StorageZones Controller 5.x

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Citrix Dokumentation maschinell übersetzt. Citrix hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Citrix Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Citrix gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Citrix kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Informationen zum StorageZones Controller

June 11, 2020

Storage Zones Controller erweitert den ShareFile Software as a Service (SaaS) Cloud-Speicher, indem Sie Ihrem ShareFile-Konto private Datenspeicherung bereitstellen, die als Speicherzonen für ShareFile-Daten bezeichnet wird.

Weitere Informationen zum Storage Zones Controller, wie die Komponenten, die Datenspeicherung und mehr, finden Sie unter StorageZones Controller 5.x.

Die neuesten Verbesserungen in dieser und Citrix Content Collaboration finden Sie unter. [Neue Features()]

Informationen zum Herunterladen der neuesten Version finden Sie unter https://www.citrix.com/downloads/share
Melden Sie sich bei Ihrem Citrix Konto an, um auf alle Anwendungsdownloads zuzugreifen.

Behobene Probleme

Behobene Probleme in Storage Zones Controller 5.10

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

Behobene Probleme in Storage Zones Controller 5.9

Diese Version enthält Korrekturen zur Verbesserung der Zuverlässigkeit und Leistung.

Behobene Probleme in Storage Zones Controller 5.8

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

Behobene Probleme in Storage Zones Controller 5.7

Diese Version enthält Fehlerbehebungen, um ein Umleitungsproblem bei Datei-Uploads in die Speicherzone und lokale Connectors zu beheben.

Behobene Probleme in Storage Zones Controller 5.6

WOPI-Fix: Enthält Änderungen, um Probleme zu beheben, die beim Versuch auftreten, Office-Dateien nachträglich zu bearbeiten.

SharePoint Connector-Fix: Diese Version enthält Änderungen zum Anzeigen gültiger Fehlermeldungen beim Erstellen von Ordnern, die bereits in SharePoint Connector vorhanden sind.

Behobene Probleme in Storage Zones Controller 5.5

Diese Version enthält Korrekturen zur Verbesserung der Zuverlässigkeit und Leistung.

Behobene Probleme in Storage Zones Controller 5.4.2

SharePoint Connector-Fix: Verschieben von Dateien, die auf SharePoint-Connector vorhanden sind, schlägt möglicherweise für bestimmte Szenarien fehl. Diese Version stellt sicher, dass das Verschieben von Dateien, die in SharePoint Connector vorhanden sind, wie erwartet funktioniert.

Sicherheitskorrekturen: Diese Version enthält Korrekturen für Sicherheit und Zuverlässigkeit.

Behobene Probleme in Storage Zones Controller 5.4.1

Sicherheitskorrekturen: Diese Version enthält Korrekturen für Sicherheit und Zuverlässigkeit.

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

Behobene Probleme in Storage Zones Controller 5.3.1

Diese Version enthält Korrekturen zur Verbesserung der Zuverlässigkeit und Leistung.

Behobene Probleme in Storage Zones Controller 5.3.1

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

Sicherheitskorrekturen: Diese Version enthält Korrekturen für Sicherheit, Leistung und Zuverlässigkeit.

Bekannte Probleme

Bekannte Probleme in Storage Zones Controller 5.10

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Storage Zones Controller 5.9

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Storage Zones Controller 5.8

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Storage Zones Controller 5.7

In diesem Release wurden keine neuen Probleme festgestellt.

Architektur im Überblick

June 11, 2020

Dieser Abschnitt bietet einen Überblick über die Bereitstellung von Storage Zones Controller für die Bewertung von Proof-of-Concept 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 Storage Zones Controllern zu bewerten, befolgen Sie die Richtlinien für eine Bereitstellung mit hoher Verfügbarkeit.

Für jedes Bereitstellungsszenario ist ein ShareFile Enterprise Konto erforderlich. Standardmäßig speichert ShareFile Daten in der sicheren ShareFile-verwalteten Cloud. Konfigurieren Sie Speicherzonen für ShareFile-Daten, um den privaten Datenspeicher entweder eine lokale Netzwerkfreigabe oder ein unterstütztes Speichersystem eines Drittanbieters zu verwenden.

Um Daten aus Netzwerkdateifreigaben oder SharePoint-Dokumentbibliotheken sicher an Benutzer bereitzustellen, konfigurieren Sie StorageZone Connector.

Storage Zones Controller Machbarkeitsnachweis Bereitstellung

> **Vorsicht:**
>
> Eine Proof-of-Concept-Bereitstellung ist nur zu Evaluierungszwecken gedacht und sollte nicht für die Speicherung kritischer Daten verwendet werden.

Bei einer Proof-of-Concept-Bereitstellung wird ein einzelner Storage Zones Controller verwendet. Für die in diesem Abschnitt erläuterte Beispielbereitstellung sind sowohl Speicherzonen für ShareFile Data als auch StorageZone Connector aktiviert.

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

Proof-of-Concept-Bereitstellung für Standardspeicherzonen

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

In diesem Szenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Der StorageZones Controller befindet sich innerhalb der Firewall, um den Zugriff zu steuern. Benutzerverbindungen zu ShareFile müssen die Firewall durchlaufen 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 des StorageZones Controller installieren.

Bereitstellung von Storage Zones Controller 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, verbinden Sie sie mit derselben Zone. StorageZones Controller, die zur gleichen 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 Speicherzonensteuerungs-Subsystem wählt zufällig einen StorageZones Controller für Vorgänge aus. 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.

Hochverfügbarkeitsbereitstellung für Standardzonen

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

Zones Controller zugeordnet sind. Die folgende Abbildung zeigt eine Bereitstellung mit hoher Verfügbarkeit für Standardspeicherzonen.

Ähnlich wie das oben genannte Proof-of-Concept-Bereitstellungsszenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Die StorageZones Controller befinden sich in der Firewall, um den Zugriff zu steuern. Benutzerverbindungen zu ShareFile müssen die Firewall durchlaufen 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 aller StorageZones Controller installieren.

Konfiguration des gemeinsam genutzten Speichers

StorageZones Controller, die zur gleichen 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.

Sie können anstelle des Netzwerkdienstkontos ein benanntes Benutzerkonto verwenden, um auf die Freigabe zuzugreifen. Um ein benanntes Benutzerkonto zu verwenden, geben Sie den Benutzernamen und das Kennwort auf der Konfigurationsseite der Speicherzonen-Konsole an. Führen Sie den IIS-Anwendungspool und die Citrix ShareFile Dienste mit dem Netzwerkdienstkonto aus.

Netzwerkverbindungen

Die Netzwerkverbindungen variieren je nach Zonentyp — von Citrix verwaltet oder Standard.

Von Citrix 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 Citrix verwalteten Zone herunterlädt. Alle Verbindungen verwenden HTTPS.

Schritt	Quelle	Ziel
1. Benutzeranmeldeanforderung	Client	`company.sharefile.com:443`
2. (Optional) Umleiten zur SAML-IdP-Anmeldung	Client	SAML-Identitätsanbieter-URL
3. Datei-/Ordner-Aufzählung und Download-Anforderung	Client	`company.sharefile.com:443`

Schritt	Quelle	Ziel
4. Dateidownload	Client	storage-location.sharefile.com:443

Standard-Speicherzonen

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

Schritt	Quelle	Ziel
1. Benutzeranmeldeanforderung	Client	company.sharefile.com
2. (Optional) Bei Verwendung von ADFS zur SAML-IdP-Anmeldung umleiten	Client	SAML-Identitätsanbieter-URL
3. Datei-/Ordner-Aufzählung und Download-Anforderung	Client	company.sharefile.com
4. Autorisierung für den Dateidownload	company.sharefile.com	szc.company.com
5. Dateidownload	Client	szc.company.com

StorageZones Controller DMZ-Proxy-Bereitstellung

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

- Stellen Sie sicher, dass alle Anforderungen an einen StorageZones Controller aus der ShareFile Cloud stammen, damit nur genehmigter Datenverkehr die StorageZones Controller erreicht.

  -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 vor dem Weiterleiten von Nachrichten verantwortlich.

- Lastausgleichsanforderungen an StorageZones Controller mithilfe von Echtzeitstatusindikatoren.

Operationen können Lastenausgleich auf StorageZones Controller erfolgen, wenn sie alle auf die gleichen Dateien zugreifen können.

- SSL von StorageZones Controllern entladen.
- Stellen Sie sicher, dass Anforderungen für Dateien auf SharePoint- oder Netzlaufwerken authentifiziert werden, bevor Sie die DMZ durchlaufen.

Citrix ADC - und Storage Zones Controller Bereitstellung

Bereitstellung für Standardspeicherzonen

Für Standardzonen konfigurierte StorageZones Controller müssen eingehende Verbindungen aus der ShareFile e-Cloud akzeptieren. Dazu muss Citrix ADC über eine öffentlich zugängliche Internetadresse und SSL für die Kommunikation mit der ShareFile Cloud verfügen.

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 durchlaufen 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 (wenn die Benutzerverbindung beendet wird).

Netzwerkverbindungen für Standardzonen

Im folgenden Diagramm und in der Tabelle werden die Netzwerkverbindungen beschrieben, 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 Verbunddienste (ADFS) für die SAML-Anmeldung.

Authentifizierungsdatenverkehr 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, wodurch SSL beendet wird, Benutzeranforderungen authentifiziert werden und dann im Auftrag authentifizierter Benutzer auf den StorageZones Controller im vertrauenswürdigen Netzwerk zugreift. Der Zugriff auf die externe Citrix ADC Adresse für ShareFile erfolgt über den Internet-FQDN szc.company.com.

Schritt	Quelle	Ziel	Protokoll
1. Benutzeranmeldeanforderung	Client	`company.sharefile.com`	HTTPS
2. (Optional) Umleiten zur SAML-IdP-Anmeldung	Client	SAML-Identitätsanbieter-URL	HTTPS

Schritt	Quelle	Ziel	Protokoll
2a. ADFS-Anmeldung	ADFS-Proxy	ADFS-Server	HTTPS
3. Datei-/Ordner-Aufzählung und Download-Anforderung	Client	`company.sharefile.com`	HTTPS
4. Autorisierung für den Dateidownload	ShareFile	`szc.company.com` (externe Adresse)	HTTP(S)
4a. Autorisierung für den Dateidownload	Citrix ADC IP (NSIP)	StorageZones Controller	HTTPS
5. Dateidownload	Client	`szc.company.com` (externe Adresse)	HTTPS
5a. Dateidownload	Citrix ADC IP (NSIP)	StorageZones Controller	HTTP(S)

Das folgende Diagramm und die Tabelle erweitern das vorherige Szenario, um die Netzwerkverbindungen für StorageZone Connectors anzuzeigen. Dieses Szenario umfasst die Verwendung von NetScaler in der DMZ zum Beenden von SSL und zur Durchführung der Benutzerauthentifizierung für Connectors-Zugriff.

Schritt	Quelle	Ziel	Protokoll
1. Benutzeranmeldeanforderung	Client	`company.sharefile.com`	HTTPS
2. (Optional) Umleiten zur SAML-IdP-Anmeldung	Client	SAML-Identitätsanbieter-URL	HTTPS
2a. ADFS-Anmeldung	ADFS-Proxy	ADFS-Server	HTTPS
3. Konnektorenumeration der obersten Ebene	Client	`company.sharefile.com`	HTTPS
4. Benutzeranmeldung am StorageZones Controller-Server	Client	`szc.company.com` (externe Adresse)	HTTPS

Schritt	Quelle	Ziel	Protokoll
5. Benutzerauthen-tifizierung	Citrix ADC IP (NSIP)	AD-Domänencontroller	LDAP (S)
6. Datei-/Ordner-Enumeration und Upload/Download Anforderungen	Citrix ADC IP (NSIP)	StorageZones Controller	HTTP (S)
7. Enumeration von Netzwerkfreigaben und Upload/Download	StorageZones Controller	Dateiserver	CIFS oder DFS
7a. SharePoint-Aufzählung und Hochladen/Herunter-laden	StorageZones Controller	SharePoint	HTTP(S)

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

Systemanforderungen

June 11, 2020

StorageZones Controller

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

Für Standardspeicherzonen:

- Verwenden Sie einen öffentlich auflösbaren Internet-Hostnamen (keine IP-Adresse).
- Aktivieren Sie SSL für die Kommunikation mit ShareFile.
  - Das SSL-Zertifikat auf dem StorageZones Controller muss von Benutzergeräten und ShareFile e-Webservern vertrauenswürdig sein. Wenn Sie SSL direkt mit IIS verwenden, finden Sie Informationen http://support.microsoft.com/kb/298805 zum Konfigurieren von SSL unter.

- Erlauben Sie eingehende TCP-Anforderungen an Port 443 über Ihre Firewall.
- Erlauben Sie ausgehende TCP-Anforderungen 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 hochverfügbare Produktionsumgebung:

- Mindestens zwei Server mit installiertem Storage Zones Controller.
- Wenn Sie keine DMZ-Proxyserver verwenden, installieren Sie ein SSL-Zertifikat auf dem IIS-Dienst.

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

Für eine DMZ-Proxy-Bereitstellung:

- Mindestens ein DMZ-Proxyserver, z. B. Citrix ADC VPX Instanzen.
- Installieren Sie für einen DMZ-Proxyserver, der die Clientverbindung beendet und HTTP verwendet, ein SSL-Zertifikat auf dem Proxyserver.

  Wenn die Kommunikation zwischen dem DMZ-Proxyserver und dem Storage Zones Controller sicher ist, können Sie HTTP verwenden. HTTPS wird jedoch als Best Practice empfohlen. Wenn Sie HTTPS verwenden, können Sie ein privates Zertifikat (Enterprise) auf dem StorageZones Controller verwenden, wenn es vom DMZ-Proxy vertrauenswürdig ist. Die externe Adresse, die vom DMZ-Proxy bereitgestellt wird, muss ein kommerziell vertrauenswürdiges Zertifikat verwenden. Weitere Informationen zu unterstützten Zertifikaten finden Sie in den Zertifikatanforderungen für Standardzonen oben.

Sonstige Anforderungen

- Das Installationsprogramm des StorageZones Controller ers erfordert Administratorrechte.
- Verwenden Sie für die Remote-Verwaltung des StorageZones Controller ein Remoting-Protokoll, z. B. RDP oder Citrix ICA, um eine Verbindung mit dem Server herzustellen und dann die Storage Zones Controller-Konsole zu öffnen.

Unterstützte Speichersysteme von Drittanbietern

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

Unterstützte Lösungen zur Prävention vor Datenverlust

- Der StorageZones Controller lässt sich in jede ICAP-konforme DLP-Lösung integrieren, einschließlich:
  - Symantec Data Loss Prevention
  - McAfee DLP Prevent
  - Websense TRITON AP-DATA
  - RSA Data Loss Prevention

Speicherzonen für ShareFile Daten

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

Anforderungen:

- ShareFile Enterprise Konto mit aktivierter Speicherzonenfunktion
- Ein ShareFile Benutzerkonto, das Berechtigungen zum Erstellen und Verwalten von Zonen enthält
- Eine CIFS-Freigabe für private Datenspeicherung

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

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

Hinweis: Der Zugriff auf ein ShareFile Konto über einen FTP-Client ist nicht mit Speicherzonen für ShareFile-Daten kompatibel.

Speicherzonen-Connector für SharePoint

Der Speicherzonenconnector für SharePoint ist ein optionales Feature, das 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 in derselben Gesamtstruktur wie der SharePoint-Server ein Domänenmitglied sein.
- Die Webserverrolle (IIS) und ASP.NET 4.x. Weitere Informationen finden Sie unter Vorbereiten des Servers für ShareFile Daten.

- SharePoint-Richtlinien:
  - Die standardmäßige maximale Uploaddateigröße für eine Webanwendung in SharePoint 2013 beträgt 250 MB und in SharePoint 2010 50 MB. So ändern Sie den Standardwert: Wechseln Sie in der SharePoint-Zentraladministration zur Seite Allgemeine Webanwendungseinstellungen, und ändern Sie die maximale Uploadgröße. Die Größenbeschränkung für Uploaddateien für SharePoint beträgt 2 GB.
  - ShareFile Clients versuchen immer, eine Hauptversion (Veröffentlichung) einer Datei einzuchecken. 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 zu lesen, muss ein SharePoint-Benutzer über Leseberechtigung verfügen.
- Benutzergeräte: Aktuelle Informationen zur Benutzergeräteunterstützung für StorageZone Connector finden Sie im ShareFile Wissensdatenbank.

Speicherzonen-Connector für die SharePoint-Authentifizierung

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

- Standard

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

- Verhandeln (Kerberos)
- Windows-Herausforderung/Antwort (NTLM)

ShareFile Mobile Clients verwenden die Standardauthentifizierung über HTTPS, um sich beim Storage Zones Controller oder DMZ-Proxy zu authentifizieren. Single Sign-On bei SharePoint unterliegt den Authentifizierungsanforderungen, die auf dem SharePoint-Server festgelegt sind. So verwenden Sie die Kerberos- oder NTLM-Authentifizierung auf dem SharePoint-Server: Konfiguration des Domänencontrollers, sodass er dem StorageZones Controller für die Delegierung vertraut.

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

Bei Bereitstellungen mit Citrix ADC ist es möglich, die grundlegende Authentifizierung am Citrix ADC zu beenden und dann andere Authentifizierungstypen am StorageZones Controller durchzuführen.

Speicherzonen-Connector für Netzwerkdateifreigaben

Der Speicherzonenconnector für Netzwerkdateifreigaben ist ein optionales Feature, das Sie auf einem StorageZones Controller aktivieren.

Anforderungen:

- ShareFile Enterprise oder Citrix Endpoint Management Konto.
- Der Speicherzonen-Connector-Server muss ein Domänenmitglied in derselben Gesamtstruktur wie die Netzwerk-Dateiserver sein.
- Die Webserverrolle (IIS) und ASP.NET 4.x. Weitere Informationen finden Sie unter Vorbereiten des Servers für ShareFile Daten.
- Benutzergeräte: Aktuelle Informationen zur Benutzergeräteunterstützung für StorageZone Connector finden Sie imShareFile Wissensdatenbank.

Connector für die Authentifizierung von Netzwerkdateifreigaben

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

- Verhandeln (Kerberos)
- Windows-Herausforderung/Antwort (NTLM)

So verwenden Sie die Kerberos- oder NTLM-Authentifizierung auf dem StorageZones Controller:Konfiguration des Domänencontrollers, sodass er dem StorageZones Controller für die Delegierung vertraut.

Bei Bereitstellungen mit Citrix ADC: Konfigurieren Sie den Connector für Negotiate (Kerberos) und NTLM-Authentifizierung, um Benutzern ein einmaliges Anmelden zu ermöglichen, wenn Citrix ADC für die Standardauthentifizierung konfiguriert ist.

PowerShell -Skripts und -Befehle

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

- Führen Sie die Skripts in der 32-Bit-Version (x86) von PowerShell aus.
- Die besten Ergebnisse erzielen Sie, wenn Sie ein Upgrade auf PowerShell 4.0 durchführen, das in Windows Management Framework 4.0.

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

Installieren

June 11, 2020

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 StorageZones Controller 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 StorageZones Controllers an eine Speicherzone

    Um eine Speicherzone für hohe Verfügbarkeit zu konfigurieren, schließen Sie mindestens zwei StorageZones Controller an.

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 den StorageZones Controller

June 11, 2020

NetScaler, Version 10.1 Build 120.1316.e und höher, enthält einen Assistenten, der Sie zur Eingabe grundlegender Informationen über Ihre Storage Zones Controller Umgebung auffordert. Dann generiert es eine Konfiguration, die:

- Lastverteilung des Datenverkehrs über StorageZones Controller hinweg
- Bietet Benutzerauthentifizierung für StorageZone Connector
- Validiert URI-Signaturen für ShareFile-Uploads und -Downloads
- Beendet SSL-Verbindungen an der Citrix ADC-Appliance

Das Diagramm zeigt die folgenden Citrix ADC Komponenten, die mit der Konfiguration erstellt wurden:

- **Citrix ADC Content Switching Virtual Server —** Sendet Benutzeranforderungen für Daten von ShareFile und von StorageZone Connector an den entsprechenden virtuellen Citrix ADC Load Balancing Server.
- **Citrix ADC Load Balancing Virtual Server:** Lastenausgleich für den Datenverkehr für die Storage Zones Controller und verarbeitet außerdem Folgendes:
  - Bei Anforderungen für Daten aus Ihrem privaten Datenspeicher führt ein virtueller Lastausgleichsserver eine Hashvalidierung durch, um sicherzustellen, dass gültige URI-Signaturen bei eingehenden Anforderungen vorhanden sind.
  - Bei Anforderungen von Daten von StorageZone Connector führt ein virtueller Lastausgleichsserver die Benutzerauthentifizierung durch. Es stoppt eine Benutzeranforderung am Citrix ADC, authentifiziert den Benutzer und führt dann eine einmalige Anmeldung des Benutzers beim StorageZones Controller durch.

  Obwohl die Authentifizierung bei Citrix ADC optional ist, ist dies eine empfohlene Best Practice.

Ab Storage Zones Controller 4.0 können Administratoren eingehende Verbindungen zu den Storage Zones Controllern auf TLS v1.2 beschränken. Wenn Protokolle vor TLS v1.2 für eingehenden Datenverkehr zum StorageZones Controller deaktiviert sind, müssen alle Clientsoftwarekomponenten, die mit der Speicherzone interagieren, auch TLS v1.2 unterstützen. Klicken Sie hier für weitere Informationen und Konfigurationshinweise.

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

Das Setup 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. Weitere Information finden Sie unter klicken Sie hier.

Voraussetzungen

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

Konfigurieren von Citrix ADC für StorageZones 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 für ShareFile einrichten.

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

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 NAT (Network Address Translation) -Zuordnung von Ihrer externen Firewall-Adresse zu dieser DMZ-IP-Adresse definieren.
ShareFile Daten	Diese Option ist aktiviert und weist darauf hin, dass Sie die Citrix ADC Verbindung für Speicherzonen für ShareFile Daten verwenden.
StorageZone Connector 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 oder für eingeschränkte Zonen mit einem externen Hostnamen müssen Zertifikate öffentlich vertrauenswürdig und nicht selbstsigniert sein.

Option	Beschreibung
IP-Adresse des StorageZones Controller	Die internen IP-Adressen für einen oder mehrere StorageZones Controller-Server. Diese IP-Adressen definieren die StorageZones 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 für jeden StorageZones Controller-Server eine interne IP-Adresse ein. Wenn Sie Citrix ADC nur für SSL und Authentifizierung verwenden möchten, geben Sie nur eine IP-Adresse ein.
Port und Protokoll	Der Port und das Protokoll, das für die Kommunikation vom Citrix ADC zu StorageZones Controllern verwendet wird.
Die IP-Adresse des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung (Citrix ADC AAA)	Eine nicht verwendete 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 des 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.
Auszeit	Die maximale Anzahl von Sekunden, die der Citrix ADC auf eine Antwort vom LDAP-Server wartet. Der Standardwert beträgt 3 Sekunden. Der Mindestwert beträgt 1 Sekunde.
Single Sign-On-Domäne	Der Active Directory Domänenname.
Basis-DN (Standort der Benutzer)	Der LDAP Base Distinguished Name (DN), in dem Benutzer gespeichert werden. Geben Sie den DN in der allgemeinen Form an: CN=Benutzer, dc=domain, dc=net

Option	Beschreibung
Administrator binden DN und Kennwort	Ein Administratorkonto, das über Berechtigungen für die 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 wird sAMAccountName verwendet, wodurch Benutzer sich mit ihren Benutzernamen anmelden können. Damit Benutzer ihre E-Mail-Adresse eingeben müssen, um sich anzumelden, ändern Sie dieses Feld in UserPrincipalName.

Konfigurieren von Citrix ADC für eingeschränkte Zonen oder Webzugriff auf Connectors

Um eingeschränkte Zonen oder den Webzugriff auf StorageZone Connector zu unterstützen, müssen Sie zusätzliche Citrix ADC Konfiguration durchführen, nachdem Sie den Citrix ADC for ShareFile Assistenten abgeschlossen haben.

- Erstellen und konfigurieren Sie einen dritten virtuellen Citrix ADC Lastenausgleich, mit dem sichergestellt wird, dass ShareFile Clients Anmeldeinformationen nur senden, wenn sie an einer vertrauenswürdigen ShareFile-Domäne angemeldet sind.

  Der StorageZones Controller verwendet den CORS-Standard (Cross-Origin Resource Sharing), um die erforderliche Sicherheit für Anforderungen an eingeschränkte Zonen und von der ShareFile e-Weboberfläche bis hin zu StorageZone Connector bereitzustellen. CORS verwendet HTTP-Header, damit Client und Server genug voneinander wissen können, um festzustellen, ob eine Anfrage oder Antwort erfolgreich sein soll.

  Wie in den folgenden Schritten beschrieben, konfigurieren Sie den zusätzlichen virtuellen Server so, dass der anonyme Zugriff von Clients für das HTTP OPTIONS-Verb erlaubt wird. Die OPTIONS-Anforderung wird an den StorageZones Controller ohne Authentifizierung und ohne HTTPS-Callouts weitergeleitet, um die Signatur zu validieren. Die CORS-Preflight-Überprüfung überprüft die Domänenvertrauensstellung, bevor die Anmeldeinformationen gesendet werden.

  Ein Verständnis von CORS ist nicht erforderlich, um die Konfiguration durchzuführen. Weitere Informationen zu CORS finden Sie jedoch unter http://enable-cors.org/.

Die Verwendung von Internet Explorer für den Webzugriff auf Connectors in eingeschränkten Zonen erfordert die Konfiguration von Internet Explorer.

- Um den Webzugriff auf StorageZone Connector zu unterstützen, fügen Sie der Inhaltswechselrichtlinie, 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 **Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server**.
   b) Klicken Sie auf 'Hinzufügen'.
   c) Geben Sie die folgenden Werte an:

Option	Wert
Name	Ein Richtlinienname, z. B. SF_ZONE_OPTIONS
Protokoll	SSL
IP-Adresstyp	Nicht adressierbar

   d) Klicken Sie durch, um den virtuellen Server zu erstellen.
   e) So binden Sie dieselben Dienste wie die virtuellen Lastausgleichsserver, die vom Assistenten erstellt wurden: Klicken Sie im Fenster "Virtueller Server für den Lastenausgleich" 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 > Policies.
   b) Klicken Sie im Detailbereich auf Hinzufügen, und geben Sie dann die Werte Name, virtueller Ziel-LB-Zielserver und Ausdruck an. Klicken Sie auf **Ausdruckseditor**, und erstellen Sie diesen Ausdruck. Wählen Sie **HTTP**. Wählen Sie **REQ**. Wählen Sie **METHOD**aus. 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 gerade 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 klicken Sie auf **Bearbeiten**.
   c) Navigieren Sie zum Abschnitt Content-Switching-Richtlinien-Bindung, und klicken Sie auf 2 Richtlinien für die Inhaltsvermittlung.
   d) Klicken Sie auf **Bindung hinzufügen**.

e) Wählen Sie die neue Inhaltsrichtlinie aus, und wählen Sie den virtuellen Ziellastenausgleich Server 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 aufweist.
Die Richtlinie mit dem niedrigsten Wert hat die höchste Priorität und wird daher zuerst behandelt.

4. Aktualisieren Sie die Richtlinie für den Datenverkehr zu StorageZone Connector (_SF_CIF_SP_CSPOL):
   a) Navigieren Sie zu **Traffic Management > Content Switching > Policies**.
   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 (_SF_SZ_CSPOL) verwendet wird:
   a) Navigieren Sie zu **Traffic Management > Content Switching > Policies**.
   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 nur Lesezugriff

Um die Freigabe mit nur Ansichten zu unterstützen, müssen Benutzer auf Ihren Microsoft Office Web Apps Server (OWA) zugreifen können. Wenn der OWA-Server extern über eine eigene Adresse

zugänglich ist, sollte keine zusätzliche Citrix ADC Konfiguration für den Storage Zones Controller erforderlich sein.

Wenn Sie den Storage Zones Controller und Office Web App Server mithilfe von Citrix ADC Richtlinien für die Inhaltsvermittlung 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 den extern zugänglichen OWA-Server weitergeleitet wird.

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

So erstellen und konfigurieren Sie einen zusätzlichen virtuellen Citrix ADC Lastausgleichsserver:

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 **Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server**.
    - Klicken Sie auf **Hinzufügen**.
    - Geben Sie die folgenden Werte an:

Option	Wert
Name	Ein Richtlinienname, z. B. SF_OWA_vServer
Protokoll	SSL
IP-Adresstyp	Nicht adressierbar

    - Klicken Sie 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 > Service auswählen**. Aktivieren Sie das Kontrollkästchen neben dem Dienst, den Sie im vorherigen Schritt erstellt haben.
    - Klicken Sie auf **Auswählen**.
    - Klicken Sie auf **Bind**.
3. Erstellen Sie eine neue Richtlinie, die zum Weiterleiten des Datenverkehrs an Ihren OWA-Server verwendet wird.
    - Navigieren Sie zu **Traffic Management > Content Switching > Policies**.
    - Wählen Sie **Hinzufügen**.

- Benennen Sie die Richtlinie.
- Fügen Sie 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 der 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 Richtlinien für die Inhaltsvermittlung aus.
   - Ändern Sie die Priorität der Richtlinien so, dass die (Beispiel) “_SF_OWA” -Richtlinie an dritter Stelle steht.

Priorität	Richtlinienname
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 Storage Zones Controller Dienst

Standardmäßig pingt Citrix ADC den StorageZones 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 StorageZones Controller, obwohl es nicht mit ShareFile kommuniziert.

Um die ausgehende Konnektivität des StorageZones Controller mit ShareFile zu überprüfen, können Sie einen Monitor erstellen, der heartbeat.aspx prüft und ihn für jeden StorageZones 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 für ShareFile Assistenten erstellt. Der Dienstname enthält die IP-Adresse des Controller, z. B. _SF_SVC_IP-Adresse.

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

Überprüfen der Citrix ADC Konfiguration

Nachdem Sie den Assistenten abgeschlossen haben, wechseln Sie zu **Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server**, um den Status der virtuellen Lastausgleichsserver anzuzeigen, die vom Assistenten erstellt wurden.

Anzeigen des Durchsatzes von ShareFile Anforderungen über Citrix ADC

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

Manuelles Konfigurieren von Citrix ADC

June 11, 2020

Ab Version 10.1 Build 120.1316 enthält Citrix ADC einen Assistenten, der die Einstellungen konfiguriert, die für Storage Zones Controller Daten und Konnektoren erforderlich sind.

In den Schritten in diesem Abschnitt werden die Citrix ADC Einstellungen beschrieben, die für den StorageZones Controller erforderlich sind. Alle Links sind für die NetScaler 10.1-Dokumentation vorgesehen. Ähnliche Themen sind für höhere Versionen von Citrix ADC verfügbar.

So überprüfen Sie auf gültige URI-Signaturen für alle eingehenden Nachrichten

1. Erstellen Sie eine HTTP-Callout namens 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 Anforderung an den Server auf **Attributbasiert** , und klicken Sie dann auf **Anforderungsattribute konfigurieren**.
   c) Wählen Sie **Methode abrufen**aus.
   d) Geben Sie unter Hostausdruck die IP-Adresse des virtuellen Servers oder die Host-IP-Adresse für einen der StorageZones Controller ein.

e) Geben Sie unter 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-Legende konfigurieren zurück.

g) Wählen Sie unter Serverantwort den **Rückgabetyp "Bool" aus**.

h) Geben Sie unter Ausdruck Folgendes ein, um Daten aus der Antwort zu extrahieren: `HTTP.RES.STATUS.EQ(200).NOT`

i) Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter HTTP-Callouts.

2. Führen Sie die vorstehenden Schritte aus, um eine HTTP-Callout namens sf_callout_y zu konfigurieren. Verwenden Sie die gleichen Einstellungen mit Ausnahme des Ausdrucks:
   - Geben Sie unter URL Stem Expression Folgendes ein: `"/validate.ashx?RequestURI="+ HTTP.REQ.URL.HTTP\\_URL\\_SAFE. B64ENCODE + "\\&h="`
3. Konfigurieren einer Responderrichtlinie:
   a) Wählen Sie im Dialogfeld Responderrichtlinie konfigurieren: Wählen Sie für Aktion die Option Drop.
   b) Geben Sie unter Ausdruck Folgendes 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 der Responderrichtlinie an den virtuellen Load Balancer-Server und konfigurieren SSL-Sitzungsbasierte Persistenz.

So laden Sie den Lastausgleich ein

1. Konfigurieren des tokenbasierten Lastenausgleichs.

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

   Tokenbasierter Lastausgleich ist für StorageZones Controller in einer Hochverfügbarkeitsbereitstellung erforderlich. Round-Robin-Lastenausgleich führt zu zeitweiligen Download- oder

Upload-Fehlern, da eine Clientanforderung für einen Upload oder Download an einen anderen StorageZones Controller als den, der die Autorisierungsanforderung von ShareFile.com erhalten hat, weitergeleitet werden kann.

2. Konfigurieren Sie Citrix ADC zum Beenden von SSL-Verbindungen.

   Weitere Informationen finden Sie unter Konfigurieren des SSL-Abladens und deren Unterthemen.

So konfigurieren Sie Inhaltsumschaltung und Authentifizierung für Connectors

1. Aktivieren Sie das Umschalten von Inhalten, wie unter beschrieben Aktivieren der Inhaltsumschaltung.
2. Erstellen Sie eine Richtlinie zum Umschalten von Inhalten für Benutzeranforderungen für ShareFile Daten aus Ihrer lokalen Speicherzone:
   a) Geben Sie im Dialogfeld Richtlinie für die Inhaltsumschaltung konfigurieren einen Namen für die Inhaltswechselrichtlinie ein. In diesen Schritten wird der Name Data_Requests verwendet.
   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 Inhaltswechselrichtlinie für Benutzeranforderungen für Daten, auf die über StorageZone Connector zugegriffen wird.
   a) Geben Sie im Dialogfeld Richtlinie für die Inhaltsumschaltung konfigurieren einen Namen für die Inhaltswechselrichtlinie an. In diesen Schritten wird der Name Connector_Requests verwendet.
   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 Controller ersetzen.
   c) Klicken Sie auf **OK**.
4. Erstellen eines virtuellen Servers zum Umschalten von Inhalten.

5. Legen Sie die Richtlinienziele für die Inhaltsvermittlung fest:
   - Geben Sie im Dialogfeld Virtuellen Server konfigurieren (Content Switching) für die Richtlinie Data_Requests den virtuellen Lastausgleichsserver für Speicherzonen für ShareFile Daten an.

     Dieser virtuelle Load Balancer Server ist derjenige, an den Sie die Responderrichtlinie in Schritt 4 von So überprüfen Sie auf gültige URI-Signaturen für alle eingehenden Nachrichten und Lastenausgleich gebunden haben.
   - Geben Sie für die Richtlinie Connector_Requests den virtuellen Load Balancer für StorageZone Connector an.
6. Konfigurieren Sie den virtuellen Authentifizierungsserver für StorageZone Connector:

   Obwohl die Authentifizierung bei Citrix ADC optional ist, ist dies eine empfohlene Best Practice.

   a) Erweitern Sie im Navigationsbereich Lastenausgleich, wählen Sie den Namen des virtuellen Load Balancer-Servers für StorageZone Connector 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-basierte Authentifizierung, und wählen Sie dann den virtuellen Authentifizierungsserver aus.

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

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

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

      Es wird ein Timeout-Wert von 240 Minuten empfohlen. Der Mindestwert sollte größer als 10 Minuten sein.

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

   Geben Sie unter SSO-Namensattribut **userPrincipalName**ein.

   Weitere Hinweise zu anderen Einstellungen finden Sie unter Authentifizierungsrichtlinien.
8. Konfigurieren Sie eine Authentifizierungsrichtlinie für den gerade erstellten Authentifizierungsserver:

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

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 unter Anmeldeinformationsindex **PRIMARY** aus.
   d) Geben Sie in der Single Sign-On-Domäne den Domänennamen für den 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 einer Sitzungsrichtlinie für Single Sign-On:
    a) Geben Sie im Dialogfeld Sitzungsrichtlinie konfigurieren einen Namen für die Richtlinie ein.
    b) Wählen Sie unter **Anforderungsprofil**den Namen des Sitzungsprofils aus, das im vorherigen Schritt konfiguriert wurde.
    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 **ProtokollSSL**.
    c) Aktivieren Sie das Kontrollkästchen Benutzer authentifizieren.
    d) Klicken Sie unter Authentifizierungsrichtlinien auf **Primär**, und wählen Sie dann die in Schritt 7 konfigurierte Authentifizierungsrichtlinie aus.
    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 Konfigurieren des virtuellen Authentifizierungsservers.

Erstellen einer Netzwerkfreigabe für die private Datenspeicherung

June 11, 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. Sie sollten jedoch den IIS-Anwendungspool und die Citrix ShareFile Dienste mit dem Netzwerkdienstkonto ausführen.

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

> **Vorsicht:**
>
> 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

June 11, 2020

Die Webserverrolle (IIS) und das in diesem Abschnitt beschriebene ASP.NET-Setup sind für Speicherzonen für ShareFile Daten und für StorageZone Connector erforderlich. Diese Anweisungen basieren auf Windows Server 2012. Die Anweisungen für Windows Server 2008 finden Sie im Legacy-Dokumentation für Storage Zones Controller.

Microsoft .NET-Version aktualisieren

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

- **Storage Zones 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 Webserverrolle (IIS) und den ASP.NET-Rollendienst

1. Melden Sie sich auf dem Server an, auf dem Sie den Storage Zones 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 Features hinzufügen**, um den Assistenten zum Hinzufügen von Rollen und Features zu öffnen.
3. Klicken Sie im Assistenten zum Hinzufügen von Rollen und Features auf **Weiter**.

4. Klicken Sie auf der Seite Installationstyp auswählen auf Rollenbasierte oder featurebasierte Installation, und klicken Sie dann auf **Weiter**.
5. Wählen Sie auf der Seite Zielserver auswählen den Server aus dem Serverpool aus, und klicken Sie dann auf **Weiter**.
6. Aktivieren Sie auf der Seite Serverrollen auswählen das Kontrollkästchen Webserver (IIS) und Windows Server Update Services Kontrollkästchen und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Features hinzufügen**, um die für IIS erforderlichen Features hinzuzufügen.
8. Klicken Sie auf **Features hinzufügen**. Die Seite Features auswählen wird angezeigt.
9. Wählen Sie die erforderlichen Einstellungen aus, die im folgenden Bildschirm angezeigt werden, und klicken Sie dann auf **Weiter**.
10. Klicken Sie auf der Seite Webserverrolle (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.

So konfigurieren Sie IIS

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

1. Öffnen Sie die IIS-Manager-Konsole, klicken Sie auf den Speicherzone Controller -Serverknoten, und doppelklicken Sie dann auf ISAPI- und CGI-Einschränkungen.
2. Legen Sie jeden ASP.NET-Eintrag auf Zulässig fest.
3. Überprüfen Sie, ob ein Domänenserver oder ein öffentliches Zertifikat auf dem Server installiert ist: Klicken Sie in der IIS-Manager-Konsole auf den Serverknoten des StorageZones Controller, und doppelklicken Sie dann auf Serverzertifikate.

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

   > **Hinweis:**
   >
   > Wenn Sie ein Citrix Gateway oder ein ähnliches Gerät mit Storage Zones 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 klicken Sie dann auf **Bindungen**.
5. Klicken Sie auf Hinzufügen, und konfigurieren Sie die Websitebindung wie folgt:
   - Der Typ ist https.
   - Die IP-Adresse lautet “Alle nicht zugewiesen”.
   - Der Port ist 443.
   - SSL-Zertifikat ist Ihr installiertes Zertifikat.
6. Um die Webserver-Verbindung 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 lokalen Hostnamen im URL-Header übereinstimmt. Dies wird erwartet und Sie können sicher zur Website fortfahren.
7. Wenn Sie den StorageZones Controller auf einer VM installieren, erstellen Sie einen Snapshot der VM.

Installieren des StorageZones Controller und Erstellen einer Speicherzone

June 11, 2020

> **Wichtig:**
>
> Stellen Sie sicher, dass Ihre Umgebung die erfüllt, Systemanforderungen bevor Sie die Installation starten.

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

Beim Konfigurieren eines primären StorageZones Controller können Sie entweder oder beide dieser Funktionen aktivieren:

- Speicherzonen für ShareFile Daten, um den privaten Datenspeicher anzugeben, entweder eine private Netzwerkfreigabe oder ein unterstütztes Speichersystem eines Drittanbieters.
- StorageZone Connector, um Benutzern Zugriff auf Dokumente auf SharePoint-Websites oder bestimmte Netzwerkdateifreigaben zu gewähren.

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

1. Führen Sie Download und Installation der StorageZones Controller-Software durch:

- Melden Sie sich auf der ShareFile Download-Seite unter http://www.citrix.com/downloads/sharefile.html an und laden Sie das neueste StorageZones Controller Installationsprogramm herunter.

> **Hinweis:**
>
> Durch die Installation des StorageZones Controller 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 des ShareFile StorageZones Controller wird gestartet.
   - Führen Sie für Mandantenfähigkeit 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) aktualisieren, damit sie mit der Nummer der MSI übereinstimmt, die Sie installieren möchten.

   - Antworten Sie auf die Eingabeaufforderungen. Deaktivieren Sie nach Abschluss der Installation das Kontrollkästchen **Speicherzonen Controller Konfigurationsseite starten**, und klicken Sie dann auf **Fertig stellen**.
3. Starten Sie den Storage Zones 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 StorageZones Controller klonen möchten, erstellen Sie zunächst ein Datenträgerimage, bevor Sie mit der Konfiguration des StorageZones Controllers 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 anderen Wert unter diesem Schlüssel.
  - Wertname: **S3ForcePathStyle**
  - Werttyp: **REG_SZ**
  - Wertdaten: **true**
- Starten Sie den Anwendungspool des StorageZones Controller (StorageCenterAppPool) neu.
- Sammeln Sie die folgenden Informationen aus Ihrem S3-kompatiblen Speichersystem:
  - Der Name eines S3-Buckets, der für ShareFile DataAccess-Schlüssel-ID verwendet werden soll
  - Zugriffs-Schlüssel-ID
  - Geheimer Zugriffsschlüssel

7. Fahren Sie mit den folgenden Schritten fort, um eine neue Speicherzone zu erstellen. Wählen Sie Amazon S3 als permanenten Speicherort. Der Storage Zones Controller verwendet anstelle des tatsächlichen Amazon S3 Dienstes die benutzerdefinierte Endpunktadresse, die Sie eingegeben haben. Wählen Sie beim Konfigurieren der S3-Details den Bucket-Namen aus, den Sie zuvor erstellt haben.
8. Navigieren Sie zur Storage Zones Controller Konsole.
9. Öffnen `http://localhost/configservice/login.aspx` oder starten Sie das Konfigurationstool über die Startseite oder das Menü. Weitere Informationen zum Verwenden der Verknüpfung “Startbildschirm” in Windows 8 finden Sie unter Verwalten von StorageZones Controllern.
10. Geben Sie auf der **Anmeldeseite für Storage Zones Controller** die **E-Mail-Adresse**, **das Kennwort** und die **vollständige Konto-URL FQDN-Unterdomäne** ein `subdomain.sharefile.com`, z. B. `subdomain.sharefile.eu` oder für Ihr Konto . Klicken Sie auf **Anmelden**.
11. Klicken Sie zum Einrichten des primären StorageZones Controller auf **Neue Zone erstellen** , und geben Sie die Zoneninformationen an:

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

Option	Beschreibung
Primäre Zone Controller	Standardmäßig 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 beim Konfigurieren eines sekundären Speicherzonen-Hosts haben, stellen Sie sicher, dass Sie die ConfigService-URL in einem lokalen Browser auf diesem Server ohne SSL-Fehler auflösen können. localhost löst in die IP-Adresse des Servers auf. Sie können stattdessen einen Servernamen angeben (z. B. `https://servername.subdomain.com/ConfigService`). Der Servername muss durch einen sekundären StorageZones Controller-Server aufgelöst werden können.
Hostname	Eine eindeutige Kennung für Ihren Storage Zones Controller. ShareFile empfiehlt, den Serverhostnamen als Bezeichner zu verwenden. Dies sollte ein Anzeigename und nicht der FQDN sein. 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 senden, validiert ShareFile die Adresse.

12. Führen Sie die folgenden Schritte aus, um den privaten Datenspeicher anzugeben.
    - Aktivieren Sie das Kontrollkästchen **Speicherzonen für ShareFile Daten aktivieren**.
    - Deaktivieren Sie das Kontrollkästchen, um eine Standardzone zu konfigurieren.

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

Der StorageZones Controller verwendet die Anmeldeinformationen des Dienstkontos, um eine Verbindung mit dem vertrauenswürdigen Active Directory Domänenserver für die E-Mail-Adressensuche herzustellen.

- Wählen Sie ein Speicher-Repository aus.

13. Wenn Sie StorageZone Connector 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 nach der Registrierung der Speicherzone:
    - Öffnen Sie den Windows-Registrierungseditor (**Ausführen > regedit.exe**).
    - Suchen Sie den `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storagezone\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 anderen Wert unter diesem Schlüssel.
        - Wertname: **S3ForcePathStyle**
        - Werttyp: **REG_SZ**
        - Wertdaten: **true**
    - Starten Sie den Anwendungspool des StorageZones Controller (StorageCenterAppPool) neu.
15. So aktivieren Sie StorageZone Connector:

    Durch Aktivieren der Connectors werden die IIS-Apps “cifs” (Connector für Netzwerkdateifreigaben) und “sp” (Connector für SharePoint) erstellt.

    - Aktivieren Sie das Kontrollkästchen für jeden Connectortyp, den Sie verwenden möchten: Speicherzonenconnector für Netzwerkdateifreigaben aktivieren und Speicherzonencon-

nector für SharePoint aktivieren. Weitere Informationen zu den Konnektoreinstellungen finden Sie unter Konfigurieren von StorageZone Connectorin diesem Abschnitt.

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

16. Informationen zum Konfigurieren von Controllern für sekundäre Speicherzonen finden Sie unter Verwalten von StorageZones Controllern.

> **Wichtig:**
>
> Ein StorageZones Controller ist auf Ihrem lokalen Standort installiert und Sie sind für die Sicherung verantwortlich. Um Ihre Bereitstellung zu schützen, sollten Sie einen Snapshot des StorageZones Controller-Servers erstellen Sichern der Konfiguration des Storage Zones Controller und Vorbereiten des StorageZones Controller für die Disaster Recovery.

Konfigurieren von Speicherzonen für ShareFile Daten

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

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

Einstellungen für die Netzwerkfreigabe

Option	Beschreibung
Speicher-Repository	Wählen Sie Lokale Netzwerkfreigabe. Nachdem Sie die Zone erstellt haben, können Sie die Option “Speicher-Repository” nicht mehr ändern. Um beispielsweise von einer lokalen Netzwerkfreigabe zu einem Drittanbieterspeicher zu wechseln, müssen Sie eine neue Zone erstellen.

Option	Beschreibung
Speicherort der Netzwerkfreigabe	Der UNC-Pfad zu der Netzwerkfreigabe, die Sie für die private Datenspeicherung und für Daten wie Verschlüsselungsschlüssel, Dateien in der Warteschlange und andere temporäre Elemente verwenden. Geben Sie den Pfad im Formular an `\\server\share`. StorageZones Controller, die zu derselben Speicherzone gehören, müssen dieselbe Dateifreigabe für die Speicherung verwenden. Achtung: 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 auf die Netzwerkfreigabe mit dem auf der Konfigurationsseite angegebenen Netzwerkfreigabebenutzername/-kennwort zu. Wenn auf der Konfigurationsseite kein Benutzername/Kennwort für die Netzwerkfreigabe angegeben wird, wird standardmäßig das Netzwerkdienstkonto 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
Benutzername für Netzwerkfreigabe und Kennwort für Netzwerkfreigabe	Die Anmeldeinformationen für den UNC-Pfad Ihres Netzwerkfreigabe-Standorts. Wenn Sie anstelle des Netzwerkdienstkontos für den Zugriff auf die Freigabe ein benanntes Benutzerkonto verwenden möchten, geben Sie diese Anmeldeinformationen an. Sie können den IIS-Anwendungspool und die Citrix ShareFile Dienste weiterhin mit dem Netzwerkdienstkonto ausführen.
Verschlüsselung aktivieren	Aktivieren Sie das Kontrollkästchen nur, wenn Sie den auf der 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, wird empfohlen, die Dateien auf der Freigabe nicht zu verschlüsseln. Diese Einstellung bezieht sich nicht auf Metadaten. Metadaten sind 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 die Festplatte durch Drittanbieter-Tools wie Antivirus-Scanner und Filer-Tools, einschließlich Datendeduplizierungstools, unlesbar. ShareFile verwendet einen Dateiverschlüsselungsschlüssel, um die Gültigkeit von Download-Anforderungen zu bestätigen und den Speicher zu verschlüsseln.

Option	Beschreibung
Passphrase	Eine Phrase, die zum Schutz des Dateiverschlüsselungsschlüssels verwendet wird. Achten Sie darauf, die Passphrase und den Verschlüsselungsschlüssel an einem sicheren Ort zu archivieren. Sie müssen dieselbe Passphrase für jeden StorageZones Controller in einer Zone verwenden. Die Passphrase ist nicht identisch mit Ihrem Kontokennwort und kann nicht wiederhergestellt werden, wenn sie verloren geht. Wenn Sie die Passphrase verlieren, können Sie Speicherzonen nicht neu installieren, zusätzliche StorageZones Controller mit der Speicherzone verbinden oder die Speicherzone wiederherstellen, wenn der Server ausfällt. Hinweis: Der Verschlüsselungsschlüssel wird im Stammverzeichnis des freigegebenen Speicherpfads angezeigt. Der Verlust der Verschlüsselungsschlüsseldatei Sckeys.txt bricht sofort den Zugriff auf alle Speicherzonen-Dateien. Stellen Sie sicher, dass Sie die Verschlüsselungsschlüsseldatei als Teil Ihrer normalen Rechenzentrumsverfahren sichern.

Konfigurationseinstellungen für gemeinsam genutzten Cache

Option	Beschreibung
Speicherort des freigegebenen Caches	den Pfad zu einer Netzwerkfreigabe, die Ihren Speicher-Cache 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. Achtung: 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, für das der Citrix ShareFile Verwaltungsdienst konfiguriert ist) muss vollen Zugriff auf diesen Speicherort haben.
Kennwort für freigegebene Cache-Anmeldung und freigegebener Cache	Die Anmeldeinformationen für den UNC-Pfad des freigegebenen Cache-Speicherorts.
Verschlüsselung aktivieren	Aktivieren Sie das Kontrollkästchen, um die im freigegebenen Cache gespeicherten Dateien zu verschlüsseln.

Windows Azure-Speichercontainer-Einstellungen

Option	Beschreibung
Speicher-Repository	Wählen Sie Azure-Speichercontainer aus. Nachdem Sie die Zone erstellt haben, können Sie die Option “Speicher-Repository” nicht mehr ändern. Wenn Sie beispielsweise von einer lokalen Netzwerkfreigabe zu einem Azure-basierten Speicher wechseln möchten, müssen Sie eine neue Zone erstellen.

Option	Beschreibung
Kontoname	Der Name Ihres Azure-Speicherkontos. Diese Namen sind immer Kleinbuchstaben.
Zugriffs-Schlüssel	Der primäre oder sekundäre Zugriffsschlüssel für Ihren Azure-Speicher. Kopieren Sie den Schlüssel aus dem Fenster Zugriffsschlüssel verwalten im Windows Azure-Verwaltungsportal.
Überprüfen	Klicken Sie auf die Schaltfläche, um den Azure-Zugriffsschlüssel zu überprüfen. 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 wurde.

Amazon S3 Speicher-Bucket-Einstellungen

Option	Beschreibung
Speicher-Repository	Wählen Sie Amazon S3 Speicher-Bucket. Nachdem Sie die Zone erstellt haben, können Sie die Option “Speicher-Repository” nicht mehr ändern. Um beispielsweise von einer lokalen Netzwerkfreigabe zu Amazon S3 Speicher zu wechseln, müssen Sie eine neue Zone erstellen.
Zugriffs-Schlüssel-ID	Die Zugriffsschlüssel-ID für Ihren Amazon S3 Speicher.
Geheimer Zugriffsschlüssel	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 eine Verbindung mit dem SMTP-Server über eine sichere Verbindung herzustellen.
Benutzername und Kennwort	Der Benutzername und das Kennwort für Ihren lokalen SMTP-Server.
Authentifizierungsmodus	Der Standardauthentifizierungsmodus verwendet die sicherste verfügbare Methode, um vom StorageZones Controller mit dem SMTP-Server zu verbinden.
Adresse des Absenders	Die E-Mail-Adresse, die im Feld Von angezeigt wird.

Google Cloud-Plattform

Generieren Sie einen Zugriffsschlüssel und einen geheimen Schlüssel über die **Google Cloud Platform > Einstellungen > Interoperabilität**.

Legen Sie vor dem Ausführen der Speicherzonenkonfiguration den Registrierungswert **S3EndpointAddress** auf `https://storage.googleapis.com` fest und starten Sie IIS neu.

Option 1

Beschreibung

Speicher-Repository

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

Zugriffsschlüssel-ID

Die Access Key-ID aus Ihrem Google Cloud Platform Speicher.

Geheimer Zugriffsschlüssel

Das Geheimnis aus Ihrem Google Cloud Platform Speicher.

Überprüfen

Klicken Sie auf die Schaltfläche, um den geheimen Zugriffsschlüssel für Google Cloud Platform zu validieren. Sie können mit der Konfiguration erst fortfahren, wenn die Validierung abgeschlossen ist und die Liste **Bucket Name** 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 Google Cloud Platform validiert wurde.

Konfigurieren von StorageZone Connector

StorageZone Connector ermöglichen Benutzern Zugriff auf Dokumente auf SharePoint-Websites oder bestimmte Netzwerkdateifreigaben. Sie müssen keine Speicherzonen aktivieren, damit ShareFile Data StorageZone Connector verwenden können.

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

Sie können StorageZone Connector 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 der zulässigen Pfade oder Verweigerte Pfade an. Nachdem Sie Ihre Änderungen gespeichert haben, starten Sie den IIS-Server neu.

Eingehende Verbindungen zu StorageZone Connector werden zunächst anhand der zulässigen Pfade überprüft. Wenn die Verbindung zulässig ist, wird der Pfad mit den verweigerten Pfaden überprüft. Um beispielsweise Zugriff auf `\\myserver\teamshare` und alle Unterordner zu gewähren, geben Sie einen zulässigen Pfad von an `\\myserver\teamshare`.

- Alle Verbindungen sind standardmäßig zulässig, die durch den Wert “Zulässige Pfade” gekennzeichnet sind. Der Wert ist für Verweigerte Pfade nicht gültig.
- Wenn die zulässigen und verweigerten Pfade miteinander in Konflikt stehen, wird der restriktivste Pfad erzwungen.
- Einträge sind durch Kommas getrennt.
- Geben Sie für Connectors zu Netzwerkdateifreigaben die zulässigen UNC-Pfade an.

  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.

- 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 Connectors zu SharePoint 2010-Dokumentbibliotheken die URLs an (ohne Pfadabschlusszeichen, z. B. 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 Minimale Download-Strategie aktiviert ist) hat das folgende Format: `https://sharepoint.company.com/\\_layouts/15/start.aspx\##/Shared%20Documents/`.

Sicherheitsempfehlung zum Entfernen des Server-Headers

IIS/ASP.NET stellt standardmäßig den Server-Header in HTTP-Antworten zur Verfügung. Dieser Header könnte für einen Angreifer nützlich sein. 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 Installationsprogramm des StorageZones Controller diesen Header nicht automatisch entfernen. Wir können unseren Kunden jedoch Empfehlungen geben, diesen Header in unserer Dokumentation/Installationshandbuch für Speicherzonen zu entfernen.

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

Überprüfen der Konfiguration des StorageZones Controller

June 11, 2020

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 den Inhaltswechsel und den 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

June 11, 2020

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

- Um die Standardzone für Benutzerkonten anzugeben, die über AD bereitgestellt werden, öffnen Sie das Benutzerverwaltungsprogramm, und klicken Sie auf das Optionssymbol.
- Um eine Zone für Ordner auf Stammebene auszuwählen, öffnen Sie die ShareFile Administratorkonsole und wechseln Sie zu Benutzer verwalten. (Erfordert Mitgliedschaft in der Super-Benutzergruppe.)
- Um die Standardzone für einen einzelnen Benutzer zu ändern, öffnen Sie die ShareFile Administratorkonsole, und wechseln Sie zu Benutzer verwalten. (Erfordert Mitgliedschaft in der Super-Benutzergruppe.) Sie können Zonenberechtigungen auch auf der Seite Benutzer verwalten erstellen und verwalten.

Festlegen eines Proxyservers für Speicherzonen

June 11, 2020

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** .
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.

Konfigurieren des Domänencontrollers für die Vertrauensstellung des StorageZones Controllers für die Delegierung

June 11, 2020

> **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 des StorageZones Controller für Web App-Vorschauen, Miniaturansichten und schreibgeschütztes Sharing

June 11, 2020

Lokale 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 die Vorschauen von Citrix verwalteten oder von Microsoft verwalteten OWA-Servern gerendert.

> **Wichtig:**
>
> **Anforderungen an die Whitelisting:**
>
> `*.sf-api.com` muss Office Online Server für die Vorschau und Bearbeitung verfügbar sein, damit die Speicherzonen Version 5.0 oder höher ordnungsgemäß funktionieren.

Anforderungen

Unterstützte Dateitypen für die lokale 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 lokale Dateibearbeitung

- .docm, .docx, .odt

- .ods, .xlsb, .xlsm, .xlsx
- .odp, .ppsx, .pptx

Unterstützte Umgebungen

- Standard-Zonen
- Mehrmandanten-Zonen
- Webanwendung

Whitelisting /Netzwerküberlegungen

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

Um lokale Dateien zu bearbeiten, Dateiversionierung muss in Ihrem ShareFile Konto aktiviert sein.

Die Einstellung zum Aktivieren der Microsoft Office Online-Bearbeitung im Menü Erweiterte ShareFile Web App-Einstellungen wirkt sich nicht auf die Möglichkeit aus, lokale Dateien zu bearbeiten. Dieser spezifische Umschalter steuert **nicht** Ihre Fähigkeit, lokale Dateien zu bearbeiten, sondern gilt für die Bearbeitung von Dateien, die in einer öffentlichen Cloud gespeichert sind. Das Aktivieren der Bearbeitung von On-Prem-Dateien wird ausschließlich durch den Storage Zones Controller Admin gesteuert, indem die unten beschriebenen Schritte ausgeführt werden.

Microsoft-Server-Kompatibilität

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

Architektur- und Netzwerkdiagramm

1. Authentifizierter Benutzer fordert eine Dateivorschau in ShareFile an.
2. ShareFile gibt eine Umleitung zum Clientgerät mit Office Online Server-FQDN aus
3. Clientgerät leitet an Office Online Server-FQDN um. **Hinweis**: HTTPS-Verbindung, DNS sollte entweder einen Datensatz für interne Server-IP oder einen Datensatz für Load Balancer VIP mit anwendbarem Routing zwischen Clientgerät und jeder Firewall auf Port 443 haben.

4. Office Online Server verarbeitet Anforderung, macht API-Aufrufe an StorageZones Controller-Server. **Hinweis**: HTTPS-Verbindung, DNS sollte entweder einen Datensatz für interne Server-IP oder einen Datensatz für Load Balancer VIP mit anwendbarem Routing zwischen Clientgerät und jeder Firewall auf Port 443 haben.
5. StorageZones Controller Prüfungen `https://\<DNSname\>/hosting/discovery` sind erreichbar. Nur wenn erreichbar, sendet SZC API-Antworten zurück an Office Online Server. **Hinweis**: Der StorageZones Controller muss eine Verbindung mit dem Office Online Server herstellen. HTTPS-Verbindung zwischen beiden intern gehosteten Servern.
6. Der StorageZones Controller verbindet ausgehend mit der ShareFile e-API (sf-api.com). **Hinweis**: Dies ist eine obligatorische ausgehende Verbindung über jede Firewall, Proxy oder ausgehende 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 ausgehend mit ShareFile API her. **Hinweis**: Dies ist eine obligatorische ausgehende Verbindung über jede Firewall, Proxy oder ausgehende Routing-Appliance. Stellen Sie sicher, dass der Office Online Server ausgehend über HTTPS/443 mit den oben dokumentierten IP-Adressen kommunizieren kann.
8. Vorschau wird angezeigt.

Um Speicherzonen Controller Dateibyte an OOS streamen, anstatt OOS, die ShareFile Steuerebene zum Herunterladen des Inhalts 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 momentan **falsch**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.

Wenn Sie diese Option verwenden, wäre es richtig, wenn Sie angeben, dass kein eingehender Verkehr von der Steuerebene zu OOS vorhanden wäre?

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 im Vergleich zur anderen?

In diesem Ansatz lädt OOS Dateiinhalte nicht direkt herunter. Der StorageZones Controller lädt die Dateibytes zu OOS herunter und streamt sie. Somit erhöht es die Last auf den StorageZones Controller-Servern.

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

Aktivieren der lokalen Vorschau und Bearbeitung

Konfigurieren Sie den StorageZones Controller wie folgt, um die Dokument- und Bildvorschau im Browser, Miniaturansichten, die gemeinsame Nutzung der in vom Kunden verwalteten Speicherzonen gespeicherten Daten und die lokale Dateibearbeitung im Browser zu unterstützen:

1. Klicken Sie in der StorageZones Controller Konsole auf die Registerkarte **ShareFile Daten**.
2. Aktivieren Sie im Abschnitt **Konfiguration der lokalen Netzwerkfreigabe** die Option **Vorschau für Office-Webanwendungen konfigurieren**.
3. Geben Sie die externe URL Ihres Microsoft Office Web Apps-Servers (OWA) 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 auf die OWA-URL extern zugegriffen werden kann.
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:**
>
> Das Bearbeiten von lokalen Dateien Dateiversionierung muss für das ShareFile Konto aktiviert sein. Wenn die Dateiversionierung für das Konto deaktiviert ist, funktioniert die lokale Bearbeitung nicht.

Wichtig:

Synchronisierung der Uhr konfigurieren:

- 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.

Ändern von OWA URAL oder Deaktivieren der Vorschau:

- Eine der oben genannten Aktionen erfordert, dass der IIS-Dienst für jeden primären und sekundären Controller neu gestartet wird.

Einschränkungen

- Mobile Apps unterstützen die Bearbeitung im Browser nicht.
- Connectors unterstützen keine Browservorschauen.

WOPI-Vorschauen werden für VDR-Konten nicht unterstützt.

Informationen zum Konfigurieren des Citrix ADC für die reine View-Only Sharing finden Sie unter Konfigurieren Sie Citrix ADC für Storage Zones Controller.

Fehlerbehebung bei OWA und OOS Problemen

Wenn Sie Probleme bei der Vorschau oder Bearbeitung von On-Prem-Dateien haben, helfen Ihnen die folgenden Schritte bei der Identifizierung und Korrektur bestimmter Probleme.

Melden Sie sich zunächst bei der OWA- oder OOS-Maschine an, um Probleme bei der Konfiguration zu beheben.

1. Stellen Sie sicher, dass die Office WebApps oder OfficeOnline Windows-Dienste in services.msc ausgeführt werden.
2. Öffnen Sie die `http://localhost/hosting/discovery` Seite 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 in der Antwort eine WARNUNG oder FEHLER angezeigt wird, überprüfen Sie Ihre Konfigurationseinstellungen auf Fehler.

Überlegungen zum Netzwerk:

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

Konfigurieren von Multi-Tenant-Speicherzonen

June 11, 2020

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

Wenn Sie ein CSP mit einem Partnerkonto sind, das von ShareFile bereitgestellt wird, können Sie eine Multi-Tenant-Standardspeicherzone in Ihrer Domäne hosten, die eine unbegrenzte Anzahl von Mandanten unterstützt. Die Verwendung einer mehrmandantenfähigen Zone ermöglicht Folgendes:

- Stellen Sie jedem Mandanten ein einzigartiges ShareFile Konto zur Verfügung und nutzen Sie alle großartigen ShareFile-Funktionen wie benutzerdefiniertes Branding, Dateiaufbewahrungseinstellungen und Sicherheitseinstellungen.
- Verwalten Sie ein einzelnes Speicher-Repository für alle Mandanten.
- Schneller an Bord neuer Kunden und reduzieren die Kosten und Verwaltungskomplexität beim Erstellen einer separaten Speicherzone für jedes Kundenkonto.

Erstellen eines Partnerkontos

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

Um ein Partnerkonto zu erstellen, müssen Sie sich beim CSP-Programm registrieren und eine Lager-SKU bei Ihrem bevorzugten Distributor bestellen, mit der Sie ShareFile als Service anbieten können. Um sich auf das CSP-Programm zu bewerben, gehen Sie zu https://www.citrix.com/partner-programs/service-provider.html.

Wenn Sie bereits als CSP registriert sind und die entsprechende ShareFile für CSPs 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 Ihnen, einen generischen Administratorbenutzer für Ihr Partnerkonto zu erstellen. Auf diese Weise kann der Admin-Benutzer der offizielle Partner-Administrator aller Ihrer Kundenkonten sein. Stellen Sie sicher, dass der Admin-Benutzer dieses Dienstkontos die Berechtigung Mandanten verwalten aktiviert hat. Damit ermutigen wir Partner, diesen Partner-Admin jetzt zu erstellen, bevor Sie das Anfrageformular für das CSP-Kundenkonto ausfüllen (in Schritt 4).

Installieren und Einrichten einer Multi-Tenant-Speicherzone

- Erstellen Sie eine neue mehrmandanteneigene Speicherzone und ordnen Sie sie Ihrem Partnerkonto zu. Einzelheiten finden Sie unter Installieren des StorageZones Controller und Erstellen einer Speicherzone.
- Installieren Sie den StorageZones Controller im Multi-Tenant-Modus. Stellen Sie sicher, dass Sie

die folgende angegebene Eingabeaufforderung im Artikel Installieren ausführen, der im vorherigen Schritt erwähnt wird.

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

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

Konfigurieren Sie die neue Speicherzone und ordnen Sie sie Ihrem Partnerkonto zu

Weitere Informationen finden Sie unter Schritt 10 in Installieren des StorageZones Controller und Erstellen einer Speicherzone.

Melden Sie sich bei Ihrem Partnerkonto an, wo 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 Multi-Tenant-Speicherzone anzeigen lassen. Klicken Sie auf die Registerkarte **Admin-Einstellungen > Speicherzonen > Partner verwaltet**.

Mandantenkonten für die Multimandantenzone anfordern

Um Mandantenkonten anzufordern, füllen Sie das aus CSP-Kundenkonto-Anfrageformular.

Wenn Sie ein Mandantenkonto anfordern, müssen Sie auch einen Partner-Admin-Benutzer angeben. Dieser Partner-Administrator muss ein Admin-Benutzer in Ihrem Partnerkonto sein, wobei die Berechtigung Mandanten verwalten aktiviert ist. Wenn ein Mandantenkonto erstellt wird, wird dieser Partner-Admin-Benutzer automatisch für das Konto als Admin-Benutzer bereitgestellt und kann sich anmelden und das Mandantenkonto verwalten. Da es nicht zwei Benutzer in einem Konto mit derselben E-Mail-Adresse geben kann, kann die im Formular angegebene Partner-Admin-E-Mail nicht mit dem Kundenadministrator im selben Formular identisch sein.

Um den schnellsten Turnaround sicherzustellen, stellen Sie sicher, dass Sie die richtige Organisations-ID und den Namen der Multimandantenzone angeben, die Sie als Speicherzone für das Mandantenkonto verwenden möchten.

Sie erhalten eine E-Mail, nachdem Citrix die angeforderten Konten bereitgestellt hat. Die E-Mail enthält Details zur Unterdomäne des Mandanten und einen Aktivierungslink zum Einrichten des Zugriffs. ShareFile sendet Ihnen und den administrativen Benutzern Ihrer Kunden separate E-Mails.

Ihre Kunden können dann ShareFile verwenden. Alle neuen Benutzer, die für das Konto eines Mandanten bereitgestellt werden, verwenden die Multi-Tenant-Zone, die Sie als Standardspeicherort für die Dateien des Benutzers angegeben haben.

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

Diese Funktionalität wird in unterstützten Office Online Server-Umgebungen unterstützt. Klicken Sie hier für Setup-Informationen.

Connector-Freigabe

Diese Funktionalität wird von Multi-Tenant-Zonen unterstützt.

Mandanten verwalten

Innerhalb des Partnerkontos befindet sich ein Mandantenverwaltungs-Dashboard unter **Admin-Einstellungen > Erweiterte Einstellungen**. Mit diesem zentralisierten Dashboard können Sie den Status aller Mandanten 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 steht nur Benutzern in Ihrem Partnerkonto zur Verfügung, für die die Benutzerberechtigung **Mandanten verwalten** aktiviert ist.

Mehrmandantenbeschränkungen

Das Feature zur Verwaltung von ShareFile Informationsrechten (IRM) wird für mehrmandantengebende 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

June 11, 2020

> **Warnung**
>
> Wenn Sie StorageZones Controller 2.x verwenden, müssen Sie zuerst ein Upgrade auf Version 3.0.1 durchführen. Wenden Sie sich an, um von 2.x auf 3.0.1 zu aktualisieren Unterstützung bei der Unterstützung. Nachdem Sie ein Upgrade auf Version 3.0.1 durchgeführt haben, können Sie ein Upgrade auf die neueste Version durchführen.

Wenn diese Version installiert ist:	Tun Sie dies:
StorageZone Konnektoren 1.0	StorageZone Connectors 1.0 kann nicht aktualisiert werden. Deinstallieren Sie StorageZone Connectors 1.0 und installieren Sie den neuesten Storage Zones Controller
Storage Center 1.0	Aktualisieren Sie Storage Center 1.0 auf Storage Center 1.1. Stellen Sie dann sicher, dass Storage Center 1.1 korrekt konfiguriert ist und funktioniert, bevor Sie fortfahren. Aktualisieren Sie anschließend Storage Center 1.1 auf StorageZones Controller 2.0 Update 1. Aktualisieren Sie anschließend StorageZones Controller 2.0 Update 1 auf StorageZones Controller 3.0.1. Führen Sie schließlich ein Upgrade auf den neuesten StorageZones Controller durch.
Storage Center 1.1	Aktualisieren Sie Storage Center 1.1 auf StorageZones Controller 2.0 Update 1. Stellen Sie sicher, dass Storage Center 2.0 Update 1 ordnungsgemäß konfiguriert ist und funktioniert, bevor Sie fortfahren. Aktualisieren Sie anschließend StorageZones Controller 2.0 Update 1 auf StorageZones Controller 3.0.1. Führen Sie schließlich ein Upgrade auf den neuesten StorageZones Controller durch.

Wenn diese Version installiert ist:	Tun Sie dies:
Storage Zones Controller 2.x	Aktualisieren Sie StorageZone Controller 2.x auf StorageZones Controller 3.0.1, und aktualisieren Sie dann auf den neuesten StorageZones Controller.
StorageZones Controller 3 Beta-Programm	StorageZones Controller 3 ist Beta Program Software und musste eine neue Installation von StorageZones sein. Andernfalls können Sie ein Upgrade auf den neuesten StorageZones Controller durchführen.
StorageZones Controller 3.x	Upgrade auf den neuesten StorageZones Controller
StorageZones Controller 4.x	Upgrade auf den neuesten StorageZones Controller

Aktualisieren Sie StorageZones Controller 3.0.1 oder höher auf die neueste Version

StorageZones Controller 3.0.1, 3.x und 4.x können wie in den folgenden Schritten beschrieben direkt aktualisiert werden.

1. Wenden Sie sich an, um die neueste Version zu erhalten Unterstützung bei der Unterstützung.

   > **Hinweis:**
   >
   > Durch die Installation eines Storage Zones Controller wird die Standardwebsite auf dem Server in den Installationspfad des Controllers geändert.

2. Auf dem Server, auf dem Sie den primären StorageZones Controller aktualisieren möchten:
   - Führen Sie StorageCenter.msi aus, um den Setupassistenten des ShareFile-StorageZones Controllers zu starten.
   - Antworten Sie auf die Eingabeaufforderungen. Nach Abschluss der Installation zeigt der Assistent die Meldung “Abgeschlossener Setup-Assistent für Citrix ShareFile Storage Zones Controller” an.
   - Klicken Sie auf Fertig stellen. Die StorageZones Controller Konsole wird geöffnet.

   > **Wichtig:**
   >
   > Wenn Sie den Storage Zones Controller klonen möchten, fahren Sie nicht mit der Konfiguration fort. Erfassen Sie das Disk-Image und konfigurieren Sie dann jeden Storage Zones

> Controller.

- Um jederzeit zur Storage Zones Controller Konsole zurückzukehren, öffnen `http://localhost/configservice/login.aspx` oder starten Sie das Konfigurationstool über das Startmenü. Nachdem Sie auf **Fertig stellen** geklickt haben oder zur Storage Zones Controller Konsole zurückkehren, wird die Seite Anmelden geöffnet.
- Um die angezeigten Informationen zu ändern, klicken Sie auf Ändern, nehmen Sie die Änderungen vor, und klicken Sie dann auf Speichern.

3. Überprüfen Sie die Registrierungseinstellungen auf dem primären StorageZones Controller:

   Nicht alle Upgrade-Pfade fügen die Registrierungseinstellungen müssen die Anzahl der Dateien pro Zone erhöhen. Um diese Funktion zu aktivieren, überprüfen Sie, ob die Einstellungen in der Registrierung enthalten sind. Einzelheiten finden Sie unter Erhöhen Sie die Anzahl der Dateien pro Zone.

4. Auf jedem sekundären StorageZones Controller:
   - Führen Sie StorageCenter.msi aus, um den Setupassistenten des ShareFile-StorageZones Controllers zu starten.
   - Beantworten Sie die Eingabeaufforderungen, und klicken Sie dann auf Fertig stellen. Die Anmeldeseite der Storage Zones Controller Konsole wird geöffnet.
   - Melden Sie sich an. Um die angezeigten Informationen zu ändern, klicken Sie auf Ändern, nehmen Sie die Änderungen vor, und klicken Sie dann auf Speichern.
5. Starten Sie den IIS-Server aller Zonenmitglieder neu.

Upgrade von StorageZones Controller 2.x auf StorageZones Controller 3.0.1

Mit diesen Schritten werden Standardzonen aktualisiert, die von früheren Versionen von StorageZones Controller erstellt wurden.

1. Sichern Sie Ihren primären StorageZones Controller, wie unter beschrieben Sichern einer primären StorageZones Controller Konfiguration.
2. Melden Sie sich auf der ShareFile Downloadseite unter an http://www.citrix.com/downloads/sharefile.htmlund laden Sie das neueste StorageZones Controller 3-Installationsprogramm herunter.

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

3. Auf dem Server, auf dem Sie den primären StorageZones Controller aktualisieren möchten:

- Führen Sie StorageCenter.msi aus, um den Setup-Assistenten für ShareFile StorageZones Controller zu starten.
- Antworten Sie auf die Eingabeaufforderungen. Nach Abschluss der Installation zeigt der Assistent die Meldung “Abgeschlossener Citrix ShareFile StorageZones Controller Setup-Assistent” an.
- Klicken Sie auf **Fertig stellen**. Die StorageZones Controller Konsole wird geöffnet.

> **Wichtig:**
>
> Wenn Sie den StorageZones Controller klonen möchten, fahren Sie nicht mit der Konfiguration fort. Zeichnen Sie das Datenträgerimage auf und konfigurieren Sie dann jeden StorageZones Controller.

- Um jederzeit zur StorageZones Controller Konsole zurückzukehren, öffnen `http://localhost/configservice/login.aspx` oder starten Sie das Konfigurationstool über das Startmenü. Nachdem Sie auf Fertig stellen geklickt haben oder zur StorageZones Controller Konsole zurückkehren, wird die Anmeldeseite geöffnet.
- Um die angezeigten Informationen zu ändern, klicken Sie auf Ändern, nehmen Sie die Änderungen vor, und klicken Sie dann auf Speichern.

4. Überprüfen Sie die Registrierungseinstellungen auf dem primären StorageZones Controller:

   Nicht alle Upgrade-Pfade fügen die Registrierungseinstellungen hinzu, die erforderlich sind, um die Anzahl der Dateien pro Zone zu erhöhen. Um diese Funktion zu aktivieren, überprüfen Sie, ob die Einstellungen in der Registrierung enthalten sind. Einzelheiten finden Sie unter Erhöhen Sie die Anzahl der Dateien pro Zone.

5. Auf jedem sekundären StorageZones Controller:

   - Führen Sie StorageCenter.msi aus, um den Setup-Assistenten für ShareFile StorageZones Controller zu starten.
   - Beantworten Sie die Eingabeaufforderungen, und klicken Sie dann auf **Fertig stellen**. Die Anmeldeseite der StorageZones Controller Konsole wird geöffnet.
   - Melden Sie sich an. Um die angezeigten Informationen zu ändern, klicken Sie auf Ändern, nehmen Sie die Änderungen vor, und klicken Sie dann auf **Speichern**.

6. Starten Sie den IIS-Server aller Zonenmitglieder neu.
7. Informationen zum Upgrade auf StorageZones Controller 3.4 finden Sie unter **So aktualisieren Sie auf StorageZones Controller 3.4 von StorageZones Controller 3.1 oder 3.0.1** weiter oben in diesem Artikel.

> **Wichtig:**
>
> Wenn Sie von einer Version vor 2.2.3 auf StorageZones Controller 3.0.1 aktualisieren und zuvor die Einstellungen ProducerTimer oder DeleteTimer angepasst haben, wenden Sie sich an ShareFile Support, um Hilfe beim Konfigurieren der Einstellungen ProducerTimerInterval und DeleteTimerInterval in FileDeleteService.exe.config zu erhalten.

Verwalten von StorageZones Controllern

June 11, 2020

Nachdem Sie Ihre primären und sekundären StorageZones Controller installiert haben, führen Sie die folgenden Verfahren aus, um die Controller zu verwalten und sie für die Disaster Recovery vorzubereiten.

Um die Storage Zones Controller Konsole zu öffnen, rufen Sie das Konfigurationstool über das Startmenü auf, `http://localhost/configservice/login.aspx` oder starten Sie es.

Verwalten des StorageZones Controller

- Anfügen eines sekundären StorageZones Controllers an eine Speicherzone
- Ändern der Adresse oder Passphrase eines primären StorageZones Controller
- Herabstufen und Heraufstufen von StorageZones Controllern
- Deaktivieren, Löschen oder erneutes Bereitstellen eines StorageZones Controller
- Übertragen von Dateien auf eine neue Netzwerkfreigabe
- Sichern einer primären StorageZones Controller Konfiguration
- Wiederherstellen einer primären StorageZones Controller-Konfiguration
- Ersetzen eines primären StorageZones Controller
- Vorbereiten des StorageZones Controller für die Dateiwiederherstellung
- Wiederherstellen von Dateien und Ordnern aus Ihrem ShareFile-Datenbackup
- Abgleichen der ShareFile Cloud mit einer Speicherzone
- Konfigurieren von Antivirus-Scans von hochgeladenen Dateien
- Migrieren von ShareFile Daten
- Aktivieren des FIPS 140-2-Modus mit StorageZones Controller Konfiguration
- Connector-Favoriten

Anfügen eines sekundären StorageZones Controllers an eine Speicherzone

June 11, 2020

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

June 11, 2020

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

Sie können die externe Adresse eines primären StorageZones Controller mithilfe dieses Verfahrens oder anderer Serververwaltungstools ändern.

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 den Hostnamen des primären StorageZones Controller.
3. Geben Sie die neue **externe Adresse** oder **lokale Adresse** an, und klicken Sie dann auf **Änderungen speichern**.
4. Starten Sie den IIS-Server aller Zonenmitglieder neu.

So ändern Sie die Passphrase eines primären StorageZones Controller

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

   Die Passphrase ist nicht identisch mit Ihrem Kontokennwort und kann nicht wiederhergestellt werden, wenn sie verloren geht. Wenn Sie die Passphrase verlieren, können Sie Speicherzonen nicht neu installieren, zusätzliche StorageZones Controller mit der Speicherzone verbinden oder die Speicherzone wiederherstellen, wenn der Server ausfällt.

   > **Hinweis:**
   >
   > Der Verschlüsselungsschlüssel wird im Stammverzeichnis des freigegebenen Speicherpfads angezeigt. Der Verlust der Verschlüsselungsschlüsseldatei unterbricht sofort den Zugriff auf alle Speicherzonen-Dateien.

4. Wenn Sie die Passphrase auf dem primären Server geändert haben: Melden Sie sich bei der Konfigurationsseite der Speicherzonen für jedes der anderen Mitglieder an, und geben Sie die Passphrase ein, wenn Sie dazu aufgefordert werden.

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

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

Herabstufen und Heraufstufen von StorageZones Controllern

June 11, 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.

> **Vorsicht:**
>
> 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 Formular`https://IPaddress` oder verwenden`https://hostname/ConfigService/`.
    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 StorageZones Controller

June 11, 2020

So deaktivieren Sie einen StorageZones Controller

> **Hinweis:**
>
> Gehen Sie folgendermaßen vor, wenn jeder StorageZones Controller über eine andere externe Adresse verfügt. Deaktivieren Sie einen Controller über die Citrix ADC Schnittstelle, wenn Sie dieselbe externe Adresse für alle StorageZones Controller verwenden.

Deaktivieren Sie einen Storage Zones Controller, bevor Sie den Server zur Wartung offline schalten.

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 den Hostnamen des StorageZones Controller.
3. Deaktivieren Sie das Kontrollkästchen aktiviert, und klicken Sie dann auf **Änderungen speichern**.
4. Starten Sie den IIS-Server aller Zonenmitglieder neu.

So löschen Sie einen StorageZones Controller

Beim Löschen eines StorageZones Controller werden die Daten oder Sckeys.txt nicht gelöscht. Wenn Sie einen primären StorageZones Controller löschen, stufen Sie ihn zurück, bevor Sie fortfahren.

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 den Hostnamen des StorageZones Controller.
3. Klicken Sie auf **Löschen**.
4. Starten Sie den IIS-Server aller Zonenmitglieder neu.

So stellen Sie einen StorageZones Controller erneut bereit

Beim erneuten Bereitstellen eines Storage Zones Controller gehen keine Informationen verloren.

1. Deinstallieren Sie Speicherzonen vom Server.
2. Klicken Sie in der ShareFile e-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 von Speicherzonen. Registrieren Sie es noch nicht.
5. Führen Sie den Konfigurationsassistenten für Speicherzonen Controller aus, um den Storage Zones 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

June 11, 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.

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**.

   > **Vorsicht:**
   >
   > 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 11, 2020

Ein StorageZones Controller ist auf Ihrem lokalen Standort installiert und Sie sind für die Sicherung verantwortlich. Um Ihre Bereitstellung vollständig zu schützen, sollten Sie einen Snapshot des StorageZones Controller-Servers erstellen, Ihre Konfiguration sichern und Vorbereiten des StorageZones Controller für die Dateiwiederherstellung.

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

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

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

Die Backup- und Wiederherstellungsbefehle erfordern, dass Sie die 32-Bit-Version von PowerShell unter demselben Benutzerkontext wie der StorageZones Controller ausführen. Um den Benutzerkontext festzulegen, verwenden Sie das Tool PSExec. Dieses Tool steht zum Download von http://technet.microsoft.com/en-us/sysinternals/bb897553.

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

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

   a) Bestimmen Sie, ob die PowerShell Ausführungsrichtlinie das Ausführen lokaler, nicht signierter Skripts ermöglicht: PS `C:\>Get-ExecutionPolicy`

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

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

2. 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.

3. Importieren Sie von 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: `Get-SfConfig -PrimaryZoneController ”server”-Passphrase ”passphrase”-FilePath ”fullpath”`

   Beispiel:

   ```
   1 Get-SfConfig -PrimaryZoneController ”`https://myserver.domain.com/ConfigService/`” -Passphrase ”mypassphrase” -FilePath ”c:\szc-backup.bak”
   ```


Befehlsparameter:

Parameter	Beschreibung	Beispiele
“Server”	Der Servername oder die IP-Adresse des primären StorageZones Controller-Servers. Es kann in einer der folgenden Formulare unter Beispiele vorliegen und muss den abschließenden Schrägstrich enthalten.	Herstellen einer Verbindung mit einem lokalen Server: `http://localhost/ConfigService/`; Verbinden mit einem Remoteserver: `http[s]://myservername.domain.com/ConfigService/`; Verbinden mit einem Remoteserver, wenn DNS-Probleme die Verbindung mit einem Servernamen verhindern: `http[s]://10.40.37.5/ConfigService/`
“passphrase”	Die für den StorageZones Controller angegebene Passphrase.	“MyPassphrase”
“fullpath”	Ein Speicherort zum Speichern der Backupdatei.	“c:\szc-backup.bak”

Mit dem Befehl Get-SfConfig wird die Backupdatei erstellt.

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

Wiederherstellen einer primären StorageZones Controller-Konfiguration

June 11, 2020

Der StorageZones Controller bietet die folgenden Optionen für die Notfallwiederherstellung, wenn ein primärer StorageZones Controller gelöscht wird oder unbrauchbar wird:

- Wenn ein sekundärer StorageZones Controller verfügbar ist, stufen Sie den sekundären Controller auf einen primären zu.
- Wenn ein sekundärer StorageZones Controller nicht verfügbar ist und Sie Ihre primäre StorageZones Controller-Konfiguration gesichert haben (wie unter beschriebenSichern einer primären

StorageZones Controller Konfiguration), stellen Sie den primären StorageZones Controller aus der Backupdatei.

- Wenn Sie kein Backup Ihrer primären Storage Zones Controller-Konfiguration haben und alle Ihre Storage Zones Controller versehentlich gelöscht oder unbrauchbar werden, ist nur eine teilweise Wiederherstellung möglich. Sie können Zonen und die Konfiguration für Speicherzonen für ShareFile Daten wiederherstellen, nicht jedoch StorageZone Connector.

> **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.

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

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

1. Das in diesem Verfahren verwendete PowerShell -Skript ist nicht signiert, daher müssen Sie möglicherweise die PowerShell Ausführungsrichtlinie ändern.
   a) Bestimmen Sie, ob die PowerShell Ausführungsrichtlinie das Ausführen lokaler, nicht signierter Skripts ermöglicht: PS `C:\>Get-ExecutionPolicy`

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

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

   > **Hinweis:**
   >
   > Laden Sie Psexec.exe von herunter, http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx und folgen Sie den Installationsanweisungen auf dieser Seite.

   - 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.

3. Importieren Sie von 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 `Set-SfConfig` folgenden Befehl aus: `Set-SfConfig -PrimaryZoneController "server"-Passphrase "passphrase"-FilePath "fullpath"`

   Wobei:

   - Server ist der Name oder die IP-Adresse des primären StorageZones Controller-Servers. Es kann in einer der folgenden Formen vorliegen und muss den abschließenden Schrägstrich enthalten.

     `http://localhost/ConfigService/`

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

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

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

   - Passphrase ist die für den StorageZones Controller angegebene.
   - 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 Data wiederherstellen, jedoch keine StorageZone Connector.

1. 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 Anwendungspool verwenden:

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

Ein PowerShell-Fenster wird geöffnet.

2. Importieren Sie von 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 möchten.

```
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 erhalten werden:

  a) Klicken Sie in der ShareFile Weboberfläche auf **Admin > Speicherzonen**, klicken Sie mit der rechten Maustaste auf den Sitename, und wählen Sie dann **Eigenschaften**.

  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 Sitename, klicken Sie mit der rechten Maustaste auf den Hostnamen, und wählen Sie dann Eigenschaften.

  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 ist nur erforderlich, 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 werden.

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

Ersetzen eines primären StorageZones Controller

June 11, 2020

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

June 11, 2020

> **Warnung:**
>
> Mit der ShareFile Wiederherstellungsfunktion wird Ihr persistenter Speicherort nicht automatisch gespeichert. Sie sind dafür verantwortlich, ein Sicherungsprogramm 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 von Drittanbietern** — Wenn Sie ein Speichersystem eines Drittanbieters mit StorageZones Controller verwenden, ist der Speicher eines Drittanbieters redundant, und eine lokale Sicherung 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 dem Wiederherstellungszeitraum wird die Datei aus der Zone und damit aus dem redundanten Speicher eines Drittanbieters entfernt. Wenn diese Wiederherstellungszeit nicht ausreichend ist, sollten Sie eine der folgenden Lösungen in Betracht ziehen:
  - Erhöhen Sie die Zeit, die eine Datei im ShareFile Papierkorb verbleibt. Ändern Sie dazu den Wert der Einstellung "Periode" in C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDelete
    Weitere Informationen finden Sie unter Anpassen von Speicher-Cache-Vorgängen. Beachten Sie, dass die Erhöhung der Aufbewahrungszeit auch die benötigte Speichermenge von Drittanbietern erhöht.
  - Erstellen Sie alle sieben Tage ein lokales Backup Ihrer StorageZone-Dateien und bestimmen Sie die entsprechende Aufbewahrungsrichtlinie für Backups.
- Lokaler**Speicher — Wenn Sie eine lokal** verwaltete Freigabe für die private Datenspeicherung verwenden, sind Sie für die Sicherung des lokalen StorageZones Controller für lokale Dateispeicherung und Registrierungseinträge verantwortlich. ShareFile archiviert die entsprechenden Dateimetadaten, die sich drei Jahre lang in der ShareFile Cloud befinden.
  Wichtig: Zum Schutz vor Datenverlust ist es wichtig, dass Sie einen Snapshot Ihres StorageZones

Controller-Servers erstellen,
Sichern der Konfiguration, und ein Backup des lokalen Dateispeichers.

Nachdem Sie den StorageZones Controller für die Dateiwiederherstellung vorbereitet haben, wie in diesem Thema beschrieben, können Sie die ShareFile e-Administratorkonsole verwenden, um:

- 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 dem Backup an den persistenten Speicherort wiederherzustellen.

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

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

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

Voraussetzungen

- Windows Server 2012 R2 oder Windows Server 2008 R2
- Windows PowerShell (32-Bit- und 64-Bit-Versionen) muss .NET 4-Laufzeit-Assemblys unterstützen. Weitere Informationen finden Sie unter “PowerShell -Skripte und -Befehle” in StorageZones Controller -Systemanforderungen.
- PsExec.exe - Mit PsExec können Sie PowerShell über das Netzwerkdienstkonto starten. Sie können PsExec auch verwenden, um Wiederherstellungsaufgaben zu planen. Laden Sie Psexec.exe von herunter, http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx und folgen Sie den Installationsanweisungen auf dieser Seite.

Zusammenfassung der Dateien, die für die Notfallwiederherstellung verwendet werden

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

Dateiname	Beschreibung
DoRecovery.ps1	PowerShell -Skript, das vom Windows Taskplaner ausgeführt wird, um den Wiederherstellungsprozess zu verarbeiten. In dieser Datei werden die Dateibackup- und Speicherorte gespeichert.
Wiederherstellung.psm1	PowerShell Modul, das die Wiederherstellungswarteschlangenvorgänge verarbeitet.
recovery.log	Protokolldatei, die die Ausgabe eines Wiederherstellungsprozesses speichert.
recoveryerror.log	Protokolldatei, in der die Fehler im Wiederherstellungsprozess gespeichert werden.
Litjson.dll	Eine .NET-Bibliothek, um Konvertierungen von und in JSON-Zeichenfolgen (JavaScript Object Notation) zu verarbeiten.

So richten Sie den Backupordner ein

Erstellen Sie auf dem Backupserver den Ordner, in dem Sie das Backup des persistentstorage-Ordners speichern.

Die Speicherzonen für die Sicherung der ShareFile Datendatei sollten dem gleichen Layout folgen wie der persistente Speicher des StorageZones Controller.

Wenn Ihr Backupspeicherort nicht dem gleichen Layout wie der persistente Speicher des StorageZones Controller entspricht, müssen Sie während des Wiederherstellungsprozesses einen zusätzlichen Schritt ausführen, um Dateien vom Backupspeicherort an den Speicherort zu kopieren, den Sie im PowerShell-Wiederherstellungsskript angeben.

Speicher-Layout

Backup-Layout

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



```
      \a024f83e-b147-437e-9f28-e7d03634af42
       \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
        \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
         \fi47cd7e_64c4_47be_beb7_1207c93c1270

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

> **Wichtig:**
>
> Mit der ShareFile Wiederherstellungsfunktion wird Ihr persistenter Speicherort nicht automatisch gespeichert. **Sie sind dafür verantwortlich, ein Backupprogramm auszuwählen und es alle 1 bis 7 Tage auszuführen.**

So erstellen Sie eine Warteschlange für die Notfallwiederherstellung

Diese einmalige Einrichtung ist erforderlich. In den folgenden Befehlsbeispielen wird der Standardinstallationsordner des StorageZones Controller verwendet.

1. Führen Sie PowerShell auf dem StorageZones Controller als Administrator aus.
2. Das in diesem Verfahren verwendete PowerShell -Skript ist nicht signiert, daher müssen Sie möglicherweise die PowerShell Ausführungsrichtlinie ändern.
   a) Stellen Sie fest, ob Sie in der PowerShell Ausführungsrichtlinie lokale, nicht signierte Skripte ausführen können: PS C:\ >Get-ExecutionPolicy

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

   b) So ändern Sie die PowerShell Ausführungsrichtlinie: PS C:\ >Set-ExecutionPolicy RemoteSigned
3. Geben Sie Folgendes ein, um zu überprüfen, ob PowerShell über die richtige CLRVersion verfügt:

   $psversiontable

   Der Wert für CLRVersion muss 4.0 oder höher sein, damit PowerShell NET-Assemblys in Skripts laden kann. Wenn dies nicht der Fall ist, ändern Sie es für Windows PowerShell 32-Bit- und 64-Bit-Versionen wie folgt:

   a) Führen Sie NotePad als Administrator aus.

b) Erstellen Sie eine Datei mit folgendem 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", benennen Sie die Datei "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 Fenster 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 mithilfe von PSExec.exe wie folgt:

   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\p

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

5. Navigieren Sie zum Ordner "Tools für die Notfallwiederherstellung" im Installationsordner des StorageZones Controller:

   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: Queue 92736b5d-1cff-4760-92c8-d8b04dc92cb2 erstellt

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

   \\server\(*Ihr* primärer Speicherort)\Queue. Sie sehen den Queue-Ordner, wie 92736b5d-1cff-4760-92c8-d8b04dc92cb2.

8. Passen Sie das PowerShell -Skript für die Wiederherstellung Ihres Standorts 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 zu verarbeiten. Diese Datei enthält die Dateibackup- 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. Legen Sie den Parameter $BackupROOT so fest, dass er auf den UNC-Pfad des Backupspeicherorts verweist. Beispiel: $backupRoot = "\\10.10.10.11\(*Your*BackupLocation)\persistentstorage"

   b. Legen Sie den Parameter $StorageRoot so fest, dass er auf den UNC-Pfad des persistenten Speichers des StorageZones Controller verweist. Beispiel: $storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"

So testen Sie den Wiederherstellungsprozess

1. Erstellen Sie eine Testdatei und laden Sie sie in ShareFile hoch.
2. Überprüfen Sie nach etwa einer Stunde, ob die Datei im persistenten Speicher (im Pfad, der für $backupROOT angegeben ist) angezeigt wird.
3. Löschen Sie die Datei aus ShareFile: Klicken Sie im ShareFile-Administrator-Tool auf **Papierkorb**, wählen Sie die Datei aus, und klicken Sie dann auf Permanent **löschen**.
4. Löschen Sie die Datei aus dem persistenten Speicher.

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

5. Wechseln Sie im ShareFile Administrator-Tool zu **Admin > Speicherzonen**, klicken Sie auf die Zone und klicken Sie dann auf **Dateien wiederherstellen**.
6. Klicken Sie in das Textfeld **Wiederherstellungsdatum**, und wählen Sie Datum und Uhrzeit aus, bevor die Datei gelöscht wurde und nachdem sie hochgeladen wurde.

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

7. Aktivieren 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 Backupwarteschlange 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. So stellen Sie die Datei wieder her:

   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”. 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 Datei-IDs ab, die für die Wiederherstellung benötigt werden. Verwenden Sie für Syntax und Parameter folgenden Befehl:

  Get-Help Get-RecoveryPendingFileIDs -full

- **Set-RecoveryQueueItemsStatus**

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

  Get-Help Set-RecoveryQueueItemsStatus -full

So erstellen und planen Sie eine Aufgabe für die Wiederherstellung

Für den Fall, dass eine geplante Wiederherstellungsaufgabe erforderlich ist, führen Sie die folgenden Schritte aus.

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 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 mit Schreibberechtigungen für den Speicherort.

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

   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 unter Start in**den Disaster Recovery-Ordner am Speicherort des StorageZones Controller an. Beispiel: `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

Standardzeitraum des Dienstes löschen

Ab StorageZone Controller 4.0 wird der Timer zum Löschen des Dienstes auf 45 Tage festgelegt. 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\S

```
<!--No. of days to keep data blob in active storage after deletion-->
<add key=”Period”value=”45”/>
```


Ändern Sie den Standardzeitraum des Dienstes nach dem Upgrade

In einigen Upgradeszenarien wird der DeletePeriod Wert in der Datei "FileDeleteService.exe.config" auf null gesetzt. Wenn dieser Wert auf null festgelegt ist, wird der Löschzeitraum standardmäßig auf 45 Tage festgelegt. Die Standardanzahl von Tagen, bevor eine Datei, die aus ShareFile gelöscht wurde, aus dem physischen Speicher entfernt wird.

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

Bei einer Neuinstallation des StorageZones Controller wird der Delete Service alle 8 Stunden ausgeführt, um temporäre Dateien und Ordner zu bereinigen. Um den Zeitgeber zu ändern, bearbeiten Sie die Datei FileDeleteService.exe.config am folgenden Speicherort: `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:

   ```
   1  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:

   ```
   1  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

June 11, 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.

> **Vorsicht:**
>
> 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.

Konfigurieren von Antivirus-Scans von hochgeladenen Dateien

June 11, 2020

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

Anforderungen/Zusammenfassung

- Benutzer mit StorageZones Controller 4.2 oder höher
- 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 werden, aktualisieren, müssen die Benutzerebene, auf der das Tool ausgeführt wird, vom lokalen Administrator zum Systemnetzwerkdienst ändern.

Um Netzwerkdienstrechte abzurufen, starten Sie PowerShell (x86) mit PSExec unter demselben Benutzerkontext wie der StorageZones Controller und beziehen Sie Netzwerkdienstrechte mit dem folgenden Befehl:

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


Speicherort der Protokolldatei aktualisieren

Administratoren müssen außerdem 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 Controller umfasst mehrere Dateien, die Antiviren-Scans unterstützen. Die Dateien werden standardmäßig in C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus. installiert.

Nachdem Sie die Konfigurationsdatei angepasst und mit dem Windows-Taskplaner die Scans planen, wie in den folgenden Schritten beschrieben, bewirkt jede Dateiuploadanforderung, dass der StorageZones Controller die Datei für einen Antiviren-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 SFANVirus.exe.config unter C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus.

Die Antivirus-Scan entfernt die Datei nicht.

Die Verwendung des ICAP-Protokolls mit Antivirus-Scanplattformen, 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.

Voraussetzung

- Wenn Sie Viren-Scans (Sfantivirus.exe) auf dem StorageZones Controller ausführen, stellen Sie sicher, dass die Verschlüsselung auf dem Controller deaktiviert ist: Überprüfen Sie auf der Konfigurationsseite der Storage Zones Konsole, ob das Kontrollkästchen Verschlüsselung aktivieren deaktiviert ist.

> **Hinweis:**
>
> Nach der Konfiguration des Antivirenprogramms 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 Storage Zones 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 legen Sie QueueSDKRestricted auf 0 fest:`<add key="QueueSDKRestricted" value="0"/>`

2. Bearbeiten Sie auf dem Server, auf dem Sie Virenscans ausführen, SfanVirus.exe.config mit den Werten für die Controller Konfiguration Ihrer Speicherzonen:

   a) Für CommandFile: Geben Sie den vollständigen Pfad zur Antivirensoftware an. Diese Software muss sich auf demselben Server wie der ShareFile-Antivirenordner befinden.

   b) Für CommandOptions und Rückgabecodes: Die Befehlszeileneinstellungen in der Konfigurationsdatei sind ein Beispiel. Geben Sie die entsprechenden Einstellungen für Ihre Antivirensoftware und -umgebung an.

   c) Für ScanFileTimeout: Größere Dateien können länger durchsucht werden. Passen Sie diese Einstellung entsprechend den 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 4.2 oder höher unterstützt die Verwendung des ICAP-Protokolls mit Antivirus-Scanplattformen, die nach dem RFC-Standard für ICAP codiert wurden. Kunden können weiterhin die CLI-Methode verwenden, wenn sie möchten. Dieses Feature wird für Mandantenzonen ab SZ 5.0.1 oder höher unterstützt.

Um einen ICAP-AV-Scanner auf Ihrem StorageZones Controller zu aktivieren, navigieren Sie zur Konfigurationsseite des Storage Zones Controllers.

Aktivieren Sie das Kontrollkästchen **Antivirenintegration aktivieren**, und geben Sie die Adresse des Antivirus-Servers in das Feld **ICAP RESPMOD-URL** ein. Dies ist die URL des ICAP-Antwortänderungsdiensts: `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 geplanter Tasks für Virenscans ist nur bei Verwendung von Befehlszeilentools er-

> forderlich. 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 über die vollständige Zugriffsberechtigung für den Speicherort verfügen.
   c) Wählen Sie **Ausführen aus, ob der Benutzer angemeldet ist oder nicht**. Lassen **Sie das Kontrollkästchen Kennwort nicht speichern** deaktiviert.
   d) Wählen Sie **Ausführen mit höchsten Berechtigungen**aus.
   e) Wählen Sie **im Menü Konfigurieren für**das Betriebssystem des Servers aus, auf dem der Task ausgeführt werden soll.
3. So erstellen Sie einen Trigger: Klicken Sie auf der Registerkarte **Trigger** auf **Neu**. Wählen Sie dann unter **Task beginnen die**Option Nach **einem 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 unter **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 unter Start in den Speicherort von SFAntiVirus.exe an: `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`
5. Wählen Sie auf der Registerkarte **Einstellungen** unter **Wenn der Task bereits ausgeführt wird**, die folgende Regel gilt, **keine neue Instanz starten**.

AV-Befehlszeilenintegration in Scan Service

Voraussetzungen

- Stellen Sie vor der Installation oder Aktualisierung des StorageZones Controller 5.2 sicher, dass Sie den vorhandenen Befehlszeilen-AV beenden oder löschen, wenn er als geplanter Task oder Cron ausgeführt wird.
- Installieren Sie .NET 4.6.2 (oder höher) auf einem Hostcomputer.

Der Scan-Dienst im lokalen StorageZones Controller unterstützt die Verwendung eines Befehlszeilen-AV-Tool wie der Symantec-Befehlszeilen-AV-Scan. Darüber hinaus bietet der Suchdienst Scans mit ICAP-unterstützten Antivirenprodukten.

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

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

Befehlszeilen-Toolspezifische Konfiguration

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

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

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

Die Konfigurationsschlüsselwerte werden unten mit Beispielwerten erläutert.

- Setzen Sie diesen Punkt auf Ihre Befehlszeilenanwendung.

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

- Überprüfen Sie die Dokumentation für die Befehlszeilenanwendung, um zu sehen, welche Optionen oder Switches von der Befehlszeilenanwendung unterstützt werden, und fügen Sie sie dann an diesem Speicherort hinzu.

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

- Geben Sie die Ausgabewerte ein, die auf einen sauberen Scan hinweisen.

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

- Geben Sie Ausgabewerte ein, die auf infizierte Datei hinweisen.

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

- Geben Sie Ausgabewerte ein, die auf nicht gescannte Dateien hinweisen.

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

Hinweise zur Erzwingung der maximalen Dateigröße, ausgenommen Erweiterungen

Vor Version 5.2 konnten Sie den Erweiterungsausschluss oder die maximale Dateigrößenerzwingung auf der Befehlszeilen-AV nicht erzwingen. Sie konnten dies nur auf dem ICAP-Scan-Dienst tun. Mit Version 5.2 gelten dieselben Einstellungen, die für den ICAP-Scandienst bezüglich ausgeschlossener Erweiterungen und maximaler Dateigröße in Byte angewendet wurden, für den AV-Befehlszeilendienst.

Diese Einstellungen wurden wie folgt benannt:

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

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


Bei einer neuen Installation von Storage Zones Controller 5.2 werden diese Einstellungen wie folgt umbenannt. 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, funktionieren dieselben Einstellungen zusätzlich zu ICAP auch für die AV-Befehlszeile.

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

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

Migrieren von ShareFile Daten

June 11, 2020

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

- Migrieren über Webportal oder Benutzerverwaltungstool
- Migrieren über PowerShell -Skript
- Migrieren über das ZoneFix Tool

Voraussetzungen

- Stellen Sie sicher, dass die Quellzone von der Zielzone aus erreichbar ist, und heben Sie die Blockierung der 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 Benutzer initiieren.

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

> setzt.

Daten für einen bestimmten Benutzer migrieren - Navigieren Sie zu **Personen**, und suchen Sie dann den Benutzer **Mitarbeiter**. Klicken Sie auf den Benutzer, um seine Profilseite anzuzeigen. Wählen Sie unter **Speicherort**eine neue Zone aus (sofern bereits eine Zone installiert und konfiguriert wurde).

Daten für einen bestimmten Ordner migrieren - Navigieren Sie zu dem Ordner, und rufen Sie das Menü **Weitere Optionen** rechts neben dem Ordnernamen auf. Klicken Sie auf **Erweiterte Ordnereinstellungen**. Wählen Sie im 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 `persistentstorage` der neuen Zone hinzugefügt.

Migrieren 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 kann heruntergeladen werden hier.

Migrieren über das Werkzeug “Zone Fix”

Das Werkzeug “Zone Fix” ist ein Befehlszeilenwerkzeug. Das von Speicherzonenentwicklern geschriebene Tool nutzt die ShareFile API, um Ordner-IDs für die Migration in eine bestimmte Zone anzuvisieren.

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

Aktivieren des FIPS 140-2-Modus mit StorageZones Controller Konfiguration

June 11, 2020

Bevor Sie die folgende Konfiguration für ShareFile anwenden, überprüfen Sie, ob der FIPS-Modus unter Windows Server aktiviert ist. Vorgehensweise:

1. Starten Sie den Registrierungseditor (regedit).
2. Navigieren Sie zum Pfad: `HKEY_LOCAL_MACHINE\SOFTWARE\PowerShell\Server\16`
3. Überprüfen Sie den Registrierungswert **useFipsCompliantAPI**.
4. Wenn die Wertdaten (DWORD) **1**sind, ist der FIPS-kompatible Modus aktiviert.

Wenn der FIPS-kompatible Modus **nicht** aktiviert ist, verwenden Sie Folgendes, um den FIPS-kompatiblen Modus zu aktivieren:

1. Melden Sie sich bei Windows als Windows-Systemadministrator an.
2. Klicken Sie auf **Start,** klicken Sie auf **Systemsteuerung**, und klicken Sie dann auf **Verwaltung**.

   > **Hinweis:**
   >
   > Möglicherweise müssen Sie für den nächsten Schritt zu großen Symbolen wechseln.

3. Klicken Sie auf **Lokale Sicherheitsrichtlinie**. Das Fenster **Lokale Sicherheitseinstellungen** wird angezeigt.
4. Klicken Sie im Navigationsbereich auf **Lokale Richtlinien**, und klicken Sie dann auf **Sicherheitsoptionen**.
5. Doppelklicken Sie im rechten Bereich auf **Systemkryptografie: FIPS-kompatible Algorithmen für Verschlüsselung, Hashing und Signatur verwenden**.

   > **Hinweis:**
   >
   > Das Aktivieren der vorherigen Einstellung kann sich auf alle Anwendungen auf dem Computer auswirken.

6. Klicken Sie im angezeigten Dialogfeld auf **Aktiviert**, klicken Sie auf **Übernehmen**, und klicken Sie dann auf **OK.**
7. Schließen Sie das Fenster **Lokale Sicherheitseinstellungen**.

Weitere Informationen, siehe diesem Artikel.

Standardmäßig kann Storage Zones Controller Kryptografiemodule verwenden, die nicht mit dem FIPS 140-2 Standard kompatibel sind. Nach der Installation des StorageZones Controller und vor dem Ausführen von ConfigService: Kunden müssen das folgende Codebeispiel hinzufügen, um die FIPS 140-2-Konformität in ihrem Controller zu aktivieren.

```
<appSettings>

<add key=”fipsOnly” value=”1” />

</appSettings>
```


Fügen Sie das vorhergehende Codebeispiel als untergeordnetes `<configuration>` Element am Ende der folgenden Datei hinzu:

`C:\Windows\Microsoft.NET\Framework\v4.0.x\Config\machine.config`

Setzen Sie als Nächstes IIS zurück und starten Sie alle ShareFile Dienste neu. Alternativ können Sie Ihren Computer neu starten.

> **Hinweis:**
>
> Information Resource Management (IRM) wird nicht unterstützt.

Connector-Favoriten

June 11, 2020

Ab Storage Zones Controller 5.0 können Benutzer Connectorordner als Favoriten unter **Netzwerkfreigaben**, **SharePoint**und **Documentum Connectors** in ShareFile WebApp erstellen. Weitere Informationen finden Sie in diesem Citrix Support Knowledge Center diesem Artikel.

Das Hinzufügen eines Connectorordners zu Ihren Favoriten wird auf ShareFile Mobile unterstützt. Beachten Sie auch, dass das Erstellen eines Favoriten eines Connectorordners in einer eingeschränkten Zone nicht unterstützt wird.

Verwalten von Speicherzonen für ShareFile Daten

June 11, 2020

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

Verschieben von Basisordnern und Dateifeldern zwischen Zonen

Gehen Sie wie folgt vor, um Basisordner und Dateifelder aus dem von ShareFile verwalteten Cloud-Speicher in eine private Zone oder zwischen privaten Zonen zu verschieben. Alternativ können Sie das ShareFile Benutzerverwaltungsprogramm verwenden, um Benutzer zwischen Zonen zu migrieren.

1. Klicken Sie auf **Startseite**, und navigieren Sie 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**.
4. Starten Sie den IIS-Server aller Zonenmitglieder neu.

Erstellen eines Ordners in einer Speicherzone

1. Klicken Sie auf **Startseite** und dann auf **Ordner**.
2. Klicken Sie auf der Registerkarte **Ordner** auf **Ordner hinzufügen**.
3. Geben Sie die Ordnerinformationen wie gewohnt an, und wählen Sie unter Speichersite die Speicherzone aus, in der dieser Ordner und sein Inhalt gespeichert werden sollen. Klicken Sie auf **Ordner erstellen**.
4. Konfigurieren Sie den Ordner wie gewohnt. Wenn Sie einen Ordner erstellen, können Sie auswählen, ob der von ShareFile verwaltete Cloudspeicher oder die lokale Speicherzone verwendet werden soll.
5. Starten Sie den IIS-Server aller Zonenmitglieder neu.

Umbenennen oder Löschen einer Speicherzone

> **Wichtig:**
>
> Bevor Sie eine Speicherzone löschen, sichern Sie sie. Wenn Sie eine Zone löschen, 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 **Speicherzonen**.
2. Klicken Sie auf den Zonennamen.
   - Um die Zone umzubenennen: 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 klicken Sie dann auf **Zone löschen**.
3. Starten Sie den IIS-Server aller Zonenmitglieder neu.

Anpassen von Speicher-Cache-Vorgängen

ShareFile Benutzeranforderungen für Datei-Uploads, Downloads und Löschvorgänge werden vom StorageZones Controller verarbeitet, der dann mit dem verbundenen Speicher kommuniziert. 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 Speicher-Cache. Der StorageZones Controller lädt die Datei dann auf das Speichersystem eines Drittanbieters hoch.

Der StorageZones Controller verwaltet den persistenten Speichercache mit konfigurierbaren Einstellungen in `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`. Die Einstellungen, die spezifisch für ein unterstütztes Speichersystem von Drittanbietern sind, werden in dieser Diskussion notiert.

Für hochgeladene Dateien:

- Der StorageZones Controller platziert hochgeladene Dateien in einen persistenten Speichercache (der Ordner PersistentStorage).
- Die folgenden Einstellungen steuern das Timing von Löschdienstvorgängen:
  - MinDeletionAge gibt die minimale Zeitspanne zwischen dem Zeitpunkt des letzten Zugriffs auf eine Datei und dem Zeitpunkt des Löschens an. Der Standardwert beträgt 1 Tag. Mindesteinstellung beträgt 8 Stunden.
  - OffPeakTimeOfDayStart und OffPeakTimeOfDayEnd geben die Start- und Stoppzeiten für das Löschen von Dateien an. Standardmäßig ist 2 Uhr und 4 Uhr vormittags.
  - ProducerTimerInterval und DeleteTimerInterval steuern die Häufigkeit von Löschdienstvorgängen. Bitte wenden Sie sich an den Support, wenn 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 legt fest, ob eine Datei im Speicher-Cache ein entsprechendes Blob im unterstützten Drittanbieter-Speicher enthält.
  - Standardmäßig ermittelt der Löschdienst alle 10 Sekunden (CheckSizeThreasHoldTimer), ob der Speichercache einen Plattenschwellenwert von 10 GB (DiskSpaceDropoutThresholdGB) überschritten hat. Wenn der Schwellenwert überschritten wird, entfernt der Löschdienst Dateien, auf die in der letzten Stunde nicht zugegriffen wurde (CacheCleanUpFileThreasHoldPeriodUnexpected). Wenn der Löschdienst als Ergebnis der normalen Planung ausgeführt wird (und nicht, weil die Datenträgergröße den Schwellenwert erreicht hat), löscht der Dienst Dateien, auf die in den letzten 24 Stunden nicht zugegriffen wurde (CacheCleanUpFileThresholdPeriodNormal), wenn sich das BLOB im unterstützten Speicher von Drittanbietern befindet. Wenn sich das Blob nicht im Speicher eines Drittanbieters befindet, verbleibt die Datei im Speicher-Cache.

Für heruntergeladene Dateien:

- Wenn der StorageZones Controller eine Download-Anforderung empfängt, lädt er die Datei aus dem persistenten Speichercache herunter, wenn die Datei vorhanden ist. Wenn sich die Datei nicht in diesem Cache befindet, lädt der Controller die Datei vom Speichersystem eines Drittanbieters in den persistenten Speicher-Cache herunter. Der Löschdienst entfernt Dateien, auf die in den letzten 24 Stunden nicht zugegriffen wurde (CacheCleanUpFileThresholdPeriodNormal).

Für gelöschte Dateien:

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

Standardzeitraum des Dienstes löschen

Ab StorageZones Controller 4.0 ist der Timer zum Löschen des Dienstes auf 45 Tage festgelegt. Der Standardzeitraum von 45 Tagen überschreibt alle vorherigen Einstellungen.

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

June 11, 2020

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.

Systemanforderungen für Steckverbinder

StorageZone Connector unterstützen nicht die gemeinsame Nutzung von Dokumenten oder die Ordnersynchronisierung über Geräte hinweg.

Connectors müssen einen eindeutigen Anzeigenamenhaben. Benutzer werden daran gehindert, einen Konnektornamen 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 Konnektor 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 beim Herstellen einer Verbindung mit persönlichen SharePoint-Websites automatisch aufzulösen. Diese Variable ersetzt Leerzeichen mit%20 und Punkte durch Unterstriche. Die Verwendung der Variablen %URLusername% 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 **Verbinder hinzufügen**. Das Dialogfeld **Ordnerzugriff anzeigen/bearbeiten** wird angezeigt.

8. Um Connectors für andere sichtbar zu machen: 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:**
>
> Nur en-US.

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.

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 Verbinder hinzufügen. Das Dialogfeld Ordnerzugriff anzeigen/bearbeiten wird angezeigt.

8. Um Connectors für andere sichtbar zu machen: 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. StorageZones Controller 4.1 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

Web-App

- Connector-Erstellung
- Surfen
- Datei-Uploads/Downloads
- Ordner Erstellung/Löschung

Nicht unterstützt

- Freigeben von Dateien, die in einem Documentum-Connector gespeichert sind
- Whitelisting/Blacklist von Pfaden

> **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 Inhaltswechsel > Richtlinien 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-Konnektoren

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 hinzufügt:

```
<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

June 11, 2020

Mit DLP-Funktionen (Data Loss Prevention) in ShareFile können Sie den Zugriff und die Freigabe basierend auf dem Inhalt in einer Datei einschränken.

Sie können die in Ihre Speicherzone hochgeladenen Dokumente mithilfe einer DLP-Sicherheitssuite eines Drittanbieters scannen, die ICAP unterstützt, einem Standardnetzwerkprotokoll für die Inline-Inhaltssuche. Anschließend passen Sie die Freigabe- und Zugriffsberechtigungen basierend auf den Ergebnissen des DLP-Scans und Ihren Einstellungen an, wie streng Sie den Zugriff steuern möchten.

Unterstützte DLP-Systeme

Der StorageZones Controller verwendet das ICAP-Protokoll, um mit DLP-Lösungen von Drittanbietern zu interagieren. Die Verwendung von ShareFile mit einer vorhandenen DLP-Lösung erfordert keine Änderungen an vorhandenen Richtlinien oder Servern. Sie können jedoch ICAP-Server für die Verarbeitung von ShareFile Daten dedizieren, wenn Sie erwarten, dass die Last signifikant ist.

Zu den beliebten ICAP-konformen DLP-Lösungen gehören:

- Symantec Data Loss Prevention
- McAfee DLP Prevent
- Websense TRITON AP-DATA
- RSA Data Loss Prevention

Da ShareFile Ihre vorhandene DLP-Sicherheitssuite verwendet, können Sie einen zentralen Richtlinienverwaltungspunkt für Dateninspektionen und Sicherheitswarnungen verwalten. Wenn Sie bereits eine der vorhergehenden Lösungen zum Scannen ausgehender E-Mail-Anhänge oder Webdatenverkehr auf vertrauliche Daten verwenden, können Sie den ShareFile StorageZones Controller auf denselben Server verweisen. Für diese bestehenden DLP-Systeme unterstützen wir auch sicheres ICAP (ICAPS), wenn das zugrunde liegende DLP-System selbst ICAPS unterstützt.

DLP aktivieren

Um DLP für ShareFile und den StorageZones Controller zu aktivieren, führen Sie die folgenden drei Aktionen aus:

1. Aktivieren Sie DLP-Funktionen für Ihr 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 von DLP-Funktionen für Ihr ShareFile Konto

Um anzufordern oder zu bestätigen, dass Ihre ShareFile Unterdomäne für DLP aktiviert ist, senden Sie eine Anfrage an Citrix Support.

Bei einigen Konten erfordert die Aktivierung von DLP möglicherweise auch eine neuere Benutzererfahrung für die ShareFile Website. Nachdem Ihr Konto für DLP aktiviert wurde, können Sie mit der Aktivierung von DLP auf dem StorageZones Controller-Server fortfahren.

Aktivieren von DLP auf dem StorageZones Controller-Server

Gehen Sie wie folgt vor, um DLP-Einstellungen für die StorageZones Controller er-Bereitstellung zu konfigurieren:

1. Installieren oder aktualisieren Sie StorageZones Controller 3.2 oder höher.
2. Klicken Sie in der Storage Zones Controller Konsole `http://*localhost*/configservice/login.aspx` auf die Registerkarte **ShareFile Daten**. Klicken Sie auf **Ändern**, wenn die Zone vorhanden ist.
3. Aktivieren Sie das Kontrollkästchen **DLP-Integration aktivieren**, und geben Sie die ICAP-Adresse Ihres DLP-Servers in das Feld **ICAP REQMOD-URL** ein. Das Adressformat lautet:

```
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**.

Überprüfen Sie nach dem Aktivieren von DLP, ob der DLP-Server erreichbar ist, indem Sie den Eintrag **DLP ICAP-Serverstatus** auf der Registerkarte **Überwachung** überprüfen.

Steuern des Zugriffs auf Basis von DLP-Scan-Ergebnissen

Nachdem DLP auf dem Konto- und StorageZones Controller 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 beschränken die normalen Berechtigungen und Freigabesteuerungen, die für Dateien basierend auf ihrer DLP-Klassifizierung verfügbar sind. Wenn ein Dokument freigegeben wird, kann ein Benutzer weiterhin anonymen Zugriff blockieren, selbst wenn DLP-Einstellungen es erlauben würden, es anonym freizugeben. Wenn der Benutzer jedoch versucht, eine Datei auf eine Weise freizugeben, die DLP-Einstellungen verletzt, verhindert ShareFile dies.

Die Datenklassifizierungen sind:

- **Gescannt**: OK — Dateien, die von einem DLP-System gescannt und OK übergeben wurden.
- **Gescannt: Abgelehnt** — Dateien, die von einem DLP-System gescannt wurden und sensible Daten enthalten.
- **Nicht gescannt** — 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, da das externe DLP-System nicht verfügbar ist oder langsam reagiert.

Die Klassifizierung jedes Elements wird durch die ICAP-Server-Antwortregel bestimmt. Wenn der DLP-ICAP-Server mit einer Meldung antwortet, dass der Inhalt blockiert oder entfernt werden soll, wird die Datei als **Gescannt: Abgelehnt**markiert. Andernfalls wird die Datei als **Gescannt gekennzeichnet: OK**.

Für jede Datenklassifizierung können Sie unterschiedliche Zugriffs- und Freigabebeschränkungen festlegen. Für jede der drei Kategorien wählt der ShareFile Administrator die Aktionen aus, die zugelassen werden sollen:

- Mitarbeiter können die Datei herunterladen oder freigeben.
- Clientbenutzer von Drittanbietern können die Datei herunterladen oder freigeben. Die Clientfreigabe ist standardmäßig deaktiviert, kann aber unter **Admin > Erweiterte Einstellungen > Clients das Freigeben von Dateien zulassen aktiviert werden**.
- Anonyme Benutzer können die Datei herunterladen

Wenn ein Benutzer eine Datei freigibt, können nur Benutzer mit Downloadberechtigungen die Datei empfangen. Wenn Sie die Freigabeberechtigung für eine Datenklassifizierung aktivieren, müssen Sie daher mindestens eine Klasse von Benutzerdownloadberechtigungen erteilen.

So konfigurieren Sie DLP-Einstellungen in ShareFile

1. Klicken Sie in der ShareFile e-Weboberfläche auf **Admin > Prävention vor Datenverlust**.
2. Ändern Sie die Option **Zugriff auf Dateien basierend auf ihrem Inhalt beschränken** auf **Ja**.
3. Konfigurieren Sie die zulässigen Aktionen für jede Datenklassifizierung.

> **Wichtig:**
>
> Für das ShareFile On-Demand Sync stool sind Downloadberechtigungen für den normalen Betrieb erforderlich. Aktivieren Sie Mitarbeiterdownloads für alle Inhaltsklassifizierungen, wenn Ihre Bereitstellung ShareFile On-Demand Sync enthält.

Wenn der StorageZones Controller eine Datei an das DLP-System sendet, enthält er 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, spezifische Details für ShareFile zu Dateien anzuzeigen, die vertraulichen Inhalt enthalten.

Erweiterte Einstellungen für DLP

Um den DLP-Scanvorgang anzupassen, bearbeiten Sie die Einstellungsdatei, die auf Ihrem StorageZones Controller unter gefunden wurde `wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`. In der folgenden Tabelle werden die einzelnen Einstellungen beschrieben, die sich auf DLP beziehen.

Einstellung	Beschreibung	Standardwert
scan-interval	Wie häufig der DLP-Dienst die DLP-Warteschlange auf neue Dateien überprüft und zur Verarbeitung an den DLP-ICAP-Server sendet.	30 Sekunden
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	Kommagetrennte Liste von Erweiterungen, die vom DLP-Scan ausgeschlossen werden sollen. Der DLP-Server verarbeitet keine Dateien mit Namen, die auf eine der folgenden Erweiterungen enden, sondern markiert die Dateien als Gescannt: OK. Beispielwert: “exe, jpg, bin, mov”	Ohne
icap-max-file-size-bytes	Maximale Dateigröße (in Byte), die zur Verarbeitung an den DLP-Server gesendet werden soll. Ein Wert von 0 bedeutet, dass kein Maximum vorhanden ist und alle Dateigrößen gesendet werden. Wenn der DLP-Server mit einem Wert ungleich Null konfiguriert ist, verarbeitet der DLP-Server keine Dateien, die größer als die konfigurierte Größe sind, sondern als “Gescannt: OK” gekennzeichnet sind.	31457280 (30 MB)

Einstellung	Beschreibung	Standardwert
x-queue-items-to-process	Die maximale Anzahl von Elementen in der Warteschlange, die pro Scan-Intervall-Iteration gescannt werden sollen. Verringern Sie diesen Wert, um die Auswirkungen auf den DLP-Server zu verringern, wenn eine große Anzahl von Dateien zur StorageZone hinzugefügt wird.	512
max-queue-processing-threads	Maximale Anzahl gleichzeitiger Prozessor-Threads, die zum Entleeren der DLP-Scan-Warteschlange verwendet werden sollen. Legen Sie diesen Wert basierend auf der maximalen Anzahl gleichzeitiger Verbindungen zu Ihrem ICAP-Server fest. 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 Netzwerkaufrufe mit dem PUT-Verb gemacht. 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 DLP-Anbietern (Data Loss Prevention, Data Loss Prevention) über ICAP.

ICAP-Dienste arbeiten jedoch durch Warteschlangen, die nur durch neu erstellte Dateien aufgefüllt werden. Das bedeutet, dass Dateien, die in einer Zone vorhanden sind, bevor ICAP aktiviert wird, nicht von den Diensten gescannt werden. Mit diesem Tool können Sie diese Dateien zum Scannen in die Warteschlange stellen und gescannte Dateien zum erneuten Scannen in die Warteschlange stellen.

Wie der Name besagt, funktioniert das Tool derzeit nur für den DLP-ICAP-Dienst.

Anforderungen

Das Tool ist ein PowerShell -Skript und benötigt daher PowerShell zum Ausführen. PsExec oder ein ähnliches Tool wird ebenfalls benötigt, da das Skript als Netzwerkdienst für den Zugriff auf den Speicherort der Netzwerkfreigabe ausgeführt werden muss.

Standort

Für einen installierten StorageZones Controller finden Sie das Tool unter `<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1`. Der Installationsort des StorageZones Controller ist standardmäßig `C:\inetpub\wwwroot\Citrix\StorageCenter`.

Überlegungen vor dem Ausführen des Werkzeugs

Das Werkzeug muss möglicherweise mehrere Male für einen einzelnen Vorgang ausgeführt werden, abhängig von der folgenden.

- Die Einschränkungen für die Warteschlangengrößenbeschränkung.
- Die Anzahl der Elemente für die angegebenen Kriterien. Diese Überlegung gilt, es sei denn, die Warteschlangengrößenbeschränkung ist auf Null oder weniger festgelegt. In diesem Fall nimmt das Tool eine maximale Größe von 200.000 Elementen im Warteschlangenverzeichnis an.

Wenn das Werkzeug beispielsweise verwendet wird, um nicht gescannte Elemente in die Warteschlange zu stellen, wird die Warteschlangengrößenbeschränkung auf 500 Elemente festgelegt. Wenn mehr als 500 nicht gescannte Elemente vorhanden sind, stoppt das Tool, nachdem 500 Elemente in der Warteschlange gefüllt wurden. Um zu verfolgen, wo es gestoppt wurde, 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 Durchlauf sucht das Tool nach dieser Datei. Wenn die Datei vorhanden ist, verwendet das Werkzeug das Erstellungsdatum darin als Markierung für den nächsten Stapel von Dateien. Das Tool löscht die temporäre Datei nach Abschluss eines bestimmten Vorgangs nicht. Stattdessen kann der Zonenadministrator die Datei löschen, sobald alle Batches für einen bestimmten Vorgang abgeschlossen sind. Aufgrund dieser Situation sollte, wenn ein vollständiger Vorgang abgeschlossen ist, die temporäre Datei, falls vorhanden, manuell entfernt werden, bevor eine andere Operation ausgeführt wird.

Ausführen des Werkzeugs mit PSExec

Öffnen Sie ein Befehlsfenster und führen Sie PSExec mit dem folgenden Befehl aus.

```
1 PsExec.exe -i -u ”nt authority\network service”
2
3 ”C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe”
```

Dadurch wird PowerShell geöffnet, die als Netzwerkdienst ausgeführt wird. Um zu überprüfen, ob es tatsächlich als Netzwerkdienst ausgeführt wird, führen Sie **whoami** aus und überprüfen Sie das Ergebnis.

Nachdem PowerShell geöffnet ist, führen Sie das Tool direkt dort aus, um alle erforderlichen Aufgaben auszuführen.

```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
     \DLPExistingFiles.ps1 <options>
```

Befehlszeilenoptionen

Für die Ausführung des Werkzeugs 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:
  - **Unscanned**: Nicht gescannte Dateien. Zum Beispiel Dateien vor der DLP-Ära, 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 in der Warteschlange zulässigen Elemente anzugeben, bevor das Werkzeug beendet wird.

- **-date** (Optional): Das maximale Erstellungsdatum der Elemente, die zum Scannen in die Warteschlange gestellt werden sollen. Wenn das Datum beispielsweise als “30.10.2017 11:30 Uhr” 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 die Warteschlange zu stellen.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Unscanned
```

Führen Sie den folgenden Befehl aus, um alle gescannten Elemente in einer Zone mit einer Warteschlangenbeschränkung von 100 in die Warteschlange einzureichen.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Scanned -queueLimit 100
```

Führen Sie den folgenden Befehl aus, um alle gescannten Elemente, die vor 11:30 Uhr am 30.10.2017 mit den folgenden Eigenschaften erstellt wurden, in einer Zone mit einer Warteschlangenbeschränkung von 200 als sauber markiert wurden.

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan ScannedOK -queueLimit 200 -date ”
    10/30/2017 11:30 AM”
```

Überwachung

June 11, 2020

Der StorageZones Controller und die ShareFile e-Administratorschnittstelle enthalten mehrere Ressourcen, mit denen Sie die Aktivität des StorageZones Controller überwachen und Probleme beheben können:

- **Allgemeiner Komponentenstatus** — Die Registerkarte Überwachung in der Storage Zones Controller Konsole enthält den Komponentenstatus, mit dem Sie den Fehlerbehebungsprozess starten können. Der Status wird für Elemente wie Zugriffsberechtigungen, Dienststatus und Heartbeat-Status bereitgestellt, der die ausgehende Konnektivität des StorageZones Controller mit der ShareFile Steuerungsebene angibt.

  Der StorageZones Controller sendet alle 5 Minuten Updates an die ShareFile e-Webanwendung. Wenn die ShareFile e-Webanwendung innerhalb von 10 Minuten kein Update erhält, markiert sie den StorageZones Controller als offline.

  Für Elemente auf der Registerkarte Überwachung, die rot angezeigt werden, überprüfen Sie die Protokolldateien, um detaillierte Informationen zu erhalten.

  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 Speicherzonen erreichen kann oder ob ein Client die Zone erreichen kann.

- Informationen zu**Speicherzonen Controller -Serverinformationen** — Informationen zur Speichernutzung, Netzwerknutzung und Dateiaktivität des Servers: Melden Sie sich über die ShareFile-Schnittstelle bei Ihrem ShareFile Enterprise-Konto an, gehen Sie zu **Admin > StorageZones** , klicken Sie auf die Speicherzone, und klicken Sie dann auf eine -Hostname des StorageZones Controller.

- **Zoneninformationen** — Informationen zur Speicherverwendung, Netzwerknutzung und Dateiaktivität für eine Zone erhalten Sie: Melden Sie sich über die ShareFile-Benutzeroberfläche bei Ihrem ShareFile Enterprise-Konto an, gehen Sie zu **Admin > StorageZones**und klicken Sie auf einen Zonennamen.

- **Integritätsstatus des StorageZones Controller** — Um festzustellen, ob ShareFile.com Heartbeat-Nachrichten von den StorageZones Controllern empfängt, die mit der Zone verbunden sind, zeigen Sie den Integritätsstatus an: Melden Sie sich über die ShareFile-Schnittstelle bei Ihrem ShareFile Enterprise-Konto an, gehen Sie zu **Admin > StorageZones**, überprüfen Sie, ob die Spalte Integrität ein grünes Häkchen hat, und klicken Sie dann auf den Standortnamen, um zu überprüfen, ob die Heartbeat-Meldung angibt, dass der StorageZones Controller reagiert.

- **Protokolldateien** — Protokolldateien enthalten detaillierte Informationen zur Konfiguration des StorageZones Controller und seiner Komponenten, wie im nächsten Abschnitt beschrieben.

Protokolldateien

Die folgenden Protokolldateien für den StorageZones Controller befinden sich standardmäßig in`C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`:

Name der Protokolldatei	Enthält Protokollierungsinformationen für:
cfgsrv-%date%.txt	Konfigurationsaktionen für StorageZones Controller, einschließlich Ändern einer vorhandenen StorageZones-Konfiguration, Erstellen einer neuen StorageZones und Verknüpfung eines neuen StorageZones Controllers mit einem vorhandenen primären StorageZones Controller
sc-%date%.txt	ShareFile Daten-Upload- und Download-Aktivität für Standardzonen
CIFS-%date%.txt	StorageZone Connector für die Upload- und Download-Aktivität von Netzwerkdateifreigaben
sharepoint-%date%.txt	StorageZone Connector für SharePoint-Upload- und Download-Aktivität
cloudstorageuploader-%date%.txt	Cloud Storage Uploader Service (auf ein unterstütztes Speichersystem eines Drittanbieters)
kopieren-%date%.txt	ShareFile Kopierdienst
löschen—%date%.txt	ShareFile Cleanup-Dienst, für den persistenten Speicher-Cache
s3uploader–%date%.txt	ShareFile Verwaltungsdienst. Beinhaltet Heartbeat-Statusmeldungen

Die erweiterte Protokollierung ist für jede der folgenden Komponenten verfügbar und ist nützlich, wenn Sie detaillierte Informationen zur Unterstützung bereitstellen müssen.

Komponente	Speicherort von AppSettingsRelease.config
ShareFile Daten	C:\inetpub\wwwroot\Citrix\StorageCenter
StorageZone Connector für Netzwerkdateifreigaben	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
StorageZone Connector für SharePoint	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

So aktivieren Sie die erweiterte Protokollierung

Die folgenden Schritte ermöglichen die erweiterte Protokollierung für alle Storage Zones Controller Komponenten und -Dienste:

1. Öffnen Sie IIS auf dem StorageZones Controller-Server.
2. Navigieren Sie zur Standardwebsite, und öffnen Sie dann die Anwendungseinstellungen.
3. Ändern Sie den Wert für Enable-Extended-Logging von 0 in 1.
4. Starten Sie den Citrix ShareFile Verwaltungsdienst neu.
5. Nachdem Sie das Problem behoben haben, empfehlen wir Ihnen, die erweiterte Protokollierung zu löschen, um die 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 IIS-Protokolle überprüfen, um festzustellen, ob der Datenverkehr den StorageZones Controller erreicht. IIS-Protokolle zeigen alle eingehenden Anforderungen an. IIS-Protokolle für StorageZones Controller sind in c:\inetpub\logs\LogFiles\W3SVC1.

Informationen zum Aktivieren der erweiterten IIS-Protokollierung finden Sie unter http://support.microsoft.com/kb/313437.

Problembehandlung bei Installation und Konfiguration

Problem	Beschreibung und Lösung
“HTTP-Fehler 404 - Datei oder Verzeichnis nicht gefunden” wird während der Konfiguration des StorageZones Controller angezeigt	Die Meldung resultiert in der Regel auf ein Problem mit IIS oder `ASP.NET`. Stellen Sie sicher, dass die IIS-Rolle bei der Windows-Installation aktiviert ist und dass das `ASP.NET` Feature auf IIS aktiviert ist.
“HTTP Error 404.2 — Not Found” erscheint beim Durchsuchen von localhost auf dem Storage Zones Controller	Die Meldung zeigt an, dass ISAPI- und CGI-Einschränkungen für nicht auf Zulässig festgelegt `ASP.NET` sind.

Problem	Beschreibung und Lösung
“HTTP Error 413 — Request Entity zu groß” wird nach einem Upload-Versuch angezeigt	Die Nachricht kann nach einem fehlgeschlagenen Upload-Versuch in eine Speicherzone in einer Netzwerkablaufverfolgung angezeigt werden und kann aus einer Clientzertifikateinstellung in IIS resultieren. Um dieses Problem zu umgehen, öffnen Sie IIS auf dem StorageZones Controller-Server. Navigieren Sie zur Standardwebsite und öffnen Sie dann SSL-Einstellungen. Wählen Sie für Clientzertifikate die Option Ignorieren aus. Starten Sie den Citrix ShareFile Verwaltungsdienst neu.
IIS-Fehler treten während der Konfiguration des StorageZones Controller auf	IIS-Fehler weisen in der Regel darauf hin, dass nicht vollständig konfiguriert `ASP.NET` ist. Überprüfen Sie im IIS-Manager unter ISAPI- und CGI-Einschränkungen, dass die Einschränkung für alle `ASP.NET` Listings auf Zulässig festgelegt ist. Überprüfen Sie, ob in IIS registriert `ASP.NET` ist: Stellen Sie im IIS-Manager unter Anwendungspools sicher, dass `ASP.NET` Angebote vorhanden sind. Informationen zur manuellen Registrierung `ASP.NET`finden Sie in den Befehlszeilen nach dieser Tabelle. Wenn weiterhin Probleme auftreten, überprüfen Sie IIS und `ASP.NET` Setup.

Problem	Beschreibung und Lösung
“Speichercenterbindung konnte nicht gespeichert werden” wird während der Konfiguration des StorageZones Controller angezeigt.	Die Meldung weist auf ein Berechtigungsproblem für den IIS-Kontenpool-Benutzer hin. Standardmäßig arbeiten Anwendungspools unter dem Netzwerkdienst-Benutzerkonto. Der StorageZones 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, keine Berechtigung zum Erstellen und Verwalten von Zonen besitzt. Verwenden Sie die ShareFile Administratorkonsole, um diese Berechtigung festzulegen.
Ausgehende Anfragen werden blockiert	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 Systemanforderungen des Storage Zones Controller angegeben sind.

Problem	Beschreibung und Lösung
“Verbindung zum Remoteserver kann nicht hergestellt werden” wird angezeigt, wenn Sie sich am StorageZones Controller anmelden	Die Meldung weist in der Regel 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 StorageZones Controller aus bei Ihrem ShareFile e-Konto anmelden können. Stellen Sie sicher, dass Sie über Berechtigungen auf Administratorebene zum Konfigurieren des StorageZones Controller verfügen und dass Port 443 auf der externen Firewall geöffnet ist.
Der Ordner ShareFileStorage auf Ihrer Netzwerkfreigabe enthält Sckeys.txt nicht, nachdem Sie Speicherzonen für ShareFile Daten aktivieren und konfigurieren	Storage Zones Controller erstellt Sckeys.txt während der Installation, es sei denn, das Konto, das Sie zum Installieren von Storage Zones Controller verwendet haben, befindet sich nicht in der Zugriffssteuerungsliste. Aktualisieren Sie die Zugriffskontrollliste und installieren Sie den StorageZones Controller neu.
Datei-Uploads in einen freigegebenen Ordner schlagen fehl, nachdem Sie eine Zone erstellen	Dieses Problem weist auf ein Problem mit Ihrem internen DNS hin. Sie müssen sowohl über einen internen als auch über einen externen DNS-Eintrag für den FQDN des StorageZones Controller verfügen.

Problem	Beschreibung und Lösung
Auf der Registerkarte **Überwachung** ist der Heartbeat-Status rot	Ein rotes Symbol zeigt an, dass der Storage Zones Controller keine Heartbeat-Nachrichten an die ShareFile Website senden kann. Überprüfen Sie, ob die Symbole für andere Komponenten rot sind. Wenn dies der Fall ist, finden Sie in den Protokollen weitere Informationen. Wenn das Protokoll s3uploader einen Fehler beim Senden des Heartbeats anzeigt, kann der StorageZones Controller-Server möglicherweise keine Verbindung mit der ShareFile-Website herstellen, es sei denn, er geht über einen Proxyserver. Um einen Proxyserver für den StorageZones Controller anzugeben, öffnen Sie die Controller-Konsole und wechseln Sie zur Registerkarte Netzwerk. Wenn der StorageZones Controller-Server nicht mit einem Netzwerkdienstbenutzer auf die ShareFile-Website zugreifen kann, gestatten 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 in der ShareFile Administratorschnittstelle nicht angezeigt	Dieses Problem kann auf ein Problem mit der externen Adresse oder Firewall hinweisen. Überprüfen Sie zunächst in der StorageZones 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 die Windows-Firewall korrekt konfiguriert ist. Standardmäßig erlauben die Windows-Firewalleinstellungen ausgehenden Datenverkehr für die ShareFile Dienste auf Port 443. Storage Zones 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
Storage Zones 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 über die ShareFile Steuerungsebene, den StorageZones Controller und ShareFile-Clients Citrix ADC erreicht. Wenn Sie eine Datei hochladen und der virtuelle Server einen Anstieg der Treffer anzeigt, wird der Datenverkehr über Citrix ADC geleitet. Überprüfen des Datenverkehrs für jeden Punkt der Citrix ADC Verbindung: Content Switching Virtual Server, Load Balancing Virtual 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 Bindung der Responderrichtlinie im virtuellen Lastausgleichsserver für ShareFile-Daten aufheben. (Die Responderrichtlinie löscht eingehenden Datenverkehr, der nicht von der ShareFile Steuerungsebene signiert ist. Geben Sie in einem Webbrowser den externen FQDN des StorageZones Controller ein. Wenn eine Verbindung besteht, wird das ShareFile Logo angezeigt. Geben Sie in einem Webbrowser die URL für einen Connector ein. Wenn die folgenden URLs die Barrierefreiheit von StorageZone Connector testen konnten, werden Sie zur Eingabe von Anmeldeinformationen aufgefordert, selbst 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 wie folgt: {“Name”:”connectorName”,”FileName”:”FileName”,”CreationD `://szc-address/cifs/v3/$metadata##`

Problem	Beschreibung und Lösung
Der Status ShareFile Connectivity von File Cleanup Services ist ein rotes Symbol nach dem Upgrade des StorageZones Controller	Ein rotes Symbol tritt auf, wenn Windows den Dateibereinigungsdienst startet, bevor der StorageZones Controller eine Netzwerkverbindung aufbaut. Der Status wird auf ein grünes Symbol zurückgesetzt, nachdem der Controller -Server wieder im Netzwerk ist.
“Pfad überschreitet die maximale Länge (1024)” wird während der Konnektorerstellung angezeigt	Die Meldung kann auftreten, wenn die für den StorageZones Controller konfigurierte externe Adresse auf die ShareFile-Website anstelle des FQDN des StorageZones Controller-Servers verweist.
“Ungültiger Name” wird angezeigt, wenn ein neuer Storage Zones Controller konfiguriert wird, nachdem ein alter gelöscht wurde.	Die Meldung kann auftreten, wenn Entitäten im Zusammenhang mit dem alten StorageZones Controller noch vorhanden sind. Um dieses Problem zu beheben: Deinstallieren Sie den neuen Storage Zones 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 Sie einen neuen Storage Zones Controller. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren Support-Mitarbeiter. Diese Meldung tritt auf, wenn Storage Zone Server den FQDN der Storage Zone nicht über DNS oder die lokale Hosts-Datei auflösen können.

So registrieren Sie sich manuell 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 Web-Apps

Wenn ein mobiles Gerät keine Verbindung zu einem Connector herstellen kann, überprüfen Sie die Konnektivität. Viele Konnektivitätsprobleme werden in der obigen Tabelle behandelt. Stellen Sie sicher, dass der Storage Zones Controller online ist. Laden Sie eine Datei in die Zone hoch. Wenn der Upload funktioniert, ist das Problem spezifisch für Connectors. Versuchen Sie, über das Mobilfunk- und Firmennetzwerk eine Verbindung vom mobilen Gerät herzustellen. Überprüfen Sie, ob der SharePoint-Server oder Dateiserver verfügbar ist.

Wenn beim Versuch, auf einen Connector zuzugreifen, ein “HTTP-Fehler 401 — Nicht autorisiert” angezeigt wird, kann es sich um eines der folgenden Probleme handeln, die verhindern können, dass ein Benutzer von ShareFile-Clients oder der ShareFile Webanwendung auf einen Connector zugreifen kann:

- Falsche Konfiguration von IIS: Stellen Sie sicher, dass die Webdienste-Rolle (IIS) Standardauthentifizierung und Windows-Authentifizierung aktiviert ist. Wenn diese Optionen nicht unter Sicherheit aufgeführt sind, verwenden Sie den Server-Manager, um sie zu installieren, und starten Sie IIS neu.
- Falsche Benutzerberechtigungen: Stellen Sie sicher, dass der AD-Benutzer Zugriff auf die Freigabe hat. Wechseln 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 Überwachungsgruppenzugriff. Informationen zur Fehlerbehebung finden Sie unter <CTX126589.

Wenn beim Herstellen einer Verbindung mit einer SharePoint-Website ein “HTTP-Fehler 403 — Forbidden” angezeigt wird, wird der SharePoint-Server möglicherweise für die Standardauthentifizierung konfiguriert, aber der StorageZones Controller ist möglicherweise nicht so konfiguriert, dass Anmeldeinformationen zwischengespeichert werden. Um dieses Problem zu beheben, fügen Sie <add key=”CacheCredentials”value=”1”/> zu hinzu `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

Wenn ein “HTTP-Fehler 503 — Dienst nicht verfügbar” angezeigt wird, wenn mobile Apps versuchen, auf einen Connector zuzugreifen, senden Connectors eine Antwort, können die HTTP-Anforderung jedoch nicht verarbeiten. Dies kann auftreten, wenn Richtlinien zum Umschalten von Inhalten, 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.

Eingeschränkte Speicherzonen

June 11, 2020

Eingeschränkte Speicherzonen werden zum Schutz vertraulicher Daten verwendet. Nur Mitarbeiter können auf eingeschränkten Speicher zugreifen.

Die Authentifizierung von Drittanbietern wird in der eingeschränkten Zone nicht unterstützt.

> **Hinweis:**
>
> Eingeschränkte Speicherzonen sind Ende der Wartung. Diese Lebenszyklusrichtlinie wird ausführlicher unter Lebenszyklus-Meilensteine Definitionen. Das Erstellen neuer eingeschränkter Speicherzonen wird nicht unterstützt. Bestehende Kunden, die eingeschränkte Lagerzonen nutzen, erhalten weitere Informationen über zukünftige Produktmeilensteine.

Eingeschränkte Zonenfunktionen

Zonenauthentifizierung: Zusätzlich zur Anmeldung bei ShareFile müssen sich Benutzer separat beim StorageZones Controller authentifizieren, um auf Dokumente zuzugreifen, die in einer eingeschränkten Zone gespeichert sind. Die Verzeichnissuche stellt sicher, dass der Benutzer, der sich bei ShareFile anmeldet, derselbe ist, der sich bei der Zone authentifiziert. Diese zusätzliche Authentifizierungsanforderung beschränkt die Freigabe. Dokumente können nur für andere freigegeben werden, die Zugriff auf den Storage Zones Controller haben und die sich mit Enterprise-Anmeldeinformationen authentifizieren können. In einer eingeschränkten Zone können Dateien nicht anonym freigegeben werden. Benutzer müssen die Berechtigung zum Anzeigen einer Datei erhalten und müssen sich immer anmelden, um eine freigegebene Datei zu erhalten.

Metadatenverschlüsselung: Alle Informationen zu Dateien und Ordnern in der Zone werden mit Ihrem Schlüssel verschlüsselt, bevor sie an ShareFile gesendet werden. Daher kann niemand außerhalb Ihrer Organisation Ordner- oder Dateinamen in eingeschränkten Zonen sehen. Der Zugriff auf Verschlüsselungsschlüssel, entschlüsselte Dateien und Metadaten ist nur über die Enterprise-Authentifizierung zum StorageZones Controller verfügbar.

Interne Adresse für Storage Zones Controller: Für eine eingeschränkte Zone erfolgt die Autorisierung zwischen Storage Zones Controller und ShareFile Clients statt zwischen Storage Zones Controller und der ShareFile-Cloud. Daher erfordert ein StorageZones Controller, der eingeschränkte Zonen hostet, keine externe Adresse oder ein externes SSL-Zertifikat. Wenn der StorageZones Controller mit einer nur internen Adresse konfiguriert ist, müssen Benutzer eine Verbindung zum

Unternehmensnetzwerk oder VPN herstellen, um auf Dokumente in der eingeschränkten Zone zuzugreifen.

E-Mail-Benachrichtigungen von Ihrem Mail-Server: Wenn Benutzer E-Mail-Benachrichtigungen über freigegebene Dateien und Ordner in einer eingeschränkten Zone erhalten, wird die E-Mail von Ihrem internen Mail-Server anstelle von einem ShareFile Server gesendet.

Unterschiede zwischen Standard- und Sperrzonen

Properties	Standardzonen	Eingeschränkte Zonen
Storage-Zonen-Server können verwaltet werden von…	Citrix oder Sie	Sie
Die Benutzerauthentifizierung wird von…	`ShareFile.com` oder `ShareFile.eu`	eine Kombination aus `ShareFile.com` oder `ShareFile.eu` plus Ihrem lokalen Storage Zones Controller
Dateien können gemeinsam genutzt werden mit…	Mitarbeiter und Drittanbieter (d. h. jeder mit einer E-Mail-Adresse)	Mitarbeiter oder andere Benutzer, die ein Domänenkonto haben
Datei- und Ordnermetadaten, die in der ShareFile Steuerungsebene gespeichert sind, sind…	im Klartext gespeichert, sichtbar für einige Citrix Mitarbeiter	verschlüsselt mit Ihren privaten Schlüsseln, die für Citrix nicht verfügbar sind
E-Mail-Benachrichtigungen werden über…	ShareFile Mailserver oder Ihre SMTP-Server	Ihre SMTP-Server
Eine externe Adresse für die Zone ist…	erforderlich	nicht erforderlich

Standard- und eingeschränkte Lagerzonen

Sie können eine Speicherzone als Standard oder eingeschränkt festlegen.

- Eine Standard-Speicherzone ist für nicht-vertrauliche Daten gedacht und ermöglicht Mitarbeitern das Freigeben von Daten für Personen, die keine Mitarbeiter sind.
- Eine eingeschränkte Speicherzone schützt sensible Daten: Nur Mitarbeiter können auf die in der Zone gespeicherten Daten zugreifen.

In der folgenden Tabelle werden die Unterschiede zwischen Standard- und eingeschränkten Zonen zusammengefasst.

Properties	Standardzonen	Eingeschränkte Zonen
Storage-Zonen-Server können verwaltet werden von…	Citrix oder Sie	Sie
Die Benutzerauthentifizierung wird von…	`ShareFile.com` oder `ShareFile.eu`	eine Kombination aus `ShareFile.com` oder `ShareFile.eu` plus Ihrem lokalen Storage Zones Controller
Dateien können gemeinsam genutzt werden mit…	Mitarbeiter und Drittanbieter (d. h. jeder mit einer E-Mail-Adresse)	Mitarbeiter oder andere Benutzer, die ein Domänenkonto haben
Datei- und Ordnermetadaten, die in der ShareFile Steuerungsebene gespeichert sind, sind…	im Klartext gespeichert, sichtbar für einige Citrix Mitarbeiter	verschlüsselt mit Ihren privaten Schlüsseln, die für Citrix nicht verfügbar sind
E-Mail-Benachrichtigungen werden über…	ShareFile Mailserver oder Ihre SMTP-Server	Ihre SMTP-Server
Eine externe Adresse für die Zone ist…	erforderlich	nicht erforderlich

In einer von Citrix verwalteten Zone führt die ShareFile Cloud alle Vorgänge mit Ausnahme der Mitarbeiterauthentifizierung durch, die vom StorageZones Controller verarbeitet wird.

In der Standardzone werden Websitewartung und -aktualisierungen, Client- und Anwendungsaktualisierungen, Dateimetadaten, Upload- und Downloadautorisierung, E-Mail-Benachrichtigungen (SMTP), Authentifizierung von Drittanbietern und Ordnerberechtigungen in der Cloud verarbeitet. Mitarbeiterauthentifizierung sowie Dateispeicherung und Verschlüsselung werden vom Controller verwaltet.

In der eingeschränkten Zone werden Websitewartung und -aktualisierungen, Client- und Anwendungsaktualisierungen sowie Ordnerberechtigungen in der Cloud verarbeitet. Mitarbeiterauthentifizierung, Dateispeicherung und Verschlüsselung, Dateimetadaten, Upload- und Download-Autorisierung sowie E-Mail-Benachrichtigungen (SMTP) werden vom Controller verarbeitet. Die Authentifizierung von Drittanbietern wird in der eingeschränkten Zone nicht unterstützt.

ShareFile unterstützt eine Mischung aus Standard- und eingeschränkten Zonen innerhalb eines Kontos. Sie können mehrere eingeschränkte Zonen erstellen, jede mit ihren eigenen eindeutigen Authentifizierungsanforderungen. Wenn Benutzer in Domäne A beispielsweise keine Dateien für Benutzer in Domäne B freigeben dürfen, installieren Sie für jede Domäne eine separate eingeschränkte Zone.

Der Rest dieses Abschnitts beschreibt den Workflow in ShareFile-verwalteten, Standard- und eingeschränkten Zonen.

Proof-of-Concept-Bereitstellung für eingeschränkte Speicherzonen

Ein StorageZones Controller, der für eingeschränkte Zonen konfiguriert ist, muss keine eingehenden Verbindungen aus der ShareFile e-Cloud akzeptieren: Sie können ihn mit einer internen Adresse konfigurieren. Die folgende Abbildung zeigt den Datenverkehr zwischen Benutzergeräten, der ShareFile Cloud und dem StorageZones Controller.

In diesem Szenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Der StorageZones Controller befindet sich innerhalb der Firewall, um den Zugriff zu steuern. Benutzerverbindungen zu ShareFile müssen die Firewall durchlaufen 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 SSL-Zertifikat, das privat sein kann, auf dem IIS-Dienst des StorageZones Controller installieren.

Bei eingeschränkten Zonen sendet der Storage Zones Controller E-Mail-Benachrichtigungen von Ihrem lokalen SMTP-Server statt von ShareFile.

Hochverfügbarkeitsbereitstellung für eingeschränkte Zonen

StorageZones Controller, die für eingeschränkte Zonen konfiguriert sind, müssen keine eingehenden Verbindungen aus der ShareFile e-Cloud akzeptieren: Sie können jeden mit einer internen Adresse konfigurieren. Die folgende Abbildung zeigt eine Bereitstellung mit hoher Verfügbarkeit für eingeschränkte Zonen.

In diesem Szenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Die StorageZones Controller befinden sich in der Firewall, um den Zugriff zu steuern. Benutzerverbindungen zu ShareFile müssen die Firewall durchlaufen 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 SSL-Zertifikat, das privat sein kann, auf dem IIS-Dienst des StorageZones Controller installieren.

Bei eingeschränkten Zonen sendet der Storage Zones Controller E-Mail-Benachrichtigungen von Ihrem lokalen SMTP-Server statt von ShareFile.

Eingeschränkte Zonen

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

Schritt	Quelle	Ziel
1. Benutzeranmeldeanforderung	Client	`company.sharefile.com`
2. Wenn Sie ADFS verwenden, leiten Sie zur SAML-IdP-Anmeldung um	Client	SAML-Identitätsanbieter-URL
3. Datei-/Ordner-Aufzählung und Download-Anforderung	Client	`szc.company.com`
4. Dateidownload-Autorisierung und verschlüsselte Metadaten abrufen	`szc.company.com`	`company.sharefile.com`
5. Dateidownload	Client	`szc.company.com`

Bereitstellung für eingeschränkte Speicherzonen

Die folgende Abbildung zeigt eine Bereitstellung mit hoher Verfügbarkeit für eingeschränkte Zonen.

Bei eingeschränkten Zonen sendet der Storage Zones Controller E-Mail-Benachrichtigungen von Ihrem lokalen SMTP-Server statt von ShareFile.

Netzwerkverbindungen für eingeschränkte Zonen

Im folgenden Diagramm und in der Tabelle werden die Netzwerkverbindungen beschrieben, die auftreten, wenn sich ein Benutzer bei ShareFile anmeldet und dann ein Dokument in eine eingeschränkte Zone hochlädt. In diesem Fall verwendet das Konto Active Directory Verbunddienste (ADFS) für die SAML-Anmeldung. Authentifizierungsverkehr wird von einem ADFS-Proxyserver verarbeitet, der mit einem ADFS-Server im vertrauenswürdigen Netzwerk kommuniziert.

Schritt	Quelle	Ziel	Protokoll
1. ShareFile Client oder Browser öffnet Verbindung	Client	`company.sharefile.com` oder `company.sharefile.eu`	HTTPS
2. (Optional) Umleiten zur SAML-IdP-Anmeldung	Client	SAML-Identitätsanbieter-URL	HTTPS
3. ShareFile leitet den Benutzer an den StorageZones Controller weiter	Client	`company.sharefile.com` oder `company.sharefile.eu`	HTTPS
4. Client sendet Windows-Anmeldeinformationen an den StorageZones Controller	Client	StorageZones Controller	HTTPS
5. Storage Zones Controller überprüft Anmeldeinformationen und gewährt Clientzugriff	StorageZones Controller	Domänencontroller	Kerberos
6. Client lädt eine Datei auf den StorageZones Controller hoch	Client	StorageZones Controller	HTTPS
7. Datei wird in das Speicher-Repository für die eingeschränkte Zone geschrieben	StorageZones Controller	Lokaler Speicher	CIFS

Schritt	Quelle	Ziel	Protokoll
8. StorageZones Controller verschlüsselt Dateimetadaten und sendet sie an ShareFile	StorageZones Controller	`company.sharefile.com` oder `company.sharefile.eu`	HTTPS

Für eingeschränkte Speicherzonen:

- Verwenden Sie einen internen oder externen Hostnamen.
- Aktivieren Sie SSL für die Kommunikation mit ShareFile.

  Wenn Sie einen internen Hostnamen verwenden, können Sie ein privates Zertifikat verwenden. Das Zertifikat muss von Benutzergeräten als vertrauenswürdig eingestuft werden.

  Wenn Sie einen externen Hostnamen verwenden, muss das SSL-Zertifikat auf dem StorageZones Controller von Benutzergeräten und ShareFile e-Webservern vertrauenswürdig sein.
- Bereitstellen des ausgehenden HTTP-Zugriffs vom StorageZones Controller auf eine der folgenden Service-Bus-URIs:
  - ShareFile.com-Konten: `sf-zk-email-use.servicebus.windows.net`
  - ShareFile.eu Konten: `sf-zk-email-euw.servicebus.windows.net`

  Stellen Sie sicher, dass Sie Netzwerkabhängigkeiten mit Ihrem Netzwerkteam arrangieren.

Client-Anforderungen für eingeschränkte Speicherzonen

Die ShareFile Webanwendung unterstützt eingeschränkte Speicherzonen von den folgenden Webbrowsern:

- Internet Explorer 11

  So aktivieren Sie den Zugriff von der ShareFile Webanwendung auf Ordner und Connectors in eingeschränkten Zonen:

  1. Öffnen Sie Internet Explorer, gehen Sie zu Internetoptionen, klicken Sie auf die Registerkarte **Sicherheit**, und klicken Sie dann auf **Vertrauenswürdige Sites**.
  2. Klicken Sie auf **Sites**, und fügen Sie dann Ihre Subdomain und die externe StorageZones Controller Adresse hinzu.
  3. Klicken Sie auf **Schließen** und dann auf **Benutzerdefinierte Ebene**.

4. Wählen Sie unter **Sonstiges > Domänen auf Datenquellen zugreifen** die Option **Aktivieren**aus.
5. Wählen Sie unter **Benutzerauthentifizierung > Anmelden**die Option Eingeben von Benutzernamen und Kennwort **auffordern** aus.

- Chrome
- Firefox
- Safari
- Secure Web

Um eingeschränkte Speicherzonen zu unterstützen, müssen ShareFile Clients auf die folgenden Versionen oder höher aktualisiert werden:

- ShareFile Sync für Windows 3.1
- ShareFile Outlook Plug-in 3.2.2
- ShareFile für iOS 3.3
- ShareFile für Android 3.4
- ShareFile für Windows Phone 2.3.10

Diese ShareFile Clients und -Tools werden für die Verwendung mit eingeschränkten Speicherzonen ab dem Veröffentlichungsdatum dieses Artikels nicht unterstützt:

Hinweis: Aktuelle Informationen zu ShareFile Clientfunktionen finden Sie auf der ShareFile Unterstützung Website, oder wenden Sie sich an Ihren ShareFile-Supportmitarbeiter.

- Verwendung von ShareFile Desktop Sync für Windows 3.1 und ShareFile Outlook Plug-in außerhalb der Domäne

  Die Clients müssen sich auf einem Windows-Desktop befinden, der sich in derselben Active Directory Gesamtstruktur wie der StorageZones Controller-Server befindet. Clients können NTLM oder Kerberos für die automatische Authentifizierung in einer eingeschränkten Zone verwenden.

- On-Demand Sync für Windows
- Sync für Mac
- ShareFile Enterprise Sync Manager
- Secure Mail für iOS
- ShareFile Desktop Widget
- ShareFile für BlackBerry
- ShareFile e-Website

Die folgenden alternativen Kontozugriffsmethoden werden für die Verwendung mit eingeschränkten Speicherzonen nicht unterstützt:

- FTP
- PowerShell
- ShareFile Befehlszeilenschnittstelle (SFCLI)
- HTTPS API (V1)
- WebDAV
- SMTP

> **Wichtig**
>
> ShareFile unterstützt nicht offiziell und empfiehlt die Verwendung der **DFS-Replikation**nicht. Es ist bekannt, dass es Sperrfehler für größere Dateien verursacht. Wenn die DFS-Replikation verwendet werden muss, verwenden Sie separate Backuplösungen außerhalb der Spitzenzeiten, wenn die Zone nicht aktiv verwendet wird.

Eingeschränkte Speicherzone aktualisieren

Wenn Sie einen StorageZones Controller auf die neueste Version aktualisieren, verwendet dieser Controller weiterhin Standardzonen. Sie können eine Standardzone nicht auf eine eingeschränkte Zone aktualisieren.

Um eine Standardzone durch eine eingeschränkte Zone zu ersetzen, müssen Sie einen neuen StorageZones Controller installieren und eine eingeschränkte Zone konfigurieren.

Um eingeschränkte Zonen oder Webzugriff auf Connectors zu unterstützen, müssen Sie nach Abschluss des Assistenten eine zusätzliche Citrix ADC Konfiguration durchführen. Die Konfiguration stellt sicher, dass ShareFile Clients Anmeldeinformationen nur senden, wenn sie an einer vertrauenswürdigen ShareFile-Domäne angemeldet sind. Um den Webzugriff auf Connectors zu unterstützen, fügen Sie auch einen Pfad (/ProxyService) zur Inhaltswechselrichtlinie hinzu, die für den Datenverkehr zu /cifs und /sp. verwendet wird.

Zusätzliche Informationen zu eingeschränkten Zonen

Die Unterstützung für eingeschränkte Speicherzonen wirkt sich auf alle Aspekte des ShareFile Dienstes aus. Aufgrund von Protokolländerungen, die zur Unterstützung der Metadatenverschlüsselung und der Zonenauthentifizierung erforderlich **sind, werden einige ShareFile Clients und -Features beim Arbeiten mit Dokumenten in einer eingeschränkten Speicherzone nicht unterstützt.**

Inhalt

- Kunden und Tools
- Browser
- Funktionen
- Sync für Windows

- Mobile Apps
- Outlook-Plug-In

Kunden und Tools

Sync für Windows	3.1 und höher
Plug-in für Microsoft Outlook	3.2.2 und höher
On-Demand Sync für Windows	Nicht unterstützt
Drive Mapper	3.01.171.0 und höher
ShareFile für iOS	3.3 — Nur MDX
ShareFile für Android	3.4 und höher
ShareFile für Windows Phone 8	2.3.10 und höher
Sync für Mac	Nicht unterstützt
ShareFile Desktop	Nicht unterstützt
XenMobile WorxMail für iOS	Nicht unterstützt
XenMobile WorxMail für Android	Unterstützt
Nach ShareFile drucken	Nicht unterstützt
Mobile Webseite	Nicht unterstützt
Andere Kontozugriffsmethoden	
PowerShell	Nicht unterstützt
SFCLI	Nicht unterstützt
REST-API (V3)	Unterstützt
HTTPS APT (V1)	Nicht unterstützt
RSZ-Testabdeckung	Nicht unterstützt
FTP	Nicht unterstützt
Dateien per E-Mail an einen Ordner senden	Nicht unterstützt
.NET SDK	Unterstützt

Browser

Windows	Internet Explorer 11, Firefox (neueste Version), Chrome (neueste Version)
macOS	Safari (neueste Version), Firefox (neueste Version), Chrome (neueste Version)
iOS	Safari, Secure Web
Android	Secure Web

Funktionen

Endbenutzer-Aktionen: Arbeiten mit Dateien:

Dateien durchsuchen und herunterladen	Unterstützt
Dateien hochladen (Uploader-Typ)	HTML5: Unterstützt; Flash: Nicht unterstützt; Java: Nicht unterstützt; Standard-HTML-Formular: Nicht unterstützt
Papierkorb	Unterstützt
Bulk-Download und -löschen	Unterstützt
Dateispeicher	Ansicht: Unterstützt; Löschen: Unterstützt; Hochladen: Unterstützt; Download: Nicht unterstützt; Von Filebox senden: Nicht unterstützt
Dateivorschau (Miniaturansichten)	Nicht unterstützt
Anzeigen von Dokumenten im Webbrowser	Nicht unterstützt
Datei erneut hochladen	Nicht unterstützt
Mehrere Versionen pro Datei	Nicht unterstützt
Suchen	Eingeschränkte Zonenelemente sind nicht in den Suchergebnissen enthalten
Markieren eines Ordners als Favorit	Nicht unterstützt
Kopieren oder Verschieben von Dateien	Nicht unterstützt
Ordneroptionen bearbeiten: Ablaufdatum des Ordners, Dateiaufbewahrungsrichtlinie	Unterstützt

Freigegebener Ordner Bubbling	Nicht unterstützt

Endbenutzer-Aktionen: Freigabe und Zusammenarbeit:

Senden Sie eine Datei: Upload erforderlich, senden Sie eine E-Mail mit ShareFile, geben Sie mir einen Link, den ich kopieren kann, fordern Sie den Benutzer, um sich anzumelden, begrenzen Sie die Anzahl der Downloads	Unterstützt
Empfangen und Herunterladen einer freigegebenen Datei	Unterstützt
Erstellen eines freigegebenen Ordners in einer eingeschränkten Speicherzone	Unterstützt
Hinzufügen von Benutzern zu einem Ordner: Steuern von Berechtigungen zum Hochladen und Herunterladen	Unterstützt
Fordern Sie eine Datei an	Unterstützt
Fordern Sie eine Datei an, bei der “ShareFile Anmeldung erforderlich” aktiviert ist	Nicht unterstützt
E-Mail-Benachrichtigungen	Unterstützt
Posteingang: An mich gesendete Dateien	Unterstützt
Posteingang: Gesendete Nachrichten	Anzeigen, ablaufen, erneut senden, bearbeiten: unterstützt
Aktivitätsprotokoll anzeigen	Unterstützt
Signatur abrufen (über RightSignature)	Nicht unterstützt

Verwaltungsmaßnahmen:

Erstellen eines Benutzers in einer eingeschränkten Zone	Unterstützt

Migrieren von Benutzern in eine andere Zone	Nicht unterstützt
Berichterstellung: Zugriffsprüfung, Nutzungsbericht, Messaging-Bericht, Bandbreitenbericht, Speicherbericht	HTML-Viewer: unterstützt; Excel/CSV/PDF-Viewer: verschlüsselte Metadaten werden angezeigt
Zonen-Verwaltung	
Überwachen der Speicherauslastung	Unterstützt
Überwachen der Bandbreitennutzung	Unterstützt
Überwachen der Dateiaktivität	Unterstützt
Wiederherstellen von Dateien	Nicht unterstützt
Abgleichen von Dateien	Nicht unterstützt
Zone löschen	Unterstützt
Hohe Verfügbarkeit	Unterstützt

Sync für Windows

Mindestversion - 3.1

Authentifizieren von einem Client, der in der Domäne beigetreten ist - NTLM oder Kerberos	Unterstützt
Authentifizieren von einem Nicht-Domänen-Client - Benutzer zur Eingabe eines Kennworts aufgefordert	Unterstützt
Synchronisieren von “Eigene Dateien und Ordner” in einer eingeschränkten Zone	Unterstützt
Synchronisieren von freigegebenen Ordnern aus einer eingeschränkten Zone	Unterstützt
Hochladen, herunterladen, synchronisieren	Unterstützt
On-Demand-Synchronisierung für XenApp - und XenDesktop Umgebungen	Nicht unterstützt
Favoritenordner anzeigen	Nicht verfügbar für Ordner mit eingeschränkten Speicherzonen

Klicken Sie mit der rechten Maustaste > Link kopieren	Unterstützt
Klicken Sie mit der rechten Maustaste > E-Mail Datei	Unterstützt

Mobile Apps

Siehe die App-spezifischen Tabellen unten:

iOS - Mindestversion 3.3

Dateien durchsuchen und herunterladen	Unterstützt
Inhalt offline anzeigen	Unterstützt
Ordner erstellen	Unterstützt
Erstellen oder Bearbeiten einer Datei	Unterstützt
Foto oder Video hochladen	Unterstützt
Authentifizieren mit Benutzername/Kennwort	Unterstützt
Single Sign-On mit Worx micro VPN	Unterstützt
Teilen: Kopieren Sie einen Link	Unterstützt
Teilen: Per E-Mail teilen	Nicht unterstützt
Hinzufügen oder Bearbeiten von Ordnernotizen	Nicht unterstützt
Erstellen einer Notiz oder Bearbeiten vorhandener Notizen	Nicht unterstützt
Hinzufügen von Personen zum Ordner oder Bearbeiten vorhandener Ordnerberechtigungen	Nicht unterstützt
Markieren/Aufheben der Markierung eines Ordners als Favorit	Nicht unterstützt
Fordern Sie eine Datei an	Nicht unterstützt
Vorschaubilder für Miniaturansichten	Nicht unterstützt

Löschen mehrerer Elemente	Nicht unterstützt
Ordner offline verfügbar machen	Unterstützt mit Ausnahme von Ordnern auf Stammebene “Für mich freigegeben”
Freigeben eines Ordners	Unterstützt mit Ausnahme von Ordnern auf Stammebene “Für mich freigegeben”
Erstellen eines Connectors in einer eingeschränkten Speicherzone	Nicht unterstützt

Android - Mindestversion 3.4

Dateien durchsuchen und herunterladen	Unterstützt
Inhalt offline anzeigen	Unterstützt
Senden einer Datei	Unterstützt
Ordner erstellen	Unterstützt
Erstellen oder Bearbeiten einer Datei	Unterstützt
Dateien hochladen	Unterstützt
Authentifizieren mit Benutzername/Kennwort	Unterstützt
Single Sign-On mit Worx micro VPN	Unterstützt
Fordern Sie eine Datei an	Nicht unterstützt
Notiz erstellen	Nicht unterstützt
Vorhandene Datei nach dem Hochladen überschreiben	Nicht unterstützt

Outlook-Plug-In

Authentifizieren von einem Client, der in der Domäne beigetreten ist - NTLM oder Kerberos	Unterstützt

Authentifizieren von einem Nicht-Domänen-Client - Benutzer zur Eingabe eines Kennworts aufgefordert	Unterstützt
Durchsuchen und Auswählen von Dateien aus ShareFile	Unterstützt
Durchsuchen und Auswählen von Dateien aus ShareFile mit aktivierter Option “Empfänger müssen sich anmelden”	Nicht unterstützt
Anhang in ShareFile Verknüpfung konvertieren	Unterstützt
Anhang in ShareFile Link mit aktivierter Option “Empfänger müssen sich anmelden” konvertieren	Nicht unterstützt
Fordern Sie eine Datei an	Unterstützt
Fordern Sie eine Datei an, bei der die Option “Empfänger müssen sich anmelden” aktiviert ist.	Nicht unterstützt

Referenz: Konfigurationsdateien des StorageZones Controller

June 11, 2020

Diese Referenz bietet einen Überblick über die Konfigurationsdateien des Storage Zones Controller:

- AppSettingsRelease.config
- FileDeleteService.exe.config
- SFAntiVirus.exe.config
- Web.config

Das StorageZones Controller Installationsprogramm erstellt diese Dateien. Änderungen, die Sie in der Storage Zones Controller Konsole vornehmen, werden in den Dateien gespeichert.

Um bestimmte Features zu verwenden oder zu konfigurieren, müssen Sie manuell einige Einstellungen in den Konfigurationsdateien hinzufügen oder aktualisieren. Diese Referenz listet diese Einstellungen auf und enthält Links zu verwandten Informationen.

AppSettingsRelease.config

AppSettingsRelease.config-Dateien sind in den folgenden Ordnern im Installationspfad des StorageZones Controller (C:\inetpub\wwwroot\Citrix\) enthalten:

- StorageCenter

  Definiert globale Einstellungen für den StorageZones Controller.

- StorageCenter\cifs

  Definiert Einstellungen für StorageZone Connector für Netzwerkdateifreigaben.

- StorageCenter\sp

  Definiert Einstellungen für StorageZone Connector für SharePoint.

Bevor Sie eine AppSettingsRelease.config-Datei bearbeiten, überprüfen Sie, ob Sie am richtigen Speicherort arbeiten.

FileDeleteService.exe.config

FileDeleteService.exe.config bietet Steuerelemente, die vom StorageZones Controller verwendet werden, um den persistenten Speichercache zu verwalten. 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 des StorageZones Controller, 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 Antivirus-Scans von hochgeladenen Dateien.

Web.config

`C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` Enthält im Allgemeinen Steuerelemente, die normalerweise nicht geändert werden sollten. Sie müssen es jedoch aktualisieren, wenn Sie ältere StorageZones Controller mit einem Proxy-Server verwenden.

Nur für StorageZones Controller 2.2 bis 2.2.2: Wenn eine Zone über mehrere StorageZones Controller verfügt und der gesamte HTTP-Datenverkehr einen Proxy-Server verwendet, müssen Sie Web.config für jeden sekundären Server eine Umgehungsliste hinzufügen.

Hinweis: Ab Version 2.2.3 ist die Bypass-Einstellung auf der Netzwerkseite der Storage Zones Controller-Konsole enthalten.

1. Öffnen Sie die Datei in einem Texteditor, und suchen Sie den <system.net> Abschnitt. Hier ist ein Beispiel für diesen Abschnitt, nachdem ein Proxyserver konfiguriert wurde:

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
    </defaultProxy>
  </system.net>
</configuration>
```

2. Fügen Sie diesem Abschnitt eine Umgehungsliste hinzu, wie hier gezeigt:

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
      <bypasslist>
        <add address="primaryServer" />
      </bypasslist>
    </defaultProxy>
  </system.net>
</configuration>
```

   Der PrimaryServer ist entweder eine IP-Adresse oder ein Hostname (servername.subdomain.com).

   Wenn Sie später die IP-Adresse oder den Hostnamen des primären StorageZones Controller ändern, müssen Sie diese Informationen in ConfigService\ Web.config für jeden sekundären Server aktualisieren.

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

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States