StorageZone-Controller 5.x

Machine translated content

Disclaimer

Contents

Informationen zum StorageZones Controller

May 28, 2024

Der StorageZone Controller erweitert den ShareFile Software-as-a-Service (SaaS) -Cloudspeicher, indem er Ihrem ShareFile-Konto privaten Datenspeicher zur Verfügung stellt.

Weitere Informationen über StorageZone Controller, wie Komponenten, Datenspeicher und mehr, finden Sie unter StorageZone Controller 5.x.

Die neuesten Verbesserungen in diesem und in ShareFile finden Sie unter Neuigkeiten.

Um die neueste Version von ShareFile Storagezone Controller herunterzuladen, besuchen Sie https://dl.sharefile.com/storagezone-controller. Melden Sie sich bei Ihrem ShareFile-Konto an, um auf alle Anwendungsdownloads zuzugreifen.

> **Tipp:**
>
> ShareFile empfiehlt Benutzern, Warnmeldungen zur Erkennung von Bedrohungenzu aktivieren.

Behobene Probleme

Behebung von Problemen im StorageZone Controller 5.11.25

In dieser Version werden mehrere Probleme behoben, die die Gesamtleistung und Stabilität verbessern.

Behebung von Problemen im StorageZone Controller 5.11.24

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Probleme beim StorageZones Controller 5.11.23 behoben

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Probleme beim StorageZones Controller 5.11.22 behoben

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Probleme mit StorageZone Controller 5.11.21 behoben

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Probleme mit StorageZone Controller 5.11.18 behoben

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Probleme beim StorageZones Controller 5.11.17 behoben

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Behebung von Problemen im StorageZone Controller 5.11

Diese Version behebt eine Reihe von Problemen, die die Gesamtleistung und Stabilität verbessern.

Probleme beim StorageZones Controller 5.10 behoben

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Probleme beim StorageZones Controller 5.9 behoben

Diese Version enthält Fehlerbehebungen zur Verbesserung der Zuverlässigkeit und Leistung.

Probleme beim StorageZones Controller 5.8 behoben

Diese Version enthält einen Fix zur Verbesserung der Fehlermeldungen für ausgecheckte Dateien und einen Fix für neu veröffentlichte verwaltete Pfade in SharePoint.

Probleme beim StorageZones Controller 5.7 behoben

Diese Version enthält Korrekturen zur Behebung eines Umleitungsproblems beim Hochladen von Dateien in die Speicherzone und on-premises Connectors.

Probleme beim StorageZones Controller 5.6 behoben

WOPI Fix: Enthält Änderungen zur Behebung von Problemen, die auftreten, wenn versucht wird, Office-Dateien nachträglich zu bearbeiten.

SharePoint Connector Fix: Diese Version enthält Änderungen zur Anzeige gültiger Fehlermeldungen beim Erstellen von Ordnern, die bereits im SharePoint Connector vorhanden sind.

Probleme beim StorageZones Controller 5.5 behoben

Diese Version enthält Fehlerbehebungen zur Verbesserung der Zuverlässigkeit und Leistung.

Probleme beim StorageZones Controller 5.4.2 behoben

SharePoint Connector-Fix: Das Verschieben von Dateien, die auf dem SharePoint-Konnektor vorhanden sind, schlägt möglicherweise in bestimmten Szenarien Diese Version stellt sicher, dass das Verschieben von Dateien, die auf SharePoint Connector vorhanden sind, wie erwartet funktioniert

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Probleme beim StorageZones Controller 5.4.1 behoben

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit und Zuverlässigkeit.

Zusätzliche Unterstützung: Unterstützung für *cloud/*cloudburrito-Konten für die Workspace-Umgebung wurde hinzugefügt.

Probleme beim StorageZones Controller 5.3.1 behoben

Diese Version enthält Fehlerbehebungen zur Verbesserung der Zuverlässigkeit und Leistung.

Probleme beim StorageZones Controller 5.3.1 behoben

WOPI-Fix: WOPI-Zugriffstoken wurden möglicherweise durch den Diebstahl des öffentlichen kryptografischen Schlüssels gefälscht. Diese Version stellte sicher, dass der Schlüssel nicht zwischen StorageZone Controllern geteilt wird.

Sicherheitsupdates: Diese Version enthält Updates für Sicherheit, Leistung und Zuverlässigkeit.

Bekannte Probleme

Bekannte Probleme mit StorageZone Controller 5.10

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme mit StorageZone Controller 5.9

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme mit StorageZone Controller 5.8

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme mit StorageZone Controller 5.7

In diesem Release wurden keine neuen Probleme festgestellt.

Architektur im Überblick

July 25, 2024

Dieser Abschnitt bietet einen Überblick über die Bereitstellung von StorageZones Controller für Machbarkeitsstudien oder Produktionsumgebungen mit hoher Verfügbarkeit. Die Bereitstellung mit hoher Verfügbarkeit wird sowohl mit als auch ohne DMZ-Proxy wie Citrix ADC angezeigt.

Um eine Bereitstellung mit mehreren StorageZones Controllern zu evaluieren, folgen Sie den Richtlinien für eine Bereitstellung mit hoher Verfügbarkeit.

Für jedes der Bereitstellungsszenarien ist ein ShareFile Enterprise-Konto erforderlich. Standardmäßig speichert ShareFile Daten in der sicheren von ShareFile verwalteten Cloud. Um privaten Datenspeicher zu verwenden, entweder eine on-premises Netzwerkfreigabe oder ein unterstütztes Speichersystem eines Drittanbieters, konfigurieren Sie Speicherzonen für ShareFile-Daten.

Um Benutzern Daten aus Netzwerkdateifreigaben oder SharePoint-Dokumentbibliotheken sicher bereitzustellen, konfigurieren Sie Speicherzonenkonnektoren.

Machbarkeitsnachweis für StorageZones Controller

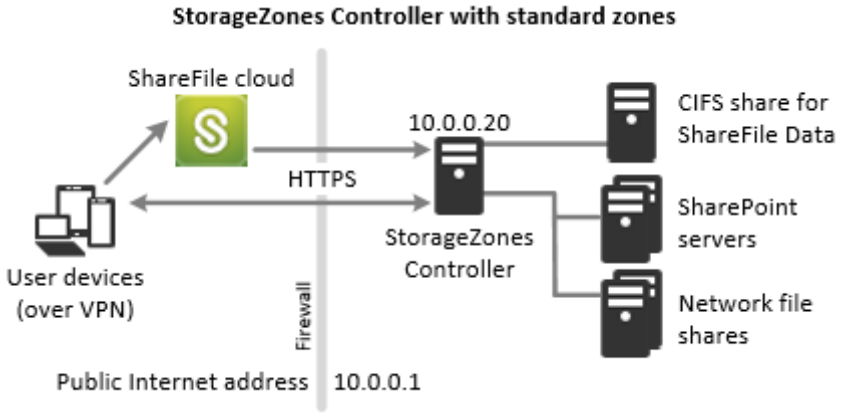
> **Achtung:**
>
> Eine Machbarkeitsstudie dient nur zu Evaluierungszwecken und sollte nicht für die Speicherung kritischer Daten verwendet werden.

Bei einer Machbarkeitsstudie wird ein einziger StorageZones Controller verwendet. Bei der in diesem Abschnitt erläuterten Beispielbereitstellung sind sowohl Speicherzonen für ShareFile-Daten als auch Speicherzonenconnectors aktiviert.

Um einen einzelnen StorageZones Controller zu evaluieren, können Sie optional Daten in einem Ordner (z. B. C:\ZoneFiles) auf der Festplatte des StorageZones Controllers statt auf einer separaten Netzwerkfreigabe speichern. Alle anderen Systemanforderungen gelten für eine Testbereitstellung.

Machbarkeitsnachweis für Standardspeicherzonen

Ein für Standardzonen konfigurierter StorageZones Controller muss eingehende Verbindungen aus der ShareFile-Cloud akzeptieren. Dazu muss der Controller über eine öffentlich zugängliche Internetadresse verfügen und SSL für die Kommunikation mit der ShareFile-Cloud aktiviert sein. Die folgende Abbildung zeigt den Datenverkehr zwischen Benutzergeräten, der ShareFile-Cloud und dem StorageZone Controller.



In diesem Szenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Der Speicherzonen-Controller befindet sich innerhalb der Firewall, um den Zugriff zu steuern Benutzerverbindungen zu ShareFile müssen die Firewall durchqueren und das SSL-Protokoll an Port 443 verwenden, um diese Verbindung herzustellen. Um diese Konnektivität zu unterstützen, müssen Sie Port 443 auf der Firewall öffnen und ein öffentliches SSL-Zertifikat auf dem IIS-Dienst des StorageZones Controllers installieren.

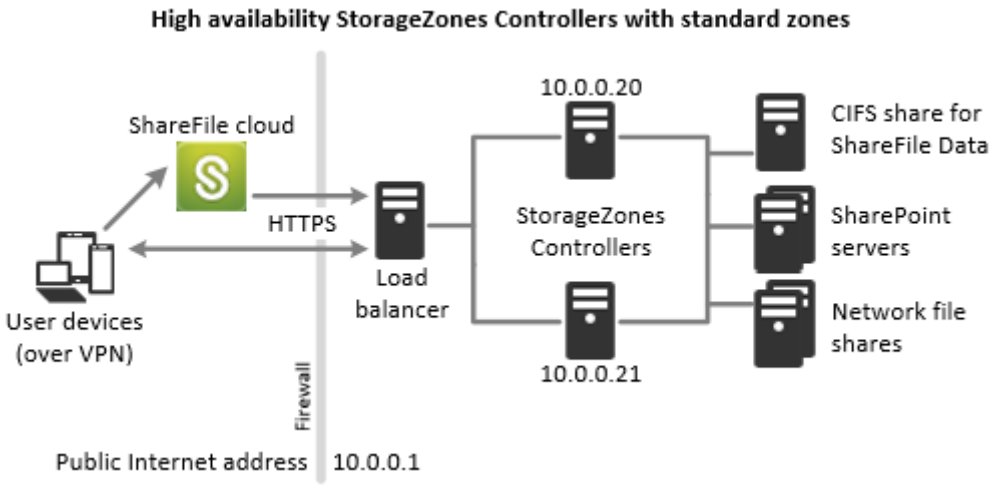
Bereitstellung von StorageZones Controllern mit hoher Verfügbarkeit

Für eine Produktionsbereitstellung von ShareFile mit hoher Verfügbarkeit empfiehlt es sich, mindestens zwei StorageZones Controller zu installieren. Wenn Sie den ersten Controller installieren, erstellen Sie eine Speicherzone. Wenn Sie die anderen Controller installieren, fügen Sie sie derselben Zone hinzu. StorageZones Controller, die zu derselben Zone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden.

In einer Hochverfügbarkeitsbereitstellung sind die sekundären Server unabhängige, voll funktionsfähige StorageZones Controller. Das Subsystem zur Speicherzonensteuerung wählt nach dem Zufallsprinzip einen Speicherzonencontroller für den Betrieb aus. Wenn der Primärserver offline geht, können Sie problemlos einen Sekundärserver zum Primärserver heraufstufen. Sie können einen Server auch vom Primär- zum Sekundärserver herabstufen.

Bereitstellung mit hoher Verfügbarkeit für Standardzonen

StorageZones Controller, die für Standardspeicherzonen konfiguriert sind, müssen eingehende Verbindungen aus der ShareFile-Cloud akzeptieren. Dazu muss jeder Controller über eine öffentlich zugängliche Internetadresse verfügen und SSL für die Kommunikation mit der ShareFile-Cloud aktiviert sein. Sie können mehrere externe öffentliche Adressen konfigurieren, die jeweils einem anderen StorageZones Controller zugeordnet sind. Die folgende Abbildung zeigt eine Hochverfügbarkeitsbereitstellung für Standardspeicherzonen.



Ähnlich wie im obigen Proof-of-Concept-Bereitstellungsszenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Die StorageZone Controller befinden sich innerhalb der Firewall, um den Zugriff zu steuern. Benutzerverbindungen zu ShareFile müssen die Firewall durchqueren und das SSL-Protokoll an Port 443 verwenden, um diese Verbindung herzustellen. Um diese Konnektivität zu unterstützen, müssen Sie Port 443 auf der Firewall öffnen und ein öffentliches SSL-Zertifikat auf dem IIS-Dienst aller StorageZones Controller installieren.

Konfiguration für gemeinsam genutzten Speicher

StorageZones Controller, die zu derselben Speicherzone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden. StorageZones Controller greifen mithilfe des IIS-Kontopool-Benutzers auf den Share zu. Standardmäßig werden Anwendungspools unter dem Netzwerkdienstbenutzerkonto betrieben, das über Benutzerrechte auf niedriger Ebene verfügt. Ein StorageZones Controller verwendet standardmäßig das Netzwerkdienstkonto.

Sie können ein benanntes Benutzerkonto anstelle des Netzwerkdienstkontos verwenden, um auf die Freigabe zuzugreifen. Um ein benanntes Benutzerkonto zu verwenden, geben Sie den Benutzernamen und das Kennwort auf der Konfigurationsseite der StorageZones Console an. Führen Sie den IIS-Anwendungspool und die ShareFile Services mithilfe des Netzwerkdienstkontos aus.

Netzwerkverbindungen

Netzwerkverbindungen variieren je nach Zonentyp —von ShareFile verwaltet oder Standard.

Von ShareFile verwaltete Zonen In der folgenden Tabelle werden die Netzwerkverbindungen beschrieben, die auftreten, wenn sich ein Benutzer bei ShareFile anmeldet und dann ein Dokument aus einer von ShareFile verwalteten Zone herunterlädt. Alle Verbindungen verwenden HTTPS.

Schritt	Quelle	Ziel
1. Anfrage zur Benutzeranmeldung	Client	`company.sharefile.com:443`
2. (Optional) Zur SAML-IdP-Anmeldung umleiten	Client	SAML-Identitätsanbieter-URL
3. Aufzählung von Dateien/Ordnern und Download-Anfrage	Client	`company.sharefile.com:443`
4. Datei herunterladen	Client	`storage-location.sharefile.com:443`

Standardlagerzonen In der folgenden Tabelle werden die Netzwerkverbindungen beschrieben, die auftreten, wenn sich ein Benutzer bei ShareFile anmeldet und dann ein Dokument von einer Standardspeicherzone herunterlädt. Alle Verbindungen verwenden HTTPS.

Schritt	Quelle	Ziel
1. Anfrage zur Benutzeranmeldung	Client	`company.sharefile.com`
2. (Optional) Wenn Sie ADFS verwenden, leiten Sie zur SAML-IdP-Anmeldung um	Client	SAML-Identitätsanbieter-URL
3. Aufzählung von Dateien/Ordnern und Download-Anfrage	Client	`company.sharefile.com`
4. Autorisierung zum Herunterladen von Dateien	`company.sharefile.com`	`szc.company.com`
5. Datei herunterladen	Client	`szc.company.com`

Schritt	Quelle	Ziel

DMZ-Proxy-Bereitstellung von StorageZones Controller

Eine demilitarisierte Zone (DMZ) bietet eine zusätzliche Sicherheitsebene für das interne Netzwerk. Ein DMZ-Proxy wie Citrix ADC VPX ist eine optionale Komponente, die verwendet wird, um:

- Stellen Sie sicher, dass alle Anfragen an einen StorageZones Controller aus der ShareFile-Cloud stammen, sodass nur zugelassener Datenverkehr die StorageZones Controller erreicht.

  Der StorageZones Controller verfügt über einen Validierungsvorgang, der für alle eingehenden Nachrichten nach gültigen URI-Signaturen sucht. Die DMZ-Komponente ist für die Validierung von Signaturen verantwortlich, bevor Nachrichten weitergeleitet werden.

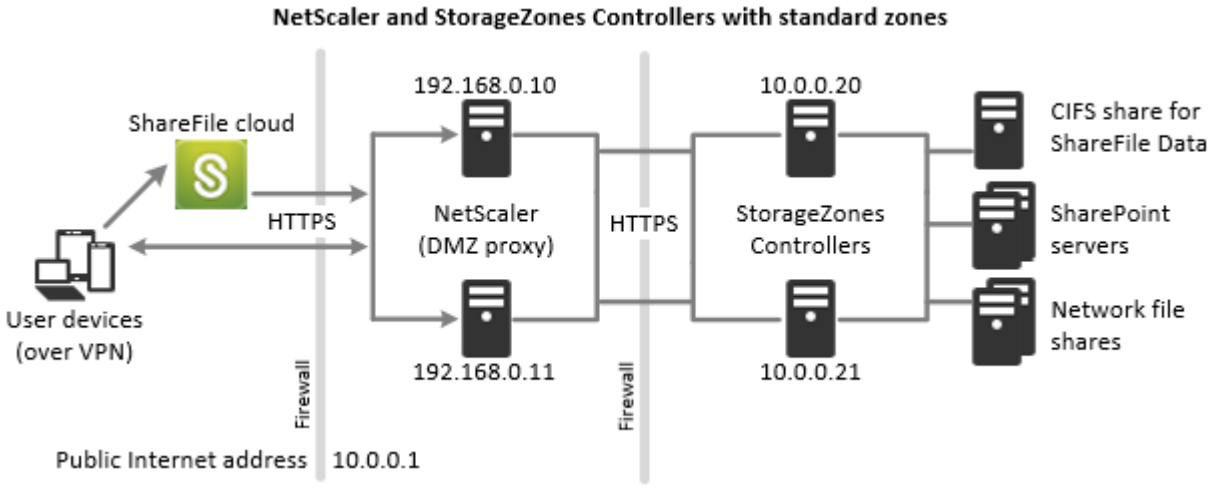
- Lastenausgleichsanforderungen an StorageZones Controller mithilfe von Statusanzeigen in Echtzeit.

  Operationen können mit einem Lastenausgleich auf StorageZones Controller verteilt werden, wenn sie alle auf dieselben Dateien zugreifen können.

- Entladen Sie SSL von den StorageZones Controllern.
- Stellen Sie sicher, dass Anfragen für Dateien auf SharePoint oder Netzlaufwerken authentifiziert werden, bevor Sie die DMZ passieren.

Bereitstellung von Citrix ADC- und StorageZones Controllern

Bereitstellung für Standardspeicherzonen StorageZones Controller, die für Standardzonen konfiguriert sind, müssen eingehende Verbindungen aus der ShareFile-Cloud akzeptieren. Dazu muss der Citrix ADC über eine öffentlich zugängliche Internetadresse verfügen und SSL für die Kommunikation mit der ShareFile-Cloud aktiviert sein.

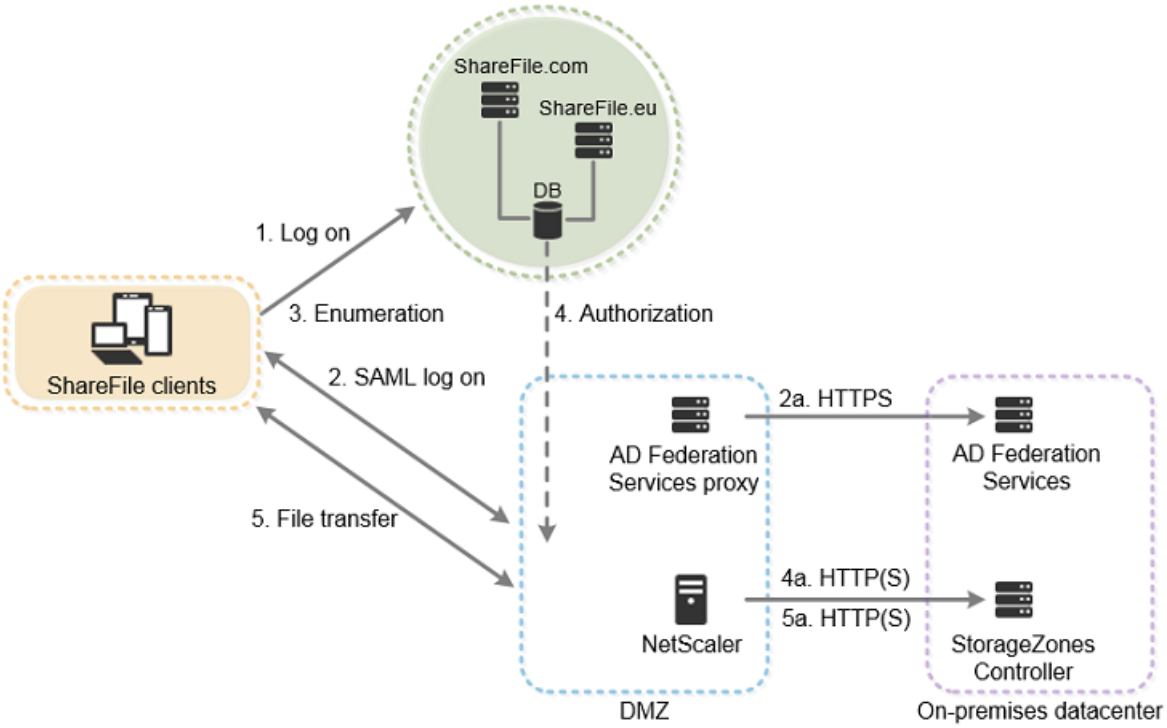


In diesem Szenario stehen zwei Firewalls zwischen dem Internet und dem sicheren Netzwerk. StorageZones Controller befinden sich im internen Netzwerk. Benutzerverbindungen zu ShareFile müssen die erste Firewall passieren und das SSL-Protokoll auf Port 443 verwenden, um diese Verbindung herzustellen. Um diese Konnektivität zu unterstützen, müssen Sie Port 443 auf der Firewall öffnen und ein öffentliches SSL-Zertifikat auf dem IIS-Dienst der DMZ-Proxyserver installieren (falls diese die Benutzerverbindung beenden).

Netzwerkverbindungen für Standardzonen

Das folgende Diagramm und die folgende Tabelle beschreiben die Netzwerkverbindungen, die auftreten, wenn sich ein Benutzer bei ShareFile anmeldet und dann ein Dokument aus einer Standardzone herunterlädt, die hinter Citrix ADC bereitgestellt wird. In diesem Fall verwendet das Konto Active Directory Federation Services (ADFS) für die SAML-Anmeldung.

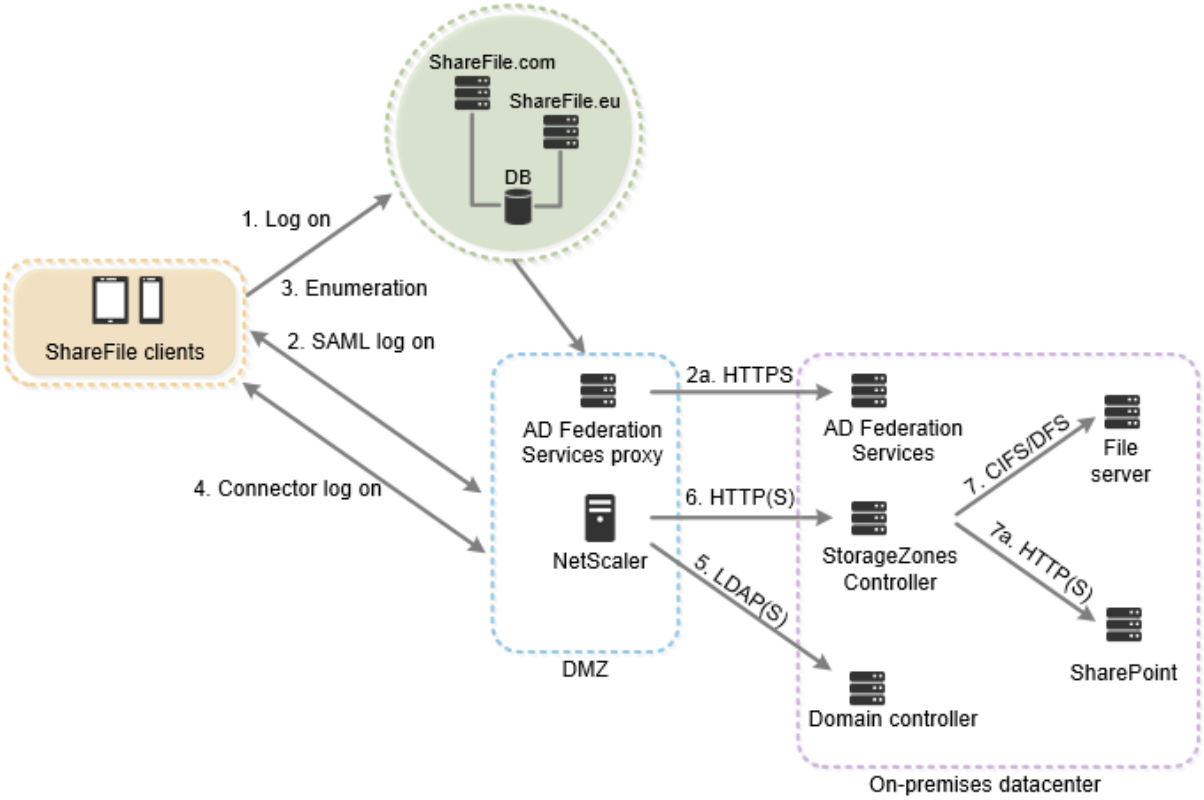
Der Authentifizierungsverkehr wird in der DMZ von einem ADFS-Proxyserver verarbeitet, der mit einem ADFS-Server im vertrauenswürdigen Netzwerk kommuniziert. Auf die Dateiaktivität wird über Citrix ADC in der DMZ zugegriffen, das SSL beendet, Benutzeranforderungen authentifiziert und dann im Namen authentifizierter Benutzer auf den StorageZones Controller im vertrauenswürdigen Netzwerk zugreift. Auf die externe Citrix ADC-Adresse für ShareFile wird über den Internet-FQDN szc.company.com zugegriffen.



Schritt	Quelle	Ziel	Protokoll
1. Anfrage zur Benutzeranmeldung	Client	company.sharefile.com	HTTPS
2. (Optional) Zur SAML-IdP-Anmeldung umleiten	Client	SAML-Identitätsanbieter-URL	HTTPS
2a. ADFS-Anmeldung	ADFS-Proxy	ADFS-Server	HTTPS
3. Aufzählung von Dateien/Ordnern und Download-Anfrage	Client	company.sharefile.com	HTTPS
4. Autorisierung zum Herunterladen von Dateien	ShareFile	szc.company.com (externe Adresse)	HTTP (S)
4a. Autorisierung zum Herunterladen von Dateien	Citrix ADC IP (NSIP)	Speicherzonencontroller	HTTPS
5. Datei herunterladen	Client	szc.company.com (externe Adresse)	HTTPS

Schritt	Quelle	Ziel	Protokoll
5a. Datei herunterladen	Citrix ADC IP (NSIP)	Speicherzonencontroller	HTTP (S)

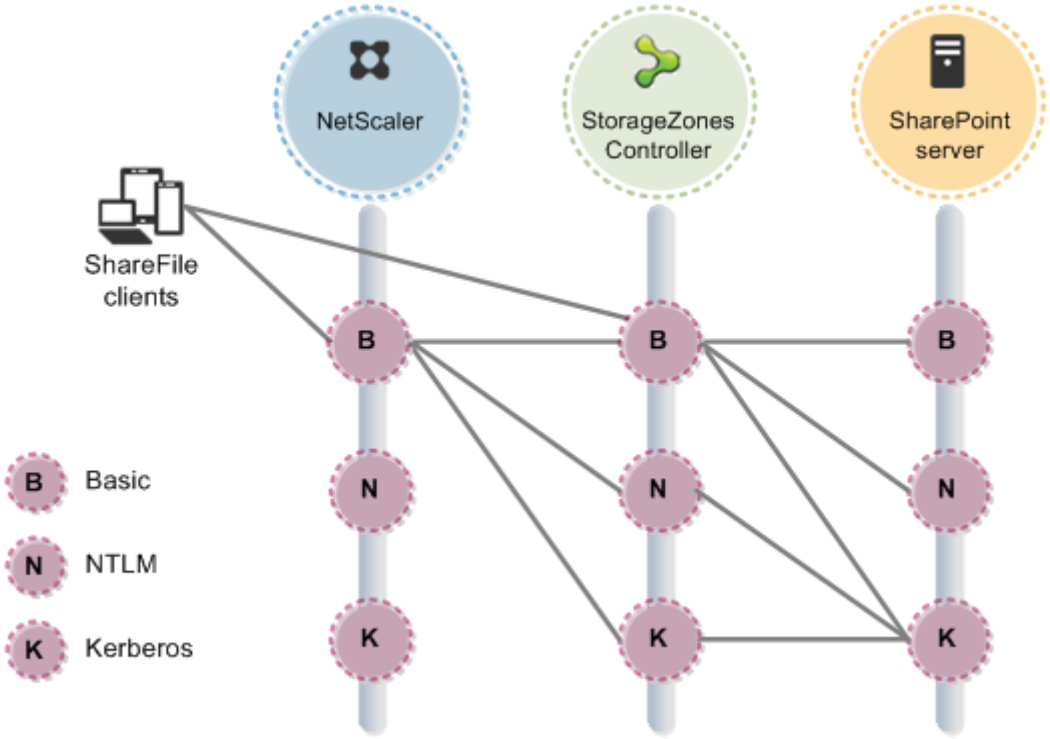
Das folgende Diagramm und die folgende Tabelle erweitern das vorherige Szenario und zeigen die Netzwerkverbindungen für StorageZone Connectors. Dieses Szenario beinhaltet die Verwendung von NetScaler in der DMZ, um SSL zu beenden und die Benutzerauthentifizierung für den Connectors-Zugriff durchzuführen.



Schritt	Quelle	Ziel	Protokoll
1. Anfrage zur Benutzeranmeldung	Client	company.sharefile.com	HTTPS
2. (Optional) Zur SAML-IdP-Anmeldung umleiten	Client	SAML-Identitätsanbieter-URL	HTTPS
2a. ADFS-Anmeldung	ADFS-Proxy	ADFS-Server	HTTPS

Schritt	Quelle	Ziel	Protokoll
3. Connector-Enumeration auf oberster Ebene	Client	company.sharefile.com	HTTPS
4. Benutzeranmeldung am StorageZones Controller-Server	Client	szc.company.com (externe Adresse)	HTTPS
5. Benutzerauthentifizierung	Citrix ADC IP (NSIP)	AD-Domänencontroller	LDAP (S)
6. Aufzählung von Dateien/Ordnern und Upload-/Download-Anfragen	Citrix ADC IP (NSIP)	Speicherzonencontroller	HTTP (S)
7. Aufzählung der Netzwerkfreigaben und Upload/Download	Speicherzonencontroller	Dateiserver	CIFS oder DFS
7a. SharePoint-Aufzählung und Upload/Download	Speicherzonencontroller	SharePoint	HTTP (S)

Das folgende Diagramm fasst die unterstützten Kombinationen von Authentifizierungstypen zusammen, je nachdem, ob sich der Benutzer authentifiziert.



Systemanforderungen

November 14, 2023

> **Wichtig:**
>
> Microsoft stellt den Support für Windows Server 2012R2 am 10. Oktober 2023 ein. Es ist wichtig, dass Sie Ihren Server vor Ablauf des Support-Datums auf eine neuere Version migrieren.

Speicherzonencontroller

- Eine dedizierte physische oder virtuelle Maschine mit 2 CPUs und 4 GB RAM
- Windows Server 2012 R2 (Rechenzentrum, Standard oder Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Für Standardlagerzonen:

- Verwenden Sie einen öffentlich auflösbaren Internet-Hostnamen (keine IP-Adresse).
- SSL für die Kommunikation mit ShareFile aktivieren.

  - Das SSL-Zertifikat auf dem StorageZones Controller muss von Benutzergeräten und ShareFile-Webservern als vertrauenswürdig eingestuft werden. Wenn Sie SSL direkt mit IIS verwenden, finden Sie Informationen zur Konfiguration von SSL unter http://support.microsoft.com/kb/298805.

- Lassen Sie eingehende TCP-Anfragen auf Port 443 über Ihre Firewall zu.
- Erlauben Sie ausgehende TCP-Anfragen an die ShareFile-Steuerungsebene auf Port 443 über Ihre Firewall.
  - Klicken Sie hier für eine detaillierte Liste der IP-Bereiche und Domänen.

Für die Serverintegritätsprüfung, die nur für Speicherzonen für ShareFile-Daten verwendet wird:

- Öffnen Sie Port 80 auf dem Localhost.

Für eine Produktionsumgebung mit hoher Verfügbarkeit:

- Mindestens zwei Server mit installiertem StorageZones Controller.
- Wenn Sie keine DMZ-Proxyserver verwenden, installieren Sie ein SSL-Zertifikat für den IIS-Dienst.

  Informationen zu den unterstützten Zertifikaten finden Sie oben in den Zertifikatsanforderungen für Standardzonen.

Für eine DMZ-Proxy-Bereitstellung:

- Ein oder mehrere DMZ-Proxyserver, z. B. NetScaler ADC VPX-Instanzen.
- Für einen DMZ-Proxyserver, der die Client-Verbindung beendet und HTTP verwendet, installieren Sie ein SSL-Zertifikat auf dem Proxyserver.

  Wenn die Kommunikation zwischen dem DMZ-Proxyserver und dem StorageZones Controller sicher ist, können Sie HTTP verwenden. HTTPS wird jedoch als bewährte Methode empfohlen. Wenn Sie HTTPS verwenden, können Sie ein privates (Enterprise) Zertifikat auf dem StorageZones Controller verwenden, sofern es vom DMZ-Proxy als vertrauenswürdig eingestuft wird. Die vom DMZ-Proxy offengelegte externe Adresse muss ein kommerziell vertrauenswürdiges Zertifikat verwenden. Informationen zu den unterstützten Zertifikaten finden Sie oben in den Zertifikatsanforderungen für Standardzonen.

Weitere Anforderungen

> **Hinweis:**
>
> ShareFile unterstützt die Verwendung der DFS-Replikation nicht offiziell und empfiehlt auch nicht. Es ist bekannt, dass es bei größeren Dateien zu Sperrfehlern kommt. Wenn die DFS-

> Replikation verwendet werden muss, verwenden Sie separate Backup-Lösungen außerhalb der Spitzenzeiten, wenn die Zone nicht aktiv verwendet wird.

- Das Storage Zones Controller-Installationsprogramm benötigt Administratorrechte.
- Verwenden Sie für die Remoteverwaltung des StorageZones Controllers ein Remoteprotokoll wie RDP oder Citrix ICA, um eine Verbindung zum Server herzustellen, und öffnen Sie dann die Storage Zones Controller-Konsole.

Unterstützte Speichersysteme von Drittanbietern

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

Unterstützte Lösungen zur Verhinderung von Datenverlust

- Der Storage Zones Controller lässt sich in jede ICAP-konforme DLP-Lösung integrieren, einschließlich:
  - Schutz vor Datenverlust durch Symantec
  - McAfee DLP Prevent
  - Websense TRITON AP-DATA
  - RSA-Schutz vor Datenverlust

Speicherzonen für ShareFile-Daten

Speicherzonen für ShareFile-Daten ist eine optionale Funktion, die Sie auf einem StorageZones Controller aktivieren.

Anforderungen:

- ShareFile Enterprise-Konto mit aktivierter Speicherzonenfunktion
- Ein ShareFile-Benutzerkonto, das die Berechtigung zum Erstellen und Verwalten von Zonen enthält
- Ein CIFS-Share für private Datenspeicherung

Wenn Sie ShareFile in einem unterstützten Speichersystem eines Drittanbieters speichern möchten, wird der CIFS-Share für temporäre Dateien (Verschlüsselungsschlüssel, Dateien in der Warteschlange) und als temporärer Speichercache verwendet.

- Die Webserver-Rolle (IIS) und ASP.NET 4.x. Weitere Informationen finden Sie unter Vorbereiten Ihres Servers für ShareFile-Daten.

Hinweis: Der Zugriff auf ein ShareFile-Konto von einem FTP-Client aus ist nicht mit Speicherzonen für ShareFile-Daten kompatibel.

Speicherzonenkonnektor für SharePoint

Der Speicherzonenconnector für SharePoint ist eine optionale Funktion, die Sie auf einem StorageZones Controller aktivieren.

Anforderungen:

- ShareFile Enterprise-Konto mit aktivierter Speicherzonenfunktion oder Citrix Endpoint Management.
- Nur **Microsoft SharePoint Server 2010 und neuer** werden unterstützt.
- Der StorageZones Controller-Server muss ein Domänenmitglied sein und sich in derselben Gesamtstruktur wie der SharePoint-Server befinden.
- Die Webserver-Rolle (IIS) und ASP.NET 4.x. Weitere Informationen finden Sie unter Vorbereiten Ihres Servers für ShareFile-Daten.
- SharePoint-Richtlinien:
  - Die standardmäßige maximale Uploaddateigröße für eine Webanwendung beträgt in SharePoint 2013 250 MB und in SharePoint 2010 50 MB. So ändern Sie die Standardeinstellung: Gehen Sie in der SharePoint-Zentraladministration zur Seite Allgemeine Einstellungen für Webanwendungen und ändern Sie die maximale Uploadgröße. Die Größenbeschränkung für Uploaddateien für SharePoint beträgt 2 GB.
  - ShareFile-Clients versuchen immer, eine Hauptversion einer Datei einzuchecken (zu veröffentlichen). SharePoint-Richtlinien bestimmen jedoch, ob eine Datei als Haupt- oder Nebenversion eingecheckt wird.
  - Die SharePoint-Berechtigung "Nur anzeigen"ermöglicht es einem Benutzer nicht, Dateien herunterzuladen. Um eine Datei von einem ShareFile-Client lesen zu können, muss ein SharePoint-Benutzer über eine Leseberechtigung verfügen.
- Benutzergeräte: Aktuelle Informationen zur Unterstützung von Speicherzonenkonnektoren durch Benutzergeräte finden Sie in der ShareFile Knowledge Base.

StorageZone-Connector für die SharePoint-Authentifizierung

Nach der Authentifizierung des Benutzers stellt der StorageZones Controller-Server im Namen des authentifizierten Benutzers Verbindungen zum SharePoint-Server her und reagiert auf Authentifizierungsprobleme, die vom SharePoint-Server auftreten. Der Speicherzonenconnector für SharePoint unterstützt die folgenden Authentifizierungsmethoden auf dem SharePoint-Server.

- Einfach

  Erfordert, dass Sie `<add key="CacheCredentials"value="1"\>` zu `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config.` hinzufügen

- Verhandeln (Kerberos)
- Windows Challenge/Response (NTLM)

Mobile ShareFile-Clients verwenden die Standardauthentifizierung über HTTPS, um sich beim StorageZones Controller oder DMZ-Proxy zu authentifizieren. Single Sign-On bei SharePoint unterliegt den Authentifizierungsanforderungen, die auf dem SharePoint-Server festgelegt sind. Um die Kerberos- oder NTLM-Authentifizierung auf dem SharePoint-Server zu verwenden, konfigurieren Sie den Domänencontroller so, dass er dem StorageZones Controller bei der Delegierung vertraut.

Wenn Ihr SharePoint-Server für die Kerberos-Authentifizierung konfiguriert ist: Konfigurieren Sie einen Dienstprinzipalnamen (SPN) für die benannten Benutzerdienstkonten für den SharePoint-Serveranwendungspool. Weitere Informationen finden Sie unter "Konfigurieren der Vertrauensstellung für die Delegierung von Webparts"unter http://support.microsoft.com/kb/832769.

Bei Bereitstellungen mit NetScaler ADC ist es möglich, die Standardauthentifizierung am NetScaler ADC zu beenden und dann andere Arten der Authentifizierung für den StorageZones Controller durchzuführen.

StorageZone-Connector für Network File Shares

Der Storage Zone Connector für Network File Shares ist eine optionale Funktion, die Sie auf einem StorageZones Controller aktivieren.

Anforderungen:

- ShareFile Enterprise- oder Citrix Endpoint Management-Konto.
- Der Storage Zone Connector-Server muss ein Domänenmitglied sein und sich in derselben Gesamtstruktur wie die Netzwerk-Dateiserver befinden.
- Die Webserver-Rolle (IIS) und ASP.NET 4.x. Weitere Informationen finden Sie unter Vorbereiten Ihres Servers für ShareFile-Daten.
- Benutzergeräte: Aktuelle Informationen zur Unterstützung von Speicherzonenkonnektoren durch Benutzergeräte finden Sie in der ShareFile Knowledge Base.

Connector für Network File Shares Authentifizierung

Nach der Authentifizierung des Benutzers stellt der StorageZones Controller-Server im Namen des authentifizierten Benutzers Verbindungen zum Netzwerk-Dateiserver her und reagiert auf Authentifizierungsprobleme, die vom Dateiserver gestellt werden. Der Storage Zone Connector für Network File Shares unterstützt die folgenden Authentifizierungsmethoden auf dem Dateiserver.

- Verhandeln (Kerberos)
- Windows Challenge/Response (NTLM)

Um die Kerberos- oder NTLM-Authentifizierung auf dem StorageZones Controller zu verwenden, konfigurieren Sie den Domänencontroller so, dass er dem StorageZones Controller bei der Delegierung vertraut.

Für Bereitstellungen mit NetScaler ADC: Um Benutzern ein Single Sign-On-Erlebnis zu bieten, wenn NetScaler ADC für die Standardauthentifizierung konfiguriert ist, konfigurieren Sie den Connector sowohl für die Negotiate- (Kerberos) als auch für die NTLM-Authentifizierung.

PowerShell-Skripts und -Befehle

Die StorageZones Controller-Installation umfasst mehrere PowerShell-Skripts und -Befehle, die sich in `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`befinden.

- Führen Sie die Skripts in der 32-Bit-Version (x86) von PowerShell aus.
- Optimale Ergebnisse erzielen Sie, wenn Sie ein Upgrade auf PowerShell 4.0 oder höher durchführen, das im Windows Management Frameworkenthalten ist.

  PowerShell 2.0 verursacht erhebliche Probleme aufgrund von Kompatibilitätsproblemen mit .NET Framework 4.

Installieren

April 20, 2021

Führen Sie die folgenden Aufgaben in der angegebenen Reihenfolge aus, um Storage Zones Controller, Storage Zones für ShareFile Data und Storage Zones Connectors zu installieren und einzurichten.

1. Konfigurieren von Citrix ADC für den StorageZones Controller

   Sie können Citrix ADC als DMZ-Proxy für den StorageZones Controller verwenden.

2. Erstellen einer Netzwerkfreigabe für die private Datenspeicherung

   Speicherzonen für ShareFile Daten erfordern eine Netzwerkfreigabe für Ihre privaten Daten, selbst wenn Sie ShareFile-Dateien in einem unterstützten Speichersystem eines Drittanbieters speichern.

3. Installieren eines SSL-Zertifikats

   Ein StorageZones Controller, der Standardzonen hostet, erfordert ein SSL-Zertifikat.

4. Vorbereiten des Servers für ShareFile Daten

   IIS- und ASP.NET-Setup ist für Speicherzonen für ShareFile Daten und für StorageZone Connector erforderlich.

5. Installieren des StorageZones Controller und Erstellen einer Speicherzone
6. Überprüfen der Konfiguration des StorageZones Controller
7. Ändern der Standardzone für Benutzerkonten

   Standardmäßig verwenden vorhandene und neu bereitgestellte Benutzerkonten den von ShareFile verwalteten Cloudspeicher als Standardzone.

8. Festlegen eines Proxyservers für Speicherzonen

   Über die StorageZones Controller-Konsole können Sie einen Proxyserver für StorageZones Controller festlegen. Sie können einen Proxyserver auch mit anderen Methoden festlegen.

9. Konfiguration des Domänencontrollers, sodass er dem Speicherzonencontroller für die Delegierung vertraut

   Legen Sie fest, dass der Domänencontroller die NTLM- oder Kerberos-Authentifizierung auf Netzwerkfreigaben oder SharePoint-Sites unterstützt.

10. Anfügen eines sekundären Speicherzonencontrollers an eine Speicherzone

    Konfigurieren Sie eine Speicherzone mit hoher Verfügbarkeit durch Einbinden von mindestens zwei StorageZones Controllers.

Eine Demonstration zum Konfigurieren des StorageZones Controller mit Microsoft Azure Storage finden Sie unter hier klicken.

Eine Demonstration zum Konfigurieren von ShareFile Enterprise für die Verwendung einer Microsoft Azure-Speicherzone finden Sie unter hier klicken.

Zusätzliche Einrichtungsanweisungen

- Konfigurieren von Multi-Tenant-Speicherzonen
- Konfigurieren des StorageZones Controller für Web App-Vorschau, Miniaturansichten und View-Only Sharing

Konfigurieren von Citrix ADC für Speicherzonencontroller

February 11, 2022

NetScaler, Version 10.1 Build 120.1316.e und höher, enthält einen Assistenten, der Sie zur Eingabe grundlegender Informationen zu Ihrer StorageZone Controller-Umgebung auffordert. Dann generiert es eine Konfiguration, die:

- Load gleicht den Datenverkehr über StorageZones Controller aus
- Bietet Benutzerauthentifizierung für Speicherzonen-Connectors
- Validiert URI-Signaturen für ShareFile-Uploads und -Downloads
- Beendet SSL-Verbindungen auf der Citrix ADC Appliance

Das Diagramm zeigt diese Citrix ADC-Komponenten, die von der Konfiguration erstellt wurden:

- **Citrix ADC virtueller Content Switching-Server** — Sendet Benutzeranforderungen für Daten von ShareFile und von StorageZone Connector an den entsprechenden virtuellen Citrix ADC Load Balancing Server.
- **Virtueller Citrix ADC Load Balancing Server -** Load gleicht den Datenverkehr für Ihre StorageZone Controller aus und verarbeitet außerdem Folgendes:
  - Für Datenanfragen aus Ihrem privaten Datenspeicher führt ein virtueller Lastausgleichsserver eine Hash-Validierung durch, um sicherzustellen, dass bei eingehenden Anforderungen gültige URI-Signaturen vorhanden sind.
  - Für Datenanfragen von Speicherzonen-Connectors kann ein virtueller Lastausgleichsserver eine Benutzerauthentifizierung durchführen. Es stoppt eine Benutzeranforderung am Citrix ADC, authentifiziert den Benutzer und führt dann Single Sign-On des Benutzers am StorageZone Controller durch.

> **Hinweis:**
>
> Die Authentifizierung bei Speicherzonen-Connectors über Citrix ADC ist optional. Aufgrund eines bekannten Problems funktionieren Speicherzonen-Connectors in WebApp nicht in Chrome-, Chromium-, Safari- und Edge-Browsern, wenn die Authentifizierung in Citrix ADC aktiviert ist. Es ist mit anderen Browsern und Desktop-/Mobile-Clients kompatibel.

Ab StorageZone Controller 4.0 können Administratoren eingehende Verbindungen zu den StorageZone Controllern auf TLS v1.2 beschränken. Wenn Protokolle vor TLS v1.2 für eingehenden Datenverkehr zum Speicherzonencontroller deaktiviert sind, müssen alle Client-Softwarekomponenten, die mit der Speicherzone interagieren, auch TLS v1.2 unterstützen. Klicken Sie hier für zusätzliche Informationen und Konfigurationsanweisungen.

> **Hinweis:**
>
> Informationen zum Einrichten von NetScaler-Versionen vor 10.1 Build 120.1316.e finden Sie unter Manuelles Konfigurieren von Citrix ADC.

Das Einrichten des Citrix ADC für ShareFile-Assistenten verarbeitet nicht die Konfiguration, die für die Verwendung von Citrix Endpoint Management als SAML-Identitätsanbieter für ShareFile erforderlich ist. Für weitere Informationen klicken Sie hier.

Voraussetzungen

- Eine funktionierende Citrix ADC-Konfiguration
- Sicherheitszertifikat: Wenn noch keines in Citrix ADC verfügbar ist, können Sie mit dem Assistenten eines auf dem virtuellen Content Switching-Server installieren.
- Informationen zu Ihrer Active Directory-Konfiguration (**Der Citrix ADC for ShareFile-Assistent muss mit der Citrix NetScaler Enterprise Edition-Lizenz abgeschlossen werden**):
  - IP-Adresse und Port Ihres Active Directory-Servers
  - Active Directory-Domainname
  - LDAP Basis-DN, in dem Benutzer gespeichert sind
  - Kontoname und Kennwort für ein Administratorkonto, das über Berechtigungen zur Kommunikation mit Active Directory verfügt

Konfigurieren von Citrix ADC für Speicherzonen-Controller

In den folgenden Schritten wird beschrieben, wie Sie den Citrix ADC für ShareFile-Assistenten verwenden.

1. Melden Sie sich bei der Citrix ADC Appliance an und navigieren Sie auf der Registerkarte Konfiguration zu Traffic Management.
2. Klicken Sie unter Citrix ShareFile auf Citrix ADC for ShareFile einrichten.

   Sie können den Assistenten auch wie folgt aufrufen: Klicken Sie unter Mobility auf **Configure Endpoint Management, ShareFile und Citrix Gateway**.
3. Geben Sie die im Assistenten angeforderten Informationen ein.

Option	Beschreibung
Name	Ein Anzeigename für den virtuellen Content Switching-Server.
IP-Adresse	Die externe (öffentliche oder DMZ) IP-Adresse, die für den virtuellen Content Switching-Server verwendet werden soll. Wenn Sie eine DMZ-IP-Adresse verwenden, müssen Sie eine Network Address Translation (NAT) -Zuordnung von Ihrer externen Firewall-Adresse zu dieser DMZ-IP-Adresse definieren.
ShareFile-Daten	Diese Option ist aktiviert und gibt an, dass Sie die Citrix ADC-Verbindung für Speicherzonen für ShareFile-Daten verwenden werden.

Option	Beschreibung
Speicherzonen-Konnektoren für Netzwerkdateifreigabe/SharePoint	Wenn Sie Connectors verwenden und die Benutzerauthentifizierung am Citrix ADC durchführen möchten, aktivieren Sie das Kontrollkästchen.
Zertifikat	Wählen Sie ein Zertifikat oder installieren Sie eines für den virtuellen Content Switching-Server. Wenn Sie ein Zertifikat installieren möchten, werden Sie aufgefordert, das Zertifikat und den privaten Schlüssel hochzuladen. Für Standardzonen müssen Zertifikate öffentlich vertrauenswürdig und nicht selbstsigniert sein.
IP-Adresse des Speicherzonen-Controllers	Die internen IP-Adressen für einen oder mehrere StorageZone Controller-Server. Diese IP-Adressen definieren die StorageZone Controller-Server als Entitäten innerhalb von Citrix ADC. Wenn Sie die Server bereits zu Citrix ADC hinzugefügt haben, klicken Sie auf Aus vorhandenem hinzufügen und wählen Sie die Server aus. Um Citrix ADC für den Lastenausgleich zu verwenden, geben Sie eine interne IP-Adresse für jeden StorageZone Controller-Server ein. Um Citrix ADC nur für SSL und Authentifizierung zu verwenden, geben Sie nur eine IP-Adresse ein.
Port und Protokoll	Der Port und das Protokoll, die für die Kommunikation vom Citrix ADC zu Speicherzonen-Controllern verwendet werden.
Die IP-Adresse des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung (Citrix ADC AAA)	Eine ungenutzte interne IP-Adresse für den virtuellen Citrix ADC AAA-Server. Citrix ADC erstellt diesen virtuellen Server für den eigenen Gebrauch. Der Server benötigt keinen Zugriff von außen.
IP-Adresse und Port des LDAP-Servers	Die IP-Adresse und der Port Ihres Active Directory-Servers. Wenn Sie Citrix ADC bereits einen LDAP-Server hinzugefügt haben, klicken Sie auf die Registerkarte LDAP auswählen und wählen Sie den Server aus.

Option	Beschreibung
Auszeit	Die maximale Anzahl von Sekunden, die der Citrix ADC auf eine Antwort vom LDAP-Server wartet. Der Standardwert ist 3 Sekunden. Der Mindestwert beträgt 1 Sekunde.
Domäne für einmaliges Anmelden	Der Active Directory-Domainname.
Basis-DN (Standort der Benutzer)	Der LDAP Base Distinguished Name (DN), in dem Benutzer gespeichert sind. Geben Sie den DN mit dem allgemeinen Formular an: cn=Users, dc=domain, DC=Net
Administrator Bind DN und Kennwort	Ein Administratorkonto, das über Berechtigungen zur Kommunikation mit Active Directory verfügt.
Anmeldename	Ein LDAP-Attribut, das von Citrix ADC verwendet wird, um zu bestimmen, ob sich Benutzer mit ihrem Benutzernamen oder ihrer E-Mail-Adresse anmelden. Standardmäßig ist sAMAccountName, sodass sich Benutzer mit ihren Benutzernamen anmelden können. Um Benutzer aufzufordern, ihre E-Mail-Adresse für die Anmeldung einzugeben, ändern Sie dieses Feld in userPrincipalName.

Konfigurieren von Citrix ADC für den Webzugriff auf Connectors

Um den Webzugriff auf Speicherzonen-Connectors zu unterstützen, müssen Sie eine zusätzliche Citrix ADC-Konfiguration durchführen, nachdem Sie den Citrix ADC für ShareFile-Assistenten abgeschlossen haben.

- Erstellen und Konfigurieren eines dritten virtuellen Citrix ADC Load Balancing-Servers, mit dem sichergestellt wird, dass ShareFile-Clients Anmeldeinformationen nur senden, wenn sie an einer vertrauenswürdigen ShareFile-Domäne angemeldet sind.

  Wie in den folgenden Schritten beschrieben, konfigurieren Sie den zusätzlichen virtuellen Server so, dass er anonymen Zugriff von Clients auf das Verb HTTP OPTIONS ermöglicht. Die OPTIONS-Anforderung wird an den Speicherzonen-Controller weitergeleitet, ohne authentifiziert zu werden und ohne HTTPS-Callouts, um die Signatur zu validieren. Die CORS-Preflight-Prüfung überprüft das Domänenvertrauen vor dem Senden von Anmeldeinformationen.

Für die Konfiguration ist kein Verständnis von CORS erforderlich. Weitere Informationen zu CORS finden Sie jedoch unter http://enable-cors.org/.

- Um den Webzugriff auf StorageZone Connector zu unterstützen, fügen Sie der Content Switching-Richtlinie, die für den Datenverkehr zu /cifs und /sp verwendet wird, einen Pfad (/ProxyService) hinzu.

Führen Sie die folgenden Schritte in Citrix ADC aus, nachdem Sie den Citrix ADC für ShareFile-Assistenten abgeschlossen haben.

1. Erstellen Sie einen dritten virtuellen Lastausgleichsserver:
   a) Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
   b) Klicken Sie auf Hinzufügen.
   c) Geben Sie die folgenden Werte an:

Option	Wert
Name	Ein Richtlinienname wie SF_ZONE_OPTIONS
Protokoll	SSL
IP-Adresstyp	Nicht adressierbar

   d) Klicken Sie sich durch, um den virtuellen Server zu erstellen.
   e) Um dieselben Dienste an ihn zu binden wie die virtuellen Lastausgleichsserver, die vom Assistenten erstellt wurden: Klicken Sie im Fenster Load Balancing Virtual Server neben Dienst auf > und dann auf Speichern.
   f) Fügen Sie dem virtuellen Server ein Zertifikat hinzu.
2. Erstellen Sie eine Richtlinie für den virtuellen Server, den Sie gerade hinzugefügt haben:
   a) Navigieren Sie zu Traffic Management > Content Switching > Richtlinien.
   b) Klicken Sie im Detailbereich auf Hinzufügen, und geben Sie dann die Werte für Name, virtuellen Ziel-LB-Server und Ausdruck an. Klicken Sie auf **Ausdruckseditor** und erstellen Sie dann diesen Ausdruck Wählen Sie **HTTP**. Wählen Sie **REQ**. Wählen Sie **METHODE**. Wählen Sie EQ (String) und geben Sie OPTIONS ein. Der Ausdruck sollte wie folgt lauten: `HTTP.REQ.METHOD.EQ("OPTIONS")`
   c) Klicken Sie auf **Fertig**.
   d) Klicken Sie auf **Erstellen**.
3. Binden Sie die soeben erstellte Richtlinie an den neuen virtuellen Lastausgleichsserver:
   a) Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**.

b) Klicken Sie in der Liste auf den virtuellen Server und dann auf **Bearbeiten**.

c) Navigieren Sie zum Abschnitt Content Switching-Richtlinienbindung, und klicken Sie auf 2 Content Switching-Richtlinien.

d) Klicken Sie auf **Bindung hinzufügen**.

e) Wählen Sie die neue Inhaltsrichtlinie und wählen Sie den virtuellen Ziel-Lastausgleichsserver aus.

f) Klicken Sie auf **Bind**.

g) Klicken Sie auf **Bindung bearbeiten** und aktualisieren Sie die **Priorität**. Ändern Sie die Priorität der neuen Richtlinie so, dass sie die niedrigste Anzahl der drei Richtlinien hat.

   Die Richtlinie mit dem niedrigsten Wert hat die höchste Priorität und wird daher zuerst behandelt.

4. Aktualisieren Sie die Richtlinie für den Datenverkehr zu den Speicherzonen-Connectors (_SF_CIF_SP_CSPOL):

   a) Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**.

   b) Wählen Sie die Richtlinie _SF_CIF_SP_CSPOL aus.

   c) Fügen Sie dem Richtlinienausdruck Folgendes hinzu:

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

   Der vollständige Richtlinienausdruck sollte wie folgt lauten:

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

5. Aktualisieren Sie die Richtlinie, die für den Datenverkehr zu Speicherzonen für ShareFile-Daten verwendet wird (_SF_SZ_CSPOL):

   a) Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**.

   b) Wählen Sie die Richtlinie **_SF_SZ_CSPOL** aus.

   c) Fügen Sie dem Richtlinienausdruck Folgendes hinzu:

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

   Der vollständige Richtlinienausdruck sollte wie folgt lauten:

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


Konfigurieren von Citrix ADC für die Freigabe mit Leserechten

Um die Freigabe mit Leserechten zu unterstützen, müssen Benutzer auf Ihren Microsoft Office Web Apps Server (OWA) zugreifen können. Wenn Ihr OWA-Server unter seiner eigenen Adresse extern zugänglich ist, sollte keine zusätzliche Citrix ADC-Konfiguration für Ihren StorageZone Controller erforderlich sein.

Wenn Sie den StorageZone Controller und Office Web App Server mithilfe von Citrix ADC Content Switching-Richtlinien in einer einzigen externen Adresse kombinieren möchten, müssen Sie nach Abschluss des Citrix ADC for ShareFile Assistenten eine zusätzliche Citrix ADC-Konfiguration durchführen. Die Citrix ADC-Konfiguration ist erforderlich, um sicherzustellen, dass der Datenverkehr ordnungsgemäß an Ihren extern zugänglichen OWA-Server weitergeleitet wird.

Sobald die folgenden Citrix ADC-Regeln konfiguriert sind, können Administratoren die vorhandene externe Adresse ihrer StorageZone Controller-Zone wiederverwenden, sodass keine zusätzliche externe Adresse für OWA erstellt werden muss.

So erstellen und konfigurieren Sie einen zusätzlichen virtuellen Citrix ADC Load Balancing-Server:

1. Erstellen Sie einen zusätzlichen Lastausgleichsdienst.
   - Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
   - Klicken Sie auf **Hinzufügen**.
   - Geben Sie die erforderlichen Informationen ein, um einen Dienst zu erstellen, der Ihren OWA-Servern entspricht. Klicken Sie auf **OK**.
2. Erstellen Sie einen zusätzlichen virtuellen Lastausgleichsserver:
   - Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
   - Klicken Sie auf **Hinzufügen**.
   - Geben Sie die folgenden Werte an:

Option	Wert
Name	Ein Richtlinienname wie sf_OWA_vServer
Protokoll	SSL
IP-Adresstyp	Nicht adressierbar

   - Klicken Sie sich durch, um den virtuellen Server zu erstellen.
   - Um den virtuellen Server an den OWA-Dienst zu binden, den Sie im vorherigen Schritt erstellt haben, klicken Sie auf **Load Balancing Virtual Service Binding > Dienst auswählen**. Klicken Sie auf das Kontrollkästchen neben dem Dienst, den Sie im vorherigen Schritt erstellt haben.

- Klicken Sie auf **Select**.
- Klicken Sie auf **Bind**.

3. Erstellen Sie eine neue Richtlinie, mit der der Datenverkehr an Ihren OWA-Server weitergeleitet wird.
   - Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**.
   - Wählen Sie **Hinzufügen**aus.
   - Nennen Sie die Richtlinie.
   - Füge den folgenden Ausdruck hinzu:
     - HTTP.REQ.URL.CONTAINS (“/hosting/discovery”)
       || HTTP.REQ.URL.CONTAINS (“/x/”)
       || HTTP.REQ.URL.CONTAINS (“/wv/”)
       || HTTP.REQ.URL.CONTAINS (“/p/”)
       Der vollständige Richtlinienausdruck sollte wie folgt lauten:
       HTTP: //REQ.URL.CONTAINS (“/hosting/discovery”)
       || HTTP: //REQ.URL.CONTAINS (”/x/”)
       || HTTP.REQ.URL.CONTAINS (“/wv/”)
       || HTTP.REQ.URL.CONTAINS (“/p/”)
4. Aktualisieren Sie die Priorität der neuen Richtlinie innerhalb des virtuellen Lastausgleichs
   - Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**.
   - Klicken Sie auf den virtuellen Server für den Lastausgleich, und wählen Sie dann Content Switching-Richtlinien aus.
   - Ändern Sie die Priorität der Richtlinien so, dass die (Beispiel) “_SF_OWA”-Richtlinie an dritter Stelle steht.

Priorität	Name der Richtlinie
90	SF_ZK_OPTIONS
95	_SF_CIF_SP_SPOL
99	_SF_OWA
100	_SF_SZ_CSPOL

- Klicken Sie auf **Schließen**. Klicken Sie auf **Fertig**

Erstellen eines Monitors für den StorageZone Controller-

Standardmäßig pingt Citrix ADC den StorageZone Controller-Server an, um festzustellen, ob er online ist. Selbst wenn der Controller online ist, kann er möglicherweise keine Heartbeat-Nachrichten an

die ShareFile-Website senden. In diesem Fall sendet Citrix ADC Datenverkehr an den StorageZone Controller, obwohl es nicht mit ShareFile kommuniziert.

Um die ausgehende Konnektivität des StorageZone Controllers mit ShareFile zu überprüfen, können Sie einen Monitor erstellen, der heartbeat.aspx überprüft und sie für jeden StorageZone Controller an den Citrix ADC-Dienst bindet.

```
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 ist der Citrix ADC-Dienst, der einem StorageZones-Controller entspricht. Dieser Dienstname wird automatisch vom Citrix ADC for ShareFile-Assistenten erstellt. Der Dienstname umfasst die IP-Adresse des Controllers, z. B. SF_SVC_IP-Adresse.

-secure YES ist erforderlich, wenn der Dienst Port 443 abhört.

Überprüfen der Citrix ADC-Konfiguration

Nachdem Sie den Assistenten abgeschlossen haben, gehen Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, um den Status der virtuellen Lastausgleichsserver anzuzeigen, die vom Assistenten erstellt wurden.

Zeigen Sie den Durchsatz von ShareFile-Anforderungen über Citrix ADC an

Durchsatzstatistiken finden Sie im **Dashboard-Menü** .

Manuelle Konfiguration von Citrix ADC

April 25, 2023

Ab Version 10.1 Build 120.1316 enthält NetScaler einen Assistenten, der die Einstellungen konfiguriert, die für die Daten und Connectors des Storage Zone Controllers erforderlich sind.

Die Schritte in diesem Abschnitt beschreiben die **Citrix ADC-Einstellungen**, die für den Storage Zone Controller erforderlich sind. Alle Links beziehen sich auf die NetScaler 10.1-Dokumentation. Ähnliche Themen sind für spätere Versionen von Citrix ADC verfügbar.

Alle eingehenden Nachrichten auf gültige URI-Signaturen überprüfen

1. Erstellen Sie einen HTTP-Callout mit dem Namen sf_callout:

a) Klicken Sie im Dialogfeld “HTTP-Callout konfigurieren”auf **Virtueller Server oder IP-Adresse** und geben Sie die Adresse an.

b) Klicken Sie unter An den Server zu sendende Anforderung auf **Attributbasiert** und dann auf **Anforderungsattribute konfigurieren**.

c) Wählen Sie **Methode abrufen**.

d) Geben Sie in Host Expression die IP-Adresse des virtuellen Servers oder die Host-IP-Adresse für einen der StorageZones-Controller ein.

e) Geben Sie für URL Stem Expression Folgendes ein:

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

f) Klicken Sie auf **OK**, und kehren Sie zum Dialogfeld HTTP-Callout konfigurieren zurück.

g) Wählen Sie unter Serverantwort einen Rückgabetyp von Bool aus.

h) Geben Sie im Feld “Ausdruck zum Extrahieren von Daten aus der Antwort”Folgendes ein:

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

i) Klicken Sie auf **Erstellen**.

2. Folgen Sie den vorherigen Schritten, um einen HTTP-Callout mit dem Namen sf_callout_y zu konfigurieren. Verwenden Sie dieselben Einstellungen mit Ausnahme des Ausdrucks:

   - Geben Sie für URL Stem Expression Folgendes ein:

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

3. Konfigurieren Sie eine Responder-Richtlinie:

   a) Wählen Sie im Dialogfeld “Responder-Richtlinie konfigurieren”als Aktion die Option “Drop”aus.

   b) Geben Sie den Ausdruck ein:

```
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)
```

   Weitere Informationen finden Sie unter Responder.

4. Binden Sie die Responder-Richtlinie an den virtuellen Load Balancer-Server und konfigurieren Sie die sitzungsbasierte SSL-Persistenz.

Zum Lastausgleich

1. Konfigurieren Sie den tokenbasierten Lastausgleich.

   Verwenden Sie den Regelausdruck: “ `http.REQ.URL.QUERY.VALUE("uploadid")` ”

   Für StorageZones-Controller in einer Bereitstellung mit hoher Verfügbarkeit ist ein tokenbasierter Lastausgleich erforderlich. Round-Robin-Lastausgleich führt zu zeitweiligen Download- oder Uploadfehlern, da eine Client-Anfrage für einen Upload oder Download an einen anderen StorageZone-Controller als den weitergeleitet werden kann, der die Autorisierungsanfrage von ShareFile.com erhalten hat.

2. Konfigurieren Sie Citrix ADC so, dass SSL-Verbindungen beendet werden.

   Weitere Informationen finden Sie unter SSL-Offloading konfigurieren.

So konfigurieren Sie Content Switching und Authentifizierung für Connectors

1. Informationen zum Aktivieren von Content Switching finden Sie unter Content Switching aktivieren.

2. Erstellen Sie eine Richtlinie zum Content Switching für Benutzeranforderungen für ShareFile Daten aus Ihren lokalen Speicherzonen:

   a) Geben Sie im Dialogfeld “Richtlinie für Content Switching konfigurieren”einen Namen für die Content Switching-Richtlinie ein. Diese Schritte verwenden den Namen Data_Requests.

   b) Geben Sie den Ausdruck ein:

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

   c) Klicken Sie auf **OK**.

   Weitere Informationen finden Sie unter Content Switching.

3. Erstellen Sie eine Content Switching-Richtlinie für Benutzeranforderungen für Daten, auf die über StorageZone Connector zugegriffen wird.

   a) Geben Sie im Dialogfeld Content Switching-Richtlinie konfigurieren einen Namen für die Content Switching-Richtlinie an. Diese Schritte verwenden den Namen Connector_Requests.

   b) Geben Sie den Ausdruck ein:


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

Stellen Sie sicher, dass Sie “StorageZonesControllerFQDN”durch den FQDN Ihres Controllers ersetzen.

c) Klicken Sie auf **OK**.

4. Erstellen Sie einen virtuellen Content Switching-Server.
5. Legen Sie die Richtlinienziele für Content Switching fest:
   - Geben Sie im Dialogfeld Virtuellen Server konfigurieren (Content Switching) für die Data_Requess-Richtlinie den virtuellen Load Balancer-Server für Speicherzonen für ShareFile-Daten an.

     Dieser virtuelle Load Balancer-Server bindet die Responder-Richtlinie in Schritt 4, um alle eingehenden Nachrichten auf gültige URI-Signaturen zu überprüfen und den Lastausgleich zu gewährleisten.
   - Geben Sie für die Connector_Requess-Richtlinie den virtuellen Load Balancer-Server für Storage Zone-Connectors an.
6. Konfigurieren Sie den virtuellen Authentifizierungsserver für den Storage Zone Controller:

   Die Authentifizierung bei Citrix ADC ist zwar optional, aber eine empfohlene bewährte Methode.

   a) Erweitern Sie im Navigationsbereich Load Balancing, wählen Sie den Namen des virtuellen Load Balancer-Servers für Storage Zones Connectors aus, und klicken Sie dann auf Öffnen.

   b) Klicken Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf die Registerkarte Erweitert und erweitern Sie dann Authentifizierungseinstellungen.

   c) Aktivieren Sie das Kontrollkästchen für 401 Based Authentication und wählen Sie dann den virtuellen Authentifizierungsserver aus.

   d) Klicken Sie auf die Registerkarte **Methode und Persistenz**.

   e) Wählen Sie für Persistenz **COOKIEINSERT**.

   f) Geben Sie für Timeout (min) **240** ein.

      Ein Timeout-Wert von 240 Minuten wird empfohlen. Verwenden Sie einen Mindestwert von mehr als 10 Minuten.

      Weitere Informationen finden Sie unter Konfiguration des virtuellen Authentifizierungsservers.
7. Verwenden Sie das Dialogfeld Authentifizierungsserver konfigurieren, um einen Authentifizierungsserver zu erstellen und zu konfigurieren.

Geben Sie im Feld SSO-Namenattribut **userPrincipalName** ein.

Weitere Informationen zu anderen Einstellungen finden Sie unterAuthentifizierungsrichtlinien.

8. Konfigurieren Sie eine Authentifizierungsrichtlinie für den Authentifizierungsserver:

   a) Geben Sie im Dialogfeld Authentifizierungsrichtlinie konfigurieren einen Namen für die Richtlinie ein und wählen Sie dann den im vorherigen Schritt konfigurierten Authentifizierungsserver aus.

   b) Geben Sie den Ausdruck ein:

   ```
   ns_true
   ```

   Weitere Informationen finden Sie unter Konfigurieren einer Authentifizierungsrichtlinie.

9. Konfigurieren Sie ein Sitzungsprofil für Single Sign-On:

   a) Geben Sie im Dialogfeld "Sitzungsprofil konfigurieren"einen Namen für das Profil ein.
   b) Aktivieren Sie das Kontrollkästchen für Single Sign-On bei Webanwendungen.
   c) Wählen Sie für Credential Index die Option **PRIMARY**aus.
   d) Geben Sie in der Single Sign-On-Domäne den Domainnamen für Ihren Storage Zones Controller ein.
   e) Aktivieren Sie die Kontrollkästchen **Global überschreiben** für jedes der drei vorangegangenen Elemente.

   Weitere Informationen finden Sie unter Sitzungsprofile.

10. Konfigurieren Sie eine Sitzungsrichtlinie für Single Sign-On:

    a) Geben Sie im Dialogfeld "Sitzungsrichtlinie konfigurieren"einen Namen für die Richtlinie ein.

    b) Wählen Sie für "Profil anfordern"den Namen des im vorherigen Schritt konfigurierten Sitzungsprofils aus.

    c) Geben Sie den Ausdruck ein:

    ```
    ns_true
    ```

    Weitere Informationen finden Sie unter Sitzungsrichtlinien.

11. Erstellen Sie einen virtuellen Authentifizierungsserver:

    a) Geben Sie im Dialogfeld Virtuellen Server konfigurieren (Authentifizierung) einen Namen und die IP-Adresse für den Server ein.
    b) Klicken Sie auf die Registerkarte Authentifizierung und wählen Sie für Protokoll die Option **SSL**aus.
    c) Aktivieren Sie das Kontrollkästchen für Benutzer authentifizieren.

d) Klicken Sie unter Authentifizierungsrichtlinien auf **Primär** und wählen Sie dann die Authentifizierungsrichtlinie aus, die Sie in Schritt 7 konfiguriert haben.
e) Klicken Sie auf die Registerkarte Richtlinien, klicken Sie auf **Sitzung** und wählen Sie dann die Sitzungsrichtlinie aus, die Sie in Schritt 9 konfiguriert haben.

Weitere Informationen finden Sie unter Konfiguration des virtuellen Authentifizierungsservers.

Erstellen einer Netzwerkfreigabe für die private Datenspeicherung

October 13, 2020

Speicherzonen für ShareFile Daten erfordern eine Netzwerkfreigabe für Ihre privaten Daten. Wenn mehrere StorageZones Controller für hohe Verfügbarkeit und Lastausgleich innerhalb einer Zone konfiguriert sind, greifen alle Controller auf denselben freigegebenen Speicherort für private Daten zu.

Selbst wenn Sie ShareFile-Dateien in einem unterstützten Speichersystem von Drittanbietern speichern, erfordert der StorageZones Controller eine Netzwerkfreigabe für Verschlüsselungsschlüssel, in der Warteschlange gestellte Dateien, andere temporäre Elemente und einen Speichercache für Datei-Uploads oder Downloads von diesem Speichersystem. Weitere Hinweise zum Speichercache finden Sie unter Anpassen von Speicher-Cache-Vorgängen.

StorageZones Controller greifen mithilfe des IIS-Kontopool-Benutzers auf eine Netzwerkfreigabe zu. Standardmäßig arbeiten Anwendungspools unter dem Netzwerkdienst-Benutzerkonto, das über Benutzerrechte auf niedriger Ebene verfügt. Der StorageZones Controller verwendet standardmäßig das Netzwerkdienstkonto. Sie können anstelle des Netzwerkdienstkontos ein benanntes Benutzerkonto verwenden, um auf die Freigabe zuzugreifen. Verwenden Sie das Netzwerkdienstkonto, um den IIS-Anwendungspool und die Citrix ShareFile Services auszuführen.

1. Wenn Sie anstelle des Netzwerkdienstkontos ein benanntes Benutzerkonto für den Zugriff auf die Freigabe verwenden möchten, erstellen Sie ein benanntes Benutzerkonto in Active Directory. Dieses benannte Benutzerkonto wird als ShareFile Dienstkonto bezeichnet.
   Hinweis: Wenn Sie den StorageZones Controller konfigurieren, geben Sie den Netzwerkfreigabebenutzernamen und das Netzwerkfreigabekennwort an. Dabei handelt es sich um die Anmeldeinformationen für das Konto, das Sie für den Zugriff auf die Freigabe verwenden, entweder das ShareFile e-Dienstkonto oder das Netzwerkdienstkonto.

   Um die Sicherheit zu verbessern, muss der Administrator allen anderen Benutzern Berechtigungen für den bestimmten Ordner mit dem ShareFile Speicher-Repository verweigern und nur dem Benutzer des Speicherorts Zugriff gewähren, der konfiguriert wird.

2. Stellen Sie eine Verbindung mit dem Server her, auf dem die Netzwerkfreigabe gehostet wird, und erstellen Sie einen Ordner für Ihre privaten ShareFile Daten.

3. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie Für bestimmte Personen freigeben…
4. Fügen Sie das Konto hinzu, mit dem Sie auf die Freigabe zugreifen möchten (Netzwerkdienstkonto oder ShareFile Dienstkonto), und ändern Sie die Berechtigungsstufe in Lese-/Schreibzugriff.
5. Klicken Sie auf Freigeben und dann auf Fertig.
6. Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie Eigenschaften.
7. Stellen Sie auf der Registerkarte Sicherheit sicher, dass das Konto, das Sie für den Zugriff auf die Freigabe (Netzwerkdienstkonto oder ShareFile Dienstkonto) verwenden möchten, über Vollzugriff verfügt.

Erhöhen Sie die Anzahl der Dateien pro Zone

Standardmäßig ist ein Storage Zones Controller so konfiguriert, dass eine CIFS-Freigabe zum Speichern von Dateien in einer Ordnerhierarchie anstelle eines einzelnen Ordners verwendet wird.

Sie können den StorageZones Controller so konfigurieren, dass er das persistente Speicherlayout aufteilt. Dies erhöht die maximale Anzahl von Dateien pro Zone für einige Arten von Speicher-Arrays von weniger als einer halben Million auf zehn Millionen oder mehr. Wenn Sie zusätzliche Kapazität benötigen, können Sie die Standardeinstellung ändern.

So aktivieren Sie den StorageZones Controller zum Speichern von Dateien in mehreren Ordnern

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.
>
> **Hinweis:**
>
> Wenn der StorageZones Controller aktualisiert wurde, überprüfen Sie bitte, ob der Wert des Registrierungsschlüssels `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone\PathSelection is set to 1. If it is set to 0, update it to 1`.

Starten Sie IIS auf den StorageZones Controllern neu, wenn Sie die Bearbeitung der Registrierung abgeschlossen haben.

So erhöhen Sie die maximale Anzahl von Ordnern

Standardmäßig verfügt das geteilte Speicherlayout über 256 Ordner der obersten Ebene, von denen jeder 256 Ordner enthält. Diese Konfiguration wird im Registrierungsschlüssel des primären StorageZones Controller dargestellt `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone: PathSelectionParams=2,2`.

Der erste Wert beschränkt die Anzahl der Ordner der obersten Ebene auf “16 to the power of 2”oder 256. Der zweite Wert beschränkt auch die Anzahl der untergeordneten Ordner der obersten Ebene auf 256.

Mit derselben Formel (16 bis zur Stärke von N) können Sie die entsprechenden Werte für Ihre Website bestimmen. Beispielsweise beschränkt PathSelectionParams=3,4,4,4 die Anzahl der Ordner der obersten Ebene auf 4096 (16 auf die Potenz von 3). Der zweite Wert beschränkt die Anzahl der untergeordneten Ordner der obersten Ebene auf 65536 (16 auf die Potenz von 4). Der dritte Wert beschränkt die Anzahl der untergeordneten Ordner der zweiten Ebene auf 65536 usw.

Starten Sie IIS auf den primären und sekundären StorageZones Controllern neu, wenn Sie die Bearbeitung der Registrierung abgeschlossen haben.

So entfernen Sie leere Ordner

Wenn der StorageZones Controller Dateien in mehreren Ordnern speichert, kann das Löschen von Dateien zu leeren Ordnern führen. Standardmäßig entfernt der Storage Zones Controller leere Ordner. Der Dateilöschdienst löscht leere Ordner, beginnt am unteren Rand des Baums und fährt fort, bis er einen nicht leeren Ordner erreicht.

Einige Upgrade-Pfade aktualisieren Ihre Einstellungen jedoch möglicherweise nicht. Stellen Sie nach einem Upgrade sicher, dass der folgende Schlüssel in angezeigt wird `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`:

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

Wenn Sie den Schlüssel hinzufügen müssen, starten Sie den Dateilöschdienst neu, wenn Sie fertig sind.

Installieren eines SSL-Zertifikats

June 11, 2020

Wenn Sie kein Platzhalterzertifikat verwenden, müssen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für den StorageZones Controller-Server erstellen und Ihre Anforderung an eine Zertifizierungsstelle senden. Hilfe finden Sie in der Dokumentation zu Ihrer Zertifizierungsstelle.

Gehen Sie folgendermaßen vor, um ein Zertifikat zu installieren.

1. Öffnen Sie auf dem StorageZones Controller-Server die MMC und wählen Sie dann **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie Zertifikate aus, und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie Computerkonto aus, klicken Sie auf **Weiter**, klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **OK**.
4. Erweitern Sie in der MMC-Konsole **Zertifikate > Persönlich**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, wählen Sie **Alle Aufgaben > Importieren**, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Durchsuchen**, und wählen Sie dann im Menü Dateinamenerweiterung die Option **Persönlicher Informationsaustausch**.
7. Navigieren Sie zum Speicherort des Zertifikats, und klicken Sie dann auf **Öffnen**.
8. Klicken Sie auf **Weiter**, geben Sie das **Kennwort** für Ihren privaten Schlüssel ein, klicken Sie zweimal auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.
9. Wenn die Meldung **Import war erfolgreich** angezeigt wird, klicken Sie auf **OK**.

Stellen Sie für ein öffentliches Zertifikat sicher, dass die Domäne, für die sie ausgestellt wird, in die lokale IP-Adresse des StorageZones Controller aufgelöst wird. Aktualisieren Sie dazu die Host-Datei auf dem StorageZones Controller, um die dem Zertifikat zugeordnete Domäne der StorageZones Controller-IP-Adresse zuzuordnen. Wenn die beiden Adressen nicht aufgelöst werden, können Benutzer keine Dateien vom StorageZones Controller hochladen.

Vorbereiten des Servers für ShareFile Daten

November 14, 2023

Die in diesem Abschnitt beschriebene Webserver-Rolle (IIS) und das ASP.NET-Setup sind für Speicherzonen für ShareFile-Daten und für Speicherzonenkonnektoren erforderlich. Diese Anweisungen basieren auf Windows Server 2012, gelten aber auch für spätere Versionen.

Microsoft.NET-Version aktualisieren

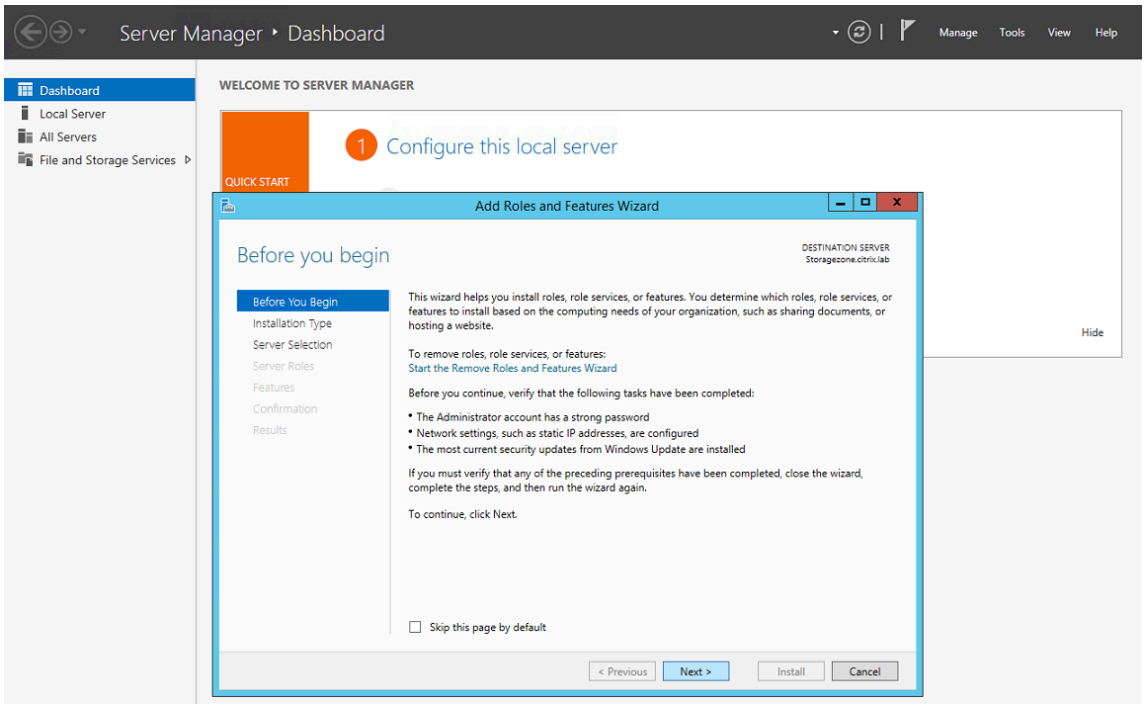
Bevor Sie mit der Installation des Storage Zones Controllers fortfahren, stellen Sie sicher, dass Sie die entsprechende Version von Microsoft.NET Framework verwenden.

- **StorageZones Controller 5.x erfordert.NET 4.8 oder höher**. Klick hier um .NET 4.8 herunterzuladen

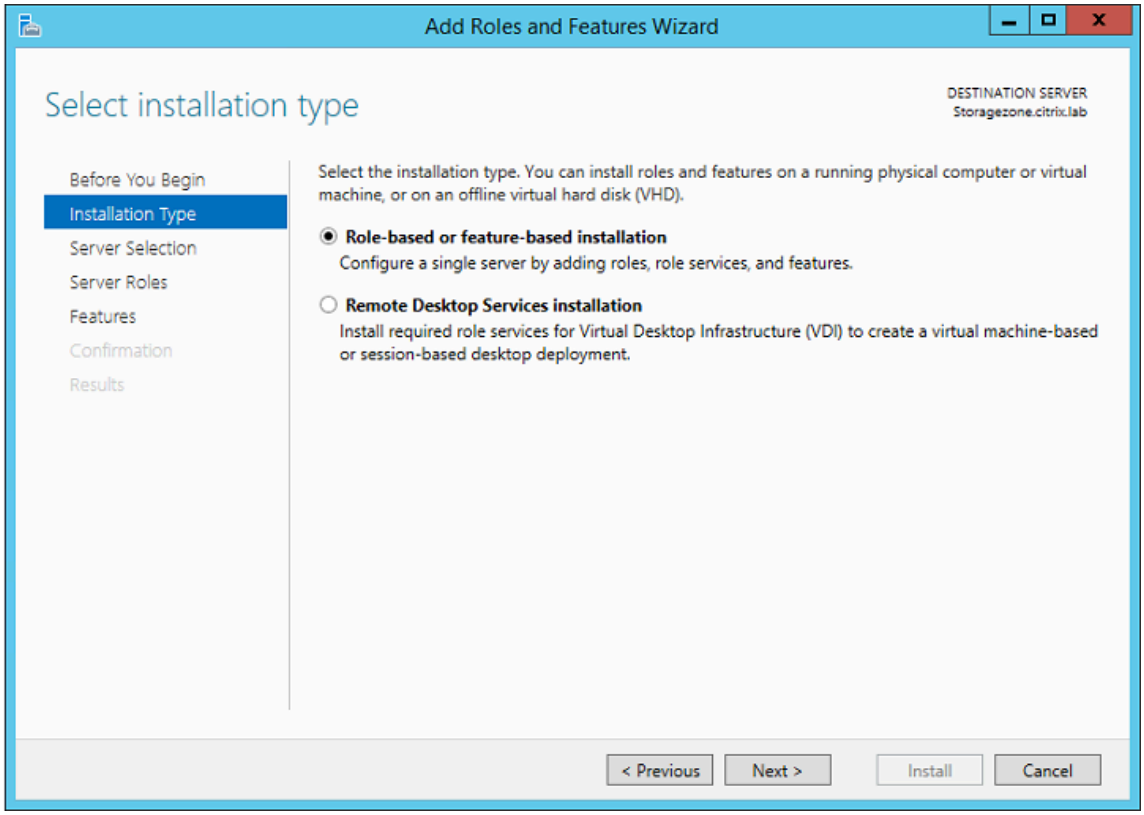
ShareFile empfiehlt, bei der Verwendung von ShareFile-Anwendungen die neueste Version von Microsoft.NET zu verwenden.

So aktivieren Sie die Webserver-Rolle (IIS) und den ASP.NET-Rollendienst

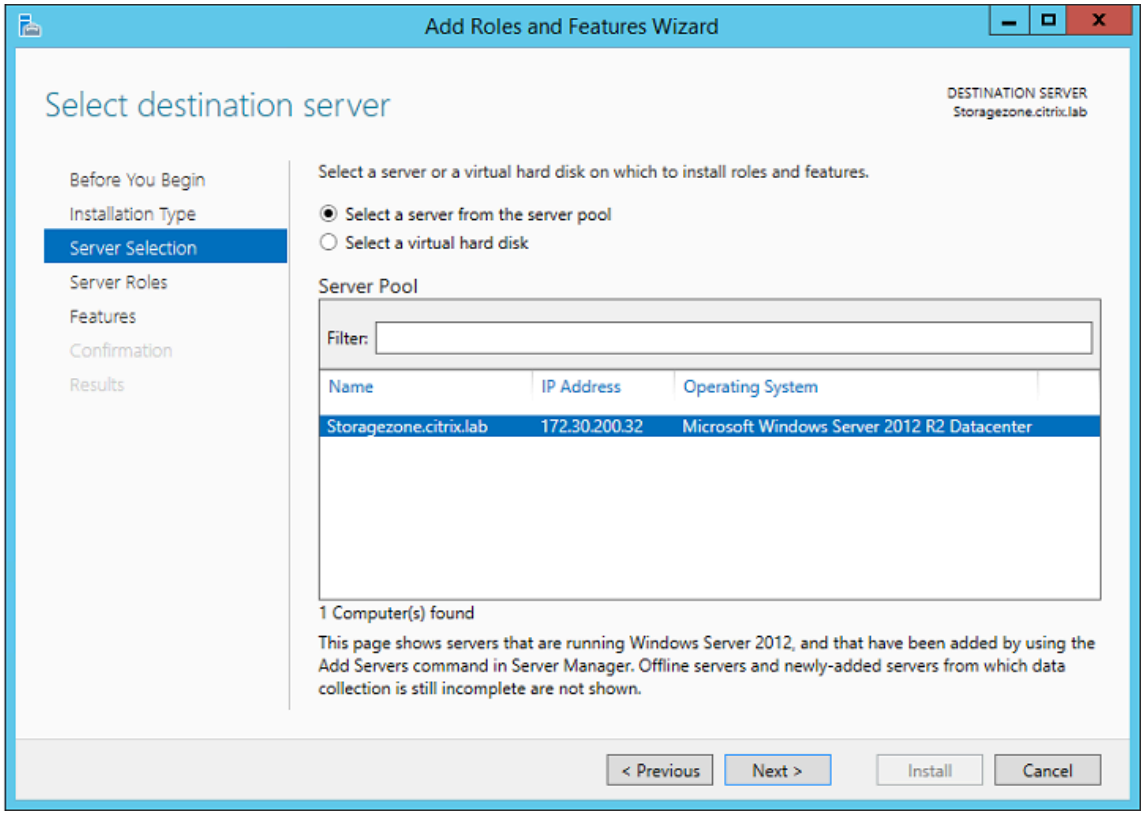
1. Melden Sie sich auf dem Server, auf dem Sie den StorageZones Controller installieren, mit einem Konto an, das über lokale Administratorrechte verfügt.
2. Öffnen Sie das Dashboard der Server-Manager-Konsole und klicken Sie dann auf **Verwalten > Rollen und Funktionen hinzufügen**, um den Assistenten zum Hinzufügen von Rollen und Funktionen zu öffnen.
3. Klicken Sie im Assistenten zum Hinzufügen von Rollen und Funktionen auf **Weiter**.



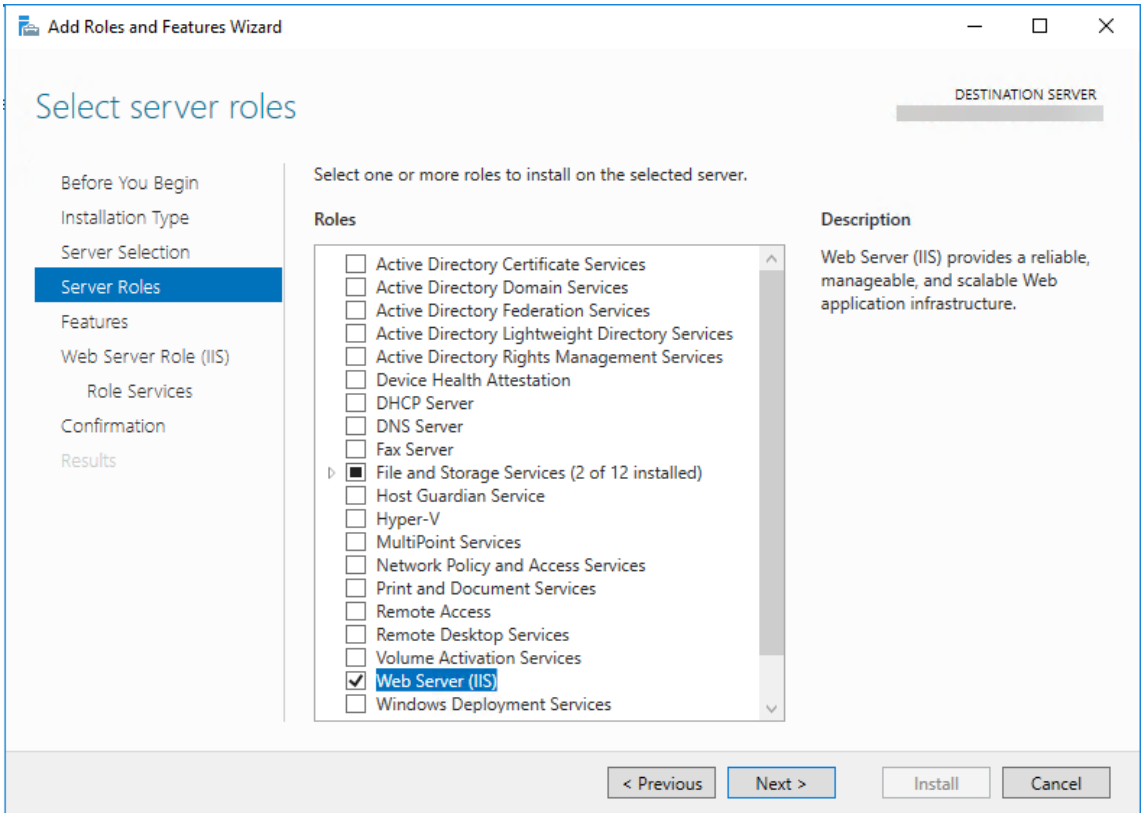
4. Klicken Sie auf der Seite Installationstyp auswählen auf Rollenbasierte oder featurebasierte Installation und dann auf **Weiter**.



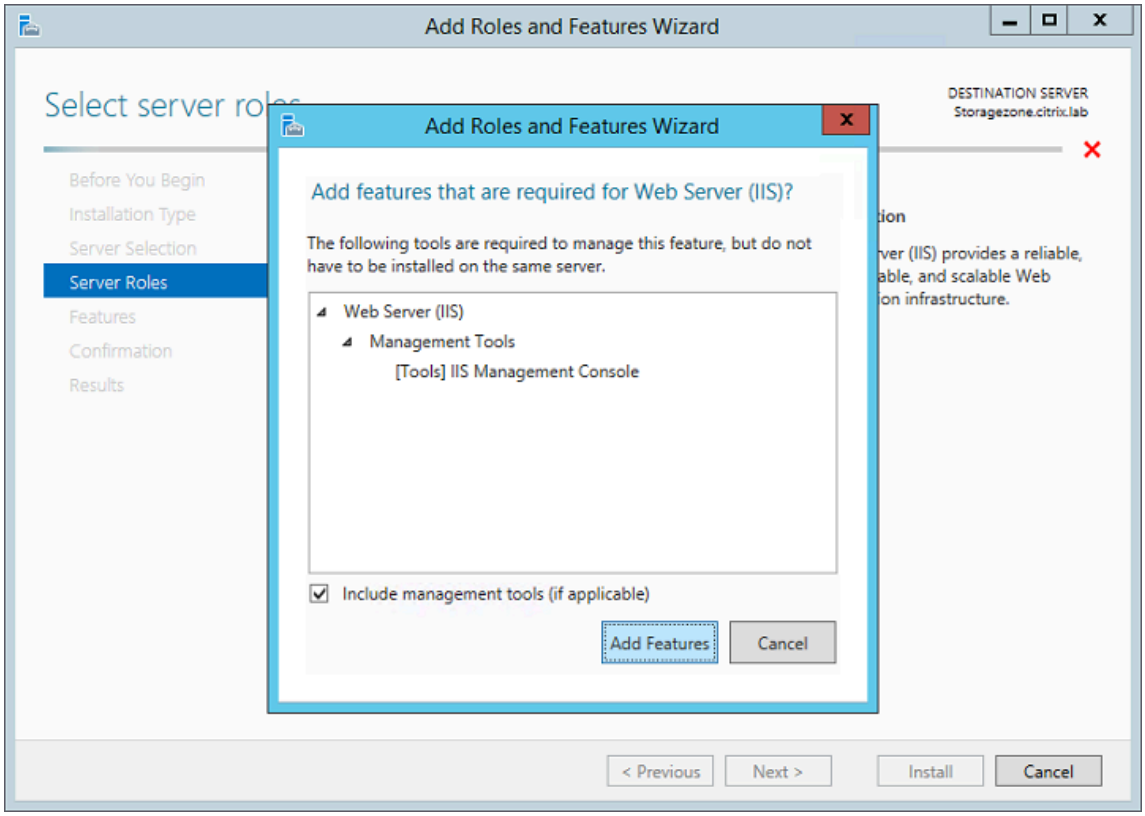
5. Wählen Sie auf der Seite Zielserver auswählen Ihren Server aus dem Serverpool aus und klicken Sie dann auf **Weiter**.



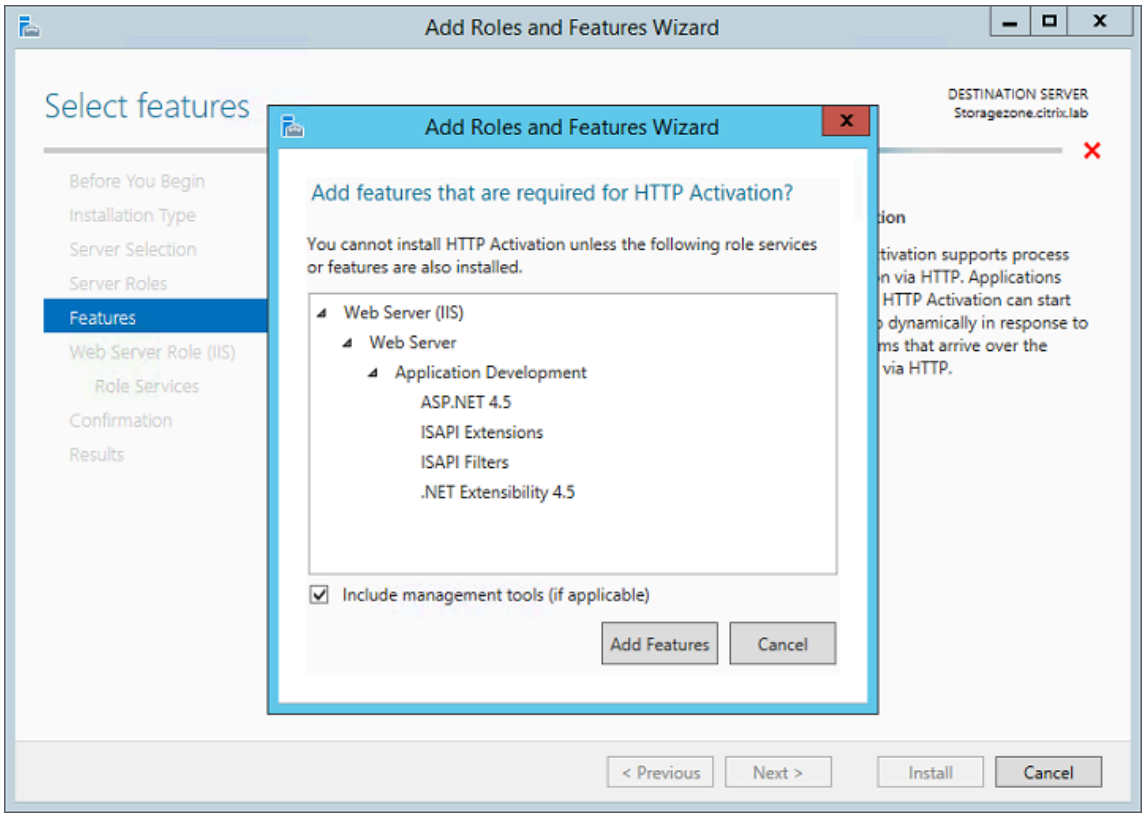
6. Aktivieren Sie auf der Seite Serverrollen auswählen das Kontrollkästchen Webserver (IIS) und klicken Sie dann auf **Weiter**.



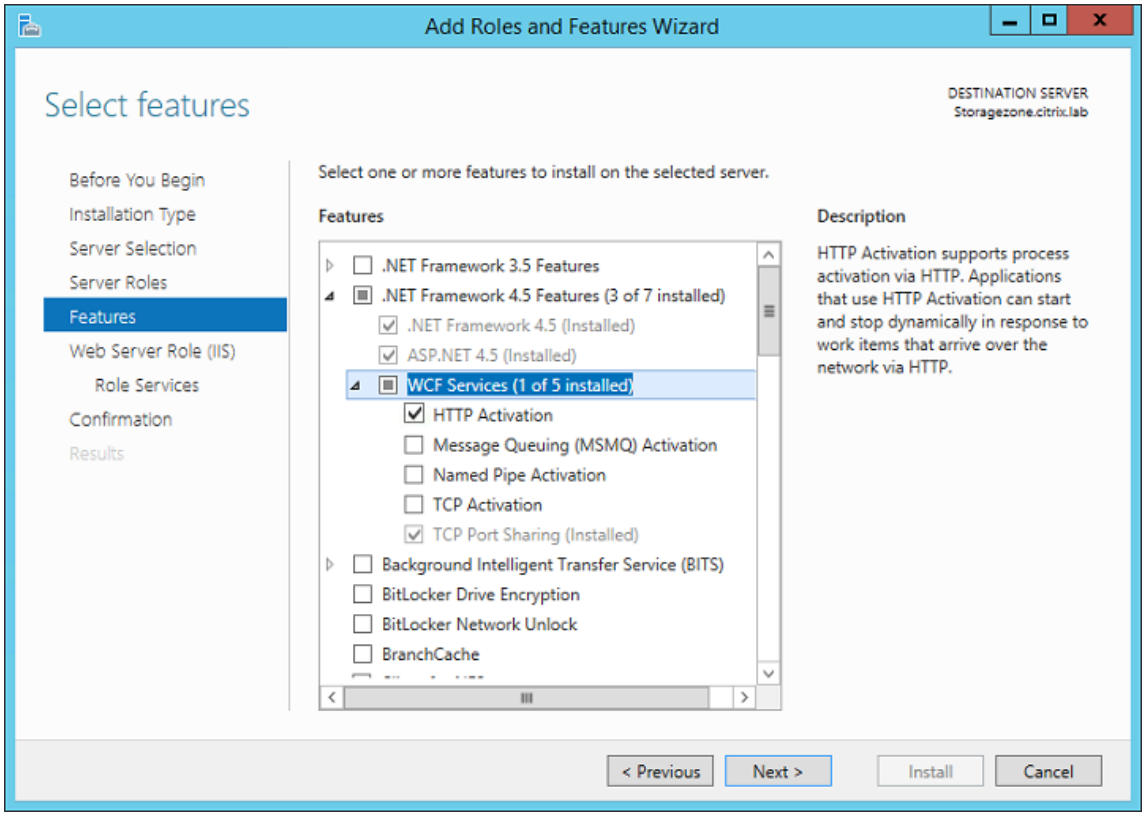
7. Klicken Sie auf **Funktionen hinzufügen**, um die für IIS erforderlichen Funktionen hinzuzufügen.



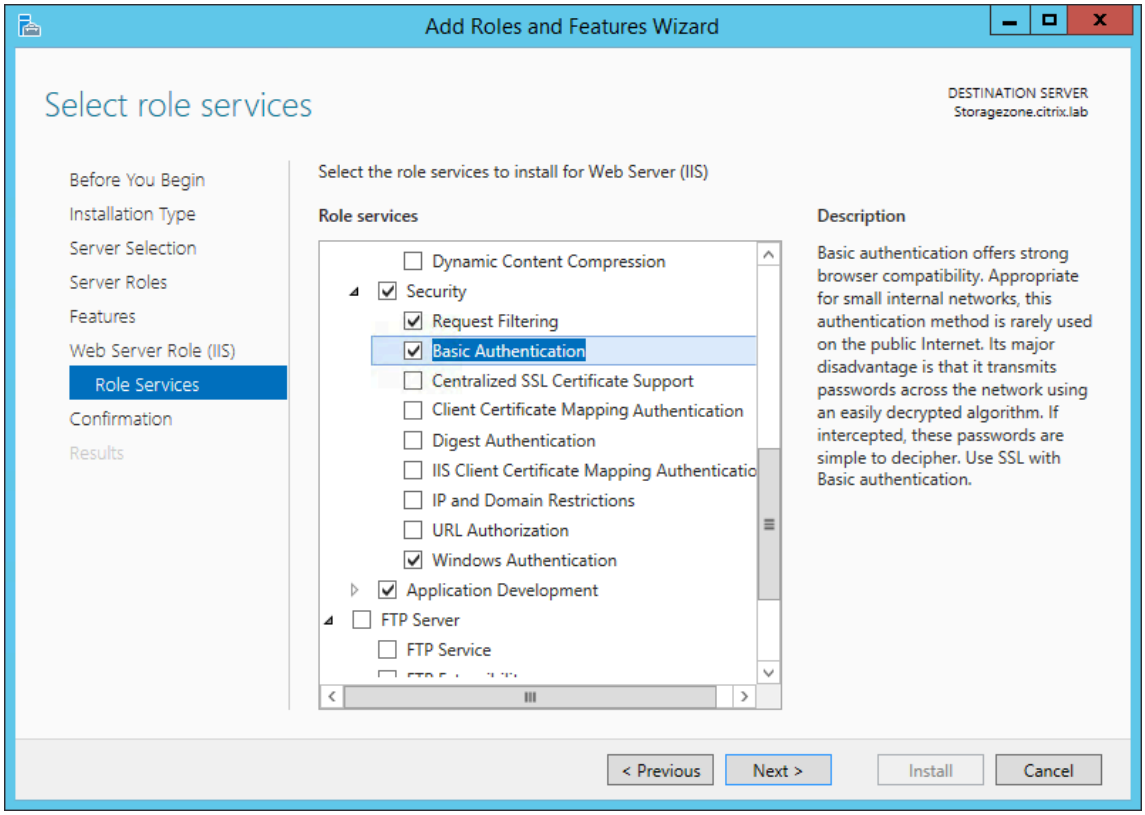
8. Klicken Sie auf **Funktionen hinzufügen**. Die Seite “Funktionen auswählen”wird angezeigt.



9. Wählen Sie die erforderlichen Einstellungen aus, die auf dem folgenden Bildschirm angezeigt werden, und klicken Sie dann auf **Weiter**.



10. Klicken Sie auf der Seite Web Server Role (IIS) auf **Weiter**.
11. Aktivieren Sie auf der Seite “Rollendienste auswählen”die Kontrollkästchen Standardauthentifizierung und Windows-Authentifizierung, und klicken Sie dann auf **Weiter**.

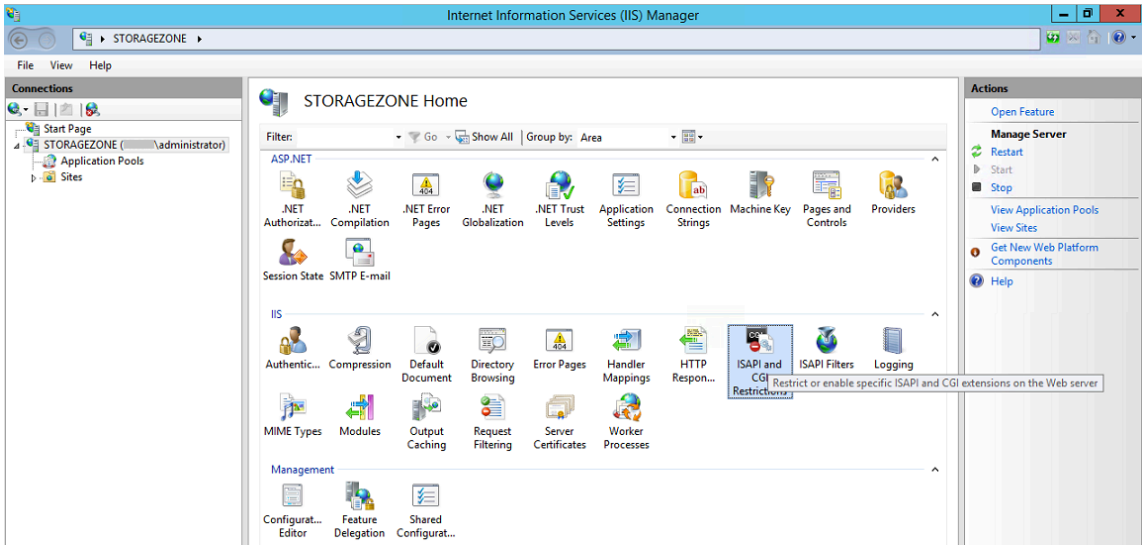


12. Klicken Sie auf der Seite “Installationsauswahl bestätigen”auf **Installieren**.
13. Wenn die Installation abgeschlossen ist, klicken Sie auf **Schließen** und starten Sie den Server neu.

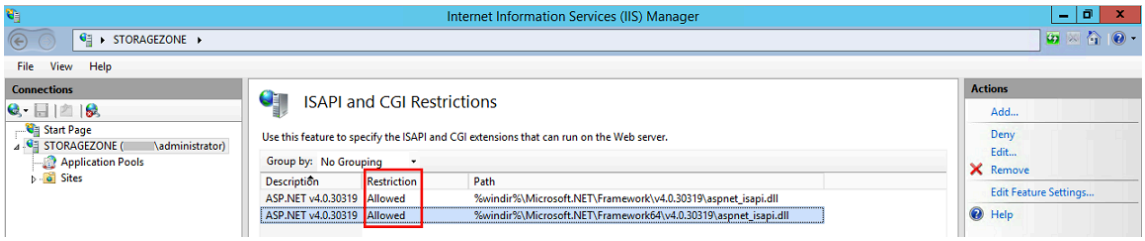
Um IIS zu konfigurieren

Nachdem Sie die Webserver-Rolle (IIS) und den ASP.NET-Rollendienst aktiviert haben, konfigurieren Sie IIS.

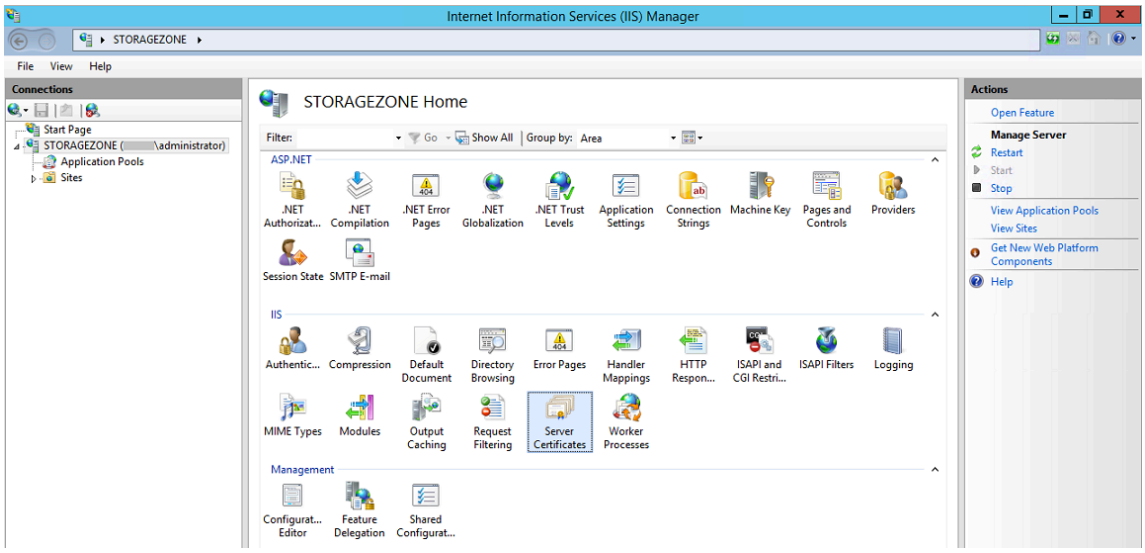
1. Öffnen Sie die IIS-Manager-Konsole, klicken Sie auf den StorageZone Controller-Serverknoten und doppelklicken Sie dann auf ISAPI- und CGI-Einschränkungen.



2. Setzen Sie jeden ASP.NET-Eintrag auf Zulässig.



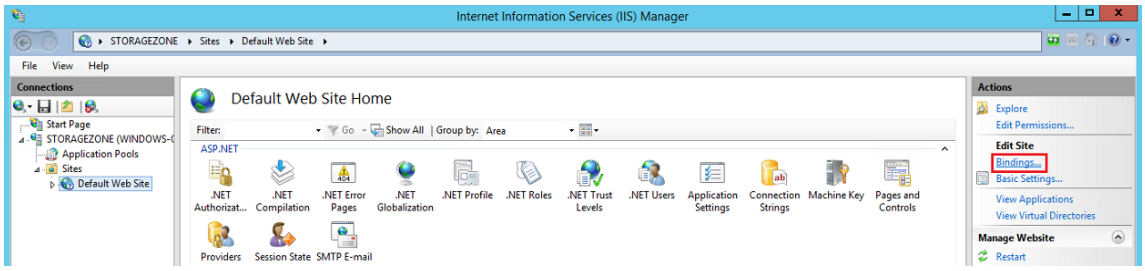
3. Stellen Sie sicher, dass ein Domänenserver oder ein öffentliches Zertifikat auf dem Server installiert ist: Klicken Sie in der IIS-Manager-Konsole auf den Serverknoten des Storage Zone Controllers und doppelklicken Sie dann auf Serverzertifikate.



Wenn kein Zertifikat mit einer öffentlichen Zertifizierungsstelle verknüpft ist, installieren Sie ein Zertifikat auf dem Server, bevor Sie fortfahren. Weitere Informationen finden Sie unter Installieren eines SSL-Zertifikats.

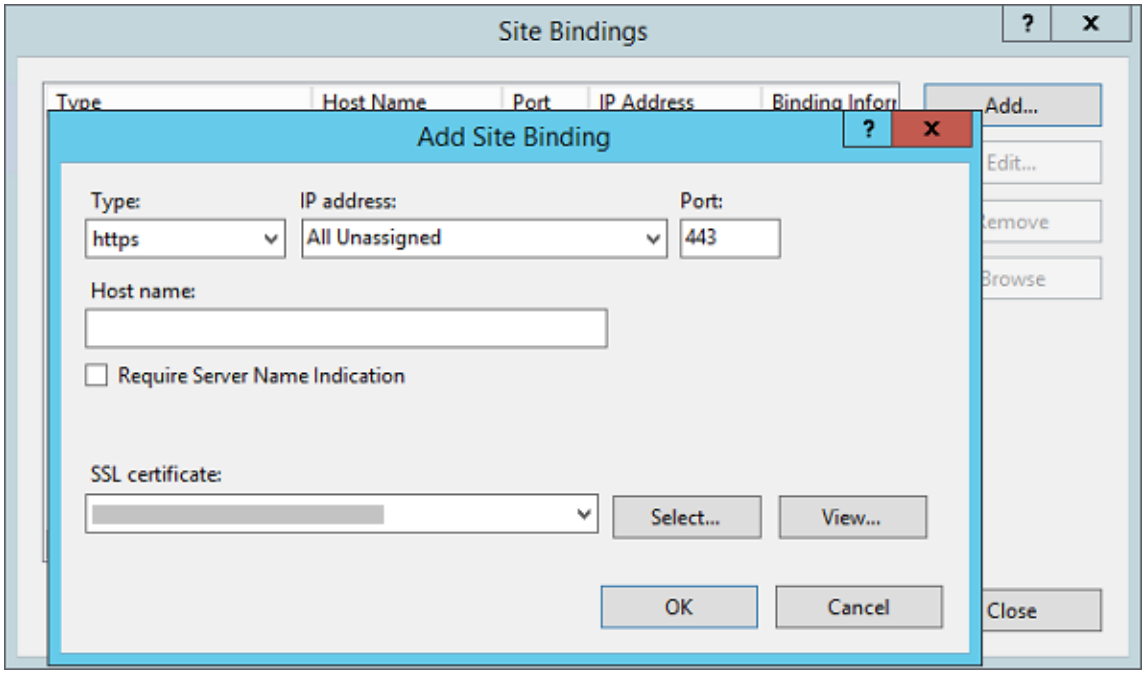
> **Hinweis:**
>
> Wenn Sie ein NetScaler Gateway oder ein ähnliches Gerät mit StorageZones Controller verwenden, können Sie ein Domänenserverzertifikat verwenden. Der gesamte Internetverkehr für Standardzonen muss mit einem öffentlichen Zertifikat abgewickelt werden.

4. Klicken Sie in der IIS-Manager-Konsole auf **Standardwebsite** und dann auf **Bindungen**.



5. Klicken Sie auf Hinzufügen und konfigurieren Sie die Site-Bindung wie folgt:

   - Der Typ ist https.
   - Die IP-Adresse lautet “Alle nicht zugewiesen”.
   - Der Port ist 443.
   - Das SSL-Zertifikat ist Ihr installiertes Zertifikat.



6. Um die Webserververbindung zu testen, navigieren Sie zu `http://localhost/` und zu `https://localhost/`. Wenn die Verbindung erfolgreich ist, wird das IIS-Logo angezeigt.

   HTTPS zeigt eine Meldung an, dass das Zertifikat nicht mit dem Localhost-Namen im URL-Header übereinstimmt. Dies wird erwartet und Sie können die Website sicher aufrufen.

7. Wenn Sie den StorageZones Controller auf einer VM installieren, erstellen Sie einen Snapshot der VM.

> **HINWEIS:**
>
> Der StorageZones Controller verwendet CORS und erfordert, dass das HTTP-Verb **OPTIONS** aktiviert ist. Bitte überprüfen Sie die Funktion zum Filtern von IIS-Anforderungen, um sicherzustellen, dass das **OPTIONS-Verb** nicht deaktiviert ist.

Installieren von Storage Zones Controller und Erstellen einer Speicherzone

March 17, 2024

> **Wichtig:**
>
> - Stellen Sie sicher, dass Ihre Umgebung die Systemanforderungen erfüllt, bevor Sie mit der Installation beginnen.
> - Der ShareFile StorageZones Controller verwendet anwendungsspezifische Passwörter. Weitere Informationen finden Sie unter Anwendungsspezifisches Passwort erstellen.

Wenn Sie einen StorageZones Controller installieren, erstellen Sie entweder eine Zone und konfigurieren einen primären StorageZones Controller oder
verbinden sekundäre StorageZones Controller mit einer Zone.

Bei der Konfiguration eines primären StorageZones Controllers können Sie eine oder beide dieser Funktionen aktivieren:

- Speicherzonen für ShareFile-Daten, um privaten Datenspeicher anzugeben, entweder eine private Netzwerkfreigabe oder ein unterstütztes Speichersystem eines Drittanbieters.
- Speicherzone-Connectors, um Benutzern Zugriff auf Dokumente auf SharePoint-Websites oder bestimmten Netzwerkdateifreigaben zu ermöglichen.

In den folgenden Schritten wird beschrieben, wie Sie den StorageZones Controller installieren, die Authentifizierung für die IIS-Standardwebsite konfigurieren, eine Zone erstellen und Funktionen aktivieren.

1. Führen Sie Download und Installation der Speicherzonencontroller-Software durch:
   - Melden Sie sich auf der ShareFile-Downloadseite unter an https://dl.sharefile.com/storagezone-controllerund laden Sie das neueste StorageZones Controller-Installationsprogramm herunter.

> **Hinweis:**
>
> Durch die Installation des StorageZones Controllers wird die Standardwebsite auf dem Server in den Installationspfad des Controllers geändert.

Die**anonyme Authentifizierung** sollte auf der Standardwebsite aktiviert sein.

2. Führen Sie auf dem Server, auf dem Sie den StorageZones Controller installieren möchten, StorageCenter.msi aus.
   - Der Setup-Assistent für den ShareFile StorageZones Controller wird gestartet.
   - Führen Sie für Mehrmandantenfähigkeit den folgenden Befehl aus: ***msiexec***/i StorageCenter_5.0.1.msi MULTITENANT=1

   > **Hinweis:**
   >
   > Im obigen Befehl müssen Sie möglicherweise die Versionsnummer (5.0.1 im Beispiel) so aktualisieren, dass sie mit der Nummer der MSI übereinstimmt, die Sie installieren möchten.

   - Antworten Sie auf die Eingabeaufforderungen. Wenn die Installation abgeschlossen ist, deaktivieren Sie das Kontrollkästchen für die **StorageZones Controller-Konfigurationsseite starten** und klicken Sie dann auf **Fertig stellen**.
3. Starten Sie den StorageZones Controller neu.
4. Um zu testen, ob die Installation erfolgreich ist, navigieren Sie zu `http://localhost/`. Bei erfolgreicher Installation wird das ShareFile-Logo angezeigt.
5. Wird das ShareFile-Logo nicht angezeigt, löschen Sie den Browsercache und versuchen es noch einmal.

   > **Wichtig:**
   >
   > Wenn Sie den Speicherzonencontroller klonen möchten, erstellen Sie zunächst ein Datenträgerimage, bevor Sie mit der Konfiguration des Speicherzonencontrollers fortfahren.

6. Um einen S3-kompatiblen Speicheranbieter mit ShareFile zu verwenden, führen Sie die folgenden Schritte aus, bevor Sie eine Speicherzone erstellen oder konfigurieren.
   - Öffnen Sie den Windows-Registrierungseditor (**Ausführen > regedit.exe**).
   - Suchen Sie den Registrierungsschlüssel HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ Citrix\ StorageCenter.
   - Erstellen Sie einen neuen REG_SZ-Wert unter diesem Schlüssel:
     - Wertname: **s3EndpointAddress**
     - Werttyp: **REG_SZ**

  - Wertdaten: Geben Sie die HTTPS-URL ein, die Ihrem S3-kompatiblen Speicherendpunkt entspricht.

- Wenn der Speicheranbieter nur den Containerzugriff im Pfadstil unterstützt (siehe http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html), erstellen Sie einen weiteren Wert unter diesem Schlüssel.
  - Wertname: **S3ForcePathStyle**
  - Werttyp: **REG_SZ**
  - Wertdaten: **wahr**
- Starten Sie den StorageZones Controller-Anwendungspool (StorageCenterAppPool) neu.
- Erfassen Sie die folgenden Informationen von Ihrem S3-kompatiblen Speichersystem:
  - Der Name eines S3-Buckets, der für die ShareFile DataAccess-Schlüssel-ID verwendet werden soll.
  - Zugriffsschlüssel-ID
  - Geheimer Zugangsschlüssel

7. Fahren Sie mit den folgenden Schritten fort, um eine neue Speicherzone zu erstellen. Wählen Sie Amazon S3 als dauerhaften Speicherort. Der StorageZones Controller verwendet die benutzerdefinierte Endpunktadresse, die Sie eingegeben haben, anstelle des tatsächlichen Amazon S3-Service. Wählen Sie bei der Konfiguration der S3-Details den Bucket-Namen, den Sie zuvor erstellt haben.
8. Navigieren Sie zur StorageZones Controller-Konsole.
9. Öffnen `http://localhost/configservice/login.aspx` oder starten Sie das Konfigurationstool über den Startbildschirm oder das Menü. Informationen zur Verwendung der Startbildschirmverknüpfung in Windows 8 finden Sie unter StorageZones Controller verwalten.
10. Geben Sie auf der **Anmeldeseite des StorageZones Controllers** die **E-Mail-Adresse**, das **Passwort** und die **vollständige Konto-URL-FQDN-Subdomain**, z. B. `subdomain.sharefile.com` oder `subdomain.sharefile.eu`, für Ihr Konto ein. Klicken Sie auf **Anmelden**.
11. Um Ihren primären StorageZones Controller einzurichten, klicken Sie auf **Neue Zone erstellen** und geben Sie die Zoneninformationen ein:

Option	Beschreibung
Zone	Ein Name, der in der ShareFile-Administratorkonsole angezeigt wird.

Option	Beschreibung
Primärer Zonencontroller	Die Standardeinstellung ist `http://localhost/ConfigService`. Wenn Sie SSL verwenden, ändern Sie HTTP in https. Beachten Sie, dass ShareFile nur gültige, vertrauenswürdige öffentliche SSL-Zertifikate für Standardzonen unterstützt. Wenn Sie Probleme bei der Konfiguration eines sekundären Speicherzonenhosts haben, stellen Sie sicher, dass Sie die ConfigService-URL in einem lokalen Browser auf diesem Server ohne SSL-Fehler auflösen können. localhost wird in die Server-IP-Adresse aufgelöst. Sie können stattdessen einen Servernamen angeben (z. B. `https://servername.subdomain.com/ConfigService`). Der Servername muss von einem sekundären StorageZones Controller-Server aufgelöst werden können.
Hostname	Eine eindeutige Kennung für Ihren StorageZones Controller. ShareFile empfiehlt, den Serverhostnamen als Bezeichner zu verwenden. Dies sollte ein benutzerfreundlicher Name sein und nicht der FQDN. Dieser Name wird in der ShareFile-Administratorkonsole angezeigt.
Externe Adresse	Der FQDN für diesen StorageZones Controller. Wenn dieser StorageZones Controller für Standardzonen verwendet wird, muss die URL über das Internet zugänglich sein. Wenn Sie einen Load Balancer verwenden, geben Sie dessen Adresse ein. Wenn Sie die Seite einreichen, überprüft ShareFile die Adresse.

12. Gehen Sie wie folgt vor, um den privaten Datenspeicher anzugeben.
    - Aktivieren Sie das Kontrollkästchen **Speicherzonen für ShareFile-Daten aktivieren**.
    - Um eine Standardzone zu konfigurieren, deaktivieren Sie das Kontrollkästchen.

> **Hinweis:**
>
> Nachdem Sie einen StorageZones Controller konfiguriert haben, können Sie seinen Zonentyp nicht mehr ändern.

Der StorageZones Controller verwendet die Anmeldeinformationen des Dienstkontos, um eine Verbindung zum vertrauenswürdigen Active Directory-Domänenserver herzustellen, um nach E-Mail-Adressen zu suchen.

- Wählen Sie ein Speicher-Repository.

13. Wenn Sie StorageZone Connectors nicht aktivieren möchten, klicken Sie auf **Registrieren**, um den StorageZones Controller bei ShareFile zu registrieren, und fahren Sie dann mit Schritt 14 fort.
14. Wenn Sie S3-kompatiblen Speicher verwenden, erstellen Sie diese zusätzlichen Registrierungseinträge, nachdem sich die Speicherzone registriert hat:
    - Öffnen Sie den Windows-Registrierungseditor (**Ausführen > regedit.exe**).
    - Suchen Sie den `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storage zone\CloudStorageUploaderConfig` Registrierungsschlüssel.
    - Erstellen Sie einen neuen REG_SZ-Wert unter diesem Schlüssel:
      - Wertname: **s3EndpointAddress**
      - Werttyp: **REG_SZ**
      - Wertdaten: Geben Sie die HTTPS-URL ein, die Ihrem S3-kompatiblen Speicherendpunkt entspricht.
    - Wenn der Speicheranbieter nur den Containerzugriff im Pfadstil unterstützt (siehe http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html), erstellen Sie einen weiteren Wert unter diesem Schlüssel.
      - Wertname: **S3ForcePathStyle**
      - Werttyp: **REG_SZ**
      - Wertdaten: **wahr**
    - Starten Sie den StorageZones Controller-Anwendungspool (StorageCenterAppPool) neu.
15. So aktivieren Sie Storage Zone Connectors:

    Durch die Aktivierung der Connectors werden die IIS-Apps „cifs“(Connector für Network File Shares) und „sp“(Connector für SharePoint) erstellt.

    - Aktivieren Sie das Kontrollkästchen für jeden Connectortyp, den Sie verwenden möchten: Speicherzonenconnector für Netzwerkdateifreigaben aktivieren und Speicherzonenconnector für SharePoint aktivieren. Informationen zu den Connector-Einstellungen finden Sie in diesem Abschnitt unter Konfigurieren von Speicherzone-Connectors.

- Klicken Sie auf **Registrieren**. Ihre StorageZones Controller-Informationen werden angezeigt.
- Wenn Sie **Zulässige Pfade oder Verweigerte Pfade** für Speicherzonenconnectors angegeben haben, starten Sie den IIS-Server neu.

16. Informationen zur Konfiguration sekundärer StorageZones Controller finden Sie unter StorageZones Controller verwalten.

> **Wichtig:**
>
> Auf Ihrem lokalen Standort ist ein StorageZone Controller installiert, für dessen Sicherung Sie verantwortlich sind. Um Ihre Bereitstellung zu schützen, sollten Sie einen Snapshot des StorageZones Controller-Servers erstellen, die StorageZones Controller-Konfiguration sichernund den StorageZones Controller für die Notfallwiederherstellung vorbereiten.

Speicherzonen für ShareFile-Daten konfigurieren

> **Hinweis:**
>
> Speicherzonen für ShareFile-Daten sind für Citrix Endpoint Management Enterprise Edition verfügbar und nicht für andere Citrix Endpoint Management-Editionen.

Sie können Speicherzonen für ShareFile-Daten über den StorageZones Controller-Assistenten konfigurieren, wenn Sie eine Speicherzone erstellen, oder über die StorageZones Controller-Konsole. Verwenden Sie die Registerkarte ShareFile-Daten, um Einstellungen für private Netzwerkfreigaben oder unterstützte Speichersysteme von Drittanbietern zu konfigurieren.

Einstellungen für Netzwerkfreigabe

Option	Beschreibung
Speicherrepository	Wählen Sie Lokale Netzwerkfreigabe. Nachdem Sie die Zone erstellt haben, können Sie die Speicher-Repository-Option nicht mehr ändern. Um beispielsweise von einer lokalen Netzwerkfreigabe zum Speicher eines Drittanbieters zu wechseln, müssen Sie eine neue Zone erstellen.

Option	Beschreibung
Standort teilen im Netzwerk	Der UNC-Pfad zur Netzwerkfreigabe, den Sie für die private Datenspeicherung und für Daten wie Verschlüsselungsschlüssel, Dateien in der Warteschlange und andere temporäre Elemente verwenden werden. Geben Sie den Pfad im Formular an `\\server\share`. StorageZones Controller, die zu derselben Speicherzone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden. Vorsicht: Der StorageZones Controller überschreibt alle Daten in diesem Pfad mit einem proprietären Speicherformat. Geben Sie niemals einen Pfad zu einem Speicherort mit Dateidaten an. Reservieren Sie diesen Speicherort nur für Speicherzonen für ShareFile-Daten. StorageZones Controller greifen mit dem auf der Konfigurationsseite angegebenen Network Share Benutzernamen/Passwort auf Network Share zu. Wenn auf der Konfigurationsseite kein Network Share-Benutzername/Passwort angegeben wird, wird standardmäßig das Network Service-Konto verwendet. Das Netzwerkdienstkonto muss vollen Zugriff auf diesen Speicherort haben. Der StorageZones Controller verwendet standardmäßig auch das Netzwerkdienstkonto für den StorageCenterAppPool. Es ist wichtig zu beachten, dass die einzige unterstützte Konfiguration die Verwendung des Netzwerkdienstkontos ist.

Option	Beschreibung
Network Share-Benutzername und Network Share-Passwort	Die Anmeldeinformationen für den UNC-Pfad Ihres Netzwerkfreigabestandorts. Um ein benanntes Benutzerkonto anstelle des Netzwerkdienstkontos für den Zugriff auf die Freigabe zu verwenden, geben Sie diese Anmeldeinformationen an. Sie können den IIS-Anwendungspool und die ShareFile-Dienste weiterhin mit dem Netzwerkdienstkonto ausführen.
Verschlüsselung aktivieren	Wählen Sie das Kontrollkästchen nur aus, wenn Sie den auf Ihrer Dateifreigabe gespeicherten Dateiinhalt verschlüsseln möchten. In einer Unternehmensumgebung, in der sich die Netzwerkfreigabe innerhalb Ihres Netzwerks befindet und bereits durch Tools von Drittanbietern gesichert ist, empfehlen wir, die Dateien auf dem Share nicht zu verschlüsseln. Diese Einstellung bezieht sich nicht auf Metadaten. Metadaten werden für Standardzonen nicht verschlüsselt. Obwohl diese zusätzliche Sicherheit bei Bedarf als Option für maximale Sicherheit angeboten wird, macht das Verschlüsseln von Dateien auf der Freigabe den Datenträger unlesbar für Drittanbieter-Tools wie Antivirus-Scanner und Filer-Tools, einschließlich Datendeduplizierungstools. ShareFile verwendet einen Dateiverschlüsselungsschlüssel, um die Gültigkeit von Download-Anfragen zu bestätigen und den Speicher zu verschlüsseln.

Option	Beschreibung
Passphrase	Eine Phrase, die zum Schutz des Dateiverschlüsselungsschlüssels verwendet wird. Die Passphrase muss mehr als sechs Zeichen enthalten. Achten Sie darauf, die Passphrase und den Verschlüsselungsschlüssel an einem sicheren Ort zu archivieren. Sie müssen dieselbe Passphrase für jeden StorageZone Controller in einer Zone verwenden. Die Passphrase stimmt nicht mit Ihrem Kontokennwort überein und kann bei Verlust nicht wiederhergestellt werden. Wenn Sie die Passphrase verlieren, können Sie keine Speicherzonen neu installieren, zusätzliche StorageZone Controller mit der Speicherzone verbinden oder die Speicherzone wiederherstellen, falls der Server ausfällt. Hinweis: Der Verschlüsselungsschlüssel wird im Stammverzeichnis des gemeinsam genutzten Speicherpfads angezeigt. Durch den Verlust der Verschlüsselungsschlüsseldatei SCKeys.txt wird der Zugriff auf alle Speicherzonendateien sofort unterbrochen. Stellen Sie sicher, dass Sie im Rahmen Ihrer normalen Rechenzentrumsprozeduren eine Sicherungskopie der Verschlüsselungsschlüsseldatei erstellen.

Shared Cache-Konfigurationseinstellungen

Option	Beschreibung
Gemeinsamer Cache-Standort	der Pfad zu einer Netzwerkfreigabe, die Ihren Speichercache und Daten wie Verschlüsselungsschlüssel, Dateien in der Warteschlange und andere temporäre Elemente enthält. Geben Sie den Pfad im Formular an `\\server\share`. StorageZones Controller, die zu derselben Speicherzone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden. Vorsicht: Der StorageZones Controller überschreibt alle Daten in diesem Pfad mit einem proprietären Speicherformat. Geben Sie niemals einen Pfad zu einem Speicherort mit Dateidaten an. Reservieren Sie diesen Speicherort nur für Speicherzonen für ShareFile-Daten. Das Netzwerkdienstkonto (oder das Konto, unter dem der ShareFile Management Service für die Ausführung konfiguriert ist) muss vollen Zugriff auf diesen Speicherort haben.
Shared Cache Logon und Shared Cache Passwort	Die Anmeldeinformationen für den UNC-Pfad Ihres gemeinsam genutzten Cache-Speicherorts.
Verschlüsselung aktivieren	Markieren Sie das Kontrollkästchen, um die in Ihrem gemeinsamen Cache gespeicherten Dateien zu verschlüsseln.

Windows Azure-Speichercontainer-Einstellungen

Option	Beschreibung
Speicherrepository	Wählen Sie Azure-Speichercontainer. Nachdem Sie die Zone erstellt haben, können Sie die Speicher-Repository-Option nicht mehr ändern. Um beispielsweise von einer lokalen Netzwerkfreigabe zu Azure-basiertem Speicher zu wechseln, müssen Sie eine neue Zone erstellen.

Option	Beschreibung
Kontoname	Der Name Ihres Azure-Speicherkontos. Diese Namen werden immer in Kleinbuchstaben geschrieben.
Zugangsschlüssel	Der primäre oder sekundäre Zugriffsschlüssel für Ihren Azure-Speicher. Kopieren Sie den Schlüssel aus dem Fenster Zugriffsschlüssel verwalten des Windows Azure-Verwaltungsportals.
Überprüfen	Klicken Sie auf die Schaltfläche, um den Azure-Zugriffsschlüssel zu validieren. Sie können mit der Konfiguration erst fortfahren, wenn die Validierung abgeschlossen ist und das Menü „Containername“alle verfügbaren Container für das angegebene Konto enthält.
Name des Containers	Wählen Sie den Azure-Container aus, der für alle StorageZones Controller in dieser Speicherzone verwendet werden soll. Diese Liste ist leer, bis Ihr Azure-Zugriffsschlüssel validiert ist.

Amazon S3-Speicher-Bucket-Einstellungen

Option	Beschreibung
Speicherrepository	Wählen Sie den Amazon S3-Speicher-Bucket. Nachdem Sie die Zone erstellt haben, können Sie die Speicher-Repository-Option nicht mehr ändern. Um beispielsweise von einer lokalen Netzwerkfreigabe zum Amazon S3-Speicher zu wechseln, müssen Sie eine neue Zone erstellen.
Zugriffsschlüssel-ID	Die Zugriffsschlüssel-ID für Ihren Amazon S3-Speicher.
Geheimer Zugangsschlüssel	Der geheime Zugriffsschlüssel für Ihren Amazon S3-Speicher.

Option	Beschreibung
Überprüfen	Klicken Sie auf die Schaltfläche, um den geheimen Amazon S3-Zugriffsschlüssel zu validieren. Sie können mit der Konfiguration erst fortfahren, wenn die Validierung abgeschlossen ist und das Menü Bucket Name alle verfügbaren Buckets für das angegebene Konto enthält.
Bucket-Name	Wählen Sie den Amazon S3-Bucket aus, der für alle StorageZones Controller in dieser Speicherzone verwendet werden soll. Diese Liste ist leer, bis Ihr geheimer Amazon S3-Zugriffsschlüssel validiert ist.

SMTP-Einstellungen

Option	Beschreibung
SMTP-Serveradresse und SMTP-Portnummer	Hostname und Port Ihres lokalen SMTP-Servers.
SSL verwenden	Aktivieren Sie das Kontrollkästchen, um über eine sichere Verbindung eine Verbindung zum SMTP-Server herzustellen.
Nutzername und Passwort	Der Benutzername und das Passwort für Ihren lokalen SMTP-Server.
Authentifizierungsmodus	Der Standardauthentifizierungsmodus verwendet die sicherste verfügbare Methode, um eine Verbindung vom StorageZones Controller zum SMTP-Server herzustellen.
Adresse des Absenders	Die E-Mail-Adresse, die im Feld Von angezeigt wird.

Google Cloud-Plattform

Generieren Sie einen Zugriffsschlüssel und ein Geheimnis über **Google Cloud Platform > Einstellungen > Interoperabilität**.

Bevor Sie die StorageZones Configuration ausführen, setzen Sie den Registrierungswert **s3EndpointAddress** auf `https://storage.googleapis.com` und starten Sie IIS neu.

Variante 1

Beschreibung

Speicherrepository

Wählen Sie **Amazon S3-Speicher-Bucket**. Nachdem Sie die Zone erstellt haben, können Sie die **Speicher-Repository-Option** nicht mehr ändern. Um beispielsweise von einer lokalen Netzwerkfreigabe zum Amazon S3-Speicher zu wechseln, müssen Sie eine neue Zone erstellen.

Zugriffsschlüssel-ID

Die Zugriffsschlüssel-ID aus Ihrem Google Cloud Platform-Speicher.

Geheimer Zugangsschlüssel

Das Geheimnis aus Ihrem Google Cloud Platform-Speicher.

Überprüfen

Klicken Sie auf die Schaltfläche, um den geheimen Zugriffsschlüssel der Google Cloud Platform zu überprüfen. Sie können mit der Konfiguration erst fortfahren, wenn die Validierung abgeschlossen ist und die Liste der **Bucket-Namen** alle verfügbaren Buckets für das angegebene Konto enthält.

Bucket-Name

Wählen Sie den richtigen Bucket aus, der für alle StorageZones Controller in dieser Speicherzone verwendet werden soll. Diese Liste ist leer, bis Ihr geheimer Zugriffsschlüssel für die Google Cloud Platform überprüft wurde.

Speicherzonenkonnektoren konfigurieren

Speicherzonenconnectors ermöglichen Benutzern den Zugriff auf Dokumente auf SharePoint-Websites oder bestimmten Netzwerkdateifreigaben. Sie müssen keine Speicherzonen für ShareFile-Daten aktivieren, um Speicherzonenconnectors verwenden zu können.

> **Hinweis:**
>
> Speicherzonen für ShareFile Daten und die Speicherzonen-Connectors können eine Zone gemeinsam nutzen. Der StorageZones Controller hält die Daten und Zugriffsregeln für die beiden Datentypen jedoch getrennt.

Sie können StorageZone Connectors konfigurieren, wenn Sie eine Zone mit dem StorageZones Controller-Assistenten oder über die StorageZones Controller-Konsole erstellen.

Um den Zugriff auf bestimmte Netzwerkdateifreigaben oder SharePoint-Dokumentbibliotheken zu steuern, geben Sie eine Liste zulässiger oder verweigerter Pfade an. Starten Sie den IIS-Server neu, nachdem Sie Ihre Änderungen gespeichert haben.

Eingehende Verbindungen zu Speicherzone-Connectors werden zunächst anhand der zulässigen Pfade überprüft. Wenn die Verbindung zulässig ist, wird der Pfad dann mit den verweigerten Pfaden

verglichen. Um beispielsweise Zugriff auf `\\myserver\teamshare` und alle Unterordner zu gewähren, geben Sie einen zulässigen Pfad von `\\myserver\teamshare`an.

- Alle Verbindungen sind standardmäßig zulässig, was durch den Wert „Zulässige Pfade "gekennzeichnet ist. Der Wert ist für verweigerte Pfade nicht gültig.
- Wenn die erlaubten und verweigerten Pfade miteinander in Konflikt geraten, wird der restriktivste Pfad durchgesetzt.
- Die Einträge sind durch Kommas getrennt.
- Geben Sie für Konnektoren zu Netzwerkdateifreigaben die zulässigen UNC-Pfade an.

  Beispiel mit FQDN: `\\fileserver.acme.com\shared`

  Sie können die folgenden Variablen im UNC-Pfad verwenden:

  - %Benutzername%

    Leitet in das Home-Verzeichnis eines Benutzers um. Beispielpfad: `\\myserver\homedirs\\%UserName%`

  - %HomeDrive%

    Leitet zum Basisordnerpfad eines Benutzers um, wie in der Active Directory-Eigenschaft Home-Directory definiert. Beispielpfad: `%HomeDrive%`

  - %ts HomeDrive%

    Leitet zum Terminaldienste-Basisverzeichnis eines Benutzers um, wie in der Active Directory-Eigenschaft MS-TS-Home-Directory definiert. Der Standort wird verwendet, wenn sich ein Benutzer von einem Terminalserver oder Citrix XenApp-Server aus bei Windows anmeldet. Beispielpfad: %tsHomeDrive%

    Im Snap-In „Active Directory-Benutzer und -Computer"kann beim Bearbeiten eines Benutzerobjekts auf der Registerkarte „Remotedesktopdienste-Profil"auf den Wert MS-TS-Home-Directory zugegriffen werden.

  - %Benutzerdomäne%

    Leitet zum NetBIOS-Domänennamen des authentifizierten Benutzers um. Lautet der Anmeldename des authentifizierten Benutzers beispielsweise „abc\ johnd", wird die Variable durch „abc"ersetzt. Beispielpfad: `\\myserver%UserDomain%_%UserName%`

  Bei den Variablen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

- Geben Sie für einen Connector zu einer SharePoint-Website auf Stammebene den Pfad auf Stammebene an.

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

- Für einen Connector zu einer SharePoint-Websitesammlung:

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

- Geben Sie für Konnektoren zu SharePoint 2010-Dokumentbibliotheken die URLs an (ohne Pfadabschlüsse wie file.aspx oder /Forms).

  Beispiele:

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

  Die standardmäßige SharePoint 2013-URL (wenn die Minimal Download Strategy aktiviert ist) hat das Format: `https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`.

Sicherheitsempfehlung zum Entfernen des Serverheaders

IIS/ASP.NET macht den Server-Header standardmäßig in HTTP-Antworten verfügbar. Dieser Header könnte für einen Angreifer nützlich werden. Der Header gibt den sendenden Servertyp und in einigen Fällen die Versionsnummer an. Dieser Header ist für Produktionsstandorte nicht erforderlich und kann deaktiviert werden.

Leider kann das StorageZones Controller-Installationsprogramm diesen Header nicht automatisch entfernen. In unserer StorageZones Controller-Dokumentation/Installationsanleitung können wir Kunden jedoch empfehlen, diesen Header zu entfernen.

Im folgenden Artikel finden Sie die spezifischen Schritte, die wir in unserer Dokumentation angeben sollten: `https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/`

Überprüfen der Konfiguration des StorageZones Controller

April 20, 2021

Überprüfen Sie, ob ein StorageZones Controller bei ShareFile registriert ist, und überprüfen Sie dann auf andere Konfigurationsprobleme, bevor Sie fortfahren.

1. Klicken Sie in der Storage Zones Controller Konsole auf die Registerkarte **Überwachung**.

2. Stellen Sie sicher, dass der Heartbeat-Status ein grünes Häkchen aufweist.

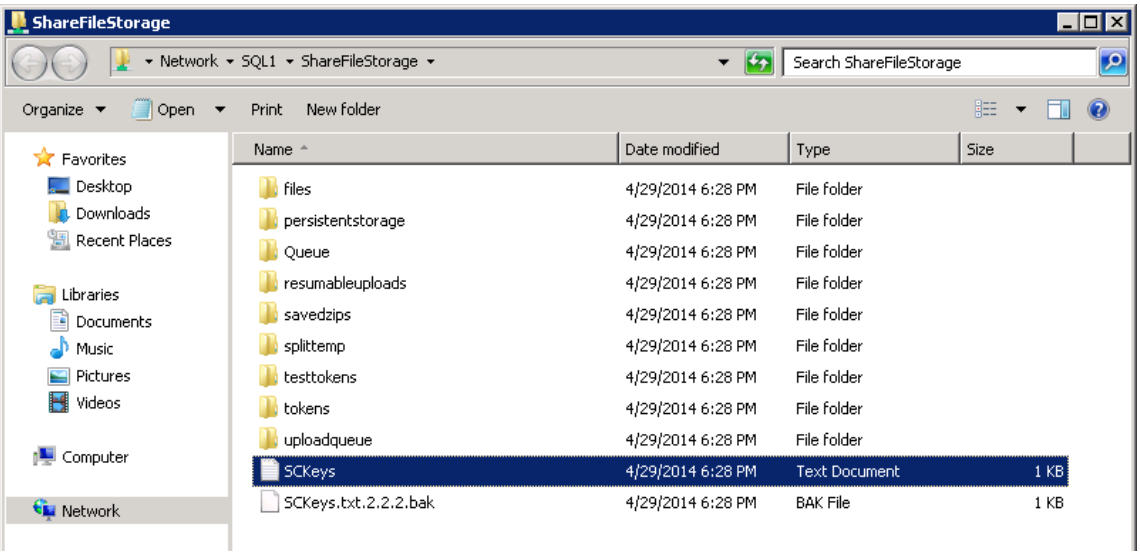
   Ein rotes Symbol zeigt an, dass ShareFile.com die Heartbeat-Nachrichten nicht empfängt. Überprüfen Sie in diesem Fall die Netzwerkkonnektivität von Ihrem Storage Zones Controller zu www.ShareFile.com und von einem externen PC zur URL Ihres Storage Zones Controllers. Für Standardzonen muss der StorageZones Controller auf Port 443 mit einem gültigen, vertrauenswürdigen öffentlichen SSL-Zertifikat zugegriffen werden.

   Nach einem Upgrade zeigt der ShareFile Connectivity von File Cleanup Services Status möglicherweise vorübergehend ein rotes Symbol an. Dies tritt auf, wenn Windows diesen Dienst startet, bevor der Storage Zones Controller eine Netzwerkverbindung herstellt. Der Status wird auf ein grünes Symbol zurückgesetzt, nachdem der Controller -Server wieder im Netzwerk ist.

3. Konnektivität zu Ihrer privaten Zone prüfen: Navigieren Sie zur externen URL (in Form von `https://server.subdomain.com`) Ihrer privaten Zone.

   Wenn der Internetverkehr an und von einem StorageZones Controller weitergeleitet werden darf, wird das ShareFile Logo angezeigt. Wenn der StorageZones Controller nicht korrekt konfiguriert ist, wird möglicherweise ein IIS-Logo oder ein Citrix ADC Anmeldebildschirm angezeigt. Stellen Sie sicher, dass eingehender und ausgehender HTTPS-Datenverkehr über Port 443 zulässig ist. Wenn Ihre externe URL auf Citrix ADC verweist, suchen Sie nach Treffern auf dem virtuellen Server für Content Switching und Lastausgleich für Daten. Weitere Informationen finden Sie unter “Storage Zones Controller lädt keine Daten in ShareFile hoch”in Problembehandlung bei Installation und Konfiguration.

4. Stellen Sie sicher, dass die Netzwerkfreigabe, die Sie für die private Datenspeicherung erstellt haben, eine Ordnerstruktur und einige Dateien aufweist, die vom StorageZones Controller erstellt wurden, einschließlich Sckeys.txt, die sich im Stammordner des freigegebenen Speichers befinden müssen.



Sckeys.txt wird erstellt, wenn der StorageZones Controller installiert ist, vorausgesetzt, es gibt keine Anmeldeinformationen oder Zugriffsrechte Probleme. Wenn Sckeys.txt nicht vorhanden ist, überprüfen Sie die Zugriffssteuerungslisten auf Ihrer Dateifreigabe, und installieren Sie dann den StorageZones Controller neu.

5. Überprüfen Sie den Status der StorageZone Connector über die ShareFile Schnittstelle:

   a) Melden Sie sich bei Ihrem ShareFile Enterprise Konto an, navigieren Sie zu **Admin > Speicherzonen**, und überprüfen Sie, ob die Spalte Health ein grünes Häkchen enthält.

   b) Klicken Sie auf den Site-Namen, und stellen Sie sicher, dass die Meldung Heartbeat angibt, dass der StorageZones Controller reagiert.

6. Testen eines Datei-Uploads: Melden Sie sich an der ShareFile Weboberfläche an, erstellen Sie einen freigegebenen Ordner, der der gerade konfigurierten Zone zugewiesen ist, laden Sie eine Datei in diesen Ordner hoch, und überprüfen Sie dann, ob die Datei im Ordner angezeigt wird.

Ändern der Standardzone für Benutzerkonten

March 17, 2024

Standardmäßig verwenden vorhandene und neu bereitgestellte Benutzerkonten den von ShareFile verwalteten Cloud-Speicher als Standardzone. Ändern Sie die Standardzone wie folgt:

- Um die Standardzone für Benutzerkonten anzugeben, die in AD bereitgestellt werden, wählen Sie während der Benutzerbereitstellung den Speicherort aus. Weitere Informationen finden Sie unter **Benutzerregeloptionen bearbeiten** im Artikel ShareFile-richtlinienbasierte Administration.
- Um die Standardzone für einen einzelnen Benutzer zu ändern, öffnen Sie die ShareFile-Administratorkonsole und gehen **Sie zu Benutzer verwalten**.

Festlegen eines Proxyservers für Speicherzonen

April 20, 2021

Über die StorageZones Controller-Konsole können Sie einen Proxyserver für StorageZones Controller festlegen. Sie können einen Proxyserver auch mit anderen Methoden festlegen.

Primär- und sekundäre StorageZones Controller kommunizieren über HTTP miteinander. Wenn der gesamte HTTP-Datenverkehr so konfiguriert ist, dass er über einen ausgehenden Proxyserver läuft,

der keine Verbindungen zu einem internen Server unterstützt, müssen Sie sowohl die primären als auch die sekundären StorageZones Controller so konfigurieren, dass der Proxyserver so umgeht, dass er miteinander kommunizieren kann, wie in den folgenden Schritten beschrieben. .

> **Wichtig:**
>
> Die Einstellungen für die Umgehungsliste werden nur für die neueste Storage Zones Controller Version angezeigt. Wenn Sie StorageZones Controller 2.2 bis 2.2.2 verwenden, müssen Sie Web.config für jeden sekundären Server manuell eine Umgehungsliste hinzufügen, wie unter beschrieben Web.config.

1. Klicken Sie in der Storage Zones Controller Konsole (`http://localhost/configservice/login.aspx`) auf die Registerkarte **Netzwerk** .

   > **Hinweis:**
   >
   > Wenn Sie Storage Zones Controller 5.11.17 verwenden, erfordert das Ändern eines Proxys eine Authentifizierung. Wenn Sie dazu aufgefordert werden, geben Sie die E-Mail-Adresse, das Kennwort und die vollständige FQDN-Subdomain für Konto-URL wie subdomain.sharefile.com oder subdomain.sharefile.eu für Ihr Konto ein. Klicken Sie auf Anmelden.

2. Aktivieren Sie das Kontrollkästchen Proxy aktivieren, und geben Sie die Adresse und den Port des Proxyservers ein.
3. Wählen Sie einen Authentifizierungsmodus aus, und geben Sie Ihr Windows-Konto an, das für den ShareFile Proxyzugriff vorgesehen ist.
4. Wenn Ihr Standort den gesamten ausgehenden HTTP-Datenverkehr proxiert und eine Zone über mehrere StorageZones Controller verfügt, konfigurieren Sie die Umgehungseinstellungen:
   - Wenn sich der Controller-Datenverkehr der Speicherzonen im selben Subnetz befindet, aktivieren Sie das Kontrollkästchen **Proxy umgehen…**, damit die Controller miteinander kommunizieren können.
   - Wenn sich die StorageZones Controller in verschiedenen Subnetzen befinden, geben Sie den Hostnamen oder die IP-Adresse des primären StorageZones Controller unter Adresse umgehen ein.
5. Starten Sie den IIS-Server aller Zonenmitglieder neu.

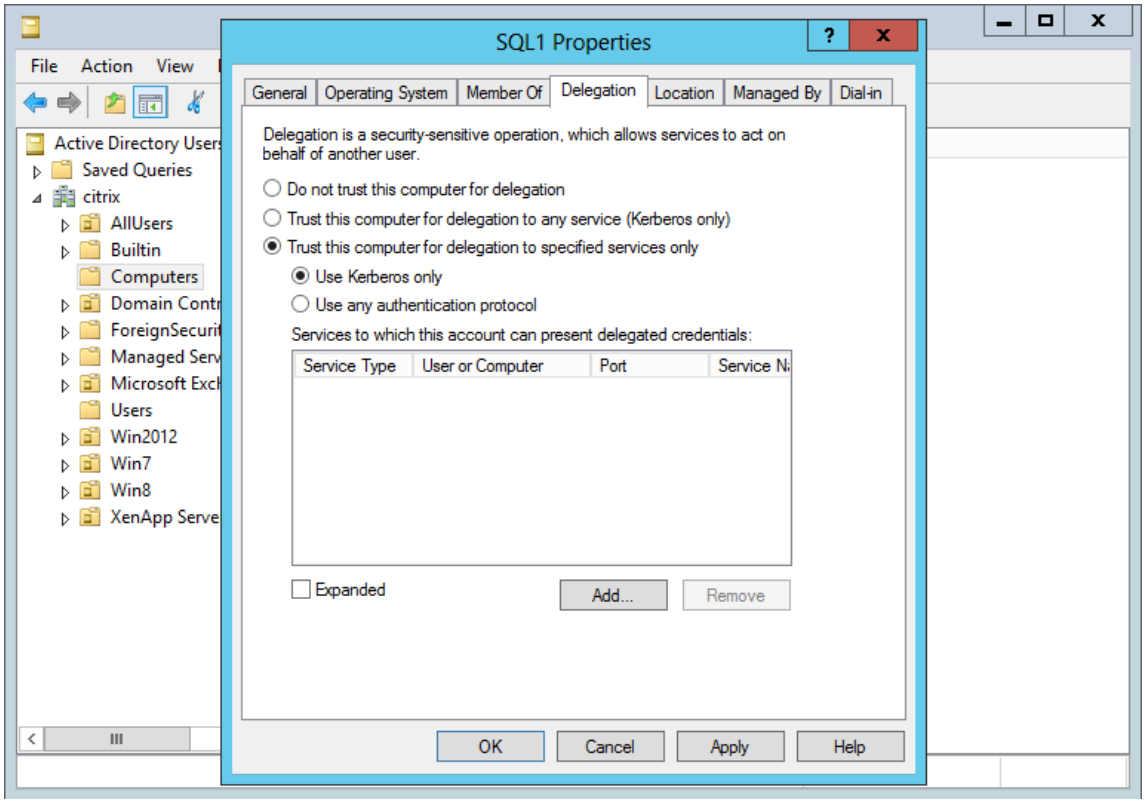
Konfiguration des Domänencontrollers, sodass er dem StorageZone Controller für die Delegierung vertraut

April 20, 2021

> **Hinweis:**
>
> Dieser Abschnitt gilt nur für StorageZone Connector.

Um die NTLM- oder Kerberos-Authentifizierung auf Netzwerkfreigaben oder SharePoint-Websites zu unterstützen, konfigurieren Sie den Domänencontroller wie folgt.

1. Klicken Sie auf dem Domänencontroller für die Speicherzonendomäne auf **Start > Verwaltung > Active Directory Benutzer und -Computer**.
2. Erweitern Sie die Domäne, und erweitern Sie den Ordner Computer.
3. Klicken Sie im rechten Bereich mit der rechten Maustaste auf den Namen des StorageZones Controller, wählen Sie **Eigenschaften**aus, und klicken Sie dann auf die Registerkarte **Delegierung**.
4. Wählen Sie für Kerberos die Option **Diesen Computer nur für die Delegierung an bestimmte Dienste vertrauen**aus.



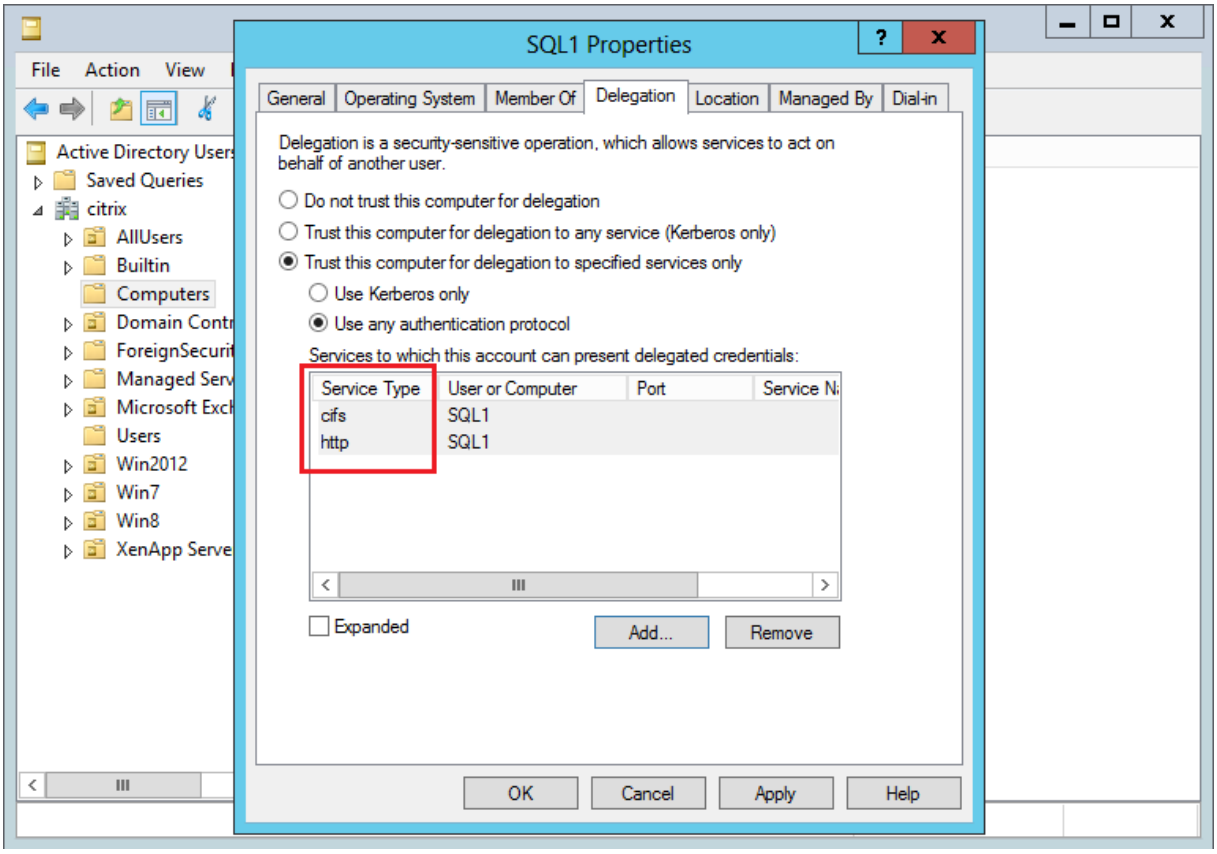
5. Für NTLM:

a) Wählen Sie **Diesen Computer nur für die Delegierung an bestimmte Dienste vertrauen** und **Authentifizierungsprotokoll verwenden**aus. Klicken Sie auf **OK**.

b) Klicken Sie auf die Schaltfläche **Add**. Klicken **Sie im Dialogfeld Dienste hinzufügen** auf **Benutzer oder Computer**, und navigieren Sie dann zu dem Hostnamen für die Netzwerkfreigabe oder SharePoint-Server, oder geben Sie diesen ein. Klicken Sie auf **OK**.

   Wenn Sie über mehrere Dateiserver oder SharePoint-Server verfügen, fügen Sie jeweils einen Dienst hinzu.

c) Wählen Sie in der Liste Verfügbare Dienste die verwendeten Dienste aus: CIFS (für Connector für Netzwerkdateifreigaben) und HTTP (für Connector für SharePoint). Klicken Sie auf OK.



Konfigurieren Sie den StorageZones Controller für Web App-Vorschauen, Miniaturansichten und das Teilen nur zum Ansehen

March 17, 2024

on-premises Dateivorschauen werden von Ihrem lokalen Microsoft Office Web Apps (OWA) -Server

gerendert. Bei der Vorschau von Dateien, die in einer von Citrix verwalteten Speicherzone gespeichert sind, werden Vorschauen von von Citrix oder Microsoft verwalteten OWA-Servern gerendert.

> **Wichtig:**
>
> **Anforderungen an Positivlisten:**
>
> `*.sf-api.com` muss für Ihren Office Online Server zugänglich sein, damit die Vorschau und Bearbeitung in StorageZones Version 5.0 oder höher ordnungsgemäß funktioniert.

Anforderungen

Unterstützte Dateitypen für die on-premises Dateivorschau

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

Unterstützte Dateitypen für die on-premises Dateibearbeitung

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

Unterstützte Umgebungen

- Standardzonen
- Zonen mit mehreren Mandanten
- Web-Applikation

Positivlisten / Überlegungen zum Netzwerk

- Der OOS-Server sollte in der Lage sein, Folgendes zu kontaktieren: **`https://\*.sf-api.com`** **(oder .eu)**
- Der SZC-Server sollte in der Lage sein, **`https://\*.sf-api.com`** und **`https://\*.sharefile.com`** **(oder .eu)** zu erreichen
- Der SZC-Server sollte in der Lage sein, den OOS-Server **`https://\<Customer OOS / OWA Endpoint\>/hosting/discovery`** (z. B. `https://oos.sharefileexample.com/hosting/discovery`) zu erreichen

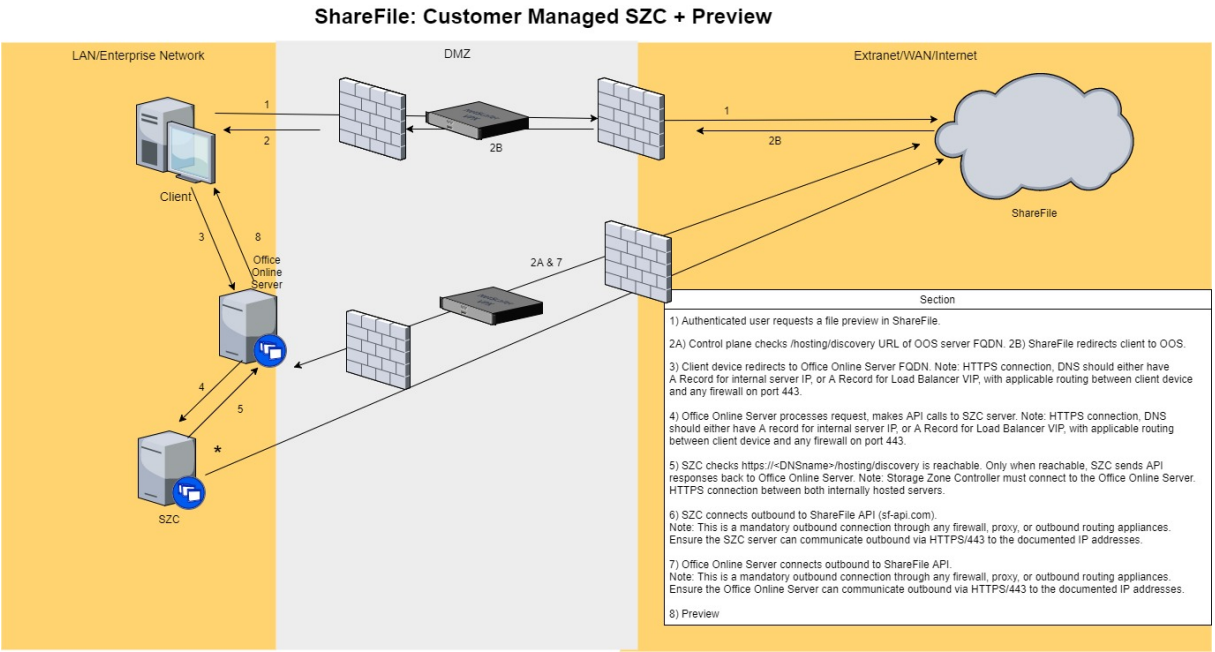
Um on-premises Dateien zu bearbeiten, muss die Dateiversionierung in Ihrem ShareFile-Konto aktiviert sein.

Die Einstellung zum Aktivieren der Microsoft Office Online-Bearbeitung im ShareFile Web App-Menü „Erweiterte Einstellungen“hat keinen Einfluss auf die Möglichkeit, on-premises Dateien zu bearbeiten. Dieser spezielle Schalter steuert **nicht** Ihre Fähigkeit, on-premises Dateien zu bearbeiten, sondern gilt für die Bearbeitung von Dateien, die in einer öffentlichen Cloud gespeichert sind. Die Aktivierung der Bearbeitung von lokalen Dateien wird ausschließlich vom Storage Zones Controller-Administrator mithilfe der unten beschriebenen Schritte gesteuert.

Microsoft-Serverkompatibilität

- **Microsoft Server 2016**: unterstützt die Möglichkeit, Dateien sowohl zu bearbeiten als auch in der Vorschau anzuzeigen. Die Bearbeitung kann auch deaktiviert werden.
- **Microsoft Server 2013**: unterstützt nur die Möglichkeit, eine Vorschau von Dateien anzuzeigen.

Architektur- und Netzwerkdiagramm



1. Der authentifizierte Benutzer fordert eine Dateivorschau in ShareFile an.
2. ShareFile gibt eine Umleitung zum Clientgerät mit Office Online Server-FQDN aus
3. Das Clientgerät leitet zum Office Online Server-FQDN um.

> **Hinweis:**
>
> HTTPS-Verbindung, DNS sollte entweder einen Record für die interne Server-IP oder einen Record für Load Balancer VIP mit passendem Routing zwischen dem Client-Gerät und einer Firewall auf Port 443 haben.

4. Office Online Server verarbeitet Anfragen und führt API-Aufrufe an den StorageZones Controller-Server durch.

   > **Hinweis:**
   >
   > HTTPS-Verbindung, DNS sollte entweder über einen Eintrag für die interne Server-IP oder über einen Datensatz für Load Balancer VIP verfügen, wobei das Routing zwischen dem Client-Gerät und einer Firewall auf Port 443 gilt.

5. Der StorageZones Controller prüft, ob `https://\<DNSname\>/hosting/discovery` erreichbar ist. Nur wenn es erreichbar ist, sendet SZC API-Antworten zurück an Office Online Server.

   > **Hinweis:**
   >
   > Der Speicherzonencontroller muss eine Verbindung zum Office Online Server herstellen. HTTPS-Verbindung zwischen beiden intern gehosteten Servern.

6. Der StorageZones Controller stellt eine ausgehende Verbindung mit der ShareFile-API (sf-api.com) her.

   > **Hinweis:**
   >
   > Dies ist eine obligatorische ausgehende Verbindung über eine Firewall, einen Proxy oder eine Outbound-Routing-Appliance. Stellen Sie sicher, dass der StorageZones Controller-Server ausgehend über HTTPS/443 mit den oben dokumentierten IP-Adressen kommunizieren kann.

7. Office Online Server stellt eine ausgehende Verbindung mit der ShareFile-API her.

   > **Hinweis:**
   >
   > Dies ist eine obligatorische ausgehende Verbindung über eine Firewall, einen Proxy oder eine Outbound-Routing-Appliance. Stellen Sie sicher, dass der Office Online Server ausgehend über HTTPS/443 mit den oben dokumentierten IP-Adressen kommunizieren kann.

8. Die Vorschau wird angezeigt.

Damit der StorageZones Controller Datei-Bytes an OOS streamt, anstatt dass OOS die ShareFile-Steuerungsebene zum Herunterladen der Inhalte aufruft: Wir müssen einen Schlüssel in einer der Konfigurationsdateien auf dem StorageZones Controller aktualisieren.

Das **C:\inetpub\wwwroot\Citrix\StorageCenter\WopiServer\AppSettingsReleaseOnPrem.config** muss aktualisiert werden.

Diese Konfigurationsdatei hat einen Schlüssel **downloadFileFromSC**, der derzeit auf **false** festgelegt ist. Ändern Sie den Schlüssel auf **true** und starten Sie IIS neu.

Dadurch wird die Konfiguration aktualisiert. OOS ruft auch nicht mehr die ShareFile-Steuerungsebene auf, um den Dateiinhalt herunterzuladen.

Wäre es richtig, wenn diese Option verwendet wird, wenn angegeben wird, dass kein eingehender Verkehr von der Kontrollebene zu OOS erfolgen würde?

Wenn die obige Option verwendet wird, stellt OOS keine ausgehenden Verbindungen mehr zur ShareFile-Steuerungsebene her.

Die ShareFile-Steuerungsebene stellt jedoch immer noch ausgehende Verbindungen zu OOS her, unabhängig davon, ob die obige Option verwendet wird oder nicht.

Gibt es Vor- oder Nachteile der Verwendung einer Methode gegenüber der anderen?

Bei diesem Ansatz lädt OOS den Dateiinhalt nicht direkt herunter. Der StorageZones Controller lädt die Datei-Bytes herunter und streamt sie an OOS. Dadurch wird die Last auf den StorageZones Controller-Servern erhöht.

Das Herunterladen und Streamen von Dateibytes ist eine ressourcenintensive Aufgabe. Abhängig von der Anzahl der Benutzer und der Anzahl der Vorschau- und Bearbeitungsvorgänge steigt die Last auf den StorageZones Controller-Servern.

on-premises Vorschau und Bearbeitung aktivieren

Um die Dokument- und Bildvorschau im Browser, Miniaturansichten, die gemeinsame Nutzung von Daten, die in vom Kunden verwalteten Speicherzonen gespeichert sind, und die on-premises Dateibearbeitung zu unterstützen, konfigurieren Sie den StorageZones Controller wie folgt:

1. Klicken Sie in der StorageZones Controller-Konsole auf die Registerkarte **ShareFile Data**.
2. Aktivieren Sie im Abschnitt **Konfiguration der lokalen Netzwerkfreigabe** die Option **Office Web Apps-Vorschauen konfigurieren**.
3. Geben Sie die externe URL Ihres Microsoft Office Web Apps (OWA) -Servers ein.
   - Benutzer müssen die OWA-Serversoftware über ihr Microsoft Office MSDN-Abonnement herunterladen und konfigurieren.
4. Wählen Sie **Office Online-Bearbeitung aktivieren** (falls erforderlich)
5. Stellen Sie sicher, dass die OWA-URL extern zugänglich ist.
6. Stellen Sie sicher, dass Ihre Office Online-Server mit kommunizieren können `*.sf-api.com`.

7. Klicken Sie in der Storage Zones Controller-Konsole auf die Registerkarte **Überwachung**.
8. Stellen Sie sicher, dass **OWA Server Connectivity** ein grünes Häkchen hat.

> **Hinweis:**
>
> Für die Bearbeitung von on-premises Dateien muss die Dateiversionierung für das ShareFile-Konto aktiviert sein. Wenn die Dateiversionsverwaltung für das Konto deaktiviert ist, funktioniert die on-premises Bearbeitung nicht.

Wichtig:

Konfigurieren Sie die Uhrsynchronisierung:

- Stellen Sie sicher, dass der Time auf Ihrem Storage Zones Controller mit time.windows.com oder einem anderen NTP-Server synchronisiert ist. Klicken Sie hier, um Informationen zum Konfigurieren der Uhrsynchronisierung zu erhalten.? redirectedfrom=MSDN)

Den OWA-URAL ändern oder Vorschauen deaktivieren:

- Für jede der oben genannten Aktionen muss der IIS-Dienst für jeden primären und sekundären Controller neu gestartet werden.

Einschränkungen

- Mobile Apps unterstützen keine Bearbeitung im Browser.
- Connectors unterstützen keine Vorschauen im Browser.

WOPI-Vorschauen werden für VDR-Konten nicht unterstützt.

Informationen zur Konfiguration Ihres Citrix ADC für View-Only Sharing finden [Sie unter Konfigurieren von Citrix ADC für]StorageZones Controller.(/en-us/storage-zones-controller/5-0/install/configure-netscaler.html)

Behebung von OWA- und OOS-Problemen

Wenn Sie Probleme bei der Vorschau oder Bearbeitung von lokalen Dateien haben, helfen Ihnen die folgenden Schritte bei der Identifizierung und Behebung bestimmter Probleme.

Um Probleme mit Ihrer Konfiguration zu beheben, melden Sie sich zuerst bei der OWA- oder OOS-Maschine an.

1. Stellen Sie sicher, dass die Office WebApps- oder OfficeOnline-Windows-Dienste in services.msc ausgeführt werden.

2. Öffnen Sie die Seite `http://localhost/hosting/discovery` in einem neuen Browser. Wenn diese Seite erfolgreich geladen wird, sollte eine XML-Antwort zurückgegeben werden.
3. Führen Sie PowerShell als Administrator aus und führen Sie den folgenden Befehl aus:

```
Get-OfficeWebAppsFarm
```

Wenn Sie in der Antwort eine WARNUNG- oder FEHLERMELDUNG erhalten, überprüfen Sie Ihre Konfigurationseinstellungen auf etwaige Fehler oder Irrtümer.

Überlegungen zum Netzwerk:

- Der OOS-Server sollte in der Lage sein, Folgendes zu kontaktieren: **`https://*.sf-api.com` (oder .eu)**
- Der SZC-Server sollte in der Lage sein, **`https://*.sf-api.com`** und **`https://*.sharefile.com` (oder .eu)** zu erreichen
- Der SZC-Server sollte in der Lage sein, den OOS-Server **`https://<CustomerOOS/OWAEndpoint\>/hosting/discovery`**zu erreichen. Beispiel: `https://oos.sharefileexample.com/hosting/discovery`.

Multitenant-Speicherzonen konfigurieren

March 17, 2024

Eine Multitenant-Speicherzone ist eine ShareFile StorageZones Controller-Funktion, mit der Citrix Service Providers (CSPs) eine einzelne Speicherzone erstellen und verwalten können, die von allen Mandanten gemeinsam genutzt wird.

Wenn Sie ein CSP mit einem von ShareFile bereitgestellten Partnerkonto sind, können Sie eine mehrmandantenfähige Standardspeicherzone auf Ihrer Domain hosten, die eine unbegrenzte Anzahl von Mandanten unterstützt. Die Verwendung einer Mehrmandantenzone ermöglicht Ihnen:

- Stellen Sie jedem Mandanten ein einzigartiges ShareFile-Konto zur Verfügung und nutzen Sie alle großartigen ShareFile-Funktionen, wie z. B. benutzerdefiniertes Branding, Voreinstellungen für die Dateiaufbewahrung und Sicherheitseinstellungen.
- Pflegen Sie ein einziges Speicher-Repository für alle Ihre Mandanten.
- Integrieren Sie neue Kunden schneller und reduzieren Sie die Kosten und den Verwaltungsaufwand, der durch die Einrichtung einer separaten Speicherzone für jedes Kundenkonto entsteht.

Erstellen Sie ein Partnerkonto

Sie müssen über ein Partnerkonto verfügen, bevor Sie eine Multitenant-Speicherzone registrieren können.

Um ein Partnerkonto zu erstellen, müssen Sie sich beim CSP-Programm registrieren und bei Ihrem bevorzugten Vertriebspartner eine Lager-SKU bestellen, die Sie berechtigt, ShareFile als Service anzubieten.

Wenn Sie bereits als CSP registriert sind und das entsprechende ShareFile für CSPs mit Lager-SKU bestellt haben, wurde bereits ein Partnerkonto für Sie erstellt. Wenn Sie dieses neue Partnerkonto nicht finden können, wenden Sie sich bitte an ShareFile Account Services unter acctsvcs@sharefile.com.

Wenn Sie mit der Bereitstellung von Kundenkonten im Rahmen Ihres CSP ShareFile-Angebots beginnen, empfehlen wir, in Ihrem Partnerkonto einen generischen Dienstkonto-Administrator zu erstellen. Auf diese Weise kann der Admin-Benutzer der offizielle Partneradministrator all Ihrer Kundenkonten sein. Stellen Sie sicher, dass für diesen Dienstkonto-Administrator die Berechtigung „Mandanten verwalten“aktiviert ist. Aus diesem Grund empfehlen wir Partnern, diesen Partneradministrator jetzt zu erstellen, bevor sie das Formular zur Beantragung eines CSP-Kundenkontos ausfüllen (in Schritt 4).

Installieren und Einrichten einer Multi-Tenant-Speicherzone

- Erstellen Sie eine neue Multitenant-Speicherzone und verknüpfen Sie sie mit Ihrem Partnerkonto. Einzelheiten finden Sie unter Installieren Sie den StorageZones Controller und erstellen Sie eine Speicherzone.
- Installieren Sie den Storage Zone Controller im Mehrmandantenmodus. Stellen Sie sicher, dass Sie die folgende im Installationsartikel angegebene Eingabeaufforderung ausführen, die im vorherigen Schritt erwähnt wurde.

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

> **Hinweis:**
>
> Im obigen Befehl müssen Sie möglicherweise die Versionsnummer (5.0.1 im Beispiel) so aktualisieren, dass sie mit der Nummer der MSI übereinstimmt, die Sie installieren möchten.

Konfigurieren Sie die neue Speicherzone und verknüpfen Sie sie mit Ihrem Partnerkonto

Einzelheiten finden Sie in Schritt 10 unter Installieren Sie den StorageZones Controller und erstellen Sie eine Speicherzone.

Loggen Sie sich in Ihr Partnerkonto ein, in dem Sie die neue Zone registrieren möchten.

> **Wichtig:**
>
> Dieses Konto muss über die folgenden ShareFile-Berechtigungen verfügen: Mandanten verwalten und Zonen erstellen und verwalten.

Sie können sich jetzt bei Ihrem Partnerkonto anmelden und die neue Multitenant-Speicherzone sehen. Klicken Sie auf den **Tab Admin-Einstellungen > Speicherzonen > Vom Partner verwaltet**.

Mandantenkonten für die Mehrmandantenzone anfordern

Um Mandantenkonten anzufordern, füllen Sie das Formular zur Beantragung eines CSP-Kundenkontosaus.

Wenn Sie ein Mandantenkonto anfordern, müssen Sie auch einen Partner-Admin-Benutzer angeben. Dieser Partneradministrator muss ein Admin-Benutzer in Ihrem Partnerkonto sein und die Berechtigung „Mandanten verwalten“aktiviert haben. Wenn ein Mandantenkonto erstellt wird, wird dieser Partner-Admin-Benutzer automatisch als Admin-Benutzer für das Konto eingerichtet und kann sich anmelden und das Mandantenkonto verwalten. Da es in einem Konto nicht zwei Benutzer mit derselben E-Mail-Adresse geben kann, kann die im Formular angegebene E-Mail-Adresse des Partneradministrators nicht mit der E-Mail-Adresse des Kundenadministrators auf demselben Formular identisch sein.

Um eine möglichst schnelle Bearbeitung zu gewährleisten, stellen Sie sicher, dass Sie die richtige Org-ID und den Multitenant-Zonennamen angeben, den Sie als Speicherzone für das Mandantenkonto verwenden möchten.

Sie erhalten eine E-Mail, nachdem Citrix die angeforderten Konten bereitgestellt hat. Die E-Mail enthält Informationen zur Tenant-Subdomain und einen Aktivierungslink zur Einrichtung des Zugriffs. ShareFile sendet Ihnen und den administrativen Benutzern Ihrer Kunden separate E-Mails.

Ihre Kunden können dann beginnen, ShareFile zu verwenden. Alle neuen Benutzer, denen ein Mandantenkonto zugewiesen wurde, verwenden die Mehrmandantenzone, die Sie als Standardspeicherort für die Benutzerdateien angegeben haben.

Vorschau von Office-Dateien und PDF-Dateien mit einem Office Online Server

Diese Funktion wird in unterstützten Office Online Server-Umgebungen unterstützt. Klicken Sie hier, um Informationen zur Einrichtung zu erhalten.

Connector teilen

Diese Funktion wird bei Mehrmandantenzonen unterstützt.

Mieter verwalten

Im Partnerkonto befindet sich ein Tenant Management-Dashboard unter **Admin-Einstellungen > Erweiterte Einstellungen**. Dieses zentrale Dashboard ermöglicht es Ihnen, den Status aller Mieter zu überprüfen, die mit Ihrem Partnerkonto verknüpft sind. Das Dashboard enthält den Lizenzverbrauch, die Standardspeicherzone, den Speicherverbrauch und den Kontostatus (Bezahlt oder Testversion) für jeden Mandanten.

> **Hinweis:**
>
> Das Dashboard ist nur für Benutzer in Ihrem Partnerkonto verfügbar, für die die Benutzerberechtigung **„Mandanten verwalten** "aktiviert ist.

Einschränkungen für mehrere Mandanten

Die ShareFile Information Rights Management-Funktion (IRM) wird für mehrinstanzenfähige Speicherzonen nicht unterstützt.

Problembehandlung

Zone konnte nicht erstellt werden: Verboten

Wenn Sie bei der Registrierung der Speicherzone die folgende Fehlermeldung erhalten: „Zone konnte nicht erstellt werden: verboten", überprüfen Sie, ob Ihre Benutzerberechtigungen die Berechtigung „Mandanten verwalten"enthalten.

Upgrade

March 17, 2024

Upgrade von Storage Zones Controller 5.10 oder höher auf die neueste Version

> **Hinweise:**
>
> ShareFile empfiehlt, vor dem Update einen Snapshot des Servers zu erstellen und die Storage Zone Server-Konfiguration zu sichern. Informationen zum Sichern der StorageZone-Konfiguration finden Sie unter Sichern einer primären StorageZones Controller-Konfiguration
>
> . Probleme beim Upgrade Ihres StorageZones Controllers finden Sie unter Problembehandlung

> bei ShareFile Storage Zone Controller-Upgrades.

Aktualisieren Sie Storage Zones Controller 5.10 mithilfe der folgenden Schritte.

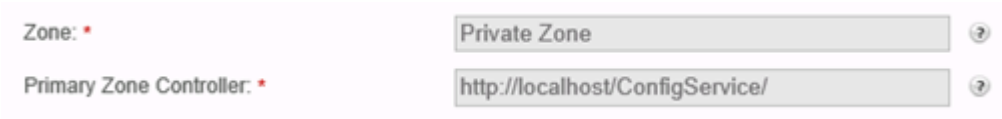
1. Laden Sie die neueste Version der Storage Zone Controller-Software von der ShareFile-Downloadseite herunter.

   > **Hinweis:**
   >
   > Speicherzonencontroller sind während des Upgrades und Serverneustarts nicht verfügbar. Um einen Datenverlust zu vermeiden, empfehlen wir, ein Wartungsfenster mit den Benutzern zu vereinbaren. Teilen Sie ihnen mit, dass die Zone während des Upgrades für Dateiübertragungen nicht verfügbar ist.

2. Installieren Sie die MSI-Datei auf dem Windows-Server, auf dem der Storage Zone Controller installiert ist. Wenn Sie mehrere Server haben, sollte das Update zuerst auf dem Primärserver und dann auf den anderen installiert werden. Es gibt zwei Möglichkeiten, herauszufinden, welcher Server der Primärserver ist:

   a) Identifizieren Sie den primären StorageZones Controller auf der **Konfigurationsseite** :

      - Navigieren Sie auf einem Controller-Server zu `http://localhost/configservice/login.aspx` oder starten Sie das Konfigurationstool über das Startmenü. Für den Zugriff auf die Konfiguration ist die Erlaubnis zum „Erstellen und Verwalten von Zonen“erforderlich.
      - Markieren Sie auf der Registerkarte **Daten** das Feld Primary Zone Controller. In dem Feld wird der Serverhostname des primären Zonencontrollers als aufgeführt `http://server/ConfigService`.

      Beachten Sie, dass der Wert localhost in `http://localhost/ConfigService` angibt, dass dieser Server der primäre Zonencontroller ist.

   b) Identifizieren Sie den primären StorageZones Controller in der Registrierung:

      - Öffnen Sie auf einem Controller-Server den Registrierungseditor (regedit.exe).
      - Suchen Sie den Registrierungsschlüssel: HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ Citrix\ StorageCenter
      - Stellen Sie sicher, dass der Schlüsselwert `isPrimaryConfigServer` wahr ist.

3. Starten Sie das Upgrade auf dem primären StorageZone-Controller:

a) Führen Sie StorageCenter.msi aus, um den Setup-Assistenten für den ShareFile Storage Zones Controller zu starten.

b) Antworten Sie auf die Eingabeaufforderungen. Nach Abschluss der Installation zeigt der Assistent die Meldung „Der Setup-Assistent für den Citrix ShareFile Storage Zones Controller wurde abgeschlossen“an.

c) Starten Sie den Server neu.

4. Auf jedem sekundären Speicherzonencontroller (falls erforderlich):

   a) Führen Sie StorageCenter.msi aus, um den Setup-Assistenten für den ShareFile Storage Zones Controller zu starten.

   b) Antworten Sie auf die Eingabeaufforderungen und wählen Sie dann **Fertig stellen aus.**

   c) Starten Sie den Server neu.

5. Starten Sie auf allen Speicherzonencontrollern den IIS-Server aller Zonenmitglieder neu.

   a) Starten Sie die CMD-Eingabeaufforderung und Als Administrator ausführen.

   b) Tippen `iisreset` Sie dann auf die **Eingabetaste**. Wenn erfolgreich, zeigt die Eingabeaufforderung “Internetdienste erfolgreich neu gestartet”an.

   c) Vergewissern Sie sich, dass die Registrierungseinstellungen auf dem primären StorageZones Controller nach dem Upgrade korrekt sind.

6. Wählen Sie nach der Upgrade-Installation die Option StorageZones-Konfigurationsseite auf einem beliebigen Zonenmitglied starten, um sich anzumelden und alle Konfigurationseinstellungen zu ändern.

   - Um jederzeit zur StorageZones Controller-Konsole zurückzukehren, öffnen Sie `http://localhost/configservice/login.aspx`. Nachdem Sie auf **Fertig stellen** geklickt oder zur StorageZones Controller-Konsole zurückgekehrt sind, wird die Anmeldeseite geöffnet.

> **Hinweis: Beachten Sie**
>
> , dass Sie für die Anmeldung auf der Konfigurationsseite des Storage Zone Controllers ein anwendungsspezifisches Kennwort verwenden müssen. Wenn Sie ein neues anwendungsspezifisches Passwort erstellen müssen, lesen Sie den folgenden Support-Artikel: Erstellen Sie ein anwendungsspezifisches Passwort.

   - Um die angezeigten Informationen zu ändern, wählen Sie **Ändern** aus, nehmen Sie Ihre Änderungen vor und wählen Sie **Speichern**.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Datenübertragungen an jeden StorageZone-Controller funktionieren, bevor Sie das Wartungsfenster beenden.

Verwalten von Storage Zones

February 11, 2022

Nachdem Sie Ihre primären und sekundären Speicherzonen-Controller installiert haben, verwenden Sie die folgenden Verfahren, um die Controller zu verwalten und sie für die Notfallwiederherstellung vorzubereiten.

Um die StorageZone Controller-Konsole zu öffnen, gehen Sie zu `http://localhost/configservice/login.aspx` oder starten Sie das Konfigurationstool über das Startmenü.

StorageZone Controller verwalten

- Verbinden eines sekundären Speicherzonen-Controllers mit einer Speicherzone
- Ändern der Adresse oder Passphrase eines primären StorageZones-Controllers
- Speicherzonen-Controller herabstufen und fördern
- Deaktivieren, Löschen oder erneutes Bereitstellen eines StorageZone Controllers
- Übertragen von Dateien auf eine neue Netzwerkfreigabe
- Sichern einer primären StorageZones Controller-Konfiguration
- Wiederherstellen einer primären StorageZone Controller-Konfiguration
- Ersetzen eines primären StorageZone Controllers
- Vorbereiten des StorageZones Controller für die Dateiwiederherstellung
- Stellen Sie Dateien und Ordner aus Ihrem ShareFile-Datenbackup wieder her
- Stimmen Sie die ShareFile-Cloud mit einer Speicherzone ab
- Konfigurieren von Antivirenscans hochgeladener Dateien
- ShareFile-Daten migrieren
- Connector-Favoriten

Anfügen eines sekundären StorageZones Controllers an eine Speicherzone

April 20, 2021

Konfigurieren Sie eine Speicherzone mit hoher Verfügbarkeit durch Einbinden von mindestens zwei StorageZones Controllers. Um dies zu tun, müssen Sie:

1. Installieren Sie einen primären StorageZones Controller und erstellen Sie eine Zone (wie unter beschriebenInstallieren eines StorageZones Controller und Erstellen einer Speicherzone).
2. Installieren Sie den StorageZones Controller auf einem zweiten Server und verbinden Sie diesen Controller mit derselben Zone.

StorageZones Controller, die zu derselben Zone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden.

Bei einer Hochverfügbarkeitsbereitstellung handelt es sich bei den sekundären Servern um unabhängige, voll funktionsfähige StorageZones Controller. Das Speicherzonen-Kontrollsubsystem wählt nach dem Zufallsprinzip einen StorageZones Controller aus, um Betriebsanforderungen zu verarbeiten, einschließlich Upload-, Download-, Kopier- und Löschvorgänge.

Wenn der primäre Server offline geschaltet wird, können Sie problemlos einen sekundären Server zum primären Server heraufstufen. Sie können auch einen Server von primär auf sekundär herabstufen.

1. Öffnen Sie einen Webbrowser auf dem Server als sekundärer StorageZones Controller. Öffnen Sie dann `http://localhost/configservice/login.aspx`, und melden Sie sich an.
2. Klicken Sie auf **Vorhandene Zone verbinden**, und wählen Sie die Speicherzone aus.
3. Geben Sie die angeforderten Informationen ein und klicken Sie dann auf **Registrieren**.

   Für den primären Zonencontroller können Sie nur den Hostnamen oder die IP-Adresse eingeben, und ShareFile füllt die vollständige URL aus. Um eine URL zu testen, geben Sie sie in das Adressfeld des Browsers ein. Wenn die URL korrekt ist, wird eine ShareFile Bannerseite angezeigt. Für Standardzonen: Wenn die URL falsch ist und Sie https angegeben haben, überprüfen Sie, ob Sie gültige, vertrauenswürdige öffentliche SSL-Zertifikate verwenden.
4. Wenn Sie einen Proxyserver für den primären StorageZones Controller verwenden, geben Sie den Proxyserver für den sekundären Controller an, wie unter beschriebenFestlegen eines Proxyservers für Speicherzonen.
5. Starten Sie den IIS-Server aller Zonenmitglieder neu.

   Ein sekundärer StorageZones Controller erbt die Konfiguration des primären Controllers während des Startvorgangs.

Ändern der Adresse oder Passphrase eines primären StorageZones-Controllers

February 11, 2022

> **Hinweis:**
>
> Nur der Kontoadministrator kann Änderungen an Adressen oder Passphrasen vornehmen.

So geben Sie eine andere externe oder lokale Adresse für einen primären Speicherzonen-Controller an

Sie können die externe Adresse eines primären StorageZone Controllers ändern, indem Sie dieses Verfahren oder andere Serververwaltungstools verwenden.

1. Öffnen Sie auf dem primären Speicherzonen-Controller-Server die **Konfigurationsseite**, oder navigieren Sie zu: `http://localhost/configservice/login.aspx`.
2. Melden Sie sich mit ShareFile-Administratoranmeldeinformationen bei der Konfigurationsseite
3. Wählen Sie auf der Registerkarte Daten die Option **Ändern**aus.
4. Geben Sie die neue **externe Adresse** oder **lokale Adresse** an und wählen Sie dann **Änderungen speichern**aus.
5. Wiederholen Sie die Schritte für alle Zonenmitglieder.
6. Starten Sie den IIS-Server aller Zonenmitglieder neu.

So ändern Sie die Passphrase eines primären StorageZone Controllers

> **Hinweis:**
>
> Die aktuelle Passphrase wird benötigt, um die Passphrase eines StorageZone Controllers zu ändern.

1. Öffnen Sie die Storage Zones-Konfigurationsseite: `http://localhost/configservice/login.aspx`.
2. Klicken Sie auf **Ändern**.
3. Geben Sie eine Passphrase an, die zum Schutz Ihres Dateiverschlüsselungsschlüssels verwendet werden soll. Achten Sie darauf, die Passphrase und den Verschlüsselungsschlüssel an einem sicheren Ort zu archivieren.

Die Passphrase stimmt nicht mit Ihrem Kontokennwort überein und kann bei Verlust nicht wiederhergestellt werden. Wenn Sie die Passphrase verlieren, können Sie keine Speicherzonen neu installieren, zusätzliche StorageZone Controller mit der Speicherzone verbinden oder die Speicherzone wiederherstellen, falls der Server ausfällt.

> **Hinweis:**
>
> Der Verschlüsselungsschlüssel wird im Stammverzeichnis des freigegebenen Speicherpfads angezeigt. Durch den Verlust der Verschlüsselungsschlüsseldatei wird der Zugriff auf alle Speicherzonendateien sofort unterbrochen.

4. Wenn Sie die Passphrase auf dem Primärserver geändert haben: Melden Sie sich auf der Storage Zones-Konfigurationsseite für jedes der anderen Mitglieder an und geben Sie die Passphrase ein, wenn Sie dazu aufgefordert werden.

   Sie müssen dieselbe Passphrase für jeden StorageZone Controller in einer Zone verwenden.

5. Starten Sie den IIS-Server aller Zonenmitglieder neu.

Herabstufen und Heraufstufen von StorageZones Controllern

October 13, 2020

Bei einer Hochverfügbarkeitsbereitstellung handelt es sich bei den sekundären Servern um unabhängige, voll funktionsfähige StorageZones Controller. Um einen primären StorageZones Controller zu verwalten oder zu ersetzen, stufen Sie ihn zuerst herab und stufen Sie dann einen sekundären Controller herauf. Wenn der primäre Server offline geschaltet wird, können Sie einen sekundären Server zum primären Server heraufstufen.

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. So stufen Sie einen primären StorageZones Controller herab:

   a) Suchen Sie den Registrierungsschlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

   b) Setzen Sie isPrimaryConfigServer auf false.

c) Legen Sie PrimaryConfigServiceUrl auf die URL des Servers fest, der der neue primäre StorageZones Controller sein soll, indem Sie das Format `https://IPaddress` oder `https://hostname/ConfigService/` verwenden.

d) Starten Sie den IIS-Server aller Zonenmitglieder neu.

2. So stufen Sie einen sekundären Storage Zones Controller herauf:

   a) Suchen Sie den Registrierungsschlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

   b) Setzen Sie isPrimaryConfigServer auf true.

   c) Setzen Sie PrimaryConfigServiceUrl auf `http://localhost/ConfigService/`.

   d) Starten Sie den IIS-Server aller Zonenmitglieder neu.

3. Ändern Sie alle zusätzlichen sekundären StorageZones Controller:

   a) Suchen Sie den Registrierungsschlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

   b) Legen Sie PrimaryConfigServiceURL auf die URL des Servers fest, der der neue primäre StorageZones Controller ist, indem Sie das Formular`https://IPaddress` oder verwenden`https://hostname/ConfigService/`.

   c) Starten Sie den IIS-Server aller Zonenmitglieder neu.

Deaktivieren, Löschen oder erneutes Bereitstellen eines StorageZone Controllers

March 13, 2023

So deaktivieren Sie einen StorageZones Controller

> **Hinweis:**
>
> Verwenden Sie dieses Verfahren, wenn jeder StorageZones Controller eine andere externe Adresse hat. Deaktivieren Sie einen Controller über die Citrix ADC-Schnittstelle, wenn Sie dieselbe externe Adresse für alle StorageZone-Controller verwenden.

Deaktivieren Sie einen StorageZones Controller, bevor Sie den Server für Wartungsarbeiten offline nehmen.

1. Klicken Sie in der ShareFile-Weboberfläche auf **Admin** und dann auf **Speicherzonen**.
2. Klicken Sie auf den Zonennamen und dann auf den Hostnamen des StorageZones Controllers.
3. Deaktivieren Sie das aktivierte Kontrollkästchen und klicken Sie dann auf **Änderungen speichern**.
4. Starten Sie den IIS-Server aller Zonenmitglieder neu.

So löschen Sie einen StorageZones Controller

Durch das Löschen eines StorageZones Controllers werden die Daten oder SCKeys.txt nicht gelöscht. Wenn Sie einen primären StorageZones Controller löschen, stufen Sie ihn herab, bevor Sie fortfahren.

1. Klicken Sie in der ShareFile-Weboberfläche auf **Admin** und dann auf **Speicherzonen**.
2. Klicken Sie auf den Zonennamen und dann auf den Hostnamen des StorageZones Controllers.
3. Klicken Sie auf **Löschen**.
4. Starten Sie den IIS-Server aller Zonenmitglieder neu.

So stellen Sie einen StorageZones Controller erneut bereit

Bei der erneuten Bereitstellung eines StorageZones Controllers gehen keine Informationen verloren.

1. Deinstallieren Sie StorageZones vom Server.
2. Klicken Sie in der ShareFile-Weboberfläche auf **Admin > Speicherzonen**und wählen Sie dann Ihre Zone aus. Löschen Sie die Zone nicht.
3. Wählen Sie den StorageZones Controller aus und löschen Sie ihn.
4. Installieren Sie Speicherzonen. Registriere es noch nicht.
5. Führen Sie den StorageZones Controller-Konfigurationsassistenten aus, um den StorageZones Controller mit einer Zone zu verbinden und die Registrierung abzuschließen.
6. Starten Sie den IIS-Server aller Zonenmitglieder neu.

Übertragen von Dateien auf eine neue Netzwerkfreigabe

October 13, 2020

Bevor Sie eine neue Netzwerkfreigabe für die private Datenspeicherung einrichten:

Anforderungen

- StorageZones Controller, die zu derselben Speicherzone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden.
- StorageZones Controller greifen mithilfe des IIS-Kontopool-Benutzers auf die Freigabe zu. Standardmäßig arbeiten Anwendungspools unter dem Netzwerkdienst-Benutzerkonto, das über Benutzerrechte auf niedriger Ebene verfügt. Ein StorageZones Controller verwendet standardmäßig das Netzwerkdienstkonto.
- Das Netzwerkdienstkonto muss **vollen** Zugriff auf diesen Speicherort haben.
- Deaktivieren Sie StorageZones Controller für neue Uploads, bevor Sie Daten auf die neue Freigabe übertragen. Navigieren Sie in der Webanwendung zu **Admin-Einstellungen** > **StorageZones**. Wählen Sie den Zonennamen aus. Wählen Sie unter **Storage Center** jeden Hostserver aus. Um den Datenverkehr zu jedem Hostserver zu beenden, deaktivieren Sie unter **Servereinstellungen** die Option **Aktiviert**.

1. Öffnen Sie die Konfigurationsseite für Speicherzonen: `http://localhost/configservice/login.aspx`.
2. Klicken Sie auf **Ändern**.
3. Geben Sie unter **Speicherort**den UNC-Pfad zu Ihrer Netzwerkfreigabe ein, `\\server\share` und klicken Sie dann auf **Speichern**.

   > **Achtung:**
   >
   > Storage Zones Controller überschreibt alle Daten in diesem Pfad mit einem proprietären Speicherformat. Als bewährte Methode sollten Sie niemals einen Pfad zu einem Speicherort mit Dateidaten angeben. Reservieren Sie diesen Speicherort nur für Speicherzonen für ShareFile Daten.

4. Wenn sich die Anmeldeinformationen für den UNC-Pfad Ihres neuen Netzwerkfreigabe-Standorts von der vorherigen unterscheiden, geben Sie das Kennwort für die Speicheranmeldung und das Speicherkennwort an.
5. Starten Sie den IIS-Server aller Zonenmitglieder neu.
6. Melden Sie sich auf der Konfigurationsseite aller Zonenmitglieder an.
7. Kopieren Sie die gesamte Verzeichnisstruktur, einschließlich SCkeys.txt, auf den neuen Server.

Sichern einer primären StorageZones Controller-Konfiguration

June 27, 2023

Auf Ihrem lokalen Standort ist ein StorageZone Controller installiert, für dessen Sicherung Sie verantwortlich sind. Um Ihre Bereitstellung vollständig zu schützen, sollten Sie einen Snapshot des StorageZone Controller-Servers erstellen, Ihre Konfiguration sichern und StorageZone Controller für die Dateiwiederherstellung vorbereiten.

Es ist wichtig, dass Sie Ihre Konfiguration wie in diesem Thema beschrieben sichern. Wenn Sie beispielsweise kein Backup haben und jemand versehentlich eine Zone löscht, können Sie die Ordner und Dateien in dieser Zone nicht wiederherstellen.

> **Wichtig:**
>
> Verwenden Sie für dieses Verfahren unbedingt PowerShell 4.0. Weitere Informationen zu PowerShell-Anforderungen finden Sie unter PowerShell-Skripte und -Befehle in StorageZone Controller-Systemanforderungen.

Das StorageZone Controller-Installationsprogramm enthält ein PowerShell-Modul mit Befehlen zum Sichern und Wiederherstellen der primären Speicherzonen-Controller-Konfigurationseinstellungen. Ihre Backup umfasst Konfigurationsinformationen für Zonen, Speicherzonen für ShareFile-Daten, Speicherzonen-Connector für SharePoint und Speicherzonen-Connector für Netzwerkdateifreigaben.

Für die Backup- und Wiederherstellungsbefehle müssen Sie die 32-Bit-Version von PowerShell unter demselben Benutzerkontext wie der Speicherzonencontroller ausführen. Um den Benutzerkontext festzulegen, verwenden Sie das Tool PsExec. Dieses Tool kann von heruntergeladen https://docs.microsoft.com/en-us/sysinternals/downloads/psexecwerden.

> **Hinweis:**
>
> Diese Schritte gelten nicht für einen sekundären StorageZone Controller. Um einen sekundären Speicherzonen-Controller wiederherzustellen, installieren Sie den Speicherzonen-Controller auf dem Server neu und verbinden Sie den Server dann mit dem primären Speicherzonen-Controller.

1. Das in diesem Verfahren verwendete PowerShell-Skript ist nicht signiert, sodass Sie Ihre PowerShell-Ausführungsrichtlinie ändern müssen.

   a) Ermitteln Sie, ob Ihre PowerShell-Ausführungsrichtlinie es Ihnen ermöglicht, lokale, unsignierte Skripte auszuführen: PS `C:\>Get-ExecutionPolicy`

      Mit einer Richtlinie von RemoteSigned, Unrestricted oder Bypass können Sie beispielsweise unsignierte Skripte ausführen.

   b) So ändern Sie Ihre PowerShell-Ausführungsrichtlinie: PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. Stellen Sie den Benutzerkontext für diese PowerShell-Sitzung ein. Führen Sie in einem Befehlsfenster einen der folgenden Befehle aus.

- Bei Verwendung des standardmäßigen Netzwerkdienstkontos:

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

- Wenn Sie einen benannten Benutzer für den Speicherzonen-Controller-Anwendungspool verwenden:

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

Ein PowerShell-Fenster öffnet sich.

3. Importieren Sie an der PowerShell-Eingabeaufforderung das Modul ConfigBR.dll: `Import-Module C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll`

   Sie müssen das Modul jedes Mal importieren, wenn Sie ein neues PowerShell-Fenster öffnen.

4. Führen Sie an der PowerShell-Eingabeaufforderung den Befehl Get-SfConfig aus und führen Sie die folgenden Eingabeaufforderungen aus:

   - **PrimaryZoneController** - Beispieleingaben:
     - Stellen Sie eine Verbindung zu einem lokalen Server her: `http://localhost/ConfigService/`
     - Stellen Sie eine Verbindung zu einem Remoteserver her: `http[s]://myservername.domain.com/ConfigService/`
     - Stellen Sie eine Verbindung zu einem Remoteserver her, wenn DNS-Probleme die Verbindung zu einem Servernamen verhindern: `http[s]://10.40.37.5/ConfigService/`
   - Passphrase —Die für den Storage Zone Controller angegebene Passphrase.
   - FilePath - Beispiel `c:\szc-backup.bak`

   Befehlsparameter:

Parameter	Beschreibung	Beispiele
“Server”	Der primäre StorageZone Controller-Servername oder die IP-Adresse. Sie kann in einer der folgenden unter Beispiele gezeigten Formen vorliegen und muss den nachgestellten Schrägstrich enthalten.	Mit einem lokalen Server verbinden: `http://localhost/ConfigService/`; Mit einem Remoteserver verbinden: `http[s]://myservername.domain.com/ConfigService/`; Stellen Sie eine Verbindung zu einem Remoteserver her, wenn DNS-Probleme die Verbindung zu einem Servernamen verhindern: `http[s]://10.40.37.5/ConfigService/`
“passphrase”	Die für den Speicherzonencontroller angegebene Passphrase.	“MyPassphrase”
“fullpath”	Ein Speicherort zum Speichern der Backupdatei.	“c:\szc-backup.bak”

Der Befehl **Get-SfConfig** erstellt die Backupdatei.

Informationen zum Wiederherstellen einer primären StorageZone Controller-Konfiguration finden Sie unter Wiederherstellen einer primären StorageZone Controller-Konfiguration.

Wiederherstellen einer primären StorageZone Controller-Konfiguration

February 11, 2022

> **Wichtig:**
>
> - Verwenden Sie für dieses Verfahren unbedingt PowerShell 4.0. Weitere Informationen zu PowerShell-Anforderungen finden Sie in den PowerShell-Skripten und -Befehlen in StorageZone Controller Systemanforderungen.

> - Weitere Informationen zur systemweiten Implementierung von TLS finden Sie im Microsoft-Artikel How to enable TLS 1.2 auf Clients.

StorageZone Controller bietet diese Optionen für die Notfallwiederherstellung, wenn ein primärer StorageZone Controller gelöscht wird oder ausfällt:

- Wenn ein sekundärer Speicherzonen-Controller verfügbar ist, stufen Sie den sekundären Controller zu einem primären Controller auf.
- Wenn kein sekundärer StorageZone Controller verfügbar ist und Sie Ihre primäre StorageZone Controller-Konfiguration gesichert haben (wie unter Sichern einer primären StorageZone Controller-Konfigurationbeschrieben), stellen Sie den primären StorageZone Controller aus der Backupdatei wieder her.
- Wenn Sie keine Backup Ihrer primären StorageZone Controller-Konfiguration haben und alle Ihre StorageZone Controller versehentlich gelöscht werden oder unbrauchbar werden, ist nur eine teilweise Wiederherstellung möglich. Sie können Zonen und die Konfiguration für Speicherzonen für ShareFile-Daten wiederherstellen, aber keine Storage Zones-Connectors.

So stellen Sie einen primären StorageZone Controller aus einer Backupdatei wieder her

> **Hinweis:**
>
> Diese Schritte gelten nur für einen primären StorageZone Controller. Um einen sekundären StorageZone Controller wiederherzustellen, installieren Sie den StorageZone Controller auf dem Server neu und verbinden Sie den Server dann mit dem primären StorageZone Controller.

1. Das in diesem Verfahren verwendete PowerShell-Skript ist nicht signiert, sodass Sie möglicherweise Ihre PowerShell-Ausführungsrichtlinie ändern müssen.

   a) Ermitteln Sie, ob Ihre PowerShell-Ausführungsrichtlinie es Ihnen ermöglicht, lokale, unsignierte Skripte auszuführen: PS `C:\>Get-ExecutionPolicy`

   Mit einer Richtlinie von RemoteSigned, Unrestricted oder Bypass können Sie beispielsweise unsignierte Skripte ausführen.

   b) So ändern Sie Ihre PowerShell-Ausführungsrichtlinie: PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. Stellen Sie den Benutzerkontext für diese PowerShell-Sitzung ein. Führen Sie in einem Befehlsfenster einen der folgenden Befehle aus.

   > **Hinweis:**

> Laden Sie PsExec.exe von https://docs.microsoft.com/en-us/sysinternals/downloads/psexec herunter und folgen Sie die Installationsanweisungen auf dieser Seite.

- Bei Verwendung des standardmäßigen Netzwerkdienstkontos:

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

- Wenn Sie einen benannten Benutzer für den Speicherzonen-Controller-Anwendungspool verwenden:

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

Ein PowerShell-Fenster öffnet sich.

3. Importieren Sie an der PowerShell-Eingabeaufforderung das Modul ConfigBR.dll: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   Sie müssen das Modul jedes Mal importieren, wenn Sie ein neues PowerShell-Fenster öffnen.

4. Führen Sie an der PowerShell-Eingabeaufforderung den Befehl `Set-SfConfig` aus: `Set-SfConfig -PrimaryZoneController "server"-Passphrase "passphrase"-FilePath "fullpath"`

   Wobei:

   - server ist der primäre StorageZone Controller-Servername oder die IP-Adresse. Es kann in einer der folgenden Formen vorliegen und muss den nachfolgenden Schrägstrich enthalten.

     `http://localhost/ConfigService/`

     `servername/` oder `serverip/` (wenn Sie HTTP verwenden)

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

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

   - Passphrase ist diejenige, die für den StorageZone Controller angegeben ist.
   - fullpath ist der Speicherort und der Name der Backupdatei. Beispiel: `c:\szc-backup.bak`.

So stellen Sie einen primären StorageZones-Controller ohne Backupdatei wieder her

Wenn Sie keine Backupdatei haben, können Sie Zonen und die Konfiguration für Speicherzonen für ShareFile-Daten, aber nicht für Storage Zones Connectors, wiederherstellen.

1. Stellen Sie den Benutzerkontext für diese PowerShell-Sitzung ein. Führen Sie in einem Befehlsfenster einen der folgenden Befehle aus.

   - Bei Verwendung des standardmäßigen Netzwerkdienstkontos:

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

   - Wenn Sie einen benannten Benutzer für den Speicherzonen-Controller-Anwendungspool verwenden:

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

   Ein PowerShell-Fenster öffnet sich.

2. Importieren Sie an der PowerShell-Eingabeaufforderung das Modul ConfigBR.dll: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   Sie müssen das Modul jedes Mal importieren, wenn Sie ein neues PowerShell-Fenster öffnen.

3. Führen Sie an der PowerShell-Eingabeaufforderung den Befehl Join-SFConfig aus:

   > **Wichtig:**
   >
   > Der Befehl Join-SFConfig unterstützt derzeit keinen Azure- oder Amazon S3-Speicher. Wenden Sie sich an den ShareFile-Support, wenn Sie diesen Befehl verwenden müssen.

   ```
   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]
   ```

   Wobei:

   - ZoneID kann wie folgt abgerufen werden:

     a) Klicken Sie in der ShareFile-Weboberfläche auf **Admin > Storage zones**, klicken Sie mit der rechten Maustaste auf den Site-Namen, und **wählen**Sie

        Die angezeigte Adresse endet mit der Zonen-ID, die wie folgt aussieht: `zae4fb8c-8520-478f-8f87-aa589a8fd181`.

b) Kopieren Sie diese ID und fügen Sie sie in den Befehl Join-SFConfig ein.

- StorageCenterID kann wie folgt abgerufen werden:

  a) Klicken Sie in der ShareFile-Weboberfläche auf Admin > Storage Zones, klicken Sie auf den Site-Namen, klicken Sie mit der rechten Maustaste auf den Hostnamen, und wählen

     Die angezeigte Adresse endet mit der Speicher-ID, die wie folgt aussieht: `scd344cf-8043-4ce2-974b-8f9cd83e2978`.

  b) Kopieren Sie diese ID und fügen Sie sie in den Befehl Join-SFConfig ein.

- StorageZoneLocation wird nur benötigt, wenn Speicherzonen für ShareFile-Daten für die Zone aktiviert sind.
- StorageUserName und StoragePassword werden nur benötigt, wenn Speicherzonen für ShareFile-Daten für die Zone aktiviert sind und Ihr Speicherort eine Authentifizierung erfordert.
- AzureAccountName, AzureAccessKey und AzureContainerName werden nur benötigt, wenn Speicherzonen für ShareFile-Daten in einem Windows Azure-Speichercontainer gespeichert sind.

4. Um Storage Zones Connectors wiederherzustellen, verwenden Sie die StorageZone Controller-Konsole (`http://localhost/configservice/login.aspx`), um Connectors zu aktivieren und

Ersetzen eines primären StorageZones Controllers

April 20, 2021

Um einen primären StorageZones Controller durch einen Controller zu ersetzen, der sich an einem anderen Speicherort befindet, z. B. in einer anderen Domäne, verwenden Sie die Backup- und Wiederherstellungsprozeduren. Die folgenden Schritte stellen sicher, dass Ihre Konfigurationseinstellungen und alle Ihre Daten übertragen werden.

1. Erstellen Sie eine Backupdatei für Ihre vorhandene Storage Zones Controller Konfiguration. Siehe Sichern einer primären StorageZones Controller-Konfiguration.
2. Installieren Sie einen StorageZones Controller am neuen Netzwerkspeicherort, aber konfigurieren Sie ihn nicht.
3. Importieren Sie die gesicherte Konfiguration auf den neuen Controller. Siehe Wiederherstellen einer primären StorageZones Controller-Konfiguration.

4. Kopieren Sie Ihre Daten in die neue Netzwerkfreigabe, melden Sie sich bei der Konfigurationskonsole für den neuen StorageZones Controller an, und geben Sie die neuen Speicherpfadinformationen ein. Siehe Übertragen von Dateien auf eine neue Netzwerkfreigabe.
5. Aktualisieren Sie in der neuen StorageZones Controller Konfigurationskonsole die externe URL des Controllers. Siehe Ändern der Adresse oder Passphrase eines primären StorageZones Controller.

Vorbereiten des StorageZones Controller für die Dateiwiederherstellung

September 4, 2023

> **Warnung:**
>
> Die ShareFile-Wiederherstellungsfunktion erstellt nicht automatisch ein Backup Ihres persistenten Speicherorts. Sie sind dafür verantwortlich, ein Backup-Hilfsprogramm auszuwählen und es alle 1 bis 7 Tage auszuführen.

Wie Sie sich auf die Dateiwiederherstellung vorbereiten, hängt davon ab, wo Ihre Daten gespeichert sind:

- **Ein unterstütztes Speichersystem eines Drittanbieters** —Wenn Sie ein Speichersystem eines Drittanbieters mit StorageZones Controller verwenden, ist Ihr Drittanbieter-Speicher redundant und ein lokales Backup ist nicht erforderlich. Beachten Sie jedoch, dass ein ShareFile-Benutzer, der eine Datei löscht, die Datei für einen kurzen Zeitraum aus dem Papierkorb wiederherstellen kann. Eine Datei kann nach 45 Tagen nicht aus dem ShareFile-Papierkorb wiederhergestellt werden. Nach der Wiederherstellungsphase wird die Datei aus der Zone und damit aus dem redundanten Speicher eines Drittanbieters entfernt. Wenn diese Wiederherstellungszeit nicht ausreicht, sollten Sie eine der folgenden Lösungen in Betracht ziehen:
  - **Um zu verhindern, dass der StorageZone Controller File Cleanup Service die eigentliche Datei von Ihrem lokalen Speicherort löscht, ändern Sie den Wert der Einstellung Zeitraum in.**`C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\SCFileCleanSvc\\FileDeleteService.exe.config` Weitere Informationen finden Sie unter Speicher-Cache-Operationen anpassen. Beachten Sie, dass eine Erhöhung der Aufbewahrungszeit auch den Speicherbedarf von Drittanbietern erhöht.
  - Erstellen Sie alle sieben Tage ein lokales Backup Ihrer StorageZone-Dateien und legen Sie die entsprechende Aufbewahrungsrichtlinie für die Backups fest.
- Lokaler**Speicher** —**Wenn Sie einen on-premises** verwalteten Share für privaten Datenspeicher verwenden, sind Sie dafür verantwortlich, die lokalen Dateispeicher- und Registrierungseinträge Ihres lokalen Speicherzonen-Controllers zu sichern. ShareFile archiviert

die entsprechenden Dateimetadaten, die sich 3 Jahre lang in der ShareFile-Cloud befinden.
Wichtig: Zum Schutz vor Datenverlust ist es wichtig, dass Sie einen Snapshot Ihres StorageZones Controller-Servers erstellen,
dessen Konfigurationsichern und Ihren lokalen Dateispeicher sichern.

Nachdem Sie Ihren StorageZones Controller wie in diesem Thema beschrieben für die Dateiwiederherstellung vorbereitet haben, können Sie die ShareFile Administratorkonsole für folgende Zwecke verwenden:

- Durchsuchen Sie Ihre Speicherzonen nach ShareFile-Datensätzen für ein bestimmtes Datum und eine bestimmte Uhrzeit und markieren Sie dann alle Dateien und Ordner, die Sie wiederherstellen möchten. ShareFile fügt die markierten Elemente einer Wiederherstellungswarteschlange hinzu. Anschließend führen Sie ein Wiederherstellungsskript aus, um die Dateien aus Ihrem Backup am persistenten Speicherort wiederherzustellen.

  Weitere Informationen finden Sie unter Wiederherstellen von Dateien und Ordnern aus Ihrem ShareFile-Datenbackup.

- Stimmen Sie die in der ShareFile-Cloud gespeicherten Metadaten mit Ihrem on-premises Speicher ab, wenn Sie Daten aus Ihrem on-premises Speicher nicht wiederherstellen können. Die ShareFile-Abgleichfunktion entfernt die Metadaten für Dateien, die sich an einem bestimmten Datum und zu einer bestimmten Uhrzeit nicht mehr in einer Speicherzone befinden, dauerhaft aus der ShareFile-Cloud.

  Weitere Informationen finden Sie unter Abgleichen der ShareFile-Cloud mit einer Speicherzone

Voraussetzungen

- Eine dedizierte physische oder virtuelle Maschine mit 2 CPUs und 4 GB RAM
- Windows Server 2012 R2 (Rechenzentrum, Standard oder Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows PowerShell (32-Bit- und 64-Bit-Versionen) muss.NET 4-Runtime-Assemblys unterstützen. Weitere Informationen finden Sie unter “PowerShell-Skripts und -Befehle”in den Systemanforderungen für den StorageZones Controller.
- PsExec.exe —Mit PsExec können Sie PowerShell mithilfe des Netzwerkdienstkontos starten. Sie können PsExec auch verwenden, um Wiederherstellungsaufgaben zu planen. Laden Sie PsExec.exe von https://docs.microsoft.com/en-us/sysinternals/downloads/psexec herunter und folgen Sie die Installationsanweisungen auf dieser Seite.

Zusammenfassung der für die Notfallwiederherstellung verwendeten Dateien

Die folgenden Dateien, die sich in C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery befinden, werden für die Notfallwiederherstellung verwendet.

Dateiname	Beschreibung
DoRecovery.ps1	PowerShell-Skript, das vom Windows Task Scheduler ausgeführt wird, um den Wiederherstellungsprozess abzuwickeln. In dieser Datei werden die Dateisicherungs- und Speicherorte gespeichert.
Recovery.psm1	PowerShell-Modul, das die Operationen in der Wiederherstellungswarteschlange abwickelt.
recovery.log	Protokolldatei, die die Ausgabe eines Wiederherstellungsprozesses speichert.
recoveryerror.log	Protokolldatei, die die Fehler im Wiederherstellungsprozess speichert.
LitJson.dll	Eine .Net-Bibliothek für Konvertierungen von und in JSON-Zeichenketten (JavaScript Object Notation).

Um den Backup-Ordner einzurichten

Erstellen Sie auf dem Backup-Server den Ordner, in dem Sie den Ordner persistentstorage sichern möchten.

Die Speicherzonen für die Backup von ShareFile-Datendateien sollten dem gleichen Layout folgen wie der persistente Speicher des StorageZones Controllers.

Wenn Ihr Backup-Speicherort nicht dem gleichen Layout wie der persistente Storage des StorageZones Controllers folgt, müssen Sie während des Wiederherstellungsprozesses einen zusätzlichen Schritt ausführen, um Dateien vom Backup-Speicherort an den Speicherort zu kopieren, den Sie im Recovery PowerShell-Skript angegeben haben.

Speicherlayout

Backuplayout

```
\\\PrimaryStorageIP
  \StorageLocation
   \persistentstorage
    \sf-us-1
```



```
5       \a024f83e-b147-437e-9f28-e7d03634af42
6        \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
7         \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
8          \fi47cd7e_64c4_47be_beb7_1207c93c1270
9
10 \\\BackupStorageIP
11  \BackupLocation
12   \persistentstorage
13    \sf-us-1
14     \a024f83e-b147-437e-9f28-e7d03634af42
15      \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
16       \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
17        \fi47cd7e_64c4_47be_beb7_1207c93c1270
```

> **Wichtig:**
>
> Die ShareFile-Wiederherstellungsfunktion erstellt nicht automatisch ein Backup Ihres persistenten Speicherorts. **Sie sind dafür verantwortlich, ein Backup-Hilfsprogramm auszuwählen und es alle 1 bis 7 Tage auszuführen.**

So erstellen Sie eine Disaster Recovery-Warteschlange

Diese einmalige Einrichtung ist erforderlich. Die folgenden Befehlsbeispiele verwenden den Standard-Installationsordner für den StorageZones Controller.

1. Führen Sie PowerShell auf dem StorageZones Controller als Administrator aus.
2. Das in diesem Verfahren verwendete PowerShell-Skript ist nicht signiert, sodass Sie möglicherweise Ihre PowerShell-Ausführungsrichtlinie ändern müssen.

   a) Stellen Sie fest, ob Ihre PowerShell-Ausführungsrichtlinie es Ihnen ermöglicht, lokale, unsignierte Skripts auszuführen: PS C:\ >Get-ExecutionPolicy

      Mit einer Richtlinie von RemoteSigned, Unrestricted oder Bypass können Sie beispielsweise unsignierte Skripte ausführen.

   b) Um Ihre PowerShell-Ausführungsrichtlinie zu ändern: PS C:\ >Set-ExecutionPolicy RemoteSigned

3. Um zu überprüfen, ob PowerShell die richtige CLRVersion hat, geben Sie Folgendes ein:

   $psversiontable

   Der Wert für CLRVersion muss 4.0 oder höher sein, damit PowerShell .NET-Assemblys in Skripts laden kann. Ist dies nicht der Fall, ändern Sie es sowohl für die 32-Bit- als auch für die 64-Bit-Versionen von Windows PowerShell wie folgt:

   a) Führen Sie NotePad als Administrator aus.

b) Erstellen Sie eine Datei mit dem folgenden Inhalt.

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

c) Wählen Sie “Datei”> “Speichern unter”, geben Sie der Datei den Namen powershell.exe.config und speichern Sie sie an den folgenden Speicherorten:

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

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

d) Schließen Sie das PowerShell-Fenster, öffnen Sie ein neues als Administrator und geben Sie $psversiontable ein, um zu überprüfen, ob die CLRVersion korrekt ist.

4. Schließen Sie das PowerShell-Fenster und starten Sie PowerShell mit PsExec.exe wie folgt:

   a) Öffnen Sie ein Befehlszeilenfenster als Administrator.

   b) Navigieren Sie zum Speicherort von PsExec.exe und geben Sie Folgendes ein:

   PsExec.exe -i -u “NT AUTHORITY\NetworkService”C:\Windows\SysWOW64\WindowsPowerShell\v1.0\p

   c) Klicken Sie auf Zustimmen, um die Lizenzvereinbarung von PsExec.exe zu akzeptieren.

5. Navigieren Sie zum Ordner Disaster Recovery Tools im StorageZones Controller-Installationsordner:

   cd ‘C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery’

6. Importieren Sie das Modul Recovery.psm1:

   Import-Module .\Recovery.psm1

7. Um die Wiederherstellungswarteschlange zu erstellen, geben Sie Folgendes ein: New-SCQueue -name recovery -operation recovery

   Die Ausgabe dieses Befehls enthält den Namen der erstellten Warteschlange. Beispiel: Die Warteschlange 92736b5d-1cff-4760-92c8-d8b04dc92cb2 wurde erstellt

   Um den neuen Ordner anzuzeigen, öffnen Sie einen Dateibrowser und navigieren Sie zu:

   \\server\(*Your* Primary Storage Location)\Queue. Sie sehen den Queue-Ordner, z. B. 92736b5d-1cff-4760-92c8-d8b04dc92cb2.

8. Passen Sie das PowerShell-Skript für die Wiederherstellung an Ihren Standort an, wie im nächsten Abschnitt beschrieben.

So passen Sie das PowerShell-Skript für die Wiederherstellung an Ihren Standort an

Das PowerShell-Skript DoRecovery.ps1 wird vom Taskplaner ausgeführt, um den Wiederherstellungsprozess abzuwickeln. Diese Datei enthält die Dateisicherungs- und Speicherorte, die Sie für Ihre Site angeben müssen.

1. Navigieren Sie auf dem StorageZones Controller zum PowerShell-Skript für die Wiederherstellung:

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

2. Bearbeiten Sie das Skript wie folgt:

   a. Stellen Sie den Parameter $backupRoot so ein, dass er auf den UNC-Pfad Ihres Backup-Speicherorts verweist. Beispiel: $backupRoot = "\\10.10.10.11\(*Ihr*BackupLocation)\persistentstorage"

   b. Stellen Sie den Parameter $storageRoot so ein, dass er auf den UNC-Pfad Ihres persistenten Speichers Ihres StorageZones Controllers verweist. Beispiel: $storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"

Wiederherstellungsprozess testen

1. Erstellen Sie eine Testdatei und laden Sie sie nach ShareFile hoch.
2. Überprüfen Sie nach etwa einer Stunde, ob die Datei im persistenten Speicher erscheint (in dem für $backupRoot angegebenen Pfad).
3. Löschen Sie die Datei aus ShareFile: Klicken Sie im ShareFile-Administratortool auf **Papierkorb**, wählen Sie die Datei aus, und klicken Sie dann auf **Dauerhaft löschen**.
4. Löschen Sie die Datei aus dem persistenten Speicher.

   In diesem Schritt wird die Aktion neu erstellt, die ShareFile 45 Tage nach dem Löschen der Datei ausführen würde.

5. Gehen Sie im ShareFile-Administratortool zu **Admin > Speicherzonen**, klicken Sie auf die Zone und dann auf **Dateien wiederherstellen**.
6. Klicken Sie in das Textfeld **Wiederherstellungsdatum** und wählen Sie ein Datum und eine Uhrzeit vor dem Löschen der Datei und nach dem Hochladen aus.

   Die Dateiliste für die Speicherzone am angegebenen Datum und zur angegebenen Uhrzeit wird angezeigt.

7. Markieren Sie das Kontrollkästchen für die Datei.
8. Wählen Sie den Ordner aus, der die wiederhergestellten Dateien enthält, und klicken Sie dann auf **Wiederherstellen**.

Die Datei wird der Wiederherstellungswarteschlange hinzugefügt und kann wiederhergestellt werden. Wenn die Datei erfolgreich wiederhergestellt wird, ändert sich der Bildschirm, um den Ordner anzuzeigen, der jetzt die wiederhergestellte Datei enthält.

9. Um die Datei wiederherzustellen:

   a. Öffnen Sie ein Befehlszeilenfenster als Administrator.

   b. Navigieren Sie zum Speicherort von PsExec.exe und geben Sie dann Folgendes ein:

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

   c. Navigieren Sie im PowerShell-Fenster zu:

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

   d. Führen Sie das Wiederherstellungsskript aus:

   `.\DoRecovery.ps1`

   Das PowerShell-Fenster enthält die Meldung “Element wiederhergestellt”. Die Datei wird dem persistenten Speicherort hinzugefügt.

10. Laden Sie die wiederhergestellte Datei von der ShareFile-Website herunter.

Verwandte PowerShell-Befehle

Die folgenden PowerShell-Befehle unterstützen die Notfallwiederherstellung.

- **Get-RecoveryPendingFileIDs**

  Ruft die Liste der für die Wiederherstellung benötigten Datei-IDs ab. Verwenden Sie für Syntax und Parameter diesen Befehl:

  Get-Help Get-RecoveryPendingFileIDs -full

- **Set-RecoveryQueueItemsStatus**

  Legt einen Status für alle oder bestimmte Elemente in der Wiederherstellungswarteschlange fest. Dadurch wird der bestehende Wiederherstellungsstatus in der Warteschlange überschrieben. Verwenden Sie für Syntax und Parameter diesen Befehl:

  Get-Help Set-RecoveryQueueItemsStatus -full

Wiederherstellungsaufgabe erstellen und planen

Falls eine geplante Wiederherstellungsaufgabe erforderlich ist, gehen Sie wie folgt vor.

1. Starten Sie den Windows Taskplaner und klicken Sie im **Aktionsbereich** auf **Aufgabe erstellen**.
2. Auf der Registerkarte **Allgemein**:

   a. Geben Sie einen aussagekräftigen Namen für die Aufgabe ein.

   b. Klicken Sie unter **Sicherheitsoptionen**auf **Benutzer oder Gruppe ändern**und geben Sie den Benutzer an, der die Aufgabe ausführen soll, entweder Netzwerkdienst oder einen benannten Benutzer, der über Schreibberechtigungen für den Speicherort verfügt.

   c. Wählen Sie im Menü **Konfigurieren für** das Betriebssystem des Servers aus, auf dem die Aufgabe ausgeführt werden soll.
3. Um einen Trigger zu erstellen, klicken Sie auf der Registerkarte **Trigger** auf **Neu**.
4. Wählen Sie für **Mit der Aufgabe beginnen** dieOption **Nach einem Zeitplan** aus und geben Sie dann einen Zeitplan an.
5. Um eine Aktion zu erstellen, klicken Sie auf der Registerkarte **Aktionen** auf **Neu**.

   a. Wählen Sie unter **Aktion**die Option **Programm starten** und geben Sie den vollständigen Pfad zum Programm an. Beispiel: `C:\Windows\System32\cmd.exe`.

   b. Geben Sie für **Argumente hinzufügen** Folgendes ein: `/c “c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1” >> .\recovery.log 2>>.\recoveryerror.log`

   c. Geben Sie für **Start in**den Ordner Disaster Recovery im Installationsverzeichnis des StorageZones Controllers an. Beispiel: `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

Standardzeitraum des Dienstes löschen

Ab StorageZone Controller 4.0 wird der Delete Service Timer auf 45 Tage eingestellt. Der Standardzeitraum von 45 Tagen überschreibt alle vorherigen Einstellungen. Um den Standardzeitraum zu ändern, bearbeiten Sie FileDeleteService.exe.config unter C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc

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

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

Standardzeitraum für den Löschdienst nach dem Upgrade ändern

In einigen Upgrade-Szenarien wird der DeletePeriod-Wert in der Datei “FileDeleteService.exe.config” auf Null gesetzt. Wenn dieser Wert auf Null gesetzt ist, beträgt der Löschzeitraum standardmäßig

45 Tage. Dies ist die Standardanzahl von Tagen, bevor eine aus ShareFile gelöschte Datei aus dem physischen Speicher entfernt wird.

Um die DeletePeriod auf dem StorageZones Controller zu ändern, bearbeiten Sie die Datei FileDeleteService.exe.config an der folgenden Stelle: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

Nach einer Neuinstallation des StorageZones Controllers wird der Löschdienst alle 8 Stunden ausgeführt, um temporäre Dateien und Ordner zu bereinigen. Um den Timer zu ändern, bearbeiten Sie die Datei FileDeleteService.exe.config an der folgenden Stelle: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

Wiederherstellen von Dateien und Ordnern aus Ihrem ShareFile-Datenbackup

June 11, 2020

Mit der ShareFile Administratorkonsole können Sie Ihre Speicherzonen nach ShareFile Datensätzen nach einem bestimmten Datum und einer bestimmten Uhrzeit durchsuchen und alle Dateien und Ordner markieren, die Sie wiederherstellen möchten. ShareFile fügt die markierten Elemente einer Wiederherstellungswarteschlange hinzu. Anschließend können Sie das bereitgestellte Skript ausführen, um die Dateien aus einem Backup am Speicherort wiederherzustellen.

> **Wichtig:**
>
> Stellen Sie sicher, dass Sie PowerShell 4.0 für dieses Verfahren verwenden. Weitere Informationen zu PowerShell Anforderungen finden Sie in den PowerShell-Skripts und -Befehlen unter Systemanforderungen für StorageZones Controller.

Voraussetzungen

- Schließen Sie das Setup und den Test ab, wie unter beschrieben Vorbereiten des StorageZones Controller für die Dateiwiederherstellung. Das Setup enthält Anweisungen zum Erstellen eines Ordners, der die wiederhergestellten Dateien enthält.

1. Klicken Sie in der ShareFile e-Weboberfläche auf **Admin** und dann auf **Speicherzonen**.
2. Klicken Sie auf den Zonennamen, und klicken Sie dann auf Dateien **wiederherstellen**.
3. Klicken Sie in das Textfeld **Wiederherstellungsdatum**, und wählen Sie ein Datum und eine Uhrzeit aus.

Die Dateiliste für die Speicherzone mit dem angegebenen Datum und der angegebenen Uhrzeit wird angezeigt.

4. Aktivieren Sie das Kontrollkästchen für jede wiederherzustellende Datei, und klicken Sie dann auf Wiederherstellen.
5. Wählen Sie den Ordner aus, der die wiederhergestellten Dateien enthält, und klicken Sie dann auf Wiederherstellen.

   In der Ordnerliste wird ein rotierendes Symbol angezeigt, um anzuzeigen, dass die Wiederherstellung in Bearbeitung ist.
6. Wenn Ihr Backupspeicherort nicht dem gleichen Layout entspricht wie der persistente Speicher der Speicherzone, kopieren Sie die Dateien vom Backupspeicherort an den Speicherort, den Sie beim Bearbeiten von DoRecovery.ps1 angegeben haben.
7. Das PowerShell -Skript DoRecovery.ps1 ist nicht signiert, daher müssen Sie möglicherweise die PowerShell-Ausführungsrichtlinie für dieses Verfahren ändern.

   a) Stellen Sie fest, ob Sie in der PowerShell Ausführungsrichtlinie lokale, nicht signierte Skripts ausführen können. In einem PowerShell Fenster: `Get-ExecutionPolicy`

      Mit einer Richtlinie “RemoteSigned”, “Unrestricted”oder “Bypass”können Sie beispielsweise nicht signierte Skripts ausführen.

   b) So ändern Sie die PowerShell Ausführungsrichtlinie: `Set-ExecutionPolicy RemoteSigned`
8. Legen Sie den Benutzerkontext für diese PowerShell-Sitzung fest. Führen Sie in einem Befehlsfenster einen der folgenden Befehle aus.

   - Wenn Sie das Standard-Netzwerkdienstkonto verwenden:

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

   - Wenn Sie einen benannten Benutzer für den StorageZones Controller er-Anwendungspool verwenden:

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

   Ein PowerShell-Fenster wird geöffnet.
9. Wiederherstellen der Datei:

   a) Öffnen Sie ein Eingabeaufforderungsfenster als Administrator.

   b) Navigieren Sie zum Speicherort von PSExec.exe und geben Sie Folgendes ein:


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

c) Navigieren Sie im PowerShell Fenster zu:

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

d) Führen Sie das Wiederherstellungsskript aus:

`.\DoRecovery.ps1`

Das PowerShell Fenster enthält die Meldung "Element wiederhergestellt". Wiederhergestellte Dateien werden aus dem Backup in den persistenten Speicherort kopiert. Nachdem Sie die Konsole aktualisiert haben, verschwinden die rotierenden Symbole aus der ShareFile Weboberfläche für Dateien, die erfolgreich wiederhergestellt wurden.

Wenn eine Datei, die aus der ShareFile e-Webanwendung gelöscht wird, noch nicht vom StorageZones Controller Löschdienst gelöscht wurde, befindet sich die Datei noch am persistenten Speicherort. In diesem Fall erfolgt die Dateiwiederherstellung sofort, und in der ShareFile Weboberfläche wird kein rotierendes Symbol angezeigt.

Wenn Sie eine Datei nicht wiederherstellen können, lesen Sie die Hilfedatei im Ordner "Notfallwiederherstellung".

Abgleichen der ShareFile Cloud mit einer Speicherzone

October 13, 2020

Ein Problem, z. B. ein Datenträgerfehler, das Datenverlust im lokalen Speicher verursacht, führt zu einem inkonsistenten Zustand zwischen dem lokalen Speicher und den in der ShareFile-Cloud gespeicherten Metadaten. Sie können diese Unterschiede automatisch abgleichen, sodass Metadaten für Dateien, die sich nicht mehr in Ihrer Speicherzone an einem bestimmten Datum und einer bestimmten Uhrzeit befinden, dauerhaft aus der ShareFile Cloud entfernt werden.

> **Achtung:**
>
> Führen Sie einen Abgleich nur durch, wenn Sie einen unwiederbringlichen Datenverlust in Ihrem lokalen Dateispeicher haben. Eine Abgleichung löscht die Metadaten dauerhaft aus der ShareFile Cloud für alle Dateien, die nicht in Ihrem lokalen Dateispeicher zu finden sind, ab dem von Ihnen angegebenen Datum und Uhrzeit.

1. Klicken Sie auf **Admin** und dann auf **Speicherzonen**.
2. Klicken Sie auf den Zonennamen, und klicken Sie dann auf **Dateien abgleichen**.

3. Klicken Sie in das Textfeld **Datum abstimmen**, und wählen Sie ein Datum und eine Uhrzeit aus.
4. Klicken Sie auf **Abgleichen**. Ein Bestätigungsdialogfeld wird angezeigt.

Windows Server 2012 R2 Migrationshandbuch für ShareFile-Speicherzonen

November 14, 2023

> **Wichtig:**
>
> Microsoft stellt den Support für Windows Server 2012R2 am 10. Oktober 2023 ein. Es ist wichtig, dass Sie Ihren Server vor Ablauf des Support-Datums auf eine neuere Version migrieren.

Dieser Artikel enthält Anleitungen zur Migration Ihres ShareFile Storage Zone-Servers von Windows Server 2012R2 auf eine neuere Version.

Um zu einer neueren Version von Windows Server zu migrieren, müssen Sie dem neuen Server einen sekundären Speicherzonencontroller hinzufügen und ihn dann zum primären Controller heraufstufen.

Systemanforderungen

Der Storage Zones Controller Server unterstützt die folgenden Versionen:

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

Anweisungen

> **Hinweis:**
>
> Die folgenden Schritte behandeln **NICHT** die Migration des ShareFile-Datenrepositorys. Wenn Sie das ShareFile-Datenrepository auf demselben Server wie den Speicherzonencontroller haben, den Sie migrieren möchten, oder wenn Sie ein Speicherzonen-Datenrepository auf einem Dateiserver unter Windows Server 2012R2 für die Migration haben, finden Sie weitere Informationen unter Dateien auf eine neue Netzwerkfreigabe übertragen .

Schritt 1 —Vorbereiten des neuen Servers für den ShareFile Storage Zone Controller

Bereiten Sie den neuen Server mithilfe der unter Vorbereiten des Servers für ShareFile-Datenbeschriebenen Schritte vor.

Schritt 2 —Installieren Sie den Storage Zone Controller auf dem neuen Server und fügen Sie ihn als sekundären Server hinzu

Nachdem Sie den neuen Server für ShareFile vorbereitet haben, müssen Sie ihn als sekundären Server zur Speicherzone hinzufügen. Weitere Informationen finden Sie unter Verbinden eines sekundären StorageZones Controllers mit einer Storagezone .

Schritt 3 —Den neuen Server zum Primärserver heraufstufen, den alten Server zum Sekundärserver herabstufen

Nachdem Sie den neuen Server als sekundären Server hinzugefügt haben, besteht der nächste Schritt darin, ihn zum primären Server hochzustufen. Der ältere Server muss ebenfalls auf einen sekundären Server herabgestuft werden. Weitere Informationen zu diesem Schritt finden Sie unter StorageZones Controller herabstufen undheraufstufen.

> **Hinweis:**
>
> ShareFile empfiehlt, die Funktionalität des neuen Speicherzonenservers eigenständig zu testen, ohne den älteren Server als sekundären Server zu verwenden. Sie können dies tun, indem Sie den älteren Server vorübergehend deaktivieren. Weitere Informationen finden Sie unter So deaktivieren Sie einen Speicherzonencontroller

Schritt 4 (optional) —Zusätzliche Sekundärserver hinzufügen

Falls erforderlich, kehren Sie für jeden weiteren sekundären Server zu Schritt 2 —Installieren Sie den Storage Zone Controller auf dem neuen Server zurück und fügen Sie ihn als sekundärenServer hinzu.

Schritt 5 (optional) —Mitglieder der NetScaler-Dienstgruppe aktualisieren

Wenn Sie über einen NetScaler verfügen, stellen Sie sicher, dass die neuen Speicherzonenserver der ShareFile-Dienstgruppe hinzugefügt werden. Weitere Informationen finden Sie unter Hinzufügen von Mitgliedern zu einer Dienstgruppe mithilfe des Konfigurationsdienstprogramms .

Schritt 6 —Löschen Sie den alten Storage Zone Controller-Server aus dem ShareFile Admin Portal

Sobald die Storage Zone-Server erfolgreich migriert wurden, können die älteren Server aus dem ShareFile Admin Portal gelöscht werden. Weitere Informationen finden Sie unter So löschen Sie einen StorageZones Controller .

Konfigurieren von Antivirenscans hochgeladener Dateien

June 28, 2022

> **Wichtig:**
>
> Aufgrund von Aktualisierungen des Anwendungscodes in StorageZones 4.2 müssen einige Kunden die Berechtigungsstufe, auf der das Tool ausgeführt wird, vom lokalen Administrator zum Systemnetzwerkdienst aktualisieren. Wenn die Berechtigungen nicht aktualisiert werden, können Antiviren-Scans nicht gestartet werden.

Anforderungen/Zusammenfassung

- Benutzer, der StorageZones Controller 4.2 oder höher verwendet
- SFAntivirus muss als Netzwerkdienst mit PsExec ausgeführt werden
- Speicherort der Protokolldatei aktualisieren

Führen Sie SfAntivirus als Netzwerkdienst mit PsExecaus:

Clients, die auf SZ 4.2 oder höher mit vorhandenen geplanten Aufgaben, die mit SFAntivirus verknüpft sind, aktualisieren, müssen die Benutzerebene, auf der das Tool ausgeführt wird, vom lokalen Administrator zum Systemnetzwerkdienst ändern.

Um Netzwerkdienstrechte zu erhalten, verwenden Sie PsExec, um PowerShell (x86) im gleichen Benutzerkontext wie den StorageZones Controller zu starten und Netzwerkdienstrechte mit dem folgenden Befehl zu erhalten:

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

Speicherort der Protokolldatei aktualisieren

Administratoren müssen auch den Speicherort der Protokolldatei ändern, indem sie den Eintrag log4net.config bearbeiten, wenn sie sich in einem Verzeichnis außerhalb des standardmäßigen

SZC-Protokollverzeichnisses anmelden, indem sie die folgende Zeile ändern:

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

Die Installation des StorageZones Controllers umfasst mehrere Dateien, die Virenscans unterstützen. Die Dateien werden standardmäßig in C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus. installiert.

Nachdem Sie die Konfigurationsdatei angepasst und den Windows-Taskplaner verwendet haben, um die Scans zu planen, wie in den folgenden Schritten beschrieben, veranlasst jede Datei-Upload-Anforderung, dass der Storage Zones Controller die Datei für einen Antivirus-Scan in die Warteschlange stellt. Wenn Probleme für eine gescannte Datei gemeldet werden, enthält die Ordneransicht ein Warnsymbol für die Datei. Wenn ein Benutzer versucht, die Datei herunterzuladen, wird eine Warnmeldung angezeigt.

Ab StorageZones Controller 4.0 kann der Speicherort der Antiviren-Protokolldatei konfiguriert werden. Um den Speicherort des Protokolls zu ändern, bearbeiten Sie die Datei Sfantivirus.exe.config unter C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus.

Der Antivirus-Scan entfernt die Datei nicht.

Die Verwendung des ICAP-Protokolls mit Antiviren-Scan-Plattformen, die nach dem RFC-Standard für ICAP codiert wurden, wird auf StorageZones Controller 4.2 oder höher unterstützt. Informationen zur Konfiguration eines ICAP AV finden Sie weiter unten in diesem Artikel.

> **Hinweis:**
>
> Nach der Konfiguration des Virenschutzes in Ihrer Zone werden alle neu hochgeladenen Elemente gescannt. Die Antivirus-Konfiguration ist nicht rückwirkend. Durch die Konfiguration werden keine Dateien und Elemente gescannt, die bereits in der Zone vorhanden sind.

So bereiten Sie die Konfiguration für Ihren Standort vor

1. So führen Sie Virenscans auf einem anderen Server als dem StorageZones Controller aus:
   a) Kopieren Sie den Ordner C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus auf den anderen Server.
   b) Öffnen Sie auf dem StorageZones Controller C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRe und setzen Sie QueueSDKRestricted auf 0: `<add key="QueueSDKRestricted" value="0"/>`
2. Bearbeiten Sie auf dem Server, auf dem Sie Virenscans ausführen, SFAntiVirus.exe.config mit den Werten für Ihre StorageZones Controller-Konfiguration:
   a) Für CommandFile: Geben Sie den vollständigen Pfad zur Antivirensoftware an. Diese Software muss sich auf demselben Server wie der ShareFile-Antivirus-Ordner befinden.

b) Für CommandOptions und Rückgabecodes: Die in der Konfigurationsdatei bereitgestellten Befehlszeileneinstellungen sind ein Beispiel. Stellen Sie die entsprechenden Einstellungen für Ihre Antivirensoftware und Umgebung bereit.

c) Für scanFileTimeout: Das Scannen größerer Dateien kann länger dauern. Passen Sie diese Einstellung an die in Ihrem Speicher erwarteten Dateigrößen an. **Andernfalls könnte dies das Risiko erhöhen, dass eine große Datei nicht gescannt wird.**

3. Führen Sie in einem Befehlszeilenfenster den folgenden Befehl aus, um Virenscans einzurichten:
   `SFAntiVirus.exe -register SFusername SFpassword`

Verwenden Sie ICAP für AV-Scans anstelle von Befehlszeilen-Tools

StorageZones Controller 5.3 und höher unterstützt die Verwendung des ICAP-Protokolls mit Antiviren-Scan-Plattformen, die nach dem RFC-Standard für ICAP codiert wurden. Kunden können weiterhin die CLI-Methode verwenden, wenn sie möchten. Diese Funktion wird für Mandantenzonen ab Storage Zones Controller 5.0.1 und höher unterstützt.

Um einen ICAP AV-Scanner auf Ihrem StorageZone Controller zu aktivieren, navigieren Sie zur StorageZones Controller-Konfigurationsseite.

Aktivieren Sie das Kontrollkästchen **Anti-Virus-Integration aktivieren** und geben Sie die Adresse Ihres Antivirus-Servers in das Feld **ICAP RESPMOD-URL** ein. Dies ist die URL des ICAP-Dienstes zur Änderung von Antworten: `ICAP://SERVER/RESPMOD`.

Klicken Sie auf **Konnektivität testen**, um Ihre Einstellung zu bestätigen.

So erstellen und planen Sie eine Aufgabe für Virenscans

> **Hinweis:**
>
> Das Erstellen von geplanten Tasks für Virenscans ist nur erforderlich, wenn Befehlszeilen-Tools verwendet werden. Dies ist bei der Verwendung von ICAP nicht erforderlich.

1. Starten Sie den Windows-Taskplaner, und klicken Sie im **Aktionsbereich** auf **Task erstellen**.
2. Auf der Registerkarte **Allgemein**:

   a) Geben Sie einen aussagekräftigen Namen für die Aufgabe an.

   b) Klicken Sie unter **Sicherheitsoptionen** auf **Benutzer oder Gruppe ändern**, und geben Sie einen Windows-Benutzer an, der die Aufgabe ausführen soll. Der Benutzer muss volle Zugriffsberechtigung für den Speicherort haben.

   c) Wählen Sie **Ausführen aus, ob der Benutzer angemeldet ist oder nicht**. Lassen **Sie das Kontrollkästchen Kennwort nicht speichern** deaktiviert.

   d) Wählen Sie **Mit den höchsten Rechten ausführen**aus.

   e) Wählen Sie **im Menü Konfigurieren für**das Betriebssystem des Servers aus, auf dem die Aufgabe ausgeführt werden soll.

3. So erstellen Sie einen Trigger: Klicken Sie auf der Registerkarte **Auslöser** auf **Neu**. Wählen Sie dann für **Aufgabe beginnen die**Option Nach **Zeitplan** aus, und geben Sie einen Zeitplan an.

4. So erstellen Sie eine Aktion: Klicken Sie auf der Registerkarte **Aktionen** auf **Neu**.

   a) Wählen Sie für **Aktion**die Option Programm **starten** und geben Sie den vollständigen Pfad zum Programm an. Beispiel:

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

   b) Geben Sie für Start in den Speicherort von SFAntiVirus.exe an: `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`

5. Wählen Sie auf der Registerkarte **Einstellungen** für **Wenn die Aufgabe bereits ausgeführt wird**, die folgende Regel zutrifft, die Option **Keine neue Instanz starten**aus.

Integration der AV-Befehlszeile in den Suchdienst

Voraussetzungen

- Stellen Sie vor der Installation oder dem Upgrade von StorageZones Controller 5.2 sicher, dass Sie das vorhandene Befehlszeilen-AV anhalten oder löschen, wenn es als geplante Aufgabe oder als Cron ausgeführt wird.
- Installieren Sie .NET 4.6.2 (oder höher) auf einem Hostcomputer.

Der Scan-Service im on-premises StorageZones Controller bietet Unterstützung für die Verwendung eines Befehlszeilen-AV-Tools wie den AV-Scan der Symantec-Befehlszeile. Darüber hinaus bietet der Suchdienst Scans mit ICAP-unterstützten Antivirenprodukten.

Um diese Funktion zu aktivieren, fügen Sie den folgenden Konfigurationsschlüssel und Wert in der Datei AntiVirus/OnPrem/AVScanService/AVScanService/appSettings.config hinzu

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

Befehlszeilentoolspezifische Konfiguration

Das Upgrade oder die Neuinstallation von Storage Zones Controller 5.2 beinhaltet eine neue Konfigurationsdatei:

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

Diese Datei verarbeitet die notwendigen Einstellungen für die AV-Befehlszeile.

Die Konfigurationsschlüsselwerte werden unten erklärt, wobei Beispielwerte enthalten sind.

- Setzen Sie diesen Punkt auf Ihre Befehlszeilen-App.

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

- Sehen Sie in der Dokumentation der Befehlszeilen-App nach, welche Optionen oder Switches sie unterstützt, und fügen Sie sie dann an dieser Stelle hinzu.

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

- Schließen Sie die Ausgabewerte ein, die auf einen sauberen Scan hinweisen

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

- Schließt Ausgabewerte ein, die auf infizierte

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

- Schließt Ausgabewerte ein, die darauf hinweisen, dass

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

Hinweise zur Durchsetzung der maximalen Dateigröße, ohne Erweiterungen

Vor Version 5.2 konnten Sie den Ausschluss von Erweiterungen oder die Durchsetzung der maximalen Dateigröße auf dem Befehlszeilen-AV nicht erzwingen. Sie konnten dies nur mit dem ICAP-Scandienst tun. Mit Version 5.2 gelten dieselben Einstellungen, die für den ICAP-Scandienst in Bezug auf ausgeschlossene Erweiterungen und maximale Dateigröße in Byte galten, für den AV-Befehlszeilendienst.

Diese Einstellungen wurden benannt als:

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

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

Eine neue Installation von Storage Zones Controller 5.2 benennt diese Einstellungen in die folgenden um. Die umbenannten Einstellungen spiegeln die Tatsache wider, dass sie sowohl für ICAP-basierte AV als auch für die Befehlszeilen-AV gelten.

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

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


Bei einem Upgrade werden diese Einstellungen nicht umbenannt. Obwohl manuelle Umbenennungen funktionieren, würden dieselben Einstellungen zusätzlich zu ICAP auch für die AV-Befehlszeile funktionieren.

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

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

ShareFile-Daten migrieren

August 1, 2023

Es gibt mehrere Möglichkeiten, ShareFile-Daten von einer on-premises Zone in eine andere zu migrieren.

- Migrieren über Webportal oder Benutzerverwaltungstool
- Migration über PowerShell Script
- Migration über das ZoneFix Tool

Voraussetzungen

- Stellen Sie sicher, dass die Quellzone von der Zielzone aus erreichbar ist, und heben Sie die ausgehenden Verbindungen zum Quellspeichercenter auf.
- Um die Verbindung zwischen Zonen zu testen, greifen Sie auf die externe Adresse der Quellzone zu, indem Sie in einem Browser in der Zielzone zu ihr navigieren. Wenn die Verbindung erfolgreich ist, wird das ShareFile-Logo angezeigt.

Migrieren über Webportal oder Benutzerverwaltungstool

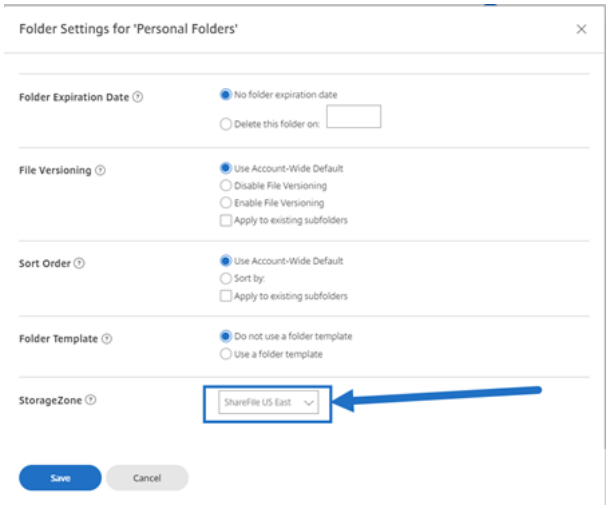
In der ShareFile-Webanwendung können Sie die Migration von Daten zwischen Zonen für einen einzelnen Benutzer oder für einen bestimmten Ordner initiieren.

> **Wichtig:**
>
> Durch das Speichern der folgenden Änderungen wird sofort ein asynchroner Migrationsvorgang ausgelöst, bei dem vorhandene Dateien in die neue Zone hochgeladen werden. Neue Dateien, die während dieses Migrationszeitraums in den Ordner hochgeladen wurden, werden in die neue Zone verschoben.

Daten für einen bestimmten Benutzer migrieren —Navigieren Sie zu **Personen**, und suchen Sie dann den **Mitarbeiterbenutzer** . Klicken Sie auf den Benutzer, um seine Profilseite aufzurufen.

Wählen Sie unter **Speicherort**eine neue Zone aus (falls bereits eine installiert und konfiguriert wurde).

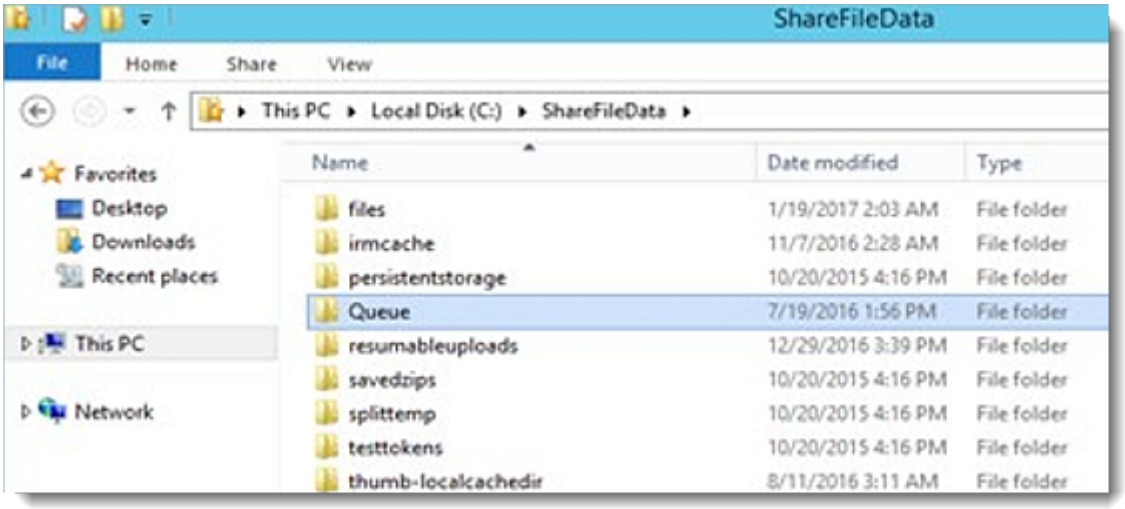
Daten für einen bestimmten Ordner migrieren —Navigieren Sie zum Ordner und rufen Sie das Menü **Weitere Optionen** rechts neben dem Ordnernamen auf. Klicken Sie auf **Erweiterte Ordnereinstellungen**. Wählen Sie über das Menü eine neue Zone aus.



Migrationsprozess

Zunächst erstellen Dateien, die für die Migration in die Warteschlange gestellt werden, eine Platzhalterdatei in einem **Warteschlangenordner** innerhalb des **Speicherorts** der ursprünglichen Zone.

Sobald die Platzhalterdatei erfolgreich verarbeitet wurde, wird die migrierte Datei aus `persistentstorage` der ursprünglichen Zone gelöscht und zu `persistentstorage` der neuen Zone hinzugefügt.



Migrieren Sie über PowerShell

Mit dem ShareFile PowerShell SDK können Benutzer große Ordnerstrukturen von ihrem ursprünglichen Zonenspeicherort herunterladen und diese Ordner in eine neue Zone hochladen.

Anforderungen —PowerShell 4+ und .NET 4.x+ sind erforderlich, um das SDK auszuführen und zu installieren. PowerShell 5.x kann hier als Teil des Windows Management Framework 5.1 heruntergeladen werden.

Migration über das Zonenfix-Tool

Das Zonenfix-Tool ist ein Befehlszeilentool. Das von Storage Zones-Entwicklern geschriebene Tool nutzt die ShareFile-API, um Ordner-IDs für die Migration in eine bestimmte Zone als Ziel zu verwenden.

Für eine optimale Leistung wird diese Methode für Ordner mit einer Größe von weniger als 2 GB empfohlen.

Connector-Favoriten

February 11, 2022

Ab StorageZone Controller 5.0 können Benutzer Connector-Ordner unter **Netzwerkfreigaben**, **SharePoint**und **Documentum Connectors** innerhalb der ShareFile-WebApp als Favoriten festlegen. Einzelheiten finden Sie in diesem Citrix Support Knowledge Center-Artikel.

Das Hinzufügen eines Connector-Ordners zu Ihren Favoriten wird in ShareFile Mobile unterstützt.

Verwalten von Speicherzonen für ShareFile-Daten

November 14, 2023

Sie können Speicherzonen für ShareFile-Daten mit oder anstelle der von ShareFile verwalteten Cloud verwenden.

> **Hinweis:**
>
> Wenn Sie einen primären Speicherzonencontroller löschen, stufen Sie ihn herab, bevor Sie fortfahren. Weitere Informationen finden Sie unter StorageZone-Controller herabstufen und heraufstufen.

Verschieben von Home-Ordnern und Dateiboxen zwischen Zonen

Gehen Sie wie folgt vor, um Basisordner und Dateiboxen zwischen Zonen zu verschieben. Verwenden Sie alternativ das ShareFile User Management Tool, um Benutzer zwischen Zonen zu migrieren.

1. Klicken Sie auf **Home** und navigieren Sie dann zum Ordner.
2. Klicken Sie im rechten Navigationsbereich auf **Ordneroptionen bearbeiten**.
3. Wählen Sie im Menü “Speicherzone”eine Zone aus, und klicken Sie dann auf **Speichern**.

Erstellen eines Ordners in einer Speicherzone

1. Klicken Sie auf **Home** und dann auf **Ordner**.
2. Klicken Sie auf der Registerkarte **Ordner** auf **Ordner hinzufügen**.
3. Geben Sie die Ordnerinformationen an. Wählen Sie unter **Storage Site** die Speicherzone aus, in der dieser Ordner und sein Inhalt gespeichert werden sollen.
4. Klicken Sie auf **Ordner erstellen**.
5. Konfigurieren Sie den Ordner wie gewohnt. Wenn Sie einen Ordner erstellen, können Sie wählen, ob Sie den von ShareFile verwalteten Cloudspeicher oder Ihre lokale Speicherzone verwenden möchten.

Umbenennen oder Löschen einer Speicherzone

> **Wichtig:**
>
> Bevor Sie eine Speicherzone löschen, sichern Sie sie. Durch das Löschen einer Zone werden alle Dateien und Ordner in dieser Zone gelöscht, und Sie können den Vorgang nicht rückgängig machen.

1. Klicken Sie auf **Admin** und dann auf **Storage zones**.

2. Klicken Sie auf den Zonennamen.
    - So benennen Sie die Zone um: Klicken Sie auf **Zone bearbeiten**, geben Sie einen neuen Namen ein, und klicken Sie dann auf **Änderungen speichern**.
    - So löschen Sie die Zone: Klicken Sie auf den Zonennamen und dann auf **Zone löschen**.

Einschränkungen

In den folgenden Fällen können Speicherzonencontroller nicht umbenannt/gelöscht werden:

- **ShareFile-Datenmigration ist im Gange** —Schließen Sie die Datenmigration ab, bevor Sie versuchen, die Speicherzone zu löschen.
- **ShareFile-Daten sind in der Zone vorhanden** —Migrieren oder löschen Sie alle vorhandenen Daten, bevor Sie versuchen, die Speicherzone zu löschen.

Speicher-Cache-Vorgänge anpassen

ShareFile-Benutzeranfragen werden mit dem StorageZones Controller verwaltet. Dazu gehören: Datei-Uploads, Downloads und Löschungen. Der StorageZones Controller kommuniziert dann mit dem verbundenen Speicher. Wenn der verbundene Speicher beispielsweise ein unterstütztes Speichersystem eines Drittanbieters ist und ein ShareFile-Benutzer eine Datei hochlädt, sendet der ShareFile-Client die Datei an den persistenten Speichercache. Der StorageZone Controller lädt die Datei dann auf das Speichersystem eines Drittanbieters hoch.

Der StorageZone Controller verwaltet den persistenten Speichercache mithilfe der konfigurierbaren Einstellungen in `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`. Die Einstellungen, die für ein unterstütztes Speichersystem eines Drittanbieters spezifisch sind, werden in dieser Diskussion beschrieben.

Für hochgeladene Dateien:

- Der StorageZone Controller legt hochgeladene Dateien in einen persistenten Speichercache (den PersistentStorage-Ordner).
- Die folgenden Einstellungen steuern das Timing von Löschdienstvorgängen:
    - `MinDeletionAge` gibt die Mindestzeitspanne zwischen dem letzten Zugriff auf eine Datei und dem Zeitpunkt an, an dem sie gelöscht werden kann. Standardeinstellung ist 1 Tag. Die Mindesteinstellung beträgt 8 Stunden.
    - `OffPeakTimeOfDayStart` und `OffPeakTimeOfDayEnd` geben die Start- und Endzeiten für das Löschen von Dateien an. Standardmäßig 2 Uhr morgens und 4 Uhr morgens.

  - `ProducerTimerInterval` und `DeleteTimerInterval` steuern die Häufigkeit der Löschvorgänge. Bitte wenden Sie sich an den Support, falls die Standardwerte (1 Tag) für Ihre Website nicht geeignet sind.

- Die Löschdienste verwalten auch Ordner, die temporäre Elemente wie Verschlüsselungsschlüssel und Dateien in der Warteschlange enthalten. Der Löschdienst entfernt diese Elemente 24 Stunden nach ihrer Erstellung.
- Nur für unterstützte Speichersysteme von Drittanbietern:
  - Der Löschdienst bestimmt, ob eine Datei im Speicher-Cache einen entsprechenden Blob im unterstützten Drittanbieter-Speicher hat.
  - Standardmäßig ermittelt der Löschdienst alle 10 Sekunden (`CheckSizeThreasholdTimer`), ob der Speichercache einen Datenträgerschwellenwert von 10 GB (`DiskSpaceDropoutThreshol`) überschritten hat. Wenn der Schwellenwert überschritten wird, entfernt der Löschdienst Dateien, auf die in der letzten Stunde nicht zugegriffen wurde (`CacheCleanupFileThreasholdPe`). Der Löschdienst wird als Ergebnis der normalen Planung ausgeführt (und nicht, weil die Datenträgergröße den Schwellenwert erreicht hat). Der Dienst löscht Dateien, auf die in den letzten 24 Stunden nicht zugegriffen wurde (`CacheCleanupFileThresholdPeriodNormal`), wenn sich der Blob im unterstützten Speicher eines Drittanbieters befindet. Wenn sich das Blob nicht im Speicher des Drittanbieters befindet, bleibt die Datei im Speichercache.

Für heruntergeladene Dateien:

- Wenn StorageZone Controller eine Download-Anforderung erhält, lädt er die Datei aus dem persistenten Speichercache herunter, falls die Datei vorhanden ist. Wenn sich die Datei nicht in diesem Cache befindet, lädt der Controller die Datei vom Speichersystem des Drittanbieters in den persistenten Speichercache herunter. Der Löschdienst entfernt Dateien, auf die in den letzten 24 Stunden nicht zugegriffen wurde (CacheCleanupFileThresholdPeriodNormal).

Für gelöschte Dateien:

- Der Löschdienst ruft aus der ShareFile-Anwendung eine Liste von Dateien ab, die vor 45 Tagen (Zeitraum) gelöscht wurden.
- Der Löschdienst entfernt dann die entsprechenden Dateien aus dem Speicherort oder die entsprechenden Objekte aus dem Speicher des Drittanbieters.

Standardzeitraum für Dienst löschen

Der Timer für den Löschdienst ist auf 45 Tage eingestellt. Der Standardzeitraum von 45 Tagen überschreibt alle vorherigen Einstellungen.

> **Hinweis:**
>
> Wenn der Löschzeitraum auf weniger als 45 Tage konfiguriert ist, wenden Sie sich bitte an den Support, um die Anzahl der Tage zu reduzieren, an denen Artikel im **Papierkorb** angezeigt werden, sodass beide Zeitrahmen gleich sind.

1. Um den Standardzeitraum zu ändern, bearbeiten Sie FileDeleteService.exe.config unter `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`
   - `<!--No. of days to keep data blob in active storage after deletion-->`
   - `<add key="Period"value="45"/>`

Erstellen und Verwalten von StorageZone Connector

April 20, 2021

StorageZone Connector bieten Zugriff auf Dokumente und Ordner in:

- SharePoint-Websites, Websitesammlungen und Dokumentbibliotheken
- Netzwerkdateifreigaben
- Documentum-Connector (erfordert SZC 4.1 oder höher)

Benutzer mit der Berechtigung zum Anzeigen einer verbundenen Ressource können verbundene SharePoint-Websites, SharePoint-Bibliotheken und Netzwerkdateifreigaben über die ShareFile Webschnittstelle und ShareFile-Clients durchsuchen.

Standardmäßig ist das Durchsuchen des Connectors für die ShareFile Weboberfläche deaktiviert. Wenden Sie sich an den ShareFile Support, um Connector-Browsing zu aktivieren.

Es stehen zusätzliche Einstellungen zur Verfügung, mit denen Benutzer angeben können, welcher Domänencontroller für Active Directory Lookups verwendet werden soll. Weitere Informationen finden Sie im Abschnitt “Authentifizierung”dieses Artikels. Diese Einstellung erfordert SZ 4.1 oder höher.

Connector-Systemanforderungen

StorageZone Connectors unterstützen keine gemeinsame Nutzung von Dokumenten oder Ordnersynchronisierung auf allen Geräten.

Connectors müssen einen eindeutigen Anzeigenamen haben. Benutzer werden daran gehindert, einen Connectornamen zu verwenden, der derzeit an anderer Stelle des Kontos verwendet wird.

Berechtigungen zum Erstellen von StorageZone Connector

Um Connectors zu erstellen und zu verwalten, **muss Ihr Admin- oder Mitarbeiterbenutzer über die folgenden Berechtigungen verfügen**:

- **Erstellen und Verwalten von Connectors**
- **Ordner auf Stammebene erstellen**

So erstellen Sie einen Speicherzonen-Connector für SharePoint

Voraussetzungen

- Wenn Sie Speicherzonen für ShareFile Daten verwenden, erstellen Sie die Zone, die für den Connector verwendet werden soll.

In den folgenden Schritten wird beschrieben, wie Sie einen Speicherzonen-Connector über die ShareFile Weboberfläche erstellen. ShareFile Benutzer können auch einen Connector von unterstützten Geräten erstellen, indem Sie die URL der SharePoint-Website eingeben.

1. Melden Sie sich mit der Berechtigung Connectors erstellen und verwalten bei Ihrem ShareFile e-Konto als Administrator an.
2. Navigieren Sie zu **Admin-Einstellungen > Connectors**.
3. Klicken Sie für den SharePoint-Connectortyp auf **Hinzufügen**.
4. Wenn Sie Speicherzonen für ShareFile Daten verwenden, wählen Sie eine Zone für den Connector aus.

   Die Zone für einen Connector muss sich entweder in derselben Domäne wie der SharePoint-Server befinden oder eine Vertrauensstellung damit aufweisen. Wenn Sie SharePoint-Server in mehreren Domänen haben und keine Vertrauensstellungen zwischen den Domänen konfigurieren können, erstellen Sie für jede Domäne einen StorageZones Controller.
5. Geben Sie für Website die URL einer SharePoint-Website, Websitesammlung oder Dokumentbibliothek in den folgenden Formularen an.

   - Beispielverbindung zu einer SharePoint-Website auf Stammebene: `https://sharepoint.company.com`

     Eine Verbindung zu einer Website auf Stammebene ermöglicht Benutzern den Zugriff auf alle Websites (jedoch nicht Websitesammlungen) und Dokumentbibliotheken unter der Stammebene. ShareFile blendet SharePoint-Systemordner vor Benutzern aus.
   - Beispielverbindung zu einer SharePoint-Websitesammlung: `https://sharepoint.company.com/site/SiteCollection`

Durch eine Verbindung zu einer Websitesammlung können Benutzer auf alle Unterwebsites innerhalb dieser Sammlung zugreifen.

- Beispielverbindung zu einer SharePoint 2010-Dokumentbibliothek:
  - `https://mycompany.com/sharepoint/`
  - `https://mycompany.com/sharepoint/sales-team/Shared Documents/`
  - `https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx`
- Beispielverbindung zu einer SharePoint 2013-Dokumentbibliothek:

  Die standardmäßige SharePoint 2013-URL (wenn Minimale Download-Strategie aktiviert ist) hat das folgende Format: `https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`.
- Beispielverbindung, die zum NetBIOS-Namen eines authentifizierten Benutzers umleitet:

  Verwenden Sie die Variable %UserDomain%, um den Anmeldenamen des authentifizierten Benutzers durch den NetBIOS-Namen dieses Benutzers zu ersetzen. Die neue Variable ermöglicht es Ihnen, einen Connector auf Site-Ebene zu einer URL wie `https://example.com/%UserDomain%\\_%UserName%/Documents` z. B.
- Beispielverbindung beim Herstellen einer Verbindung mit "Meine Website"oder OneDrive for Business:

  Verwenden Sie die Variable %`URLusername`%, um ausgewählte Sonderzeichen bei der Verbindung mit persönlichen SharePoint-Websites automatisch aufzulösen. Diese Variable ersetzt Leerzeichen mit%20 und Punkte durch Unterstriche. Die Verwendung der %`URLusername`% Variablen erfordert SZ v3.4.1.

  Wenn die "Domäne\ Benutzername"des Benutzers "acme\ rip.van winkle"lautet, dann

  `https://sharepoint.acme.com/personal/%URLusername%`
  wird aufgelöst auf:
  `https://sharepoint.acme.com/personal/rip van%20winkle`

6. Geben Sie einen benutzerfreundlichen Namen für den Connector ein.

   Der Name wird verwendet, um die SharePoint-Website für Benutzer zu identifizieren. Der Name sollte kurz sein, damit er auf mobilen Geräten mit kleinen Bildschirmen gut angezeigt wird.

7. Klicken Sie auf **Connector hinzufügen**. Das Dialogfeld **Ordnerzugriff anzeigen/bearbeiten** wird angezeigt.

8. So machen Sie Connectors für andere sichtbar: Fügen Sie unter Ordnerzugriff anzeigen/bearbeiten Benutzer und Verteilergruppen hinzu, und klicken Sie dann auf **Änderungen speichern**.

Dieser Schritt bestimmt nur, ob ein Connector für Benutzer sichtbar ist. **StorageZone Connector erben Zugriffsberechtigungen vom SharePoint-Server.**

So aktivieren Sie SharePoint-Metadaten-Tagging

Stellen Sie beim Konfigurieren des StorageZones Controller sicher, dass SharePoint-Connectors aktiviert sind.

Metadaten-Tagging wird für mobile Clients mit SharePoint 2013 und höher unterstützt.

> **Hinweis:**
>
> `en-us` Nur für.

So erstellen Sie einen Speicherzonen-Connector für Netzwerkdateifreigaben

Voraussetzungen

- Wenn Sie Speicherzonen für ShareFile Daten verwenden, erstellen Sie die Zone, die für den Connector verwendet werden soll.
- Damit Network Share Connectors mit den neuesten Versionen von Chrome, Edge und Firefox funktionieren, wenden Sie das neueste .NET-Update für Ihre Umgebung an. Weitere Informationen finden Sie unter KB-Artikel, die SameSite im .NET Framework unterstützen. Wenden Sie dies auf alle Ihre StorageZone Connectors an. Dies ist erforderlich, damit das SameSite-Attribut unter Berücksichtigung der neuesten Version der Browser für Cookies festgelegt werden kann.
- Wenn Sie Version 5.10.1 oder niedriger verwenden, fügen Sie in allen StorageZone Connectors `<httpCookies sameSite="None"requireSSL="true"/` innerhalb des `<system.web>` Tags der Datei C:\inetpub\wwwroot\Citrix\StorageCenter\cifs\Web.config hinzu. Dies ist erforderlich, damit das SameSite-Attribut unter Berücksichtigung der neuesten Version der Browser für Cookies festgelegt werden kann.

In den folgenden Schritten wird beschrieben, wie Sie einen Connector über die ShareFile Weboberfläche erstellen. ShareFile Benutzer können auch einen Connector von unterstützten Geräten erstellen, indem Sie den Pfad einer Dateifreigabe eingeben.

1. Melden Sie sich bei Ihrem ShareFile Konto als Administrator mit der Berechtigung Connectors erstellen und verwalten an.
2. Navigieren Sie zu **Admin-Einstellungen > Connectors**.
3. Klicken Sie für den Connectortyp Netzwerkfreigaben auf **Hinzufügen**.

4. Wenn Sie Speicherzonen für ShareFile Daten verwenden, wählen Sie eine Zone für den Connector aus.

   Die Zone für einen Connector muss sich entweder in derselben Domäne wie die Dateifreigabe befinden oder eine Vertrauensstellung damit aufweisen. Wenn Sie Dateifreigaben in mehreren Domänen haben und keine Vertrauensstellungen zwischen den Domänen konfigurieren können, erstellen Sie für jede Domäne einen StorageZones Controller.

5. Geben Sie unter Pfad den UNC-Pfad ein.

   Beispiel mit FQDN:\\ fileserver.acme.com\ shared

   Sie können die folgenden Variablen im UNC-Pfad verwenden:

   - %UserName%

     Leitet in das Home-Verzeichnis eines Benutzers um. Beispielpfad: \\myserver\homedirs\%UserName%

   - %HomeDrive%

     Leitet zum Pfad des Basisordners eines Benutzers um, wie in der Active Directory Eigenschaft Home-Directory definiert. Beispielpfad: %HomeDrive%

   - %TSHomeDrive%

     Leitet in das Stammverzeichnis der Terminaldienste eines Benutzers um, wie in der Active Directory Eigenschaft MS-TS-Home-Directory definiert. Der Speicherort wird verwendet, wenn sich ein Benutzer von einem Terminalserver oder Citrix XenApp -Server an Windows anmeldet. Beispielpfad: %TSHomeDrive%

     Im Snap-In Active Directory Benutzer und -Computer ist der MS-TS-Home-Directory-Wert auf der Registerkarte Remotedesktopdienste-Profil verfügbar, wenn Sie ein Benutzerobjekt bearbeiten.

   - %UserDomain%

     Leitet zum NetBIOS-Domänennamen des authentifizierten Benutzers um. Wenn beispielsweise der Anmeldename des authentifizierten Benutzers “abc\ johnd”lautet, wird die Variable durch “abc”ersetzt. Beispielpfad: \\myserver\%UserDomain%_%UserName%

   Bei den Variablen wird die Groß- und Kleinschreibung nicht beachtet.

   Wichtig: Erstellen Sie keinen Connector für den Speicherort von ShareFile Data. Abhängig von den Benutzerberechtigungen können Benutzer auf diese Weise alle ShareFile Daten entfernen.

6. Geben Sie einen benutzerfreundlichen Namen für den Connector ein.

   Der Name wird verwendet, um die Dateifreigabe für Benutzer zu identifizieren. Der Name sollte kurz sein, damit er auf mobilen Geräten mit kleinen Bildschirmen gut angezeigt wird.

7. Klicken Sie auf Connector hinzufügen. Das Dialogfeld Ordnerzugriff anzeigen/bearbeiten wird angezeigt.
8. So machen Sie Connectors für andere sichtbar: Fügen Sie unter Ordnerzugriff anzeigen/bearbeiten Benutzer und Verteilergruppen hinzu, und klicken Sie dann auf Änderungen speichern.

   Dieser Schritt bestimmt nur, ob ein Connector für Benutzer sichtbar ist. **StorageZone Connector erben Zugriffsberechtigungen von der Netzwerkfreigabe. Berechtigungen für Lese-/Schreibzugriff werden durch die Sicherheitseinstellungen der Netzwerkfreigabe bestimmt und sind auch vom ShareFile Plan betroffen.**

So aktivieren Sie das Ein- und Auschecken von Dateien für Netzwerkdateifreigaben

Voraussetzungen

Storage Zones Controller Version 5.8 und Network File Shares Connector müssen konfiguriert werden.

Schritte

1. Melden Sie sich bei Storage Center an. Die Konfigurationsseite wird angezeigt.
2. Klicken Sie auf der Konfigurationsseite auf **Ändern**.
3. Aktivieren Sie das Kontrollkästchen Ein- **und Auschecken für Netzwerkdateifreigaben aktivieren**.
4. Geben Sie den Namen der Domäne ein, in der sich die Benutzer und Netzwerkfreigaben befinden.
5. Geben Sie den Benutzernamen und das Kennwort des Dienstkontos ein. Dieses Dienstkonto ist erforderlich, um Lese- und Schreibzugriff auf alle Dateien und Ordner im Speicherort der Netzwerkfreigabe zu haben.

So erstellen Sie einen Speicherzonen-Connector für Documentum

> **Hinweis:**
>
> Für das Setup des Documentum Connectors wird nur die Standardauthentifizierung unterstützt. Bei Documentum Content Server wird zwischen Groß- und Kleinschreibung unterschieden. Daher sollte der bei der Authentifizierung eingegebene Benutzername mit den Anmeldeinformationen übereinstimmen, sofern die Groß- und Kleinschreibung nicht auf dem Documentum Content Server deaktiviert ist.

Voraussetzungen

1. StorageZone Controller 5.3 oder höher
2. Documentum ECM-Einstellung aktiviert durch den ShareFile Kundensupport.
3. Der Documentum Rest-Service muss auf Ihrem Documentum-Server bereitgestellt werden. Klicken Sie hier, um weitere Informationen zum Documentum Rest Service zu erhalten..
4. Bei Verwendung von Citrix ADC sind bestimmte Konfigurationsänderungen erforderlich. Diese Änderungen sind weiter unten in diesem Artikel detailliert.

Sobald diese Funktion durch den ShareFile Kundensupport aktiviert wurde, navigieren Sie zu Ihrem StorageZones Controller und suchen Sie das Storage Zones Connector-Menü. Aktivieren Sie das Kontrollkästchen "Zugriff auf vorhandene ECM-Datenquellen (Enterprise Content Management) aktivieren". Speichern Sie Ihre Änderungen.

Melden Sie sich als Nächstes bei der ShareFile e-Webanwendung an und navigieren Sie zu **Admin-Einstellungen > Connectors.**

Klicken Sie neben dem Documentum-Connector-Typ auf die Schaltfläche **Hinzufügen**.

Geben Sie den Pfad des EMC Servers an, und geben Sie einen Namen für den Connector ein. Weiter.

Erteilen Sie Benutzern als Nächstes den Zugriff auf den Documentum-Connector.

Sobald der Connector erstellt wurde, können Sie über die Web- und mobile Apps darauf zugreifen.

Unterstützte Aktionen

Mobile (iOS/Android/universelle Windows-Plattform):

- Surfen
- Datei-Uploads/Downloads
- Datei- und Ordnererstellung/Löschung
- Offline-Bearbeitung

WebApp

- Connector-Erstellung
- Surfen
- Datei-Uploads/Downloads
- Ordner Erstellung/Löschung

Nicht unterstützt

- Freigeben von Dateien, die in einem Documentum-Connector gespeichert sind
- Positiv-/Sperrlisten für Pfade

> **Hinweis:**
>
> Bei Documentum Content Server wird zwischen Groß- und Kleinschreibung unterschieden. Daher sollte der bei der Authentifizierung eingegebene Benutzername mit den Anmeldeinformationen übereinstimmen, sofern die Groß- und Kleinschreibung nicht auf dem Documentum Content Server deaktiviert ist.

Citrix ADC Konfiguration für Documentum-Connector

Wenn Sie einen Citrix ADC mit Ihrer Umgebung verwenden, nehmen Sie die folgende Änderung an der Citrix ADC-Konfiguration vor:

1. Fügen Sie Folgendes an die Richtlinie _SF_CIFS_SP unter Content Switching > Policies an:

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

2. Fügen Sie Folgendes an die Richtlinie _SF_SZ_CSPOL unter Content Switching > Policies an:

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

So ändern Sie einen Connectornamen

Ein Connectorname wird verwendet, um eine SharePoint-Website oder Netzwerkdateifreigabe für Benutzer zu identifizieren.

1. Melden Sie sich als Administrator bei Ihrem ShareFile Konto an und klicken Sie dann auf die Registerkarte Connectors.
2. Klicken Sie in der Spalte **Titel** auf den Connectornamen.
3. Geben Sie einen benutzerfreundlichen Namen für den Connector ein, und klicken Sie dann auf **Speichern**.

So löschen Sie einen Connector

Beim Löschen eines Connectors werden keine Daten aus SharePoint oder einer Netzwerkdateifreigabe entfernt.

1. Melden Sie sich als Administrator bei Ihrem ShareFile Konto an und klicken Sie dann auf die Registerkarte Connectors.

2. Aktivieren Sie das Kontrollkästchen für den Connector, klicken Sie auf **Löschen**, und klicken Sie dann auf **OK**.

Connector-Authentifizierung

Adminbenutzer können nun die folgende Einstellung verwenden, um anzugeben, welcher Domänencontroller bei AD-Lookups für CIFS- oder SP-Authentifizierung verwendet werden soll.

```
<add key="Domaincontrollers"value="DC01,dc02.domain.com,123.456.789.1
"/>
```

Der obige Wert "Value="kann auf einen einzelnen DC oder mehrere DCs festgelegt werden, die durch Hostnamen, FQDN oder IP-Adresse identifiziert werden. Mehrere DCs sollten durch Kommas oder Semikolons getrennt werden.

Wenn mehrere DCs angegeben sind, wird die Suche für den ersten DC ausgeführt. Wenn ein Fehler auftritt, wird der zweite DC verwendet usw.

Die obige Eigenschaft kann hinzugefügt werden,`C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config` sodass sie von allen IIS-Anwendungen des StorageZones Controller (einschließlich CIFS, SP und ProxyService) geerbt wird.

Wenn die neue App-Einstellung nicht vorhanden ist, wird das Standardverhalten der automatischen Auswahl eines DC fortgesetzt.

Abrufen einer direkten Verknüpfung von Netzwerkfreigabe/SharePoint-Connectors

Benutzer können jetzt über die Netzwerkfreigabe/SharePoint-Connectors "Einen direkten Link abrufen", während sie die neueste Version der ShareFile App für iOS oder Android verwenden.

Wenn der Admin diese Funktion deaktivieren möchte, kann er dies tun, indem er Folgendes hinzufügen:

```
<add key="disable-direct-link"value="1"/>
```

Das obige kann hinzugefügt werden `C:\inetpub\wwwroot\Citrix\StorageCenter\sps\AppSettingsRelease.config`.

Grundlegende Authentifizierung und lokalisierte Benutzernamen

Die Standardauthentifizierung unterstützt keine Nicht-ASCII-Zeichen. Bei Verwendung lokalisierter Benutzernamen wird empfohlen, dass Benutzer NTLM und Negotiate verwenden.

Verhindern von Datenverlust

May 28, 2024

Mit den Funktionen zum Schutz vor Datenverlust (DLP) in ShareFile können Sie den Zugriff und die gemeinsame Nutzung auf der Grundlage der in einer Datei enthaltenen Inhalte einschränken.

Sie können die in Ihre Speicherzone hochgeladenen Dokumente mit jeder DLP-Sicherheitssuite eines Drittanbieters scannen, die ICAP, ein Standardnetzwerkprotokoll für das Scannen von Inline-Inhalten, unterstützt. Anschließend passen Sie die Freigabe- und Zugriffsrechte auf der Grundlage der Ergebnisse des DLP-Scans und Ihrer Einstellungen an, wie streng Sie den Zugriff kontrollieren möchten.

Unterstützte DLP-Systeme

Der StorageZones Controller verwendet das ICAP-Protokoll für die Interaktion mit DLP-Lösungen von Drittanbietern. Die Verwendung von ShareFile mit einer vorhandenen DLP-Lösung erfordert keine Änderungen an vorhandenen Richtlinien oder Servern. Möglicherweise möchten Sie jedoch ICAP-Server für die Verarbeitung von ShareFile-Daten bereitstellen, wenn Sie mit einer erheblichen Belastung rechnen.

Zu den beliebten ICAP-konformen DLP-Lösungen gehören:

- Schutz vor Datenverlust durch Symantec
- McAfee DLP Prevent
- Websense TRITON AP-DATA

Da ShareFile Ihre bestehende DLP-Sicherheitssuite verwendet, können Sie eine zentrale Richtlinienverwaltung für Dateninspektionen und Sicherheitswarnungen verwalten. Wenn Sie bereits eine der vorherigen Lösungen verwenden, um ausgehende E-Mail-Anhänge oder Web-Traffic nach vertraulichen Daten zu durchsuchen, können Sie den ShareFile Storage Zones Controller auf denselben Server verweisen. Für diese bestehenden DLP-Systeme unterstützen wir auch sicheres ICAP (ICAPS), sofern das zugrunde liegende DLP-System selbst ICAPS unterstützt.

DLP aktivieren

Führen Sie die folgenden drei Aktionen aus, um DLP für ShareFile und StorageZones Controller zu aktivieren:

1. Aktivieren Sie DLP-Funktionen in Ihrem ShareFile-Konto.
2. Aktivieren Sie DLP auf Ihrem StorageZones Controller-Server.
3. Konfigurieren Sie die zulässigen Aktionen für jede Dateiklassifizierung.

Diese Aktionen werden in den folgenden Abschnitten ausführlich beschrieben.

Aktivieren Sie DLP-Funktionen in Ihrem ShareFile-Konto

Um anzufordern oder zu bestätigen, dass Ihre ShareFile-Unterdomäne für DLP aktiviert ist, senden Sie eine Anfrage an den Citrix Support.

Bei einigen Konten erfordert die Aktivierung von DLP möglicherweise auch die Aktivierung einer neueren Benutzererfahrung für die ShareFile-Website. Nachdem Ihr Konto für DLP aktiviert wurde, können Sie mit der Aktivierung von DLP auf Ihrem StorageZones Controller-Server fortfahren.

Aktivieren Sie DLP auf Ihrem StorageZones Controller-Server

Gehen Sie wie folgt vor, um die DLP-Einstellungen in Ihrer StorageZones Controller-Bereitstellung zu konfigurieren:

1. Installieren Sie den StorageZones Controller 5.3 oder höher oder führen Sie ein Upgrade auf diesen durch.
2. Klicken Sie in der Storage Zones Controller-Konsole `http://*localhost*/configservice/login.aspx`auf die Registerkarte **ShareFile-Daten** . Klicken Sie auf **Ändern**, falls die Zone existiert.
3. Markieren Sie das Kontrollkästchen **DLP-Integration aktivieren** und geben Sie die ICAP-Adresse Ihres DLP-Servers in das Feld **ICAP REQMOD URL** ein. Das Adressformat ist:

```
icap://<*name or IP address of your DLP server*>:<*port*>/reqmod

OR

*icaps://\<name or IP address of your DLP server\>:\<port\>/reqmod*

The default ICAP port is 1344 (non-secure DLP) and the default ICAPS port is 11344 (secure DLP).

For example, if your DLP server is dlp-server.example.com, type the following into the ICAP REQMOD URL field:

icap://*dlp-server.example.com*:1344/reqmod

OR

*icaps://dlp-server.example.com:11344/reqmod*
```

4. Klicken Sie auf **Speichern** oder **Registrieren**.

Nachdem Sie DLP aktiviert haben, überprüfen Sie, ob der DLP-Server erreichbar ist, indem Sie auf der Registerkarte **Überwachung** den Eintrag **DLP-ICAP-Serverstatus** überprüfen.

Zugriff auf der Grundlage von DLP-Scanergebnissen kontrollieren

Nachdem DLP auf dem Konto- und Speicherzonencontroller aktiviert wurde, wird jede Version jeder Datei, die in die DLP-fähige Speicherzone hochgeladen wurde, auf vertrauliche Inhalte gescannt. Die Ergebnisse des Scans werden in der ShareFile-Datenbank als Datenklassifizierung gespeichert.

DLP-Einstellungen schränken die normalen Berechtigungen und Freigabekontrollen ein, die für Dateien auf der Grundlage ihrer DLP-Klassifizierung verfügbar sind. Beim Teilen eines Dokuments kann sich ein Benutzer immer noch dafür entscheiden, den anonymen Zugriff zu blockieren, selbst wenn die DLP-Einstellungen es ihm ermöglichen würden, es anonym zu teilen. Wenn der Benutzer jedoch versucht, eine Datei auf eine Weise freizugeben, die gegen die DLP-Einstellungen verstoßen würde, verhindert ShareFile, dass er dies tut.

Die Datenklassifizierungen sind:

- **Gescannt**: OK —Dateien, die von einem DLP-System gescannt wurden und als OK bestanden haben.
- **Gescannt: Abgelehnt** —Dateien, die von einem DLP-System gescannt wurden und bei denen festgestellt wurde, dass sie vertrauliche Daten enthielten.
- **Ungescannt** —Dateien, die nicht gescannt wurden.

Die Klassifizierung "**Nicht gescannt** "gilt für alle Dokumente, die in von Citrix verwalteten Speicherzonen oder anderen Speicherzonen gespeichert sind, in denen DLP nicht aktiviert ist. Die Klassifizierung gilt auch für Dateien in den DLP-fähigen Speicherzonen, die vor der Konfiguration von DLP hochgeladen wurden. Die Klassifizierung gilt auch für Dateien, die darauf warten, gescannt zu werden, weil das externe DLP-System nicht verfügbar ist oder nur langsam reagiert.

Die Klassifizierung jedes Elements wird durch die Antwortregel des ICAP-Servers bestimmt. Wenn der DLP-ICAP-Server mit der Meldung antwortet, dass der Inhalt blockiert oder entfernt werden sollte, wird die Datei als **Gescannt:**Abgelehnt markiert. Andernfalls wird die Datei als **Gescannt markiert: OK**.

Für jede Datenklassifizierung können Sie unterschiedliche Zugriffs- und Freigabebeschränkungen festlegen. Für jede der drei Kategorien wählt der ShareFile-Administrator aus, welche Aktionen zugelassen werden sollen:

- Mitarbeiter können die Datei herunterladen oder teilen.
- Client-Benutzer von Drittanbietern können die Datei herunterladen oder teilen. Die gemeinsame Nutzung von Clients ist standardmäßig deaktiviert, kann aber unter **Admin > Erweiterte Einstellungen > Kunden das Teilen von Dateien ermöglichen**aktiviert werden.

- Anonyme Benutzer können die Datei herunterladen

Wenn ein Benutzer eine Datei teilt, können nur Benutzer mit Download-Rechten die Datei empfangen. Wenn Sie die Freigabeberechtigung für eine Datenklassifizierung aktivieren, müssen Sie daher mindestens einer Klasse von Benutzerberechtigungen zum Herunterladen gewähren.

So konfigurieren Sie DLP-Einstellungen in ShareFile

1. Klicken Sie in der ShareFile-Weboberfläche auf **Admin > Schutz vor Datenverlust.**
2. Ändern Sie die Option für **Zugriff auf Dateien anhand ihres Inhalts einschränken auf Ja**.
3. Konfigurieren Sie die zulässigen Aktionen für jede Datenklassifizierung.

> **Wichtig:**
>
> Das ShareFile On-Demand Sync On-Demand-Sync-Tool benötigt Downloadberechtigungen für den normalen Betrieb. Ermöglichen Sie Mitarbeiterdownloads für alle Inhaltsklassifizierungen, wenn Ihre Bereitstellung ShareFile On-Demand Sync beinhaltet.

Wenn der StorageZones Controller eine Datei an das DLP-System sendet, enthält sie Metadaten, die den Besitzer der Datei angeben. Die Datei enthält auch den Ordnerpfad, in dem sich die Datei in ShareFile befindet. Diese Informationen ermöglichen es dem DLP-Serveradministrator, ShareFile-spezifische Details zu Dateien einzusehen, die vertrauliche Inhalte enthalten.

Erweiterte Einstellungen für DLP

Um den DLP-Scanvorgang anzupassen, bearbeiten Sie die Einstellungsdatei auf Ihrem StorageZones Controller unter `wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`. In der folgenden Tabelle werden alle Einstellungen im Zusammenhang mit DLP beschrieben.

Einstellung	Beschreibung	Standardwert
scan-interval	Wie oft der DLP-Dienst die DLP-Warteschlange auf neue Dateien überprüft und diese zur Verarbeitung an den DLP-ICAP-Server sendet.	30 Sekunden

Einstellung	Beschreibung	Standardwert
icap-response-timeout	Wie lange der StorageZones Controller auf eine ICAP-Antwort wartet, bevor er den ICAP-Server als nicht verfügbar markiert.	30 Sekunden
icap-exclude-extensions	Durch Kommas getrennte Liste von Erweiterungen, die vom DLP-Scan ausgeschlossen werden sollen. Der DLP-Server verarbeitet keine Dateien, deren Namen auf eine dieser Erweiterungen enden, sondern markiert die Dateien als Gescannt: OK. Beispielwert: exe, jpg, bin, mov	Ohne
icap-max-file-size-bytes	Maximale Größe der Datei (in Byte), die zur Verarbeitung an den DLP-Server gesendet werden soll. Ein Wert von 0 bedeutet, dass es kein Maximum gibt und alle Dateigrößen gesendet werden. Bei einer Konfiguration mit einem Wert ungleich Null verarbeitet der DLP-Server keine Dateien, die die konfigurierte Größe überschreiten, sondern sind als Gescannt: OK gekennzeichnet.	31457280 (30 MB)

Einstellung	Beschreibung	Standardwert
x-queue-items-to-process	Die maximale Anzahl von Elementen in der Warteschlange, die pro Scanintervall-Iteration gescannt werden sollen. Verringern Sie diesen Wert, um die Auswirkungen auf Ihren DLP-Server zu verringern, wenn der StorageZone eine große Anzahl von Dateien hinzugefügt wird.	512
max-queue-processing-threads	Maximale Anzahl gleichzeitiger Prozessor-Threads, die verwendet werden, um die DLP-Scan-Warteschlange zu leeren. Stellen Sie diesen Wert auf der Grundlage der maximal zulässigen Anzahl gleichzeitiger Verbindungen zu Ihrem ICAP-Server ein. Es sollte innerhalb angemessener Grenzen liegen, um zu vermeiden, dass andere Netzwerkdienste blockiert werden, die denselben ICAP-Server verwenden.	4
Icap-reqmod-http-request-verb	Standardmäßig werden Netzwerkanrufe mit dem PUT-Verb getätigt. Sie können diese Einstellung bei Bedarf in POST ändern.	PUT

DLPExistingFiles tool

Der ShareFile Storage Zones Controller bietet Optionen zur Integration des Storage Centers mit Anbietern von Data Loss Prevention (DLP) über ICAP.

ICAP-Dienste arbeiten jedoch in Warteschlangen, die nur mit neu erstellten Dateien gefüllt werden.

Das bedeutet, dass Dateien, die vor der Aktivierung von ICAP in einer Zone vorhanden waren, von den Diensten nicht gescannt werden. Dieses Tool hilft dabei, diese Dateien für den Scan in die Warteschlange zu stellen, und kann auch gescannte Dateien für ein erneutes Scannen in die Warteschlange stellen.

Wie der Name schon sagt, funktioniert das Tool nur für den DLP-ICAP-Dienst.

Anforderungen

Das Tool ist ein PowerShell-Skript und benötigt daher PowerShell, um ausgeführt zu werden. PsExec oder ein ähnliches Tool wird ebenfalls benötigt, da das Skript als Netzwerkdienst ausgeführt werden muss, um auf den Netzwerk-Share-Standort zuzugreifen.

Standort

Für einen installierten StorageZones Controller finden Sie das Tool unter `<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1`. Das Installationsverzeichnis des Storage Zones Controllers ist standardmäßig `C:\inetpub\wwwroot\Citrix\StorageCenter`.

Überlegungen vor der Ausführung des Tools

Abhängig von den folgenden Faktoren muss das Tool möglicherweise mehrmals für einen einzelnen Vorgang ausgeführt werden.

- Die Beschränkungen sahen die Begrenzung der Warteschlangengröße vor.
- Die Anzahl der Elemente für die angegebenen Kriterien. Diese Überlegung trifft zu, es sei denn, das Limit für die Warteschlangengröße ist auf Null oder weniger festgelegt. In diesem Fall geht das Tool von einer maximalen Größe von 200.000 Elementen im Warteschlangenverzeichnis aus.

Wenn das Tool beispielsweise verwendet wird, um ungescannte Elemente in die Warteschlange einzureihen, ist das Limit für die Warteschlangengröße auf 500 Elemente festgelegt. Wenn mehr als 500 nicht gescannte Artikel vorhanden sind, stoppt das Tool, nachdem 500 Artikel in der Warteschlange aufgefüllt wurden. Um zu verfolgen, wo es aufgehört hat, speichert das Tool das Erstellungsdatum des zuletzt abgerufenen Elements. Das Tool speichert das Datum in einer temporären Datei unter `<storage zones controller installation location>`\SC mit dem Namen DLPExistingFiles-enddate.temp.

Vor jedem Lauf sucht das Tool nach dieser Datei. Wenn die Datei vorhanden ist, verwendet das Tool das darin enthaltene Erstellungsdatum als Markierung für den nächsten Stapel von Dateien. Das

Tool löscht die temporäre Datei nicht, wenn ein bestimmter Vorgang abgeschlossen ist. Stattdessen kann der Zonenadministrator die Datei löschen, sobald alle Batches für einen bestimmten Vorgang abgeschlossen sind. Aufgrund dieser Situation sollte die temporäre Datei, falls vorhanden, nach Abschluss eines vollständigen Vorgangs manuell entfernt werden, bevor ein anderer Vorgang ausgeführt wird.

Das Tool mit PsExec ausführen

Öffnen Sie ein Befehlsfenster und führen Sie PsExec mit dem folgenden Befehl aus.

```
PsExec.exe -i -u "nt authority\network service"

"C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
```

Dadurch wird PowerShell als Netzwerkdienst geöffnet. Um zu überprüfen, ob es tatsächlich als Netzwerkdienst läuft, führen Sie **whoami** aus und überprüfen Sie das Ergebnis.

Sobald PowerShell geöffnet ist, führen Sie das Tool dort direkt aus, um alle erforderlichen Aufgaben auszuführen.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 <options>
```

Befehlszeilenoptionen

Für die Ausführung des Tools stehen die folgenden Optionen zur Verfügung:

- **-runscan** (Erforderlich): Diese Option wird verwendet, um anzugeben, welche Art von Dateien zum Scannen in die Warteschlange gestellt werden sollen. Unteroptionen:
  - **Ungescannt**: Ungescannte Dateien. Zum Beispiel Dateien aus der Zeit vor DLP, die nicht gescannt wurden.
  - **ScannedOK**: Gescannte Dateien, die als sauber markiert wurden.
  - **ScannedRejected**: Gescannte Dateien, die als nicht sauber markiert wurden.
  - **Scanned**: Alle gescannten Dateien.
- **-queueLimit** (optional): Diese Option wird verwendet, um die Anzahl der Elemente anzugeben, die in der Warteschlange zulässig sind, bevor das Tool beendet wird.
- **-date** (optional): Das maximale Erstellungsdatum der Elemente, die zum Scannen in die Warteschlange gestellt werden sollen. Wenn das Datum beispielsweise als “10/30/2017 11:30 AM”angegeben ist, werden nur die Dateien, die vor diesem Datum/dieser Uhrzeit erstellt wurden, zum Scannen in die Warteschlange gestellt.

Beispiele:

Öffnen Sie für alle Beispiele **PowerShell als Netzwerkdienst über PsExec**. Anweisungen finden Sie in den Schritten weiter oben in diesem Artikel.

Führen Sie den folgenden Befehl aus, um nicht gescannte Elemente in einer Zone in eine Warteschlange zu stellen.

```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Unscanned
```

Führen Sie den folgenden Befehl aus, um alle gescannten Elemente innerhalb einer Zone mit einem Warteschlangenlimit von 100 in die Warteschlange zu stellen.

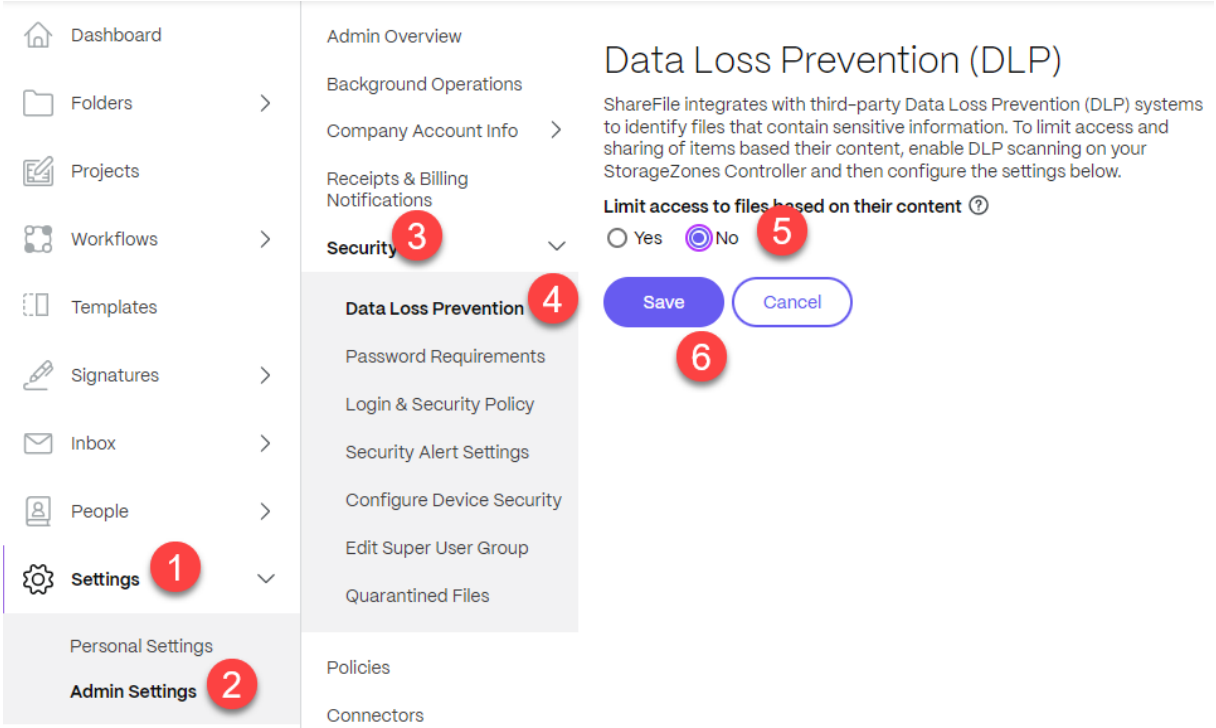
```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Scanned -queueLimit 100
```

Führen Sie den folgenden Befehl aus, um alle gescannten Elemente, die am 30.10.2017 vor 11:30 Uhr erstellt wurden und die folgenden Merkmale aufweisen: Als sauber markiert, in einer Zone mit einem Warteschlangenlimit von 200 in die Warteschlange aufzunehmen.

```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan ScannedOK -queueLimit 200 -date "
    10/30/2017 11:30 AM"
```

DLP deaktivieren

Gehen Sie wie folgt vor, um DLP für ShareFile und den StorageZones Controller zu deaktivieren:



1. Melden Sie sich bei Ihrem Sharefile-Konto an und klicken Sie auf **Einstellungen**.
2. Wählen Sie in der sich öffnenden Dropdownliste die Option **Admin-Einstellungen** aus.
3. Klicken Sie in dem sich öffnenden Menü auf **Sicherheit**.
4. Wählen Sie im Menü Sicherheit die Option **Prävention vor Datenverlust**.
5. Gehen Sie auf dem DLP-Bildschirm zum Abschnitt **Zugriff auf Dateien anhand ihres Inhalts einschränken** und klicken Sie auf **Nein**.
6. Wählen Sie **Speichern**.

Überwachung

February 11, 2022

Der StorageZone Controller und die ShareFile-Administratorschnittstelle enthalten mehrere Ressourcen, mit denen Sie die Storage Zones-Controller-Aktivität überwachen und Probleme beheben können:

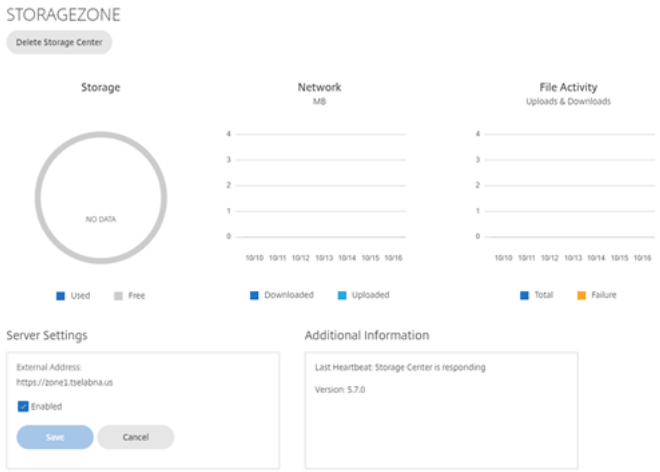
- **Allgemeiner Komponentenstatus** —Die Registerkarte Überwachung in der StorageZone Controller-Konsole bietet den Komponentenstatus, damit Sie mit der Problembehandlung beginnen können. Der Status wird für Elemente wie Zugriffsberechtigungen, Dienststatus und Heartbeat-Status bereitgestellt, der die ausgehende Konnektivität des StorageZone Controllers mit der ShareFile-Steuerungsebene angibt.

Der StorageZone Controller sendet alle 5 Minuten Aktualisierungen an die ShareFile-Webanwendung. Wenn die ShareFile-Webanwendung innerhalb von 10 Minuten kein Update erhält, wird der StorageZone Controller als offline markiert.

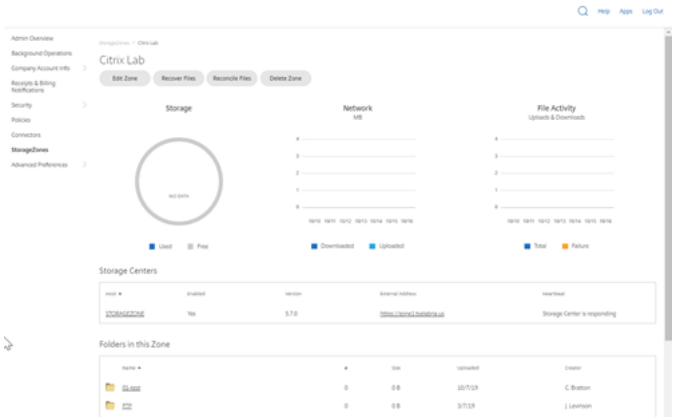
Für Elemente auf der Registerkarte Überwachung, die rot angezeigt werden, überprüfen Sie die Protokolldateien auf ausführliche Informationen.

Die Registerkarte Überwachung zeigt nicht an, ob eine Speicherzone in Bezug auf die Konnektivität funktioniert. Dazu gehört, ob die ShareFile-Steuerungsebene die URL der externen Speicherzone erreichen kann oder ob ein Client die Zone erreichen kann.

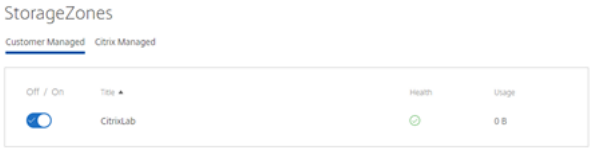
- **StorageZone Controller Serverinformationen** —Informationen zur Speichernutzung, Netzwerknutzung und Dateiaktivität des Servers: Melden Sie sich über die ShareFile-Oberfläche bei Ihrem ShareFile Enterprise-Konto an, gehen Sie zu **Admin > StorageZones**, klicken Sie auf die Speicherzone, und klicken Sie dann auf einen Speicher Zonen-Controller-Hostname



- **Zoneninformationen** —Informationen zur Speichernutzung, zur Netzwerknutzung und zur Dateiaktivität einer Zone: Melden Sie sich über die ShareFile-Oberfläche bei Ihrem ShareFile Enterprise-Konto an, gehen Sie zu **Admin > StorageZones**, und klicken Sie auf einen Zonennamen.



- **Integritätsstatus des StorageZone Controllers** —Um festzustellen, ob ShareFile.com Heartbeat-Nachrichten von den Storage Zones-Controllern empfängt, die mit der Zone verbunden sind, zeigen Sie den Integritätsstatus an: Melden Sie sich über die ShareFile-Oberfläche bei Ihrem ShareFile Enterprise-Konto an und gehen Sie zu **Admin**, überprüfen Sie, ob in der Spalte "Integrität"ein grünes Häkchen angezeigt wird, und klicken Sie dann auf den Site-Namen, um zu überprüfen, ob die Heartbeat-Meldung anzeigt, dass der Storage Zones



- **Protokolldateien** —Protokolldateien enthalten detaillierte Informationen zur StorageZone Controller-Konfiguration und ihren Komponenten, wie im nächsten Abschnitt beschrieben.

Protokolldateien

Die folgenden Protokolldateien für den StorageZone Controller befinden sich standardmäßig in `C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`:

Name der Protokolldatei	Enthält Protokollierungsinformationen für
cfgsrv-%date%.txt	StorageZone Controller-Konfigurationsaktionen, einschließlich Ändern einer vorhandenen StorageZones-Konfiguration, Erstellen einer neuen Speicherzone und Verbinden eines neuen StorageZone Controllers mit einem vorhandenen primären StorageZone Controller
sc-%Datum%.txt	ShareFile-Datenupload und -Download-Aktivitäten für Standardzonen
CIFS-%Date%.txt	Speicherzonen-Connectors für Upload- und Download-Aktivitäten von Netzwerkdatei
sharepoint-%date%.txt	Speicherzonen-Konnektoren für SharePoint-Upload- und Downloadaktivität
cloudstorageuploader-%date%.txt	Cloud Storage Uploader Service (auf ein unterstütztes Speichersystem eines Drittanbieters)
copy-%date%.txt	ShareFile-Kopierdienst
delete–%date%.txt	ShareFile Cleanup Service, für den persistenten Speichercache

Name der Protokolldatei	Enthält Protokollierungsinformationen für
s3uploader–%date%.txt	ShareFile-Verwaltungsdienst. Beinhaltet Heartbeat-Statusmeldungen

Die erweiterte Protokollierung ist für jede der folgenden Komponenten verfügbar und nützlich, wenn Sie detaillierte Informationen für den Support bereitstellen müssen.

Komponente	Speicherort von AppSettingsRelease.config
ShareFile-Daten	C:\inetpub\wwwroot\Citrix\StorageCenter
Speicherzonen-Konnektoren für Netzwerkdateifreigaben	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
Speicherzonen-Konnektoren für SharePoint	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

Aktivieren der erweiterten Protokollierung

Die folgenden Schritte ermöglichen eine erweiterte Protokollierung für alle StorageZone Controller-Komponenten und Dienste:

1. Öffnen Sie auf dem StorageZone Controller-Server IIS.
2. Navigieren Sie zur Standardwebsite und öffnen Sie dann Anwendungseinstellungen.
3. Ändern Sie den Wert für die aktivieren-erweiterte Protokollierung von 0 auf 1.
4. Starten Sie den Citrix ShareFile-Verwaltungsdienst neu.
5. Nachdem Sie das Problem gelöst haben, empfehlen wir Ihnen, die erweiterte Protokollierung zu löschen, um den Umfang der Protokollierung zu reduzieren.

Um die erweiterte Protokollierung für eine bestimmte Komponente zu aktivieren, bearbeiten Sie die Datei AppSettingsRelease.config: Ändern Sie den Wert `<add key="enable-extended-logging"value="0"/>` von 0 auf 1.

Sie können auch die IIS-Protokolle überprüfen, um festzustellen, ob der Datenverkehr den StorageZone Controller erreicht. IIS-Protokolle zeigen alle eingehenden Anforderungen an. IIS-Protokolle für den StorageZone Controller befinden sich in c:\inetpub\logs\LogFiles\W3SVC1.

Informationen zur erweiterten IIS-Protokollierung finden Sie unter http://support.microsoft.com/kb/313437.

Problembehandlung bei der Installation und Konfiguration

Problem	Beschreibung und Lösung
“HTTP-Fehler 404 - Datei oder Verzeichnis nicht gefunden”wird während der Speicherzonen-Controller-Konfiguration angezeigt	Die Meldung ergibt sich normalerweise aus einem Problem mit IIS oder ASP.NET. Stellen Sie sicher, dass die IIS-Rolle in der Windows-Installation aktiviert ist und dass die ASP.NET-Funktion auf IIS aktiviert ist.
“HTTP Error 404.2 —Not Found”erscheint beim Durchsuchen von localhost auf dem StorageZone Controller	Die Meldung weist darauf hin, dass ISAPI- und CGI-Beschränkungen für ASP.NET nicht auf Zulässig festgelegt sind.
“HTTP-Fehler 413 —Request-Entity zu groß” erscheint nach einem Upload-Versuch	Die Meldung kann nach einem fehlgeschlagenen Uploadversuch in eine Speicherzone in einer Netzwerkablaufverfolgung angezeigt werden und kann sich aus einer Clientzertifikatseinstellung in IIS ergeben. Um dieses Problem zu umgehen, öffnen Sie auf dem StorageZone Controller-Server IIS. Navigieren Sie zur Standardwebsite und öffnen Sie dann die SSL-Einstellungen. Wählen Sie für Clientzertifikate Ignorieren aus. Starten Sie den Citrix ShareFile-Verwaltungsdienst neu.
IIS-Fehler treten während der Konfiguration des Storage Zones	IIS-Fehler weisen normalerweise darauf hin, dass ASP.NET nicht vollständig konfiguriert ist. Vergewissern Sie sich im IIS-Manager unter ISAPI- und CGI-Einschränkungen, dass Beschränkung für alle ASP.NET-Listenelemente auf Zulässig festgelegt ist. Stellen Sie sicher, dass ASP.NET in IIS registriert ist: Stellen Sie im IIS-Manager unter Anwendungspools sicher, dass ASP.NET-Listenelemente vorhanden sind. Informationen zur manuellen Registrierung ASP.NETfinden Sie in den Befehlszeilen nach dieser Tabelle. Wenn Sie weiterhin Probleme haben, überprüfen Sie IIS und das ASP.NET-Setup.

Problem	Beschreibung und Lösung
“Storage Center Bindung konnte nicht gespeichert werden”wird während der Speicherzonen-Controller-Konfiguration	Die Meldung weist auf ein Berechtigungsproblem für den IIS-Kontopool-Benutzer hin. Standardmäßig werden Anwendungspools unter dem Benutzerkonto des Netzwerkdienstes ausgeführt. Der StorageZone Controller verwendet standardmäßig das Netzwerkdienstkonto. Wenn Sie anstelle des Netzwerkdienstkontos ein benanntes Benutzerkonto verwenden, muss das benannte Benutzerkonto vollen Zugriff auf die Netzwerkfreigabe haben, die für die private Datenspeicherung verwendet wird.
“Zugriff verweigert”wird während der Zonenkonfiguration angezeigt	Die Meldung kann auftreten, wenn das ShareFile-Konto, bei dem Sie angemeldet sind, nicht über die Berechtigung zum Erstellen und Verwalten von Zonen verfügt. Verwenden Sie die ShareFile-Administratorkonsole, um diese Berechtigung festzulegen.
Ausgehende Anfragen sind gesperrt	Wenn ausgehende Anforderungen blockiert werden, enthält das cfgsrv-Protokoll System.Net.WebException: Der Remoteserver hat einen Fehler zurückgegeben: (403) Forbidden. Dieses Problem ist wahrscheinlich darauf zurückzuführen, dass der Proxyserver ausgehende Anfragen blockiert. Stellen Sie sicher, dass Ihre Firewall die Anforderungen erfüllt, die in den StorageZone Controller
“Verbindung zum Remoteserver kann nicht hergestellt werden”wird angezeigt, wenn Sie sich am StorageZone Controller anmelden	Die Meldung weist normalerweise auf ein Proxy-Problem hin. Stellen Sie sicher, dass Ihre Proxy-Einstellungen konfiguriert sind. Wenn die Proxy-Einstellungen korrekt sind, stellen Sie sicher, dass Sie sich vom StorageZone Controller aus bei Ihrem ShareFile-Konto anmelden können. Stellen Sie sicher, dass Sie über Administratorberechtigungen zum Konfigurieren des StorageZone Controller verfügen und dass Port 443 in der externen Firewall geöffnet ist.

Problem	Beschreibung und Lösung
Der Ordner mit dem Namen ShareFileStorage auf Ihrer Netzwerkfreigabe enthält SCKeys.txt nicht, nachdem Sie Speicherzonen für ShareFile-Daten aktiviert und konfiguriert haben.	StorageZone Controller erstellt während der Installation SCKeys.txt, sofern das Konto, mit dem Sie den Speicherzonencontroller installiert haben, nicht in der Zugriffssteuerungsliste enthalten ist. Aktualisieren Sie die Zugriffssteuerungsliste und installieren Sie den StorageZone Controller neu.
Das Hochladen von Dateien in einen freigegebenen Ordner schlägt fehl, nachdem Sie eine Zone erstellt haben	Dieses Problem weist auf ein Problem mit Ihrem internen DNS hin. Sie benötigen sowohl einen internen als auch einen externen DNS-Eintrag für den FQDN des StorageZone Controllers.
Auf der Registerkarte **Überwachung** ist der Heartbeat-Status rot	Ein rotes Symbol zeigt an, dass der Speicherzonen-Controller keine Heartbeat-Nachrichten an die ShareFile-Website senden kann. Prüfen Sie, ob die Icons für andere Komponenten rot sind. Wenn ja, lesen Sie die Protokolle für weitere Informationen. Wenn das s3uploader-Protokoll einen Fehler beim Senden des Heartbeats anzeigt, kann der StorageZone Controller-Server möglicherweise die ShareFile-Website nur kontaktieren, wenn er einen Proxy-Server durchläuft. Um einen Proxyserver für den StorageZone Controller anzugeben, öffnen Sie die Controller-Konsole und gehen Sie zur Registerkarte Netzwerk. Wenn der StorageZone Controller-Server nicht mit einem Netzwerkdienstbenutzer auf die ShareFile-Website zugreifen kann, erlauben Sie dem Netzwerkdienstbenutzer entweder den Zugriff auf die ShareFile-Website oder richten Sie ein Windows-Benutzerkonto mit ausgehendem Zugriff auf den Proxyserver ein.

Problem	Beschreibung und Lösung
Eine Speicherzone wird nicht in der ShareFile-Administratoroberfläche angezeigt	Dieses Problem kann auf ein Problem mit der externen Adresse oder Firewall hinweisen. Überprüfen Sie zunächst in der StorageZone Controller-Konsole, dass die externe Adresse den Port nicht enthält. Wenn dies der Fall ist, entfernen Sie den Port und starten Sie den Controller neu. Wenn die externe Adresse den Port nicht enthält, stellen Sie sicher, dass Ihre Windows-Firewall richtig konfiguriert ist. Standardmäßig erlauben die Windows-Firewall-Einstellungen ausgehenden Datenverkehr für die ShareFile-Dienste auf Port 443. StorageZone Controller erfordert diese Einstellung. Stellen Sie sicher, dass die Windows-Firewall ausgehenden Datenverkehr auf Port 443 für die folgenden Prozesse zulässt: `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`

Problem	Beschreibung und Lösung
StorageZone Controller lädt keine Daten in ShareFile hoch	Klicken Sie in der Citrix ADC-Konsole mit der rechten Maustaste auf den virtuellen Lastausgleichsserver für Statistiken, um zu überprüfen, ob der Datenverkehr Citrix ADC von der ShareFile-Steuerungsebene, dem Speicherzonen-Controller und den ShareFile-Clients erreicht. Wenn Sie eine Datei hochladen und der virtuelle Server eine Zunahme der Treffer anzeigt, wird der Datenverkehr über Citrix ADC geleitet. Überprüfen des Datenverkehrs für jeden Punkt der Citrix ADC Verbindung: virtueller Content Switching-Server, virtueller Load Balancing-Server für Connectors und ShareFile Daten, HTTP-Callouts, die an einen der beiden virtuellen Server gebunden sind, Responderrichtlinie, die an den virtuellen ShareFile-Datenserver gebunden ist, Connectors Virtual Server Bindung an Citrix ADC AAA. Testen Sie anschließend Uploads für ShareFile-Daten, indem Sie die Responder Policy im virtuellen Lastausgleichsserver für ShareFile-Daten aufheben. (Die Responder Policy verwirft eingehenden Datenverkehr, der nicht von der ShareFile-Steuerungsebene signiert wurde. Geben Sie in einem Webbrowser den externen FQDN des StorageZone Controller ein. Wenn Konnektivität besteht, wird das ShareFile-Logo angezeigt. Geben Sie in einem Webbrowser die URL für einen Konnektor ein. Wenn die folgenden URLs den Zugriff auf Speicherzonen-Connectors erfolgreich testen können, werden Sie zur Eingabe der Anmeldeinformationen aufgefordert, auch wenn der Back-End-Server ausgefallen ist. Oder wenn Sie als Benutzer angemeldet sind, erhalten Sie eine API-Antwort. `https://szc-address/cifs/v3/Items/ByPath?path=\\path`, `https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server`. Die API-Antwort lautet in folgendem Format: {“Name”:”connectorName”,“FileName”:”FileName”,“CreationDate”:”date”, “ProgenyEditDate”:”date”,“IsHidden”:false,

Problem	Beschreibung und Lösung
Der Status ShareFile-Konnektivität von File Cleanup Services ist ein rotes Symbol, nachdem Sie den StorageZone Controller aktualisiert haben.	Ein rotes Symbol erscheint, wenn Windows den File Cleanup Service startet, bevor der StorageZone Controller eine Netzwerkverbindung herstellt. Der Status kehrt zu einem grünen Symbol zurück, nachdem der Controller-Server wieder im Netzwerk ist.
“Pfad überschreitet die maximale Länge (1024)” wird während der Connectorerstellung angezeigt	Die Meldung kann auftreten, wenn die für den StorageZone Controller konfigurierte externe Adresse anstelle des FQDN des StorageZone Controller-Servers auf die ShareFile-Website verweist
“Ungültiger Name”wird angezeigt, wenn ein neuer StorageZone Controller konfiguriert wird, nachdem ein alter gelöscht wurde.	Die Meldung kann auftreten, wenn Entitäten, die sich auf den alten StorageZone Controller beziehen, noch existieren Um dieses Problem zu beheben: Deinstallieren Sie den neuen Speicherzonen-Controller. Löschen Sie den freigegebenen Netzwerkordner. Löschen Sie den Ordner c:\inetpub\wwwroot\Citrix. Öffnen Sie Regedit und löschen Sie den Schlüssel **HKEY_LOCAL_Machine/Software/WOW6432Note/Citrix**. Installieren und Konfigurieren eines neuen StorageZone Controllers. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren Supportmitarbeiter. Diese Meldung tritt auf, wenn Speicherzonenserver den FQDN der Speicherzone nicht über DNS oder die lokale Hosts-Datei auflösen können.

Um sich manuell zu registrieren 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
/[path='%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll'
    ].allowed:True
```

Problembehandlung bei ShareFile-Clients und Webanwendungen

Wenn ein Mobilgerät keine Verbindung zu einem Connector herstellen kann, überprüfen Sie die Konnektivität. Viele Verbindungsprobleme werden in der vorherigen Tabelle behandelt. Stellen Sie sicher, dass der Speicherzonen-Controller online ist. Laden Sie eine Datei in die Zone hoch. Wenn der Upload funktioniert, ist das Problem spezifisch für die Konnektoren. Versuchen Sie, vom Mobilgerät aus eine Verbindung sowohl über das Mobilfunk- als auch über das Firmennetzwerk herzustellen. Stellen Sie sicher, dass der SharePoint-Server oder Dateiserver verfügbar ist.

Wenn beim Versuch, auf einen Connector zuzugreifen, ein "HTTP-Fehler 401 —Unautorisiert" angezeigt wird, kann eines der folgenden Probleme verhindern, dass ein Benutzer von ShareFile-Clients oder der ShareFile-Webanwendung auf einen Connector zugreift:

- Falsche Konfiguration von IIS: Stellen Sie sicher, dass für die Rolle Webdienste (IIS) Standardauthentifizierung und Windows-Authentifizierung aktiviert sind. Wenn diese Optionen nicht unter Sicherheit aufgeführt sind, verwenden Sie Server Manager, um sie zu installieren, und starten Sie dann IIS neu.
- Falsche Benutzerberechtigungen: Stellen Sie sicher, dass der AD-Benutzer Zugriff auf die Freigabe hat. Gehen Sie im Server-Manager zu Freigabe- und Speicherverwaltung und fügen Sie den Benutzer hinzu oder ändern Sie die Benutzerberechtigungen nach Bedarf.
- Ein Problem mit der Citrix ADC-Authentifizierung, Autorisierung und Überwachung des Gruppenzugriffs.

Wenn beim Herstellen einer Verbindung mit einer SharePoint-Website ein "HTTP-Fehler 403 —Forbidden"angezeigt wird, ist der SharePoint-Server möglicherweise für die Standardauthentifizierung konfiguriert, der Speicherzonen-Controller ist jedoch möglicherweise nicht für das Zwischenspeichern von Anmeldeinformationen Um dieses Problem zu beheben, fügen Sie `<add key="CacheCredentials"value="1"/>` zu `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config` hinzu.

Wenn ein "HTTP-Fehler 503 —Dienst nicht verfügbar"angezeigt wird, wenn mobile Apps versuchen, auf einen Connector zuzugreifen, senden die Konnektoren eine Antwort, können die HTTP-Anforderung jedoch nicht verarbeiten. Dies kann auftreten, wenn Content Switching-Richtlinien, VIPs für den Lastausgleich oder die Responderrichtlinie falsch konfiguriert oder an Citrix ADC gebunden sind. Um dieses Problem zu beheben, überprüfen Sie die Citrix ADC-Konfiguration für ShareFile und korrigieren Sie die Konfiguration.

Referenz: Konfigurationsdateien für den Storage Zones Controller

December 5, 2022

Diese Referenz bietet einen Überblick über die Konfigurationsdateien des StorageZones Controllers:

- Konfigurieren des StorageZonen-Controllers mit ShareFile-Daten auf Microsoft Azure
- AppSettingsRelease.config
- FileDeleteService.exe.config
- SFAntiVirus.exe.config
- Web.config

Das Storage Zones Controller-Installationsprogramm erstellt diese Dateien. Änderungen, die Sie in der StorageZones Controller-Konsole vornehmen, werden in den Dateien gespeichert.

Um bestimmte Funktionen verwenden oder konfigurieren zu können, müssen Sie einige Einstellungen in den Konfigurationsdateien manuell hinzufügen oder aktualisieren. Diese Referenz listet diese Einstellungen auf und enthält Links zu verwandten Informationen.

ShareFile-Daten auf Microsoft Azure Storage

Kundenverwaltete Speicherzonen unterstützt das native Hosten von Citrix ShareFile-Daten in Ihrem Microsoft Azure-Konto. Die Verwendung von kompatiblem Drittanbieter-Speicher hilft der IT, eine kostengünstige und maßgeschneiderte Lösung für ihr Unternehmen zu entwickeln Diese Lösung integriert ShareFile mit dem Binary Large Object (Blob) -Speicher von Microsoft Azure. Dieser Speicher ist ein Cloud-Dienst zum Speichern großer Mengen unstrukturierter Daten, auf die von überall mit HTTP oder HTTPS zugegriffen werden kann.

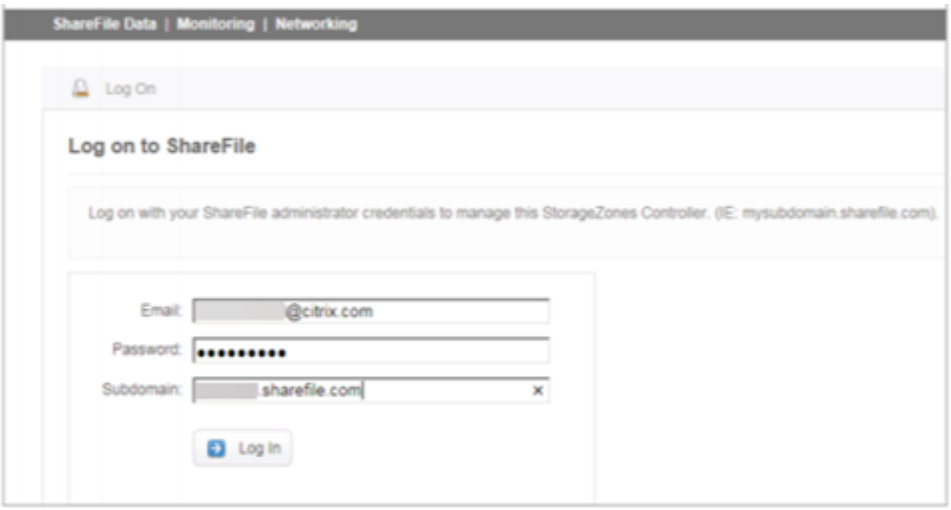
Konfigurieren des StorageZonen-Controllers mit ShareFile-Daten auf Microsoft Azure

Bevor Sie eine Speicherzone mit ShareFile-Daten in Microsoft Azure erstellen, lesen Sie bitte die Systemanforderungen und Installationsschritte:

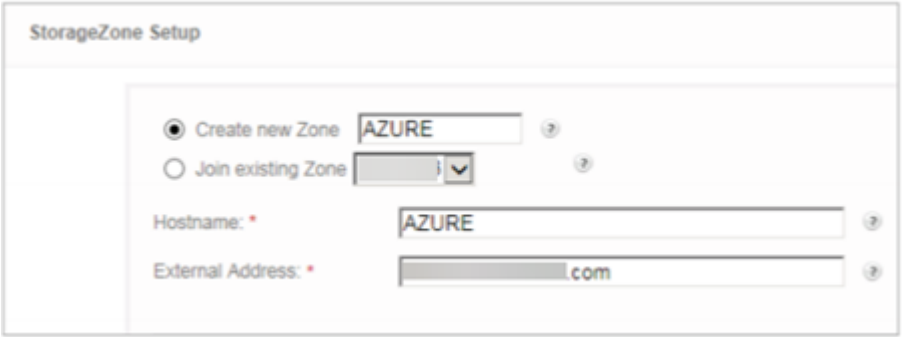
- Erstellen Sie eine Netzwerkfreigabe für den Speicher-Cache. Weitere Informationen finden Sie unter Netzwerkfreigabe für private Datenspeicherung erstellen.
- Installieren Sie die erforderlichen SSL-Zertifikate. Weitere Informationen finden Sie unter Installieren eines SSL-Zertifikats.
- Bereiten Sie den Server auf die Installation von Storage Weitere Informationen finden Sie unter Vorbereiten Ihres Servers für ShareFile-Daten.

Sobald die StorageZones Controller-Software installiert ist, gehen Sie zu **Citrix ShareFile Storage Zones Controller** und wählen Sie **Konfigurationsseite**.

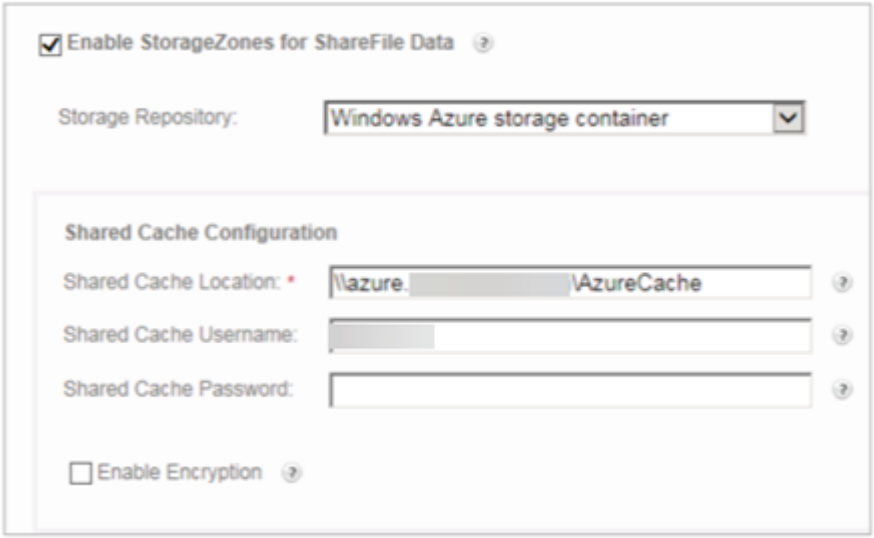
1. Melden Sie sich bei ShareFile mit Ihrem zugewiesenen Administratorkonto



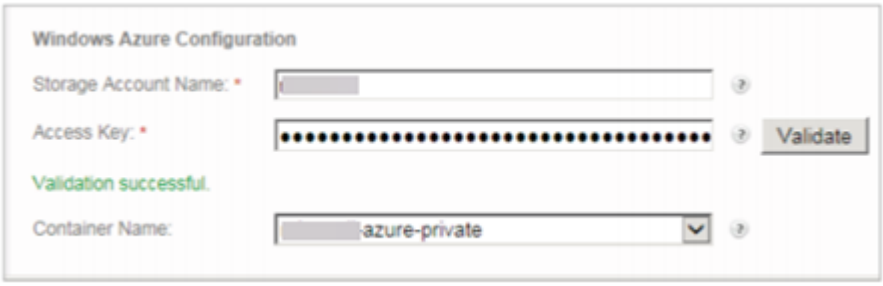
2. Wählen Sie die Option **Neue Zone erstellen** und geben Sie einen eindeutigen Namen für die neue Zone ein.
3. Geben Sie den **Hostnamen**ein, normalerweise wird der Computername des Servers verwendet.
4. Geben Sie die **externe Adresse** für diese Zone ein. Dies ist die öffentlich auflösbare FQDN-Adresse für diesen Server oder Load Balancer.



5. **Aktivieren Sie das Kästchen StorageZones für ShareFile-Daten** aktivieren.
6. Wählen Sie im Dropdown-Menü **Speicher-Repository** die Option **Windows Azure-Speichercontainer** aus.
7. Geben Sie den **gemeinsam genutzten Cache-Speicherort** ein, der bei der Installation der Voraussetzungen erstellt wurde. Weitere Informationen finden Sie unter Netzwerkfreigabe für private Datenspeicherung erstellen. Geben Sie einen Benutzernamen und ein Kennwort mit Zugriff auf den Ordner Shared Cache ein.

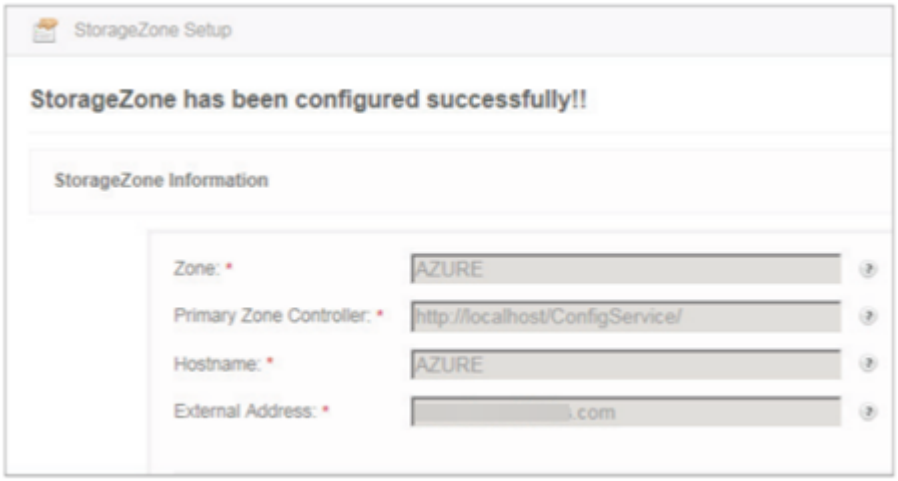


8. Geben Sie den **Namen des Speicherkontos** und den **Zugriffsschlüssel** ein. Diese Informationen stammen von Ihrem Microsoft Azure-Konto.
9. Wählen Sie **Validieren**aus.
10. Nach der Validierung werden Ihnen die Container vorgelegt, die Ihnen bei Azure zur Verfügung stehen. Wählen Sie den entsprechenden Container aus dem Dropdown-Menü **Containername** aus.

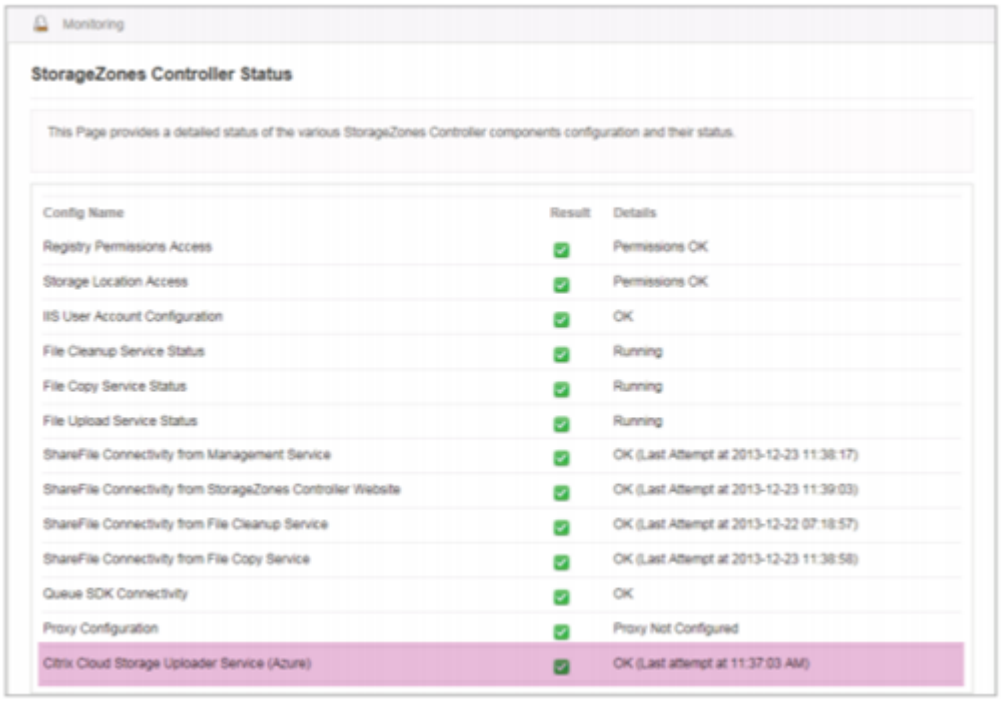


11. Geben Sie unten auf der Seite eine Passphrase ein und geben Sie sie zur Überprüfung erneut ein.
12. Wählen Sie **Register**.

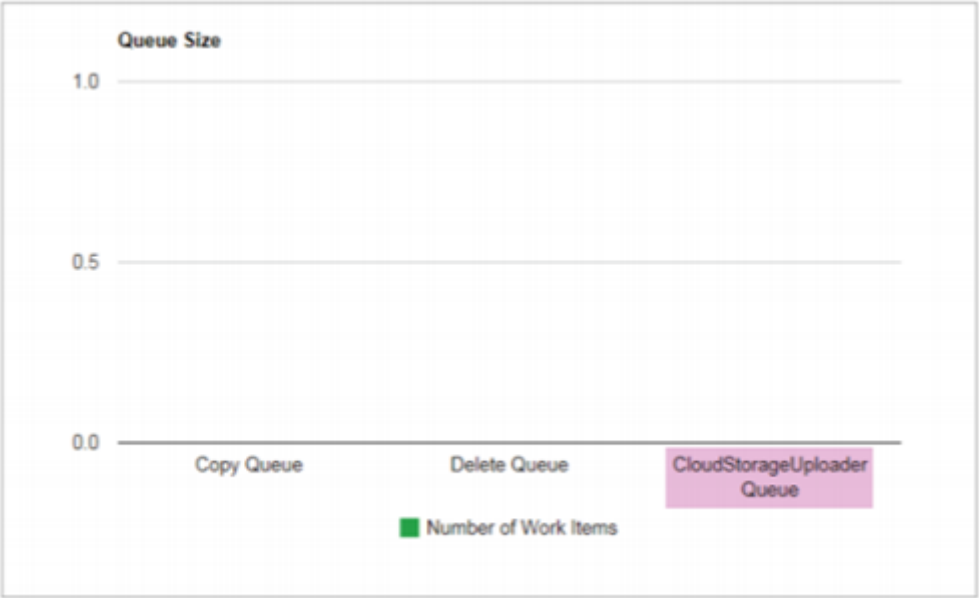
    Sobald Sie abgeschlossen sind, wird die folgende Meldung angezeigt: StorageZone wurde erfolgreich konfiguriert!!



13. Wählen Sie die Registerkarte **Monitoring** und überprüfen Sie den StorageZones Controller-Status. Der Citrix Cloud Storage Uploader Service (Azure) überwacht den Hintergrund-Uploader-Dienst auf Azure.



Die **CloudStorageUploader-Queue** überwacht den Ordner für die Upload-Warteschlange von Azure.



AppSettingsRelease.config

AppSettingsRelease.config-Dateien sind in den folgenden Ordnern im Installationspfad des Storage Zones Controllers (C:\inetpub\wwwroot\Citrix\) enthalten:

- StorageCenter

  Definiert globale Einstellungen für den Storage Zones Controller.

- StorageCenter\cifs

  Definiert Einstellungen für StorageZonen Connectors für Network File Shares.

- StorageCenter\sp

  Definiert Einstellungen für StorageZonen Connectors für SharePoint.

Bevor Sie eine AppSettingsRelease.config-Datei bearbeiten, stellen Sie sicher, dass Sie am richtigen Ort arbeiten.

FileDeleteService.exe.config

FileDeleteService.exe.config bietet Steuerelemente, die vom Storage Zones Controller zur Verwaltung des persistenten Speichercaches verwendet werden. Diese Konfigurationsdatei ist in: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

Weitere Informationen finden Sie unter Anpassen von Speicher-Cache-Vorgängen.

SFAntiVirus.exe.config

SFAntiVirus.exe.config stellt der Scannersoftware Informationen über die Konfiguration Ihres Storage Zones Controllers, den Speicherort der Scannersoftware und verschiedene Befehlsoptionen zur Verfügung. Diese Konfigurationsdatei ist in: `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

Weitere Informationen finden Sie unter Konfigurieren von Antiviren-Scans hochgeladener Dateien.

Web.config

Im Allgemeinen enthält `C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` Steuerelemente, die normalerweise nicht geändert werden sollten. Sie müssen es jedoch aktualisieren, wenn Sie ältere StorageZonen-Controller mit einem Proxyserver verwenden.

Nur für StorageZones Controller 2.2 bis 2.2.2: Wenn eine Zone mehrere StorageZonen-Controller hatund der gesamte HTTP-Verkehr einen Proxyserver verwendet, müssen Sie Web.config für jeden sekundären Server eine Bypassliste hinzufügen.

Hinweis: Ab Version 2.2.3 ist die Bypass-Einstellung auf der Netzwerkseite der StorageZones Controller-Konsole enthalten.

1. Öffnen Sie die Datei in einem Texteditor und suchen Sie den Abschnitt `<system.net>`. Hier ist ein Beispiel für diesen Abschnitt nach der Konfiguration eines Proxyservers:

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
    </defaultProxy>
  </system.net>
</configuration>
```

2. Fügen Sie diesem Abschnitt eine Bypassliste hinzu, wie in der Abbildung gezeigt:

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
      <bypasslist>
        <add address="primaryServer" />
      </bypasslist>
    </defaultProxy>
  </system.net>
</configuration>
```

primaryServer ist entweder eine IP-Adresse oder ein Hostname (servername.subdomain.com).

Wenn Sie später die IP-Adresse oder den Hostnamen des primären StorageZones ändern, müssen Sie diese Informationen in ConfigService\Web.config für jeden sekundären Server

aktualisieren.

3. Starten Sie den IIS-Server aller Zonenmitglieder neu.