Citrix Secure Private Access - Sur site

Machine translated content

Disclaimer

Contents

Nouveautés

December 27, 2023

Décembre 2023

Citrix Secure Private Access pour les applications sur site : disponibilité générale

Citrix Secure Private Access pour les applications locales est désormais disponible dans le cadre de la version 2311 de Citrix Virtual Apps and Desktops. La solution Citrix Secure Private Access sur site améliore la posture globale de sécurité et de conformité d'une organisation en permettant de fournir facilement un accès réseau Zero Trust aux applications basées sur un navigateur (applications Web internes et applications SaaS) en utilisant StoreFront comme portail d'accès unifié aux applications Web et SaaS, ainsi qu'aux applications et bureaux virtuels intégrés à Citrix Workspace. La solution est compatible avec les versions existantes de NetScaler et StoreFront sans aucune modification des versions. Pour plus de détails, consultez la section Secure Private Access pour déploiement sur site.

Programme d'installation d'accès privé sécurisé intégré à Citrix Virtual Apps and Desktops

Le programme d'installation de Secure Private Access est intégré au Desktop Delivery Controller (DDC) et peut désormais être installé à l'aide de la ligne de commande et de l'interface graphique. Pour plus de détails, consultez la section Installation des composants principaux .

Problèmes connus

December 27, 2023

La solution Citrix Secure Private Access pour locaux présente les problèmes connus suivants qui devraient être résolus dans les prochaines versions.

Configurations des contrôleurs de domaine

- L'approbation unidirectionnelle ou bidirectionnelle avec le type de confiance « Forêt » entre les domaines de différentes forêts AD n'est pas prise en charge.

  Par exemple, si les domaines .com et b.com se trouvent dans deux forêts AD différentes et que SPA est installé sur une machine sur laquelle le domaine est joint à a.com/b.com, les autres utilisateurs du domaine ne peuvent pas accéder aux applications publiées par SPA.

- Si le domaine de la machine sur lequel Secure Private Access for on-premises est installé est différent de celui de l'administrateur connecté à Secure Private Access, vous devez procéder comme suit :
  - Ajoutez un compte de service de domaine différent comme identifiant dans le pool d'applications IIS pour le service Secure Private Access Admin et le service Runtime.
- Le suffixe UPN alternatif n'est pas pris en charge par la connexion Secure Private Access for Intranet (StoreFront) et l'énumération des applications Internet/Extranet (passerelle).
- Les groupes distribués ne sont pas pris en charge dans Secure Private Access. Par conséquent, les politiques ne peuvent pas rechercher de groupes distribués pour ajouter des conditions relatives aux utilisateurs et aux groupes.
- Secure Private Access ne capture pas les détails du domaine dans la console d'administration ou le service. Par conséquent, il dépend entièrement du domaine fourni par l'utilisateur. Par conséquent, si le domaine correspondant n'est pas accessible ou si le nom de domaine n'est pas valide, ce domaine n'est pas pris en charge.

NetScaler Gateway

Le serveur virtuel SSL avec configuration de profil SSL n'est pas pris en charge dans le scénario suivant.

- Le client utilise NetScaler Gateway 13.1—48.47 et versions ultérieures ou 14.1—4.42 et versions ultérieures.
- La bascule `ns_vpn_enable_spa_onprem` est activée.

Solution :

Liez les paramètres SSL configurés dans le profil SSL directement au serveur virtuel SSL ou désactivez la bascule `ns_vpn_enable_spa_onprem`.

Pour plus de détails sur cette option, voir Prise en charge des balises d'accès intelligentes.

RFWeb/Workspace pour le Web

RFWeb/Workspace pour Web n'est pas pris en charge. Bien que les applications soient énumérées, le lancement de l'application peut échouer.

Icônes de l'application

Seul le format d'icône ICO est pris en charge. Les formats PNG, JPEG et autres ne sont pas pris en charge.

Gestion de l'administration

Les modifications apportées au rôle RBAC de l'administrateur ne sont prises en compte qu'après l'invalidation de la session en cours (par déconnexion ou expiration du jeton).

Mises à niveau

La mise à niveau « Build-to-Build » n'est pas prise en charge. Secure Private Access pour déploiement sur site vous invite à supprimer l'installation existante et à la réinstaller dans le cadre d'une mise à niveau intégrée.

StoreFront

- Dans **Stores > Configurer Unified Experience**, le récepteur par défaut pour Website doit être configuré sur /Citrix/<StoreName>Web. Dans les versions précédentes de StoreFront, le récepteur par défaut pour Website était défini sur une valeur vide, ce qui ne fonctionnait pas pour Secure Private Access. En outre, la version précédente de l'interface utilisateur du récepteur est affichée sur le client.
- Si vous utilisez les versions 2308 ou antérieures de StoreFront, la page **Stores > Manage Delivery Controller** affiche le type de plug-in Secure Private Access sous la forme **XenMobile**. Cela n'a aucune incidence sur les fonctionnalités.

Logging

- La génération de packs de support pour le cluster n'est pas prise en charge.
- Les dossiers de journaux des services d'administration et d'exécution ne doivent pas être supprimés. Secure Private Access ne peut pas être recréé si ces dossiers sont supprimés.

Configuration requise du compte administrateur pour installer Secure Private Access

- Pour installer Secure Private Access, vous devez être connecté avec un compte d'administrateur de machine local.
- Pour configurer Secure Private Access, vous devez vous connecter à la console d'administration Secure Private Access avec un utilisateur du domaine qui est également un administrateur de machine local pour la machine sur laquelle Secure Private Access est installé.
- Une fois la configuration terminée, cet utilisateur devient le premier administrateur de Secure Private Access et peut ensuite ajouter d'autres administrateurs.
- Pour gérer Secure Private Access après la configuration, vous devez vous connecter à la console d'administration Secure Private Access avec un compte administrateur Secure Private Access.

Restrictions relatives

Les restrictions de sécurité associées à une application ne fonctionnent pas si un domaine associé initialement publié est remplacé par un autre domaine.

Par exemple, vous créez une application avec un domaine associé en tant que `edition.test.com`et vous appliquez des restrictions d'impression et un filigrane à l'application. Les restrictions de sécurité sont appliquées lors de l'accès à l'URL de l'application. Toutefois, si vous modifiez la même application et remplacez le domaine `edition.test.com` associé par , les `*.1800flowers.com` restrictions de sécurité ne sont pas appliquées lors de l'accès à la nouvelle URL de l'application.

Console d'administration

La **page Modifier**l'application ne se ferme pas automatiquement lorsque la **page Modifier**l'application (**Accès privé sécurisé > Applications > Modifier l'application) **d'une application publiée ne se ferme pas après la modification d'une entrée de domaine associée.

Par exemple, si le domaine associé que vous avez saisi lors de la création d'une application était `www.example.com`. Une fois l'application publiée, vous remplacez le domaine `www.example.com` associé par `abc.com`, puis vous cliquez sur **Enregistrer** . La page **Modifier l'application** ne se ferme pas, bien que l'application ait été correctement mise à jour.

Affichage du programme d'installation dans la page Désinstaller ou modifier un programme

Lorsque vous mettez à niveau Secure Private Access de 2308 à 2311 à l'aide du fichier ISO, la page Désinstaller **ou modifier un programme** (**Panneau de configuration > Programmes > Programmes et fonctionnalités**) affiche deux entrées pour le programme d'installation de Secure Private Access au lieu de remplacer l'entrée initiale.

- **Applications et bureaux virtuels Citrix 7 2311**
- **Citrix Virtual Apps and Desktops 7 2308 - Accès privé sécurisé**

Vous pouvez désinstaller le programme d'installation de la version préliminaire en sélectionnant **Citrix virtual apps and desktops 7 2308 - Secure private access** .

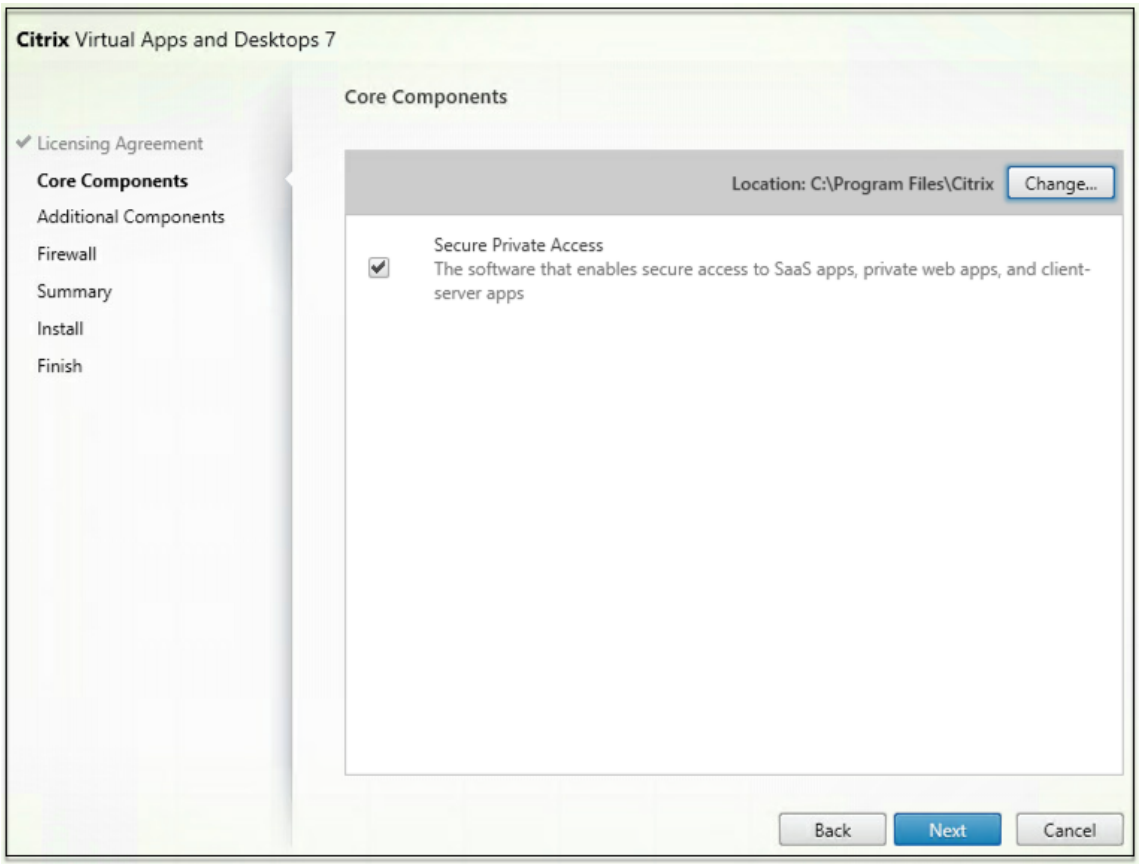
> **Remarque :**
>
> Ce problème n'est pas observé lorsque le programme d'installation autonome de Secure Private Access 2308 est mis à niveau à l'aide du programme d'installation autonome 2311.

Programme d'installation Secure Private Access

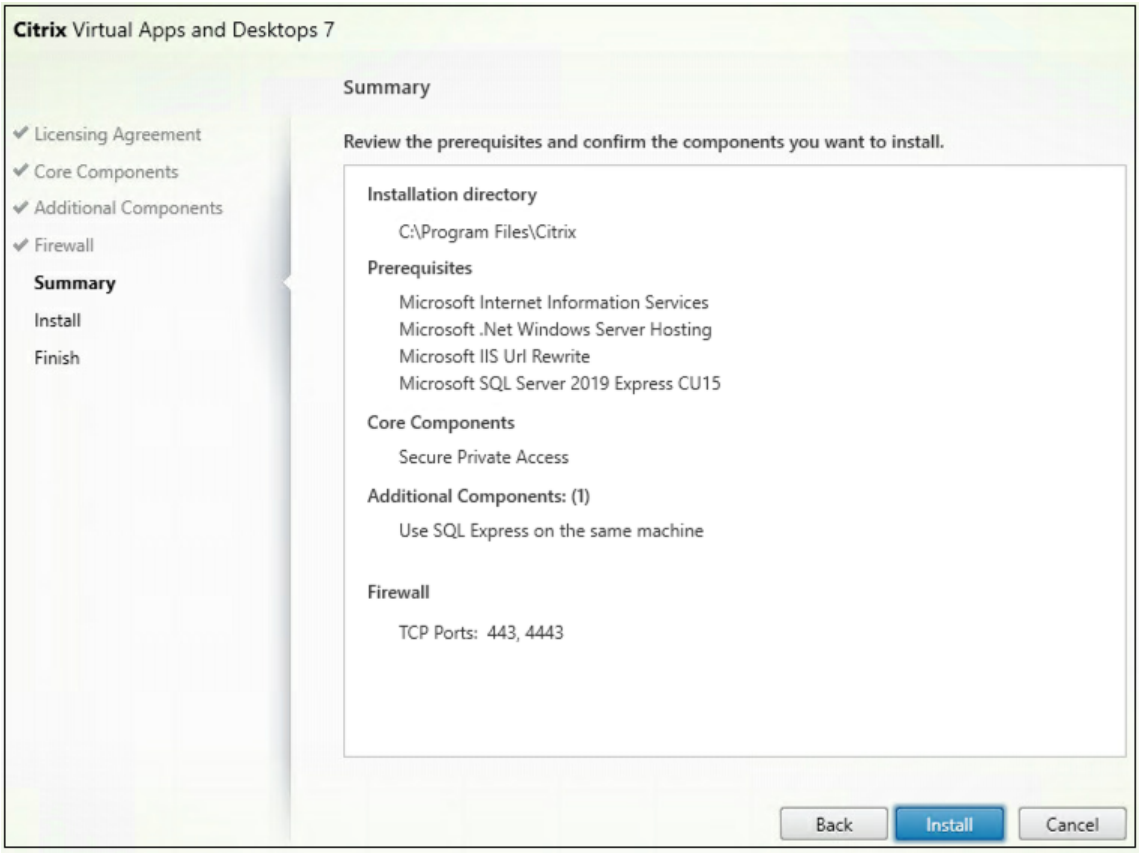
February 16, 2024

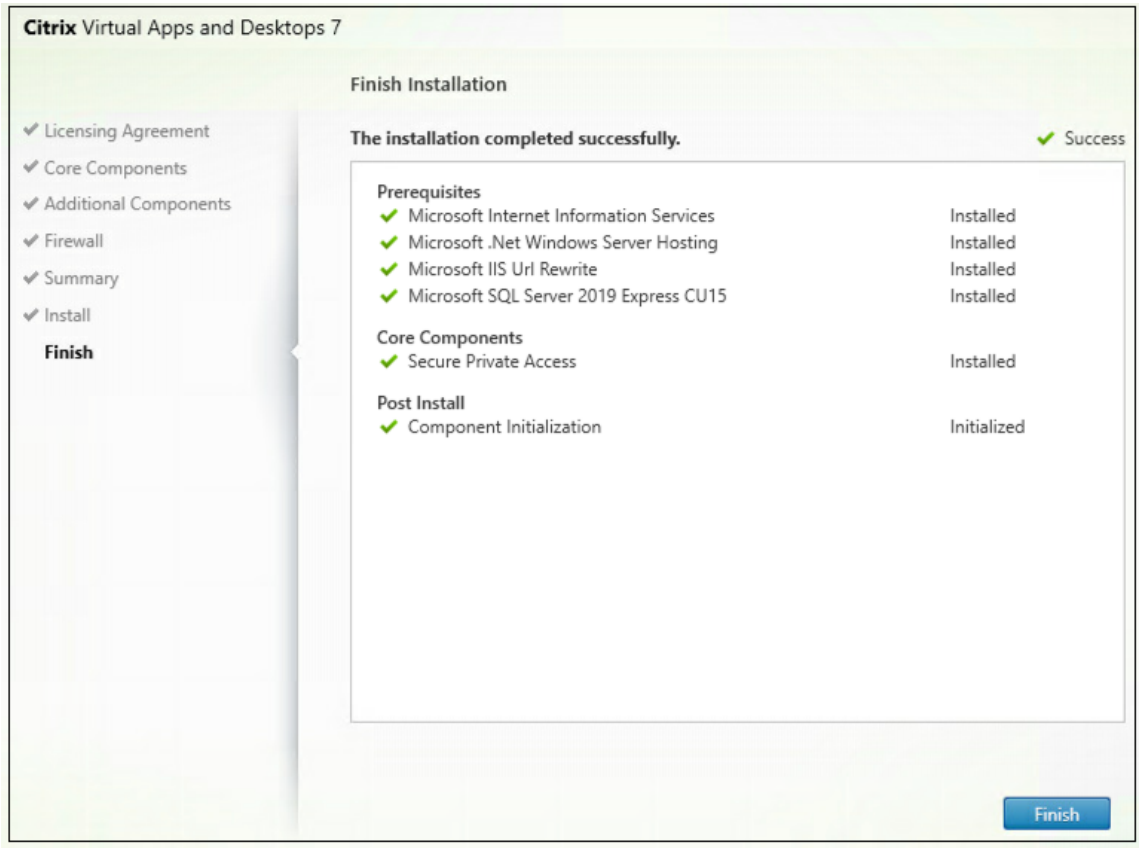
1. Téléchargez le programme d'installation de Citrix Secure Private Access depuis https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.
2. Exécutez le fichier .exe en tant qu'administrateur sur une machine associée à un domaine.

   > **Remarque :**
   >
   > à des fins de POC, il est recommandé d'installer Secure Private Access sur la même machine que celle sur laquelle StoreFront est installé.

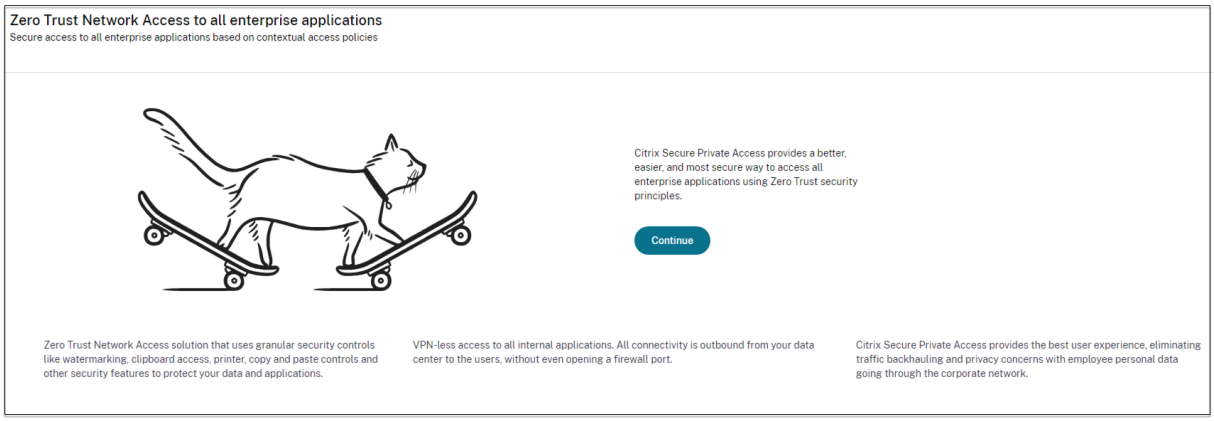


3. Suivez les instructions qui s'affichent à l'écran pour terminer l'installation.

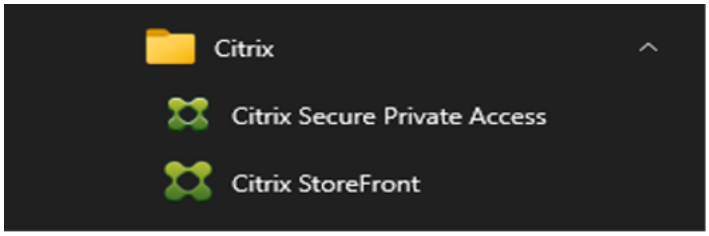




Une fois l'installation terminée, la console d'administration de la première installation s'ouvre automatiquement dans la fenêtre du navigateur par défaut. Vous pouvez cliquer sur **Continuer** pour configurer Secure Private Access.



Vous pouvez également voir le raccourci Secure Private Access dans le menu Démarrer du bureau (**Citrix > Citrix Secure Private Access)**.



Pour plus d'informations, consultez les rubriques suivantes :

- Installer les composants principaux
- Installer à l'aide de la ligne de commande

SSO vers la console d'administration

Il est recommandé de configurer l'authentification Kerberos pour le navigateur que vous utilisez pour la console d'administration Secure Private Access. En effet, Secure Private Access utilise l'authentification Windows intégrée (IWA) pour son authentification d'administrateur.

Si l'authentification Kerberos n'est pas définie, le navigateur vous invite à saisir vos informations d'identification lorsque vous accédez à la console d'administration Secure Private Access.

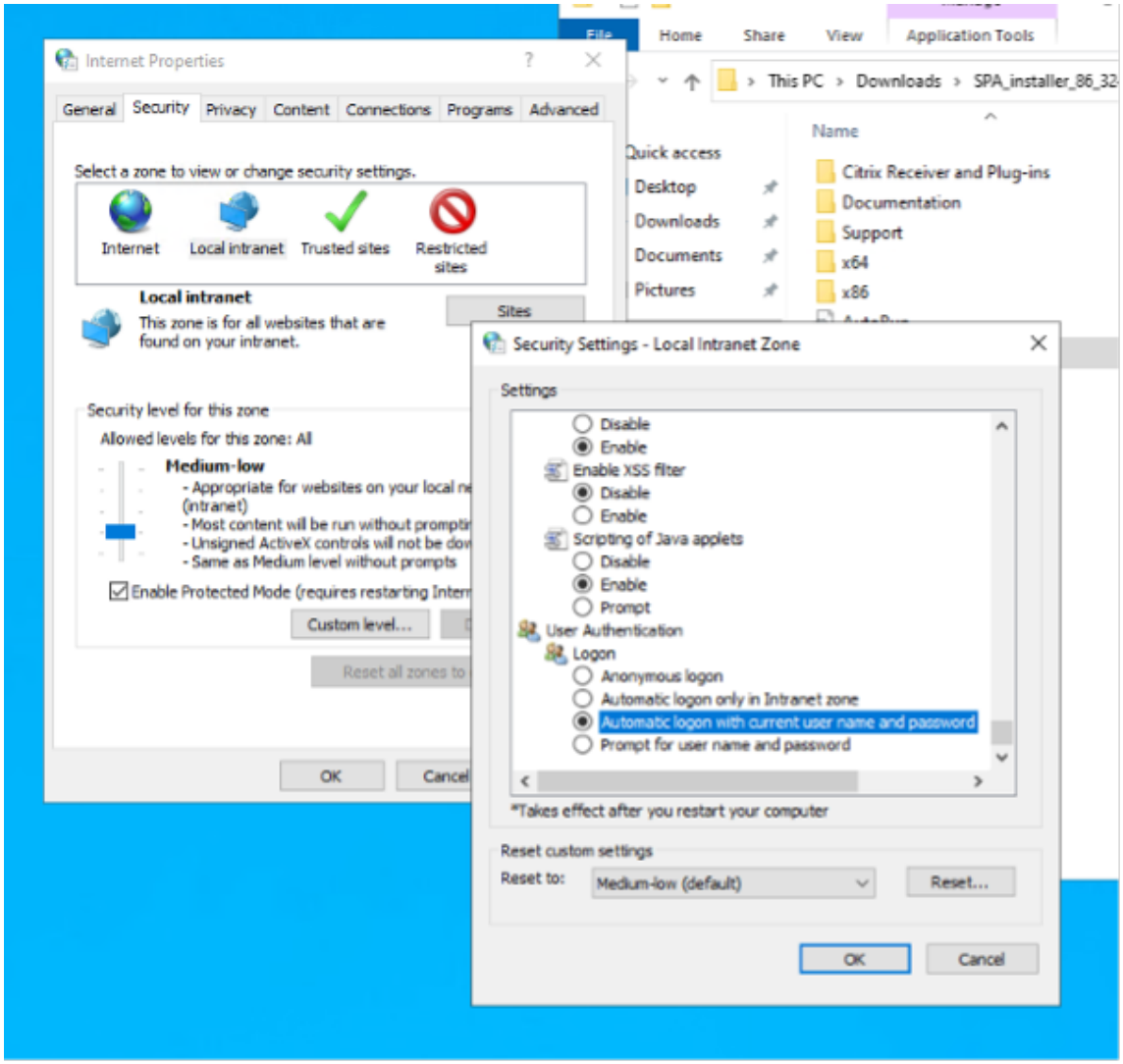
- Si vous entrez vos informations d'identification, vous activez l'authentification Windows intégrée (IWA).
- Si vous ne saisissez pas vos informations d'identification, la page de connexion Secure Private Access s'affiche.

Vous devez vous connecter à la console d'administration pour poursuivre la configuration de Secure Private Access. Vous pouvez configurer l'accès privé sécurisé avec n'importe quel utilisateur appartenant au même domaine que la machine d'installation, s'il dispose de privilèges d'administrateur local sur la machine d'installation.

Pour les navigateurs Google Chrome et Microsoft Edge, effectuez les étapes suivantes pour activer Kerberos.

1. Ouvrez les **options Internet**.
2. Sélectionnez l'onglet **Sécurité** et cliquez sur **Zone intranet locale**.
3. Cliquez sur **Sites** et ajoutez l'URL Secure Private Access.

   Vous pouvez également utiliser un caractère générique si vous prévoyez d'installer Secure Private Access sur plusieurs machines. Par exemple, `"https://*.fabrikam.local"`.
4. Cliquez sur **Personnaliser le niveau**, puis dans **Authentification utilisateur > Connexion**, sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuels**.



Remarque :

- Si vous utilisez des sessions Chrome Incognito, créez une clé de registre DWORD Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AmbientAuthenticationInPrivateModes et définissez-la sur la valeur 1.
- Vous devez redémarrer toutes les fenêtres Chrome (y compris les fenêtres autres que la navigation privée) avant que Kerberos ne soit activé pour le mode navigation privée.
- Pour les autres navigateurs, consultez la documentation du navigateur spécifique sur l'authentification Kerberos.

Étapes suivantes

- Configurer Secure Private Access
- Configurer NetScaler Gateway

- Configurer les applications
- Configuration des stratégies d'accès pour les applications

Mise à niveau de la base de données à l'aide

December 27, 2023

Vous pouvez utiliser l'outil de configuration d'administration pour télécharger les scripts de mise à niveau de la base de données pour le plug-in Secure Private Access.

1. Ouvrez le PowerShell ou la fenêtre d'invite de commande avec les privilèges d'administrateur.
2. Remplacez le répertoire par le dossier Admin \ AdminConfigTool dans le dossier d'installation de Secure Private Access (par exemple, cd « C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool »).
3. Exécutez la commande suivante :

   ```
   .\AdminConfigTool.exe /DOWNLOAD_UPGRADE_DB_SCRIPTS <output folder
   >
   ```

Directives de dimensionnement

February 16, 2024

Exigences de stockage des bases de données

La majeure partie de l'espace de stockage de la base de données est utilisée par les journaux. La consommation d'espace de stockage par l'application et la configuration des politiques sont négligeables par rapport aux journaux.

Le tableau suivant affiche les besoins de stockage du serveur en fonction de paramètres tels que les sessions utilisateur, les journaux, l'énumération des applications par utilisateur et par jour.

Sessions pour les utilisateurs	Énumération des applications par utilisateur et par jour	Accès à l'application par utilisateur et par jour	Accès total à l'application par jour	Stockage consommé par jour	Période de conservation des journaux en jours	Utilisation totale de l'espace de stockage pendant la période de conservation des journaux (7 jours)
1000	20	100	100000	2.5 GB	7	17.5 GB
1000	10	50	50000	1.27 GB	7	9 GB

Remarque :

- Les mesures sont dérivées sur la base de l'hypothèse que le nettoyage des événements des journaux est désactivé et que la période de conservation des journaux est fixée à 7 jours.
- Par défaut, les journaux sont conservés pendant 90 jours ou jusqu'à 100 000 événements de journal sont conservés en fonction des paramètres configurés. Ces paramètres sont disponibles dans le fichier appsettings.json du service Secure Private Access Runtime et peuvent être modifiés selon les besoins. Pour plus de détails, voir Paramètres de conservation des journaux d'événements .

Directives de déploiement

Le tableau suivant affiche les exigences de taille de base de données en fonction de paramètres tels que l'accès simultané aux applications, les sessions utilisateur, l'énumération des applications par minute et les processeurs utilisés par Secure Private Access.

Sessions utilisateur simultanées avec accès aux applications	Énumération des applications par minute	Mémoire Secure Private Access en Go	Processeurs à accès privé sécurisé	Stockage en Go	Remarques
< 20 (à des fins PoC)	2	4 GB	2	40 GB*	À des fins de PoC, le SPA peut être déployé sur la même machine que StoreFront sans aucune modification des spécifications des machines virtuelles existantes.
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	2 nœuds SPA ou plus peuvent être déployés pour de meilleures performances

Remarque :

- * Le stockage est principalement utilisé par les journaux CDF. Par défaut, Secure Private Access conserve 600 fichiers journaux de survol, chaque fichier ayant une taille de 10 Mo. Ainsi, si les services d'administration et d'exécution de Secure Private Access sont exécutés sur la même machine, l'utilisation maximale du stockage par les journaux est de 12 Go. SQL Express peut également être installé sur la machine virtuelle locale à des fins de PoC.
- ** Pour ce profil de charge et supérieur, il est recommandé de déployer Secure Private Access sur un serveur dédié au lieu de co-héberger avec StoreFront, sauf si la version de NetScaler Gateway est inférieure à 13.0 ou inférieure à 13.1-48.47.

> - *** Il est recommandé d'utiliser au moins deux clusters de nœuds Secure Private Access pour une telle charge car certains problèmes de performances sont connus. Ces problèmes devraient être résolus dans les prochaines versions.

Configuration des autres composants

Composant	Processeurs virtuels	Memory
SQL Server	4	16 Go
Storefront	4	8 Go
Active Directory	8	16 Go

Configurer Secure Private Access

February 16, 2024

Vous pouvez configurer Secure Private Access en créant un nouveau site ou en rejoignant un site existant. Dans les deux scénarios, vous pouvez utiliser la console d'administration Web pour configurer l'environnement Secure Private Access.

- Configurer Secure Private Access en créant un nouveau site
- Configurez Secure Private Access en rejoignant un site existant

Conditions préalables

- Vous devez vous connecter à la console d'administration Secure Private Access avec un utilisateur du domaine qui est également un administrateur de machine local pour la machine sur laquelle Secure Private Access est installé.
- Le serveur de base de données SQL doit être installé avant de créer un site.

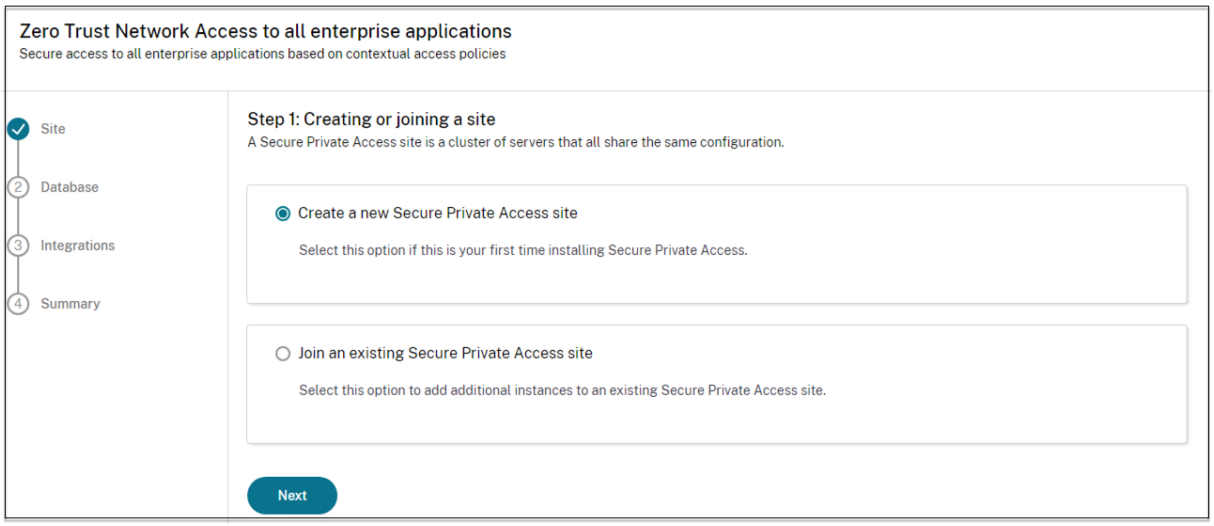
Configurer Secure Private Access en créant un nouveau site

Étape 1 : configurer un site Secure Private Access

Un site est le nom de votre déploiement Secure Private Access. Vous pouvez créer un site ou rejoindre un site existant.

1. Lancez la console d'administration Web à Secure Private Access.
2. Sur la page **Création ou adhésion à un site**, l'option **Créer un nouveau site Secure Private Access** est sélectionnée par défaut.

3. Cliquez sur **Suivant**.



Lorsque vous choisissez de créer un site, vous devez configurer automatiquement ou manuellement une base de données pour le nouveau site, car la base de données correspondant au nom du site peut ne pas être disponible dans la configuration.

Étape 2 : configurer les bases de données

Vous devez créer une base de données pour le nouveau site Secure Private Access. Cela peut être fait manuellement ou automatiquement.

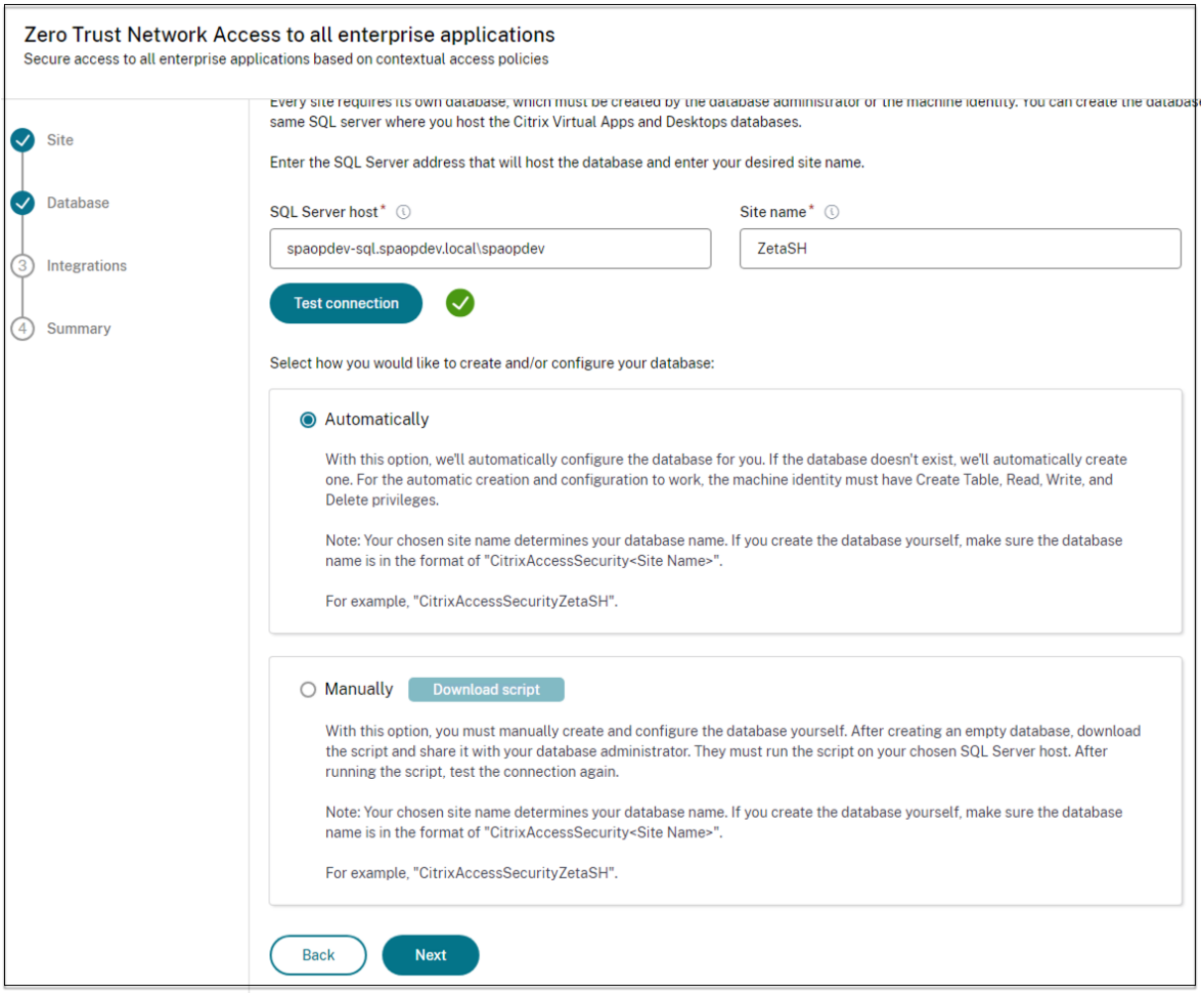
1. Dans **SQL Server Host**, entrez le nom d'hôte du serveur. Par exemple, `sql1.fabrikam.local\citrix`.

   Vous pouvez spécifier une adresse de base de données dans l'un des formats suivants :

   - NomServeur
   - NomServeur\NomInstance
   - Nom du serveur, numéro de port

   Pour plus d'informations, consultez la section Bases de données.

2. Dans **Site**, tapez le nom du site Secure Private Access.
3. Cliquez sur **Tester la connectivité** pour vérifier que l'instance du serveur SQL est valide et également pour confirmer que la base de données spécifiée existe pour le site.



> **Remarque :**

- Si aucun serveur SQL n'est disponible pour le site, le contrôle de connectivité échoue.
- Si un serveur SQL est disponible mais que la base de données n'existe pas, le contrôle de connectivité est réussi. Toutefois, un message d'avertissement s'affiche.
- Secure Private Access utilise l'authentification Windows à l'aide de l'identité de la machine pour s'authentifier auprès d'un serveur SQL.

Configuration automatique :

- Vous pouvez utiliser l'option de **configuration automatique** uniquement si l'identité de la machine possède les privilèges de base de données requis.
- Si aucune base de données n'existe à l'adresse spécifiée, une base de données est automatiquement créée.
- Lorsque vous créez une base de données, assurez-vous qu'elle est vide mais qu'elle possède les privilèges de base de données requis. Pour plus de détails sur les privilèges, voir Autorisations requises pour configurer les bases de données.

Configuration manuelle :

Vous pouvez utiliser l'option **de configuration manuelle** pour configurer les bases de données.

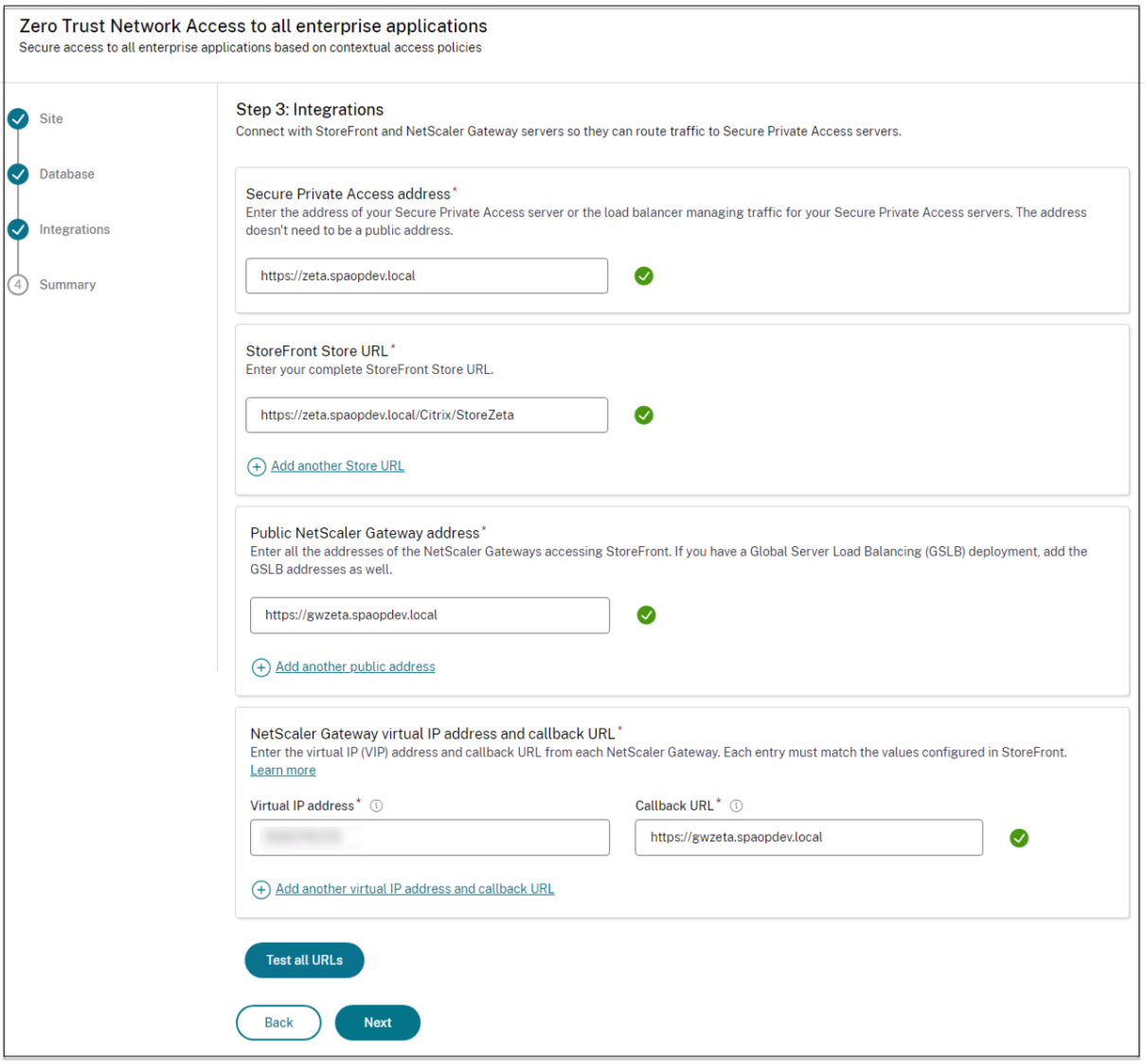
Dans la configuration manuelle, vous devez d'abord télécharger les scripts, puis les exécuter sur le serveur de base de données que vous avez spécifié dans le champ **SQL Server Host** .

> **Remarque :**
>
> La création de la base de données peut échouer si la machine ne dispose pas des autorisations READ, WRITE, UPDATE pour créer des tables dans la base de données sur le serveur SQL. Vous devez activer les autorisations appropriées sur la machine. Pour plus de détails, voir Autorisations requises pour configurer les bases de données.

Étape 3 : intégrer les serveurs StoreFront et NetScaler Gateway

Vous devez spécifier les détails des serveurs StoreFront et NetScaler Gateway pour connecter Secure Private Access aux serveurs StoreFront et NetScaler Gateway. Cette connexion doit être établie pour permettre à StoreFront et à NetScaler Gateway d'acheminer le trafic vers Secure Private Access.

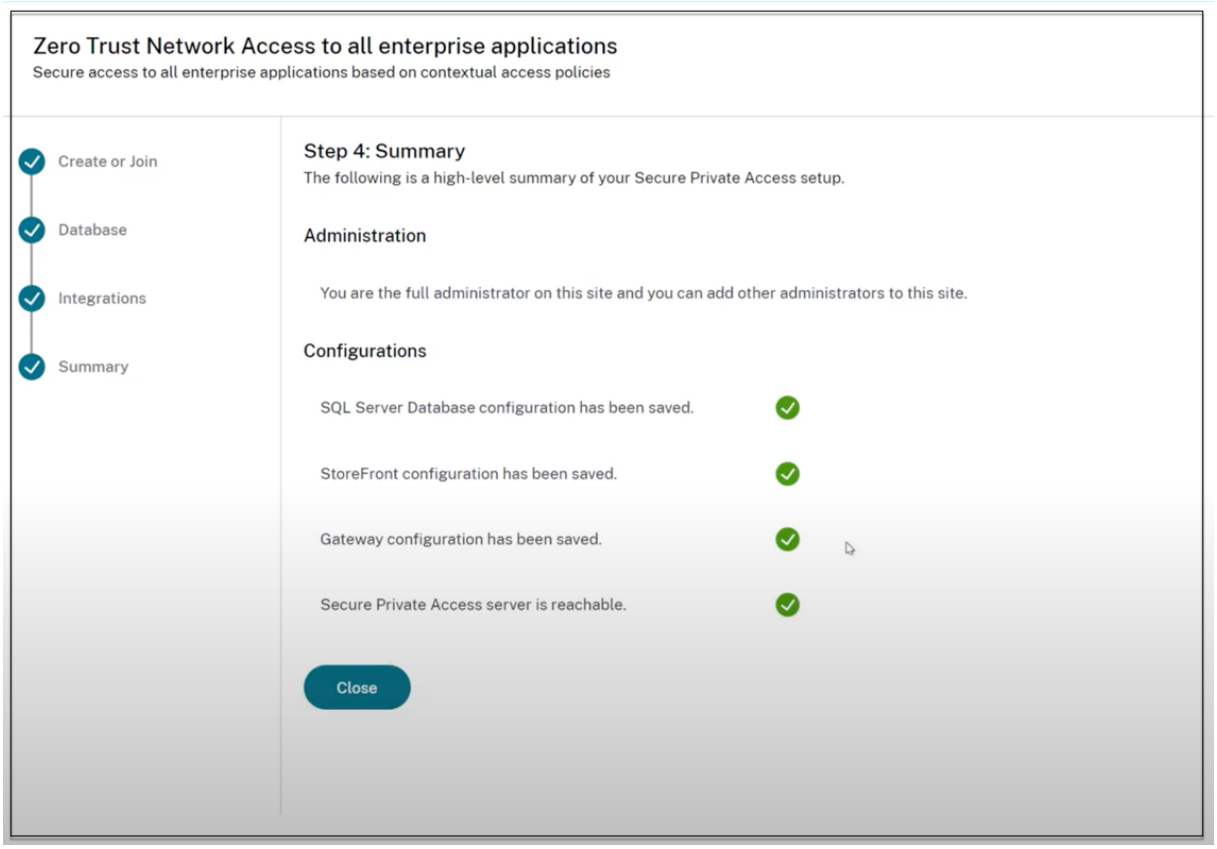
1. Entrez les détails suivants.
    - **Adresse du serveur Secure Private Access**. Par exemple, `https://secureaccess.domain.com`.
    - **URL du magasin StoreFront**. Par exemple, `https://storefront.domain.com/Citrix/StoreMain`.
    - **Adresse de passerelle publique** : URL de NetScaler Gateway. Par exemple, `https://gateway.domain.com`.
    - **Adresse de rappel de la passerelle** : cette URL doit être identique à celle configurée dans StoreFront. Par exemple, `https://gateway.domain.com`.
    - **Gateway VIP** : cette adresse IP virtuelle doit être identique à celle configurée dans StoreFront pour les rappels.
2. Cliquez sur **Valider toutes les URL**.
3. Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.



Étape 4 : Résumé de la configuration

Une fois la configuration terminée, une validation est effectuée pour s'assurer que les serveurs configurés sont accessibles. En outre, une vérification est effectuée pour s'assurer que le serveur Secure Private Access est accessible.

Si la page récapitulative de la configuration affiche des erreurs, voir Résolution des erreurs pour plus de détails. Si cela ne résout pas le problème, contactez le support Citrix.



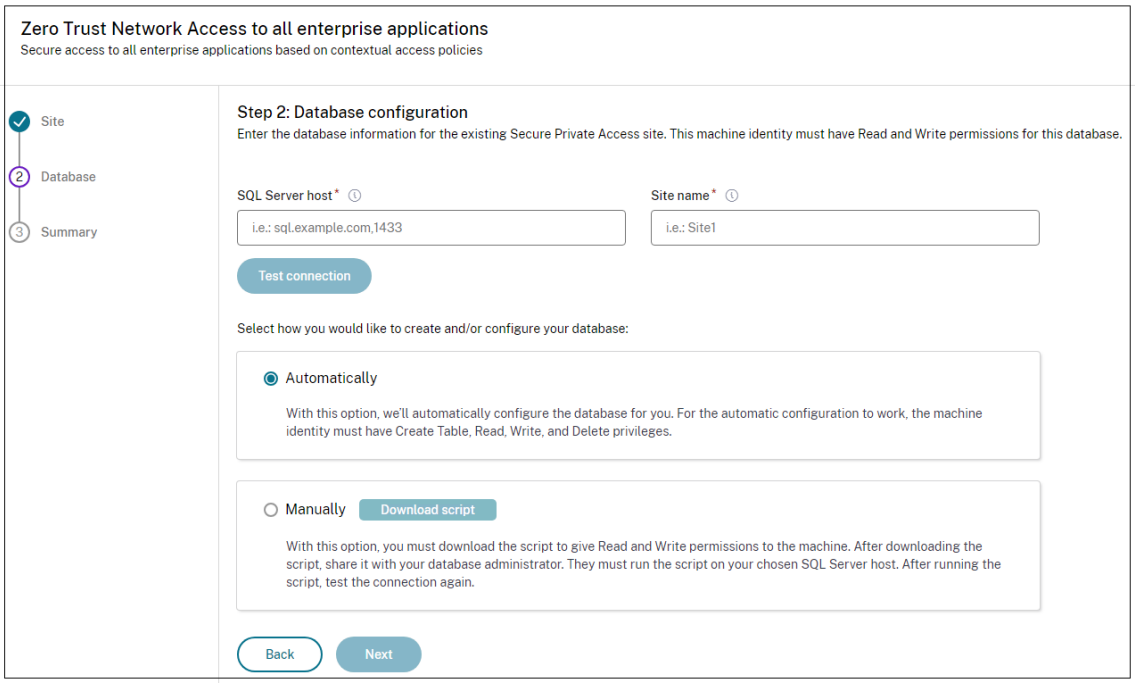
Remarque :

- Après avoir configuré l'environnement, vous pouvez modifier les paramètres dans Paramètres > Intégrations dans la console d'administration Web.
- L'administrateur qui installe Secure Private Access pour la première fois bénéficie d'une autorisation complète. Cet administrateur peut ensuite ajouter d'autres administrateurs à la configuration. Vous pouvez consulter la liste des administrateurs **dans Paramètres > Administrateurs**.
- Vous pouvez également ajouter des groupes d'administrateurs afin que l'accès soit activé pour tous les administrateurs de ce groupe.

Pour plus de détails, voir Gérer les paramètres après l'installation.

Configurez Secure Private Access en rejoignant un site existant

1. Sur la page **Création ou adhésion à un site**, sélectionnez **Rejoindre un site existant**, puis cliquez sur **Suivant**.



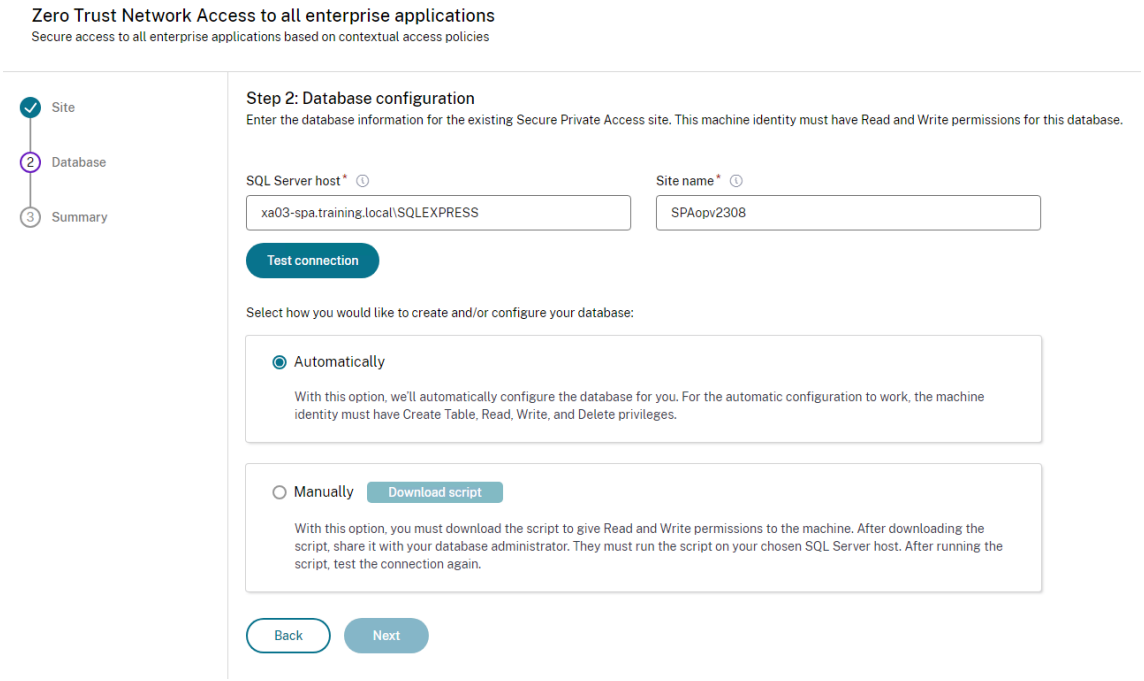
2. Dans **SQL Server Host**, entrez le nom d'hôte du serveur. Assurez-vous qu'une base de données correspondant au nom du site que vous entrez est déjà présente dans le serveur SQL que vous avez sélectionné. Vous pouvez spécifier une adresse de base de données dans l'un des formats suivants :

   - NomServeur
   - NomServeur\NomInstance
   - Nom du serveur, numéro de port

   Pour plus d'informations, consultez la section Bases de données.

3. Dans **Site**, tapez le nom du site Secure Private Access.

4. Cliquez sur **Tester la connectivité** pour vérifier que l'instance de SQL Server est valide et également pour confirmer que le site spécifié existe dans la base de données.



S'il n'existe aucune base de données correspondante pour le site, le contrôle de connectivité échoue.

5. Cliquez sur **Enregistrer**.

Le contrôle de validation de la configuration a pour but de s'assurer que le serveur de base de données SQL est configuré et que le serveur Secure Private Access est accessible.

Prochaines étapes

- Configurer NetScaler Gateway
- Configurer les applications
- Configuration des stratégies d'accès pour les applications

Configurer NetScaler Gateway

February 16, 2024

> **Important :**
>
> nous vous recommandons de créer des instantanés NetScaler ou d'enregistrer la configuration NetScaler avant d'appliquer ces modifications.

1. Téléchargez le script depuis https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html.

   Pour créer un nouveau NetScaler Gateway, utilisez *ns_gateway_secure_access.sh*.
   Pour mettre à jour un NetScaler Gateway existant, utilisez *ns_gateway_secure_access_update.sh*.

2. Téléchargez ces scripts sur la machine NetScaler. Vous pouvez utiliser l'application WinSCP ou la commande SCP. Par exemple, *`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*.

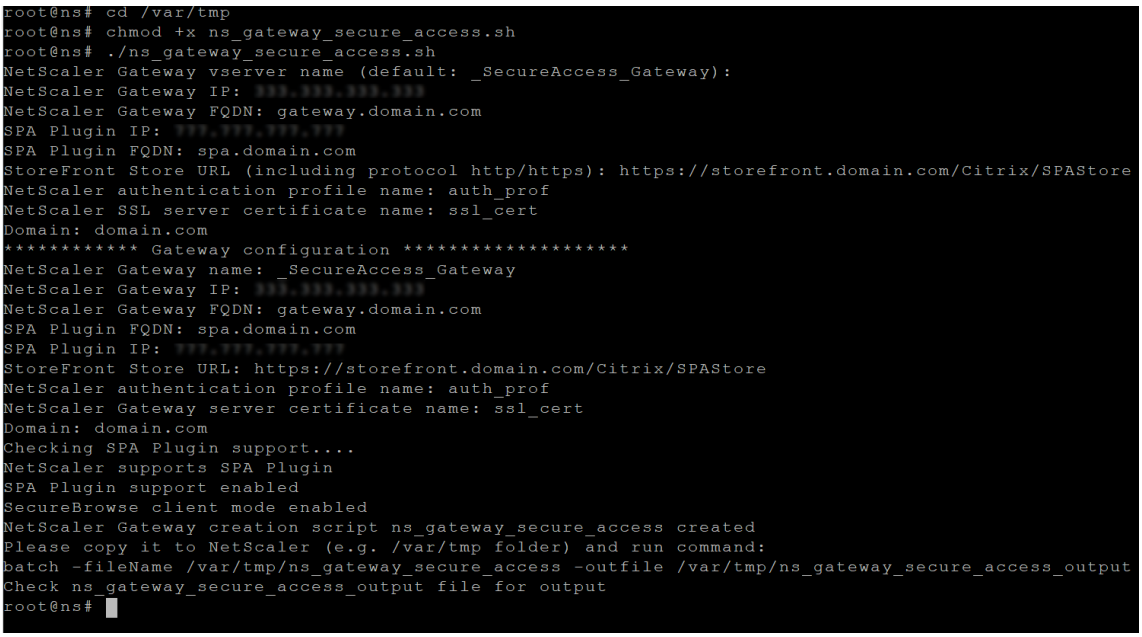
   > **Remarque :**
   >
   > - Il est recommandé d'utiliser le dossier NetScaler /var/tmp pour stocker les données temporaires.
   > - Assurez-vous que le fichier est enregistré avec des fins de ligne LF. FreeBSD ne supporte pas le CRLF.
   > - Si vous voyez l'erreur `-bash: /var/tmp/ns_gateway_secure_access.sh : /bin/sh^M: bad interpreter: No such file or directory`, cela signifie que les fins de ligne sont incorrectes. Vous pouvez convertir le script à l'aide de n'importe quel éditeur de texte enrichi, tel que Notepad++.

3. Connectez-vous à NetScaler en SSH et passez au shell (tapez « shell » sur NetScaler CLI).

4. Rendez le script chargé exécutable. Pour ce faire, utilisez la commande chmod.

   ```
   chmod +x /var/tmp/ns_gateway_secure_access.sh
   ```

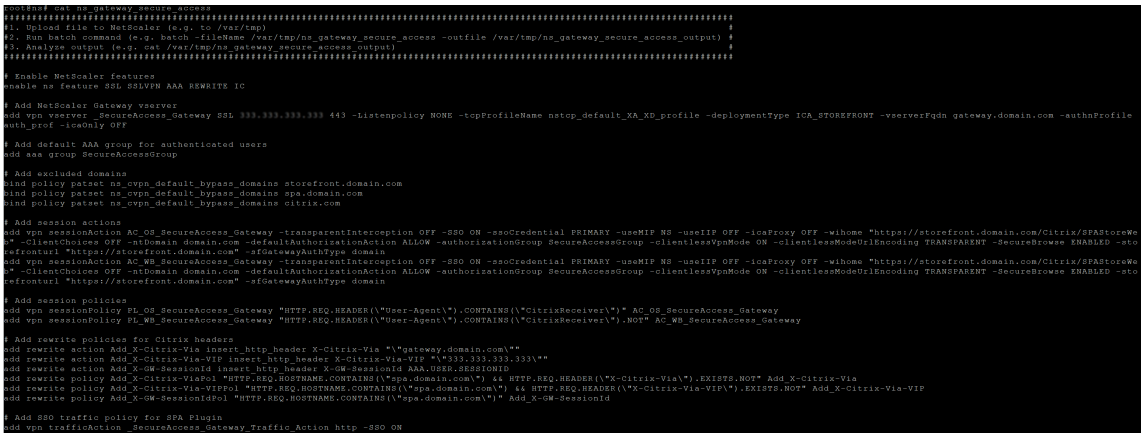
5. Exécutez le script chargé sur le shell NetScaler.

6. Entrez les paramètres requis. Pour la liste des paramètres, consultez la section Prérequis.

Pour le profil d'authentification et le certificat SSL, vous devez fournir des noms sur NetScaler.

Un nouveau fichier contenant plusieurs commandes NetScaler (la valeur par défaut est var/tmp/ns_gateway_secure_access) est généré.



7. Passez à la CLI NetScaler et exécutez les commandes NetScaler résultantes à partir du nouveau fichier à l'aide de la commande batch. Par exemple, `batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output`

   NetScaler exécute les commandes du fichier une par une. Si une commande échoue, elle passe à la commande suivante.

   Une commande peut échouer si une ressource existe ou si l'un des paramètres saisis à l'étape 6 est incorrect.

8. Assurez-vous que toutes les commandes sont correctement exécutées.

> **Remarque :**
>
> en cas d'erreur, NetScaler exécute toujours les commandes restantes et crée/met à jour/lie partiellement les ressources. Par conséquent, si vous constatez une erreur inattendue en raison de l'inexactitude de l'un des paramètres, il est recommandé de recommencer la configuration depuis le début.

Configurer Secure Private Access sur NetScaler Gateway avec la configuration existante

Vous pouvez également utiliser les scripts sur un NetScaler Gateway existant pour prendre en charge Secure Private Access. Toutefois, le script ne met pas à jour les éléments suivants :

- Serveur virtuel NetScaler Gateway existant
- Actions de session existantes et stratégies de session liées à NetScaler Gateway

Assurez-vous de passer en revue chaque commande avant de l'exécuter et de créer des sauvegardes de la configuration de la passerelle.

Paramètres du serveur virtuel NetScaler Gateway

Lorsque vous ajoutez ou mettez à jour le serveur virtuel NetScaler Gateway existant, assurez-vous que les paramètres suivants sont définis sur les valeurs définies.

tcpProfileName: nstcp_default_XA_XD_profile
deploymentType: ICA_STOREFRONT
icaOnly: OFF

Exemples :

Pour ajouter un serveur virtuel :

```
`add vpn vserver _SecureAccess_Gateway SSL 192.0.2.210 443 -
   Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
   deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
   authnProfile auth_prof_name -icaOnly OFF`
```

Pour mettre à jour un serveur virtuel :

```
`set vpn vserver  _SecureAccess_Gateway -icaOnly OFF`
```

Pour plus de détails sur les paramètres du serveur virtuel, consultez VPN-SessionAction.

Actions de session NetScaler Gateway

L'action de session est liée à un serveur virtuel de passerelle avec des stratégies de session. Lorsque vous créez une action de session, assurez-vous que les paramètres suivants sont définis sur les valeurs définies.

- `transparentInterception`: OFF
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: OFF
- `wihome`: `"https://storefront.mydomain.com/Citrix/MyStoreWeb"` - remplacer par l'URL réelle du magasin
- `ClientChoices`: OFF
- `ntDomain`: mydomain.com - utilisé pour le SSO
- `defaultAuthorizationAction`: ALLOW

- authorizationGroup: SecureAccessGroup (assurez-vous que ce groupe est créé, il est utilisé pour lier les stratégies d'autorisation spécifiques à Secure Private Access)
- clientlessVpnMode: ON
- clientlessModeUrlEncoding: TRANSPARENT
- SecureBrowse: ENABLED
- Storefronturl: "https://storefront.mydomain.com"
- sfGatewayAuthType: domain

Exemples :

Pour ajouter une action de session :

```
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy
 OFF -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb"-
ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
 ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

Pour mettre à jour une action de session :

```
set vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON
```

Pour plus de détails sur les paramètres d'action de session, consultez https://developer-docs.netscaler.com/en-us/adc-command-reference-int/13-1/vpn/vpn-sessionaction.

Compatibilité avec les applications ICA

La passerelle NetScaler Gateway créée ou mise à jour pour prendre en charge le plug-in Secure Private Access peut également être utilisée pour énumérer et lancer des applications ICA. Dans ce cas, vous devez configurer le Secure Ticket Authority (STA) et le lier à NetScaler Gateway.
Remarque : le serveur STA fait généralement partie du déploiement de Citrix Virtual Apps and Desktops DDC.

Pour plus de détails, consultez les rubriques suivantes :

- Configuration de la Secure Ticket Authority sur NetScaler Gateway
- Questions fréquentes : Citrix Secure Gateway/NetScaler Gateway Secure Ticket Authority

Prise en charge des balises d'accès intelligentes

Dans les versions suivantes, NetScaler Gateway envoie les balises automatiquement. Il n'est pas nécessaire d'utiliser l'adresse de rappel de la passerelle pour récupérer les balises d'accès intelligentes.

- 13.1.48.47 et versions ultérieures
- 14.1—4.42 et versions ultérieures

Des balises d'accès intelligentes sont ajoutées en tant qu'en-tête dans la demande de plug-in Secure Private Access.

Utilisez le bouton `ns_vpn_enable_spa_onprem` ou pour `ns_vpn_disable_spa_onprem` activer/désactiver cette fonctionnalité sur ces versions de NetScaler.

- Vous pouvez basculer avec la commande (shell FreeBSD) :

  ```
  nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem
  ```

- Activez le mode client SecureBrowse pour la configuration des légendes HTTP en exécutant la commande suivante (shell FreeBSD).

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode
  ```

- Pour désactiver, réexécutez la même commande.
- Pour vérifier si le bouton est activé ou désactivé, exécutez la commande `nsconmsg`.
- Pour configurer les balises d'accès intelligentes sur NetScaler Gateway, consultez la section Configuration de balises personnalisées (balises SmartAccess) sur NetScaler Gateway.

Limitations connues

- NetScaler Gateway existant peut être mis à jour à l'aide d'un script, mais il peut y avoir un nombre infini de configurations NetScaler possibles qui ne peuvent pas être couvertes par un seul script.
- N'utilisez pas de proxy ICA sur NetScaler Gateway. Cette fonctionnalité est désactivée lorsque NetScaler Gateway est configuré.
- Si vous utilisez NetScaler déployé dans le cloud, vous devez apporter certaines modifications au réseau. Par exemple, autorisez les communications entre NetScaler et d'autres composants sur certains ports.
- Si vous activez l'authentification unique sur NetScaler Gateway, assurez-vous que NetScaler communique avec StoreFront à l'aide d'une adresse IP privée. Vous devrez peut-être ajouter un nouvel enregistrement DNS StoreFront à NetScaler avec une adresse IP privée StoreFront.

Télécharger le certificat de passerelle publique

Si la passerelle publique n'est pas accessible depuis la machine Secure Private Access, vous devez télécharger un certificat de passerelle publique dans la base de données Secure Private Access.

Procédez comme suit pour télécharger un certificat de passerelle publique :

1. Ouvrez PowerShell ou la fenêtre d'invite de commande avec les privilèges d'administrateur.
2. Remplacez le répertoire par le dossier Admin\AdminConfigTool dans le dossier d'installation de Secure Private Access (par exemple, cd « C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool »)
3. Exécutez la commande suivante :

   ```
   \AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
   > <PublicGatewayCertificatePath>
   ```

Configuration des balises contextuelles

February 16, 2024

Le plug-in Secure Private Access fournit un accès contextuel (accès intelligent) aux applications Web ou SaaS en fonction du contexte de la session utilisateur, tel que la plate-forme et le système d'exploitation de l'appareil, les logiciels installés, la géolocalisation.

Les administrateurs peuvent ajouter des conditions avec des balises contextuelles à la stratégie d'accès. La balise contextuelle du plug-in Secure Private Access est le nom d'une stratégie NetScaler Gateway (session, pré-authentification, EPA) appliquée aux sessions des utilisateurs authentifiés.

Le plug-in Secure Private Access peut recevoir des balises d'accès intelligentes sous forme d'en-tête (nouvelle logique) ou en effectuant des rappels vers Gateway. Pour plus de détails, consultez la section Tags d'accès intelligents .

> **Remarque :**
>
> Le plug-in Secure Private Access prend en charge uniquement les stratégies de pré-authentification de passerelle classiques qui peuvent être configurées sur NetScaler Gateway.

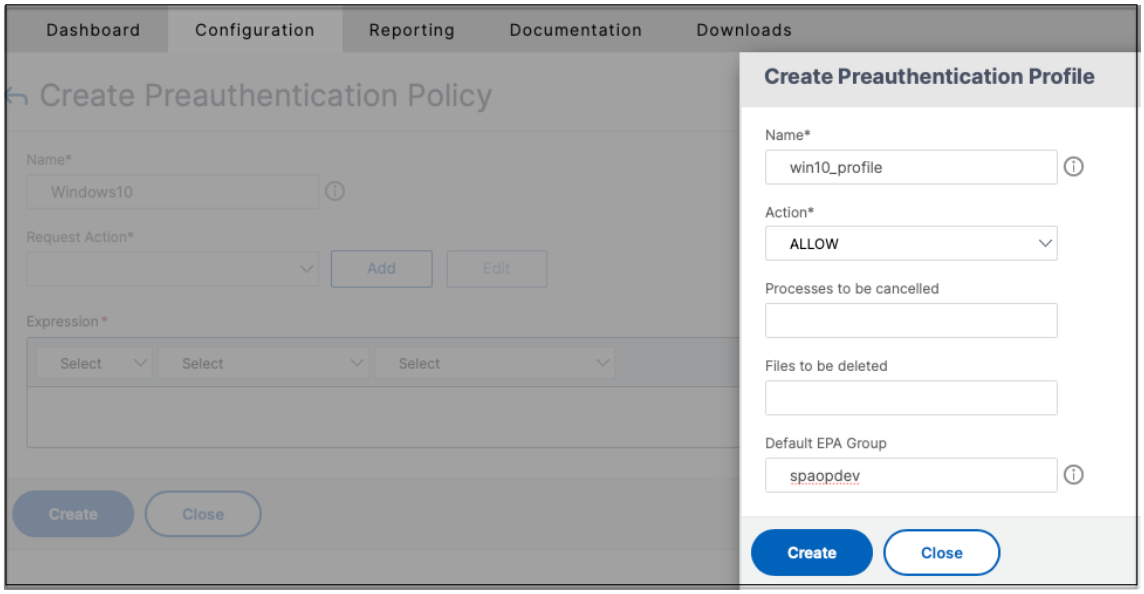
Configurer des balises personnalisées à l'aide de l'interface graphique

Les étapes de haut niveau suivantes sont impliquées dans la configuration des balises contextuelles.

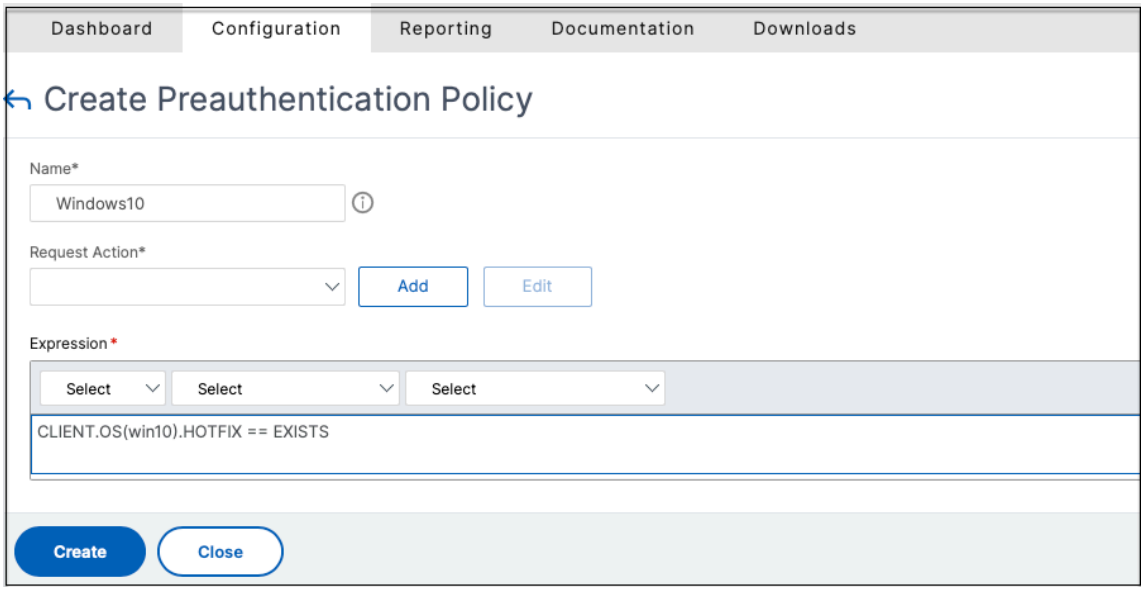
1. Configurer une stratégie de pré-authentification de passerelle classique
2. Liez la stratégie de préauthentification classique au serveur virtuel de passerelle

Configurer une stratégie de pré-authentification de passerelle classique

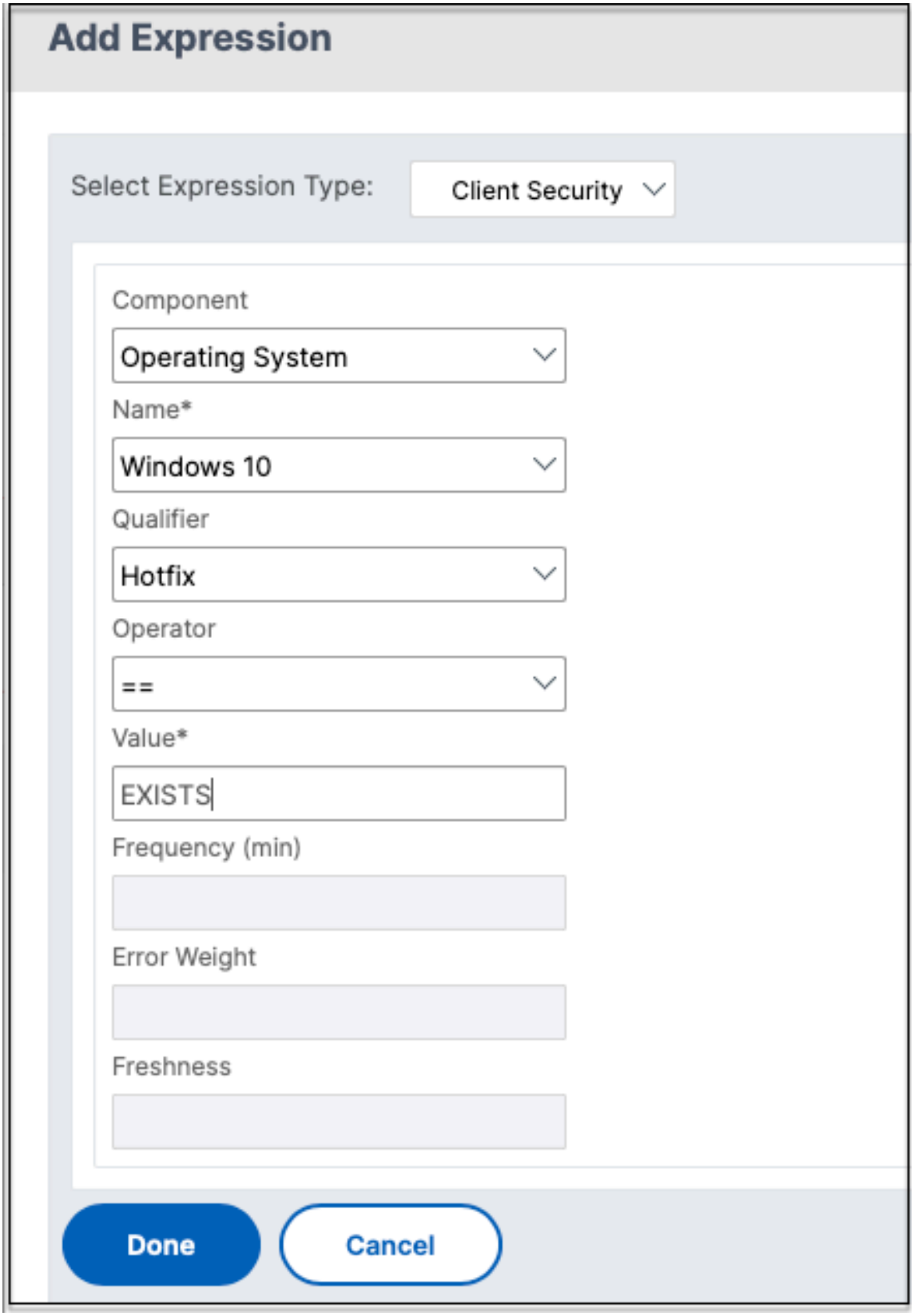
1. Accédez à **NetScaler Gateway > Stratégies > Préauthentification** , puis cliquez sur **Ajouter**.
2. Sélectionnez une stratégie existante ou ajoutez-y un nom. Ce nom de stratégie est utilisé comme valeur de balise personnalisée.
3. Dans **Demander une action** , cliquez sur **Ajouter** pour créer une action. Vous pouvez réutiliser cette action pour plusieurs stratégies, par exemple, utiliser une action pour autoriser l'accès, une autre pour refuser l'accès.



4. Renseignez les informations dans les champs obligatoires et cliquez sur **Créer** .
5. Dans **Expression** , entrez l'expression manuellement ou utilisez l'éditeur d'expression pour créer une expression pour la stratégie.



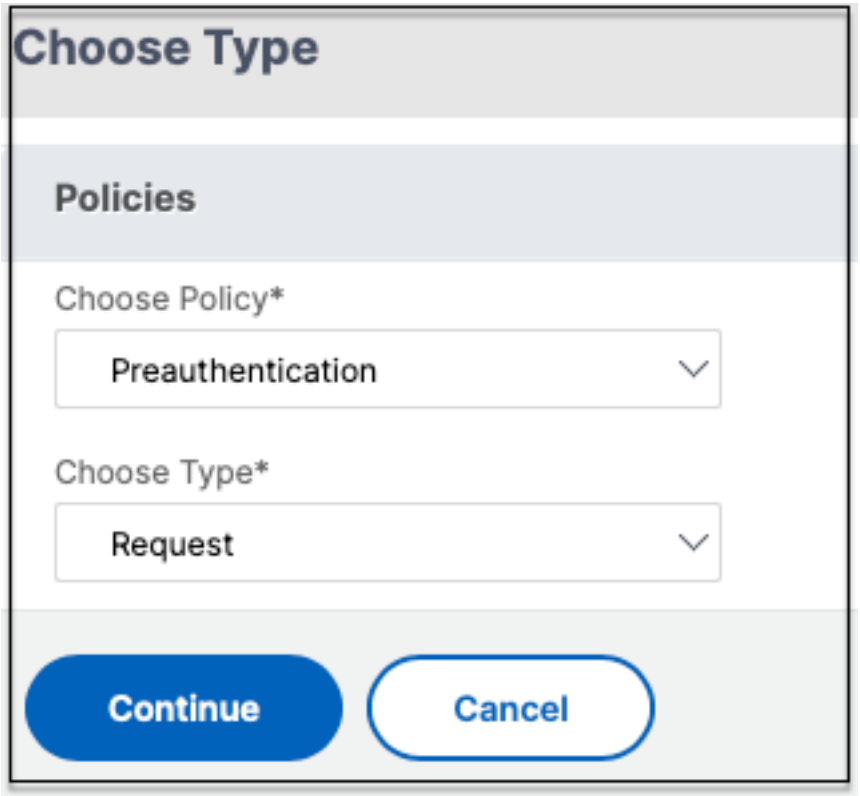
La figure suivante montre un exemple d'expression conçu pour vérifier le système d'exploitation Windows 10.



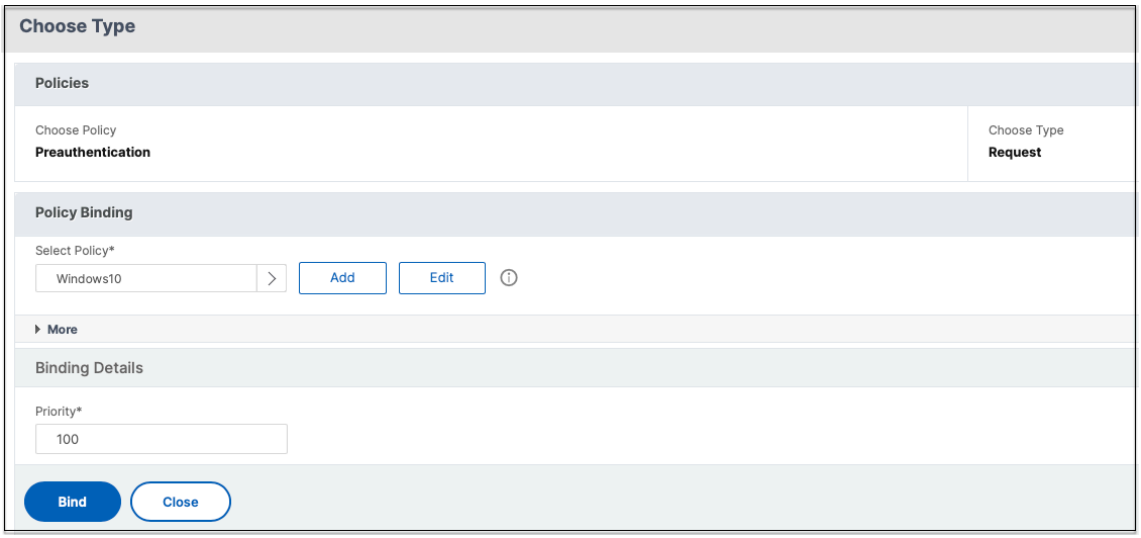
6. Cliquez sur **Créer**.

Liez la balise personnalisée à NetScaler Gateway

1. Accédez à **NetScaler Gateway > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel auquel la stratégie de préauthentification doit être liée, puis cliquez sur **Modifier** .
3. Dans la section **Stratégies** , cliquez sur **+** pour lier la stratégie.
4. Dans **Choisir une stratégie** , sélectionnez la stratégie de préauthentification, puis sélectionnez **Demander** dans **Choisir un type** .



5. Sélectionnez le nom de la stratégie et la priorité de l'évaluation de la stratégie.
6. Cliquez sur **Bind**.



Configurer des balises personnalisées à l'aide de la CLI

Exécutez les commandes suivantes sur la CLI NetScaler pour créer et lier une stratégie de préauthentification :

Exemple :

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

Ajouter une nouvelle balise contextuelle

1. Ouvrez la console d'administration Secure Private Access et cliquez sur **Stratégies** d'accès .
2. Créez une nouvelle stratégie ou sélectionnez une stratégie existante.
3. Dans la section **Si la condition suivante** est remplie , cliquez sur **Ajouter une condition** et sélectionnez **Balises** contextuelles , correspondent à **toutes**, puis entrez le nom de la balise contextuelle (par exemple, `Windows10`).

Références

- Configurez les stratégies d'accès pour les applications.
- Prise en charge des balises d'accès intelligentes.

Configurer StoreFront

December 27, 2023

Si Secure Private Access est co-hébergé avec StoreFront, la configuration de Secure Private Access sur StoreFront est effectuée automatiquement par l'assistant de première configuration.

Toutefois, si Secure Private Access n'est pas co-hébergé avec StoreFront, certaines modifications de configuration doivent être effectuées manuellement.

Effectuez les étapes suivantes pour configurer StoreFront manuellement.

1. Téléchargez le script depuis la console d'administration de Secure Private Access (**Paramètres > Intégrations**).
2. Cliquez sur **Télécharger le script** correspondant à l'entrée StoreFront pour laquelle les modifications de configuration doivent être effectuées.

   Le fichier zip téléchargé contient un script de configuration, un fichier README et un script de nettoyage de configuration. Le script de nettoyage peut être utilisé au cas où l'intégration entre StoreFront et Secure Private Access serait supprimée.
3. Exécutez le script en tant qu'administrateur sur une instance PowerShell 64 bits à l'aide de la commande `./ConfigureStorefront.ps1`.

   - Aucun autre paramètre n'est requis.
   - La politique d'exécution du script PowerShell doit être définie sur Unrestricted ou Bypass pour exécuter le script StoreFront.
   - Le script propage également la configuration aux autres serveurs StoreFront si StoreFront est configuré en tant que cluster.

Une fois que StoreFront est configuré avec les paramètres Secure Private Access, la configuration du plug-in Secure Private Access est visible dans l'interface d'administration de StoreFront (écran **Gérer les Delivery Controllers**).

Le script StoreFront configure automatiquement le paramètre de groupe d'agrégation pour Secure Private Access s'il est configuré pour le Delivery Controller Citrix Virtual Apps and Desktops. Par défaut, le script configure l'accès privé sécurisé pour tous (**Configuration du mappage des utilisateurs et de l'agrégation multisite > Configuré**).

> **Important :**
>
> - Il est recommandé d'utiliser le script StoreFront téléchargé depuis l'interface d'administration de Secure Private Access pour configurer StoreFront pour Secure Private Access uniquement. Ne configurez pas Secure Private Access depuis l'interface d'administration de Store-

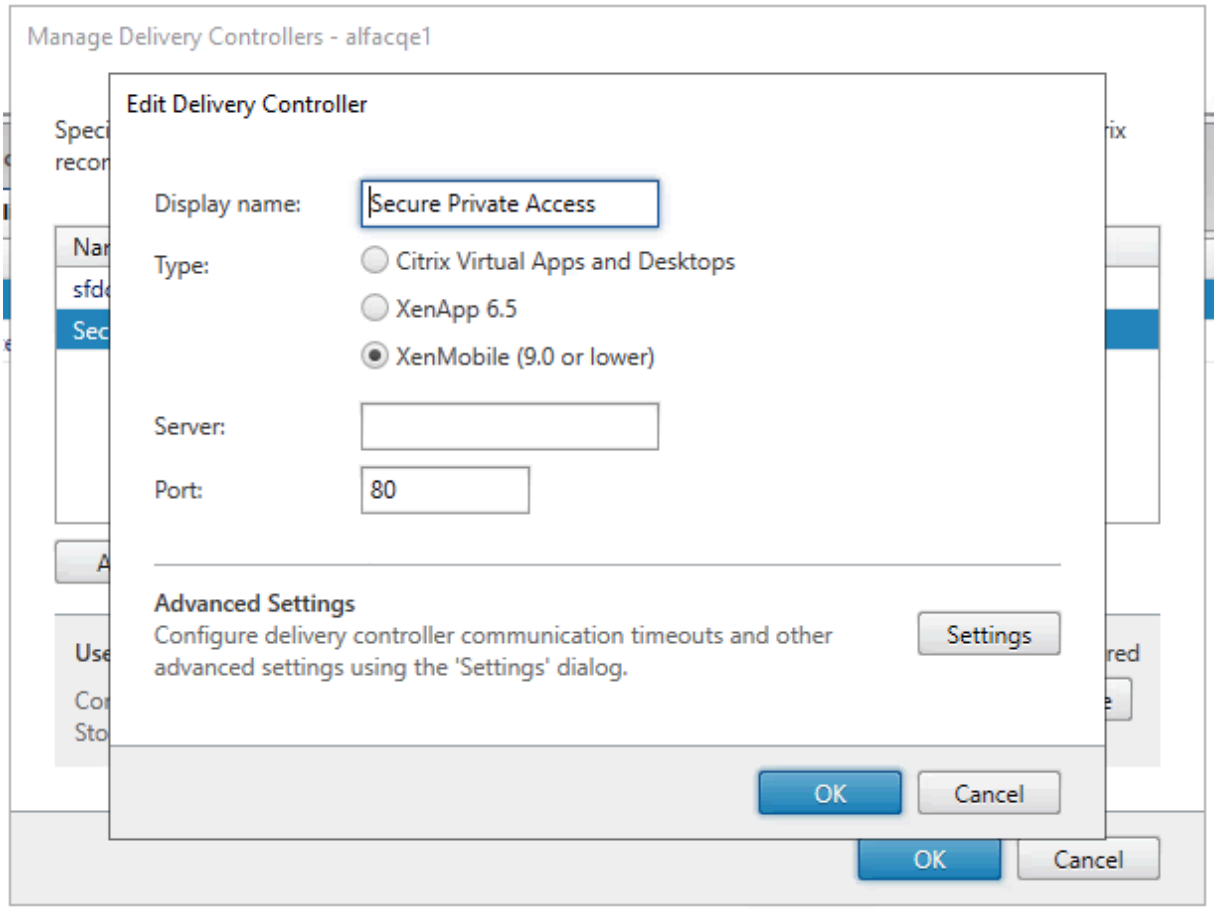
Front car celle-ci ne couvre pas toutes les configurations requises sur StoreFront. Le script doit être exécuté pour effectuer toutes les configurations nécessaires.

- Un site Secure Private Access peut également être configuré sur plusieurs déploiements StoreFront (soit sur un autre magasin sur le même StoreFront, soit sur un déploiement StoreFront différent).
  StoreFront peut être ajouté depuis la page **Paramètres > Intégrations** .
- La configuration automatique de StoreFront ne fonctionne pas depuis la page **Paramètres > Intégration** , même si Secure Private Access est co-hébergé avec StoreFront. La configuration automatique n'est effectuée que lors de la première configuration. Si une nouvelle configuration de magasin est ajoutée depuis la page **Paramètres** , le script StoreFront doit être téléchargé et exécuté sur la machine StoreFront correspondante.

Lors de l'utilisation de StoreFront version 2308 ou antérieure

Si vous utilisez la version 2308 ou une version antérieure de StoreFront, l'interface d'administration de StoreFront présente les problèmes connus suivants :

- Le type de plug-in Secure Private Access est affiché sous la forme XenMobile.
- L'URL du serveur Secure Private Access n'est pas affichée.
- Le port d'accès privé sécurisé est toujours indiqué comme 80.



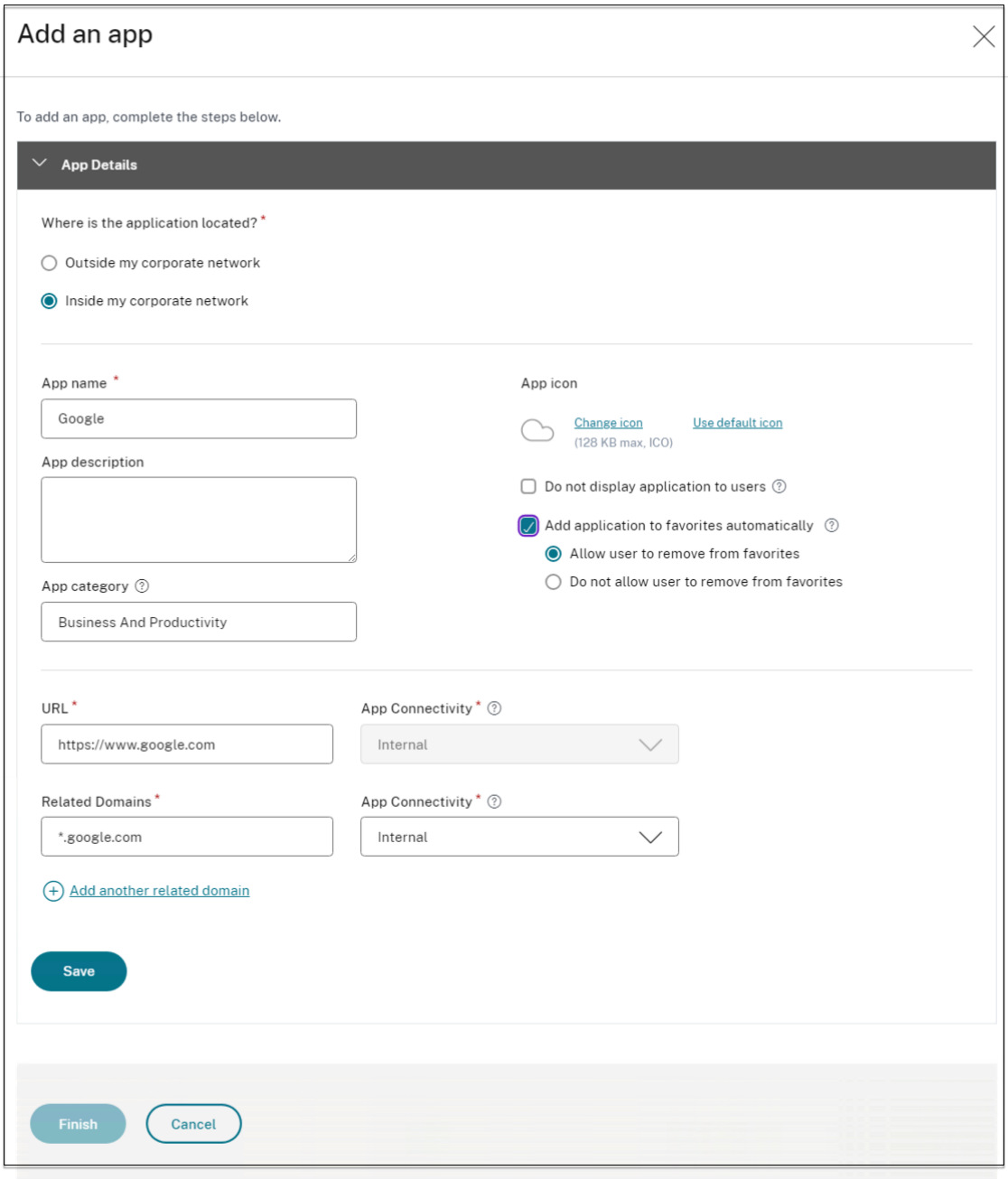
Lors de l'utilisation de StoreFront version 2311 ou ultérieure

Dans StoreFront version 2311 et versions ultérieures, le client Citrix Workspace for Web n'énumère pas les applications Secure Private Access. Cela est dû au fait que Secure Private Access ne prend pas en charge le lancement de l'application Secure Private Access sur la plateforme Workspace for Web.

Configurer les applications

February 16, 2024

1. Sélectionnez l'emplacement où se trouve l'application.
    - **En dehors de mon réseau d'entreprise** pour des applications externes.
    - **Au sein de mon réseau d'entreprise** pour les applications internes.
2. Entrez les informations suivantes dans la section Détails de l'application et cliquez sur **Suivant**.



- **Nom de l'application** : nom de l'application.
- **Description de l'application** : brève description de l'application. Cette description est présentée à vos utilisateurs dans l'espace de travail. Vous pouvez également saisir des mots clés pour les applications au format `KEYWORDS: <keyword_name>`. Vous pouvez utiliser les mots clés pour filtrer les applications. Pour plus de détails, voir Filtrer les ressources en fonction des mots clés inclus.
- **Catégorie d'applications** : ajoutez la catégorie et le nom de la sous-catégorie (le cas échéant) sous lesquels l'application que vous publiez doit apparaître dans l'interface util-

isateur de Citrix Workspace. Vous pouvez ajouter une nouvelle catégorie pour chaque application ou utiliser les catégories existantes depuis l'interface utilisateur de Citrix Workspace. Une fois que vous avez spécifié une catégorie pour une application Web ou SaaS, l'application s'affiche dans l'interface utilisateur de Workspace sous la catégorie spécifique.

- La catégorie/sous-catégorie est configurable par l'administrateur et les administrateurs peuvent ajouter une nouvelle catégorie pour chaque application.
- Les noms des catégories/sous-catégories doivent être séparés par une barre oblique inverse. Par exemple, Business And Productivity \ Engineering . De plus, ce champ distingue les majuscules et les minuscules. Les administrateurs doivent s'assurer de définir la bonne catégorie. En cas de divergence entre le nom dans l'interface utilisateur de Citrix Workspace et le nom de catégorie saisi dans le champ Catégorie d' applications, la catégorie est répertoriée en tant que nouvelle catégorie.

  Par exemple, si vous saisissez incorrectement la catégorie Business and Productivity en tant que Business and productivity dans le champ Catégorie App , une nouvelle catégorie nommée Business and productivity est répertoriée dans l'interface utilisateur de Citrix Workspace en plus de la catégorie Business and Productivity .

- **Icône de l'application** : cliquez sur **Modifier l'icône** pour modifier l'icône de l'application. La taille du fichier d'icône doit être de 128 x 128 pixels et seul le format Ico est pris en charge. Si vous ne modifiez pas l'icône, l'icône par défaut est affichée.
- **Ne pas afficher l'application aux utilisateurs** - Sélectionnez cette option si vous ne souhaitez pas afficher l'application aux utilisateurs.
- **URL** : URL de l'application.
- **Domaines associés** : le domaine associé est renseigné automatiquement en fonction de l'URL de l'application. Les administrateurs peuvent ajouter d'autres domaines internes ou externes connexes.
  Ajouter automatiquement l'application aux favoris : cliquez sur cette option pour ajouter cette application en tant qu'application favorite dans l'application Citrix Workspace.
- **Autoriser l'utilisateur à supprimer des favoris** : cliquez sur cette option pour autoriser les abonnés à supprimer l'application de la liste des applications favorites de l'application Citrix Workspace.
  Lorsque vous sélectionnez cette option, une étoile jaune apparaît dans le coin supérieur gauche de l'application Citrix Workspace.
- **Ne pas autoriser l'utilisateur à supprimer des favoris** : cliquez sur cette option pour empêcher les abonnés de supprimer l'application de la liste des applications favorites de l'application Citrix Workspace.

Lorsque vous sélectionnez cette option, une étoile avec un cadenas apparaît dans le coin supérieur gauche de l'application Citrix Workspace.

Si vous supprimez les applications marquées comme favorites de la console Secure Private Access, elles doivent être supprimées manuellement de la liste des favoris dans Citrix Workspace. Les applications ne sont pas automatiquement supprimées de StoreFront si elles sont supprimées de la console Secure Private Access.
Connectivité des applications : sélectionnez Interne pour les applications Web et Externe pour les applications SaaS.

3. Cliquez sur **Enregistrer**, puis sur **Terminer**.

Vous pouvez consulter tous les domaines d'application configurés dans **Paramètres > Domaine d'application**. Pour plus de détails, voir Gérer les paramètres après l'installation.

Prochaines étapes

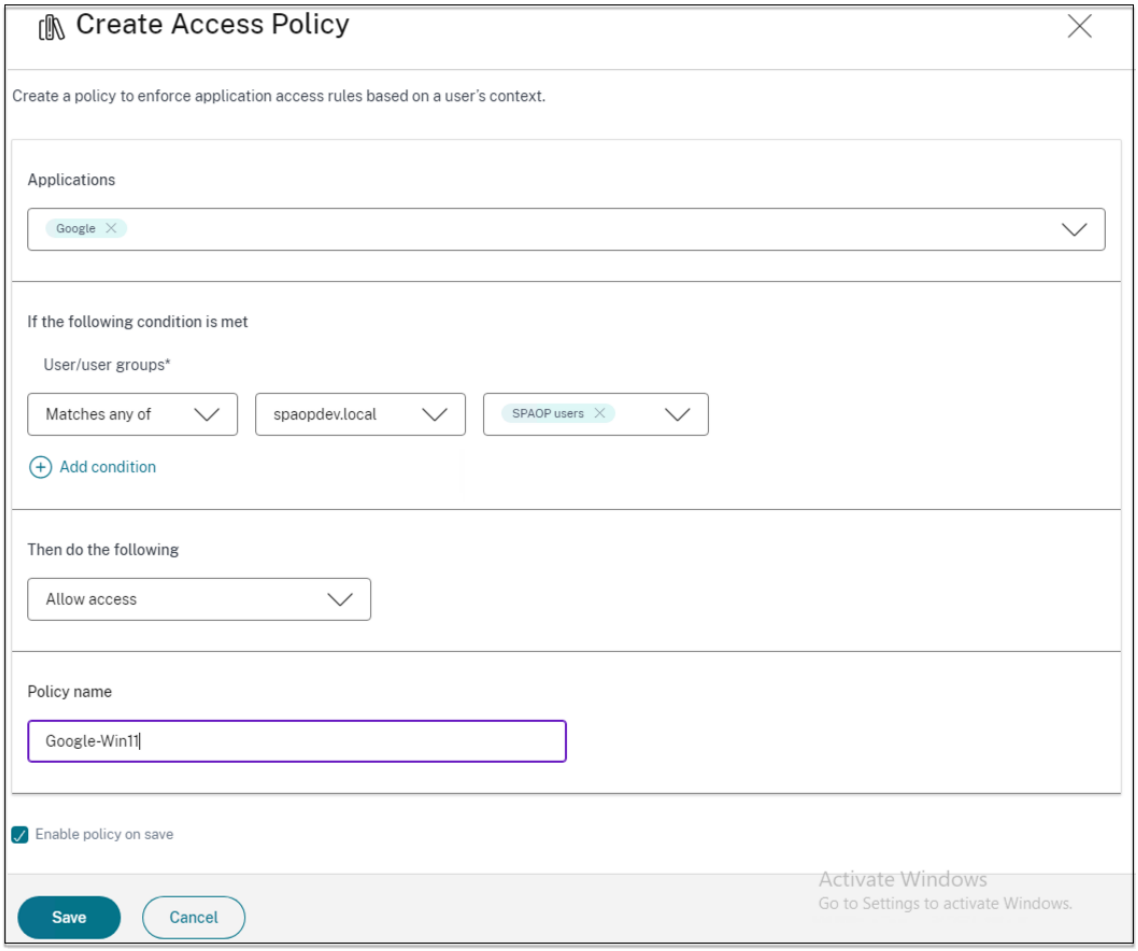
Configuration des stratégies d'accès pour les applications

Configuration des stratégies d'accès pour les applications

December 27, 2023

Les stratégies d'accès vous permettent d'activer ou de désactiver l'accès aux applications en fonction de l'utilisateur ou des groupes d'utilisateurs. En outre, vous pouvez activer l'accès restreint aux applications en ajoutant des restrictions de sécurité.

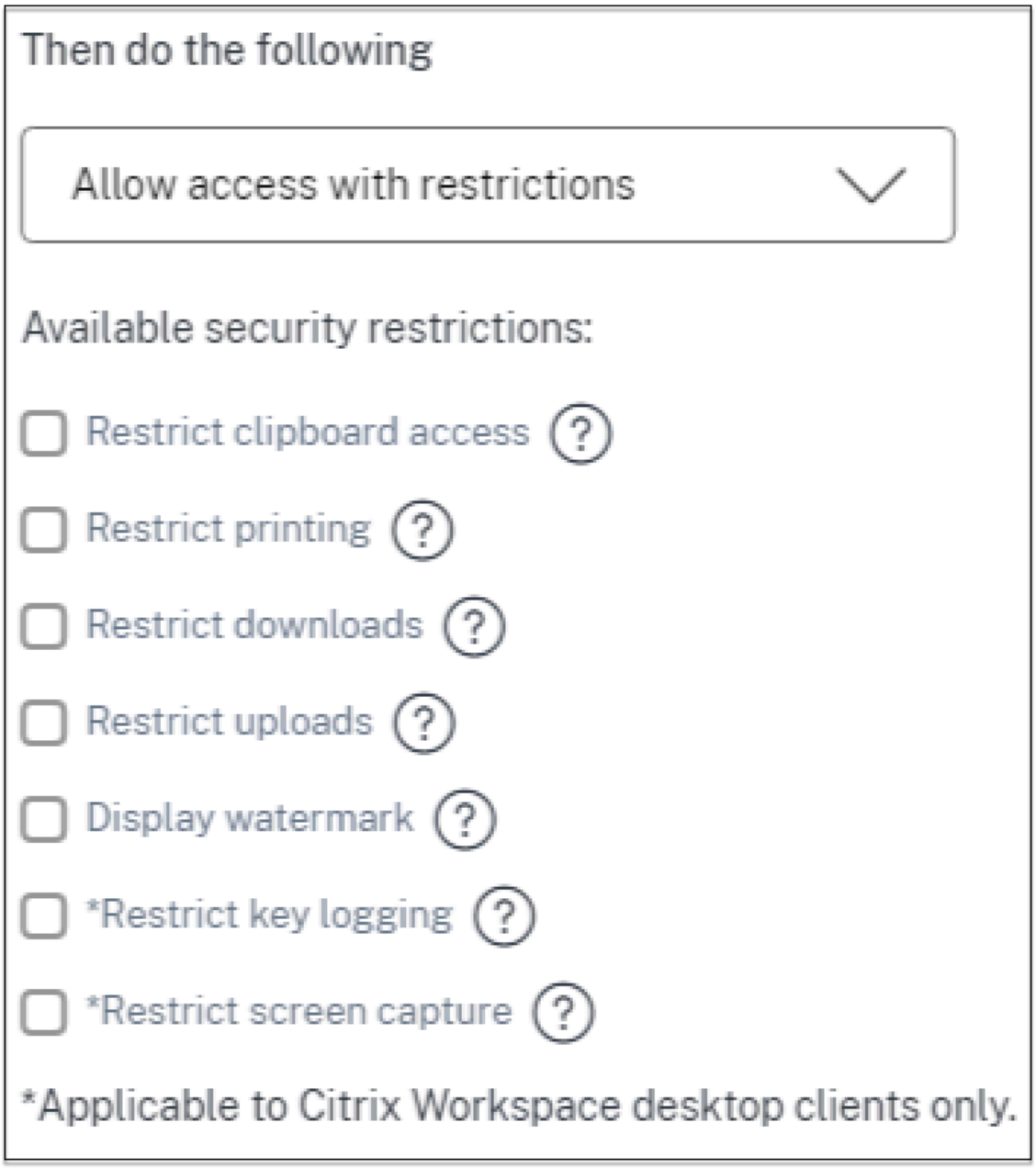
1. Cliquez sur **Créer une stratégie**.



2. Dans **Applications**, sélectionnez les applications pour lesquelles vous souhaitez appliquer les stratégies d'accès.
3. Dans **Utilisateurs/Groupes d'utilisateurs** : sélectionnez les conditions et les utilisateurs ou groupes d'utilisateurs en fonction desquels l'accès à l'application doit être autorisé ou refusé.
    - **Correspond à l'un des**noms suivants : seuls les utilisateurs ou groupes correspondant à l'un des noms répertoriés dans le champ sont autorisés à y accéder.
    - **Ne correspond à aucun** : tous les utilisateurs ou groupes, à l'exception de ceux répertoriés dans le champ, sont autorisés à accéder.
4. Cliquez sur **Ajouter une condition** pour ajouter une autre condition en fonction des balises contextuelles. Ces balises sont dérivées de NetScaler Gateway.
5. Sélectionnez **Balises conditionnelles**, puis sélectionnez les conditions selon lesquelles l'accès à l'application doit être autorisé ou refusé.
6. Dans **Ensuite, sélectionnez l'**une des actions suivantes qui doit être appliquée à l'application en fonction de l'évaluation des conditions.
    - **Autoriser l'accès**

- **Autoriser l'accès avec restriction**
- **Refuser l'accès**

Lorsque vous sélectionnez **Autoriser l'accès avec restrictions**, vous pouvez sélectionner les restrictions suivantes.



- **Restreindre l'accès au presse-papiers** : désactive les opérations couper/copier/coller entre l'application et le presse-papiers du système.
- **Restreindre l'impression** : désactive la possibilité d'imprimer depuis le navigateur Citrix Enterprise.
- **Restreindre les téléchargements** : désactive la possibilité pour l'utilisateur de

télécharger depuis l'application.

- **Restreindre les téléchargements** : désactive la capacité de l'utilisateur à télécharger dans l'application.
- **Afficher le filigrane** : affiche un filigrane sur l'écran de l'utilisateur indiquant le nom d'utilisateur et l'adresse IP de la machine de l'utilisateur.
- **Restreindre l'enregistrement des clés** : protège contre les enregistreurs de clés. Lorsqu'un utilisateur tente de se connecter à l'application à l'aide du nom d'utilisateur et du mot de passe, toutes les clés sont chiffrées sur les enregistreurs de frappe. De plus, toutes les activités que l'utilisateur effectue sur l'application sont protégées contre l'enregistrement des clés.

  Par exemple, si les stratégies de protection des applications sont activées pour Office 365 et que l'utilisateur modifie un document Word Office 365, toutes les touches sont chiffrées dans les enregistreurs de touches.
- **Restreindre la capture d'écran** : désactive la possibilité de capturer les écrans à l'aide de l'un des programmes ou applications de capture d'écran. Si un utilisateur tente de capturer l'écran, un écran vide est capturé.

> **Remarque :**
>
> les restrictions relatives à la journalisation des touches et à la capture d'écran ne s'appliquent qu'aux clients de bureau Citrix Workspace.

7. Dans **Nom de la stratégie**, entrez le nom de la stratégie.
8. Sélectionnez **Activer la stratégie lors de la sauvegarde**. Si vous ne sélectionnez pas cette option, la stratégie est uniquement créée et n'est pas appliquée aux applications. Vous pouvez également activer la stratégie depuis la page Stratégies d'accès à l'aide de l'interrupteur à bascule.

Priorité de la stratégie d'accès

Une fois qu'une stratégie d'accès est créée, un numéro de priorité lui est attribué par défaut. Vous pouvez consulter la priorité sur la page d'accueil des stratégies d'accès.

Une priorité dont la valeur est inférieure a la préférence la plus élevée et est évaluée en premier. Si cette stratégie ne correspond pas aux conditions définies, la stratégie suivante avec le numéro de priorité le plus faible est évaluée et ainsi de suite.

Vous pouvez modifier l'ordre de priorité en déplaçant les stratégies vers le haut ou vers le bas à l'aide de l'icône haut-bas dans la colonne **Priorité** .

Étapes suivantes

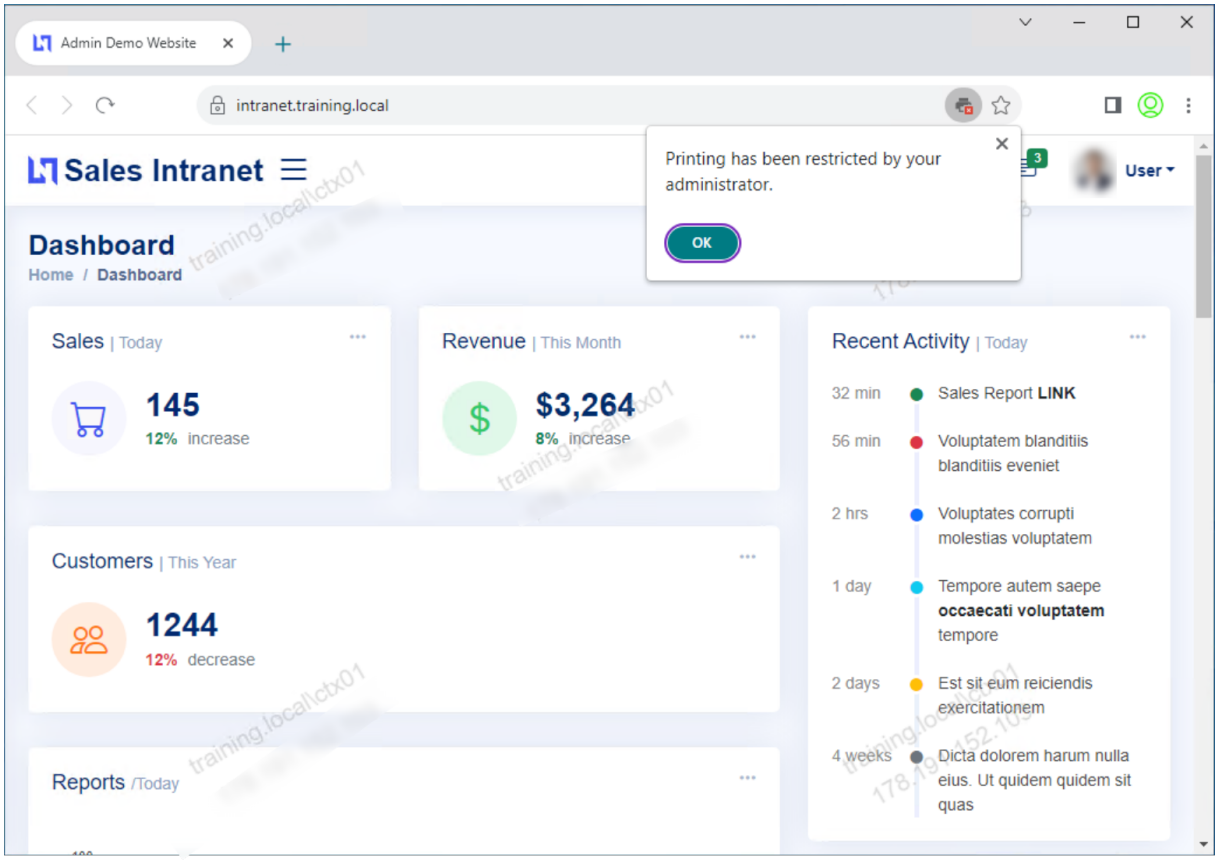
Validez votre configuration depuis les machines clientes (Windows et macOS).

Example

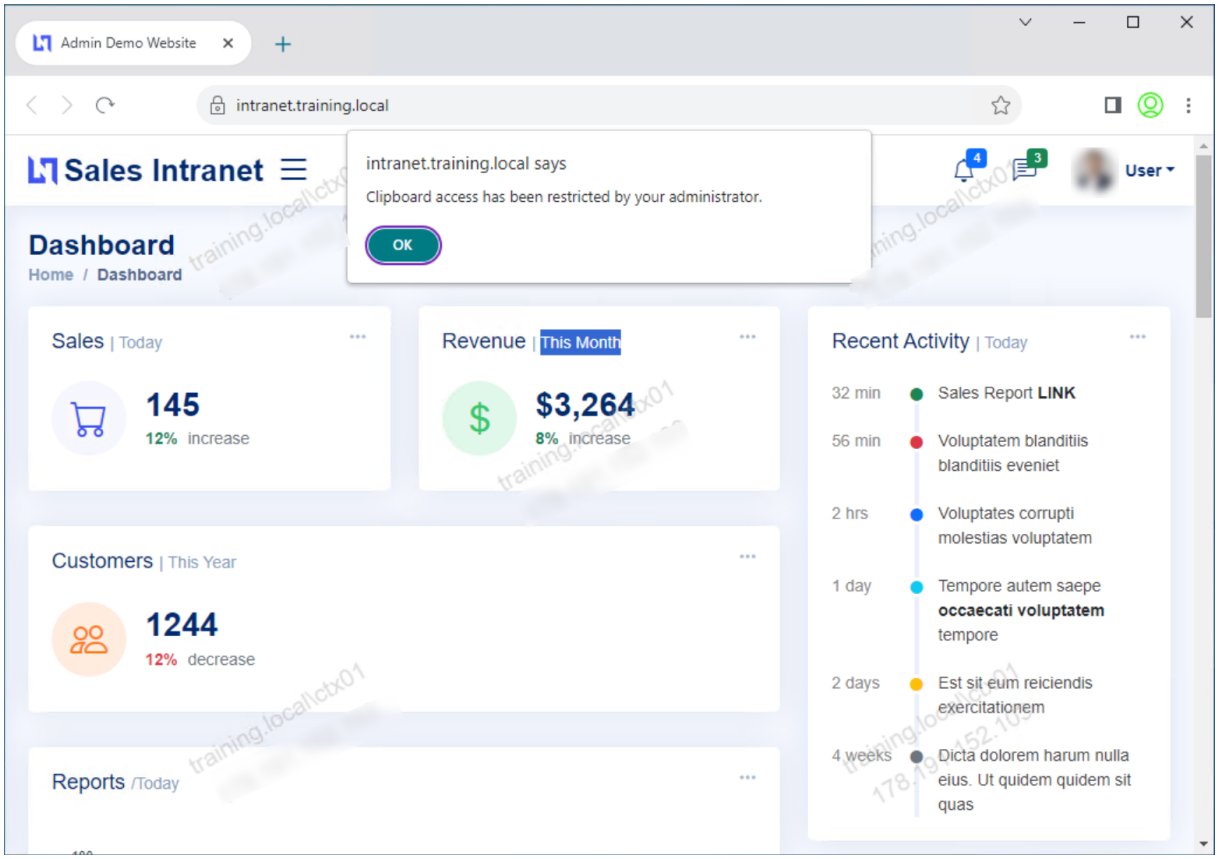
Flux d'utilisateurs finaux

December 27, 2023

Supposons que vous ayez créé une stratégie d'accès pour une application avec des restrictions d'accès au presse-papiers et d'impression. Désormais, lorsque l'utilisateur final accède à l'application depuis StoreFront, l'application s'ouvre dans le navigateur Citrix Enterprise et l'utilisateur peut l'utiliser. Toutefois, si l'utilisateur essaie d'imprimer depuis l'application, le message suivant s'affiche.



De même, si l'utilisateur essaie d'accéder au presse-papiers, le message suivant apparaît.



> **Remarque :**
>
> Les administrateurs doivent fournir aux utilisateurs les informations de compte dont ils ont besoin pour accéder aux applications et bureaux virtuels. Pour plus d'informations, consultez la section Ajout d'une URL de magasin à l'application Citrix Workspace.

Intégration de Secure Private Access à l'intégration de Web Studio

December 27, 2023

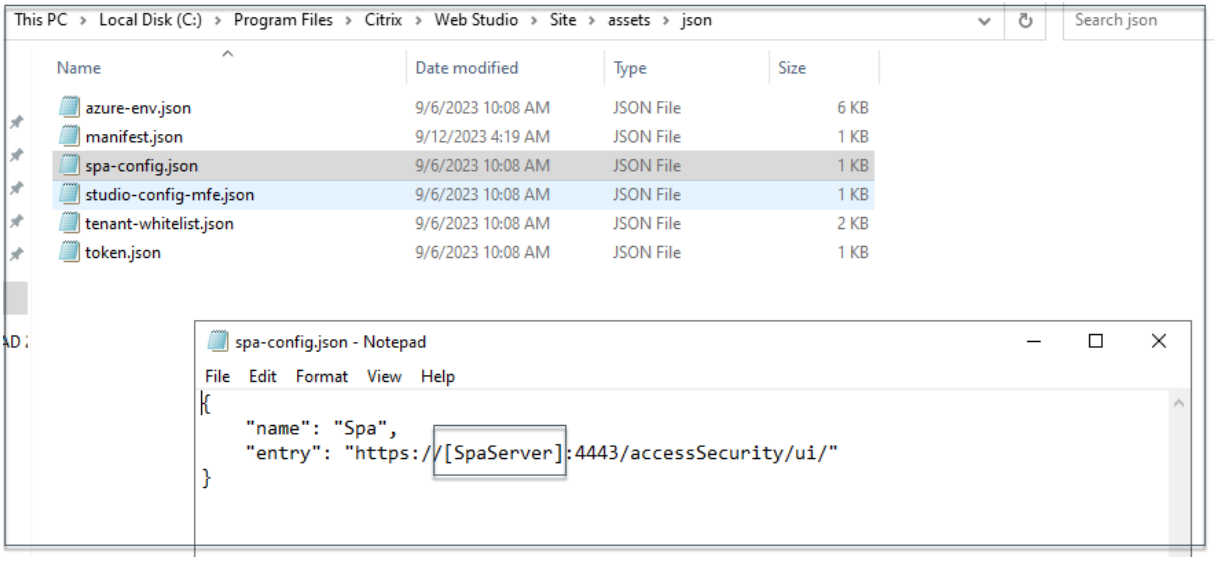
Citrix Secure Private Access est également intégré à la console Web Studio pour permettre aux utilisateurs d'accéder facilement au service via Web Studio.

Vous devez installer Web Studio version 2308 ou ultérieure.

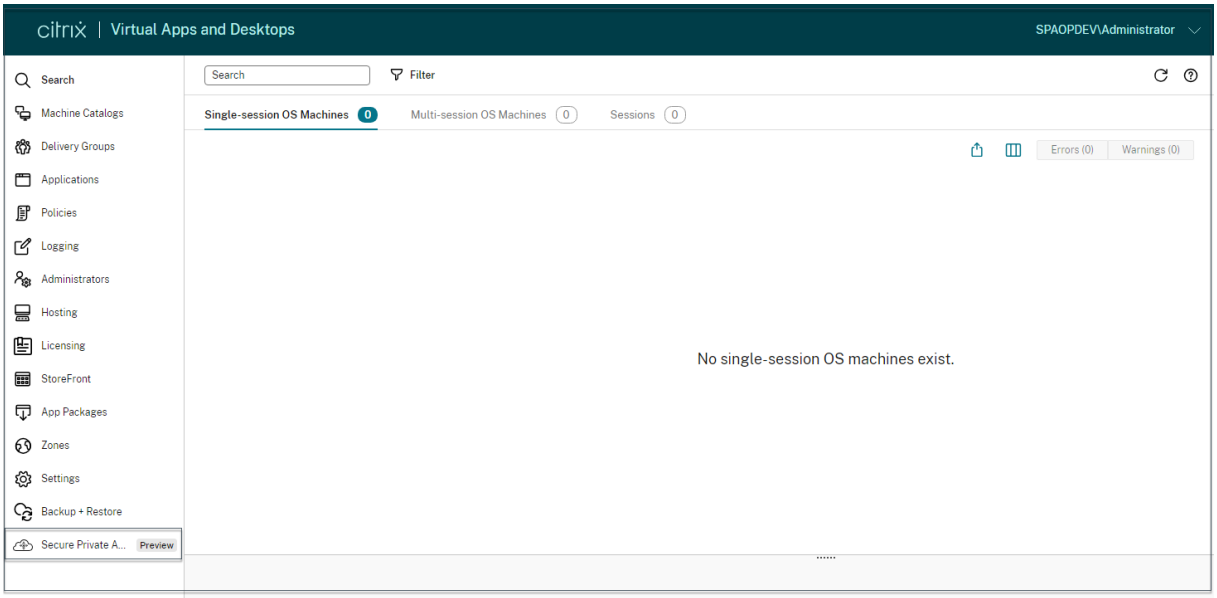
Procédez comme suit pour activer l'intégration de Web Studio :

1. Installez Citrix Web Studio à l'aide du programme d'installation Citrix Virtual Apps and Desktops ou du programme d'installation DDC intégré.

2. Suivez les instructions qui s'affichent à l'écran et terminez l'installation. Lorsque vous êtes invité à saisir une adresse de contrôleur, entrez le nom de domaine complet DDC comme adresse du contrôleur.
3. Une fois l'installation réussie, accédez au dossier C:\Program Files\Citrix\Web Studio\Site\assets\json et modifiez le contenu du fichier spa-config.json.
   Si un emplacement autre que celui par défaut a été utilisé pour l'installation de Web Studio, remplacez l'emplacement d'installation par défaut dans C:\Program Files\Citrix par l'emplacement correct.



1. Remplacez « SpaServer » par le nom de domaine complet de votre plug-in Secure Private Access.
2. Connectez-vous à Web Studio.



1. Dans le menu de navigation de gauche, cliquez sur **Secure Private Access <Preview>** pour

accéder à la console d'administration Secure Private Access depuis Web Studio.

Déployez un accès privé sécurisé en tant que cluster

February 16, 2024

La solution d'accès privé sécurisé sur site peut être déployée sous forme de cluster pour fournir une haute disponibilité, un haut débit et une évolutivité. Il est recommandé de déployer des nœuds d'accès privé sécurisé autonomes pour les déploiements de grande envergure (par exemple, plus de 5 000 utilisateurs).

Si vous utilisez les versions 13.0 ou 13.1 build 48.47 ou antérieures de NetScaler Gateway, il est recommandé de co-héberger Secure Private Access avec StoreFront.

Création de nœuds d'accès privé sécurisés

- Créez un nouveau site d'accès privé sécurisé. Pour plus de détails, voir Configuration d'un site d'accès privé sécurisé .
- Ajoutez le nombre requis de nœuds de cluster au site Secure Private Access. Pour plus de détails, voir Configurer un accès privé sécurisé en rejoignant un site existant .
- Dans chaque nœud Secure Private Access, configurez les mêmes certificats de serveur. Le nom commun du sujet du certificat ou le nom alternatif du sujet doit correspondre au nom de domaine complet de l'équilibreur de charge.

Configuration de l'équilibreur de charge

Il n'existe aucune exigence de configuration d'équilibrage de charge spécifique pour la configuration du cluster Secure Private Access. Si vous utilisez NetScaler comme équilibreur de charge, tenez compte des points suivants :

- Les services d'accès privé sécurisé (à la fois d'administration et d'exécution) sont sans état, et la persistance n'est donc pas requise.
- Il est recommandé que les services d'accès privé sécurisé soient exécutés en HTTPS, mais ce n'est pas une exigence obligatoire. Les services d'accès privé sécurisé peuvent également être déployés en HTTP.
- Le déchargement SSL ou le pont SSL sont pris en charge, de sorte que n'importe quelle configuration d'équilibreur de charge peut être utilisée. Lorsque vous utilisez un pont SSL, assurez-vous de configurer les mêmes certificats de serveur dans chaque nœud d'accès privé sécurisé.

En outre, le nom commun du sujet du certificat ou le nom alternatif du sujet (SAN) doit correspondre au nom de domaine complet de l'équilibreur de charge. Le SAN doit également être configuré dans le service Load Balancer.

- Les équilibreurs de charge (par exemple NetScaler) sont dotés de moniteurs intégrés par défaut (sondes) pour les serveurs principaux. Si vous devez configurer un moniteur (sonde) HTTP personnalisé pour les serveurs locaux Secure Private Access, le point de terminaison suivant peut être utilisé :

  `/secureAccess/health`

  Réponse attendue :

```
Http status code: 200 OK

Payload:

{
"status":"OK","details":{
"duration":"00:00:00.0084206","status":"OK" }
 }

<!--NeedCopy-->
```

Pour plus d'informations sur la configuration d'un équilibreur de charge NetScaler, consultez la section Configuration de l'équilibrage de charge de base.

Gérer les paramètres après l'installation

December 27, 2023

Après avoir installé Secure Private Access, vous pouvez modifier les paramètres depuis la page Paramètres.

Pour modifier les paramètres, vous devez vous connecter à la console d'administration Secure Private Access avec un compte administrateur Secure Private Access.

Gérer le routage des domaines d'applications

Vous pouvez consulter la liste des domaines d'application ajoutés dans votre configuration Secure Private Access. Le tableau des domaines d'application répertorie tous les domaines associés et la manière dont le trafic de l'application est acheminé (en externe ou en interne).

1. Cliquez sur **Paramètres > Domaine de l'application**.
2. Vous pouvez cliquer sur l'icône d'édition et modifier le type de routage, si nécessaire.

Gérez les administrateurs pour Secure Private Access

Vous pouvez consulter la liste des administrateurs et ajouter des administrateurs depuis la page **Paramètres > Administrateurs** . L'administrateur qui installe Secure Private Access pour la première fois bénéficie d'une autorisation complète. Cet administrateur peut ensuite ajouter d'autres administrateurs à la configuration.

Vous pouvez également ajouter des groupes d'administrateurs afin que l'accès soit activé pour tous les administrateurs de ce groupe.

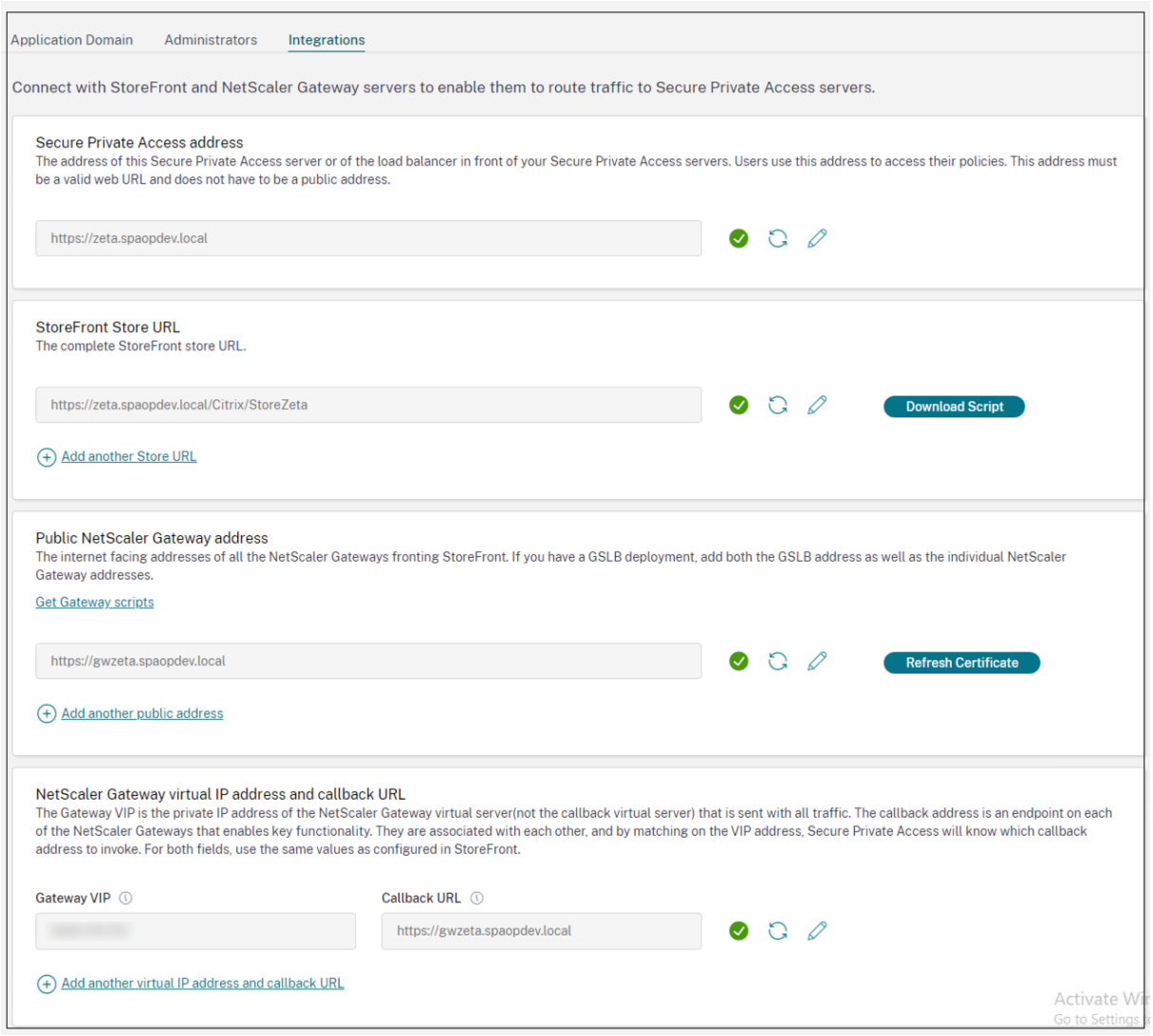
1. Sur la page **Administrateurs** , cliquez sur **Ajouter** .
2. Dans **Domaine**, sélectionnez le domaine auquel cet administrateur doit être ajouté.
3. Dans **Utilisateurs ou groupe** d'utilisateurs , sélectionnez l'utilisateur ou le groupe auquel appartient cet utilisateur.
4. Dans **Type d'administrateur**, sélectionnez le type d'autorisation qui doit être attribué à cet utilisateur.

Mettez à jour les détails de StoreFront ou du serveur NetScaler Gateway après la configuration

Après avoir configuré Secure Private Access, vous pouvez modifier ou mettre à jour les entrées StoreFront et NetScaler Gateway depuis l'onglet **Intégrations**.

1. Cliquez sur **Paramètres > Intégrations.**
2. Cliquez sur l'icône de modification correspondant au paramètre que vous souhaitez modifier et mettez à jour l'entrée.
3. Cliquez sur l'icône d'actualisation pour vérifier que les paramètres sont valides.

> **Remarque :**
>
> Si Secure Private Access est installé sur une machine différente de StoreFront, téléchargez le script StoreFront et exécutez-le sur StoreFront.



Aperçu du tableau de bord

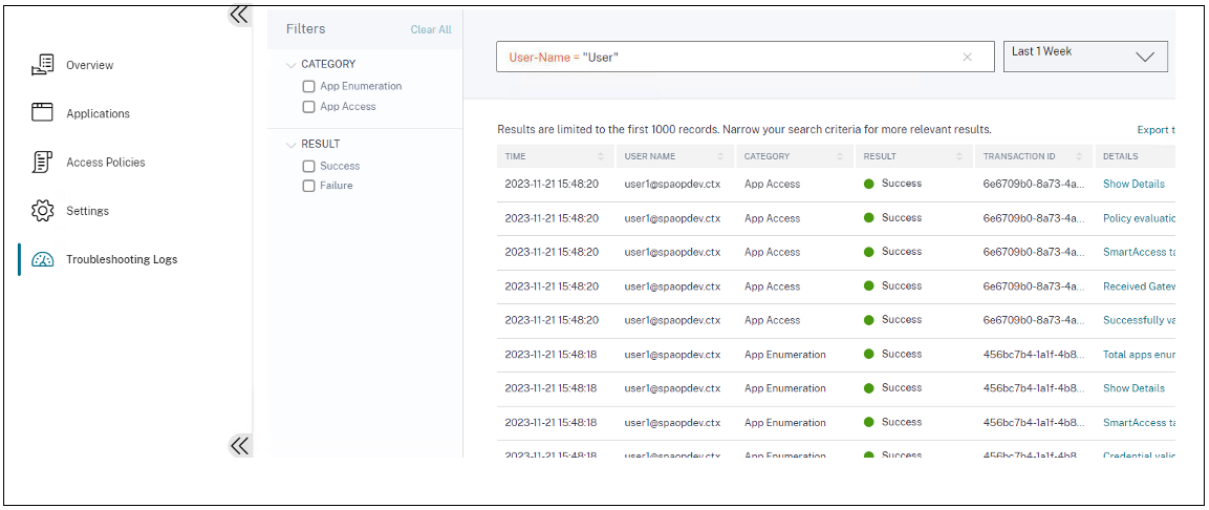
December 27, 2023

Le tableau de bord des journaux de résolution des problèmes liés à Secure Private Access affiche les journaux relatifs au lancement des applications, à l'énumération des applications et à leur statut.

Vous pouvez afficher les journaux pour l'heure prédéfinie ou pour une chronologie personnalisée. Vous pouvez ajouter des colonnes au graphique en cliquant sur le signe + en fonction des informations que vous souhaitez voir dans le tableau de bord. Vous pouvez exporter les journaux des utilisateurs au format CSV.

Vous pouvez utiliser les filtres (CATÉGORIE et RÉSULTAT) pour affiner les résultats de votre

recherche.



Vous pouvez également affiner votre recherche en fonction des paramètres suivants ainsi que des opérateurs du champ de recherche.

- Nom d'utilisateur
- Catégorie
- Type d'événement
- Résultat
- ID de transaction
- Détails

Vous trouverez ci-dessous les opérateurs de recherche que vous pouvez utiliser pour affiner votre recherche dans les journaux des utilisateurs et les tableaux d'application des stratégies d'accès les plus populaires .

- = : Pour rechercher les logs/stratégies qui correspondent exactement aux critères de recherche.
- != : Pour rechercher les logs/stratégies qui ne contiennent pas les critères spécifiés.
- ~ : Pour rechercher les logs/stratégies qui correspondent partiellement aux critères de recherche.
- !~ : Pour rechercher les logs/stratégies qui ne contiennent pas certains des critères spécifiés.

Par exemple, vous pouvez rechercher un type d'événement « DSAuth » en utilisant la chaîne **Event-Type = DSAuth** dans le champ de recherche.

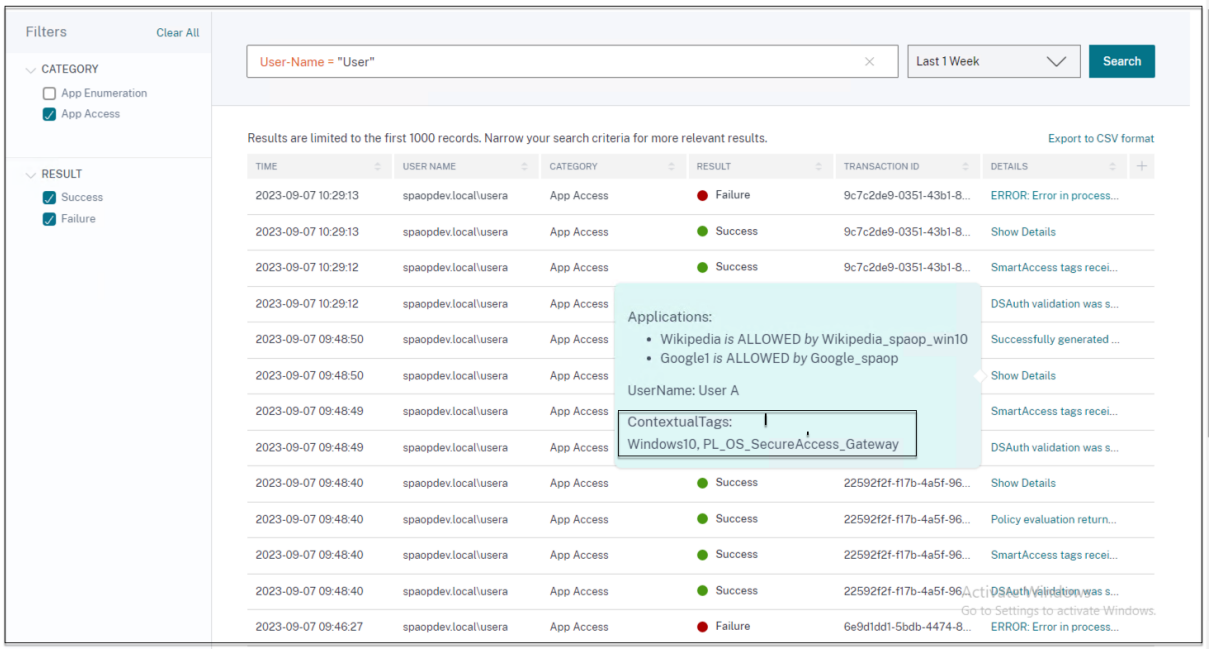
De même, pour rechercher des utilisateurs contenant partiellement le terme « opérateur », utilisez la chaîne **User-Name ~ operator**. Cette recherche répertorie tous les noms d'utilisateur contenant le terme « opérateur ». Par exemple, « opérateur local », « opérateur administrateur »

Vous pouvez rechercher tous les journaux relatifs à un seul événement à l'aide de l'ID de transaction. L'ID de transaction met en corrélation tous les journaux Secure Private Access d'une demande d'accès. Une demande d'accès à une application peut générer plusieurs journaux, en commençant par l'

authentification, puis l'énumération des applications et enfin l'accès à l'application lui-même. Tous ces événements génèrent leurs propres journaux. L'ID de transaction est utilisé pour corréler tous ces journaux. Vous pouvez filtrer les journaux de résolution des problèmes à l'aide de l'ID de transaction pour trouver tous les journaux liés à une demande d'accès à une application particulière.

Afficher les balises contextuelles à partir des journaux

Le lien **Afficher les détails** dans la colonne **Détails** affiche la liste des applications associées à la stratégie d'accès spécifique ainsi que les balises contextuelles associées à la stratégie.



Résolution de certaines erreurs courantes

February 16, 2024

Cette rubrique répertorie certaines des erreurs que vous pouvez rencontrer lors de la configuration de Secure Private Access.

Erreurs de certificat

Erreurs de création de base de données

Défaillances de StoreFront

Défaillances de la passerelle publique/de la passerelle de rappel

Le serveur Secure Private Access n'est pas accessible

Erreurs de certificat

Message d'erreur : Impossible d'obtenir automatiquement les certificats d'un ou de plusieurs serveurs Gateway.

Ce message d'erreur s'affiche lorsque vous essayez d'ajouter une adresse NetScaler Gateway publique et qu'un problème survient lors de la récupération du certificat. Ce problème peut survenir lors de la configuration de l'accès privé sécurisé ou de la mise à jour des paramètres une fois la configuration terminée.

Solution: mettez à jour le certificat de passerelle de la même manière que vous le feriez pour Citrix Virtual Apps and Desktops.

Erreurs de création de base de données

- **Message d'erreur** : Impossible de créer la base de données

  Résolution : pour le cas automatique : la machine doit disposer des autorisations READ, WRITE et UPDATE pour créer des tables dans la base de données du serveur SQL.

- **Message d'erreur** : Impossible de créer la base de données : une base de données existe déjà.

  Ce message d'erreur peut apparaître dans l'un des scénarios suivants.

  - Si l'option **Configuration automatique** est sélectionnée lors de la configuration des bases de données.
  - Si l'administrateur crée une base de données, celle-ci doit être vide. Ce message d'erreur peut apparaître si la base de données n'est pas vide.

    Résolution : vous devez créer une base de données vide.
  - Vous désinstallez Secure Private Access et réessayez la configuration avec le même nom de site. Dans ce cas, la base de données de l'installation précédente n'aurait pas été supprimée.

    Résolution : vous devez supprimer manuellement la base de données.
  - Vous choisissez de configurer la base de données manuellement (en sélectionnant Configuration manuelle sur la page Configuration des bases de données) à l'aide du script, puis de passer à l'option Configuration automatique tout en utilisant le même nom de site. Dans ce cas, une base de données portant le même nom est déjà créée lors de l'exécution du script.

    Résolution : vous devez renommer le site, puis réexécuter le script.
  - La machine ne dispose pas des autorisations READ, WRITE, UPDATE pour créer des tables dans la base de données sur le serveur SQL.

Résolution : Activez les autorisations appropriées sur la machine. Pour plus de détails, voir Autorisations requises pour configurer les bases de données.

- **Message d'erreur** : Impossible de créer la base de données : échec de la connexion

  Résolution :

  - Vérifiez la connectivité réseau de la base de données depuis votre machine. Assurez-vous que le port du serveur SQL est ouvert sur le pare-feu.
  - Si vous utilisez un serveur SQL distant, vérifiez si un identifiant a été créé sur le serveur SQL avec l'identité de machine Secure Private Access, Domain\hostname$.
  - Si vous utilisez un serveur SQL distant, vérifiez que le rôle approprié a été attribué à l'identité de la machine, à savoir le rôle d'administrateur système.
  - Si vous utilisez un serveur SQL local (qui ne provient pas du programme d'installation), vérifiez si l'utilisateur NT AUTHORITY \ SYSTEM doit avoir créé un identifiant.

Défaillances de StoreFront

- **Message d'erreur** : Impossible de créer une entrée StoreFront pour : `<Store URL>`

  Mettez à jour les entrées de StoreFront depuis l'onglet **Paramètres** si elles ne sont pas visibles. Après avoir configuré Secure Private Access à l'aide de l'assistant, vous pouvez modifier les entrées de StoreFront depuis l'onglet **Paramètres** . Notez l'URL du StoreFront Store pour laquelle cette erreur s'est produite.

  Résolution :

  1. Cliquez sur **Paramètres**, puis sur l'onglet **Intégrations** .
  2. Dans l'**URL du magasin** StoreFront, ajoutez l'entrée StoreFront si elle n'est pas visible.

- **Message d'erreur** : Impossible de configurer l'entrée StoreFront pour : `<Store URL>`

  Résolution :

  1. Il se peut qu'une restriction de la stratégie d'exécution de PowerShell soit en place. Exécutez la commande de script PowerShell `Get-ExecutionPolicy` pour plus de détails.
  2. S'il est restreint, vous devez le contourner et exécuter un script de configuration StoreFront manuellement.
  3. Cliquez sur **Paramètres**, puis sur l'onglet **Intégrations** .
  4. Dans **StoreFront Store URL**, identifiez l'entrée d'URL StoreFront pour laquelle l'erreur s'est produite.
  5. Cliquez sur le bouton **Télécharger le script** à côté de l'URL de ce magasin et exécutez ce script PowerShell avec des privilèges d'administrateur sur la machine sur laquelle l'

installation StoreFront correspondante est présente. Ce script doit être exécuté sur toutes les machines StoreFront.

> **Remarque :**
>
> Si vous réessayez l'installation après la désinstallation, assurez-vous qu'aucune entrée portant le nom « Secure Private Access » ne figure dans la configuration de StoreFront (StoreFront**> store> Delivery Controller**-> Secure Private Access). Si Secure Private Access est présent, supprimez cette entrée. Téléchargez et exécutez le script manuellement depuis la page Paramètres > Intégrations.

- **Message d'erreur** : la configuration de StoreFront n'est pas locale pour : <`Store URL`>

  Après avoir configuré Secure Private Access à l'aide de l'assistant, vous pouvez modifier les entrées de la passerelle depuis l'onglet Paramètres . Notez l'URL du StoreFront Store pour laquelle cette erreur s'est produite.

  Résolution :

  Ce problème se produit si StoreFront n'est pas installé sur la même machine que Secure Private Access. Vous devez exécuter manuellement la configuration de StoreFront sur la machine sur laquelle vous avez installé StoreFront.

  1. Cliquez sur **Paramètres**, puis sur l'onglet **Intégrations** .
  2. Dans **StoreFront Store URL**, identifiez l'entrée d'URL StoreFront pour laquelle l'erreur s'est produite.
  3. Cliquez sur le bouton Télécharger le script à côté de l'URL de ce magasin et exécutez ce script PowerShell avec des privilèges d'administrateur sur la machine sur laquelle l'installation StoreFront correspondante est présente. Ce script doit être exécuté sur toutes les machines StoreFront.

  > **Remarque :**
  >
  > pour exécuter le script StoreFront PowerShell, ouvrez la fenêtre PowerShell compatible avec Windows x64 avec des privilèges d'administrateur, puis exécutez ConfigureStoreFront.ps1. Le script StoreFront n'est pas compatible avec Windows PowerShell (x86).

- **Message d'erreur** : « Get-STFStoreService : une exception de type 'Citrix.DeliveryServices.Framework.Featu
  a été générée. » lors de l'exécution du script StoreFront à l'aide de PowerShell.

  Cette erreur se produit lorsque le script StoreFront est exécuté sur une fenêtre PowerShell compatible x86.

  Résolution :

Pour exécuter le script StoreFront PowerShell, ouvrez la fenêtre PowerShell compatible avec Windows x64 avec des privilèges d'administrateur, puis exécutez`ConfigureStorefront.ps1`.

Défaillances de la passerelle publique/de la passerelle de rappel

Message d'erreur : Impossible de créer une entrée de passerelle pour : <`Gateway URL`> OU Impossible de créer une entrée de passerelle de rappel pour : <`Callback Gateway URL`>

Résolution :

Notez l'URL de la passerelle publique ou de la passerelle de rappel pour laquelle l'échec s'est produit. Après avoir configuré Secure Private Access à l'aide de l'assistant, vous pouvez modifier les entrées de la passerelle depuis l'onglet **Paramètres** .

1. Cliquez sur **Paramètres**, puis sur l'onglet **Intégrations** .
2. Mettez à jour l'adresse de la passerelle publique ou l'adresse de la passerelle de rappel et l'adresse IP virtuelle pour laquelle l'échec s'est produit.

Le serveur Secure Private Access n'est pas accessible

Message d'erreur : Impossible de mettre à jour le pool IIS. Impossible de redémarrer le pool IIS

Résolution :

Accédez aux pools d'applications dans Internet Information Services (IIS) et vérifiez que les pools d'applications suivants ont démarré et sont en cours d'exécution :

- Pool d'exécution à accès privé sécurisé
- Pool d'administrateurs d'accès privé sécurisé

Vérifiez également que le site IIS par défaut `"Default Web Site"` est opérationnel.

Échec des contrôles de connectivité de la base

Message d'erreur : échec de la vérification de connectivité

La vérification de la connectivité de la base de données peut échouer pour plusieurs raisons :

- Le serveur de base de données n'est pas accessible depuis la machine hôte du plug-in Secure Private Access en raison d'un pare-feu.

  Résolution : Vérifiez si le port de base de données (port 1433 par défaut) est ouvert sur le pare-feu.

- La machine hôte du plug-in Secure Private Access n'est pas autorisée à se connecter à la base de données.

  Résolution : consultez les autorisations de base de données SQL pour Secure Private Access.

La vérification de la connectivité de la passerelle a échoué. Impossible de récupérer le certificat public

Message d'erreur : La configuration après l'installation échoue avec l'erreur « La vérification de la connectivité de la passerelle a échoué. Impossible de récupérer un certificat public… »

Résolution :

- Téléchargez manuellement le certificat public de la passerelle dans la base de données Secure Private Access à l'aide de l'outil de configuration.
- Ouvrez le PowerShell ou la fenêtre d'invite de commande avec les privilèges d'administrateur.
- Remplacez le répertoire par le dossier Admin\AdminConfigTool dans le dossier d'installation de Secure Private Access (par exemple, cd « C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool »)
- Exécutez la commande suivante :

```
.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

Échec de l'énumération des applications

L'énumération des applications est interrompue si l'URL StoreFront ou l'URL NetScaler Gateway contient une barre oblique (/) à la fin.

Résolution :

Supprimez la barre oblique finale dans l'URL du magasin StoreFront ou dans l'URL de NetScaler Gateway. Pour plus de détails, consultez Mettre à jour StoreFront ou les informations relatives au serveur NetScaler Gatewayaprès la configuration.

Divers

Créez un pack d'assistance pour les diagnostics Secure Private Access

Procédez comme suit pour créer un pack de support pour les diagnostics Secure Private Access :

- Ouvrez le PowerShell ou la fenêtre d'invite de commande avec les privilèges d'administrateur.

- Remplacez le répertoire par le dossier Admin \ AdminConfigTool dans le dossier d'installation de Secure Private Access (par exemple, cd « C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool »).
- Exécutez la commande suivante :

```
.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>
```

Autorisations de base de données SQL pour Secure Private Access

Pour la création automatique de la base de données, la machine hôte du plug-in Secure Private Access doit disposer des autorisations nécessaires pour se connecter à la base de données et créer le schéma de base de données.

Base de données distante :

Procédez comme suit pour configurer les autorisations pour une base de données distante.

1. Créez une base de données vide avec la syntaxe du nom `CitrixAccessSecurity<Site Name>`. Ici `<Site Name>` est le nom du site Secure Private Access. (par exemple. CitrixAccessSecuritySPA).

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. Créez un identifiant SQL Server pour l'identité de la machine virtuelle Secure Private Access. Par exemple, si le nom de votre machine de courtage Secure Private Access est HOST1 et que le domaine de la machine est DOMAIN1, l'identité de la machine est « DOMAIN1\HOST1$ ». Si l'identifiant est déjà créé, vous pouvez ignorer cette étape.

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
   ```

   Le nom de domaine peut être trouvé à l'aide de la requête suivante :

   ```
   SELECT DEFAULT_DOMAIN()[DomainName]
   ```

3. Attribuez le rôle db_owner à l'identité de la machine.

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'

   ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
   ```

Base de données locale :

Procédez comme suit pour configurer les autorisations pour une base de données locale.

1. Créez une base de données vide avec la syntaxe du nom `CitrixAccessSecurity<Site Name>`. Ici `<Site Name>` est le nom du site Secure Private Access. (par exemple, Citrix AccessSecuritySPA).

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. Créez un identifiant SQL Server pour l'utilisateur `NT AUTHORITY\SYSTEM`. Si l'identifiant est déjà créé, vous pouvez ignorer cette étape.

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS
   ```

3. Attribuez le rôle db_owner à l'utilisateur « NT AUTHORITY\SYSTEM ».

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'NT AUTHORITY\SYSTEM'

   ALTER USER [NT AUTHORITY\SYSTEM] WITH DEFAULT_SCHEMA = dbo;
   ```

Lorsque vous créez manuellement la base de données, le script de base de données téléchargé ajoute les autorisations à l'identité de la machine.

Conserver les journaux de dépannage

December 27, 2023

Les journaux de la page **Logs de dépannage** sont stockés dans la base de données Secure Private Access pendant 90 jours. Si le nombre total de journaux devient trop important, par exemple plus de 100 000, vous pouvez supprimer les journaux les plus anciens datant de plus de 90 jours. Par défaut, la tâche de nettoyage est exécutée toutes les 12 heures. La tâche s'exécute également chaque fois que le service d'exécution redémarre.

Personnalisation des paramètres de conservation des journaux de dépannage

Le nettoyage des journaux est configurable via le fichier appsettings.json dans le dossier d'installation du service Runtime. Vous pouvez configurer le nettoyage en fonction de l'âge des journaux et du nombre de journaux pouvant être stockés dans la base de données. Modifiez les entrées suivantes dans le fichier appsettings.json, selon les besoins :

Exemple de fichier appsettings.json :

```
1   "TroubleshootingLogs": {
2
```



```
    "CleanupPeriodInHours": 12,
    "CleanupDataOlderThanDays": 90,
    "CleanupOldestDataIfEntriesCountAbove": 100000
   }

<!--NeedCopy-->
```

Pour désactiver le nettoyage, configurez les paramètres suivants selon vos besoins :

- Pour conserver les journaux pendant 7 jours uniquement, réglez sur `CleanupDataOlderThanDays` 7.
- Pour désactiver le nettoyage basé sur les jours, réglez `CleanupDataOlderThanDays`sur 0.
- Pour désactiver le nettoyage basé sur le nombre, réglez `CleanupOldestDataIfEntriesCountAbove` sur 0.
- Si ces deux paramètres sont définis sur 0, ou s'ils `CleanupPeriodInHours`sont définis sur 0, les journaux sont conservés pour toujours.
  - Il n'est pas recommandé de définir `CleanupPeriodInHours`les deux `CleanupDataOlderThanD` sur `CleanupOldestDataIfEntriesCountAbove`0 ou sur 0, car cela pourrait entraîner un problème d'utilisation du disque à 100 %.
  - La fréquence de nettoyage des journaux peut également être modifiée en modifiant l`CleanupPeriodInHours`'entrée.

> **Remarque :**
>
> Si Secure Private Access est déployé en tant que cluster, ces paramètres doivent être modifiés dans chaque nœud du cluster. En cas de non-concordance entre les paramètres du nœud, l'instance nettoyée le plus fréquemment est prioritaire.

Nettoyage des journaux et de la télémétrie

December 27, 2023

Nettoyage des données de télémétrie

Les données de télémétrie sont stockées dans la base de données Secure Private Access pendant 3 mois. Les contrôles visant à identifier les données de télémétrie devant être nettoyées sont effectués toutes les 30 secondes.

> **Remarque :**
>
> Le service Runtime doit être en cours d'exécution pour déclencher le nettoyage des données de télémétrie.

Nettoyage des journaux CDF

Les journaux CDF sont stockés sur la machine d'installation de Secure Private Access, dans les dossiers d'installation des services Admin et Runtime. Les journaux CDF sont placés dans des fichiers .csv avec une limite de taille de 10 Mo appliquée à chaque fichier.
Le service Admin peut conserver jusqu'à 90 fichiers journaux CDF à la fois, après quoi il supprime les fichiers les plus anciens afin de libérer de l'espace pour la création des nouveaux fichiers journaux CDF.
Le service Runtime fonctionne de la même manière que le service Admin mais peut conserver un plus grand nombre de fichiers à la fois, jusqu'à 600.

Nettoyage personnalisé des journaux CDF

Le nettoyage des journaux CDF est configurable via les fichiers appsettings.json situés dans les dossiers d'installation des services Admin et Runtime. Pour modifier la taille et le nombre maximum de fichiers, mettez à jour les entrées suivantes dans le fichier appsettings.json :

```
"CdfFile": {

      "fileSizeLimitBytes": 10485760, // 10 MB
      "retainedFileCountLimit": 600
     }

<!--NeedCopy-->
```

> **Remarque :**
>
> Si plusieurs instances de Secure Private Access sont configurées pour le site, mettez à jour les fichiers appsettings.json pour le nettoyage du CDF sur chaque machine d'installation de Secure Private Access.

Désinstallez Secure Private Access

December 27, 2023

Vous pouvez désinstaller Secure Private Access depuis **le Panneau de configuration > Programmes > Programmes et fonctionnalités**.

1. Sélectionnez **Citrix Virtual Apps and Desktops 7 2308 —Secure Private Access**.
2. Cliquez sur **Désinstaller**.
3. Suivez les instructions qui s'affichent à l'écran et terminez la désinstallation.

> **Remarque :**
>
> Si la configuration post-installation de Secure Private Access est terminée, téléchargez le fichier StoreFrontScripts.zip depuis la console d'administration avant de désinstaller Secure Private Access pour supprimer le plug-in Secure Private Access de la configuration du magasin StoreFront.

Pour télécharger le fichier zip StorefrontScripts, procédez comme suit :

1. Connectez-vous à la console d'administration Secure Private Access.
2. Cliquez sur **Paramètres**, puis sur l'onglet **Intégrations** .
3. Cliquez sur **Télécharger le script** dans la section URL de StoreFront Store.

Supprimer le plug-in Secure Private Access de la configuration du magasin StoreFront

Après avoir désinstallé Secure Private Access, vous devez supprimer le plug-in Secure Private Access de la configuration du magasin StoreFront.

1. Connectez-vous à la machine StoreFront.
2. Téléchargez le fichier StoreFrontScripts.zip.
3. Décompressez StoreFrontScripts.zip dans un dossier.
4. Ouvrez une fenêtre PowerShell avec les privilèges d'administrateur.
5. Exécutez la commande suivante :

```
cd <unzipped folder>
.\RemoveStorefrontConfiguration.ps1
```

Compatibilité de Secure Private Access 2311 avec les anciennes versions

February 16, 2024

Secure Private Access 2311 n'est pas compatible avec les anciennes versions. NetScaler Gateway doit être configuré à l'aide du nouveau script, comme décrit précédemment dans la section Configurer NetScaler Gateway. Aucune configuration n'est requise dans le Delivery Controller Citrix Virtual Apps and Desktops pour les anciennes versions de Secure Private Access.

La meilleure façon de migrer des anciennes versions vers la version 2311 est de nettoyer les points suivants :

- Contrôleur de livraison Citrix Virtual Apps and Desktops à partir d'applications Web/SaaS
- Mettez à jour la configuration par défaut de Citrix StoreFront ou créez un nouveau magasin sur StoreFront
- NetScaler Gateway

Nettoyage du Citrix Virtual Apps and Desktops Delivery Controller

Les applications Secure Private Access créées sur Citrix Virtual Apps and Desktops Delivery Controller peuvent être supprimées manuellement ou à l'aide du script PowerShell.

Manuel :

1. Ouvrez Citrix Studio ou Citrix WebStudio.
2. Cliquez sur **Applications**.
3. Sélectionnez l'application, cliquez avec le bouton droit de la souris, puis sélectionnez **Supprimer**.

À l'aide d'un script :

1. Récupérez les applications Secure Private Access actuelles en exécutant la commande suivante :

   ```
   Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"
   ```

   Pour plus de détails, voir Remove-BrokerApplication.

2. Après avoir vérifié les applications, exécutez la commande suivante pour les supprimer :

   ```
   Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"| Remove-BrokerApplication
   ```

Nettoyage de Citrix StoreFront

Vous pouvez créer un nouveau magasin StoreFront ou nettoyer le magasin existant.

- Créer une nouvelle boutique StoreFront : vous devez créer une nouvelle boutique StoreFront pour Secure Private Access 2311 car les boutiques StoreFront existantes créées pour les anciennes versions ne sont pas compatibles avec 2311. Il s'agit de l'option recommandée pour éviter les problèmes liés à la configuration.
- Nettoyer le magasin StoreFront existant : le magasin existant sur StoreFront peut être nettoyé manuellement ou à l'aide du script. Toutefois, la meilleure option pour migrer Secure Private Access sur site vers 2311 est de créer un nouveau Store sur StoreFront.

Manuel :

1. Recherchez et supprimez policy.json (par exemple C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrow

2. Recherchez et supprimez les dossiers SecureBrowser (par exemple C:\inetpub\wwwroot\Citrix\Store\Resour et Resources (par exemple C:\inetpub\wwwroot\Citrix\Store\Resources).
3. Supprimez le nœud « route » de web.config (vous le trouverez dans C:\inetpub\wwwroot\Citrix\Store) avec le nom « WebSecurePolicy » pour le routage vers l'URL « Resources \ SecureBrowser \ policy.json ».
4. Redémarrez le **site Web par défaut sur la console Internet Information Service (IIS) Manager** pour appliquer les modifications.

À l'aide d'un script :

1. Téléchargez le script depuis https://www.citrix.com/downloads/citrix-secure-private-access/.
2. Téléchargez le script sur une machine StoreFront.
3. Exécutez le script en tant qu'administrateur sur PowerShell.
4. Entrez le nom du magasin.

   Le script supprime le dossier C:\inetpub\wwwroot\Citrix\Store\Resources, le sous-dossier et les fichiers, et met à jour le fichier web.config.
5. Redémarrez le **site Web par défaut sur la console Internet Information Service (IIS) Manager** pour appliquer les modifications.

Nettoyage de NetScaler Gateway

Serveur virtuel NetScaler Gateway

Le serveur virtuel NetScaler Gateway créé pour les anciennes versions peut être réutilisé pour Secure Private Access 2311.

- Pour mettre à jour un NetScaler Gateway existant, voir Mettre à jour un NetScaler Gateway existant.
- Pour configurer un nouveau NetScaler Gateway, voir Configurer NetScaler Gateway.

Stratégies et actions relatives aux sessions

Les politiques de session et les actions créées pour les anciennes versions peuvent être réutilisées par Secure Private Access 2311.

- Pour mettre à jour les stratégies/actions d'une session NetScaler Gateway existante, consultez la section Actions de session NetScaler Gateway.
- Pour configurer un nouveau NetScaler Gateway, voir Configurer NetScaler Gateway

Le script crée également des stratégies/actions de session entièrement configurées.

Stratégies d'autorisation

Les politiques d'autorisation créées sur NetScaler Gateway pour les anciennes versions peuvent interférer avec les politiques Secure Private Access 2311 et interrompre le flux.

Vous pouvez effectuer les opérations suivantes pour nettoyer les stratégies d'autorisation.

- Dissociez manuellement les stratégies d'autorisation des groupes d'authentification et d'autorisation utilisés comme groupes par défaut sur NetScaler Gateway. Dans ce cas, les stratégies peuvent être réutilisées.
- Supprimez les stratégies d'autorisation.

Notifications de tiers

December 27, 2023

Citrix Secure Private Access pour locaux