# StorageZones Controller 5.x

**Machine translated content**

## Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

# Contents



# A propos de StorageZones Controller

May 28, 2024

Storage Zones Controller étend le stockage cloud ShareFile Software as a Service (SaaS) en fournissant à votre compte ShareFile un stockage de données privé.

Pour plus d'informations sur le StorageZones Controller, telles que les composants, le stockage des données, etc., consultez Storage Zones Controller 5.x.

Consultez la section Nouveautés pour connaître les dernières améliorations apportées à ce logiciel et à ShareFile.

Pour télécharger la dernière version du contrôleur ShareFile Storagezone, rendez-vous sur https://dl.sharefile.com/storagezone-controller. Connectez-vous à votre compte ShareFile pour accéder à tous les téléchargements d'applications.

> **Conseil :**
>
> ShareFile recommande aux utilisateurs d'activer les alertes de détection des menaces.

## Problèmes résolus

### Problèmes résolus dans StorageZones Controller 5.11.25

Cette version corrige plusieurs problèmes qui améliorent les performances et la stabilité globales.

### Problèmes résolus dans StorageZones Controller 5.11.24

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.11.23

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.11.22

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.11.21

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.11.18

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.11.17

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.11

Cette version résout un certain nombre de problèmes qui améliorent les performances et la stabilité globales.

### Problèmes résolus dans StorageZones Controller 5.10

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales.

### Problèmes résolus dans StorageZones Controller 5.9

Cette version contient des correctifs pour améliorer la fiabilité et les performances.

### Problèmes résolus dans StorageZones Controller 5.8

Cette version contient un correctif visant à améliorer les messages d'erreur pour les fichiers retirés et un correctif pour les nouveaux chemins gérés publiés dans SharePoint.

### Problèmes résolus dans StorageZones Controller 5.7

Cette version contient des correctifs visant à résoudre un problème de redirection lors du téléchargement de fichiers vers la zone de stockage et les connecteurs locaux.

### Problèmes résolus dans StorageZones Controller 5.6

**Correctif WOPI :** inclut des modifications visant à résoudre les problèmes rencontrés lors de tentatives ultérieures de modification de fichiers Office.

**Correction du connecteur SharePoint :** cette version inclut des modifications visant à afficher des messages d'erreur valides lors de la création de dossiers qui existent déjà sur SharePoint Connector.

### Problèmes résolus dans StorageZones Controller 5.5

Cette version contient des correctifs pour améliorer la fiabilité et les performances.

### Problèmes résolus dans StorageZones Controller 5.4.2

**Correctif du connecteur SharePoint :** le déplacement de fichiers présents sur le connecteur SharePoint peut échouer dans des scénarios spécifiques. Cette version garantit que le déplacement des fichiers présents sur SharePoint Connector fonctionne comme prévu.

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

### Problèmes résolus dans StorageZones Controller 5.4.1

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité et la fiabilité.

**Support supplémentaire :** La prise en charge des comptes *cloud/*cloudburrito a été ajoutée pour l' environnement Workspace.

### Problèmes résolus dans StorageZones Controller 5.3.1

Cette version contient des correctifs pour améliorer la fiabilité et les performances.

### Problèmes résolus dans StorageZones Controller 5.3.1

**Correctif WOPI : les** jetons d'accès WOPI étaient potentiellement falsifiés par le vol de la clé cryptographique publique. Cette version garantit que la clé n'est pas partagée entre les StorageZones Controller.

**Correctifs de sécurité :** cette version contient des correctifs pour la sécurité, les performances et la fiabilité.

## Problèmes connus

### Problèmes connus dans Storage Zones Controller 5.10

Aucun nouveau problème n'a été observé dans cette version.

### Problèmes connus dans Storage Zones Controller 5.9

Aucun nouveau problème n'a été observé dans cette version.

### Problèmes connus dans Storage Zones Controller 5.8

Aucun nouveau problème n'a été observé dans cette version.

### Problèmes connus dans Storage Zones Controller 5.7

Aucun nouveau problème n'a été observé dans cette version.

## Aperçu de l'architecture

July 25, 2024

Cette section fournit une vue d'ensemble du déploiement de StorageZones Controller pour des évaluations de validation de principe ou des environnements de production à haute disponibilité. Le déploiement à haute disponibilité s'affiche à la fois avec et sans proxy DMZ tel que Citrix ADC.

Pour évaluer un déploiement avec plusieurs StorageZones Controller, suivez les instructions relatives à un déploiement à haute disponibilité.

Chacun des scénarios de déploiement nécessite un compte ShareFile Enterprise. Par défaut, ShareFile stocke les données dans le cloud géré sécurisé par ShareFile. Pour utiliser le stockage de données privé, qu'il s'agisse d'un partage réseau local ou d'un système de stockage tiers pris en charge, configurez des zones de stockage pour ShareFile Data.

Pour fournir en toute sécurité des données aux utilisateurs à partir de partages de fichiers réseau ou de bibliothèques de documents SharePoint, configurez les connecteurs de zone de stockage.

### Déploiement de preuve de concept du StorageZones Controller

> **Attention :**
>
> Un déploiement de validation de principe est uniquement destiné à des fins d'évaluation et ne doit pas être utilisé pour le stockage de données critiques.

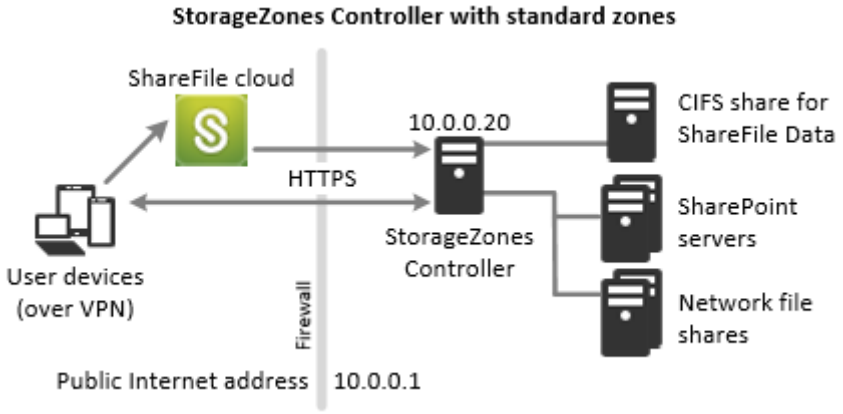
Un déploiement de validation de principe utilise un seul StorageZones Controller. L'exemple de déploiement décrit dans cette section comporte à la fois des zones de stockage pour ShareFile Data et des connecteurs de zone de stockage activés.

Pour évaluer un seul StorageZones Controller, vous pouvez éventuellement stocker les données dans un dossier (tel que C:\ZoneFiles) sur le disque dur du StorageZones Controller plutôt que sur un partage réseau distinct. Toutes les autres exigences du système s'appliquent à un déploiement d'évaluation.

### Déploiement de preuve de concept pour les zones de stockage standard

Un StorageZones Controller configuré pour les zones standard doit accepter les connexions entrantes depuis le cloud ShareFile. Pour ce faire, le responsable du traitement doit disposer d'une adresse Internet accessible au public et le protocole SSL doit être activé pour les communications avec le cloud ShareFile. La figure suivante indique le flux de trafic entre les appareils utilisateur, le cloud ShareFile et le StorageZones Controller.




Dans ce scénario, un pare-feu se trouve entre Internet et le réseau sécurisé. Le StorageZones Controller se trouve à l'intérieur du pare-feu pour contrôler l'accès. Les connexions utilisateur à ShareFile doivent traverser le pare-feu et utiliser le protocole SSL sur le port 443 pour établir cette connexion. Pour prendre en charge cette connectivité, vous devez ouvrir le port 443 sur le pare-feu et installer un certificat SSL public sur le service IIS du StorageZones Controller.

## Déploiement de StorageZones Controller à haute disponibilité

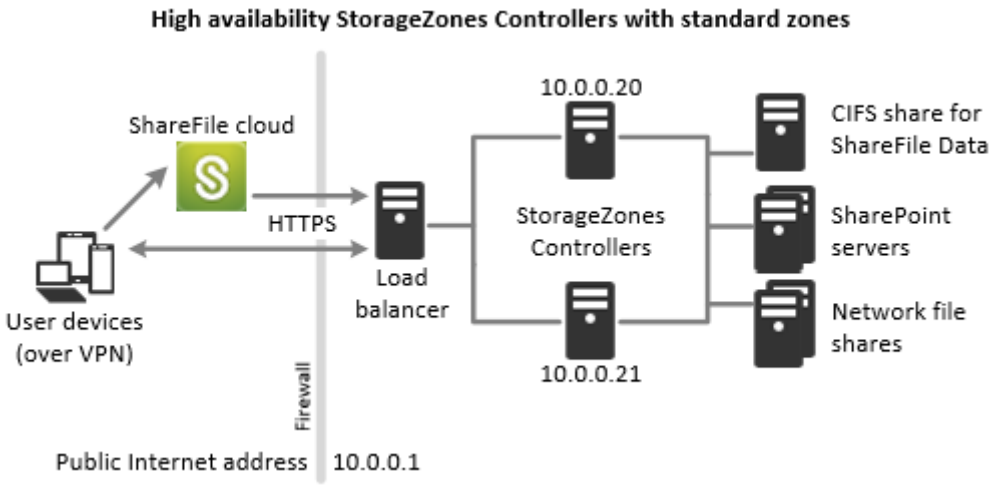
Pour un déploiement en production de ShareFile avec haute disponibilité, la meilleure pratique recommandée consiste à installer au moins deux StorageZones Controller. Lorsque vous installez le premier contrôleur, vous créez une zone de stockage. Lorsque vous installez les autres contrôleurs, vous les connectez à la même zone. Les StorageZones Controller qui appartiennent à la même zone doivent utiliser le même partage de fichiers pour le stockage.

Dans un déploiement à haute disponibilité, les serveurs secondaires sont des StorageZones Controller indépendants et pleinement opérationnels. Le sous-système de contrôle des zones de stockage choisit de manière aléatoire un contrôleur de zones de stockage pour les opérations. Si le serveur principal est hors ligne, vous pouvez facilement promouvoir un serveur secondaire au rang de serveur principal. Vous pouvez également rétrograder un serveur du statut principal au serveur secondaire.

### Déploiement à haute disponibilité pour les zones standard

Les StorageZones Controller configurés pour les zones de stockage standard doivent accepter les connexions entrantes depuis le cloud ShareFile. Pour ce faire, chaque responsable du traitement doit disposer d'une adresse Internet accessible au public et le protocole SSL doit être activé pour les communications avec le cloud ShareFile. Vous pouvez configurer plusieurs adresses publiques externes, chacune étant associée à un StorageZones Controller différent. La figure suivante montre un déploiement à haute disponibilité pour des zones de stockage standard.




Comme dans le scénario de déploiement de preuve de concept ci-dessus, un pare-feu se trouve entre Internet et le réseau sécurisé. Les StorageZones Controller se trouvent à l'intérieur du pare-feu pour contrôler l'accès. Les connexions utilisateur à ShareFile doivent traverser le pare-feu et utiliser le protocole SSL sur le port 443 pour établir cette connexion. Pour prendre en charge cette connectivité, vous devez ouvrir le port 443 sur le pare-feu et installer un certificat SSL public sur le service IIS de tous les StorageZones Controller.

### Configuration du stockage partagé

Les StorageZones Controller qui appartiennent à la même zone de stockage doivent utiliser le même partage de fichiers pour le stockage. Les StorageZones Controller accèdent au partage à l'aide de l'utilisateur du pool de comptes IIS. Par défaut, les pools d'applications fonctionnent sous le compte d'utilisateur Service réseau, qui dispose de droits d'utilisateur de bas niveau. Un StorageZones Controller utilise le compte Network Service par défaut.

Vous pouvez utiliser un compte d'utilisateur nommé au lieu du compte de service réseau pour accéder au partage. Pour utiliser un compte utilisateur nommé, spécifiez le nom d'utilisateur et le mot de passe sur la page de configuration de la console StorageZones. Exécutez le pool d'applications IIS et les services ShareFile à l'aide du compte Network Service.

### Connexions réseau

Les connexions réseau varient en fonction du type de zone : ShareFile géré ou standard.

**Zones gérées par ShareFile** Le tableau suivant décrit les connexions réseau qui se produisent lorsqu'un utilisateur ouvre une session sur ShareFile, puis télécharge un document depuis une zone gérée ShareFile. Toutes les connexions utilisent HTTPS.

| Étape | Source | Destination |
|---|---|---|
| 1. Demande d'ouverture de session utilisateur | Client | `company.sharefile.com:443` |
| 2. (Facultatif) Redirection vers l'ouverture de session SAML IdP | Client | URL du fournisseur d'identité SAML |
| 3. Enumération de fichiers/dossiers et demande de téléchargement | Client | `company.sharefile.com:443` |
| 4. Téléchargement du fichier | Client | `storage-location.sharefile.com:443` |

**Zones de stockage standard** Le tableau suivant décrit les connexions réseau qui se produisent lorsqu'un utilisateur ouvre une session sur ShareFile, puis télécharge un document depuis une zone de stockage standard. Toutes les connexions utilisent HTTPS.

| Étape | Source | Destination |
|---|---|---|
| 1. Demande d'ouverture de session utilisateur | Client | `company.sharefile.com` |
| 2. (Facultatif) Si vous utilisez ADFS, redirigez vers l'ouverture de session SAML IdP | Client | URL du fournisseur d'identité SAML |
| 3. Enumération de fichiers/dossiers et demande de téléchargement | Client | `company.sharefile.com` |
| 4. Autorisation de téléchargement de fichiers | `company.sharefile.com` | `szc.company.com` |

| Étape | Source | Destination |
|---|---|---|
| 5. Téléchargement du fichier | Client | `szc.company.com` |

### Déploiement du proxy DMZ du StorageZones Controller

Une zone démilitarisée (DMZ) fournit un niveau de sécurité supplémentaire au réseau interne. Un proxy DMZ, tel que Citrix ADC VPX, est un composant facultatif utilisé pour :

- Assurez-vous que toutes les demandes adressées à un StorageZones Controller proviennent du cloud ShareFile, afin que seul le trafic approuvé parvienne aux StorageZones Controller.

  Le StorageZones Controller dispose d'une opération de validation qui vérifie la validité des signatures URI pour tous les messages entrants. Le composant DMZ est chargé de valider les signatures avant de transférer les messages.

- Demandes d'équilibrage de charge adressées aux StorageZones Controller à l'aide d'indicateurs d'état en temps réel.

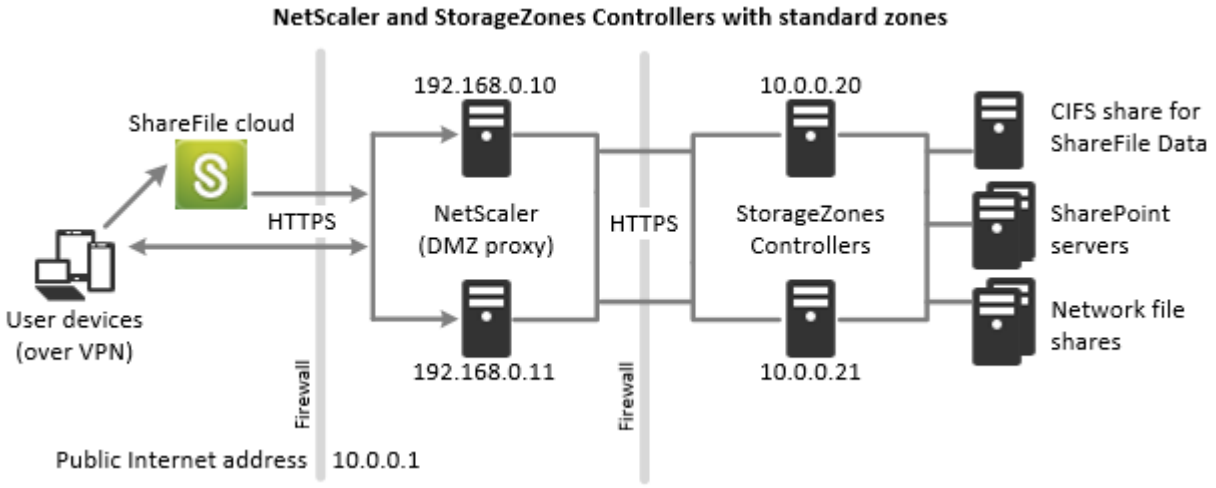
  Les opérations peuvent être équilibrées en charge par rapport aux StorageZones Controller s' ils peuvent tous accéder aux mêmes fichiers.

- Déchargez le protocole SSL des StorageZones Controller.
- Assurez-vous que les demandes de fichiers sur SharePoint ou sur des lecteurs réseau sont authentifiées avant de passer par la zone démilitarisée.

#### Déploiement de Citrix ADC et de StorageZones Controller

**Déploiement pour les zones de stockage standard** Les StorageZones Controller configurés pour les zones standard doivent accepter les connexions entrantes depuis le cloud ShareFile. Pour ce faire, le Citrix ADC doit disposer d'une adresse Internet accessible au public et le protocole SSL doit être activé pour les communications avec le cloud ShareFile.



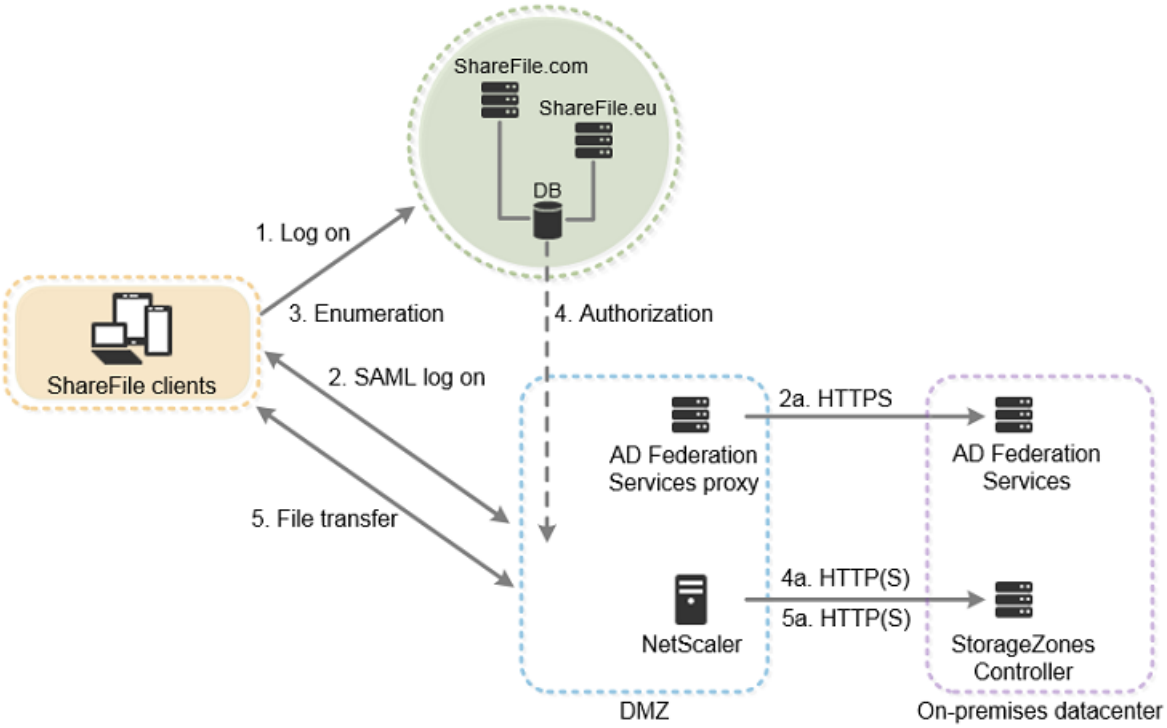

Dans ce scénario, deux pare-feux se situent entre Internet et le réseau sécurisé. Les StorageZones Controller résident dans le réseau interne. Les connexions utilisateur à ShareFile doivent traverser le premier pare-feu et utiliser le protocole SSL sur le port 443 pour établir cette connexion. Pour prendre en charge cette connectivité, vous devez ouvrir le port 443 sur le pare-feu et installer un certificat SSL public sur le service IIS des serveurs proxy DMZ (s'ils interrompent la connexion utilisateur).

### Connexions réseau pour les zones standard

Le schéma et le tableau suivants décrivent les connexions réseau qui se produisent lorsqu'un utilisateur se connecte à ShareFile, puis télécharge un document depuis une zone standard déployée derrière Citrix ADC. Dans ce cas, le compte utilise les services ADFS (Active Directory Federation Services) pour l'ouverture de session SAML.

Le trafic d'authentification est géré dans la zone démilitarisée par un serveur proxy ADFS qui communique avec un serveur ADFS sur le réseau sécurisé. L'activité des fichiers est accessible via Citrix ADC dans la zone démilitarisée, qui met fin au protocole SSL, authentifie les demandes des utilisateurs, puis accède au StorageZones Controller du réseau sécurisé pour le compte des utilisateurs authentifiés. L'adresse externe Citrix ADC pour ShareFile est accessible via le nom de domaine complet Internet szc.company.com.

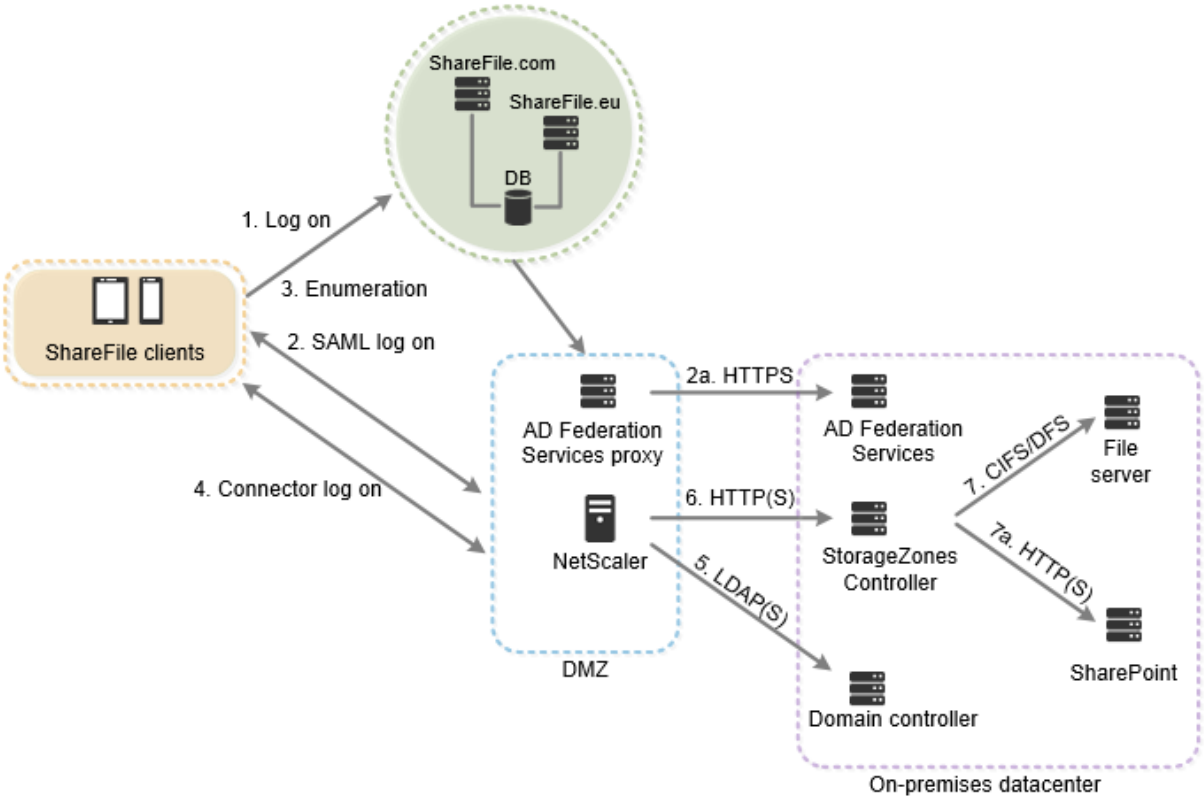



| Étape | Source | Destination | Protocole |
|---|---|---|---|
| 1. Demande d'ouverture de session utilisateur | Client | company.sharefile.com | HTTPS |
| 2. (Facultatif) Redirection vers l'ouverture de session SAML IdP | Client | URL du fournisseur d'identité SAML | HTTPS |
| 2a. Ouverture de session ADFS | Proxy ADFS | serveur ADFS | HTTPS |
| 3. Enumération de fichiers/dossiers et demande de téléchargement | Client | company.sharefile.com | HTTPS |
| 4. Autorisation de téléchargement de fichiers | ShareFile | szc.company.com (adresse externe) | HTTP(S) |

| Étape | Source | Destination | Protocole |
|---|---|---|---|
| 4a. Autorisation de téléchargement de fichiers | IP NetScaler ADC (NSIP) | StorageZones Controller | HTTPS |
| 5. Téléchargement du fichier | Client | szc.company.com (adresse externe) | HTTPS |
| 5a. Téléchargement du fichier | IP NetScaler ADC (NSIP) | StorageZones Controller | HTTP(S) |

Le schéma et le tableau suivants étendent le scénario précédent pour montrer les connexions réseau pour les connecteurs StorageZone. Ce scénario inclut l'utilisation de NetScaler dans la zone démilitarisée pour mettre fin au protocole SSL et authentifier les utilisateurs pour l'accès aux connecteurs.

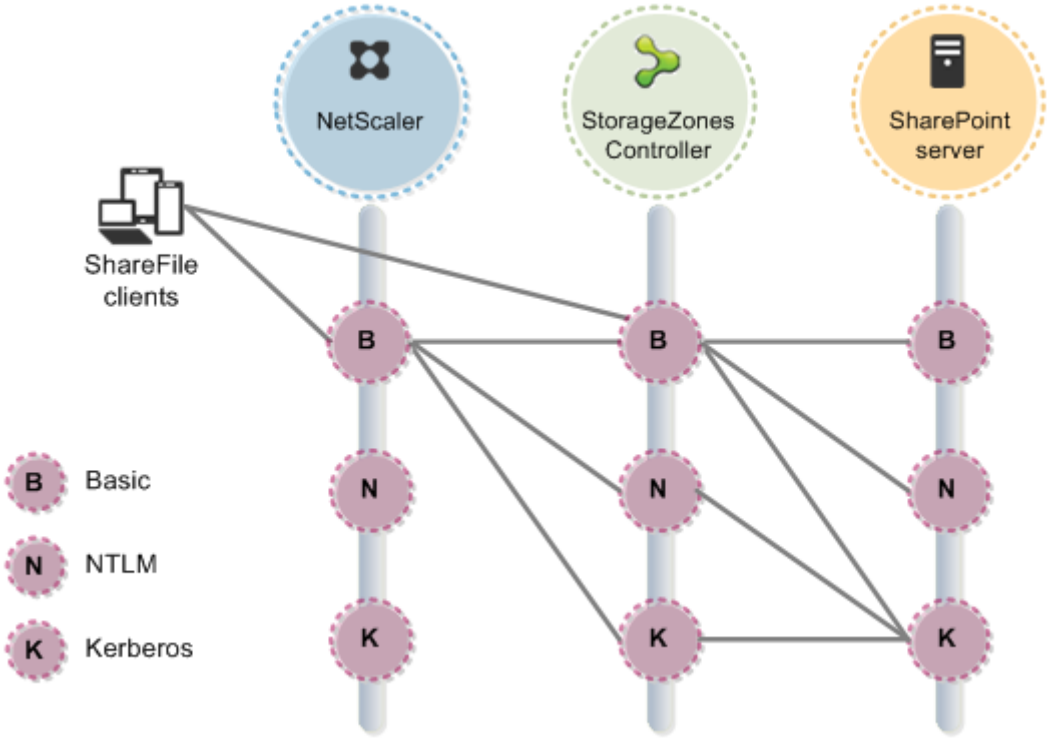


| Étape | Source | Destination | Protocole |
|---|---|---|---|
| 1. Demande d'ouverture de session utilisateur | Client | company.sharefile.com | HTTPS |
| 2. (Facultatif) Redirection vers l'ouverture de session SAML IdP | Client | URL du fournisseur d'identité SAML | HTTPS |
| 2a. Ouverture de session ADFS | Proxy ADFS | serveur ADFS | HTTPS |
| 3. Énumération des connecteurs de niveau supérieur | Client | company.sharefile.com | HTTPS |
| 4. L'utilisateur ouvre une session sur le serveur StorageZones Controller | Client | szc.company.com (adresse externe) | HTTPS |
| 5. Authentification des utilisateurs | IP NetScaler ADC (NSIP) | Contrôleur de domaine AD | LDAP (S) |
| 6. Enumération de fichiers/dossiers et demandes de chargement/téléchargement | IP NetScaler ADC (NSIP) | StorageZones Controller | HTTP(S) |
| 7. Énumération des partages réseau et chargement/téléchargement | StorageZones Controller | Serveur de fichiers | CIFS ou DFS |
| 7a. Énumération et chargement/téléchargement dans SharePoint | StorageZones Controller | SharePoint | HTTP(S) |

Le schéma suivant récapitule les combinaisons de types d'authentification prises en charge selon que l'utilisateur s'authentifie ou non.




## Configuration système requise

November 15, 2023

> **Important :**
>
> Microsoft mettra fin au support de Windows Server 2012R2 le 10 octobre 2023. Il est important de migrer votre serveur vers une version plus récente avant la date de fin du support.

### StorageZones Controller

- Une machine physique ou virtuelle dédiée avec 2 processeurs et 4 Go de RAM
- Windows Server 2012 R2 (Datacenter, Standard ou Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

**Pour les zones de stockage standard :**

- Utilisez un nom d'hôte Internet pouvant être résolu publiquement (et non une adresse IP).
- Activez SSL pour les communications avec ShareFile.

  - Le certificat SSL du StorageZones Controller doit être approuvé par les appareils des utilisateurs et les serveurs Web ShareFile. Si vous utilisez le protocole SSL directement avec IIS, reportez-vous à la section http://support.microsoft.com/kb/298805 pour plus d'informations sur la configuration du protocole SSL.

- Autorisez les requêtes TCP entrantes sur le port 443 via votre pare-feu.
- Autorisez les requêtes TCP sortantes vers le plan de contrôle ShareFile sur le port 443 via votre pare-feu.
  - Cliquez ici pour obtenir une liste détaillée des plages d'adresses IP et des domaines.

**Pour le contrôle de l'état du serveur utilisé uniquement pour les zones de stockage pour ShareFile Data :**

- Ouvrez le port 80 sur l'hôte local.

**Pour un environnement de production à haute disponibilité :**

- Au moins deux serveurs sur lesquels StorageZones Controller est installé.
- Si vous n'utilisez pas de serveurs proxy DMZ, installez un certificat SSL sur le service IIS.

  Pour plus d'informations sur les certificats pris en charge, consultez les exigences relatives aux certificats pour les zones standard ci-dessus.

**Pour un déploiement de proxy DMZ :**

- Un ou plusieurs serveurs proxy DMZ, tels que des instances NetScaler ADC VPX.
- Pour un serveur proxy DMZ qui met fin à la connexion client et utilise HTTP, installez un certificat SSL sur le serveur proxy.

  Si les communications entre le serveur proxy DMZ et le StorageZones Controller sont sécurisées, vous pouvez utiliser le protocole HTTP. Toutefois, le protocole HTTPS est recommandé en tant que meilleure pratique. Si vous utilisez le protocole HTTPS, vous pouvez utiliser un certificat privé (Enterprise) sur le StorageZones Controller s'il est approuvé par le proxy DMZ. L'adresse externe exposée par le proxy DMZ doit utiliser un certificat commercialement fiable. Pour plus d'informations sur les certificats pris en charge, consultez les exigences relatives aux certificats pour les zones standard ci-dessus.

### Autres configurations requises

> **Remarque :**
>
> ShareFile ne prend pas officiellement en charge et ne recommande pas d'utiliser la réplication DFS. Il est connu pour provoquer des échecs de verrouillage pour les fichiers plus volumineux. Si la réplication DFS doit être utilisée, utilisez des solutions de sauvegarde distinctes pendant les

> heures creuses lorsque la zone n'est pas activement utilisée.

- Le programme d'installation du StorageZones Controller nécessite des privilèges administratifs.
- Pour l'administration à distance du StorageZones Controller, utilisez un protocole distant, tel que RDP ou Citrix ICA, pour vous connecter au serveur, puis ouvrez la console du StorageZones Controller.

#### Systèmes de stockage tiers pris en charge

- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure

#### Solutions de prévention des pertes de données prises en charge

- Le Storage Zones Controller s'intègre à toutes les solutions DLP conformes à la norme ICAP, notamment :
  - Prévention de la perte de données Symantec
  - McAfee DLP Prevent
  - Websense TRITON AP-DATA
  - Prévention des pertes de données RSA

### Zones de stockage pour les données ShareFile

Les zones de stockage pour ShareFile Data sont une fonctionnalité facultative que vous activez sur un StorageZones Controller.

Exigences :

- Compte ShareFile Enterprise, avec la fonctionnalité de zone de stockage activée
- Un compte utilisateur ShareFile qui inclut l'autorisation de créer et de gérer des zones
- Un partage CIFS pour le stockage de données privées

Si vous envisagez de stocker des fichiers ShareFile dans un système de stockage tiers compatible, le partage CIFS est utilisé pour les fichiers temporaires (clés de chiffrement, fichiers en file d'attente) et comme cache de stockage temporaire.

- Le rôle de serveur Web (IIS) et ASP.NET 4.x. Pour plus d'informations, voir Préparer votre serveur pour les données ShareFile.

Remarque : L'accès à un compte ShareFile depuis un client FTP n'est pas compatible avec les zones de stockage pour ShareFile Data.

### Connecteur de zone de stockage pour SharePoint

Le connecteur de zone de stockage pour SharePoint est une fonctionnalité facultative que vous activez sur un StorageZones Controller.

Exigences :

- Compte ShareFile Enterprise, avec la fonctionnalité de zone de stockage activée, ou Citrix Endpoint Management.
- Seuls **Microsoft SharePoint Server 2010 et versions ultérieures** sont pris en charge.
- Le serveur StorageZones Controller doit être membre du domaine, dans la même forêt que le serveur SharePoint.
- Le rôle de serveur Web (IIS) et ASP.NET 4.x. Pour plus d'informations, voir Préparer votre serveur pour les données ShareFile.
- Stratégies SharePoint :
  - La taille maximale par défaut du fichier de téléchargement pour une application Web est de 250 Mo dans SharePoint 2013 et de 50 Mo dans SharePoint 2010. Pour modifier la valeur par défaut : dans l'administration centrale de SharePoint, accédez à la page Paramètres généraux de l'application Web et modifiez la taille maximale de téléchargement. La taille limite du fichier de téléchargement pour SharePoint est de 2 Go.
  - Les clients ShareFile tentent toujours d'archiver une version majeure (publication) d'un fichier. Toutefois, les stratégies de SharePoint déterminent si un fichier est archivé en tant que version principale ou secondaire.
  - L'autorisation d'affichage uniquement de SharePoint ne permet pas à un utilisateur de télécharger des fichiers. Pour lire un fichier à partir d'un client ShareFile, un utilisateur SharePoint doit disposer d'une autorisation de lecture.
- Appareils utilisateurs : pour obtenir les informations les plus récentes sur la prise en charge des machines utilisateur pour les connecteurs de zone de stockage, consultez la base de connaissances ShareFile.

#### Connecteur de zone de stockage pour l'authentification SharePoint

Après avoir authentifié l'utilisateur, le serveur StorageZones Controller établit des connexions au serveur SharePoint au nom de l'utilisateur authentifié et répond aux défis d'authentification présentés par le serveur SharePoint. Le connecteur de zone de stockage pour SharePoint prend en charge les méthodes d'authentification suivantes sur le serveur SharePoint.

- De base

  Nécessite que vous ajoutiez `<add key="CacheCredentials"value="1"\>` à `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`

- 
- Négocier (Kerberos)
- Défi/Réponse Windows (NTLM)

Les clients mobiles ShareFile utilisent l'authentification de base via HTTPS pour s'authentifier auprès du Storage Zones Controller ou du proxy DMZ. L'authentification unique à SharePoint est régie par les exigences d'authentification définies sur le serveur SharePoint. Pour utiliser l'authentification Kerberos ou NTLM sur le serveur SharePoint : configurez le contrôleur de domaine pour qu'il approuve le StorageZones Controller pour la délégation.

Si votre serveur SharePoint est configuré pour l'authentification Kerberos : configurez un nom principal de service (SPN) pour les comptes de service utilisateur nommés pour le pool d'applications du serveur SharePoint. Pour plus d'informations, voir « Configurer la confiance pour la délégation pour les composants WebPart » dans http://support.microsoft.com/kb/832769.

Pour les déploiements avec Citrix ADC, il est possible de mettre fin à l'authentification de base auprès du Citrix ADC, puis d'effectuer d'autres types d'authentification auprès du StorageZones Controller.

### Connecteur de zone de stockage pour les partages de fichiers réseau

Le connecteur de zone de stockage pour les partages de fichiers réseau est une fonctionnalité facultative que vous activez sur un StorageZones Controller.

Exigences :

- Compte ShareFile Enterprise ou Citrix Endpoint Management.
- Le serveur StorageZone Connector doit être membre du domaine, dans la même forêt que les serveurs de fichiers réseau.
- Le rôle de serveur Web (IIS) et ASP.NET 4.x. Pour plus d'informations, voir Préparer votre serveur pour les données ShareFile.
- Appareils utilisateurs : pour obtenir les informations les plus récentes sur la prise en charge des machines utilisateur pour les connecteurs de zone de stockage, consultez la base de connaissances ShareFile.

### Connecteur pour l'authentification des partages de fichiers réseau

Après avoir authentifié l'utilisateur, le serveur StorageZones Controller établit des connexions au serveur de fichiers réseau au nom de l'utilisateur authentifié et répond aux défis d'authentification présentés par le serveur de fichiers. Le connecteur de zone de stockage pour les partages de fichiers réseau prend en charge les méthodes d'authentification suivantes sur le serveur de fichiers.

- Négocier (Kerberos)
- Défi/Réponse Windows (NTLM)

Pour utiliser l'authentification Kerberos ou NTLM sur le StorageZones Controller : configurez le contrôleur de domaine pour qu'il approuve le StorageZones Controller pour la délégation.

Pour les déploiements avec NetScaler ADC : pour fournir aux utilisateurs une expérience d'authentification unique lorsque NetScaler ADC est configuré pour l'authentification de base, configurez le connecteur pour l'authentification Negotiate (Kerberos) et NTLM.

### Scripts et commandes PowerShell

L'installation du StorageZones Controller inclut plusieurs scripts et commandes PowerShell, situés dans `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`.

- Exécutez les scripts dans la version 32 bits (x86) de PowerShell.
- Pour de meilleurs résultats, effectuez une mise à niveau vers PowerShell 4.0 ou version ultérieure, inclus dans Windows Management Framework.

  PowerShell 2.0 provoque des problèmes importants en raison de problèmes de compatibilité avec .NET Framework 4.

## Installation

October 13, 2020

Effectuez les tâches suivantes, dans l'ordre présenté, pour installer et configurer le StorageZones Controller, les zones de stockage pour les données ShareFile et les connecteurs de zones de stockage.

1. Configurer Citrix ADC pour StorageZones Controller

   Vous pouvez utiliser Citrix ADC en tant que proxy DMZ pour le StorageZones Controller.

2. Création d'un partage réseau pour le stockage de données privées

   Les zones de stockage pour ShareFile Data nécessitent un partage réseau pour vos données privées, même si vous stockez des fichiers ShareFile dans un système de stockage tiers pris en charge.

3. Installer un certificat SSL

   Un StorageZones Controller qui héberge des zones standard nécessite un certificat SSL.

4. Préparer votre serveur pour les données ShareFile

   La configuration IIS et ASP.NET est requise pour les zones de stockage pour les données ShareFile et pour les StorageZone Connector.

5. Installer StorageZones Controller et créer une zone de stockage
6. Vérifier la configuration du Controller de vos zones de stockage
7. Modifier la zone par défaut des comptes d'utilisateur

   Par défaut, les comptes d'utilisateurs existants et nouvellement provisionnés utilisent le stockage cloud géré par ShareFile comme zone par défaut.

8. Spécifier un serveur proxy pour les zones de stockage

   La console StorageZones Controller vous permet de spécifier un serveur proxy correspondant. Vous pouvez également spécifier un serveur proxy à l'aide d'autres méthodes.

9. Configurer le contrôleur de domaine pour faire confiance au StorageZones Controller pour la délégation

   Configurez le contrôleur de domaine pour prendre en charge l'authentification NTLM ou Kerberos sur des partages réseau ou des sites SharePoint.

10. Joindre un StorageZones Controller secondaire à une zone de stockage

    Pour configurer une zone de stockage pour une haute disponibilité, connectez au moins deux StorageZones Controller à celle-ci.

Pour une démonstration de la configuration du StorageZones Controller avec Microsoft Azure Storage,cliquez ici.

Pour une démonstration de la configuration de ShareFile Enterprise pour utiliser une zone de stockage Microsoft Azure, cliquez ici.

### Instructions de configuration supplémentaires

- Configurer les zones de stockage multi-locataires
- Configurer le StorageZones Controller pour les aperçus Web App, les vignettes et le partage en lecture seule

## Configurer Citrix ADC pour StorageZones Controller

February 14, 2022

NetScaler, version 10.1 build 120.1316.e et ultérieures, inclut un assistant qui vous invite à entrer des informations de base sur votre environnement Storage Zones Controller. Il génère ensuite une configuration qui :

- Équilibre la charge du trafic entre les StorageZones Controller
- Fournit l'authentification des utilisateurs pour les connecteurs de zone
- Valide les signatures URI pour les chargements et téléchargements ShareFile
- Arrête les connexions SSL au niveau de l'appliance Citrix ADC

Le diagramme montre les composants Citrix ADC créés par la configuration :

- **Serveur virtuel de commutation de contenu Citrix ADC :** envoie les demandes de données des utilisateurs à partir de ShareFile et des connecteurs de zone de stockage vers le serveur virtuel d'équilibrage de charge Citrix ADC approprié.
- **Serveur virtuel d'équilibrage de charge Citrix ADC :** équilibre la charge du trafic pour vos StorageZones Controller et gère également les éléments suivants :
  - Pour les demandes de données provenant de votre stockage de données privé, un serveur virtuel d'équilibrage de charge effectue une validation de hachage, afin de s'assurer que des signatures URI valides sont présentes sur les demandes entrantes.
  - Pour les demandes de données provenant de connecteurs de zone de stockage, un serveur virtuel d'équilibrage de charge peut effectuer une authentification utilisateur. Il arrête une demande utilisateur au niveau de Citrix ADC, authentifie l'utilisateur, puis effectue l'authentification unique de l'utilisateur au StorageZones Controller.

> **Remarque :**
>
> L'authentification auprès des connecteurs de zone de stockage via Citrix ADC est facultative. En raison d'un problème connu, si l'authentification est activée dans Citrix ADC, les connecteurs de zone de stockage dans WebApp ne fonctionnent pas dans les navigateurs Chrome, Chromium, Safari et Edge. Il est compatible avec d'autres navigateurs et clients de bureau/mobiles.

À partir de Storage Zones Controller 4.0, les administrateurs peuvent limiter les connexions entrantes aux StorageZones Controller au protocole TLS v1.2. Si les protocoles antérieurs à TLS v1.2 sont désactivés pour le trafic entrant vers le contrôleur de zone de stockage, tous les composants logiciels clients qui interagissent avec la zone de stockage doivent également prendre en charge TLS v1.2. Cliquez ici pour obtenir des informations supplémentaires et des instructions de configuration.

> **Remarque :**
>
> Pour configurer les versions de NetScaler antérieures à 10.1 build 120.1316.e, reportez-vous à la section

> Configurer Citrix ADC manuellement.

L'assistant d'installation de Citrix ADC pour ShareFile ne gère pas la configuration requise pour utiliser Citrix Endpoint Management en tant que fournisseur d'identité SAML pour ShareFile. Pour plus d'informations, cliquez ici.

### Conditions préalables

- Une configuration Citrix ADC fonctionnelle
- Certificat de sécurité : si aucun n'est déjà disponible dans Citrix ADC, l'assistant vous permet d'en installer un sur le serveur virtuel de commutation de contenu.
- Informations sur votre configuration Active Directory (**l'assistant Citrix ADC pour ShareFile doit être complété par la licence Citrix NetScaler Enterprise Edition**) :
  - Adresse IP et port de votre serveur Active Directory
  - Nom de domaine Active Directory
  - DN de base LDAP où les utilisateurs sont stockés
  - Nom et mot de passe du compte d'administrateur autorisé à communiquer avec Active Directory

### Configurer Citrix ADC pour les StorageZones Controller

Les étapes suivantes expliquent comment utiliser l'assistant Citrix ADC pour ShareFile.

1. Ouvrez une session sur l'appliance Citrix ADC et, sous l'onglet Configuration, accédez à Gestion du trafic.
2. Sous Citrix ShareFile, cliquez sur Configurer Citrix ADC pour ShareFile.

   Vous pouvez également accéder à l'Assistant comme suit : Sous Mobilité, cliquez sur **Configurer Endpoint Management, ShareFile et Citrix Gateway**.
3. Fournissez les informations demandées dans l'assistant.

| Option | Description |
|---|---|
| Nom | Nom d'affichage du serveur virtuel de commutation de contenu. |

| Option | Description |
| --- | --- |
| IP Address | L'adresse IP externe (publique ou DMZ) à utiliser pour le serveur virtuel de commutation de contenu. Si vous utilisez une adresse IP DMZ, vous devez définir un mappage de traduction d'adresses réseau (NAT) entre votre adresse de pare-feu externe et cette adresse IP DMZ. |
| Données ShareFile | Cette option est activée, indiquant que vous utiliserez la connexion Citrix ADC pour les zones de stockage pour ShareFile Data. |
| connecteurs de zone de stockage pour partage de fichiers réseau/SharePoint | Si vous utilisez des connecteurs et que vous souhaitez effectuer une authentification utilisateur au niveau de Citrix ADC, cochez la case. |
| Certificat | Choisissez un certificat ou installez-en un pour le serveur virtuel de commutation de contenu. Si vous choisissez d'installer un certificat, vous êtes invité à télécharger le certificat et la clé privée. Pour les zones standard, les certificats doivent être approuvés publiquement et non auto-signés. |
| Adresse IP du StorageZones Controller | Les adresses IP internes pour un ou plusieurs serveurs de StorageZones Controller. Ces adresses IP définissent les serveurs Storage Zones Controller en tant qu'entités internes à Citrix ADC. Si vous avez déjà ajouté les serveurs à Citrix ADC, cliquez sur Ajouter à partir d'un serveur existant et sélectionnez les serveurs. Pour utiliser Citrix ADC pour l'équilibrage de charge, entrez une adresse IP interne pour chaque serveur Storage Zones Controller. Pour utiliser Citrix ADC uniquement pour SSL et l'authentification, entrez une seule adresse IP. |
| Port et protocole | Port et protocole utilisés pour la communication entre Citrix ADC et les StorageZones Controller. |

| Option | Description |
| --- | --- |
| L'adresse IP du serveur virtuel d'authentification, d'autorisation et d'audit (Citrix ADC AAA) | Adresse IP interne inutilisée pour le serveur virtuel Citrix ADC AAA. Citrix ADC crée ce serveur virtuel pour son propre usage. Le serveur n'a pas besoin d'accès extérieur. |
| Adresse IP et port du serveur LDAP | L'adresse IP et le port de votre serveur Active Directory. Si vous avez déjà ajouté un serveur LDAP à Citrix ADC, cliquez sur l'onglet Choisir LDAP et choisissez le serveur. |
| Tempo-out | Nombre maximal de secondes pendant lesquelles le Citrix ADC attend une réponse du serveur LDAP. Le délai par défaut est 3 secondes. La valeur minimale est de 1 seconde. |
| Domaine d'authentification unique | Le nom de domaine Active Directory. |
| DN de base (emplacement des utilisateurs) | Nom distinctif (DN) de base LDAP dans lequel les utilisateurs sont stockés. Spécifiez le DN à l'aide du formulaire général : CN=Users, dc=domain, DC=Net |
| DN et mot de passe de liaison administrateur | Compte d'administrateur autorisé à communiquer avec Active Directory. |
| Nom d'ouverture de session | Attribut LDAP, utilisé par Citrix ADC pour déterminer si les utilisateurs ouvrent une session avec leur nom d'utilisateur ou leur adresse e-mail. La valeur par défaut est SAMAccountName, qui permet aux utilisateurs de se connecter avec leur nom d'utilisateur. Pour demander aux utilisateurs de saisir leur adresse e-mail pour ouvrir une session, remplacez ce champ par UserPrincipalName. |

### Configurer Citrix ADC pour l'accès Web aux connecteurs

Pour prendre en charge l'accès Web aux connecteurs de zone de stockage, vous devez effectuer une configuration Citrix ADC supplémentaire après avoir terminé l'assistant Citrix ADC pour ShareFile.

- Créez et configurez un troisième serveur virtuel d'équilibrage de charge Citrix ADC, utilisé pour garantir que les clients ShareFile envoient des informations d'identification uniquement lorsqu'ils sont connectés à un domaine ShareFile approuvé.

Comme décrit dans les étapes suivantes, vous allez configurer le serveur virtuel supplémentaire pour autoriser l'accès anonyme des clients pour le verbe HTTP OPTIONS. La demande OPTIONS passe au StorageZones Controller sans être authentifiée et sans appels HTTPS pour valider la signature. Le contrôle en amont CORS valide l'approbation du domaine avant d'envoyer des informations d'identification.

Il n'est pas nécessaire de comprendre CORS pour effectuer la configuration. Toutefois, pour plus d'informations sur CORS, reportez-vous à la section http://enable-cors.org/.

- Pour prendre en charge l'accès Web aux connecteurs de zone de stockage, ajoutez un chemin (/ProxyService) à la stratégie de commutation de contenu utilisée pour le trafic vers /cifs et /sp.

Effectuez les étapes suivantes dans Citrix ADC après avoir terminé l'assistant Citrix ADC pour ShareFile.

1. Créez un troisième serveur virtuel d'équilibrage de charge :
   a) Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
   b) Cliquez sur Ajouter.
   c) Spécifiez les valeurs suivantes :

| Option | Valeur |
|---|---|
| Nom | Un nom de stratégie, tel que SF_ZONE_OPTIONS |
| Protocole | SSL |
| Type d'adresse IP | Non adressable |

   d) Cliquez ici pour créer le serveur virtuel.
   e) Pour y lier les mêmes services que les serveurs virtuels d'équilibrage de charge créés par l'Assistant : Dans l'écran Serveur virtuel d'équilibrage de charge, en face de Service, cliquez sur > puis sur Enregistrer.
   f) Ajoutez un certificat au serveur virtuel.
2. Créez une stratégie pour le serveur virtuel que vous venez d'ajouter :
   a) Accédez à Gestion du trafic > Changement de contenu > Stratégies.
   b) Dans le volet d'informations, cliquez sur Ajouter, puis spécifiez les valeurs Nom, Serveur virtuel LB cible et Expression. Cliquez sur **Expression Editor**, puis créez cette expression. Sélectionnez **HTTP**. Sélectionnez **REQ**. Sélectionnez **METHOD**. Sélectionnez EQ (String) et saisissez OPTIONS. L'expression doit se lire comme suit : `HTTP.REQ.METHOD.EQ("OPTIONS")`
   c) Cliquez sur **Terminé**.

d) Cliquez sur **Créer**.

3. Liez la stratégie que vous venez de créer au nouveau serveur virtuel d'équilibrage de charge :

   a) Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**.

   b) Dans la liste, cliquez sur le serveur virtuel, puis sur **Modifier**.

   c) Accédez à la section Liaison de stratégie de commutation de contenu et cliquez sur 2 stratégies de commutation de contenu.

   d) Cliquez sur **Ajouter une liaison**.

   e) Sélectionnez la nouvelle stratégie de contenu et sélectionnez le serveur virtuel d'équilibrage de charge cible.

   f) Cliquez sur **Bind**.

   g) Cliquez sur **Modifier la liaison** et mettez à jour la **priorité**. Modifiez la priorité de la nouvelle stratégie afin qu'elle ait le plus petit nombre des trois stratégies.

   La stratégie dont la valeur est la plus faible a la priorité la plus élevée et est donc traitée en premier.

4. Mettez à jour la stratégie utilisée pour le trafic vers les connecteurs de zone de stockage (_SF_CIF_SP_CSPOL) :

   a) Accédez à **Gestion du trafic > Changement de contenu > Stratégies**.

   b) Sélectionnez la stratégie _SF_CIF_SP_CSPOL.

   c) Ajoutez ce qui suit à l'expression de stratégie :

```
|| HTTP.REQ.URL.CONTAINS("/ProxyService/")
```

   L'expression politique complète doit être la suivante :

```
HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/sp/
    ") ||
HTTP.REQ.URL.CONTAINS("/ProxyService/")
```

5. Mettez à jour la stratégie utilisée pour le trafic vers les zones de stockage pour ShareFile Data (_SF_SZ_CSPOL) :

   a) Accédez à **Gestion du trafic > Changement de contenu > Stratégies**.

   b) Sélectionnez la stratégie **_SF_SZ_CSPOL** .

   c) Ajoutez ce qui suit à l'expression de stratégie :

```
&& HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT
```

   L'expression politique complète doit être la suivante :

```
HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("
    /sp/ “ ).NOT
&& HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT
```

### Configurez Citrix ADC pour le partage en lecture seule

Pour prendre en charge le partage en lecture seule, les utilisateurs doivent pouvoir accéder à votre serveur Microsoft Office Web Apps Server (OWA). Si votre serveur OWA est accessible en externe sur sa propre adresse, aucune configuration Citrix ADC supplémentaire ne doit être requise pour votre StorageZones Controller.

Si vous souhaitez combiner le StorageZones Controller et Office Web App Server sur une seule adresse externe à l'aide des stratégies de commutation de contenu Citrix ADC, vous devez effectuer une configuration Citrix ADC supplémentaire après avoir terminé l'assistant Citrix ADC pour ShareFile. La configuration Citrix ADC est requise pour garantir que le trafic est correctement acheminé vers votre serveur OWA accessible en externe.

Une fois les règles Citrix ADC suivantes configurées, les administrateurs peuvent réutiliser l'adresse externe existante de leur zone de StorageZones Controller, éliminant ainsi le besoin de créer une adresse externe supplémentaire pour OWA.

Pour créer et configurer un serveur virtuel d'équilibrage de charge Citrix ADC supplémentaire :

1. Créez un service d'équilibrage de charge supplémentaire.
   - Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
   - Cliquez sur **Ajouter**.
   - Entrez les informations requises pour créer un service qui correspond à votre/vos serveur (s) OWA. Cliquez sur **OK**.
2. Créez un serveur virtuel d'équilibrage de charge supplémentaire :
   - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
   - Cliquez sur **Ajouter**.
   - Spécifiez les valeurs suivantes :

| Option | Valeur |
|---|---|
| Nom | Un nom de stratégie, tel que SF_OWA_vServer |
| Protocole | SSL |
| Type d'adresse IP | Non adressable |

   - Cliquez ici pour créer le serveur virtuel.
   - Pour lier le serveur virtuel au service OWA que vous avez créé à l'étape précédente, cliquez sur **Liaison de service virtuel d'équilibrage de charge > Sélectionner un service**. Cochez la case en regard du service que vous avez créé à l'étape précédente.

- Cliquez sur **Sélectionner**.
- Cliquez sur **Bind**.

3. Créez une nouvelle stratégie utilisée pour acheminer le trafic vers votre serveur OWA.
   - Accédez à **Gestion du trafic > Changement de contenu > Stratégies**.
   - Sélectionnez **Ajouter**.
   - Nommez la stratégie.
   - Ajoutez l'expression suivante :
     - HTTP.REQ.URL.CONTAINS("/hosting/discovery")
       || HTTP.REQ.URL.CONTAINS("/x/")
       || HTTP.REQ.URL.CONTAINS("/wv/")
       || HTTP.REQ.URL.CONTAINS("/p/")
       L'expression politique complète doit être la suivante :
       HTTP.REQ.URL.CONTAINS("/hosting/discovery")
       || HTTP.REQ.URL.CONTAINS("/x/")
       || HTTP.REQ.URL.CONTAINS("/wv/")
       || HTTP.REQ.URL.CONTAINS("/p/")
4. Mettre à jour la priorité de la nouvelle stratégie dans le virtuel d'équilibrage de charge
   - Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**.
   - Cliquez sur le serveur virtuel d'équilibrage de charge, puis sélectionnez Stratégies de commutation de contenu.
   - Modifiez la priorité des stratégies afin que la stratégie (Exemple) « _SF_OWA » soit la troisième priorité.

| Priority | Nom de la stratégie |
|---|---|
| 90 | SF_ZK_OPTIONS |
| 95 | _SF_CIF_SP_SPOL |
| 99 | _SF_OWA |
| 100 | _SF_SZ_CSPOL |

- Cliquez sur **Fermer**. Cliquez sur **Terminé**

### Création d'un moniteur pour le service Storage Zones Controller

Par défaut, Citrix ADC envoie une requête ping au serveur Storage Zones Controller pour déterminer s'il est en ligne. Toutefois, même si le contrôleur est en ligne, il se peut qu'il ne soit pas en mesure

d'envoyer des messages de pulsation au site Web ShareFile. Dans ce cas, Citrix ADC enverra le trafic vers Storage Zones Controller bien qu'il ne communique pas avec ShareFile.

Pour vérifier la connectivité sortante du Storage Zones Controller à ShareFile, vous pouvez créer un moniteur qui vérifie heartbeat.aspx et le lie au service Citrix ADC pour chaque StorageZones Controller.

```
1     add lb monitor SZC_Heartbeat HTTP-ECV -send "GET /heartbeat.aspx" -
         recv "\*\*\*ONLINE\*\*\* ”  -secure YES
2 bind service StorageZone_Svc -monitorName SZC_Heartbeat
```

StorageZone_SVC est le service Citrix ADC qui correspond à un StorageZones Controller. Ce nom de service est automatiquement créé par l'assistant Citrix ADC pour ShareFile. Le nom du service inclut l'adresse IP du contrôleur, telle que SF_SVC_IP-Address.

-secure YES est requis si le service écoute sur le port 443.

### Vérifiez la configuration de Citrix ADC

Une fois l'Assistant terminé, accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** pour afficher l'état des serveurs virtuels d'équilibrage de charge créés par l'Assistant.

### Afficher le débit des demandes ShareFile via Citrix ADC

Les statistiques de débit se trouvent dans le menu **Tableau de bord** .

## Configurer manuellement Citrix ADC

April 20, 2023

Depuis la version 10.1 build 120.1316, NetScaler inclut un assistant qui configure les paramètres nécessaires pour les données et les connecteurs du contrôleur de zone de stockage.

Les étapes de cette section décrivent les paramètres **Citrix ADC** nécessaires pour le contrôleur de zone de stockage. Tous les liens renvoient à la documentation de NetScaler 10.1. Des rubriques similaires sont disponibles pour les versions ultérieures de Citrix ADC.

### Pour vérifier la validité des signatures URI sur tous les messages entrants

1. Créez une légende HTTP nommée sf_callout :

a) Dans la boîte de dialogue Configurer la légende HTTP, cliquez sur **Serveur virtuel ou Adresse IP** et spécifiez l'adresse.

b) Sous Demande à envoyer au serveur, cliquez sur **Basée sur les attributs**, puis sur **Configurer les attributs de demande**.

c) Sélectionnez **Obtenir la méthode**.

d) Dans Host Expression, entrez l'adresse IP du serveur virtuel ou l'adresse IP de l'hôte de l'un des contrôleurs de zones de stockage.

e) Dans l'expression de tige d'URL, entrez :

```
1 "/validate.ashx?RequestURI=" + HTTP.REQ.URL.BEFORE_STR("&h").
    HTTP_URL_SAFE.B64ENCODE + "&h="+ HTTP.REQ.URL.QUERY.VALUE("
    h")
```

f) Cliquez sur **OK**, puis revenez à la boîte de dialogue Configurer la légende HTTP.

g) Sous Réponse du serveur, choisissez le type de retour Bool.

h) Dans l'expression pour extraire les données de la réponse, entrez :

`HTTP.RES.STATUS.EQ(200).NOT`

i) Cliquez sur **Create**.

2. Suivez les étapes précédentes pour configurer une légende HTTP nommée sf_callout_y. Utilisez les mêmes paramètres à l'exception de l'expression :

   - Dans l'expression de tige d'URL, entrez :

```
1  "/validate.ashx?RequestURI=" + HTTP.REQ.URL.HTTP_URL_SAFE.
     B64ENCODE + "&h="
```

3. Configurez une politique de réponse :

   a) Dans la boîte de dialogue Configurer la politique du répondeur : pour Action, choisissez Supprimer.

   b) Entrez l'expression :

```
1 http.REQ.URL.CONTAINS("&h=") && http.req.url.contains("/
    crossdomain.xml").not && http.req.url.contains("/validate.
    ashx?requri").not && SYS.HTTP_CALLOUT(sf_callout) || http.
    REQ.URL.CONTAINS("&h=").NOT && http.req.url.contains("/
    crossdomain.xml").not && http.req.url.contains("/validate.
    ashx?requri").not && SYS.HTTP_CALLOUT(sf_callout_y)
```

   Pour plus d'informations, voir Répondeur.

4. Liez la politique du répondeur au serveur virtuel de l'équilibreur de charge et configurez la persistance basée sur les sessions SSL.

### Pour équilibrer la charge

1. Configurez l'équilibrage de charge basé sur des jetons.

   Utilisez l'expression de règle : “ `http.REQ.URL.QUERY.VALUE("uploadid")` ”

   L'équilibrage de charge basé sur des jetons est requis pour les contrôleurs de zones de stockage dans le cadre d'un déploiement à haute disponibilité. L'équilibrage de charge circulaire entraîne des échecs intermittents de téléchargement ou de chargement, car une demande de chargement ou de téléchargement d'un client peut être dirigée vers un contrôleur de zone de stockage autre que celui qui a reçu la demande d'autorisation de Sharefile.com.

2. Configurez Citrix ADC pour mettre fin aux connexions SSL.

   Pour plus d'informations, consultez la section Configuration du déchargement SSL.

### Pour configurer la commutation de contenu et l'authentification pour les connecteurs

1. Pour activer le changement de contenu, consultez la section Activation du changement de contenu.

2. Créez une politique de changement de contenu pour les demandes des utilisateurs concernant les données ShareFile provenant de vos zones de stockage sur site :

   a) Dans la boîte de dialogue Configurer la politique de commutation de contenu, entrez le nom de la stratégie de commutation de contenu. Ces étapes utilisent le nom Data_Requests.

   b) Entrez l'expression :

   ```
   HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerHostName")
       && HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.
       CONTAINS("/sp/").NOT
   ```

   c) Cliquez sur **OK**.

   Pour plus d'informations, voir Commutation de contenu.

3. Créez une politique de changement de contenu pour les demandes des utilisateurs concernant les données accessibles via des connecteurs de zone de stockage.

   a) Dans la boîte de dialogue Configurer la politique de commutation de contenu, indiquez le nom de la stratégie de commutation de contenu. Ces étapes utilisent le nom Connector_Requests.

   b) Entrez l'expression :

```
HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerFQDN") && (
    HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/
    sp/"))
```

Veillez à remplacer « StorageZonesControllerFQDN » par le FQDN de votre contrôleur.

c) Cliquez sur **OK**.

4. Créez un serveur virtuel de commutation de contenu.
5. Définissez les objectifs de la politique de changement de contenu :
   - Dans la boîte de dialogue Configurer le serveur virtuel (commutation de contenu), pour la politique Data_Requests, spécifiez le serveur virtuel d'équilibrage de charge pour les zones de stockage des données ShareFile.

     Ce serveur virtuel d'équilibrage de charge est celui qui applique la politique de réponse à l'étape 4 afin de vérifier la validité des signatures URI sur tous les messages entrants et d'équilibrer la charge.
   - Pour la politique Connector_Requests, spécifiez le serveur virtuel d'équilibrage de charge pour les connecteurs de zone de stockage.
6. Configurez le serveur virtuel d'authentification pour le Storage Zone Controller :

   Bien que l'authentification auprès de Citrix ADC soit facultative, il s'agit d'une bonne pratique recommandée.

   a) Dans le volet de navigation, développez l'équilibrage de charge, sélectionnez le nom du serveur virtuel d'équilibrage de charge pour les connecteurs StorageZones, puis cliquez sur Ouvrir.

   b) Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), cliquez sur l'onglet Avancé, puis développez les paramètres d'authentification.

   c) Cochez la case pour l'authentification basée sur 401, puis choisissez le serveur virtuel d'authentification.

   d) Cliquez sur l'onglet **Méthode et persistance** .

   e) Pour Persistence, choisissez **COOKIEINSERT**.

   f) Pour Délai d'expiration (min), entrez **240**.

      Une valeur de délai d'attente de 240 minutes est recommandée. Utilisez une valeur minimale supérieure à 10 minutes.

      Pour plus d'informations, voir Configuration du serveur virtuel d'authentification.

7. Utilisez la boîte de dialogue Configurer le serveur d'authentification pour créer et configurer un serveur d'authentification.

   Dans Attribut de nom SSO, entrez **UserPrincipalName**.

   Pour plus d'informations sur les autres paramètres, consultez la sectionPolitiques d'authentification.

8. Configurez une politique d'authentification pour le serveur d'authentification :

   a) Dans la boîte de dialogue Configurer la stratégie d'authentification : entrez un nom pour la stratégie, puis sélectionnez le serveur d'authentification configuré à l'étape précédente.

   b) Entrez l'expression :

   ```
   ns_true
   ```

   Pour plus d'informations, voir Configurer une politique d'authentification.

9. Configurez un profil de session pour l'authentification unique :

   a) Dans la boîte de dialogue Configurer le profil de session, entrez le nom du profil.
   b) Cochez la case pour l'authentification unique aux applications Web.
   c) Pour Credential Index, sélectionnez **PRIMARY**.
   d) Dans le domaine d'authentification unique, entrez le nom de domaine de votre contrôleur de zones de stockage.
   e) Cochez les cases **Ignorer le global** pour chacun des trois éléments précédents.

   Pour plus d'informations, consultez la section Profils de session.

10. Configurez une politique de session pour l'authentification unique :

    a) Dans la boîte de dialogue Configurer la politique de session, entrez le nom de la stratégie.

    b) Pour Profil de demande, sélectionnez le nom du profil de session configuré à l'étape précédente.

    c) Entrez l'expression :

    ```
    ns_true
    ```

    Pour plus d'informations, voir Politiques de session.

11. Créez un serveur virtuel d'authentification :

    a) Dans la boîte de dialogue Configurer le serveur virtuel (authentification), entrez le nom et l'adresse IP du serveur.
    b) Cliquez sur l'onglet Authentification et dans Protocole, sélectionnez **SSL**.
    c) Cochez la case Authentifier les utilisateurs.

d) Sous Stratégies d'authentification, cliquez sur **Principal**, puis choisissez la politique d'authentification que vous avez configurée à l'étape 7.
e) Cliquez sur l'onglet Politiques, cliquez sur **Session**, puis choisissez la politique de session que vous avez configurée à l'étape 9.

Pour plus d'informations, voir Configuration du serveur virtuel d'authentification.

## Création d'un partage réseau pour le stockage de données privées

October 13, 2020

Les zones de stockage pour ShareFile Data nécessitent un partage réseau pour vos données privées. Lorsque plusieurs StorageZones Controller sont configurés pour une haute disponibilité et un équilibrage de charge au sein d'une zone, tous les contrôleurs accèdent au même emplacement partagé pour les données privées.

Même si vous stockez des fichiers ShareFile dans un système de stockage tiers pris en charge, le StorageZones Controller nécessite un partage réseau pour les clés de chiffrement, les fichiers en file d'attente, d'autres éléments temporaires et un cache de stockage pour les téléchargements de fichiers vers ce système de stockage ou les téléchargements à partir de ce système de stockage. Pour plus d'informations sur le cache de stockage, reportez-vous à la section Personnaliser les opérations de mémoire cache.

Les contrôleurs de zone de stockage accèdent à un partage réseau à l'aide de l'utilisateur de pool de comptes IIS. Par défaut, les pools d'applications fonctionnent sous le compte d'utilisateur Service réseau, qui dispose de droits d'utilisateur de bas niveau. StorageZones Controller utilise le compte de service réseau par défaut. Vous pouvez utiliser un compte d'utilisateur nommé au lieu du compte de service réseau pour accéder au partage. Utilisez le compte de service réseau pour exécuter le pool d'applications IIS et Citrix ShareFile Services.

1. Si vous souhaitez utiliser un compte d'utilisateur nommé au lieu du compte de service réseau pour accéder au partage, créez un compte d'utilisateur nommé dans Active Directory. Nous désignerons ce compte d'utilisateur nommé en tant que compte de service ShareFile.
   Remarque : Lorsque vous configurez le StorageZones Controller, vous spécifiez le nom d'utilisateur de partage réseau et le mot de passe de partage réseau, qui sont les informations d'identification du compte que vous utiliserez pour accéder au partage, soit le compte de service ShareFile ou le compte de service réseau.

   Pour améliorer la sécurité, l'administrateur doit refuser les autorisations à tous les autres utilisateurs sur le dossier particulier contenant le référentiel de stockage ShareFile et n'accorder l'accès qu'à l'utilisateur de l'emplacement de stockage en cours de configuration.

2. Connectez-vous au serveur qui hébergera le partage réseau et créez un dossier pour vos données privées ShareFile.
3. Cliquez avec le bouton droit sur le dossier et choisissez Partager avec des personnes spécifiques …
4. Ajoutez le compte que vous utiliserez pour accéder au partage (compte de service réseau ou compte de service ShareFile) et modifiez le niveau d'autorisation en lecture/écriture.
5. Cliquez sur Partager, puis sur Terminé.
6. Cliquez avec le bouton droit sur le dossier et choisissez Propriétés.
7. Sous l'onglet Sécurité, vérifiez que le compte que vous allez utiliser pour accéder au partage (compte de service réseau ou compte de service ShareFile) dispose d'autorisations d'accès complet.

## Augmenter le nombre de fichiers par zone

Par défaut, un Controller de zones de stockage est configuré pour utiliser un partage CIFS pour stocker des fichiers dans une hiérarchie de dossiers au lieu d'un seul dossier.

Vous pouvez configurer le StorageZones Controller pour diviser la disposition de stockage persistante. Cela augmente le nombre maximal de fichiers par zone pour certains types de baies de stockage de moins d'un demi-million à dix millions ou plus. Si vous avez besoin d'une capacité supplémentaire, vous pouvez modifier la valeur par défaut.

### Pour activer le StorageZones Controller pour stocker des fichiers dans plusieurs dossiers

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.
>
> **Remarque :**
>
> Si le contrôleur de zone de stockage a été mis à niveau, vérifiez si la valeur de la clé de Registre `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone\PathSelection is set to 1. If it is set to 0, update it to 1`.

Redémarrez IIS sur les StorageZones Controller lorsque vous avez terminé de modifier le Registre.

#### Pour augmenter le nombre maximal de dossiers

Par défaut, la disposition de stockage divisée comporte 256 dossiers de niveau supérieur, chacun contenant 256 dossiers. Cette configuration est représentée dans la clé de Registre du StorageZones Controller primaire`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone: PathSelectionParams=2,2`.

La première valeur limite le nombre de dossiers de niveau supérieur à « 16 à la puissance de 2”ou 256. La deuxième valeur limite également le nombre de dossiers enfants des dossiers de niveau supérieur à 256.

En utilisant cette même formule (16 à la puissance de N), vous pouvez déterminer les valeurs appropriées pour votre site. Par exemple, PathSelectionParams=3,4,4,4 limite le nombre de dossiers de niveau supérieur à 4096 (16 à la puissance de 3). La deuxième valeur limite le nombre de dossiers enfants des dossiers de niveau supérieur à 65536 (16 à la puissance de 4). La troisième valeur limite le nombre de dossiers enfants des dossiers de deuxième niveau à 65536, etc.

Redémarrez IIS sur les StorageZones Controller principaux et secondaires si vous avez terminé de modifier le Registre.

#### Pour supprimer des dossiers vides

Lorsque le StorageZones Controller stocke des fichiers dans plusieurs dossiers, la suppression de fichiers peut entraîner des dossiers vides. Par défaut, le StorageZones Controller supprime les dossiers vides. Le service de suppression de fichiers supprime les dossiers vides, en commençant au bas de l’arborescence et en continuant jusqu’à ce qu’il atteigne un dossier non vide.

Toutefois, certains chemins de mise à niveau peuvent ne pas mettre à jour vos paramètres. Après une mise à niveau, vérifiez que la clé suivante apparaît dans `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`:

```
<add key="DeleteEmptyFoldersAfterFileDeletion” value=“1”/>
```

Si vous devez ajouter la clé, redémarrez le service de suppression de fichiers lorsque vous avez terminé.

## Installer un certificat SSL

October 13, 2020

Si vous n’utilisez pas de certificat générique, vous devez créer une demande de signature de certificat (CSR) pour le serveur de StorageZones Controller et soumettre votre demande à une autorité de certification (CA). Pour obtenir de l’aide, consultez la documentation de votre autorité de certification.

Procédez comme suit pour installer un certificat.

1. Sur le serveur du StorageZones Controller, ouvrez MMC, puis choisissez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.
2. Sélectionnez Certificats, puis cliquez sur **Ajouter**.
3. Sélectionnez Compte d'ordinateur, cliquez sur **Suivant**, cliquez sur **Terminer**, puis sur **OK**.
4. Dans la console MMC, développez **Certificats > Personnel**.
5. Cliquez avec le bouton droit sur **Certificats**, choisissez **Toutes les tâches > Importer**, puis cliquez sur **Suivant**.
6. Cliquez sur **Parcourir, puis dans** le menu d'extension de nom de fichier, choisissez **Échange d'informations personnelles**.
7. Accédez à l'emplacement du certificat, puis cliquez sur **Ouvrir**.
8. Cliquez sur **Suivant**, entrez le **mot de passe** associé à votre clé privée, cliquez deux fois sur **Suivant**, puis cliquez sur **Terminer**.
9. Lorsque le message **Importer a réussi** s'affiche, cliquez sur **OK**.

Pour un certificat public, assurez-vous que le domaine qu'il est émis pour résout à l'adresse IP locale du StorageZones Controller. Pour ce faire, mettez à jour le fichier hosts sur le StorageZones Controller pour mapper le domaine associé au certificat à l'adresse IP du StorageZones Controller. Si les deux adresses ne résolvent pas, les utilisateurs ne seront pas en mesure de télécharger des fichiers à partir du StorageZones Controller.

## Préparer votre serveur pour les données ShareFile

November 15, 2023

Le rôle de serveur Web (IIS) et la configuration d'ASP.NET décrits dans cette section sont obligatoires pour les zones de stockage pour les données ShareFile et pour les connecteurs de zone de stockage. Ces instructions sont basées sur Windows Server 2012 mais sont également valables pour les versions ultérieures.

### Mettre à jour la version Microsoft .NET

Avant de procéder à l'installation du StorageZones Controller, assurez-vous d'utiliser la version appropriée de Microsoft .NET Framework.

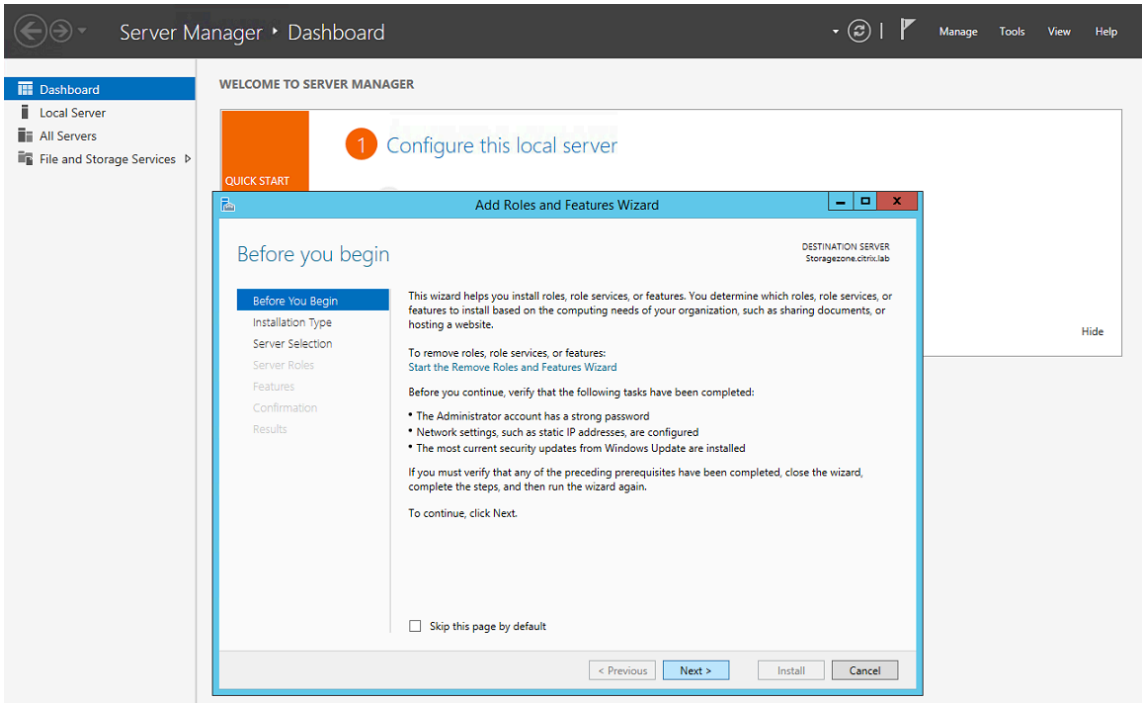
- **StorageZones Controller 5.x nécessite .NET 4.8 ou version ultérieure**. Cliquez ici pour télécharger .NET 4.8

ShareFile recommande d'utiliser la dernière version de Microsoft .NET lors de l'utilisation des applications ShareFile.

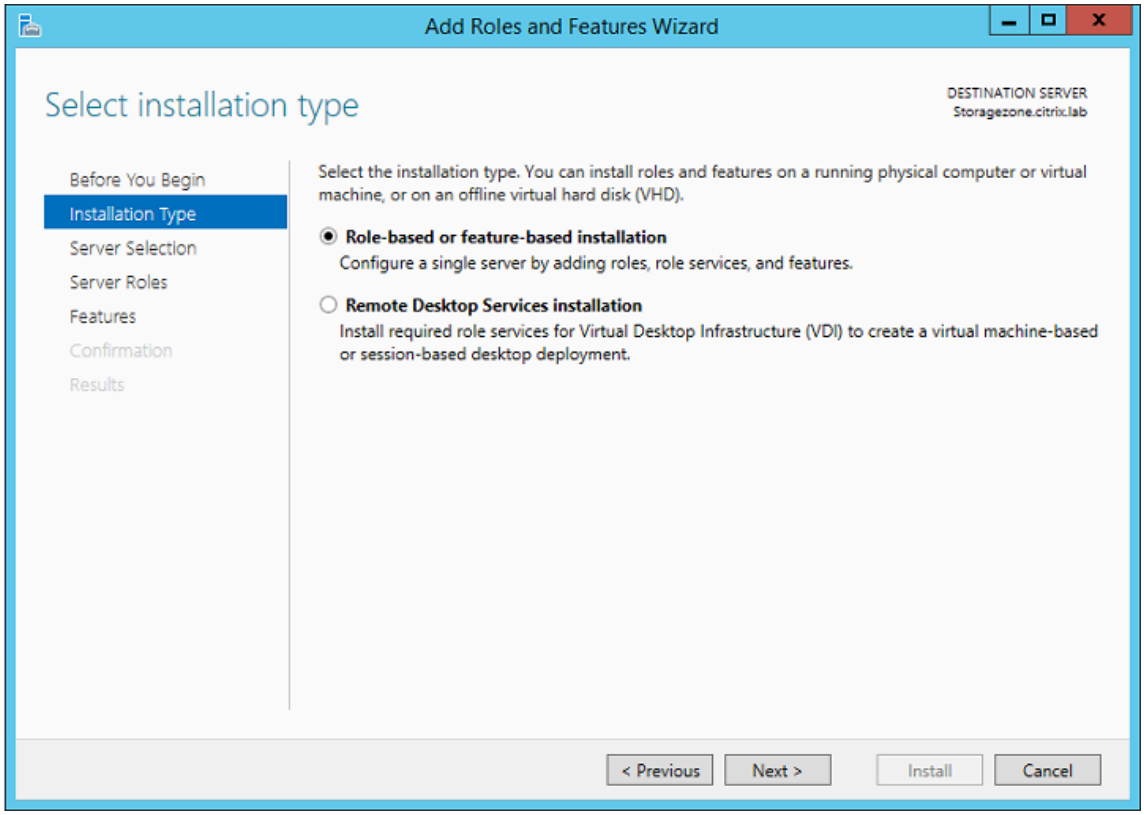
### Pour activer le rôle de serveur Web (IIS) et le service de rôle ASP.NET

1. Sur le serveur sur lequel vous installez le StorageZones Controller, connectez-vous avec un compte doté de privilèges d'administrateur local.
2. Ouvrez le tableau de bord de la console Server Manager, puis cliquez sur **Gérer > Ajouter des rôles et des fonctionnalités** pour ouvrir l'assistant d'ajout de rôles et de fonctionnalités.
3. Dans l'assistant d'ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.



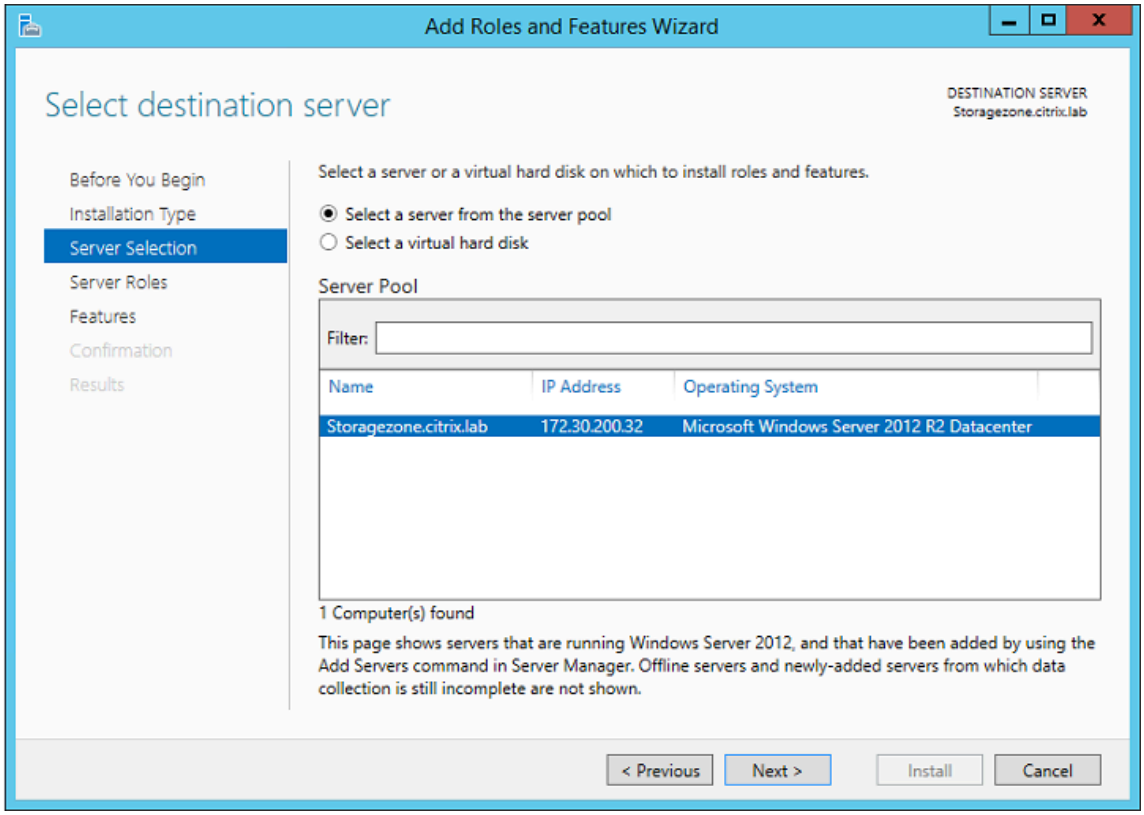

4. **Sur la page Sélectionner le type d'installation, cliquez sur Installation basée sur les rôles ou les fonctionnalités, puis sur Suivant.**



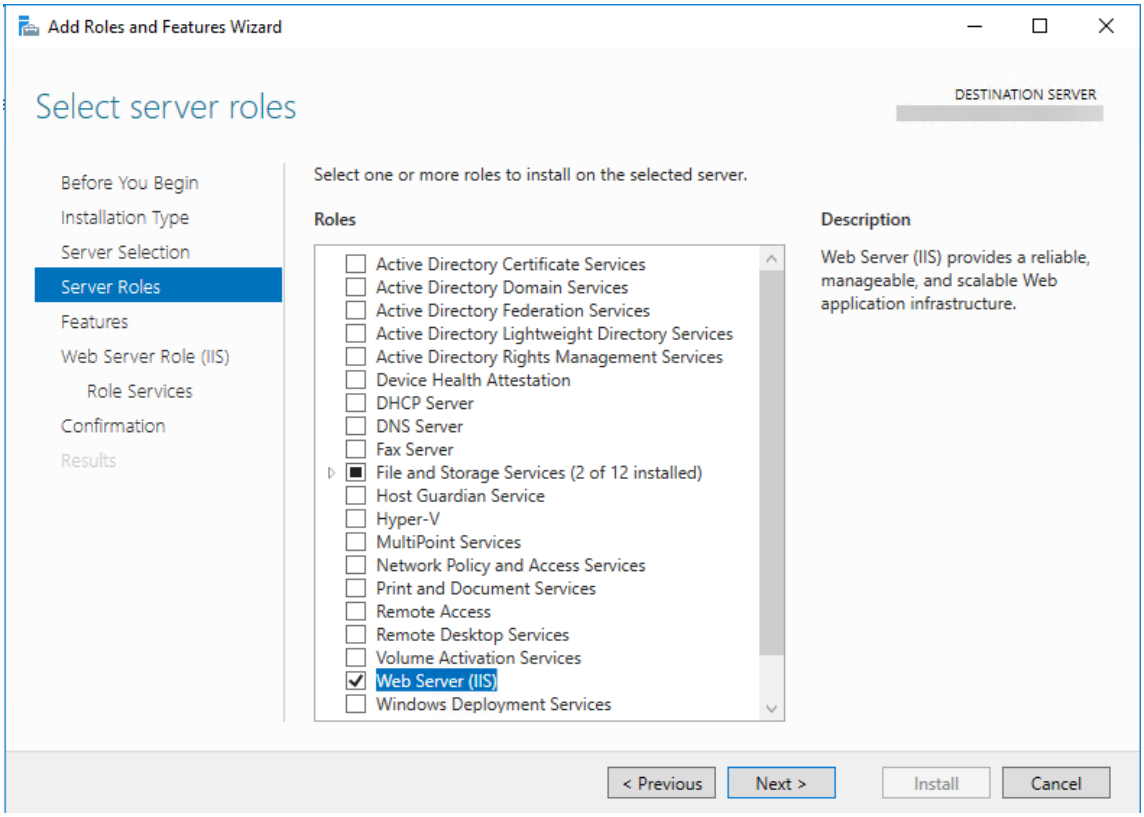

5. Sur la page Sélectionner le serveur de destination, choisissez votre serveur dans le pool de serveurs, puis cliquez sur **Suivant**.

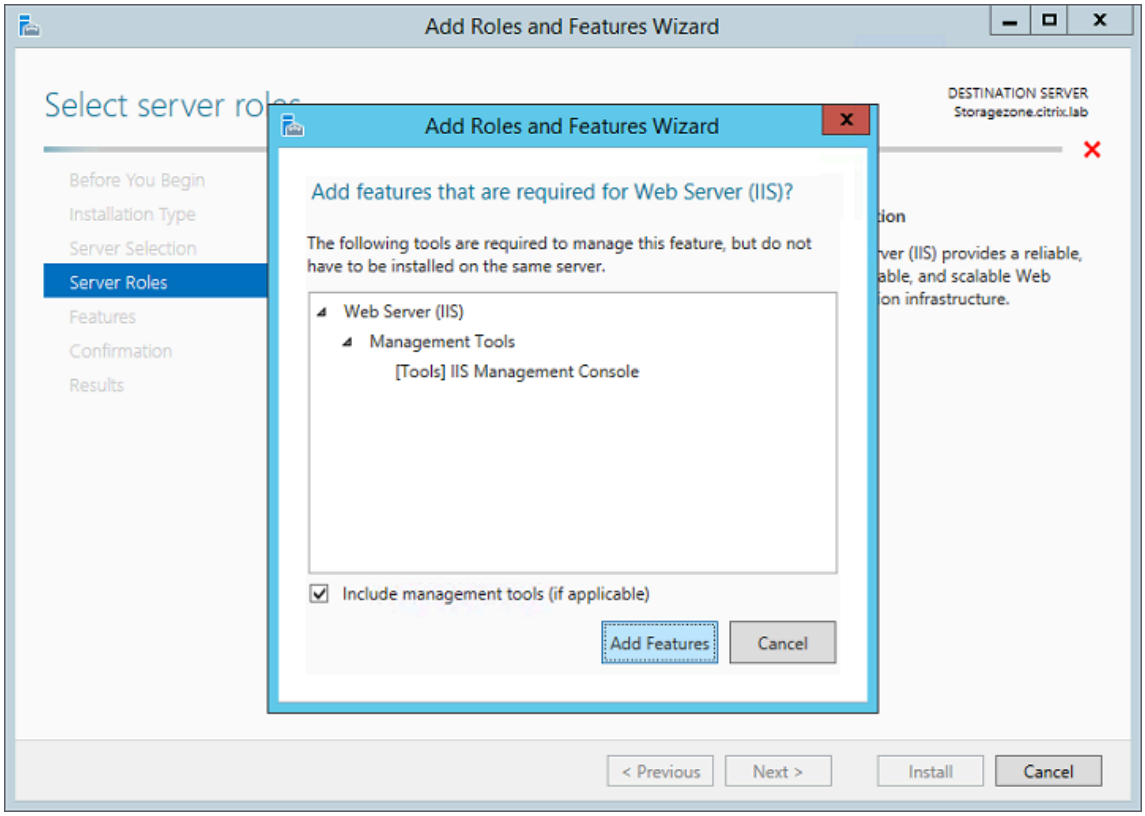



6. Sur la page Sélectionner les rôles de serveur, cochez la case Serveur Web (IIS), puis cliquez sur **Suivant**.

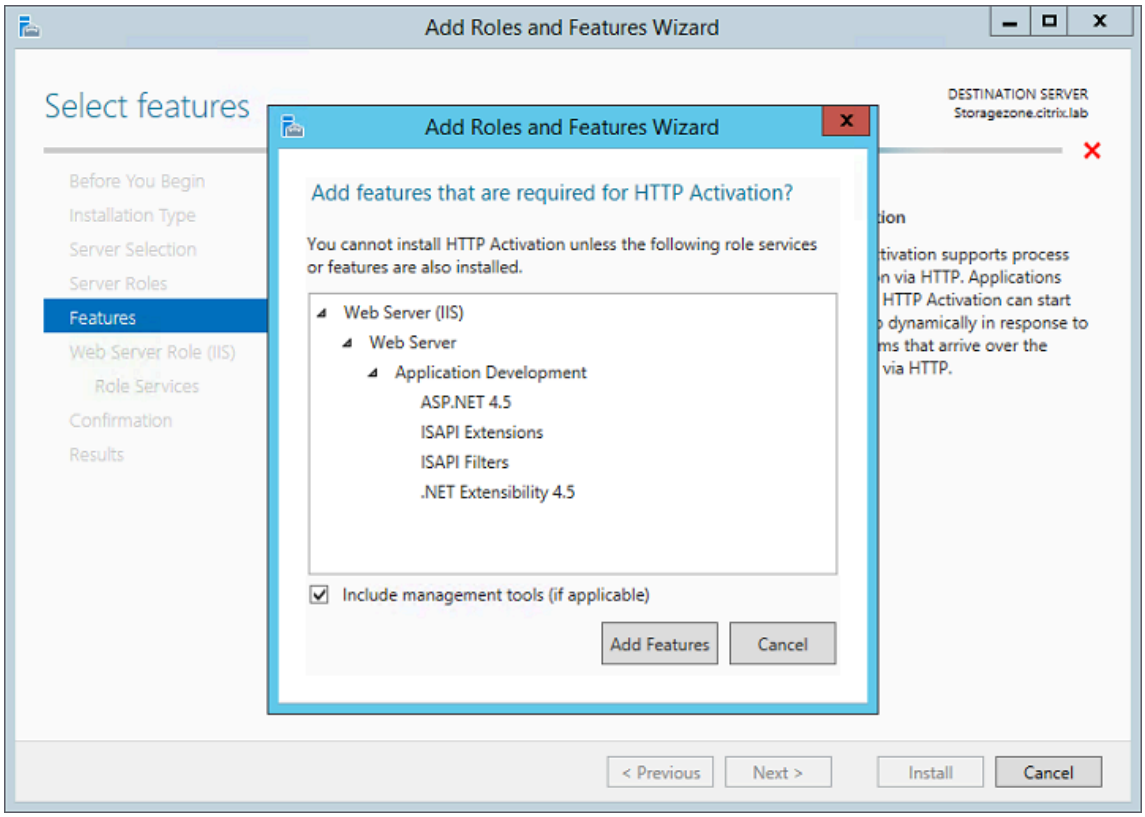



7. Cliquez sur **Ajouter des fonctionnalités** pour ajouter les fonctionnalités requises pour IIS.



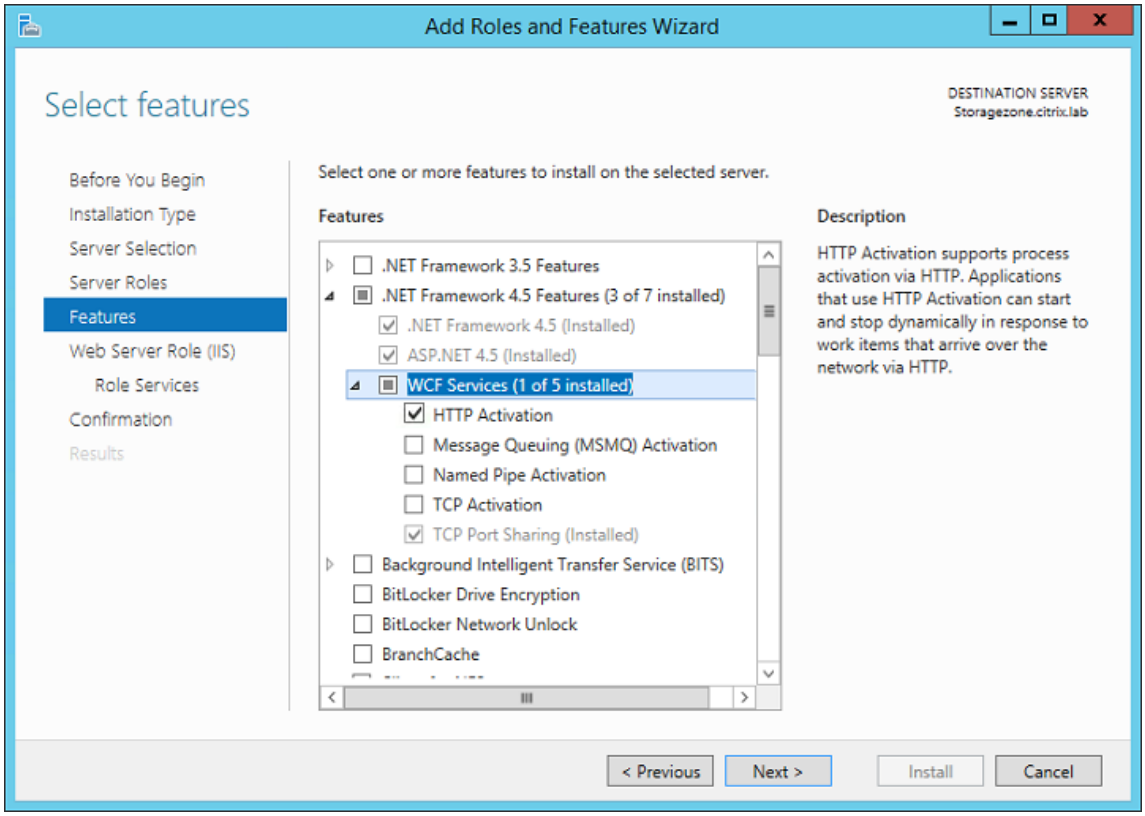

 

8. Cliquez sur **Ajouter des fonctionnalités**. La page Sélectionner les fonctionnalités s'affiche.



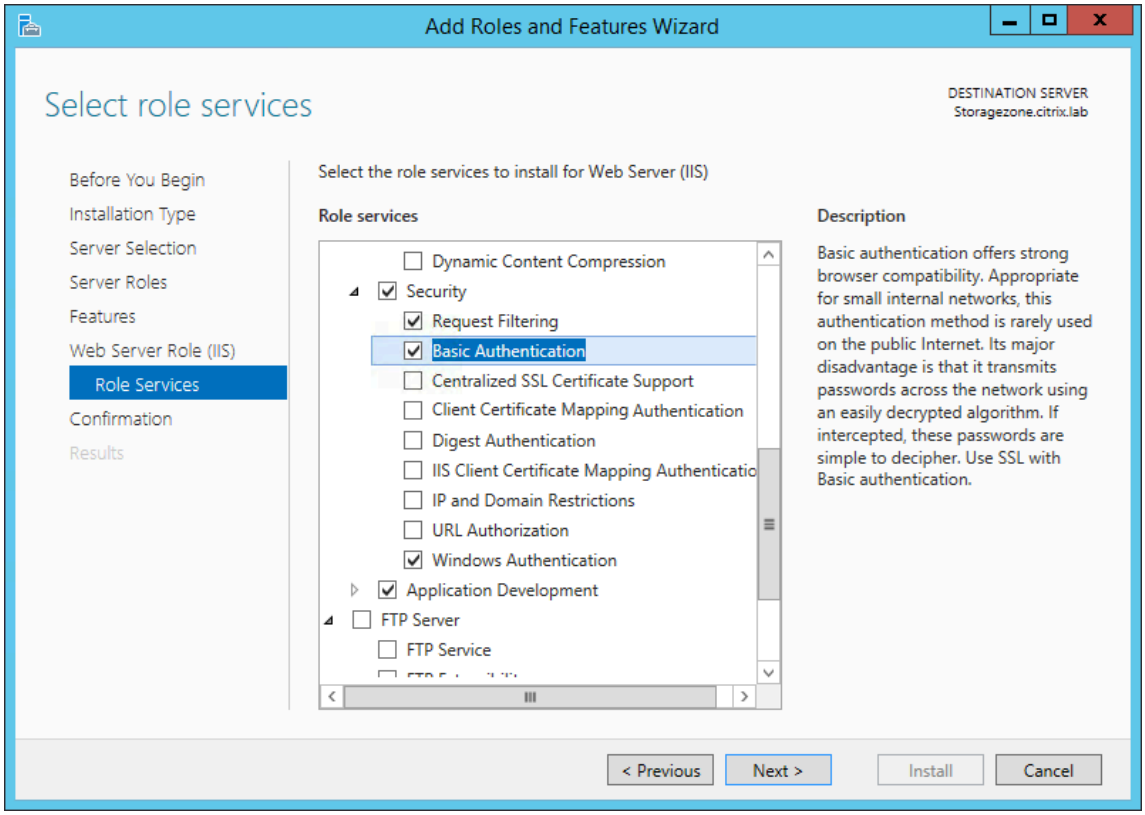

9. Sélectionnez les paramètres requis affichés dans l'écran suivant, puis cliquez sur **Suivant**.




10. Sur la page Rôle de serveur Web (IIS), cliquez sur **Suivant**.
11. Sur la page Sélectionner les services de rôle, cochez les cases Authentification de base et Authentification Windows, puis cliquez sur **Suivant**.



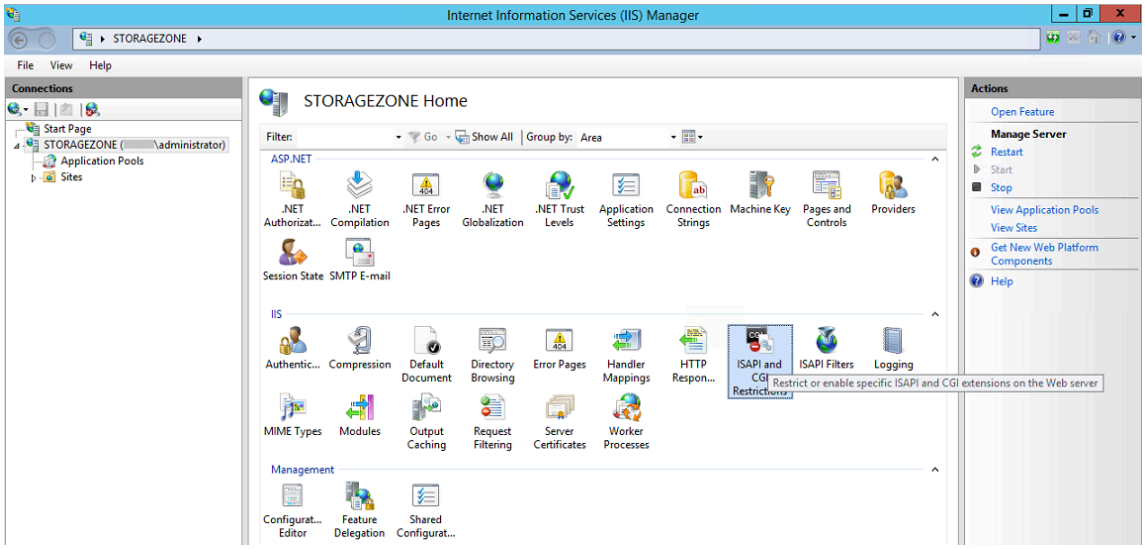

12. Sur la page Confirmer les sélections d'installation, cliquez sur **Installer**.
13. Lorsque l'installation est terminée, cliquez sur **Fermer**, puis redémarrez le serveur.

### Pour configurer IIS

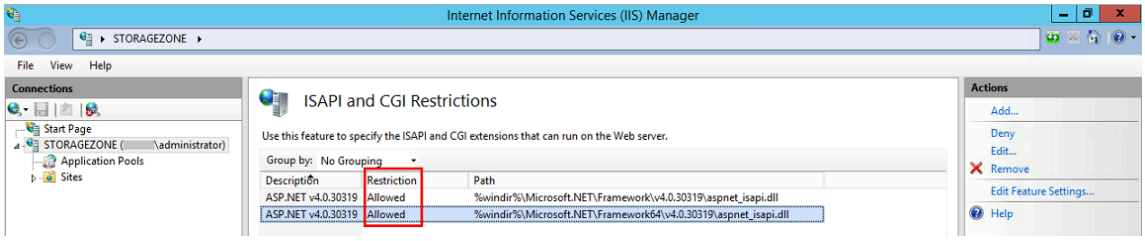
Après avoir activé le rôle de serveur Web (IIS) et le service de rôle ASP.NET, configurez IIS.

1. Ouvrez la console du gestionnaire IIS, cliquez sur le nœud du serveur StorageZone Controller, puis double-cliquez sur Restrictions ISAPI et CGI.

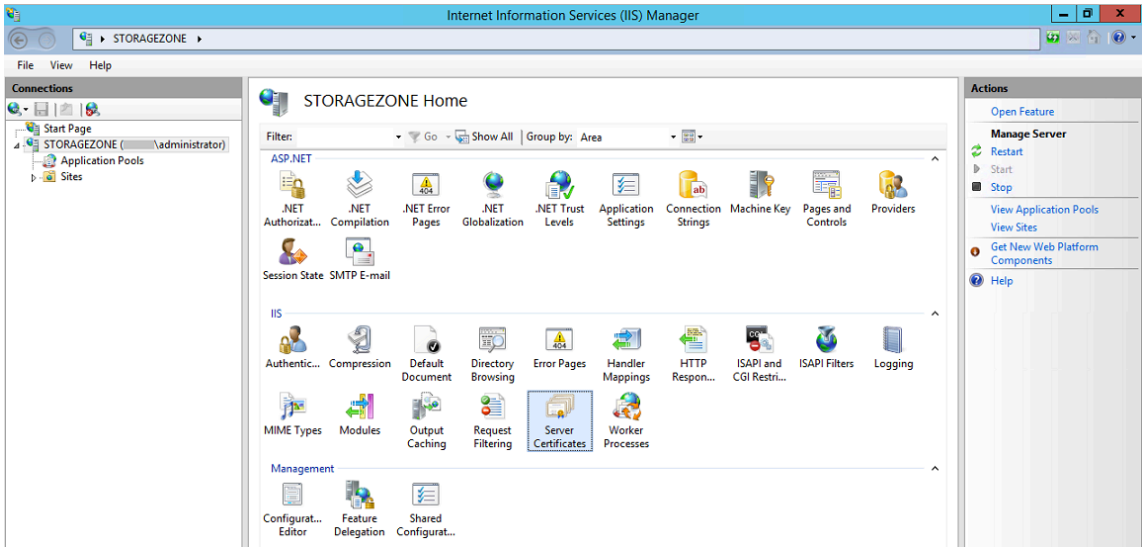
 




2. Définissez chaque entrée ASP.NET sur Autorisée.




3. Vérifiez qu'un serveur de domaine ou un certificat public est installé sur le serveur : dans la console du gestionnaire IIS, cliquez sur le nœud du serveur StorageZone Controller, puis double-cliquez sur Certificats de serveur.

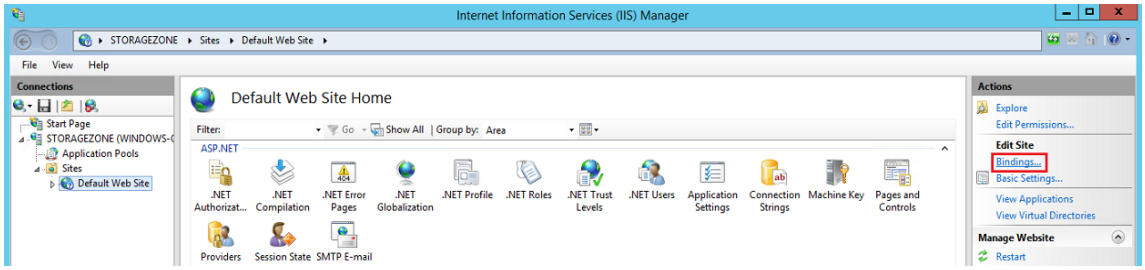



Si aucun certificat n'est associé à une autorité de certification publique, installez un certificat sur le serveur avant de continuer. Pour plus d'informations, consultez la section Installation d'un certificat SSL.

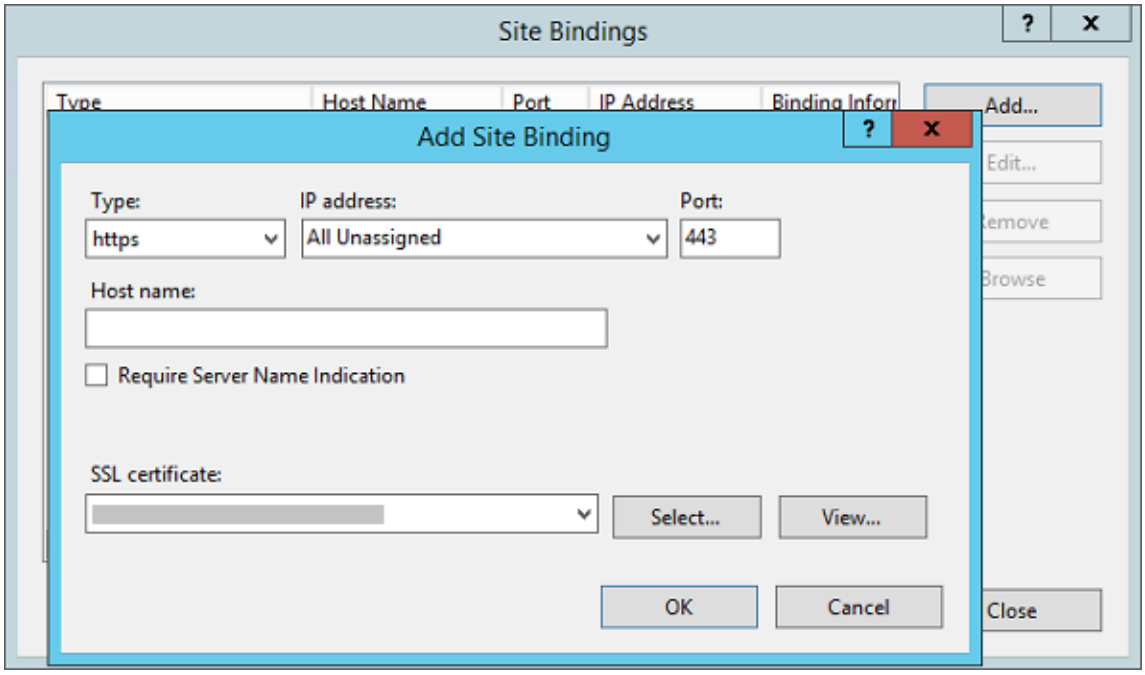
> **Remarque :**
>
> Si vous utilisez une appliance Citrix Gateway ou similaire avec StorageZones Controller, vous pouvez utiliser un certificat de serveur de domaine. Tout le trafic Internet pour les zones standard doit être géré à l'aide d'un certificat public.

4. Dans la console du gestionnaire IIS, cliquez sur **Site Web par défaut**, puis sur **Liaisons**.




5. Cliquez sur Ajouter et configurez la liaison au site comme suit :

   - Le type est https.
   - L'adresse IP est entièrement non attribuée.
   - Le port est 443.
   - Le certificat SSL est le certificat que vous avez installé.




6. Pour tester la connexion au serveur Web, accédez à `http://localhost/` et à `https://localhost/`. Si la connexion est établie, le logo IIS s'affiche.

   HTTPS affiche un message indiquant que le certificat ne correspond pas au nom de l'hôte local dans l'en-tête de l'URL. Cela est normal et vous pouvez continuer à accéder au site Web en toute

sécurité.

7. Si vous installez le StorageZones Controller sur une machine virtuelle, prenez un instantané de la machine virtuelle.

> **REMARQUE :**
>
> Le Storage Zones Controller utilise CORS et nécessite l'activation du verbe HTTP **OPTIONS** . Vérifiez la fonctionnalité de filtrage des requêtes IIS pour vous assurer que le verbe **OPTIONS** n'est pas désactivé.

## Installer StorageZones Controller et créer une zone de stockage

March 17, 2024

> **Important :**
>
> - Vérifiez que votre environnement répond à la configuration requise avant de démarrer l'installation.
> - Le contrôleur de zones de stockage ShareFile utilise des mots de passe spécifiques à l'application. Pour plus d'informations, voir Création d'un mot de passe spécifique à l'application.

Lorsque vous installez un StorageZones Controller, vous créez une zone et configurez un StorageZones Controller principal ou vous
associez des StorageZones Controller secondaires à une zone.

Lors de la configuration d'un StorageZones Controller principal, vous pouvez activer l'une des fonctionnalités suivantes ou les deux :

- Zones de stockage pour ShareFile Data, afin de spécifier un stockage de données privé, qu'il s'agisse d'un partage réseau privé ou d'un système de stockage tiers pris en charge.
- Connecteurs de zone de stockage, pour permettre aux utilisateurs d'accéder à des documents sur des sites SharePoint ou des partages de fichiers réseau spécifiés.

Les étapes suivantes décrivent comment installer le StorageZones Controller, configurer l'authentification pour le site Web IIS par défaut, créer une zone et activer les fonctionnalités.

1. Téléchargez et installez le logiciel du StorageZones Controller :
   - Sur la page de téléchargement de ShareFile à l'adresse https://dl.sharefile.com/storagezone-controller, connectez-vous et téléchargez le dernier programme d'installation du StorageZones Controller.

> **Remarque :**
>
> Lors de l'installation du StorageZones Controller, le site Web par défaut du serveur est remplacé par le chemin d'installation du contrôleur.

**L'authentification anonyme** doit être activée sur le site Web par défaut.

2. Sur le serveur sur lequel vous souhaitez installer le StorageZones Controller, exécutez StorageCenter.msi.
   - L'assistant de configuration du contrôleur de zones de stockage ShareFile démarre.
   - Pour le multitenant, exécutez la commande suivante : ***msiexec***/i StorageCenter_5.0.1.msi MULTITENANT=1

   > **Remarque :**
   >
   > Dans la commande précédente, vous devrez peut-être mettre à jour le numéro de version (5.0.1 dans l'exemple) pour qu'il corresponde au numéro de msi que vous essayez d'installer.

   - Répondez aux invites. Une fois l'installation terminée, désactivez la case à cocher correspondant à la **page de configuration du Launch StorageZones Controller**, puis cliquez sur **Terminer**.
3. Redémarrez le StorageZones Controller.
4. Pour vérifier que l'installation est réussie, accédez à `http://localhost/`. Si l'installation est réussie, le logo de ShareFile s'affiche.
5. Si le logo de ShareFile n'apparaît pas, désactivez le cache du navigateur et essayez à nouveau.

   > **Important :**
   >
   > Si vous prévoyez de cloner le StorageZones Controller, capturez l'image de disque avant de procéder à la configuration du StorageZones Controller.

6. Pour utiliser un fournisseur de stockage compatible S3 avec ShareFile, effectuez les étapes suivantes avant de créer ou de configurer une zone de stockage.
   - Ouvrez l'Éditeur du Registre Windows (**Exécuter > regedit.exe**).
   - Recherchez la clé de registre HKEY_LOCAL_MACHINE \ SOFTWARE \ Wow6432Node \ Citrix \ StorageCenter.
   - Créez une nouvelle valeur REG_SZ sous cette clé :
     - Nom de la valeur : **S3EndPointAddress**
     - Type de valeur : **REG_SZ**

  - Données de valeur : entrez l'URL HTTPS qui correspond à votre point de terminaison de stockage compatible S3.

- Si le fournisseur de stockage ne prend en charge que l'accès aux conteneurs de type chemin (voir http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html), créez une autre valeur sous cette clé.
  - Nom de la valeur : **S3ForcePathStyle**
  - Type de valeur : **REG_SZ**
  - Données de valeur : **true**

- Redémarrez le pool d'applications StorageZones Controller (StorageCenterAppPool).
- Recueillez les informations suivantes à partir de votre système de stockage compatible S3 :
  - Le nom d'un compartiment S3 à utiliser pour l'ID de clé ShareFile DataAccess
  - ID de clé d'accès
  - Clé d'accès secrète

7. Procédez comme suit pour créer une nouvelle zone de stockage. Choisissez Amazon S3 comme emplacement de stockage persistant. StorageZones Controller utilise l'adresse de point de terminaison personnalisée que vous avez saisie au lieu du service Amazon S3 proprement dit. Lors de la configuration des détails S3, choisissez le nom du compartiment que vous avez créé précédemment.
8. Accédez à la console StorageZones Controller.
9. Ouvrez `http://localhost/configservice/login.aspx` ou démarrez l'outil de configuration depuis l'écran ou le menu Démarrer. Pour plus d'informations sur l'utilisation du raccourci de l'écran d'accueil dans Windows 8, voir Gérer les StorageZones Controller.
10. Sur la page d'ouverture de **session du StorageZones Controller**, entrez l'**adresse e-mail**, le **mot de passe** et le sous-domaine **complet du sous-domaine FQDN de l'URL du compte**, tel que `subdomain.sharefile.com` ou `subdomain.sharefile.eu`, pour votre compte. Cliquez sur **Ouvrir une session**.
11. Pour configurer votre StorageZones Controller principal, cliquez sur **Créer une nouvelle zone** et fournissez les informations de zone :

| Option | Description |
|---|---|
| Zone | Nom qui apparaît dans la console ShareFile Administrator. |

| Option | Description |
| --- | --- |
| Contrôleur de zone principal | Valeur par défaut `http://localhost/ConfigService`. Si vous utilisez le protocole SSL, remplacez HTTP par https. N'oubliez pas que ShareFile ne prend en charge que les certificats SSL publics valides et fiables pour les zones standard. Si vous rencontrez des problèmes lors de la configuration d'un hôte de zone de stockage secondaire, assurez-vous de pouvoir résoudre l'URL ConfigService dans un navigateur local sur ce serveur, sans erreur SSL. localhost renvoie l'adresse IP du serveur. Vous pouvez spécifier un nom de serveur à la place (par exemple `https://servername.subdomain.com/ConfigService`). Le nom du serveur doit pouvoir être résolu par un serveur StorageZones Controller secondaire. |
| Nom d'hôte | Identifiant unique pour votre StorageZones Controller. ShareFile vous recommande d'utiliser le nom d'hôte du serveur comme identifiant. Il doit s'agir d'un nom convivial et non du nom de domaine complet. Ce nom apparaît dans la console ShareFile Administrator. |
| Adresse externe | Le nom de domaine complet de ce StorageZones Controller. Si ce StorageZones Controller doit être utilisé pour les zones standard, l'URL doit être accessible depuis Internet. Si vous utilisez un équilibreur de charge, entrez son adresse. Lorsque vous soumettez la page, ShareFile valide l'adresse. |

12. Pour spécifier un stockage de données privé, procédez comme suit.
    - Cochez la case **Activer les zones de stockage pour les données ShareFile**.
    - Pour configurer une zone standard, désactivez la case à cocher.

> **Remarque :**
>
> Une fois que vous avez configuré un StorageZones Controller, vous ne pouvez pas modifier son type de zone.

Le StorageZones Controller utilise les informations d'identification du compte de service pour se connecter au serveur de domaine Active Directory approuvé afin de rechercher une adresse e-mail.

- Choisissez un référentiel de stockage.

13. Si vous ne souhaitez pas activer les StorageZone Connectors, cliquez sur **Enregistrer pour enregistrer** StorageZones Controller auprès de ShareFile, puis passez à l'étape 14.
14. Si vous utilisez un stockage compatible S3, créez ces entrées de registre supplémentaires après les registres de la zone de stockage :
    - Ouvrez l'Éditeur du Registre Windows (**Exécuter > regedit.exe**).
    - Trouvez la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storage zone\CloudStorageUploaderConfig`.
    - Créez une nouvelle valeur REG_SZ sous cette clé :
      - Nom de la valeur : **S3EndPointAddress**
      - Type de valeur : **REG_SZ**
      - Données de valeur : entrez l'URL HTTPS qui correspond à votre point de terminaison de stockage compatible S3.
    - Si le fournisseur de stockage ne prend en charge que l'accès aux conteneurs de type chemin (voir http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html), créez une autre valeur sous cette clé.
      - Nom de la valeur : **S3ForcePathStyle**
      - Type de valeur : **REG_SZ**
      - Données de valeur : **true**
    - Redémarrez le pool d'applications StorageZones Controller (StorageCenterAppPool).
15. Pour activer les connecteurs StorageZone, procédez comme suit :

    L'activation des connecteurs crée les applications IIS « cifs » (connecteur pour les partages de fichiers réseau) et « sp » (connecteur pour SharePoint).

    - Cochez la case correspondant à chaque type de connecteur que vous souhaitez utiliser : Activer le connecteur de zone de stockage pour les partages de fichiers réseau et Activer le connecteur de zone de stockage pour SharePoint. Pour plus d'informations sur les

paramètres du connecteur, consultez la section Configuration des connecteurs de zone de stockagedans cette section.

- Cliquez sur **Enregistrer**. Les informations relatives à votre StorageZones Controller apparaissent.
- Si vous avez spécifié **des chemins autorisés ou des chemins refusés** pour les connecteurs de zone de stockage, redémarrez le serveur IIS.

16. Pour configurer les StorageZones Controller secondaires, reportez-vous à la section Gérer les StorageZones Controller.

> **Important :**
>
> Un StorageZones Controller est installé sur votre site local et vous êtes responsable de sa sauvegarde. Pour protéger votre déploiement, vous devez prendre un instantané du serveur StorageZones Controller, sauvegarder la configuration du StorageZones Controlleret préparer StorageZones Controller pour la reprise après sinistre.

## Configuration des zones de stockage pour ShareFile Data

> **Remarque :**
>
> Les zones de stockage pour les données ShareFile sont disponibles pour Citrix Endpoint Management Enterprise Edition et ne sont pas disponibles pour les autres éditions de Citrix Endpoint Management.

Vous pouvez configurer des zones de stockage pour ShareFile Data depuis l'assistant StorageZones Controller lorsque vous créez une zone de stockage ou depuis la console StorageZones Controller. Utilisez l'onglet ShareFile Data pour configurer les paramètres des partages réseau privés ou des systèmes de stockage tiers pris en charge.

### Paramètres de partage réseau

| Option | Description |
|---|---|
| Dépôt de stockage | Choisissez Partage réseau local. Après avoir créé la zone, vous ne pouvez pas modifier l'option Référentiel de stockage. Par exemple, pour passer d'un partage réseau local à un stockage tiers, vous devez créer une nouvelle zone. |

| Option | Description |
| --- | --- |
| Emplacement du partage réseau | Le chemin UNC vers le partage réseau que vous utiliserez pour le stockage de données privées et pour des données telles que les clés de chiffrement, les fichiers en file d'attente et d'autres éléments temporaires. Spécifiez le chemin dans le formulaire `\\server\share`. Les contrôleurs de zones de stockage appartenant à la même zone de stockage doivent utiliser le même partage de fichiers pour le stockage. Attention : StorageZones Controller remplacera toutes les données de ce chemin par un format de stockage propriétaire. Ne spécifiez jamais de chemin d'accès à un emplacement contenant des données de fichier. Réservez cet emplacement de stockage pour les zones de stockage pour les données ShareFile uniquement. Les contrôleurs de zones de stockage accèdent au partage réseau à l'aide du nom d'utilisateur/mot de passe de partage réseau fourni sur la page de configuration. Si aucun nom d'utilisateur/mot de passe Network Share n'est fourni sur la page de configuration, le compte Network Service sera utilisé par défaut. Le compte Network Service doit disposer d'un accès complet à cet emplacement de stockage. Le StorageZones Controller utilisera également le compte de service réseau par défaut pour le StorageCenterAppPool. Il est important de noter que la seule configuration prise en charge est l'utilisation du compte Network Service. |

| Option | Description |
| --- | --- |
| Nom d'utilisateur et mot de passe Network Share | Les informations d'identification du chemin UNC de votre emplacement de partage réseau. Pour utiliser un compte utilisateur nommé au lieu du compte de service réseau pour accéder au partage, spécifiez ces informations d'identification. Vous pouvez continuer à exécuter le pool d'applications IIS et les services ShareFile à l'aide du compte Network Service. |
| Activer le chiffrement | Cochez la case uniquement si vous souhaitez chiffrer le contenu du fichier stocké sur votre partage de fichiers. Dans un environnement d'entreprise où le partage réseau se trouve à l'intérieur de votre réseau et est déjà sécurisé par des outils tiers, nous vous recommandons de ne pas chiffrer les fichiers du partage. Ce paramètre ne concerne pas les métadonnées. Les métadonnées ne sont pas cryptées pour les zones standard. Bien que cette sécurité supplémentaire soit proposée en option pour une sécurité maximale lorsque cela est nécessaire, le chiffrement des fichiers sur le partage rendra le disque illisible par des outils tiers tels que des scanners antivirus et des outils de gestion de fichiers, y compris des outils de déduplication de données. ShareFile utilise une clé de chiffrement de fichier pour confirmer la validité des demandes de téléchargement et chiffrer le stockage. |

| Option | Description |
| --- | --- |
| Phrase secrète | Expression utilisée pour protéger votre clé de chiffrement de fichier. La phrase secrète doit contenir plus de six caractères. Veillez à archiver la phrase secrète et la clé de chiffrement dans un emplacement sécurisé. Vous devez utiliser la même phrase secrète pour chaque StorageZones Controller d'une zone. La phrase secrète n'est pas la même que le mot de passe de votre compte et ne peut pas être récupérée en cas de perte. Si vous perdez la phrase secrète, vous ne pouvez pas réinstaller des zones de stockage, joindre des StorageZones Controller supplémentaires à la zone de stockage ou récupérer la zone de stockage en cas de défaillance du serveur. Remarque : La clé de chiffrement apparaît à la racine du chemin de stockage partagé. La perte du fichier de clé de chiffrement, SCKeys.txt, interrompt immédiatement l'accès à tous les fichiers de zone de stockage. Veillez à sauvegarder le fichier de clé de chiffrement dans le cadre des procédures habituelles de votre centre de données. |

**Paramètres de configuration du cache partagé**

| Option | Description |
| --- | --- |
| Emplacement du cache partagé | le chemin d'accès à un partage réseau qui contiendra votre cache de stockage et des données telles que des clés de chiffrement, des fichiers en file d'attente et d'autres éléments temporaires. Spécifiez le chemin dans le formulaire `\\server\share`. Les contrôleurs de zones de stockage appartenant à la même zone de stockage doivent utiliser le même partage de fichiers pour le stockage. Attention : StorageZones Controller remplacera toutes les données de ce chemin par un format de stockage propriétaire. Ne spécifiez jamais de chemin d'accès à un emplacement contenant des données de fichier. Réservez cet emplacement de stockage pour les zones de stockage réservées à ShareFile Data uniquement. Le compte Network Service (ou le compte sous lequel le ShareFile Management Service est configuré pour fonctionner) doit disposer d'un accès complet à cet emplacement de stockage. |
| Connexion au cache partagé et mot de passe du cache partagé | Les informations d'identification du chemin UNC de votre emplacement de cache partagé. |
| Activer le chiffrement | Cochez la case pour chiffrer les fichiers stockés dans votre cache partagé. |

**Paramètres du conteneur de stockage Windows Azure**

| Option | Description |
| --- | --- |
| Dépôt de stockage | Choisissez Azure Storage Container. Après avoir créé la zone, vous ne pouvez pas modifier l'option Référentiel de stockage. Par exemple, pour passer d'un partage réseau local à un stockage basé sur Azure, vous devez créer une nouvelle zone. |

| Option | Description |
| --- | --- |
| Account Name | Le nom de votre compte de stockage Azure. Ces noms sont toujours en minuscules. |
| Clé d'accès | La clé d'accès principale ou secondaire pour votre stockage Azure. Copiez la clé depuis l'écran Gérer les clés d'accès du portail de gestion Windows Azure. |
| Valider | Cliquez sur le bouton pour valider la clé d'accès Azure. Vous ne pouvez pas poursuivre la configuration tant que la validation n'est pas terminée et que le menu Nom du conteneur inclut tous les conteneurs disponibles pour le compte spécifié. |
| Nom du conteneur | Sélectionnez le conteneur Azure à utiliser pour tous les StorageZones Controller de cette zone de stockage. Cette liste est vide jusqu'à ce que votre clé d'accès Azure soit validée. |

**Paramètres du compartiment de stockage Amazon S3**

| Option | Description |
| --- | --- |
| Dépôt de stockage | Choisissez le compartiment de stockage Amazon S3. Après avoir créé la zone, vous ne pouvez pas modifier l'option Référentiel de stockage. Par exemple, pour passer d'un partage réseau local à un stockage Amazon S3, vous devez créer une nouvelle zone. |
| ID de clé d'accès | L'ID de clé d'accès pour votre stockage Amazon S3. |
| Clé d'accès secret | La clé d'accès secrète pour votre espace de stockage Amazon S3. |

| Option | Description |
|---|---|
| Valider | Cliquez sur le bouton pour valider la clé d'accès secrète Amazon S3. Vous ne pouvez pas poursuivre la configuration tant que la validation n'est pas terminée et que le menu Nom du compartiment n'inclut pas tous les compartiments disponibles pour le compte spécifié. |
| Nom du compartiment | Sélectionnez le compartiment Amazon S3 à utiliser pour tous les StorageZones Controller de cette zone de stockage. Cette liste est vide jusqu'à ce que votre clé d'accès secrète Amazon S3 soit validée. |

**Paramètres SMTP**

| Option | Description |
|---|---|
| Adresse du serveur SMTP et numéro de port SMTP | Le nom d'hôte et le port de votre serveur SMTP local. |
| Utiliser le protocole SSL | Cochez la case pour vous connecter au serveur SMTP via une connexion sécurisée. |
| Nom d'utilisateur et mot de passe | Nom d'utilisateur et mot de passe de votre serveur SMTP local. |
| Mode d'authentification | Le mode d'authentification par défaut utilise la méthode la plus sécurisée disponible pour se connecter entre le StorageZones Controller et le serveur SMTP. |
| Adresse de l'expéditeur | Adresse e-mail qui apparaît dans le champ De. |

## Plateforme Google Cloud

Générez une clé d'accès et un secret depuis **Google Cloud Platform > Paramètres > Interopérabilité**.

Avant d'exécuter la configuration des zones de stockage, définissez la valeur de registre **S3EndpointAddress** sur, `https://storage.googleapis.com` puis redémarrez IIS.

Option 1

Description

Référentiel de stockage

Choisissez le **compartiment de stockage Amazon S3**. Une fois la zone créée, vous ne pouvez pas modifier l'option **Référentiel de stockage**. Par exemple, pour passer d'un partage réseau local à un stockage Amazon S3, vous devez créer une nouvelle zone.

ID de clé d'accès

L'identifiant de la clé d'accès de votre espace de stockage Google Cloud Platform.

Clé d'accès secret

Le secret de votre stockage sur Google Cloud Platform.

Valider

Cliquez sur le bouton pour valider la clé d'accès secrète de Google Cloud Platform. Vous ne pouvez pas poursuivre la configuration tant que la validation n'est pas terminée et que la liste des **noms des compartiments** inclut tous les compartiments disponibles pour le compte spécifié.

Nom du compartiment

Sélectionnez le compartiment approprié à utiliser pour tous les StorageZones Controller de cette zone de stockage. Cette liste est vide jusqu'à ce que votre clé d'accès secrète à Google Cloud Platform soit validée.

## Configuration des connecteurs de zone de stockage

Les connecteurs de zone de stockage permettent aux utilisateurs d'accéder à des documents sur des sites SharePoint ou à des partages de fichiers réseau spécifiques. Il n'est pas nécessaire d'activer les zones de stockage pour que ShareFile Data utilise les StorageZone Connectors.

> **Remarque :**
>
> Les zones de stockage pour ShareFile Data et les fonctionnalités des connecteurs StorageZones peuvent partager une zone. Cependant, StorageZones Controller sépare les données et les règles d'accès pour les deux types de données.

Vous pouvez configurer les connecteurs StorageZone lorsque vous créez une zone à l'aide de l'assistant StorageZones Controller ou de la console StorageZones Controller.

Pour contrôler l'accès à des partages de fichiers réseau ou à des bibliothèques de documents SharePoint spécifiques, spécifiez une liste de chemins autorisés ou refusés. Après avoir enregistré vos modifications, redémarrez le serveur IIS.

Les connexions entrantes aux connecteurs de zone de stockage sont d'abord vérifiées par rapport aux chemins autorisés. Si la connexion est autorisée, le chemin est ensuite comparé aux chemins refusés.

Par exemple, pour donner accès à `\\myserver\teamshare` et à tous ses sous-dossiers, spécifiez un chemin autorisé de `\\myserver\teamshare`.

- Toutes les connexions sont autorisées par défaut, comme indiqué par la valeur Allowed Paths. La valeur n'est pas valide pour les chemins refusés.
- Si les chemins autorisés et refusés entrent en conflit, le chemin le plus restrictif est appliqué.
- Les entrées sont séparées par des virgules.
- Pour les connecteurs vers des partages de fichiers réseau, spécifiez les chemins UNC autorisés.

  Exemple avec FQDN : `\\fileserver.acme.com\shared`

  Vous pouvez utiliser les variables suivantes dans le chemin UNC :

  - %Nom d'utilisateur%

    Redirige vers le répertoire personnel d'un utilisateur. Exemple de chemin : `\\myserver\homedirs\\%UserName%`

  - %HomeDrive%

    Redirige vers le chemin d'accès du dossier d'accueil d'un utilisateur, tel que défini dans la propriété Répertoire d'accueil Active Directory. Exemple de chemin : `%HomeDrive%`

  - %TSHomeDrive%

    Redirige vers le répertoire personnel des services Terminal Server d'un utilisateur, tel que défini dans la propriété Active Directory MS-TS-Home-Directory. L'emplacement est utilisé lorsqu'un utilisateur ouvre une session Windows à partir d'un serveur Terminal Server ou d'un serveur Citrix XenApp. Exemple de chemin : %TSHomeDrive%

    Dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, la valeur MS-TS-Home-Directory est accessible dans l'onglet Profil des services Remote Desktop lors de la modification d'un objet utilisateur.

  - %Domaine utilisateur%

    Redirige vers le nom de domaine NetBIOS de l'utilisateur authentifié. Par exemple, si le nom de connexion de l'utilisateur authentifié est « abc \ johnd », la variable est remplacée par « abc ». Exemple de chemin : `\\myserver%UserDomain%_%UserName%`

  Les variables ne sont pas sensibles à la casse.

- Pour un connecteur vers un site SharePoint de niveau racine, spécifiez le chemin d'accès de niveau racine.

  Exemple : `https://sharepoint.company.com`

- Pour un connecteur vers une collection de sites SharePoint :

  Exemple : `https://sharepoint.company.com/site/SiteCollection`

- Pour les connecteurs vers les bibliothèques de documents SharePoint 2010, spécifiez les URL (sans compter les terminateurs de chemin, tels que file.aspx ou /Forms).

  Exemples :

  - https://mycompany.com/sharepoint/
  - https://mycompany.com/sharepoint/sales-team/Shared Documents/
  - https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx

  L'URL par défaut de SharePoint 2013 (lorsque la stratégie de téléchargement minimale est activée) se présente sous la forme : https://sharepoint.company.com/_layouts/15/start.aspx\\#/Shared%20Documents/.

### Recommandation de sécurité pour supprimer l'en-tête du serveur

IIS/ASP.NET expose par défaut l'en-tête du serveur dans les réponses HTTP. Cet en-tête pourrait être utile à un attaquant. L'en-tête indique le type de serveur d'envoi et, dans certains cas, le numéro de version. Cet en-tête n'est pas nécessaire pour les sites de production et peut être désactivé.

Malheureusement, le programme d'installation du StorageZones Controller n'est pas en mesure de supprimer automatiquement cet en-tête. Nous pouvons toutefois recommander aux clients de supprimer cet en-tête dans notre guide de documentation/d'installation du StorageZones Controller.

Reportez-vous à l'article suivant pour connaître les étapes spécifiques que nous devons fournir dans notre documentation : https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

## Vérifier la configuration du Controller de vos zones de stockage

October 13, 2020

Vérifiez qu'un StorageZones Controller enregistré auprès de ShareFile, puis vérifiez les autres problèmes de configuration avant de continuer.

1. Dans la console du StorageZones Controller, cliquez sur l'onglet **Surveillance** .
2. Vérifiez que l'état des pulsations a une coche verte.

   Une icône rouge indique que Sharefile.com ne reçoit pas les messages de pulsation. Dans ce cas, vérifiez la connectivité réseau à partir de votre StorageZones Controller vers www.ShareFile.com et à partir d'un PC externe vers l'URL de votre StorageZones Controller.

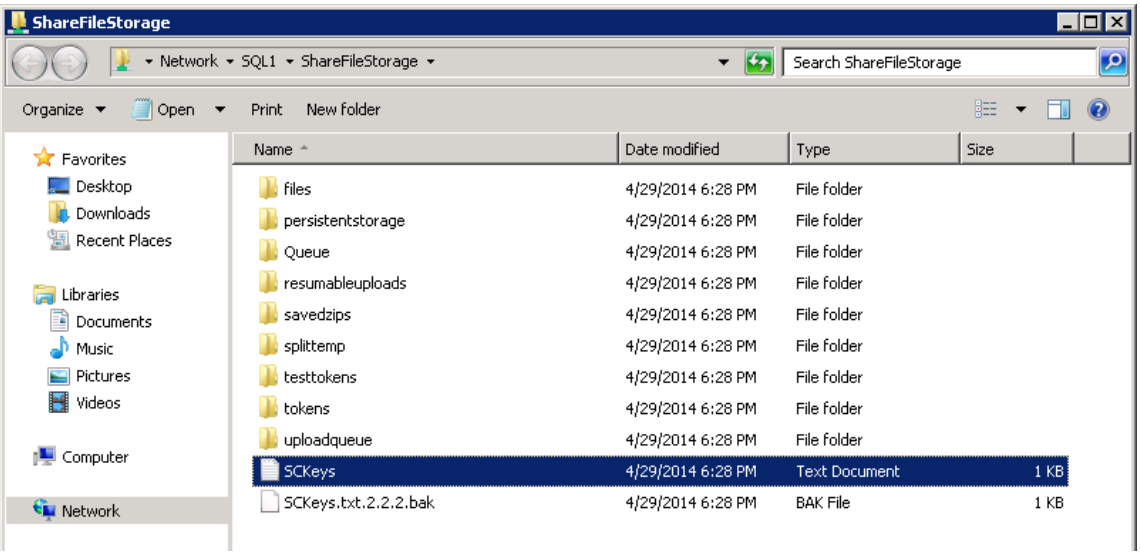
Pour les zones standard, le StorageZones Controller doit être accessible sur le port 443 avec un certificat SSL public valide et fiable.

Après une mise à niveau, l'état Connectivité ShareFile à partir des Services de nettoyage de fichiers peut afficher temporairement une icône rouge. Cela se produit si Windows démarre ce service avant que le StorageZones Controller établit une connexion réseau. L'état revient à une icône verte une fois que le serveur de Controller est de retour sur le réseau.

3. Vérifiez la connectivité à votre zone privée : accédez à l'URL externe (sous la forme de `https://server.subdomain.com`) de votre zone privée.

   Si le trafic Internet est autorisé à passer à et à partir d'un StorageZones Controller, vous verrez le logo ShareFile. Si le StorageZones Controller n'est pas configuré correctement, vous pouvez voir un logo IIS ou un écran d'ouverture de session Citrix ADC. Assurez-vous que le trafic HTTPS entrant et sortant est autorisé sur le port 443. Si votre URL externe pointe vers Citrix ADC, recherchez les accès sur le commutateur de contenu et le serveur virtuel d'équilibrage de charge pour les données. Pour plus d'informations, voir « StorageZones Controller ne charge pas les données dans ShareFile » dansRésoudre les problèmes d'installation et de configuration.

4. Vérifiez que le partage réseau que vous avez créé pour le stockage de données privées a une structure de dossier et quelques fichiers créés par le StorageZones Controller, y compris Sckeys.txt, qui doit résider dans le dossier racine du stockage partagé.




   Sckeys.txt est créé lorsque le StorageZones Controller est installé, à condition qu'il n'y ait pas d'informations d'identification ou de droits d'accès problèmes. Si Sckeys.txt n'est pas présent, vérifiez les listes de contrôle d'accès sur votre partage de fichiers, puis réinstallez le StorageZones Controller.

5. Vérifiez l'état des StorageZone Connector à partir de l'interface ShareFile :

a) Connectez-vous à votre compte ShareFile Enterprise, accédez à **Admin > Zones de stockage**et vérifiez que la colonne Santé contient une coche verte.

b) Cliquez sur le nom du site et vérifiez que le message Heartbeat indique que le StorageZones Controller répond.

6. Tester un téléchargement de fichier : connectez-vous à l'interface Web ShareFile, créez un dossier partagé affecté à la zone que vous venez de configurer, téléchargez un fichier dans ce dossier, puis vérifiez que le fichier apparaît dans le dossier.

## Modifier la zone par défaut des comptes d'utilisateurs

March 17, 2024

Par défaut, les comptes d'utilisateurs existants et nouvellement provisionnés utilisent le stockage cloud géré par ShareFile comme zone par défaut. Modifiez la zone par défaut comme suit :

- Pour spécifier la zone par défaut pour les comptes utilisateur provisionnés à partir d'AD, lors du provisionnement des utilisateurs, sélectionnez l'emplacement de stockage. Pour plus d'informations, consultez la section **Modifier les options des règles utilisateur** dans l'article Administration basée sur les politiques de ShareFile.
- Pour modifier la zone par défaut d'un utilisateur individuel, ouvrez la console d'administration de ShareFile et accédez à **Gérer les**utilisateurs.

## Spécifier un serveur proxy pour les zones de stockage

April 19, 2021

La console StorageZones Controller vous permet de spécifier un serveur proxy correspondant. Vous pouvez également spécifier un serveur proxy à l'aide d'autres méthodes.

Les contrôleurs de zones de stockage primaires et secondaires communiquent entre eux en utilisant HTTP. Si tout le trafic HTTP est configuré pour passer par un serveur proxy sortant qui ne prend pas en charge les connexions à un serveur interne, vous devez configurer les StorageZones Controller principaux et secondaires pour contourner le serveur proxy afin qu'ils puissent communiquer entre eux, comme décrit dans les étapes suivantes.

> **Important :**
>
> Les paramètres de la liste de contournement apparaissent uniquement pour la dernière version du StorageZones Controller. Si vous utilisez StorageZones Controller 2.2 à 2.2.2, vous devez ajouter manuellement une liste de contournement à Web.config pour chaque serveur secondaire, comme décrit à la section Web.config.

1. Dans la console du StorageZones Controller (`http://localhost/configservice/login.aspx`), cliquez sur l'onglet **Mise en réseau**.

   > **Remarque :**
   >
   > Si vous utilisez le contrôleur de zones de stockage 5.11.17, la modification d'un proxy nécessite une authentification. Lorsque vous y êtes invité, entrez l'adresse e-mail, le mot de passe et le sous-domaine complet de l'URL du compte complet, tel que subdomain.sharefile.com ou subdomain.sharefile.eu, pour votre compte. Cliquez sur Ouvrir une session.

2. Activez la case à cocher Activer le proxy et entrez l'adresse et le port du serveur proxy.
3. Sélectionnez un mode d'authentification et spécifiez votre compte Windows désigné pour l'accès proxy ShareFile.
4. Si votre site proxie tout le trafic HTTP sortant et qu'une zone possède plusieurs StorageZones Controller, configurez les paramètres de contournement :
   - Si tous les StorageZones Controller trafic se trouvent sur le même sous-réseau, activez la case à cocher **Bypass proxy…** afin que les contrôleurs puissent communiquer entre eux.
   - Si les contrôleurs des zones de stockage se trouvent sur des sous-réseaux différents, entrez le nom d'hôte du StorageZones Controller principales ou l'adresse IP dans l'adresse de contournement.
5. Redémarrez le serveur IIS de tous les membres de la zone.

## Configurer le contrôleur de domaine pour faire confiance au StorageZones Controller pour la délégation

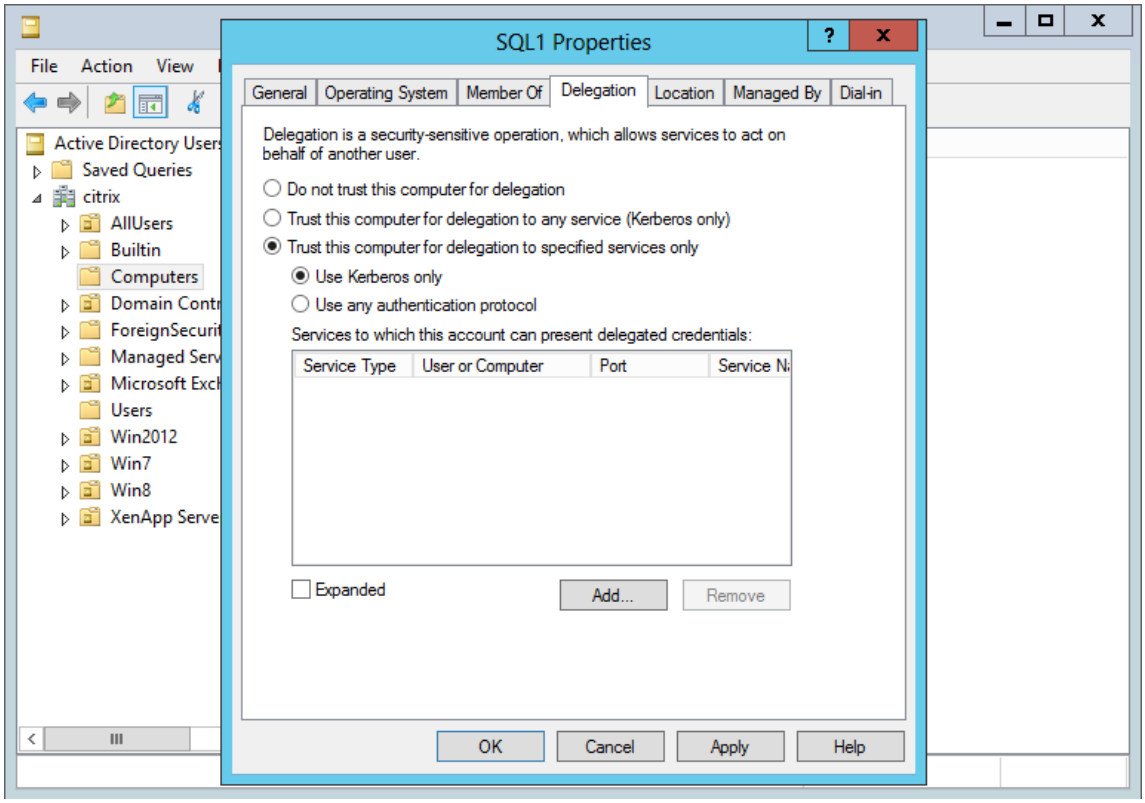
October 13, 2020

> **Remarque :**
>
> Cette section s'applique uniquement aux StorageZone Connector.

Pour prendre en charge l'authentification NTLM ou Kerberos sur des partages réseau ou des sites SharePoint, configurez le Controller de domaine, comme suit.

1. Sur le Controller de domaine pour le domaine des zones de stockage, cliquez sur **Démarrer > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
2. Développez le domaine et développez le dossier Ordinateurs.
3. Dans le volet droit, cliquez avec le bouton droit sur le nom du StorageZones Controller, sélectionnez **Propriétés**, puis cliquez sur l'onglet **Délégation**.
4. Pour Kerberos, sélectionnez **Approuver cet ordinateur pour la délégation aux services spécifiés uniquement**.




5. Pour NTLM :

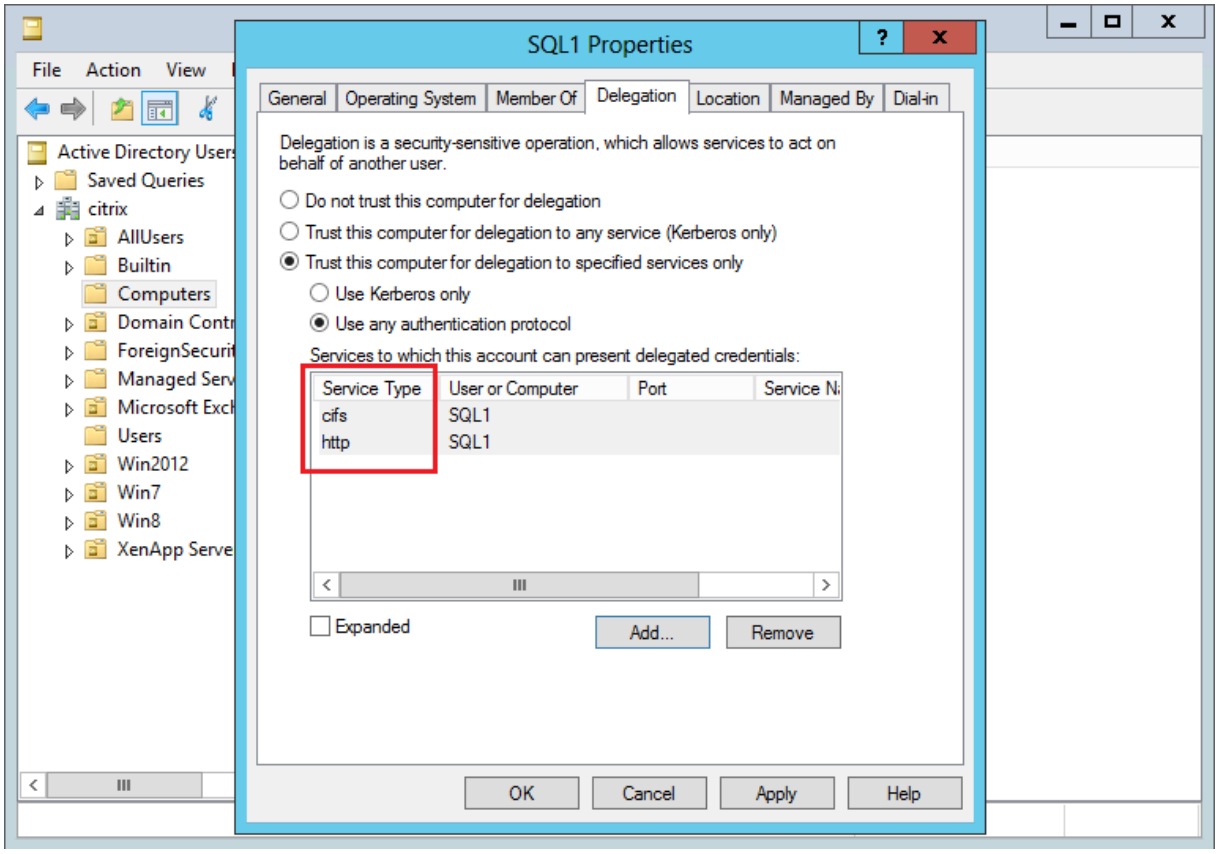
   a) Sélectionnez **Approuver cet ordinateur pour la délégation aux services spécifiés uniquement** et **Utiliser un protocole d'authentification**. Cliquez sur **OK**.

   b) Cliquez sur le bouton **Add**. Dans la boîte de dialogue **Ajouter des services**, cliquez sur **Utilisateurs ou Ordinateurs**, puis accédez ou tapez le nom d'hôte du partage réseau ou du serveur SharePoint. Cliquez sur **OK**.

   Si vous disposez de plusieurs serveurs de fichiers ou serveurs SharePoint, ajoutez un service pour chacun.

c) Dans la liste Services disponibles, sélectionnez les services utilisés : CIFS (pour le connecteur pour les partages de fichiers réseau) et HTTP (pour le connecteur pour SharePoint). Cliquez sur OK.




## Configurer StorageZones Controller pour les aperçus des applications Web, les miniatures et le partage en lecture seule

March 17, 2024

Les aperçus de fichiers locaux sont rendus par votre serveur Microsoft Office Web Apps (OWA) local. Lorsque vous prévisualisez des fichiers stockés dans une zone de stockage gérée par Citrix, les aperçus sont rendus par des serveurs OWA gérés par Citrix ou Microsoft.

> **Important :**
>
> Exigences relatives à la**liste blanche :**
>
> `*.sf-api.com` doit être accessible par votre serveur Office Online à des fins de prévisualisation et de modification afin de fonctionner correctement sur StorageZones version 5.0 ou

> ultérieure.

## Exigences

### Types de fichiers pris en charge pour l'aperçu des fichiers sur site

- doc, .docm, .docx, .dot, .dotm, .dotx, .odt
- .ods, .xls, .xlsb, .xlsm, .xlsx
- .odp, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx
- .pdf
- Fichiers d'images (bmp, gif, jpg, jpeg, png, tif, tiff)

### Types de fichiers pris en charge pour l'édition de fichiers sur site

- .docm, .docx, .odt
- .ods, .xlsb, .xlsm, .xlsx
- .odp, .ppsx, .pptx

### Environnements pris en charge

- Zones standard
- Zones multi-locataires
- Application Web

### Liste blanche/considérations relatives au réseau

- Le serveur OOS devrait pouvoir accéder à `https://\*.sf-api.com` **(ou .eu)**
- Le serveur SZC devrait pouvoir atteindre `https://\*.sf-api.com` et `https://\*.sharefile.com` **(ou .eu)**
- Le serveur SZC devrait pouvoir atteindre le serveur OOS `https://\<Customer OOS / OWA Endpoint\>/hosting/discovery` (par exemple, `https://oos.sharefileexample.com/hosting/discovery`)

Pour modifier des fichiers locaux, la gestion des versions des fichiers doit être activée sur votre compte ShareFile.

Le paramètre d'activation de Microsoft Office Online Editing dans le menu Préférences avancées de ShareFile Web App n'a aucune incidence sur la possibilité de modifier des fichiers locaux. Cette option spécifique **ne contrôlera pas** votre capacité à modifier des fichiers sur site, mais s'appliquera à la modification de tous les fichiers stockés dans un cloud public. L'activation de la modification

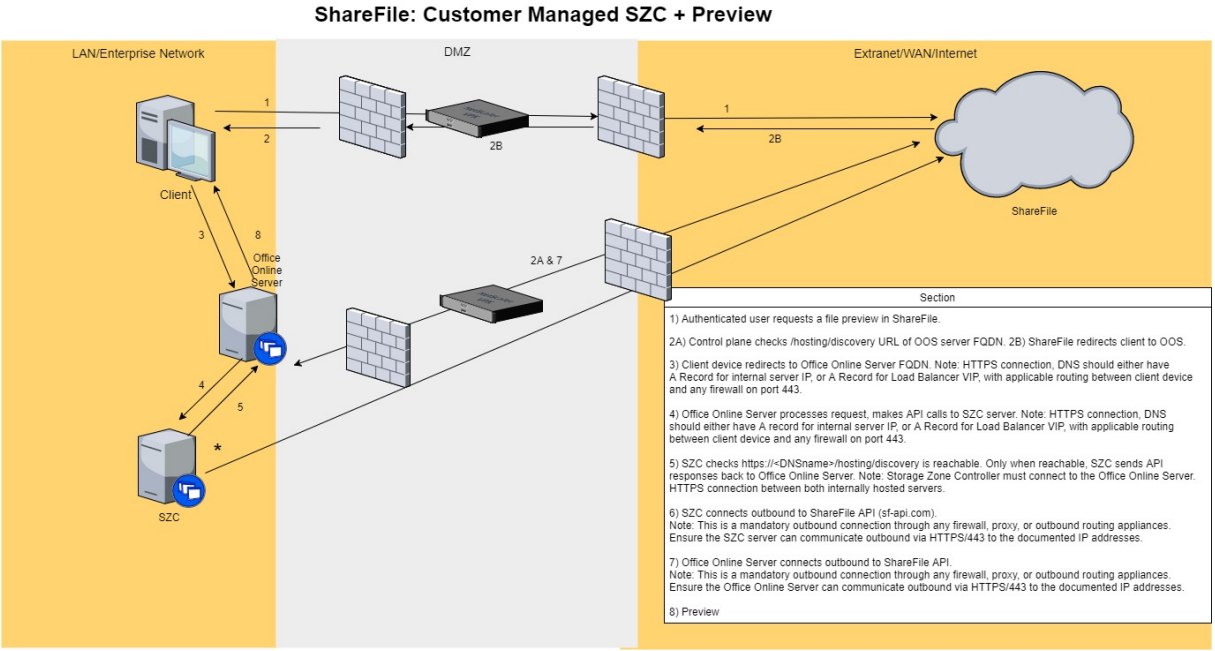
 

des fichiers sur site est contrôlée exclusivement par l'administrateur du StorageZones Controller en suivant les étapes décrites ci-dessous.

## Compatibilité avec les serveurs Microsoft

- **Microsoft Server 2016** : permet à la fois de modifier et de prévisualiser des fichiers. L'édition peut également être désactivée.
- **Microsoft Server 2013** : prend uniquement en charge la possibilité de prévisualiser les fichiers.

## Schéma architectural et réseau




1. L'utilisateur authentifié demande un aperçu du fichier dans ShareFile.
2. ShareFile émet une redirection vers l'appareil client avec le nom de domaine complet d'Office Online Server
3. L'appareil client est redirigé vers le nom de domaine complet d'Office Online Server.

   > **Remarque :**
   >
   > connexion HTTPS, DNS doit disposer soit d'un enregistrement pour l'adresse IP interne du serveur, soit d'un enregistrement pour l'équilibreur de charge VIP, avec un routage applicable entre l'appareil client et tout pare-feu sur le port 443.

4. Office Online Server traite les demandes et effectue des appels d'API vers le serveur StorageZones Controller.

> **Remarque :**
>
> Connexion HTTPS, DNS doit comporter soit un enregistrement pour l'adresse IP interne du serveur, soit un enregistrement pour l'équilibreur de charge VIP, avec un routage applicable entre l'appareil client et tout pare-feu sur le port 443.

5. Le Storage Zones Controller vérifie que `https://\<DNSname\>/hosting/discovery` est accessible. Ce n'est que lorsqu'il est joignable que SZC renvoie les réponses d'API à Office Online Server.

   > **Remarque :**
   >
   > le Storage Zone Controller doit se connecter au serveur Office Online. Connexion HTTPS entre les deux serveurs hébergés en interne.

6. Storage Zones Controller se connecte en sortie à l'API ShareFile (sf-api.com).

   > **Remarque :**
   >
   > Il s'agit d'une connexion sortante obligatoire via n'importe quel pare-feu, proxy ou appliance de routage sortant. Assurez-vous que le serveur StorageZones Controller peut communiquer en sortie via HTTPS/443 vers les adresses IP documentées ci-dessus.

7. Office Online Server connecte les données sortantes à l'API ShareFile.

   > **Remarque :**
   >
   > Il s'agit d'une connexion sortante obligatoire via n'importe quel pare-feu, proxy ou appliance de routage sortant. Assurez-vous que le serveur Office Online peut communiquer en sortie via HTTPS/443 vers les adresses IP documentées ci-dessus.

8. L'aperçu se produit.

Pour que le StorageZones Controller diffuse des octets de fichiers vers OOS plutôt que celui-ci n'appelle le plan de contrôle ShareFile pour télécharger le contenu : nous devons mettre à jour une clé dans l'un des fichiers de configuration du StorageZones Controller.

Le **fichier C:\inetpub\wwwroot\Citrix\StorageCenter\WopiServer\AppSettingsReleaseOnPrem.config** doit être mis à jour.

Ce fichier de configuration possède une clé **downloadFileFromSC** qui est actuellement **false**. Changez la clé sur **true** et redémarrez IIS.

Cela met à jour la configuration. De plus, OOS n'appelle plus le plan de contrôle ShareFile pour télécharger le contenu du fichier.

Lors de l'utilisation de cette option, serait-il correct d'indiquer qu'il n'y aurait pas de trafic entrant depuis le plan de contrôle vers OOS ?

Si l'option ci-dessus est utilisée, OOS n'établit plus de connexions sortantes vers le plan de contrôle ShareFile.

Toutefois, le plan de contrôle ShareFile établit toujours des connexions sortantes vers OOS, que l'option ci-dessus soit utilisée ou non.

Y a-t-il des avantages ou des inconvénients à utiliser une méthode par rapport à l'autre ?

Dans cette approche, OOS ne télécharge pas directement le contenu des fichiers. Le StorageZones Controller télécharge et diffuse les octets du fichier vers OOS. Cela augmentera ainsi la charge sur les serveurs StorageZones Controller.

Le téléchargement et la diffusion d'octets de fichiers sont des tâches gourmandes en ressources. En fonction du nombre d'utilisateurs et du nombre d'opérations de prévisualisation et de modification, la charge sur les serveurs StorageZones Controller augmente.

## Activez la prévisualisation et l'édition sur site

Pour prendre en charge l'aperçu des documents et des images dans le navigateur, les miniatures, le partage en lecture seule des données stockées dans des zones de stockage gérées par le client et l'édition de fichiers sur site, configurez le StorageZones Controller comme suit :

1. Dans la console StorageZones Controller, cliquez sur l'**onglet ShareFile Data**.
2. Dans la section **Configuration du partage du réseau local**, activez **Configurer les aperçus des applications Web Office**.
3. Entrez l'URL externe de votre serveur Microsoft Office Web Apps (OWA).
   - Les utilisateurs doivent télécharger et configurer le logiciel du serveur OWA via leur abonnement Microsoft Office MSDN.
4. Sélectionnez **Activer les modifications Office Online** (si nécessaire)
5. Vérifiez que l'URL OWA est accessible de l'extérieur.
6. Vérifiez que vos serveurs Office Online peuvent communiquer avec `*.sf-api.com`.
7. Dans la console StorageZones Controller, cliquez sur l'onglet **Surveillance**.
8. Vérifiez que la **connectivité du serveur OWA** est cochée en vert.

> **Remarque :**
>
> La modification de fichiers sur site nécessite l'activation de la gestion des versions des fichiers pour le compte ShareFile. Si la gestion des versions des fichiers est désactivée pour le compte, la modification sur site ne fonctionnera pas.

**Important :**

**Configurer la synchronisation de l'horloge** :

- Vérifiez que le Controller Heure sur vos zones de stockage est synchronisé avec time.windows.com ou un autre serveur NTP. Cliquez ici pour plus d'informations sur la configuration de la synchronisation de l'horloge.

**Modifier l'OWA URAL ou désactiver les aperçus** :

- L'une ou l'autre des actions ci-dessus nécessite le redémarrage du service IIS pour chaque contrôleur principal et secondaire.

## Limitations

- Les applications mobiles ne prennent pas en charge la modification dans le navigateur.
- Les connecteurs ne prennent pas en charge les aperçus dans le navigateur.

Les aperçus WOPI ne sont pas pris en charge pour les comptes VDR.

Pour plus d'informations sur la configuration de votre Citrix ADC pour le partage en lecture seule, consultez la section Configurer Citrix [ADC pour StorageZones Controller].(/en-us/storage-zones-controller/5-0/install/configure-netscaler.html)

## Résolution des problèmes liés à l'OWA et à l'OOS

Si vous rencontrez des difficultés pour prévisualiser ou modifier des fichiers sur site, les étapes suivantes vous aideront à identifier et à corriger des problèmes spécifiques.

Pour résoudre les problèmes liés à votre configuration, connectez-vous d'abord à la machine OWA ou OOS.

1. Vérifiez que les services Office WebApps ou OfficeOnline Windows sont exécutés dans services.msc.
2. Dans un nouveau navigateur, ouvrez la page `http://localhost/hosting/discovery`. Si cette page se charge correctement, une réponse XML doit être renvoyée.
3. Exécutez PowerShell en tant qu'administrateur et exécutez la commande suivante :

```
Get-OfficeWebAppsFarm
```

Si vous recevez un message d'AVERTISSEMENT ou d'ERREUR dans la réponse, vérifiez vos paramètres de configuration pour détecter d'éventuelles erreurs ou erreurs.

**Considérations relatives au réseau** :

- Le serveur OOS devrait pouvoir accéder à `https://*.sf-api.com` **(ou .eu)**
- Le serveur SZC devrait pouvoir atteindre `https://*.sf-api.com` et `https://*.sharefile.com` **(ou .eu)**
- Le serveur SZC devrait pouvoir atteindre le serveur OOS. `https://<CustomerOOS/OWAEndpoint\>/hosting/discovery` Par exemple, `https://oos.sharefileexample.com/hosting/discovery`.

## Configurer les zones de stockage multi-locataires

March 17, 2024

Une zone de stockage mutualisée est une fonctionnalité du contrôleur de zones de stockage ShareFile qui permet aux Citrix Service Providers (CSP) de créer et de gérer une zone de stockage unique partagée par tous les locataires.

Si vous êtes un CSP avec un compte partenaire provisionné par ShareFile, vous pouvez héberger une zone de stockage standard multitenant sur votre domaine qui prend en charge un nombre illimité de locataires. L'utilisation d'une zone multilocataire vous permet de :

- Fournissez à chaque locataire un compte ShareFile unique et tirez parti de toutes les fonctionnalités exceptionnelles de ShareFile, telles que la personnalisation de la marque, les préférences de conservation des fichiers et les paramètres de sécurité.
- Conservez un référentiel de stockage unique pour tous vos locataires.
- Intégrez de nouveaux clients plus rapidement et réduisez les coûts et la complexité de gestion liés à la création d'une zone de stockage distincte pour chaque compte client.

### Créez un compte partenaire

Vous devez disposer d'un compte partenaire pour pouvoir enregistrer une zone de stockage mutualisée.

Pour créer un compte partenaire, vous devez vous inscrire au programme CSP et commander un SKU de stockage auprès de votre distributeur préféré qui vous autorise à proposer ShareFile en tant que service.

Si vous êtes déjà enregistré en tant que CSP et que vous avez commandé le ShareFile approprié pour les CSP stockant un SKU, un compte partenaire a déjà été créé pour vous. Si vous ne parvenez pas à localiser ce nouveau compte partenaire, veuillez contacter les services de compte ShareFile à l'adresse acctsvcs@sharefile.com.

Lorsque vous commencez à provisionner des comptes clients dans le cadre de votre offre CSP ShareFile, nous vous recommandons de créer un administrateur de compte de service générique sur votre compte partenaire. De cette façon, l'utilisateur administrateur peut être l'administrateur partenaire officiel de tous vos comptes clients. Assurez-vous que l'autorisation Gérer les locataires est activée pour cet utilisateur administrateur du compte de service. Nous encourageons donc les partenaires à créer cet administrateur partenaire dès maintenant avant de remplir le formulaire de demande de compte client CSP (à l'étape 4).

### Installation et configuration d'une zone de stockage multi-locataires

- Créez une nouvelle zone de stockage mutualisée et associez-la à votre compte partenaire. Pour plus de détails, voir Installer StorageZones Controller et créer une zone de stockage.
- Installez le StorageZone Controller en mode multitenant. Assurez-vous d'exécuter l'invite de commande spécifiée ci-dessous dans l'article d'installation mentionné à l'étape précédente.

```
msiexec /i StorageCenter\\_5.0.1.msi MULTITENANT=1
```

> **Remarque :**
>
> Dans la commande précédente, vous devrez peut-être mettre à jour le numéro de version (5.0.1 dans l'exemple) pour qu'il corresponde au numéro de msi que vous essayez d'installer.

### Configurez la nouvelle zone de stockage et associez-la à votre compte partenaire

Pour plus de détails, reportez-vous à l'étape 10 de la section Installer StorageZones Controller et créer une zone de stockage.

Connectez-vous à votre compte partenaire sur lequel vous souhaitez enregistrer la nouvelle zone.

> **Important :**
>
> Ce compte doit disposer des autorisations ShareFile suivantes : Gérer les locataires et Créer et gérer des zones.

Vous pouvez désormais vous connecter à votre compte partenaire et voir la nouvelle zone de stockage mutualisé. Cliquez sur l'onglet **Paramètres d'administration > Zones de stockage > Gestion par les partenaires**.

### Demander des comptes de locataires pour la zone multilocataire

Pour demander des comptes locataires, remplissez le formulaire de demande de compte client CSP.

Lorsque vous demandez un compte locataire, vous devez également spécifier un utilisateur Partner Admin. Cet administrateur partenaire doit être un administrateur de votre compte partenaire avec l'autorisation Gérer les locataires activée. Lorsqu'un compte de locataire est créé, cet utilisateur administrateur partenaire sera automatiquement configuré sur le compte en tant qu'utilisateur administrateur et pourra se connecter et gérer le compte de locataire. Comme il ne peut pas y avoir deux utilisateurs sur un compte avec la même adresse e-mail, l'adresse e-mail de l'administrateur du partenaire spécifiée sur le formulaire ne peut pas être la même que celle de l'administrateur du client sur le même formulaire.

Pour garantir le délai d'exécution le plus rapide possible, assurez-vous de fournir l'ID d'organisation correct et le nom de zone multilocataire que vous souhaitez utiliser comme zone de stockage pour le compte du locataire.

Vous recevrez un e-mail une fois que Citrix aura configuré les comptes demandés. L'e-mail contiendra des informations sur le sous-domaine du locataire et un lien d'activation pour configurer l'accès. ShareFile vous enverra, à vous et aux utilisateurs administratifs de vos clients, des e-mails séparés.

Vos clients peuvent alors commencer à utiliser ShareFile. Tous les nouveaux utilisateurs connectés au compte d'un locataire utiliseront la zone multilocataire que vous avez spécifiée comme emplacement par défaut pour les fichiers de l'utilisateur.

#### Prévisualisation de fichiers Office et de PDF à l'aide d'un serveur Office Online

Cette fonctionnalité est prise en charge par les environnements Office Online Server pris en charge. Cliquez ici pour obtenir des informations de configuration.

#### Partage de connecteurs

Cette fonctionnalité est prise en charge avec les zones multilocataires.

### Gérer les locataires

Dans le compte partenaire, vous trouverez un tableau de bord de gestion des locataires situé sous **Paramètres d'administration > Préférences avancées**. Ce tableau de bord centralisé vous permet de vérifier le statut de tous les locataires associés à votre compte partenaire. Le tableau de bord inclut la consommation de licences, la zone de stockage par défaut, la consommation de stockage et l'état du compte (payant ou essai) pour chaque locataire.

> **Remarque :**

> Le tableau de bord n'est disponible que pour les utilisateurs de votre compte partenaire dont l'autorisation **Manage Tenants** est activée.

#### Limites liées à la multilocation

La fonctionnalité IRM (ShareFile Information Rights Management) n'est pas prise en charge pour les zones de stockage mutualisées.

### Dépannage

#### Impossible de créer la zone : Interdit

Lors de l'enregistrement de la zone de stockage, si le message d'erreur suivant s'affiche : « Impossible de créer la zone : interdit », vérifiez que vos autorisations utilisateur incluent l'autorisation « Gérer les locataires ».

## Mettre à niveau

March 17, 2024

### Mettez à niveau StorageZones Controller 5.10 ou version ultérieure vers la dernière version

> **Remarques :**
>
> ShareFile recommande de prendre un instantané du serveur avant de procéder à la mise à jour et de sauvegarder la configuration du serveur Storage Zone. Pour savoir comment sauvegarder la configuration de la zone de stockage, voir Sauvegarder la configuration d'une configuration principale de StorageZones Controller
>
> Pour les problèmes liés à la mise à niveau de votre StorageZones Controller, voir Résolution des problèmes de mise à niveau du StorageZones Controller ShareFile.

Mettez à niveau StorageZones Controller 5.10 en suivant les étapes suivantes.

1. Téléchargez la dernière version du logiciel Storage Zone Controller depuis la page de téléchargement de ShareFile.

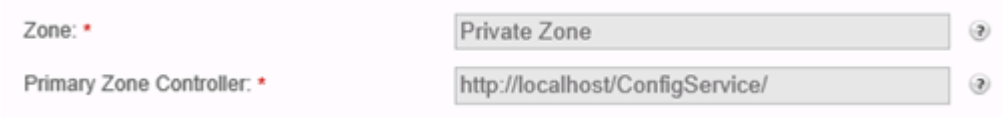
 

> **Remarque :**
>
> Les contrôleurs de zone de stockage ne sont pas disponibles pendant la mise à niveau et les redémarrages du serveur. Pour éviter toute perte de données, nous vous recommandons de planifier une fenêtre de maintenance avec les utilisateurs. Faites-leur savoir que la zone n'est pas disponible pour les transferts de fichiers lors de la mise à niveau.

2. Installez le fichier MSI sur le serveur Windows sur lequel le StorageZone Controller est installé. Si vous avez plusieurs serveurs, la mise à jour doit être installée d'abord sur le serveur principal, puis sur les autres. Il existe deux manières d'identifier le serveur principal :

   a) Identifiez le StorageZones Controller principal sur la page **de configuration** :

      - Sur un serveur Controller, accédez à l'outil de configuration `http://localhost/configservice/login.aspx` ou démarrez-le depuis le menu Démarrer. L'autorisation de « créer et gérer des zones » est requise pour accéder à la configuration.
      - Dans l'onglet **Données**, vérifiez le champ Contrôleur de zone principal. Le champ répertorie le nom d'hôte du serveur du contrôleur de zone principal sous la forme `http://server/ConfigService`.




      Notez que l'hôte local `http://localhost/ConfigService` indique que ce serveur est le contrôleur de zone principal.

   b) Identifiez le StorageZones Controller principal à partir du registre :

      - Sur un serveur de contrôleur, ouvrez l'éditeur du registre (regedit.exe).
      - Localisez la clé de registre : HKEY_LOCAL_MACHINE \ SOFTWARE \ Wow6432Node \ Citrix \ StorageCenter
      - Vérifiez que la valeur de la clé `isPrimaryConfigServer` est vraie.

3. Démarrez la mise à niveau sur le Storage Zone Controller principal :

   a) Exécutez StorageCenter.msi pour démarrer l'assistant de configuration du contrôleur de zones de stockage ShareFile.

   b) Répondez aux invites. Une fois l'installation terminée, l'assistant affiche le message « Assistant de configuration du contrôleur de zones de stockage Citrix ShareFile terminé ».

   c) Redémarrez le serveur.

4. Sur chaque contrôleur de zone de stockage secondaire (si nécessaire) :

a) Exécutez StorageCenter.msi pour démarrer l'assistant de configuration du contrôleur de zones de stockage ShareFile.

b) Répondez aux instructions, puis sélectionnez **Terminer.**

c) Redémarrez le serveur.

5. Sur tous les contrôleurs de zone de stockage, redémarrez le serveur IIS de tous les membres de la zone.

   a) Lancez l'invite CMD et Exécuter en tant qu'administrateur.

   b) Tapez `iisreset` puis appuyez sur la touche **Entrée**. En cas de succès, l'invite indique « Les services Internet ont été redémarrés avec succès ».

   c) Vérifiez que les paramètres de registre du StorageZones Controller principal sont corrects après la mise à niveau.

6. Après l'installation de la mise à niveau, choisissez de lancer la page de configuration des zones de stockage sur n'importe quel membre de la zone pour vous connecter et modifier les paramètres de configuration.

   - Pour revenir à tout moment à la console StorageZones Controller, ouvrez `http://localhost/configservice/login.aspx`. Une fois que vous avez **cliqué sur Terminer** ou que vous êtes retourné à la console StorageZones Controller, la page d'ouverture de session s'ouvre.

   > **Remarque :**
   >
   > N'oubliez pas que pour vous connecter à la page de configuration du Storage Zone Controller, vous devez utiliser un mot de passe spécifique à l'application. Si vous devez créer un nouveau mot de passe spécifique à une application, consultez l'article d'assistance suivant : Créer un mot de passe spécifique à une application.

   - Pour modifier les informations affichées, sélectionnez **Modifier**, apportez vos modifications, puis sélectionnez **Enregistrer**.

   > **Remarque :**
   >
   > Vérifiez que les transferts de données vers chaque StorageZone Controller fonctionnent avant de terminer la fenêtre de maintenance.

## Gérer les StorageZones Controller

February 14, 2022

Après avoir installé vos contrôleurs de zone de stockage principal et secondaire, suivez les procédures suivantes pour gérer les contrôleurs et les préparer à la reprise après sinistre.

Pour ouvrir la console Storage Zones Controller, accédez à l'outil de configuration `http://localhost/configservice/login.aspx` ou démarrez l'outil de configuration à partir du menu Démarrer.

### Contrôleur de gestion des zones de stockage



## Joindre un StorageZones Controller secondaire à une zone de stockage

October 13, 2020

Pour configurer une zone de stockage pour une haute disponibilité, connectez au moins deux StorageZones Controller à celle-ci. Pour ce faire, vous devez :

1. Installez un StorageZones Controller principal et créez une zone (comme décrit à la section Installer un StorageZones Controller et créer une zone de stockage).
2. Installez le StorageZones Controller sur un deuxième serveur et joignez ce Controller à la même zone.

**Les StorageZones Controller appartenant à la même zone doivent utiliser le même partage de fichiers pour le stockage.**

Dans un déploiement à haute disponibilité, les serveurs secondaires sont des StorageZones Controller indépendants et entièrement fonctionnels. Le sous-système de contrôle des zones de stockage choisit aléatoirement un StorageZones Controller pour gérer les demandes d'opération, y compris les opérations de téléchargement, de téléchargement, de copie et de suppression.

Si le serveur principal se déconnecte, vous pouvez facilement promouvoir un serveur secondaire au rang de serveur principal. Vous pouvez également rétrograder un serveur primaire au rang de serveur secondaire.

1. Ouvrez un navigateur Web sur le serveur pour être un StorageZones Controller secondaire. Ensuite ouvrez `http://localhost/configservice/login.aspx` et connectez-vous.
2. Cliquez sur **Joindre une zone existante** et sélectionnez la zone de stockage.
3. Entrez les informations demandées, puis cliquez sur **Enregistrer**.

   Pour le Controller de zone principal, vous pouvez entrer uniquement le nom d'hôte ou l'adresse IP, et ShareFile remplira l'URL complète. Pour tester une URL, saisissez-la dans le champ d'adresse du navigateur. Si l'URL est correcte, une page de bannière ShareFile apparaît. Pour les zones standard : si l'URL est incorrecte et que vous avez spécifié https, vérifiez que vous utilisez des certificats SSL publics approuvés valides.
4. Si vous utilisez un serveur proxy pour le StorageZones Controller principal, spécifiez le serveur proxy pour le Controller secondaire, comme décrit à la section Spécifier un serveur proxy pour les zones de stockage.
5. Redémarrez le serveur IIS de tous les membres de la zone.

   Un StorageZones Controller secondaire hérite de la configuration du Controller principal au démarrage.

## Modifier l'adresse ou la phrase secrète d'un StorageZones Controller principal

February 14, 2022

> **Remarque :**
>
> Seul l'administrateur du compte peut apporter des modifications d'adresse ou de phrase secrète.

### Pour spécifier une adresse externe ou locale différente pour un StorageZones Controller principal

Vous pouvez modifier l'adresse externe d'un StorageZones Controller principal à l'aide de cette procédure ou d'autres outils de gestion de serveur.

1. Sur le serveur Storage Zone Controller principal, ouvrez la **page Configuration** ou accédez à : `http://localhost/configservice/login.aspx`.
2. Connectez-vous à la page de configuration avec les informations d'identification d'administrateur ShareFile.
3. Dans l'onglet Données, sélectionnez **Modifier**.
4. Spécifiez la nouvelle **adresse externe** ou la nouvelle **adresse locale**, puis sélectionnez **Enregistrer les modifications**.
5. Répétez les étapes pour tous les membres de zone.
6. Redémarrez le serveur IIS de tous les membres de la zone.

### Pour modifier la phrase secrète d'un StorageZones Controller principal

> **Remarque :**
>
> La phrase secrète actuelle est nécessaire pour modifier la phrase secrète d'un StorageZones Controller.

1. Ouvrez la page de configuration des zones de stockage : `http://localhost/configservice/login.aspx`.
2. Cliquez sur **Modifier**.
3. Spécifiez une phrase secrète à utiliser pour protéger votre clé de chiffrement de fichiers. Veillez à archiver la phrase secrète et la clé de chiffrement dans un emplacement sécurisé.

   La phrase secrète n'est pas la même que le mot de passe de votre compte et ne peut pas être récupérée en cas de perte. Si vous perdez la phrase secrète, vous ne pouvez pas réinstaller des zones de stockage, joindre des StorageZones Controller supplémentaires à la zone de stockage ou récupérer la zone de stockage en cas de défaillance du serveur.

   > **Remarque :**
   >
   > La clé de chiffrement apparaît à la racine du chemin de stockage partagé. La perte du fichier de clé de chiffrement bloque immédiatement l'accès à tous les fichiers de la zone de stockage.

4. Si vous avez modifié la phrase secrète sur le serveur principal : ouvrez une session sur la page de configuration des zones de stockage pour chacun des autres membres et entrez la phrase secrète lorsque vous y êtes invité.

   Vous devez utiliser la même phrase secrète pour chaque StorageZones Controller d'une zone.

5. Redémarrez le serveur IIS de tous les membres de la zone.

## Rétrograder et promouvoir les StorageZones Controller

October 13, 2020

Dans un déploiement à haute disponibilité, les serveurs secondaires sont des StorageZones Controller indépendants et entièrement fonctionnels. Pour gérer ou remplacer un StorageZones Controller principal, rétrogradez-le d'abord, puis promouvrez un Controller secondaire. Si le serveur principal se déconnecte, vous pouvez promouvoir un serveur secondaire en serveur principal.

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Pour rétrograder un StorageZones Controller principal :

   a) Localisez la clé de Registre : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

   b) Définissez IsPrimaryConfigServer sur false.

   c) Définissez PrimaryConfigServiceURL sur l'URL du serveur qui sera le nouveau StorageZones Controller principal, en utilisant le formulaire`https://IPaddress` ou`https://hostname/ConfigService/`.

   d) Redémarrez le serveur IIS de tous les membres de la zone.

2. Pour promouvoir un StorageZones Controller secondaire :

   a) Localisez la clé de Registre : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

   b) Définissez IsPrimaryConfigServer sur true.

   c) Définissez PrimaryConfigServiceURL sur `http://localhost/ConfigService/`.

   d) Redémarrez le serveur IIS de tous les membres de la zone.

3. Modifier tous les StorageZones Controller secondaires supplémentaires :

   a) Localisez la clé de Registre : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

   b) Définissez PrimaryConfigServiceURL sur l'URL du serveur qui sera le nouveau StorageZones Controller principal à l'aide du formulaire`https://IPaddress` ou`https://hostname/ConfigService/`.

   c) Redémarrez le serveur IIS de tous les membres de la zone.

## Désactiver, supprimer ou redéployer un StorageZones Controller

March 13, 2023

### Pour désactiver un StorageZones Controller

> **Remarque :**
>
> Utilisez cette procédure si chaque StorageZones Controller possède une adresse externe différente. Désactivez un contrôleur depuis l'interface Citrix ADC si vous utilisez la même adresse externe pour tous les contrôleurs de zones de stockage.

Désactivez un StorageZones Controller avant de mettre le serveur hors ligne à des fins de maintenance.

1. Dans l'interface Web de ShareFile, cliquez sur **Admin**, puis sur **Zones de stockage**.
2. Cliquez sur le nom de la zone, puis sur le nom d'hôte du StorageZones Controller.
3. Décochez la case activée, puis cliquez sur **Enregistrer les modifications**.
4. Redémarrez le serveur IIS de tous les membres de la zone.

### Pour supprimer un StorageZones Controller

La suppression d'un StorageZones Controller n'entraîne pas la suppression des données ni du fichier SCKeys.txt. Si vous supprimez un contrôleur de zones de stockage principal, rétrogradez-le avant de continuer.

1. Dans l'interface Web de ShareFile, cliquez sur **Admin**, puis sur **Zones de stockage**.
2. Cliquez sur le nom de la zone, puis sur le nom d'hôte du StorageZones Controller.

3. Cliquez sur **Delete**.
4. Redémarrez le serveur IIS de tous les membres de la zone.

### Pour redéployer un StorageZones Controller

Aucune information n'est perdue lorsque vous redéployez un StorageZones Controller.

1. Désinstallez les zones de stockage du serveur.
2. Dans l'interface Web de ShareFile, cliquez sur **Admin > Zones de stockage**, puis sélectionnez votre zone. Ne supprimez pas la zone.
3. Sélectionnez le StorageZones Controller et supprimez-le.
4. Installez des zones de stockage. Ne l'enregistrez pas encore.
5. Exécutez l'assistant de configuration du StorageZones Controller pour associer le StorageZones Controller à une zone et terminer l'enregistrement.
6. Redémarrez le serveur IIS de tous les membres de la zone.

## Transfert de fichiers vers un nouveau partage réseau

October 13, 2020

Avant de configurer un nouveau partage réseau pour le stockage de données privé :

### Exigences

- Les StorageZones Controller appartenant à la même zone de stockage doivent utiliser le même partage de fichiers pour le stockage.
- Les StorageZones Controller accèdent au partage à l'aide de l'utilisateur du pool de comptes IIS. Par défaut, les pools d'applications fonctionnent sous le compte d'utilisateur Service réseau, qui dispose de droits d'utilisateur de bas niveau. Un StorageZones Controller utilise le compte de service réseau par défaut.
- Le compte de service réseau doit disposer d'un accès **complet** à cet emplacement de stockage.
- Désactivez les contrôleurs de zone de stockage pour les nouveaux chargements avant de transférer des données vers le nouveau partage. Dans l'application Web, accédez à **Paramètres d'administration** > **StorageZones**. Sélectionnez le nom de la zone. Sous **Centres de stockage**, sélectionnez chaque serveur hôte. Pour mettre fin au trafic vers chaque serveur hôte, désélectionnez l'option **Activé** sous **Paramètres du serveur**.

1. Ouvrez la page de configuration des zones de stockage : `http://localhost/configservice/login.aspx`.

2. Cliquez sur **Modifier**.
3. Dans **Emplacement de stockage**, entrez le chemin UNC vers votre partage réseau, dans l'écran, `\\server\share` puis cliquez sur **Enregistrer**.

   > **Attention :**
   >
   > Le StorageZones Controller écrase toutes les données de ce chemin avec un format de stockage propriétaire. Il est recommandé de ne jamais spécifier de chemin d'accès à un emplacement contenant des données de fichier. Réservez cet emplacement de stockage pour les zones de stockage pour les données ShareFile uniquement.

4. Si les informations d'identification du chemin UNC de votre nouvel emplacement de partage réseau diffèrent de la précédente, spécifiez l'ouverture de session de stockage et le mot de passe de stockage.
5. Redémarrez le serveur IIS de tous les membres de la zone.
6. Connectez-vous à la page de configuration de tous les membres de la zone.
7. Copiez toute la structure de répertoire, y compris SCkeys.txt, sur le nouveau serveur.

## Sauvegarde d'une configuration de StorageZones Controller principales

June 27, 2023

Un StorageZones Controller est installé sur votre site local et vous êtes responsable de sa sauvegarde. Pour protéger complètement votre déploiement, vous devez prendre un instantané du serveur Storage Zones Controller, sauvegarder votre configuration et préparer le StorageZones Controller pour la récupération des fichiers.

Il est essentiel que vous sauvegardiez votre configuration comme décrit dans cette rubrique. Par exemple, si vous ne disposez pas d'une sauvegarde et que quelqu'un supprime accidentellement une zone, vous ne pouvez pas récupérer les dossiers et les fichiers de cette zone.

> **Important :**
>
> Veillez à utiliser PowerShell 4.0 pour cette procédure. Pour plus d'informations sur la configuration requise pour PowerShell, consultez la section Scripts et commandes PowerShell dans la section Configuration système requise pour Storage Zones Controller

Le programme d'installation du StorageZones Controller comprend un module PowerShell avec des commandes qui sauvegardent et restaurent les paramètres de configuration d'un StorageZones Controller principal. Votre sauvegarde inclut des informations de configuration pour les zones, les zones

de stockage pour ShareFile Data, le connecteur de zone de stockage pour SharePoint et le connecteur de zone de stockage pour les partages de fichiers réseau.

Les commandes de sauvegarde et de restauration nécessitent que vous exécutiez la version 32 bits de PowerShell dans le même contexte utilisateur que le contrôleur de zone de stockage. Pour définir le contexte utilisateur, utilisez l'outil PsExec. Cet outil est disponible en téléchargement à partir de https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.

> **Remarque :**
>
> Ces étapes ne s'appliquent pas à un StorageZones Controller secondaire. Pour récupérer un StorageZones Controller secondaire, réinstallez le contrôleur de zone de stockage sur le serveur, puis connectez le serveur au StorageZones Controller principal.

1. Le script PowerShell utilisé dans cette procédure n'étant pas signé, vous devez modifier votre stratégie d'exécution PowerShell.

   a) Déterminez si votre stratégie d'exécution PowerShell vous permet d'exécuter des scripts locaux non signés : PS `C:\>Get-ExecutionPolicy`

      Par exemple, une stratégie RemoteSigned, Unrestricted ou Bypass vous permet d'exécuter des scripts non signés.

   b) Pour modifier votre stratégie d'exécution PowerShell : PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. Définissez le contexte utilisateur pour cette session PowerShell. Dans une fenêtre de commandes, exécutez l'une des commandes suivantes.

   - Si vous utilisez le compte de service réseau par défaut :

     ```
     PsExec.exe -i -u "NT AUTHORITY\NetworkService"C:\Windows\
     SysWOW64\WindowsPowerShell\v1.0\powershell
     ```

   - Si vous utilisez un utilisateur nommé pour le pool d'applications Storage Zones Controller :

     ```
     PsExec.exe -i -u "domain\username"C:\Windows\SysWOW64\WindowsPowerShel
     \v1.0\powershell
     ```

   Une fenêtre PowerShell s'ouvre.

3. À partir de l'invite PowerShell, importez le module ConfigBR.dll : `Import-Module C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll`

   Vous devez importer le module chaque fois que vous ouvrez une nouvelle fenêtre PowerShell.

4. À partir de l'invite PowerShell, exécutez la commande Get-SFConfig et suivez les instructions suivantes :

   - **PrimaryZoneController** - Exemples d'entrées :
     - Connectez-vous à un serveur local : `http://localhost/ConfigService/`
     - Connectez-vous à un serveur distant : `http[s]://myservername.domain.com/ConfigService/`
     - Connectez-vous à un serveur distant si des problèmes de DNS empêchent la connexion à un nom de serveur : `http[s]://10.40.37.5/ConfigService/`
   - Phrase secrète : phrase secrète spécifiée pour le Storage Zone Controller.
   - FilePath - Exemple `c:\szc-backup.bak`

   Paramètres de commande :

| Paramètres | Description | Exemples |
|---|---|---|
| "server" | Nom du serveur ou adresse IP du StorageZones Controller principal. Il peut se présenter sous l'une des formes suivantes, indiquées sous Exemples, et doit inclure la barre oblique de fin. | Se connecter à un serveur local : `http://localhost/ConfigService/` ; Se connecter à un serveur distant : `http[s]://myservername.domain.com/ConfigService/` ; Se connecter à un serveur distant si des problèmes DNS empêchent la connexion à un nom de serveur : `http[s]://10.40.37.5/ConfigService/` |
| "passphrase" | La phrase secrète spécifiée pour le contrôleur de zone de stockage. | "MyPassphrase" |
| "fullpath" | Emplacement où enregistrer le fichier de sauvegarde. | "c:\szc-backup.bak" |

La commande **Get-SFConfig** crée le fichier de sauvegarde.

Pour restaurer la configuration d'un StorageZones Controller principal, reportez-vous à la section Récupérer une configuration de StorageZones Controller principale

# Restauration d'une configuration de StorageZones Controller principal

February 14, 2022

> **Important :**
>
> - Veillez à utiliser PowerShell 4.0 pour cette procédure. Pour plus d'informations sur la configuration requise pour PowerShell, consultez les scripts et les commandes PowerShell dans Configuration système requise pour le StorageZones Controller.
> - Pour plus d'informations sur la mise en œuvre de TLS à l'échelle du système, consultez l'article Microsoft sur Comment activer TLS 1.2 sur les clients.

Storage Zones Controller fournit les options suivantes pour la reprise après sinistre lorsqu'un StorageZones Controller principal est supprimé ou tombe en panne :

- Si un StorageZones Controller secondaire est disponible, promouvez le contrôleur secondaire au rang de contrôleur principal.
- Si aucun StorageZones Controller secondaire n'est disponible et que vous avez sauvegardé la configuration de votre StorageZones Controller principal (comme décrit dans Sauvegarder une configuration de StorageZones Controller principal), récupérez le StorageZones Controller principal à partir du fichier de sauvegarde.
- Si vous ne disposez pas d'une sauvegarde de la configuration de votre StorageZones Controller principal et que tous vos StorageZones Controller sont accidentellement supprimés ou deviennent inutilisables, seule une restauration partielle est possible. Vous pouvez récupérer des zones et la configuration des zones de stockage pour ShareFile Data, mais pas les connecteurs de zones de stockage.

## Pour récupérer un StorageZones Controller principal à partir d'un fichier de sauvegarde

> **Remarque :**
>
> Ces étapes s'appliquent uniquement à un StorageZones Controller principal. Pour récupérer un StorageZones Controller secondaire, réinstallez le StorageZones Controller sur le serveur, puis connectez le serveur au StorageZones Controller principal.

1. Le script PowerShell utilisé dans cette procédure n'étant pas signé, il peut être nécessaire de modifier votre stratégie d'exécution PowerShell.

   a) Déterminez si votre stratégie d'exécution PowerShell vous permet d'exécuter des scripts locaux non signés : PS `C:\>Get-ExecutionPolicy`

Par exemple, une stratégie RemoteSigned, Unrestricted ou Bypass vous permet d'exécuter des scripts non signés.

b) Pour modifier votre stratégie d'exécution PowerShell : PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. Définissez le contexte utilisateur pour cette session PowerShell. Dans une fenêtre de commandes, exécutez l'une des commandes suivantes.

> **Remarque :**
>
> Téléchargez PsExec.exe à partir de https://docs.microsoft.com/en-us/sysinternals/downloads/psexec et suivez les instructions d'installation indiquées sur cette page.

- Si vous utilisez le compte de service réseau par défaut :

```
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
```

- Si vous utilisez un utilisateur nommé pour le pool d'applications Storage Zones Controller :

```
PsExec.exe -i -u "domain\username" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
```

Une fenêtre PowerShell s'ouvre.

3. À partir de l'invite PowerShell, importez le module ConfigBR.dll : `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

Vous devez importer le module chaque fois que vous ouvrez une nouvelle fenêtre PowerShell.

4. À partir de l'invite PowerShell, exécutez la commande `Set-SfConfig`: `Set-SfConfig -PrimaryZoneController "server"-Passphrase "passphrase"-FilePath "fullpath"`

Où :

- server est le nom du serveur ou l'adresse IP du StorageZones Controller principal. Il peut se présenter sous l'une des formes suivantes et doit inclure la barre oblique de fin.

  `http://localhost/ConfigService/`

  `servername/` ou `serverip/` (si vous utilisez HTTP)

  `http[s]://servername.domain.com/ConfigService/`

  `http[s]://serverip/ConfigService/`

- la phrase secrète est celle spécifiée pour le StorageZones Controller.

- fullpath est l'emplacement et le nom du fichier de sauvegarde. Par exemple, `c:\szc-backup.bak`.

### Pour restaurer un StorageZones Controller principal sans fichier de sauvegarde

Si vous n'avez pas de fichier de sauvegarde, vous pouvez récupérer des zones et la configuration des zones de stockage pour ShareFile Data, mais pas les connecteurs de zones de stockage.

1. Définissez le contexte utilisateur pour cette session PowerShell. Dans une fenêtre de commandes, exécutez l'une des commandes suivantes.

   - Si vous utilisez le compte de service réseau par défaut :

     ```
     PsExec.exe -i -u "NT AUTHORITY\NetworkService"C:\Windows\
     SysWOW64\WindowsPowerShell\v1.0\powershell
     ```

   - Si vous utilisez un utilisateur nommé pour le pool d'applications Storage Zones Controller :

     ```
     PsExec.exe -i -u "domain\username"C:\Windows\SysWOW64\WindowsPowerShel
     \v1.0\powershell
     ```

   Une fenêtre PowerShell s'ouvre.

2. À partir de l'invite PowerShell, importez le module ConfigBR.dll : `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   Vous devez importer le module chaque fois que vous ouvrez une nouvelle fenêtre PowerShell.

3. À partir de l'invite PowerShell, exécutez la commande Join-SFConfig :

   > **Important :**
   >
   > La commande Join-SFConfig ne prend actuellement pas en charge le stockage Azure ou Amazon S3. Contactez le support ShareFile si vous devez utiliser cette commande.

   ```
   1 Join-SfConfig -ShareFileUserName "ShareFileUserName" -
       ShareFilePassword "ShareFilePassword" -subdomain "subdomain.
       sharefile.com" -ZoneId "ZoneId" -SCID "StorageCenterId" -
       Passphrase "passphrase" [-StorageZoneLocation "
       StorageZoneLocation"] [-StorageUsername "StorageUserName"] [-
       Storagepass "StoragePassword"] [-AzureAccountName "
       StorageAccount"] [-AzureSecretKey "PrimaryOrSecondaryAccessKey"
       ] [-AzureContainerName "Container"] [-S3AccessKey "S3AccessKey"
       ] [-S3SecretKey "S3SecretKey"] [-S3ContainerName "
       S3ContainerName"] [-S3EndpointAddress "S3EndpointAddress"] [-
       S3ForcePathStyle]
   ```

Où :

- ZoneID peut être obtenu comme suit :
  a) Dans l'interface Web ShareFile, cliquez sur **Admin > Zones de stockage**, cliquez avec le bouton droit sur le nom du site, puis choisissez **Propriétés**.

     L'adresse affichée se termine par l'ID de zone qui ressemble à ceci : `zae4fb8c-8520-478f-8f87-aa589a8fd181`.

  b) Copiez et collez cet identifiant dans la commande Join-SFConfig.
- StorageCenterID peut être obtenu comme suit :
  a) Dans l'interface Web ShareFile, cliquez sur Admin > zones de stockage, cliquez sur le nom du site, cliquez avec le bouton droit sur le nom d'hôte, puis choisissez Propriétés.

     L'adresse affichée se termine par l'ID de stockage qui ressemble à ceci : `scd344cf-8043-4ce2-974b-8f9cd83e2978`.

  b) Copiez et collez cet identifiant dans la commande Join-SFConfig.
- StorageZoneLocation n'est nécessaire que si les zones de stockage pour ShareFile Data sont activées pour la zone.
- StorageUserName et StoragePassword ne sont nécessaires que si les zones de stockage pour ShareFile Data sont activées pour la zone et si votre emplacement de stockage nécessite une authentification.
- AzureAccountName, AzureAccessKey et AzureContainerName ne sont nécessaires que si les zones de stockage pour ShareFile Data sont stockées dans un conteneur de stockage Windows Azure.

4. Pour récupérer des connecteurs de zones de stockage, utilisez la console Storage Zones Controller (`http://localhost/configservice/login.aspx`) pour activer et configurer les connecteurs.

## Remplacer un StorageZones Controller principal

April 19, 2021

Pour remplacer un StorageZones Controller principal par un contrôleur situé à un emplacement différent, par exemple sur un domaine différent, utilisez les procédures de sauvegarde et de restauration. Les étapes suivantes garantissent que vos paramètres de configuration et toutes vos données sont transférés.

1. Créez un fichier de sauvegarde pour la configuration de votre StorageZones Controller existante. Consultez Sauvegarde d'une configuration de StorageZones Controller principales.
2. Installez, mais ne configurez pas, un StorageZones Controller dans le nouvel emplacement réseau.
3. Importez la configuration sauvegardé sur le nouveau Controller. Consultez Restauration d'une configuration de StorageZones Controller principal.
4. Copiez vos données dans le nouveau partage réseau, connectez-vous à la console de configuration du nouveau StorageZones Controller et saisissez les nouvelles informations de chemin de stockage. Voir Transfert de fichiers vers un nouveau partage réseau.
5. Dans la nouvelle console de configuration du StorageZones Controller, mettez à jour l'URL externe du Controller. Voir Modifier l'adresse ou la phrase secrète d'un StorageZones Controller principal.

## Préparer le StorageZones Controller pour la récupération de fichiers

September 4, 2023

> **Avertissement :**
>
> La fonctionnalité de récupération ShareFile ne sauvegarde pas automatiquement votre emplacement de stockage persistant. Vous êtes responsable du choix d'un utilitaire de sauvegarde et de son exécution tous les 1 à 7 jours.

La façon dont vous vous préparez à la restauration de fichiers dépend de l'endroit où vos données sont stockées :

- **Un système de stockage tiers compatible** : si vous utilisez un système de stockage tiers avec StorageZones Controller, votre stockage tiers est redondant et aucune sauvegarde locale n'est requise. Sachez toutefois qu'un utilisateur de ShareFile qui supprime un fichier a la possibilité de récupérer le fichier à partir de la corbeille pendant une courte période. Un fichier ne peut pas être récupéré à partir de la corbeille ShareFile après 45 jours. Après la période de restauration, le fichier est supprimé de la zone et donc du stockage tiers redondant. Si ce temps de récupération n'est pas suffisant, envisagez l'une des solutions suivantes :
  - **Pour empêcher le service de nettoyage de fichiers StorageZone Controller de purger le fichier lui-même de votre emplacement de stockage sur site, modifiez la valeur du paramètre Période dans.**`C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\SCFileCleanSvc\\FileDeleteService.exe.config` Pour plus d'informations, voir Personnaliser les opérations de cache de stockage. N'

oubliez pas que l'augmentation de la durée de rétention augmente également la quantité de stockage tiers nécessaire.
  - Créez une sauvegarde locale de vos fichiers StorageZone tous les sept jours et déterminez la politique de conservation appropriée pour les sauvegardes.

- **Stockage sur site** : si vous utilisez un partage géré localement pour le stockage de données privées, vous êtes responsable de la sauvegarde des fichiers locaux et des entrées de registre du StorageZones Controller sur site. ShareFile archive les métadonnées des fichiers correspondants qui résident dans le cloud ShareFile pendant 3 ans.
  Important : Pour vous protéger contre la perte de données, il est essentiel de prendre un instantané de votre serveur StorageZones Controller, de
  sauvegarder sa configurationet de sauvegarder votre stockage de fichiers local.

Après avoir préparé votre StorageZones Controller pour la restauration de fichiers comme décrit dans cette rubrique, vous pouvez utiliser la console ShareFile Administrator pour :

- Parcourez vos zones de stockage pour rechercher des enregistrements ShareFile Data correspondant à une date et à une heure spécifiques, puis balisez les fichiers et dossiers que vous souhaitez restaurer. ShareFile ajoute les éléments balisés à une file d'attente de récupération. Vous exécutez ensuite un script de restauration pour restaurer les fichiers de votre sauvegarde vers l'emplacement de stockage persistant.

  Pour plus d'informations, consultez la section Récupérer des fichiers et des dossiers à partir de votre sauvegarde de données ShareFile.

- Réconciliez les métadonnées stockées sur le cloud ShareFile avec votre stockage sur site lorsque vous ne pouvez pas récupérer de données depuis votre stockage sur site. La fonctionnalité de réconciliation de ShareFile supprime définitivement du cloud ShareFile les métadonnées des fichiers qui ne se trouvent plus dans une zone de stockage à une date et une heure spécifiées.

  Pour plus d'informations, consultez Réconcilier le cloud ShareFile avec une zone de stockage

## Conditions préalables

- Une machine physique ou virtuelle dédiée avec 2 processeurs et 4 Go de RAM
- Windows Server 2012 R2 (Datacenter, Standard ou Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows PowerShell (versions 32 bits et 64 bits) doit prendre en charge les assemblages d'exécution .NET 4. Pour plus d'informations, reportez-vous à la section « Scripts et commandes PowerShell » dans la section Configuration système requise pour StorageZones Controller.

- PsExec.exe - PsExec vous permet de lancer PowerShell à l'aide du compte de service réseau. Vous pouvez également utiliser PsExec pour planifier des tâches de restauration. Téléchargez PsExec.exe à partir de https://docs.microsoft.com/en-us/sysinternals/downloads/psexec et suivez les instructions d'installation indiquées sur cette page.

### Récapitulatif des fichiers utilisés pour la reprise après sinistre

Les fichiers suivants, situés dans C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery, sont utilisés pour la reprise après sinistre.

| Nom du fichier | Description |
|---|---|
| DoRecovery.ps1 | Script PowerShell exécuté par le Planificateur de tâches Windows pour gérer le processus de restauration. Ce fichier contient les emplacements de sauvegarde et de stockage des fichiers. |
| Recovery.psm1 | Module PowerShell qui gère les opérations de la file d'attente de restauration. |
| recovery.log | Fichier journal qui enregistre le résultat d'un processus de restauration. |
| recoveryerror.log | Fichier journal qui enregistre les erreurs du processus de restauration. |
| LitJson.dll | Une bibliothèque .Net pour gérer les conversions depuis et vers des chaînes JSON (JavaScript Object Notation). |

### Pour configurer le dossier de sauvegarde

Sur le serveur de sauvegarde, créez le dossier dans lequel vous allez sauvegarder le dossier persistentstorage.

Les zones de stockage pour la sauvegarde des fichiers ShareFile Data doivent suivre la même disposition que le stockage persistant du StorageZones Controller.

Si votre emplacement de sauvegarde ne suit pas la même disposition que le stockage persistant du StorageZones Controller, vous devez effectuer une étape supplémentaire au cours du processus de restauration pour copier les fichiers depuis l'emplacement de sauvegarde vers l'emplacement que vous spécifiez dans le script Recovery PowerShell.

Disposition du stockage

Disposition de sauvegarde

```
\\\PrimaryStorageIP
  \StorageLocation
   \persistentstorage
    \sf-us-1
     \a024f83e-b147-437e-9f28-e7d03634af42
      \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
       \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
        \fi47cd7e_64c4_47be_beb7_1207c93c1270

\\\BackupStorageIP
 \BackupLocation
  \persistentstorage
   \sf-us-1
    \a024f83e-b147-437e-9f28-e7d03634af42
     \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
      \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
       \fi47cd7e_64c4_47be_beb7_1207c93c1270
```

> **Important :**
>
> La fonctionnalité de récupération ShareFile ne sauvegarde pas automatiquement votre emplacement de stockage persistant. **Vous êtes responsable du choix d'un utilitaire de sauvegarde et de son exécution tous les 1 à 7 jours.**

### Pour créer une file d'attente de reprise après sinistre

Cette configuration unique est requise. Les exemples de commandes suivants utilisent le dossier d'installation par défaut du StorageZones Controller.

1. Sur le StorageZones Controller, exécutez PowerShell en tant qu'administrateur.
2. Le script PowerShell utilisé dans cette procédure n'est pas signé. Vous devrez peut-être modifier votre politique d'exécution PowerShell.
   a) Déterminez si votre politique d'exécution PowerShell vous permet d'exécuter des scripts locaux non signés : PS C : \ >Get-ExecutionPolicy

      Par exemple, une stratégie RemoteSigned, Unrestricted ou Bypass vous permet d'exécuter des scripts non signés.

   b) Pour modifier votre politique d'exécution PowerShell : PS C : \ >Set-ExecutionPolicy RemoteSigned
3. Pour vérifier que PowerShell possède la version CLR correcte, tapez :

   tableau des versions de $ps

La valeur de CLRVersion doit être 4.0 ou supérieure pour permettre à PowerShell de charger des assemblages .NET dans des scripts. Si ce n'est pas le cas, modifiez-le pour les versions 32 bits et 64 bits de Windows PowerShell comme suit :

a) Exécutez NotePad en tant qu'administrateur.

b) Créez un fichier avec le contenu suivant.

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

c) Choisissez Fichier > Enregistrer sous, nommez le fichier powershell.exe.config et enregistrez-le aux emplacements suivants :

C:\Windows\System32\WindowsPowerShell\v1.0

C:\Windows\SysWOW64\WindowsPowerShell\v1.0

d) Fermez la fenêtre PowerShell, ouvrez-en une nouvelle en tant qu'administrateur et tapez $psversiontable pour vérifier que la CLRVersion est correcte.

4. Fermez la fenêtre PowerShell et lancez PowerShell à l'aide du fichier PsExec.exe comme suit :

a) Ouvrez une fenêtre d'invite de commandes en tant qu'administrateur.

b) Accédez à l'emplacement du fichier PsExec.exe et entrez :

PsExec.exe -i -u « NT AUTHORITY \ NetworkService » C:\Windows\SysWOW64\WindowsPowerShell\v1.0 powershell

c) Cliquez sur Accepter pour accepter le contrat de licence PsExec.exe.

5. Accédez au dossier Disaster Recovery tools dans le dossier d'installation du StorageZones Controller :

cd 'C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery'

6. Importez le module Recovery.psm1 :

Module d'importation. \ Récupération.psm1

7. Pour créer la file de restauration, entrez : New-SCQueue -name recovery -operation recovery

La sortie de cette commande inclut le nom de la file d'attente créée. Par exemple : la file d'attente 92736b5d-1cff-4760-92c8-d8b04dc92cb2 a été créée

Pour afficher le nouveau dossier, ouvrez un navigateur de fichiers et accédez à :

\ \ server \ (*Votre* emplacement de stockage principal) \ Queue. Vous verrez le dossier Queue, tel que 92736b5d-1cff-4760-92c8-d8b04dc92cb2.

8. Personnalisez le script PowerShell de restauration en fonction de votre emplacement, comme décrit dans la section suivante.

### Pour personnaliser le script de restauration PowerShell en fonction de votre emplacement

Le script PowerShell DoRecovery.ps1 est exécuté par le planificateur de tâches pour gérer le processus de restauration. Ce fichier inclut les emplacements de sauvegarde et de stockage des fichiers que vous devez spécifier pour votre site.

1. Sur le StorageZones Controller, accédez au script PowerShell de restauration :

   C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery \ DoRecovery.ps1

2. Modifiez le script comme suit :

   a. Définissez le paramètre $BackupRoot pour qu'il pointe vers le chemin UNC de votre emplacement de sauvegarde. *Par exemple : $backupRoot = « \ \ 10.10.11 \ (Your BackupLocation) \ persistentstorage »*

   b. Définissez le paramètre $storageRoot pour qu'il pointe vers le chemin UNC du stockage persistant de votre StorageZones Controller. Par exemple : $StorageRoot = "\\10.10.10.10\StorageLocation\persistentstorage »

### Pour tester le processus de restauration

1. Créez un fichier de test et téléchargez-le dans ShareFile.
2. Au bout d'une heure environ, vérifiez que le fichier apparaît dans le stockage persistant (dans le chemin spécifié pour $BackupRoot).
3. Supprimer le fichier de ShareFile : dans l'outil administrateur de ShareFile, cliquez sur **Corbeille**, sélectionnez le fichier, puis cliquez sur **Supprimer définitivement**.
4. Supprimez le fichier du stockage persistant.

   Cette étape recrée l'action que ShareFile exécuterait 45 jours après la suppression du fichier.

5. Dans l'outil d'administration ShareFile, accédez à **Administrateur > Zones de stockage**, cliquez sur la zone, puis sur **Récupérer des fichiers**.
6. Cliquez dans la zone de texte **Date de restauration** et sélectionnez une date et une heure avant la suppression du fichier et après son chargement.

   La liste des fichiers de la zone de stockage à la date et l'heure spécifiées s'affiche.

7. Cochez la case correspondant au fichier.
8. Sélectionnez le dossier qui doit contenir les fichiers restaurés, puis cliquez sur **Restaurer**.

   Le fichier est ajouté à la file de restauration et est prêt à être restauré. Lorsque le fichier est récupéré avec succès, l'écran change pour afficher le dossier qui contient maintenant le fichier récupéré.
9. Pour récupérer le fichier :

   a. Ouvrez une fenêtre d'invite de commandes en tant qu'administrateur.

   b. Accédez à l'emplacement du fichier PsExec.exe, puis tapez :

   ```
   ```
   PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
   ```
   ```

   c. Dans la fenêtre PowerShell, accédez à :

   cd `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

   d. Exécutez le script de restauration :

   `.\DoRecovery.ps1`

   La fenêtre PowerShell inclura le message « Élément récupéré ». Le fichier est ajouté à l'emplacement de stockage persistant.
10. Téléchargez le fichier restauré depuis le site Web de ShareFile.

### Commandes PowerShell associées

Les commandes PowerShell suivantes prennent en charge la reprise après sinistre.

- **Get-RecoveryPendingFileIds**

  Obtient la liste des identifiants de fichiers nécessaires à la restauration. Pour la syntaxe et les paramètres, utilisez la commande suivante :

  Get-Help Get-RecoveryPendingFileIds - complet

- **État des éléments de la file d'attente Set-Recovery**

  Définit le statut de tous les éléments ou de certains éléments de la file d'attente de restauration. Cela remplace l'état de restauration existant dans la file d'attente. Pour la syntaxe et les paramètres, utilisez la commande suivante :

  Get-Help Set-RecoveryQueueItemsStatus - complet

### Pour créer et planifier une tâche de restauration

Si une tâche de restauration planifiée est nécessaire, suivez les étapes ci-dessous.

1. Démarrez le planificateur de tâches Windows et dans le volet **Actions**, cliquez sur **Créer une**tâche.
2. Sous l'onglet **Général** :

   a. Entrez un nom significatif pour la tâche.

   b. Dans **Options de sécurité**, cliquez sur **Changer d'utilisateur ou de groupe**et spécifiez l'utilisateur qui exécutera la tâche, soit le service réseau, soit un utilisateur nommé disposant d'autorisations d'écriture sur l'emplacement de stockage.

   c. Dans le menu **Configurer pour**, sélectionnez le système d'exploitation du serveur sur lequel la tâche sera exécutée.
3. Pour créer un déclencheur, dans l'onglet **Déclencheurs**, cliquez sur **Nouveau**.
4. Pour **Commencer la tâche**, choisissez **Selon un calendrier**, puis spécifiez un calendrier.
5. Pour créer une action, dans l'onglet **Actions**, cliquez sur **Nouveau**.

   a. Dans **Action**, choisissez **Démarrer un programme** et spécifiez le chemin complet vers le programme. Par exemple : `C:\Windows\System32\cmd.exe`.

   b. Pour **Ajouter des arguments,** tapez : `/c "c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1" >> .\recovery.log 2>>.\recoveryerror.log`

   c. Pour **Start in**, spécifiez le dossier Disaster Recovery dans l'emplacement d'installation du StorageZones Controller. Pa exemple : `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

### Supprimer la période par défaut du service

À compter de StorageZone Controller 4.0, le délai de suppression du service sera réglé sur 45 jours. La période par défaut de 45 jours remplacera tous les paramètres précédents. Pour modifier la période par défaut, modifiez FileDeleteService.exe.config à l'adresse C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileClea

```
<!--No. of days to keep data blob in active storage after deletion-->

<add key="Period"value="45"/>
```

#### Modifier la période par défaut du service de suppression après la mise à niveau

Dans certains scénarios de mise à niveau, la valeur DeletePeriod sera définie sur null dans le fichier « FileDeleteService.exe.config ». Lorsqu'elle est définie sur null, la période de suppression est définie par défaut sur 45 jours, soit le nombre de jours par défaut avant qu'un fichier supprimé de ShareFile ne soit supprimé du stockage physique.

Pour modifier la DeletePeriod sur le StorageZones Controller, modifiez le fichier FileDeleteService.exe.config à l'emplacement suivant : `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

Lors d'une nouvelle installation du StorageZones Controller, le service de suppression s'exécute toutes les 8 heures pour nettoyer les fichiers et dossiers temporaires. Pour modifier le minuteur, modifiez le fichier FileDeleteService.exe.config à l'emplacement suivant : `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

## Récupérer des fichiers et des dossiers à partir de votre sauvegarde de données ShareFile

October 13, 2020

La console Administrateur ShareFile vous permet de parcourir vos zones de stockage pour les enregistrements ShareFile Data pour une date et une heure particulières et de marquer tous les fichiers et dossiers que vous souhaitez restaurer. ShareFile ajoute les éléments balisés à une file d'attente de récupération. Vous pouvez ensuite exécuter le script fourni pour restaurer les fichiers d'une sauvegarde vers l'emplacement de stockage.

> **Important :**
>
> Veillez à utiliser PowerShell 4.0 pour cette procédure. Pour plus d'informations sur la configuration requise pour PowerShell, consultez les
> scripts et commandes PowerShell dans
> Configuration système requise pour les StorageZones Controller.

### Conditions préalables

- Terminez la configuration et les tests décrits à la section Préparer le StorageZones Controller pour la récupération de fichiers. Le programme d'installation comprend des instructions pour créer un dossier contenant les fichiers récupérés.

1. Dans l'interface Web ShareFile, cliquez sur **Admin**, puis sur **Zones de stockage**.

2. Cliquez sur le nom de la zone, puis cliquez sur **Récupérer** les fichiers.
3. Cliquez dans la zone de texte **Date de récupération** et sélectionnez une date et une heure.

   La liste des fichiers de la zone de stockage à la date et l'heure spécifiées s'affiche.
4. Activez la case à cocher correspondant à chaque fichier à restaurer, puis cliquez sur Restaurer.
5. Sélectionnez le dossier contenant les fichiers restaurés, puis cliquez sur Restaurer.

   La liste des dossiers affiche une icône de rotation pour indiquer que la récupération est en cours.
6. Si votre emplacement de sauvegarde ne suit pas la même disposition que le stockage persistant de la zone de stockage, copiez les fichiers de l'emplacement de sauvegarde à l'emplacement spécifié lors de la modification de DoRecovery.ps1.
7. Le script PowerShell DoRecovery.ps1 n'est pas signé. Vous devrez donc peut-être modifier votre stratégie d'exécution PowerShell pour cette procédure.

   a) Déterminez si votre stratégie d'exécution PowerShell vous permet d'exécuter des scripts locaux non signés. Dans une fenêtre PowerShell : `Get-ExecutionPolicy`

      Par exemple, une stratégie RemoteSigned, Unrestricted ou Bypass vous permet d'exécuter des scripts non signés.

   b) Pour modifier votre stratégie d'exécution PowerShell : `Set-ExecutionPolicy RemoteSigned`
8. Définissez le contexte utilisateur pour cette session PowerShell. Dans une fenêtre de commandes, exécutez l'une des commandes suivantes.

   - Si vous utilisez le compte de service réseau par défaut :

     ```
     PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\
        SysWOW64\WindowsPowerShell\v1.0\powershell
     ```

   - Si vous utilisez un utilisateur nommé pour le pool d'applications du StorageZones Controller :

     ```
     PsExec.exe -i -u "domain\username" C:\Windows\SysWOW64\
        WindowsPowerShell\v1.0\powershell
     ```

   Une fenêtre PowerShell s'ouvre.
9. Récupérer le fichier :

   a) Ouvrez une fenêtre d'invite de commandes en tant qu'administrateur.

   b) Accédez à l'emplacement de PsExec.exe et entrez :

     ```
     PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\
        SysWOW64\WindowsPowerShell\v1.0\powershell
     ```

c) Dans la fenêtre PowerShell, accédez à :

```
cd C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery
```

d) Exécutez le script de récupération :

```
.\DoRecovery.ps1
```

La fenêtre PowerShell inclura le message “Item recovered”. Les fichiers récupérés sont copiés de la sauvegarde vers l’emplacement de stockage persistant. Après avoir actualisé la console, les icônes de rotation disparaissent de l’interface Web ShareFile pour les fichiers récupérés avec succès.

Si un fichier qui est supprimé de l’application Web ShareFile n’a pas encore été supprimé par le service de suppression du StorageZones Controller, le fichier se trouve toujours dans l’emplacement de stockage persistant. Dans ce cas, la récupération de fichier est immédiate et une icône de rotation n’apparaît pas dans l’interface Web ShareFile.

Si vous ne pouvez pas restaurer un fichier, reportez-vous au fichier d’aide fourni dans le dossier de reprise après sinistre.

## Réconcilier le cloud ShareFile avec une zone de stockage

October 13, 2020

Un problème, tel qu’une panne de disque, qui provoque une perte de données dans votre stockage local entraîne un état incohérent entre votre stockage local et les métadonnées stockées dans le nuage ShareFile. Vous pouvez rapprocher automatiquement ces différences afin que les métadonnées des fichiers qui ne se trouvent plus dans votre zone de stockage à une date et une heure spécifiées soient définitivement supprimées du cloud ShareFile.

> **Attention :**
>
> Effectuez une réconciliation uniquement si vous avez une perte de données irréversible dans votre stockage de fichiers local. Une réconciliation efface définitivement les métadonnées du nuage ShareFile pour tous les fichiers qui ne sont pas trouvés dans votre stockage de fichiers local à la date et l’heure spécifiées.

1. Cliquez sur **Admin**, puis sur **Zones de stockage**.
2. Cliquez sur le nom de la zone, puis cliquez sur **Réconcilier les fichiers**.
3. Cliquez dans la zone de texte **Rapprocher la date** et sélectionnez une date et une heure.
4. Cliquez sur **Réconcilier**. Une boîte de dialogue de confirmation s’affiche.

# Guide de migration vers Windows Server 2012R2 pour les zones de stockage ShareFile

November 15, 2023

> **Important :**
>
> Microsoft mettra fin au support de Windows Server 2012R2 le 10 octobre 2023. Il est important de migrer votre serveur vers une version plus récente avant la date de fin du support.

Cet article fournit des conseils sur la façon de migrer votre serveur ShareFile Storage Zone de Windows Server 2012R2 vers une version plus récente.

Pour migrer vers une version plus récente de Windows Server, vous devez ajouter un contrôleur de zone de stockage secondaire sur le nouveau serveur, puis le promouvoir en tant que contrôleur principal.

## Configuration système requise

Le serveur Storage Zones Controller prend en charge les versions suivantes :

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

## Instructions

> **Remarque :**
>
> Les étapes suivantes **NE couvrent PAS** la migration du référentiel de données ShareFile. Si le référentiel de données ShareFile se trouve sur le même serveur que le contrôleur de zone de stockage que vous prévoyez de migrer ou si vous avez un référentiel de données de zone de stockage sur un serveur de fichiers exécutant Windows Server 2012R2 à migrer, voir Transférer des fichiers vers un nouveau partage réseau pour plus d'informations.

### Étape 1 - Préparer le nouveau serveur pour le contrôleur de zone de stockage ShareFile

Préparez le nouveau serveur en suivant les étapes indiquées dans Préparer votre serveur pour les données ShareFile.

**Étape 2 - Installez le Storage Zone Controller sur le nouveau serveur et ajoutez-le en tant que périphérique secondaire**

Après avoir préparé le nouveau serveur pour ShareFile, vous devez l'ajouter à la zone de stockage en tant que serveur secondaire. Voir Joindre un StorageZones Controller secondaire à une zone de stockage pour plus d'informations.

**Étape 3 - Promouvoir le nouveau serveur en serveur principal, rétrograder l'ancien serveur en serveur secondaire**

Après avoir ajouté le nouveau serveur en tant que serveur secondaire, l'étape suivante consiste à le promouvoir au niveau principal. L'ancien serveur doit également être rétrogradé au niveau secondaire. Pour plus d'informations sur cette étape, consultez la section Rétrogradation et promotion des contrôleurs de zones de stockage.

> **Remarque :**
>
> ShareFile vous recommande de tester seul les fonctionnalités du nouveau serveur de zone de stockage, sans utiliser l'ancien serveur comme serveur secondaire. Vous pouvez le faire en désactivant temporairement l'ancien serveur. Pour plus d'informations, voir Pour désactiver un contrôleur de zone de stockage

**Étape 4 (facultatif) - Ajouter des serveurs secondaires supplémentaires**

Si nécessaire, pour chaque serveur secondaire supplémentaire, revenez à l'étape 2 - Installation du Storage Zone Controller sur le nouveau serveur et ajoutez-le en tant que serveur secondaire.

**Étape 5 (facultatif) - Mettre à jour les membres du groupe de services NetScaler**

Si vous possédez un NetScaler, assurez-vous que les nouveaux serveurs de zone de stockage sont ajoutés au groupe de services ShareFile. Pour plus d'informations, voir Ajouter des membres à un groupe de services à l'aide de l'utilitaire de configuration .

**Étape 6 - Supprimer l'ancien serveur StorageZone Controller du portail d'administration ShareFile**

Une fois que les serveurs Storage Zone ont migré avec succès, les anciens serveurs peuvent être supprimés du portail d'administration ShareFile. Pour plus d'informations, reportez-vous à la section Pour supprimer un StorageZones Controller .

# Configurer les analyses antivirus des fichiers téléchargés

June 30, 2022

> **Important :**
>
> En raison des mises à jour du code de l'application dans StorageZones 4.2, certains clients doivent mettre à jour le niveau d'autorisation de l'outil depuis l'administrateur local vers le service réseau système. Si vous ne mettez pas à jour les autorisations, les analyses antivirus ne démarreront pas.

## Exigences/Résumé

- Utilisateur utilisant StorageZones Controller 4.2 ou version ultérieure
- SFAntivirus doit être exécuté en tant que service réseau à l'aide de PsExec
- Mettre à jour l'emplacement du fichier

**Exécutez SFAntivirus en tant que service réseau à l'aide de PsExec** :

Les clients effectuant une mise à jour vers SZ 4.2 ou une version ultérieure avec des tâches planifiées existantes liées à SFAntivirus doivent modifier le niveau utilisateur auquel l'outil s'exécute, de l'administrateur local au service réseau système.

Pour obtenir des droits de service réseau, utilisez PsExec pour lancer PowerShell (x86) dans le même contexte utilisateur que le StorageZones Controller et obtenir les droits de service réseau à l'aide de la commande suivante :

```
PsExec.exe -i -u "NT AUTHORITY\NetworkService"C:\\Windows\\SysWOW64\\
WindowsPowerShell\\v1.0\\powershell
```

## Mettre à jour l'emplacement du fichier

Les administrateurs doivent également modifier l'emplacement du fichier journal en modifiant l'entrée log4net.config, s'ils se connectaient à un répertoire en dehors du répertoire journal SZC par défaut, en modifiant la ligne suivante :

```
\<file value="..\\..\\SC\\logs\\avscantool-"/\>
```

L'installation de StorageZones Controller inclut plusieurs fichiers qui prennent en charge les analyses antivirus. Les fichiers sont installés par défaut dans C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus.

Après avoir personnalisé le fichier de configuration et utilisé le Planificateur de tâches Windows pour planifier les analyses, comme décrit dans les étapes suivantes, chaque demande de téléchargement

de fichier amène le StorageZones Controller à mettre le fichier en file d'attente pour une analyse antivirus. Si des problèmes sont signalés pour un fichier analysé, la vue Dossiers inclut une icône d'avertissement pour le fichier. Si un utilisateur essaie de télécharger le fichier, un message d'avertissement s'affiche.

À partir de StorageZones Controller 4.0, l'emplacement du fichier journal de l'antivirus peut être configuré. Pour modifier l'emplacement du journal, modifiez le fichier SFAntiVirus.exe.config à l'adresse C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus.

L'analyse antivirus ne supprime pas le fichier.

L'utilisation du protocole ICAP avec les plates-formes d'analyse antivirus qui ont été codées selon la norme RFC pour ICAP est prise en charge sur StorageZones Controller 4.2 ou version ultérieure. Vous trouverez des informations sur la configuration d'un AV ICAP plus bas dans cet article.

> **Remarque :**
>
> Après avoir configuré l'antivirus sur votre zone, tous les éléments récemment téléchargés sont analysés. La configuration de l'antivirus n'est pas rétroactive. Sa configuration ne permet pas d'analyser les fichiers et les éléments qui existent déjà dans la zone.

### Pour préparer la configuration de votre site

1. Pour exécuter des analyses de virus sur un serveur autre que le StorageZones Controller :
   a) Copiez le dossier C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus sur l'autre serveur.
   b) Sur le StorageZones Controller, ouvrez C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease. et définissez QueueSDKRestricted sur 0 : `<add key="QueueSDKRestricted" value="0"/>`
2. Sur le serveur sur lequel vous exécutez des analyses de virus, modifiez SFAntiVirus.exe.config avec les valeurs de configuration de votre StorageZones Controller :
   a) Pour CommandFile : Spécifiez le chemin complet du logiciel antivirus. Ce logiciel doit résider sur le même serveur que le dossier antivirus ShareFile.
   b) Pour CommandOptions et les codes de retour : les paramètres de ligne de commande fournis dans le fichier de configuration sont un exemple. Fournissez les paramètres appropriés à votre logiciel antivirus et à votre environnement.
   c) Pour ScanFileTimeout : l'analyse des fichiers plus volumineux peut prendre plus de temps. Réglez ce paramètre en fonction des tailles de fichier attendues dans votre espace de stockage. **Dans le cas contraire, cela peut augmenter le risque qu'un fichier volumineux ne soit pas analysé.**

3. Dans une fenêtre de ligne de commande, exécutez la commande suivante pour configurer les analyses de virus : `SFAntiVirus.exe -register SFusername SFpassword`

### Utiliser ICAP pour les analyses AV au lieu des outils de ligne de commande

StorageZones Controller 5.3 et versions ultérieures prennent en charge l'utilisation du protocole ICAP avec les plates-formes d'analyse antivirus qui ont été codées selon la norme RFC pour ICAP. Les clients peuvent toujours utiliser la méthode CLI s'ils le souhaitent. Cette fonctionnalité est prise en charge pour les zones tenant à partir de StorageZones Controller 5.0.1 et versions ultérieures.

Pour activer un scanner AV ICAP sur votre StorageZone Controller, accédez à la page de configuration du StorageZones Controller.

Cochez la case **Activer l'intégration antivirus** et entrez l'adresse de votre serveur antivirus dans le champ **URL ICAP RESPMOD** . Il s'agit de l'URL du service de modification de réponse ICAP : `ICAP:` `//SERVER/RESPMOD`.

Cliquez sur **Tester la connectivité** pour confirmer votre réglage.

### Pour créer et planifier une tâche de recherche de virus

> **Remarque :**
>
> La création de tâches planifiées pour les analyses de virus n'est nécessaire que lors de l'utilisation des outils de ligne Cela n'est pas nécessaire lors de l'utilisation d'ICAP.

1. Démarrez le Planificateur de tâches Windows et, dans le volet **Actions**, cliquez sur **Créer une tâche**.
2. Sous l'onglet **Général** :
   a) Donnez un nom significatif à la tâche.
   b) Sous Options **de sécurité**, cliquez sur **Changer d'utilisateur ou de groupe**et spécifiez un utilisateur Windows pour exécuter la tâche. L'utilisateur doit disposer d'une autorisation d'accès complète sur l'emplacement de stockage.
   c) Sélectionnez **Exécuter, que l'utilisateur soit connecté ou non**. Laissez la case à cocher **Ne pas enregistrer le mot de passe** désactivée.
   d) Sélectionnez **Exécuter avec les privilèges les plus élevés**.
   e) Dans le **menu Configurer pour**, sélectionnez le système d'exploitation du serveur sur lequel la tâche sera exécutée.
3. Pour créer un déclencheur : Dans l'onglet **Déclencheurs**, cliquez sur **Nouveau**. Ensuite, pour **Commencer la tâche**, choisissez **Selon un calendrier** et spécifiez un calendrier.

4. Pour créer une action : Dans l'onglet **Actions**, cliquez sur **Nouveau**.

   a) Pour **Action**, choisissez **Démarrer** un programme et spécifiez le chemin complet du programme. Par exemple :

   `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus\\SFAntiVirus.exe`

   b) Pour Démarrer dans, spécifiez l'emplacement du fichier SFAntiVirus.exe : `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`

5. Dans l'onglet **Paramètres**, pour **Si la tâche est déjà en cours d'exécution**, la règle suivante s'applique, sélectionnez **Ne pas démarrer une nouvelle instance**.

## Intégration de la ligne de commande AV dans Scan Service

### Conditions préalables

- Avant d'installer ou de mettre à niveau StorageZones Controller 5.2, assurez-vous d'arrêter ou de supprimer l'AV de ligne de commande existant s'il s'exécute en tant que tâche planifiée ou cron.
- Installez .NET 4.6.2 (ou version ultérieure) sur une machine hôte.

Le service d'analyse du StorageZones Controller sur site inclut la prise en charge de l'utilisation d'un outil AV en ligne de commande, tel que l'analyse AV en ligne de commande Symantec. En outre, le service d'analyse fournit des analyses avec les produits antivirus pris en charge par ICAP.

Pour activer cette fonctionnalité, ajoutez la clé et la valeur de configuration suivantes dans le fichier Antivirus/OnPrem/AVScanService/AppSettings.config

```
<add key="use-command-line-av"value="true"/>
```

### Configuration spécifique à l'outil de ligne de commande

La mise à niveau ou la nouvelle installation de StorageZones Controller 5.2 inclut un nouveau fichier de configuration :

`AntiVirus/OnPrem/AVScanService/AVScanService/avCommandLineSettings.json`

Ce fichier gère les paramètres nécessaires pour la ligne de commande AV.

Les valeurs de clé de configuration sont expliquées ci-dessous avec des exemples de valeurs inclus.

- Définissez ce point sur votre application de ligne de commande.

  `"command-file": "c:\\\\\vscan\\\\\scan.exe"`

- Consultez la documentation de l'application de ligne de commande pour connaître les options ou les commutateurs qu'elle prend en charge, puis ajoutez-les à cet emplacement.

  ```
  "command-options": "/ALL /ANALYZE /MIME /NOMEM /NORENAME /SECURE
  ",
  ```

- Incluez les valeurs de sortie qui indiquent une analyse propre.

  ```
  "scanner-codes-for-clean-file": "0, 19",
  ```

- Incluez des valeurs de sortie indiquant un fichier infecté.

  ```
  "scanner-codes-for-infected-file": "12, 13",
  ```

- Incluez des valeurs de sortie indiquant des fichiers non analysés.

  ```
  "scanner-codes-for-notscanned-file": "2, 6, 8, 15, 20, 21, 102"
  ```

#### Remarques sur l'application de la taille maximale des fichiers, à l'exception des

Avant la version 5.2, vous ne pouviez pas appliquer l'exclusion d'extension ou l'application de la taille maximale des fichiers sur l'AV en ligne de commande. Vous ne pouviez le faire que sur le service d'analyse ICAP. Avec la version 5.2, les mêmes paramètres que ceux appliqués au service d'analyse ICAP concernant les extensions exclues et la taille maximale des fichiers en octets s'appliquent au service de ligne de commande AV.

Ces paramètres ont été nommés comme suit :

```
<add key="icap-exclude-extensions"value=""/>
```

```
<add key="icap-max-file-size-bytes"value="0"/>
```

Une nouvelle installation de StorageZones Controller 5.2 renomme ces paramètres comme suit. Les paramètres renommés reflètent le fait qu'ils sont applicables à la fois à l'AV basé sur ICAP et à l'AV en ligne de commande.

```
<add key="exclude-extensions"value=""/>
```

```
<add key="max-file-size-bytes"value="0"/>
```

Lors d'une mise à niveau, ces paramètres ne sont pas renommés. Bien que les renommages manuels fonctionnent, les mêmes paramètres fonctionneraient également pour la ligne de commande AV en plus d'ICAP.

```
<add key="icap-exclude-extensions"value=""/>
```

```
<add key="icap-max-file-size-bytes"value="0"/>
```

# Migrer les données ShareFile

August 4, 2023

Il existe plusieurs façons de migrer des données ShareFile d'une zone locale vers une autre.

- Migrer via le portail Web ou User Management Tool
- Migrer via PowerShell Script
- Migrer via ZoneFix Tool

## Conditions préalables

- Assurez-vous que la zone source est accessible depuis la zone de destination et débloquez les connexions sortantes vers le centre de stockage source.
- Pour tester la connexion entre les zones, accédez à l'adresse externe de la zone source en accédant à celle-ci dans un navigateur de la zone de destination. Si la connexion est établie, le logo ShareFile apparaît.

## Migrer via le portail Web ou User Management Tool

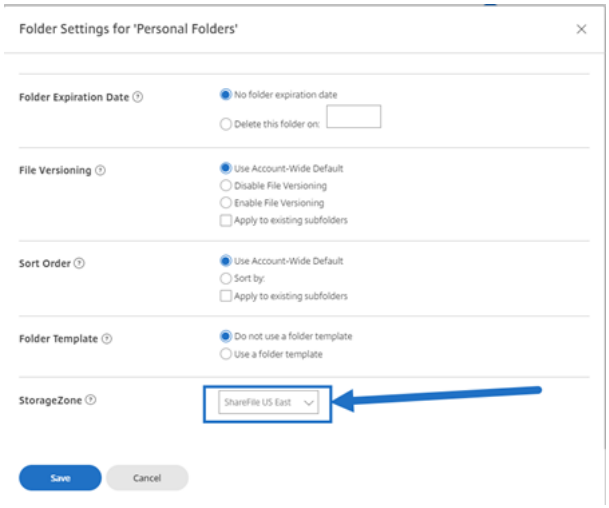
Dans l'application Web ShareFile, vous pouvez lancer la migration des données entre les zones pour un utilisateur individuel ou pour un dossier spécifique.

> **Important :**
>
> L'enregistrement des modifications suivantes déclenche immédiatement une opération de migration asynchrone pour télécharger les fichiers existants vers la nouvelle zone. Les nouveaux fichiers chargés dans le dossier au cours de cette période de migration sont transférés vers la nouvelle zone.

**Migrer les données d'un utilisateur spécifique** : accédez à **Personnes**, puis localisez l'utilisateur **Employé** . Cliquez sur l'utilisateur pour afficher sa page de profil. Sous **Emplacement de stockage**, sélectionnez une nouvelle zone (si elle a déjà été installée et configurée).

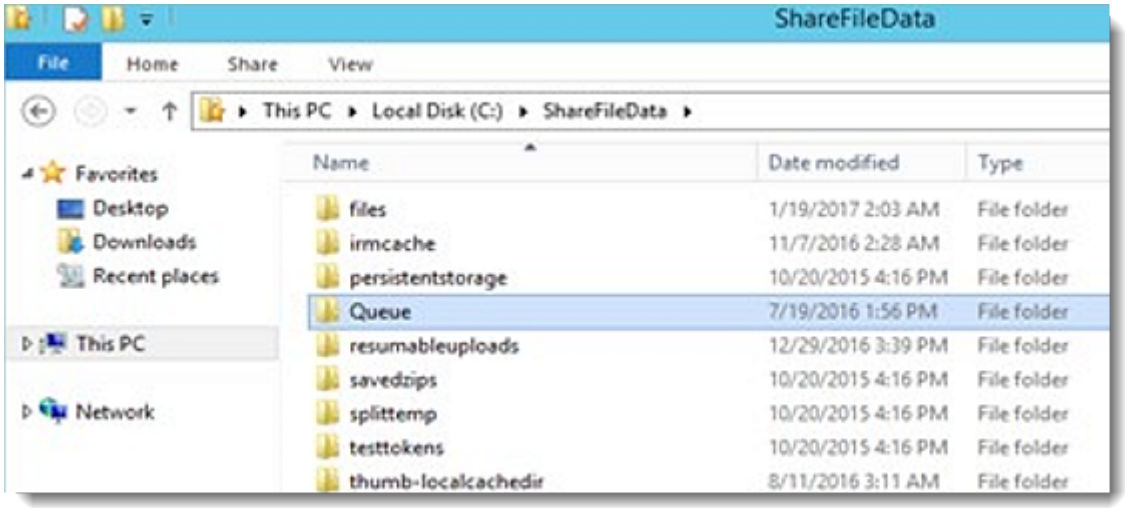
**Migrer les données d'un dossier spécifique** : accédez au dossier et accédez au menu **Plus d'options** situé à droite du nom du dossier. Cliquez sur **Paramètres avancés des dossiers**. Dans le menu, sélectionnez une nouvelle zone.




## Processus de migration

Tout d'abord, les fichiers mis en file d'attente pour la migration créent un fichier d'espace réservé dans un dossier File **d'attente** situé dans l'**emplacement de stockage** de la zone d'origine.

Une fois le fichier d'espace réservé traité avec succès, le fichier migré est supprimé de `persistentstorage` de la zone d'origine et ajouté à la zone `persistentstorage` de la nouvelle zone.



### Migrer via PowerShell

Le SDK ShareFile PowerShell permet aux utilisateurs de télécharger de grandes structures de dossiers à partir de leur emplacement de zone d'origine et de télécharger ces dossiers dans une nouvelle zone.

**Exigences** : PowerShell 4+ et .NET 4.x+ sont nécessaires pour exécuter et installer le SDK. PowerShell 5.x peut être téléchargé ici dans le cadre de Windows Management Framework 5.1.

### Migrer via l'outil Zone Fix

L'outil Correction de zone est un outil de ligne de commande. Écrit par des développeurs de zones de stockage, l'outil exploite l'API ShareFile pour cibler les ID de dossier en vue de la migration vers une zone spécifique.

Pour des performances optimales, cette méthode est recommandée pour les dossiers dont la taille est inférieure à 2 Go.

## Favoris du connecteur

February 14, 2022

À partir de Storage Zones Controller 5.0, les utilisateurs peuvent créer des dossiers de connecteurs en tant que favoris sous **Partages réseau**, **Connecteurs**SharePoint**et Documentum** dans la WebApp ShareFile. Pour plus de détails, consultez cet articledu centre de connaissances du support Citrix.

L'ajout d'un dossier de connecteur à vos favoris est pris en charge sur ShareFile Mobile.

## Gérer les zones de stockage pour les données ShareFile

November 15, 2023

Vous pouvez utiliser des zones de stockage pour ShareFile Data avec ou à la place du cloud géré par ShareFile.

> **Remarque :**
>
> Si vous supprimez un StorageZone Controller principal, rétrogradez-le avant de continuer. Pour plus d'informations, consultez Rétrograder et promouvoir les contrôleurs de zone de stockage.

### Déplacer les dossiers personnels et les boîtes de fichiers entre les zones

Procédez comme suit pour déplacer les dossiers de base et les boîtes de fichiers d'une zone à l'autre. Vous pouvez également utiliser l'ShareFile User Management Tool pour migrer les utilisateurs entre les zones.

1. Cliquez sur **Accueil**, puis accédez au dossier.
2. Dans le volet de navigation droit, cliquez sur **Modifier les options des dossiers**.
3. Dans le menu de la zone de stockage, sélectionnez une zone, puis cliquez sur **Enregistrer**.

### Création d'un dossier dans une zone de stockage

1. Cliquez sur **Accueil**, puis sur **Dossiers**.
2. Dans l'onglet **Dossier**, cliquez sur **Ajouter un dossier**.
3. Spécifiez les informations du dossier. Dans **Storage Site**, sélectionnez la zone de stockage dans laquelle vous souhaitez stocker ce dossier et son contenu.
4. Cliquez sur **Créer un dossier**.
5. Configurez le dossier comme d'habitude. Lorsque vous créez un dossier, vous pouvez choisir d'utiliser le stockage cloud géré par ShareFile ou votre zone de stockage local.

### Renommer ou supprimer une zone de stockage

> **Important :**
>
> Avant de supprimer une zone de stockage, sauvegardez-la. La suppression d'une zone efface tous les fichiers et dossiers de cette zone et vous ne pouvez pas annuler l'opération.

1. Cliquez sur **Admin**, puis sur **Zones de stockage**.
2. Cliquez sur le nom de la zone.
   - Pour renommer la zone : Cliquez sur **Modifier la zone**, saisissez un nouveau nom, puis cliquez sur **Enregistrer les modifications**.
   - Pour supprimer la zone : Cliquez sur le nom de la zone, puis sur **Supprimer la zone**.

#### Limitations

Les contrôleurs de zone de stockage ne peuvent pas être renommés/supprimés si :

- **La migration des données ShareFile est en cours** : terminez la migration des données avant de tenter de supprimer la zone de stockage.
- Des**données ShareFile existent dans la zone** : migrez ou supprimez toutes les données existantes avant de tenter de supprimer la zone de stockage.

### Personnaliser les opérations de mémoire cache

Les demandes des utilisateurs de ShareFile sont gérées à l'aide du StorageZones Controller. Cela inclut : les chargements, les téléchargements et les suppressions de fichiers. Le contrôleur de zones de stockage communique ensuite avec le stockage connecté. Par exemple, si le stockage connecté est un système de stockage tiers pris en charge et qu'un utilisateur ShareFile télécharge un fichier, le client ShareFile envoie le fichier au cache de stockage persistant. Storage Zones Controller télécharge ensuite le fichier sur le système de stockage tiers.

Storage Zones Controller gère le cache de stockage persistant à l'aide des paramètres configurables dans `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`. Les paramètres spécifiques à un système de stockage tiers pris en charge sont décrits dans cette discussion.

Pour les fichiers téléchargés :

- Storage Zones Controller place les fichiers téléchargés dans un cache de stockage persistant (le dossier PersistentStorage).
- Les paramètres suivants contrôlent la durée des opérations de suppression du service :
  - `MinDeletionAge` spécifie l'intervalle de temps minimum entre le dernier accès à un fichier et le moment où il peut être supprimé. La valeur par défaut est 1 jour. Le réglage minimum est de 8 heures.
  - `OffPeakTimeOfDayStart` et `OffPeakTimeOfDayEnd` spécifiez les heures de début et de fin de la suppression du fichier. Par défaut, 2 h et 4 h du matin.
  - `ProducerTimerInterval` et `DeleteTimerInterval` contrôlez la fréquence des opérations de service de suppression. Veuillez contacter le support technique si les valeurs par défaut (1 jour) ne conviennent pas à votre site.
- Les services de suppression gèrent également les dossiers contenant des éléments temporaires tels que des clés de chiffrement et des fichiers en file d'attente. Le service de suppression supprime ces éléments 24 heures après leur création.
- Pour les systèmes de stockage tiers pris en charge uniquement :
  - Le service de suppression détermine si un fichier du cache de stockage possède un objet blob correspondant dans le stockage tiers pris en charge.
  - Par défaut, toutes les 10 secondes (`CheckSizeThreasholdTimer`), le service de suppression détermine si le cache de stockage a dépassé un seuil de disque de 10 Go (`DiskSpaceDropoutThresholdGB`). Si le seuil est dépassé, le service de suppression supprime les fichiers qui n'ont pas été consultés au cours de la dernière heure (`CacheCleanupFileThreasholdPeriodUnExpected`). Le service de suppression s'exécute dans le cadre d'une planification normale (et non parce que la taille du disque a atteint le seuil). Le service supprime les fichiers qui n'ont pas été consultés au cours

des dernières 24 heures (`CacheCleanupFileThresholdPeriodNormal`) si le blob se trouve dans un stockage tiers compatible. Si le blob ne se trouve pas dans le stockage tiers, le fichier reste dans le cache de stockage.

Pour les fichiers téléchargés :

- Lorsque Storage Zones Controller reçoit une demande de téléchargement, il télécharge le fichier à partir du cache de stockage persistant si le fichier s'y trouve. Si le fichier ne se trouve pas dans ce cache, le contrôleur télécharge le fichier du système de stockage tiers vers le cache de stockage persistant. Le service de suppression supprime les fichiers qui n'ont pas été consultés au cours des dernières 24 heures (CacheCleanUpFileThresholdPeriodNormal).

Pour les fichiers supprimés :

- Le service de suppression obtient de l'application ShareFile une liste des fichiers qui ont été supprimés il y a 45 jours (période).
- Le service de suppression supprime ensuite les fichiers correspondants de l'emplacement de stockage ou les objets correspondants du stockage tiers.

### Période par défaut de suppression du service

Le délai de suppression du service est réglé sur 45 jours. La période par défaut de 45 jours remplace tous les paramètres précédents.

> **Remarque :**
>
> Si le délai de suppression est configuré pour être inférieur à 45 jours, veuillez contacter le support technique pour réduire le nombre de jours pendant lesquels les articles sont affichés dans la **corbeille** afin que les deux délais soient égaux.

1. Pour modifier la période par défaut, modifiez FileDeleteService.exe.config à l'adresse `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`
   - `<!--No. of days to keep data blob in active storage after deletion-->`
   - `<add key="Period"value="45"/>`

## Création et gestion de StorageZone Connector

April 19, 2021

Les StorageZone Connector permettent d'accéder aux documents et aux dossiers dans :

- Sites, collections de sites et bibliothèques de documents SharePoint
- Partages de fichiers réseau
- Connecteur Documentum (nécessite SZC 4.1 ou version ultérieure)

Les utilisateurs autorisés à afficher une ressource connectée peuvent parcourir les sites SharePoint connectés, les bibliothèques SharePoint et les partages de fichiers réseau à partir de l'interface Web ShareFile et des clients ShareFile.

Par défaut, la navigation du connecteur est désactivée pour l'interface Web ShareFile. Pour activer la navigation du connecteur, contactez le support ShareFile.

Des paramètres supplémentaires sont disponibles pour permettre aux utilisateurs de spécifier le Controller de domaine à utiliser pour les recherches Active Directory. Veuillez vous référer à la section Authentification de cet article. Ce paramètre nécessite SZ 4.1 ou une version ultérieure.

Configuration système requise pour le connecteur

Les connecteurs de zone de stockage ne prennent pas en charge le partage de documents ou la synchronisation de dossiers entre appareils.

**Les connecteurs doivent avoir un nom d'affichage unique**. Les utilisateurs ne sont pas autorisés à utiliser un nom de connecteur actuellement utilisé ailleurs sur le compte.

## Autorisations pour créer des StorageZone Connector

Pour créer et gérer des connecteurs, votre utilisateur Admin ou Employé **doit disposer des autorisations suivantes** :

- **Créer et gérer des connecteurs**
- **Créer des dossiers de niveau racine**

## Pour créer un StorageZone Connector pour SharePoint

### Conditions préalables

- Si vous utilisez des zones de stockage pour les données ShareFile, créez la zone à utiliser pour le connecteur.

Les étapes suivantes décrivent comment créer un StorageZone Connector à partir de l'interface Web ShareFile. Les utilisateurs ShareFile peuvent également créer un connecteur à partir de périphériques pris en charge en tapant l'URL du site SharePoint.

1. Connectez-vous à votre compte ShareFile en tant qu'administrateur avec l'autorisation Créer et gérer des connecteurs.

2. Accédez à **Paramètres d'administration > Connecteurs**.
3. Cliquez sur **Ajouter** pour le type de connecteur SharePoint.
4. Si vous utilisez des zones de stockage pour ShareFile Data, choisissez une zone pour le connecteur.

   La zone d'un connecteur doit être dans le même domaine que le serveur SharePoint ou doit avoir une relation d'approbation avec lui. Si vous avez des serveurs SharePoint dans plusieurs domaines et que vous ne pouvez pas configurer les approbations entre les domaines, créez un StorageZones Controller pour chaque domaine.
5. Pour Site, spécifiez l'URL d'un site de niveau racine, d'une collection de sites ou d'une bibliothèque de documents SharePoint dans les formulaires suivants.

   - Exemple de connexion à un site de niveau racine SharePoint : `https://sharepoint.company.com`

     Une connexion à un site de niveau racine permet aux utilisateurs d'accéder à tous les sites (mais pas aux collections de sites) et aux bibliothèques de documents au niveau racine. ShareFile masque les dossiers système SharePoint aux utilisateurs.
   - Exemple de connexion à une collection de sites SharePoint : `https://sharepoint.company.com/site/SiteCollection`

     Une connexion à une collection de sites permet aux utilisateurs d'accéder à tous les sous-sites de cette collection.
   - Exemple de connexion à une bibliothèque de documents SharePoint 2010 :

     - `https://mycompany.com/sharepoint/`
     - `https://mycompany.com/sharepoint/sales-team/Shared Documents/`
     - `https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx`
   - Exemple de connexion à une bibliothèque de documents SharePoint 2013 :

     L'URL par défaut de SharePoint 2013 (lorsque la stratégie de téléchargement minimal est activée) se présente au format suivant : `https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`.
   - Exemple de connexion qui redirige vers le nom NetBIOS d'un utilisateur authentifié :

     Utilisez la variable%USERDomain% pour remplacer le nom d'ouverture de session de l'utilisateur authentifié par le nom NetBIOS de cet utilisateur. La nouvelle variable vous permet de créer un connecteur au niveau du site vers une URL telle que `https://example.com/%UserDomain%\\_%UserName%/Documents`.

- Exemple de connexion lors de la connexion à « Mon site » ou OneDrive Entreprise :

  Utilisez la variable `%URLusername%` pour résoudre automatiquement les caractères spéciaux sélectionnés lors de la connexion à des sites personnels SharePoint. Cette variable remplace les espaces par%20 et les points par les traits de soulignement. L'utilisation de la `%URLusername%` variable nécessite SZ v3.4.1.

  Si le « domainusername » de l'utilisateur est « acme\rip.van winkle » alors

  `https://sharepoint.acme.com/personal/%URLusername%`
  sera résolu en :
  `https://sharepoint.acme.com/personal/rip van%20winkle`

6. Tapez un nom convivial pour le connecteur.

   Le nom est utilisé pour identifier le site SharePoint aux utilisateurs. Le nom doit être bref afin qu'il s'affiche correctement sur les appareils mobiles avec de petits écrans.

7. Cliquez sur **Ajouter un connecteur**. La boîte de dialogue **Afficher/Modifier l'accès au dossier** s'affiche.

8. Pour rendre les connecteurs visibles pour les autres : dans Afficher/Modifier l'accès aux dossiers, ajoutez des utilisateurs et des groupes de distribution, puis cliquez sur **Enregistrer les modifications**.

   Cette étape détermine uniquement si un connecteur est visible pour les utilisateurs. **Les StorageZone Connector héritent des autorisations d'accès du serveur SharePoint.**

### Pour activer le balisage des métadonnées SharePoint

Lors de la configuration du StorageZones Controller, assurez-vous que les connecteurs SharePoint sont activés.

Le balisage des métadonnées est pris en charge pour SharePoint 2013 et les clients mobiles ultérieurs.

> **Note :**
>
> Pour `en-us` seulement.

### Pour créer un StorageZone Connector pour les partages de fichiers réseau

#### Conditions préalables

- Si vous utilisez des zones de stockage pour les données ShareFile, créez la zone à utiliser pour le connecteur.

- Pour que les connecteurs de partage réseau fonctionnent avec les dernières versions des navigateurs Chrome, Edge et Firefox, appliquez la dernière mise à jour .NET pour votre environnement. Pour de plus amples informations, consultez la section Articles de base de connaissances qui prennent en charge SameSite dans .NET Framework. Appliquez ceci à tous vos connecteurs de zone de stockage. Ceci est nécessaire pour permettre à l'attribut SameSite d'être configuré pour les cookies en tenant compte de la dernière version des navigateurs.
- Si vous utilisez la version 5.10.1 ou inférieure, ajoutez `<httpCookies sameSite="None" requireSSL="true" /` dans la `<system.web>` balise du fichier C:\inetpub\wwwroot\Citrix\StorageCen dans tous les connecteurs de zone de stockage. Ceci est nécessaire pour permettre à l'attribut SameSite d'être configuré pour les cookies en tenant compte de la dernière version des navigateurs.

Les étapes suivantes décrivent comment créer un connecteur à partir de l'interface Web ShareFile. Les utilisateurs ShareFile peuvent également créer un connecteur à partir de périphériques pris en charge en tapant le chemin d'accès d'un partage de fichiers.

1. Connectez-vous à votre compte ShareFile en tant qu'administrateur avec l'autorisation Créer et gérer des connecteurs.
2. Accédez à **Paramètres d'administration > Connecteurs**.
3. Cliquez sur **Ajouter** pour le type de connecteur Partage réseau.
4. Si vous utilisez des zones de stockage pour ShareFile Data, choisissez une zone pour le connecteur.

   La zone d'un connecteur doit être dans le même domaine que le partage de fichiers ou doit avoir une relation d'approbation avec lui. Si vous avez des partages de fichiers dans plusieurs domaines et que vous ne pouvez pas configurer les approbations entre les domaines, créez un StorageZones Controller pour chaque domaine.
5. Dans Path, tapez le chemin UNC.

   Exemple avec FQDN : \\fileserver.acme.com\shared

   Vous pouvez utiliser les variables suivantes dans le chemin UNC :

   - %UserName%

     Redirige vers le répertoire personnel d'un utilisateur. Exemple de chemin d'accès : \\myserver\homedirs\%UserName%
   - %HomeDrive%

     Redirige vers le chemin d'accès du dossier d'accueil d'un utilisateur, tel que défini dans la propriété Répertoire d'accueil Active Directory. Chemin d'accès d'exemple :%HomeDrive%

- %TSHomeDrive%

  Redirige vers le répertoire d'accueil des services Terminal Server d'un utilisateur, tel que défini dans la propriété Active Directory ms-TS-Home-Directory. L'emplacement est utilisé lorsqu'un utilisateur ouvre une session sur Windows à partir d'un serveur Terminal Server ou Citrix XenApp Server. Exemple de chemin : %TSHomeDrive%

  Dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, la valeur de répertoire ms-TS-Home-Directory est accessible dans l'onglet Profil des services Bureau à distance lors de la modification d'un objet utilisateur.

- %UserDomain%

  Redirige vers le nom de domaine NetBIOS de l'utilisateur authentifié. Par exemple, si le nom d'ouverture de session de l'utilisateur authentifié est "abc\johnd", la variable est remplacée par "abc". Exemple de chemin d'accès : \\myserver\%UserDomain%_%UserName%

Les variables ne sont pas sensibles à la casse.

Important : ne créez pas de connecteur à l'emplacement de stockage ShareFile Data. En fonction des autorisations utilisateur, cela peut permettre aux utilisateurs de supprimer toutes les données ShareFile.

6. Tapez un nom convivial pour le connecteur.

   Le nom est utilisé pour identifier le partage de fichiers pour les utilisateurs. Le nom doit être bref afin qu'il s'affiche correctement sur les appareils mobiles avec de petits écrans.

7. Cliquez sur Ajouter un connecteur. La boîte de dialogue Afficher/Modifier l'accès aux dossiers s'affiche.

8. Pour rendre les connecteurs visibles par d'autres : dans Afficher/Modifier l'accès aux dossiers, ajoutez des utilisateurs et des groupes de distribution, puis cliquez sur Enregistrer les modifications.

   Cette étape détermine uniquement si un connecteur est visible pour les utilisateurs. **Les StorageZone Connector héritent des autorisations d'accès du partage réseau. Les autorisations d'accès en lecture/écriture sont déterminées par les paramètres de sécurité du partage réseau et sont également affectées par le plan ShareFile.**

## Pour activer l'archivage et l'extraction de fichiers pour les partages de fichiers réseau

### Conditions préalables

La version 5.8 du StorageZones Controller et le connecteur de partage de fichiers réseau doivent être configurés.

### Étapes

1. Connectez-vous au centre de stockage. La page de configuration s'affiche.
2. Cliquez sur **Modifier** dans la page de configuration.
3. Activez la case à **cocher Activer l'archivage et l'extraire pour les partages de fichiers réseau**.
4. Tapez le nom du domaine où se trouvent les utilisateurs et les partages réseau.
5. Tapez le nom d'utilisateur et le mot de passe du compte de service. Ce compte de service doit disposer d'un accès en lecture et en écriture sur tous les fichiers et dossiers présents dans l'emplacement de partage réseau.

## Pour créer un StorageZone Connector pour Documentum

> **Remarque :**
>
> Seule l'authentification de base est prise en charge pour la configuration du connecteur Documentum. Documentum Content Server est sensible à la casse, de sorte que le nom d'utilisateur saisi lors de l'authentification doit correspondre aux informations d'identification sensibles à la casse, sauf si la sensibilité à la casse est désactivée sur le serveur de contenu Documentum.

### Conditions préalables

1. Controller de zones de stockage 5.3 ou ultérieur
2. Paramètre ECM Documentum activé par le support client ShareFile.
3. Le service Documentum Rest doit être déployé sur votre serveur Documentum. Cliquez ici pour plus d'informations sur le service Documentum Rest.
4. Si vous utilisez Citrix ADC, certaines modifications de configuration sont nécessaires. Ces changements sont détaillés plus loin dans cet article.

Une fois cette fonctionnalité activée par le service clientèle ShareFile, accédez à votre Controller de zone de stockage et recherchez le menu du connecteur de zones de stockage. Cochez la case « Activer l'accès aux sources de données ECM (Enterprise Content Management) existantes ». Enregistrez vos modifications.

Ensuite, connectez-vous à l'application Web ShareFile et accédez à **Paramètres d'administration > Connecteurs.**

Cliquez sur le bouton **Ajouter** en regard du type de connecteur Documentum.

Spécifiez le chemin d'accès de votre serveur EMC et entrez un nom pour votre connecteur. Continue.

Ensuite, accordez aux utilisateurs l'accès au connecteur Documentum.

Une fois le connecteur créé, vous pouvez y accéder à partir du Web et des applications mobiles.

#### Actions supportées

Mobile (iOS/Android/Universal Windows Platform) :

- Navigation
- Chargements/Téléchargements de fichiers
- Création/Suppression de fichiers et de dossiers
- Modification hors ligne

WebApp

- Création du connecteur
- Navigation
- Chargements/Téléchargements de fichiers
- Création/Suppression de dossiers

#### Non pris en charge

- Partage de fichiers stockés dans un connecteur Documentum
- Liste blanche et liste noire des chemins

> **Remarque :**
>
> Documentum Content Server est sensible à la casse, de sorte que le nom d'utilisateur saisi lors de l'authentification doit correspondre aux informations d'identification sensibles à la casse, sauf si la sensibilité à la casse est désactivée sur le serveur de contenu Documentum.

### Configuration Citrix ADC pour le connecteur Documentum

Si vous utilisez un Citrix ADC avec votre environnement, apportez les modifications suivantes à votre configuration Citrix ADC :

1. Ajoutez les éléments suivants à la stratégie _SF_CIFS_SP sous Changement de contenu > Stratégies :

   ```
   HTTP.REQ.URL.CONTAINS("/cifs/")|| HTTP.REQ.URL.CONTAINS("/sp/")||
    HTTP.REQ.URL.CONTAINS("/documentum/")|| HTTP.REQ.URL.CONTAINS("/
   ProxyService/")
   ```

2. Ajoutez les éléments suivants à la stratégie _SF_SZ_CSPOL sous Changement de contenu > Stratégies :

   ```
   HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("/sp
   /").NOT && HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT && HTTP.
   REQ.URL.CONTAINS("/documentum/").NOT
   ```

#### Pour modifier le nom d'un connecteur

Un nom de connecteur est utilisé pour identifier un site SharePoint ou un partage de fichiers réseau pour les utilisateurs.

1. Connectez-vous à votre compte ShareFile en tant qu'administrateur, puis cliquez sur l'onglet Connecteurs.
2. Dans la colonne **Titre**, cliquez sur le nom du connecteur.
3. Tapez un nom convivial pour le connecteur, puis cliquez sur **Enregistrer**.

#### Pour supprimer un connecteur

La suppression d'un connecteur ne supprime pas les données de SharePoint ou d'un partage de fichiers réseau.

1. Connectez-vous à votre compte ShareFile en tant qu'administrateur, puis cliquez sur l'onglet Connecteurs.
2. Activez la case à cocher correspondant au connecteur, cliquez sur **Supprimer**, puis cliquez sur **OK**.

### authentification des connecteurs

Les utilisateurs d'administration peuvent désormais utiliser le paramètre suivant pour spécifier le Controller de domaine à utiliser lors de recherches AD pour l'authentification CIFS ou SP.

```
<add key="Domaincontrollers"value="DC01,dc02.domain.com,123.456.789.1
"/>
```

La valeur « Valeur= » ci-dessus peut être définie sur un contrôleur de domaine unique ou plusieurs contrôleurs de domaine identifiés par le nom d'hôte, le nom de domaine complet ou l'adresse IP. Plusieurs contrôleurs de domaine doivent être séparés par des virgules ou des points-virgules.

Si plusieurs contrôleurs de domaine sont spécifiés, la recherche sera exécutée sur le premier contrôleur de domaine. Si une erreur se produit, le second contrôleur de domaine est utilisé, et ainsi de suite.

La propriété ci-dessus peut être ajoutée à `C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config` afin qu'elle soit héritée par toutes les applications IIS du StorageZones Controller (y compris CIFS, SP et ProxyService).

Si le nouveau paramètre d'application n'est pas présent, le comportement par défaut de sélection automatique d'un contrôleur de domaine continue.

### Obtenir un lien direct à partir des connecteurs Partager réseau/SharePoint

Les utilisateurs peuvent désormais « Obtenir un lien direct » à partir des connecteurs Partager réseau/SharePoint tout en utilisant la dernière version de l'application ShareFile pour iOS ou Android.

Si l'administrateur souhaite désactiver cette fonctionnalité, il peut le faire en ajoutant :

```
<add key="disable-direct-link"value="1"/>
```

Ce qui précède peut être ajouté à `C:\inetpub\wwwroot\Citrix\StorageCenter\sps\AppSettingsRelease.config`.

### Authentification de base et noms d'utilisateurs localisés

L'authentification de base ne prend pas en charge les caractères non-ASCII. Si vous utilisez des noms d'utilisateurs localisés, il est suggéré aux utilisateurs d'utiliser NTLM et Negotiate.

## Protection contre la perte de données

May 28, 2024

Les fonctionnalités de prévention contre la perte de données (DLP) de ShareFile vous permettent de restreindre l'accès et le partage en fonction du contenu d'un fichier.

Vous pouvez numériser les documents chargés dans votre zone de stockage à l'aide de n'importe quelle suite de sécurité DLP tierce qui prend en charge le protocole réseau ICAP, un protocole réseau standard pour l'analyse de contenu en ligne. Vous ajustez ensuite les privilèges de partage et d'accès en fonction des résultats de l'analyse DLP et de vos préférences quant à la rigueur avec laquelle vous souhaitez contrôler l'accès.

### Systèmes DLP pris en charge

Storage Zones Controller utilise le protocole ICAP pour interagir avec des solutions DLP tierces. L'utilisation de ShareFile avec une solution DLP existante ne nécessite aucune modification des stratégies ou des serveurs existants. Toutefois, vous souhaiterez peut-être dédier des serveurs ICAP au traitement des données ShareFile si vous pensez que la charge sera importante.

Les solutions DLP conformes à la norme ICAP les plus populaires incluent :

- Prévention de la perte de données Symantec
- McAfee DLP Prevent

- Websense TRITON AP-DATA

Comme ShareFile utilise votre suite de sécurité DLP existante, vous pouvez gérer un point unique de gestion des stratégies pour l'inspection des données et les alertes de sécurité. Si vous utilisez déjà l'une des solutions précédentes pour analyser les pièces jointes des e-mails sortants ou le trafic Web à la recherche de données sensibles, vous pouvez pointer le ShareFile StorageZones Controller vers le même serveur. Pour ces systèmes DLP existants, nous prenons également en charge l'ICAP sécurisé (ICAPS) si le système DLP sous-jacent prend lui-même en charge l'ICAPS.

### Activer le DLP

Pour activer la DLP pour ShareFile et StorageZones Controller, effectuez les trois actions suivantes :

1. Activez les fonctionnalités DLP sur votre compte ShareFile.
2. Activez la DLP sur votre serveur StorageZones Controller.
3. Configurez les actions autorisées pour chaque classification de fichiers.

Ces actions sont décrites en détail dans les sections suivantes.

### Activez les fonctionnalités DLP sur votre compte ShareFile

Pour demander ou confirmer que votre sous-domaine ShareFile est activé pour le DLP, envoyez une demande au support Citrix.

Pour certains comptes, l'activation de la DLP peut également nécessiter l'activation d'une nouvelle expérience utilisateur pour le site Web ShareFile. Une fois la DLP activée sur votre compte, vous pouvez procéder à l'activation de la DLP sur votre serveur StorageZones Controller.

### Activez la DLP sur votre serveur StorageZones Controller

Suivez les étapes suivantes pour configurer les paramètres DLP lors de votre déploiement de StorageZones Controller :

1. Installez ou effectuez une mise à niveau vers Storage Zones Controller 5.3 ou version ultérieure.
2. Dans la console StorageZones Controller `http://*localhost*/configservice/login.aspx`, cliquez sur l'onglet **ShareFile Data**. Cliquez sur **Modifier** si la zone existe.
3. Cochez la case **Activer l'intégration DLP** et saisissez l'adresse ICAP de votre serveur DLP dans le champ URL **ICAP** REQMOD. Le format de l'adresse est le suivant :

```
icap://<*name or IP address of your DLP server*>:<*port*>/reqmod

OR
```

```
4
5  *icaps://\<name or IP address of your DLP server\>:\<port\>/reqmod
      *
6
7  The default ICAP port is 1344 (non-secure DLP) and the default
      ICAPS port is 11344 (secure DLP).
8
9  For example, if your DLP server is dlp-server.example.com, type
      the following into the ICAP REQMOD URL field:
10
11 icap://*dlp-server.example.com*:1344/reqmod
12
13 OR
14
15 *icaps://dlp-server.example.com:11344/reqmod*
```

4. Cliquez sur **Enregistrer** ou sur **Enregistrer**.

Après avoir activé la DLP, vérifiez que le serveur DLP est accessible en vérifiant l'entrée **État du serveur DLP ICAP** dans l'onglet **Surveillance**.

### Contrôlez l'accès en fonction des résultats du scan DLP

Une fois la DLP activée sur le contrôleur de comptes et de zones de stockage, chaque version de chaque fichier chargé vers la zone de stockage compatible DLP est analysée pour détecter tout contenu sensible. Les résultats de l'analyse sont enregistrés dans la base de données ShareFile sous forme de classification des données.

Les paramètres DLP limitent les autorisations normales et les contrôles de partage disponibles pour les fichiers en fonction de leur classification DLP. Lors du partage d'un document, un utilisateur peut toujours choisir de bloquer l'accès anonyme même si les paramètres DLP lui permettent de le partager de manière anonyme. Mais si l'utilisateur tente de partager un fichier d'une manière qui enfreindrait les paramètres DLP, ShareFile l'en empêche.

Les classifications des données sont les suivantes :

- **Numérisé** : OK —Fichiers scannés par un système DLP et approuvés.
- **Numérisés : rejetés** : fichiers scannés par un système DLP et dont on a découvert qu'ils contenaient des données sensibles.
- **Non numérisés** : fichiers qui n'ont pas été scannés.

La classification **Non numérisée** s'applique à tous les documents stockés dans des zones de stockage gérées par Citrix ou dans d'autres zones de stockage dans lesquelles le DLP n'est pas activé. La classification s'applique également aux fichiers des zones de stockage compatibles DLP qui ont été téléchargés avant la configuration du DLP. La classification s'applique également aux fichiers en attente d'analyse en raison de l'indisponibilité du système DLP externe ou de la lenteur de réponse.

La classification de chaque élément est déterminée par la règle de réponse du serveur ICAP. Si le serveur DLP ICAP répond par un message indiquant que le contenu doit être bloqué ou supprimé, le fichier est marqué comme **Numérisé : rejeté**. Dans le cas contraire, le fichier est marqué comme **numérisé : OK**.

Pour chaque classification de données, vous pouvez définir différentes restrictions d'accès et de partage. Pour chacune des trois catégories, l'administrateur ShareFile choisit les actions à autoriser :

- Les employés peuvent télécharger ou partager le fichier.
- Les utilisateurs clients tiers peuvent télécharger ou partager le fichier. Le partage de clients est désactivé par défaut mais peut être activé sous **Administration > Préférences avancées > Autoriser les clients à partager des fichiers**.
- Les utilisateurs anonymes peuvent télécharger le fichier

Lorsqu'un utilisateur partage un fichier, seuls les utilisateurs disposant d'autorisations de téléchargement peuvent le recevoir. Par conséquent, lorsque vous activez l'autorisation de partage pour une classification de données, vous devez également accorder au moins une autorisation de téléchargement à une catégorie d'utilisateurs.

#### Pour configurer les paramètres DLP dans ShareFile

1. Dans l'interface Web de ShareFile, cliquez sur **Admin > Prévention de la perte de données**.
2. Modifiez l'option **Limiter l'accès aux fichiers en fonction de leur contenu** sur **Oui**.
3. Configurez les actions autorisées pour chaque classification de données.

> **Important :**
>
> L'outil ShareFile On-Demand Sync nécessite des autorisations de téléchargement pour fonctionner normalement. Activez les téléchargements par les employés pour toutes les classifications de contenu si votre déploiement inclut ShareFile On-Demand Sync.

Lorsque le StorageZones Controller envoie un fichier au système DLP, il inclut des métadonnées indiquant le propriétaire du fichier. Le fichier inclut également le chemin du dossier dans lequel le fichier se trouve dans ShareFile. Ces informations permettent à l'administrateur du serveur DLP de consulter les détails spécifiques à ShareFile concernant les fichiers contenant du contenu sensible.

### Paramètres avancés pour la DLP

Pour ajuster le processus d'analyse DLP, modifiez le fichier de paramètres situé sur votre StorageZones Controller à l'adresse `wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`. Le tableau suivant décrit chaque paramètre lié à la DLP.

| Paramètre | Description | Valeur par défaut |
|---|---|---|
| intervalle de numérisation | Fréquence à laquelle le service DLP vérifie la présence de nouveaux fichiers dans la file d'attente DLP et les envoie au serveur DLP ICAP pour traitement. | 30 secondes |
| délai de réponse ICAP | Durée pendant laquelle le StorageZones Controller attend une réponse ICAP avant de marquer le serveur ICAP comme indisponible. | 30 secondes |
| extensions d'exclusion ICAP | Liste des extensions à exclure de l'analyse DLP, séparées par des virgules. Le serveur DLP ne traite pas les fichiers dont le nom se termine par l'une de ces extensions, mais marque les fichiers comme étant scannés : OK. Exemple de valeur : « exe, jpg, bin, mov » | Aucun |
| icap-max-file-size-bytes | Taille maximale du fichier (en octets) à envoyer au serveur DLP pour traitement. Une valeur de 0 signifie qu'il n'y a pas de maximum et que toutes les tailles de fichier sont envoyées. Lorsqu'il est configuré avec une valeur différente de zéro, le serveur DLP ne traite pas les fichiers dont la taille est supérieure à la taille configurée, mais ils sont marqués comme numérisés : OK. | 31457280 (30 MB) |

| Paramètre | Description | Valeur par défaut |
|---|---|---|
| éléments de la file d'attente à traiter | Le nombre maximum d'éléments en file d'attente à scanner par itération d'intervalle de numérisation. Diminuez cette valeur afin de limiter l'impact sur votre serveur DLP lorsqu'un grand nombre de fichiers sont ajoutés à la StorageZone. | 512 |
| fils de traitement des files d'attente maximum | Nombre maximal de threads de processeur simultanés à utiliser pour vider la file d'attente d'analyse DLP. Définissez cette valeur en fonction du nombre maximum de connexions simultanées autorisées à votre serveur ICAP. Il doit se situer dans des limites raisonnables afin d'éviter de bloquer d'autres services réseau qui utilisent le même serveur ICAP. | 4 |
| Verbe de demande ICAP-REQMOD-HTTP | Par défaut, les appels réseau sont effectués avec le verbe PUT. Vous pouvez modifier ce paramètre sur POST si nécessaire. | METTRE |

## Outil DLP pour les fichiers existants

Le contrôleur de zones de stockage ShareFile propose des options pour intégrer le centre de stockage aux fournisseurs de prévention contre la perte de données (DLP) via ICAP.

Les services ICAP fonctionnent toutefois par le biais de files d'attente qui ne sont remplies que par des fichiers nouvellement créés. Cela signifie que les fichiers existant dans une zone avant l'activation d'ICAP ne seront pas analysés par les services. Cet outil permet de mettre ces fichiers en file d'attente pour numérisation et peut également mettre en file d'attente les fichiers numérisés pour une nouvelle numérisation.

Comme son nom l'indique, l'outil ne fonctionne que pour le service DLP ICAP.

### Exigences

L'outil est un script PowerShell et nécessite donc PowerShell pour s'exécuter. PsExec ou un outil similaire est également nécessaire car le script doit être exécuté en tant que service réseau pour accéder à l'emplacement de partage réseau.

### Emplacement

Pour un contrôleur de zones de stockage installé, l'outil se trouve à l'adresse `<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1`. L'emplacement d'installation du StorageZones Controller est par défaut `C:\inetpub\wwwroot\Citrix\StorageCenter`.

### Considérations avant d'exécuter l'outil

L'outil peut avoir besoin de s'exécuter plusieurs fois pour une seule opération, en fonction des éléments suivants.

- Les limites prévues pour la taille maximale de la file d'attente.
- Le nombre d'éléments correspondant aux critères donnés. Cette considération est vraie sauf si la limite de taille de file d'attente est définie sur zéro ou moins. Dans ce cas, l'outil suppose une taille maximale de 200 000 éléments dans le répertoire de file d'attente.

Par exemple, si l'outil est utilisé pour mettre en file d'attente des éléments non numérisés, la taille limite de la file d'attente est fixée à 500 éléments. Lorsqu'il y a plus de 500 éléments non numérisés, l'outil s'arrête une fois que 500 éléments sont remplis dans la file d'attente. Pour savoir où il s'est arrêté, l'outil enregistre la date de création du dernier élément extrait. L'outil enregistre la date dans un fichier temporaire dans `<storage zones controller installation location>\SC` avec le nom DLPExistingFiles-EndDate.temp.

Avant chaque exécution, l'outil recherche ce fichier. Si le fichier est présent, l'outil utilise la date de création qu'il contient comme marqueur pour le lot de fichiers suivant. L'outil ne supprime pas le fichier temporaire à la fin d'une certaine opération. Au lieu de cela, l'administrateur de zone peut supprimer le fichier une fois que tous les lots relatifs à une opération donnée sont terminés. Dans ce cas, lorsqu'une opération complète est terminée, le fichier temporaire, s'il est présent, doit être supprimé manuellement avant d'effectuer une autre opération.

#### Exécution de l'outil avec PsExec

Ouvrez une fenêtre de commande et exécutez PsExec à l'aide de la commande suivante.

```
PsExec.exe -i -u "nt authority\network service"

"C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
```

Cela ouvre PowerShell en tant que service réseau. Pour vérifier qu'il fonctionne bien en tant que service réseau, exécutez **whoami** et vérifiez le résultat.

Une fois que PowerShell est ouvert, exécutez-y directement l'outil pour effectuer toutes les tâches nécessaires.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 <options>
```

### Options de ligne de commande

Les options suivantes sont disponibles pour exécuter l'outil :

- **-runscan** (obligatoire) : cette option est utilisée pour spécifier le type de fichiers à mettre en file d'attente pour analyse. Sous-options :
  - **Non numérisés** : fichiers non numérisés. Par exemple, les fichiers de l'ère pré-DLP qui n'ont pas été scannés.
  - **ScannedOK** : fichiers numérisés marqués comme propres.
  - **ScannedRejected** : fichiers scannés qui ont été marqués comme non propres.
  - **Numérisé** : tous les fichiers numérisés.
- **-QueueLimit** (facultatif) : cette option est utilisée pour spécifier le nombre d'éléments autorisés dans la file d'attente avant que l'outil ne s'arrête.
- **-date** (facultatif) : date de création maximale des éléments à mettre en file d'attente pour la numérisation. Par exemple, si la date spécifiée est « 30/10/2017 11h30 », seuls les fichiers créés avant cette date/heure seront mis en file d'attente pour être numérisés.

**Exemples :**

Pour tous les exemples, ouvrez **PowerShell en tant que service réseau via**PsExec. Pour obtenir des instructions, reportez-vous aux étapes décrites plus haut dans cet article.

Pour mettre en file d'attente des éléments non scannés dans une zone, exécutez la commande suivante.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Unscanned
```

Pour mettre en file d'attente tous les éléments scannés dans une zone dont la limite de file d'attente est de 100, exécutez la commande suivante.

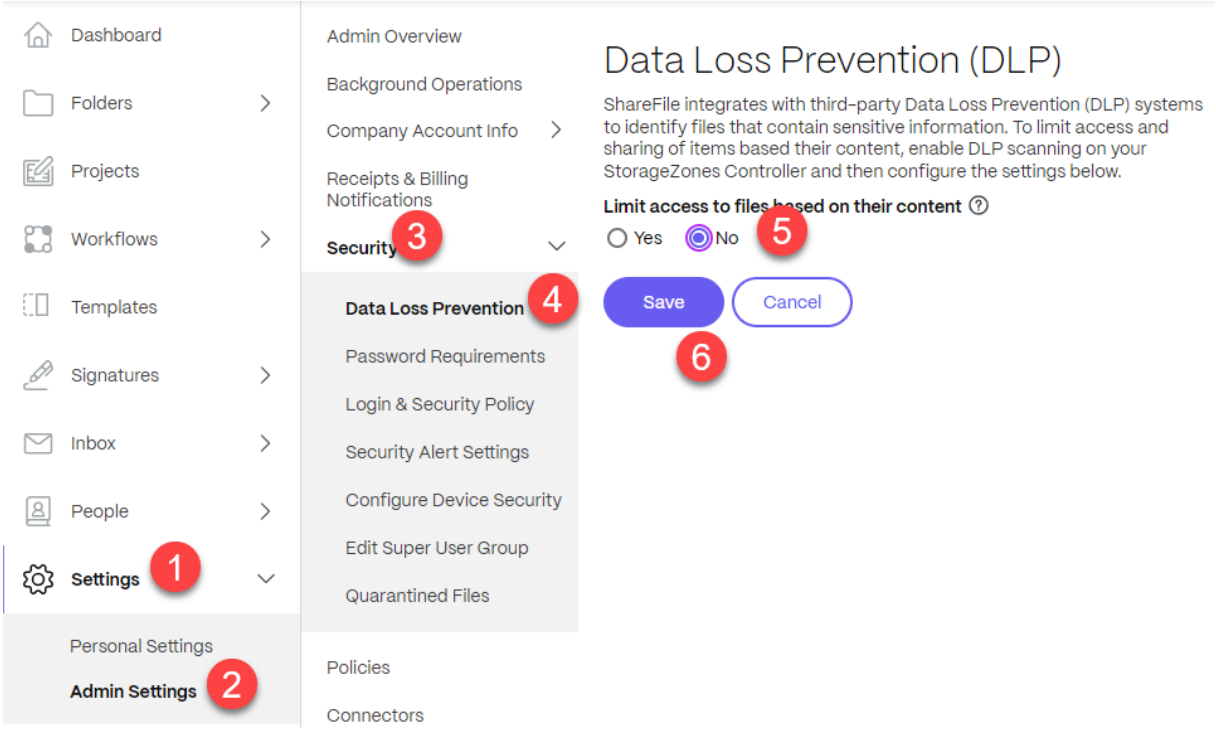
```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Scanned -queueLimit 100
```

Pour mettre en file d'attente tous les éléments scannés créés avant 11 h 30 le 30/10/2017 et présentant les caractéristiques suivantes : marqués comme propres, dans une zone avec une limite de 200 files d'attente, exécutez la commande suivante.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan ScannedOK -queueLimit 200 -date "
    10/30/2017 11:30 AM"
```

## Désactiver DLP

Pour désactiver la DLP pour ShareFile et StorageZones Controller, effectuez les actions suivantes :




1. Connectez-vous à votre compte Sharefile et cliquez sur **Paramètres**.
2. Dans la liste déroulante qui s'ouvre, sélectionnez **Paramètres d'administration**.
3. Dans le menu qui s'ouvre, cliquez sur **Sécurité**.
4. Dans le menu Sécurité, choisissez l'option **Prévention contre la perte de données**.
5. Depuis l'écran DLP, accédez à la section **Limiter l'accès aux fichiers en fonction de leur contenu** et cliquez sur **Non**.
6. Sélectionnez **Save**.

# Surveillance

February 14, 2022

Storage Zones Controller et l'interface administrateur ShareFile incluent plusieurs ressources pour vous aider à surveiller l'activité du StorageZones Controller et à résoudre les problèmes :

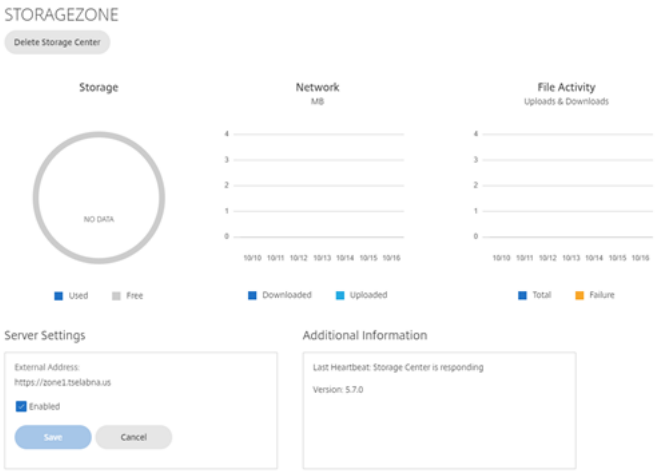
- **État général des composants** : l'onglet Surveillance de la console Storage Zones Controller fournit l'état des composants pour vous aider à démarrer le processus de dépannage. L'état est fourni pour des éléments tels que les autorisations d'accès, l'état du service et l'état Heartbeat, qui indique la connectivité sortante du StorageZones Controller au plan de contrôle ShareFile.

  Storage Zones Controller envoie des mises à jour à l'application Web ShareFile toutes les 5 minutes. Si l'application Web ShareFile ne reçoit pas de mise à jour dans les 10 minutes, elle marque le StorageZones Controller comme étant hors ligne.

  Pour les éléments de l'onglet Surveillance qui apparaissent en rouge, consultez les fichiers journaux pour obtenir des informations détaillées.

  L'onglet Surveillance n'indique pas si une zone de stockage fonctionne en termes de connectivité. Cela inclut si le plan de contrôle ShareFile peut atteindre l'URL de la zone de stockage externe ou si un client est en mesure d'atteindre la zone.

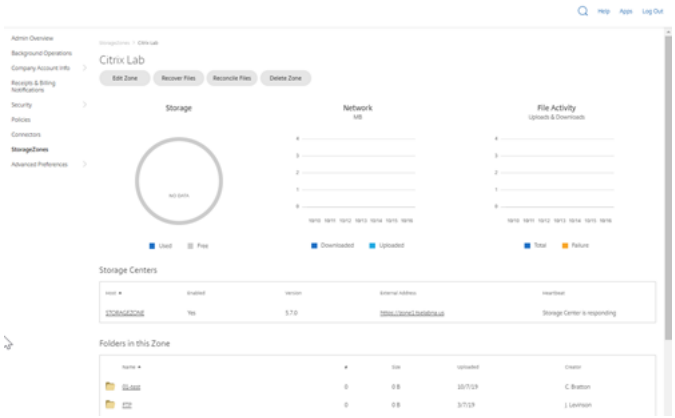
- **Informations sur le serveur Storage Zones Controller** : pour plus d'informations sur l'utilisation du stockage, l'utilisation du réseau et l'activité des fichiers du serveur : à partir de l'interface ShareFile, connectez-vous à votre compte ShareFile Enterprise, accédez à **Admin > StorageZones**, cliquez sur la zone de stockage, puis cliquez sur un stockage nom d'hôte du contrôleur de zones.



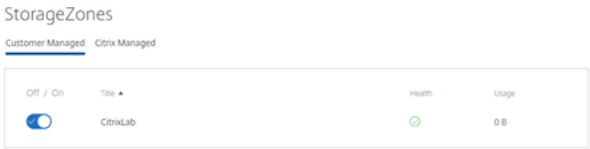

- **Informations sur la zone** : pour plus d'informations sur l'utilisation du stockage, l'utilisation du réseau et l'activité des fichiers pour une zone : Dans l'interface ShareFile, connectez-vous à

votre compte ShareFile Enterprise, accédez à **Admin > StorageZones**, puis cliquez sur le nom d'une zone.




- **État de santé du StorageZones Controller** —Pour déterminer si ShareFile.com reçoit des messages de pulsation des StorageZones Controller joints à la zone, affichez l'état de santé : à partir de l'interface ShareFile, connectez-vous à votre compte ShareFile Enterprise, accédez à **Admin > StorageZones**, vérifiez que la colonne Santé est cochée en vert, puis cliquez sur le nom du site pour vérifier que le message Heartbeat indique que le Storage Zones Controller répond.




- **Fichiers journaux : les** fichiers journaux fournissent des informations détaillées sur la configuration du StorageZones Controller et ses composants, comme décrit dans la section suivante.

## Fichiers journaux

Les fichiers journaux suivants pour le StorageZones Controller se trouvent par défaut dans `C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs` :

| Nom du fichier journal | Contient des informations de journalisation pour |
|---|---|
| cfgsrv-%date%.txt | actions de configuration du StorageZones Controller, y compris la modification d'une configuration de zones de stockage existante, la création d'une nouvelle zone de stockage et l'association d'un nouveau StorageZones Controller à un StorageZones Controller principal existant |
| sc-%date%.txt | Activité de chargement et de téléchargement de données ShareFile pour les zones standard |
| CIFS-%date%.txt | connecteurs de zone de stockage pour les activités de chargement et de téléchargement de partages de |
| sharepoint-%date%.txt | connecteurs de zone de stockage pour les activités de chargement et de téléchargement SharePoint |
| cloudstorageuploader-%date%.txt | Service Cloud Storage Uploader (vers un système de stockage tiers pris en charge) |
| copy-%date%.txt | Service de copie ShareFile |
| delete–%date%.txt | ShareFile Cleanup Service, pour le cache de stockage persistant |
| s3uploader–%date%.txt | Service de gestion ShareFile. Comprend des messages d'état du rythme cardiaque |

La journalisation étendue est disponible pour chacun des composants suivants et est utile lorsque vous devez fournir des informations détaillées au support technique.

| Composant | Emplacement de AppSettingsRelease.config |
|---|---|
| Données ShareFile | C:\inetpub\wwwroot\Citrix\StorageCenter |
| connecteurs de zone de stockage pour partages de fichiers réseau | C:\inetpub\wwwroot\Citrix\StorageCenter\cifs |
| connecteurs de zone de stockage pour SharePoint | C:\inetpub\wwwroot\Citrix\StorageCenter\sp |

**Pour activer la journalisation étendue**

Les étapes suivantes permettent d'activer la journalisation étendue pour tous les composants et services de Storage Zones Controller :

1. Sur le serveur Storage Zones Controller, ouvrez IIS.
2. Accédez au site Web par défaut, puis ouvrez Paramètres de l'application.
3. Changez la valeur de l'activation-extended-logging de 0 à 1.
4. Redémarrez le service de gestion Citrix ShareFile.
5. Une fois le problème résolu, nous vous recommandons d'effacer la journalisation étendue pour réduire la quantité de journalisation.

Pour activer la journalisation étendue pour un composant particulier, modifiez son fichier AppSettingsRelease.config : Changez la valeur `<add key="enable-extended-logging"value="0"/>` de 0 à 1.

Vous pouvez également consulter les journaux IIS pour déterminer si le trafic atteint le StorageZones Controller. Les journaux IIS affichent toutes les demandes entrantes. Les journaux IIS pour le StorageZones Controller se trouvent dans c:\inetpub\logs\LogFiles\W3SVC1.

Pour activer la journalisation IIS étendue, consultez http://support.microsoft.com/kb/313437.

## Résoudre les problèmes d'installation et de configuration

| Problème | Description et résolution |
|---|---|
| « Erreur HTTP 404 - Fichier ou répertoire introuvable » apparaît lors de la configuration du StorageZones Controller | Le message résulte généralement d'un problème avec IIS ou `ASP.NET`. Assurez-vous que le rôle IIS est activé sur l'installation de Windows et que la fonctionnalité `ASP.NET` est activée sur IIS. |
| « Erreur HTTP 404.2 —Introuvable » s'affiche lorsque vous parcourez localhost sur le StorageZones Controller | Le message indique que les restrictions ISAPI et CGI pour `ASP.NET` ne sont pas définies sur Autorisé. |

| Problème | Description et résolution |
| --- | --- |
| « Erreur HTTP 413 —Entité de requête trop grande » s'affiche après une tentative de téléchargement | Le message peut apparaître sur une trace réseau après l'échec d'une tentative de téléchargement vers une zone de stockage et peut résulter d'un paramètre de certificat client dans IIS. Pour contourner ce problème, ouvrez IIS sur le serveur Storage Zones Controller. Accédez au site Web par défaut, puis ouvrez Paramètres SSL. Pour les certificats clients, sélectionnez Ignorer. Redémarrez le service de gestion Citrix ShareFile. |
| Des erreurs IIS se produisent pendant la configuration du contrôleur de zones | Les erreurs IIS indiquent généralement que `ASP.NET` n'est pas complètement configuré. Vérifiez dans le Gestionnaire des services Internet (IIS), sous Restrictions ISAPI et CGI, que la valeur Restriction est définie sur Autorisée pour toutes les listes `ASP.NET`. Vérifiez que `ASP.NET` est enregistré dans IIS : Dans le Gestionnaire des services Internet, sous Pools d'applications, vérifiez qu'il existe des listes `ASP.NET`. Pour vous inscrire manuellement `ASP.NET`, consultez les lignes de commande qui suivent ce tableau. Si les problèmes persistent, passez en revue votre service Internet (IIS) et la configuration de `ASP.NET`. |
| « Impossible d'enregistrer la liaison du centre de stockage » apparaît lors de la configuration du StorageZones Controller | Le message indique un problème d'autorisation sur l'utilisateur du pool de comptes IIS. Par défaut, les pools d'applications fonctionnent sous le compte d'utilisateur du service réseau. Storage Zones Controller utilise le compte de service réseau par défaut. Si vous utilisez un compte d'utilisateur nommé au lieu du compte de service réseau, le compte d'utilisateur nommé doit avoir un accès complet au partage réseau utilisé pour le stockage de données privées. |

| Problème | Description et résolution |
| --- | --- |
| « Accès refusé » apparaît lors de la configuration de la zone | Le message peut apparaître si le compte ShareFile sous lequel vous êtes connecté n'est pas autorisé à créer et à gérer des zones. Utilisez la console administrateur ShareFile pour définir cette autorisation. |
| Les demandes sortantes sont bloquées | Lorsque les demandes sortantes sont bloquées, le journal cfgsrv inclut System.Net.WebException : Le serveur distant a renvoyé une erreur : (403) Interdit. Ce problème est probablement dû au fait que le serveur proxy bloque les demandes sortantes. Vérifiez que votre pare-feu répond aux exigences spécifiées dans la configuration système requise pour le StorageZones Controller |
| « Impossible de se connecter au serveur distant » s'affiche lorsque vous ouvrez une session sur le StorageZones Controller | Le message indique généralement un problème de proxy. Assurez-vous que vos paramètres de proxy sont configurés. Si les paramètres du proxy sont corrects, vérifiez que vous pouvez vous connecter à votre compte ShareFile à partir du StorageZones Controller. Vérifiez que vous disposez des autorisations de niveau administrateur pour configurer le StorageZones Controller et que le port 443 est ouvert sur le pare-feu externe. |
| Le dossier nommé ShareFileStorage sur votre partage réseau n'inclut pas SCKeys.txt une fois que vous avez activé et configuré des zones de stockage pour ShareFile Data | storage zones Controller crée SCKeys.txt lors de l'installation, sauf si le compte que vous avez utilisé pour installer le contrôleur de zone de stockage ne figure pas dans la liste de contrôle d'accès. Mettez à jour la liste de contrôle d'accès et réinstallez le StorageZones Controller. |
| Les chargements de fichiers vers un dossier partagé échouent après la création d'une zone | Ce problème indique un problème lié à votre DNS interne. Vous devez disposer d'un enregistrement DNS interne et externe pour le nom de domaine complet du StorageZones Controller. |

| Problème | Description et résolution |
| --- | --- |
| Dans l'onglet **Monitoring**, le Heartbeat Status est rouge | Une icône rouge indique que le contrôleur de zone de stockage n'est pas en mesure d'envoyer des messages de pulsation au site Web ShareFile. Vérifiez si les icônes des autres composants sont rouges. Si c'est le cas, reportez-vous aux journaux pour plus d'informations. Si le journal s3uploader indique un échec d'envoi du battement de cœur, le serveur Storage Zones Controller peut ne pas être en mesure de contacter le site Web ShareFile à moins qu'il ne passe par un serveur proxy. Pour spécifier un serveur proxy pour le StorageZones Controller, ouvrez la console du contrôleur et accédez à l'onglet Mise en réseau. Si le serveur Storage Zones Controller ne peut pas accéder au site Web ShareFile à l'aide d'un utilisateur de service réseau, autorisez l'utilisateur du service réseau à accéder au site Web ShareFile ou configurez un compte utilisateur Windows avec un accès sortant au serveur proxy. |

| Problème | Description et résolution |
| --- | --- |
| Une zone de stockage n'apparaît pas dans l'interface administrateur ShareFile | Ce problème peut indiquer un problème lié à l'adresse externe ou au pare-feu. Vérifiez d'abord dans la console Storage Zones Controller que l'adresse externe n'inclut pas le port. Si tel est le cas, retirez le port, puis redémarrez le contrôleur. Si l'adresse externe n'inclut pas le port, assurez-vous que votre pare-feu Windows est correctement configuré. Par défaut, les paramètres du pare-feu Windows autorisent le trafic sortant pour les services ShareFile sur le port 443. Le StorageZones Controller nécessite ce paramètre. Vérifiez que le pare-feu Windows autorise le trafic sortant sur le port 443 pour les processus suivants : `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCopySvc\FileCopyService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\s3uploader\S3UploaderService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\CloudStorageUploaderSvc\CloudStorageUploaderService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\SCProxyEmailSvc\ProxyEmailService.exe` |

| Problème | Description et résolution |
| --- | --- |
| Storage Zones Controller ne télécharge pas de données vers ShareFile | Dans la console Citrix ADC, cliquez avec le bouton droit sur le serveur virtuel d'équilibrage de charge pour obtenir des statistiques, afin de vérifier si le trafic atteint Citrix ADC à partir du plan de contrôle ShareFile, du StorageZones Controller et des clients ShareFile. Lorsque vous chargez un fichier et que le serveur virtuel affiche une augmentation du nombre d'accès, le trafic passe par Citrix ADC. Vérifiez le trafic pour chaque point de la connexion Citrix ADC : serveur virtuel de commutation de contenu, serveurs virtuels d'équilibrage de charge pour les connecteurs et pour les données ShareFile, appels HTTP liés à l'un des deux serveurs virtuels, stratégie de répondeur liée au serveur virtuel de données ShareFile, serveur virtuel de connecteurs liaison à Citrix ADC AAA. Ensuite, testez les chargements de données ShareFile en dissociant la stratégie de répondeur dans le serveur virtuel d'équilibrage de charge pour les données ShareFile. (La stratégie de répondeur supprime le trafic entrant qui n'est pas signé par le plan de contrôle ShareFile. Dans un navigateur Web, saisissez le nom de domaine complet externe du StorageZones Controller. S'il existe une connectivité, le logo ShareFile apparaît. Dans un navigateur Web, saisissez l'URL d'un connecteur. Si les URL suivantes réussissent à tester l'accessibilité des connecteurs de zone de stockage, vous serez invité à entrer des informations d'identification même si le serveur principal est hors service. Ou, si vous êtes connecté en tant qu'utilisateur, vous obtiendrez une réponse d'API. `https://szc-address/cifs/v3/Items/ByPath?path=\\path`, `https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server`. La réponse de l'API se présente sous cette forme : The API response is in this form: { “Name”:”connectorName”,“FileName”:” FileName”,“CreationDate”:”date”, “ProgenyEditDate”:”date”,“IsHidden”:false, “Path”:”*“,”StreamID”:”id”,“odata.metadata”:” |

| Problème | Description et résolution |
|---|---|
| L'état Connectivité ShareFile à partir des services de nettoyage de fichiers est une icône rouge après la mise à niveau du StorageZones Controller | Une icône rouge apparaît si Windows démarre le service de nettoyage de fichiers avant que le StorageZones Controller n'établisse une connexion réseau. L'état revient à une icône verte une fois que le serveur de Controller est de retour sur le réseau. |
| « Le chemin dépasse la longueur maximale (1024) » apparaît lors de la création du connecteur | Le message peut se produire si l'adresse externe configurée pour le StorageZones Controller pointe vers le site Web ShareFile au lieu du nom de domaine complet du serveur StorageZones Controller. |
| « Nom non valide » s'affiche lors de la configuration d'un nouveau StorageZones Controller après la suppression d'un ancien. | Le message peut apparaître si des entités liées à l'ancien StorageZones Controller existent toujours. Pour résoudre ce problème : désinstallez le nouveau StorageZones Controller. Supprimez le dossier réseau partagé. Supprimez le dossier c:\inetpub\wwwroot\Citrix. Ouvrez regedit et supprimez la clé **HKEY_LOCAL_MACHINE/Software/WOW6432Note/Citrix**. Installez et configurez un nouveau StorageZones Controller. Si le problème persiste, contactez votre représentant du support technique. Ce message se produit lorsque les serveurs de zone de stockage ne peuvent pas résoudre le nom de domaine complet de zone de stockage via DNS ou le fichier d'hôtes locaux. |

**Pour inscrire manuellement ASP.NET**

```
cd /d C:\Windows\Microsoft.NET\Framework\v4.0.30319
iisreset /stop
aspnet_regiis -i
iisreset /start
%systemroot%\system32\inetsrv\appcmd set config /section:
    isapiCgiRestriction
/[path='%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll'].
    allowed:True
%systemroot%\system32\inetsrv\appcmd set config /section:
    isapiCgiRestriction
```

```
8 /[path='%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll'
    ].allowed:True
```

### Dépannage des clients ShareFile et de l'application Web

Si un appareil mobile ne se connecte pas à un connecteur, vérifiez la connectivité. De nombreux problèmes de connectivité sont abordés dans le tableau précédent. Vérifiez que le contrôleur de zone de stockage est en ligne. Téléchargez un fichier dans la zone. Si le téléchargement fonctionne, le problème est spécifique aux connecteurs. Essayez de vous connecter à partir de l'appareil mobile en utilisant le réseau cellulaire et le réseau de l'entreprise. Vérifiez que le serveur SharePoint ou le serveur de fichiers est disponible.

Si un message « Erreur HTTP 401 —Non autorisé » apparaît lorsque vous tentez d'accéder à un connecteur, l'un des problèmes suivants peut empêcher un utilisateur d'accéder à un connecteur à partir de clients ShareFile ou de l'application Web ShareFile :

- Configuration incorrecte d'IIS : Vérifiez que l'authentification de base et l'authentification Windows sont activées pour le rôle Services Web (IIS). Si ces options ne sont pas répertoriées sous Sécurité, utilisez le Gestionnaire de serveur pour les installer, puis redémarrez IIS.
- Autorisations utilisateur incorrectes : vérifiez que l'utilisateur AD a accès au partage. Dans le Gestionnaire de serveur, accédez à Gestion du partage et du stockage, puis ajoutez l'utilisateur ou modifiez les autorisations utilisateur selon vos besoins.
- Un problème lié à l'authentification, à l'autorisation et à l'audit de l'accès au groupe Citrix ADC.

Si un message « Erreur HTTP 403 —Interdit » s'affiche lors de la connexion à un site SharePoint, le serveur SharePoint peut être configuré pour l'authentification de base, mais le contrôleur de zone de stockage peut ne pas être configuré pour mettre en cache les informations d'identification. Pour résoudre ce problème, ajoutez `<add key="CacheCredentials"value="1"/>` à `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

Si un message « Erreur HTTP 503 —Service indisponible » apparaît lorsque des applications mobiles tentent d'accéder à un connecteur, cela signifie que les connecteurs envoient une réponse mais ne sont pas en mesure de traiter la demande HTTP. Cela peut se produire si les stratégies de commutation de contenu, les adresses IP virtuelles d'équilibrage de charge ou la stratégie de répondeur ne sont pas correctement configurées ou liées à Citrix ADC. Pour résoudre ce problème, consultez la configuration Citrix ADC pour ShareFile et corrigez la configuration.

## Référence : fichiers de configuration du contrôleur de zones de stockage

December 5, 2022

Cette référence fournit une vue d'ensemble des fichiers de configuration du StorageZones Controller :

- Configurer le contrôleur de zone de stockage avec les données ShareFile sur Microsoft Azure
- AppSettingsRelease.config
- Fichier DeleteService.exe.config
- sfantivirus.exe.config
- Web.config

Le programme d'installation du StorageZones Controller crée ces fichiers. Les modifications que vous apportez dans la console StorageZones Controller sont enregistrées dans les fichiers.

Pour utiliser ou configurer certaines fonctionnalités, vous devez ajouter ou mettre à jour manuellement certains paramètres dans les fichiers de configuration. Cette référence répertorie ces paramètres et fournit des liens vers des informations connexes.

## ShareFile Data sur Microsoft Azure Storage

Les zones de stockage gérées par le client prennent en charge l'hébergement natif des données Citrix ShareFile dans votre compte Microsoft Azure. L'utilisation d'un stockage tiers compatible aide les services informatiques à créer une solution rentable et personnalisée pour leur entreprise. Cette solution intègre ShareFile au stockage Binary Large Object (Blob) de Microsoft Azure. Ce stockage est un service cloud permettant de stocker de grandes quantités de données non structurées accessibles de n'importe où via HTTP ou HTTPS.

### Configurer le contrôleur de zone de stockage avec les données ShareFile sur Microsoft Azure

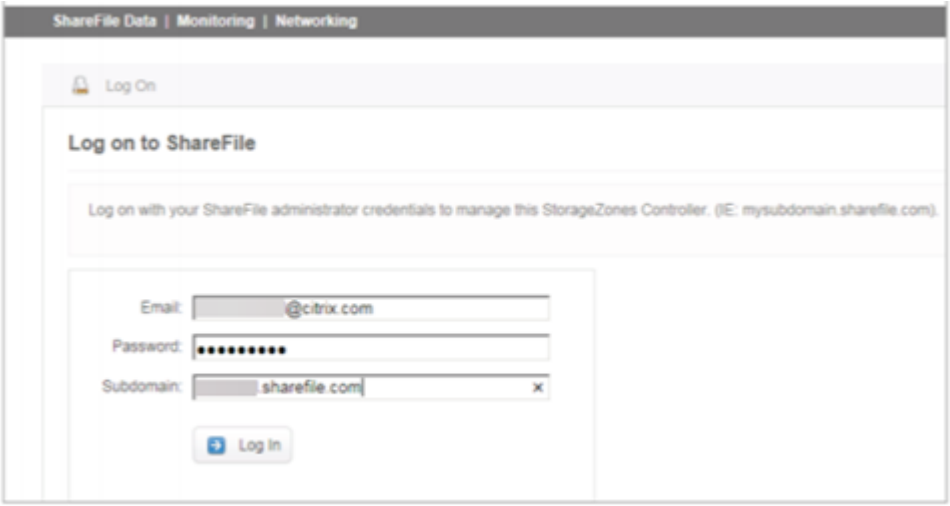
Avant de créer une zone de stockage avec ShareFile Data sur Microsoft Azure, consultez la configuration système requise et les étapes d'installation :

- Créez un partage réseau pour le cache de stockage. Pour plus d'informations, voir Création d'un partage réseau pour le stockage de données privées.
- Installez les certificats SSL nécessaires. Pour plus d'informations, voir Installer un certificat SSL.
- Préparez le serveur pour l'installation de la zone de stockage. Pour plus d'informations, voir Préparer votre serveur pour les données ShareFile.

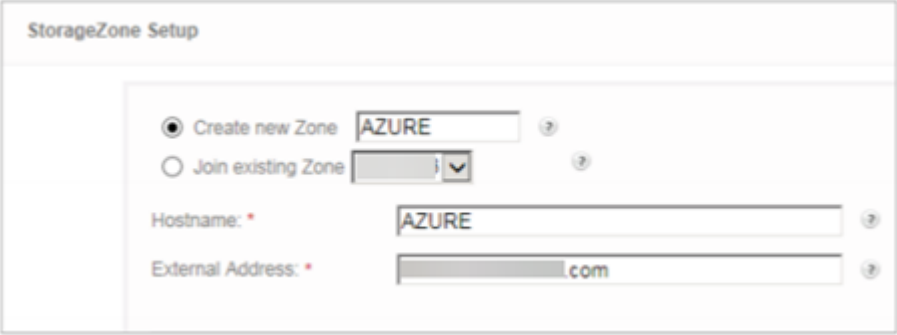
Une fois le logiciel StorageZones Controller installé, accédez à **Citrix ShareFile Storage Zones Controller** et sélectionnez **la page de configuration**.

1. Connectez-vous à ShareFile à l'aide du compte administrateur qui vous a été attribué.

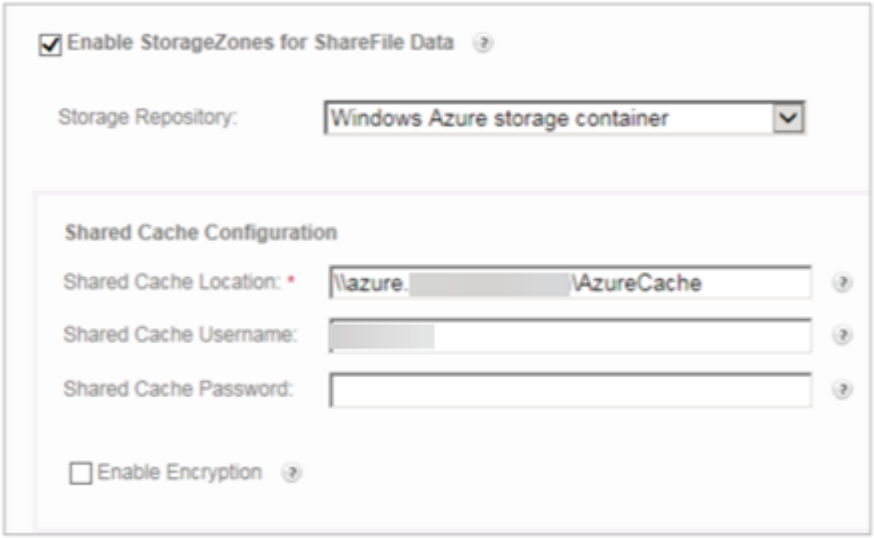



2. Sélectionnez l'option **Créer une nouvelle zone** et entrez un nom unique pour la nouvelle zone.
3. Entrez le **nom d'hôte**, généralement le nom de l'ordinateur du serveur sera utilisé.
4. Entrez l'**adresse externe** de cette zone. Il s'agit de l'adresse FQDN pouvant être résolue publiquement pour ce serveur ou équilibreur de charge.

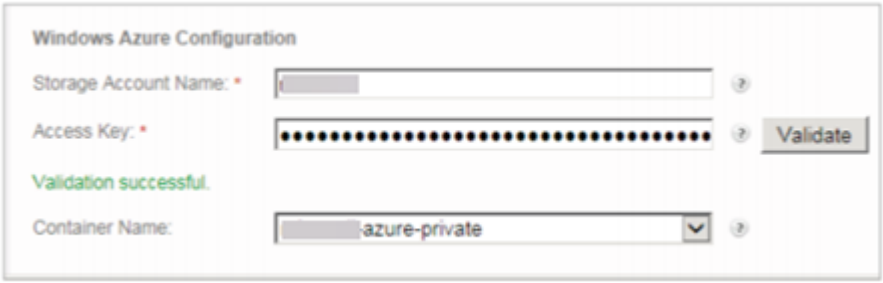



5. Cochez la case **Activer les zones de stockage pour les données ShareFile** .
6. Sélectionnez le **conteneur de stockage Windows Azure** dans le menu déroulant **Référentiel de stockage** .
7. Entrez l'**emplacement du cache partagé** créé lors de l'installation des prérequis, voir Création d'un partage réseau pour le stockage de données privées. Entrez un nom d'utilisateur et un mot de passe permettant d'accéder au dossier Shared Cache.



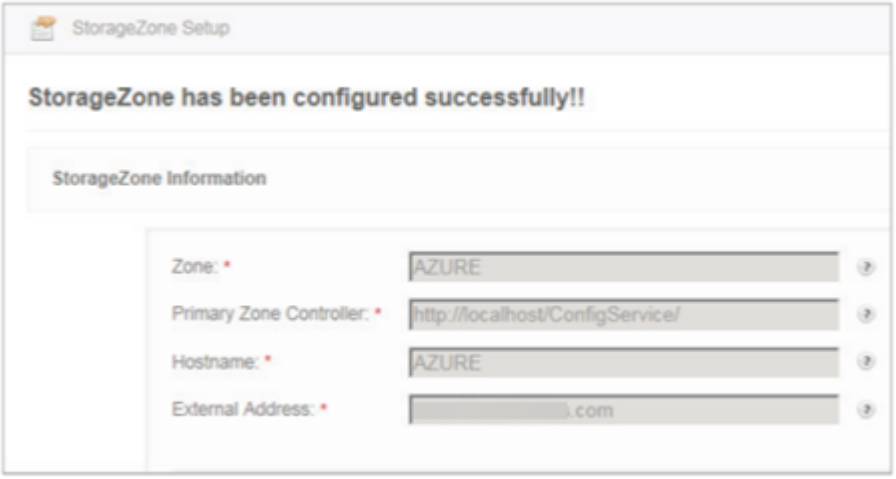

8. Entrez le **nom du compte de stockage** et la **clé d'accès**. Ces informations proviennent de votre compte Microsoft Azure.
9. Sélectionnez **Valider**.
10. Une fois validés, les conteneurs mis à votre disposition par Azure vous sont présentés. Sélectionnez le conteneur approprié dans le menu déroulant **Nom du conteneur** .



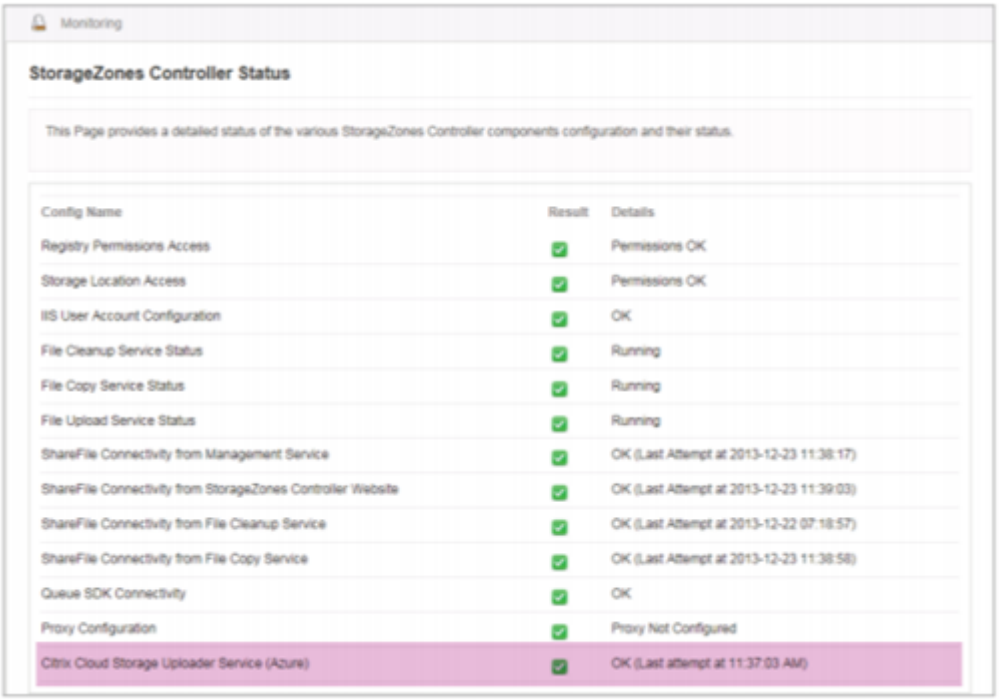

11. Au bas de la page, entrez une phrase secrète et saisissez-la à nouveau pour vérification.
12. Sélectionnez **Register**.

    Une fois terminé, le message suivant s'affiche : StorageZone a été correctement configurée !

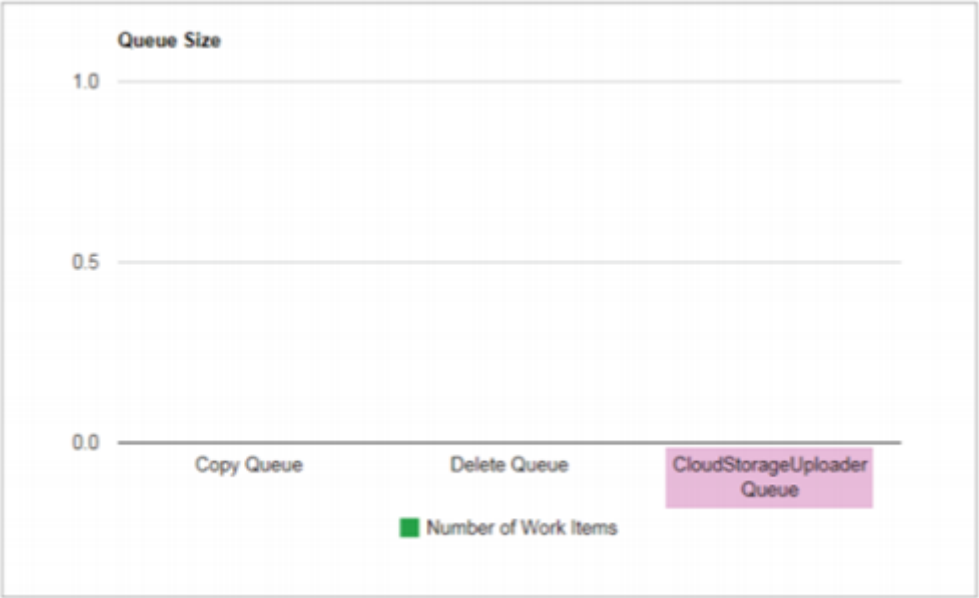



13. Sélectionnez l'onglet **Surveillance** et vérifiez l'état du StorageZones Controller. Le service Citrix Cloud Storage Uploader (Azure) surveille le service de téléchargement en arrière-plan pour Azure.




La **file d'attente CloudStorageUploader** surveille le dossier de file d'attente de téléchargement Azure.




### AppSettingsRelease.config

Les fichiers AppSettingsRelease.config se trouvent dans les dossiers suivants du chemin d'installation du StorageZones Controller (C:\inetpub\wwwroot\Citrix \) :

- Centre de stockage

  Définit les paramètres globaux pour le StorageZones Controller.

- Centre de stockage \ cifs

  Définit les paramètres des connecteurs de zones de stockage pour les partages de fichiers réseau.

- Centre de stockage \ sp

  Définit les paramètres des connecteurs de zones de stockage pour SharePoint.

Avant de modifier un fichier AppSettingsRelease.config, vérifiez que vous travaillez au bon emplacement.

### Fichier DeleteService.exe.config

FileDeleteService.exe.config fournit des contrôles utilisés par StorageZones Controller pour gérer le cache de stockage persistant. Ce fichier de configuration se trouve dans : `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

Pour plus d'informations, voir Personnaliser les opérations du cache de stockage.

### sfantivirus.exe.config

SFAntivirus.exe.config fournit au logiciel du scanner des informations sur la configuration de votre contrôleur de zones de stockage, l'emplacement du logiciel de numérisation et les différentes options de commande. Ce fichier de configuration se trouve dans : `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

Pour plus d'informations, voir Configurer les scans antivirus des fichiers téléchargés.

### Web.config

En général, `C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` contient des commandes qui ne doivent généralement pas être modifiées. Vous devrez toutefois le mettre à jour si vous utilisez d'anciens contrôleurs de zones de stockage avec un serveur proxy.

**Pour StorageZones Controller 2.2 à 2.2.2 uniquement :** si une zone possède plusieurs contrôleurs de zones de stockage et que tout le trafic HTTP utilise un serveur proxy, vous devez ajouter une liste de contournement à Web.config pour chaque serveur secondaire.

Remarque : Depuis la version 2.2.3, le paramètre de contournement est inclus dans la page Réseau de la console StorageZones Controllers.

1. Ouvrez le fichier dans un éditeur de texte et localisez la `<system.net>` section. Voici un exemple de cette section une fois qu'un serveur proxy est configuré :

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
    </defaultProxy>
  </system.net>
</configuration>
```

2. Ajoutez une liste de contournement à cette section, comme indiqué :

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
      <bypasslist>
        <add address="primaryServer" />
      </bypasslist>
    </defaultProxy>
  </system.net>
</configuration>
```

   Le serveur principal est une adresse IP ou un nom d'hôte (servername.subdomain.com).

Si vous modifiez ultérieurement l'adresse IP ou le nom d'hôte du StorageZones Controller principal, vous devez mettre à jour ces informations dans ConfigService \ Web.config pour chaque serveur secondaire.

3. Redémarrez le serveur IIS de tous les membres de la zone.