ストレージゾーンコントローラ 5.x

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

Contents

Storage Zones Controller について

May 28, 2024

Storage Zones Controller は、ShareFile アカウントにプライベートデータストレージを提供することにより、サービスとしてのソフトウェア (SaaS) クラウドストレージを拡張します。

コンポーネント、データストレージなどの Storage Zones Controller の詳細については、「Storage Zones Controller 5.x」を参照してください。

これと ShareFile の最新の拡張機能については、「新機能」を参照してください。

ShareFile Storagezone コントローラーの最新バージョンをダウンロードするには、https://dl.sharefile.com/storagezone-controller を参照してください。すべてのアプリケーションのダウンロードにアクセスするには、ShareFile アカウントにサインインしてください。

> ヒント：
>
> ShareFile は、ユーザーが脅威検出アラートを有効にすることを推奨します。

解決された問題

Storage Zones Controller 5.11.25 で解決された問題

このリリースでは、全体的なパフォーマンスと安定性を向上させるいくつかの問題に対処しています。

Storage Zones Controller 5.11.24 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller 5.11.23 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller 5.11.22 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller 5.11.21 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller 5.11.18 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller 5.11.17 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller5.11 で解決された問題

このリリースでは、全体的なパフォーマンスと安定性を向上させる多くの問題に対処しています。

Storage Zones Controller 5.10 で解決された問題

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

Storage Zones Controller5.9 で解決された問題

このリリースには、信頼性とパフォーマンスを向上させるための修正が含まれています。

Storage Zones Controller5.8 で解決された問題

このリリースには、チェックアウトされたファイルのエラーメッセージを改善する修正と、SharePoint で新しく発行された管理パスの修正が含まれています。

Storage Zones Controller5.7 で解決された問題

このリリースには、ストレージゾーンおよびオンプレミスコネクタへのファイルアップロードのリダイレクトの問題に対処するための修正が含まれています。

Storage Zones Controller5.6 で解決された問題

WOPI Fix: Office ファイルを後で編集しようとしたときに発生する問題を解決するための変更が含まれています。

SharePoint コネクタの修正**:** このリリースには、SharePoint Connector に既に存在するフォルダを作成するときに有効なエラーメッセージを表示するための変更が含まれています。

Storage Zones Controller5.5 で解決された問題

このリリースには、信頼性とパフォーマンスを向上させるための修正が含まれています。

Storage Zones Controller 5.4.2 で解決された問題

SharePoint コネクタの修正**:** SharePoint コネクタに存在するファイルを移動すると、特定のシナリオで失敗することがあります。このリリースでは、SharePoint コネクタ上に存在するファイルの移動が期待どおりに動作することが保証されます。

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

Storage Zones Controller 5.4.1 で解決された問題

セキュリティ修正**:** このリリースには、セキュリティと信頼性に関する修正が含まれています。

追加のサポート**:** ワークスペース環境のクラウド**/cloudburrito** アカウントのサポートが追加されました。

Storage Zones Controller 5.3.1 で解決された問題

このリリースには、信頼性とパフォーマンスを向上させるための修正が含まれています。

Storage Zones Controller 5.3.1 で解決された問題

WOPI Fix: WOPI アクセストークンは、公開暗号鍵の盗難によって偽装される可能性がありました。このバージョンでは、Storage Zones Controller 間でキーが共有されなくなりました。

セキュリティ修正**:** このリリースには、セキュリティ、パフォーマンス、および信頼性に関する修正が含まれています。

既知の問題

Storage Zones Controller 5.10 の既知の問題

このリリースで確認されている新しい問題はありません。

Storage Zones Controller 5.9 の既知の問題

このリリースで確認されている新しい問題はありません。

Storage Zones Controller 5.8 の既知の問題

このリリースで確認されている新しい問題はありません。

Storage Zones Controller 5.7 の既知の問題

このリリースで確認されている新しい問題はありません。

アーキテクチャの概要

July 25, 2024

このセクションでは、概念実証評価や高可用性実稼働環境のためのストレージゾーン Controller のデプロイの概要を説明します。高可用性展開は、NetScaler ADC などの DMZ プロキシの有無の両方で表示されます。

複数のストレージゾーン Controller を使用するデプロイを評価するには、高可用性デプロイのガイドラインに従ってください。

各展開シナリオには、ShareFile Enterprise アカウントが必要です。デフォルトでは、ShareFile は安全な ShareFile マネージドクラウドにデータを保存します。プライベートデータストレージ (オンプレミスのネットワーク共有またはサポートされているサードパーティ製ストレージシステム) を使用するには、ShareFile Data 用のストレージゾーンを構成します。

ネットワークファイル共有または SharePoint ドキュメントライブラリからユーザーにデータを安全に配信するには、ストレージゾーンコネクタを構成します。

Storage Zone Controller の概念実証導入

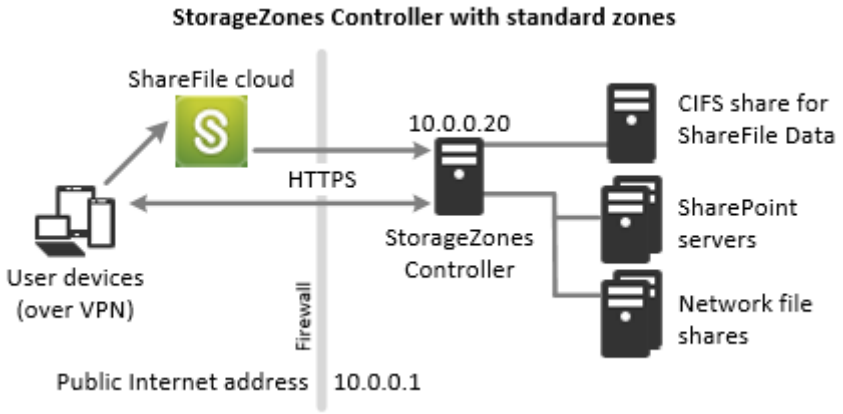
> 注意：
>
> 概念実証の導入は評価目的のみを目的としており、重要なデータストレージには使用しないでください。

概念実証デプロイメントでは、単一の Storage Zone Controller を使用します。このセクションで説明した展開例では、ShareFile Data のストレージゾーンとストレージゾーンコネクタの両方が有効になっています。

単一の Storage Zone Controller を評価するには、オプションで、別のネットワーク共有ではなく、Storage Zone Controller のハードドライブ上のフォルダー (C:\ZoneFiles など) にデータを保存できます。他のすべてのシステム要件は、評価展開に適用されます。

標準ストレージゾーンの概念実証導入

標準ゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからのインバウンド接続を受け入れる必要があります。そのためには、コントローラがパブリックにアクセス可能なインターネットアドレスと、ShareFile クラウドとの通信用に SSL を有効にする必要があります。次の図は、ユーザーデバイス、ShareFile クラウド、および Storage Zone Controller 間のトラフィックフローを示しています。



このシナリオでは、1 つのファイアウォールがインターネットとセキュリティで保護されたネットワークの間に立っています。Storage Zone Controller は、アクセスを制御するためにファイアウォールの内側に常駐します。ShareFile へのユーザー接続は、ファイアウォールを通過し、ポート 443 の SSL プロトコルを使用してこの接続を確立する必要があります。この接続をサポートするには、ファイアウォールでポート 443 を開き、Storage Zone Controller の IIS サービスにパブリック SSL 証明書をインストールする必要があります。

Storage Zone Controller の高可用性デプロイ

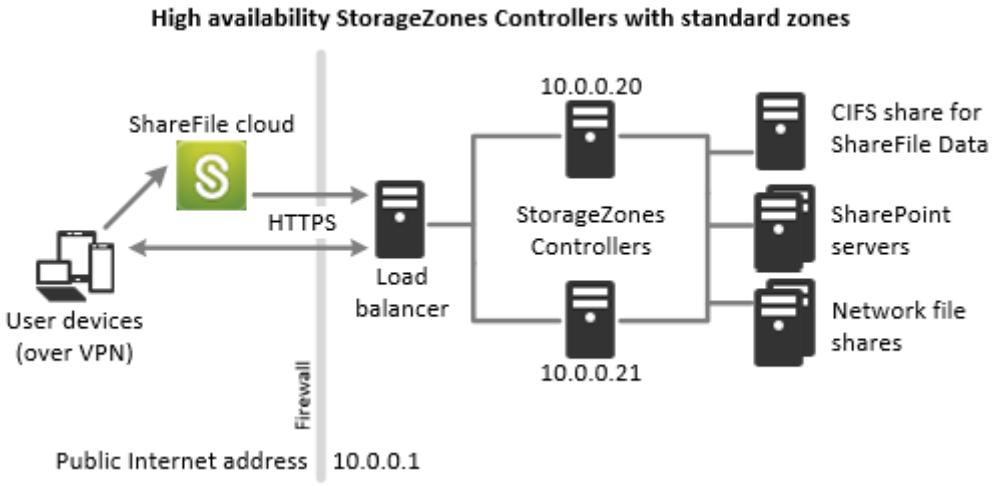
可用性の高い ShareFile を本番環境に導入する場合、推奨されるベストプラクティスは、少なくとも 2 つのストレージゾーン Controller をインストールすることです。最初のコントローラをインストールすると、ストレージゾーンが作成されます。他のコントローラをインストールすると、それらは同じゾーンに参加します。同じゾーンに属する Storage Zone Controller は、同じファイル共有をストレージに使用する必要があります。

高可用性展開では、セカンダリサーバーは独立しており、完全に機能する Storage Zone Controller です。ストレージゾーン制御サブシステムは、操作用の Storage Zone Controller をランダムに選択します。プライマリサーバがオフラインになった場合は、セカンダリサーバをプライマリサーバに簡単に昇格できます。また、サーバをプライマリからセカンダリに降格することもできます。

標準ゾーンの高可用性の導入

標準ストレージゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからのインバウンド接続を受け入れる必要があります。そのためには、各コントローラーがパブリックにアクセス可能なインターネットアドレスと、ShareFile クラウドとの通信用に SSL を有効にする必要があります。複数の外部パブリックアドレスを構成

でき、それぞれが異なるストレージゾーン Controller に関連付けられます。次の図は、標準ストレージゾーンの高可用性展開を示しています。



上記の概念実証の展開シナリオと同様に、1 つのファイアウォールがインターネットとセキュリティで保護されたネットワークの間にあります。Storage Zone Controller はファイアウォールの内側に配置され、アクセスを制御します。ShareFile へのユーザー接続は、ファイアウォールを通過し、ポート 443 の SSL プロトコルを使用してこの接続を確立する必要があります。この接続をサポートするには、ファイアウォールでポート 443 を開き、すべての Storage Zone Controller の IIS サービスにパブリック SSL 証明書をインストールする必要があります。

共有ストレージ構成

同じストレージゾーンに属する Storage Zone Controller は、同じファイル共有をストレージに使用する必要があります。Storage Zone Controller は IIS アカウントプールユーザーを使用して共有にアクセスします。既定では、アプリケーションプールは、低レベルのユーザー権限を持つ Network Service ユーザーアカウントで動作します。Storage Zone Controller は、デフォルトでネットワークサービスアカウントを使用します。

ネットワークサービスアカウントの代わりに名前付きユーザーアカウントを使用して、共有にアクセスできます。名前付きユーザーアカウントを使用するには、ストレージゾーンコンソールの [構成] ページでユーザー名とパスワードを指定します。ネットワークサービスアカウントを使用して IIS アプリケーションプールと ShareFile サービスを実行します。

ネットワーク接続

ネットワーク接続は、ゾーンのタイプ（ShareFile マネージドまたはスタンダード）によって異なります。

ShareFile マネージドゾーン　次の表では、ユーザーが ShareFile にログオンし、ShareFile 管理ゾーンからドキュメントをダウンロードするときに発生するネットワーク接続について説明します。すべての接続は HTTPS を使用します。

手順	接続元	接続先
1. ユーザーログオン要求	クライアント	company.sharefile.com:443
2. (オプション) SAML IdP ログオンへのリダイレクト	クライアント	SAML ID プロバイダー URL
3. ファイル/フォルダーの列挙とダウンロード要求	クライアント	company.sharefile.com:443
4. ファイルダウンロード	クライアント	storage-location.sharefile.com:443

標準ストレージゾーン　次の表に、ユーザーが ShareFile にログオンし、標準記憶域ゾーンからドキュメントをダウンロードするときに発生するネットワーク接続を示します。すべての接続は HTTPS を使用します。

手順	接続元	接続先
1. ユーザーログオン要求	クライアント	company.sharefile.com
2. (オプション) ADFS を使用している場合は、SAML IdP ログオンにリダイレクトします	クライアント	SAML ID プロバイダー URL
3. ファイル/フォルダーの列挙とダウンロード要求	クライアント	company.sharefile.com
4. ファイルダウンロード認証	company.sharefile.com	szc.company.com
5. ファイルダウンロード	クライアント	szc.company.com

Storage Zone Controller DMZ プロキシデプロイ

非武装地帯（DMZ）は、内部ネットワークのセキュリティを強化します。NetScaler ADC VPX などの DMZ プロキシは、次の目的で使用されるオプションのコンポーネントです。

- Storage Zone Controller へのすべてのリクエストが ShareFile クラウドから送信され、承認されたトラフィックのみが Storage Zone Controller に到達するようにします。

  ストレージゾーン Controller には、すべての受信メッセージの有効な URI 署名をチェックする検証操作があります。DMZ コンポーネントは、メッセージを転送する前に署名を検証します。

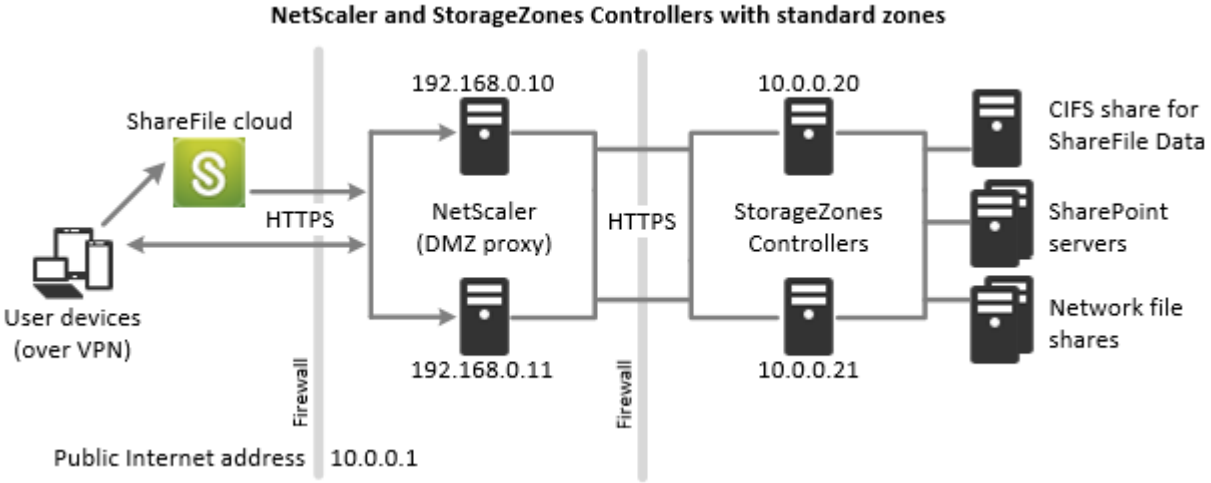
- リアルタイムのステータスインジケーターを使用して、Storage Zone Controller へのリクエストを負荷分散します。

すべての Storage Zone Controller が同じファイルにアクセスできる場合、操作を Storage Zone Controller に負荷分散できます。

- Storage Zone Controller から SSL をオフロードします。
- DMZ を通過する前に、SharePoint またはネットワーク・ドライブ上のファイルに対する要求が認証されていることを確認します。

Citrix ADC と **Storage Zone Controller** の導入

標準ストレージゾーンの導入　標準ゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからのインバウンド接続を受け入れる必要があります。そのためには、NetScaler ADC で公開可能なインターネットアドレスと、ShareFile クラウドとの通信用に SSL を有効にする必要があります。



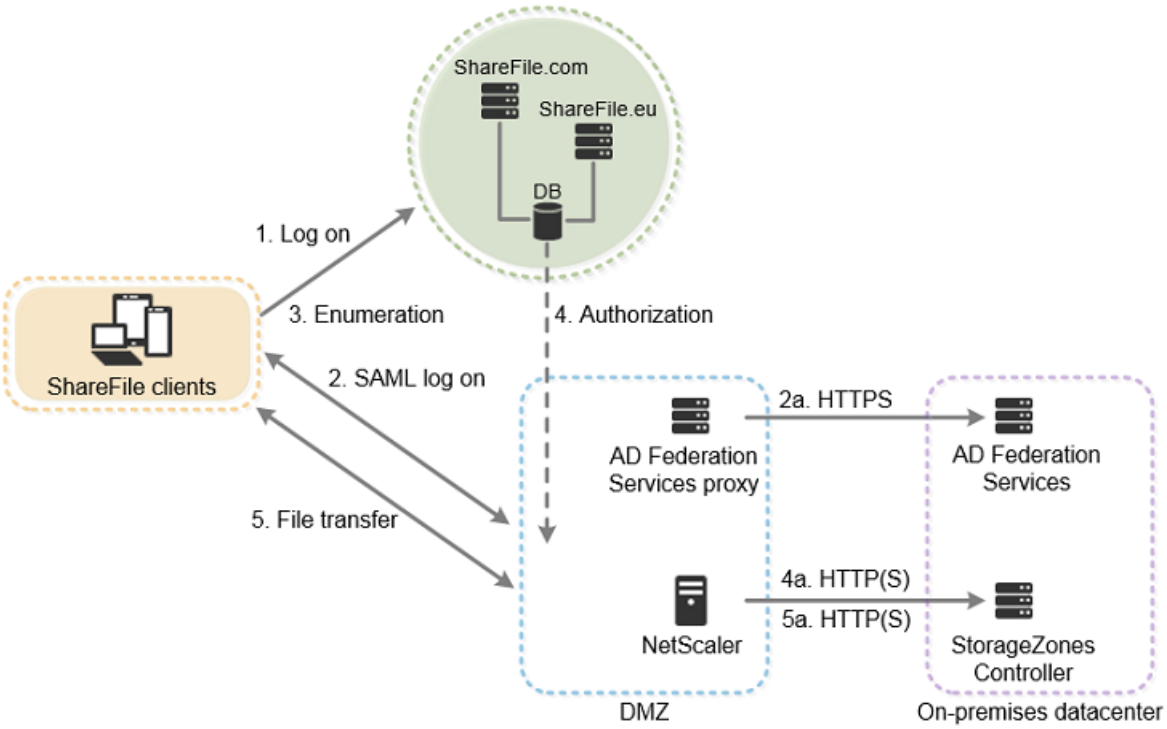
このシナリオでは、インターネットとセキュリティで保護されたネットワークの間に 2 つのファイアウォールがあります。Storage Zone Controller は内部ネットワークにあります。ShareFile へのユーザー接続は、最初のファイアウォールを通過し、ポート 443 の SSL プロトコルを使用してこの接続を確立する必要があります。この接続をサポートするには、ファイアウォールのポート 443 を開き、DMZ プロキシサーバーの IIS サービスに (ユーザーがユーザー接続を終了する場合) パブリック SSL 証明書をインストールする必要があります。

標準ゾーンのネットワーク接続

次の図と表は、ユーザーが ShareFile にログオンし、NetScaler ADC 背後に展開された標準ゾーンからドキュメントをダウンロードしたときに発生するネットワーク接続を示しています。この場合、アカウントは SAML ログオンに Active Directory フェデレーションサービス (ADFS) を使用します。

認証トラフィックは、信頼されたネットワーク上の ADFS サーバーと通信する ADFS プロキシサーバーによって DMZ 内で処理されます。ファイルアクティビティには、DMZ の Citrix ADC を介してアクセスします。Citrix ADC は、SSL を終了し、ユーザー要求を認証してから、認証されたユーザーに代わって信頼できるネットワーク内の

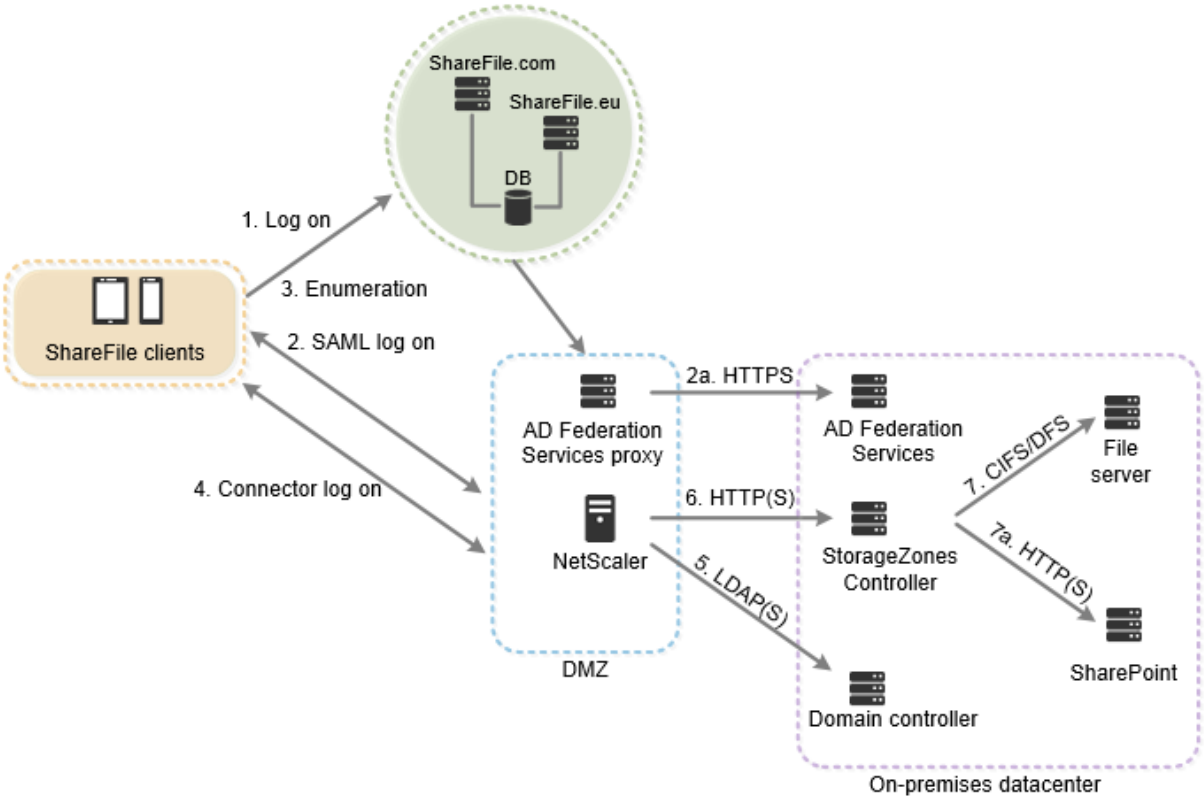
Storage Zone Controller にアクセスします。ShareFile の NetScaler ADC 外部アドレスは、インターネット FQDN szc.company.company.com を使用してアクセスします。



手順	接続元	接続先	プロトコル
1. ユーザーログオン要求	クライアント	company.sharefile.com	HTTPS
2. (オプション) SAML IdP ログオンへのリダイレクト	クライアント	SAML ID プロバイダー URL	HTTPS
2a. ADFS ログオン	ADFS プロキシ	ADFS サーバ	HTTPS
3. ファイル/フォルダーの列挙とダウンロード要求	クライアント	company.sharefile.com	HTTPS
4. ファイルダウンロード認証	ShareFile	szc.company.com (外部アドレス)	HTTP (S)
4a. ファイルダウンロード認証	NetScaler ADC IP (NSIP)	Storage Zone Controller	HTTPS
5. ファイルダウンロード	クライアント	szc.company.com (外部アドレス)	HTTPS

手順	接続元	接続先	プロトコル
5a. ファイルダウンロード	NetScaler ADC IP (NSIP)	Storage Zone Controller	HTTP (S)

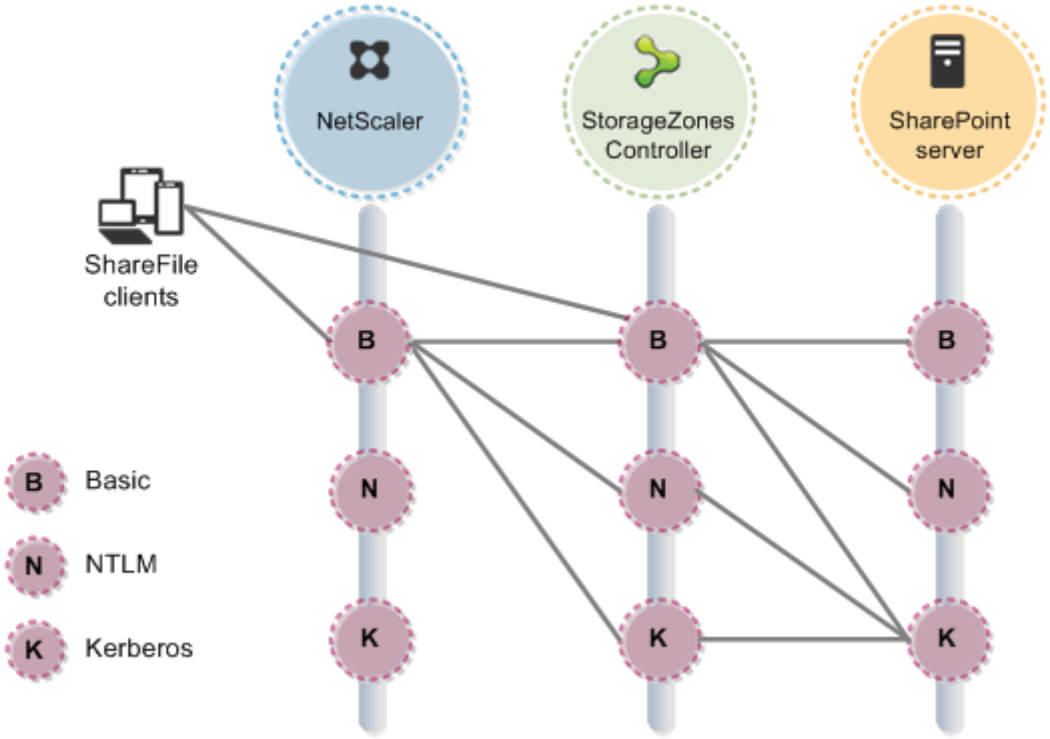
次の図と表は、StorageZone コネクタのネットワーク接続を示すために、前のシナリオを拡張したものです。このシナリオには、DMZ で NetScaler を使用して SSL を終了し、コネクタアクセスのユーザー認証を実行することが含まれます。



手順	接続元	接続先	プロトコル
1. ユーザーログオン要求	クライアント	company.sharefile.com	HTTPS
2. (オプション) SAML IdP ログオンへのリダイレクト	クライアント	SAML ID プロバイダー URL	HTTPS
2a. ADFS ログオン	ADFS プロキシ	ADFS サーバ	HTTPS
3. トップレベルのコネクタ列挙	クライアント	company.sharefile.com	HTTPS

手順	接続元	接続先	プロトコル
4. StorageZone Controller サーバーへのユーザーログオン	クライアント	szc.company.com (外部アドレス)	HTTPS
5. ユーザー認証	NetScaler ADC IP (NSIP)	AD ドメインコントローラー	LDAP
6. ファイル/フォルダーの列挙とアップロード/ダウンロード要求	NetScaler ADC IP (NSIP)	Storage Zone Controller	HTTP (S)
7. ネットワーク共有の列挙とアップロード/ダウンロード	Storage Zone Controller	ファイルサーバ	CIFS または DFS
7a. SharePoint の列挙とアップロード/ダウンロード	Storage Zone Controller	SharePoint	HTTP (S)

次の図は、ユーザーが認証したかどうかに基づいて、サポートされている認証タイプの組み合わせをまとめたものです。



システム要件

November 17, 2023

> 重要:
>
> Microsoft は、2023 年 10 月 10 日をもって Windows Server 2012R2 のサポートを終了します。サポート終了日までにサーバーを新しいバージョンに移行することが重要です。

Storage Zone Controller

- 2 つの CPU と 4 GB RAM を備えた専用の物理マシンまたは仮想マシン
- Windows サーバー 2012 R2 (データセンター、スタンダード、またはエッセンシャル)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

標準ストレージゾーンの場合:

- パブリックに解決可能なインターネットホスト名を使用します (IP アドレスではありません)。
- ShareFile との通信で SSL を有効にします。
  - Storage Zones Controller の SSL 証明書は、ユーザーデバイスと ShareFile Web サーバーから信頼されている必要があります。IIS で SSL を直接使用する場合は、SSL http://support.microsoft.com/kb/298805 の設定に関する情報を参照してください。
- ファイアウォール経由でポート 443 でインバウンド TCP リクエストを許可します。
- ファイアウォールを介したポート 443 の ShareFile コントロールプレーンへのアウトバウンド TCP リクエストを許可します。
  - IP 範囲とドメインの詳細なリストについては、ここをクリックしてください。

ShareFile Data 用のストレージ・ゾーンにのみ使用されるサーバのヘルスチェックの場合:

- ローカルホストでポート 80 を開きます。

高可用性実稼働環境の場合:

- Storage Zones Controller がインストールされたサーバが 2 台以上必要です。
- DMZ プロキシサーバーを使用していない場合は、IIS サービスに SSL 証明書をインストールします。

  サポートされている証明書について詳しくは、上記の標準ゾーンの証明書の要件を参照してください。

DMZ プロキシ配置の場合:

- NetScaler ADC VPX インスタンスなど、1 つ以上の DMZ プロキシサーバー。
- クライアント接続を終了し、HTTP を使用する DMZ プロキシサーバの場合は、プロキシサーバに SSL 証明書をインストールします。

  DMZ プロキシサーバと Storage Zones Controller 間の通信が安全であれば、HTTP を使用できます。ただし、ベストプラクティスとして HTTPS を使用することをお勧めします。HTTPS を使用する場合、DMZ プロキシによって信頼されていれば、Storage Zones Controller のプライベート (エンタープライズ) 証明書を使用できます。DMZ プロキシによって公開される外部アドレスは、商業的に信頼できる証明書を使用する必要があります。サポートされている証明書について詳しくは、上記の標準ゾーンの証明書の要件を参照してください。

そのほかの要件

> 注:
>
> ShareFile は DFS レプリケーションの使用を公式にはサポートしておらず、推奨していません。これは、大きなファイルのロックエラーを引き起こすことが知られています。DFS レプリケーションを使用する必要がある場合は、ゾーンがアクティブに使用されていないオフピーク時に別のバックアップ・ソリューションを使用してください。

- Storage Zones Controller のインストーラーには管理者権限が必要です。
- Storage Zones Controller をリモート管理するには、RDP や Citrix ICA などのリモートプロトコルを使用してサーバーに接続し、Storage Zones Controller コンソールを開きます。

サポート対象のサードパーティ製ストレージシステム

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

サポートされている情報漏えい対策ソリューション

- Storage Zones Controller は、以下を含むあらゆる ICAP 準拠の DLP ソリューションと統合できます。
  - Symantec Data Loss Prevention
  - マカフィー DLP プリベント
  - Websense TRITON AP-DATA
  - RSA 情報漏えい防止

ShareFile データのストレージゾーン

ShareFile Data のストレージゾーンは、Storage Zones Controller で有効にするオプション機能です。

要件:

- ストレージゾーン機能を有効にした ShareFile Enterprise アカウント
- ゾーンを作成および管理するためのアクセス許可を含む ShareFile ユーザーアカウント
- プライベートデータストレージ用の CIFS 共有

サポートされているサードパーティのストレージシステムに ShareFile 保存する場合、CIFS 共有は一時ファイル（暗号化キー、キューに入れられたファイル）および一時ストレージキャッシュとして使用されます。

- Web サーバー (IIS) の役割と ASP.NET 4.x。詳細については、「ShareFile データ用にサーバーを準備する」を参照してください。

注:FTP クライアントから ShareFile アカウントへのアクセスは、ShareFile データのストレージゾーンと互換性がありません。

SharePoint 用のストレージゾーンコネクタ

SharePoint のストレージゾーンコネクタは、Storage Zones Controller で有効にするオプション機能です。

要件:

- ストレージゾーン機能を有効にした ShareFile Enterprise アカウント、または Citrix Endpoint Management を使用します。
- **Microsoft SharePoint Server 2010** 以降のみがサポートされています。
- Storage Zones Controller サーバーは、SharePoint サーバーと同じフォレスト内のドメインメンバーである必要があります。
- Web サーバー (IIS) の役割と ASP.NET 4.x。詳細については、「ShareFile データ用にサーバーを準備する」を参照してください。
- SharePoint ポリシー:
  - SharePoint 2013 の Web アプリケーションの既定のアップロードファイルの最大サイズは 250 MB で、SharePoint 2010 では 50 MB です。既定の設定を変更するには:SharePoint サーバーの全体管理で、[Web アプリケーションの全般設定] ページに移動し、[最大アップロードサイズ] を変更します。SharePoint のアップロードファイルサイズの制限は 2 GB です。
  - ShareFile クライアントは、常にファイルのメジャーバージョン (公開) をチェックイン (発行) しようとします。ただし、SharePoint ポリシーは、ファイルをメジャーバージョンとマイナーバージョンのどちらとしてチェックインするかを決定します。
  - SharePoint 表示専用アクセス許可では、ユーザーがファイルをダウンロードすることはできません。ShareFile クライアントからファイルを読み込むには、SharePoint ユーザーが読み取りアクセス許可を持っている必要があります。
- ユーザーデバイス: ストレージゾーンコネクタのユーザーデバイスサポートに関する最新情報については、ShareFile ナレッジベースを参照してください。

SharePoint 認証用のストレージゾーンコネクタ

ユーザーを認証すると、Storage Zones Controller サーバーは、認証されたユーザーに代わって SharePoint サーバーに接続し、SharePoint サーバーから提示された認証チャレンジに応答します。SharePoint 用のストレージゾーンコネクタは、SharePoint サーバー上で次の認証方法をサポートしています。

- 基本

  `<add key="CacheCredentials"value="1"\>` に追加する必要があります `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

- ネゴシエート (Kerberos)
- Windows チャレンジ/レスポンス (NTLM)

ShareFile モバイルクライアントは、HTTPS 経由の基本認証を使用して Storage Zones Controller または DMZ プロキシを認証します。SharePoint へのシングルサインオンは、SharePoint サーバーで設定された認証要件によって制御されます。SharePoint サーバーで Kerberos または NTLM 認証を使用するには、Storage Zones Controller の委任を信頼するようにドメインコントローラーを構成します。

SharePoint サーバーが Kerberos 認証用に構成されている場合:SharePoint サーバーアプリケーションプールの名前付きユーザーサービスアカウントのサービスプリンシパル名 (SPN) を構成します。詳細については、の「Web パーツの委任に対する信頼の設定」を参照してください。http://support.microsoft.com/kb/832769

NetScaler ADC を使用する展開環境では、NetScaler ADC で基本認証を終了してから、Storage Zones Controller に対して他の種類の認証を実行できます。

ネットワークファイル共有用のストレージゾーンコネクタ

ネットワークファイル共有用のストレージゾーンコネクタは、Storage Zones Controller で有効にするオプション機能です。

要件:

- ShareFile Enterprise アカウントまたは Citrix Endpoint Management アカウント。
- ストレージゾーンコネクタサーバーは、ネットワークファイルサーバーと同じフォレスト内のドメインメンバーである必要があります。
- Web サーバー (IIS) の役割と ASP.NET 4.x。詳細については、「ShareFile データ用にサーバーを準備する」を参照してください。
- ユーザーデバイス: ストレージゾーンコネクタのユーザーデバイスサポートに関する最新情報については、ShareFile ナレッジベースを参照してください。

ネットワークファイル共有認証用コネクタ

ユーザーを認証すると、Storage Zones Controller サーバーは、認証されたユーザーに代わってネットワークファイルサーバーに接続し、ファイルサーバーから提示された認証チャレンジに応答します。ネットワークファイル共有のストレージゾーンコネクタは、ファイルサーバー上で次の認証方法をサポートします。

- ネゴシエート (Kerberos)
- Windows チャレンジ/レスポンス (NTLM)

Storage Zones Controller で Kerberos または NTLM 認証を使用するには: Storage Zones Controller の委任を信頼するようにドメインコントローラーを構成します。

NetScaler ADC を使用した展開の場合: NetScaler ADC が基本認証用に構成されているときにユーザーにシングルサインオンエクスペリエンスを提供するには、ネゴシエート（Kerberos）認証と NTLM 認証の両方に対してコネクタを構成します。

PowerShell スクリプトとコマンド

Storage Zones Controller のインストールには、にいくつかの PowerShell スクリプトとコマンドが含まれています。`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`

- スクリプトは、32 ビット（x86）バージョンの PowerShell で実行します。
- 最良の結果を得るには、Windows Management Frameworkに含まれている PowerShell 4.0 以降にアップグレードしてください。

  PowerShell 2.0 は、.NET Framework 4 との互換性の問題により、重大な問題を引き起こします。

インストール

April 27, 2021

Storage Zone Controller と ShareFile Data のストレージゾーンのインストールとセットアップを行うには、次の作業を記載順に実行します。

1. Storage Zone Controller 用に Citrix ADC を構成する

   Citrix ADC を Storage Zone Controller の DMZ プロキシとして使用できます。

2. プライベートデータストレージ用のネットワーク共有を作成する

   ShareFile Data のストレージゾーンでは、サポートされているサードパーティストレージシステムに ShareFile ファイルを格納する場合でも、プライベートデータのネットワーク共有が必要です。

3. SSL 証明書のインストール

   Storage Zone Controller で標準ゾーンをホストする場合、SSL 証明書が必要になります。

4. ShareFile データ用にサーバーを準備する

   IIS と ASP.NET のセットアップは、ShareFile データおよび記憶域ゾーンコネクタ用の記憶域ゾーンに対して必要です。

5. Storage Zone Controller をインストールし、ストレージゾーンを作成する
6. Storage Zone Controller のセットアップを確認する
7. ユーザーアカウントのデフォルトゾーンを変更する

   デフォルトでは、既存のユーザーアカウントと新しくプロビジョニングされたユーザーアカウントは、ShareFile 管理のクラウドストレージをデフォルトゾーンとして使用します。

8. ストレージゾーンのプロキシサーバーを指定する

   Storage Zone Controller コンソールでは、Storage Zone Controller のプロキシサーバーを指定できます。プロキシサーバーは他の方法で指定することもできます。

9. 委任のために Storage Zone Controller を信頼するようにドメインコントローラーを構成する

   ネットワーク共有上または SharePoint サイト上の NTLM か Kerberos 認証をサポートするようにドメインコントローラーを構成します。

10. ストレージゾーンにセカンダリ Storage Zone Controller を統合する

    ストレージゾーンを高可用性に構成するには、2 つ以上の Storage Zone Controller を接続します。

Microsoft Azure ストレージを使用して Storage Zone Controller を構成するデモについては、次を参照してください：ここをクリックしてください。

Microsoft Azure ストレージゾーンを使用するように ShareFile Enterprise を構成する方法のデモンストレーションについては、ここをクリックしてください。

追加のセットアップ手順

- マルチテナントストレージゾーンの構成
- Web App プレビュー、サムネイル、および表示専用共有用の Storage Zone Controller を構成する

ストレージゾーンコントローラー用の **Citrix ADC** の構成

February 14, 2022

NetScaler、バージョン 10.1 ビルド 120.1316.e 以降には、ストレージゾーンコントローラー環境に関する基本情報の入力を求めるウィザードが含まれています。次に、次のような構成を生成します。

- ストレージゾーンコントローラー 間でトラフィックの負荷を分散します
- ストレージゾーンコネクタのユーザー認証を提供
- ShareFile アップロードとダウンロードの URI 署名を検証します。
- Citrix ADC アプライアンスでの SSL 接続を終了します

この図は、構成によって作成される次の Citrix ADC コンポーネントを示しています。

- **Citrix ADC** コンテンツスイッチング仮想サーバー— ShareFile およびストレージゾーンコネクタからのデータに対するユーザー要求を、適切な Citrix ADC 負荷分散仮想サーバーに送信します。
- **Citrix ADC** 負荷分散仮想サーバー**-** ストレージゾーンコントローラーのトラフィックを負荷分散し、次の処理も行います。
  - プライベートデータストレージからのデータの要求については、負荷分散仮想サーバーがハッシュ検証を実行し、着信要求に有効な URI シグネチャが存在することを確認します。
  - ストレージゾーンコネクタからのデータの要求に対して、負荷分散仮想サーバーはユーザー認証を実行できます。これは、Citrix ADC でユーザー要求を停止し、ユーザーを認証し、ストレージゾーンコントローラー にユーザーのシングルサインオンを実行します。

> 注:
>
> Citrix ADC を介したストレージゾーンコネクタへの認証はオプションです。既知の問題により、Citrix ADC で認証が有効になっている場合、WebApp のストレージゾーンコネクタは Chrome、Chromium、Safari、Edge ブラウザーでは機能しません。他のブラウザーやデスクトップ/モバイルクライアントと互換性があります。

ストレージゾーンコントローラー 4.0 以降、管理者はストレージゾーンコントローラーへの受信接続を TLS v1.2 に制限できます。TLS v1.2 より前のプロトコルがストレージゾーンコントローラーへのインバウンドトラフィックに対して無効になっている場合、ストレージゾーンと対話するすべてのクライアントソフトウェアコンポーネントも TLS v1.2 をサポートしている必要があります。詳細および構成手順については、ここをクリックしてください。

> 注:
>
> 10.1 ビルド 120.1316.e より前の NetScaler バージョンをセットアップするには、「Citrix ADC を手動で構成する」を参照してください。

Citrix ADC for ShareFile ウィザードのセットアップでは、Citrix Endpoint Management を ShareFile の SAML ID プロバイダーとして使用するために必要な構成は処理されません。詳しくは、ここをクリックしてください。

前提条件

- 動作中の Citrix ADC 構成

- セキュリティ証明書：Citrix ADC でセキュリティ証明書がまだ利用できない場合は、ウィザードでコンテンツスイッチング仮想サーバーにインストールできます。
- Active Directory 構成に関する情報（**ShareFile** 用 **Citrix ADC** ウィザードは、**Citrix NetScaler** エンタープライズエディションのライセンスを使用して完了する必要があります）
  - Active Directory サーバーの IP アドレスとポート
  - Active Directory ドメイン名
  - ユーザーが格納される LDAP ベース DN
  - Active Directory と通信するためのアクセス許可を持つ管理者アカウントのアカウント名とパスワード

Citrix ADC をストレージゾーンコントローラー用に構成する

次の手順では、ShareFile 用 Citrix ADC ウィザードの使用方法について説明します。

1. Citrix ADC アプライアンスにログオンし、[Configuration] タブで [Traffic Management] に移動します。
2. [Citrix ShareFile] で、[ShareFile 用に Citrix ADC をセットアップする] をクリックします。

   次の方法でウィザードにアクセスすることもできます。[モビリティ] で、[**Endpoint Management]**、**[ShareFile]**、および **[Citrix Gateway**] をクリックします。
3. ウィザードで要求された情報を入力します。

オプション	説明
名前	コンテンツスイッチング仮想サーバーの表示名。
IP アドレス	コンテンツスイッチング仮想サーバーに使用される外部（パブリックまたは DMZ）の IP アドレス。DMZ IP アドレスを使用する場合は、外部ファイアウォールアドレスからこの DMZ IP アドレスへのネットワークアドレス変換（NAT）マッピングを定義する必要があります。
ShareFile データ	このオプションが有効になり、ShareFile Data 用のストレージゾーンに Citrix ADC 接続を使用することを示します。
ネットワークファイル共有/SharePoint のストレージゾーンコネクタ	コネクタを使用し、Citrix ADC でユーザー認証を実行する場合は、チェックボックスをオンにします。
証明書	コンテンツスイッチ仮想サーバー用の証明書を選択するか、証明書をインストールします。証明書をインストールする場合は、証明書と秘密キーをアップロードするように求められます。標準ゾーンの場合、証明書はパブリックに信頼され、自己署名されていない必要があります。

オプション	説明
ストレージゾーンコントローラ IP アドレス	1 つ以上のストレージゾーンコントローラー サーバーの内部 IP アドレス。これらの IP アドレスは、ストレージゾーンコントローラサーバーを Citrix ADC 内のエンティティとして定義します。Citrix ADC にサーバーを追加済みの場合は、［既存から追加］をクリックしてサーバーを選択します。Citrix ADC を負荷分散に使用するには、各ストレージゾーンコントローラーサーバーの内部 IP アドレスを入力します。SSL と認証にのみ Citrix ADC を使用するには、IP アドレスを 1 つだけ入力します。
ポートとプロトコル	Citrix ADC からストレージゾーンコントローラーへの通信に使用されるポートとプロトコル。
認証、承認、監査（Citrix ADC AAA）仮想サーバーの IP アドレス	Citrix ADC AAA 仮想サーバーの未使用の内部 IP アドレス。Citrix ADC は、この仮想サーバーを独自に使用するために作成します。サーバーは外部アクセスを必要としません。
LDAP サーバーの IP アドレスとポート	Active Directory サーバーの IP アドレスとポート。Citrix ADC に LDAP サーバーを追加済みの場合は、［LDAP の選択］タブをクリックしてサーバーを選択します。
タイムアウト	Citrix ADC が LDAP サーバーからの応答を待機する最大秒数。デフォルトは 3 秒です。最小値は 1 秒です。
シングルサインオンドメイン	Active Directory ドメイン名。
ベース DN（ユーザーの場所）	ユーザーが格納される LDAP ベース識別名 (DN)。CN= ユーザー、dc= ドメイン、DC=NET という一般的な形式を使用して DN を指定します。
管理者バインド DN とパスワード	Active Directory と通信するためのアクセス許可を持つ管理者アカウント。
ログオン名	ユーザーがユーザー名または電子メールアドレスのどちらでログオンするかを判断するために Citrix ADC が使用する LDAP 属性。デフォルトは sAMAccountName で、ユーザーは自分のユーザー名でログオンできます。ログオン時に電子メールアドレスの入力をユーザーに要求するには、このフィールドを userPrincipalName に変更します。

コネクタへの **Web** アクセス用に **Citrix ADC** を構成する

ストレージゾーンコネクタへの Web アクセスをサポートするには、Citrix ADC for ShareFile ウィザードを完了した後に、追加の Citrix ADC 構成を実行する必要があります。

- 3 番目の Citrix ADC 負荷分散仮想サーバーを作成して構成します。この仮想サーバーを使用して、ShareFile クライアントが信頼された ShareFile ドメインにログオンしたときにのみ資格情報が送信されるようにします。

  次の手順で説明するように、HTTP OPTIONS 動詞のクライアントからの匿名アクセスを許可するように、追加の仮想サーバーを構成します。OPTIONS リクエストは、認証されず、HTTPS コールアウトなしでストレージゾーンコントローラー に渡されて署名を検証します。CORS プリフライトチェックは、資格情報を送信する前にドメインの信頼を検証します。

  設定を実行するために、CORS を理解する必要はありません。ただし、CORS の詳細については、「」を参照してください http://enable-cors.org/。

- ストレージゾーンコネクタへの Web アクセスをサポートするには、/cifs および /sp へのトラフィックに使用されるコンテンツスイッチングポリシーにパス (/ProxyService) を追加します。

ShareFile 用 Citrix ADC ウィザードを完了したら、Citrix ADC で以下の手順を実行します。

1. 3 番目の負荷分散仮想サーバを作成します。

   a) **Traffic Management > Load Balancing > Virtual Servers** に移動します。

   b) ［追加］をクリックします。

   c) 次の値を指定します。

オプション	値
名前	ポリシー名（SF_ZONE_OPTIONS など）
プロトコル	SSL
IP アドレスの種類	アドレス不能

   d) クリックして仮想サーバを作成します。

   e) ウィザードで作成した負荷分散仮想サーバーと同じサービスをバインドするには、[負荷分散仮想サーバー] 画面の [サービス] で、[>] をクリックし、[保存] をクリックします。

   f) 仮想サーバーに証明書を追加します。

2. 追加した仮想サーバーのポリシーを作成します。

   a) Traffic Management > Content Switching > Policies に移動します。

b) 詳細ウィンドウで、[追加] をクリックし、[名前]、[ターゲット LB 仮想サーバー]、および [式] の値を指定します。エクスプレッションエディタ **(Expression Editor)** をクリックし、このエクスプレッションを作成します。[**HTTP**] を選択します。[**REQ**] を選択します。「方法」を選択します。EQ (文字列) を選択し、「オプション」と入力します。式は次のように読む必要があります。
`HTTP.REQ.METHOD.EQ("OPTIONS")`

c) ［完了］をクリックします。

d) ［**Create**］をクリックします。

3. 作成したポリシーを新しい負荷分散仮想サーバーにバインドします。

a) **Traffic Management > Content Switching > Virtual Servers** に移動します。

b) 一覧で、仮想サーバーをクリックし、[編集] をクリックします。

c) [Content Switching Policy Binding] セクションに移動し、[2 Content Switching Policies] をクリックします。

d) [バインドを追加**]** をクリックします。

e) 新しいコンテンツポリシーを選択し、ターゲット負荷分散仮想サーバを選択します。

f) ［バインド］をクリックします。

g) [バインドを編集] をクリックし、[優先度] を更新します。新しいポリシーの優先順位を変更して、3 つのポリシーのうち最も小さい番号にします。

値が最も小さいポリシーは最も高いプライオリティを持つため、最初に処理されます。

4. ストレージゾーンコネクタ (_SF_CIF_SP_CSPOL) へのトラフィックに使用されるポリシーを更新します。

a) **Traffic Management > Content Switching > Policies** に移動します。

b) _SF_CIF_SP_CSPOL ポリシーを選択します。

c) ポリシー式に以下を追加します。

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

完全なポリシー表現は、次のようになります。

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

5. ShareFile データ（_SF_SZ_CSPOL）のストレージゾーンへのトラフィックに使用されるポリシーを更新します。

a) **Traffic Management > Content Switching > Policies** に移動します。

b) **_SF_SZ_CSPOL** ポリシーを選択します。

c) ポリシー式に以下を追加します。

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


完全なポリシー表現は、次のようになります。

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

表示専用共有用に **Citrix ADC** を構成する

表示専用の共有をサポートするには、ユーザーが Microsoft Office Web アプリケーションサーバー (OWA) にアクセスできる必要があります。OWA サーバーが独自のアドレスで外部からアクセスできる場合は、ストレージゾーンコントローラーに追加の Citrix ADC 構成は必要ありません。

Citrix ADC コンテンツスイッチングポリシーを使用してストレージゾーンコントローラーと Office Web App Server を単一の外部アドレスに結合する場合は、Citrix ADC for ShareFile ウィザードの完了後に追加の Citrix ADC 構成を実行する必要があります。トラフィックが外部からアクセス可能な OWA サーバーに正しくルーティングされるようにするには、Citrix ADC 構成が必要です。

次の Citrix ADC ルールを構成すると、管理者はストレージゾーンのコントローラゾーンの既存の外部アドレスを再利用できるため、OWA 用に追加の外部アドレスを作成する必要がなくなります。

追加の Citrix ADC 負荷分散仮想サーバーを作成して構成するには:

1. 追加の負荷分散サービスを作成します。
   - **Traffic Management > Load Balancing > Services** に移動します。
   - ［追加］をクリックします。
   - OWA サーバーに対応するサービスを作成するために必要な情報を入力します。［**OK**］をクリックします。
2. 追加の負荷分散仮想サーバを作成します。
   - **Traffic Management > Load Balancing > Virtual Servers** に移動します。
   - ［追加］をクリックします。
   - 次の値を指定します。

オプション	値
名前	ポリシー名（SF_owa_vServer など）
プロトコル	SSL
IP アドレスの種類	アドレス不能

   - クリックして仮想サーバを作成します。

- 前の手順で作成した OWA サービスに仮想サーバーをバインドするには、[負荷分散仮想サービスバインド]、[サービスの選択] の順にクリックします。前の手順で作成したサービスの横にあるチェックボックスをクリックします。
- ［選択］をクリックします。
- ［バインド］をクリックします。

3. OWA サーバーへのトラフィックのルーティングに使用する新しいポリシーを作成します。

   - **Traffic Management > Content Switching > Policies** に移動します。
   - ［**Add**］を選択します。
   - ポリシーの名前を指定します。
   - 次の式を追加します。
     - HTTP.REQ.URL.CONTAINS (「/wv/」)
       || HTTP.REQ.URL.CONTAINS (「/x/」)
       || HTTP.REQ.URL.CONTAINS (「/wv/」)
       || HTTP.REQ.URL.CONTAINS (「/p/」)
       完全なポリシー表現は、次のようになります。
       HTTP.REQ.URL.CONTAINS (「/ホスティング/ディスカバリー」)
       || HTTP.REQ.URL.CONTAINS (「/x/」)
       || HTTP.REQ.URL.CONTAINS (「/wv/」)
       || HTTP.REQ.URL.CONTAINS (「/p/」)

4. 負荷分散仮想内の新しいポリシーの優先順位を更新します。

   - **Traffic Management > Content Switching > Virtual Servers** に移動します。
   - 負荷分散仮想サーバをクリックし、[コンテンツスイッチングポリシー] を選択します。
   - （例）「_SF_OWA」ポリシーが 3 番目に優先されるように、ポリシーの優先度を変更します。

優先度	ポリシー名
90	SF_ZK_OPTIONS
95	_SF_CIF_SP_SPOL
99	_SF_OWA
100	_SF_SZ_CSPOL

   - ［閉じる］をクリックします。[完了] をクリックします

ストレージゾーンコントローラー サービスのモニターを作成する

デフォルトでは、Citrix ADC はストレージゾーンコントローラーサーバーに ping を送信して、オンラインかどうかを判断します。ただし、コントローラーがオンラインであっても、ShareFile Web サイトにハートビートメッセー

ジを送信できない場合があります。その場合、Citrix ADC は ShareFile と通信していませんが、ストレージゾーンコントローラーにトラフィックを送信します。

ShareFile へのストレージゾーンコントローラーのアウトバウンド接続を確認するには、heartbeat.aspx をチェックするモニターを作成し、各ストレージゾーンコントローラーの Citrix ADC サービスにバインドします。

```
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 は、ストレージゾーンコントローラーに対応する Citrix ADC サービスです。このサービス名は、Citrix ADC for ShareFile ウィザードによって自動的に作成されます。サービス名には、SF_SVC_IP-Address など、コントローラの IP アドレスが含まれます。

-secure サービスがポート 443 でリッスンしている場合は、YES が必要です。

Citrix ADC の構成を確認する

ウィザードを完了したら、[トラフィック管理**] > [**負荷分散**] > [**仮想サーバー] の順に選択し、ウィザードによって作成された負荷分散仮想サーバーのステータスを表示します。

Citrix ADC を介した **ShareFile** 要求のスループットを表示する

スループット統計は、[ダッシュボード**]** メニューに表示されます。

Citrix ADC を手動で構成する

January 5, 2023

バージョン 10.1 ビルド 120.1316 以降、NetScaler には、ストレージゾーンコントローラのデータとコネクタに必要な設定を構成するウィザードが含まれています。

このセクションの手順では、ストレージゾーンコントローラに必要な **Citrix ADC** 設定について説明します。すべてのリンクは、NetScaler 10.1 のドキュメント用です。これ以降のバージョンの Citrix ADC でも同様のトピックを使用できます。

すべての着信メッセージで有効な **URI** 署名をチェックするには

1. sf_callout という名前の HTTP コールアウトを作成します。
   a)「HTTP コールアウトの設定」ダイアログ・ボックスで、「仮想サーバー」または「**IP** アドレス」をクリックし、アドレスを指定します。

b) [サーバーに送信する要求] で、[属性ベース] をクリックし、[要求属性の構成] をクリックします。

c) [メソッドを取得] を選択します。

d) Host Expression に、任意のストレージゾーンコントローラの仮想サーバーの IP アドレスまたはホスト IP アドレスを入力します。

e) URL ステムの式に、次のように入力します。

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

f)「**OK**」をクリックし、「HTTP コールアウトの設定」ダイアログボックスに戻ります。

g) [サーバー応答] で、[戻り値の型] の [Bool] を選択します。

h) 応答からデータを抽出する式に、次のように入力します。

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

i) [作成] をクリックします。

2. 上記の手順に従って、sf_callout_y という名前の HTTP コールアウトを設定します。エクスプレッション以外の同じ設定を使用します。

   - URL ステムの式に、次のように入力します。

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

3. レスポンダーポリシーを設定します。

   a) [レスポンダーポリシーの構成] ダイアログボックスで、[操作] で [削除] を選択します。

   b) 次の式を入力します。

```
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)
```

   詳しくは、「レスポンダー」を参照してください。

4. レスポンダーポリシーをロードバランサー仮想サーバーにバインドし、SSL セッションベースのパーシステンスを設定します。

負荷分散するには

1. トークンベースの負荷分散を設定します。

   ルール式を使用します。 “`http.REQ.URL.QUERY.VALUE("uploadid")`”

トークンベースの負荷分散は、高可用性展開の Storage Zone Controller に必要です。ラウンドロビン負荷分散では、アップロードまたはダウンロードのクライアント要求が ShareFile.com から認証要求を受信した以外のストレージゾーンコントローラに転送される可能性があるため、ダウンロードまたはアップロードが断続的に失敗します。

2. SSL 接続を終了するように Citrix ADC を構成します。

   詳細については、SSL オフロードの設定を参照してください。

コネクタのコンテンツの切り替えと認証を構成するには

1. コンテンツスイッチングを有効にするには、「コンテンツ切り替えの有効化」を参照してください。
2. オンプレミスストレージゾーンからの ShareFile データに対するユーザーリクエストに対するコンテンツスイッチングポリシーを作成します。

   a) コンテンツスイッチングポリシーの設定ダイアログボックスで、コンテンツスイッチングポリシーの名前を入力します。以下の手順では、Data_Requests という名前を使用します。

   b) 次の式を入力します。

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

   c) [**OK**] をクリックします。

   詳しくは、「コンテンツスイッチ」を参照してください。

3. ストレージゾーンコネクタからアクセスされるデータに対するユーザー要求に対するコンテンツスイッチングポリシーを作成します。

   a) コンテンツスイッチングポリシーの設定ダイアログボックスで、コンテンツスイッチングポリシーの名前を指定します。以下の手順では、Connector_Requests という名前を使用します。

   b) 次の式を入力します。

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

   必ず「StorageZonesControllerFQDN」をご使用のコントローラの FQDN に置き換えてください。

   c) [**OK**] をクリックします。

4. コンテンツスイッチング仮想サーバーを作成します。
5. コンテンツスイッチングポリシーのターゲットを設定します。

- ［仮想サーバーの構成（コンテンツスイッチング）］ダイアログボックスの［Data_Requests］ポリシーで、ShareFile データのストレージゾーンのロードバランサー仮想サーバーを指定します。

  このロードバランサーの仮想サーバーは、ステップ 4 でレスポンダーポリシーをバインドし、すべての受信メッセージで有効な URI 署名をチェックし、負荷分散を行うものです。

- Connector_Requests ポリシーで、ストレージゾーンコネクタのロードバランサーの仮想サーバーを指定します。

6. ストレージゾーンコントローラの認証仮想サーバを設定します。

   Citrix ADC への認証はオプションですが、推奨されるベストプラクティスです。

   a) ナビゲーションペインで、[負荷分散] を展開し、ストレージゾーンコネクタ用のロードバランサー仮想サーバーの名前を選択し、[開く] をクリックします。

   b) [仮想サーバーの構成 (負荷分散)] ダイアログボックスで、[詳細設定] タブをクリックし、[認証の設定] を展開します。

   c) [401 ベース認証] のチェックボックスをオンにし、[認証] 仮想サーバーを選択します。

   d) [メソッドと永続性] タブをクリックします。

   e) [永続性] で、[**COOKIEINSERT]** を選択します。

   f) [タイムアウト (最小)] に **240** と入力します。

      タイムアウト値は 240 分をお勧めします。10 分を超える最小値を使用してください。

      詳細については、「認証仮想サーバーの構成」を参照してください。

7. [認証サーバーの構成] ダイアログボックスを使用して、認証サーバーを作成および構成します。

   「SSO 名属性」に「**userPrincipalName**」と入力します。

   その他の設定の詳細については、「認証ポリシー」を参照してください。

8. 認証サーバの認証ポリシーを設定します。

   a) [認証ポリシーの設定] ダイアログボックスで、ポリシーの名前を入力し、前の手順で構成した認証サーバーを選択します。

   b) 次の式を入力します。

      ```
      ns_true
      ```

   詳細については、「認証ポリシーの設定」を参照してください。

9. シングルサインオン用のセッションプロファイルを構成します。

   a) [セッションプロファイルの構成] ダイアログボックスで、プロファイルの名前を入力します。
   b) [Web アプリケーションへのシングルサインオン] チェックボックスをオンにします。
   c) [資格情報インデックス] で、[プライマリ] を選択します。

d) シングルサインオンドメインに、ストレージゾーン Controller のドメイン名を入力します。
e) 上記の 3 つの項目のそれぞれの「オーバーライド・グローバル」チェック・ボックスを選択します。

詳細については、「セッションプロファイル」を参照してください。

10. シングルサインオン用のセッションポリシーを設定します。

a) [セッションポリシーの構成] ダイアログボックスで、ポリシーの名前を入力します。

b) [Request Profile] で、前のステップで設定したセッションプロファイルの名前を選択します。

c) 次の式を入力します。

```
ns_true
```

詳細については、「セッションポリシー」を参照してください。

11. 認証仮想サーバーを作成します。

a) [仮想サーバーの構成 (認証)] ダイアログボックスで、サーバーの名前と IP アドレスを入力します。
b) [認証] タブをクリックし、[プロトコル] で [**SSL**] を選択します。
c) [ユーザーを認証する] チェックボックスをオンにします。
d) [認証ポリシー] で [プライマリ] をクリックし、手順 7 で構成した認証ポリシーを選択します。
e) [ポリシー] タブをクリックし、[セッション] をクリックして、ステップ 9 で設定したセッションポリシーを選択します。

詳細については、「認証仮想サーバーの構成」を参照してください。

プライベートデータストレージ用のネットワーク共有を作成する

April 27, 2021

ShareFile Data のストレージゾーンには、プライベートデータ用のネットワーク共有が必要です。複数の Storage Zone Controller が 1 つのゾーン内で高可用性および負荷分散用に構成されている場合、すべてのコントローラーが同じ共有場所でプライベートデータにアクセスします。

サポートされているサードパーティ製ストレージシステムに ShareFile ファイルを格納する場合でも、Storage Zone Controller には、暗号化キー、キューに入れられたファイル、その他の一時項目、およびストレージシステムへのファイルのアップロードまたはダウンロードに使用されるストレージキャッシュ用のネットワーク共有が必要です。ストレージキャッシュについて詳しくは、「ストレージキャッシュ操作のカスタマイズ」を参照してください。

ストレージゾーンコントローラは、IIS アカウントプールユーザーを使用してネットワーク共有にアクセスします。既定では、アプリケーションプールは、低レベルのユーザー権限を持つ Network Service ユーザーアカウントで動作します。Storage Zone Controller は、デフォルトでネットワークサービスアカウントを使用します。ネットワークサービスアカウントの代わりに名前付きユーザーアカウントを使用して、共有にアクセスできます。ネットワークサービスアカウントを使用して、IIS アプリケーションプールおよび Citrix ShareFile サービスを実行します。

1. ネットワークサービスアカウントの代わりに名前付きユーザーアカウントを使用して共有にアクセスする場合は、Active Directory に名前付きユーザーアカウントを作成します。この名前付きユーザーアカウントを ShareFile サービスアカウントと呼びます。
   注：Storage Zone Controller を構成するときは、ネットワーク共有ユーザー名およびネットワーク共有パスワードを指定します。このパスワードは、共有へのアクセスに使用するアカウントの資格情報（ShareFile サービスアカウントまたはネットワークサービスアカウント）です。

   セキュリティを向上させるために、管理者は、ShareFile ストレージリポジトリを含む特定のフォルダに対する他のすべてのユーザーに対する権限を拒否し、構成中のストレージロケーションユーザーにのみアクセスを許可する必要があります。
2. ネットワーク共有をホストするサーバーに接続し、ShareFile プライベートデータ用のフォルダーを作成します。
3. フォルダを右クリックし、[特定のユーザーと共有…] を選択します。
4. 共有へのアクセスに使用するアカウント (ネットワークサービスアカウントまたは ShareFile サービスアカウント) を追加し、アクセス許可レベルを [読み取り/書き込み] に変更します。
5. [共有] をクリックし、[完了] をクリックします。
6. フォルダを右クリックし、[プロパティ] を選択します。
7. [セキュリティ] タブで、共有へのアクセスに使用するアカウント (ネットワークサービスアカウントまたは ShareFile サービスアカウント) に [フルアクセス] アクセス許可が付与されていることを確認します。

ゾーンあたりのファイル数を増やす

デフォルトでは、Storage Zone Controller は、CIFS 共有を使用して、単一のフォルダではなくフォルダの階層にファイルを格納するように構成されています。

永続的なストレージレイアウトを分割するように Storage Zone Controller を構成できます。これにより、ストレージアレイのタイプによっては、ゾーンあたりの最大ファイル数が 50 万未満から 1,000 万以上に増加します。追加の容量が必要な場合は、デフォルトを変更できます。

複数のフォルダーにファイルを保存する **Storage Zone Controller** を有効にするには

> 注意：
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
>
> 注：

> Storage Zone Controller がアップグレードされている場合は、レジストリキーの値HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone\PathSelection is set to 1. If it is set to 0, update it to 1かどうかを確認してください。

レジストリの編集が終了したら、Storage Zone Controller で IIS を再起動します。

フォルダの最大数を増やすには

既定では、分割されたストレージレイアウトには 256 の最上位フォルダがあり、各フォルダには 256 個のフォルダが含まれています。その構成は、プライマリ Storage Zone Controller レジストリキーHKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone: PathSelectionParams=2,2で表されます。

最初の値は、最上位フォルダの数を「16」または 256 の累乗に制限します。2 番目の値は、最上位フォルダの子フォルダの数も 256 に制限されます。

同じ式 (N の累乗数 16) を使用して、サイトに適切な値を決定できます。たとえば、PathSelectionParams=3,4,4,4 は、最上位フォルダの数を 4096 (16 から 3 の累乗) に制限します。2 番目の値は、最上位フォルダの子フォルダの数を 65536 (16 から 4 の累乗) に制限します。3 番目の値は、第 2 レベルのフォルダの子フォルダの数を 65536 に制限します。

レジストリの編集が終了したら、プライマリおよびセカンダリの Storage Zone Controller で IIS を再起動します。

空のフォルダを削除するには

Storage Zone Controller が複数のフォルダーにファイルを格納する場合、ファイルを削除すると、空のフォルダーになることがあります。デフォルトでは、Storage Zone Controller は空のフォルダーを削除します。ファイル削除サービスは、空のフォルダを削除します。このフォルダはツリーの一番下から始まり、空でないフォルダに達するまで続きます。

ただし、アップグレードパスによっては、設定が更新されない場合があります。アップグレード後、C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.configに次のキーが表示されていることを確認します。

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

キーを追加する必要がある場合は、完了したらファイル削除サービスを再起動します。

SSL 証明書のインストール

April 27, 2021

ワイルドカード証明書を使用しない場合は、Storage Zone Controller サーバーの証明書署名要求 (CSR) を作成し、要求を認証局 (CA) に送信する必要があります。ヘルプについては、CA のマニュアルを参照してください。

証明書をインストールするには、次の手順に従います。

1. Storage Zone Controller サーバーで MMC を開き、［ファイル］**>**［スナップインの追加と削除］を選択します。
2. [証明書] を選択し、[追加] をクリックします。
3. [コンピューターアカウント]、[次へ]、[完了]、[**OK**] の順にクリックします。
4. MMC コンソールで、[証明書**] > [**個人**]** を展開します。
5. [証明書] を右クリックし、[すべてのタスク**] > [**インポート] を選択し、[次へ] をクリックします。
6. [参照] をクリックし、ファイル名拡張子メニューから [個人情報交換] を選択します。
7. 証明書の場所を参照し、[開く] をクリックします。
8. [次へ] をクリックし、秘密キーに関連付けられたパスワードを入力し、[次へ] を 2 回クリックし、[完了] をクリックします。
9.「インポートに成功しました」というメッセージが表示されたら、「**OK**」をクリックします。

パブリック証明書の場合は、発行されるドメインが Storage Zone Controller ローカル IP アドレスに解決されていることを確認します。これを行うには、Storage Zone Controller の hosts ファイルを更新して、証明書に関連付けられたドメインを Storage Zone Controller の IP アドレスにマップします。2 つのアドレスが解決されない場合、ユーザーは Storage Zone Controller からファイルをアップロードできません。

ShareFile データ用にサーバーを準備する

November 17, 2023

このセクションで説明する Web サーバー (IIS) の役割と ASP.NET セットアップは、ShareFile データおよび記憶域ゾーンコネクタ用の記憶域ゾーンに必要です。これらの手順は Windows Server 2012 に基づいていますが、それ以降のバージョンでも有効です。

Microsoft .NET バージョンの更新

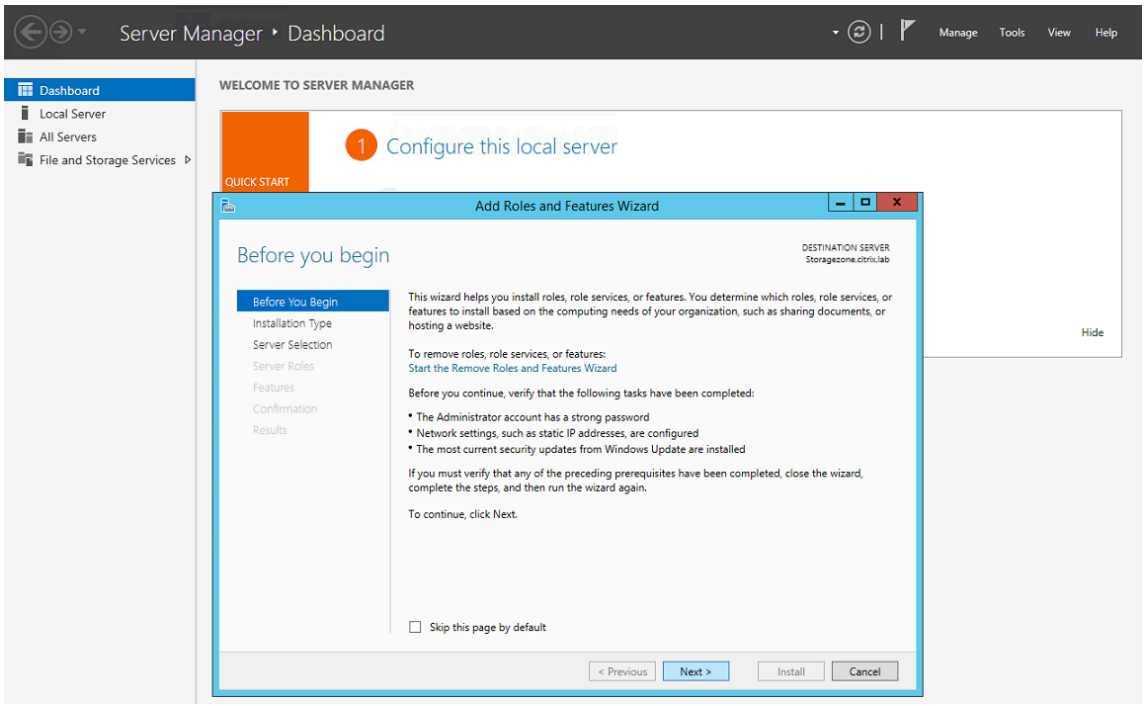
ストレージゾーンコントローラーのインストールに進む前に、適切なバージョンの Microsoft .NET Framework を使用していることを確認してください。

- ストレージゾーンコントローラ **5.x** には、**.NET 4.8** 以降が必要です。.NET 4.8 をダウンロードするにはここをクリックしてください

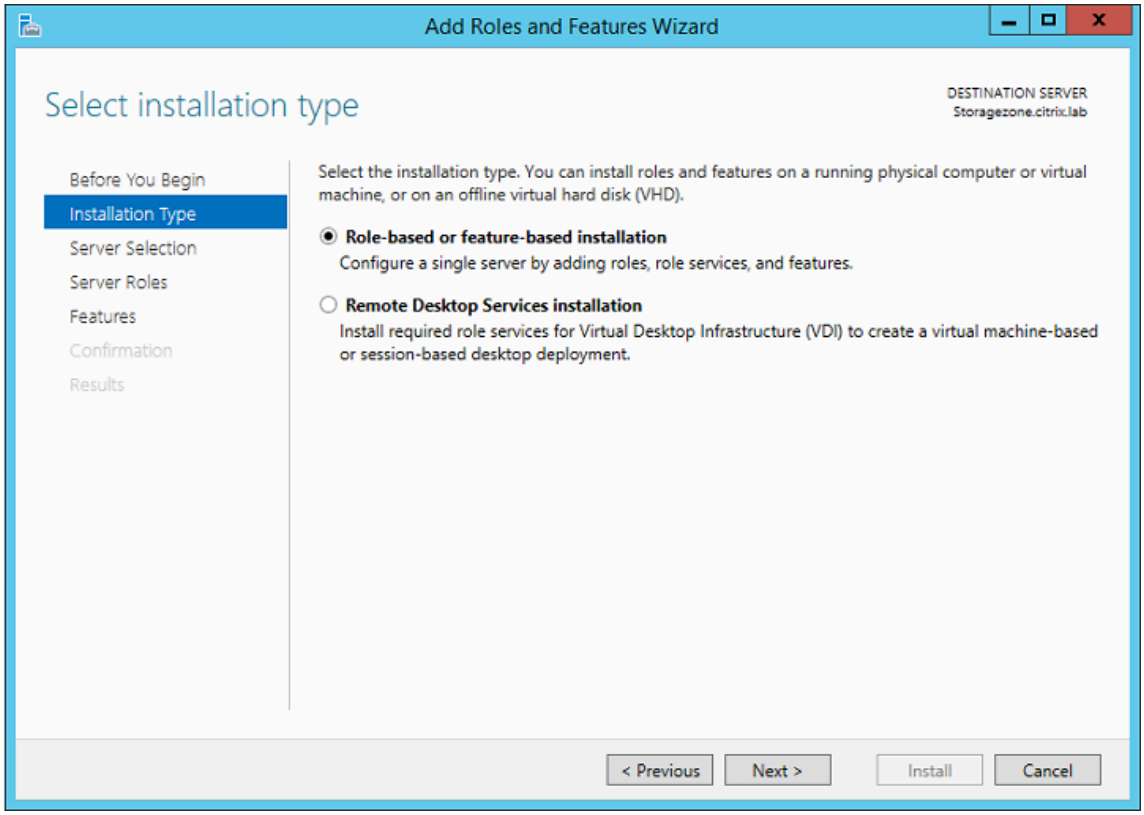
ShareFile アプリケーションを使用する場合は、Microsoft.NET の最新バージョンを利用することを推奨します。

Web サーバー **(IIS)** の役割と **ASP.NET** 役割サービスを有効にするには

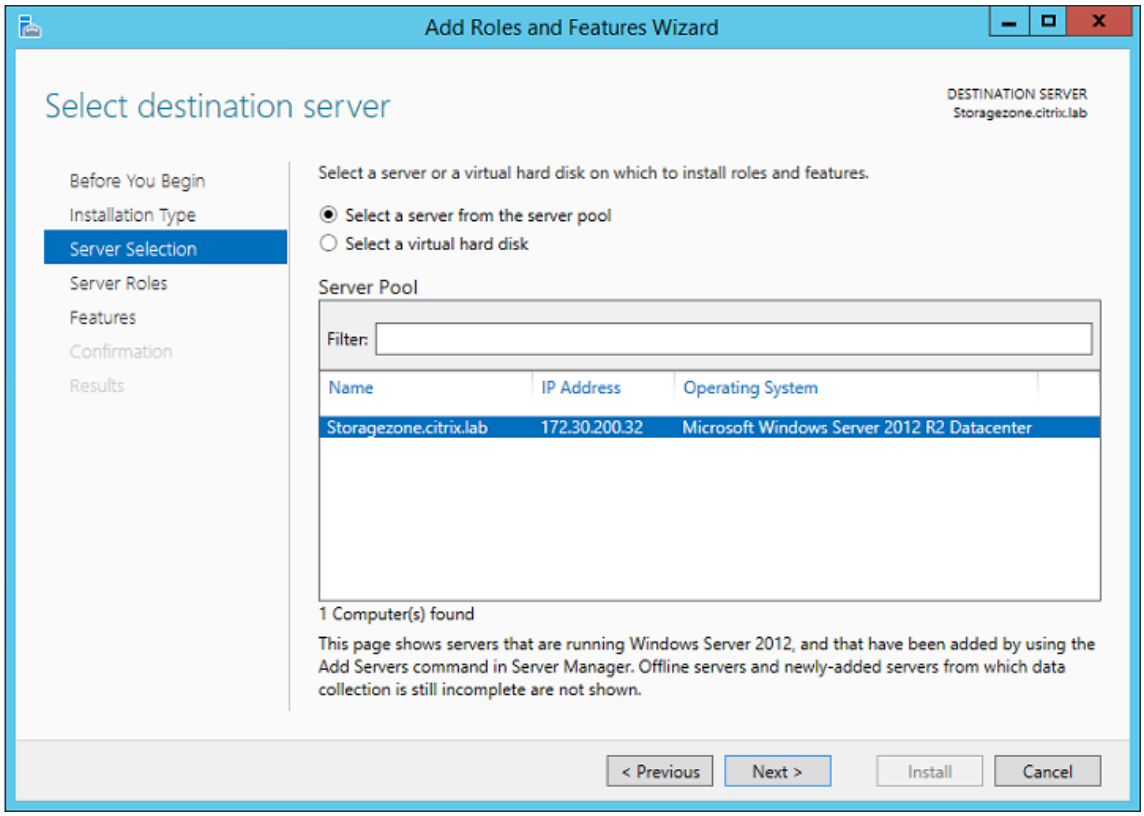
1. ストレージゾーンコントローラーをインストールするサーバーに、ローカル管理者権限を持つアカウントでログオンします。
2. サーバーマネージャーコンソールのダッシュボードを開き、[管理**] > [**役割と機能の追加] をクリックして、役割と機能の追加ウィザードを開きます。
3. 役割と機能の追加ウィザードで、[次へ] をクリックします。



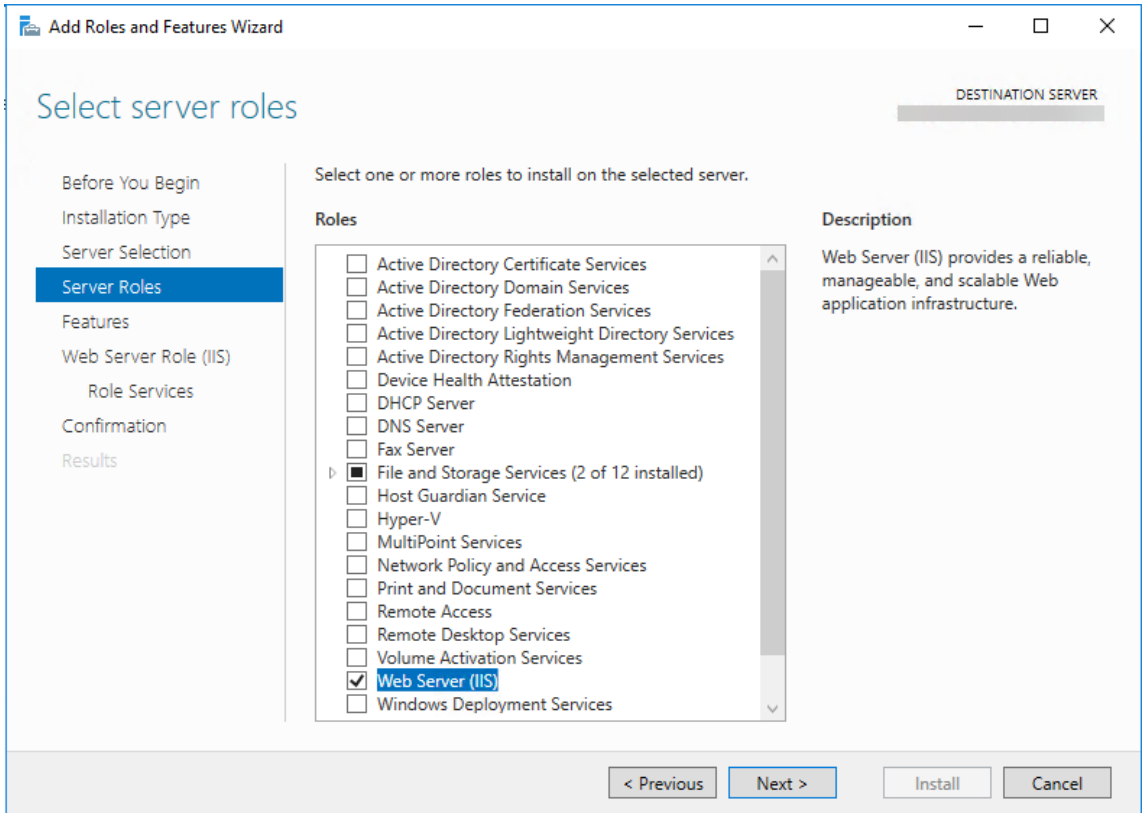
4. [インストールの種類を選択] ページで、[役割ベースまたは機能ベースのインストール] をクリックし、[次へ] をクリックします。



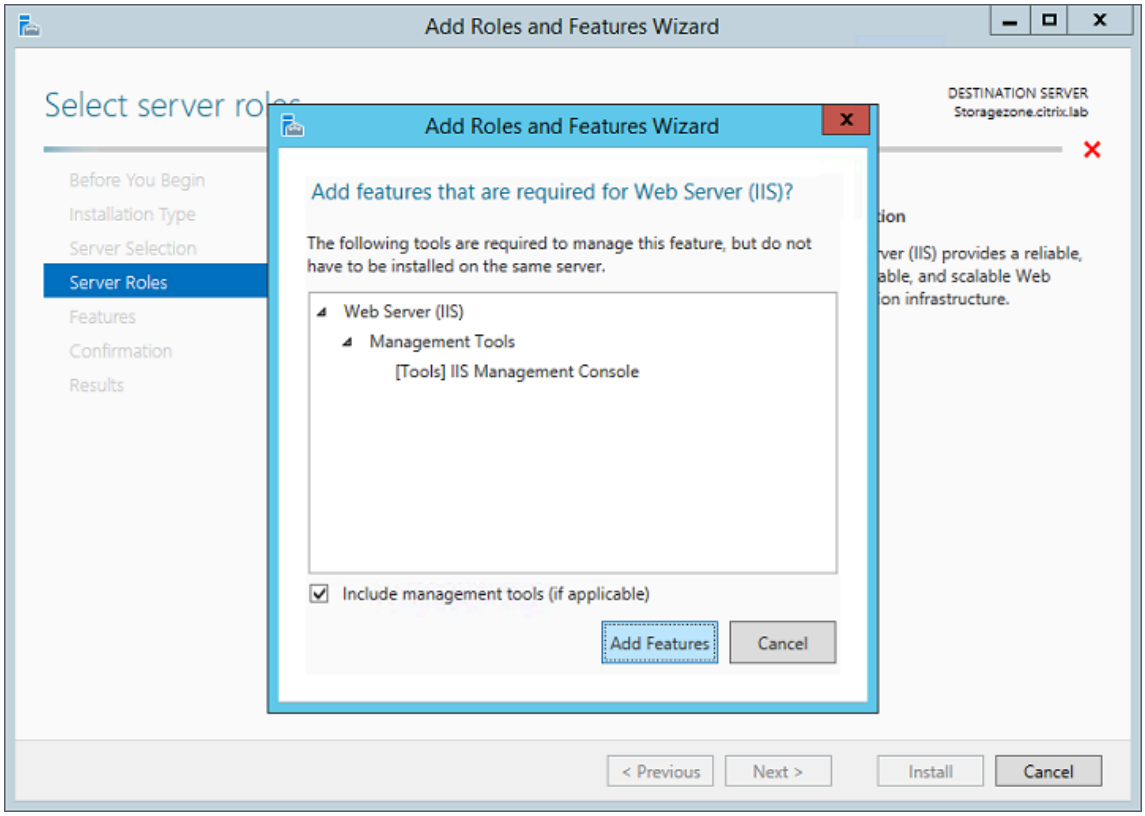
5. [宛先サーバーの選択] ページで、サーバープールからサーバーを選択し、[次へ] をクリックします。



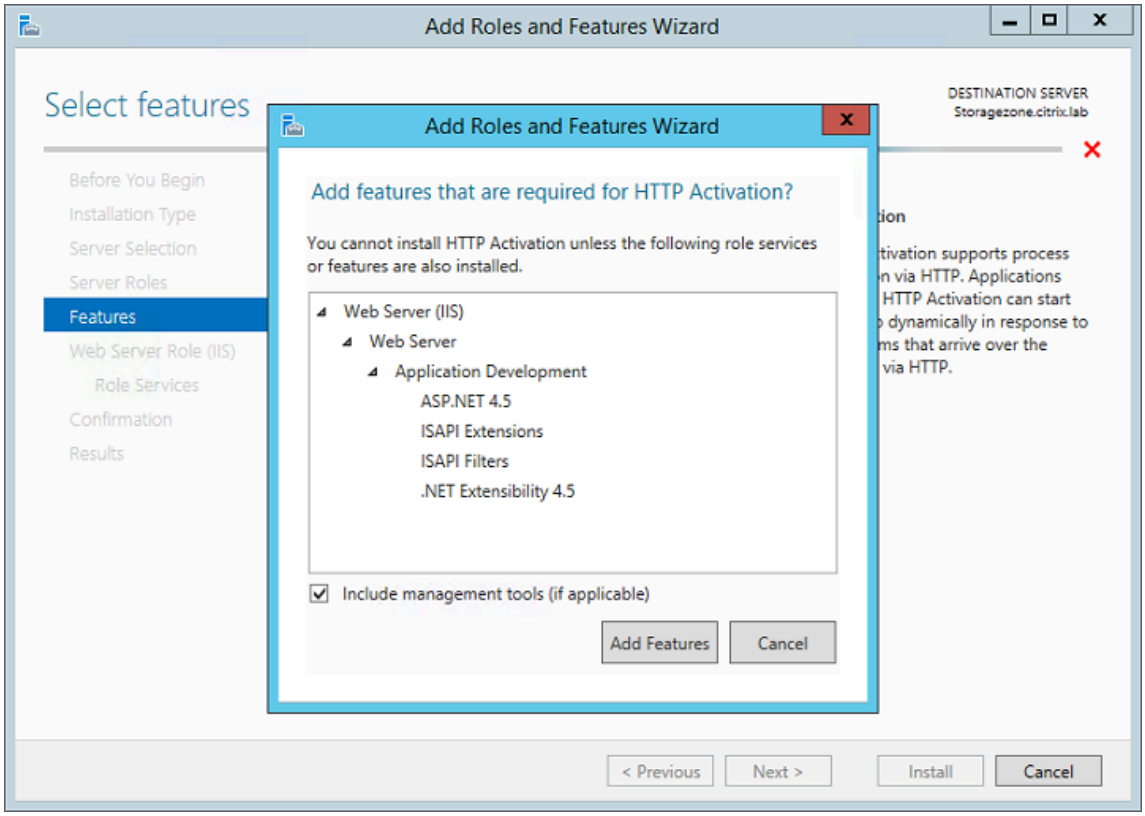
6. [サーバーの役割の選択] ページで、[Web サーバー (IIS)] チェックボックスをオンにし、[次へ] をクリックします。



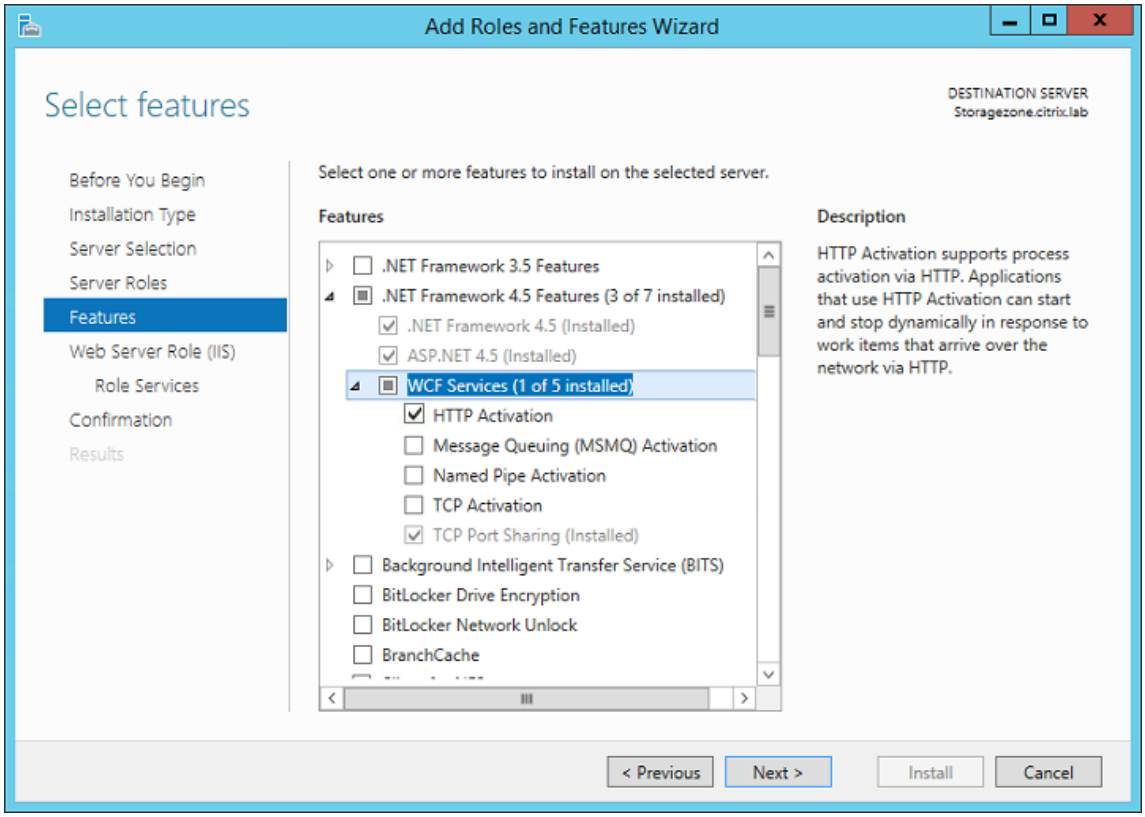
7. [機能の追加] をクリックして、IIS に必要な機能を追加します。



8. [機能を追加] をクリックします。[機能の選択] ページが表示されます。

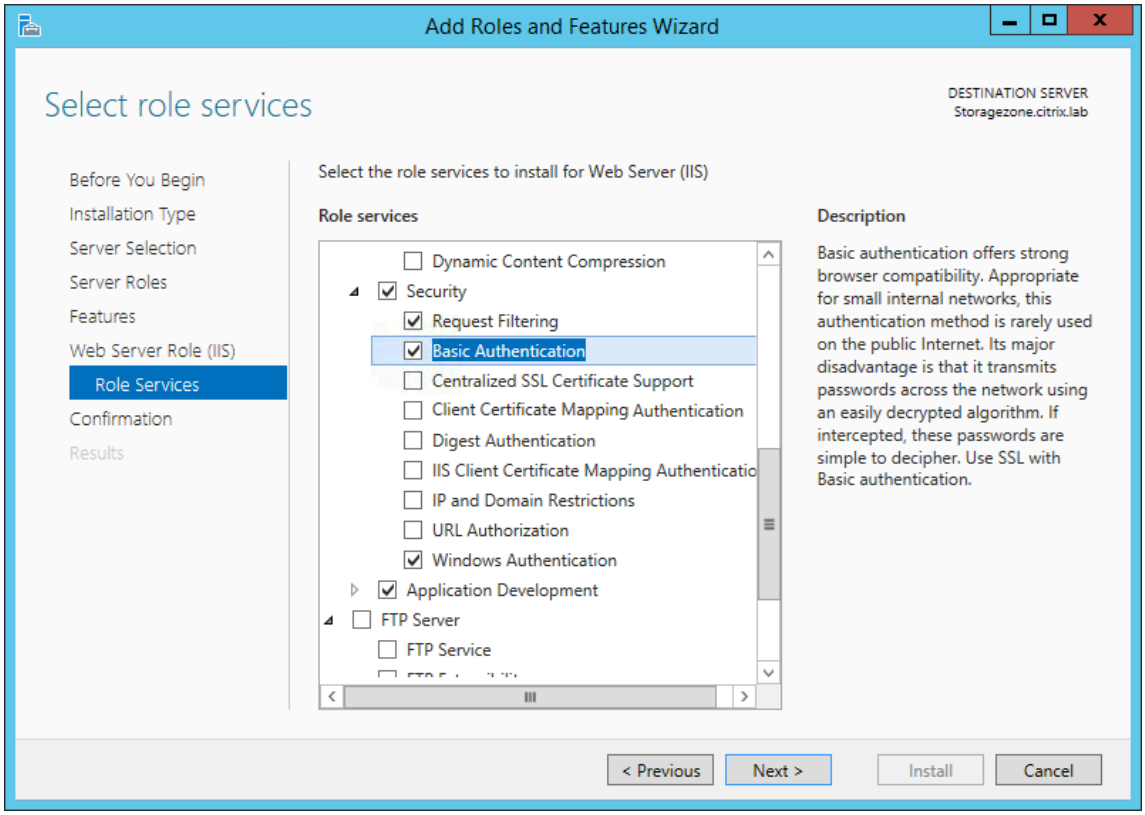


9. 次の画面に表示されている必要な設定を選択し、[次へ] をクリックします。



10. [Web サーバーの役割 (IIS)] ページで、[次へ] をクリックします。

11. [役割サービスの選択] ページで、[基本認証] および [Windows 認証] チェックボックスをオンにし、[次へ] をクリックします。

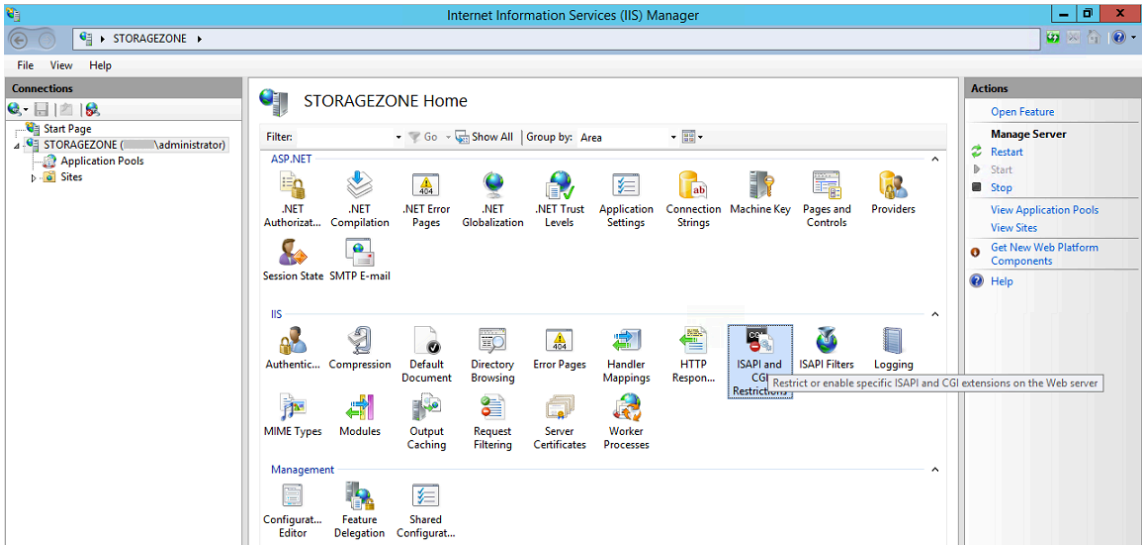


12. [インストールの選択の確認] ページで、[インストール] をクリックします。
13. インストールが完了したら、[閉じる] をクリックし、サーバーを再起動します。

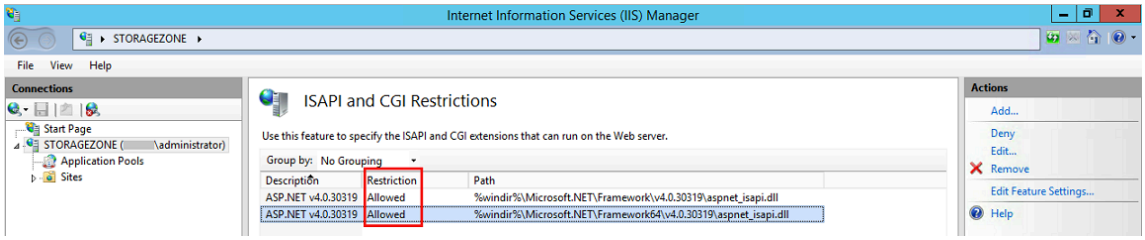
IIS を構成するには

Web サーバー (IIS) の役割と ASP.NET 役割サービスを有効にした後、IIS を構成します。

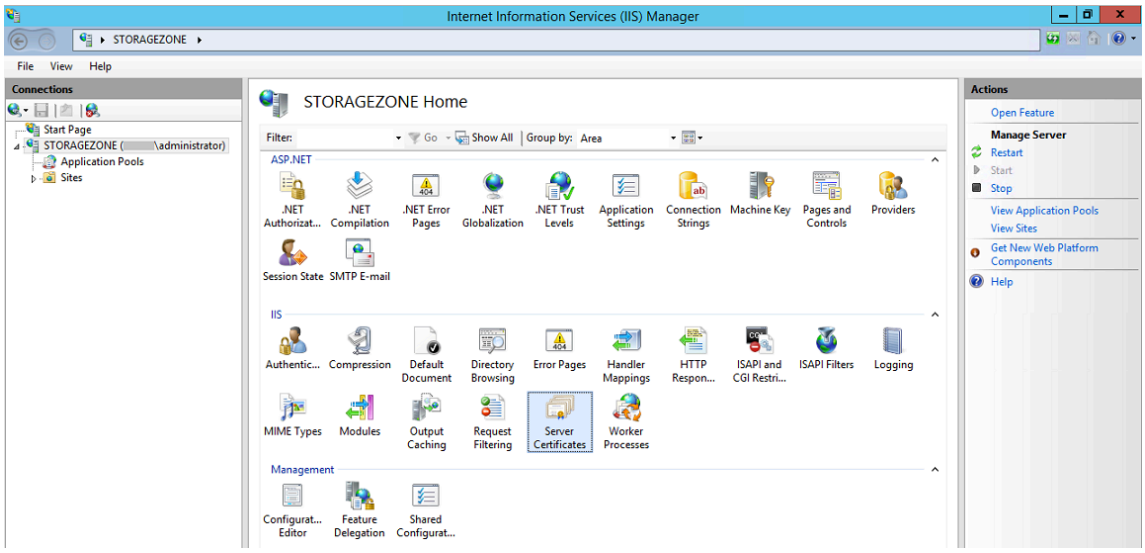
1. IIS マネージャーコンソールを開き、ストレージゾーンコントローラーのサーバーノードをクリックし、次に [ISAPI と CGI の制限] をダブルクリックします。



2. 各 ASP.NET エントリを [許可] に設定します。



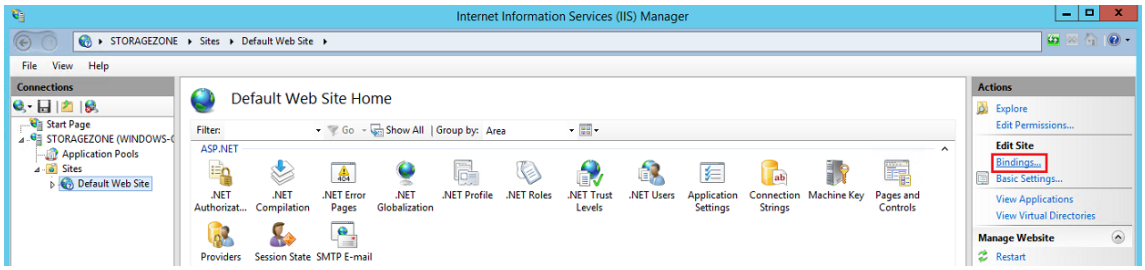
3. ドメインサーバーまたはパブリック証明書がサーバーにインストールされていることを確認します。IIS マネージャーコンソールで、ストレージゾーンコントローラーサーバーノードをクリックし、「サーバー証明書」をダブルクリックします。



パブリック認証局に関連付けられた証明書がない場合は、続行する前にサーバーに証明書をインストールしてください。詳細については、「SSL 証明書のインストール」を参照してください。

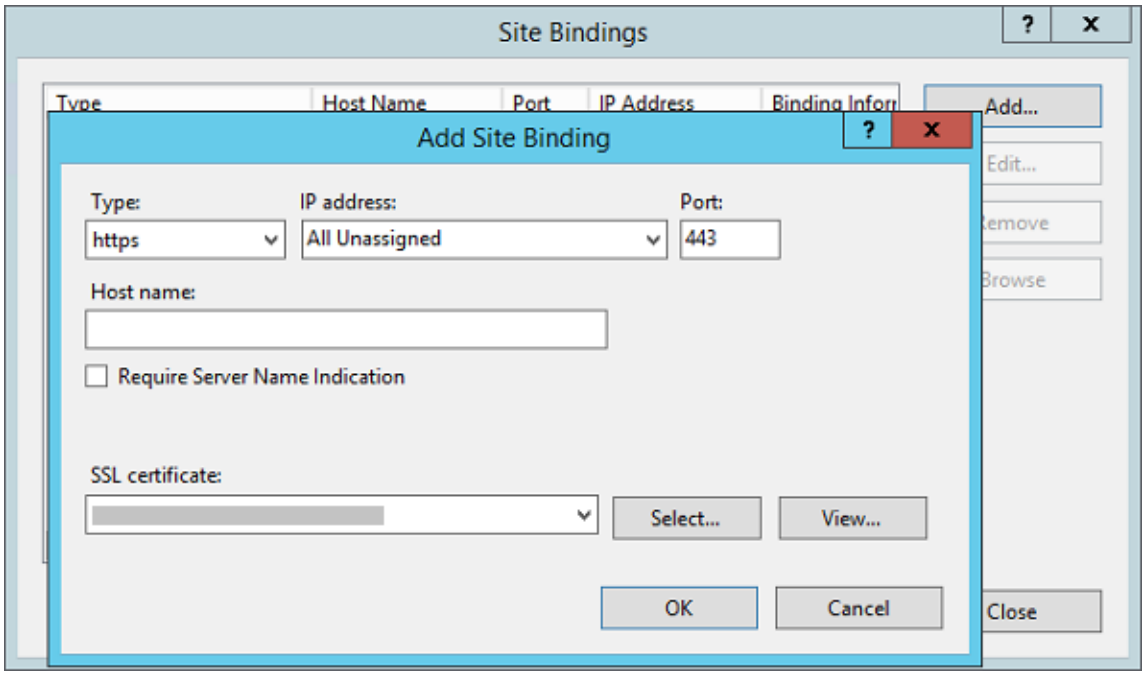
> 注:
>
> ストレージゾーンコントローラーを備えた NetScaler Gateway または同様のアプライアンスを使用している場合は、ドメインサーバー証明書を使用できます。標準ゾーンのすべてのインターネットトラフィックは、パブリック証明書を使用して処理する必要があります。

4. IIS マネージャーコンソールで、[既定の **Web** サイト] をクリックし、[バインド] をクリックします。



5. [追加] をクリックし、次のようにサイトバインドを設定します。

   - タイプは https です。
   - IP アドレスはすべて未割り当てです。
   - ポートは 443 です。
   - SSL 証明書は、インストールされている証明書です。



6. Web サーバ接続をテストするには、`http://localhost/`と`https://localhost/`に移動します。接続に成功すると、IIS ロゴが表示されます。

   HTTPS は、URL ヘッダーのローカルホスト名と一致しない証明書に関するメッセージを表示します。これは期待されており、安全にウェブサイトに進むことができます。

7. ストレージゾーンコントローラーを VM にインストールする場合は、VM のスナップショットを撮ります。

> 注:
>
> ストレージゾーンコントローラーは CORS を使用するため、**OPTIONS** http 動詞を有効にする必要があります。IIS リクエストフィルタリング機能をチェックして、**OPTIONS** 動詞が無効になっていないことを確認してください。

ストレージゾーンコントローラをインストールし、ストレージゾーンを作成する

March 20, 2024

> 重要:
>
> - インストールを開始する前に、環境がシステム要件を満たしていることを確認してください 。
> - ShareFile ストレージゾーンコントローラーは、アプリケーション固有のパスワードを使用します。詳しくは、「アプリケーション固有のパスワードの作成」を参照してください。

ストレージゾーンコントローラーをインストールするときは、ゾーンを作成してプライマリストレージゾーンコントローラーを構成するか、
セカンダリストレージゾーンコントローラーをゾーンに追加します。

プライマリストレージゾーン Controller の設定時に、次の機能のいずれかまたは両方を有効にできます:

- ShareFile Data のストレージゾーン。プライベートデータストレージ (プライベートネットワーク共有またはサポートされているサードパーティストレージシステムのいずれか) を指定します。
- ストレージゾーンコネクタ:SharePoint サイトまたは指定されたネットワークファイル共有上のドキュメントへのアクセスをユーザーに許可します。

次の手順では、ストレージゾーンコントローラのインストール、IIS の既定の Web サイトの認証の構成、ゾーンの作成、および機能を有効にする方法について説明します。

1. Storage Zone Controller ソフトウェアをダウンロードしてインストールします:

   - の ShareFile ダウンロードページからログオンし https://dl.sharefile.com/storagezone-controller、最新のストレージゾーンコントローラーインストーラーをダウンロードします。

   > 注:
   >
   > ストレージゾーンコントローラをインストールすると、サーバ上の Default Web サイトがコントローラのインストールパスに変更されます。

   匿名認証は、既定の Web サイトで有効にする必要があります。

2. ストレージゾーンコントローラをインストールするサーバで、StorageCenter.msi を実行します。
   - ShareFile Storage Zone Controller セットアップウィザードが起動します。
   - マルチテナントの場合は、次のコマンドを実行します。***msiexec***/i StorageCenter_5.0.1.msi マルチテナント =1

   > 注:
   >
   > 上記のコマンドでは、インストールしようとしている msi の番号と一致するようにバージョン番号（この例では 5.0.1）を更新する必要がある場合があります。

   - プロンプトに応答します。インストールが完了したら、「ストレージゾーンコントローラーの構成ページを起動する」のチェックボックスをオフにし、「完了」をクリックします。
3. ストレージゾーンコントローラーを再起動します。
4. インストールが成功したかどうかをテストするには、に移動します `http://localhost/`。インストールが成功している場合、ShareFile のロゴが表示されます。
5. ShareFile のロゴが表示されない場合は、ブラウザーのキャッシュを削除してもう一度アクセスしてください。

   > 重要:
   >
   > Storage Zone Controller を複製する予定がある場合は、Storage Zone Controller の構成に進む前にディスクイメージをキャプチャします。

6. ShareFile で S3 互換のストレージプロバイダーを使用するには、ストレージゾーンを作成または構成する前に、次の手順を実行します。
   - Windows レジストリエディタを開きます ([ファイル名を指定して実行] **> [regedit.exe]**)。
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter レジストリキーを見つけてください。
   - このキーの下に新しい REG_SZ 値を作成します。
     - 値の名前: **S3EndpointAddress**
     - 値の種類: **REG_SZ**
     - 値のデータ:S3 互換のストレージエンドポイントに対応する HTTPS URL を入力します。
   - ストレージプロバイダーがパス形式のコンテナーアクセスのみをサポートしている場合 (http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.htmlを参照)、このキーの下に別の値を作成します。
     - 値の名前: **S3ForcePathStyle**
     - 値の種類: **REG_SZ**
     - 値データ: 真

- Storage Zone Controller アプリケーションプール (StorageCenterAppPool) を再起動します。
- S3 互換ストレージシステムから次の情報を収集します:
  - ShareFile データアクセスキー ID に使用する S3 バケットの名前
  - アクセスキー ID
  - シークレットアクセスキー

7. 次の手順に進み、新しいストレージゾーンを作成します。永続的なストレージの場所として Amazon S3 を選択します。ストレージゾーンコントローラーは、実際の Amazon S3 サービスの代わりに、入力したカスタムエンドポイントアドレスを使用します。S3 の詳細を設定するときは、前に作成したバケット名を選択します。
8. ストレージゾーンのコントローラーコンソールに移動します。
9. `http://localhost/configservice/login.aspx` スタート画面またはメニューから設定ツールを開くか起動します。Windows 8 でのスタート画面ショートカットの使用方法については、「ストレージゾーンコントローラーの管理」を参照してください。
10. **Storage Zones Controller Logon** ページで、アカウントのメールアドレス、パスワード、およびフルアカウント **URL** の **FQDN** サブドメイン（`subdomain.sharefile.com`または`subdomain.sharefile.eu`など）を入力します。［ログオン］をクリックします。
11. プライマリストレージゾーンコントローラーを設定するには、[**Create new Zone**] をクリックし、ゾーン情報を入力します:

オプション	説明
ゾーン	ShareFile 管理コンソールに表示される名前。
プライマリゾーンコントローラー	デフォルトは`http://localhost/ConfigService`です。SSL を使用する場合は、HTTP を https に変更します。ShareFile は、標準ゾーンに対して有効な信頼されたパブリック SSL 証明書のみをサポートしていることに注意してください。セカンダリストレージゾーンホストの設定に問題がある場合は、そのサーバーのローカルブラウザで ConfigService URL を SSL エラーなしで解決できることを確認してください。localhost はサーバーの IP アドレスに解決します。代わりにサーバー名 (など `https://servername.subdomain.com/ConfigService`) を指定できます。サーバー名は、セカンダリストレージゾーンの Controller サーバーで解決できる必要があります。

オプション	説明
ホスト名	ストレージゾーンコントローラーの一意の識別子。ShareFile では、識別子としてサーバーのホスト名を使用することをお勧めします。これは、FQDN ではなく、フレンドリ名である必要があります。この名前は、ShareFile 管理コンソールに表示されます。
外部住所	このストレージゾーンコントローラーの FQDN。このストレージゾーンコントローラーを標準ゾーンに使用する場合、URL はインターネットからアクセスできる必要があります。ロードバランサーを使用している場合は、そのアドレスを入力します。ページを送信すると、ShareFile によって住所が検証されます。

12. プライベートデータストレージを指定するには、次の手順を実行します。
    - [**ShareFile** データのストレージゾーンを有効にする] チェックボックスをオンにします。
    - 標準ゾーンを構成するには、このチェックボックスをオフにします。

    > 注:
    >
    > ストレージゾーン Controller を構成した後は、そのゾーンタイプを変更することはできません。

    ストレージゾーンコントローラーは、サービスアカウントの認証情報を使用して信頼できる Active Directory ドメインサーバーに接続し、電子メールアドレスを検索します。

    - ストレージリポジトリを選択します。
13. ストレージゾーンコネクタを有効にしたくない場合は、[登録] をクリックしてストレージゾーン Controller を ShareFile に登録し、手順 14 に進みます。
14. S3 互換のストレージを使用している場合は、ストレージゾーンの登録後に次の追加のレジストリエントリを作成します:
    - Windows レジストリエディタを開きます ([ファイル名を指定して実行] **> [regedit.exe]**)。
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storage zone\CloudStorageUploaderConfig` レジストリキーを探します。
    - このキーの下に新しい REG_SZ 値を作成します。
        - 値の名前: **S3EndpointAddress**
        - 値の種類: **REG_SZ**
        - 値のデータ:S3 互換のストレージエンドポイントに対応する HTTPS URL を入力します。

- ストレージプロバイダーがパス形式のコンテナーアクセスのみをサポートしている場合 (http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.htmlを参照)、このキーの下に別の値を作成します。
  - 値の名前: **S3ForcePathStyle**
  - 値の種類: **REG_SZ**
  - 値データ: 真
- Storage Zone Controller アプリケーションプール (StorageCenterAppPool) を再起動します。

15. ストレージゾーンコネクタを有効にするには:

    コネクタを有効にすると、IIS アプリ「cifs」(ネットワークファイル共有用のコネクタ) と「sp」(SharePoint 用のコネクタ) が作成されます。

    - 使用するコネクタの種類ごとに、[ネットワークファイル共有の記憶域ゾーンコネクタを有効にする] と [SharePoint の記憶域ゾーンコネクタを有効にする] チェックボックスをオンにします。コネクタ設定の詳細については、このセクションの「ストレージゾーンコネクタの構成」を参照してください。
    - [登録] をクリックします。ストレージゾーンのコントローラー情報が表示されます。
    - ストレージゾーンコネクタに [許可パス] または [拒否されたパス] を指定した場合は、IIS サーバーを再起動します。

16. セカンダリストレージゾーンコントローラーを設定するには、「ストレージゾーンコントローラーの管理」を参照してください。

> 重要:
>
> Storage Zones Controller がローカルサイトにインストールされており、バックアップはユーザーが担当します。デプロイメントを保護するには、ストレージゾーンコントローラーサーバーのスナップショットを作成し、ストレージゾーンコントローラー構成をバックアップして、障害復旧に備えてストレージゾーンコントローラーを準備する必要があります。

ShareFile データのストレージゾーンの構成

> 注:
>
> ShareFile データのストレージゾーンは、Citrix Endpoint Management エンタープライズエディションで使用でき、他の Citrix Endpoint Management エディションでは使用できません。

ShareFile Data 用のストレージゾーンは、ストレージゾーンを作成するときのストレージゾーンコントローラーウィザードまたはストレージゾーンコントローラーコンソールから構成できます。ShareFile Data タブを使用して、プライベートネットワーク共有またはサポートされているサードパーティストレージシステムの設定を構成します。

ネットワーク共有設定

オプション	説明
ストレージリポジトリ	[ローカルネットワーク共有] を選択します。ゾーンの作成後、[ストレージリポジトリ] オプションを変更することはできません。たとえば、ローカルネットワーク共有からサードパーティのストレージに切り替えるには、新しいゾーンを作成する必要があります。
ネットワーク共有場所	プライベートデータストレージ、および暗号化キー、キューに格納されたファイル、およびその他の一時アイテムなどのデータに使用するネットワーク共有への UNC パス。`\\server\share`形式でパスを指定します。同じストレージゾーンに属するストレージゾーンコントローラーは、同じファイル共有をストレージに使用する必要があります。注意: ストレージゾーンコントローラーは、このパスのデータを独自のストレージ形式で上書きします。ファイルデータのある場所へのパスを指定しないでください。この保存場所は、ShareFile Data 専用のストレージゾーン用に予約してください。ストレージゾーンコントローラーは、構成ページに記載されているネットワーク共有ユーザー名/パスワードを使用してネットワーク共有にアクセスします。構成ページにネットワーク共有のユーザー名/パスワードが指定されていない場合は、ネットワークサービスアカウントがデフォルトで使用されます。ネットワークサービスアカウントには、この格納場所へのフルアクセス権が必要です。ストレージゾーンコントローラーは、StorageCenterAppPool のネットワークサービスアカウントもデフォルトで使用します。サポートされている構成は、ネットワークサービスアカウントを使用することだけであることに注意することが重要です。
ネットワーク共有のユーザー名とネットワーク共有パスワード	ネットワーク共有の場所の UNC パスの資格情報。ネットワークサービスアカウントの代わりに名前付きユーザーアカウントを使用して共有にアクセスするには、これらの資格情報を指定します。ネットワークサービスアカウントを使用して、IIS アプリケーションプールと ShareFile サービスを引き続き実行できます。

オプション	説明
暗号化を有効にする	ファイル共有に格納されているファイルコンテンツを暗号化する場合にのみ、このチェックボックスをオンにします。ネットワーク共有がネットワーク内部にあり、サードパーティ製のツールによって既にセキュリティで保護されているエンタープライズ環境では、共有上のファイルを暗号化しないことをお勧めします。この設定はメタデータに関連しません。標準ゾーンのメタデータは暗号化されません。この追加のセキュリティは、必要に応じて最大限のセキュリティを確保するためのオプションとして提供されますが、共有上のファイルを暗号化すると、ウイルス対策スキャナーやファイラーツール (データ重複除外ツールなど) などのサードパーティツールではディスクが読み取れなくなります。ShareFile は、ファイル暗号化キーを使用してダウンロードリクエストの有効性を確認し、ストレージを暗号化します。
パスフレーズ	ファイル暗号化キーを保護するために使用されるフレーズ。パスフレーズは 6 文字以上である必要があります。パスフレーズと暗号化キーは、安全な場所にアーカイブしてください。ゾーン内の各ストレージゾーンコントローラー に同じパスフレーズを使用する必要があります。パスフレーズはアカウントのパスワードと同じではなく、紛失した場合は復元できません。パスフレーズを紛失した場合、ストレージゾーンを再インストールしたり、ストレージゾーンに追加のストレージゾーンコントローラーをストレージゾーンに追加したり、サーバーに障害が発生した場合にストレージゾーンを回復したりすることはできません。注: 暗号化キーは、共有ストレージパスのルートに表示されます。暗号化キーファイル SCKeys.txt が失われると、すべてのストレージゾーンファイルへのアクセスが直ちに切断されます。通常のデータセンター手順の一部として、暗号化キーファイルを必ずバックアップしてください。

共有キャッシュの構成設定

オプション	説明
共有キャッシュの場所	ストレージキャッシュと、暗号化キー、キューに格納されたファイル、その他の一時アイテムなどのデータを格納するネットワーク共有へのパス。`\\server\share`形式でパスを指定します。同じストレージゾーンに属するストレージゾーンコントローラーは、同じファイル共有をストレージに使用する必要があります。注意: ストレージゾーンコントローラーは、このパスのデータを独自のストレージ形式で上書きします。ファイルデータのある場所へのパスを指定しないでください。このストレージ場所は、ShareFile データ専用のストレージゾーン用に予約します。ネットワークサービスアカウント (または ShareFile Management サービスを実行するように構成されているアカウント) には、この保存場所へのフルアクセス権が必要です。
共有キャッシュログオンと共有キャッシュパスワード	共有キャッシュの場所の UNC パスの資格情報。
暗号化を有効にする	共有キャッシュに格納されているファイルを暗号化するには、このチェックボックスをオンにします。

Windows Azure ストレージコンテナの設定

オプション	説明
ストレージリポジトリ	Azure ストレージコンテナを選択します。ゾーンの作成後、[ストレージリポジトリ] オプションを変更することはできません。たとえば、ローカルネットワーク共有から Azure ベースのストレージに切り替えるには、新しいゾーンを作成する必要があります。
アカウント名	Azure ストレージアカウントの名前。これらの名前は、常に小文字です。
アクセスキー	Azure ストレージのプライマリアクセスキーまたはセカンダリアクセスキー。Windows Azure 管理ポータルの [アクセスキーの管理] 画面からキーをコピーします。
検証	Azure アクセスキーを検証するには、ボタンをクリックします。検証が完了し、[Container Name] メニューに指定されたアカウントで使用可能なすべてのコンテナが表示されるまで、構成を続行することはできません。

オプション	説明
コンテナ名	このストレージゾーンのすべてのストレージゾーンコントローラーに使用する Azure コンテナーを選択します。Azure アクセスキーが検証されるまで、この一覧は空です。

Amazon S3 ストレージバケットの設定

オプション	説明
ストレージリポジトリ	Amazon S3 ストレージバケットを選択します。ゾーンの作成後、[ストレージリポジトリ] オプションを変更することはできません。たとえば、ローカルネットワーク共有から Amazon S3 ストレージに切り替えるには、新しいゾーンを作成する必要があります。
アクセスキー ID	Amazon S3 ストレージのアクセスキー ID。
シークレットアクセスキー	Amazon S3 ストレージのシークレットアクセスキー。
検証	ボタンをクリックして、Amazon S3 シークレットアクセスキーを検証します。検証が完了し、[Bucket Name] メニューに指定されたアカウントで使用可能なすべてのバケットが表示されるまで、設定を続行することはできません。
バケット名	このストレージゾーンのすべてのストレージゾーンコントローラーに使用する Amazon S3 バケットを選択します。Amazon S3 シークレットアクセスキーが検証されるまで、このリストは空です。

SMTP 設定

オプション	説明
SMTP サーバのアドレスと SMTP ポート番号	ローカル SMTP サーバのホスト名とポート。
SSL を使用する	安全な接続で SMTP サーバーに接続するには、このチェックボックスをオンにします。
ユーザー名とパスワード	ローカル SMTP サーバのユーザ名とパスワード。

オプション	説明
認証モード	デフォルト認証モードでは、ストレージゾーンコントローラから SMTP サーバへの接続に使用できる最も安全な方法が使用されます。
送信者アドレス	差出人フィールドに表示される電子メールアドレス。

グーグルクラウドプラットフォーム

Google Cloud Platform > [設定**] > [**相互運用性] から、アクセスキーとシークレットを生成します。

ストレージゾーンの構成を実行する前に、**S3EndpointAddress** レジストリ値を`https://storage.googleapis.com`に設定し、IIS を再起動します。

オプション 1

説明

ストレージリポジトリ

Amazon S3 ストレージバケットを選択します。ゾーンの作成後、[ストレージリポジトリ] オプションを変更することはできません。たとえば、ローカルネットワーク共有から Amazon S3 ストレージに切り替えるには、新しいゾーンを作成する必要があります。

アクセスキー ID

Google Cloud Platform ストレージからのアクセスキー ID。

シークレットアクセスキー

Google Cloud Platform ストレージからの秘密。

検証

ボタンをクリックして Google Cloud Platform シークレットアクセスキーを確認します。検証が完了し、指定したアカウントで使用可能なすべてのバケットが **[Bucket Name**] リストに表示されるまで、設定を続行することはできません。

バケット名

このストレージゾーンのすべてのストレージゾーン Controller に使用する正しいバケットを選択してください。Google Cloud Platform シークレットアクセスキーが検証されるまで、このリストは空になります。

ストレージゾーンコネクタの構成

ストレージゾーンコネクタにより、ユーザーは SharePoint サイトまたは指定されたネットワークファイル共有上のドキュメントにアクセスできます。ストレージゾーンコネクタを使用するために、ShareFile Data のストレージゾ

ーンを有効にする必要はありません。

> 注:
>
> ShareFile Data のストレージゾーンおよびストレージゾーンコネクタ機能は、ゾーンを共有できます。ただし、ストレージゾーン Controller は 2 つのデータタイプのデータとアクセスルールを別々に保持します。

ストレージゾーンコネクタは、ストレージゾーンコントローラーウィザードまたはストレージゾーンコントローラーコンソールを使用してゾーンを作成するときに構成できます。

特定のネットワークファイル共有または SharePoint ドキュメントライブラリへのアクセスを制御するには、[許可されたパス] または [拒否されたパス] の一覧を指定します。変更を保存したら、IIS サーバーを再起動します。

ストレージゾーンコネクタへのインバウンド接続は、最初に許可されたパスと照合されます。接続が許可されている場合、パスは拒否されたパスに対してチェックされます。たとえば、`\\myserver\teamshare`とそのすべてのサブフォルダにアクセスできるようにするには、許可パスを`\\myserver\teamshare`に指定します。

- デフォルトでは、すべての接続が許可され、[許可されたパス] の値で示されます。この値は拒否されたパスには無効です。
- 許可されたパスと拒否されたパスが互いに競合する場合は、最も制限の厳しいパスが適用されます。
- エントリはカンマで区切ります。
- ネットワークファイル共有へのコネクタで、許可される UNC パスを指定します。

  FQDN の例: `\\fileserver.acme.com\shared`

  UNC パスでは、次の変数を使用できます。

  - %UserName%

    ユーザーのホームディレクトリにリダイレクトします。パスの例: `\\myserver\homedirs\\%UserName%`

  - %HomeDrive%

    Active Directory プロパティの [ホームディレクトリ] で定義されているユーザーのホームフォルダーパスにリダイレクトします。パスの例: %`HomeDrive`%

  - %TSHomeDrive%

    Active Directory プロパティ ms-TS-Home-Directory で定義されているように、ユーザーのターミナルサービスのホームディレクトリにリダイレクトします。この場所は、ユーザーがターミナルサーバーまたは Citrix XenApp サーバーから Windows にログオンするときに使用されます。パスの例:%TSHomeDrive%

    Active Directory ユーザーとコンピュータスナップインでは、ユーザーオブジェクトの編集時に [リモートデスクトップサービスプロファイル] タブで MS-TS-Home-Directory 値にアクセスできます。

  - %UserDomain%

    認証されたユーザーの NetBIOS ドメイン名にリダイレクトします。たとえば、認証されたユーザーのログオン名が「abc\johnd」の場合、変数は「abc」に置き換えられます。パスの例: `\\myserver%UserDomain%_%UserName%`

変数は大文字と小文字を区別しません。

- ルートレベルの SharePoint サイトへのコネクタの場合、ルートレベルのパスを指定します。

  例: `https://sharepoint.company.com`

- SharePoint サイトコレクションへのコネクタの場合:

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

- SharePoint 2010 ドキュメントライブラリへのコネクタの場合は、URL を指定します (file.aspx や /Forms など)。

  例:

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

  デフォルトの SharePoint 2013 URL (最小ダウンロード戦略が有効になっている場合) の形式は次のとおりです: `https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`。

サーバーヘッダーを削除するためのセキュリティ推奨

デフォルトでは、IIS/ASP.NET は、HTTP 応答でサーバーヘッダーを公開します。このヘッダーは攻撃者に役立つ可能性があります。ヘッダーは、送信サーバーの種類と、場合によってはバージョン番号を表示します。このヘッダーは、実稼働サイトでは不要で、無効にすることができます。

残念ながら、ストレージゾーンの Controller インストーラーはこのヘッダーを自動的に削除できません。ただし、ストレージゾーンコントローラーのドキュメント/インストールガイドでは、このヘッダーを削除するようお客様に推奨できます。

ドキュメントに記載すべき具体的な手順については、次の記事を参照してください。`https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/`

Storage Zone Controller のセットアップを確認する

April 27, 2021

Storage Zone Controller が ShareFile に登録されていることを確認し、続行する前に他の構成の問題がないか確認してください。

1. Storage Zone Controller コンソールで、[**Monitoring**] タブをクリックします。
2. [ハートビートステータス] に緑色のチェックマークが付いていることを確認します。

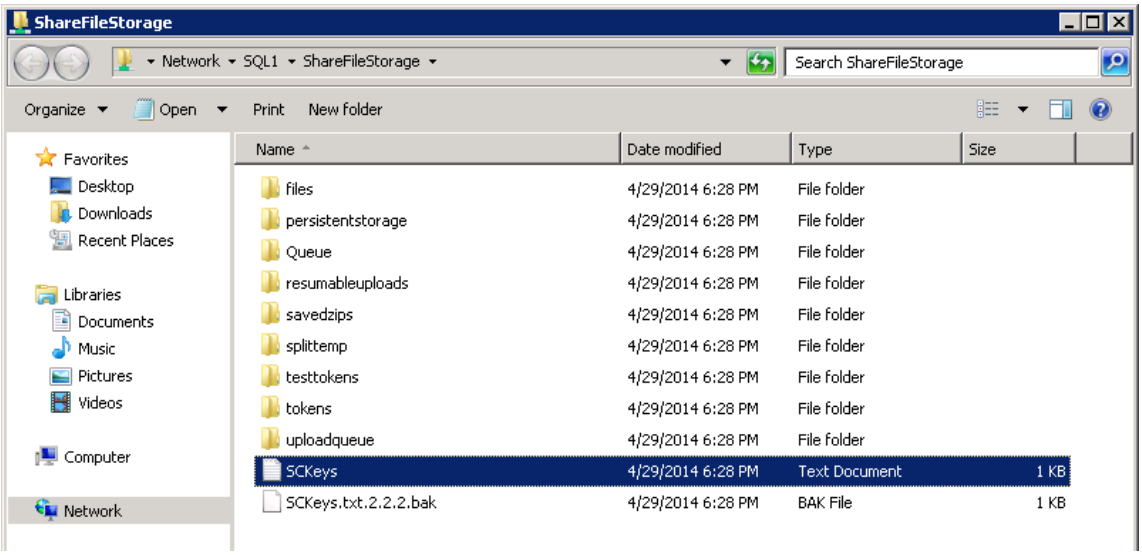
   赤いアイコンは、ShareFile.com がハートビートメッセージを受信していないことを示します。この場合は、Storage Zone Controller から www.ShareFile.com へのネットワーク接続と、外部の PC から Storage Zone Controller の URL へのネットワーク接続を確認します。標準ゾーンの場合、Storage Zone Controller は、有効な信頼できるパブリック SSL 証明書を使用してポート 443 でアクセス可能である必要があります。

   アップグレード後、ファイルクリーンアップサービスからの ShareFile Connectivity ステータスに、一時的に赤いアイコンが表示されることがあります。これは、Storage Zone Controller がネットワーク接続を確立する前に、Windows がそのサービスを開始した場合に発生します。コントローラサーバがネットワークに戻ると、ステータスは緑色のアイコンに戻ります。

3. プライベートゾーンへの接続を確認する: プライベートゾーンの外部 URL (`https://server.subdomain.com`の形式) に移動します。

   インターネットトラフィックが Storage Zone Controller との間で送受信される場合は、ShareFile ロゴが表示されます。Storage Zone Controller が正しく構成されていない場合、IIS ロゴまたは Citrix ADC ログオン画面が表示されることがあります。受信および送信方向の HTTPS トラフィックがポート 443 で許可されていることを確認します。外部 URL が Citrix ADC を指している場合は、コンテンツの切り替えと負荷分散仮想サーバーのデータのヒットを探します。詳しくは、インストールと設定のトラブルシューティングの「Storage Zone Controller が ShareFile にデータをアップロードしない」を参照してください。

4. プライベートデータストレージ用に作成したネットワーク共有に、フォルダー構造と SCKeys.txt などの Storage Zone Controller によって作成されたいくつかのファイルがあることを確認します。これらのファイルは、共有ストレージのルートフォルダーに存在する必要があります。



SCKeys.txt は、資格情報またはアクセス権の問題がない限り、Storage Zone Controller がインストールされたときに作成されます。SCKeys.txt が存在しない場合は、ファイル共有のアクセス制御リストを確認し、Storage Zone Controller を再インストールします。

5. ShareFile インタフェースからストレージゾーンコネクタのステータスを確認します。

   a) ShareFile Enterprise アカウントにログオンし、［管理者］**>**［ストレージゾーン］の順に選択し、［健全性］列に緑色のチェックマークが表示されていることを確認します。

   b) サイト名をクリックし、Storage Zone Controller が応答していることを示すハートビートメッセージを確認します。

6. ファイルアップロードのテスト：ShareFile Web インターフェイスにログオンし、構成したゾーンに割り当てられた共有フォルダを作成し、そのフォルダにファイルをアップロードして、ファイルがフォルダ内に表示されることを確認します。

ユーザーアカウントのデフォルトゾーンを変更する

March 20, 2024

デフォルトでは、既存のユーザーアカウントと新しくプロビジョニングされたユーザーアカウントは、ShareFile 管理のクラウドストレージをデフォルトゾーンとして使用します。デフォルトゾーンを次のように変更します。

- AD からプロビジョニングされたユーザーアカウントのデフォルトゾーンを指定するには、ユーザーのプロビジョニング中に、ストレージの場所を選択します。詳しくは、ShareFile ポリシーベースの管理記事の「ユーザールールオプションの編集」を参照してください。
- 個々のユーザーのデフォルトゾーンを変更するには、ShareFile 管理コンソールを開き、ユーザーの管理に移動します。

ストレージゾーンのプロキシサーバーを指定する

April 27, 2021

Storage Zone Controller コンソールでは、Storage Zone Controller のプロキシサーバーを指定できます。プロキシサーバーは他の方法で指定することもできます。

プライマリ Storage Zone Controller とセカンダリ Storage Zone Controller は HTTP を使用して相互に通信します。すべての HTTP トラフィックが、内部サーバーへの接続をサポートしていない送信プロキシサーバーを通過するように構成されている場合、次の手順で説明するように、プロキシサーバーをバイパスするようにプライマリとセカンダリの両方の Storage Zone Controller を構成して、プロキシサーバーが相互に通信できるようにする必要があります。

> 重要:
>
> バイパスリストの設定は、最新の Storage Zone Controller リリースでのみ表示されます。StorageZones Controller 2.2～2.2 を使用している場合は、Web.configの説明に従って、各セカンダリサーバーのバイパスリストを Web.config に手動で追加する必要があります。

1. Storage Zone Controller コンソールで（`http://localhost/configservice/login.aspx`）で、［**Monitoring**］タブをクリックします。

   > 注:
   >
   > ストレージゾーンコントローラ 5.11.17 を使用している場合は、プロキシを変更するには認証が必要です。プロンプトが表示されたら、アカウントのメールアドレス、パスワード、フルアカウント URL の FQDN サブドメイン (サブドメイン.sharefile.com、サブドメイン.sharefile.eu など) を入力します。［ログオン］をクリックします。

2. [Enable Proxy] チェックボックスをオンにし、プロキシサーバのアドレスとポートを入力します。
3. 認証モードを選択し、ShareFile プロキシアクセス用に指定された Windows アカウントを指定します。
4. サイトがすべての送信 HTTP トラフィックをプロキシし、ゾーンに複数の Storage Zone Controller がある場合は、バイパス設定を構成します。
   - すべての Storage Zone Controller トラフィックが同じサブネット上にある場合は、コントローラーが相互に通信できるように、［プロキシサーバーをバイパス］チェックボックスをオンにします。
   - Storage Zone Controller が異なるサブネット上にある場合は、「バイパスアドレス」にプライマリ Storage Zone Controller ホスト名または IP アドレスを入力します。
5. すべてのゾーンメンバーの IIS サーバーを再起動します。

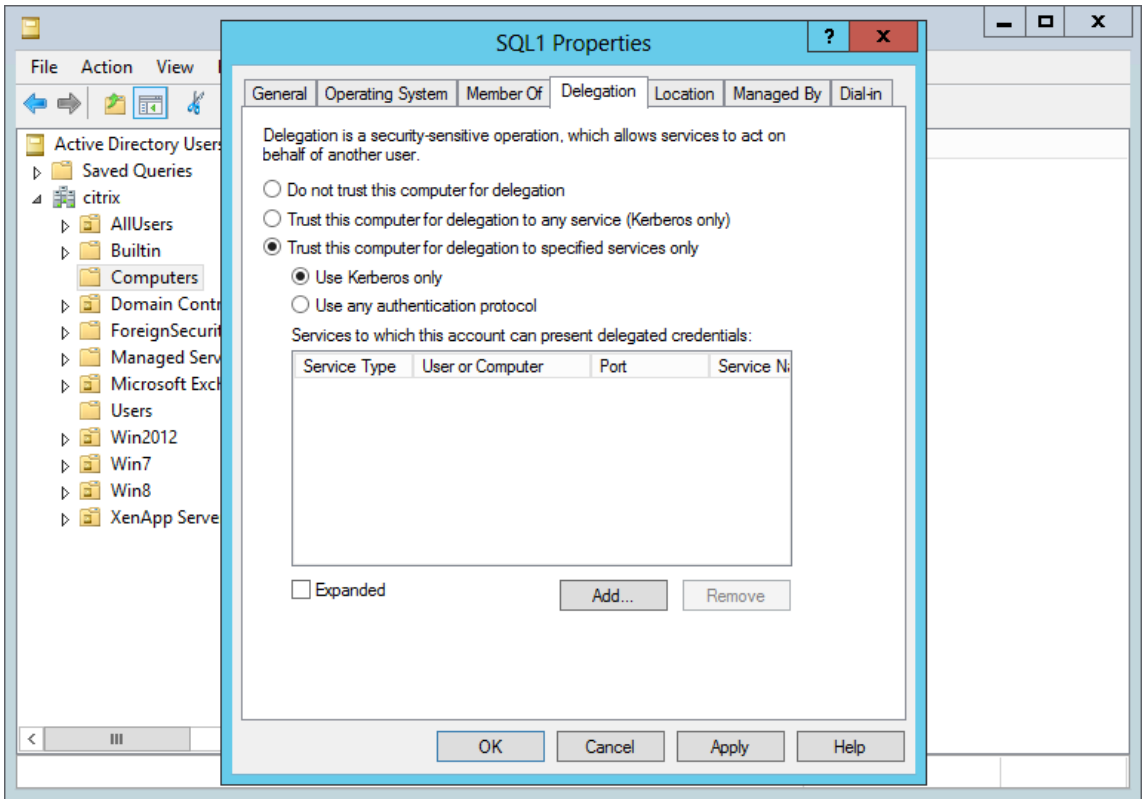
委任のために **Storage Zone Controller** を信頼するようにドメインコントローラーを構成する

April 27, 2021

> 注:
>
> このセクションは、ストレージゾーンコネクタにのみ適用されます。

ネットワーク共有または SharePoint サイトで NTLM または Kerberos 認証をサポートするには、ドメインコントローラーを次のように構成します。

1. ストレージゾーンドメインのドメインコントローラで、[スタート]、[管理ツール]、**[Active Directory** ユーザーとコンピューター] の順にクリックします。
2. ドメインを展開し、[コンピュータ] フォルダを展開します。
3. 右側のペインで、Storage Zone Controller 名を右クリックし、[プロパティ] を選択し、[委任] タブをクリックします。
4. [Kerberos] で、[このコンピュータを特定のサービスへの委任にのみ信頼する] を選択します。



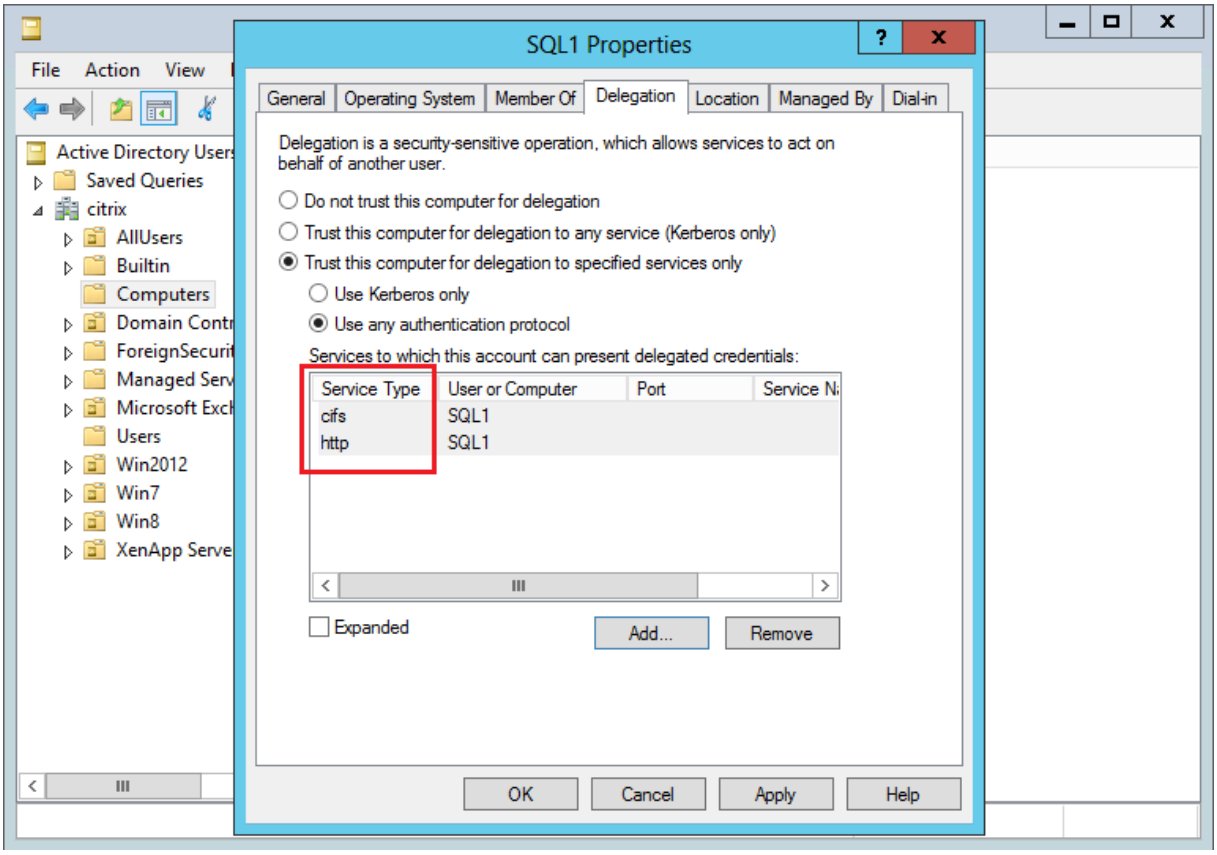
5. NTLM の場合:

a) [指定したサービスへの委任にのみこのコンピュータを信頼する] と [任意の認証プロトコルを使用する] を選択します。[**OK**] をクリックします。

b) [追加] をクリックします。[サービスの追加] ダイアログボックスで、[ユーザー] または [コンピューター] をクリックし、ネットワーク共有または SharePoint サーバーのホスト名を参照または入力します。[**OK**] をクリックします。

複数のファイルサーバーまたは SharePoint サーバーがある場合は、それぞれにサービスを追加します。

c) [利用可能なサービス] の一覧で、[CIFS] (ネットワークファイル共有用のコネクタ) と [HTTP] (SharePoint 用のコネクタ) の [使用するサービス] を選択します。[OK] をクリックします。



Web アプリのプレビュー、サムネイル、および表示のみの共有用にストレージゾーンコントローラーを設定

March 20, 2024

オンプレミスのファイルプレビューは、オンプレミスの Microsoft Office Web アプリ (OWA) サーバーによってレンダリングされます。Citrix 管理ストレージゾーンに格納されているファイルをプレビューすると、Citrix 管理または Microsoft が管理する OWA サーバーによってプレビューがレンダリングされます。

> 重要:
>
> ホワイトリスト登録要件:
>
> バージョン 5.0 以降のストレージゾーンで正しく機能するには、プレビューと編集を行うために`*.sf-api.com`が Office Online Server からアクセスできる必要があります。

要件

オンプレミスのファイルプレビューでサポートされているファイルタイプ

- doc、.docm、.docx、.dot、.dotm、.dotx、.odt
- .ods、.xls、.xlsb、.xlsm、.xlsx
- .odp, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx
- .pdf
- 画像ファイル (bmp, GIF, jpg, jpeg, png, tif, TIF)

オンプレミスのファイル編集でサポートされているファイルの種類

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

サポートされる環境

- 標準ゾーン
- マルチテナントゾーン
- Web アプリケーション

ホワイトリスト/ネットワークに関する考慮事項

- OOS サーバーは **`https://\*.sf-api.com`** (または**.eu**) に到達できるはずです
- SZC サーバーは、**`https://\*.sf-api.com`** と **`https://\*.sharefile.com`** (または**.eu**) に到達できるはずです。
- SZC サーバが OOS サーバに到達できる必要があります **`https://\<Customer OOS / OWA Endpoint\>/hosting/discovery`** (例: `https://oos.sharefileexample.com/hosting/discovery`)

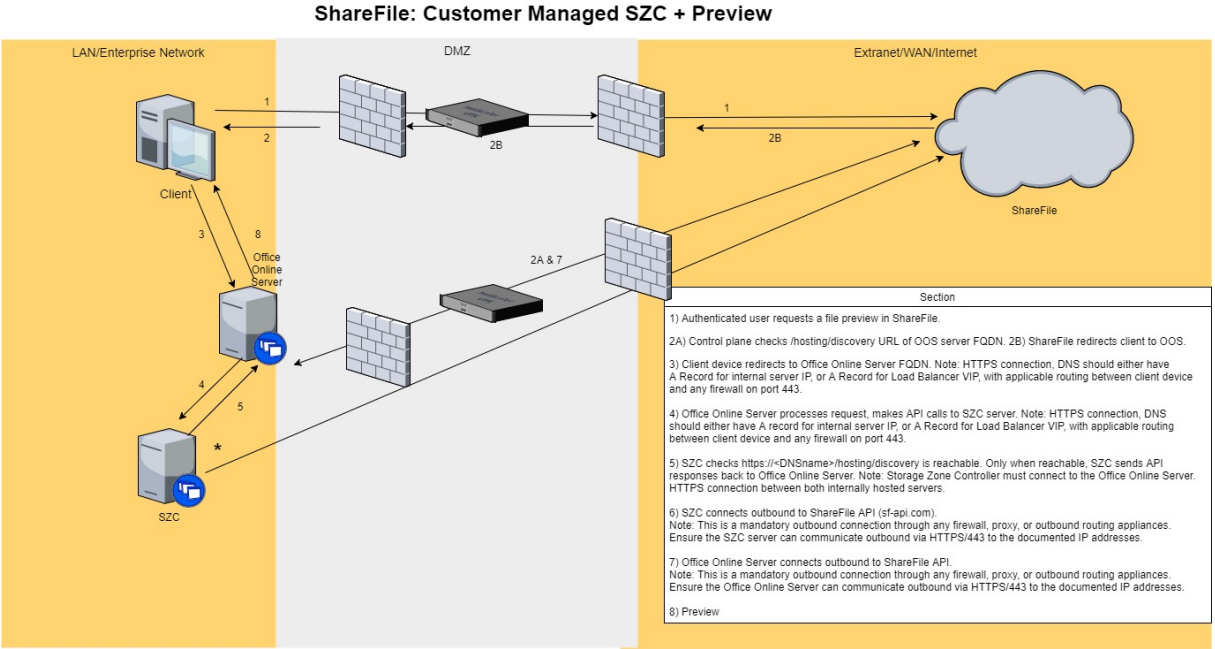
オンプレミスのファイルを編集するには、ShareFile アカウントでファイルバージョン管理を有効にする必要があります 。

ShareFile Web App の [詳細設定] メニューの [Microsoft Office オンライン編集] をオンにする設定は、オンプレミスのファイルを編集する機能には影響しません。この特定の切り替えは、オンプレミスのファイルを編集する機能を制御しませんが、パブリッククラウドに保存されているファイルの編集に適用されます。オンプレミスファイルの編集を有効にするかどうかは、以下に概説する手順を使用して、ストレージゾーンの Controller Admin が独占的に制御します。

Microsoft サーバー互換性

- **Microsoft Server 2016**: ファイルの編集とプレビューの両方の機能をサポートしています。編集を無効にすることもできます。
- **Microsoft Server 2013**: ファイルのプレビュー機能のみをサポートしています。

アーキテクチャとネットワークダイアグラム



1. 認証されたユーザーは、ShareFile でファイルのプレビューを要求します。
2. ShareFile は、Office オンラインサーバー FQDN を使用してクライアントデバイスにリダイレクトを発行します。
3. クライアントデバイスが Office オンラインサーバー FQDN にリダイレクトされます。

> **注:**
>
> HTTPS 接続の場合、DNS には内部サーバー IP 用の A レコードまたはロードバランサー VIP 用の A レコードがあり、クライアントデバイスとポート 443 上のファイアウォール間の適切なルーティングが必

> 要です。

4. Office Online サーバーは要求を処理し、ストレージゾーンコントローラーサーバーに API 呼び出しを行います。

> **注:**
>
> HTTPS 接続、DNS には、クライアントデバイスとポート 443 のファイアウォール間の適切なルーティングを含む、内部サーバー IP 用の A レコードまたはロードバランサー VIP 用の A レコードが必要です。

5. ストレージゾーンのコントローラーは`https://\<DNSname\>/hosting/discovery`がアクセスできるかチェックします。到達可能な場合にのみ、SZC は API 応答を Office オンラインサーバーに送り返します。

> **注:**
>
> ストレージゾーンコントローラは Office Online サーバーに接続する必要があります。内部でホストされている両方のサーバー間の HTTPS 接続。

6. ストレージゾーンコントローラーはアウトバウンドを ShareFile API (sf-api.com) に接続します。

> **注:**
>
> これは、ファイアウォール、プロキシ、またはアウトバウンドルーティングアプライアンスを介した必須のアウトバウンド接続です。ストレージゾーン Controller サーバーが、上記のドキュメント化された IP アドレスに HTTPS/443 経由でアウトバウンド通信できることを確認します。

7. Office オンラインサーバーは、送信を ShareFile API に接続します。

> **注:**
>
> これは、ファイアウォール、プロキシ、またはアウトバウンドルーティングアプライアンスを介した必須のアウトバウンド接続です。Office オンラインサーバーが HTTPS または 443 経由で上記のドキュメント化された IP アドレスに送信通信できることを確認します。

8. プレビューが発生します。

ストレージゾーンコントローラが、コンテンツをダウンロードするために ShareFile コントロールプレーンを呼び出して OOS ではなく OOS にファイルバイトをストリームするようにするには、ストレージゾーンコントローラのいずれかの設定ファイルのキーを更新する必要があります。

C:\inetpub\wwwroot\Citrix\StorageCenter\WopiServer\AppSettingsReleaseOnPrem.config を更新する必要があります。

この設定ファイルには DownloadFileFromSc というキーがありますが、現在は **false** になっています。キーを **true** に変更し、IIS を再起動します。

これにより、設定が更新されます。また、ファイルの内容をダウンロードするために ShareFile コントロールプレーンを呼び出さなくなります。

このオプションを使用する場合、コントロールプレーンから OOS へのインバウンドトラフィックは発生しないと言ってもよろしいでしょうか。

上記のオプションを使用すると、OOS は ShareFile コントロールプレーンへのアウトバウンド接続を行わなくなります。

ただし、ShareFile コントロールプレーンは、上記のオプションを使用するかどうかにかかわらず、引き続き OOS へのアウトバウンド接続を行います。

1 つの方法と他方の方法を使用するには長所と短所がありますか?

この方法では、OOS はファイルの内容を直接ダウンロードしません。ストレージゾーンコントローラは、ファイルバイトをダウンロードして OOS にストリーミングします。したがって、ストレージゾーンの Controller サーバーの負荷が増加します。

ファイルバイトのダウンロードとストリーミングは、リソースを大量に消費するタスクです。ユーザー数とプレビューおよび編集操作の数によっては、ストレージゾーンの Controller サーバーの負荷が増加します。

オンプレミスのプレビューと編集を有効にする

ブラウザー内でのドキュメントと画像のプレビュー、サムネイル、顧客管理のストレージゾーンに保存されているデータの表示専用共有、およびオンプレミスのファイル編集をサポートするには、ストレージゾーンコントローラーを次のように構成します:

1. ストレージゾーン Controller コンソールで、**ShareFile Data** タブをクリックします。
2. [ローカルネットワーク共有の構成] セクションで、[**Office Web** アプリのプレビューを構成する] を有効にします。
3. Microsoft Office Web アプリ (OWA) サーバーの外部 URL を入力します。
   - ユーザーは、Microsoft Office MSDN サブスクリプションを使用して OWA サーバーソフトウェアをダウンロードして構成する必要があります。
4. [**Office** オンライン編集を有効にする] を選択します (必要な場合)
5. OWA URL が外部からアクセス可能であることを確認します。
6. Office Online サーバーが`*.sf-api.com`と通信できることを確認します。
7. ストレージゾーンの Controller コンソールで、モニタリングタブをクリックします。
8. **OWA** サーバー接続に緑色のチェックマークが付いていることを確認します。

> 注:
>
> オンプレミスのファイルを編集するには、ShareFile アカウントのファイルバージョン管理を有効にす

> る必要があります 。アカウントのファイルのバージョン管理が無効になっている場合、オンプレミスの編集は機能しません。

重要:

クロック同期の設定:

- Storage Zone Controller の時刻が time.windows.com または別の NTP サーバーと同期されていることを確認します。クロック同期の設定については、ここをクリックしてください。

OWA URAL の変更またはプレビューの無効化:

- 上記のいずれかの操作では、プライマリおよびセカンダリコントローラごとに IIS サービスを再起動する必要があります。

制限事項

- モバイルアプリは、ブラウザー内での編集をサポートしていません。
- コネクタはブラウザ内プレビューをサポートしていません。

WOPI プレビューは、VDR アカウントではサポートされていません。

Citrix ADC を表示専用共有用に構成する方法については、「[ストレージゾーン Controller 用の Citrix ADC の構成]」を参照してください。(/en-us/storage-zones-controller/5-0/install/configure-netscaler.html)

OWA および **OOS** の問題のトラブルシューティング

オンプレミスのファイルのプレビューまたは編集で問題が発生した場合は、次の手順で特定の問題の識別と修正に役立ちます。

構成のトラブルシューティングを行うには、まず OWA または OOS マシンにサインインします。

1. Office WebApps または OfficeOnline Windows サービスが services.msc 内で実行されていることを確認します。
2. 新しいブラウザで、`http://localhost/hosting/discovery` ページを開きます。このページが正常にロードされた場合は、XML 応答が返されます。
3. PowerShell を管理者として実行し、次のコマンドを実行します。

```
Get-OfficeWebAppsFarm
```

応答に WARNING または ERROR メッセージが表示された場合は、構成設定を確認し、エラーまたは間違いがないかどうかを確認します。

ネットワークに関する考慮事項:

- OOS サーバーは **https://*.sf-api.com** (または**.eu**) に到達できるはずです
- SZC サーバーは、**https://*.sf-api.com** と **https://*.sharefile.com** (または**.eu**) に到達できるはずです。
- SZC サーバーは OOS サーバー**https://<CustomerOOS/OWAEndpoint\>/hosting/discovery**にアクセスできるはずです。例: https://oos.sharefileexample.com/hosting/discovery。

マルチテナントストレージゾーンの構成

March 20, 2024

マルチテナントストレージゾーンは、Citrix サービスプロバイダー（CSP）がすべてのテナントで共有される単一のストレージゾーンを作成および管理できるようにする ShareFile ストレージゾーンコントローラー機能です。

ShareFile によってプロビジョニングされたパートナーアカウントを持つ CSP の場合は、無制限数のテナントをサポートする 1 つのマルチテナントの標準ストレージゾーンをドメイン上にホストできます。マルチテナントゾーンを使用すると、次のことが可能になります。

- 各テナントに固有の ShareFile アカウントを提供し、カスタムブランディング、ファイル保持の設定、セキュリティ設定など、優れた ShareFile 機能をすべて活用できます。
- すべてのテナントに対して 1 つのストレージリポジトリを維持します。
- 新規のお客様への導入を迅速に行い、お客様のアカウントごとに個別のストレージゾーンを作成する際のコストと管理の複雑さを軽減します。

パートナーアカウントを作成する

マルチテナントストレージゾーンを登録するには、パートナーアカウントが必要です。

パートナーアカウントを作成するには、CSP プログラムに登録し、ShareFile をサービスとして提供する権利が与えられる、希望のディストリビューターにストッキング SKU を注文する必要があります。

すでに CSP として登録されており、SKU を保管する CSP に適切な ShareFile を注文している場合は、パートナーアカウントはすでに作成されています。< acctsvcs@sharefile.com > この新しいパートナーアカウントが見つからない場合は、ShareFile アカウントサービスにお問い合わせください。

CSP ShareFile オファリングで顧客アカウントのプロビジョニングを開始するときは、パートナーアカウントに汎用サービスアカウント管理者ユーザーを作成することをお勧めします。このようにして、管理者ユーザーは、すべての顧客アカウントの公式パートナー管理者になることができます。このサービスアカウント管理者ユーザーに、テナントの管理権限が有効になっていることを確認します。これにより、CSP カスタマーアカウントリクエストフォーム（ステップ 4）に記入する前に、パートナーがこのパートナー管理者を作成することをお勧めします。

マルチテナントストレージゾーンのインストールとセットアップ

- 新しいマルチテナントストレージゾーンを作成し、パートナーアカウントに関連付けます。詳細については、「ストレージゾーンコントローラーのインストールとストレージゾーンの作成」を参照してください。
- ストレージゾーンコントローラーをマルチテナントモードでインストールします。前の手順で説明した「インストール」の資料で、次の指定されたコマンドプロンプトを実行してください。

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

> 注:
>
> 上記のコマンドでは、インストールしようとしている msi の番号と一致するようにバージョン番号（この例では 5.0.1）を更新する必要がある場合があります。

新しいストレージゾーンを構成し、パートナーアカウントに関連付けます

詳細については、「ストレージゾーンコントローラーのインストールとストレージゾーンの作成」の手順 10 を参照してください。

新しいゾーンを登録するパートナーアカウントにログインします。

> 重要:
>
> このアカウントには、テナントの管理およびゾーンの作成と管理の ShareFile 権限が必要です。

これで、パートナーアカウントにログインして、新しいマルチテナントストレージゾーンを表示できます。[管理者設定] **>** [ストレージゾーン] **>** [パートナー管理] タブをクリックします。

マルチテナントゾーンのテナントアカウントの要求

テナントアカウントをリクエストするには、CSP カスタマーアカウントリクエストフォームに記入してください。

テナントアカウントを要求するときは、パートナー管理者ユーザーも指定する必要があります。このパートナー管理者は、テナントの管理権限が有効になっているパートナーアカウントの管理ユーザーである必要があります。テナントアカウントが作成されると、このパートナー管理者ユーザーは Admin ユーザーとしてアカウントに自動的にプロビジョニングされ、サインインしてテナントアカウントを管理できるようになります。1 つのアカウントに同じメールアドレスを持つユーザーが 2 人いることはできないため、フォームで指定されたパートナー管理者のメールアドレスを、同じフォームの顧客管理者のメールアドレスと同じにすることはできません。

ターンアラウンドを迅速に実行するには、テナントアカウントのストレージゾーンとして使用する正しい Org ID とマルチテナントゾーン名を指定してください。

シトリックスが要求されたアカウントをプロビジョニングすると、メールが届きます。電子メールには、テナントサブドメインの詳細と、アクセスをセットアップするためのアクティベーションリンクが含まれます。ShareFile は、あなたとあなたの顧客の管理ユーザーに別々のメールを送信します。

その後、顧客は ShareFile の使用を開始できます。テナントのアカウントにプロビジョニングされた新しいユーザーは、ユーザーのファイルの既定の場所として指定したマルチテナントゾーンを使用します。

Office オンラインサーバーで **Office** ファイルと **PDF** をプレビューする

この機能は、サポートされている Office オンラインサーバー環境でサポートされます。セットアップ情報については、ここをクリックしてください。

コネクタの共有

この機能は、マルチテナントゾーンでサポートされます。

テナントを管理する

パートナーアカウント内には、**[**管理者設定**] > [**詳細設定**]** にテナント管理ダッシュボードがあります。この一元化されたダッシュボードでは、パートナーアカウントにリンクされているすべてのテナントのステータスを確認できます。ダッシュボードには、各テナントのライセンス消費、既定のストレージゾーン、ストレージ使用量、およびアカウントの状態 (有料または試用版) が含まれます。

> 注:
>
> ダッシュボードは、テナントの管理ユーザー権限が有効になっているパートナーアカウント内のユーザーのみが使用できます。

マルチテナントの制限

ShareFile 情報権利管理機能 (IRM) は、マルチテナントストレージゾーンではサポートされていません。

トラブルシューティング

ゾーンの作成に失敗しました**:** 禁止されています

ストレージゾーンの登録時に、「ゾーンの作成に失敗しました: 禁止」というエラーが表示された場合は、ユーザーのアクセス許可に「テナントの管理」アクセス許可が含まれていることを確認します。

アップグレード

March 20, 2024

Storage Zones Controller 5.10 以降を最新バージョンにアップグレードする

> 注:
>
> ShareFile では、更新前にサーバーのスナップショットを取得し、ストレージゾーンサーバーの構成をバックアップすることをお勧めします。ストレージゾーン構成をバックアップする方法については、「プライマリ Storage Zones Controller 構成のバックアップ」を参照してください。Storage Zones Controller のアップグレードに関する問題については
>
> 、「ShareFile Storage Zone Controller のアップグレードのトラブルシューティング」を参照してください。

次の手順を使用して、Storage Zones Controller 5.10 をアップグレードします。

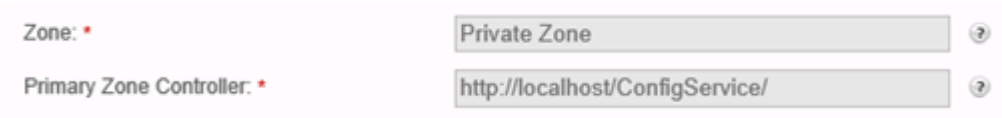
1. ShareFile ダウンロードページからストレージゾーンコントローラソフトウェアの最新バージョンをダウンロードします。

   > 注:
   >
   > アップグレードおよびサーバの再起動中は、Storage Zones Controller を使用できません。データの損失を避けるため、メンテナンスウィンドウをユーザーにスケジュールすることをお勧めします。アップグレード中は、ゾーンがファイル転送に使用できないことを知らせます。

2. Storage Zones Controller がインストールされている Windows サーバに MSI ファイルをインストールします。複数のサーバーがある場合は、更新プログラムを最初にプライマリサーバーにインストールし、次に他のサーバーにインストールする必要があります。どのサーバーがプライマリサーバーであるかを識別するには、次の 2 つの方法があります。

   a) ［構成］ページから、プライマリ Storage Zones Controller を特定します。

      - コントローラサーバで、[スタート] `http://localhost/configservice/login.aspx` メニューから設定ツールに移動するか、または開始します。構成にアクセスするには、「ゾーンの作成と管理」権限が必要です。
      - [データ] タブで、[プライマリゾーンコントローラ] フィールドを確認します。このフィールドには、`http://server/ConfigService`プライマリゾーンコントローラのサーバホスト名がとしてリストされます。

      `http://localhost/ConfigService`の localhost は、このサーバがプライマリゾーンコントローラであることを示しています。

   b) レジストリからプライマリ Storage Zones Controller を特定します。

      - コントローラーサーバーで、レジストリエディター (regedit.exe) を開きます。
      - レジストリキーを見つけます:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCente

- キーの値`isPrimaryConfigServer`が true であることを確認します。

3. プライマリ Storage Zones Controller でアップグレードを開始します。

   a) StorageCenter.msi を実行して、ShareFile Storage Zone Controller セットアップウィザードを起動します。

   b) プロンプトに応答します。インストールが完了すると、ウィザードに「Citrix ShareFile Storage Zone Controller セットアップウィザードが完了しました」というメッセージが表示されます。

   c) サーバーを再起動します:

4. 各セカンダリ Storage Zones Controller で (必要な場合):

   a) StorageCenter.msi を実行して、ShareFile Storage Zone Controller セットアップウィザードを起動します。

   b) プロンプトに応答し、[完了] を選択します。

   c) サーバーを再起動します:

5. すべての Storage Zones Controller で、すべてのゾーンメンバーの IIS サーバーを再起動します。

   a) CMD プロンプトを起動し、管理者として実行します。

   b) `iisreset`を入力し、**Enter** キーを押します。正常に終了すると、プロンプトに「インターネットサービスは正常に再起動しました」と表示されます。

   c) アップグレード後に、プライマリ Storage Zones Controller のレジストリ設定が正しいことを確認します。

6. アップグレードのインストール後、任意のゾーンメンバーで [Storage zones Configuration] ページを起動してログインし、構成設定を変更します。

   - Storage Zones Controller コンソールにいつでも戻るには、`http://localhost/configservice/login.aspx`を開きます。**[完了]** をクリックするか、Storage Zone Controller コンソールに戻ると、[ログオン] ページが開きます。

> **注:**
>
> Storage Zone Controller の設定ページにログインするには、アプリケーション固有のパスワードを使用する必要があることに注意してください。新しいアプリケーション固有のパスワードを作成する必要がある場合は、次のサポート記事を参照してください。アプリケーション固有のパスワードを作成する。

   - 表示された情報を変更するには、[修正] を選択して変更し、[保存] を選択します。

> 注:

> メンテナンスウィンドウを終了する前に、各 Storage Zones Controller へのデータ転送が機能していることを確認します。

ストレージゾーンコントローラーの管理

February 14, 2022

プライマリおよびセカンダリのストレージゾーンコントローラー をインストールしたら、次の手順に従ってコントローラを管理し、障害回復に備えます。

ストレージゾーンコントローラー コンソールを開くには、`http://localhost/configservice/login.aspx`にアクセスするか、[スタート] メニューから構成ツールを起動します。

ストレージゾーンコントローラー の管理

ストレージゾーンにセカンダリ **Storage Zone Controller** を統合する

April 27, 2021

ストレージゾーンを高可用性に構成するには、2 つ以上の Storage Zone Controller を接続します。そのためには、以下を行う必要があります。

1. プライマリ Storage Zone Controller をインストールし、ゾーンを作成します（Storage Zone Controller をインストールし、ストレージゾーンを作成するを参照）。
2. 2 台目のサーバーに Storage Zone Controller をインストールし、そのコントローラを同じゾーンに参加させます。

同じゾーンに属する **Storage Zone Controller** は、ストレージに同じファイル共有を使用する必要があります。

高可用性展開では、セカンダリサーバーは独立しており、完全に機能する Storage Zone Controller です。ストレージゾーン制御サブシステムは、アップロード、ダウンロード、コピー、削除などの操作要求を処理する Storage Zone Controller をランダムに選択します。

プライマリサーバがオフラインになった場合は、セカンダリサーバをプライマリサーバに簡単に昇格できます。また、サーバをプライマリからセカンダリに降格することもできます。

1. セカンダリ Storage Zone Controller になるサーバー上で Web ブラウザーを開きます。次に`http://localhost/configservice/login.aspx`を開き、ログオンします。
2. [既存のゾーンに参加] をクリックし、ストレージゾーンを選択します。
3. 必要な情報を入力し、[登録] をクリックします。

   プライマリゾーンコントローラーの場合は、ホスト名または IP アドレスのみを入力できます。ShareFile は完全な URL を入力します。URL をテストするには、ブラウザーのアドレスフィールドに入力します。URL が正しい場合は、ShareFile バナーページが表示されます。標準ゾーンの場合:URL が正しくない場合に https を指定した場合は、有効で信頼されたパブリック SSL 証明書を使用していることを確認します。
4. プライマリ Storage Zone Controller にプロキシサーバーを使用している場合は、ストレージゾーンのプロキシサーバーを指定するの説明に従って、セカンダリコントローラのプロキシサーバーを指定します。
5. すべてのゾーンメンバーの IIS サーバーを再起動します。

   セカンダリ Storage Zone Controller は、起動時にプライマリコントローラーの構成を継承します。

プライマリストレージゾーンコントローラー アドレスまたはパスフレーズの変更

February 14, 2022

> 注:
>
> アドレスまたはパスフレーズを変更できるのは、アカウント管理者のみです。

プライマリストレージゾーンコントローラー に別の外部アドレスまたはローカルアドレスを指定するには

この手順または他のサーバー管理ツールを使用して、プライマリストレージゾーンコントローラー の外部アドレスを変更できます。

1. プライマリストレージゾーンコントローラーサーバーで、[構成] ページを開くかhttp://localhost/configservice/login.aspxに移動します。
2. ShareFile 管理者の資格情報を使用して構成ページにログインします。
3. [データ] タブで [変更] を選択します。
4. 新しい外部アドレスまたはローカルアドレスを指定し、**[変更を保存]** を選択します。
5. すべてのゾーンメンバーに対して手順を繰り返します。
6. すべてのゾーンメンバーの IIS サーバーを再起動します。

プライマリストレージゾーンコントローラー のパスフレーズを変更するには

> 注:
>
> 現在のパスフレーズは、ストレージゾーンコントローラー のパスフレーズを変更するために必要です。

1. ストレージゾーンの構成ページを開きます: http://localhost/configservice/login.aspx
2. **[修正]** をクリックします。
3. ファイル暗号化キーを保護するために使用するパスフレーズを指定します。パスフレーズと暗号化キーは、安全な場所にアーカイブしてください。

   パスフレーズはアカウントのパスワードと同じではなく、紛失した場合は復元できません。パスフレーズを紛失した場合、ストレージゾーンを再インストールしたり、ストレージゾーンに追加のストレージゾーンコントローラーをストレージゾーンに追加したり、サーバーに障害が発生した場合にストレージゾーンを回復したりすることはできません。

   > 注:
   >
   > 暗号化キーは、共有ストレージパスのルートに表示されます。暗号化キーファイルを失うと、すべてのストレージゾーンファイルへのアクセスが直ちに切断されます。

4. プライマリサーバーでパスフレーズを変更した場合: 他の各メンバーのストレージゾーン設定ページにログオンし、プロンプトが表示されたらパスフレーズを入力します。

   ゾーン内の各ストレージゾーンコントローラー に同じパスフレーズを使用する必要があります。

5. すべてのゾーンメンバーの IIS サーバーを再起動します。

Storage Zone Controller を降格および昇格する

June 15, 2020

高可用性展開では、セカンダリサーバーは独立しており、完全に機能する Storage Zone Controller です。プライマリ Storage Zone Controller を維持または交換するには、まずコントローラを降格してから、セカンダリコントローラを昇格させます。プライマリサーバーがオフラインになった場合は、セカンダリサーバーをプライマリに昇格できます。

> 注意:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. プライマリ Storage Zone Controller を降格するには、次の手順に従います。
   a) レジストリキーを見つけます: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) isPrimaryConfigServer を false に設定します。
   c) PrimaryConfigServiceUrl を、`https://IPaddress` または `https://hostname/ConfigService/` の形式を使用して、新しいプライマリ Storage Zone Controller となるサーバーの URL に設定します。
   d) すべてのゾーンメンバーの IIS サーバーを再起動します。
2. セカンダリ Storage Zone Controller を昇格するには、次の手順に従います。
   a) レジストリキーを見つけます: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) isPrimaryConfigServer を true に設定します。
   c) PrimaryConfigServiceUrl を `http://localhost/ConfigService/` に設定します。
   d) すべてのゾーンメンバーの IIS サーバーを再起動します。
3. 追加のセカンダリ Storage Zone Controller をすべて変更します。
   a) レジストリキーを見つけます: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) PrimaryConfigServiceUrl を、`https://IPaddress` または `https://hostname/ConfigService/` の形式を使用して、新しいプライマリ Storage Zone Controller となるサーバの URL に設定します。
   c) すべてのゾーンメンバーの IIS サーバーを再起動します。

ストレージゾーンコントローラを無効化、削除、または再デプロイする

March 14, 2023

ストレージゾーンコントローラーを無効にするには

> 注:
>
> 各ストレージゾーンコントローラーの外部アドレスが異なる場合は、この手順を使用してください。すべてのストレージゾーンコントローラーに同じ外部アドレスを使用する場合は、Citrix ADC インターフェイスからコントローラーを無効にします。

メンテナンスのためにサーバーをオフラインにする前に、ストレージゾーンコントローラーを無効にします。

1. ShareFile Web インターフェイスで、［管理］をクリックし、［ストレージゾーン］をクリックします。
2. ゾーン名をクリックし、Storage Zone Controller のホスト名をクリックします。
3. [有効] チェックボックスをオフにし、[変更の保存] をクリックします。
4. すべてのゾーンメンバーの IIS サーバーを再起動します。

Storage Zone Controller を削除するには

Storage Zone Controller を削除しても、データまたは SCKeys.txt は削除されません。プライマリストレージゾーンコントローラを削除する場合は、続行する前に降格してください。

1. ShareFile Web インターフェイスで、［管理］をクリックし、［ストレージゾーン］をクリックします。
2. ゾーン名をクリックし、Storage Zone Controller のホスト名をクリックします。
3. ［削除］をクリックします。
4. すべてのゾーンメンバーの IIS サーバーを再起動します。

ストレージゾーンコントローラーを再デプロイするには

ストレージゾーンコントローラを再デプロイしても、情報は失われません。

1. サーバからストレージゾーンをアンインストールします。
2. ShareFile Web インターフェイスで、［管理］**>**［ストレージゾーン］の順にクリックし、ゾーンを選択します。ゾーンを削除しないでください。
3. ストレージゾーンコントローラーを選択して削除します。
4. ストレージゾーンをインストールします。まだ登録しないでください。
5. ストレージゾーンコントローラ設定ウィザードを実行して、ストレージゾーンコントローラをゾーンに参加させ、登録を完了します。
6. すべてのゾーンメンバーの IIS サーバーを再起動します。

新しいネットワーク共有にファイルを転送する

April 27, 2021

プライベートデータストレージ用に新しいネットワーク共有を設定する前に、次の手順を実行します。

要件

- 同じストレージゾーンに属する Storage Zone Controller は、ストレージに同じファイル共有を使用する必要があります。
- Storage Zone Controller は、IIS アカウントプールユーザーを使用して共有にアクセスします。既定では、アプリケーションプールは、低レベルのユーザー権限を持つ Network Service ユーザーアカウントで動作します。Storage Zone Controller は、デフォルトでネットワークサービスアカウントを使用します。
- ネットワークサービスアカウントには、この格納場所へのフルアクセス権が必要です。
- 新しい共有にデータを転送する前に、新しいアップロードのストレージゾーンコントローラーを無効にします。Web アプリケーションで、[管理者設定] > [**StorageZones**] に移動します。ゾーン名を選択します。[ストレージセンター] で、各ホストサーバを選択します。各ホストサーバへのトラフィックを終了するには、[サーバ設定] の [有効] オプションの選択を解除します。

1. ストレージゾーンの構成ページを開きます: `http://localhost/configservice/login.aspx`
2. [修正] をクリックします。
3. [ストレージの場所] で、ネットワーク共有への UNC パスをフォーム`\\server\share`に入力し、[保存] をクリックします。

   > 注意:
   >
   > Storage Zone Controller は、このパス内のデータを独自のストレージフォーマットで上書きします。ベストプラクティスとして、ファイルデータを含む場所へのパスを指定しないでください。このストレージ場所は、ShareFile データ専用のストレージゾーン用に予約します。

4. 新しいネットワーク共有の場所の UNC パスの資格情報が以前のものと異なる場合は、ストレージログオンとストレージパスワードを指定します。
5. すべてのゾーンメンバーの IIS サーバーを再起動します。
6. すべてのゾーンメンバーの構成ページにログインします。
7. SCKeys.txt を含むディレクトリ構造全体を新しいサーバーにコピーします。

プライマリ **Storage Zones Controller** 構成のバックアップ

June 28, 2023

Storage Zones Controller がローカルサイトにインストールされており、バックアップはユーザーが担当します。展開を完全に保護するには、Storage Zones Controller サーバーのスナップショットを作成し、設定をバックアップし、ファイル回復用に Storage Zones Controller を準備する必要があります。

このトピックの説明に従って、構成をバックアップすることが重要です。たとえば、バックアップがないときに、誰かが誤ってゾーンを削除した場合、そのゾーン内のフォルダーとファイルを回復することはできません。

> 重要:
>
> この手順では、必ず PowerShell 4.0 を使用してください。PowerShell の要件の詳細については、「Storage Zones Controller のシステム要件」の「PowerShell スクリプトとコマンド」を参照してください。

Storage Zones Controller インストーラーには、プライマリ Storage Zones Controller 構成設定をバックアップおよび回復するコマンドを含む PowerShell モジュールが含まれています。バックアップには、ゾーン、ShareFile データのストレージゾーン、SharePoint 用のストレージゾーンコネクタ、ネットワークファイル共有の記憶域ゾーンコネクタなどの構成情報が含まれます。

バックアップと復元コマンドでは、Storage Zones Controller と同じユーザーコンテキストで 32 ビットバージョンの PowerShell を実行する必要があります。ユーザーコンテキストを設定するには、ツール PSExec を使用します。このツールは、からダウンロードできます https://docs.microsoft.com/en-us/sysinternals/downloads/psexec。

> 注:
>
> この手順は、セカンダリ Storage Zones Controller には適用されません。セカンダリ Storage Zones Controller をリカバリするには、サーバーに Storage Zones Controller を再インストールし、サーバをプライマリ Storage Zones Controller に接続します。

1. この手順で使用する PowerShell スクリプトは署名されていないので、PowerShell 実行ポリシーを変更する必要があります。

   a) PowerShell 実行ポリシーで、署名のないローカルのスクリプトを実行できるかどうかを確認します: PS `C:\>Get-ExecutionPolicy`

      たとえば、RemoteSigned、Unrestricted、または Bypass のポリシーでは、署名されていないスクリプトを実行できます。

   b) PowerShell 実行ポリシーを変更するには:PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. この PowerShell セッションのユーザーコンテキストを設定します。コマンドウィンドウで、次のいずれかのコマンドを実行します。

- デフォルトのネットワークサービスアカウントを使用している場合:

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

- Storage Zones Controller アプリケーションプールに指定ユーザーを使用する場合:

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

PowerShell ウィンドウが開きます。

3. PowerShell プロンプトから、モジュール ConfigBR.dll をインポートします: `Import-Module C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll`

   新しい PowerShell ウィンドウを開くたびに、モジュールをインポートする必要があります。

4. PowerShell プロンプトから Get-SFConfig コマンドを実行し、次のプロンプトを完了します。

   - プライマリゾーンコントローラー -入力例:
     - ローカルサーバーへの接続: `http://localhost/ConfigService/`
     - リモートサーバーへの接続: `http[s]://myservername.domain.com/ConfigService/`
     - DNS の問題でサーバー名に接続できない場合は、リモートサーバーに接続します。`http[s]://10.40.37.5/ConfigService/`
   - パスフレーズ-Storage Zones Controller に指定されたパスフレーズ。
   - ファイルパス-例 `c:\szc-backup.bak`

   コマンドパラメータ:

パラメーター	説明	例
「サーバー」	プライマリ Storage Zones Controller サーバー名または IP アドレス。これは、[例] の下に示す次のいずれかの形式で、末尾にスラッシュを含める必要があります。	ローカルサーバーへの接続: `http://localhost/ConfigService/`; リモートサーバーへの接続: `http[s]://myservername.domain.com/ConfigService/`; DNS の問題によりサーバー名への接続が妨げられた場合にリモートサーバーに接続する: `http[s]://10.40.37.5/ConfigService/`
“passphrase”	Storage Zones Controller に指定されているパスフレーズ。	“MyPassphrase”
「フルパス」	バックアップファイルを保存する場所。	「c:\szc-backup.bak」

Get-SFConfig コマンドは、バックアップファイルを作成します。

プライマリ Storage Zones Controller 設定を復元するには、「プライマリ Storage Zones Controller 構成の復元」を参照してください

プライマリストレージゾーンコントローラー構成を回復する

February 14, 2022

> 重要:
>
> - この手順では、必ず PowerShell 4.0 を使用してください。PowerShell の要件について詳しくは、「ストレージゾーンコントローラー のシステム要件」の PowerShell スクリプトとコマンドを参照してください。
> - TLS をシステム全体に実装する方法の詳細については、Microsoft の記事「クライアントで TLS 1.2 を有効にする方法」を参照してください。

ストレージゾーンコントローラー には、プライマリストレージゾーンコントローラー が削除または障害が発生した場合の障害回復のための次のオプションがあります。

- セカンダリストレージゾーンコントローラー が使用可能な場合は、セカンダリコントローラをプライマリコントローラに昇格させます。

- セカンダリストレージゾーンコントローラー が使用できず、プライマリストレージゾーンコントローラー 構成 (「プライマリストレージゾーンコントローラー 構成のバックアップ」を参照) をバックアップした場合は、バックアップファイルからプライマリストレージゾーンコントローラー を回復します。
- プライマリストレージゾーンコントローラー 構成のバックアップがなく、すべてのストレージゾーンコントローラー が誤って削除されたり使用できなくなったりした場合は、部分的な回復しかできません。ShareFile Data 用のストレージゾーンのゾーンと構成はリカバリできますが、ストレージゾーンコネクタはリカバリできません。

プライマリストレージゾーンコントローラー をバックアップファイルから復元するには

> 注:
>
> これらの手順は、プライマリストレージゾーンコントローラー にのみ適用されます。セカンダリストレージゾーンコントローラをリカバリするには、ストレージゾーンコントローラー をサーバーに再インストールし、サーバをプライマリストレージゾーンコントローラに参加させます。

1. この手順で使用する PowerShell スクリプトは署名されていないため、PowerShell 実行ポリシーの変更が必要になる場合があります。

   a) PowerShell 実行ポリシーで、署名のないローカルのスクリプトを実行できるかどうかを確認します: PS `C:\>Get-ExecutionPolicy`

   たとえば、RemoteSigned、Unrestricted、または Bypass のポリシーでは、署名されていないスクリプトを実行できます。

   b) PowerShell 実行ポリシーを変更するには:PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. この PowerShell セッションのユーザーコンテキストを設定します。コマンドウィンドウで、次のいずれかのコマンドを実行します。

   > 注:
   >
   > https://docs.microsoft.com/en-us/sysinternals/downloads/psexecから PsExec.exe をダウンロードし、そのページのインストール手順に従います。

   - デフォルトのネットワークサービスアカウントを使用している場合:

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

   - ストレージゾーンコントローラー アプリケーションプールに指定ユーザーを使用する場合:

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

   PowerShell ウィンドウが開きます。

3. PowerShell プロンプトから、モジュール ConfigBR.dll をインポートします: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   新しい PowerShell ウィンドウを開くたびに、モジュールをインポートする必要があります。

4. PowerShell プロンプトから、次の`Set-SfConfig`コマンドを実行します: `Set-SfConfig -PrimaryZoneController "server"-Passphrase "passphrase"-FilePath "fullpath"`

   各項目の意味は次の通りです:

   - server は、プライマリストレージゾーンコントローラー サーバー名または IP アドレスです。次の形式のいずれかで指定でき、末尾にスラッシュを含める必要があります。

     `http://localhost/ConfigService/`

     `servername/` または `serverip/` （HTTP を使用している場合）

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

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

   - passphrase は、ストレージゾーンコントローラー に指定されたものです。
   - fullpath は、バックアップファイルの場所と名前です。例: `c:\szc-backup.bak`。

バックアップファイルなしでプライマリストレージゾーンコントローラー をリカバリするには

バックアップファイルがない場合は、ShareFile Data 用のゾーンとストレージゾーンの構成をリカバリできますが、ストレージゾーンコネクタはリカバリできません。

1. この PowerShell セッションのユーザーコンテキストを設定します。コマンドウィンドウで、次のいずれかのコマンドを実行します。

   - デフォルトのネットワークサービスアカウントを使用している場合:

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

   - ストレージゾーンコントローラー アプリケーションプールに指定ユーザーを使用する場合:

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

   PowerShell ウィンドウが開きます。

2. PowerShell プロンプトから、モジュール ConfigBR.dll をインポートします: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

新しい PowerShell ウィンドウを開くたびに、モジュールをインポートする必要があります。

3. PowerShell プロンプトから、join-SFConfig コマンドを実行します。

> 重要:
>
> Join-SFConfig コマンドは現在、Azure または Amazon S3 ストレージをサポートしていません。このコマンドを使用する必要がある場合は、ShareFile サポートにお問い合わせください。

```
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]
```

場所:

- ZoneID は次のように取得できます。
  a) ShareFile Web インターフェイスで、[管理**] > [**ストレージゾーン] の順にクリックし、サイト名を右クリックして [プロパティ**]** を選択します。

     表示されるアドレスは、次のようなゾーン ID で終わります `zae4fb8c-8520-478f-8f87-aa589a8fd181`。

  b) この ID をコピーして Join-SFConfig コマンドに貼り付けます。
- StorageCenterID は次のようにして取得できます。
  a) ShareFile Web インターフェイスで、[管理] > [ストレージゾーン] の順にクリックし、サイト名をクリックし、ホスト名を右クリックして [プロパティ] を選択します。

     表示されるアドレスは、次のようなストレージ ID で終わります: `scd344cf-8043-4ce2-974b-8f9cd83e2978`。

  b) この ID をコピーして Join-SFConfig コマンドに貼り付けます。
- StorageZoneLocation は、ShareFile データのストレージゾーンがゾーンに対して有効な場合にのみ必要です。
- StorageUsername および StoragePassword が必要となるのは、そのゾーンで ShareFile Data のストレージゾーンが有効で、ストレージの場所で認証が必要な場合のみです。
- AzureAccountName、AzureAccessKey、および AzureContainerName は、ShareFile データのストレージゾーンが Windows Azure ストレージコンテナーに格納されている場合にのみ必要です。

4. ストレージゾーンコネクタを復元するには、ストレージゾーンコントローラー コンソール (`http://localhost/configservice/login.aspx`) を使用してコネクタを有効にして構成します。

プライマリ **Storage Zone Controller** の置き換え

April 27, 2021

プライマリ Storage Zone Controller を別の場所 (別のドメインなど) にあるコントローラーに置き換えるには、バックアップ手順と回復手順を使用します。次の手順に従って、構成設定とすべてのデータが転送されます。

1. 既存の Storage Zone Controller 構成のバックアップファイルを作成します。「プライマリ Storage Zone Controller 構成のバックアップ」を参照してください。
2. 新しいネットワークの場所に Storage Zone Controller をインストールしますが、構成しないでください。
3. バックアップした設定を新しいコントローラにインポートします。「プライマリ Storage Zone Controller 構成を回復する」を参照してください。
4. データを新しいネットワーク共有にコピーし、新しい Storage Zone Controller 構成コンソールにログオンし、新しいストレージパス情報を入力します。「新しいネットワーク共有にファイルを転送する」を参照してください。
5. 新しい Storage Zone Controller の構成コンソールで、コントローラーの外部 URL を更新します。「プライマリ Storage Zone Controller アドレスまたはパスフレーズの変更」を参照してください。

ファイル回復用のストレージゾーンコントローラの準備

September 6, 2023

> 警告:
>
> ShareFile 回復機能では、永続的なストレージの場所が自動的にバックアップされません。バックアップユーティリティを選択し、1〜7 日おきに実行する責任があります。

ファイルリカバリの準備方法は、データの保存場所によって異なります。

- サポートされているサードパーティ製ストレージシステム—Storage Zones Controller を搭載したサードパーティ製ストレージシステムを使用する場合、サードパーティ製ストレージは冗長化され、ローカルバックアップは不要です。ただし、ファイルを削除する ShareFile ユーザーは、短い期間ごみ箱からファイルを回復できることに注意してください。45 日が経過すると、ShareFile ごみ箱からファイルを復元することはできません。復旧期間が過ぎると、ファイルはゾーンから削除されます。そのため、サードパーティの冗長ストレージからも削除されます。回復時間が十分でない場合は、次のいずれかの解決策を検討してください。

  - StorageZone Controller のファイルクリーンアップサービスが実際のファイルをオンプレミスのストレージロケーションから削除しないようにするには、`C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\SCFileCleanSvc\\FileDeleteService.exe.config`での **Period** 設定の値を変更します。詳細については、「ストレージキャッシュ操作のカスタマイズ」を参照してください。保存期間を長くすると、サード・パーティ製ストレージの容量も増えることに注意してください。
  - StorageZone ファイルのローカルバックアップを 7 日ごとに作成し、バックアップの適切な保存ポリシーを決定します。

- オンプレミスストレージ—ローカルで管理されている共有をプライベートデータストレージに使用する場合、オンプレミスストレージゾーン、コントローラー、ローカルファイルストレージ、およびレジストリエントリをバックアップする必要があります。ShareFile は、ShareFile クラウドに存在する対応するファイルメタデータを 3 年間アーカイブします。
  重要: データ損失を防ぐには、ストレージゾーンコントローラーサーバーのスナップショットを撮り、その構成をバックアップし、ローカルファイルストレージをバックアップすることが重要です。

このトピックの説明に従ってストレージゾーンコントローラーをファイル回復用に準備したら、ShareFile 管理者コンソールを使用して次のことが可能になります。

- 特定の日付と時刻の ShareFile Data レコードのストレージゾーンを参照し、復元するファイルとフォルダーにタグを付けます。ShareFile、タグ付けされたアイテムを回復キューに追加します。次に、回復スクリプトを実行して、バックアップから永続的なストレージ場所にファイルを復元します。

  詳しくは、「ShareFile Data バックアップからファイルとフォルダーを復元する」を参照してください。

- オンプレミスのストレージからデータを回復できない場合は、ShareFile クラウドに格納されたメタデータをオンプレミスストレージと調整します。ShareFile リコンサイル機能は、指定された日時にストレージゾーンに存在しなくなったファイルのメタデータを ShareFile クラウドから永久に削除します。

  詳細については、「ShareFile クラウドとストレージゾーンの調整」を参照してください。

前提条件

- 2 つの CPU と 4 GB RAM を備えた専用の物理マシンまたは仮想マシン
- Windows サーバー 2012 R2 (データセンター、スタンダード、またはエッセンシャル)
- Windows Server 2016
- Windows Server 2019
- Windows PowerShell (32 ビットおよび 64 ビットバージョン) は、.NET 4 ランタイムアセンブリをサポートする必要があります。詳細については、ストレージゾーンコントローラーのシステム要件の「PowerShell スクリプトとコマンド」を参照してください。

- PsExec.exe-PSExec を使用すると、ネットワークサービスアカウントを使用して PowerShell を起動できます。PSExec を使用して、回復タスクをスケジュールすることもできます。https://docs.microsoft.com/en-us/sysinternals/downloads/psexecから PsExec.exe をダウンロードし、そのページのインストール手順に従います。

障害復旧に使用されるファイルの概要

C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery にある次のファイルは、障害回復に使用されます。

ファイル名	説明
DoRecovery.ps1	回復プロセスを処理するために Windows タスクスケジューラによって実行される PowerShell スクリプト。このファイルには、ファイルのバックアップおよび保存場所が格納されます。
Recovery.psm1	リカバリキュー操作を処理する PowerShell モジュール。
recovery.log	回復プロセスの出力を保存するログファイル。
recoveryerror.log	回復プロセスのエラーを格納するログファイル。
LitJson.dll	JSON (JavaScript オブジェクト記法) 文字列からの変換を処理する.Net ライブラリ。

バックアップフォルダを設定するには

バックアップサーバで、persistentStorage フォルダをバックアップするフォルダを作成します。

ShareFile Data ファイルバックアップ用のストレージゾーンは、ストレージゾーンコントローラの永続ストレージと同じレイアウトに従う必要があります。

バックアップの場所が Storage Zone Controller の永続ストレージと同じレイアウトになっていない場合は、回復プロセス中に追加の手順を実行して、バックアップの場所から Recovery PowerShell スクリプトで指定した場所にファイルをコピーする必要があります。

ストレージレイアウト

バックアップレイアウト

```
\\\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
```

> 重要:
>
> ShareFile 回復機能では、永続的なストレージの場所が自動的にバックアップされません。バックアップユーティリティを選択し、**1**〜**7** 日おきに実行する責任があります。

障害回復キューを作成するには

この 1 回限りのセットアップが必要です。以下のコマンド例では、デフォルトのストレージゾーン Controller インストールフォルダーを使用しています。

1. ストレージゾーンコントローラーで、管理者として PowerShell を実行します。
2. この手順で使用する PowerShell スクリプトは署名されていないので、PowerShell 実行ポリシーの変更が必要になる場合があります。
   a) お使いの PowerShell 実行ポリシーで、署名のないローカルのスクリプトを実行できるかどうかを確認してください。PS C:\ >Get-ExecutionPolicy

      たとえば、RemoteSigned、Unrestricted、または Bypass のポリシーでは、署名されていないスクリプトを実行できます。

   b) PowerShell 実行ポリシーを変更するには:PS C:\ >Set-ExecutionPolicy (リモート署名)
3. PowerShell の CLR バージョンが正しいことを確認するには、次のように入力します。

   $ps バージョンテーブル

   PowerShell がスクリプトで.NET アセンブリをロードできるようにするには、clrVersion の値は 4.0 以上である必要があります。そうでない場合は、Windows PowerShell 32 ビットバージョンと 64 ビットバージョンの両方で次のように変更します。

   a) 管理者としてメモ帳を実行します。
   b) 次の内容でファイルを作成します。

```
<?xml version="1.0"?>
<configuration>
```



```
3         <startup useLegacyV2RuntimeActivationPolicy="true">
4             <supportedRuntime version="v4.0.30319"/>
5             <supportedRuntime version="v2.0.50727"/>
6         </startup>
7     </configuration>
```

c) ファイル／別名で保存を選択し、ファイルに powershell.exe.config という名前を付けて、次の場所に保存します。

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

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

d) PowerShell ウィンドウを閉じ、管理者として新しいウィンドウを開き、$psversiontable と入力して clrVersion が正しいことを確認します。

4. PowerShell ウィンドウを閉じ、PsExec.exe を使用して PowerShell を次のように起動します。

   a) 管理者として [コマンドプロンプト] ウィンドウを開きます。

   b) PsExec.exe の場所に移動し、次のように入力します。

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

   c) PsExec.exe ライセンス契約に同意するには、[同意する] をクリックします。

5. ストレージゾーンコントローラのインストールフォルダにあるディザスタリカバリツールフォルダに移動します。

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

6. Recovery.psm1 モジュールをインポートします。

   Import-Module .\Recovery.psm1

7. リカバリキューを作成するには、「New-scQueue-名前リカバリ-オペレーションリカバリ」と入力します。

   このコマンドの出力には、作成されたキューの名前が含まれます。例: キュー 92736b5d-1cff-4760-92c8-d8b04dc92cb2 が作成されました

   新しいフォルダを表示するには、ファイルブラウザを開き、次の場所に移動します。

   \\ サーバ\ (プライマリストレージの場所)\ キュー 92736b5d-1cff-4760-92c8-d8b04dc92cb2 のように、キューフォルダが表示されます。

8. 次のセクションの説明に従って、場所に合わせて回復用 PowerShell スクリプトをカスタマイズします。

場所に合わせて回復する **PowerShell** スクリプトをカスタマイズするには

DoreRecovery.ps1 PowerShell スクリプトは、リカバリプロセスを処理するためにタスクスケジューラによって実行されます。このファイルには、サイトに指定する必要があるファイルのバックアップと格納場所が含まれます。

1. ストレージゾーンコントローラーで、リカバリ PowerShell スクリプトに移動します。

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

2. スクリプトを次のように編集します。

   a. バックアップ場所の UNC パスを指すように $backuProot パラメーターを設定します。例: $backupRoot = “\\10.10.10.11\(*Your*BackupLocation)\persistentstorage”

   b. $StorageRoot パラメータを、ストレージゾーンコントローラの永続ストレージの UNC パスを指すように設定します。例: $storageRoot = “\\10.10.10.10\StorageLocation\persistentstorage”

回復プロセスをテストするには

1. テストファイルを作成し、ShareFile にアップロードします。
2. 1 時間ほど経ったら、ファイルが永続ストレージ ($backupRoot に指定されたパス) に表示されていることを確認します。
3. ShareFile からファイルを削除する:ShareFile 管理者ツールで、[ごみ箱] をクリックし、ファイルを選択し、[完全に削除] をクリックします。
4. 永続ストレージからファイルを削除します。

   この手順では、ファイルが削除されてから 45 日後に ShareFile が実行するアクションが再作成されます。

5. ShareFile 管理者ツールで、[管理**] > [**ストレージゾーン] に移動し、ゾーンをクリックして [ファイルの回復] をクリックします。
6. **Recovery Date** テキストボックスをクリックし、ファイルが削除される前とアップロードされた後の日付と時刻を選択します。

   指定した日時のストレージゾーンのファイルリストが表示されます。

7. ファイルのチェックボックスをオンにします。
8. 復元したファイルを格納するフォルダを選択し、[復元] をクリックします。

   ファイルがリカバリキューに追加され、リストアする準備が整います。ファイルが正常に回復されると、画面が変わり、回復されたファイルが格納されているフォルダが表示されます。

9. ファイルをリカバリするには:

   a. 管理者として [コマンドプロンプト] ウィンドウを開きます。

   b. PsExec.exe の場所に移動し、次のように入力します。

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


c. PowerShell ウィンドウで、次の場所に移動します。

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

d. リカバリスクリプトを実行します。

```
.\DoRecovery.ps1
```

PowerShell ウィンドウには、「アイテムが回復されました」というメッセージが表示されます。ファイルは、永続的な格納場所に追加されます。

10. ShareFile の Web サイトから復元されたファイルをダウンロードします。

関連する **PowerShell** コマンド

次の PowerShell コマンドは障害回復をサポートします。

- **Get-RecoveryPendingFileIDs**

  回復に必要なファイル ID のリストを取得します。構文とパラメータについては、次のコマンドを使用します。

  Get-Help Get-RecoveryPendingFileIDs -full

- **Set-RecoveryQueueItemsStatus**

  リカバリキュー内のすべてのアイテムまたは指定されたアイテムのステータスを設定します。これにより、キュー内の既存の回復ステータスが上書きされます。構文とパラメータについては、次のコマンドを使用します。

  Get-Help Set-RecoveryQueueItemsStatus -full

リカバリのタスクを作成してスケジュールするには

スケジュールされたリカバリタスクが必要な場合は、以下の手順に従ってください。

1. Windows タスクスケジューラを起動し、[操作] ウィンドウで [タスクの作成] をクリックします。
2. [全般] タブで、次の操作を行います。

   a. タスクにわかりやすい名前を入力します。

   b. [セキュリティオプション] で、[ユーザーまたはグループの変更] をクリックし、タスクを実行するユーザー (ネットワークサービスまたは格納場所への書き込み権限を持つ名前付きユーザー) を指定します。

   c. 「**Configure for** 」メニューから、タスクを実行するサーバーのオペレーティングシステムを選択します。
3. トリガーを作成するには、「トリガー」タブで「新規」をクリックします。
4. [タスクを開始する**]** で、[スケジュールに基づいて] を選択し、スケジュールを指定します。

5. アクションを作成するには、「アクション」タブで「新規」をクリックします。

   a. [アクション] で、**[**プログラムの開始] を選択し、プログラムへのフルパスを指定します。例: `C:\Windows\System32\cmd.exe`。

   b.「引数の追加」に、次のように入力します。`/c “c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1” >> .\recovery.log 2>>.\recoveryerror.log`

   c. **Start in** には、ストレージゾーンコントローラのインストール場所の Disaster Recovery フォルダーを指定します。たとえば、次のようになります: `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

サービスのデフォルト期間の削除

StorageZone コントローラ 4.0 以降、サービスの削除タイマーは 45 日に設定されます。45 日のデフォルト期間は、以前の設定を上書きします。デフォルトの期間を変更するには、C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc で FileDeleteService.exe.config を編集してください

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

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

アップグレード後のデフォルトサービスの削除期間の変更

いくつかのアップグレードシナリオでは、deletePeriod の値は、「fileDeleteService.exe.config」で null に設定されます。null に設定すると、削除期間はデフォルトで 45 日になります。これは、ShareFile から削除されたファイルが物理ストレージから削除されるまでのデフォルトの日数です。

ストレージゾーンコントローラの DeletePeriod を変更するには、次の場所にある FileDeleteService.exe.config ファイルを編集します。`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

ストレージゾーンコントローラーをクリーンインストールすると、削除サービスが 8 時間ごとに実行され、一時ファイルとフォルダーがクリーンアップされます。タイマーを変更するには、次の場所にある FileDeleteService.exe.config ファイルを編集します。`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

ShareFile データのバックアップからファイルとフォルダを回復する

April 27, 2021

ShareFile 管理者コンソールでは、特定の日時の ShareFile Data レコードのストレージゾーンを参照し、回復するファイルやフォルダにタグを付けることができます。ShareFile、タグ付けされたアイテムを回復キューに追加します。その後、提供されたスクリプトを実行して、バックアップから保存場所にファイルを回復できます。

> 重要:
>
> この手順では、必ず PowerShell 4.0 を使用してください。PowerShell の要件について詳しくは、Storage Zone Controller システム要件の
> PowerShell スクリプトとコマンドを参照してください。

前提条件

- ファイル回復用の Storage Zone Controller の準備の説明に従って、セットアップとテストを完了します。セットアップには、回復されたファイルを格納するフォルダを作成する手順が含まれています。

1. ShareFile Web インターフェイスで、[管理] をクリックし、[ストレージゾーン] をクリックします。
2. ゾーン名をクリックし、[ファイルの回復] をクリックします。
3. [回復日] テキストボックスをクリックし、日付と時刻を選択します。

   指定した日時のストレージゾーンのファイルリストが表示されます。
4. 回復する各ファイルのチェックボックスをオンにし、[回復] をクリックします。
5. 回復したファイルを格納するフォルダを選択し、[回復] をクリックします。

   フォルダリストには、回復が進行中であることを示す回転アイコンが表示されます。
6. バックアップの場所がストレージゾーンの永続ストレージと同じレイアウトに従っていない場合は、バックアップの場所から doRecovery.ps1 の編集時に指定した場所にファイルをコピーします。
7. doRecovery.ps1 PowerShell スクリプトは署名されていないので、この手順の PowerShell 実行ポリシーを変更する必要がある場合があります。

   a) PowerShell 実行ポリシーで、ローカルの署名されていないスクリプトを実行できるかどうかを確認します。PowerShell ウィンドウで: `Get-ExecutionPolicy`

      たとえば、RemoteSigned、Unrestricted、または Bypass のポリシーでは、署名されていないスクリプトを実行できます。

   b) PowerShell 実行ポリシーを変更するには: `Set-ExecutionPolicy RemoteSigned`
8. この PowerShell セッションのユーザーコンテキストを設定します。コマンドウィンドウで、次のいずれかのコマンドを実行します。

   - デフォルトのネットワークサービスアカウントを使用している場合:

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


- Storage Zone Controller アプリケーションプールに指定されたユーザーを使用している場合:

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

PowerShell ウィンドウが開きます。

9. ファイルを回復します。

   a) 管理者として [コマンドプロンプト] ウィンドウを開きます。

   b) PsExec.exe の場所に移動し、次のように入力します。

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

   c) PowerShell ウィンドウで、次の場所に移動します。

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

   d) 回復スクリプトを実行します。

   `.\DoRecovery.ps1`

PowerShell ウィンドウには、「アイテムが回復されました」というメッセージが表示されます。回復されたファイルは、バックアップから永続的なストレージ場所にコピーされます。コンソールを更新すると、正常にリカバリされたファイルの ShareFile Web インターフェイスから回転するアイコンが消えます。

ShareFile Web アプリケーションから削除されたファイルが、Storage Zone Controller 削除サービスによってまだ削除されていない場合、ファイルは永続的なストレージの場所に残っています。この場合、ファイルの回復は即座に実行され、回転アイコンは ShareFile Web インターフェイスに表示されません。

ファイルを回復できない場合は、[障害回復] フォルダにあるヘルプファイルを参照してください。

ShareFile クラウドとストレージゾーンを調整する

April 27, 2021

ディスク障害などの問題により、ローカルストレージでデータが失われると、ローカルストレージと ShareFile クラウドに格納されたメタデータの間で一貫性のない状態になります。これらの差異を自動的に調整して、指定した日時にストレージゾーンに存在しなくなったファイルのメタデータを ShareFile クラウドから完全に削除することができます。

> 注意:
>
> ローカルファイルストレージに回復不能なデータ損失がある場合にのみ、リコンサイルを実行します。リコン

> サイルは、指定した日時の時点でローカルファイルストレージに見つからないファイルについて、ShareFile クラウドからメタデータを永続的に消去します。

1. [管理] をクリックし、[ストレージゾーン] をクリックします。
2. ゾーン名をクリックし、[ファイルの調整] をクリックします。
3.「調整日」テキストボックスをクリックし、日付と時刻を選択します。
4.「調整」をクリックします。確認ダイアログボックスが開きます。

Windows サーバー 2012R2 ShareFile ストレージゾーン用移行ガイド

November 17, 2023

> 重要:
>
> Microsoft は、2023 年 10 月 10 日をもって Windows Server 2012R2 のサポートを終了します。サポート終了日までにサーバーを新しいバージョンに移行することが重要です。

この記事では、ShareFile ストレージゾーンサーバーを Windows Server 2012R2 から新しいバージョンに移行する方法について説明します。

新しいバージョンの Windows Server に移行するには、セカンダリストレージゾーンコントローラを新しいサーバに追加し、それをプライマリコントローラとして昇格させる必要があります。

システム要件

ストレージゾーン Controller サーバーは、以下のバージョンをサポートします。

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

手順

> 注:
>
> 以下の手順には、**ShareFile** データリポジトリの移行は含まれていません。移行する予定のストレージゾーンコントローラと同じサーバーに ShareFile データリポジトリがある場合、または移行する Windows Server 2012R2 を実行しているファイルサーバーにストレージゾーンデータリポジトリがある場合は、「新しいネットワーク共有へのファイルの転送 」を参照してください。

ステップ **1-ShareFile** ストレージゾーンコントローラ用の新しいサーバーの準備

「ShareFile データ用のサーバーの準備」に記載されている手順に従って、新しいサーバーを準備します。

ステップ **2-**ストレージゾーンコントローラを新しいサーバにインストールし、セカンダリサーバとして追加する

ShareFile 用に新しいサーバーを準備したら、そのサーバーをセカンダリサーバーとしてストレージゾーンに追加する必要があります。詳細については 、「セカンダリストレージゾーン Controller をストレージゾーンに参加させる 」を参照してください。

ステップ **3-**新しいサーバをプライマリに昇格させ、古いサーバをセカンダリに降格させる

新しいサーバーをセカンダリとして追加したら、次のステップはそのサーバーをプライマリに昇格させることです。古いサーバーもセカンダリに降格する必要があります。この手順の詳細については、「ストレージゾーンコントローラーの降格と昇格」を参照してください。

> 注**:**
>
> ShareFile では、古いサーバーをセカンダリとして使用せずに、新しいストレージゾーンサーバーの機能を単独でテストすることをお勧めします。これを行うには、古いサーバーを一時的に無効にします。詳細については、「ストレージゾーンコントローラを無効にするには」を参照してください。

ステップ **4 (**オプション**)-**セカンダリサーバーの追加

必要に応じて、セカンダリサーバーを追加するたびに、ステップ 2-新しいサーバーに Storage Zone Controller をインストールし、セカンダリサーバーとして追加します。

手順 **5 (**オプション**)-NetScaler** サービスグループメンバーの更新

NetScaler を使用している場合は、新しいストレージゾーンサーバーが ShareFile サービスグループに追加されていることを確認します。詳細については 、「構成ユーティリティを使用してサービスグループにメンバーを追加するには 」を参照してください。

ステップ **6-ShareFile** 管理ポータルから古いストレージゾーンコントローラーサーバーを削除する

ストレージゾーンサーバーが正常に移行されたら、古いサーバーを ShareFile 管理ポータルから削除できます。詳細については 、「ストレージゾーン Controller を削除するには 」を参照してください。

アップロードされたファイルのウイルス対策スキャンの構成

July 1, 2022

> 重要:
>
> StorageZones 4.2 のアプリケーションコードを更新するため、一部のお客様は、ローカル管理者からシステムネットワークサービスに、ツールを実行する権限レベルを更新する必要があります。アクセス許可の更新に失敗すると、ウイルス対策スキャンの開始に失敗します。

要件/要約

- StorageZones Controller 4.2 以降を使用しているユーザー
- sfAntivirus は、PSExec を使用してネットワークサービスとして実行する必要があります
- ログファイルの場所を更新する

PSExec を使用して **SFAntivirus** をネットワークサービスとして実行します。

SFAntivirus にリンクしている既存のスケジュールされたタスクを使用して SZ 4.2 以降に更新するクライアントは、ツールを実行するユーザーレベルをローカル管理者からシステムネットワークサービスに変更する必要があります。

ネットワークサービス権限を取得するには、PSExec を使用してストレージゾーン Controller と同じユーザーコンテキストで PowerShell (x86) を起動し、次のコマンドを使用してネットワークサービス権限を取得します。

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

ログファイルの場所を更新する

管理者は、次の行を変更して、デフォルトの SZC ログディレクトリ以外のディレクトリにログインしている場合は、log4net.config エントリを編集してログファイルの場所を変更する必要もあります。

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

ストレージゾーン Controller のインストールには、ウイルス対策スキャンをサポートするいくつかのファイルが含まれています。ファイルは C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus. にデフォルトでインストールされます

次の手順で説明するように、構成ファイルをカスタマイズし、Windows タスクスケジューラを使用してスキャンをスケジュールすると、ファイルアップロード要求ごとにストレージゾーンコントローラがファイルをウイルス対策スキャン用にキューイングします。スキャンされたファイルに関する問題が報告された場合、フォルダビューにはファイルの警告アイコンが表示されます。ユーザーがファイルをダウンロードしようとすると、警告メッセージが表示されます。

StorageZones Controller 4.0 以降では、ウイルス対策ログファイルの場所を構成できます。ログの場所を変更するには、C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus. で SFAntivirus.exe.config ファイルを編集します。

ウイルス対策スキャンでは、ファイルは削除されません。

StorageZones Controller 4.2 以降では、ICAP の RFC 標準にコード化されたウイルス対策スキャンプラットフォームで ICAP プロトコルを使用することがサポートされます。ICAP AV の設定に関する情報は、この記事のさらに下にあります。

> 注意:
>
> ゾーンでウイルス対策を構成すると、新しくアップロードされたアイテムがスキャンされます。ウイルス対策の設定は遡及的ではありません。ゾーンにすでに存在するファイルおよびアイテムはスキャンされません。

場所の設定を準備するには

1. ストレージゾーン Controller 以外のサーバーでウイルススキャンを実行するには
   a) フォルダー C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus を別のサーバーにコピーします。
   b) ストレージゾーンコントローラーで C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config を開き、queuesdkRestricted を 0 に設定します。`<add key="QueueSDKRestricted" value="0"/>`
2. ウイルススキャンを実行するサーバーで、sfAntiVirus.exe.config をストレージゾーン Controller 構成の値で編集します。
   a) CommandFile: ウイルス対策ソフトウェアのフルパスを指定します。このソフトウェアは、ShareFile ウイルス対策フォルダと同じサーバー上に存在する必要があります。
   b) CommandOptions とリターンコードの場合: 設定ファイルに提供されるコマンドライン設定の例を示します。ウイルス対策ソフトウェアおよび環境に適した設定を指定します。
   c) ScanFileTimeout の場合: 大きいファイルのスキャンに時間がかかる場合があります。ストレージで予想されるファイルサイズに応じて、この設定を調整します。そうしないと、大きなファイルがスキャンされないリスクが高まる可能性があります。
3. コマンドラインウィンドウで、次のコマンドを実行して、ウイルススキャンを設定します。`SFAntiVirus.exe -register SFusername SFpassword`

コマンドラインツールの代わりに **ICAP** を **AV** スキャンで使用する

ストレージゾーンコントローラ 5.3 以降では、ICAP の RFC 標準にコード化されたウイルス対策スキャンプラットフォームでの ICAP プロトコルの使用がサポートされています。お客様は、必要に応じて CLI メソッドを使用できます。

この機能は、ストレージゾーンコントローラ 5.0.1 以降では、テナントゾーンでサポートされています。

Storage Zone Controller で ICAP AV スキャナーを有効にするには、Storage Zone Controller の設定ページに移動します。

[ウイルス対策統合を有効にする] チェックボックスをオンにし、[**ICAP RESPMOD URL**] フィールドにウイルス対策サーバのアドレスを入力します。これは、ICAP 応答変更サービスの URL `ICAP://SERVER/RESPMOD`です。

[接続のテスト] をクリックして設定を確認します。

ウイルススキャンのタスクを作成してスケジュールするには

> 注意**:**
>
> ウイルススキャンのスケジュールされたタスクの作成は、コマンドラインツールを使用する場合にのみ必要です。ICAP を利用する場合、これは必須ではありません。

1. Windows タスクスケジューラを起動し、[操作] ウィンドウで [タスクの作成] をクリックします。
2. [全般] タブで、次の操作を行います。
   a) タスクにわかりやすい名前を指定します。
   b) [セキュリティオプション] で、[ユーザーまたはグループの変更] をクリックし、タスクを実行する Windows ユーザーを指定します。ユーザーは、格納場所に対するフルアクセス権を持っている必要があります。
   c) [ユーザーがログオンしているかどうかに関係なく実行する] を選択します。[パスワードを保存しない] チェックボックスはオフのままにします。
   d) [最高の権限で実行する] を選択します。
   e) [**Configure for]** メニューから、タスクを実行するサーバーのオペレーティングシステムを選択します。
3. トリガーを作成するには:[トリガー] タブで、[新規] をクリックします。次に、[タスクの開始**]** で **[**スケジュールに従う] を選択し、スケジュールを指定します。
4. アクションを作成するには:[アクション] タブで、[新規作成] をクリックします。
   a) [操作] で、[プログラムの開始] を選択し、プログラムへのフルパスを指定します。次に例を示します:

      `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus\\SFAntiVirus.exe`
   b) [開始場所] で、SFAntiVirus.exe の場所を指定します。`C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`
5. [設定] タブの [タスクが既に実行されている場合、次のルールが適用されます] で、[新しいインスタンスを開始しない] を選択します。

スキャンサービスへの **AV** コマンドライン統合

前提条件

- ストレージゾーン Controller 5.2 をインストールまたはアップグレードする前に、既存のコマンドライン AV がスケジュールされたタスクまたは cron として実行されている場合は、そのコマンドライン AV を停止または削除してください。
- ホストマシンに.NET 4.6.2 (またはそれ以降) をインストールします。

オンプレミスのストレージゾーンコントローラのスキャンサービスには、Symantec コマンドライン AV スキャンなどのコマンドラインの AV ツールの使用がサポートされています。さらに、スキャンサービスは、ICAP がサポートするウイルス対策製品を使用してスキャンを提供します。

この機能を有効にするには､次の設定キーと値をアンチウイルス/onprem/AVscanService/AVScanService/appSettings.config に追加します。

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

コマンドラインツール固有の構成

ストレージゾーン Controller 5.2 のアップグレードまたは新規インストールには、新しい構成ファイルが含まれます。

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

このファイルは、AV コマンドラインに必要な設定を処理します。

次に、設定キーの値について説明し、値の例を挙げます。

- このポイントをコマンドラインアプリに設定します。

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

- コマンドラインアプリのマニュアルを参照して、サポートされているオプションまたはスイッチを確認し、この場所にそれらを追加します。

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

- クリーンスキャンを示す出力値を含めます。

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

- 感染ファイルを示す出力値を含めます。

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

- スキャンされていないファイルを示す出力値を含めます。

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


拡張子の除く最大ファイルサイズの強制に関する注意事項

バージョン 5.2 より前のバージョンでは、コマンドライン AV で拡張子の除外または最大ファイルサイズの強制を実行できませんでした。この操作は、ICAP スキャンサービスでのみ実行できます。バージョン 5.2 では、除外された拡張子および最大ファイルサイズ (バイト単位) に関する ICAP スキャンサービスに適用したのと同じ設定が AV コマンドラインサービスに適用されます。

これらの設定の名前は次のとおりです。

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

ストレージゾーン Controller 5.2 を新規インストールすると、これらの設定の名前が次のように変更されます。名前が変更された設定は、ICAP ベースの AV とコマンドライン AV の両方に適用できるという事実を反映しています。

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

アップグレードでは、これらの設定の名前は変更されません。手動による名前の変更も機能しますが、ICAP に加えて AV コマンドラインでも同じ設定が機能します。

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

ShareFile データの移行

August 7, 2023

ShareFile データをオンプレミスゾーンから別のオンプレミスゾーンに移行する方法は複数あります。

- Web ポータルまたはユーザー管理ツールによる移行
- PowerShell スクリプトを使用して移行する
- ZoneFix ツールを使用して移行

前提条件

- ソースゾーンが宛先ゾーンから到達可能であることを確認し、ソースストレージセンターへのアウトバウンド接続のブロックを解除します。
- ゾーン間の接続をテストするには、移行先ゾーンのブラウザーでソースゾーンの外部アドレスに移動して、ソースゾーンの外部アドレスにアクセスします。接続に成功すると、ShareFile ロゴが表示されます。

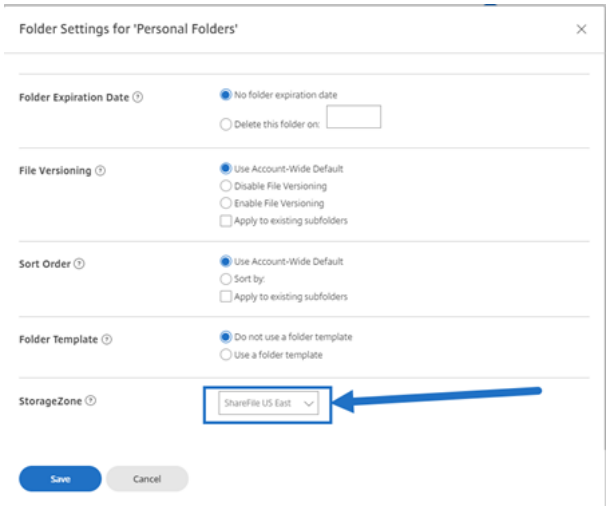
Web ポータルまたはユーザー管理ツールによる移行

ShareFile Web アプリケーションでは、個々のユーザーまたは特定のフォルダーについて、ゾーン間のデータの移行を開始できます。

> 重要:
>
> 次の変更を保存すると、すぐに非同期移行操作がトリガーされ、既存のファイルが新しいゾーンにアップロードされます。この移行期間中にフォルダーにアップロードされた新しいファイルは、新しいゾーンに進みます。

特定のユーザーのデータを移行する - **[People]** に移動し、従業員ユーザーを探します。ユーザーをクリックして、自分のプロファイルページを表示します。[ストレージの場所] で、新しいゾーンを選択します (ゾーンがすでにインストールおよび構成されている場合)。

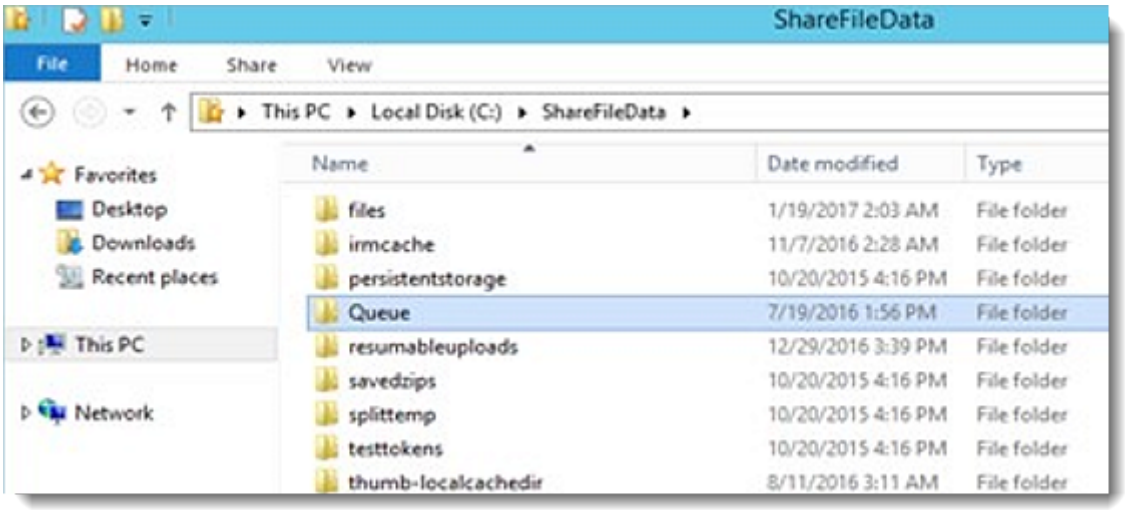
特定のフォルダーのデータを移行する - フォルダーに移動し、フォルダー名の右側にある **[**その他のオプション**]** メニューにアクセスします。[フォルダーの詳細設定**]** をクリックします。メニューを使用して、新しいゾーンを選択します。



移行プロセス

まず、移行のためにキューに入れられたファイルによって、元のゾーンの [ストレージの場所] 内の [キュー] フォルダーにプレースホルダファイルが作成されます。

プレースホルダファイルが正常に処理されると、移行されたファイルは元のゾーンの`persistentstorage`から削除され、新しいゾーンの`persistentstorage`に追加されます。



PowerShell 経由で移行する

ShareFile PowerShell SDK を使用すると、ユーザーは元のゾーンの場所から大きなフォルダー構造をダウンロードし、それらのフォルダーを新しいゾーンにアップロードできます。

要件 -SDK を実行およびインストールするには、PowerShell 4+ および.NET 4.x+ が必要です。PowerShell 5.x は、Windows Management Framework 5.1 の一部としてここからダウンロードできます 。

ゾーン修正ツールによる移行

[ゾーン修復] ツールは、コマンドラインツールです。このツールは、ストレージゾーンの開発者によって作成され、ShareFile API を活用して、特定のゾーンに移行するためのターゲットフォルダ ID です。

最適なパフォーマンスを得るには、2 GB 未満のフォルダーにこの方法を推奨します。

コネクタのお気に入り

February 14, 2022

ストレージゾーンコントローラー 5.0 以降では、ShareFile WebApp 内の [ネットワーク共有]、[**SharePoint**]、および [**Documentum** コネクタ] で、コネクタフォルダーをお気に入りにすることができます詳しくは、Citrix サポートナレッジセンターの記事を参照してください。

ShareFile Mobile では、お気に入りへのコネクタフォルダーの追加がサポートされています。

ShareFile データのストレージゾーンを管理する

November 17, 2023

ShareFile データ用のストレージゾーンは、ShareFile で管理されるクラウドとまたは共有ファイル管理クラウドの代わりに使用できます。

> 注:
>
> プライマリストレージゾーンコントローラを削除する場合は、続行する前にそのプライマリストレージゾーンコントローラを降格させてください。詳細については、「ストレージゾーンコントローラーの降格と昇格」を参照してください。

ゾーン間でホームフォルダーとファイルボックスを移動する

次の手順を使用して、ホームフォルダーとファイルボックスをゾーン間で移動します。または、ShareFile ユーザー管理ツールを使用して、ゾーン間でユーザーを移行します。

1. **[**ホーム**]** をクリックし、フォルダーに移動します。
2. 右側のナビゲーションウィンドウで、[フォルダオプションの編集] をクリックします。
3. ストレージゾーンメニューからゾーンを選択し、[保存] をクリックします。

ストレージゾーンにフォルダーを作成する

1. [ホーム] をクリックし、[フォルダ] をクリックします。
2. [フォルダ] タブで、[フォルダーの追加] をクリックします。
3. フォルダ情報を指定します。ストレージサイトでは、このフォルダとその内容を保存するストレージゾーンを選択します。
4. [フォルダーの作成] をクリックします。
5. 通常どおりフォルダーを設定します。フォルダーを作成するときに、ShareFile が管理するクラウドストレージを使用するか、ローカルストレージゾーンを使用するかを選択できます。

ストレージゾーンの名前変更または削除

> 重要:
>
> ストレージゾーンを削除する前に、ストレージゾーンをバックアップしてください。ゾーンを削除すると、そのゾーン内のすべてのファイルとフォルダーが消去され、操作を元に戻すことはできません。

1. [管理] をクリックし、[ストレージゾーン] をクリックします。
2. ゾーン名をクリックします。

- ゾーンの名前を変更するには:[ゾーンの編集] をクリックし、新しい名前を入力し、[変更の保存] をクリックします。
- ゾーンを削除するには: ゾーン名をクリックし、[**Delete Zone**] をクリックします。

制限事項

以下の場合、ストレージゾーンコントローラーの名前変更や削除はできません。

- **ShareFile** データ移行が進行中です -ストレージゾーンを削除する前に、データ移行を完了してください。
- **ShareFile** データがゾーンに存在します。ストレージゾーンを削除する前に、既存のデータをすべて移行または削除してください。

ストレージキャッシュ操作のカスタマイズ

ShareFile ユーザーリクエストは、ストレージゾーンコントローラーで管理されます。これには、ファイルのアップロード、ダウンロード、削除が含まれます。次に、ストレージゾーンコントローラは、接続されたストレージと通信します。たとえば、接続されたストレージがサポートされているサードパーティ製ストレージシステムで、ShareFile ユーザーがファイルをアップロードした場合、ShareFile クライアントはファイルを永続ストレージキャッシュに送信します。ストレージゾーンコントローラー は、サードパーティのストレージシステムにファイルをアップロードします。

ストレージゾーンコントローラー は、`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`で構成可能な設定を使用して永続ストレージキャッシュを管理します。ここでは、サポートされているサード・パーティ製ストレージ・システムに固有の設定について説明します。

アップロードされたファイルの場合:

- ストレージゾーンコントローラー は、アップロードされたファイルを永続ストレージキャッシュ (persistentStorage フォルダー) に配置します。
- サービスの削除操作のタイミングは、次の設定によって制御されます。
  - `MinDeletionAge` はファイルが最後にアクセスされてから削除できるようになるまでの最小時間を指定します。デフォルトは 1 日です。最小設定は 8 時間です。
  - `OffPeakTimeOfDayStart`と`OffPeakTimeOfDayEnd`はファイル削除の開始時刻と終了時刻を指定します。デフォルトは午前 2 時と午前 4 時です。
  - `ProducerTimerInterval`と`DeleteTimerInterval`はサービスの削除操作の頻度を制御できます。デフォルト値 (1 日) がお客様のサイトに適切でない場合は、サポートにお問い合わせください。
- 削除サービスは、暗号化キーやキューに格納されたファイルなどの一時アイテムを含むフォルダも管理します。削除サービスでは、アイテムが作成されてから 24 時間後に削除されます。

- サポートされるサードパーティ製ストレージ・システムのみ:
  - 削除サービスは、ストレージキャッシュ内のファイルに、サポートされているサードパーティストレージに対応する BLOB があるかどうかを判別します。
  - デフォルトでは､ストレージキャッシュがディスクしきい値の 10 GB(CheckSizeThreasholdTimer) を超えているかどうかが、削除サービスが 10 秒（DiskSpaceDropoutThresholdGB) ごとに判断します。しきい値を超えると、削除サービスは過去 1 時間以内にアクセスされていないファイルを削除します (CacheCleanupFileThreasholdPeriodUnExpected)。削除サービスは通常のスケジューリングの結果として実行されます (ディスクサイズがしきい値に達したからではありません)。BLOB がサポート対象のサードパーティストレージにある場合、サービスは過去 24 時間以内にアクセスされていないファイルを削除します (CacheCleanupFileThresholdPeriodNormal)。BLOB がサードパーティストレージにない場合、ファイルはストレージキャッシュに残ります。

ダウンロードしたファイルの場合:

- ストレージゾーンコントローラー がダウンロード要求を受け取ると、ファイルが存在する場合、永続ストレージキャッシュからファイルをダウンロードします。ファイルがそのキャッシュにない場合、コントローラはサード・パーティ製ストレージ・システムからパーシステント・ストレージ・キャッシュにファイルをダウンロードします。削除サービスは、過去 24 時間アクセスされていないファイル (cacheCleanupFileThresholdPeriodNormal) を削除します。

削除されたファイルの場合:

- 削除サービスは、ShareFile アプリケーションから、45 日前（ピリオド）に削除されたファイルのリストを取得します。
- 削除サービスは、ストレージの場所から対応するファイル、またはサードパーティストレージから対応するオブジェクトを削除します。

サービスのデフォルト期間の削除

サービスの削除タイマーは 45 日に設定されます。45 日のデフォルト期間は、以前の設定をすべて上書きします。

> 注:
>
> 削除期間が 45 日未満に設定されている場合は、サポートに連絡して、アイテムがごみ箱に表示される日数を減らして、両方の期間が同じになるようにしてください。

1. デフォルトの期間を変更するには、次の場所で FileDeleteService.exe.config を編集します。C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc
   - <!--No. of days to keep data blob in active storage after deletion-->
   - <add key="Period"value="45"/>

ストレージゾーンコネクタの作成と管理

April 27, 2021

ストレージゾーンコネクタは、次のドキュメントおよびフォルダへのアクセスを提供します。

- SharePoint サイト、サイトコレクション、およびドキュメントライブラリ
- ネットワークファイル共有
- Documentum コネクタ (SZC 4.1 以降が必要)

接続されたリソースを表示する権限を持つユーザーは、ShareFile Web インターフェイスおよび ShareFile クライアントから、接続された SharePoint サイト、SharePoint ライブラリ、およびネットワークファイル共有を参照できます。

デフォルトでは、ShareFile Web インターフェイスのコネクタの参照は無効になっています。コネクタの参照を有効にするには、ShareFile サポートにお問い合わせください。

Active Directory のルックアップに使用するドメインコントローラをユーザーが指定できる追加設定を使用できます。この記事の「認証」セクションを参照してください。 この設定には、SZ 4.1 以降が必要です。

コネクタのシステム要件

ストレージゾーンコネクタは、デバイス間でのドキュメントの共有またはフォルダ同期をサポートしていません。

コネクタには一意の表示名が必要です。ユーザーは、アカウントの別の場所で使用中のコネクタ名を使用できません。

ストレージゾーンコネクタを作成する権限

コネクタを作成および管理するには、管理者または従業員ユーザーに次の権限が必要です。

- コネクタを作成、管理する
- ルートレベルフォルダーを作成する

SharePoint 用のストレージゾーンコネクタを作成するには

前提条件

- ShareFile Data にストレージゾーンを使用している場合は、コネクタに使用するゾーンを作成します。

次の手順では、ShareFile Web インターフェイスからストレージゾーンコネクタを作成する方法について説明します。ShareFile ユーザーは、SharePoint サイトの URL を入力して、サポートされているデバイスからコネクタを作成することもできます。

1. ShareFile アカウントに、コネクタの作成と管理権限で管理者としてサインインします。
2. [管理者設定**] > [**コネクタ**]** に移動します。
3. SharePoint コネクタの種類の [追加] をクリックします。
4. ShareFile データにストレージゾーンを使用している場合は、コネクタのゾーンを選択します。

   コネクタのゾーンは、SharePoint サーバーと同じドメイン内にあるか、SharePoint サーバーとの信頼関係が必要です。複数のドメインに SharePoint サーバーがあり、ドメイン間の信頼を構成できない場合は、ドメインごとに Storage Zone Controller を作成します。
5. [サイト] には、SharePoint ルートレベルのサイト、サイトコレクション、またはドキュメントライブラリの URL を次のフォームで指定します。

   - SharePoint ルートレベルのサイトへの接続例: `https://sharepoint.company.com`

     ルートレベルのサイトに接続すると、ユーザーはルートレベルの下にあるすべてのサイト (サイトコレクションではなく) およびドキュメントライブラリにアクセスできます。ShareFile は、ユーザーから SharePoint システムフォルダを非表示にします。
   - SharePoint サイトコレクションへの接続例: `https://sharepoint.company.com/site/SiteCollection`

     サイトコレクションに接続すると、ユーザーはそのコレクション内のすべてのサブサイトにアクセスできます。
   - SharePoint 2010 ドキュメントライブラリへの接続例:
     - `https://mycompany.com/sharepoint/`
     - `https://mycompany.com/sharepoint/sales-team/Shared Documents/`
     - `https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx`
   - SharePoint 2013 ドキュメントライブラリへの接続例:

     既定の SharePoint 2013 URL (最小ダウンロード戦略が有効になっている場合) は、`https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`の形式です。
   - 認証されたユーザーの NetBIOS 名にリダイレクトする接続の例:

     認証されたユーザーのログオン名をそのユーザーの NetBIOS 名で置き換えるには、変数%UserDomain% を使用します。新しい変数を使用すると、`https://example.com/%UserDomain%\\_%UserName%/Documents`などの URL へのサイトレベルのコネクタを作成できます。
   - 「個人用サイト」または OneDrive for Business に接続する場合の接続例:

SharePoint 個人用サイトに接続するときに、選択した特殊文字を自動的に解決するには、%URLusername% 変数を使用します。この変数は、スペースを%20、ピリオドをアンダースコアに置き換えます。%URLusername% 変数の使用には SZ v3.4.1 が必要です。

ユーザーの「domain\username」が「acme\rip.van winkle」の場合、

`https://sharepoint.acme.com/personal/%URLusername%`
は以下のように解決されます。
`https://sharepoint.acme.com/personal/rip van%20winkle`

6. コネクタのわかりやすい名前を入力します。

   この名前は、SharePoint サイトをユーザーに識別するために使用されます。小さな画面のモバイルデバイスでもよく表示されるように、名前は簡潔にする必要があります。

7. [コネクタを追加] をクリックします。[フォルダアクセスの表示/編集] ダイアログボックスが表示されます。

8. コネクタを他のユーザーに表示するには:[フォルダアクセスの表示/編集] で、ユーザーと配布グループを追加し、[変更の保存] をクリックします。

   この手順では、コネクタがユーザーに表示されるかどうかだけを決定します。ストレージゾーンコネクタは、**SharePoint** サーバーからアクセス許可を継承します。

SharePoint メタデータのタグ付けを有効にするには

Storage Zone Controller を構成するときは、SharePoint コネクタが有効になっていることを確認します。

メタデータのタグ付けは、SharePoint 2013 以降のモバイルクライアントでサポートされています。

> 注:
>
> en-us のみ。

ネットワークファイル共有用のストレージゾーンコネクタを作成するには

前提条件

- ShareFile Data にストレージゾーンを使用している場合は、コネクタに使用するゾーンを作成します。
- ネットワーク共有コネクタが Chrome、Edge、および Firefox の最新バージョンで動作するには、ご使用の環境に最新の.NET 更新プログラムを適用します。詳しくは、「.NET フレームワークで SameSite をサポートする KB 記事」を参照してください。これをすべてのストレージゾーンコネクタに適用します。これは、ブラウザの最新バージョンを考慮して、sameSite 属性を Cookie に設定できるようにするために必要です。
- バージョン 5.10.1 以降を使用する場合は、すべてのストレージゾーンコネクタで C:\inetpub\wwwroot\Citrix\StorageCe ファイルの<`system.web`>タグ内に<`httpCookies sameSite="None"requireSSL="true"`/>を追加します。これは、ブラウザの最新バージョンを考慮して、sameSite 属性を Cookie に設定できるようにするために必要です。

次の手順では、ShareFile Web インターフェイスからコネクタを作成する方法について説明します。ShareFile ユーザーは、ファイル共有のパスを入力して、サポートされているデバイスからコネクタを作成することもできます。

1. コネクタの作成と管理権限を持つ管理者として ShareFile アカウントにログオンします。
2. [管理者設定**] > [**コネクタ**]** に移動します。
3. [ネットワーク共有] コネクタの種類の [追加] をクリックします。
4. ShareFile データにストレージゾーンを使用している場合は、コネクタのゾーンを選択します。

   コネクタのゾーンは、ファイル共有と同じドメイン内にあるか、またはファイル共有との信頼関係が必要です。複数のドメインにファイル共有があり、ドメイン間の信頼を構成できない場合は、ドメインごとに Storage Zone Controller を作成します。
5. [パス] に、UNC パスを入力します。

   FQDN の例: \\fileserver.acme.com\shared

   UNC パスでは、次の変数を使用できます。

   - %UserName%

     ユーザーのホームディレクトリにリダイレクトします。パスの例: \\myserver\homedirs\%UserName%
   - %HomeDrive%

     Active Directory プロパティの [ホームディレクトリ] で定義されているユーザーのホームフォルダーパスにリダイレクトします。パスの例: %HomeDrive%
   - %TSHomeDrive%

     Active Directory プロパティ ms-TS-Home-Directory で定義されているように、ユーザーのターミナルサービスのホームディレクトリにリダイレクトします。この場所は、ユーザーがターミナルサーバーまたは Citrix XenApp サーバーから Windows にログオンするときに使用されます。パスの例: %TSHomeDrive%

     Active Directory ユーザーとコンピュータスナップインでは、ユーザーオブジェクトの編集時に [リモートデスクトップサービスプロファイル] タブで MS-TS-Home-Directory 値にアクセスできます。
   - %UserDomain%

     認証されたユーザーの NetBIOS ドメイン名にリダイレクトします。たとえば、認証されたユーザーのログオン名が「abc\ johnd」の場合、変数は「abc」に置き換えられます。パスの例: \\myserver\%UserDomain%_%UserName%

   変数は大文字と小文字を区別しません。

   重要:ShareFile データの格納場所へのコネクタを作成しないでください。ユーザーの権限によっては、ユーザーがすべての ShareFile データを削除できるようになります。

6. コネクタのわかりやすい名前を入力します。

   この名前は、ユーザーに対するファイル共有を識別するために使用されます。小さな画面のモバイルデバイスでもよく表示されるように、名前は簡潔にする必要があります。

7. [コネクタを追加] をクリックします。[フォルダアクセスの表示/編集] ダイアログボックスが表示されます。
8. コネクタを他のユーザーに表示するには:[フォルダアクセスの表示/編集] で、ユーザーと配布グループを追加し、[変更の保存] をクリックします。

   この手順では、コネクタがユーザーに表示されるかどうかだけを決定します。ストレージゾーンコネクタは、ネットワーク共有からアクセス許可を継承します。読み取り/書き込みアクセスのアクセス許可は、ネットワーク共有のセキュリティ設定によって決定され、**ShareFile** プランの影響も受けます。

ネットワークファイル共有でファイルのチェックインとチェックアウトを有効にするには

前提条件

Storage Zone Controller バージョン 5.8 およびネットワークファイル共有コネクタを構成する必要があります。

手順

1. Storage Center にサインインします。設定ページが表示されます。
2. 設定ページで [変更] をクリックします。
3. ネットワークファイル共有の **[**チェックインとチェックアウトを有効にする**]** チェックボックスをオンにします。
4. ユーザーとネットワーク共有が配置されているドメインの名前を入力します。
5. サービスアカウントのユーザー名とパスワードを入力します。このサービスアカウントは、ネットワーク共有の場所に存在するすべてのファイルとフォルダに対する読み取りおよび書き込みアクセス権を持っている必要があります。

Documentum のストレージゾーンコネクタを作成するには

> 注:
>
> Documentum コネクタのセットアップでは、基本認証のみがサポートされています。Documentum Content Server では大文字と小文字が区別されるため、Documentum Content Server で大文字と小文字の区別が無効になっている場合を除き、認証時に入力したユーザー名は大文字と小文字を区別する資格情報と一致する必要があります。

前提条件

1. ストレージゾーンコントローラ 5.3 以降

2. Documentum ECM 設定は、ShareFile カスタマーサポートによって有効になっています。
3. Documentum レストサービスは、Documentum サーバ上に展開する必要があります。「Documentum Rest サービスについて詳しくは、ここをクリックしてください。」を参照してください。
4. Citrix ADC を使用する場合は、特定の構成変更が必要です。これらの変更については、この記事でさらに詳しく説明します。

ShareFile カスタマーサポートでこの機能が有効になったら、Storage Zone Controller に移動し、ストレージゾーンのコネクタメニューを探します。「既存の ECM（Enterprise Content Management）データソースへのアクセスを有効にする」のチェックボックスをクリックします。変更を保存します。

次に、ShareFile Web アプリケーションにサインインし、**[**管理者設定**] > [**コネクタ**]** に移動します。

Documentum コネクタタイプの横にある [追加] ボタンをクリックします。

EMC サーバのパスを指定し、コネクタの名前を入力します。Continue-

次に、Documentum コネクタへのアクセス権をユーザーに付与します。

コネクタを作成したら、Web アプリとモバイルアプリからアクセスできます。

サポートされているアクション

モバイル（iOS/Android/ユニバーサル Windows プラットフォーム）:

- ブラウジング
- ファイルのアップロード/ダウンロード
- ファイルとフォルダの作成/削除
- オフライン編集

WebApp

- コネクタの作成
- ブラウジング
- ファイルのアップロード/ダウンロード
- フォルダの作成/削除

未サポート

- Documentum コネクタに格納されたファイルの共有
- パスのホワイトリスト/ブラックリスト

> 注:
>
> Documentum Content Server では大文字と小文字が区別されるため、Documentum Content Server で大文字と小文字の区別が無効になっている場合を除き、認証時に入力したユーザー名は大文字と小文字を区

> 別する資格情報と一致する必要があります。

Documentum コネクタの **Citrix ADC** 構成

ご使用の環境で Citrix ADC を使用する場合は、Citrix ADC 構成に次の変更を加えます。

1. [コンテンツスイッチング] > [ポリシー] の [_SF_CIFS_SP] ポリシーに次の項目を追加します。

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

2. [コンテンツスイッチング] > [ポリシー] の _SF_SZ_CSPOL ポリシーに以下を追加します。

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

コネクタ名を変更するには

コネクタ名は、SharePoint サイトまたはネットワークファイル共有をユーザーに対して識別するために使用されます。

1. ShareFile アカウントに管理者としてサインインし、[コネクタ] タブをクリックします。
2. [タイトル] 列で、コネクタ名をクリックします。
3. コネクタのわかりやすい名前を入力し、[保存] をクリックします。

コネクタを削除するには

コネクタを削除しても、SharePoint またはネットワークファイル共有からデータは削除されません。

1. ShareFile アカウントに管理者としてサインインし、[コネクタ] タブをクリックします。
2. コネクタのチェックボックスをオンにし、[削除] をクリックし、[**OK**] をクリックします。

コネクタ認証

管理者ユーザーは、次の設定を使用して、CIFS または SP 認証の AD ルックアップを実行するときに使用するドメインコントローラーを指定できるようになりました。

```
<add key="Domaincontrollers"value="DC01,dc02.domain.com,123.456.789.1
"/>
```

上記の「Value=」は、ホスト名、FQDN、または IP アドレスで識別される 1 つの DC または複数の DC に設定できます。複数の DC は、カンマまたはセミコロンで区切る必要があります。

複数の DC が指定されている場合、ルックアップは最初の DC に対して実行されます。エラーが発生した場合は、2 番目の DC が使用されます。

上記のプロパティは、すべての Storage Zone Controller IIS アプリケーション（CIFS、SP、ProxyService を含む）に継承されるように、`C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config`に追加できます。

新しいアプリ設定が存在しない場合、DC を自動的に選択する既定の動作が続行されます。

ネットワーク共有/ **SharePoint** コネクタから直接リンクを取得する

ユーザーは、ShareFile for iOS または ShareFile for Android の最新バージョンを使用している間、ネットワーク共有/SharePoint コネクタから「ダイレクトリンクを取得」できるようになりました。

管理者がこの機能を無効にしたい場合は、次の項目を追加して無効にすることができます。

```
<add key="disable-direct-link"value="1"/>
```

上記は、`C:\inetpub\wwwroot\Citrix\StorageCenter\sps\AppSettingsRelease.config`に追加することができます。

基本認証とローカライズされたユーザー名

基本認証では、非 ASCII 文字はサポートされていません。ローカライズされたユーザー名を使用する場合は、ユーザーが NTLM および Negotiate を利用することをお勧めします。

データ損失防止

May 28, 2024

ShareFile のデータ漏えい防止 (DLP) 機能を使用すると、ファイル内のコンテンツに基づいてアクセスと共有を制限できます。

インラインコンテンツスキャン用の標準ネットワークプロトコルである ICAP をサポートするサードパーティの DLP セキュリティスイートを使用して、ストレージゾーンにアップロードされたドキュメントをスキャンできます。次に、DLP スキャンの結果と、アクセスを厳密に制御する設定に基づいて、共有とアクセス権を調整します。

サポートされている **DLP** システム

Storage Zones Controller は、ICAP プロトコルを使用してサードパーティの DLP ソリューションと通信します。ShareFile を既存の DLP ソリューションで使用する場合、既存のポリシーまたはサーバーを変更する必要がありま

せん。ただし、負荷が大きいと予想される場合は、ShareFile データを処理するために ICAP サーバー専用にすることもできます。

一般的な ICAP 準拠の DLP ソリューションは次のとおりです。

- Symantec Data Loss Prevention
- マカフィー DLP プリベント
- Websense TRITON AP-DATA

ShareFile は既存の DLP セキュリティスイートを使用するため、データ検査とセキュリティアラートのための単一のポリシー管理ポイントを維持できます。送信メールの添付ファイルまたは Web トラフィックをスキャンして機密データをスキャンするために前述のソリューションをすでに使用している場合は、ShareFileStorage Zones Controller を同じサーバーに指定できます。これらの既存の DLP システムでは、基盤となる DLP システム自体が ICAP をサポートしている場合は、セキュリティで保護された ICAP (ICAPS) もサポートします。

DLP を有効にする

ShareFile と Storage Zones Controller の DLP を有効にするには、次の 3 つのアクションを実行します。

1. ShareFile アカウントで DLP 機能を有効にします。
2. Storage Zones Controller サーバーで DLP を有効にします。
3. ファイル分類ごとに許可されるアクションを設定します。

これらのアクションについては、以降のセクションで詳しく説明します。

ShareFile アカウントで DLP 機能を有効にする

ShareFile サブドメインが DLP に対応していることをリクエストまたは確認するには、Citrix サポートにリクエストを送信してください。

一部のアカウントでは、DLP を有効にするために ShareFile Web サイトの新しいユーザーエクスペリエンスを有効にする必要もあります。アカウントで DLP を有効にしたら、Storage Zone Controller サーバーで DLP を有効にできます。

Storage Zones Controller サーバーで DLP を有効にする

以下の手順に従って、Storage Zone Controller 展開で DLP 設定を構成します。

1. Storage Zones Controller5.3 以降をインストールするか、アップグレードします。
2. Storage Zone Controller コンソールhttp://*localhost*/configservice/login.aspxで、[**ShareFile Data**] タブをクリックします。ゾーンが存在する場合は、[修正] をクリックします。

3. [**DLP** 統合を有効にする] チェックボックスをオンにし、[ICAP **REQMOD URL]** フィールドに **DLP** サーバーの **ICAP** アドレスを入力します。アドレスの形式は次のとおりです。

```
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. [保存] または [登録] をクリックします。

DLP を有効にした後で、[**Monitoring**] タブの [DLP **ICAP** サーバーステータス**]** エントリをチェックして、**DLP** サーバに到達できることを確認します。

DLP スキャン結果に基づいてアクセスを制御する

アカウントと Storage Zones Controller で DLP を有効にすると、DLP が有効なストレージゾーンにアップロードされたすべてのファイルのすべてのバージョンがスキャンされ、機密コンテンツがないかスキャンされます。スキャンの結果は、データ分類として ShareFile データベースに保存されます。

DLP 設定は、DLP 分類に基づいて、ファイルで使用できる通常のアクセス許可と共有コントロールを制限します。ドキュメントを共有する場合、DLP 設定で匿名で共有できる場合でも、ユーザーは匿名アクセスをブロックすることができます。しかし、ユーザーが DLP 設定に違反するような方法でファイルを共有しようとすると、ShareFile は共有できないようにします。

データの分類は次のとおりです。

- スキャン済み: OK —DLP システムによってスキャンされ、OK に合格したファイル。
- スキャン済み**:** 拒否—DLP システムによってスキャンされ、機密データが含まれていることが判明したファイル。
- **Unscanned** —スキャンされていないファイル。

スキャンされていない分類は、Citrix で管理されるストレージゾーン、または DLP が有効になっていないその他のストレージゾーンに格納されているすべてのドキュメントに適用されます。この分類は、DLP が構成される前にアップ

ロードされた DLP 対応のストレージゾーン内のファイルにも適用されます。この分類は、外部 DLP システムが使用できないか、応答が遅いため、スキャンを待機しているファイルにも適用されます。

各項目の分類は、ICAP サーバーの応答規則によって決定されます。DLP ICAP サーバーがコンテンツをブロックまたは削除する必要があるというメッセージで応答した場合、ファイルは「スキャン済み**:** 拒否」としてマークされます。それ以外の場合は、ファイルは「スキャン済み**:OK**」とマークされます。

データ分類ごとに、異なるアクセス制限と共有制限を設定できます。3 つのカテゴリのそれぞれについて、ShareFile 管理者は許可するアクションを選択します。

- 従業員はファイルをダウンロードまたは共有できます。
- サードパーティクライアントユーザーは、ファイルをダウンロードまたは共有できます。クライアント共有はデフォルトでは無効になっていますが、[管理**] > [**詳細設定**] > [**クライアントにファイル共有を許可する] で有効にできます。
- 匿名ユーザーはファイルをダウンロードできます

ユーザーがファイルを共有すると、ダウンロード権限を持つユーザーのみがファイルを受信できます。したがって、データ分類の共有アクセス許可を有効にする場合は、少なくとも 1 つのクラスのユーザーダウンロードアクセス許可を付与する必要があります。

ShareFile で **DLP** 設定を構成するには

1. ShareFile Web インターフェイスで、[管理**] > [**情報漏えい防止] の順にクリックします。
2. [コンテンツに基づいてファイルへのアクセスを制限する] のオプションを **[**はい**]** に変更します。
3. データ分類ごとに許可されるアクションを設定します。

> 重要:
>
> ShareFile On-Demand Sync ツールでは、通常の操作ではダウンロード権限が必要です。展開環境に ShareFile On-Demand Sync が含まれている場合は、すべてのコンテンツ分類で従業員のダウンロードを有効にします。

Storage Zones Controller が DLP システムにファイルを送信すると、ファイルの所有者を示すメタデータが含まれます。このファイルには、ShareFile 内のファイルが存在するフォルダパスも含まれます。DLP サーバー管理者は、この情報を使用して、機密コンテンツを含むファイルに関する ShareFile に固有の詳細を表示できます。

DLP の詳細設定

DLP スキャンプロセスを調整するには、`wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`にある Storage Zones Controller にある設定ファイルを編集します。次の表では、DLP に関連する各設定について説明します。

設定	説明	デフォルト値
スキャン間隔	DLP サービスが DLP キューをチェックして新しいファイルを処理するために DLP ICAP サーバーに送信する頻度。	30 秒
ICAP 応答タイムアウト	Storage Zones Controller が ICAP 応答を待ってから ICAP サーバーを使用不可とマークするまでの時間。	30 秒
ICAP エクスクルードエクステンション	DLP スキャンから除外する拡張機能のコンマ区切りのリスト。DLP サーバーは、これらの拡張子の 1 つで終わる名前のファイルを処理しませんが、ファイルを Scanned: OK としてマークします。例値:「exe, jpg, bin, mov」	なし
ICAP 最大ファイルサイズバイト数	DLP サーバーに送信して処理するファイルの最大サイズ (バイト単位)。値 0 は、最大値が存在せず、すべてのファイルサイズが送信されることを意味します。ゼロ以外の値で構成すると、DLP サーバーは構成されたサイズより大きいファイルを処理しませんが、スキャン済み:OK としてマークされます。	31457280 (30 メガバイト)
処理対象の X キューアイテム	スキャン間隔ごとにスキャンするキューアイテムの最大数。StorageZone に多数のファイルが追加された場合に DLP サーバへの影響を軽減するには、この値を小さくします。	512
最大キュー処理スレッド数	DLP スキャンキューの排出に使用する同時プロセッサスレッドの最大数。この値は、ICAP サーバーに許可される同時接続の最大数に基づいて設定します。同じ ICAP サーバーを使用する他のネットワークサービスがブロックされないようにするには、妥当な制限内にする必要があります。	4

設定	説明	デフォルト値
ICAP-ReqMod-HTTP リクエスト動詞	デフォルトでは、ネットワーク呼び出しは PUT 動詞で行われます。必要に応じて、この設定を POST に変更することもできます。	PUT

DLP 既存ファイルツール

ShareFileStorage Zones Controller は、ICAP を通じてストレージセンターをデータ損失防止（DLP）プロバイダーと統合するオプションを提供します。

ただし、ICAP サービスは、新しく作成されたファイルによってのみ入力されるキューを介して動作します。つまり、ICAP が有効になる前にゾーンに存在するファイルは、サービスによってスキャンされません。このツールは、スキャンのためにそれらのファイルをキューに入れるのに役立ちます。また、再スキャンのためにスキャンされたファイルをキューに入れることもできます。

名前のとおり、ツールは DLP ICAP サービスに対してのみ機能します。

要件

このツールは PowerShell スクリプトであるため、PowerShell を実行する必要があります。ネットワーク共有の場所にアクセスするには、スクリプトをネットワークサービスとして実行する必要があるため、PsExec または同様のツールも必要です。

位置情報

インストールされている Storage Zones Controller については、ツールが`<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1`にあります。Storage Zones Controller のインストール場所はデフォルトで`C:\inetpub\wwwroot\Citrix\StorageCenter`です。

ツールを実行前の考慮事項

次の条件に応じて、ツールを 1 回の操作で複数回実行する必要がある場合があります。

- キューサイズの制限について提供される制限。
- 指定された条件に対する項目の数。キューサイズの制限が 0 以下に設定されていない限り、この考慮事項は真です。この場合、ツールはキューディレクトリ内の項目の最大サイズを 200,000 と仮定します。

たとえば、スキャンされていないアイテムをキューに入れるためにツールが使用されている場合、キューサイズの制限は 500 項目に設定されます。500 個を超えるスキャンされていない項目がある場合、500 項目がキューに満杯になった後、ツールは停止します。ツールは停止した場所を追跡するために、最後に取得したアイテムの作成日を格納します。このツールは、日付を <storage zones controller installation location>\SC にあるテンポラリファイルに dlpExistingFiles-EndDate.temp という名前で保存します。

各実行前に、ツールはこのファイルを検索します。ファイルが存在する場合、ツールはそのファイルの次のバッチのマーカーとして作成日を使用します。ツールは、特定の操作の完了時に一時ファイルを削除しません。代わりに、ゾーン管理者は、特定の操作のすべてのバッチが完了すると、ファイルを削除できます。このような状況では、完全な操作が完了すると、別の操作を実行する前に、一時ファイル (存在する場合) を手動で削除する必要があります。

PSExec でツールを実行する

コマンドウィンドウを開き、次のコマンドを使用して PSExec を実行します。

```
PsExec.exe -i -u "nt authority\network service"

"C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
```

これにより、ネットワークサービスとして実行される PowerShell が開きます。ネットワークサービスとして実際に実行されていることを確認するには、**whoami** を実行し、結果を確認します。

PowerShell が開いたら、そこでツールを直接実行し、必要なタスクを実行します。

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

コマンド・ライン・オプション

ツールの実行には、次のオプションを使用できます。

- **-runscan** (必須): このオプションは、スキャンのためにキューに入れるファイルの種類を指定するために使用されます。サブオプション:
  - **Unscanned**: スキャンされていないファイル。たとえば、スキャンされなかった以前の DLP 時代のファイルなどです。
  - **ScannedOK**: クリーンとマークされたスキャン済みファイル。
  - **ScannerdRejected**: クリーンではないとマークされたスキャン済みファイル。
  - **Scanned**: すべてのスキャンされたファイル。
- **-queueLimit** (オプション): このオプションは、ツールが停止する前にキューで許可される項目の数を指定するために使用されます。
- **-date** (オプション): スキャンのためにキューに入れられるアイテムの最大作成日。たとえば、日付が「2017/10/30 午前 11:30」と指定されている場合、この日付/時刻より前に作成されたファイルだけがスキャンのためにキューに入れられます。

例:

すべての例については、**PSExec** を通じてネットワークサービスとして **PowerShell** を開きます。手順については、この記事の前の手順を参照してください。

ゾーン内のスキャンされていないアイテムをキューに入れるには、次のコマンドを実行します。

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

キュー制限が 100 のゾーン内でスキャンされたすべてのアイテムをキューに入れるには、次のコマンドを実行します。

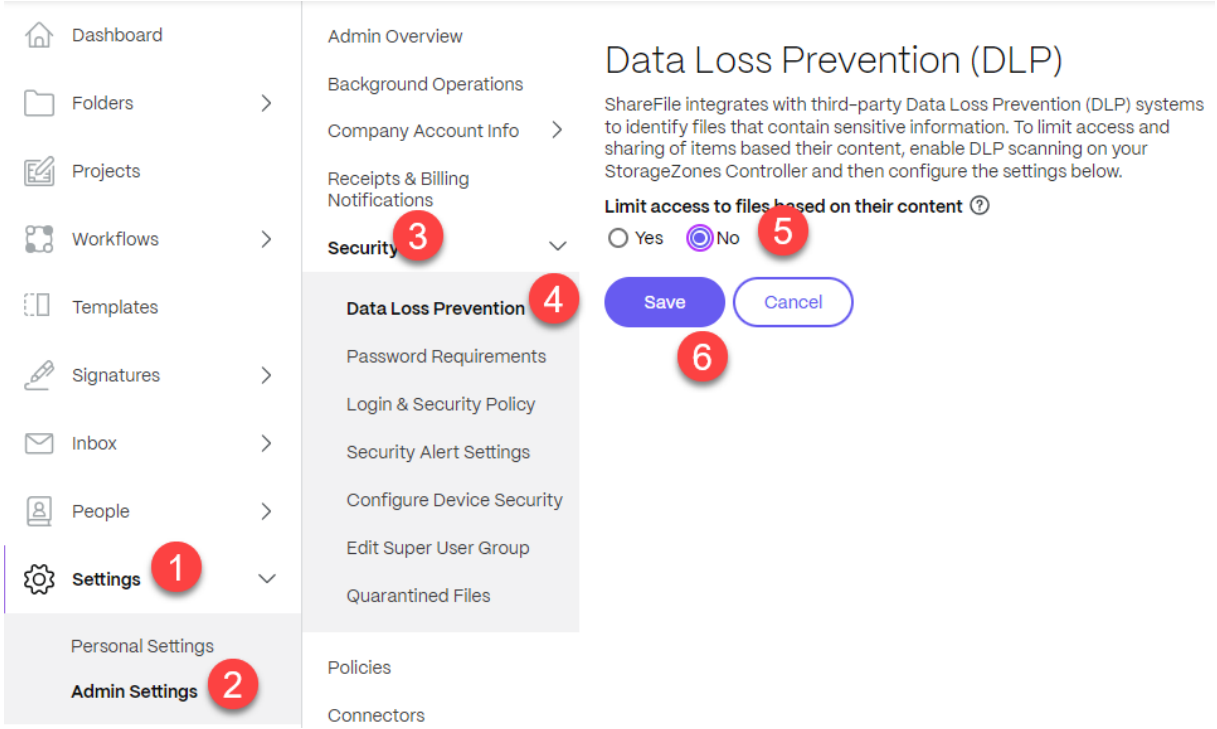
```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Scanned -queueLimit 100
```

2017 年 10 月 30 日午前 11 時 30 分以前に作成されたすべてのスキャン済みアイテムを次の特性でキューに入れるには、キュー制限が 200 のゾーンで、クリーンとしてマークされ、次のコマンドを実行します。

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

DLP を無効にする

ShareFile と StorageZone コントローラーの DLP を無効にするには、次の操作を実行します:



1. Sharefile アカウントにログインし、[設定] をクリックします。
2. 開いたドロップダウンリストから、[管理者設定] を選択します。
3. 開いたメニューから [セキュリティ] をクリックします。
4. [セキュリティ] メニューから、[データ損失防止] オプションを選択します。
5. DLP 画面から、「コンテンツに基づいてファイルへのアクセスを制限する」セクションに移動し、「いいえ」をクリックします。
6. ［**Save**］を選択します。

監視

February 14, 2022

ストレージゾーンコントローラー と ShareFile 管理者インターフェイスには、ストレージゾーンコントローラー アクティビティの監視と問題のトラブルシューティングに役立ついくつかのリソースが含まれています。

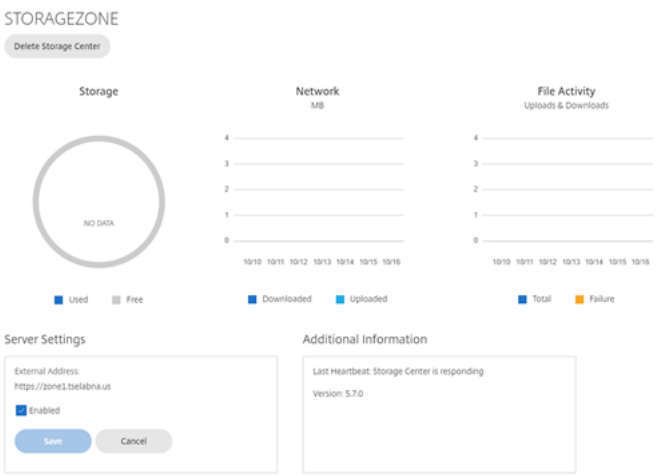
- コンポーネントの全般ステータス—ストレージゾーンコントローラー コンソールの [モニタリング] タブには、トラブルシューティングプロセスの開始に役立つコンポーネントのステータスが表示されます。ステータスは、アクセス許可、サービスステータス、ShareFile コントロールプレーンへのストレージゾーンコントローラーアウトバウンド接続を示すハートビートステータスなどの項目に対して提供されます。

  ストレージゾーンコントローラー は 5 分ごとに更新を ShareFile Web アプリケーションに送信します。ShareFile Web アプリケーションが 10 分以内に更新を受信しない場合、ストレージゾーンコントローラーはオフラインとしてマークされます。

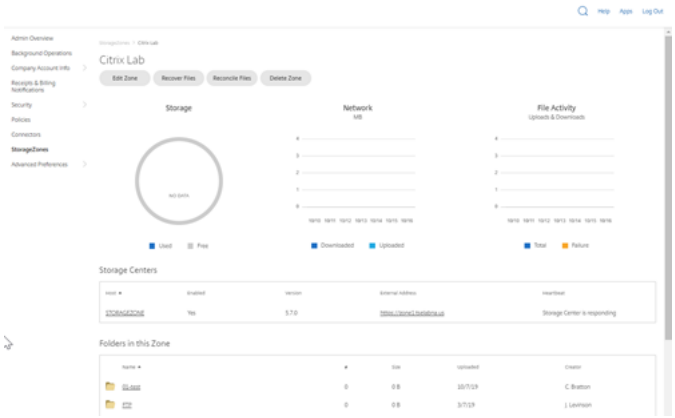
  [Monitoring] タブの項目が赤で表示されている場合は、ログファイルを確認して詳細情報を確認します。

  [Monitoring] タブには、ストレージゾーンが接続に関して機能しているかどうかは表示されません。これには、ShareFile コントロールプレーンが外部ストレージゾーンの URL に到達できるかどうか、またはクライアントがゾーンに到達できるかどうかが含まれます。

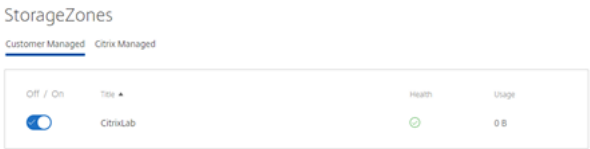
- ストレージゾーンコントローラー サーバー情報—サーバーのストレージ使用量、ネットワーク使用量、ファイルアクティビティに関する情報:ShareFile インターフェイスから、ShareFile Enterprise アカウントにログオンし、[管理者**] > [StorageZones**] に移動し、ストレージゾーンをクリックし、ストレージをクリックします。ゾーンコントローラのホスト名。



- ゾーン情報—ゾーンのストレージ使用量、ネットワーク使用量、ファイルアクティビティについては、ShareFile インターフェイスから ShareFile Enterprise Enterprise アカウントにログオンし、[管理者] **> [StorageZones]** に移動し、ゾーン名をクリックします。



- ストレージゾーンコントローラーのヘルスステータス—ShareFile.com がゾーンに参加しているストレージゾーンコントローラー からハートビートメッセージを受信しているかどうかを確認するには、ヘルスステータスを表示します。ShareFile インターフェイスから、ShareFile Enterprise アカウントにログオンし、[管理] **> [StorageZones]** に移動します。で、[Health] 列に緑色のチェックマークが付いていることを確認し、サイト名をクリックして、ストレージゾーンコントローラー が応答していることをハートビートメッセージに示していることを確認します。



- ログファイル—ログファイルには、次のセクションで説明するように、ストレージゾーンコントローラー の構成とそのコンポーネントに関する詳細情報が表示されます。

ログファイル

ストレージゾーンコントローラの次のログファイルは、デフォルトでにあります `C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`。

ログファイル名	次のログ情報が含まれます。
cfgsrv-%date%.txt	既存のストレージゾーン設定の変更、新しいストレージゾーンの作成、新しいストレージゾーンコントローラーを既存のプライマリストレージゾーンコントローラー に参加させるなど、ストレージゾーンコントローラー 設定アクション
sc-%date%.txt	標準ゾーンの ShareFile データのアップロードおよびダウンロードアクティビティ
CIFS-%Date%.txt	ネットワークファイル共有のストレージゾーンコネクタアップロードおよびダウンロードアクティビティ
sharepoint-%date%.txt	SharePoint アップロードおよびダウンロードアクティビティ用のストレージゾーンコネクタ
クラウドストレージアップローダー-%date%.txt	クラウドストレージアップローダサービス（サポートされているサードパーティ製ストレージシステムへ）
copy-%date%.txt	ShareFile コピーサービス
削除-%date%.txt	ShareFile クリーンアップサービス、永続ストレージキャッシュ用
s3uploader-%date%.txt	ShareFile 管理サービス。ハートビートステータスメッセージを含む

拡張ログは次の各コンポーネントで使用でき、サポートするために詳細な情報を提供する必要がある場合に役立ちます。

コンポーネント	AppSettingsRelease.config の場所
ShareFile データ	C:\inetpub\wwwroot\Citrix\StorageCenter
ネットワークファイル共有用のストレージゾーンコネクタ	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
SharePoint 用のストレージゾーンコネクタ	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

拡張ログを有効にするには

次の手順では、すべてのストレージゾーンコントローラー コンポーネントおよびサービスの拡張ロギングを有効にします。

1. ストレージゾーンコントローラー サーバーで、IIS を開きます。
2. 既定の Web サイトに移動し、[アプリケーション設定] を開きます。
3. enable-extended-logging の値を 0 から 1 に変更します。
4. Citrix ShareFile 管理サービスを再起動します。
5. 問題を解決した後、ログの量を減らすために、拡張ログをクリアすることをお勧めします。

特定のコンポーネントの拡張ログを有効にするには、AppSettingsRelease.config ファイルを編集します。`<add key="enable-extended-logging"value="0"/>`の値を 0 から 1 に変更します。

また、IIS ログをチェックして、トラフィックがストレージゾーンコントローラに到達しているかどうかを確認することもできます。IIS ログには、すべての着信要求が表示されます。ストレージゾーンコントローラの IIS ログは c:\inetpub\logs\LogFiles\W3SVC1.

拡張 IIS ロギングを有効にするには、http://support.microsoft.com/kb/313437を参照してください。

インストールと設定のトラブルシューティング

問題	説明と解決策
ストレージゾーンコントローラー の構成中に「HTTP エラー 404-ファイルまたはディレクトリが見つかりません」が表示される	通常、このメッセージは IIS または ASP.NET. IIS ロールが Windows インストールで有効になっていること、および IIS でASP.NET機能が有効になっていることを確認します。
ストレージゾーンコントローラー で localhost を参照すると、「HTTP エラー 404.2 —見つかりません」が表示される	このメッセージは、の ISAPI および CGI 制限が [許可] ASP.NET に設定されていないことを示しています。
アップロードの試行後に「HTTP エラー 413-要求エンティティが大きすぎます」が表示される	メッセージは、ストレージゾーンへのアップロードに失敗した後にネットワークトレースに表示され、IIS のクライアント証明書設定から発生することがあります。この問題を回避するには、ストレージゾーンコントローラーサーバーで IIS を開きます。デフォルトの Web サイトに移動し、[SSL 設定] を開きます。[クライアント証明書] で、[無視] を選択します。Citrix ShareFile 管理サービスを再起動します。

問題	説明と解決策
ストレージゾーンコントローラー の構成中に IIS エラーが発生する	IIS エラーは通常、ASP.NET が完全に構成されていないことを示します。IIS マネージャの [ISAPI と CGI の制限] で、すべてのASP.NET一覧で [制限] が [許可] に設定されていることを確認します。ASP.NET が IIS に登録されていることを確認します。IIS マネージャの [アプリケーションプール] で、ASP.NET 一覧が表示されていることを確認します。手動で登録するには ASP.NET、この表の後のコマンドラインを参照してください。問題が引き続き発生する場合は、IIS とASP.NETセットアップを確認します。
ストレージゾーンコントローラー の構成中に「ストレージセンターバインディングの保存に失敗しました」と表示される	メッセージは、IIS アカウントプールユーザーのアクセス許可の問題を示します。既定では、アプリケーションプールは Network Service ユーザーアカウントで動作します。ストレージゾーンコントローラー は、デフォルトでネットワークサービスアカウントを使用します。ネットワークサービスアカウントの代わりに名前付きユーザーアカウントを使用する場合、名前付きユーザーアカウントには、プライベートデータ格納に使用されるネットワーク共有へのフルアクセス権が必要です。
ゾーンの構成中に「アクセスが拒否されました」が表示される	このメッセージは、ログオンしている ShareFile アカウントにゾーンを作成および管理する権限がない場合に発生することがあります。ShareFile 管理コンソールを使用して、その権限を設定します。
アウトバウンドリクエストはブロックされる	送信要求がブロックされると、cfgsrv ログに System.net.WebException が含まれます。リモートサーバーからエラー (403) Forbidden が返されました。この問題は、プロキシサーバーがアウトバウンド要求をブロックしていることが原因である可能性があります。ファイアウォールが、ストレージゾーンコントローラーシステム要件で指定された要件を満たしていることを確認します。

問題	説明と解決策
ストレージゾーンコントローラにログオンすると「リモートサーバーに接続できません」が表示される	このメッセージは、通常、プロキシの問題を示しています。プロキシ設定が構成されていることを確認します。プロキシ設定が正しい場合は、ストレージゾーンコントローラから ShareFile アカウントにログインできることを確認します。ストレージゾーンコントローラを構成するための管理者レベルのアクセス許可があり、ポート 443 が外部ファイアウォールで開いていることを確認します。
有効にし、ShareFile データのストレージゾーンを構成した後、ネットワーク共有上の ShareFileStorage という名前のフォルダーに SCKeys.txt が含まれません。	ストレージゾーンコントローラは、ストレージゾーンコントローラのインストールに使用したアカウントがアクセス制御リストに含まれていない場合を除き、インストール中に SCKeys.txt を作成します。アクセス制御リストを更新し、ストレージゾーンコントローラを再インストールします。
ゾーンを作成した後、共有フォルダーへのファイルのアップロードが失敗する	この問題は、内部 DNS に問題があることを示しています。ストレージゾーンコントローラー FQDN には、内部 DNS レコードと外部 DNS レコードの両方が必要です。
[監視] タブで、[ハートビート状態] が赤で表示されます	赤いアイコンは、ストレージゾーンコントローラが ShareFile Web サイトにハートビートメッセージを送信できないことを示します。他のコンポーネントのアイコンが赤であるかどうかを確認します。その場合は、ログを参照してください。s3uploader ログにハートビートの送信に失敗したことを示す場合、ストレージゾーンコントローラー サーバーがプロキシサーバーを経由しない限り、ShareFile Web サイトにアクセスできないことがあります。ストレージゾーンコントローラのプロキシサーバを指定するには、コントローラコンソールを開き、[ネットワーク] タブに移動します。ストレージゾーンコントローラー サーバーがネットワークサービスユーザーを使用して ShareFile Web サイトにアクセスできない場合は、ネットワークサービスユーザーに ShareFile Web サイトへのアクセスを許可するか、プロキシサーバーへの送信アクセスで Windows ユーザーアカウントを設定します。

問題	説明と解決策
ShareFile 管理者インタフェースにストレージゾーンが表示されない	この問題は、外部アドレスまたはファイアウォールに問題がある可能性があります。まず、ストレージゾーンコントローラー コンソールで、外部アドレスにポートが含まれていないことを確認します。その場合は、ポートを削除してからコントローラを再起動します。外部アドレスにポートが含まれていない場合は、Windows ファイアウォールが正しく構成されていることを確認します。既定では、Windows ファイアウォールの設定では、ポート 443 で ShareFile サービスのアウトバウンドトラフィックが許可されます。ストレージゾーンコントローラー には、その設定が必要です。Windows ファイアウォールで、ポート 443 の送信トラフィックが次のプロセスで許可されていることを確認します: `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`

問題	説明と解決策
ストレージゾーンコントローラー が ShareFile にデータをアップロードしない	Citrix ADC コンソールで、負荷分散仮想サーバーを右クリックして統計を表示し、トラフィックが ShareFile コントロールプレーン、ストレージゾーンコントローラー、および ShareFile クライアントから Citrix ADC に到達しているかどうかを確認します。ファイルをアップロードし、仮想サーバーでヒット数が増加すると、トラフィックは Citrix ADC を通過しています。Citrix ADC 接続のすべてのポイントのトラフィックを確認します。コンテンツスイッチング仮想サーバー、コネクタおよび ShareFile データの負荷分散仮想サーバー、2 つの仮想サーバーのいずれかにバインドされた HTTP コールアウト、ShareFile データ仮想サーバーにバインドされたレスポンダーポリシー、コネクタ仮想サーバー Citrix ADC AAA へのバインド。次に、ShareFile データの負荷分散仮想サーバーでレスポンダーポリシーのバインドを解除して、ShareFile データのアップロードをテストします。（レスポンダーポリシーは、ShareFile コントロールプレーンによって署名されていない着信トラフィックをドロップします。Web ブラウザーから、ストレージゾーンコントローラー の外部 FQDN を入力します。接続がある場合は、ShareFile ロゴが表示されます。Web ブラウザーから、コネクタの URL を入力します。ストレージゾーンコネクタのアクセシビリティをテストするために次の URL が成功した場合、バックエンドサーバーがダウンしている場合でも、資格情報の入力を求められます。また、ユーザーとしてログオンしている場合は、API レスポンスが返されます。`https://szc-address/cifs/v3/Items/ByPath?path=\\path`、`https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server`。API レスポンスの形式は次のとおりです: { “Name” :” connectorName” , “FileName” :” FileName” , “CreationDate” :” date” , “ProgenyEditDate” :” date” , “IsHidden” :false, “Path” :” “,” StreamID” :” id” , “odata.metadata” :`https://szc-address/cifs/v3/$metadata#` “Items/ShareFile.Api.Models.Folder@Element” , “Id” :” id” }. その他の例: `https://szc-address/cifs/v3/getItems(itemID)`、`https://szc-address/sp/v3/getItems(itemID)`。iOS の場合: `https://szc-address/cifs/v3/Items/(connector-folder-ID)?$select=`

問題	説明と解決策
ストレージゾーンコントローラをアップグレードすると、ファイルクリーンアップサービスからの ShareFile 接続ステータスが赤いアイコンが表示される	ストレージゾーンコントローラがネットワーク接続を確立する前に Windows がファイルクリーンアップサービスを開始すると、赤いアイコンが表示されます。コントローラサーバがネットワークに戻ると、ステータスは緑色のアイコンに戻ります。
コネクタ作成時に「パスが最大長 (1024) を超えています」が表示される	このメッセージは、ストレージゾーンコントローラー に構成された外部アドレスが、ストレージゾーンコントローラー サーバーの FQDN ではなく ShareFile Web サイトを指している場合に発生することがあります。
古いストレージゾーンコントローラー を削除した後に新しいストレージゾーンコントローラー を構成すると、「無効な名前」が表示されます。	このメッセージは、古いストレージゾーンコントローラー に関連するエンティティがまだ存在する場合に発生することがあります。この問題を解決するには: 新しいストレージゾーンコントローラー をアンインストールします。共有ネットワークフォルダーを削除します。c:\inetpub\wwwroot\Citrix フォルダーを削除します。regedit を開き、**HKEY_LOCAL_MACHINE/Software/Wow6432Note/Citrix** キーを削除します。新しいストレージゾーンコントローラー をインストールして構成します。問題が解決しない場合は、サポート担当者に問い合わせてください。このメッセージは、ストレージゾーンサーバーが DNS またはローカルホストファイルを介してストレージゾーンの FQDN を解決できない場合に発生します。

ASP.NET を手動で登録するには

```
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
```


ShareFile クライアントと **Web** アプリのトラブルシューティング

モバイルデバイスがコネクタに接続しない場合は、接続を確認します。上記の表では、接続に関する問題の多くについて説明します。ストレージゾーンコントローラがオンラインであることを確認します。ゾーンにファイルをアップロードします。アップロードが機能する場合、問題はコネクタに固有です。携帯ネットワークと会社のネットワークの両方を使用して、モバイルデバイスから接続してみてください。SharePoint サーバーまたはファイルサーバーが使用できることを確認します。

コネクタにアクセスしようとするときに「HTTP エラー 401 —権限がありません」と表示される場合は、ShareFile クライアントまたは ShareFile Web アプリからコネクタにアクセスできないことが原因として、以下のいずれかの問題がある可能性があります。

- IIS の構成が正しくありません:Web サービス (IIS) の役割で、基本認証と Windows 認証が有効になっていることを確認します。これらのオプションが [セキュリティ] に表示されない場合は、サーバーマネージャーを使用してそれらをインストールし、IIS を再起動します。
- 不正なユーザー権限:AD ユーザーが共有にアクセスできることを確認します。サーバーマネージャーから [共有と記憶域の管理] に移動し、必要に応じてユーザーを追加するか、ユーザー権限を変更します。
- Citrix ADC 認証、承認、および監査グループアクセスの問題。

SharePoint サイトへの接続時に「HTTP エラー 403-禁止」が表示される場合は、SharePoint サーバーが基本認証用に構成されている可能性がありますが、ストレージゾーンコントローラが資格情報をキャッシュするように構成されていない可能性があります。この問題を解決するには、`C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`に`<add key="CacheCredentials"value="1"/>`を追加します。

モバイルアプリがコネクタにアクセスしようとしたときに「HTTP エラー 503 —サービスを使用できません」が表示される場合は、コネクタは応答を送信していますが、HTTP 要求を処理できません。これは、Citrix ADC でコンテンツスイッチングポリシー、負荷分散 VIP、またはレスポンダーポリシーが正しく構成されていないか、バインドされている場合に発生します。この問題を解決するには、ShareFile の Citrix ADC 構成を確認し、構成を修正します。

参考**:** ストレージゾーンのコントローラ設定ファイル

December 6, 2022

このリファレンスでは、Storage Zone Controller 構成ファイルの概要について説明します。

- Microsoft Azure で ShareFile データを使用してストレージゾーンコントローラーを構成する
- AppSettingsRelease.config
- FileDeleteService.exe.config
- SFAntiVirus.exe.config
- Web.config

ストレージゾーン Controller インストーラーがこれらのファイルを作成します。ストレージゾーンの Controller コンソールで行った変更は、ファイルに保存されます。

特定の機能を使用または構成するには、構成ファイルの一部の設定を手動で追加または更新する必要があります。このリファレンスでは、これらの設定を一覧表示し、関連情報へのリンクを提供します。

Microsoft Azure ストレージ上の **ShareFile**

顧客管理のストレージゾーンでは、Microsoft Azure アカウント内で Citrix ShareFile データをネイティブにホスティングできます。互換性のあるサードパーティ製ストレージを使用することで、IT 部門はコスト効率に優れたカスタマイズソリューションを組織向けに構築できます。このソリューションは、ShareFile を Microsoft Azure のバイナリラージオブジェクト (BLOB) ストレージと統合します。このストレージは、HTTP または HTTPS を使用してどこからでもアクセスできる大量の非構造化データを格納するためのクラウドサービスです。

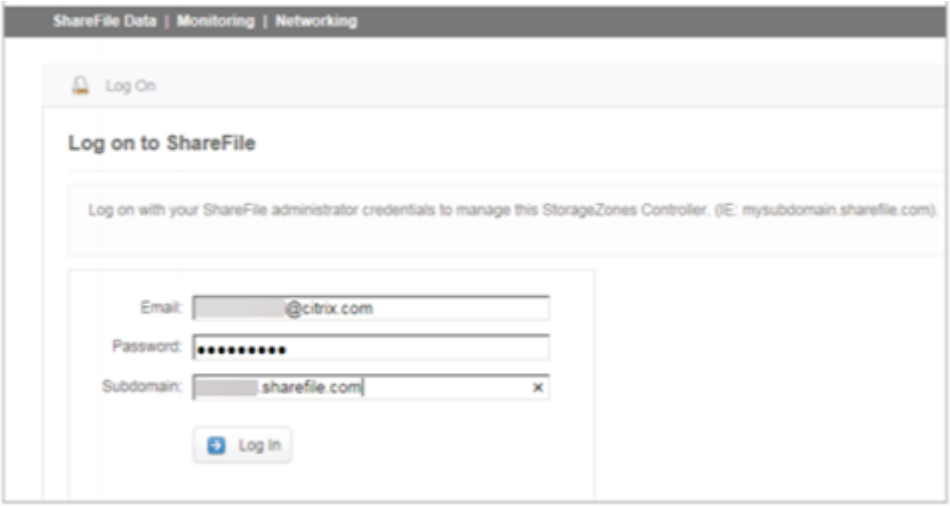
Microsoft Azure で **ShareFile** データを使用してストレージゾーンコントローラーを構成する

Microsoft Azure で ShareFile データを使用してストレージゾーンを作成する前に、システム要件とインストール手順を確認してください。

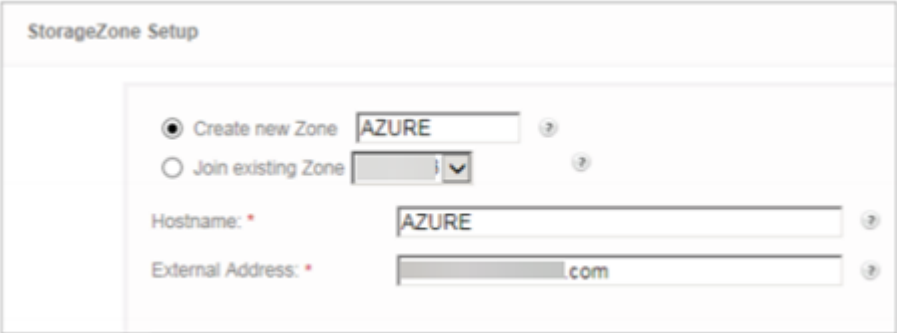
- ストレージキャッシュ用のネットワーク共有を作成します。詳細については、「プライベートデータストレージ用のネットワーク共有の作成」を参照してください。
- 必要な SSL 証明書をインストールします。詳細については、「SSL 証明書のインストール」を参照してください。
- ストレージゾーンのインストール用にサーバーを準備します。詳細については、「ShareFile データ用にサーバーを準備する」を参照してください。

ストレージゾーンコントローラソフトウェアがインストールされたら、**Citrix ShareFile** ストレージゾーンコントローラに移動し、［構成］ページを選択します。

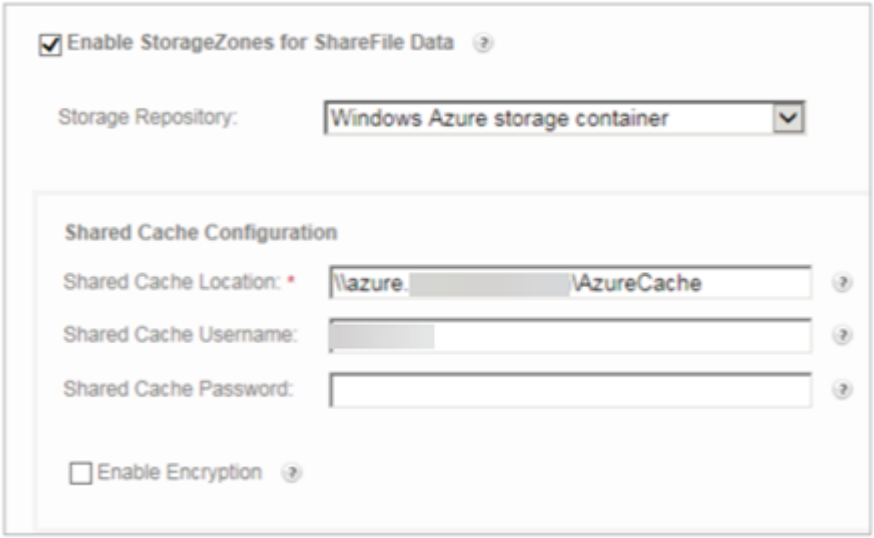
1. 割り当てられた管理者アカウントを使用して ShareFile にログオンします。



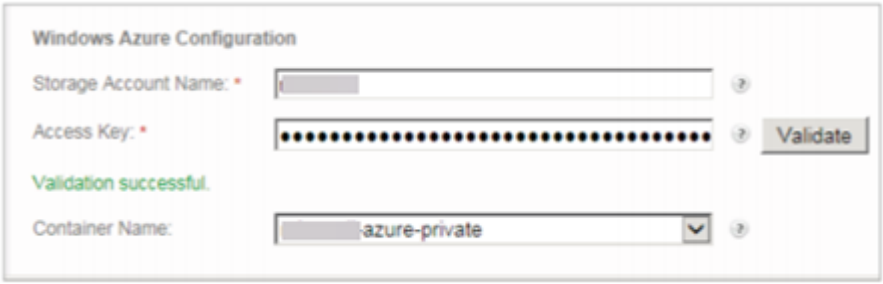
2. [**Create New Zone**] オプションを選択し、新しいゾーンの一意の名前を入力します。
3. ホスト名を入力します。通常は、サーバのコンピュータ名が使用されます。
4. このゾーンの外部アドレスを入力します。これは、このサーバーまたはロードバランサーに対してパブリックに解決可能な FQDN アドレスです。



5. [**ShareFile** データのストレージゾーンを有効にする] チェックボックスをオンにします。
6. [****** ストレージリポジトリ**]** ドロップダウンメニューから **[Windows Azure** ストレージコンテナ **] を選択します。
7. 前提条件のインストール時に作成した共有キャッシュの場所を入力します。プライベートデータストレージ用のネットワーク共有の作成を参照してください。共有キャッシュフォルダへのアクセス権を持つユーザー名とパスワードを入力します。

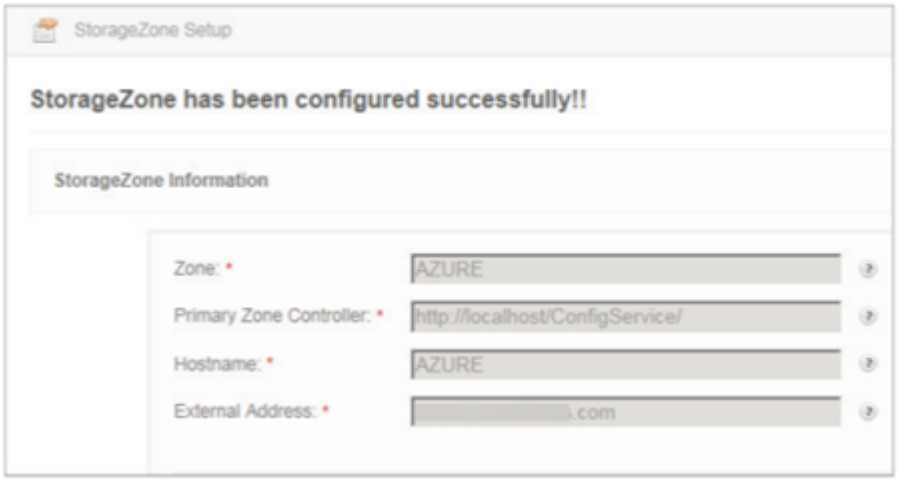


8. ****** ストレージアカウント名とアクセスキーを入力します **。この情報は、Microsoft Azure アカウントから取得されます。
9. 「検証」を選択します。
10. 検証が完了すると、Azure から利用できるコンテナーが表示されます。[Container **Name]** ドロップダウンメニューから適切なコンテナを選択します。

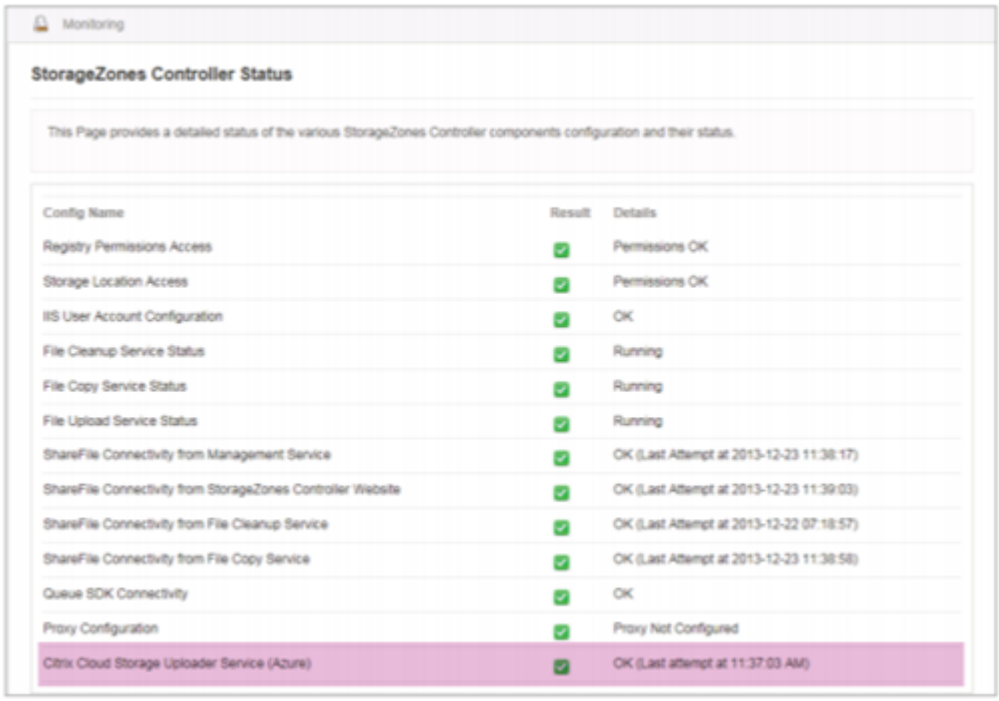


11. ページの下部で、パスフレーズを入力し、検証のために再入力します。
12. ［**Register**］を選択します。

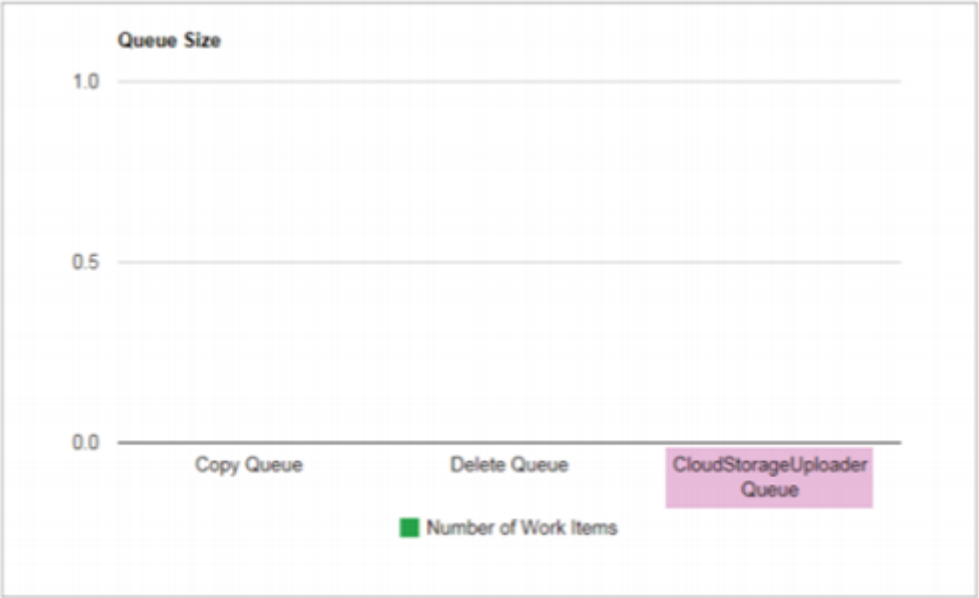
    完了すると、次のメッセージが表示されます:StorageZone は正常に構成されました!!



13. ［監視］タブを選択し、［StorageZones Controller ステータス］を確認します。Citrix Cloud ストレージアップローダーサービス（Azure）は、Azure のバックグラウンドアップローダーサービスを監視します。



CloudStorageUploader キューは、Azure アップロードキューフォルダーを監視します。



AppSettingsRelease.config

AppSettingsRelease.config ファイルは、ストレージゾーンコントローラーのインストールパス (C:\inetpub\wwwroot\Citrix\) の次のフォルダーに含まれています。

- StorageCenter

  ストレージゾーンコントローラのグローバル設定を定義します。

- StorageCenter\cifs

  ネットワークファイル共有のストレージゾーンコネクタの設定を定義します。

- StorageCenter\sp

  SharePoint のストレージゾーンコネクタの設定を定義します。

AppSettingsRelease.config ファイルを編集する前に、正しい場所で作業していることを確認してください。

FileDeleteService.exe.config

FileDeleteService.exe.config は、ストレージゾーンコントローラが永続ストレージキャッシュを管理するために使用するコントロールを提供します。この構成ファイルは次の場所にあります。`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

詳細については、「ストレージキャッシュ操作のカスタマイズ」を参照してください。

SFAntiVirus.exe.config

SFAntivirus.exe.config は、ストレージゾーンのコントローラ構成、スキャナソフトウェアの場所、およびさまざまなコマンドオプションに関する情報をスキャナソフトウェアに提供します。この構成ファイルは次の場所にあります。`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

詳細については、「アップロードしたファイルのウイルス対策スキャンの設定」を参照してください。

Web.config

一般に、`C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` には、通常変更すべきでないコントロールが含まれています。ただし、プロキシサーバーで古いストレージゾーンコントローラーを使用している場合は、更新する必要があります。

StorageZones Controller 2.2 ～2.2.2 のみ: ゾーンに複数のストレージゾーンコントローラがあり、すべての HTTP トラフィックがプロキシサーバーを使用する場合は、セカンダリサーバーごとに Web.config にバイパスリストを追加する必要があります。

注: リリース 2.2.3 以降、バイパス設定はストレージゾーンコントローラーコンソールの [ネットワーク] ページに含まれています。

1. テキストエディタでファイルを開き、`<system.net>` セクションを見つけます。プロキシサーバーを設定した後のセクションの例を次に示します。

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

2. 図のように、そのセクションにバイパスリストを追加します。

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

   プライマリサーバーは、IP アドレスまたはホスト名 (サーバー名.subdomain.com) のいずれかです。

   プライマリストレージゾーンのコントローラの IP アドレスまたはホスト名を後で変更する場合は、各セカンダリサーバーの ConfigService\ Web.config でその情報を更新する必要があります。

3. すべてのゾーンメンバーの IIS サーバーを再起動します。