Dell PowerStore

SMB の構成

3.x

10 月 2023 年
Rev. A05

DELL Technologies

メモ、注意、警告

メモ: 「メモ」は、製品をより上手に使用するための重要な情報であることを示します。

注意: **「注意」は、ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。**

警告: **「警告」は、物的損害、けが、または死亡の原因となる可能性があることを示しています。**

目次

前書き

改善努力の一環として、ソフトウェアおよびハードウェアのリビジョンを定期的にリリースしています。本書で説明されている機能の中には、現在お使いのソフトウェアまたはハードウェアの一部のバージョンによってサポートされていないものがあります。製品のリリース ノートには、製品の機能に関する最新情報が掲載されています。製品が正常に機能しない、またはこのマニュアルの説明どおりに動作しない場合には、サービス プロバイダーにお問い合わせください。

問い合わせ先

サポート情報、製品情報、ライセンス情報は、次の場所で入手できます。

- ［製品情報］

  製品および機能のドキュメントまたはリリース ノートについては、https://www.dell.com/powerstoredocs にある［PowerStore Documentation］ページを参照してください。

- ［のトラブルシューティング］

  製品、ソフトウェア アップデート、ライセンス、サービスの詳細については、https://www.dell.com/support にアクセスし、該当する製品サポートページを参照してください。

- ［テクニカル サポート］

  テクニカル サポートおよびサービス リクエストについては、https://www.dell.com/support にアクセスし、［Service Requests］ページを参照してください。サービス リクエストを利用するには、有効なサポート契約が結ばれている必要があります。有効なサポート契約を結ぶ方法の詳細や、アカウントに関するご質問については、セールス担当者にお問い合わせください。

1

概要

この章では、次の情報について説明します。

トピック：

SMB のサポート

PowerStore T モデルでは SMB 1 から SMB 3.1.1 までをサポートしています。SMB サポートが NAS サーバーで有効化されていると、SMB 対応のファイル システムが作成できます。SMB サポートがある NAS サーバーは、スタンドアロンと Active Directory ドメイン参加のいずれかです。ドメインに参加させた NAS サーバーは、デフォルトで OU=Computers, OU=EMC NAS サーバー組織ユニットに配置されます。

SMB ファイル システムと SMB 共有には、次の高度なプロトコル オプションがあります。

メモ: これらのオプションは、Oplock の有効を除き、デフォルトで無効になっています。

表 1. SMB の高度なプロトコル オプション

プロトコル オプション	レベル
同期書き込みの有効	ファイル システム
Oplock の有効	ファイル システム
書き込み時の通知有効	ファイル システム
アクセス時の通知有効	ファイル システム
継続的な可用性	共有
プロトコル暗号化	共有
アクセス ベース列挙	共有
分岐キャッシュの有効化	共有
オフライン可用性	共有

プランニング時の考慮事項

NAS サーバーおよびファイル システムを構成する前に、次の情報を確認してください。

ファイル ストレージのサポートは、PowerStore T モデルアプライアンスでのみ使用できます。ファイル ストレージは、PowerStore X モデルアプライアンスではサポートされていません。

NAS サーバー ネットワーク

SMB プロトコルを使用して NAS サーバーを構成する前に、次のように構成します。

1. DNS サーバーを 1 つ以上構成します。
2. NAS サーバーを AD（Active Directory）に参加させる場合は、ストレージ システムで NTP サーバーを少なくとも 1 つ構成して、日付と時刻を同期します。単一障害点防止のため、NTP サーバーを最低でもドメインにつき 2 つセット アップすることを推奨します。

   メモ: AD の作成中に NTP が構成されています。
3. Active Directory でのドメイン アカウントの作成。

NAS サーバーでは、ネットワーク VLAN および IP アドレスの作成はオプションです。NAS サーバーの VLAN を作成する予定がある場合、VLAN を PowerStore T モデル管理ストレージまたはストレージ ネットワークと共有することはできません。また、ネットワーク管理者と連携してネットワーク リソースを確保し、スイッチ上でネットワークを構成するようにしてください。詳しくは、*PowerStore T* モデル向け *PowerStore* ネットワーキング ガイドを参照してください。

拡張性

PowerStore バージョン 3.5 には、ファイル システム ボリュームと vVols に関する共有制限があります。オブジェクトの合計数は、3 つのオブジェクト タイプの上限に基づいて決まります。

プラットフォームごとのファイル システム制限を表示するには、PowerStore ドキュメント ページに掲載されている *Dell Technologies PowerStore* 簡易サポート マトリックスを参照してください。

導入環境の要件

NAS サービスは、PowerStore T モデルアプライアンスでのみ使用できます。PowerStore X モデルアプライアンスを実行中の場合、このサービスは使用できません。

PowerStore T モデルアプライアンスの初期構成時に［ユニファイド］を選択する必要があります。初期構成ウィザードの実行中に［ブロック最適化］を選択した場合、NAS サービスはインストールされませんでした。NAS サービスをインストールするには、カスタマー サポート担当者がお客様のシステムを再初期化する必要があります。システムの再初期化：

- アプライアンスの設定を工場出荷時の状態に戻します。
- システムで［初期設定ウィザード］によって実行されたすべての構成を削除します。
- 初期構成後に PowerStore で実行されるすべての構成を削除します。

その他の考慮事項

NAS サーバーを作成するには、アプライアンス上の両方のノードが動作している必要があります。アプライアンスのいずれかのノードがダウンしている場合、NAS サーバーの作成は失敗します。

NAS トラフィック用のネットワーク インターフェイスの作成

Link Aggregation Control Protocol (LACP)ボンディングを使用するか、NAS トラフィック用のフェールセーフ ネットワークを作成して、NAS ネットワークを構成できます。

NAS トラフィック用の LACP ボンドの作成

スイッチが MC-LAG で構成されている場合に、ネットワーク ボンディングを使用するには、NAS トラフィック用のリンク アグリゲーション グループ(LAG)を作成します。

このタスクについて

トップオブラック(ToR)スイッチが MC-LAG インターコネクトで構成されている場合は、リンク アグリゲーション グループ(LAG)を使用して、LACP ボンディングを介した NAS インターフェイスを構成することをお勧めします。LACP ボンディングとは、2 つ以上のネットワーク インターフェイスを 1 つのインターフェイスに結合するプロセスです。LACP ボンディングを使用すると、ネットワーク スループットと帯域幅が拡大し、パフォーマンスと冗長性が向上します。結合インターフェイスの 1 つがダウンしている場合でも、他のインターフェイスを使用して安定した接続を維持できます。

手順

1. ［ハードウェア］ > ［[アプライアンス]］ > ［ポート］を選択します。
2. ポート リストから、NAS トラフィックを提供する Link Aggregate Control Protocol (LACP)ボンドを集約して NAS トラフィックにサービスを提供するノード上の同じ速度の 2～4 個のポートを選択します。

   メモ: 構成はピア ノード全体で対称的です。

3. ［Link Aggregation］ > ［リンクを集約］を選択します。
4. オプションで、ボンドの説明を提供します。

5. ［集約］を選択します。
6. ポート リストをスクロールして、生成されたボンド名を見つけます。

   メモ: NAS サーバーを作成する場合は、このボンド名を選択する必要があります。

フェールセーフ ネットワークの作成

このタスクについて

トップオブラック(ToR)スイッチが MC-Lag インターコネクトで構成されていない場合は、フェールセーフ ネットワーク(FSN)を作成する必要があります。FSN は、スイッチ レベルの冗長性を提供することで、ネットワークへのリンク フェールオーバーを拡張します。FSN は、ポート、リンク アグリゲーション、またはこれら 2 つを任意に組み合わせで構成できます。

手順

1. ［ハードウェア］ > ［[アプライアンス]］ > ［ポート］を選択します。
2. FSN に統合リンクを使用する予定の場合は、最初にリンク アグリゲーション グループを作成します。詳細については、NAS トラフィック用の LACP ボンディングの作成を参照してください。
3. リストから、ノード A の FSN に使用するポート 2 つまたはリンク アグリゲーション 2 つ、あるいはポート 1 つとリンク アグリゲーション グループ 1 つの組み合わせを選択し、［FSN］ > ［FSN の作成］を選択します。
4. ［FSN の作成］パネルで、プライマリー（アクティブ）ネットワークとして使用するポートまたはリンク アグリゲーションを選択します。

   メモ: プライマリー ポートは、NAS サーバーの作成に使用した後は変更できません。

5. 必要に応じて、フェールセーフ ネットワークの説明を追加します。
6. ［作成］をクリックします。

   PowerStore Manager は、「BaseEnclosure-<Node>-fsn<nextLACPbondcreated>」の形式で、フェールセーフ ネットワークの名前を自動的に作成します。
   - BaseEnclosure は定数です。
   - Node は、［Node-Module-Name］リストに表示されるノードです。
   - nextLACPbondcreated には、PowerStore Manager でボンドが作成された順番を表す数値が割り振られます。最初に作成されたボンドの 0 から始まります。

   ノード A の PowerStore Manager で作成された最初の FSN は、BaseEnclosure-NodeA-FSN0 という名前になります。

   反対側のノードで同じ FSN が構成されています。たとえば、ノード A に FSN を構成した場合は、同じ FSN がノード B で構成されます。
7. フェールセーフ ネットワークを使用して NAS サーバーを作成します。

   フェールセーフ ネットワークは、PowerStore Manager で NAS サーバーを作成する際に NAS サーバーに適用されます。SMB ファイル システム用 NAS サーバーの作成を参照してください。

SMB 共有の作成

SMB 共有を PowerStore で作成するには、次の手順を実行します。

1. SMB プロトコルを使用した NAS サーバーの作成
2. SMB 共有用ファイル システムの追加

ドキュメントのリソース

詳細については、以下を参照してください。

表 2. ドキュメントのリソース

ドキュメント	説明	場所
PowerStore T モデル向け *PowerStore* ネットワーキング ガイド	ネットワーク プランニングと構成情報を提供します。	https://www.dell.com/powerstoredocs

表 2. ドキュメントのリソース （続き）

ドキュメント	説明	場所
PowerStore NFS 構成ガイド	PowerStore Manager で NFS エクスポートを構成するために必要な情報を提供します。	
PowerStore ファイル機能に関するホワイト ペーパー	Dell PowerStore ファイル アーキテクチャでサポートされている特長、機能、プロトコルについて説明します。	
PowerStore オンライン ヘルプ	PowerStore Manager で開かれているページについて、コンテキストに応じた情報を提供します。	PowerStore Manager に組み込み

2

NAS サーバーの作成

この章では、次の情報について説明します。

トピック：

NAS サーバーの構成の概要

ファイル ストレージを PowerStore T モデルアプライアンスでプロビジョニングするには、NAS サーバーがシステムで実行されている必要があります。NAS サーバーは、SMB プロトコル、NFS プロトコル、またはその両方を使用して、ネットワーク ホストとデータを共有するファイル サーバーです。また、このサーバは、関連するファイル システムに対する読み取り/書き込み処理を、カタログ化、整理、最適化します。

このドキュメントでは、SMB プロトコルを使用して NAS サーバーを構成する方法について説明します。そこでは、SMB 共有のあるファイル システムが作成できます。

SMB ファイル システム用 NAS サーバーの作成

ファイル システムを作成する前に、NAS サーバーを作成します。

前提条件

次の情報を取得します。

- NAS サーバーのネットワーク ポート、IP アドレス、サブネット マスク/プレフィックス長、ゲートウェイ情報。
  メモ: Ip アドレスとサブネット マスク/プレフィックス長は必須です。
- スイッチ ポートで VLAN タグ機能がサポートされる場合は、VLAN 識別子。
  メモ: 管理ネットワークおよびストレージ ネットワークに使用されている VLAN を再使用することはできません。
- スタンドアロン NAS サーバーを構成している場合は、ワークグループおよび NetBIOS 名を取得します。その後に、SMB サーバー アカウントのスタンドアロン ローカル管理者に使用するものを定義します。
- NAS サーバーを AD（Active Directory）に参加させる場合は、ストレージ システムで NTP を構成し t おきます。SMB システム名（SMB 共有へのアクセスに使用）、Windows ドメイン名、ドメイン管理者または AD に参加するための十分なドメイン アクセス レベルを持つユーザーのユーザー名とパスワードを取得します。

手順

1. ［Storage］ > ［NAS Servers］を選択します。
2. ［Create］を選択します。
3. ［Create NAS Server］ウィザードで作業を続行します。

ウィザード画面	説明
詳細	• NAS サーバー名 • NAS サーバーの説明 • ネットワーク インターフェイス：リンク アグリゲーション グループまたはフェールセーフ ネットワークを選択します（NAS トラフィック用のネットワーク インターフェイスの作成を参照）。 **メモ:** フェールセーフ ネットワーク(FSN)を選択した場合、NAS サーバーが FSN を使用して構成された後で、プライマリー ネットワークを変更することはできません。 • ネットワーク情報

ウィザード画面	説明
Sharing Protocol	[Select Sharing Protocol] [SMB] を選択します。 **メモ:** SMB と NFS プロトコルの両方を選択すると、NAS サーバーで自動的に、マルチプロトコルがサポートされるようになります。マルチプロトコル構成については、このドキュメントでは説明しません。 [Windows Server 設定] [Standalone] を選択してスタンドアロンの SMB サーバーを作成するか、[Join to the Active Directory Domain] を選択してドメイン メンバーの SMB サーバーを作成します。 NAS サーバーを AD に参加させる場合は、必要に応じて [Advanced] を選択し、デフォルトの NetBIOS 名と組織単位を変更します。 [DNS] [Join to the Active Directory Domain] を選択した場合、DNS サーバーの追加は必須です。 必要に応じて、DNS サーバーをスタンドアロン SMB サーバーとして使用する場合は、DNS を有効化します。 [ユーザー マッピング] Active Directory ドメインへの参加を選択した場合は、[User Mapping] ページが表示されます。 Active Directory ドメインへの参加をサポートするために、[Enable automatic mapping for unmapped Windows accounts/users] をデフォルトのままにしておきます。Active Directory ドメインに参加する場合は、自動マッピングが必要です。
保護ポリシー	リストから保護ポリシーを選択します。
概要	コンテンツを確認したら [Previous] を選択して戻り、必要に応じて修正を加えます。

4. [Create NAS Server] を選択します。
   [Status] ウィンドウが開きます。サーバーが追加されると [NAS Servers] ページにリダイレクトされます。

次の手順

NAS サーバーを SMB 用に作成したら、サーバー設定の構成、またはファイル システムの作成を続行できます。

NAS サーバーをクリックして設定を続行するか、NAS サーバー設定を変更します。

NAS サーバー設定の変更

NAS サーバーを作成したら、サーバーに構成変更できます。

このタスクについて

メモ: リモート システム接続がある場合、NAS サーバー構成の変更がリモート NAS サーバーに反映されるまでに最大 15 分かかる場合があります。

手順

1. [Storage] > [NAS Servers] > [[nas server]] を選択します。
2. [Network] ページで、必要に応じて、ネットワーク インターフェイス、または外部ネットワークへのルートを設定します（「NAS サーバー ネットワークの構成」を参照）。
3. [Naming Services] ページで、必要に応じて NAS サーバー DNS を追加、変更、または削除します。

   メモ: SMB ファイル共有をサポートし、AD（Active Directory）に参加している NAS サーバーは、DNS を無効化できません。

4. [共有プロトコル] ページで、次の操作を実行します。
   - [SMB サーバー] カードを選択し、Windows 共有のサポートを有効化または無効化するか、SMB サーバーが使用するルックアップのタイプを変更します。

     メモ: [Windows Server Type] を [Standalone] から [Join to the Active Directory Domain] に変更するには、[User Mapping] タブに移動して、[Enable automatic mapping for unmapped Windows accounts/users] を選択する必要があります。
   - [FTP] カードを選択して、FTP または SFTP の有効化または無効化、FTP プロパティまたは SFTP プロパティの変更、ユーザー認証の構成、ユーザー ホーム ディレクトリーの構成、認証メッセージの設定を行います。

詳細については、「FTP 共有プロトコルの構成」を参照してください。

- ［User Mapping ］を選択して、サーバーがマッピングされていない Windows アカウント/ユーザーへの自動マッピング、またはマッピングされていない Windows アカウント ユーザーのデフォルト アカウントを使用できるようにします。

5. ［Protection & Events］ページで、NDMP を有効化または無効化します。
   詳細については、「NDMP の保護およびイベントの有効化」を参照してください。
6. ［セキュリティ］タブで、次の操作を実行します。
   - ［Kerberos］を選択して、Kerberos 認証用に AD（Active Directory）レルムを追加するか、カスタム Kerberos レルムを構成します。
   - ［Antivirus］を選択し、ウイルス対策サービスを有効化または無効化して、ウイルス対策構成ファイルを取得またはアップロードします。

   詳細については、「NAS サーバー セキュリティの構成」を参照してください。

3

NAS サーバーの追加機能

この章では、次の情報について説明します。

トピック：

FTP または SFTP 共有プロトコルの構成

NAS サーバーが作成されていれば、FTP または SFTP（FTP over SSH）が構成できます。

前提条件

パッシブ モードの FTP はサポートされていません。

このタスクについて

FTP アクセスは、SMB と同じ方法で認証できます。認証が完了すると、セキュリティおよび権限に関して、アクセスは SMB と同じになります。形式が `domain@user` または `domain\user` の場合は、SMB 認証が使用されます。SMB 認証では、Windows ドメイン コントローラーを使用します。

手順

1. ［Storage］ > ［NAS Servers］ > ［[nas server]］ > ［Sharing Protocols］ > ［FTP］タブを選択します。
2. ［FTP］で、無効になっている場合は、ボタンをスライドさせて［有効］にします。
3. オプションとして、SSH FTP も有効にします。［SFTP］で、無効になっている場合は、ボタンをスライドさせて［有効］にします。
4. ファイルへのアクセス権が付与される、認定ユーザーのタイプを選択します。
5. 必要に応じて、［Home Directory and Audit］オプションを表示します。
   - ［Home directory restrictions］を選択またはクリアします。無効化する場合は、［Default home directory］を入力します。
   - ［Enable FTP/SFTP Auditing］を選択または選択解除します。チェックボックスをオンにした場合は、監査ファイルの保存先となるディレクトリーの場所と、監査ファイルで許可される最大サイズを入力します。
6. 必要に応じて、［Show Messages］で、デフォルトのようこそメッセージとその日のメッセージを入力します。
7. 必要に応じて、［Access Control List］を表示し、FTP アクセスを許可または拒否するユーザー、グループ、ホストのリストを追加します。
8. ［Apply］を選択します。

NAS サーバー ネットワークの構成

NAS サーバー ネットワークは構成や変更ができます。

NAS サーバー ネットワークの場合は、次について構成します。

- ファイル インターフェイス
- ホストなどの外部サービスへのルート

NAS サーバーのファイル　インターフェイスの構成

NAS サーバーは、PowerStore に追加してあれば、サーバーのファイル インターフェイスを構成できます。

このタスクについて

ファイル インターフェイスをさらに追加したり、優先的に使用するインターフェイスとして定義したりすることができます。また、本番とバックアップにどのインターフェイスを使用するか、IPv4 と IPv6 のどちらを使用するかを定義することもできます。

手順

1. ［Storage］ > ［NAS Servers］ > ［[nas server]］を選択します。
2. ［ネットワーク］ページで［追加］をクリックして、別のファイル インターフェイスを NAS サーバーに追加します。
3. ファイル インターフェイスのプロパティを入力します。

   メモ: 管理ネットワークおよびストレージ ネットワークに使用されている VLAN を再使用することはできません。

4. リストからファイル インターフェイスを選択すると、ファイル インターフェイスで次の操作を実行できます。次をクリックします。

オプション	説明
変更	ファイル インターフェイス プロパティのプロパティを変更します。
削除	NAS サーバーからファイル インターフェイスを削除します。
ping	NAS サーバーから外部 IP アドレスへの接続をテストします。
優先インターフェイス	本番インターフェイスとバックアップ インターフェイスが複数定義されている場合に、PowerStore のデフォルトで使用するインターフェイスを定義します。

外部接続用ファイル インターフェイスのルートの構成

ファイル システムで外部接続に使用されるルートが構成できます。

前提条件

［File Interface］カードで［Ping］オプションを使用すれば、ファイル インターフェイスが外部リソースにアクセスできるかどうかが判断できます。

このタスクについて

通常、NAS サーバ インターフェイスは、NAS サーバー インターフェイスからのリクエストを外部サービスにルーティングするために使用されるデフォルト ゲートウェイで構成されます。

次の手順を実行します。

- 外部サービスに対し、より細分性の高いルートを構成する必要がある場合。
- 特定のゲートウェイを通じて特定のインターフェイスからサーバーにアクセスするためのルートを追加します。

手順

1. ［ストレージ］ > ［NAS サーバー］ > ［[NAS サーバー]］ > ［ネットワーク］ > ［外部サービスへのルート］を選択します。
2. ［Add］をクリックして、［Add Route］ウィザードでルート情報を入力します。

NDMP バックアップの有効化

NAS サーバーの標準バックアップは NDMP を使用して構成できます。NDMP（Network Data Management Protocol）は、ネットワーク上でファイル サーバをバックアップするための基準を示しています。NDMP が有効化されると、Dell Networker などのサード パーティー製データ管理アプリケーション(DMA)で NAS サーバーの IP アドレスを使用して PowerStore NDMP を検出できます。

このタスクについて

NDMP の有効化は、NAS サーバーが作成されてから実行されます。

PowerStore では、次がサポートされています。

- 3 方向 NDMP - データは、ローカル エリア ネットワーク LAN(LAN)またはワイド エリア ネットワーク(WAN)を介して、DMA 経由で転送されます。
- フル バックアップと増分バックアップ

手順

1. ［ストレージ］ > ［NAS サーバー］ > ［[NAS サーバー]］ > ［保護］を選択します。
2. ［NDMP Backup］が［Disabled］になっている場合は、ボタンをスライドさせて［Enabled］に変更します。
3. ［New Password］にパスワードを入力します。
   ユーザー名は常に `ndmp` です。
4. ［パスワードの確認入力］に新しいパスワードと同じパスワードを再入力します。
5. ［Apply］をクリックします。

次の手順

NDMP ページを終了し、NDMP ページに戻って NDMP が有効化されていることを確認します。

NAS サーバー セキュリティの構成

NAS サーバーのセキュリティは、［Kerberos］または［ウイルス対策］で構成できます。

NAS サーバー セキュリティの構成には、次のオプションがあります。

- Kerberos
- アンチウイルス

NAS サーバー用の Kerberos セキュリティの構成

NAS サーバーは Kerberos セキュリティで構成できます。

このタスクについて

Kerberos を構成する前に、SMB サーバーを AD ドメインに追加するようにしてください。

SMB 専用の NAS サーバーを構成している場合、キータブ ファイルは必要ありません。キータブ ファイルが要求されるのは Secure NFS 構成のみです。

手順

1. ［Storage］ > ［NAS Servers］ > ［[nas server]］ > ［Security］ > ［Kerberos］を選択します。
2. 無効になっている場合は、ボタンをスライドさせて［有効］に変更します。
3. ［Realm］の名前を入力します。
4. Kerberos IP アドレスを入力し、［追加］をクリックします。
5. Kerberos に使用する TCP ポートを入力します。デフォルトのポートは 88 です。
6. ［Apply］をクリックします。

Common Anti-Virus Agent (CAVA)について

CAVA（Common AntiVirus Agent）は、NAS サーバーを使用しているクライアントにウイルス対策ソリューションを提供します。Microsoft Windows Server 環境で業界標準の SMB プロトコルを使用します。CAVA は、サード パーティーのウイルス対策ソフトを使用して、ストレージ システムのファイルに感染する前に既知のウイルスを識別して排除します。

ストレージ システムはそのアーキテクチャによってウイルスの侵入を阻止するため、ウイルス対策ソフトウェアは重要です。NAS サーバーは組み込みオペレーティング システムを使用して、データ アクセスをリアルタイムに実行します。サード パーティーがこのオペレーティング システム上でウイルスを含むプログラムを実行することはできません。オペレーティング システムのソフトウェアはウイルスを阻止しますが、ストレージ システムにアクセスする Windows クライアントにはウイルスからの保護が必要です。クライアントをウイルスから保護することによって、ウイルスに感染したファイルをクライアントがサーバーに格納する確率が低くなり、感染ファイルがクライアントで開かれた場合も、クライアントが保護されます。このウイルス対策ソリューションは、オペレーティング システムのソフトウェア、CAVA エージェント、サード パーティー製ウイルス対策エンジンの組み合わせで構成されます。CAVA ソフトウェアおよびサード パーティー製ウイルス対策エンジンは、ドメイン内の Windows Server 上にインストールする必要があります。

PowerStore がサポートする CEE CAVA のバージョンについては、*PowerStore* リリース ノートを参照してください。CEE（Common Event Enabler）の一部である CAVA の詳細については、https://www.dell.com/support の「*Windows* プラットフォームでの *Common Event Enabler* の使用」を参照してください。

Common Anti-Virus Agent (CAVA)の有効化

ウイルス対策による保護を SMB 共有に追加する場合は、CAVA を有効化し、CAVA 構成ファイルをアップロードします。

前提条件

ウイルス対策スキャンを有効にするには、Active Directory にユーザーを作成し、CAVA サーバーでスキャンを実行する権限を付与する必要があります。

手順

1. PowerStore Manager から、［ストレージ］ > ［NAS サーバー］ > ［[NAS サーバー]］ > ［セキュリティとイベント］ > ［ウイルス対策］タブの順に移動します。
2. 無効になっている場合は、ボタンをスライドさせて［有効］に変更します。
3. 最新の CAVA 構成ファイルがない場合は、次の手順を実行します。
   a. ［現在の構成を取得］をクリックします。
   b. CAVA 構成ファイル テンプレートを実行します。
   c. 更新された CAVA 構成ファイルをアップロードします。
4. ウイルス対策スキャンを有効にするには、［有効］と［適用］をクリックします。

設定可能なウイルス対策パラメーター

次の表は、`viruschecker.conf` CAVA 構成ファイルで構成できるパラメーターの詳細を示しています。構成ファイルを作成し、PowerStore にアップロードできます。

表 3. ウイルス対策パラメーター

パラメーター	説明	必須	例
`addr=`	CAVA サーバーの IP アドレスを設定します。	Yes	`addr=10.205.20.130`
`masks=`	スキャン対象のファイルの拡張子を構成します。	Yes	`masks=*.exe:*.docx:*.com`
`excl=`	スキャン時に除外するファイル拡張子を一覧表示します。	No	`excl=pagefile.sys`
`maxsize=<n>`	整数。チェック対象のファイルの最大サイズを設定します。このサイズを超えるファイルはチェックされません。	No	`maxsize=4294967290`
`surveyTime=<n>`	すべての AV サーバーをスキャンしてオンラインかオフラインかを確認する間隔（秒）を設定します。応答する AV サーバーがない場合は、構成された shutdown パラメーター（次の行を参照）を使用してシャットダウン処理が開始されます。	No	`surveyTime=600`
`shutdown=`	利用可能なサーバがない場合に行うシャットダウン アクションを指定します。デフォルト値は `Allow Access` である。	No	`Allow Access`、`Stop_SMB_Access`、`Disable_Virus_Checker`
`highWaterMark=<n>`	進行中のリクエストの数が `highWaterMark` を超えた場合にシステムにアラートを送信します。	No	`highWaterMark=200`
`lowWaterMark=<n>`	処理中のリクエストの数が `lowWaterMark` を下回った場合にシステムにアラートを送信します。	No	`lowWaterMark=50`
`msrcpuser=`	シンプル ユーザー アカウント、または CEE マシンで CAVA サービスを実行しているドメインの一部であるユーザー アカウントのいずれかに割り当てられる名前を指定します。	No	ユーザー アカウント `msrpcuser=user1` ドメイン/ユーザー アカウント：

表 3. ウイルス対策パラメーター （続き）

パラメーター	説明	必須	例
			msrpcuser=CEE1/user1
httpport=	システムが使用する CEE マシン上の HTTP ポート番号を指定します。	No	httpport=12228
RPCRetryTimeout	RPC リトライのタイムアウト（ミリ秒）を設定します。	No	RPCRetryTimeout=4000 milliseconds
RPCRequestTimeout	RPC リクエストのタイムアウト（ミリ秒）を設定します。RPC が CAVA サーバーに送信され、サーバーが RPCRetryTimeout を過ぎた後に応答した場合、 NAS サーバーは RPCRequestTimeout に達するまでリトライし、その後、次の使用可能な CAVA サーバーに移動します。	No	RPCRequestTimeout=20000 milliseconds
reference time	最初の読み取りでスキャンを有効にします。ファイルの前回のアクセス時刻が、reference time より前の場合は、アクセス時に、クライアントにアクセス権が付与される前にファイルがウイルス チェッカーに送信されます。	No	reference_time=2022-10-27T18:30:00

4

ファイル システムと SMB 共有の作成

この章では、次の情報について説明します。

トピック：

ファイル システムの作成

SMB 共有を作成する前に、NAS サーバーにファイル システムを作成する必要があります。

前提条件

SMB プロトコルをサポートするよう構成されている NAS サーバーが存在するようにします（「NAS サーバーの構成」を参照）。

手順

1. ［Storage］ > ［File Systems］を選択し、［Create］をクリックします。
2. ［Create File System］ウィザードで作業を続行します。

オプション	説明
タイプの選択	［一般］ファイル システム タイプを選択します。
NAS サーバーの選択	SMB に対して有効な NAS サーバーを選択します。
Advanced SMB Settings	必要に応じて次から選択します。 ● ［同期書き込みの有効 ］ ● ［Oplock の有効］ ● ［書き込み時の通知有効 ］ ● ［アクセス時の通知有効 ］ ● ［SMB Events Publishing の有効化］ 詳細については、「SMB 共有のファイル システムの詳細設定」を参照してください。
ファイル システムの詳細	ファイル システム名とファイル システムのサイズを指定します。 ファイルシステムのサイズは 3 GB～256 TB です。 **メモ:** サイズに関係なく、すべてのシン ファイル システムではメタデータの作成時に 1.5GB が予約されます。たとえば、100GB のシン ファイル システムを作成するとすぐに、1.5GB が使用されたことが PowerStore T モデルに表示されます。ファイル システムがホストにマウントされると、有効容量として 98.5GB が表示されます。 これは、使用可能なファイル システム容量からメタデータのスペースが予約されているためです。
ファイルレベル リテンション設定[ふぁいるれべるりてんしょんせってい]	必要に応じて、ファイル保存タイプを選択します。 ● エンタープライズ(FLR-E)：CIFS および FTP を介してユーザーが行う変更からコンテンツを保護します。管理者は、保護されたファイルを含む FLR-E ファイル システムを削除できます。 ● コンプライアンス(FLR-C)：ユーザーと管理者が行った変更からコンテンツを保護し、SEC 規則 17a-4(f)の要件に準拠します。FLR-C ファイル システムは、保護されたファイルが含まれていない場合にのみ削除できます。 **メモ:** FLR 状態とファイル保存タイプはファイル システムの作成時に設定され、変更はできません。 保存期間を設定します。 ● Minimum：ファイルをロックできる最短の期間を指定します（デフォルト値は 1 日）。

オプション	説明
	• Default：ファイルがロックされており、保存期間が指定されていない場合に使用されます。 • Maximum：ファイルをロックできる最長の期間を指定します。
SMB 共有	必要に応じて、初期 SMB 共有を構成します。初期ファイル システム構成の後であれば、ファイル システムに共有を追加できます。 SMB 共有オプションの詳細については、「SMB 共有の作成」を参照してください。
保護ポリシー	必要に応じて、ファイル システムの保護ポリシーを指定します。PowerStore は、ファイル ストレージ保護のスナップショットとレプリケーションの両方をサポートしています。
概要	サマリーを確認します。戻って必要なアップデートを行います。

3. ［Create File System］をクリックします。
ファイル システムが［File System］リストに表示されます。SMB 共有を作成した場合は［SMB Share］リストに表示されます。

SMB のファイル システムの詳細設定

ファイル システムの作成時、SMB 対応のファイル システムに高度な設定を追加することができます。

表 4. SMB のファイル システムの詳細設定

設定	説明
同期書き込みの有効	Windows（SMB）またはマルチプロトコル ファイル システムに対して同期書き込みオプションを有効にすると、SMB プロトコルによる書き込み処理の実行方法にかかわらず、ストレージ システムはストレージ操作に対して即時同期書き込みを実行します。同期書き込み処理を有効にすると、データベース ファイル（MySQL など）をストレージ システムの SMB 共有に格納してアクセスできます。このオプションでは、共有への書き込みが同期的に実行されることが保証され、停電などのさまざまな障害シナリオでデータロスやファイル破損の可能性が減少します。 このオプションはデフォルトで無効になっています。 **メモ:** 同期書き込みオプションは、パフォーマンスに重大な影響を及ぼすことがあります。Windows ファイル システムを使用してデータベース アプリケーション向けのストレージを提供する場合以外は、推奨されません。
Oplock の有効	（デフォルトで有効）便宜的ファイル ロック機能（oplocks、別名レベル 1 opslock）を有効化すると、SMB クライアントは、ファイル データをサーバーに送信する前にローカルでバッファリングすることができます。これにより、SMB クライアントでは、ファイルに対してローカルな操作を行い、ストレージ システムに対するすべての操作をネットワーク経由で通知するのではなく、変更内容を定期的にストレージ システムに通知できます。この機能は、Windows（SMB）およびマルチプロトコル ファイル システムに対してデフォルトで有効になっています。アプリケーションが重要なデータを処理しているか、このモードまたは操作が現実的でなくなるような特殊な要件がない限り、便宜的ロックは有効なままにしておくことをお勧めします。 サポートされている便宜的ロックの種類は次のとおりです。 • レベル 2：複数のクライアントがファイルにアクセスしているが、どのクライアントもまだそのファイルを修正していないことを、クライアントに通知します。クライアントは、ローカルのキャッシュ内情報または先読みした情報を使用して、データ読み取り処理とファイル属性取得処理を行います。その他のファイル アクセス要求は、サーバーに送信する必要があります。 • 排他：そのファイルを開いている唯一のクライアントであることを、クライアントに通知します。クライアントは、ファイルを閉じるまでの間、キャッシュ内情報または先読みした情報を使用して、すべてのファイル処理を実行できます。サーバー上のファイル（コンテンツおよび属性）に変更を加えた場合は、ファイルを閉じるときに、その変更内容で更新する必要があります。 • バッチ：そのファイルを開いている唯一のクライアントであることを、クライアントに通知します。クライアントは、キャッシュ内情報または先読みした情報を使用して、すべてのファイル処理（オープンとクローズを含む）を実行します。サーバ側では、あるクライアント マシン上のローカル プロセスによってファイルが閉じられた場合でも、そのクライアントに対してファイルを開いたままにしておくことができます。このしくみには、クライアントが無意味なクローズ要求およびオープン要求を送信する必要がないため、ネットワーク トラフィック量を削減する効果があります。
書き込み時の通知有効	ファイル システムに書き込みがあった場合の通知を有効にします。

表 4. SMB のファイル システムの詳細設定 （続き）

設定	説明
	このオプションはデフォルトで無効になっています。
アクセス時の通知有効	ファイル システムがアクセスされた場合の通知を有効にします。 このオプションはデフォルトで無効になっています。
SMB Events Publishing の有効化	このファイル システムの SMB イベントの処理を有効にします。

SMB 共有の作成

SMB 共有を作成できるのは、SMB 対応の NAS サーバーで作成されたファイル システムです。

手順

1. ［Storage］ > ［File System］ > ［SMB Share］を選択します。
2. ［Create］をクリックして、［Create SMB Share ］ウィザードの作業を続行します。

オプション	説明
［File System］を選択します。	SMB が有効化されているファイル システムを選択します。
ファイル システムのスナップショットを選択	オプションで、共有を作成するファイル システム スナップショットのいずれか 1 つを選択します。 ファイル システム保護ポリシーでは、スナップショットのみがサポートされています。レプリケーションは、ファイル システムではサポートされていません。
SMB 共有の詳細	共有の名前とローカル パスを入力します。ローカル パスを入力すると、次のようになります。 ● 1 つの SMB ファイル システムに、同じローカル パスで複数の共有を作成できます。複数作成する場合、ホスト側ではユーザーごとに別々のアクセス制御が指定できますが、ファイル システム内の共有はすべて共通コンテンツにアクセスします。 ● 共有を作成する前に、ディレクトリーが存在しなければなりません。同じファイル システム内にある SMB 共有が別々のコンテンツにアクセスするようにするには、まず、そのファイル システムにマッピングしている Windows ホストでディレクトリーを作成する必要があります。そうすることにより、PowerStore を使用して、対応する共有を作成できます。Microsoft 管理コンソールから SMB 共有を作成し、管理することもできます。 PowerStore には、ホストを使用して共有に接続する SMB 共有パスも作成されています。 エクスポート パスは、ファイル システムの IP アドレスであり、共有の名前でもあります。ホストはファイル名か共有パスを使用して、ネットワーク ホストから共有にマウントまたはマッピングします。
高度な SMB プロパティ	Advanced SMB Settings を 1 つ以上有効にします。 ● 継続的な可用性 ● プロトコル暗号化 ● アクセス ベース列挙 ● 分岐キャッシュの有効化 共有がオフラインの場合、どのオブジェクトを利用可能にするかを決定します。 詳細については、「高度な SMB プロパティ詳細」を参照してください。

次の手順

共有を作成すると、その共有は、PowerStore によって、または Microsoft 管理コンソールを使用して変更できます。

PowerStore によって共有を変更するには、［SMB Share］ページのリストから共有を選択し、［Modify］をクリックします。

高度な SMB 共有プロパティ

SMB 共有を作成またはそのプロパティを変更するときは、次の高度な SMB 共有プロパティを構成することができます。

表 5. 高度な SMB プロパティ

オプション	説明
継続的な可用性	（フェールオーバー処理時に保存またはリストアされた NAS サーバーの内部状態を利用して）システム上の NAS サーバーをフェールオーバーした後、共有へのホスト アプリケーションの透過的かつ継続的なアクセスを可能にします。 **メモ:** 共有に対する継続的な可用性は、特定の共有で Microsoft SMB（サーバー メッセージ ブロック）3.0 プロトコル クライアントを使用する場合にのみ有効にします。
プロトコル暗号化	共有を経由するネットワーク トラフィックの SMB の暗号化を有効にします。SMB 3.0 以降のクライアントでは、SMB 暗号化がサポートされています。デフォルトでは、プロトコル暗号化が有効な状態で SMB 2 クライアントが共有にアクセスしようとすると、アクセスが拒否されます。 これを制御するには、NAS サーバーで RejectUnencryptedAccess レジストリ キーを構成します。1（デフォルト）を指定すると、暗号化されていないアクセスを拒否します。0 を指定すると、暗号化をサポートしていないクライアントは暗号化なしでファイル システムにアクセスできます。
アクセス ベース列挙	共有上の使用可能なファイルとディレクトリーのリストを、要求ユーザーが読み取りアクセス権を持つファイルのみが含まれるようにフィルタリングします。 **メモ:** 管理者は常にすべてのファイルを表示できます。
分岐キャッシュの有効化	共有からコンテンツをコピーして、それを支社でキャッシュします。これにより、支社のクライアント コンピューターで、WAN 経由ではなくローカルでコンテンツにアクセスできるようになります。 BranchCache は、Microsoft ホストから管理されます。
オフライン可用性	オフライン ファイルのクライアント側キャッシュを構成します。 • ［マニュアル］：キャッシュが明示的に要求された場合のみ、ファイルがキャッシュされ、オフラインで使用可能になります。 • ［ユーザーが開いたプログラムおよびファイル］：クライアントが共有から開いたすべてのファイルが、自動的にキャッシュされ、オフラインで使用可能になります。クライアントが共有に接続している場合は、共有からこれらのファイルを開きます。このオプションは、作業を共有するファイルで推奨されます。 • ［ユーザーが開いたプログラムおよびファイル、パフォーマンスについて最適化］：クライアントが共有から開いたすべてのファイルが自動的にキャッシュされ、オフラインで使用可能になります。クライアントは、ネットワークに接続している場合でも、可能であれば、共有のローカル キャッシュからファイルを開きます。このオプションは、実行可能プログラムで推奨されます。 • ［なし］：オフライン ファイルのクライアント側のキャッシュが構成されていません。

ACL の管理

SMB 共有（アクセス制御リストまたは ACL）のアクセス権は、MMC コンソールを使用して Windows クライアントによって設定および変更されます。UI または REST API を使用して、SDNAS クラスター上の SMB 共有の ACL を PowerStore から直接管理できるようになりました。

メモ: REST API を使用して ACL を設定する方法の詳細については、https://www.dell.com/powerstoredocs にある *Dell PowerStore REST API* リファレンス ガイドを参照してください。

メモ: SMB 共有内のファイルとディレクトリーのアクセス権は、Windows クライアントを使用してのみ管理できます。

PowerStore Manager を使用して［アクセス制御リスト］画面を開くには、［ストレージ］ > ［ファイル システム］ > ［SMB 共有］ > ［[SMB 共有]］ > ［その他のアクション］ > ［アクセス制御リスト］を選択します。

［アクセス制御リスト］画面には、選択した SMB に対して定義されているアクセス制御エントリー(ACE)のリストが表示されます。ACE ごとに、トラスティ名または ID、アクセス レベル、アクセス タイプが一覧表示されます。このリストはいずれかの属性でフィルタリングできます。

メモ: デフォルトの ACE は、すべてのユーザーにフル アクセス権を付与します。

［アクセス制御リスト］ダイアログでは、次の操作を実行できます。

- ACE の追加 - 詳細については、アクセス制御エントリーの追加を参照してください。
- ACE の変更 - 選択した ACE フィールドのいずれかを編集します。
- 選択した ACE を削除します。
- ACL の更新（［その他のアクション］） - Windows MMC コンソールまたは REST API を使用して ACL を変更した場合は、このオプションを使用します。［更新］オプションを選択すると、ACL が変更内容で更新されます。

アクセス制御エントリーの追加

このタスクについて

ACE は次の属性で構成されます。

- トラスティ タイプ - ユーザー、グループ、セキュリティ識別子(SID)、ウェルノウン
- トラスティ名/ID - このフィールドの形式は、次のトラスティ タイプに基づいて決定されます。
  - ユーザー名 - ドメイン/ユーザー名
  - グループ名 - ドメイン/グループ名
  - SID - SID 形式（例：S-1-2-34-567890123-456789012-3456789012-34）
  - ウェルノウン - 例：「Everyone」
- アクセス レベル - 読み取り、変更、フル
- アクセス タイプ - 許可または拒否

手順

1. ［ストレージ］ > ［ファイル システム］ > ［SMB 共有］ > ［[SMB 共有]］ > ［その他のアクション］ > ［アクセス制御リスト］を選択します。
2. ［アクセス制御リスト］ウィンドウで［ACE の追加］を選択します。
3. ACE のフィールドを設定して、［保存］をクリックします。
   新しい ACE が ACL に追加されます。
4. ［[Apply]］をクリックして変更を保存します。

5

その他のファイル システム機能

この章では、次の情報について説明します。

トピック：

ファイル レベル保存期間設定

ファイル レベル保存期間設定（FLR）により、指定した保存期間のロックの変更や削除を防止できます。FLR を使用してファイル システムを保護することで、永続的で変更不可能な一連のファイルとディレクトリーを作成できます。FLR は、データ インテグリティ/アクセシビリティを確保し、管理者にとってのアーカイブ手順をシンプルにし、ストレージ管理の柔軟性を向上するものです。

ファイル レベル保存期間設定には、次の 2 つのレベルがあります。

- エンタープライズ（FLR-E） - ユーザーやストレージ管理者が SMB、NFS、FTP を使用して行った変更からデータを保護します。管理者には、ロックされたファイルを含む FLR-E ファイル システムの削除ができます。
- コンプライアンス（FLR-C） - ユーザーやストレージ管理者が SMB、NFS、FTP を使用して行った変更からデータを保護します。管理者にも、ロックされたファイルを含む FLR-C ファイル システムの削除はできません。FLR-C は、SEC ルール 17a-4（f）に準拠しています。

次の制限事項が適用されます。

- ファイル レベル保存期間設定は、統合 PowerStore システム 3.0 以降で利用可能です。
- FLR は、VMware のファイル システムではサポートされません。
- ファイル システムのファイル レベル保存期間設定と FLR レベルの有効化は、ファイル システムの作成時に設定され、変更はできません。
- FLR-C では、スナップショットからのリストアはサポートしません。
- スナップショットを使用して更新する場合、両方のファイル システムで FLR レベルを同じにする必要があります。
- ファイル システムをレプリケートする場合、ソース ファイル システムとデスティネーション ファイル システムとで FLR レベルを同じにする必要があります。
- クローン作成によるファイル システムの FLR レベルはソースと同じです（変更はできません）。

FLR モードは［File Systems］画面に表示されます。

DHSM サーバーの設定

前提条件

ファイル レベル保存期間設定には、DHSM サーバーの認証情報が必要です。

DHSM サーバーは、FLR を使用することが考えられ、FLR が有効化されているファイル システムの管理を可能にする FLR ツールキットをインストールするために必要とされる Windows ホストにも必要です。

手順

1. ［Storage］ > ［NAS Servers］ > ［[NAS server]］ > ［Protection］ > ［DHSM］を選択します。
2. 無効化されている場合は、ボタンを［Enabled］にスライドさせます。
3. DHSM サーバーのユーザー名とパスワードを入力し、パスワードを検証します。
4. ［Apply］を選択します。

ファイル レベル保存期間の構成

ファイル レベル保存期間は、ファイル システムの作成時に構成されます。詳細については、「ファイル システムの作成」を参照してください。

メモ: 保存期間のパラメーターは、後で変更できます。

ファイル レベル保存期間設定の変更

このタスクについて

保存期間パラメーターは、ファイル システムの作成時に設定され、それ以降にも設定、変更できます。保存期間パラメーターを変更しても、すでにロックされているファイルには影響しません。

手順

1. ［Storage］ > ［File Systems］ > ［[file system]］ > ［Security & Events］ > ［File-Level Retention］を選択します。
2. 次の保存期間パラメーターを設定します。
   - Minimum retention period - FLR が有効化されているファイル システムを保護できる最短期間を指定します（デフォルト値は 1 日）。
   - Default retention period - ファイルがロックされ、保存期間が指定されていない場合に使用されます（デフォルト値は 1 年）。
   - Maximum retention period - FLR が有効化されているファイル システムを保護できる最長期間を指定します（デフォルト値は infinite）。
3. 必要に応じて、Advanced Settings を設定します。
   - Automatic file locking - FLR が有効化されているファイル システムにあるファイルを自動的にロックするかどうかを指定し、ファイルの変更と自動ロックとの間の期間を決定するポリシー インターバルを設定できます（ポリシー インターバルのデフォルト値は 1 時間）。
   - Automatic file deletion - ロックされているファイルの保存期間が切れたら自動的に削除するかどうかを指定します。削除対象のファイルを特定するための最初のスキャンは、この機能が有効化されてから 7 日後です。
4. ［Apply］を選択します。

ファイル システム クォータ

ファイル システム レベルまたはディレクトリー レベルでファイル システムのクォータを構成することで、ドライブ領域の使用量をトラッキングおよび制限することができます。クォータはいつでも有効化または無効化することができますが、ファイル システム操作に影響しないように、ピーク時以外の本番稼働時間中に有効化または無効化することをお勧めします。

メモ: 読み取り専用ファイル システムのクォータを有効にすることはできません。

メモ: クォータは VMware ファイル システムではサポートされていません。

クォータのタイプ

ファイル システムには 3 つのタイプのクォータを設定できます。

表 6. クォータのタイプ

Type	説明
ユーザー クォータ	個々のユーザーがファイル システムにデータを格納することによって消費するストレージの量を制限します。
ツリー クォータ	ツリー クォータは、特定のディレクトリー ツリーで使用されるストレージの合計容量を制限します。ツリー クォータは次の目的で使用できます。 ● プロジェクト ベースでストレージ制限を設定する。たとえば、複数のユーザーがプロジェクト ディレクトリーでファイルを共有および作成する場合、そのプロジェクト ディレクトリーにクォータ ツリーを確立できます。 ● ツリー クォータのハード制限とソフト制限を 0（ゼロ）に設定して、ディレクトリーの使用量をトラッキングする。 メモ: ツリー クォータの制限を変更した場合、ファイル システム操作を中断することなく即座に変更内容が反映されます。
クォータ ツリーのユーザー クォータ	個々のユーザーがクォータ ツリーにデータを格納することによって消費するストレージの量を制限します。

クォータの制限

表 7. ハード制限とソフト制限

Type	説明
ハード	ハード制限は、ストレージの使用量の絶対的な制限です。 ファイル システムまたはクォータ ツリーのユーザー クォータのハード制限に到達すると、追加の領域が使用可能になるまで、ユーザーはファイル システムまたはツリーにデータを書き込むことができません。クォータ ツリーのハード制限に到達すると、追加の領域が使用可能になるまで、どのユーザーもツリーにデータを書き込むことができません。
ソフト制限	ソフト制限は、ストレージ使用量の推奨される制限です。 ユーザーは、猶予期間に達するまでは容量を使用できます。 猶予期間が終わるまでにソフト制限に達した場合は、ユーザーにアラートが発行されます。その後は、ユーザーがソフト制限を下回るまで、スペース不足状態になります。

クォータの猶予期間

ファイル システム上の各ツリー クォータに、特定の猶予期間を設定できます。猶予期間は、ソフト制限とハード制限の間の時間をカウントし、ハード制限を超過するまでの残り時間をユーザーに通知します。猶予期間が経過すると、ハード制限に達していない場合でも、スペースが追加されるまで、ユーザーはファイル システムやクォータ ツリーへの書き込みができなくなります。

猶予期間に有効期限を設定することができます。デフォルトは 7 日です。猶予期間の有効期限を無期限に設定して猶予期間が期限切れにならないようにしたり、指定した日数、時間数、分数のいずれかに設定したりすることもできます。猶予期間の有効期限が切れると、猶予期間はファイル システム ディレクトリーに適用されなくなります。

関連情報

クォータの詳細については、*Dell PowerStore* ファイル機能ホワイト ペーパーを参照してください。

ユーザー クォータの有効化

ファイル システムにユーザー クォータを追加するには、クォータを有効化し、ユーザー クォータのデフォルト値を設定する必要があります。

手順

1. ［Storage］ > ［File Systems］ > ［[file system]］ > ［Quotas］を選択します。
2. ［Storage］ > ［File Systems］ > ［[file system]］ > ［Quotas］ > ［Properties］を選択します。
3. ［Disabled］ボタンを右にスライドさせて、［Enabled］にします。
4. ファイル システムのユーザー クォータのデフォルトの［Grace Period］を入力します。これにより、ソフト制限が満たされた後、ハード制限に到達するまでの時間がカウントされます。
5. デフォルトの［Soft Limit］、デフォルトの ［Hard Limit］の順に入力して、［Update］をクリックします。

ファイル システムへのユーザー クォータの追加

個々のユーザーがファイル システムで消費できるストレージ領域の量を制限またはトラッキングするには、そのファイル システムでユーザー クォータを作成します。ユーザー クォータを作成または変更する際は、ファイル システム レベルで設定されたデフォルトのハード制限とソフト制限が使用できます。

前提条件

ファイル システムにユーザー クォータを追加するには、クォータを有効化し、ユーザー クォータのデフォルト値を設定する必要があります。ユーザー クォータの有効化を参照してください。

メモ: 読み取り専用ファイル システムのクォータを作成することはできません。

手順

1. ［ストレージ］ > ［ファイル システム］ > ［[ファイル システム]］ > ［クォータ］ > ［ユーザー］を選択します。
2. ［User Quota］ページで［Add］をクリックします。
3. ［Add User Quota］ウィザードで、要求されている情報を入力します。制限を設定せず領域の消費量をトラッキングするには、［Soft Limit］と［Hard Limit］を 0（制限なしを意味します）に設定します。
4. ［Add］を選択します。

ファイル システムへのクォータ ツリーの追加

このタスクについて

ディレクトリーに消費される総ストレージ スペースを制限したりトラッキングしたりするには、ファイル システムのディレクトリー レベルでクォータ ツリーを作成します。

手順

1. ［Storage］ > ［File Systems］ > ［[file system]］ > ［Quotas］ > ［Tree Quotas］を選択します。
2. ［Add］を選択します。
3. ツリー クォータのユーザー クォータのデフォルト値を有効にするには、［Enforce User Quota］を右にスライドさせます。
4. 要求された情報を入力します。
   - ソフト制限とハード制限の間の時間をカウントダウンする［猶予期間］を入力します。猶予期間に達すると、アラートの受信が開始されます。
   - 制限を設定せず領域の消費量をトラッキングするには、［Soft Limit］フィールドと［Hard Limit］フィールドを 0（制限なしを意味します）に設定します。
5. ［Add］を選択します。

クォータ ツリーへのユーザー クォータの追加

個々のユーザーがクォータ ツリーで消費できるストレージ領域の量を制限またはトラッキングするには、そのクォータ ツリーでユーザー クォータを作成します。ツリーでユーザー クォータを作成する際は、ツリークォータ レベルで設定されたデフォルトのハード制限とソフト制限を使用できます。

手順

1. ［Storage］ > ［File Systems］ > ［[file system]］ > ［Quotas］ > ［Tree Quotas］を選択します。
2. パスを選択して、［Add User Quota］をクリックします。
3. ［Add User Quota］画面で、要求されている情報を入力します。制限を設定せず領域の消費量をトラッキングするには、［Soft Limit］フィールドと［Hard Limit］フィールドを 0（制限なしを意味します）に設定します。

6

NAS サーバーのレプリケーション

この章では、次の情報について説明します。

トピック：

概要

PowerStore では、ローカル システムとリモート システム間で NAS サーバーを非同期的にレプリケートできます。レプリケーションは NAS サーバー レベルで実行されます。レプリケートされた NAS サーバー内のすべてのファイル システムがリモート システムにレプリケートされます。RPO は NAS サーバー レベルで構成され、関連づけられているすべてのファイル システムで同一になります。

NAS サーバーに個別の保護ポリシーを定義する必要はありません。同じ保護ポリシーをブロック レプリケーションとファイル レプリケーションの両方に適用できます。

レプリケーション セッションはリモート システムにフェールオーバーできます。フェールオーバーは、フェールオーバーされた NAS サーバー内のすべてのファイル システムに対して行われます。

ファイル レプリケーションを有効にするには、次の前提条件が必要です。

- ファイル リモート システム
- File Mobility ネットワークを構成し、マッピングする必要があります（PowerStore ドキュメント ページの *PowerStore T* モデルのネットワーキング ガイドを参照）。
- レプリケーション ルールを含む保護ポリシー。

NAS サーバーのレプリケーション手順の詳細については、PowerStore ドキュメント ページのデータの保護を参照してください。

レプリケーション中の NAS サーバーのディザスター リカバリー テスト

ディザスター リカバリー テストでは、ディザスター リカバリー計画を実行して、災害が発生した場合にシステムがデータと操作をリカバリー/リストアできることを確認します。

PowerStore には、システムが災害から復旧して機能を回復できるかどうかをテストするためのオプションがいくつか用意されています。

- 固有の IP アドレスを使用してディザスター リカバリー テスト用の NAS サーバーのクローンを作成
- 重複する IP アドレスを持つ分離されたネットワークを使用して、ディザスター リカバリー テスト用の NAS サーバーのクローンを作成
- 計画的なフェールオーバーの実行

固有の IP アドレスを使用してディザスター リカバリー テスト用の NAS サーバーのクローンを作成

このタスクについて

NAS サーバーのクローンを作成することは、DR をテストするための推奨オプションです。PowerStore Manager を使用して NAS サーバーのクローンを作成し、本番環境に影響を与えることなくテストできます。新しくクローン作成された NAS サーバーへのアクセスを有効にするには、新しい一意のネットワーク インターフェイスを構成する必要があります。設定する IP アドレスは、ソースとデスティネーションのいずれの NAS サーバーでも使用されていてはなりません。サーバーを AD ドメインに参加させる場合は、一意の設定も必要です。

クローン作成されたファイル システムでの変更と本番ファイル システムでの変更は、相互に影響しません。DR テストが完了したら、クローン作成されたサーバーを削除できます。

次のいずれかのオプションを選択できます。

- ソース システム上の NAS サーバーのクローンを作成し、デスティネーションにレプリケートして、デスティネーション システムへの計画的なフェールオーバーを実行します。
- デスティネーション システムで NAS サーバーのクローンを作成し、データにアクセスします（クローン作成されたリソースはデスティネーション システムですでにアクセスできるため、フェールオーバーは必要ありません）。

手順

1. PowerStore Manager で、［ストレージ］ > ［NAS サーバー］を選択します。
2. クローンを作成する NAS サーバーを選択し、［再利用］ > ［NAS サーバーのクローン作成］を選択します。
3. ［クローンの作成］ウィンドウで、クローンの名前を入力し、クローンを作成するファイル システムを選択します。
4. ［Create］を選択します。
   クローン作成された NAS サーバーがサーバー リストに追加されます。
5. クローン作成された NAS サーバーの名前を選択して、サーバーの詳細ウィンドウを開きます。
6. ファイル インターフェイスを追加するには、次の手順を実行します。
   a. ［ネットワーク］タブを選択します。
   b. ［ファイル インターフェイス］で［追加］を選択します。
   c. インターフェイス情報を入力し、［追加］を選択します。
7. 共有プロトコルを設定するには、次の手順を実行します。
   a. ［共有プロトコル］タブを選択します。
   b. 適切なプロトコル（SMB、NFS、FTP）を選択します。
   c. 必要な情報を設定して、［適用］を選択します。
8. ソース NAS サーバーのクローンを作成した場合は、次の手順を実行します。
   a. NAS サーバーをデスティネーション システムにレプリケートします。詳細については、「NAS サーバー レプリケーション」を参照してください。
   b. デスティネーションへの計画的なフェールオーバーを実行します。詳細については、「計画的なフェールオーバー」を参照してください。
   c. ホストがデータにアクセスできるかどうかを確認します。
9. デスティネーション システム上のレプリケートされた本番サーバーのクローンを作成した場合、フェールオーバーは必要ありません。ホスト アクセスを確認します。

重複する IP アドレスを持つ分離されたネットワークを使用して、ディザスター リカバリー テスト用の NAS サーバーのクローンを作成

本番環境と同じ構成を使用してディザスター リカバリーをテストできます。同じ設定を使用すると、障害シナリオのリスクを低減し、再現可能性を高めることができます。ただし、重複する IP アドレスを使用すると競合が生じます。本番環境から分離された環境で DR テストを実行すると、これらの競合を回避できます。

PowerStore バージョン 3.6 以降では、本番環境から分離されたディザスター リカバリー テスト(DRT)環境を作成して、災害に備えることができます。

分離された環境を作成すると、本番システムと同じ IP アドレスとホスト名を使用し、本番環境に影響を与えることなく、レプリケーション中の NAS サーバーに対して DRT を実行できるようになります。

DRT 環境を作成するには、個別の DLT ルーターを使用して分離されたネットワークをセットアップし、ネットワーク I/O ポートを使用してリンク アグリゲーションを作成する必要があります。

PSTCLI または REST API を使用して、デスティネーション PowerStore システム上でレプリケーション中の NAS サーバーのクローンを作成することにより、宛先サーバー上に専用のネットワーキング環境を作成します。クローンは、本番環境のフル コピーであり、本番環境から分離された専用のテスト環境です。分離されたネットワーキング環境を作成し、本番システムと同じ IP アドレスとホスト名を使用してテスト環境を構成できます。DRT NAS サーバーは本番環境に影響を与えず、レプリケーション NAS サーバーでフェールオーバーとフェールバックが発生したときに、IP アドレスの競合なしで実行できます。

分離されたテスト環境を使用して DR をテストするには、次の手順を実行します。

1. デスティネーション システムで NAS サーバーのクローンを作成します。`is_dr_test` フラグを使用します。
2. ソース NAS サーバーと同じ IP アドレスを使用して、NAS のユーザー ボンド インターフェイスを作成します。
3. クローンを AD に参加させます（必要な場合）。
4. ホストがデータにアクセスできることを確認します。

メモ: スタンドアロン NAS サーバーで DRT を使用することもできます。

前提条件と制限事項

DRT 環境を作成するには、次の要件が満たされていることを確認します。

- プライベート ネットワーク情報を取得します。
  - Gateway
  - ネットマスク
  - VLAN ID（オプション）
- 分離されたネットワークのネットワーク ポートと本番ネットワークのネットワーク ポートを特定します。

DRT 環境を作成する場合は、次の制限事項に注意してください。

- DRT 専用のボンド インターフェイスを使用して、他の本番 NAS サーバーを作成することはできません。
- 本番環境として構成されている NAS サーバーは、DRT の一部として再構成できません。
- DRT の一部として構成されている NAS サーバーは、本番環境として再構成できません。
- DRT の一部でなくなった NAS サーバーは再構成できず、削除する必要があります。
- NAS サーバーがアクティブになり、ネットワーク情報で構成された後で、追加の構成（DNS、CAVA、Kerberos など）を手動で実行する必要があります。
- DRT 対応 NAS サーバーはレプリケートできません。
- NAS サーバーの変更と削除は、PowerStore Manager を使用して行うことができます。

PSTCLI を使用したディザスター リカバリー テスト環境の構成

手順

1. デスティネーション サイト（クローン作成対象）上の NAS サーバーの名前を取得します。

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+-------------+--------+--------------------+------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. クローンの新しい名前を入力し、`-is_dr_test true` スイッチを使用して NAS サーバーのクローンを作成します。

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. 分離されたネットワークに接続されている NAS ファイル ボンドの IP ポート ID を検索します。

   メモ: NAS ファイル ボンドが作成されていない場合は、PSTCLI または PowerStore Manager を使用して作成できます。

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. クローン作成された NAS サーバー用のインターフェイスを作成します。

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. ファイル インターフェイスを表示します。

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

REST API を使用した DRT 環境での NAS サーバーの構成

このタスクについて

メモ: REST API を使用していない場合は、このセクションをスキップしてください。

手順

1. 指定したネームスペースで NAS サーバーのクローンを作成するには、`/nas_server/{id}/clone` を実行して、`is_dr_test` を true として指定します。
2. ネットワーク インターフェイスを作成するには、`/file_interface` を実行して、プライベート ネットワーク パラメーターを指定します。

   メモ: このステップによって、本番 NAS サーバーと同じ IP アドレス、ネットマスク、ゲートウェイを使用して、クローンを作成した NAS サーバーのファイル インターフェイスを作成します。プライベート ネットワークに関連づけられているボンド インターフェイス/IP_Port を使用します。

タスクの結果

NAS サーバーが稼働し、分離されたネットワークでの DRT に使用できるようになります。

計画的なフェールオーバーの実行

計画的なフェールオーバーを使用して、ディザスター リカバリーをテストできます。計画的なフェールオーバーを実行すると、NAS サーバーのレプリケーション セッションが、ソース システムからデスティネーション システムに手動でフェールオーバーされます。フェールオーバーの前に、デスティネーション システムがソース システムと同期されるため、データ ロスの発生を防ぐことができます。

メモ: 本番 NAS サーバーをデスティネーション システムにフェールオーバーすると、本番環境に影響する可能性があります。

計画的なフェールオーバーを実行する前に、すべてのアプリケーションとホストの I/O 動作を停止するようにしてください。計画されたフェールオーバーを行っているレプリケーション セッションを一時停止することはできません。

DR テスト中に NAS サーバーとファイル システムに加えられた変更は保持され、再保護が開始されると元のソースに(手動または自動で)レプリケートされます。NAS サーバーが再保護された後、計画的なフェールオーバーを再度開始して、リソースを元のソース システムでオンラインにすることができます。

メモ: ディザスター リカバリー目的で計画外フェールオーバーを実行しないでください。計画外フェールオーバーは、ソース システムにアクセスできない場合にのみ使用してください。

計画的なフェールオーバーを開始するには、次の 2 つの方法があります。

- ［Protection］ > ［Replication］で、関連するレプリケーション セッションを選択してから、［Planned Failover］を選択します。
- リソースの［Protection］タブで、［Replication］を選択してから、［Planned Failover］を選択します。

計画されたフェールオーバー後は、レプリケーション セッションが非アクティブになります。デスティネーションストレージ リソースを同期し、レプリケーション セッションを再開するには、［再保護］アクションを使用します。フェールオーバーの前に自動再保護オプションを選択することもできます。これにより、フェールオーバーが完了した後で、同期が逆方向（次の RPO で）に自動的に開始され、ソースとターゲット システムが通常の状態に戻ります。

DRT 中のネットワーク切断

DRT を実行する際に、ローカル システムとリモート システム間のネットワーク障害をシミュレートしてから、デスティネーション システムへの計画外フェールオーバーを実行し、DR NAS サーバーへのアクセスを有効にすることは推奨されません。システム間の通信がないため、PowerStore は両方の NAS サーバーが互換性のある状態であることを確認できません。接続がリストアされた後、両方の NAS サーバーが本番モード（スプリット ブレイン状態）になります。その結果、両方のシステムがメンテナンス モードに切り替わり、データを両方の場所に書き込めなくなります。

この状態を解決するには、テクニカル サポートの介入が必要です。

詳細については、Dell ナレッジベース記事 000215482（サイト間のネットワーク接続の切断）を参照してください。

7

PowerStore での CEPA の使用

この章では、次の情報について説明します。

トピック：

イベント パブリッシング

CEE は、ファイル システムにアクセスしたサードパーティー アプリケーションで、ストレージ システムからのイベント情報を受信できるようにするものです。

CEE（Common Event Enabler）とは PowerStore クライアント向けのイベント パブリッシング ソリューションであり、ファイル システムにアクセスしたサードパーティー アプリケーションでストレージ システムからのイベント通知とコンテキストを登録したり受信したりできるようにするものです。イベント通知を受信して、イベント主導型のアクションをストレージで実行すると、ランサムウェアや不正アクセスといったセキュリティ上の脅威を防ぐことができます。

CEE Common Events Publishing Agent（CEPA）は、SMB ファイル、NFS ファイル、ディレクトリー イベント通知を処理するよう設計されているアプリケーション群で構成されています。CEPA では、イベント通知と関連コンテキストの両方を 1 つのメッセージでアプリケーションに送ります。コンテキストを構成するのは、ビジネス ポリシーの決定に必要なファイル メタデータまたはディレクトリー メタデータです。

CEE CEPA サポートを有効化するには、CEE CEPA を有効化してイベント パブリッシング プールを NAS サーバーに作成する必要があります。

イベント パブリッシング プールでは、CEPA サーバーと、通知をトリガーする特定のイベントを定義します。

NAS サーバーを設定した後であれば、イベント パブリッシングは、イベントを受信させるファイル システムで有効化することができます。ホストによりイベントをファイル システムで SMB または NFS 経由で生成すると、その情報が CEPA サーバーへ HTTP 接続経由で転送されます。サーバーでは、イベントを CEE CEPA ソフトウェアで受信してパブリッシュするので、サードパーティー製ソフトウェアで処理できるようになるわけです。

Events Publishing Agent を使用するには、PowerStore システムの NAS サーバーがネットワークで少なくとも 1 つ設定されていることが必要です。

Common Event Enabler (CEE)の一部である CEPA の詳細については、https://www.dell.com/support の「*Windows* プラットフォームでの *Common Event Enabler* の使用」を参照してください。

パブリッシング プールの作成

前提条件

イベント パブリッシング プールを作成するには、イベント パブリッシング（CEPA）サーバーの FQDN が必要です。

このタスクについて

イベント パブリッシング プールでは、CEPA サーバーと、通知をトリガーする特定のイベントを定義します。次のイベント オプションのうち、少なくとも 1 つを定義します。

- Pre Events：承認を得るため処理前に CEPA サーバーへ送信されるイベント。
- Post Event：発生してからログ記録や監査の目的で CEPA サーバーへ送信されるイベント。
- Post Error Event：発生してからログ記録や監査の目的で CEPA サーバーへ送信されるエラー イベント。

手順

1. ［Storage］ > ［NAS Servers］を選択します。
2. ［NAS Settings］を選択します。
3. ［Event Publishing］ウィンドウで、 ［Publishing Pools］ を選択して、［Create］を選択します。

4. ［Pool Name］を入力します。
5. CEPA サーバーの FQDN を入力します。
6. ［Event Configuration］セクションでイベント タイプをクリックし、プールへ追加するイベントを選択します。
7. ［Apply］をクリックして、イベント パブリッシング プールを作成します。

イベント パブリッシャーの作成

このタスクについて

パブリッシング プールを設定したら、イベント パブリッシャーを作成して、さまざまなイベント タイプに対する応答を設定します。

メモ: イベント パブリッシャーはシステム レベルで作成され、1 つのイベント パブリッシャーを複数の NAS サーバーに関連付けることができます。

手順

1. ［Storage］ > ［NAS Servers］を選択します。
2. ［NAS Settings］を選択します。
3. ［Event Publishers］ を選択して、［Create］ を選択します。
4. ［Create Event Publisher］ウィザードで作業を続行します。

ウィザード画面	Description
Select Publishing Pools	● 名前を入力します。 ● パブリッシング プールを最大 3 つ選択します。新しいパブリッシング プールを作成するには、［Create］をクリックします。
Configure Event Publisher	● Pre-Events Failure Policy - すべての CEPA サーバーがイベント前にオフラインになっている場合の、望まれる動作を選択します。 ○ Ignore（デフォルト） - すべてのイベントが受信確認されているとみなします。 ○ Deny - CEPA サーバーがオンラインになるまでは、承認が必要なイベントを拒否します。 ● Post-Events Failure Policy - すべての CEPA サーバーがイベント後にオフラインになる場合の、望まれる動作を選択します。 ○ Ignore（デフォルト） - 動作を続行します。CEPA サーバーがダウンしている間に発生したイベントは、失われます。 ○ Accumulate - 動作を続行し、イベントをローカル バッファー（最大 500 MB）に保存します。 ○ Guarantee - 動作を続行し、イベントをローカル バッファー（最大 500 MB）に保存します。バッファーが満杯になると、アクセスを拒否します。 ○ Deny - CEPA サーバーがオフラインの場合、ファイル システムへのアクセスを拒否します。 ● HTTP/Microsoft RPC ● HTTP Port

5. ［Apply］を選択して、イベント パブリッシャーを作成します。

NAS サーバーのイベント パブリッシャーを有効化する

このタスクについて

イベント パブリッシャーを設定したら、NAS サーバーとそこで定義されているすべてのファイル システムで有効化します。

手順

1. ［ストレージ］ > ［NAS サーバー］ > ［[NAS サーバー]］を選択します。
2. ［セキュリティとイベント］ページで［イベントのパブリッシュ］を選択します。
3. リストからイベント パブリッシャーを選択し、有効化します。
4. NAS サーバーで定義されているすべてのファイル システムでイベント パブリッシャーを有効化するかどうかを選択します。
   代わりに、イベント パブリッシャーを特定のファイル システムで有効化するという選択もできます。詳細については、「ファイル システムでのイベント パブリッシャーの有効化」を参照してください。
5. ［適用］をクリックします。

ファイル システムでのイベント パブリッシャーの有効化

このタスクについて

ファイル システムを選択してイベント パブリッシャーを有効化することができます。

手順

1. ［ストレージ］ > ［ファイル システム］ > ［[ファイル システム]］を選択します。
2. ［保護］ページで［イベントのパブリッシュ］を選択します。
3. ファイル システムのイベントパブリッシャーを有効化し、プロトコルを選択します。
4. ［適用］をクリックします。