Citrix Secure Private Access - Sur site

Machine translated content

Disclaimer

Contents

Vue d'ensemble technique

August 26, 2024

La solution Citrix Secure Private Access locale est une solution ZTNA (Zero Trust Network Access) gérée par le client qui fournit un accès sans VPN aux applications Web et SaaS internes avec les éléments suivants, ainsi qu'une expérience utilisateur fluide pour l'utilisateur final :

- Principe du moindre privilège
- Authentification unique (SSO)
- Authentification multifacteur
- Évaluation de la posture de périphérique
- Contrôles de sécurité au niveau des applications
- Fonctionnalités App Protection

La solution s'appuie sur l'application StoreFront sur site et Citrix Workspace pour offrir une expérience d'accès fluide et sécurisée permettant d'accéder aux applications Web et SaaS dans Citrix Enterprise Browser. Cette solution s'appuie également sur NetScaler Gateway pour appliquer les contrôles d'authentification et d'autorisation.

La solution Citrix Secure Private Access locale 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 une instance locale de StoreFront comme portail d'accès unifié aux applications Web et SaaS, ainsi qu'aux applications et bureaux virtuels intégrés à Citrix Workspace.

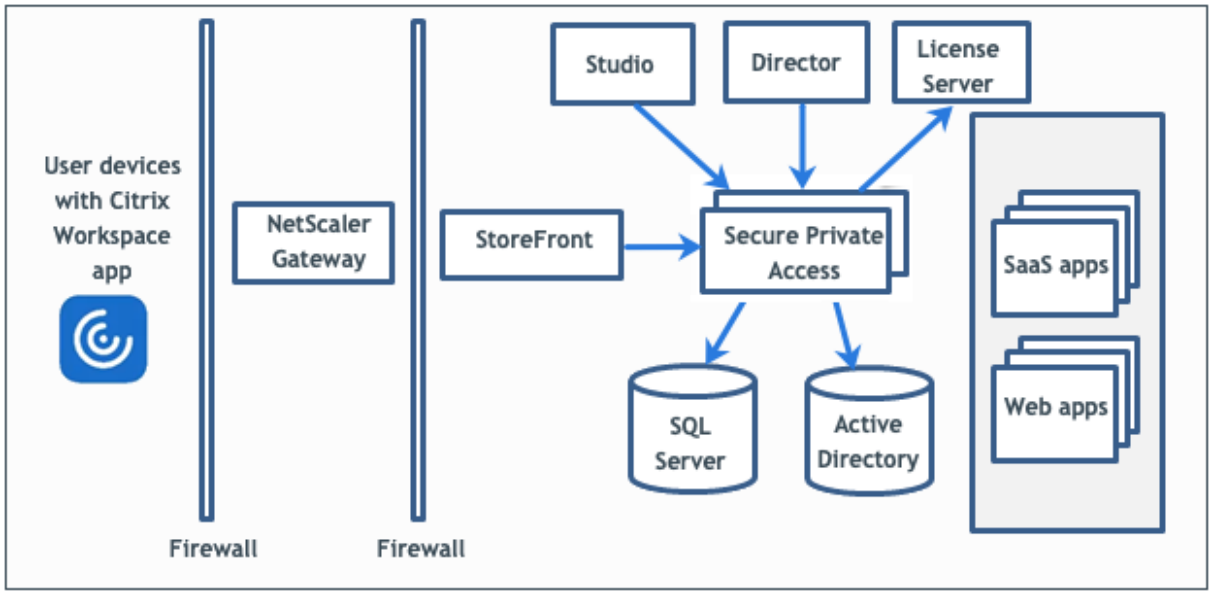
Citrix Secure Private Access combine les éléments de NetScaler Gateway et de StoreFront pour offrir une expérience intégrée aux utilisateurs et aux administrateurs.

Fonctionnalité	Service/Composant fournissant la fonctionnalité
Interface utilisateur cohérente pour accéder aux applications	Application StoreFront sur site/Citrix Workspace
SSO vers SaaS et applications Web	NetScaler Gateway
Authentification multifactorielle (MFA) et état de sécurité de l'appareil (également appelée analyse du point de terminaison)	NetScaler Gateway
Contrôles de sécurité et contrôles de protection des applications pour les applications Web et SaaS	Citrix Enterprise Browser
Stratégies d'autorisation	Secure Private Access

Fonctionnalité	Service/Composant fournissant la fonctionnalité
Contrôle de l'accès	Clients NetScaler Gateway et Citrix Secure Access
Configuration et gestion	Secure Private Access
Visibilité, surveillance et résolution des problèmes	Secure Private Access, console NetScaler (anciennement ADM) et Citrix Director

Composants

Cette illustration montre les composants d'un déploiement type de Secure Private Access.



Pour plus d'informations sur chaque composant, voir Composants principaux.

Nouveautés

August 26, 2024

Février 2023

Intégration de Citrix Secure Private Access à Director

Citrix Secure Private Access est désormais intégré à Director pour la gestion des performances et un dépannage amélioré. Pour plus de détails, consultez la section Intégration de Secure Private Access à

Director.

Afficher les sessions utilisateur de Secure Private Access dans Director

Vous pouvez désormais consulter les sessions utilisateur de View Secure Private Access dans Director. Vous pouvez consulter les détails concernant les sessions actives et celles ayant échoué. Vous pouvez également accéder à des informations relatives aux applications, aux stratégies et aux détails des sessions ayant échoué et réussi. Pour plus de détails, voir Afficher les sessions Secure Private Access par utilisateur.

Intégration de Citrix Secure Private Access au serveur de licences

Citrix Secure Private Access est désormais intégré au serveur de licences pour collecter et traiter les données de licence. Pour plus de détails, voir Serveur de licences avec Secure Private Access.

Problèmes résolus

August 26, 2024

Les problèmes suivants sont résolus dans la version 2402.

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).

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.

Problèmes connus

August 26, 2024

Les problèmes suivants existent dans la version 2402.

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 en tant qu'identité dans le pool d'applications IIS pour le service d'administration et d'exécution Secure Private Access.

- 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 de distribution ne sont pas pris en charge dans Secure Private Access. Par conséquent, les stratégies ne peuvent pas rechercher de groupes de distribution 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 le Web n'est pas pris en charge et les applications ne sont donc pas énumérées. Pour plus de détails, consultez la section Utilisation de StoreFront version 2311 ou ultérieure.

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.

Lancement d'application

Le lancement d'application échoue si toutes les conditions suivantes sont remplies :

- Les versions 13.0.x et 13.1 de Netscaler antérieures à 13.1-48.47 et 14.1 antérieures à 14.1—4.42 sont utilisées.
- Les UPN LDAP sont configurés avec un suffixe différent de celui du domaine réel.
- L'UPN LDAP et sAMAccountName sont différents.

Mises à niveau

- La mise à niveau de la version 2308 avec les versions 2402 et ultérieures n'est pas prise en charge.
- Si un certificat SSL personnalisé est utilisé pour le service d'administration Secure Private Access, le certificat doit être à nouveau lié au site « Citrix Access Security Admin » sur Internet Information Service (IIS).

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 de Receiver est affichée sur le client. Pour plus d'informations sur la configuration de StoreFront, consultez StoreFront.

- 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.

Console d'administration

- Lors de l'ajout d'une application, si le nom de l'application contient une virgule, un avertissement s'affiche. L'application est toutefois créée.

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

Lorsque vous mettez à niveau Secure Private Access 2311 avec la version 2402 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.

- **Citrix Virtual Apps and Desktops 7 2402 LTSR**
- **Citrix Virtual Apps and Desktops 7 2311 - Secure Private Access**

Vous pouvez désinstaller le programme d'installation de la version 2311 en sélectionnant **Citrix Virtual Apps and Desktops 7 2311 -Secure Private Access**.

> **Remarque :**
>
> Ce problème n'est pas observé lorsque le programme d'installation autonome de Secure Private Access 2311 est mis à niveau avec le programme d'installation autonome 2402.

Configuration système requise

August 26, 2024

Assurez-vous que votre produit répond aux exigences minimales de la version.

- Application Citrix Workspace
  - Windows —2309 et versions ultérieures
  - macOS —2309 et versions ultérieures
- Système d'exploitation pour le serveur de plug-in Secure Private Access - Windows Server 2019 et versions ultérieures
- StoreFront —LTSR 2203 ou CR 2212 et versions ultérieures
- NetScaler : versions 13.0, 13.1, 14.1 et versions ultérieures. Il est recommandé d'utiliser les dernières versions de NetScaler Gateway version 13.1 ou 14.1 pour optimiser les performances.
- Director 2402 ou version ultérieure
- Ports de communication : assurez-vous d'avoir ouvert les ports requis pour le plug-in Secure Private Access. Pour plus de détails, consultez la section Ports de communication.

> **Remarque :**
>
> Secure Private Access pour les applications locales n'est pas pris en charge sur l'application Citrix Workspace pour iOS et Android.

Logiciels requis

Pour créer ou mettre à jour un NetScaler Gateway existant, assurez-vous de disposer des informations suivantes :

- Une machine serveur Windows sur laquelle IIS est en cours d'exécution, configurée avec un certificat SSL/TLS, sur laquelle le plug-in Secure Private Access sera installé.
- StoreFront stocke les URL à saisir lors de la configuration.
- Store on StoreFront doit avoir été configuré et l'URL du service Store doit être disponible. Le format de l'URL du service Store est `https://store.domain.com/Citrix/StoreSecureAccess`.
- Adresse IP NetScaler Gateway, nom de domaine complet et URL de rappel NetScaler Gateway.
- Adresse IP et nom de domaine complet de la machine hôte du plug-in Secure Private Access (ou d'un équilibreur de charge si le plug-in Secure Private Access est déployé en tant que cluster).
- Nom du profil d'authentification configuré sur NetScaler.
- Certificat de serveur SSL configuré sur NetScaler.
- Nom de domaine.

- Les configurations des certificats sont terminées. Les administrateurs doivent s'assurer que les configurations des certificats sont complètes. Le programme d'installation de Secure Private Access configure un certificat auto-signé si aucun certificat n'est trouvé sur la machine. Cependant, cela peut ne pas toujours fonctionner.

> **Remarque :**
>
> Le service d'exécution (application SecureAccess du site Web par défaut d'IIS) nécessite l'activation de l'authentification anonyme, car il ne prend pas en charge l'authentification Windows. Ces paramètres sont définis par défaut par le programme d'installation de Secure Private Access et ne doivent pas être modifiés manuellement.

Exigences relatives au compte d'administrateur

Les comptes d'administrateur suivants sont requis lors de la configuration de l'accès privé sécurisé.

- Installez Secure Private Access : vous devez être connecté avec un compte d'administrateur de machine local.
- Configurer Secure Private Access : vous devez vous connecter à la console d'administration Secure Private Access avec un utilisateur du domaine qui est également l'administrateur de la machine sur laquelle Secure Private Access est installé.
- Gérer Secure Private Access : vous devez vous connecter à la console d'administration de Secure Private Access avec un compte administrateur de Secure Private Access.

Ports de communication

Le tableau suivant répertorie les ports de communication utilisés par le plug-in Secure Private Access.

Source	Destination	Type	Port	Détails
Poste de travail administrateur	Plug-in Secure Private Access	HTTPS	4443	Plug-in Secure Private Access - Console d'administration
Plug-in Secure Private Access	Service NTP	TCP, UDP	123	Synchronisation de l'heure
	Service DNS	TCP, UDP	53	Recherche DNS
	Active Directory	TCP, UDP	88	Kerberos

Source	Destination	Type	Port	Détails
	Director	HTTP, HTTPS	80, 443	Communication avec le serveur Director pour la gestion des performances et l'amélioration du dépannage
	Serveur de licences	TCP	8083	Communication avec le serveur de licences pour la collecte et le traitement des données de licence
		TCP	389	LDAP sur Plaintext (LDAP)
		TCP	636	LDAP sur SSL (LDAPS)
	Microsoft SQL Server	TCP	1433	Plug-in Secure Private Access - Communication de base de données
	StoreFront	HTTPS	443	Validation d'authentification
	NetScaler Gateway	HTTPS	443	Rappel NetScaler Gateway
StoreFront	Service NTP	TCP, UDP	123	Synchronisation de l'heure
	Service DNS	TCP, UDP	53	Recherche DNS
	Active Directory	TCP, UDP	88	Kerberos
		TCP	389	LDAP sur Plaintext (LDAP)
		TCP	636	LDAP sur SSL (LDAPS)

Source	Destination	Type	Port	Détails
		TCP, UDP	464	Protocole d'authentification Windows natif permettant aux utilisateurs de modifier les mots de passe expirés
	Plug-in Secure Private Access	HTTPS	443	Authentification et énumération des applications
	NetScaler Gateway	HTTPS	443	Rappel NetScaler Gateway
NetScaler Gateway	Plug-in Secure Private Access	HTTPS	443	Validation des autorisations d'application
	StoreFront	HTTPS	443	Authentification et énumération des applications
	Applications Web	HTTP, HTTPS	80, 443	Communication NetScaler Gateway vers les applications Secure Private Access configurées *(les ports peuvent varier en fonction*des exigences de l'application)
Périphérique utilisateur	NetScaler Gateway	HTTPS	443	Communication entre l'appareil de l'utilisateur final et NetScaler Gateway

Références

- Profils d'authentification.
- Comment fonctionnent les stratégies d'authentification
- Liez un certificat SSL à un serveur virtuel (SSL) sur NetScaler.

Directives de dimensionnement

August 26, 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 stratégies sont négligeables par rapport aux journaux.

La figure suivante montre les exigences de stockage du serveur :

Number of users	Number of Secure Private Access server nodes	Secure Private Access node configuration			SQL Server (Secure Private Access Database only)			Active Directory		StoreFront	
		CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	CPU	Memory (GB)
1000	3	8	16	80	4	16	250	4	16	4	16
5000	8	8	16	80	16	16	750	16	16	4	16

Remarque :

- Les mesures sont dérivées en supposant que le nettoyage des événements du journal est désactivé et que la période de rétention 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 .

Configuration du serveur

Le tableau suivant présente les détails de configuration du serveur :

Configuration	Détails
Nombre total de requêtes	250
Nombre total de stratégies	50
Nombre d'applications par utilisateur	15
Configuration d'AD	Les utilisateurs font partie de 20 groupes, avec jusqu'à 20 niveaux d'imbrication
Résolution des problèmes liés à la période de rétention	7 jours (par défaut)
Résolution des problèmes au niveau du journal	Erreur (par défaut)
Rétention des journaux du serveur Secure Private Access	90 jours ou 600 dossiers

Profil de trafic

Le tableau suivant affiche les détails du profil de trafic par jour et par utilisateur.

Profil	Détails
Énumérations	10
Synchronisation des stratégies Enterprise Browser	20
Lancement de l'application depuis l'application Citrix Workspace	4
Accès aux applications depuis Citrix Enterprise Browser	500
Requêtes de dépannage du service d'assistance (par jour), via Citrix Director	1000

Directives de déploiement

Le tableau suivant indique les exigences de taille de la 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	Mémoire
Plug-in Secure Private Access	8	16 GB
Serveur SQL Secure Private Access	8	16 GB
StoreFront	16	8 GB
Gateway	4	8 GB
Active Directory	8	14 GB
Client	4	8 GB

Installer et configurer

August 26, 2024

Le programme d'installation de Secure Private Access est disponible en tant que programme autonome ou en tant que programme d'installation intégré de Citrix Virtual Apps and Desktops. Pour de plus amples informations, consultez Installer les composants principaux ou Installer à l'aide de la ligne de commande.

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**).

Configuration requise du compte administrateur pour installer et gérer 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.

Configurer Secure Private Access

Vous pouvez configurer Secure Private Access en suivant les étapes suivantes :

- Configurer Secure Private Access en créant un nouveau site ou configurer Secure Private Access en joignant un site existant
- Configuration des bases de données
- Intégrez StoreFront, NetScaler Gateway, Director et les serveurs de licences

Configuration des applications et des stratégies d'accès

Après avoir configuré l'environnement Secure Private Access, vous devez configurer les applications et les stratégies d'accès pour les applications.

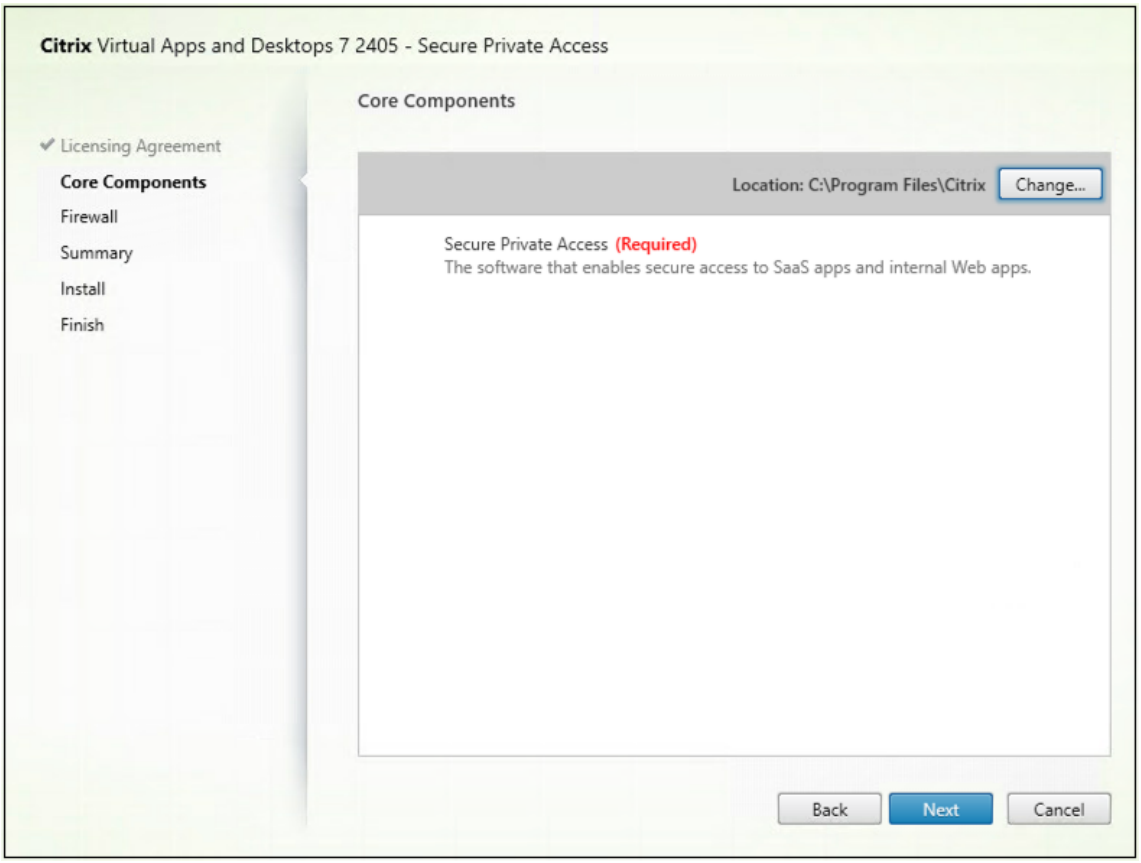
- Configurer les applications
- Configuration des stratégies d'accès pour les applications

Programme d'installation Secure Private Access

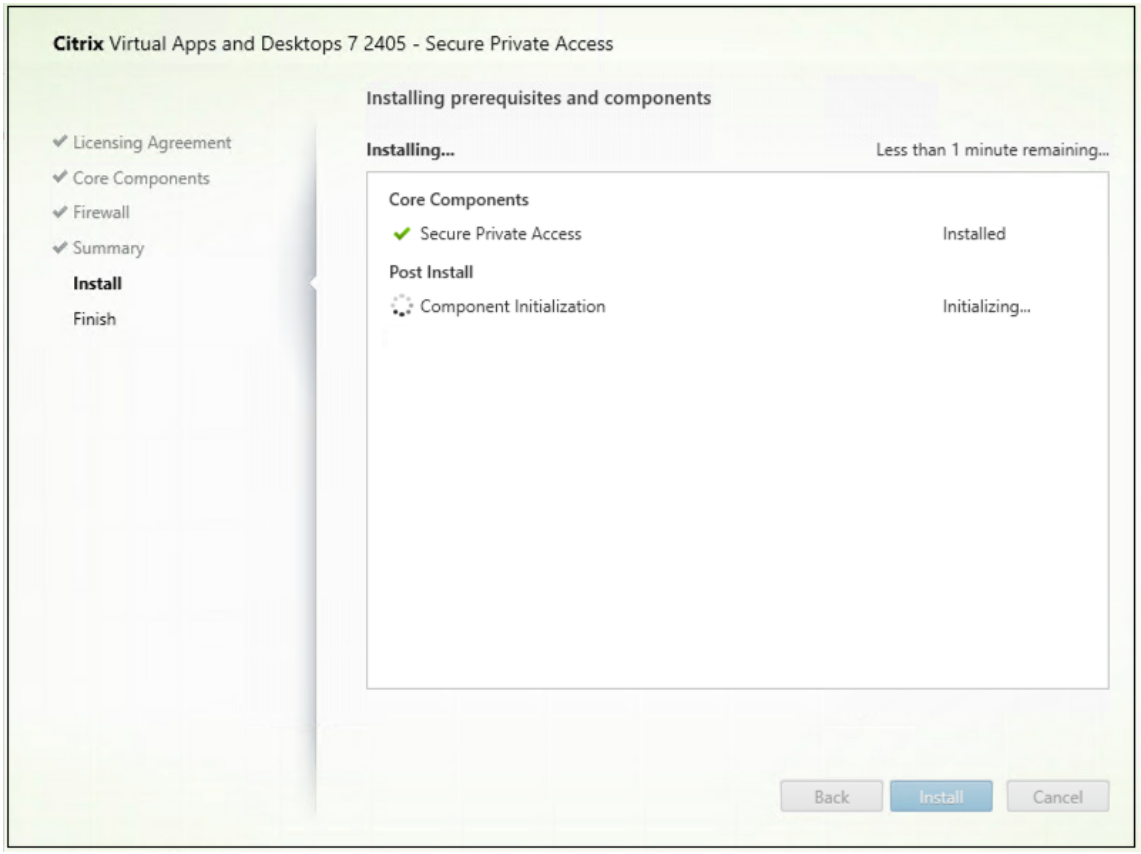
August 26, 2024

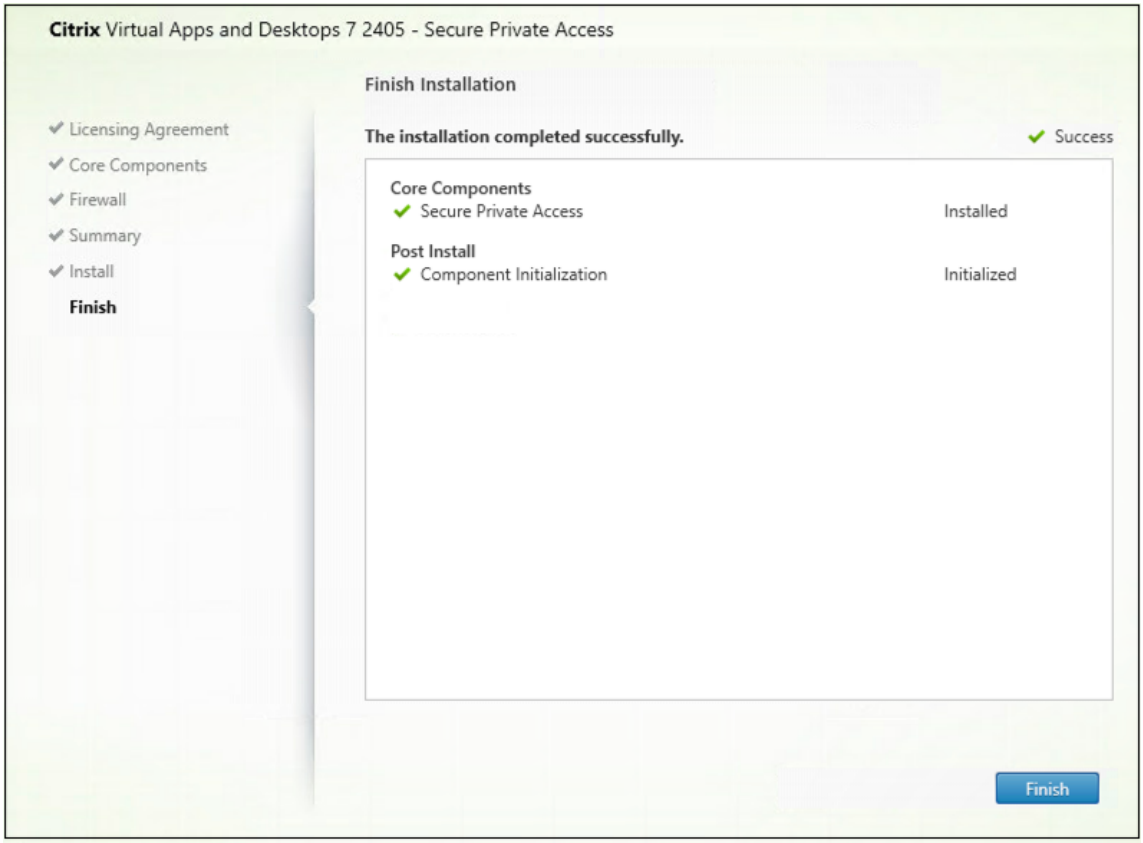
1. Téléchargez le programme d'installation de Citrix Secure Private Access depuis https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.
2. Exécutez le fichier .exe en tant qu'administrateur sur une machine associée à un domaine.

   > **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.

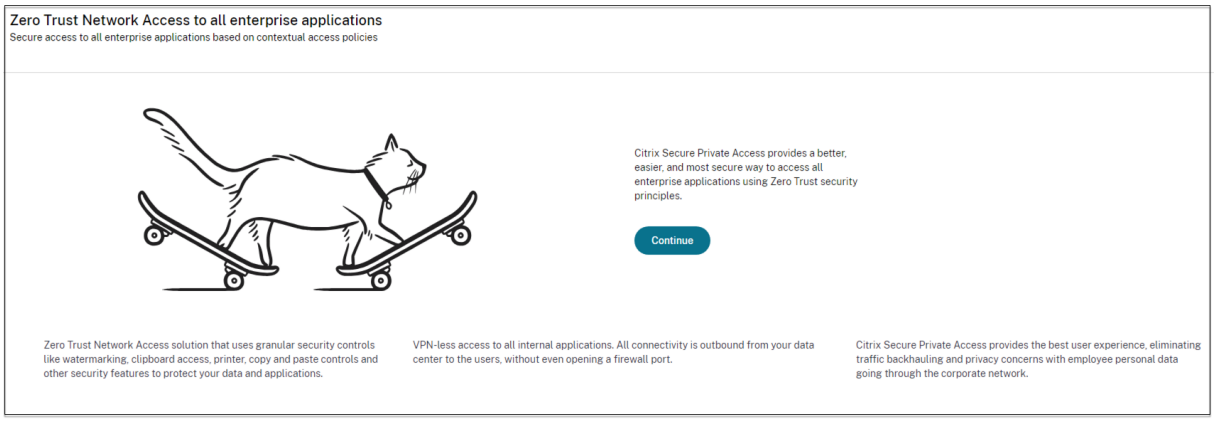


3. Suivez les instructions qui s'affichent à l'écran pour terminer l'installation.

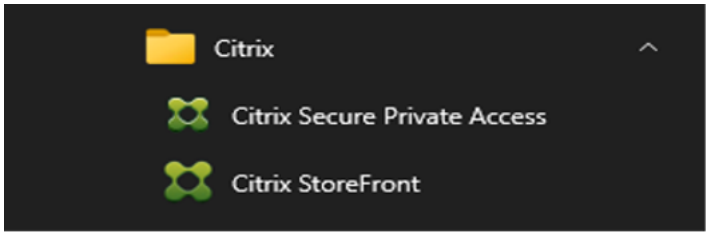




Une fois l'installation terminée, la console d'administration de la première installation s'ouvre automatiquement dans la fenêtre du navigateur par défaut. Vous pouvez cliquer sur **Continuer** pour configurer Secure Private Access.



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.

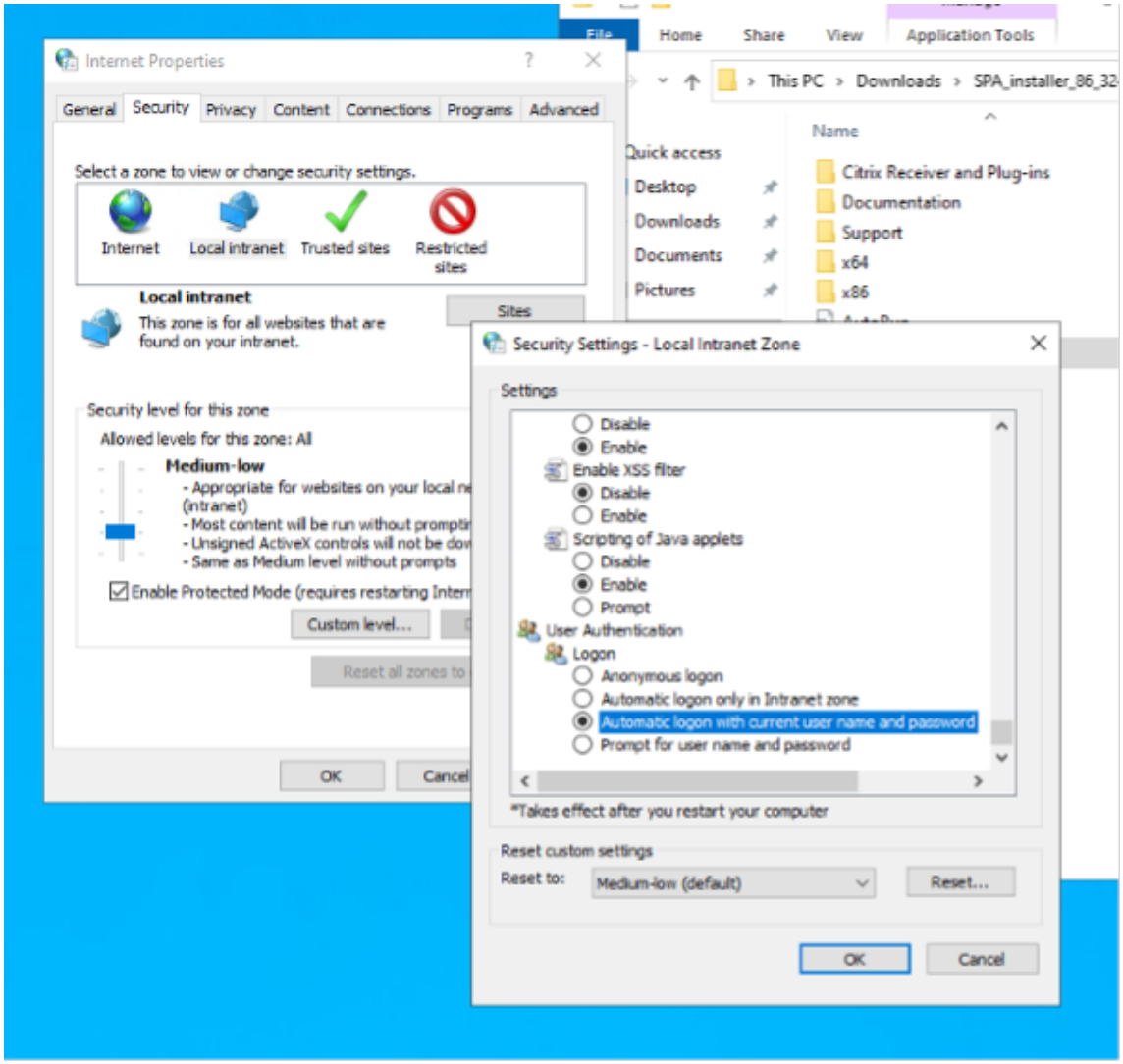
- Si vous entrez vos informations d'identification, vous activez l'authentification Windows intégrée (IWA).
- Si vous ne saisissez pas vos informations d'identification, la page de connexion Secure Private Access s'affiche.

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

Configurer Secure Private Access

August 26, 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

Logiciels requis

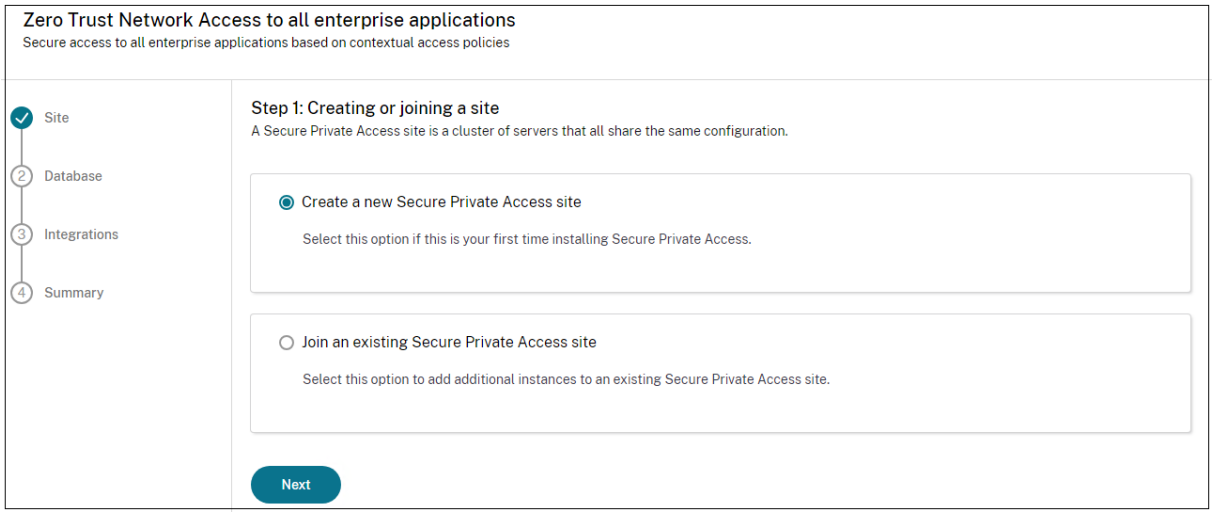
- Vous devez vous connecter à la console d'administration Secure Private Access avec un utilisateur du domaine qui est également un administrateur de machine local pour la machine sur laquelle Secure Private Access est installé.
- Le serveur de base de données SQL doit être installé avant de créer un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

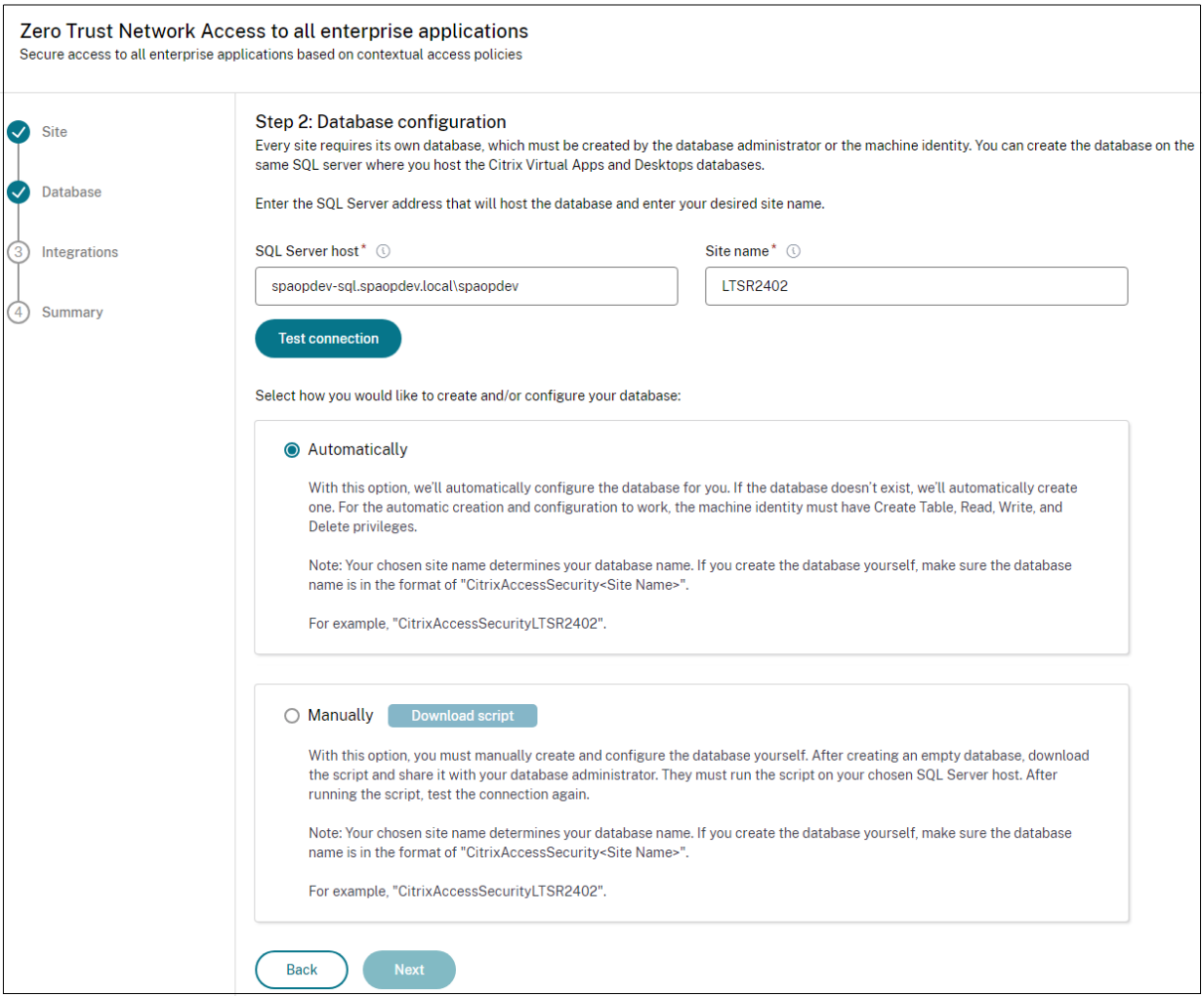
   - NomServeur
   - NomServeur\NomInstance
   - Nom du serveur, numéro de port

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

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

   > **Remarque :**
   >
   > Le nom du site que vous entrez est suffixé au nom de la base de données. Le format du nom de base de données est `CitrixAccessSecurity<sitename>` et ne peut pas être modifié. Si vous devez personnaliser le nom de la base de données, contactez le support Citrix.

3. Cliquez sur **Tester la connexion** pour vérifier que l'instance de SQL Server 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.

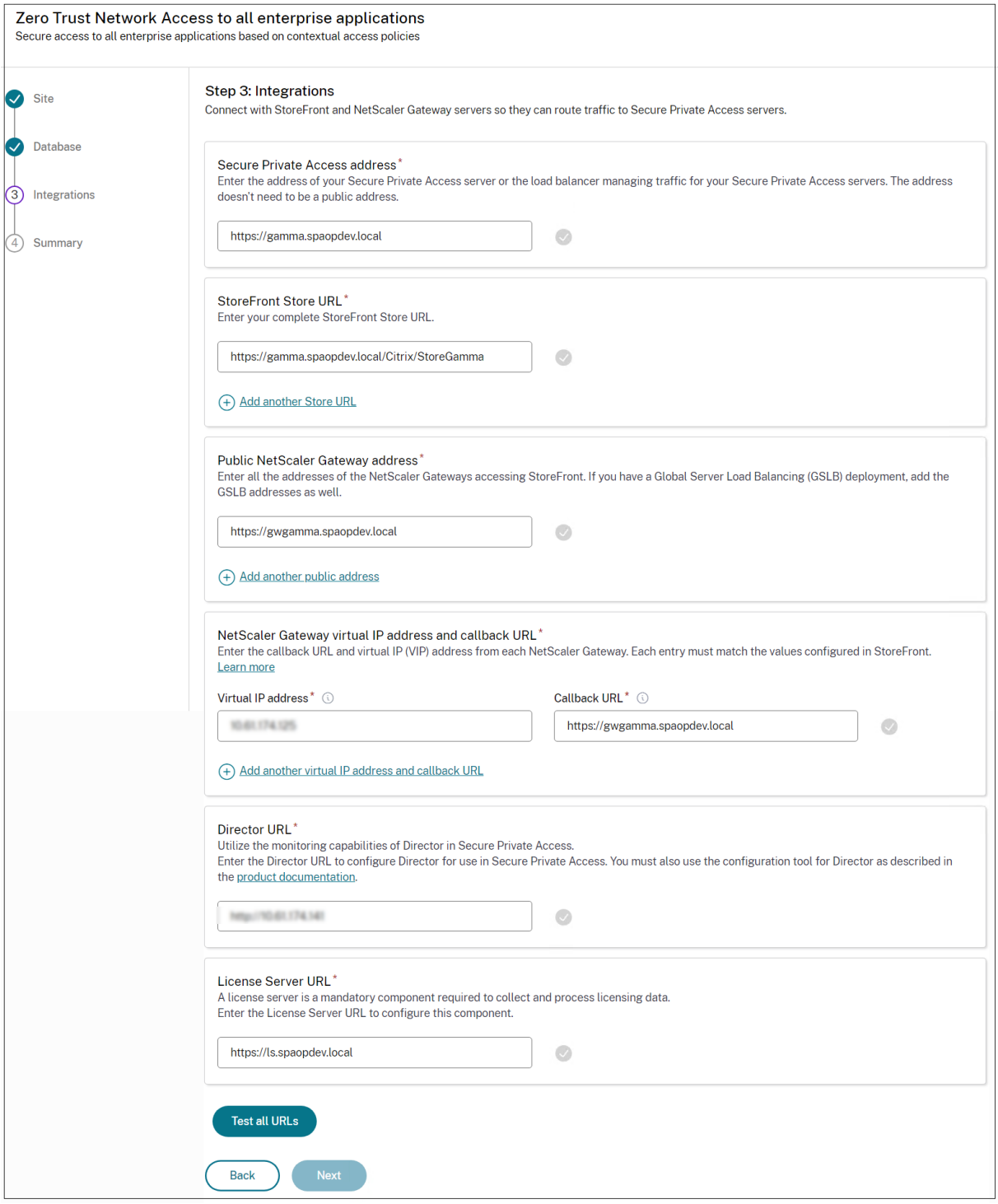
Dans la configuration manuelle, vous devez d'abord télécharger les scripts, puis les exécuter sur le serveur de base de données que vous avez spécifié dans le champ **SQL Server Host** .

> **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

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. Vous devez également spécifier les détails du serveur Director et du serveur de licences.

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 NetScaler Gateway publique : URL de NetScaler Gateway**. Par exemple, `https://gateway.domain.com`.
    - **Adresse IP virtuelle** : cette adresse IP virtuelle doit être la même que celle configurée dans StoreFront pour les rappels.
    - **URL de rappel** : cette URL doit être la même que celle configurée dans StoreFront. Par exemple, `https://gateway.domain.com`.
    - **URL du serveur Director :** - L'adresse IP ou le nom de domaine complet du serveur Director pour connecter Secure Private Access à Citrix Director.
    - **URL du serveur de licences :** - L'adresse IP du serveur de licences pour collecter et traiter les données de licence.
2. Cliquez sur **Valider toutes les URL**
3. Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.

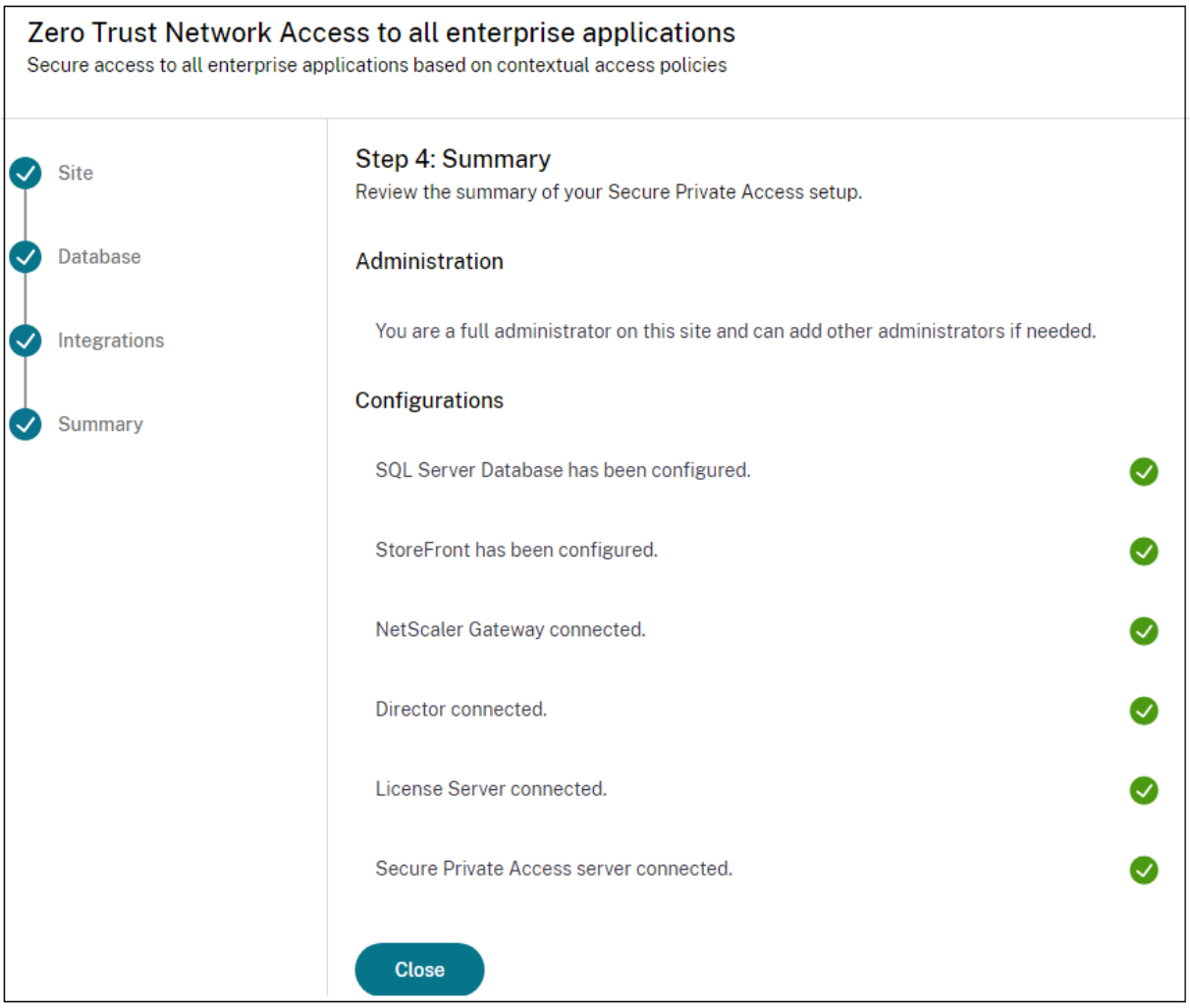


Étape 4 : Résumé de la configuration

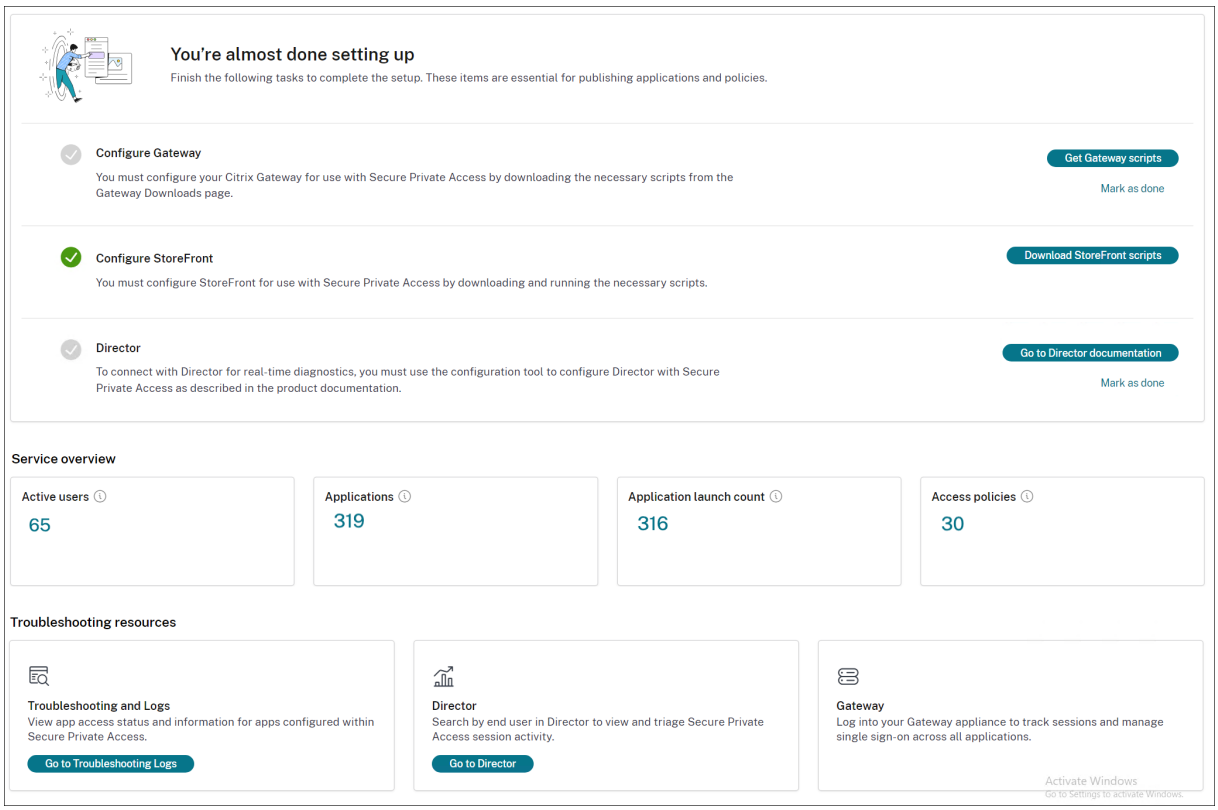
Une fois la configuration terminée, une validation est effectuée pour s'assurer que les serveurs configurés sont accessibles. En outre, une vérification est effectuée pour s'assurer que le serveur Secure

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.



Une fois la configuration terminée, la page suivante s'affiche lorsque vous cliquez sur **Fermer** sur la page de **résumé** .



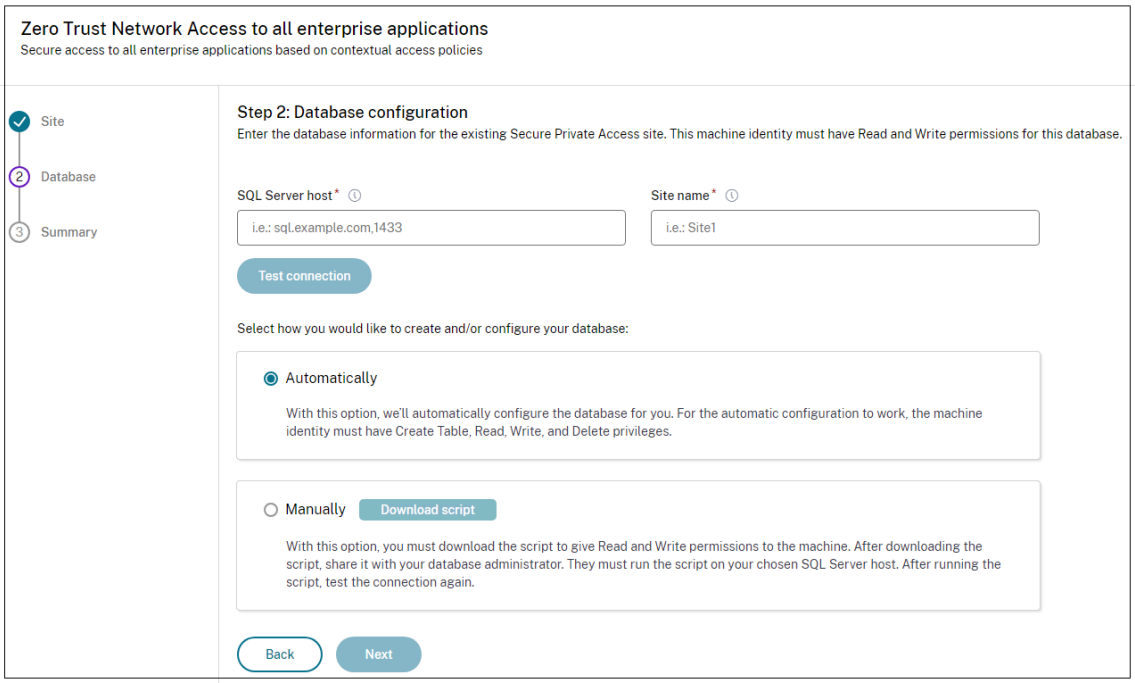
Remarque :

- 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**.



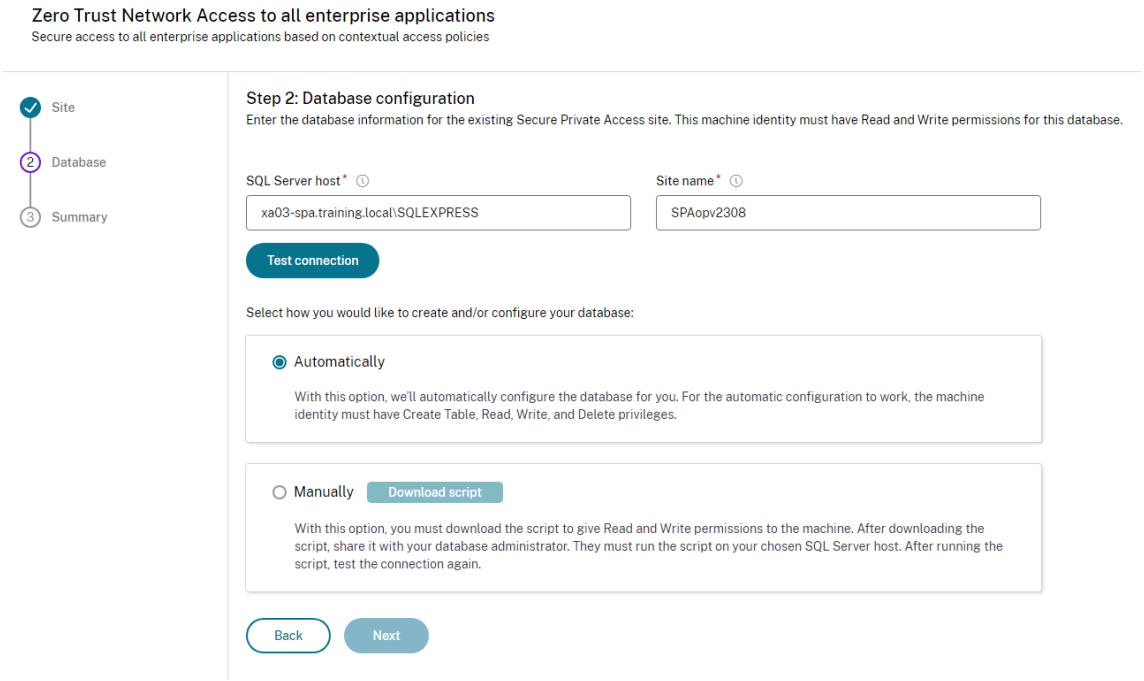
2. Dans **SQL Server Host**, entrez le nom d'hôte du serveur. Assurez-vous qu'une base de données correspondant au nom du site que vous entrez est déjà présente dans le serveur SQL que vous avez sélectionné. Vous pouvez spécifier une adresse de base de données dans l'un des formats suivants :

   - 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 connexion** 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.

Étapes suivantes

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

Composants

August 26, 2024

Voici les principaux composants d'un déploiement local type de Secure Private Access.

- **StoreFront : -** StoreFront authentifie les utilisateurs et gère les magasins de bureaux et d'applications auxquels les utilisateurs accèdent. Il peut héberger votre magasin d'applications d'entreprise qui fournit aux utilisateurs un accès en libre-service aux bureaux et aux applications

que vous mettez à leur disposition. Il assure également le suivi des abonnements aux applications des utilisateurs, des noms de raccourcis et d'autres données. Cela permet de garantir que les utilisateurs ont une expérience cohérente sur plusieurs périphériques. Pour plus de détails sur l'intégration de StoreFront à Secure Private Access, consultez StoreFront.

- **NetScaler Gateway : - NetScaler** Gateway fournit un point d'accès sécurisé unique via le pare-feu de l'entreprise. Pour plus d'informations sur l'intégration de NetScaler Gateway à Secure Private Access, consultez NetScaler Gateway.
- **Director :** Director vous permet de surveiller efficacement les performances et de résoudre les problèmes. Pour intégrer Director à Secure Private Access, vous devez saisir l'adresse IP du nom de domaine complet du serveur Director qui doit être enregistré auprès de Secure Private Access. Pour plus de détails sur l'intégration de Director à Secure Private Access, consultez la section Intégration de Secure Private Access à Director.
- **Serveur de licences :** le serveur de licences collecte et traite les données de licence. Pour plus de détails sur l'intégration du serveur de licences à Secure Private Access, voir Intégration du serveur de licences à Secure Private Access.
- **Web Studio :** Citrix Secure Private Access est intégré à la console Web Studio pour permettre aux utilisateurs d'accéder facilement au service via Web Studio. Pour plus de détails sur l'intégration de Secure Private Access à Web Studio, voir Intégration de Secure Private Access à Web Studio.

> **Remarque :**
>
> Director et License Server sont intégrés à Secure Private Access à partir de la version 2402.

NetScaler Gateway

August 26, 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, 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*`.

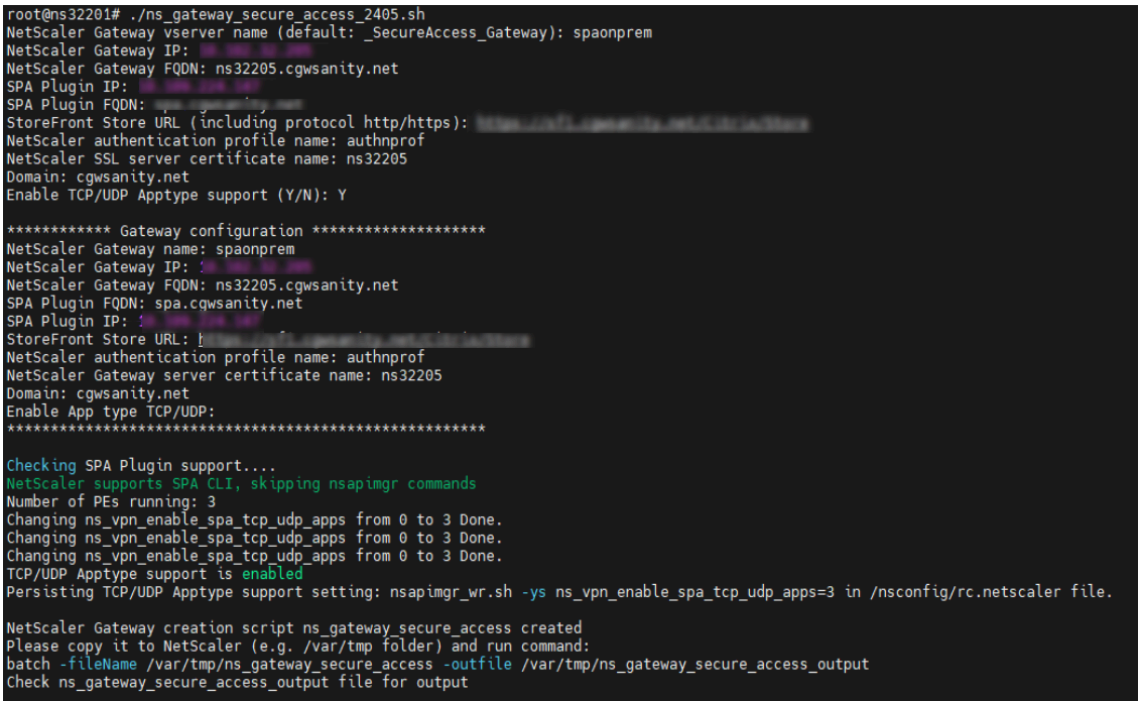
Par exemple, *`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*

> **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.

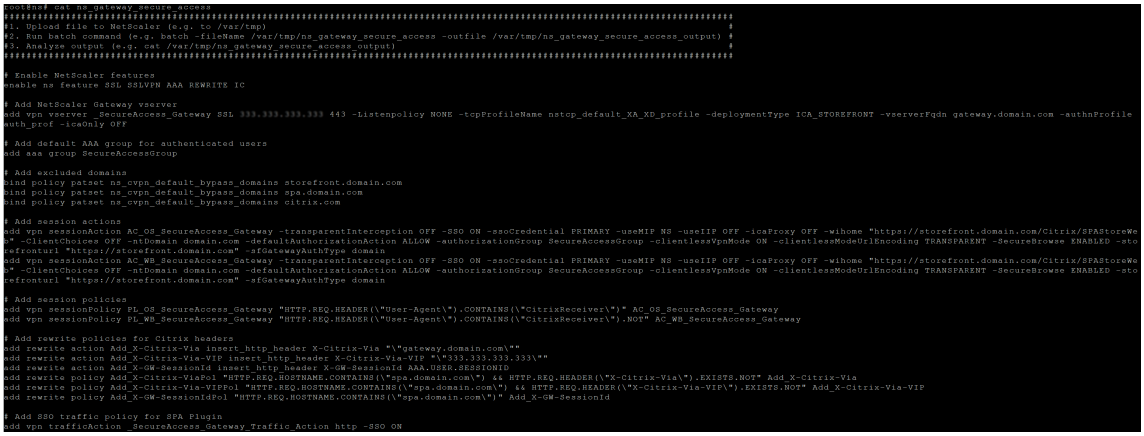


6. Entrez les paramètres requis. Pour la liste des paramètres, consultez la section Prérequis.

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

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

> **Remarque :**
>
> lors de l'exécution du script, la compatibilité entre NetScaler et le plug-in Secure Private Access est vérifiée. Si NetScaler prend en charge le plug-in Secure Private Access, le script active les fonctionnalités NetScaler pour prendre en charge les balises smartaccess, l'envoi d' améliorations et la redirection vers la nouvelle page de refus lorsque l'accès à la ressource est restreint. Pour plus de détails sur les balises intelligentes, consultez la section Prise en charge des balises d'accès intelligentes.
>
> Les fonctionnalités du plug-in Secure Private Access conservées dans le fichier /nsconfig/rc.netscaler permettent de les garder activées après le redémarrage de NetScaler.



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.

Ajouter un serveur virtuel :

- tcpProfileName : nstcp_default_XA_XD_profile
- deploymentType : ICA_STOREFRONT (disponible uniquement avec la commande`add vpn vserver`)
- icaOnly : OFF

Mettre à jour un serveur virtuel :

- tcpProfileName : nstcp_default_XA_XD_profile
- icaOnly : OFF

Exemples :

Pour ajouter un serveur virtuel :

```
add vpn vserver _SecureAccess_Gateway SSL 999.999.999.999 443 -
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"` - remplacez par l'URL réelle du magasin. Le chemin d'accès au magasin `/Citrix/MyStoreWeb` est facultatif.
- `ClientChoices`: OFF
- `ntDomain`: mydomain.com - utilisé pour l'authentification unique (facultatif)
- `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
  ```

- Activez la redirection vers la page « Accès restreint » si l'accès est refusé.

  ```
  nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny
  ```


- Utilisez la page « Accès restreint » hébergée sur CDN.

  ```
  nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
  ```

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

Conserver les paramètres du plug-in Secure Private Access sur NetScaler

Pour conserver les paramètres du plug-in Secure Private Access sur NetScaler, procédez comme suit :

1. Créez ou mettez à jour le fichier /nsconfig/rc.netscaler.
2. Ajoutez les commandes suivantes au fichier.

   ```
   nsapimgr -ys call=ns_vpn_enable_spa_onprem
   nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
   nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny

   nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. Enregistrez le fichier.

Les paramètres du plug-in Secure Private Access sont automatiquement appliqués au redémarrage de NetScaler.

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

August 26, 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.

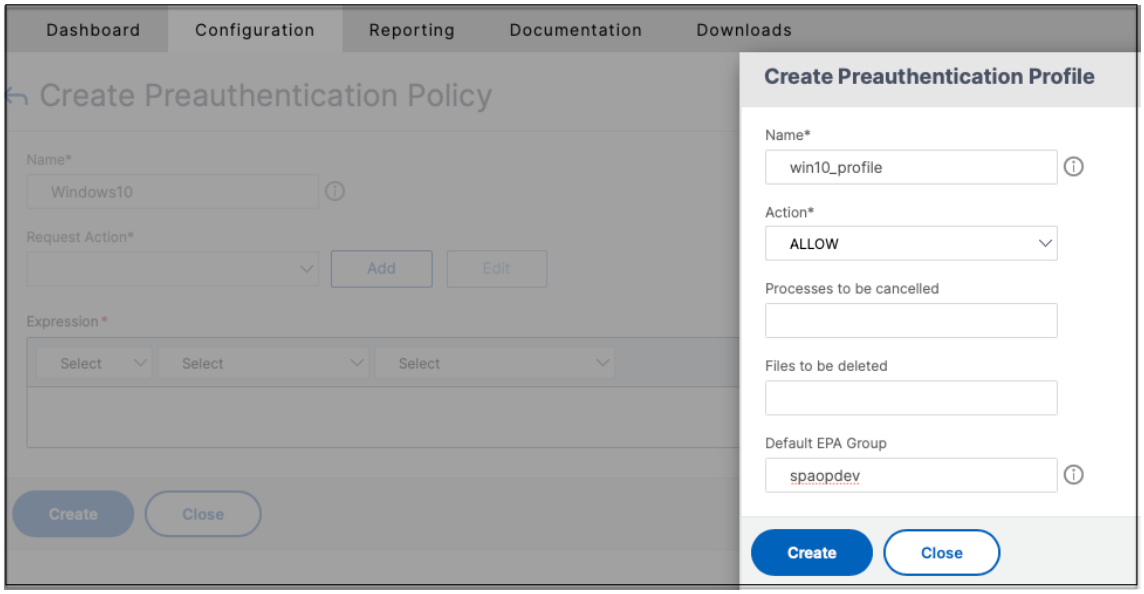
Configurer des balises personnalisées à l'aide de l'interface graphique

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

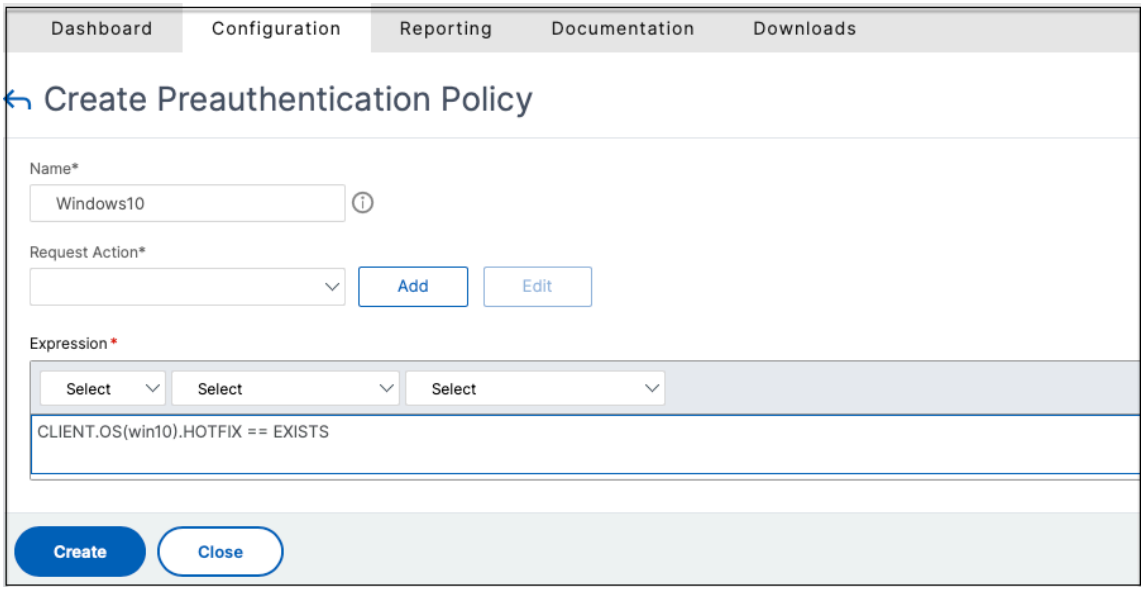
1. Configurer une stratégie de pré-authentification de passerelle classique
2. Liez la stratégie de préauthentification classique au serveur virtuel de passerelle

Configurer une stratégie de pré-authentification de passerelle classique

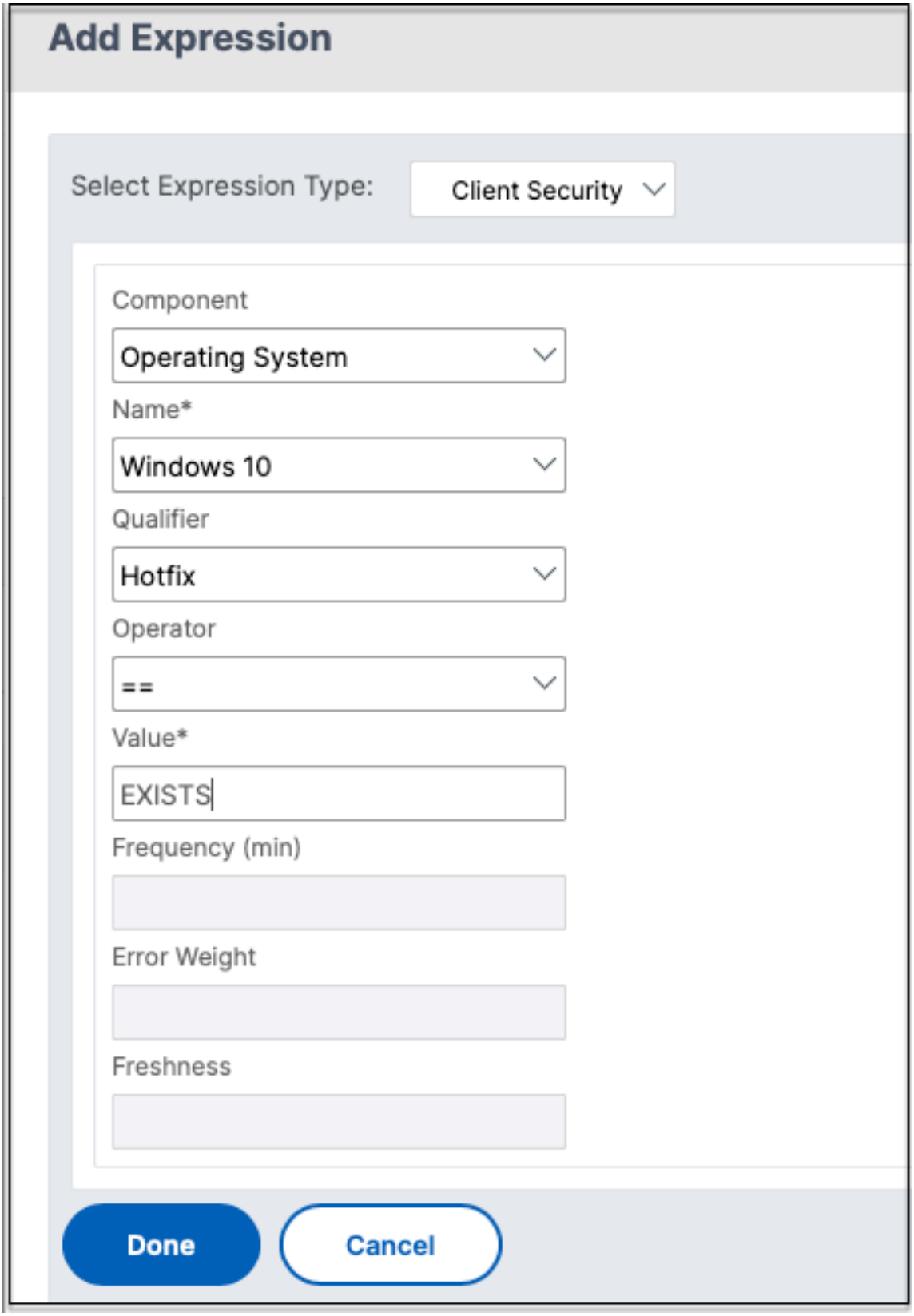
1. Accédez à **NetScaler Gateway > Stratégies > Préauthentification** , puis cliquez sur **Ajouter**.
2. Sélectionnez une stratégie existante ou ajoutez-y un nom. Ce nom de stratégie est utilisé comme valeur de balise personnalisée.
3. Dans **Demander une action** , cliquez sur **Ajouter** pour créer 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.



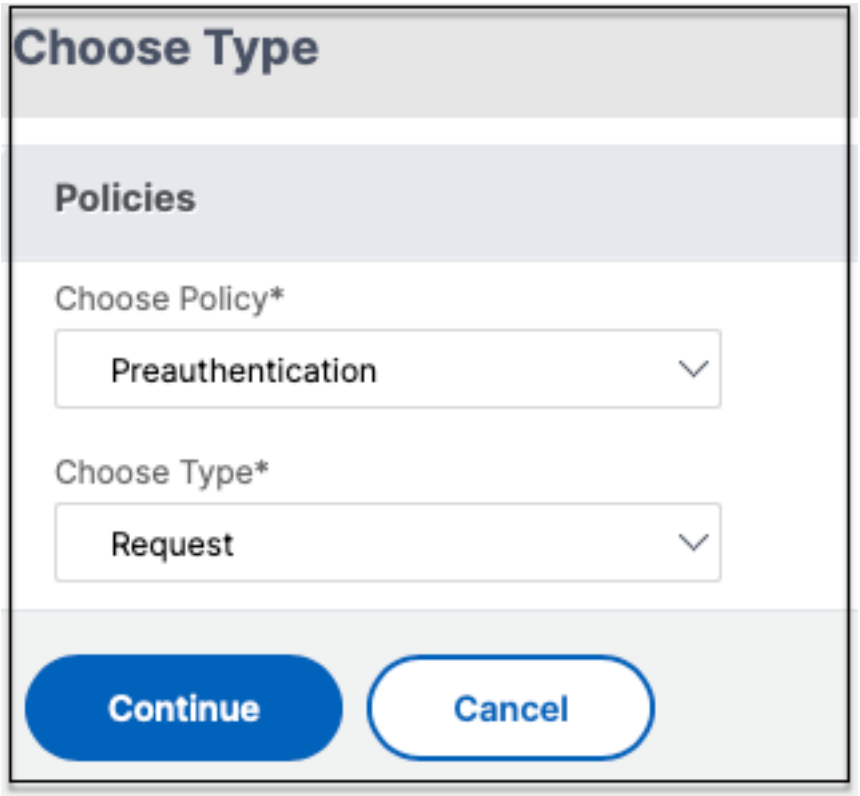
La figure suivante montre un exemple d'expression conçu pour vérifier le système d'exploitation Windows 10.



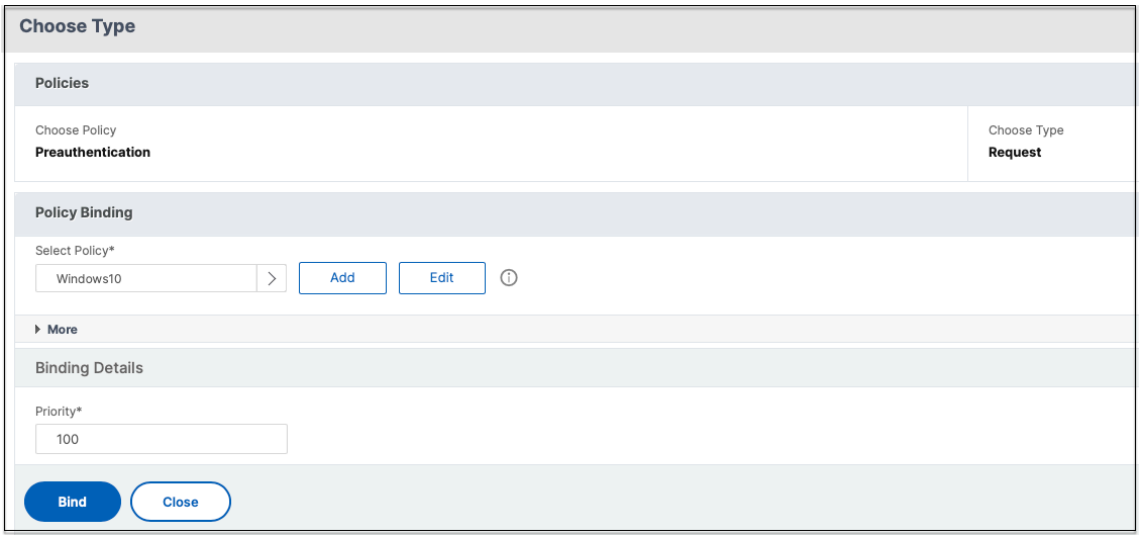
6. Cliquez sur **Créer**.

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.

StoreFront

August 26, 2024

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 stratégie 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**).

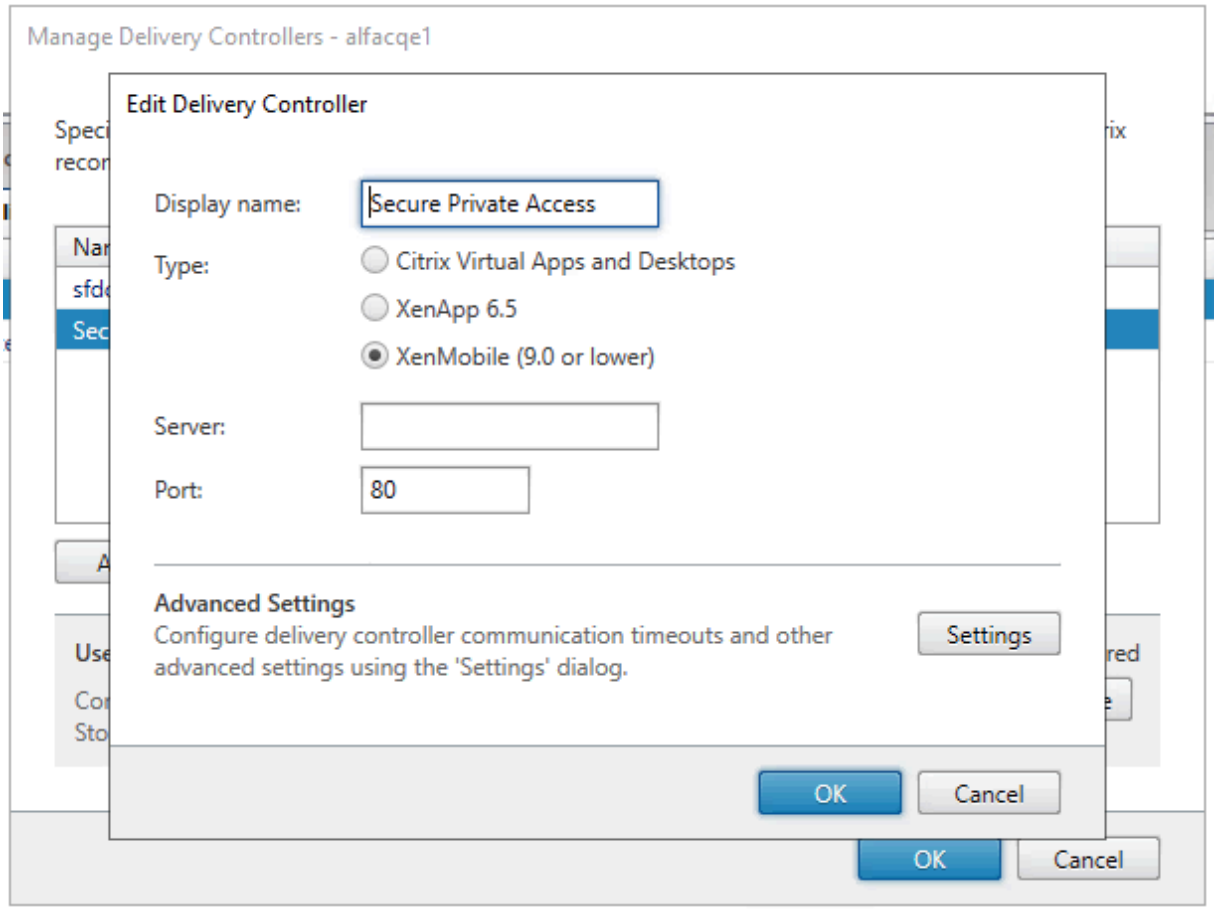
> **Important :**
>
> - Il est recommandé d'utiliser le script StoreFront téléchargé depuis l'interface d'administration de Secure Private Access pour configurer StoreFront pour Secure Private Access uniquement. Ne configurez pas Secure Private Access depuis l'interface d'administration de Store-

> 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.

Director

August 26, 2024

L'intégration de Director à Secure Private Access permet de surveiller efficacement les performances et de résoudre les problèmes. Pour intégrer Director à Secure Private Access, vous devez saisir l'adresse IP du nom de domaine complet du serveur Director qui doit être enregistré auprès de Secure Private Access. Pour plus de détails, voir Intégrer des serveurs.

L'enregistrement de Director auprès de Secure Private Access est une configuration obligatoire de Secure Private Access pour les utilisateurs de la version 2402 locale. Si Director n'est pas configuré,

vous devez installer la dernière version de Director, LTSR 2402 ou une version ultérieure. Si Director est déjà configuré, vous devez le mettre à niveau avec la dernière version, LTSR 2402 ou une version ultérieure. La configuration de Secure Private Access ne peut pas être terminée sans l'enregistrement de Director. La validation échoue également dans les cas suivants.

- Director n'est pas enregistré auprès de Secure Private Access.
- L'adresse IP du service Director ou le nom de domaine complet que vous avez saisi n'existe pas.

Pour plus d'informations sur l'enregistrement de Director auprès de Secure Private Access, voir Intégrer les serveurs StoreFront et NetScaler Gateway et Gérer les paramètres après l'installation.

> **Remarque :**
>
> - L'enregistrement ou la connexion à Director ne prennent pas en charge l'authentification Windows intégrée (IWA). Si l'administrateur s'est connecté à la console Secure Private Access à l'aide d'IWA, il est invité à saisir les informations d'identification pour l'enregistrement de Director.
> - Si l'administrateur a effectué une connexion manuelle à la console Secure Private Access, ces informations sont utilisées pour s'authentifier auprès du serveur Director. Si cela échoue, l'administrateur est invité à saisir les informations d'identification.
> - Si l'administrateur doit ajouter un autre serveur Director une fois la configuration terminée, enregistrez le nouveau serveur Director depuis la page **Gérer les paramètres**. Lors de la mise à jour des informations du serveur Director après la configuration, les administrateurs doivent saisir les informations d'identification pour effectuer les modifications. L'authentification unique n'est pas prise en charge pour modifier l'URL du serveur Director IPv6, SSLv3.

Configurer Director avec Secure Private Access à l'aide de l'outil de configuration Director

La configuration de Director avec Secure Private Access à l'aide de l'outil de configuration est une étape obligatoire pour terminer l'intégration. Pour plus de détails, consultez la section Intégration de Secure Private Access à Director.

Afficher les sessions utilisateur de Secure Private Access dans Director

Vous pouvez consulter les sessions utilisateur Secure Private Access dans Director. Pour plus de détails, voir Afficher les sessions Secure Private Access par utilisateur.

Serveur de licences

August 26, 2024

Un serveur de licences pour le plug-in Secure Private Access est un composant obligatoire pour collecter et traiter les données de licence. Un serveur de licences peut être enregistré auprès de Secure Private Access lors de la configuration initiale, mais il peut également être configuré ou mis à jour une fois la configuration terminée. Pour plus d'informations sur l'enregistrement d'un serveur de licences avec Secure Private Access, consultez Intégrer les serveurs StoreFront et NetScaler Gateway et Gérer les paramètres après l'installation.

Vous devez spécifier l'URL du serveur de licences pour connecter Secure Private Access au serveur de licences. Le plug-in Secure Private Access s'enregistre automatiquement sur le serveur de licences.

> **Remarque :**
>
> - Vous devez installer au moins une licence de broker Citrix Virtual Apps and Desktops sur le serveur de licences pour enregistrer le plug-in Secure Private Access sur le serveur de licences.
> - Le serveur de licences pour le plug-in Secure Private Access est pris en charge à partir de la version 11.17.2 build 45000 et des versions ultérieures. Si vous possédez déjà un serveur de licences, vous devez le mettre à niveau avec la version 11.17.2 build 45000 ou ultérieure.

Pour plus d'informations sur le serveur de licences, consultez la section Serveur de licences.

Studio Web

August 26, 2024

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

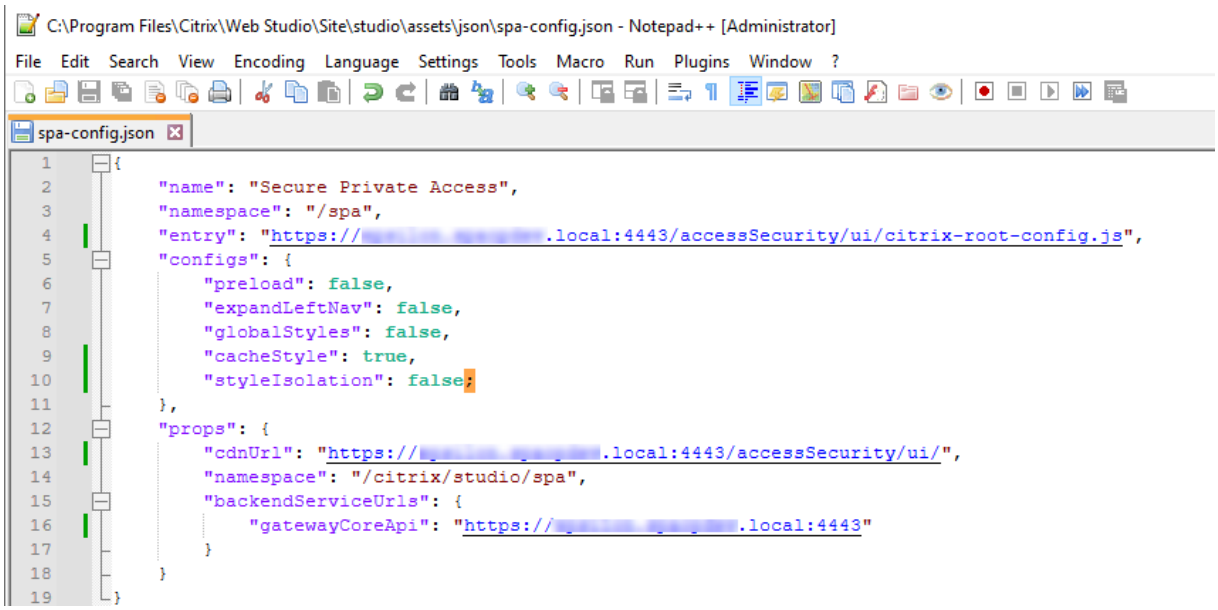
Vous devez installer Web Studio version 2308 ou ultérieure.

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

1. Installez Citrix Web Studio à l'aide du programme d'installation de 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 terminée, accédez au dossier C:\Program Files \ Citrix \ Web Studio \ Site \ studio \ 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.
3. Dans le menu de navigation de gauche, cliquez sur **Secure Private Access** pour accéder à la console d'administration Secure Private Access depuis Web Studio.

Configurer les applications

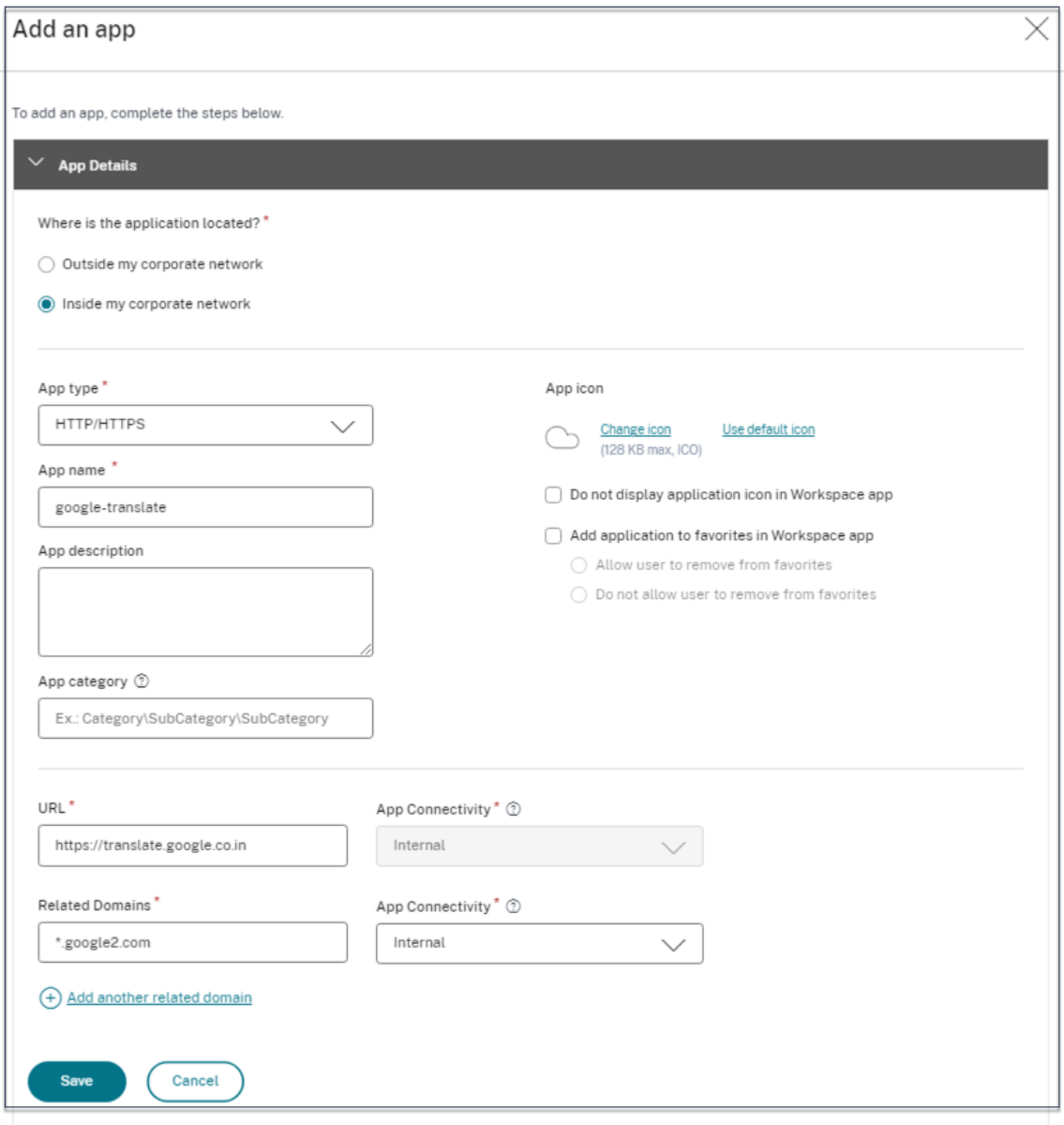
August 26, 2024

Après avoir configuré Secure Private Access, vous pouvez configurer les applications et les stratégies d'accès depuis la console d'administration.

1. Dans la console d'administration, cliquez sur **Applications**.
2. Cliquez sur **Ajouter une application**.
3. 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.

4. 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 utilisateur de Citrix Workspace. Vous pouvez ajouter une nouvelle catégorie pour chaque ap-

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

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.

5. 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.

Étapes suivantes

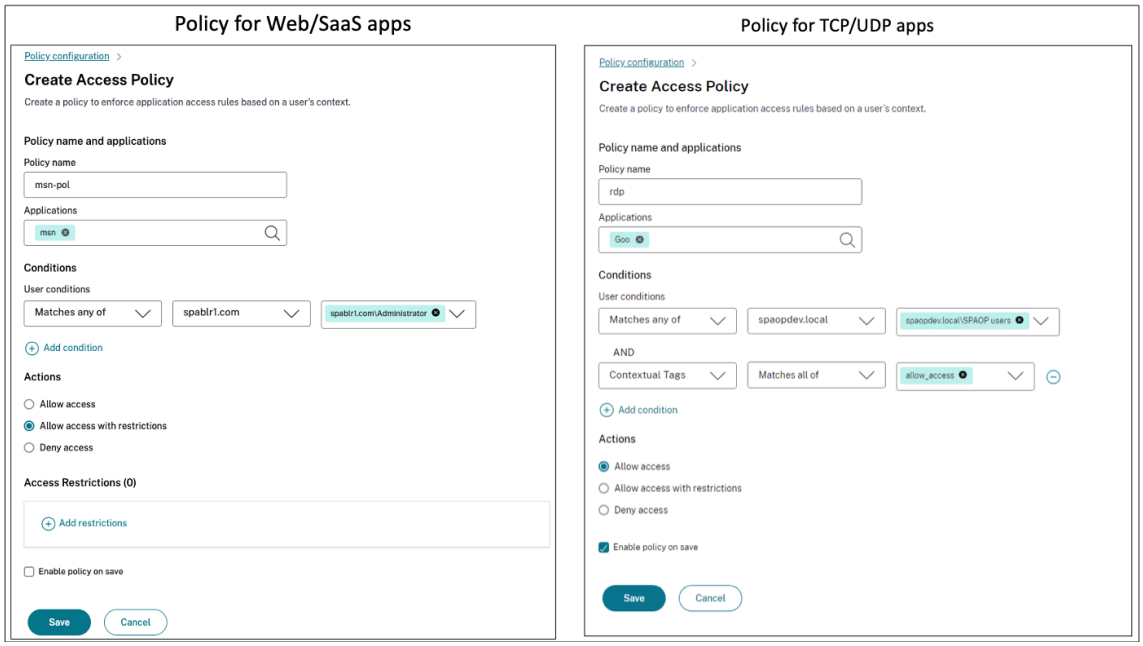
Configuration des stratégies d'accès pour les applications

Configuration des stratégies d'accès pour les applications

August 26, 2024

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. Dans la console d'administration, cliquez sur **Stratégies d'accès**.
2. Cliquez sur **Créer une stratégie**.



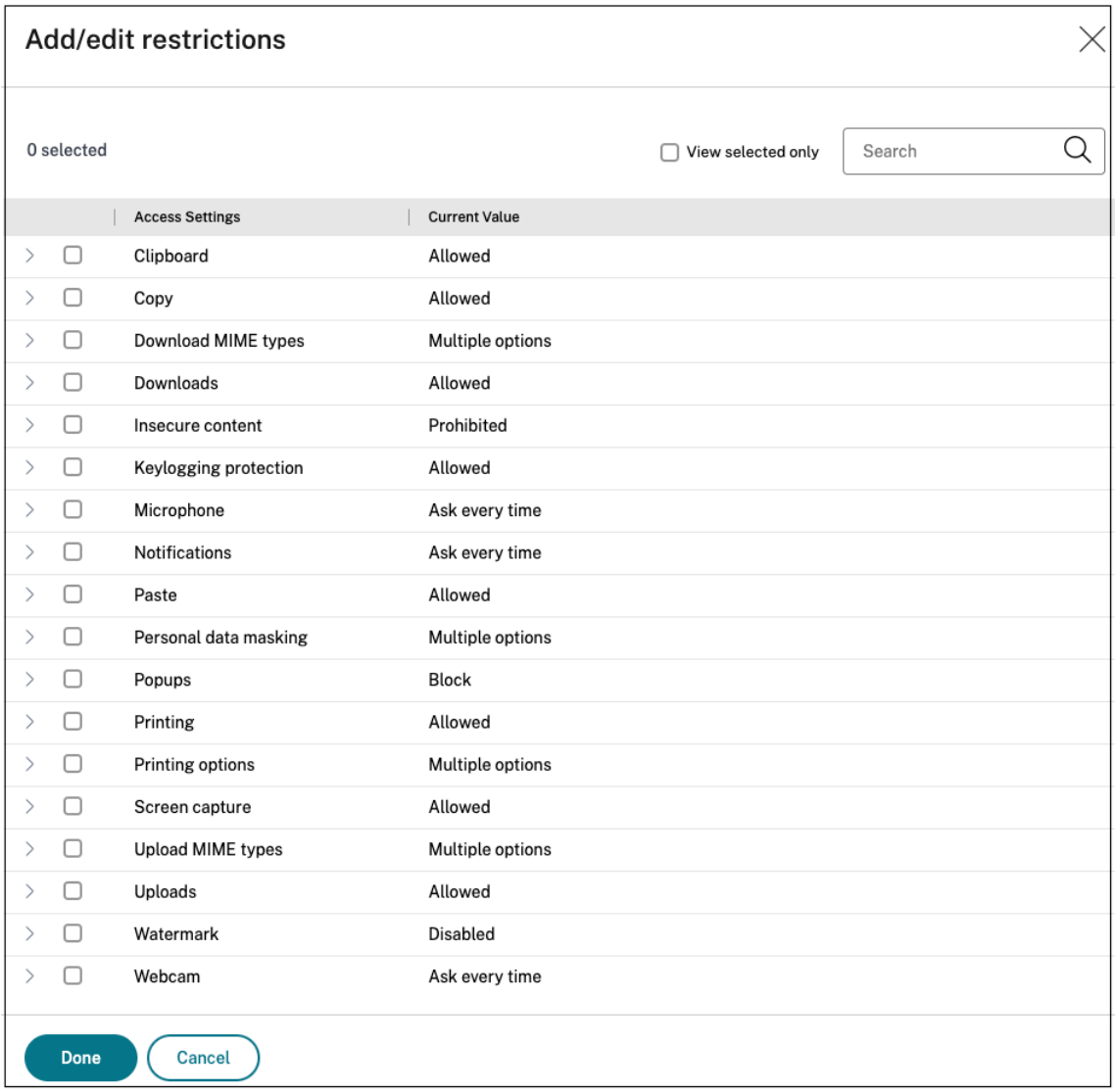
3. Dans **Applications**, sélectionnez les applications pour lesquelles vous souhaitez appliquer les stratégies d'accès.
4. Dans **Utilisateurs/Groupes d'utilisateurs** : sélectionnez les conditions et les utilisateurs ou groupes d'utilisateurs en fonction desquels l'accès à l'application doit être autorisé 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.

5. Cliquez sur **Ajouter une condition** pour ajouter une autre condition en fonction des balises contextuelles. Ces balises sont dérivées de NetScaler Gateway.
6. Sélectionnez **Balises conditionnelles**, puis sélectionnez les conditions selon lesquelles l'accès à l'application doit être autorisé ou refusé.
7. 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 de couper/copier/coller entre l'application et le presse-papiers du système.
- **Restreindre l'impression**: désactive la possibilité d'imprimer depuis Citrix Enterprise Browser.
- **Restreindre les téléchargements**: désactive la possibilité pour l'utilisateur de télécharger depuis l'application.
- **Restreindre les chargements**: désactive la possibilité pour l'utilisateur de charger dans l'application.
- **Afficher le filigrane**: affiche un filigrane sur l'écran de l'utilisateur avec le nom d'utilisateur et l'adresse IP de la machine de l'utilisateur.
- **Restreindre l'enregistrement de frappe**: protège contre l'enregistrement de frappe. 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.

8. Dans **Nom de la stratégie**, entrez le nom de la stratégie.
9. 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).

Exemple de validation de configuration

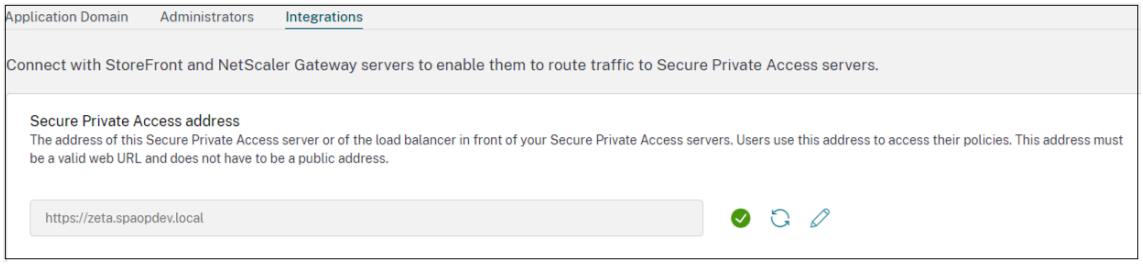
Déployez Secure Private Access en tant que cluster

August 26, 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).

Création de nœuds Secure Private Access

- 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.
- Lors de la configuration du premier nœud dans Secure Private Access, utilisez les noms de l'équilibreur de charge. Pour ajouter les nœuds suivants, spécifiez l'adresse de la base de données dans l'onglet Intégrations et exécutez manuellement le script de la base de données. Pour plus d'informations sur la mise à niveau de la base de données à l'aide de scripts, voir Mettre à niveau la base de données à l'aide de scripts.



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 noms de domaine complets utilisés pour accéder à StoreFront sont inclus dans le champ DNS en tant que nom alternatif du sujet (SAN). Si vous utilisez un équilibreur de charge, incluez à la fois le nom de domaine complet du serveur individuel et le nom de domaine complet de l'équilibreur de charge. Cela s'applique aux certificats SSL. Pour Secure Private Access, la configuration d'un équilibrage de charge est suffisante. Pour plus de détails, consultez la section Équilibrage de charge avec NetScaler.

Avant de configurer Secure Private Access, le magasin StoreFront doit être configuré. Si vous utilisez un équilibreur de charge, configurez l'URL de base avec le nom de l'équilibreur de charge et utilisez le protocole HTTPS pour sécuriser les communications. Pour plus de détails, consultez la section Sécurisation de StoreFront avec HTTPS.

- Il est recommandé d'exécuter les services Secure Private Access 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.
- Le certificat SSL correct est lié au serveur IIS et à NetScaler.
- Des chiffrements sécurisés sont utilisés.
- 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.
- 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" }
 }
```

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

Créer un moniteur pour Secure Private Access

Utilisez la commande CLI suivante pour créer un moniteur pour Secure Private Access.


```
add lb monitor SPAHealth HTTP -respCode 200 -httpRequest "GET /
secureAccess/health"-secure YES
```

Après avoir créé un moniteur, liez le certificat au moniteur.

Pour plus d'informations sur la création de moniteurs à l'aide de l'interface utilisateur de NetScaler, consultez la section Créer des moniteurs.

Désinstallez Secure Private Access

August 26, 2024

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

1. Sélectionnez **Citrix Virtual Apps and Desktops 7 2402 —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
```

Mettre à niveau

August 26, 2024

Vous pouvez mettre à niveau vos déploiements Secure Private Access avec une version plus récente sans avoir à configurer au préalable de nouvelles machines ou de nouveaux sites. Avant de procéder à la mise à niveau, nous vous recommandons de créer des instantanés ou d'enregistrer les configurations. Pour démarrer une mise à niveau, vous exécutez le programme d'installation à partir de la nouvelle version afin de mettre à niveau le plug-in Secure Private Access précédemment installé.

Séquence de mise à niveau

La séquence de mise à niveau est la suivante :

1. Vous pouvez mettre à niveau Secure Private Access via le Delivery Controller ou via la vignette Secure Private Access dédiée dans l'interface utilisateur du programme d'installation en fonction de la manière dont vous avez initialement installé Secure Private Access.
    - Si vous avez installé Secure Private Access via Delivery Controller, vous ne pouvez pas mettre à niveau le composant Secure Private Access seul. Au lieu de cela, vous devez mettre à niveau tous les composants. Pour de plus amples informations, consultez la section Mettre un déploiement à niveau.
    - Si vous avez installé Secure Private Access via la vignette dédiée Secure Private Access, vous pouvez le mettre à niveau indépendamment. Pour plus de détails, voir Mettre à niveau le programme d'installation de Secure Private Access.

    > **Remarque :**
    >
    > nous vous recommandons d'installer Secure Private Access via le Delivery Controller pour les environnements POC. Toutefois, pour les environnements de production, nous vous recommandons d'utiliser le programme d'installation dédié afin de pouvoir adapter les nouvelles fonctionnalités.

2. Exécutez les scripts de base de données. Pour plus de détails, voir Mettre à niveau la base de données à l'aide de scripts.

3. Exécutez à nouveau la configuration de StoreFront. Téléchargez les scripts StoreFront depuis **Paramètres > Configuration**, puis exécutez les scripts sur les machines StoreFront correspondantes. Pour plus de détails, consultez la section Modifier les paramètres d'intégration.

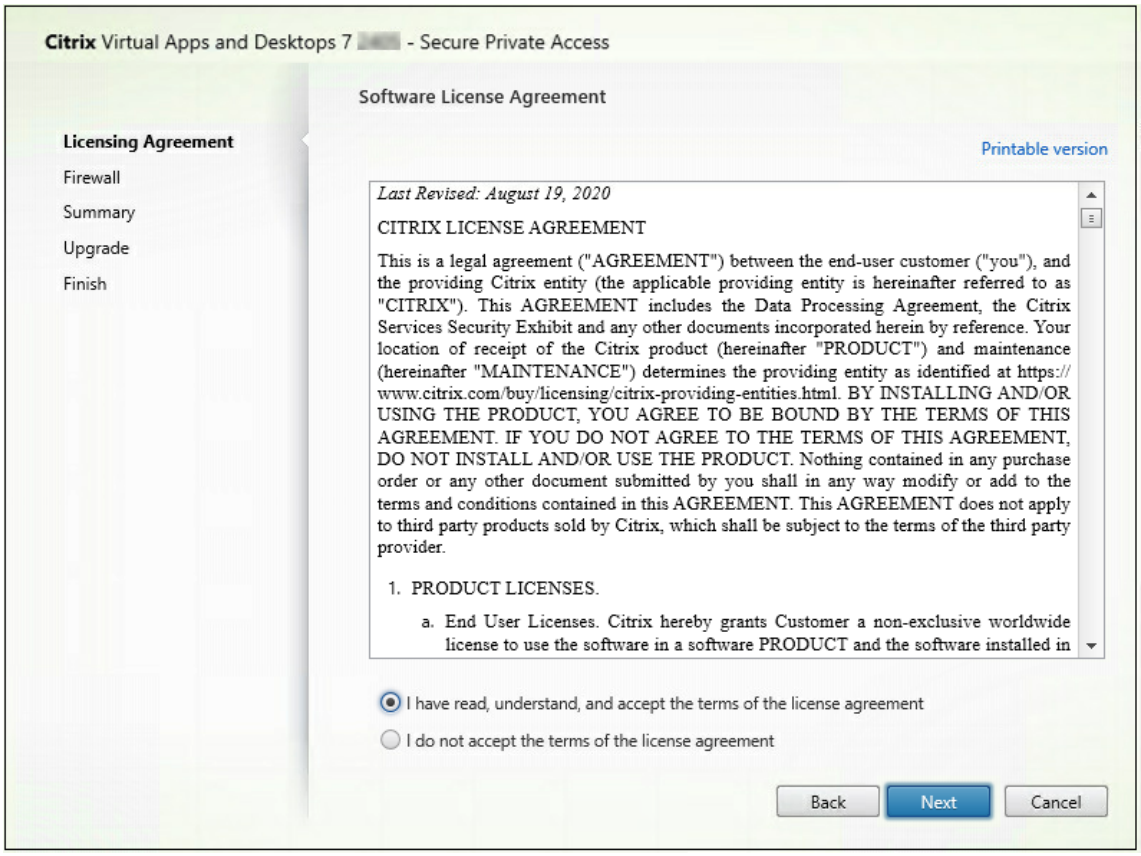
   > **Remarque :**
   >
   > Si vous n'exécutez pas les scripts, les points de terminaison ne sont pas déclenchés.

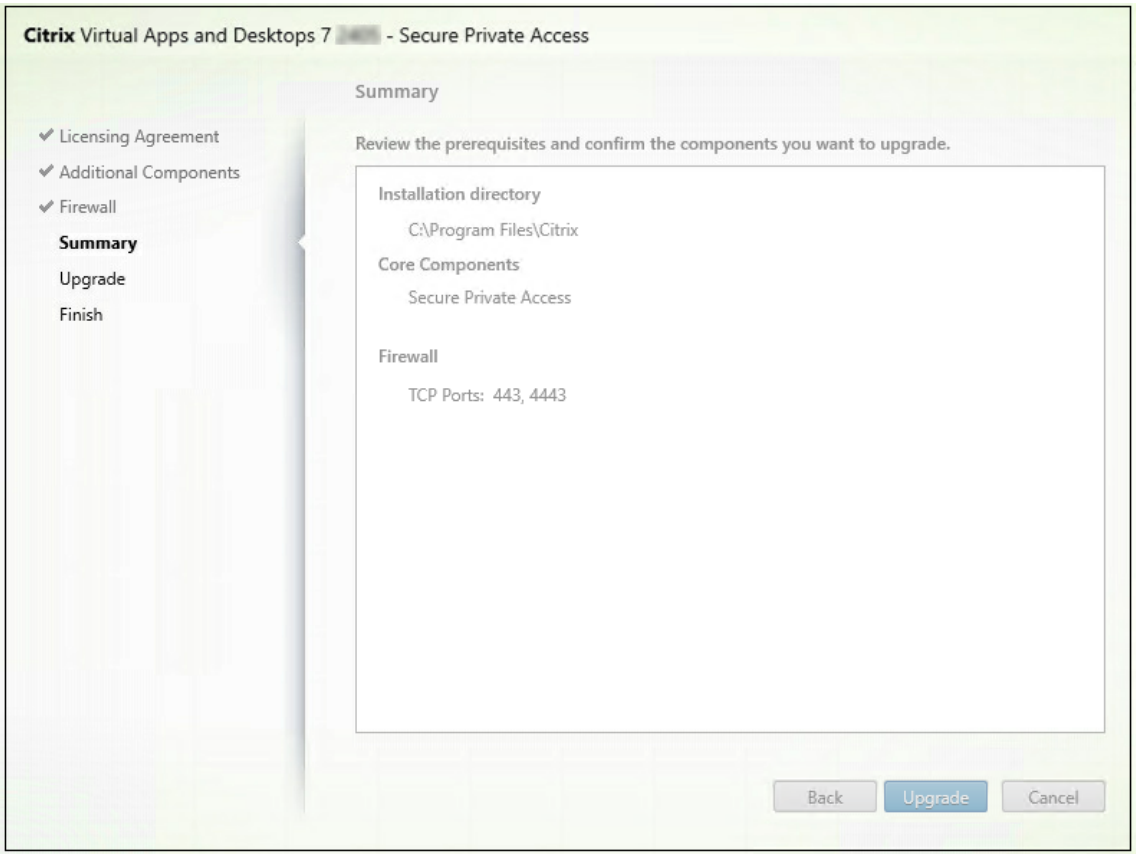
4. (Facultatif) Exécutez le script NetScaler Gateway. Pour plus de détails, consultez NetScaler Gateway.

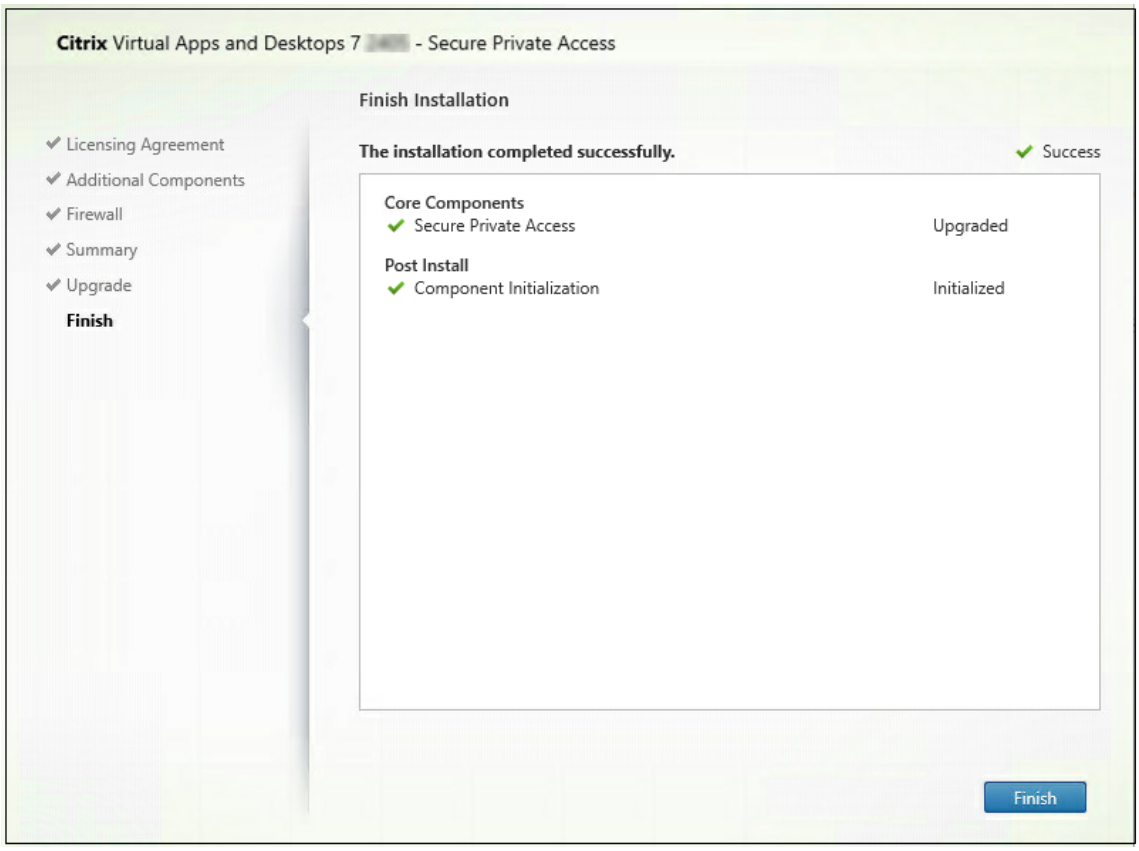
Mettez à niveau le programme d'installation Secure Private Access

August 26, 2024

1. Téléchargez le programme d'installation de Citrix Secure Private Access 2402 à l'adresse 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.
3. Suivez les instructions qui s'affichent à l'écran pour terminer l'installation.







> **Important :**
>
> après avoir mis à niveau le programme d'installation avec la version 2402, vous devez réexécuter le script StoreFront afin que les détails du nouveau point de terminaison soient disponibles.

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

August 26, 2024

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
   >
   ```

Gérer

August 26, 2024

Après avoir installé Secure Private Access, vous pouvez modifier les paramètres depuis la page Paramètres. Vous pouvez gérer le routage des domaines d'application, des administrateurs et modifier les paramètres d'intégration.

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

Pour plus d'informations sur la mise à jour ou la modification des paramètres, consultez les rubriques suivantes :

- Gérer le routage des domaines d'applications
- Gérer les administrateurs
- Modifier les paramètres d'intégration

Gérer les paramètres après l'installation

August 26, 2024

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.

Gérer les administrateurs

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.

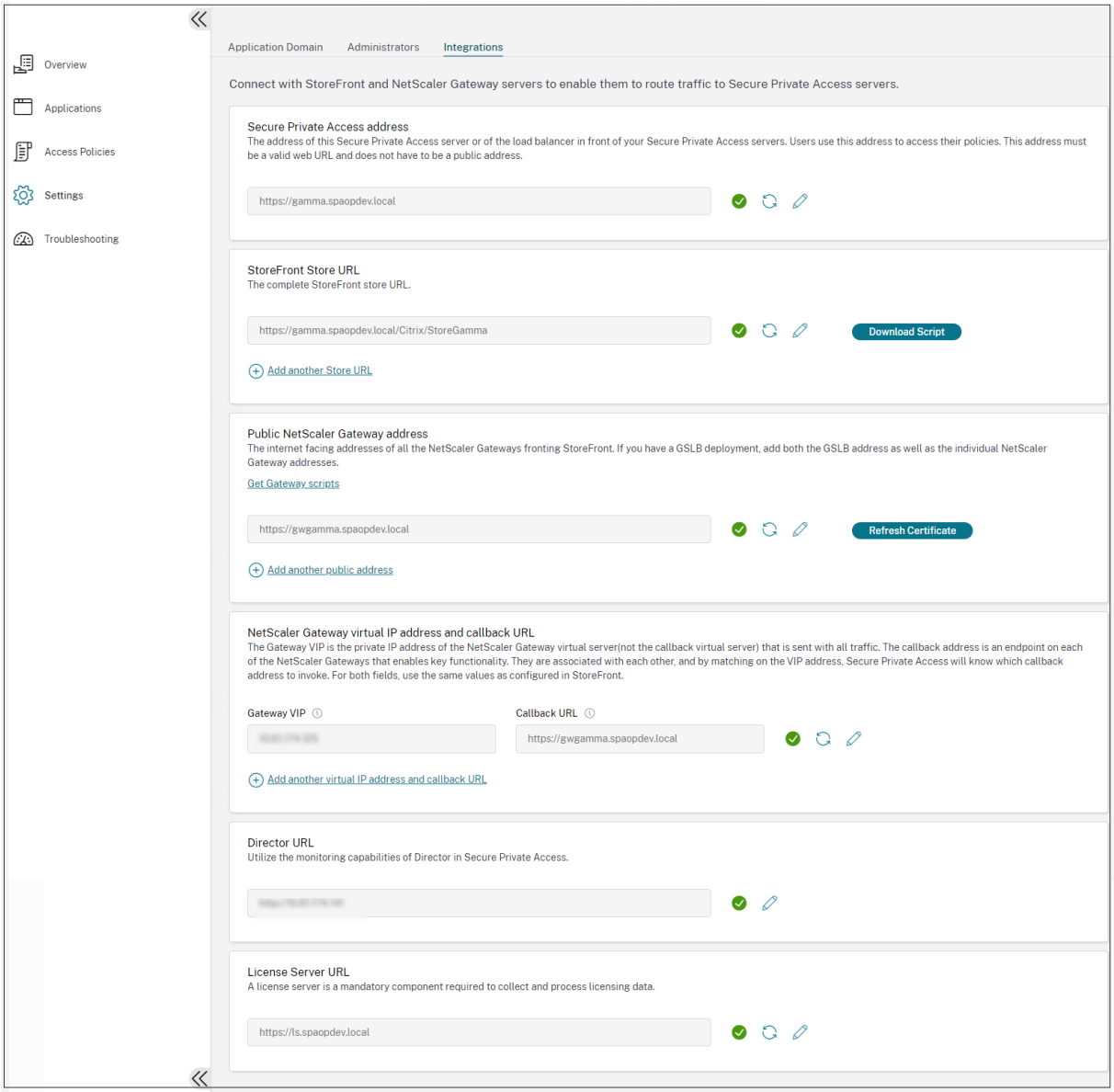
1. Sur la page **Administrateurs** , cliquez sur **Ajouter** .
2. Dans **Domaine**, sélectionnez le domaine auquel cet administrateur doit être ajouté.
3. Dans **Utilisateurs ou groupe** d'utilisateurs , sélectionnez l'utilisateur ou le groupe auquel appartient cet utilisateur.
4. Dans **Type d'administrateur**,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

Modifier les paramètres d'intégration

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.



Gérer les applications et les stratégies

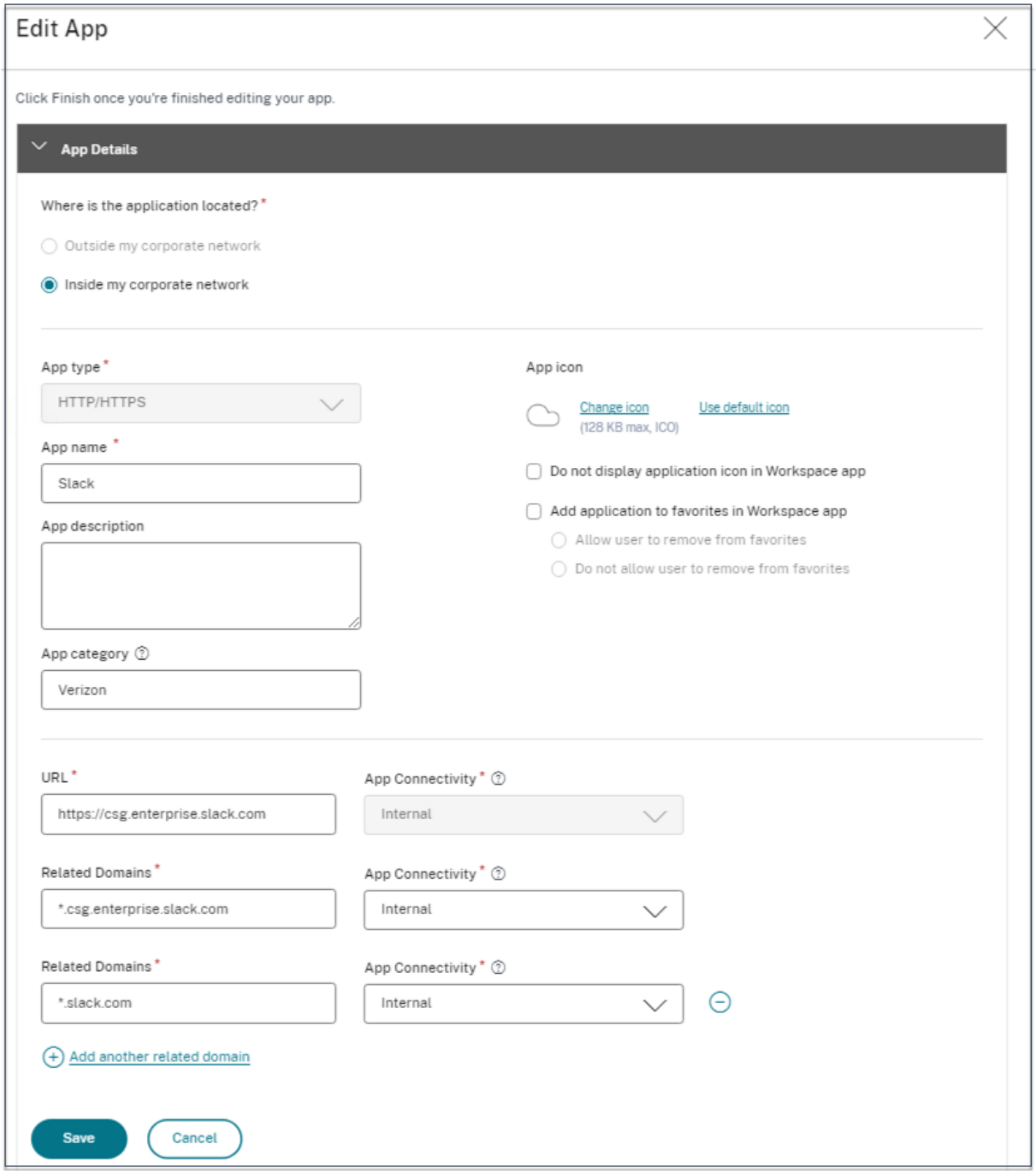
August 26, 2024

Après avoir configuré les applications et les stratégies d'accès, vous pouvez les modifier si nécessaire.

Modifier une application

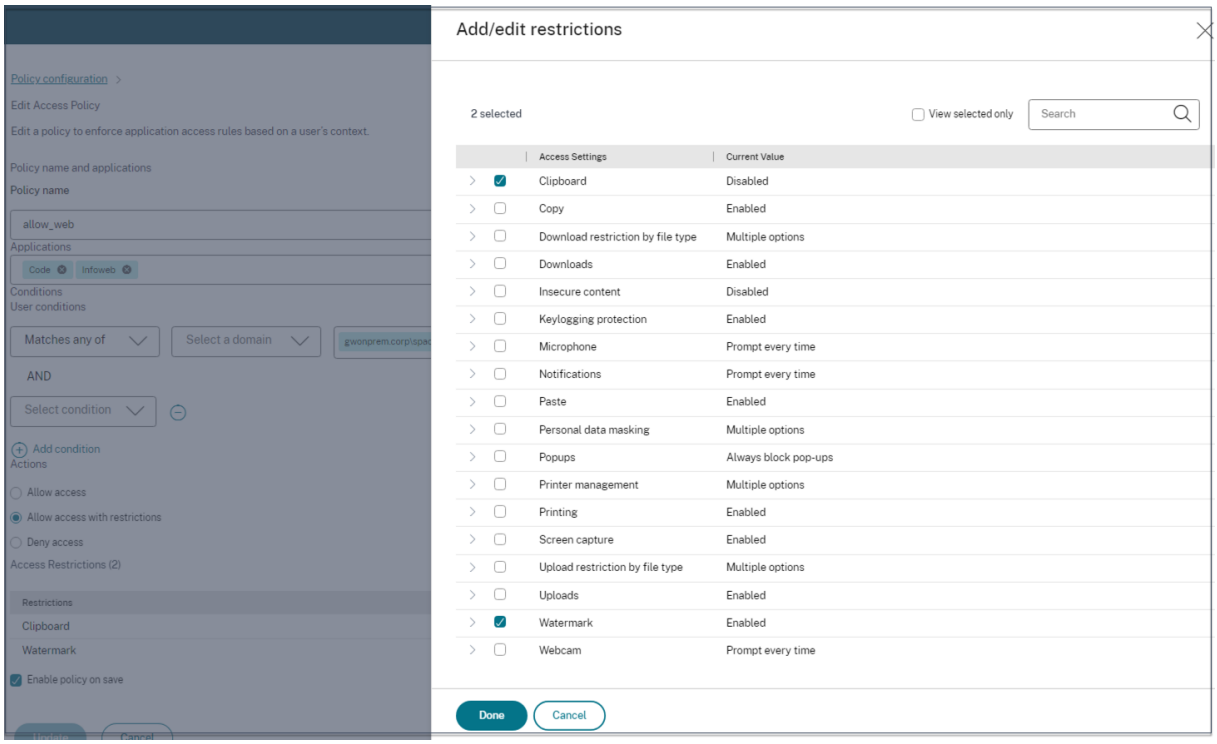
1. Dans la console d'administration Secure Private Access, cliquez sur **Applications**.

2. Cliquez sur le bouton en forme de point de suspension correspondant à l'application que vous souhaitez modifier, puis cliquez sur **Modifier l'application**.
3. Modifiez les détails de l'application.
4. Cliquez sur **Enregistrer**.



Modifier une stratégie d'accès

1. Dans la console d'administration Secure Private Access, cliquez sur **Stratégies d'accès**.
2. Cliquez sur le bouton représentant des points de suspension correspondant à la stratégie que vous souhaitez modifier, puis cliquez sur **Modifier la stratégie d'accès**.
3. Modifiez les détails de la stratégie.
4. Cliquez sur **Update**.



Flux d'utilisateurs finaux

August 26, 2024

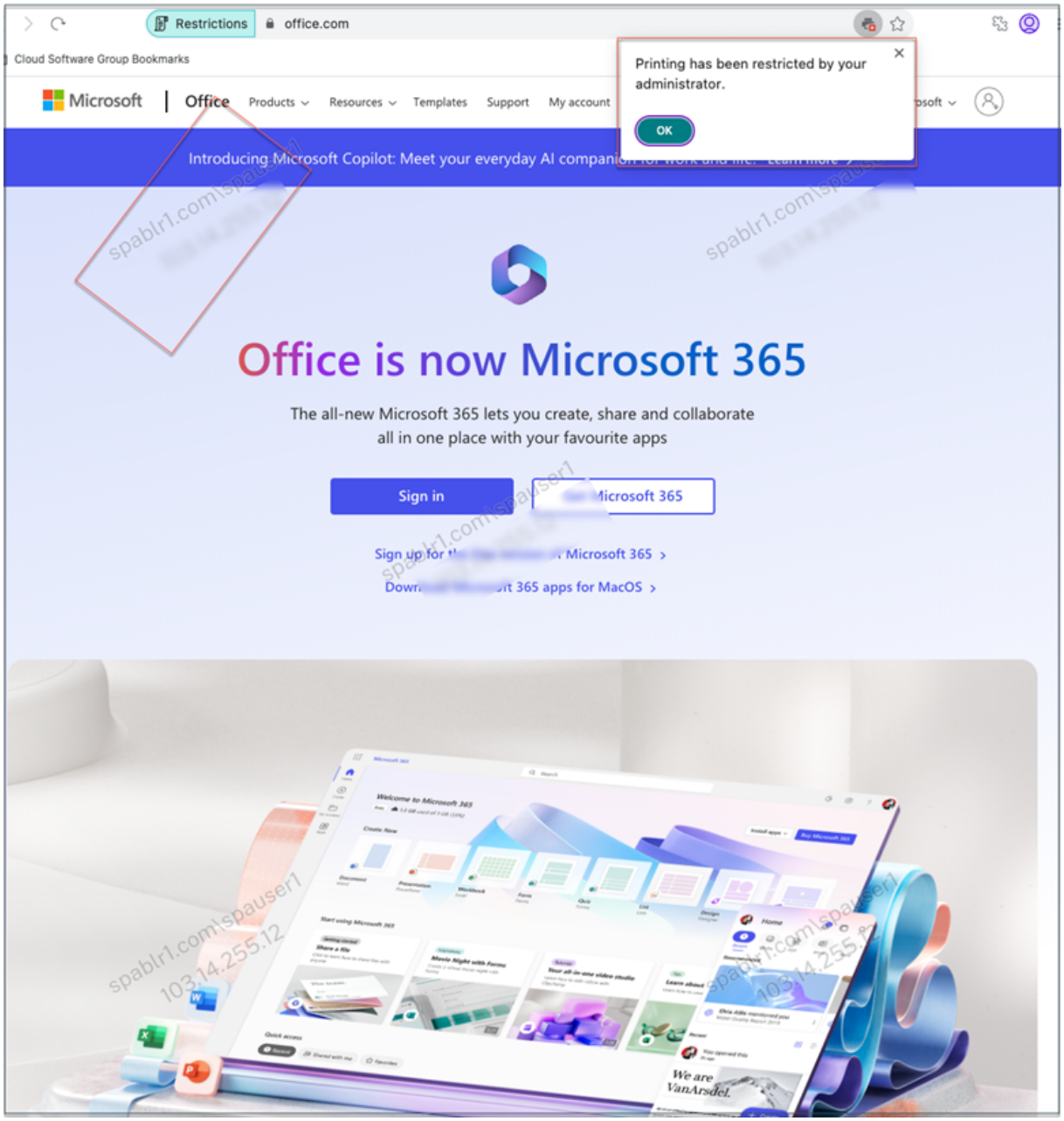
Supposons qu'un administrateur ait configuré l'application Office365 avec le filigrane et la restriction d'impression pour l'utilisateur final. Désormais, lorsque l'utilisateur final accède à l'application Office365, les restrictions relatives au filigrane et à l'impression doivent être appliquées à l'application.

L'utilisateur final doit suivre les étapes suivantes pour accéder à l'application Office365 :

1. Accédez au magasin StoreFront depuis l'application Citrix Workspace.
2. Connectez-vous au magasin.

3. Cliquez sur l'onglet **Applications**, puis sur l'application **Office365**.

   L'utilisateur final doit maintenant remarquer que l'application Office365 est lancée et contient le filigrane. En outre, si l'utilisateur final essaie d'imprimer certaines données depuis l'application Office365, le message de restriction d'impression doit lui être affiché.



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.

Surveiller et résoudre les problèmes

August 26, 2024

Le tableau de bord **Dépannage** de Secure Private Access affiche les journaux relatifs au lancement d'application, à l'énumération d'applications et à leur statut. Pour plus de détails, consultez la section Présentation du tableau de bord.

Dépannage

Vous pouvez rencontrer des problèmes liés aux éléments suivants pendant ou après 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

Pour plus d'informations sur la résolution de ces problèmes, consultez la section Dépannage de base.

Codes relatifs aux sessions dans Director

L'intégration de Director à Secure Private Access permet de surveiller les performances et de résoudre efficacement les problèmes liés à tous les composants d'une configuration Secure Private Access, car ils sont capturés dans Director. Il est recommandé de résoudre les problèmes d'échec ou d'exception en examinant les journaux. Si cela ne permet pas de résoudre le problème, contactez le support.

Références

- Configurer Director avec Secure Private Access
- Afficher une session Secure Private Access dans Director
- Liste des codes de session Secure Private Access dans Director.
- Director.

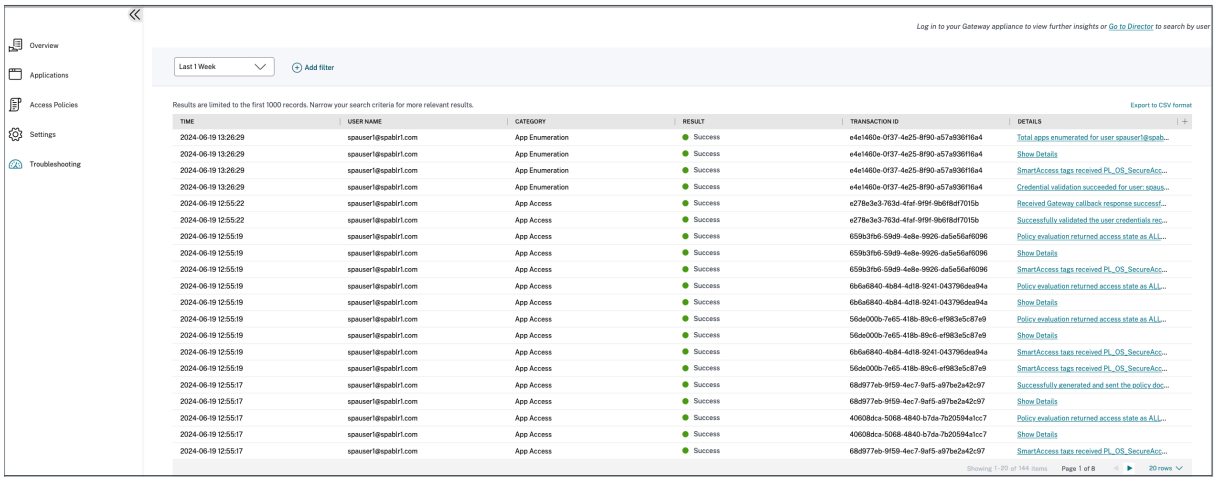
Aperçu du tableau de bord

August 26, 2024

Le tableau de bord Dépannage de Secure Private Access affiche les journaux relatifs au lancement d'application, à l'énumération d'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
- Résultats
- 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 stratégies d'accès les plus populaires par tableaux d'application .

- = : 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 journaux/stratégies qui ne contiennent pas certains des critères spécifiés.

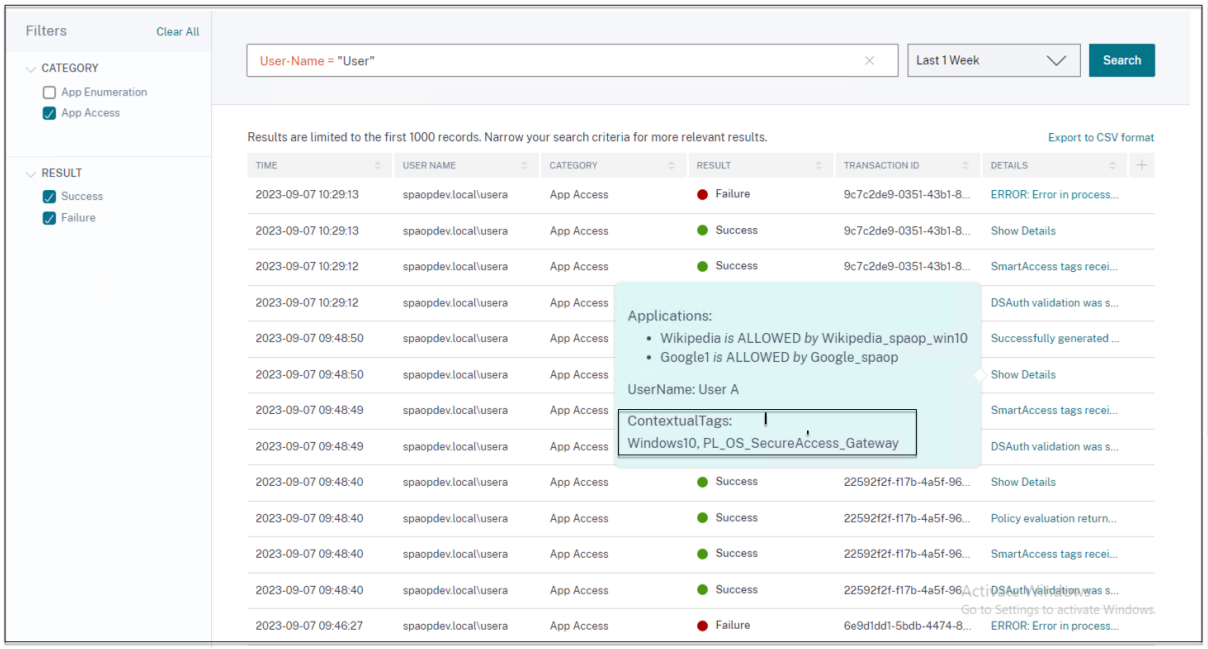
Par exemple, vous pouvez rechercher un type d'événement « DSAuth » en utilisant la chaîne **Event-Type = DSAuth** dans le champ de recherche.

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.



Dépannage de base

August 26, 2024

Cette rubrique répertorie certaines des erreurs que vous pourriez rencontrer pendant ou après la configuration de Secure Private Access.

Erreurs de certificat

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

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'instal-

lation 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

La première configuration ne peut pas être terminée

Il est possible que vous ne puissiez pas reconfigurer le serveur de licences si la configuration de Director échouait lors de la première installation.

Résolution :

Nettoyez manuellement la table license_server.

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.

Modifier le niveau de journalisation pour les journaux de dépannage

Les journaux de dépannage constituent le niveau de journal des erreurs par défaut.

Pour modifier le niveau de journalisation des journaux de dépannage, dans le service d'exécution appsettings.json (C:\Program Files \ Citrix \ Citrix Access Security \ Runtime \ RuntimeService), mettez à jour `restrictedToMinimumLevel` pour `TroubleshootingSql` avec l'une des valeurs suivantes :

```
- Information
- Debug
- Warning
- Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

Résolution des problèmes à l'aide de Director

August 26, 2024

L'intégration de Director à Secure Private Access permet de surveiller les performances et de résoudre efficacement les problèmes, liés à tous les composants d'une configuration Secure Private Access, car ils sont capturés dans Director. Les tableaux suivants répertorient les différents codes d'erreur et les conditions associées qui sont affichés dans Director.

Pour plus d'informations, consultez les rubriques suivantes.

- Configurer Director avec Secure Private Access
- Afficher une session Secure Private Access dans Director

> **Remarque :**
>
> - Les codes dont le deuxième chiffre contient « 0 » représentent un flux d'exécution normal. Par exemple, 1000 représente une énumération d'applications réussie.
> - Les codes dont le deuxième chiffre contient « 1 » représentent un échec ou une exception. Par exemple, 2101 représente un échec de session. En cas d'échec ou d'exception, il est recommandé de résoudre ces problèmes en examinant les journaux. Si cela ne permet pas de résoudre le problème, contactez le support.

Codes relatifs à l'énumération

Code	État	Description
1101	échec	Une erreur interne s'est produite lors de l'énumération.
1102	échec	Certaines applications ont été énumérées, mais l'évaluation d'au moins une application a échoué.
1103	échec	Aucune application n'a été énumérée et l'évaluation d'au moins une application a échoué.
1000	Réussite	L'énumération a été effectuée avec succès. Au moins une application a été énumérée.
1001	Réussite	Aucune application n'a été énumérée, car elles ont toutes été refusées par les stratégies.
1002	Réussite	Aucune application n'a été énumérée, car aucune stratégie ne correspondait.
1003	Réussite	Aucune application n'a été énumérée, car certaines ont été refusées et pour d'autres, aucune stratégie ne correspondait.
1004	Réussite	Aucune application n'a été énumérée, car il n'y avait aucune stratégie à évaluer.

Codes relatifs à la session

Code	État	Description
2101	Échec	Échec de session.

Code	État	Description
2102	active/inactive/en échec	La session est active ou arrêtée, ou au moins un lancement d'application au cours de la session a échoué.
2000	Active	La session est active.
2001	Inactif	La session est arrêtée/inactive.

Codes des messages d'énumération des applications

Code	État	Description
3101	Échec	Énumération des applications : une erreur interne s'est produite (actuellement inutilisée).
3102	Échec	L'application n'a pas été énumérée, car une exception s'est produite lors de l'évaluation de la stratégie.
3103	Échec	L'état de l'énumération des applications est nul : une erreur interne s'est produite lors de l'évaluation de la stratégie.
3104	Autoriser/refuser/échec	Erreur lors de la récupération des informations relatives à la stratégie de l'application.
3000	Autoriser	L'énumération des applications est autorisée.
3001	Refuser	L'énumération des applications est refusée par la stratégie.
3002	Refuser	Les applications n'ont pas été énumérées, car aucune stratégie ne correspondait.
3003	Inconnu	L'état de l'énumération d'applications est inconnu.

Code	État	Description
3004	Lancement d'application depuis CEB	Tentative de lancement d'application depuis Citrix Enterprise Browser.

Codes de message de lancement d'application

Code	État	Description
4101	Échec	Erreur de lancement d'application : une erreur interne s'est produite lors du lancement d'application
4102	Échec	Erreur de lancement d'application (interne)
4103	Autoriser/refuser/échec	Erreur lors de la récupération des informations relatives à la stratégie d'application
4000	Autoriser	Le lancement d'application est autorisé.
4001	Refuser	Le lancement d'application a été refusé en raison d'une stratégie.
4002	Refuser	Le lancement d'application a été refusé, car aucune stratégie ne correspondait.

Paramètres de rétention des journaux

August 26, 2024

Les journaux sont stockés dans la base de données Secure Private Access pendant sept 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
3     "CleanupPeriodInHours": 12,
4     "CleanupDataOlderThanDays": 7,
5     "CleanupOldestDataIfEntriesCountAbove": 0
6    }
```

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

August 26, 2024

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 d'exécution 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 de l'administrateur et du service d'exécution. 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 d'administration et d'exécution. 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
     }
```

> **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.

Notifications de tiers

August 26, 2024

Citrix Secure Private Access pour locaux