Dell EMC PowerStore

セキュリティ構成ガイド

1.x

July 2020
Rev. A02

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

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

警告: 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、テクニカル サポート プロフェッショナル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、www.dell.com/powerstoredocs で [PowerStore Documentation] ページを参照してください。

- **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、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、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

認証とアクセス

この章では、次の情報について説明します。

トピック：

ユーザー アカウント、役割、権限の認証と管理を行う

クラスターへのアクセスの認証は、ユーザー アカウントの認証情報に基づいて実行されます。ユーザー アカウントは、**Users** ページで作成され、その後、管理されます。このページには、PowerStore Manager の **Settings** > **Users** > **Users** でアクセスできます。適用される許可は、ユーザー アカウントに関連づけられた役割に基づいています。ユーザーがクラスターのネットワーク アドレスを Web ブラウザーに URL として指定すると、ログイン ページが表示され、ローカル ユーザーとして認証できます。ユーザーが入力する認証情報が認証され、システム上でセッションが作成されます。その後、ユーザーは、ユーザーに割り当てられた役割の機能内でクラスターの監視と管理を行うことができます。

クラスターは、管理サーバーとの安全な接続を介してユーザー名とパスワードを検証することによりユーザーを認証します。

工場出荷時デフォルトの管理

アプライアンスは、アプライアンスに初めてアクセスして構成する際に使用するデフォルトのユーザー アカウント設定が行われた状態で出荷されます。

メモ: リリース 1.0.x の PowerStore の初期構成には、API、コマンド ライン インターフェイス (CLI)、サービス スクリプト インターフェイスを使用するよりも、PowerStore Manager UI を使用することが推奨されます。これにより、すべてのデフォルトのパスワードが確実に変更されます。

アカウント タイプ	ユーザー名	パスワード	権限
システム管理	admin	Password123#	デフォルトのパスワードのリセット、アプライアンス設定の構成、ユーザー アカウントの管理を行うための Administrator 権限。
サービス	service	service	保守作業の実行用。 **メモ:** サービス ユーザーは、セキュア シェル (SSH)アクセスのために存在しています。ただし、サービス ユーザーを使用して PowerStore Manager にログインすることはできません。

セッション規則

クラスター上のセッションには、次の特性があります。

- 有効期限は 1 時間。

  メモ: セッションが 1 時間非アクティブになると、ユーザーは自動的にクラスターからログオフします。
- セッション タイムアウトは構成できない。

ユーザー名とパスワードの使用

システム アカウントのユーザー名は、次の要件を満たしている必要があります。

制限	ユーザー名の要件
構造	先頭と末尾の文字は英数字である必要があります。
ケース	すべてのユーザー名は大文字と小文字が区別されます。
英数字の最小数	1
英数字の最大数	64
サポートされる特殊文字：	.（ドット）

システム アカウントのパスワードは、次の要件を満たしている必要があります。

制限	パスワードの要件
文字の最小数	8
大文字の最小数	1
小文字の最小数	1
数字の最小数	1
特殊文字の最小数 • 使用可能な文字：! @ # $ % ^ * _ ~ ? メモ: パスワードには、一重引用符 (')、アンパサンド (&)、またはスペース文字を含めることはできません。	1
文字の最大数	40

メモ: 最新の 5 つのパスワードは、再使用することができません。以前のパスワードを再使用できるのは、パスワードを 5 回以上、変更した後です。

ESXi パスワード

PowerStore X model アプライアンス上の ESXi のデフォルト root パスワードは、次の形式になっています：***<Service_Tag>*123!**（*<Service_Tag>* はアプライアンスの 7 文字のサービス タグ）。

初期のクラスター構成が完了するまでは、ESXi のデフォルト パスワードを変更しないでください。ESXi のパスワードの変更について詳しくは、VMware ESXi のマニュアルを参照してください。

注意: ESXi のパスワードは紛失しないようにしてください。ESXi がダウンした際にパスワードが分からない場合は、アプライアンスを再初期化する必要があります。この動作は ESXi にとって正常ですが、パスワードを紛失したために再初期化すると、データが失われる可能性があります。

注意: ESXi のデフォルト パスワードは、PowerStore X model アプライアンスごとに個別に構成されます。アプライアンス内のノードが vCenter クラスターに追加されると、このパスワードが ESXi ホストでの認証に使用されます。クラスターが完全に構成される前にデフォルト パスワードを変更した場合は、アプライアンスを再初期化する必要があります。

役割と権限

ロールベースのアクセス制御により、ユーザーにさまざまな権限を付与することができます。これにより、スキルセットや責任に適合するように管理者の役割を分離することができます。

システムでは、次の役割と権限がサポートされています。

メモ: ✓のある欄は、その役割で権限がサポートされていることを示し、空欄は、その役割で権限がサポートされていないことを示しています。

タスク	オペレーター	VM 管理者	セキュリティ管理者	ストレージ管理者	管理者
システムのローカル パスワードの変更	✓	✓	✓	✓	✓
システム設定、ステータス、パフォーマンス情報の表示	✓		✓	✓	✓
システム設定の変更					✓
リソースと保護ポリシーの作成、変更、削除、および SSH の有効化/無効化				✓	✓
vCenter への接続		✓		✓	✓
ローカル アカウントのリストの表示			✓		✓
ローカル アカウントの追加、削除、変更			✓		✓
システムの VASA プロバイダーに接続されている vCenter サーバーを介したシステム ストレージ情報の表示と、VMware 認証局 (VMCA) /CA 証明書の登録/再登録		✓			✓

ファイルに関連する役割と権限

システムでは、次のような、ファイルに関連する役割と権限がサポートされています。

メモ: ✓のある欄は、その役割で権限がサポートされていることを示し、空欄は、その役割で権限がサポートされていないことを示しています。

タスク	オペレーター	VM 管理者	セキュリティ管理者	ストレージ管理者	管理者
次の項目を表示します。 • ファイル システム アラート • NAS サーバー リスト • ファイル システム リスト • ファイル ユーザー クォータ リスト • ファイル インターフェイス ルート リスト • ファイル インターフェイス リスト	✓		✓	✓	✓

タスク	オペレーター	VM 管理者	セキュリティ管理者	ストレージ管理者	管理者
• SMB 共有リスト • NFS エクスポート リスト					
次の項目を表示します。 • ファイル DNS サーバーのリストまたは指定した DNS サーバー • ファイル FTP サーバーのリストまたは指定した FTP サーバー • ファイル インターフェイスのリストまたは指定したファイル インターフェイス • ファイル インターフェイス ルートのリストまたは指定したインターフェイス ルート • ファイル Kerberos サーバーのリストまたは指定した Kerberos サーバー • ファイル LDAP サーバーのリストまたは指定した LDAP サーバー • ファイル NDMP サーバーのリストまたは指定した NDMP サーバー • ファイル NIS サーバーのリストまたは指定した NIS サーバー • ファイル システムのリストまたは指定したファイル システム • ファイル ツリー クォータのリストまたは指定したファイル ツリー クォータ • ファイル ユーザー クォータのリストまたは指定したユーザー クォータ • ファイル ウイルス チェッカーのリストまたは指定したファイル ウイルス チェッカー • NAS サーバーのリストまたは指定した NAS サーバー • NFS エクスポートのリストまたは指定した NFS エクスポート • NFS サーバーのリストまたは指定した NFS サーバー • SMB サーバーのリストまたは指定した SMB サーバー • SMB 共有のリストまたは指定した SMB 共有	✓		✓	✓	✓
指定した NAS サーバーの追加、変更、削除、Ping、または指定した NAS サーバーへのパスワード、ホスト、グループのアップロード				✓	✓
指定した NAS サーバーのパスワードまたはホストの表示			✓		✓

タスク	オペレーター	VM 管理者	セキュリティ管理者	ストレージ管理者	管理者
ファイル システムの追加、または既存の NAS サーバーにある指定したファイル システムの変更や削除				✓	✓
指定したファイル システムに対するクローンやスナップショットの追加、指定したファイル システムの更新やリストア、または指定したファイル システムのクォータの更新				✓	✓
ファイル ツリー クォータの追加、または指定したファイル ツリー クォータの変更、削除、更新				✓	✓
ファイル ユーザー クォータの追加、または指定したファイル ユーザー クォータの変更、削除、更新				✓	✓
ファイル ウイルス チェッカーの追加、指定したファイル ウイルス チェッカーの変更、削除、または指定したファイル ウイルス チェッカー構成のアップロード					✓
指定したファイル ウイルス チェッカー構成のダウンロード			✓		✓
SMB や NFS サーバーの追加、または指定した SMB や NFS サーバーの変更、削除、参加、分離				✓	✓
SMB 共有の追加、または指定した SMB 共有の変更、削除				✓	✓
NFS エクスポートの追加、または指定した NFS エクスポートの変更、削除				✓	✓
ファイル インターフェイスの追加、または指定したファイル インターフェイスの変更、削除				✓	✓
ファイル インターフェイス ルートの追加、または指定したファイル インターフェイス ルートの変更、削除				✓	✓
ファイル DNS、ファイル FTP、ファイル Kerberos、ファイル LDAP、ファイル NDMP、ファイル NIS サーバーの追加、または指定したファイル DNS、ファイル FTP、ファイル Kerberos、ファイル LDAP、ファイル NDMP、ファイル NIS サーバーの変更、削除				✓	✓
ファイル Kerberos キータブのアップロード					✓
ファイル Kerberos キータブのダウンロード	✓		✓		✓
ファイル LDAP 構成または LDAP 証明書のアップロード					✓

タスク	オペレーター	VM 管理者	セキュリティ管理者	ストレージ管理者	管理者
ファイル LDAP 証明書のダウンロード			✓		✓

役割の権限に基づくユーザー アカウント管理

管理者またはセキュリティ管理者の役割を持つユーザーは、ユーザー アカウント管理に関して次の操作を実行できます。

- 新規ユーザー アカウントを作成する。
- 組み込みの管理者アカウント以外のすべてのユーザー アカウントを削除する。

  メモ: 組み込みの管理者アカウントは削除できません。
- 別のユーザーを任意の役割に変更する。
- 別のユーザーのパスワードをリセットする。
- 別のユーザー アカウントをロックするか、アンロックする。

  メモ: 管理者またはセキュリティ管理者の役割を持つログイン中のユーザーは、自分のアカウントをロックできません。

ログインしているユーザーは自分のユーザー アカウントを削除できません。また、セキュリティ管理者または管理者の役割を持つユーザーを除き、ログインしているユーザーは自分のパスワードのみを変更できます。ユーザーがパスワードを変更するには、自分の古いパスワードを入力する必要があります。ログインしているユーザーは、自分のパスワードのリセット、自分の役割の変更、さらに自分のアカウントのロックまたはアンロックはできません。

組み込みの管理者アカウント プロファイル (管理者の役割を持つ) は、編集することも、ロックすることもできません。

ユーザーの役割またはロックのステータスが変更されるとユーザーは削除されます。また、セキュリティ管理者または管理者によってパスワードが変更されると、そのユーザーに関連づけられているすべてのセッションは無効になります。

メモ: ユーザーがセッション内の自分のパスワードを更新した場合、セッションは有効のままになります。

管理者アカウントとサービス アカウントのパスワードのリセット

アプライアンスには、デフォルトの管理者ユーザー アカウントがあり、これにより初期構成を実行できます。また、デフォルトのサービス ユーザー アカウントも含まれており、これにより専門的なサービス機能を実行できます。REST API やコマンド ライン インターフェイス (CLI) などの別の方法ではなく、まず PowerStore Manager UI を使用して PowerStore を構成することを推奨します。PowerStore Manager UI を使用することで、すべてのデフォルトのパスワードが確実に変更されます。新しいパスワードを忘れた場合は、パスワードをデフォルト値にリセットできます。

これらのパスワードをリセットする方法は、アプライアンスが PowerStore T model と PowerStore X model のどちらであるかによって異なります。アプライアンスに対応する方法を使用して、管理者、サービス、またはその両方のパスワードをリセットします。

PowerStore T model アプライアンスでの管理者アカウント パスワードとサービス アカウント パスワードのデフォルト値へのリセット

このタスクについて

PowerStore T model アプライアンスの場合、管理者またはサービス ユーザーのパスワードをリセットする主な方法は、USB ドライブを使用することです。サポートされているファイルシステムには、FAT32 と ISO 9660 が含まれます。

メモ: アプライアンスがサービス モードになっているときにパスワードをリセットするには、次のように手順が 1 つ異なります。USB リセット プロセスを各ノードに適用します。このアクションでシステムが標準モードに戻り、PowerStore Manager へのログイン時に、管理者とサービス ユーザーの両方の新しいパスワードを入力するように求められます。

手順

1. USB ドライブがフォーマットされている場合は、次のステップに進みます。それ以外の場合は、 `format <d:> /FS:FAT32` などのコマンド プロンプトを使用してドライブをフォーマットします。

   ここで、`d:` は、ノートパソコンまたは PC に挿入された USB ドライブのドライブ レターです。

2. 次のコマンドでラベルを設定します。

```
label d:
RSTPWD
```

メモ: アプライアンスでは、RSTPWD ラベルのない USB ドライブはマウントされません。USB ドライブにラベルを付けた後、リセットするアカウント パスワード用の空のファイルを挿入します。管理者パスワード、サービス アカウント パスワード、またはその両方をリセットすることができます。

3. ドライブ上に空のファイルを作成するには、必要に応じて次のコマンドのいずれかまたは両方を使用します。

```
copy NUL d:\admin
copy NUL d:\service
```

4. アプライアンスのいずれかのノードの USB ポートに USB ドライブを挿入し、10 秒間待ってから取り外します。
これで、リセットした各アカウントのパスワードがデフォルト値になります。
5. クラスターの IP アドレスを使用して、ブラウザーを介してクラスターに接続し、デフォルトの初期パスワード (**Password123#**) を使用して管理者としてログインします。
管理者パスワード、サービス パスワード、またはその両方をリセットするプロンプトが表示されます。セキュア シェル (SSH) を使用してサービス パスワードをリセットする場合、サービス アカウントの初期デフォルト パスワードは **service** です。
6. デフォルトから、ユーザーが指定したパスワードに管理者パスワードを変更します。
7. 管理者パスワードとは異なるサービス アカウント　パスワードを設定する場合は、関連するチェックボックスをオフにします。

タスクの結果

この手順を実行した後も、ログイン試行時にパスワードのリセットを求められない場合は、サービス プロバイダーにお問い合わせください。

PowerStore X model アプライアンスでの管理者アカウント パスワードとサービス アカウント パスワードのデフォルト値へのリセット

前提条件

プライマリー アプライアンスのプライマリー ノード名 (たとえば、PSTX-44W1BW2-A および PowerStore D6013) を確認します。必要に応じて、reset.iso ファイルを生成します。

このタスクについて

PowerStore X model アプライアンスの場合は、ISO イメージを使用して vSphere からマウントします。事前に作成されたイメージ ファイルは www.dell.com/support からダウンロードできます。また、どのパスワードをリセットする必要があるかに応じて、次のタッチ コマンドのいずれかまたは両方を使用して、Linux システムから独自のイメージを作成することもできます。

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

メモ: vSphere から仮想 CD としてマウントするには、ISO イメージ、reset.iso がデータストアに存在している必要があります。

メモ: アプライアンスがサービス モードになっているときにパスワードをリセットするには、次のように手順が 2 つ異なります。パブリック データストアを使用できないため、まず、ISO イメージをコントローラー仮想マシン (VM) 自体の PRIVATE-C9P42W2.A.INTERNAL データストアにアップロードする必要があります。次に、reset.iso ファイルをアップロードして、コントローラー VM ノード A と B の両方に適用します。このアクションでシステムが標準モードに戻り、PowerStore Manager アクセスが利用可能になり、管理者とサービス ユーザーの両方の新しいパスワードを入力するように求められます。

手順

1. vSphere の **Storage** で、お使いの PowerStore X model アプライアンスを選択します。

例：**DataCenter-WX-D6013** > **PowerStore D6013**

2. **Files** で **ISOs** を選択します。
3. **Upload** を選択し、`reset.iso` ファイル（www.dell.com/support にある事前作成済みのイメージ ファイル、または Linux システムで自身で作成したイメージ ファイルのいずれか）をアップロードします。
`reset.iso` ファイルが **ISOs** フォルダーに表示されます。
4. vSphere の **Host and Clusters** で、クラスター内のプライマリー PowerStore X model アプライアンスのプライマリー ノードを選択します。

例：**DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. **Summary** で **CD/DVD drive 1** をクリックして、**Connect to datastore ISO file** を選択します。
Choose an ISO image to mount ウィンドウが表示されます。
6. **Datastores** でクラスター内のプライマリー PowerStore X model アプライアンスをクリックして、**ISOs** フォルダーを選択します。
`reset.iso` ファイルは **Contents** に表示されます。
7. `reset.iso` ファイルを選択し、**OK** をクリックします。
Summary の **CD/DVD drive 1** で約 10 秒 **Connected** と表示され、その後 **Disconnected** に変わります。クラスター管理者パスワードかサービス パスワード、またはその両方がデフォルトにリセットされます。
8. クラスターの IP アドレスを使用して、ブラウザーを介してクラスターに接続し、デフォルトの初期パスワード（**Password123#**）を使用して管理者としてログインします。
管理者パスワード、サービス パスワード、またはその両方をリセットするプロンプトが表示されます。SSH を使用してサービス パスワードをリセットする場合、サービス アカウントの初期デフォルト パスワードは **service** です。
9. デフォルトから、ユーザーが指定したパスワードに管理者パスワードを変更します。
10. 管理者パスワードとは異なるサービス アカウント　パスワードを設定する場合は、関連するチェックボックスをオフにします。

タスクの結果

この手順を実行した後も、ログイン試行時にパスワードのリセットを求められない場合は、サービス プロバイダーにお問い合わせください。

証明書

PowerStore の証明書ストア内のデータは永続的です。証明書ストアには、次のタイプの証明書が保存されます。

- CA（認証局）の証明書
- クライアント証明書
- サーバー証明書

証明書を表示する

このタスクについて

アプライアンスに保存されている各証明書について、PowerStore Manager に次の情報が表示されます。

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

メモ: 追加の証明書情報を表示するには、REST API または CLI を使用します。

証明書情報を表示するには、次の操作を実行します。

手順

1. PowerStore Manager を起動します。

2. **Settings** をクリックし、**Support** で **Certificates** をクリックします。
   アプライアンスに保存されている証明書に関する情報が表示されます。
3. 1 つの証明書を構成する一連の証明書とサービスの関連情報を表示するには、該当するサービスをクリックします。
   View Certificate Chain が表示され、証明書を構成する一連の証明書についての情報が一覧表示されます。

クラスター内の PowerStore アプライアンス間のセキュアな通信

クラスターの作成時に、クラスター マスター アプライアンスのプライマリー ノードは、クラスター CA とも呼ばれる認証局 (CA) 証明書を作成します。マスター アプライアンスによって、クラスター CA 証明書が、クラスターに参加するアプライアンスに渡されます。

クラスター内の各 PowerStore アプライアンスは、クラスター CA 証明書によって署名される固有の IPsec 証明書を生成します。PowerStore アプライアンスがそのクラスター ネットワーク上で送信する機密データは IPsec と TLS で保護されるため、データのセキュリティと整合性は確保されます。

レプリケーションとデータ インポートのためのセキュアな通信

PowerStore の証明書と認証情報インフラストラクチャにより、サーバーとクライアントの証明書およびユーザー資格情報の交換が可能になります。このプロセスには、以下が含まれます。

- TLS ハンドシェイク中のサーバー証明書の取得と検証
- リモート システムから認証情報ストアへの信頼済み CA 証明書の追加
- 認証情報ストアへの信頼済みサーバー/クライアント証明書の追加
- 信頼が確立された後の安全な接続の確立への支援

PowerStore は、次の証明書管理機能をサポートしています。

- レプリケーションについては、2 つの PowerStore クラスター間での証明書の交換による信頼済み管理通信の確立。PowerStore クラスター間のレプリケーションを容易にするために、クラスタ間に双方向信頼を確立して、レプリケーション REST 制御リクエストの発行時に双方向 TLS 認証が行われるようにする必要があります。
- データのインポートについては、証明書、およびデータ保全を備えた認証情報交換による、Dell EMC ストレージ システム (VNX、Unity、Storage Center (SC)、Peer Storage (PS) システム) と PowerStore クラスターの間で安全な接続の確立。

vSphere Storage API for Storage Awareness のサポート

vSphere Storage API for Storage Awareness (VASA) は、VMware が定義した、特定のベンダーに依存しないストレージ認識 API です。VASA プロバイダーは、着信 VASA API リクエストを処理するために協力して動作する複数のコンポーネントで構成されています。すべての着信 VASA API を受信する VASA API ゲートウェイは、PowerStore クラスター内のプライマリー アプライアンス (フローティング管理 IP を所有するもの) に導入されます。ESXi ホストおよび vCenter Server は、VASA プロバイダーに接続し、利用可能なストレージ トポロジー、機能、ステータスに関する情報を取得します。次に、vCenter Server は、この情報を vSphere クライアントに提供します。VASA は、PowerStore Manager クライアントではなく、VMware クライアントによって使用されます。

vSphere ユーザーは、この VASA プロバイダー インスタンスを、クラスターの VASA 情報のプロバイダーとして構成する必要があります。主要なアプライアンスがダウンした場合は、関連するプロセスが VASA プロバイダーとともに、次のプライマリーとなるアプライアンスで再開されます。IP アドレスは自動的にフェイルオーバーします。内部的には、新しくアクティブになった VASA プロバイダーからの構成の変更イベントをプロトコルが取得したときに、障害が認識されますが、これによってユーザー介入を必要とせずに VASA オブジェクトの自動再同期化が実行されます。

PowerStore は、vSphere 6.5 および 6.7 の VASA 3.0 インターフェイスを提供します。

VASA 3.0 は、Virtual Volumes (VVols) をサポートしています。VASA 3.0 は、VVols やストレージ コンテナなど、ストレージの抽象化にクエリーを実行するためのインターフェイスをサポートしています。この情報は、ストレージのポリシーベースの管理 (SPBM) で仮想ドライブの配置およびコンプライアンスに関する決定を行うために役立ちます。VASA 3.0 は、仮想ドライブのバックアップに使用される VVols のライフサイクルのプロビジョニングおよび管理を行うためのインターフェイスもサポートしています。こうしたインターフェイスは、VMware ESXi ホストによって直接起動されます。

VASA、vSphere、VVols の詳細については、VMware のドキュメントおよび PowerStore Manager オンライン ヘルプを参照してください。

VASA に関連する認証

vCenter から PowerStore Manager VASA プロバイダーへの接続を開始するには、vSphere クライアントを使用して、次の情報を入力します。

- VASA プロバイダーの URL。VASA 3.0 のフォーマット、https://<管理 IP アドレス>:8443/version.xml を使用します。
- PowerStore Manager ユーザー (役割が VM 管理者または管理者) のユーザー名。

  メモ: VM 管理者ロールは厳密に、証明書を登録する手段として使用されます。
- そのユーザーに関連づけられているパスワード。

ここで使用される PowerStore Manager 認証情報は、接続のこの最初のステップでのみ使用されます。PowerStore Manager 認証情報がターゲット クラスターに有効である場合は、vCenter Server の証明書が自動的にクラスターに登録されます。この証明書を使用して、vCenter からの以降のすべてのリクエストが認証されます。この証明書を VASA プロバイダーにインストールまたはアップロードするために手動の操作は必要ありません。この証明書が期限切れになった場合、新しいセッションをサポートするために vCenter で新しい証明書を登録する必要があります。証明書がユーザーによって取り消された場合、セッションは無効化され、接続は切断されます。

vCenter セッション、安全な接続と認証情報

vCenter セッションは、vSphere 管理者が vSphere クライアントを使用して、VASA プロバイダーの URL とログイン認証情報を vCenter Server に入力したときに開始されます。vCenter Server は、この URL、認証情報、VASA プロバイダーの SSL 証明書を使用して、VASA プロバイダーとの安全な接続を確立します。vCenter セッションは、次のいずれかのイベントが発生すると終了します。

- 管理者が vSphere クライアントを使用して、vCenter の構成から VASA プロバイダーを削除し、vCenter Server が接続を終了したとき。
- vCenter Server または vCenter Server サービスが失敗し、接続が終了したとき。vCenter または vCenter Server サービスが SSL 接続を再確立できない場合は、新しいサービスを起動します。
- VASA プロバイダーが失敗し、接続が終了したとき。VASA プロバイダーが開始すると、SSL 接続および VASA セッションを再確立するために、vCenter Server からの通信に応答できます。

vCenter セッションは、vCenter Server と VASA プロバイダーの間のセキュア HTTPS 通信を基にしています。VASA 3.0 では、vCenter Server が VMware 認証局 (VMCA) として動作します。VASA プロバイダーは、リクエストの許可後、リクエストに応じて自己署名された証明書を送信します。そして、VMCA 証明書をトラストストアに追加した後、証明書署名リクエストを発行し、自己署名された証明書を VMCA 署名証明書にリプレースします。以降の接続は、以前に登録したルート署名証明書と照合して確認されたクライアントの Storage Monitoring Service (SMS) 証明書を使用して VASA プロバイダーによって認証されます。VASA プロバイダーは、ストレージ エンティティー オブジェクトの一意の識別子を生成し、vCenter Server は、この識別子を使用して、特定のエンティティーのデータをリクエストします。

VASA プロバイダーは、VASA セッションを確認するために SSL 証明書および VASA セッション識別子を使用します。セッションの確立後、VASA プロバイダーは vCenter Server からの各関数呼び出しに関連づけられた SSL 証明書および VASA セッション識別子の両方を確認する必要があります。VASA プロバイダーは、そのトラストストアに格納された VMCA 証明書を使用して、vCenter SMS からの関数呼び出しに関連づけられた証明書を確認します。VASA セッションは、複数の SSL 接続間で継続されます。SSL 接続がドロップすると、vCenter Server は同じ VASA セッションのコンテキストで SSL 接続を再確立するために VASA プロバイダーに対して SSL ハンドシェイクを実行します。SSL 証明書の有効期限が切れた場合、vSphere 管理者は新しい証明書を生成する必要があります。vCenter Server は新しい SSL 接続を確立し、VASA プロバイダーに新しい証明書を登録します。

注意: SMS は、3.0 VASA プロバイダーに対して `unregisterVASACertificate` 関数を呼び出しません。したがって、登録解除した後でも、VASA プロバイダーは SMS から取得した VMCA 署名済み証明書を引き続き使用できます。

CHAP 認証

チャレンジ ハンドシェイク認証プロトコル (CHAP) は、iSCSI イニシエーター (ホスト) とターゲット (ボリュームとスナップショット) を認証する方法です。CHAP では、iSCSI ストレージが公開され、セキュアな標準ストレージ プロトコルが確保されます。認証は、パスワードと同様に、認証システムとピアの両方が知っているシークレットを使用して行われます。CHAP プロトコルには、次の 2 つのタイプがあります。

- 単方向 CHAP 認証では、iSCSI ターゲットがイニシエーターを認証できます。イニシエーターは、(標準モードまたは検出モードにより) ターゲットに接続しようとする際に、ユーザー名とパスワードをターゲットに提供します。

- 双方向 CHAP 認証は、単方向 CHAP に加えて適用されます。双方向 CHAP では、iSCSI ターゲットとイニシエーターが相互に認証を行うことができます。グループによって示される各 iSCSI ターゲットは、iSCSI イニシエーターによって認証されます。イニシエーターがターゲットに接続しようとする際に、ターゲットは、ユーザー名とパスワードをイニシエーターに提供します。イニシエーターは、提供されたユーザー名とパスワードを、自身が持つ情報と比較します。情報が一致した場合は、イニシエーターがターゲットに接続できます。

メモ: 環境内で CHAP を使用する場合は、CHAP 認証をセットアップして有効にしてから、データを受信するボリュームを準備することをお勧めします。CHAP 認証を設定して有効化する前にデータを受信するようにドライブを準備すると、ボリュームへのアクセスが失われる可能性があります。

PowerStore は iSCSI CHAP 検出モードをサポートしていません。次の表は iSCSI CHAP 検出モードに関連する PowerStore の制限事項を示しています。

表 1. iSCSI CHAP 検出モードの制限事項

CHAP モード	シングル モード (イニシエーターが有効)	相互モード (イニシエーターとターゲットが有効)
検出	PowerStore はホストの認証 (チャレンジ) を行いません。認証を使用してターゲットの検出を妨げることはできません。これによって、ユーザー データへの意図しないアクセスが発生することはありません。	PowerStore はホストからの認証リクエスト (チャレンジ) には応答せず、ホストが PowerStore にチャレンジする場合、検出は失敗します。
標準	予期したとおりに作動します。認証情報は PowerStore によりテストされます。	予期したとおりに作動します。認証情報は PowerStore により転送されます。

ソースとターゲットのアプライアンス間のリモート レプリケーションでは、検証と更新のプロセスによって、ローカル システムとリモート システムでの変更が検出され、データ接続が再確立されます。このとき、CHAP 設定も考慮されます。

CHAP を構成する

PowerStore クラスターでは、CHAP の単方向 (イニシエーターが有効) 認証または双方向 (イニシエーターとターゲット) 認証を有効にすることができます。CHAP は、1 つのアプライアンスまたは複数 PowerStore アプライアンスと外部ホストのクラスター実装に対して有効にすることができます。

単方向認証が有効である場合、外部ホストが追加されるときに、各イニシエーターのユーザー名とパスワードの入力が必要になります。双方向認証が有効である場合は、クラスターのユーザー名とパスワードの入力も必要になります。ホストを追加し、CHAP を有効にしてイニシエーターを追加する場合、イニシエーターのパスワードは一意である必要があります。同じホストの複数のイニシエーターに同じパスワードを使用することはできません。外部ホストの CHAP 構成の構成方法の詳細は、状況により異なります。この機能を使用するには、ホストのオペレーティング システムと、その構成方法を熟知している必要があります。

メモ: システムでホストが構成された後に CHAP を有効にすると、外部ホストが停止する結果となります。外部ホストとアプライアンスの両方で構成が設定されるまで、I/O の中断が発生します。CHAP 構成を実装する場合は、CHAP 構成タイプを決定してから、外部ホストをアプライアンスに追加することをお勧めします。

ホストを追加した後に CHAP を有効化する場合は、各ホストのイニシエーターを更新します。CHAP が有効である場合は、CHAP 認証情報がないホスト グループにホストを追加することはできません。CHAP を有効にし、後でホストを追加する場合は、PowerStore Manager でホストを手動で登録 (**Compute** で **Hosts & Host Groups** を選択) します。認証を使用するには、iSCSI レベルで認証情報を入力する必要があります。この場合は、ホストから IQN をコピーしてから、各イニシエーターの関連 CHAP 認証情報を追加します。

次のいずれかの方法を使用してクラスターの CHAP を構成します。

- **CHAP**：PowerStore Manager から設定ページにアクセスします (**Settings** をクリックし、**Security** で **CHAP** を選択)。
- REST API サーバー：アプリケーション インターフェイスで、CHAP の設定を構成するための REST API リクエストを受け取ります。REST API の詳細については、*PowerStore REST API Reference Guide* を参照してください。

CHAP のステータスを特定するには、PowerStore Manager で **Settings** をクリックし、**Security** で **CHAP** を選択します。

外部 SSH アクセス

各アプライアンスはオプションで、アプライアンスの IP アドレスの SSH ポートに外部セキュア シェル (SSH) がアクセスできるようにすることができます。これにより、ユーザーは、アプライアンスのプライマリー ノードのサービス機能を使用できます。アプ

ライアンスの IP アドレスは、プライマリー指定の変更に従って、アプライアンスの 2 つのノード間でフローティングします。外部 SSH が無効化されている場合、SSH アクセスは許可されません。

アプライアンスが最初に起動し、構成されていない際は、SSH はデフォルトで有効になります。これにより、アプライアンスは、クラスターに追加される前に問題が発生した場合でもサービスを実行できるようになります。新しいクラスターが作成された場合、またはクラスターへの参加操作では、すべてのアプライアンスで SSH の初期設定が無効である必要があります。

外部 SSH アクセスの構成

次のいずれかの方法を使用して、クラスター内のアプライアンスへの外部 SSH アクセスを構成します。

- **SSH Management**：PowerStore Manager からアクセスできる SSH 設定ページ（**Settings** をクリックし、**Security** で **SSH Management** を選択）。
- REST API サーバー：アプリケーション インターフェイスで、SSH の設定を構成するための REST API リクエストを受け取ります。REST API の詳細については、*PowerStore REST API Reference Guide* を参照してください。
- `svc_service_config` - アプライアンスにサービス ユーザーとして直接入力できるサービスコマンド。このコマンドの詳細については、*PowerStore Service Scripts Guide* を参照してください。

クラスター内のアプライアンスでの SSH のステータスを特定するには、PowerStore Manager で **Settings** をクリックし、**Security** で **SSH Management** を選択します。選択した 1 つまたは複数のアプライアンスで SSH を有効にしたり、無効にしたりすることもできます。

SSH サービスが正常に有効化されたら、任意の SSH クライアントを使用してアプライアンスの IP アドレスにログインします。アプライアンスにアクセスするには、サービス ユーザーの認証情報が必要です。

サービス アカウントを使用して、ユーザーは次の機能を実行できます。

- アプライアンス システムの設定とオペレーションを監視およびトラブルシューティングするためにアプライアンス サービス スクリプトを実行します。
- 制限付きシェル モードでは、特権のない Linux ユーザー アカウントのメンバーとして割り当てられた、限定セットのコマンドのみを操作します。このアカウントには、専用のシステム ファイル、構成ファイル、ユーザー/お客様データなどに対するアクセス権はありません。

アプライアンスのセキュリティを最大限に高めるために、外部 SSH サービス インターフェイスは、アプライアンスで特に実行しなければならないサービス操作がある場合を除き、常に無効にしておくことをお勧めします。必要なサービス操作を実行したら、SSH インターフェイスを無効にして、アプライアンスの安全性を確保します。

SSH セッション

PowerStore SSH サービス インタフェイス セッションは、SSH クライアントによって確立された設定に基づいて維持されます。セッションの特性は、SSH クライアント構成設定によって決まります。

サービス アカウントのパスワード

サービス アカウントは、基本的な Linux コマンドを実行するためにサービス担当者が使用できるアカウントです。

アプライアンスの初期構成時に、デフォルトのサービス パスワードを変更する必要があります。サービス パスワードへの制限事項は、システム管理アカウントに適用される制限事項と同じです（ユーザー名とパスワードの使用 、p. 7 を参照）。

SSH 認証

サービス アカウント認証は、次のものに基づいています。

- アプリケーション分離：PowerStore ソフトウェアは、アプリケーション分離を提供するコンテナー テクノロジーを使用します。サービス コンテナーはアプライアンス サービスへのアクセスを提供し、サービス スクリプトのセットと Linux コマンドのセットのみを使用できます。サービス アカウントには、ファイル システムを提供しユーザーへの I/O をブロックする他のコンテナーにアクセスする機能はありません。
- Linux ファイル システムの権限：ほとんどの Linux ツールとユーティリティーは、何らかの方法でシステム オペレーションを変更するものであり、サービス ユーザーに対しては使用できません。これには、スーパーユーザー アカウントの権限が必要です。サービス アカウントにはこれらの権限がないため、サービス アカウントでは、実行に必要なアクセス権限がない Linux のツールやユーティリティの使用や、読み取りや変更に root アクセスを必要とする構成ファイルの編集はできません。

- アクセス制御：コンテナー テクノロジーによって提供されるアプリケーション分離に加えて、アプライアンス上のアクセス制御リスト（ACL）メカニズムでは、サービス アカウントによるシステム リソースへのアクセスを明示的に許可または拒否する、非常に特殊なルールのリストを使用します。標準の Linux ファイル システム権限によって定義されない、アプライアンスの他の領域に対するサービス アカウント権限は、これらの規則によって指定されます。

アプライアンス サービス スクリプト

アプライアンスのソフトウェア バージョンには、問題の診断、システム構成、システム リカバリーに関する一連のスクリプトがインストールされています。これらのスクリプトを使用すると、PowerStore Manager を使用した場合よりも、さらに詳しい情報を収集し、より深いレベルのシステム制御を行うことができます。*PowerStore Service Scripts Guide* では、これらのスクリプトとその一般的な使用例について説明します。

アプライアンス ノード Ethernet サービス ポートと IPMItool

ご使用のアプライアンスは、各ノードの Ethernet サービス ポートを介したコンソール アクセスを提供します。このアクセスには、IPMItool を使用する必要があります。IPMItool は、SSH や Telnet に似たネットワーク ツールであり、IPMI プロトコルを使用して、Ethernet 接続を介した各ノードとのインターフェイスを確立します。IPMItool は、アプライアンスのノード コンソールにアクセスするための安全な通信チャネルをネゴシエートする Windows ユーティリティーです。このユーティリティーでは、コンソールをアクティブ化するために物理アクセスが必要です。

ノード Ethernet サービス ポート インターフェイスでは、サービス SSH インターフェイス（サービス LAN インターフェイス）と同じ機能が提供され、同じ制限が適用されます。ただし、ユーザーはインターフェイスにアクセスするために、SSH クライアントではなく Ethernet ポート接続を使用します。このインターフェイスはフィールド サービス担当者向けに設計されており、ネットワークを妨害することなくアプライアンスに接続できます。専用の管理コンソールは必要ありません。

このインターフェイスは、直接的なポイントツーポイントでルーティング不可能な接続を提供します。サービス担当者は、コンソールの出力にサービス LAN インターフェイスを使用して、PowerStore サービス コンテナーと PowerStore Manager（ICW（初期構成ウィザード）を含む）に SSH アクセスできます。サービス LAN インターフェイスを介したサービス コンテナーへの SSH アクセスは常に有効であり、無効にすることはできません。ただし、サービス アカウントの認証情報は管理できます。

サービス スクリプトのリストについては、*PowerStore Service Scripts Guide* を参照してください。

NFS セキュア

NFS セキュアでは、NFSv3 および NFSv4 でユーザーを認証するために Kerberos を使用します。Kerberos は、整合性（署名）とプライバシー（暗号化）を提供します。整合性とプライバシーは有効化に必須ではなく、NFS のエクスポート オプションです。

Kerberos を使用しない場合、サーバーはユーザー認証についてクライアントに全く依存することになります。サーバーはクライアントを信頼します。Kerberos を使用する場合、サーバーは KDC（キー配布センター）を信頼します。KDC は、認証を処理し、アカウント（プリンシパル）とパスワードを管理します。さらに、パスワードが送信されることもありません。

Kerberos を使用しない場合、ユーザーの認証情報が暗号化されずに送信されるため、簡単になりすましの被害に遭います。Kerberos を使用すると、ユーザーの ID（プリンシパル）は暗号化された Kerberos のチケットに含まれ、それを読み取れるのはターゲット サーバーと KDC だけです。暗号化キーを知ることができるのは、ここだけです。

NFS セキュアに関連して、Kerberos では AES128 および AES256 暗号化がサポートされます。NFS セキュアとともに、SMB と LDAP にインパクトを与えます。これらの暗号化は、Windows および Linux でデフォルトでサポートされています。これらの新しい暗号化は非常に安全ですが、それを使用するかどうかはクライアントにかかっています。サーバーはそのユーザー プリンシパルからアクティブ Unix ディレクトリー サービス（UDS）をクエリーして、ユーザーの認証情報を構築します。NIS はセキュアでないため、NFS セキュアと使用することは推奨されません。Kerberos は LDAP または LDAPS と併用することが勧められています。

NFS セキュアは、PowerStore Manager を使用して構成できます。

ファイル プロトコルの関係

Kerberos を使用するには、次が必要です。

- DNS：IP アドレスの代わりに DNS 名を使用する必要があります。
- NTP：PowerStore には NTP サーバーが構成されている必要があります。

  メモ: Kerberos を使用するには、ネットワークで KDC、サーバー、クライアントの時刻が正確に同期されている必要があります。

- UDS：認証情報の構築用。
- ホスト名：Kerberos は、IP アドレスではなく、名前を使用します。

NFS では、ホスト名の値に応じて、1 つまたは 2 つのサービス プリンシパル名（SPN）を使用します。ホスト名が完全修飾ドメイン名形式である host.domain の場合：

- 短い SPN：**nfs/host@REALM**
- 長い SPN：**nfs/host.domainFQDN@REALM**

ホスト名が完全修飾ドメイン名形式でない場合、短い SPN のみが使用されます。

SMB と同様に、SMB サーバーをドメインに結合できるように、NFS サーバーをレルム（Kerberos でドメインに相当）に結合することができます。これには 2 つのオプションがあります。

- 構成された Windows ドメインがある場合はそれを使用します
- UNIX KDC ベースの Kerberos レルムを全部構成します

管理者が、構成された Windows ドメインを使用するよう選択した場合、ほかに行うことはありません。NFS サービスで使用されるすべての SPN は、SMB サーバーの参加/参加解除時に、KDC に自動的に追加/削除されます。NFS セキュアが SMB 構成を使用するよう構成されている場合、SMB サーバーは破棄できないことにご注意ください。

管理者が、UNIX ベースの Kerberos レルムを使用するよう選択した場合、さらに構成する必要があります。

- レルム名：Kerberos レルムの名前で、一般にすべて大文字です。
- UNIX KDC ベースの Kerberos レルムを全部構成します。

クライアントが特定のセキュリティで NFS エクスポートをマウントできるよう、セキュリティ パラメーター（sec）が提供されており、どの最小限のセキュリティが許可されているかを示します。セキュリティには 4 種類のあります。

- `AUTH_SYS`：標準的な従来のセキュリティです。Kerberos を使用しません。サーバーはクライアントが提供する認証情報を信頼します。
- `KRB5`：Kerberos v5 を使用した認証
- `KRB5i`：Kerberos の認証および整合性（署名）
- `KRB5p`：Kerberos の認証および整合性とプライバシー（暗号化）

NFS クライアントが、構成されている最小限のセキュリティを下回っているセキュリティでエクスポートをマウントした場合、アクセスは拒否されます。たとえば、最小限のアクセスが `KRB5i` の場合、`AUTH_SYS` または `KRB5` を使用したマウントはすべて拒否されます。

認証情報の作成

ユーザーがシステムに接続すると、そのシステムのプリンシパルである **user@REALM** のみが表示されます。これは、Kerberos チケットから抽出されています。`AUTH_SYS` セキュリティとは異なり、認証情報は NFS リクエストに含まれません。プリンシパルからユーザーの部分（@の前）が抽出され、対応する UID の UDS を検索するために使用されます。その UID から、システムはアクティブ UDS を使って認証情報を作成します。これは拡張 NFS 認証情報が有効な場合と同様です（例外は、Kerberos がない場合、UID はリクエストによって直接提供されます）。

プリンシパルが UDS でマッピングされていない場合、構成されたデフォルト UNIX ユーザーの認証情報が代わりに使用されます。デフォルト UNIX ユーザーが設定されていない場合、使用される認証情報は nobody のものとなります。

ファイル システム オブジェクトに対するセキュリティ

マルチプロトコル環境では、セキュリティ ポリシーはファイル システム レベルで設定されて、ファイル システムごとに独立しています。各ファイル システムはアクセス ポリシーを使用して、NFS と SMB との間のアクセス制御セマンティックの違いを解決する方法を判別します。アクセス ポリシーを選択することで、特定のファイル システムでファイル セキュリティを適用するために使用するメカニズムが決定します。

メモ: ご自分の環境で古い SMB1 プロトコルをサポートする必要がある場合、`svc_nas_cifssupport` サービス コマンドを使用して有効にできます。このサービス コマンドの詳細については、*PowerStore Service Scripts Guide* を参照してください。

UNIX セキュリティ モデル

UNIX ポリシーを選択した場合、SMB プロトコルからのファイル レベル セキュリティの変更、ACL（アクセス制御リスト）への変更の試行は無視されます。UNIX のアクセス権は、ファイルシステム オブジェクトのモード ビットまたは NFSv4 ACL と呼ばれます。モード ビットは、ビット文字列で表されます。各ビットは、ファイルを所有するユーザー、ファイル システム オブジェクトに

関連づけられているグループ、その他のすべてのユーザーに許可されているアクセス モードまたは権限を表します。UNIX のモード ビットは、ユーザーのカテゴリー (ユーザー、グループ、その他) ごとに連結された 3 文字 rwx (読み取り、書き込み、実行) の 3 個のセットとして表されます。ACL は、サービスへのアクセスの許可や拒否を制御するためのユーザーとユーザー グループのリストです。

Windows セキュリティ モデル

Windows セキュリティ モデルは、SD (セキュリティ ディスクリプター) およびその ACL の使用を含み、主にオブジェクト権限単位に基づきます。SMB ポリシーを選択した場合、NFS プロトコルのモード ビットに対する変更は無視されます。

ファイル システム オブジェクトへのアクセスは、権限がセキュリティ ディスクリプターを使用して許可または拒否に設定されているかどうかにより異なります。SD は、オブジェクトの所有者とグループ SID、その ACL を記述します。ACL は、各オブジェクトのセキュリティ ディスクリプターの一部です。各 ACL には、ACE (アクセス制御エントリー) が含まれます。各 ACE には、ユーザー、グループ、コンピューターを示す単一 SID、その SID で拒否または許可されている権限のリストが含まれます。

マルチプロトコル環境のファイル システム アクセス

ファイル アクセスは NAS サーバーを使用して提供されます。NAS サーバには、データが格納される一連のファイル システムが含まれます。NAS サーバでは、SMB 共有および NFS 共有を使用してファイル システムを共有することによって、NFS、SMB ファイル プロトコルのこのデータへのアクセスを提供します。マルチプロトコル共有の NAS サーバ モードでは、SMB と NFS 間の同じデータの共有が可能です。マルチプロトコル共有モードではファイル システムへの同時 SMB および NFS アクセスを提供するため、Windows ユーザーの UNIX ユーザーへのマッピング、使用するセキュリティ ルール (モード ビット、ACL、ユーザー資格情報) の定義を考慮に入れ、マルチプロトコル共有用に適切に構成する必要があります。

メモ: マルチプロトコル共有、ユーザー マッピング、アクセス ポリシー、ユーザー資格情報に関する NAS サーバーの構成および管理については、PowerStore Manager オンライン ヘルプを参照してください。

ユーザー マッピング

マルチプロトコル コンテキストでは、Windows ユーザーは UNIX ユーザーと一致する必要があります。ただし、UNIX ユーザーを Windows ユーザーにマッピングする必要があるのは、アクセス ポリシーが Windows である場合のみです。この一致が必要なのは、プロトコルに対してネイティブでない場合でも、ファイル システムのセキュリティを適用させるためです。ユーザー マッピングには次のコンポーネントが必要です。

- UNIX ディレクトリ サービスまたはローカル ファイル、もしくはその両方
- Windows リゾルバー
- secmap(セキュア マッピング): SID と NAS サーバーによって使用される UID または GID との間のすべてのマッピングを格納するキャッシュです。
- ntxmap

メモ: ユーザー マッピングは、SMB サーバーのローカルのユーザーまたはグループには影響しません。

UNIX ディレクトリ サービスとローカル ファイル

UDS (UNIX ディレクトリ サービス) とローカル ファイルを使用して、以下が行われます。

- 特定の UID (ユーザー識別子) の場合、対応する UNIX アカウント名を返す。
- 特定の UNIX アカウント名の場合、応する UID およびプライマリ GID (グループ識別子) を返す。

サポートされるサービスとは、次のとおりです。

- LDAP
- NIS
- ローカル ファイル
- なし (考えられるマッピングは、デフォルトのユーザーを介したものだけです)

マルチプロトコル共有が有効のときは、NAS サーバーに対して、1 つの UDS を有効にするか、ローカル ファイルを有効にするか、またはローカル ファイルと UDS の両方を有効にする必要があります。NAS サーバーの Unix ディレクトリー サービスのプロパティによって、ユーザー マッピングにどれを使用するかが決定します。

Windows リゾルバー

Windows リゾルバーを使用して、ユーザー マッピングを行うために次を行います。

- 特定の SID (セキュリティ識別子) の場合、対応する Windows アカウント名を返す
- 特定の Windows アカウント名の場合、対応する SID を返す

Windows リゾルバーは次のとおりです。

- ドメインの DC (ドメイン コントローラー)
- SMB サーバーの LGDB (ローカル グループ データベース)

secmap

secmap の機能は、すべての SID から UID/プライマリー GID、UID から SID へのマッピングを格納し、NAS サーバーのすべてのファイル システムで一貫性を保ちます。

ntxmap

名前が異なる場合、ntxmap を使用して、Windows アカウントを UNIX アカウントに関連づけます。たとえば、Windows 上で Gerald というアカウントを持つユーザーが、UNIX 上のアカウントでは Gerry という場合、ntxmap を使用して両者間の関連づけを作成します。

SID から UID、プライマリ GID マッピング

次の手順は、SID から UID への、プライマリ GID マッピングの解決に使用するプロセスです。

1. secmap で SID が検索されます。SID が見つかった場合は、UID と GID のマッピングが解決されます。
2. secmap で SID が見つからない場合は、SID に関連する Windows の名前を見つける必要があります。
   a. NAS の SMB サーバーのローカル グループのデータベースで、SID が検索されます。SID が見つかった場合、関連する Windows の名前は SMB サーバー名とローカル ユーザー名です。
   b. ローカル グループ データベースで SID が見つからない場合は、ドメインの DC が検索されます。SID が見つかった場合、関連する Windows の名前がユーザー名です。SID を解決できない場合、アクセスは拒否されます。
3. Windows 名は UNIX 名に変換されます。ntxmap は、この目的のために使用されます。
   a. Windows の名前が ntxmap で見つかった場合、エントリは UNIX の名前として使用されます。
   b. ntxmap で Windows の名前が見つからない場合、Windows の名前が UNIX の名前として使用されます。
4. UDS (NIS サーバー、LDAP サーバー、またはローカル ファイル) は、UNIX の名前を使用して検索されます。
   a. UDS で UNIX のユーザー名が見つかった場合は、UID と GID のマッピングが解決されます。
   b. UNIX 名が見つからないが、割り当てが解除された Windows アカウントの自動マッピング機能が有効になっている場合、UID は自動的に割り当てられます。
   c. UDS で UNIX のユーザー名が見つからないのに、デフォルトの UNIX アカウントが存在する場合は、UID と GID のマッピングは、そのデフォルトの UNIX アカウントのものに対して解決されます。
   d. SID を解決できない場合、アクセスは拒否されます。

マッピングが見つかった場合は、永続的な Secmap データベースに追加されます。マッピングが見つからない場合は、失敗したマッピングが永続的な secmap データベースに追加されます。

次の図は、SID から UID へのプライマリ GID マッピングの解決に使用するプロセスを表しています。

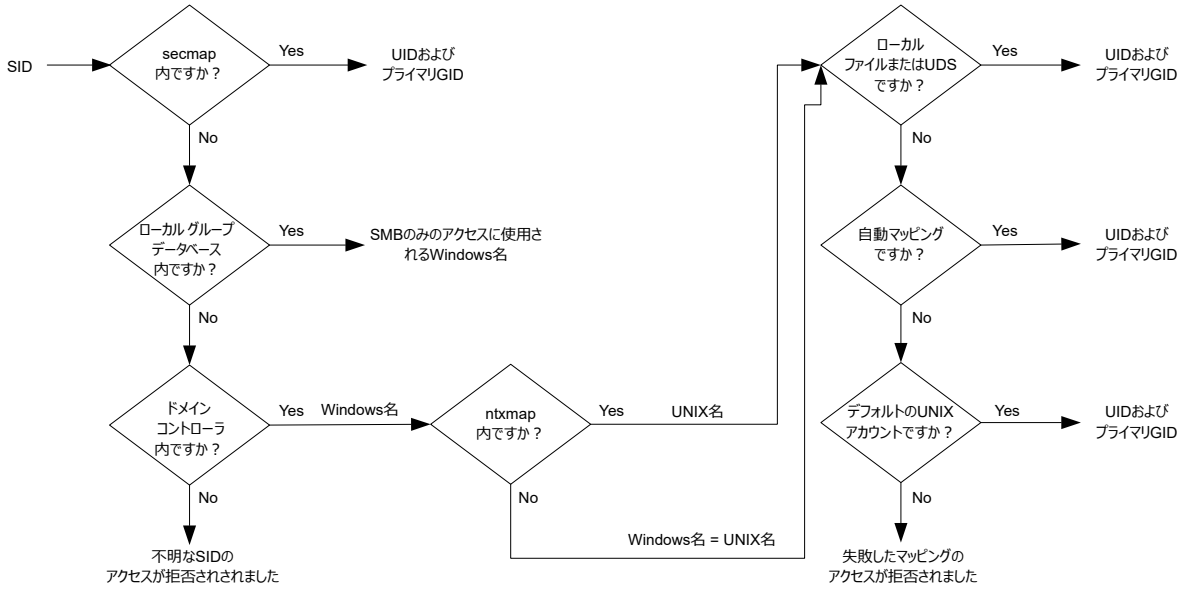

図 1. SID から UID へのプライマリ GID マッピングを解決するためのプロセス

UID から SID へのマッピング

次の手順は、UID から SID へのマッピングの解決に使用するプロセスです。

1. secmap で、UID が検索されます。UID が見つかった場合、SID マッピングが解決されます。
2. secmap で UID が見つからない場合は、UID に関連する UNIX の名前を見つける必要があります。
   a. UDS (NIS サーバー、LDAP サーバー、またはローカル ファイル) は、UID を使用して検索されます。UID が見つかった場合、関連する UNIX の名前がユーザー名です。
   b. UDS で UID は見つからないが、デフォルトの Windows アカウントがある場合、UID はデフォルト Windows アカウントの SID にマッピングされます。
3. デフォルトの Windows アカウント情報を使用しない場合、UNIX の名前が Windows の名前に変換されます。ntxmap は、この目的のために使用されます。
   a. UNIX の名前が ntxmap で見つかった場合、エントリーは Windows の名前として使用されます。
   b. UNIX の名前が ntxmap で見つからない場合、UNIX 名は Windows の名前として使用されます。
4. Windows DC またはローカル グループ データベースは、Windows の名前を使用して検索されます。
   a. Windows 名が見つかった場合、SID マッピングが解決されます。
   b. Windows の名前にピリオドが使われている場合に、最後のピリオド (.) に続く名前の一部が SMB サーバー名と一致していると、SMB サーバーのローカル グループ データベースが SID マッピングの解決のために検索されます。
   c. Windows 名は見つからないが、デフォルトの Windows アカウントがある場合、SID はデフォルトの Windows アカウントのものにマッピングされます。
   d. SID を解決できない場合、アクセスは拒否されます。

マッピングが見つかった場合は、永続的な Secmap データベースに追加されます。マッピングが見つからない場合は、失敗したマッピングが永続的な secmap データベースに追加されます。

次の図は、UID から SID へのマッピングの解決に使用するプロセスを表しています。

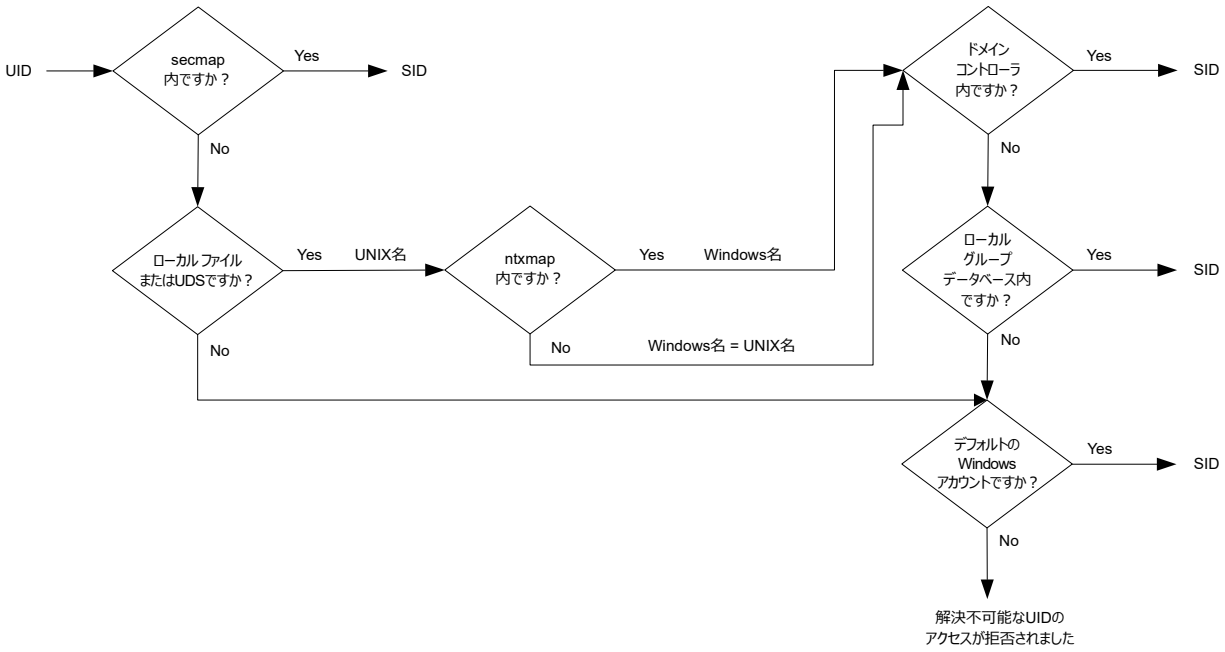

図 2. UID から SID へのマッピングの解決に使用されるプロセス

NFS、SMB、FTP のアクセス ポリシー

マルチプロトコル環境では、ストレージ システムがファイル システムのアクセス ポリシーを使用して、そのファイル システムのユーザー アクセス制御を管理します。UNIX と Windows の 2 種類のセキュリティがあります。

UNIX セキュリティ認証の場合、認証情報は、非 Secure NFS アクセスの例外を使用して UDS (UNIX ディレクトリ サービス) から作成されます。この認証情報はホスト クライアントから提供されます。ユーザー権限はモード ビットと NFSv4 ACL から判断されます。ユーザーおよびグループの識別子 (それぞれ、UID、GID) が ID に使用されます。UNIX セキュリティに関連づいた権限はありません。

Windows セキュリティ認証の場合、認証情報は Windows の DC (ドメイン コントローラー) および SMB サーバーの LGDB (ローカル グループ データベース) から作成されます。ユーザー権限は SMB ACL から判断されます。SID (セキュリティ識別子) は ID に使用されます。SMB サーバーの LGDB または GPO (グループ ポリシー オブジェクト) によって許可される、Windows セキュリティに関連した、所有権の取得、バックアップ、リストアなどの権限があります。

次の表に、どのプロトコルでどのようなセキュリティを使用するかを定義する、アクセス ポリシーについて説明します。

アクセス ポリシー	説明
native (デフォルト)	• 各プロトコルは独自のネイティブ セキュリティによりアクセスを管理します。 • NFS 共有のセキュリティでは、リクエストに関連づけられた UNIX 認証情報を使用し、NFSv3 UNIX モード ビットまたは NFSv4 ACL をチェックします。次に、アクセスが許可または拒否されます。 • SMB 共有のセキュリティでは、リクエストに関連づけられた Windows 認証情報を使用し、SMB ACL をチェックします。次に、アクセスが許可または拒否されます。 • NFSv3 UNIX モード ビットと NFSv4 ACL の権限の変更は、互いに同期されます。 • UNIX と Windows の権限の間で同期することはありません。
Windows	• Windows セキュリティを使用して、Windows および UNIX に対するファイル レベル アクセスのセキュリティを保護します。 • Windows 認証情報を使用して SMB ACL をチェックします。 • 新しく作成したファイルの権限は SMB ACL 変換によって決定されます。SMB ACL 権限の変更は、NFSv3 UNIX モード ビットまたは NFSv4 ACL に同期されます。 • NFSv3 モード ビットおよび NFSv4 ACL の権限の変更は拒否されます。
UNIX	• UNIX セキュリティを使用して、Windows と UNIX に対してファイル レベルのアクセスを保護します。 • SMB アクセスの要求に応じて、ローカル ファイルまたは UDS から作成された UNIX 認証情報が使用され、NFSv3 モード ビットまたは NFSv4 ACL で権限を確認します。 • 新しく作成したファイルの権限は UMASK によって決定されます。 • NFSv3 UNIX モード ビットまたは NFSv4 ACL の権限の変更は、SMB ACL に同期されます。 • SMB ACL 権限の変更は、システム停止が発生しないようにするために可能ですが、これらの権限は保持されません。

FTP では、Windows または UNIX での認証は、NAS サーバーへの認証時に使用されるユーザー名の形式に依存します。Windows 認証が使用されている場合、FTP アクセス制御は SMB の場合と似ています。それ以外は NFS の場合と似ています。FTP と SFTP クライアントは、NAS サーバーに接続すると認証されます。SMB 認証 (ユーザー名の形式が `domain\user` または `user@domain`) または UNIX 認証 (他の単一ユーザー名の形式) の場合があります。SMB 認証は、NAS サーバーで定義されたドメインの Windows DC で保証されています。UNIX 認証は、リモート LDAP サーバー上、リモート NIS サーバー上、または NAS サーバーのローカル パスワード ファイル内に格納されている暗号化されたパスワードに従って NAS サーバーで保証されています。

ファイル レベル セキュリティの認証情報

ファイル レベルのセキュリティを適用するには、処理されている SMB または NFS リクエストに関連づけられた認証情報をストレージ システムで作成する必要があります。Windows と UNIX の 2 種類の認証情報があります。次の用途の場合、Windows と UNIX の認証情報は NAS サーバーで作成されます。

- NFS リクエストに対し 16 個を超えるグループを使用して UNIX 認証情報を作成する場合。NAS サーバーの拡張された認証情報のプロパティは、この機能を提供するために設定する必要があります。
- ファイル システムのアクセス ポリシーが UNIX のときに、SMB リクエストに対して UNIX 認証情報を作成する場合。
- SMB リクエストに対し Windows 資格情報を作成する場合。
- ファイル システムのアクセス ポリシーが Windows のときに、NFS リクエストに対して Windows 認証情報を作成する場合。

メモ: 拡張された認証情報のプロパティが設定されていないときの NFS リクエストに対しては、NFS リクエストから UNIX 認証情報が使用されます。SMB リクエストに対して Kerberos 認証を使用するときは、ドメイン ユーザーの Windows 認証情報がセッション構成リクエストの Kerberos チケットに組み入れられます。

永続認証情報キャッシュは次のために使用されます。

- Windows アクセス ポリシーを持つファイル システムにアクセスするために作成された Windows 認証情報。
- 拡張認証情報オプションが有効な場合に NFS をとおしてアクセスするために作成された UNIX 認証情報。

NAS サーバーごとにキャッシュ インスタンスが 1 個あります。

マッピング解除されたユーザーへのアクセスの許可

マルチプロトコルは、次の要件を満たす必要があります。

- Windows ユーザーが UNIX ユーザーにマップされていること。
- Windows アクセス ポリシーを持つファイル システムにユーザーがアクセスしているときに Windows 認証情報を作成するため、UNIX ユーザーが Windows ユーザーにマップされていること。

2 つのプロパティは、次の未割り当てのユーザーに関して NAS サーバーに関連付けられています。

- デフォルト UNIX ユーザー。
- デフォルト Windows ユーザー。

未割り当ての Windows ユーザーがマルチプロトコル ファイル システムへの接続を試行した場合に、NAS サーバーに対してデフォルトの UNIX ユーザー アカウントが設定されていれば、デフォルトの UNIX ユーザーの UID (ユーザー識別子) とプライマリ GID (グループ識別子) が使用されます。同様に、未割り当ての UNIX ユーザーがマルチプロトコル ファイル システムへの接続を試行した場合に、NAS サーバーに対してデフォルトの Windows ユーザー アカウントが設定されていれば、デフォルトの Windows ユーザーの Windows 認証情報が使用されます。

メモ: デフォルトの UNIX ユーザーが UDS(UNIX ディレクトリ サービス) で設定されていない場合、未割り当てユーザーの SMB アクセスが拒否されます。デフォルトの Windows ユーザーが Windows DC または LGDB に見つからない場合は、Windows アクセス ポリシーを持つファイル システム上で未割り当てユーザーの NFS アクセスが拒否されます。

メモ: デフォルト UNIX ユーザーは、有効な既存の UNIX アカウント名にするか、新しい形式「`@uid=`*xxxx*`,gid=`*yyyy*`@`」(*xxxx* と *yyyy* はそれぞれ、UID およびプライマリー GID の 10 進数値) に従うことができ、PowerStore Manager を使用してシステム上で設定することができます。

NFS リクエストの UNIX 認証情報

UNIX アクセス ポリシーまたはネイティブ アクセス ポリシーで NFS のみまたはマルチ プロトコル ファイル システムの NFS リクエストを処理するには、UNIX 認証情報を使用する必要があります。UNIX 認証情報は常に各リクエストに組み込まれますが、認証情報は追加グループが 16 個に制限されます。NFS サーバーの `extendedUnixCredEnabled` プロパティを使用して、16 個を超えるグループを持つ認証情報を作成できます。このプロパティを設定した場合、プライマリ GID およびそれに属するすべてのグループ GID を取得するためにアクティブな UDS が UID でクエリーされます。UID が UDS に見つからない場合、リクエストに組み込まれた UNIX 認証情報が使用されます。

メモ: NFS への安全なアクセスを確保するために、認証情報は常に UDS を使用して作成されます。

SMB リクエストの UNIX 認証情報

UNIX アクセス ポリシーでマルチ プロトコル ファイル システムの SMB リクエストを処理するには、まず、セッション構成時に SMB ユーザーに対して Windows 認証情報を作成する必要があります。Windows ユーザーの SID は、AD から名前を見つけるために使用します。その後、その名前は UDS またはローカル ファイル (passwd ファイル) から Unix の UID と GID を (必要に応じて ntxmap を使用して) 見つけるために使用されます。ユーザーの所有者 UID は Windows 認証情報に含まれます。UNIX アクセス ポリシーでファイル システムにアクセスする場合、NFS の拡張認証情報を作成するのと同様に、UNIX 認証情報の作成で UDS をクエリーするときにユーザーの UID が使用されます。UID は、クォータ管理に必要です。

SMB リクエストの Windows 認証情報

Windows アクセス ポリシーまたはネイティブ アクセス ポリシーで SMB のみまたはマルチ プロトコル ファイル システムの SMB リクエストを処理するには、Windows 認証を使用する必要があります。ユーザーが接続するときは、セッション構成リクエスト時に一度だけ、SMB の Windows 認証情報を作成する必要があります。

NTLM (NT LAN Manager) の使用時とは異なり、Kerberos 認証の使用時には、ユーザーの認証情報がセッション構成リクエストの Kerberos チケットに含まれます。Windows DC または LGDB から他の情報がクエリーされます。Kerberos の場合、追加グループ SID のリストが Kerberos チケットから取得され、追加ローカル グループ SID のリストと特権のリストは LGDB から取得されます。NTLM の場合、追加グループ SID のリストが Windows DC から取得され、追加ローカル グループ SID のリストと特権のリストは LGDB から取得されます。

さらに、対応する UID およびプライマリ GID もユーザー マッピング コンポーネントから取得されます。プライマリ グループ SID はアクセス チェックには使用しないため、UNIX プライマリ GID が代わりに使用されます。

メモ: NTLM は、ユーザーに認証、整合性、および機密性を提供する独自のセキュリティ プロトコルの古いスイートです。Kerberos は、チケット システムを使用してより高速な認証を実現するオープン スタンダード プロトコルです。Kerberos により、NTLM よりも優れたセキュリティがネットワーク上のシステムに追加されます。

NFS リクエストの Windows 認証情報

ユーザーが NFS リクエストを介して Windows アクセス ポリシーを持つファイル システムへのアクセスを試行しているときにのみ、Windows 認証情報が作成され、取得されます。UID が NFS リクエストから抽出されます。関連づけられた保存期間内に各 NFS リクエストで認証情報が作成されないようにするため、グローバルな Windows 認証情報のキャッシュがあります。Windows 認証情報がこのキャッシュに見つかった場合、他のアクションは必要ありません。Windows 認証情報が見つからない場合、UID の名前の検索には UDS またはローカル ファイルが照会されます。その後、この名前を使用して(必要に応じて ntxmap を使用して)Windows ユーザーを検索し、認証情報を Windows DC または LGDB から取得します。マッピングが見つからない場合、デフォルト Windows ユーザーの Windows 認証情報が代わりに使用されるか、アクセスが拒否されます。

CAVA (Common AntiVirus Agent) 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。

ウイルス対策はなぜ重要なのでしょうか。

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します。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。

Common Event Enabler (CEE) の一部である CAVA の詳細については、*Using the Common Event Enabler on Windows Platforms* (www.dell.com/powerstoredocs) を参照してください。

コード署名

PowerStore は、新しいリリースとパッチのリリースの両方のソフトウェア アップグレードを受け入れるように設計されています。マスター GNU Privacy Guard (GPG) キーは、すべての PowerStore ソフトウェア パッケージに署名し、Dell EMC によって制御されます。PowerStore ソフトウェア アップグレード プロセスによってソフトウェア パッケージの署名が検証され、改ざんまたは破損の可能性があることを示す無効な署名が拒否されます。検証手順がアップグレード プロセスに組み込まれているため、ソフトウェア パッケージの署名はインストール前のフェーズで自動的に検証されます。

2

通信のセキュリティの設定

本セクションでは、以下の項目について説明します。

トピック：

- ポートの使用

ポートの使用

次のセクションは、アプライアンスに存在する可能性のある各種ネットワーク ポートおよび対応するサービスの概要をまとめたものです。アプライアンスは、vCenter Server との通信など、一部の状況でネットワーク クライアントとして機能します。このような状況では、アプライアンスが通信を開始し、ネットワーク インフラストラクチャがこれらの接続をサポートしている必要があります。

メモ: ポートの詳細については、ナレッジベース記事 542240 (*PowerStore：お客様ネットワーク ファイアウォールのルール - TCP/UDP ポート*) を参照してください。https://www.dell.com/support/kbdoc/en-us/542240 にアクセスします。「お客様ネットワーク ファイアウォールのルール」ツールを使用すると、お使いの PowerStore 導入環境に関連するファイアウォールのルールとポートのリストをフィルタリングし、確認することができます。

アプライアンス ネットワーク ポート

次の表は、アプライアンスに存在する可能性のある各種ネットワーク ポートおよび対応するサービスの概要をまとめたものです。

表 2. アプライアンス ネットワーク ポート

ポート	サービス	プロトコル	アクセス方向	説明
22	SSH クライアント、SupportAssist Connect Home	TCP	双方向	• SSH アクセスを許可します (有効化されている場合)。 • SupportAssist Connect Home の場合に必要です。 閉じている場合、SSH を使用した管理接続は使用できなくなります。
25	SMTP	TCP	送信	アプライアンスの E メール送信を許可します。閉じている場合、メール通知を使用できなくなります。
26	SSH クライアント	TCP	双方向	ポート 22 への SSH アクセスはこのポートにリダイレクトされます。閉じている場合、SSH を使用した管理接続は使用できなくなります。
53	DNS	TCP/UDP	送信	DNS クエリーを DNS サーバーに送信するために使用します。閉じている場合は、DNS 名の解決が機能しません。
80、8080、8128	SupportAssist	TCP	送信	SupportAssist プロキシ接続に使用されます。
123	NTP	TCP/UDP	送信	NTP 時間の同期化。閉じている場合は、アプライアンス間で時刻が同期されません。

表 2. アプライアンス ネットワーク ポート（続き）

ポート	サービス	プロトコル	アクセス方向	説明
443	HTTPS	TCP	双方向	PowerStore Manager へのセキュア HTTP トラフィック。閉じている場合、アプライアンスと通信できなくなります。
500	IPsec（IKEv2）	UDP	双方向	ファイアウォール経由で IPSec を機能させるには、UDP ポート 500 を開き、受信と送信の両方のファイアウォール フィルターで IP プロトコル番号 50 および 51 を許可します。ファイアウォール経由で Internet Security Association and Key Management Protocol（ISAKMP）トラフィックが転送されるには、UDP ポート 500 が開いている必要があります。IP プロトコル ID 50 は、IPSec Encapsulating Security Protocol（ESP）トラフィックが転送されるように設定する必要があります。IP プロトコル ID 51 は、認証ヘッダー（AH）トラフィックが転送されるように設定する必要があります。閉じている場合、PowerStore アプライアンスとの間の IPsec 接続が使用できなくなります。
587	SMTP	TCP	送信	アプライアンスの E メール送信を許可します。閉じている場合、メール通知を使用できなくなります。
3033	インポート	TCP/UDP	送信	レガシー EqualLogic ピア ストレージおよび Compellent Storage Center システムからのストレージ インポートに必要です。
3260	iSCSI	TCP	• ホストおよび ESXi ホスト アクセスの受信 • 双方向コピー • ストレージ インポートの送信	iSCSI サービスに次のアクセスを提供するために必要です。 • 外部ホスト iSCSI アクセス • 外部または PowerStore の組み込み ESXi ホスト iSCSI アクセス • レプリケーションのクラスター間アクセス • レガシー EqualLogic ピア ストレージ、Compellent Storage Center、Unity、VNX2 システムからのストレージ インポート アクセス 閉じている場合、iSCSI サービスは使用できなくなります。低レイテンシー接続での妥当なレプリケーション パフォーマンスをサポートするために、データ モビリティーによって使用されます。
3261	データ モビリティー	TCP	双方向	高レイテンシー接続での妥当なレプリケーション パフォーマンスをサポートするために、データ モビリティーによって使用されます。
5353	マルチキャスト DNS（mDNS）	UDP	双方向	マルチキャスト DNS クエリー。閉じている場合は、mDNS 名前解決が機能しなくなります。
8443	VASA、SupportAssist	TCP	• VASA の受信 • SupportAssist の送信	• VASA 3.0 の VASA ベンダー プロバイダーに必要です。 • 関連する SupportAssist Connect Home 機能に必要です。

表 2. アプライアンス ネットワーク ポート（続き）

ポート	サービス	プロトコル	アクセス方向	説明
8443、50443、55443、または 60443	Windows インポート ホスト エージェント、Linux インポート ホスト エージェント、または VMware インポート ホスト エージェント	TCP	送信	レガシー ストレージ システムからデータ ストレージをインポートする場合は、これらのポートのいずれかを開く必要があります。
9443	SupportAssist	TCP	送信	Connect Home に関連する SupportAssist REST API に必要です。

ファイルに関連するアプライアンスのネットワーク ポート

次の表は、ファイルに関連するアプライアンスに存在する可能性のある各種ネットワーク ポートおよび対応するサービスの概要をまとめたものです。

メモ: 送信ポートは一時的なものです。

表 3. ファイルに関連するアプライアンスのネットワーク ポート

ポート	サービス	プロトコル	アクセス方向	説明
20	FTP	TCP	送信	FTP データ転送に使用されるポート。FTP を有効にすると、このポートを開くことができます。認証は、ポート 21 上で実行され、FTP プロトコルによって定義されます。
21	FTP	TCP	受信	ポート 21 は、制御ポートであり、FTP サービスはこのポート上で着信 FTP リクエストをリスンします。
22	SFTP	TCP	受信	SFTP (FTP over SSH) を介したアラート通知を許可します。SFTP はクライアント/サーバー プロトコルです。ユーザーは SFTP を使用して、ローカル サブネット上にあるアプライアンスでファイル転送を実行できます。送信 FTP 制御接続も提供します。閉じている場合、FTP は使用できなくなります。
53	DNS	TCP/UDP	送信	DNS クエリーを DNS サーバーに送信するために使用します。閉じている場合は、DNS 名の解決が機能しません。SMB v1 に必要です。
88	Kerberos	TCP/UDP	送信	Kerberos 認証サービスに必要です。
111	RPC バインド (SDNAS ネームスペースの場合。それ以外の場合はホスト サービス)	TCP/UDP	双方向	標準の portmapper または rpcbind サービスにより開かれており、補助的なアプライアンス ネットワーク サービスです。このサービスを停止することはできません。定義では、クライアント システムがポートにネットワーク接続されている場合は、ポートに対してクエリーを実行できます。認証は実行されません。
123	NTP	UDP	送信	NTP 時間の同期化。閉じている場合は、アプライアンス間で時刻が同期されません。
135	Microsoft RPC	TCP	受信	MicroSoft Client 用の多目的。NDMP にも使用されます。

表 3. ファイルに関連するアプライアンスのネットワーク ポート（続き）

ポート	サービス	プロトコル	アクセス方向	説明
137	Microsoft Netbios WINS	UDP、TCP/UDP	受信、送信	NETBIOS Name Service は、アプライアンス SMB ファイル共有サービスに関連づけられており、この機能のコア コンポーネントです（Windows）。このポートが無効になっている場合は、すべての SMB 関連のサービスが無効になります。
138	Microsoft Netbios BROWSE	UDP	送信	NETBIOS Datagram Service は、アプライアンス SMB ファイル共有サービスに関連づけられており、この機能のコア コンポーネントです。参照サービスのみ使用されます。無効にすると、このポートで参照機能が無効になります。
139	Microsoft CIFS	TCP	双方向	NETBIOS セッション サービスは、アプライアンス SMB ファイル共有サービスと関連づけられており、この機能のコア コンポーネントです。SMB サービスが有効である場合、このポートは開かれています。これは、特に SMB v1 のために必要です。
389	LDAP	TCP/UDP	送信	セキュリティ保護なしの LDAP クエリー。閉じている場合、セキュリティ保護なしの LDAP 認証クエリーを使用できなくなります。代わりにセキュリティ保護された LDAP を構成できます。
445	Microsoft SMB	TCP	受信	SMB（ドメイン コントローラー上）および Windows 2000 以降のクライアント用の SMB 接続ポート。アプライアンス SMB サービスへの正当なアクセス権を持つクライアントは、継続的な処理を行うために、このポートへのネットワーク接続が可能である必要があります。このポートが無効になっている場合は、すべての SMB 関連のサービスが無効になります。ポート 139 も無効になっている場合は、SMB ファイル共有が無効になります。
464	Kerberos	TCP/UDP	送信	Kerberos 認証サービスと SMB に必要です。
500	IPsec（IKEv2）	UDP	双方向	ファイアウォール経由で IPSec を機能させるには、UDP ポート 500 を開き、受信と送信の両方のファイアウォール フィルターで IP プロトコル番号 50 および 51 を許可します。ファイアウォール経由で Internet Security Association and Key Management Protocol（ISAKMP）トラフィックが転送されるには、UDP ポート 500 が開いている必要があります。IP プロトコル ID 50 は、IPSec Encapsulating Security Protocol（ESP）トラフィックが転送されるように設定する必要があります。IP プロトコル ID 51 は、認証ヘッダー（AH）トラフィックが転送されるように設定する必要があります。閉じている場合、PowerStore アプライアンスとの間の IPsec 接続が使用できなくなります。
636	LDAPS	TCP/UDP	送信	セキュリティで保護された LDAP クエリー。閉じている場合、セキュリティで保護された LDAP 認証を使用できなくなります。

表 3. ファイルに関連するアプライアンスのネットワーク ポート（続き）

ポート	サービス	プロトコル	アクセス方向	説明
1234	NFS mountd	TCP/UDP	双方向	マウント サービスに使用されます。これは、NFS サービスのコア コンポーネントです（バージョン 2、3、4）。
2000	SSHD	TCP	受信	保守用の SSHD（オプション）
2049	NFS I/O	TCP/UDP	双方向	NFS サービスの提供に使用されます。
3268	LDAP	UDP	送信	セキュリティ保護なしの LDAP クエリー。閉じている場合、セキュリティ保護なしの LDAP 認証クエリーを使用できなくなります。
4,000	NFSv3 用 STATD	TCP/UDP	双方向	NFS statd サービスの提供に使用されます。statd は、NFS ファイル ロックのステータス モニターであり、lockd と連動して機能して、NFS にクラッシュおよびリカバリ機能を提供します。閉じている場合、NAS statd サービスは使用できなくなります。
4001	NFSv3 用 NLMD	TCP/UDP	双方向	NFS lockd サービスの提供に使用されます。lockd は、NFS ファイル ロック デーモンです。このデーモンは、NFS クライアントからのロック リクエストを処理し、statd デーモンと連携して機能します。閉じている場合、NAS lockd サービスは使用できなくなります。
4002	NFSv3 の RQUOTAD	TCP/UDP、UDP	受信、送信	NFS rquotad サービスの提供に使用されます。rquotad デーモンは、ファイル システムをマウントしている NFS クライアントに対してクォータ情報を提供します。閉じている場合、NAS rquotad サービスは使用できなくなります。
4003	XATTRPD(拡張ファイル属性）	TCP/UDP	受信	マルチプロトコル環境でファイル属性を管理するために必要です。
4658	PAX（NAS サーバー アーカイブ）	TCP	受信	PAX は、標準的な UNIX テープ形式で動作するアプライアンス アーカイブ プロトコルです。
8888	RCPD(レプリケーション データ パス）	TCP	受信	レプリケーターにより使用されます（セカンダリ側）。データをレプリケートする必要が生じると、直ちにレプリケーターによって開かれたままにされます。サービスが開始された後にサービスを停止する方法はありません。
10000	NDMP	TCP	受信	• サード パーティー製ソフトウェアをサーバーにインストールしなくても、ネットワーク バックアップ アプリケーションで Network Data Management Protocol（NDMP）サーバーのバックアップ/リカバリーを制御できるようになります。アプライアンスでは、NAS サーバーが NDMP サーバーとして機能します。 • NDMP テープ バップアップを使用しない場合は、NDMP サービスを無効化できます。 • NDMP サービスは、ユーザー名/パスワードの組み合わせを使用して認証されま

表 3. ファイルに関連するアプライアンスのネットワーク ポート（続き）

ポート	サービス	プロトコル	アクセス方向	説明
				す。ユーザー名は構成可能です。さまざまな環境に合わせてパスワードを構成する方法については、NDMP のドキュメントを参照してください。
[10500, 10531]	NDMP 動的ポート用の NDMP 予約範囲	TCP	受信	3 方向バックアップ/リストア セッションでは、NAS サーバーはポート 10500 ~ 10531 を使用します。
12228	ウイルス対策チェッカー サービス	TCP	送信	ウイルス対策チェッカー サービスに必要です。

PowerStore X モデル アプライアンスに関連するネットワーク ポート

次の表は、PowerStore X model アプライアンスに存在する可能性のある各種ネットワーク ポートおよび対応するサービスの概要をまとめたものです。

表 4. PowerStore X model アプライアンスに関連するネットワーク ポート

ポート	サービス	プロトコル	アクセス方向	説明
22	SSH サーバー	TCP	受信	SSH アクセスを許可します（有効化されている場合）。閉じている場合、SSH を使用した管理接続は使用できなくなります。
80、9000	vSphere Web Access	TCP	受信	vSphere Web Client 用の vSphere Update Manager Web Client プラグインへのアクセス。
427	CIM サービス ロケーション プロトコル（SLP）	TCP/UDP	双方向	CIM クライアントは、サービス ロケーション プロトコルであるバージョン 2（SLPv2）を使用して CIM サーバーを検索します。
443	vSphere Web クライアント	TCP	受信	クライアント接続に使用されます。
902	ネットワークファイルコピー（NFC）、VMware vCenter、vSphere Web Client	TCP	• 双方向 NFC • VMware vCenter の送信 • vSphere Web Client の受信	• NFC は、vSphere コンポーネント用のファイルタイプに対応する FTP サービスを提供します。ESXi は、データストア間でのデータのコピーや移動などの操作にデフォルトで NFC を使用します。 • VMware vCenter エージェント • vSphere Web Client の場合、クライアント接続に使用します。
5900、5901、5902、5903、5904	RFB プロトコル	TCP	受信	VNC などのグラフィカル ユーザー インターフェイスへのリモート アクセス。
5988	共通情報モデル（CIM）サーバー	TCP	受信	CIM 用のサーバー。
5989	CIM セキュア サーバー	TCP	受信	CIM 用のサーバー。
6999	NSX 仮想分散論理ルーター、rabbitmqproxy	UDP	• 双方向 NSX 仮想分散ルーター サービス • Rabbitmqproxy のアウトバウンド	• NSX 仮想分散ルーター サービスの場合、このサービスに関連づけられているファイアウォール ポートは、NSX VIB がインストールされ、VDR モジュールが作成されるときに開かれます。ホストに関連づけられている VDR インスタンスが

表 4. PowerStore X model アプライアンスに関連するネットワーク ポート（続き）

ポート	サービス	プロトコル	アクセス方向	説明
				ない場合は、ポートを開く必要はありません。 ● Rabbitmqproxy の場合、ESXi ホストで実行されているプロキシ。このプロキシを使用すると、仮想マシン内部で実行されているアプリケーションが、vCenter ネットワーク ドメインで実行されている AMQP ブローカーと通信できるようになります。仮想マシンがネットワーク上に存在する必要はありません。つまり、NIC は必要ありません。送信接続の IP アドレスに、少なくとも使用中または今後使用されるブローカーが含まれていることを確認します。ブローカーは後で追加して拡張することができます。
8,000	vMotion	TCP	双方向	vMotion を使用した仮想マシンの移行に必要です。ESXi ホストは、vMotion トラフィック用のリモート ESXi ホストからの TCP 接続について、ポート 8000 をリスンします。
8100、8200、8300	フォールト トレランス	TCP/UDP	双方向	vSphere フォールト トレランス（FT）のホスト間トラフィックに使用されます。
8301、8302	DVSSync	UDP	双方向	DVSSync ポートは、VMware FT のレコード/リプレイが有効化されているホスト間で、分散仮想ポートの状態を同期するために使用されます。プライマリーまたはバックアップ仮想マシンを実行するホストでのみ、これらのポートが開いている必要があります。VMware FT を使用していないホストでは、これらのポートを開く必要はありません。
9080	I/O フィルター	TCP	送信	I/O フィルター ストレージ機能により使用されます。
31031	vSphere Replication、VMware Site Recovery Manager	TCP	送信	vSphere Replication および VMware Site Recovery Manager による進行中のレプリケーション トラフィックに使用されます。
44046	vSphere Replication、VMware Site Recovery Manager	TCP	送信	vSphere Replication および VMware Site Recovery Manager による進行中のレプリケーション トラフィックに使用されます。

3

監査

この章では、次の情報について説明します。

トピック：

- 監査

監査

監査により、システム上のユーザー アクティビティの履歴が表示されます。管理者、セキュリティ管理者、またはストレージ管理者の役割を持つユーザーは、REST API を使用して、システム上の構成の変更イベントを検索し、表示することができます。監査されるこれらのイベントは、セキュリティに関連するものではなく、すべての設定操作（ポスト/パッチ/削除）が監査ログに記録されます。

PowerStore Manager UI やコマンド ライン インターフェイス（CLI）などの他のインターフェイスを使用して、監査イベントの検索や表示を行うことができます。

4

データ セキュリティ設定

本セクションでは、以下の項目について説明します。

トピック：

静止データ暗号化

PowerStore の静止データ暗号化（D@RE）では、プライマリー ストレージ（NVMe SSD、NVMe SCM、SAS SSD）に対して FIPS 140-2 の検証済み自動暗号化ドライブ（SED）を使用します。NVRAM キャッシュ デバイスは暗号化されますが、現時点では FIPS 140-2 は検証されません。

各ドライブ内で暗号化が実行されてから、データがメディアに書き込まれます。これにより、ドライブ上のデータは、盗難や損失、およびドライブを物理的に分解してドライブを直接読み取ろうとする行為から保護されます。暗号化には、ドライブ上の情報を迅速かつ安全に消去する手段も用意されており、情報がリカバリされないようになっています。メディアの物理的な除去に関連する脅威からの保護に加え、以前にメディアに保管されていたデータの保護に使用した暗号化キーを破棄することで、メディアをすぐに転用することができます。

暗号化されたデータの読み取りには、SED がドライブのアンロックするための認証キーが必要です。認証された SED のみがアンロックされ、アクセス可能になります。ドライブがアンロックされると、SED は、暗号化されたデータを復号化して元の形式に戻します。

PowerStore アプライアンスには、すべての SED が含まれている必要があります。非自動暗号化ドライブをアプライアンスに追加しようとすると、アプライアンスでエラーが発生します。また、暗号化されたクラスター内への非暗号化アプライアンスの配置はサポートされていません。

暗号化のアクティブ化

PowerStore アプライアンスの静止データ暗号化機能は、工場出荷時に設定されています。暗号化をサポートしているアプライアンスの輸入が許可されている国では、暗号化がデフォルトで有効になっています。暗号化が有効になっている場合は、無効にすることはできません。暗号化をサポートしているアプライアンスの輸入が許可されていない国では、静止データ暗号化が無効になっています。

メモ: 静止データ暗号化をサポートしていないアプライアンスは、暗号化されたアプライアンスを使用するクラスターには使用できません。

暗号化ステータス

アプライアンスの暗号化ステータスは、次のレベルで報告されます。

- クラスター レベル
- アプライアンス レベル
- ドライブ レベル

クラスター レベルの暗号化ステータスは、アプライアンスの暗号化が有効であるかどうかを単純に反映します。これは、ドライブのステータスには関連していません。

アプライアンスの暗号化ステータスは、次のいずれかで表示されます。

- Encrypted：アプライアンスで暗号化機能が有効になっています。
- Unencrypted：アプライアンスでは暗号化機能がサポートされません。
- Encrypting：暗号化のアクティブ化プロセス中に表示されます。暗号化プロセスが正常に完了すると、クラスター レベルの暗号化ステータスが暗号化済みとして表示されます。

ドライブ レベルの暗号化ステータスは、アプライアンス内の各ドライブについて、次のいずれかで表示されます。

- Encrypted：ドライブは暗号化されています。これは、暗号化可能なアプライアンスのドライブの一般的な状態です。
- Encrypting：アプライアンスがドライブでの暗号化を有効にしています。このステータスは、アプライアンスでの暗号化を初めてアクティブ化している間、または構成済みアプライアンスに新しいドライブを追加している間に表示されます。
- Disabled：各国固有のインポートの制限により、ドライブで暗号化を有効にすることができません。いずれかのドライブでこのステータスが報告される場合は、クラスター内のすべてのドライブでも同じステータスが報告されます。
- Unknown：アプライアンスはまだ、ドライブで暗号化を有効にしようとしていません。このステータスは、アプライアンスでの暗号化を初めてアクティブ化している間、または構成済みアプライアンスに新しいドライブを追加している間に表示されます。
- Unsupported：ドライブは暗号化をサポートしていません。
- Foreign：ドライブはサポートされていますが、別のアプライアンスによってロックされています。使用する前に廃止する必要があります。

キー管理

埋め込みのキー管理サービス（KMS）が、各 PowerStore アプライアンスのアクティブなノードで実行されます。このサービスは、ローカル キーストア ファイル ロックボックス ストレージを管理して、システムおよびブート ドライブへの自動暗号化キーのバックアップをサポートしています。また、アプライアンスでの自動暗号化ドライブ（SED）のロックとアンロックのプロセスも制御しており、アプライアンスのローカル キーストア コンテンツの管理も行います。ローカル キーストア ファイルは、256 ビット AES キーで暗号化され、キーストア ファイル ロックボックス ストレージは RSA の BSAFE テクノロジーを活用します。

KMS によって、アプライアンスの初期化時に、SED のランダム認証キーが自動的に生成されます。各ドライブには、固有の認証キーがあり、アプライアンスに後で追加されて、SED のロックおよびアンロックのプロセスで使用されるものも含まれます。キー暗号化キーにより、キーストア ファイル ストレージ内の、およびアプライアンス内で転送中の認証キーと暗号化キーが暗号化されます。メディア暗号化キーは、SED の専用ハードウェアに保存されており、アクセスできません。暗号化が有効である場合は、すべての認証キーがアプライアンス内に保存されます。

キーストア バックアップ ファイル

KMS では、キーストア アーカイブ ファイルのオフアプライアンス バックアップの作成とダウンロードがサポートされています。オフアプライアンス バックアップにより、キーが失われ、アプライアンスやクラスターが使用できなくなるという重大な事態の可能性を削減できます。クラスター キーストアのバックアップが開始されたときに特定のアプライアンスが使用できない場合、動作全体は完了しますが、バックアップにはクラスター内の一部のアプライアンスのキーストア ファイルが含まれていないことと、オフラインのアプライアンスが使用可能なときに操作を再試行する必要があることを示す警告が発行されます。

メモ: クラスター内のプライマリー アプライアンスには、クラスター内で検出された各アプライアンス（プライマリー アプライアンスを含む）からのキーストア バックアップを含むクラスター キーストア アーカイブ ファイル が含まれています。

クラスター内のシステムの構成が変更されたためにキーストアが変更された場合は、新しいキーストア アーカイブ ファイルを生成してダウンロードすることをお勧めします。キーストア アーカイブ ファイルのバックアップ ダウンロード操作は、一度に 1 つのみ実行できます。

メモ: 生成したキーストア アーカイブ ファイルは、外部の安全な場所にダウンロードすることを強くお勧めします。システム上のキーストア ファイルが破損によりアクセスできなくなった場合、そのシステムはサービス モードになります。この場合は、問題の解決に、キーストア アーカイブ ファイルとサービス契約が必要になります。

キーストア アーカイブ ファイルをバック アップするには、管理者またはストレージ管理者のユーザー役割が必要です。キーストア アーカイブ ファイルをバック アップするには、**Settings** をクリックし、**Security** で **Encryption** を選択します。**Lockbox backup** の **Encryption** ページで、**Download Keystore Backup** をクリックします。

メモ: 障害が発生した場合にキーストアのバックアップをリストアするには、サービス プロバイダーにお問い合わせください。

暗号化が有効であるアプライアンスでのドライブの転用

このタスクについて

自動暗号化ドライブ (SED) は、アプライアンスが初期化された場合、またはすでに初期化されているアプライアンスに挿入された場合はロックされます。ドライブは、最初にアンロックしなければ、別のシステムで使用できません。ロックされたドライブは、別のアプライアンスに挿入されると使用できなくなり、新しいアプライアンスでは、その暗号化ステータスが `Foreign` と表示されます。ドライブは、新しいアプライアンス用に転用できますが、ドライブ上の既存のデータはすべて失われます。

アプライアンスで `Foreign` という暗号化ステータスを持つドライブを転用するには、次の手順を実行します。

手順

1. ドライブの背面にあるラベルに記載されている PSID (物理セキュリティ ID) を記録します。PSID は、転用プロセスの一部として入力する必要があります。
2. PowerStore Manager で、**Hardware** をクリックし、アプライアンスを選択してから、**Hardware** カードを選択します。
3. 転用するドライブを選択します。
   ドライブの **Encryption Status** が `Foreign` と表示されます。
4. **Repurpose Drive** をクリックします。
   Repurpose Drive スライドが表示されます。
5. ドライブの PSID を入力し、**Apply** をクリックします。

タスクの結果

ドライブは、新しいドライブとしてアプライアンスで転用され、転用プロセスが完了すると、その暗号化ステータスが `Encrypted` に変わります。

暗号化が有効なシステムのベース エンクロージャとノードの交換

暗号化が有効になっているアプライアンスの base enclosure および nodes で交換を実行するには、サービス契約が必要です。

アプライアンスを工場出荷時設定にリセットする

サービス スクリプト、`svc_factory_reset` により、シングル アプライアンス クラスターが工場出荷時の状態に戻され、すべてのユーザー データと持続的な構成が削除されます。

マルチ アプライアンス クラスターの場合、`svc_factory_reset` はセカンダリー アプライアンスでは実行できません。代わりに、サービス スクリプト、`svc_remove_appliance` を実行する必要があります。このスクリプトは、セカンダリー アプライアンスを出荷時の状態に戻し、すべてのユーザー データと持続的な構成を削除します。プライマリー アプライアンスのみがクラスターに残っている場合は、`svc_factory_reset` を実行してそのアプライアンスをリセットすることができます。

メモ: これらのスクリプトは、認定されたサービス プロバイダーのみによって実行することを推奨します。

これらのスクリプトの詳細については、*PowerStore Service Scripts Guide* を参照してください。

5

安全な保守設定

この章では、次の情報について説明します。

トピック：

運用に関する説明： SupportAssist™

SupportAssist 機能は、IP ベースの接続を提供します。これにより、Dell EMC サポートがアプライアンスからエラー ファイルとアラート メッセージを受け取り、リモートでトラブルシューティングを実行できるため、問題を迅速かつ効果的に解決できるようになります。

メモ: 問題を迅速に診断してトラブルシューティングを実行し、解決までの時間を短縮するために、SupportAssist 機能を有効にすることが強く推奨されます。SupportAssist 機能を有効にしていない場合は、Dell EMC サポートがアプライアンスに関する問題のトラブルシューティングと解決を実行できるよう、手作業でのアプライアンス情報の収集が必要になることがあります。また、データを CloudIQ に送信するには、SupportAssist 機能がアプライアンスで有効になっている必要があります。CloudIQ の詳細については、www.dell.com/support にアクセスしてください。ログインした後、CloudIQ **Product Support** ページに移動します。

SupportAssist とセキュリティ

SupportAssist 機能は、お客様と Dell EMC が信頼できる方法でソリューションを確実に使用できるように、リモート接続性プロセスの各ステップで複数のセキュリティ レイヤーを採用しています。

- Dell EMC に対する通知はすべてお客様のサイトから実行され、外部ソースから実行されることは決してありません。さらに AES（高度暗号化標準）の 256 ビット暗号化テクノロジーを使用して安全性が確保されます。
- IP ベースのアーキテクチャは、既存のインフラストラクチャと統合され、お使いの環境のセキュリティを確保します。
- サイトと Dell EMC 間の通信は、RSA®デジタル証明書を使用して双方で認証されます。
- 2 要素認証で検証された、認定済み Dell EMC カスタマー サービス プロフェッショナルだけが、サイトからの通知を表示するのに必要なデジタル証明書をダウンロードできます。
- オプションの SupportAssist v3 ポリシー マネージャー アプリケーションを使用すると、独自のガイドラインと要件に基づいて Dell EMC サポートのアクセス権を付与または制限できます。このアプリケーションには詳細な監査ログが含まれています。

SupportAssist 管理

SupportAssist 機能は、PowerStore Manager または REST API を使用して管理できます。サービスを有効または無効にし、選択した SupportAssist オプションに必要な関連情報を提供することができます。

メモ: 一元型 SupportAssist の **Gateway Connect with remote assist** と **Gateway Connect without remote assist** オプションは、高可用性（HA）をサポートしていません。これらのオプションでは、アクティブな HA SupportAssist クラスターにフェールオーバー能力が提供されません。PowerStore アプライアンスが単一の HA ゲートウェイ クラスター サーバーに導入されている（これが唯一の構成オプションです）場合、クラスター内で障害を避けることができたゲートウェイ サーバーへのフェール

オーバー能力はありません。アプライアンスが接続されている HA ゲートウェイ サーバーがダウンした場合、アプライアンスは、オートコールや CloudIQ ファイルなど、すべてのアウトバウンド ファイルの Dell EMC サポートへの転送を停止します。アプライアンスへのリモート アクセス用の SupportAssist 受信接続は、クラスター内で障害を避けることができた HA ゲートウェイ サーバーを使用して引き続き機能します。また、SupportAssist の **Gateway Connect with remote assist** と **Gateway Connect without remote assist** オプションは、システム上の指定されたプライマリー アプライアンスでのみ設定する必要があります。

アプライアンス自体には、いずれのポリシーも実装されません。アプライアンスに対するリモート アクセスをより細かく管理する必要がある場合は、ポリシー マネージャーを使用して権限を設定できます。ポリシー マネージャー ソフトウェア コンポーネントは、お客様提供のサーバーにインストールすることができます。このコンポーネントは、デバイスへのリモート アクセスを管理したり、リモート接続の監査ログを維持したりします。また、ファイル転送処理をサポートします。また、アプライアンスにアクセスするユーザー、デバイス、時間帯を管理することができます。ポリシーマネージャーの詳細については、www.dell.com/support にアクセスしてください。ログインした後、該当する **Support by Product** ページを見つけ、特定の SupportAssist 製品テクニカル ドキュメントへのリンクを探します。

SupportAssist 通信

メモ: 管理ネットワーク用に IPv6 で構成された PowerStore モデルで SupportAssist を有効にすることはできません。SupportAssist は IPv6 ではサポートされていません。また、クラスター上で SupportAssist を構成している場合、IPv4 から IPv6 への管理ネットワークの再構成は許可されません。

SupportAssist 機能を使用するには、DNS サーバーへのアクセスが必要です。

SupportAssist の **Connection Status** では、PowerStore と Dell EMC バックエンド サポート サービス間の接続状態、および接続のサービス品質（QoS）が表示されます。接続状態は 5 分間で判定され、接続のサービス品質（QoS）は 24 時間で判定されます。接続の **Connection Status** では、クラスター内の任意のアプライアンスに基づき、次のいずれかが表示されます。

- `Unavailable` - 接続データが使用できません。アプライアンスとの接続が失われたか、SupportAssist が有効化されたばかりであるため、状態を判定するためのデータが不十分です。
- `Disabled` - SupportAssist が有効化されていません。
- `Not connected` - 接続が失われました。5 回連続でキープアライブに失敗しました。
- `Reconnecting` - 接続が失われた後に PowerStore が再接続しようとしています。接続状態に戻るには、キープアライブ リクエストが 5 回連続で成功する必要があります。

PowerStore が Dell EMC バックエンド サポート サービスに接続されている場合、接続の **Connection Status** では、クラスター内のすべてのアプライアンスの平均に基づき次のいずれかが表示されます。

- `Evaluating` - SupportAssist が最初に初期化された後の最初の 24 時間は、接続のサービス品質（QoS）を判定できません。
- `Good` - 連続するキープアライブ リクエストの成功率は 80%以上です。
- `Fair` - 連続するキープアライブ リクエストの成功率は 50%～80%です。
- `Poor` - 連続するキープアライブ リクエストの成功率は 50%未満です。

SupportAssist オプション

SupportAssist 機能は、IP ベースの接続を提供します。これにより、Dell EMC サポートがシステムからエラー ファイルとアラート メッセージを受け取り、リモートでトラブルシューティングを実行できるため、問題を迅速かつ効果的に解決できるようになります。

SupportAssist オプションを使用して、リモート トラブルシューティングのためにアプライアンス情報を Dell EMC サポートに送信することができます。

- Gateway Connect without remote access（リモート アクセスを含まないゲートウェイ接続）: 双方向ファイル転送を行う、お客様が用意したゲートウェイ サーバー上で実行される一元的型 SupportAssist 用であり、次が含まれます。
  - オートコール
  - CloudIQ サポート
  - ソフトウェア通知
  - Dell EMC サポートからクラスターへの操作環境/ファームウェアのダウンロード

  SupportAssist ゲートウェイ サーバーは、ゲートウェイに関連づけられたアプライアンスの、IP ベースのすべての SupportAssist アクティビティーに関する単一の出入り口ポイントです。
- Gateway Connect with remote access（リモート アクセスを含むゲートウェイ接続）: Gateway Connect without remote access と同じ双方向ファイル転送を行う、お客様が用意したゲートウェイ サーバー上で実行される一元型 SupportAssist 用で、Dell EMC サポート担当者向けのリモート アクセスが含まれます。

- Direct Connect without remote access (リモート アクセスを含まない直接接続): Gateway Connect without remote access と同じ双方向ファイル転送を行う個々のアプライアンス上で実行される分散型 SupportAssist 用です。
- Direct Connect with remote access (リモート アクセスを含む直接接続): Gateway Connect without remote access と同じ双方向ファイル転送を行う個々のアプライアンス上で実行される分散型 SupportAssist 用で、Dell EMC サポート担当者向けのリモート アクセスが含まれます。

無効化することも可能ですが、推奨しません。このオプションを選択した場合、Dell EMC サポートは、アプライアンスでの問題に関する通知を受け取りません。アプライアンスに関する問題のトラブルシューティングと解決をサポート担当者が実行できるように、お客様が手作業でアプライアンス情報を収集することが必要になる場合があります。

SupportAssist Gateway Connect オプション

SupportAssist Gateway Connect は、ゲートウェイ サーバー上で作動します。**Gateway Connect without remote access** オプションまたは **Gateway Connect with remote access** オプションを選択すると、アプライアンスが SupportAssist クラスター内の他のアプライアンスに追加されます。クラスターは、Dell EMC サポート サーバーとオフアレイ ゲートウェイ サーバーの間の単一の安全な共通 (集中型) 接続の背後に配置されます。ゲートウェイ サーバーは、ゲートウェイに関連づけられたアプライアンスの、IP ベースのすべての Dell EMC SupportAssist アクティビティーに関する単一の出入り口ポイントです。

ゲートウェイ サーバーは、お客様の専用サーバーの 1 台以上にインストールされるリモート サポート ソリューション アプリケーションです。ゲートウェイ サーバーは、関連づけられているアプライアンスと Dell EMC エンタープライズの間の通信の仲介役として機能します。

SupportAssist ゲートウェイの詳細については、Dell サポート Web サイト (www.dell.com/support) の SupportAssist 製品ページをご覧ください。

SupportAssist の **Gateway Connect without remote access** オプションまたは **Gateway Connect with remote access** オプションを使用するようにアプライアンスを構成するには、ゲートウェイ サーバーの IP アドレスとポート番号 (デフォルトは 9443) を指定する必要があります。また、ゲートウェイ サーバーとアプライアンス間でポートが開いていることを確認します。

メモ: ゲートウェイ サーバーを使用するようにアプライアンスを構成するには、ゲートウェイ サーバーが動作している必要があります。アプライアンスは、PowerStore Manager からのみゲートウェイに追加できます。ゲートウェイ サーバーからアプライアンスを追加すると、アプライアンスは接続済みとして表示されますが、システム情報が正常に送信されません。

SupportAssist Direct Connect オプション

SupportAssist Direct Connect は、各アプライアンスのプライマリー ノードで直接実行されます。クラスターでは、各アプライアンスが、Dell EMC サポートへの独自の接続を確立します。トラフィックは、クラスター内のプライマリー アプライアンス経由ではルーティングされません。ただし、SupportAssist は、クラスター レベルでのみ管理できます。つまり、すべての変更がクラスター内のすべてのアプライアンスに適用されます。

Support Assist ページから SupportAssist Direct Connect を有効化して構成します。これは PowerStore Manager の **Settings** からアクセスでき、**Support** にリストされています。これらのアクションにより、アプライアンス自身と Dell EMC サポートとの間で安全な接続を使用するようにアプライアンスを設定できます。SupportAssist Direct Connect に対して、次のリモート サービス接続オプションのいずれかを選択できます。

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Direct Connect without remote access オプションを選択し、エンド ユーザー ライセンス契約 (EULA) に同意すると、アプライアンス自体が Dell EMC サポートとの間に安全な接続をセットアップします。このオプションを使用すると、双方向ファイル転送接続機能が Dell EMC サポートとの間で有効になります。該当する場合は、アプライアンスから、関連づけられているプロキシ サーバー (オプション) への接続を構成できます。必要な場合は、後でリモート アクセス構成セットアップを使用して Direct Connect にアップグレードすることができます。

Direct Connect with Remote Access オプションを選択し、エンド ユーザー使用許諾契約 (EULA) に同意すると、アプライアンス自体が Dell EMC サポートとの間に安全な接続をセットアップします。このオプションにより、アプライアンスのリモート アクセス サービス接続機能が、双方向ファイル転送とともに、Dell EMC サポートとの間で有効になります。該当する場合は、PowerStore Manager を介して、アプライアンスから、ポリシー マネージャー (オプション) および関連づけられているプロキシ サーバー (オプション) への接続を構成できます。

新しいアプライアンスが既存のクラスターに追加されると、新しいアプライアンスがクラスター SupportAssist 設定を検出し、適合するように自動的に構成されます。SupportAssist Direct Connect が現在有効になっている場合は、新しいアプライアンスで自動的に有効になります。追加の操作は必要ありません。SupportAssist Direct Connect を有効にすることができない場合でも、アプライアンス追加プロセスの完了が妨げられることはありません。

SupportAssist Gateway Connect の要件

次の要件が、**Gateway Connect without remote access** と **Gateway Connect with remote access** の両方の SupportAssist 実装に適用されます。

- アプライアンスと SupportAssistGateway サーバーの間のネットワーク トラフィック (HTTPS) が、ポート 9443 (または、お客様が別のポートを指定している場合は、そのポート) で許可されている必要があります。
- SupportAssist は、バージョン 4.0.5 またはバージョン 3.38 である必要があります。

メモ: ゲートウェイ サーバーからの手動によるアプライアンスの追加と削除はいずれも、決して行わないでください。PowerStore Manager SupportAssist 構成ウィザードでのみ、ゲートウェイ サーバーからのアプライアンスの追加または削除を行ってください。

SupportAssist Direct Connect の要件

次の要件が、**Direct Connect without remote access** と **Direct Connect with remote access** の両方の SupportAssist 実装に適用されます。

- ネットワーク トラフィック (HTTPS) を、ポート 443 および 8443 (アウトバウンド) で Dell EMC サポートに対して許可する必要があります。ポート 8443 のオープンに失敗すると、大幅なパフォーマンス インパクト (30 ~ 45%) を生じます。ポートのオープンに両方とも失敗すると、エンド デバイスに関する問題の解決が遅れる可能性があります。

以下の要件は、**Direct Connect with Remote Access** の SupportAssist 実装にのみ適用されます。

- アプライアンスへのリモート アクセスをより細かく管理するためのポリシー マネージャーを実装に含める場合は、SupportAssist 機能の設定時にそのことを示す必要があります。

SupportAssist を設定する

次のいずれかの方法で、アプライアンス用に SupportAssist を構成できます。

- 初期構成ウィザード : PowerStore Manager の初期設定を案内し、システムを利用できるように準備するユーザー インターフェイスです。
- **Suppoprt Assist** : PowerStore Manager から設定ページにアクセスします (**Settings** をクリックし、**Support** で **SupportAssist** を選択)。
- REST API サーバー : アプリケーション インターフェイスで、SupportAssist の設定項目を構成するための REST API リクエストを受け取ります。REST API の詳細については、PowerStore REST API Reference Guide を参照してください。

SupportAssist 機能のステータスを特定するには、PowerStore Manager で **Settings** をクリックし、**Support** で **SupportAssist** を選択します。

SupportAssist の構成

このタスクについて

PowerStore Manager を使用して SupportAssist を構成するには、次の手順を実行します。

メモ: **Direct Connect with remote access** オプションを **Direct Connect without remote access** または **Gateway Connect** オプションに変更するには、Dell EMC サポート担当者の支援が必要です。

手順

1. **Settings** をクリックし、**Support** で **SupportAssist** を選択します。
2. SupportAssist のステータスが無効と表示されている場合は、**SupportAssist** コントロール アイコンをクリックして SupportAssist を有効にします。

   SupportAssist 機能は無効にすることは可能ですが、推奨されません。

   ボタンを右方向に動かし、表示を `Enabled` に変更する必要があります。ただし、必要な構成情報を入力して **Apply** をクリックするまで、**Connection Status** は変更されません。

3. **SupportAssist** では、**Connect to CloudIQ** チェックボックスがデフォルトでオンになっています。ファイルを CloudIQ に送信しない場合は、チェックボックスをオフにします。それ以外の場合は、オンのままにします。
4. 使用する SupportAssist オプションの **Type** をリストで選択します。
5. 選択した SupportAssist オプションのタイプに応じて、次のいずれかを実行します。
   - **Gateway Connect without remote access** または **Gateway Connect with remote access** オプション：
     - ゲートウェイ サーバーの IP アドレスを指定します。
       メモ: ゲートウェイ サーバーを使用するようにアプライアンスを構成するには、ゲートウェイ サーバーが動作している必要があります。
     - ゲートウェイ サーバーへの接続に使用するポートがデフォルト (9443) と異なる場合は、コントロールを使用して、ネットワークで使用するポートの番号を選択します。
   - **Direct Connect without remote access** オプションの場合：
     - ネットワーク接続でプロキシ サーバーを使用する場合は、プロキシ サーバーの IP アドレスを指定します。
       メモ: プロキシ サーバーを使用するようにシステムを構成するには、プロキシ サーバーが動作している必要があります。
     - コントロールを使用して、ネットワーク内のプロキシ サーバーへの接続に使用するポートの番号を選択します。
   - **Direct Connect with remote access** オプションの場合：
     - ネットワーク接続でプロキシ サーバーを使用する場合は、プロキシ サーバーの IP アドレスを指定します。
       メモ: プロキシ サーバーを使用するようにアプライアンスを構成するには、プロキシ サーバーが動作している必要があります。
     - コントロールを使用して、ネットワーク内のプロキシ サーバーへの接続に使用するポートの番号を選択します。
     - ポリシー マネージャーを使用してシステムへのリモート アクセスを制御する場合は、ポリシー マネージャーの IP アドレスを指定します。
       メモ: ポリシー マネージャーを使用するようにアプライアンスを構成するには、ポリシー マネージャーが動作している必要があります。
     - ポリシー マネージャーへの接続に使用するポートがデフォルト (9443) と異なる場合は、ネットワークで使用するポートの番号を入力します。
6. 選択した SupportAssist オプションのタイプに応じて、次のいずれかを実行します。
   - **Direct Connect without remote access** または **Direct Connect with Remote Access** オプションの場合は、次の手順に進みます。
   - **Gateway Connect without remote access** または **Gateway Connect with Remote Access** オプションの場合は、**Test Connection** を選択して、ゲートウェイ サーバーへの接続のステータスを確認します。

   メモ: ステータスが `Transitioning` と表示されたままで、数分間 (接続をテストするために必要な時間) たっても変わらない場合は、オンライン サポートにお問い合わせください。
7. **Send Test Alert** を選択して、エンドツーエンドの接続性を確保するためにテスト アラートを Dell EMC サポートに送信します。
8. 表示されている連絡先情報が正確であることを確認します。誤った情報や古い情報が表示されている場合は、それを修正します。

   SupportAssist 連絡先情報は、迅速に対応して問題解決をサポートするために不可欠です。また、正確かつ最新である必要があります。
9. **Apply** を選択して、SupportAssist 構成情報を保持します。

A

TLS 暗号スイート

この付録には、次の情報が含まれます。

トピック：

- サポートされている TLS 暗号スイート

サポートされている TLS 暗号スイート

暗号スイートでは、TLS 通信をセキュリティで保護するための一連のテクノロジーを定義します。

- 鍵交換アルゴリズム (データの暗号化に使用される秘密鍵がクライアントからサーバーに伝達される仕組み)。例 : RSA キーまたは Diffie-Hellman (DH)
- 認証方法 (ホストでリモート ホストの ID を認証する仕組み)。例 : RSA 証明書、DSS 証明書、認証なし
- 暗号化サイファ (データを暗号化する仕組み)。例 : AES (256 または 128 ビット)
- ハッシュ アルゴリズム (データの変更を特定する手段を提供し、データの整合性を確保する仕組み)。例 : SHA-2 または SHA-1

サポートされている暗号スイートは、これらすべての仕組みを兼ね備えています。

次のリストは、アプライアンスおよび関連ポートの TLS 暗号スイートの OpenSSL 名を示しています。

表 5. アプライアンスでサポートされるデフォルト/サポート対象 TLS 暗号スイート

暗号スイート	プロトコル	ポート
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443、8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443、8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443、8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443、8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443、8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443、8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443、8443