StoreFront 2402

Contents

Vue d'ensemble

February 22, 2024

StoreFront est un magasin d'applications d'entreprise qui regroupe les applications et les bureaux des sites Citrix Virtual Apps and Desktops et Citrix DaaS en un seul magasin facile à utiliser pour les utilisateurs.

Dans StoreFront, vous pouvez configurer un ou plusieurs magasins. Chaque magasin possède sa propre configuration, notamment :

- Liste des flux de ressources que StoreFront interroge pour énumérer les applications et les bureaux disponibles pour l'utilisateur
- Apparence du site Web utilisé pour accéder au magasin.
- Méthodes d'authentification utilisées par les utilisateurs pour se connecter.
- Accès externe via une passerelle NetScaler.

Les utilisateurs peuvent utiliser l'application Citrix Workspace installée localement ou l'application Citrix Workspace pour HTML5 dans un navigateur Web pour accéder aux magasins StoreFront. Pour plus d'informations, veuillez consulter la section Options d'accès utilisateur.

Pour commencer, planifiez votre déploiement de StoreFront, consultez la configuration requise et installez StoreFront.

Nouveautés

Consultez la section Nouveautés.

Versions précédentes

La documentation pour les autres versions actuellement disponibles se trouve ici.

Pour connaître les étapes à suivre pour effectuer une mise à niveau depuis une version antérieure, consultez la section Mise à niveau.

Cycle de vie du support

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

Nouveautés

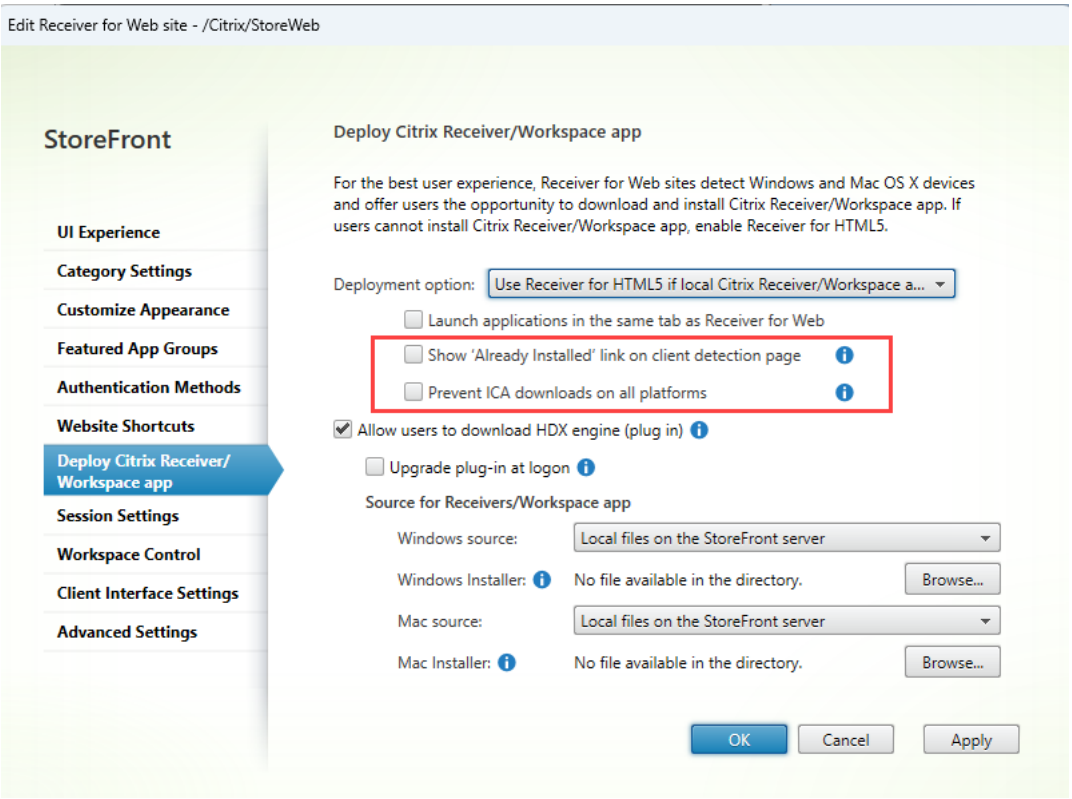
May 30, 2024

2402

Téléchargement de fichiers .ica empêché lors du lancement hybride

Afin de minimiser les risques de sécurité découlant du téléchargement de fichiers .ica sur des systèmes locaux, les paramètres suivants ont été introduits. Les administrateurs peuvent configurer ces paramètres depuis la console d'administration StoreFront à titre de mesure préventive contre l'utilisation abusive des fichiers .ica téléchargés.
Ces paramètres comprennent :

- Afficher le lien **Déjà installé** sur la page de détection des clients
- Empêcher les téléchargements de fichiers ICA sur toutes les plateformes



Pour plus d'informations, consultez Empêcher le téléchargement de fichiers ICA.

Activez la nouvelle interface utilisateur à l'aide d'une commande PowerShell Les administrateurs peuvent activer la nouvelle interface utilisateur à l'aide de la commande PowerShell `Set-STFWebReceiverService`.

Par exemple :

```
$rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperence
   Workspace

<!--NeedCopy-->
```

pour plus d'informations sur la nouvelle interface utilisateur, consultez Nouvelle interface utilisateur

Activer la vérification de l'intégrité pour tous les magasins La vérification de l'intégrité est désormais activée pour tous les magasins existants afin d'améliorer leur résilience. Grâce aux vérifications de l'intégrité avancées, StoreFront peut détecter de manière plus fiable tout problème dans le composant Delivery Controller.
Lorsqu'elles sont utilisées conjointement avec Citrix Desktops as a Service, les vérifications de l'intégrité avancées fournissent des informations supplémentaires sur les connecteurs présents dans les emplacements de ressources. Ceci est utile en cas de panne. Lorsqu'un utilisateur lance une ressource, un connecteur approprié pour lancer la ressource est automatiquement sélectionné à l'aide du cache d'hôte local.

Si vous souhaitez désactiver la vérification de l'intégrité avancée pour tous les magasins, vous pouvez utiliser le script PowerShell suivant :

```
foreach ($store in Get-STFStoreService)
{

    Set-STFStoreFarmConfiguration -StoreService $store -
       AdvancedHealthCheck $False
 }

<!--NeedCopy-->
```

> **Remarque :**
>
> À partir de la version 2308 CR de StoreFront, la vérification de l'intégrité avancée a été activée par défaut pour les nouveaux magasins.

Annonce de fin de prise en charge de Windows Server 2016

La prise en charge de l'installation de StoreFront sur Windows Server 2016 ne sera plus disponible dans la prochaine version. Afin de bénéficier d'une prise en charge continue, nous vous recomman-

dons d'effectuer une mise à niveau avec une version plus récente de Windows Server. Pour de plus amples informations sur les éléments obsolètes, consultez la section Avis de fin de prise en charge.

Problèmes résolus

- Si vous définissez les paramètres de marque par défaut sur la nouvelle interface utilisateur (version Technical Preview), l'ancienne palette de couleurs par défaut de l'interface utilisateur est appliquée. [WSUI-8930]
- L'énumération des applications sur les serveurs StoreFront peut échouer par intermittence. [CVADHELP-23196]
- Les opérations du Gestionnaire d'activités telles que Fermer la session, Déconnecter, etc. ne sont pas prises en charge pour les applications pour lesquelles des stratégies App Protection sont activées. [WSP-21324]
- Le paramètre powershell `-override` est requis pour modifier les paramètres de journalisation des diagnostics. [WSP-22214]
- Les noms contenant des caractères spéciaux peuvent apparaître endommagés dans le menu déroulant Paramètres. [WSP-22210]
- La première fois qu'un utilisateur ouvre le site Web d'un magasin dans son navigateur sur ChromeOS, il est invité à effectuer une détection du client, mais l'application Citrix Workspace pour ChromeOS ne prend pas en charge cette fonctionnalité. Par conséquent, la détection du client échoue et les utilisateurs doivent cliquer sur « déjà installé » pour continuer. Grâce à ce correctif, le site Web ignore la détection du client sur ChromeOS. [WSP-22390]
- Dans la version 2311 de StoreFront, les stratégies configurées dans Studio qui ne doivent s'appliquer qu'aux utilisateurs se connectant via une passerelle s'appliquent également aux utilisateurs internes. [WSP-22766]

Problèmes connus

Il n'existe aucun nouveau problème connu dans cette version.

2311

Citrix Secure Private Access sur StoreFront

Vous pouvez désormais vous connecter au serveur local Citrix Secure Private Access à l'aide des nouvelles commandes PowerShell ou des commandes de l'interface utilisateur d'administration de StoreFront. Il permet aux utilisateurs d'accéder en toute sécurité aux applications Web et SaaS via Store-

Front.
Pour plus d'informations, consultez la section Gérer les ressources mises à disposition dans les magasins.

Lancement ininterrompu du VDA en cas d'indisponibilité du serveur FAS

Vous pouvez désormais configurer StoreFront pour que le lancement du VDA soit réussi même si le serveur FAS n'est pas disponible. Dans ce cas, les utilisateurs finaux peuvent se connecter à l'aide de leur nom d'utilisateur et de leur mot de passe. Auparavant, le lancement du VDA échouait si les serveurs FAS étaient inaccessibles.
Cette fonctionnalité est désactivée par défaut et peut être activée à l'aide de la commande Powershell suivante.

`Set-STFStoreLaunchOptions` avec le paramètre `FederatedAuthenticationServiceFailover`

Vous pouvez utiliser la même commande pour désactiver cette fonctionnalité, si nécessaire.
Pour plus d'informations, consultez FAS.

Journaux améliorés de l'expérience utilisateur

Auparavant, par défaut, seules les erreurs étaient enregistrées. Le niveau de journalisation par défaut a été modifié pour inclure les avertissements et les informations de suivi. De plus, les messages de journal ont été améliorés. Cela garantit par défaut que tous les événements qui font partie de l'expérience utilisateur sont désormais enregistrés. La taille du fichier journal par défaut est augmentée à 1 Go (5*200 Mo) pour chaque service. Cela nécessite généralement 1 Go (pour le service d'itinérance) + 3 Go par magasin (car chaque service de magasin dispose généralement d'un service d'authentification et d'un service Receiver pour Web correspondants). Assurez-vous de disposer d'un espace disque suffisant. Pour plus d'informations, consultez la section Enregistrement des diagnostics.

Extensions Web Citrix Workspace –Disponibilité générale

Les extensions Web Citrix Workspace sont désormais généralement disponibles pour une utilisation avec StoreFront. Ces extensions Web vous permettent de lancer des ressources dans votre application Citrix Workspace installée localement sans être invité à ouvrir le lanceur Workspace ou à télécharger un fichier `.ica`, ce qui rend votre expérience plus sûre et plus fiable. Pour plus d'informations, consultez la section Extensions Web Citrix.

L'utilisation des extensions Web de Citrix Workspace est activée par défaut pour chaque nouvelle installation de StoreFront. Cependant, les utilisateurs finaux doivent toujours télécharger les extensions pour utiliser cette fonctionnalité.

> **Remarque :**
>
> L'extension Web Citrix Workspace n'est pas activée automatiquement lors d'une mise à niveau de la version de StoreFront. Si cette fonctionnalité a été désactivée avant la mise à niveau, elle reste inchangée après la mise à jour de la version. Elle sera activée pour tous les déploiements dans une prochaine version.

Lors de la mise à niveau d'un déploiement, vous pouvez activer cette fonctionnalité à l'aide de la commande suivante :

```
Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension "
-IsEnabled $True
```

Nouvelle interface utilisateur pour les magasins locaux (Technical Preview)

La nouvelle interface utilisateur est désormais disponible pour les magasins locaux. Cette interface utilisateur, qui n'était auparavant disponible que pour les magasins cloud, garantit une apparence cohérente entre les magasins cloud et locaux.

La nouvelle interface utilisateur apporte les améliorations clés suivantes :

- **Interface utilisateur conviviale** : Réduit la complexité visuelle et permet d'accéder facilement aux fonctionnalités essentielles. Pour plus d'informations, consultez la section Apparence et disposition de Workspace améliorées.
- **Gestionnaire d'activités** : permet d'effectuer des actions rapides sur les applications et les bureaux virtuels actifs, et ainsi d'économiser des ressources et d'optimiser les performances. Pour plus d'informations, consultez Gestionnaire d'activités.
- **Catégorisation améliorée des applications** : structure de dossiers à plusieurs niveaux qui s'adapte à la taille de l'écran de votre utilisateur final. Pour plus d'informations, consultez la section Catégorisation des applications.
- **Capacités de recherche améliorées** : les nouvelles fonctionnalités de recherche permettent d'obtenir de meilleurs résultats, plus rapidement. Pour plus d'informations, consultez la section Options de recherche.

Pour plus d'informations sur cet aperçu, consultez la section Nouvelle interface utilisateur (Tech Preview).

> **Remarque :**
>
> Vous pouvez nous faire part de vos commentaires sur cette fonctionnalité via le formulaire Podio.

Application Citrix Workspace pour HTML5

Cette version inclut l'application Citrix Workspace pour HTML5 2402.

Problèmes résolus

- L'application Citrix Workspace pour Mac peut se bloquer lorsque vous sortez du mode veille lorsque vous êtes connecté à un magasin StoreFront. [CVADHELP-23217]
- Une situation de concurrence peut entraîner la fermeture inattendue du service Citrix Subscriptions Store sur le serveur StoreFront avec des messages d'avertissement. [CVADHELP-23326]

Problèmes connus

- Les noms d'utilisateur comportant des caractères spéciaux peuvent apparaître endommagés dans le menu déroulant **Paramètres**. [WSP-22210]
- Le paramètre PowerShell `-override` est obligatoire pour modifier les paramètres TraceLevel. [WSP-22214]
- Dans la version 2311 de StoreFront, les stratégies configurées dans Studio qui ne doivent s'appliquer qu'aux utilisateurs se connectant via une passerelle s'appliquent également aux utilisateurs internes. [WSP-22766]

2308.1

Problèmes résolus

- Cette version corrige une vulnérabilité de sécurité dans un composant sous-jacent. Pour obtenir davantage d'informations, veuillez consulter l'article CTX583759. [CVADHELP-23724]

2308

App Protection pour les lancements hybrides

La protection des applications fournit un niveau de sécurité supplémentaire en bloquant l'enregistrement de frappe et la capture d'écran. Auparavant, cette fonctionnalité n'était disponible que lors de l'accès à un magasin via les applications Citrix Workspace pour Windows, Mac et Linux. Lorsque vous consultiez un magasin via un navigateur Web, les applications protégées ne s'affichaient pas. Avec cette version, il est désormais possible de configurer le site Web d'un magasin pour afficher les applications nécessitant une protection des applications lorsqu'elles sont consultées via un navigateur, à condition que StoreFront ait détecté que l'utilisateur possède une version suffisamment récente de l'application Citrix Workspace pour Windows, Mac ou Linux installée pour lancer l'application.

Pour plus d'informations, consultez Protection des applications.

Contrôle d'intégrité avancé activé par défaut

À partir de cette version, la fonctionnalité de vérification avancée de l'intégrité est activée par défaut pour les nouveaux magasins. Auparavant, elle devait être activée manuellement.

Lorsqu'il est utilisé avec Citrix DaaS, le contrôle d'intégrité avancé permet à StoreFront de détecter les connecteurs présents aux emplacements des ressources. En cas de panne, lorsqu'un utilisateur lance une ressource, StoreFront choisit un connecteur approprié pour lancer la ressource à l'aide du cache d'hôte local.

Problèmes résolus

Cette version inclut tous les correctifs de 2203 CU3, ainsi que les correctifs suivants :

- [CVADHELP-22435] Un an après avoir détecté que l'application Citrix Workspace est installée sur la machine utilisateur, les applications sont lancées dans un navigateur plutôt que dans l'application Citrix Workspace.
- [CVADHELP-21886] Lorsque vous utilisez l'API du service StoreFront pour lancer une application, que vous remplacez des paramètres tels que la qualité audio et que vous désactivez des imprimantes, les paramètres peuvent être appliqués à toutes les demandes suivantes plutôt qu'uniquement à la demande en cours.

Fin de prise en charge de XenApp Services

À partir de cette version, les adresses URL XenApp Services (également connu sous le nom de PNAgent) pour la connexion aux magasins ne sont plus prises en charge, Ce service sera supprimé dans une prochaine version. Utilisez l'application Citrix Workspace pour vous connecter aux magasins à l'aide de l'URL du magasin.

Suppression de la possibilité d'ajout de Delivery Controller XenApp 6.5

Il n'est plus possible d'ajouter de nouveaux flux de ressources XenApp 6.5 à l'aide de la console de gestion StoreFront. Il est toujours possible de les ajouter à l'aide de PowerShell Add-STFStoreFarm en spécifiant le paramètre « FarmType » comme XenApp. Par exemple :

```
1 $store = Get-STFStoreService
2 Add-STFStoreFarm -StoreService $store -FarmName "XenApp" -FarmType
     XenApp -Port 80 -TransportType HTTP -Servers Xen1
3 <!--NeedCopy-->
```

Les flux de ressources XenApp 6.5 existants peuvent être modifiés à l'aide de la console de gestion.

> **Remarque :**
>
> XenApp 6.5 n'est pas pris en charge par Citrix. La possibilité d'utilisation des Delivery Controller XenApp 6.5 sera supprimée dans une future version.

Suppression de la possibilité d'ouverture de ressources dans Internet Explorer 11

Il n'est plus possible d'ouvrir des ressources dans le navigateur Web Internet Explorer 11. Il est toujours possible d'accéder à votre magasin depuis Internet Explorer 11, mais vous devez installer l'application Citrix Workspace pour Windows pour pouvoir lancer des ressources.

Problèmes connus

Il n'existe aucun nouveau problème connu dans cette version.

Nouvelle interface utilisateur pour les magasins locaux (Technical Preview)

May 30, 2024

La nouvelle interface utilisateur est désormais disponible pour les magasins locaux. Cette interface utilisateur, qui n'était auparavant disponible que pour les magasins cloud, garantit une apparence cohérente entre les magasins cloud et locaux.

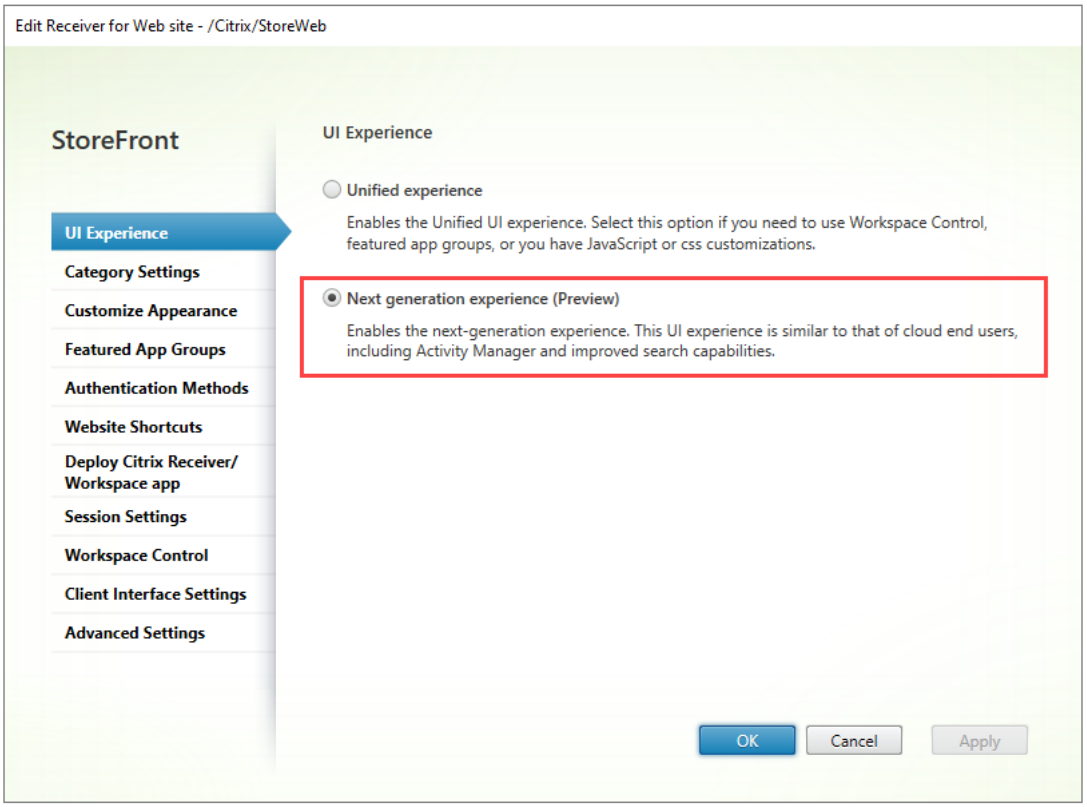
La nouvelle interface utilisateur est conçue pour améliorer et simplifier l'expérience de l'utilisateur final lors de l'accès aux applications et bureaux Citrix. Elle réduit la complexité visuelle, facilite l'accès aux fonctionnalités essentielles et optimise l'expérience de l'application StoreFront. Elle prend en charge de nouvelles fonctionnalités, telles que le Gestionnaire d'activités qui optimise la gestion de vos applications virtuelles et de vos ressources de bureau.

> **Remarque :**
>
> Dans cet article, l'expérience d'interface utilisateur actuelle est appelée expérience d'interface utilisateur unifiée.

Activer la nouvelle expérience d'interface utilisateur pour les magasins locaux

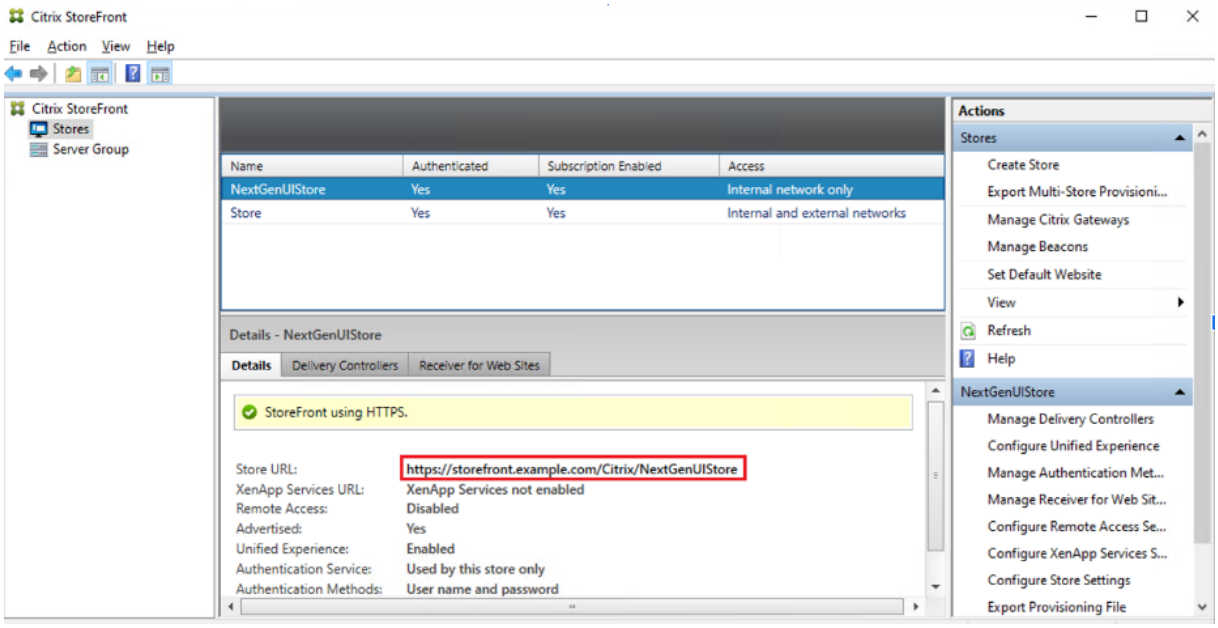
Cette fonctionnalité étant actuellement en version préliminaire, il est recommandé de créer un nouveau magasin, puis d'activer la nouvelle interface utilisateur pour ce magasin en particulier.

Une fois que vous avez créé le magasin, vous devez activer la nouvelle interface utilisateur en sélectionnant **Expérience de nouvelle génération** sur la page de configuration du site Web. L'activation de la nouvelle interface utilisateur pour un nouveau magasin vous permet de tester l'interface utilisateur avec un nombre limité d'utilisateurs.

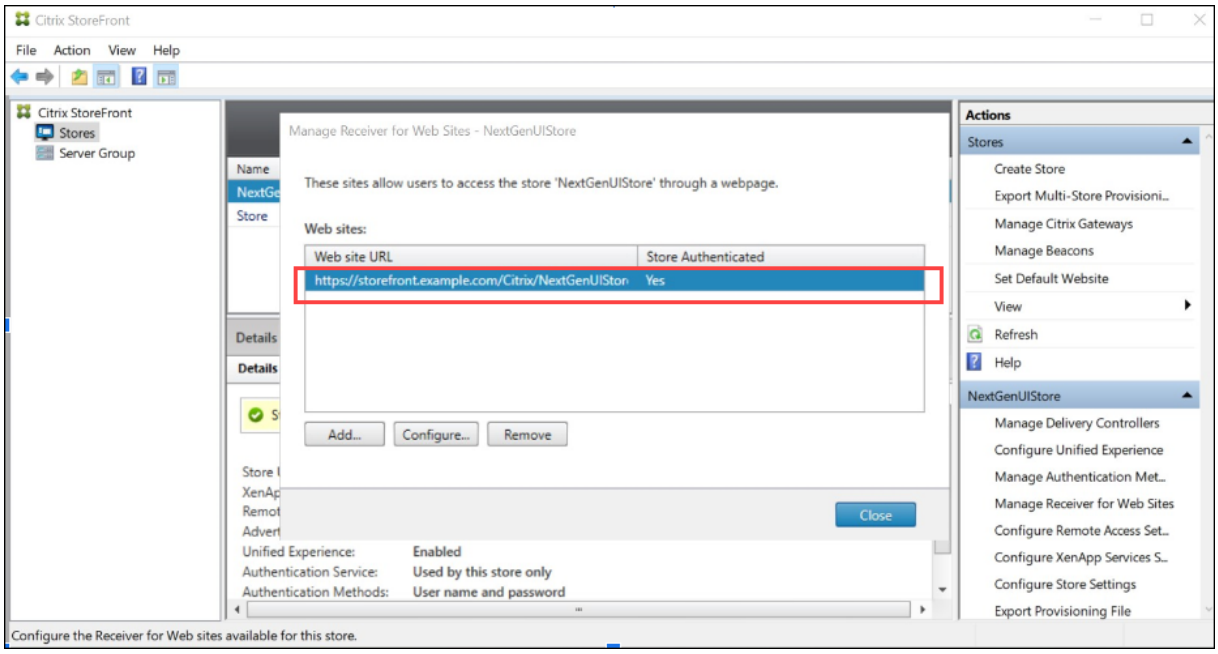


Une fois que vous avez créé un magasin avec la nouvelle interface utilisateur activée, vous devez partager le site Web ou le lien vers le magasin avec vos utilisateurs finaux.

- Si vos utilisateurs finaux utilisent l'application native, vous devez partager le lien vers le nouveau magasin avec eux.



- Si vos utilisateurs finaux sont connectés via un navigateur, vous devez partager le lien vers le nouveau site Web avec eux.



Activez la nouvelle interface utilisateur à l'aide d'une commande PowerShell

Les administrateurs peuvent activer la nouvelle interface utilisateur à l'aide de la commande PowerShell `Set-STFWebReceiverService`.

Par exemple :


```
$rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperence
    Workspace

<!--NeedCopy-->
```

Personnaliser le thème et le logo

Vous pouvez personnaliser le thème et le logo de votre magasin présentant la nouvelle interface utilisateur. Vous pouvez gérer ces paramètres dans l'onglet **Personnaliser l'apparence** sous **Gérer votre site Web**. Pour plus d'informations sur la configuration d'un thème et d'un logo, consultez la section Personnaliser l'apparence.

Principaux avantages

La nouvelle interface utilisateur apporte les améliorations clés suivantes :

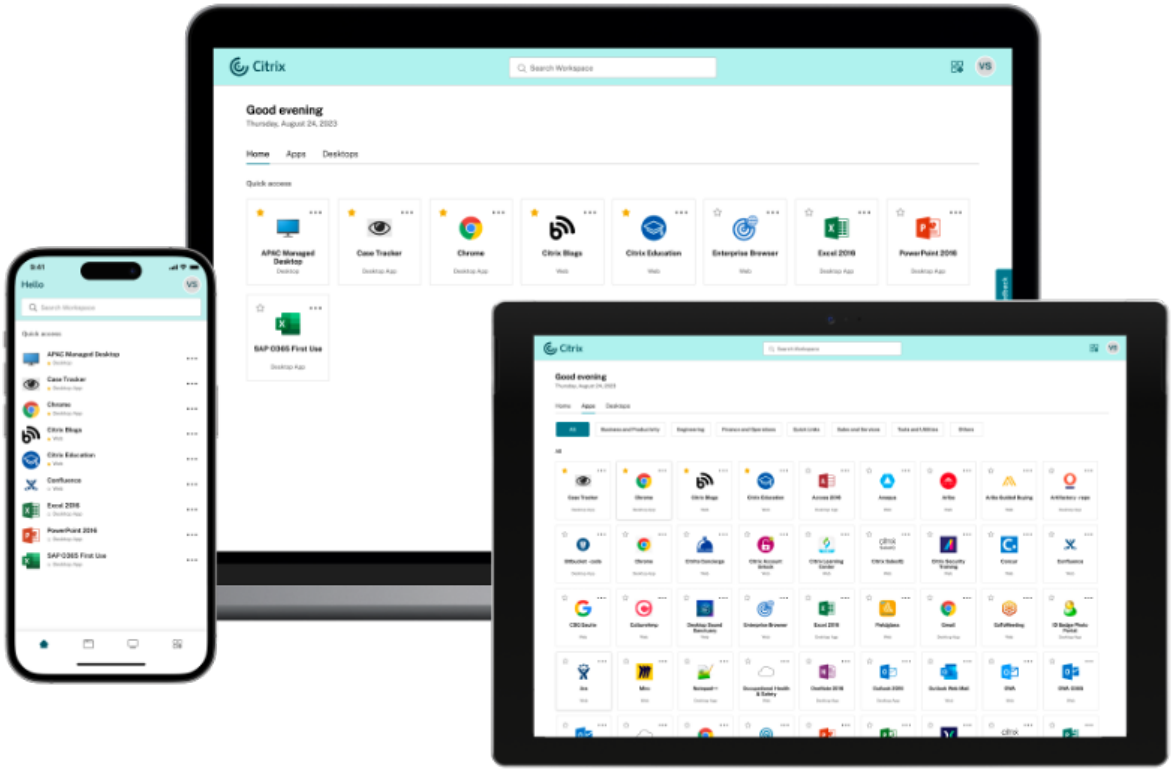
- **Interface utilisateur conviviale** : Réduit la complexité visuelle et permet d'accéder facilement aux fonctionnalités essentielles. Pour plus d'informations, consultez la section Apparence et disposition de Workspace améliorées.
- **Gestionnaire d'activités** : permet d'effectuer des actions rapides sur les applications et les bureaux virtuels actifs, et ainsi d'économiser des ressources et d'optimiser les performances. Pour plus d'informations, consultez Gestionnaire d'activités.
- **Catégorisation améliorée des applications** : structures de dossiers à plusieurs niveaux qui s'adaptent à la taille de l'écran de l'utilisateur. Pour plus d'informations, consultez la section Catégorisation des applications.
- **Capacités de recherche améliorées** : les nouvelles fonctionnalités de recherche permettent d'obtenir de meilleurs résultats, plus rapidement. Pour plus d'informations, consultez la section Options de recherche.

Apparence et disposition de Workspace améliorées

La nouvelle expérience utilisateur est conçue pour fournir une expérience intuitive et simplifiée. Les applications et les bureaux ont été organisés sur les pages **Accueil**, **Applications** et **Bureaux** pour faciliter la navigation. Les applications et les bureaux marqués comme favoris sont placés au début de la liste pour en faciliter l'accès.

Si vos utilisateurs possèdent moins de 20 applications, une vue simple leur est présentée, sans onglets ni catégories. Toutes les applications et tous les bureaux sont affichés sur la même page. Les applications marquées comme favorites sont placées au début de la liste, suivies des autres applications, dans l'ordre alphabétique.

Les utilisateurs finaux peuvent marquer n'importe quelle application ou n'importe quel bureau comme favori en cliquant sur l'icône en forme d'étoile correspondante. De même, ils peuvent retirer une application ou un bureau des favoris en cliquant sur l'icône en forme d'étoile correspondante.



Si vos utilisateurs possèdent plus de 20 applications, ils accèdent à la page **Accueil** une fois connectés. Les applications et bureaux favoris et les cinq applications et bureaux les plus récemment utilisés sont accessibles depuis la page **Accueil**. Les applications et les bureaux mandatés par les administrateurs sont indiqués par une icône en forme d'étoile. Les utilisateurs finaux ne peuvent pas supprimer ces applications et bureaux de la liste des favoris.

Si l'administrateur n'a pas encore activé la page d'accueil, les utilisateurs accèdent à la page **Applications**. Sur cette page également, les applications favorites sont répertoriées en premier, suivies de toutes les autres applications, par ordre alphabétique. Si l'administrateur a créé des catégories d'applications, les utilisateurs peuvent cliquer sur les catégories pour localiser leurs applications.

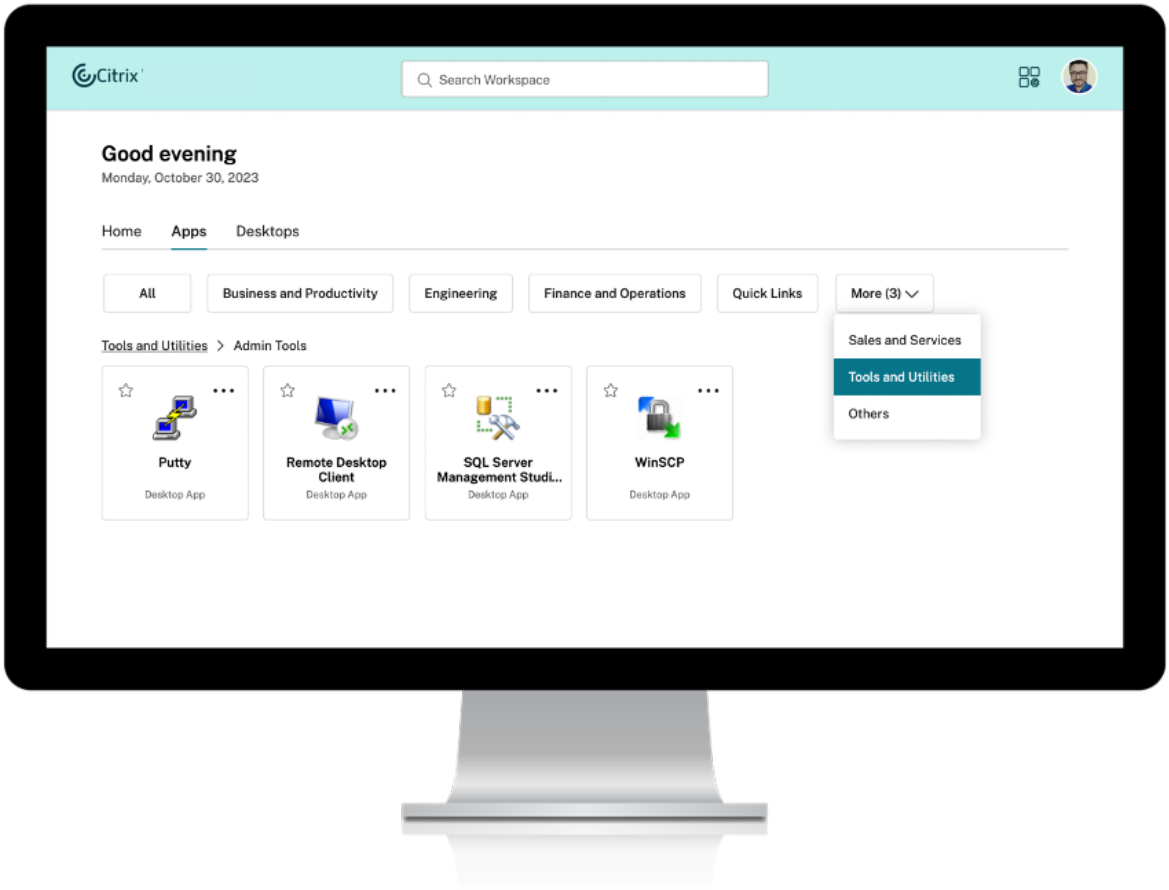
Catégorisation des applications sur la nouvelle interface utilisateur

Sur la nouvelle interface utilisateur, les utilisateurs finaux peuvent afficher leurs applications organisées en catégories et sous-catégories. Les sous-catégories apparaissent dans une structure de dossiers. La structure organisée en plusieurs niveaux permet une expérience optimisée et sans encombrement qui contribue à améliorer la satisfaction globale des utilisateurs. Pour plus d'

informations sur la création de dossiers et de sous-dossiers, consultez la section Paramètres de catégorie.

Lorsque le nombre de catégories principales créées par les administrateurs dépasse l'espace disponible sur l'écran de l'utilisateur, l'interface utilisateur s'ajuste en fonction de la taille de l'écran et déplace les catégories de manière dynamique dans le **menu déroulant Plus**. Les fils de navigation sont également visibles par les utilisateurs.

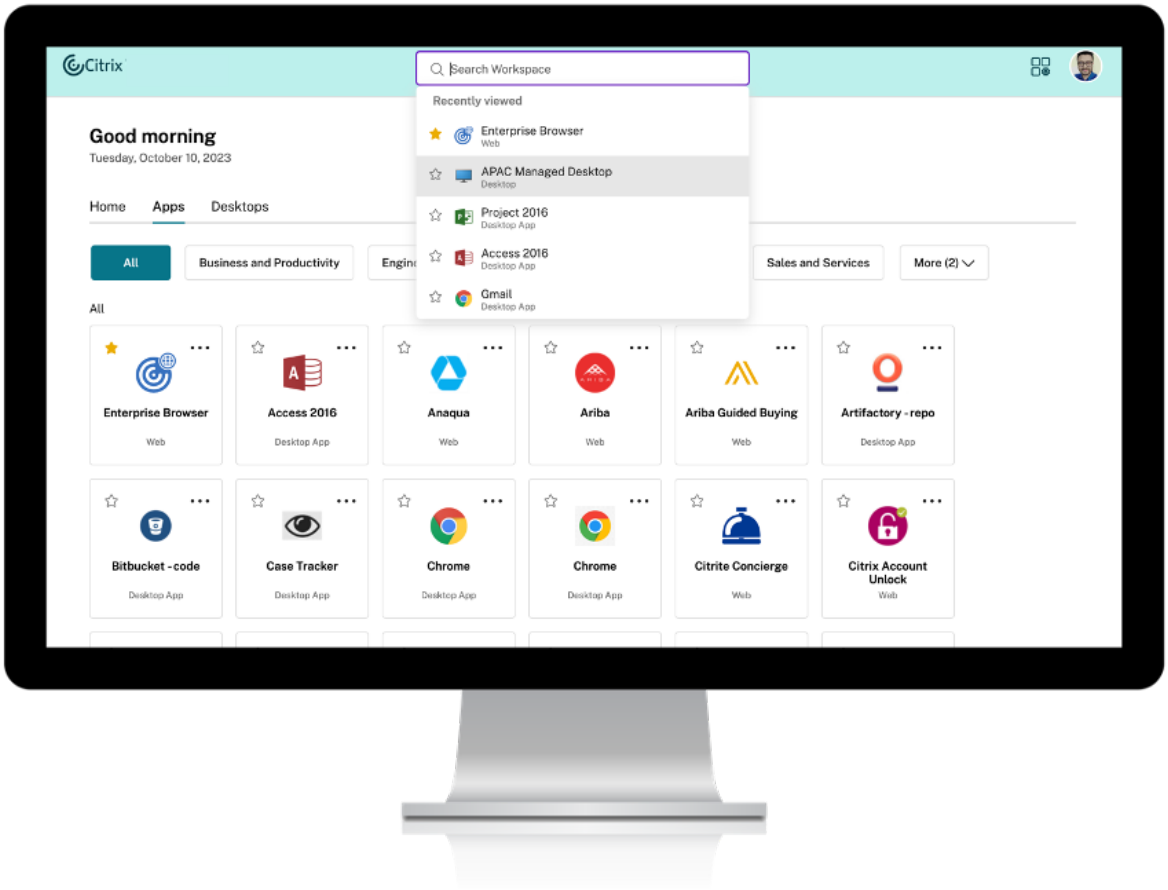
Sur les plates-formes mobiles, accédez à l'onglet **Applications** et cliquez sur le menu déroulant **Catégories** pour afficher la liste des catégories disponibles. Les sous-catégories apparaissent sous forme de dossiers. Les sous-dossiers peuvent contenir d'autres sous-dossiers ou applications selon la configuration effectuée par l'administrateur.



> **Remarque :**
>
> Dans l'interface utilisateur unifiée, les applications sont classées dans des dossiers. La hiérarchie des dossiers est visible sous forme de fils de navigation lorsque vous parcourez les applications ou les bureaux. Pour plus d'informations, consultez la section Paramètres de catégorie.

Options de recherche

La fonctionnalité de recherche de la nouvelle interface utilisateur constitue une amélioration par rapport à l'interface utilisateur unifiée. La fonction de recherche améliorée de la nouvelle interface utilisateur vous permet d'obtenir de meilleurs résultats grâce aux moteurs de recherche utilisant des mécanismes de recherche analogique. L'option Rechercher apparaît dans la barre d'outils pour une utilisation simplifiée et vous permet d'effectuer une recherche rapide et intuitive.



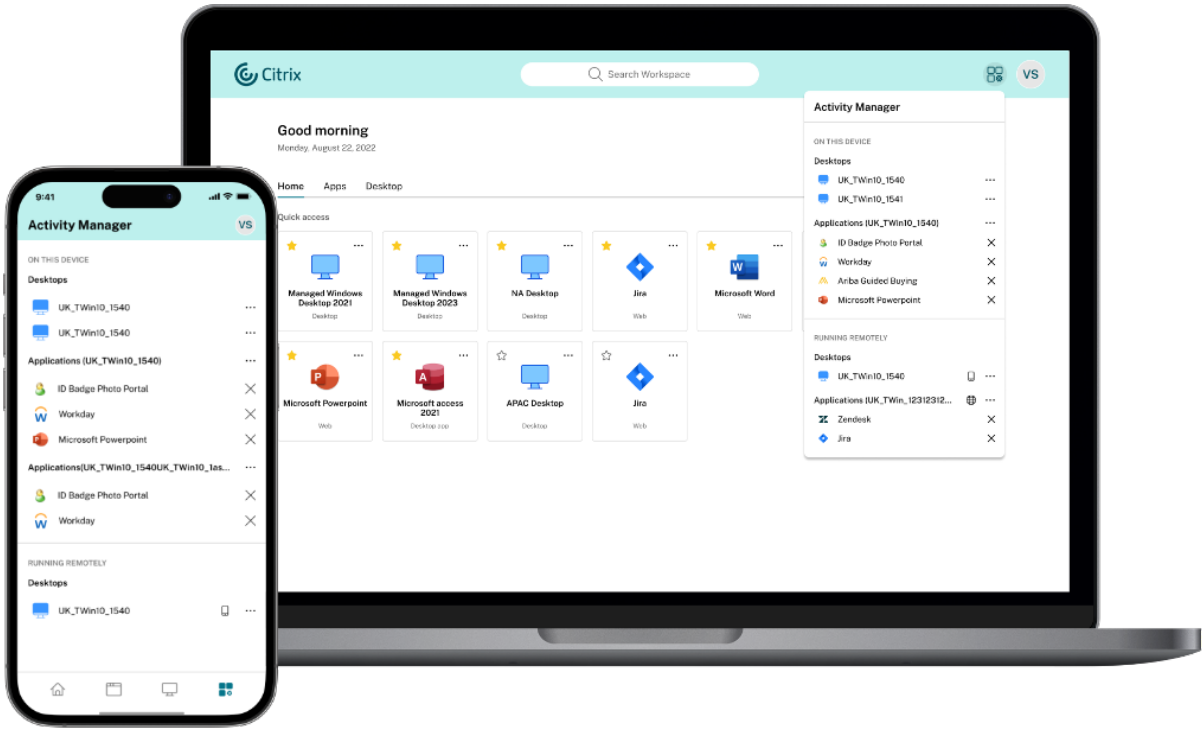
Les améliorations suivantes ont été apportées :

- La recherche par défaut affiche les cinq applications ou bureaux les plus récemment utilisés
- La vérification orthographique est activée pour les recherches et les résultats de la saisie automatique sont affichés
- Possibilité d'effectuer une recherche par catégories créées par l'administrateur
- Les favoris apparaissent en haut des résultats de la recherche
  L'interface utilisateur unifiée déploie des mécanismes de recherche de base qui peuvent ne pas être aussi efficaces que les fonctionnalités de recherche de la nouvelle interface utilisateur.

Gestionnaire d'activités

Le Gestionnaire d'activités est une fonctionnalité simple mais puissante de Citrix Workspace qui permet aux utilisateurs de gérer efficacement leurs ressources. Il améliore la productivité en facilitant des actions rapides sur les applications et les bureaux actifs depuis n'importe quel appareil. Les utilisateurs peuvent interagir de manière fluide avec leurs sessions, mettre fin ou déconnecter les sessions qui ne sont plus nécessaires, libérant ainsi des ressources et optimisant les performances.

Le panneau Gestionnaire d'activités affiche une liste consolidée des applications et des bureaux actifs non seulement sur l'appareil actuel, mais également sur tout appareil distant sur lequel des sessions sont actives. Les utilisateurs peuvent consulter cette liste en cliquant sur l'icône du Gestionnaire d'activités située à côté de l'icône de profil sur le bureau et en bas de leur écran sur les appareils mobiles.

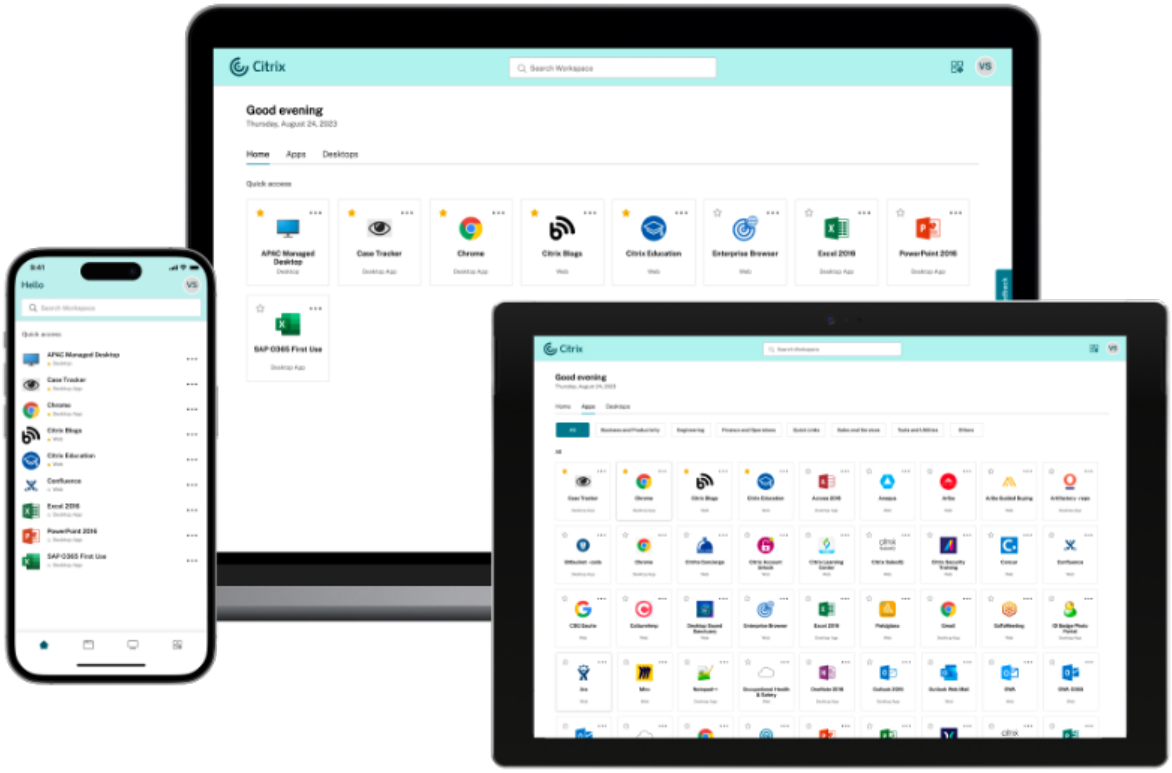


> **Important :**
>
> La fonctionnalité Gestionnaire d'activités n'est disponible que pour les magasins dans lesquels la nouvelle interface utilisateur est activée. Elle n'est pas disponible dans l'expérience d'interface utilisateur unifiée.

Utiliser le Gestionnaire d'activités

Les applications et les bureaux actifs sont regroupés comme suit dans le panneau Gestionnaire d'activités.

- Les applications et les bureaux actifs sur l'appareil actuel sont regroupés sous **Sur cet appareil**.
- Les applications et les bureaux actifs sur d'autres appareils sont regroupés sous **Exécuté à distance**.



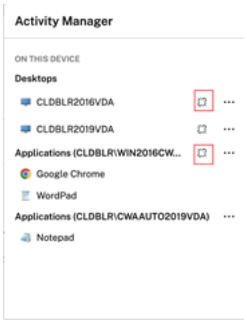
Les utilisateurs peuvent effectuer les actions suivantes sur une application ou un bureau en cliquant sur le bouton des points de suspension (…) correspondant.

- **Déconnecter** : la session à distance est déconnectée, mais les applications et les bureaux sont actifs en arrière-plan.
- **Fermer la session** : ferme la session en cours. Toutes les applications de la session sont fermées et tous les fichiers non enregistrés sont perdus.
- **Arrêter** : ferme les bureaux déconnectés.
- **Forcer la fermeture** : met hors tension votre bureau en cas de problème technique.
- **Redémarrer** : arrête le bureau et le redémarre.

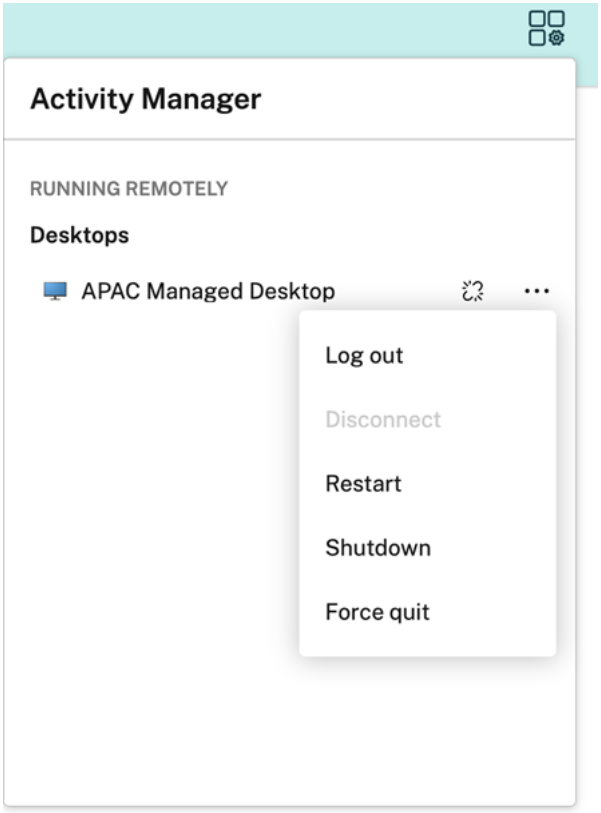
Applications et bureaux déconnectés

Le Gestionnaire d'activités permet désormais aux utilisateurs d'afficher les applications et les bureaux qui s'exécutent en mode déconnecté, localement ou à distance, et d'intervenir sur ceux-ci. Les sessions peuvent être gérées à partir d'appareils mobiles ou de bureau, ce qui permet aux utilisateurs

d'intervenir lorsqu'ils sont en déplacement. L'intervention sur les sessions déconnectées, telles que la fermeture de session ou l'arrêt, favorise une utilisation optimisée des ressources et réduit la consommation d'énergie.



- Les applications et les bureaux déconnectés sont affichés sur le panneau du Gestionnaire d'activités et sont marqués d'une icône de déconnexion.
- Les applications déconnectées sont regroupées sous les sessions respectives qui sont marquées d'une icône de déconnexion.



Les utilisateurs peuvent effectuer les actions suivantes sur leurs bureaux déconnectés en cliquant sur le bouton représentant des points de suspension :

- **Fermer la session** : utilisez cette option pour vous déconnecter de votre bureau déconnecté.

Toutes les applications de la session sont fermées et tous les fichiers non enregistrés sont perdus.

- **Arrêter** : utilisez cette option pour fermer vos bureaux déconnectés.
- **Forcer la fermeture** : utilisez cette option pour forcer la mise hors tension de vos bureaux déconnectés en cas de problème technique.
- **Redémarrer** : utilisez cette option pour arrêter et redémarrer le bureau déconnecté.

Le comportement des sessions déconnectées sur le Gestionnaire d'activités est différent comme suit.

- Si vous êtes connecté via un navigateur et que vous vous déconnectez d'une session locale, la session apparaît d'abord sous la section **Sur cet appareil**. Toutefois, une fois que vous fermez et rouvrez le Gestionnaire d'activités, la session déconnectée est déplacée sous la section **Exécuté à distance**.
- Si vous êtes connecté à un appareil natif et que vous vous déconnectez d'une session locale, la session déconnectée disparaît de la liste. Toutefois, une fois que vous fermez et rouvrez à nouveau le Gestionnaire d'activités, la session déconnectée est déplacée sous la section **Exécuté à distance**.

Limitations connues

La nouvelle interface utilisateur présente les limites suivantes. Ces fonctionnalités ne sont disponibles que dans l'interface utilisateur unifiée.

- La nouvelle interface utilisateur ne prend pas en charge la personnalisation approfondie à l'aide de l'API JavaScript et CSS.
- La nouvelle interface utilisateur ne prend pas en charge les raccourcis URL intégrés qui mènent directement à votre application ou à votre bureau.
- Actuellement, la fonctionnalité Contrôle de l'espace de travail, qui permet aux utilisateurs de se reconnecter à leurs sessions depuis un appareil distant, n'est pas prise en charge dans la nouvelle interface utilisateur.
- La fonctionnalité de changement de mot de passe n'est pas disponible sur la nouvelle interface utilisateur.
- Lesextensions Web de Citrix Workspace ne sont pas prises en charge. [WSUI-8503]
- L'authentification SAML directe n'est pas disponible si vous l'activez lors de la connexion à l'aide d'un navigateur Web. Vous pouvez toutefois utiliser l'authentification SAML avec Citrix Gateway.

Problèmes connus

- Lorsque vous modifiez l'interface utilisateur d'un magasin existant, les utilisateurs qui se connectent via l'application Citrix Workspace installée localement ne sont pas mis à jour. Ils doivent supprimer le magasin et le réintégrer à leur application. [WSP-21493]
- Les opérations du Gestionnaire d'activités telles que Fermer la session, Déconnecter, etc. ne sont pas prises en charge pour les applications pour lesquelles les stratégies App Protection sont activées. [WSP-21324]
- Sur l'application Citrix Workspace pour iOS, les initiales de l'utilisateur ne sont pas affichées sur l'avatar. [WSUI-8482]
- Dans les magasins Netscaler de l'application Citrix Workspace pour Mac, l'option **Retour à la connexion** risque de ne pas fonctionner. [RFMAC-15496]
- Dans les magasins Netscaler de l'application Citrix Workspace pour iOS, les utilisateurs ne pourront peut-être pas se connecter à la nouvelle interface utilisateur si l'accès privé sécurisé est activé avec des stratégies VPN sans client (cVPN). [RFIOS-13733]

Installer, configurer, mettre à niveau et désinstaller

January 25, 2024

Tâche	Détails
Planifier votre déploiement StoreFront	Aperçu des composants impliqués dans un déploiement de StoreFront
Options d'accès utilisateur	Aperçu des moyens par lesquels les utilisateurs peuvent accéder à vos magasins
Configuration système requise	Pour vous assurer de disposer des prérequis pour installer StoreFront
Installer StoreFront	Pour installer StoreFront sur un nouveau serveur
Sécurisation de StoreFront avec HTTPS	Pour chiffrer l'accès client à StoreFront à l'aide du protocole HTTPS
Sécuriser votre déploiement StoreFront	Pour configurer StoreFront avec une sécurité renforcée
Créer un nouveau déploiement	Pour configurer un nouveau serveur StoreFront avec un nouveau magasin
Joindre un groupe de serveurs existant	Pour configurer un nouveau serveur StoreFront pour rejoindre un groupe de serveurs existant

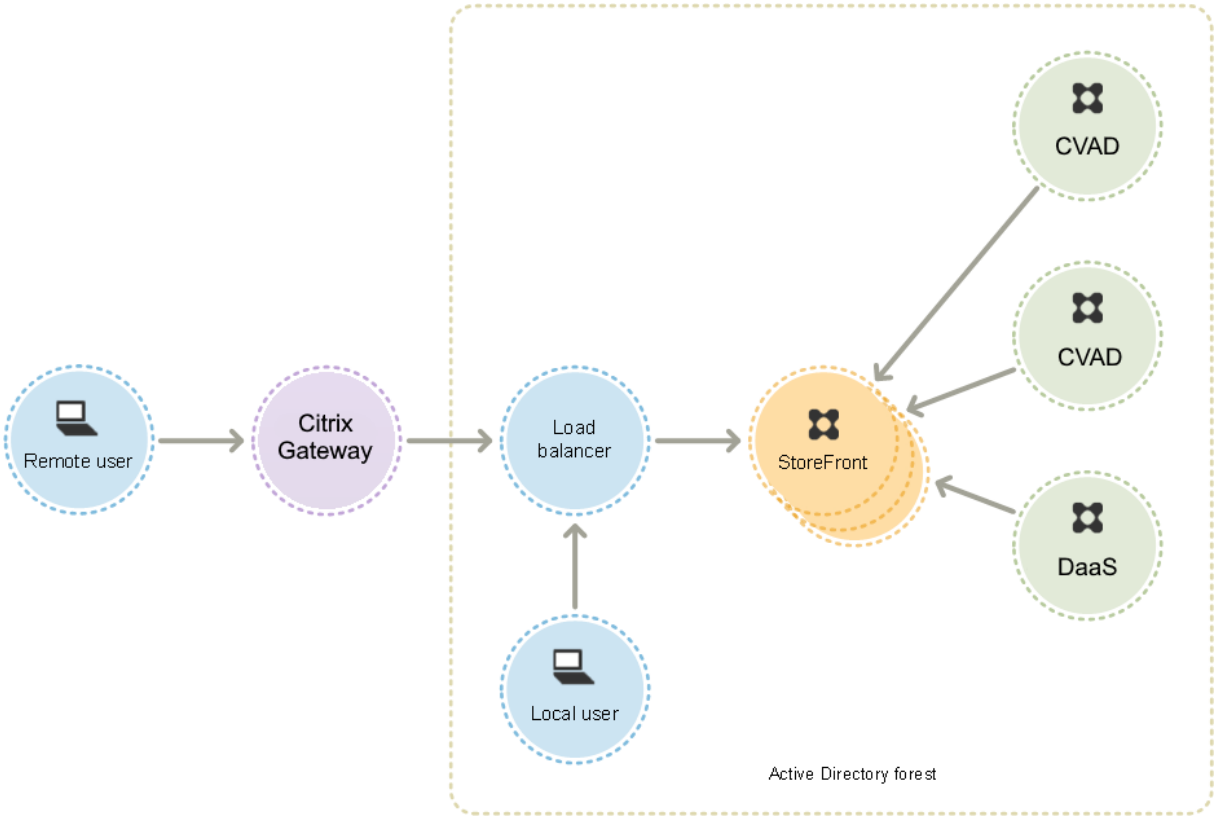
Tâche	Détails
Mettre à niveau StoreFront	Pour mettre à niveau un serveur StoreFront exécutant une ancienne version
CEIP	Participer ou non au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP)
Citrix Analytics Service	Pour configurer StoreFront pour envoyer des données au service Citrix Analytics
Désinstallez StoreFront	Pour supprimer StoreFront de votre serveur
Réinitialiser les paramètres d'usine du serveur	Pour effacer tous les paramètres de StoreFront afin de pouvoir le reconfigurer.

Planifier votre déploiement StoreFront

May 30, 2024

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.

La figure suivante présente un déploiement StoreFront classique.



Active Directory

StoreFront utilise Active Directory pour authentifier les utilisateurs, rechercher l'appartenance à un groupe et d'autres informations, ainsi que pour synchroniser les données entre les serveurs StoreFront.

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.

Groupe de serveurs StoreFront

StoreFront peut être configuré sur un serveur unique ou en tant que déploiement de plusieurs serveurs appelé groupe de serveurs StoreFront. Les groupes de serveurs fournissent non seulement une capacité supplémentaire, mais également une plus grande disponibilité. 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.

Citrix recommande un maximum de six serveurs par groupe de serveurs. Si vous utilisez plus de six serveurs, les coûts liés à la synchronisation des données l'emportent sur les avantages liés aux serveurs supplémentaires et les performances sont dégradées.

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.

Équilibrage de charge

Pour plusieurs serveurs d'un groupe de serveurs StoreFront, vous devez configurer l'équilibrage de charge externe. Utilisez un équilibreur de charge avec analyses et persistance de session intégrés, tel que NetScaler ADC. Pour plus d'informations sur l'équilibrage de la charge avec NetScaler ADC, consultez la section Équilibrage de charge.

Citrix Gateway pour l'accès distant

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.

Équilibrage de charge globale des serveurs

Dans les déploiements Citrix de grande taille, vous pouvez avoir des déploiements StoreFront et NetScaler dans plusieurs centres de données. À l'aide d'un équilibreur de charge de serveur global (GSLB), vous pouvez configurer une URL globale unique que le GSLB redirige vers l'URL spécifique d'une passerelle dans l'une des régions. Généralement, le GSLB choisit la passerelle la plus proche en fonction d'un algorithme d'équilibrage de charge tel que le temps d'aller-retour (RTT) ou la proximité statique.

Par exemple, vous pouvez avoir 3 passerelles régionales :

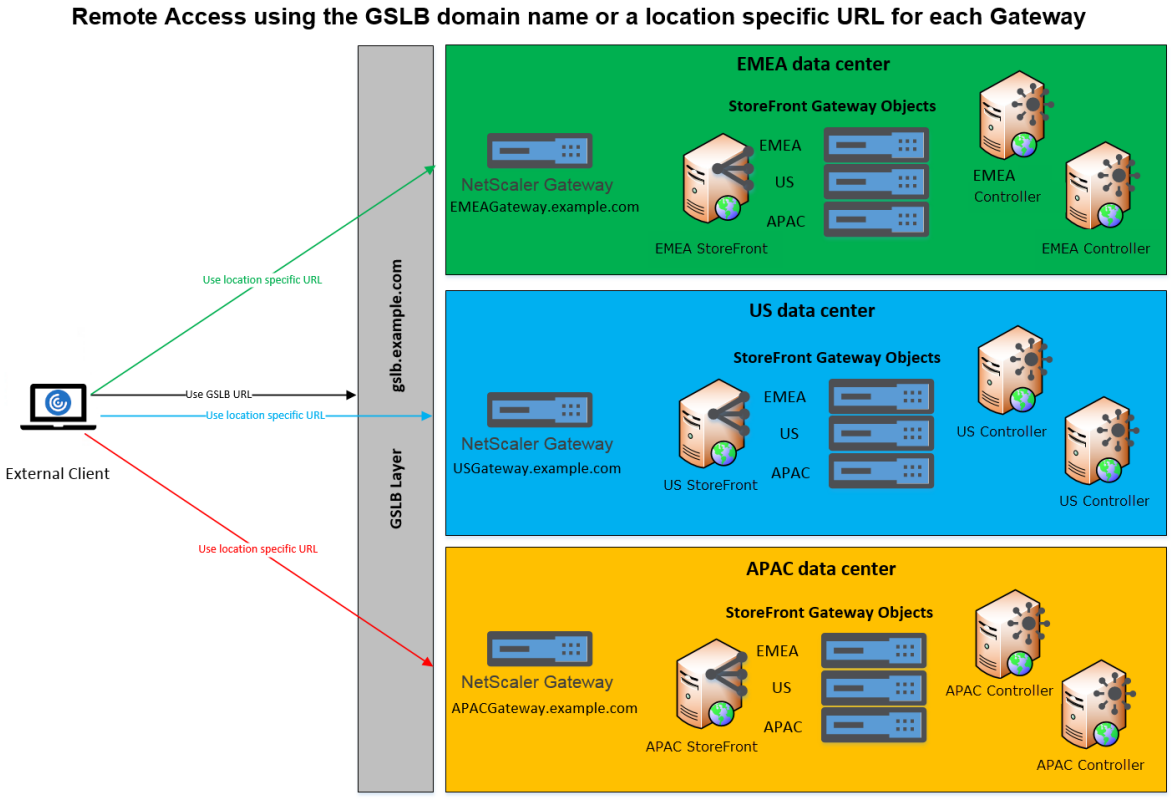
`emeagateway.example.com` - Passerelle Europe

`usgateway.example.com` - Passerelle États-Unis

`apacgateway.example.com` - Passerelle Asie-Pacifique

Avec un GSLB

`gslb.example.com`



Avant de configurer un GSLB, examinez les certificats de serveur que vous avez mis en place et la manière dont votre organisation exécute 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.

StoreFront ne dispose d'aucun mécanisme intégré permettant de synchroniser la configuration entre les groupes de serveurs ; il appartient à l'administrateur de configurer chaque groupe de serveurs StoreFront de la même manière afin que les utilisateurs bénéficient d'une expérience cohérente, quel que soit le groupe de serveurs auquel ils se connectent.

StoreFront peut synchroniser périodiquement les abonnements (favoris) entre les groupes de serveurs. Consultez Synchronisation des abonnements.

Accès des utilisateurs

Consultez la section Options d'accès utilisateur.

Options d'accès utilisateur

May 30, 2024

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

- Application Citrix Workspace installée localement : les utilisateurs disposant de versions compatibles de l'application Citrix Workspace peuvent accéder aux magasins StoreFront depuis l'interface utilisateur de l'application Citrix Workspace. Cet accès offre la meilleure expérience utilisateur et davantage de fonctionnalités.
- Application Citrix Workspace pour HTML5 : les utilisateurs disposant de navigateurs Web compatibles peuvent accéder aux magasins StoreFront en accédant au site Web du magasin. Par défaut, les utilisateurs doivent également disposer d'une version compatible de Citrix Workspace pour pouvoir accéder à leurs bureaux et applications. Ce processus est connu sous le nom de lancement hybride. Vous pouvez toutefois configurer votre site Web pour permettre aux utilisateurs d'accéder à leurs ressources via leur navigateur sans installer l'application Citrix Workspace.
- URL XenApp Services : les utilisateurs dont les anciens clients Citrix ne peuvent pas être mis à niveau peuvent accéder aux magasins à l'aide de l'URL XenApp Services du magasin. Lorsque vous créez un nouveau magasin, l'adresse URL du site XenApp Services est activée par défaut.

Application Citrix Workspace installée localement

L'accès aux magasins à partir de l'application Citrix Workspace installée localement offre la meilleure expérience utilisateur. Pour connaître les versions 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.

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 plus d'informations, veuillez consulter la section Configurer des points balises.

Ajouter un magasin à l'application Workspace

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 Paramètres de configuration du magasin dans la documentation de l'application Citrix Workspace pour Windows.

Configuration manuelle Les utilisateurs peuvent connecter l'application Citrix Workspace à leur magasin en saisissant les URL du magasin dans l'application Citrix Workspace. Pour plus d'informations, consultez la documentation de l'application Citrix Workspace.

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, le site Web offre 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 Web des magasins auxquels ils souhaitent accéder et télécharger les fichiers de provisioning à partir de ces sites. Éventuellement, pour un niveau de contrôle plus élevé, vous pouvez utiliser la console de gestion Citrix StoreFront pour générer des fichiers de provisioning contenant les détails de connexion à un ou plusieurs magasins. Vous pouvez distribuer ces fichiers après des utilisateurs appropriés. Pour plus d'informations, consultez la section Exporter les fichiers de provisioning de magasin pour des utilisateurs.

Adresses URL de configuration générées automatiquement Pour les utilisateurs exécutant macOS, vous pouvez utiliser le générateur d'adresse URL de configuration 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.

Découverte de compte basée sur une adresse e-mail Grâce à la découverte de comptes basée sur l'adresse e-mail, au lieu de devoir connaître les détails d'accès à leurs magasins, les utilisateurs saisissent leurs adresses e-mail lors du processus de configuration initiale de l'application Citrix Workspace. Pour plus de détails sur la procédure à suivre, consultez la section Découverte de compte basée sur une adresse e-mail.

Global App Config Service

Utilisez Global App Config Service pour configurer l'application Citrix Workspace pour vos magasins StoreFront. Voir Configurer les paramètres des magasins locaux.

Application Citrix Workspace pour HTML5

Au lieu d'utiliser une application Workspace installée localement, les utilisateurs peuvent accéder à leur magasin via un navigateur Web avec l'application Workspace pour HTML5. Lorsque les utilisateurs lancent leurs ressources, deux possibilités s'offrent à eux.

1. Les ressources sont lancées dans l'application Citrix Workspace installée localement. C'est ce que l'on appelle un lancement hybride. Cela offre aux utilisateurs la meilleure expérience possible car ils peuvent tirer parti de l'intégration complète du système d'exploitation. Pour plus d'informations consultez Lancement hybride.
2. Les ressources sont lancées dans le navigateur. Cela permet aux utilisateurs d'accéder aux ressources sans avoir à installer de logiciel localement.

La configuration par défaut exige que l'application Citrix Workspace soit installée localement pour un lancement hybride. Vous pouvez modifier la configuration pour que les ressources soient toujours lancées dans le navigateur ou pour laisser le choix à l'utilisateur. Consultez Déployer l'application Workspace.

Si l'administrateur a sélectionné **Utiliser Receiver pour HTML5 si une installation Receiver locale n'est pas disponible**, lorsque l'utilisateur ouvre le site Web du magasin pour la première fois dans son navigateur, il a la possibilité de cliquer sur **Utiliser la version simplifiée** pour lancer les ressources dans son navigateur Web.

Conditions requises pour ouvrir des ressources dans votre navigateur

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, activez 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 plus d'informations, veuillez consulter la section Paramètres de stratégie WebSockets.

Pour que les lancements de ressources Citrix Virtual Apps and Desktops réussissent, configurez les connexions TLS aux VDA qui hébergent les applications et les bureaux. 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.

Lancement hybride

Le processus par lequel les utilisateurs ouvrent Citrix Workspace pour HTML5 pour la première fois via leur navigateur, mais lancent des applications dans l'application Citrix Workspace installée localement est connu sous le nom de lancement hybride. Le site Web peut communiquer de différentes manières avec l'application Workspace installée localement pour lancer des ressources.

Citrix Workspace Launcher

Lorsque l'utilisateur accède pour la première fois à un site Web StoreFront doté d'un système d'exploitation et d'un navigateur compatibles, l'application Citrix Workspace pour HTML5 tente d'appeler Citrix Workspace Launcher. Si une version prise en charge de l'application Citrix Workspace est installée, l'application en informe StoreFront. L'application Citrix Workspace pour HTML5 s'en souvient et utilise Citrix Workspace Launcher lorsqu'elle lance une application.

Le site Web du magasin appelle Citrix Workspace Launcher sous Windows, Mac et Linux lorsque vous utilisez les navigateurs suivants :

- Firefox 52 ou version ultérieure
- Chrome 42 ou version ultérieure
- Safari 12 ou version ultérieure
- Edge 25 ou version ultérieure

Citrix Workspace Launcher requiert les versions minimales suivantes de Citrix Receiver ou de l'application Citrix Workspace.

- Receiver pour Windows 4.3 ou supérieur
- Receiver pour Mac 12.0 ou supérieur
- Application Workspace pour Linux 2003 ou version ultérieure

Si Citrix Workspace Launcher n'est pas disponible ou si l'utilisateur ne l'autorise pas à s'ouvrir, l'application Citrix Workspace installée localement ne pourra pas être détectée. L'utilisateur a la possibilité de réessayer ou de cliquer sur **Déjà installé**, auquel cas le lancement d'applications à l'aide de fichiers .ica est utilisé. L'utilisateur peut réessayer ultérieurement en accédant à l'écran Paramètres et en cliquant sur **Changer l'application Citrix Workspace**.

Si vous utilisez plusieurs groupes de serveurs StoreFront actifs derrière l'équilibrage de charge globale des serveurs, le lanceur Citrix Workspace peut échouer par intermittence. Pour éviter cela, vous devez configurer l'équilibrage de charge globale de vos serveurs de manière à ce que la session Web de l'utilisateur soit persistante sur un groupe de serveurs StoreFront pendant toute la durée du processus de détection des clients. Consultez CTX460312. Vous pouvez également déployer les extensions Web Citrix Workspace.

Lors de la connexion au site Web via Citrix Gateway, le lanceur Citrix Workspace utilise le routage HDX de la passerelle pour renvoyer les requêtes proxy de l'application Citrix Workspace au serveur StoreFront. Si la passerelle est configurée pour **l'authentification uniquement** (et pas pour le routage HDX), le lanceur Citrix Workspace ne fonctionne pas. Activez le routage HDX ou déployez les extensions Web Citrix Workspace.

Extensions Web de Citrix Workspace

Les extensions Web de Citrix Workspace désignent des extensions pour les navigateurs Web les plus courants qui améliorent l'expérience utilisateur lors de la détection de l'application Citrix Workspace installée localement et du lancement d'applications et de bureaux virtuels. Par rapport à Citrix Workspace Launcher, cette configuration offre une meilleure expérience utilisateur et évite les problèmes liés à l'équilibrage de charge globale des serveurs.

Pour activer la détection des clients basée sur les extensions de navigateur, procédez comme suit :

- Activer la fonctionnalité sur le serveur StoreFront.
- Déployez l'extension de navigateur sur les appareils clients.
- Déployez l'application Citrix Workspace pour Windows 2303, Mac 2304 ou Linux 2302 ou version ultérieure.

La première fois qu'un utilisateur accède au site Web d'un magasin sur une plate-forme prise en charge, il est invité à détecter l'application Workspace installée localement. Le site Web essaie d'abord d'utiliser l'extension Web et, en cas d'échec, il essaie Citrix Workspace Launcher. Les utilisateurs existants qui ont déjà terminé la détection de l'application Workspace peuvent accéder aux

paramètres du compte, puis cliquer sur **Modifier l'application Citrix Workspace** pour détecter à nouveau l'application Workspace.

> **Important**
>
> Cette fonctionnalité est activée par défaut pour les nouvelles installations. Toutefois, si vous effectuez une mise à niveau à partir d'une version précédente, vous devez activer cette fonctionnalité manuellement. Les administrateurs peuvent activer cette fonctionnalité à l'aide du script PowerShell suivant sur un serveur StoreFront : `Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension" -IsEnabled $True`

Internet Explorer

La première fois que l'utilisateur ouvre le site Web du magasin dans Internet Explorer, il est invité à installer l'application Citrix Workspace qui inclut le module complémentaire client ICA Citrix pour Internet Explorer. Une fois le plug-in installé, il est utilisé pour lancer des applications et des bureaux via l'application Citrix Workspace installée localement.

Téléchargements de fichiers ICA

Si l'application Citrix Workspace pour HTML5 ne parvient pas à détecter une application Citrix Workspace installée localement par d'autres moyens, lorsqu'un utilisateur lance une application ou un bureau, un fichier .ica est téléchargé. L'utilisateur peut ouvrir ce fichier à l'aide de l'application Citrix Workspace installée localement.

Raccourcis vers les ressources

Vous pouvez générer des URL qui fournissent un accès aux bureaux et applications disponibles dans votre magasin. 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 Web du magasin, où ils ouvrent une session si ce n'est pas déjà fait. Le site Web du magasin démarre automatiquement la ressource. Pour plus d'informations sur la création des raccourcis vers les ressources, consultez la section Raccourcis de site Web.

Lorsque vous créez un raccourci d'application, assurez-vous qu'aucune autre application disponible sur le magasin 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 magasin, 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.

Personnaliser l'interface utilisateur

Citrix StoreFront fournit un mécanisme de personnalisation de l'interface utilisateur. Cela s'applique que vous accédiez à un magasin via l'application Citrix Workspace ou un navigateur Web. 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. Pour plus d'informations, consultez Personnaliser l'apparence.

Adresses URL XenApp Services

> **Remarque :**
>
> XenApp Services (également connu sous le nom de PNAgent) est obsolète depuis StoreFront 2308. Il est recommandé d'utiliser l'application Citrix Workspace pour vous connecter à StoreFront à l'aide d'une URL de magasin.

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 plus d'informations, consultez la documentation Citrix Workspace 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 plus d'informations, consultez la section Authentification XML.
- Le contrôle de l'espace de travail est activé par défaut pour les adresses URL XenApp Services et ne peut pas être configuré ou désactivé.
- Les requêtes des utilisateurs pour modifier leur mot de passe sont directement transférées vers le contrôleur de domaine par le biais des serveurs Citrix Virtual Apps and Desktops fournissant des bureaux et des applications au magasin, en contournant le service d'authentification de StoreFront.

Configuration système requise

May 30, 2024

Avant d'installer StoreFront, consultez la section Planifier votre déploiement StoreFront.

Configuration requise pour le serveur StoreFront

Logiciel

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

- Windows Server 2022 éditions Standard et Datacenter
- Windows Server 2019 éditions Standard et Datacenter
- Windows Server 2016 éditions Standard et Datacenter

> **Remarque :**
>
> StoreFront nécessite une expérience de bureau Windows et ne peut donc pas être installé sur Windows Server Core.

Tous les serveurs StoreFront d'un groupe de serveurs doivent utiliser la même version du système d'exploitation, la même langue et les mêmes paramètres régionaux.

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.

Avant de pouvoir installer StoreFront, les fonctionnalités Windows suivantes doivent être activées sur le serveur Web. Ces composants sont activés par défaut sur une nouvelle installation Windows. Aucune action n'est donc requise sauf s'ils ont été explicitement désinstallés.

- NET-Framework-45-Features
  - NET-Framework-45-Core
- PowerShellRoot
  - PowerShell

Si la version de .NET Framework installée est antérieure à 4.7.2, le programme d'installation installe automatiquement .NET Framework 4.7.2. Cela nécessite que la fonctionnalité Windows NET-Framework-45-Core soit déjà installée.

Si le programme d'installation de StoreFront détecte l'absence de l'une des fonctionnalités Windows suivantes, celles-ci sont automatiquement installées :

- Web-Server
  - Web-WebServer
    - Web-Common-Http
      - Web-Default-Doc

        - Web-Http-Errors
        - Web-Static-Content
        - Web-Http-Redirect
    - Web-Health
        - Web-Http-Logging
    - Web-Security
        - Web-Filtering
        - Web-Basic-Auth
        - Web-Windows-Auth
    - Web-App-Dev
        - Web-Net-Ext45
        - Web-AppInit
        - Web-Asp-Net45
        - Web-ISAPI-Ext
        - Web-ISAPI-Filter
    - Web-Mgmt-Tools
        - Web-Mgmt-Console
    - Web-Scripting-Tools
- NET-Framework-45-Features
    - NET-Framework-45-ASPNET
    - NET-WCF-Services45
        - NET-WCF-TCP-PortSharing45

Il est possible de déplacer le site Web IIS vers un autre répertoire ou lecteur avant d'installer StoreFront. Le chemin d'accès relatif à StoreFront dans IIS doit être identique sur tous les serveurs d'un groupe de serveurs.

Matériel

Les serveurs Storefront doivent répondre aux exigences suivantes :

- Processeur : au moins 2 processeurs virtuels, 4 processeurs virtuels recommandés
- RAM : 4 Go, plus 700 octets par ressource disponible et par utilisateur.
- Stockage :
    - 250 Mo pour StoreFront
    - 30 Mo pour chaque magasin, en supposant un site Web par magasin.
    - Pour chaque magasin dont les favoris sont activés, 5 Mo plus 8 Mo pour 1 000 favoris

  - Espace suffisant pour les fichiers journaux IIS en fonction de vos besoins. Consultez la documentation Microsoft sur la gestion du stockage de fichiers journaux IIS.
  - Espace suffisant pour les journaux de diagnostic de StoreFront. Par défaut, StoreFront conserve 1 Go de journaux par service. Un déploiement StoreFront comprend généralement 1 service d'itinérance et 3 services par magasin (service de magasin, service d'authentification et service Receiver pour Web). Consultez Résolution des problèmes de StoreFront.

Réseau

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 clients utilisent les ports TCP 80 et 443 pour se connecter à StoreFront via les communications HTTP et HTTPS, respectivement.
- Le port TCP 808 est utilisé pour les communications entre les serveurs StoreFront dans un groupe de serveurs.
- 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 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.

Active Directory

De nombreuses fonctionnalités de StoreFront nécessitent d'associer le serveur Windows sur lequel StoreFront est installé à un domaine Active Directory.

Si vous installez StoreFront sur un serveur ne faisant pas partie d'un domaine, les fonctionnalités suivantes ne sont pas disponibles :

- Groupes de serveurs
- Favoris
- Méthodes d'authentification autres que le nom d'utilisateur et le mot de passe explicites, soit directement auprès de StoreFront, soit via une passerelle. Vous devez configurer StoreFront pour déléguer l'authentification au Delivery Controller.

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.

Citrix Virtual Apps and Desktops

StoreFront prend en charge les versions suivantes de Citrix Virtual Apps and Desktops :

- Citrix Virtual Apps and Desktops 2402 LTSR
- Citrix Virtual Apps and Desktops 2311
- Citrix Virtual Apps and Desktops 2308
- Citrix Virtual Apps and Desktops 2305
- Citrix Virtual Apps and Desktops 2203 LTSR
- Citrix Virtual Apps and Desktops 1912 LTSR

Citrix Gateway

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

- Citrix Gateway 14.1
- Citrix Gateway 13.1
- Citrix Gateway 13.0

Les connexions établies via Citrix Gateway peuvent être effectuées à l'aide du proxy ICA, de Citrix Gateway Plug-in ou du VPN sans client (cVPN).

Configuration requise pour la machine utilisateur

StoreFront propose différentes options permettant aux utilisateurs d'accéder à leurs bureaux et applications. Les utilisateurs de Citrix peuvent accéder aux magasins via l'application Citrix Workspace installée localement ou utiliser l'application Citrix Workspace pour HTML5 dans leur navigateur.

Application Citrix Workspace installée localement

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 les dates de cycle de vie des applications Citrix Workspace, consultez https://www.citrix.com/support/product-lifecycle/workspace-app.html.

Application Citrix Workspace pour HTML5 dans un navigateur Web

Vous pouvez utiliser l'application Citrix Workspace pour HTML5 pour accéder à votre magasin à l'aide d'un navigateur Web. Les applications et les bureaux peuvent être lancés soit via une application Citrix Workspace installée en mode natif (appelée lancement hybride), soit depuis le navigateur Web. Selon la configuration de votre site Web, les utilisateurs peuvent basculer entre les deux méthodes de lancement.

Utilisez les dernières versions des navigateurs suivants.

Sous Windows :

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11 : uniquement pour naviguer dans le magasin, et non pour se connecter à des ressources

Sous Mac :

- Safari
- Google Chrome
- Mozilla Firefox

Sur Linux :

- Google Chrome
- Mozilla Firefox

Pour plus d'informations sur les exigences relatives à l'utilisation de l'application Citrix Workspace pour HTML5 pour se connecter à des ressources via un navigateur Web, consultez la documentation de l'application Citrix Workspace pour HTML5.

Anciens appareils

Les anciens clients Citrix peuvent 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. Cette fonctionnalité est obsolète et sera supprimée d'une future version.

Spécifications de la carte à puce

Utiliser l'application Citrix Workspace avec des cartes à puce

Citrix teste la compatibilité des cartes avec des agences gouvernementales américaines telles le Government Common Access Card (CAC), le National Institute of Standards and Technology Personal Identity Verification (NIST PIV) et avec certains jetons de carte à puce USB. Vous pouvez utiliser des lecteurs de carte de contact conformes aux spécifications des lecteurs USB CCID qui sont classés par le German Zentraler Kreditausschuss (ZKA) en tant que lecteurs de carte à puce de classe 1. Les lecteurs de carte de contact de classe ZKA 1 exigent que les utilisateurs insèrent leur carte à puce dans le lecteur. Les autres types de lecteurs de carte à puce, y compris les lecteurs de classe 2 (qui ont équipés de pavés numériques pour la saisie de codes PIN), les lecteurs sans contacts et les cartes à puce virtuelles basées sur les puces TPM, ne sont pas pris en charge.

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

Pour de plus amples informations sur les cartes à puce et middleware compatibles avec Citrix, consultez la section Cartes à puce dans la documentation de Citrix Virtual Apps and Desktops et http://www.citrix.com/ready.

Configuration requise pour 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 Citrix Analytics Service. Cette fonctionnalité est prise en charge pour les scénarios suivants :

- Magasins accessibles par les navigateurs Web
- 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

Installer StoreFront

December 6, 2023

Avant l'installation et la configuration

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

1. Vérifiez la configuration système requise.
2. 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.

3. Éventuellement, si vous prévoyez de configurer un déploiement StoreFront comprenant de multiples serveurs, configurez un environnement à équilibrage de charge pour vos serveurs StoreFront.

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

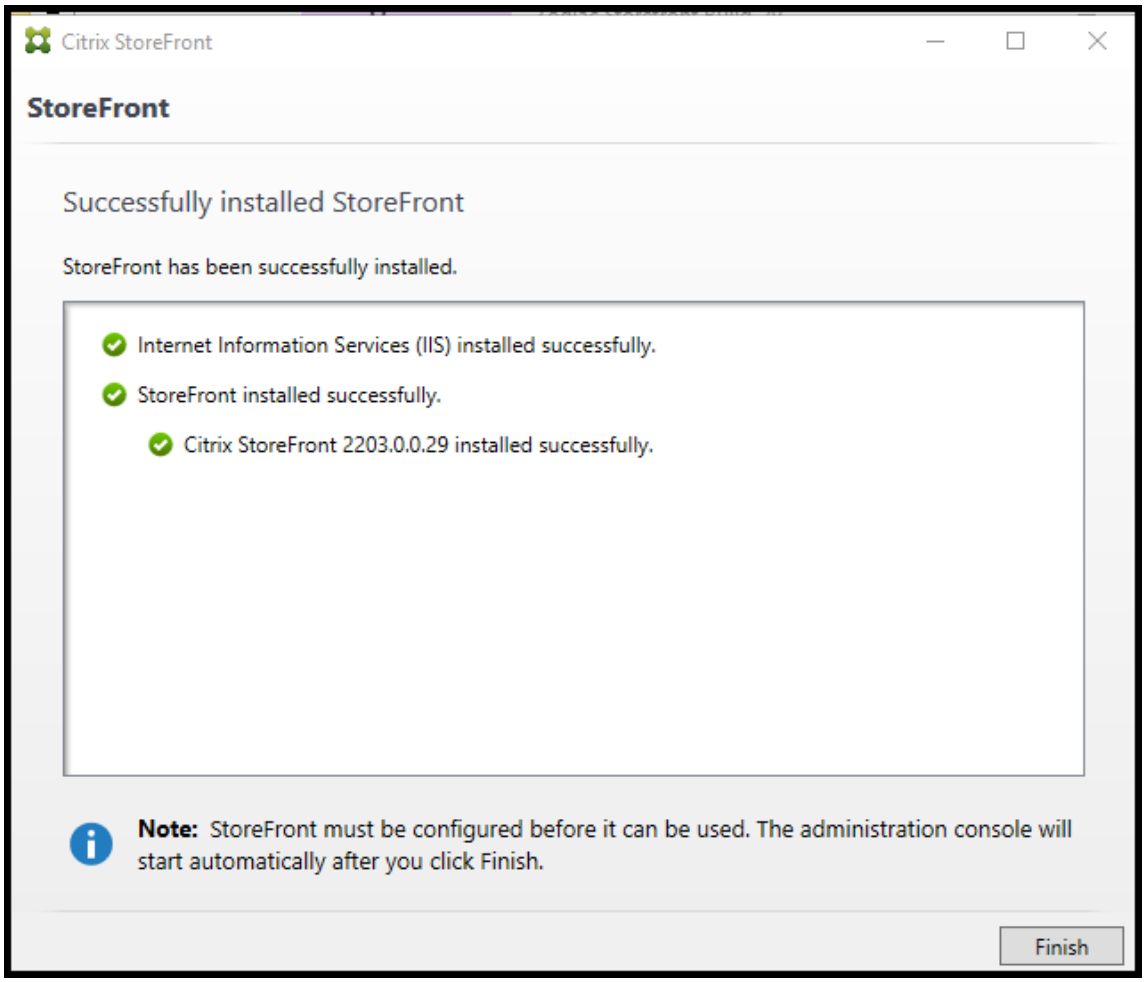
4. Assurez-vous que votre pare-feu et autres périphériques réseau autorisent l'accès au port TCP 80 ou 443, aussi bien à l'intérieur qu'à l'extérieur du réseau d'entreprise. En outre, vérifiez que tous les pare-feu ou autres périphériques sur votre réseau interne ne bloquent pas le trafic des ports TCP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

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. Recherchez le fichier CitrixStoreFront-x64.exe, puis exécutez-le en tant qu'administrateur.
4. Lisez et acceptez le contrat de licence, puis cliquez sur **Suivant**.
5. Si la page Vérifier les composants requis s'affiche, cliquez sur **Suivant**.
6. Sur la page Prêt pour l'installation, vérifiez que les prérequis et les composants StoreFront sont répertoriés pour l'installation et cliquez sur **Installer**.
7. Une fois l'installation terminée, cliquez sur **Terminer**.



8. StoreFront peut vous demander de redémarrer pour terminer l'installation. Cliquez sur **Oui** pour redémarrer maintenant.
9. Configurez Microsoft Internet Information Services (IIS) pour HTTPS. Pour connaître les étapes à suivre, reportez-vous à la section Sécurisation de StoreFront avec HTTPS.

Pour installer StoreFront à partir d'une invite de commandes

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

```
1 CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR
     installationlocation] [-WINDOWS_CLIENT filelocation\filename.
     exe] [-MAC_CLIENT filelocation\filename.dmg]
2 <!--NeedCopy-->
```

   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.

   Lorsqu'un utilisateur ouvre un magasin dans un navigateur Web sous Windows ou macOS, par défaut, si l'application Citrix Workspace n'est pas détectée, 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 plus d'informations, consultez la section Configurer la manière dont les ressources s'affichent auprès des utilisateurs.

   Si vous envisagez de modifier cette configuration, spécifiez les arguments **-WINDOWS_CLIENT** et **-MAC_CLIENT** afin de copier les fichiers d'installation de Citrix Receiver pour Windows ou

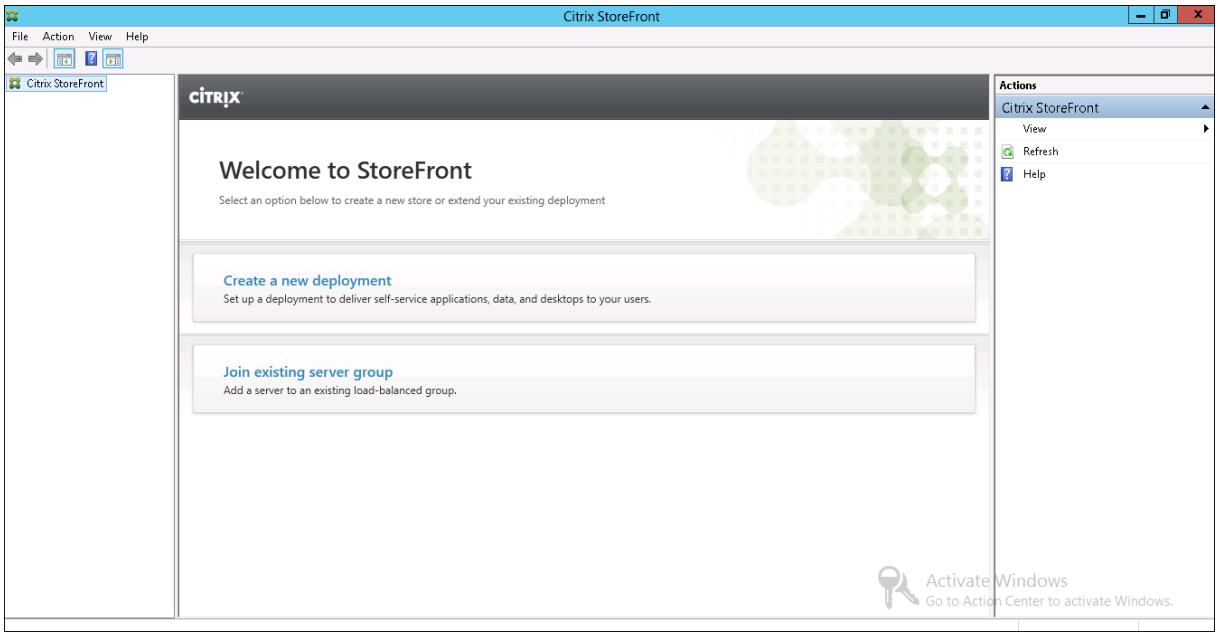
de l'application Citrix Workspace pour Windows et de Citrix Receiver pour Mac ou de l'application Citrix Workspace pour Mac, respectivement, sur l'emplacement approprié de votre déploiement StoreFront. Remplacez *filelocation* par le répertoire contenant le fichier d'installation que vous voulez copier et *filename* par le nom du fichier d'installation. Les fichiers d'installation de 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.

Journaux d'installation

Pour plus de détails sur les fichiers journaux, consultez la section Journaux d'installation.

Configurer StoreFront

Une fois l'installation terminée, la console de gestion Citrix StoreFront démarre automatiquement. Vous pouvez également accéder à StoreFront à partir du menu de démarrage. 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.

Les utilisateurs peuvent désormais accéder à votre magasin via un navigateur ou l'application Citrix Workspace. Consultez le guide de l'utilisateur.

Programme d'amélioration de l'expérience du client Citrix

January 25, 2024

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
<!--NeedCopy-->
```

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

February 22, 2024

Si vous êtes un client Monitor 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 Monitor. Une fois configurés, l'application Citrix Workspace et les navigateurs Web envoient les événements 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 dans la documentation de Citrix Analytics, consultez la section Intégrer des sites Virtual Apps and Desktops à l'aide de StoreFront.

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.

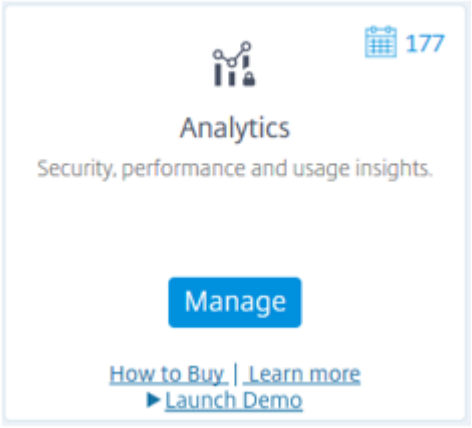
> **Important :**
>
> Votre déploiement StoreFront doit pouvoir contacter les adresses suivantes sur le port 443 pour que cette fonctionnalité fonctionne correctement et utilise les services Monitor :
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

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 Monitor (`https://citrix.cloud.com/`) à l'aide d'un compte administrateur.
2. Sélectionnez un client Monitor.

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"
 }

<!--NeedCopy-->
```

où

customerId est l'ID unique du client Monitor actuel.

cwsServiceKey est une clé unique identifiant le compte client Monitor actuel.

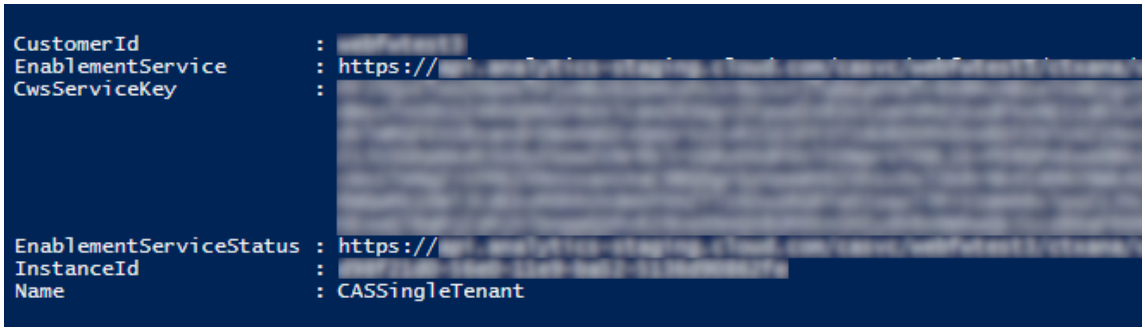
instanceID est un ID généré utilisé pour signer des requêtes (sécurisées) effectuées à partir de l'application Citrix Workspace vers Citrix Analytics. Si vous enregistrez plusieurs serveurs StoreFront ou groupes de serveurs avec Monitor, chacun possède un ID instanceID unique.

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 :

```
Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
    StoreFrontConfigurationFile.json"
Get-STFCasConfiguration
<!--NeedCopy-->
```

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 Monitor 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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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.

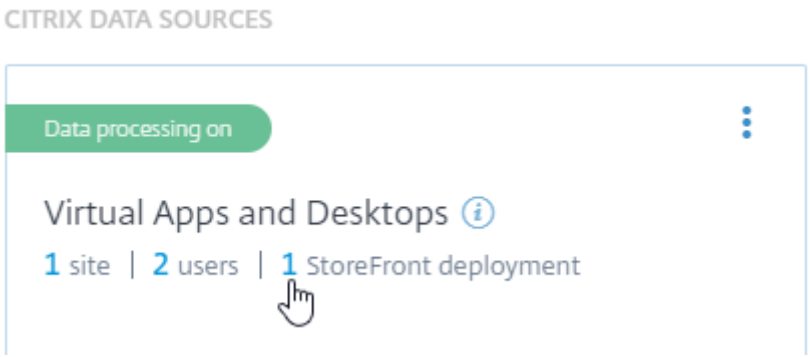
3. Si vous effectuez ces actions sur un groupe de serveurs StoreFront, propagez la modification et supprimez les données Citrix Analytics importées de tous les membres du groupe de serveurs. Sur un serveur du groupe de serveurs, exécutez la commande suivante :

```
Publish-STFServerGroupConfiguration
```

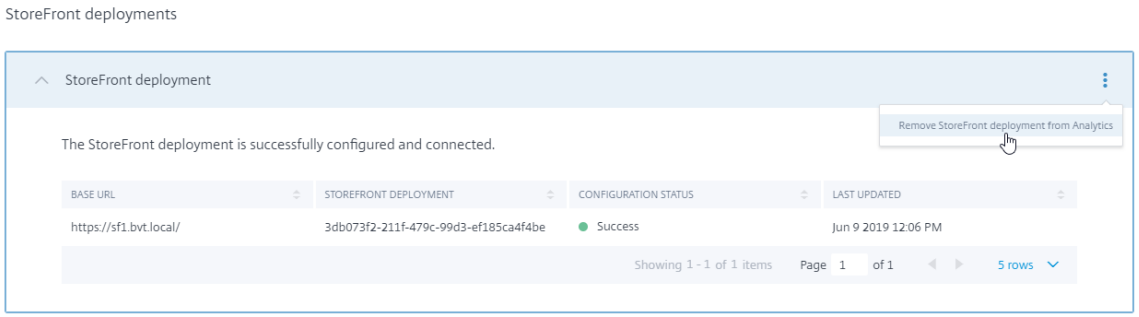

4. Sur tous les autres membres du groupe de serveurs, exécutez la commande suivante pour confirmer que la configuration de Citrix Analytics a bien été supprimée de tous les serveurs du groupe :

   ```
   Get-STFCasConfiguration
   ```

5. Connectez-vous à Monitor (`https://citrix.cloud.com/`) à l'aide d'un compte administrateur.
6. Sélectionnez un client Monitor.
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 deploy-

> ment 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 Monitor 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
{

    [CmdletBinding()]
    param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
       Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
       array]$Stores,
        [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
           string]$ProxyIP,
        [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
           string]$ProxyFQDN,
        [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
           Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
           ][int]$ProxyPort)

    foreach($Store in $Stores)
    {

        Write-Host "Backing up the Store web.config file for store
            $Store before making changes..." -ForegroundColor "
           Yellow"
        Write-Host "`n"

        if(!(Test-Path "$env:UserProfile\desktop$Store"))
        {

            Write-Host "Creating $env:UserProfile\desktop$Store\
               directory for backup..." -ForegroundColor "Yellow"
            New-Item -Path "$env:UserProfile\desktop$Store" -
               ItemType "Directory" | Out-Null
            Write-Host "`n"
         }


        Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
           config to $env:UserProfile\desktop$Store..." -
           ForegroundColor "Yellow"
        Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
           config" -Destination "$env:UserProfile\desktop$Store" -
           Force | Out-Null

        if(Test-Path "$env:UserProfile\desktop$Store\web.config")
        {

            Write-Host "$env:UserProfile\desktop$Store\web.config
               file backed up" -ForegroundColor "Green"
         }

        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
99  <!--NeedCopy-->
```

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>
10  <!--NeedCopy-->
```

6. Importez les données de Citrix Analytics comme décrit dans 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>
<!--NeedCopy-->
```

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>
<!--NeedCopy-->
```

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" />
    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
       9.0.0.0" />
    </dependentAssembly>
</assemblyBinding>
</runtime>

Insert the <system.net> element here

</configuration>
<!--NeedCopy-->
```

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

Sécurisation de StoreFront avec HTTPS

April 17, 2024

Citrix vous recommande fortement de sécuriser les communications entre StoreFront et les machines des utilisateurs à l'aide du protocole HTTPS. Cela garantit que les mots de passe et autres données envoyés entre le client et StoreFront sont cryptés. De plus, les connexions HTTP simples peuvent être compromises par diverses attaques, telles que les attaques de type « man-in-the-middle », en particulier lorsque les connexions sont établies à partir d'emplacements non sécurisés tels que des hotspots Wi-Fi publics. En l'absence de la configuration IIS appropriée, StoreFront utilise le protocole HTTP pour les communications.

Selon votre configuration, les utilisateurs peuvent accéder à StoreFront via une passerelle ou un équilibreur de charge. Vous pouvez mettre fin à la connexion HTTPS au niveau de la passerelle ou de l'équilibreur de charge. Toutefois, dans ce cas, Citrix vous recommande toujours de sécuriser les connexions entre la passerelle et StoreFront à l'aide du protocole HTTPS.

Si StoreFront n'est pas configuré pour HTTPS, l'avertissement suivant s'affiche :

Création de certificats

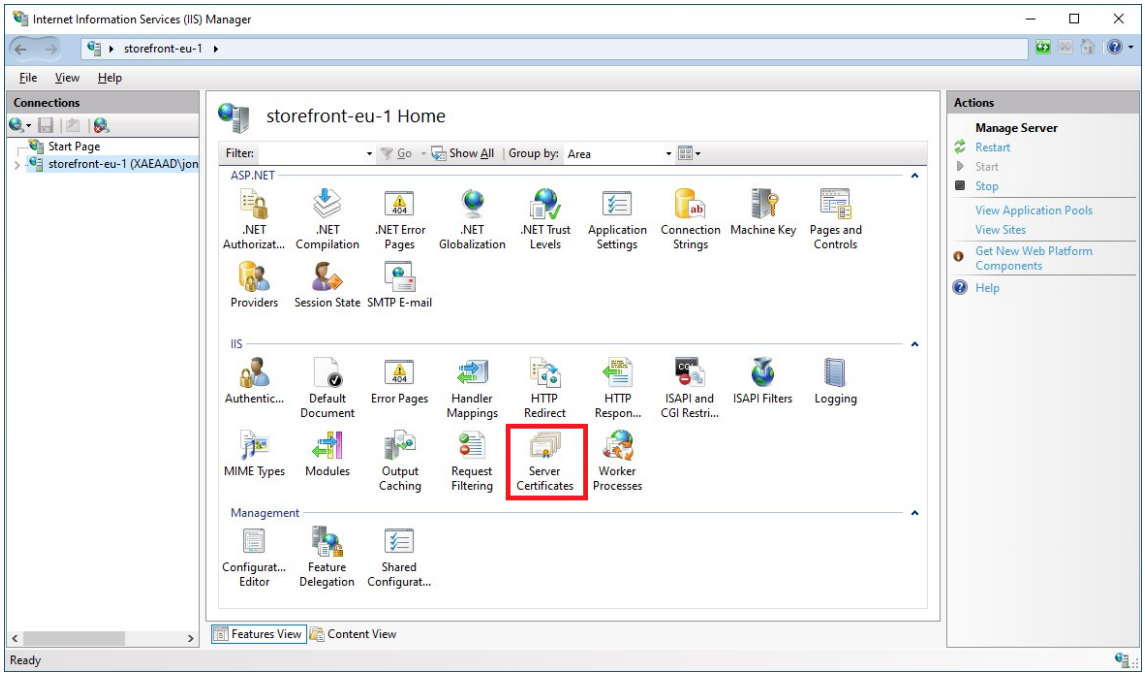
- Assurez-vous que le ou les noms de domaine complets utilisés pour accéder à StoreFront sont inclus dans le champ DNS en tant que Subject Alternative Name (SAN). Si vous utilisez un équilibrage de charge, incluez à la fois le nom de domaine complet du serveur individuel et celui de l'équilibreur de charge
- 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.
- Exportez le certificat au format PFX y compris la clé privée.

Configurer IIS pour HTTPS

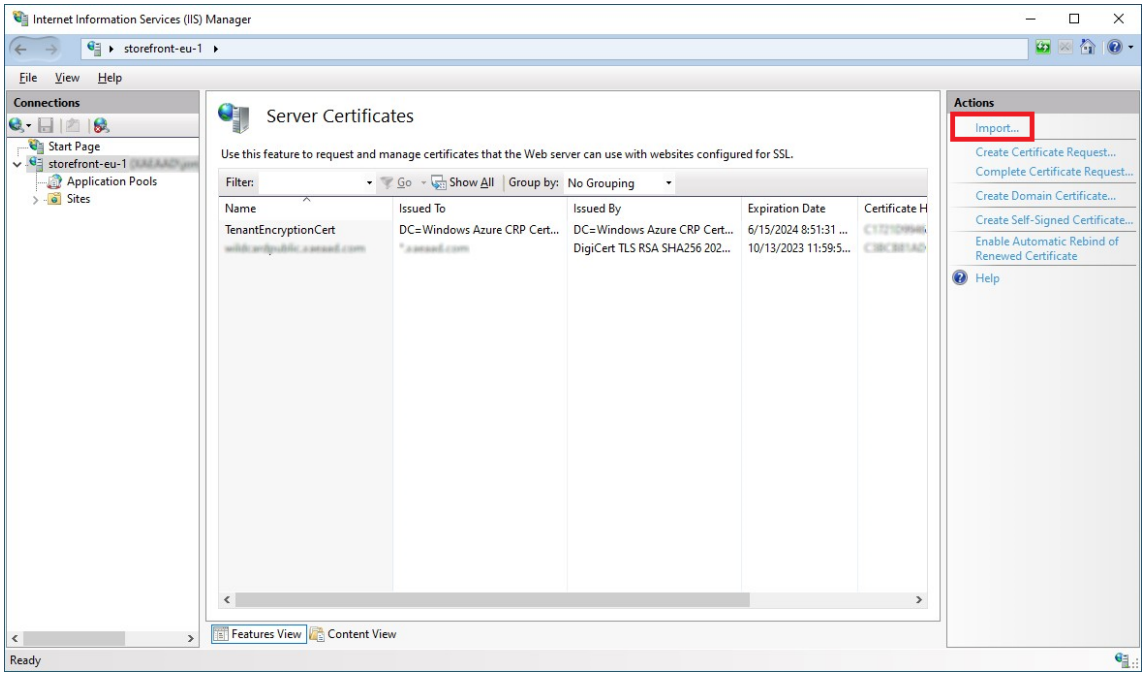
Pour configurer Microsoft Internet Information Services (IIS) pour HTTPS sur le serveur StoreFront :

1. Ouvrir la console du Gestionnaire des services Internet Information Services (IIS)
2. Dans l'arborescence de gauche, sélectionnez le serveur.

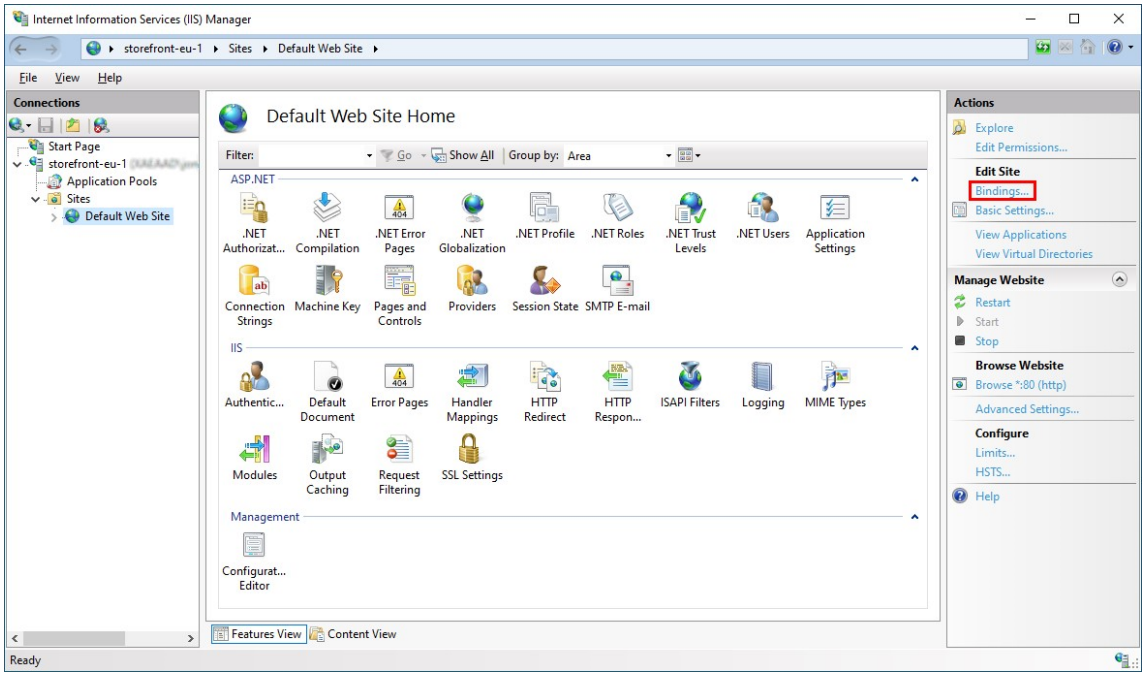
3. Dans le volet droit, double-cliquez sur **Certificats de serveur**.



4. À partir de l'écran Certificats de serveur, vous pouvez importer un certificat existant ou en créer un nouveau.

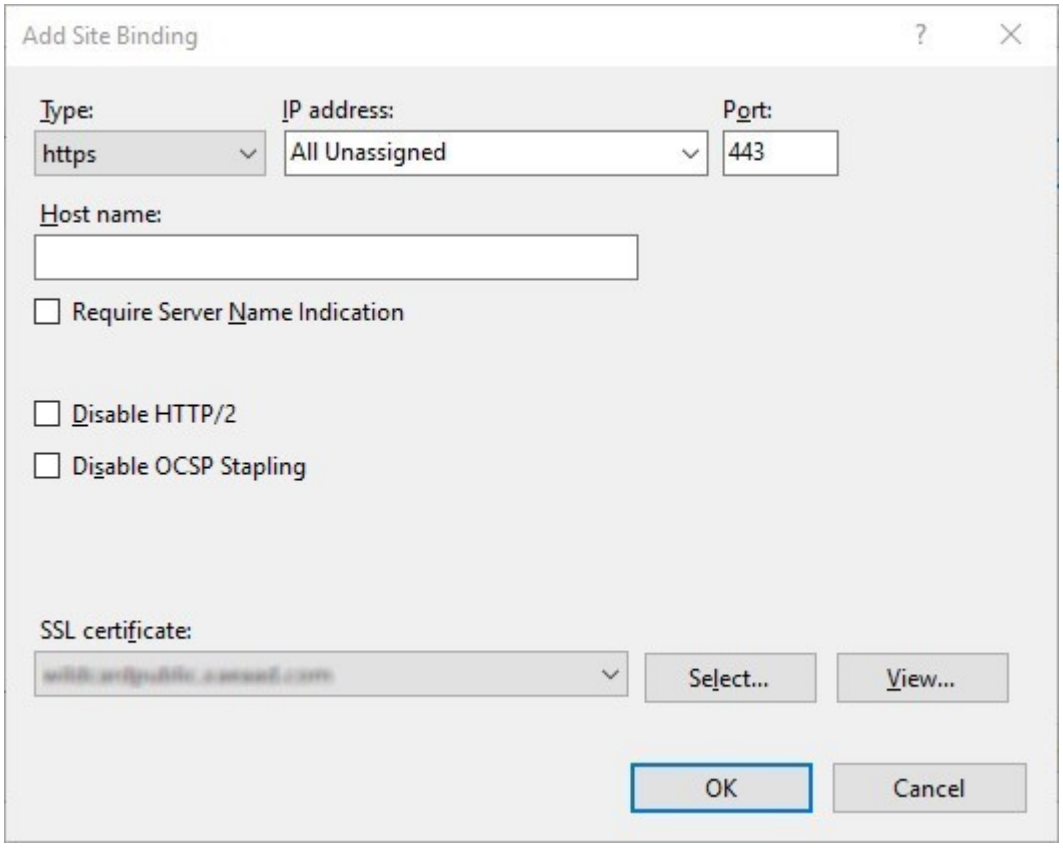


5. Dans l'arborescence de gauche, sélectionnez **Site Web par défaut** (ou le site Web approprié)
6. Dans le volet Actions, cliquez sur **Liaisons…**

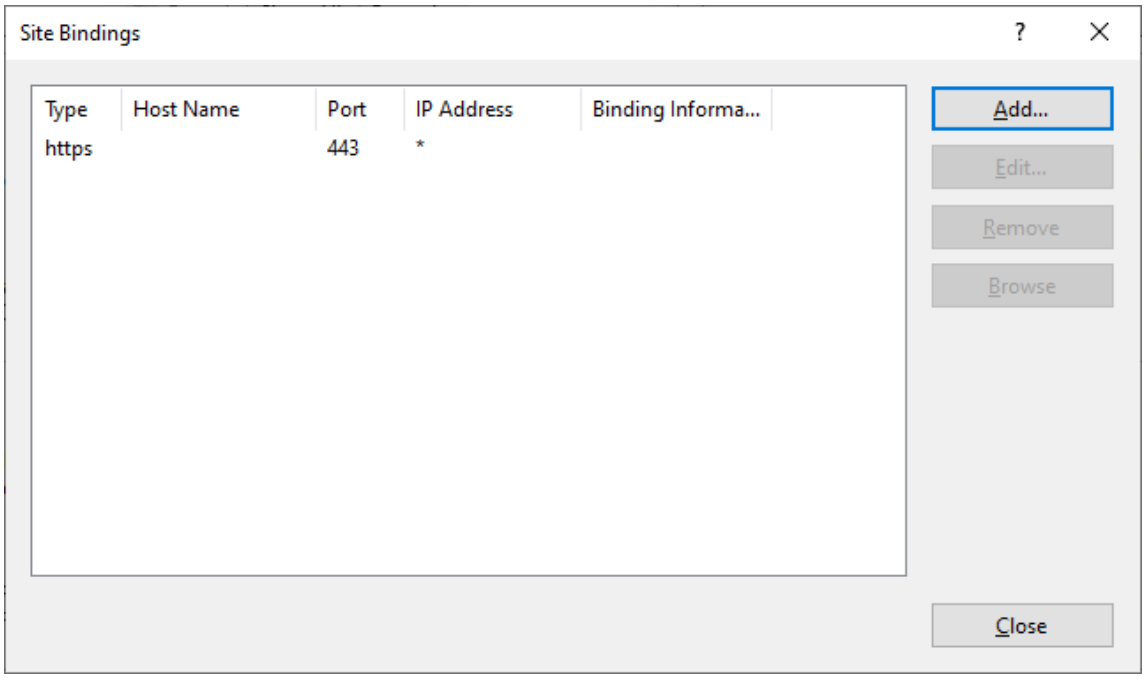


7. Dans la fenêtre des liaisons, cliquez sur **Ajouter…**
8. Dans la liste déroulante **Type**, sélectionnez **https**.
9. Sur Windows Server 2022 ou version ultérieure, cliquez sur **Désactiver l'ancien protocole TLS** pour désactiver le protocole TLS antérieur à la version 1.2.

   Sur les anciennes versions de Windows Server, vous pouvez désactiver les anciennes versions du protocole TLS à l'aide des paramètres de registre Windows. Consultez la documentation Windows Server.
10. Sélectionnez le certificat précédemment importé. Sélectionnez OK.



11. Pour supprimer l'accès HTTP, sélectionnez HTTP et cliquez sur **Supprimer**.

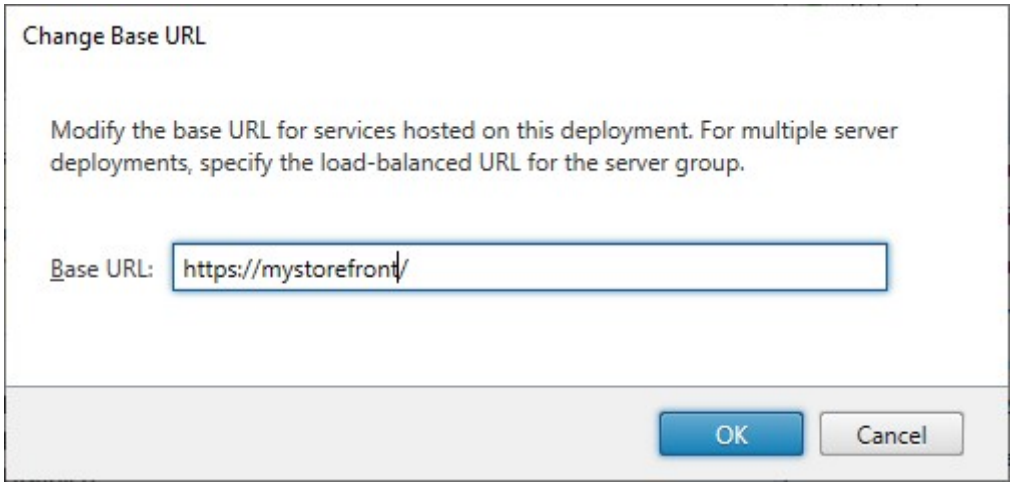


Modifier l'URL de base du serveur StoreFront HTTP et la remplacer par HTTPS

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.

1. Dans la console de gestion Citrix StoreFront, dans le panneau de gauche, sélectionnez **Groupe de serveurs**.
2. Dans le panneau Actions, sélectionnez **Changer l'URL de base**.
3. Mettez à jour l'URL de base pour qu'elle commence par `https:` et cliquez sur **OK**.



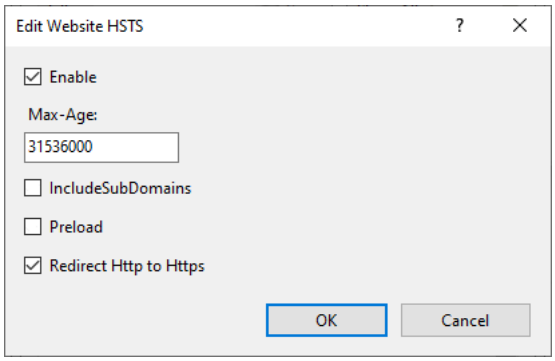
HSTS

La machine cliente de l'utilisateur est vulnérable même après l'activation du protocole HTTPS côté serveur. Par exemple, un attaquant de type « man-in-the-middle » pourrait usurper le serveur StoreFront et inciter l'utilisateur à se connecter au serveur falsifié via HTTP. Il pourrait alors accéder à des informations sensibles telles que les informations d'identification de l'utilisateur. La solution consiste à s'assurer que le navigateur de l'utilisateur ne tente pas d'accéder au serveur RfWeb via HTTP. Vous pouvez y parvenir grâce au protocole HTTP Strict Transport Security (HSTS).

Lorsque HSTS est activé, le serveur indique aux navigateurs Web que les requêtes adressées au site Web doivent uniquement être effectuées via HTTPS. Si un utilisateur tente d'accéder à l'URL via HTTP, le navigateur bascule automatiquement vers HTTPS. Cela garantit la validation côté client d'une connexion sécurisée ainsi que la validation côté serveur dans IIS. Le navigateur Web conserve cette validation pendant une période définie.

Sur Windows Server 2019 et versions ultérieures :

1. Ouvrez le **Gestionnaire des services Internet Information Services (IIS)**.
2. Sélectionnez le **site Web par défaut** (ou le site Web approprié).
3. Dans le volet Actions sur le côté droit, cliquez sur **HSTS…**
4. Cochez **Activer**, entrez l'âge maximal du cache, par exemple 31536000 pour un an et cochez **Rediriger HTTP vers HTTPS**.
5. Sélectionnez **OK**.



> **Remarque :**
>
> L'activation du protocole HSTS affecte tous les sites Web du même domaine. Par exemple, si le site Web est accessible sur https://www.company.com/Citrix/StoreWeb, la stratégie HSTS s'applique à tous les sites Web sous https://www.company.com, ce qui n'est peut-être pas souhaitable.

Sécuriser votre déploiement StoreFront

May 30, 2024

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.

Communication entre les utilisateurs et StoreFront

Citrix vous recommande de sécuriser les communications entre les machines des utilisateurs et StoreFront à l'aide du protocole HTTPS. Cela garantit que les mots de passe et autres données envoyés entre le client et StoreFront sont cryptés. De plus, les connexions HTTP simples peuvent être compromises par diverses attaques, telles que les attaques de type « man-in-the-middle », en particulier lorsque les connexions sont établies à partir d'emplacements non sécurisés tels que des hotspots Wi-Fi publics. En l'absence de la configuration IIS appropriée, StoreFront utilise le protocole HTTP pour les communications.

Selon votre configuration, les utilisateurs peuvent accéder à StoreFront via une passerelle ou un équilibreur de charge. Vous pouvez mettre fin à la connexion HTTPS au niveau de la passerelle ou de l'équilibreur de charge. Toutefois, dans ce cas, Citrix vous recommande toujours de sécuriser les connexions entre la passerelle ou l'équilibreur de charge et StoreFront à l'aide du protocole HTTPS.

Pour activer le protocole HTTPS, désactiver le protocole HTTP et activer le protocole HSTS, consultez Sécurisation de StoreFront avec HTTPS.

Communications entre StoreFront et les serveurs Citrix Virtual Apps and Desktops

Citrix recommande d'utiliser le protocole HTTPS pour sécuriser le transfert de données entre StoreFront et vos Delivery Controller Citrix Virtual Apps and Desktops. Consultez Installer les certificats de serveur TLS sur des Controller. StoreFront ne prend pas en charge les protocoles TLS 1.0 ou TLS 1.1 entre StoreFront et le Delivery Controller. Vous pouvez également configurer Windows pour sécuriser la communication entre les serveurs à l'aide d'IPsec.

Vous pouvez configurer le Delivery Controller et StoreFront pour vous assurer que seuls les serveurs StoreFront de confiance peuvent communiquer avec le Delivery Controller. Consultez Gérer les clés de sécurité.

Communications StoreFront avec les Cloud Connector

Citrix recommande d'utiliser le protocole HTTPS pour sécuriser le transfert de données entre StoreFront et vos Cloud Connector. Découvrez comment activer le protocole SSL sur les Cloud Connector pour sécuriser le trafic XML. StoreFront ne prend pas en charge les protocoles TLS 1.0 ou TLS 1.1 entre StoreFront et les Cloud Connector. Vous pouvez également configurer Windows pour sécuriser la communication entre les serveurs à l'aide d'IPsec.

Accès distant

Citrix ne recommande pas d'exposer votre serveur StoreFront directement sur Internet. Citrix recommande d'utiliser une passerelle Citrix Gateway pour fournir l'authentification et l'accès aux utilisateurs distants.

Renforcement de 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 utiliser le filtrage des requêtes pour configurer une liste d'extensions de fichiers autorisées et interdire les extensions de nom de fichier non répertoriées. Consultez la documentation IIS.

StoreFront requiert les extensions de nom de fichier suivantes :

- . (extension vierge)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .png
- .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 le site Web d'un magasin, 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
- .wasm

Verbes

Vous pouvez utiliser le filtrage des requêtes pour configurer une liste de verbes autorisés et interdire les verbes non répertoriés. Consultez la documentation IIS.

- GET
- POST
- HEAD

Caractères non ASCII dans les URL

Si vous vous assurez que le nom du magasin et le nom du site Web n'utilisent que des caractères ASCII, les URL de StoreFront ne contiendront pas de caractères ASCII. Vous pouvez utiliser le filtrage des demandes pour interdire les caractères non ASCII. Consultez la documentation IIS.

Types MIME

Vous pouvez supprimer les types MIME du shell du système d'exploitation correspondant aux extensions de fichiers suivantes :

- .exe
- .dll
- .com
- .bat
- .csh

Consultez la documentation IIS.

Supprimer l'en-tête X-Powered-By

Par défaut, IIS indique qu'il utilise ASP.NET en ajoutant un en-tête `X-Powered-By` avec la valeur `ASP.NET`. Vous pouvez configurer IIS pour supprimer cet en-tête. Consultez la documentation IIS sur les en-têtes personnalisés.

Supprimer l'en-tête Server avec la version IIS

Par défaut, IIS indique la version d'IIS en ajoutant un en-tête `Server`. Vous pouvez configurer IIS pour supprimer cet en-tête. Consultez la documentation IIS sur le filtrage des demandes.

Déplacer le site Web StoreFront vers une partition distincte

Vous pouvez héberger les sites Web StoreFront sur une partition distincte de celle des fichiers système. Dans IIS, vous devez déplacer le **site Web par défaut** ou créer un site distinct sur la partition appropriée avant de créer votre déploiement StoreFront.

Fonctionnalités IIS

Pour obtenir la liste des fonctionnalités IIS installées et utilisées par StoreFront, consultez la section Configuration système requise. Vous pouvez supprimer d'autres fonctionnalités IIS.

Bien que StoreFront n'utilise pas directement les filtres ISAPI, cette fonctionnalité est requise par ASP.NET et ne peut donc pas être désinstallée.

Mappages de gestionnaires

StoreFront requiert les mappages de gestionnaires suivants. Vous pouvez supprimer d'autres mappages de gestionnaires.

- ExtensionlessUrlHandler-Integrated-4.0
- PageHandlerFactory-Integrated-4.0
- StaticFile

Consultez la documentation IIS sur les gestionnaires.

Filtres ISAPI

StoreFront ne requiert aucun filtre ISAP. Vous pouvez supprimer tous les filtres ISAPI. Consultez la documentation IIS sur les filtres ISAPI.

Règles d'autorisation .NET

Par défaut, la « règle d'autorisation .NET » est définie sur Autoriser tous les utilisateurs sur les serveurs IIS. Par défaut, le site Web utilisé par StoreFront hérite de cette configuration.

Si vous supprimez ou modifiez la règle d'autorisation .NET au niveau du serveur, vous devez remplacer les règles du site Web utilisé par StoreFront pour ajouter une règle d'autorisation pour « Tous les utilisateurs » et supprimer toute autre règle.

Mode Retail

Vous pouvez activer le mode Retail, consultez la documentation IIS.

Pools d'applications

StoreFront crée les pools d'applications suivants :

- API de configuration Citrix
- Authentification Citrix Delivery Services
- Ressources de Citrix Delivery Services
- Citrix Receiver pour Web

Ne modifiez pas les pools d'applications utilisés par chaque application IIS ni l'identité de chaque pool. Si vous utilisez plusieurs sites, il n'est pas possible de configurer chaque site pour qu'il utilise des pools d'applications distincts.

Dans les paramètres Recyclage, vous pouvez définir le délai d'inactivité du pool d'applications et la limite de mémoire virtuelle. Notez que lorsque le pool d'applications « Citrix Receiver pour Web » est recyclé, les utilisateurs connectés via un navigateur Web sont déconnectés. Par conséquent, le recyclage est configuré par défaut à 2 h 00 chaque jour afin de minimiser les perturbations. Si vous modifiez l'un des paramètres de recyclage, cela peut entraîner la déconnexion des utilisateurs à d'autres moments de la journée.

Paramètres requis

- Ne modifiez pas les paramètres d'authentification IIS. StoreFront gère l'authentification et configure les répertoires du site StoreFront avec les paramètres d'authentification appropriés.
- Pour le serveur StoreFront sous **Paramètres SSL**, ne sélectionnez pas **Certificats clients : Exiger**. L'installation de StoreFront configure les pages appropriées du site StoreFront avec ce paramètre.
- StoreFront requiert des cookies pour l'état de la session et pour d'autres fonctionnalités. Dans certains répertoires, sous **État de la session**, **Paramètres des cookies**, le paramètre **Mode** doit être défini sur **Utiliser les cookies**.
- StoreFront exige que le paramètre **Niveau de confiance .NET** soit défini sur **Confiance totale**. Ne définissez pas le niveau de confiance .NET sur une autre valeur.

Services

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)

Ces comptes se connectent en tant que `Network Service`. Ne modifiez pas cette configuration.

Si vous configurez la délégation Kerberos contrainte de StoreFront pour XenApp 6.5, le service Citrix StoreFront Protocol Transition (NT SERVICE\CitrixStoreFrontProtocolTransition) est également créé. Ce service fonctionne en tant que `NT AUTHORITY\SYSTEM`. Ne modifiez pas cette configuration.

Attribution des droits d'utilisateur

La modification de l'attribution des droits d'utilisateur par rapport aux valeurs par défaut peut entraîner des problèmes avec StoreFront. En particulier :

- 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 l'installez, StoreFront crée des pools d'applications auxquels IIS accorde les droits d'utilisateur **Ouvrir une session en tant que service**, **Ajuster les quotas de mémoire pour un processus**, **Générer des audits de sécurité** et **Remplacer un jeton de niveau processus**.
- Pour créer ou modifier un déploiement, l'administrateur doit disposer des droits permettant de **Restaurer les fichiers et les répertoires**.
- Pour qu'un serveur rejoigne un groupe de serveurs, le groupe Administrateurs doit disposer des droits **Restaurer les fichiers et les répertoires**, **Accéder à cet ordinateur à partir du réseau** et **Gérer le journal d'audit et de sécurité**.
- Pour que les utilisateurs puissent se connecter à l'aide d'un nom d'utilisateur et d'un mot de passe (directement ou via une passerelle), ils doivent disposer du droit « Autoriser la connexion en local », sauf si vous avez configuré StoreFront pour valider les mots de passe via Delivery Controller.

Cette liste n'est pas exhaustive et d'autres droits d'accès utilisateur peuvent être requis.

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
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- 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.

NTLM

StoreFront utilise NTLM pour s'authentifier entre les serveurs d'un groupe de serveurs. Si vous désactivez NTLM, StoreFront ne peut pas synchroniser les données entre les serveurs StoreFront d'un groupe de serveurs.

Vous pouvez configurer le serveur pour utiliser uniquement NTLMv2 et rejeter NTLMv1, consultez la documentation Microsoft.

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 plus d'informations, consultez Communication entre les utilisateurs et StoreFront et Signature du fichier ICA.

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*>\Scripts. L'installation de StoreFront par défaut ne peut pas utiliser ces scripts. Ils simplifient les étapes de configuration des tâches spécifiques ou non fréquentes. Ces scripts sont signés, ce qui permet à StoreFront de prendre en charge la stratégie d'exécution PowerShell. Nous recommandons la stratégie **AllSigned**. (La stratégie **Restreint** n'est pas prise en charge car elle empêche l'exécution des scripts PowerShell.) StoreFront ne modifie pas la stratégie d'exécution de PowerShell.

Bien que StoreFront n'installe pas de certificat de signature de code dans le magasin Éditeurs approuvés, Windows peut automatiquement y ajouter le certificat de signature de code. Cela se produit lorsque le script PowerShell est exécuté avec l'option **Toujours exécuter**. (Si vous sélectionnez l'

option **Ne jamais exécuter**, le certificat est ajouté au magasin Certificats non autorisés, et les scripts PowerShell StoreFront ne seront pas exécutés.) Une fois que le certificat de code de signature a été ajouté au magasin Éditeurs approuvés, sa date d'expiration n'est plus vérifiée par Windows. Vous pouvez supprimer ce certificat du magasin Éditeurs approuvés après que les tâches StoreFront ont été effectuées.

Désactivation des anciennes versions TLS

Citrix vous recommande de désactiver les protocoles TLS 1.0 et 1.1 pour les communications client et serveur sur le serveur Windows. Vous pouvez le faire via la stratégie de groupe ou via les paramètres de registre Windows. Consultez la documentation Microsoft.

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.

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 qui ouvrent une session via un navigateur Web 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 modifier leurs mots de passe, même s'

ils ont expiré. Pour plus d'informations, consultez la section Autoriser les utilisateurs à modifier leurs mots de passe.

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 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.

En-têtes de sécurité

Lorsque vous consultez le site Web d'un magasin via un navigateur Web, StoreFront renvoie les en-têtes de sécurité suivants qui imposent des restrictions au navigateur Web.

Nom de l'en-tête	Valeur	Description
`content-security-policy`	`frame-ancestors 'none'`	Cela empêche d'autres sites d'intégrer des sites Web StoreFront dans un cadre, ce qui évite les attaques de détournement de clic. StoreFront utilise des scripts et des styles intégrés. Il n'est donc pas possible d'utiliser une stratégie de sécurité du contenu qui les bloque. Les sites Web StoreFront n'affichent que le contenu configuré par les administrateurs et n'affichent aucun contenu saisi par l'utilisateur. Il n'est donc pas nécessaire de bloquer les scripts intégrés.
`X-Content-Type-Options`	`nosniff`	Cela permet d'éviter la détection malveillante de type MIME.

Nom de l'en-tête	Valeur	Description
`X-Frame-Options`	`deny`	Cela empêche d'autres sites d'intégrer des sites Web StoreFront dans un cadre, ce qui évite les attaques de détournement de clic. Ce paramètre est rendu obsolète par `content-security-policy` avec la définition de `frame-ancestors 'none'` mais est compris par certains navigateurs plus anciens qui ne prennent pas en charge `content-security-policy`.
`X-XSS-Protection`	`1; mode=block`	Utilisé par certains navigateurs pour atténuer les attaques par script intersites (XSS).

Cookies

StoreFront utilise plusieurs cookies. Certains des cookies utilisés dans le cadre du fonctionnement du site Web sont les suivants :

Cookie	Description
`ASP.NET_SessionId`	Suit la session de l'utilisateur, y compris l'état d'authentification. Le paramètre `HttpOnly` est défini.
`CtxsAuthId`	Pour empêcher les attaques de réparation de session, StoreFront vérifie en outre si l'utilisateur est authentifié à l'aide de ce cookie. Le paramètre `HttpOnly` est défini.

Cookie	Description
`CsrfToken`	Utilisé pour empêcher la falsification de requêtes intersites via le modèle standard de jeton cookie-to-header. Le serveur définit un jeton dans le cookie. Le client lit le jeton à partir du cookie et inclut le jeton dans la chaîne de requête ou dans un en-tête dans les requêtes suivantes. Le paramètre `HttpOnly` ne doit pas être défini sur ce cookie pour que le JavaScript du client puisse le lire.
`CtxsDeviceId`	Identifie l'appareil. Le paramètre `HttpOnly` est défini.

StoreFront définit un certain nombre d'autres cookies pour suivre l'état des utilisateurs, dont certains qui doivent être lus par JavaScript et sur lesquels le paramètre `HttpOnly` ne doit pas être défini. Ces cookies ne contiennent aucune information relative à l'authentification ni aucune autre information confidentielle.

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.

Découverte de compte basée sur une adresse e-mail

August 25, 2023

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 sans avoir besoin de connaître l'URL du magasin en entrant leurs adresses 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. Si l'utilisateur saisit une adresse e-mail, l'application Citrix Workspace recherche le domaine de messagerie à plusieurs emplacements afin de déterminer le serveur StoreFront. Il répertorie ensuite tous les magasins visibles parmi lesquels l'utilisateur peut choisir.

Citrix recommande d'utiliser le Global App Config Service pour configurer la découverte basée sur une adresse e-mail. Vous pouvez également configurer la découverte basée sur une adresse e-mail à l'aide d'enregistrements SVR DNS ou d'un alias DNS.

Global App Config Service

Pour configurer la découverte basée sur une adresse e-mail à l'aide du service Global App Config, consultez la section Configurer la découverte basée sur une adresse e-mail.

Enregistrements SVR DNS

Comme alternative au service Global App Config, vous pouvez utiliser les enregistrements SVR DNS pour configurer le serveur StoreFront que l'application Citrix Workspace doit utiliser pour un domaine de messagerie.

Sur votre serveur DNS pour votre domaine de messagerie, ajoutez un enregistrement **SRV** avec les propriétés suivantes :

Propriété	Valeur
Service	_citrixreceiver
Proto	TCP
Cible	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.

Enregistrement DNS discoverReceiver

Pour revenir aux autres méthodes, vous pouvez créer un alias DNS pour le serveur StoreFront `discoverReceiver` sur le domaine de messagerie. Par exemple, si votre domaine de messagerie est `example.com`, créez un alias DNS appelé `discoverReceiver.example.com`. Si aucun enregistrement SRV n'est détecté, l'application Citrix Workspace recherche une machine appelée « discoverReceiver » afin d'identifier un serveur StoreFront.

Si vous utilisez ce mécanisme, assurez-vous que `discoverReceiver` figure en tant que nom alternatif de l'objet dans le certificat HTTPS de votre serveur StoreFront.

Créer un nouveau déploiement

December 6, 2023

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. S'il existe plusieurs sites IIS, choisissez dans la liste déroulante des sites **IIS** le site que vous souhaitez utiliser.
4. Si vous utilisez un seul serveur StoreFront, entrez l'URL du serveur (**URL de base**). Si vous comptez configurer plusieurs serveurs StoreFront derrière un équilibrage de charge, entrez l'URL d'équilibreur de charge comme **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.
5. Cliquez sur **Suivant** et configurez votre premier magasin comme décrit dans Créer un magasin.
6. Une fois que vous avez terminé toutes les étapes de configuration, cliquez sur **Créer** pour créer le déploiement et le magasin.
7. StoreFront affiche un résumé du magasin qui vient d'être créé. Cliquez sur **Terminer**.

Créer un déploiement à l'aide du SDK PowerShell

Pour créer un déploiement à l'aide du SDK PowerShell, exécutez l'applet de commande Add-STFDeployment.

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.

Pour créer plusieurs sites Web, consultez la documentation Microsoft IIS.

Il n'est pas possible de créer plusieurs déploiements StoreFront à l'aide de la console de gestion ; vous devez utiliser le SDK PowerShell. Par exemple, pour créer deux déploiements de sites Web IIS, l'un pour les applications et l'autre pour les bureaux, utilisez les commandes suivantes :

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"
Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
<!--NeedCopy-->
```

Une fois que vous avez activé plusieurs sites, StoreFront désactive la console de gestion et il n'est pas possible de faire revenir StoreFront en mode site unique. Vous devez configurer les sites à l'aide du SDK StoreFront et inclure `SiteID` dans chaque commande.

Joindre un groupe de serveurs existant

December 6, 2023

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.

> **Remarque :**
>
> Pour obtenir des recommandations sur la taille des groupes de serveurs, consultez Groupes de

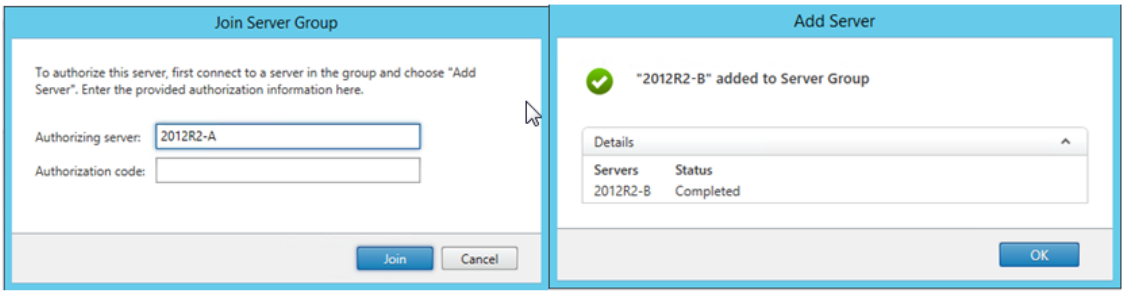
> serveurs StoreFront.

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. Consultez 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 empêcher l'ajout de nouveaux membres au groupe d'administrateurs locaux ou que vous limitez les autorisations du groupe d'administrateurs locaux sur vos serveurs, StoreFront ne peut pas s'associer à un groupe de serveurs.

1. Si la console de gestion Citrix StoreFront n'est pas déjà ouverte après installation de StoreFront, sur l'écran Démarrer de Windows où l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus.
2. Dans le panneau des résultats de la console de gestion Citrix StoreFront, cliquez sur **Joindre un groupe de serveurs existant**.
3. Connectez-vous à un serveur du déploiement StoreFront que vous souhaitez rejoindre et ouvrez la console de gestion Citrix StoreFront. Sélectionnez le nœud Groupe de serveurs dans le panneau gauche de la console puis, dans le panneau Actions, cliquez sur **Ajouter un serveur**. Notez le code d'autorisation qui s'affiche.
4. Retournez sur le nouveau serveur et, dans la boîte de dialogue Joindre groupe de serveurs, spécifiez le nom du serveur existant dans la zone Serveur d'autorisation. Saisissez le code d'autorisation que vous avez obtenu auprès de ce serveur, puis cliquez sur **Joindre**.

   Une fois joint au groupe, la configuration du nouveau serveur est mise à jour pour correspondre à la configuration du serveur existant. Tous les autres serveurs du groupe sont mis à jour avec les détails du nouveau serveur.



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

Mettre à niveau StoreFront

May 30, 2024

La mise à niveau préserve votre configuration de StoreFront et conserve les favoris des utilisateurs intacts. En revanche, la désinstallation de StoreFront supprime StoreFront et les services, les sites et les favoris (sur des serveurs autonomes) associés, ainsi que la configuration associée.

Prendre en charge les chemins de mise à niveau

Vous pouvez passer à StoreFront 2402 depuis :

- StoreFront 2311
- StoreFront 2308
- StoreFront 2203 LTSR (n'importe quelle CU)
- StoreFront 1912 LTSR (n'importe quelle CU)
- StoreFront 3.12 LTSR CU9

Pour effectuer une mise à niveau depuis des versions antérieures à la version 3.12 CU9, vous devez d'abord effectuer une mise à niveau vers StoreFront 3.12 CU9.

> **Avertissement :**
>
> Lorsque vous effectuez une mise à niveau depuis des versions antérieures à 1912, tous les sites Desktop Appliance de votre déploiement sont automatiquement supprimés. Citrix recommande également d'utiliser l'application Citrix Workspace Desktop Lock pour tous les cas d'utilisation ne faisant pas partie d'un domaine.

À savoir

- La mise à niveau vers la dernière version de StoreFront à partir d'une version plus ancienne qui est en fin de vie n'est pas prise en charge. Pour plus d'informations, voir 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.
- 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.
- 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 de StoreFront que vous avez exportée avant la mise à niveau (voir Exporter et importer la configuration de StoreFront)
  - Suivre les conseils de dépannage de 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.
- Vérifiez que vous ne tentez pas de mise à niveau à partir d'une version StoreFront en fin de vie. Pour plus d'informations, voir CTX200356.
- Vérifiez que vous effectuez une mise à niveau d'une version prise en charge de StoreFront vers la version actuelle uniquement.
- Téléchargez le programme d'installation de StoreFront sur le site Web de Citrix.

Mettre à niveau un serveur StoreFront unique

1. Sauvegardez le serveur en créant un instantané de la VM.
2. Exportez la configuration de StoreFront existante. Si vous avez plusieurs serveurs dans un groupe de serveurs, exportez uniquement la configuration du groupe de serveurs à partir d'un

seul 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, de sorte que vous puissiez facilement restaurer la configuration en cas de problème. Notez que vous ne pourrez restaurer cette sauvegarde que sur un serveur exécutant la même version que celle depuis laquelle elle a été exportée.

3. Si vous avez apporté des modifications aux fichiers dans `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, tels que default.ica et usernamepassword.tfrm, sauvegardez-les pour chaque magasin. Après la mise à niveau, vous pouvez les restaurer pour rétablir vos modifications.
4. Empêchez les utilisateurs de se connecter en supprimant le serveur de tout équilibreur de charge ou en bloquant les connexions.
5. Redémarrez le serveur.
6. Assurez-vous qu'aucune application n'est en cours d'exécution, y compris la console de gestion StoreFront, les fenêtres de ligne de commande et PowerShell ou toute autre application susceptible de verrouiller les fichiers StoreFront. 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.
7. Assurez-vous qu'aucun explorateur Windows ou aucune invite de commande n'est ouvert sur les répertoires contenant des fichiers StoreFront.
8. Désactivez toutes les applications antivirus.
9. Exécutez le fichier d'installation de la version requise 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. La mise à niveau simultanée des serveurs d'un groupe de serveurs StoreFront n'est pas prise en charge.

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 suivant les instructions de la section Mettre à niveau un serveur StoreFront unique.
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 la configuration de StoreFront à l'aide de **Export-STFConfiguration**. Cette sauvegarde est nécessaire car les serveurs sont réinitialisés aux paramètres d'usine plus tard dans le processus, ce qui supprime les données de configuration.
2. 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 de configuration. Consultez Gérer les données d'abonnement d'un magasin.
3. Désactivez l'accès des utilisateurs au serveur C en le supprimant de l'équilibreur de charge. Cela empêche les utilisateurs de se connecter au serveur C pendant le processus de mise à niveau. L'équilibreur de charge continue d'envoyer des requêtes aux serveurs A et B.

4. 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.
5. Réinitialisez les paramètres d'usine par défaut du serveur orphelin C à l'aide de **Clear-STFDeployment**.
6. Importez la configuration de StoreFront que vous avez précédemment exportée sur le serveur C à l'aide de **Import-STFConfiguration**. Le serveur C a désormais une configuration identique à l'ancien groupe de serveurs. Il *n'est pas* nécessaire de répéter cette étape plus tard. Un seul serveur a besoin d'une copie des données de configuration pour les propager sur les autres serveurs qui sont associés au groupe.
7. Mettez à niveau le serveur C en suivant les instructions de la section Mettre à niveau un serveur StoreFront unique. 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.
8. 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.
9. Répétez les étapes 3, 4, 5 et 7 à l'aide du serveur B (ne répétez pas l'étape 6). Pendant ce temps, seul le serveur A fournit aux utilisateurs l'accès aux ressources. Il est donc recommandé d'effectuer cette étape pendant les périodes de travail plus calmes, où la charge sur le groupe de serveurs StoreFront devrait être minime.
10. 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).
11. Ajoutez les serveurs B et C au service d'équilibrage de charge afin qu'ils puissent prendre la place du serveur A.
12. Supprimez le serveur A du service d'équilibrage de charge afin que les utilisateurs soient redirigés vers les serveurs B et C récemment mis à niveau.
13. Répétez les étapes 3, 4, 5 et 7 à l'aide du serveur A (ne répétez pas l'étape 6). 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.

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 plus de détails sur les fichiers journaux, consultez la section Journaux d'installation.

Réinitialiser les paramètres d'usine du serveur

August 25, 2023

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')
<!--NeedCopy-->
```

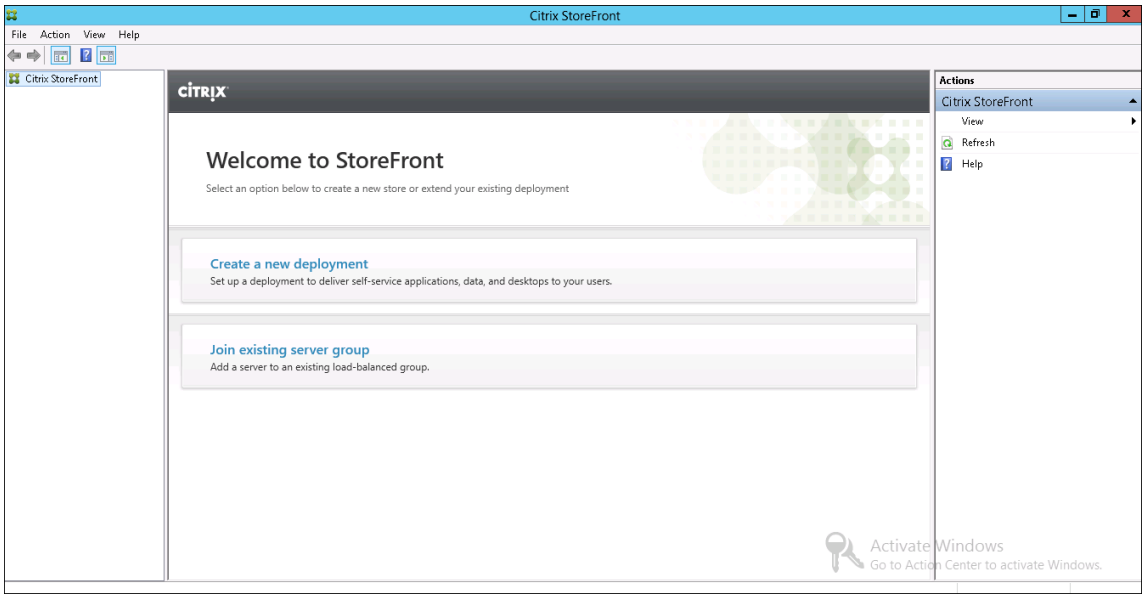
4. Importez le module Citrix StoreFront.

```
Import-Module citrix.storefront -verbose
<!--NeedCopy-->
```

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

```
Clear-STFDeployment -Confirm $False
<!--NeedCopy-->
```

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.



Désinstallez StoreFront

February 22, 2024

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 de gestion StoreFront si elle est ouverte.
3. Fermez toutes les sessions PowerShell qui ont pu être utilisées pour gérer StoreFront via son SDK PowerShell.
4. Ouvrez le menu **Démarrer**, sélectionnez **Paramètres** (icône en forme d'engrenage), puis accédez à **Applications**.
5. Dans les fenêtres **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**.

Pour supprimer manuellement StoreFront

Après avoir désinstallé StoreFront, pour vous assurer que StoreFront est complètement supprimé :

1. Supprimez le rôle serveur Web.
2. Supprimez le dossier *C:\Program Files\Citrix\Receiver StoreFront*.
3. Supprimez tous les sous-répertoires sous *C:\Program Files\Citrix\StoreFront Install*.
4. Supprimez le dossier *C:\Inetpub*.

Vous pouvez désormais réinstaller StoreFront.

Journaux d'installation

Pour plus de détails sur les fichiers journaux, consultez la section Journaux d'installation.

Configurer l'authentification et la délégation

December 6, 2023

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

Méthode	Détails
Configuration de l'authentification	Configurer les méthodes que les utilisateurs peuvent utiliser pour se connecter à StoreFront via l'application Citrix Workspace.
Authentification par carte à puce	Configurer l'authentification par carte à puce.
Authentification par nom d'utilisateur et mot de passe	Autoriser les utilisateurs à s'authentifier à l'aide de leur nom d'utilisateur et de leur mot de passe Active Directory et configurer les options de modification des mots de passe et les notifications d'expiration des mots de passe.
Authentification pass-through au domaine	Autoriser les appareils Windows à effectuer une connexion unique à l'aide de leurs informations d'identification Windows.
Authentification SAML	Déléguer l'authentification à des fournisseurs d'identité tiers à l'aide de SAML.
Configuration du Service d'authentification fédérée	Configurer StoreFront pour l'intégrer au Service d'authentification fédérée pour l'authentification unique aux VDA

Configuration de l'authentification

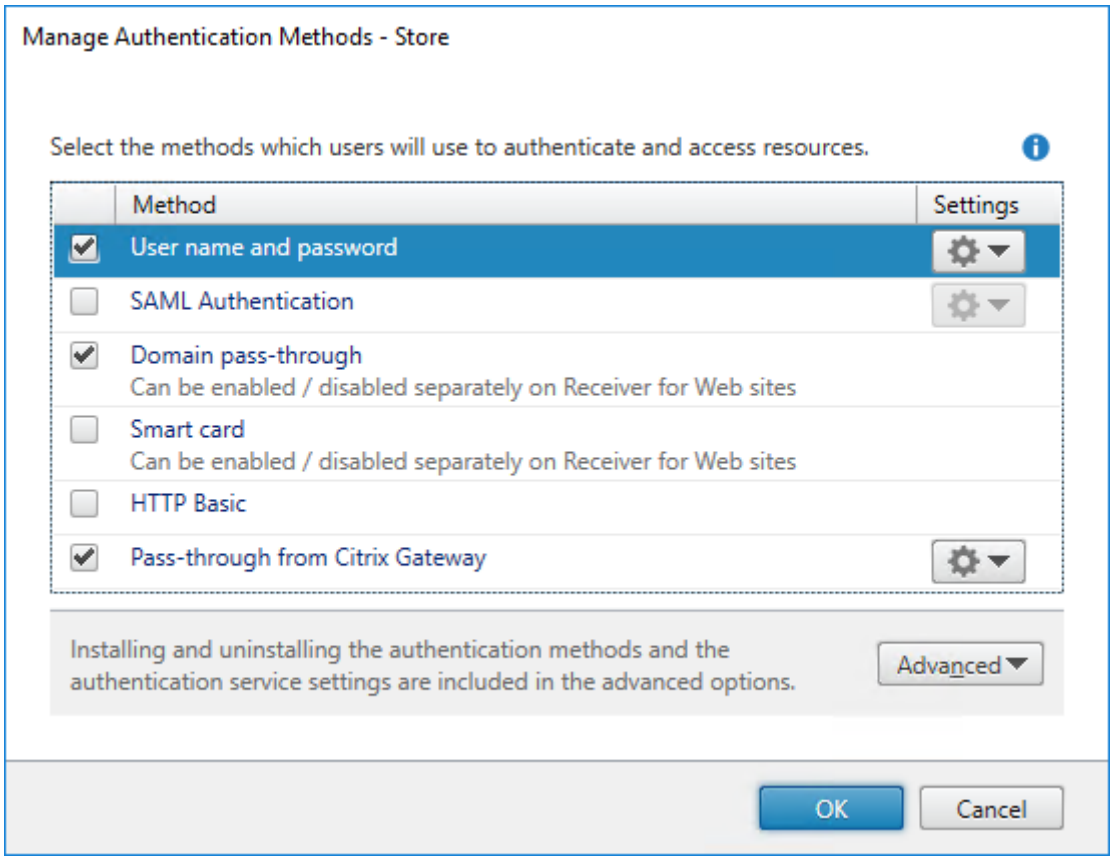
February 22, 2024

Gérer les méthodes d'authentification

Pour chaque magasin, vous pouvez choisir une ou plusieurs méthodes d'authentification disponibles lorsque vous vous connectez au magasin via l'application Citrix Workspace.

1. 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**.

2. 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 par nom d'utilisateur et mot de passe Active Directory. Pour plus d'informations, consultez Authentification par nom d'utilisateur et mot de passe.
- Sélectionnez la case **Authentification SAML** pour activer l'intégration avec un fournisseur d'identité SAML. Pour plus d'informations, consultez Authentification SAML.
- 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. Pour plus d'informations, consultez la section Authentification pass-through au domaine.
- Sélectionnez **Carte à puce** pour activer l'authentification par carte à puce. Pour plus d'informations, consultez Authentification par carte à puce.
- 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. Activez cette option si les utilisateurs se connectent à StoreFront via Citrix Gateway avec l'authentification activée. Pour plus d'informations, consultez Authentification pass-through via Citrix Gateway.

La modification des méthodes d'authentification d'un magasin met également à jour les méthodes d'authentification utilisées lors de l'accès au magasin via un navigateur Web. Pour modifier les méthodes d'authentification lors de la connexion via un navigateur Web, reportez-vous à la section Méthodes d'authentification.

Gérer les méthodes d'authentification à l'aide du SDK PowerShell

Pour configurer l'authentification à l'aide du SDK PowerShell, procédez comme suit :

1. Exécutez Get-STFAuthenticationService pour obtenir le service d'authentification d'un magasin ou d'un répertoire virtuel et pour consulter sa configuration actuelle.
2. Sur le service d'authentification, activez ou désactivez les protocoles d'authentification requis. Pour obtenir la liste des protocoles disponibles, exécutez Get-STFAuthenticationServiceProtocol. Pour activer les protocoles, exécutez Enable-STFAuthenticationServiceProtocol avec la liste des protocoles à activer. Pour désactiver les protocoles, exécutez Disable-STFAuthenticationServiceProtocol avec la liste des protocoles à désactiver.
3. Configurez les protocoles d'authentification que vous avez activés. Pour plus de détails, consultez la documentation de chaque protocole.

Paramètres du service d'authentification partagé

Utilisez la tâche Paramètres du service d'authentification partagé pour spécifier les magasins qui partagent le service d'authentification activant l'authentification unique entre eux.

1. Sélectionnez le nœud **Magasins** 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**.
2. Dans le menu déroulant **Avancé**, sélectionnez **Paramètres du service d'authentification partagé**.
3. 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.

Authentification par carte à puce

April 17, 2024

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, des navigateurs 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 Endpoint Management. Toutefois, les utilisateurs doivent s'authentifier à nouveau pour accéder aux applications Web de Endpoint Management 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.

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.

Pré-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.
- Assurez-vous 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 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. Voir Accès sécurisé à StoreFront à l'aide de HTTPS.
- Pour activer l'authentification par carte à puce lors de la connexion à un magasin via l'application Citrix Workspace, cochez ou décochez la case **Carte à puce** dans Méthodes d'authentification.
- L'activation par défaut de l'authentification par carte à puce pour un magasin l'active également pour tous les sites Web de ce magasin. Vous pouvez activer ou désactiver indépendamment l'authentification par carte à puce pour un site Web spécifique dans l'onglet Méthodes d'authentification - Gérer les sites Receiver pour Web.
- Si vous configurez l'authentification par carte à puce et par nom d'utilisateur et mot de passe, 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.

Configurer Delivery Controller pour qu'il approuve StoreFront

Lorsque vous utilisez l'authentification par carte à puce, StoreFront n'a pas accès aux informations d'identification de l'utilisateur et ne peut donc pas s'authentifier auprès de Citrix Virtual Apps and Desk-

tops. Vous devez donc configurer le Delivery Controller pour qu'il approuve les demandes provenant de StoreFront. Consultez les considérations et les meilleures pratiques relatives à la sécurité de Citrix Virtual Apps and Desktops.

Accès à distance via Citrix Gateway

Pour l'accès à distance, vous pouvez activer la carte à puce sur Citrix Gateway, puis activer l'authentification pass-through à StoreFront à l'aide de l'authentification déléguée. Pour plus de détails, consultez Authentification pass-through passerelle.

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 une deuxième passerelle et désactivez l'authentification du client dans les paramètres SSL (Secure Sockets Layer). Pour plus d'informations, veuillez consulter la section Configuration de l'authentification par carte à puce. Lorsque vous accédez à StoreFront via une passerelle avec authentification par carte à puce. Configurez le routage Citrix Gateway optimal via ce serveur virtuel pour les connexions aux déploiements fournissant des bureaux et des applications au magasin. Pour plus d'informations, consultez la section Configurer un routage HDX optimal pour un magasin.

Authentification unique aux VDA

Vous pouvez activer l'authentification unique pour les VDA en transmettant les informations d'identification des cartes à puce des utilisateurs. Le magasin est accessible via un navigateur Web ou l'application Citrix Workspace pour Windows, mais la ressource doit être ouverte dans l'application Citrix Workspace pour Windows. Sur d'autres systèmes d'exploitation ou lorsqu'ils accèdent aux ressources via un navigateur, les utilisateurs doivent saisir à nouveau leurs informations d'identification lorsqu'ils se connectent à un VDA.

1. Incluez le composant Single Sign On lors de l'installation de Citrix Workspace pour Windows et configurez-le pour l'authentification unique. Voir Configurer l'authentification pass-through au domaine.
2. Utilisez un éditeur de texte pour ouvrir le fichier default.ica du magasin. Consultez Paramètres de default.ica.
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].

   ```
   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.

4. 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.

Connexion via authentification unique aux VDA à l'aide de FAS

Vous pouvez également configurer le service d'authentification fédérée pour la connexion via authentification unique aux VDA lorsque vous utilisez l'application Citrix Workspace installée localement, mais pas l'application Citrix Workspace pour HTML5.

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 alors que celle-ci se trouve 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 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 Workspace pour Windows équipés de machines appartenant à un domaine accédant 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.

Authentification pass-through au domaine

April 17, 2024

Les utilisateurs s'authentifient sur leurs ordinateurs Windows membres d'un domaine et leurs informations d'identification sont utilisées pour les connecter automatiquement à l'application Citrix Workspace. Cette méthode est prise en charge par l'application Citrix Workspace pour Windows et par les navigateurs Web suivants sous Windows :

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

Configuration de StoreFront

Pour activer l'authentification pass-through au domaine pour l'application Citrix Workspace pour Windows, dans les méthodes d'authentification, sélectionnez **Authentification pass-through au domaine**.

L'activation par défaut de l'authentification pass-through au domaine pour un magasin l'active également pour l'application Citrix Workspace pour HTML5 pour tous les sites Web de ce magasin. Vous pouvez désactiver l'authentification pass-through au domaine pour un site Web spécifique dans l'onglet Gérer les sites Receiver pour Web - Méthodes d'authentification.

Configurer Delivery Controller pour qu'il approuve StoreFront

Lorsque vous utilisez l'authentification pass-through au domaine, StoreFront n'a pas accès aux informations d'identification de l'utilisateur et ne peut donc pas s'authentifier auprès de Citrix Virtual Apps and Desktops. Vous devez donc configurer le Delivery Controller pour qu'il approuve les demandes provenant de StoreFront. Consultez les considérations et les meilleures pratiques relatives à la sécurité de Citrix Virtual Apps and Desktops.

Authentification unique aux VDA

Pour vous connecter via authentification unique aux VDA, vous devez utiliser l'application Citrix Workspace pour Windows avec le composant **Activer l'authentification unique**. Reportez-vous à la section Configurer l'authentification pass-through au domaine. Si vous utilisez l'application Citrix Workspace pour HTML5, elle doit être configurée pour se connecter aux ressources de l'application Citrix Workspace pour Windows plutôt qu'au navigateur.

Configuration de l'application Citrix Workspace pour Windows

Pour activer l'authentification pass-through au domaine vers l'authentification unique au magasin et aux VDA à l'aide de l'application Citrix Workspace pour Windows, consultez la documentation de l'application Citrix Workspace pour Windows.

Configuration de l'application Citrix Workspace pour HTML5

Vous devrez peut-être mettre à jour la configuration du navigateur Web des utilisateurs pour autoriser l'authentification pass-through au domaine. Vous pouvez utiliser l'authentification pass-through au domaine pour vous connecter à un magasin via un navigateur Web. Pour utiliser l'authentification unique pour les VDA, les utilisateurs doivent ouvrir des ressources dans l'application Citrix Workspace pour Windows plutôt que dans le navigateur Web.

Internet Explorer, Edge et Chrome La plupart des navigateurs Web utilisent la configuration des zones de Windows Internet Explorer pour décider d'activer ou non l'authentification unique. Par défaut, elle n'est activée que pour les sites de la zone d'intranet locale. Pour ajouter votre site à la zone intranet :

1. Ouvrez le panneau de configuration.
2. Ouvrez les options Internet.
3. Accédez à l'onglet **Sécurité**.
4. Sélectionnez **Intranet local**.
5. Cliquez sur **Sites**.
6. Cliquez sur **Avancé**.
7. Ajoutez votre site Web StoreFront.

Ces paramètres peuvent être déployés à l'aide d'une stratégie de groupe.

Firefox Modifiez les paramètres avancés du navigateur pour faire confiance à l'URI du site Web StoreFront pour l'authentification unique.

> **Avertissement :**
>
> La modification incorrecte des paramètres avancés peut entraîner de graves problèmes. Apportez des modifications à vos risques et périls.

1. Ouvrez Firefox sur l'ordinateur qui s'authentifiera à l'aide du transfert de domaine.
2. Dans la barre d'adresses, saisissez about:config.
3. Cliquez sur Accepter le risque.
4. Dans la barre de recherche, entrez negotiate.

5. Double-cliquez sur network.negotiate-auth.delegation-uris.
6. Entrez le nom de votre domaine Windows d'entreprise (par exemple, mydomain.com).
7. Cliquez sur OK.
8. Double-cliquez sur network.negotiate-auth.trusted-uris.
9. Entrez le nom de votre domaine Windows d'entreprise (par exemple, mydomain.com).
10. Cliquez sur OK.
11. Fermez et redémarrez Firefox.

Connexion via authentification unique aux VDA à l'aide de FAS

Vous pouvez également configurer le service d'authentification fédérée pour la connexion via authentification unique aux VDA lorsque vous utilisez l'application Citrix Workspace installée localement, mais pas l'application Citrix Workspace pour HTML5.

Authentification pass-through via Citrix Gateway

April 17, 2024

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 d'un navigateur Web. Pour plus d'informations sur la configuration de StoreFront pour Citrix Gateway, consultez Configurer une instance de Citrix Gateway.

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

- **Domaine** Les utilisateurs ouvrent une session à l'aide de leur nom d'utilisateur et de leur mot de passe Active Directory.
- **RSA** 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, et 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.
- **Carte à puce** Les utilisateurs se connectent à l'aide de cartes à puce
- **RSA + Domaine** 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.

Si vous avez désactivé l'authentification sur Citrix Gateway ou si vous avez désactivé l'authentification unique, l'authentification pass-through n'est pas utilisée et vous devez configurer l'une des autres méthodes d'authentification.

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 plus d'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 de Citrix Virtual Apps and Desktops sur la base de stratégies de session Citrix Gateway.

Activer l'authentification pass-through via Gateway

Pour activer ou désactiver l'authentification pass-through via Gateway pour un magasin lors de la connexion via les applications Workspace, cochez ou décochez la case **Authentification pass-through via Citrix Gateway** dans la fenêtre Méthodes d'authentification.

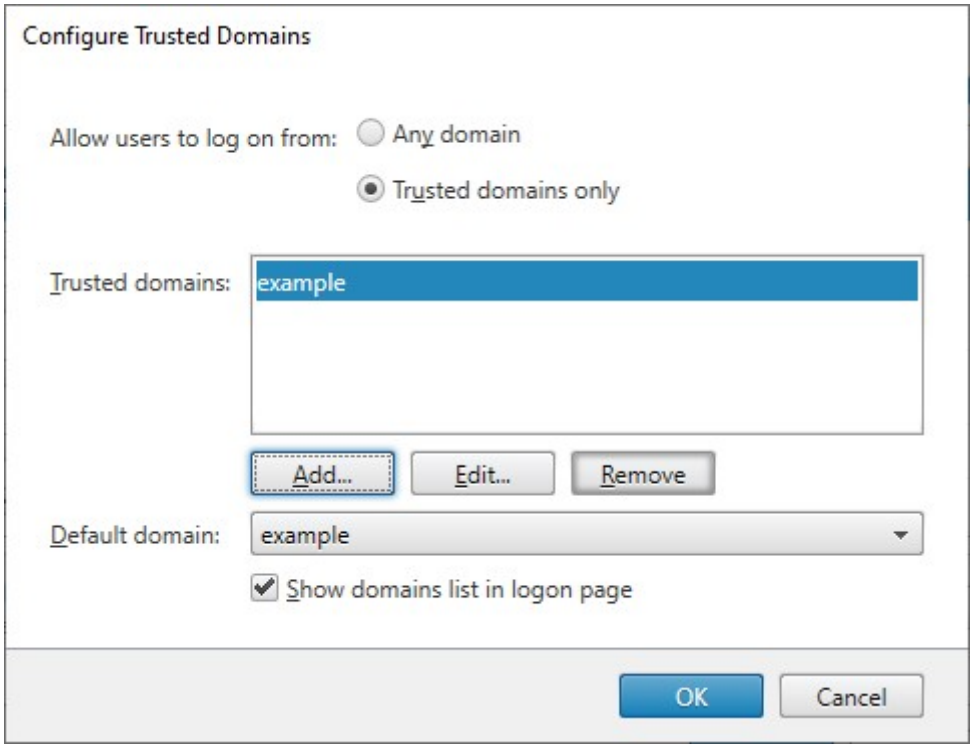
L'activation par défaut de l'authentification pass-through via Citrix Gateway pour un magasin l'active également pour tous les sites Web de ce magasin. Vous pouvez désactiver l'authentification par nom d'utilisateur et mot de passe pour un site Web spécifique dans l'onglet Méthodes d'authentification.

Configurer des domaines utilisateur approuvés

Si votre instance de Citrix Gateway est configurée pour utiliser l'authentification LDAP, vous pouvez limiter l'accès à des domaines spécifiques.

1. Dans la fenêtre « Gérer les méthodes d'authentification », dans le menu déroulant **Authentification pass-through via Citrix Gateway** > **Paramètres**, sélectionnez **Configurer les domaines approuvés**.
2. Sélectionnez **Domaines approuvés uniquement**, cliquez sur **Ajouter** pour entrer le nom d'un domaine approuvé. Les utilisateurs disposant de comptes dans ce domaine peuvent 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.

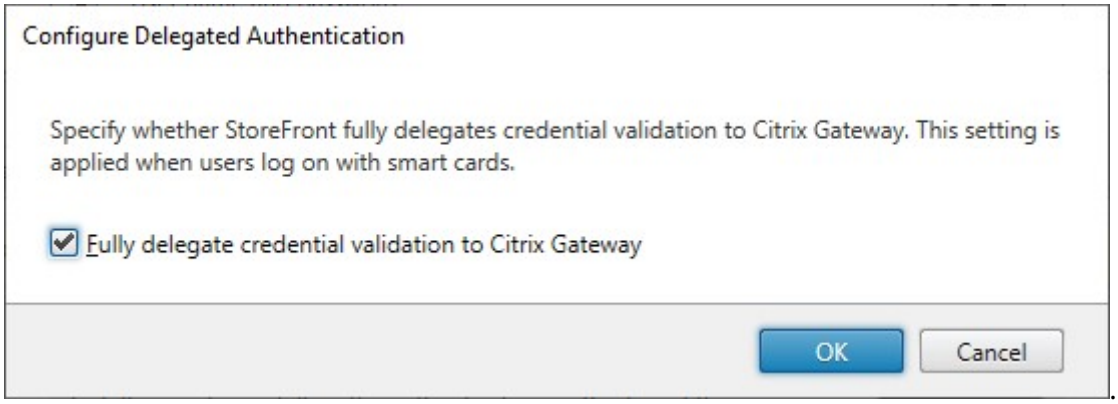
   La manière dont vous spécifiez le nom de domaine détermine le format auquel les utilisateurs devront saisir leurs informations d'identification. Si vous souhaitez que les utilisateurs saisissent leurs informations d'identification au format de nom d'utilisateur de domaine, ajoutez le nom NetBIOS à la 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.
3. Si vous configurez plusieurs domaines approuvés, sélectionnez dans la liste Domaine par défaut le domaine sélectionné par défaut lorsque les utilisateurs ouvrent une session.
4. 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.



Déléguer la validation des informations d'identification à Citrix Gateway

Par défaut, StoreFront valide le nom d'utilisateur et le mot de passe qu'il reçoit de Gateway. Si votre instance de Citrix Gateway est configurée pour utiliser des méthodes d'authentification sans mot de passe, telles que les cartes à puce, vous devez configurer StoreFront de telle sorte qu'il ne valide pas les informations d'identification et qu'il dépende donc de l'authentification de Gateway. Dans ce cas, il est recommandé de saisir une URL de rappel lors de la configuration de Gateway afin que StoreFront puisse vérifier que la demande provient de Gateway. Consultez Gérer des appliances Citrix Gateway.

1. Dans la fenêtre **Gérer les méthodes d'authentification**, dans le menu déroulant **Authentification pass-through via Citrix Gateway** > **Paramètres**, sélectionnez **Configurer l'authentification déléguée**.
2. Sélectionnez **Déléguer entièrement la validation des informations d'identification à Citrix Gateway**.



SDK PowerShell

Pour configurer le magasin afin de déléguer l'authentification à la passerelle à l'aide du SDK PowerShell, utilisez l'applet de commande Set-STFCitrixAGBasicOptions pour définir `CredentialValidationMode` sur `Auto`. Pour configurer StoreFront afin de valider les informations d'identification, définissez `CredentialValidationMode` sur `Password`.

Autoriser les utilisateurs à modifier les mots de passe expirés lors de la connexion

Si votre appliance Citrix Gateway est configurée pour utiliser l'authentification LDAP (nom d'utilisateur et mot de passe), vous pouvez configurer NetScaler pour autoriser la modification des mots de passe expirés lors de la connexion.

1. Se connecter au site Web d'administration de NetScaler
2. Dans le menu latéral, accédez à **Authentification** > **Tableau de bord**.
3. Cliquez sur le serveur d'authentification.
4. Sous **Autres paramètres**, cochez **Autoriser la modification du mot de passe**.

Autoriser les utilisateurs à modifier leurs mots de passe après la connexion

Avec **Authentification pass-through via Citrix Gateway**, l'appliance Citrix Gateway est chargée de gérer l'authentification. Vous pouvez configurer StoreFront pour permettre aux utilisateurs de modifier leur mot de passe après leur connexion. Cette fonctionnalité n'est disponible que lorsque vous accédez aux magasins StoreFront via l'application Citrix Workspace pour HTML5, et non via les applications Citrix Workspace installées localement.

La configuration par défaut de StoreFront empêche les utilisateurs de modifier leurs mots de passe, même s'ils 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. Dans la fenêtre **Gérer les méthodes d'authentification**, dans le menu déroulant **Authentification pass-through via Citrix Gateway** > **Paramètres**, sélectionnez **Gérer les options de mot de passe**
2. Pour autoriser les utilisateurs à modifier les mots de passe, cochez la case **Autoriser les utilisateurs à modifier les mots de passe**.

> **Remarque :**
>
> Si vous sélectionnez ou désactivez **Autoriser les utilisateurs à modifier les mots de passe**, cela affectera également les paramètres de la section **Gérer les options de mot de passe** pour l'authentification par nom d'utilisateur et mot de passe.

SDK PowerShell

Pour modifier les options de modification du mot de passe à l'aide du SDK PowerShell, utilisez l'applet de commande Set-STFExplicitCommonOptions.

Configurer Delivery Controller pour qu'il approuve StoreFront

Lorsque Citrix Gateway est configuré avec l'authentification LDAP, il transmet les informations d'identification à StoreFront. Pour les autres méthodes d'authentification, StoreFront n'a pas accès aux informations d'identification et ne peut donc pas s'authentifier auprès de Citrix Virtual Apps and Desktops. Vous devez donc configurer le Delivery Controller pour qu'il approuve les demandes provenant de StoreFront. Consultez les considérations et les meilleures pratiques relatives à la sécurité de Citrix Virtual Apps and Desktops.

Authentification unique aux VDA à l'aide du Service d'authentification fédérée

Lorsque la passerelle est configurée avec l'authentification LDAP, elle transmet les informations d'identification à StoreFront afin de permettre l'authentification unique (Single Sign-On) aux VDA. Pour les autres méthodes d'authentification, StoreFront n'a pas accès aux informations d'identification. L'authentification unique n'est donc pas disponible par défaut. Vous pouvez utiliser le Service d'authentification fédérée pour fournir une authentification unique.

Authentification SAML

May 30, 2024

SAML (Security Assertion Markup Language) est une norme ouverte utilisée par les produits d'identité et d'authentification. À l'aide de SAML, vous pouvez configurer StoreFront pour rediriger les utilisateurs vers un fournisseur d'identité externe à des fins d'authentification.

> **Remarque**
>
> Configurez StoreFront avec l'authentification SAML pour l'accès interne. Pour l'accès externe, vous devez configurer Citrix Gateway avec l'authentification SAML, puis configurer StoreFront avec l'authentification unique Gateway.

StoreFront nécessite un fournisseur d'identité (IdP) conforme à SAML 2.0 tel que :

- Microsoft AD Federation Services à l'aide de liaisons SAML (et non des liaisons WS-Federation). Pour plus d'informations, consultez Déploiement AD FS et Opérations AD FS.
- Citrix Gateway (configuré en tant qu'IdP)
- ID Microsoft Entra. Pour plus d'informations, veuillez consulter l'article CTX237490.

L'assertion SAML doit contenir un attribut `saml:Subject` contenant l'UPN de l'utilisateur.

Pour activer ou désactiver l'authentification SAML pour un magasin lors de la connexion via les applications Workspace, sélectionnez **Authentification SAML** dans la fenêtre Méthodes d'authentification. L'activation par défaut de l'authentification SAML pour un magasin l'active également pour tous les sites Web de ce magasin. Vous pouvez configurer SAML indépendamment pour un site Web spécifique dans l'onglet Méthodes d'authentification.

Points de terminaison SAML StoreFront

Pour configurer SAML, votre fournisseur d'identité peut avoir besoin des points de terminaison suivants :

- L'URL de l'ID de l'entité. Il s'agit du chemin d'accès au service d'authentification du magasin, généralement https://[storefront host]/Citrix/[StoreName]Auth
- L'URL ACS, généralement https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/AssertionConsumer
- Le service de métadonnées, généralement https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/Ser

En outre, il existe un point de terminaison de test, généralement https://[storefront host]/Citrix/[StoreName]Auth/S

Vous pouvez utiliser le script PowerShell suivant pour répertorier les points de terminaison d'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:
Entity ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest
<!--NeedCopy-->
```

Exemple de sortie :

```
SAML Service Provider information:
Entity 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
<!--NeedCopy-->
```

Configuration à l'aide de l'échange de métadonnées

Pour simplifier la configuration, vous pouvez échanger des métadonnées (identifiants, certificats, points de terminaison et autres configurations) entre le fournisseur d'identité et le fournisseur de services, qui est StoreFront dans ce cas.

Si votre fournisseur d'identité prend en charge l'importation de métadonnées, vous pouvez le faire pointer vers le point de terminaison des métadonnées StoreFront. **Remarque :** cette opération doit

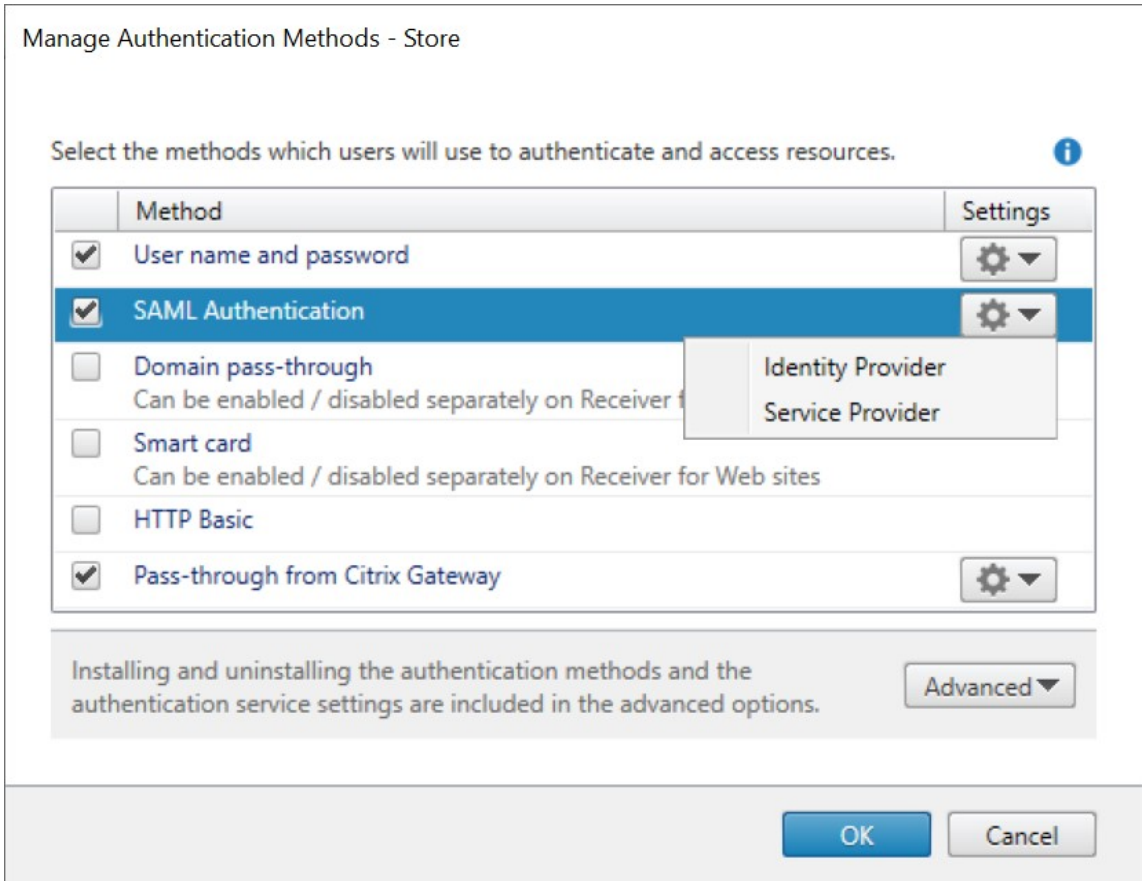
être effectuée sur HTTPS.

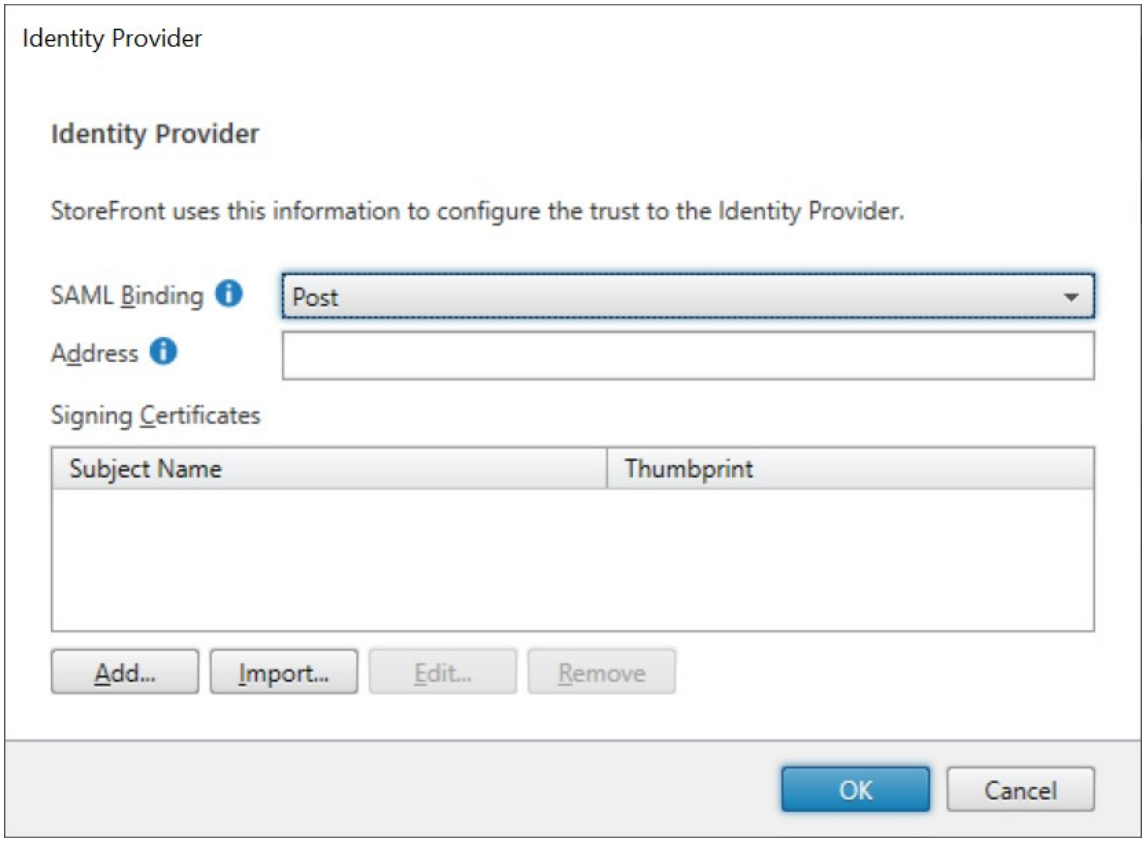
Pour configurer StoreFront à l'aide des métadonnées d'un fournisseur d'identité, utilisez l'applet de commande Update-STFSamlIdPFromMetadata, par exemple :

```
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"
<!--NeedCopy-->
```

Configurer le fournisseur d'identité

1. Cliquez sur le menu déroulant des paramètres sur la ligne **Authentification SAML**, puis cliquez sur **Fournisseur d'identité**.

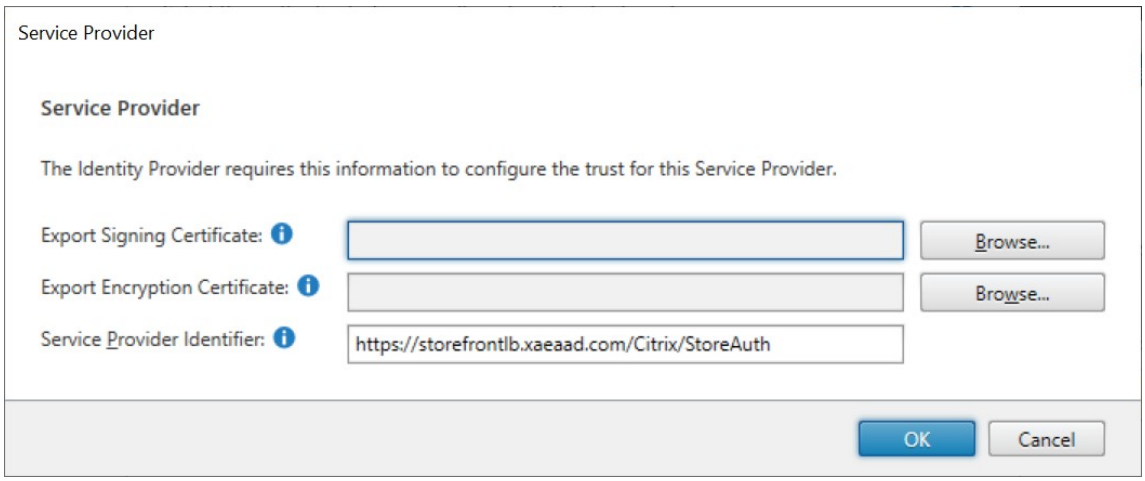




2. Choisissez **Post** ou **Redirect** pour **Liaison SAML**.
3. Entrez l'**adresse** du fournisseur d'identité.
4. Importez le certificat utilisé pour signer les jetons SAML.
5. Sélectionnez **OK** pour enregistrer les modifications.

Configurer le fournisseur de services

1. Cliquez sur le menu déroulant des paramètres sur la ligne **Authentification SAML**, puis cliquez sur **Fournisseur de services**.



2. Vous pouvez également choisir le **certificat de signature d'exportation** utilisé pour signer les messages adressés au fournisseur d'identité.
3. Vous pouvez également choisir le **certificat de chiffrement d'exportation** utilisé pour déchiffrer les messages reçus du fournisseur d'identité.
4. L'**identifiant du fournisseur de services** est pré-rempli avec le service d'authentification du magasin.
5. Sélectionnez **OK** pour enregistrer les modifications.

SDK PowerShell

À l'aide du SDK PowerShell :

- Pour importer un certificat de signature, appelez l'applet de commande Import-STFSamlSigningCertificate.
- Pour importer un certificat de chiffrement, appelez l'applet de commande Import-STFSamlEncryptionCertifi

Test

Pour tester l'intégration SAML :

1. Accédez à la page de test SAML. Consultez Points de terminaison SAML StoreFront.
2. Cela vous redirige vers le fournisseur d'identité. Entrez vos informations d'identification.
3. Vous êtes redirigé vers la page de test qui affiche les revendications et assertions d'identité.

Configurer Delivery Controller pour qu'il approuve StoreFront

Lorsque vous utilisez l'authentification SAML, StoreFront n'a pas accès aux informations d'identification de l'utilisateur et ne peut donc pas s'authentifier auprès de Citrix Virtual Apps and Desktops.

Vous devez donc configurer le Delivery Controller pour qu'il approuve les demandes provenant de StoreFront. Consultez les considérations et les meilleures pratiques relatives à la sécurité de Citrix Virtual Apps and Desktops.

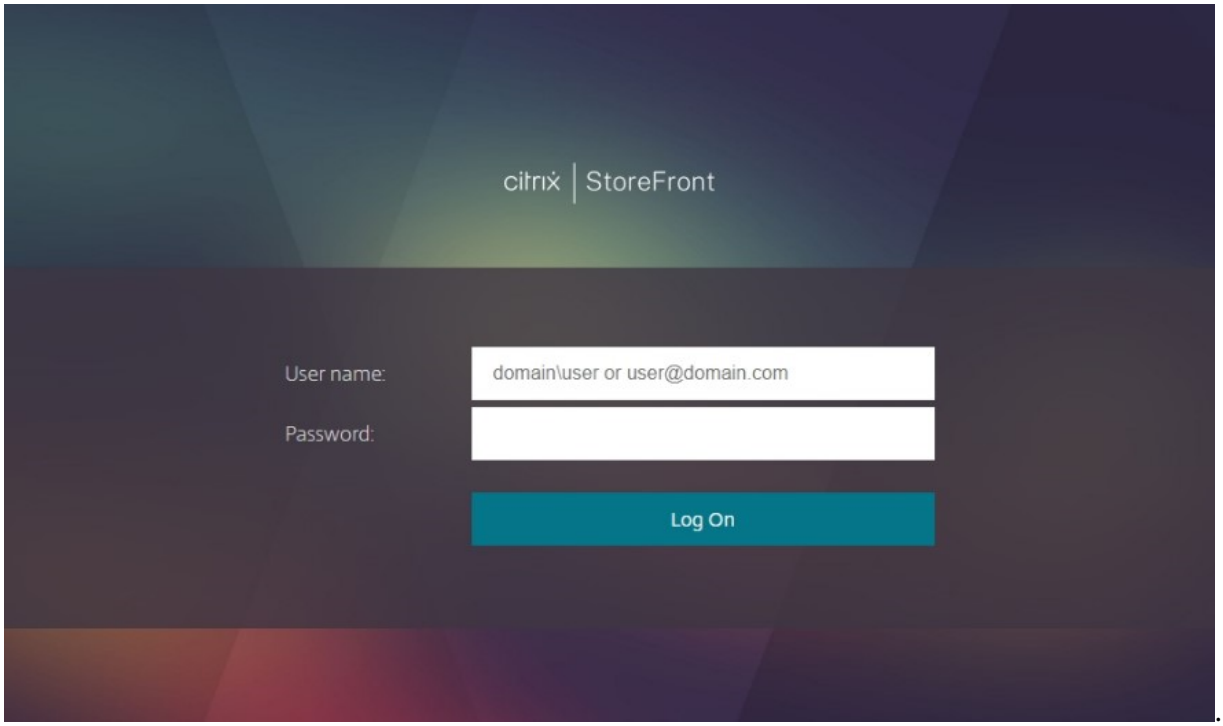
Authentification unique aux VDA à l'aide du Service d'authentification fédérée

Lors de l'utilisation de l'authentification SAML, StoreFront n'a pas accès aux informations d'identification de l'utilisateur. L'authentification unique aux VDA n'est donc pas disponible par défaut. Vous pouvez utiliser le Service d'authentification fédérée pour fournir une authentification unique.

Authentification par nom d'utilisateur et mot de passe

February 22, 2024

Avec l'authentification par nom d'utilisateur et mot de passe, les utilisateurs saisissent leurs informations d'identification Active Directory.



Pour activer ou désactiver l'authentification par nom d'utilisateur et mot de passe pour un magasin lors de la connexion via les applications Workspace, cochez ou décochez **Nom d'utilisateur et mot de passe** dans la fenêtre Méthodes d'authentification.

L'activation par défaut de l'authentification par nom d'utilisateur et mot de passe pour un magasin l'active également pour tous les sites Web de ce magasin. Vous pouvez désactiver l'authentification par

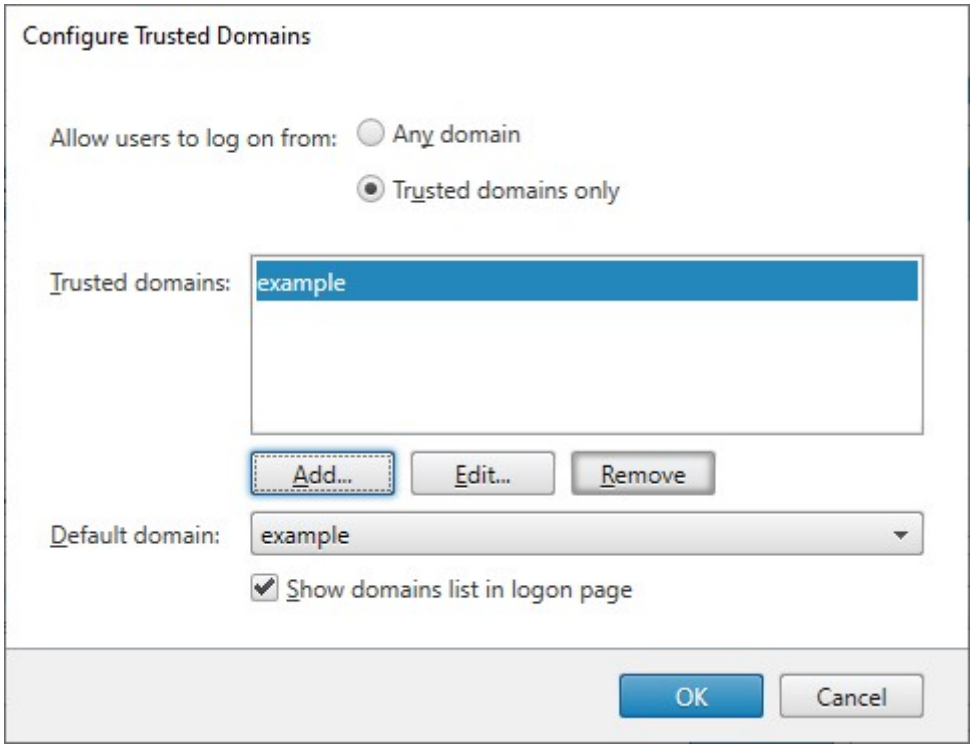
nom d'utilisateur et mot de passe pour un site Web spécifique dans l'onglet Gérer les sites Receiver pour Web - Méthodes d'authentification.

Configurer des domaines utilisateur approuvés

Vous pouvez 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. 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**.
2. Dans le menu déroulant **Nom d'utilisateur et mot de passe > Paramètres**, sélectionnez **Configurer Domaines approuvés**.
3. Sélectionnez **Domaines approuvés uniquement**, cliquez sur **Ajouter** pour entrer le nom d'un domaine approuvé. Les utilisateurs disposant de comptes dans ce domaine peuvent 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.
4. Si vous configurez plusieurs domaines approuvés, sélectionnez dans la liste Domaine par défaut le domaine sélectionné par défaut lorsque les utilisateurs ouvrent une session.
5. 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

Vous pouvez autoriser les utilisateurs à modifier leur mot 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.

La fonctionnalité de modification du mot de passe est disponible dans les clients suivants :

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

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

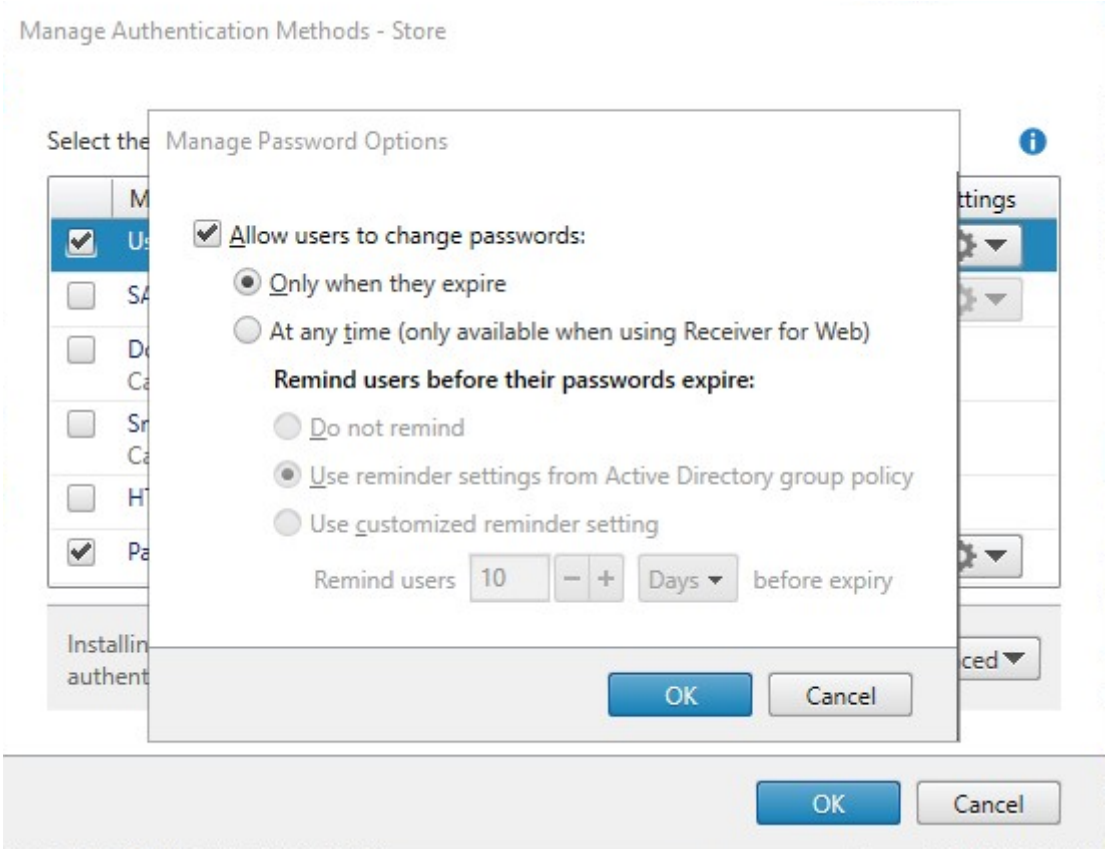
La configuration par défaut empêche les utilisateurs de l'application Citrix Workspace et du navigateur Web de modifier leurs mots de passe, même s'ils ont expiré. Si vous choisissez d'activer cette fonctionnalité, assurez-vous que les stratégies des domaines contenant vos serveurs n'empêchent pas les 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.

Si vous autorisez les utilisateurs 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. Vous pouvez également configurer une période de notification personnalisée.

1. Dans la fenêtre **Gérer les méthodes d'authentification**, dans le menu déroulant **Nom d'utilisateur et mot de passe** > **Paramètres**, sélectionnez **Gérer les options de mot de passe**
2. Pour autoriser les utilisateurs à modifier les mots de passe, cochez la case **Autoriser les utilisateurs à modifier les mots de passe**.

   > **Remarque :**
   > 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.

3. Choisissez d'autoriser les utilisateurs à modifier leurs mots de passe **À l'expiration uniquement** ou **À tout moment**.
4. Choisissez si vous souhaitez envoyer un rappel aux utilisateurs avant l'expiration de leur mot de passe.



Remarque 1 :

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

Remarque 2 :

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.

Remarque 3 :

Si vous activez ou désactivez à tout moment la modification des mots de passe, cela affecte également les paramètres de la section **Gérer les options de mot de passe** pour l'authentification pass-through via Citrix Gateway.

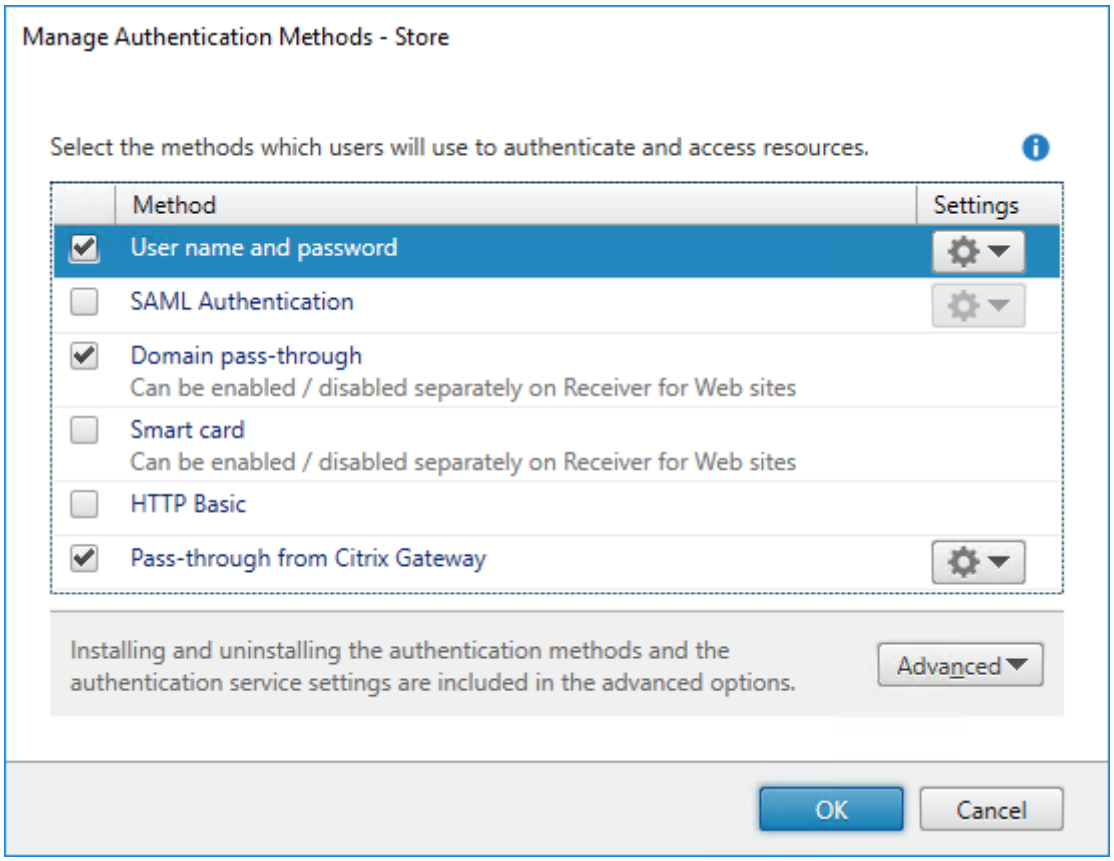
Validation du mot de passe d'identification

Normalement, StoreFront communique directement avec Active Directory pour valider les informations d'identification.

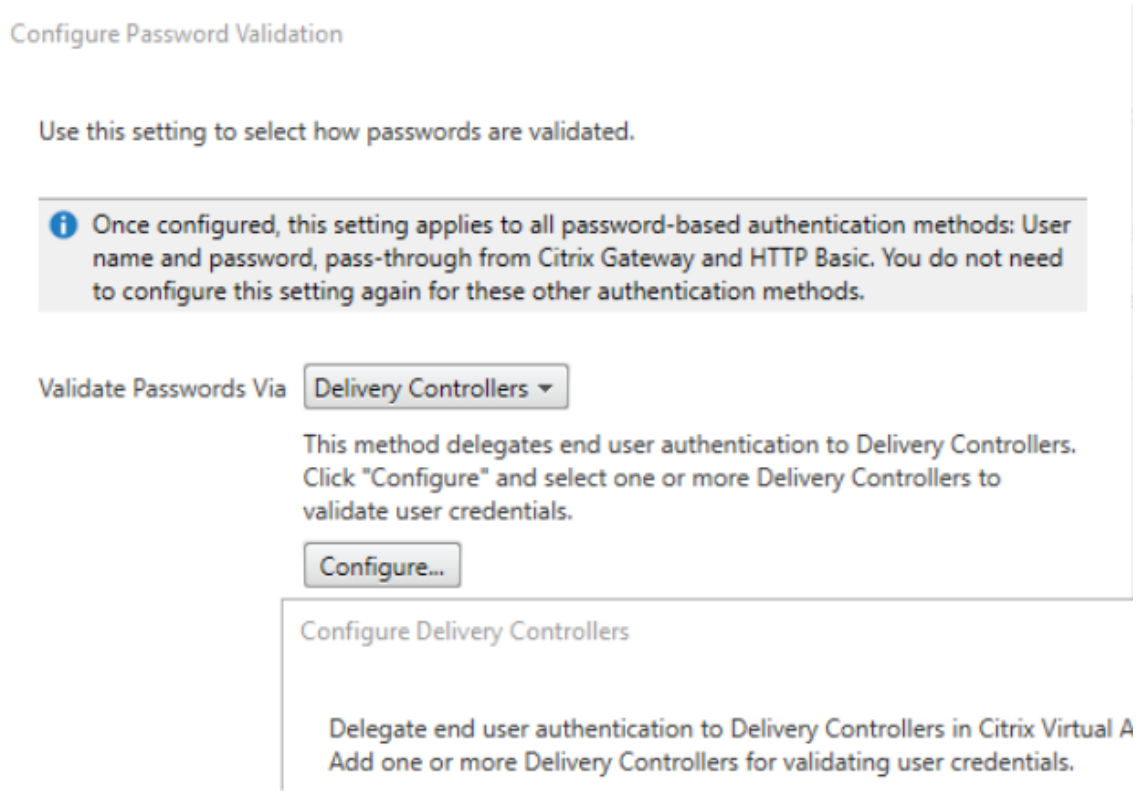
Lorsque StoreFront ne se trouve pas dans le même domaine que Citrix Virtual Apps and Desktops, et

qu'il n'est pas possible de mettre des approbations Active Directory en place, vous pouvez configurer StoreFront pour que les Delivery Controller Citrix Virtual Apps and Desktops soient utilisés pour l'authentification des noms d'utilisateur et mots de passe :

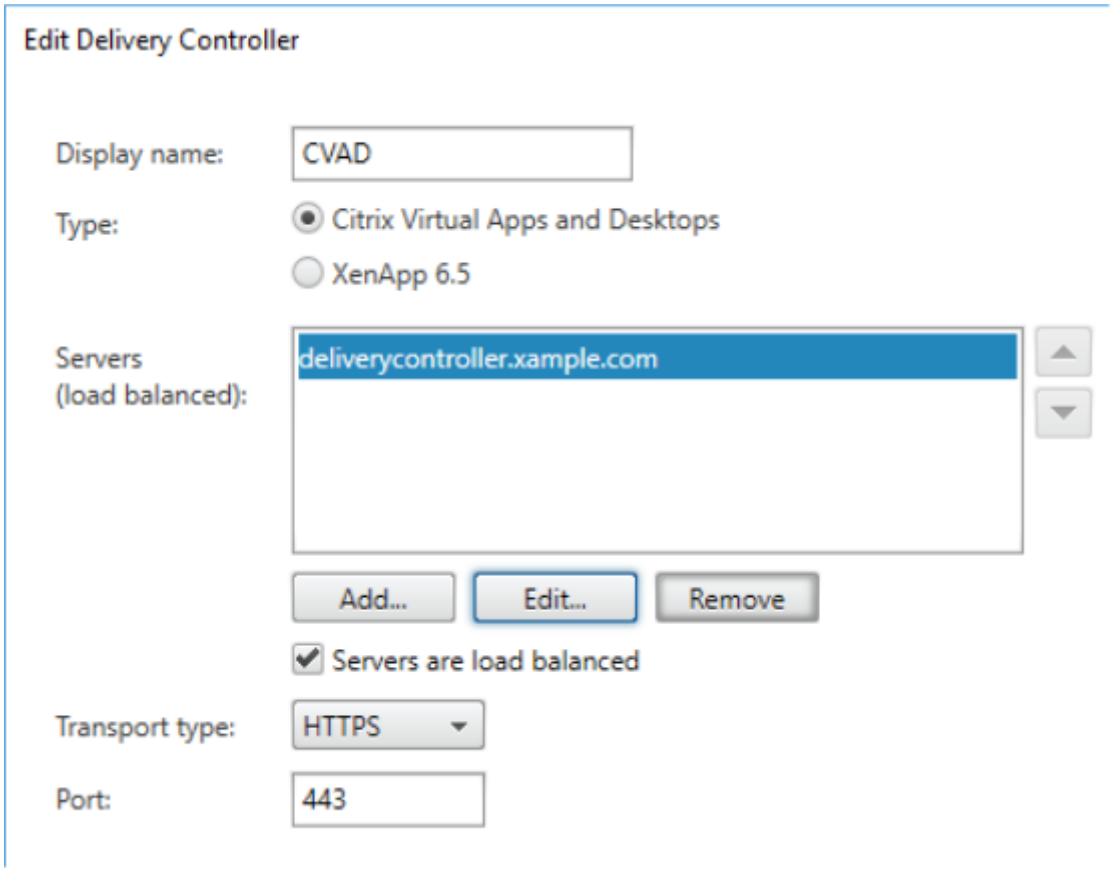
1. Dans la fenêtre **Gérer les méthodes d'authentification**, à partir du menu déroulant **Nom d'utilisateur et mot de passe > Paramètres**, sélectionnez **Configurer la validation du mot de passe**.



2. À partir du menu déroulant **Valider les mots de passe via**, sélectionnez **Delivery Controller**, puis cliquez sur **Configurer**.



3. 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**.



Utiliser Active Directory

1. 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**.
2. À partir du menu déroulant **Valider les mots de passe via**, sélectionnez **Active Directory**, puis cliquez sur **OK**.

Authentification unique aux VDA

Lorsque les utilisateurs lancent une ressource, StoreFront utilise les informations d'identification que l'utilisateur a utilisées pour se connecter au magasin pour l'authentification unique aux VDA.

Personnaliser l'écran d'ouverture de session

L'écran d'ouverture de session est généré à partir d'un modèle, généralement situé sous C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templates\UsernamePassword.tfrm. Vous pouvez personnaliser l'écran.

Texte de titre

Lorsque les utilisateurs se connectent à un magasin, aucun texte de titre ne s'affiche dans la boîte de dialogue d'ouverture de session. Vous pouvez afficher le texte « Please log on » ou composer votre propre message personnalisé :

1. Utilisez un éditeur de texte pour ouvrir le fichier UsernamePassword.tfrm pour le service d'authentification.
2. Recherchez les lignes suivantes dans le fichier.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
<!--NeedCopy-->
```

3. Supprimez les marques de commentaire pour l'instruction en supprimant le début **@*** et la fin ***@**.

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
<!--NeedCopy-->
```

   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\[Store name]Auth\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>
<!--NeedCopy-->
```

   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 l'application Citrix Workspace

pour Windows de mettre en cache les mots de passe des utilisateurs, vous devez modifier les fichiers du service d'authentification.

1. Utilisez un éditeur de texte pour ouvrir le fichier inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templ
2. Recherchez la ligne suivante dans le fichier.

```
1 @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
     "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
     ControlValue("SaveCredentials"))
2 <!--NeedCopy-->
```

3. Commentez l'instruction comme indiqué ci-dessous.

```
1 <!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
     labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
     initiallyChecked: ControlValue("SaveCredentials")) -->
2 <!--NeedCopy-->
```

   Les utilisateurs doivent entrer leur mot de passe chaque fois qu'ils se connectent à des magasins utilisant ce service d'authentification.

   Par défaut, l'application Citrix Workspace pour Windows remplit automatiquement le dernier nom d'utilisateur saisi. Pour supprimer le remplissage du champ Nom d'utilisateur ou pour découvrir un autre mécanisme permettant de supprimer la mise en cache des mots de passe, consultez Empêcher l'application Citrix Workspace pour Windows de mettre les mots de passe et les noms d'utilisateur en cache.

Accès à distance via Citrix Gateway

Vous pouvez configurer votre instance de Citrix Gateway pour que les utilisateurs se connectent à la passerelle à l'aide du nom d'utilisateur et du mot de passe de leur domaine. Ces informations d'identification sont transmises à StoreFront pour l'authentification au magasin. Pour configurer votre instance de Citrix Gateway pour l'authentification par nom d'utilisateur et mot de passe LDAP, consultez la documentation NetScaler sur l'authentification LDAP. Pour configurer StoreFront, consultez Authentification pass-through via Citrix Gateway.

Configuration du Service d'authentification fédérée

April 17, 2024

Lors de l'utilisation de méthodes d'authentification telles que SAML, dans lesquelles l'utilisateur ne saisit pas ses informations d'identification directement dans l'application Citrix Workspace, par défaut il n'est pas possible de s'authentifier uniquement dans les VDA. Dans ces cas, vous pouvez utiliser

le Service d'authentification fédérée (FAS) pour fournir une authentification unique aux VDA à l'aide de l'authentification du certificat.

Pour utiliser FAS avec StoreFront, vous devez configurer StoreFront à l'aide du SDK PowerShell. Utilisez Set-STFClaimsFactoryNames pour définir la fabrique de revendication sur `FASClaimsFactory` et utilisez Set-STFStoreLaunchOptions pour définir le fournisseur de données de connexion du VDA sur `FASLogonDataProvider`.

Par exemple, pour activer le FAS pour un magasin :

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
<!--NeedCopy-->
```

Pour désactiver le FAS pour un magasin, procédez comme suit :

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
<!--NeedCopy-->
```

Remplacez `[VirtualPath]` par le chemin virtuel approprié, par exemple `/Citrix/Store`.

Pour configurer la liste des serveurs FAS et d'autres paramètres, vous devez utiliser la stratégie de groupe. Pour plus d'informations, consultez la documentation FAS.

Le FAS n'est pas utilisé lors de l'authentification à l'aide d'un transfert de domaine ou d'une carte à puce via un navigateur.

Indisponibilité du serveur FAS

Si le serveur FAS n'est pas disponible, le lancement échoue par défaut. Vous pouvez toutefois configurer StoreFront de telle sorte que, si le serveur FAS n'est pas disponible, les utilisateurs puissent se connecter au VDA en saisissant leurs informations d'identification. Pour modifier la configuration, utilisez l'applet de commande Powershell Set-STFStoreLaunchOptions avec un paramètre `FederatedAuthenticationServiceFailover`. Par exemple, pour activer le basculement pour un magasin :

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]
Set-STFStoreLaunchOptions $storeService -
    FederatedAuthenticationServiceFailover $True
<!--NeedCopy-->
```


Configurer et gérer des magasins

February 22, 2024

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	Détails
Créer un magasin	Permet de configurer autant de magasins supplémentaires que vous le souhaitez.
Configurer un magasin	Configurer les paramètres du magasin
Supprimer un magasin	Supprimer un magasin inutile.
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.
Publier et masquer 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.
Configurer la délégation Kerberos	Configurer si StoreFront utilise la délégation Kerberos pour s'authentifier auprès des Delivery Controller.
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.
Vérification des listes de révocation de certificats (CRL)	Configurez 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.
Configurer deux magasins StoreFront pour partager un magasin de données d'abonnement commun	Configurez deux magasins StoreFront pour partager un magasin de données d'abonnement commun.

Tâche	Détails
Activer ou désactiver les favoris	Activer ou désactiver les favoris du magasin.
Gérer les données d'abonnement d'un magasin	Afficher, importer, exporter et purger les données d'abonnement (favoris).
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.
Stocker les données des favoris à l'aide de Microsoft SQL Server	Utiliser une base de données SQL Server externe pour stocker les données d'abonnement (favoris).
Configuration Citrix Virtual Apps and Desktops	Configurer les paramètres Citrix Virtual Apps and Desktops qui affectent la façon dont les ressources sont affichées sur le site Web du magasin.
Paramètres de magasin avancés	Configurez les paramètres avancés du magasin.
Routage HDX optimal	Configurer quelle passerelle est utilisée pour se connecter à quelles ressources
Paramètres ICA par défaut	Configurer les paramètres HDX en les ajoutant à default.ica
Signature de fichier ICA	Configurer la signature de fichiers ica
Raccourcis Windows	Configurer la façon dont l'application Citrix Workspace pour Windows crée le menu Démarrer et les raccourcis du bureau pour les applications préférées et obligatoires

Créer un magasin

December 6, 2023

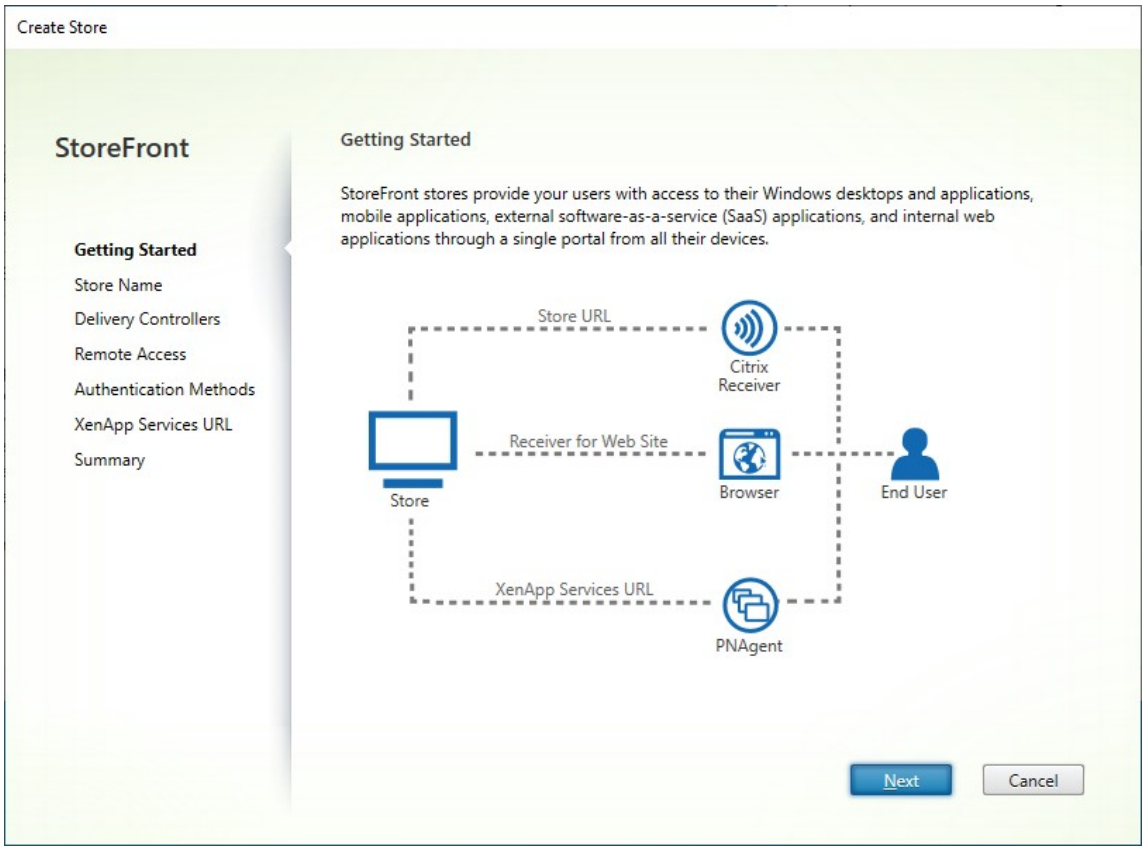
Vous pouvez créer autant de magasins que vous le souhaitez. Par exemple, vous pouvez créer un magasin pour un groupe particulier d'utilisateurs ou regrouper un ensemble spécifique de ressources.

> Important :
>
> Dans les déploiements faisant appel à de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la

> console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois les modifications terminées,
> propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

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.

1. Dans le volet Actions, cliquez sur **Créer un magasin**.

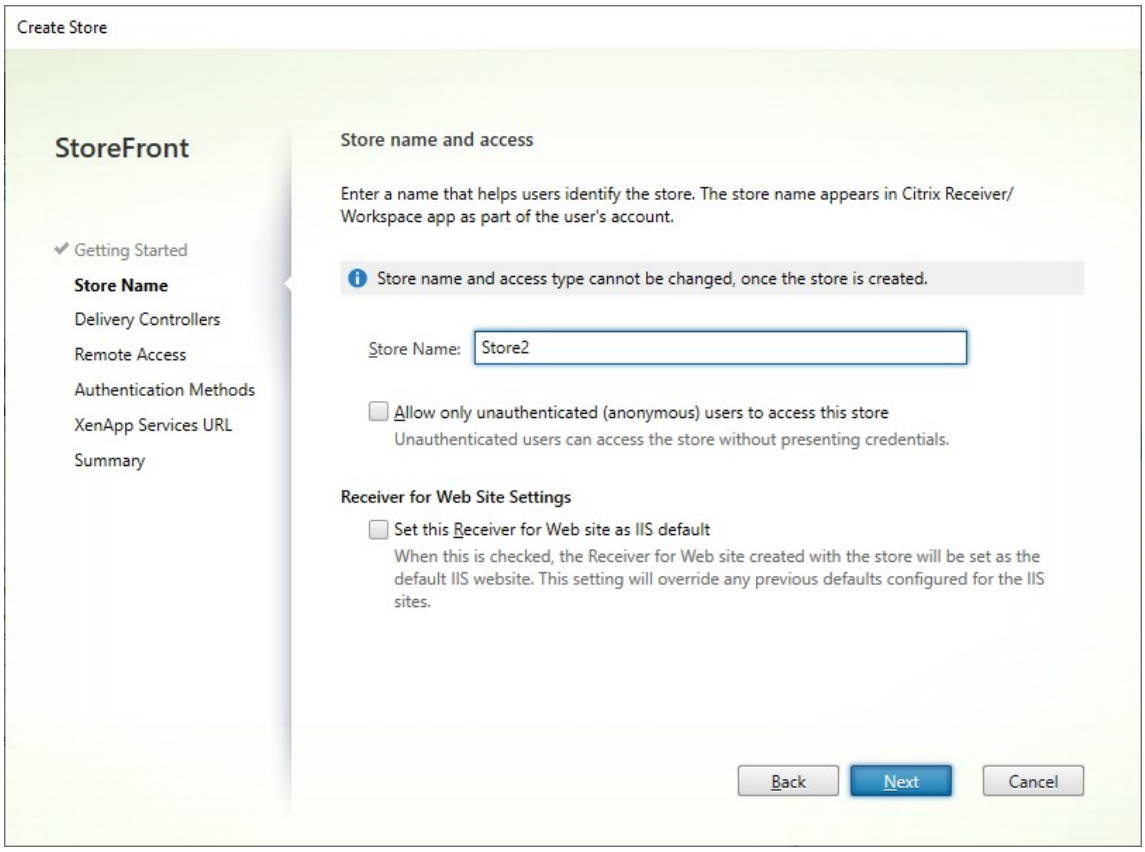


   Cliquez sur **Suivant**.

2. Dans l'onglet **Nom du magasin**, renseignez les informations suivantes :

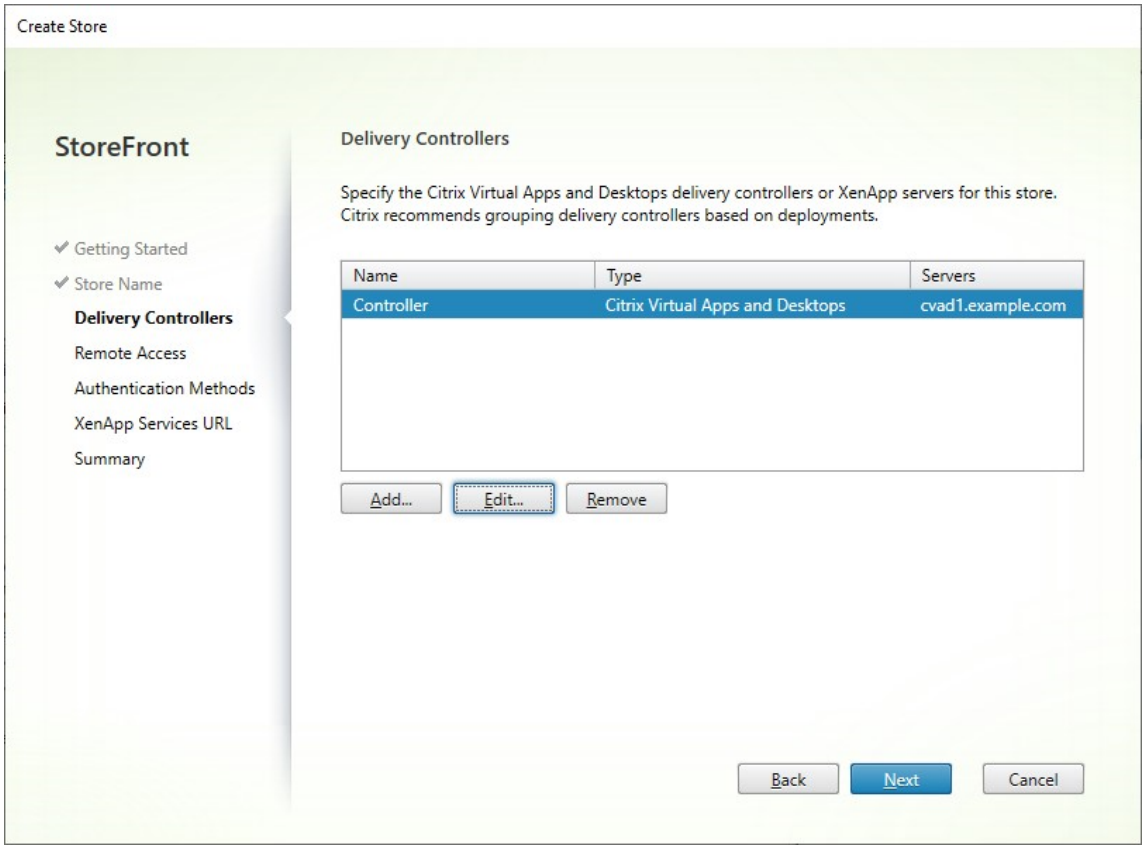
   - Entrez le nom du magasin.
   - Si vous souhaitez autoriser les utilisateurs à accéder au magasin de manière anonyme ou non authentifiée, cochez **Autoriser uniquement les utilisateurs non authentifiés (anonymes) à accéder à ce magasin**. Lorsque vous créez un magasin non authentifié, les pages **Méthodes 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.)



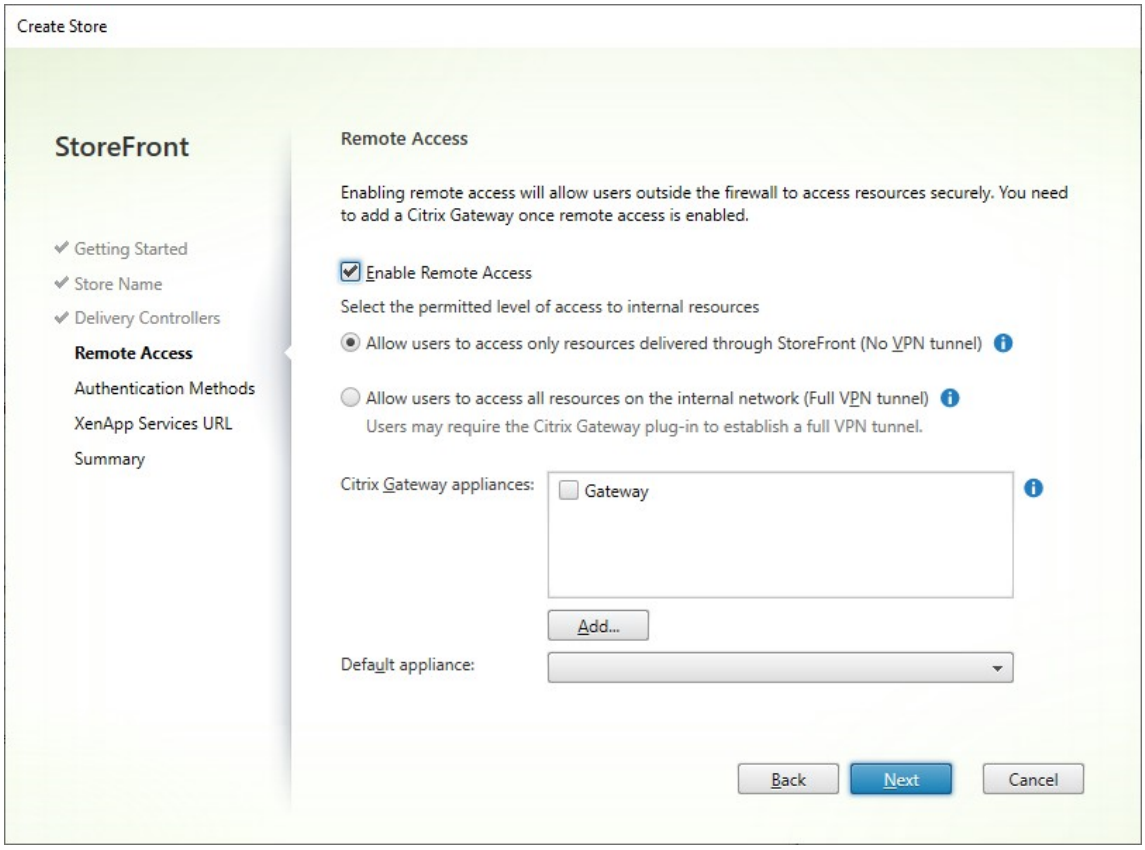
Cliquez sur **Suivant**.

3. Dans l'onglet **Delivery Controller**, ajoutez des flux de ressources pour vos bureaux et applications virtuels. Pour plus de détails, voir Gérer les ressources mises à disposition dans les magasins.



Cliquez sur **Suivant**.

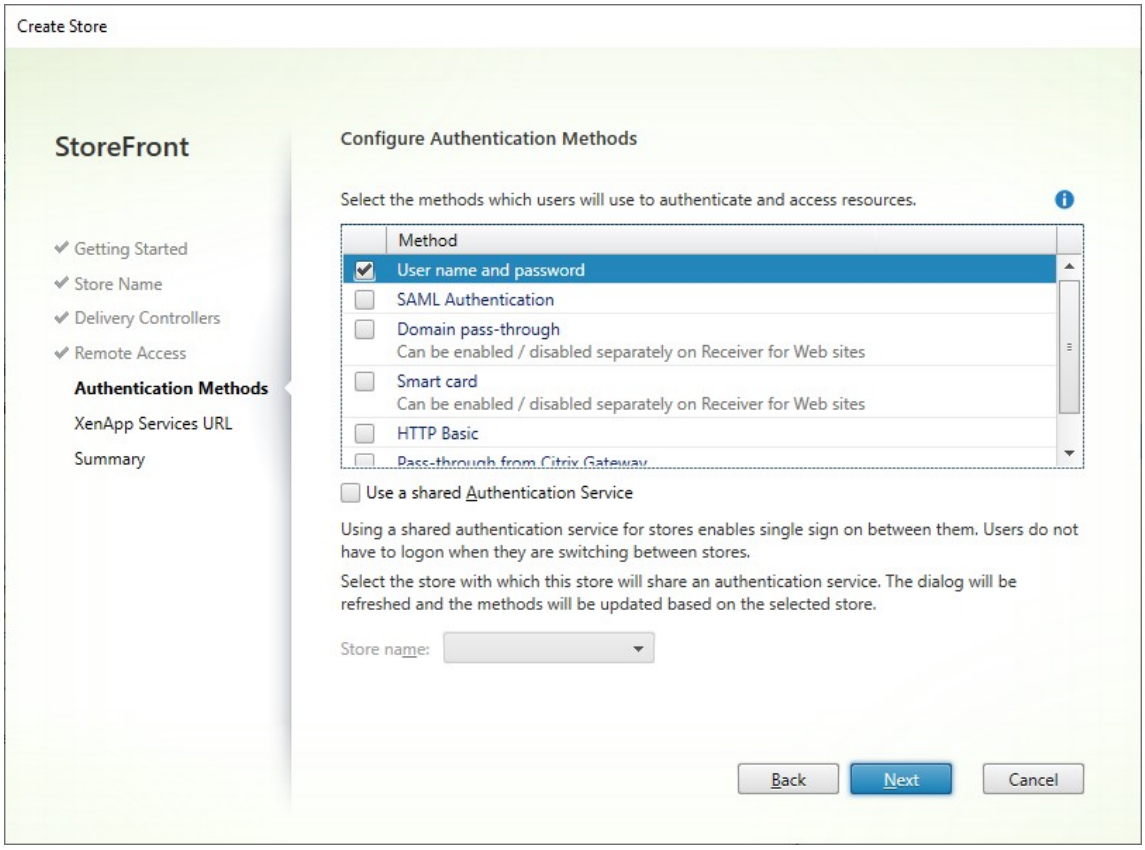
4. Dans l'onglet **Accès distant**, choisissez si vous souhaitez rendre le magasin disponible via Citrix Gateway. Pour plus de détails, consultez Gérer l'accès à distance aux magasins via Citrix Gateway.



5. Sur l'onglet **Méthodes d'authentification**, sélectionnez les méthodes que les utilisateurs utiliseront pour s'authentifier au magasin, puis cliquez sur **Suivant**.

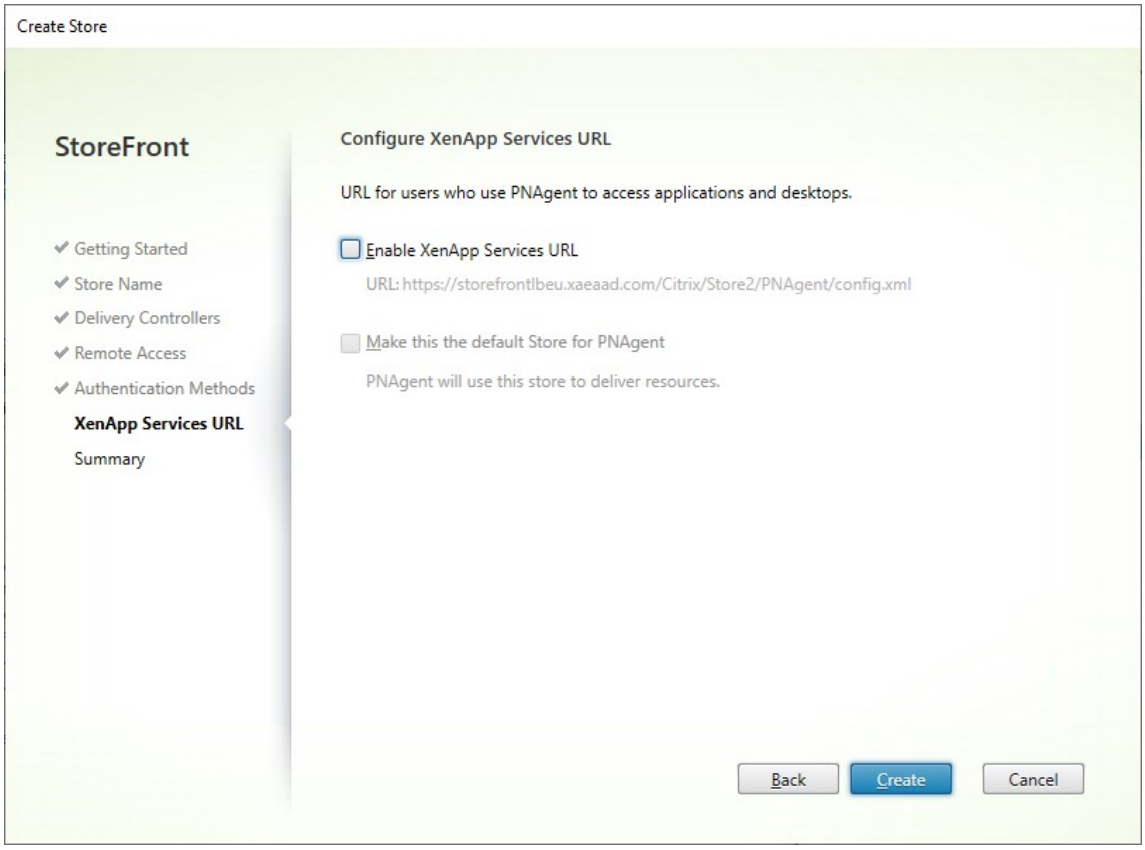
   Pour plus de détails sur les méthodes d'authentification disponibles, consultez la section Configurer l'authentification.

   Plutôt que de configurer les méthodes d'authentification séparément pour ce magasin, il est possible de partager la configuration d'authentification avec un autre magasin. Pour ce faire, cochez **Utiliser un service d'authentification partagé**, puis choisissez un magasin existant.



Cliquez sur **Suivant**.

6. Dans l'onglet **URL XenApp Services**, si vous possédez d'anciens appareils nécessitant PNAgent, laissez la case **Activer l'URL XenApp Services** cochée, sinon décochez-la.



Cliquez sur **Créer**.

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

Lorsqu'un nouveau magasin est créé, un nouveau site Web est également créé pour permettre aux utilisateurs d'accéder au magasin. Vous pouvez configurer ce site Web ou créer d'autres sites Web.

SDK PowerShell

Pour créer un magasin à l'aide du SDK PowerShell, procédez comme suit :

1. Créez un service d'authentification à l'aide de Add-STFAuthenticationService. Par convention, le chemin virtuel est généralement `/Citrix/[StoreName]Auth`. Vous pouvez également obtenir un service d'authentification existant à l'aide de Get-STFAuthenticationService. Cette étape n'est pas obligatoire pour un magasin anonyme.
2. Configurez le service d'authentification selon vos besoins. Consultez Configuration de l'authentification.
3. Exécutez Add-STFStoreService.
    - Choisissez un chemin virtuel pour le magasin et définissez-le en tant que paramètre `-VirtualPath`. Il s'agit généralement de /Citrix/[Nom magasin].

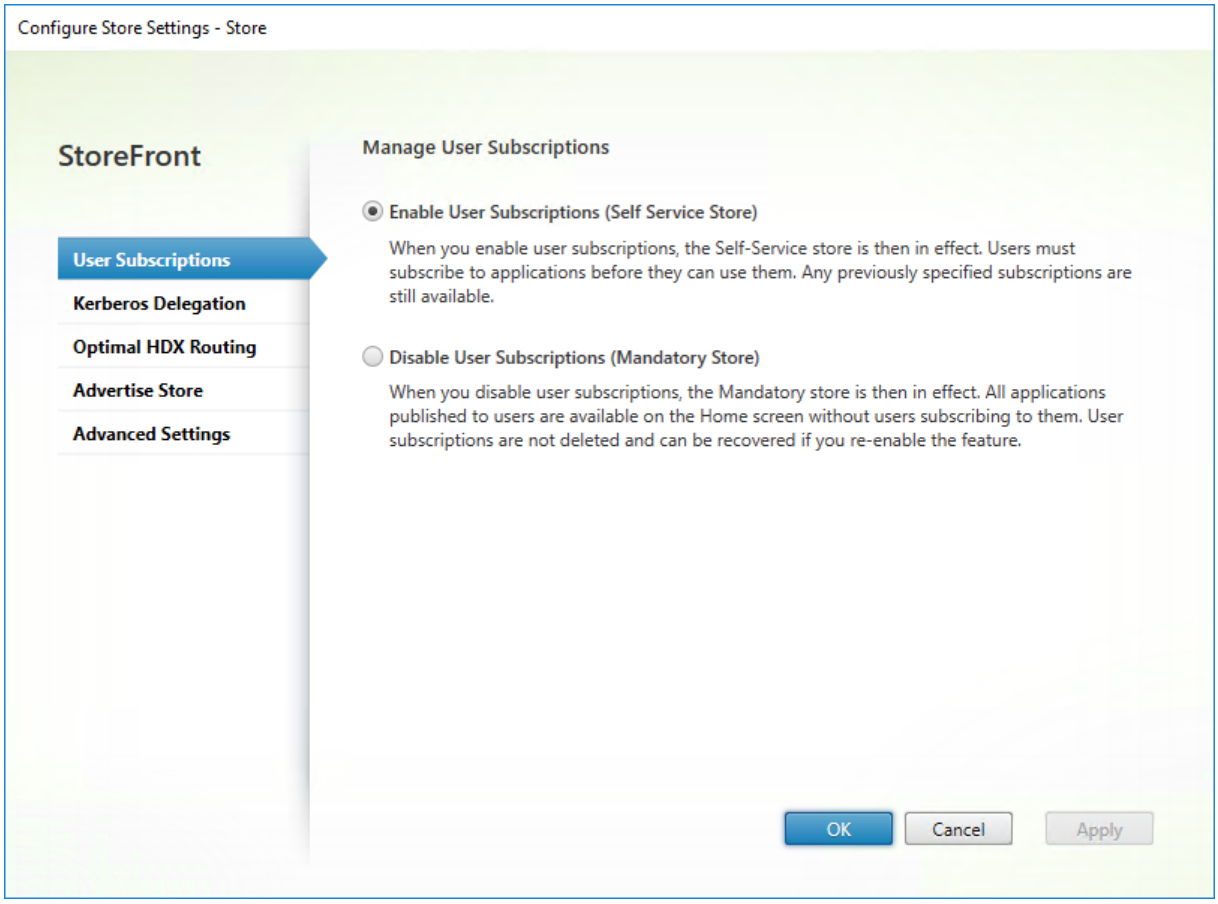
- Définissez `-AuthenticationService` sur le service d'authentification créé à l'étape 1. Vous pouvez également définir `-Anonymous $True` s'il s'agit d'un magasin anonyme.
- Vous pouvez inclure les détails d'un flux de ressources. Les flux de ressources supplémentaires doivent être configurés séparément.

Configurer un magasin

August 25, 2023

Pour modifier un magasin, procédez comme suit :

1. 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**.
2. Accédez à l'onglet Abonnements utilisateur pour configurer si les favoris sont activés.
3. Accédez à l'onglet Délégation Kerberos pour configurer si le magasin utilise la délégation Kerberos pour s'authentifier auprès du Delivery Controller.
4. Accédez à l'onglet Routage HDX optimal pour configurer la passerelle utilisée pour lancer les applications et les bureaux en fonction de leur emplacement.
5. Accédez à l'onglet Publier magasin pour configurer si l'application Workspace présente le magasin à l'utilisateur lorsqu'il saisit le nom de domaine complet ou l'adresse e-mail.

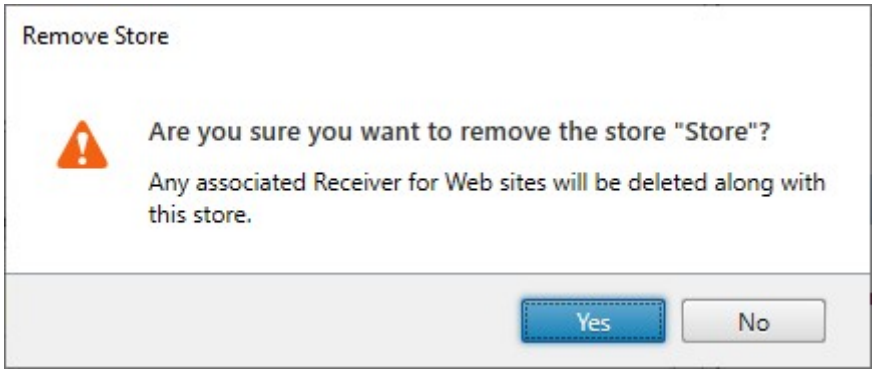


Supprimer un magasin

August 25, 2023

Pour supprimer un magasin :

1. Sélectionnez le nœud **Magasins** dans le volet gauche de la console de gestion Citrix StoreFront.
2. Dans le volet **Actions**, cliquez sur **Supprimer le magasin**.
3. Dans la fenêtre de confirmation, cliquez sur **Oui**.



Lorsque vous supprimez un magasin, tous les sites Web associés sont également supprimés.

Exporter des fichiers de provisioning de magasin pour des utilisateurs

February 22, 2024

Vous pouvez générer des fichiers contenant les détails de connexion aux magasins, y compris tout déploiement Citrix Gateway et balise configurés 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 télécharger les fichiers de provisioning de l'application Citrix Workspace lorsqu'ils accèdent à un magasin via un navigateur Web.

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

1. 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.
2. Cliquez sur **Exporter** et **Enregistrer** pour enregistrer le fichier de provisioning avec une extension .cr sur un emplacement approprié de votre réseau.

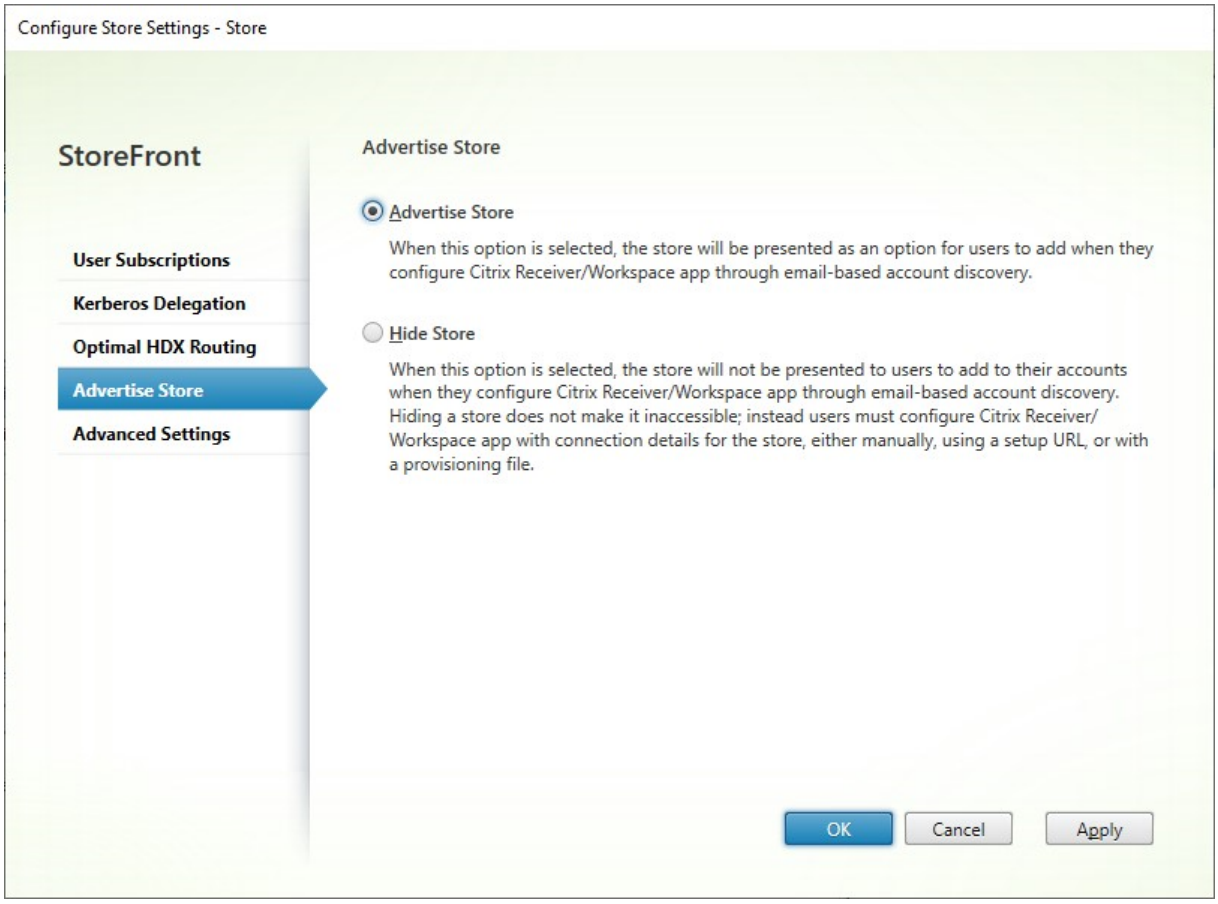
Publier et masquer des magasins pour les utilisateurs

January 25, 2024

Vous pouvez choisir si les magasins sont présentés aux utilisateurs pour qu'ils les ajoutent 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.

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

1. 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**.
2. Sur la page **Publier le magasin**, sélectionnez **Publier le magasin** ou **Masquer le magasin**.



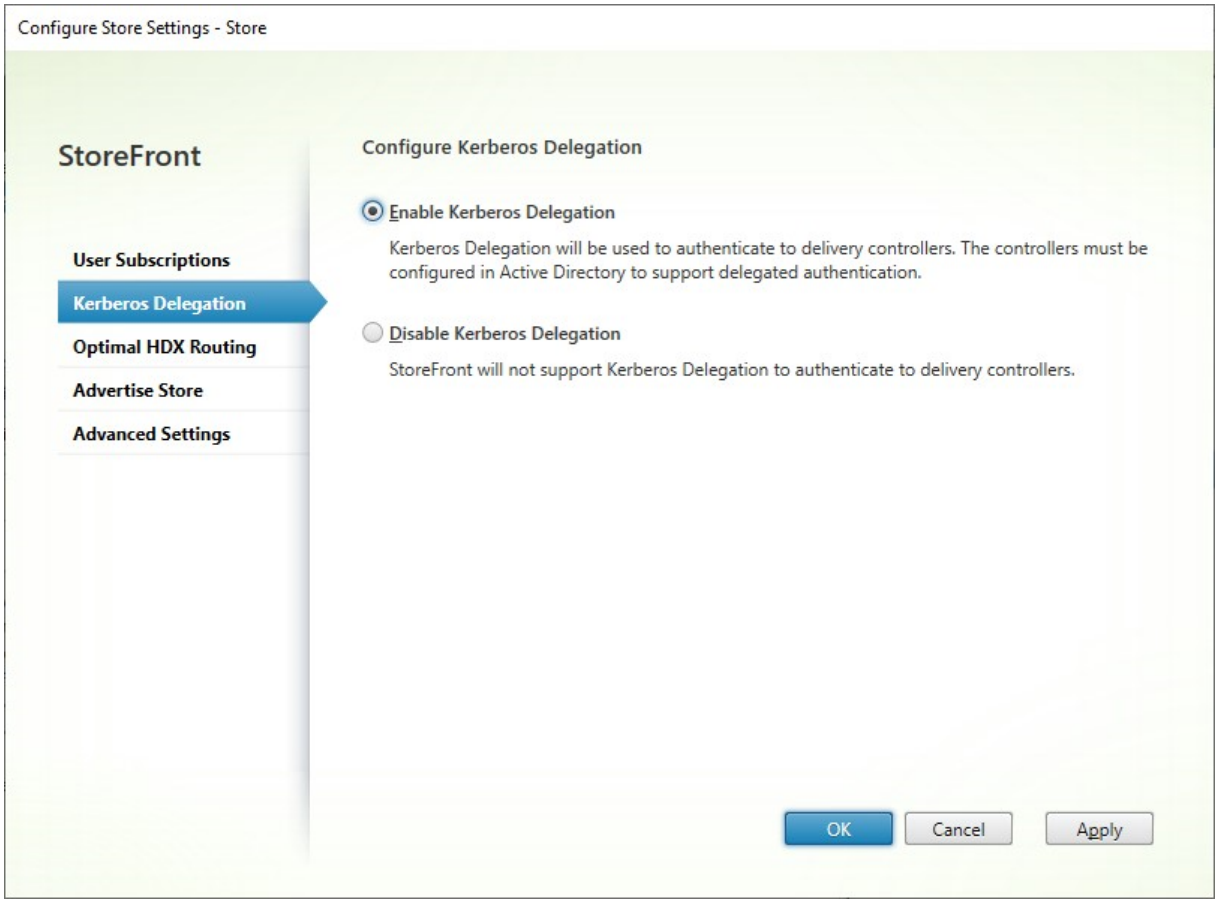
Délégation Kerberos

April 17, 2024

> **Remarque :**
>
> La délégation Kerberos est obsolète et ne peut être utilisée qu'avec XenApp 6.5 et versions antérieures. Elle ne peut être utilisée avec aucune version prise en charge de Citrix Virtual Apps and Desktops.

Lorsque vous utilisez l'authentification directe de domaine ou par carte à puce, directement ou via Citrix Gateway, StoreFront ne dispose pas des informations d'identification de l'utilisateur et ne peut donc pas s'authentifier auprès du Delivery Controller avec les informations d'identification de l'utilisateur. Lorsque vous utilisez XenApp 6.5 et versions antérieures, vous pouvez activer la délégation Kerberos pour permettre à StoreFront de se faire passer pour l'utilisateur afin de s'authentifier auprès du Delivery Controller. Cela nécessite que la délégation soit configurée dans Active Directory.

1. Sélectionnez un magasin et, dans le volet Actions, cliquez sur **Configurer les paramètres du magasin**.
2. Sélectionnez l'onglet **Délégation Kerberos**.
3. Choisissez **Activer la délégation Kerberos** ou **Désactiver la délégation Kerberos**.
4. Sélectionnez **Appliquer** ou sur **OK** pour enregistrer les modifications.



SDK PowerShell

Pour configurer la délégation Kerberos, utilisez l'applet de commande Set-STFStoreService avec le paramètre `-KerberosDelegation`.

Gérer les ressources mises à disposition dans les magasins

May 30, 2024

Utilisez l'écran **Gérer les Delivery Controller** pour ajouter, modifier et supprimer des flux de ressources fournis par Citrix Virtual Apps and Desktops, Citrix Desktops as a Service et Citrix Secure Private Access.

Afficher les flux de ressources

1. Dans la console de gestion Citrix StoreFront, dans le volet gauche, sélectionnez le nœud **Magasins** .
2. Sélectionnez un magasin dans le volet des résultats.
3. Dans le panneau **Actions**, cliquez sur **Gérer les Delivery Controller**.

Afficher les flux de ressources à l'aide du SDK PowerShell

À l'aide du SDK PowerShell, utilisez la commande Get-STFStoreFarm pour répertorier tous les flux de ressources ou un flux de ressources spécifique.

Ajouter des flux de ressources

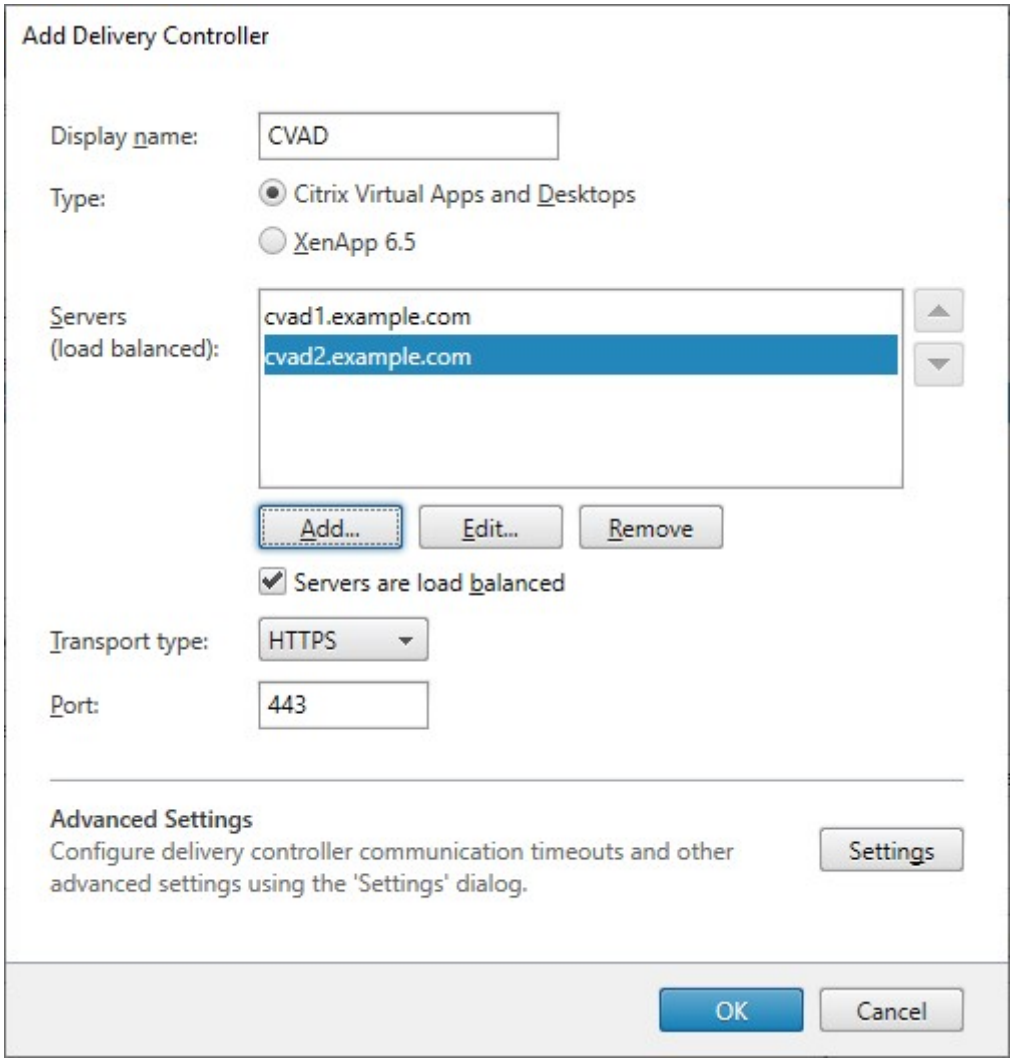
Ajouter des flux de ressources pour Citrix Virtual Apps and Desktops

1. Dans l'écran **Gérer les Delivery Controller**, cliquez sur **Ajouter**
2. Entrez un **nom d'affichage** qui vous permet d'identifier le flux.
3. Sélectionnez le **type Citrix Virtual Apps and Desktops**.
4. Sous **Serveurs**, cliquez sur **Ajouter** et entrez le nom du Delivery Controller. Répétez l'opération pour chaque Delivery Controller. Citrix vous recommande de disposer d'au moins deux serveurs pour l'équilibrage de charge ou le basculement.
5. Citrix vous recommande de sélectionner l'option **Serveurs avec équilibrage de charge**. StoreFront répartit ainsi la charge entre tous les Delivery Controller ou connecteurs en sélectionnant un serveur dans la liste au hasard lors de chaque lancement. Si cette option n'est pas sélectionnée, la liste des serveurs est traitée comme une liste de basculement par ordre de priorité. Dans ce cas, 100% des lancements se produisent sur le premier Delivery Controller ou connecteur actif dans la liste. Si ce serveur se déconnecte, 100% des lancements utilisent le second Delivery Controller dans la liste, etc.
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 des connexions cryptées (recommandé), 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 des 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 HTTP et 443 pour les connexions HTTPS. Le port spécifié doit être le port utilisé par le service XML Citrix.



Ajouter des flux de ressources pour Citrix Desktops as a Service

1. Dans l'écran **Gérer les Delivery Controller**, cliquez sur **Ajouter**
2. Entrez un **nom d'affichage** qui vous permet d'identifier le flux.
3. Sélectionnez le **type Citrix Virtual Apps and Desktops**.
4. Sous **Serveurs**, cliquez sur **Ajouter** et entrez le nom d'un connecteur cloud. Répétez l'opération pour chaque serveur ou connecteur. Citrix vous recommande de disposer d'au moins deux connecteurs pour la redondance. Si vous disposez de plusieurs emplacements de ressources, Citrix vous recommande d'ajouter les connecteurs cloud à partir de tous les emplacements de ressources afin qu'en cas de panne, StoreFront puisse utiliser le cache de l'hôte local pour lancer les VDA à l'emplacement approprié.
5. Si vous disposez de connecteurs provenant de plusieurs emplacements, Citrix vous recommande de placer les connecteurs présentant la latence la plus faible vers le serveur StoreFront

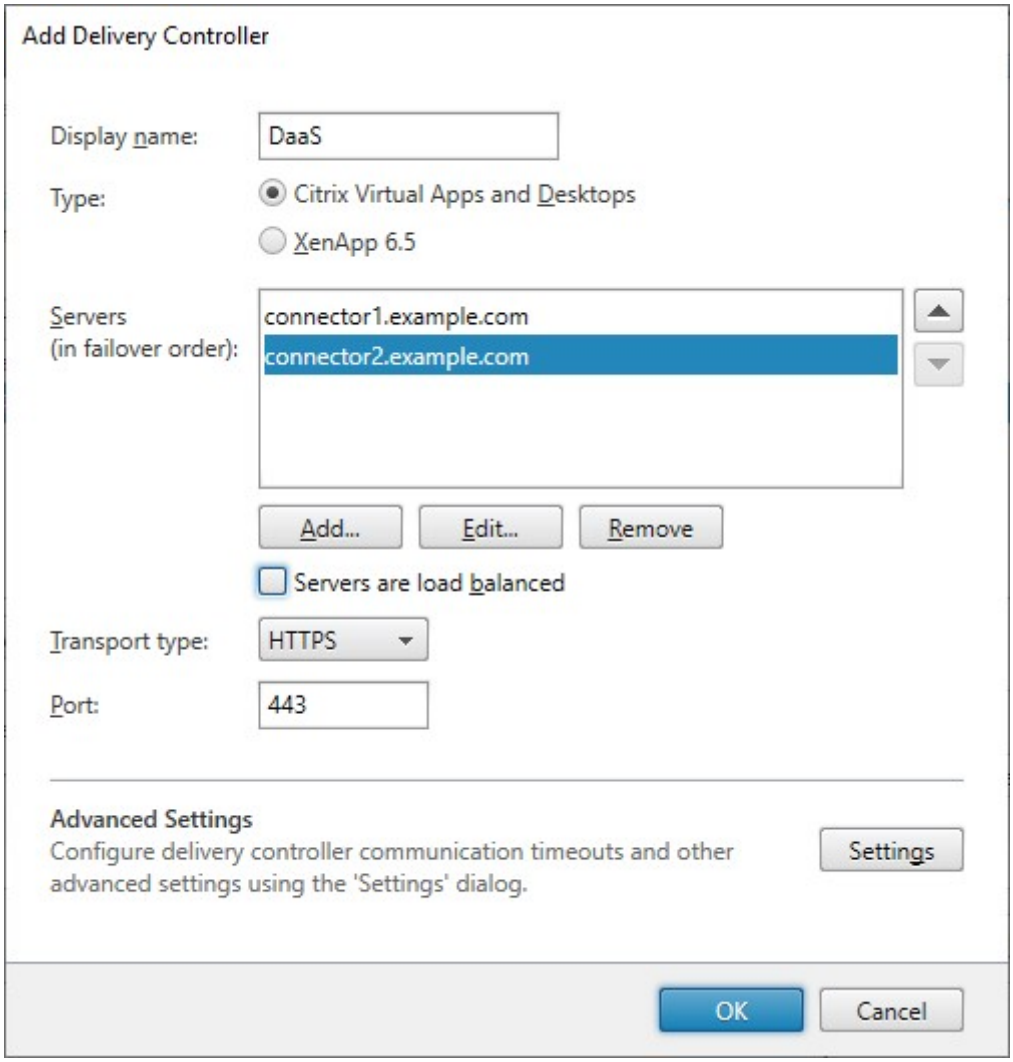
en haut de la liste et de désactiver l'option **Serveurs avec équilibrage de charge**. Comme les connecteurs ne font que transmettre des informations aux Delivery Controller DaaS, l'utilisation de l'équilibrage de charge présente des avantages limités.

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 Cloud Connector.
   - Pour envoyer des données via des connexions cryptées (recommandé), sélectionnez **HTTPS**. Si vous sélectionnez cette option, vous devez vous assurer que les Cloud Connector sont configurés pour 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 des 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 HTTP et 443 pour les connexions HTTPS.



Ajouter des flux de ressources pour XenApp 6.5

XenApp 6.5 n'est pas pris en charge par Citrix. Depuis la version 2308 de StoreFront, il n'est plus possible d'ajouter de nouveaux flux de ressources XenApp 6.5 à l'aide de la console de gestion. Vous pouvez toutefois continuer à utiliser PowerShell.

Ajouter des flux de ressources pour Citrix Secure Private Access

Si votre serveur StoreFront est configuré pour Citrix Secure Private Access, vous pouvez ajouter des flux de ressources Citrix Secure Private Access.

1. Accédez à **Magasins** > **Delivery Controller** sur StoreFront.
2. Cliquez sur **Ajouter**.

3. Dans la fenêtre **Ajouer Delivery Controller**, indiquez un **nom d'affichage** pour identifier le flux.
4. Sélectionnez le **type Citrix Secure Private Access**.
5. Entrez le nom du serveur Citrix Secure Private Access.
6. Dans la liste déroulante **Type de transport**, sélectionnez le type de connexion qui peut être utilisé pour les communications avec les serveurs.

   - **HTTP :** envoie des données via des connexions non chiffrées

   > **Remarque :**
   >
   > Si vous sélectionnez **HTTP**, vous devez prendre vos propres dispositions pour sécuriser les connexions entre StoreFront et vos serveurs.

   - **HTTPS :** envoie des données via une connexion HTTP sécurisée à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security).
7. Spécifiez le port à utiliser pour les connexions aux serveurs. Le port par défaut pour **HTTP** est 80 et, pour **HTTPS**, 443.
8. Cliquez sur **OK**.

Créer un flux de ressources à l'aide du SDK PowerShell

Pour ajouter un flux de ressources, utilisez la commande Add-STFStoreFarm.

- Pour Citrix Virtual Apps and Desktops ou Citrix Desktops as a Service, définissez `FarmType` sur `XenDesktop`.
- Pour XenApp 6.5, définissez `FarmType` sur `XenApp`.
- Pour Citrix Secure Private Access, définissez `FarmType` sur `SPA`.

Modifier un flux de ressources

Dans l'écran **Gérer les Delivery Controller**, sélectionnez un flux de ressources et cliquez sur **Modifier**.

Modifier un flux de ressources à l'aide du SDK PowerShell

Pour modifier un flux de ressources à l'aide de PowerShell, utilisez la commande Set-STFStoreFarm.

Supprimer un flux de ressources

Dans l'écran **Gérer les Delivery Controller**, sélectionnez un flux de ressources et cliquez sur **Supprimer**.

Supprimer un flux de ressources à l'aide du SDK PowerShell

Pour supprimer un flux de ressources à l'aide de PowerShell, utilisez la commande Remove-STFStoreFarm.

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

1. Dans la console de gestion Citrix StoreFront, dans le volet gauche, sélectionnez le nœud **Magasins** .

2. Sélectionnez un magasin dans le volet des résultats.
3. Dans le panneau **Actions**, cliquez sur **Gérer les Delivery Controller**.
4. Sélectionnez un Controller, cliquez sur **Modifier**, puis sur **Paramètres** dans l'écran **Modifier Delivery Controller**.
5. Sous Paramètres avancés, cliquez sur **Paramètres**.
6. 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.

Mapper les utilisateurs aux flux de ressources

Par défaut, les utilisateurs qui accèdent à un magasin voient un agrégat de toutes les ressources disponibles à partir de tous les flux de ressources 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. Vous pouvez également 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.

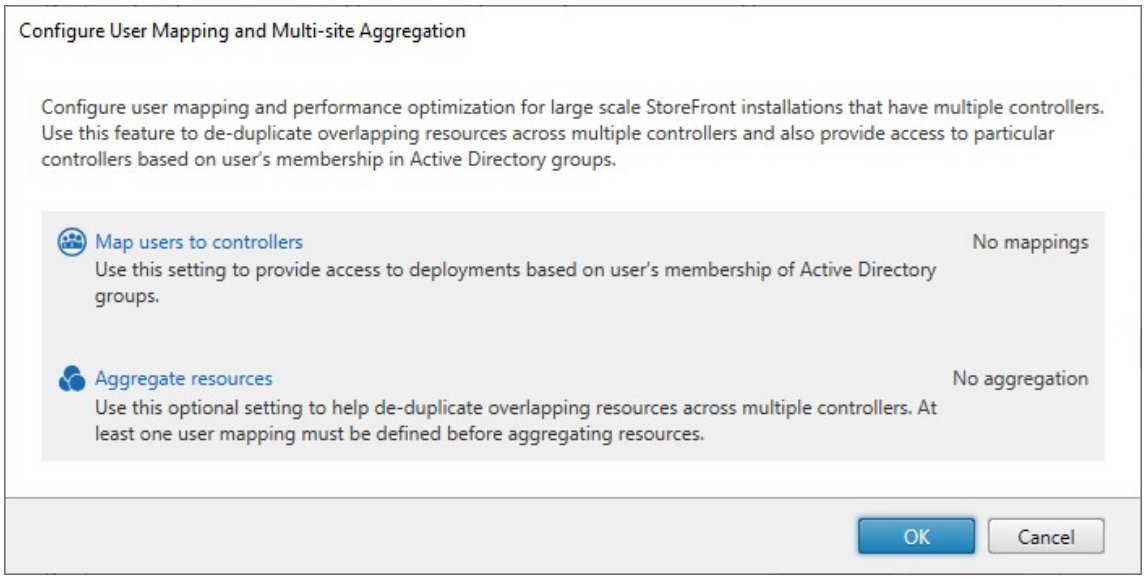
Éventuellement, vous pouvez créer un déploiement pour les utilisateurs avancés qui offre les mêmes ressources que vos autres déploiements, mais avec un matériel plus rapide et plus puissant. Cela vous permet de fournir une expérience améliorée pour les utilisateurs essentiels à l'entreprise, tels que 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.

> Remarque :
>
> Cela filtre l'intégralité des flux de ressources. En outre, dans un flux de ressources, les applications peuvent être filtrées par groupe d'utilisateurs dans la configuration Studio de Citrix Virtual Apps and Desktops.

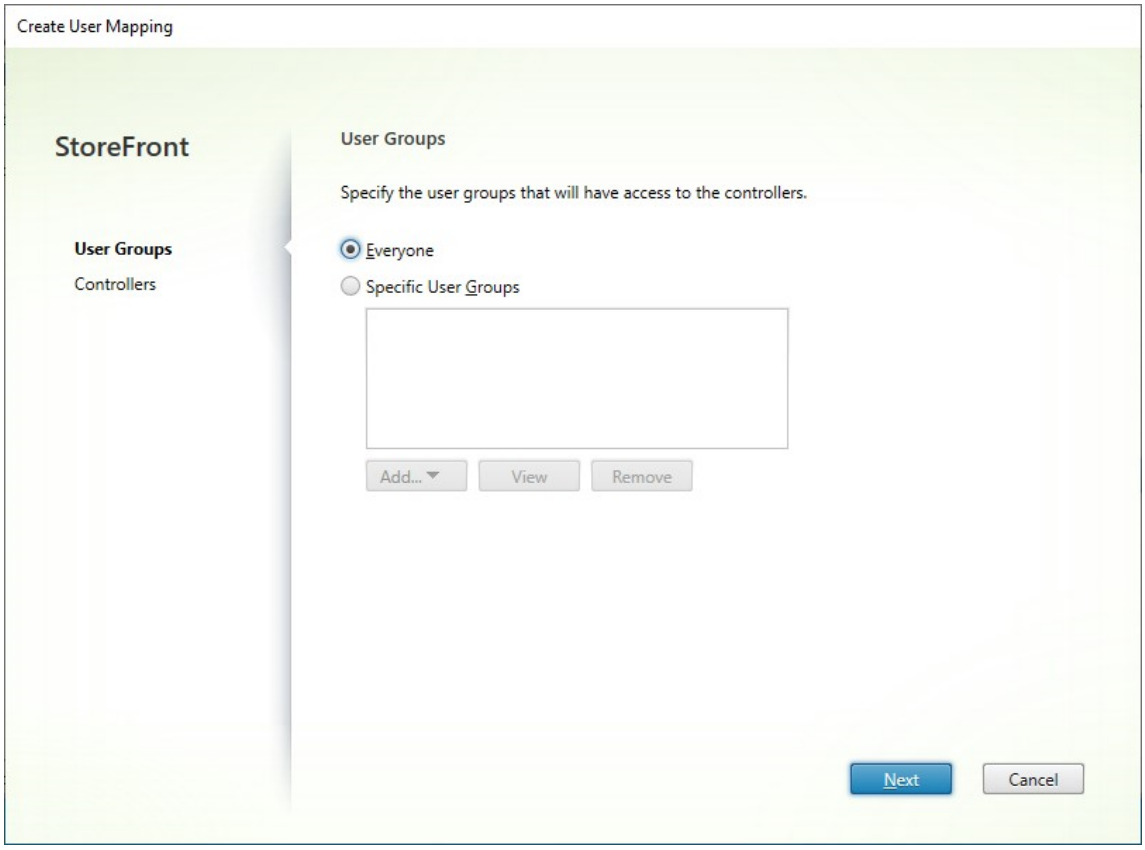
Pour configurer des flux de ressources spécifiques pour des groupes d'utilisateurs spécifiques :

1. Dans la fenêtre **Gérer les Delivery Controller**, sous **Configuration du mappage utilisateur et de l'agrégation multisite**, cliquez sur **Configurer**. Cette option n'est disponible que si au moins deux flux de ressources sont configurés.

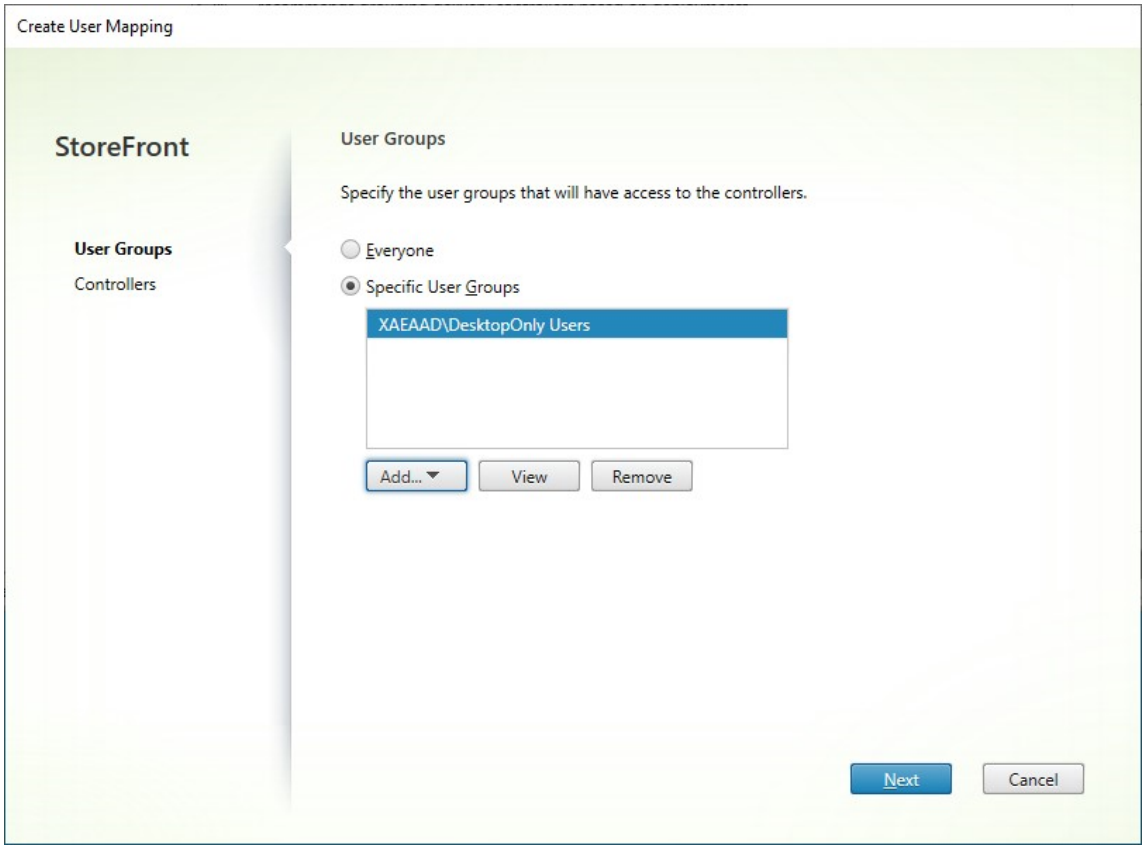
   L'écran **Configurer le mappage utilisateur et l'agrégation multisite** s'affiche.



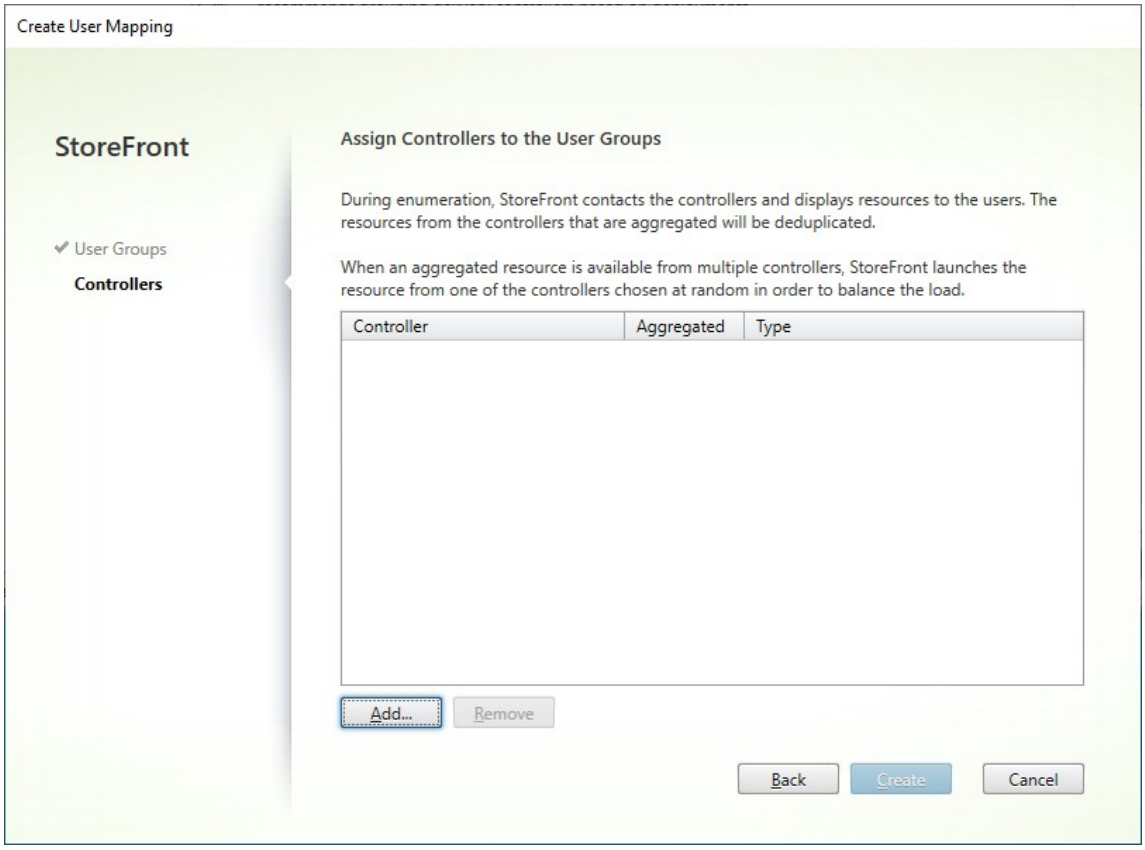
2. Cliquez sur **Mapper des utilisateurs avec des Controller**. L'écran **Créer un mappage utilisateur** s'affiche et vous permet de créer votre premier mappage. Vous pourrez créer d'autres mappages ultérieurement.



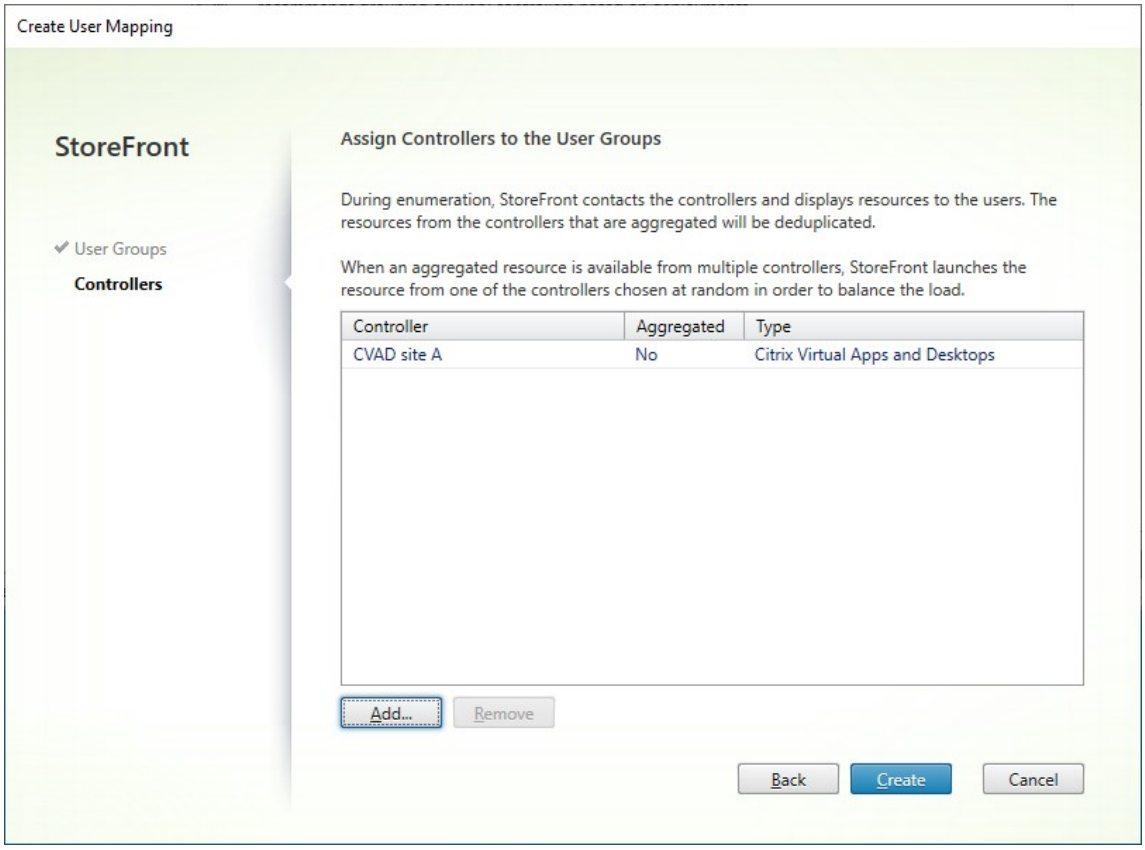
3. Choisissez **Tous** ou choisissez **Groupes d'utilisateurs spécifiques** et ajoutez un ou plusieurs groupes.



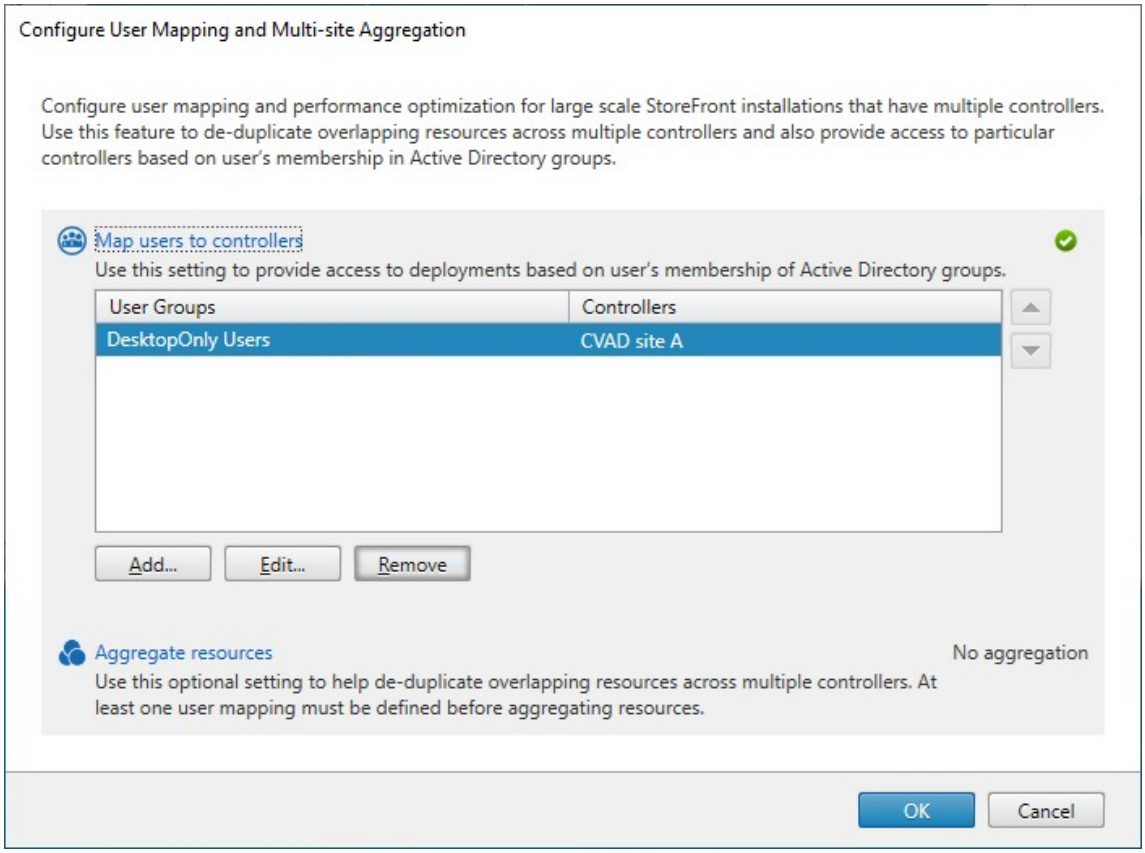
4. Cliquez sur **Suivant**. Vous êtes redirigé vers l'onglet **Delivery Controller**.



5. Cliquez sur **Ajouter** et ajoutez un ou plusieurs Delivery Controller.



6. Cliquez sur **Créer**.



7. Cliquez sur **Ajouter…** pour créer d'autres mappages selon les besoins.

Mapper les utilisateurs aux ressources à l'aide du SDK PowerShell

Vous pouvez mapper des utilisateurs à des ressources à l'aide du SDK PowerShell.

1. Pour chaque flux de ressources, créez un élément EquivalentFarmSet. Tous les flux de ressources doivent faire partie d'un ensemble de batteries, sinon ils ne seront accessibles pour aucun utilisateur. Exécutez New-STFEquivalentFarmSet avec les paramètres suivants :

   - `Name` : nom unique pour l'élément EquivalentFarmSet
   - `PrimaryFarms` : nom du flux de ressources non agrégé (batterie)

2. Pour chaque ensemble d'utilisateurs qui ont besoin d'accéder à un ensemble différent de flux de ressources, créez des mappages entre ces utilisateurs et chacun des éléments Equivalent-FarmSet. Pour créer le mappage UserFarmMapping, exécutez Add-STFUserFarmMapping avec les paramètres suivants :

   - `StoreService` : service de magasin auquel ajouter le mappage UserFarmMapping
   - `Name` : nom unique du mappage

- `GroupMembers` : table de hachage contenant les noms et les SID des groupes d'utilisateurs qui font partie du mappage. Le nom est utilisé à des fins d'affichage uniquement ; le SID définit le groupe. Pour ajouter tous les utilisateurs, créez une seule entrée dans la table de hachage avec le nom `Everyone` et la valeur `Everyone`.
- `EquivalentFarmSet` : élément EquivalentFarmSet créé à l'étape précédente

Vous devez vous assurer que chaque flux de ressources (batterie) est inclus dans au moins un mappage UserFarmMapping, sinon aucun utilisateur ne pourra accéder à cette ressource.

Agrégation multisite

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.

Avec l'agrégation multisite, 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. 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.

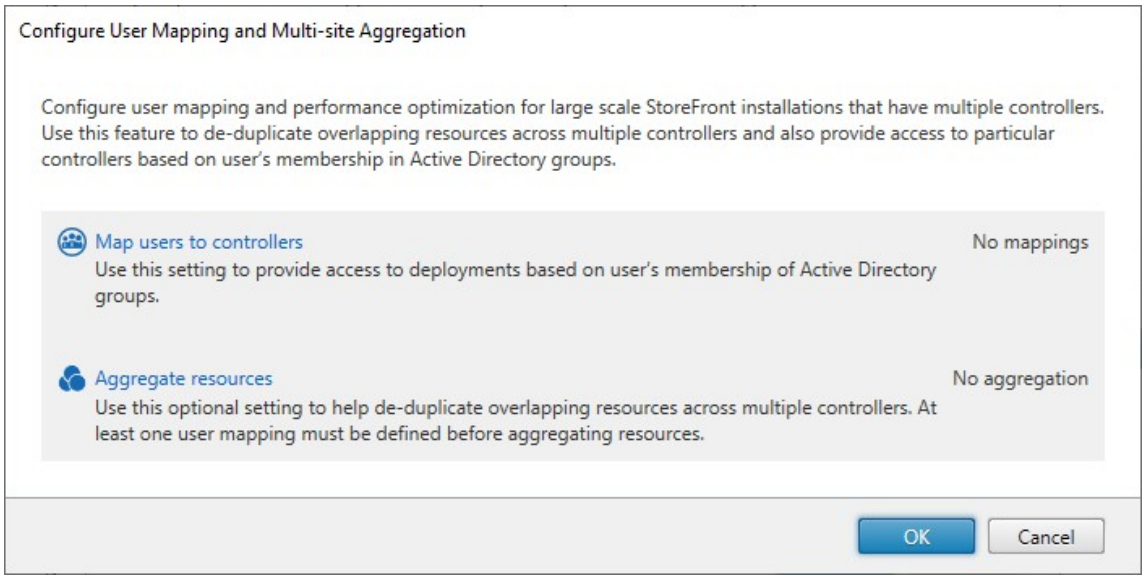
StoreFront surveille dynamiquement les serveurs qui ne répondent pas aux requêtes parce qu'ils sont surchargés ou temporairement indisponibles. Les utilisateurs sont dirigés vers les instances de la ressource sur d'autres serveurs jusqu'à ce que les communications soient rétablies. Lorsque cela est pris 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

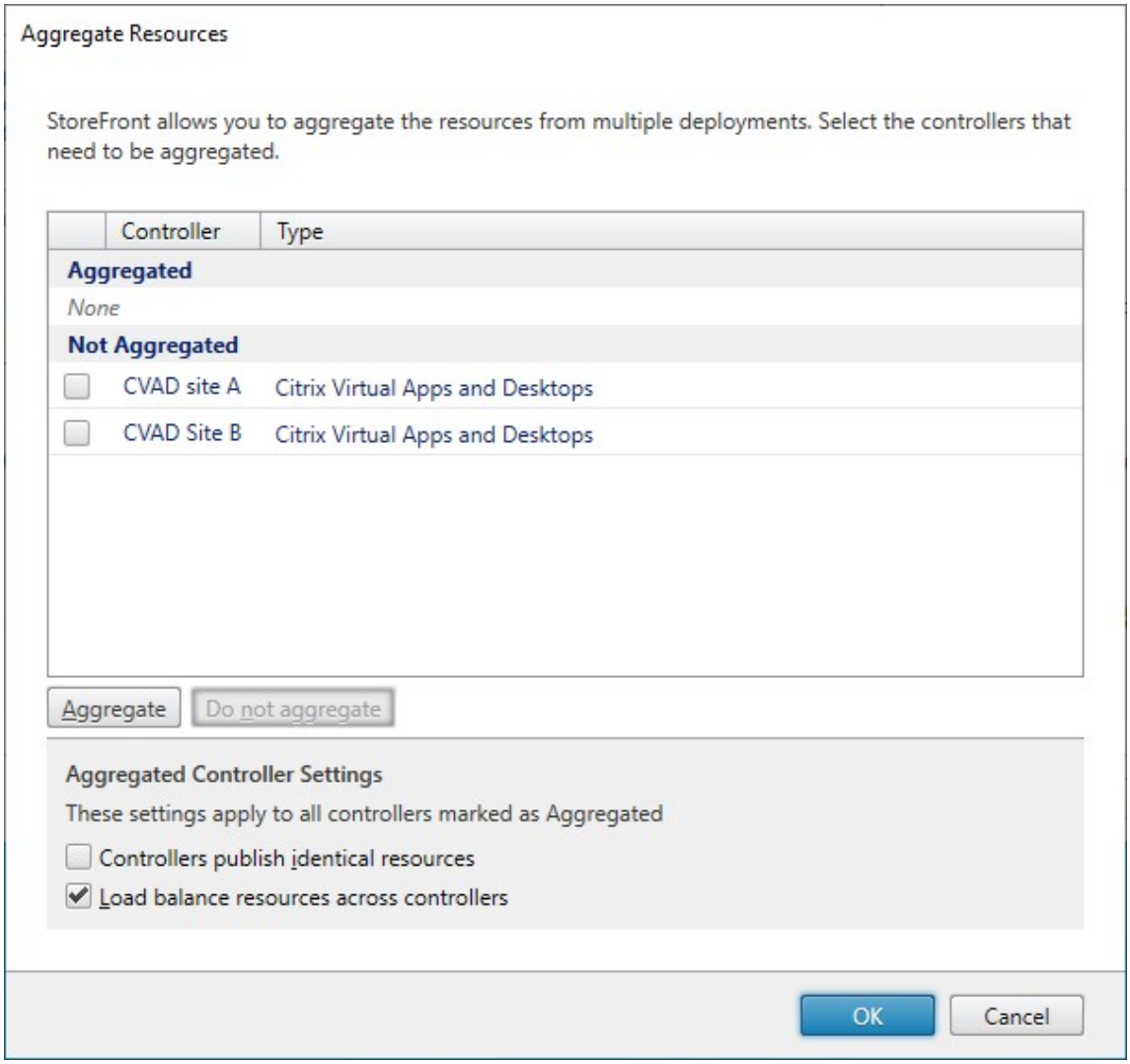
utilisateurs sont connectés au premier déploiement disponible ou de manière aléatoire à tout déploiement dans la liste. Le fait de connecter les utilisateurs au premier déploiement disponible vous permet de réduire le nombre de déploiements utilisés pour le nombre actuel d'utilisateurs. Le fait de connecter 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.

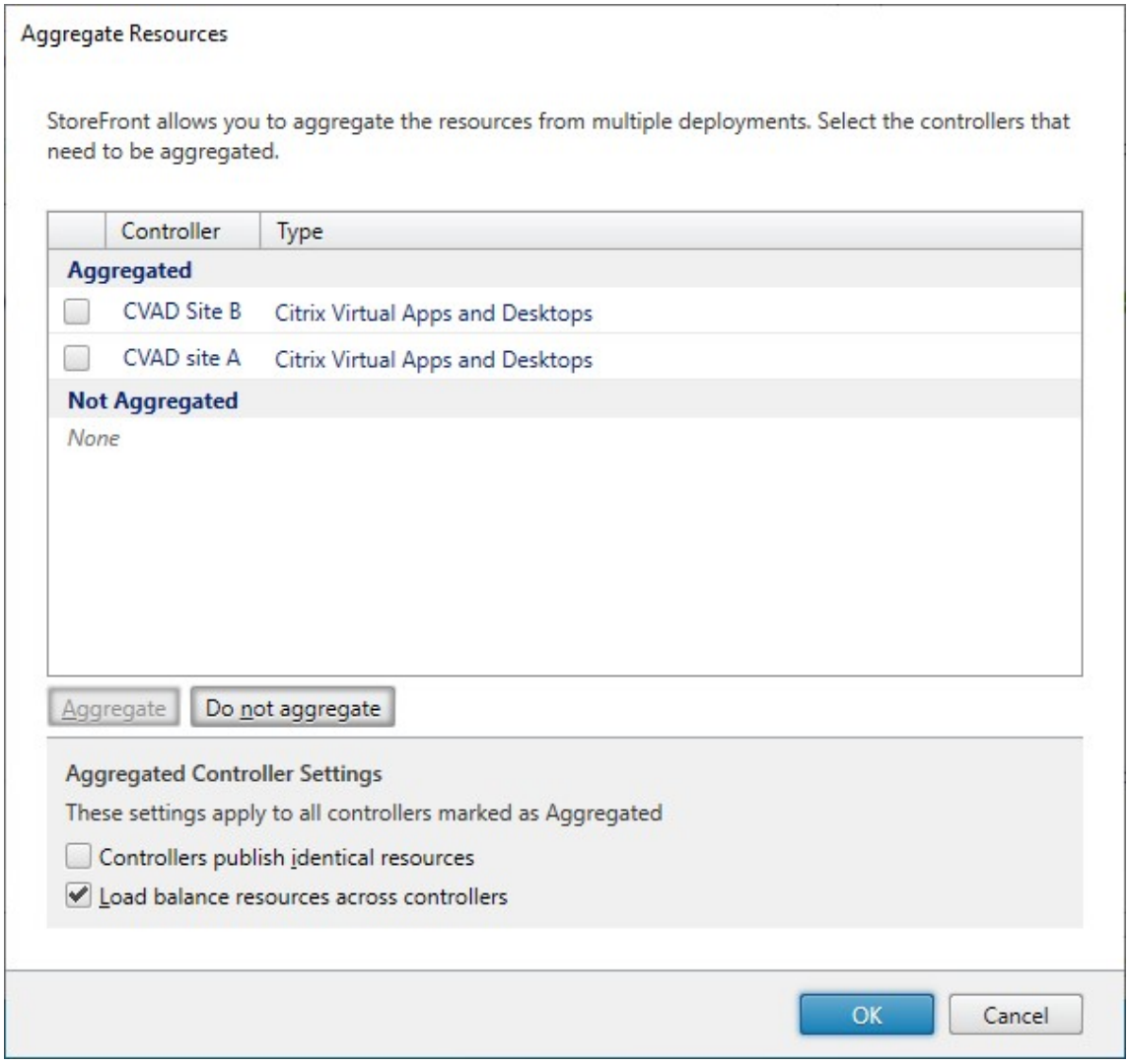
1. Sur l'écran **Gérer les Delivery Controller**, sous **Configuration du mappage utilisateur et de l'agrégation multisite**, cliquez sur **Configurer**. Cette option n'est disponible que si au moins deux flux de ressources sont configurés.



2. Cliquez sur **Agréger les ressources**. L'écran **Agréger les ressources** s'affiche.



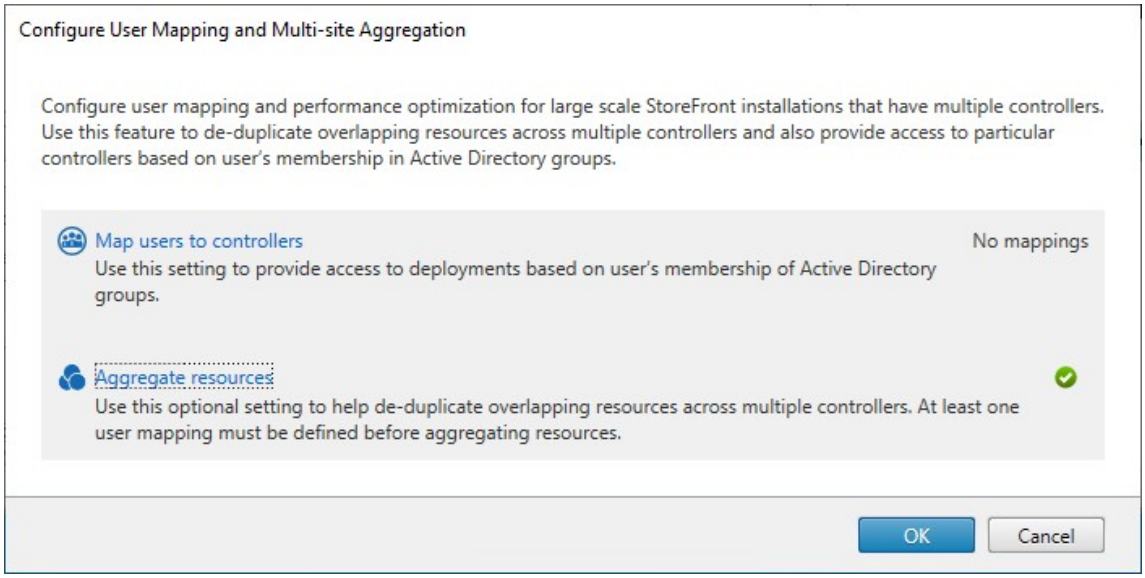
3. Choisissez les flux de ressources qui contiennent les mêmes ressources et cliquez sur **Agréger**.



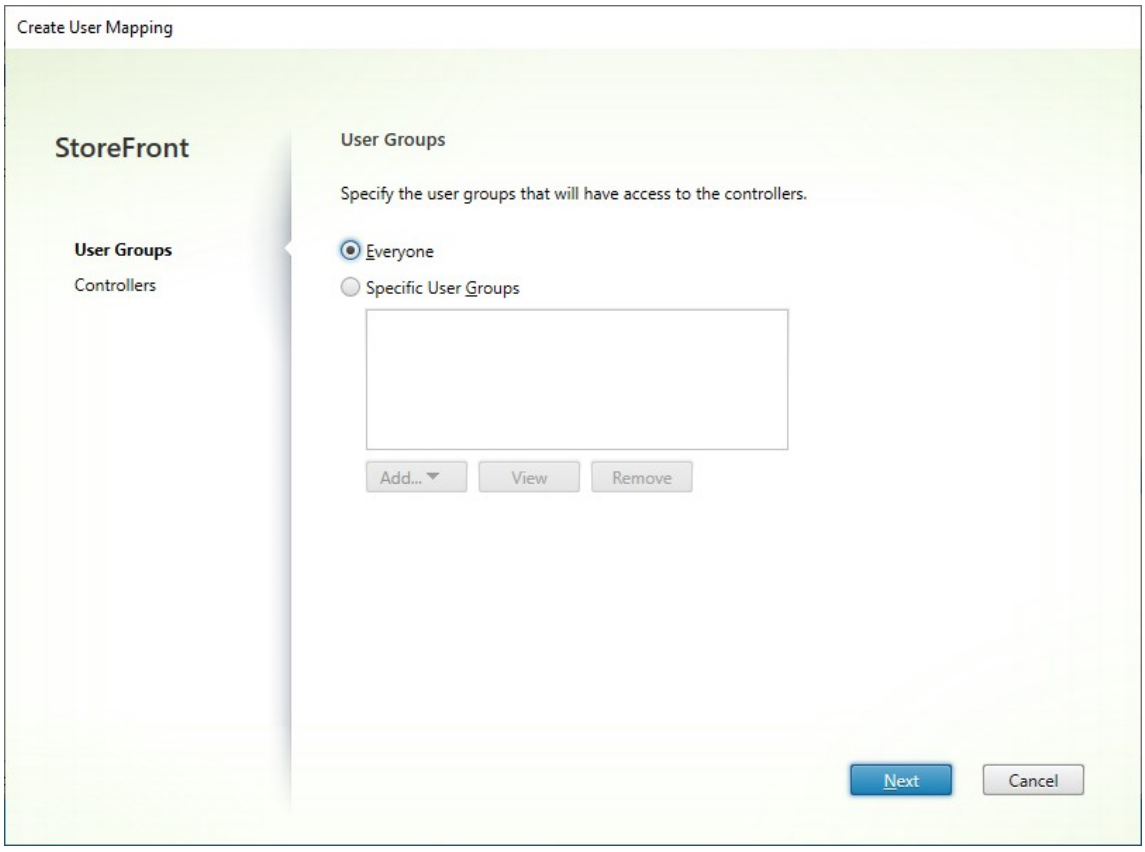
4. Sélectionnez les options **Paramètres Controller agrégés** selon les besoins :

   - **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 flux 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.

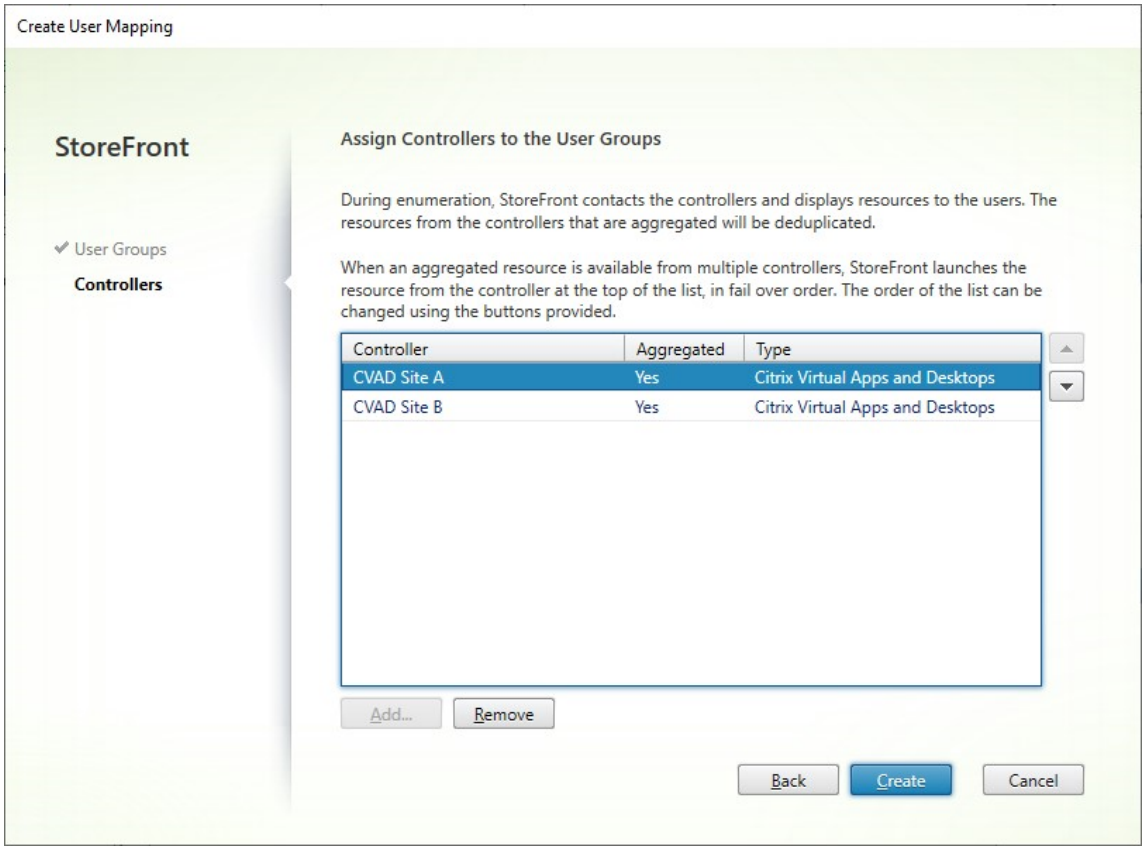
5. Cliquez sur **OK** pour revenir à l'écran **Configurer le mappage utilisateur et l'agrégation multisite**. L'option **Agréger les ressources** est désormais cochée.



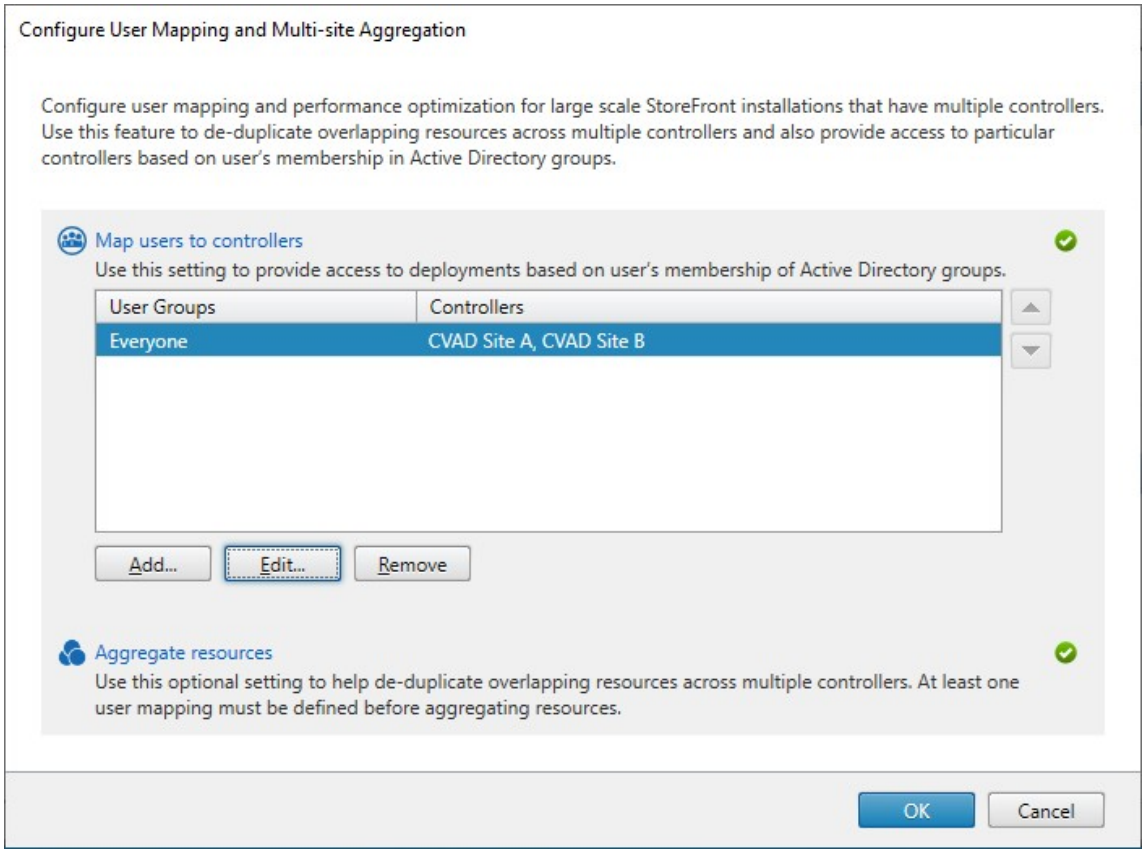
6. Lorsque les ressources sont agrégées, par défaut, aucun utilisateur n'a accès aux ressources. Vous devez donc ajouter les mappages utilisateur. Cliquez sur **Mapper des utilisateurs avec des Controller**. L'écran **Créer un mappage utilisateur** s'affiche.



7. Choisissez **Tous** ou choisissez **Groupes d'utilisateurs spécifiques** et ajoutez un ou plusieurs groupes. Par exemple, vous pouvez choisir un groupe représentant les utilisateurs d'un emplacement particulier.
8. Ajoutez les flux de ressources agrégés. Vous devez ajouter tous les flux de ressources agrégés ; ceux qui ne sont pas inclus sont alors définis sur Non agrégé. Vous pouvez également inclure des ressources non agrégées.
9. Si vous n'avez pas coché la case **Équilibrer la charge sur tous les Controller**, vous pouvez choisir l'ordre dans lequel StoreFront doit lancer les ressources.



10. Appuyez sur **Créer** pour revenir à l'écran **Configurer le mappage utilisateur et l'agrégation multisite**.



11. Ajoutez d'autres mappages si nécessaire. Assurez-vous que chaque flux de ressources est mappé sur un groupe d'utilisateurs, sinon ces ressources ne seront utilisables par personne.
12. Cliquez sur **OK**.

Configurations avancées à l'aide du SDK PowerShell

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 du SDK PowerShell 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. À l'aide de PowerShell, vous pouvez disposer de plusieurs groupes de flux dont la charge est équilibrée et basculer entre différents groupes.

> **Avertissement :**
>
> Après avoir configuré des options multisite avancées à l'aide de PowerShell, il n'est pas possible de modifier les options à l'aide de la console de gestion.

1. Décidez quels groupes d'agrégation vous souhaitez utiliser. Au sein d'un groupe d'agrégation, les applications portant le même nom d'affichage sont regroupées en une seule icône. Chaque groupe d'agrégation requiert un nom. Avec la console de gestion, vous ne pouvez créer qu'un seul groupe d'agrégation. PowerShell vous permet de définir plusieurs groupes d'agrégation.
2. Pour chaque groupe d'agrégation, créez un ou plusieurs éléments EquivalentFarmSet répertoriant les flux de ressources (appelés batteries dans le SDK) que vous souhaitez agréger. Si différents flux de ressources au sein du groupe d'agrégation sont attribués à différents utilisateurs, vous devez créer un élément EquivalentFarmSet qui est distinct pour chaque ensemble d'utilisateurs mais qui utilise le même `AggregationGroupName`. Pour créer l'élément EquivalentFarmSet, exécutez New-STFEquivalentFarmSet avec les paramètres suivants :

   - `Name` : nom unique pour l'élément EquivalentFarmSet
   - `AggregationGroupName` : nom du groupe d'agrégation auquel appartient l'ensemble de batteries
   - `LoadBalanceMode` : soit, `LoadBalanced` soit `Failover`
   - `PrimaryFarms` : batteries que vous souhaitez regrouper. Si le paramètre `LoadBalanceMode` est défini sur `Failover`, assurez-vous que les batteries sont répertoriées dans l'ordre requis. S'il existe plusieurs éléments EquivalentFarmSet pour un groupe d'agrégation, cet ordre est combiné avec la valeur IndexNumber définie dans le mappage UserFarmMapping lors de l'évaluation du flux de ressources à utiliser pour lancer une ressource.
   - `BackupFarms` : liste de batteries à utiliser au cas où aucune des batteries principales n'est disponible. Cette fonctionnalité est obsolète. Ajoutez plutôt des éléments EquivalentFarmSet supplémentaires avec une valeur IndexNumber plus élevée.

3. Pour chaque flux de ressources ne faisant pas partie d'un groupe d'agrégation, créez un élément EquivalentFarmSet sans spécifier `AggregationGroupName`. Tous les flux de ressources doivent faire partie d'un ensemble de batteries. Exécutez New-STFEquivalentFarmSet avec les paramètres suivants :

   - `Name` : nom unique pour l'élément EquivalentFarmSet
   - `PrimaryFarms` : nom de la batterie non agrégée

4. Pour chaque ensemble d'utilisateurs qui ont besoin d'accéder à un ensemble différent de flux de ressources, créez des mappages entre ces utilisateurs et chacun des éléments EquivalentFarmSet. Pour créer le mappage UserFarmMapping, exécutez Add-STFUserFarmMapping avec les paramètres suivants :

   - `StoreService` : service de magasin auquel ajouter le mappage UserFarmMapping

- `Name` : nom unique du mappage
- `GroupMembers` : table de hachage contenant les noms et les SID des groupes d'utilisateurs qui font partie du mappage. Le nom est utilisé à des fins d'affichage uniquement ; le SID définit le groupe. Pour ajouter tous les utilisateurs, créez une seule entrée dans la table de hachage avec le nom `Everyone` et la valeur `Everyone`.
- `EquivalentFarmSet` : élément EquivalentFarmSet créé à l'étape précédente
- `IndexNumber` : définit l'ordre dans lequel les flux de ressources sont évalués. Cela permet de définir l'ordre de préférence du flux de ressources à utiliser pour lancer une ressource.

Vous devez vous assurer que chaque flux de ressources (batterie) est inclus dans au moins un mappage UserFarmMapping, sinon aucun utilisateur ne pourra accéder à cette ressource.

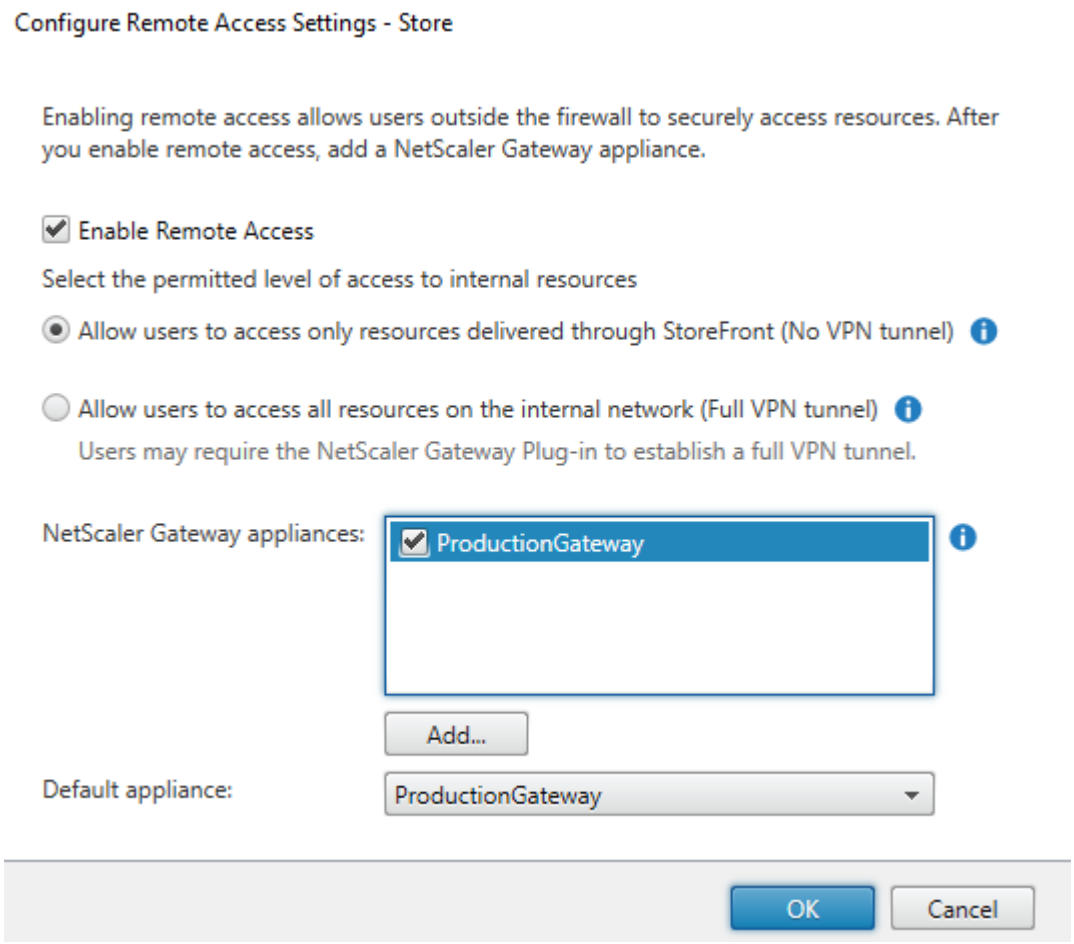
Gérer l'accès distant aux magasins via Citrix Gateway

February 22, 2024

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

1. 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**.



2. 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 util-

isateurs s'authentifient sur Citrix Gateway et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins.

3. 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 autre déploiement à la liste, cliquez sur **Ajouter** et suivez les étapes de la section Configurer Citrix Gateway.
4. 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 depuis l'application Citrix Workspace.
5. Cliquez sur **OK** pour enregistrer la configuration et fermer la boîte de dialogue Configurer l'accès distant.

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. Pour plus d'informations sur la modification des points balises, consultez la section Configurer des points balises.

Par défaut, StoreFront utilise la passerelle par laquelle l'utilisateur est connecté au magasin pour lancer des ressources. Pour configurer StoreFront afin de lancer des ressources à l'aide d'une passerelle alternative ou sans passerelle, consultez la section Routage HDX optimal.

Vérification des listes de révocation de certificats (CRL)

April 17, 2024

Introduction

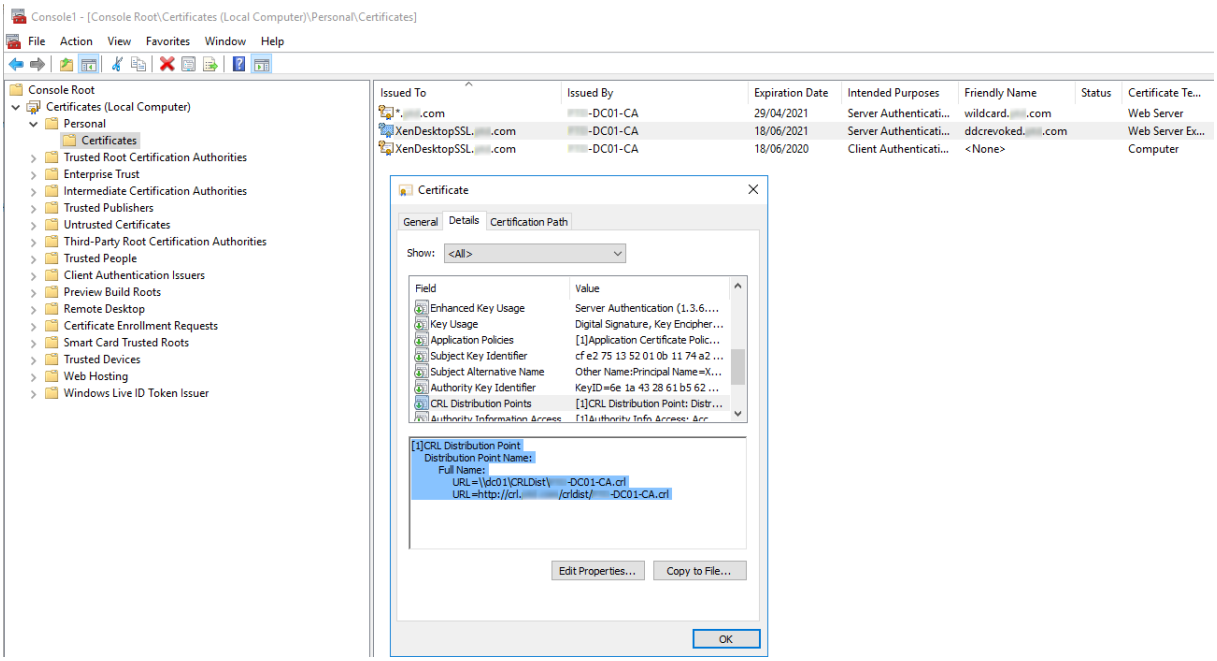
Vous pouvez configurer StoreFront pour vérifier l'état des certificats TLS utilisés par les Delivery Controller CVAD à l'aide d'une liste de révocation de certificats (CRL) publiée. Il peut être nécessaire de révoquer l'accès à un certificat si :

- 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)

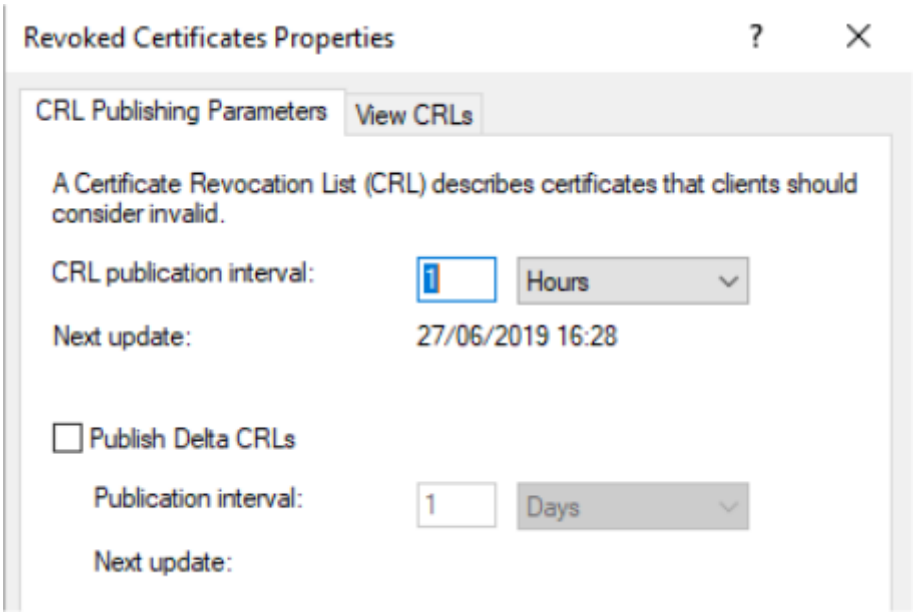
StoreFront n'énumère pas les ressources des Delivery Controller Citrix Virtual Apps and Desktops qui utilisent des certificats révoqués dont les numéros de série sont répertoriés dans la liste de révocation de certificats publiée. Pour détecter les certificats révoqués, StoreFront doit pouvoir accéder 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 StoreFront PowerShell, consultez 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.

```
1 $SiteID = 1
2 $StoreVirtualPath = "/Citrix/Store"
3 $StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
4 $StoreVirtualPath
5 Set-STFStoreFarmConfiguration -StoreService $StoreObject -
     CertRevocationPolicy "MustCheck"
6 <!--NeedCopy-->
```

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

```
1 (Get-STFStoreFarmConfiguration -StoreService $StoreObject).
     CertRevocationPolicy
2 <!--NeedCopy-->
```


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

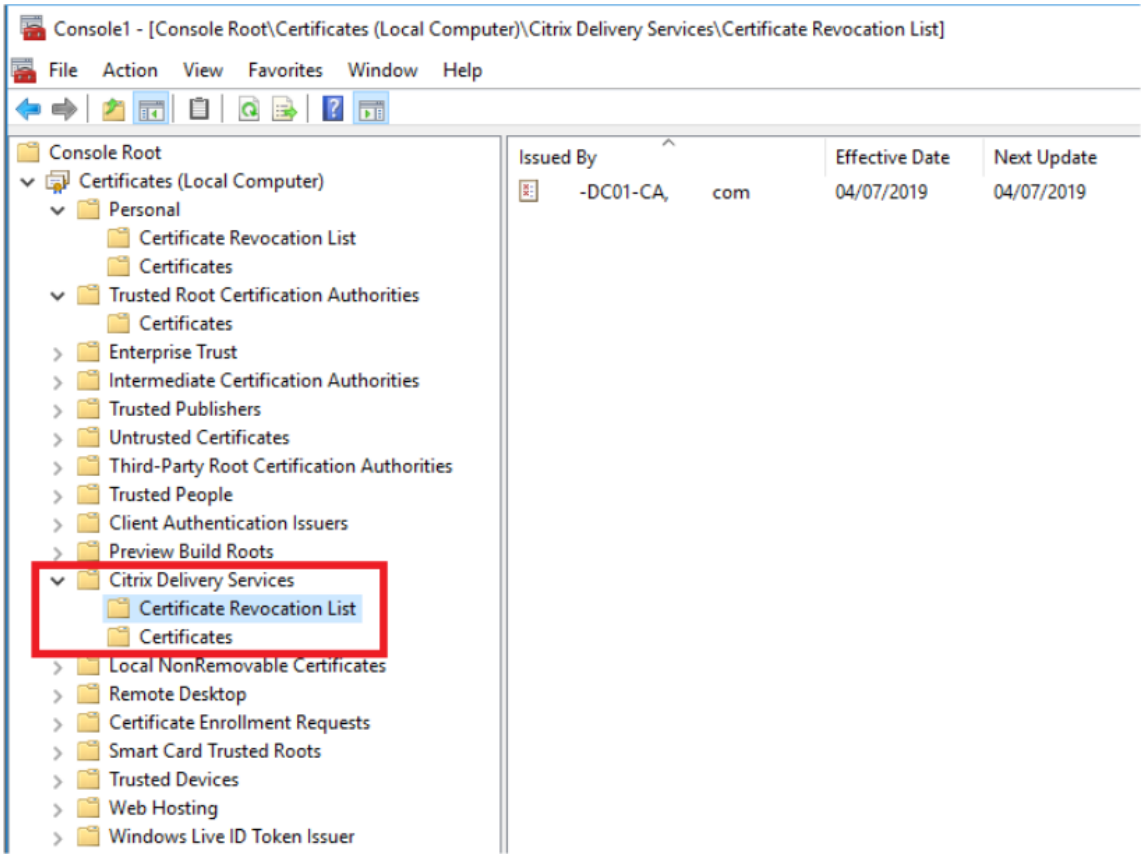
L'utilisation de listes de révocation de certificats importées localement est prise en charge, mais Citrix ne le recommande pas
car :

- 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 Configurer un magasin pour la vérification de la révocation de certificats précédente.
2. Configurez le Delivery Controller pour utiliser HTTPS, en suivant la procédure décrite dans 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 mêmes paramètres de stratégie de révocation de certificats que ceux décrits dans la section précédente.

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

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$AuthVirtualPath = "/Citrix/StoreAuth"
<!--NeedCopy-->
```


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
<!--NeedCopy-->
```

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

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

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

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
<!--NeedCopy-->
```

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

```
An SSL connection could not be established: An error occurred during
    SSL crytography: Access is denied.

This message was reported from the Citrix XML Service at address https:
    //deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.
```



```
4
5 The specified Citrix XML Service could not be contacted and has been
     temporarily removed from the list of active services.
6 <!--NeedCopy-->
```

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

```
1 An unexpected response was received during the authentication process.
2
3 Citrix.DeliveryServicesClients.Authentication.Exceptions.
     ExplicitAuthenticationFailure,
4 Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
5 Culture=neutral, PublicKeyToken=null
6
7 General Authentication Failure
8
9 ExplicitResult.State: 5
10
11 AuthenticationControllerRequestUrl:
12 https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
     LoginAttempt
13
14 ActionType: LoginAttempt
15
16 at
17 Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
     GetExplicitAuthResult(ActionType
18 type, Dictionary`2 postParams)
19 <!--NeedCopy-->
```

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

February 22, 2024

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>
<!--NeedCopy-->
```

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>
<!--NeedCopy-->
```

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 favoris d'un magasin

May 30, 2024

Vous pouvez gérer les données d'abonnement (favoris) d'un magasin 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

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

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService
 }


Remove-SubscriptionData -Store "YourStore"
<!--NeedCopy-->
```


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.

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

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.

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

Pour plus d'informations sur Restore-STFStoreSubscriptions, consultez https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/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/<
    yourstore>"
2 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
    :USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```


Pour plus d'informations sur Import-STFStoreSubscriptions, consultez https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/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

Nombre d'enregistrements	Taille en Mo
0	6,02
1 000	7,02

Nombre d'enregistrements	Taille en Mo
10 000	40,00
100 000	219,00
200 000	358,00
500 000	784,00
800 000	1213,02
1 000 000	1597,15
1 300 000	1919,15
1 500 000	2205,15
2 000 000	2915,15

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

Nombre d'enregistrements	Taille en Mo
0	0,00
1 000	0,13
10 000	1,30
100 000	12,80
200 000	25,60
500 000	64,10
800 000	102,00
1 000 000	128,00
1 300 000	166,00
1 500 000	192,00
1 700 000	218,00
2 000 000	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"
<!--NeedCopy-->
```

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

April 17, 2024

> **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'in-

tégralité 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. Consultez 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 configura-

tion.

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.

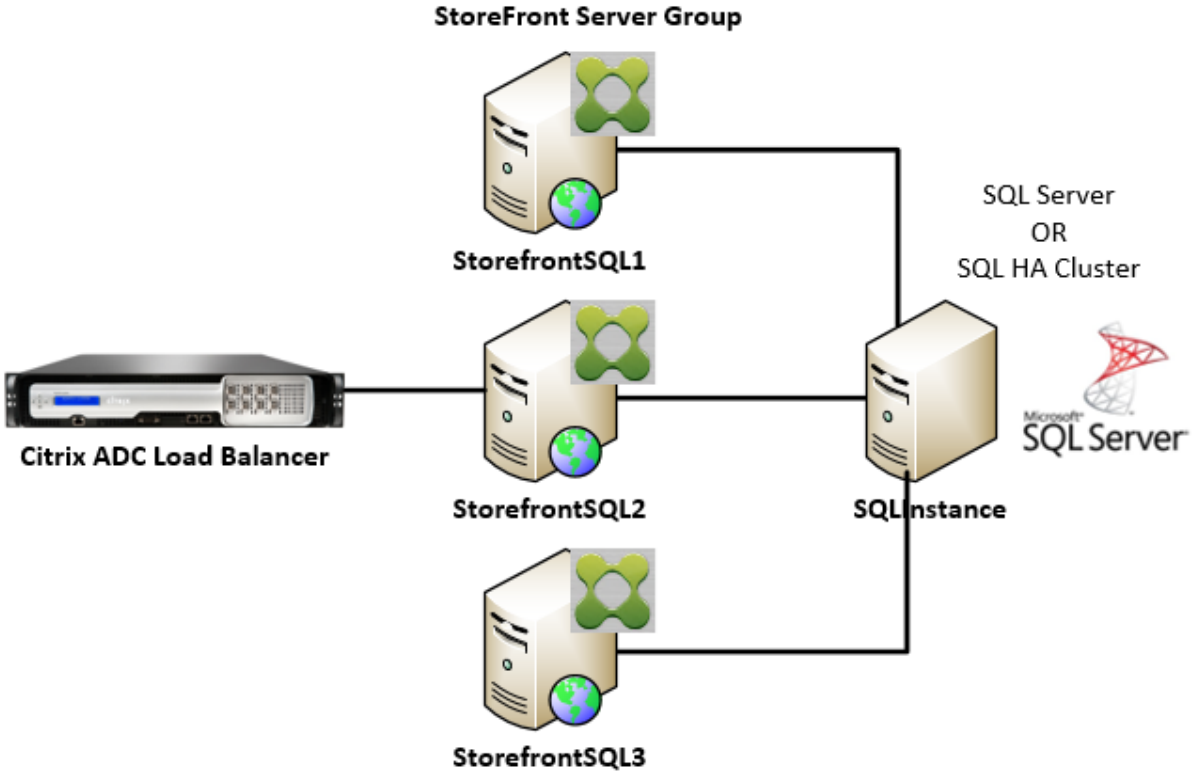
Vous pouvez utiliser quatre scénarios pour stocker des données d'abonnement dans SQL Server :

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

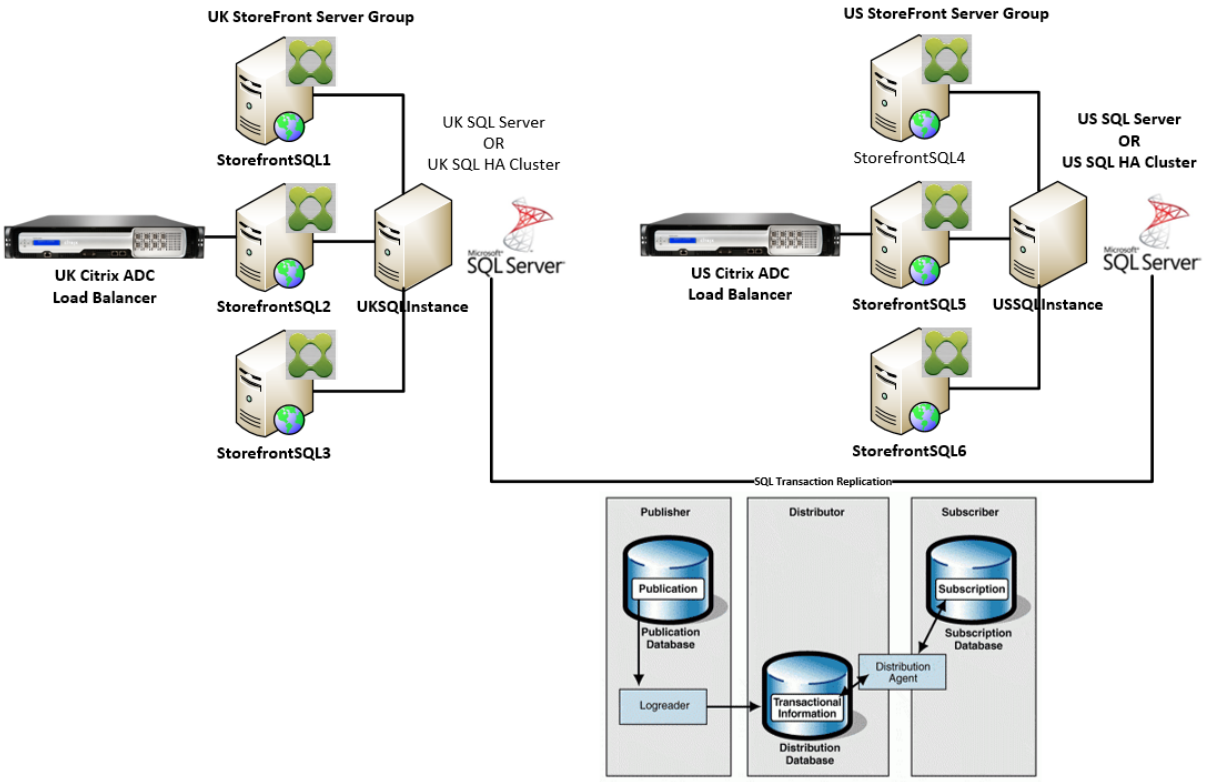
SQL. Il s'agit du modèle le plus approprié pour les déploiements de grande taille où les administrateurs Citrix souhaitent modifier fréquemment les noms de Delivery Controller ou effectuer des tâches de gestion fréquentes sur leurs données d'abonnement, telles que la suppression ou la mise à jour d'anciens 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.

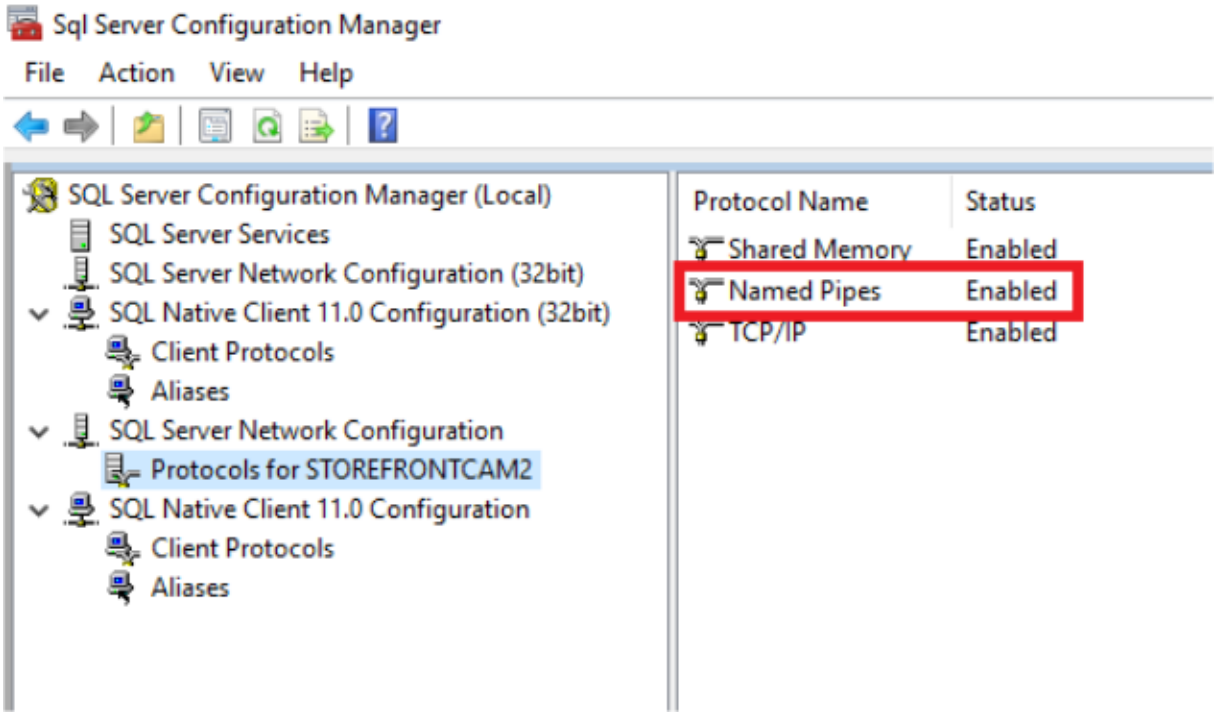
Installez StoreFront avant d'exécuter le script *Add-LocalAppPoolAccounts.ps1*. Le script dépend de la capacité de localiser le compte IIS virtuel IIS APPPOOL\Citrix Receiver for Web, qui n'existe pas tant que StoreFront n'a pas été installé et configuré. IIS APPPOOL\DefaultAppPool est créé automatiquement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

# Create Local User Group
$Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
$LocalGroup = $Computer.Create("group",$LocalGroupName)
```



```
$LocalGroup.setinfo()
$LocalGroup.description = $Description
$Localgroup.SetInfo()
Write-Host "$LocalGroupName local security group created" -
    ForegroundColor "Green"
 }

$Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"

# Add IIS APPPOOL\DefaultAppPool
$objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\DefaultAppPool")
$StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
$DefaultSID = $StrSID.Value

$Account = [ADSI]"WinNT://$DefaultSID"
$Group.Add($Account.Path)

# Add IIS APPPOOL\Citrix Receiver for Web
$objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\Citrix Receiver for Web")
$StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
$WebRSID = $StrSID.Value

$Account = [ADSI]"WinNT://$WebRSID"
$Group.Add($Account.Path)

Write-Host "AppPools added to $LocalGroupName local group" -
    ForegroundColor "Green"
<!--NeedCopy-->
```

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.

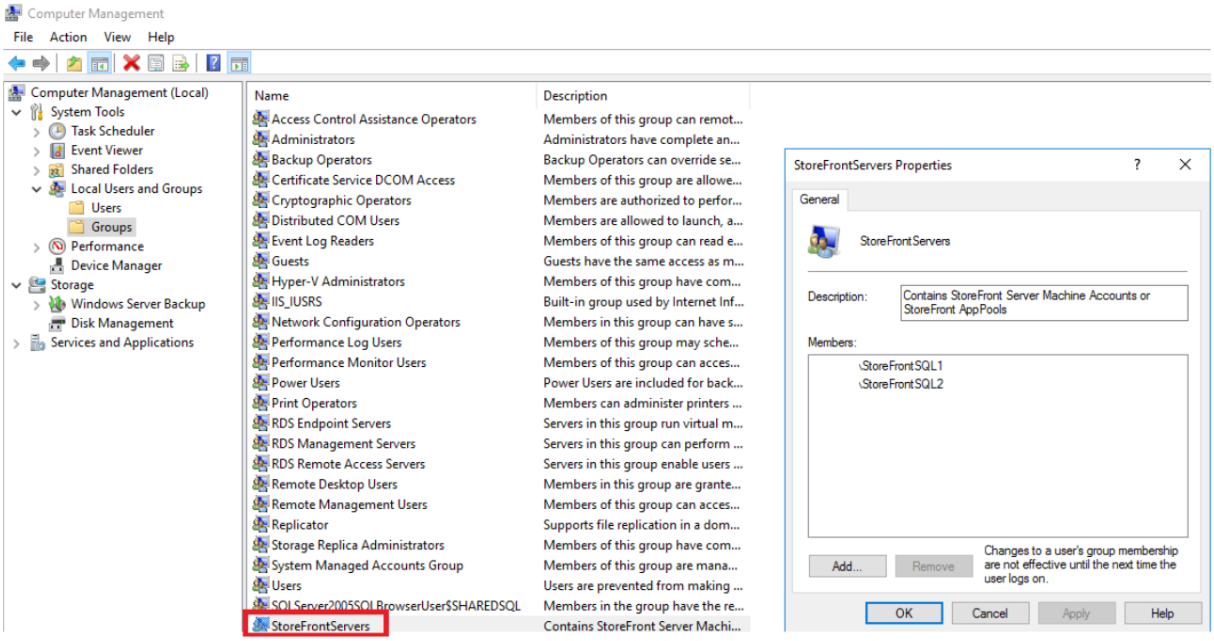


Vérifiez que les règles de pare-feu Windows sont correctement configurées pour autoriser les connexions SQL Server à l'aide d'un port spécifique ou de ports dynamiques. Reportez-vous à la documentation Microsoft pour savoir comment procéder dans votre environnement.

> **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"
 }

else
{

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

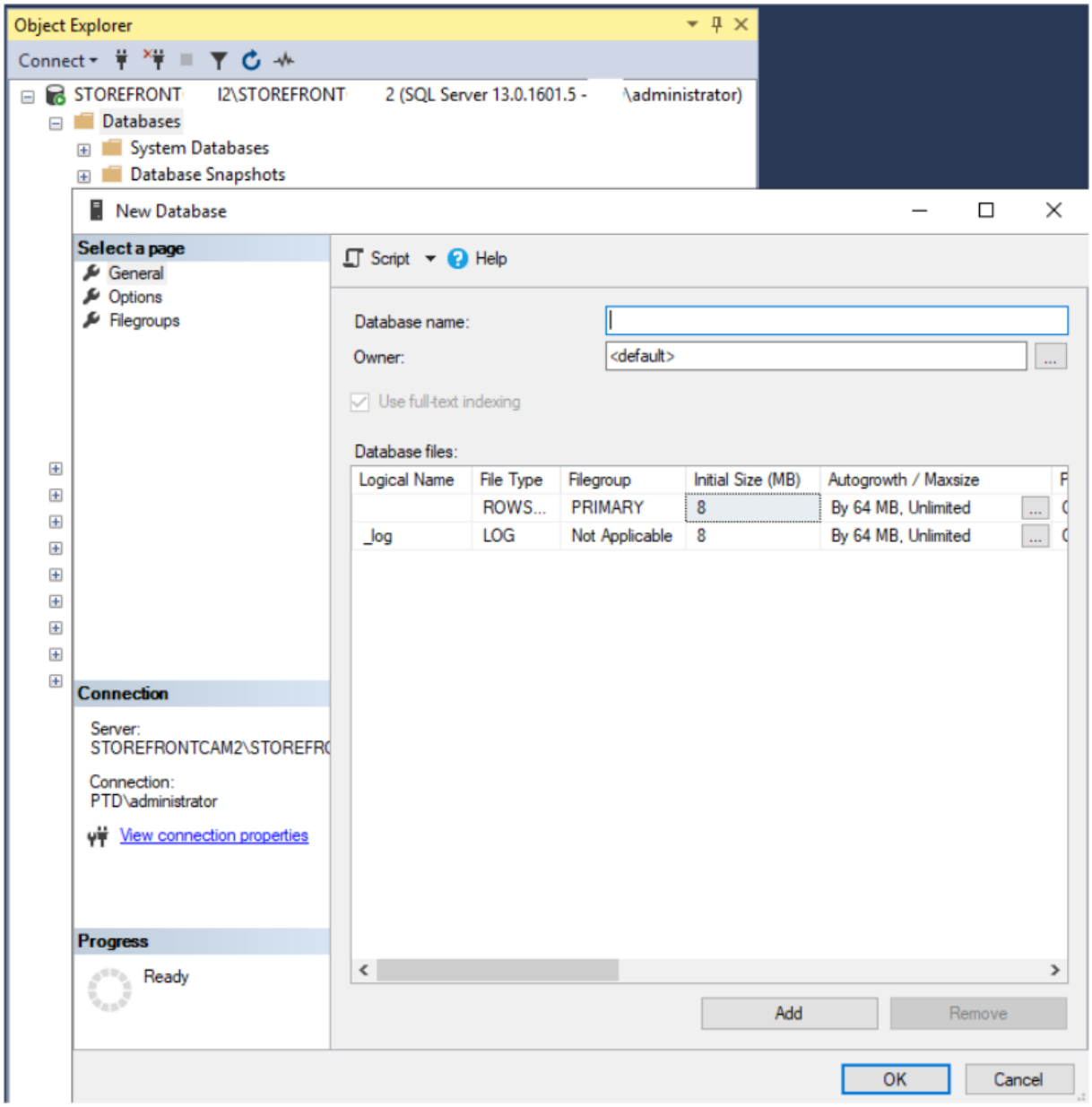


```
        "Yellow"

    # Create Local Security Group
    $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
    $LocalGroup = $Computer.Create("group",$LocalGroupName)
    $LocalGroup.setinfo()
    $LocalGroup.description = $Description
    $Localgroup.SetInfo()
Write-Host "$LocalGroupName local group created" -ForegroundColor "
    Green"
 }

Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -
    ForegroundColor "Yellow"

foreach ($StoreFrontServer in $StoreFrontServers)
{

    $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
    $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
    $Group.Add($Computer.Path)
 }

Write-Host "$StoreFrontServers added to $LocalGroupName" -
    ForegroundColor "Green"
 }

Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @("
    StoreFrontSQL1","StoreFrontSQL2")
<!--NeedCopy-->
```

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 :

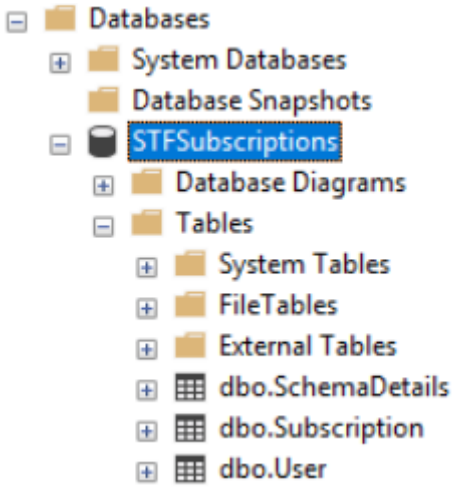
- Nommez chaque base de données que vous créez pour qu'elle corresponde au nom du magasin dans StoreFront dans `USE [STFSubscriptions]`.
- Définissez le chemin d'accès aux fichiers .mdf et .ldf de la base de données sur l'emplacement où vous souhaitez stocker la base de données.


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

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

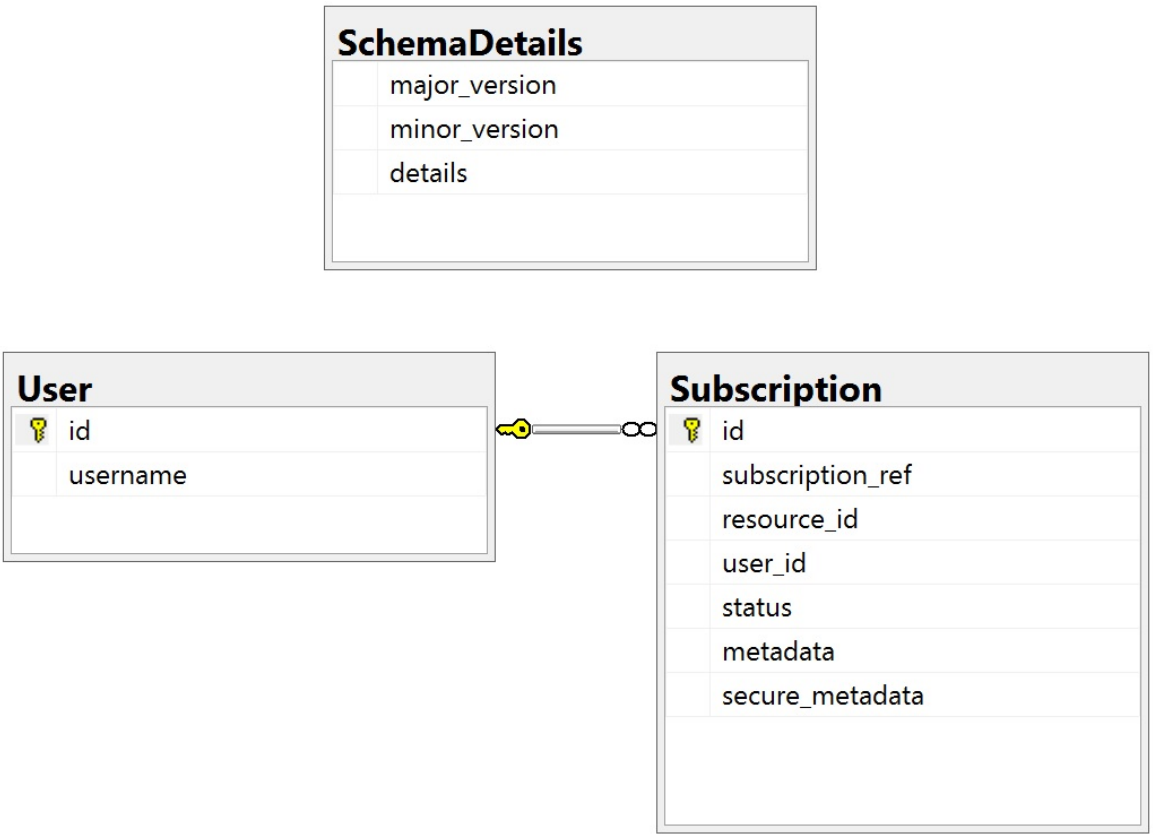
- Définissez la référence sur le nom de votre instance SQL Server dans le script :

```
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
<!--NeedCopy-->
```

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"
$SQLInstance = "StoreFrontInstance"

# For a remote database instance
$ConnectionString = "Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"
<!--NeedCopy-->
```

OU

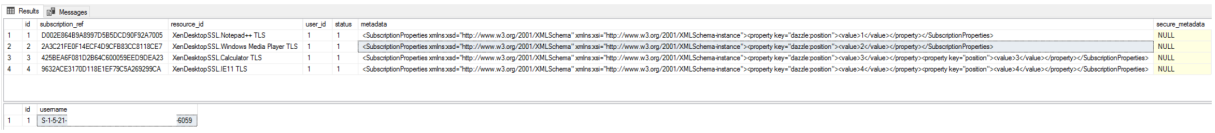
```
# For a locally installed database instance
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/
    Citrix/Store"
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

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` depuis 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.

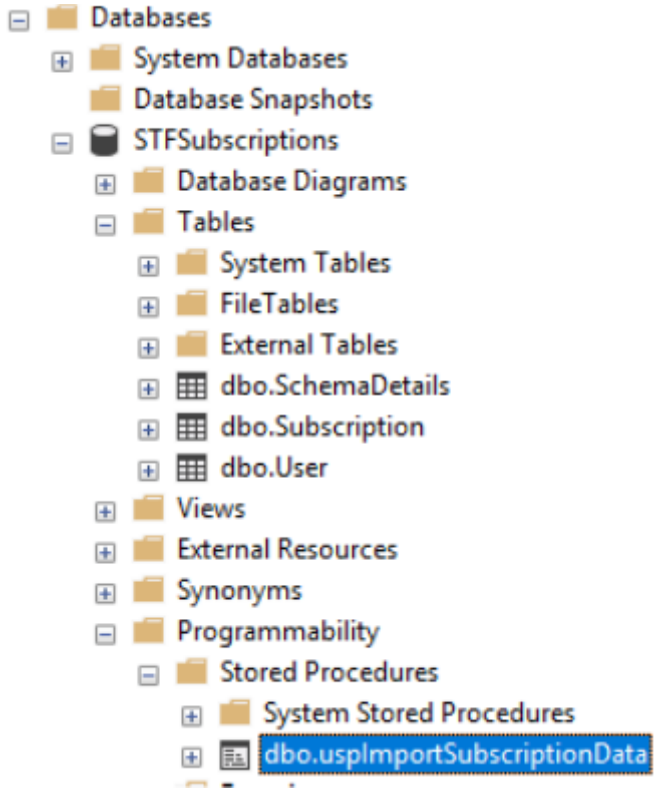
Le script Create-ImportSubscriptionDataSP.sql crée une procédure stockée T-SQL afin d'importer en bloc les données d'abonnement. Il supprime les entrées en double pour chaque utilisateur unique afin que les données SQL résultantes soient correctement normalisées et divisées en tables correctes.

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.

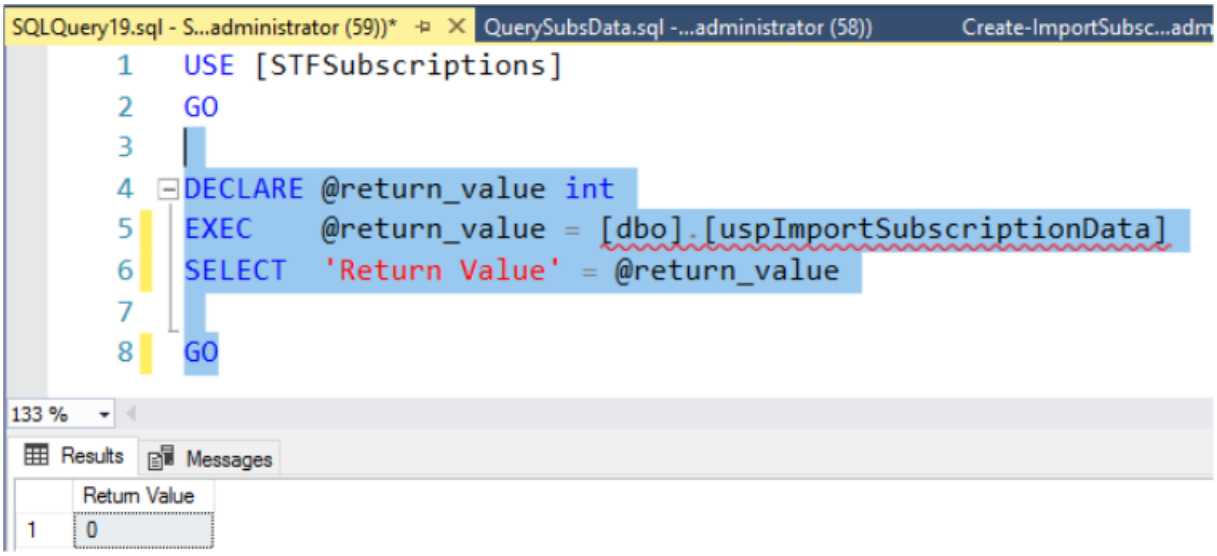
Ouvrez le fichier *Create-ImportSubscriptionDataSP.sql* à l'aide de SQL Server Management Studio et exécutez le code qui s'y trouve. Ce script ajoute la procédure stockée *ImportSubscriptionDataSP* à la base de données que vous avez créée précédemment.

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 fournis 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]
<!--NeedCopy-->
```

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]
<!--NeedCopy-->
```

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]
<!--NeedCopy-->
```

```
-- 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'
<!--NeedCopy-->
```

```
-- 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'
<!--NeedCopy-->
```

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.%'
<!--NeedCopy-->
```

```
-- After enabling multi-site aggregation, update the resource_id
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

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

```
-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
<!--NeedCopy-->
```



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

```
-- 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'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular user SID
-- relies on cascade to delete records from [Subscription]
Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

```
-- 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)
<!--NeedCopy-->
```

Activer ou désactiver les favoris

December 6, 2023

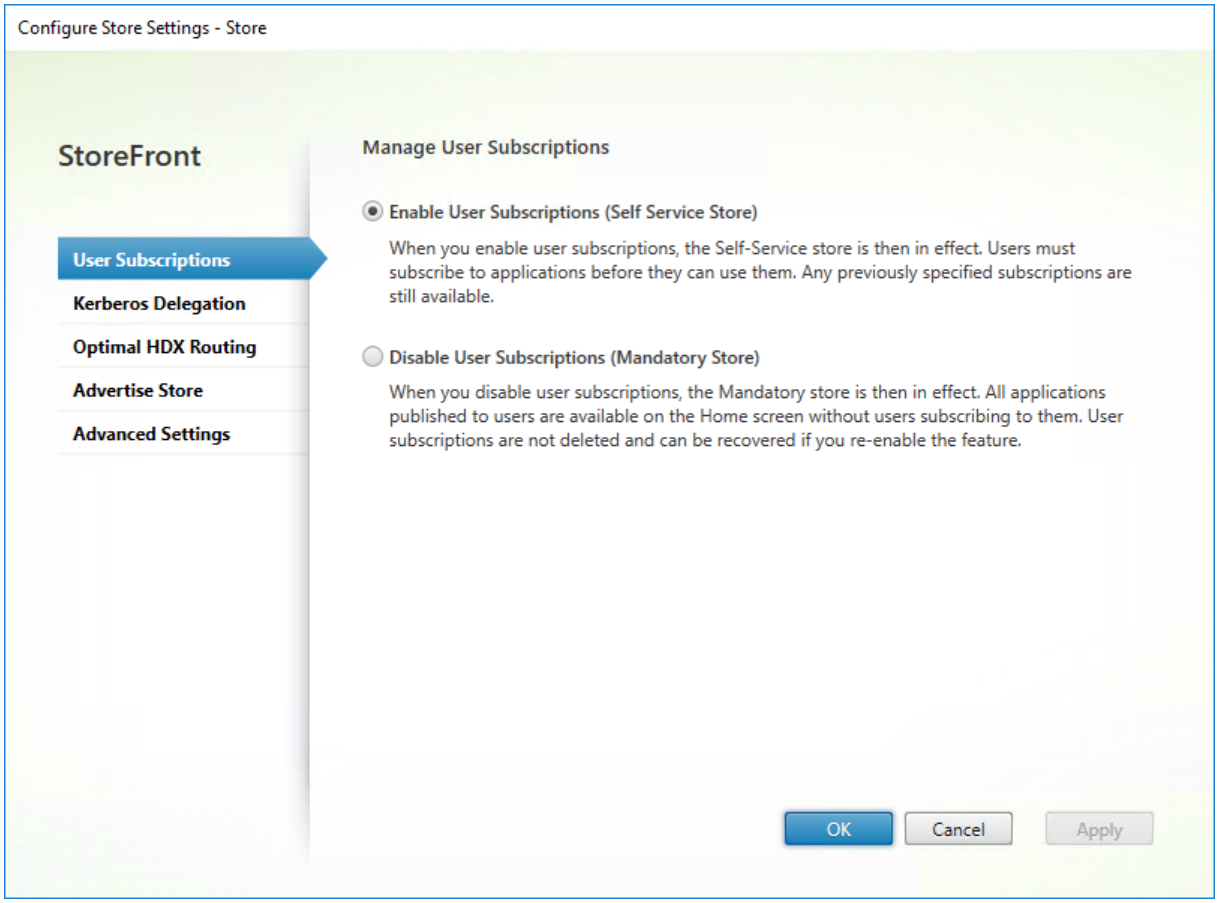
Utilisez l'écran Abonnements utilisateur pour sélectionner l'une des options suivantes :

- Permettre aux utilisateurs de créer et de supprimer des favoris (magasin en libre-service). Les utilisateurs peuvent ajouter une application à leurs favoris en cliquant sur l'étoile sur la vignette de l'application. Les utilisateurs peuvent à nouveau cliquer sur l'étoile pour retirer une application de leurs favoris. Les applications figurant dans les favoris sont affichées dans l'onglet **Accueil**.

- Désactiver les favoris (magasin obligatoire). Les utilisateurs ne peuvent pas ajouter ou retirer des applications de leurs favoris. L'onglet Accueil ne s'affiche pas.

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 ses favoris lors de la prochaine connexion.

1. Sélectionnez le nœud **Magasins** 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. Cliquez sur l'onglet **Abonnements utilisateur** pour activer ou désactiver la fonctionnalité des favoris de l'utilisateur.
3. Choisissez **Activer les abonnements utilisateur (Magasin en libre-service)** pour activer les favoris.
4. Choisissez **Désactiver les abonnements utilisateur (Magasin obligatoire)** pour désactiver les favoris.



Vous pouvez également utiliser l'applet de commande PowerShell Get-STFStoreService pour configurer les abonnements utilisateur pour un magasin, par exemple :


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

Configuration Citrix Virtual Apps and Desktops

April 17, 2024

Lors de la mise à disposition d'applications avec Citrix Virtual Apps and Desktops ou Citrix Desktops as a Service, 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 Applications.

- Dans le champ **Nom de l'application (pour l'utilisateur)**, saisissez le nom de l'application tel que vous souhaitez qu'il apparaisse sur le site Web de votre magasin.
- Dans le champ **Description et mots clés**, entrez la description qui s'affiche sur le site Web du magasin lorsque vous développez les détails de l'application, à côté des mots clés.
- Choisissez l'**icône Application** pour aider les utilisateurs à identifier visuellement une application sur le site Web StoreFront.
- Dans le champ facultatif **Catégorie d'application**, entrez une catégorie. Incluez \ dans le nom de la catégorie pour créer une hiérarchie de dossiers. Vous pouvez, par exemple, regrouper les applications en fonction de leur type ou créer des dossiers pour différents rôles d'utilisateur dans votre organisation. Dans l'onglet **Applications** du site Web du magasin, la vue **Catégories** affiche la liste des catégories et les applications de chaque catégorie.

Mots clés

Vous pouvez ajouter des mots clés à une application ou à un bureau en ajoutant la chaîne `KEYWORDS:[keywordname]` à la description de l'application. Les mots-clés multiples doivent uniquement être séparés par des espaces ; par exemple, `KEYWORDS:Accounts Featured`. Les mots clés peuvent être utilisés de différentes manières :

- Filtrer les applications (voir Paramètres avancés du magasin)
- Créer des groupes d'applications recommandées
- Certains mots clés ont une signification particulière.

Nom du mot clé	Description
Mandatory	Ajoute une application dans l'onglet Accueil. Contrairement aux applications préférées, les applications obligatoires ne peuvent pas être supprimées de l'onglet Accueil. Cela n'a aucun effet si les applications préférées sont désactivées pour le magasin.
Auto	Lorsque les utilisateurs se connectent au magasin, l'application ou le magasin est automatiquement mis en favoris et ajouté à leur onglet Accueil. Les utilisateurs peuvent supprimer ces applications de leurs favoris. Cela n'a aucun effet si les applications préférées sont désactivées pour le magasin.
TreatAsApp	Appliquez ce mot clé aux bureaux pour obliger StoreFront à le traiter comme une application. Le bureau est affiché dans l'onglet **Applications** plutôt que dans l'onglet **Bureaux**. De plus, le bureau n'est pas automatiquement démarré lorsque l'utilisateur ouvre une session sur le site Web du magasin 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.
prefer="*application*"	Où *application* représente une application installée localement. S'applique uniquement à l'application Citrix Workspace sous Windows. Cela indique 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 plus d'informations, consultez Configuration des applications Local App Access.
Primary et **Secondary**	Lorsque vous utilisez l'agrégation multisite, l'application associée au mot clé **primary** est toujours préférée à celle associée au mot clé **secondary**.

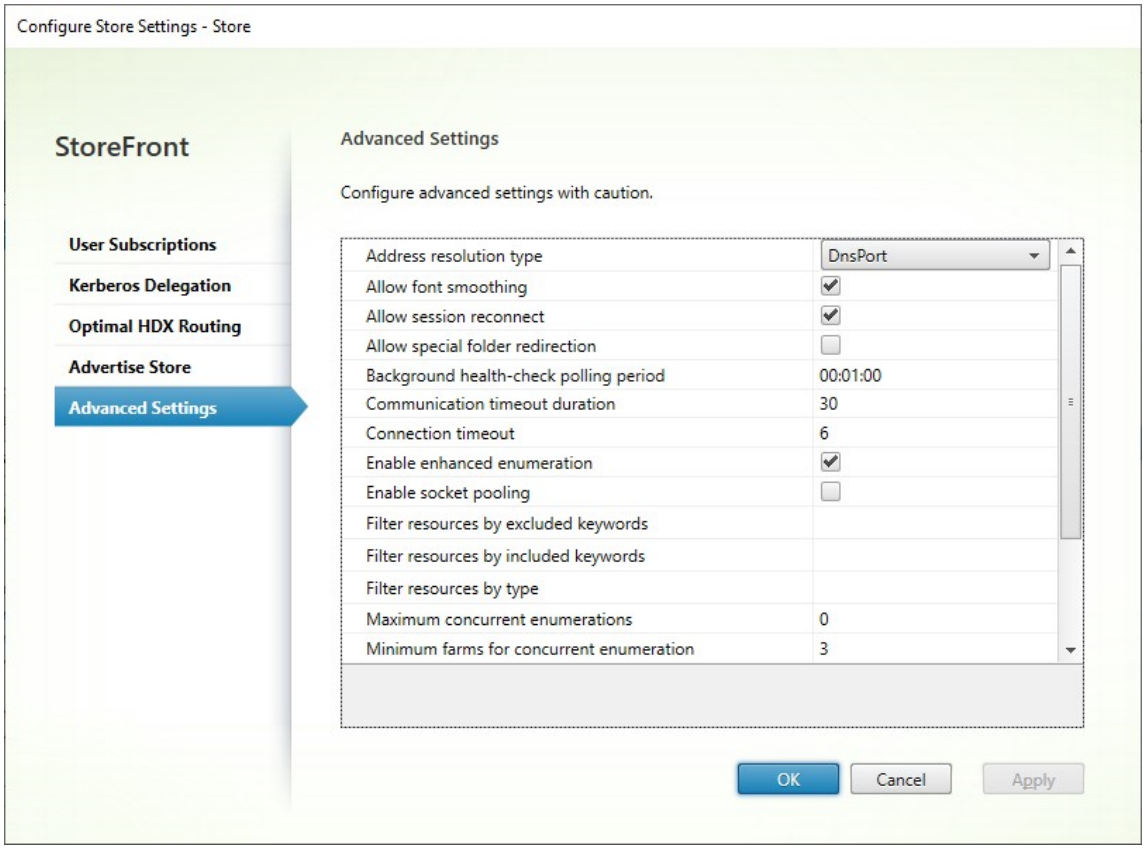
Paramètres de magasin avancés

April 17, 2024

Vous pouvez configurer la plupart des propriétés avancées pour un magasin en utilisant les paramètres avancés dans la page Configurer les paramètres du magasin. Certains paramètres ne peuvent être modifiés qu'à l'aide de PowerShell.

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

1. 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**.
2. Sur la page **Configurer les paramètres du magasin**, sélectionnez **Paramètres avancés** et apportez les modifications requises.



3. Cliquez sur **OK** pour enregistrer vos modifications.

Type de résolution d'adresses

Vous pouvez spécifier le type d'adresse à demander au serveur. La valeur par défaut est DnsPort.

Dans la fenêtre **Paramètres avancés**, choisissez une valeur dans la liste déroulante **Type de résolution d'adresse**.

- 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.

Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **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.

Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **Autoriser la reconnexion de sessions**.

Autoriser 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.

Dans la fenêtre **Paramètres avancés**, sélectionnez ou désélectionnez **Autoriser la redirection de dossiers spéciaux** pour activer ou désactiver la redirection de dossiers spéciaux, puis cliquez sur **OK**.

Contrôle avancé de l'état

StoreFront exécute des vérifications de l'intégrité périodiques sur chaque Delivery Controller Citrix Virtual Apps and Desktops, chaque Cloud Connector et chaque serveur Secure Private Access pour réduire l'impact d'une disponibilité intermittente des serveurs. Grâce à la vérification avancée de l'intégrité, StoreFront effectue un contrôle plus approfondi qui est plus susceptible de détecter d'éventuels problèmes.

Lors de la connexion à Citrix Desktops as a Service via un Cloud Connector, le contrôle d'intégrité avancé présente également l'avantage de récupérer des informations supplémentaires sur les VDA qui se trouvent au même endroit que le Cloud Connector. Si les Cloud Connector ne parviennent pas à contacter Citrix Desktops as a Service, ils utiliseront leur cache d'hôte local pour faciliter les connexions aux VDA colocalisés. StoreFront utilise les informations supplémentaires issues des résultats du contrôle d'intégrité avancé pour contacter le connecteur en ligne le plus approprié afin de lancer des applications et des bureaux.

Pour garantir la disponibilité des ressources pendant une panne, sans avoir à publier les ressources dans chaque zone (emplacement des ressources), assurez-vous de configurer le flux de ressources sur tous les serveurs StoreFront de manière à inclure tous les Cloud Connector dans tous les emplacements de ressources et d'activer la fonction de contrôle d'intégrité avancé.

À partir de StoreFront 2308, la vérification avancée de l'intégrité est activée par défaut pour les nouveaux magasins. Citrix vous recommande de laisser cette fonction activée pour tous les déploiements de StoreFront. Pour activer ou désactiver le contrôle d'intégrité avancé, utilisez la commande PowerShell Set-STFStoreFarmConfiguration avec le paramètre `AdvancedHealthCheck`.

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

StoreFront exécute des vérifications de l'intégrité périodiques sur chaque Delivery Controller Citrix Virtual Apps and Desktops, chaque Cloud Connector et chaque serveur Secure Private Access pour réduire l'impact d'une disponibilité intermittente des serveurs. La valeur par défaut est toutes les minutes (00:01:00). Dans la fenêtre **Paramètres avancés**, spécifiez une durée sous **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. Il n'est pas recommandé de définir la période de sondage sur une valeur faible lorsque la vérification avancée de l'intégrité est activée, car cela peut avoir un impact sur les performances.

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. Dans la fenêtre **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.

Dans la fenêtre **Paramètres avancés**, spécifiez les secondes à attendre pour établir la connexion initiale, puis cliquez sur **OK**.

Activer l'énumération améliorée

Cette option détermine si StoreFront interroge les Delivery Controller simultanément ou séquentiellement lors de l'énumération d'applications et de bureaux sur plusieurs sites Citrix Virtual Apps and

Desktops. L'énumération simultanée fournit des réponses plus rapides aux requêtes des utilisateurs lors de l'agrégation de ressources sur plusieurs sites. Lorsque cette option est sélectionnée (valeur par défaut), StoreFront envoie les demandes d'énumération à tous les Delivery Controller en même temps et agrège les réponses lorsqu'ils ont tous répondu. Vous pouvez utiliser les options **Nombre maximal d'énumérations simultanées** et **Nombre minimal de batteries pour les énumérations simultanées** pour régler ce comportement.

Dans la fenêtre **Paramètres avancés**, sélectionnez (ou désélectionnez) l'option **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. Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **Activer le regroupement de sockets**, puis cliquez sur **OK** pour activer le regroupement de sockets.

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, utilisez la commande PowerShell Set-STFStoreFarmConfiguration. Par exemple :

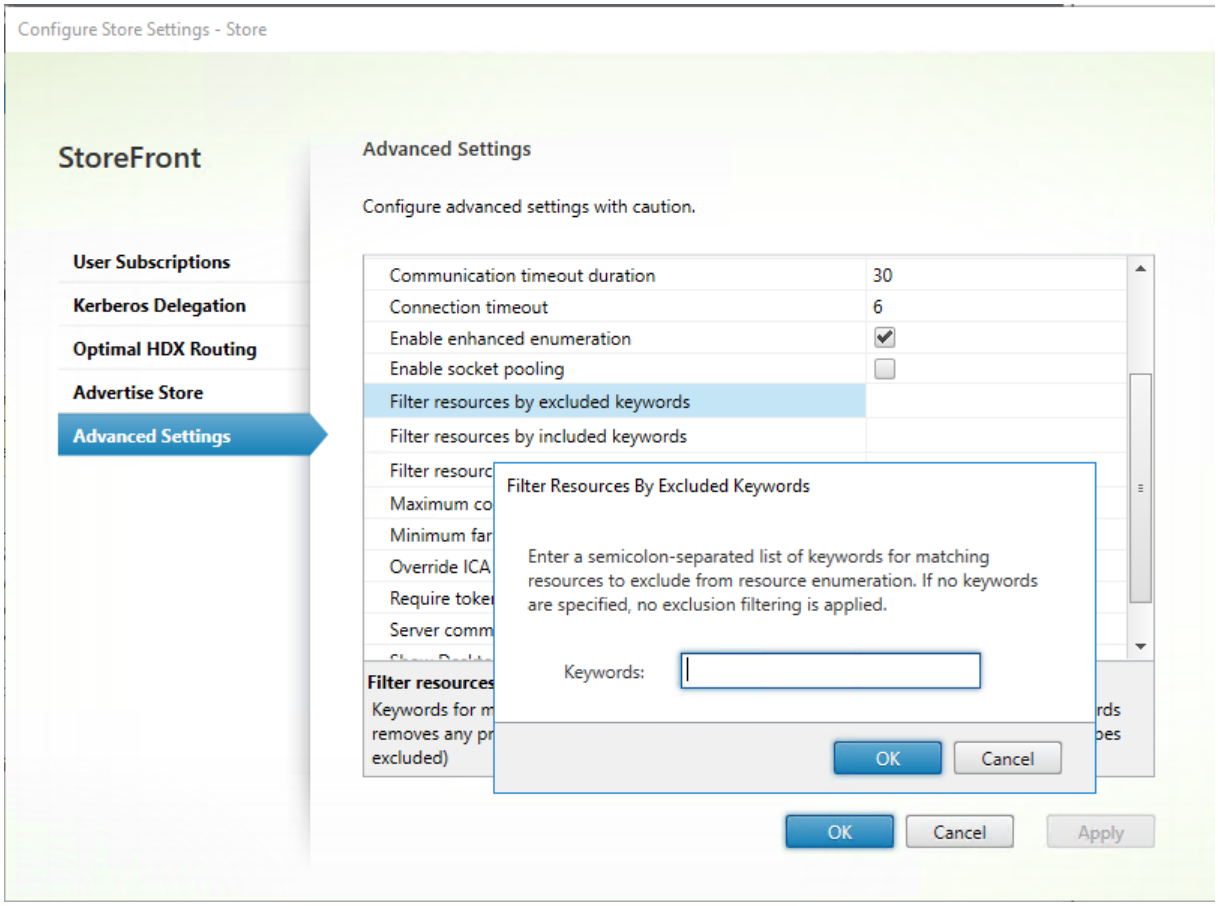
```
1 $storeService = Get-STFStoreService –VirtualPath '/Citrix/Store'
2 Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
     $false
3 <!--NeedCopy-->
```

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).

1. Dans la fenêtre **Paramètres avancés**, recherchez la ligne **Filtrer les ressources par mots clés exclus**.

2. Cliquez dans la colonne de droite pour faire apparaître la fenêtre **Filtrer les ressources par mots clés exclus**.
3. Entrer une liste de mots clés séparés par des points-virgules dans la zone de saisie des mots clés
4. Cliquez sur **OK**.



Pour modifier le paramètre à l'aide de PowerShell, utilisez l'applet de commande Set-STFStoreEnumerationOption avec le paramètre `-FilterByKeywordsExclude`.

Les mots-clés suivants sont réservés et ne doivent pas être utilisés pour le filtrage :

- Auto
- Mandatory

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).

1. Dans la fenêtre **Paramètres avancés**, recherchez la ligne **Filtrer les ressources par mots clés inclus**.

2. Cliquez dans la colonne de droite pour faire apparaître la fenêtre **Filtrer les ressources par mots clés inclus**.
3. Entrer une liste de mots clés séparés par des points-virgules dans la zone de saisie des mots clés
4. Cliquez sur **OK**.

Pour modifier le paramètre à l'aide de PowerShell, utilisez l'applet de commande Set-STFStoreEnumerationOption avec le paramètre `-FilterByKeywordsInclude`.

Les mots-clés suivants sont réservés et ne doivent pas être utilisés pour le filtrage :

- Auto
- Mandatory

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).

Dans la fenêtre **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**.

Pour modifier le paramètre à l'aide de PowerShell, utilisez l'applet de commande Set-STFStoreEnumerationOption avec le paramètre `-FilterByTypesInclude`, en spécifiant un tableau de types de ressources (applications, bureaux ou documents).

Nombre maximal d'énumérations simultanées

Spécifiez le nombre maximal de demandes simultanées à envoyer à tous les Delivery Controller. Cette option prend effet lorsque l'option **Activer l'énumération améliorée** est activée. La valeur par défaut est 0 (pas limite).

Dans la fenêtre **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 minimal de Delivery Controller requis pour déclencher l'énumération simultanée. Cette option prend effet lorsque l'option **Activer l'énumération améliorée** est activée. La valeur par défaut est 3.

Dans la fenêtre **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 par un identifiant unique généré par le navigateur Web. Lorsque cette option est désactivée, l'application Citrix Workspace spécifie le nom du client. La valeur par défaut est Désactivé.

Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **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. Vous devez désactiver cette option si les utilisateurs accèdent au magasin via une passerelle pour laquelle l'authentification est désactivée. La valeur par défaut est Activé.

Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **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.

Dans la fenêtre **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.

Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **Afficher Desktop Viewer pour les clients d'ancienne génération** et cliquez sur **OK**.

Traiter les bureaux comme des applications

Spécifiez si, lors de l'accès au magasin, les bureaux sont affichés dans la vue Applications plutôt que dans la vue Bureaux. La valeur par défaut est Désactivé.

Dans la fenêtre **Paramètres avancés**, sélectionnez l'option **Traiter les bureaux comme des applications**, puis cliquez sur **OK**.

Configurer un routage HDX optimal pour un magasin

February 22, 2024

Configurez un routage Citrix Gateway optimal afin d'optimiser le traitement du routage de la connexion ICA depuis le moteur HDX vers 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.

Vous pouvez mapper les passerelles à des Delivery Controller spécifiques ou à des zones. Une zone est un regroupement de Delivery Controller et représente généralement un centre de données situé dans un emplacement géographique. Les zones sont définies dans Citrix Virtual Apps and Desktops et toutes les zones définies dans StoreFront doivent correspondre exactement aux noms de zone définis 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.

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

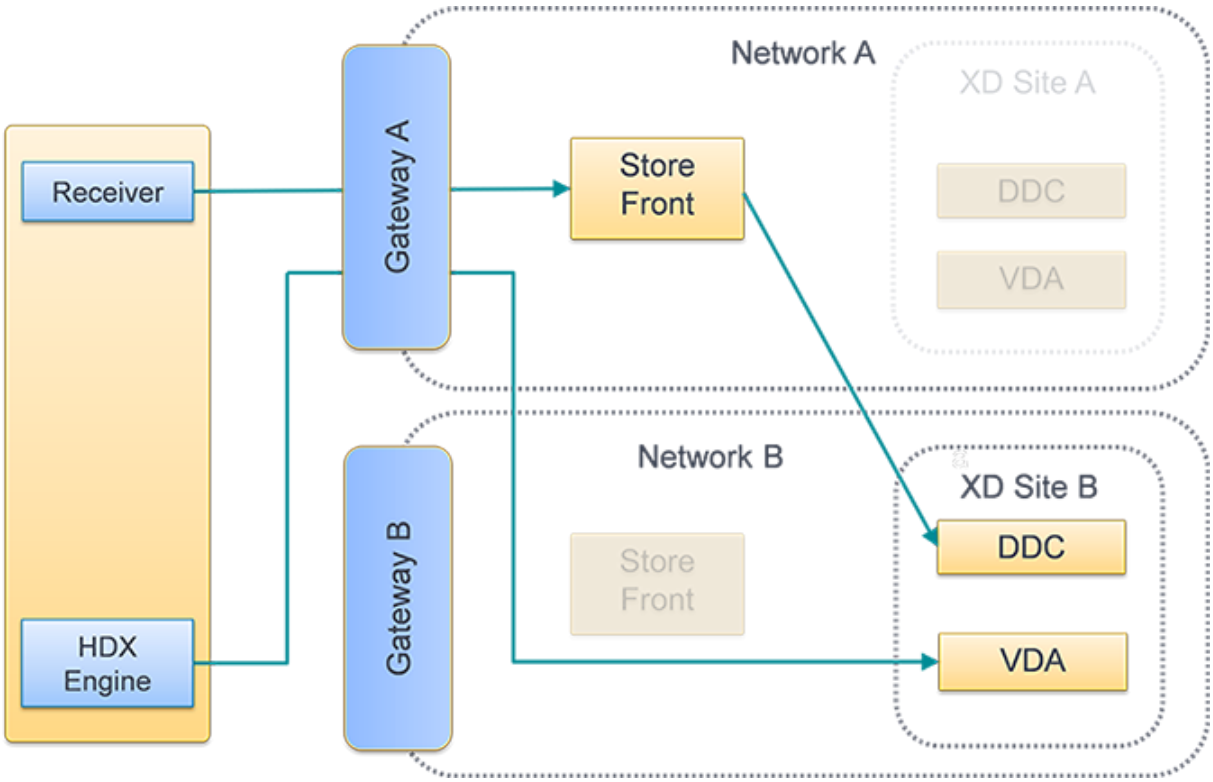
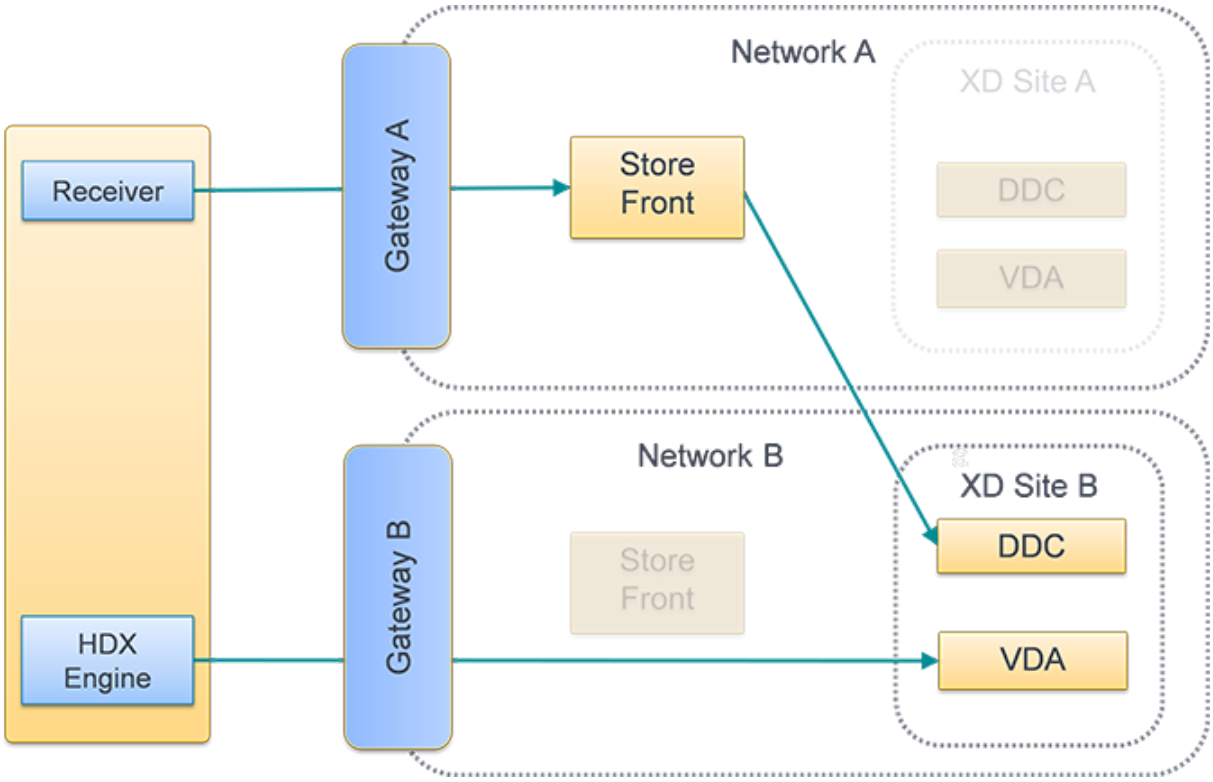


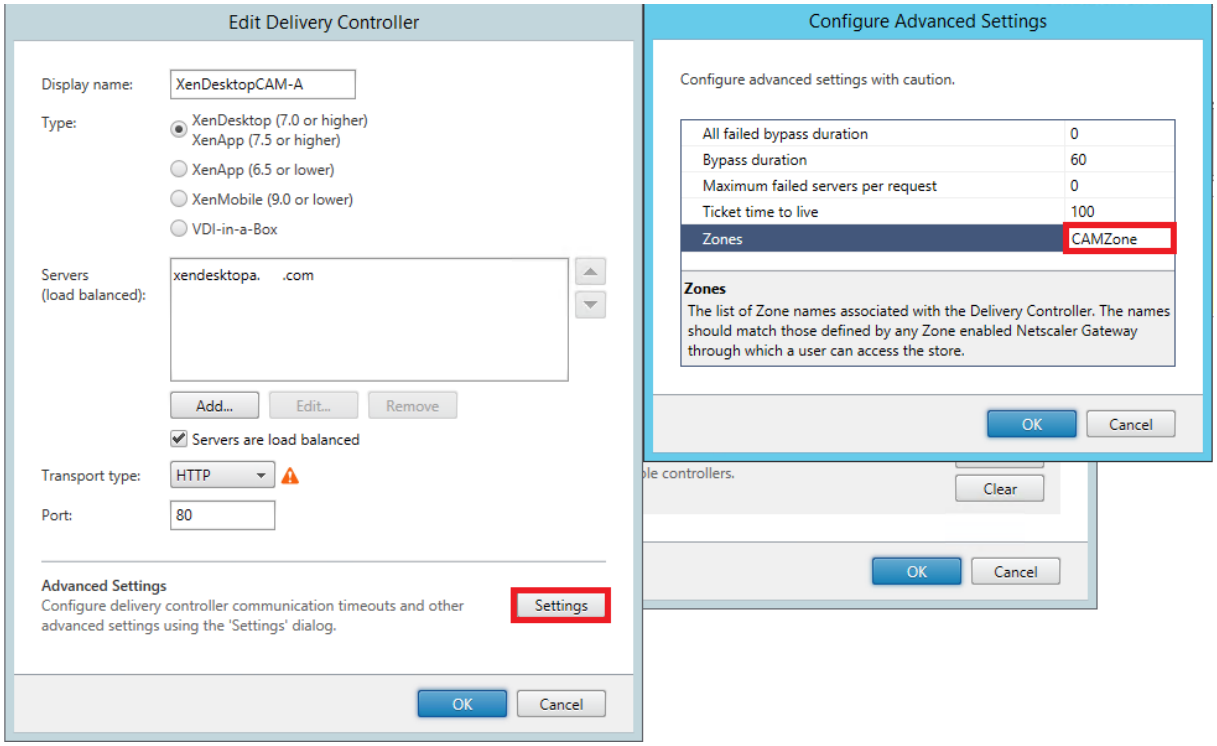
Figure 2. Routage vers la passerelle optimal



Placer un Delivery Controller dans une zone

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

1. 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**.
2. Sélectionnez un Controller, cliquez sur **Modifier**, puis sur **Paramètres** dans l'écran **Modifier Delivery Controller**.
3. Sur la ligne **Zones**, cliquez dans la deuxième colonne.
4. Cliquez sur **Ajouter** dans l'écran **Noms de zone de Delivery Controller** et ajoutez un nom de zone.



Configurer le routage HDX optimal

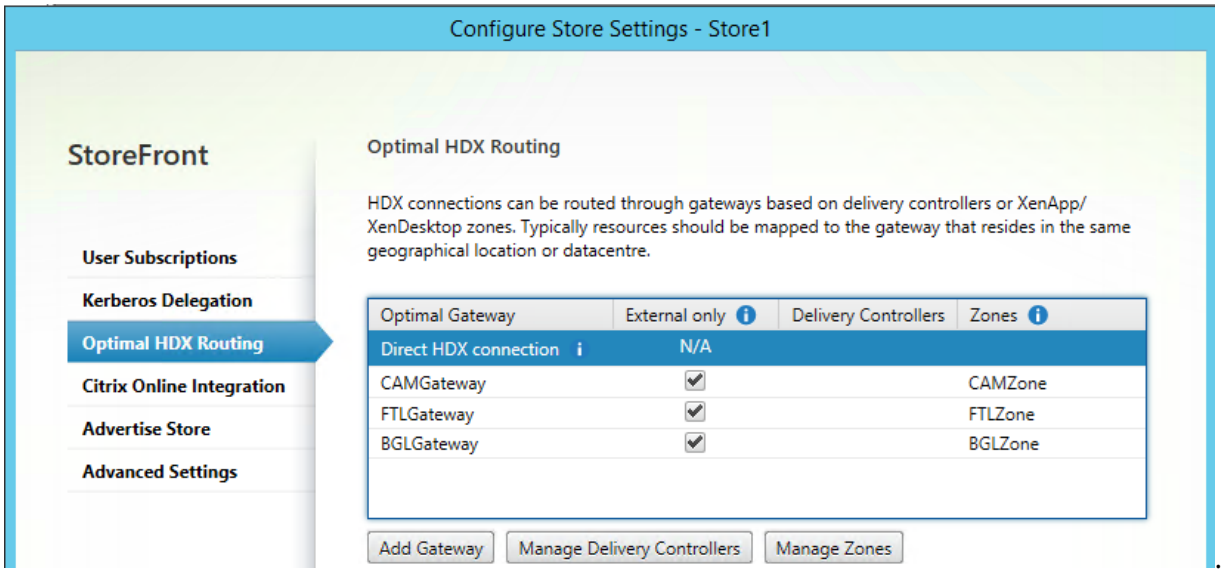
1. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau **Actions**, cliquez sur **Configurer les paramètres du magasin**.
2. Sélectionnez l'onglet **Routage HDX optimal**.
3. Sélectionnez une passerelle.

    a) Pour utiliser la passerelle lors de l'accès aux ressources de Delivery Controller spécifiques, cliquez sur **Gérer les Delivery Controller** et cochez un ou plusieurs Delivery Controller.

b) Pour utiliser la passerelle lors de l'accès aux ressources d'un groupe de Delivery Controller dans une zone, cliquez sur **Gérer les zones** et entrez une ou plusieurs zones.

c) Par défaut, lorsque vous ajoutez un Delivery Controller ou une zone, la case **Externes uniquement** est cochée, ce qui signifie que StoreFront utilise la passerelle uniquement pour lancer StoreFront pour les utilisateurs connectés à StoreFront via une passerelle. Si vous souhaitez également utiliser la passerelle pour lancer des ressources pour les utilisateurs qui se sont connectés directement à StoreFront sans passer par une passerelle, décochez **Externes uniquement**.

4. Si vous souhaitez toujours vous connecter directement à certaines ressources sans utiliser de passerelle, même pour les utilisateurs accédant à distance à StoreFront via une passerelle, sélectionnez **Connexion HDX directe** et choisissez des Delivery Controller ou des zones.



Utiliser PowerShell pour configurer un routage Citrix Gateway optimal pour un magasin

- Pour configurer un routage de passerelle optimal pour un magasin, utilisez Register-STFStoreOptimalLaunchGateway.
- Pour supprimer le routage de passerelle optimal pour un magasin, utilisez Unregister-STFStoreOptimalLaunchGateway.
- Pour afficher le routage optimal pour un magasin, utilisez Get-STFStoreRegisteredOptimalLaunchGateway.

Synchronisation de l'abonnement

February 22, 2024

StoreFront synchronise automatiquement les abonnements entre les serveurs d'un groupe de serveurs StoreFront. Si vous avez plusieurs groupes de serveurs (généralement situés dans des zones géographiques différentes), vous pouvez configurer la synchronisation périodique des abonnements des utilisateurs depuis les magasins de différents déploiements StoreFront. Cela doit être fait à l'aide de 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 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, *CVAD_US* ne correspond pas à *Cvad_Us*.

1. Utilisez un compte disposant des autorisations d'administrateur local pour démarrer Windows PowerShell ISE.
2. Pour configurer la synchronisation, utilisez la commande Publish-STFServerGroupConfiguration. Vous pouvez spécifier une heure de début et un intervalle récurrent ou une liste d'heures. Par exemple, pour démarrer la synchronisation à 08h00, puis toutes les 30 minutes :

   ```
   Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime
       08:00:00 -RecurringInterval 30
   <!--NeedCopy-->
   ```

   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"
     <!--NeedCopy-->
     ```

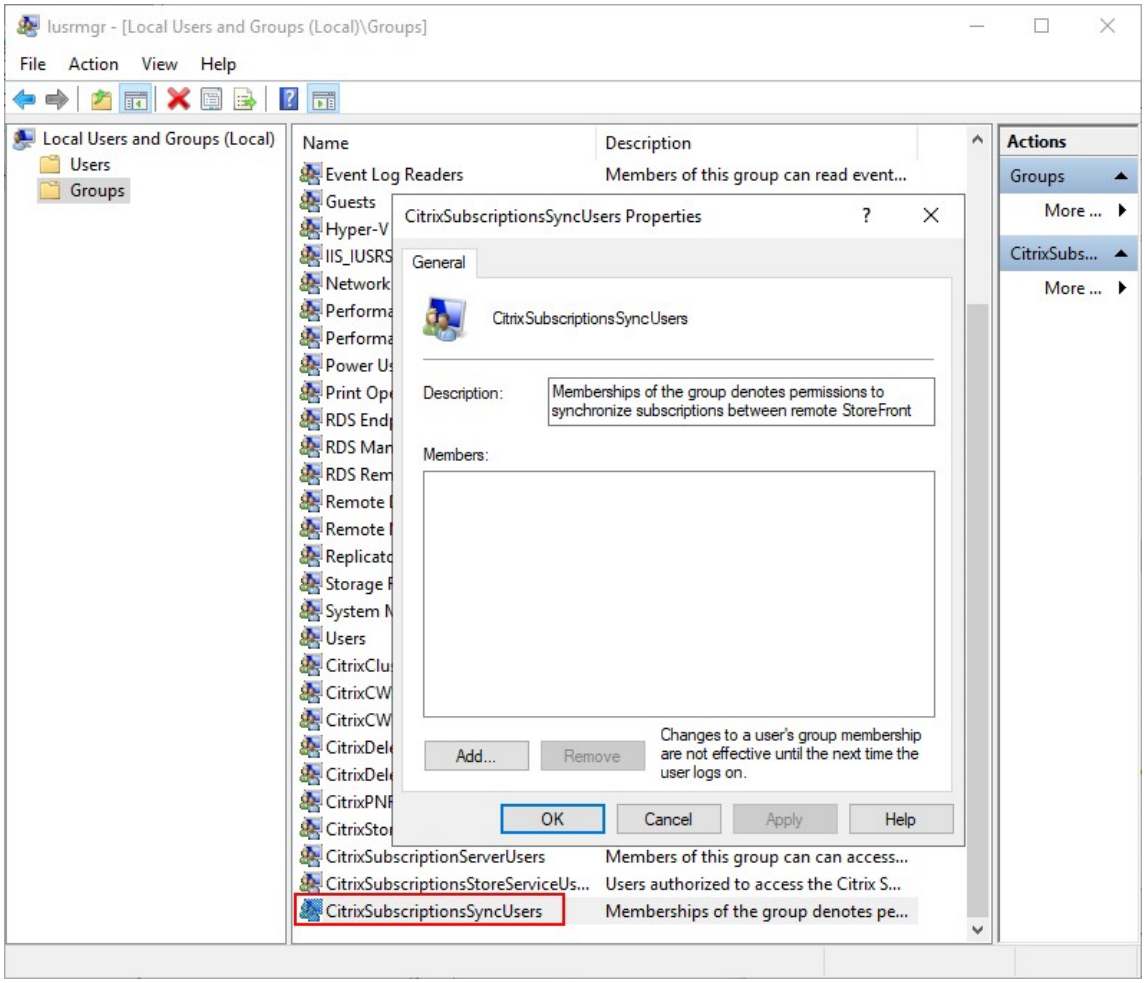
   - Exécutez cette commande sur les serveurs StoreFront du data center au Royaume-Uni pour extraire les données des serveurs du data center aux États-Unis :

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

   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 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11).



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.

```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

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.

```
Clear-STFSubscriptionSynchronizationSchedule
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

7. Pour supprimer une source de synchronisation d'abonnement spécifique, exécutez la com-

mande suivante ; propagez ensuite les modifications apportées à la configuration aux autres serveurs StoreFront dans le déploiement.

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

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
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

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

```
Get-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

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

```
Get-STFSubscriptionSynchronizationSource
<!--NeedCopy-->
```

Configurer les paramètres de session

February 22, 2024

Lorsqu'un utilisateur lance une application, StoreFront génère un document (appelé fichier .ica) qui contient tous les paramètres dont l'application Citrix Workspace a besoin pour lancer et configurer cette session.

Dans la plupart des cas, il est recommandé de modifier les paramètres de session à l'aide des stratégies Citrix Virtual Apps and Desktops ou des stratégies Citrix DaaS. Cependant, dans certains cas, il est utile de modifier ces paramètres pour un magasin en particulier. Cela peut être utile si un magasin regroupe des ressources provenant de plusieurs sites et que vous souhaitez appliquer les mêmes paramètres à toutes les ressources de ce magasin.

Pour définir les paramètres de session d'un magasin, vous pouvez soit :

- Utiliser le Global App Config Service. Il s'agit d'un service sur Citrix Cloud. Pour plus d'informations, consultez Configurer l'application Citrix Workspace à l'aide de Global App Configuration Service.
- Sur le serveur StoreFront, ajoutez des paramètres au fichier default.ica du magasin.

Vous pouvez trouver default.ica sur le serveur StoreFront dans le répertoire `\inetpub\wwwroot\Citrix\[StoreName]\App_Data`.

Pour obtenir la liste des paramètres disponibles, consultez la référence des paramètres ICA. Certains paramètres s'appliquent à l'échelle mondiale. Vous pouvez également ajouter des sections qui s'appliquent à des applications spécifiques en ajoutant une section dont le nom correspond exactement au nom de l'application tel que configuré dans Studio.

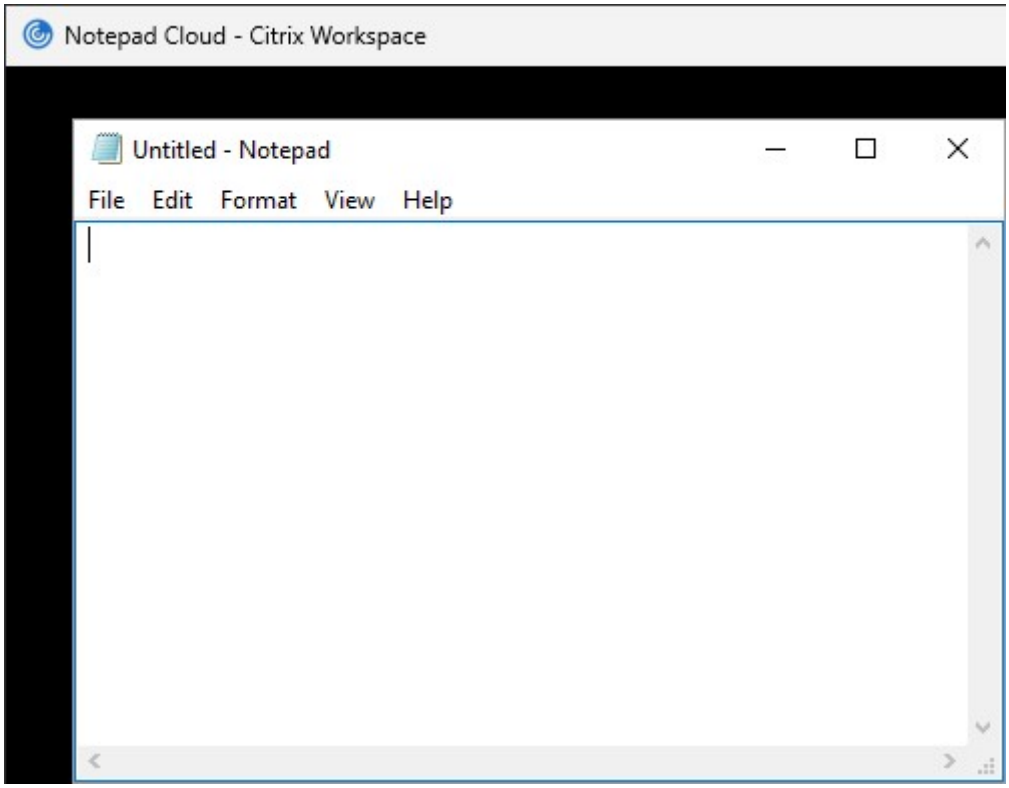
Exemple : Lancer le Bloc-notes en mode fenêtré

Pour configurer le lancement d'une application en mode fenêtré, dans default.ica, ajoutez une section pour l'application avec les paramètres suivants :

- TWIMode : défini sur Désactivé pour activer le mode fenêtré.
- DesiredHRES : éventuellement le nombre horizontal de pixels.
- DesiredVRES : éventuellement le nombre vertical de pixels.

Par exemple :

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
<!--NeedCopy-->
```

Signature de fichier ICA

April 17, 2024

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 l'application Citrix Workspace, dont la configuration détermine si le fichier non signé sera accepté ou non.

Pour pouvoir être utilisés pour la signature de fichier ICA avec StoreFront, les certificats doivent inclure la clé privée et se situer dans la période de validité autorisée. Si le certificat contient une extension d'utilisation de la clé, celle-ci doit permettre l'utilisation de la clé pour les signatures numériques. Si une extension d'utilisation de la clé prolongée est incluse, elle doit être définie sur la signature de code ou l'authentification de serveur.

Pour la signature de fichier ICA, Citrix vous recommande d'utiliser un certificat de signature de code ou SSL que vous pouvez vous procurer auprès d'une autorité de certification publique ou de l'autorité de certification publique de votre organisation. Si vous ne parvenez pas à obtenir un certificat approprié auprès d'une autorité de certification, vous pouvez utiliser un certificat SSL existant, par exemple un certificat de serveur ou créer un nouveau certificat racine d'autorité de certification et le distribuer sur les périphériques des utilisateurs.

La signature de fichier ICA est désactivée par défaut dans les magasins. Pour activer la signature de fichier ICA, modifiez le fichier de configuration du magasin et exécutez les commandes Windows PowerShell. Pour plus d'informations sur l'activation de la signature de fichier ICA dans l'application Citrix Workspace pour Windows, consultez la section Signature de fichier ICA.

> 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. Activez la signature à l'aide de l'applet de commande PowerShell `Set-STFStoreService` :

```
$storeService = Get-STFStoreService
Set-STFStoreService $storeService -IcaFileSigning $true -
    IcaFileSigningCertificateThumbprint [certificatethumbprint]
<!--NeedCopy-->
```

   Où **[certificatethumbprint]** est le condensé (ou empreinte numérique) des données de certificat produites par l'algorithme de hachage.

   Si vous souhaitez utiliser un algorithme de hachage autre que SHA-1, ajoutez un paramètre **-IcaFileSigningHashAlgorithm** défini sur sha256, sha384 ou sha512, selon les besoins.

Configuration de l'application Citrix Workspace

February 22, 2024

Global App Config Service

Le service Global App Config est un service cloud permettant de gérer la configuration de l'application Citrix Workspace. Dans votre compte Citrix Cloud, vous pouvez revendiquer les URL de vos magasins et définir la configuration de chacun d'entre eux. Pour plus d'informations, consultez Configurer les paramètres des magasins locaux.

Paramètres de compte de magasin

Comme alternative à Global App Config Service, vous pouvez configurer l'application Citrix Workspace via les paramètres de compte de magasin. Lorsqu'un utilisateur ajoute un magasin à une application Citrix Workspace installée localement, il récupère les paramètres de compte de magasin StoreFront. qui peuvent inclure des propriétés de configuration, par exemple, pour indiquer à l'application Citrix Workspace pour Windows si elle doit créer des raccourcis du menu Démarrer pour les applications. Consultez la documentation de l'application Workspace pour plus de détails sur les propriétés, par exemple Utilisation des paramètres de compte StoreFront pour personnaliser l'emplacement des raccourcis d'applications.

Pour modifier ces paramètres :

1. Ouvrez le fichier web.config dans `C:\inetpub\wwwroot\Citrix\Roaming`.
2. Dans la section <Accounts>, localisez l'élément <account ... name="Store"... > du magasin que vous souhaitez modifier.
3. Dans la section Account, localisez la section <annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>.
4. Après l'élément <clear/>, ajoutez les propriétés sous la forme <property name="[name]"value="[value]"/>. Par exemple :

```
<properties>
    <clear/>
    <property name="PutShortcutsOnDesktop" value="true"/>
    <property name="DesktopDir" value="Citrix Applications"/>
</properties>
<!--NeedCopy-->
```

> **Important**
>
> Dans les déploiements faisant appel à de multiples serveurs, n'utilisez qu'un serveur à la fois pour changer la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois les mod-

> ifications terminées, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

Site Web de l'application Workspace

Pour configurer la configuration de site Web utilisée par l'application Citrix Workspace installée localement, consultez Configurer le site Web de l'application Workspace.

Gérer un site Web

August 25, 2023

Pour chaque magasin, vous pouvez configurer un ou plusieurs sites Web auxquels les utilisateurs peuvent accéder via un navigateur ou via l'application Citrix Workspace.

Utilisez la console de gestion StoreFront pour effectuer les tâches suivantes :

Tâche	Détails
Créer un site Web	Pour créer des sites Web qui permettent aux utilisateurs d'accéder aux magasins via une page Web ou l'application Workspace.
Configurer le site Web	Pour modifier les paramètres de votre site Web.
Supprimer un site Web	Pour supprimer un site Citrix Receiver pour Web.
Configurer le site Web de l'application Workspace	Choisissez le site Web à utiliser dans l'application Citrix Workspace.

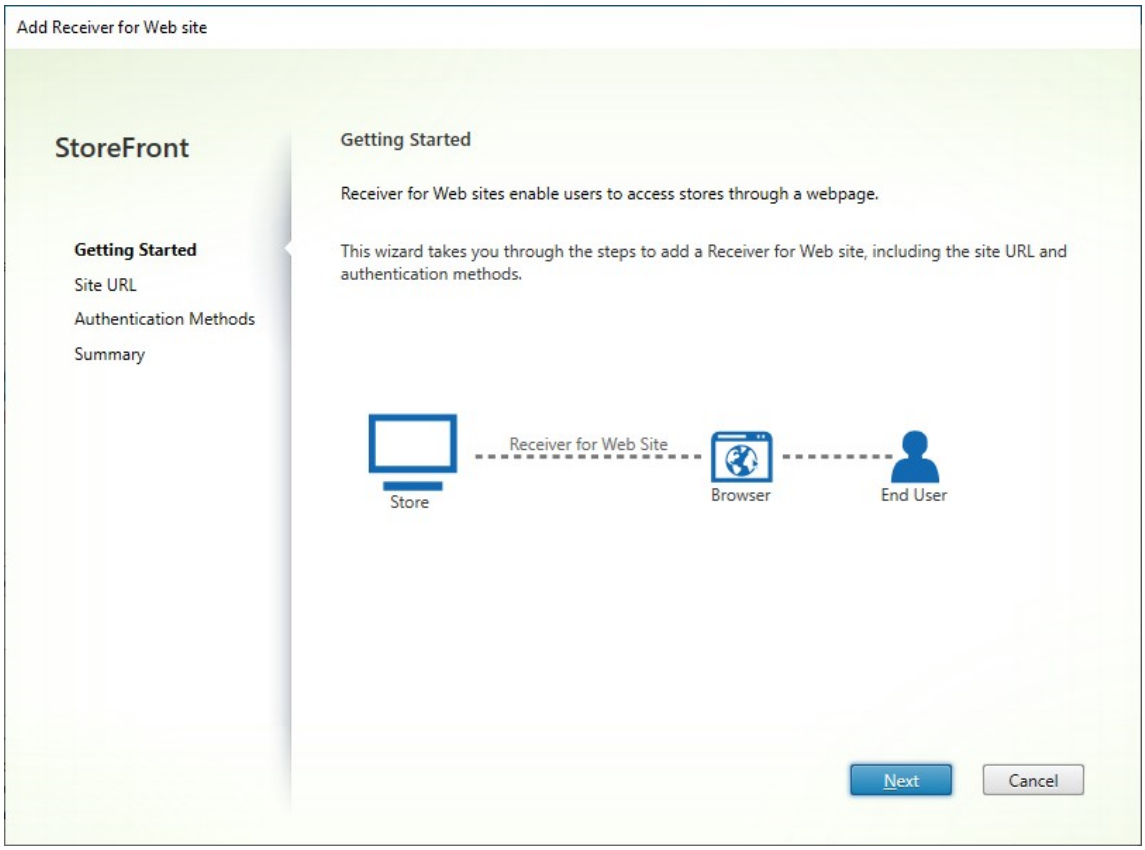
Créer un site Web

December 6, 2023

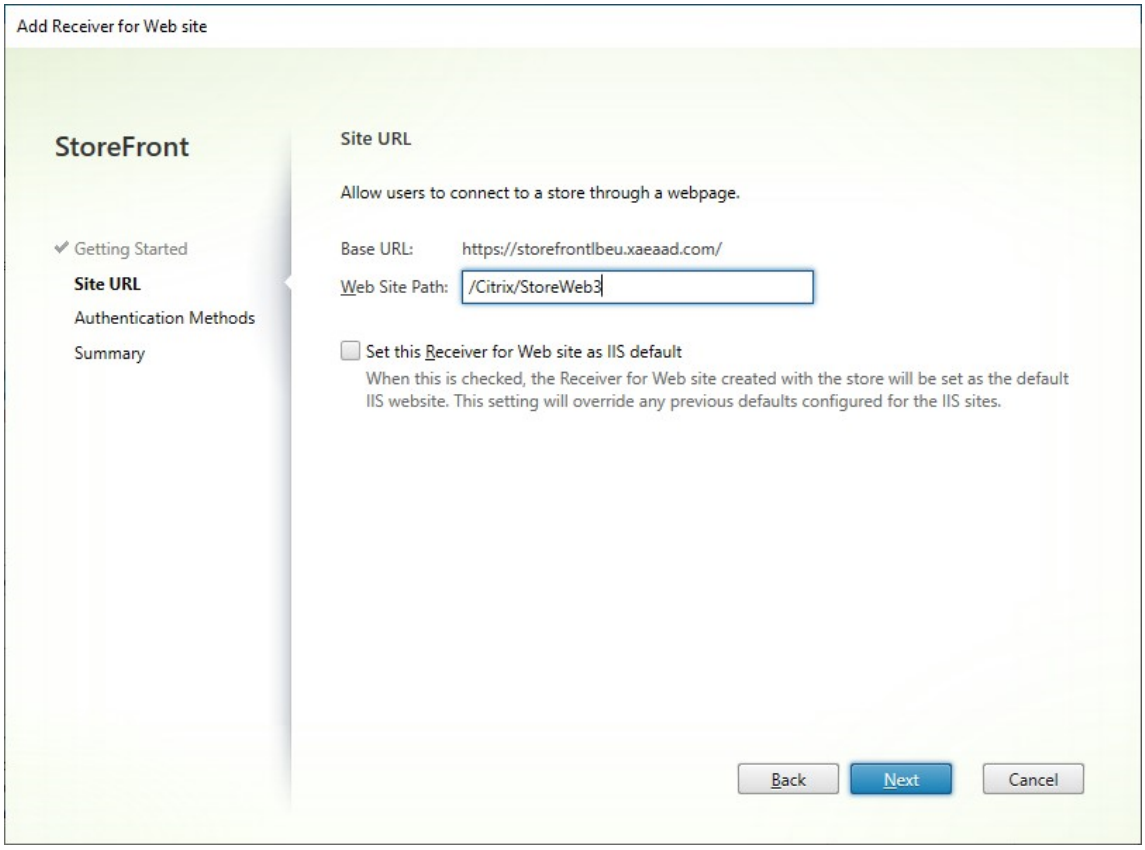
Lorsque vous créez un magasin, un site Web est automatiquement créé pour ce magasin. Vous pouvez ajouter des sites Web supplémentaires aux magasins existants. Cela vous permet de fournir différentes URL avec différentes configurations à vos utilisateurs. Toutefois, plusieurs sites Web ne sont accessibles que via un navigateur Web, car les applications Citrix Workspace sont configurées pour utiliser un seul site Web spécifique pour un magasin. Reportez-vous à la section Configurer le site Web de l'application Workspace.

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

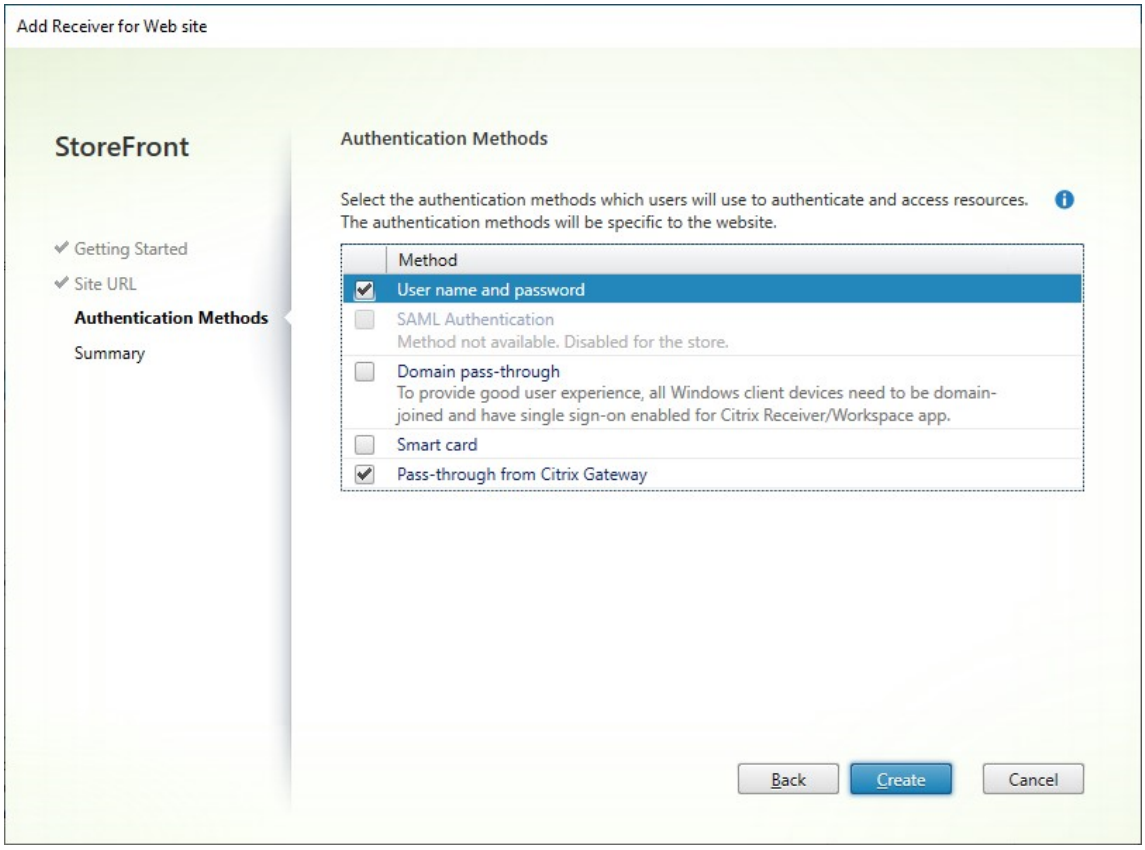
1. Dans la console de gestion, sélectionnez le magasin pour lequel vous souhaitez créer le site Web et, dans le volet Actions, cliquez sur **Gérer les sites Receiver pour Web**.
2. Cliquez sur **Ajouter**, puis sur **Suivant**.



3. Entrez le **chemin du site Web** souhaité, choisissez si vous souhaitez qu'il s'agisse du site Web par défaut pour l'URL de base et cliquez sur **Suivant**.



4. Cochez ou décochez les méthodes d'authentification souhaitées. Certaines méthodes ne sont disponibles que si elles ont été configurées pour le magasin. Appuyez sur **Suivant**.



5. Une fois que le site a été créé, cliquez sur **Terminer**.
6. Sélectionnez le site que vous venez de créer et appuyez sur **Modifier** pour configurer votre site Web selon vos besoins. Reportez-vous à la section Configurer des sites Web.

Créer un site Web à l'aide du SDK PowerShell

Pour créer un site Web à l'aide du SDK PowerShell, appelez l'applet de commande Add-STFWebReceiverService.

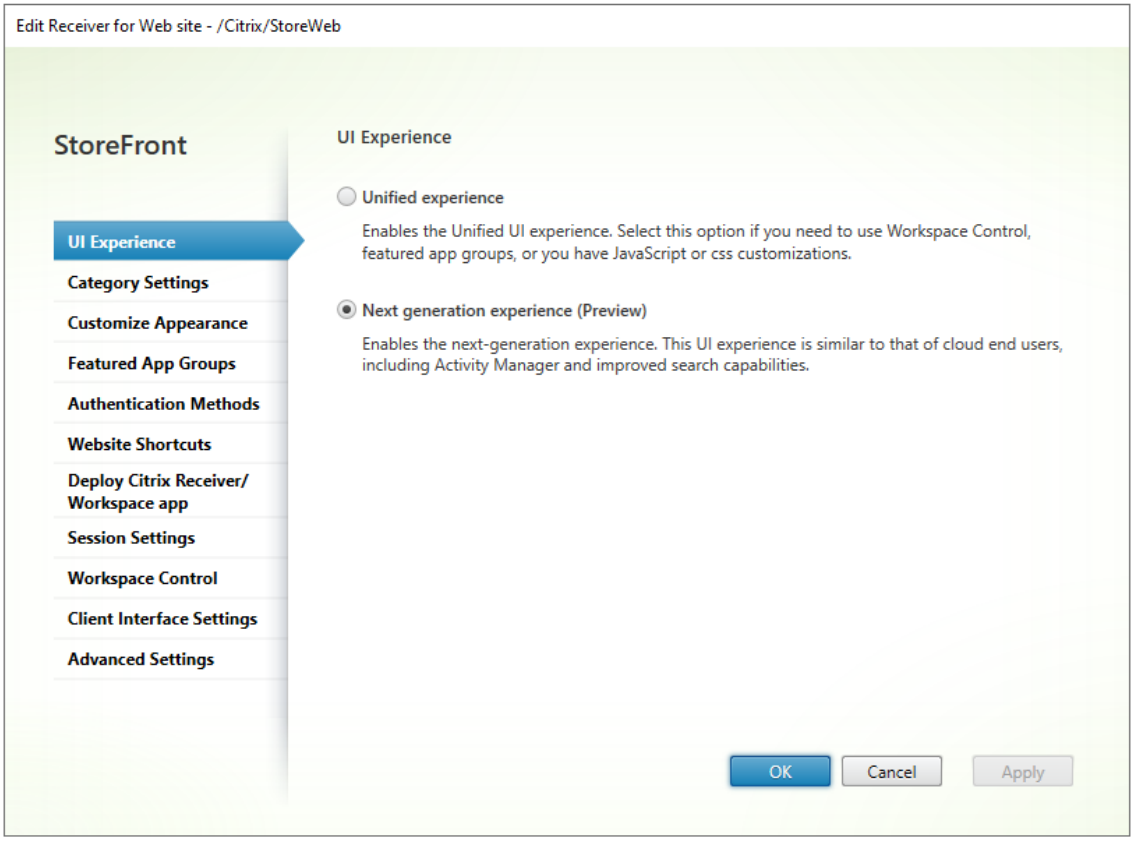
Configurer le site Web

January 25, 2024

Pour configurer un site Web, procédez comme suit :

1. Sélectionnez le nœud **Magasins** dans le panneau de gauche, et dans le panneau **Actions**, cliquez sur **Gérer les sites Receiver pour Web**.

2. Sélectionnez un site Web et appuyez sur **Configurer...**



3. Modifiez les paramètres dans les onglets appropriés.

   - Expérience d'interface utilisateur
   - Paramètres de catégorie
   - Personnaliser l'apparence
   - Groupes d'applications recommandées
   - Méthodes d'authentification
   - Raccourcis de site Web
   - Déployer l'application Workspace/Citrix Receiver
   - Paramètres de session
   - Contrôle de l'espace de travail
   - Paramètres de l'interface client
   - Paramètres avancés

4. Lorsque vous avez terminé vos modifications, cliquez sur **OK**.

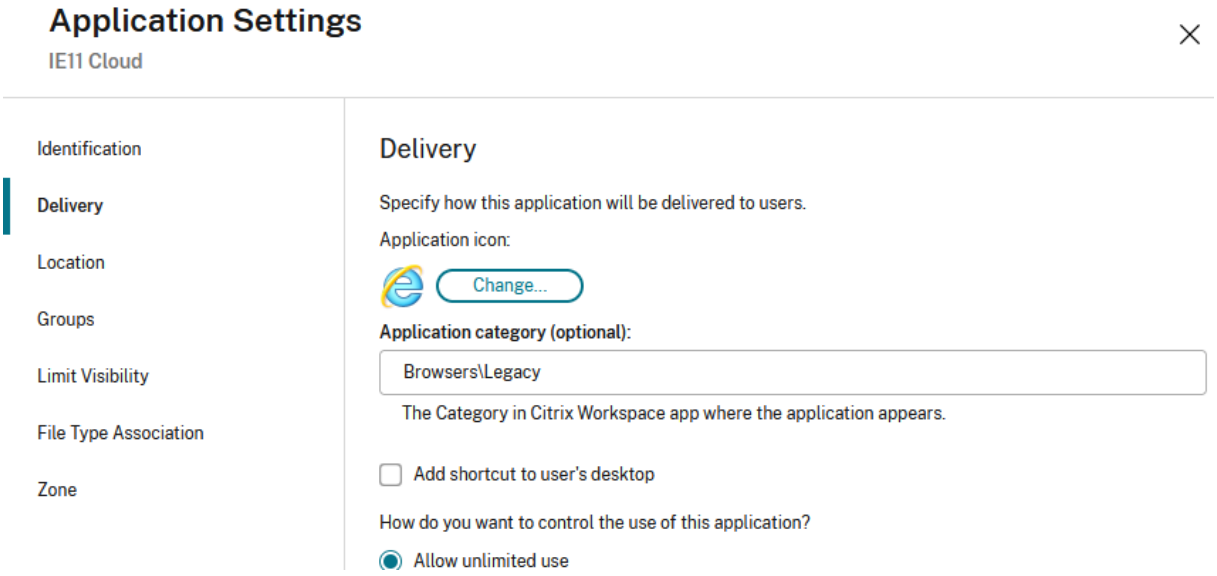
5. Pour configurer App Protection, vous devez utiliser PowerShell. Assurez-vous de fermer la console de gestion StoreFront avant d'exécuter des commandes PowerShell.

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

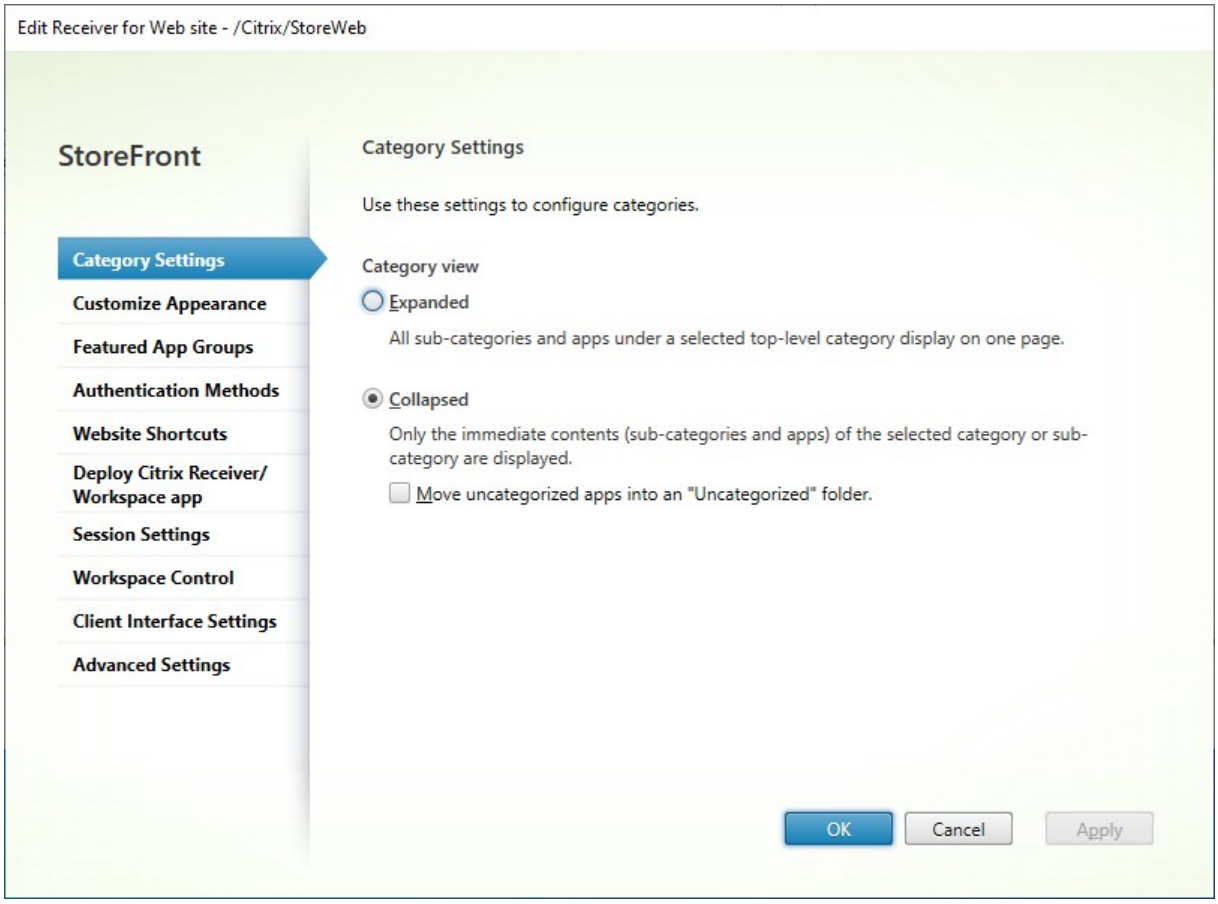
Paramètres de catégorie

December 6, 2023

Dans Citrix Virtual Apps and Desktops, vous pouvez attribuer chaque application à une catégorie, comme décrit dans l'article Applications. Utilisez le symbole \ pour créer une hiérarchie de dossiers des catégories. Dans StoreFront, vous pouvez configurer la façon dont cette hiérarchie de dossiers est affichée.



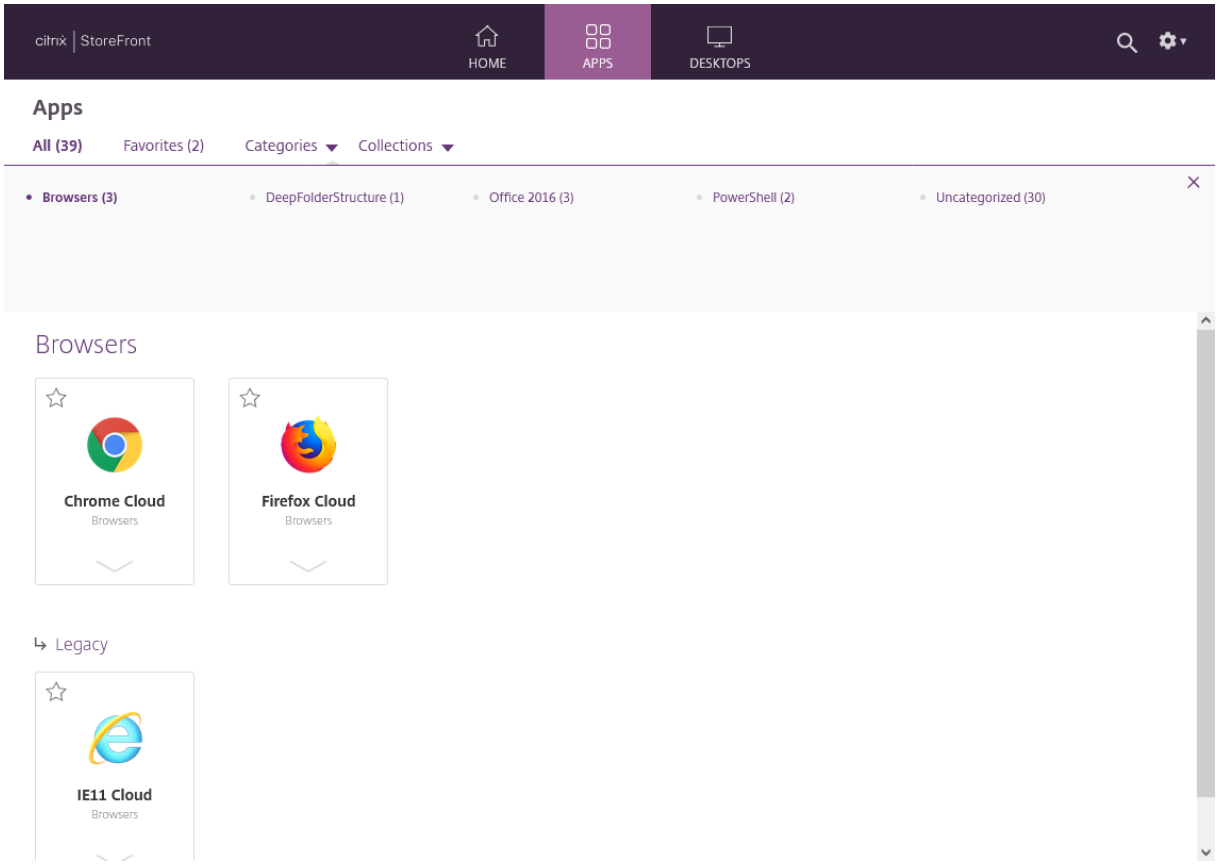
Pour modifier les paramètres de catégorie, accédez à Modifier le site Receiver pour Web et sélectionnez l'onglet **Paramètres de catégorie**.



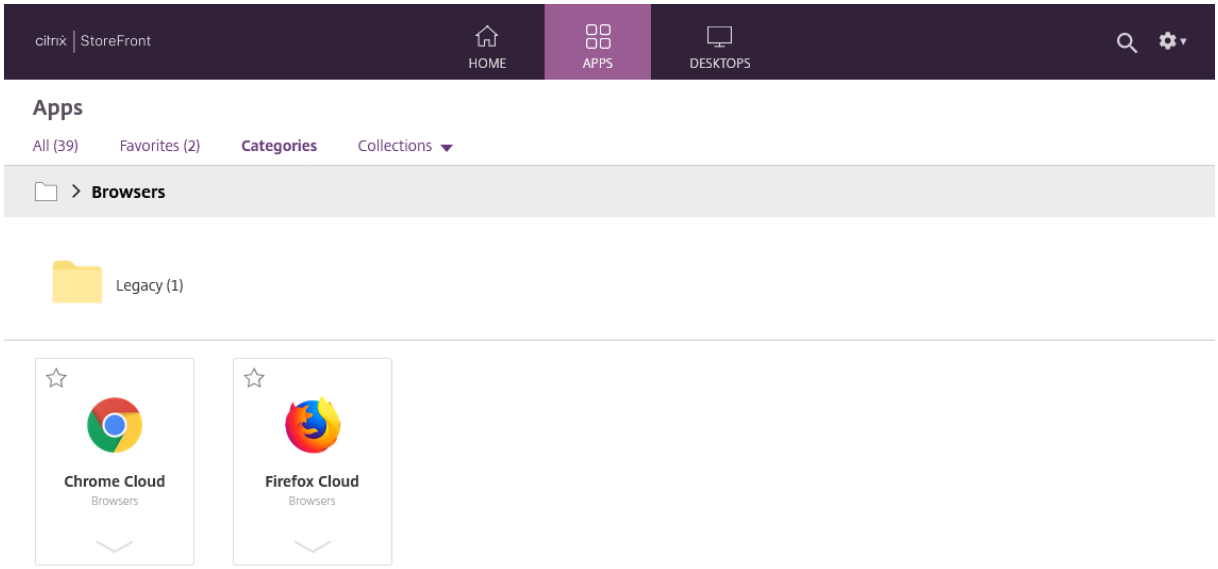
Vue des catégories

Dans la vue étendue, StoreFront affiche une liste des catégories de premier niveau. Lorsque l'utilisateur clique sur une catégorie de premier niveau, StoreFront affiche toutes les applications de toutes les sous-catégories sur une seule page.

Par exemple, si vous avez une catégorie Navigateur avec la sous-catégorie Ancienne, elle affiche tous les navigateurs, y compris ceux de la catégorie Ancienne, sur une seule page :

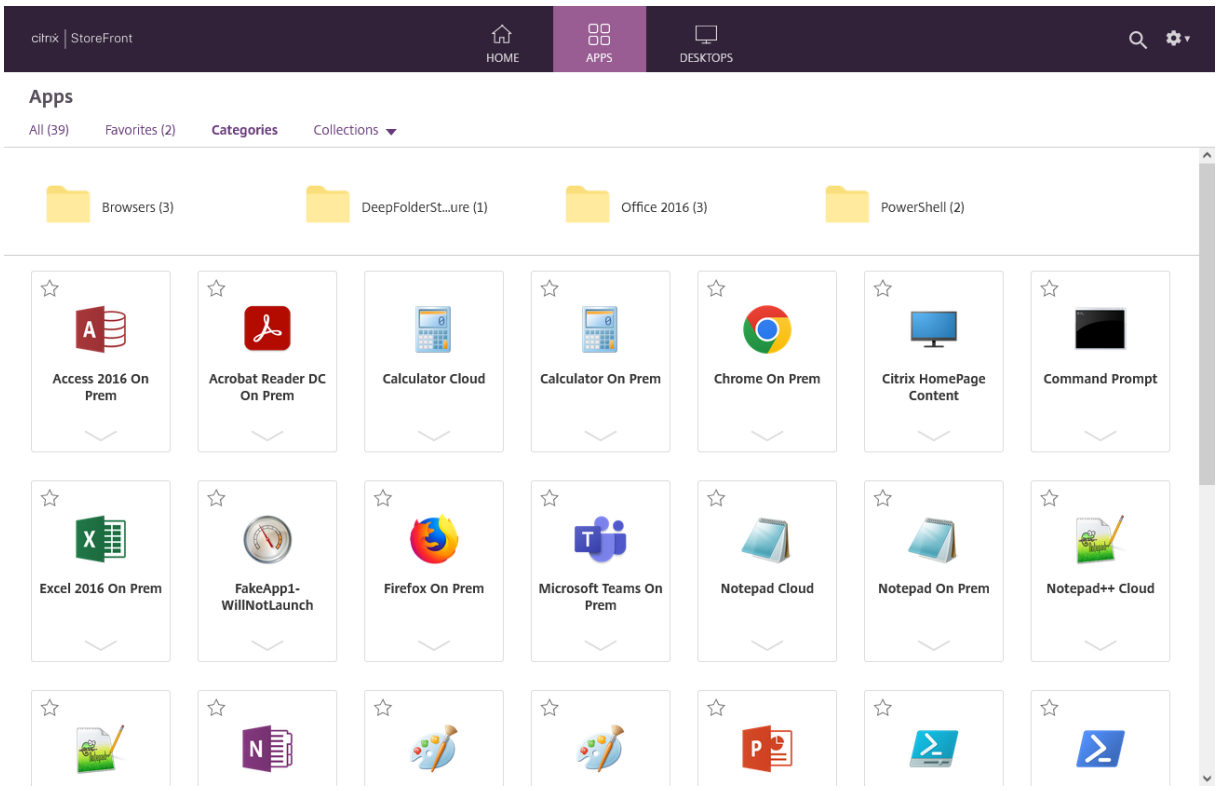


Dans la vue réduite, StoreFront affiche initialement une liste des catégories de haut niveau et, éventuellement, de toutes les applications sans catégorie. Lorsque l'utilisateur clique sur une catégorie, StoreFront affiche uniquement le contenu immédiat (sous-catégories et applications) de la catégorie sélectionnée. L'utilisateur peut cliquer sur chaque sous-catégorie pour en développer le contenu.

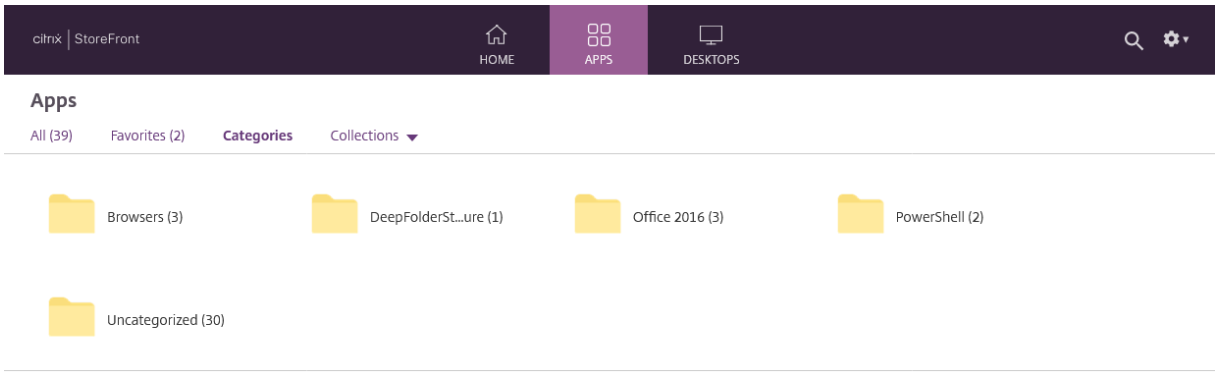


Applications sans catégorie

Dans la vue réduite, désactivez l'option **Déplacez les applications sans catégorie dans un dossier "Sans catégorie"** pour afficher toutes les applications et tous les bureaux sans catégories dans la vue initiale. Ce comportement est similaire à celui des versions précédentes de StoreFront.



Dans la vue réduite, cochez la case **Déplacez les applications sans catégorie dans un dossier "Sans catégorie"** pour déplacer toutes les applications et tous les bureaux sans catégories dans un dossier **Sans catégorie** distinct.



Configurer les paramètres de catégorie à l'aide du SDK PowerShell

Pour utiliser le SDK PowerShell afin d'activer ou de désactiver la vue des catégories, appelez l'applet de commande Set-STFWebReceiverUserInterface avec le paramètre `EnableAppsFolderView`.

Pour utiliser le SDK PowerShell afin de modifier la vue des catégories, appelez l'applet de commande Set-STFWebReceiverUserInterface avec le paramètre `CategoryViewCollapsed`.

Personnaliser l'apparence

December 6, 2023

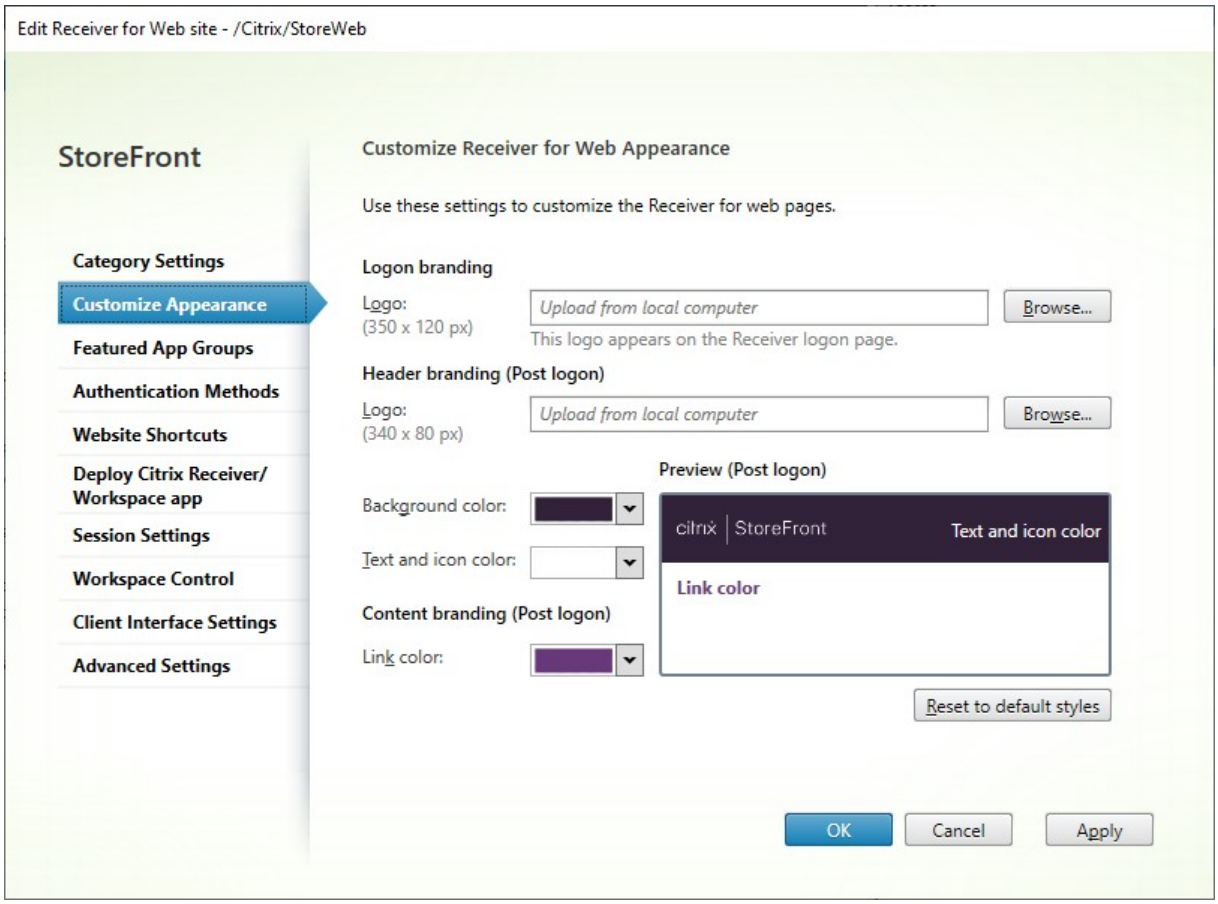
Vous pouvez modifier le logo et les couleurs utilisés sur le site Web de votre magasin.

Modifier le logo et les couleurs

Pour personnaliser l'apparence, accédez à Modifier le site Receiver pour Web et sélectionnez l'onglet **Personnaliser l'apparence**. Vous pouvez modifier les éléments suivants :

- **Logo de marque d'ouverture de session** : logo affiché sur l'écran d'ouverture de session. Il ne s'affiche pas lors de la connexion via Citrix Gateway. Appuyez sur **Parcourir…** et sélectionnez un fichier de type .jpg, .jpeg, .png, .png ou .bmp. Il est recommandé d'utiliser une image de 350 x 120 pixels.

- **Logo de marque d'en-tête** : logo affiché dans le coin supérieur gauche après la connexion. Appuyez sur **Parcourir...** et sélectionnez un fichier de type .jpg, .jpeg, .png, .png ou .bmp. Il est recommandé d'utiliser une image de 340 x 80 pixels.
- **Couleur d'arrière-plan** : couleur d'arrière-plan de la section de navigation en haut de la page.
- **Couleur des icônes et du texte** : couleur du texte et des icônes dans la section de navigation en haut de la page.
- **Couleur des liens** : couleur utilisée pour mettre en évidence l'élément actuellement sélectionné.



Modifier le logo et les couleurs à l'aide du SDK PowerShell

À l'aide du SDK PowerShell, appelez l'applet de commande Set-STFWebReceiverSiteStyle.

Rétablir l'apparence par défaut

Appuyez sur **Rétablir les styles par défaut** pour rétablir le style par défaut des logos et des couleurs.

Rétablir l'apparence par défaut à l'aide du SDK PowerShell

À l'aide du SDK PowerShell, appelez l'applet de commande Clear-STFWebReceiverSiteStyle.

Personnalisation à l'aide de Javascript et CSS

Vous pouvez personnaliser davantage le site Web à l'aide de l'API de personnalisation de l'interface utilisateur du client StoreFront.

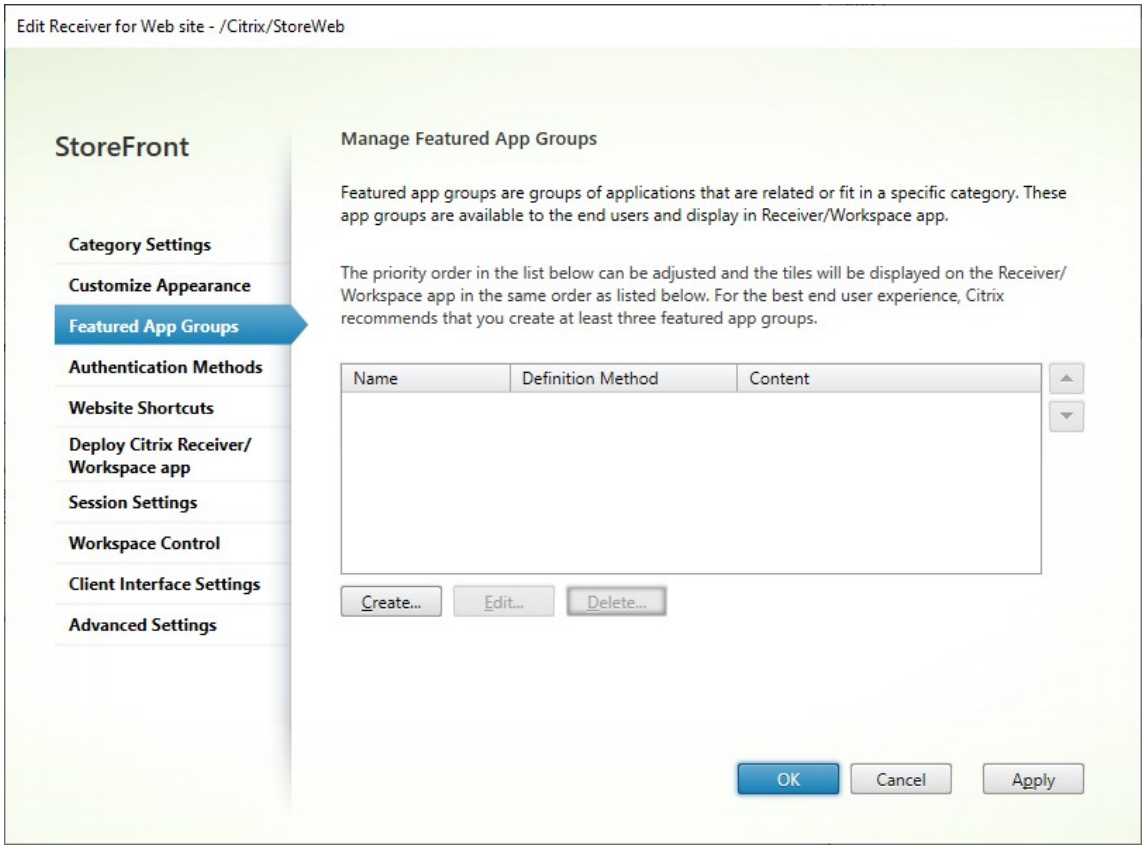
Groupes d'applications recommandées

December 6, 2023

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.

Créer un groupe d'applications recommandées

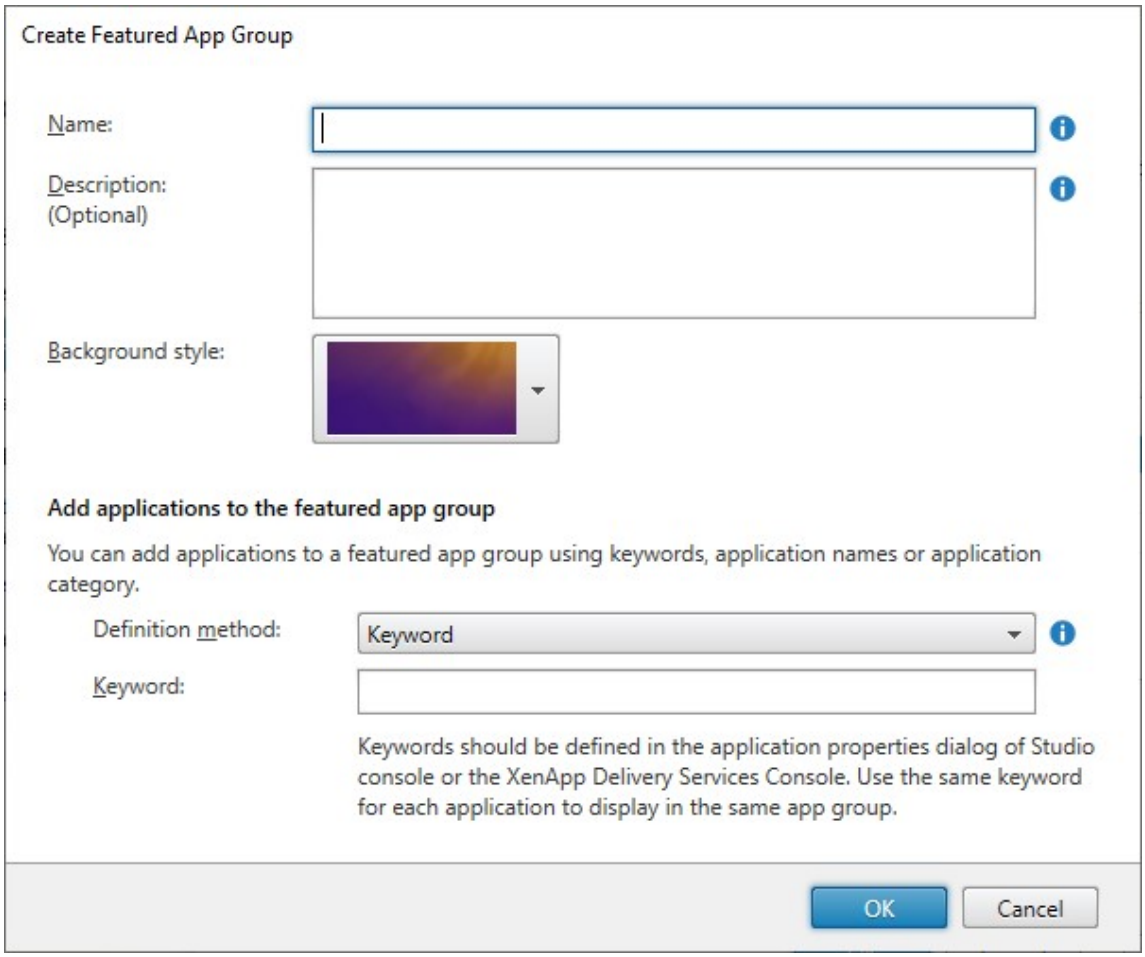
1. Dans l'écran Modifier le site Receiver pour Web, sélectionnez l'onglet **Groupes d'applications recommandées**.



2. Cliquez sur **Créer** pour définir un nouveau groupe d'applications recommandées.
3. Spécifiez le nom du groupe d'applications recommandées, sa description (facultatif), son arrière-plan et la méthode par laquelle vous définissez les groupes d'applications recommandées. Choisissez des mots clés, les noms des applications ou une catégorie d'applications.

Option	Description
Mots clés	Renvoie les applications en fonction du mot clé, défini dans Studio en incluant des mots clés dans la description de l'application, par exemple « Utiliser pour envoyer et recevoir des e-mails KEYWORDS:Collaboration »
Catégorie d'application	Renvoie les applications d'une catégorie d'applications spécifique saisie dans Studio.

Option	Description
Noms des 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.

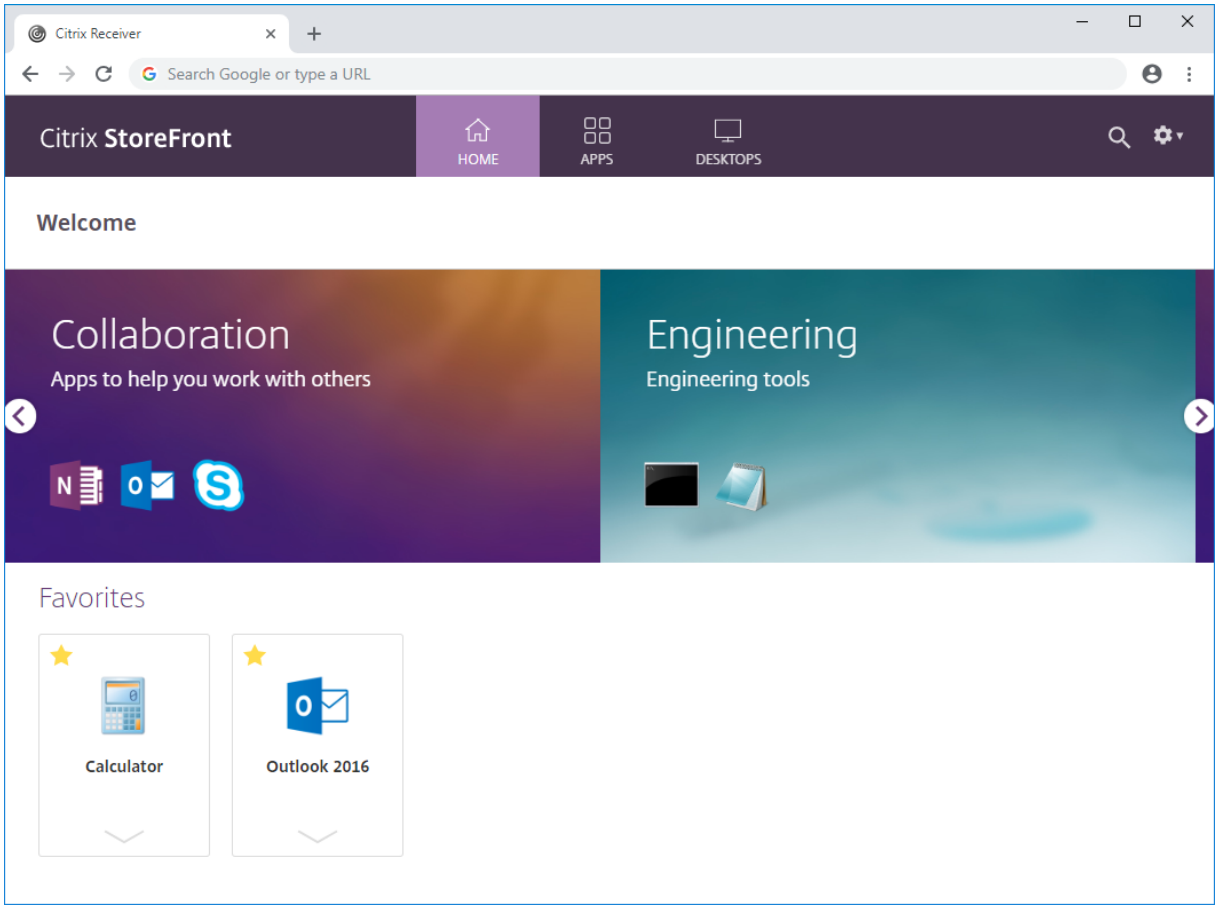


4. Cliquez sur **OK**.

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.



Créer un groupe d'applications recommandées à l'aide du SDK PowerShell

Pour ajouter un groupe d'applications recommandées avec le SDK PowerShell, utilisez l'applet de commande New-STFWebReceiverFeaturedAppGroup.

Modifier le groupe d'applications recommandées

Dans l'écran Modifier le site Receiver pour Web, sélectionnez l'onglet **Groupes d'applications recommandées**. Sélectionnez le groupe que vous souhaitez modifier et cliquez sur **Modifier…**

Modifier le groupe d'applications recommandées à l'aide du SDK PowerShell

Pour modifier un groupe d'applications recommandées avec le SDK PowerShell, utilisez l'applet de commande Set-STFWebReceiverFeaturedAppGroup.

Supprimer un groupe d'applications recommandées

Dans l'écran Modifier le site Receiver pour Web, sélectionnez l'onglet **Groupes d'applications recommandées**. Sélectionnez le groupe que vous souhaitez modifier et cliquez sur **Supprimer...**

Supprimer le groupe d'applications recommandées à l'aide du SDK PowerShell

Utilisez le SDK PowerShell pour supprimer un groupe d'applications recommandées à l'aide de l'applet de commande Remove-STFWebReceiverFeaturedAppGroup. Pour supprimer tous les groupes d'applications recommandées, utilisez l'applet de commande Clear-STFWebReceiverFeaturedAppGroup.

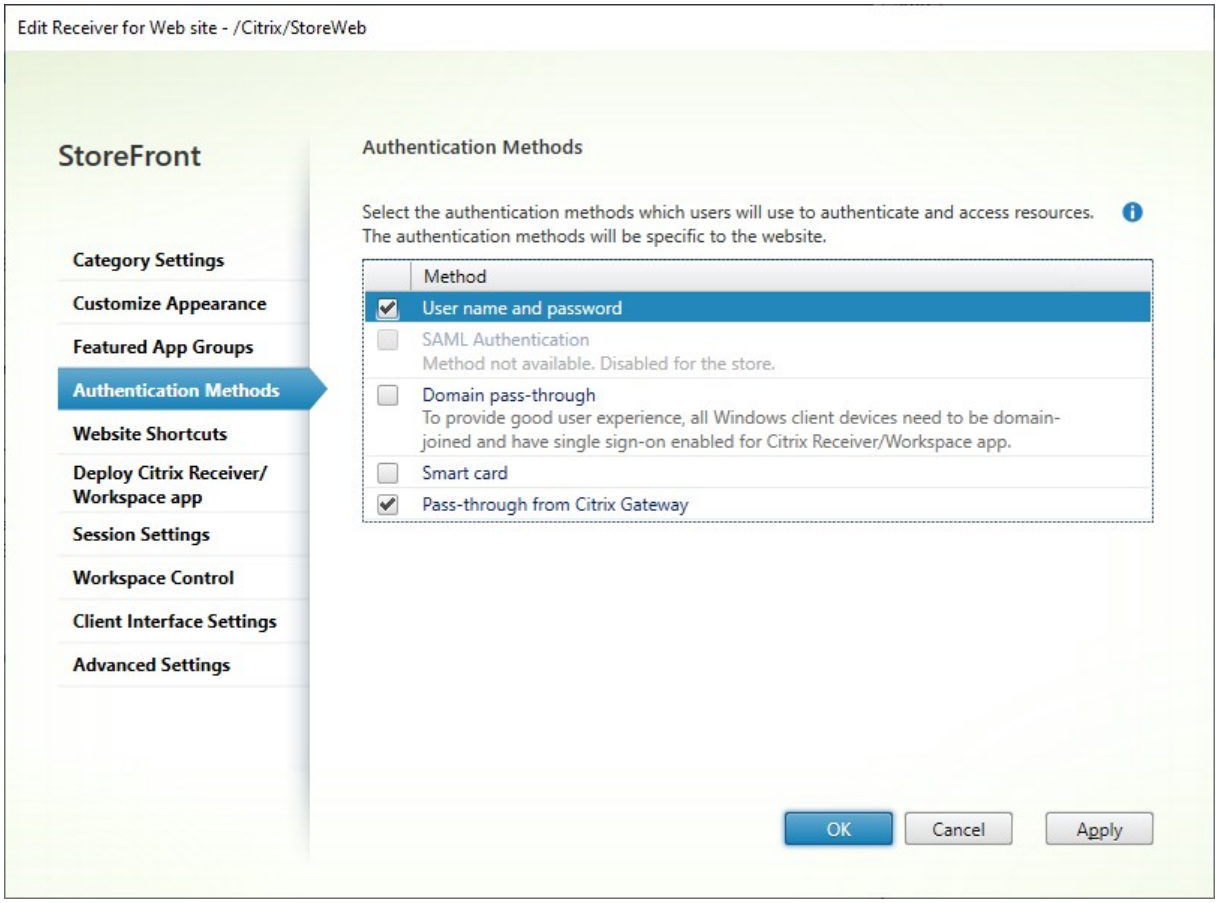
Méthodes d'authentification

April 17, 2024

Pour configurer les méthodes d'authentification disponibles pour un magasin, consultez la section Configurer l'authentification. Vous pouvez modifier certains de ces paramètres pour un site Web en particulier. Ces modifications s'appliquent uniquement à l'aide de l'application Citrix Workspace pour HTML5 via un navigateur Web. L'application Citrix Workspace installée localement utilise les paramètres du magasin plutôt que ceux du site Web.

> **Avertissement :**
> chaque fois que vous modifiez les méthodes d'authentification d'un magasin, cela remplace les paramètres de tous les sites Web de ce magasin. Toute modification doit donc être réappliquée.

Pour modifier les méthodes d'authentification, accédez à Modifier le site Receiver pour Web et sélectionnez l'onglet **Méthodes d'authentification**.



- Cochez la case **Nom d'utilisateur et mot de passe** pour activer l'authentification explicite. Voir Authentification par nom d'utilisateur et mot de passe. Cette option n'est disponible que si elle est activée pour le magasin.
- Sélectionnez la case **Authentification SAML** pour activer l'intégration avec un fournisseur d'identité SAML. Voir Authentification SAML. Cette option n'est disponible que si elle a été activée pour le magasin.
- 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. Voir Authentification pass-through au domaine. Cette option n'est disponible que si elle a été activée pour le magasin.
- Sélectionnez **Carte à puce** pour activer l'authentification par carte à puce. Voir Authentification par carte à puce.
- Sélectionnez **Authentification pass-through via Citrix Gateway** pour activer l'authentification pass-through à partir de Citrix Gateway. Activez cette option si les utilisateurs se connectent à StoreFront via Citrix Gateway avec l'authentification activée. Voir Authentification pass-through via Citrix Gateway.

Configuration à l'aide du SDK PowerShell

Pour configurer les méthodes d'authentification disponibles à l'aide du SDK PowerShell, utilisez l'applet de commande Set-STFWebReceiverAuthenticationMethods.

Raccourcis de site Web

December 6, 2023

Utilisez des raccourcis de site Web pour fournir aux utilisateurs un accès rapide aux bureaux et aux applications à partir de sites Web approuvés 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.

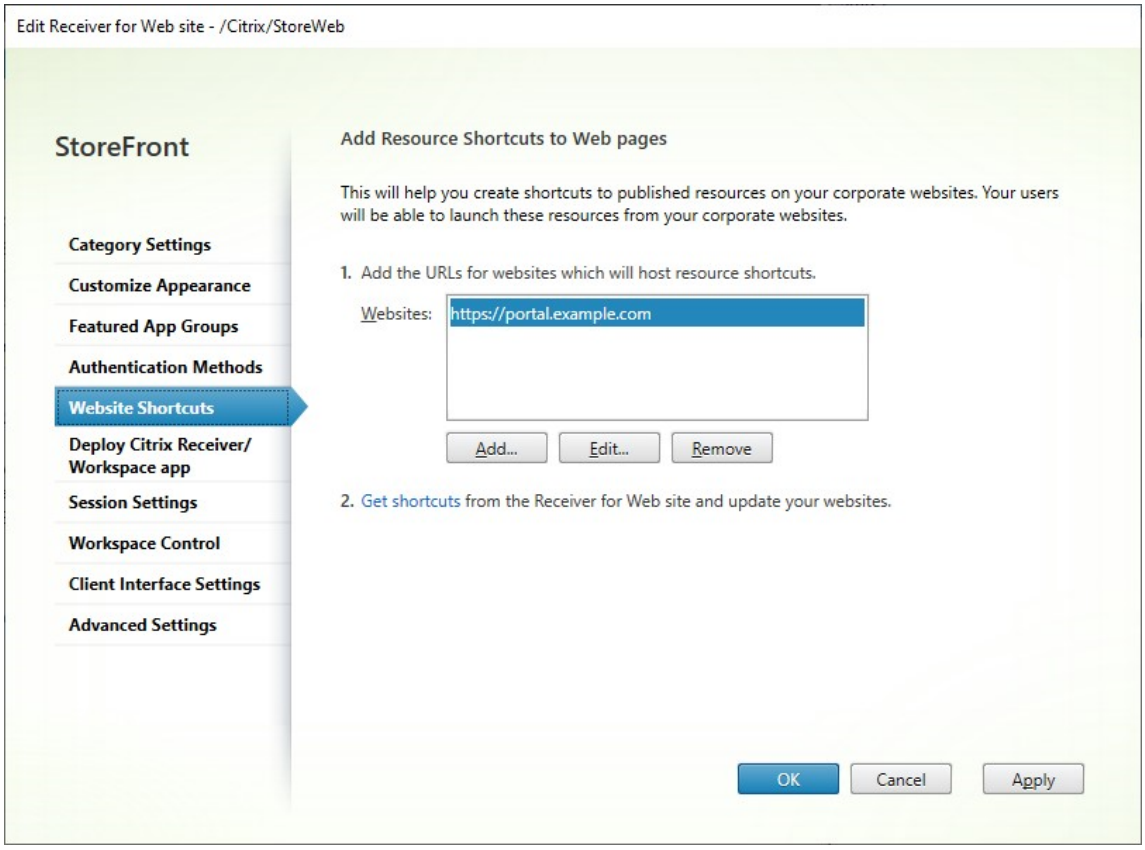
Avant de pouvoir créer des raccourcis vers les ressources, vous devez ajouter les adresses URL des sites Web hôtes à la liste des *adresses URL approuvées* à l'aide de la console de gestion Citrix StoreFront ou à l'aide de PowerShell.

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, cliquez sur **Gérer les sites Receiver pour Web** dans le panneau Magasins **>** cliquez sur **Configurer >** choisissez **Paramètres avancés >** décochez l'option **Invite pour les raccourcis non approuvés**.

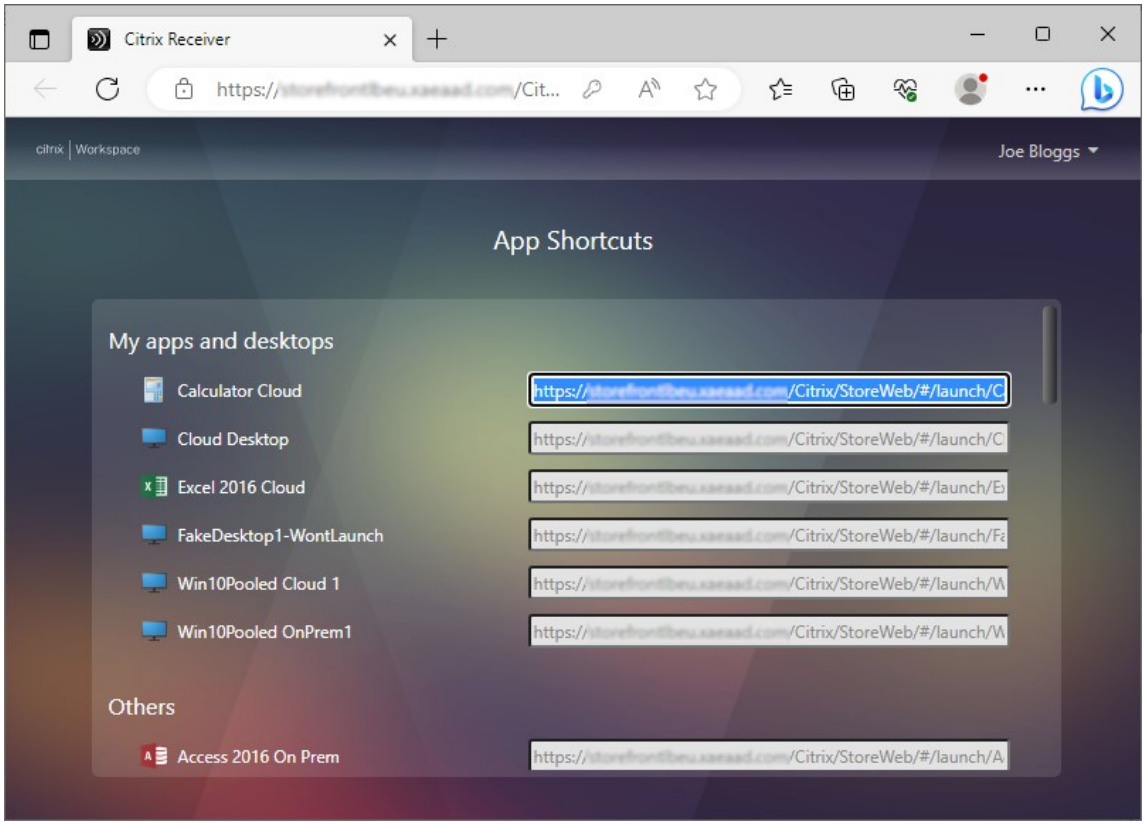
Pour des raisons de sécurité, les utilisateurs d'Internet Explorer peuvent être invités à confirmer qu'ils souhaitent démarrer les ressources accessibles via les raccourcis. Demandez à vos utilisateurs d'ajouter le nom de domaine complet du serveur StoreFront à la zone Intranet local ou Sites de confiance dans Internet Explorer pour éviter cette étape supplémentaire.

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

1. Dans l'écran Modifier le site Receiver pour Web, sélectionnez l'onglet **Raccourcis de site Web**.



2. 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.
3. Cliquez sur **Obtenir raccourcis** et copiez les URL dont vous avez besoin pour votre site Web.



Ajouter des sites Web approuvés à l'aide du SDK PowerShell

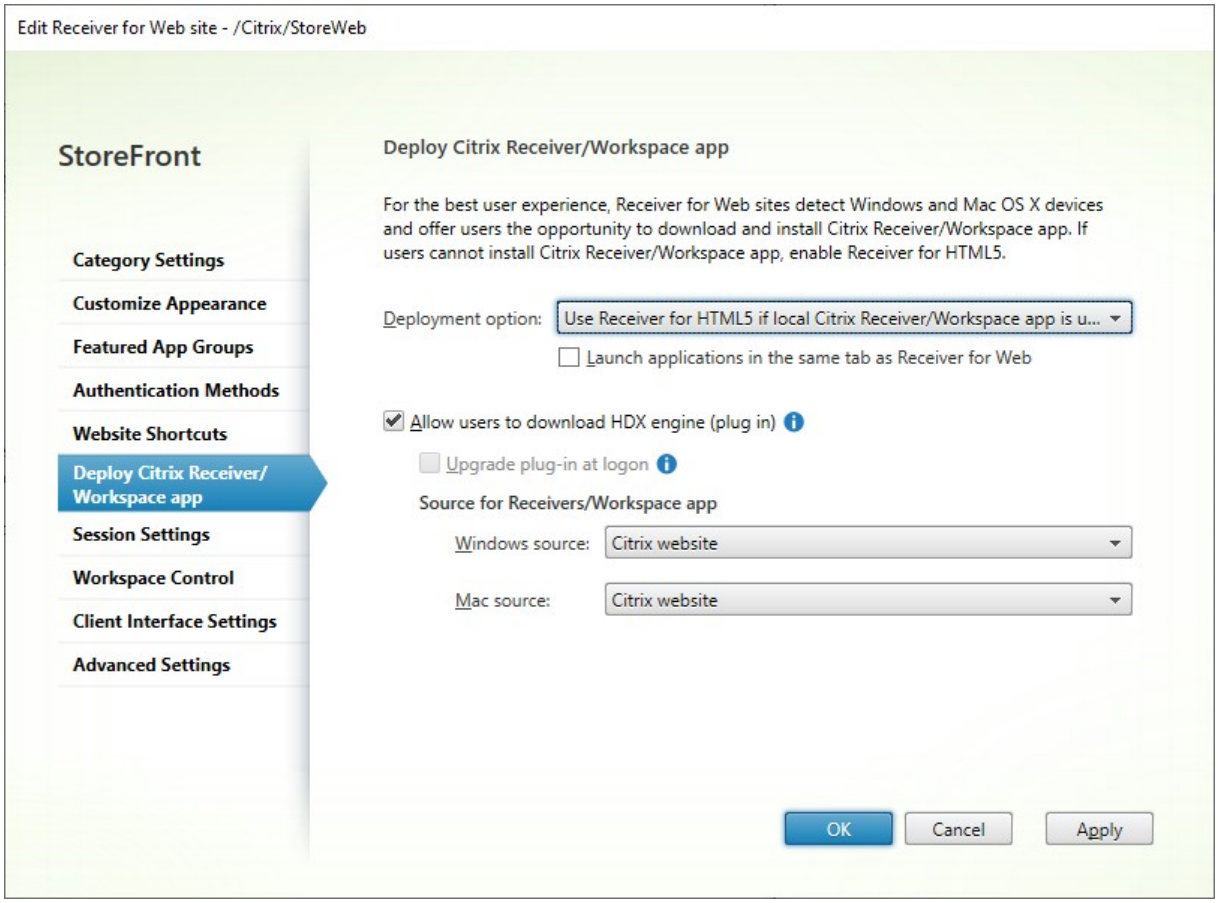
Vous pouvez ajouter des adresses URL approuvées à l'aide de l'applet de commande PowerShell Set-STFWebReceiverApplicationShortcuts.

Déploiement de l'application Citrix Workspace

May 30, 2024

Par défaut, lorsqu'un utilisateur accède pour la première fois à un magasin via un navigateur Web sous Windows, macOS ou Linux, StoreFront tente automatiquement de déterminer si l'application Citrix Workspace est installée localement.

Si une application Citrix Workspace déployée localement ne peut être détectée, l'utilisateur est invité à la télécharger et à l'installer. L'emplacement de téléchargement par défaut est le site Web de Citrix, mais vous pouvez également héberger les programmes d'installation sur le serveur StoreFront ou ailleurs. Les utilisateurs qui ne peuvent pas installer l'application Citrix Workspace localement peuvent utiliser l'application Citrix Workspace pour HTML5 via leur navigateur Web.



Pour modifier les options de déploiement, accédez à Modifier le site Receiver pour Web et sélectionnez l'onglet **Déployer l'application Workspace/Citrix Receiver**.

Option de déploiement

- Sélectionnez **Toujours utiliser Receiver pour HTML5** si vous souhaitez que l'utilisateur puisse toujours accéder aux ressources via un navigateur Web sans l'inviter à télécharger et installer l'application Citrix Workspace localement. Lorsque cette option est sélectionnée, les utilisateurs de Workspace pour HTML5 accèdent toujours aux ressources directement via leur navigateur.
- Sélectionnez **Utiliser Receiver pour HTML5 si une installation Receiver locale n'est pas disponible** si vous souhaitez que le site Web du magasin invite l'utilisateur à télécharger et à installer l'application Citrix Workspace localement, mais qu'il se replie sur un navigateur pour accéder aux ressources si 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. Les

utilisateurs peuvent continuer à accéder au magasin via un navigateur Web, mais lorsqu'ils lancent une ressource, celle-ci s'ouvre dans l'application Workspace installée localement.

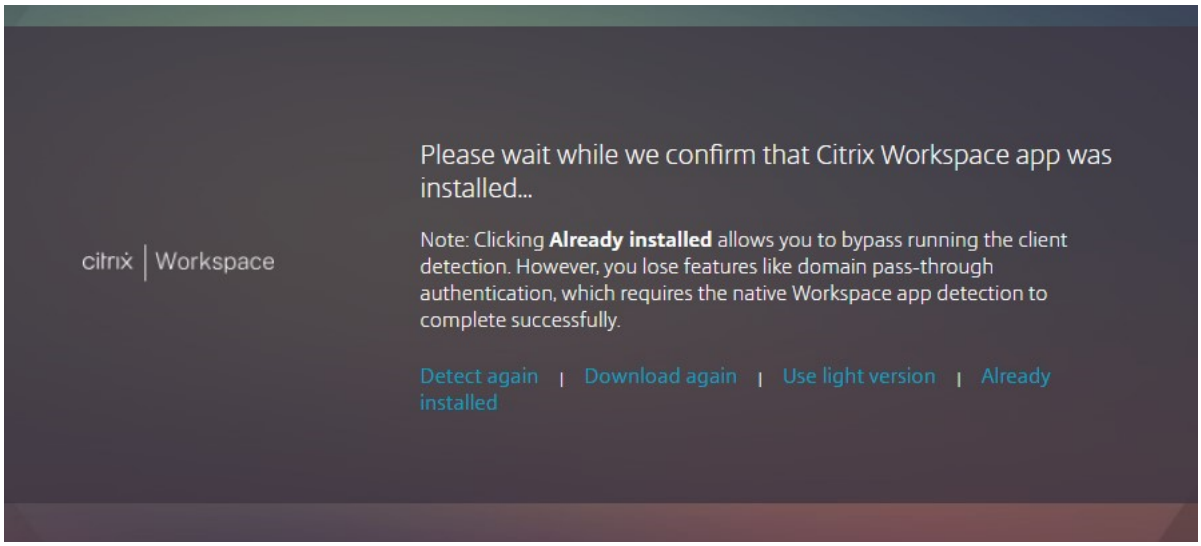
Lancer des applications dans le même onglet

Si vous avez sélectionné **Toujours utiliser Receiver pour HTML5** ou **Utiliser Receiver pour HTML5 si une installation Receiver locale n'est pas disponible**, les ressources lancées dans le navigateur ouvrent un nouvel onglet de navigateur par défaut. Si vous souhaitez que vos ressources s'ouvrent dans le même onglet, au lieu de l'application Workspace pour HTML5, sélectionnez **Lancer les applications dans le même onglet que Receiver pour Web**.

Afficher l'option Déjà installé sur la page de détection des clients

> **Remarque :**
>
> Ce paramètre ne s'applique qu'aux appareils Windows, MacOS et Linux. Si un utilisateur a installé des extensions Web de Workspace, la détection et le lancement du client sont gérées par les extensions Web. Dans ce cas, ce paramètre ne s'applique pas.

Lorsque les utilisateurs ouvrent un magasin dans leur navigateur pour la première fois sous Windows, macOS ou Linux, le site Web tente de détecter l'application installée localement à l'aide du lanceur Citrix Workspace. Par la suite, lorsque les utilisateurs lancent une ressource, le lanceur Citrix Workspace communique avec l'application Citrix Workspace installée localement. Si les utilisateurs cliquent sur l'option Déjà installé, le processus de détection du client est ignoré. Par conséquent, lorsque les utilisateurs lancent une ressource, un fichier `.ica` est téléchargé, qui peut être ouvert avec l'application Citrix Workspace installée localement. Les fonctionnalités telles que l'authentification unique de domaine et la protection des applications ne sont pas prises en charge.



Ce fichier `.ica` téléchargé peut présenter un risque de sécurité. Citrix vous recommande de désactiver la case à cocher **Afficher le lien Déjà installé sur la page de détection des clients** de façon à masquer l'option **Déjà installé**.

Empêcher les téléchargements de fichiers .ica sur toutes les plateformes

Ajoutez un niveau de protection supplémentaire en bloquant complètement les téléchargements de fichiers `.ica` sur toutes les plateformes. Le lanceur Citrix Workspace n'étant pas disponible sur iOS, Android ou Chrome, les utilisateurs doivent soit sélectionner **Utiliser la version simplifiée** si disponible, soit ajouter leur magasin à leur application Citrix Workspace installée localement.

> **Important :**
>
> Cette option ne doit pas être utilisée conjointement avec l'option **Afficher Déjà installé** sur la page de détection des clients.

Autoriser les utilisateurs à télécharger l'application Citrix Workspace pour Windows ou Mac

Si vous sélectionnez **Installer localement** ou **Utiliser Receiver pour HTML5 si une installation Receiver locale n'est pas disponible** et que vous activez **Autoriser les utilisateurs à télécharger le moteur HDX (plug-in)**, si l'application Workspace pour HTML5 ne détecte pas l'application Workspace installée localement, elle donne à l'utilisateur la possibilité de télécharger l'application Citrix Workspace pour Windows ou Mac.

Mettre à niveau l'application Workspace lors de l'ouverture de session

Si vous sélectionnez **Mettre le plug-in à niveau à l'ouverture de session**, l'application Workspace pour HTML5 permet aux utilisateurs de mettre à niveau le client installé localement de 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 ne soient effacés. Pour activer cette fonctionnalité, assurez-vous que les fichiers de l'application Citrix Workspace sont disponibles sur le serveur StoreFront.

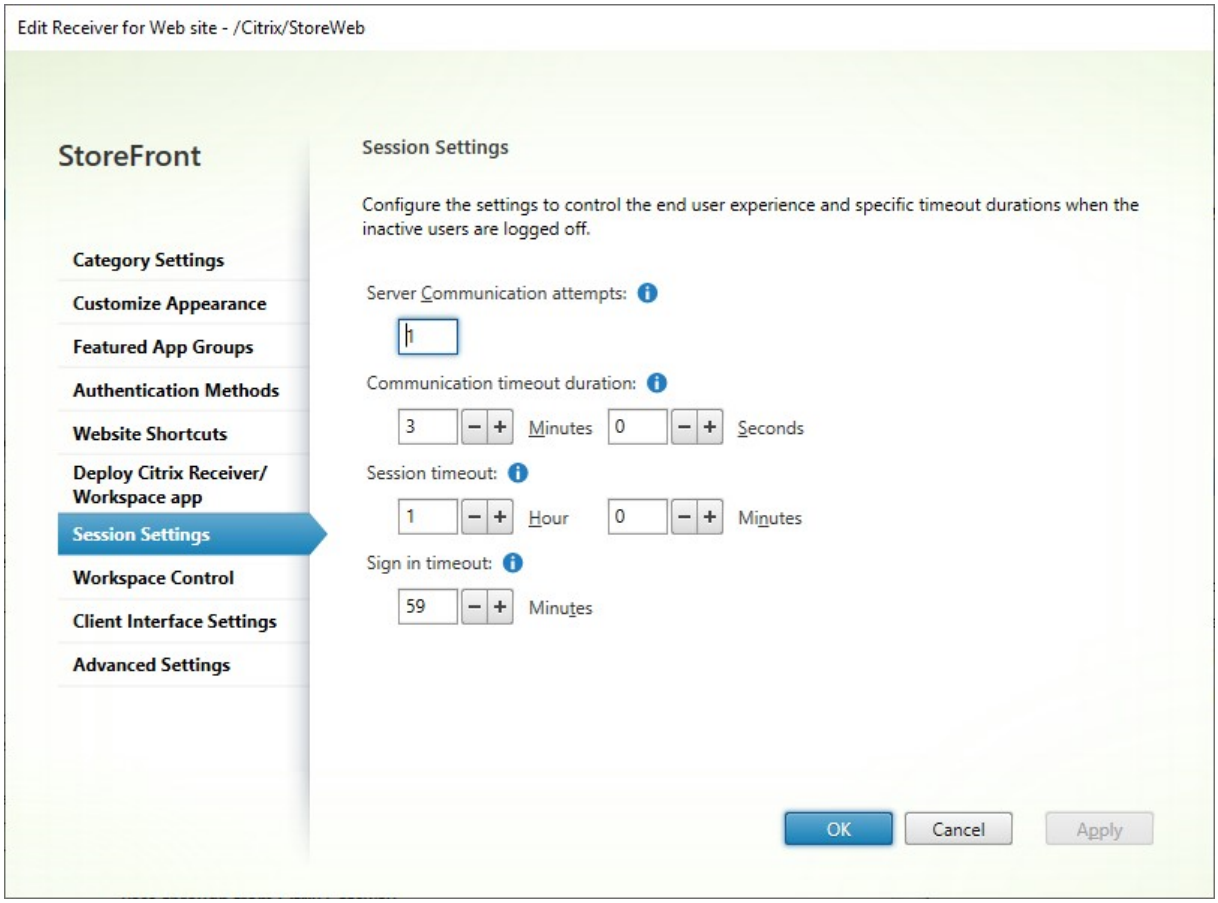
Télécharger la source

Lorsque les utilisateurs cliquent sur le bouton de téléchargement, vous pouvez choisir s'ils sont redirigés vers le site Web de Citrix ou s'ils peuvent télécharger des fichiers directement depuis le serveur. Les options disponibles sont **Site Web Citrix**, **Fichiers locaux sur le serveur StoreFront** ou **Fichiers sur un serveur distant (via URL)**.

Configurer les paramètres de session

November 10, 2023

Pour modifier les paramètres de session, accédez à l'écran Modifier le site Receiver pour Web, puis sélectionnez l'onglet **Paramètres de session**.



Tentatives de communication avec le serveur

Nombre de tentatives d'appels entre le proxy Web et les services de magasin, internes à StoreFront. Normalement, il n'est pas nécessaire de modifier ce paramètre.

Délai d'expiration des communications

Durée autorisée pour les appels entre le proxy Web et les services de magasin, internes à StoreFront. Normalement, il n'est pas nécessaire de modifier ce paramètre.

Délai d'inactivité de session

Lorsqu'il accède à un magasin StoreFront via un navigateur Web, après une période d'inactivité, l'utilisateur voit le message **Votre session a expiré pour cause d'inactivité**. Vous pouvez modifier le **délai d'expiration de session** en fonction des besoins de vos utilisateurs. Cela n'affecte pas les applications Citrix Workspace.

Vous pouvez également utiliser PowerShell. Par exemple, pour définir le délai d'expiration du site Web « /Citrix/StoreWeb » à 30 minutes :

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'
Set-STFWebReceiverService $rfw -SessionStateTimeout 30
<!--NeedCopy-->
```

Si vous modifiez le délai d'expiration de session de manière à ce qu'il soit supérieur à la durée de vie du jeton d'authentification ou la durée de vie maximale du jeton, cela met également à jour la durée de vie du jeton d'authentification et la durée de vie maximale.

Durée de vie du jeton d'authentification

Lorsqu'un utilisateur accède à un magasin StoreFront via un navigateur, l'utilisateur est déconnecté par défaut au bout de huit heures, quelle que soit son activité. Cela n'affecte pas les applications Citrix Workspace. Pour augmenter ce délai, procédez comme suit :

1. Sur StoreFront, accédez à **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Ouvrez le fichier `web.config`.
3. Repérez l'entrée : **`<authentication tokenLifeTime="08:00:00"method="Auto"/>`**
4. Définissez **`tokenLifeTime`** sur la valeur souhaitée. Pour saisir une valeur d'un jour ou plus, utilisez le format `d.h:m:s`.

Si vous augmentez le délai d'expiration de session à plus de 20 heures, vous devez également augmenter la durée de vie maximale des jetons du service d'authentification.

Durée de vie maximale du jeton du service d'authentification

Le service d'authentification émet des jetons qui sont utilisés lors de la connexion à un magasin via un navigateur Web ou des applications Citrix Workspace. Pour les applications Citrix Workspace, il s'agit du seul délai de connexion qui doit être mis à jour. Lorsque vous accédez à StoreFront via un navigateur, ce délai est utilisé avec les autres délais. Contrairement aux autres paramètres décrits sur cette page, cela s'applique à tous les sites Web du magasin.

Lorsque vous utilisez StoreFront avec Citrix Gateway, Citrix Gateway dispose des informations d'identification de l'utilisateur et s'authentifie via SSO à StoreFront. Si le jeton StoreFront expire, StoreFront présente un challenge CitrixAG Basic et Citrix Gateway fournit les informations d'identification pour se connecter à StoreFront. Par conséquent, si vous utilisez également Citrix Gateway, vous devez également configurer son propre délai d'expiration de session.

1. Pour l'application Citrix Workspace installée sur le serveur StoreFront, accédez au chemin du service d'authentification de votre magasin **`c:\inetpub\wwwroot\Citrix\<Store>Auth`** (qui peut être l'un de plusieurs services d'authentification en fonction du nombre de magasins dont vous disposez).
2. Dans le fichier `web.config`, localisez le service **Authentication Token Producer**, puis recherchez l'élément `add` dont l'`id` correspond à celui du **Authentication Token Producer**. Dans l'exemple suivant, vous avez besoin de l'élément `add` avec `id="f7cac185-57c1-4629-a33c-88a89dd4295d"encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b"` :

```
1 <service id="f7cac185-57c1-4629-a33c-88a89dd4295d" displayName="
     Authentication Token Producer">
2      <relyingParties signingId="2948f7ad-735e-4e03-8e01-8
          d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="
          01:00:00">
3      <clear />
4      <add id="f7cac185-57c1-4629-a33c-88a89dd4295d" encipherId="
          2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="
          01:00:00" maxLifetime="20:00:00" />
5 <!--NeedCopy-->
```

3. Définissez **`maxLifetime`** sur la valeur souhaitée. La valeur par défaut est `20:00:00`. Pour saisir une valeur d'un jour ou plus, utilisez le format `dd.hh:mm:ss`.
4. Exécutez la commande **`iisreset`** pour appliquer les modifications. L'exécution de cette commande déconnecte les utilisateurs de Citrix StoreFront Web, mais elle n'impacte pas leur session ICA en cours.

Contrôle de l'espace de travail

April 17, 2024

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.

Lorsque les utilisateurs ouvrent une session, ils sont automatiquement reconnectés à toutes les applications qu'ils ont laissées en cours d'exécution. Imaginons, par exemple, qu'un utilisateur ouvre une session dans un magasin 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 de l'accès à un magasin via un navigateur Web, le même navigateur doit être utilisé pour ouvrir une session, démarrer les applications et se déconnecter.

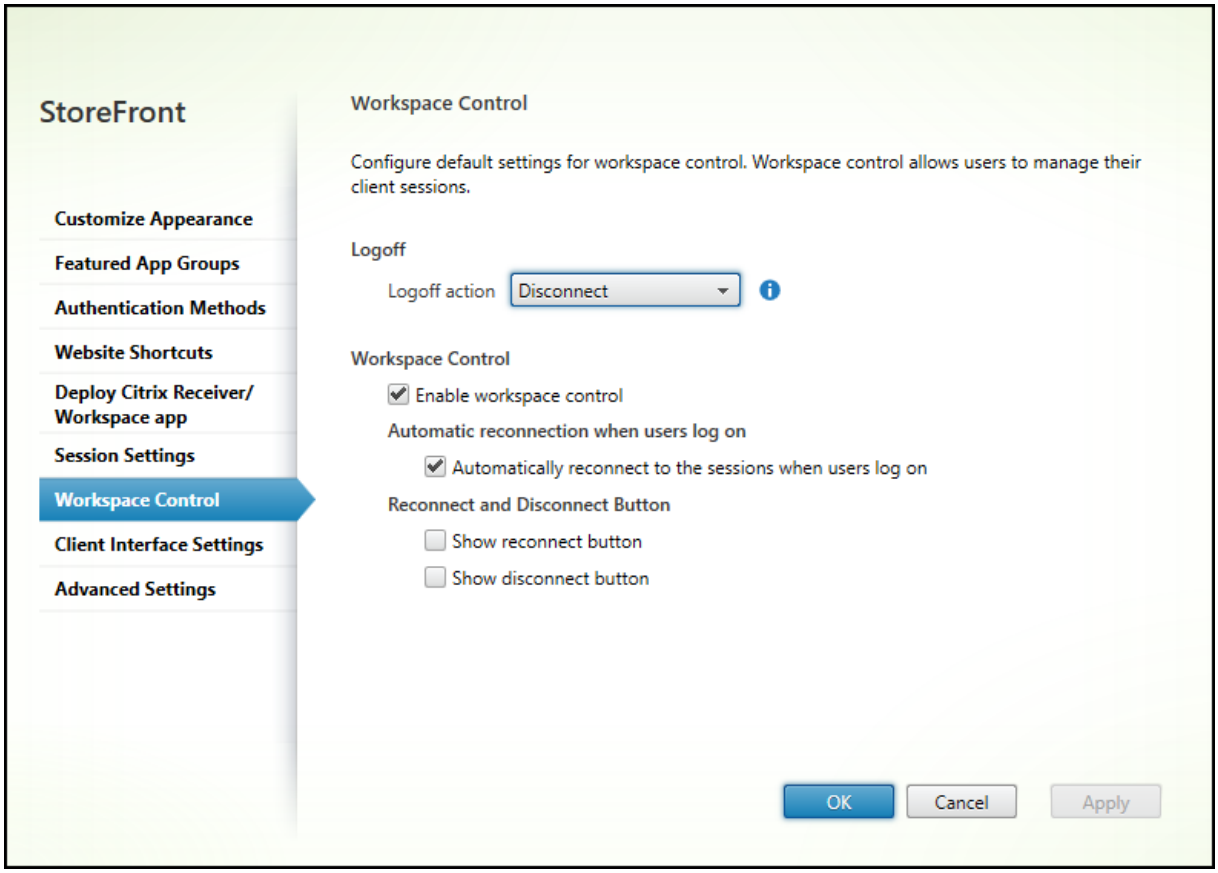
Configurer le contrôle de l'espace de travail sur l'application Workspace pour HTML5

Les paramètres de contrôle de l'espace de travail dans la console de gestion StoreFront s'appliquent uniquement lorsque vous accédez au magasin via un navigateur Web. Ceci est soumis aux exigences et restrictions suivantes :

- Le contrôle de l'espace de travail n'est pas disponible lorsque l'application Workspace pour HTML est exécutée sur une application ou un bureau hébergé(e).
- Pour les utilisateurs qui accèdent à des sites 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 pour Windows 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 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 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 l'application Citrix Workspace pour HTML5.
- Le contrôle de l'espace de travail n'est pas disponible lorsque les ressources s'ouvrent dans le même onglet de navigateur. Pour configurer ce paramètre, consultez la section Déploiement de l'application Citrix Workspace.

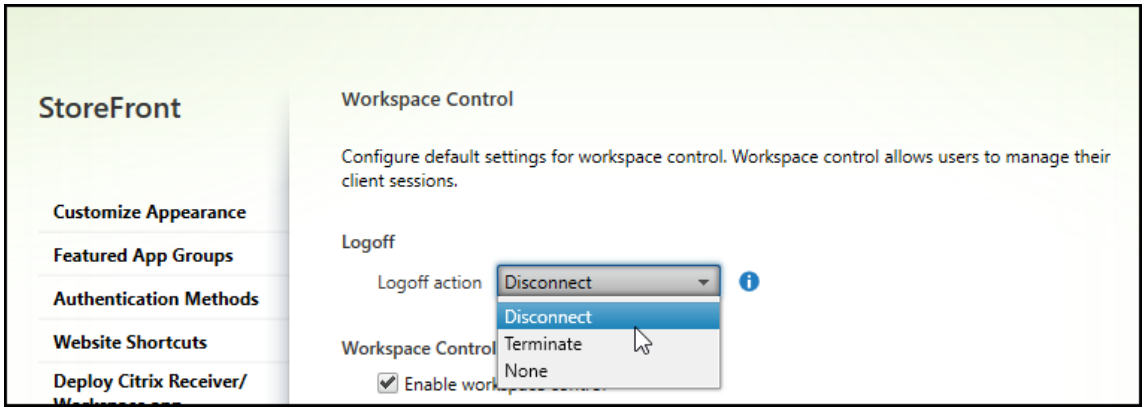
Pour modifier les paramètres de contrôle de l'espace de travail lorsqu'un magasin est accessible via

un navigateur Web, sélectionnez **Contrôle de l'espace de travail** sur l'écran Modifier le site Receiver pour Web.



Configurez les paramètres du contrôle de l'espace de travail comme suit :

- Spécifiez l'**action de fermeture de session**. Les actions de fermeture de session sont les suivantes :
  - **Déconnexion** : lorsque vous vous déconnectez du site, les sessions d'application et de bureau sont automatiquement déconnectées de l'appareil client.
  - **Terminer** : lorsque vous vous déconnectez du site, les sessions d'application et de bureau sont automatiquement fermées sur le serveur.
  - **Aucune** : lorsque vous vous déconnectez du site, les sessions d'application et de bureau restent actives.



- Cochez la case **Activer le contrôle de l'espace de travail**.
- Activez la case à cocher **Se reconnecter automatiquement aux sessions quand les utilisateurs ouvrent une session** sous **Reconnexion automatique quand les utilisateurs ouvrent une session**.

Configurer le contrôle de l'espace de travail à l'aide du SDK PowerShell

Vous pouvez configurer le contrôle de l'espace de travail à l'aide de l'applet de commande Set-STFWebReceiverUserInterface.

Configurer le contrôle de l'espace de travail sur l'application Workspace pour Windows

Pour configurer le contrôle de l'espace de travail sur Workspace pour Windows, consultez Gérer la reconnexion au contrôle de l'espace de travail.

Configurer le contrôle de l'espace de travail sur l'application Workspace pour Mac

Pour configurer le contrôle de l'espace de travail sur Workspace pour Mac, consultez Configurer les paramètres du contrôle de l'espace de travail.

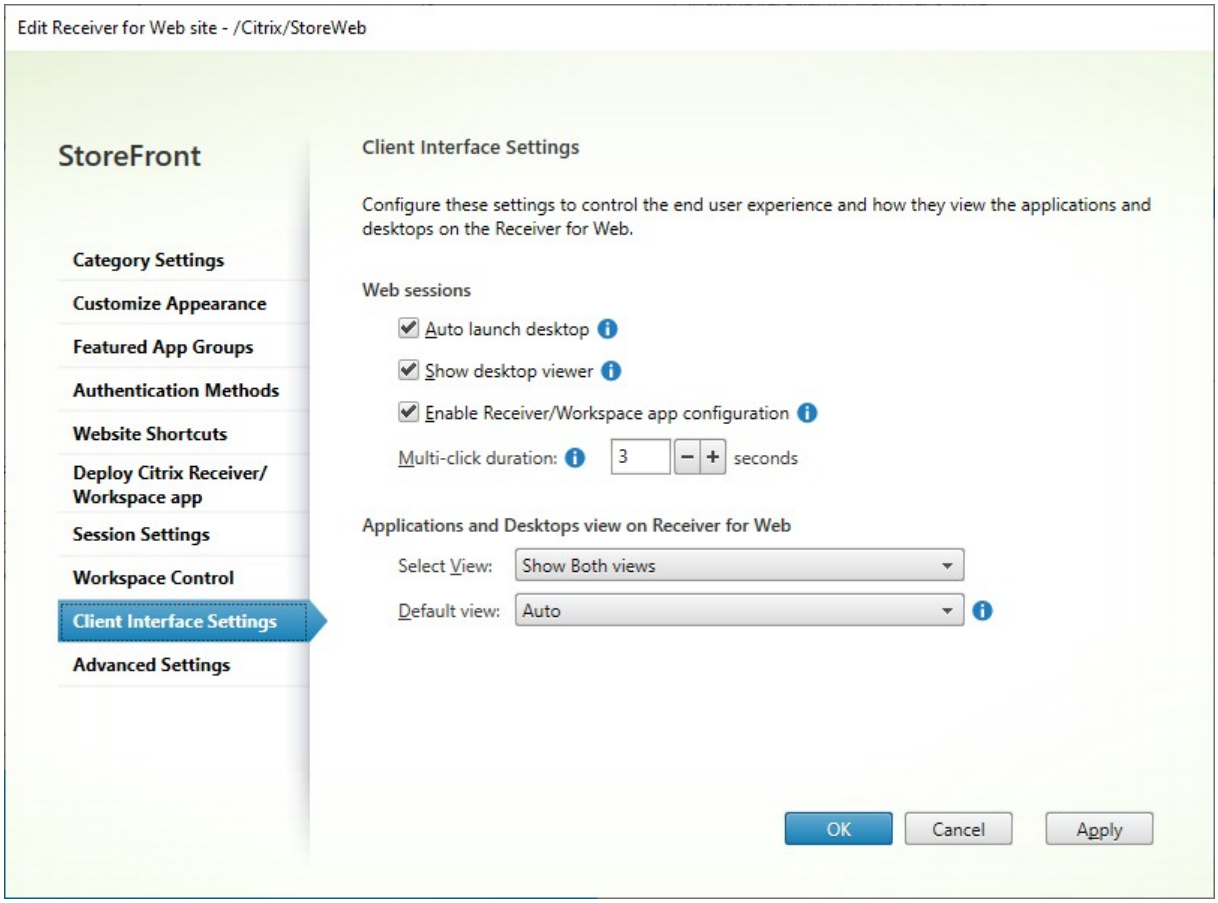
Désactiver le contrôle de l'espace de travail dans toutes les applications

Pour désactiver la reconnexion de sessions dans StoreFront entre les applications Workspace, quelle que soit la manière dont elles sont configurées, accédez à l'onglet **Paramètres avancés** et décochez **Autoriser la reconnexion de sessions**.

Paramètres de l'interface client

February 22, 2024

Pour modifier les paramètres de l'interface client à partir de l'écran Modifier le site Receiver pour Web, sélectionnez l'onglet **Paramètres de l'interface client**.



Lancement automatique du bureau

Si ce paramètre est activé et qu'un utilisateur ne possède qu'un bureau, celui-ci est lancé lorsque l'utilisateur se connecte.

Pour utiliser le SDK PowerShell afin de modifier les paramètres de lancement automatique du bureau, appelez l'applet de commande Set-STFWebReceiverUserInterface avec le paramètre `AutoLaunchDesktop`.

Ce paramètre s'applique uniquement à l'application Citrix Workspace pour HTML5. Il ne s'applique pas aux applications Citrix Workspace installées localement.

Afficher Desktop Viewer

Le Desktop Viewer est la barre d'outils qui permet d'accéder facilement aux préférences HDX. Utilisez ce paramètre pour choisir s'il doit être affiché.

Ce paramètre s'applique uniquement à l'application Citrix Workspace pour HTML5. Il ne s'applique pas aux applications Citrix Workspace installées localement.

Durée des clics multiples

Ce paramètre empêche les utilisateurs de lancer la même application plusieurs fois au cours de la durée configurée. Cela s'applique uniquement à l'application Citrix Workspace pour HTML5, et non à l'application Citrix Workspace native.

Pour utiliser le SDK PowerShell afin de modifier la durée des clics multiples, appelez l'applet de commande Set-STFWebReceiverUserInterface avec le paramètre `MultiClickTimeout`.

Ce paramètre s'applique uniquement à l'application Citrix Workspace pour HTML5. Il ne s'applique pas aux applications Citrix Workspace installées localement.

Activer la configuration de l'application Workspace/Receiver

Si cette option est sélectionnée, l'application Citrix Workspace pour HTML5 offre des fichiers de provisioning qui permettent aux utilisateurs de configurer automatiquement l'application Citrix Workspace native 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.

Pour utiliser le SDK PowerShell afin de modifier cette option, appelez l'applet de commande Set-STFWebReceiverUserInterface avec le paramètre `ReceiverConfigurationEnabled`.

Affichage des applications et des bureaux

Lorsque des bureaux et des applications sont disponibles, l'application Citrix Workspace affiche par défaut des vues distinctes des bureaux et des applications. Les favoris s'affichent dans la vue **Accueil**. Les utilisateurs voient tout d'abord la vue **Accueil** lorsqu'ils ouvrent une session sur le site.

Dans la liste déroulante **Sélectionner l'affichage**, sélectionnez si vous souhaitez afficher les applications ou les bureaux, ou les deux.

Dans la liste déroulante **Affichage par défaut**, sélectionnez la vue qui s'affiche lorsque l'utilisateur se connecte.

Option	Description
Auto	Afficher la vue d'accueil
Applications	Afficher la vue des applications
Bureaux	Afficher la vue des bureaux

Pour utiliser le SDK PowerShell afin de modifier ces options, appelez l'applet de commande Set-STFWebReceiverUserInterface avec les paramètres `ShowAppsView`, `ShowDesktopsView` et `DefaultView`.

App Protection

May 30, 2024

App Protection fournit un niveau de sécurité supplémentaire en bloquant l'enregistrement de frappe et la capture d'écran. Pour plus d'informations, consultez la documentation App Protection.

Application Workspace

La protection des applications est disponible par défaut lors de l'accès à un magasin via les applications Citrix Workspace pour Windows, Mac et Linux.

Protection des applications pour un lancement hybride

Lorsque vous accédez à un magasin via un navigateur Web, les applications nécessitant la fonction App Protection sont masquées par défaut. Vous pouvez configurer StoreFront 2308 pour afficher les applications protégées lorsqu'il détecte les versions minimales suivantes de l'application Citrix Workspace :

Application	Version
Application Citrix Workspace pour Windows	1912
Application Citrix Workspace pour Mac	2001
Application Citrix Workspace pour Linux	2108

StoreFront n'affiche pas les applications protégées lors de l'utilisation de versions antérieures de l'application Workspace, ou sur iOS, Android, ChromeOS, ou lors du lancement d'applications dans le navigateur à l'aide de l'application Citrix Workspace pour HTML5.

Pour autoriser StoreFront à afficher des applications protégées sur les versions de Workspace prises en charge, utilisez l'applet de commande du SDK PowerShell Set-STFWebReceiverAppProtection.

Si l'utilisateur a choisi de lancer des applications d'espace de travail via un navigateur (via une configuration administrateur ou parce qu'il a choisi d'utiliser **Workspace Lite**), App Protection n'est pas disponible. Vous pouvez configurer le magasin pour qu'il soit toujours lancé à l'aide de l'application Citrix Workspace installée localement. Consultez Déploiement de l'application Citrix Workspace.

StoreFront détermine la version de l'application Citrix Workspace à l'aide de l'extension Web Citrix Workspace si elle est disponible et configurée. Consultez Détection des clients basée sur une extension de navigateur. Sinon, StoreFront détermine la version de l'application Workspace dans le cadre de la détection du client lors de la première visite de l'utilisateur sur le site Web du magasin. Si l'utilisateur ignore la détection en choisissant **Déjà installé**, StoreFront n'est pas en mesure de déterminer la version de l'application et n'affiche donc pas les applications protégées. Il est donc recommandé de désactiver l'option **Déjà installé**, consultez Déploiement de l'application Citrix Workspace.

> **Avertissement**
>
> Si l'extension Web Citrix Workspace n'est pas disponible, StoreFront détermine la version de l'application Citrix Workspace la première fois que l'utilisateur accède au site Web. Si l'utilisateur installe ensuite une version différente de l'application Workspace, StoreFront ne sera pas averti de la modification et pourra donc autoriser ou interdire à tort le lancement d'applications protégées. Citrix recommande de configurer la vérification de l'état de la protection des applications qui bloque le lancement d'applications et de bureaux virtuels à partir de versions de l'application Citrix Workspace qui ne prennent pas en charge la protection des applications.

Supprimer un site Web

August 25, 2023

1. 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 cliquez sur **Gérer les sites Receiver pour Web** dans le panneau **Actions**.
2. Sélectionnez un site et cliquez sur **Supprimer**. Lorsque vous supprimez un site, les utilisateurs ne peuvent plus utiliser cette page Web pour accéder au magasin.

Configurer le site Web de l'application Workspace

August 25, 2023

Lorsque vous créez un nouveau magasin à l'aide de StoreFront, un site Web est créé automatiquement et associé au magasin. Lorsqu'un magasin possède plusieurs sites Web, sélectionnez le site Web qui s'affiche lorsque les utilisateurs accèdent au magasin à l'aide de l'application Citrix Workspace.

1. Sélectionnez le nœud **Magasins** dans le volet gauche de la console de gestion Citrix StoreFront.
2. Sélectionnez un magasin dans le volet central, 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 Web que vous souhaitez que les clients de l'application Citrix Workspace affichent lorsque les utilisateurs accèdent à ce magasin.
4. Cliquez sur **OK**.

Configurer des groupes de serveurs

April 17, 2024

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

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

Ajouter un serveur à un groupe de serveurs

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

votre déploiement StoreFront pour évaluer le nombre de serveurs dont vous avez besoin dans votre groupe.

Supprimer des serveurs d'un groupe de serveurs

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

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. Consultez 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\CitrixWorkspaceAppWe.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 Vérification des listes de révocation de certificats (CRL).

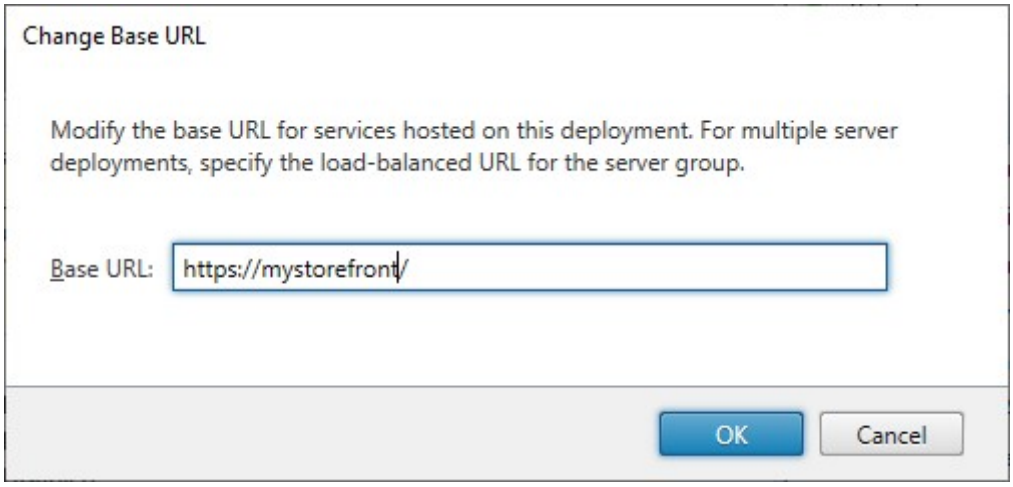
> **Remarque :**
>
> Les données d'abonnement sont synchronisées avec les autres serveurs indépendamment du mécanisme Propager les modifications. Cette opération se produit automatiquement sans que la tâche Propager les modifications soit lancée.

Modifier l'URL de base d'un déploiement

L'URL de base est 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.

Pour modifier l'URL de base :

1. Dans la console de gestion Citrix StoreFront, dans le panneau de gauche, sélectionnez le nœud **Groupe de serveurs**.
2. Dans le volet Actions, cliquez sur **Modifier l'URL de base…**
3. Entrez la nouvelle URL.
4. Sélectionnez **OK**.



Intégrer avec Citrix Gateway et NetScaler ADC

May 30, 2024

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

Tâche	Détails
Importer une appliance Citrix Gateway	Exporter la configuration depuis votre appliance Citrix Gateway et l'importer dans StoreFront
Gérer des appliances Citrix Gateway	Ajouter, supprimer et modifier les paramètres de connexion de Citrix Gateway
Équilibrage de charge avec NetScaler ADC	Configurer NetScaler ADC en tant qu'équilibreur de charge devant un groupe de serveurs StoreFront
Configurer NetScaler ADC et StoreFront pour l'authentification DFA	
Authentification à l'aide de domaines différents	Configurer StoreFront et Citrix Gateway afin que les utilisateurs s'authentifient d'abord auprès de la passerelle sur un domaine, puis auprès de StoreFront sur un autre domaine
Configurer des points balises	Configurer les URL de balises que l'application Citrix Workspace peut utiliser pour déterminer si elle se trouve à l'intérieur ou à l'extérieur de votre réseau d'entreprise
Créer un seul nom de domaine complet (FQDN) utilisé en interne et externe	Créer un nom de domaine complet (FQDN) unique qui peut accéder à un magasin directement depuis le réseau de votre entreprise et à distance via Citrix Gateway.

Configurer Citrix Gateway

February 22, 2024

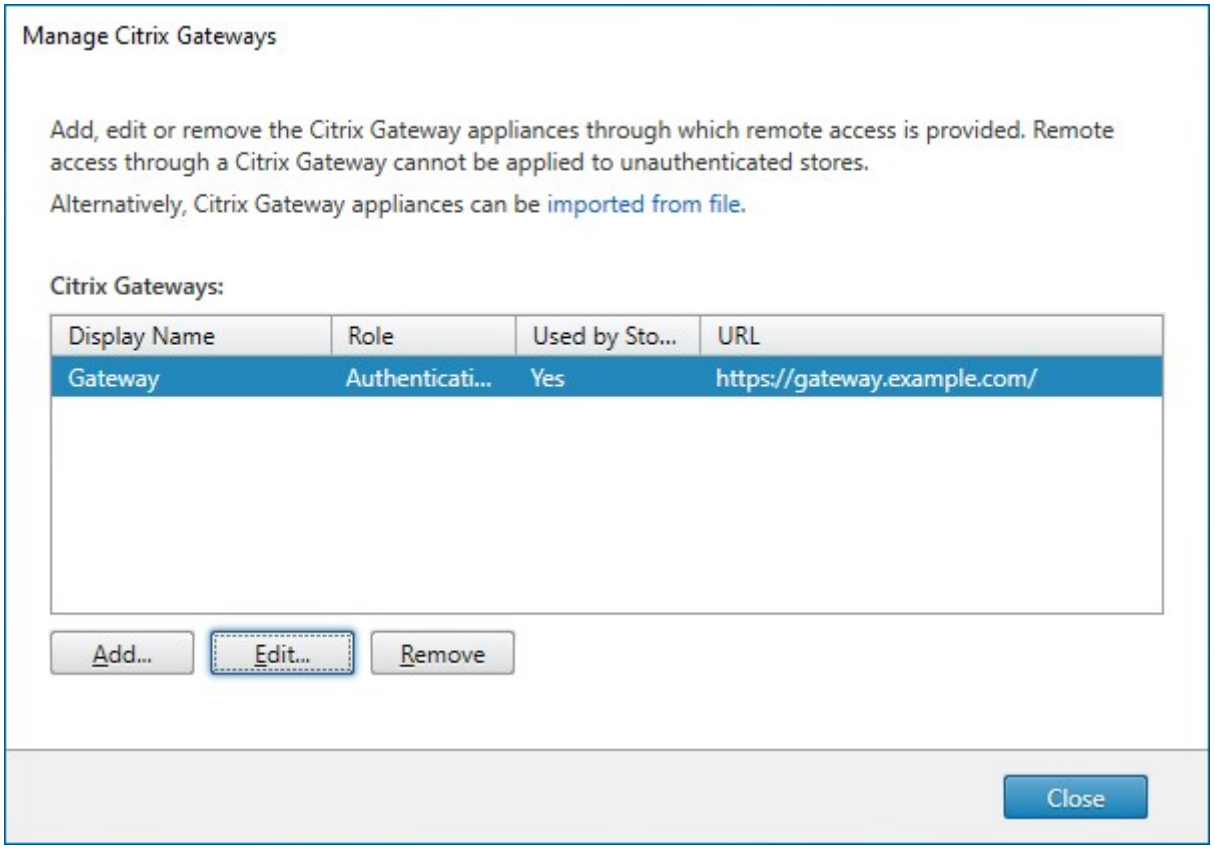
Utilisez Citrix Gateway pour fournir un accès à distance à StoreFront. Citrix Gateway s'exécute sur un matériel ou un logiciel NetScaler ADC ou une appliance NetScaler Gateway.

Pour plus d'informations sur la configuration de votre Gateway, consultez Intégrer NetScaler Gateway à StoreFront.

Vous devez configurer votre passerelle dans StoreFront pour que StoreFront autorise l'accès via cette passerelle.

Afficher les passerelles

Pour afficher les passerelles configurées dans StoreFront, sélectionnez le nœud Magasins dans le panneau gauche de la console de gestion Citrix StoreFront, puis cliquez sur **Gérer Citrix Gateway**. La fenêtre **Gérer Citrix Gateway** s'affiche.



PowerShell

Pour obtenir la liste des passerelles et leur configuration, appelez Get-STFRoamingGateway.

Ajouter Citrix Gateway

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

1. Dans la fenêtre **Gérer Citrix Gateway**, cliquez sur **Ajouter**.
2. Dans l'onglet Paramètres généraux, entrez les paramètres, puis sélectionnez **Suivant**.

   - Indiquez 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 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.

   - Entrez l'URL de la passerelle.

     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. La passerelle ajoute l'URL à l'en-tête HTTP `X-Citrix-Via`. StoreFront utilise cet en-tête pour déterminer quelle passerelle est utilisée.

     Dans l'interface graphique, il n'est possible d'ajouter qu'une seule URL de passerelle. Si plusieurs URL permettent d'accéder à une passerelle, vous devez ajouter deux fois la même passerelle avec une configuration identique à l'exception de l'URL. Pour simplifier la configuration, vous pouvez configurer une URL secondaire utilisée pour accéder à la passerelle. Cette option n'étant pas disponible dans l'interface graphique, vous devez la configurer à l'aide de PowerShell. Vous devez fermer la console de gestion avant d'exécuter des commandes PowerShell. Par exemple, si vous avez plusieurs passerelles derrière un équilibreur de charge de serveur global, il est généralement utile d'ajouter à la fois l'URL GSLB et une URL qui peut être utilisée pour accéder à chaque passerelle régionale spécifique, par exemple à des fins de test ou de résolution de problèmes. Une fois que vous avez créé la passerelle, vous pouvez ajouter une URL supplémentaire à l'aide de `Set-STFRoamingGateway`, en utilisant le paramètre `-GSLBurl` de l'URL secondaire. Bien que le paramètre soit appelé `GSLBurl`, il peut être utilisé dans toutes les situations où vous souhaitez ajouter une deuxième URL. Par exemple :

     ```
     1  Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl "
           eugateway.example.com" -GatewayUrl "gslb.example.com"
     2  <!--NeedCopy-->
     ```

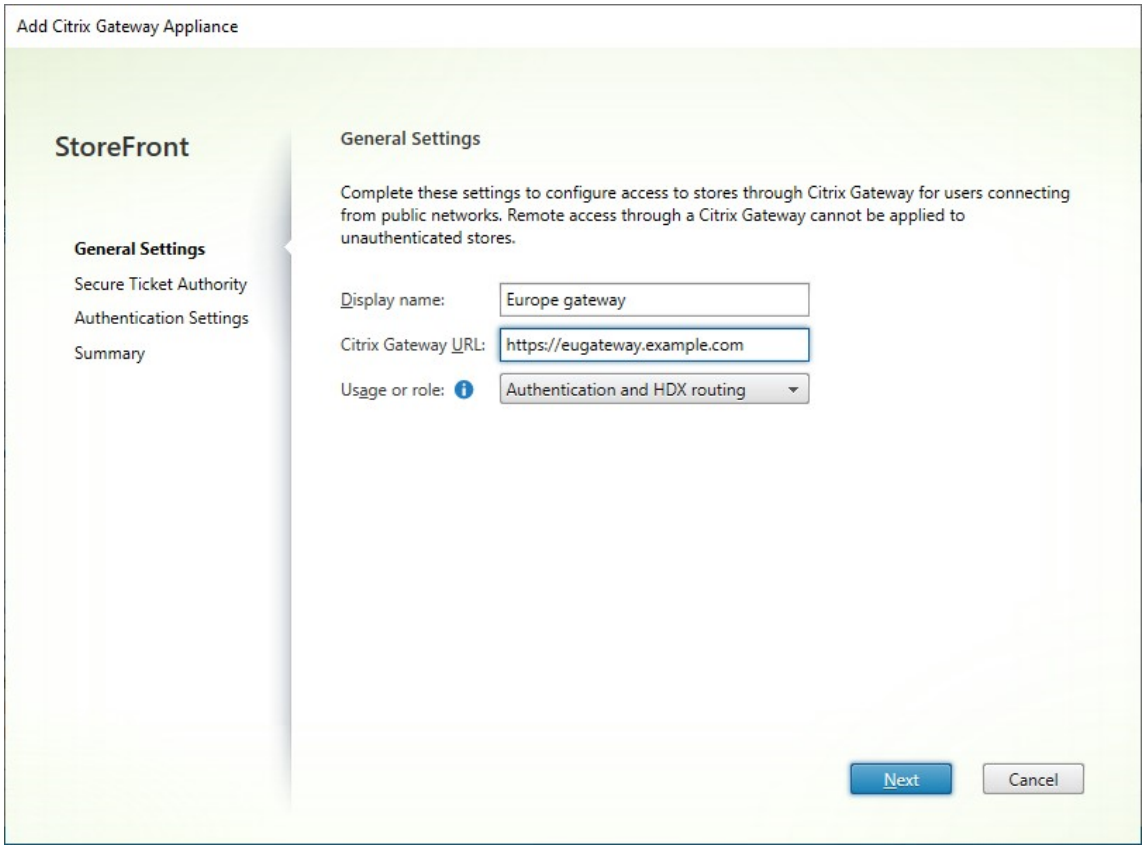
     > Remarque :
     >
     > Contre toute attente, dans cet exemple, le paramètre `GSLBurl` contient l'URL régionale alors que le paramètre `GatewayUrl` contient l'URL GSLB. Dans la plupart

> des cas, les URL sont traitées de la même manière et, si le magasin n'est accessible que via un navigateur Web, elles peuvent être configurées d'une façon ou d'une autre. Toutefois, lors de l'accès à StoreFront via l'application Citrix Workspace, il lit le contenu `GatewayUrl` de StoreFront et l'utilise ensuite pour un accès distant. Il est préférable de le configurer pour toujours se connecter à l'URL GSLB.

Si vous avez besoin de plus de deux URL, vous devrez les configurer en tant que passerelle distincte.

- Sélectionnez l'utilisation ou le rôle :

Utilisation ou rôle	Description
Authentification et routage HDX	Utilisez la passerelle à la fois pour fournir un accès distant à StoreFront et pour accéder aux VDA.
Authentification uniquement	Sélectionnez cette option si la passerelle est utilisée uniquement pour l'accès à distance à StoreFront.
Routage HDX uniquement	Sélectionnez cette option si la passerelle est utilisée uniquement pour fournir un accès HDX aux VDA, par exemple sur un site ne disposant pas d'instance StoreFront.



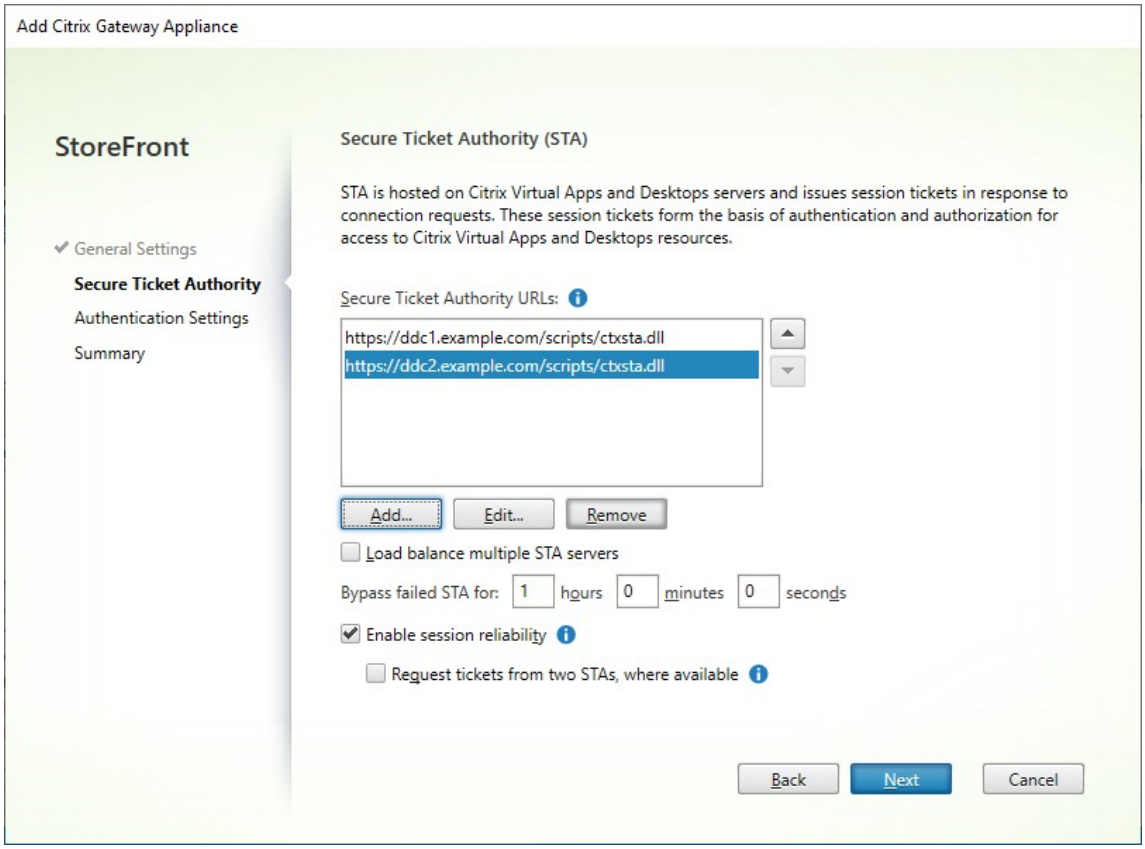
3. Renseignez les paramètres dans l'onglet **Secure Ticketing Authority**.

   Secure Ticketing Authority 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.

   - Entrez au moins une URL de serveur Secure Ticket Authority. Si vous utilisez Citrix Virtual Apps and Desktops, vous pouvez utiliser le Delivery Controller comme STA. Si vous utilisez Citrix Desktop as a Service, vous pouvez accéder aux Cloud Connector qui envoient des requêtes par proxy au service STA de Citrix Cloud. Les entrées de cette liste doivent correspondre exactement à la liste configurée dans Citrix Gateway.
   - Cochez la case **Équilibrer la charge des serveurs multiples** pour répartir les demandes entre les serveurs STA. Si cette case n'est pas cochée, StoreFront essaiera les serveurs dans l'ordre dans lequel ils sont répertoriés.
   - Si StoreFront ne parvient pas à accéder à un serveur STA, il évite d'utiliser ce serveur pendant un certain temps. Par défaut, il s'agit d'une heure, mais vous pouvez personnaliser cette valeur.
   - 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 con-

figuré 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.



Une fois que vous avez terminé de remplir les paramètres, sélectionnez **Suivant**.

4. Renseignez les paramètres dans l'onglet **Paramètres d'authentification**.

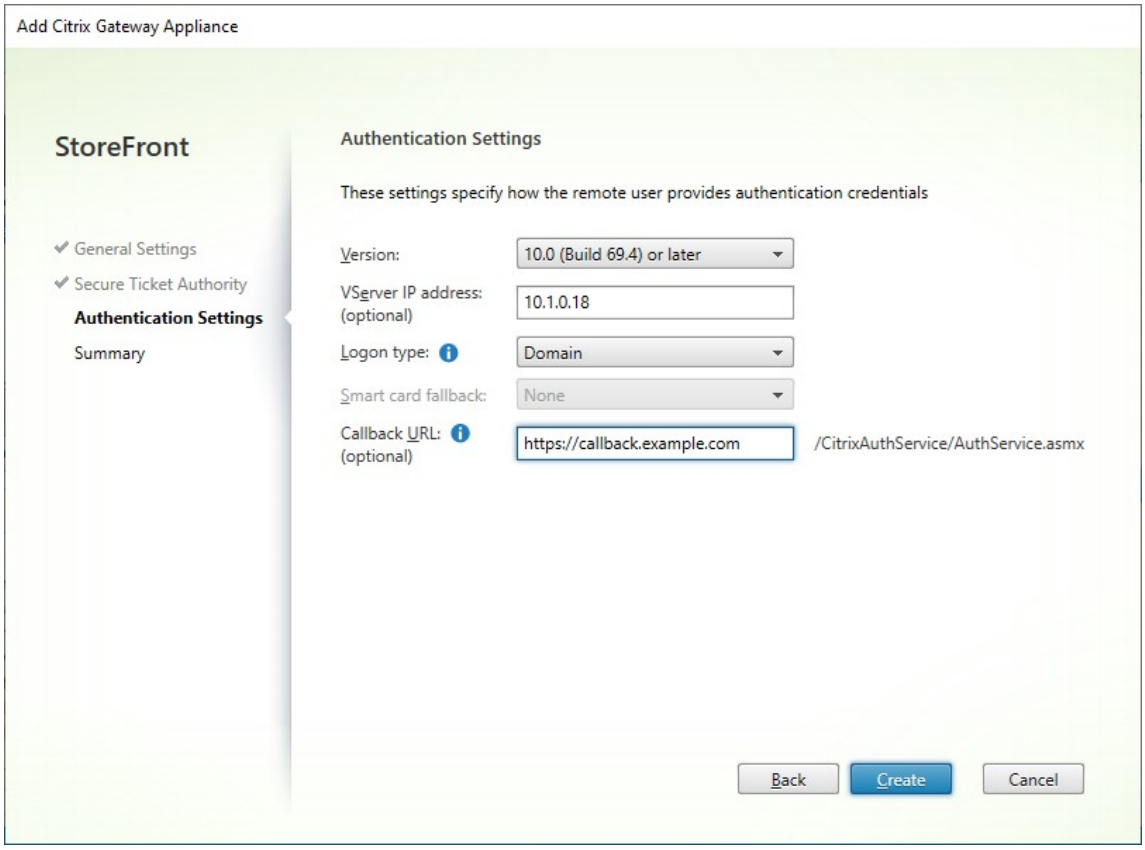
   - Choisissez la version de NetScaler.
   - S'il existe plusieurs passerelles avec la même URL (généralement lors de l'utilisation d'un équilibreur de charge de serveur global) et que vous avez saisi une URL de rappel, vous devez saisir l'adresse IP virtuelle de la passerelle. Cela permet à StoreFront de déterminer de quelle passerelle provenait la demande et, par conséquent, quel serveur contacter à l'aide de l'URL de rappel. Sinon, vous pouvez laisser ce champ vide.
   - Sélectionnez dans la liste **Type d'ouverture de session** la méthode d'authentification que vous avez configurée sur le boîtier 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.

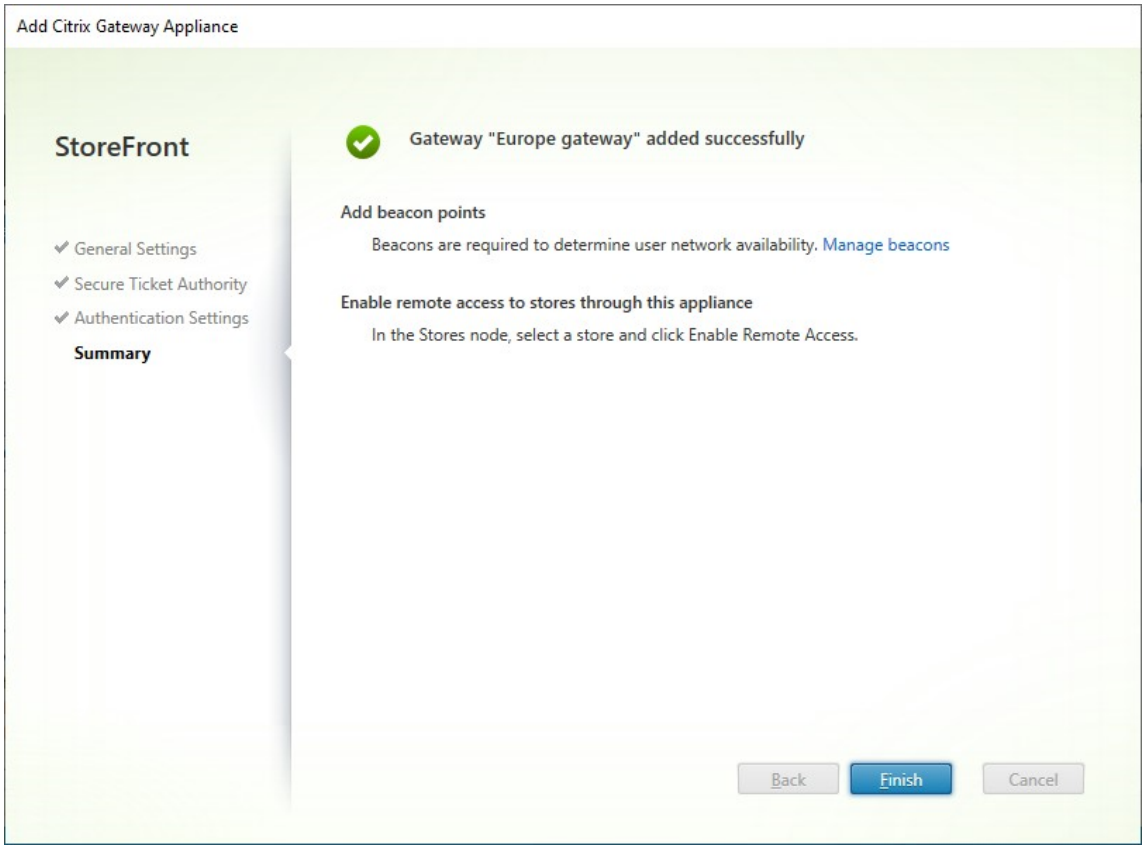
Si vous configurez l'authentification avec carte à puce avec une méthode d'authentification secondaire sur laquelle les utilisateurs peuvent se rabattre s'ils rencontrent des problèmes avec leur carte à puce, sélectionnez la méthode d'authentification secondaire dans la liste Carte à puce de remplacement.

- Entrez éventuellement l'URL accessible en interne de la passerelle dans la zone URL de rappel. Cela permet à StoreFront de contacter le service d'authentification Citrix Gateway pour vérifier que les requêtes reçues de Citrix Gateway proviennent de cette appliance. Elle est requise pour l'accès intelligent et pour les scénarios d'authentification sans mot de passe tels que la carte à puce ou le SAML, sinon vous pouvez laisser ce champ vide. Si vous avez plusieurs appliances Citrix Gateway avec la même URL, cette URL doit correspondre au serveur de passerelle spécifique.



Une fois que vous avez terminé de remplir les paramètres, sélectionnez **Suivant**.

5. Cliquez sur **Créer** pour appliquer la configuration.



6. Une fois le déploiement appliqué, cliquez sur **Terminer**.
7. Pour permettre aux utilisateurs d'accéder à vos magasins via Gateway, configurez l'accès à distance des utilisateurs.

SDK PowerShell

Pour ajouter une passerelle à l'aide du SDK PowerShell, appelez l'applet de commande New-STFRoamingGateway.

Modifier Citrix Gateway

1. Dans la fenêtre **Gérer Citrix Gateway**, cliquez sur la passerelle que vous souhaitez modifier et sélectionnez **Modifier**.

   Pour obtenir une description des paramètres, consultez Ajouter Citrix Gateway.
2. Sélectionnez **Enregistrer** pour enregistrer vos modifications.

SDK PowerShell

Pour modifier la configuration de la passerelle à l'aide du SDK PowerShell, appelez l'applet de commande Set-STFRoamingGateway.

Supprimer Citrix Gateway

1. Dans la fenêtre **Gérer Citrix Gateway**, cliquez sur la passerelle que vous souhaitez modifier et sélectionnez **Supprimer**.
2. Dans la fenêtre de confirmation, sélectionnez **Oui**.

SDK PowerShell

Pour supprimer la passerelle à l'aide du SDK PowerShell, appelez Remove-STFRoamingGateway.

Importer une appliance Citrix Gateway

February 22, 2024

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 Gateway peuvent uniquement exporter les vServers de passerelle créés à l'aide de l'assistant Citrix Virtual Apps and Desktops.

- Le DNS doit pouvoir être résolu et StoreFront doit pouvoir contacter toutes les adresses URL de serveurs STA (Secure Ticket Authority) du fichier GatewayConfig.json dans le fichier ZIP généré par Citrix Gateway.

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

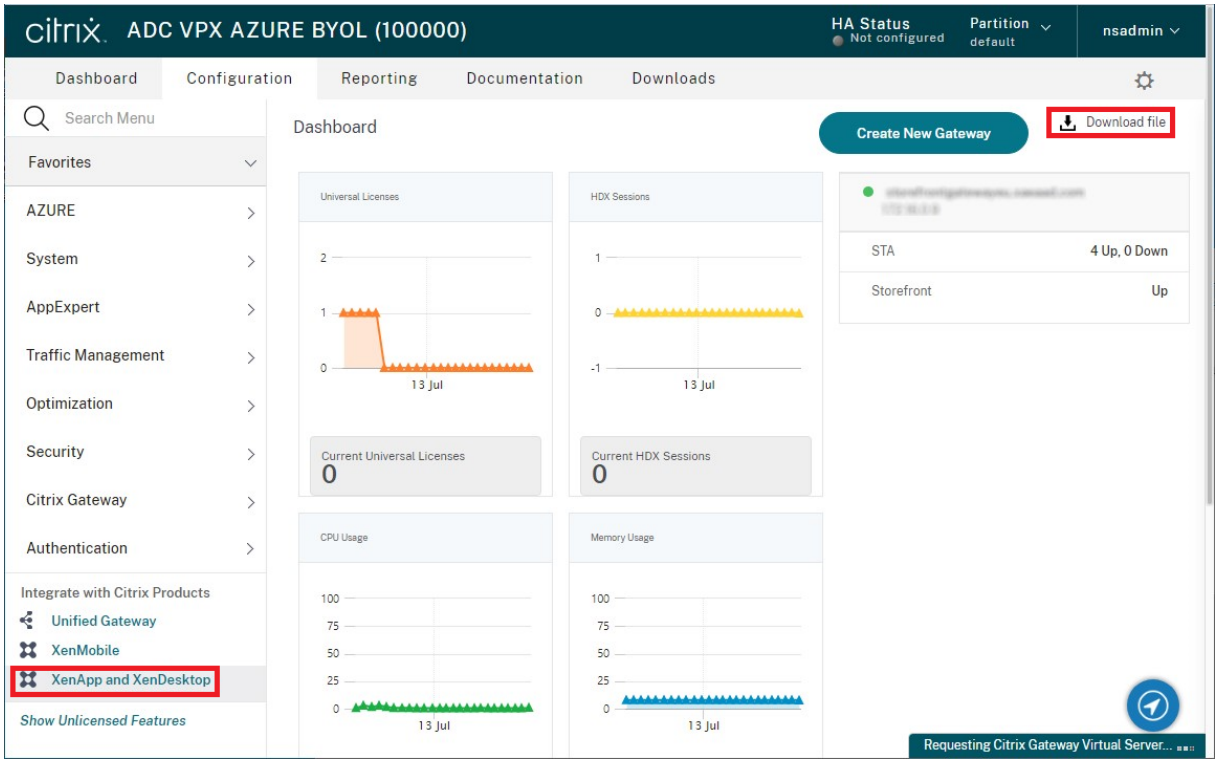
  L'URL de rappel et de la combinaison de ports que vous utilisez sont généralement les mêmes que l'adresse URL et la combinaison de ports de la passerelle, à condition que StoreFront puisse résoudre cette adresse URL.

  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.

Exporter la configuration depuis Citrix Gateway

1. Connectez-vous à Citrix Gateway.
2. Accédez à l'onglet Configuration.
3. Sous « Integrate with Citrix Products », cliquez sur XenApp et XenDesktop.
4. En haut à droite, cliquez sur « Download file ».



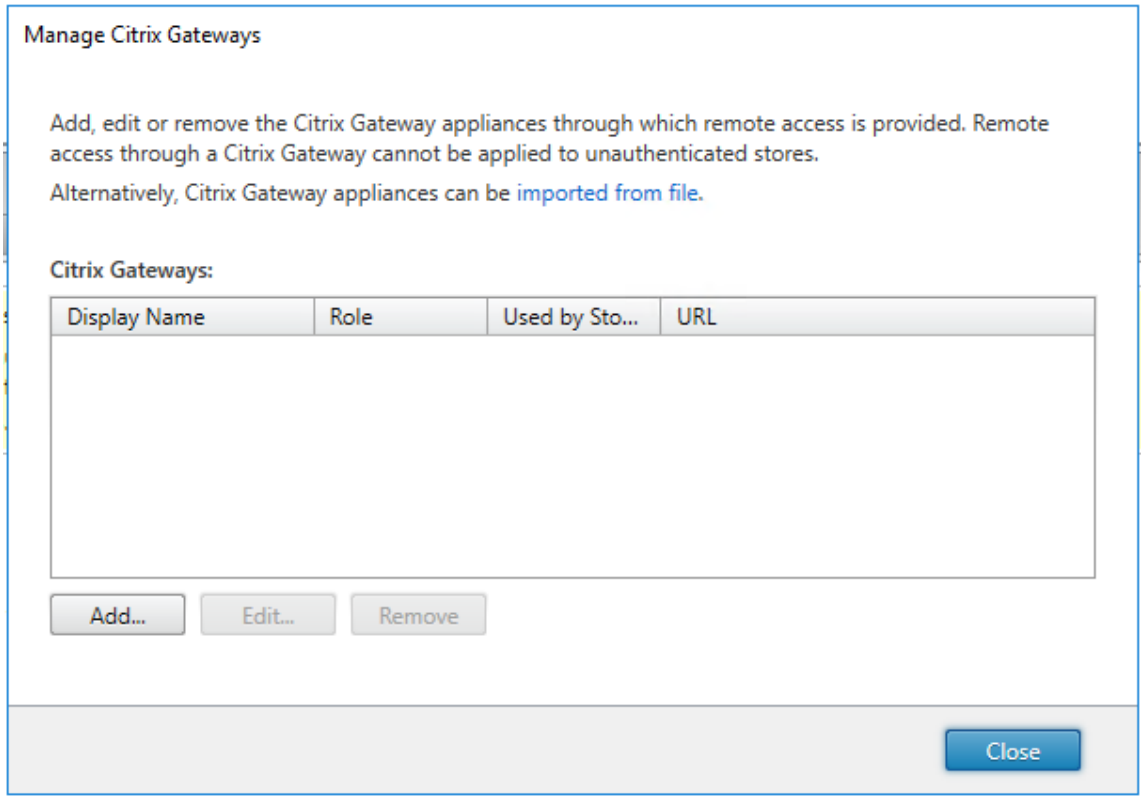
1. Choisissez si vous souhaitez télécharger la configuration de toutes les passerelles ou d'une passerelle spécifique.

Importer une appliance Citrix Gateway à l'aide de la console

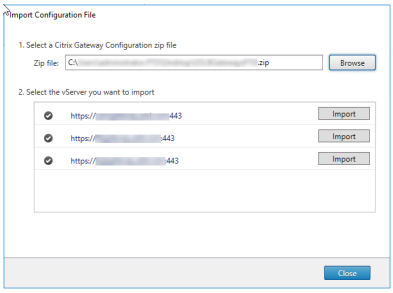
Vous pouvez importer une ou plusieurs configurations de serveur virtuel Citrix Gateway à l'aide du même fichier d'importation. Si vous disposez de plusieurs serveurs virtuels de passerelle provenant de différentes appliances Citrix Gateway, vous devez utiliser plusieurs fichiers d'importation.

> 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**.



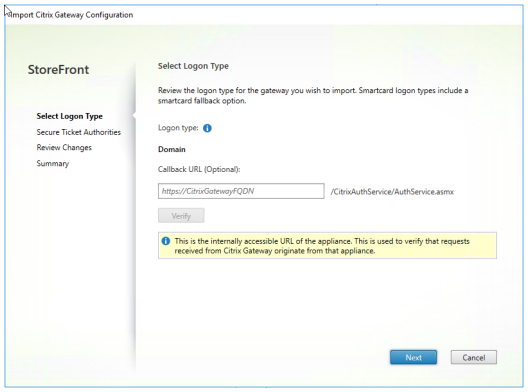
3. Accédez au fichier de configuration du serveur virtuel Citrix Gateway.
4. Une liste des vServers de passerelle du fichier ZIP sélectionné s'affiche. Sélectionnez le vServer de passerelle que vous souhaitez importer et cliquez sur **Importer**. Si vous répétez l'importation d'un vServer, le bouton 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 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.

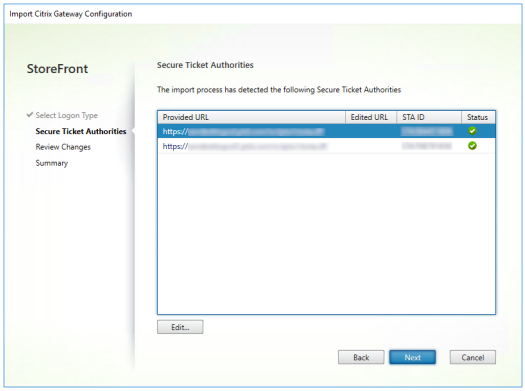


Type de connexion dans la console	LogonType dans le fichier JSON	URL de rappel requise
Domaine	Domaine	Non
Domaine et jeton de sécurité	DomainAndRSA	Non
Jeton de sécurité	RSA	Oui
Carte à puce - Sans solution alternative	SmartCard	Oui
Carte à puce - Domaine	SmartCardDomain	Oui
Carte à puce - Domaine et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

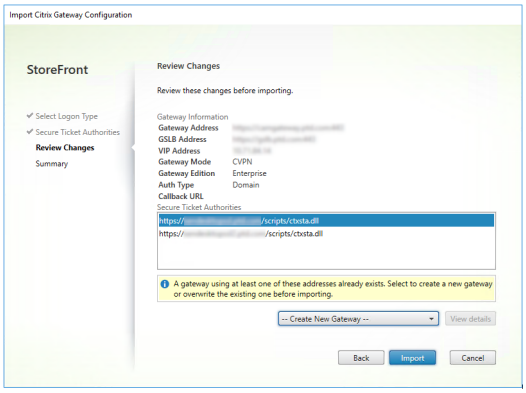
Si une URL de rappel est requise, StoreFront remplira automatiquement l'adresse URL de rappel en fonction de l'adresse URL de passerelle trouvée dans le fichier ZIP. Vous pouvez modifier cette adresse au profit de toute adresse URL valide qui pointe vers l'adresse IP virtuelle de Citrix Gateway. Pour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

Pour utiliser Smart Access ou l'authentification sans mot de passe, 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

Paramètre de passerelle	Peut être mis à jour
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"
<!--NeedCopy-->
```

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 }

GatewayAuthType         :SmartCard
GatewayEdition          : Enterprise
```



```
ReceiverForWebSites     : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }

<!--NeedCopy-->
```

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.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

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.

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -Confirm:$False
<!--NeedCopy-->
```

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.

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

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False

```



```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
<!--NeedCopy-->
```

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.

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

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
<!--NeedCopy-->
```

Équilibrage de charge avec NetScaler ADC

April 17, 2024

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 NetScaler ADC pour équilibrer la charge des requêtes entrantes de l'application Citrix Workspace et des navigateurs Web entre les serveurs StoreFront du groupe de serveurs.

Certificat de serveur requis pour le déploiement avec charge équilibrée

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 serveur virtuel d'équilibrage de charge de l'appliance NetScaler 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 serveur virtuel d'équilibrage de charge de l'appliance NetScaler 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.

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 NetScaler ADC.

Exemple : `storefront.example.com` se résout sur l'adresse IP virtuelle (VIP) du serveur virtuel d'équilibrage de charge.

Configurer des serveurs StoreFront

Tous les serveurs StoreFront entre lesquels vous souhaitez effectuer l'équilibrage de charge doivent être configurés dans le cadre d'un groupe de serveurs StoreFront qui synchronise la configuration entre les serveurs pour garantir qu'ils sont configurés de manière identique. Pour plus de détails sur l'ajout de serveurs à un groupe de serveurs, voir Joindre un groupe de serveurs existant.

Chaque serveur doit être configuré pour le protocole HTTPS afin que la communication entre l'équilibreur de charge et les serveurs StoreFront soit chiffrée. Consultez la section Sécurisation de StoreFront avec HTTPS. Le certificat doit contenir le nom de domaine complet (FQDN) avec équilibrage de charge en tant que nom courant (CN) ou nom de sujet alternatif (SAN).

Définissez l'URL de base du groupe de serveurs comme étant l'URL de l'équilibreur de charge. Pour modifier l'URL de base, dans la console de gestion Citrix StoreFront, dans le volet gauche, cliquez avec le bouton droit de la souris sur **Groupe de serveurs**, puis sur **Modifier l'URL de base**. Entrez l'URL du serveur virtuel d'équilibrage de charge.

Configurer Citrix Service Monitor pour HTTPS (facultatif)

L'installation de StoreFront inclut le service Windows **Citrix Service Monitor**. Ce service ne dépend d'aucun autre service et surveille l'état des services StoreFront critiques. Cela permet à NetScaler ADC

et à d'autres applications tierces de surveiller l'état relatif du déploiement d'un serveur StoreFront.

Par défaut, le moniteur utilise le protocole HTTP sur le port 8000. Vous pouvez éventuellement le modifier pour utiliser le protocole HTTPS sur 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
<!--NeedCopy-->
```

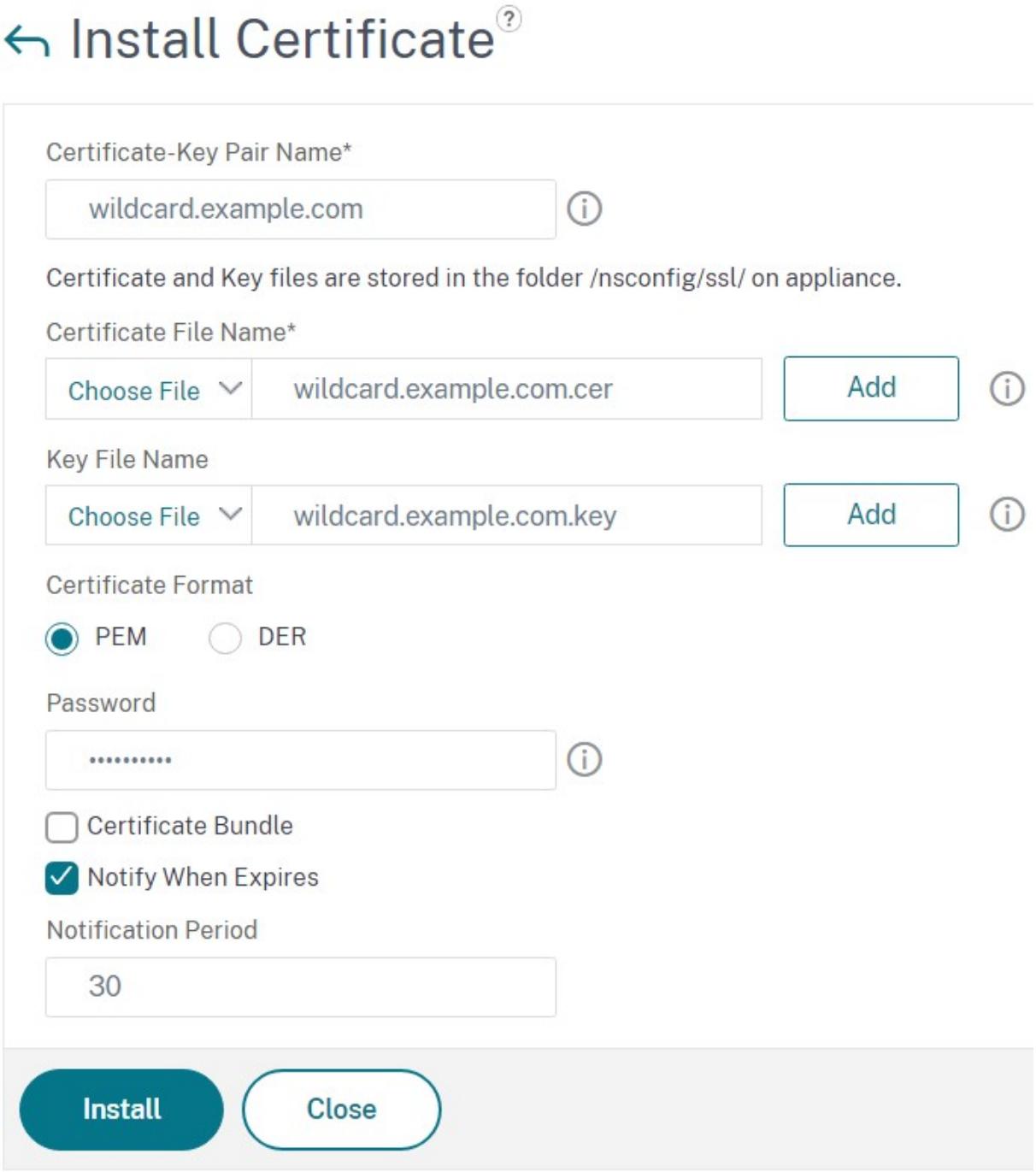
2. Une fois ce processus terminé, propagez les modifications à tous les autres serveurs du groupe de serveurs StoreFront.
3. Pour effectuer un test rapide sur le moniteur, entrez l'adresse URL suivante dans le navigateur sur le serveur StoreFront ou toute autre machine avec accès réseau au serveur StoreFront.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

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

Configurer l'équilibreur de charge dans NetScaler

Configurer le certificat de serveur sur NetScaler ADC

1. Ouvrez une session sur la console de gestion de l'appliance NetScaler ADC.
2. Sélectionnez **Traffic Management > SSL > Certificates > Server Certificates** (Gestion du trafic > SSL > Certificats > Certificats de serveur).
3. Cliquez sur **Installer**.
4. Sur la page **Install Server Certificate** (Installer le certificat du serveur), entrez un nom de paire de clés de certificat, cliquez sur **Choose File** (Choisir un fichier) et recherchez le fichier de certificat. Si le fichier de certificat n'inclut pas la clé privée, vous devez également sélectionner un **fichier clé**.

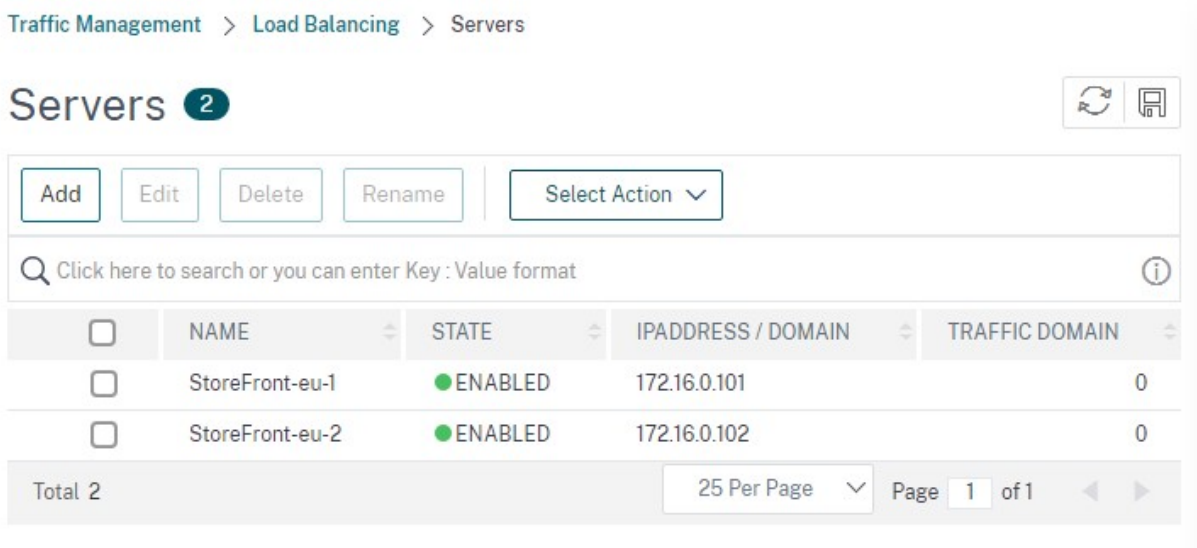


Ajouter des nœuds de serveur StoreFront individuels à l'équilibrage de charge de l'appliance NetScaler ADC

1. Accédez à **Traffic Management > Load Balancing > Servers**. Cliquez sur **Add** et ajoutez chacun des serveurs StoreFront à inclure dans l'équilibrage de charge.

   Exemple = 2 serveurs StoreFront nommés StoreFront-eu-1 et StoreFront-eu-2

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



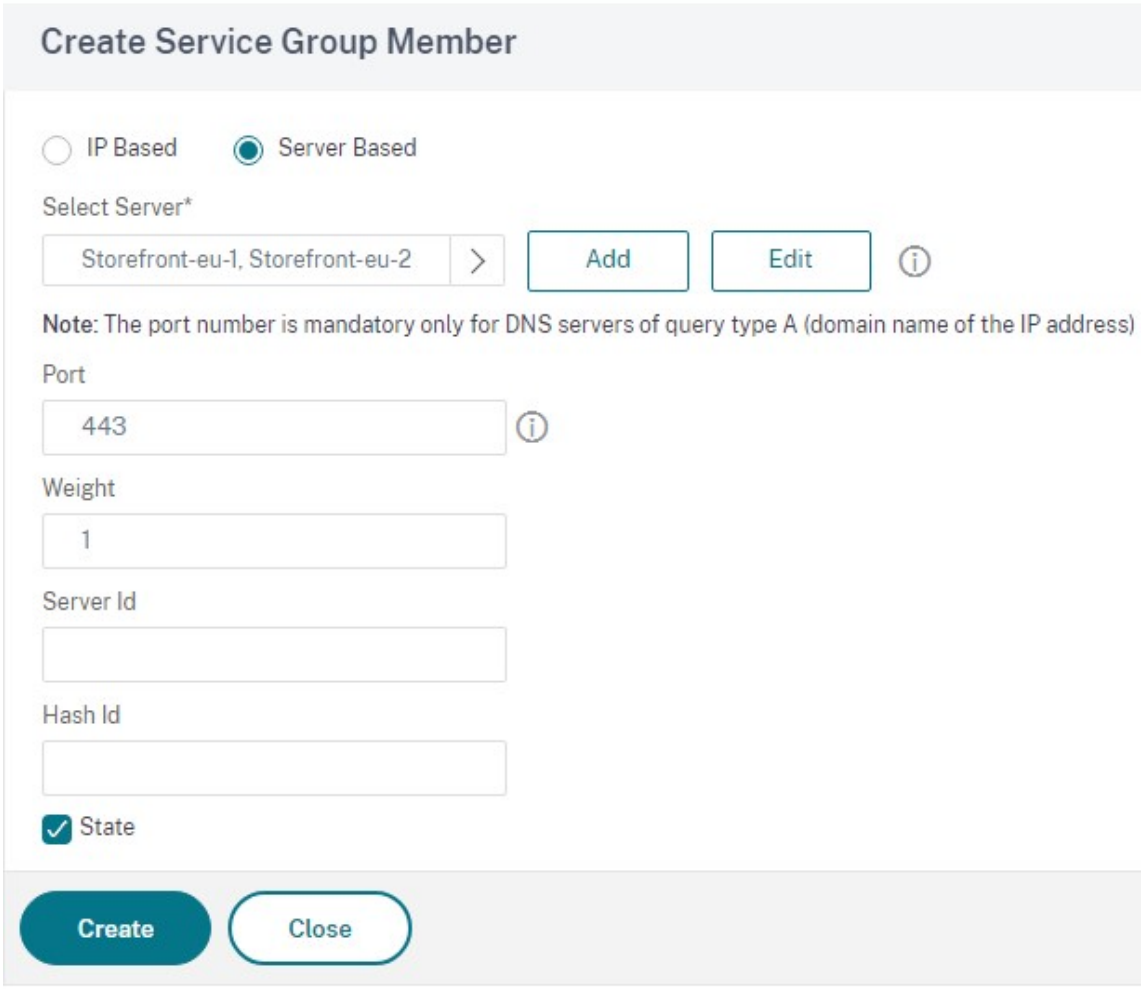
Définir un moniteur StoreFront pour vérifier l'état de tous les nœuds StoreFront dans le groupe de serveurs

1. Ouvrez une session sur la console de gestion de NetScaler 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. Si vous avez configuré votre moniteur StoreFront pour HTTPS, assurez-vous que l'option **Secure** est sélectionnée. Sinon, laissez cette option désélectionnée et entrez le port 8000.
5. Sélectionnez l'option **Check 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 :

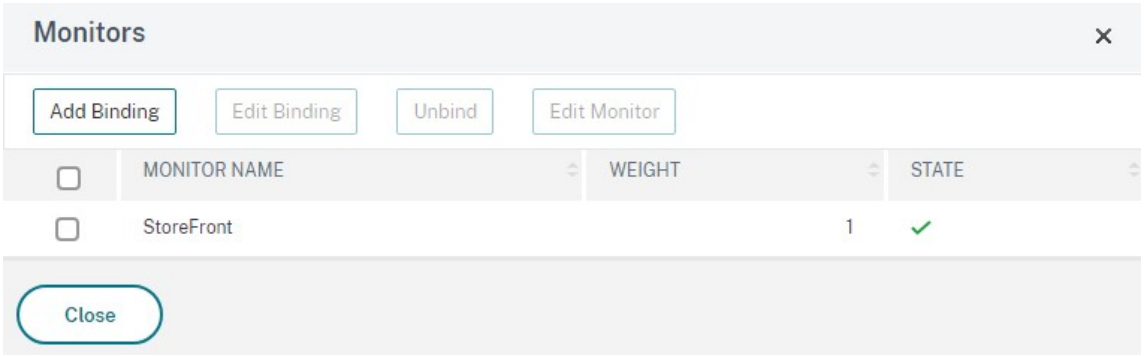
   - W3SVC (IIS)
   - WAS (Service d'activation des processus Windows)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

Créer un groupe de services contenant tous les serveurs StoreFront

1. Accédez à **Traffic Management > Load Balancing > Service Groups**. Sélectionnez **Add**. Pour vous connecter aux serveurs StoreFront via HTTPS, sélectionnez un protocole SSL. Conservez les autres paramètres par défaut. Sélectionnez **OK**.
2. Au sein de votre groupe de services, sous **Service Group Members**, cliquez sur **No Service Group Member**.
   a) Cliquez sur **Service Based**.
   b) Sélectionnez tous les serveurs que vous avez définis précédemment.
   c) Pour utiliser le protocole SSL entre l'équilibreur de charge et le serveur StoreFront, entrez le port 443. Sinon, entrez le port 80.

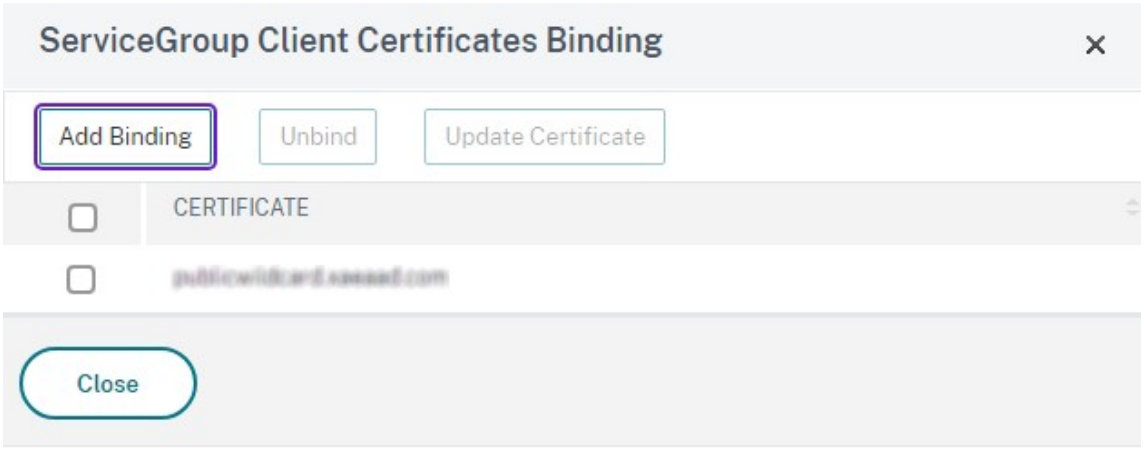


3. Ajoutez la section **Monitors** et sélectionnez le moniteur StoreFront que vous avez créé précédemment.



4. Ajoutez la section **Certificates**.

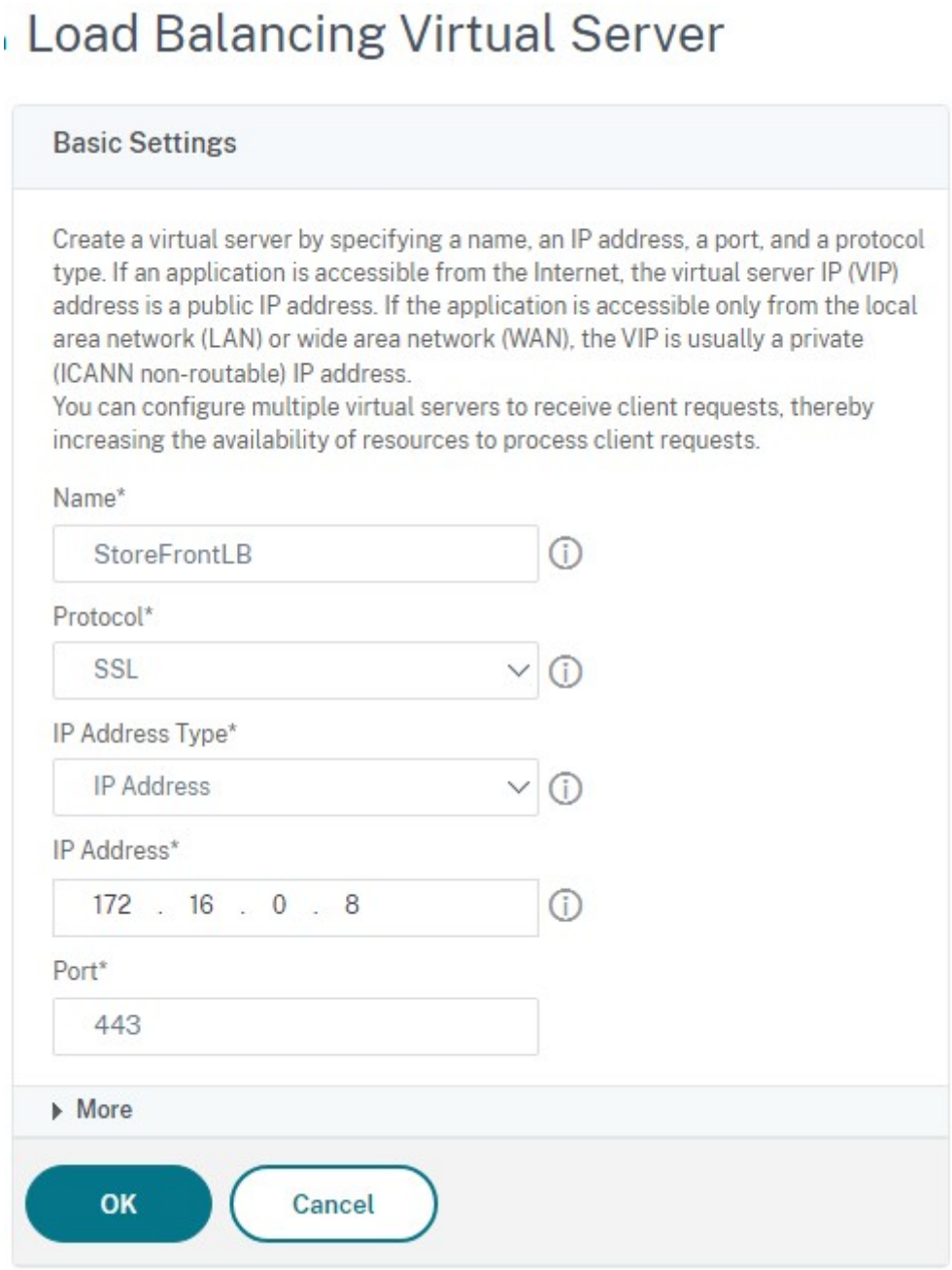
   a) Liez le certificat client.
   b) Liez le certificat CA utilisé pour signer le certificat de serveur que vous avez importé précédemment et les autres autorités de certification faisant partie de la chaîne de confiance PKI.



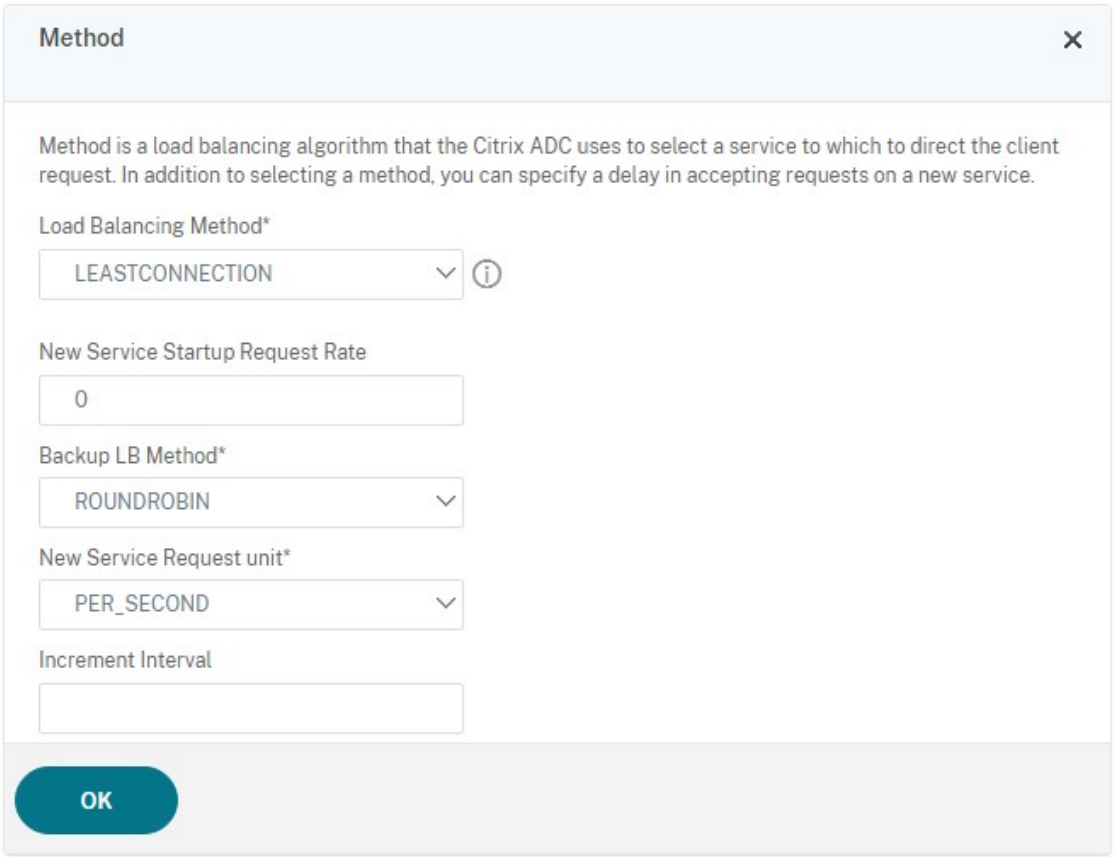
5. Ajoutez la section **Settings**. Sélectionnez **Settings** et entrez le nom d'en-tête **X-Forwarded-For**. Cela permet d'utiliser l'adresse IP du client dans les stratégies Citrix Virtual Apps and Desktops.

Créer un serveur virtuel d'équilibrage de charge pour le trafic utilisateur

1. Ouvrez une session sur la console de gestion de l'appliance NetScaler ADC.
2. Sélectionnez **Traffic Management > Load Balancing > Virtual Servers > Add** pour créer un nouveau serveur virtuel.
3. Entrez un nom, choisissez un protocole SSL et entrez le **port**. Cliquez sur OK pour créer le serveur virtuel.



4. Liez le **groupe de services** que vous avez créé précédemment au serveur virtuel d'équilibrage de charge.
5. Liez le même serveur et le même certificat CA que vous avez précédemment liés au groupe de services.
6. Ajoutez la section **Method** et sélectionnez la méthode d'équilibrage de charge. Les options courantes pour l'équilibrage de charge StoreFront sont **round robin** ou **least connection**.



7. Ajoutez la section **Persistance**.

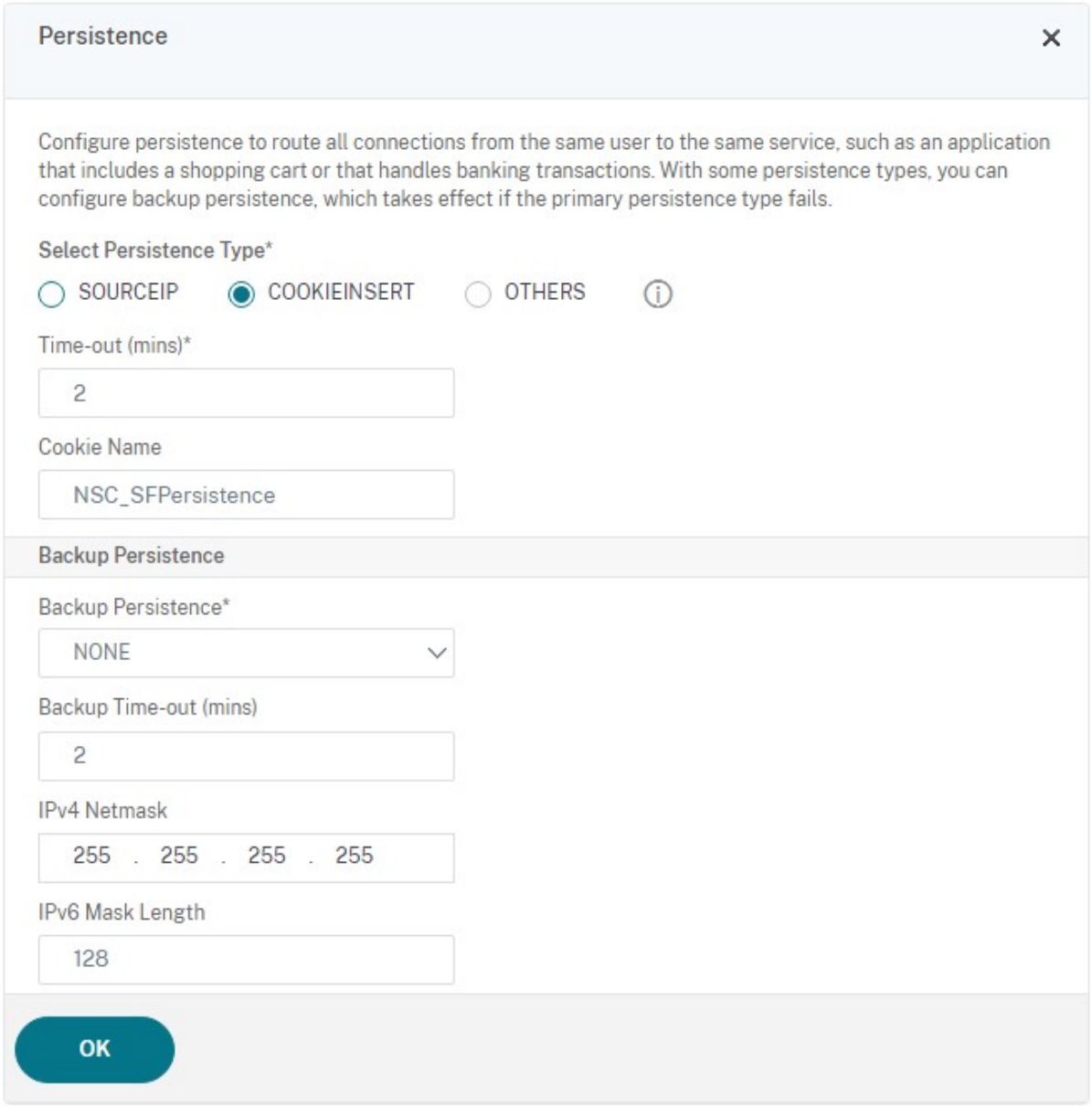
   a) Définissez la méthode de persistance sur **COOKIEINSERT**.

   b) Définissez le délai d'expiration de manière à ce qu'il soit identique au délai d'expiration de session dans StoreFront, qui est par défaut de 20 minutes.

   c) Attribuez un nom au cookie. Par exemple, **NSC_SFPersistence**, car cela facilite l'identification lors du débogage.

   d) Définissez la persistance de sauvegarde sur **NONE**.

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

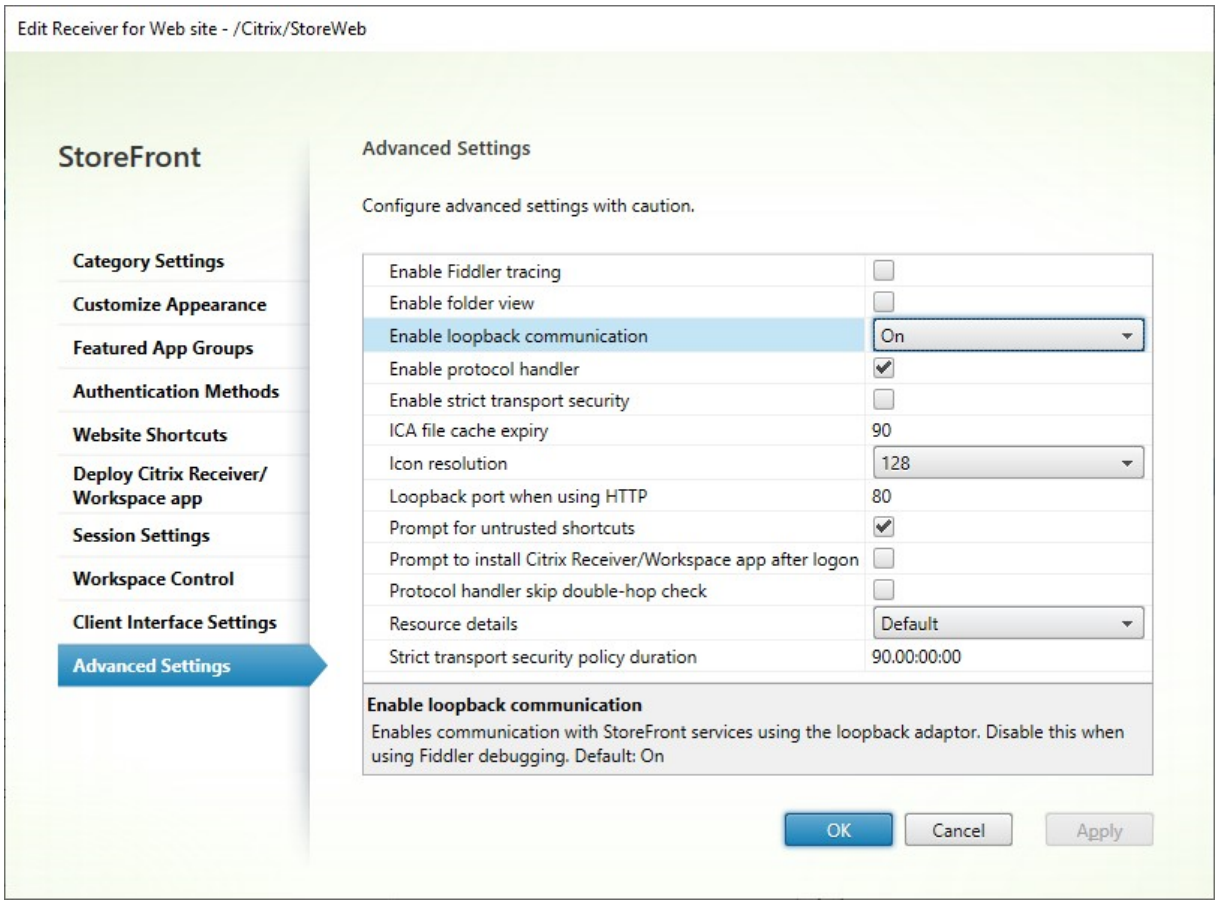


Configurer le bouclage StoreFront

Lorsque l'adresse de base est un équilibreur de charge, pour la communication interne entre les services StoreFront, cela peut entraîner l'acheminement du trafic vers l'équilibreur de charge et potentiellement vers un autre serveur. Cela se traduit par des performances médiocres et un comportement inattendu. Utilisez le paramètre StoreFront **Activer la communication en boucle** pour éviter ces problèmes. Par défaut, ce paramètre est défini sur **On**, ce qui signifie qu'il remplace la partie hôte de l'adresse de service par l'adresse IP de bouclage 127.0.0.1, tout en conservant le schéma (HTTP ou HTTPS) tel quel. 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.

Si vous utilisez un équilibrage de charge d'arrêt SSL et que ce dernier communique avec StoreFront via HTTP (non recommandé), il est nécessaire de configurer la communication en boucle de StoreFront sur **OnUsingHttp**, ce qui signifie que StoreFront modifiera également le schéma de HTTPS sur HTTP.

1. Ouvrez Citrix StoreFront.
2. Pour chaque magasin, accédez à **Gérer les sites Receiver pour Web**. Pour chaque site Web, accédez à **Configurer**.
3. Accéder aux **paramètres avancés**.
4. Modifiez le paramètre **Activer la communication en boucle** sur **OnUsingHttp**.



Si vous utilisez un équilibrage de charge d'arrêt SSL et que ce dernier communique avec StoreFront via HTTP (non recommandé), il est nécessaire de configurer la communication en boucle de StoreFront sur **OnUsingHttp**, ce qui signifie que StoreFront modifiera également le schéma de HTTPS sur HTTP.

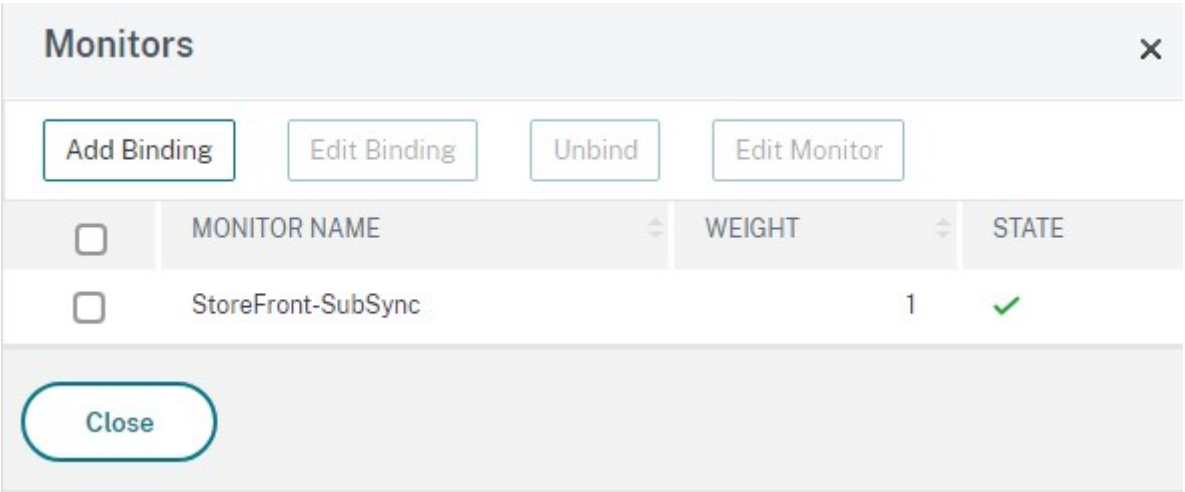
Configurer l'équilibreur de charge NetScaler ADC pour la synchronisation des abonnements entre groupes de serveurs

Si vous disposez d'un déploiement multisite composé de deux groupes de serveurs StoreFront ou plus, vous pouvez répliquer les données d'abonnement entre eux à l'aide d'une stratégie « pull » selon un calendrier récurrent. La réplication d'abonnement StoreFront utilise le port TCP 808, donc l'utilisation d'un serveur virtuel 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 serveur virtuel sur chaque appliance NetScaler ADC de votre déploiement pour équilibrer la charge du port TCP 808 pour chacun des groupes de serveurs StoreFront.

Configurez un groupe de services pour la synchronisation d'abonnement

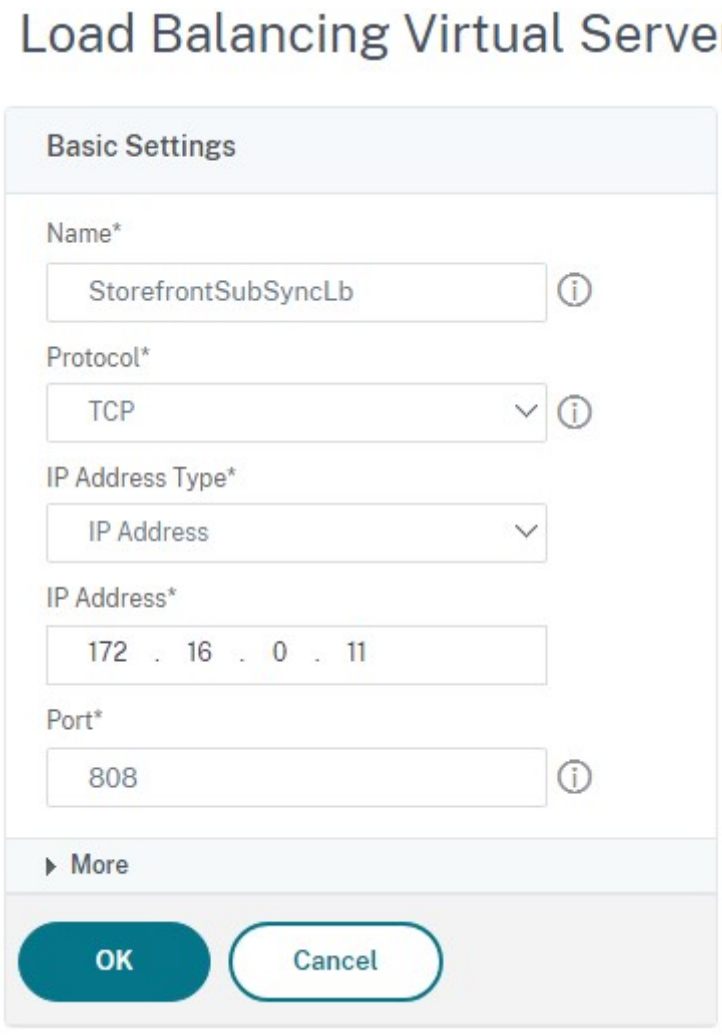
1. Ouvrez une session sur la console de gestion de l'appliance NetScaler ADC.
2. Sélectionnez **Traffic Management > Load Balancing > Service Groups > Add**.
3. Entrez un nom de groupe de services, changez le protocole sur **TCP** et cliquez sur **OK** pour enregistrer.
4. Dans la section **Service Group Members**, ajoutez tous les nœuds de serveur StoreFront que vous avez définis précédemment dans la section Servers et spécifiez le **port 808**.
5. Ajoutez la section **Monitors**.

    a) Cliquez sur **No Service Group to Monitor Binding**.
    b) Cliquez sur Ajouter. Entrez le **nom** du moniteur et définissez son **type** sur **TCP**. Cliquez sur **Créer**.
    c) Cliquez sur **Bind**.



Créer un serveur virtuel d'équilibrage de charge pour la synchronisation des abonnements

1. Ouvrez une session sur la console de gestion de l'appliance NetScaler ADC.
2. Sélectionnez **Traffic Management> Load Balancing > Virtual Servers > Add** et ajoutez un nouveau groupe de services.
3. Entrez un **nom**.
4. Définissez le protocole sur **TCP**.
5. Entrez une adresse IP.
6. Entrez **le port 808**.



7. Cliquez sur **OK**.
8. Cliquez sur **No Load Balancing Virtual Server ServiceGroup Binding**, sélectionnez le groupe de services que vous avez créé précédemment et cliquez sur **Bind**.
9. Ajoutez la section **Method** et définissez **Load Balancing Method** sur **ROUNDROBIN**.

10. Cliquez sur **Terminé** pour terminer vos modifications.

Configurer StoreFront pour extraire les données d'abonnement via un équilibreur de charge

Consultez Configurer la synchronisation des abonnements.

Lors de la configuration du planning de réplication, spécifiez une adresse de groupe de serveur qui correspond à l'adresse IP virtuelle d'équilibrage de charge du serveur virtuel de synchronisation d'abonnement.

Configurer Citrix Gateway et StoreFront pour l'authentification DFA

November 10, 2023

L'authentification extensible fournit un seul point de personnalisation pour l'extension de l'authentification basée sur formulaires de StoreFront et de Citrix Gateway. Pour réaliser une solution d'authentification à l'aide du SDK Extensible Authentication, vous devez configurer l'authentification DFA entre Citrix Gateway 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 Citrix Gateway 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 Citrix Gateway 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 }
```



```
28
29 IsDeployed                    : True
30 FeatureClass                  : Citrix.DeliveryServices.Framework
       .Feature.FeatureClass
31 <!--NeedCopy-->
```

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

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

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

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

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

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


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

February 22, 2024

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'appliances 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

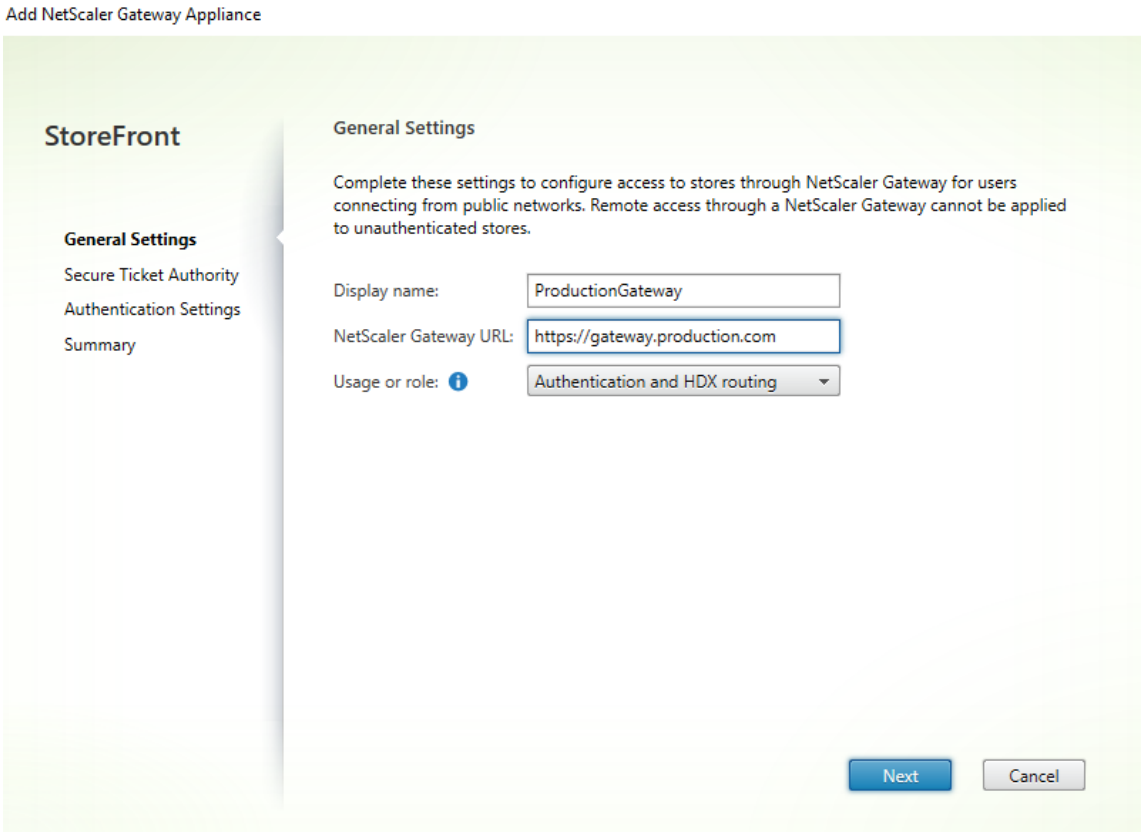
Le domaine `development.com` dans cet exemple est configuré comme suit :

- 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.

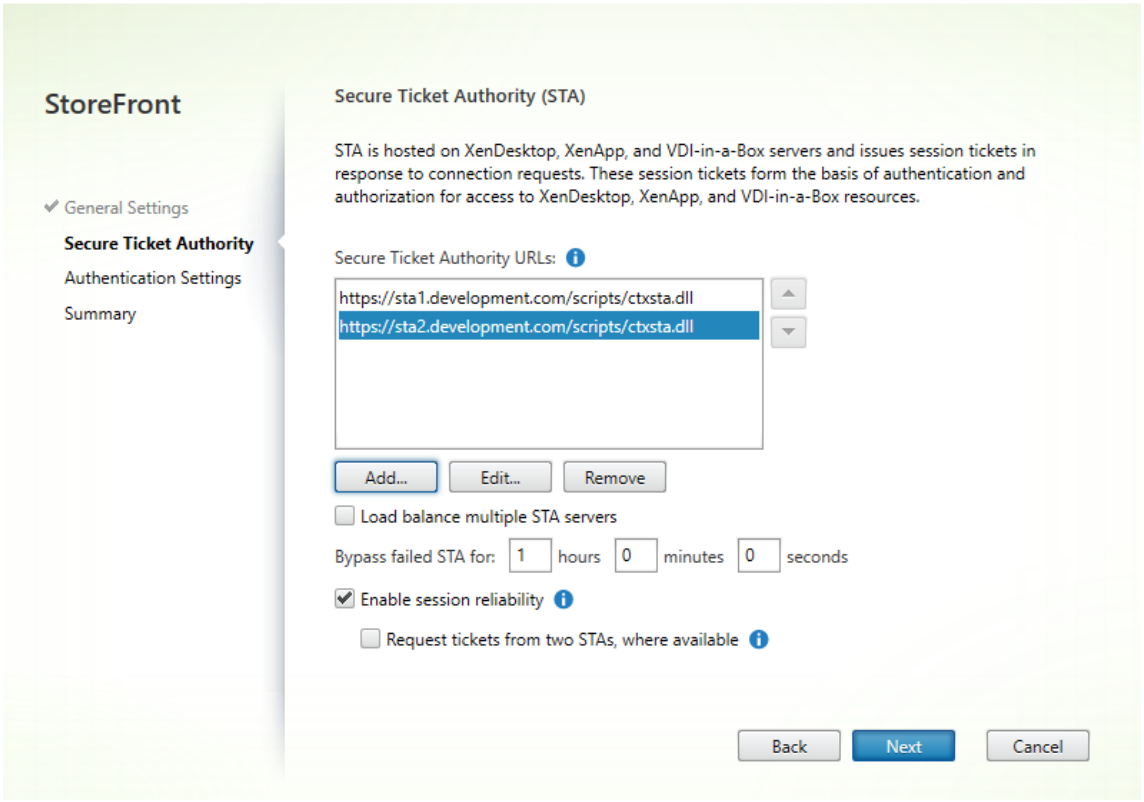
Configurer une passerelle Citrix Gateway pour le magasin

Pour configurer une passerelle Citrix Gateway pour le magasin :

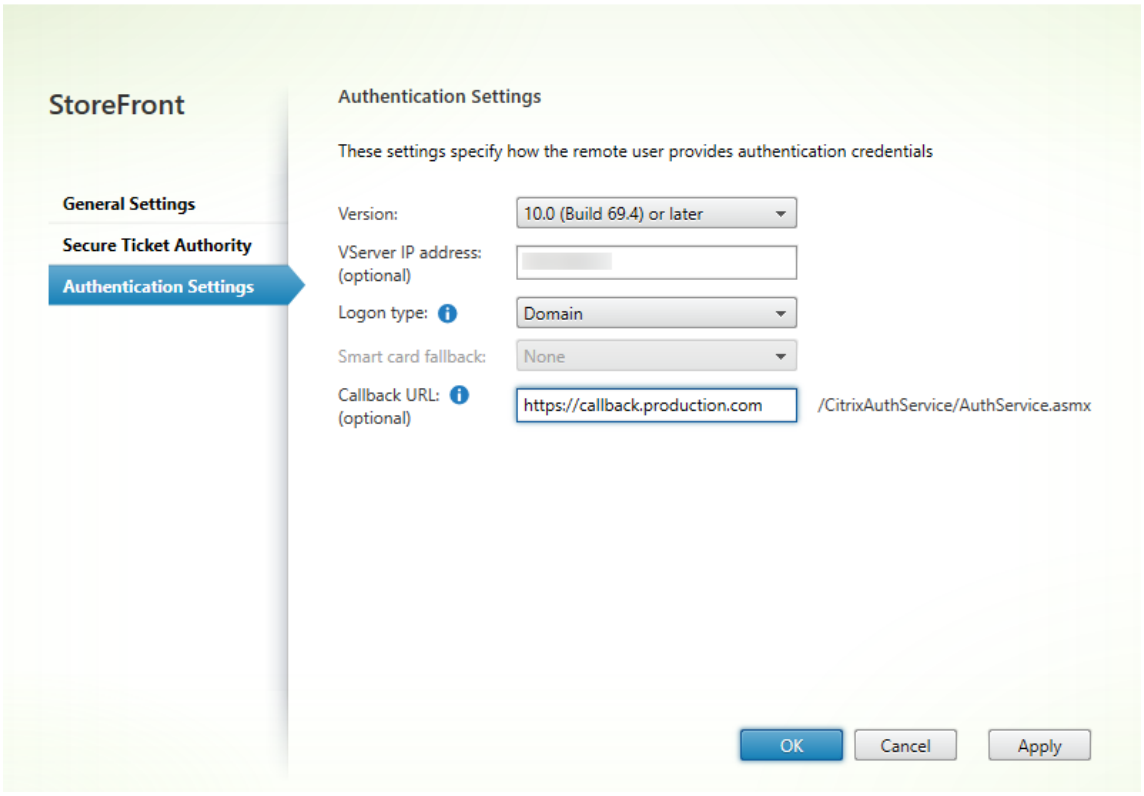
1. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau **Actions**, cliquez sur **Gérer Citrix Gateway**.
2. Sur l'écran Gérer Citrix Gateway, cliquez sur le bouton **Ajouter**.
3. Complétez les paramètres généraux, les paramètres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



Add NetScaler Gateway Appliance



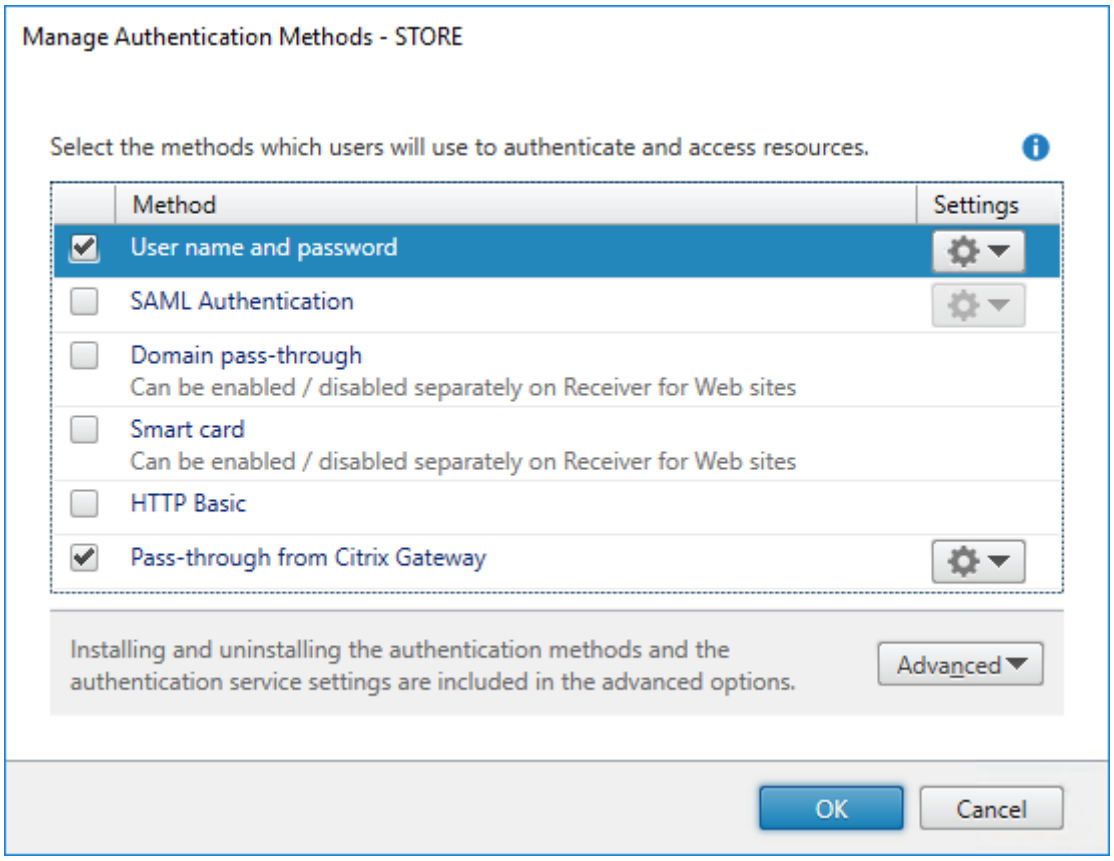
Edit NetScaler Gateway appliance - ProductionGateway



> **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 Gateway 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.

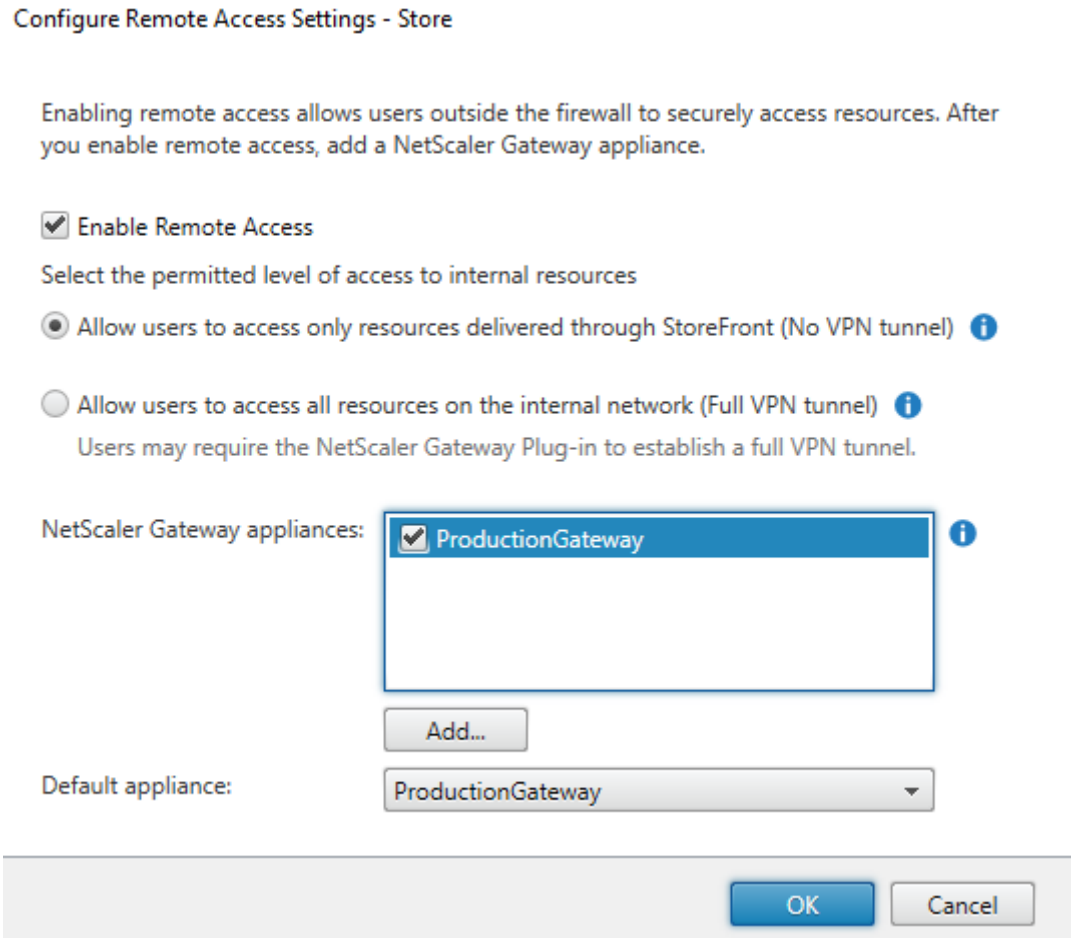
Activer l'authentification pass-through depuis Citrix Gateway

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

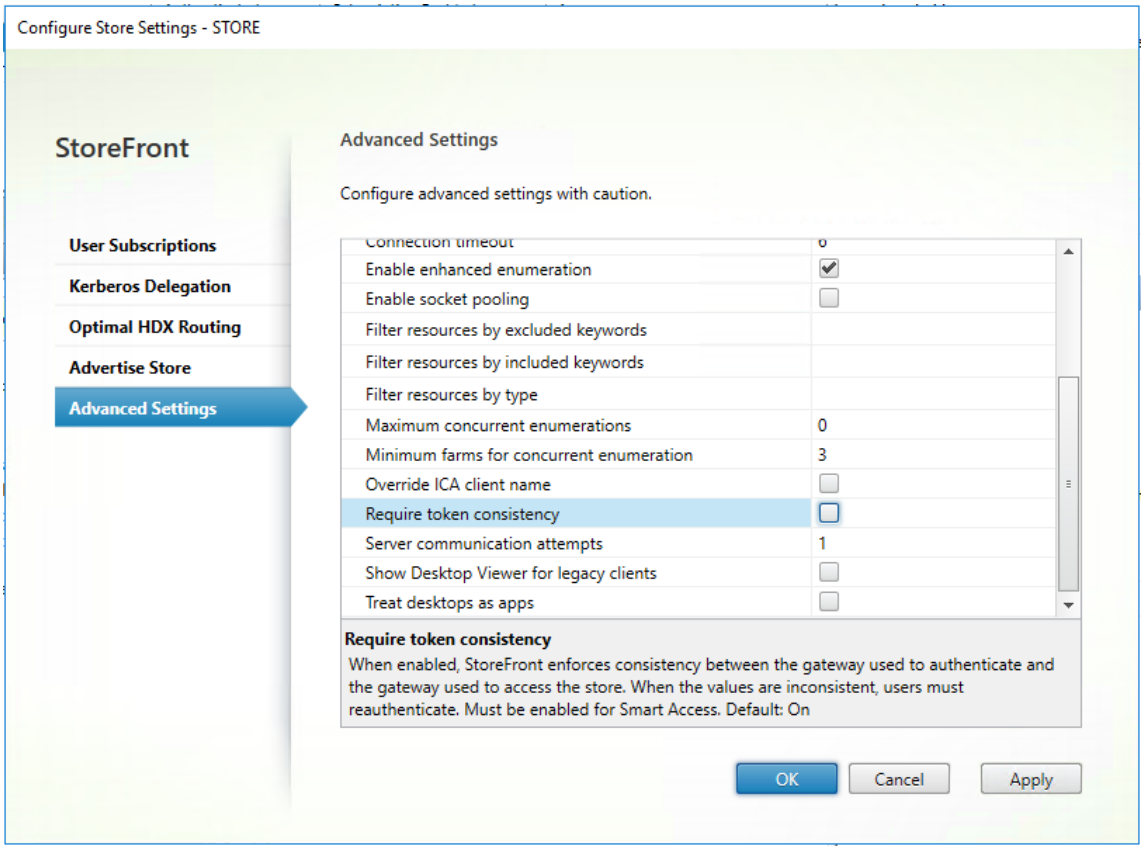
1. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau **Actions**, cliquez sur **Configurer les paramètres d'accès distant**.
2. Sélectionnez **Activer l'accès à distance**.
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 **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront puis, dans le panneau des résultats, sélectionnez un magasin. Dans le panneau **Actions**, cliquez sur **Configurer les paramètres du magasin**.
2. Sur la page Configurer les paramètres du magasin, sélectionnez **Paramètres avancés**.

3. Décochez la case **Exiger la cohérence des jetons**. Pour plus d'informations, consultez la section Paramètres de magasin avancés.



4. Cliquez sur **OK**.

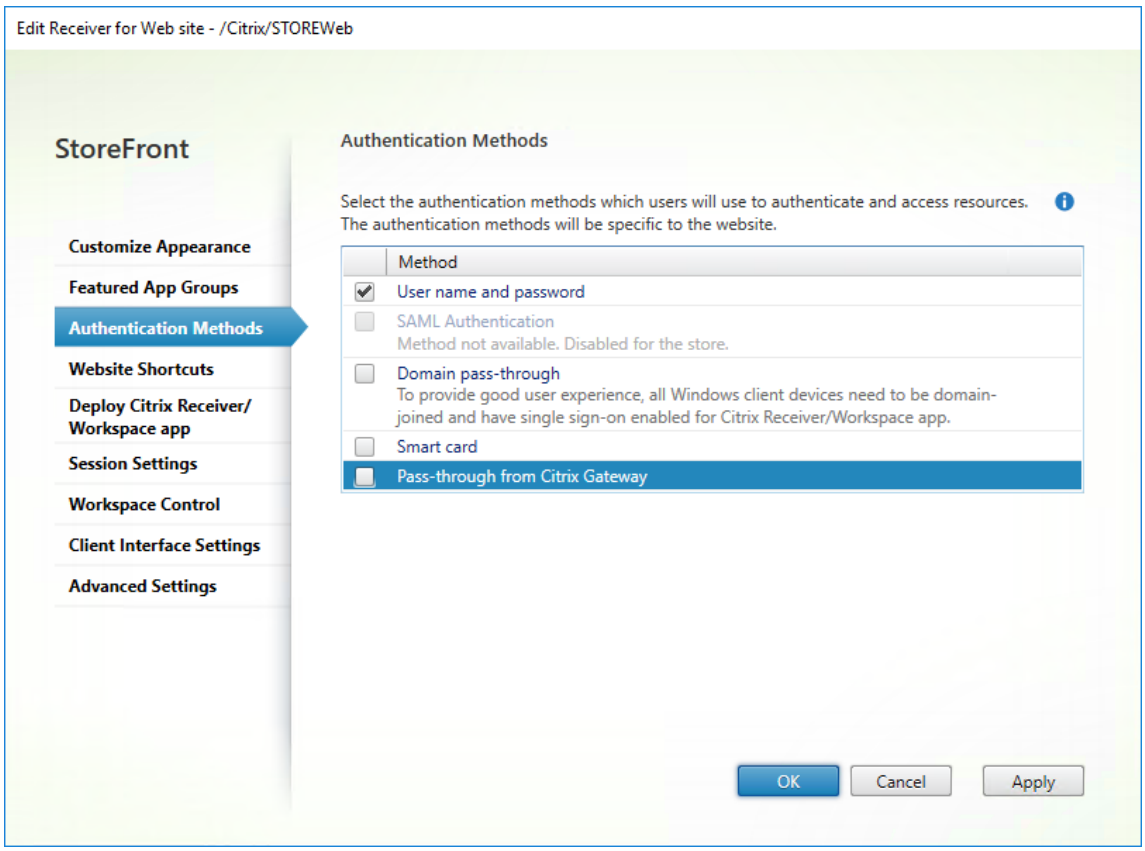
> Remarque :
>
> Le paramètre Exiger la cohérence des jetons est sélectionné (activé) par défaut. Si vous désactivez ce paramètre, les fonctionnalités SmartAccess utilisées pour l'analyse de point de terminaison (EPA) Citrix Gateway cessent de fonctionner. Pour plus d'informations sur SmartAccess, consultez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

Désactiver l'authentification pass-through depuis Citrix Gateway pour le site Web

> **Important :**
>
> La désactivation de l'authentification pass-through depuis Citrix Gateway empêche le site Web d'utiliser les informations d'identification incorrectes du domaine `production.com` transmises depuis l'appliance Citrix Gateway. Lorsque l'authentification pass-through est désactivée depuis Citrix Gateway, le site Web invite l'utilisateur à entrer des informations d'identification. Ces informations d'identification sont différentes des informations d'identification utilisées

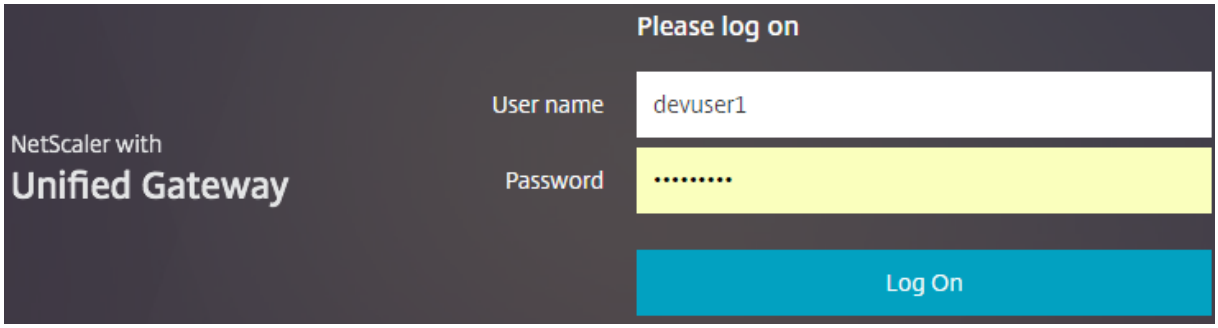
> pour se connecter via Citrix Gateway.

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**.

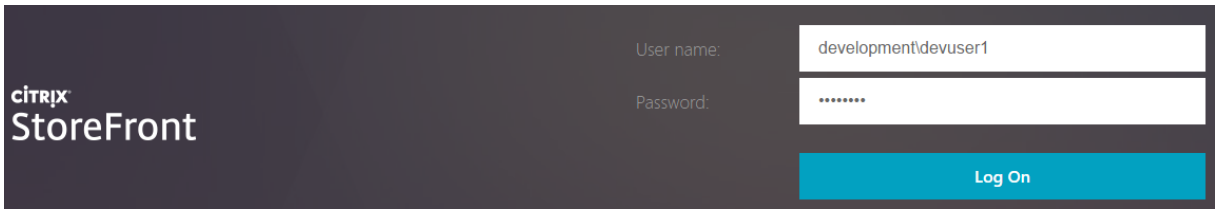


Connexion à Gateway à l'aide d'un utilisateur `production.com` et d'informations d'identification

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`.

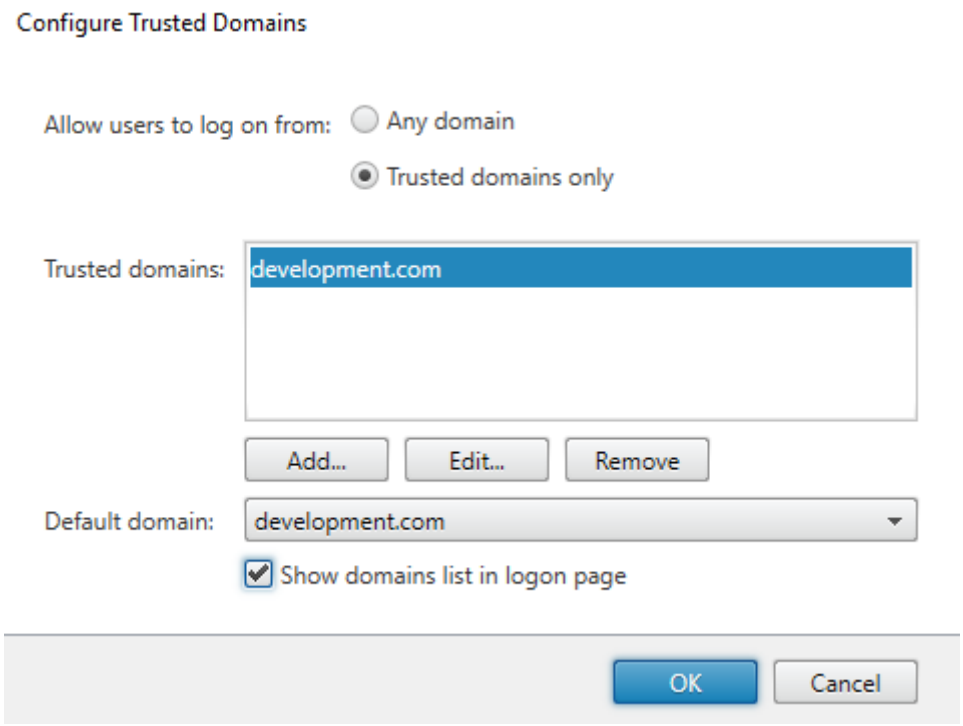


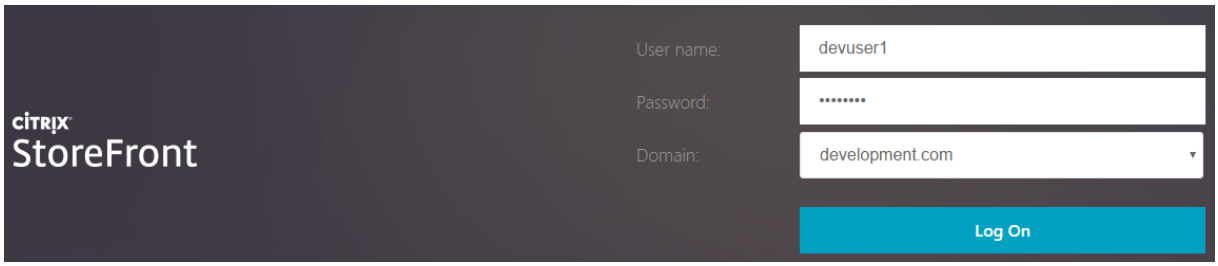
Ajouter une liste déroulante de domaine de confiance dans StoreFront (facultatif)

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**.

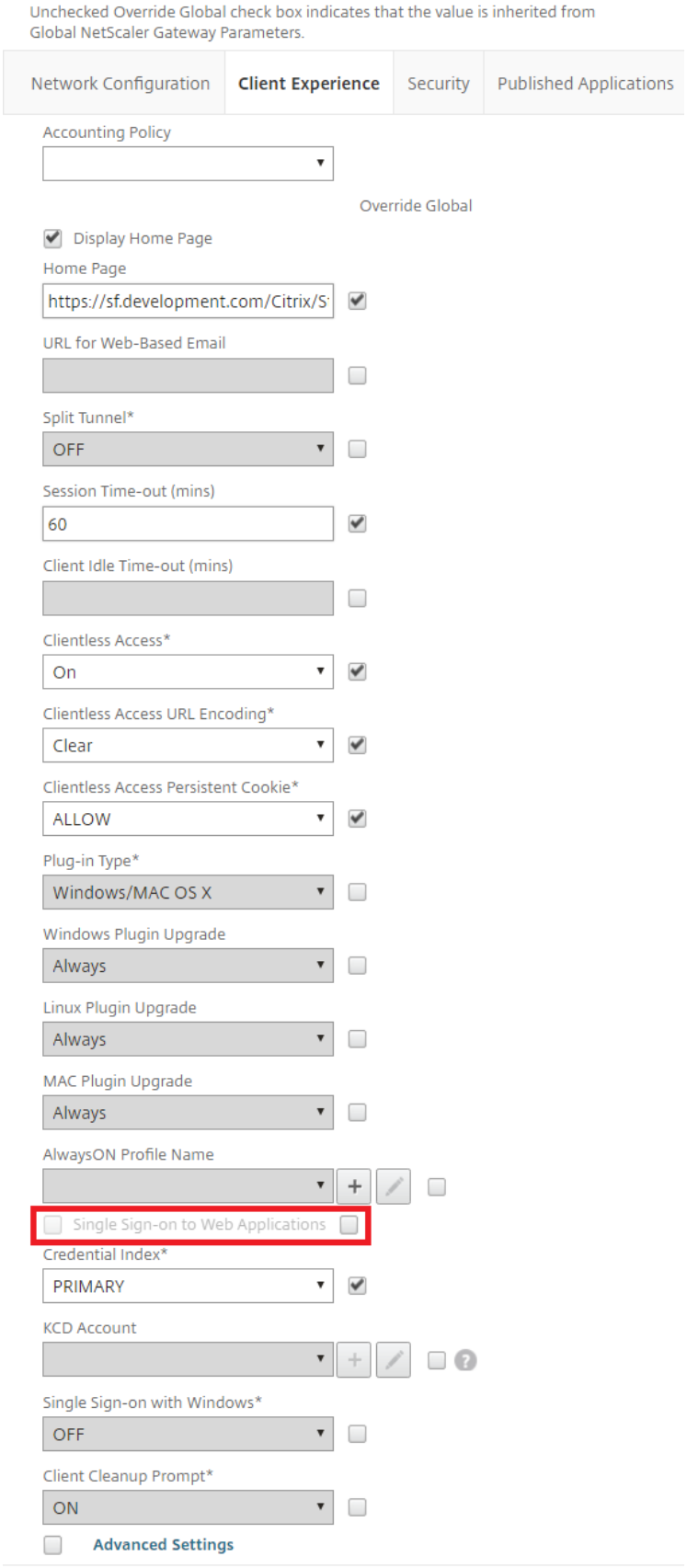


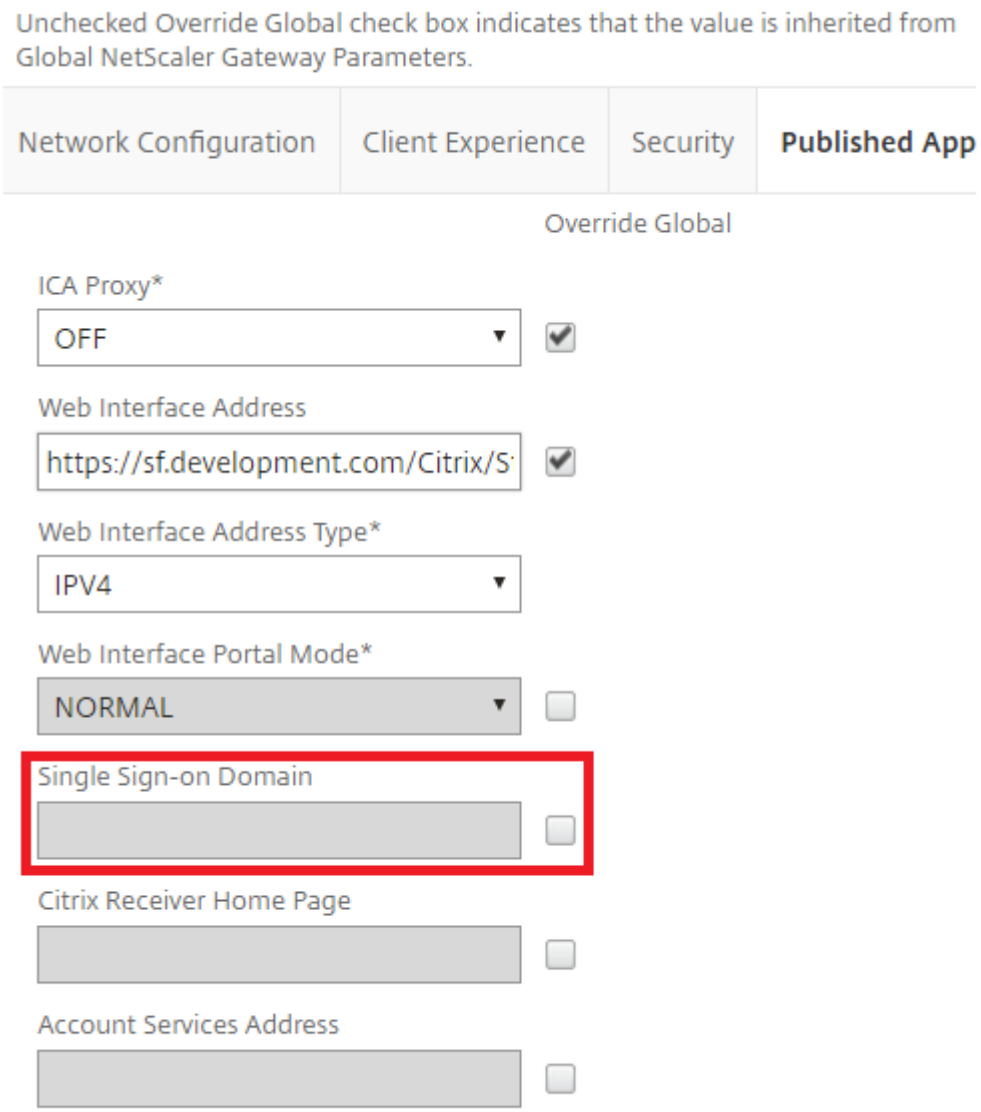


> **Remarque :**
>
> La mise en cache du mot de passe de navigateur n'est pas recommandée dans ce scénario d'authentification. Si les utilisateurs disposent de mots de passe différents pour les deux comptes de domaine différents, la mise en cache du mot de passe peut entraîner une mauvaise expérience.

Stratégie d'action de session NetScaler

- 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 Citrix Gateway au site Web sont ignorées car vous avez désactivé la méthode d'authentification **Authentification pass-through via Citrix Gateway** sur le site Web. Le site 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 Expérience client et Publier l'application de Citrix Gateway ne change pas le comportement décrit dans cet article.





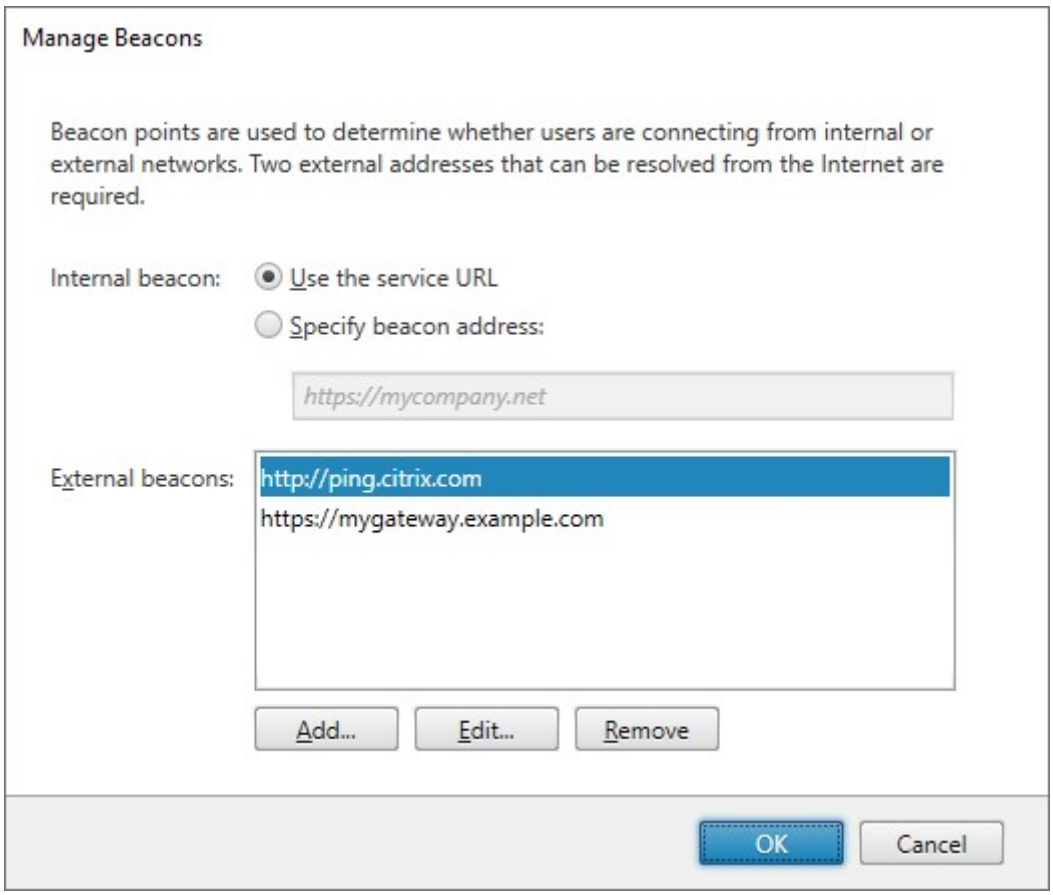
Configurer des points balises

May 30, 2024

> **Important :**
>
> `http://ping.citrix.com` n'est pas disponible actuellement, vous devez donc définir une balise alternative.
>
> N'utilisez pas de sites Web tiers dont vous n'êtes pas propriétaire comme balise externe. Utilisez

> plutôt des sites Web contrôlés par votre organisation.

Sur l'écran Gérer les balises, spécifiez les adresses URL à l'intérieur et à l'extérieur de votre réseau interne à utiliser comme beacon points. L'application Citrix Workspace installée localement tente de contacter des beacon points 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. L'application Citrix Workspace pour HTML5 n'utilise pas de balises.



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 définit :

- La balise interne à l'URL de base de votre déploiement.
- Les balises externes vers `http://ping.citrix.com` et l'URL du premier déploiement Citrix Gateway que vous ajoutez.

Pour configurer des points balises :

1. 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**.
2. 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.
3. 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. Vous devez utiliser des adresses URL contrôlées par votre organisation et non des sites Web tiers.

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. Les utilisateurs peuvent obtenir un fichier de provisioning de l'application Citrix Workspace mis à jour auprès de l'application Citrix Workspace pour HTML5. Sinon, vous pouvez exporter un fichier de provisioning pour le magasin et mettre ce fichier à la disposition de vos utilisateurs.

SDK PowerShell

Pour obtenir les balises actuelles, utilisez Get-STFRoamingBeacon.

Pour ajouter une balise, utilisez Set-STFRoamingBeacon.

Pour régler les balises sur leurs valeurs par défaut, utilisez Clear-STFRoamingBeacon.

Créer un seul nom de domaine complet (FQDN) utilisé en interne et externe

February 22, 2024

Vous pouvez créer un nom de domaine complet (FQDN) unique qui peut accéder à un magasin directement depuis le réseau de votre entreprise et à distance via Citrix Gateway.

Dans le document suivant, ces exemples sont utilisés :

- `https://storefront.example.com` comme URL unique utilisée par les utilisateurs pour accéder à StoreFront. Lorsqu'elle se trouve dans le réseau, elle est résolue sur le serveur StoreFront ou l'équilibreur de charge. En dehors du réseau, elle est résolue sur la passerelle.
- `https://storefrontcb.example.com` comme URL de rappel. Elle est résolue en interne sur la passerelle. Elle n'est requise que pour l'accès intelligent ou l'authentification sans mot de passe. Vous devez vous assurer que le certificat de la passerelle inclut cette adresse en tant que SAN. Utilisez un certificat générique.

URL de base du groupe de serveurs

Modifiez l'URL de base pour qu'elle soit l'URL unique. Voir Modifier l'URL de base d'un déploiement.

Balises StoreFront pour l'application Citrix Workspace installée localement

L'application Citrix Workspace installée localement tente de contacter des beacon points et utilise les réponses pour déterminer si les utilisateurs sont connectés à des réseaux locaux ou publics.

Par défaut, StoreFront utilise l'URL de base du groupe de serveurs comme URL de balise interne. Dans cette configuration, la même URL est valide à la fois en interne et en externe et ne peut donc pas être utilisée comme balise. Par conséquent, vous devez définir la balise interne sur une URL que vous savez accessible uniquement en interne.

Consultez la section Configurer une balise.

DNS externe

- storefront.example.com est résolu sur l'adresse IP externe du serveur virtuel Citrix Gateway.

DNS interne

- storefront.exemple.com est résolu sur l'équilibrage de charge StoreFront ou sur une adresse IP du serveur StoreFront.
- storefrontcb.example.com est résolu sur l'adresse IP virtuelle du serveur virtuel de la passerelle. S'il existe un pare-feu entre la zone démilitarisée et le réseau local de l'entreprise, prenez-le en compte.

Exporter et importer la configuration StoreFront

February 22, 2024

> 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 Windows Server 2019 vers Windows 2022. Les mises à niveau du système d'exploitation sur place ne sont pas prises en charge.
- 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) -Credential (Objet PSCredential)	Chemin d'accès d'exportation à l'archive de configuration. Exemple : $env:userprofile\desktop Utilisez ce paramètre pour créer une copie non cryptée de l'archive de sauvegarde cryptée. Spécifiez l'objet d'information d'identification PowerShell contenant le mot de passe à utiliser pour le décryptage. Exemple : `$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) -Force (Booléen)	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 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 :

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath','Machine')
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
<!--NeedCopy-->
```

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.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -zipFileName "backup" -NoEncryption
```



```
<!--NeedCopy-->
```

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.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
<!--NeedCopy-->
```

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.

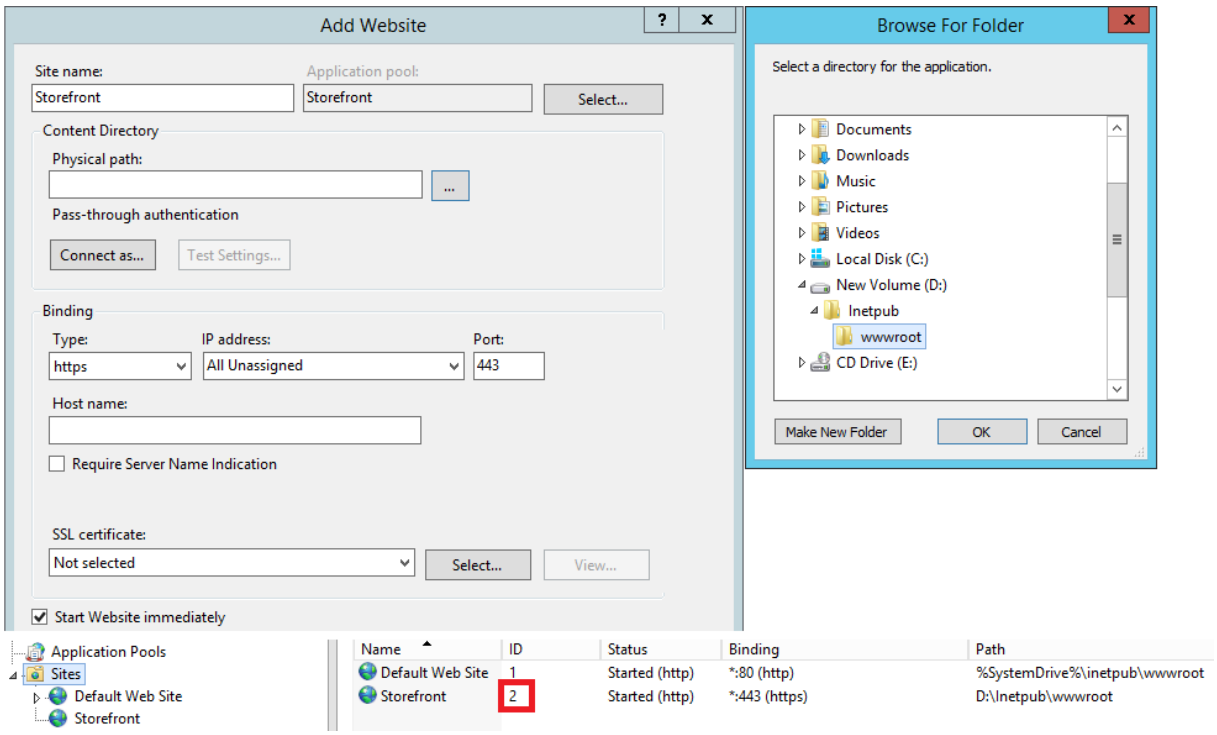
```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

Copiez le fichier backup.zip sur le bureau du Serveur B.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
<!--NeedCopy-->
```

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.

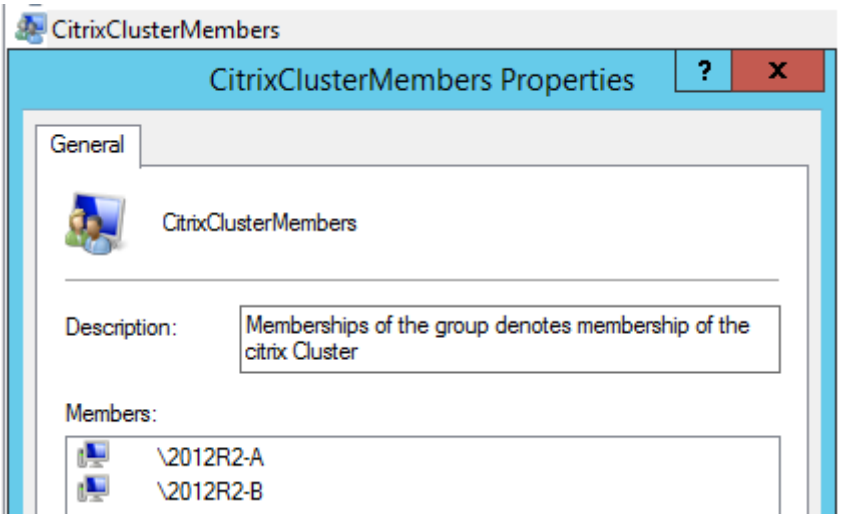
```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
    com"
<!--NeedCopy-->
```

Scénarios de groupe de serveurs

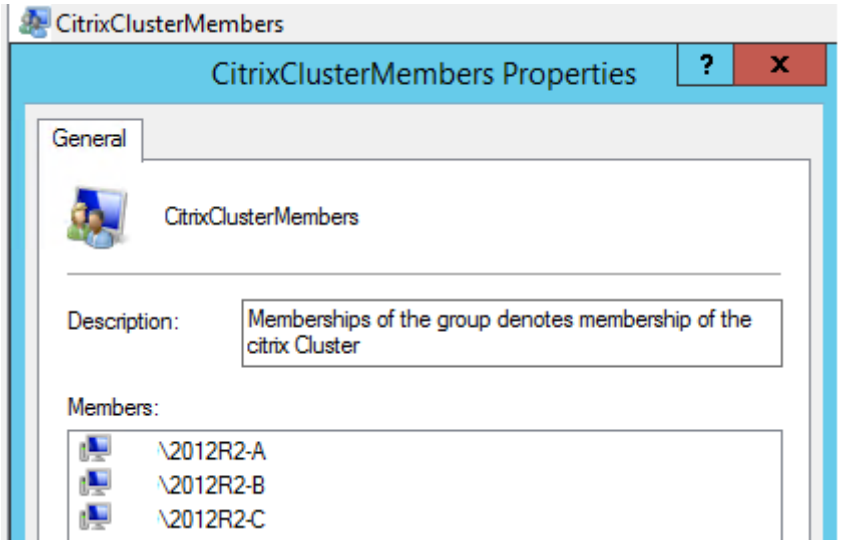
Scénario 1 : sauvegarder une configuration de groupe de serveurs existante et la restaurer plus tard sur le même déploiement de groupe de serveurs Une sauvegarde de configuration précédente a été effectuée lorsque seulement deux serveurs StoreFront, 2012R2-A et 2012R2-B, étaient membres du groupe de 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.



2. Ajoutez ensuite un serveur supplémentaire 2012R2-C au groupe de serveurs existant.



3. 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.

4. Réimportez la configuration du Groupe de serveurs 1 sur le nœud 2012R2-A.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
     desktop\backup.ctxzip" -HostBaseURL "https://servergroup1.
     example.com"
2 <!--NeedCopy-->
```

5. 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.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
     desktop\backup.ctxzip" -HostBaseURL "https://servergroup2.
     example.com"
2 <!--NeedCopy-->
```

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.zip" -NoEncryption -HostBaseURL "https://
    servergroup2.example.com"
<!--NeedCopy-->
```

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.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
```



```
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
<!--NeedCopy-->
```

Exportez la configuration vers backup.ctxzip, un fichier zip crypté.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -Credential $CredObject
<!--NeedCopy-->
```

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"
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

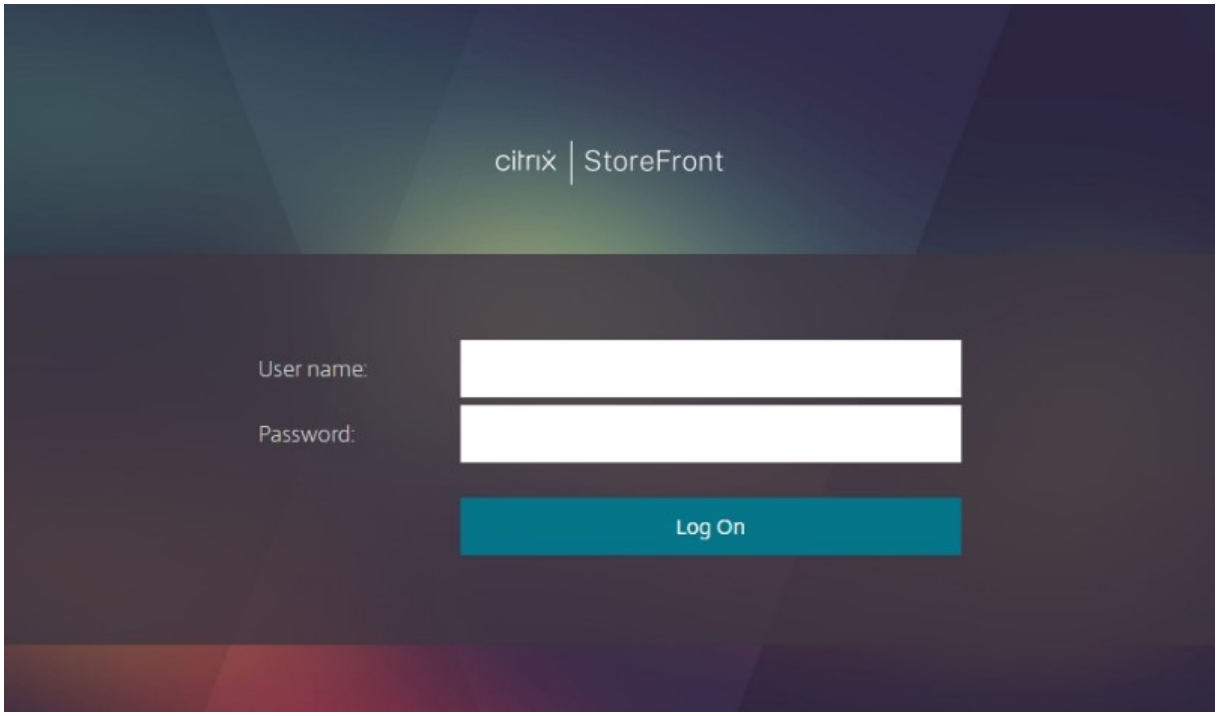
Guide de l'utilisateur

January 25, 2024

Cette section décrit les fonctionnalités et l'apparence d'un magasin lorsqu'il est affiché via un navigateur Web ou via l'application Citrix Workspace.

Connexion

En fonction de la méthode d'authentification et selon que l'authentification unique est activée ou non, vous pouvez être invité à vous connecter.

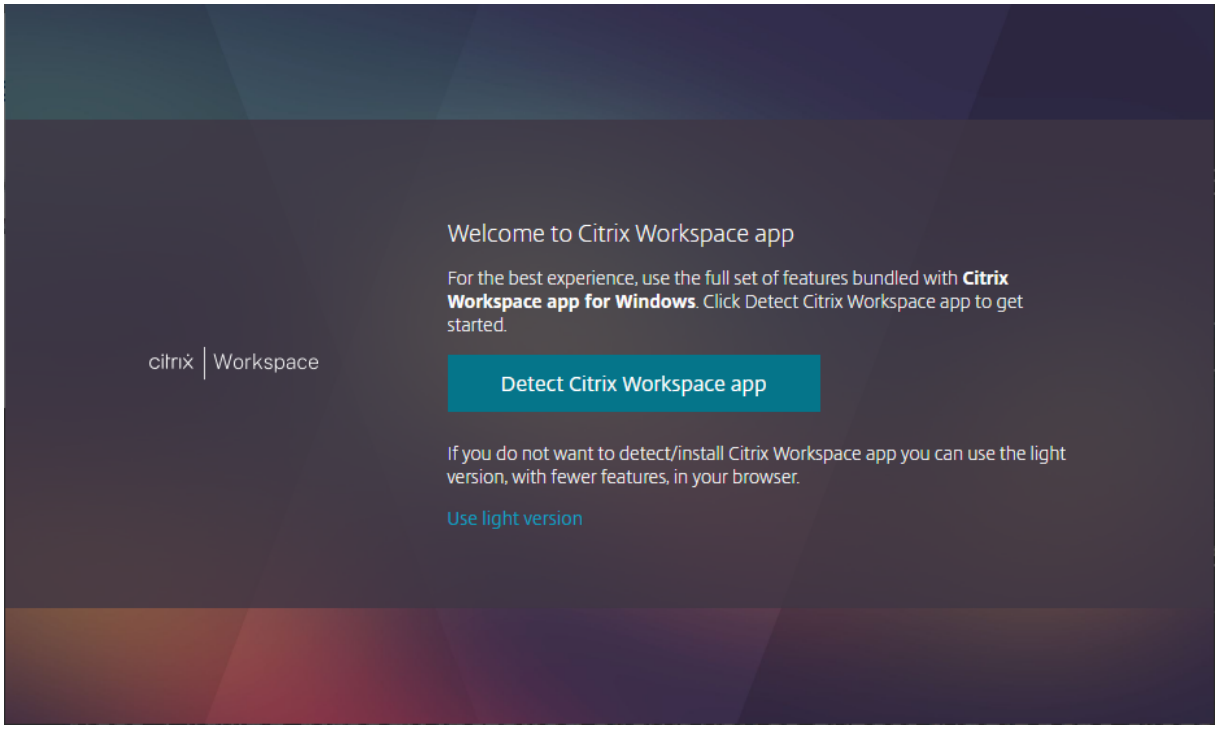


Détection de l'application Citrix Workspace

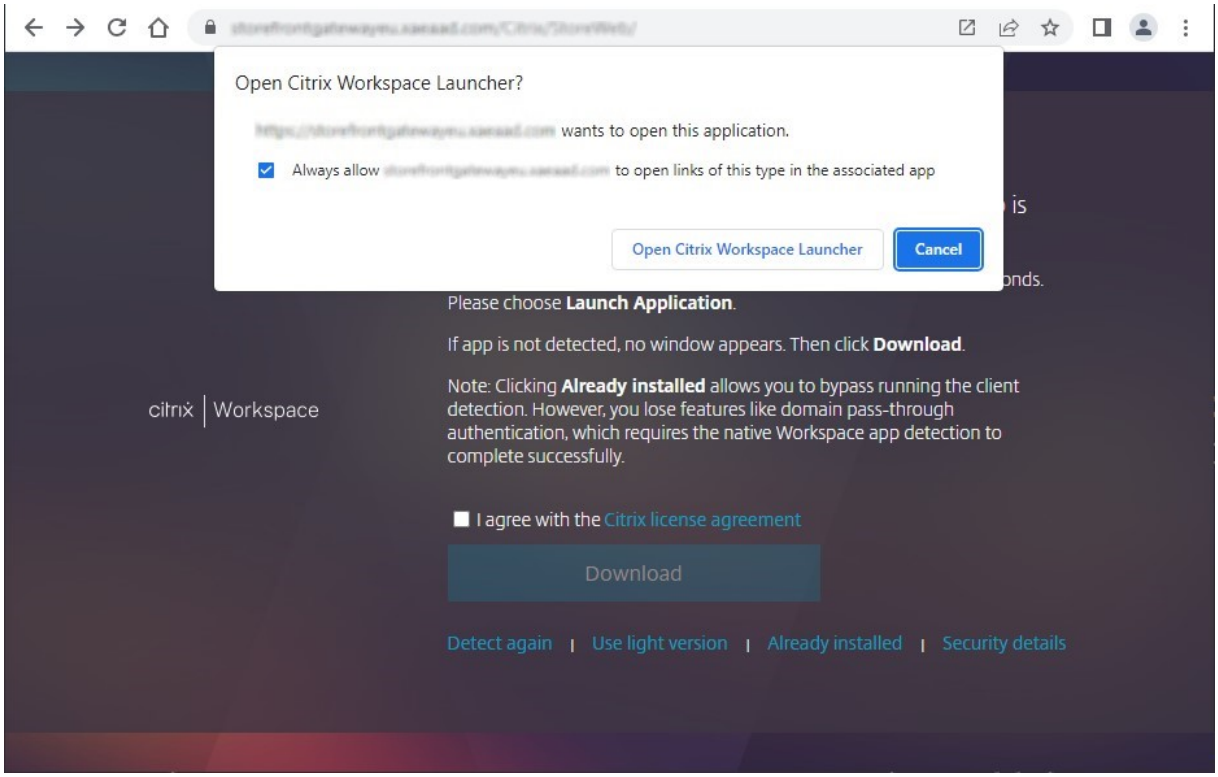
> **Remarque :**
>
> Cette étape s'applique uniquement lorsque vous accédez au magasin via un navigateur Web, et non via l'application Citrix Workspace installée localement. Cette étape peut avoir lieu avant ou après la connexion, selon la configuration.

Selon la configuration, lorsque vous accédez au magasin via un navigateur Web pour la première fois ou après avoir effacé vos cookies, l'écran **Bienvenue sur l'application Citrix Workspace** peut s'afficher. Vous pouvez effectuer l'une des actions suivantes :

- Cliquez sur **Détecter l'application Citrix Workspace** si vous souhaitez lancer des ressources dans l'application Citrix Workspace installée localement. Ceci est recommandé pour une expérience optimale.
- Cliquez sur **Utiliser la version simplifiée** (si disponible) pour toujours lancer les ressources dans le navigateur.



Lorsque vous cliquez sur **Détecter l'application Citrix Workspace**, le système tente de détecter une application Citrix Workspace installée localement. Il essaie d'abord d'utiliser les extensions Web de Citrix Workspace. Si l'application n'est pas installée localement ou si le système ne détecte pas l'application Citrix Workspace installée localement, il tente d'ouvrir **Citrix Workspace Launcher**, qui est un composant de l'application Citrix Workspace. Si l'application Citrix Workspace est installée, votre navigateur affiche une fenêtre vous demandant d'exécuter **Citrix Workspace Launcher**. Cliquez sur **Ouvrir Citrix Workspace Launcher** ou sur **Ouvrir le lien** (selon le navigateur). Il est également recommandé de cocher **Toujours autoriser *domaine* à ouvrir des liens de ce type dans l'application associée** afin d'éviter que cette fenêtre n'apparaisse chaque fois que vous lancez une ressource.



Si une application Citrix Workspace installée localement est détectée, l'écran suivant est affiché au bout de quelques secondes. Lorsque vous lancez ensuite une ressource, le système utilise les extensions Web de Citrix Workspace ou Citrix Workspace Launcher, selon ce qui a été détecté, pour ouvrir les ressources dans l'application Citrix Workspace installée localement.

Si l'application Citrix Workspace n'est pas installée ou si vous annulez Citrix Workspace Launcher, les options suivantes s'offrent à vous en fonction de la configuration :

- **Téléchargement** : télécharge l'application Citrix Workspace depuis le site Web de Citrix ou depuis le serveur StoreFront. Après avoir installé l'application Citrix Workspace, cliquez sur **Détecter à nouveau**.
- **Détecter à nouveau** : tente de détecter à nouveau l'application Citrix Workspace installée localement.
- **Utiliser la version simplifiée** : ignore la détection de l'application Workspace et ouvre toujours les ressources dans votre navigateur Web.
- **Déjà installé** : utilisez cette option si vous avez installé une ancienne version de Citrix Receiver qui ne prend pas en charge Citrix Workspace Launcher ou les extensions Web de Citrix Workspace. Si vous sélectionnez cette option, lorsque vous lancez une application ou un bureau virtuel, votre navigateur télécharge un fichier **launch.ica** que vous pouvez ouvrir avec Citrix Receiver. Cette option entraîne une réduction des fonctionnalités et n'est donc pas recommandée.

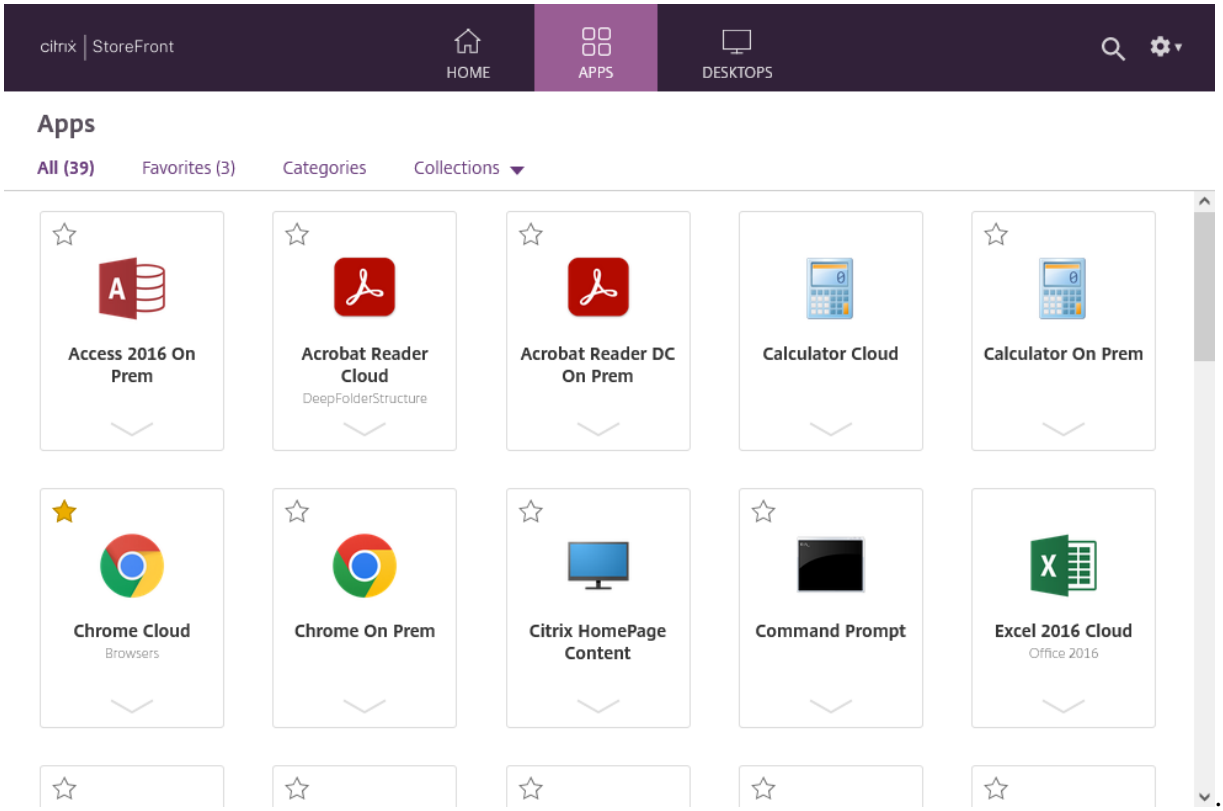
Onglet Accueil

L'onglet **Accueil** affiche tous les groupes d'applications recommandées, ainsi que les applications et bureaux favoris ou obligatoires. L'onglet **Accueil** n'est affiché que si les favoris sont activés pour le magasin.

Onglet Applications

L'onglet **Applications** comporte plusieurs vues secondaires :

- **Tout** : affiche toutes les applications.
- **Favoris** : affiche toutes les applications préférées.
- **Catégories** : affiche les catégories et les applications qui s'y trouvent. La façon dont les catégories sont affichées dépend des paramètres de catégorie.
- **Collections** : affiche les groupes d'applications recommandées.



Onglet Bureaux

L'onglet **Bureaux** comporte deux vues secondaires :

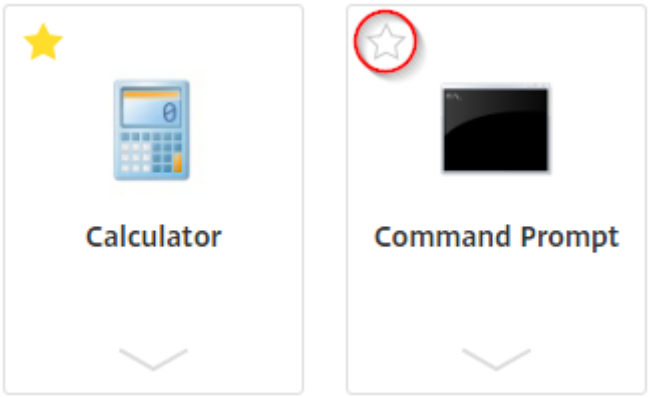
- **Tout** : affiche tous les bureaux.
- **Favoris** : affiche les bureaux préférés.

Vignettes d'application et de bureau

Cliquez sur une icône pour lancer l'application ou le bureau.

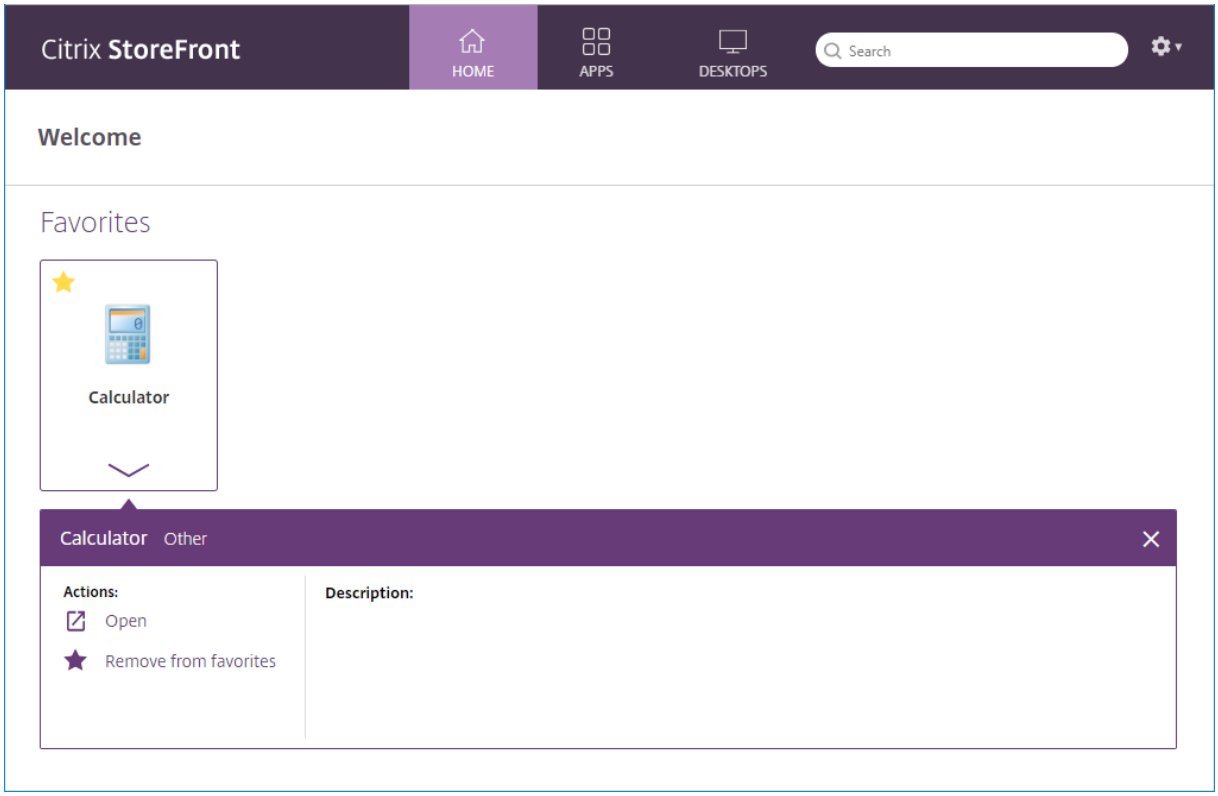
Favoris

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



Afficher les détails et les actions

Vous pouvez développer un panneau sous chaque icône pour afficher la description et les actions de l'application.



Les actions suivantes peuvent être disponibles :

- **Ouvrir** : lance l'application ou le bureau ou s'y reconnecte.
- **Ajouter aux favoris** : si l'élément n'est pas un favori, qu'il n'est pas obligatoire et que les favoris sont activés pour le magasin, l'application ou le bureau est ajouté(e) à vos favoris.

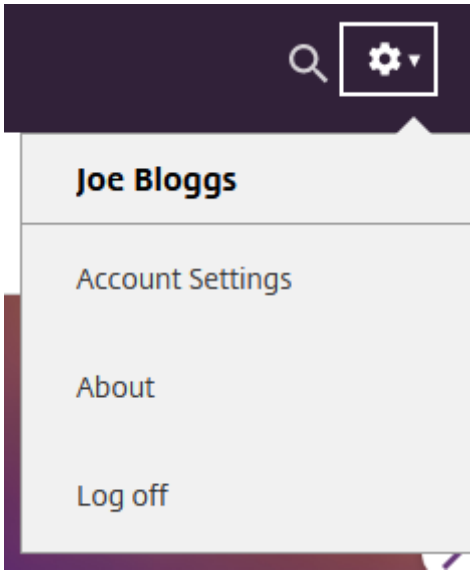
- **Supprimer des favoris** : si l'élément est un favori, qu'il n'est pas obligatoire et que les favoris sont activés pour le magasin, l'application ou le bureau est supprimé(e) de vos favoris.
- **Redémarrer** : pour les bureaux assignés où le redémarrage est disponible, le bureau redémarre.

Rechercher

Cliquez sur l'icône en forme de loupe pour faire apparaître le champ de recherche. Recherchez dans toutes les applications, tous les bureaux et toutes les catégories :

Paramètres

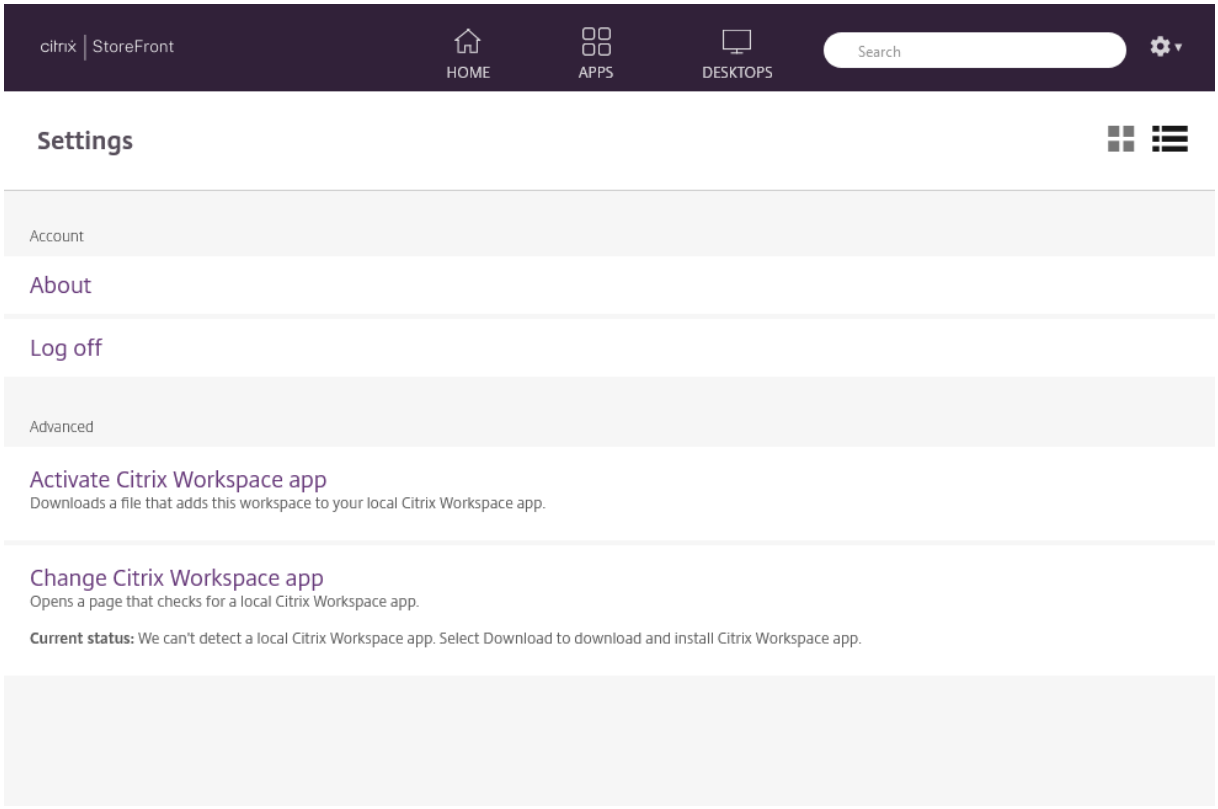
Le menu des paramètres n'est disponible que lorsque vous accédez au magasin via un navigateur Web.



Le menu des paramètres contient les options suivantes :

- **Paramètres du compte** : ouvre la page des paramètres.
- **À propos** : affiche des informations sur l'application.
- **Déconnexion** : déconnecte du site Web.

Paramètres du compte



Les options suivantes peuvent être disponibles :

Connecter. Reprend les sessions déconnectées.

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

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

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

Fermer la session

Pour fermer la session, ouvrez le menu des paramètres et cliquez sur **Fermer la session**. Cela vous déconnecte du magasin. Si vous êtes connecté à une ressource, selon la configuration, cette action aura pour effet de :

- arrêter les ressources ; ou

- vous déconnecter des ressources ; ou
- laisser les ressources connectées.

SDK StoreFront

April 17, 2024

Citrix StoreFront fournit un kit de développement logiciel (SDK) basé sur un certain nombre de modules Microsoft Windows PowerShell version 2.0. 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.

> **Remarque :**
>
> Le SDK PowerShell n'est pas compatible avec PowerShell 6 ou une version ultérieure.

Pour la référence SDK, consultez SDK StoreFront.

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. Lancez une invite de ligne de commande PowerShell ou **Windows PowerShell ISE** en tant qu'administrateur.

   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 tous 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.

Exemples	Description
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 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
```



```
17      Import-Module Citrix.StoreFront
18      Import-Module Citrix.StoreFront.Stores
19      Import-Module Citrix.StoreFront.Authentication
20      Import-Module Citrix.StoreFront.WebReceiver
21  <!--NeedCopy-->
```

- 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 ».

```
1  # Determine the Authentication and Receiver virtual path to use
      based of the Store
2  $authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
3  $receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
4  <!--NeedCopy-->
```

- Crée un nouveau déploiement, si ce n'est pas déjà fait, pour préparer l'ajout des services StoreFront requis. **-Confirm:$false** supprime le besoin de confirmer que le déploiement peut se poursuivre.

```
1  # Determine if the deployment already exists
2  $existingDeployment = Get-STFDeployment
3  if(-not $existingDeployment)
4  {
5
6      # Install the required StoreFront components
7      Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
          Confirm:$false
8   }
9
10 elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
11 {
12
13     # The deployment exists but it is configured to the desired
          hostbase url
14     Write-Output "A deployment has already been created with the
          specified hostbase url on this server and will be used."
15  }
16
17 else
18 {
19
20     Write-Error "A deployment has already been created on this
          server with a different host base url."
21  }
22
23 <!--NeedCopy-->
```

- 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."
 }

<!--NeedCopy-->
```

- 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
{

    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."
    # 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   }
21
22  <!--NeedCopy-->
```

- 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   }
15
16  <!--NeedCopy-->
```

- 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    }
9
10  <!--NeedCopy-->
```


Créer un déploiement avec accès à distance

L'exemple suivant est basé sur le script précédent et ajoute un déploiement avec accès à distance.

Avant de commencer, suivez les étapes détaillées dans Démarrage avec SDK. Cet exemple peut être personnalisé à l'aide des méthodes décrites pour produire un script qui automatise le déploiement StoreFront.

> **Remarque :**
>
> Pour vous assurer que vous obtiendrez toujours les dernières améliorations et correctifs, Citrix vous recommande de suivre la procédure décrite dans ce document, plutôt que de copier et de coller le script exemple.

Compréhension du script Cette section décrit la fonction de chaque partie du script généré par StoreFront. Ceci vous aidera à la personnalisation de votre propre script.

- Définit la gestion des erreurs et importe les modules StoreFront requis. Les importations ne sont pas nécessaires dans des versions plus récentes de PowerShell.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [Parameter(Mandatory=$true)]
    [long]$SiteId = 1,
    [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",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName
)
Set-StrictMode -Version 2.0

# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
```



```
# 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.Roaming
<!--NeedCopy-->
```

- 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.

```
# Create a simple deployment by invoking the SimpleDeployment example
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `
 -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType $TransportType
<!--NeedCopy-->
```

- 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.

```
# Determine the Authentication and Receiver sites based on the Store
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$authentication = Get-STFAuthenticationService -StoreService $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

Exemple : Créer un déploiement avec accès à distance et passerelle de lancement optimale

L'exemple suivant est basé sur le script précédent et ajoute un déploiement avec accès à distance et passerelle de lancement optimale.

Avant de commencer, suivez les étapes détaillées dans Démarrage avec SDK. Cet exemple peut être personnalisé à l'aide des méthodes décrites pour produire un script qui automatise le déploiement StoreFront.

> **Remarque :**
>
> Pour vous assurer que vous obtiendrez toujours les dernières améliorations et correctifs, Citrix vous recommande de suivre la procédure décrite dans ce document, plutôt que de copier et de coller le script exemple.

Compréhension du script Cette section décrit la fonction de chaque partie du script généré par StoreFront. Ceci vous aidera à la personnalisation de votre propre script.

- Définit la gestion des erreurs et importe les modules StoreFront requis. Les importations ne sont pas nécessaires dans des versions plus récentes de PowerShell.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$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",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# 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.Roaming
```



```
<!--NeedCopy-->
```

- Appels dans le script de déploiement avec accès à distance pour configurer le déploiement de base et ajouter l'accès à distance.

```
# Create a remote access deployment
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
    ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype `
     -LoadbalanceServers $LoadbalanceServers -Port $Port  -
        SSLRelayPort $SSLRelayPort -TransportType $TransportType `
     -GatewayUrl $GatewayUrl -GatewayCallbackUrl
        $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
        GatewayName $GatewayName
<!--NeedCopy-->
```

- Ajoute la passerelle de lancement optimale préférée à partir de la liste de passerelles configurées.

```
# Add a new Gateway used for remote HDX access to desktops and
    apps
$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -
    LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -
    SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
<!--NeedCopy-->
```

- Oblige le service de magasin à utiliser la passerelle optimale, l'enregistrer, et l'attribuer aux lancements depuis la batterie désignée.

```
# Get the Store configured by SimpleDeployment.ps1
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all
    of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
    StoreService $store -FarmName $farmNames
<!--NeedCopy-->
```

Résolution des problèmes de StoreFront

February 22, 2024

Journaux d'installation

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.

Journaux d'événements

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.

Limitation des événements consignés dans le 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.

Journaux de Powershell et de la console de gestion

Les modifications de configuration effectuées via PowerShell ou la console de gestion sont enregistrées dans `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs`. 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.

Enregistrement des diagnostics

StoreFront écrit les journaux de diagnostic dans `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`

Pour les versions 2311 et supérieures de StoreFront, par défaut, les messages de niveau **Erreur**, **Avertissement**et **Infos** sont enregistrés. Dans la plupart des cas, ils incluent suffisamment d'informations pour diagnostiquer les éventuels problèmes.

> **Remarque :**
>
> Dans les versions 2308 et antérieures de StoreFront, seuls les messages de niveau **Erreur** sont enregistrés par défaut.

Vous pouvez activer une journalisation détaillée supplémentaire à des fins de dépannage. Cela n'est requis que si le support Citrix le demande. Cette journalisation peut avoir un impact sur les performances. Vous devez donc redéfinir `TraceLevel` sur `Info` une fois le dépannage terminé.

Pour activer la journalisation détaillée :

1. À l'aide d'un compte disposant d'autorisations d'administrateur local, démarrez Windows PowerShell
2. Entrez la commande :

```
Set-STFDiagnostics -All -TraceLevel "Verbose" -Override -confirm:
    $False
<!--NeedCopy-->
```

> **Remarque :**

> Le paramètre `-Override` est obligatoire uniquement pour StoreFront 2311. Ce paramètre sera supprimé des versions ultérieures de StoreFront.

Cela active une journalisation détaillée pour tous les services, sans demande de confirmation. Lorsque cette commande est entrée, les services StoreFront sont redémarrés. Attendez le retour de l'invite PowerShell pour vérifier que le redémarrage des services est terminé. Pendant le redémarrage de ces services, le serveur StoreFront ne sera pas accessible aux utilisateurs.

3. Reproduisez le problème pour créer les journaux.
4. Redéfinissez le niveau de journalisation par défaut pour tous les services

```
1  Set-STFDiagnostics -All -TraceLevel "Info" -Override -confirm:
       $False
2  <!--NeedCopy-->
```

> **Remarque :**
>
> Le paramètre `-Override` est obligatoire uniquement pour la version 2311 de StoreFront.

Vous pouvez personnaliser davantage la journalisation de diagnostic :

- StoreFront écrit un fichier journal distinct pour chaque service. Par défaut, la taille maximale de chaque fichier journal est de 200 Mo. StoreFront écrit jusqu'à cinq fichiers journaux par service avant de purger les anciens fichiers journaux. Si vous devez personnaliser la taille ou le nombre de journaux écrits, vous pouvez le faire à l'aide des paramètres `-FileSizeKb` et `-FileCount`.
- Modifiez le niveau de détail enregistré à l'aide de `-TraceLevel`. Les valeurs autorisées sont `Off`, `Error`, `Warning`, `Info` ou `Verbose`.
- L'utilisation du paramètre `-All` définit les paramètres de journalisation pour tous les services. Vous pouvez personnaliser la journalisation pour un service individuel en utilisant `-Service [Service name]`.

Pour plus d'informations sur l'applet de commande `Set-STFDiagnostics`, consultez la documentation StoreFront PowerShell SDK.

Journalisation du fichier launch.ica

Lorsqu'un utilisateur lance une application ou un bureau, StoreFront génère un fichier appelé launch.ica que l'application Workspace lit pour déterminer comment se connecter à l'application ou au bureau. Selon la configuration, ce fichier peut être stocké en mémoire et ne pas être directement accessible. Pour diagnostiquer les erreurs de lancement, il peut être utile de consulter le contenu de launch.ica.

Pour autoriser la journalisation du fichier launch.ica sur le PC client, 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 :

```
LogFile=C:\ica\ica.log
LogICAFile=true
<!--NeedCopy-->
```

> Remarque :
>
> L'utilisation d'un fichier ICA dans votre environnement pour autre chose qu'un dépannage est abordée dans l'article CTX200126.

Annonces de fin de prise en charge

May 30, 2024

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître pour que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître. Pour obtenir des informations sur la prise en charge du cycle de vie d'un produit, consultez l'article Politique de prise en charge du cycle de vie des produits. Pour plus d'informations sur l'option de maintenance LTSR (Long Term Service Release), reportez-vous à la section https://support.citrix.com/article/CTX205549.

Fins de prise en charge

Les éléments obsolètes ne sont pas retirés immédiatement. Citrix continue de les prendre en charge, mais ils seront retirés dans le futur.

Élément	Abandon annoncé dans la version	Solution alternative
XenApp Services (également connus sous le nom de PNAgent)	2308	Dans l'application Workspace, connectez-vous aux magasins à l'aide de l'URL du magasin plutôt que de l'URL de XenApp Services
Windows Server 2016	2402	Effectuer une mise à niveau avec une version plus récente de Windows Server

Retraits

Les éléments retirés sont supprimés ou ne sont plus pris en charge.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Internet Explorer 11 pour la connexion à des ressources à l'aide de l'application Workspace pour HTML5	2308	2308	Utilisez un navigateur Web compatible ou installez l'application Citrix Workspace pour Windows. Il est toujours possible d'utiliser Internet Explorer 11 pour accéder à votre magasin, mais l'application Citrix Workspace pour Windows doit être installée pour lancer des ressources.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Flux de ressources XenApp 6.5	2308	2308	Passez à la dernière version de Citrix Virtual Apps and Desktops. Il est également possible d'ajouter des flux de ressources XenApp 6.5 à l'aide de PowerShell, mais notez que XenApp 6.5 n'est plus pris en charge.
Prise en charge de la fonctionnalité Réinitialisation en libre-service des mots de passe	2203	2203	-
Prise en charge des protocoles TLS 1.0 et TLS 1.1 entre Citrix Virtual Apps and Desktops et l'application Citrix Workspace.	3.14	2203	Mettez à niveau les Citrix Receiver vers une application Citrix Workspace qui prend en charge TLS 1.2.
Installation de StoreFront sur Windows Server 2012 R2	2203	2203	Installez StoreFront sur un système d'exploitation pris en charge.
Prise en charge des versions de Microsoft .NET Framework antérieures à la version 4.7.2.	2203	2203	Mettez à niveau vers .NET Framework version 4.7.2 ou ultérieure. (Le programme d'installation installe automatiquement .NET Framework 4.7.2 s'il n'est pas déjà installé.)

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Suppression des options de Delivery Controller pour les produits en fin de vie suivants : VDI-in-a-Box et XenMobile (9.0 ou version antérieure).	1903	1903	—
Internet Explorer 9 and 10	1903	1903	—
Prise en charge pour l'accès utilisateur aux bureaux sur les sites Desktop Appliance	1811	1912	Utilisez Desktop Lock pour les cas d'utilisation n'appartenant pas à un domaine.
Expérience classique Citrix (interface utilisateur avec « bulles vertes »)	3.12	1903	Utiliser l'interface utilisateur unifiée
Installation de StoreFront sur Windows Server 2012 et Windows Server 2008 R2 (y compris les Service Packs)	3.12 LTSR	3.15	Installez les composants sur un système d'exploitation pris en charge.
Intégration de Citrix Online Integration (produit Goto)	3.11	3.12	—
Mises à niveau sur place depuis StoreFront 2.0, 2.1, 2.5 et 2.5.2.	3.9	1818	Passer de l'une de ces versions à la version 3.12, puis à une version plus récente
Installation de StoreFront sur des machines 32 bits (x86).	3.8	3.13	Installez sur un système d'exploitation x64 pris en charge.

Pour plus d'informations sur les fins de prise en charge dans l'application Citrix Workspace pour

HTML5, consultez la page Fin de prise en charge.

Avis de tiers

May 30, 2024

StoreFront peut inclure des composants de logiciel tiers fournis sous licence selon les conditions suivantes. Cette liste a été générée à l'aide d'un logiciel tiers à la date indiquée dans la liste. Cette liste peut changer en fonction des versions spécifiques du produit et peut ne pas être complète ; elle est fournie « telle quelle ». DANS LA LIMITE AUTORISÉE PAR LA LOI APPLICABLE, CITRIX ET SES FOURNISSEURS N'OFFRENT AUCUNE REPRÉSENTATION OU GARANTIE, EXPRESSE OU TACITE, LÉGALE OU AUTRE, CONCERNANT LA LISTE, SA PRÉCISION OU SON EXHAUSTIVITÉ, OU CONCERNANT TOUT RÉSULTAT DÉCOULANT DE L'UTILISATION OU DE LA DISTRIBUTION DE LA LISTE. EN UTILISANT OU DISTRIBUANT LA LISTE, VOUS CONVENEZ QU'EN AUCUN CAS CITRIX NE POURRA ÊTRE TENU RESPONSABLE DE TOUT DOMMAGE SPÉCIAL, DIRECT, INDIRECT OU ACCESSOIRE OU TOUT AUTRE DOMMAGE RÉSULTANT DE L'UTILISATION OU DE LA DISTRIBUTION DE CETTE LISTE.

Castle Windsor 3.3.0

Copyright 2004-2013 Castle Project - http://www.castleproject.org/

Sous licence Apache, version 2.0

Bloc d'applications Microsoft Unity (Unity) 2.1

Copyright © 2011 Microsoft Corporation.

Sous licence Microsoft Public License (MS-PL) https://msdn.microsoft.com/en-us/library/hh237493.aspx

Microsoft Patterns and Practices: Prism 2.2

Copyright © 2010 Microsoft Corporation.

Sous licence Microsoft Public License (MS-PL) http://compositewpf.codeplex.com/releases/view/46046

Microsoft patterns & practices: Common Service Locator 1.0

Copyright © Microsoft Corporation.

Sous licence Microsoft Public License (MS-PL)

Source de référence .Net Microsoft

Copyright © Microsoft Corporation. Sous licence MIT.

ManagedEsent version 1.9.4

Copyright © Microsoft Corporation.

Sous licence Microsoft Public License (MS-PL) http://managedesent.codeplex.com/license

jQuery UI - v1.10.4 - 2014-03-12

http://jqueryui.com/

Copyright 2014 jQuery Foundation et autres contributeurs ; sous licence MIT

Bibliothèque JavaScript jQuery v1.12.4

http://jquery.com/

Inclut Sizzle.js

http://sizzlejs.com/

Copyright jQuery Foundation et autres contributeurs

Publié sous licence MIT

http://jquery.org/license

Date : 2016-05-20T 17:17 Z

jQuery jScrollPane v2.0.0beta11

jScrollPane - v2.0.0beta11 - 2011-07-04 http://jscrollpane.kelvinluck.com/

Copyright (c) 2010 Kelvin Luck

Double licence sous licences MIT et GPL.

jquery.contextmenu.js

Plug-in jQuery pour les menus contextuels

http://www.JavascriptToolbox.com/lib/contextmenu

Copyright (c) 2008 Matt Kruse (javascripttoolbox.com)

Double licence sous licences MIT et GPL.

Plug-in jQuery pour Hammer.JS - v1.0.0 - 2014-01-02

http://eightmedia.github.com/hammer.js

Copyright (c) 2014 Jorik Tangelder j.tangelder@gmail.com;

Sous licence MIT

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

Sous licence MIT (LICENSE.txt).

WPF Toolkit 3.5

WPF Toolkit (http://wpf.codeplex.com/) Copyright (c) 2006-2014 Microsoft

Licence MS-PL http://wpf.codeplex.com/license

Extended WPF Toolkit 3.0

Copyright (C) 2007-2013 Xceed Software Inc.

Ce programme vous est fourni selon les termes de la licence publique Microsoft (ms-PL) telle que publiée sur http://wpftoolkit.codeplex.com/license

Pour plus de fonctionnalités, de commandes et une assistance professionnelle rapide, procurez-vous l'édition Plus sur http://xceed.com/wpf_toolkit

Restez informés : suivez @datagrid sur Twitter ou aimez http://facebook.com/datagrids

WiX Toolset

Copyright (c) Outercurve Foundation. Common Public License Version 1.0.

CLR Security

Copyright (c) Microsoft Corporation. Microsoft Limited Permissive License (MS-LPL)

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 https://stackexchange.github.io/StackExchange.Redis Copyright (c) 2014 Stack Exchange

Sous licence MIT

Newtonsoft JSON

Copyright (c) 2007 James Newton-King

Sous licence MIT.

Bibliothèque JavaScript jQuery v3.7.0

https://jquery.com/

Inclut Sizzle.js

https://sizzlejs.com/

Copyright JS Foundation et autres contributeurs

Publié sous licence MIT

https://jquery.org/license

Date : 2020-05-04T22:49Z

jQuery UI - v1.13.2 -2022 -07-14

http://jqueryui.com

Copyright jQuery Foundation et autres contributeurs ; sous licence MIT

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

http://hammerjs.github.io/

Copyright (c) 2016 Jorik Tangelder;

Sous licence MIT

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

Sous licence MIT. Voir le fichier LICENSE à la racine du projet pour plus de détails.

slick.js - 1.8.0

La licence MIT (MIT)

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

Double licence sous licences MIT ou GPL version 2.

ANNEXE : Licences référencées

Licence MIT

```
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
```



```
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
<!--NeedCopy-->
```

Licence Apache, version 2.0

```
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/


TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by
   the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all
   other entities that control, are controlled by, or are under common
   control with that entity. For the purposes of this definition,
   "control" means (i) the power, direct or indirect, to cause the
   direction or management of such entity, whether by contract or
   otherwise, or (ii) ownership of fifty percent (50%) or more of the
   outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity
   exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications,
   including but not limited to software source code, documentation
   source, and configuration files.

   "Object" form shall mean any form resulting from mechanical
   transformation or translation of a Source form, including but
   not limited to compiled object code, generated documentation,
   and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or
   Object form, made available under the License, as indicated by a
```



```
    copyright notice that is included in or attached to the work
    (an example is provided in the Appendix below).

    "Derivative Works" shall mean any work, whether in Source or Object
    form, that is based on (or derived from) the Work and for which the
    editorial revisions, annotations, elaborations, or other modifications
    represent, as a whole, an original work of authorship. For the purposes
    of this License, Derivative Works shall not include works that remain
    separable from, or merely link (or bind by name) to the interfaces of,
    the Work and Derivative Works thereof.

    "Contribution" shall mean any work of authorship, including
    the original version of the Work and any modifications or additions
    to that Work or Derivative Works thereof, that is intentionally
    submitted to Licensor for inclusion in the Work by the copyright owner
    or by an individual or Legal Entity authorized to submit on behalf of
    the copyright owner. For the purposes of this definition, "submitted"
    means any form of electronic, verbal, or written communication sent
    to the Licensor or its representatives, including but not limited to
    communication on electronic mailing lists, source code control systems,
    and issue tracking systems that are managed by, or on behalf of, the
    Licensor for the purpose of discussing and improving the Work, but
    excluding communication that is conspicuously marked or otherwise
    designated in writing by the copyright owner as "Not a Contribution."

    "Contributor" shall mean Licensor and any individual or Legal Entity
    on behalf of whom a Contribution has been received by Licensor and
    subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
    this License, each Contributor hereby grants to You a perpetual,
    worldwide, non-exclusive, no-charge, royalty-free, irrevocable
    copyright license to reproduce, prepare Derivative Works of,
    publicly display, publicly perform, sublicense, and distribute the
    Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
    this License, each Contributor hereby grants to You a perpetual,
    worldwide, non-exclusive, no-charge, royalty-free, irrevocable
    (except as stated in this section) patent license to make, have made,
    use, offer to sell, sell, import, and otherwise transfer the Work,
    where such license applies only to those patent claims licensable
    by such Contributor that are necessarily infringed by their
```



```
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
```



```
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing
      the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this
      License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS
<!--NeedCopy-->
```

Microsoft Public License (MS-PL)

```
This license governs use of the accompanying software. If you use the
```



```
    software, you accept this license. If you do not accept the license,
     do not use the software.

1. Definitions
The terms "reproduce," "reproduction," "derivative works," and "
    distribution" have the
same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or
    changes to the software.

A "contributor" is any person that distributes its contribution under
     this license.

"Licensed patents" are a contributor's patent claims that read
    directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including
    the license conditions and limitations in section 3, each
    contributor grants you a non-exclusive, worldwide, royalty-free
    copyright license to reproduce its contribution, prepare derivative
    works of its contribution, and distribute its contribution or any
    derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the
    license conditions and limitations in section 3, each contributor
    grants you a non-exclusive, worldwide, royalty-free license under
    its licensed patents to make, have made, use, sell, offer for sale,
    import, and/or otherwise dispose of its contribution in the software
     or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use
     any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents
    that you claim are infringed by the software, your patent license
    from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all
    copyright, patent, trademark, and attribution notices that are
    present in the software.

(D) If you distribute any portion of the software in source code form,
    you may do so only under this license by including a complete copy
    of this license with your distribution. If you distribute any
    portion of the software in compiled or object code form, you may
    only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it.
```



```
      The contributors give no express warranties, guarantees or
      conditions. You may have additional consumer rights under your local
       laws which this license cannot change. To the extent permitted
      under your local laws, the contributors exclude the implied
      warranties of merchantability, fitness for a particular purpose and
      non-infringement.
<!--NeedCopy-->
```