vServer d'équilibrage de charge :

- **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 appliance Citrix ADC 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.

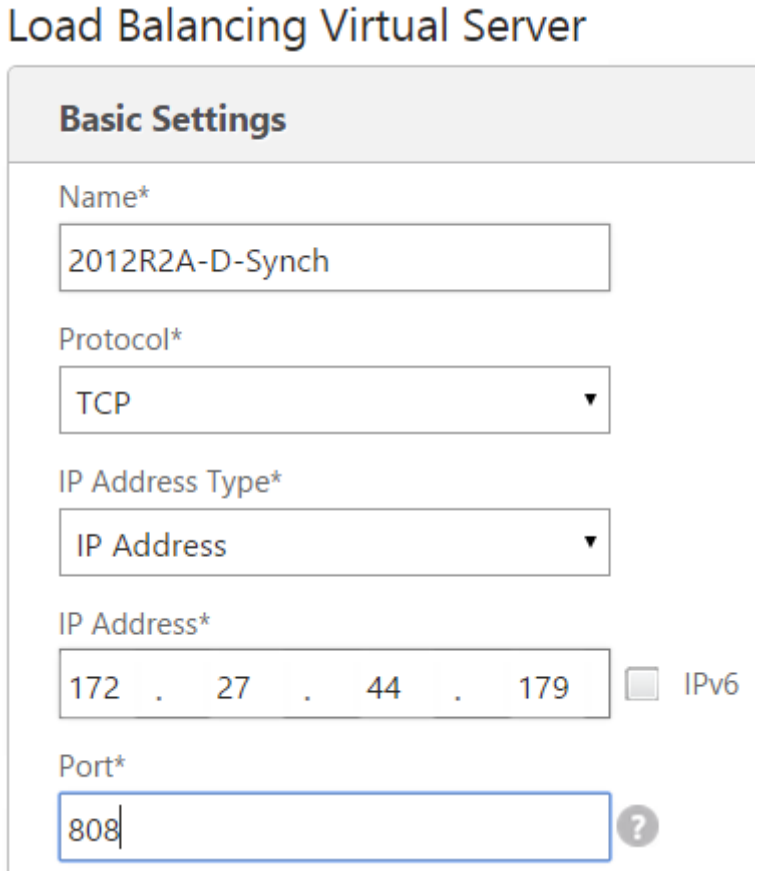
Configurez un groupe de services pour la synchronisation d'abonnement

1. Ouvrez une session sur la console de gestion de l'appliance Citrix ADC.
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.



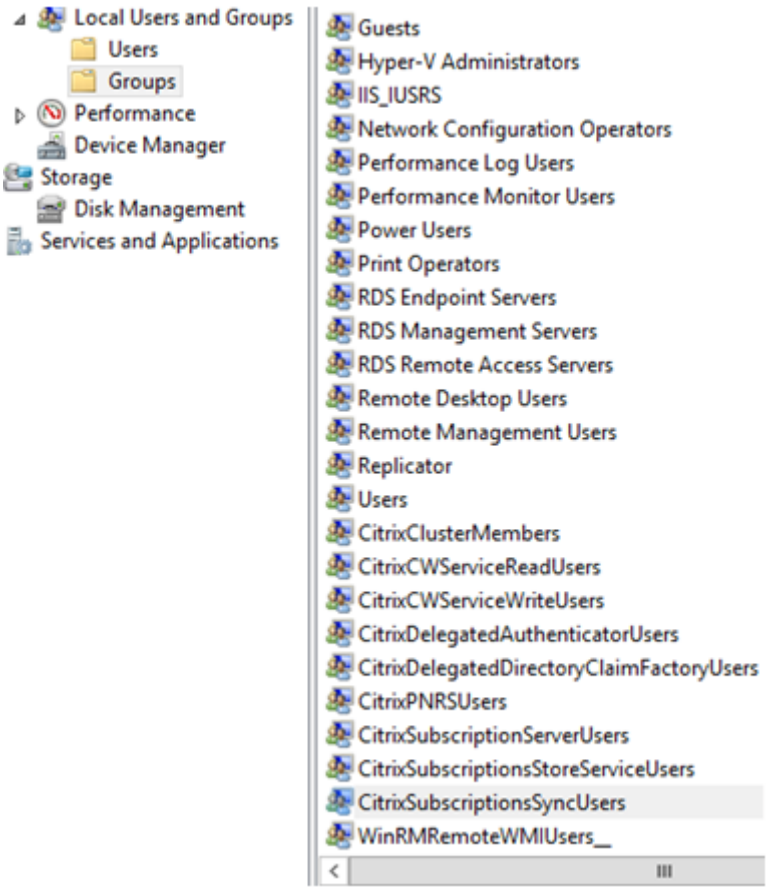
Créer un équilibrage de charge vServer pour la synchronisation des abonnements entre les groupes de serveurs

1. Ouvrez une session sur la console de gestion de l'appliance Citrix ADC.
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.



Appartenance au groupe CitrixSubscriptionsSyncUsers

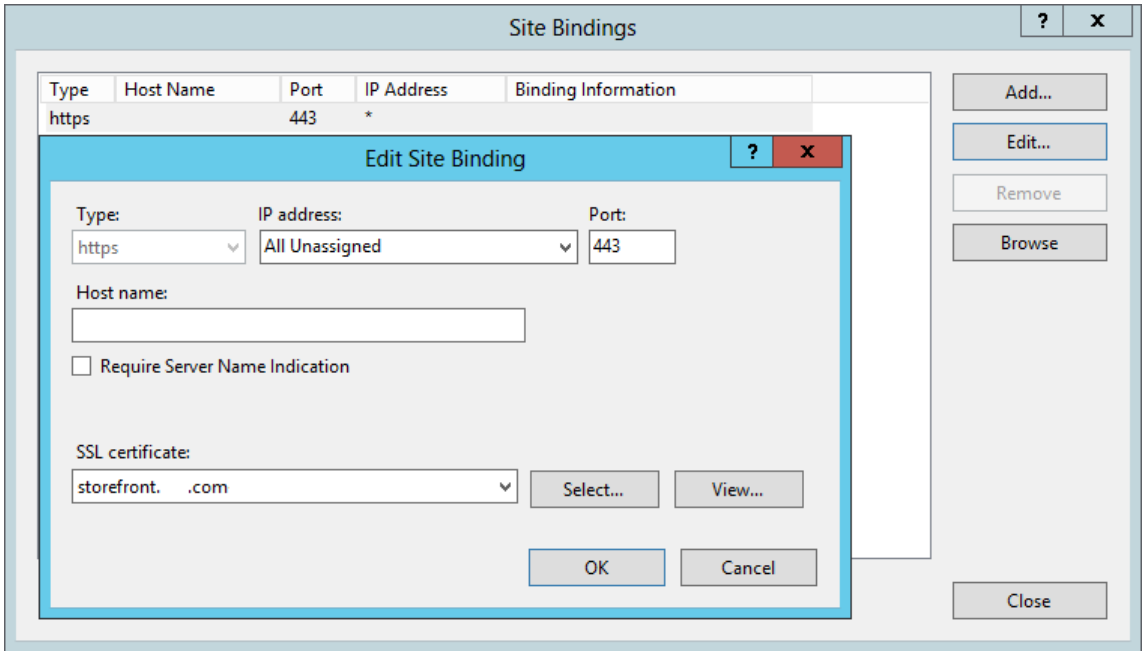
Pour que le **serveur StoreFront A** dans l'**emplacement A** demande et récupère des données d'abonnement à partir du **serveur B** à un emplacement différent, le serveur A doit être un membre du groupe de sécurité local **CitrixSubscriptionsSyncUsers** sur le serveur B. Le groupe local **CitrixSubscriptionsSyncUsers** 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.



Scénario 1 – Configurer le groupe de serveurs StoreFront à l'aide de HTTPS entre Citrix ADC et StoreFront

1. Importez la clé certificat et privée qui a été déployée sur le vServer d'équilibrage de charge de l'appliance Citrix ADC 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.

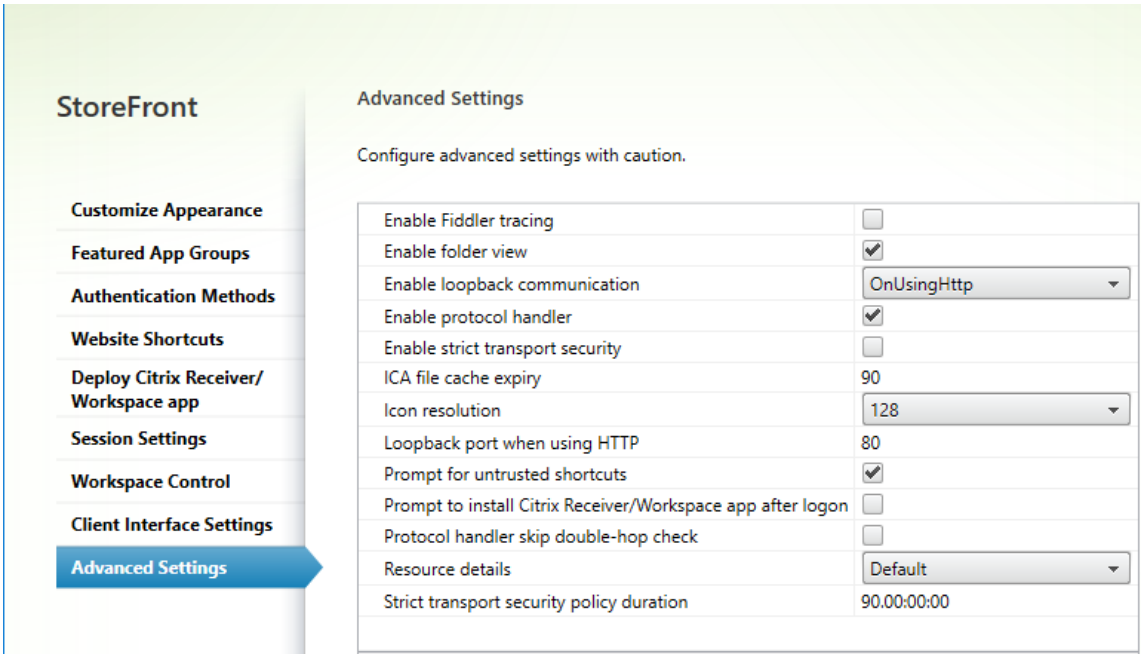


3. Si vous utilisez HTTPS entre l'équilibrage de charge Citrix ADC et StoreFront, vous devez utiliser un certificat contenant le nom de domaine complet (FQDN) avec équilibrage de charge en tant que nom courant (CN) ou nom de sujet alternatif (SAN).

   Voir Créer un certificat de serveur pour l'équilibrage de charge de l'appliance Citrix ADC et les serveurs StoreFront.

Scénario 2 – Configurer le groupe de serveurs StoreFront à l'aide de HTTPS entre Citrix ADC et StoreFront

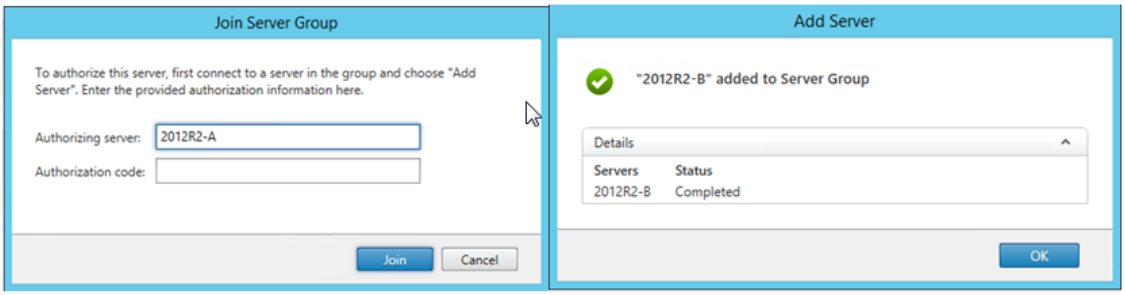
1. Supprimez la liaison HTTPS dans IIS de chaque nœud StoreFront le cas échéant.
2. Assurez-vous que la liaison HTTP est présente dans IIS et qu'elle est définie pour utiliser le port 80.
3. Définissez les paramètres de bouclage dans Receiver pour Web sur **OnUsingHTTP** et port **80**. Cette étape est essentielle pour garantir la réussite de la détection du client entre l'application Citrix Workspace native et Receiver pour Web.



Étapes communes aux scénarios 1 et 2

1. Installez StoreFront sur chaque nœud du groupe de serveurs.
2. 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. L'URL doit toujours être définie sur `https://storefrontlb.domain.com` pour les scénarios 1 et 2 et doit correspondre au nom de domaine complet du vServer d'équilibrage de charge de Citrix ADC.

   Consultez la section Créer un certificat de serveur pour l'équilibrage de charge de l'appliance Citrix ADC et les serveurs StoreFront.
3. 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.
4. Sélectionnez **Server Group > Add Server > Copy the Authorization Code** pour le serveur à associer.



5. Propagez la configuration à partir du nœud principal vers tous les autres nœuds du groupe de serveurs.
6. 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 l'appliance Citrix ADC, 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 applets de commande PowerShell pour afficher ou reconfigurer l'URL de service du moniteur StoreFront.

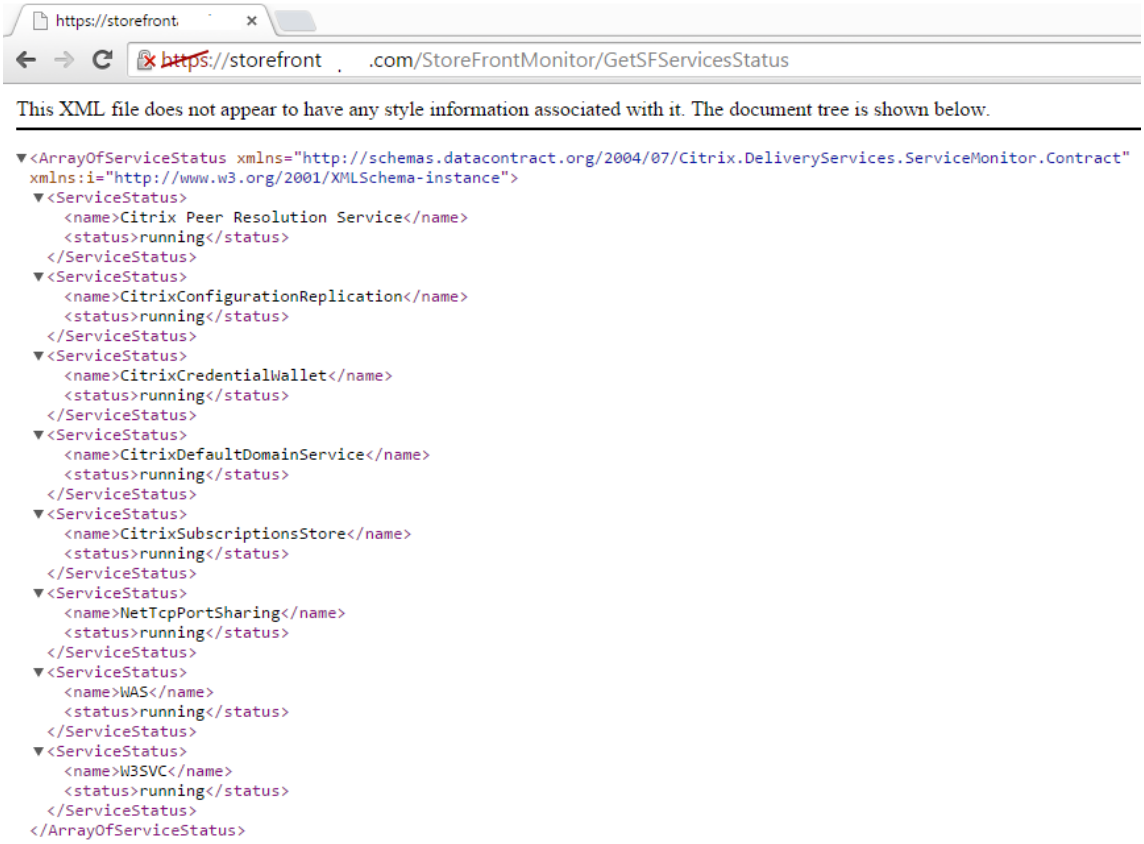
Supprimer le moniteur de services par défaut et le remplacer par un moniteur qui utilise le protocole HTTPS et le port 443

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.

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

2. Une fois ce processus 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
```

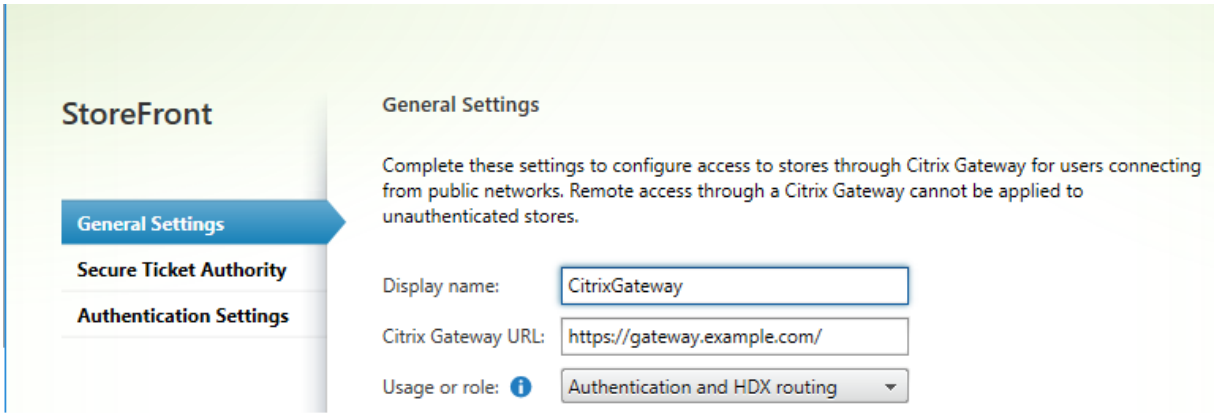



Citrix Gateway et serveurs virtuels d'équilibrage de charge sur la même appliance Citrix ADC

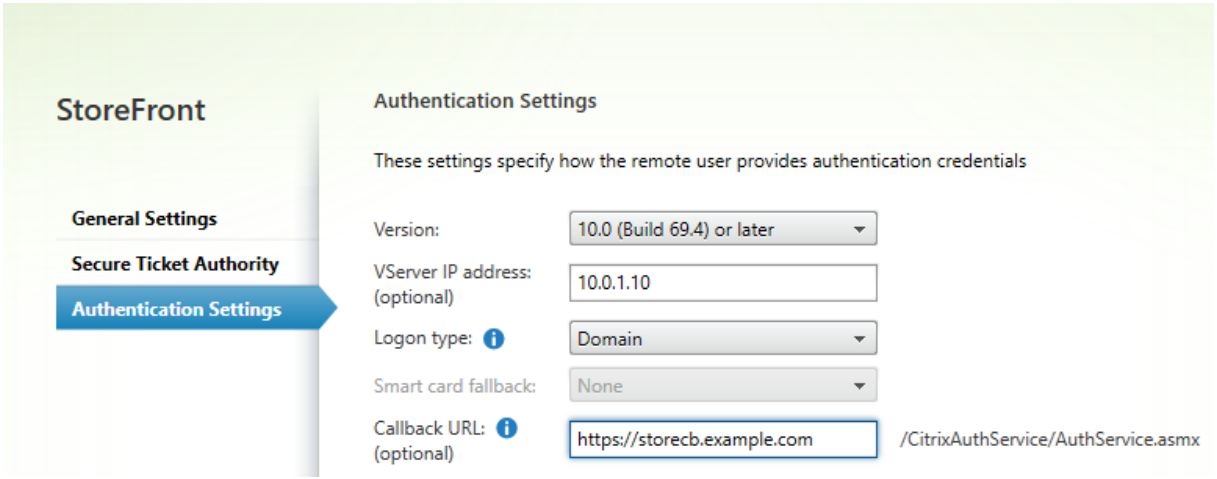
Si vous avez configuré le serveur virtuel Citrix Gateway et le serveur virtuel d'équilibrage de charge sur la même appliance Citrix ADC, les utilisateurs de domaine internes peuvent rencontrer des problèmes lors d'une tentative d'accès direct à l'URL de base de l'hôte avec équilibrage de charge StoreFront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

Dans ce scénario, StoreFront suppose que l'utilisateur a déjà été authentifié sur Citrix Gateway, car StoreFront associe l'adresse IP source de l'utilisateur entrant avec l'adresse IP de sous-réseau (SNIP) de Citrix Gateway. StoreFront essaie alors d'utiliser le protocole AGBasic pour effectuer l'authentification silencieuse sur Citrix 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 ou saisissez une adresse IP virtuelle afin que l'authentification par nom d'utilisateur et mot de passe soit utilisée à la place du protocole de connexion AGBasic.

Configurer une instance Citrix Gateway sur le groupe de serveurs StoreFront



Entrez l'adresse IP virtuelle de Citrix Gateway dans le champ VServer IP address. N'utilisez PAS l'adresse SNIP pour Citrix Gateway si le vServer d'équilibrage de charge réside sur la même appliance Citrix ADC.



Options de bouclage lors de l'équilibrage de charge d'un groupe de serveurs StoreFront à l'aide d'une appliance Citrix ADC

Vous pouvez définir les options de bouclage à l'aide de PowerShell.

Exemple de fichier web.config Receiver pour Web

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


Exemple de commande PowerShell

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

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

Valeur	Contexte
On : 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 TLS est utilisé.
OnUsingHttp : change l'hôte sur 127.0.0.1 et le schéma sur HTTP et modifie la valeur du port configurée pour l'attribut **loopbackPortUsingHttp**.	À utiliser uniquement avec un équilibrage de charge d'arrêt TLS. 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.
Off : 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 **On**.

Configurer deux adresses URL pour la même instance Citrix Gateway

December 23, 2019

Dans StoreFront, vous pouvez ajouter une seule adresse URL Citrix Gateway à partir de la console de gestion StoreFront dans **Gérer Citrix Gateway > Ajouter** ou **Modifier**. Il est également possible d'ajouter une URL publique Citrix Gateway et une URL GSLB (équilibrage de charge globale des serveurs) dans **Gérer Citrix 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 Citrix Gateway dans StoreFront dans les cas d'utilisation suivants :

1. **Répartiteur GSLB avec plusieurs instances Citrix Gateway**. Utilisez un répartiteur GSLB et plusieurs instances Citrix 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. **Instance Citrix Gateway unique avec adresse URL publique ou privée**. Utilisez la même instance Citrix 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 et d'un sujet avancés. Si vous n'êtes pas familier avec les concepts de passerelle StoreFront et 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 Citrix 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 tests plus courts pour valider la configuration de la passerelle StoreFront lors de l'utilisation de plusieurs passerelles GSLB.
- Possibilité d'utiliser le même objet Citrix Gateway dans StoreFront au sein de la DMZ pour l'accès externe et interne.
- Prend en charge les deux adresses URL pour un routage optimal de la passerelle. Pour plus d'informations sur le routage optimal de 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

- Le nom de domaine complet gatewayURL s'affiche pour chaque passerelle dans la console d'administration StoreFront. La propriété GSLBURL de chaque passerelle n'est visible que via l'utilisation des applets de commande PowerShell.
- L'URL gatewayURL est utilisée par les applications Citrix Receiver natives et l'application Citrix Workspace pour l'authentification.
- L'URL gatewayURL est incluse dans la balise d'emplacement dans le fichier de provisioning (receiver.cr) utilisé pour configurer les applications Citrix Receiver et l'application Citrix Workspace avec des informations de magasin et de passerelle.
- Utilisez le Powershell fourni pour modifier les fichiers web.config du magasin et du service d'itinérance. N'effectuez pas cette opération manuellement.

> **Important :**
>
> Avant de configurer une deuxième adresse URL de passerelle à l'aide du paramètre -gslburl, vérifiez 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 Citrix Gateway et StoreFront doivent être présentes dans vos certificats de serveur. Pour plus d'informations sur les certificats de serveur, consultez 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 résolution 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.

```
loadbalancer.storefront.example.net
server1.storefront.example.net
server2.storefront.example.net
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 :


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

Exemple de certificat de serveur pour une instance Citrix 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.

```
gateway.example.com
gateway.example.net
```

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

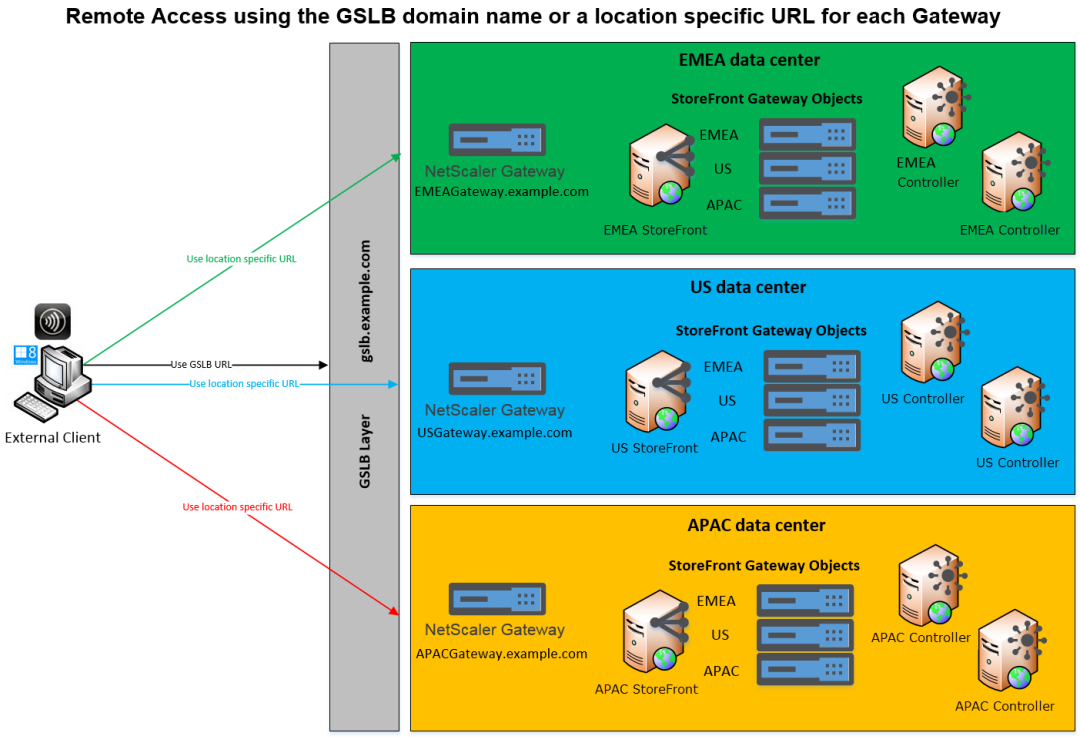
Un certificat de serveur SAN signé publiquement pour l'accès externe via un répartiteur GSLB doit contenir les noms de domaine complets.

```
gslbdomain.example.com
emeagateway.example.com
usgateway.example.com
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 – Receiver pour Web : GSLB et plusieurs instances Citrix Gateway

L'administrateur utilise un répartiteur GSLB et plusieurs instances Citrix 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 appliances GSLB Citrix ADC dans le déploiement global représente un vServer VPN de passerelle. Tous les serveurs StoreFront du déploiement doivent être configurés pour contenir tous les serveurs virtuels Citrix Gateway qui constituent la couche du répartiteur GSLB. Les instances GSLB Citrix Gateway sont utilisées 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 contrôleurs Citrix Virtual Apps and Desktops 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 passerelle 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 1 – Receiver pour Web, et applications Citrix Receiver ou application Citrix Workspace : GSLB et plusieurs instances Citrix Gateway

Attributs de passerelle

Pour utiliser GSLB avec des applications Citrix Receiver natives ou l'application Citrix Workspace, utilisez **Add-STFRoamingGateway** (create) ou **Set-STFRoamingGateway** (modify) pour spécifier les attributs suivants :

-GatewayUrl : défini comme nom de domaine complet partagé pour toutes les passerelles GSLB

-GSLBurl : défini comme nom de domaine complet de la passerelle unique pour chaque passerelle

> Remarque :
>
> Cette opération peut sembler paradoxale, mais elle n'a aucun impact sur ce cas d'utilisation Web. Cela permet de garantir que les applications Citrix Receiver natives ou l'application Citrix Workspace se voient attribuer le nom de domaine complet partagé utilisé par GSLB dans le document de découverte situé dans le point de terminaison `https://storefront.domain.com/citrix/<storename>/discovery`. Cela garantit également que le fichier de provisioning (receiver.cr) exporté par la commande d'**exportation du fichier de provisioning** de StoreFront contient le nom de domaine complet GSLB partagé.

Exemple de fichiers de provisioning

Exemple de fichier 1 utilisant `–GatewayUrl https://gslb.domain.com`. Cela permet aux applications Citrix Receiver natives ou à l'application Citrix Workspace d'utiliser GSLB pour se connecter aux passerelles.


```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

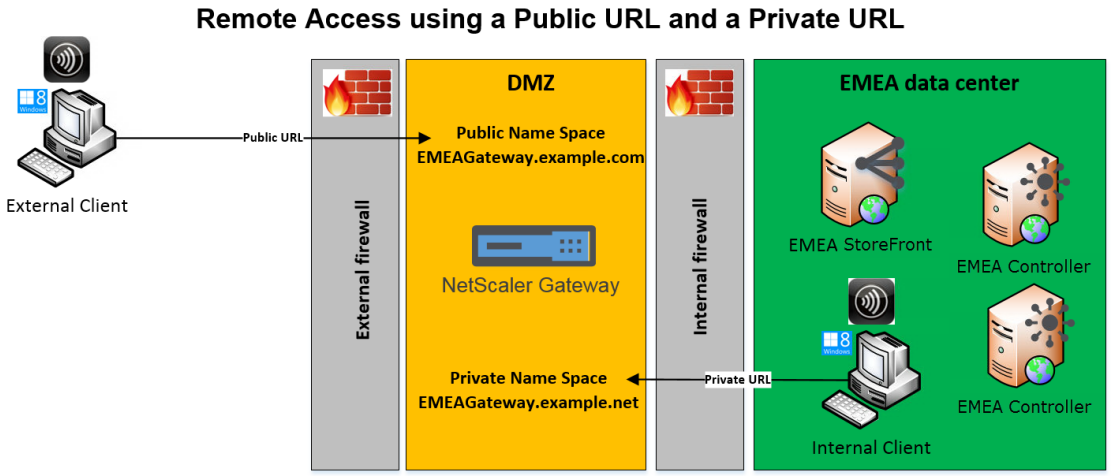
Exemple de fichier 2 utilisant `-GatewayUrl https://emeagateway.domain.com, https://usgateway.domain.com and https://apacgateway.domain.com`. Cela permet aux applications Citrix Receiver natives ou à l'application Citrix Workspace d'utiliser les adresses URL uniques pour se connecter aux passerelles.

```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://emeagateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://ftlgateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://bglgateway.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

Le nom de domaine complet partagé est utilisé pour l'authentification par les applications Citrix Receiver natives et par l'application Citrix Workspace.

Cas d'utilisation 2 – Instance Citrix Gateway unique avec adresse URL publique ou privée

L'administrateur utilise la même instance Citrix 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 une instance Citrix Gateway, même si le client est interne.
- Citrix Gateway se trouve dans une DMZ.
- Il existe deux itinéraires réseau différents vers Citrix 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"
```



```
Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com"
Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA
    gateway object)
Or
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.

```
$EMEAGateway = Get-STFRoamingGateway
$EMEAGateway.GslbLocation = $Null
Set-STFRoamingGateway -Gateway $EMEAGateway
```

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

```
Name: EMEAGateway
Location: https://emeagateway.example.com/ (Unique URL for the EMEA
    Gateway)
GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)

Name: USGateway
Location: https://USgateway.example.com/ (Unique URL for the US Gateway
    )
GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)

Name: APACGateway
Location: https://APACgateway.example.com/ (Unique URL for the APAC
    Gateway)
GslbLocation:  https://gslb.example.com/ (GSLB URL for all three
    gateways)
```

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

```
Name: EMEAGateway
Location: https://emeagateway.example.com/ (Public URL for the Gateway)
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-STFStoreRegisteredOptimall**
:

```
$StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<
    YourStore>"

Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject

Hostnames:       {
 emeagateway.example.com, gslb.example.com }

Hostnames:       {
 usgateway.example.com, gslb.example.com }

Hostnames:       {
 apacgateway.example.com, gslb.example.com }
```

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

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 1 – Passerelles dans le fichier web.config du service d'itinérance

```
<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" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" /><gslbLocation path=
    "https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
```



```
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<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" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://usgateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<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" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://apacGateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><
```



```
    clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll"
    />
<location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>
```

Cas d'utilisation 2 – Passerelles dans le fichier web.config du service d'itinérance

```
<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"
    requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" />
<gslbLocation path=" https://emeagateway.example.net/" />
<clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.net/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>
```


Informations connexes

Dans la documentation du développeur, reportez-vous à la section Citrix StoreFront SDK PowerShell Modules.

Configurer Citrix ADC et StoreFront pour l'authentification DFA

July 9, 2019

L'authentification extensible fournit un seul point de personnalisation pour l'extension de l'authentification basée sur formulaires de StoreFront et de l'appliance Citrix ADC. Pour réaliser une solution d'authentification à l'aide du SDK Extensible Authentication, vous devez configurer l'authentification DFA entre l'appliance Citrix ADC 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, Citrix Gateway 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 l'appliance Citrix ADC 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 StoreFront de l'appliance Citrix ADC 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.

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                                   vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                                   970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840] }

```



```
AdditionalInstanceDependencies : {
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                     : True
FeatureClass                   : Citrix.DeliveryServices.Framework
    .Feature.FeatureClass
```

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

```
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.

```
<example connectorURL="http://Example.connector.url:8080/adapters-
    sf-aaconnector-webapp">
      <routeTable order="1000">
        <routes>
          <route name="StartExampleAuthentication" url="Example-
              Bridge-Forms/Start">
            <defaults>
              <add param="controller" value="
                  ExplicitFormsAuthentication" />
              <add param="action" value="AuthenticateStart" />
              <add param="postbackAction" value="Authenticate" />
              <add param="cancelAction" value="CancelAuthenticate"
                   />
              <add param="conversationFactory" value="
                  ExampleBridgeAuthentication" />
              <add param="changePasswordAction" value="
                  StartChangePassword" />
              <add param="changePasswordController" value="
                  ChangePassword" />
              <add param="protocol" value="CustomForms" />
            </defaults>
          </route>
```

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

BridgeAuthentication.

```
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**.

Désinstallez 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

December 23, 2019

Certaines organisations adoptent des stratégies qui ne leur 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 Citrix 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 Citrix 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, d'instances Citrix Receiver mobiles ou d'applications Citrix Workspace.

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 :

- Citrix 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

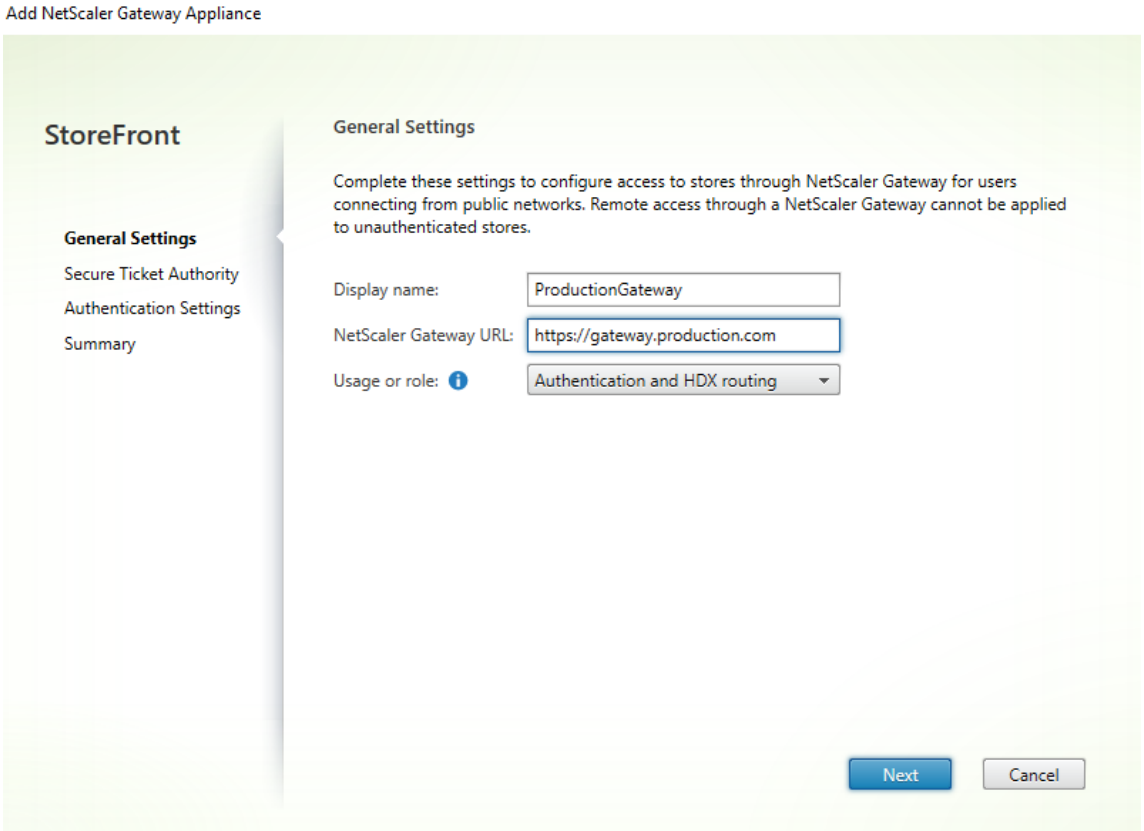
Le domaine `development.com` dans cet exemple est configuré comme suit :

- StoreFront, Citrix Virtual App and Desktops et les VDA se trouvent sur le même 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.

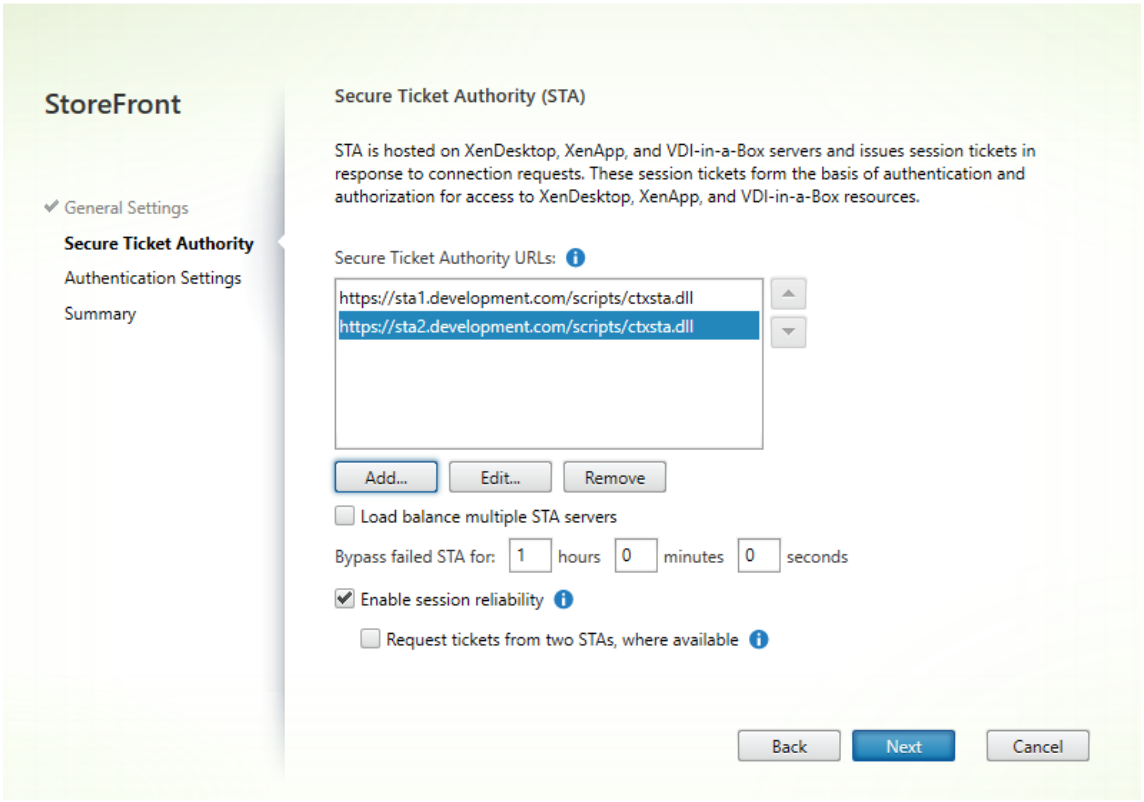
Configurer une passerelle Citrix Gateway pour le magasin

Pour configurer une passerelle Citrix Gateway pour le magasin :

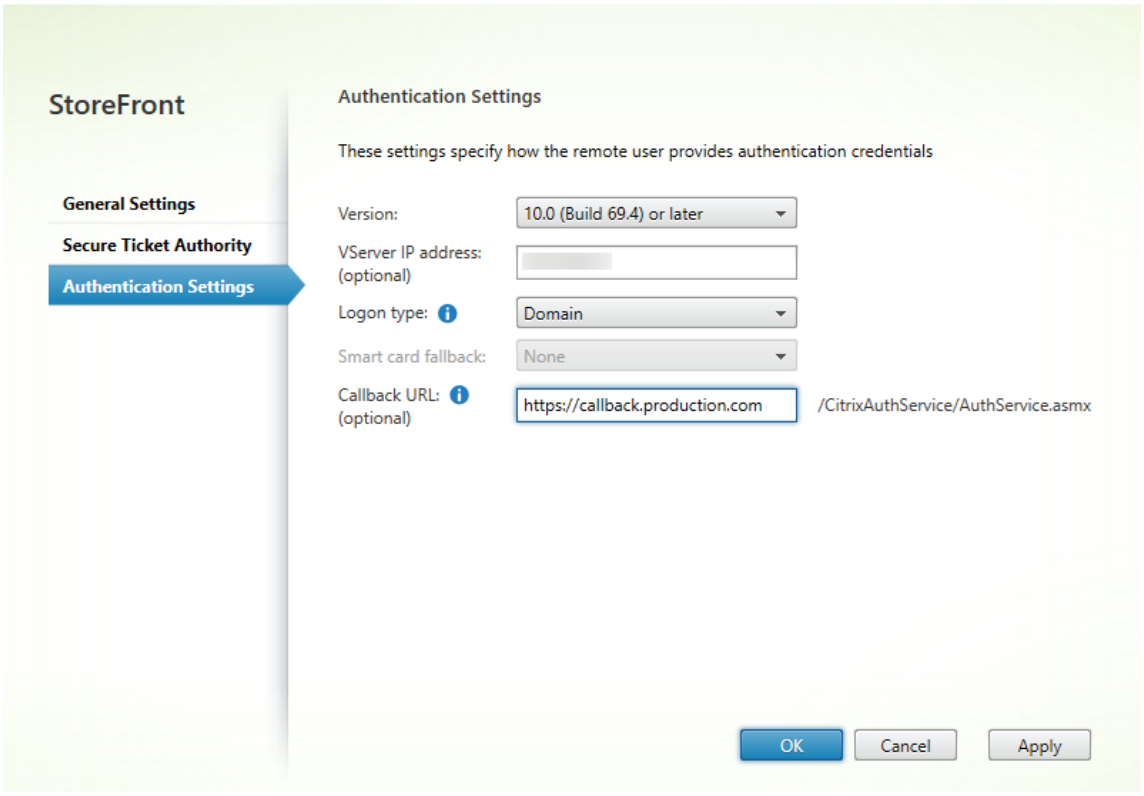
1. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Gérer Citrix Gateway**.
2. Sur l'écran Gérer Citrix Gateway, cliquez sur le bouton **Ajouter**.
3. Complétez les paramètres généraux, les paramètres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



Add NetScaler Gateway Appliance



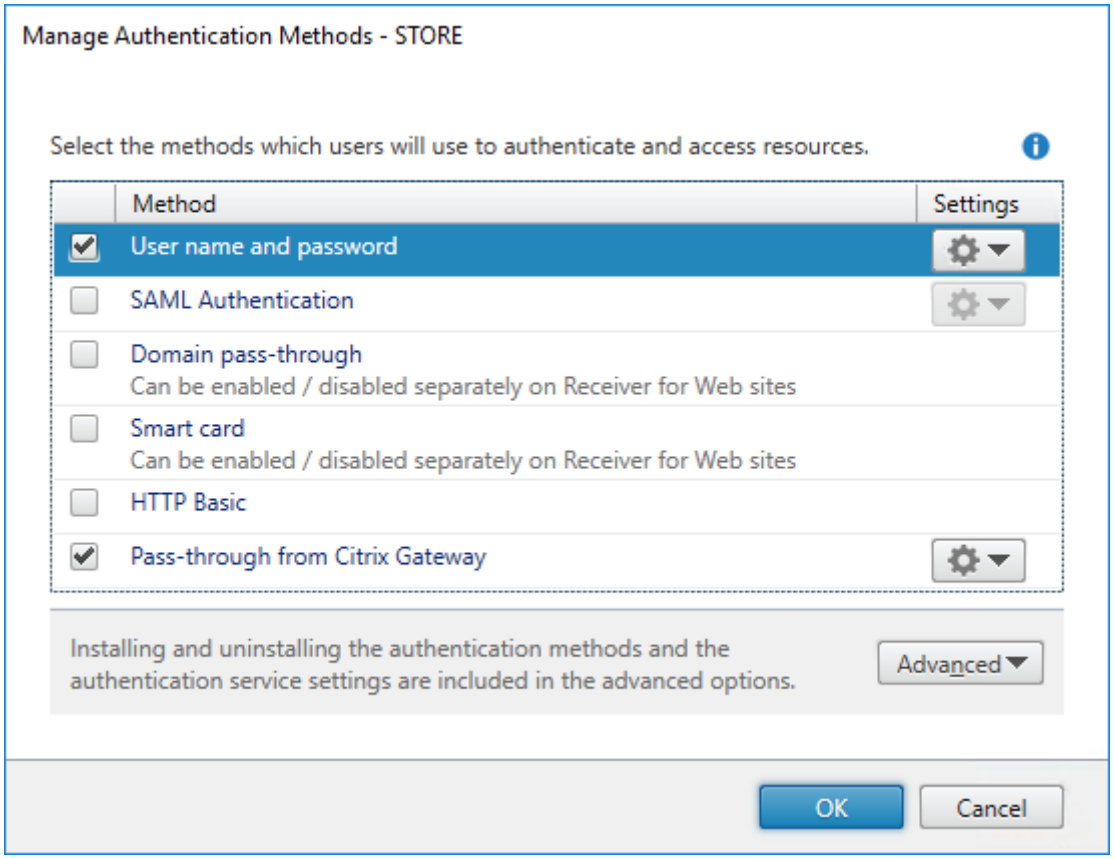
Edit NetScaler Gateway appliance - ProductionGateway



> **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. L'appliance Citrix ADC 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 serveur virtuel Citrix Gateway.

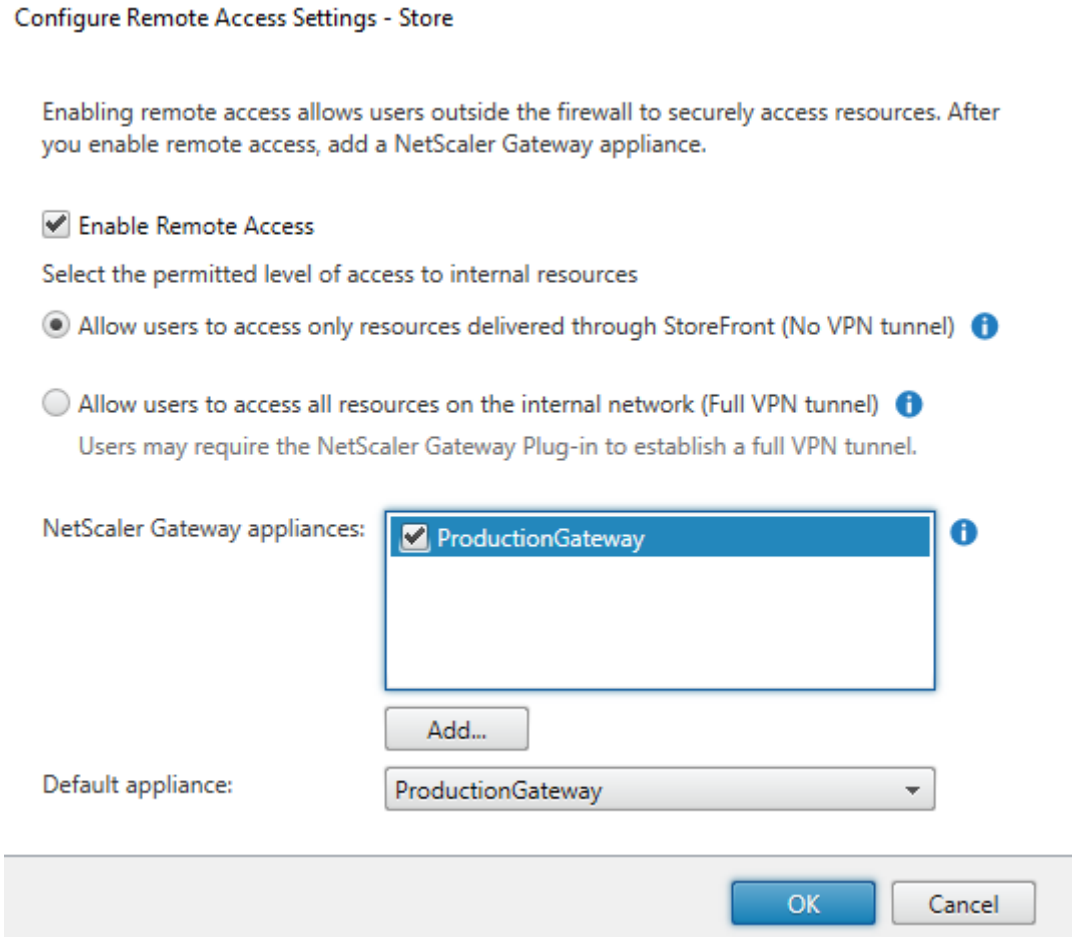
Activer l'authentification pass-through depuis Citrix Gateway

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 Citrix Gateway**.
3. Cliquez sur **OK**.



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

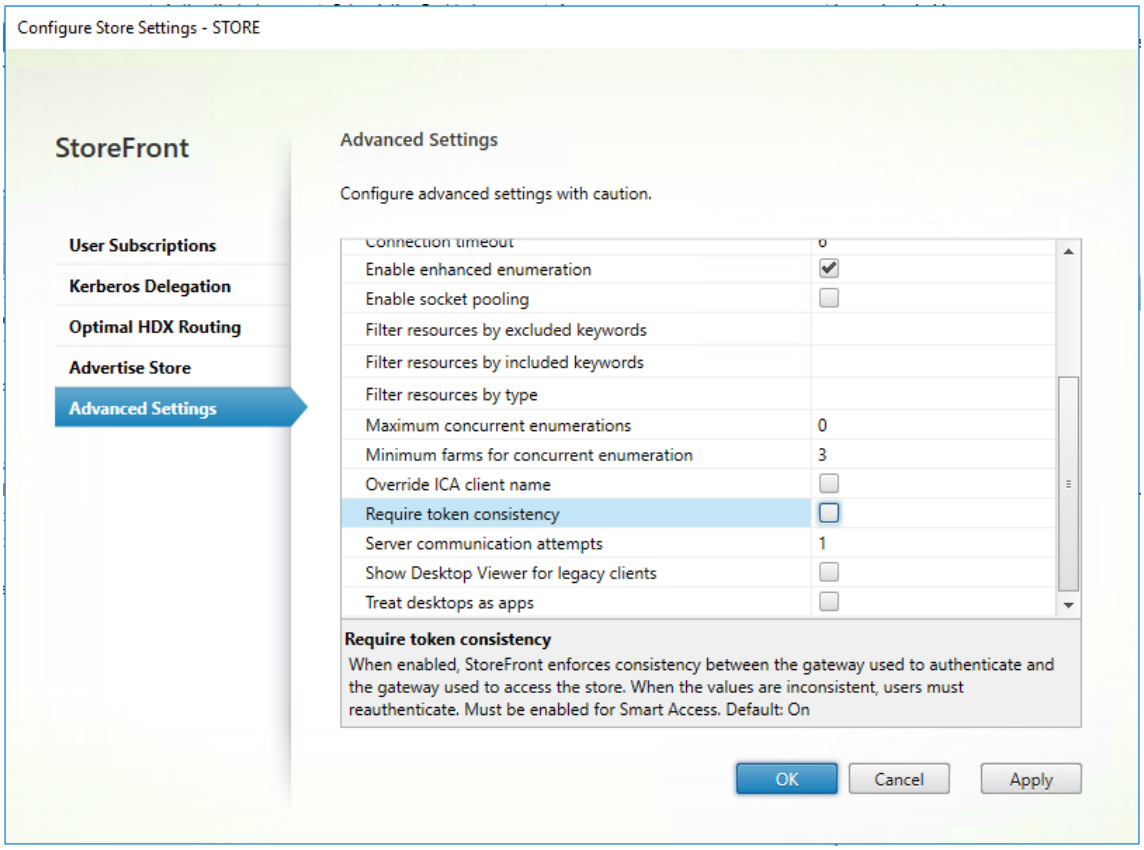
1. Sélectionnez le nœud **Magasin** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau **Actions**, cliquez sur **Configurer les paramètres d'accès distant**.
2. Sélectionnez **Activer l'accès à distance**.
3. Assurez-vous que vous avez enregistré la passerelle Citrix Gateway auprès de votre magasin. Si vous n'enregistrez pas la passerelle Citrix Gateway, la fonctionnalité de ticket STA ne fonctionnera pas.



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 de plus amples informations, consultez la section Paramètres de magasin avancés.
4. Cliquez sur **OK**.



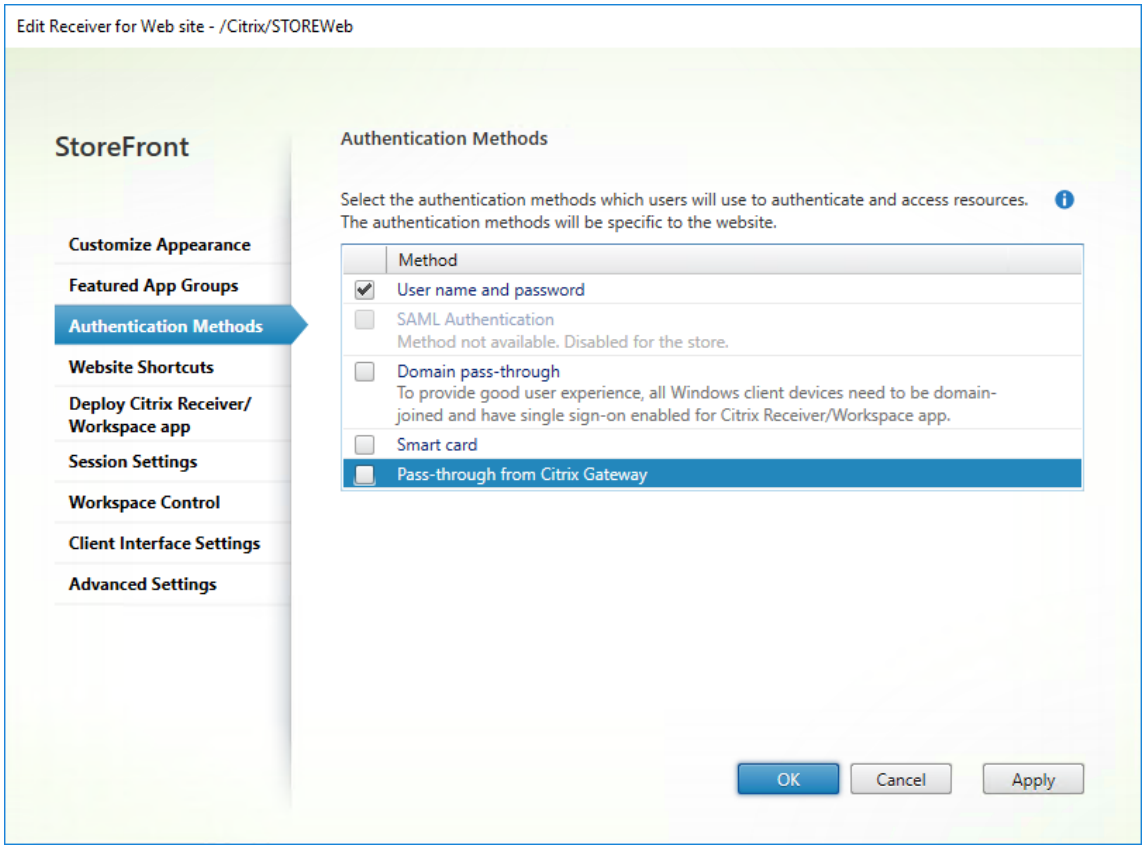
> Remarque :
>
> Le paramètre Exiger la cohérence des jetons est sélectionné (activé) par défaut. Si vous désactivez ce paramètre, les fonctionnalités SmartAccess utilisées pour l'analyse de point de terminaison (EPA) Citrix ADC cessent de fonctionner. Pour plus d'informations sur SmartAccess, consultez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

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

> **Important :**
>
> La désactivation de l'authentification pass-through depuis Citrix Gateway empêche Receiver pour Web d'utiliser les informations d'identification incorrectes du domaine `production.com` transmises depuis l'appliance Citrix ADC. Lorsque l'authentification pass-through est désactivée depuis Citrix Gateway, Receiver pour Web invite l'utilisateur à entrer des informations d'identification. Ces informations d'identification sont différentes des informations

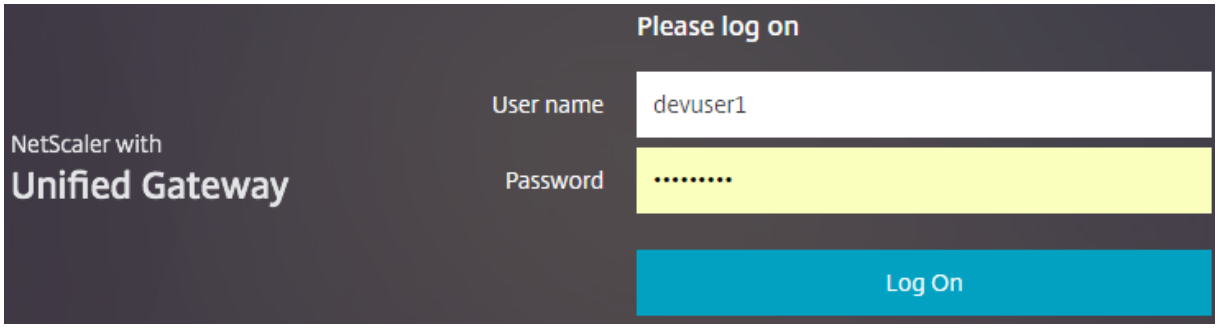
> d'identification utilisées pour se connecter via Citrix Gateway.

1. Sélectionnez le nœud **Magasins** dans le volet gauche de la console de gestion Citrix StoreFront.
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'option **Authentification pass-through via Citrix Gateway**.
5. Cliquez sur **OK**.

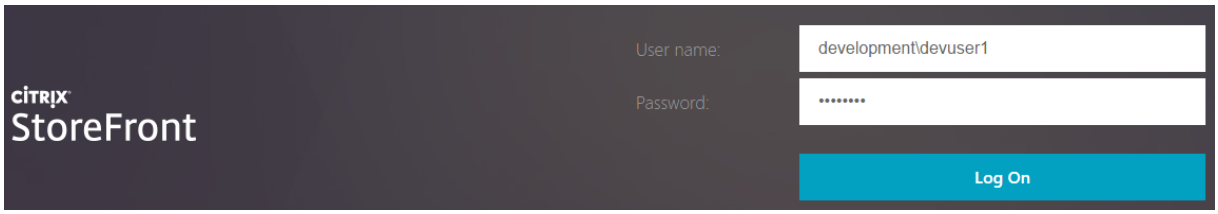


Connexion à Gateway à l'aide d'un utilisateur `production.com` et d'informations d'identification

Pour tester, connectez-vous à 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`.

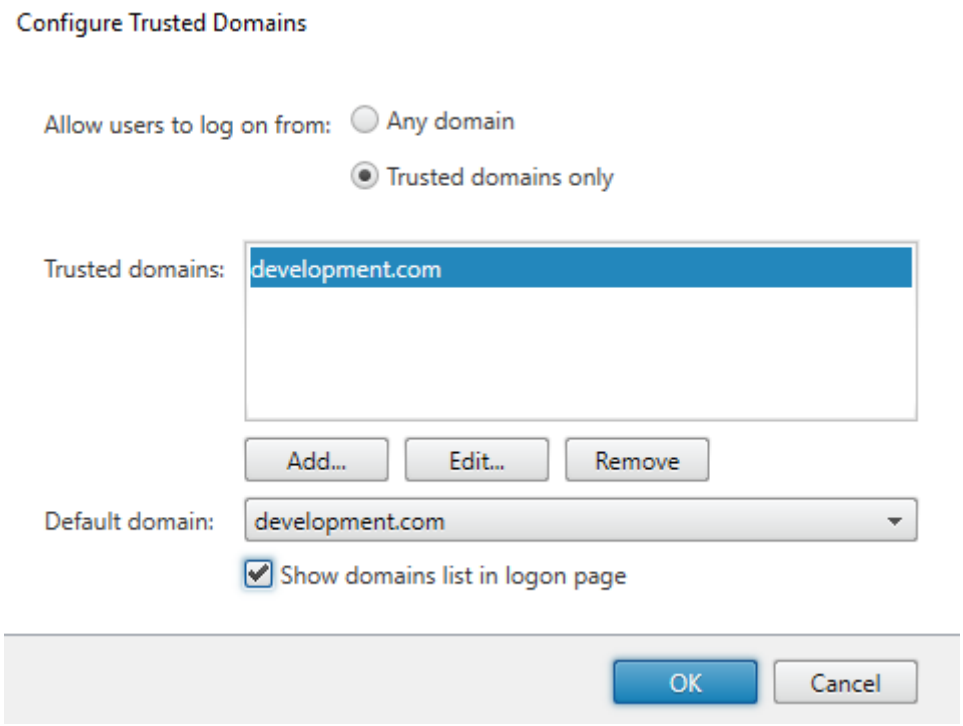


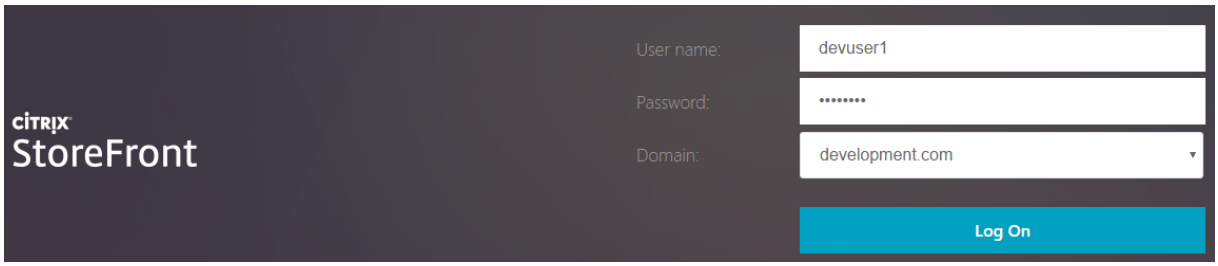
Ajouter une liste déroulante de domaine de confiance dans StoreFront (facultatif)

Ce paramètre est facultatif, mais il peut vous aider à empêcher l'utilisateur d'entrer accidentellement le domaine incorrect pour l'authentification via Citrix 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 Citrix Gateway. Il se peut que les utilisateurs oublient d'entrer le domaine\nomd'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**.



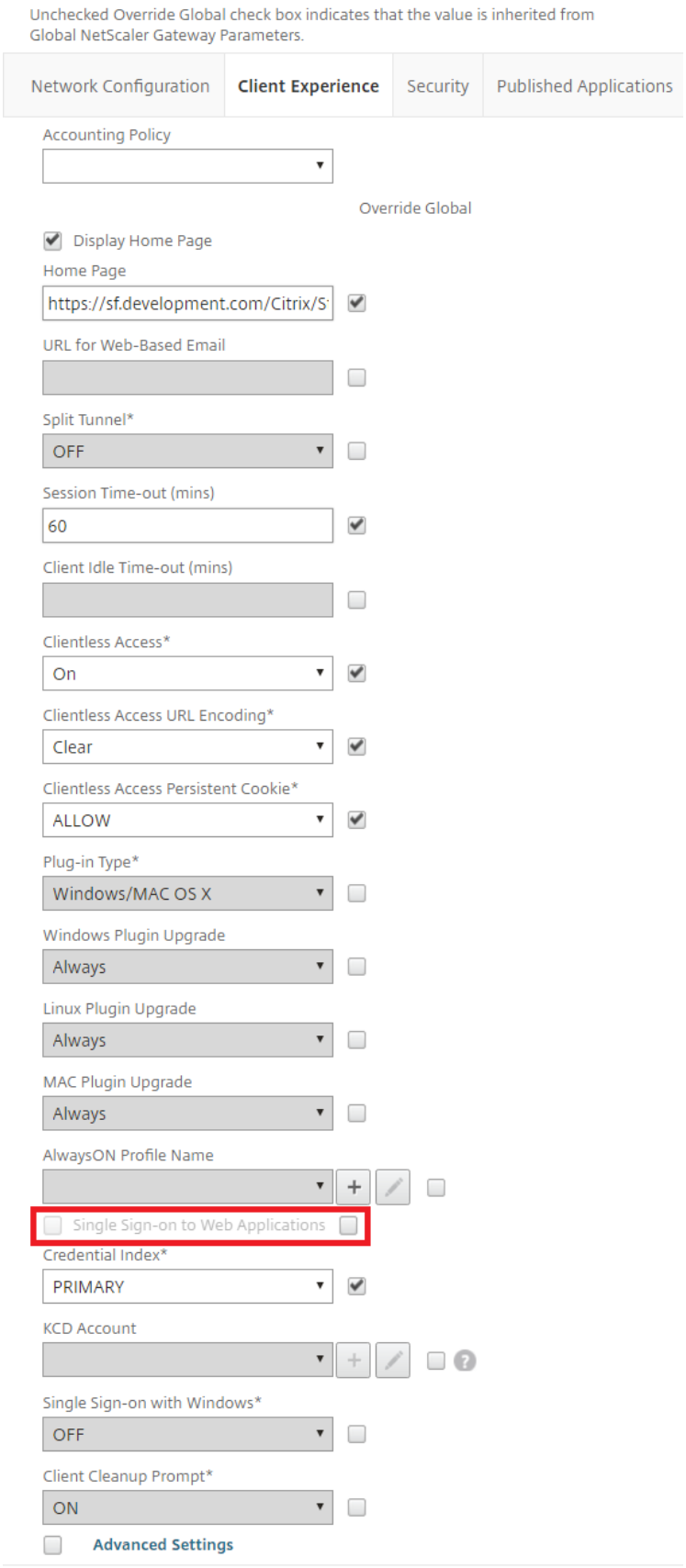


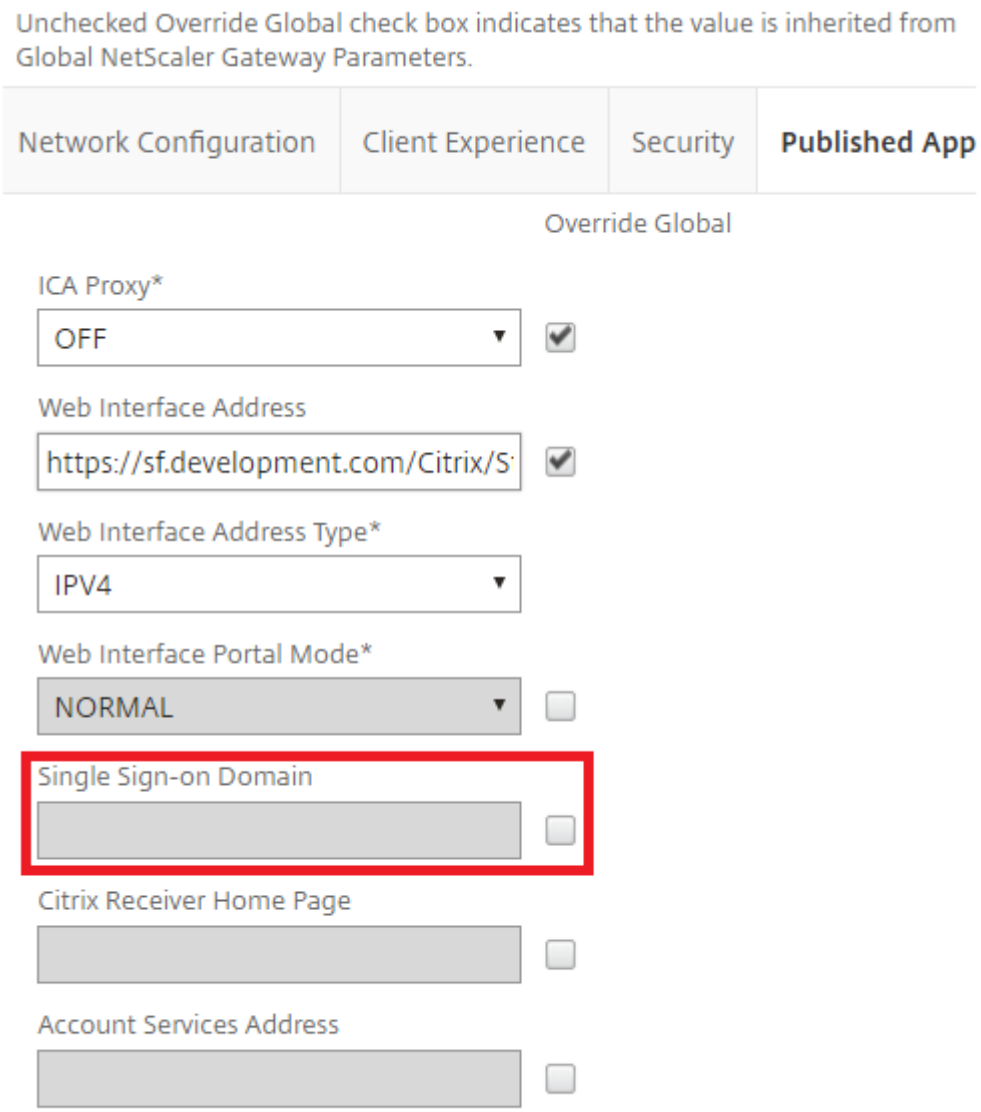
> **Remarque :**
>
> La mise en cache du mot de passe de navigateur n'est pas recommandée dans ce scénario d'authentification. Si les utilisateurs disposent de mots de passe différents pour les deux comptes de domaine différents, la mise en cache du mot de passe peut entraîner une mauvaise expérience.

Stratégie d'action de session VPN Citrix Gateway sans client (CVPN)

- Si le paramètre Authentification unique auprès des applications Web est activé dans votre stratégie de session Citrix Gateway, les informations d'identification incorrectes envoyées par l'appliance Citrix ADC à Receiver pour Web sont ignorées car vous avez désactivé la méthode d'authentification **Authentification pass-through via Citrix 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 l’appliance Citrix ADC ne change pas le comportement décrit dans cet article.





Configurer des points balises

March 3, 2020

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. L'application Citrix Workspace 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 connex-

ion appropriés puissent être renvoyés à l'application Citrix Workspace. 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 l'application Citrix Workspace 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 Citrix 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 à l'appliance Citrix Gateway par le biais duquel la connexion doit être routée. Cela signifie que l'utilisateur n'a pas besoin d'ouvrir une session sur l'appliance 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 Citrix 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 l'application Citrix Workspace 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 de l'application Citrix Workspace 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 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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 l'application Citrix Workspace 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.

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

August 28, 2019

Vous pouvez fournir un accès aux ressources depuis le réseau de votre entreprise et depuis Internet par le biais d'un Citrix 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 l'application Citrix Workspace

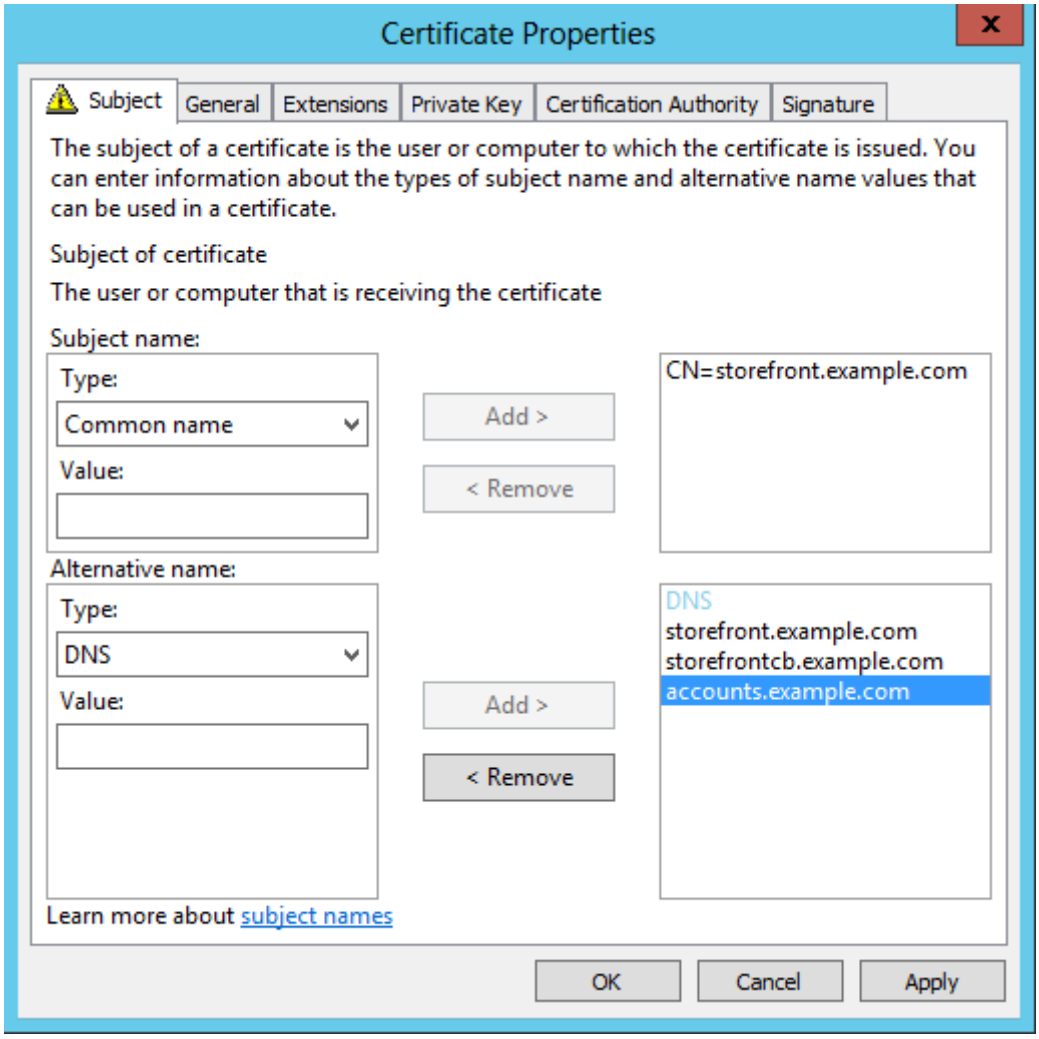
L'application Citrix Workspace tente de contacter des points balises et utilise les réponses pour déterminer si les utilisateurs sont connectés à des réseaux locaux ou publics. Lorsqu'un utilisateur accède à un bureau ou une application, les informations d'emplacement sont transmises au serveur fournissant les ressources afin que les détails de connexion appropriés puissent être renvoyés à l'application Citrix Workspace. 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 d'indicateur, reportez-vous à la section Configurer des points balises.

> Remarque :
>
> Dans cet article, les mentions de « Application Citrix Workspace » s'appliquent également aux versions prises en charge de Citrix Receiver, sauf indication contraire.

Configurer le serveur virtuel Citrix 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 du serveur virtuel Citrix Gateway dans la zone démilitarisée (DMZ) lorsque les clients externes essayent 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 Citrix 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 de serveur virtuel Citrix Gateway :`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 Citrix 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 du serveur virtuel Citrix 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 serveur virtuel Citrix 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 serveur virtuel Citrix 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.exemple.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 serveur virtuel Citrix 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 Citrix Gateway

WinSCP est un outil tiers utile pour déplacer des fichiers d'un ordinateur Windows sur un système de fichiers Citrix Gateway. Copiez les certificats à importer sur le dossier /nsconfig/ssl/ dans le système de fichiers Citrix Gateway. Vous pouvez utiliser les outils OpenSSL de Citrix 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 Citrix Gateway.

1. Copiez le fichier PFX dans /nsconfig/ssl sur l'appliance Citrix Gateway ou VPX.
2. Ouvrez l'interface de ligne de commande Citrix Gateway.
3. Pour basculer vers le shell FreeBSD, tapez **Shell** pour quitter l'interface de ligne de commande Citrix 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 Citrix Gateway, tapez sur Exit.

Stratégie de session Citrix Receiver pour Windows, Citrix Receiver pour Mac ou Citrix Gateway

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

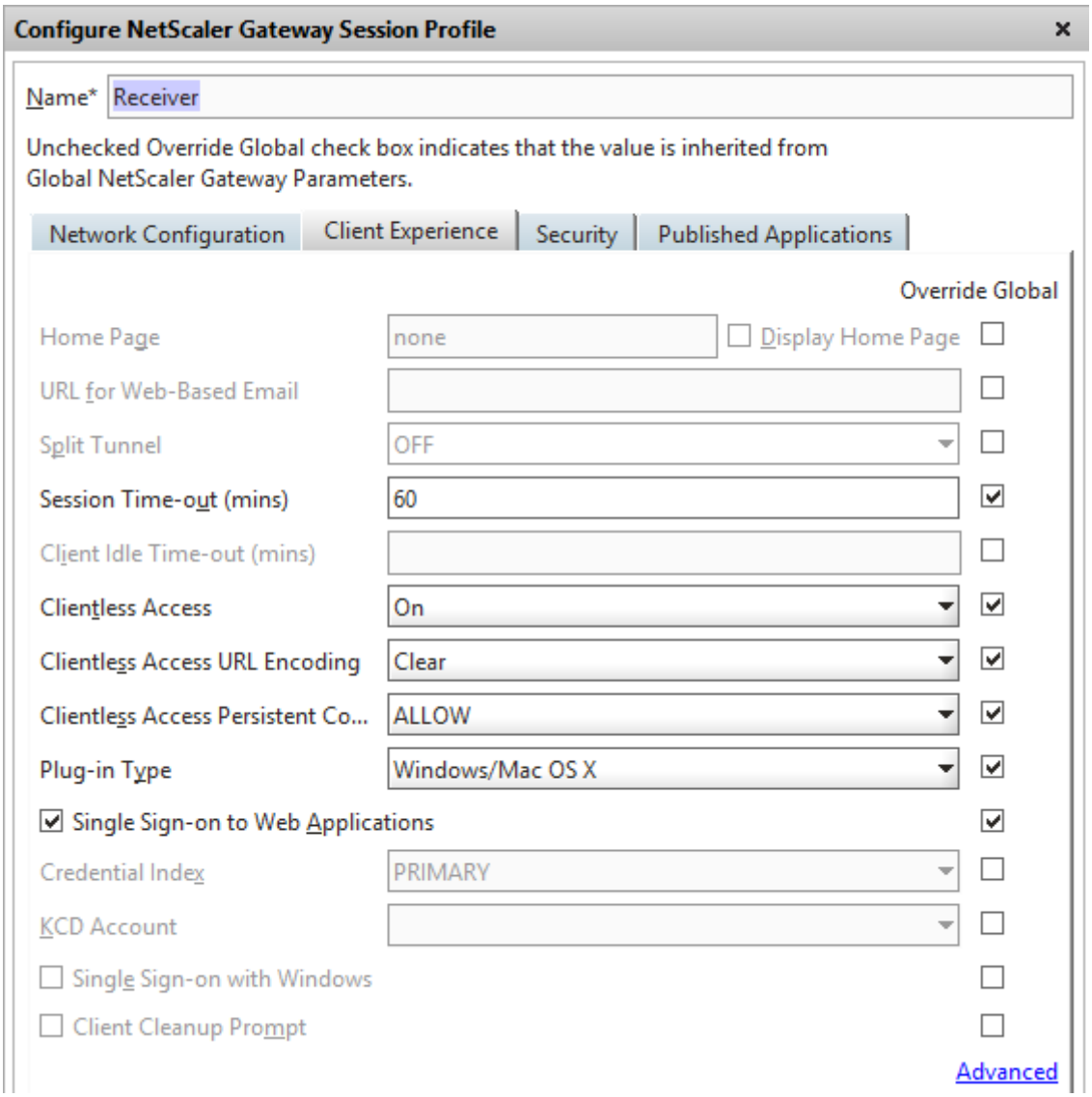
Stratégie de session de la passerelle Receiver pour Web

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

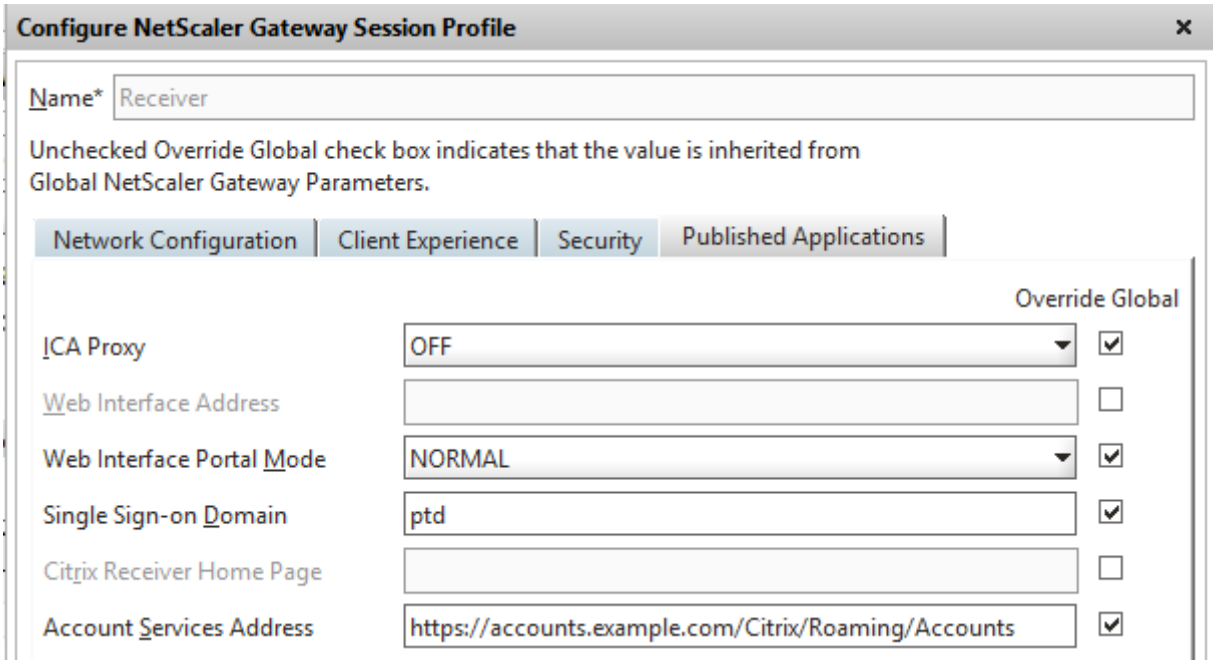
Paramètres cVPN et Smart Access

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

Profil Receiver

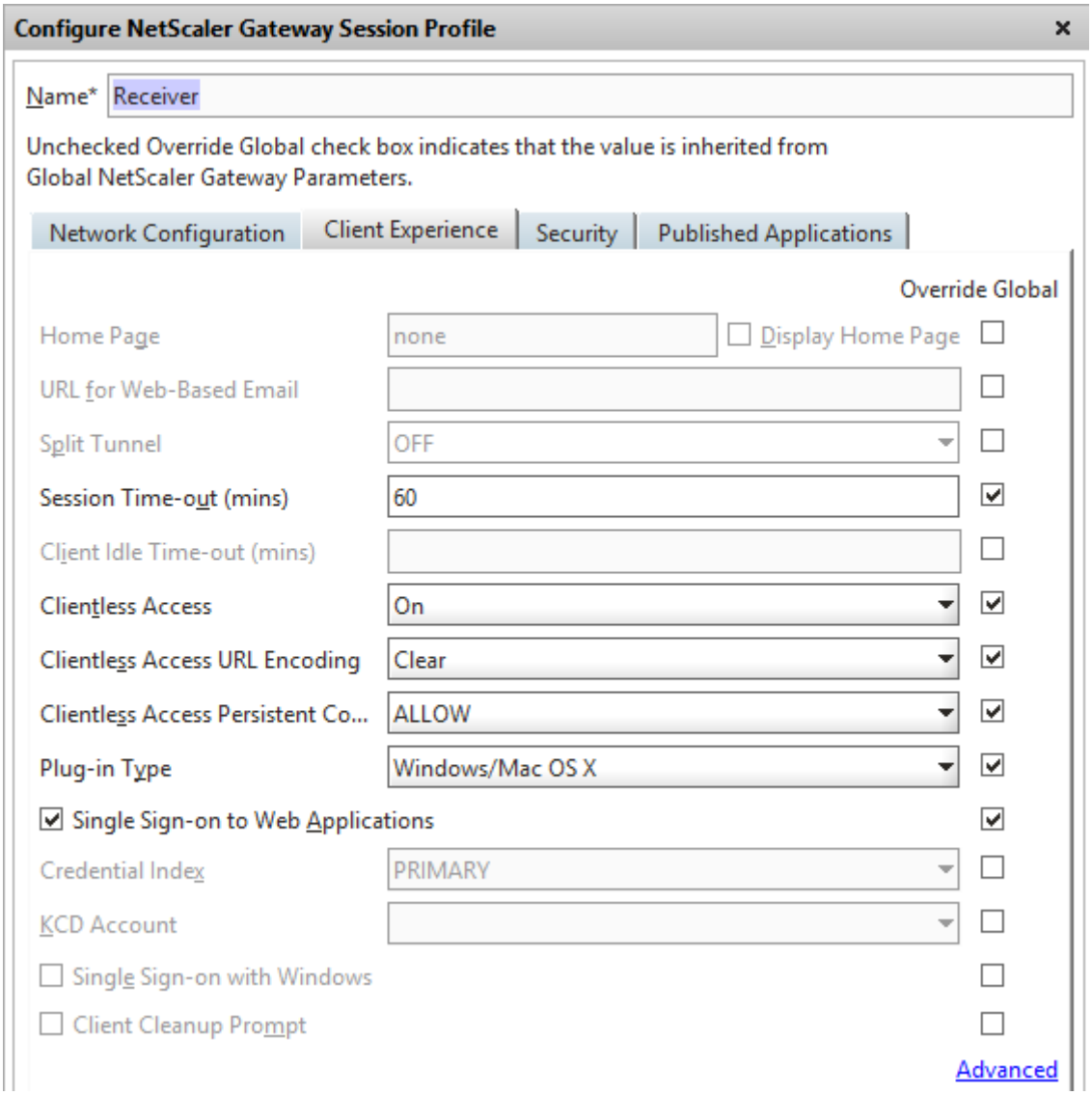


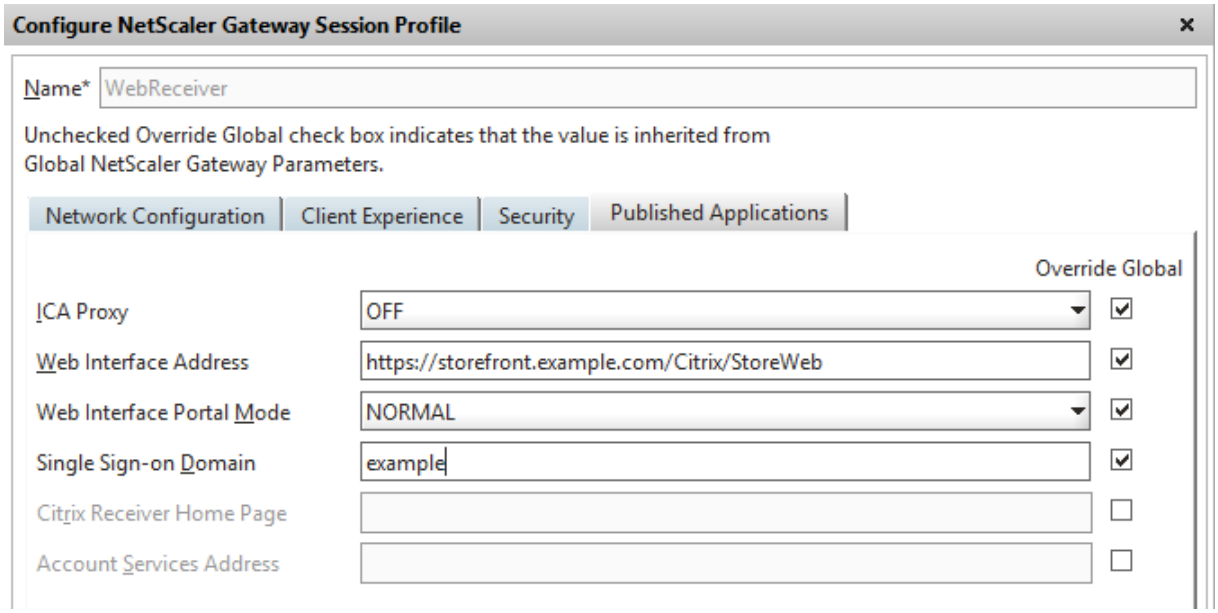
Configurez l'URL du service de comptes de profil de session sur `https://accounts.example.com/Citrix/Roaming/Accounts` et NON sur `https://storefront.example.com/Citrix/Roaming/Accounts`.



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

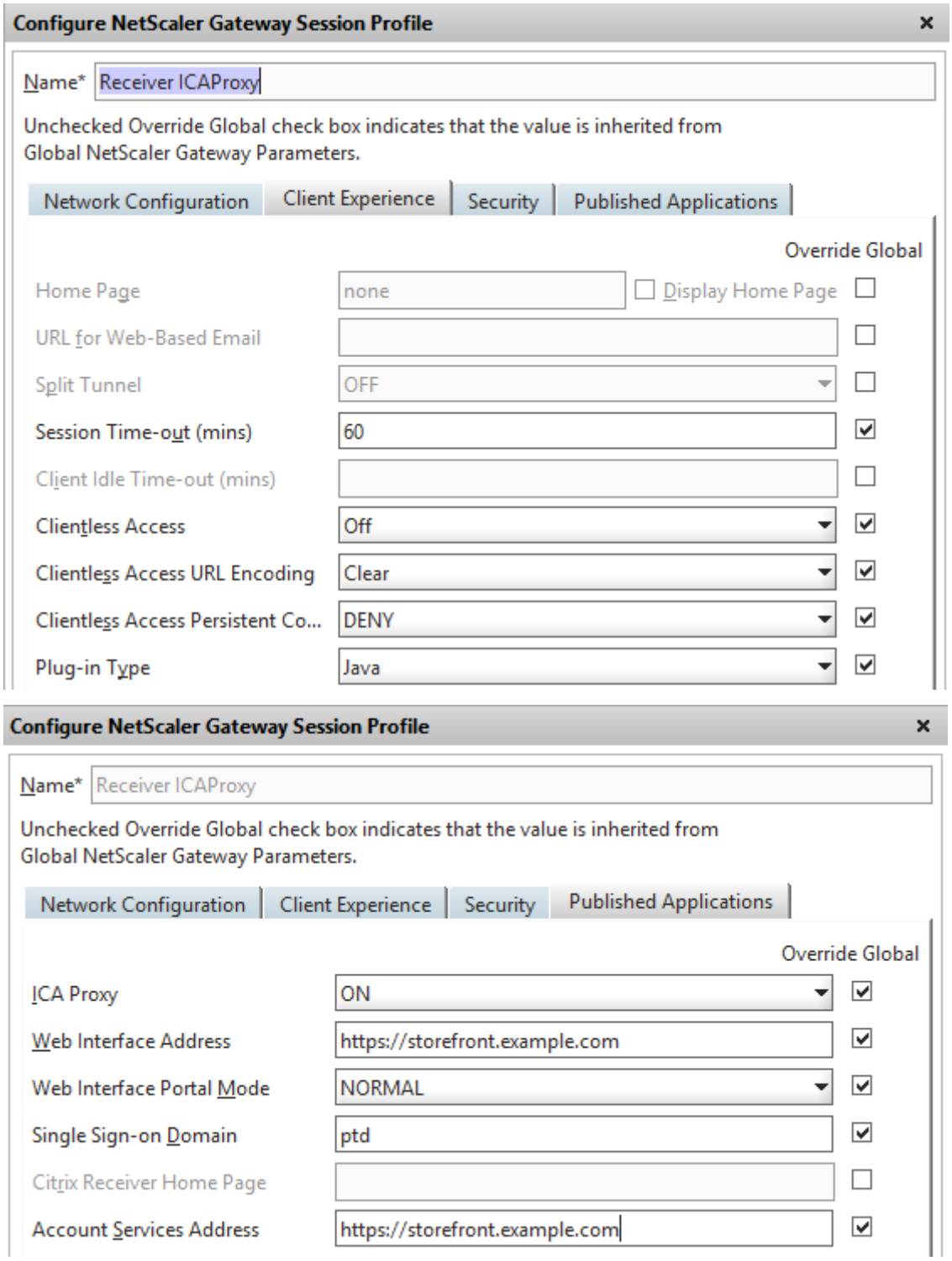




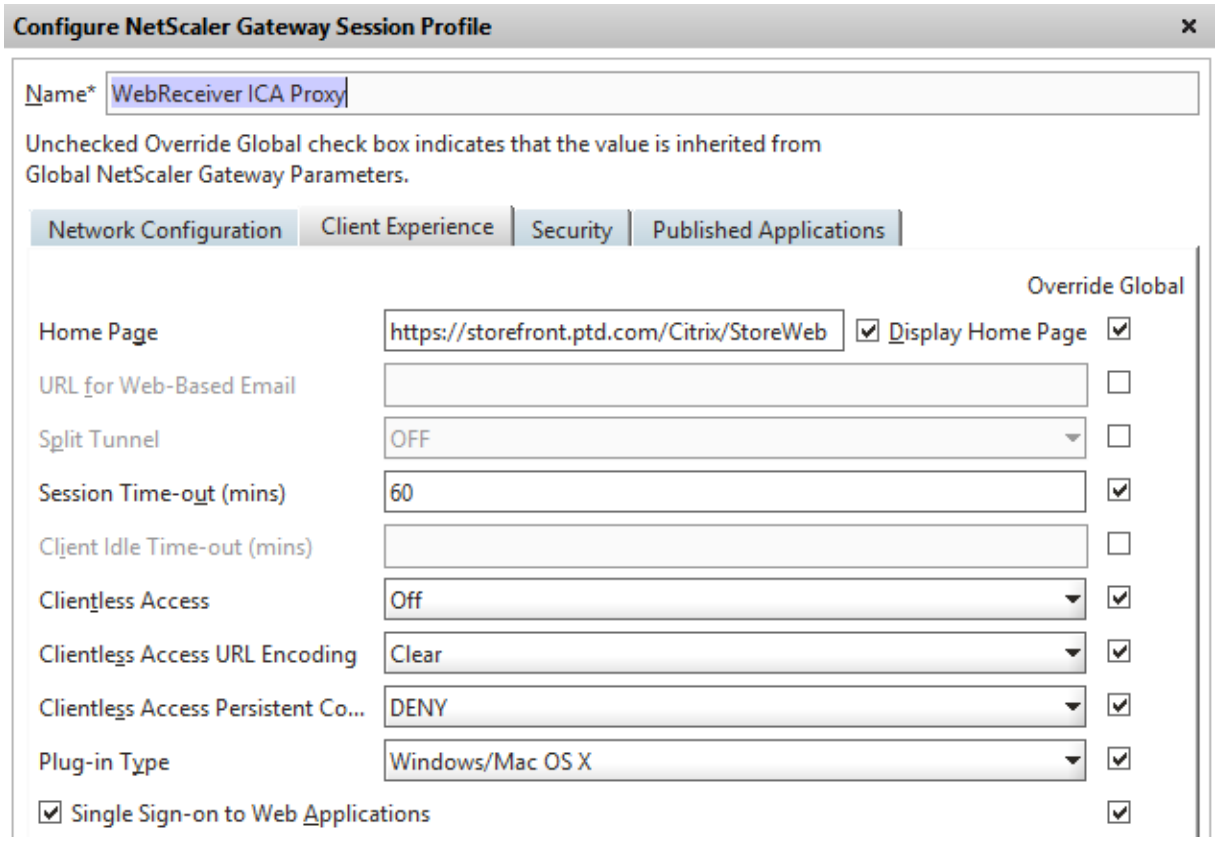
Paramètres ICA Proxy et du mode Basic

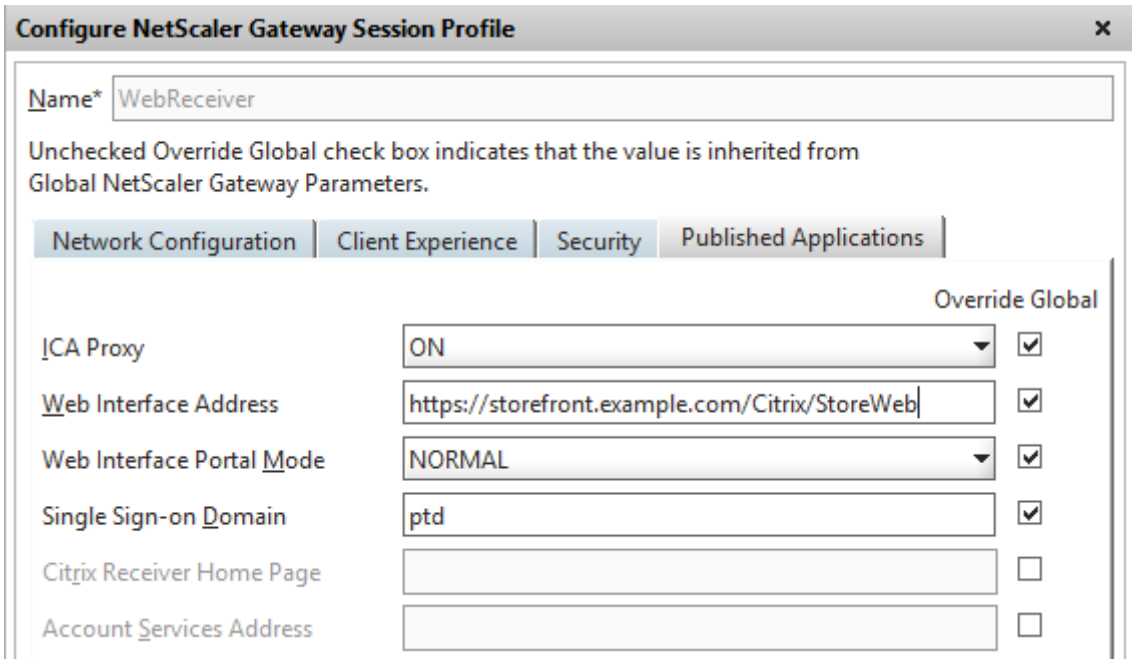
Si vous utilisez un serveur proxy ICA, activez le mode de base sur la page des propriétés du serveur virtuel Citrix Gateway. Seule une licence de plate-forme Citrix ADC est requise.

Profil Receiver



Profil Receiver pour Web





Configurer l'URL de base de l'hôte serveur StoreFront, la passerelle et le certificat SSL

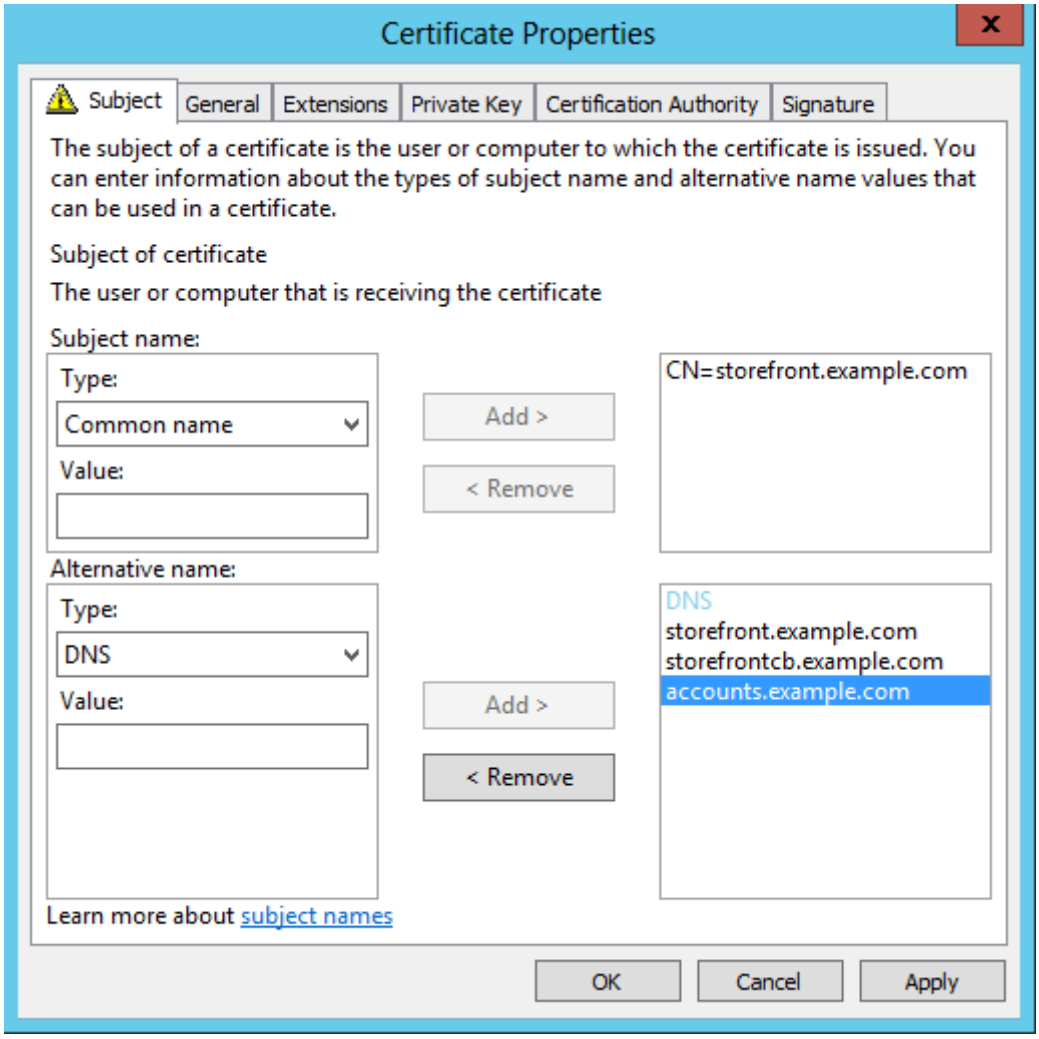
Le même nom de domaine complet (FQDN) partagé résolu sur le serveur virtuel Citrix Gateway doit également être résolu directement sur l'équilibrage de la charge StoreFront, si un cluster StoreFront a été créé ou qu'une seule adresse IP StoreFront héberge le magasin.

DNS interne : créez trois enregistrements A DNS

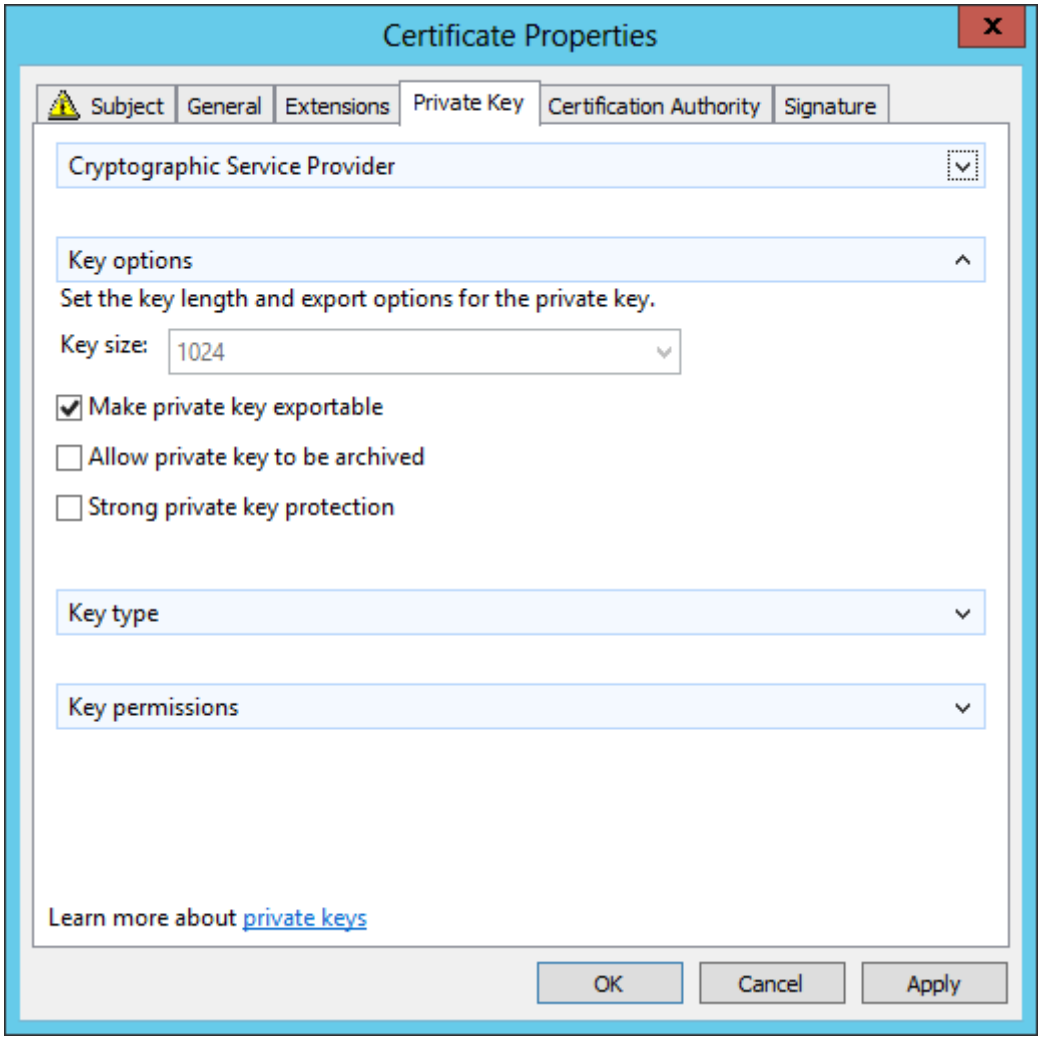
- storefront.exemple.com doit être résolu sur l'équilibrage de charge StoreFront ou sur une adresse IP du serveur StoreFront.
- storefrontcb.exemple.com doit être résolu sur l'adresse IP virtuelle du vServer de la passerelle, par conséquent si un pare-feu est présent entre la DMZ et le réseau local d'entreprise, 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

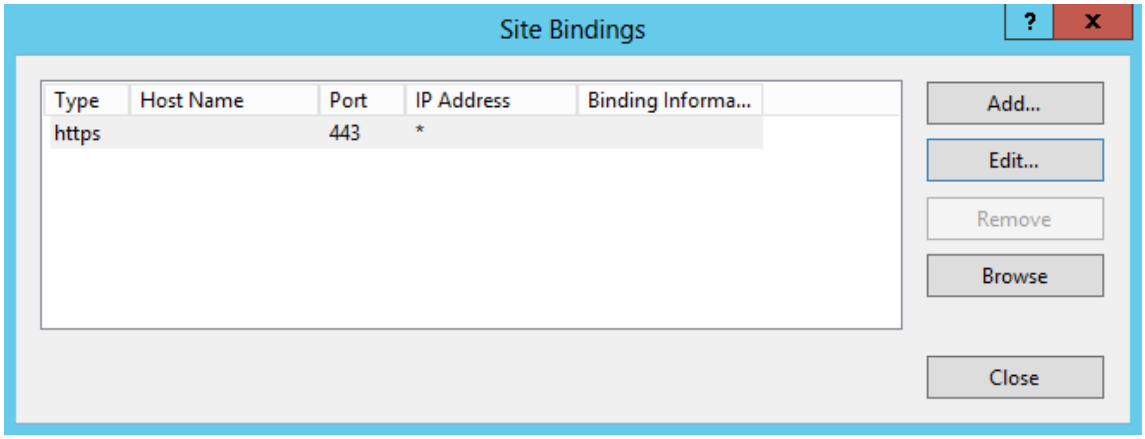
1. Créez un certificat approprié pour le serveur StoreFront ou groupe de serveurs avant l'installation de StoreFront.
2. Ajoutez le nom de domaine complet partagé aux champs Nom commun et DNS. Assurez-vous qu'ils correspondent au nom de domaine complet (FQDN) utilisé dans le certificat SSL lié au serveur virtuel Citrix Gateway que vous avez créé précédemment ou utilisez le même certificat lié au serveur virtuel Citrix Gateway.
3. Ajoutez l'alias de compte (`accounts.example.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 Citrix 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.

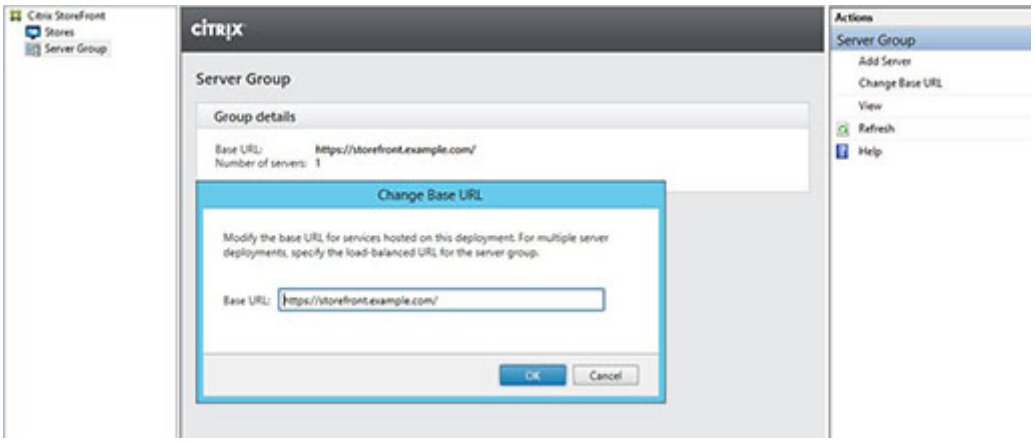


5. Signez le certificat à l'aide d'une autorité de certification tierce telle que Verisign, l'autorité de certification racine de votre entreprise ou une autorité de certification intermédiaire.
6. Exportez le certificat au format PFX y compris la clé privée.
7. Importez le certificat et la clé privée 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 serveur virtuel d'équilibrage de charge Citrix ADC, importez le certificat sur ce dernier.
8. Créez une liaison HTTPS dans IIS sur le serveur StoreFront et liez-y le certificat SSL importé.



9. 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>` valide à condition qu'elle existe dans le certificat en tant que SAN. Exemple : `https://storefront.example.com`.



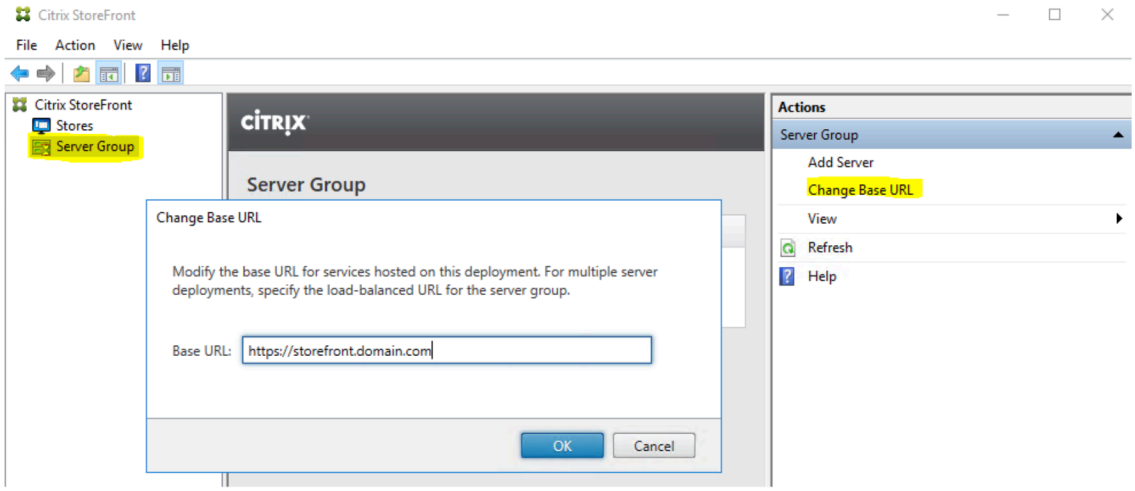
Modifier l'URL de base du serveur HTTP et la remplacer par HTTPS

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.

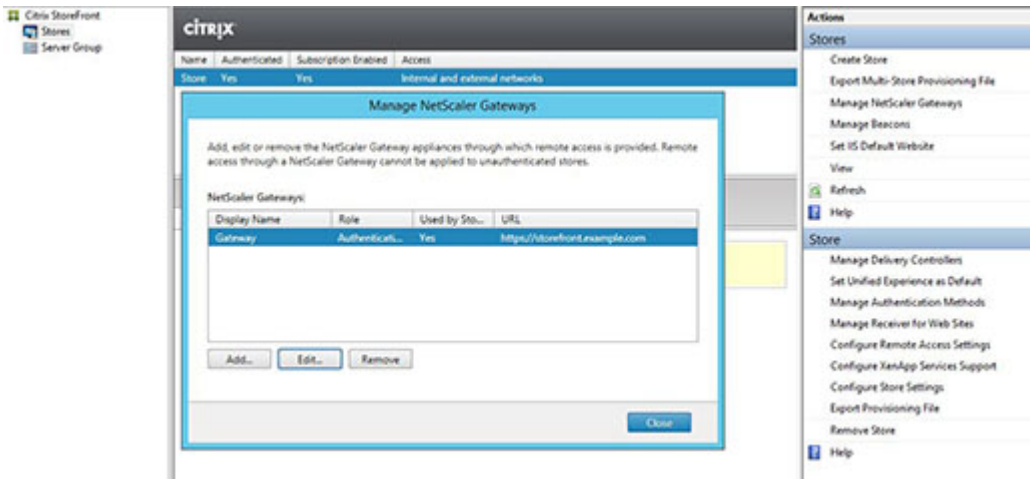
Procédez comme suit pour modifier l'URL de base sur StoreFront 3.x :

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**.

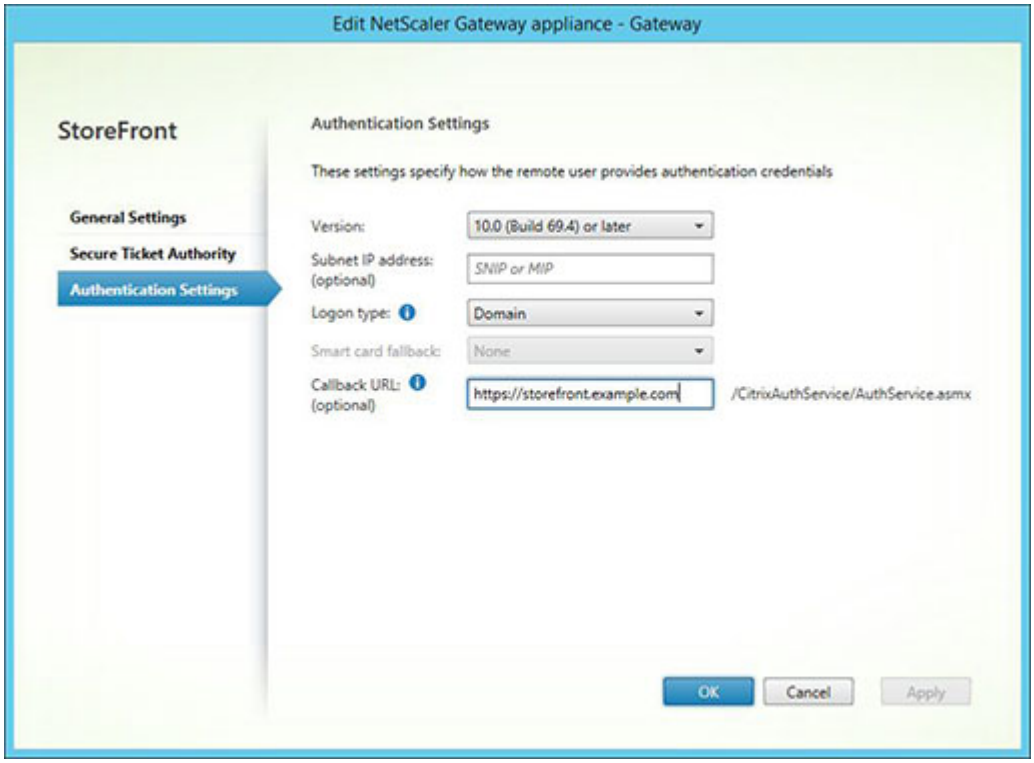


Configurez la passerelle sur le serveur StoreFront : storefront.example.com

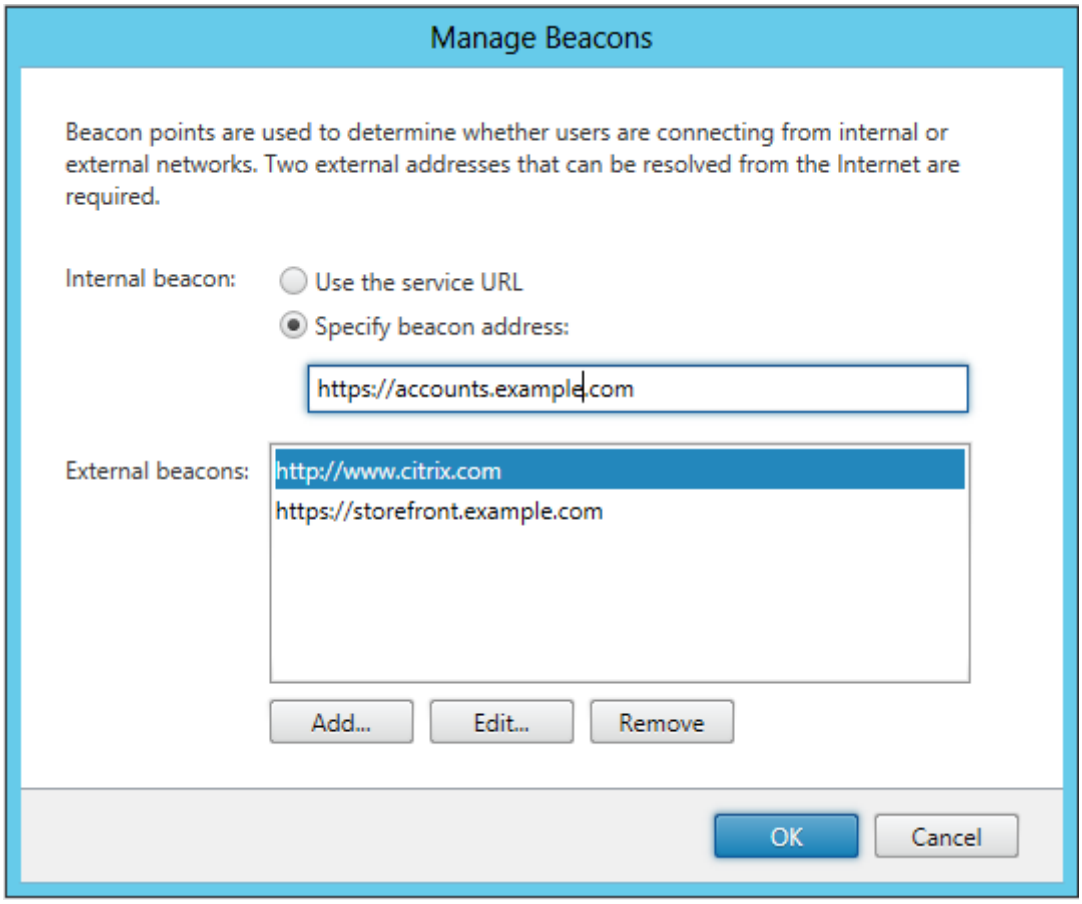
1. Dans le nœud **Magasins**, cliquez sur **Gérer Citrix Gateway** dans le panneau **Actions**.
2. Sélectionnez la passerelle dans la liste **Passerelle** et cliquez sur **Modifier**.



3. Sur la page **Paramètres généraux**, indiquez le nom de domaine complet partagé dans le champ **URL Citrix Gateway**.
4. Sélectionnez l'onglet **Paramètres d'authentification** et entrez le nom de domaine complet (FQDN) de rappel dans le champ d'adresse **URL de rappel**.



5. Sélectionnez l'onglet **Secure Ticket Authority** et vérifiez que les serveurs Secure Ticket Authority (STA) correspondent à la liste des Delivery Controller déjà configurés dans le nœud **Magasin**.
6. Activez l'accès à distance pour le magasin.
7. 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 serveur virtuel Citrix 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.



Prise en charge de la découverte à l'aide de noms de domaine complets

Pour 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.co*
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. Dans la section <service id>, trouvez la chaîne <allowedAudiences>. Ajoutez une ligne pour audience="https://accounts.example.com/" comme indiqué ici. Enregistrez et fermez le fichier web.config.

```
1 <service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="
     Authentication Token Producer">
2 ...
3 <allowedAudiences>
```

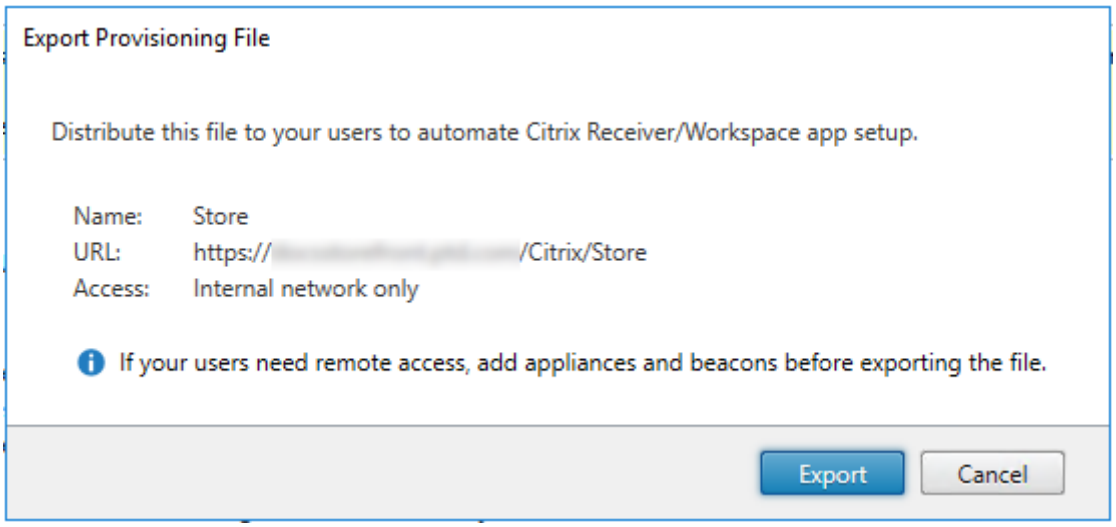


```
<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
<add name="https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
```

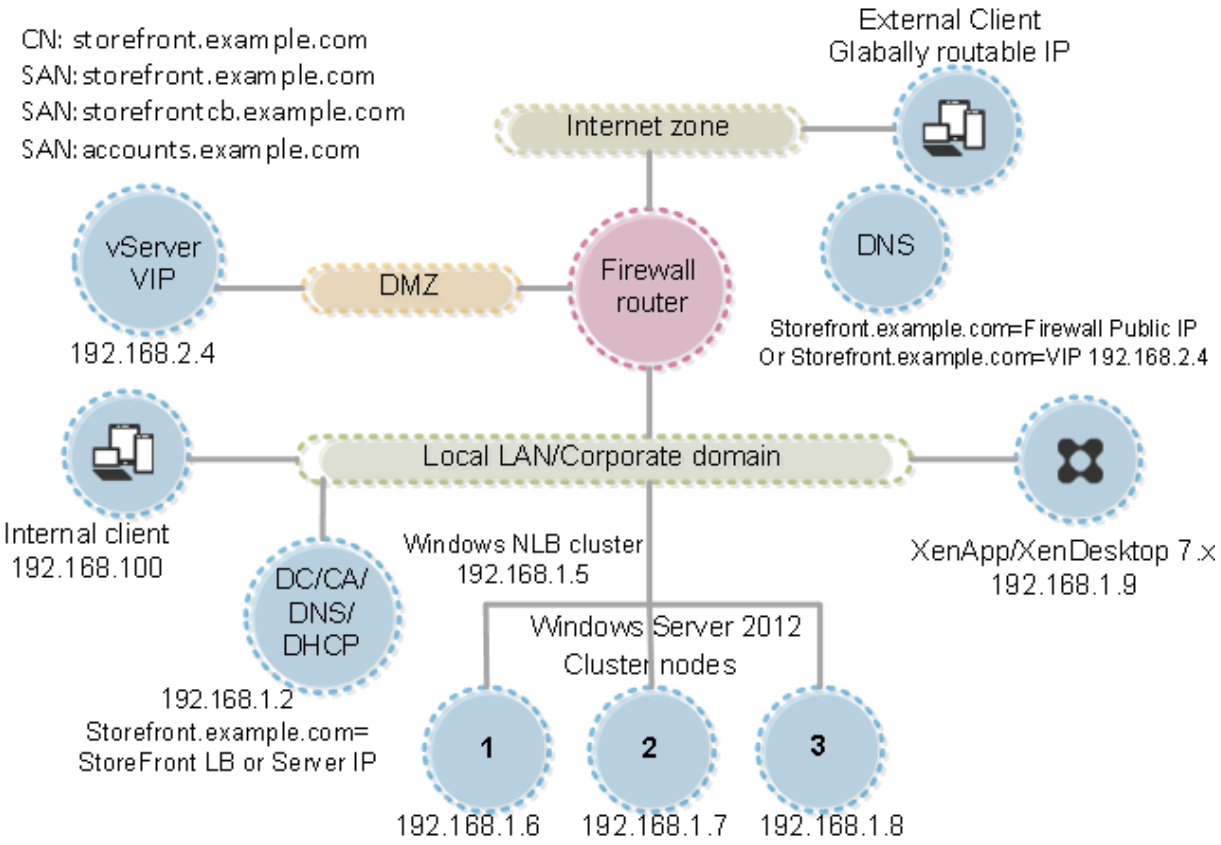
2. Dams *C:\inetpub\wwwroot\Citrix\Roaming\web.config*, recherchez la section <tokenManager> et ajoutez une ligne pour `audience="https://accounts.example.com/"` comme indiqué ici. Enregistrez et fermez le fichier web.config.

```
<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>
```

Vous pouvez également exporter le fichier de provisioning natif Receiver .CR pour le magasin. Cela élimine la nécessité de configurer la première utilisation de l'application Citrix Workspace. Distribuez ce fichier à tous les clients des applications Citrix Workspace pour Windows et Mac.



Si l'application Citrix Workspace est installée sur le client, le type de fichier .CR est reconnu et il suffit de double-cliquer sur le fichier de provisioning pour démarrer l'importation.



Configurations avancées

January 8, 2020

Vous pouvez configurer l'option avancée suivante à l'aide de la console StoreFront, de PowerShell, de propriétés de certificat ou de fichiers de configuration.

Tâche	Détail
Configurer le filtrage des ressources	Permet de filtrer les ressources d'énumération en fonction du type de ressource et de mots clés.

Configurer le filtrage des ressources

March 3, 2020

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 plus d'informations, veuillez consulter Citrix StoreFront SDK PowerShell Modules.

> 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 :

```
$dsInstallProp = Get-ItemProperty '
 -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name
    InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $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 renvoyer 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 Citrix Virtual Apps and Desktops. 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 :

- Auto
- Obligatoire

Pour plus d'informations sur les mots-clés, reportez-vous aux sections Optimiser l'expérience utilisateur et Configuration de 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

January 8, 2020

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 l'application Citrix Workspace
- Empêcher l'application Citrix Workspace 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

March 3, 2020

Cet article décrit les tâches de configuration supplémentaires qui ne peuvent pas être effectuées à l'aide de la console de gestion Citrix 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

Activer la signature de fichier ICA

StoreFront permet de signer numériquement les fichiers ICA afin que les versions de l'application Citrix Workspace 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 fichiers ICA dans l'application Citrix Workspace, consultez la section 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.

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.

```
<certificateManager>
    <certificates>
        <clear />
        <add ... />
        ...
    </certificates>
</certificateManager>
```

4. Incluez les détails du certificat à utiliser pour la signature.


```
<certificateManager>
    <certificates>
        <clear />
        <add id="certificateid" thumb="certificatethumbprint" />
        <add ... />
    ...
    </certificates>
</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.

```
<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 hashAgorithm 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.

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
  $certificate = Get-DSCertificate "certificatethumbprint"
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.

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.

```
<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 l'application Citrix Workspace

Lorsque les utilisateurs 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, modifiez les fichiers du service d'authentification.

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.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
```

3. Supprimez les marques de commentaire pour l'instruction en supprimant le début **@*** et la fin ***@**.

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
```

   Les utilisateurs de l'application Citrix Workspace 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 lorsqu'ils accèdent aux magasins qui utilisent ce service d'authentification.


```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
```

Pour modifier le texte de titre de la boîte de dialogue d'ouverture de session pour les utilisateurs d'autres paramètres régionaux, modifiez les fichiers localisés *ExplicitAuth.languagecode.resx*, où **languagecode** est l'identificateur de paramètres régionaux.

Empêcher l'application Citrix Workspace pour Windows de mettre les mots de passe et les noms d'utilisateur en cache

Par défaut, l'application Citrix Workspace pour Windows stocke les mots de passe des utilisateurs lorsqu'ils se connectent à des magasins StoreFront. Pour empêcher Citrix Receiver pour Windows ou l'application Citrix Workspace 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.

1. Utilisez un éditeur de texte pour ouvrir le fichier inetpub\wwwroot\Citrix\Authentication\App_Data\Template
2. Recherchez la ligne suivante dans le fichier.

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
```

3. Commentez l'instruction comme indiqué ci-dessous.

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
```

Les utilisateurs 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 l'Éditeur du Registre. 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

March 3, 2020

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.

> **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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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.

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.

```
<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

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.

```
<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

January 8, 2020

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 StoreFront 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 l'application Citrix Workspace est activé(e) pour Citrix Receiver pour Web, StoreFront requiert également ces extensions de nom de fichier :

- .dmg
- .exe

Si l'application Citrix Workspace pour HTML5 est activée, 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. Ne modifiez pas cette configuration. 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 assemblys 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 l'application Citrix Workspace 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 messagerie de vos utilisateurs peuvent également être utilisés, mais les utilisateurs apercevront une boîte de dialogue d'avertissement de certificat lorsque l'application Citrix Workspace 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 l'application Citrix Workspace 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 *<Répertoired'installation>*\Scri
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 Citrix Virtual Apps. Le relais SSL est un composant par défaut de Citrix Virtual Apps 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 Citrix 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 potentiellement 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.

Mettre à disposition des applications SaaS et Web via Storefront

Vous pouvez mettre à disposition en toute sécurité vos applications SaaS et Web aux utilisateurs via votre magasin StoreFront. Citrix Cloud et l'utilitaire de synchronisation du contrôle d'accès pour StoreFront vous permettent d'utiliser des stratégies de filtrage Web et de contrôle de sécurité améliorées pour ces applications afin de protéger vos utilisateurs et votre réseau contre les logiciels malveillants et les fuites de données. Les utilisateurs accèdent à leur magasin StoreFront comme ils le font d'habitude pour lancer les applications SaaS et Web que vous avez configurées dans Citrix Cloud. Pour plus d'informations, consultez Contrôle d'accès pour les applications SaaS et Web dans StoreFront.

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 l'application Citrix Workspace 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

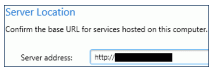
votre organisation possède une stratégie de sécurité qui restreint les fonctions de modification des mots de passe utilisateur à un usage interne uniquement, vous devez vous assurer qu'aucun des magasins ne sont accessibles depuis l'extérieur de votre réseau interne. Lorsque vous créez le service d'authentification, 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 utilisateur.

Modifier l'URL de base du serveur StoreFront HTTP et la remplacer par HTTPS

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. Si vous installez et configurez Citrix StoreFront sans installer et configurer au préalable un certificat SSL, StoreFront utilise HTTP pour les communications.

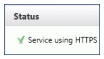
Si vous installez et configurez un certificat SSL ultérieurement, procédez comme suit pour vous assurer que StoreFront et ses services utilisent des connexions HTTPS.

Exemple :



Avant de modifier l'URL de base et la remplacer par HTTPS :

Après avoir modifié l'URL de base et l'avoir remplacée par HTTPS :



1. Configurez Microsoft Internet Information Services (IIS) pour HTTPS sur le serveur StoreFront :
   a) Utilisez la console Gestionnaire des services Internet (IIS) pour importer un certificat de serveur SSL signé par votre autorité de certification de domaine Microsoft Active Directory.
   b) Ajoutez une liaison IIS via HTTPS (443) au site Web par défaut.

   Pour obtenir des instructions détaillées, consultez la section CTX200292.
2. Dans la console de gestion Citrix StoreFront, dans le panneau de gauche, sélectionnez **Groupe de serveurs**.
3. Dans le panneau Actions, sélectionnez **Changer l'URL de base**.
4. Tapez l'URL de base et cliquez sur **OK**.

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.

Informations supplémentaires sur la sécurité

> **Remarque :**
>
> Ces informations peuvent changer à tout moment, sans préavis.

Votre organisation peut vouloir effectuer des analyses de sécurité de StoreFront pour des raisons réglementaires. Les options de configuration précédentes peuvent aider à éliminer certaines détections dans les rapports d'analyse de sécurité.

S'il existe une passerelle entre l'analyseur de sécurité et StoreFront, certains résultats peuvent être liés à la passerelle plutôt qu'à StoreFront lui-même. Les rapports d'analyse de sécurité ne distinguent généralement pas ces résultats (par exemple, configuration TLS). Pour cette raison, les descriptions techniques contenues dans les rapports d'analyse de sécurité peuvent être trompeuses.

Lors de l'interprétation des rapports d'analyse de sécurité, notez ce qui suit :

- Les pages HTML de StoreFront peuvent ne pas inclure de protection contre le détournement de clic (par la stratégie de sécurité du contenu ou les en-têtes de réponse X-Frame-Options). Cependant, ces pages HTML sont constituées uniquement de contenu statique, et par conséquent, les attaques de détournement de clic ne sont pas pertinentes.
- La version de Microsoft IIS et l'utilisation d'ASP.NET sont visibles dans les en-têtes HTTP. Cependant, cette information est déjà évidente par la présence de StoreFront lui-même, car il repose sur ces technologies.
- Lors du lancement d'applications et de bureaux, StoreFront utilise un jeton pour se protéger contre la falsification de requêtes inter-sites (CSRF). Ce jeton est envoyé en tant que cookie dans une réponse sans être marqué comme Secure ou HttpOnly. Lorsqu'il est envoyé ultérieurement dans une requête, le jeton est inclus dans la chaîne de requête d'une URL. Cependant, StoreFront ne s'appuie pas sur ce mécanisme pour authentifier les requêtes HTTP.
- StoreFront utilise le composant open source jQuery. Une version utilisée est jQuery 1.3.2. Selon le projet open source jQuery, une modification a été apportée dans jQuery 1.12.0 pour atténuer les vulnérabilités potentielles dans une forme spécifique de requête inter-domaines. Ce changement n'était pas une atténuation d'une vulnérabilité dans jQuery même ; c'était une atténuation

de l'utilisation abusive potentielle par la logique d'application. La logique d'application Citrix concernée, dans la fonctionnalité Receiver pour Web partagée par NetScaler et StoreFront, n'utilise pas cette forme spécifique de requête inter-domaines, n'est pas affectée par cette vulnérabilité et n'a pas bénéficié de cette atténuation.

Cette atténuation a ensuite été supprimée dans jQuery 1.12.3 pour des raisons de compatibilité. Étant donné que la logique d'application Citrix n'a pas bénéficié de cette atténuation, cette suppression n'a aucun impact matériel sur les versions de NetScaler et StoreFront utilisant jQuery 1.12.4.

Exporter et importer la configuration StoreFront

March 3, 2020

> Remarque :
>
> Vous pouvez uniquement importer des configurations StoreFront qui proviennent de la même version de StoreFront que l'installation StoreFront cible.

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.

Scénarios dans lesquels l'exportation et l'importation de la configuration peuvent être utilisées

- Sauvegardez uniquement les déploiements StoreFront dans un bon état de fonctionnement et dans un état approuvé. Toute modification de la configuration nécessite une nouvelle sauvegarde pour remplacer l'ancienne sauvegarde. Vous ne pouvez pas modifier les sauvegardes existantes car un hachage de fichier sur backup.zip empêche la modification.
- Effectuez une sauvegarde AVANT la mise à niveau de StoreFront pour la récupération d'urgence.
- Clonage des déploiements StoreFront de test existants à mettre en production
- Création d'environnements d'acceptation par l'utilisateur en clonant des déploiements de production dans un environnement de test

- Déplacement de StoreFront pendant les migrations du système d'exploitation, telles que la mise à niveau du système d'exploitation d'hébergement de 2008R2 à 2019
- Création de groupes de serveurs supplémentaires dans des déploiements multigéographiques, par exemple dans les grandes entreprises disposant de plusieurs data centers

Éléments à prendre en considération lors de l'exportation et de l'importation d'une configuration StoreFront

- 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.

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 **-Credential** conjointement avec le paramètre **-NoEncryption**. Exemple : $CredObject
-NoEncryption (Commutateur)	Indique que l'archive de sauvegarde doit être un fichier .zip non crypté. N'utilisez pas **-NoEncryption** conjointement avec le paramètre **-Credential**.
-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 **-Credential** ou **-NoEncryption** 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** 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 : `$env:userprofile\desktop\backup.ctxzip`
-Credential (Objet PSCredential)	Spécifiez un objet d'information d'identification pour décrypter un fichier de sauvegarde crypté durant l'importation. Exemple : `$CredObject`
-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 : `https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

Paramètre	Description
-TargetFolder (chaîne)	Chemin d'accès d'exportation à l'archive de configuration. Exemple : `$env:userprofile\desktop\`
-Credential (Objet PSCredential)	Utilisez ce paramètre pour créer une copie non cryptée de l'archive de sauvegarde cryptée. Spécifiez l'objet d'information d'identification PowerShell contenant le mot de passe à utiliser pour le décryptage. Exemple : `$CredObject`
-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 : `$env:userprofile\\desktop\\backup.ctxzip`

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 : `$env:userprofile\desktop\`
-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 l'applet de commande StoreFront dans la session PowerShell en cours

Ouvrez la console PowerShell (ISE) sur le serveur StoreFront principal et exécutez :

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath
    ','Machine')
2 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
    PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
    Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
    verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
    verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
    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

Exportez la configuration du serveur que vous souhaitez sauvegarder.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

Copiez le fichier backup.zip dans un emplacement sécurisé. Vous pouvez utiliser cette sauvegarde pour la récupération d'urgence pour restaurer le serveur à son état précédent.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
```

Sauvegarder une configuration existante sur le Serveur A et la restaurer sur le Serveur B pour créer un clone d'un serveur existant

Exportez la configuration du serveur que vous souhaitez sauvegarder.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

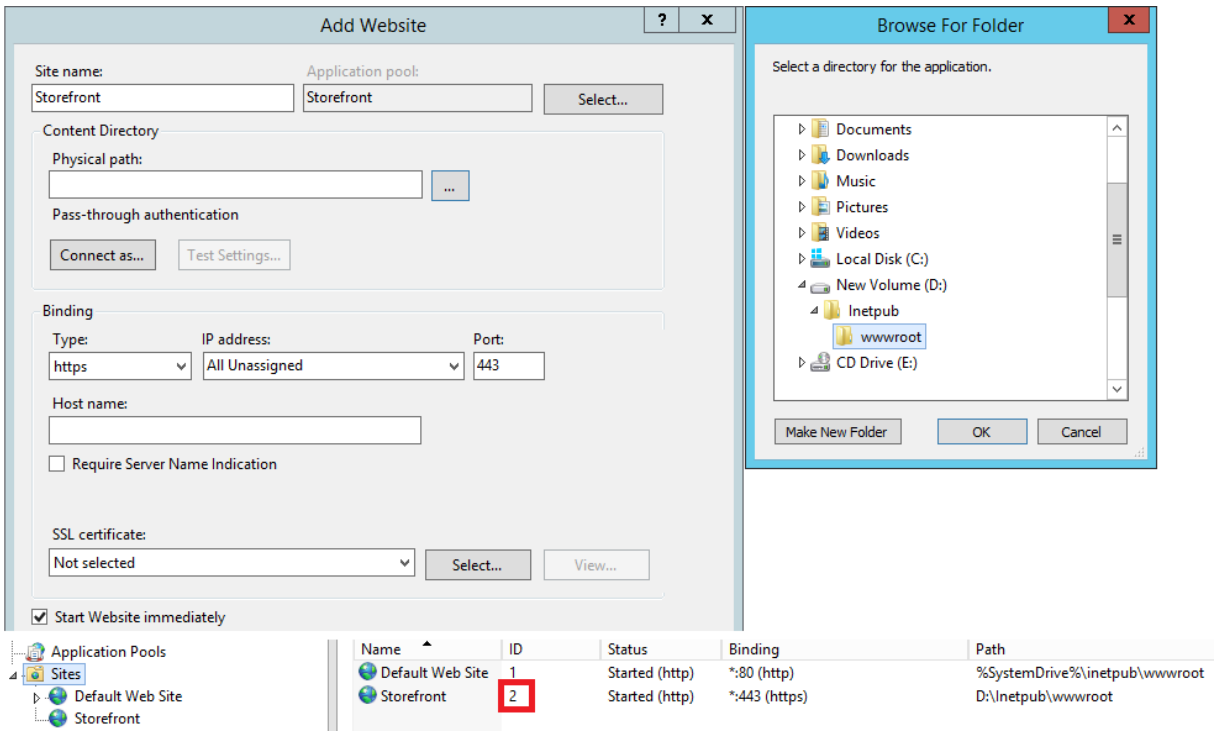
Copiez le fichier backup.zip sur le bureau du Serveur B.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
```

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\wwwrooot`.



1. Exportez une copie 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. Importez la configuration du Serveur A sur le Serveur B. L'élément SiteID contenu dans la copie de sauvegarde est utilisé et doit correspondre au site Web cible sur lequel vous souhaitez importer la configuration de StoreFront.

   ```
   Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
   backup.ctxzip"-HostBaseURL "https://serverB.example.com"
   ```

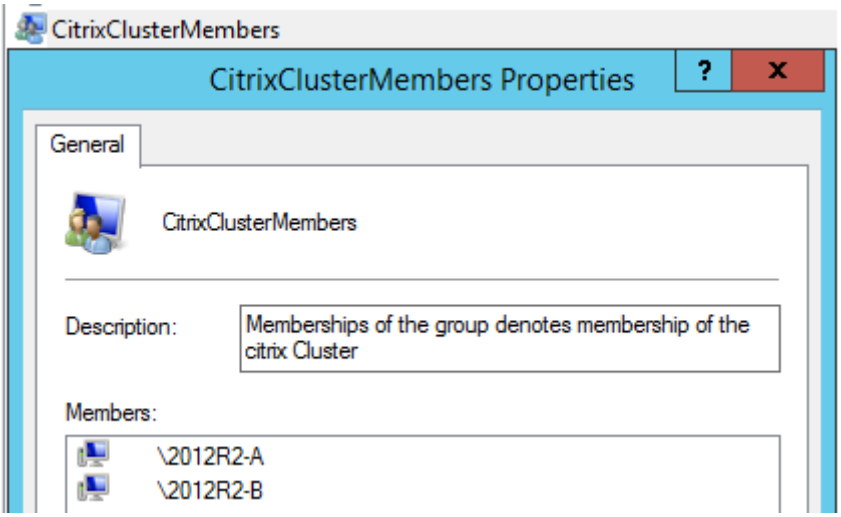
Scénarios de groupe de serveurs

Scénario 1 : sauvegarder une configuration de groupe de serveurs existante et la restaurer plus tard sur le même déploiement de groupe de serveurs

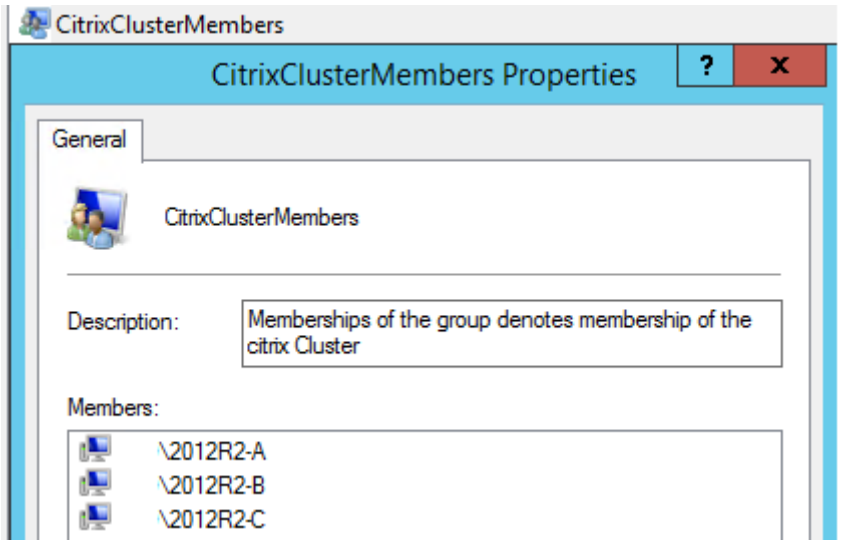
Une sauvegarde de configuration précédente a été effectuée lorsque seulement deux serveurs StoreFront, 2012R2-A et 2012R2-B, étaient membres du groupe de serveurs. L'archive de sauvegarde contient un enregistrement de **CitrixClusterMembership** correspondant au moment où la sauvegarde a été effectuée. 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 StoreFront 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"-HostBaseURL "https://servergroup1.example.com"
```

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"-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"-NoEncryption -HostBaseURL "https://servergroup2.example.
   com"
   ```

Créer une sauvegarde cryptée de la configuration du serveur

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'informations 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 spécifiiez un utilisateur lors de la création d'un nouvel objet d'information d'identification. Pour des raisons pratiques, cet exemple de code renvoie l'utilisateur Windows connecté.

Créez un objet d'informations d'identification PowerShell dans votre session PowerShell sur le serveur d'exportation.

```
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)
```

Exportez la configuration vers backup.ctxzip, un fichier zip crypté.


```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -Credential $CredObject
```

Créez un objet d'informations d'identification PowerShell identique dans votre session PowerShell sur le serveur d'importation.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.example.com"
```

Ôter la protection d'une archive de sauvegarde cryptée existante

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)

Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
```

SDK StoreFront

January 8, 2020

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 la section 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 Citrix 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.

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 la section 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.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
        ")]
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP"
    )
    # Import StoreFront modules. Required for versions of
        PowerShell earlier than 3.0 that do not support
        autoloading
    Import-Module Citrix.StoreFront
    Import-Module Citrix.StoreFront.Stores
    Import-Module Citrix.StoreFront.Authentication
    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 **$StoreIISPath** fourni. **$StoreVirtualPath** est équivalent à **$StoreIISpath** car les chemins virtuels sont toujours le chemin dans IIS. Par conséquent, dans Powershell, ils ont une valeur telle que « /Citrix/Store », « /Citrix/StoreWeb », ou « /Citrix/StoreAuth ».

```
# Determine the Authentication and Receiver virtual path to use
    based of the Store
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($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.

```
# Determine if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired
        hostbase url
    Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
 }

else
{

    Write-Error "A deployment has already been created on this
        server with a different host base url."
 }
```

- 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.

```
# Determine if the authentication service at the specified virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath
if(-not $authentication)
{

    # Add an Authentication service using the IIS path of the Store appended with Auth
    $authentication = Add-STFAuthenticationService $authenticationVirtualPath
 }

else
{

    Write-Output "An Authentication service already exists at the specified virtual path and will be used."
 }
```

- 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.

```
# Determine if the store service at the specified virtual path exists
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
if(-not $store)
{

# Add a Store that uses the new Authentication service configured to publish resources from the supplied servers
$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `
     -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType
 }

else
{
```



```
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 ou de l'application Citrix Workspace 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 la section 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 Citrix Gateway. Obtenir la méthode d'authentification ExplicitForms et CitrixAGBasic de Citrix Receiver pour Web à partir des protocoles pris en charge.

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be used directly if known
$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object { $_ -match "Explicit" -or $_ -match "CitrixAG" }

# Enable CitrixAGBasic in Receiver for Web (required for remote access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods $receiverMethods
```

- Active CitrixAGBasic sur le service d'authentification. Requis pour l'accès distant.

```
# Get the CitrixAGBasic authentication method from the protocols installed.
# Included for demonstration purposes as the protocol name can be used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object {
 $_ -match "CitrixAGBasic" }

# Enable CitrixAGBasic in the Authentication service (required for remote access)
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.

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-STFRoamingGateway will return the new Gateway if -PassThru is supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
```



```
    object
if($GatewaySubnetIP)
{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
 }

# Register the Gateway with the new Store
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 la section 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.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$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 : 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 la section 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 :

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the
    following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https:
    //example.com/FederationMetadata/2007-06/FederationMetadata.xml

# If the metadata has already been download, use the following:
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C
    :\Users\exampleusername\Downloads\FederationMetadata.xml"
```

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.

```
# Change this value for your Store
$storeVirtualPath = "/Citrix/Store"

$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
    VirtualPath $storeVirtualPath)
$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
    ServiceProvider.Uri.AbsoluteUri
```



```
$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/AssertionConsumerService")
$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/ServiceProvider/Metadata")
$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlTest")
Write-Host "SAML Service Provider information:
Service Provider ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest"
```

Exemple de sortie :

```
SAML Service Provider information:
Service Provider ID: https://storefront.example.com/Citrix/StoreAuth
Assertion Consumer Service: https://storefront.example.com/Citrix/
    StoreAuth/SamlForms/AssertionConsumerService
Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
    ServiceProvider/Metadata
Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
```

Résolution des problèmes de StoreFront

March 3, 2020

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 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 ce processus terminé,
> propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

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">
   ```

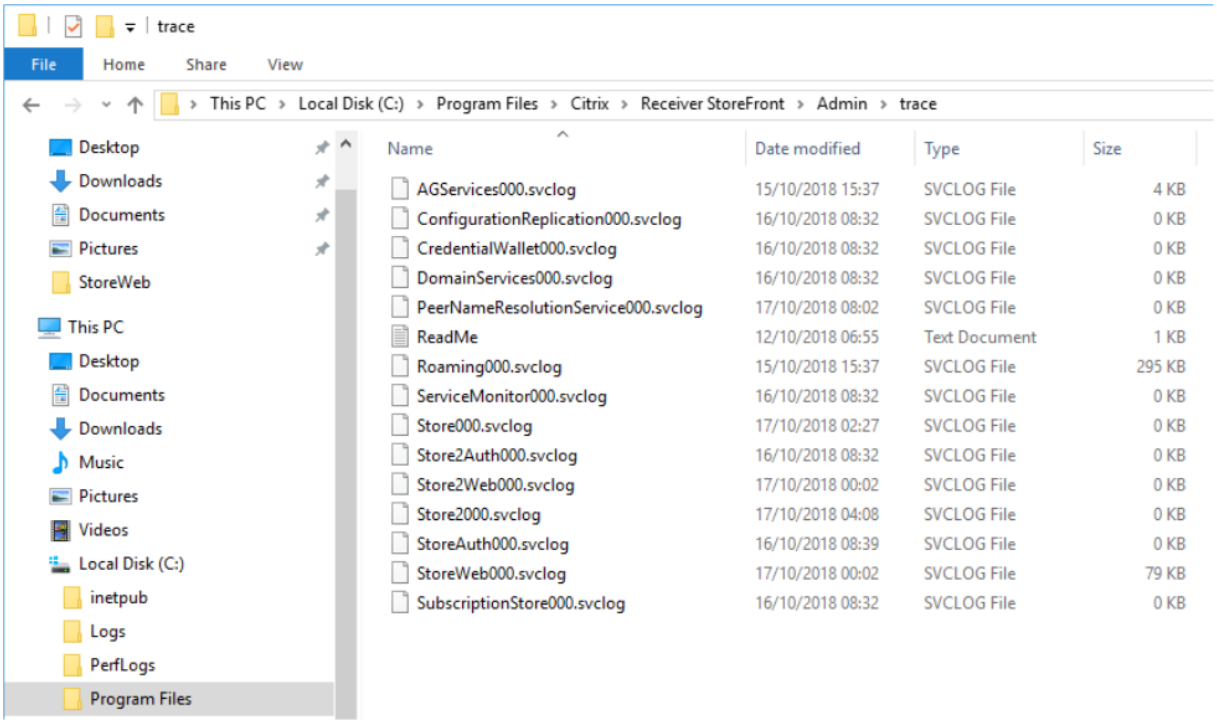
   Par défaut, StoreFront est configuré pour limiter le nombre de doublons d'entrées du journal à 10 par minute.
3. Modifiez la valeur de l'attribut duplicateInterval sur la durée définie en heures, minutes et secondes pendant laquelle les doublons d'entrées du journal seront analysés. Utilisez l'attribut 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 (Détaillé). 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 SDK PowerShell StoreFront.

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 les deux valeurs de clé de chaîne suivantes :

   - LogFile ="chemin vers le fichier journal"
   - LogICAFile=true

   Par exemple :

   ```
   1 LogFile=C:\ica\ica.log
   2 LogICAFile=true
   ```


Ressources supplémentaires

> Remarque :
>
> L'utilisation d'un fichier ICA dans votre environnement pour autre chose qu'un dépannage est abordée dans l'article CTX200126.

Résolution des problèmes de mise à niveau de StoreFront

Suivez les étapes suivantes pour résoudre les problèmes de mise à niveau de StoreFront.

Avant de tenter une mise à niveau

1. Vérifiez que vous disposez d'une sauvegarde de tous les serveurs StoreFront.
2. Vérifiez que vous ne tentez pas de mise à niveau à partir d'une version StoreFront en fin de vie. Pour plus d'informations, consultez CTX200356.
3. Vérifiez que vous effectuez une mise à niveau d'une version prise en charge de StoreFront vers la version actuelle uniquement.
4. Si le serveur StoreFront fait partie d'un groupe de serveurs StoreFront, tous les serveurs du groupe doivent être mis à niveau séquentiellement. La mise à niveau simultanée d'un groupe de serveurs StoreFront n'est pas prise en charge.
5. Supprimez tous les fichiers *thumbs.db* à l'intérieur de *C:\inetpub\wwwroot\citrix* ou de ses sous-répertoires. Affichez les fichiers cachés pour terminer cette étape : dans **Options des dossiers > Afficher**, sélectionnez l'option **Afficher les fichiers, dossiers et lecteurs cachés**et désactivez l'option **Masquer les fichiers protégés du système d'exploitation (recommandé)**.
6. Désactivez le logiciel antivirus avant de démarrer la procédure de mise à niveau.
7. Vérifiez que les serveurs en cours de mise à niveau sont supprimés de tout programme d'équilibreur de charge et qu'aucune session utilisateur active n'est connectée.
8. Redémarrez le serveur StoreFront avant d'effectuer la mise à niveau.
9. Arrêtez manuellement les services suivants :
    - CitrixConfigurationReplication
    - CitrixCredentialWallet
    - CitrixDefaultDomainService
    - CitrixPeerResolutionService
    - CitrixSubscriptionsStore
10. Assurez-vous que la console de gestion StoreFront est fermée.

Si la mise à niveau échoue

1. Dans *C:\Windows\Temp\StoreFront*, ouvrez le fichier *CitrixMsi*.log* le plus récent et recherchez les erreurs d'exception.

   Exceptions de type **Thumbs.db Access** : provoquées par des fichiers *thumbs.db* dans *C:\inetpup\wwwroot\citrix* ou dans ses sous-répertoires. Supprimez tous les fichiers *thumbs.db* trouvés.

   Exceptions de type **Cannot get exclusive file access \in use** : si l'instantané ou la sauvegarde est disponible, restaurez-le/la, ou redémarrez le serveur et arrêtez manuellement tous les services StoreFront.

   Exceptions de type **Service cannot be started** : si l'instantané ou la sauvegarde est disponible, restaurez-le/la, ou installez la version complète de .NET Framework 4.5 (pas le profil client).

2. Si aucune erreur d'exception se trouve dans *CitrixMsi*.log*, vérifiez l'**Observateur d'événements > Delivery Services** du serveur pour toute erreur contenant les messages d'erreur d'exception précédents. Suivez les instructions correspondantes.

3. Si aucune erreur d'exception se trouve dans l'Observateur d'événements, vérifiez les journaux d'administration dans *C:\Program Files\Citrix\Receiver StoreFront\logs* pour toute erreur contenant les messages d'erreur d'exception précédents. Suivez les instructions correspondantes.

Pour supprimer manuellement StoreFront

> Avertissement :
>
> La suppression manuelle de StoreFront efface toutes les informations existantes.

Pour supprimer manuellement StoreFront :

1. Désinstallez StoreFront.
2. Supprimez le rôle serveur Web.
3. Supprimez le dossier *C:\Program Files\Citrix\Receiver StoreFront*.
4. Supprimez tous les sous-répertoires sous *C:\Program Files\Citrix\StoreFront Install*.
5. Supprimez le dossier *C:\Inetpub*.

Vous pouvez maintenant réinstaller StoreFront.

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