

PowerProtect Data Manager 19.11

セキュリティ構成ガイド

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 ロスの可能性を示し、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。

表.....	6
免責事項.....	7
はじめに.....	8
章 1: はじめに.....	13
このガイドについて.....	13
PowerProtect Data Manager ソフトウェアの紹介.....	14
サポートされているインターネット プロトコルバージョン.....	15
認証および許可の管理.....	15
ロードマップ.....	15
章 2: 認証.....	17
コンポーネントのアクセス制御.....	17
PowerProtect Data Manager へのログイン.....	17
PowerProtect Data Manager REST API へのログイン.....	18
ユーザーと認定資格の管理.....	18
事前にロードされたアカウントとデフォルトの認証情報.....	18
一般的なパスワード ポリシー.....	20
ローカル ID プロバイダーユーザーの管理.....	20
パスワードの複雑さと有効期限の構成.....	23
ログイン セキュリティ設定.....	24
ログインに失敗した場合の UI の作動構成.....	24
パスワードの期限が切れたオペレーティング システムの作動.....	26
パスワードの期限が切れたオペレーティング システムの影響.....	27
認証のタイプとセットアップ.....	27
ID プロバイダー s.....	27
外部管理 ID プロバイダー.....	28
外部 ID プロバイダーの構成.....	28
外部 ID プロバイダーの編集.....	29
外部 ID プロバイダーの削除.....	30
例：ADID プロバイダーの構成.....	30
例：LDAPID プロバイダーの構成.....	31
LDAP 構成に関する問題のトラブルシューティング.....	31
外部システムの認証.....	32
認定資格セキュリティ.....	32
リモート コンポーネントの認証.....	33
保護エンジンおよび Search Engine ノード, Search Engine node の認証.....	34
章 3: 許可.....	37
デフォルトの許可.....	37
外部との許可の関連付け.....	37
ID プロバイダーグループからロールへのマッピングの追加.....	37
ID プロバイダーグループからロールへのマッピングの変更.....	38
ID プロバイダーグループからロールへのマッピングの削除.....	39
RBAC (ロール ベースのアクセス制御)	40

ロール.....	40
システムが提供するロールと関連する権限.....	40
ロール権限の定義.....	43
権限の範囲.....	46
例：権限の範囲を使用した機密情報の保護と分離.....	47
例：権限の範囲を指定したセルフサービス リストアの提供.....	47
リソースとリソース グループ.....	48
リソース グループの作成.....	48
リソース グループの編集.....	50
リソース グループの削除.....	52
章 4: ログの設定.....	53
認証サーバーのログ.....	53
ログ バンドルの追加.....	53
syslog を使用したサーバーのモニタリング.....	53
Syslog 転送用 TLS の構成.....	54
Syslog サーバーの構成.....	54
Syslog 接続のトラブルシューティング.....	55
章 5: ネットワークおよび通信のセキュリティ設定.....	56
ポートの使用方法.....	56
通信セキュリティ設定.....	62
仮想ネットワーク (VLAN).....	62
SSH セッション タイムアウトの構成.....	62
REST API トークンの有効期限の構成.....	62
PowerProtect Data Manager ファイアウォールのサポート.....	63
ファイアウォール ルールの変更.....	64
章 6: データ セキュリティ設定.....	65
データ ストレージのセキュリティ設定.....	65
保護エンジンの設定.....	65
機密データの暗号化.....	65
バックアップおよびリストアの暗号化.....	65
バックアップとリストアの暗号化を有効にする.....	66
システム アクティビティの監査ログとモニタリング.....	67
監査サービスの構成.....	67
UI での監査イベントの表示.....	68
アラートの表示と管理.....	68
監査ログのエクスポート.....	69
コンプライアンス検証の構成.....	69
章 7: 暗号化.....	70
セキュリティ証明書.....	70
保護エンジンとセキュリティ証明書.....	71
アプリケーション エージェントとセキュリティ証明書.....	71
アプリケーション エージェントのセキュリティ証明書ファイル.....	71
外部コンポーネントとの PowerProtect Data Manager セキュリティ証明書の交換.....	71
REST API を使用した外部コンポーネント用セキュリティ証明書のインポート.....	72
PowerProtect Data Manager の証明書管理.....	73

仮想ネットワーク	74
UI を使用したセキュリティ証明書の置き換え	74
CLI ツールを使用したセキュリティ証明書の置き換え	74
vSphere Client 用 PowerProtect プラグインの再インストール	75
Web サービスの再開	76
SPBM 用の vCenter との新しいセキュリティ証明書の交換	76
章 8: セキュリティのアップデートとパッチ適用	78
セキュリティのアップデートとパッチ適用	78
PowerProtect Data Manager によって使用されている Velero または OADP バージョンのアップデート	78
章 9: 完全性と整合性	80
製品の完全性と整合性について	80
検証	80
Windows バイナリーの署名者の検証	80
Linux (RPM ベース) パッケージのベンダーの検証	81
Linux (Debian ベース) パッケージのベンダーの確認	81
Linux (RPM ベース) パッケージの GPG 署名の検証	81
JAR ファイルの署名の検証	82
Windows での SHA-256 Checksum の検証	82
Linux での SHA-256 Checksum の検証	83
AIX での SHA-256 Checksum の検証	83
章 10: その他の構成と管理の構成要素	84
ライセンス	84
クライアントソフトウェアのインストール	84
アプリケーションとアプリケーション データのバックアップ	84
付録 A: REST API の手順	85
証明書の手動置き換え	85
キーストアからのパブリック証明書とプライベート キーの準備	85
REST API を使用したカスタム セキュリティ証明書の手動インストール	86
REST API を使用したローカル ユーザー パスワードの変更	87
REST API を使用したコンプライアンス検証の構成	88

1	変更履歴.....	9
2	関連ドキュメント.....	9
3	表記規則.....	10
4	主要機能.....	14
5	メリット.....	14
6	Linux オペレーティング システムの事前にロードされたアカウント.....	19
7	PowerProtect Data Manager ソフトウェアの事前にロードされたアカウント.....	19
8	ID プロバイダー属性.....	28
9	デフォルトの属性値.....	29
10	ロール権限.....	41
11	監視権限.....	43
12	セキュリティとシステム監査権限.....	43
13	サポートのアシスタンスとログ管理権限.....	43
14	ユーザーとセキュリティ管理の権限.....	44
15	システム管理権限.....	44
16	アセット管理権限.....	44
17	ストレージ管理権限.....	45
18	保護ポリシー権限.....	45
19	リカバリーおよび再使用の管理権限.....	45
20	SLA コンプライアンス管理権限.....	46
21	コピー管理権限.....	46
22	リソース グループ権限.....	46
23	リソース グループ.....	47
24	権限の範囲.....	47
25	リソース グループ.....	48
26	権限の範囲.....	48
27	PowerProtect Data Manager のポート要件.....	56
28	サポート対象のワークロード.....	66

免責事項

本文書に記載される情報は、「現状有姿」の条件で提供されています。Dell は、本文書に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定目的への適合性に対する黙示的保証はいたしません。いかなる場合も、デル・テクノロジーズ、その関連会社またはサプライヤーは、本文書に含まれる情報または本文書に基づき実施することが決定した行為に起因または関連する一切の損害について、デル・テクノロジーズ、その関連会社またはサプライヤーがかかる損害の可能性について通知を受けていた場合であっても、直接、間接的、付随的、派生的な事業利益の損失または特別な損害を含め、責任を負いません。

セキュリティ構成ガイドはあくまでも参照用です。本ガイダンスは、広範なインストール済みシステムに基づいて提供されており、ローカルインストールや個々の環境に対する実際のリスク/ガイダンスについては説明していない場合があります。個々の環境に本情報を適用できるかどうかを判断し、適切なアクションを実行することがすべてのユーザーに推奨されます。本セキュリティ構成ガイドに記載されているすべての内容は、通告なく、適宜変更されることがあります。本書に記載されている情報または本書にリンクをしている資料は、自らの責任において使用してください。Dell は、独自の裁量により、随時通告なく本文書の変更またはアップデートを行う権利を留保します。

脆弱性の報告

Dell は、製品に潜む脆弱性を非常に深刻なものとして報告します。セキュリティの問題を Dell に報告する方法の最新情報については、「[Dell.com の Dell の脆弱性対応ポリシー](#)」を参照してください。

はじめに

製品ラインを改善するための努力の一環として、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リリースしています。そのため、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すべてのバージョンでサポートされているわけではない機能もあります。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通りに作動しない場合には、カスタマーサポートにお問い合わせください。

メモ: このマニュアルには、発行時点で正確だった情報が記載されています。カスタマーサポートの Web サイトにアクセスして、このマニュアルの最新バージョンを使用していることを確認してください。

製品名

Data Domain (DD) は現在 PowerProtect DD です。このドキュメント、ユーザーインターフェイス、および製品の他の場所に記載されている Data Domain または Data Domain システムの参考資料には、PowerProtect DD システムと旧 Data Domain システムが含まれています。多くの場合、ユーザーインターフェイスはまだアップデートが行われていないため、今回の変更が反映されていません。

使用言語

このドキュメントには、デル・テクノロジーズ, Dell Technologies の現在のガイドラインと一致していない言語が含まれている場合があります。デル・テクノロジーズ, Dell Technologies では、将来のリリースでドキュメントをアップデートし、それに応じて言語を訂正する予定です。

このドキュメントには、デル・テクノロジーズ, Dell Technologies の管理下ではなく、デル・テクノロジーズ, Dell Technologies のコンテンツに関する現在のガイドラインと一致していない、サードパーティーのコンテンツの言語が含まれている場合があります。関連するサードパーティーによってこのようなサードパーティーのコンテンツがアップデートされる場合、このドキュメントはそれに応じて訂正されます。

Web サイトのリンク

このドキュメントで使用されている Web サイトのリンクは、発行時点で有効だったリンクです。リンク切れに気付いた場合は、ドキュメントのフィードバックとして提供していただければ、デル・テクノロジーズ, Dell Technologies の従業員が必要に応じてドキュメントをアップデートします。

目的

このガイドでは、Dell PowerProtect Data Manager のインストール、構成、管理、使用に関連するセキュリティ情報について説明しています。

対象読者

このドキュメントは、PowerProtect Data Manager を導入することで、企業全体でデータを管理、保護、および再使用する作業に関係するホストシステム管理者を対象としています。

変更履歴

次の表に、このドキュメントの変更履歴を示します。

表 1. 変更履歴

リビジョン	日付	説明
01	2022 年 6 月 21 日	PowerProtect Data Manager バージョン 19.11 向けの本書のイニシャルリリース。

互換性情報

PowerProtect Data Manager ソフトウェアのソフトウェア互換性情報については、[E-Lab Navigator](#) を参照してください。

関連ドキュメント

次の資料は「[カスタマーサポート](#)」で入手可能であり、追加情報を提供しています。

表 2. 関連ドキュメント

役職	コンテンツ
PowerProtect Data Manager 管理およびユーザー ガイド	ソフトウェアの構成方法が記載されています。
PowerProtect Data Manager 導入ガイド	ソフトウェアを導入する方法について説明します。
PowerProtect Data Manager ライセンス ガイド	ソフトウェアのライセンスを取得する方法について説明しています。
PowerProtect Data Manager リリース ノート	ソフトウェアの新機能、既知の制限、環境、システム要件に関する情報が記載されています。
PowerProtect Data Manager セキュリティ構成ガイド	セキュリティに関する情報が含まれます。
PowerProtect Data Manager Amazon Web Services 導入ガイド	Amazon Web Services (AWS) にソフトウェアを導入する方法について説明しています。
PowerProtect Data Manager Azure 導入ガイド	Microsoft Azure にソフトウェアを導入する方法について説明しています。
PowerProtect Data Manager Google Cloud Platform 導入ガイド	Google Cloud Platform (GCP) にソフトウェアを導入する方法について説明しています。
PowerProtect Data Manager クラウド ディザスター リカバリー 管理およびユーザー ガイド	クラウド ディザスター リカバリー(クラウド DR)の導入、AWS クラウドや Azure クラウドでの仮想マシンの保護、およびリカバリー操作の実行方法について説明しています。
PowerProtect Data Manager Cyber Recovery ユーザー ガイド	PowerProtect Cyber Recovery ソフトウェアのインストール、アップデート、パッチ、アンインストールの方法について説明しています。
PowerProtect Data Manager ファイル システム ユーザー ガイド	ファイルシステム データ保護のために File System Agent でソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager Kubernetes ユーザー ガイド	Kubernetes クラスターにおいてネームスペースと PVC をバックアップおよびリストアするためにソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager Microsoft Exchange Server ユーザー ガイド	Microsoft Exchange Server 環境においてデータをバックアップおよびリストアするためにソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager Microsoft SQL Server ユーザー ガイド	Microsoft SQL Server 環境においてデータをバックアップおよびリストアするためにソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager Oracle RMAN ユーザー ガイド	Oracle Server 環境においてデータをバックアップおよびリストアするためにソフトウェアを構成および使用する方法について説明しています。

表 2. 関連ドキュメント (続き)

役職	コンテンツ
PowerProtect Data Manager SAP HANA ユーザー ガイド	SAP HANA サーバー環境においてデータをバックアップおよびリストアするためにソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager Storage Direct ユーザー ガイド	Storage Direct エージェントでソフトウェアを構成および使用し、スナップショットバックアップテクノロジーを活用して VMAX ストレージ アレイ上のデータを保護する方法について説明しています。
PowerProtect Data Manager ネットワーク接続型ストレージ ユーザー ガイド	ネットワーク接続型ストレージ(NAS)の共有とアプライアンスにあるデータを保護およびリカバリーするために、ソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager 仮想マシン ユーザー ガイド	vCenter Server 環境において仮想マシンと仮想マシン ディスク (VMDK)をバックアップおよびリストアするためにソフトウェアを構成および使用する方法について説明しています。
PowerProtect Data Manager による VMware Cloud Foundation デザスター リカバリー	VMware Cloud Foundation (VCF)環境のエンドツーエンドのデザインスター リカバリーを実行する方法について詳しく説明しています。
PowerProtect Data Manager パブリック REST API のドキュメント	デル・テクノロジーズ, Dell Technologies API が含まれていて、その使用方法を説明するチュートリアルが用意されています。
vRealize Automation Data Protection Extension (データ保護システムのインストールおよび管理ガイド用)	vRealize Data Protection Extension のインストール、構成、使用方法を説明しています。

表記規則

本書では次の表記規則を使用します。

表 3. 表記規則

Formatting	説明
[太字]	ボタン名、フィールド名、タブ名、メニューパス名など (ユーザーが選択またはクリックする) インターフェイス要素を示します。ダイアログボックス、ページ、ペイン、タイトル付きの画面領域、表ラベル、ウィンドウの名前にも使用します。
斜体	本文内で参照される出版物の完全なタイトルを示します。
Monospace	以下の場合に使用 : <ul style="list-style-type: none"> システムコード エラーメッセージやスクリプトなどのシステム出力 パス名、ファイル名、ファイル名拡張子、プロンプト、構文 コマンドおよびオプション
モノスペース斜体	変数に使用します。
モノスペース太字	ユーザーによる入力値を示します。
[]	角括弧は、オプション値を示します。
	垂直線は、他の選択を示します。垂直線は他の選択があることを示します。
{ }	中括弧内は、ユーザーが指定する必要がある内容を示します (例 : x, y, z)。
...	省略記号は、例の中で省略した必須ではない情報を示します。

以下の関連資料を使用して、この製品に関する詳細な情報を入手したり、サポートを受けたり、フィードバックを送信したりすることができます。

製品ドキュメントの入手先

- [カスタマーサポートの Web サイト](#)
- [コミュニティ ネットワーク](#)

サポートの取得方法

[カスタマーサポート](#)の Web サイトを利用すると、製品ライセンス、ドキュメント、アドバイザリー、ダウンロード、ハウツーおよびトラブルシューティングの情報にアクセスできます。[カスタマーサポート](#)に問い合わせる前に、この情報に基づいて、製品に関する問題を解決できる場合があります。

製品専用ページにアクセスするには、以下の手順を実行します。

1. [カスタマーサポート](#)の Web サイトにアクセスします。
2. 検索ボックスに、製品名を入力して、表示される一覧から製品を選択します。

ナレッジベース

ナレッジベースには適用可能なソリューションが含まれており、ソリューション番号（たとえば、KB000xxxxxx）またはキーワードで検索することができます。

ナレッジベースを検索するには、以下の手順を実行します。

1. [カスタマーサポート](#)の Web サイトにアクセスします。
2. [Support] タブで、[ナレッジベース] をクリックします。
3. 検索ボックスにソリューション番号またはキーワードを入力します。（オプション）検索ボックスに製品名を入力し、表示されたリストから製品を選択して、検索を特定の製品に限定することができます。

ライブチャット

サポート エージェントとの対話型ライブチャットに参加するには、次の手順を実行します。

1. [カスタマーサポート](#)の Web サイトにアクセスします。
2. [Support] タブで、[Contact Support] をクリックします。
3. [[Contact Information]] ページで、関連するサポートをクリックし、続行します。

サービスリクエスト

サポート エージェントからの詳細なヘルプが必要な場合は、サービスリクエストを送信します。サービスリクエストを送信するには、次の手順を実行します。

1. [カスタマーサポート](#)の Web サイトにアクセスします。
 2. [Support] タブで、[Service Requests] をクリックします。
- ① メモ:** サービスリクエストを作成するには、有効なサポート契約が結ばれている必要があります。アカウントや有効なサポート契約の入手方法の詳細については、セールス担当者にお問い合わせください。サービスリクエストの詳細を取得するには、Service Request Number フィールドにサービスリクエスト番号を入力し、右矢印をクリックします。

オープンしたサービスリクエストを確認するには、次の手順を実行します。

1. [カスタマーサポート](#)の Web サイトにアクセスします。
2. [Support] タブで、[Service Requests] をクリックします。
3. [[Service Requests]] ページの [Manage Your Service Requests] で [View All Dell Service Requests] をクリックします。

オンライン コミュニティ

ピアの連絡先、対話、製品サポートおよびソリューションのコンテンツについては、[コミュニティ ネットワーク](#)にアクセスしてください。対話形式により、お客様、パートナー、認定専門資格保持者とオンラインで対話します。

フィードバックを提供する方法

マニュアルの正確性、構成、全体的な品質向上のため、お客様からのフィードバックをお待ちしております。フィードバックは、こちらのアドレス宛にお寄せください。DPAD.Doc.Feedback@emc.com

はじめに

トピック：

- このガイドについて
- PowerProtect Data Manager ソフトウェアの紹介
- サポートされているインターネット プロトコルバージョン
- 認証および許可の管理
- ロードマップ

このガイドについて

このガイドでは、製品の安全な運用を保証するために必要とされる、PowerProtect Data Manager で使用可能なセキュリティ構成設定、安全な導入、および物理的なセキュリティ管理に関する概要について説明します。

認証	認証では、ユーザーと外部システムが PowerProtect Data Manager に対して自身を証明する時に使用する設定、構成オプション、手段を説明します。
許可	許可では、PowerProtect Data Manager によって認証済みユーザーまたは外部システムをアクセスまたはアクセス権のレベルにマッピングする方法を説明します。大まかに言うと、認証ではユーザーが実行できることを説明します。
ログの設定	ログとは、発生順の記録であり、オペレーション、手順、またはセキュリティ関連のトランザクションにおけるイベント（最初から最後まで）に関連する、あるいは、これらを引き起こした一連の処理を検証するうえで役立ちます。この章では、PowerProtect Data Manager で使用可能なログ ファイルへのアクセス方法とその管理方法について説明します。
ネットワークおよび通信のセキュリティ設定	通信セキュリティ設定により、PowerProtect Data Manager コンポーネント間、PowerProtect Data Manager コンポーネントと外部システムの間、および PowerProtect Data Manager コンポーネントと外部コンポーネントの間での安全な通信チャネルを確立することができます。この章では、PowerProtect Data Manager での通信にセキュアなチャネルが使用されていること、およびファイアウォール環境で PowerProtect Data Manager を構成する方法について説明します。
データ セキュリティ設定	データ セキュリティ設定により、不正アクセスや、PowerProtect Data Manager が永続的に保存しているデータの漏えいを防止する制御方法を定義できます。この章では、PowerProtect Data Manager によって処理されるデータを確実に保護するための設定について説明します。
暗号化	この章では、使用中のセキュリティ証明書の管理方法など、PowerProtect Data Manager の暗号形式オプションとコンポーネントについて説明します。
セキュリティのアップデートとパッチ適用	PowerProtect Data Manager ソフトウェアのアップデートとパッチを取得して適用するための手順。該当する場合、これらの手順には特定のコンポーネントにオフサイクル アップデートを適用する方法が含まれます。
完全性と整合性	PowerProtect Data Manager とそのダウンロードを導入またはインストール前に検証するための情報と手順。通常、検証はデジタル署名や Checksum などの方法で行われます。
その他の構成と管理の構成要素	この章では、前掲のカテゴリのいずれにも属さないその他すべてのトピックについて説明します。
REST API の手順	この付録では、推奨される手順で Web ユーザー インターフェイス (UI) またはコマンドライン インターフェイス (CLI) を使用するという目的を果たすことができるその他の方法について説明します。

PowerProtect Data Manager ソフトウェアの紹介

PowerProtect Data Manager ソフトウェアは、ソフトウェアデファインドのデータ保護、重複排除、運用の俊敏性、セルフサービス、IT ガバナンスを提供するソリューションです。

PowerProtect Data Manager には、次のような主要機能があります。

表 4. 主要機能

統合された重複排除、レプリケーション、および再利用によるソフトウェアデファインドのデータ保護
集中型 IT ガバナンスと結合されたネイティブ アプリケーションからのデータ バックアップ/リカバリー セルフサービス動作
統合クラウド階層化によるマルチクラウド最適化
SaaS ベースのモニタリングおよびレポート作成
導入、拡張、およびアップデートを容易にする先進サービスベースのアーキテクチャ

PowerProtect Data Manager は、データ保護ポートフォリオ内で複数のデータ保護製品を統合し、データ保護アズ ア サービスを実現します。これにより、次のようなメリットが得られます。

表 5. メリット

データ保護チームは、プロビジョニング、オートメーション、およびスケジュールを備えたデータ パスを作成して、ハイパフォーマンスのバックアップ/リカバリーを実現する保護エンジンをデータ保護インフラストラクチャに組み込むことができます
大規模環境のバックアップ管理者は、PowerProtect Data Manager サーバー上の一元的な場所から次の資産タイプのバックアップをスケジュール設定できます。 <ul style="list-style-type: none">VMware 仮想マシンファイル システムVMAX ストレージ グループKubernetes クラスタMicrosoft Exchange Server および Microsoft SQL Server データベースOracle DatabaseSAP HANA データベースネットワーク接続型ストレージ(NAS)共有
エージェントベースのアプローチにより、アプリケーション サーバー上のデータベースを自動的に検出し、保護することができます。
次の方法で、セルフサービスと一元化された保護を有効化します。 <ul style="list-style-type: none">サービスレベル目標(SLO)のモニタリング目標リカバリーポイント(RPO)違反の特定
大容量バックアップ ストリームの実行に最適化された VM Direct Engine を使用してデータを移動する外部 VM Direct アプライアンスの導入をサポート
次の機能を備えた基本的な組み込み型 VM Direct Engine が付属しています。 <ul style="list-style-type: none">これは、外部 VM Direct Engine で障害が発生した場合、またはそれが無効になっているか使用不可の場合に、バックアップおよびリストア操作を実行するための代替プロキシとして自動的に使用されますバックアップ ストリームを実行するための容量が限られているTransparent Snapshot Data Mover (TSDM)保護メカニズムを使用する仮想マシンのクラッシュコンシステント保護ポリシーで動作可能これにより、PowerProtect Search で使用される検索サービスが有効になります
PowerProtect Search がサポートされています。これにより、バックアップ管理者は、VM/NAS ファイルのコピーを迅速に検索し、リストアできます
仮想マシンとオンデマンド バックアップ/リストアの自動プロビジョニングが可能な、vRealize Automation DP 拡張機能をサポート
クラウド ディザスター リカバリー(Cloud DR)と統合。これには、AWS および Azure のクラウドにおける Cloud DR の導入、保護、およびリカバリー操作作用ワークフローが含まれる
PowerProtect Cloud Snapshot Manager と統合して、統一された PowerProtect Data Manager ダッシュボードで PowerProtect Cloud Snapshot Manager のジョブ、アラート、レポートを表示

表 5. メリット (続き)

PowerProtect Cyber Recovery と統合して、サイバー脅威から PowerProtect Data Manager 環境の整合性を保護
PowerProtect Data Manager の監視、構成、オーケストレーションを可能にする RESTful API インターフェイスを提供します。 <ul style="list-style-type: none">● 既存の自動化フレームワークを統合可能● 新しいスクリプトを迅速に書き込み可能● 簡単に実行できるチュートリアルを用意

サポートされているインターネット プロトコル バージョン

PowerProtect Data Manager は、IPv4 アドレスの使用のみをサポートします。

IPv6 アドレスを使用すると、エラーまたはその他の予期しない反応が発生する可能性があります。PowerProtect Data Manager を使用してネットワーク経由で接続するようにデバイスを構成する場合は、IPv4 アドレスのみを使用します。

認証および許可の管理

PowerProtect Data Manager では、複数の小規模なビルディング ブロックを通じて認証と許可を制御するセキュリティ モデルを提供します。

ユーザーとグループは、ローカルの ID プロバイダーまたは外部の ID プロバイダーとグループ マッピングによって定義されます。これらのソースは、ユーザーが PowerProtect Data Manager に自分を識別させる手段となります。 [認証](#) で、ID プロバイダーおよびユーザーとグループの管理に関する詳細について説明しています。

認証後、各ユーザーまたはグループには少なくとも 1 個のロールが割り当てられます。ロールは、ユーザーが実行できるタスクを定義する一連の権限を関連づけることによって、システム管理者からユーザーに許可を委任するものです。ユーザーまたはグループの作成や変更の一環として、ユーザーまたはグループにロールを割り当てることができます。 [RBAC \(ロール ベースのアクセス制御 \)](#) で、ロールとロールの割り当てに関する詳細を説明しています。

デフォルトでは、指定されたロールを持つユーザーとグループは、PowerProtect Data Manager 環境全体のリソースに対して操作を行うことができます。しかし、ユーザーとグループの作成や変更の一環として、割り当てるロールの適用範囲を絞り込むことができます。 [権限の範囲](#) で、ユーザーが操作を行う権限の範囲と、関連する構造を定義する方法の詳細について説明しています。リソース グループを使用すると、個々のユーザーに特定の資産に対する責任とアクセス権を割り当てることができます。

ロードマップ

次の手順では、新規導入におけるセキュリティ関連イベントに推奨されるコースを説明します。外部 ID プロバイダーなどの一部の手順は、すべての環境に適用されない可能性があります。

手順

1. 必要に応じて、ポート要件を確認し、環境の接続を構成します。
[ポートの使用方法](#) で詳細を参照してください。
2. E メール サーバーのセットアップを行います。
手順については、『[PowerProtect Data Manager 管理およびユーザー ガイド](#)』を参照してください。E メール サーバーは、パスワードの期限とパスワードのリセットに関連する Eメールのために部分的に使用されます。
3. 管理者ユーザーの連絡先情報のアップデートを行い、パスワード関連の通知に使用する有効な E メール アドレスを含めます。
[ユーザーと認定資格の管理](#) で手順を参照してください。
4. 自己署名セキュリティ証明書を変更します。
[セキュリティ証明書](#) と [PowerProtect Data Manager の証明書管理](#) では、手順について説明しています。
5. 外部 ID プロバイダーを構成します。
[認証のタイプとセットアップ](#) と [外部管理 ID プロバイダー](#) では、手順について説明しています。
6. PowerProtect Data Manager のロールを確認します。
[RBAC \(ロール ベースのアクセス制御 \)](#) で詳細を参照してください。

7. 権限の範囲に関する情報を確認して、セキュリティユースケースの計画を立てます。
[権限の範囲](#) で詳細を参照してください。
8. 保存されたデータを保護するリソースグループを作成します。
[リソースとリソースグループ](#) で手順を参照してください。
9. ローカルユーザーを追加して、ローカルユーザーのパスワードを変更します。ローカルユーザーを PowerProtect Data Manager ロールに割り当て、適切な権限の範囲を作成します。
[ユーザーと認定資格の管理](#) で手順を参照してください。
10. 外部 ID プロバイダーユーザーを PowerProtect Data Manager ロールにマッピングをし、適切な権限の範囲を作成します。
[外部との許可の関連付け](#) で手順を参照してください。

次の手順

ご使用の環境に適用するその他のセキュリティタスクを実施します。

認証では、ユーザーと外部システムが PowerProtect Data Manager に対して自身を証明する時に使用する設定、構成オプション、手段を説明します。

トピック：

- コンポーネントのアクセス制御
- PowerProtect Data Manager へのログイン
- PowerProtect Data Manager REST API へのログイン
- ユーザーと認定資格の管理
- ログインセキュリティ設定
- 認証のタイプとセットアップ
- ID プロバイダー s
- 外部システムの認証

コンポーネントのアクセス制御

コンポーネントのアクセス制御設定では、外部システムと内部システム、またはコンポーネントの製品に対するアクセスを制御する方法を定義します。

PowerProtect Data Manager では、検証済みのトークンを使用して、コンポーネント間のセキュアなオペレーションとデータ転送を提供します。

認証されたユーザーのみが、UI を使用してオペレーションを実行できます。ユーザーが UI にログインすると、ユーザー アカウントの認証情報を確認するために、ユーザー検証プロセスまたはリクエストによる認証サービスへの問い合わせが行われます。認証サービスによるユーザー検証が成功すると、アプリケーションによってリクエストにトークンが発行されます。認証を必要とするすべての PowerProtect Data Manager コンポーネントについて、トークンを使用したユーザー検証を行うことができます。認証サービスでトークンを使用したユーザー認証が行われた後、認証サービスによってユーザーが要求されたオペレーションを実行するために必要な権限レベルが決定されます。

PowerProtect Data Manager へのログイン

PowerProtect Data ManagerUI にログインする際に、アクティブなユーザー名とパスワードを入力します。

ユーザー名は、`user[@domain]` の形式に従います。ここでの `domain` は、ユーザーを特定の ID プロバイダーに関連付けるオプションの識別子です。

例：`jsmith` または `administrator@test-lab`。

- ドメインを指定しない場合、認証サービスはデフォルト ID プロバイダーを確認します。
- ドメインを指定すると、認証サービスはそのドメインの外部 ID プロバイダーを調べて、ログインを許可するかどうかを判断します。

ドメインは大文字と小文字が区別されます。ID プロバイダーの構成時と同じ大文字と小文字を使用してドメインを指定します。そうでない場合、次のようなエラーメッセージが表示されることがあります：`500: Resources cannot be retrieved.`

ID プロバイダーが認証情報を検証すると、認証サービスはユーザー トークンを発行します。PowerProtect Data ManagerUI では、トークン情報を使用してアクティビティ許可します。

システム構成を変更していない場合は、デフォルト ID プロバイダーがローカル ID プロバイダーになります。

メモ:

ユーザー インターフェイスが 30 分以上放置され、タイムアウトをした場合、ログイン ページにエラー 503: Unknown Error が表示されることがあります。この問題が発生した場合は、エラーを破棄し、ユーザー名とパスワードを使用して再度ログインをしてください。

期限切れのパスワードを使用してログインをする場合は、すぐにパスワードのリセットを行います。パスワードを変更する前に [Cancel] をクリックするか、ブラウザを閉じるか、ページから移動すると、今後のログインで認証情報が無効になります。認証情報を再度有効にする手順については、[[REST API を使用したローカルユーザー パスワードの変更](#)] を参照してください。

PowerProtect Data Manager REST API へのログイン

PowerProtect Data Manager REST API にログインをする際に、アクティブなユーザー名とパスワードを入力します。ユーザー名とドメインは、PowerProtect Data Manager UI のものと同じ形式です。

任意の curl または REST API クライアントを使用し、適切なロールを持つユーザーとして次のように PowerProtect Data Manager REST API にログインをします。

POST `https://{{server}}:{{port}}/api/v2/login`

Headers:

```
Content-Type: application/json
```

Request Payload:

```
{
  "username": "{{username}}",
  "password": "{{password}}"
}
```

各項目の意味は以下のとおりです。

- `{{server}}`は、PowerProtect Data Manager サーバーの FQDN または IP アドレスです。
- `{{port}}`は REST API ポートで、通常は 8443 です。
- `{{username}}`と`{{password}}`は、PowerProtect Data Manager REST API の認証情報です。

ログインに成功すると、REST API サービスからアクセス トークンを受信します。

200 OK

```
{
  "access_token": "eyJraWQiOiJkMjc5M",
  "token_type": "Bearer",
  "expires_in": 28800,
  "jti": "dadda4ef-c4ad-4153-9bee-82f5ad69c75a",
  "scope": "aaa",
  "refresh_token": "eyJraWQiOiJkMjc5M"
}
```

将来の REST API コールのために `access_token` 値を記録しますが、このアクセス トークンは一連の認証情報のように保護してください。この例におけるトークンは、分かりやすくするため、またスペースの都合上シンプルにされています。

ユーザーと認定資格の管理

次のトピックでは、ローカル アカウントの場合について説明します。これには、導入にあるアカウントのリスト、ユーザー アカウントを管理する方法、パスワードを変更する方法、認証情報を保護する方法などが含まれます。

事前にロードされたアカウントとデフォルトの認証情報

このトピックでは、デフォルトの PowerProtect Data Manager のインストールに付属のローカル ID プロバイダーユーザー アカウントと該当するデフォルトの認証情報について説明します。

デフォルトの認証情報の大半は、導入から初期構成までの期間のみ存在します。[変更が必要] の列に、構成プロセス中に置き換える必要がある認証情報を示しています。

[目的] の列では、各項目の想定される用途を示しています。[アクション] の列では、お客様とのやり取りが必要な箇所を示しています。

Linux オペレーティング システム

この表では、PowerProtect Data Manager が実行されている Linux オペレーティング システムにアクセスするためのアカウントについて説明します。

表 6. Linux オペレーティング システムの事前にロードされたアカウント

アカウントまたは認証資格	デフォルトのパスワード	期限の間隔	変更が必要	目的	アクション
root	changeme	60 日	可	コマンドに root 権限の昇格を与える。	N/A
support	\$upp0rt!	60 日	可	システム コンソールへの SSH アクセスを制御する。	N/A
admin	@ppAdm1n	60 日	可	システム コンソールへの SSH アクセスを制御する。	N/A

導入時に [共通のパスワードを使用] を無効にして異なるコンポーネントパスワードを設定した場合でも、構成プロセスでは、オペレーティング システムの各アカウントに同じパスワードが設定されます。

PowerProtect Data Manager ソフトウェア

この表では、PowerProtect Data Manager ソフトウェアを操作するための認証情報について説明します。

表 7. PowerProtect Data Manager ソフトウェアの事前にロードされたアカウント

アカウントまたは認証資格	デフォルトのパスワード	期限の間隔	変更が必要	目的	アクション
UI 管理者	admin	60 日	可	Web UI へのアクセスを制御する。 REST API リクエストへのアクセスを制御する。	N/A

PowerProtect Data Manager は、導入時に、強固で一意的なパスワードを自動的に構成します。[認定資格セキュリティ](#) ロックボックスの詳細が記載されています。

管理者アカウントのパスワードの期限

PowerProtect Data Manager にログインをして、通常の管理タスクを実行するには、管理者アカウントの有効なパスワードが必要です。パスワードの期限切れを防ぐことは、システム メンテナンスに欠かせません。

重大アラートの通知を構成して、管理者パスワードの期限が切れる 15 日前、7 日前、3 日前、1 日前にアラートを受信するようにしてください。アラート通知の構成の詳細については、『*PowerProtect Data Manager 管理およびユーザー ガイド*』を参照してください。

期限が切れる前に管理者パスワードを変更するには、「[オペレーティング システムのパスワードの変更](#)」を参照してください。

管理者パスワードの期限が切れ、リセットが必要な場合は、「[パスワードの期限が切れたオペレーティング システムの作動](#)」を参照してください。

Server DR リストア

PowerProtect Data Manager を server DR バックアップからリストアすると、すべてのプリロードされたアカウントのパスワードがデフォルトのパスワードにリセットされます。

UI 管理者アカウントのパスワードはリセットされず、最後に設定した値が保持されます。server DR バックアップからリストアしたら、事前に読み込まれたアカウントのパスワードをできるだけ早く変更します。

一般的なパスワードポリシー

ローカルの ID プロバイダーアカウント パスワードを設定する場合は、認定資格が次の要件を満たしていることを確認します。

- 最小 9 文字で最大 100 文字
- 1 個以上の数字 (0~9)
- 1 文字以上の英大文字 (A~Z)
- 1 文字以上の英小文字 (a~z)
- 次の有効な文字のうち 1 個以上の特殊文字

```
!@#$%^&*()_+~{}[]<>?/\`.:|\"
```

スペースは使用できません。

- 英語のアルファベットからの文字のみ
- 氏名、ユーザー名、E メール アドレスなど、ユーザー アカウントに関連づけられているその他の機密情報を記入しないこと

ローカル ID プロバイダーユーザーの管理

ユーザーを管理できるのは、管理者とセキュリティ管理者ロールのみです。管理者、セキュリティ管理者、ユーザーのロールは、ユーザーを表示できます。

① メモ: ユーザー権限によって、PowerProtect Data Manager のリソースへのユーザー アクセスが許可または拒否されます。権限は、ローカル ID プロバイダーユーザーと外部 ID プロバイダーユーザーで同じです。

事前に読み込まれている管理者アカウントの名前やロールの割り当てを変更することはできません。

ローカル ユーザーの追加

管理者およびセキュリティ管理者ロールのみが、ローカルの ID プロバイダーにユーザーを追加できます。

前提条件

この手順には、特定のタスクを実行する許可を委任するためのロール割り当てプロセスが含まれています。システム定義ロールのリストを確認し、必要なすべてのロールを特定します。

この手順では、このロール割り当てで操作を行う権限の範囲を定義することもできます。適用する範囲について計画を立て、必要なリソース グループを作成します。権限の範囲の作成はオプションです。許可はすべての資産に割り当てることができます。

① メモ: 特定のリソース グループに対して、バックアップ管理者、管理者のリストア、ユーザーのロールのみを制限できます。管理者およびセキュリティ管理者のロールは、すべてのリソースに対するフル アクセス権があります。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Users/Groups] タブをクリックします。
PowerProtect Data Manager は、関連するロールを含む、設定済みのユーザー アカウントおよび外部 ID プロバイダーグループのリストを表示します。
3. [Add User/Group] をクリックします。
[User Type] タブで [Add User/Group] ウィンドウが開きます。
4. [Local User] を選択します。
5. 次の情報を入力します。
 - [名]
 - [姓]
 - [E メール アドレス]
 - [ユーザー名]
 - [パスワード]
 - パスワードを再入力して確認します。
 - [Force Password Change] —デフォルトでは有効です。最初のログイン時に、ユーザーがパスワードをアップデートする必要があります。
6. [次へ] をクリックします。

- [Add User/Group] ウィンドウが [Role] タブに移動します。
- 1 個以上の適切なロールを選択します。
各ロールの許可のリストを表示するには、[>] をクリックします。次のタブで、各ロールの適用範囲をさらに絞り込むことができます。
 - [次へ] をクリックします。
[Add User/Group] ウィンドウが [Resources] タブに移動します。
 - ロールごとに、そのロールの許可を [All Assets] に適用するか、[Selected Resource Groups] に適用するかを選択します。
選択したリソース グループにのみ許可を適用すると、権限の範囲が作成されます。
[Selected Resource Groups] を選択した場合は、リソース グループのリストが表示されます。
 - 使用可能なリソース グループを 1 個以上選択します。
 - 選択したリソース グループをリストから削除するには、そのリソース グループの [X] をクリックします。
 - [次へ] をクリックします。
[Add User/Group] ウィンドウが [Summary] タブに移動します。
 - 選択内容を確認し、エラーがあれば修正して、[Finish] をクリックします。

タスクの結果

新しいユーザーが、構成されたユーザー アカウントとグループのリストに表示されます。

ローカル ユーザーの編集または削除

ローカルの ID プロバイダーユーザーを編集または削除できるのは、管理者ロールとセキュリティ管理者ロールのみです。

前提条件

この手順には、特定のタスクを実行する許可を委任するためのロール割り当てプロセスが含まれています。システム定義ロールのリストを確認し、必要なすべてのロールを特定します。

この手順では、このロール割り当てで操作を行う権限の範囲を定義することもできます。適用する範囲について計画を立て、必要なリソース グループを作成します。権限の範囲の作成はオプションです。許可はすべての資産に割り当てることができます。

メモ: 特定のリソース グループに対して、バックアップ管理者、管理者のリストア、ユーザーのロールのみを制限できます。管理者およびセキュリティ管理者のロールは、すべてのリソースに対するフル アクセス権があります。

手順

- 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
- [Users/Groups] タブをクリックします。
PowerProtect Data Manager は、関連するロールを含む、設定済みのユーザー アカウントおよび外部 ID プロバイダーグループのリストを表示します。
- 任意のユーザー アカウントの  をクリックして、次の情報を表示します。
 - ユーザー名
 - 名
 - 姓
 - E メール アドレス
 - ユーザーの役割
 - ユーザーが作成された日付
- 編集または削除するユーザーを選択します。
- ユーザーを削除するには、[Delete] をクリックします。
ユーザーが、構成済みのユーザー アカウントとグループのリストから消えます。
- ユーザーを編集するには、[Edit] をクリックします。
[User Type] タブで [Edit User/Group] ウィンドウが開きます。
- 次の情報を変更できます。
 - [名]
 - [姓]
 - [E メール アドレス]

- [ユーザー名]
 - [パスワード]
 - パスワードを再入力して確認します。
 - [Force Password Change] —デフォルトでは有効です。最初のログイン時に、ユーザーがパスワードをアップデートする必要があります。
8. [次へ] をクリックします。
[Edit User/Group] ウィンドウが [Role] タブに移動します。
 9. 1 個以上の適切なロールを選択します。
各ロールの許可のリストを表示するには、[>] をクリックします。次のタブで、各ロールの適用範囲をさらに絞り込むことができます。
 10. [次へ] をクリックします。
[Edit User/Group] ウィンドウが [Resources] タブに移動します。
 11. ロールごとに、そのロールの許可を [All Assets] に適用するか、[Selected Resource Groups] に適用するかを選択します。
選択したリソース グループにのみ許可を適用すると、権限の範囲が作成されます。
[Selected Resource Groups] を選択した場合は、リソース グループのリストが表示されます。
 - a. 使用可能なリソース グループを 1 個以上選択します。
 - b. 選択したリソース グループをリストから削除するには、そのリソース グループの [X] をクリックします。
 12. [次へ] をクリックします。
[Edit User/Group] ウィンドウが [Summary] タブに移動します。
 13. 選択内容を確認し、エラーがあれば修正して、[Finish] をクリックします。

タスクの結果

構成されたユーザー アカウントとグループのリストに変更が表示されます。

ローカル ユーザーのパスワードの変更

セルフサービス機能を使用して、ローカル ID プロバイダーユーザーのパスワードを変更します。

前提条件

現在のパスワードがわからない場合は、「[ローカルユーザーのパスワードをリセットする。](#)」で詳細情報を確認してください。外部 ID プロバイダーユーザーは、この手順を使用してパスワードをリセットすることはできません。ID プロバイダー管理者にパスワードのリセットを依頼してください。

手順

1. PowerProtect Data Manager UI にログインします。
2. バナーから、[User Options] > [Change Password] を順に選択します。
3. ローカル ユーザーの現在のパスワードを入力します。
4. 確認のため、新しいパスワードを 2 回入力します。
新しいパスワードは、「[一般的なパスワード ポリシー](#)」に準拠している必要があります。
5. [保存] をクリックします。

ローカルユーザーのパスワードをリセットする。

ローカル ユーザーがパスワードを忘れた場合は、セルフサービス機能を使用してパスワードをリセットします。

前提条件

- アカウントは、ローカル ID プロバイダーユーザーである必要があります。
- PowerProtect Data Manager でメール サーバーを構成する必要があります。
- 外部 ID プロバイダーユーザーは、この手順を使用してパスワードをリセットすることはできません。ID プロバイダー管理者にパスワードのリセットを依頼してください。

新しいパスワードを選択する前に、[一般的なパスワード ポリシー](#)を確認します。

このタスクについて

ローカル ユーザーは、パスワードをリセットするためのリンクを含む E メールを受信できます。Eメールのリセットパスワードリンクは 20 分で期限切れになり、その後は別のリンクを要求する必要があります。

手順

1. PowerProtect Data Manager ログイン ページで、[Forgot Password] をクリックします。
2. [Forgot Password] ダイアログ ボックスで、ユーザー名を入力して、[Send Link] をクリックします。それから、[OK] をクリックして情報ダイアログ ボックスを閉じます。
システムは、ユーザー名に関連づけられた E メール アドレスにメッセージを送信します。
3. E メールを開き、リンクをクリックします。
4. [Reset Password] ダイアログ ボックスで、[New Password] および [Confirm New Password] フィールドに新しいパスワードを入力し、[Save] をクリックします。
PowerProtect Data Manager のログイン ページが表示されます。
5. ユーザー名と新しいパスワードを使用してログインします。

オペレーティング システムのパスワードの変更

オペレーティング システムのパスワードを変更できるのは、管理者ロールのみです。PowerProtect Data ManagerUI を使用して、Linux オペレーティング システムの root、管理者、サポート ユーザーのパスワードを変更することができます。

このタスクについて

root ユーザーの場合、この方法は、現在のパスワードが期限切れになっておらず、現在のパスワードを知っている場合に使用できます。root パスワードの期限が切れている場合、操作は失敗します。

新しいパスワードを選択する前に、「[一般的なパスワード ポリシー](#)」を確認してください。

手順

1. 管理者ロールを持つユーザーとして PowerProtect Data Manager ユーザー インターフェイスにログインします。
2.  をクリックし、[Authentication] を選択します。
[System Users] ウィンドウが表示されます。
3. 変更するパスワードを選択します。
 - root およびサポート ユーザーの場合は、[Edit] をクリックします。
 - オペレーティング システムの管理者ユーザーは、[Reset] をクリックします。既存のパスワードを入力しなくても、オペレーティング システムの管理者ユーザー パスワードを変更することができます。
4. フォームを更新し、[Save] をクリックします。

パスワードの複雑さと有効期限の構成

このトピックでは、REST API を使用して PowerProtect Data Manager のパスワード ポリシーを構成する方法について説明します。正規表現を変更する場合は、ルールの整合性を維持するために、両方の正規表現を変更します。

このタスクについて

REST API の使用方法に関する例など、詳細については、PowerProtect Data Manager REST API のドキュメントを参照してください。任意の curl またはクライアントを使用し、ログインをしてから各コールに有効なアクセス トークンを指定します。クライアントでは、自己署名証明書を使用するサーバーへの接続を許可するために追加のパラメーターが必要になる場合があります。

[一般的なパスワード ポリシー](#) では、デフォルトのパスワード ポリシーについて説明します。

手順

1. 管理者ロールを持つユーザーとして、PowerProtect Data Manager REST API にログインをします。
アクセス トークンを記録します。
2. 次のように既存のパスワード ポリシーを取得します (デフォルトとは異なる場合があります)。

```
GET https://{{server}}:{{port}}/api/v2/policies/password
```


REST API の使用方法に関する例など、詳細については、PowerProtect Data Manager REST API のドキュメントを参照してください。任意の curl またはクライアントを使用し、ログインをしてから各コールに有効なアクセストークンを指定します。クライアントでは、自己署名証明書を使用するサーバーへの接続を許可するために追加のパラメーターが必要になる場合があります。

手順

1. 管理者ロールを持つユーザーとして、PowerProtect Data Manager REST API にログインをします。
アクセストークンを記録します。
2. 次のようにして、UI ログイン失敗の動作を変更します。

PUT https://{{server}}:{{port}}/api/v2/common-settings/USER_LOCKOUT_SETTING

```
Headers:
Content-Type: application/json
Authorization: Bearer {{access-token}}
```

```
{
  "id": "USER_LOCKOUT_SETTING",
  "properties": [
    {
      "name": "durationMinutes",
      "value": "{{lockout-duration-minutes}}",
      "type": "INTEGER"
    },
    {
      "name": "loginAttempts",
      "value": "{{number-login-attempts}}",
      "type": "INTEGER"
    }
  ]
}
```

ここで、

オプション	説明
<code>{{lockout-duration-minutes}}</code>	失敗回数の上限を上回った後に PowerProtect Data Manager によってユーザー アカウントがロックされる分数デフォルト値は 5 です。
<code>{{number-login-attempts}}</code>	PowerProtect Data Manager によってユーザー アカウントがロックされるログイン試行の失敗回数デフォルト値は 5 です。

すべての値を整数とし、すべての値が必須です。

REST API サービスから次の状態コードが返されます。

```
200 OK
{
  "id": "USER_LOCKOUT_SETTING",
  "properties": [
    {
      "name": "durationMinutes",
      "value": "5",
      "type": "INTEGER"
    },
    {
      "name": "loginAttempts",
      "value": "5",
      "type": "INTEGER"
    }
  ]
}
```

パスワードの期限が切れたオペレーティング システムの作動

Linux オペレーティング システムの管理者、root、サポート ユーザーのパスワードについては、別の期限切れのシナリオが発生する可能性があります。各シナリオには、そのアカウントの期限切れのパスワードを知っているかどうかに応じて、対応方法が2種類あります。

期限切れのパスワードをリセットするには、少なくとも1個のパスワードを知っている必要があります。そうでない場合は、カスタマー サポートにお問い合わせください。

管理者パスワードの期限が切れている場合

管理者ロールを持つアカウントで PowerProtect Data Manager UI にログインをすると、管理者パスワードをリセットできます。[オペレーティング システムのパスワードの変更](#) で手順を参照してください。有効期限切れのパスワードを把握する必要はありません。

管理者ロールで UI にログインができない場合は次の手順を実行します。

- 管理者ユーザーとして PowerProtect Data Manager に SSH セッションを確立します。コンソールでは、期限切れのパスワードを入力した後で、新しいパスワードを設定するように求められます。
- 期限切れのパスワードは知らなくても、root パスワードは知っている場合は、vSphere コンソールを使用して管理者パスワードをリセットできます。vSphere コンソールを使用して、root ユーザーとして PowerProtect Data Manager にログインします。次に、`[passwd admin]` と入力して管理者パスワードをリセットします。再起動する必要はありません。
- root パスワードまたは期限切れのパスワードを知らない場合は、カスタマー サポートにお問い合わせください。

root パスワードの期限が切れている場合

期限切れのパスワードを知っている場合は、PowerProtect Data Manager コンソールから root パスワードをリセットできます。期限切れの root パスワードを UI でリセットすることはできません。

管理者ユーザーとして PowerProtect Data Manager に SSH セッションを確立し、`[su -]` と入力して root ユーザーに変更します。コンソールでは、期限切れの root パスワードを入力した後で、新しいパスワードを設定するように求められます。

期限切れのパスワードは知らなくても、管理者パスワードは知っている場合は、コンソールを使用して root パスワードをリセットできます。管理者ユーザーとして PowerProtect Data Manager に SSH セッションを確立します。次に、`[sudo passwd root]` と入力して root パスワードをリセットします。再起動する必要はありません。

管理者パスワードまたは期限切れのパスワードを知らない場合は、カスタマー サポートにお問い合わせください。

管理者パスワードおよび root パスワード両方の期限が切れている場合

期限切れのパスワードを知っている場合は、期限切れのパスワードそれぞれの方法を組み合わせて、PowerProtect Data Manager コンソールで両方のパスワードをリセットできます。

管理者ユーザーとして PowerProtect Data Manager に SSH セッションを確立します。コンソールでは、期限切れの管理者パスワードを入力した後で、新しい管理者パスワードを設定するように求められます。次に、`[su -]` と入力して root ユーザーに変更します。コンソールでは、期限切れの root パスワードを入力した後で、新しい root パスワードを設定するように求められます。

期限切れのパスワードを知らない場合は、カスタマー サポートにお問い合わせください。この解決方法では、PowerProtect Data Manager を再起動する必要があります。

サポート パスワードの期限が切れている場合

期限切れのパスワードを知っている場合は、PowerProtect Data Manager コンソールまたは UI からサポート パスワードをリセットできます。

- コンソールの場合、サポート ユーザーとして PowerProtect Data Manager に SSH セッションを確立します。コンソールでは、期限切れのパスワードを入力した後で、新しいパスワードを設定するように求められます。
- UI の場合、[「オペレーティング システムのパスワードの変更」](#) を参照してください。

期限切れのパスワードは知らなくても、管理者パスワードまたは root パスワードは知っている場合は、次の手順を実行します。

- 管理者パスワードを知っている場合は、コンソールを使用してサポート パスワードをリセットできます。管理者ユーザーとして PowerProtect Data Manager に SSH セッションを確立します。次に、`[sudo passwd support]` と入力してサポート パスワードをリセットします。再起動する必要はありません。

- root パスワードを知っている場合は、vSphere コンソールを使用してサポート パスワードをリセットできます。vSphere コンソールを使用して、root ユーザーとして PowerProtect Data Manager にログインします。次に、「passwd support」と入力してサポート パスワードをリセットします。再起動する必要はありません。

管理者パスワード、root パスワード、期限切れのパスワードのいずれも知らない場合は、カスタマー サポートにお問い合わせください。

管理者、root、およびサポートのパスワードすべての期限が切れている場合

期限切れのパスワードの一部またはすべてを知っている場合は、期限切れのパスワードそれぞれの方法を組み合わせて、PowerProtect Data Manager コンソールからすべてのパスワードをリセットできます。「[管理者パスワードおよび root パスワード両方の期限が切れている場合](#)」の手順を実行した後で、「[サポートパスワードの期限が切れている場合](#)」の手順を実行します。

期限切れのパスワードをすべて知らない場合は、カスタマー サポートにお問い合わせください。

パスワードの期限が切れたオペレーティング システムの影響

Linux オペレーティング システムの管理者ユーザー パスワードと root ユーザー パスワードでは、一方または両方のパスワードの期限が切れると、PowerProtect Data Manager の一部の機能が正しく動作しなくなることがあります。

保護エンジンと Search Engine ノード、Search Engine node オペレーティング システムのパスワードには、期限がありません。システムのみが使用するこれらのパスワードは、PowerProtect Data Manager によって自動的に管理されます。

これらのセクションに記載されていないすべての機能は、パスワードの期限が切れた後も引き続き機能します。

管理パスワードの期限が切れている場合

- ソフトウェア アップデートの事前チェックが失敗し、アップデート プロセスが妨げられます。
- サーバー DR サービス スクリプトは、root ユーザーが実行する必要があります。root ユーザーとしてスクリプトを実行すると、サービス スクリプトの所有権と関連ファイルの所有権が root ユーザーに変更されます。

root パスワードの期限が切れている場合

- PowerProtect Data Manager の再起動後に System Manager を起動できません。root 権限を必要とするシステム操作が失敗します。例えば、有効期限の変更、ネットワーク ポートの解放、ファイル所有権の変更などです。
- ソフトウェア アップデートの事前チェックが失敗し、アップデート プロセスが妨げられます。
- sudo 操作 (マウント、アンマウント、権限や所有権の変更など) がサーバー DR において失敗し、次のような関連操作が妨げられます。
 - NFS から DD Boost、または DD Boost から NFS へのサーバー DR ストレージ ターゲットの変更。
 - 保護ストレージ システム間でのサーバー DR ストレージ ターゲットの変更。
 - ストレージ ターゲットとのパスワードの同期。
 - サーバー DR リストア。
- コンプライアンス検証 Docker サービスとコンプライアンス検証サービスを開始できません。

認証のタイプとセットアップ

次のトピックでは、PowerProtect Data Manager の認証ソースと構成オプションについて説明します。たとえば、外部 ID プロバイダーを構成して使用する方法についてです。

ID プロバイダー s

ID プロバイダーは、対応するロールに対し、PowerProtect Data Manager によってマップできるユーザーおよびグループ データの抽象ソースです。抽象化により、ユーザーおよびロールの管理が簡素化されます。

サポートされる外部の ID プロバイダーリストに加えて、PowerProtect Data Manager にはアプリケーションおよびオペレーティング システム ユーザー用にローカルで定義された ID プロバイダーが含まれます。

PowerProtect Data Manager は、複数のアクティブ ID プロバイダーをサポートします。各 ID プロバイダーには、その ID プロバイダーのすべてのユーザーを識別する一意の関連ドメインがあります。

ユーザーを直接 PowerProtect Data Manager ロールにマッピングすることも、ID プロバイダーのユーザー グループを介してロールにマッピングすることもできます。ID プロバイダーを構成し、ユーザーまたはグループをロールにマッピングしたら、そのユーザーまたはそのグループのユーザーとして PowerProtect Data Manager にログインすることができます。

一部のローカルユーザーの機能は制限されています。たとえば、オペレーティングシステムユーザーはアプリケーション ロールにマップされず、SSH アクセスに制限されます。ローカル ID プロバイダーは、オペレーティングシステムユーザーの追加や削除をサポートしておらず、既存のアカウントのパスワードの変更のみをサポートしています。

サポートされている外部 ID プロバイダー

- LDAP (Lightweight Directory Access Protocol)
- LDAP over SSL (LDAPS)
- Microsoft Active Directory (AD) サーバー
- Microsoft AD server over SSL (AD over SSL)

制限事項

PowerProtect Data Manager では、同じ ID プロバイダー上の複数のドメインまたはフォレストをサポートしていません。代わりに、ドメインまたはベースごとに個別に ID プロバイダーを設定します。

外部管理 ID プロバイダー

ユーザー名とパスワードを管理する外部 ID プロバイダーを構成することができます。

管理者ロールおよびセキュリティ管理者ロールのみが外部 ID プロバイダーを管理できます。[Administration] > [Access Control] ペインを使用して ID プロバイダーおよびロールの管理を行います。

各外部 ID プロバイダーに関連づけられているドメインでは、大文字と小文字が区別されています。外部 ID プロバイダーのユーザーがログインをする場合は、ID プロバイダーの構成時と同じ大文字と小文字を使用してドメインを指定します。そうでない場合、次のようなエラーメッセージが表示されることがあります：500: Resources cannot be retrieved.

外部 ID プロバイダーの構成

外部 ID プロバイダーを構成できるのは、管理者ロールとセキュリティ管理者ロールのみです。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Directory Settings] タブをクリックします。
PowerProtect Data Manager は、構成済みの ID プロバイダーのリストを表示します。
3. [Add] をクリックします。
[Add Directory] ウィンドウが表示されます。
4. 次の属性を設定します。

表 8. ID プロバイダー属性

属性	説明
[サーバーのタイプ]	サポートされている ID プロバイダータイプを選択します。
[サーバー アドレス]	ID プロバイダーのホスト名または IP アドレスを入力します。プロトコル プレフィックスは必要ありません。
[セキュアな接続]	ID プロバイダーが、LDAPS や AD over SSL などのセキュアな接続方法を使用する場合は、この属性を選択します。この属性を選択すると、証明書の検証コントロールが有効になります。
[ポート]	ID プロバイダーのポート番号を入力します。

表 8. ID プロバイダー属性（続き）

属性	説明
[ドメイン]	ID プロバイダーがユーザーを認証するドメインを入力します。例：ldap.example.com。
[ユーザー名]	ディレクトリーへの完全な読み取りアクセス権を持つユーザー アカウントを入力します。ドメインは必要はありません。
[パスワード]	指定されたユーザー アカウントのパスワードを入力します
[グループ検索属性]	ID プロバイダーが階層内のグループ名を検証するために使用する属性名を入力します。
[[グループ メンバー属性]]	ID プロバイダーが階層内のグループ メンバーを検証するために使用する属性名を入力します。
[グループ検索ベース]	検索をデフォルト ベースから開始しない場合は、検索を開始するベースの名前を入力します。例えば、ドメインが ldap.example.com の場合は、admin と入力して、admin.ldap.example.com から検索を開始します。そうでない場合は、この属性を空のままにします。単一の検索ベースのみに対応しています。

必要に応じて、この表のデフォルト値を適切なフィールドに入力します。

表 9. デフォルトの属性値

属性	値または形式	
	AD および AD over SSL	LDAP および LDAPS
[ポート]	<ul style="list-style-type: none"> セキュアでない接続の場合、デフォルトのポート番号は 389 です。 セキュア接続の場合、デフォルトのポート番号は 636 です。 	
[グループ検索属性]	sAMAccountName	cn
[[グループ メンバー属性]]	メンバー	memberUid

5. セキュアな接続方法を選択した場合：

- a. [検証] をクリックします。
- b. [Verify Certificate] ウィンドウで、ID プロバイダー TLS 証明書の詳細を確認し、[Accept] をクリックします。

メモ: LDAPS プロトコルを指定すると、PowerProtect Data Manager は ID プロバイダーに接続するために必要な証明書を自動的にダウンロードします。ダウンロードが完了すると、[Certificate Validation] フィールドが表示されます。[Verify] をクリックして、表示されている証明書の情報と想定される証明書の情報を比較します。証明書が一致している場合は、[Accept] をクリックして、セットアップを続行します。一致しない場合は、[Cancel] をクリックして、セットアップをキャンセルします。

6. [保存] をクリックします。

次の手順

ID プロバイダーグループをロールに割り当てます。手順については、「ID プロバイダーグループからロールへのマッピングの追加」のセクションを参照してください。ユーザーまたはグループをロールにマッピングしないと、外部ユーザーとしてログインすることができません。

各外部 ID プロバイダーに関連づけられているドメインでは、大文字と小文字が区別されています。外部 ID プロバイダーのユーザーがログインをする場合は、ID プロバイダーの構成時と同じ大文字と小文字を使用してドメインを指定します。そうでない場合、次のようなエラー メッセージが表示されることがあります：500: Resources cannot be retrieved.

外部 ID プロバイダーの編集

外部 ID プロバイダーを編集できるのは、管理者ロールとセキュリティ管理者ロールのみです。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。

2. [Directory Settings] タブをクリックします。
PowerProtect Data Manager は、構成済みの ID プロバイダーのリストを表示します。
3. ID プロバイダーの詳細情報を表示するには、その ID プロバイダーにある [Details] 列の ⓘ をクリックします。
PowerProtect Data Manager によって [Details] ペインが開き、ID プロバイダーの構成に関する情報が表示されます。
4. ID プロバイダーを選択して [Edit] をクリックします。
5. 必要に応じて属性を編集します。
6. [保存] をクリックします。

外部 ID プロバイダーの削除

外部 ID プロバイダーを削除できるのは、管理者ロールとセキュリティ管理者ロールのみです。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Directory Settings] タブをクリックします。
PowerProtect Data Manager は、構成済みの ID プロバイダーのリストを表示します。
3. 削除する ID プロバイダーを選択し、[Delete] をクリックします。

例 : ADID プロバイダーの構成

この例では、*ad.forest1.org* という名前の AD サーバーに、*TestGroup_99* という AD グループがあります。*TestGroup_99* には、Meghan、Patrick、Liam の 3 人のユーザーが含まれています。これらのユーザーには、ユーザー ロールに割り当てられている権限による PowerProtect Data Manager UI へのアクセスが必要です。

AD 構成のプロパティを表示する

AD 構成のプロパティを表示するには、AD Explorer プログラムなど、サードパーティ製ツールを使用します。

この AD 構成に基づいて、PowerProtect Data Manager LDAP 構成オプションに次のような値を指定します。

- ドメイン : **forest1.org**
- サーバー アドレス : **ad.forest1.org**

ad.forest1.org の構成 ID プロバイダー

次の図は、*ad.forest1.org* ID プロバイダーの構成に必要なグループ属性の例を示しています。

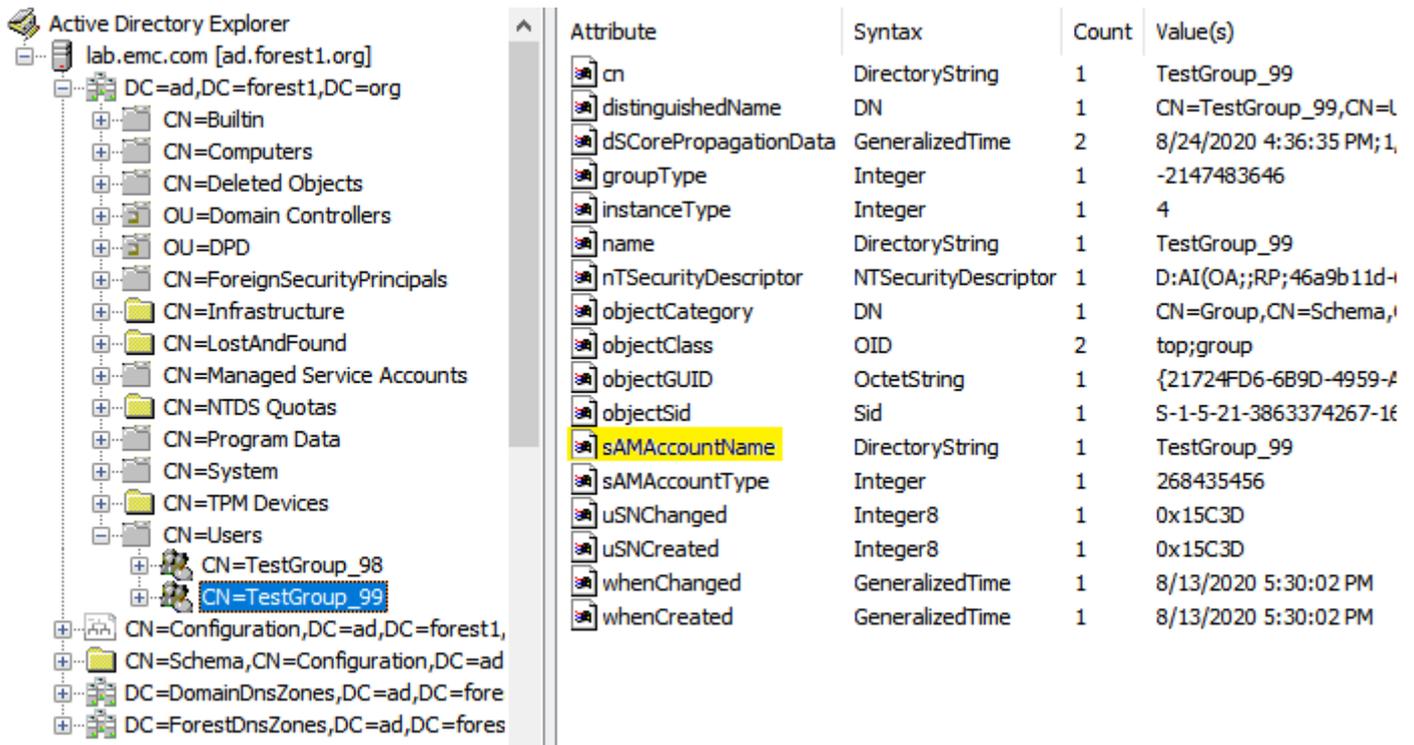


図 1. AD Explorer での AD グループのプロパティ

TestGroup_99 のプロパティに基づいて、LDAP 構成オプションに次のような値を指定します。

- グループ検索属性：sAMAccountName

例：LDAPID プロバイダーの構成

この例では、alberta.lss.emc.com という LDAP サーバに、AlbertaAllGroups というグループがあります。AlbertaAllGroups には 3 人の LDAP ユーザー alberta_user1、alberta_user2、alberta_user3 が含まれています。これらのユーザーには、ユーザー ロールに割り当てられている権限による PowerProtect Data Manager UI へのアクセスが必要です。

LDAP 構成プロパティを表示する

LDAP 構成のプロパティを表示するには、LDAP Admin プログラムなど、サードパーティ製ツールを使用します。

この構成に基づいて、LDAP 構成オプションに次のような値を指定します。

- ドメイン：alberta.emc.com
- サーバー アドレス：alberta.lss.emc.com
- グループ検索属性：cn
- グループ メンバー属性：uniqueMember

LDAP 構成に関する問題のトラブルシューティング

このセクションでは、認証用に外部 ID プロバイダーを構成するときに表示されることがあるエラーメッセージについて説明します。

LDAP 構成のエラーの詳細については、次を参照してください。

http://wiki.servicenow.com/index.php?title=LDAP_Error_Codes#gsc.tab=0.

ユーザー資格情報が正しくない

次のメッセージは、指定したユーザー資格情報が正しくない場合に表示されます。

```
Error Code: 49: Invalid credentials
```

この課題を解決するには、[User Name] フィールドおよび [Password] フィールドの値が正しいことを確認してください。

ドメインが正しくない

[Domain] フィールドが正しくない場合は、次のいずれかのメッセージが表示されます。

- Error Code: 32: No such object exists.
- Error Code: -3: LDAP error: Invalid name: [invalidName].
- LdapIdentitySource cannot have an empty base.
- Error Code: 34: An invalid DN syntax.

この課題を解決するには、[Domain] フィールドの値が正しいことを確認します。

[Server Address] フィールドの形式が正しくない場合

次のいずれかのメッセージは、[Server Address] フィールドの形式が正しくない場合に表示されます。

- Error Code: 2: Protocol error
- Error Code: -3: LDAP error: Cannot parse url: [url]

この問題を解決するには、[Server Address] フィールドがプロトコルプレフィックスなしで入力されていることを確認します。ホスト名または IP アドレスのみを入力します。

外部システムの認証

次のトピックでは、PowerProtect Data Manager が他のコンポーネントと通信し、認証する方法について説明します。

認定資格セキュリティ

PowerProtect Data Manager ロックボックスでは、既知のシークレットを一元的な場所に安全に格納します。

ロックボックスに格納されているすべてのシークレットは暗号化されます。アクティビティにロックボックスからの情報が必要な場合、要求元のプロセスはロックボックスのパスフレーズを提供し、必要な情報を復号化された形式で受信します。

ロックボックスは次のようなシークレットを保持します。

- ローカルユーザーアカウントの認証情報
- アプライアンスの構成時に入力した保護ストレージの認証情報。
- アプリケーション エージェントが保護された資産を認証するために使用する認証情報。

PowerProtect Data Manager は、ロックボックスの中身を保護するために、導入時に強力な一意のパスフレーズを作成します。導入後、PowerProtect Data Manager は、ユーザーの操作なしでロックボックスパスフレーズを自動的に暗号化して管理します。自動管理を使用すると、サポートされているリリースからアップデートする際に、ロックボックスのパスフレーズを入力する必要がなくなります。Server DR バックアップは、ロックボックスとその中身を保護します。

File System agent はまた、保護対象ホスト上の個別のロックボックスを使用して、アプリケーション エージェントが外部ストレージインフラストラクチャにアクセスするために使用する認証情報などの機密情報を格納します。

Kubernetes の場合、PowerProtect Data Manager は、保護操作に必要な証明書と認証情報を Kubernetes クラスター上のシークレットリソースに格納します。このシークレットリソースの暗号化を有効にする方法の詳細については、「[Kubernetes のドキュメント](#)」を参照してください。

リモートコンポーネントの認証

PowerProtect Data Manager ロックボックスでは、既知のシークレットを安全に保存します。これらのシークレットには、ソフトウェアの構成時に指定したユーザー アカウントと保護ストレージの認証情報が含まれています。

認定資格セキュリティ ロックボックスの詳細が記載されています。

PowerProtect Data Manager では、保存された認証情報を複数のコンテキストで使用することができます。「Consumer」という用語は、アプライアンスが任意の目的のために、資格情報を使用する場所を意味します。例：

- ユーザー名とパスワードは、1つの個別のホストまたは資産に適用することができます。この場合、ホストまたは資産は Consumer です。
- すべての資産が同じユーザー名とパスワードで認証される場合は、同じ保護ポリシーのすべての資産に同じ資格証明を適用することもできます。この場合、そのポリシーに基づいてクレデンシャルが資産に適用される場合でも、保護ポリシーは Consumer です。

保存された認証情報は、PowerProtect Data ManagerUI または REST API を使用して管理することができます。

認定資格の追加

ストレージ ターゲット、資産、資産ソースなどの外部システムにアクセスするために必要な認証情報を PowerProtect Data Manager に提供します。保護ポリシーの作成時に、認証情報を追加することもできます。

手順

1. 左ナビゲーション ペインで、[管理] > [認証情報] の順に選択します。
[[認証情報]] ウィンドウが表示されます。
2. [Add] をクリックします。
[Add Credential] ダイアログ ボックスが開きます。
3. 認証情報の名前を入力する。
認定資格の名称は、目的と使用方法を明確に示している必要があります。
4. ドロップダウン リストから認定資格のタイプを選択します。
認定資格のタイプによって、残りのフィールドが決定されます。たとえば、ユーザー名とパスワード、トークン、キーなどです。
5. 選択したタイプに応じて、残りのフィールドに入力します。
6. [保存] をクリックします。
PowerProtect Data Manager はキーストアに認証情報を追加します。

認定資格の使用状況の表示

保存されている各認定資格について、その認定資格を使用しているアイテムのリストを表示することができます。

手順

1. 左ナビゲーション ペインで、[管理] > [認証情報] の順に選択します。
[[認証情報]] ウィンドウが表示されます。
2. 保存された認証情報のリストで認定資格を見つけます。
フィルターおよび列のソート オプションを使用して、認証情報のリストを整理します。
3. リストから認定資格を選択します。
その認定資格の [Consumer Count] 列を確認します。カウントがゼロの場合、認定資格はどこでも使用されません。
4. [Consumer Count] 列で数を選択します。
[Details] ペインが開き、選択した認定資格を使用する Consumer のリストが表示されます。リストには、タイプ別にアイテムがグループ化されます。たとえば、資産、保護ポリシー、ストレージ ターゲットなどです。

認定資格の編集

認定資格の名称、または保存されているユーザー名やパスワードなどの認証の詳細を変更することができます。認定資格のタイプを変更することはできません。

手順

1. 左ナビゲーション ペインで、[管理] > [認証情報] の順に選択します。
[[認証情報]] ウィンドウが表示されます。
2. 保存された認証情報のリストで認定資格を見つけます。
フィルターおよび列のソート オプションを使用して、認証情報のリストを整理します。
3. リストから認定資格を選択して、[Edit] をクリックします。
[Edit Credential] ダイアログ ボックスが表示されます。
4. 任意の適切な値を変更します。
使用可能な値は、認定資格のタイプに依存します。たとえば、ユーザー名とパスワード、トークン、キーなどです。
5. [保存] をクリックします。
PowerProtect Data Manager は、保存されている認定資格を更新します。

認証情報の削除

使用されなくなった、または不要になったすべての認証情報を削除することができます。認定資格を削除すると、監査ログにエントリーが作成されます。

前提条件

認証情報は、すべての場所で使用することができません。認定資格の使用状況と、消費者数がゼロであることを確認します。必要に応じて、保護ポリシーや資産など、認証情報を使用するすべてのものを更新します。

手順

1. 左ナビゲーション ペインで、[管理] > [認証情報] の順に選択します。
[[認証情報]] ウィンドウが表示されます。
2. 保存された認証情報のリストで認定資格を見つけます。
フィルターおよび列のソート オプションを使用して、認証情報のリストを整理します。
3. リストから認定資格または認証情報を選択します。
4. [Consumer Count] 列では Consumer がゼロになっていることを確認します。
カウントがゼロの場合、認定資格はどこでも使用されていないので、認定資格を削除することができます。選択されたすべての認証情報の Consumer がゼロの場合、[Delete] ボタンがアクティブになります。
5. [Delete] をクリックします。
6. [OK] をクリックして、削除を確認します。
PowerProtect Data Manager は、認定資格を削除します。

保護エンジンおよび Search Engine ノード, Search Engine node の認証

保護エンジンと Search Engine ノード, Search Engine nodes は、別個に存在する仮想マシン, virtual machines ですが、PowerProtect Data Manager の制御下にあります。

これらのコンポーネントは、その機能上、外部アクセスを許可する IP アドレスを持っています。各コンポーネントには、PowerProtect Data Manager の機能を提供し、トラブルシューティングを行うためにのみ使用される管理者ユーザー アカウントと root ユーザー アカウントがあります。例えば、Search Engine ノード, Search Engine node 管理者ユーザー アカウントを使用すると、PowerProtect Data Manager により、各ノードでさまざまな操作を実行できます (ノードの正常性ステータスの取得など)。

これらのアカウントのパスワード管理ポリシーは、5 分以内に試行が 3 回失敗すると、管理者ユーザー アカウントのロックが行われるように設定されています。管理者ユーザー アカウントのロック中にコンポーネントにアクセスをしようとすると、アカウントがロックをされたままになる時間が長くなります。

管理者の認証情報を使用して保護エンジンまたは Search Engine ノード, Search Engine node にアクセスができるパブリック インターフェイスはありません。これらのコンポーネントに対して必要な操作には、すべて PowerProtect Data Manager UI を使用します。

保護エンジンまたは Search Engine ノード, Search Engine node 認証情報の取得

保護エンジンおよび Search Engine ノード, Search Engine nodes の管理ツールは、PowerProtect Data Manager で提供されています。その管理ツールを使用して、これらのコンポーネントの認証情報を取得します。

このタスクについて

ここでの用語保護エンジンには、VM Direct エンジン、NAS 保護エンジン、Kubernetes 保護エンジンを含みます。

手順

1. PowerProtect Data Manager コンソールに接続し、root ユーザーに変更します。
2. 環境変数を次のように設定します。

```
source /opt/emc/vmdirect/unit/vmdirect.env
```

3. 保護エンジンの認証情報を次のように取得します。

```
/opt/emc/vmdirect/bin/vproxymgmt get -secret
```

多数の保護エンジンがある環境では、次のように保護エンジン ID を指定して結果を絞り込むことができます。

```
/opt/emc/vmdirect/bin/vproxymgmt get -vproxy_id <id> -secret
```

```
Total '2' vProxies VMs available.
```

```
VProxy ID: f102c755-d084-4425-a151-a0ade4d1a4c7
```

```
Type: Embedded
```

```
Hostname: localhost
```

```
Disabled: false
```

```
Status: Ready
```

```
Protection Type: VM
```

```
VM Configured Capacity Units: 16
```

```
VM Capacity Units in use: 0
```

```
VM Control Sessions in use: 0
```

```
VM Transport Sessions in use: 0
```

```
VProxy ID: 7bb57817-588f-46cc-b6ac-0dbf357dff92
```

```
Type: External
```

```
Hostname: vmdirect.test.emc.com
```

```
Disabled: false
```

```
Status: Ready
```

```
Protection Type: VM
```

```
VCenter inventory source ID: 28d387df-452f-5992-820a-720e6c6a60fe
```

```
VCenter: vcenter.test.emc.com
```

```
VM Name: vproxy-vmdirect
```

```
AdminCredentials-Username: 'admin' Password: '%%%%%%%%'
```

```
RootCredentials-Username: 'root' Password: '%%%%%%%%'
```

```
VM Configured Capacity Units: 100
```

```
VM Capacity Units in use: 0
```

```
VM Control Sessions in use: 0
```

```
VM Transport Sessions in use: 0
```

保護エンジンの認証情報を記録します。

4. Search Engine ノード, Search Engine node の認証情報を次のように取得します。

```
/opt/emc/vmdirect/bin/infranodemgmt get -secret
```

多数の Search Engine ノード, Search Engine nodes がある環境では、次のように Search Engine ノード, Search Engine nodeID を指定して結果を絞り込むことができます。

```
/opt/emc/vmdirect/bin/infranodemgmt get -node_id <id> -secret
```

```
Total '1' node VMs available.
```

```
Node ID: 14c16c75-2c8b-4dff-b93c-d95bdba5a1f6
```

```
Node Type: SearchNode
```

```
Hostname: search.test.emc.com
```

```
Disabled: false
```

```
Status: Ready
```

```
VM Name: search
```

```
VCenter inventory source ID: 3f94030f-090d-5439-a426-ce9945e8cd89
```

```
VCenter: vcenter.test.emc.com
```

```
AdminCredentials-Username: 'admin' Password: '%%%%%%%%'
```

```
RootCredentials-Username: 'root' Password: '%%%%%%%%'
```

Search Engine ノード, Search Engine node の認証情報を記録します。

Search Engine ノード, Search Engine node 認証情報のリセット

vCenter コンソールを使用して、Search Engine ノード, Search Engine node 管理者ユーザーの認証情報のリセットをすることができます。vCenter コンソールを使用して Search Engine ノード, Search Engine node にアクセスをする前に、ユーザー アカウントがロックをされている理由を確認します。

このタスクについて

このタスクに関連する Search Engine のトラブルシューティングについては、『PowerProtect Data Manager 管理およびユーザー ガイド』を参照してください。

手順

1. Search Engine ノード, Search Engine node の root 認証情報を取得します。 [保護エンジンまたは Search Engine ノード, Search Engine node 認証情報の取得](#) で手順を参照してください。
2. Search Engine ノード, Search Engine node が導入されている vCenter Server にログインをします。
3. vSphere Client ホーム ページの左ペインにある [VMs and Templates] ビューから Search Engine ノード, Search Engine node を選択します。
4. Search Engine ノード, Search Engine node の仮想マシン, virtual machine vCenter コンソールを起動します。
5. root 認証情報を使用して Search Engine ノード, Search Engine node にログインをします。
6. 管理者ユーザー アカウントの認証情報のリセットを行います。

```
/sbin/pam_tally2 --user admin --reset
```

許可では、PowerProtect Data Manager によって認証済みユーザーまたは外部システムをアクセスまたはアクセス権のレベルにマッピングする方法を説明します。大まかに言うと、認証ではユーザーが実行できることを説明します。

トピック：

- デフォルトの許可
- 外部との許可の関連付け
- RBAC (ロール ベースのアクセス制御)
- 権限の範囲
- リソースとリソース グループ

デフォルトの許可

ユーザーを許可する場合、またはユーザーをロールやグループに追加する場合は、次のユーザー、グループ、ロールに関する考慮事項に留意してください。

デフォルト管理ユーザー

デフォルトの管理者ユーザーには PowerProtect Data Manager の導入時に管理者ロールが事前に割り当てられます。

デフォルト管理ユーザーは、PowerProtect Data Manager に対するスーパー ユーザーの制御を持ち、削除できません。ただし、デフォルトの管理ユーザーの属性を変更することはできません。

Oracle グループのユーザー

Oracle グループのユーザーは、ロックボックス構成ファイルを削除する権限を持っていることに注意してください。データ ロスを防ぐため、このグループには信頼できるユーザーのみを追加してください。

外部との許可の関連付け

このセクションでは、PowerProtect Data Manager の許可を ID プロバイダーベースのサブジェクトに接続する方法を説明します。

外部 ID プロバイダーグループを追加できるのは、管理者とセキュリティ管理者のロールのみです。

外部 ID プロバイダーユーザーを関連づける前に、外部 ID プロバイダーグループを構成します。外部 ID プロバイダーで、このグループに PowerProtect Data Manager ユーザーを追加します。

ID プロバイダーグループに対して PowerProtect Data Manager ロールのマッピングをすると、マッピングによってグループ内のすべてのユーザーにそのロールが付与されます。

ID プロバイダーグループからロールへのマッピングの追加

ID プロバイダー group-to-role マッピングを追加できるのは、管理者ロールとセキュリティ管理者ロールのみです。

前提条件

この手順には、特定のタスクを実行する許可を委任するためのロール割り当てプロセスが含まれています。システム定義ロールのリストを確認し、必要なすべてのロールを特定します。

この手順では、このロール割り当てで操作を行う権限の範囲を定義することもできます。適用する範囲について計画を立て、必要なリソース グループを作成します。権限の範囲の作成はオプションです。許可はすべての資産に割り当てることができます。

メモ: 特定のリソース グループに対して、バックアップ管理者、管理者のリストア、ユーザーのロールのみを制限できます。管理者およびセキュリティ管理者のロールは、すべてのリソースに対するフル アクセス権があります。

このタスクについて

メモ: Windows Active Directory からの Protected Users グループのマッピングはサポートされていません。このグループにマッピングを追加した場合、そのメンバーは PowerProtect Data Manager にログインをすることができません。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Users/Groups] タブをクリックします。
PowerProtect Data Manager は、関連するロールを含む、設定済みのユーザー アカウントおよび外部 ID プロバイダーグループのリストを表示します。
3. [Add User/Group] をクリックします。
[User Type] タブで [Add User/Group] ウィンドウが開きます。
4. [AD/LDAP User Group] を選択します。
5. グループからロールへのマッピングを追加する ID プロバイダーに対応するドメインを選択します。
6. [Groups] で ID プロバイダーグループの名称を入力します。
PowerProtect Data Manager は ID プロバイダーを検索し、一致するグループを表示します。
7. 結果のリストから 1 つ以上のグループを選択します。
8. [次へ] をクリックします。
[Add User/Group] ウィンドウが [Role] タブに移動します。
9. 1 個以上の適切なロールを選択します。
各ロールの許可のリストを表示するには、[>] をクリックします。次のタブで、各ロールの適用範囲をさらに絞り込むことができます。
10. [次へ] をクリックします。
[Add User/Group] ウィンドウが [Resources] タブに移動します。
11. ロールごとに、そのロールの許可を [All Assets] に適用するか、[Selected Resource Groups] に適用するかを選択します。
選択したリソース グループにのみ許可を適用すると、権限の範囲が作成されます。
[Selected Resource Groups] を選択した場合は、リソース グループのリストが表示されます。
 - a. 使用可能なリソース グループを 1 個以上選択します。
 - b. 選択したリソース グループをリストから削除するには、そのリソース グループの [X] をクリックします。
12. [次へ] をクリックします。
[Add User/Group] ウィンドウが [Summary] タブに移動します。
13. 選択内容を確認し、エラーがあれば修正して、[Finish] をクリックします。

タスクの結果

新しいグループが、構成されたユーザー アカウントとグループのリストに表示されます。

ID プロバイダーグループからロールへのマッピングの変更

ID プロバイダーグループからロールへのマッピングを変更できるのは、管理者ロールとセキュリティ管理者ロールのみです。

前提条件

この手順には、特定のタスクを実行する許可を委任するためのロール割り当てプロセスが含まれています。システム定義ロールのリストを確認し、必要なすべてのロールを特定します。

この手順では、このロール割り当てで操作を行う権限の範囲を定義することもできます。適用する範囲について計画を立て、必要なリソース グループを作成します。権限の範囲の作成はオプションです。許可はすべての資産に割り当てることができます。

メモ: 特定のリソース グループに対して、バックアップ管理者、管理者のリストア、ユーザーのロールのみを制限できます。管理者およびセキュリティ管理者のロールは、すべてのリソースに対するフル アクセス権があります。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Users/Groups] タブをクリックします。
PowerProtect Data Manager は、関連するロールを含む、設定済みのユーザー アカウントおよび外部 ID プロバイダーグループのリストを表示します。
3. 任意のグループの  をクリックすると、次の情報が表示されます。
 - グループ名
 - グループ タイプ
 - グループ ロール
 - グループがマッピングされた日付
4. 編集するグループを選択して、[Edit] をクリックします。
[User Type] タブで [Edit User/Group] ウィンドウが開きます。
5. [User Type] タブの情報を確認します。
ドメインとグループ名は読み取り専用です。
6. [次へ] をクリックします。
[Edit User/Group] ウィンドウが [Role] タブに移動します。
7. 1 個以上の適切なロールを選択します。
各ロールの許可のリストを表示するには、[>] をクリックします。次のタブで、各ロールの適用範囲をさらに絞り込むことができます。
8. [次へ] をクリックします。
[Edit User/Group] ウィンドウが [Resources] タブに移動します。
9. ロールごとに、そのロールの許可を [All Assets] に適用するか、[Selected Resource Groups] に適用するかを選択します。
選択したリソース グループにのみ許可を適用すると、権限の範囲が作成されます。
[Selected Resource Groups] を選択した場合は、リソース グループのリストが表示されます。
 - a. 使用可能なリソース グループを 1 個以上選択します。
 - b. 選択したリソース グループをリストから削除するには、そのリソース グループの [X] をクリックします。
10. [次へ] をクリックします。
[Edit User/Group] ウィンドウが [Summary] タブに移動します。
11. 選択内容を確認し、エラーがあれば修正して、[Finish] をクリックします。

タスクの結果

構成されたユーザー アカウントとグループのリストに変更が表示されます。

ID プロバイダーグループからロールへのマッピングの削除

ID プロバイダー group-to-role のマッピングを削除できるのは、管理者ロールとセキュリティ管理者ロールのみです。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Users/Groups] タブをクリックします。
PowerProtect Data Manager は、関連するロールを含む、設定済みのユーザー アカウントおよび外部 ID プロバイダーグループのリストを表示します。
3. 削除するグループを選択して、[Delete] をクリックします。
4. [OK] をクリックして、削除を確認します。

RBAC (ロール ベースのアクセス制御)

次のトピックでは、使用できるシステム ロール、各ロールに付随する権限、ロールを使用して権限を認証済みユーザーに割り当てる方法について説明します。また、外部 ID プロバイダーサブジェクトを PowerProtect Data Manager のロールにマッピングする方法も説明します。

ロール

ロールは、ユーザーが一連のタスクの実行に必要な権限と許可を定義します。ユーザーにロールが割り当てられると、ロールに定義されているすべての権限がユーザーに付与されます。

事前定義されたロールを使用すると、最小権限の原則を適用することで、PowerProtect Data Manager 操作へのアクセスを制限できます。 [システムが提供するロールと関連する権限](#) で、共通環境に適用できる組み込みのロールの詳細について説明しています。

ロールは、リソース グループを使用したリソース (バックアップ データやインフラストラクチャ オブジェクトなど) へのアクセスも制御します。 [データストレージのセキュリティ設定](#) で、リソース グループの詳細を説明しており、[権限の範囲](#) で、ロールとリソース グループを使用した情報セキュリティの強化方法について説明しています。

ロールは、ユーザー作成時またはグループ マッピング時にユーザーとグループに割り当てられます。ユーザーまたはグループを編集することで、ロールの割り当てを変更できます。 [ローカル ID プロバイダーユーザーの管理](#) と [外部との許可の関連付け](#) では、手順について説明しています。

1人のユーザーを複数のロールに割り当てることができます。例えば、バックアップ管理者と管理者のリストアの両方のロールを持っているものの、完全なシステム管理権限を持たないユーザーなどです。

使用可能なロールのリストを表示するには、[Administration] > [Access Control] を選択して、[Roles] タブを選択します。このテーブルには、各ロールの簡単な説明と、そのロールを割り当てられているユーザーの数が表示されます。🔍をクリックすると、任意のロールに関連する権限の完全なリストが表示されます。

システムが提供するロールと関連する権限

以降のセクションでは、ユーザーを割り当てることができる組み込みのロールについて説明します。

管理者ロール

システムの管理者ロールは、セットアップ、構成、およびすべての PowerProtect Data Manager 管理機能を担います。管理者ロールは、全組織にわたるあらゆる機能にシステム全体でアクセスできるようにします。PowerProtect Data Manager の導入時に、デフォルトの管理者ロールが1個割り当てられます。システムへのフルアクセスを必要とする組織内のユーザーに、追加の管理者ロールを追加して割り当てることができます。

ユーザーロール

ユーザーロールは、PowerProtect Data Manager ダッシュボードのモニタリング、アクティビティのモニタリング、および通知を担います。ユーザーロールは、アクティビティと操作をモニタリングするために読み取り専用アクセスを可能にします。ダッシュボード アクティビティ、アクティビティ モニター、通知をモニターする組織内のユーザーにユーザーロールを割り当てます。このロールを持つユーザーには、システムを構成したり、バックアップ データにアクセスしたりする機能は不要です。このロールに付与されている権限のほとんどは、読み取り専用です。

セキュリティ管理者ロール

セキュリティ管理者ロールは、ユーザー アカウントとロール、権限、監査ログ、認証ソースを管理する限られたユーザーを対象に定義されています。これらの機能は、管理者ロールとは分けられています。このロールは、日常的な運用を担うことにはないものの、他のユーザーのアクセスにおける安全を確認するセキュリティ上のクリアランスを持つ個人に割り当てることができます。

バックアップ管理者ロール

バックアップ管理者ロールは、バックアップ オペレーションなど、保護タスクの定義、構成、実行を担当します。このアクセスが制限されたロールを持つ個人には、システムの完全な管理者アクセス許可は不要です。これらのユーザーは、システム管理者がす

でに構成したリソースを使用して作業します。バックアップ管理者ロールは資産をバックアップし、資産レベルでコピーを管理できますが、保護ポリシーレベルではバックアップできません。

管理者のリストアロール

管理者のリストアロールは、リストア操作の実行を担います。このアクセスが制限されたロールを持つ個人には、システムの完全な管理者アクセス許可は不要です。これらの個人は、保護ストレージに存在するバックアップと、システム管理者がすでに構成したリソースを使用して作業します。

ロール権限

次の表に、事前定義された各ロールに対応する権限の詳細を示します。[ロール権限の定義](#)では、各権限で許可されるアクティビティの詳細を示します。

表 10. ロール権限

カテゴリ	ロール				
	管理者	ユーザー	セキュリティ管 理者	バックアップ管 理者	管理者のリスト ア
[監視]					
View Alerts	Y	Y	N	Y	Y
Manage Alerts	Y	N	N	Y	Y
View Historical Data	Y	Y	N	N	N
View Activities	Y	Y	N	Y	Y
Manage Activities	Y	N	N	Y	Y
Manage External Notifications	Y	N	N	N	N
Workflow Execution	Y	N	N	N	N
View Protection Activities	Y	Y	N	Y	N
View Recovery Activities	Y	Y	N	N	Y
View System Activities	Y	Y	N	N	N
[セキュリティとシステム監査]					
View Security/System Audit	Y	Y	Y	N	N
Manage Security/System Audit	Y	N	Y	N	N
[ユーザーとセキュリティの管理]					
View User Security	Y	Y	Y	N	N
Manage User Security	Y	N	Y	N	N
[サポートのアシスタンスとログ管理]					
View Diagnostic Logs	Y	Y	N	N	N
Manage Diagnostic Logs	Y	N	N	N	N
[システム管理]					
View System Settings	Y	Y	Y	Y	Y
Manage System Settings	Y	N	N	N	N
[アセット管理]					
View Assets	Y	Y	Y	Y	Y

表 10. ロール権限 (続き)

カテゴリ	ロール				
	管理者	ユーザー	セキュリティ管 理者	バックアップ管 理者	管理者のリスト ア
Manage Assets	Y	N	N	Y	N
View Asset Sources	Y	Y	N	Y	Y
Manage Asset Sources	Y	N	N	N	N
Manage Discovery Jobs	Y	N	N	N	N
View Host	Y	Y	N	Y	Y
Manage Host	Y	N	N	N	Y
View Protection Engines	Y	Y	N	Y	Y
Manage Protection Engines	Y	N	N	N	N
View Search Engines	Y	Y	N	Y	Y
Manage Search Engines	Y	N	N	N	N
Manage Application Agents	Y	N	N	Y	N
[ストレージ管理]					
View Protection Storage Targets	Y	Y	N	Y	Y
Manage Protection Storage Targets	Y	N	N	N	N
View Storage Array	Y	Y	N	Y	Y
Manage Storage Array	Y	N	N	N	N
Manage Network	Y	N	N	N	N
[保護ポリシー]					
View Policies	Y	Y	N	Y	N
Manage Policies	Y	N	N	N	N
[リカバリーおよび再使用の管理]					
Rollback to Production	Y	N	N	N	Y
Recovery to Alternate Location	Y	N	N	N	Y
Export for Reuse	Y	N	N	N	Y
[SLA コンプライアンスの管理]					
View SLA/SLO	Y	Y	N	Y	N
Manage SLA/SLO	Y	N	N	N	N
[コピーの管理]					
View Copies	Y	N	N	Y	Y
Manage Copies	Y	N	N	Y	N
View Retention Range	Y	N	N	Y	N
Manage Retention Range	Y	N	N	N	N
Delete Copies	Y	N	N	N	N
All Copies Search	Y	N	N	N	N

表 10. ロール権限 (続き)

カテゴリ	ロール				
	管理者	ユーザー	セキュリティ管 理者	バックアップ管 理者	管理者のリスト ア
[リソース グループ]					
View Resource Groups	Y	Y	Y	N	N
Manage Resource Groups	Y	N	Y	N	N

ロール権限の定義

システムが提供するロールと関連する権限には、PowerProtect Data Manager の各統合ロールに関連する権限のリストが用意されています。その権限を持つユーザーが実行できる特定のタスクを、権限ごとに次の表に示します。

表 11. 監視権限

権限	タスク
View Alerts	<ul style="list-style-type: none"> アラートと外部通知を表示する。
Manage Alerts	<ul style="list-style-type: none"> アラートと外部通知の作成、公開、キャンセル、無視、昇格、降格を行う。 アラートを確認し、アラートにメモを追加する。
View Historical Data	<ul style="list-style-type: none"> 計画、アレイ、データ ターゲット、データ ソース、容量データに関連するデータの履歴を表示します。
View Activities	<ul style="list-style-type: none"> ジョブを表示する。
Manage Activities	<ul style="list-style-type: none"> アクティビティ リソースを作成、表示、編集、キャンセルする。
Manage External Notifications	<ul style="list-style-type: none"> アラート通知のユーザーの登録または登録解除を行う。
Workflow Execution	<ul style="list-style-type: none"> ワークフローの実行を開始、キャンセルする。 ワークフローの実行のステータスを表示する。
View Protection Activities	<ul style="list-style-type: none"> 保護アクティビティを表示する。
View Recovery Activities	<ul style="list-style-type: none"> リカバリー アクティビティを表示する。
View System Activities	<ul style="list-style-type: none"> システム アクティビティを表示する。

表 12. セキュリティとシステム監査権限

権限	タスク
View Security/System Audit	<ul style="list-style-type: none"> セキュリティ監査関連のイベントとアクティビティを表示する。
Manage Security/System Audit	<ul style="list-style-type: none"> セキュリティ監査関連のイベントとアクティビティを確認する。 イベントとアクティビティの監査/変更ログをエクスポートする。

表 13. サポートのアシスタンスとログ管理権限

権限	タスク
View Diagnostic Logs	<ul style="list-style-type: none"> ログバンドル リソースを表示する。 ログ情報リソースを表示する。 ログソース リソースを表示する。 ログを表示します。
Manage Diagnostic Logs	<ul style="list-style-type: none"> ログバンドル リソースを表示および管理する。 ログソース リソースを表示および編集する。

表 13. サポートのアシスタンスとログ管理権限 (続き)

権限	タスク
	<ul style="list-style-type: none"> ● ログをエクスポートします。

表 14. ユーザーとセキュリティ管理の権限

権限	タスク
View User Security	<ul style="list-style-type: none"> ● ユーザーとロールを表示する。 ● ID プロバイダーおよび AD/LDAP グループを表示する。 ● 外部ホストの TLS 証明書を表示する。 ● 許可リストを表示する。
Manage User Security	<ul style="list-style-type: none"> ● ユーザーを作成、表示、編集、削除する。 ● ロールを表示する。 ● 許可リストを作成、表示、編集、削除する。 ● 外部ホストの TLS 証明書を作成、表示、編集、削除する。 ● ID プロバイダーを作成、表示、編集、削除する。 ● ユーザーグループを作成、表示、編集、削除する。

表 15. システム管理権限

権限	タスク
View System Settings	<ul style="list-style-type: none"> ● サーバー ディザスター リカバリー アーティファクトを表示する。 ● メンテナンス モードを表示する。 ● ライセンス情報を表示する。 ● サーバー ディザスター リカバリー ステータスを表示する。 ● SupportAssist 情報を表示する。 ● ノード、構成 EULA、オペレーティング システム ユーザー、アップデート パッケージ、コンポーネント、構成ステータス、構成ログ、タイムゾーン、状態リソースを表示する。
Manage System Settings	<ul style="list-style-type: none"> ● サーバー ディザスター リカバリーのアクティビティを管理する。 ● SupportAssist ゲートウェイ接続およびその他のテレメトリー通信を管理する。 ● ノード状態リソースを表示および編集する。 ● ライセンス情報を更新します。 ● コンポーネント、構成ステータス、構成ログ、タイムゾーン、状態リソースを表示する。 ● ノード、構成 EULA、オペレーティング システム ユーザー、Lockbox リソースを表示および編集する。 ● アップデート パッケージ リソースを作成、表示、編集、削除する。

表 16. アセット管理権限

権限	タスク
View Assets	<ul style="list-style-type: none"> ● 資産を表示する。
Manage Assets	<ul style="list-style-type: none"> ● 資産を作成、表示、編集、削除する。 ● 保護ポリシーの資産を追加、表示、編集、削除する。 ● 保護された資産の手動バックアップを実行する。
View Asset Sources	<ul style="list-style-type: none"> ● 資産ソースを表示する。
Manage Asset Sources	<ul style="list-style-type: none"> ● 資産ソースを作成、表示、編集、削除する。
Manage Discovery Jobs	<ul style="list-style-type: none"> ● ディスカバリー ジョブを作成、表示、編集、削除する。
View Host	<ul style="list-style-type: none"> ● 資産ホストを表示する。
Manage Host	<ul style="list-style-type: none"> ● 資産ホストを作成、表示、編集、削除する。
View Protection Engines	<ul style="list-style-type: none"> ● 保護エンジンを表示する。

表 16. アセット管理権限 (続き)

権限	タスク
Manage Protection Engines	<ul style="list-style-type: none"> 保護エンジンを作成、表示、編集、削除する。
View Search Engine	<ul style="list-style-type: none"> 検索エンジンを表示する。
Manage Search Engine	<ul style="list-style-type: none"> 検索エンジンを作成、表示、編集、削除する。
Manage Application Agents	<ul style="list-style-type: none"> アプリケーション ホストでエージェントのインストールとアップデートを実行する。

表 17. ストレージ管理権限

権限	タスク
View Protection Storage Targets	<ul style="list-style-type: none"> ストレージ ターゲットを表示する。
Manage Protection Storage Targets	<ul style="list-style-type: none"> ストレージ ターゲットを作成、表示、編集、削除する。
View Storage Array	<ul style="list-style-type: none"> ストレージ アレイを表示する。
Manage Storage Array	<ul style="list-style-type: none"> ストレージ アレイを作成、表示、編集、削除する。
Manage Network	<ul style="list-style-type: none"> ネットワーク インターフェイスを作成してストレージ アレイに割り当てる。

表 18. 保護ポリシー権限

権限	タスク
View Policies	<ul style="list-style-type: none"> すべての保護ポリシーのリストを表示する。 保護ポリシーのストレージ ターゲットを表示する。 保護ポリシーに割り当てられているアクセス可能な資産を表示する。 保護ポリシーのスケジュールを表示する。 保護ポリシーのネットワーキングとその他の詳細オプションを表示する。 ファイルフィルターを表示する。 保護ルールを表示する。 SLA ポリシーを表示する。 ストレージ容量クォータを表示する。 ストリーム数を表示する。 保存期間を表示する。
Manage Policies	<ul style="list-style-type: none"> 保護ポリシーを作成、表示、編集、削除する。 保護ポリシーを無効にする。 スケジュール設定リソースの作成、表示、編集、削除します。 保護ポリシーのストレージ ターゲットを追加、表示、編集する。 保護された資産の手動バックアップを実行する。 ファイルフィルターを作成、表示、編集、削除する。 保護ルールのフィルターを作成、表示、編集、削除する。 SLA ポリシーを割り当てる。 ストレージ容量クォータを割り当てる。 ストリーム数を割り当てる。 保存期間を設定する。

表 19. リカバリーおよび再使用の管理権限

権限	タスク
Rollback to Production	<ul style="list-style-type: none"> 本番環境へのリストア操作を作成、表示、編集、開始する。
Recovery to Alternate Location	<ul style="list-style-type: none"> 代替場所へのリストア操作を作成、表示、編集、開始する。

表 19. リカバリーおよび再使用の管理権限（続き）

権限	タスク
Export for Reuse	<ul style="list-style-type: none"> エクスポートと再利用操作を作成、表示、編集、開始します。

表 20. SLA コンプライアンス管理権限

権限	タスク
View SLA/SLO	<ul style="list-style-type: none"> コンプライアンス結果を表示する。 SLA/SLO ポリシーを表示する。
Manage SLA/SLO	<ul style="list-style-type: none"> 資産コンプライアンス結果のエクスポートを行う。 SLA/SLO ポリシーを作成、表示、編集、削除する。

表 21. コピー管理権限

権限	タスク
View Copies	<ul style="list-style-type: none"> 資産のコピーとバックアップを表示する。
Manage Copies	<ul style="list-style-type: none"> 資産のコピーとバックアップの保存を編集する。 クラウドからのコピーをリコールする。 資産のコピーとバックアップ リコールの保存を編集する。
View Retention Range	<ul style="list-style-type: none"> 保存範囲を表示する。
Manage Retention Range	<ul style="list-style-type: none"> すべてのコピーとバックアップの保存範囲を管理する。
Delete Copies	<ul style="list-style-type: none"> コピーとバックアップを削除する。
All Copies Search	<ul style="list-style-type: none"> 使用可能なコピーとバックアップを管理する。

表 22. リソース グループ権限

権限	タスク
View Resource Groups	<ul style="list-style-type: none"> すべてのリソース グループのリストを表示する。 リソース グループの詳細を表示する。
Manage Resource Groups	<ul style="list-style-type: none"> リソース グループを作成、表示、編集、削除する。

権限の範囲

権限の範囲は、ユーザー、ロール、データ間の完全な関連づけを示すもので、誰がどの操作をどこで実行できるかを表します。このように、権限の範囲はユーザー アクションの境界を設定します。

権限の範囲を定義するには、次の手順を実行します。

1. アクセスを制御する必要があるユース ケースを特定します。
2. ユース ケースごとに、関連するリソースを特定し、対応するリソース グループを作成または編集します。 [リソースとリソースグループ](#) で手順を参照してください。
3. 各ユース ケースで、ユーザーまたはグループごとに必要な操作を特定します。
4. 許可のリストを確認し、各ユーザーまたはグループを適切なロールに対応させます。 [RBAC \(ロールベースのアクセス制御\)](#) で詳細を参照してください。

ユーザーまたはグループでは、ロールの組み合わせが必要になることがあります (ある資産には管理者のリストアで、他の資産にはユーザーなど)。

5. ユーザーとグループに必要なマッピングを追加または編集して、必要なロールを指定します。 [ローカル ID プロバイダーユーザーの管理](#) と [外部との許可の関連付け](#) では、手順について説明しています。

ロールの割り当てプロセス中に、指定したロールを適用するリソース グループを選択します。

- ① メモ:** 特定のリソース グループに対して、バックアップ管理者、管理者のリストア、ユーザーのロールのみを制限できます。管理者およびセキュリティ管理者のロールは、すべてのリソースに対するフル アクセス権があります。

権限の範囲が異なることで、異なる部門やプロジェクトの管理者など、さまざまな状況で同じロールを持つ個人を区別できます。
例：権限の範囲を使用した機密情報の保護と分離 では、実践的な例を示しています。

また、管理者の介入なしでセルフサービス リストアを実行するなど、指名ユーザーが自分のデータをより詳細に制御できるよう権限の範囲を定義することもできます。**例：権限の範囲を指定したセルフサービス リストアの提供** では、実践的な例を示しています。

権限の範囲により、他のユーザーに属するリソースについて知識を得たり、アクセスをしたりすることを制限できます。ユーザーは、権限の範囲に含まれるリソースのみを表示および操作できます。

例：権限の範囲を使用した機密情報の保護と分離

次の例では、ロールとリソース グループで権限の範囲を定義するための実用的な適用方法を示しています。

環境の構成は次のとおりです。

- **Finance、Engineering、HumanResources** と指定された3個の保護ストレージ システム。
- **Payroll、Prototypes、Investigations** と指定された3個の資産ソース。
- 全員が管理者のリストアロールを持つ **Gurpreet、Lisa、Eric** という3人の指名ユーザー。
- 各指名ユーザーは、異なる部門の資産を管理します。

リソース グループがない場合、権限の範囲は定義されません。3人のユーザー全員が、あらゆる資産ソースのバックアップからリストアを行うことができます。これは資産が別の部門に属し、そのバックアップに機密情報が含まれている場合でも可能です。

情報セキュリティを確保するために、**FinDeptRG、EngDeptRG、HRDeptRG** という3個のリソース グループを定義できます。それにより、これらのリソース グループを使用して、ユーザーごとに権限の範囲を個別に作成できます。

表 23. リソース グループ

リソース グループ名	含まれるリソース	
FinDeptRG	財務	給与計算
EngDeptRG	エンジニアリング	Prototypes
HRDeptRG	HumanResources	Investigations

表 24. 権限の範囲

ユーザー	ロール	対象範囲
Gurpreet	管理者のリストア	FinDeptRG
	ユーザー	すべての資産
Lisa	管理者のリストア	EngDeptRG
	ユーザー	すべての資産
Eric	管理者のリストア	HRDeptRG
	ユーザー	すべての資産

依然として3人のユーザーは、同じ組織内で共通のロールを担っています。しかし、個別に範囲を指定することで、ユーザーは別の部門に属するリソースに対してアクションを起こすことができなくなります。

例：権限の範囲を指定したセルフサービス リストアの提供

次の例では、ロールとリソース グループで権限の範囲を定義するための実用的な適用方法を示しています。

環境の構成は次のとおりです。

- **Gurpreet、Lisa、Eric** という3人の指名一般ユーザー。
- **Payroll、Prototypes、Investigations** と指定された3個の資産ソース。
- 各指名ユーザーは、指定された資産ソースのいずれかを所有しており、日常業務のために特別なアクセスを追加する必要はありません。
- システム管理者が保護ポリシーと操作を管理するため、通常、これらの指名ユーザーは PowerProtect Data Manager の操作を行いません。

- これらの指名ユーザーは、システム管理者の支援を受けずに、バックアップから各々の資産のリストアをしたいと考えています。

システム管理者はこのようなリクエストがあるまで、これらの3人のユーザーに慣習的にユーザーロールを割り当てるか、一切アクセス許可を与えていませんでした。ユーザーロールには、バックアップから資産のリストアをする許可がありません。

セルフサービス リストアを有効にするには、各ユーザーに管理者のリストアロールが必要です。しかし、権限の範囲が定義されていない場合、このロールを3人のユーザー全員に提供すると、どのユーザーに属するバックアップへのアクセスも可能になります。

そこで、各ユーザーのリソース グループを定義し、そのユーザーの資産または資産ソースのみを関連づけることで、安全性を担保しつつ、リクエストに応えることができます。各リソース グループでは、権限の範囲を個別に許可して、それらの資産に限定された管理者のリストアロールをユーザーに付与できます。

表 25. リソース グループ

リソース グループ名	含まれるリソース
GurpreetRG	給与計算
LisaRG	Prototypes
EricRG	Investigations

表 26. 権限の範囲

ユーザー	ロール	対象範囲
Gurpreet	管理者のリストア	GurpreetRG
	ユーザー	GurpreetRG
Lisa	管理者のリストア	LisaRG
	ユーザー	LisaRG
Eric	管理者のリストア	EricRG
	ユーザー	EricRG

3人のユーザー全員が PowerProtect Data Manager UI にアクセス可能となり、各々のデータに対してリストア操作を実行できるようになりました。個別の範囲により、各ユーザーは他のすべてのユーザーから分離されます。

リソースとリソース グループ

リソースとは、ユーザーが操作できる PowerProtect Data Manager の資産を指します。

リソース グループは、管理者が許可を適用する関連リソースにタグ付けをすることで、許可を管理および絞り込むことができる構造になっています。リソース グループで、特定のロールを持つユーザーがその権限を行使できる範囲を定義または制限します。

リソース グループを定義した後は、1個以上のリソースをグループに割り当てます。リソース グループには、手動でリソースを割り当てるか、保護ポリシーでリソースを割り当てることができます。リソースは複数のリソース グループに属することができ、リソース グループでは異なるタイプのリソースを使用できます。例えば、所有権や部門でリソースをグループ化できます。

許可は加算されていくため、ユーザー許可は、該当するリソース グループとロールの合算になります。例えば、1人のユーザーに対してある部門のバックアップ管理者と別の部門の管理者のリストアを指定できます。

メモ: リソース グループは、Cloud Snapshot Manager 資産ではサポートされていません。

RBAC ([ロール ベースのアクセス制御](#)) で、ロールと許可の詳細について説明しています。 [権限の範囲](#) で、リソース グループを使用して許可を絞り込む方法について説明しています。

メモ: 特定のリソース グループに対して、バックアップ管理者、管理者のリストア、ユーザーのロールのみを制限できます。管理者およびセキュリティ管理者のロールは、すべてのリソースに対するフル アクセス権があります。

リソース グループの作成

リソース グループを作成すると、リソースが新しいリソース グループと関連づけられます。

前提条件

- リソース グループの表示や変更ができるのは、管理者とセキュリティ管理者のロールのみです。
- 管理者とセキュリティ管理者の両方のロールでは、リソース グループに資産を割り当てる際に、手動で選択するか、すべての資産を選択するオプションを使用できます。
- 管理者ロールのみが、保護ポリシーを選択してリソース グループに資産を割り当てることができます。

このタスクについて

[All Assets] を使用した場合や保護ポリシーで資産を選択した場合、結果として選択される資産の数が非常に多くなる場合があります。資産数は、資産の列挙プロセス中に 10 回更新されます。ほとんどの場合、この動作だけで資産数に含まれているすべての資産を列挙できます。ただし、資産の数が非常に多い場合、UI に一部の数しか表示されないことがあります。このようなケースでは、[Resource Group Configuration] ウィンドウに戻るか、[Summary] ページで数を確認して、最終的な数を確認します。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Resource Groups] タブをクリックします。
PowerProtect Data Manager により、構成済みのリソース グループのリストが表示されます。これには、各グループで保護されているリソースの数が含まれます。
3. リソース グループを追加するには、[New] をクリックします。
[New Resource Group] ウィンドウが開きます。
4. リソース グループの名前と説明を入力します。
5. [Create] をクリックします。
[Resource Group Configuration] ウィンドウが開きます。
[Select Assets] リストでは、有効な資産タイプにつき 1 行が使用され、そのタイプの資産選択を制御するドロップダウン リストがあります。使用可能なオプションは [None]、[All Assets]、[Selected Assets] です。
[Select Assets] リストに選択可能な資産が含まれていない場合は、資産を含む資産ソースを追加します。手順については、*PowerProtect Data Manager 管理およびユーザー ガイド*と各資産ソースのユーザー ガイドを参照してください。
このタスクの残りの手順では、3 個の関連するユース ケースを扱います。
リソース グループから 1 個のタイプの資産をすべて削除するには、次の手順を実行します。
6. ドロップダウン リストを [None] に変更します。
ウィザードに確認メッセージが表示されます。
7. [Save] をクリックします。
ウィザードが [Resource Group Configuration] ウィンドウに戻ります。
1 個のタイプの資産すべてをリソース グループに追加するには、次の手順を実行します。
8. ドロップダウン リストを [All Assets] に変更します。
ウィザードに確認メッセージが表示されます。
9. [Save] をクリックします。
ウィザードが [Resource Group Configuration] ウィンドウに戻り、PowerProtect Data Manager でドロップダウン リストの横に 1 個のタイプの資産数が表示されます。
1 個のタイプで特定の資産を選択し、それらの資産をリソース グループに追加するには、次の手順を実行します。
10. ドロップダウン リストを [Selected Assets] に変更します。
[Select Assets] ダイアログ ボックスが表示されます。このダイアログ ボックスには、ポリシーによる資産の選択と手動による選択のオプションが 2 個表示されます。リソース グループに資産を追加する際は、いずれかまたは両方の方法を使用できます。
11. [次へ] をクリックします。
ウィザードが [Select By Policy] ページに移動します。このページには、このタイプの資産を含むすべての保護ポリシーがリスト表示され、選択した資産の累積リストが表示されます。
12. 保護ポリシーの資産を含める場合は、そのポリシーのスライダーを右に移動させます。
ウィザードで、選択した資産のリストに対応する資産が追加されます。該当するポリシーごとにこの手順を繰り返します。
13. 選択した資産のリストに含まれているコンテンツを確認し、[Next] をクリックします。
ウィザードが、[Manual Selection] ページの [Available Assets] タブに移動します。このタブには、保護されていない (ポリシーによってまだ選択されていない) 資産など、選択したタイプの資産すべてがリスト表示されます。
14. 各行のフィルター、ページング コントロール、チェックボックスを使用し、資産を検索して選択します。
ウィザードに、[Manually Selected] タブのリストに選択した資産が追加されます。該当する資産ごとにこの手順を繰り返します。
15. [Manually Selected] タブをクリックし、リストのコンテンツを確認してから、[Next] をクリックします。

ウィザードが [Summary] ページに移動します。このページには、リソース グループに追加する資産がリスト表示されます。各保護ポリシーの資産数などの選択方法ごとに、資産がそれぞれリスト表示されます。

- [>] をクリックしていずれかのリストを展開し、リスト表示された資産と予想される数を確認してから、[Save] をクリックします。

[Select Assets] ダイアログ ボックスが閉じ、ウィザードが [Resource Group Configuration] ウィンドウに戻ります。

PowerProtect Data Manager により、ドロップダウン リストの横にそのタイプの資産の数が表示されます。

- このタイプで個々の資産の選択を変更するには、[Edit] をクリックします。

リソース グループの資産の選択が完了したら、次の手順を実行します。

- [View Assets] をクリックして、資産タイプに関する選択を確認します。

- [完了] をクリックします。

PowerProtect Data Manager により、新しいリソース グループがリソース グループのリストに追加されます。

リソース グループの編集

リソース グループの名前と説明を変更したり、グループに関連づけられている資産選択を変更したりできます。

前提条件

- リソース グループの表示や変更ができるのは、管理者とセキュリティ管理者のロールのみです。
- 管理者とセキュリティ管理者の両方のロールでは、リソース グループに資産を割り当てる際に、手動で選択するか、すべての資産を選択するオプションを使用できます。
- 管理者ロールのみが、保護ポリシーを選択してリソース グループに資産を割り当てることができます。

このタスクについて

[All Assets] を使用した場合や保護ポリシーで資産を選択した場合、結果として選択される資産の数が非常に多くなる場合があります。資産数は、資産の列挙プロセス中に 10 回更新されます。ほとんどの場合、この動作だけで資産数に含まれているすべての資産を列挙できます。ただし、資産の数が非常に多い場合、UI に一部の数しか表示されないことがあります。このようなケースでは、[Resource Group Configuration] ウィンドウに戻るか、[Summary] ページで数を確認して、最終的な数を確認します。

個別に選択された多数の資産を含むリソース グループを編集しようとすると、504 Gateway Timeout Error という通知が表示されることがあります。このエラーは、資産の選択を編集しようとした際に、[Select Assets] ダイアログ ボックスが開き、[Summary] ページが表示されるために発生します。

リソース グループから資産を削除する際、場合によってはそれらの資産のサブセットが削除されないことがあります。削除操作をしても一部の資産が所定の場所に残っている場合は、すべての不要な資産がリソース グループから削除されるまで操作を繰り返します。

手順

- 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。

[Access Control] ウィンドウが表示されます。

- [Resource Groups] タブをクリックします。

PowerProtect Data Manager により、構成済みのリソース グループのリストが表示されます。これには、各グループで保護されているリソースの数が含まれます。

- リソース グループ内の資産を表示するには、 をクリックします。

[Details] ペインが開き、タイプ別に分類された資産のリストが表示されます。

- リストからリソース グループを選択して、[Edit] をクリックします。

[Resource Group Configuration] ウィンドウが開きます。

[Select Assets] リストでは、有効な資産タイプにつき 1 行が使用され、そのタイプの資産選択を制御するドロップダウン リストがあります。PowerProtect Data Manager では、有効資産タイプのうち選択済みである資産の数がドロップダウン リストの横に表示されます。

各行で使用可能なオプションは [None] [All Assets] [Selected Assets] です。

このタスクの残りの手順では、ドロップダウン リストの現在の状態に応じて、関連するユースケースを扱います。

- リソース グループの名前または説明を変更するには、 をクリックします。

[Edit Resource Group] ウィンドウが開きます。[Save] をクリックして、変更内容を適用します。

リソース グループから1個のタイプの資産をすべて削除するには、次の手順を実行します。

6. ドロップダウン リストを [None] に変更します。
ウィザードに確認メッセージが表示されます。

7. [Save] をクリックします。
ウィザードが [Resource Group Configuration] ウィンドウに戻ります。

1個のタイプの資産すべてをリソース グループに追加するには、次の手順を実行します。

8. ドロップダウン リストを [All Assets] に変更します。
ウィザードに確認メッセージが表示されます。

9. [Save] をクリックします。
ウィザードが [Resource Group Configuration] ウィンドウに戻り、PowerProtect Data Manager でドロップダウン リストの横に1個のタイプの資産数が表示されます。

資産の選択が以前 [None] または [All Assets] であった場合に、特定の資産を選択できるようにするには、次の手順を実行します。

10. 資産の選択が [All Assets] である場合は、ドロップダウン リストを [None] に変更します。
ウィザードによって既存の資産の選択が解除され、特定の資産を選択できるようになります。

11. ドロップダウン リストを [Selected Assets] に変更します。
[Select Assets] ダイアログ ボックスが表示されます。このダイアログ ボックスには、ポリシーによる資産の選択と手動による選択のオプションが2個表示されます。リソース グループに資産を追加する際は、いずれかまたは両方の方法を使用できます。

12. [次へ] をクリックします。
ウィザードが [Select By Policy] ページに移動します。このページには、このタイプの資産を含むすべての保護ポリシーがリスト表示され、選択した資産の累積リストが表示されます。

資産の選択が以前 [Selected Assets] であった場合に、既存の資産を選択できるように変更するには、次の手順を実行します。

13. [編集] をクリックします。
[Select Assets] ダイアログ ボックスが開き、[Summary] ページが表示されます。このダイアログ ボックスには、ポリシーによる資産の選択と手動による選択のオプションが2個表示されます。リソース グループに資産を追加する際は、いずれかまたは両方の方法を使用できます。

14. [Select By Policy] コンテナで [Edit] をクリックします。
ウィザードが [Select By Policy] ページに移動します。このページには、このタイプの資産を含むすべての保護ポリシーがリスト表示され、選択した資産の累積リストが表示されます。

[Select By Policy] ページで資産を選択し、それらの資産をリソース グループに追加するには、次の手順を実行します。

15. 保護ポリシーの資産を含める場合は、そのポリシーのスライダーを右に移動させます。
ウィザードで、選択した資産のリストに対応する資産が追加されます。該当するポリシーごとにこの手順を繰り返します。
16. 保護ポリシーから資産を除外するには、そのポリシーのスライダーを左に移動させます。
ウィザードによって、選択した資産のリストから対応する資産が削除されます。該当するポリシーごとにこの手順を繰り返します。
17. 選択した資産のリストに含まれているコンテンツを確認し、[Next] をクリックします。
ウィザードが、[Manual Selection] ページの [Available Assets] タブに移動します。このタブには、保護されていない (ポリシーによってまだ選択されていない) 資産など、選択したタイプの資産すべてがリスト表示されます。
18. 各行のフィルター、ページング コントロール、チェックボックスを使用して、資産の検索と選択や解除を行います。
ウィザードで [Manually Selected] タブのリストから選択した資産の追加や削除が行われます。該当する資産ごとにこの手順を繰り返します。
19. [Manually Selected] タブをクリックし、リストのコンテンツを確認してから、[Next] をクリックします。
ウィザードが [Summary] ページに移動します。このページには、リソース グループに追加する資産がリスト表示されます。
各保護ポリシーの資産数などの選択方法ごとに、資産がそれぞれリスト表示されます。
20. [>] をクリックしていずれかのリストを展開し、リスト表示された資産と予想される数を確認してから、[Save] をクリックします。

[Select Assets] ダイアログ ボックスが閉じ、ウィザードが [Resource Group Configuration] ウィンドウに戻ります。

PowerProtect Data Manager により、ドロップダウン リストの横にそのタイプの資産の数が表示されます。

21. このタイプで個々の資産の選択を変更するには、[Edit] をクリックします。

リソース グループの資産の選択が完了したら、次の手順を実行します。

22. [View Assets] をクリックして、資産タイプに関する選択を確認します。

23. [完了] をクリックします。

PowerProtect Data Manager により、リソース グループ リストのアップデートが行われ、変更が反映されます。

リソース グループの削除

使用されなくなったリソース グループをすべて削除します。リソース グループを削除する前に、リソース グループを空にする必要があります。

前提条件

- リソース グループの表示や変更ができるのは、管理者とセキュリティ管理者のロールのみです。
- 管理者とセキュリティ管理者の両方のロールでは、リソース グループに資産を割り当てる際に、手動で選択するか、すべての資産を選択するオプションを使用できます。
- 管理者ロールのみが、保護ポリシーを選択してリソース グループに資産を割り当てることができます。

手順

1. 左ナビゲーション ペインで、[Administration] > [Access Control] の順に選択します。
[Access Control] ウィンドウが表示されます。
2. [Resource Groups] タブをクリックします。
PowerProtect Data Manager により、構成済みのリソース グループのリストが表示されます。これには、各グループで保護されているリソースの数が含まれます。
3. リストからリソース グループを選択します。
4. リソース グループの [Assets] 列を確認して、リソース グループが空であることを確かめます。
[Assets] 列の割り当て数は 0 となっている必要があります。リソース グループが空でない場合は、すべての資産を削除します。 [リソース グループの編集](#) で手順を参照してください。
5. リソース グループを削除するには、[Delete] をクリックします。
[OK] をクリックして、削除を確定します。
PowerProtect Data Manager により、リストからリソース グループが削除されます。

ログの設定

トピック：

- 認証サーバーのログ
- ログバンドルの追加
- syslog を使用したサーバーのモニタリング

認証サーバーのログ

認証サーバーには、2種類のログファイルがあります。

- 管理ログ：トラブルシューティングとメンテナンスに使用される情報が含まれています。
- 監査ログ：日付順に表示されるセキュリティ関連の情報が含まれています。

ログバンドルの追加

ログバンドルを追加するには、次の手順を実行します。

このタスクについて

 **メモ:** 最大 10 個のログバンドルを追加できます。

手順

1. PowerProtect Data Manager ユーザー インターフェイスで、 をクリックしてから、[Logs] をクリックします。
2. [Add] をクリックしてログバンドルを追加します。
[Add Log Bundle] ウィンドウが表示されます。
3. ログバンドルのシステム ([データ マネージャー]、[VM ダイレクト エンジン]、または [CDRS] (クラウド DR を導入している場合)) を選択し、ログバンドルの期間を設定し、[保存] をクリックします。
[Jobs] ウィンドウには、ログバンドルの作成の進行状況が表示されます。また、UI の緑色のバナーは、ログバンドルが正常に作成されたことを示します。バナーを無視する場合は、[X] をクリックします。
4. ログバンドルを削除するには、ログバンドルの左のボックスを選択し、[Delete] をクリックします。
[ログ キャパシティ] は、ログ用にディスク上に残っている容量 (GB) とログストレージで使用されているディスクの割合を示します。
5. ログバンドルをダウンロードするには、[Bundle Name] 列で該当するバンドル名をクリックします。

syslog を使用したサーバーのモニタリング

Syslog システム ログ機能によって、システム ログのメッセージが収集され、指定ログファイルに収集されたメッセージが書き込まれます。Syslog 形式でイベント情報を送信するように、PowerProtect Data Manager サーバーを構成できます。

PowerProtect Data Manager は、Syslog サーバーに診断およびモニタリング データを送信する Syslog クライアントとして機能します。このデータにアクセスをして、監査、モニタリング、トラブルシューティングのタスクを実行できます。

Syslog サーバーのファイアウォールは、「[ネットワークおよび通信のセキュリティ設定](#)」にリスト表示されているポートを使用して PowerProtect Data Manager からデータを受信するように構成されています。Syslog サーバーでリスト表示されていないポートを使用している場合は、その章の手順を使用して、PowerProtect Data Manager システム上の対応するポートを開きます。

NTP サーバーを使用するように PowerProtect Data Manager システムを構成することが推奨されています。PowerProtect Data Manager システムの時間を Syslog サーバーと同期するには、NTP 構成が必要です。

選択した重大度レベルは、選択したすべてのコンポーネントに適用されます。各コンポーネントに別個の重大度レベルを適用することはできません。例えば、[Critical] を選択すると、選択したすべてのコンポーネントから重大なメッセージが転送されます。例外として、[OS Kernel] または [PPDM Alert and Audit] を選択すると、選択した重大度レベルに関係なく、対応する監査ログがデフォルトで転送されます。

24 時間の間にログメッセージが転送されない場合、PowerProtect Data Manager によって PowerProtect Data Manager と Syslog サーバーの接続を確かめ、メッセージの交換を妨げる問題がないことを確認するよう促すアラートが生成されます。

Syslog 転送用 TLS の構成

TLS を使用して Syslog サーバーにログを転送するには、PowerProtect Data Manager に Syslog サーバーのセキュリティ証明書が必要です。TLS 接続を有効にするには、次の手順で、PowerProtect Data Manager に Syslog サーバーのセキュリティ証明書のインポートを行います。

前提条件

PowerProtect Data Manager では、デフォルトで anon 認証が使用されています。rsyslog プロトコルがサポートされている別の認証形式 (x509 認証など) を使用する場合は、[カスタマーサポート](#)にお問い合わせください。

手順

1. PowerProtect Data Manager サーバーの `/etc/ssl/certificates/extserver/syslog-server-ca.pem` に Syslog サーバー認証局(CA)の自己署名証明書のコピーを行います。

 **メモ:** ファイル名やパスを変更しないでください。

2. 以下のコマンドを実行します。

```
chown admin:app /etc/ssl/certificates/extserver/syslog-server-ca.pem
```

```
chmod 770 /etc/ssl/certificates/extserver/syslog-server-ca.pem
```

 **メモ:** Syslog サーバーを変更した場合や CA 証明書の期限が切れた場合は、証明書のコピーを再度行います。

Syslog サーバーの構成

Syslog サーバーの有効化、Syslog サーバーの変更、転送されるイベントの変更、Syslog 転送の無効化を行うには、次の手順を使用します。

前提条件

Syslog 接続に TLS を使用するには、次の手順を実行します。

- PowerProtect Data Manager に Syslog サーバーセキュリティ証明書のインポートを行います。
- PowerProtect Data Manager では、デフォルトで anon 認証が使用されています。Syslog サーバーで別の認証形式を使用している場合は、[カスタマーサポート](#)にお問い合わせください。

手順

1. PowerProtect Data Manager UI で  をクリックし、[Logs] を選択してから [Syslog] をクリックします。
[Logs] ウィンドウが開き、[Syslog] ページが表示されます。

Syslog 転送を有効にするには、次の手順を実行します。

2. [Syslog Forwarding] スライダーを右に移動させて、Syslog 転送を有効にします。
3. 次の情報を入力します。
 - [IP Address / FQDN]: Syslog サーバーの IP アドレスまたは完全修飾ドメイン名。
 - [Port]: PowerProtect Data Manager および Syslog サーバーの通信用ポート番号。
 - [Protocol]: 通信に使用するプロトコル (TLS、UDP、TCP)。
 - [Components]: Syslog メッセージコンポーネント。
 - [Severity Level]: Syslog サーバーに転送するメッセージの範囲を指定します。

Syslog サーバーを変更するには、次の手順を実行します。

- PowerProtect Data Manager UI で  をクリックし、[Logs] を選択してから [Syslog] をクリックします。
[Logs] ウィンドウが開き、[Syslog] ページが表示されます。
- 次の Syslog 構成の詳細を変更します。
 - [IP Address / FQDN]: Syslog サーバーの IP アドレスまたは完全修飾ドメイン名。
 - [Port]: PowerProtect Data Manager および Syslog サーバーの通信用ポート番号。
 - [Protocol]: 通信に使用するプロトコル (TLS、UDP、TCP)。

転送されるイベントを変更するには、次の手順を実行します。

- PowerProtect Data Manager UI で  をクリックし、[Logs] を選択してから [Syslog] をクリックします。
[Logs] ウィンドウが開き、[Syslog] ページが表示されます。
- [Components] と [Severity Level] を変更します。
Syslog 転送を無効にするには、次の手順を実行します。
- PowerProtect Data Manager UI で  をクリックし、[Logs] を選択してから [Syslog] をクリックします。
[Logs] ウィンドウが開き、[Syslog] ページが表示されます。
- [Syslog Forwarding] スライダーを左に移動させて、Syslog 転送を無効にします。
次の手順を実行して、変更を適用します。
- [Save] をクリックします。

次の手順

Syslog の構成が完了したら、接続ステータスを確認します。[System Settings] > [Logs] > [Syslog] に移動し、Syslog サーバーの接続ステータスが [Connected] であることを確認します。Syslog サーバーが接続されていない場合、ステータスは [Not Connected] と表示されます。

Syslog 接続のトラブルシューティング

Syslog 接続のトラブルシューティングに関連する次の情報を確認してください。

Syslog サーバーにメッセージが転送されない

ログメッセージは PowerProtect Data Manager サービス ログ ファイルで生成されますが、これらのメッセージは Syslog サーバーに転送されません。このような問題が発生する場合は、次のタスクを実行します。

- PowerProtect Data Manager のファイアウォールで、必要なポートが使用されていることを確認します。Syslog サーバーで別のポートが使用されている場合は、PowerProtect Data Manager システム上の対応するポートを開きます。
- Syslog サーバーのファイアウォールを確認します。ポートがデータを受け入れるように構成されていることを確認します。
- PowerProtect Data Manager と Syslog サーバーの両方のプロトコルが同じであることを確認します。TLS を使用している場合、PowerProtect Data Manager ではデフォルトで anon 認証が使用されています。Syslog サーバーで別の認証形式を使用している場合は、[カスタマー サポート](#)にお問い合わせください。

ネットワークおよび通信のセキュリティ設定

この章では、PowerProtect Data Manager でのネットワーク通信にセキュアなチャネルを使用する方法と、ファイアウォール環境で PowerProtect Data Manager を構成する方法について説明します。

トピック：

- [ポートの使用方法](#)
- [通信セキュリティ設定](#)
- [PowerProtect Data Manager ファイアウォールのサポート](#)

ポートの使用方法

この表では、PowerProtect Data Manager および関連する内部と外部のコンポーネントまたはシステムのポート要件について説明します。PowerProtect Data Manager では、次のリストにないすべてのポートの監査およびブロックが行われます。

DD システムのポートとプロトコルの詳細については、『PowerProtect DD Security 構成ガイド』を参照してください。

表 27. PowerProtect Data Manager のポート要件

ソース システム	デスティネーション システム	ポート	プロトコル	サポートされている TLS	注
バックアップクライアント ^a	DD システム	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
バックアップクライアント ^a	DD システム	2049	独自のプロトコル	TLS 1.2	オプションの DD Boost クライアント TLS 暗号化。
バックアップクライアント ^a	DD システム	2052	TCP	不可	NFS mountd。データ用ではない。
バックアップクライアント	DD グローバル スケール	2053	TCP	TLS 1.2	DD Boost 接続。
バックアップクライアント ^a	PowerProtect Data Manager	8443	HTTPS	TLS 1.2	REST API サービス。
バックアップクライアント	VMAX SE サーバー	2707	独自のプロトコル	TLS 1.2	バックアップクライアントには、VMAX SE サーバーのデフォルトポート 2707 へのアクセスが必要。Storage Direct に適用。
Callhome (SupportAssist)	PowerProtect Data Manager	22	SSH	TLS 1.2	サポートと管理用の SSH。プライベートキーまたはオプションの証明書で暗号化。
Callhome (SupportAssist)	PowerProtect Data Manager	443	HTTPS	TLS 1.2	リモートサポート用の SSH。
ESXi	DD システム ^b	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
ESXi	DD システム ^b	2049	独自のプロトコル	TLS 1.2	NFS データストアと DD Boost。NFS は暗号化されない。DD Boost は暗号化される。
ESXi	DD システム ^b	2052	TCP	不可	NFS mountd。データ用ではない。

表 27. PowerProtect Data Manager のポート要件 (続き)

ソース システム	デスティネーション システム	ポート	プロトコル	サポートされている TLS	注
Kubernetes クラスター	DD システム	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
Kubernetes クラスター	DD システム	2049	独自のプロトコル	TLS 1.2	オプションの DD Boost クライアント TLS 暗号化。
Kubernetes クラスター	DD システム	2052	TCP	TLS 1.2	NFS mountd。データ用ではない。
Kubernetes クラスター	ESXi	902	TCP	TLS 1.2	VMware CSI を使用した PVC 用の vSphere Client アクセス。Tanzu Kubernetes ゲスト クラスターには不要。
Kubernetes クラスター	保護エンジン	9090	HTTPS	TLS 1.2/1.3	Tanzu Kubernetes ゲスト クラスターには必須。
Kubernetes クラスター	vCenter	443	HTTPS	TLS 1.2	vCenter Server を使用する vSphere 用のプライマリ管理インターフェイス (VMware CSI を使用する PVC 用の vSphere Client を含む)。Tanzu Kubernetes ゲスト クラスターには不要。
NAS 保護エンジン	NAS アプライアンス	443	HTTPS	TLS 1.2	Unity および PowerStore のアプライアンス用の管理アクセス。
NAS 保護エンジン	NAS アプライアンス	8080	HTTPS	TLS 1.2	PowerScale/Isilon アプライアンス用の管理アクセス。
PowerProtect Data Manager	バックアップクライアント	7,000	HTTPS	TLS 1.2	Microsoft SQL Server、Oracle、Microsoft Exchange Server、SAP HANA、ファイルシステム。要件は、アプリケーションダイレクトおよび VM Direct に適用されます。
PowerProtect Data Manager	Callhome (SupportAssist)	25	SMTP	TLS 1.2	使用される TLS のバージョンは、メールサーバーによって異なる。可能であれば TLS が使用される。
PowerProtect Data Manager	Callhome (SupportAssist)	465	TCP	TLS 1.2	
PowerProtect Data Manager	Callhome (SupportAssist)	587	TCP	TLS 1.2	
PowerProtect Data Manager	Callhome (SupportAssist)	9443	HTTPS	TLS 1.2	サービス通知用の REST API。
PowerProtect Data Manager	DD システム	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
PowerProtect Data Manager	DD システム	2049	独自のプロトコル	不可	サーバー DR NFS 接続。メタデータ、クライアント名、インデックス作成にのみ使用。バックアップデータには使用されない。
PowerProtect Data Manager	DD システム	2052	TCP/UDP	不可	NFS mountd。データ用ではない。
PowerProtect Data Manager	DD システム	3009	HTTPS	TLS 1.2	構成と検出のために DDMC と通信。

表 27. PowerProtect Data Manager のポート要件 (続き)

ソース システム	デスティネーション システム	ポート	プロトコル	サポートされている TLS	注
PowerProtect Data Manager	ESXi	443	HTTPS	TLS 1.2	ESXi の構成とバージョンにより異なる。
PowerProtect Data Manager	Kubernetes クラスター	6443	独自のプロトコル	TLS 1.2	Kubernetes API サーバーに接続。暗号化は、Kubernetes クラスターの構成によって異なる。PowerProtect Data Manager では TLS 1.2 をサポート。
PowerProtect Data Manager	LDAP サーバー	389	TCP/UDP	不可	セキュリティで保護されていない LDAP ポート、アウトバウンドのみ。暗号化にはポート 636 を使用。
PowerProtect Data Manager	LDAP サーバー	636	TCP	TLS 1.2	LDAPS、使用中の LDAP 構成によって異なる。アウトバウンドのみ。
PowerProtect Data Manager	NAS アプライアンス	443	HTTPS	TLS 1.2	Unity および PowerStore のアプライアンス用の管理アクセス。
PowerProtect Data Manager	NAS アプライアンス	8080	HTTPS	TLS 1.2	PowerScale/Isilon アプライアンス用の管理アクセス。
PowerProtect Data Manager	NAS 共有	139	TCP	TLS 1.2	Windows ファイル サーバー共有 (CIFS)。
PowerProtect Data Manager	NAS 共有	443	HTTPS	TLS 1.2	NetApp 共有 (NFS および CIFS)。NAS 共有検証チェックにも使用される。
PowerProtect Data Manager	NAS 共有	445	TCP	TLS 1.2	Windows ファイル サーバー共有 (CIFS)。
PowerProtect Data Manager	NAS 共有	2049	TCP	TLS 1.2	Linux ファイル サーバー共有 (NFS)。
PowerProtect Data Manager	NTP サーバー	123	NTP	不可	時間の同期化。
PowerProtect Data Manager	PowerProtect Data Manager : カタログ	9760	TCP		内部のみ。ファイアウォールによるブロック。
PowerProtect Data Manager	PowerProtect Data Manager : Configuration Manager	55555	TCP		内部のみ。ファイアウォールによるブロック。
PowerProtect Data Manager	PowerProtect Data Manager : Elastic Search	9200	TCP		内部のみ。
PowerProtect Data Manager	PowerProtect Data Manager : Elastic Search	9300	TCP		内部のみ。
PowerProtect Data Manager	PowerProtect Data Manager : 組み込み VM プロキシ	9095	TCP		内部のみ。ファイアウォールによるブロック。
PowerProtect Data Manager	PowerProtect Data Manager : Quorum ピア	2181	TCP		内部のみ。ファイアウォールによるブロック。
PowerProtect Data Manager	PowerProtect Data Manager : RabbitMQ	5672	TCP		内部のみ。ファイアウォールによるブロック。
PowerProtect Data Manager	PowerProtect Data Manager : Secrets Manager	9092	TCP		内部のみ。
PowerProtect Data Manager	PowerProtect Data Manager : VM Direct イン	9097	TCP		内部のみ。ファイアウォールによるブロック。

表 27. PowerProtect Data Manager のポート要件 (続き)

ソース システム	デスティネーション システム	ポート	プロトコル	サポートされている TLS	注
	フラストラクチャ マネージャー				
PowerProtect Data Manager	PowerProtect Data Manager : VM Direct オペレーション	9096	TCP		内部のみ。ファイアウォールによるブロック。
PowerProtect Data Manager	保護エンジン	22	SSH	TLS 1.2	サポートと管理用の SSH。プライベートキーまたはオプションの証明書で暗号化。
PowerProtect Data Manager	保護エンジン	9090	HTTPS	TLS 1.2	REST API サービス。
PowerProtect Data Manager	保護エンジン	9613 ^c	独自のプロトコル	TLS 1.2	
PowerProtect Data Manager	Reporting Engine	9002	TCP	TLS 1.2	REST API サービス。
PowerProtect Data Manager	Search Engine	9613 ^c	独自のプロトコル	TLS 1.2	Search Engine ノード, Search Engine nodes のインフラストラクチャ ノードエージェントの管理。
PowerProtect Data Manager	Search Engine	14251	独自のプロトコル	TLS 1.2	検索クエリ REST API エンドポイント。
PowerProtect Data Manager	SMI-S	5989	HTTPS	TLS 1.2	SMI-S プロバイダーと通信。検出します。
PowerProtect Data Manager	Storage Direct システム	3009	HTTPS	TLS 1.2	検出します。
PowerProtect Data Manager	Syslog サーバ	514	TCP/UDP	TLS 1.2	Syslog サーバへのログ転送。
PowerProtect Data Manager	Syslog サーバ	6514	TCP	TLS 1.2	Syslog サーバへのログ転送。
PowerProtect Data Manager	Syslog サーバ	10514	TCP	TLS 1.2	Syslog サーバへのログ転送。
PowerProtect Data Manager	UI	443	HTTPS	TLS 1.2	ブラウザ ホストと PowerProtect Data Manager システムとの間。
PowerProtect Data Manager	Update Manager UI	14443	HTTPS	TLS 1.2	アップデート パッケージを含んだホストを PowerProtect Data Manager システムに接続。
PowerProtect Data Manager	vCenter	443	HTTPS	TLS 1.2	ダイレクト リストア、検出、ホットアド転送モードの開始、インスタント アクセス リストアを含む リストア用の vSphere API。vCenter 構成により異なる。
PowerProtect Data Manager	vCenter	7444	独自のプロトコル	TLS 1.2	vCenter シングル サインオン
PowerProtect Data Manager	VMAX Solutions Enabler サーバ	2707	独自のプロトコル	TLS 1.2	Storage Direct の機能。PowerProtect Data Manager では、構成手順のためと、PP-VMAX を含む SnapVX のアクティブなスナップショット管理をコントロールするために Solutions Enabler のデフォルト サーバ ポートを使用。

表 27. PowerProtect Data Manager のポート要件 (続き)

ソース システム	デスティネーション システム	ポート	プロトコル	サポートされている TLS	注
保護エンジン	DD システム	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
保護エンジン	DD システム	2049	独自のプロトコル	TLS 1.2	オプションの DD Boost クライアント TLS 暗号化。
保護エンジン	DD システム	2052	TCP	不可	NFS mountd。データ用ではない。
保護エンジン	DD システム	3009	HTTPS	TLS 1.2	DD REST API サービス。
保護エンジン	ESXi	443	HTTPS	TLS 1.2	クライアント接続。
保護エンジン	ESXi	902	TCP	TLS 1.2	vSphere Client アクセス。
保護エンジン	ゲスト VM	9613 ^c	独自のプロトコル	TLS 1.2	VM Direct Agent は、ファイルレベルのリストア機能とアプリケーション対応の保護機能を提供。
保護エンジン	NAS エージェント Docker コンテナ	443	HTTPS	TLS 1.2	NAS にのみ適用。内部のみ。ファイアウォールによるブロック。
保護エンジン	Search Engine	14251	TCP	TLS 1.2	検索クエリ REST API エンドポイント。
保護エンジン	vCenter	443	HTTPS	TLS 1.2	vCenter Server を使用する vSphere 用のプライマリー管理インターフェイス (vSphere Client を含む)。
保護エンジン	vCenter	7444	TCP	TLS 1.2	セキュア トークン サービス。
保護エンジン	保護エンジン : RabbitMQ	4369	TCP		内部のみ。ファイアウォールによるブロック。
保護エンジン	保護エンジン : RabbitMQ	5672	TCP		内部のみ。ファイアウォールによるブロック。
Reporting Engine	PowerProtect Data Manager	8443	TCP	TLS 1.2	レポート データを収集するための REST API サービス。
Search Engine	DD システム	111	TCP	不可	サーバーの DR。動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
Search Engine	DD システム	2049	独自のプロトコル	不可	サーバー DR NFS 接続。メタデータ、クライアント名、インデックス作成にのみ使用。バックアップ データには使用されない。
Search Engine	DD システム	2052	TCP/UDP	不可	サーバーの DR。NFS mountd。データ用ではない。
ソース DD システム	ターゲット DD システム	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。
ソース DD システム	ターゲット DD システム	2049	独自のプロトコル	TLS 1.2	
ソース DD システム	ターゲット DD システム	2051	独自のプロトコル	TLS 1.2	
ソース DD システム	ターゲット DD システム	2052	TCP	不可	NFS mountd。データ用ではない。
ターゲット DD システム	ソース DD システム	111	TCP	不可	動的ポートの検出およびマッピング。データではなく、ポートの検証にのみ使用。

表 27. PowerProtect Data Manager のポート要件 (続き)

ソース システム	デスティネーション システム	ポート	プロトコル	サポートされている TLS	注
ターゲット DD システム	ソース DD システム	2049	独自のプロトコル	TLS 1.2	
ターゲット DD システム	ソース DD システム	2051	独自のプロトコル	TLS 1.2	
ターゲット DD システム	ソース DD システム	2052	TCP	不可	NFS mountd。データ用ではない。
Update Manager UI	PowerProtect Data Manager	14443	HTTPS	TLS 1.2	アップデート パッケージを含んだホストを PowerProtect Data Manager システムに接続。
ユーザー	PowerProtect Data Manager	22	SSH	TLS 1.2	サポートと管理用の SSH。プライベート キーまたはオプションの証明書で暗号化。
ユーザー	PowerProtect Data Manager	80	HTTP	不可	HTTPS にリダイレクト。
ユーザー	PowerProtect Data Manager	443	HTTPS	TLS 1.2	ブラウザー ホストを PowerProtect Data Manager システムに接続。
ユーザー	PowerProtect Data Manager	8443	HTTPS	TLS 1.2	REST API サービス。
ユーザー	Search Engine	22	SSH	TLS 1.2	サポートと管理用の SSH。プライベート キーまたはオプションの証明書で暗号化。
ユーザー	保護エンジン	22	SSH	TLS 1.2	サポートと管理用の SSH。プライベート キーまたはオプションの証明書で暗号化。
vCenter	ESXi	443	HTTPS	TLS 1.2	vSphere Client から ESXi/ESX ホストへの管理接続。
vCenter	PowerProtect Data Manager	443	HTTPS	TLS 1.2	vCenter プラグイン UI。
vCenter	PowerProtect Data Manager	8443	HTTPS	TLS 1.2	REST API サービス。
vCenter	PowerProtect Data Manager	9009	HTTPS	TLS 1.2/1.3	vSphere APIs for Storage Awareness (VASA) プロバイダー、PowerProtect Data Manager 内でのストレージのポリシー ベースの管理 (SPBM) サービス。

- a. Application Direct、Storage Direct、VM Direct に適用 (VM アプリケーション対応のみ)。
- b. インスタント アクセス リストア。ESXi ノードから DD システムへの vSphere の PowerProtect Data Manager 制御下で確立された NFS 接続。任意の ESXi ノードに向けることができるため、許可されたポートは、任意の ESXi ノードと PowerProtect Data Manager で使用される任意の DD システムとの間のものになります。
- c. ポート番号はデフォルト値で、エージェントごとに変更でき、リスニングの競合が発生した場合は動的に変更可能。

この表の「保護エンジン」という用語は、特に指定のない限り、すべてのタイプの保護エンジン (VM Direct、NAS、Kubernetes) を指します。

VM アプリケーション対応バックアップの場合、保護エンジン用とゲスト VM のバックアップクライアント用のポートを開いてください。

NAS 資産の場合は、特定の共有へのアクセスに必要な可能性がある PowerProtect Data Manager、NAS 保護エンジン、NAS の間のカスタム ポートを開きます。NAS 資産ソースを追加するプロセスの一環として、NAS アプライアンスおよび共有への接続用カスタム ポート情報を提供できます。

通信セキュリティ設定

以下のトピックでは、PowerProtect Data Manager とリモート システム (クライアントなど) の間の通信を保護する方法について説明します。

仮想ネットワーク (VLAN)

PowerProtect Data Manager では、管理トラフィックとバックアップトラフィックを異なる仮想ネットワーク (VLAN) に分離できます。仮想ネットワークを使用すると、データトラフィックのルーティング、セキュリティ、機構を改善できます。

各仮想ネットワークの構成および追加における最初の手順を行うのは、1 回限りです。保護ポリシーまたは資産に仮想ネットワークを割り当てるためのその後の手順は、必要に応じて行うことになります。

対応しているネットワークトポロジーと仮想ネットワークを構成する方法の詳細については、『PowerProtect Data Manager 管理およびユーザーガイド』を参照してください。仮想ネットワークの構成は、システム設定の変更の一部と見なされます。

通常は、保護ポリシーの作成時に仮想ネットワークを保護ポリシーと資産に割り当てます。このプロセスについては、各エージェントタイプのユーザーガイドを参照してください。ただし、仮想ネットワークを既存のポリシーに割り当て、資産ごとにネットワーク割り当てのオーバーライドをする手順については、『PowerProtect Data Manager 管理およびユーザーガイド』を参照してください。

SSH セッション タイムアウトの構成

このトピックでは、長時間非アクティブ状態の接続に対する PowerProtect Data Manager コンソールの動作について説明します。これらの手順は、SSH セッションを制御するタイムアウトメカニズムの動作も変更します。

このタスクについて

デフォルトの SSH セッション タイムアウトは 3600 秒 (60 分) です。

手順

1. PowerProtect Data Manager コンソールに接続し、root ユーザーに変更します。
2. Linux テキストエディターを使用して /etc/ssh/sshd_config を開きます。
3. 次のプロパティを変更します。

プロパティ	説明
ClientAliveInterval	PowerProtect Data Manager が SSH セッションを終了するまでの非アクティブ状態の秒数。

4. ファイルを保存して閉じます。
5. SSH デモンを再起動して、変更を適用します。

```
systemctl reload sshd
```

REST API トークンの有効期限の構成

このトピックでは PowerProtect Data Manager REST API トークンと、デフォルトのトークンの有効期限の間隔について説明します。これらの手順では、トークンの期限切れメカニズムの動作も変更されます。

このタスクについて

REST API では、アクセス、更新、コンポーネントの 3 タイプのトークンが使用されます。アクセストークンは REST API コールを認証するベアラー トークンです。更新トークンは、アクセス トークンの有効期限が切れた後に新しいアクセス トークンを取得するために十分な情報を提供します。コンポーネント トークンは、システムの内部コンポーネント間の操作を許可します。

更新トークンを使用すると、頻繁な認定資格のリクエストを発生させることなく、アクセス トークンの有効期間を短く設定できます。アクセス トークンの有効期間を短くすることで、トークン値が侵害されるリスクを軽減できます。トークンタイプの詳細については、「OAuth Authorization Framework」を参照してください。

すべてのタイプのデフォルト時間単位は MINUTES です。更新トークンの時間単位のみを変更できます。これらのトークンで使用可能な時間単位は、DAYS、HOURS、MINUTES、MONTHS、SECONDS、WEEKS です。

デフォルトのアクセス トークンの有効期間は 480 です。デフォルトの更新トークンの有効期間は 1440 です。デフォルトのコンポーネントトークンの期限時間は 480 です。

メモ: PowerProtect Data Manager の以前のリリースでは、`application-server-custom.properties` で `aaa.jwt.token.access-expiration-time` プロパティを使用して、アクセス トークンの期限が構成されていました。アップデート後は、`aaa.jwt.token.access-expiration-time` 用に構成された値が無視され、新しいプロパティのデフォルト値が優先されます。アップデート後にアクセス トークンの期限を再構成するには、こちらに示されている手順を実行してください。

手順

1. 管理者ユーザーとして PowerProtect Data Manager コンソールに接続します。
アクセス トークンおよびコンポーネント トークンの期限を構成するには、次の手順を実行します。
2. Linux テキスト エディターを使用して `/usr/local/brs/lib/aaa/config/application-jwt-token.yml` を開きます。
3. 次のプロパティを変更します。

プロパティ	説明
<code>user-access-expiration-time</code>	アクセス トークンが期限切れになるまでの時間 (分)。
<code>component-access-expiration-time</code>	コンポーネント トークンが期限切れになるまでの時間 (分)。

推奨されている最小期限時間は、アクセス トークンで 15 分、コンポーネント トークンで 120 分です。

4. ファイルを保存して閉じます。
更新トークンの期限を構成するには、次の手順を実行します。
5. Linux テキスト エディターを使用して `/usr/local/brs/lib/aaa/config/application-server-custom.properties` を開きます。
6. 次のプロパティを変更します。

プロパティ	説明
<code>aaa.jwt.token.chrono-unit</code>	有効期限のプロパティの単位。
<code>aaa.jwt.token.access-expiration-time</code>	(廃止) アクセス トークンが期限切れになるまでの時間。
<code>aaa.jwt.token.refresh-expiration-time</code>	更新トークンが期限切れになるまでの時間。

このファイルの `aaa.jwt.token.access-expiration-time` プロパティに値が表示されることがあります。ただし、このプロパティは廃止されており、この手順の前のステップでアクセス トークン構成に置き換えられています。このプロパティに表示されている値は、`user-access-expiration-time` プロパティが使用不可である場合にのみ使用されます。

7. ファイルを保存して閉じます。
トークン タイプの期限切れメカニズムを構成した後、次の手順を実行します。
8. `root` ユーザーに変更します。
9. 新しい構成を適用します。

```
aaa restart
```

PowerProtect Data Manager ファイアウォールのサポート

PowerProtect Data Manager は、仮想アプライアンス内のシングル ノードであり、Linux SLES 12 のファイアウォールを使用して、システムに対する外部アクセスを保護および制限します。PowerProtect Data Manager では、最小限のオーバーヘッドで、必要なサービスとネットワーク内全体で通信し、データを移動するために、直接ソケット接続が使用されます。

PowerProtect Data Manager システムとその他のアプリケーションの間の通信を有効にするには、PowerProtect Data Manager でインバウンド通信とアウトバウンド通信に使用されるポートのファイアウォール ルールを構成します。

ファイアウォール ルールの変更

PowerProtect Data Manager システムでは、ファイアウォール ルールを構成することで、PowerProtect Data Manager コンポーネントでの通信に必要なポートのインバウンド通信とアウトバウンド通信をブロックできます。

このタスクについて

次の3通りの方法で、ファイアウォール ルールを変更することができます。

- 恒久的な変更の場合は、カスタム ポートのリストにエントリーを追加できます。
- 一時的な変更の場合は、Linux オペレーティング システムに組み込まれている iptables コマンドを使用できます。この方法を使用する前に、iptables の操作と構文（優先順位を含む）を十分に理解しておく必要があります。一時的な変更は、ファイアウォールが再起動されると維持されなくなります。
- また、PowerProtect Data Manager REST API を使用して、アウトバウンド ポートを開くこともできます。この方法の手順については、「[PowerProtect Data Manager パブリック REST API のドキュメント](#)」を参照してください。

メモ: ファイアウォール ルールを変更することで正常な動作に影響を与える可能性があるため、既存のファイアウォール ルールを変更しないことが推奨されています。

手順

1. PowerProtect Data Manager コンソールに接続し、root ユーザーに変更します。

恒久的な変更の場合：

2. ポート番号を `/etc/sysconfig/scripts/custom-ports` に別の行で追加します。

例：

```
139
445
6443
8080
```

ファイルを保存して閉じます。

3. 次のようにファイアウォール サービスを停止します。

```
SuSEfirewall2 stop
```

4. 次のようにファイアウォール サービスを開始します。

```
SuSEfirewall2 start
```

一時的な変更の場合：

5. 次のようにアウトバウンド ポートを開きます。

```
/usr/sbin/iptables -I OUTPUT -p tcp --dport <num> -j ACCEPT
```

ここでの `<num>` は新しいアウトバウンド ポートです。

この例では、ルール チェーンの前頭に新しいルールを挿入し、PowerProtect Data Manager から任意の宛先への指定した TCP ポートを開きます。

6. 次のように受信ポートを開きます。

```
/usr/sbin/iptables -I INPUT -p tcp --dport <num> -j ACCEPT
```

ここでの `<num>` は新しいアウトバウンド ポートです。

この例では、ルール チェーンの前頭に新しいルールを挿入し、任意の宛先から PowerProtect Data Manager への指定した TCP ポートを開きます。

データ セキュリティ 設定

トピック：

- データ ストレージのセキュリティ設定
- 機密データの暗号化
- バックアップおよびリストアの暗号化
- システム アクティビティの監査ログとモニタリング
- コンプライアンス検証の構成

データ ストレージのセキュリティ設定

以降のトピックでは、PowerProtect Data Manager リソースとバックアップ データを不正アクセスから保護する方法について説明します。

権限の範囲 と **リソースとリソース グループ** でも、許可されたユーザーによるリソースおよびバックアップ データへのアクセスを制限する方法を説明しています。

保護エンジンの設定

*PowerProtect Data Manager 仮想マシン ユーザー ガイド*には、保護エンジンにおいてユーザーがアクセス可能なオプションの構成に関する情報が記載されています。

Transparent Snapshot Data Mover (TSDM)などの一部の保護エンジンには、構成オプションがありません。*PowerProtect Data Manager 仮想マシン ユーザー ガイド*では、MAC アドレスの変更、偽造転送、無差別モード接続を拒否するデフォルトの仮想スリッチ構成を使用することを推奨しています。

このユーザー ガイドには、TSDM 専用の vCenter ユーザー アカウントを構成するために必要な手順と権限も記載されています。

機密データの暗号化

PowerProtect Data Manager は、暗号化されたロックボックスを使用して、機微情報を一元的な場所に安全に保存します。

認定資格セキュリティ PowerProtect Data Manager がロックボックスを使用する方法と、保存されたシークレットが保護される方法について詳しく説明します。

バックアップおよびリストアの暗号化

Transport Layer Security (TLS)を使用すると、DD Boost の暗号化を使って、一元化されたセルフサービス操作のために、転送中のバックアップまたはリストア データを暗号化できます。バックアップおよびリストアのインフライト データの暗号化は、エージェント ホスト資産、Kubernetes クラスター資産、ネットワーク接続型ストレージ(NAS)資産でのみ使用できます。

デフォルトでは、PowerProtect Data Manager によって HIGH の暗号化強度がサポートされ、DD Boost 匿名認証モードを使用します。DD Boost 暗号化ソフトウェアにより、[ADH-AES256-SHA] 暗号化スイートが使用されます。高度な暗号化に用いる暗号化スイートの詳細については、*DD Boost for OpenStorage 管理ガイド*を参照してください。

次の表に、インフライト データの暗号化をサポートするワークロードと操作を示します。

メモ: サポートされる、一元化されたセルフサービス操作の詳細については、エージェントのユーザー ガイドを参照してください。

表 28. サポート対象のワークロード

ワークロード	一元的なバックアップ	一元的なリストア	セルフサービス バックアップ	セルフサービス リストア
Application Direct を使用したファイル システム	可	可 (イメージ レベルのリストアのみ)	可	可 (イメージ レベルのリストアのみ)
Kubernetes クラスター	可	可	N/A	可(最新のバックアップから)
アプリケーション ディレクトリを使用した Microsoft SQL Server	可	可 (データベース レベルのリストアのみ)	可 ●	可 (データベース レベルのリストアのみ)
アプリケーション ディレクトリを使用した Microsoft Exchange Server	可	N/A	可	可
NAS	可	可	N/A	N/A
Application Direct を使用した Oracle	可	N/A	可	可
Application Direct を使用した SAP HANA	可	N/A	可	可

暗号化を有効にすると、追加のオーバーヘッドが発生します。暗号化が有効になっている場合、クライアントのバックアップとリストアのパフォーマンスは 5~20%の影響を受ける可能性があります。

PowerProtect Data Manager UI でバックアップおよびリストア暗号化を有効または無効にすることができます。

PowerProtect Data Manager は、サポートされているすべての DD Boost および DDOS バージョンを対象に、バックアップおよびリストアの暗号化をサポートします。PowerProtect Data Manager の最新のソフトウェア互換性に関する情報については、[E-Lab Navigator](#) を参照してください。

① メモ: 接続された DD システムでインフライト暗号化を有効にする必要はありません。DD 暗号化設定が存在する場合は、上位の設定が優先されます。

バックアップとリストアの暗号化を有効にする

ソース システムでの読み取り、暗号化された形式での転送の際に、バックアップおよびリストアされたコンテンツが暗号化されていることを確認できます。そして、デスティネーション ストレージに保存される前に復号できます。

前提条件

バックアップおよびリストアの暗号化の詳細については、「[バックアップおよびリストアの暗号化](#)」を参照してください。

暗号化設定は、バックアップおよびリストアの操作中に、実行中のデータ転送が暗号化されるかどうかを決定します。

- Microsoft SQL Server、Microsoft Exchange Server、ファイル システム、SAP HANA、Oracle のワークロードの場合、バックアップとリストアの暗号化はアプリケーション ディレクトリ ホストでのみサポートされます。
- 新しいホストが PowerProtect Data Manager に追加されると、ホスト構成が実行され、暗号化設定がホストにプッシュされます。
- ホスト構成をサポートするのは、PowerProtect Data Manager アプリケーション エージェントの同じバージョンがインストールされているホストのみです。

このタスクについて

手順

1. PowerProtect Data Manager UI で、 をクリックし、[Security] を選択します。
[[セキュリティ]] ダイアログ ボックスが表示されます。
2. [Backup/Restore Encryption] スイッチをクリックして有効にし、[Save] をクリックします。

次の手順

PowerProtect Data Manager UI の [Jobs] > [System Job] ウィンドウで、保護の暗号化を有効にするジョブを作成します。このジョブは、セルフサービス操作に使用するホストに暗号化設定をプッシュします。システム ジョブ内では、ホストごとにホスト構成ジョブが作成されます。エラーが発生した場合は、システム ジョブまたは個々のホスト構成ジョブを再試行できます。

メモ: 一元的なバックアップおよびリストア操作の場合、PowerProtect Data Manager によって、アプリケーション ディレクトリホストおよびネットワーク接続型ストレージ(NAS)上のアプリケーション エージェントに暗号化設定が送信されます。

[Backup/Restore Encryption] スイッチをクリックして、コンテンツのバックアップおよびリストアの暗号化を無効にすることができます。PowerProtect Data Manager は、[Jobs] > [System Job] ウィンドウにシステム ジョブを作成し、保護の暗号化を無効にします。

システム アクティビティの監査ログとモニタリング

Linux audit daemon (`auditd`) によって、PowerProtect Data Manager システム上のセキュリティ関連イベントの追跡と記録が行われます。

管理者ロールを持つユーザーは、`auditd` を使用して次のイベントをモニターできます。

- ファイル アクセス
- システム コール
- ユーザーのログイン/ログアウト アクティビティ

監査ログを使用すると、アクセス違反、変更または削除されたファイル、失敗した認証などを検出できます。

監査サービスの構成

Linux `auditd` デーモンでは、Linux カーネルからイベントを収集し、そのエントリーを調査用ログ ファイルに記録します。`auditd` ログのエントリーは、ログ ファイルに定義されるイベントを指定するルール セットに基づくものです。監査はデフォルトで無効になっています。デフォルトの監査ルールを変更するには、`/etc/audit/audit.rules` ファイルを編集します。

このタスクについて

監査を有効にするには、次の手順を実行します。

メモ: YaST ツールを使用して、監査を有効/無効にすることもできます。

手順

1. PowerProtect Data Manager コンソールに接続し、`root` ユーザーに変更します。
2. `auditd` を開始するには、次のいずれかのコマンドを入力します。
 - 継続的なログ : `systemctl enable auditd`
 - システム再起動までのログ : `service auditd start`

メモ: 継続的な `auditd` ログを無効にするには、`systemctl disable auditd` を入力します。`auditd` を停止するには、`service auditd stop` を入力します
3. `auditd` ログのエントリーをレビューするには、`/var/log/audit/audit.log` ディレクトリー内のファイルをレビューします。

メモ: `/var/log/audit/audit.log` ディレクトリーのファイル上限数は 5 個となっており、ファイル サイズが 6 MB に達するとログのローテーションが実行されます。デフォルトの構成を変更するには、`/etc/audit/auditd.conf` ファイルを編集します。ここでの引数は次のとおりです。

 - `num_logs` : ディレクトリー内で同時に保持するログ ファイルの数を指定します。
 - `max_log_file` : ログ ファイルの最大サイズを MB 単位で指定します。
 - `max_log_file_action` : ログ ファイルが最大サイズに達したときに、ログ ファイルをローテーションするよう `auditd` デーモンに指示します。

サポートから特に指示がない限り、その他のパラメーターは変更しないでください。
4. 監査ログからサマリー レポートを生成するには、`aureport --summary` を入力します。

UIでの監査イベントの表示

管理者、バックアップ管理者、管理者のリストア、ユーザーロールでは、監査イベントを表示してシステムアクティビティをモニタリングすることができます。

このタスクについて

次のアクションを実行すると、監査イベントが生成されます。

- ユーザーのログインとログアウト
- ユーザーの作成、削除、またはアップデート
- ユーザーに対するロールの割り当てまたは割り当て解除

UIで監査イベントを表示するには、次の手順を実行します。

手順

1. 示されたロールのいずれかを持つアカウントを使用して、PowerProtect Data Manager UIにログインします。
2. [Alerts] > [Audit Logs] に移動します。

アラートの表示と管理

アラートを使用すると、サービスレベル目標に準拠しているかどうかを判断できるように、PowerProtect Data Manager でデータ保護操作のパフォーマンスを追跡できます。管理者、バックアップ管理者、管理者のリストア、またはユーザーロールを使用すると、[Alerts] ウィンドウで、アラートにアクセスできます。ただし、アラートを管理できるのは、これらのロールの一部のみです。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインから、[アラート] を選択します。

上部バナーの  アイコンをクリックし、リンクをクリックして、すべてのステータス（重大、警告、情報）の未確認アラート、または未確認の重大アラートのみを表示することができます。

 **メモ:** [New] タグをクリックすると、過去 24 時間以内に生成された未確認のアラートのみが表示されます。  の横に表示される数は、過去 24 時間の未確認の重大なアラートの合計数です。

[Alerts] ウィンドウが表示されます。

2. [System] タブを選択します。該当する各アラートのエントリーを含むテーブルが表示されます。

デフォルトでは、  アイコンの下のリンクから未確認のすべてのアラートを表示するように選択していない限り、過去 24 時間の未確認の重大なアラートのみが表示されます。

フィルター タグがすでに適用されている場合は、ウィンドウにこれらのフィルター タグが表示されます。これらのフィルター タグの横にある [X] をクリックしてフィルターをクリアすると、テーブルビューが該当する選択でアップデートされます。重大度（重大、警告、情報）、日付、カテゴリ、ステータス（確認済みまたは未確認）で、テーブル内のアラートを分類できます。

3. 表示するアラートの時刻（過去 24 時間、過去 3 日/7 日/30 日）、特定の日付、または時間範囲を選択します。フィルター タグに一致するすべてのアラートの情報を表示するには、このリストから [All Alerts] を選択することもできます。
4. 確認済みアラートと未確認アラートの両方を表示する場合は、必要に応じて、[Show only unacknowledged alerts] チェックボックスをオフにします。このチェックボックスをオフにすると、[Unacknowledged] フィルター タグもクリアされます。
5. 特定のエントリーの詳細を表示するには、表内のエントリーの横にある  をクリックします。
6. 次の手順を実行するには、管理者、バックアップ管理者、または管理者のリストアロールのアカウントを使用して PowerProtect Data Manager UI にログインします。
7. 1 件以上のアラートを確認するには、アラートを選択し、[Acknowledge] をクリックします。
8. アラートのメモを追加または編集するには、[メモの追加または編集] をクリックし、終了したら [保存] をクリックします。
9. アラート情報のレポートを Excel でダウンロード可能な .csv ファイルにエクスポートをするには、[Export All] をクリックします。

 **メモ:** テーブル内でフィルターを適用すると、エクスポートされるアラートにはフィルター条件を満たすアラートのみが含まれます。

監査ログのエクスポート

管理者またはセキュリティ管理者ロールで、監査ログレコードを監査データの CSV ファイルにエクスポートし、ダウンロードして Excel で開くことができます。保存期間を変更できるのは管理者ロールのみです。

手順

- [Administration] > [Audit Logs] に移動します。
次の情報を含む監査ログのリストが表示されます。
 - 変更時刻
 - 監査タイプ
 - 説明
 - 変更者
 - 変更されたオブジェクト
 - 前の値
 - 新しい値
- 監査ログの保存期間（日数）を設定するには、[Set Boundaries] を選択して保存期間をアップデートします。
この手順を実行できるのは管理者ロールのみです。
- 監査ログにメモを追加するには、[>] をクリックして [Note] フィールドにメモを入力し、[Save] をクリックします。
- [Export All] をクリックします。

コンプライアンス検証の構成

一部のメンテナンス手順では、コンプライアンス検証を一時的に無効にしなければならない場合があります。このタスクは、他の場所で言及されている場合にものみ使用してください。

このタスクについて

付録「[REST API の手順](#)」では、上級ユーザーが検証サービスを再起動せずにコンプライアンス検証を構成するための代替方法について説明します。

手順

- 管理者ユーザーとして PowerProtect Data Manager コンソールに接続します。
- ディレクトリを次のように変更します。

```
cd /usr/local/brs/lib/compliance-verification/config
```
- 次のようにコンプライアンス検証を無効にします。
 - 次のコマンドを入力して、構成ファイルを作成し、コンプライアンス検証フラグを追加します。

```
echo compliance.copydeletion.enable=false > application.properties
```
 - Linux テキスト エディターを使用して `docker-compose.yml` を開きます。
 - 次のエントリをファイルの末尾に 1 行で追加して、新しい構成ファイルを使用するように PowerProtect Data Manager を構成します。

```
- /usr/local/brs/lib/compliance-verification/config/application.properties:/compliance-verification/config/application.properties
```
 - ファイルを保存して閉じます。
 - root ユーザーに変更します。
 - 新しい構成を適用します。

```
compliance-verification restart
```
- 次のようにコンプライアンス検証を有効にします。
 - Linux テキスト エディターを使用して `application.properties` を開きます。
 - コンプライアンス検証の `compliance.copydeletion.enable` フラグを `true` に変更します。
 - ファイルを保存して閉じます。
 - root ユーザーに変更します。
 - 新しい構成を適用します。

```
compliance-verification restart
```

トピック：

- [セキュリティ証明書](#)
- [PowerProtect Data Manager の証明書管理](#)

セキュリティ証明書

PowerProtect Data Manager のデフォルト インストールでは、他のコンポーネントとの通信を保護する自己署名セキュリティ証明書が作成されます。サーバーを構成し、資産を追加する際に、PowerProtect Data Manager によって各コンポーネントの追加の証明書が保存されます。

管理者とセキュリティ管理者のロールでは、UI の [Administration] > [Certificates] ページを確認できます。このページには、インストール済みのセキュリティ証明書をリスト表示する 3 個のタブがあります。各タブには、証明書の使用、有効期限、発行者などに関する情報が表示されます。

各アプリケーション エージェントまたは外部コンポーネントに分かりやすいホスト名と完全修飾ドメイン名を使用すると、セキュリティ証明書を資産やシステムと照合する際に役立ちます。証明書の [Host] 列の値を、資産ソースや保護ストレージなどのホスト名およびアドレスと比較できます。共通名は任意の文字列ですが、多くの場合にホスト名と IP アドレスが含まれています (特に外部コンポーネントの場合)。

内部コンポーネント

[Internal] タブの証明書により、UI および REST API など、PowerProtect Data Manager サーバーに含まれるコンポーネントへのアクセスが保護されます。

- `ppdmserver` には、UI および REST API との通信を保護するために PowerProtect Data Manager によって提示される証明書があります。
- `restserver` には、導入時のデフォルトの自己署名証明書があります。

[PowerProtect Data Manager の証明書管理](#) では、[Internal] タブのデフォルトの自己署名セキュリティ証明書を、任意の承認済み認証局 (CA) の証明書に置き換える手順について説明しています。

自己署名証明書を置き換えた場合、PowerProtect Data Manager により、`ppdmserver` と `restserver` の証明書が `custom` と呼ばれる新しい証明書に置き換えられます。この単一のエントリーには、置き換える際に指定したホスト証明書があります。UI と REST API の両方で `custom` 証明書が使用されます。

アプリケーション エージェント

[Application Agents] タブの証明書によって、PowerProtect Data Manager の制御下にあるものの、サーバーの外部に存在するエージェントへのアクセスが保護されます。アプリケーション エージェントにより、登録の処理中に証明書署名リクエストが作成され、PowerProtect Data Manager から署名入りのセキュリティ証明書が取得されます。このリストには、署名入り証明書を受信したアプリケーション エージェントが表示されます。

アプリケーション エージェント証明書作成の処理によって、資産ソースの完全修飾ドメイン名と IP アドレスに関する情報が組み込まれます。エージェントにより、署名リクエスト中に一意の共通名が提供されます。

外部コンポーネント

[External Servers] タブの証明書によって、サーバーの制御下でないものの、通信が承認されているコンポーネントまたはシステムへのアクセスが保護されます。

たとえば、PowerProtect Data Manager にサービスを提供するディレクトリー サービスと保護ストレージ システムは外部コンポーネントです。

保護エンジンとセキュリティ証明書

VM Direct、NAS、Kubernetes のいずれの保護エンジンも、PowerProtect Data Manager の制御下にあると見なされます。

PowerProtect Data Manager によって、導入、アップグレード、削除など、保護エンジンのライフサイクルにおけるあらゆる側面が管理されます。通常は、お客様が PowerProtect Data Manager 以外を使用して保護エンジンを操作することはありません。

他のコンポーネントのデフォルト自己署名セキュリティ証明書を置き換えた場合であっても、保護エンジンでは元の自己署名証明書が引き続き使用されます。

アプリケーション エージェントとセキュリティ証明書

インストールをしたエージェントのソフトウェアバージョンにより、デフォルトの自己署名セキュリティ証明書を置き換えた場合のアプリケーション エージェントの挙動が異なります。

PowerProtect Data Manager 19.8 以前のアプリケーション エージェントの場合、これらのレガシー エージェントでは、サーバーとの通信を保護する証明書の変更が認識されません。レガシー エージェントには、新しいセキュリティ証明書を使用するための機能がありません。UI と REST API の証明書を置き換えたその後も、レガシー エージェントでは常にデフォルトの自己署名セキュリティ証明書が使用され、PowerProtect Data Manager とのすべての通信が保護されます。これは、UI では [Internal] タブの `restserver` 証明書となります。

PowerProtect Data Manager 19.9 以降のアプリケーション エージェントでは、登録時にサーバーから新しいセキュリティ証明書を自動的に取得できます。その後、エージェントでは新しい証明書が使用されて、PowerProtect Data Manager との通信が保護されます。

アプリケーション エージェントのセキュリティ証明書ファイル

Windows 資産の場合、証明書は `DPSAPPS\AgentService\ssl` フォルダーにあります。このフォルダーはアプリケーション エージェントのソフトウェアのインストールをした場所に関連づけられています。

- `globalca.pem` : カスタム サーバー証明書。
- `ecdm-rootca.pem` : PowerProtect Data Manager サーバーのルート証明書。
- `privKey.csr` : 署名入りアプリケーション エージェント証明書の生成元となる証明書署名リクエスト。
- `privKey.pem` : アプリケーション エージェント証明書の署名リクエスト用プライベートキー。
- `agent-cert.pem` : 署名入りアプリケーション エージェント証明書。

PowerProtect Data Manager サーバーの証明書を置き換えた場合には、サーバーの新しいセキュリティ証明書が `globalca.pem` に格納されます。

外部コンポーネントとの PowerProtect Data Manager セキュリティ証明書の交換

PowerProtect Data Manager で信頼できる外部コンポーネントの証明書ストアを維持しながら、サーバー証明書を外部コンポーネントと交換して保護を強化することもできます。

外部コンポーネントからサーバーに接続する際には、最初のハンドシェイク中に PowerProtect Data Manager によってサーバー証明書が自動的に表示されます。今後の使用および認証のために、外部コンポーネントでは通常サーバー証明書が受け入れられて保存されます。他のアクションは必要ありません。

サーバー証明書が自動的に表示または保存されなかった場合は、REST API を使用して証明書を取得できます。詳細については、[PowerProtect Data Manager パブリック REST API のドキュメント](#)を参照してください。

任意の `curl` または REST API クライアントを使用します。アクセス トークンは必要ありません。ただし、REST API クライアントでは、自己署名証明書を使用するサーバーとの接続を許可するために追加のパラメーターが必要になる場合があります。

```
GET https://{{server}}:{{port}}/api/v2/jwks
```

REST API サービスにより、次のような状態コードとサーバー証明書が返されます。

```
200 OK
{
  "keys": [
    {
      "kty": "EC",
```

```

    "use": "sig",
    "crv": "P-256",
    "kid": "a86a7118-99f9-4768-bdda-8012474c8685",
    "x5c": [
      "MIIDBTCCAe2gAwIBAgIESvEK5DANBgkqhkiG",
      "MIIDizCCAnOgAwIBAgIEMayrSDANBgkqhkiG"
    ],
    "x": "GdPBk9pB5VkppISLMHhKaQ5EIBsPeaoERgarTagRJko",
    "y": "QivYHOUdiGPzCW8NvJifB5qVkShDcmsKd8F2g_zdGvE",
    "alg": "ES256"
  },
  {
    "kty": "RSA",
    "e": "AQAB",
    "use": "sig",
    "kid": "7452f2bb-3a83-4569-a0fc-7fe255284fb4",
    "alg": "RS256",
    "n": "jTgO5NHdgzLhkv619gjh5Uz07v8-ZFHtpsDT"
  }
]
}

```

この例の一部の値は、使用可能なスペースに合わせるため省略されています。

REST API を使用した外部コンポーネント用セキュリティ証明書のインポート

外部コンポーネントとの通信にセキュリティ証明書が必要な場合は、REST API を使用して PowerProtect Data Manager にセキュリティ証明書のインポートを行うことができます。外部コンポーネントには、PEM 形式または Base64 形式のパブリック証明書チェーンが必要です。

このタスクについて

このタスクの証明書の例は、分かりやすくするため、またスペースの都合上シンプルに記載されています。

REST API の使用方法に関する例など、詳細については、PowerProtect Data Manager REST API のドキュメントを参照してください。任意の curl またはクライアントを使用し、ログインをしてから各コールに有効なアクセス トークンを指定します。クライアントでは、自己署名証明書を使用するサーバーへの接続を許可するために追加のパラメーターが必要になる場合があります。

外部コンポーネントの証明書は `host:port:type` という 3 個のパラメーターで構成されるエイリアスで、PowerProtect Data Manager の truststore にインポートが行われます。証明書 ID には、Base64 でエンコードをしたこのエイリアスが表示されます。

このタスクにおいて、`{{external-component}}` は外部コンポーネントの FQDN を表します。`{{remote-port}}` は、コンポーネントとの通信に使用するポート番号を表します。`{{cert-type}}` は、HOST、ROOT、INTERMEDIATE のいずれかの証明書タイプを表します。

手順

1. 管理者またはセキュリティ管理者のロールを持つユーザーとして、PowerProtect Data Manager REST API にログインをします。アクセス トークンを記録します。
2. (オプション) 次のように PEM 形式でセキュリティ証明書のインポートを行います。

POST https://{{server}}:{{port}}/api/v2/certificates

Headers:

```

Content-Type: application/json
Authorization: Bearer {{access-token}}

```

```

{
  "host": "{{external-component}}",
  "port": "{{remote-port}}",
  "type": "{{cert-type}}",
  "certificateChain": "{{PEM-cert}}"
}

```

`{{PEM-cert}}` を、証明書チェーンのコンテンツを表す \n で区切った 1 行の文字列に置き換えます。例：

```

-----BEGIN CERTIFICATE-----
\nMIIDdzCCA1+gAwIBAgI\nUzERMA8GA1UEChMIU21\nMDkyMjE4MDEzNFoXDTI\nBAoTC1BQRE0gU2VydjV\n-----
END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----

```

```
\nEHD0fXjANBgkqhkiG9w\nnd3cuc2lnbi5jb20gYz1\nnZ24gUm9vdCBDQTAeFw0\nnBgNVBAYTAlVTMREwDwY\nn-----\nEND CERTIFICATE-----\n-----BEGIN CERTIFICATE-----\n\nMIIDSTCCAjGgAwIBAgI\nnd3cuc2lnbi5jb20gYz1\nnZ24gUm9vdCBDQTAeFw0\nnBgNVBAsTExd3dy5zaWd\nn-----\nEND CERTIFICATE-----\n
```

REST API サービスから状態コードが返されます。

3. (オプション) 次のように Base64 形式でセキュリティ証明書のインポートを行います。

POST https://{{server}}:{{port}}/api/v2/certificates

```
Headers:  
Content-Type: application/json  
Authorization: Bearer {{access-token}}
```

```
{  
  "host": "{{external-component}}",  
  "port": "{{remote-port}}",  
  "type": "{{cert-type}}",  
  "certificateChain": "{{Base64-cert}}"  
}
```

{{Base64-cert}} を、証明書チェーンのコンテンツを表す Base64 でエンコードをした 1 行の文字列に置き換えます。例：

```
"certificateChain": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURRS0tLS0tCk1JSU9rRENDRF"
```

REST API サービスから状態コードが返されます。

PowerProtect Data Manager の証明書管理

次のトピックでは、PowerProtect Data Manager のデフォルトの自己署名セキュリティ証明書を、承認された CA からの証明書に置き換える方法について説明します。UI サーバーおよび REST API の証明書を置き換えることができます。

vCenter Server を追加した場合は、セキュリティ証明書を置き換えた後、PowerProtect プラグインを再インストールします。[vSphere Client 用 PowerProtect プラグインの再インストール](#) で詳細を参照してください。

選択した方法に関係なく、デフォルトの自己署名セキュリティ証明書が引き続き UI に表示される場合は、[Web サービスの再開](#)で手順を参照してください。

前提条件

新しいホスト証明書は次の条件を満たす必要があります。

- [Subject Common Name (CN)] および [Subject Alternative Name (SAN)] フィールドに PowerProtect Data Manager サーバーの完全修飾ドメイン名が含まれていること。
- [SAN] フィールドに PowerProtect Data Manager サーバーの IP アドレスが含まれていないこと。

UI に関する方法

ほとんどの環境では、HTTPS を経由してセキュリティ証明書を送信すると、十分なセキュリティを得られます。さらに予防策が必要な場合は、手動による方法を使用して証明書を置き換えてください。

PowerProtect Data Manager UI を使用してセキュリティ証明書を置き換えるには、PKCS#1 (RSA) PEM 形式のプライベート証明書と PEM 形式のパブリック証明書チェーンが必要です。

[[UI を使用したセキュリティ証明書の置き換え](#)] を実行します。

CLI に関する方法

CLI を使用する場合は、PKCS#1 (RSA) PEM 形式のプライベートキーと PEM 形式のパブリック証明書チェーンが必要です。安全な方法を使用して、証明書とキーを PowerProtect Data Manager サーバーに送信してください。

[[CLI ツールを使用したセキュリティ証明書の置き換え](#)] を実行します。付録「[REST API の手順](#)」では、上級ユーザー向けにセキュリティ証明書を手動で置き換える別の方法を説明しています。

仮想ネットワーク

仮想ネットワークを追加すると、その仮想ネットワークに PowerProtect Data Manager のインターフェイスが作成されます。デフォルトの自己署名証明書を置き換えた後に仮想ネットワークを追加すると、置き換えた後の証明書が新しいインターフェイスに適合しない場合があります。この場合、デフォルトのインターフェイスでは生成されなかった場合でも、新しいインターフェイスから接続すると証明書の警告が生成される可能性があります。

この状態を回避するために、仮想ネットワークのある環境ではワイルドカード証明書をインストールし、FQDN を使用して仮想ネットワーク インターフェイスにアクセスします。例えば、PowerProtect Data Manager サーバーが *test.example.com* の場合は次のようになります。

- *vlan-10.test.example.com*、*vlan-20.test.example.com* などのサブドメイン パターンを使用して仮想ネットワーク インターフェイスに名前を付けます。
- デフォルトの証明書を **.test.example.com* の署名付きワイルドカード証明書に置き換えます。
- FQDN *vlan-10.test.example.com* を使用して、VLAN 10 などから PowerProtect Data Manager にアクセスをします。

セキュリティ証明書を置き換える前に、ワイルドカード証明書の該当する制限事項とサブジェクト代替名の要件を確認してください。

UI を使用したセキュリティ証明書の置き換え

この方法によって、UI サーバーと REST API の証明書が置き換えられます。証明書を置き換えることができるのは、管理者とセキュリティ管理者のロールのみです。

前提条件

PowerProtect Data Manager の [証明書管理](#) で情報を確認します。

手順

1. 左ナビゲーション ペインで、[管理] > [証明書] の順に選択します。
[[証明書]] ウィンドウが表示されます。
2. [内部] タブで [証明書の置き換え] をクリックします。
[[証明書の置き換え]] ダイアログ ボックスが表示されます。
3. サーバーのプライベート証明書の場合、[ファイルの選択] をクリックし、RSA プライベート証明書を含んでいるファイルを参照します。
または、証明書ファイルの内容を対応するフィールドに貼り付けることもできます。
PowerProtect Data Manager によって入力内容が検証されます。エラーがあれば修正します。
4. プライベート証明書が暗号化されている場合は、[Encrypted Private Key Password] フィールドが表示されます。パスワードを入力します。
5. サーバーのパブリック証明書チェーンの場合、[ファイルの選択] をクリックし、署名付き証明書チェーンを含んでいるファイルを参照します。
または、証明書ファイルの内容を対応するフィールドに貼り付けることもできます。
PowerProtect Data Manager によって入力内容が検証されます。エラーがあれば修正します。
6. [置き換え] をクリックします。
PowerProtect Data Manager が、UI サーバーと REST API のセキュリティ証明書を置き換えます。
7. 既存の UI セッションの場合、ページを更新して新しい証明書が有効になるようにします。

次の手順

vCenter Server を追加した場合は、PowerProtect プラグインを再インストールします。 [vSphere Client 用 PowerProtect プラグインの再インストール](#) で詳細を参照してください。

CLI ツールを使用したセキュリティ証明書の置き換え

この方法によって、UI サーバーと REST API のセキュリティ証明書が置き換えられます。

前提条件

PowerProtect Data Manager の [証明書管理](#) で情報を確認します。

このタスクについて

このタスクでは、`private-key.pem` にセキュリティ証明書のプライベートキーがあり、`public-cert.pem` にパブリック証明書チェーンがあることを前提としています。

手順

1. 管理者ユーザーとして PowerProtect Data Manager コンソールに接続します。
2. `private-key.pem` と `public-cert.pem` を `/home/admin/.config` ディレクトリーに安全にコピーします。
3. `/home/admin/.config` ディレクトリーに変更します。

```
cd /home/admin/.config
```

4. 証明書とキーのアクセス権を確認します。

```
ls -l
```

コンソールに次のような出力が表示されます。

```
-rwx----- 1 admin admin 1675 Aug 28 16:57 private-key.pem
-rwx----- 1 admin admin 3824 Aug 28 16:58 public-cert.pem
```

5. 既存のセキュリティ証明書を置き換えます。

```
ppdmtool -replacecert -key /home/admin/.config/private-key.pem -cert /home/admin/.config/public-cert.pem
```

暗号化されたキーの場合は、`-password <password>` パラメーターを含めます。

6. 既存の UI セッションの場合、ページを更新して新しい証明書が有効になるようにします。

次の手順

vCenter Server を追加した場合は、PowerProtect プラグインを再インストールします。 [vSphere Client 用 PowerProtect プラグインの再インストール](#) で詳細を参照してください。

vSphere Client 用 PowerProtect プラグインの再インストール

デフォルトの自己署名セキュリティ証明書を置き換えた後、PowerProtect Data Manager によって接続されている vCenter と新しい証明書が交換されるまでに少し時間がかかることがあります。

このタスクについて

この間に仮想マシンを選択すると、vSphere Client の PowerProtect ポートレットにエラーが表示される場合があります。

- Service Unavailable: Please contact your administrator.
- No healthy upstream.

PowerProtect プラグインでは、接続が約1時間ごとに自動的に更新され、新しい証明書を適用して状態が修正されます。新しい証明書をすぐに適用するには、このタスクを完了して、接続されている各 vCenter に PowerProtect プラグインの再インストールを行ってください。

PowerProtect ポートレットとプラグインの詳細については、[PowerProtect Data Manager 管理およびユーザー ガイド](#)を参照してください。

プラグインの再インストールを行うことができるのは、管理者ロールのみです。

手順

1. 左ナビゲーション ペインで、[インフラストラクチャ] > [資産ソース] の順に選択します。
[Asset Sources] ウィンドウが表示されます。
2. [vCenter] タブで、対象の vCenter を選択し、[Edit] をクリックします。
[Edit vCenter] ダイアログが表示されます。
3. [vSphere Plugin] の場合は、[Install] をクリアします。
4. [保存] をクリックします。

PowerProtect Data Manager は vCenter から PowerProtect プラグインを削除します。

5. vSphere Client で、PowerProtect プラグインが削除されたことを示す通知を探してから、[REFRESH BROWSER] をクリックします。
通知がない場合は、ログアウトをしてから再度ログインをします。
6. 仮想マシンを選択したときに、PowerProtect ポートレットが表示されないことを確認します。
7. PowerProtect Data ManagerUI で、対象の vCenter を再度選択し、[Edit] をクリックします。
[Edit vCenter] ダイアログが表示されます。
8. [vSphere Plugin] の場合は、[Install] を選択します。
9. [保存] をクリックします。
PowerProtect Data Manager は vCenter の PowerProtect プラグインをインストールします。
10. vSphere Client で、PowerProtect プラグインが正常に導入されたことを示す通知を探してから、[REFRESH BROWSER] をクリックします。
通知がない場合は、ログアウトをしてから再度ログインをします。
11. 仮想マシンを選択した際に PowerProtect ポートレットが表示され、エラーが表示されないことを確認します。

Web サービスの再開

セキュリティ証明書を置き換えた場合、デフォルトの自己署名セキュリティ証明書が UI に引き続き表示される場合があります。このような結果は、証明書の置き換えに使用する方法に関わりなく発生する可能性があります。この場合は、Web サービスを再開して変更を適用します。

手順

1. PowerProtect Data Manager コンソールに接続し、root ユーザーに変更します。
2. 次のように Web サービスを停止します。

```
systemctl stop nginx
```
3. 次のように Web サービスを再開します。

```
systemctl start nginx
```

次の手順

Web サービスが開始したら、置き換えられたセキュリティ証明書が UI に表示されていることを確認します。

SPBM 用の vCenter との新しいセキュリティ証明書の交換

セキュリティ証明書を置き換える場合や PowerProtect Data Manager のアップグレードを行う場合は、ストレージ ポリシーベースの管理 (SPBM) 用に、新しい証明書を vCenter と交換しなければならない場合があります。

手順

1. PowerProtect Data Manager の新しいルート証明書を取得します。
SCP または別のファイル転送ユーティリティを使用して、`/etc/ssl/certificates/custom/globalca.pem` にある証明書をサーバーからダウンロードします。
2. vCenter を資産ソースとして追加し、資産の検出を完了させます。
詳細については、*PowerProtect Data Manager 管理およびユーザー ガイド*を参照してください。
3. PowerProtect Data Manager の新しいルート証明書を vCenter の証明書ストアに追加します。
詳細については、[VMware documentation](#) を参照してください。
4. SPBM への PowerProtect Data Manager の登録
詳細については、[VMware documentation](#) を参照してください。最上位の vCenter ホストを選択します。

値	説明
名前	任意の記述名。たとえば、 <code>PowerProtectDataManager-FQDN</code> などです。
URL	<code>https://PowerProtectDataManager-FQDN:9009/vasa/version.xml</code>
ユーザー名	管理者ロールを持つ PowerProtect Data Manager ユーザー。

値	説明
パスワード	対応するアカウント パスワード。

プレースホルダーを PowerProtect Data Manager の完全修飾ドメイン名に置き換えます。

タスクの結果

SPBM を使用して PowerProtect Data Manager を運用する準備が整いました。

次の手順

セキュリティ証明書を置換し、その証明書を SPBM と交換した後に、PowerProtect Data Manager のアップグレードを行う場合は、次の手順を実行します。

1. このタスクの説明に従って、PowerProtect Data Manager のルート証明書を取得します。
2. このタスクの説明に従って、ルート証明書を vCenter の証明書ストアに追加します。

セッションが更新されて新しいセキュリティ証明書が使用されるまで、登録ステータスは Rescanning error または Offline と表示されます。更新は約1時間ごとに実行されます。新しい証明書をすぐに適用するには、SPBM ストレージ プロバイダーを削除してから、4 の手順を繰り返してください。

vCenter からの PowerProtect Data Manager SPBM セキュリティ証明書の削除

セキュリティ証明書を置き換える際に、古い証明書を vCenter から削除して証明書ストアを整理することができます。

前提条件

VMware の KB 記事 [2111411] と [2146011] を参照してください。

 **注意:** SPBM を使用した PowerProtect Data Manager の運用を有効にするルート証明書のみを削除します。

手順

1. vCenter Server Appliance 管理インターフェイスを開きます。
https://vCenter:5480 に移動します。
2. SSH アクセスを有効にします。
詳細については、[VMware documentation](#) を参照してください。
3. vCenter Server Appliance への SSH セッションを確立してから、管理者権限で BASH シェル セッションを開始します。
手順については、VMware の KB 記事 [2111411] を参照してください。
4. 証明書ストアから PowerProtect Data Manager の SPBM セキュリティ証明書を削除します。

VMware の KB 記事 [2146011] には、有効期限が満了または差し迫った証明書に関する手順が記載されていますが、PowerProtect Data Manager のルート証明書を削除する手順と同じです。VMware の KB 記事には、vCenter Server Appliance と Windows vCenter Server の手順について記載されています。

/etc/ssl/certificates/custom/globalca.pem にある PowerProtect Data Manager サーバーの証明書の情報を使用して、証明書を識別します。

セキュリティのアップデートとパッチ適用

トピック：

- セキュリティのアップデートとパッチ適用
- PowerProtect Data Manager によって使用されている Velero または OADP バージョンのアップデート

セキュリティのアップデートとパッチ適用

PowerProtect Data Manager のほとんどのセキュリティ アップデートは、後続のリリースに対する製品アップデートの一部として提供されます。

PowerProtect Data Manager のアップデート手順については、各サポート プラットフォームの『*PowerProtect Data Manager 管理およびユーザー ガイド*』および『*PowerProtect Data Manager 導入ガイド*』を参照してください。「[完全性と整合性](#)」の手順を使用して、製品のアップデートを確認します。

PowerProtect Data Manager のセキュリティ アップデートおよび該当するサイクル外のアップデートに関する情報は、[カスタマーサポート](#)に該当する Dell セキュリティ アドバイザリー(DSA)の一部として掲載されています。

以降のトピックでは、サードパーティーおよび組み込みコンポーネントのセキュリティ アップデートに関する情報を提供します。

PowerProtect Data Manager によって使用されている Velero または OADP バージョンのアップデート

PowerProtect Data Manager が Kubernetes クラスターを保護するように構成されている場合、Kubernetes リソースのバックアップには Velero が使用されています。OpenShift 環境では、PowerProtect Data Manager によって Velero の導入に OADP が使用されます。デフォルトでは、PowerProtect Data Manager リリースごとに特定の Velero バージョンが使用されます。このバージョンはファイル `/usr/local/brs/lib/cndm/config/k8s-image-versions.info` に記載されています。セキュリティに関する最新の修正を受け取るために、PowerProtect Data Manager が使用する Velero または OADP バージョンのアップデートが必要な場合は、次の手順を実行します。

前提条件

- ① メモ:** 増分パッチ ビルドへの Velero バージョンのアップデートのみを実行してください。PowerProtect Data Manager が使用するデフォルト バージョンより後の Velero または OADP のマイナー バージョンまたはメジャー バージョンとは互換性がない可能性があります。

手順

1. PowerProtect Data Manager に **admin** ユーザーとしてログインをします。
2. `/usr/local/brs/lib/cndm/config/k8s-dependency-versions-app.properties` ファイルを開きます。
3. OpenShift 以外の環境では、このファイルに次の行を追加して Velero バージョンのアップデートを行い、ファイルを保存します。

```
k8s.velero.version=vx.y.z
```

ここでの vx.y.z は Velero 増分パッチ バージョンです。

4. OpenShift 環境では、このファイルに次の行を追加して OADP バージョンのアップデートを行い、ファイルを保存します。

```
k8s.oadp.version=x.y.z
```

ここでの x.y.z は OADP 増分パッチ バージョンです。

5. コマンド `cndm restart` を実行して CNDM サービスを再起動し、サービスが再開されるまで数秒待ちます。
6. PowerProtect Data Manager UI から、Kubernetes クラスターを手動で検出します。

検出が正常に完了すると、Kubernetes クラスタ `powerprotect` ネームスペースの構成マップ `ppdm-controller-config` に保存されている構成のアップデートが行われます。

7. 次のコマンドを実行して、Kubernetes クラスタ上の `powerprotect-controller pod` を削除します。このアクションにより強制的に再起動が行われ、その間に変更が有効になります。このステップは、バックアップまたはリストア操作が進行中でないときに実行する必要があります。

```
kubect1 get pod -n powerprotect
```

```
kubect1 delete pod powerprotect controller pod name -n powerprotect
```

8. PowerProtect Data Manager によって保護されている Kubernetes クラスタごとにステップ 6 と 7 を繰り返します。

完全性と整合性

トピック：

- [製品の完全性と整合性について](#)
- [検証](#)

製品の完全性と整合性について

PowerProtect Data Manager では、複数の方法を使用して、製品コードとダウンロードを侵害や破損から保護します。こういった方法には SHA-256 Checksum とデジタル署名があり、この章に記載されている方法を使用して検証することができます。

[カスタマーサポート](#)の [ドライバーおよびダウンロード] の箇所で、あらゆるファイルに対する一連の Checksum 値を提供しています。

導入ワークフローやアップデートワークフローなどの重要なプロセスでは、完全性と整合性が自動的に確認され、どちらか一方が侵害されている場合は失敗となります。しかしながら、コンポーネントとバイナリーの使用前に、次に示すいくつかの時点でこれらの確認が必要です。

- 導入パッケージまたはアップデートパッケージのダウンロード後。
- アプリケーション エージェントとその他のインストール可能な PowerProtect Data Manager バイナリーをダウンロード後。
- ホットフィックスのダウンロード後。

PowerProtect Data Manager の導入やアップデートなどの一部の手順には、証明書または署名を検証するための手順や機会が用意されています。

検証

以降のトピックでは、PowerProtect Data Manager のコンポーネントとバイナリーの完全性と整合性を検証する方法について説明します。通常、検証ではデジタル署名の適用以降にコンポーネントが変更されていないことを確認します。

一般的に、PowerProtect Data Manager のコンポーネントとバイナリーは、デジタル署名されているか、ファイルの検証に使用できる暗号形式の Checksum とともに提供されています。

各コンポーネントまたはバイナリーの Checksum は、[カスタマーサポート](#)、KB 記事、このガイド、または PowerProtect Data Manager 内で提供されている可能性があります。

Entrust Code Signing Root Certification Authority - CSBR1 の信頼できるルート認証局(CA)が環境にまだ含まれていない場合は、一部の検証操作が失敗する可能性があります。このような場合は、必要なルート証明書のインポートを行うことで署名を検証できます。例えば、vCenter Server にインポートをするなどです。

Windows バイナリーの署名者の検証

Windows の実行可能ファイルまたはドライバーが Dell によって署名され、署名以降変更されていないことを確かめるには、次の手順を実行します。

このタスクについて

ファイル システムエージェントや Microsoft Exchange Server エージェントなどの一部のコンポーネントは、Dell と Microsoft の両方が署名したドライバーを使用します。これらのエージェントは、バックアップおよびリストア操作にブロックベース バックアップ(BBB)ドライバーを使用します。通常、ドライバー(nsrbbb.sys)は、Windows システム フォルダーの C:\Windows\System32\drivers にあります。デュアル署名バイナリーの場合は、署名リストに Dell と Microsoft の両方のエンタリが含まれていることを確認します。

手順

1. Windows エクスプローラーでファイルを見つけて選択します。
2. ファイルを右クリックし、[Properties] を選択します。
[Properties] シートが、[General] タブで開きます。
3. [Digital Signatures] タブを選択します。
ファイルに関連づけられているデジタル署名のリストがタブに表示されます。
4. 署名リストに Dell Technologies のエントリーが含まれていることを確認します。
5. (オプション) [Details] をクリックして、デジタル署名フィールドを確認します。

Linux (RPM ベース) パッケージのベンダーの検証

Linux RPM パッケージ ファイルが Dell によって署名され、署名以降変更されていないことを確かめるには、次の手順を実行します。

手順

1. ターミナル ウィンドウまたはシェル セッションを開きます。
2. パッケージ ファイルがあるディレクトリーに移動します。
3. 次のように、パッケージ ファイルのプロパティを確認します。

```
rpm -qip package | grep Vendor
```

ここでの *package* は、パッケージ ファイル名です。

4. パッケージのベンダーが Dell EMC Corporation であることを確認します。

Linux (Debian ベース) パッケージのベンダーの確認

Linux Debian パッケージ ファイルが Dell によって署名され、署名以降変更されていないことを確かめるには、次の手順を実行します。

手順

1. ターミナル ウィンドウまたはシェル セッションを開きます。
2. パッケージ ファイルがあるディレクトリーに移動します。
3. 次のように、パッケージ ファイルのプロパティを確認します。

```
dpkg-deb --showformat='${Package}\t${Version}\t${Maintainer}\n' --show package
```

ここでの *package* は、パッケージ ファイル名です。

4. パッケージのベンダーが Dell EMC support <support@emc.com>であることを確認します。

Linux (RPM ベース) パッケージの GPG 署名の検証

Linux RPM パッケージ ファイルが Dell によって署名され、署名以降変更されていないことを確かめるには、次の手順を実行します。

前提条件

GnuPG (GPG)署名済み RPM パッケージ ファイルの場合、公開キーの有効期間は1年間です。各パッケージ ファイルを確認する際は、パッケージが署名された年の Dell 公開キーを使用します。これらの年次公開キーは、ナレッジベース(KB)記事 [KB000180913](#) および [KB000197389](#) 内に記載されています。

手順

1. ターミナル ウィンドウまたはシェル セッションを開きます。
2. パッケージ ファイルがあるディレクトリーに移動します。
3. 次のように、パッケージ ファイルが署名されていることを確認します。

```
rpm --checksig -v package
```

ここでの *package* は、パッケージ ファイル名です。

パッケージ ファイルが署名されている場合は、次のような出力が表示されます。

```
package:
Header V3 RSA/SHA1 Signature, key ID c5dfe03d: NOKEY
Header SHA1 digest: OK (81e359380a5e229d96c79135aea58d935369c827)
V3 RSA/SHA1 Signature, key ID c5dfe03d: NOKEY
MD5 digest: OK (cc2ac691f115f7671900c8896722159c)
```

NOKEY というメッセージは、Linux システムが署名キーを認識していないことを示しています。

4. KB 記事で該当する Dell 公開キーを見つけます。

Linux システム上の新しいテキスト ファイルに公開キーのコピーを作成し、ファイルを保存します。

5. 次のようにして、ローカルのトラストストアに Dell 公開キーのインポートを行います。

```
rpm --import keyfile
```

ここで、*keyfile* は前のステップで作成したテキスト ファイルです。

6. Dell 公開キーのインポートをした状態で、パッケージ ファイルに有効な署名が行われていることを再確認します。

```
rpm --checksig -v package
```

ここでの *package* は、パッケージ ファイル名です。

パッケージ ファイルに有効な署名が行われている場合は、次のような出力が表示されます。

```
package:
Header V3 RSA/SHA1 Signature, key ID c5dfe03d: OK
Header SHA1 digest: OK (81e359380a5e229d96c79135aea58d935369c827)
V3 RSA/SHA1 Signature, key ID c5dfe03d: OK
MD5 digest: OK (cc2ac691f115f7671900c8896722159c)
```

OK メッセージは、パッケージが信頼できるキーによって署名されていることを Linux システムが認識したことを示します。

JAR ファイルの署名の検証

一部の PowerProtect Data Manager コンポーネントは Java Archive (JAR)形式で提供されます。署名された JAR ファイルが署名後に変更されていないことを確認できます。

Java 環境が正しく構成されていることを確認し、Java Runtime Environment (JRE)または Java Development Kit (JDK)のインストール場所を把握しておきます。例えば、Java の場所を自分のシステムパスにするなどです。JDK の現在のバージョンには、適切なルート認証局が含まれています。

コマンドプロンプト、ターミナル ウィンドウ、またはシェル セッションを開き、次のコマンドを入力します。

```
jarsigner -verify <file>
```

ここで、*<file>* は JAR ファイルの名前です。JAR ファイルが現在のディレクトリーにない場合は、ファイルパスも必要です。

次の出力が表示されます。

```
jar verified.
```

Java により、アーカイブの署名以降、JAR ファイルの内容が変更されていないかどうかを検証されます。出力にエラーがないか確認します。

JAR ファイルの署名の詳細を確認するには、*-verbose* パラメーターを使用します。

Windows での SHA-256 Checksum の検証

ダウンロードをしたファイルを使用する前に、Dell が提供する SHA-256 暗号形式の Checksum と照合してファイルを検証できます。

コマンドプロンプトを開き、次のコマンドを入力します。

```
certutil -hashfile <file> SHA256
```

ここで、<file>はダウンロードをしたファイルの名前です。ダウンロードをしたファイルが現在のディレクトリーにない場合は、ファイルパスも必要です。

次のようなメッセージが表示されます。

```
SHA256 hash of file <file>:  
61 00 a8 28 82 99 86 f6 0c 43 dd e4 f8 8d 44 53 25 ab 55 48 1f 50 d9 9d 65 4a 87 70 67 54 f7 b2  
CertUtil: -hashfile command completed successfully.
```

計算された Checksum を、ダウンロードをしたファイルから取得した Checksum と比較します。このコマンドの出力にはスペースが含まれていますが、提供された Checksum には含まれていない場合があります。

Linux での SHA-256 Checksum の検証

ダウンロードをしたファイルを使用する前に、Dell が提供する SHA-256 暗号形式の Checksum と照合してファイルを検証できます。Checksum は、個別のファイルまたは文字列として提供されている場合があります。

Checksum ファイルが提供されている場合

ターミナル ウィンドウまたはシェルセッションを開き、次のコマンドを入力します。

```
sha256sum -c <file>*.sha256
```

ここで、<file>はダウンロードをしたファイルの名前です。ダウンロードをしたファイルが現在のディレクトリーにない場合は、ファイルパスも必要です。

次のようなメッセージが表示されます。

```
<file>: OK
```

Checksum ユーティリティにより、計算された Checksum と Checksum ファイルに保存されている値が自動的に比較されます。出力にエラーがないか確認します。

Checksum ファイルが提供されていない場合

ターミナル ウィンドウまたはシェルセッションを開き、次のコマンドを入力します。

```
sha256sum <file>
```

ここで、<file>はダウンロードをしたファイルの名前です。ダウンロードをしたファイルが現在のディレクトリーにない場合は、ファイルパスも必要です。

次のようなメッセージが表示されます。

```
43c403cb8a86fd3a3c75dc73c83cc81bae507ecf92195ee5fd1196eedc6e3076 <file>
```

計算された Checksum と Dell が提供する Checksum を手動で比較します。

AIX での SHA-256 Checksum の検証

ダウンロードをしたファイルを使用する前に、Dell が提供する SHA-256 暗号形式の Checksum と照合してファイルを検証できます。

ターミナル ウィンドウまたはシェルセッションを開き、次のコマンドを入力します。

```
openssl dgst -sha256 <file>
```

ここで、<file>はダウンロードをしたファイルの名前です。ダウンロードをしたファイルが現在のディレクトリーにない場合は、ファイルパスも必要です。

次のようなメッセージが表示されます。

```
SHA256(<file>) = 91ce20bc1a3db3001463125df6f136ff692356d122e09a4cb1044bce2d1063e9
```

計算された Checksum と Dell が提供する Checksum を手動で比較します。

その他の構成と管理の構成要素

トピック：

- ライセンス
- クライアントソフトウェアのインストール
- アプリケーションとアプリケーションデータのバックアップ

ライセンス

製品ライセンスのオプションと機能の詳細については、『*PowerProtect Data Manager ライセンス ガイド*』を参照してください。

クライアントソフトウェアのインストール

保護に関するクライアント側の要件は、資産タイプと操作環境ごとに異なります。PowerProtect Data Manager のアプリケーションエージェントおよび資産ユーザー ガイドには、必要なアカウント、認証情報、システムやリソースの権限など、データ保護のセキュリティ要件に関する具体的な情報が記載されています。

[ポートの使用方法](#) で、資産、エージェント、PowerProtect Data Manager コンポーネント間の通信に関する詳細を説明しています。

アプリケーションとアプリケーションデータのバックアップ

サーバー ディザスター リカバリー(DR)保護を構成し、サーバー DR バックアップからリカバリーをする手順については、『*PowerProtect Data Manager 管理およびユーザー ガイド*』を参照してください。バックアップの保存を構成し、既存のバックアップを管理できます。

デフォルトでは、PowerProtect Data Manager により、最初に保護ストレージシステムを使用するようサーバー DR が自動構成されます。デスティネーションは、『*PowerProtect Data Manager 管理およびユーザー ガイド*』の手順を使用して構成できます。

REST API の手順

この付録では、推奨されている方法が当てはまらない場合に、一部の手順を実行するための手順について説明します。

PowerProtect Data Manager REST API へのログインに、この付録に記載されているタスクの重要な動作条件である、アクセストークンを取得するための手順が記載されています。

トピック：

- 証明書の手動置き換え
- REST API を使用したローカル ユーザー パスワードの変更
- REST API を使用したコンプライアンス検証の構成

証明書の手動置き換え

さらに予防策が必要な一部の環境では、セキュリティ証明書を置き換えるための推奨方法が当てはまらない場合があります。次のトピックでは、推奨方法が当てはまらない場合に、PowerProtect Data Manager のデフォルトの自己署名セキュリティ証明書を、承認された認証局からの証明書に手動で置き換えるその他の方法について説明します。

「仮想ネットワーク」のガイダンスを確認してください。安全な方法を使用して、証明書とキーを PowerProtect Data Manager サーバーに送信してください。

証明書の手動置き換えトピックでは、必要な証明書とキーストアに次のファイル名プレースホルダーと命名表記法を使用します。

- *custom.pem* : PEM 形式で認証局 (CA) によって署名されたパブリック証明書チェーン
- *customkey.pem* : PKCS#1 (RSA) PEM 形式の対応するプライベート キー

オプション：

- *custom.keystore* : CA によって署名されたプライベート キーとパブリック証明書を含む Java キーストア
- *globalca.pem* : パブリック証明書に署名した CA の root 証明書

必要に応じて「キーストアからのパブリック証明書とプライベート キーの準備」を実行し、適切な形式の必要なファイルを準備します。次に、REST API を使用して、「REST API を使用したカスタム セキュリティ証明書の手動インストール」に従ってセキュリティ証明書を置き換えます。

キーストアからのパブリック証明書とプライベート キーの準備

プライベート キーとパブリック証明書を含んでいる Java キーストアがある場合、キーストアからキーと証明書を抽出します。

手順

1. PowerProtect Data Manager コンソールに接続し、root ユーザーに変更します。
2. *custom.keystore* を */etc/ssl/certificates/custom* ディレクトリーに安全にコピーします。
3. */etc/ssl/certificates/custom* ディレクトリーに変更します。

```
cd /etc/ssl/certificates/custom
```
4. キーストアから PEM 形式でパブリック証明書をエクスポートします。

```
keytool -list -alias custom -keystore custom.keystore -storepass custompass -rfc > custom.pem
```

custom をパブリック証明書に対応するキーストア エイリアスに置き換え、*custompass* をキーストアのパスワードに置き換えます。
5. キーストアからプライベート キーを PKCS#12 形式でエクスポートします。

```
keytool -importkeystore -srckeystore custom.keystore -srcalias custom -srcstorepass jkspass -destkeystore custom.p12 -deststoretype PKCS12 -storepass pkcspass
```

custom をプライベート キーに対応するキーストア エイリアスに置き換えます。 *jkspass* を Java キーストアのパスワードに置き換え、 *pkcspass* を PKCS ファイルのパスワードに置き換えます。

6. プライベート キーを PEM 形式に変換します。

```
openssl pkcs12 -in custom.p12 -passin pass:pkcspass -nocerts -nodes -out customkey.rsa
```

```
openssl rsa -in customkey.rsa -out customkey.pem
```

pkcspass を PKCS ファイルのパスワードに置き換えます。

7. 証明書の内容を出力します。

```
openssl x509 -text -in custom.pem
```

8. 出力から CA ルート証明書を抽出します。

CA ルート証明書を *globalca.pem* として保存します。

REST API を使用したカスタム セキュリティ 証明書の手動インストール

または、REST API を使用して、セキュリティ証明書を置き換えることもできます。 PEM 形式のパブリック証明書チェーンと、PKCS#1 (RSA) PEM 形式のプライベート キーが必要です。

このタスクについて

このタスクの証明書とキーの例は、分かりやすくするため、またスペースの都合上シンプルにされています。

REST API の使用方法に関する例など、詳細については、PowerProtect Data Manager REST API のドキュメントを参照してください。 任意の *curl* またはクライアントを使用し、ログインをしてから各コールに有効なアクセス トークンを指定します。 クライアントでは、自己署名証明書を使用するサーバーへの接続を許可するために追加のパラメーターが必要になる場合があります。

手順

1. 管理者またはセキュリティ管理者のロールを持つユーザーとして、PowerProtect Data Manager REST API にログインをします。 アクセス トークンを記録します。
2. セキュリティ証明書を置き換えます。

```
POST https://{{server}}:{{port}}/api/v2/certificates-replacement
```

```
Headers:
Content-Type: application/json
Authorization: Bearer {{access-token}}
```

```
{
  "privateKey": "{{private-key}}",
  "certificateChain": "{{cert-chain}}"
  "password": "{{password}}"
}
```

{{private-key}} を、*customkey.pem* の内容を表す \n で区切った 1 行の文字列に置き換えます。例：

```
-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEArG7\n7HmzXgmP+7owxddYeId\nuXzfA7hedyuxRSV7Whb\nQQKvO3fQz3ywb6i56Lq\n-----
END RSA PRIVATE KEY-----\n
```

{{cert-chain}} を、*custom.pem* の内容を表す \n で区切った 1 行の文字列に置き換えます。例：

```
-----BEGIN CERTIFICATE-----
\nMIIDdzCCA1+gAwIBAgI\nUzERMA8GA1UEChMIU21\nMDkyMjE4MDEzNFoXDTI\nBAoTC1BQRE0gU2VydmV\n-----
END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----
\nEHD0fXjANBgkqhkiG9w\nnd3cuc21nbi5jb20gYz1\nZ24gUm9vdCBDQTAeFw0\nBgNVBAYTA1VTMREwDwY\n-----
END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----
\nMIIDSTCCAjGgAwIBAgI\nnd3cuc21nbi5jb20gYz1\nZ24gUm9vdCBDQTAeFw0\nBgNVBAsTExd3dy5zaWd\n-----
END CERTIFICATE-----\n
```

パスワードは任意のフィールドで、暗号化されたプライベート キーを指定するときに使用されます。

REST API サービスから次の状態コードが返されます。

```

201 Created
{
  "id": "004c443c-3e55-44da-ac1a-59fe65fec13a",
  "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEARg7\n7HmzXgmP+7owxddYeId\nuXzfA7hedyuxRSV7Whb\nnQQKvO3fQz3ywb6i56Lq\n-----
END RSA PRIVATE KEY-----\n",
  "certificateChain": "-----BEGIN CERTIFICATE-----
\nMIIDdzCCAl+gAwIBAgI\nUzERMA8GA1UEChMIU21\nMDkyMjE4MDEzNFoXDTI\nBAoTC1BQRE0gU2VydMv\n-----
END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----
\nEHD0fXjANBgkqhkiG9w\nnd3cuc2lnbi5jb20gYz1\nnZ24gUm9vdCBDQTAEfw0\nBgNVBAYTAlVTMREwDwY\n-----
END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----
\nMIIDSTCCAjGgAwIBAgI\nnd3cuc2lnbi5jb20gYz1\nnZ24gUm9vdCBDQTAEfw0\nBgNVBAsTExd3dy5zaWd\n-----
END CERTIFICATE-----\n"
}

```

3. 既存の UI セッションの場合、ページを更新して新しい証明書が有効になるようにします。

次の手順

vCenter Server を追加した場合は、PowerProtect プラグインを再インストールします。 [vSphere Client 用 PowerProtect プラグインの再インストール](#) で詳細を参照してください。

デフォルトの自己署名セキュリティ証明書が UI に引き続き表示される場合は、 [Web サービスの再開](#) の手順を参照してください。

REST API を使用したローカル ユーザー パスワードの変更

ローカル ID プロバイダーユーザーのパスワードの期限が切れていて、そのユーザーが UI のパスワード期限切れプロンプトから移動した場合は、REST API を使用してパスワードを変更します。

前提条件

現在のパスワードがわからない場合は、「[ローカル ユーザーのパスワードをリセットする。](#)」で詳細情報を確認してください。外部 ID プロバイダーユーザーは、この手順を使用してパスワードをリセットすることはできません。ID プロバイダー管理者にパスワードのリセットを依頼してください。

このタスクについて

REST API の使用方法に関する例など、詳細については、PowerProtect Data Manager REST API のドキュメントを参照してください。任意の curl またはクライアントを使用します。クライアントでは、自己署名証明書を使用するサーバーへの接続を許可するために追加のパラメーターが必要になる場合があります。

手順

次のようにローカル ユーザーのパスワードを変更します。

POST https://*server*:*port*}/api/v2/account/change-password

Headers:
Content-Type: application/json

```

{
  "username": "username",
  "password": "existing-password",
  "newPassword": "new-password"
}

```

ここでの *username* と *existing-password* は期限切れの認証情報であり、*new-password* は一般的なパスワードポリシーに準拠する新しいパスワードです。

REST API サービスにより、状態コードとユーザー名が返されます。

REST API を使用したコンプライアンス検証の構成

一部のメンテナンス手順では、コンプライアンス検証を一時的に無効にしなければならない場合があります。このタスクは、他の場所で言及されている場合にのみ使用してください。

このタスクについて

REST API の使用方法に関する例など、詳細については、PowerProtect Data Manager REST API のドキュメントを参照してください。任意の curl またはクライアントを使用し、ログインをしてから各コールに有効なアクセス トークンを指定します。クライアントでは、自己署名証明書を使用するサーバーへの接続を許可するために追加のパラメーターが必要になる場合があります。

手順

1. 管理者ロールを持つユーザーとして、PowerProtect Data Manager REST API にログインをします。
アクセス トークンを記録します。
2. 次のようにコンプライアンス検証を無効にします。

POST https://{{server}}:{{port}}/api/v2/common-settings/COMPLIANCE_SETTING

Headers:

```
Content-Type: application/json
Authorization: Bearer {{access-token}}
```

```
{
  "id": "COMPLIANCE_SETTING",
  "properties": [
    {
      "name": "scheduleEnable",
      "value": "false",
      "type": "BOOLEAN"
    }
  ]
}
```

REST API サービスから状態コードが返されます。

3. 次のようにコンプライアンス検証を有効にします。

POST https://{{server}}:{{port}}/api/v2/common-settings/COMPLIANCE_SETTING

Headers:

```
Content-Type: application/json
Authorization: Bearer {{access-token}}
```

```
{
  "id": "COMPLIANCE_SETTING",
  "properties": [
    {
      "name": "scheduleEnable",
      "value": "true",
      "type": "BOOLEAN"
    }
  ]
}
```

REST API サービスから状態コードが返されます。