Storage Zone Controller 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。Citrix 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。Citrix 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 Citrix 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 Citrix 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、Citrix は責任を負わないものとします。

Contents

© 1999-2021 Citrix Systems, Inc. All rights reserved.

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller について

October 13, 2020

Storage Zone Controller を使用すると、ShareFile アカウントでプライベートデータストレージ（Storage Zone for ShareFile Data と呼ばれる）を使用できるようになり、ShareFile SaaS（Software as a Service）のクラウドストレージが拡張されます。

コンポーネント、データストレージなど、Storage zones controller について詳しくは、次を参照してください: Storage Zone Controller 5.x

このコンテンツおよび Citrix Content Collaboration の最新の機能強化については、「新機能」を参照してください。

最新バージョンをダウンロードするには、https://www.citrix.com/downloads/ShareFile/を参照してください。Citrix アカウントにサインインして、すべてのアプリケーションのダウンロードにアクセスします。

解決された問題

Storage Zone 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 Zone Controller 5.9 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 Zone Controller 5.8 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ための修正と、SharePoint で新しく公開された管理パスの修正が含まれています。

Storage Zone Controller 5.7 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のアップロードにおける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 Zone Controller 5.6 で解決された問題

WOPI Fix: それ以降オフィスファイルを編集しようとしたときに表示され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 コネクタ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が表示されるように変更が加えられています。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller 5.5 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 Zone 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の移動は、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を移動することが期待どおりに動作することを保証します。

セキュリティ修正プログラム**:** このリリースには、セキュリティと信頼性の修正が含まれています。

Storage Zone Controller 5.4.1 で解決された問題

セキュリティ修正プログラム**:** このリリースには、セキュリティと信頼性の修正が含まれています。

追加サポート: **Workspace** 環境の ***cloud/ *cloudburrit** o アカウントのサポートが追加されました。

Storage Zone 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 Zone Controller 5.3.1 で解決された問題

WOPI 修正**:** WOPI アクセストークンが、公開暗号鍵の盗難によってなりすましになる可能性があります。このバージョンでは、キーが Storage Zone Controller 間で共有されないことが保証されました。

セキュリティ修正プログラム**:** このリリースには、セキュリティ、パフォーマンス、および信頼性の修正が含まれています。

既知の問題

Storage Zone 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 Zone 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 Zone 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone 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

June 15, 2020

このセクションでは、概念実証評価または高可用性実稼働環境向けの Storage Zone Controller 導入の概要を説明します。高可用性展開は、Citrix ADC などの DMZ プロキシを使用する場合と使用しない場合の両方を示しています。

複数の Storage Zone Controller がある展開を評価するには、高可用性展開のガイドラインに従います。

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、セキュアな ShareFile で管理されたクラウドにデータを保存します。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のプライベートデータストレージを使用するには、ShareFile Data 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データをユーザーに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 の概念実証展開

> 注意:
>
> 概念実証デプロイメント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。

概念実証展開では、単一の Storage Zone Controller を使用します。このセクションで説明する展開例では、ShareFile Data 用のストレージゾーンとストレージゾーンコネクターの両方が有効になっています。

単一の Storage Zone Controller を評価するためには、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 (C:\ZoneFiles など) にデータを保存することもできます。他のすべてのシステム要件は、評価の展開に適用されます。

標準ストレージゾーンの概念実証の導入

標準ゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからの受信接続を受け入れる必要があります。そのためには、Controller 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、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あります。Storage Zone Controller は、アクセスを制御するためにファイアウォール内に存在します。ShareFile へ

© 1999-2021 Citrix Systems, Inc. All rights reserved.

のユーザー接続は、ファイアウォールを通過し、ポート 443 で 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 の高可用性展開

高可用性を備えた ShareFile の実稼働環境の場合、推奨されるベストプラクティスは、少なくとも 2 つの Storage Zone Controller をインストールすることです。最初の Controller 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、同じゾーンに参加します。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た、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が、稼働する 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簡単にプライマリに昇格できます。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展開

標準ストレージゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからの受信接続を受け入れる必要があります。そのためには、各 Controller が ShareFile クラウドとの通信にパブリックアクセス可能なインターネットアドレスと SSL を有効にする必要があります。異なる Storage Zone Controller に関連付けられた複数の外部パブリックアドレスを構成できます。次の図に、標準ストレージゾーンの高可用性展開を示します。

上記の概念実証導入シナリオと同様に、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、アクセスを制御するためにファイアウォール内に存在します。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 で 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、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。デフォルトでは、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。指定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 Citrix ShareFile サービスを実行します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ネットワーク接続

ネットワーク接続は、ゾーンの種類（Citrix 管理または標準）によって異なります。

Citrix-managed zones

次の表は、ユーザーが ShareFile にログオンし、Citrix 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を示しています。すべての接続で HTTPS が使用されます。

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」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. ファイルのダウンロード	クライアント	storage-location.sharefile.com:443

標準ストレージゾーン

次の表は、ユーザーが ShareFile にログオンし、標準ストレージ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ています。すべての接続で HTTPS が使用されます。

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. ファイルのダウンロードの承認	company.sharefile.com	szc.company.com
5. ファイルのダウンロード	クライアント	szc.company.com

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller DMZ プロキシの展開

非武装地帯 (DMZ) は、内部ネットワークのセキュリティをさらに強化します。Citrix 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 クラウドから発信され、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。

  Storage Zone Controller には、すべての受信メッセージに対して有効な 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シグニチャを検証します。

- リアルタイムのステータスインジケータを使用して、Storage Zone Controller への要求を負荷分散します。

  すべての操作が同じファイルにアクセスできる場合は、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の要求が認証されていることを確認します。

Citrix ADC と **Storage Zone Controller** 展開

標準ストレージゾーンの展開

標準ゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからの受信接続を受け入れる必要があります。そのためには、Citrix ADC が ShareFile クラウドとの通信にパブリックアクセス可能なインターネットアドレスと SSL を有効にする必要があります。

このシナリオでは、2 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、内部ネットワークに存在します。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 で 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、DMZ プロキシサーバーの 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 (ユーザー接続が終了した場合)。

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、Citrix ADC 背後に展開されている標準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、信頼できるネットワーク上の ADFS サーバーと通信する ADFS プロキシサーバーによって DMZ で処理されます。ファイルアクティビティは、DMZ の Citrix ADC を介してアクセスされます。DMZ は、SSL を終了し、ユーザー要求を認証し、認証されたユーザーに代わって信頼されたネットワーク内の Storage Zone Controller にアクセスします。ShareFile 用の Citrix ADC 外部アドレスには、インターネット FQDN szc.company.com を使用してアクセスします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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」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	HTTPS
2a. ADFS ログオン	ADFS プロキシ	ADFS サーバー	HTTPS
3. ファイル/フォルダの列挙とダウンロード要求	クライアント	company.sharefile.com	HTTPS
4. ファイルのダウンロードの承認	ShareFile	szc.company.com (外部アドレス)	HTTP
4a. ファイルのダウンロードの承認	Citrix ADC IP（NSIP）	Storage Zone Controller	HTTPS
5. ファイルのダウンロード	クライアント	szc.company.com (外部アドレス)	HTTPS
5a. ファイルのダウンロード	Citrix ADC IP（NSIP）	Storage Zone Controller	HTTP

次の図と表は、前のシナリオを拡張して、StorageZone コネクタのネットワーク接続を示しています。このシナリオには、DMZ で NetScaler を使用して SSL を終了し、Connector 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」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	HTTPS
2a. ADFS ログオン	ADFS プロキシ	ADFS サーバー	HTTPS
3. 最上位コネクタの列挙	クライアント	company.sharefile.com	HTTPS
4. ユーザーの Storage Zone Controller サーバーへのログオン	クライアント	szc.company.com (外部アドレス)	HTTPS
5. ユーザー認証	Citrix ADC IP（NSIP）	AD ドメイン Controller	LDAP

© 1999-2021 Citrix Systems, Inc. All rights reserved.

手順	接続元	接続先	プロトコル
6. ファイル/フォルダの列挙とファイル/フォルダのリクエスト	Citrix 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

次の図は、ユーザーが認証する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

June 15, 2020

Storage Zone Controller

- 2 つの CPU と 4 GB の RAM を搭載した専用の物理マシンまたは仮想マシン
- Windows Server 2012 R2 (Datacenter, Standard, または Essentials)
- Windows Server 2016

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 (IP アドレスではない) を使用します。
- ShareFile との通信で SSL を有効にします。
  - Storage Zone Controller 上の SSL 証明書は、ユーザーデバイスおよび ShareFile Web サーバーによって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 の設定について詳しくは、http://support.microsoft.com/kb/298805を参照してください。
- ファイアウォール経由で、ポート 443 で受信 TCP 要求を許可します。
- ファイアウォール経由でポート 443 の ShareFile コントロールプレーンへの送信 TCP 要求を許可します。
  - 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 データのストレージゾーンにのみ使用されるサーバーのヘルスチェックの場合:

- ローカルホストのポート 80 を開きます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

高可用性の本番環境の場合：

- Storage Zone Controller がインストールされた最低 2 台のサーバ。
- 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：

- 1 つ以上の DMZ プロキシサーバー（Citrix ADC VPX インスタンスなど）。
- 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 プロキシサーバーと Storage Zone Controller 間の通信がセキュリティで保護されている場合は、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 を使用する場合は、DMZ プロキシによって信頼されている場合は、Storage Zone Controller でプライベート (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

- Storage Zone Controller インストーラーには、管理者権限が必要です。
- Storage Zone Controller のリモート管理には、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 Zone Controller コンソールを開きます。

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

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

サポートされる情報漏えい対策ソリューション

- Storage Zone Controller は、以下を含む ICAP 準拠の DLP ソリューションと統合されます。
  - シマンテックの情報漏えい対策
  - McAfee DLP Prevent
  - Websense TRITON AP-DATA
  - RSA データ損失防止

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 Zone Controller で有効にするオプション機能です。

要件：

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- ストレージゾーン機能を有効にした ShareFile Enterprise アカウント
- ゾーンの作成と管理権限を含む 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製のストレージシステムに ShareFile ファイルを保存する場合、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。詳しくは、「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 クライアントからの 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 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 Zone 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 のいずれかを選択します。
- サポートされているのは **Microsoft SharePoint Server 2010** 以降のみです。
- Storage Zone 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。詳しくは、「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最大アップロードファイルサイズは 250 MB で、SharePoint 2010 では 50 MB です。既定を変更するには、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のサイズ制限は 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（パブリッシュ）をチェックインしようとします。ただし、SharePoint ポリシーによって、ファイルがメジャーバージョンまたはマイナーバージョンとしてチェックインされるかが決まります。
  - SharePoint の表示のみのアクセス許可では、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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

SharePoint 認証用のストレージゾーンコネクタ

ユーザーを認証した後、Storage Zone 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 サーバーによって提示される認証のチャレンジに応答します。SharePoint 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”\>`を`C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.に追加する必要があります。

- ネゴシエート (Kerberos)
- Windows Challenge/Response (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 Zone Controller または DMZ プロキシに対して認証します。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管理されます。SharePoint サーバーで Kerberos 認証または NTLM 認証を使用するには、次の手順を実行します。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

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指定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。詳しくは、http://support.microsoft.com/kb/832769の「Web パーツの委任に対する信頼を構成する」を参照してください。

Citrix ADC を使用した展開では、Citrix ADC で基本認証を終了してから、Storage Zone 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ストレージゾーンコネクタは、Storage Zone 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。詳しくは、「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

ユーザーの認証後、Storage Zone 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への接続を行い、ファイルサーバーによって提示される認証の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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- ネゴシエート (Kerberos)
- Windows Challenge/Response (NTLM)

Storage Zone Controller で Kerberos または NTLM 認証を使用するには、次の手順を実行します。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

Citrix ADC を使用した展開の場合：Citrix ADC が基本認証用に構成されている場合にシングルサインオンエクスペリエンスをユーザーに提供するには、コネクタをネゴシエート（Kerberos）認証と NTLM 認証の両方で構成します。

PowerShell スクリプトとコマンド

Storage Zone Controller インストールには、`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`にある複数の PowerShell スクリプトとコマンドが含まれています。

- 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 4.0に付属の PowerShell 4.0 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す。

インストール

June 15, 2020

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 用の Citrix ADC の構成

   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 用のストレージゾーンには、サポートされているサードパーティ製のストレージシステムに ShareFile ファイルを保存する場合でも、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 セットアップは、ShareFile データおよびストレージゾーンコネクタのストレージゾーンに必要です。

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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

6. Storage Zone Controller の設定を確認する
7. ユーザーアカウントの既定のゾーンの変更

   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

Storage Zone Controller 用の Citrix ADC の構成

June 15, 2020

NetScaler バージョン 10.1 ビルド 120.1316.e 以降には、Storage Zone Controller 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、次の設定を生成します。

- Storage Zone Controller 間でトラフィックの負荷分散
- ストレージゾーンコネクタのユーザー認証を提供
- ShareFile アップロードおよびダウンロードの URI 署名を検証する
- 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- **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適切な Citrix ADC 負荷分散仮想サーバーにデータに対するユーザー要求を送信します。
- **Citrix ADC** 負荷分散仮想サーバー — Storage Zone Controller のトラフィックを負荷分散し、以下の処理も行います。
  - 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、受信要求に有効な URI 署名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ついては、負荷分散仮想サーバーがユーザー認証を実行します。これは、Citrix ADC でユーザー要求を停止し、ユーザーを認証し、Storage Zone Controller にユーザーのシングルサインオンを実行します。

  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。

Storage Zone Controller 4.0 以降、管理者は Storage Zone Controller 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 Storage Zone Controller への受信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 をサポートする必要があります。詳細情報と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 より前のバージョンの NetScaler 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。

ShareFile 用 Citrix ADC ウィザードのセットアップでは、Citrix Endpoint Management を ShareFile 用の SAML アイデンティティプロバイダ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、ここをクリックを参照してください。

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

Storage Zone Controller 用に **Citrix ADC** を構成する

以下の手順では、Citrix ADC for ShareFile ウィザードの使用方法を説明します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

1. Citrix ADC アプライアンスにログオンし、［構成］タブで［トラフィック管理］に移動します。
2. ［Citrix ShareFile］で Citrix ADC を ShareFile 用にセットアップする］をクリックします。

   ウィザードにアクセスするには、［モビリティ］で［**Endpoint Management**］、［**ShareFile**］、および **Citrix Gateway** の構成］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）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 データ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	証明書を選択するか、コンテンツスイッチング仮想サーバー用の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。標準ゾーンまたは外部ホスト名を持つ制限付きゾーンの場合、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。
Storage Zone Controller IP アドレス	1 つ以上の Storage Zone Controller サーバーの内部 IP アドレス。これらの IP アドレスは、Storage Zone Controller サーバーを Citrix ADC 内のエンティティとして定義します。すでに Citrix ADC にサーバーを追加している場合は、［既存から追加］をクリックしてサーバーを選択します。負荷分散に Citrix ADC を使用するには、各 Storage Zone Controller 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

オプション	説明
ポートとプロトコル	Citrix ADC から Storage Zone Controller 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、独自の使用のためにこの仮想サーバーを作成します。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。すでに Citrix ADC に LDAP サーバーを追加している場合は、［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ている LDAP ベース識別名 (DN)。一般的な形式で DN を指定します。CN= ユーザー、DC= ドメイン、DC= ネット
管理者バインド DN およびパスワード	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	Citrix ADC によって使用される LDAP 属性。ユーザーがユーザー名またはメールアドレスのどちらでログオンするかを決定します。デフォルトは sAMAccountNam です。これにより、ユーザーは自分のユーザー名を使用してログオンできます。ログオン時に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。

制限ゾーンまたはコネクタへの **Web** アクセス用に **Citrix ADC** を構成する

制限ゾーンまたは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 ウィザードの完了後に、追加の Citrix ADC 構成を実行する必要があります。

- 3 台目の Citrix ADC 負荷分散仮想サーバーを作成して構成します。これにより、信頼された ShareFile ドメインにログオンしたときにのみ ShareFile クライアントが資格情報を送信できます。

  Storage Zone Controller は、Cross-Origin Resource Sharing (CORS) 標準を使用して、制限ゾーンへの要求や、ShareFile Web インターフェイスからストレージゾーンコネクタへの要求に必要なセキュリティ

© 1999-2021 Citrix Systems, Inc. All rights reserved.

を提供します。CORS は HTTP ヘッダーを使用して、クライアントとサーバーがお互いを十分に知って、要求または応答が成功するかどうかを判断できるようにします。

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 要求は、認証されることなく、署名を検証するための HTTPS コールアウトなしで Storage Zone Controller に渡されます。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。

構成を実行するために CORS について理解する必要はありません。ただし、CORS について詳しくは、「http://enable-cors.org/」を参照してください。

制限ゾーン内のコネクタへの Web アクセスに Internet Explorer を使用するには、Internet Explorer の構成が必要です。

- 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。

Citrix ADC for ShareFile 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. 第 3 の負荷分散仮想サーバーを作成します。
   a) [トラフィック管理] **>** [負荷分散] **>** [仮想サーバー] に移動します。
   b) [追加] をクリックしてください。
   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 アドレスタイプ	アドレス不可能

   d) クリックして仮想サーバーを作成します。
   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］から［>］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のポリシーを作成します。
   a) [トラフィック管理] > [コンテンツの切り替え] > [ポリシー] 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。[式エディタ] をクリックし、この式を作成します。[**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、OPTIONS と入力します。式は次のように読み取ります。`HTTP.REQ.METHOD.EQ("OPTIONS")`
   c) ［完了］をクリックします。
   d) ［作成］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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

a) [トラフィック管理] **>** [コンテンツスイッチング] **>** [仮想サーバー] 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) [コンテンツスイッチングポリシーのバインド] のセクションに移動し、[2 コンテンツスイッチングポリシー] 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ーを選択します。
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。新しいポリシーのプライオリティを変更して、3 つのポリシーのうち最も低い数にします。
最も低い値のポリシーが最高の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) [トラフィック管理] **>** [コンテンツの切り替え] **>** [ポリシー] 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) [トラフィック管理] **>** [コンテンツの切り替え] **>** [ポリシー] 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
```

© 1999-2021 Citrix Systems, Inc. All rights reserved.

読み取り専用共有用に **Citrix ADC** を構成する

読み取り専用共有をサポートするには、ユーザーが Microsoft Office Web Apps 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、Storage Zone Controller 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、Storage Zone Controller 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 サーバーに適切に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 Storage Zone Controller のゾーンの既存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。
   - [トラフィック管理**] > [**負荷分散**] > [**サービス**]** に移動します。
   - ［追加］をクリックします。
   - 必要な情報を入力して、OWA サーバーに対応するサービスを作成します。［**OK**］をクリックします。
2. 追加の負荷分散仮想サーバーを作成します。
   - [トラフィック管理**] > [**負荷分散**] > [**仮想サーバー] 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 アドレスタイプ	アドレス不可能

   - クリックして仮想サーバーを作成します。
   - 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**]** をクリックします。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 サーバーにトラフィックをルーティングするために使用する新しいポリシーを作成します。
   - [トラフィック管理**] > [**コンテンツの切り替え**] > [**ポリシー**]** に移動します。
   - ［追加］を選択します。
   - ポリシーに名前を付けます。
   - 次の式を追加します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- HTTP.REQ.URL.CONTAINS(“/hosting/discovery”)
  || 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(“/hosting/discovery”)
  || HTTP.REQ.URL.CONTAINS(“/x/”)
  || HTTP.REQ.URL.CONTAINS(“/wv/”)
  || HTTP.REQ.URL.CONTAINS(“/p/”)

4. ロードバランシング仮想内の新しいポリシーの優先順位の更新
   - [トラフィック管理] **>** [コンテンツスイッチング] **>** [仮想サーバー] に移動します。
   - 負荷分散仮想サーバーをクリックし、[コンテンツスイッチングポリシー] を選択します。
   - （例）「_SF_OWA」ポリシーの優先順位が 3 番目になるようにポリシーの優先順位を変更します。

優先度	ポリシー名
90	SF_ZK_OPTIONS
95	SF_CIF_SPOL
99	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。

Storage Zone Controller サービス用のモニターを作成する

デフォルトでは、Citrix ADC は Storage Zone Controller サーバーに ping を実行し、オンラインかどうかを確認します。ただし、Controller 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ことがあります。この場合、Citrix ADC は、ShareFile と通信していないが、Storage Zone Controller にトラフィックを送信します。

ShareFile への Storage Zone Controller 送信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 Storage Zone Controller 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、Storage Zone Controller 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 などの Controller の IP アドレスが含まれます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

Citrix ADC の構成を確認します

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 を使用した ShareFile 要求のスループットの表示

スループット統計は、[ダッシュボード] メニューにあります。

Citrix ADC を手動で構成する

June 15, 2020

バージョン 10.1 のビルド 120.1316 以降、Citrix ADC には、Storage Zone Controller 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、Storage Zone Controller に必要な Citrix ADC の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。

すべての受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 コールアウトの構成] 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)「メソッドの取得」を選択します。
   d) [ホストの式] に、仮想サーバの IP アドレスまたは Storage Zone Controller のホスト IP アドレスを入力します。
   e)「URL 幹式」に次のように入力します。

```
1 "/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 コールアウトの構成] 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] を **[Bool]** として選択します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

h)「式」で、応答からデータを抽出するには、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。

詳しくは、「HTTP コールアウト」を参照してください。

2. 前述の手順に従って、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を除き、同じ設定を使用します。
   - 「URL 幹式」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構成します。
   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)「式」に、次のように入力します。

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

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する。SSL セッションベースの永続性を構成します。

ロードバランシングするには

1. 「トークンベースのロードバランシングの構成」を参照してください。

   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 Storage Zone Controller 以外の Storage Zone Controller 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。

   詳しくは、「SSL オフロードの設定」とそのサブトピック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の有効化の説明に従って、コンテンツの切り替えを有効にします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

2. オンプレミスのストレージゾーンからの ShareFile 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構成] 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。この手順では、Data_Requests という名前を使用します。

   b) 式を入力します。

   ```
   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構成] 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。この手順では、Connector_Requests という名前を使用します。

   b) 式を入力します。

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

   「Storage Zone ControllerFQDN」を Controller 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の作成」を参照してください。

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で、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仮想サーバーは、すべての受信メッセージで有効な URI 署名を確認して負荷分散の手順 4 で応答側ポリシーをバインドしたサーバーです。

   - 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仮想サーバーを指定します。

6. ストレージゾーンコネクタの認証仮想サーバーを構成します。

   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) ナビゲーションウィンドウで、[負荷分散] を展開し、ストレージゾーンコネクタ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、[認証設定] を展開します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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 (分)] に **240** と入力します。

240 分のタイムアウト値を推奨します。最小値は 10 分より大きくする必要があります。

詳しくは、「認証仮想サーバの設定」を参照してください。

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

「SSO 名属性」に、「ユーザープリンシパル名」と入力します。

その他の設定について詳しくは、「認証ポリシー」を参照してください。

8. 作成した認証サーバーの認証ポリシーを設定します。

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

b) 式を入力します。

```
ns_true
```

詳しくは、「認証ポリシーの構成」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の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 [**PRIMARY**] を選択します。
d) シングルサインオンドメインで、Storage Zone Controller のドメイン名を入力します。
e) 上記の 3 つの項目ごとに、[グローバルをオーバーライド] チェックボックスをオンにします。

詳しくは、「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のセッションポリシーを構成します。

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) [要求プロファイル] で、前の手順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) 式を入力します。

```
ns_true
```

詳しくは、「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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

c) [ユーザーの認証] 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 で設定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、手順 9 で構成したセッションポリシーを選択します。

詳しくは、「認証仮想サーバの設定」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

June 15, 2020

ShareFile Data のストレージゾーンには、プライベートデータ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。

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。デフォルトでは、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。ただし、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 Citrix ShareFile サービスを実行する必要があります。

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 で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は、ShareFile サービスアカウントとして参照されます。
   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アクセス許可を拒否し、構成されているストレージロケーションユーザーのみにアクセス権を付与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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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] アクセス許可があ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

デフォルトでは、分割されたストレージレイアウトには 256 個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 番目の値では、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(16 から N の累乗)を使用して、サイトに適した値を決定できます。たとえば、PathSelectionParams=3,4,4,4 を指定すると、最上位フォルダの数が 4096 (16 から 3 の累乗) に制限されます。2 番目の値は、最上位フォルダの子

© 1999-2021 Citrix Systems, Inc. All rights reserved.

フォルダの数を 65536 に制限します (16 から 4 の累乗)。3 番目の値は、2 番目のレベル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。ツリーの一番下から始まり、空でないフォルダに到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

June 15, 2020

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 のドキュメントを参照してください。

証明書をインストールする手順は、次のとおりです。

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] の順に選択し、[次へ] をクリックします。
6. [参照] をクリックし、ファイル名拡張子のメニューから [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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ShareFile データ用にサーバーを準備する

June 15, 2020

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 データおよびストレージゾーンコネクタ用のストレージゾーンに必要です。これらの手順は、Windows Server 2012 に基づいています。Windows Server 2008 の手順については、Storage Zone Controller の古いドキュメントを参照してください。

Microsoft .NET バージョンを更新する

Storage Zone Controller インストールを進める前に、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。

- **Storage Zone Controller 5.x** には、**.NET 4.8** 以降が必要です。ここをクリックして.NET 4.8 をダウンロードしてください

ShareFile アプリケーションを使用する場合は、最新バージョンの Microsoft .NET を利用することをお勧めします。

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

1. Storage Zone Controller をインストールするサーバーで、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. [ターゲットサーバーの選択] 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)] チェックボックスと [Windows Server Update Services] 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. [機能の追加] 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] と [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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

13. インストールが完了したら、[**Close**] をクリックして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 の役割サービスを有効にした後で、IIS を構成します。

1. IIS マネージャーコンソールを開き、Storage Zone Controller サーバーノードをクリックし、[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、Storage Zone Controller 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、続行する前に証明書をサーバーにインストールします。詳しくは、「SSL 証明書のインストール」を参照してください。

   > 注:
   >
   > Storage Zone Controller を備えた Citrix 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構成します。
   - 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 番です。
   - 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/` およびに移動します `https://localhost/`。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 localhost 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. 仮想マシンに Storage Zone Controller をインストールする場合は、仮想マシンのスナップショットを作成します。

Storage Zone Controller をインストールし、ストレージゾーンを作成する

June 15, 2020

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> 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。

Storage Zone Controller をインストールするときは、ゾーンを作成し、プライマリ Storage Zone Controller または
セカンダリ Storage Zone Controller をゾーンに結合するを設定します。

プライマリ Storage Zone Controller を構成するときに、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のいずれか、プライベートデータストレージを指定します。
- ストレージゾーンコネクタ。ユーザーが SharePoint サイトまたは指定し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るようにします。

次の手順では、Storage Zone Controller 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:
   - http://www.citrix.com/downloads/sharefile.htmlの ShareFile ダウンロードページから、最新の Storage Zone Controller インストーラにログオンしてダウンロードします。

   > 注:
   >
   > Storage Zone Controller をインストールすると、サーバー上のデフォルトの 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、デフォルトの Web サイトで有効にする必要があります。
2. Storage Zone Controller をインストールするサーバー上で 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。
   - マルチテナンシーの場合は、次のコマンドを実行します: ***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（例では 5.0.1）を更新する必要があります。

   - プロンプトに応答します。インストールが完了したら、[**Storage Zone Controller** の構成ページを起動] チェックボックスをオフにして [完了] をクリックします。
3. Storage Zone Controller を再起動します。
4. インストールが正常に完了したことをテストするには、`http://localhost/`に移動します。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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> 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 互換ストレージプロバイダを使用するには、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がパス形式のコンテナ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**
     - 値のデータ: 真
   - Storage Zone Controller アプリケーションプール (StorageCenterAppPool) を再起動します。
   - S3 互換の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。Storage Zone Controller は、実際の Amazon S3 サービスではなく、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. Storage Zone Controller コンソールに移動します。
9. `http://localhost/configservice/login.aspx`を開くかスタート画面またはメニューから設定ツールを起動します。Windows 8 で [スタート] 画面のショートカットを使用する方法については、「Storage Zone Controller の管理」を参照してください。
10. **Storage Zone Controller** ログオンページで、アカウントのメールアドレス、パスワード、および 完全なアカウント **URL** の **FQDN** サブドメイン（`subdomain.sharefile.com`、`subdomain.sharefile.eu`など）を入力します。［ログオン］をクリックします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

11. プライマリ Storage Zone Controller 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 管理者コンソールに表示される名前。
プライマリ Zone Controller	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 では、標準ゾーンに対して有効で信頼されたパブリック SSL 証明書のみがサポートされています。セカンダリストレージゾーンのホスト構成に問題がある場合は、そのサーバー上のローカルブラウザーで、SSL エラーなしで ConfigService URL を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、サーバ名（`https://servername.subdomain.com/ConfigService`など）を指定できます。サーバー名は、セカンダリ Storage Zone Controller サーバーによって解決可能である必要があります。
ホスト名	Storage Zone Controller の一意の識別子。ShareFile では、サーバーのホスト名を識別子として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 管理者コンソールに表示されます。
外部アドレス	この Storage Zone Controller の FQDN。この Storage Zone Controller を標準ゾーンに使用する場合は、インターネットから URL に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。このページを送信すると、ShareFile によってアドレスが検証されます。

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、チェックボックスをオフにします。

    > 注:
    >
    > Storage Zone Controller を構成した後は、ゾーンの種類を変更できません。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller は、サービスアカウントの資格情報を使用して、信頼された Active Directory ドメインサーバーに接続してメールアドレス検索を行います。

- 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ない場合は、[登録] をクリックして Storage Zone Controller を ShareFile に登録し、手順 14 に進みます。
14. S3 互換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\CloudStorageUploa` レジストリキーを見つけます。
    - 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がパス形式のコンテナ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**
        - 値のデータ: 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、次の手順に従います。

    コネクタを有効にすると、IIS アプリケーション「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ストレージゾーンコネクタを有効にする] と [SharePoint のストレージゾーンコネクタを有効にする] のチェックボックスをオンにします。コネクタの設定については、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。Storage Zone Controller 情報が表示されます。
    - ストレージゾーンコネクタに [許可されたパス] 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 Storage Zone Controller を構成する方法については、「Storage Zone Controller の管理」を参照してください。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> 重要:
>
> Storage Zone 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 Zone Controller サーバーのスナップショットを作成し、構成をバックアップし、Storage Zone Controller 構成のバックアップおよび障害回復用の Storage Zone Controller 準備をバックアップする必要があります。

ShareFile データのストレージゾーンを構成する

> 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 のストレージゾーンは、ストレージゾーンの作成時に Storage Zone Controller ウィザードから、または Storage Zone Controller コンソールから設定できます。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製ストレージシステムの設定を構成するには、[ShareFile Data] タブを使用します。

ネットワーク共有の設定

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。ゾーンの作成後は、[ストレージリポジトリ] オプションを変更できません。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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

オプション	説明
ネットワーク共有の場所	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 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。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。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。このストレージの場所は、ShareFile Data のみのストレージゾーン用に予約します。Storage Zone Controller は、構成ページで提供されるネットワーク共有のユーザー名/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。構成ページで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、デフォルトでネットワークサービスアカウントが使用されます。ネットワークサービスアカウントには、この保存場所へのフルアクセス権が必要です。Storage Zone Controller は、StorageCenterAppPool の既定でネットワークサービスアカウントを使用します。サポートされている構成は、Network Service アカウントを使用するだけです。
ネットワーク共有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。Network Service 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 Citrix ShareFile サービスを引き続き実行できます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

オプション	説明
暗号化を有効にする	ファイル共有に保存されているファイルの内容を暗号化する場合のみ、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にあり、サードパーティ製のツールによって既に保護されている企業環境では、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とは関係ありません。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、必要なときに最大限のセキュリティを提供する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製のツールによってディスクが読み取れなくなります。ShareFile では、ファイル暗号化キーを使用してダウンロード要求の妥当性を確認し、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。パスフレーズと暗号化キーは、安全な場所に保管してください。ゾーン内の各 Storage Zone Controller 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、紛失した場合は回復できません。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 Storage Zone Controller 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、すぐにすべてのストレージゾーンファイルへのアクセスが切断されます。暗号化キーファイルは、通常のデータセンターの手順の一部としてバックアップしてください。

共有キャッシュの構成設定

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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、およびその他の一時項目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 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。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。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 データ用のストレージゾーンにのみ予約します。ネットワークサービスアカウント（または Citrix ShareFile Management Service が実行するように構成されているアカウント）には、このストレージ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	共有キャッシュに保存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ーを選択します。ゾーンの作成後は、[ストレージリポジトリ] オプションを変更できません。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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

オプション	説明
検証	ボタンをクリックして、Azure アクセスキーを検証します。検証が完了し、[Container Name] メニューに指定したアカウントで使用可能なすべてのコンテナが含まれるまでは、設定を続行できません。
コンテナ名	このストレージゾーンのすべての Storage Zone Controller 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、このリストは空です。

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。ゾーンの作成後は、[ストレージリポジトリ] オプションを変更できません。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] メニューに指定し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は、設定を続行できません。
バケット名	このストレージゾーンのすべての Storage Zone Controller 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 サーバーのアドレスと SMTP ポート番号	ローカル SMTP サーバーのホスト名とポート。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

オプション	説明
SSL を使用	セキュリティで保護された接続を介して 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 サーバーのユーザー名とパスワードです。
認証モード	既定の認証モードは、Storage Zone Controller から SMTP サーバーに接続するために使用できる最も安全な方法を使用します。
送信者のアドレス	[差出人] フィールドに表示されるメールアドレス。

Google 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。ゾーンの作成後は、[ストレージリポジトリ] オプションを変更できません。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。

アクセスキーの ID

Google Cloud Platform 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

Google Cloud Platform ストレージの秘密。

検証

ボタンをクリックして、Google Cloud Platform のシークレットアクセスキーを検証します。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は、設定を続行できません。

バケット名

このストレージゾーン内のすべての Storage Zone Controller に使用する正しいバケットを選択します。Google Cloud Platform シークレットアクセスキーが検証されるまで、このリストは空です。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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は、ユーザーが SharePoint サイトまたは指定し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るようにします。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のコネクタ機能は、ゾーンを共有できます。ただし、Storage Zone 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、Storage Zone Controller ウィザードを使用するか、Storage Zone Controller 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受信接続は、最初に許可されたパスに対してチェックされます。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` およびそのすべてのサブフォルダへのアクセスを提供するには、`\\myserver\teamshare`の許可パスを指定します。

- 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。
- エントリはカンマ区切りです。
- ネットワークファイル共有へのコネクタには、許可される UNC パスを指定します。

  FQDN を使用した例: `\\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] で定義されているように、ユーザーのホームフォルダパスにリダイレクトします。パスの例: `%HomeDrive%`

  - %TSHomeDrive%

    Active Directory Directory プロパティ MS-TS-ホームディレクトリ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%

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Active Directory ユーザーとコンピュータースナップインでは、ユーザーオブジェクトを編集するときに、[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ログオン名が「abc\ johnd」の場合、変数は「abc」で置き換えられます。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については、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 などのパス終端記号は含まれません)。

  例:

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

  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。

サーバーヘッダーを削除するセキュリティ上の推奨事項

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、攻撃者にとって有用になる可能性があります。ヘッダーは、送信側サーバーの種類、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、本番サイトでは必要なく、無効にできます。

Storage Zone Controller インストーラーは、このヘッダーを自動的に削除することはできません。このヘッダーを削除するための推奨事項については、Storage Zone Controller ドキュメント/インストールガイドを参照してください。

ドキュメントで提供する必要がある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/

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller のセットアップを確認する

June 15, 2020

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 接続のステータスが一時的に赤いアイコンが表示される場合があります。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。Controller 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でデータを検索します。詳しくは、インストールと構成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 インターフェイ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] に移動し、[健全性] 列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。

   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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

6. ファイルの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、そのファイルがフォルダに表示されることを確認します。

ユーザーアカウントの既定のゾーンの変更

June 15, 2020

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、ユーザー管理ツールを開き、オプションアイコンをクリックします。
- ルートレベルフォルダーのゾーンを選択するには、ShareFile 管理コンソールを開き、「ユーザーの管理」に移動します。（スーパーユーザグループのメンバシップが必要です）。
- 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。（スーパーユーザグループのメンバシップが必要です）。[ユーザーの管理] ページで、ゾーン権限を作成および管理することもできます。

ストレージゾーンのプロキシサーバーを指定する

June 15, 2020

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。
2. [プロキシを有効にする] チェックボックスをオンにし、プロキシサーバーのアドレスとポートを入力します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

June 15, 2020

> 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 Controller 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 Controller で、[スタート**] > [**管理ツール**] > [Active Directory** ユーザーとコンピュータ] をクリックします。
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、[指定したサービスへの委任のみに対してこのコンピューターを信頼する] を選択します。
5. NTLM の場合:
   a) [指定したサービスへの委任のみに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 1 つのサービスを追加します。
   c) [使用可能なサービス] リストで、使用するサービスを選択します。CIFS (ネットワークファイル共有用のコネクタ用) と HTTP (SharePoint 用のコネクタ用)。［OK］をクリックします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

June 15, 2020

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 Apps (OWA) サーバーによってレンダリングされます。Citrix が管理するストレージゾーンに保存されているファイルをプレビューすると、Citrix が管理するまたは 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:
>
> ホワイトリストの要件**:**
>
> `*.sf-api.com`は、バージョン 5.0 以降のストレージゾーンでプレビューおよび編集が適切に機能するためには、Office Online Server からアクセスできる必要があります。

要件

オンプレミスファイルプレビューでサポートされるファイルタイプ

- 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、tiff）

オンプレミスのファイル編集でサポートされるファイルの種類

- .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

ホワイトリスト作成/ネットワークに関する考慮事項

- OOS サーバは **`https://*.sf-api.com`**（または**.eu**）に到達できる必要があります

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- SZC Server は、**https://*.sf-api.com** および **https://*.sharefile.com** **(**または**.eu)** に到達できる必要があります。
- SZC サーバーが OOS サーバーにアクセス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のバージョン管理が有効になっている必要があります。

ShareFile Web App の詳細設定メニューで Microsoft Office オンライン編集を有効にする設定は、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。オンプレミスファイルの編集機能は制御されませんが、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には、以下の手順で Storage Zone Controller 管理者によって排他的に制御されます。

Microsoft サーバーの互換性

- **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。

建築図とネットワーク図

1. 認証されたユーザーは、ShareFile でファイルプレビューを要求します。
2. ShareFile は、Office オンラインサーバーの FQDN を持つクライアントデバイスへの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の FQDN にリダイレクトします。注: HTTPS 接続の場合、DNS は内部サーバー IP 用の A レコード、または Load Balancer VIP 用の A レコード、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ルーティングを適用する必要があります。
4. Office Online Server は要求を処理し、Storage Zone Controller サーバーへの API 呼び出しを行います。注: HTTPS 接続、DNS には、内部サーバー IP 用の A レコード、または Load Balancer VIP 用の A レコード、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ルーティングを適用する必要があります。
5. Storage Zone Controller チェック https://\<DNSname\>/hosting/discovery は到達可能です。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信します。注: Storage Zone Controller 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. Storage Zone Controller は、ShareFile API（sf-api.com）へ送信方向に接続します。注：これは、ファイアウォール、プロキシ、または送信ルーティングアプライアンスを経由する必須の送信接続です。Storage Zone Controller サーバーが、HTTPS/443 経由で、上記の文書化された IP アドレスに送信方向に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、ShareFile API への送信に接続します。注：これは、ファイアウォール、プロキシ、または送信ルーティングアプライアンスを経由する必須の送信接続です。Office Online Server が

© 1999-2021 Citrix Systems, Inc. All rights reserved.

HTTPS/443 経由で上記の文書化された 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。

Storage Zone Controller は、コンテンツをダウンロードするために OOS が ShareFile コントロールプレーンを呼び出すのではなく、OOS にファイルバイトをストリームします。Storage Zone Controller の構成ファイルの 1 つで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、現在 **false** のキー **downloadFileFromSC** があります。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、OOS は ShareFile コントロールプレーンを呼び出してファイルの内容をダウンロードしなくなりました。

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 への受信トラフィックがないことを示すのは正しいでしょうか。

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送信接続を確立しなくなります。

ただし、ShareFile コントロールプレーンは、上記のオプションが使用されているかどうかにかかわらず、OOS への送信接続を行います。

1 つの方法と他の方法を使用することの長所と短所はありますか?

このアプローチでは、OOS はファイルの内容を直接ダウンロードしません。Storage Zone Controller は、ファイルバイトを OOS にダウンロードし、ストリームします。したがって、Storage Zone Controller サーバーの負荷が増大します。

ファイルの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。ユーザーの数とプレビューおよび編集操作の数に応じて、Storage Zone Controller サーバーの負荷が増大します。

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格納された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、Storage Zone Controller を次のように構成します。

1. Storage Zone 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、[オフィス **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 アプリケーション (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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

4. [**Office** オンライン編集を有効にする (必要な場合)] を選択します。
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. Storage Zone Controller コンソールで、[**Monitoring**] 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 アカウントに対してファイルのバージョン管理を有効にする必要があります。アカウントに対して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、プライマリコントローラとセカンダリ Controller 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、ブラウザ内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 を読み取り専用共有用に構成する方法については、[Storage Zone Controller 用の Citrix ADC を構成します。] を参照してください。(/ja-jp/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や編集で問題が発生した場合は、次の手順で特定の問題を特定して修正できます。

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. services.msc 内で OOffice WebApps または OfficeOnline Windows サービスが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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

3. 管理者として PowerShell を実行し、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、エラーや間違いがないか構成設定を確認してください。

ネットワークに関する考慮事項:

- OOS サーバは **https:**//*.sf-api.com（または**.eu**）に到達できる必要があります
- SZC Server は、**https:**//*.sf-api.com および **https:**//*.sharefile.com **(**または**.eu)** に到達できる必要があります。
- SZC サーバが OOS サーバ**https:**//<CustomerOOS/OWAEndpoint\>/hosting/discovery に到達できる必要があります。たとえば、https://oos.sharefileexample.com/hosting/discoveryのようになります。

マルチテナントストレージゾーンの構成

June 15, 2020

マルチテナントストレージゾーンは、Citrix Service Providers（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 Storage Zone Controller 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、無制限の数のテナントをサポートする 1 つのマルチテナント標準ストレージゾーンをドメイン上でホストできます。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、ファイル保存期間の設定、セキュリティ設定など、ShareFile のすべての優れた機能を活用します。
- 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。
- 新規顧客への迅速な導入が可能で、顧客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が軽減されます。

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資格のある販売代理店に在庫 SKU を注文する必要があります。CSP プログラムに適用するには、https://www.citrix.com/partner-programs/service-provider.htmlに進みます。

すでに CSP として登録されており、SKU を在庫している CSP 用の適切な ShareFile を注文している場合は、パートナーアカウントがすでに作成されています。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（）までお問い合わせください < acctsvcs@ShareFile.com >。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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。この方法で、admin 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」権限がオン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、それをパートナーアカウントに関連付けます。詳しくは、「Storage Zone Controller をインストールし、ストレージゾーンを作成する」を参照してください。
- マルチテナントモードで Storage Zone Controller をインストールします。前の手順で説明した Install の記事で、次の指定されたコマンドプロンプトを必ず実行してください。

```
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（例では 5.0.1）を更新する必要があります。

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

詳しくは、「Storage Zone Controller をインストールし、ストレージゾーンを作成する」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、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を要求する

テナントアカウントをリクエストするには、CSP 顧客アカウント要求フォームに入力します。

テナントアカウントをリクエストするときは、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 admin 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、テナントアカウントにログインして管理できるようになります。同じメールアドレスを持つアカウントには 2 人のユーザーが存在できないため、フォームで指定されているパートナー管理者のメールを、同じフォームの顧客管理者と同じにすることはできません。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

最も迅速に処理できるように、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する必要があります。

Citrix が要求されたアカウントをプロビジョニングすると、メールが送信されます。メールには、テナントサブドメインの詳細と、アクセスを設定するためのアクティベーションリンクが含まれます。ShareFile、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を使用した **Office** ファイルおよび **PDF** のプレビュー

この機能は、サポートされている Office Online サーバー環境でサポートされます。「セットアップについて詳しくは、ここをクリックしてください。」を参照してください。

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。

テナントの管理

パートナーアカウントには、**[**管理者設定**] > [**詳細設定**]** の下にある [テナント管理] ダッシュボードがあります。この集中管理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、デフォルトのストレージゾーン、ストレージ消費、アカウントステータス (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 情報権限管理機能 (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

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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

アップグレード

June 15, 2020

> 警告 StorageZones Controller 2.x
>
> を使用している場合は、まずバージョン 3.0.1 にアップグレードする必要があります。2.x から 3.0.1 にアップグレードするには、にお問い合わせください 支援のサポート。バージョン 3.0.1 にアップグレードしたら、最新バージョンにアップグレードできます。

このバージョンがインストールされている場合:	方法:
StorageZone コネクタ 1.0	StorageZone Controller 1.0 はアップグレードできません。StorageZone Controller 1.0 をアンインストールし、最新の Storage Zone Controller をインストールしてください
Storage Center 1.0	Storage Center 1.0 を Storage Center 1.1 にアップグレードします。次に、続行する前に、Storage Center 1.1 が正しく構成され、機能していることを確認します。次に、Storage Center 1.1 を StorageZones Controller 2.0 Update 1 にアップグレードします。その後、StorageZones Controller 2.0 アップデート 1 を StorageZones Controller 3.0.1 にアップグレードします。最後に、最新の Storage Zone Controller にアップグレードします。
Storage Center 1.1	Storage Center 1.1 を StorageZones Controller 2.0 アップデート 1 にアップグレードします。続行する前に、Storage Center 2.0 Update 1 が正しく構成され、機能していることを確認します。その後、StorageZones Controller 2.0 アップデート 1 を StorageZones Controller 3.0.1 にアップグレードします。最後に、最新の Storage Zone Controller にアップグレードします。
Storage Zone Controller 2.x	StorageZone Controller ー 2.x を StorageZones Controller 3.0.1 にアップグレードしてから、最新の Storage Zone Controller にアップグレードします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

このバージョンがインストールされている場合:	方法:
StorageZones Controller 3 のベータプログラム	StorageZones Controller 3 はベータ版プログラムソフトウェアであり、StorageZones を新たにインストールする必要がありました。それ以外の場合は、最新の Storage Zone Controller にアップグレードできます。
StorageZones Controller 3.x	最新の Storage Zone Controller へのアップグレード
StorageZones Controller 4.x	最新の Storage Zone Controller へのアップグレード

StorageZones Controller 3.0.1 以降を最新バージョンにアップグレードする

StorageZones Controller 3.0.1、3.x、4.x は、次の手順で説明するように、直接アップグレードできます。

1. 最新バージョンを入手するには、にお問い合わせください 支援のサポート。

   > 注:
   >
   > Storage Zone Controller をインストールすると、サーバー上のデフォルトの Web サイトがコントローラーのインストールパスに変更されます。

2. プライマリ Storage Zone Controller をアップグレードするサーバーで、次のようにします。
   - 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。
   - 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。
   - [完了] をクリックします。Storage Zone Controller コンソールが開きます。

   > 重要:
   >
   > Storage Zone Controller クローンを作成する場合は、構成を続行しないでください。ディスクイメージをキャプチャし、各 Storage Zone Controller を構成します。

   - Storage Zone Controller コンソールに戻るには、`http://localhost/configservice/login.aspx`を開くか [スタート] メニューから構成ツールを起動します。**[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。
   - 表示された情報を変更するには、[変更] をクリックして変更を行い、[保存] をクリックします。
3. プライマリ Storage Zone Controller のレジストリ設定を確認します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

すべてのアップグレードパスでレジストリ設定が追加されるわけではありません。ゾーンごとのファイル数を増やす必要があります。この機能を有効にするには、設定がレジストリに含まれていることを確認します。詳しくは、「ゾーンあたりのファイル数を増やす」を参照してください。

4. 各セカンダリ Storage Zone Controller で、次の手順を実行します。
   - 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。
   - プロンプトに応答して、[完了] をクリックします。Storage Zone Controller コンソールの [ログオン] ページが開きます。
   - ログオンします。表示された情報を変更するには、[変更] をクリックして変更を行い、[保存] をクリックします。
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。

StorageZones Controller 2.x を StorageZones Controller 3.0.1 にアップグレードする

以下の手順では、以前のバージョンの StorageZones Controller で作成された標準ゾーンをアップグレードします。

1. プライマリ StorageZones Controller 構成のバックアップの説明に従って、プライマリ StorageZones Controller をバックアップします。
2. http://www.citrix.com/downloads/sharefile.htmlの ShareFile ダウンロードページから、最新の StorageZones Controller 3 インストーラにログオンしてダウンロードします。

   > 注:
   >
   > StorageZones Controller をインストールすると、サーバー上のデフォルトの 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。

3. プライマリ StorageZones Controller をアップグレードするサーバで、次の手順を実行します。
   - StorageCenter.msi を実行して、ShareFile StorageZones Controller セットアップウィザードを起動します。
   - 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 StorageZones 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。
   - ［完了］をクリックします。StorageZones Controller コンソールが開きます。

   > 重要:
   >
   > StorageZones Controller クローンを作成する場合は、構成を続行しないでください。ディスクイメージをキャプチャし、各 StorageZones Controller を構成します。

   - StorageZones Controller コンソールに戻るには、`http://localhost/configservice/login.aspx`を開くか［スタート］メニューから構成ツールを起動します。［完了］をクリックするか、StorageZones Controller コンソールに戻ると、［ログオン］ページが開きます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- 表示された情報を変更するには、[変更] をクリックして変更を行い、[保存] をクリックします。

4. プライマリ StorageZones Controller レジストリ設定を確認します。

   すべてのアップグレードパスで、ゾーンごとのファイル数を増やすために必要なレジストリ設定が追加されるわけではありません。この機能を有効にするには、設定がレジストリに含まれていることを確認します。詳しくは、「ゾーンあたりのファイル数を増やす」を参照してください。

5. 各セカンダリ StorageZones Controller で、次の手順を実行します。

   - StorageCenter.msi を実行して、ShareFile StorageZones Controller セットアップウィザードを起動します。
   - プロンプトに応答して、[完了] をクリックします。StorageZones Controller コンソールの［ログオン］ページが開きます。
   - ログオンします。表示された情報を変更するには、[変更] をクリックして変更を行い、[保存] をクリックします。

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。
7. StorageZones Controller 3.4 にアップグレードするには、この記事で前述の「**StorageZones Controller 3.1** または **3.0.1** から **StorageZones** コントローラ **3.4** にアップグレードするには」を参照してください。

> 重要:
>
> 2.2.3 より前のバージョンから StorageZones Controller 3.0.1 にアップグレードし、以前に ProducerTimer または DeleteTimer の設定をカスタマイズしている場合は、FileDeleteService.exe.config で ProducerTimerInterval と eleteTimerInterval 設定を構成する方法については、ShareFile サポートにお問い合わせください。

Storage Zone Controller の管理

June 15, 2020

プライマリ Storage Zone Controller とセカンダリ Storage Zone Controller をインストールしたら、以下の手順に従ってコントローラーを管理し、障害回復に備えます。

Storage Zone Controller コンソールを開くには、`http://localhost/configservice/login.aspx`に移動するか、[スタート] メニューから設定ツールを起動します。

Storage Zone Controller 管理

- ストレージゾーンにセカンダリ Storage Zone Controller を統合する
- プライマリ Storage Zone Controller アドレスまたはパスフレーズの変更
- Storage Zone Controller を降格および昇格する

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- Storage Zone Controller を無効化、削除、または再デプロイする
- 新しいネットワーク共有にファイルを転送する
- プライマリ Storage Zone Controller 構成のバックアップ
- プライマリ Storage Zone Controller 構成を回復する
- プライマリ Storage Zone Controller の置き換え
- ファイル回復用の Storage Zone Controller の準備
- 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
- ShareFile クラウドとストレージゾーンを調整
- 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
- ShareFile データの移行
- Storage Zone Controller 構成で FIPS 140-2 モードを有効にする
- コネクタのお気に入り

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

June 15, 2020

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、次のことが必要です。

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簡単にプライマリに昇格できます。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 Controller 場合は、ホスト名または IP アドレスのみを入力でき、ShareFile が完全な URL を入力します。URL をテストするには、ブラウザのアドレスフィールドに URL を入力します。URL が

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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、有効な信頼できるパブリック 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 **Storage Zone Controller** アドレスまたはパスフレーズの変更

June 15, 2020

プライマリ **Storage Zone Controller** 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 Storage Zone Controller 外部アドレスを変更できます。

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、プライマリ Storage Zone Controller のホスト名をクリックします。
3. 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。

プライマリ **Storage Zone Controller** パスフレーズを変更するには

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の保護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、安全な場所に保管してください。

   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、紛失した場合は回復できません。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 Storage Zone Controller 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が失われると、すぐにすべてのストレージゾーンファイルへのアクセスが切断されます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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構成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 Storage Zone Controller 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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。

Storage Zone Controller を無効化、削除、または再デプロイする

June 15, 2020

Storage Zone Controller を無効にするには

> 注:
>
> 各 Storage Zone Controller 外部アドレスが異なる場合は、この手順を使用します。すべての Storage Zone Controller 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。

保守のためにサーバーをオフラインにする前に、Storage Zone Controller 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. 有効になっているチェックボックスをオフにし、[変更を保存] 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 Storage Zone Controller を削除する場合は、続行する前にそのコントローラーを降格します。

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. [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。

Storage Zone Controller を再デプロイするには

Storage Zone Controller 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

2. ShareFile Web インターフェイスで、「管理」**>**「ストレージゾーン」をクリックし、ゾーンを選択します。ゾーンは削除しないでください。
3. Storage Zone Controller を選択し、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. Storage Zone Controller 構成ウィザードを実行して、Storage Zone Controller 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

June 15, 2020

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、次の操作を行います。

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。デフォルトでは、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、この保存場所への フルアクセス権が必要です。

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. [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 データ用のストレージゾーンにのみ予約します。

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設定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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

June 15, 2020

Storage Zone 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 Zone Controller サーバーのスナップショットを作成し、構成をバックアップし、ファイル回復用の Storage Zone Controller の準備を行います。

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、バックアップがなくても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、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。

Storage Zone Controller インストーラーには、プライマリ Storage Zone 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、ゾーンの構成情報、ShareFile Data 用のストレージゾーン、SharePoint 用のストレージゾーンコネクタ、および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が含まれます。

バックアップおよび回復コマンドでは、Storage Zone 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、http://technet.microsoft.com/en-us/sysinternals/bb897553からダウンロードできます。

> 注:
>
> この手順は、セカンダリ Storage Zone Controller には適用されません。セカンダリ Storage Zone Controller を回復するには、サーバーに Storage Zone Controller を再インストールし、プライマリ StorageZones Controller にサーバーを接続します。

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ため、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、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 のポリシーを使用すると、署名の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。
   - 既定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
     ```

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- 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。

3. PowerShell プロンプトから、ConfigBR.dll モジュール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 Get-SfConfig コマンドを実行します: Get-SfConfig -PrimaryZoneController ”server”-Passphrase ”passphrase”-FilePath ”fullpath”

   次に例を示します:

   ```
   1 Get-SfConfig -PrimaryZoneController ”`https://myserver.domain.com/ConfigService/`” -Passphrase ”mypassphrase” -FilePath ”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」	プライマリ Storage Zone Controller サーバー名または IP アドレス。これは、[例] の下に示されている次の形式のいずれかであり、末尾にスラッシュを含める必要があります。	ローカルサーバーに接続する: http://localhost/ConfigService/; リモートサーバーに接続する: http[s]://myservername.domain.com/ConfigService/; DNS の問題によってサーバー名への接続が妨げられる場合は、リモートサーバーに接続する: http[s]://10.40.37.5/ConfigService/
“passphrase”	Storage Zone Controller に指定されたパスフレーズ。	“MyPassphrase”
“fullpath”	バックアップファイルを保存する場所。	“c:\szc-backup.bak”

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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 Zone Controller の構成を回復する方法は、「プライマリ Storage Zone Controller 構成を回復する」を参照してください。

プライマリ **Storage Zone Controller** 構成を回復する

June 15, 2020

Storage Zone Controller は、プライマリ Storage Zone Controller が削除されたり、使用できなくなった場合に、障害回復用の次のオプションを提供します。

- セカンダリ Storage Zone Controller が使用可能な場合は、セカンダリコントローラーをプライマリコントローラーに昇格させます。
- セカンダリ Storage Zone Controller が使用できず、プライマリ Storage Zone Controller 構成（プライマリ Storage Zone Controller 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を作成します。
- プライマリ Storage Zone Controller 構成のバックアップがない場合に、すべての Storage Zone Controller が誤って削除されたり、使用できなくなった場合は、部分的な回復のみが可能です。ShareFile Data 用のストレージゾーンのゾーンと構成は回復できますが、ストレージゾーンコネクタは回復できません。

> 重要:
>
> この手順では、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。

バックアップファイルからプライマリ **Storage Zone Controller** を回復するには

> 注:
>
> 以下の手順は、プライマリ Storage Zone Controller にのみ適用されます。セカンダリ Storage Zone Controller を回復するには、サーバーに Storage Zone Controller を再インストールし、プライマリ Storage Zone Controller にサーバーを接続します。

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ため、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、署名のないローカルのスクリプトの実行が許可されてい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 のポリシーを使用すると、署名の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`

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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:
   >
   > http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx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。

   - 既定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。

3. PowerShell プロンプトから、ConfigBR.dll モジュール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とおりです。

   - サーバーには、プライマリ Storage Zone Controller サーバー名または IP アドレスを指定します。次の形式のいずれかで、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/`

   - パスフレーズには、Storage Zone Controller 用に指定されたものを使用します。
   - fullpath は、バックアップファイルの場所と名前です。たとえば、`c:\szc-backup.bak`のようになります。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

バックアップファイルを使用せずにプライマリ **Storage Zone Controller** を回復するには

バックアップファイルがない場合は、ゾーンと ShareFile Data のストレージゾーンの構成を回復できますが、ストレージゾーンコネクタは回復できません。

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。

   - 既定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
     ```

   - StorageZones 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。

2. PowerShell プロンプトから、ConfigBR.dll モジュール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。

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

   各項目の意味は次のとおりです。

   - ZoneID は次のように取得できます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

a) ShareFile Web インターフェイスで、[管理] **>** **[**ストレージゾーン] をクリックし、サイト名を右クリックし、**[**プロパティ**]** を選択します。

表示されるアドレスは、次のゾーン 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。

- Storage Center ID 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] をクリックし、サイト名をクリックしてホスト名を右クリックし、[プロパティ] を選択します。

表示されるアドレスは、次のストレージ 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、そのゾーンで ShareFile データのストレージゾーンが有効になっている場合にのみ必要です。
- StorageUsername と StoragePassword は、ShareFile データのストレージゾーンがゾーンに対して有効になっており、ストレージロケーションが認証を必要とする場合にのみ必要です。
- 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回復するには、Storage Zone Controller 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

June 15, 2020

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。次の手順では、構成設定とすべてのデータが確実に転送されます。

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 Controller 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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 **Storage Zone Controller** の準備

June 15, 2020

> 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 日ごとに実行する必要があります。

ファイル回復の準備方法は、データの格納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 — サードパーティ製ストレージシステムを Storage Zone Controller と使用する場合、サードパーティ製ストレージは冗長であり、ローカルバックアップは不要です。ただし、ファイルを削除した ShareFile ユーザーは、しばらくの間、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 日後、ShareFile のごみ箱からファイルを回復できません。回復期間の後、ファイルはゾーンから削除され、したがって冗長なサードパーティストレージから削除されます。回復時間が適切でない場合は、次の解決策のいずれかを検討してください。
  - ShareFile のごみ箱に残っている時間を増やします。これを行うには、C:\inetpub\wwwroot\Citrix\StorageCenter で [期間] の設定の値を変更します。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。保存期間を長くすると、必要なサードパーティ製ストレージの量も増加す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、バックアップに適切なリテンション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る共有をプライベートデータストレージとして使用する場合は、オンプレミス Storage Zone Controller ローカルファイルストレージとレジストリエントリのバックアップはお客様が担当します。ShareFile、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: データ損失から保護するために、Storage Zone Controller サーバー構成をバックアップするのスナップショットを作成し、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 Storage Zone Controller 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操作を実行できます。

- 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、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回復します。

  詳しくは、「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」を参照してください。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- 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 クラウドに保存されたメタデータをオンプレミスの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 File クラウドから完全に削除します。

  詳しくは、「ShareFile クラウドとストレージゾーンを調整」を参照してください。

前提条件

- Windows Server 2012 R2 または Windows Server 2008 R2
- Windows PowerShell (32 ビット版と 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している必要があります。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。
- 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。http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx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。

障害回復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.psm	回復キュー操作を処理する PowerShell モジュール。
recovery.log	回復処理の出力を保存するログファイル。
recoveryerror.log	回復処理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）文字列との変換を処理するための.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ーで、persistentStorage フォルダーをバックアップするフォルダーを作成します。

ShareFile Data ファイルバックアップ用のストレージゾーンは、Storage Zone Controller 永続ストレージと同

© 1999-2021 Citrix Systems, Inc. All rights reserved.

じレイアウトにする必要があります。

バックアップの場所が Storage Zone Controller 永続ストレージと同じレイアウトになっていない場合、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

バックアップのレイアウト

```
\\\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** 日ごとに実行する必要があります。

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。次のコマンド例では、デフォルトの Storage Zone Controller インストールフォルダーを使用します。

1. Storage Zone Controller 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ため、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、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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

たとえば、RemoteSigned、Unrestricted、または Bypass のポリシーを使用すると、署名の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

3. PowerShell に正しい CLRVersion があることを確認するには、次のように入力します:

   $psversiontable

   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 の値を 4.0 以上にする必要があります。そうでない場合は、Windows PowerShell の 32 ビット版と 64 ビット版の両方で、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) 次の内容のファイルを作成します。

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

   c) ファイル／名前を付けて保存を選択し、powershell.exe.config というファイルに名前を付け、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 を使用して次のように PowerShell を起動します。

   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\p

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

5. Storage Zone Controller インストールフォルダーにある障害回復ツールフォルダーに移動します。

   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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

7. 回復キューを作成するには、次のように入力します: New-SCQueue -name recovery -operation recovery

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

   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。

   \\server\(*Your* Primary Storage Location)\Queue. 92736b5d-1cff-4760-92c8-d8b04dc92cb2 などのキューフォルダが表示されます。

8. 次のセクションで説明するように、PowerShell の回復スクリプトをカスタマイズします。

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

DoRecovery.ps1 PowerShell スクリプトは、回復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および保存場所が含まれます。

1. Storage Zone Controller で、回復 PowerShell スクリプトに移動します。

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

2. スクリプトを次のように編集します。

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

   b. Storage Zone Controller の永続ストレージの UNC パスを指すように $StorageRoot パラメーターを設定します。例: $storageRoot = “\\10.10.10.10\StorageLocation\persistentstorage”

回復処理をテストするには

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 時間ほど経つと、ファイルが永続的なストレージ ($backupRoot に指定されたパス) に表示され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、ファイルを選択して、[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] の順に選択し、ゾーンをクリックし、[ファイルの回復] をクリックします。
6. [回復日] 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およびアップロードされた後の日時を選択します。

   指定した日時のストレージゾーンのファイル一覧が表示されます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

7. ファイルのチェックボックスをオンにします。
8. 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。

   ファイルがバックアップキューに追加され、回復する準備が整いました。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. ファイルを回復するには、次の手順で行います。

   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、「アイテムが回復しました」というメッセージが表示されます。ファイルが永続的な保存場所に追加されます。
10. リストアした ShareFile Web サイトから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**

  回復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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

回復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回復タスクが必要な場合は、次の手順に従います。

1. Windows タスクスケジューラを起動し、[アクション] 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. タスクの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、またはストレージ場所への書き込み権限を持つ指定ユーザー) 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. **[**タスクの開始**]** で **[**スケジュールに従って**]** を選択してから、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**]** タブの **[**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.**[**作業フォルダ**]** で、Storage Zone Controller インストール場所にある [障害回復] フォルダを指定します。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 Controller4.0 では、削除サービスのタイマーは 45 日に設定されます。45 日間のデフォルト期間は、以前の設定を上書きします。既定の期間を変更するには、FileDeleteService.exe.config を C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc で編集します。

```
<!--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サービスの削除デフォルト期間の変更

一部のアップグレードシナリオでは、DeletePeriod の値が「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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller で 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

Storage Zone Controller 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

June 15, 2020

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、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一覧が表示されます。
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ため、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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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。PowerShell ウィンドウで：`Get-ExecutionPolicy`

たとえば、RemoteSigned、Unrestricted、または Bypass のポリシーを使用すると、署名の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。

- 既定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、「アイテムが回復しました」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、正常に回復されたファイルの回転アイコンが ShareFile Web インターフェイスから消えます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

June 15, 2020

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 クラウドに保存されているメタデータとの間に一貫性のない状態になります。これらの相違点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:
>
> リコンサイルは、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実行します。リコンサイルは、指定した日時にローカルファイルストレージに見つからないファイルのメタデータを ShareFile クラウドから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、日時を選択します。
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。

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

June 15, 2020

> 重要:
>
> StorageZones 4.2 のアプリケーションコードの更新により、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/概要

- StorageZones Controller 4.2 以降を使用するユーザー
- 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。
- 更新ログファイルの場所

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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。

SZ 4.2 以降にアップデートするクライアントは、SF Antivirus にリンクする既存のスケジュールされたタスクを使用して、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 Storage Zone 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
```

更新ログファイルの場所

管理者は、log4net.config エントリを編集して、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、次の行を変更して、ログファイルの場所を変更する必要があります。

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

Storage Zone 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、デフォルトで C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus. に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した後、ファイルのアップロード要求ごとに、Storage Zone Controller がファイルをウイルス対策スキャン用にキューに入れます。スキャンしたファイルの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 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. にある 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。

ICAP の RFC 標準に準拠したウイルス対策スキャンプラットフォームでの ICAP プロトコルの使用は、StorageZones Controller 4.2 以降でサポートされています。ICAP AV の設定に関する情報は、この記事でさらに詳しく説明します。

前提条件

- Storage Zone Controller でウイルススキャン (SfAntivirus.exe) を実行する場合は、Controller で暗号化が無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ソールの構成ページで、[Enable Encryption] チェックボックスがオフになっていることを確認します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> 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。このファイルを構成しても、ゾーンにすでに存在するファイルやアイテムはスキャンされません。

ロケーションの設定を準備するには

1. Storage Zone Controller 以外のサーバーでウイルススキャンを実行するには、以下の手順に従ってください。
    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) Storage Zone Controller 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 Storage Zone Controller の設定の値で編集します。
    a) CommandFile の場合: 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: 構成ファイルに用意されているコマンドライン設定の例です。ウイルス対策ソフトウェアと環境に適した設定を指定します。
    c) ScanFileTimeout の場合: ファイルのサイズが大きくなると、スキャンに時間がかかることがあります。ストレージに期待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くなります。
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** スキャンに使用する

StorageZones Controller 4.2 以降では、ICAP の RFC 標準に準拠し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、SZ 5.0.1 以降の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ーのアドレスを入力します。ICAP 応答変更サービスの URL です。`ICAP://SERVER/RESPMOD`

[接続のテスト] をクリックして設定を確認します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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:
>
> 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) タスクに意味のある名前を指定します。
   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、ストレージの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かかわらず実行する**]** 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) [最も高い権限で実行する] 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 **[**スケジュールに従って**]** 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] 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] では、次の規則が適用され、[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

- Storage Zone 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、必ず停止または削除してください。
- .NET 4.6.2 以降をホストマシンにインストールします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

オンプレミスの Storage Zone Controller の Scan Service には、Symantec コマンドラインの 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行います。

この機能を有効にするには、AntiVirus/OnPrem/AVScanService/AVScanService/appSettings.config に次の構成キーと値を追加します。

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

コマンドラインツール固有の構成

Storage Zone Controller 5.2 のアップグレードまたは新規インストールには、新しい設定ファイルが含まれています。

```
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。

設定キーの値については、例の値を含めて説明します。

- 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ドキュメントを参照して、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”
  ```

最大ファイルサイズの強制に関する注意事項（拡張子を除く）

バージョン 5.2 より前のバージョンでは、拡張機能の除外または最大ファイルサイズの強制をコマンドライン AV で強制できませんでした。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、除外された拡張子と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。

これらの設定は次のように命名されました。

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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

Storage Zone 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 の両方に適用可能であ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”/>
```

アップグレード時に、これらの設定の名前は変更されません。手動で名前を変更することはできますが、ICAP に加えて AV コマンドラインでも同じ設定を使用できます。

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

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

ShareFile データの移行

June 15, 2020

あるオンプレミスのゾーンから別のゾーンに ShareFile データを移行するには、複数の方法があります。

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

前提条件

- ソースゾーンがターゲット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送信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、宛先ゾーンのブラウザ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を使用した移行

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ユーザーのゾーン間で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、非同期移行操作がすぐにトリガーされ、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-「ユーザー」に移動し、「従業員」ユーザーを見つけます。ユーザーをクリックして、自分のプロフィー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 (既にインストールおよび構成されている場合)。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

特定のフォルダのデータを移行する- 対象フォルダに移動し、フォルダ名の右側にある [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は、元のゾーンの ［ストレージの場所］内で ［キュー］フォルダーにプレースホルダーファイルを作成します。

プレースホルダー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 による移行

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 は、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

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

最適なパフォーマンスを得るために、この方法は、サイズが 2 GB 未満のフォルダーに推奨されます。

Storage Zone Controller 構成で **FIPS 140-2** モードを有効にする

June 15, 2020

ShareFile に次の構成を適用する前に、Windows Server で FIPS モードが有効になっていることを確認します。必要な操作:

1. レジストリエディタ（regedit）を起動します。
2. パスを参照します: `HKEY_LOCAL_MACHINE\SOFTWARE\PowerShell\Server\16`
3. レジストリ値 **UseFipsCompriantAPI** を確認します。
4. 値データ (DWORD) が **1** の場合、FIPS 準拠モードが有効になります。

FIPS 準拠モードが有効になっていない場合は、次を使用して FIPS 準拠モードを有効にします。

1. Windows システム管理者として Windows にログオンします。
2. **[スタート]** ボタン、**[コントロールパネル]**、**[管理ツール]** の順にクリックします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> 次の手順では、大きなアイコンに切り替える必要があります。

3. **[**ローカルセキュリティポリシー**]** をクリックします。[ローカルセキュリティ設定] ウィンドウが開きます。
4. ナビゲーションウィンドウで、[ローカルポリシー] をクリックし、[セキュリティオプション] をクリックします。
5. 右側のウィンドウで、**[**システム暗号化**:** 暗号化、ハッシュ、署名に **FIPS** 準拠アルゴリズムを使用する**]** をダブルクリックします。

   > 注:
   >
   > 上記の設定を有効にすると、マシン上のすべてのアプリケーションに影響する可能性があります。

6. 表示されるダイアログボックスで、**[**有効**]**、**[**適用**]**、**[OK]** の順にクリックします。
7. **[**ローカルセキュリティ設定**]** ウィンドウを閉じます。

詳しくは、Microsoft サポート記事を参照してください。

既定では、Storage Zone Controller は、FIPS 140-2 規格に準拠していない暗号化モジュールを使用できます。Storage Zone Controller をインストールした後、ConfigService を実行する前に、顧客が自分の Controller で次のコード例を追加して、FIPS 140-2 準拠を有効にする必要があります。

```
<appSettings>

<add key=”fipsOnly” value=”1” />

</appSettings>
```

次のファイルの末尾に、<configuration> 要素の子として前述のコードサンプルを追加します。

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

次に、IIS をリセットし、すべての ShareFile サービスを再起動します。または、コンピュータを再起動します。

> 注:
>
> 情報リソース管理 (IRM) はサポートされていません。

コネクタのお気に入り

June 15, 2020

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ストレージゾーン Controller 5.0 では、ユーザーは、ShareFile WebApp 内の **[**ネットワーク共有**]**、**[SharePoint]**、および **[Documentum** コネクタ**]** の下に、コネクタフォルダをお気に入りとして作成できます。詳しくは、Knowledge Center の記事を参照してください。

お気に入りへのコネクタフォルダの追加は、ShareFile モバイルでサポートされています。また、制限ゾーンでのコネクタフォルダの [お気に入り] の作成はサポートされていません。

ShareFile データのストレージゾーンを管理する

June 15, 2020

ShareFile Data のストレージゾーンは、ShareFile で管理されるクラウドまたはクラウドの代わりに使用できます。

ゾーン間でホームフォルダとファイルボックスを移動する

以下の手順に従って、ホームフォルダーとファイルボックスを ShareFile 管理クラウドストレージからプライベートゾーンまたはプライベート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。
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、[フォルダの追加] をクリックします。
3. 通常どおりにフォルダ情報を指定し、[ストレージサイト] で、このフォルダとその内容を格納するストレージゾーンを選択します。[フォルダを作成] をクリックします。
4. 通常どおりにフォルダを構成します。フォルダーを作成するときに、ShareFile 管理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のどちらを使用するかを選択できます。
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。

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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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て、[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。
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。

ストレージキャッシュ操作のカスタマイズ

ShareFile ユーザーによるファイルのアップロード、ダウンロード、削除のリクエストは、Storage Zone Controller によって処理され、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の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する場合、ShareFile クライアントはそのファイルを永続ストレージキャッシュに送信します。次に、Storage Zone Controller がファイルをサードパーティ製のストレージシステムにアップロードします。

Storage Zone Controller は、`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`で設定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:

- Storage Zone Controller 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) に配置します。
- 次の設定は、サービス削除操作のタイミングを制御します。
  - minDeletionAge は、ファイルが最後にアクセスされた時点からファイルが削除できる時点までの最小期間を指定します。デフォルトは 1 日です。最小設定は 8 時間です。
  - offPeaktimeOfDayStart および 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、午前 4 時。
  - ProducerTimerInterval と DeleteTimerInterval は、サービス削除操作の頻度を制御します。デフォルト値 (1 日) がサイトに適さない場合は、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入れられたファイルなどの一時的な項目を含むフォルダも管理します。削除サービスは、それらのアイテムを作成してから 24 時間後に削除します。
- 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が、サポートされているサードパーティストレージで対応する BLOB を持っているかどうかを判別します。
  - デフォルトでは、10 秒ごと (CheckSizeThreaSholdTimer) 削除サービスは、ストレージキャッシュがディスクしきい値 10 GB (DiskSpaceDropOutThresholdGB) を超えているかどうかを判断します。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 (CacheCleanupFileThreasholdPeriodUnExpected) を削除します。ディスクサイズがしきい値に達したためではなく、通常のスケジューリングの結果として削除サービスが実行されると、過去 24 時間以内にアクセスされていないファイル (CacheLeanUpFileThresholdPerioDNormal) がサポートされているサードパーティ製のストレージ内にある場合、サービスは削除します。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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ダウンロードしたファイルの場合:

- Storage Zone Controller は、ダウンロード要求を受信すると、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。ファイルがキャッシュにない場合、Controller はサードパーティ製のストレージシステムから永続的な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 (CacheLeanUpFileThresholdPerioDNormal) 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 日前に削除されたファイルのリストを取得します（期間）。
- 次に、delete サービスは、対応するファイルをストレージの場所から削除するか、対応するオブジェクトをサードパーティのストレージから削除します。

サービスのデフォルト期間の削除

StorageZones Controller 4.0 では、削除サービスタイマーは 45 日に設定されています。45 日のデフォルト期間は、以前の設定を上書きします。

1. 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 を編集します
   - `<!--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

June 15, 2020

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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Active Directory ルックアップに使用するドメイン Controller をユーザーが指定できるようにする追加設定を使用できます。本記事の「認証」の項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やフォルダーの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、Admin または Employee ユーザーに 次の権限が必要です。

- コネクタの作成と管理
- 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。

以下の手順では、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. コネクタの作成と管理のアクセス許可を持つ管理者として、ShareFile アカウントにサインインします。
2. [管理設定] **>** [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 Data 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にあるか、コネクタのゾーンと信頼関係を持っている必要があります。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] で、SharePoint ルートレベルサイト、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 を次の形式で指定します。

   - SharePoint ルートレベルサイトへの接続例: `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、SharePoint システムフォルダをユーザーから隠します。
   - SharePoint サイトコレクションへの接続例: `https://sharepoint.company.com/site/SiteCollection`

© 1999-2021 Citrix Systems, Inc. All rights reserved.

サイトコレクションへの接続により、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:

  変数%USERDomain% を使用して、認証されたユーザーのログオン名を、そのユーザーの NetBIOS 名に置き換えます。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、変数%URLUserName% 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% 変数を使用するには、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%`
  は次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対して識別するために使用されます。小さな画面を持つモバイルデバイスに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、ユーザーおよび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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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。

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 Data 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にあるか、またはコネクタとの信頼関係を持っている必要があります。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] で定義されているように、ユーザーのホームフォルダパスにリダイレクトします。パスの例: %HomeDrive%
   - %TSHomeDrive%

     Active Directory Directory プロパティ MS-TS-ホームディレクトリ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ースナップインでは、ユーザーオブジェクトを編集するときに、[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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- %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ログオン名が「abc\ johnd」の場合、変数は「abc」で置き換えられます。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。ユーザーの権限に応じて、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、ユーザーに対してファイル共有を識別するために使用されます。小さな画面を持つモバイルデバイスに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、ユーザーおよび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の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。

ステップ

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 [**Modify**] 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存在す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あ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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> 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ます。Documentum Content Server では大文字と小文字が区別されるため、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。ただし、Documentum Content Server では大文字と小文字が区別されます。

前提条件

1. StorageZones Controller 4.1 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 サーバ上に配置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、特定の構成の変更が必要です。これらの変更については、この記事で詳しく説明します。

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。

コネクタが作成されると、Web アプリおよびモバイルアプリからコネクタにアクセスできます。

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）:

- ブラウズ
- 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

Web アプリ

- コネクタを作成
- ブラウズ
- 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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

未サポート

- Documentum コネクタ内に保存されているファイルの共有
- 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、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。ただし、Documentum Content Server では大文字と小文字が区別されます。

Documentum コネクタの Citrix ADC 構成

お使いの環境で Citrix ADC を使用する場合は、Citrix ADC 構成を次のように変更します。

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

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

2. [コンテンツの切り替え] > [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. 管理者として ShareFile アカウントにサインインし、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. 管理者として ShareFile アカウントにサインインし、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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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単一の DC または複数の DC に設定できます。複数の DC は、コ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** コネクタからダイレクトリンクを取得する

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する場合は、以下を追加することで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、NTLM と Negotiate を使用することをお勧めします。

データ損失防止

June 15, 2020

ShareFile のデータ損失防止（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。

ストレージゾーンにアップロードされたドキュメントは、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、共有およびアクセス権限を調整します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

サポートされている **DLP** システム

Storage Zone Controller は、ICAP プロトコルを使用して、サードパーティの DLP ソリューションと対話します。既存の DLP ソリューションで ShareFile を使用した場合、既存のポリシーやサーバーを変更する必要がありません。ただし、負荷が大きくなると予想される場合は、ICAP サーバーを ShareFile データの処理専用にすることもできます。

一般的な ICAP 準拠の DLP ソリューションには、次のものがあります。

- シマンテックの情報漏えい対策
- McAfee DLP Prevent
- Websense TRITON AP-DATA
- RSA データ損失防止

ShareFile e 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警告のポリシー管理を一元管理することができます。送信メールの添付ファイルや Web トラフィックの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のいずれかをすでに使用している場合は、ShareFile Storage Zone Controller を同じサーバーに接続できます。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 ICAPS をサポートしている場合、セキュア ICAP (ICAPS) もサポートします。

DLP を有効にする

ShareFile および Storage Zone 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 Zone 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 に対して有効になっていることを要求または確認するには、に要求を送信します Citrix サポート。

一部のアカウントでは、DLP を有効化するには、ShareFile Web サイトの新しいユーザーエクスペリエンスを有効化する必要があります。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 Zone 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. StorageZones Controller 3.2 以降をインストールまたはアップグレードします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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、[監視] 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** サーバーに到達可能であ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

アカウントおよび Storage Zone 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るすべてのファイルのバージョンが機密コンテンツについてスキャンされます。スキャンの結果は、データの分類として 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、ファイルに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できます。ただし、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 は共有できません。

データの分類は次のとおりです。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- **Scanned**: OK — DLP システムによってスキャンされ、正常に渡されたファイル。
- **Scanned: Reject** ed — 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検出されたファイル。
- **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 が管理す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保存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 を構成する前にアップロードされた DLP が有効な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**:** 拒否」とマークされます。それ以外の場合、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。ShareFile 管理者は、3 つのカテゴリごとに、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。
- サードパーティの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無効になっていますが、**[**管理者**] > [**詳細設定**] > [**クライアントによるファイルの共有を許可**]** 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場合、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、データ分類の共有権限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権限も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」**>**「情報漏えい対策」をクリックします。
2. [ファイルの 内容に基づいてファイルへのアクセスを制限する] オプションを **[**はい**]** に変更します。
3. 各データ分類に対して許可されるアクションを構成します。

> 重要:
>
> ShareFile On-Demand Sync ツールでは、通常の操作にはダウンロード権限が必要です。展開に 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に対して従業員のダウンロードを有効にします。

Storage Zone Controller から DLP システムにファイルを送信する場合、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。この情報により、DLP サーバー管理者は、機密性の高いコンテンツを含む ShareFile 固有の詳細を表示できます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

DLP の詳細設定

DLP スキャンプロセスを調整するには、Storage Zone Controller の`wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`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
scan-interval	DLP サービスが DLP キューに新しいファイルをチェックし、処理のために DLP ICAP サーバーに送信する頻度。	30 秒
icap-response-timeout	Storage Zone Controller が ICAP 応答を待機してから、ICAP サーバーを使用不可とマークする時間。	30 秒
icap-exclude-extensions	DLP スキャンから除外する拡張子のカンマ区切りリスト。DLP サーバーは、これらの拡張子で終わる名前を持つファイルを処理しませんが、スキャン済み:OK とマークします。値の例:「exe, jpg, bin, mov」	なし
icap-max-file-size-bytes	処理のために DLP サーバーに送信するファイルの最大サイズ（バイト単位）。値 0 は、最大値がないことを意味し、すべてのファイルサイズが送信されます。ゼロ以外の値で構成すると、DLP サーバーは構成サイズより大きいファイルを処理しませんが、Scanned: OK とマークされます。	31457280 (30 MB)
x-queue-items-to-process	各スキャン間隔反復ごとにスキャンするキュー内のアイテムの最大数。この値を小さくすると、StorageZone に大量のファイルが追加される場合に DLP サーバーへの影響が軽減されます。	512

© 1999-2021 Citrix Systems, Inc. All rights reserved.

設定	説明	デフォルト値
max-queue-processing-threads	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 サーバを使用する他のネットワークサービスをブロックしないようにするには、妥当な制限内である必要があります。	4
Icap-reqmod-http-request-verb	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 に変更できます。	PUT

DLPExistingFiles tool

ShareFile Storage Zone Controller は、ICAP を介してストレージセンターとデータ損失防止（DLP）プロバイダを統合するための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のみによって読み込まれるキューを処理します。つまり、ICAP が有効になる前にゾーン内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、スキャンしたファイルを再スキャンするためにキューに入れることもできます。

名前の通り、ツールは現在 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、実行するには PowerShell が必要です。PsExec または、ネットワーク共有の場所にアクセスするために Network Service としてスクリプトを実行する必要があるため、同様のツールも必要です。

場所

インストール済みの Storage Zone Controller の場合、ツールは`<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1`にあります。Storage Zone Controller のインストール場所は、デフォルトで `C:\inetpub\wwwroot\Citrix\StorageCenter`です。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ツールの実行前の考慮事項

次の状況に応じて、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規定されている制限。
- 指定された基準の項目数。この考慮事項は、キューサイズの制限が 0 以下に設定されていない限り当てはまります。この場合、キューディレクトリ内の最大サイズが 200,000 個であると想定されます。

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、キューのサイズ制限は 500 アイテムに設定されます。スキャンされていないアイテムが 500 個を超える場合、キューに 500 個のアイテムがいっぱいになると、ツールが停止します。停止した場所を追跡するために、ツールは最後に取得されたアイテムの作成日を格納します。このツールは、DLPExistingFiles-enddate.temp という名前の<storage zones controller installation location>\SC の一時ファイルに日付を保存します。

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。ツールでは、特定の操作が完了しても一時ファイルは削除されません。代わりに、特定の操作のすべてのバッチが完了した時点で、ゾーン管理者はファイルを削除できます。このような状況のため、完全な操作が完了すると、別の操作を実行する前に、一時ファイルが存在する場合は、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。

```
1 PsExec.exe -i -u ”nt authority\network service”
2
3 ”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ている PowerShell が開きます。実際にネットワークサービスとして実行されていることを確認するには、**whoami** を実行して結果を確認します。

PowerShell が開いたら、そこでツールを直接実行して、必要なタスクを実行します。

```
1 <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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- **-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します。サブオプション:
  - スキャンなし: 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 DLP 以前の時代ファイルなどです。
  - **ScannedOK**: クリーンとしてマークされたスキャン済みファイル。
  - **ScannedRepeded**: クリーンでないとマークされたスキャンされたファイル。
  - スキャン済み: すべてのスキャン済みファイル。
- **-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数を指定するために使用します。
- **-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 AM 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のみ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 を介し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、この記事で前述した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 のゾーン内のすべてのスキャン済み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 日の午前 11 時 30 分まで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」としてマークし、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”
```

監視

June 15, 2020

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Storage Zone Controller と ShareFile 管理者インターフェースには、Storage Zone Controller アクティビティを監視し、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。

- 一般的なコンポーネントのステータス — Storage Zone Controller コンソールの [Monitoring] タブには、トラブルシューティングプロセスを開始するための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、ハートビートステータスなどの項目に提供されます。ハートビートステータスは、Storage Zone Controller が ShareFile コントロールプレーンへの送信接続を示します。

  Storage Zone Controller は、ShareFile Web アプリケーションに 5 分ごとに更新を送信します。ShareFile Web アプリケーションが 10 分以内にアップデートを受信しない場合、Storage Zone Controller はオフラインとしてマークされます。

  [Monitoring] タブの赤色で表示される項目については、ログファイルで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 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。

- **Storage Zone Controller** のサーバー情報 — ストレージの使用、ネットワークの使用、およびサーバーの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 アカウントにログオンし、**[管理者] > [StorageZones]** の順に選択し、ストレージゾーンをクリックし、Storage Zone Controller のホスト名をクリックします。

- ゾーン情報 — ゾーンのストレージ使用、ネットワーク使用、および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 アカウントにログオンし、**[管理者] > [StorageZones]** の順に選択し、ゾーン名をクリックします。

- **Storage Zone Controller** 正常性ステータス — ShareFile.com がゾーンに参加している Storage Zone Controller 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、正常性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、**[管理者] > [StorageZones]** で、[正常性] 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、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。

- 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、Storage Zone Controller 構成とそのコンポーネントに関する詳細情報が提供されます。

ログファイル

次の Storage Zone Controller ログファイルは、デフォルトで`C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`にあります:

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ログファイル名	次のログ情報が含まれます。
cfgsrv-%date%.txt	Storage Zone Controller 構成アクション (既存のストレージゾーン構成の変更、新しいストレージゾーンの作成、既存のプライマリ Storage Zone Controller への新しい Storage Zone Controller の結合など)
sc-%date%.txt	標準ゾーンの ShareFile データのアップロードと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アップロードと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
sharepoint-%date%.txt	SharePoint の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
cloudstorageuploader-%date%.txt	クラウドストレージアップローダーサービス（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へ）
copy-%date%.txt	ShareFile コピーサービス
delete–%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便利です。

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のストレージゾーンコネクタ	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
SharePoint 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 Storage Zone Controller コンポーネントとサービスの拡張ログを有効にします。

1. Storage Zone Controller サーバーで、IIS を開きます。
2. 既定の Web サイトに移動し、[アプリケーションの設定] 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

5. 問題を解決した後、ログ記録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。

トラフィックが Storage Zone Controller に到達しているかどうかを確認するのには、IIS ログ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。Storage Zone Controller の IIS ログは c:\inetpub\logs\LogFiles\W3SVC1. にあります。

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。

インストールと構成のトラブルシューティング

問題	説明と解決策
Storage Zone Controller 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	このメッセージは、通常、IIS またはASP.NETに問題がある場合に発生します。IIS の役割が 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 有効になっていることを確認します。
Storage Zone Controller 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、ASP.NETの ISAPI および CGI の制限が [許可] に設定されていないことを示します。
アップロード試行後に「HTTP エラー 413 — リクエストエンティティが大きすぎます」が表示される	このメッセージは、ストレージゾーンへのアップロードが失敗した後で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の設定が原因である可能性があります。この問題を回避するには、Storage Zone Controller 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。
Storage Zone Controller 構成中に IIS エラーが発生する	IIS エラーは通常、ASP.NETが完全に設定されていないことを示します。IIS マネージャーの [ISAPI および 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。が IIS に登録 ASP.NET されていることを確認します。IIS マネージャーの [アプリケーションプール] で、ASP.NET 一覧があることを確認します。手動でASP.NETを登録するには、次の表に続くコマンドラインを参照してください。問題が解決しない場合は、IIS と ASP.NET セットアップを確認してください。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

問題	説明と解決策
Storage Zone Controller 構成中に「ストレージセンターのバインドを保存できませんでした」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ています。デフォルトでは、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。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。Network Service アカウントの代わりに指定ユーザーアカウントを使用する場合、指定ユーザーアカウントには、プライベートデータストレージ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の作成と管理権限がない場合に発生することがあります。ShareFile 管理者コンソールを使用して、その権限を設定します。
送信要求はブロックされる	送信要求がブロックされると、cfgsrv ログに System.Net.WebException: リモートサーバーがエラーを返しました:(403) Forbidden。この問題は、プロキシサーバーが送信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、Storage Zone Controller 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。
Storage Zone Controller 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	通常、このメッセージは、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、Storage Zone Controller から ShareFile アカウントにログインできることを確認します。Storage Zone Controller 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かれ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。	Storage Zone Controller は、Storage Zone Controller 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、Storage Zone Controller を再インストールします。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

問題	説明と解決策
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。Storage Zone Controller 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] タブの [ハートビートステータス] が赤で表示されます。	赤いアイコンは、Storage Zone Controller 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になっているかどうかを確認します。その場合は、ログを参照して詳細を確認してください。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、Storage Zone Controller 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。Storage Zone Controller 用のプロキシサーバーを指定するには、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。Storage Zone Controller 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

問題	説明と解決策
ストレージゾーンが ShareFile 管理者インターフェイスに表示されない	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ことを示している可能性があります。まず、Storage Zone Controller 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、ポートを取り外し、Controller 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てください。デフォルトでは、Windows ファイアウォール設定では、ポート 443 上の ShareFile サービスの送信トラフィックが許可されます。Storage Zone Controller には、その設定が必要です。Windows ファイアウォールが、ポート 443 で次のプロセスに対して送信トラフィックを許可す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

© 1999-2021 Citrix Systems, Inc. All rights reserved.

問題	説明と解決策
Storage Zone Controller 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、Storage Zone Controller、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のバインドを、Citrix ADC AAA にバインドします。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をバインド解除して、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、Storage Zone Controller 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 ブラウザから、コネクタの URL を入力します。次の URL が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のに成功した場合、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。または、ユーザーとしてログオンしている場合は、API 応答を取得します。 `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”,“CreationD `://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=Name,FileName,CreationDate,ProgenyEditDate...`。外部ネットワークからデ

© 1999-2021 Citrix Systems, Inc. All rights reserved.

問題	説明と解決策
Storage Zone Controller をアップグレードした後、ファイルクリーンアップサービスから ShareFile への接続の状態として、赤いアイコンが表示されます。	Storage Zone Controller 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。Controller 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。
コネクタ作成中に「パスが最大長 (1024) を超えています」と表示される	このメッセージは、Storage Zone Controller 用に構成された外部アドレスが、Storage Zone Controller サーバー 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 Storage Zone Controller を削除した後に新しい Storage Zone Controller 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 Storage Zone Controller 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可能性があります。この問題を解決するには：新しい Storage Zone Controller をアンインストールします。共有ネットワークフォルダを削除します。フォルダー c:\inetpub\wwwroot\Citrix を削除します。regedit を開き、キー **HKEY_LOCAL_MACHINE/Software/Wow6432Note/Citrix** を削除します。新しい Storage Zone Controller 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 hosts ファイルを介してストレージゾーン 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
```

© 1999-2021 Citrix Systems, Inc. All rights reserved.

ShareFile クライアントおよび **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されない場合は、接続を確認します。上記の表では、多くの接続の問題について説明します。Storage Zone Controller 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。携帯電話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可能かどうかを確認します。

コネクタにアクセスしようとしたときに「HTTP Error 401-権限がありません」と表示された場合、ユーザーが ShareFile クライアントまたは ShareFile Web アプリケーションからコネクタにアクセスできないようにするには、次のいずれかの問題で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] に表示されていない場合は、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、[共有とストレージの管理] 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、およびグループアクセスの監査に関する問題。トラブルシューティング情報については、「CTX126589」を参照してください。

SharePoint サイトへの接続時に「HTTP エラー 403 — 禁止」と表示された場合、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、Storage Zone Controller 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 Error 503 — サービスが利用できません」と表示された場合、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 用の Citrix ADC 構成を確認し、構成を修正します。

制限付きストレージゾーン

June 15, 2020

制限付きストレージゾーンは、機密データを保護するために利用されます。制限付きストレージにアクセスできるのは従業員だけです。

サードパーティのユーザー認証は、制限ゾーンではサポートされていません。

> 注:
>
> 制限付きストレージゾーンは [保守終了] です。このライフサイクルポリシーについては、「ライフサイクルマイ

© 1999-2021 Citrix Systems, Inc. All rights reserved.

> ルストーンの定義」で詳しく説明します。新しい制限付きストレージゾーンの作成はサポートされていません。制限付きストレージゾーンを利用している既存のお客様は、将来の製品マイルストーンについてさらに連絡を受けることができます。

制限されたゾーン機能

ゾーン認証：ユーザーは、ShareFile へのログオンに加えて、制限されたゾーンに保存されているドキュメントにアクセスするには、Storage Zone Controller に対して個別に認証する必要があります。ディレクトリ検索により、ShareFile にログオンしているユーザーがゾーンに対して認証しているユーザーと同じであることが保証されます。この追加の認証要件により、共有が制限されます。ドキュメントを共有できるのは、Storage Zone Controller へのアクセス権を持ち、エンタープライズ認証情報を使用して認証できるユーザーのみです。制限付きゾーンでは、ファイルを匿名で共有することはできません。ユーザーは、ファイルを表示するためのアクセス許可を付与し、共有ファイルを受信するには常にログオンする必要があります。

メタデータの暗号化：ゾーン内のファイルやフォルダに関するすべての情報は、ShareFile に送信される前にキーで暗号化されます。その結果、組織外の誰も制限区域内のフォルダ名またはファイル名を表示できません。暗号化キー、復号化されたファイル、およびメタデータへのアクセスは、Storage Zone Controller へのエンタープライズ認証を介してのみ使用できます。

Storage Zone Controller 内部アドレス：制限付きゾーンでは、Storage Zone Controller と ShareFile クラウドの間ではなく、Storage Zone Controller と ShareFile クライアント間で承認が行われます。その結果、制限付きゾーンをホストする Storage Zone Controller は、外部アドレスまたは外部 SSL 証明書を必要としません。Storage Zone Controller が内部のみのアドレスで構成されている場合、ユーザーは制限付きゾーン内のドキュメントにアクセスするために会社のネットワークまたは VPN に接続する必要があります。

メールサーバーからのメール通知：ユーザーが制限付きゾーン内の共有ファイルとフォルダに関するメール通知を受信すると、そのメールは ShareFile サーバーではなく内部メールサーバーから送信されます。

標準ゾーンと制限付きゾーンの違い

プロパティ	標準ゾーン	制限付きゾーン
Storage zone servers can be managed by…	Citrix またはあなた	あなた
User authentication is handled by…	`ShareFile.com` または `ShareFile.eu`	`ShareFile.com`または`ShareFile.eu`とオンプレミスの Storage Zone Controller の組み合わせ
Files can be shared with…	従業員およびサードパーティのユーザー（つまり、メールアドレスを持つすべてのユーザー）	従業員またはドメインアカウントを持つ他のユーザー

© 1999-2021 Citrix Systems, Inc. All rights reserved.

プロパティ	標準ゾーン	制限付きゾーン
File and folder metadata stored in the ShareFile control plane is…	クリアテキストで格納され、一部の Citrix 従業員が閲覧できます	秘密鍵で暗号化され、Citrix では利用できません
Email notifications are sent using…	ShareFile メールサーバーまたは SMTP サーバー	SMTP サーバー
An external address for the zone is…	必須	必須ではありません

標準ストレージゾーンと制限付きストレージゾーン

ストレージゾーンは、標準または制限付きとして指定できます。

- 標準ストレージゾーンは機密性の低いデータを対象としており、従業員は非従業員とデータを共有できます。
- 制限付きストレージゾーンは機密データを保護する: 従業員のみがゾーンに格納されているデータにアクセスできます。

次の表は、標準ゾーンと制限ゾーンの違いをまとめたものです。

プロパティ	標準ゾーン	制限付きゾーン
Storage zone servers can be managed by…	Citrix またはあなた	あなた
User authentication is handled by…	ShareFile.com または ShareFile.eu	ShareFile.comまたはShareFile.euとオンプレミスの Storage Zone Controller の組み合わせ
Files can be shared with…	従業員およびサードパーティのユーザー（つまり、メールアドレスを持つすべてのユーザー）	従業員またはドメインアカウントを持つ他のユーザー
File and folder metadata stored in the ShareFile control plane is…	クリアテキストで格納され、一部の Citrix 従業員が閲覧できます	秘密鍵で暗号化され、Citrix では利用できません
Email notifications are sent using…	ShareFile メールサーバーまたは SMTP サーバー	SMTP サーバー
An external address for the zone is…	必須	必須ではありません

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Citrix 管理ゾーンでは、ShareFile クラウドは、Storage Zone Controller によって処理される従業員認証を除くすべての操作を実行します。

標準ゾーンでは、Web サイトのメンテナンスと更新、クライアントとアプリケーションの更新、ファイルのメタデータ、アップロードとダウンロードの承認、メール通知 (SMTP)、サードパーティのユーザー認証、フォルダのアクセス許可がクラウドで処理されます。従業員の認証、ファイルストレージと暗号化は、Controller によって処理されます。

制限ゾーンでは、Web サイトのメンテナンスと更新、クライアントとアプリケーションの更新、フォルダのアクセス許可がクラウドで処理されます。従業員認証、ファイルストレージと暗号化、ファイルメタデータ、アップロードとダウンロードの承認、メール通知（SMTP）は Controller によって処理されます。サードパーティのユーザー認証は、制限ゾーンではサポートされていません。

ShareFile では、アカウント内の標準ゾーンと制限ゾーンの組み合わせがサポートされています。複数の制限ゾーンを作成し、それぞれに固有の認証要件を設定できます。たとえば、ドメイン A のユーザーがドメイン B のユーザーとファイルを共有することを許可しない場合は、ドメインごとに個別の制限ゾーンをインストールします。

このセクションの残りの部分では、ShareFile 管理ゾーン、標準ゾーン、および制限されたゾーンのワークフローについて説明します。

制限付きストレージゾーンの概念実証の導入

制限ゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからの受信接続を受け入れる必要はありません。内部アドレスで設定できます。次の図は、ユーザーデバイス、ShareFile クラウド、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あります。Storage Zone Controller は、アクセスを制御するためにファイアウォール内に存在します。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 で 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 SSL 証明書をインストールする必要があります。パブリック証明書も使用できます。

制限ゾーンの場合、Storage Zone Controller は、ShareFile からではなく、ローカル SMTP サーバーからメール通知を送信します。

制限付きゾーンの高可用性展開

制限ゾーン用に構成された Storage Zone Controller は、ShareFile クラウドからの受信接続を受け入れる必要はありません。各コントローラーを内部アドレスで設定できます。次の図は、制限付きゾーンの高可用性展開を示しています。

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あります。Storage Zone Controller は、アクセスを制御するためにファイアウォール内に存在します。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 で 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 SSL 証明書をインストールする必要があります。パブリック証明書も使用できます。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

制限ゾーンの場合、Storage Zone Controller は、ShareFile からではなく、ローカル SMTP サーバーからメール通知を送信します。

制限付きゾーン

次の表は、ユーザーが ShareFile にログオンし、制限された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ています。すべての接続で HTTPS が使用されます。

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. 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/フォルダの列挙とダウンロード要求	クライアント	szc.company.com
4. ファイルのダウンロード許可と暗号化されたメタデータの取得	szc.company.com	company.sharefile.com
5. ファイルのダウンロード	クライアント	szc.company.com

制限付きストレージゾーンの展開

次の図は、制限付きゾーンの高可用性展開を示しています。

制限ゾーンの場合、Storage Zone Controller は、ShareFile からではなく、ローカル SMTP サーバーからメール通知を送信します。

制限付き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、制限されたゾーンにドキュメントをアップロードする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、信頼できるネットワーク上の ADFS サーバーと通信する ADFS プロキシサーバーによって処理されます。

手順	接続元	接続先	プロトコル
1. ShareFile クライアントまたはブラウザが接続を開く	クライアント	company.sharefile.com または company.sharefile.eu	HTTPS

© 1999-2021 Citrix Systems, Inc. All rights reserved.

手順	接続元	接続先	プロトコル
2. (オプション)「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	HTTPS
3. ShareFile がユーザーを Storage Zone Controller にリダイレクトする	クライアント	company.sharefile.com または company.sharefile.eu	HTTPS
4. クライアントが Windows 認証情報を Storage Zone Controller に送信する	クライアント	Storage Zone Controller	HTTPS
5. Storage Zone Controller が認証情報を検証し、クライアントアクセスを許可する	Storage Zone Controller	ドメインコントローラー	kerberos
6. クライアントが Storage Zone Controller にファイルをアップロードする	クライアント	Storage Zone Controller	HTTPS
7. 制限ゾーンのストレージリポジトリにファイルが書き込まれる	Storage Zone Controller	ローカルストレージ	CIFS
8. Storage Zone Controller がファイルメタデータを暗号化し、ShareFile に送信する	Storage Zone Controller	company.sharefile.com または company.sharefile.eu	HTTPS

制限付きストレージゾーンの場合:

- 内部ホスト名または外部ホスト名を使用します。
- ShareFile との通信で SSL を有効にします。

  内部ホスト名を使用する場合は、プライベート証明書を使用できます。証明書は、ユーザーデバイスによって信頼されている必要があります。

  外部ホスト名を使用する場合、Storage Zone Controller の SSL 証明書は、ユーザーデバイスおよび ShareFile Web サーバーによって信頼されている必要があります。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

- Storage Zone Controller から次のサービスバス URI のいずれかに送信 HTTP アクセスを提供します。
  - ShareFile.com アカウント: `sf-zk-email-use.servicebus.windows.net`
  - ShareFile.eu アカウント: `sf-zk-email-euw.servicebus.windows.net`

  ネットワークチームとネットワークの依存関係を整理してください。

制限付きストレージゾーンのクライアント要件

ShareFile Web アプリケーションは、次の Web ブラウザから制限されたストレージゾーンをサポートします。

- Internet Explorer 11

  ShareFile Web アプリケーションから制限ゾーン内のフォルダおよびコネクタへのアクセスを有効にするには:

  1. Internet Explorer を開き、[インターネットオプション] に移動し、[セキュリティ] タブをクリックし、[信頼済みサイト] をクリックします。
  2. **[**サイト**]** をクリックし、サブドメインと外部 Storage Zone Controller アドレスを追加します。
  3. [閉じる] をクリックし、[レベルのカスタマイズ] をクリックします。
  4. 各ドメインの **[**その他**]** > **[**データソースにアクセス**]** では、[有効化] を選択します。
  5. **[**ユーザー認証**]** > **[**ログオン**]** では、ユーザー名とパスワードを **[**要求する**]** を選択します。

- Chrome
- Firefox
- Safari
- Secure Web

制限付きストレージゾーンをサポートするには、ShareFile クライアントを次のバージョン以降にアップグレードする必要があります。

- ShareFile Sync for Windows 3.1
- ShareFile Outlook プラグイン 3.2.2
- ShareFile for iOS 3.3
- ShareFile for Android 3.4
- ShareFile for Windows Phone 2.3.10

これらの ShareFile クライアントとツールは、この資料の公開日現在、制限付きストレージゾーンでの使用はサポートされていません。

注: ShareFile クライアント機能の最新情報については、
ShareFile サポート サイトを参照するか、ShareFile サポート担当者にお問い合わせください。

- ShareFile Desktop Sync for Windows 3.1 および ShareFile Outlook Plug-in のオフドメイン使用

© 1999-2021 Citrix Systems, Inc. All rights reserved.

クライアントは、Storage Zone Controller サーバーと同じ Active Directory フォレストにあるドメインに参加している Windows デスクトップ上に存在する必要があります。クライアントは、NTLM または Kerberos を使用して、制限付きゾーンへのサイレント認証を行うことができます。

- On-Demand Sync for Windows
- Sync for Mac
- ShareFile Enterprise Sync Manager
- Secure Mail for iOS
- ShareFile Desktop ウィジェット
- ShareFile for BlackBerry
- ShareFile モバイルサイト

以下の代替アカウントアクセス方法は、制限付きストレージゾーンでの使用にはサポートされていません。

- FTP
- PowerShell
- ShareFile コマンドラインインターフェイス（SFCLI）
- HTTPS API (V1)
- WebDav
- SMTP

> 重要
>
> ShareFile、**DFS** レプリケーションを公式に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障害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間帯に個別のバックアップソリューションを使用します。

制限付きストレージゾーンのアップグレード

StorageZones Controller を最新バージョンにアップグレードすると、そのコントローラは引き続き標準ゾーンを使用します。標準ゾーンを制限ゾーンにアップグレードすることはできません。

標準ゾーンを制限ゾーンに置き換えるには、新しい Storage Zone Controller をインストールし、制限ゾーンを構成する必要があります。

制限ゾーンまたはコネクタへの Web アクセスをサポートするには、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。この構成により、信頼された ShareFile ドメインにログオンしたときにのみ、ShareFile クライアントが資格情報を送信することが保証されます。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) も追加します。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

制限ゾーンの追加情報

制限付きストレージゾーンのサポートは、ShareFile サービスのすべての側面に影響します。メタデータの暗号化とゾーン認証をサポートするために必要なプロトコルの変更により、一部の **ShareFile** クライアントおよび機能は制限付きストレージゾーン内のドキュメントを操作する際にサポートされません。

コンテンツ

- クライアントとツール
- Web ブラウザー
- 機能
- Sync for Windows
- モバイルアプリ
- Outlook プラグイン

クライアントとツール

Sync for Windows	3.1 以降に
Microsoft Outlook のプラグイン	3.2.2 以降
On-Demand Sync for Windows	未サポート
Drive Mapper	3.01.171.0 以降
ShareFile for iOS	3.3 — MDX のみ
ShareFile for Android	3.4 およびアップ
ShareFile for Windows Phone 8	2.3.10 以降
Sync for Mac	未サポート
ShareFile Desktop	未サポート
XenMobile WorxMail for iOS	未サポート
XenMobile WorxMail for Android	サポートされている
ShareFile への出力	未サポート
モバイルサイト	未サポート
その他のアカウントアクセス方法	
PowerShell	未サポート
SFCLI	未サポート

© 1999-2021 Citrix Systems, Inc. All rights reserved.

REST API(V3)	サポートされている
HTTPS APT(V1)	未サポート
RSZ Test Coverage	未サポート
FTP	未サポート
フォルダにファイルをメールで送信する	未サポート
.Net SDK	サポートされている

Web ブラウザー

Windows	Internet Explorer 11, Firefox (最新バージョン), Chrome (最新バージョン)
macOS	Safari (最新バージョン), Firefox (最新バージョン), Chrome (最新バージョン)
iOS	Safari, Secure Web
Android	Secure Web

機能

エンドユーザーのアクション**:** ファイルの操作**:**

ファイルの参照とダウンロード	サポートされている
ファイルのアップロード (アップローダの種類)	HTML5: サポート; Flash: サポートされていません; Java: サポートされていません; 標準 HTML フォーム: サポートされていません
ごみ箱	サポートされている
一括ダウンロードおよび削除	サポートされている
ファイルボックス	表示: サポート; 削除: サポート; アップロード: サポート; ダウンロード: サポートなし; ファイルボックスから送信: サポートなし
ファイルプレビュー (サムネイル)	未サポート

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Web ブラウザでのドキュメントの表示	未サポート
ファイルの再アップロード	未サポート
ファイルごとに複数のバージョン	未サポート
検索	検索結果に含まれない制限付きゾーンアイテム
フォルダをお気に入りとしてマークする	未サポート
ファイルのコピーまたは移動	未サポート
フォルダオプションの編集: フォルダの有効期限、ファイルの保存ポリシー	サポートされている
共有フォルダのバブリング	未サポート

エンドユーザーのアクション**:** 共有とコラボレーション**:**

ファイルの送信: アップロードの要求、ShareFile を使用したメールの送信、コピー可能なリンクの送信、ユーザーのログオン要求、ダウンロード数の制限	サポートされている
共有ファイルの受信とダウンロード	サポートされている
制限付きストレージゾーンに共有フォルダーを作成する	サポートされている
フォルダへのユーザーの追加: アップロードとダウンロードの権限の制御	サポートされている
ファイルをリクエストする	サポートされている
「ShareFile ログインが必要」を有効にしてファイルをリクエストする	未サポート
メール通知	サポートされている
受信トレイ: ファイルが送信されました	サポートされている
受信トレイ: 送信済みメッセージ	表示、期限切れ、再送信、編集: サポート
アクティビティログの表示	サポートされている
署名を取得する（RightSignature 経由）	未サポート

管理アクション**:**

© 1999-2021 Citrix Systems, Inc. All rights reserved.

制限付きゾーンでのユーザーの作成	サポートされている
ユーザーを別のゾーンに移行する	未サポート
レポート: アクセス監査、使用状況レポート、メッセージングレポート、帯域幅レポート、ストレージレポート	HTML ビューア: サポート; Excel/CSV/PDF ビューア: 暗号化されたメタデータを表示
ゾーン管理	
ストレージ使用率の監視	サポートされている
帯域幅の使用状況を監視する	サポートされている
ファイルアクティビティの監視	サポートされている
ファイルの回復	未サポート
ファイルをリコンサイルする	未サポート
ゾーンの削除	サポートされている
高可用性	サポートされている

Sync for Windows

最小バージョン-3.1

ドメインに参加しているクライアントからの認証 (NTLM または Kerberos)	サポートされている
ドメイン以外のクライアントからの認証-パスワードの入力を求められたユーザー	サポートされている
制限付きゾーンで「マイファイルとフォルダ」を同期する	サポートされている
制限付きゾーンから共有フォルダーを同期する	サポートされている
アップロード、ダウンロード、同期	サポートされている
XenApp 環境および XenDesktop ktop 環境でのオンデマンド同期	未サポート
お気に入りフォルダを表示する	制限付きストレージゾーンフォルダでは使用できません。
右クリック／リンクをコピー	サポートされている

© 1999-2021 Citrix Systems, Inc. All rights reserved.

右クリック／メールファイル	サポートされている

モバイルアプリ

以下のアプリ固有の表を参照してください。

iOS-最低バージョン **3.3**

ファイルの参照とダウンロード	サポートされている
コンテンツをオフラインで表示	サポートされている
フォルダーの作成	サポートされている
ファイルの作成または編集	サポートされている
写真またはビデオをアップロードする	サポートされている
ユーザー名/パスワードによる認証	サポートされている
Worx マイクロ VPN によるシングルサインオン	サポートされている
共有: リンクをコピーする	サポートされている
共有: メールで共有	未サポート
フォルダメモを追加または編集する	未サポート
メモの作成または既存のメモの編集	未サポート
フォルダーにユーザーを追加するか、既存のフォルダーのアクセス許可を編集する	未サポート
フォルダをお気に入りとしてマーク/マーク解除	未サポート
ファイルをリクエストする	未サポート
サムネイルプレビュー	未サポート
複数項目の削除	未サポート
フォルダをオフラインで使用できるようにする	ルートレベルの「私と共有」フォルダを除いてサポート
フォルダを共有する	ルートレベルの「私と共有」フォルダを除いてサポート
制限付きストレージゾーンにコネクタを作成する	未サポート

© 1999-2021 Citrix Systems, Inc. All rights reserved.

Android-最低バージョン **3.4**

ファイルの参照とダウンロード	サポートされている
コンテンツをオフラインで表示	サポートされている
ファイルを送信する	サポートされている
フォルダーの作成	サポートされている
ファイルの作成または編集	サポートされている
ファイルのアップロード	サポートされている
ユーザー名/パスワードによる認証	サポートされている
Worx マイクロ VPN によるシングルサインオン	サポートされている
ファイルをリクエストする	未サポート
メモを作成	未サポート
アップロード後に既存のファイルを上書き	未サポート

Outlook プラグイン

ドメインに参加しているクライアントからの認証 (NTLM または Kerberos)	サポートされている
ドメイン以外のクライアントからの認証-パスワードの入力を求められたユーザー	サポートされている
ShareFile からファイルを参照して選択する	サポートされている
「受信者にログインを要求する」が有効になっている ShareFile からファイルを参照して選択	未サポート
添付 ShareFile リンクに変換する	サポートされている
「受信者にログインを要求する」を有効にして添付 ShareFile リンクに変換する	未サポート
ファイルをリクエストする	サポートされている
[受信者にログインを要求する] を有効にしたファイルを要求する	未サポート

© 1999-2021 Citrix Systems, Inc. All rights reserved.

リファレンス：**Storage Zone Controller** 構成ファイル

June 15, 2020

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。

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

Storage Zone Controller インストーラーは、これらのファイルを作成します。Storage Zone 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。

AppSettingsRelease.config

AppSettingsRelease.config ファイルは、Storage Zone Controller 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

  Storage Zone Controller 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、永続的なストレージキャッシュを管理するために、Storage Zone Controller によって使用されるコントロールを提供します。この設定ファイルは、次の場所にあります。`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

SFAntiVirus.exe.config

sfAntivirus.exe.config は、Storage Zone Controller 構成、スキャナー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ーソフトウェアに提供します。この設定ファイルは、次の場所にあります。`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

詳しくは、「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」を参照してください。

Web.config

一般に、`C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` には、通常変更すべきでは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 Storage Zone Controller 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 Storage Zone Controller 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している場合は、各セカンダリサーバーの 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、Storage Zone Controller 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。プロキシサーバーの設定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. 次のように、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>
```

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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。

後でプライマリ Storage Zone Controller の IP アドレスまたはホスト名を変更する場合は、セカンダリサーバごとに 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。

© 1999-2021 Citrix Systems, Inc. All rights reserved.

© 1999-2021 Citrix Systems, Inc. All rights reserved.

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

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).