PowerProtect Data Manager 19.14
管理者ガイド

2023 年 7 月
Rev. 01

DELL Technologies

メモ、注意、警告

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

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

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

目次

前書き

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に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。

Isilon は PowerScale になりました。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 Isilon、Isilon 製品または Isilon アプライアンスの参考資料には、PowerScale 製品およびアプライアンスが含まれています。

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されておらず、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。

頭字語

このドキュメントでは、なじみのない頭字語が使用されているかもしれません。ほとんどの頭字語は、初回使用時にその定義が記載されますが、それ以降の箇所では定義が記載されない場合があります。すべての頭字語とその定義のリストについては、ドキュメントの最後にある用語集を参照してください。

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次のリリース時にリンクをアップデートします。

目的

『*Dell PowerProtect Data Manager* 管理者ガイド』では、PowerProtect Data Manager ソフトウェアの構成、使用、管理の方法を説明します。

対象読者

このドキュメントは、PowerProtect Data Manager ソフトウェアを導入することで、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	2023 年 7 月 11 日	PowerProtect Data Manager バージョン 19.14 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 管理者ガイド	ソフトウェアを構成、使用、管理する方法について説明します。このガイドには、ディザスター リカバリー手順も含まれています。資産保護に固有の手順については、個々のユーザー ガイドを参照してください。
PowerProtect Data Manager 導入ガイド	ソフトウェアの導入方法およびライセンスの取得方法が記載されています。
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記載されています。
PowerProtect Data ManagerAmazon 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 ManagerAzure 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 ManagerGoogle 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 ManagerCyber 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 ManagerKubernetes ユーザー ガイド	Kubernetes クラスターまたは Tanzu Kubernetes 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 ManagerMicrosoft 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 ManagerMicrosoft 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。

表 2. 関連ドキュメント （続き）

役職	コンテンツ
PowerProtect Data ManagerOracle 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。
PowerProtect Data ManagerSAP 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 ManagerStorage 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	VADP または Transparent Snapshots Data Mover (TSDM)のある 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 アップし、リストアするためにソフトウェアを構成し、使用する方法について説明しています。
PowerProtect Data Manager ストレージ アレイ ユーザー ガイド	ソフトウェアを構成し、使用して PowerStore ストレージ アレイ上のデータを保護し、リストアする方法について説明します。
PowerProtect Data Manager による *VMware Cloud Foundation* ディザスター リカバリー	VMware Cloud Foundation (VCF)環境のエンドツーエンドのディザスター 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 と、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 for Data Protection Systems インストールおよび管理ガイド	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： ● 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の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

最新のドキュメントを入手するには、PowerProtect Data Manager の情報ハブに移動するか、ブラウザーに `www.dell.com/ppdmdocs` と入力するか、モバイル デバイスで次の QR コードをスキャンします。

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。

サポート ライブラリー

サポート ライブラリーには適用可能なソリューションのナレッジ ベースが含まれています。ソリューション番号（例：KB000xxxxxx）またはキーワードでナレッジ ベースを検索できます。

サポート ライブラリーを検索するには、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、[Support Library] 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。

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、コミュニティー 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。DPADDocFeedback@dell.com

1

はじめに

トピック：

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。 ● 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 クラスター ● Microsoft Exchange Server および Microsoft SQL Server データベース ● Oracle Database ● SAP HANA データベース ● ネットワーク接続型ストレージ(NAS)共有 ● PowerStore ブロック ボリューム
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。

表 5. メリット （続き）

• 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。 • 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
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。 • 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 とそのコンポーネントは、特定の構成で IPv4 アドレスと IPv6 アドレスをサポートします。

表 6. サポートされる構成

コンポーネント	インターネット プロトコル
PowerProtect Data Manager コア	IPv4 のみ、または IPv4 と IPv6 の両方
PowerProtect Data Manager クラウド導入（AWS、Azure、GCP）	IPv4 のみ **メモ:** このチャートの他の項目とは異なり、PowerProtect Data Manager がクラウド環境に導入されている場合、クラウド内のコンポーネントは一切 IPv6 を使用できなくなります。
VM Direct、TSDM、検索	IPv4 のみまたは IPv6 のみ **メモ:** バック アップされる仮想マシンは、VM Direct が使用するのと同じプロトコルを使用する必要があります。仮想マシンでは IPv4 も IPv6 も使用できますが、VM Direct と TSDM ではできません。
PowerProtect Data Manager と統合されたアプリケーション エージェント：	**メモ:** IPv4 と IPv6 の両方が構成されていて、PowerProtect Data Manager の FQDN が使用されている場合、エージェントはネットワーク通信に IPv6 を使用します。
• ファイル システム	IPv4、IPv6、またはその両方
• Microsoft Exchange Server	IPv4 のみ、または IPv4 と IPv6 の両方
• Microsoft SQL Server（アプリケーション ダイレクト）	IPv4、IPv6、またはその両方
• Microsoft SQL Server (VM Direct)	IPv4 のみまたは IPv6 のみ **メモ:** VM Direct をサポートしているのは、Microsoft SQL Server エージェントのみです。
• Oracle RMAN	IPv4、IPv6、またはその両方

表 6. サポートされる構成 （続き）

コンポーネント	インターネット プロトコル
• SAP HANA • Storage Direct	IPv4、IPv6、またはその両方 IPv4 のみ
スタンドアロン アプリケーション エージェント	IPv4 のみ
NAS（ネットワーク接続型ストレージ）	IPv4、IPv6、またはその両方
ストレージ アレイ(PowerStore)	IPv4 のみ
Kubernetes	IPv4 のみ
PowerProtect Data Manager 管理	IPv4 または IPv6
PowerProtect DD 通信	IPv4 または IPv6
レポート ブラウザー	IPv4 のみ **メモ:** PowerProtect Data Manager が IPv4 と IPv6 の両方を使用するように構成されている場合、レポートの正確な日付と時刻の情報を得るために、NTP サーバーを構成し、タイム ゾーンを設定する必要があります。
SupportAssist	IPv4、IPv6、またはその両方
Syslog ログ サーバー ゲートウェイ	IPv4 または IPv6

次の制限事項と考慮事項が適用されます。

コンポーネントとの通信

PowerProtect Data Manager が 1 個のプロトコルのみを使用するように構成されている場合、通信するすべてのコンポーネントもそのプロトコルを使用する必要があります。PowerProtect Data Manager が通信するコンポーネントの中に、IPv4 を使用するものと IPv6 を使用するものがある場合は、IPv4 と IPv6 の両方を使用するように PowerProtect Data Manager 構成する必要があります。

DD システムと DDVE

DD システムまたは DDVE インスタンスが IPv6 のみを使用する場合は、保護ポリシーを追加または編集するときに、必要な IPv6 インターフェイスを手動で選択する必要があります。

ネットワーク接続型ストレージと DD システム ストレージ ユニット

保護ポリシーのストレージ ユニットが異なる場合、またはターゲット資産ソースから変更された場合は、リストアを正常に行うために、ターゲット資産にネットワークを割り当てる必要があります。たとえば、ソース資産が IPv6 ネットワークでバックアップされている場合、リストアを正常に行うには、ターゲット資産に IPv6 ネットワークを割り当てる必要があります。

ターゲット資産にネットワークを割り当てるには、次の手順を実行します。

1. PowerProtect Data Manager UI で、[Infrastructure] > [Assets] > [NAS] の順に選択します。
2. ターゲット資産を選択し、[More Actions] をクリックして、[Assign Network] を選択します。[Assign Network] ページが表示されます。
3. [Network Label] リストからネットワークを選択し、[Save] をクリックします。
4. 間違ったターゲット アドレスが原因でリストアが失敗した場合は、操作を再試行します。

ディザスター リカバリー

PowerProtect Data Manager サーバーをリカバリーすると、保護ポリシーの構成と競合する可能性があります。たとえば、リカバリーされたサーバーが IPv4 のみを使用するように構成されている場合、IPv6 を使用するように構成された保護ポリシーは実行できません。

名前解決

名前解決とリバース IP ルックアップを構成して、次の動作が確実に行われるようにする必要があります。

- PowerProtect Data Manager、そのコンポーネント、DD コンポーネントの完全修飾ドメイン名が有効な IPv4 アドレスまたは IPv6 アドレスに解決される。
- IPv4 アドレスと IPv6 アドレスの両方が DD に使用されている場合、両方のアドレスが同じ FQDN に解決される。
- すべての IPv4 アドレスと IPv6 アドレスが有効で、到達可能である。
- FQDN を優先ホスト アドレスとして使用するアプリケーション エージェント ホストの FQDN は、有効な IPv4 または IPv6 アドレスに解決されます。
- FQDN を優先ホスト アドレスとして使用する各アプリケーション エージェント ホストは、それ自体が使用する同じプロトコルの IP アドレスに PowerProtect Data Manager の FQDN を解決します。たとえば、ホストが IPv4 を使用している場合、PowerProtect Data Manager の FQDN は IPv4 アドレスに解決されます。

サーバーのアップデート

IPv6 は、PowerProtect Data Manager 19.12 以降の新規導入でのみサポートされます。PowerProtect Data Manager 19.11 以前のバージョンからアップデートした後に IPv6 を使用することはサポートされていません。

Search Engine のインデックス作成と IPv4 のみのシステムへの IPv6 の追加

IPv4 のみのシステムに IPv6 を追加すると、既存の Search Engine のクラスターからのインデックス作成は一切使用できなくなります。IPv6 を追加した後、すべての IPv4 Search Engine ノードを削除して Search Engine クラスターを削除し、新しい IPv6 ノードを新しいクラスターに追加する必要があります。

他の PowerProtect Data Manager コンポーネントとは異なり、Search Engine で IPv6 をが使用されている場合、すべての Search Engine ノード, Search Engine nodes システムおよび関連 DD システムの FQDN は、IPv4 アドレスではなく、常に IPv6 アドレスに解決される必要があります。

ストレージ ポリシー ベースの管理

vCenter または ESXi 7.0u2 以前のバージョンが IPv6 のみを使用している場合は、PowerProtect Data Manager FQDN を使用して SPBM プロバイダーを追加する必要があります。

vSphere Client 用 PowerProtect プラグインの `Service Unavailable` メッセージ

vCenter が vSphere Client 用 PowerProtect プラグインと IPv6 を使用していて、その IPv6 アドレスまたは FQDN を使用して vCenter ホストを PowerProtect Data Manager に追加した場合、`Service Unavailable` メッセージが保護されている仮想マシンに対して表示されることがあります。保護されている仮想マシンのバックアップとリストアは影響を受けず、これらのメッセージは無視しても構いません。

伸長されている IPv6 形式

DD 7.4.x 以前のシステムにあり、伸長されている IPv6 形式を使用するように構成されたネットワーク インターフェイスは、検出できません。伸長されている IPv6 形式は、`2620:0000:0170:0597:0000:0000:0001:001a` のようになります。短縮された IPv6 形式は、`2620:0:170:597::1:1a` のようになります。これらのネットワーク インターフェイスを使用するには、IPv4 アドレスまたは短縮された IPv6 アドレスのいずれかを使用するように再構成してから、検出を開始してください。

サポートされていないファイルシステムの変更

PowerProtect Data Manager および PowerProtect DD システムのファイルとディレクトリーは、のドキュメントとガイダンスに従っている場合にのみ変更する必要があります。

製品ガイドに記載されていないか、カスタマー サポートから伝達されていない、次のファイルシステム操作の実行はサポートされていません。

- ファイルまたはディレクトリーの追加、削除、編集、その他の変更

- 読み取り専用権限以外を使用した DD ファイル システムの手動マウント
- ファイルシステム手順の変更
- ファイルシステム手順のステップのコマンドを別のコマンドで置き換えること

参考情報

本書の手順の一部に関するさらなる詳細については、他の関連資料を参照してください。

PowerProtect Data Manager 出版物のリストについては、「はじめに」の「関連ドキュメント」を参照してください。

DD Virtual Edition の詳細については、カスタマー サポートで次の文書を参照してください。

表 7. 関連する PowerProtect DD Virtual Edition ドキュメント

PowerProtect DD Virtual Edition in VMware Cloud インストールおよび管理ガイド
PowerProtect DD Virtual Edition in Google Cloud Platform インストールおよび管理ガイド
PowerProtect DD Virtual Edition on Premise インストールおよび管理ガイド
PowerProtect DD Virtual Edition in Azure インストールおよび管理ガイド
PowerProtect DD Virtual Edition in Amazon Web Services インストールおよび管理ガイド

の用語

PowerProtect Data Manager ユーザー インターフェイスおよびドキュメントの用語を理解しておいてください。

次の表には、PowerProtect Data Manager を使用するために知る必要がある名前と用語の詳細情報が記載されています。

表 8. 用語リスト

用語	説明
アプリケーション エージェント	PowerProtect Data Manager を使用して、保護を管理するアプリケーション エージェントは、アプリケーションまたはデータベース ホスト サーバーに、インストールされています。これらのエージェントは、データベースとアプリケーション向けで、一般的に DD Boost Enterprise Agents (DDBEA)と呼ばれています。
アプリケーション対応	Microsoft SQL Server 用の追加のアプリケーション対応データ保護を含む仮想マシンの保護ポリシーです。アプリケーション対応の仮想マシン保護ポリシーでは、仮想マシンのイメージのバックアップ中にアプリケーションを停止して、Microsoft SQL Server データベースのフル バックアップを実行する機能が提供されます。また、ポリシー内にある仮想マシンの Microsoft SQL Server のログ バックアップをスケジュールすることもできます。
資産	資産とは、仮想マシン、データベース、ファイル システムなどを含め、保護を管理する PowerProtect Data Manager のオブジェクトを指します。
資産ソース	PowerProtect Data Manager の保護対象の資産は、vCenter Server、アプリケーションまたはデータベース ホスト、およびファイル サーバーを含む資産ソース内に存在します。
クラウド階層ストレージ	クラウド階層ストレージを保護ストレージ システムに追加して、重複排除ストレージ容量を、Elastic Cloud Storage のセキュアなアプライアンスを含む、パブリックまたはプライベート オブジェクト ストレージ クラウド内の低コストのオブジェクト ストレージに拡張できます。
コピー	PowerProtect Data Manager のコピーは、資産の point-in-time バックアップ コピーとなります。
コピー マップ	PowerProtect Data Manager コピー マップは、保護ストレージ上のバックアップ コピーの場所を視覚的に表示したものであり、コピーがある保護されたすべての資産に対して使用できます。
検出	検出は、インフラストラクチャ コンポーネントを保護してスキャンし、その稼働状態とステータスを監視するために、資産ソースをスキャンして新しい資産を検索する内部処理です。
インスタント アクセス	PowerProtect Data Manager 仮想マシンバックアップ コピーは、実行中の仮想マシンとして、保護ストレージ ターゲットから直接アクセス、マウントおよび起動できます。この操作は、インスタント アクセスと呼ばれます。vMotion を使用して、コピーを本番環境の VMware データストアに移動することもできます。PowerProtect Data Manager 仮想マシンのアプリケーション対応バックアップ コピーを、実行中の Microsoft SQL Server データベースとして保護ストレージから直接マウントできます。これには、ログ バックアップをロール フォワードする機能

表 8. 用語リスト （続き）

用語	説明
	が含まれます。vMotion を使用して、これらの Microsoft SQL Server データベース ディスクを本番 VMware データストアに移動させることもできます。
PowerProtect Data Manager エージェント	PowerProtect Data Manager を介してアプリケーション エージェントをモニタリングおよび管理するために、PowerProtect Data Manager に含まれるエージェントです。各アプリケーション エージェント ホスト サーバーにインストールされます。
保護ポリシー	保護ポリシーは、バックアップ タイプ、資産、バックアップの開始時間と終了時間、バックアップ デバイス、バックアップの保存期間を含む、バックアップ データのライフ サイクル全体を構成し、管理します。
サービスレベル アグリーメント(SLA)	保護ポリシーの上に重ねることのできるオプションのポリシーです。SLA では、保護アクティビティーについて追加でチェックを実行することにより、保護目標が組織の基準を満たしていることを確認します。SLA は、1 個以上のサービスレベル目標で構成されています。
サービスレベル目標(SLO)	企業の要件に従って、バックアップの目標リカバリーポイント(RPO)、暗号化、場所の基準を設定する定義可能なルール。

PowerProtect Data Manager UI へのアクセス

PowerProtect Data Manager では、Web ベースの UI を使用して、ネットワーク上の任意の場所からシステム機能と設定を管理および監視できます。

このタスクについて

非アクティブ状態が 30 分を超えると、このインターフェイスが応答しなくなったり、次のエラーのいずれかが表示されたりすることがあります。

- `401: Authentication Required`
- `503: Unknown Error`

これらの問題を解決するには、ブラウザーを更新してログインします。それまでログインしていた場合も、再度ログインする必要があります。

手順

1. 仮想アプライアンスへのネットワーク アクセス権を持つホストから、Google Chrome の最新版を使用してアプライアンスに接続します。
   `https://<appliance_hostname>`
   メモ: アプライアンスのホスト名または IP アドレスを指定できます。

2. ユーザー名とパスワードを使用してログ インします。

   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。
   - 多要素認証 (MFA)が有効になっている場合、［Multi-Factor Authentication］ダイアログ ボックスで パスコードが求められます。PowerProtect Data Manager は、MFA サービスでこの パスコードを検証してからログインを許可します。

   メモ:

   期限切れのパスワードを使用してログ インをしている場合は、すぐにパスワードのリセットを行ってください。パスワードを変更する前に［Cancel］をクリックするか、ブラウザーを閉じるか、ページから移動すると、認証情報が以降のログインで無効になります。ログ インした際に、ログイン認証情報が古くなっているためパスワードを変更するように求めるメッセージが表示された場合は、現在のパスワードと新しいパスワードを入力し、確認のために新しいパスワードをもう一度入力してから続行してください。

   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。

   使用可能なユーザー ロールと関連する権限の詳細については、『*PowerProtect Data Manager* セキュリティ構成ガイド』を参照してください。アカウントに関連づけられたロールによって、ユーザーが表示および使用できる UI の部分と、ユーザーが実行できる操作が決まります。

初めて PowerProtect Data Manager UI にアクセスする場合は、未署名の証明書についての警告が web ブラウザーに表示されることがあります。

PowerProtect Data Manager UI と Web ブラウザーとの間の通信を暗号化するセキュリティ証明書は、自己署名されています。自己署名証明書は、安全な web ページをホストしている Web サーバーによって署名されます。この証明書は問題ありません。この証明書は、Web ブラウザーとサーバーとの間で暗号化されたチャネルを確立するには十分なものです。ただし、これは信頼できる認証局によって署名されていません。

［Get Started］ウィンドウが表示され、最初の導入時に必要な構成オプションが表示されます。このウィンドウをスキップして、［Dashboard］に直接移動するには、［Launch］をクリックします。

［Dashboard］ウィンドウの詳細は、次のとおりです。

- 左ペインには、使用可能なメニュー アイテムへのリンクが表示されます。その他のオプションを表示するには、メニュー アイテムを展開します。
- PowerProtect Data Manager バナー内のアイコンで、その他のオプションが提供されます。

Get Started ウィンドウ

［Get Started］のウィンドウから、PowerProtect Data Manager システムを最初に導入する際に必要な構成オプションを利用できます。このウィンドウは、［Launch］をクリックするまで、毎回のログ イン時にデフォルトで表示されます。

［Get Started］ウィンドウには、いつでもアクセスできます。未構成の開始オプションを表示するには、  をクリックして、［Getting Started］を選択します。

［Get Started］ウィンドウでは、次のメニュー項目を構成または編集できます。

表 9. PowerProtect Data Manager Get Started のメニュー項目

オプション	説明
［License］	［License］ウィンドウを起動すると、ライセンス ファイルを PowerProtect Data Manager に追加するよう求められます。ライセンスがアップロードされると、ライセンスの詳細（容量の使用状況やソフトウェア ID など）が表示されます。
［サポート］	［Support］ウィンドウを起動すると、SupportAssist と AutoSupport を構成し、アプリケーション通知とメッセージ用に E メール サーバーをセット アップできます。
［資産］	［Asset Sources］ウィンドウを起動すると、PowerProtect Data Manager がサポートする資産ソース タイプを有効化できます。資産ソースを有効にした後で、資産の保護のためにソースを追加および登録できます。
［ストレージ］	［Add Storage］ウィンドウを起動すると、プライマリ バックアップおよび複製されたコピーの保護ストレージとして、PowerProtect DD システムまたは PowerProtect DD Management Center を追加できます。

UI ツールおよびオプション

PowerProtect Data Manager UI で使用可能なツール、ウィンドウ、バナーのオプションについて説明します。

PowerProtect Data Manager UI ツールとウィンドウ

次の表に、PowerProtect Data Manager UI 左ナビゲーション ペインのツールとウィンドウを示します。

表 10. PowerProtect Data Manager ツール

メニュー項目	説明
 ダッシュボード	［Dashboard］をクリックして、PowerProtect Data Manager システムの全体的な状態を表示します。
 正常性	［Health］をクリックすると、PowerProtect Data Manager システム全体の正常性（良好、正常、不良）のスコアが表示されます。

表 10. PowerProtect Data Manager ツール （続き）

メニュー項目	説明
インフラストラクチャ	[Infrastructure] をクリックして次の操作を行います。 ● すべての資産を表示して管理します。 ○ VMware 仮想マシン ○ ファイル システム ○ VMAX ストレージ グループ メモ: PowerProtect Data Manager アプライアンスは対象外です。 ○ Kubernetes クラスター ○ Microsoft Exchange Server データベース ○ ネットワーク接続型ストレージ(NAS) ○ Microsoft SQL Server データベース ○ Oracle Database ○ SAP HANA データベース ○ ブロック ボリューム ● vCenter と、アプリケーションおよびファイル システムのホスト資産ソースを追加します。 ● 統合ストレージを表示して管理します。 ● 仮想マシンのデータ保護を目的とする VM Direct 保護エンジンを備えた VM Direct アプライアンスを追加します。 ● Transparent Snapshot Data Mover （TSDM） 保護メカニズムを使用して実行される、仮想マシンのクラッシュ コンシステントなデータ保護用の vSphere Installation Bundle （VIB） を管理します。 ● Oracle RMAN エージェント、Microsoft Application Agent、SAP HANA エージェント、File System Agent の登録を管理します。 ● クラウド ディザスター リカバリーを表示して管理します。 ● 検索クラスターの作成と管理 ● PowerProtect Cloud Snapshot Manager テナントを、ジョブ、アラート、レポートの資産ソースとして追加します。
保護	[Protection] をクリックして次の操作を行います。 ● 保護ポリシーを追加して、資産をバックアップします。 ● サービスレベル アグリーメント(SLA)を管理します。 ● ポリシーに含まれる資産の保護ルールを追加、編集、削除します。 ● ファイル システム保護ポリシーのファイル除外テンプレートを追加、編集、削除します。
リストア	[リストア] をクリックして、次の手順を実行します。 ● 資産コピーの場所の詳細を表示し、リストア操作を開始します。 ● インスタント アクセス セッションを管理します。 ● ファイル検索機能を使用して、仮想マシン ファイルのコピーを検索およびリストアします。
アラート	[Alerts] をクリックして次の操作を行います。 ● アラートとイベントを表示し、確認する ● 重大、警告、情報の各ステータスでアラートをフィルタリングし、時間範囲を指定します。 ● 監査ログを表示および分析します。 ● 監査ログを .csv ファイルにエクスポートする ● 監査ログの境界を設定する ● アラート通知の構成。 また、  で表されるバナー UI オプションもあります。このアイコンは、未確認のすべてのアラートを表示するためのリンクです。
管理	[Administration] をクリックして次の操作を行います。 ● ユーザーとロールを設定します。 ● パスワードの認証情報を設定し、キー チェーンを管理します。 ● 証明書を表示および置換します。 ● 外部 ID プロバイダーを追加します。 ● リソース グループを表示および管理します。

表 10. PowerProtect Data Manager ツール （続き）

メニュー項目	説明
 レポート	［Reports］をクリックして、PowerProtect Data Manager の［Report Browser］と［Reporting Engine］にアクセスします。
 ジョブ	［ジョブ］をクリックして、ジョブの管理、保護別またはシステム別の表示、絞り込み、詳細の表示を行うことができます。

バナー UI のオプション

次の表で、PowerProtect Data Manager UI バナーのアイコンについて説明します。

表 11. バナー UI のオプション

オプション	説明
	クリックするとお客様からのフィードバックを提出します。
	これをクリックして検索基準を入力し、資産、ジョブ、ログおよびアラートを検索します。
	このアイコンの横にある数字は、過去 24 時間の重大な未確認アラートを示します。 クリックして展開できる未確認のアラートの詳細には、次のようなものがあります。 ● 未確認のアラートの合計数（すべてのステータス：重大、警告、情報）、または過去 24 時間の未確認のアラート（［New］タグでマーク）です。 ● 未確認の重大アラートの数、または過去 24 時間の未確認の重大アラート（［New］タグでマーク）の数。 このメニュー内で、これらのリンクのいずれかをクリックして［Alerts］ウィンドウを開きます。ここでは、未確認のアラートに関する具体的な詳細を表示できます。
	クリックすると、クイック リカバリーを使用して、レプリケートしたコピーから資産をリストアできます。このアイコンは、システムがソース システムからレプリケートしたメタデータを受信している場合にのみ表示されます。
	クリックして、PowerProtect Data Manager システム ネットワーク、タイム ゾーンと NTP 設定、DR バックアップ、セキュリティ、ライセンス、アップデート、認証、エージェントのダウンロード、およびサポートを構成して管理し、［Get Started］ウィンドウにアクセスします。
	クリックすると、PowerProtect Data Manager に関する詳細情報の取得、カスタマー サポートへのアクセス、REST API ドキュメントの表示を実行できます。
	クリックしてログ アウトするか別のユーザーとしてログ インする、または現在のユーザー パスワードを変更します。
	クリックして、CloudIQ、Dell APEX Backup Services、Cloud Snapshot Manager、vProtect を起動します。 **メモ:** Cloud Snapshot Manager のみが PowerProtect Data Manager アプライアンスに適用されます。

ダッシュボード

PowerProtect Data Manager UI にログ インするとダッシュボードが表示され、左側のナビゲーション ペインからアクセスできます。

［Dashboard］ウィンドウには、6 個のウィジェットを通じて PowerProtect Data Manager システムの全体的な状態のハイレベル ビューが表示されます。次の表に、各ウィジェットの説明を示します。

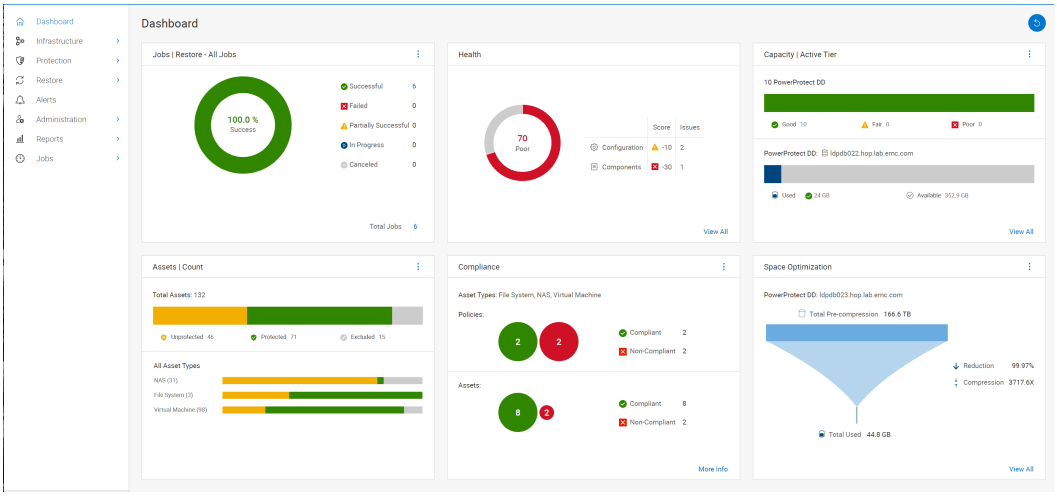


図 1. ダッシュボードのウィジェット

表 12. PowerProtect Data Manager ダッシュボード

ダッシュボード ウィジェット	説明
[ジョブ|保護] [ジョブ|リストア] [ジョブ|システム] [ジョブ|資産レベル]	このウィジェットは、PowerProtect Data Manager で進行中の、または指定された期間に実行されたバックアップ、リストア、システム ジョブのステータスを色分けで表示します。[Jobs | Protection] はデフォルトで表示され、過去 24 時間に実行されたジョブが表示されます。 ウィジェットの上部にある 3 個の縦のドットをクリックして、次の操作を実行します。 ● [Protection]、[Restore]、[System]、[Asset Level] のいずれかを選択して、ウィジェットのジョブ ビューを切り替えます。 ● 表示するジョブの期間（過去 24 時間、過去 3 日間、過去 7 日間、またはすべて）を選択します。期間を選択すると、ウィジェットがアップデートされ、その期間内に実行されたジョブのみが表示されます。 チャート内の色をクリックして、特定のステータスのジョブに関する詳細を表示するか、各ステータスの横にあるリンクをクリックします。これにより、選択したステータスと期間に一致するジョブが表示されるようフィルタリングされた対応する [Jobs] ウィンドウが開きます。このウィンドウから、ジョブの管理、詳細の表示、ジョブの検索を行うことができます。
[Assets | Count] および [Assets | Size]	このウィジェットの詳細には、PowerProtect Data Manager で追加および有効化された各資産ソースの保護対象資産、保護されていない資産、除外された資産の数が含まれます。また、各資産ソースの資産の合計数と、これらの資産の合計サイズを表示することもできます。[Assets | Count] はデフォルトで表示され、資産タイプは、ビューに応じて、保護されていない資産総数の割合、または資産ソースの保護されていない資産の合計サイズに基づいて分類されます。 ウィジェットの上部にある 3 個の縦のドットをクリックして、次の操作を実行します。 ● [Count] または [Size] を選択して、ウィジェットの資産ビューを切り替えます。 ● リストから 1 個以上の資産ソースを選択します。単一の資産ソース、複数の資産ソース、またはすべての資産ソースの資産統計を表示できます。 色にカーソルを合わせると、保護されている資産、保護されていない資産、除外された資産の正確な数、およびこれらの資産の合計サイズが表示されます。色をクリックして、選択したステータスに一致する資産を表示するようにフィルタリングされた [Infrastructure] > [Assets] ウィンドウを開きます。
[正常性]	このウィジェットには、PowerProtect Data Manager システム全体の正常性（良好、普通、不良）のスコアが表示されます。正常性の詳細とステータスは、次のカテゴリーで提供されます。 ● コンポーネント：ハードウェアおよびソフトウェア サービスの状態（例：実行中または失敗）を識別します。 ● 構成：システム サポートの構成など、PowerProtect Data Manager 構成の要素が不完全であるかどうかを示します。 ● 容量：関連したストレージ システムのプロビジョニング済みおよび現在割り当て済みのサイズを識別します。 ● パフォーマンス：主要なパフォーマンス インジケーター（例：メモリー使用）を識別します。 ● データ保護：主要な保護インジケーター（例：サービスレベル アグリーメントが満たされていない、ディザスターリカバリーのバックアップ コピーが存在しない）を識別します。

表 12. PowerProtect Data Manager ダッシュボード （続き）

ダッシュボード ウィジェット	説明
	すべてのカテゴリーにあるシステム正常性の問題の詳細を表示するには、［View All］をクリックします。
［コンプライアンス］	このウィジェットには、サービス レベル アグリーメント(SLA)にリンクされている保護ポリシーのコンプライアンス検証統計情報が表示されます。ウィジェットは、これらのポリシー内にある資産の内、準拠している資産と非準拠の資産の数も識別します。 ウィジェットの上部にある 3 個の縦のドットをクリックして、リストから 1 個以上の資産ソースを選択します。単一の資産ソース、複数の資産ソース、またはすべての資産ソースのコンプライアンス統計を表示できます。デフォルトでは、準拠および非準拠資産の保護ポリシーの合計数と数は、すべての資産ソースに対して表示されます。 ［View All］をクリックして［Protection］ > ［SLA Compliance］ウィンドウを開きます。ここでは、非準拠の特定のポリシーと資産の詳細を表示できます。
［Capacity | Active Tier］および［Capacity | Cloud Tier］	このウィジェットには、アクティブ階層およびクラウド階層の PowerProtect Data Manager のこのインスタンスに関連付けられている DD 保護ストレージ システムの容量ステータスが表示されます。各 DD システムで使用可能な容量に基づいて、色分けされた棒グラフには、［Good］（>20%使用可能）、［Fair］（<20%使用可能）、［Poor］ (<10%)のシステムの数が表示されます。 ウィジェットの上部にある 3 個の縦のドットをクリックして、次の操作を実行します。 ● ［Active Tier］または［Cloud Tier］を選択して、ウィジェット内のアクティブ階層とクラウド階層の保護ストレージ システムのビューを切り替えます。デフォルトでは、ウィジェットには［Capacity | Active Tier］が表示されます。 ● リストから DD システムを選択します。ウィジェットがアップデートされ、選択した DD システムの容量統計が表示されます。一度に表示できる容量統計は、1 個のシステムのみです。 ［View All］をクリックして、［Infrastructure］ > ［Storage］ウィンドウを開きます。ここでは、特定の保護ストレージ システムの詳細を表示できます。
［領域の最適化］	このウィジェットには、PowerProtect Data Manager のインスタンスに関連付けられた個々の DD システムにおけるアクティブ階層ストレージ容量の効率性に関する情報が表示されます。効率性は、システム上の圧縮後データのサイズと比較した圧縮前データのサイズに基づいて決定されます。 ウィジェットの上部にある 3 個の縦のドットをクリックして、リストから DD システムを選択します。ウィジェットがアップデートされ、選択した DD システムの領域の最適化統計が表示されます。

データをエクスポートする

PowerProtect Data Manager では、CSV 形式でテーブル データのエクスポートと保存を行うことができます。

前提条件

PowerProtect Data Manager UI で、［Export All］機能を含むウィンドウを参照します。

このタスクについて

次の表に、［Export All］機能がサポートされているウィンドウがリスト表示されています。

表 13. サポートされているウィンドウ

メニュー項目	ウィンドウ
正常性	正常性
インフラストラクチャ	資産
	アプリケーション エージェント
保護	保護ポリシー 保護ポリシーに割り当てられている資産のレコードをエクスポートできます。保護ポリシーを選択して詳細を表示し、［Assets］の横にある資産数のリンクをクリックします。

表 13. サポートされているウィンドウ （続き）

メニュー項目	ウィンドウ
	SLA コンプライアンス
	保護ルール 保護ルールに適用されている資産のレコードもエクスポートできます。保護ルールの［Assigned Assets Count］列のリンクをクリックします。
リストア	資産
アラート	システム
管理	［Access Control］ > ［Users/Groups ］
	［Access Control］ > ［Resource Groups ］ リソース グループに割り当てられている資産のレコードもエクスポートできます。リソース グループの横にあるをクリックしてから、右ペインで［View Assets］をクリックします。
	監査ログ
ジョブ	保護ジョブ
	システム ジョブ
システム設定	メッセージ カタログ

手順

1. （オプション）テーブルに表示される情報のフィルタリングおよび分類を行います。
2. ウィンドウで、［Export All］をクリックして、 `.csv` ファイルとしてデータをエクスポートします。

   メモ: ［Protection Policy］ウィンドウの表に適用されたフィルターは、エクスポートした `.csv` ファイルには適用されません。エクスポートした保護レコードには、テーブルに示されているすべてのデータが含まれます。保護結果の分類およびフィルタリングを行うには、Excel ファイルのダウンロードを実行してください。

エクスポート対象フィールド

次の表では、［Export All］機能を使用したエクスポート対象となるフィールドが一覧表示されています。フィールドのエクスポートは、CSV 形式で行われます。

表 14. エクスポート対象フィールド

Resource	エクスポート対象フィールド
ジョブ	`Asset Name, Host, Component Type, Component Description, Schedule Frequency, Job ID, Status, Description, Job Type, Sub Type, Asset Type, Assets, Start Time, End Time, Duration, Next Scheduled, Policy Name, Data Transferred, Storage System, Asset Size, Data Compressed, Average Throughput, Total Compression Factor, Reduction Percentage`
アプリケーション エージェント	`Host Name, IP, Registration Status, OS, Agent Type, Current Version, Update Status, Port, Application Version, Created Date, Registered Date, Throttling Status, CPU Throttling`
アラート	`Message ID, Details, Recommended Action, Severity, Date, Summary, Category, Status,Component Type, Component Description`
メッセージ カタログ	`Message ID, Message, Details, Recommended Action, Severity, Category`
保護ポリシー	`Name, Category, Asset Type, Asset Count, Protected Asset Size, Last Run Status, Violations, State`

表 14. エクスポート対象フィールド （続き）

Resource	エクスポート対象フィールド
リソース グループ	Name, Description, Created At, Number of Resources
SLA コンプライアンス	Name, Compliance Type, Policies At Risk, Objectives out of Compliance, Impacted Assets
システム稼働状態の問題	Deduction, Issue, Category, Component, Remediation, Date
ユーザー	User/Group Name, Type, First Name, Last Name, Email Address, Roles and Resources, Added Date

次のフィールドは、各資産タイプに共通しています。

ID, Status, Asset Type, Sub Type, Protection Policy ID, Protection Policy, Protection, Size, Protection Capacity Size, Protection Capacity Time, Last Copy, Network, Protection Rule Name, Resource Group Name

次の表では、各資産タイプに固有のフィールドが一覧表示されています。

表 15. 資産タイプ別のエクスポート対象フィールド

リソース（資産タイプ）	エクスポート対象フィールド
VMware 仮想マシン	Name, Tags, Operating System, Apps, Disk Excluded, vCenter, Protection Mechanism, ESX Host Name, VM BIOS Uuid, Resource Pool, VM Folder, Data Center
Kubernetes	Namespace, Labels, Age, Cluster, PVCs Excluded, Storage Class Name, Volume Mode, PVC Namespace
Microsoft SQL Server	Name, Protection Engine Flow, Host Type, Host/Cluster/Group Name, Application Server ID, Application Server Name
Oracle	Name, Host/Cluster/Group Name, Host Type, OS Type, Application Server Name, Application Server ID, SID, Data Guard Name, Data Guard Role, Protocol, Backup Technology
Microsoft Exchange Server	Name, Host/Cluster/Group Name, Host Type, Application Server Name, Application Server ID
SAP HANA	Name, Host/Cluster/Group Name, Host Type, Application Server Name, Application Server ID
ファイル システム	Name, OS Type, File System Type, Host Name, Host Operating System
NAS	Name, Asset Source, Appliance Name, Array Type, Server Name/IP, Protocol, File Stubs, File System Path, File System Name
VMAX ストレージ グループ	Name, VMAX Serial No, Host

顧客フィードバック

PowerProtect Data Manager UI のカスタマー フィードバック機能を使用して、PowerProtect Data Manager に関する満足度の報告、フィードバックの提供、機能拡張のリクエスト送信が行えます。お客様からのフィードバックは、カスタマー エクスペリエンスの改善に使用されます。

一般フィードバックの提供

次の手順に従って、PowerProtect Data Manager の満足度をレポートし、フィードバックを提供します。

手順

1. PowerProtect Data Manager UI にログ インします。
2. バナーで  をクリックします。

お客様のフィードバックに関するアンケートが新しいウィンドウに表示されます。

メモ: ダーク サイトなどの外部接続が制限されている環境では、Web ブラウザーにエラーが表示され、お客様のフィードバックに関するアンケートは表示されません。

3. （オプション）お客様のフィードバックに関するアンケートを各フィールドに入力したら、［Submit］をクリックします。

   PowerProtect Data Manager に関する満足度の評価と、カスタマー エクスペリエンスの改善方法を提案するオプションが用意されています。また、がフィードバックに関するフォロー アップを行えるように E メール アドレスを入力することもできます。

   メモ: お客様の連絡先情報は、マーケティング目的では使用されません。

セキュリティ構成

別のガイドには、PowerProtect Data Manager ホスト システム管理者とは別の役割を持つ PowerProtect Data Manager セキュリティ管理者専用のサーバー構成タスクについて説明されています。

『*PowerProtect Data Manager* セキュリティ構成ガイド』には、すべてのセキュリティ関連タスクに関する詳細な手順が記載されています。それは次を含みますがこれらに限定されません。

- 次のコンポーネント間のポート要件
  - PowerProtect Data Manager
  - 構成済み DD システム
  - VM Direct アプライアンス（組み込み型および外部）
  - アプリケーションエージェント ホスト
  - Web および REST API クライアント
  - Callhome (SupportAssist)
  - ESXi
  - vCenter
- ID プロバイダーの構成
- ローカルおよび外部ユーザー アカウントの管理
- パスワードの変更とリセット
- ロールおよび関連する権限へのユーザーとグループの割り当て
- ローカル コンポーネントおよびリモート コンポーネントの認証情報の管理
- 権限の範囲を定義するためのリソース グループの作成
- セキュリティ証明書の管理（該当する場合）

ロールベースのセキュリティ

PowerProtect Data Manager では、ユーザー インターフェイスの領域と保護された操作へのアクセスを制御するユーザー ロールがあらかじめ定義されています。PowerProtect Data Manager の機能の一部は特定のロール用に予約されており、どのユーザー アカウントからもアクセスできない場合があります。

事前定義されたロールを使用すると、最小権限の原則が適用され、PowerProtect Data Manager へのアクセスとバックアップ データへのアクセスを制限できます。

関連する権限や各ロールが実行できるタスクなど、ユーザー ロールの詳細については『*PowerProtect Data Manager* セキュリティ構成ガイド』を参照してください。

2

システム メンテナンス

トピック：

PowerProtect Data Manager の導入と正常性の維持

PowerProtect Data Manager を可能な限り効率的に機能させるには、推奨ガイドラインに従って導入および維持する必要があります。

PowerProtect Data Manager の導入とアップデート

PowerProtect Data Manager を導入し、最新バージョンにアップデートし、その他の重要なパッケージ アップデートをインストールすることができます。

更新パス

注意: 推奨されているガイドラインに従っていない場合、PowerProtect Data Manager またはそのいずれかのコンポーネントのアップデートに失敗する可能性があります。

PowerProtect Data Manager の導入またはアップデートを行う際は、『*PowerProtect Data Manager* 導入ガイド』を参照してください。このマニュアルには、特定の環境および構成で従う必要がある詳細な手順とガイドラインが記載されています。

PowerProtect Data Manager バージョン 19.10～19.13 からバージョン 19.14 へのアップデートがサポートされています。

セキュリティ アドバイザリー

注意: 最新の Dell セキュリティ アドバイザリー(DSA)に従っていない場合、PowerProtect Data Manager のセキュリティが脆弱になる可能性があります。

最新の DSA を確認するには、デル・テクノロジーズ, Dell Technologies セキュリティ アドバイザリーと通告の Web サイトで `PowerProtect Data Manager` を検索してください。

PowerProtect Data Manager のライセンス取得

PowerProtect Data Manager のライセンスは、いくつかの異なる方法で使用できます。このセクションでは、使用可能なライセンスのさまざまなタイプと、ライセンスをインストールする方法について説明します。

ライセンスの詳細については、*PowerProtect Data Manager* 導入ガイドを参照してください。

ライセンス タイプ

ライセンスにはさまざまなタイプがあり、さまざまな期間のライセンスを提供できます。

使用可能なライセンス タイプが次の表に示されています。

表 16. ライセンス タイプ

ライセンス タイプ	説明
評価版	PowerProtect Data Manager の導入時に使用するデフォルトのライセンスです。ライセンス キーを追加することなく、最大 90 日間、製品の機能をすべて利用できます。トライアル期間が終了するとき、PowerProtect Data Manager は引き続き全機能で動作するため、恒久ライセンスを追加できます。 **メモ:** 評価版ライセンスでは、SupportAssist を使用できません。
テラバイト（FETB）によるフロントエンド保護容量	ライセンスのプライマリー モデルであり、保護する必要のある実際の容量に基づきます。たとえば、100TB ライセンスを購入すると、最大 100 TB のデータを保護できます。
ソケットベース	バック アップまたはレプリケートされている仮想マシン ホスト上の CPU ソケットごとのライセンスです。

無期限および期限ベース（サブスクリプション）のライセンス

ライセンス供与されたソフトウェアは、無期限または期限ベースのライセンスで提供されます。見積書は、ライセンスの権利が無期限であるか期限ベースであるかを示します。

無期限ライセンスがあると、ライセンス契約の条項に準拠している間はソフトウェアを使用することができます。

期限ベースのライセンスを使用すると、ライセンス契約の条項に準拠している間は、ソフトウェアを指定された期間使用することができます。ライセンス期間が終了したら、ソフトウェアの使用を停止するか、ライセンス期間を延長するか、または新しいライセンスを購入する必要があります。

ライセンスの追加

ライセンス ファイルを PowerProtect Data Manager に追加して、容量の使用状況やソフトウェア ID 番号などのライセンスの詳細を表示することができます。

前提条件

ライセンス管理 Web サイトから XML ライセンス ファイルを取得するには、から E メールで送信されるライセンス認証コード(LAC)が必要です。LAC が届かない場合には、カスタマー サポート担当者にお問い合わせください。

このタスクについて

既存のライセンス情報を確認するには、［Settings］ > ［License］に移動します。

ライセンスを追加するには、次の手順を実行します。

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、［License］を選択します。
2. ［License］ウィンドウで、次のいずれかのアクションを実行します。
   - ライセンス ファイルのテキストをコピーしてテキスト ボックスに貼り付けます。
   - ［Upload File］をクリックしてライセンス ファイルの場所を参照し、ファイルを選択して［Open］をクリックします。

   ライセンス ファイルのコンテンツが［License］ウィンドウに表示されます。
3. ［Apply］をクリックします。

タスクの結果

ライセンスが正常に追加されたことを確認するメッセージが［License］ウィンドウに表示されます。

PowerProtect Data Manager ホストの指定

vCenter Server を PowerProtect Data Manager ホストとして指定すると、vCenter Server は PowerProtect Data Manager に固有の操作を実行できます。

PowerProtect Data Manager ホストは、次を含むいくつかの操作を実行します。

- 仮想マシンの構成およびその他のシステム アクティビティー。
- ソフトウェア アップデート中に、必要な場合は PowerProtect Data Manager スナップショットを作成します。
- ソフトウェア アップデートの実行時に、必要に応じて PowerProtect Data Manager に割り当てられたメモリーを自動的に増加できるようにします。
- 必要な PowerProtect Data Manager CPU とメモリーを増やすためにクラウド ディザスター リカバリー(Cloud DR)を有効にします。PowerProtect Data Manager ユーザー インターフェイスの［Infrastructure］ > ［Asset Sources］ウィンドウの［Cloud Disaster Recovery］タブで指定されているように、vCenter ホストは Cloud DR の動作条件です。

vCenter Server を PowerProtect Data Manager ホストとして指定する

すでに追加または検出されたものから PowerProtect Data Manager ホストとして使用する vCenter Server を選択します。

このタスクについて

次の操作を実行します：

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、［Hosting vCenter］を選択します。
   ［Hosting vCenter］ウィンドウが表示されます。
2. 以下オプションのいずれかを選択してください。
   - ［Enter FQDN/IP］：このオプションでは、vCenter Server の完全修飾ドメイン名または IP、ポート番号を手動で入力し、vCenter［Host Credentials］を選択します。［Host Credentials］リストは、PowerProtect Data Manager で追加および検出済みの vCenter Server に追加されます。ホスト vCenter の認証情報がリストに表示されない場合は、［Add Credentials］を選択してこの情報を入力します。
   - ［ Select FQDN/IP from asset sources］：このオプションでは、PowerProtect Data Manager で追加および検出済みの vCenter 資産ソースからホスト vCenter Server 情報が自動的に取得されます。
3. ［Save］をクリックします。

タスクの結果

ホスト vCenter Server が PowerProtect Data Manager の資産ソースとして追加されている場合、［Infrastructure］ > ［Asset Sources］ウィンドウの、この vCenter Server の横に  が表示されます。

vCenter ServerPowerProtect Data Manager ホストに必要な最小権限

PowerProtect Data Manager ホストとして指定された vCenter サーバーに関連づけられたユーザー アカウントには、次の最小権限が必要です。これらの権限は、ソフトウェアのインストールとアップデート、仮想マシンのスナップショットとロールバック、仮想マシン メモリーの構成に関連する機能に必要です。

設定	vCenter 6.0 以降で必要な権限	PowerCLI に相当する必要な権限
Global	• カスタム属性の管理 • カスタム属性の設定	• Global.ManageCustomFields • Global.SetCustomField
ネットワーク	• ネットワークの割り当て	• Network.AssignNetwork
権限	• 権限の変更	• Authorization.ModifyPermissions
セッション	• Impersonate User • メッセージ • セッションの確認 • セッションの表示と停止	• Sessions.ImpersonateUser • Sessions.Message • Sessions.ValidateSession • Sessions.ViewandStopSessions

設定	vCenter 6.0 以降で必要な権限	PowerCLI に相当する必要な権限
仮想マシン	• 構成の変更>デバイスの追加または削除 • 構成の変更>CPU 数の変更 • 構成の変更>メモリーの変更 • 構成の変更>設定の変更	• VirtualMachine.Config.AddorRemoveDevice • VirtualMachine.Config.CpuCount • VirtualMachine.Config.Memory • VirtualMachine.Config.Settings
仮想マシン	• スナップショットの管理>スナップショットの作成 • スナップショットの管理>スナップショットへの復元 • スナップショットの管理>スナップショットの削除 • スナップショットの管理>スナップショット名の変更	• VirtualMachine.State.CreateSnapshot • VirtualMachine.State.RevertToSnapshot • VirtualMachine.State.RemoveSnapshot • VirtualMachine.State.RenameSnapshot

メモ: 専用の vCenter ユーザー アカウントに必要な権限の全リストは、『*PowerProtect Data Manager* 仮想マシン ユーザー ガイド』に記載されています。

メモリーの最適化

サーバーのパフォーマンスを最適化するために、PowerProtect Data Manager 仮想マシンに割り当てられているメモリーの量を調整できます。

次の表は、標準環境で PowerProtect Data Manager 仮想マシンに割り当てられているデフォルトのメモリー容量を示しています。デフォルト値は、推奨される最小値です。

表 17. PowerProtect Data Manager のメモリー要件

導入タイプ	メモリー	スワップ領域	コア
デフォルト	24 GB	8 GB	10
クラウド ディザスター リカバリー(Cloud DR)アドオンあり	28 GB	8 GB	14

推奨されるコア数は 14 です。また、次の点も考慮してください。

- 環境によっては、メモリー量を増やすとパフォーマンスが向上する可能性があります。
- メモリー不足アラートが表示された場合は、メモリーの量を増やします。
- 32 GB の RAM を超えてメモリー容量を増やさないでください。PowerProtect Data Manager は、32 GB を超える RAM をサポートするようには設計されていません。
- クラウド マーケットプレイス環境の仮想マシンに PowerProtect Data Manager を導入する場合は、32 GB の RAM が自動的に割り当てられます。このメモリーの容量は、導入後に変更しないでください。
- PowerProtect Data Manager のサービスのほとんどは、メモリーを大量に消費します。使用可能な物理メモリーが特定のしきい値まで低下すると、これらのサービスはスワップ メモリーの活用を開始します。スワップ メモリーが低速ディスクに存在する場合、最近使用されていないメモリーを物理メモリーにスワップする必要がある場合に、これらの各サービスからの Java ガベージ コレクション アクティビティーに大きな影響を与える可能性があります。
- ソリッドステート ドライブ(SSD)でスワップ メモリーを構成することを強く推奨します。PowerProtect Data Manager サーバーの導入の際に SSD データ ストアを使用することにより、スワップおよびメタデータ操作時の高レイテンシーによるディスク インパクトを回避します。

メモ: メモリーの最適化については、カスタマー サポート担当者にお問い合わせください。

以前のバージョンの PowerProtect Data Manager のメモリーとアップデート

PowerProtect Data Manager の現在のバージョンの機能では、以前のバージョンよりも多くのメモリーが必要になる場合があります。PowerProtect Data Manager の以前のバージョンからアップデートする場合は、必要に応じて割り当てるメモリーの量を増やしてください。

仮想マシンメモリーの調整

保護環境の変更に対応するために、PowerProtect Data Manager 仮想マシンに割り当てるメモリー量を調整します。

手順

1. [vSphere Web Client] にログインします。
2. アプライアンスを右クリックし、[Edit Settings] を選択します。

［Edit Settings］ウィンドウが表示されます。［Virtual Hardware］ボタンが選択されています。

3. ［Memory］フィールドに、新しいメモリ値を指定します。
   指定した値がメモリーの 32 GB を超えないようにし、4 GB の倍数であることを確認します。
4. ［OK］をクリックします。

制限モード

制限モードを有効にして、ストレージへのスケジュール設定された書き込みを防止できます。制限モードを有効にして、ストレージのアップグレード中にストレージへのアクセスを制限することができます。

ストレージのアップグレード中に制限モードを有効にすると、次のようなメリットがあります。

- ストレージの書き込みを、制御された方法で排除できます。書き込みが停止すると、ストレージをアップグレードできます。
- ストレージの書き込みは、ストレージのアップグレード後にテストできます。テストが完了すると、ストレージを包括的な本番環境に戻すことができます。

制限モードでは、次のスケジュール設定された操作を防止します。

- バックアップとレプリケーション
- バックアップコピーの削除
- サーバー ディザスターリカバリー バックアップ

制限モードでは、次の操作を実行できます。

- 実行中のジョブまたはキューに登録されているジョブの実行
- 手動でのバックアップおよびリストア
- 検出ジョブ

PowerProtect Data Manager ユーザー インターフェイスから制限モードを有効にするには、  をクリックし、［Support］ > ［Restricted Mode］の順に選択してから［Enable Restricted Mode］をクリックします。

システム サポート

PowerProtect Data Manager ユーザー インターフェイスを使用して、通常導入時に構成されるサポート設定を管理し変更することができます。通常、構成されているサポート設定には、メール サーバーのセットアップと Secure Remote Services の登録が含まれます。

［Support］ウィンドウにアクセスするには、  をクリックし、［Support］を選択します。

PowerProtect Data Manager の SupportAssist の設定

SupportAssist は、PowerProtect Data Manager と通信して環境を監視し、現在および潜在的な問題を自動的に検出し、診断データを収集して保存するサポートツールです。SupportAssist は、問題のトラブルシューティングに必要なデータを、診断とお客様サポートのためにカスタマー サポートに安全に送信します。

SupportAssist は、PowerProtect Data Manager とカスタマー サポートの間のユニファイド コミュニケーション ポイントとして、接続プラットフォームの重要な部分を占めています。

SupportAssist には、次の機能とメリットがあります。

- プロアクティブな監視と問題の予防
- アップデート パッケージのダウンロードの簡易化
- ヘルス チェックの自動化
- テレメトリー データの通信
- リアルタイム トラブルシューティング
- カスタマー サポート

PowerProtect Data Manager システムの自動サポート機能を利用するには、SupportAssist を設定します。

PowerProtect Data Manager の評価版ライセンスを使用している場合、SupportAssist を構成することはできません。

SupportAssist のアクセス キーと PIN の生成

アクセス キーと PIN は、PowerProtect Data Manager と SupportAssist との間で安全な接続を設定するために必要です。アクセス キーと PIN を適用する必要があるのは 1 回だけです。

このタスクについて

SupportAssist のアクセス キーと PIN を生成するには、次の手順を実行します。

手順

1. カスタマー サポートの Web サイトにアクセスし、アカウントにログ インします。
2. 検索ボックスに PowerProtect Data Manager と入力し、［Search］をクリックします。
3. ［Quick links］ペインの［Generate Access Key］をクリックします。
4. 検索ボックスに製品 ID（シリアル番号）を入力します。
5. ［Create PIN］フィールドに、4 桁の PIN を入力します。
   後で使用するために、PIN を記録します。
6. ［Generate Access Key］をクリックします。
   アクセス キーは、お使いのアカウントの E メール アドレスに送信されます。
   メモ: アクセス キーが E メールに届くまでに 5 分ほどかかる場合があります。

SupportAssist を使用したサポート サービスへの接続

SupportAssist を介して接続を確立して、カスタマー サポートへのアクセスを確実に行います。SupportAssist を使用すると、PowerProtect Data Manager でサポート サービスに直接接続することも、ゲートウェイ サーバーを通して接続することもできます。

前提条件

- 有効なライセンスを適用 PowerProtect Data Manager します。
- ゲートウェイ サーバーを経由して接続する場合、SCG ゲートウェイ バージョンは 5.10 以降である必要があります。
- 有効なアクセス キーと PIN を適用します。
- *esrs3-core.emc.com* と *esrs3-coredr.emc.com* の HTTPS ポート 443 は、ネットワーク ファイアウォールによってブロックされません。

手順

1. PowerProtect Data Manager UI で  をクリックし、［Support］を選択してから、［SupportAssist］をクリックします。
   ［Support］ウィンドウが開き、［SupportAssist］ページが表示されます。
2. ［Connection］タブで、［Connect Now］をクリックします。
3. 以下のいずれかを選択してください。
   - ［直接接続］

     PowerProtect Data Manager を直接接続するには、このオプションを選択します。
   - ［ゲートウェイ経由で接続］

     PowerProtect Data Manager をゲートウェイ サーバーを介して接続するには、このオプションを選択し、ゲートウェイ サーバーの IP アドレスとポート番号を入力します。
4. SupportAssist アクセス キーと PIN を入力します。
5. ［Enable Connect］をクリックします。

タスクの結果

PowerProtect Data Manager がサポート サービスに接続されます。

連絡先データのアップデートまたは設定

カスタマー サポートが診断レポートに関して連絡する担当者の連絡先情報を入力します。SupportAssist の連絡先データをいつでも追加またはアップデートすることができます。

手順

1. PowerProtect Data Manager UI で  をクリックし、［Support］を選択してから、［SupportAssist］をクリックします。
［Support］ウィンドウが開き、［SupportAssist］ページが表示されます。
2. ［Contacts］タブを選択します。
3. 主要連絡先を追加するには、次のステップを行います。
   a. 次の情報を入力します。
      - ［名］
      - ［姓］
      - ［メール］
      - ［電話］
   b. リストから［Preferred Language］を選択します。
   c. ［保存］をクリックします。
4. 第 2 連絡先を追加するには、［+ Add Secondary Contact］をクリックし、必要な情報を入力します。

SupportAssist 接続の設定の変更

次の手順に従って、SupportAssist 接続の設定を変更します。

手順

1. PowerProtect Data Manager UI で  をクリックし、［Support］を選択してから、［SupportAssist］をクリックします。
［Support］ウィンドウが開き、［SupportAssist］ページが表示されます。
2. 次のいずれかの接続オプションを選択してください。
   - ［直接接続］
   - ［ゲートウェイ経由で接続］

     新しいゲートウェイ接続を追加するには、以下の手順を実行します。

     a. ゲートウェイの IP アドレスとポート番号を入力します。
     b. ［テスト］をクリックします。

        接続テストが完了するまで待ってください。接続に成功すると、ゲートウェイ IP アドレスとポート番号の横に緑色のチェック マークが表示されます。
3. SupportAssist アクセス キーと PIN を入力します。

   メモ: 新しいアクセス キーで接続しない場合は、このステップをスキップします。

4. ［Reconnect］をクリックします。

SupportAssist の有効化または無効化

SupportAssist 機能を有効にして、問題を自動的に検出し、診断データと使用状況データを収集します。また、SupportAssist はいつでも無効にすることができます。

手順

1. PowerProtect Data Manager UI で  をクリックし、［Support］を選択してから、［SupportAssist］をクリックします。
［Support］ウィンドウが開き、［SupportAssist］ページが表示されます。
2. SupportAssist を有効にするには、［Connect to SupportAssist］スライダーを右に動かします。SupportAssist を無効にするには、［Connect to SupportAssist］スライダーを左に動かします。

   この動作は完了までに最長 5 分かかることがあります。

SupportAssist のトラブルシューティング

SupportAssist 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ます。

SupportAssist の接続の確立に失敗

すでに使用されているアクセス キーと PIN を使用して SupportAssist に接続している場合、接続は次のエラーにより失敗します。

```
Connection is failed: Get universalkey error: Access Key and Pin used
```

この問題が発生した場合は、カスタマー サポートから新しいアクセス キーと PIN を入手してください。 SupportAssist のアクセス キーと PIN の生成 で手順を参照してください。

SWID が PowerProtect Data Manager バックエンドに追加されていない場合、次のエラーが表示されることがあります。 `Connection is failed: Get universalkey error: Invalid Access Key and Pin`

この問題が発生した場合は、カスタマー サポートに連絡して、SWID が PowerProtect Data Manager バックエンドに追加されているかどうかを確認してください。

接続状態が「未接続」に変わります

接続のステータスが「未接続」に変わった場合：

1. SupportAssist を使用したサポート サービスへの接続において、すべての必要要件が満たされていることを確認します。
2. 問題が解決しない場合は、カスタマー サポートにお問い合わせください。

Telemetry Collector

Telemetry Collector は、構成、使用特性、パフォーマンス、導入場所など、このシステムに関連する情報を収集します。Telemetry Collector は、Dell Inc.またはその関連会社を使用して、リモート アクセスとシステム データの交換を管理します。Telemetry Collector によって収集された情報は機密情報であり、このデータを共有することはできません。

SupportAssist を有効にすると、Telemetry Collector も有効になり、カスタマー サポートエンジニア型社員は、デバイスのトラブルシューティングや PowerProtect Data Manager ソフトウェアの問題に関連するデータを収集できます。Telemetry Collector は個人情報を収集しません。

Telemetry Collector は 3 個のレポートを収集します。これには、テレメトリー レポート、アラート サマリー レポート、および CloudIQ レポートがあります。Telemetry Collector は、次のオブジェクトの詳細を収集します。

- アラート
- 資産
- 資産ソース
- 監査ログ
- クラウド データ リカバリー
- [Cloud Disaster Recovery] メトリックス
- コンプライアンスの詳細
- 過去 24 時間のコンプライアンス
- データ ターゲット
- DD インベントリー
- ホストの情報
- 統合型ストレージ
- ライセンス
- PowerProtect Data Manager の運用インベントリ
- 保護の詳細
- 保護ポリシー
- クイック リカバリー同期情報
- サービスレベル アグリーメント
- ストレージ システム
- レポートの生成に費やされる時間
- トラフィック メトリック
- サマリーのアップデート

- 使用方法

CloudIQ レポート作成

AutoSupport を有効にして SupportAssist を選択すると、レポート作成も有効になります。CloudIQ は、インテリジェントで包括的な予測分析によって、システム全体の稼働状態をプロアクティブに監視して測定する、無償の SaaS/クラウドベース管理アプリケーションです。CloudIQ に報告されるデータには、構成データ、履歴メトリクス、正常性スコア データが含まれます。

以下の必要条件を満たしていることを確認します。

- ［System Settings］ > ［License］に有効なライセンスを追加します。
- ［System Settings］ > ［Support］ > ［SupportAssist］で SupportAssist をセットアップします。
- AutoSupport を有効にし、［SupportAssist］を選択します。

AutoSupport が有効になっている場合、 CloudIQ レポートは自動的に送信されます。CloudIQ にログ インするには、  をクリックし、CloudIQ をクリックします。https://cloudiq.dell.com に移動することもできます。CloudIQ の詳細については、CloudIQ オンライン サポート サイトを参照してください。

E メール サーバーの設定

PowerProtect Data Manager の［Support］ウィンドウの［Email Setup］ページでは、ローカル ユーザー パスワードのリセットとアラート通知のカスタマイズに関連する E メールの送受信を制御する SMTP E メール サーバー設定を構成できます。

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、［Support］を選択してから、［Email Setup］をクリックします。
2. 次のフィールドにデータを入力します。
   a. ［Mail Server］
      SMTP E メール サーバー。
   b. ［Email from］:
      PowerProtect Data Manager の AutoSupport E メールを受信する E メール アドレス。
   c. （オプション）［Recipient for Test Email］:
      PowerProtect Data Manager のテスト E メールの送信先となる E メール アドレス。
   d. （オプション）［Port］:
      デフォルト ポートは 25 です。PowerProtect Data Manager は、デフォルト以外のポートの使用もサポートしています。
      E メール設定が削除された場合、他の場所で使用されていないデフォルト以外のポートを手動で選択する必要があります。
   e. ［User Name］:
      PowerProtect Data Manager SMTP E メール サーバーに関連付けられたユーザー名。このフィールドはオプションです。
   f. ［ Password］:
      PowerProtect Data Manager SMTP E メール サーバーに関連付けられているパスワード。このフィールドはオプションです。
3. ［Send Test Email］をクリックします。
   PowerProtect Data Manager から、テスト E メールが送信されます。
4. ［Save］をクリックします。

AutoSupport の追加

AutoSupport が有効になっている場合、自動サポート情報、テレメトリー レポート、アラート サマリー、および CloudIQ レポートが送信されます。

このタスクについて

SupportAssist Enterprise と SMTP の両方が構成されている場合、この情報は、［System Settings］ > ［Support］ > ［AutoSupport］ウィンドウで選択したオプションを使用して送信されます。

手順

1. PowerProtect Data Manager UI で  をクリックし、［Support］を選択してから［AutoSupport］をクリックします。

［AutoSupport］ウィンドウが表示されます。

2. `Enable AutoSupport` オプションを［Disabled］または［Enabled］に変更し、［Save］をクリックします。

   AutoSupport を有効にする場合、SupportAssist または E メール サーバーを介して AutoSupport 通信を受信するかどうかを選択します。

   AutoSupport を有効にすると、［Telemetry Software Terms］ページが表示されます。ページの一番下までスクロールしてレビューし、条件に同意したら、［Save］をクリックして変更を保存します。

   AutoSupport を無効にすると、PowerProtect Data Manager は SupportAssist または SMTP サーバーへのエラーおよびテレメトリー データの送信を停止します。PowerProtect Data Manager は、アップデートおよびその他の情報の送信を続行します。

   メモ: SupportAssist を無効にするには、AutoSupport ウィンドウで SupportAssist オプションをオフにします。

自動アップデート パッケージのチェックとダウンロードの有効化

SupportAssist が有効になっている場合は、PowerProtect Data Manager でアップデート パッケージを自動的にチェックし、アラートを送信するか自動的にダウンロードするように構成できます。

これらのオプションの詳細については、*PowerProtect Data Manager* 導入ガイドを参照してください

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。

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。

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. ［Administration］ > ［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、［Alerts］を選択します。

   上部バナーの  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字は、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、  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ーすると、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、カテゴリー、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. 過去 24 時間、過去 3 日間、過去 7 日間、過去 30 日間から期間を選択するか、アラートを表示する特定の日を選択するか、カスタム時間範囲を指定します。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 タグもクリアーされます。
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、［Add/Edit Note］をクリックし、終了したら［Save］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

1. ［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

2. 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。
3. 監査ログにメモを追加するには、［>］をクリックして［Notes］フィールドにメモを入力し、［Save］をクリックします。
4. ［Export All］をクリックします。

システム サービスとシステムの稼働状態の監視

システム サービスのステータスは［System Services Status］ペインから監視でき、システムの稼働状態に関する情報は［Health］ペインから監視できます。

システム サービスのモニタリング

［System Services Status］ペインから、各システム サービスのステータスを監視できます。

システム サービスのステータスを表示するには、  をクリックし、［Support］を選択して［System Services Status］をクリックします。

次の表には、各システム サービスとシステム コンポーネントのステータスの概要が示されています。

表 18. システム サービスとコンポーネントのステータス

ステータス	説明
実行中	この状態は関連するサービスまたはコンポーネントがフル機能で実行されている場合に表示されます。すべてのサービスが実行状態にある場合、アプライアンスの状態は操作可能です。
［Initializing］	この状態は、サービスの開始時に表示されます。サービスが正常に起動すると、状態は実行中に変わります。
メンテナンス	この状態は、関連するサービスのメンテナンス中に表示されます。メンテナンス状態では、コンポーネントの機能が制限されます。インフラストラクチャ サービスは、メンテナンス状態になりません。他のサービスまたはコンポーネントがメンテナンス中の場合、アプライアンスの状態もメンテナンス中です。
［Quiesce］	この状態は、サービスまたはコンポーネントに関連するサービスが停止中の場合に表示されます。
Shut down	この状態は、サービスが停止した場合に表示されます。
［No response］	この状態は、コンポーネントに関連づけられたサービスが実行されている一方で、このサービスが応答しない場合に表示されます。

システムの稼働状態の監視

PowerProtect Data Manager UI の［Health］ペインからシステムの稼働状態に関する情報をモニターできます。

PowerProtect Data Manager の稼働状態に影響する問題のサマリーを表示するには、ナビゲーション ペインで［Health］を選択するか、ダッシュボードの［health］ウィジェットで［View All］を選択します。

PowerProtect Data Manager により、2 分ごとにヘルス チェックが自動的に実行されます。問題が検出された場合は、重大度に基づいてカテゴリーと控除値が割り当てられます。すべての問題が［Health］ウィンドウに表示されます。解決済みの問題は、次回のヘルス チェック実行時に自動的に削除されます。

正常性の詳細とステータスは、次のカテゴリーで提供されます。

- ［Components］は、ハードウェアおよびソフトウェア サービスの状態（例：実行中または失敗）を識別します。
- ［Configuration］は、システム サポートの構成など、PowerProtect Data Manager 構成に不完全な要素があるかどうかを示します。
- ［Capacity］は、関連したストレージ システムのプロビジョニング済みおよび現在割り当て済みのサイズを識別します。

- ［Performance］は、主要なパフォーマンス インジケーター（例：メモリー使用）を識別します。
- ［Data Protection］は、主要な保護インジケーター（例：サービスレベル アグリーメントが満たされていない、ディザスターリカバリーのバックアップ コピーが存在しない）を識別します。

各カテゴリーのスコアの初期値は 100 です。これらのカテゴリーのいずれかに未解決のヘルス チェックの問題がある場合、問題に割り当てられた減点値の分だけスコアが減点されます。カテゴリーに複数の未解決の問題がある場合、最も重大な問題の減点値の分だけスコアが減点されます。

エントリーの横にあるをクリックして、問題の詳細を表示します。

［Health］ウィンドウでは、［Export All］機能を使用して稼働状態に関するデータをエクスポートできます。

システム全体の稼働状態スコアは、最も重大な問題と最も低いスコアのカテゴリーによって表されます。

表 19. 全体的な稼働状態スコア

稼働状態スコア	意味
95～100	システムの稼働状態は良好です。
71～94	システムの稼働状態は適性です。
0～70	システムの稼働状態は不良です。

表 20. ヘルス チェックの説明

Category	ヘルス チェック	最大減点	説明
構成	資産ソース構成	-30	PowerProtect Data Manager で資産ソースが追加および有効化されていない場合に減点が発生します。少なくとも 1 つの資産ソースが追加されると、稼働状態スコアは正常に戻ります。
	ストレージ構成	-30	システムにストレージ ターゲットが構成されていない場合に減点が発生します。少なくとも 1 つのストレージ ターゲットが設定されると、稼働状態スコアは正常に戻ります。 **メモ:** PowerProtect Data Manager アプライアンスは対象外です。
	サポート構成	-10	システムにサポート オプションが構成されていない場合に減点が発生します。次のようなサポート オプションがあります。 • E メールのセットアップ • サポートアシスト • 自動サポート サポート オプションが構成されると、稼働状態スコアは正常に戻ります。サポート オプションが構成されていても、初期化がまだ進行中の場合、初期化が完了するまで、稼働状態スコアの減点は-5 に設定されます。
	すべての資産の定義済みポリシー	-2	PowerProtect Data Manager で有効になっている資産ソースの資産のいずれかが保護されていない場合に（Protected/Exclude など）減点が発生します。保護されていない資産の合計が 0 より大きくなると、減点は-2 になります。 すべての資産が保護された状態に移行すると、稼働状態スコアは正常に戻ります。
	システム ディザスター リカバリー(DR)バックアップ スケジュール	-10	スケジュール設定されたシステム DR バックアップがない場合に減点が発生します。 システム DR スケジュールが設定されると、稼働状態スコアは正常に戻ります。

表 20. ヘルス チェックの説明 （続き）

Category	ヘルス チェック	最大減点	説明
	License	-30	ライセンス ステータスが有効でない場合、または有効期限が近づいている場合に減点が発生します。 • ライセンスが無効または有効期限が切れている場合：-30 • ライセンスの有効期限まで 7 日未満の場合：-20 有効な PowerProtect Data Manager ライセンスが適用されると、稼働状態スコアは正常に戻ります。
	オペレーティング システム アカウントのヘルス チェック	-60	オペレーティング システム アカウントのパスワードのいずれかの有効期限が近づいているか、すでに期限が切れている場合に減点が発生します。 • オペレーティング システム アカウントのパスワードが期限切れの前：-15 • パスワードが期限切れ：-60 オペレーティング システム アカウントの期限エラーが修正されると、稼働状態スコアは正常に戻ります。
	検索クラスターの構成	検索クラスターが無効：-5 検索ノードの親 vCenter Server が削除されている：-5	検索クラスターが無効になっている場合、または親 vCenter Server が削除されている場合に減点が発生します。 **メモ:** PowerProtect Data Manager アプライアンスは対象外です。 検索クラスターが適切に構成されると、稼働状態スコアは正常に戻ります。
	レポート クラスターの構成	レポート ノードの親 vCenter Server が削除されている：-5	レポート ノードの親 vCenter Server が削除されている場合に減点が発生します。 **メモ:** PowerProtect Data Manager アプライアンスは対象外です。 レポート クラスターのエラーが修正されると、稼働状態スコアは正常に戻ります。
	ES の構成	-5	未定義の ES 設定が追加されたときに減点が発生します。 エラーが ES 側で修正されると、稼働状態スコアは正常に戻ります。
コンポーネント	PowerProtect Data Manager コア インフラストラクチャ サービス ステータス	ビジネス サービス：30 コア サービス：30 インフラストラクチャ サービス：60 管理サービス：40 保護サービス：20	1 つ以上の PowerProtect Data Manager サービスが実行されていない場合、または無効になっている場合に減点が発生します。 すべてのサービスが稼働するようになると、稼働状態スコアは正常に戻ります。
	保護エンジン ステータス	-10	保護エンジンに注意が必要な場合に減点が発生します。 保護エンジン ステータスが動作状態になると、稼働状態スコア/ステータスは正常に戻ります。
	レポート作成	-10	1 つ以上のレポート ノードが検出できなくなると減点が発生します。

表 20. ヘルス チェックの説明 （続き）

Category	ヘルス チェック	最大減点	説明
			ヘルス チェック エラーが修正されると、稼働状態スコアは正常に戻ります。
	検索クラスター	-25	1 つ以上の検索クラスターまたはノードが無効になるか、検出できない場合に減点が発生します。 すべての検索クラスターの問題が解決されると、稼働状態スコア/ステータスは正常に戻ります。
	Cloud Disaster Recovery	-25	PowerProtect Data Manager 内の Cloud DR Server を検出できないか、パスワードが無効な場合に減点が発生します。 DD Cloud Disaster Recovery サーバーの問題が解決されると、正常性ステータス/スコアは正常に戻ります。
	ヒープ ダンプ	-2	java サービス ログ フォルダーで java ヒープ ダンプ ファイルが検出された場合に減点が発生します。 検出された java ヒープ ダンプ ファイルがなくなると、稼働状態スコアは正常に戻ります。
	DNS	-60	すべての DNS サーバーに到達できない場合に減点が発生します。 少なくとも 1 台の DNS サーバーに到達できる場合、稼働状態スコアは正常に戻ります。
	NTP	-10	すべての NTP サーバーが利用できない場合に減点が発生します。 少なくとも 1 台の構成済み NTP サーバーに到達できる場合、稼働状態スコアは正常に戻ります。
	ES シャード ヘルス チェック	-50（レプリカ シャード未割り当て） -70（プライマリー シャード未割り当て）	レプリカまたはプライマリー シャードが割り当てられていない場合に減点が発生します。 ES シャード エラーが修正されると、稼働状態スコアは正常に戻ります。
Data Protection	サービス レベル アグリーメント(SLA)コンプライアンス	-50	SLA コンプライアンスが定義されているが満たされていない場合に減点が発生します。たとえば、資産コンプライアンス率は次のように定義されます。コンプライアンス違反資産数/コンプライアンス遵守資産数+コンプライアンス違反資産数 ● 低比率：コンプライアンス率<= 1/3 ● 高比率：1/3 <コンプライアンス率<= 2/3 ● 臨界比率：コンプライアンス率> 2/3 定義された SLA のコンプライアンスに違反している保護ポリシーが 2/3 を超えている場合、スコアの減点は-50 になります。 SLA コンプライアンスが満たされると、稼働状態スコアは通常に戻ります（例：`complianceRatio=0`）。
	システム DR バックアップ コピーの存在	-40	システム DR バックアップ コピーが存在しない場合に、減点が発生します。DR バックアップ コピーが存在する場合、稼働状態スコアは正常に戻ります。
	検出ステータス	-20（PowerProtect Data Manager の場合）	PowerProtect Data Manager または Cloud Snapshot Manager (CSM)の検出ジョブがエラーを

表 20. ヘルス チェックの説明 （続き）

Category	ヘルス チェック	最大減点	説明
		-5（Cloud Snapshot Manager の場合）	表示して完了した場合に減点が発生します。検出ジョブのエラーが修正されると、稼働状態スコアは正常に戻ります。
容量	PowerProtect Data Manager のディスク領域	-60	ディスク パーティション領域の空きが少なくなってくると減点が発生します。ディスク領域の使用率が 75～90%の場合、スコアの減点は-15 です。ディスク領域の使用率が 90%を超えると、スコアの減点は-60 になります。 ディスク領域の使用率が 75%のしきい値を下回ると、稼働状態スコアは正常に戻ります。
パフォーマンス	メモリ使用量	-40	オペレーティング システムのメモリー使用率が高い場合に減点が発生します。メモリー使用率が 80~95%の場合、スコアの減点は-15 です。メモリー使用率が 95%を超えた場合、スコアの減点は-40 になります。 ディスク領域の使用率が 80%のしきい値を下回ると、稼働状態スコアは正常に戻ります。

次のヘルス チェックは猶予期間を与え、導入後の一定期間、全体的な稼働状態スコアを大幅に低下させずにシステムを構成することができます。スコアの減点が発生する 24 時間前までに、情報アラート通知が表示されます。

表 21. 猶予期間のある減点

ヘルス チェック コンポーネント	猶予期間による減点
資産ソース構成	• 最大 48 時間構成されていない：-5 • 48 時間を超えて 1 週間未満構成されていない：-20 • 1 週間後以降も構成されていない：-30
ストレージ構成	• 最大 24 時間構成されていない：-5 • 24 時間後以降も構成されていない：-30
システム サポートの構成	• 最大 1 週間構成されていない：-5 • 1 週間後以降も構成されていない：-10
システム ディザスター リカバリー(DR)バックアップ スケジュール	• 最大 48 時間構成されていない：-5 • 48 時間を超えて構成されていない：-10

オープン ソース ソフトウェア パッケージ情報へのアクセス

PowerProtect Data Manager で使用されるオープン ソース ソフトウェア（OSS）パッケージ情報は、すべて共通のディレクトリーに格納されます。

この情報にアクセスをするには、PowerProtect Data Manager に SSH でログインし、 `/usr/local/brs/puppet/licenses` ディレクトリーから OSS レポートを取得してください。

セキュリティ証明書

PowerProtect Data Manager のデフォルトの導入では、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 は各コンポーネントの追加の証明書を格納します。

管理者ロールとセキュリティ管理者ロールでは、UI の［Administration］ > ［Certificates］ページが表示されます。このページには、インストールされているセキュリティ証明書を一覧表示する 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。

［Internal］タブの証明書は、UI や REST API など、PowerProtect Data Manager サーバーの一部であるコンポーネントへのアクセスを保護します。［Application Agents］タブの証明書は、PowerProtect Data Manager の制御下では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を保護します。［External Servers］タブの証明書は、サーバーの制御下ではないものの通信を承認したコンポーネントまたはシステムへのアクセスを保護します。

暗号形式とセキュリティ証明書の詳細については、*PowerProtect Data Manager* セキュリティ構成ガイドを参照してください。このガイドでは、インストールされている証明書の管理方法について説明しています。重要な前提条件、運用上の考慮事項、関連タスク、トラブルシューティングが含まれます。例えば、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置き換えることができます。また、外部コンポーネントおよびシステムとの証明書ベースの信頼を確立する手順についても記載されています。

PowerProtect Data Manager の再起動

PowerProtect Data Manager の再起動が必要な場合は、必要な場合を除き、仮想マシンの電源を直接オフにしないことをお勧めします。

PowerProtect Data Manager を正常に再起動するには、`reboot` または `shutdown` コマンドを使用します。例えば、Linux では、`shutdown -r` または `shutdown -h now` コマンドを実行します。

システム メンテナンスのトラブルシューティング

PowerProtect Data Manager の再起動後にサービスが開始されない

オペレーティング システムの root パスワードの有効期限が切れ、PowerProtect Data Manager を再起動する前にパスワードを変更しない場合、一部のスクリプトは root 権限の取得に失敗します。この状況では、PowerProtect Data Manager サービスを開始できません。

オペレーティング システムの有効期限が切れたパスワードの動作については、*PowerProtect Data Manager* セキュリティ構成ガイドのガイダンスに従って root パスワードを変更します。次に、PowerProtect Data Manager をもう一度再起動します。

メッセージ カタログ

PowerProtect Data Manager UI のメッセージ カタログには、PowerProtect Data Manager が生成するすべての情報メッセージ、警告メッセージ、重要なメッセージのリストが表示されます。メッセージの詳細と推奨アクションは、問題のトラブルシューティングに使用できます。メッセージ ID は、Dell カスタマー サポートへのお問い合わせの際に参照目的で使用するために提供されています。

PowerProtect Data Manager UI で、  をクリックし、［Messages Catalog］を選択してカタログ全体を表示します。各列を基準に情報をソートしたり、リストにフィルターを適用して、特定の条件に一致するメッセージを表示したりすることができます。

- ［Message ID］、［Message］、［Details］、［Recommended Action］列では、テキストを検索して、検索テキストに一致する結果のみを表示することができます。
- ［Category］列と［Severity］列では、使用可能なオプションから 1 つまたは複数を選択して、選択内容に一致するメッセージのみを表示することができます。

すべてのメッセージまたはフィルターが適用されたメッセージのリストを `.csv` ファイルとしてエクスポートするには、［Export］をクリックします。

3

ストレージの管理

トピック：

保護ストレージ

保護ストレージは、PowerProtect Data Manager がバックアップ コピー、レプリケートされたコピー、その他の重要な情報を格納する構成済みストレージ システムのセットです。保護ストレージには、次の内容を含めることができます。

- 高可用性 PowerProtect DD モードを含む DD システム
- 複数の DD システムを管理する PowerProtect DD Management Center (DDMC)のインスタンス
- DDMC Smart Scale システム プール

メモ: 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。

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。

保護ストレージを構成する前に、次の内容を順守してください。

- 保護ストレージの追加と構成には、管理者ロールが必要です。
- DDOS の互換性のないバージョンを実行する保護ストレージを追加することはできません。
- ホスト名、FQDN、IP アドレスのどれを指定しても、同じ保護ストレージ システムを追加できるのは 1 回だけです。
- 管理対象 DD のシステムがない PowerProtect DD Management Center インスタンスを追加することはできません。
- 保護ストレージを初めて追加すると、PowerProtect Data Manager によりサーバー DR が自動的に構成され、有効化されます。最初の保護ストレージ システムはデフォルトのターゲットです。 サーバー DR のシステム リカバリー で詳細を参照してください。
- ホスト名または FQDN を使用して保護ストレージを追加すると、将来、IP アドレスを非常に柔軟に変更できます。管理ネットワーク インターフェイスに対してこれらのエントリーを選択すると、PowerProtect Data Manager は DNS を使用してホスト名と FQDN を解決します。後で DNS マッピングを変更する場合、PowerProtect Data Manager は新しいアドレスを解決し、そこに管理通信を転送します。データネットワークとの通信は IP アドレスで行われます。

保護ストレージは、関連データを保持し、より詳細な構成オプションを適用するストレージ ユニットと呼ばれる論理グループにさらに分割されます。

をクリックして［Details］ペインを開き、既存の保護ストレージ システムに関する詳細情報を表示します。

メモ: Storage Direct エージェントに、PowerProtect DD Management Center インスタンスを追加する必要はありません。

PowerProtect DD Management Center の自動検出

PowerProtect DD Management Center のインスタンスを追加すると、PowerProtect Data Manager は、PowerProtect DD Management Center インスタンスが管理する、サポート対象のすべての DD システムを自動的に検出します。

検出の完了後、PowerProtect Data Manager は、［Infrastructure］ > ［Storage］ウィンドウの［Protection Storage］タブに検出された DD システムを表示します。検出されたシステムが表示されるまで数分かかる場合があります。

各 DD システムの場合、表の［Managed By］列には DD システムを管理する PowerProtect DD Management Center インスタンスが表示されます。

PowerProtect Data Manager に DD システムを直接追加する場合、［Managed By］列に、DD システムに指定した名前が表示されます。

高可用性 PowerProtect DD サポート

PowerProtect Data Manager は、高可用性（HA）が有効になっている DD システムをサポートします。アクティブ-スタンバイ構成では、システム障害が発生した場合に冗長性を提供します。HA では、アクティブ システムとスタンバイ システムの同期を保つため、アクティブ ノードに障害が発生しても、スタンバイ ノードがサービスを引き継いで、障害が発生したノードが中断したところから続行することができます。

アクティブな高可用性 PowerProtect DD システムがスタンバイ高可用性 PowerProtect DD システムにフェール オーバーした場合、バックアップ、リストア、レプリケーション、クラウド階層を含む進行中のすべての PowerProtect Data Manager 操作は、影響を受けることなく継続します。

高可用性 PowerProtect DD 構成をストレージ ターゲットとして PowerProtect Data Manager で追加するには、PowerProtect Data Manager UI で［Infrastucture］ > ［Storage］の順に選択します。 保護ストレージの追加 で詳細を参照してください。

仮想マシンのアプリケーションアウェア保護は、HA の DDOS バージョン 7.0 以降でのみサポートされます。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。

HA が有効になっている DD システムの詳細については、*DDOS* 管理ガイドを参照してください。

Smart Scale システム プール

システム プールは、柔軟なストレージ オプションへの 1 個のインターフェイスを持つ DD システムの論理グループです。PowerProtect Data Manager は、保護ストレージとしてシステム プールを使用できます。

Smart Scale、システム プールに関する詳細情報と使用可能な機能については、*DDOS* 管理ガイドおよび *PowerProtect DD Management Center* インストールおよび管理ガイドを参照してください。システム プールを使用するには、DDMC インスタンスが Smart Scale 対応である必要があります。

DDMC インスタンスを追加すると、PowerProtect Data Manager によって使用可能なすべてのシステム プールが自動的に検出されます。［Protection Storage］タブの［Model］列は、保護ストレージ システムがシステム プールであることを示します。

保護ポリシーを使用する場合は、保護ストレージ選択肢リスト内の、別の見出しの下にある PowerProtect Data Manager グループ システム プールを選択します。

メモ:

システム プールとともに DDMC インスタンスを追加すると、システム プール内の個々のシステムも検出されます。PowerProtect Data Manager は、保護ポリシーの作成時などに、これらのシステムを利用可能なストレージ ターゲットのリストに含めます。非 Smart Scale DDMC インスタンスの場合と同様に、［Infrastructure］ > ［Storage］ページは、保護ストレージ システムのリストの［Managed By］列を使用してこれらのシステムをグループ化し、識別します。

一部のロールでは、システムとシステム プールの間の関係を識別するために［Infrastructure］ > ［Storage］ページを表示することはできません。ロールが理由でこの情報を表示できない場合は、システム管理者にストレージ ターゲットの割り当てを調整してもらいます。

システム プールをターゲットとする保護ポリシーは、別のシステム プールまたはスタンドアロンの保護ストレージ システムに複製できます。反対に、スタンドアロンの保護ストレージ システムをターゲットとするポリシーは、別の保護ストレージ システムまたはシステム プールに複製できます。

システム プールレポート作成

保護ストレージレポート作成は、個々の保護ストレージ システムとシステム プール間で若干異なります。これらの違いは、［Storage］ページと保護ストレージ詳細ペインに表示されます。

次の表に、システム プールを対象とした保護ストレージ システムのリスト内にある特定の列の反応を示します。

表 22. システム プールレポート作成

列	説明
［合計］	システム プールの合計容量。
［可］	システム プールの単一システムにストレージ ユニットを配置するための最大の空き容量。
［空き］	プール内の残りの未使用領域。
［暗号化］	On システム プールの DD システムで暗号化が有効になっている場合。

［Available］と［Free］の値を追加すると、システム プール内の未使用領域の合計容量が得られます。

モバイル DD Boost ユーザー

Smart Scale モバイル DD Boost ユーザーは、システム プールにモバイル ストレージ ユニットを所有しています。この概念は、DD Boost ユーザーと通常のストレージ ユニット間の関連付けをシステム プール範囲に拡張します。

モバイル DD Boost ユーザーは、DDMC データ センター内で一意のユーザー ID を提供し、関連するモバイル ストレージ ユニットへのアクセスを制御します。これらのユーザーは、データ センター全体で一元管理され、一意です。

モバイル DD Boost ユーザーは、システム プール全体を管理する DDMC インスタンスにリクエストを送信します。DDMC では次に、リクエストをシステム プール内の正しいシステムに転送します。

他のストレージ ユニットと同様に、PowerProtect Data Manager は、PowerProtect Data Manager の制御下でモバイル DD Boost ユーザーを各モバイル ストレージ ユニットに関連付けます。

ストレージ ユニット にはモバイル ストレージ ユニットの詳細が記載されています。

システム プールの制限事項

システム プールを使用する前に、次の情報を確認してください。

- Storage Direct ポリシーは、システム プールをサポートしていません。ストレージ ターゲット リストには、メンバーシップに関係なく、すべての保護ストレージ システムが表示されますが、システム プールは表示されません。
- Storage Direct ポリシーは、システム プールをサポートしていません。
- クラウド階層化は、システム プールをサポートしていません。プライマリー バックアップまたは保存でシステム プールがターゲットとされている場合、保護ポリシーにクラウド階層化目的を追加できません。レプリケーション目的でシステム プールがターゲットとされている場合、レプリケーション目的にクラウド階層化目的を追加できません。
- サーバー ディザスター リカバリー(DR)は、保護ポリシーのシステム プールをサポートしていません。システム プールをターゲットとする保護ポリシーはリモート サーバーと同期しません。
- サーバー DR は、システム プールをリカバリー ターゲットとしてサポートしていません。ターゲット保護ストレージ システムのリストには、システム プールは含まれません。
- 保護ポリシーのシステム プールにモバイル ストレージ ユニットを自動的に作成する場合は、次の手順を実行します。
    - ポリシー暗号化設定が有効になっている場合、PowerProtect Data Manager は、DD Boost ファイル レプリケーションの暗号化が有効になっているプール メンバー, pool member への配置を要求します。
    - ポリシー暗号化設定が無効になっている場合、PowerProtect Data Manager は特定の配置要求を行いません。モバイル ストレージ ユニットは、DD Boost ファイル レプリケーションの暗号化を有効または無効にできるプール メンバー, pool member に存在する場合があります。
    - システム プールおよびプール メンバー, pool members の保存ロック設定は、保護ポリシーの保存ロック設定と一致する必要があります。システム プールまたはプール メンバー, pool members に対して保存ロックが無効になっているものの、保護ポリシーに対して有効になっている場合、またはその逆の場合、モバイル ストレージ ユニットの作成は失敗します。

システム プール内のモバイル ストレージ ユニットの移行

DDMC を使用してシステム プール内のモバイル ストレージ ユニットを移行する前に、次に示す PowerProtect Data Manager の前提条件と移行後の条件を確認してください。

移行中、選択したストレージ ユニットは保護ワークフローで使用できません。ただし、バックアップと移行のスケジュールを調整して、影響を受けたワークフローのダウンタイムを短縮できます。

ユニットを移行できるのは、モバイル ストレージ ユニットの要件に一致するデスティネーションのみです。これらの要件の詳細については、PowerProtect DD のドキュメントを参照してください。

サポートされている資産タイプ

- VMware 仮想マシン
- Oracle Database
- Microsoft SQL Server データベース
- Microsoft Exchange Server データベース
- ファイル システム
- ネットワーク接続型ストレージ(NAS)共有
- SAP HANA データベース
- Kubernetes クラスター

移行

次の手順を実行します：

1. 移行手順については、PowerProtect DD のドキュメントを確認してください。
2. 移行を開始し、実行段階に至るまでのすべてのステップを実行します。
3. 移行を行う前に、選択したストレージ ユニットに関連する PowerProtect Data Manager 操作を停止します。 モバイル ストレージ ユニット移行前の PowerProtect Data Manager 操作の停止 で手順を参照してください。
4. 移行を行い、移行が完了するまで待機します。
5. すべての PowerProtect Data Manager 操作のリストアを実行します。 モバイル ストレージ ユニット移行後の PowerProtect Data Manager 操作のリストア で詳細を参照してください。
6. 必要に応じて、操作を確認します。 モバイル ストレージ ユニット移行後の動作確認 で詳細を参照してください。

モバイル ストレージ ユニット移行前の PowerProtect Data Manager 操作の停止

移行を行う前に PowerProtect Data Manager を停止するには、次のアクションを実行します。

手順

1. 選択したストレージ ユニットが使用されているすべての保護ポリシーを無効にします。 保護ポリシーの無効化 で手順を参照してください。
2. 影響を受けた保護ポリシーにレプリケーション目的がある場合は、手動レプリケーションを実行して、レプリケーションのバックログをすべて排除します。 保護された資産の手動レプリケーション で手順を参照してください。

   保護ポリシーを無効にした後も、スケジュール設定されたレプリケーション アクティビティーは続行されます。
3. 影響を受けた保護ポリシーで実行中の保護アクティビティーとリストア アクティビティーをすべて完了させます。
4. サーバーのディザスター リカバリー(DR)を無効にします。 サーバー DR バックアップの無効化 で手順を参照してください。
5. 選択したストレージ ユニットで開始されたインスタント アクセス セッションをすべて削除します。*PowerProtect Data Manager* 仮想マシン ユーザー ガイドに、手順が記載されています。
6. コンプライアンスの検証を無効にします。*PowerProtect Data Manager* セキュリティ構成ガイドに、手順が記載されています。

次の手順

移行が完了し、通常のオペレーションが再開されるまで、次のアクティビティーを控えてください。

- 影響を受けた保護ポリシーの資産手動バックアップ。
- 影響を受けた保護ポリシーの保存期間変更。

モバイル ストレージ ユニット移行後の PowerProtect Data Manager 操作のリストア

移行後に、PowerProtect Data Manager の停止を解除するには、次のアクションを実行します。

手順

1. コンプライアンスの検証を有効にします。*PowerProtect Data Manager* セキュリティ構成ガイドに、手順が記載されています。
2. サーバー DR を有効にします。 サーバー DR バックアップの手動構成 で手順を参照してください。
3. 選択したストレージ ユニットが使用されているすべての保護ポリシーを有効にします。 無効化された保護ポリシーの有効化 で手順を参照してください。

モバイル ストレージ ユニット移行後の動作確認

移行後に PowerProtect Data Manager の停止を解除した後、必要な場合には選択したモバイル ストレージ ユニットが使用されている保護ポリシーすべての動作を確認します。

手順

1. 影響を受けた保護ポリシーごとに手動バックアップを実行します。 保護された資産の手動バックアップ で手順を参照してください。
2. 影響を受けた保護ポリシーにレプリケーション目的がある場合は、手動レプリケーションを実行します。 保護された資産の手動レプリケーション で手順を参照してください。
3. 影響を受けた保護ポリシーについて、資産の既存および新規のバックアップを参照します。
4. インスタント アクセス リストアなど、新しいバックアップとそのレプリカからリストアができることを確認します。

5. 既存のバックアップとレプリカを削除できることを確認します。 バックアップ コピーの削除 で手順を参照してください。

保護ストレージの追加

保護ポリシーのターゲットとして使用するストレージ システムを追加および構成します。 保護ストレージを追加できるのは管理者ロールのみです。

前提条件

メモ:

高可用性 PowerProtect DD システムを追加する場合は、 次の点を順守してください。

- PowerProtect Data Manager には、 個々のアクティブおよびスタンバイ DD システムを追加しないでください。
- ［Address］フィールドでは、 高可用性 PowerProtect DD システムのフローティング IP アドレスに対応するホスト名を使用します。
- 高可用性 PowerProtect DD システムは、 ルート証明書により検証されます。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。
   ［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブで、［Add］をクリックします。
3. ［Add Storage］ダイアログ ボックスで、ストレージ システム（［PowerProtect DD System］または［PowerProtect DD Management Center］）を選択します。
   システム プールの場合は、［DDMC］を選択します。
4. 高可用性 PowerProtect DD システムを追加するには、 チェックボックスを選択します。
5. ストレージ システムの属性を指定します。
   a. ［Name］フィールドで、ストレージの名前を指定します。
   b. ［Address］フィールドで、ホスト名、 完全修飾ドメイン名（FQDN）、 または IP アドレスを指定します。
   c. ［Port］フィールドで、 SSL 通信に使用するポートを指定します。 デフォルトは 3009 です。
6. ［Host Credentials］で［Add］をクリックします。 ストレージ システム間で共通の保護ストレージ認証情報をすでに構成している場合は、 既存のパスワードを選択します。 または、 新しい認証情報を追加し、［Save］をクリックできます。
7. 信頼できる証明書がストレージ システムに存在しない場合は、 証明書の承認を求めるダイアログ ボックスが表示されます。［Verify］をクリックして証明書を確認し、［Accept］をクリックします。
8. ［Save］をクリックして［Add Storage］ダイアログを終了し、ストレージ システムの検出を開始します。
   ストレージの追加要求が開始されたことを示すダイアログ ボックスが表示されます。
9. ［Storage］ウィンドウで、［Discover］をクリックし、 新しく検出されたストレージ システムを使用してウィンドウを更新します。
   検出が正常に完了すると、［Status］列が［OK］に更新されます。［DDMC］を選択すると、 ホストによって管理されている DD システムすべてが検出後に一覧表示されます。
10. ストレージ システムの場所を変更するには、 次の手順を実行します。
    ストレージ システムの場所は、 ストレージ システムに適用されるラベルに示されています。 特定の場所にコピーを保存する場合、 ラベルを使用して、 ポリシーの作成中に正しいストレージ システムを選択できます。
    a. ［Storage］ウィンドウで、 テーブルからストレージ システムを選択します。
    b. ［More Actions］ > ［Set Location］をクリックします。
       ［Set Location］ウィンドウが表示されます。
    c. ［Location］のリストで、［Add］をクリックします。
       ［Add Location］ウィンドウが表示されます。
    d. ［Name］フィールドで、 資産の場所の名前を入力し、［Save］をクリックします。

タスクの結果

PowerProtect Data Manager は使用可能な保護ストレージ システムを表示します。 各保護ストレージ システムについて、［Managed By］列には、 次のいずれかが含まれます。

表 23. ［Managed By］列の値

保護ストレージタイプ	値
スタンドアロン保護ストレージ システム。	保護ストレージ システムの名前。

表 23. ［Managed By］列の値 （続き）

保護ストレージタイプ	値
DDMC によって管理される保護ストレージ システムまたはシステム プール。	DDMC インスタンスの名前。

保護ストレージの編集

既存の保護ストレージ システムの名前、アドレス、ポート番号、認証情報を変更できます。保護ストレージを編集できるのは管理者ロールのみです。

前提条件

サーバーの DR と Search Engine ノード, Search Engine nodes の動作条件を以下に示します。 DD システムの IP アドレスまたはホスト名の変更 で詳細を参照してください。資産ソースの中には保護ストレージ システムのアドレスの変更をサポートしていないものがあるため、有効になっている各資産ソースの制限事項を確認します。

バックアップ、リストア、FLR ジョブが実行されていないことを確認します。

このタスクについて

このタスクは、保護ストレージ システムの保存済み管理インターフェイスを変更します。他のネットワーク インターフェイスを変更する場合は、この保護ストレージ システムをターゲットとする各保護ポリシー目的の優先ネットワーク インターフェイスもアップデートする必要があります。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。
   ［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブで、保護ストレージ システムを選択し、［Managed By］列のリンクをクリックします。
   ［Edit Storage］ダイアログ ボックスが開きます。
3. ［Edit Storage］ダイアログ ボックスで、ストレージ システムの属性を指定します。
   a. ［Name］フィールドで、新しいストレージの名前を指定します。
   b. ［Address］フィールドで、新しい完全修飾ドメイン名(FQDN)または IP アドレスを指定します。
   c. ［Port］フィールドで、SSL 通信に使用するポートを指定します。デフォルトは 3009 です。
   d. ［Host Credentials］で、新しい認証情報のセットを選択するか、［Add］をクリックします。
4. 保護ストレージ システムの信頼できる証明書が存在しない場合は、証明書の承認を求めるダイアログ ボックスが表示されます。［Verify］をクリックして証明書を確認し、［Accept］をクリックします。
5. ［Save］をクリックして、［Edit Storage］ダイアログ ボックスを終了します。
6. この保護ストレージ システムを使用する Microsoft SQL Server または Oracle 保護ポリシーの場合は、ロックボックスをアップデートします。
   a. 左ナビゲーション ペインで、［Protection］ > ［Protection Policies］の順に選択します。
      ［Protection Policies］ウィンドウが表示されます。
   b. この保護ストレージ システムをターゲットとする Microsoft SQL Server および Oracle 保護ポリシーを選択し、［Set Lockbox］をクリックします。

保護ストレージの交換

DD 保護ストレージ システムを交換した後、PowerProtect Data Manager UI を使用して交換用ストレージに合わせ、PowerProtect Data Manager で必要なストレージ設定を更新できます。PowerProtect Data Manager の保護ストレージ設定を更新できるのは管理者ロールのみです。このプロセスは、スタンドアロンの DD システム（Dell PowerProtect DD Management Center によって管理されていない DD システム）のみが対象です。

PowerProtect Data Manager とともに使用する DD 保護ストレージ システムを交換する場合、次のユースケースが考えられます。

- データ移行を必要とせず DD システムを交換する DD コントローラーのアップグレードまたはヘッド スワップを実行します。
- コレクション レプリケーションまたは DD クラウド移行を実行して、元の DD システムから同じ容量かそれ以上の新しい交換用システムにデータを移行します。

注意: 元の DD に存在していたすべてのストレージ ユニット、DD Boost ユーザー、データが新しい交換用 DD に含まれている必要があります。

DD システムを交換したら、PowerProtect Data Manager UI を使用してストレージ設定を更新する前に、次の要件を満たしていることを確認してください。

- DD ストレージ システムを使用するすべての保護ポリシーが無効になっている。

- 実行中のすべての保護ジョブが完了している。
- 必要なすべてのデータが、必要に応じて元の DD データから交換用 DD に手動で移行されている。

DD ストレージ システムを交換したら、次のいずれかの手順を実行して PowerProtect Data Manager の保護ストレージ設定を更新します。

データ IP が変更されていない場合のストレージ設定のアップデート

DD ストレージ システムを交換し、ネットワーク設定とデータ IP のいずれも変更されていない場合は、次の手順を実行します。

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。

   ［Storage］ウィンドウが表示されます。

2. ［Protection Storage］タブで、DD を選択し、［Discover］をクリックします。

PowerProtect Data Manager が、交換用 DD ストレージを自動的に検出し、交換用システムのストレージ設定を更新します。検出されると、［Infrastructure］ > ［Storage］ウィンドウの［Protection Storage］タブに交換用 DD の属性が表示されます。

データ IP が変更された場合のストレージ設定の更新

DD ストレージ システムを交換し、ネットワーク設定またはデータ IP のいずれかが変更された場合は、次の手順を実行します。

メモ: データ IP が変更されている場合、交換用 DD システムのネットワーク インターフェイス情報を更新します。

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。

   ［Storage］ウィンドウが表示されます。

2. ［Protection Storage］タブで、DD を選択した後、［More Actions］ > ［Replace System］を選択します。
3. ポリシーと実行中のジョブに関する警告メッセージを確認し、［Continue］をクリックします。
4. ［Replace System］ダイアログ ボックスで、交換用 DD システムの設定を指定し、［Apply］をクリックします。
   - ［Address］フィールドで、DD システム管理アドレスを、完全修飾ドメイン名(FQDN)または IP アドレスとして指定します。
   - ［Port］フィールドで、SSL 通信に使用するポートを指定します。デフォルトは 3009 です。
   - ［Host Credentials］で、新しい認証情報のセットを選択するか、［Add］をクリックします。

     ストレージ システムの信頼できる証明書が存在しない場合は、証明書の承認を求めるダイアログ ボックスが表示されます。［Verify］をクリックして証明書を確認し、［Accept］をクリックします。

   - ［Network Mapping］で、一覧表示されている変更された各データ IP に換わるデータ IP を指定します。

交換用 DD のストレージ設定を更新するためのシステム ジョブが作成されます。このシステム ジョブは［System Jobs］ウィンドウで監視できます。

メモ: 交換する DD システムを使用した PowerProtect Data Manager 操作を実行する前に、交換用システム ジョブが完了するまで待つ必要があります。

システム ジョブが完了すると、［Infrastructure］ > ［Storage］ウィンドウの［Protection Storage］タブに交換用 DD の属性が表示されます。DD システムを使用する保護ポリシーは、交換用 DD の設定に自動的に更新されます。

ストレージ ユニット

PowerProtect Data Manager は、保護ストレージ システム上でストレージ ユニットを作成、構成、再使用できます。これらのストレージ ユニットは、保護ポリシーおよびレプリケーション ポリシーのターゲットです。

「PowerProtect Data Manager の制御下にあるストレージ ユニット」という用語は、ここで説明されているいずれかの方法を使用して作成されたストレージ ユニットを表しています。

ストレージ ユニットを作成または変更する前、またはポリシーの保護ターゲットまたはレプリケーション ターゲットを変更する前に、適用される制限を確認します。ストレージ ユニット（MTree）の詳細については、適切なプラットフォーム向けの『*PowerProtect DD Virtual Edition* インストールおよび管理ガイド』を参照してください。

モバイル ストレージ ユニット

Smart Scale の場合、モバイル ストレージ ユニットは、ストレージ ユニットの概念をシステム プール全体の範囲に拡張します。モバイル ストレージ ユニットは、1 個のプール メンバー, pool member から別のものへ移動する可能性があります。したがって、次のとおりです。

- システム プールでストレージ ユニットを参照すると、PowerProtect Data Manager にはモバイル ストレージ ユニットのみが表示されます。
- DD システム上のストレージ ユニットを参照すると、PowerProtect Data Manager は通常の（モバイル以外の）ストレージ ユニットのみを表示します。
- システム プール レベルでモバイル ストレージ ユニットを使用する必要があります。

範囲の違いとは別に、PowerProtect Data Manager はモバイル ストレージ ユニットと通常のストレージ ユニットを同等に扱います。

ストレージ ユニットの作成と構成

PowerProtect Data Manager では、保護ストレージ システム上にストレージ ユニットを作成する方法が 2 個用意されています。

- 保護ポリシーの作成時に既存のストレージ ユニットを選択しない場合、PowerProtect Data Manager は、自動的にストレージ ユニットを作成します。
- PowerProtect Data Manager UI を使用して、必要に応じてストレージ ユニットを直接作成できます。

UI を使用して、PowerProtect Data Manager の制御下にあるストレージ ユニットのクォータと認証情報を構成できます。

をクリックして［Details］ペインを開き、構成値を含む既存のストレージ ユニットに関する詳細情報を表示します。

ストレージ ユニットの選択

保護ポリシーを作成または編集する場合、PowerProtect Data Manager では、保護ターゲットまたはレプリケーション ターゲットとしてストレージ ユニットを選択するオプションが提供されています。ストレージ ユニットは、同一のまたは別の保護ストレージ システム上で利用できます。

［Storage］ページには、保護ストレージ システムで検出されたすべてのストレージ ユニットが一覧表示されます。PowerProtect Data Manager により直接作成されたストレージ ユニットのみを保護ポリシーとして選択できます。他のストレージ ユニットは、既知の場合でも選択できません。

PowerProtect Data Manager の制御下にあるストレージ ユニットは、複数の保護ポリシーのターゲットにすることができます。ポリシーのターゲットとして既存のストレージ ユニットを選択すると、そのポリシーはストレージ ユニットのクォータ設定を継承します。

各資産タイプの保護ポリシーの作成および管理手順では、ポリシーの設定されたストレージ ユニットの使い方の詳細について説明します。

セキュリティ

ストレージ ユニットを共有するすべての保護ポリシーとアプリケーションは、そのストレージ ユニット内のすべてのデータにアクセスできます。ストレージ ユニットは、同一の組織単位に属する、または信頼関係を共有するポリシーとアプリケーションに対してのみ再使用してください。異なる組織単位のポリシーとアプリケーションでは、異なるストレージ ユニットを使用する必要があります。

また、ストレージ ユニットを使用する他のすべての外部アプリケーションでは、DD Boost の認証情報へのアクセスを保護し、制限する必要があります。これらの認証情報は、PowerProtect Data Manager データへのアクセスを提供します。

ストレージ ユニットの自動メンテナンス

自動的に作成されたストレージ ユニットの場合、次の両方の条件に該当する場合は、自動メンテナンスによってストレージ ユニットが削除されます。

- バックアップまたはレプリケーションのためにストレージ ユニットをターゲットとする保護ポリシーがありません。
- ストレージ ユニットにバックアップが含まれていません。

自動メンテナンスによって、これらの空の未使用ストレージ ユニットが削除されます。ガバナンス モードの保存では、保存ロックが有効の場合でも、自動メンテナンスによってこれらのストレージ ユニットが削除されます。コンプライアンス モードが有効になっているストレージ ユニットを削除するには、セキュリティ担当者の認証情報が必要なため、自動メンテナンスではこれらのストレージ ユニットを削除できません。

直接作成されたストレージ ユニットの場合、これらの条件が該当する場合でも、自動メンテナンスによりストレージ ユニットは削除されません。この場合は、保護ストレージ システムの管理者に問い合わせてストレージ ユニットを削除してください。

以前のリリースからのアップデート

保護ポリシーは、PowerProtect Data Manager の以前のリリースにおけるポリシーに対して自動的に作成されたストレージ ユニットを使用できます。以前のリリースで作成されたポリシーは、引き続き以前と同様に機能します。

Oracle エージェントの以前のリリースでは、複数の保護ポリシーを持つストレージ ユニットはサポートされていません。詳細については、『*PowerProtect Data ManagerOracle RMAN* ユーザー ガイド』を参照してください。

ストレージ ユニットの制限事項

複数の保護ポリシーを持つストレージ ユニットを使用する場合は、次の制限事項が適用されます。

- PowerProtect Data Manager は、PowerProtect Data Manager を使用して作成されていないストレージ ユニットをターゲットにしたり構成したりすることはできません。
- PowerProtect Data Manager は、クラウド階層化のために別の場所に構成されたストレージ ユニットをターゲットにすることはできません。
- 保護ポリシーを別のストレージ ユニットまたは保護ストレージ システムに移動すると、フル バックアップが必要になる場合があります。
  - 仮想マシン、ファイル システムのバックアップ、Kubernetes、Microsoft Exchange Server バックアップの場合、次回のバックアップは自動的にフル バックアップに昇格されます。
  - Microsoft SQL Server、Oracle、SAP HANA のバックアップの場合は、新しいストレージ ユニットでこれらの資産の手動フル バックアップを完了させます。
- ストレージ データ管理の保護ポリシーでは、ストレージ ユニットを他の保護ポリシーと共有することはできません。
- ストレージ ユニットのいずれかの保護ポリシーで保存ロックが無効化されている場合、ストレージ ユニットの保存ロックは無効になります。
- Oracle エージェントの以前のリリースでは、保護ポリシー間のストレージ ユニットの共有はサポートされていません。詳細については、*PowerProtect Data ManagerOracle RMAN* ユーザー ガイドを参照してください。

PowerProtect DD のストレージ ユニットに関する考慮事項

PowerProtect DD に関しては、ストレージ ユニットに一定の制限とベスト プラクティスがあります。次の考慮事項に注意してください。

- PowerProtect Data Manager との同期の問題を回避するには、PowerProtect Data Manager が管理または使用しているストレージ ユニットを DD から直接変更しないでください。
- PowerProtect Data Manager で作成されたストレージ ユニットは、DD 管理者がストレージ ユニット レプリケーションを設定する目的で変更することはできません。
- PowerProtect Data Manager で作成されたストレージ ユニットは、クラウド階層化の目的で構成することはできません。
- PowerProtect DD のモデルごとに適用されるサポートされているストレージ ユニットの制限事項については、E-Lab Navigator を参照してください。

保存ロック

保存ロックを使用すると、指定した期間内に保護ストレージ システム上のデータが削除または変更されないようにすることができます。PowerProtect Data Manager では、バックアップとレプリカについて、ガバナンス モードとコンプライアンス モード両方の保存ロックをサポートします。

モード別の違いなど、保存ロック モード別の詳細については、PowerProtect DD のドキュメントを参照してください。保存ロックを PowerProtect Data Manager で使用するには、保護ストレージ システム上で有効にし、ライセンスを取得する必要があります。

保存ロックは、次の 2 段階のプロセスです。

1. 適切な保存ロック モードを設定するストレージ ユニットを作成します。構成によって保存ロックは有効化されますが、アクティブ化されません。
2. このストレージ ユニットをターゲットにし、保存ロックをアクティブ化する保護ポリシーを構成します。保護ポリシーの保存ロック設定を切り替えると、選択したストレージ ユニットの構成に従って保存ロックがアクティブ化されます。

一度設定すると、ストレージ ユニットの保存ロック モードを変更できません。保護ポリシーで別の保存ロック モードを使用するには、別のストレージ ユニットをターゲットにしてください。元の保存ロック モードは、変更前に作成された既存のバックアップまたはレプリカに対して保持されます。

保存ロック モードを選択すると、どの保護ポリシーがストレージ ユニットを共有できるかに影響する場合があります。ストレージ ユニット アーキテクチャを設計する際は、保存ロックの設定を考慮してください。

コンプライアンス モード

コンプライアンス モードの保存ロックを構成またはアクティブ化する前に、次の詳細を確認してください。

- コンプライアンス モードには DDOS 7.10 以降が必要です。以前のバージョンでは、ガバナンス モードのみをサポートしています。

- コンプライアンス モードでは、関連する保護ストレージ システムにセキュリティ担当者の認証情報が必要です。PowerProtect Data Manager は、セキュリティ担当者の認証情報を保存しません。
- ストレージ データ管理の Storage Direct エージェントは、コンプライアンス モードをサポートしていません。
- 保護ポリシーの構成中に選択ドロップダウン リストからストレージ ユニットを作成するオプションでは、ガバナンス モードのみをサポートします。コンプライアンス モードはサポートしません。コンプライアンス モードを使用するには、関連する保護ポリシーを構成する前に、ストレージ ユニットを作成して構成します。
- コンプライアンス モードが有効になっているストレージ ユニットを削除するには、関連する保護ストレージ システムのセキュリティ担当者の認証情報が必要です。

システム プールとコンプライアンス モードの保存ロック

モバイル ストレージ ユニットを作成すると、ストレージ ユニットが任意のプール メンバー, pool member に配置される可能性があります。ただし、セキュリティ担当者の認証情報は、プール メンバー, pool member ごとに異なります。次のロードマップを使用してモバイル ストレージ ユニットを作成し、作成後に保存ロックを有効にしてください。

1. すべてのプール メンバー, pool members に対してコンプライアンス モードが有効になっていることを確認します。
2. モバイル ストレージ ユニットを作成し、保存ロック モードを `None` に設定します。
3. モバイル ストレージ ユニットの詳細を確認し、ストレージ ユニットが配置されているプール メンバー, pool member をメモします。
4. モバイル ストレージ ユニットを編集し、保存ロック モードをコンプライアンス モードに変更します。そのプール メンバー, pool member のセキュリティ担当者の認証情報を入力します。

ストレージ ユニットの作成

保護ポリシーで使用するために、PowerProtect Data Manager UI を使用してストレージ ユニットを直接作成します。

前提条件

保護ストレージ システムに PowerProtect Data Manager を少なくとも 1 個追加します。

手順

1. 左ナビゲーション ペインで、[Infrastructure] > [Storage] の順に選択します。
   [Storage] ウィンドウが表示されます。
2. [Protection Storage] タブで、ストレージ システムを選択してから、[More Actions] > [Manage Storage Units] の順に選択します。
   [[ストレージ ユニット]] ページが開き、PowerProtect Data Manager の制御下にあるストレージ ユニットのリストが表示されます。
3. [Add] を選択します。
   [Create Storage Unit] または [Create Mobile Storage Unit] ダイアログ ボックスが開きます。
4. 新しいストレージ ユニットの名前を入力します。
5. システム プールのモバイル ストレージ ユニットの場合は、[Network Group] を選択します。
   ネットワーク グループは、DDMC で構成され、異なる物理ネットワークまたは仮想ネットワーク経由でシステム プールへのアクセスを提供します。ネットワーク グループには、プール メンバー, pool members の IP アドレスと、システム プールへのアクセスにクライアントが使用する IP アドレスに関する情報が含まれています。
6. ストレージ ユニット リソースの消費量を制限する容量とストリーム クォータを設定します。
   クォータ制限には、ハード制限とソフト制限の 2 種類があります。ソフト制限かハード制限、またはソフト制限とハード制限の両方を設定できます。値は両方整数である必要があり、ソフト値はハード値よりも小さい必要があります。

   メモ: ソフト制限を設定して制限に達すると、アラートが生成されますが、データは引き続き書き込まれます。ハード制限を設定して制限に達すると、データを書き込むことができなくなります。データがストレージ ユニットから削除されるまで、すべてのデータ保護操作が失敗します。クォータ構成の詳細については、適切なプラットフォーム向けの『*PowerProtect DD Virtual Edition* インストールおよび管理ガイド』を参照してください。

   a. [Capacity Quota]：保護ストレージに書き込まれた圧縮前データの合計サイズを制御します。
   b. [Stream Quota]：データ保護操作中に許可されているコンカレント ストリームの数。[Stream Quota] 制限を設定することにより、データ保護操作によってリソースを大量に消費している場合に、パフォーマンスに悪影響が及ぶのを防ぐことができます。
7. [Retention Lock Mode] を選択可能なモード（`None`、`Compliance`、または `Governance`）に設定します。
   このフィールドに表示されるのは、選択した保護ストレージ システムについてライセンスがあるオプションと有効になっているオプションのみです。有効になっている保存ロック モードがない場合、選択できるオプションは `None` だけです。

Compliance を選択した場合、保護ストレージ システムに関連付けられているセキュリティ担当者のユーザー名とパスワードを指定します。

8. ［Save］を選択します。

タスクの結果

PowerProtect Data Manager は、選択された保護ストレージ システム上にストレージ ユニットを作成します。

ストレージ ユニットの編集

PowerProtect Data Manager UI を使用して、既存のストレージ ユニットの設定を構成します。ストレージ ユニットをターゲットとする保護ポリシーのリストを表示することもできます。

このタスクについて

保護ストレージ システム上で直接行ったこれらのストレージ ユニット属性の変更は、PowerProtect Data Manager にも反映されます。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。
   ［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブで、ストレージ システムを選択してから、［More Actions］ > ［Manage Storage Units］の順に選択します。
   ［[ストレージ ユニット]］ページが開き、PowerProtect Data Manager の制御下にあるストレージ ユニットのリストが表示されます。
3. ストレージ ユニットの詳細または使用状況を表示するには、そのストレージ ユニットのを選択します。
   ［[詳細]］ペインが開き、名前、タイプ、容量、クォータ情報、および現在ストレージ ユニットをターゲットとしている保護ポリシーのリストが表示されます。
   ストレージ ユニットには、ストレージ ユニットのターゲットではなくなった保護ポリシーからのコピーが含まれている場合があります。
4. リストからストレージ ユニットを選択して、［編集］を選択します。
   ［Edit Storage Unit］または［Edit Mobile Storage Unit］ダイアログ ボックスが開きます。
5. システム プールのモバイル ストレージ ユニットの場合は、［Network Group］を選択します。
   ネットワーク グループは、DDMC で構成され、異なる物理ネットワークまたは仮想ネットワーク経由でシステム プールへのアクセスを提供します。ネットワーク グループには、プール メンバー, pool members の IP アドレスと、システム プールへのアクセスにクライアントが使用する IP アドレスに関する情報が含まれています。
6. ストレージ ユニット リソースの消費量を制限する容量とストリーム クォータを設定します。
   クォータ制限には、ハード制限とソフト制限の 2 種類があります。ソフト制限かハード制限、またはソフト制限とハード制限の両方を設定できます。値は両方整数である必要があり、ソフト値はハード値よりも小さい必要があります。

   メモ: ソフト制限を設定して制限に達すると、アラートが生成されますが、データは引き続き書き込まれます。ハード制限を設定して制限に達すると、データを書き込むことができなくなります。データがストレージ ユニットから削除されるまで、すべてのデータ保護操作が失敗します。クォータ構成の詳細については、適切なプラットフォーム向けの『*PowerProtect DD Virtual Edition* インストールおよび管理ガイド』を参照してください。

   a. ［Capacity Quota］：保護ストレージに書き込まれた圧縮前データの合計サイズを制御します。
   b. ［Stream Quota］：データ保護操作中に許可されているコンカレント ストリームの数。［Stream Quota］制限を設定することにより、データ保護操作によってリソースを大量に消費している場合に、パフォーマンスに悪影響が及ぶのを防ぐことができます。
7. ［Retention Lock Mode］が None の場合、［Retention Lock Mode］を選択可能なモード（Compliance または Governance）に設定します。
   このフィールドに表示されるのは、選択した保護ストレージ システムについてライセンスがあるオプションと有効になっているオプションのみです。有効になっている保存ロック モードがない場合、選択できるオプションは None だけです。
   Compliance を選択した場合、保護ストレージ システムに関連付けられているセキュリティ担当者のユーザー名とパスワードを指定します。
8. ［Save］を選択します。

タスクの結果

PowerProtect Data Manager は、ストレージ ユニットの設定をアップデートします。

ストレージ ユニットの削除

コンプライアンス モードの保存ロックを使用しているストレージ ユニットを削除するには、セキュリティ担当者の認証情報が必要なため、自動メンテナンスではこれらのストレージ ユニットを削除できません。コンプライアンス モードの保存ロックを使用しているストレージ ユニットを削除するには、この手順を使用してください。

前提条件

ストレージ ユニットを削除する前に、ストレージ ユニットを空にし、保護ポリシーのターゲットから除外する必要があります。ストレージ ユニットは PowerProtect Data Manager の管理下にあり、PowerProtect Data Manager のこのインスタンスによって作成されている必要があります。

コンプライアンス モードの保存ロックが有効になっている場合は、関連付けられている保護ストレージ システムのセキュリティ担当者の認証情報が必要です。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。
   ［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブで、ストレージ システムを選択してから、［More Actions］ > ［Manage Storage Units］の順に選択します。
   ［［ストレージ ユニット］］ページが開き、PowerProtect Data Manager の制御下にあるストレージ ユニットのリストが表示されます。
3. リストからストレージ ユニットを選択して、［Delete］を選択します。
   ［Enter Security Officer Credential］ダイアログ ボックスが開きます。
4. セキュリティ担当者認証情報を指定して、［OK］をクリックします。

タスクの結果

PowerProtect Data Manager によってストレージ ユニットが削除されます。

ストレージ ユニットでの Infifinite Retention Hold の有効化

Infifinite Retention Hold (IRH)は、ストレージ ユニット上のデータの変更または削除を無期限に防止します。IRH によって、ストレージ ユニットの Retention Lock Governance を無効にできなくなりますが、Retention Lock 属性の変更は可能です。IRH でファイルの削除も変更もできなくするには、ファイルがロックされているか、ロックの有効期限が過ぎている必要があります。ロック履歴のないファイルは、IRH の影響を受けません。

前提条件

ストレージ ユニットで Retention Lock モード（ガバナンスまたはコンプライアンス）が有効になっていることを確認します。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。
   ［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブからストレージ システムを選択した後、［More Actions］ > ［Manage Storage Units］の順に選択します。
3. リストからストレージ ユニットを選択し、［More Actions］ > ［Enable Indefinite Retention Hold］ を選択します。
4. セキュリティ担当者の認証情報を入力し、［Enable］をクリックします。
   コンプライアンス モードが有効になっているストレージ ユニットで IRH を有効または無効にする場合は、セキュリティ担当者の認証情報が必要です。

ストレージ ユニットでの Infifinite Retention Hold の無効化

ストレージ ユニットで Indefinite Retention Hold (IRH)を無効にして、期限切れのファイルを削除したり、ストレージ ユニットで Retention Lock Governance を無効にしたりできます。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Storage］の順に選択します。
   ［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブからストレージ システムを選択した後、［More Actions］ > ［Manage Storage Units］の順に選択します。
3. リストからストレージ ユニットを選択した後、［More Actions］ > ［Disable Indefinite Retention Hold］ を選択します。

4. 必要に応じて、セキュリティ担当者の認証情報を入力し、［Disable］をクリックします。
   コンプライアンス モードが有効になっているストレージ ユニットで IRH を有効または無効にする場合は、セキュリティ担当者の認証情報が必要です。

ストレージ ユニットのパスワードに関する操作

『*PowerProtect Data Manager* セキュリティ構成ガイド』では、次のトピックの手順について説明しています。

- 既存のストレージ ユニット パスワードの表示
- UI を使用したストレージ ユニットのパスワード変更
- ストレージ ユニット パスワードのポリシー変更

ストレージ システムとストレージ ユニット領域のレポート作成の違い

PowerProtect Data Manager におけるストレージ領域のレポート方法に関する違いの詳細については、次のセクションを参照してください。

PowerProtect Data Manager UI でのサイズ計算に使用される 10 進法

サイズの計算（例えば、資産のサイズやストレージ システムの容量）について、PowerProtect Data Manager UI は 10 進法を使用します。これにより、MB、GB、TB のサイズを指定します。

ただし、その他のコンポーネントは 2 進法を使用する場合があります。これは、MiB、GiB、および TiB のサイズを指定します。レポート サイズに不一致がある場合は、UI を使用して、最も正しい情報を取得します。

PowerProtect Data Manager および DD Virtual Edition でのストレージ ユニット容量のレポート方法

領域の計算（物理容量と論理容量）の違いにより、ストレージ ユニット容量のレポート方法に関して、PowerProtect Data Manager と DD Virtual Edition の間に不一致があります。

例えば、PowerProtect Data Manager では DD ストレージ ユニットの論理容量が表示されるため、PowerProtect Data Manager UI の［Infrastructure］ > ［Storage］ウィンドウで［More Actions］ > ［Manage Storage Units］を選択したときにレポートされる値は、DDVE で報告される物理容量よりも大きく表示される場合があります。

物理的なストレージ ユニットの容量を確認するには、代わりに DDVE を使用してください。

ストレージ容量しきい値のモニタリング

PowerProtect Data Manager は保護ストレージの使用状況を定期的にモニターし、システムが 2 個の容量しきい値に達した際にアラートを報告します。システムがストレージ容量を完全に消費する前に、これらのアラートを確認して対処します。

容量が 80%になると、PowerProtect Data Manager によって週次警告アラートが生成されます。このしきい値に達した場合は、容量を追加するか、別のストレージ ターゲットに保護ポリシーを移動する計画を立てる必要があります。保護ポリシーの管理 で、ポリシーの移動に関する詳細を参照してください。

容量が 95%になると、PowerProtect Data Manager によって日次重大アラートが生成されます。このしきい値に達した場合、間もなく容量が完全に消費されます。

容量アラートのしきい値を変更するには、サポートに問い合わせる必要があります。

4

PowerProtect 検索エンジンの使用

トピック：

PowerProtect Search Engine

PowerProtect Data Manager を導入すると、PowerProtectSearch Engine ソフトウェアがデフォルトでインストールされます。

PowerProtect Search Engine では、仮想マシンのファイル メタデータのインデックスを作成し、構成可能なパラメーターに基づいて検索できるようにします。この機能を使用するには、Search Engine に少なくとも 1 個の Search Engine ノード, Search Engine node を追加し、クラスターを形成します。Search Engine ノード, Search Engine node を追加すると、インデックス作成機能が有効になります。

保護ポリシーを作成する際、資産のバック アップ中にインデックスが作成されるように、インデックス作成オプションを有効化することができます。ディザスター リカバリーとしてインデックスをリカバリーする場合は、手動プロセスで行います。インデックス作成のリカバリー手順は、今後のリリースで自動化されます。

DR バックアップを実行するか、スケジュール設定するか、手動でトリガーすると、クラスターのバックアップ ワークフローがクラスターのインデックス データをバック アップします。バックアップ タスクが作成されると、[Details] の下で、検索コンポーネントのバックアップのステータスを個別で確認することができます。

メモ: 検索クラスターを統合し、スケジュール設定されたバックアップは、[Jobs] ペインで 2 個の同一ジョブとして表示されます。1 個はただちに実行される初期化ジョブ、もう 1 個はサーバー DR と検索クラスターのバックアップを両方実行するバックアップ ジョブとして表示されます。

完全修飾ドメイン名(FQDN)のみを使用して Search Engine ノード, Search Engine nodes を導入します。PowerProtect Data Manager は、導入前にホスト名が FQDN であることを確認します。

制限事項

- PowerProtect Search Engine は、仮想マシンのバックアップおよび保護ポリシーのセット アップ、構成が可能なオプション機能です。この機能を有効にすると、Search Engine のバックアップがサーバー バックアップ プロセスの一部とみなされます。このリリースでは、これらのバックアップを無効にできません。したがって、[Search] が有効になっている場合は、ServerBackup MTree を含む DD システム上の Search Engine ノード, Search Engine node を [Allow] リストに追加する必要があります。NFS をサーバー DR に使用する場合は、NFS エクスポートのクライアント リストに Search Engine ノード, Search Engine node の IP アドレスまたはホスト名を追加します。
- PowerProtect Data Manager へのアップデート後、Search Engine がすでに構成されていて、初めて [Networks] ページを使用して仮想ネットワークを環境に追加した場合、PowerProtect Data Manager は、仮想ネットワークを自動的に Search Engine に追加しません。代わりに、各ノードを手動で編集して、仮想ネットワークを追加します。このアクションにより、Search Engine は仮想ネットワークを認識します。以降のすべての新しい仮想ネットワークは、自動的に Search Engine に追加されます。
- 運用中の Search Engine ノード, Search Engine node が失敗し、ノードをリカバリーできず、Search Engine クラスターのステータスが `Failed` になった場合、クラスターを削除し、新しいクラスターを作成する必要があります。

インデックス作成の設定と管理

Search Engine ノード, Search Engine node をセット アップし、インデックス作成を構成します。

前提条件

次の事項を確認：

- vCenter データストアが構成されます。*PowerProtect Data Manager* 仮想マシン ユーザー ガイドでは、資産ソースとして vCenter Server を追加するための詳細な手順について説明しています。
- PowerProtect Data Manager で、vCenter Server のネットワークを検出します。
- PowerProtect Search Engine で次の要件を満たします。

  メモ: 各 Search Engine ノード, Search Engine node は次のシステム要件を満たしている必要があります。

  - CPU：4 * 2 GHz（4 個の仮想ソケット、ソケットごとに 1 個のコア）。
  - メモリー：8 GB RAM
  - ディスク：3 基のディスク（各 50 GB）と 1 基のディスク（1TB）
  - Internet Protocol：IPv4 のみまたは IPv6 のみ
  - NIC：1 個のポートで 1 つの vmxnet3 NIC
- PowerProtect Data Manager システムは NTP サーバーを使用するように構成されています。マルチノード クラスター内の Search Engine ノード, Search Engine nodes 間で時刻を同期するには、NTP サーバー構成が必要です。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［検索エンジン］の順に選択してから、［ノードの追加］をクリックします。
2. ［検索エンジン ノードの追加］ウィザードで、必要なパラメーターを入力します。
   - ［Hostname］、［IP Address］、［Gateway］、［DNS］、［Netmask］。
   - ［vCenter］：複数の vCenter Server インスタンスを追加してある場合、Search Engine ノード, Search Engine node を導入する vCenter Server を選択します。

     メモ: 内部 vCenter Server を選択していないことを確認します。
   - ［ESX Host/Cluster］：Search Engine ノード, Search Engine node を導入するクラスターまたは ESXi ホストを選択します。
   - ［ネットワーク］：選択した ESXi ホスト/クラスターで使用可能なすべてのネットワークが表示されます。仮想ネットワーク（VLAN）の場合、このネットワークは管理トラフィックを伝送します。
   - ［データ ストア］：選択した ESXi ホスト/クラスターからアクセスできるすべてのデータストアが表示されます。
3. ［次へ］をクリックします。
   ［［ネットワーク構成］］ページが表示されます。
4. ［［ネットワーク構成］］ページで次の手順を実行します。

   ［Networks Configuration］ページでは、管理コンポーネントのデータ, Data for Management Components トラフィックに使用する仮想ネットワーク(VLAN)を構成できます。仮想ネットワークを構成せずに続行するには、［優先ネットワーク ポートグループ］の選択欄を空のままにして、［次へ］をクリックします。

   a. ［優先ネットワーク ポートグループ］リストから、仮想ゲスト タギング（VGT）グループを選択します。
      VST（仮想スイッチ タギング）グループはサポートされていません。

      リストには、トランク範囲内のすべての仮想ネットワークが表示されます。複数のネットワークを含むポートグループを選択した場合、PowerProtect Data Manager は、自動的にすべてのネットワークを選択します。個々のネットワークを選択することはできません。

      Search Engine ノード, Search Engine node には、選択した各仮想ネットワークの固定 IP プールの IP アドレスが必要です。プール内に十分な数の IP アドレスがない場合は、そのネットワークに他のアドレスを追加するよう求めるウィザードが表示されます。

      選択した仮想ネットワークが、Search Engine ノード, Search Engine nodes と互換性のあるトラフィック タイプをサポートしていることを確認します。
   b. 必要に応じて、指摘された仮想ネットワークの［追加の IP アドレス］列に、使用可能な固定 IP アドレスまたは IP アドレス範囲を入力します。

      複数の仮想ネットワークを使用している場合は、利便性を高めるために、いずれかの［自動展開］オプションを使用することもできます。

      - ［IP 末尾の拡張］：ウィザードによって、固定 IP プール内の IP アドレス末尾のホスト部分が追加されます。［適用］をクリックします。
      - ［同じ最後の数字］：ウィザードによって、指定値に IP アドレスのネットワーク部分が追加されます。IP アドレスのホスト部分を入力し、［適用］をクリックします。

      ウィザード上で、各ネットワーク用に［追加の IP アドレス］列の値がアップデートされます。提案された IP アドレスを確認します。
   c. ［次へ］をクリックします。
5. ［［サマリー］］ページで情報を確認し、［完了］をクリックします。
   新しい Search Engine ノード, Search Engine node が導入され、詳細が下のパネルに表示されます。
6. （オプション）前述の手順を繰り返して、クラスターに追加の Search Engine ノード, Search Engine nodes を導入します。

   メモ: 以前の Search Engine ノード, Search Engine node が正常に導入されていることを確認してから別のものを追加します。

7. ［Configure Search Engine］ダイアログ ボックスで、インデックス作成の有効化または無効化、有効期限の承認または変更を行い、［OK］をクリックします。

メモ:

- インデックス クラスターが 70 パーセントに達すると、アラートが生成されます。90 パーセントに達すると、アラートが生成され、インデックス作成が一時停止されます。グローバル インデックスの有効期限の間隔を指定し、定期的にインデックスをクリーン アップします。これにより、容量が解放されます。
- インデックス作成をオフまたは変更するには、［インフラストラクチャ］ > ［検索エンジン］を選択し、クラスターを選択して、［クラスターの構成］をクリックします。［［検索クラスターの構成］］ダイアログ ボックスでは、サービスを有効化/無効化したり、有効日数を変更したりすることができます。
- インデックスは、グローバル設定の期限、または関連づけられているコピー期限のどちらが早い方で期限切れとなります。
- 保護された保護ポリシーに追加された資産のインデックス作成を停止するには、保護ポリシーの構成中にインデックス作成オプションを無効にします。
- 最大 5 個の Search Engine ノード, Search Engine nodes を追加できます。

次の手順

メモ:

失敗した操作を編集または再試行し、アドレス プールに追加の IP アドレスがある場合、PowerProtect Data Manager は、最後に失敗した IP アドレスを破棄済みとマークします。PowerProtect Data Manager は、破棄済みとマークされている IP アドレスを再使用しません。UI では、この状態は表示されません。

REST API を使用して、IP アドレスが破棄済みとマークされていることを検出する方法の詳細については、KB 記事 000181120 を参照してください。この記事では、破棄された IP アドレスを再び使用するために検出条件を修正する手順についても説明されています。

Search Engine ノード, Search Engine node の削除

PowerProtect Data Manager UI は、マルチノード クラスターからの Search Engine ノード, Search Engine node の削除をサポートしています。

次の修復は、Search Engine ノード, Search Engine node 上で実行できます。

- 領域が不要になった場合は、Search Engine クラスターから運用ノードを削除してクラスターの容量を減らします。
- Search Engine クラスターへの導入に失敗したノードを再導入または削除します。
- Search Engine クラスター内のすべてのノードを削除して、クラスターを削除します。

運用中の Search Engine ノード, Search Engine node の削除

領域が不要になった場合は、運用中の Search Engine ノード, Search Engine node を削除して、クラスター容量を減らすことができます。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Search Engine］の順に選択します。
2. 削除するノードをリストから選択し、［More Actions］ > ［Delete Node］を選択します。
3. ［Delete Search Engine Node］ウィンドウで、［Delete Node］をクリックします。

注意: ［Delete node without moving the index data］**を選択しないでください。このオプションを選択すると、Search Engine クラスターが非アクティブになり、リカバリーできなくなります。**

4. ［Jobs］ > ［System Jobs］ウィンドウに移動し、ノード削除の進行状況をモニターします。

導入に失敗した Search Engine ノード, Search Engine node の再導入または削除

PowerProtect Data Manager を使うと、正常に導入できなかった Search Engine ノード, Search Engine node を再導入したり削除したりできます。

このタスクについて

［Redeploy Node］機能は、追加したものの、Search Engine に正常に導入できなかったノードに対してのみ有効です。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Search Engine］の順に選択します。
2. 導入に失敗したノードを選択します。
3. 次のいずれかを実行します。
   - ノードを再導入するには、［More Actions］ > ［Redeploy Node］を選択します。

     ［Redeploy Search Engine Node］ウィザードが開きます。Search Engine は、ノードの追加時に入力した情報をフィールドに入力します。情報が正しいことを確認します。
   - ノードを削除するには、［More Actions］ > ［Delete Node］の順に選択します。
4. ［Jobs］ > ［System Jobs］ウィンドウの順に移動し、ノードの再導入または削除の進行状況をモニターします。

すべての Search Engine ノード, Search Engine nodes を削除して、Search Engine クラスターを削除する

Search Engine クラスター内のすべての Search Engine ノード, Search Engine nodes を削除して、クラスターを削除できます。

このタスクについて

クラスターの削除が必要になるのは、運用ノードの 1 台に障害が発生し、そのノードをリカバリーできず、クラスターのステータスが `Failed` になった場合です。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Search Engine］の順に選択します。
2. 各ノードに対して次の手順を実行します。
   a. リストからノードを選択します。
   b. ［More Actions］ > ［Delete Node］を選択します。
   c. ［Delete Node］をクリックします。

      メモ: 障害が発生している運用ノードがない場合は、［Delete nodes without move the index data］オプションを使用できます。このオプションを選択すると、クラスターはリカバリーできない状態で非アクティブになります。

   d. ［Jobs］ > ［System Jobs］ウィンドウの順に移動して、ノード削除操作の進行状況をモニタリングします。

タスクの結果

すべての Search Engine ノード, Search Engine nodes が削除され、Search Engine クラスターが削除されます。

Search Engine ノード, Search Engine node のネットワーク構成の編集

仮想ネットワーク構成を変更するには、次の手順を実行します。他のネットワーク構成設定を変更するには、カスタマー サポートにお問い合わせください。

前提条件

ネットワークを削除する前に、インデックス作成を無効にします。 インデックス作成の設定と管理 で手順を参照してください。

このタスクについて

仮想ネットワーク構成の問題によって Search Engine ノード, Search Engine node の導入に失敗した場合は、構成のアップデートを行い、静的 IP プールに他の IP アドレスを追加できます。初期導入時に仮想ネットワークを構成しなかった場合は、同じ仮想ゲスト タギング(VGT)ポート グループ内の仮想ネットワークに Search Engine ノード, Search Engine node を追加することもできます。

手順

1. PowerProtect Data Manager UI から、[Infrastructure] > [Search Engine] の順に選択してから、該当する Search Engine ノード, Search Engine node を選択します。
2. [その他のアクション] > [ネットワークの編集] の順に選択します。
   [検索エンジン ノードの編集] ウィザードが開き、[[ネットワーク構成]] ページが表示されます。
3. 該当する場合は、[Preferred Network Portgroup] リストから管理コンポーネントのデータ, Data for Management Components トラフィックを伝送する VGT ネットワークを選択します。

   リストには、トランク範囲内のすべての仮想ネットワークが表示されます。複数のネットワークを含むポートグループを選択した場合、PowerProtect Data Manager は、自動的にすべてのネットワークを選択します。個々のネットワークを選択することはできません。

   Search Engine ノード, Search Engine node には、選択した各仮想ネットワークの固定 IP プールの IP アドレスが必要です。プール内に十分な数の IP アドレスがない場合は、そのネットワークに他のアドレスを追加するよう求めるウィザードが表示されます。

   ネットワーク名の横に警告記号（⚠）が付いた仮想ネットワークには、注意と確認が必要です。例えば、ネットワーク構成を変更した場合、構成したトラフィック タイプが Search Engine ノード, Search Engine nodes をサポートしていない可能性があります。Search Engine ノード, Search Engine node に適用されなくなったインターフェイスをすべてクリアーします。
4. 必要に応じて、指摘された仮想ネットワークの [追加の IP アドレス] 列に、使用可能な固定 IP アドレスまたは IP アドレス範囲を入力します。

   複数の仮想ネットワークを使用している場合は、利便性を高めるために、いずれかの [自動展開] オプションを使用することもできます。

   - [IP 末尾の拡張]：ウィザードによって、固定 IP プール内の IP アドレス末尾のホスト部分が追加されます。[適用] をクリックします。
   - [同じ最後の数字]：ウィザードによって、指定値に IP アドレスのネットワーク部分が追加されます。IP アドレスのホスト部分を入力し、[適用] をクリックします。

   ウィザード上で、各ネットワーク用に [追加の IP アドレス] 列の値がアップデートされます。提案された IP アドレスを確認します。
5. [次へ] をクリックします。
6. [[サマリー]] ページで情報を確認し、[完了] をクリックします。

次の手順

インデックス作成を無効にした場合は、インデックス作成を再度有効にします。 インデックス作成の設定と管理 で手順を参照してください。

検索の実行

Search Engine を導入して構成すると、PowerProtect Data Manager UI の [File Search] 機能を使用して、すべてのインデックス データを検索し、バックアップ コピー内の保護されたファイルとフォルダを見つけることができます。資産タイプがインデックス検索用にセット アップされている場合は、[File Search] ボタンが、資産の [Restore] メニューに表示されます。

検索を実行する前に、次のことを確認します。

- Search Engine ノード, Search Engine node がセット アップされている。
- インデックス作成検索が有効になっていること。

Search Engine 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、Search Engine に関する問題のトラブルシューティングについて説明します。

一部の Search Engine のトラブルシューティング手順では、個々の Search Engine ノード, Search Engine nodes の認証情報が必要です。Search Engine ノード, Search Engine nodes には、ソフトウェアの問題のトラブルシューティングに使用される管理者アカウントと root ユーザー アカウントがあります。Search Engine ノード, Search Engine node 認証情報を管理する手順については、*PowerProtect Data Manager* セキュリティ構成ガイドを参照してください。

Search Engine ノード, Search Engine node 障害時にエラーが表示される

Search Engine ノード, Search Engine node に障害が発生した場合、検索中に次のエラーが表示されることがあります。

```
Not able to deploy search-node.com. Another session "<host_name>" is already configured with the same hostname. Would you like to redeploy search node or delete the node?
```

このエラーが発生した場合は、Search Engine ノード, Search Engine node を削除して、操作をやり直します。編集する場合は、ノードを削除します。次に、新しいモード モーダルが以前の入力とともに表示されます。エラーの原因となった入力は重要としてマークされます。

証明書に関する問題

Search Engine ノード, Search Engine node に導入した証明書が破損すると、インデックス作成のバックアップや検索クエリーの実行に問題が発生する場合があります。

次のいずれかのテストを実行して、証明書に関する問題を特定してください。

- PowerProtect Data Manager でログ バンドルのダウンロード ユーティリティーを使用して、VM Direct のバックアップ VM ログを確認し、次のようなログ エントリーを探す。

```
ERROR: Failed to Upload File: /opt/emc/vproxy/runtime/tmp/vproxyd/
plugin/search/e6c356a1-fbaf-4231-9f6f-a0166b74909a/<search
node>-e081fdea-3599-4a6c-abc4-1b5487cb9a32-e523a94c-2d01-5234-ab3c-
7771cfab3c58-7f16bcbb72d7b49ea073356f0d7388ac08461827.db.zip to
https://<search node>:14251/upload, Error sending data chunk. Post
https://<search node>:14251/upload: x509: certificate signed by unknown authority
(possibly because of "crypto/rsa: verification error" while trying to verify candidate
authority certificate "PPDM Root CA ID-d5ec56b8-69ec-4183-9c94-7c0230408765"
```

- Search Engine ノード, Search Engine node(`/opt/emc/search/logs/rest-engine/*.log`)内の REST エンジン ログを確認し、証明書の検証エラーを探す。
- UI または API`<PowerProtect Data Manager>/api/v2/file-instances` を使用して検索を行い、証明書の検証エラーを探す。

各 Search Engine ノード, Search Engine node 内の証明書ファイルを調べて、詳細を調査します。必要に応じて、証明書ファイルを再生成してください。

証明書の検証

証明書が有効で破損していないことを確認するには、この手順を使用してください。

1. 関連するすべてのノード（Search Engine ノード, Search Engine node、PowerProtect Data Manager、VM Direct ノード）の `rootca.pem` ファイルが同じであることを確認します。

   メモ: `rootca.pem` というファイル名はノードによって次のように異なります。

   - PowerProtect Data Manager：`/etc/ssl/certificates/rootca/rootca.pem`
   - Search Engine ノード, Search Engine node：`/var/lib/dellemc/vmboot/trust/thumbprint`
   - VM Direct：`/var/lib/dellemc/vmboot/trust/thumbprint`

2. 次の OpenSSL コマンドを実行して、root 証明書ファイルが破損していたり、無効になっていたりしないかを確認します。 `openssl verify <rootca.pem>`

   レスポンス：

```
/var/lib/dellemc/vmboot/trust/thumbprint: C = US,
O = DELL Corporation,
CN = PPDM Root CA ID-4c9de850-24ab-42ec-a9a7-6080849d0d24

error 18 at 0 depth lookup:self signed certificate


OK
```

   CN の値が一致していることを確認します。

証明書の検証の失敗

証明書の検証手順が失敗した場合は、Search Engine ノード, Search Engine node または VM Direct ノードで証明書を再作成する必要があります。

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. `infranodemgmt` ユーティリティーで `Get` コマンドを使用して、Search Engine ノード, Search Engine node の FQDN を確認します。
3. 実行 `/usr/local/brs/puppet/scripts/generate_certificates.sh -n -c -b <node FQDN>`

   `<node FQDN>.properties` と呼ばれる`/root` ディレクトリーにプロパティ ファイルが作成されます。

4. 生成された証明書の場所を確認するには、このファイルを開いてください。これらは`/etc/ssl/certificates/<node FQDN>`に配置する必要があります。
5. Search Engine ノード, Search Engine node の認証情報を取得します。手順については、『*PowerProtect Data Manager* セキュリティ構成ガイド』を参照してください。
6. 別の端末から、Search Engine ノード, Search Engine node に SSH 接続します。
7. ディレクトリーを`/var/lib/dellemc/vmboot/trust` に変更して `key`、`cert`、`thumbprint` のファイルを移動します。
8. 次のように PowerProtect Data Manager で生成された証明書ファイルをコピーします。
   - `rootca.pem` 変更後： `thumbprint`
   - `<search node FQDN>key.pem` 変更後： `key`
   - `<search node FQDN>.pem` 変更後： `cert`
9. これらのファイルを`/var/lib/dellemc/vmboot/trust` に貼り付けます。
10. `key`、`cert`、`thumbprint` ファイルの権限を「**0644**」に設定し、これらのファイルの所有権を「**root:app**」に設定します。
11. REST エンジン サービスを再起動して、新しい証明書(`systemctl restart search-rest-engine`)を取得します。
12. REST エンジンのログ ファイル(`/opt/emc/search/logs/rest-engine/rest-engine-daemon-<fqdn>.log`)を確認して、サービスが正常に開始されたことを確認します。

    次のメッセージが表示されていることを確認します。

    ```
    A valid Root CA certificate of backup server was provided during deployment
    ```

その結果、インデックス作成のバックアップが正常に実行され、Search Engine が機能します。

Search Engine クラスターがいっぱい

Search Engine がいっぱいになった場合は、インデックス作成の設定と管理の手順に従って追加のノードを導入できます。

Search Engine の領域が不足しており、追加のノードを導入したくない場合は、次のオプションがあります。

- サービスの無効化
- 有効期限を短縮し、インデックスをより迅速に削除
- インデックスの手動削除

サービスを無効にするには、次のステップを実行します。

1. PowerProtect Data Manager UI から、[Infrastructure] > [Search Engine] の順に選択します。
2. クラスターを選択し、[クラスターの構成] をクリックします。
3. [[検索クラスターの構成]] ダイアログ ボックスで、[インデックス作成検索] ボタンをオフに切り替え、[保存] をクリックします。
   メモ: この設定は、検索クラスター内のすべての保護ポリシーに含まれるすべてのインデックスに適用されます。

インデックスを早く削除するために有効期限を短くするには、次のステップを実行します。

1. PowerProtect Data Manager UI から、[Infrastructure] > [Search Engine] の順に選択します。
2. クラスターを選択し、[クラスターの構成] をクリックします。
3. [[検索クラスターの構成]] ダイアログ ボックスで、[検索インデックスの有効期限] を変更し、[保存] をクリックします。有効期限を決定するための推奨される計算式は次のとおりです。`Delete Index when Today = Backup-Date + Expiration Days + 1 day`。つまり、バックアップの有効期限の 1 日後とします。
   メモ: この設定は、Search Engine 内のすべての保護ポリシーに含まれるすべてのインデックスに適用されます。

インデックスを手動で削除するには、次のステップを実行します。

1. SSH を使用して Search Engine にログ インします。
2. 次の形式を使用して、クラスターのスナップショットを作成します。

```
        {
            Command:  "APP_SNAPSHOT",
            Title:    "Initiate Index/Search Cluster Snapshot Process",
            AsyncCmd: false,
            Properties: {
                "Name": {
                    Description: "Used to uniquely identify a particular snapshot",
                    Type:        STRING
                },
                "Action": {
                    Description: "Action to perform, 'Create', 'Delete', 'Restore' or 'Canc
```

```
el' a Snapshot",
                    Type:        STRING
                },
                "NFSHost": {
                    Description: "NFS Host serving snapshot backup area.",
                    Type:        STRING
                },
                "NFSExport": {
                    Description: "NFS Export path to mount too.",
                    Type:        STRING
                },
                "NFSDirPath": {
                    Description: "NFS directory path to write too.",
                    Type:        STRING
                }
            }
        }
```

例：

```
{
    "Command": "APP_SNAPSHOT",
    "Title": "",
    "AsyncCmd": false,
    "Properties": {
        "Action": {
            "Description": "",
            "Required": false,
            "Type": "string",
            "IsArray": false,
            "Value": "Create",
            "Default": null
        },
        "Name": {
            "Description": "",
            "Required": false,
            "Type": "string",
            "IsArray": false,
            "Value": "DataManager_Catalog_Cluster_snapshot_2019-10-16-12-57-16",
            "Default": null
        },
        "NFSHost": {
            "Value": "10.25.87.88"
        },
        "NFSExport": {
            "Value": "/mnt/shared"
        },
        "NFSDirPath": {
            "Value": ""
        }
    }
}
```

3. インデックスは、保護ポリシーまたは資産ごとに削除することができます。JSON コマンドが/home/admin/remove-plc.json に保存されている場合は、./searchmgmt -I /home/admin/remove-plc.json コマンドを実行します。
   - 保護ポリシーごとにインデックスを削除するには、次の形式を使用します。

```
{
            "Command": "APP_REMOVE_ITEMS",
            "AsyncCmd": false,
            "Properties": {
                        "Action": {
                                    "Description": "Action to perform, 'AssetDelete',
'PLCDelete'",
                                    "Required": true,
                                    "Value": "PLCDelete",
                        }
                        "PLCID": {
                                    "Description": "PLC ID of item(s) to delete.",
                                    "Required": true,
                                    "Value": "7676d753-b57e-a572-6daf-33689933456d",
```

```
                        }
            }
}
```

- 資産タイプごとにインデックスを削除するには、次の形式を使用します。

```
{
            "Command": "APP_REMOVE_ITEMS",
            "AsyncCmd": false,
            "Properties": {
                        "Action": {
                                    "Description": "Action to perform, 'AssetDelete',
'PLCDelete'",
                                    "Required": true,
                                    "Value": "AssetDelete",
                        },
                        "AssetID": {
                                    "Description": "Optional, Asset ID of item(s) to
delete.",
                                    "Required": false,
                                    "Value": "503dd753-b57e-a572-6daf-44680033755f",
                        },
                        "PLCID": {
                                    "Description": "PLC ID of item(s) to delete.",
                                    "Required": true,
                                    "Value": "7676d753-b57e-a572-6daf-33689933456d",
                        }
            }
}
```

メモ:

- これらの手順の実行完了にかかる時間は、削除されるバックアップ コピーの資産インデックスの数によって異なります。
- この手順は、クラスターの通常の操作には影響しません。

ロックされた Search Engine ノード, Search Engine node のトラブルシューティング

PowerProtect Data Manager セキュリティ構成ガイドには、パスワード管理ポリシーを含む、Search Engine ノード, Search Engine node のユーザー アカウントと認証情報に関する情報が記載されています。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 回失敗した場合に、管理者ユーザー アカウントをロックす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ノードにアクセスしようとすると、アカウントがロックされたままになる時間が長くなります。

Search Engine ノード, Search Engine node がロックされる理由には、次のようなものが考えられます。

- ユーザーまたはプログラムが、Search Engine ノード, Search Engine node への SSH 接続に 3 回失敗した。
- 間違った管理者の認証情報を使用して Search Engine ノード, Search Engine node へのログ インを試行してモニタリング ソフトウェアを実行している。
- vCenter Server 内の仮想マシンに対して侵入テストを実行している。

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 システムはノードの正常性ステータスの取得など、各ノードでの操作を実行できます。アカウントがロックされている場合、ノードの正常性ステータスは「失敗」とレポートされます。クラスター内のいずれかのノードが失敗した状態になると、クラスター全体が使用不可になります。そうなると、クラスターは、インデックス作成や検索操作を実行できません。

[解決策]

この問題を回避するには、Search Engine ノード, Search Engine node 管理者の認証情報をリセットします。認証情報をリセットする前に、管理者アカウントがロックされている理由を確認します。

Search Engine ノード, Search Engine node の root 認証情報を取得します。次に、Search Engine ノード, Search Engine node 管理者の認証情報をリセットします。手順については、『*PowerProtect Data Manager* セキュリティ構成ガイド』を参照してください。

5

資産の管理

トピック：

資産のソース、資産、ストレージについて

PowerProtect Data Manager では、資産は PowerProtect Data Manager が保護する基本単位です。資産ソースとは、PowerProtect Data Manager で資産を管理し、資産のバックアップ コピーが保存されている保護ストレージと通信するために使用されるメカニズムを指しています。

PowerProtect Data Manager では、保護ストレージ システムを制御するためのストレージおよびプログラム インターフェイスとして PowerProtect DD Management Center (DDMC)がサポートされています。

サポートされている資産ソース

資産ソースには、vCenter Server、Kubernetes クラスター、ネットワーク接続型ストレージ(NAS)アプライアンスまたは共有、アプリケーション ホスト、SMIS Server、ストレージ アレイ、Cloud Snapshot Manager テナントがあります。資産には、仮想マシン、Kubernetes ネームスペース、永続ボリューム要求(PVC)、NAS アプライアンスまたは共有資産、Microsoft Exchange Server データベース、Microsoft SQL Server データベース、Oracle データベース、SAP HANA データベース、ファイル システム、ストレージ グループ、PowerStore ブロック ボリュームなどがあります。

サポートされている資産言語

PowerProtect Data Manager は、オペレーティング システムでホストされている複数の言語のデータの保護をサポートします。詳細については、E-Lab Navigator を参照してください。

資産ソースを追加するための前提条件

資産ソースを追加する前に、PowerProtect Data Manager ユーザー インターフェイス内でソースを有効にする必要があります。

［Assets］ウィンドウでは、［Export All］機能を使用して資産レコードのエクスポートを行うことができます。

［Asset Sources］ウィンドウに IPv6 情報が表示されない

［Asset Sources］ウィンドウには IPv6 情報が表示されません。資産で使用されているのが IPv6 のみの場合は、［IPV4］列に空白のエントリーが表示されます。IPv6 のみの資産を選択するには、［Name］列を参照してください。

資産名またはストレージ名でサポートされる最大文字数は 25 文字

PowerProtect Data Manager は、25 文字を超える資産名またはストレージ名をサポートしません。

注意: この最大値を超えると、保護ポリシーを構成できません。

その他の資産ソースについて

PowerProtect Data Manager では、vCenter Server の資産ソースに加えて、その他の資産タイプを保護するために他の資産ソースを有効にするオプションを提供しています。

『*PowerProtect Data Manager* 管理者ガイド』には、Kubernetes クラスターまたはエージェント資産ソース管理の手順は記載されていません。詳細については、PowerProtect Data Manager のオンライン ヘルプ、または個々の Kubernetes およびエージェントのユーザー ガイドを参照してください。

メモ: エージェント ユーザー ガイドに従ってエージェントをインストールする場合は、インストール ディレクトリーのドライブまたはパーティションに十分な空き領域があることを確認してください。

次の他の資産ソースがサポートされています：

File System agent

File System agent が PowerProtect Data Manager UI で承認され、登録されると、PowerProtect Data Manager はエージェントと統合され、アプリケーション管理者は、ファイル システムホスト上のデータの保護とリカバリーを行い、保護ポリシーに対するバックアップ コンプライアンスを確認し、監視することができます。

Kubernetes クラスター

Kubernetes クラスター資産ソースを追加して PowerProtect Data ManagerUI に登録すると、Kubernetes または Tanzu Kubernetes クラスター上の PVC とネームスペース データの保護が PowerProtect Data Manager で有効になります。

NAS エージェント

NAS 資産ソースが追加され PowerProtect Data ManagerUI に登録されると、PowerProtect Data Manager により NAS 資産の保護が有効になります。

Microsoft application agent for Microsoft Exchange Server

Microsoft Application Agent が PowerProtect Data Manager UI で承認され、登録されると、PowerProtect Data Manager はエージェントと統合され、アプリケーション管理者は、アプリケーション ホスト上の Microsoft Exchange Server アプリケーション データの保護とリカバリーを行い、保護ポリシーに対するバックアップ コンプライアンスを確認し、監視することができます。

Microsoft application agent for Microsoft SQL Server

Microsoft Application Agent が PowerProtect Data Manager UI で承認され、登録されると、PowerProtect Data Manager はエージェントと統合され、アプリケーション管理者は、アプリケーション ホスト上の Microsoft SQL Server アプリケーション データの保護とリカバリーを行い、保護ポリシーに対するバックアップ コンプライアンスを確認し、監視することができます。

Oracle RMAN エージェント

Oracle RMAN エージェントが PowerProtect Data Manager UI で承認され、登録されると、PowerProtect Data Manager はエージェントと統合され、アプリケーション管理者は、アプリケーション ホスト上の Oracle アプリケーション データの保護とリカバリーを行い、保護ポリシーに対するバックアップ コンプライアンスを確認し、監視することができます。

SAP HANA エージェント

SAP HANA エージェントが PowerProtect Data Manager UI で承認され、登録されると、PowerProtect Data Manager はエージェントと統合され、アプリケーション管理者は、アプリケーション ホスト上の SAP HANA アプリケーション データの保護とリカバリーを行い、保護ポリシーに対するバックアップ コンプライアンスを確認し、監視することができます。

ストレージ データ管理用 Storage Direct エージェント

ストレージ データ管理は、スナップショット バックアップ テクノロジーを使用してストレージ グループのデータをアレイから DD システムに移動することにより、VMAX と PowerMax のストレージ アレイ上のデータを保護します。Storage Direct エージェントが PowerProtect Data Manager UI で承認され、登録され、DD システムと SMIS サーバーが追加され、検出されると、Storage Direct エージェントを使用して、ストレージ アレイ内のストレージ グループを検出し、バックアップ/リカバリー操作のために保護されていないストレージ グループを保護ポリシーに割り当てることができます。

ストレージ アレイ

PowerProtect Data Manager では、Dell PowerStore との統合のために、ストレージ アレイ上のデータを保護するために一元的なバックアップ/リストア操作を実行できます。ストレージ アレイ資産ソースが追加され、PowerProtect Data Manager UI で検出されると、PowerProtect Data Manager によりブロック ボリューム資産の保護が有効になります。

資産ソースを検出するための前提条件

資産ソースを検出する前に、次の要件を確認します。

- PowerProtect Data Manager が環境内に導入され、構成されていることを確認します。詳細については、『PowerProtect Data Manager 導入ガイド』を参照してください。
- 管理者ロールを持つユーザーとしてにログ インします。管理者資産ソースを管理できるのは、ロールのみです。
- 新しいシステムの場合は、保護する資産のタイプで 1 個または複数の資産ソースを有効化します。 資産ソースの有効化 で詳細を参照してください。
- NTP サーバとすべての資産ソースを構成します。
- Transparent Snapshots Data Mover (TSDM)保護メカニズムを使用するように構成される仮想マシンから、管理対象スナップショットをすべて削除します。
- Microsoft SQL Server アプリケーションを登録する前に、DD システムが正常に検出されていることを確認してください。
- アプリケーション エージェントとファイル システムの資産ソースを検出するには、次の手順を実行します。
  - バックアップの検出が確実になるように、アプリケーション、ファイル システムホスト、PowerProtect Data Manager のすべての時刻が、ローカル NTP サーバーと同期していることを確認します。
  - アプリケーション ホスト、ファイル システムホスト、PowerProtect Data Manager ネットワークが相互に参照および解決できることを確認します。
  - アプリケーションとファイル システムホストでポート 7,000 が開いていることを確認します。
- vCenter Server 資産ソースが検出されると、次のものが除外されます。
  - ステータスが［Inaccessible］、［Invalid］、または［Orphaned］の仮想マシン。
  - 仮想マシン テンプレート。
  - RecoverPoint for Virtual Machines（vRPA コピーとも呼ばれる）によって作成されたシャドーまたはスタンバイ仮想マシン。
  - vSphere クラスター サービス(vCLS)仮想マシン。

    メモ: vCLS によって作成された仮想マシンは VMware によって管理されるため、PowerProtect Data Manager による保護は必要ありません。コンテナの一部として選択されていても、保護から自動的に除外されます。`vmdm-discovery.log` には、保護から除外された vCLS 仮想マシンのリストが記載されます。

vCenter 検出を実行する前に s、検出するすべての仮想マシンのステータスを確認します。

不透明なネットワークでの資産ソースの検出

PowerProtect Data Manager は、不透明なネットワークに配置された vCenter サーバーの検出をサポートしています。

VMware は、ネットワークに配置されている vCenter Server が NSX または vSphere によって管理されていない場合、そのネットワークを不透明と見なします。不透明なネットワーク上の vCenter サーバーを検出し、その資産を NSX または vSphere によって管理される vCenter サーバーと同様に保護できます。

GCVE 環境での資産ソースの検出

GCVE 環境では、検出に関する特別な考慮事項があります。GCVE に配置された vCenter Server に追加の権限がない限り、検出は失敗します。

GCVE に配置された vCenter Server の次の権限を確認します。

- *GVE.LOCAL\CloudOwner* ユーザーは、vCenter レベルで *Cloud-Owner-Role* ロールにマッピングされます。

- *GVE.LOCAL\CloudOwner* から *Cloud-Owner-Role* へのマッピングは、vSphere オブジェクト階層内の下位レベルのコンテナ オブジェクトに限定されません。

アプリケーション資産ソースの完全な検出

一部のアプリケーション資産が検出されない場合は、PowerProtect Data Manager UI のオンデマンド検出機能を使用して、アプリケーション資産ソースの包括的な検出をすぐに実行できます。

包括的な検出は、次のアプリケーション資産ソースで使用できます。

- Microsoft SQL Server
- Microsoft Exchange Server
- Oracle
- SAP HANA
- ファイル システム

アプリケーション資産ソースの包括的な検出を開始するには、次の手順を実行します。

1. ［Infrastructure］ > ［Asset Sources］を選択します。
2. アプリケーション資産ソースを選択し、［Discover］をクリックします。
3. ［Initiate a full discovery］オプションを選択し、［Yes］をクリックします。

資産ソースの有効化

資産ソースは、PowerProtect Data Manager 内で有効にした後、資産ソースを追加および登録して資産を保護する必要があります。

このタスクについて

管理者資産ソースを管理できるのは、ロールのみです。

特定の状況では、複数の資産ソースを有効化する必要があります。例えば、Tanzu Kubernetes ゲスト クラスターを保護するために、vCenter Server および Kubernetes クラスターの資産ソースを有効にする必要があります。

次のような他の状況では、資産ソースを有効にする必要がありません。

- アプリケーション エージェントや、ファイル システムおよび Storage Direct などの他のエージェントでは、エージェント ホストを登録して承認すると、資産ソースが自動的に有効になります。例えば、Oracle 資産ソースを有効にしていないものの、API または PowerProtect Data Manager ユーザー インターフェイスを使用してアプリケーション ホストを登録した場合、PowerProtect Data Manager によって Oracle 資産ソースが自動的に有効になります。
- PowerProtect Data Manager の最新バージョンにそれより前のリリースからアップデートすると、それまで有効になっていたすべての資産ソースが PowerProtect Data Manager ユーザー インターフェイスに表示されます。ただし、新規導入の場合、デフォルトでは資産ソースが有効になりません。

手順

1. PowerProtect Data Manager ユーザー インターフェイスから、［Infrastructure］ > ［Asset Sources］の順に選択してから、［+］をクリックすると、［New Asset Source］タブが表示されます。
2. 追加する資産ソースのペインで、［ソースの有効化］をクリックします。
［[資産ソース]］ウィンドウのアップデートが行われ、新規資産ソースのタブが表示されます。

タスクの結果

これで、PowerProtect Data Manager で使用する資産ソースを追加または承認できます。vCenter Server、Kubernetes クラスター、SMIS Server、PowerProtect Cloud Snapshot Manager テナントの場合は、このウィンドウで該当するタブを選択して、［Add］をクリックします。アプリケーション ホストの場合は、［Infrastructure］ > ［Application Agents］の順に選択し、必要に応じて［Add］または［Approve］をクリックします。

メモ: Cloud Snapshot Manager テナントを PowerProtect Data Manager に追加してその稼働状態、アラート、および保護ジョブ、リカバリー ジョブ、システム ジョブのステータスを表示させることはできますが、PowerProtect Data Manager から資産の保護を管理することはできません。資産の保護を管理するには、Cloud Snapshot Manager を使用します。詳細については、*PowerProtect Cloud Snapshot Manager* オンライン ヘルプを参照してください。

資産ソースの無効化

不要になった資産ソースを有効にしていて、ホストを PowerProtect Data Manager に登録していない場合は、次の手順を実行して資産ソースを無効にします。

このタスクについて

メモ: 1 個または複数のソースが登録されたままの場合や、ソース資産のバックアップ コピーが存在する場合は、資産ソースを無効にできません。例えば、vCenter Server を登録して、vCenter Server 仮想マシンのポリシー バックアップを作成してある場合、vCenter Server の資産ソースを無効にできません。ただし、vCenter Server を登録してから、バックアップを一切作成していない状態でそれを削除する場合は、資産ソースを無効にできます。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［資産ソース］の順に選択し、無効にする資産ソースのタブを選択します。登録されているホストが検出されない場合は、赤い［無効化］ボタンが表示されます。
2. ［無効化］をクリックします。

タスクの結果

PowerProtect Data Manager によってこの資産ソースのタブが削除されます。

資産ソースの削除

不要になった資産ソースを削除する場合は、次の手順を実行して、PowerProtect Data Manager UI で資産ソースを削除します。

このタスクについて

資産ソースを管理できるのは、管理者ロールのみです。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Asset Sources］の順に選択し、削除する資産ソース タイプのタブを選択します。
2. 資産ソース リストで資産ソース名を選択し、［Delete］をクリックします。
3. 表示された警告プロンプトで、［Continue］をクリックします。
資産ソースがリストから削除されます。

タスクの結果

PowerProtect Data Manager は、［Asset Sources］ウィンドウで指定された資産ソースを削除します。

vCenter Server を除くすべての資産ソースでは、保護ポリシーによって保護されているすべての関連資産が保護ポリシーから削除され、それらのステータスが `deleted` に変更されます。これらの資産は、関連するすべてのバックアップ コピーが削除された後に、日次 PowerProtect Data Manager クリーンアップの一環として自動的に削除されます。これらの資産は手動で削除することもできます。PowerProtect Data Manager から資産を削除する方法の詳細については、『*PowerProtect Data Manager* 管理者ガイド』を参照してください。

資産ソースからの資産のコピーは保持されます（削除されません）。必要に応じて、コピー ページからコピーを削除できます。

Cloud Snapshot Manager テナントの追加

PowerProtect Data Manager を使用して Cloud Snapshot Manager テナントの資産ソースを有効にしてから、PowerProtect Data Manager の［Asset Sources］ウィンドウを使用して、Cloud Snapshot Manager テナントを PowerProtect Data Manager 環境に追加します。

統合済みの PowerProtect Data Manager ダッシュボードで Cloud Snapshot Manager のジョブ、アラート、レポートを表示する場合は、Cloud Snapshot Manager テナントを追加する必要があります。

Cloud Snapshot Manager テナントの追加

PowerProtect Data Manager UI で資産ソースとして Cloud Snapshot Manager テナントを追加するには、次の手順を実行します。

前提条件

- 資産ソースが有効になっていることを確認します。

  資産ソースの有効化 で手順を参照してください。
- 管理者ロールを持つユーザーとしてにログ インします。管理者資産ソースを管理できるのは、ロールのみです。
- PowerProtect Data Manager サーバーにはインターネット アクセスがあり、*https://ssgosge.emc.com* にアクセスできます。

  メモ: 通常のオペレーション中にこのアクセスが削除されても、既存の Cloud Snapshot Manager の情報は引き続き［Dashboard］ウィンドウに表示されますが、インターネット アクセスが回復するまではアップデートされません。
- この手順を実行するには、Cloud Snapshot Manager に固有の値を入力する必要があります。詳細については、『*PowerProtect Cloud Snapshot Manager* オンライン ヘルプ』を参照してください。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Asset Sources］の順に選択します。

   ［Asset Sources］ウィンドウが表示されます。
2. ［Cloud Snapshot Manager］タブを選択します。
3. ［Add］をクリックします。

   ［Add Cloud Snapshot Manager Account Details］ダイアログが表示されます。
4. ［Name］フィールドに、Cloud Snapshot Manager テナントの記述名を入力します。
5. ［Tenant ID］フィールドに、Cloud Snapshot Manager のテナント ID を入力します。
6. ［Cloud Snapshot Manager Credentials］の横にあるドロップダウン コントロールをクリックして、［Add Credentials］をクリックします。
   a. ［Name］フィールドに、Cloud Snapshot Manager のテナント認証情報の名前を入力します。
   b. ［Client ID］フィールドに、Cloud Snapshot Manager のテナント ID を入力します。
   c. ［Client Secret］フィールドに、Cloud Snapshot Manager のテナント シークレットを入力します。
   d. ［Save］をクリックします。
7. ［Save］をクリックします。

タスクの結果

PowerProtect Data Manager では、保護された Cloud Snapshot Manager リソースに関連するジョブ、アラート、レポートを表示できます。

6

保護ポリシーの管理

トピック：

保護ポリシー

保護ポリシーでは、特定の期間に適用される目標のセットを定義します。これらの目標は、指定したデータのビジネス要件を満たす構成、アクティブな保護、コピー データ管理の操作を促進します。それぞれのポリシー タイプには、ユーザー目標の独自の設定があります。

保護ポリシーの作成または編集ができるのは、管理者ロールのみです。

次の資産タイプの保護ポリシーを作成することができます。

- VMware 仮想マシン
- Microsoft Exchange Server データベース
- Microsoft SQL Server データベース
- Oracle Database
- SAP HANA データベース
- ファイル システム
- Kubernetes クラスター
- ストレージ グループ
- ブロック ボリューム
- NAS（ネットワーク接続型ストレージ）

各ポリシー タイプについては、それぞれのユーザー ガイドを参照してください。

［Protection Policies］ウィンドウでは、［Export All］機能を使用して保護ポリシー データのエクスポートを行うことができます。

保護ポリシーを作成する前に

保護ポリシーを作成する前に、次のベスト プラクティスを考慮してください。

- 一度に 1 個のポリシーで保護できる資産は 1 個だけです。保護ルールは、手動でポリシーに追加された資産を別のポリシーに自動的に移動しません。

  メモ: Microsoft SQL Server が仮想マシンにインストールされている場合は、Microsoft SQL Server エージェントベースのバックアップに影響を与えることなく、アプリケーションコンシステントなバックアップを使用して Microsoft SQL Server データベースを保護できます。
- ポリシーを作成する場合は、ポリシー内のデータベース資産の数を 500 未満に制限し、ポリシーのレプリケーション開始時間をずらします。これらのアクションにより、レプリケーション障害の発生可能性を回避します。
- 保護ポリシーにレプリケーションを追加する前に、レプリケーションの場所としてリモート保護ストレージが追加されていることを確認します。

  保護ストレージの追加 に、リモート保護ストレージを追加する手順の詳細が示されています。
- 週次、月次、年次のバックアップをスケジュールする前に、PowerProtect Data Manager のタイム ゾーンがローカル タイム ゾーンに設定されていることを確認します。

バックアップ テクノロジーの理解

PowerProtect Data Manager は、フル バックアップまたはシンセティックフル バックアップの実行時にブロックベースのバックアップ テクノロジーを使用します。File System Agent は、ボリュームまたはディスクをスキャンし、割り当てられているファイル システム上のすべてのブロックをバック アップします。変更されたデータのみがバック アップされる場合、ブロックベースのバックアップでは更新ブロック追跡が使用されます。

ブロックベースのバックアップは、次の機能をサポートしています。

- 予測可能バックアップ ウィンドウを備えたハイパフォーマンス バックアップ
- PowerProtect DD によって使用される重複排除ファイル システムの効率的なバックアップ
- ファイル システムとしてのバックアップのマウント
- スパースファイル バックアップのサポート

PowerProtect Data Manager は、特定のファイルまたはディレクトリーのセットをバック アップする際に、従来のファイルベースのバックアップ テクノロジーを使用します。これらのバックアップ中に、ファイル システムのディレクトリー構造全体がトラバースされます。これらのバックアップは、ブロックベースのバックアップよりも完了に時間がかかります。

メモ: 除外フィルターを保護ポリシーに適用すると、ファイルベースのバックアップの際に、それが自動的に反映されます。大容量ファイル システムをバック アップする場合は、代わりにすべてのデータをバック アップする方が効率的な場合があります。または、フィルタリング対象の資産を別の保護ポリシーに移動して、フィルター処理されていない残りの資産がブロックベースのバックアップを使用できるようにします。

バックアップ用語の理解とバックアップ頻度の管理

保護ポリシーでバックアップをスケジュール設定する場合は、次の点に注意してください。

- 保護ポリシー タイプごとに異なる用語を使用して、使用可能なバックアップ レベルを説明している場合があります。この用語は、保護ポリシー タイプ間で異なるだけでなく、従来の用語とも異なることがあります。
- 障害の原因となる高い CPU 使用率を回避するには、推奨されている頻度以上にバックアップをスケジュール設定しないようにします。

バックアップ頻度を管理するためのさまざまなバックアップ レベルを理解するには、次の表を参照します。

表 24. バックアップの用語と頻度

保護ポリシーのタイプ	使用可能なバックアップ レベル	説明	相当する従来の用語	推奨される最小バックアップ間隔
VMware アプリケーション対応	フル	すべてのデータがバック アップされます。	フル	月次
	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に変更されたデータのみがバック アップされます。これらの変更を最後のシンセティックフル バックアップまたはフル バックアップとマージする操作では、ストレージにフル バックアップが生成されます。ネットワーク経由でコピーが	差分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間

表 24. バックアップの用語と頻度 （続き）

保護ポリシーのタイプ	使用可能なバックアップ レベル	説明	相当する従来の用語	推奨される最小バックアップ間隔
		行われるのは変更されたブロックのみですが、その結果はストレージ内のフル バックアップのままになります。		
	ログ	トランザクション ログがバック アップされます。		30 分
VMware クラッシュコンシステント	フル	すべてのデータがバック アップされます。	フル	月次
	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に変更されたデータのみがバック アップされます。これらの変更を最後のシンセティックフル バックアップまたはフル バックアップとマージする操作では、ストレージにフル バックアップが生成されます。ネットワーク経由でコピーが行われるのは変更されたブロックのみですが、その結果はストレージ内のフル バックアップのままになります。	差分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間
Kubernetes クラッシュコンシステント	フル	ネームスペース メタデータと永続ボリュームがバック アップされます。	フル	日単位
	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に VMware のファーストクラス ディスク上の永続ボリュームに対して変更されたデータのみがバック アップされます。ネームスペース メタデータとその他のすべての永続ボリュームが、フル バック アップされます。ネットワーク経由でのコピーが行われていないデータがある場合でも、結果はストレージのフル バックアップのままになります。	フル バックアップと差分バックアップを組み合わせた操作が実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間
ファイル システム集中型	フル	すべてのデータがバック アップされます。	フル	月次
	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に変更されたデータのみがバック アップされます。これらの変更を最後のシンセティックフル バックアップまたはフル バックアップとマージする操作では、ストレージにフル バックアップが生成されます。ネットワーク経由でコピーが行われるのは変更されたブロックのみですが、その結果はストレージ内のフル バックアップのままになります。	差分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間
Microsoft Exchange Server 集中型	フル	すべてのデータがバック アップされます。	フル	週次
	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に変更されたデータのみがバック アップされます。これらの変更を最後のシンセティックフル バックアップまたはフル バックアップとマージする操作では、ストレージにフル バックアップが生成され	差分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間

表 24. バックアップの用語と頻度 （続き）

保護ポリシーのタイプ	使用可能なバックアップ レベル	説明	相当する従来の用語	推奨される最小バックアップ間隔
		ます。ネットワーク経由でコピーが行われるのは変更されたブロックのみですが、その結果はストレージ内のフル バックアップのままになります。		
Microsoft SQL Server 集約型	フル	すべてのデータがバック アップされます。	フル	日単位
	差分	前回の差分バックアップ以降（他に差分バックアップが存在しない場合は前回のフル バックアップ以降）に変更されたデータのみバック アップします。	差分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間
	ログ	トランザクション ログがバック アップされます。		30 分
ネットワーク接続型ストレージ	フル	すべてのデータがバック アップされます。	フル	日単位 **メモ:** PowerProtect Data Manager 19.12 にアップデートした後、フル バックアップを実行することをお勧めします。
	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に変更されたデータのみがバック アップされます。これらの変更を最後のシンセティックフル バックアップまたはフル バックアップとマージする操作では、ストレージにフル バックアップが生成されます。ネットワーク経由でコピーされるのは変更されたファイルのみですが、その結果はストレージ内のフル バックアップのままになります。	増分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	日単位
Oracle 集約型	フル	すべてのデータがバック アップされます。	フル	日単位
	増分累積	前回のレベル 0 フル バックアップ以降に変更されたデータのみバック アップします。	差分	12 時間
	増分差分	前回の増分差分バックアップ以降（他に増分差分バックアップが存在しない場合は前回のフル バックアップ以降）に変更されたデータのみバック アップします。	増分	6 時間
	ログ	アーカイブされたログがバック アップされます。		30 分
SAP HANA 集約型	フル	すべてのデータがバック アップされます。	フル	日単位
	差分	前回のフル バックアップ以降に変更されたデータのみバック アップします。	差分	12 時間
	増分	前回のデータ バックアップ以降に変更されたデータのみです。前回のデータ バックアップは、増分バックアップ、差分バックアップ、フル バックアップの場合があります。	増分	6 時間

表 24. バックアップの用語と頻度 （続き）

保護ポリシーのタイプ	使用可能なバックアップ レベル	説明	相当する従来の用語	推奨される最小バックアップ間隔
VMAX ストレージ グループ集約型 **メモ:** PowerProtect Data Manager アプライアンスは対象外です。	シンセティック フル	最後のシンセティックフル バックアップまたはフル バックアップ以降に変更されたデータのみがバック アップされます。これらの変更を最後のシンセティックフル バックアップまたはフル バックアップとマージする操作では、ストレージにフル バックアップが生成されます。ネットワーク経由でコピーが行われるのは変更されたブロックのみですが、その結果はストレージ内のフル バックアップのままになります。	差分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	12 時間
ブロック ボリューム	シンセティック フル	前回のシンセティックフル バックアップまたはフル バックアップ以降に変更されたブロックのみバック アップした後、ストレージ内のフル バックアップを作成するために、これらの変更を最後のシンセティックフル バックアップまたはフル バックアップにマージする操作を行います。ネットワーク経由でコピーが行われるのは変更されたブロックのみですが、その結果はストレージ内のフル バックアップのままになります。	増分バックアップが実行され、その後、ストレージ内のフル バックアップを作成するマージ操作が行われます。	6 時間
	スナップショット	ボリュームまたはボリューム グループの状態、および含まれるすべてのファイルとデータを特定の時点で保存します。破損したデータまたは誤って削除されたデータのリカバリーがスナップショットによって可能になります。スナップショットを使用して、ボリュームまたはボリューム グループを前の状態にリストアできます。		15 分

メモ: 状況によっては、シンセティックフル バックアップがスケジュール設定された場合でも、フル バックアップが実行されることがあります。フル バックアップの考えられる理由は次のとおりです。

- 既存のフル バックアップが存在しない。
- ボリュームのサイズが変更された。
- ファイル パスが変更された。
- 資産ホストが再起動された。

ログ、差分、累積増分、増分差分、増分の各バックアップのバックアップ頻度は、フル バックアップまたはシンセティックフル バックアップのバックアップ頻度より早くすることはできません。無効なバックアップ頻度を使用する保護ポリシーを追加または編集しようとした場合、PowerProtect Data Manager によってその保護ポリシーは保存されません。保存期間が異なるフル バックアップまたはシンセティックフル バックアップを追加してスケジュール設定することで要件を満たし、保護ポリシーのバックアップ頻度を早めることができます。

レプリケーション トリガー

PowerProtect Data Manager では、プライマリー バックアップとは別に、保護ポリシー レプリケーション目的のオーケストレーションが行われます。ポリシーにレプリケーション目的を追加する場合は、使用可能なトリガーのいずれかを選択します。

デフォルトのレプリケーション トリガーは、繰り返し期間、開始時間、終了時間を設定して定義するスケジュール ウィンドウです。レプリケーションは、定められたウィンドウの間で実行されます。例えば、毎日午後 8 時から午前 12 時までなどです。

また、スケジュール設定されている場合や手動の場合のどちらでも、関連するプライマリー バックアップが完了した直後にレプリケーションを開始させることができます。プライマリー バックアップの開始時には、PowerProtect Data Manager によって、関連するレプリケーション ジョブが生成されます。このジョブは、保護ジョブが終了するまでキューに残ります。バックアップが失敗するか、例外付きで完了した場合、関連するレプリケーション ジョブがスキップされます。保護ジョブが再開すると、関連するレプリケーション ジョブが再びキューに登録されます。

レプリケーション目標を作成する場合は、スケジュール設定されたレプリケーションまたはバックアップ完了後のレプリケーションのいずれかを指定できます。これは、一元化された保護ポリシーとセルフサービス保護ポリシーの両方に適用されます。

メモ: バックアップ完了後にレプリケーションを実行する場合は、アプリケーション エージェントを最新バージョンにアップデートすることをお勧めします。

バックアップのタイプに応じて、バックアップが完了した直後にレプリケーションが実行されるようにするには、次のバージョンが必要です。

- セルフサービス プライマリー バックアップの場合、すべてのアプリケーション エージェントを PowerProtect Data Manager バージョン 19.12 以降にアップデートします。
- 一元的なプライマリー バックアップの場合、すべてのアプリケーション エージェントを PowerProtect Data Manager バージョン 19.11 以降にアップデートします。

特定のバックアップのみをレプリケートする場合は、事前にこれらのバックアップの手動レプリケーションを実行します。

スケジュールを使用することで、ピーク時間外にレプリケーションを行えるため、ネットワーク トラフィックが管理しやすくなります。ただし、大規模なバックアップ セットの場合、レプリケーション スケジュールの開始前にプライマリー バックアップが完了せず、レプリケーション バックログが生成されることがあります。バックアップ完了後のレプリケーションでは、レプリケーション バックログが生成されません。

データ ロスを防ぐために、バックアップ完了後のレプリケーション トリガーによって、プライマリー目的の新しいバックアップとまだレプリケーションが行われていない未処理のバックアップが複製されます。

レプリケーション中の Completed with Exceptions ジョブ ステータス

トリガーされたレプリケーション ジョブの後に、次のようなジョブ ステータス メッセージが表示されることがあります。

```
Completed with Exceptions
ABA0017: plc_linux_rac: Backup was successful for the ORACLE_DATABASE asset ORCLPP on the
host oracle.test.com but the copy metadata information is currently unavailable.

The backup of this asset completed successfully but the copy metadata information has not yet
been discovered by PowerProtect Data Manager. If the 'Replicate immediately upon backup
completion' option is enabled for this protection policy, the replication job for the copy
might appear in 'Unknown' or 'Cancel' state. Once the copy metadata is discovered by
PowerProtect Data Manager, the copy will be replicated.

Review the backup copy details in the View Copies pane of the PowerProtect Data Manager UI
Infrastructure > Assets window to determine when the discovery is complete.
```

このメッセージが表示された場合、レプリケーション バックアップをすぐに使用することはできません。

この問題を解決するには、次の自動検出を待つか、検出を開始してください。

保護ポリシーの追加または編集

PowerProtect Data Manager ユーザー インターフェイスを使用して、資産を保護するための保護ポリシーを追加できます。既存の保護ポリシーの詳細を変更することもできます。

保護ポリシーの追加

保護ポリシーを追加して、次の資産タイプを保護できます。詳細については、該当するドキュメントを参照してください。

表 25. 保護ポリシーの資産タイプ

資産タイプ	ドキュメント名
ファイル システム データ	*PowerProtect Data Manager* ファイル システム ユーザー ガイド
Kubernetes クラスター ネームスペースと PVC	*PowerProtect Data ManagerKubernetes* ユーザー ガイド
Microsoft Exchange Server データベース	*PowerProtect Data ManagerMicrosoft Exchange Server* ユーザー ガイド
Microsoft SQL Server データベース	*PowerProtect Data ManagerMicrosoft SQL Server* ユーザー ガイド

表 25. 保護ポリシーの資産タイプ （続き）

資産タイプ	ドキュメント名
ネットワーク接続型ストレージ (NAS)共有とアプライアンス データ	*PowerProtect Data Manager* ネットワーク接続型ストレージ ユーザー ガイド
Oracle RMAN データベース	*PowerProtect Data ManagerOracle RMAN* ユーザー ガイド
SAP HANA データベース	*PowerProtect Data ManagerSAP HANA* ユーザー ガイド
Storage Direct データ	*PowerProtect Data ManagerStorage Direct* ユーザー ガイド
仮想マシン	*PowerProtect Data Manager* 仮想マシン ユーザー ガイド
ブロック ボリューム	*PowerProtect Data Manager* ストレージ アレイ ユーザー ガイド

保護ポリシーの編集

既存の有効または無効な保護ポリシーに関する次の情報を変更できます。

- ポリシーの名前と説明
- ポリシーに対する資産の追加または削除
- バックアップとレプリケーションのスケジュール

  メモ: 最初に作成されたバックアップ スケジュールを除いて、任意のフル バックアップまたは合成フル バックアップ スケジュールを削除できます。最初に作成されたバックアップ スケジュールは削除できません。
- バックアップの最適化モード
- ネットワーク インターフェイス、ストレージ ターゲット、ストレージ ユニット、保存ロック、サービス レベル アグリーメント(SLA)の設定

保護ポリシーのタイプまたは目的を変更することはできません。これらのアクションに対しては、ポリシーを追加します。ポリシーを編集しても、ストレージ クォータを変更できません。

メモ: 有効または無効なポリシーの変更を保存すると、ほとんどの変更はすぐに反映されます。ただし、無効化されたポリシーのプライマリー バックアップ スケジュールについては、［Disabled］状態では実行されないことから、ポリシーを再度有効にするまで変更が有効になりません。

ポリシーの名前と説明、目的、オプションの変更

次の手順では、既存のポリシーの名前と説明、スケジュールと目的、追加のバックアップ オプションを PowerProtect Data Manager UI で変更する方法について説明します。

前提条件

該当する場合は、仮想ネットワークの構成タスクをすべて完了してから、仮想ネットワークを保護ポリシーに割り当てます。

このタスクについて

メモ: 保護ポリシーを編集して、資産を追加または削除することもできます。ポリシーに資産を追加したり、ポリシーから資産を削除したりするための詳細な手順については、セクション保護ポリシーでの資産の追加または削除を参照してください。

手順

1. 左ナビゲーション ペインで、［Protection］ > ［Protection Policies］の順に選択します。
   ［Protection Policies］ウィンドウが表示されます。
2. 変更する保護ポリシーを選択し、［Edit］をクリックします。
   ［Summary］ページで、［Edit Policy］ウィンドウが開きます。このページから、選択可能な行の横にある［edit］をクリックして、特定のポリシーの詳細を変更できます。
3. ［Name］または［Description］の行で［Edit］をクリックします。
   ［Type］ページが表示されます。

   メモ: 既存のポリシーのタイプや目的は変更できません。
4. ［Objectives］行で、［Edit］をクリックします。

［Objectives］ページが表示されます。このページでは、バックアップ スケジュールの変更、ネットワーク インターフェイス設定の変更、保存ロックの有効化または無効化を行うことができます。

［Primary Backup］行と［Replicate］行では、新しい `Storage Name` を選択してストレージ ターゲットを変更することもできます。ストレージ ターゲットの変更の詳細については、「ストレージ ターゲットの変更」のセクションを参照してください。

5. ［Options］行で、［Edit］をクリックします。
［Options］ページが表示されます。このページでは、バックアップの最適化モード（パフォーマンスや容量など）の変更、バックアップでスワップ ファイルを含むか除外するかどうかの選択、バックアップ中にゲスト ファイル システムを停止するかどうかの選択を行うことができます。

   メモ: 仮想マシンの保護ポリシーでは、Transparent Snapshot Data Mover (TSDM)と VMware vStorage API for Data Protection (VADP)の 2 タイプの保護メカニズムが使用されます。ポリシー オプションをアップデートすると、仮想マシン データの移動に使用される保護メカニズムが変更される場合があります。保護メカニズムが変更されると、新しいフル バックアップが実行され、完了するまでに時間がかかる場合があります。

6. 変更を行った後、［Next］をクリックして変更を保存し、［Summary］ページに戻ります。
7. ［Summary］ページで、［Finish］をクリックします。
情報ダイアログが表示されます。
8. ［OK］をクリックしてダイアログを終了するか、［Go to Jobs］をクリックして［Jobs］ウィンドウを開き、新しい保護ポリシーのバックアップを監視します。

ストレージ ターゲットの変更

ストレージ ターゲットは、保護ストレージ システムと関連するストレージ ユニットで構成されています。各保護ポリシー用に、選択したストレージ ターゲットのエレメントを変更できます。

保護ポリシーのプライマリー バックアップとレプリケーション目的を編集する場合は、次の手順を実行します。

- ［Storage Name］ドロップダウン リストには、現在の保護ストレージ システムが表示されます。ドロップダウン リストには、使用可能なその他の保護ストレージ システムも含まれています。［Add］を選択して、追加の保護ストレージを構成します。
- ［Storage Unit］ドロップダウン リストには、選択した保護ストレージ システム上で PowerProtect Data Manager のターゲットになっているストレージ ユニットが表示されます。このドロップダウン リストから、PowerProtect Data Manager によって制御されている他のストレージ ユニットを選択できます。ストレージ ユニットを作成するには、［New］を選択します。

ストレージ ターゲットを変更する場合は、依存関係を適切に構成します。たとえば、従属の保護ポリシーの目標で、アップデートされたストレージ ターゲットのクラウド プロバイダーを構成します。

メモ: DD 7.4.x 以前のシステムにあり、伸長されている IPv6 形式を使用するように構成されたネットワーク インターフェイスは、検出できません。伸長されている IPv6 形式は、`2620:0000:0170:0597:0000:0000:0001:001a` のようになります。短縮された IPv6 形式は、`2620:0:170:597::1:1a` のようになります。これらのネットワーク インターフェイスを使用するには、IPv4 アドレスまたは短縮された IPv6 アドレスのいずれかを使用するように再構成してから、検出を開始してください。

影響

次に示されている一部資産タイプのプライマリー目的のストレージ ターゲットを変更すると、スケジュール設定された次回のフル バックアップまでバックアップのスキップが発生することがあります。

- アプリケーション対応の VMware 仮想マシン
- SAP HANA
- Oracle RMAN

これらのポリシーでは、手動フル バックアップを実行します。 保護された資産の手動バックアップ で手順を参照してください。

次の資産タイプでは、追加のアクションは不要です。

- クラッシュ整合性のある VMware 仮想マシン
- Kubernetes
- ネットワーク接続型ストレージ（NAS）
- ストレージ グループ
- Microsoft Exchange Server
- Microsoft SQL Server
- ファイル システム

これらの資産タイプでは、次回のバックアップが自動的にフル バックアップになります。

レプリケーション目的では、追加のアクションは不要です。

保護ストレージ

ストレージの管理 に、追加の保護ストレージ システムの構成およびクォータ設定の変更など、保護ストレージの扱いに関する詳細が記載されています。

選択されていて使用可能な保護ストレージ システムのリストを確認する場合は、次の点を考慮してください。

- ポリシーの目標で保護ストレージ システムを共有することは、この構成でデータの可用性が向上しないため推奨されていません。ただし、複数の目的で保護ストレージ システムが共有されている一部の環境では、異なる保存期間を設定したレプリカが必要になることがあります。
- 現在の保護ポリシーで使用するためにライセンスが付与された構成済みの保護ストレージのみがドロップダウン リストに表示されます。
- ストレージ グループ保護ポリシーの保護ストレージ システムを変更することはサポートされていません。

ストレージ ユニット

ストレージ ユニット 適用される制限事項やメンテナンスに関する考慮事項など、ストレージ ユニットの扱いに関する詳細情報が提供されています。

［New］を選択すると、PowerProtect Data Manager によってこの保護ポリシーのストレージ ユニットが作成されます。新しいストレージ ユニット名は、保護ポリシー名と識別子に基づいています。ストレージ ユニット に、クォータ構成を変更するための詳細な手順が記載されています。

また、PowerProtect Data Manager によって制御されている既存のストレージ ユニットを選択することもできます。ドロップダウン リストには、選択した保護ストレージ システムで使用可能なストレージ ユニットが表示されます。スペースの制限によってストレージ ユニット名が短縮されている場合は、リスト エントリーにカーソルを合わせると、ストレージ ユニット名とクォータの完全な情報が表示されます。

ストレージ グループ保護ポリシーのストレージ ターゲットの変更はサポートされていません。

ストレージ ターゲットの再導入

保護ポリシーのストレージ ターゲットを再導入すると、特定の手順に従わない限り、検出後にエントリーが重複します。

［Replication Targets］ウィンドウで再導入したストレージ ターゲットのエントリーが重複しないようにするには、ストレージ ターゲットを PowerProtect Data Manager から削除し、関連するすべての保護ポリシーを削除した後に再導入します。ストレージ ターゲットを再導入した後、再度検出されるまで待ってから、関連する保護ポリシーに追加し直します。

共有保護ストレージへのレプリケーション

外部ワークフローの柔軟性を高め、インフラストラクチャ コストを削減するために、PowerProtect Data Manager では、複数の目的間で保護ストレージを共有できます。

PowerProtect Data Manager 以外のワークフローに対応するには、レプリカごとに異なる保存期間が必要になる場合があります。保存期間は目的レベルで設定されているため、異なる保存期間を構成するには追加のレプリケーション目的が必要です。

ほとんどの場合、追加のレプリケーション目的では、別の保護ストレージ システムに存在するストレージ ユニットがターゲットとなっています。個別の保護ストレージにレプリケートを行うと、データの可用性が向上します。

追加の目的ごとに個別の保護ストレージ システムを必要とせずに、外部ワークフローに対応するため、PowerProtect Data Manager では、同じ保護ストレージ システム上の異なるストレージ ユニットをターゲットに設定できます。コストをさらに削減するため、プライマリー バックアップと同じ場所にある保護ストレージ システムをターゲットに設定できます。このようなケースでは、外部ワークフローによってデータの安全性が向上します。

メモ:

PowerProtect Data Manager では外部ワークフローが認識されないため、同じ保護ストレージ システムを共有する複数の目的でポリシーを構成すると、UI に警告が表示されます。この構成は一般的ではないため、続行前にストレージ ターゲットとユース ケースを確認してください。

また、選択したストレージ ユニットが MTree レプリケーション ワークフローのソースである場合にも、UI に警告が表示されます。このワークフローは、別のアプリケーションに属している可能性があります。続行前に、ストレージ ターゲットを確認してください。これらの通知が表示されるには、DDOS 7.7 以降が必要です。

保護ポリシーでの資産の追加または削除

PowerProtect Data Manager UI で次の手順を実行して、保護ポリシーに資産を追加または削除します。

このタスクについて

保護ポリシーを編集して新しい資産を追加すると、新しい資産のバックアップが、保護ポリシーで次にスケジュール設定されたフル バックアップ ジョブから開始されます。

手順

1. 左ナビゲーション ペインで、[Protection] > [Protection Policies] の順に選択します。
   [Protection Policies] ウィンドウが表示されます。
2. 変更する保護ポリシーを選択し、[Edit] をクリックします。
   [Summary] ページで、[Edit Policy] ウィンドウが開きます。
3. [Assets] の行で、[Edit] をクリックします。
   [Assets] ページが表示されます。
   メモ: 仮想マシンの保護ポリシーでは、ポリシーの作成時に選択したビューはこのページに保持され、変更することはできません。例えば、[View Asset Table] を選択してこのポリシーを設定した場合、このポリシーによって保護されているすべての資産がこのページの表に表示され、[View by Host] を選択するオプションは無効になります。両方のビューには、現在関連付けられているタグ、保護ルール、仮想マシンがすでに別のポリシーに割り当てられているかどうかなど、仮想マシンに関する追加情報が表示されるため、このポリシーに対して追加または削除を行う資産の特定に役立ちます。
4. 保護ポリシーからコンテナーまたは資産を削除するには、オブジェクトを選択し、[Remove] をクリックします。
   [Assets] ページは変更に応じてアップデートされます。
   メモ: バックアップの進行中に資産がポリシーの外に移動されると、PowerProtect Data Manager は、その資産のデフォルト保存期間を 30 日に設定します。必要に応じて、その資産の保存期間を変更できます。
5. 保護ポリシーにコンテナーまたは資産を追加するには、次のようにします。
   a. [+ Add] をクリックします。
      [Add Unprotected Assets] ダイアログには、保護されていないすべてのオブジェクトが表示されます。
   b. ポリシーに追加する、個別の保護されていない資産を選択するか、階層内でコンテナー レベルを選択してそのレベルのすべての資産を追加してから、[Add] をクリックします。
      [Assets] ページは変更に応じてアップデートされます。
6. オプションとして、ネットワーク共有、または保護ポリシーのディスクのテストなど、本番以外の VMDK を除外する場合は、次のようにします。
   a. リストから仮想マシンの資産を選択し、[Disk Excluded] 列の [Manage Exclusions] をクリックします。
      [Exclude Disks] ダイアログ ボックスが表示されます。デフォルトでは、各 VMDK の横にあるスライダーは、[Included] に設定されています。
   b. 除外する各ディスクについて、スライダーを右に移動させます。ステータスが [Excluded] にアップデートされます。
   c. [Save] をクリックします。[Assets] ページがアップデートされ、保護ポリシーから除外される特定の資産のディスク数が示されます。
7. [Next] をクリックして変更を保存し、[Summary] ページに移動します。
8. [Summary] ページで、[Finish] をクリックします。
   情報ダイアログ ボックスが表示されます。
9. [OK] をクリックしてダイアログ ボックスを終了するか、[Go to Jobs] をクリックして [Jobs] ウィンドウを開き、新しい保護ポリシーのバックアップを監視します。

バックアップ コピーの保存期間の編集

1 個または複数のバックアップ コピーの保存期間を編集して、バックアップを保持する時間を延長または短縮することができます。

このタスクについて

すべての資産タイプとバックアップ タイプの保存を編集できます。ただし、ブロック ボリュームを除きます。

手順

1. PowerProtect Data Manager UI から、[Infrastructure] > [Assets] の順に選択します。
2. [Assets] ウィンドウで保存について編集する資産タイプのタブを選択します。ポリシーが割り当てられている場合、表には、検出された資産とともに、関連付けられている保護ポリシーがリスト表示されます。

    アイコンを使用して、vCenter サーバー階層のツリー ビューまたはフォルダー ビュー、あるいは vCenter サーバー内で検出されたすべての仮想マシン資産のリスト ビューを切り替えます。

メモ: 仮想マシン資産の場合は、仮想マシン資産の横にある［Disk Excluded］列のリンクをクリックして、保護ポリシーから除外されている VMDK を表示することができます。ただし、このウィンドウからディスクのインクルージョンまたは除外を編集することはできません。保護対象の資産から除外されているディスクを変更するには、［Protection Policies］ウィンドウでポリシーを選択して、［Edit］をクリックします。

3. 表から保護対象の資産を選択し、［View Copies］をクリックします。［Copy Locations］ペインでは、バックアップが保存されている場所を識別します。
4. 左ペインで、資産のアイコンの右側にある をクリックします。右ペインの表にバックアップ コピーがリストされます。
5. 表から 1 個または複数のバックアップ コピーを選択し、［Edit Retention］をクリックします。

   メモ: 資産バックアップ コピーの削除が失敗すると、［Copy Status］は［Available］から別の状態に変化し、その結果［Edit Retention］ボタンが無効になります。［Edit Retention］ボタンは、［Copy Status］が［Available］の場合のみ有効です。

6. 次のいずれかの方法を選択してください。
   - バックアップの有効期限としてカレンダーの日付を選択するには、［Retention Date］を選択します。
   - 確定保存期間を、バックアップが行われてからの日数、週数、月数、年数で定義するには、［Retention Value］を選択します。例えば、バックアップの有効期限を 6 か月後に指定できます。

   メモ: 保存ロック済みコピーの保存期間を編集する場合は、保存期間の延長のみが可能です。

7. 変更に問題がなければ、［Save］をクリックします。
   資産が変更内容と共にリスト表示されます。［Retention］列には、元の保存期間と新しい保存期間の両方が表示されて、保存期間が延長または短縮されたかどうかを示します。

保護ポリシーのサマリーの表示

PowerProtect Data Manager UI を使用して、保護ポリシーに関する情報のサマリーを表示できます。

左側のナビゲーション ペインで、［Protection］ > ［Protection Policies］を選択して［Protection Policies］ウィンドウを表示します。

［Protection Policies］ウィンドウには、各保護ポリシーに関する次の情報列が表示されます。

- ［名前］
- ［カテゴリ］
- ［資産タイプ］
- ［保護対象資産サイズ］
- ［最終実行ステータス］
- ［違反］
- ［状態］

［Name］列と［Last Run Status］列のエントリーは、関連する保護ポリシーに関する追加情報へのリンクです。

保護ポリシーに割り当てられた資産の表示

保護ポリシーに割り当てられている資産を表示します。資産が保護ポリシー間で移動する場合は、保護ポリシーの詳細ウィンドウから結果を確認できます。

このタスクについて

保護ポリシーに割り当てられている資産を表示するには、次の手順を実行します。

手順

1. 左ナビゲーション ペインで、［保護］ > ［保護ポリシー］の順に選択します。
   ［Protection Policies］ウィンドウが開きます。
2. 保護ポリシーの名前リンクをクリックすると、その詳細が表示されます。
   選択した保護ポリシーの詳細ウィンドウが開き、ポリシーに関する情報が表示されます。
3. ［Assets］の横にある資産カウントのリンクをクリックします。
   ［Assets］ウィンドウが表示され、保護ポリシーに割り当てられている資産が表示されます。
4. 保護ポリシーの資産レコードのエクスポートを行うには、［Assets］ウィンドウで［Export All］をクリックします。

保護ポリシーの最後に実行されたジョブのステータスの表示

［Protection Plicies］ウィンドウを使用して、保護ポリシーの最後に実行されたジョブが成功したかどうかを判断できます。

このタスクについて

保護ポリシーの最後に実行されたジョブのステータスを表示するには、次の手順を実行します。

手順

1. 左ナビゲーション ペインで、［保護］ > ［保護ポリシー］の順に選択します。
   ［Protection Policies］ウィンドウが開きます。
2. 保護ポリシーの［Last Run Status］列に表示される情報を確認します。
3. オプションとして、保護ポリシーの最後に実行されたステータス リンクをクリックして、［Protection Jobs］ウィンドウが表示され、ジョブの詳細を確認できます。

   メモ: ［Protection Jobs］ウィンドウには、最近実行された保護ジョブのみが表示されます。最近実行されたシステム ジョブを表示するには、左側のナビゲーション ペインから［Jobs］ > ［System Jobs］を選択して、［System Jobs］ウィンドウを表示します。

資産保護レポートの実行

このオプションにより、資産保護レポートを実行して、そのレポートを CSV 形式で保存し、保護結果データを Excel ファイルとしてダウンロードできるようになります。

手順

1. PowerProtect Data Manager UI から、［Protection］ > ［Protection Policies］の順に選択します。
2. 保護レコードをエクスポートする保護ポリシーを選択します。
   保護ポリシーを選択しないと、PowerProtect Data Manager はすべての保護ポリシーの保護レコードをエクスポートします。
3. ［Run Asset Protection Report］をクリックします。
   ［Export Asset Protection］ウィンドウが表示されます。
4. エクスポートに関する次のフィールドを指定します。
   a. ［Time Range］。
      デフォルト値は［過去 24 時間］です。
      これは、真夜中から真夜中までの完全な 24 時間の最新の期間を指します。つまり、昨日です。したがって、直近の深夜以降に発生したイベントは、CSV エクスポートには含まれません。たとえば、午前 9 時に CSV エクスポートを実行した場合、過去 9 時間以内に発生したいずれのイベントも CSV エクスポートに含まれません。これは、日中に定期的または不定期ベースでクエリーが実行された場合に、エクスポートが重複するか、部分的になるのを防止するためです。
   b. ［Job Status］。
   c. ［Download］をクリックします。
      該当する場合、.csv ファイルを保存する場所を選択するためのナビゲーション ウィンドウが表示されます。
5. 必要に応じて、目的の場所を指定して［Save］をクリックし、.csv ファイルを保存します。

サービスレベル アグリーメントの追加

PowerProtect Data Manager UI の［SLA Compliance］では、サービスレベル目標(SLO)を特定するサービスレベル アグリーメント(SLA)を追加することができます。SLO を使用して、保護された資産がサービスレベル アグリーメント(SLA)を満たしていることを確認します。

このタスクについて

メモ: クラウド階層の SLA を作成すると、SLA にフル バックアップのみを含めることができます。

メモ: ［Extended Retention］ SLA は、PowerProtect Data Manager 19.11 以前で作成された保護ポリシーにのみ適用されます。Extended Retention 目標は PowerProtect Data Manager 19.12 で削除されました。それより前のリリースで、［Extend Retention］ SLA で作成された保護ポリシーはサポートされます。ただし、これらのポリシーで［Extended Retention］ SLA を編集することはできません。

［SLA Compliance］ウィンドウでは、［Export All］機能を使用してコンプライアンス データのエクスポートを行うことができます。

手順

1. PowerProtect Data Manager UI から、［Protection］ > ［SLA Compliance］の順に選択します。
   ［SLA Compliance］ウィンドウが表示されます。
2. ［Add］をクリックするか、SLA を適用する資産がリストになっている場合は、これらの資産を選択して［Add］をクリックします。
   ［Add Service Level Agreement］ウィザードが開きます。
3. 追加する SLA のタイプを選択し、［Next］をクリックします。
   - ［Policy］。このタイプを選択した場合は、ステップ 4 に進みます。
   - ［Backup］。このタイプを選択した場合は、ステップ 5 に進みます。
   - ［Replication］。このタイプを選択した場合は、ステップ 6 に進みます。
   - ［Cloud Tier］。このタイプを選択した場合は、ステップ 7 に進みます。

   1 つのタイプのサービス レベル アグリーメントのみを選択できます。
4. ［Policy］を選択した場合は、新しいポリシー SLA の目的に関する次のフィールドを指定します。
   a. ［SLA Name］。
   b. 該当する場合は、［Minimum Copies］を選択して、バックアップ、レプリケーション、クラウド階層のコピーの数を指定します。
   c. 該当する場合は、［Maximum Copies］を選択して、バックアップ、レプリケーション、クラウド階層のコピーの数を指定します。
   d. 該当する場合は、［Available Location］を選択して、該当する場所を選択します。場所を追加するには、［Add Location］をクリックします。

      オプションには、次のようなものがあります。
      - ［In］：SLO の場所にあるすべてのコピーの場所を含めます。このオプションを選択する場合、すべての SLO の場所にコピーを保持する必要はありません。
      - ［Must In］：SLO の場所にあるすべてのコピーの場所を含めます。このオプションを選択する場合、すべての SLO の場所に少なくとも 1 つのコピーを含める必要があります。
      - ［Exclude］：すべてのコピーの場所は SLO の場所以外である必要があります。

      メモ: Idefinite Retention Hold (IRH)が有効になっているストレージ ユニットにバックアップされたポリシー ファイルは、Retention Lock の期限切れ後あっても、削除も変更もできません。したがって、この設定は IRH と競合するため、［Maximum Copies］オプションを選択しないことをお勧めします。そうしないと、コピーの数が指定された数を超えた場合に SLA を正常に満たせません。

   e. 該当する場合は、［Allowed in Cloud through Cloud Tier/Cloud DR］を選択します。
   f. ［Finish］をクリックしてから、ステップ 9 に進みます。
5. ［Backup］を選択した場合は、新しい［Backup］ SLA の目的に関する次のフィールドを指定します。
   a. ［SLA Name］。
   b. 該当する場合は、［Recovery Point Objective required］ (RPO)を選択して、期間を設定します。RPO の目的はビジネス継続性プランニングです。これは、主なインシデントにより、IT サービスからデータ（トランザクション）が失われる可能性がある最大対象期間を意味します。

      メモ: ［Recovery Point Objective required］のみを選択して、SLA で独立した目標として設定するか、または［Recovery Point Objective required］と［Compliance Window for copy type］の両方を選択できます。両方を選択する場合は、RPO 設定を次のいずれかにする必要があります。
      - 24 時間より長い期間またはコンプライアンス ウィンドウの期間より長い期間。この場合は、コンプライアンス ウィンドウに関係なく RPO の検証が行われます。
      - コンプライアンス ウィンドウの期間と同じかより短い期間。この場合は、コンプライアンス ウィンドウ内で RPO の検証が行われます。

   c. 該当する場合は、［Compliance Window for copy type］を選択し、リストからスケジュール レベル（例えば［All］、［Full］、［Cumulative］など）を選択して、期間を設定します。［Duration］は、バックアップ コピーを作成するために必要な時間を示します。バックアップ コピー作成の［Start Time］と［End Time］が[Compliance Window]で指定した期間内であることを確認します。

      このウィンドウでは指定したアクティビティーの実行にかかる予想時間を指定します。この［Start Time］と［End Time］外に指定されたアクティビティが発生すると、アラートをトリガーします。
   d. 該当する場合は、［Verify expired copies are deleted］オプションを選択します。

      ［Verify expired copies are deleted］は、PowerProtect Data Manager が期限切れのコピーを削除しているかどうかを確認するコンプライアンス チェックです。このオプションはデフォルトで無効になっています。

      メモ: IRH が有効になっているストレージ ユニットにバックアップされたデータは、Retention Lock の有効期限が切れた後であっても、削除も変更できません。したがって、この設定は IRH と競合するため、［Verify expired copies are deleted］オプションを選択しないことをお勧めします。そうしないと、SLA を正常に満たせません。

   e. 該当する場合は、［Retention Time Objective］を選択して、日数、月数、週数、または年数を指定します。

メモ: ［Retention Time Objective］の値は、このポリシーのターゲット目標のバックアップ レベルの保存期間の最小値と一致する必要があります。たとえば、統合フル バックアップの［Retain For］が 30 日で、フル バックアップの［Retain For］が 60 日の場合は、［Retention Time Objective］を 30 日に設定します。

f. 該当する場合は、［Verify Retention Lock is enabled for all copies］オプションを選択します。このオプションはデフォルトで無効になっています。
g. ［Finish］をクリックして、ステップ 9 に進みます。
［SLA Compliance］ウィンドウに、新しい SLA が表示されます。

6. ［Replication］を選択した場合は、新しいレプリケーション SLA の目的について、次のフィールドを指定します。
a. ［SLA Name］。
b. 該当する場合は、［Compliance Window］を選択し、［Start Time］と［End Time］を指定します。
このウィンドウでは、許容範囲内の時間および指定したアクティビティーの実行に予想される時間範囲を指定します。この開始時間と終了時間外に指定されたアクティビティが発生すると、アラートをトリガーします。
c. 該当する場合は、［Verify expired copies are deleted］オプションを選択します。
［Verify expired copies are deleted］は、PowerProtect Data Manager が期限切れのコピーを削除しているかどうかを確認するコンプライアンス チェックです。このオプションはデフォルトで無効になっています。
メモ: IRH が有効になっているストレージ ユニットでレプリケートされたデータは、Retention Lock の有効期限が切れた後であっても、削除も変更もできません。したがって、この設定は IRH と競合するため、［Verify expired copies are deleted］オプションを選択しないことをお勧めします。そうしないと、SLA を正常に満たせません。
d. 該当する場合は、［Retention Time Objective］を選択して、日数、月数、週数、または年数を指定します。
メモ: ［Retention Time Objective］の値は、このポリシーのターゲット目標のバックアップ レベルの保存期間の最小値と一致するように設定します。
e. 該当する場合は、［Verify Retention Lock is enabled for all copies］オプションを選択します。このオプションはデフォルトで無効になっています。
f. ［Finish］をクリックして、ステップ 9 に進みます。
［SLA Compliance］ウィンドウに、新しく追加された SLA が表示されます。

7. ［Cloud Tier］タイプの SLA を選択した場合は、新しいクラウド階層 SLA の目的について、次のフィールドを指定します。
a. ［SLA Name］。
b. 該当する場合は、［Verify expired copies are deleted］オプションを選択します。
このオプションは、PowerProtect Data Manager が期限切れのコピーを削除しているかどうかを判別するためのコンプライアンス チェックです。このオプションはデフォルトで無効になっています。
c. 該当する場合は、［Retention Time Objective］を選択して、日数、月数、週数、または年数を指定します。
メモ: ［Retention Time Objective］の値は、このポリシーのターゲット目標のバックアップ レベルの保存期間の最小値と一致するように設定します。
d. 該当する場合は、［Verify Retention Lock is enabled for all copies］オプションを選択します。このオプションはデフォルトで無効になっています。
e. ［Finish］をクリックします。

8. SLA がまだ保護ポリシーに適用されていない場合は、次の手順を実行します。
a. ［Protection］ > ［Protection Policies］に移動します。
b. ポリシーを選択して、［Edit］をクリックします。

9. ［Summary］ウィンドウの［Objectives］行で、［Edit］をクリックします。

10. 以下のいずれかのオプションを選択して、［Next］をクリックします。
- ［Set Policy Level SLA］リストから、追加されたポリシー SLA を選択します。
- ［Set Policy Level SLA］リストから、SLA ポリシーを作成して追加します。

［Summary］ウィンドウが表示されます。

11. ［Finish］をクリックします。
PowerProtect Data Manager が保護ポリシーを保存したことを確認する情報メッセージが表示されます。

12. ［Go to Jobs］をクリックして［Jobs］ウィンドウを開き、バックアップとコンプライアンスの結果を監視するか、［OK］をクリックして終了します。
メモ: コンプライアンス チェックは毎日午前 2 時（協定世界時(UTC)）に自動的に実行されます。いずれかの目標がコンプライアンスに違反している場合、アラートが午前 2 時に生成されます。UTC。［System Jobs］ウィンドウのジョブの［Validate］には、日次コンプライアンス チェックの結果が表示されます。

必要な RPO 設定が 24 時間未満のバックアップ SLA の場合、PowerProtect Data Manager はリアルタイムのコンプライアンス チェックを実行します。［Compliance Window for copy type］を選択し、バックアップ レベルを［All］に設定した場合、コンプライアンス ウィンドウ内でのみ 15 分ご

とにリアルタイムのコンプライアンス チェックが実行されます。バックアップ レベルが［All］でない場合、またはコンプライアンス ウィンドウが指定されていない場合は、リアルタイムのコンプライアンス チェックが停止することなく 15 分ごとに実行されます。

メモ: バックアップ SLA に必要な RPO 設定が 24 時間以上ある場合、コンプライアンス チェックは毎日午前 2 時に行われます。UTC。RPO 設定が 24 時間以上のバックアップ SLA では、リアルタイムのコンプライアンス チェックは実行されません。

［Real-time compliance-check behavior］

RPO バックアップ間隔の上限以内に資産がバックアップされなかった場合、資産の RPO がコンプライアンス違反であることを示すアラートが表示されます。このアラートは、RPO 期間内に 1 回生成されます。次回のコンプライアンス チェックの実行時に同じバックアップ コピーが失われると、それ以上のアラートは生成されません。

RPO バックアップ間隔の上限以内に資産がバックアップされた場合、資産の RPO は SLA に準拠しています。

コンプライアンス違反の資産が 1 つのポリシーに複数ある場合、アラートは 1 件生成されます。このアラートには、ポリシーのすべての資産に関する情報が含められます。［Alerts］ウィンドウで、アラート サマリーの横にある資産数は、ポリシーのコンプライアンス違反である資産の数を示します。

13. ［Jobs］ウィンドウで、エントリーの横にあるをクリックして、SLA コンプライアンスの結果の詳細を表示します。

コンプライアンス レポートの実行

このオプションにより、コンプライアンス レポートを実行して、CSV 形式でレポートを保存し、Excel ファイルとしてコンプライアンス結果データのダウンロードを行うことができます。

手順

1. PowerProtect Data Manager UI から、［Protection］ > ［SLA Compliance］の順に選択します。
   ［SLA Compliance］ウィンドウが表示されます。PowerProtect Data Manager の［SLA Compliance］ウィンドウには、次の情報が表示されます。
   - SLA 名
   - ステージ タイプ
   - リスクにさらされるポリシー
   - コンプライアンス違反の目標
   - 影響を受ける資産
2. コンプライアンス レコードをエクスポートする SLA を選択します。
3. ［Run Compliance Report］をクリックします。
   ［Run Compliance Report］ウィンドウが表示されます。
4. エクスポートに関する次のフィールドを指定します。
   a. ［Time Range］。
      デフォルト値は［過去 24 時間］です。
      これは、真夜中から真夜中までの完全な 24 時間の最新の期間を指します。つまり、昨日です。したがって、直近の深夜以降に発生したイベントは、CSV エクスポートには含まれません。たとえば、午前 9 時に CSV エクスポートを実行した場合、過去 9 時間以内に発生したいずれのイベントも CSV エクスポートに含まれません。これは、日中に定期的または不定期ベースでクエリーが実行された場合に、エクスポートが重複するか、部分的になるのを防止するためです。
   b. ［Job Status］。
   c. ［Download .CSV］をクリックします。
      該当する場合、.csv ファイルを保存する場所を選択するためのナビゲーション ウィンドウが表示されます。
5. 必要に応じて、目的の場所を指定して［Save］をクリックして .csv ファイルを保存します。

保護ポリシーの無効化

PowerProtect Data Manager UI で保護ポリシーを無効化して、このポリシーに含まれている特定のバックアップ目的を一時的に実行停止できます。

このタスクについて

保護ポリシーを無効にする理由はいくつかあります。例えば、ポリシーを無効にすると、次のようなことが行えます。

- ポリシーを編集し、その変更が有効になる前に影響について判断する。

- ストレージがメンテナンス中の場合、または一時的に使用できない場合（ストレージのアップグレード中など）に、プライマリー ストレージのバックアップ アクティビティを停止する。

デフォルトでは、一元的な保護ポリシーを無効にすると、このポリシーのプライマリー バックアップ目的の統合フル バックアップ、フル バックアップなどが停止します。ただし、レプリケーションとクラウド階層の目的は、ポリシーが無効になっている間も引き続き実行されます。PowerProtect Data Manager UI の［Protect Now］機能を使用して、［Disabled］状態のポリシーの手動プライマリー バックアップを実行することもできます。

REST API でシステム レベルの上書きを使用することで、デフォルトの反応を変更して、ポリシーが無効化されたときに実行を継続するジョブについて変更を行うことができます。PowerProtect Data Manager パブリック REST API のドキュメントに、手順が記載されています。

保護ポリシーが無効になっている場合は、有効なポリシーを編集するのと同じ方法でポリシーを編集できます。［Disabled］状態のポリシーを編集する利点は、ポリシーのプライマリー バックアップを再開する前に変更をプレビューできる点です。 保護ポリシーの追加または編集 に、既存のポリシーの詳細を変更する際の情報が記載されています。

手順

1. 左ナビゲーション ペインで、［Protection］ > ［Protection Policies］の順に選択します。
   ［Protection Policies］ウィンドウが開きます。
2. ［Enabled］状態のポリシーを 1 個または複数選択します。表の上部にあるチェックボックスを選択して、現在のページにあるすべてのポリシーを選択することもできます。
3. ［Disable］をクリックします。

タスクの結果

ポリシーのステータスが［Disabled］に変更されます。［Disabled］状態の場合：

- このポリシーに関連づけられている進行中のプライマリー バックアップ ジョブが、完了するまで引き続き実行されます。プライマリー バックアップの実行が、ポリシーが無効化されている間にスケジュール設定されている場合は、ポリシーを再度有効にしても、それらのバックアップは実行されません。ポリシーを再度有効にすると、以降にスケジュール設定されたバックアップが再開されます。
- プライマリー バックアップ コピーがポリシーに存在しない限り、ポリシーの他のすべての保護ジョブはスケジュールに沿って実行されます。この場合、保護ジョブはスキップされます。
- プライマリー目的の手動バックアップは引き続き実行できます。

無効化されたポリシーに対して実行されている保護ジョブ

保護ポリシーが無効化されると、プライマリー バックアップ目的に関連する保護ジョブのみが実行を停止します。

次の表では、ポリシーが［Disabled］状態のときに引き続き実行される保護ジョブのタイプについて説明します。［System level ovewrite?］列は、API コマンドを使用して、このジョブのデフォルトの反応を上書きできるかどうかを示します。ただし、ポリシーが無効になっている場合は、これらのジョブの少なくとも 1 個の設定を無効にしておく必要があることに注意してください。

メモ: 無効なポリシーにプライマリー バックアップ コピーが存在しない場合、レプリケーションなどのスケジュール設定されたその他の保護ジョブは、PowerProtect Data Manager UI の［Protection Jobs］ウィンドウに［Skipped］と表示されます。

表 26. ポリシーが無効になっている場合に実行される保護ジョブ

ジョブ カテゴリー	目的	ポリシーが無効になっている場合に実行されますか？	システム レベルで上書きされますか？
スケジュール設定された一元的なプライマリー保護	プライマリー バックアップの作成	不可	可
手動バックアップとレプリケーション（今すぐ保護、今すぐレプリケート）	• プライマリー バックアップの作成（今すぐ保護） • プライマリー バックアップのレプリケートする（今すぐレプリケート）	可	不可
セルフサービス保護	プライマリー バックアップの作成	可	不可
ポリシーと資産の構成	保護またはコピー管理ジョブの準備	可	不可
レプリケーション	コピー管理（場所）	可	可
Cloud DR	コピー管理（場所）	可	可
長期保存	コピー管理（保存）	可	可
クラウド階層	コピー管理（場所）	可	可

表 26. ポリシーが無効になっている場合に実行される保護ジョブ （続き）

ジョブ カテゴリー	目的	ポリシーが無効になっている場合に実行されますか？	システム レベルで上書きされますか？
SLA コンプライアンスの検証	コピー管理（レポートとアラート）	可	可
使用期限が終了したコピーの削除	コピー管理（DD 上の領域の再利用）	可	可

無効化された保護ポリシーの有効化

無効化されたポリシーを再度有効化するには、次の手順を実行します。

手順

1. PowerProtect Data Manager UI から、［保護］ > ［保護ポリシー］の順に選択します。
2. ［Disabled］状態のポリシーを 1 個または複数選択します。表の上部にあるチェックボックスを選択して、現在のページにあるすべてのポリシーを選択することもできます。
3. ［[有効化]］をクリックします。

タスクの結果

ステータスが［Enabled］に変更されます。再度有効化されたポリシーのプライマリー バックアップは、保護ポリシーのスケジュールに沿って再開されます。

無効化されたポリシーのデフォルトの反応をカスタマイズする

デフォルトでは、［Disabled］状態の保護ポリシーによって、このポリシーのプライマリー バックアップ目的の実行が防がれますが、他の保護ジョブは停止されません。ただし、REST API を使用して、レプリケーションやクラウド階層化などの他のアクティビティを停止するようにデフォルトの反応を変更することもできます。

PowerProtect Data Manager パブリック REST API のドキュメントに、手順が記載されています。

保護ポリシーの削除

どの資産も保護していない保護ポリシーを削除するには、次の手順を実行します。

前提条件

削除するポリシーが資産を保護している場合は、ポリシーを削除する前に、それらの資産を別の保護ポリシーに関連づける必要があります。

手順

1. PowerProtect Data Manager UI から、［保護］ > ［保護ポリシー］の順に選択します。
2. 削除するポリシーを選択して、［Delete］をクリックします。

タスクの結果

ポリシーを削除すると、スケジュールに従って保護ストレージ上の不要なコンポーネントのクリーンアップが自動的に実行されます。ストレージ ユニットのルールに応じて、クリーンアップには、PowerProtect Data Manager の制御下にあるストレージ ユニットと、対応する DDBoost ユーザーの制御下にあるストレージ ユニットが含まれます。

PowerProtect Data Manager クラウド階層の概要

PowerProtect Data Manager クラウド階層機能は、DD システムのクラウド階層機能と連携して PowerProtect Data Manager のバックアップをクラウドに移動します。これは、クラウドへデータをシームレスかつ安全に階層化することにより、PowerProtect Data Manager バックアップの長期保管を提供します。

PowerProtect Data Manager UI で、クラウド階層を構成して PowerProtect Data Manager のバックアップを保護ストレージからクラウドに移動し、これらのバックアップのシームレスなリカバリーを実行できます。

クラウド ストレージ ユニットは、PowerProtect Data Manager UI でクラウド階層用に構成される前に、保護ストレージ システムで事前構成済みである必要があります。詳細については、*DDOS* 管理ガイドを参照してください。

保護ポリシーへのクラウド階層目的の追加

一部の保護ポリシー タイプでは、事前定義された日数が経過した後にローカルのフル バックアップをクラウド階層に移動するために、クラウド階層目的を保護ポリシーに追加できます。

前提条件

- システム パスフレーズが設定された状態で、クラウド階層化用に保護ストレージ システムがセットアップされていることを確認します。
- クラウド ストレージ ユニットは、PowerProtect Data Manager UI でクラウド階層用に構成される前に、保護ストレージ システムで事前構成済みである必要があります。
- データ移動スケジュールを構成し、クラウド ストレージ ユニット上で実行されている必要があります。
- クラウド階層 目的は、［Primary Backup］および［Replicate］ 目的に追加できます。［Primary Backup］と［Replicate］ 目的は、クラウド階層化用にセットアップされた保護ストレージ システムを使用している必要があります。

このタスクについて

クラウド階層化は、毎日 00:00 UTC に行われます。タイムゾーンによっては、この時間が営業時間内であるため、クラウド階層化によって使用可能なネットワーク帯域幅に影響が及ぶ可能性があります。クラウド階層化は、一元管理およびセルフサービス保護の両方のポリシーに適用されます。

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. PowerProtect Data Manager UI から、［Protection］ > ［Protection Policies］の順に選択してから［Add］をクリックします。
   ［Add Policy］ウィザードが表示されます。
3. ［Type］ページで名前と説明を入力し、バックアップするシステムのタイプを選択して、［Next］をクリックします。
   次の保護ポリシー タイプがクラウド階層化をサポートしています。
   - 仮想マシン
   - Microsoft SQL Server
   - Microsoft Exchange Server
   - ネットワーク接続型ストレージ(NAS)
   - Oracle
   - SAP HANA
   - ファイル システム
   - Kubernetes
   - ブロック ボリューム
4. ［Purpose］ページで、使用可能なオプションから新しい保護ポリシーの目的を示すものを選択して、［Next］をクリックします。
5. ［Assets］ページで、このポリシーで保護する資産を選択し、［Next］をクリックします。
6. プライマリー バックアップの目的をまだ作成していない場合は、［Objectives］ページで、［Primary Backup］の下にある［Add］をクリックし、［Add Primary Backup］ダイアログの［Target］ペインおよび［Schedules］ペインのフィールドに入力します。

   メモ: クラウド目的では最小限の繰り返しを行う必要はありません。ただし、クラウド階層の目的では、［Retain for］フィールドの最小保存期間を 14 日にする必要があります。

7. ［Primary Backup］の横にある［Cloud Tier］をクリックします。または、追加したレプリケーション目的にクラウド目的を追加する場合は、［Replicate］の下にある［Cloud Tier］をクリックします。
   ［Cloud Tier］のエントリーは、プライマリー バックアップ目的の右、またはレプリケーション目的の下に作成されます。
8. ［Cloud Tier］のエントリーの下にある［Add］をクリックします。
   ［Add Cloud Tier Backup］ダイアログが親ノードのサマリー情報と一緒に表示されます。この情報は、プライマリー バックアップ目的またはレプリケーション目的用に、このクラウド階層の目的を追加しているかどうかを示しています。
9. ［Add Cloud Tier Backup］ダイアログ ボックスで次のパラメーターを設定して、［Save］をクリックします。
   - 1 個以上のアップストリーム フル バックアップを選択します。
   - ［Cloud Target］リストから適切なクラウド ユニットを選択します。
   - ［Tier After］では、14 日以上の期間を設定します。

   クラウド階層化により、保護ポリシーが有効になりました。

メモ: コピーの保存期間が［Tier After］フィールドに指定された期間よりも短く、コピーの保存期間が期限切れになる前に、このスケジュールまたはそのコピーの［Retain for］の値を［Tier After］フィールドよりも大きい値に編集しなかった場合、コピーはクラウド階層化されません。

10. ［Next］をクリックして［Add Policy］ウィザードの残りのページに進み、情報を確認してから、［Finish］をクリックします。
新しいジョブが作成され、ジョブが完了した後に［Jobs］タブの下に表示できるようになります。

クラウド階層資産コピーの管理

コピーの保存期間を変更したり、コピーを削除したり、コピーをリコールしたりすることで、クラウド階層の資産のコピーを管理できます。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Assets］の順に選択します。
2. 資産を選択し、［View Copies］をクリックします。
3. 資産のコピー アイコンをクリックします。
クラウド階層のバックアップは、クラウド ストレージの［Location］列に表示されます。
4. クラウド ストレージに保持するコピーの長さを変更するには、次の手順を実行します。
   a. クラウド階層のバックアップを選択し、［Edit Retention］をクリックします。
   b. 次のいずれかの方法を選択してください。
      - バックアップの有効期限としてカレンダーの日付を選択するには、［Retention Date］を選択します。
      - 確定保存期間を、バックアップが行われてからの日数、週数、月数、年数で定義するには、［Retention Value］を選択します。例えば、バックアップの有効期限を 6 か月後に指定できます。
   c. 変更に問題がなければ、［Save］をクリックします。
   資産が変更内容と共にリスト表示されます。［Retention］列には、元の保存期間と新しい保存期間の両方が表示されて、保存期間が延長または短縮されたかどうかを示します。

   メモ: 保存ロック済みコピーの保存期間を編集する場合は、保存期間の延長のみが可能です。

5. クラウド ストレージのコピーを削除するにはクラウド階層のバックアップを選択して、［Delete］をクリックします。保護ストレージにコピーが残っているときに PowerProtect Data Manager のデータベースからコピー レコードを削除するには、［Remove from PowerProtect］を選択します。
   バックアップ コピーの削除 および Exchange、ファイル システム、Kubernetes、ブロック ボリューム、SQL バックアップ コピーの PowerProtect Data Manager データベースからの削除に詳細を示します。
6. リカバリーまたはバックアップ用にクラウド バックアップをローカルの保護ストレージに戻すには、クラウド階層バックアップを選択して［Recall from Cloud］をクリックします。

   メモ: Amazon のネットワークを使用して AWS ストレージからデータをコピーする場合、Amazon ではデータ転送料金を請求します。

7. コピーをクラウドに戻して再階層化する日付を延長するには、［Edit Recall Retention］を選択します。
8. コピーを手動でクラウド ストレージに戻すには、［Retier］を選択します。

クラウド階層バックアップの保護ストレージへのリストア

クラウド階層のバックアップをリコールすると、これらのバックアップのリストア操作は通常のリストア操作と同じになります。

PowerProtect Data Manager ソフトウェアは、クラウド ユニットから保護ストレージのローカル（アクティブな）階層にバックアップ コピーのリコールを行い、アクティブな階層からクライアントにバックアップのリストアを行えるようにします。ステータスは［Cloud］と表示され、クラウドからのリコールが完了すると［Local Recalled］に変わります。リストア後、バックアップ コピーはクラウド階層から削除され、保護ストレージのアクティブな階層に少なくとも 14 日間保存されます。その後は、保護ポリシーに応じてバックアップがクラウドに戻される場合があります。

クラウド階層からのリコールとリストア

保護ストレージのアクティブ階層にクラウド階層のバックアップをリコールして、このバックアップをリストアするには、次の手順を実行します。

前提条件

メモ: クラウド階層からアクティブ階層にバックアップをリコールすると、そのコピーがクラウド階層から削除されます。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［資産］の順に選択します。
2. ［Assets］ウィンドウで、クラウド階層からリコールする資産を含むタブを選択し、［View Copies］をクリックします。
3. ［DD］をクリックして、表に表示されている利用できるコピーのいずれかを選択します。
4. ［Recall］をクリックします。
   ［［Recall from Cloud］］ダイアログ ボックスが表示されます。
5. ［Retain until］ボックスで、アクティブ階層にコピーを保存する期間を指定し、［OK］をクリックします。
6. ［［Jobs］］ウィンドウに移動して、リコール操作を監視します。
   コピーが正常に移動されると、［Location］が［Cloud］から［Local］に変わります。
7. ［リストア］ > ［Assets］を選択して、リコールした資産を含むタブを選択します。
8. リコールした資産を選択し、［Restore］をクリックします。

   メモ: 資産のリコールが行われたかどうか不明な場合は、［View Copies］をクリックし、［DD］を選択して、利用できるバックアップ コピーを表示してください。リコールしたコピーが資産のバックアップの場合は、ステータス列に［Local Recalled］と表示されます。

9. リコールしたコピーを選択して、コピーをアクティブ階層に再階層化します。

PowerProtect Data Manager 19.11 以前に作成された保護ポリシーの長期保存

メモ: このセクションは、PowerProtect Data Manager 19.11 以前に作成された保護ポリシーにのみ適用されます。PowerProtect Data Manager 19.12 以降に作成された保護ポリシーでは、プライマリー バックアップとレプリケーションの対象に対して複数のフル スケジュールを追加します。以前のリリースで［Extend Retention］の対象に作成された保護ポリシーがサポートされます。ただし、既存の長期保存の対象を編集したり、これらのポリシーに新しい長期保存の対象を追加したりすることはできません。PowerProtect Data Manager をアップデートする場合、特定の［Extend Retention］の対象を移行するシナリオの詳細については、https://www.dell.com/support/でナレッジベース記事「000204454」を参照してください。

PowerProtect Data Manager 19.11 以前に作成された保護ポリシーの場合、［Extend Retention］の対象で、長期保存用にプライマリー バックアップ コピーの保存期間を延長できます。たとえば、定期的な日次バックアップのスケジュールでは、30 日間の保存期間を使用します。ただし、保存期間を延長して、月曜日に行われるフル バックアップを 10 週間保持できます。

一元的保護ポリシーおよびセルフサービス保護ポリシーの両方で週次、月次、年次の繰り返しスケジュールがサポートされており、コンプライアンス方針の要件を満たしています。たとえば、会計年度の最新トランザクションを含む最新のフル バックアップを 10 年間保存できます。保存期間を延長すると、指定した期間繰り返すようにスケジュール設定されたフル バックアップを保存できます。

例：

- 1 月の最初の日に繰り返すように設定された年次フル バックアップを 5 年間保存します。
- 毎月の最終日に繰り返すように設定された月次フル バックアップを 1 年間保存します。
- 12 月の第 3 月曜日に繰り返すように設定された年次フル バックアップを 7 年間保存します。

推奨代案

保護ポリシーの長期保存目的を決める際に、保存する推奨バックアップを選択するための照合基準を定めます。照合基準に一致するバックアップが見つからない場合は、PowerProtect Data Manager によって、推奨代案のバックアップが次のいずれかの方法に従って自動的に保存されます。

- 後読み：照合基準の前に取得された、最新の使用可能なフル バックアップを保存します。
- 先読み：照合基準の後に取得された、次に使用可能なフル バックアップを保存します。

たとえば、その月の最終日の日次バックアップを長期保存に保存するように保護ポリシーを構成したとします。しかし、ネットワークの問題によってバックアップが失敗してしまいました。このケースでは、後読み照合によって前日に取得されたバックアップが保存されるか、先読み照合により次の日に取得されるバックアップが保存されます。

デフォルトでは、PowerProtect Data Manager で後読み照合を使用して推奨代案のバックアップが選択されます。猶予期間は、代案バックアップの構成方向において PowerProtect Data Manager でどの程度先を読むことができるかを意味します。PowerProtect Data Manager によって猶予期間内に代案のバックアップを見つけられない場合、長期保存は失敗します。

REST API を使用して、照合方法を変更したり、先読み照合の猶予期間を変更したりすることができます。PowerProtect Data Manager パブリック REST API のドキュメントに、手順が記載されています。規定された照合期間に使用可能なバックアップがない場合は、照合方法を別のバックアップに変更できます。

先読み照合の場合、次に使用可能なバックアップが手動バックアップまたは次にスケジュール設定されたバックアップになる可能性があります。

平日のバックアップの選択

このセクションは一元的保護ポリシーに適用されます。セルフサービス保護ポリシーには、プライマリー バックアップ目的の構成がありません。

平日のバックアップと照合するように長期保存期間を設定すると、PowerProtect Data Manager では、バックアップの取得日が正しく識別されない場合があります。この動作は、バックアップ ウィンドウとその日の開始時間が合っていない場合に起こります。PowerProtect Data Manager では、バックアップそのものの開始ではなく、対応するバックアップ ウィンドウが開始する日に基づいてバックアップが認識されます。

たとえば、バックアップが午後 8:00～午前 6:00 のバックアップ ウィンドウでスケジュール設定されているとします。

- 日曜日の午前 0:00 に始まり日曜日の午前 6:00 に終了するバックアップは、土曜日にバックアップ ウィンドウが開始したため、土曜日のバックアップとして識別されます。
- 日曜日の午後 8:01 に始まり月曜日の午前 0:00 に終了するバックアップは、日曜日にバックアップ ウィンドウが開始したため、日曜日のバックアップとして識別されます。
- 月曜日の午前 0:00 に始まり月曜日の午前 6:00 に終了するバックアップは、日曜日にバックアップ ウィンドウが開始したため、日曜日のバックアップとして識別されます。

この例では、長期保存に日曜日のバックアップを選択する場合、PowerProtect Data Manager では、次の時間帯に取得されたバックアップは保存されません（午前 0:00～午後 8:00）。この動作は日曜日にバックアップが行われる場合にも起こります。代わりに、PowerProtect Data Manager によって、日曜日の午後 8:00 以降に開始した、最初の使用可能なバックアップが長期保存用に選択されます。

次の時間帯にバックアップが作成されていない場合（日曜日の午後 8:01～月曜日の午前 6:00 の間）は、PowerProtect Data Manager によって、次の代案が長期保存に保存されます。この例の代案は月曜日の午前 6:00 以降に取得されたものです。

長期保存バックアップの動作

PowerProtect Data Manager によって一致するバックアップが見つかった場合、プライマリー目的用のバックアップ ウィンドウが始まる際に長期保存のジョブが自動的に作成されます。このジョブはバックアップ ウィンドウの終了まで待機状態のままになります。

次の例では、一元的保護とセルフサービス保護用の長期保存によるバックアップの動作について説明します。

一元的保護

1 時間ごとのプライマリー バックアップ スケジュールが日曜日の午後 8:00 に開始して月曜日の午後 6:00 に終了する場合、週次の長期保存の目的が毎週日曜日に繰り返すよう設定されます。PowerProtect Data Manager によって、日曜日の午後 8:00 以降に開始した、最初の使用可能なバックアップが長期保存用に選択されます。

次の図は、構成済み保護ポリシー用の長期保存によるバックアップの動作を示しています。この例では、フルの日次バックアップが午後 10:00 に始まり午前 6:00 に終了して、1 週間保存されます。フルの週次バックアップは、毎週日曜日に繰り返すように設定されており、1 か月間保存されます。

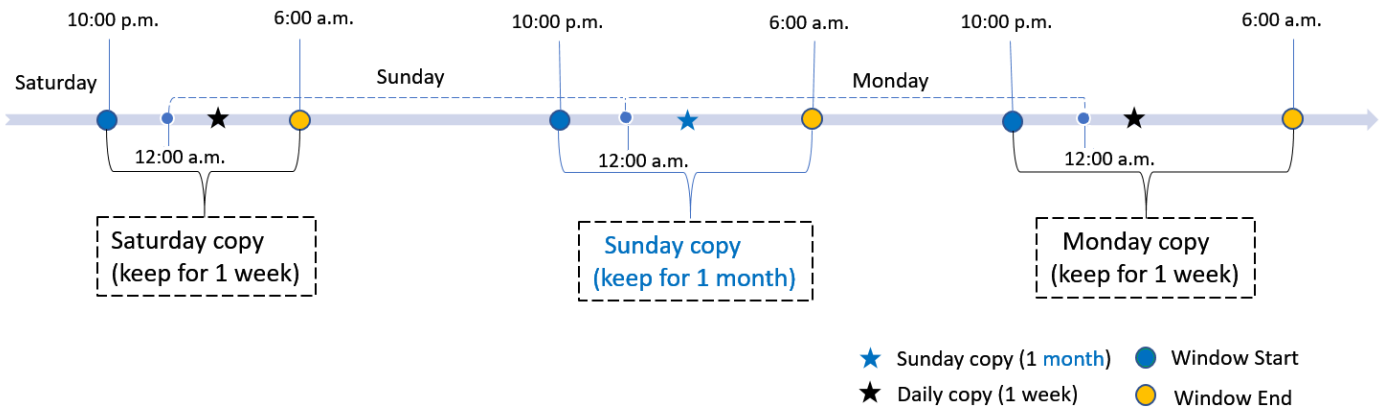


図 2. 長期保存バックアップの動作

セルフサービス保護

セルフサービス バックアップの場合は、PowerProtect Data Manager でデフォルトの 24 時間のバックアップ ウィンドウが使用されます。バックアップ スケジュールが日曜日の午後 0:00 に開始して月曜日の午後 0:00 に終了する場合、週次の長期保存の目的が毎週日曜日に繰り返すよう設定されます。PowerProtect Data Manager によって、日曜日の午後 0:00 から月曜日の午後 0:00）が長期保存用に選択されます。

長期保存バックアップのレプリケーション

レプリケーション目的を長期保存バックアップに追加して、レプリケーション目的で選択したフル プライマリー バックアップの保存期間を変更できます。長期保存目的のルールにより、選択したフル プライマリー バックアップが定義されます。長期保存バックアップのレプリケーションに関する次の情報を確認します。

- 長期保存バックアップのレプリケーションを構成する前に、プライマリー バックアップのレプリケーション目的を作成します。
- 長期保存のレプリケーション目的を構成し、プライマリー バックアップに基づいてこの目的を既存レプリケーション目的のいずれかと一致させます。長期保存レプリケーション目的またはプライマリー バックアップのレプリケーション目的にある、新規または既存のストレージ ユニットに対する変更は、両方のレプリケーション目的に適用されます。
- 長期保存バックアップのレプリケーション目的では、レプリケートされたバックアップ コピーの保存期間のみが更新されます。新しいバックアップ コピーは、レプリケーション ストレージには作成されません。

保護された資産の手動バックアップ

保護ポリシーに資産を追加すると、PowerProtect Data Manager UI の［今すぐ保護］機能を使用して、手動バックアップを実行できます。

このタスクについて

［保護］ > ［保護ポリシー］ウィンドウの単一手動バックアップを使用して、指定された保護ポリシーで保護されている複数の資産をバックアップできます。保護ポリシーは有効または無効にすることができますが、その目的を［Exclusion］にしたり、［Self-Service Protection］にしたりすることはできません。

仮想マシンがアプリケーション対応保護ポリシーの一部である場合、手動バックアップはアプリケーションに対応したフル バックアップになります。

手動バックアップは、親保護ポリシーの他の構成済み目的（レプリケーション、クラウド階層、Cloud DR）によって管理されます。保存ロック、ストレージ ターゲット、クォータ、ネットワーク インターフェイスなどその他のプロパティは、親保護ポリシーから継承されます。この保護ポリシー（レプリケーション、クラウド階層化、Cloud DR など）によって管理されるジョブは、手動バックアップ ジョブが完了した後も引き続き実行されます。

手順

1. 左ナビゲーション ペインで、［Protection］ > ［Protection Policies］の順に選択します。
   ［Protection Policies］ウィンドウが表示されます。
2. バックアップする資産を含む保護ポリシーを選択し、［今すぐ保護］をクリックします。
   ［今すぐ保護］ウィザードが表示されます。
3. ［Assets Selection］ページで、すべての資産をバック アップするか、保護ポリシーで定義されている個々の資産を選択するかを選択して、［Next］をクリックします。
   すべての資産ではなく手動バックアップ用に個別の資産を選択するオプションを選択した場合、［Assets］ページに、選択可能な個々の資産が表示されます。
   a. 手動バックアップに含める資産を選択し、［Next］をクリックして［Configuration］ページを表示します。
   すべての資産のバック アップを選択した場合は、［Configuration］ページが表示されます。
4. ［Configuration］ページで［Back up now］を選択し、使用可能なバックアップ タイプから選択します。
5. デフォルト設定を変更する場合は、保存期間を編集して、［次へ］をクリックします。
   デフォルト設定は、親保護ポリシーのプライマリー バックアップ目的から継承されます。
6. ［トラブルシューティング モードを］選択してデバッグ ログを有効にし、使用するログのレベルを選択できます。
   - ［Info］：ステータスの変更などの情報が含まれます。これは、スケジュール設定されたバックアップとリストアのデフォルトのログ レベルです。
   - ［Debug］：問題の診断に役立つ追加情報
   - ［Trace］：複雑な問題診断のための最も詳細な情報
7. ［Summary］ページで設定を確認し、［Protect Now］をクリックします。
   要求が正常に処理されたかどうかを示す通知が表示されます。

保護された単一資産の手動バックアップ

［インフラストラクチャ］ > ［資産］ウィンドウから手動バックアップを実行することもできますが、一度に 1 個の資産に対してのみ、手動バックアップを実行できます。

このタスクについて

「保護された資産の手動バックアップ」の情報を確認します。保護ポリシーは有効または無効にすることができますが、その目的を［Exclusion］にしたり、［Self-Service Protection］にしたりすることはできません。このタスクでは、選択した資産のフル バックアップを作成します。

手順

1. 左ナビゲーション ペインで、［Infrastructure］ > ［Assets］の順に選択します。
   ［Assets］ウィンドウが表示されます。
2. バック アップする資産タイプのタブを選択します。
   資産のリストが表示されます。
3. 関連づけられている保護ポリシーを持つ資産を表から選択します。
4. ［今すぐバックアップ］をクリックします。
   要求が正常に処理されたかどうかを示す通知が表示されます。

保護された資産の手動レプリケーション

PowerProtect Data Manager UI の［Protect Now］機能を使用して、保護ポリシー内で、1 個以上の保護された資産のレプリケーションを実行できます。レプリケーションには、保護ポリシーまたはこれらの資産のサブセットに定義されているすべての資産を含めることができます。資産を選択した後、すべてのバックアップまたはバックアップのサブセットを複製できます。

前提条件

保護ポリシーの目的を［Exclusion］にすることはできません。また、ポリシーはすでにレプリケーション目的で構成されている必要があります。プライマリー バックアップのレプリケーション目的のみを手動で複製できます。

メモ: VMAX ストレージ グループでは、DD システムから実行およびスケジュール設定された MTree レプリケーションのみをサポートします。したがって、VMAX ストレージ グループの資産の手動レプリケーションはサポートされません。

このタスクについて

バックアップのサブセットを複製すると、レプリケーションのバックログが大きすぎて追いつかない場合に便利です。例えば、デスティネーションが長期間オフラインであった場合や、帯域幅と容量の問題により、使用可能な期間中にフル レプリケーションができなかった場合などです。

バックログが大きすぎる場合は、デスティネーションが確実に最新のバックアップを最初に受け取るようにすることができます。また、選択基準に一致しないほど古いバックアップの将来のレプリケーションをスキップすることで、バックログを削減することもできます。

手順

1. PowerProtect Data Manager UI から、［Protection］ > ［Protection Policies］の順に選択します。
2. レプリケートする資産を含む保護ポリシーを選択し、［Protect Now］をクリックします。
   ［Protect Now］ウィザードが開き、［Assets Selection］ページが表示されます。
3. ［All Assets］を複製するか、資産の［Custom］選択を複製するかを選択します。
   - ［All Assets］を選択した場合は、［Next］をクリックします。
   - ［Custom］を選択した場合は、個々の資産を選択できるリストが表示されます。これらの資産は、ツリー ビューまたはリスト ビューで表示できます。
   a. 手動で複製する資産を選択して、［Next］をクリックします。
   ［Configuration］ページが表示されます。
4. ［Replicate Now］を選択します。
5. ［Storage Name］および［Storage Unit］のドロップダウン リストからデスティネーションのストレージ ターゲットを選択します。
   これらのドロップダウン リストのストレージ システムとストレージ ユニットに関する選択肢は、プライマリー バックアップの関連づけられているレプリケーション目的に対応しています。場合によっては、保護ストレージ システムに、このポリシー用の複数のストレージ ユニットがある場合があります。
   ウィザードは、保護ポリシーからデフォルト設定をロードします。
6. デフォルト設定を変更する場合は次の点に留意します。

- 該当するすべてのバックアップ タイプに対して異なる保存期間を構成することも、すべてのバックアップ タイプに対して同じ保存期間を構成することもできます。
- デフォルトの保存期間設定は、保護ポリシーの対応するレプリケーション目的の設定から継承されます。
- VMDM、ファイル システム、Microsoft Exchange Server、NAS 資産の場合、フル バックアップとシンセティック フル バックアップの保存期間は同じ値にする必要があります。

a. [Set the same retention time for all replicated copies] を選択または選択解除します。
b. 該当するすべてのバックアップ タイプの保存期間を編集します。
c. ⚠記号と✖記号で示されている、競合やエラーを解決します。

7. [All Copies] を複製するか、バックアップの [Custom] サブセットを複製するかを選択します。
   [Custom] を選択した場合は、次のような追加のオプションが表示されます。
   a. 時間範囲内の最新のバックアップを複製するには、最初のオプションを選択し、日数を入力します。
   b. 最近のバックアップに含まれる特定の数を複製するには、2 番目のオプションを選択し、バックアップの数を入力します。
   c. (オプション) この目的のレプリケーション バックログからすべての一致しないバックアップを削除するには、[Do not replicate copies outside the selection and mark them as skipped] を選択します。
      PowerProtect Data Manager によって、この目的による将来のレプリケーション アクティビティーでスキップされたバックアップが除外されます。この決定は永続的であり、ウィザードは確認を求めるプロンプトを表示します。
   選択したバックアップのチェーンがまだ複製されていない場合、結果のアクティビティーは、最後のフル バックアップから選択したバックアップにチェーンを複製します。
   メモ: 依存関係チェーンを持つ資産タイプ (トランザクション ログを含むバックアップなど) のフル バックアップの手動レプリケーションは、依存関係がまだ複製されていない場合でも、フル コピーがすでに複製されている場合はスキップされます。これらの依存関係のいずれかをバックアップ チェーンに複製するには、スケジュール設定されたレプリケーションを待つか、[Custom] オプションの代わりに [All Copies] オプションを選択して手動レプリケーションを実行します。
8. (オプション) [Select Replication] をクリックし、前の手順を繰り返して、追加のレプリケーション ポリシー目的用に手動レプリケーションを構成します。
9. [Next] をクリックします。
10. [Summary] ページで設定を確認し、[Protect Now] をクリックします。
    要求が正常に処理されたかどうかを示す通知が表示されます。

保護された資産の手動でのクラウド階層化

クラウド階層の目的が含まれている保護ポリシーに資産を追加すると、PowerProtect Data Manager UI を使用して、これらの資産について手動での階層化を実行できます。

メモ: コピー セットの手動によるクラウド階層化を行うには、関連づけられている保護ポリシーにクラウド階層の目的が必要です。

オンデマンドで実行するには、クラウド階層化で次の手順を実行します。

1. PowerProtect Data Manager UI から、[Infrastructure] > [Assets] の順に選択します。
2. [Assets] ウィンドウで、階層化する資産タイプのタブを選択します。資産のリストが表示されます。
3. 関連づけられている保護ポリシーがある資産を表から選択し、[View Copies] をクリックします。
   メモ: 一度に 1 個の資産のみを選択できます。また、この資産に関連づけられている保護ポリシーを除外ポリシーにすることはできません。
4. 左側のペインで、資産のアイコンの右にある ⛁ をクリックすると、右側のペインに使用可能なバックアップ コピーが表示されます。
5. バックアップ コピーを選択して、[Tier] をクリックします。要求が正常に処理されたかどうかを示す通知が表示されます。

[Jobs] ウィンドウに移動して、階層化操作の進行状況を監視します。

バックアップ コピーの削除

PowerProtect Data Manager では、保存期間の満了後に行われるバックアップの削除に加えて、保護ストレージからバックアップ コピーを手動で削除できます。

このタスクについて

バックアップ コピーが不要になり、保存ロックが有効になっていない場合は、期限日より前にバックアップ コピーを削除できます。

バックアップ コピー チェーンの指定した部分のみを削除するというバックアップ コピーの削除を実行できます。この削除は、チェーン内の他のバックアップ コピーのリストアを行う機能に影響を与えません。削除する特定のバックアップ コピーを選択した場合は、選択したそのバックアップ コピーと、それに依存するバックアップ コピーのみが削除されます。例えば、フル バックアップ コピーの削除を選択した場合、フル バックアップ コピーに依存する他のバックアップ コピーもすべて削除されます。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Assets］の順に選択します。
2. ［Assets］ウィンドウで削除するコピーの、資産タイプのタブを選択します。ポリシーが割り当てられている場合、表には、検出された資産とともに、関連付けられている保護ポリシーがリスト表示されます。
3. 表から保護対象の資産を選択し、［View Copies］をクリックします。［Copy Locations］ペインでは、バックアップが保存されている場所を識別します。
4. 左ペインで、資産のアイコンの右側にある をクリックします。右ペインの表にバックアップ コピーがリストされます。
5. DD システムから削除する 1 個または複数のコピーを表から選択し、［Delete］をクリックします。

   プレビュー ウィンドウが開き、選択したバックアップ コピーが表示されます。

   メモ: Microsoft SQL Server データベース、Oracle データベース、SAP HANA データベース、アプリケーション対応仮想マシンなど、連結されたバックアップ コピーがある資産については、プレビュー ウィンドウに、指定されたバックアップ コピーに依存するすべてのバックアップ コピーがリスト表示されます。バックアップ コピーを削除すると、PowerProtect Data Manager によって指定したバックアップ コピーと、指定したバックアップ コピーに依存するすべてのバックアップ コピーが削除されます。
6. すべての資産タイプで、最新のバックアップ コピーを保持するか、削除するかを選択できます。デフォルトでは、PowerProtect Data Manager によって最新のバックアップ コピーが保持されます。最新のバックアップ コピーを削除するには、［Include latest copies］の横にあるチェックボックスをオフにします。

   VMAX ストレージ グループのバックアップ コピーの場合は、同じ保護トランザクションにグループ化されているコピーを削除するか、選択したコピーのみを削除するかを選択できます。デフォルトでは、PowerProtect Data Manager によって同じ保護トランザクションでグループ化されたコピーが削除されます。選択したコピーのみを削除するには、［Include copies in the same protection transaction］の横にあるチェックボックスをオフにします。
7. バックアップ コピーを削除するには、プレビュー ウィンドウで、［削除］をクリックします。

   メモ: 削除操作には数分かかる場合があり、元に戻すことはできません。

   コピーが削除されていることを確認するための情報ダイアログ ボックスが開きます。操作の進行状況を監視するには、［Go to Jobs］をクリックします。バックアップ コピーのリストとそのステータスのリストを表示するには、［OK］をクリックします。

   メモ: データの削除が成功してもカタログの削除に失敗した場合、全体的な削除ジョブのステータスは `Completed with Exceptions` と表示されます。

   ジョブが完了すると、各コピーの作成時刻、バックアップ レベル、保存期間など、削除された各バックアップ コピーの詳細がタスク サマリーに表示されます。コピーの作成時刻と保存期間は UTC で表示されます。

   また、監査ログも生成され、そこで各コピーの作成時刻、バックアップ レベル、保存期間など、削除された各バックアップ コピーの詳細を確認できます。コピーの作成時刻と保存期間は UTC で表示されます。［アラート］ > ［監査ログ］に移動して、監査ログを表示します。
8. 保護ストレージからコピーが正常に削除されていることを確認します。削除が成功すると、削除されたコピーが表に表示されなくなります。

失敗したバックアップ コピー削除の再試行

バックアップ コピーが正常に削除されない場合は、手動で操作を再試行できます。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Assets］の順に選択します。
2. ［Assets］ウィンドウで削除するコピーの、資産タイプのタブを選択します。ポリシーが割り当てられている場合、表には、検出された資産とともに、関連付けられている保護ポリシーがリスト表示されます。
3. 表から保護対象の資産を選択し、［View Copies］をクリックします。［Copy Locations］ペインでは、バックアップが保存されている場所を識別します。
4. 左ペインで、資産のアイコンの右側にある をクリックします。右ペインの表にバックアップ コピーがリストされます。
5. ステータスが［Deletion Failed］となっている 1 個または複数のバックアップ コピーを表から選択し、［Delete］をクリックします。

   他にも、［Copy Status］列のステータスで、バックアップ コピーのリストを絞り込んだり、並べ替えたりできます。

   選択したバックアップ コピーを削除するかどうかを確認する警告が、システムによって表示されます。
6. ［OK］をクリックします。

コピーが削除されていることを確認するための情報ダイアログ ボックスが開きます。操作の進行状況を監視するには、［Go to Jobs］をクリックします。バックアップ コピーのリストとそのステータスのリストを表示するには、［OK］をクリックします。

7. コピーが保護ストレージから正常に削除されたことを確認します。削除が成功すると、削除されたコピーが表に表示されなくなります。

削除された Oracle、SAP HANA、Storage Direct バックアップ コピーのデータのエクスポート

このオプションにより、削除したバックアップ コピー結果を .csv ファイルにエクスポートし、Excel ファイルとしてそのデータのダウンロードができるようになります。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Assets］の順に選択します。
2. ［Assets］ウィンドウで、削除したバックアップ コピー結果のエクスポートを行う資産タイプのタブを選択します。ポリシーが割り当てられている場合、表には、検出された資産とともに、関連付けられている保護ポリシーがリスト表示されます。
3. テーブルから 1 個以上の保護資産を選択してから、［More Actions］ > ［Export Deleted Copies］の順に選択します。
   資産を選択しない場合、PowerProtect Data Manager によって特定の資産タイプの資産すべてについて、削除されたバックアップ コピーに関するデータのエクスポートが行われます。
4. エクスポートに関する次のフィールドを指定します。
   a. ［Time Range］
      デフォルト値は［Last 24 Hours］です。
   b. ［Copy Status］
      削除されたバックアップ コピーに関するデータのエクスポートを行うには、バックアップ コピーが次のいずれかの状態になっている必要があります。
      - ［Deleted］：コピーが保護ストレージから正常に削除され、対応する場合は、エージェント カタログがエージェント ホストから正常に削除されます。
      - ［Deleting］：コピーの削除が進行中です。
      - ［Deletion Failed］：保護ストレージからのコピーの削除に失敗しました。
      - ［Deletion Failed (Agent Catalog)］：コピーは保護ストレージから正常に削除されていますが、エージェント ホストからは削除されていません。
        メモ: この状態は、仮想マシンおよび Kubernetes のバックアップ コピーには適用されません。

      メモ: ［Available］状態にあるバックアップ コピーに関するデータのエクスポートは行うことができません。
5. ［Download］をクリックします。
   該当する場合、csv ファイルを保存する場所を選択するためのナビゲーション ウィンドウが表示されます。csv。
6. 目的の場所に .csv ファイルを保存した後、［Save］をクリックします。

Exchange、ファイル システム、Kubernetes、ブロック ボリューム、SQL バックアップ コピーの PowerProtect Data Manager データベースからの削除

このオプションを使用すると、PowerProtect Data Manager のデータベースからバックアップ コピー レコードを削除できますが、バックアップ コピーは保護ストレージに保持されます。

このタスクについて

保護ストレージから削除できなかったバックアップ コピーは、PowerProtect Data Manager データベースから削除することができます。PowerProtect Data Manager からバックアップ コピーを削除しても、保護ストレージにあるコピーは削除されません。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Assets］の順に選択します。
2. ［Assets］ウィンドウで削除するコピーの、資産タイプのタブを選択します。ポリシーが割り当てられている場合、表には、検出された資産とともに、関連付けられている保護ポリシーがリスト表示されます。
3. 表から保護対象の資産を選択し、［View Copies］をクリックします。［Copy Locations］ペインでは、バックアップが保存されている場所を識別します。

4. 左ペインで、資産のアイコンの右側にある をクリックします。右ペインの表にバックアップ コピーがリストされます。
5. ステータスが［Deletion Failed］となっている 1 個以上のバックアップ コピーを表から選択し、［Remove from PowerProtect］をクリックします。
選択したバックアップ コピーを削除するかどうかを確認する警告が、システムによって表示されます。
6. ［OK］をクリックします。
コピーが削除されていることを確認するための情報ダイアログ ボックスが開きます。操作の進行状況を監視するには、［Go to Jobs］をクリックします。バックアップ コピーのリストとそのステータスのリストを表示するには、［OK］をクリックします。
7. コピーが PowerProtect Data Manager のデータベースから削除されていることを確認します。削除が成功すると、削除されたコピーが表に表示されなくなります。バックアップ コピーは保護ストレージに残ります。

期限切れのバックアップ コピーの削除

PowerProtect Data Manager では、コピーの保存期間の期限が切れると、資産のバックアップ コピーが自動的に削除されます。

保護ポリシー目的の保存期間を指定する方法については、各資産タイプのユーザー ガイドを参照してください。

期限切れのコピーを削除するには、次のいずれかの状態で、PowerProtect Data Manager によって資産を管理する必要があります。

- ［Exclusion］：資産は除外保護ポリシーに割り当てられています。
- ［Disabled］：資産は無効な保護ポリシーに割り当てられています。
- ［Protected］：資産は有効な保護ポリシーに割り当てられています。
- ［Previously Protected］：資産は保護ポリシーから割り当て解除されており、別のポリシーに再割り当てされていないか、除外ポリシーに割り当てられています。

除外または無効化された保護ポリシーのいずれかに割り当てられた資産の場合、次の設定が「**true**」に設定されていると、PowerProtect Data Manager が資産の期限切れのバックアップ コピーを削除します。

- `expiredCopyDeletionEnabledForAssetInExclusionPolicy`
- `expiredCopyDeletionEnabledForAssetInDisabledPolicy`

除外ポリシー、および無効化された保護ポリシーの期限切れコピーの削除設定は、デフォルトで「**true**」に設定されています。いずれかの設定が「**false**」に設定されている場合、PowerProtect Data Manager は期限切れのバックアップ コピーの削除をスキップします。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。

期限切れのコピーのクリーンアップは、毎日午前 0 時（UTC）に実行されます。コピーの削除に失敗した場合、［Alerts］ > ［System］にある監査ログに警告アラートが表示されます。

[[ジョブ]] ウィンドウから、期限切れコピーの削除ジョブの進行状況を監視できます。

PowerProtect Data Manager からの資産の削除

PowerProtect Data Manager は、特定の条件が満たされた場合に資産を自動的に削除します。ただし、一部の資産は手動で削除できます。

次の条件が満たされた場合、資産は自動的に削除されます。

- 資産のステータスが［Deleted］である。
- 資産にバックアップ コピーがない。
- 資産が資産の TTL 設定の値よりも長い間存在している。デフォルトでは *0* 分ですが、REST API を使用して変更できます。詳細については、「PowerProtect Data Manager Public REST API のドキュメント」を参照してください。
  メモ: この値は、PowerProtect Data Manager の以前のバージョンの値から変更されました。

資産を手動で削除すると、次のようにプロセスの制御が向上します。

- 資産をオン デマンドで削除できます。
- 資産のステータスを［Not Detected］にすることができます。
- 複製されたコピーやクラウド階層型のコピーなど、資産のすべての保護コピーを手動で削除すると、資産を手動で削除できます。
- PowerProtect Data Manager から手動で資産を削除する際にこのオプションを選択した場合、資産のすべての保護コピーを自動的に削除できます。

資産と関連する保護コピーの削除

PowerProtect Data Manager UI では、スケジュール設定された削除が行われる前に一部の資産を手動で削除したり、自動的に削除されていない資産を削除したりできます。

前提条件

- 資産のステータスが［Deleted］または［Not Detected］です。
- 資産に保護コピーがない。資産のストレージ システムにコピーがまだ存在する場合は、この前提条件の手順に従う前に、これらのコピーを削除するか、資産が削除されたときにコピーを自動的に削除するオプションを選択できます。バックアップ コピーの削除の詳細については、「バックアップ コピーの削除」を参照してください。

手順

1. ［インフラストラクチャ］ > ［Assets］を選択します。
2. 削除する資産のタイプに対応するタブを選択します。例えば、vCenter 仮想マシン資産の場合であれば、［Virtual Machine］をクリックします。
   このタイプの保護コピーに関連づけられている資産が一覧表示されます。デフォルトでは、ステータスが［Available］または［Not Detected］の資産のみが表示されます。名前で資産を検索することもできます。
3. リストから 1 個または複数の資産を選択します。［More Actions］ > ［Remove Asset］をクリックします。
   ［Remove Assets］ダイアログが表示されます。
4. 以下オプションのいずれかを選択してください。

   メモ: 選択した資産に対して、これらのオプションがすべて表示されない場合があります。使用可能なオプションは、選択した資産の保護コピーのステータスによって異なります。

   - ［Remove assets and associated protection copies］：これらの資産を PowerProtect Data Manager から削除し、これらの資産の保護コピーをストレージから自動的に削除します。
   - ［Only remove assets with no associated protection copies］：PowerProtect Data Manager がこれらの資産の保護コピーがストレージ システムにまだ存在することを検出した場合、これらの資産は削除されません。
   - ［Mark "Not Detected" assets as "Deleted" but keep associated protection copies］：PowerProtect Data Manager UI では、ステータスが［Not Detected］の資産を［Deleted］としてマークしますが、これらの資産の保護コピーはストレージ システムに保持されます。［Infrastructure］ > ［Assets］ペインで、［Deleted］としてマークされた資産が表示されます。
5. ［OK］をクリックして、資産の削除を確定します。

クライアント ホスト名変更後のクライアント資産の保護

クライアントのホスト名が変更され、何もアクションを実行しないと、その資産は保護されなくなります。

クライアントのホスト名を変更する場合は、既存のロックボックス ファイルを削除し、新しいロックボックス ファイルを生成する必要があります。詳細については、関連するアプリケーション エージェントのドキュメントを参照してください。

ifGroup の構成と PowerProtect Data Manager のポリシー

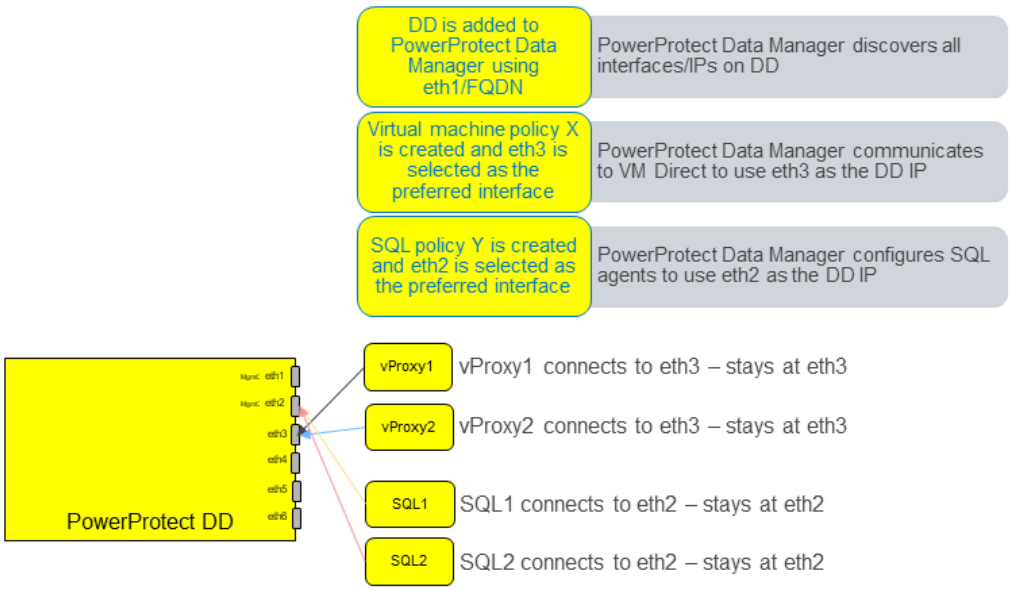
`ifGroup` が DD で構成されている場合、PowerProtect Data Manager 保護ポリシーで選択された IP アドレスは最初の接続にのみ使用され、リダイレクト（ロード バランシングなど）は DD の `ifGroup` 設定に従って行われます。DD 上の LACP およびその他のフェールオーバー オプションは、PowerProtect Data Manager ポリシーで選択されているものとは独立して機能します。

次の例と図は、`ifGroup` が DD で構成されている場合の PowerProtect Data Manager の一般的なシナリオを示しています。

次がない場合の PowerProtect Data Manager ポリシー： `ifGroup`

DD 構成：

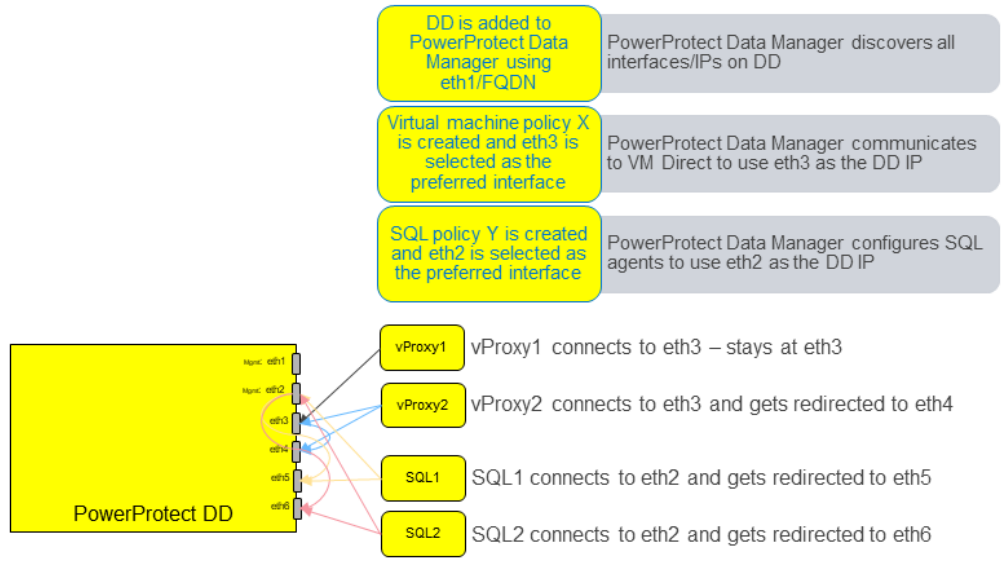
- eth1/eth2 1G
- eth3/eth4/eth5/eth6 10G
- IfGroup なし



次が 1 個ある場合の PowerProtect Data Manager ポリシー： `ifGroup`

DD 構成：

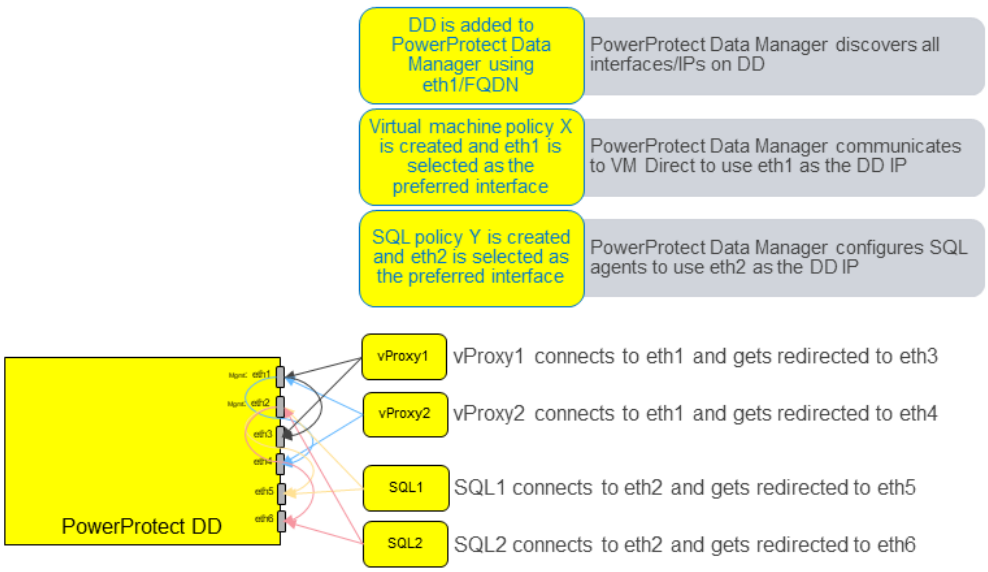
- eth1/eth2 1G
- eth3/eth4/eth5/eth6 10G
- ifGroup * eth3/eth4/eth5/eth6



次が複数ある場合の PowerProtect Data Manager ポリシー： `ifGroups`

DD 構成：

- eth1/eth2 1G
- eth3/eth4/eth5/eth6 10G
- ifGroup VLAN-VM eth3/eth4
- ifGroup VLAN-SQL eth5/eth6



失敗したレプリケーション ジョブのトラブルシューティング

以下のセクションでは、レプリケーション ジョブが失敗した場合のトラブルシューティングについて説明します。

DD システムへのレプリケーションが認証エラーで失敗する

レプリケーション ジョブが、次のエラーで失敗する場合があります。

```
The backup copies cannot be replicated because the username and password for the source
storage system are not valid or cannot be detected.
```

この障害は断続的に発生する可能性がありますが、ほとんどのバックアップ ジョブとレプリケーション ジョブは障害なく完了して、DD システムが正常に検出されます。

この問題を解決するには、以下の手順を実行してください。

1. DD サポート バンドルを収集し、`/ddvar/log/messages` で `Failed password` または `Invalid user` を検索します。
   メモ: サポート バンドルの収集手順については、『*DDOS* 管理ガイド』を参照してください。
2. 検索するテキストが見つかった場合は、次のようなエントリーが表示されます。

```
Oct 15 16:36:26 <DD hostname> sshd[25116]: Failed password for sysadmin from <IP address>
port 55351
Oct 11 11:18:00 <DD hostname> sshd[31750]: Invalid user <username> from <IP address> port
64425
```

3. `<IP address>`を使用して資産ソース ホストを見つけ、DD システムへの接続に使用している認証情報を修正します。

DD システムへのレプリケーションが証明書エラーで失敗する

レプリケーション ジョブが次のようなエラーで失敗する場合があります。

```
error = I/O error on POST request for "https://<DD-System>:3009/rest/v1.0/auth": PKIX path
building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target; nested exception is
javax.net.ssl.SSLHandshakeException: PKIX path
```

メモ: この例では、<DD_System>がレプリケーション DD システムのホスト名に置き換えられます。

このエラーは、DD システムの PowerProtect Data Manager に保存されている証明書の有効期限が過ぎているか、破損しているか、見つからないことを示します。

証明書を再生成するには、次の手順を実行します。

1. 必要に応じて、カスタマー サポートに連絡して `ppcp` を入手します。

   メモ: この `ppcp` ツールは、PowerProtect Data Manager では導入されていません。別途取得する必要があります。
2. 管理者認証情報を使用して PowerProtect Data Manager サーバー コンソールにログインし、root ユーザーに変更します。
3. ディレクトリーを `ppcp` ツールのある場所に変更します。
4. コマンド `./ppcp rest --uri certificates --params "host=<DD_System>&port=3009&type=HOST"` を実行し、*<DD_System>* を DD システムのホスト名に置き換えます。
5. 次のようなコマンド出力の `"id"` の直後にある引用符で囲まれた *id* の値を記録します。

```
"fingerprint":"473303EFF3EFE6D6AAC2D76F1FB94561B12A321F","host":"<DD_System>","id":"ZG1vYms
tcGRiMDAwMS1wLmQuaW50LmluZnJhLjdhbmRpLmNvLmpwOjMwMDk6aG9zdA==","issuerName":"CN=<DD_System>
, OU=Root CA, O=Valued Datadomain Customer, L=Santa Clara, ST=CA,
C=US","notValidAfter":"Sun Dec 07 15:28:39 JST 2025","notValidBefore":"Mon Dec 09 00:28:39
JST 2019","port":"3009","state":"UNKNOWN","subjectName":"CN=<DD_System>, O=Valued
DataDomain customer, OU=Host Certificate, ST=CA, C=US","type":"HOST"
```

   メモ: この例では、*id* の値は `ZG1vYmstcGRiMDAwMS1wLmQuaW50LmluZnJhLjdhbmRpLmNvLmpwOjMwMDk6aG9zdA==` です。
6. 次のコマンドを実行して、証明書の状態を `UNKNOWN` から `ACCEPTED` に変更します。
   - ステップ 5 で記録した *Id* の値を使用します。*id* の値は、`certificates/` の直後に入力します。
   - `UNKNOWN` から `ACCEPTED` に変更する場合を除き、ステップ 4 でのコマンド出力を `{` と `}` の間にコピーします。
   - *<DD_System>* を DD システムのホスト名に置き換えます。
   - このコマンドは、1 行のテキストとして入力します。

```
./ppcp rest --method PUT --uri certificates/
ZG1vYmstcGRiMDAwMS1wLmQuaW50LmluZnJhLjdhbmRpLmNvLmpwOjMwMDk6aG9zdA== --data
'{"fingerprint":"473303EFF3EFE6D6AAC2D76F1FB94561B12A321F","host":"dmobk-pdb0001-
p.d.int.infra.7andi.co.jp","id":"ZG1vYmstcGRiMDAwMS1wLmQuaW50LmluZnJhLjdhbmRpLmNvLmpwOjMwMD
k6aG9zdA==","issuerName":"CN=dmobk-pdb0001-p.d.int.infra.7andi.co.jp, OU=Root CA, O=Valued
Datadomain Customer, L=Santa Clara, ST=CA, C=US","notValidAfter":"Sun Dec 07 15:28:39 JST
2025","notValidBefore":"Mon Dec 09 00:28:39 JST
2019","port":"3009","state":"ACCEPTED","subjectName":"CN=dmobk-pdb0001-
p.d.int.infra.7andi.co.jp, O=Valued DataDomain customer, OU=Host Certificate, ST=CA,
C=US","type":"HOST"}'
```

7

データおよび資産のリストア

トピック：

リストアに利用できるバックアップ コピーの表示

保護ポリシーが正常にバックアップされると、PowerProtect Data Manager に、資産のバックアップを含むストレージ システムの名前、場所、作成と有効期限の日付、およびサイズなどの詳細が表示されます。バックアップの概要を表示するには、次のようにします。

手順

1. PowerProtect Data Manager UI から、［Infrastructure］ > ［Assets］または［リストア］ > ［Assets］を選択します。
2. 表示する資産に対応するタブをクリックします。例えば、vCenter 仮想マシン資産の場合であれば、［Virtual Machine］をクリックします。
   このタイプの保護コピーに関連づけられている資産が一覧表示されます。デフォルトでは、ステータスが［Available］または［Not Detected］の資産のみが表示されます。名前で資産を検索することもできます。

   仮想マシンの場合は、［File Search］ボタンをクリックして、特定の基準を検索することもできます。

   メモ: ［リストア］ > ［Assets］ウィンドウでは、PowerProtect Data Manager の表示内のリストアでサポートされている資産タイプのタブのみが表示されます。サポートされている資産のタイプは次のとおりです。
   - ［Virtual Machine］
   - ［ファイル システム］
   - ［Storage Group］
   - ［Kubernetes］
   - ［ネットワーク接続型ストレージ(NAS)］
   - ［Oracle］
   - ［SQL］
   - ［ブロック ボリューム］
3. 詳細を表示するには、資産を選択し、［View copies］をクリックします。
   コピー マップは、ルート ノードとその子ノードで構成されます。左ペインのルート ノードは資産を表し、コピーの場所に関する情報が右側のペインに表示されます。子ノードは、ストレージ システムを表します。

   子ノードをクリックすると、右ペインに次の情報が表示されます。

   - コピーが格納されているストレージ システム。
   - コピーの数
   - 各コピーの詳細（各コピーの作成時刻、整合性レベル、コピーのサイズ、バックアップ タイプ、コピー ステータス、保存時間を含む）。
   - コピー作成時の各コピーのインデックス作成ステータス：
     - ［Success］は、すべてのファイルまたはディスクのインデックスが正常に作成されたことを示します。
     - ［Partial Success］は、一部のディスクまたはファイルのみインデックスが作成され、ファイル検索時に部分的な結果が返される可能性があることを示します。
     - ［Failed］は、すべてのファイルまたはディスクでインデックスが作成されていないことを示します。
     - ［In Progress］は、インデックス作成ジョブが進行中であることを示します。

バックアップ コピーに対するインデックス作成が未構成の場合や、グローバル期限が構成されていて、バックアップ コピーの有効期限が切れる前にインデックス付きのディスクまたはファイルが削除された場合、［File Indexing］列には［N/A］と表示されます。

インデックス作成ステータスのアップデートは定期的に行われるため、最新のステータスを表示できます。

- 仮想マシンのバックアップの場合は、［Disk Excluded］列を使用して、バックアップから除外されたすべての仮想ディスク(VMDK)を表示することができます。

保護ポリシーのリストア

PowerProtect Data Manager ユーザー インターフェイスを使用して、次のいずれかの資産タイプで保護ポリシー バックアップの一元化されたリストアとセルフサービス リストアを実行できます。詳細については、該当するドキュメントを参照してください。

表 27. 保護ポリシーの資産タイプ

資産タイプ	ドキュメント名
ファイル システム データ	*PowerProtect Data Manager* ファイル システム ユーザー ガイド
Kubernetes クラスター ネームスペースと PVC	*PowerProtect Data ManagerKubernetes* ユーザー ガイド
Microsoft Exchange Server データベース	*PowerProtect Data ManagerMicrosoft Exchange Server* ユーザー ガイド
Microsoft SQL Server データベース	*PowerProtect Data ManagerMicrosoft SQL Server* ユーザー ガイド
ネットワーク接続型ストレージ (NAS)共有とアプライアンス データ	*PowerProtect Data Manager* ネットワーク接続型ストレージ ユーザー ガイド
Oracle RMAN データベース	*PowerProtect Data ManagerOracle RMAN* ユーザー ガイド
SAP HANA データベース	*PowerProtect Data ManagerSAP HANA* ユーザー ガイド
Storage Direct の VMAX ストレージ グループ	*PowerProtect Data ManagerStorage Direct* ユーザー ガイド
仮想マシン	*PowerProtect Data Manager* 仮想マシン ユーザー ガイド
ブロック ボリューム	*PowerProtect Data Manager* ストレージ アレイ ユーザー ガイド

PowerProtect Data Manager サーバーのリストア

任意のバックアップを使用して、PowerProtect Data Manager サーバーの保全データを新しいインスタンスとしてリストアできます。リストアを実行できるのは管理者ロールのみです。

前提条件

次の事項を確認：

- システムにデプロイされている PowerProtect Data Manager のバージョンと、リストアに使用しているバックアップが一致します。
- リストア対象の障害が発生したインスタンスと、新しく展開された PowerProtect Data Manager システムとでネットワーク構成が同じです。

手順

1. PowerProtect Data Manager OVA を展開し、電源をオンにします。
2. ［Restore Backup］を選択します。

   指定するまで、保護ポリシーによって定義されているジョブを遅延させるには、［After restore, keep the product in recovery mode so that scheduled workflows are not triggered］を選択します。選択すると、復元後にシステムがリカバリー メンテナンス モードに入ります。リカバリー メンテナンス モード中は、次のようになります。

   - バックアップ ストレージを変更する保護ポリシーによって定義されているすべてのジョブ（バックアップの作成、バックアップの削除、および PowerProtect Data Manager Server DR のジョブなど）は、トリガーされません。
   - バックアップ ストレージに書き込むすべての操作は無効になります。

- システム アラートは PowerProtect Data Manager に表示されます。

自動的にスケジュール設定された操作とバックアップ ストレージに書き込むユーザー操作を有効にするには、アラートの［Return to full Operational mode］をクリックします。

3. 以下のストレージ情報を指定します。
   a. リカバリー バックアップが保存されている DD システムの IP。
   b. リカバリー バックアップが保存されている DD の NSF エクスポート パス。
   c. ［Connect］をクリックします。
4. リストアする PowerProtect Data Manager インスタンスを選択し、［OK］をクリックします。
5. リカバリーに使用するバックアップ ファイルを選択し、［リカバリー］をクリックします。
6. バックアップに関連付けられている Lockbox パスフレーズを指定し、リカバリーを開始します。
   このステップでリカバリーが開始され、進行状況が表示されます。リカバリー プロセスは、URI が PowerProtect Data Manager のログインにリダイレクトされるまでに約 8 分かかる場合があります。

タスクの結果

PowerProtect Data Manager サーバーがリカバリーされます。

次の手順

リカバリーの成功後：

- PowerProtect Data Manager インスタンスのタイムゾーンは、バックアップと同じものに設定されます。
- プリロードされたすべてのアカウントは、*PowerProtect Data Manager* セキュリティ構成ガイドに説明されているように、デフォルトのパスワードにリセットされます。例外として、プリロードされた UI 管理者アカウントのパスワードは保持されます。できるだけ早く、すべてのプリロードされたアカウントのパスワードを変更してください。

クラウド階層バックアップの保護ストレージへのリストア

クラウド階層のバックアップをリコールすると、これらのバックアップのリストア操作は通常のリストア操作と同じになります。

PowerProtect Data Manager ソフトウェアは、クラウド ユニットから保護ストレージのローカル（アクティブな）階層にバックアップ コピーのリコールを行い、アクティブな階層からクライアントにバックアップのリストアを行えるようにします。ステータスは［Cloud］と表示され、クラウドからのリコールが完了すると［Local Recalled］に変わります。リストア後、バックアップ コピーはクラウド階層から削除され、保護ストレージのアクティブな階層に少なくとも 14 日間保存されます。その後は、保護ポリシーに応じてバックアップがクラウドに戻される場合があります。

クラウド階層からのリコールとリストア

保護ストレージのアクティブ階層にクラウド階層のバックアップをリコールして、このバックアップをリストアするには、次の手順を実行します。

前提条件

メモ: クラウド階層からアクティブ階層にバックアップをリコールすると、そのコピーがクラウド階層から削除されます。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［資産］の順に選択します。
2. ［Assets］ウィンドウで、クラウド階層からリコールする資産を含むタブを選択し、［View Copies］をクリックします。
3. ［DD］をクリックして、表に表示されている利用できるコピーのいずれかを選択します。
4. ［Recall］をクリックします。
   「［Recall from Cloud］」ダイアログ ボックスが表示されます。
5. ［Retain until］ボックスで、アクティブ階層にコピーを保存する期間を指定し、［OK］をクリックします。
6. 「［Jobs］」ウィンドウに移動して、リコール操作を監視します。

コピーが正常に移動されると、［Location］が［Cloud］から［Local］に変わります。

7. ［リストア］ > ［Assets］を選択して、リコールした資産を含むタブを選択します。
8. リコールした資産を選択し、［Restore］をクリックします。

   メモ: 資産のリコールが行われたかどうか不明な場合は、［View Copies］をクリックし、［DD］を選択して、利用できるバックアップ コピーを表示してください。リコールしたコピーが資産のバックアップの場合は、ステータス列に［Local Recalled］と表示されます。

9. リコールしたコピーを選択して、コピーをアクティブ階層に再階層化します。

8

災害対策と災害復旧

トピック：

サーバー ディザスター リカバリーについて

PowerProtect Data Manager のシステム保護サービスでは、一連のサーバー ディザスター リカバリー(DR)バックアップを作成することにより、致命的な損失から PowerProtect Data Manager システムの永続的なデータを保護する機能を提供できます。

サーバー DR の準備には、PowerProtect Data Manager サーバーの損失とサイト全体の損失という 2 種類のシナリオを考慮する必要があります。サーバー DR 構成処理中に記録する情報の一部は、どちらか一方のシナリオにのみ適用される場合があります。ベスト プラクティスとして、両方のシナリオに該当するすべての情報を収集して記録する必要があります。

PowerProtect Data Manager は、3 種類のサーバー DR 方式をサポートしています。

システム リカバリー

システム リカバリーは、保護ストレージで PowerProtect Data Manager サーバーのポイントインタイム スナップショットを作成します。DR アクティビティー中に、保護ストレージからサーバーをリカバリーしてから、保護対象資産をリストアします。

サーバー DR のシステム リカバリー で詳細を参照してください。

クイック リカバリー

クイック リカバリーによって、リモートの PowerProtect Data Manager レプリケーション デスティネーションに複製されたバックアップが認識され、リカバリー ビューが有効になります。DR アクティビティー中は、最初にソース サーバーをリストアすることなく、デスティネーションでこれらの複製されたバックアップから資産をリストアできます。

サーバー DR のクイック リカバリー で詳細を参照してください。

Cloud Disaster Recovery

Cloud DR を使用すると、サポートされているパブリック クラウド環境の DR サイトにリストアできます。DR アクティビティー中に、仮想マシンを Cloud DR サーバーにリストアし、クラウド内のワークロードをリカバリーします。

PowerProtect Data Manager クラウド ディザスター リカバリーの概要 で詳細を参照してください。

サーバー DR 方式の違い

次の表は、3 種類のサーバー DR 方式の違いを明確に示しています。

表 28. サーバー DR の比較

基準	システム リカバリー	クイック リカバリー	Cloud DR
別の実行中の PowerProtect Data Manager サーバーが必要	不可 [a]	可	不可
セットアップ後に追加の構成が必要	オプション [b]	不可	不可

表 28. サーバー DR の比較 （続き）

基準	システム リカバリー	クイック リカバリー	Cloud DR
リカバリー中に PowerProtect Data Manager UI 以外の構成が必要	可	不可	不可
バックアップ ワークフローを保持	可	不可	不可
サーバー DR レプリケーションをサポート	可	自動	自動
バックアップ インフラストラクチャの目標リカバリー時間(RTO)	>1 時間 [a]	N/A	N/A

a. 必要に応じて、2 台目のサーバーを構成し、このサーバーを未構成のままにして、システム リカバリーの RTO を減らすことができます。ただし、システム リカバリーの RTO は、クイック リカバリーまたは Cloud DR の RTO と一致しません。
b. サーバー DR レプリケーションの構成。

サーバー DR のシステム リカバリー

システム リカバリー プロセスでは、PowerProtect Data Manager サーバーの定期的なバックアップが作成され、そのバックアップから災害後にサーバーをリストアできます。増分方式で作成されている場合でも、各バックアップはフル バックアップと見なされます。

システム リカバリー バックアップには、ロックボックス、PowerProtect Data Manager データベースなどの永続的なデータが含まれます。バックアップ オペレーションはサーバーを停止し、データベースのポイントインタイム スナップショットを作成します。この停止状態により、ユーザーの機能は制限されます。スナップショットの作成の完了後は、PowerProtect Data Manager で保護ストレージにスナップショットをコピーしている間に、サーバーでのユーザーの機能は完全に回復します。システム リカバリー バックアップには、ファイル検索インデックスやその他のコンポーネント DR バックアップも含まれます。

システム保護サービスでは、自動サーバー DR バックアップの頻度と保存期間を管理できます。手動バックアップを実行することもできます。ただし、システム保護サービスは手動バックアップの保存期間を管理しないため、古い手動バックアップは自分で削除する必要があります。 PowerProtect Data Manager サーバー DR バックアップの管理 で手順を参照してください。

1 個の保護ストレージ システムをサーバー DR バックアップ ターゲットとして選択し、もう 1 個の保護ストレージ システムをレプリケーション ターゲットとして選択できます。レプリケーションによって、サーバー DR バックアップ用に追加の保護レイヤーが提供されます。 サーバー DR バックアップの手動構成 にサーバー DR レプリケーションを構成する手順が記載されていますが、「サーバー DR バックアップからの PowerProtect Data Manager のリカバリー」にはレプリカからリストアをする手順が記載されています。

一度にサポートされるのは、1 個のバックアップ ターゲットと 1 個のレプリケーション ターゲットのみであるため、新しい保護ストレージ システムを指定すると、既存の選択内容が上書きされます。保護ストレージ システムの数が多い場合は、どの保護ストレージ システムでサーバー DR バックアップを保持するか、レプリカを受信するかを変更できます。

PowerProtect Data Manager のサーバー DR レプリケーションは、従来の方法（個々の DD システムでの MTree レプリケーションなど）に依存していません。従来の方法によるバックアップと構成は、検出されたり移行されたりしません。

サーバー DR 保護ストレージタイプ

PowerProtect Data Manager は、NFS と DD Boost の 2 種類のサーバー DR 用保護ストレージをサポートしています。

DD Boost は、PowerProtect Data Manager サーバー DR に推奨されるストレージ タイプです。NFS は、PowerProtect Data Manager サーバー DR のレガシー ストレージ タイプです。

PowerProtect Data Manager サーバーをアップデートしても、ストレージ タイプが自動的に変更されることはありません。代わりに、適切なストレージ タイプを選択し、サーバー DR バックアップを手動で構成します。ストレージ タイプは切り替えないでください。

NFS から DD Boost に切り替えることで、既存のバックアップを移行するのではなく、新しいサーバー DR バックアップを作成します。以前の NFS バックアップは、DR バックアップのリストに表示されなくなります。ただし、最初の DD Boost システムのバックアップが完了する前に災害が発生した場合は、DD Boost に切り替えた後でも、古い NFS サーバーの DR バックアップからリカバリーできます。

DD Boost

DD Boost には、パスワードで保護された認証など、NFS よりもセキュリティと効率性の面で利点があります。DD Boost を使用すると、PowerProtect Data Manager によって DD システム上のストレージ ユニットと対応するユーザー アカウントが作成および管理されます。

- ストレージ ユニットとユーザー アカウント名は、PowerProtect Data Manager のホスト名に基づいています。例えば、`SysDR_<hostname>`のようになります。
- DD Boost のユーザー パスワードは、PowerProtect Data Manager の事前に定義された管理者アカウントの(`admin`)パスワードに基づいています。

メモ: パスワードは、外部 ID プロバイダーユーザーなどの管理者ロールを持つ他のアカウントを使用して PowerProtect Data Manager を管理する場合でも、`admin` アカウントに基づいています。

事前に定義された PowerProtect Data Manager 管理者のパスワードを変更すると、対応する DD Boost のユーザー パスワードのアップデート プロンプトが表示されます。サーバー DR レプリケーションを構成した場合、パスワードの変更により、レプリケーション ターゲット上の認証情報についても対応するアップデートが求められます。サーバー DR バックアップからのリカバリーには、事前に定義された PowerProtect Data Manager 管理者のパスワードが必要です。このパスワードがわからない場合は、カスタマー サポートにお問い合わせください。

DD Boost を使用する予定がある場合は、サーバー DR を構成する前に、DD システムを保護ストレージとして追加します。 保護ストレージ で手順を参照してください。

DD Boost ストレージ タイプでは、サーバー DR の自動構成が可能です。 自動サーバー DR で詳細を参照してください。

DD Boost ストレージ タイプのみでサーバー DR レプリケーションがサポートされています。

NFS

NFS を介してバックアップを保存するには、PowerProtect Data Manager システム用のプライベート ストレージ ユニットを構成して割り当てる必要があります。次に、NFS エクスポートを作成して DD リカバリー ターゲットを準備します。DD システム アドレスと NFS エクスポート パスを使用すると、サーバー DR バックアップを実行するように PowerProtect Data Manager を構成できます。

NFS ストレージは、DD Boost を優先して廃止されました。

自動サーバー DR

PowerProtect Data Manager の新規導入では、最小限の入力でサーバー DR を自動的に構成し、有効化できます。この処理により、保護ストレージを追加するとすぐにサーバーが確実に保護されます。

自動サーバー DR は、保護ストレージ システムを初めて追加したときに検出を行います。自動構成メカニズムでは、推奨される DD Boost ストレージ タイプとデフォルト設定を使用して、サーバー DR 用の管理対象ストレージ ユニットを作成します。この処理では、[Jobs] ページで追跡できるサーバー DR ジョブが生成されます。

自動構成では、最初に PowerProtect Data Manager に追加する保護ストレージ システムを選択します。ただし、ターゲットを別の保護ストレージ システムに変更するか、レプリケーションを有効化するようにサーバー DR を構成できます。 サーバー DR バックアップの手動構成 で手順を参照してください。別の保護ストレージ システムをターゲットにする必要がある場合を除き、バックアップ ターゲットの手動構成は推奨されていません。

自動サーバー DR が失敗した場合、サーバー DR バックアップの手動構成は、サーバー DR を構成するための代替方法を提供します。ジョブの詳細には、構成処理のトラブルシューティングに使用できる情報が記載されています。

DD システムのリカバリー ターゲット（NFS）の準備

システム バックアップ ストレージに NFS を使用する予定の場合は、DD ターゲット システムで NFS エクスポートを構成し、必要な権限を選択します。PowerProtect Data Manager をバックアップ/リカバリー用に構成するには、この NFS エクスポート パスが必要です。

このタスクについて

メモ: NFS は、PowerProtect Data Manager サーバー DR のレガシー ストレージ タイプです。

手順

1. Web ブラウザーを使用してシステム管理者ユーザーとして DD System Manager にログ インします。
2. [Protocols] ペインの [Summary] タブで、[NFS Exports] > [Create Export] を選択します。
3. [Create NFS Export] ウィンドウで、次の情報を入力し、[OK] をクリックします。
   - [Export Name]：DD MTree の名前。
   - [Directory Path]：作成した DD MTree のフル ディレクトリー パス。ディレクトリに同じ名前を使用していることを確認します。
     メモ: 外部 DD システムの場合は、次のようなパスを指定します。`/data/col1/<path>`、ここで、 *<path>*は、システム バックアップを格納する MTree です。
4. PowerProtect Data Manager をホスト名または IP アドレスごとに NFS クライアント リストに追加します。
   既存の検索クラスターの DR リカバリー保護を構成するには、検索クラスターの IP アドレスまたはホスト名を NFS クライアント リストに追加します。
5. [Current Selection] リストに `no_root_squash` が含まれていることを確認します。PowerProtect Data Manager が NFS 共有のディレクトリー構造を変更する権限で必要になります。

6. 保存操作が完了したことを示す進行状況メッセージが表示されたら、［Close］をクリックします。

サーバー DR バックアップの手動構成

新規導入の場合、PowerProtect Data Manager がサーバー DR を自動的に構成し、有効化します。しかし、手動で PowerProtect Data Manager システムとシステム メタデータの DR 保護を構成することができます。

前提条件

保護ストレージに NFS を使用する予定がある場合は、DD システムのリカバリー ターゲット（NFS）の準備の説明に従って、ターゲット DD システムを準備します。

保護ストレージに DD Boost を使用する予定がある場合は、DD システムを保護ストレージとして追加します。 保護ストレージ で手順を参照してください。サーバー DR バックアップのレプリケートを計画している場合、レプリケーション ターゲットは別の保護ストレージ システムである必要があります。

手順

1. 管理者ロールを持つユーザーとして PowerProtect Data Manager 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、［Disaster Recovery］を選択して、［Configuration］をクリックします。
3. ［Enable backup］を選択します。
4. DD Boost の場合は、次の属性を使用してバックアップを構成します。
   a. ［Protocol］には、［DDBoost］を選択します。
   b. ［PowerProtect DD System］ドロップダウン リストで、既存の保護ストレージ システムのリストからバックアップ デスティネーションを選択するか、［Add］を選択してシステムを追加し、［Add Storage］ウィンドウに詳細を入力します。
   最初の DR 構成の場合、［Storage Unit］フィールドは空です。DR がすでに構成されている場合は、［Storage Unit］フィールドに、サーバー DR バックアップを保持するストレージ ユニットの名前が表示されます。
5. NFS の場合は、次の属性を使用してバックアップを構成します。
   a. ［Protocol］には、［NFS］を選択します。
   b. ［PowerProtect DD System］フィールドに、バックアップ用の DD システムの IP アドレスまたはホスト名を入力します。
   c. ［NFS Export Path］フィールドに、ターゲット DD システム上のサーバー DR バックアップが保存されている NFS パスを入力します。
6. バックアップの頻度と期間を構成します。
   a. サーバー DR バックアップの間隔を時間単位で入力します。
   この設定はバックアップの頻度を制御し、指定できる値は 1～24 時間です。
   b. PowerProtect Data Manager でサーバー DR バックアップを保持する必要がある日数を入力します。
   指定できる値は 2～30 日です。
7. サーバー DR レプリケーションを有効にするには、次の手順を実行します。
   a. ［Enable Replication］をオンにします。
   b. ［Replicate Backup To］ドロップダウン リストで、既存の保護ストレージ システムのリストからターゲットを選択するか、［Add］を選択してシステムを追加し、［Add Storage］ウィンドウに詳細を入力します。
   レプリケーション ターゲットをバックアップ先にすることはできません。
   レプリケーションの頻度と保存期間は、バックアップの場合と同じです。
8. ［Save］をクリックします。

タスクの結果

DD Boost の場合、PowerProtect Data Manager を使用すれば、システム ジョブを作成し、新しいストレージ ユニットを準備し、サーバー DR 保護ポリシーを構成できます。

両方のストレージ タイプに対して、PowerProtect Data Manager によって最初のサーバー DR バックアップ用にシステム ジョブが作成されます。

レプリケーションを構成した場合、PowerProtect Data Manager によってデスティネーションに DD Boost ユーザーとストレージ ユニットが作成されます。サーバー DR バックアップにより、保護スケジュールに従ってレプリケーションが開始されます。

次の手順

システム ジョブが成功したことを確認します。

サーバー DR のレコード設定

重要な情報を記録して、DR の計画を立てます。大規模なアウテージが発生した場合は、システムをリカバリーするためにこの情報が必要になります。一部の項目は、特定の DR シナリオでのみ必要です。PowerProtect Data Manager の外部にあるローカル ドライブに次の情報を記録します。

手順

1. PowerProtect Data Manager が vSphere に導入されている場合は、ポート グループを記録します。
   a. vSphere Client にログインします。
   b. アプライアンス名を右クリックし、[Edit Settings] を選択します。
   c. PowerProtect Data Manager に割り当てられているポート グループの設定を記録します。
   この情報は、同じ VMware 環境にリストアする場合に役立ちます。
2. PowerProtect Data Manager FQDN を記録します。
3. 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。
4. PowerProtect Data Manager のバージョンとビルド番号の記録。
   カスタマー サポートは、この情報を提供できますが、必須ではありません。
5.  をクリックし、[Disaster Recovery] を選択して、[Configuration] をクリックします。
6. サーバー DR ストレージが NFS または DD Boost を使用しているかどうかを記録します。
7. 保護ストレージ システムの IP アドレスまたは FQDN を記録します。
8. サーバー DR レプリケーションを構成した場合は、レプリケーション ターゲットの FQDN を記録します。
9. NFS をサーバー DR ストレージに使用する場合は、NFS エクスポート パスを記録します。
10. DD Boost をサーバー DR ストレージに使用する場合は、次のサブステップを実行します。
    a. PowerProtect Data Manager コンソールに接続し、root ユーザーに変更します。
    b. ディレクトリーを次のように変更します。
    ```
    cd /usr/local/brs/puppet/scripts
    ```
    c. サーバーの DR DD Boost 認証情報を取得して記録します。
    ```
    ./get_sdr_config_credential.py SysDR_$(hostname -s)
    ```
    d. 保護ストレージ システムコンソールに接続します。
    e. サーバー DR DD Boost ユーザーのユーザー ID (UID)を取得して記録します。
    ```
    user show list
    ```

タスクの結果

表 29. 記録された DR 設定

システム	設定またはプロパティ	例	記録された値
PowerProtect Data Manager	バージョンとビルド	19.14	
	FQDN	server1.example.com	
	バックアップ プロトコル	NFS または DD Boost	
サーバー DR レプリカ	FQDN	dd-replica.example.com	
保護ストレージシステム	FQDN	dd.example.com	
	NFS エクスポート パス	N/A	
	DD Boost ユーザー名	SysDR_server1	
	DD Boost パスワード	zD0_56c-b4e-ad4-dbb-	
	DD Boost UID	501	

PowerProtect Data Manager サーバー DR バックアップの管理

PowerProtect Data Manager サーバー DR バックアップを表示し、手動バックアップを実行します。

このタスクについて

DR バックアップの場合、PowerProtect Data Manager は 7 日間のデフォルトの保存期間と、当日の過去 3 時間のバックアップ コピーをサポートします。［Disaster Recovery］ > ［Configuration］タブから、DR バックアップの頻度と保存期間を変更できます。

システム保護サービスは、構成された保存ポリシーに従ってスケジュール設定されたバックアップを自動的に削除します。

［FULL］とマークされた最新のバックアップと［PARTIAL］とマークされた最新のバックアップを除き、バックアップをすべて手動で削除できます。

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、［Disaster Recovery］を選択して、［Manage Backups］をクリックします。
3. 手動バックアップを実行するには、次の手順を実行します。
   a. ［今すぐバックアップ］をクリックします。
      ［Enter a name for your backup］ダイアログが表示されます。
   b. （オプション）バックアップの名前を入力します。
      バックアップ名を空白のままにすると、PowerProtect Data Manager は、命名規則 `UserDR-`を使用して、バックアップの名前を指定します。スケジュール設定されたバックアップに PowerProtect Data Manager が使用する規則 `SystemDR` が付いた名前を指定した場合、PowerProtect Data Manager にはエラーが表示されます。
   c. ［Start Backup］をクリックします。

      バックアップは、テーブルのエントリーとして表示されます。バックアップの詳細を表示するには、>をクリックします。

      検索エンジンが導入されている場合は、PowerProtect Data Manager も検索エンジンをバックアップします。バックアップの詳細には、検索エンジンのバックアップのステータスが表示されます。

      バックアップのステータスを監視するには、［ジョブ］ > ［保護］を選択して、［サーバー データストアの保護］という名前のジョブを検索します。
4. 有効期限切れのバックアップを削除するには、以下の手順を実行します。
   a. リストからバックアップを選択します。
   b. 該当する行の🗑をクリックします。
      バックアップを削除するかどうかを確認する警告が表示されます。［Yes］をクリックして続行します。
5. ［キャンセル］をクリックします。

サーバー DR バックアップからの PowerProtect Data Manager のリカバリー

保護ストレージ システム上のサーバー DR バックアップから PowerProtect Data Manager をリカバリーできます。

前提条件

- リカバリーを実行できるのは管理者ロールのみです。
- サーバー DR のレコード設定に記載されているすべての情報が使用可能であることを確認します。
- PowerProtect Data Manager の FQDN がホスト名と同じであることを確認します。
- NFS からデータをリストアするには、リカバリー ターゲット システムがセット アップされていることを確認します。DD システムのリカバリー ターゲット（NFS）の準備を参照してください。
- DD Boost からデータをリストアするには、PowerProtect Data Manager UI で事前定義された管理者アカウントの現在のパスワードがあることを確認します。このパスワードがわからない場合は、カスタマー サポートにお問い合わせください。
- サーバー DR レプリカからデータをリストアするには、レプリケーション ターゲットの IP アドレスまたは FQDN、PowerProtect Data Manager のホスト名に加え、PowerProtect Data Manager UI で事前定義された管理者アカウントの現在のパスワードを必ず用意してください。
- 以前の PowerProtect Data Manager 導入の検索エンジン ノードまたはレポート エンジン, reporting engine ノードが vCenter Server でホストされている場合は、PowerProtect Data Manager システムをリカバリーする前に、vCenter Server から検索エンジン ノードとレポート エンジン, reporting engine ノードを削除します。リカバリー プロセスは、検索エンジン ノードとレポート エンジン, reporting engine ノードをリカバリー操作の一部として再導入します。
- リカバリー プロセスは、保護エンジンを自動的に再導入しません。リカバリー後に、保護エンジンを再導入します。

このタスクについて

主要なイベントが原因でプライマリー PowerProtect Data Manager システムに障害が発生した場合は、新しい PowerProtect Data Manager システムを導入し、外部の DD システムからバックアップをリカバリーします。

メモ: リカバリー システムの FQDN が異なる場合は、PowerProtect Data Manager のリカバリーに関するトラブルシューティングを参照してください。

PowerProtect Data Manager システムをリカバリーするときに、リカバリー バックアップに検索エンジンが存在する場合、検索エンジンは自動的にリカバリーされます。

手順

1. 新しい PowerProtect Data Manager 仮想アプライアンスを導入します。
   該当するプラットフォームの *PowerProtect Data Manager* 導入ガイドに手順が記載されています。
2. 仮想アプライアンスへのネットワーク アクセス権を持つホストから、Google Chrome の最新版を使用してアプライアンスに接続します。
   `https://<appliance_hostname>`
   メモ: アプライアンスのホスト名または IP アドレスを指定できます。
3. [Welcome] の下の [Install] ウィンドウで、[Restore Backup] を選択します。
4. [After restore, keep the product in recovery mode so that scheduled workflows are not triggered] を選択します。
   リカバリー モード で詳細を参照してください。
5. NFS からデータをリストアするには、次の手順を実行します。
   a. [Protocol] には、[NFS] を選択します。
   b. [Select File] で、DD システムとバックアップが存在する NFS エクスポート パスを入力し、[Connect] をクリックします。
   使用可能なリカバリー バックアップのリストが表示されます。
6. DD Boost からデータをリストアするには、次の手順を実行します。
   a. [Protocol] には、[DDBoost] を選択します。
   b. サーバー DR バックアップを格納する保護ストレージ システムのホスト名または IP アドレスを入力します。
   c. ホスト名がまだ入力されていない場合は、元の PowerProtect Data Manager システムのホスト名を入力します。
   d. サーバー DR レプリカからリストアをするには、ホスト名に「**`/R`**」を追加します。
      例えば、**`system1.example.com/R`** などです。
   e. 元の PowerProtect Data Manager の事前定義された管理者アカウントのパスワード(`admin`)を入力します。
   f. [Connect] をクリックします。
   使用可能なリカバリー バックアップのリストが表示されます。レプリカからデータをリストアする場合、バックアップのリストにはレプリカ上のバックアップが含まれます。
7. システムのリカバリー元のバックアップを選択し、[Recover] をクリックします。
   リカバリーが開始されます。リカバリは数分間かかることがあります。
   メモ: リカバリー プロセス中にビジー状態を示すインジケーターはありません。現在のリカバリー状態は、リカバリー ウィンドウに表示されるテキストでモニターできます。

タスクの結果

リカバリが完了すると、PowerProtect Data Manager ログイン ページが表示されます。

PowerProtect Data Manager インスタンスのタイム ゾーンは、バックアップと同じものに設定されます。

レプリカからリストアをする場合、レプリケーション ターゲット保護ストレージ システムは新しいサーバー DR バックアップ ターゲットとして構成されます。

プリロードされたすべてのアカウントは、*PowerProtect Data Manager* セキュリティ構成ガイドに説明されているように、デフォルトのパスワードにリセットされます。例外として、プリロードされた UI 管理者アカウントのパスワードは保持されます。できるだけ早く、すべてのプリロードされたアカウントのパスワードを変更してください。

メモ: リカバリー プロセスで使用された Server DR リカバリー バックアップより後に作成されたバックアップ コピーは、サーバーのリカバリー後に検出されます。ただし、リカバリー操作の前にレプリケーションまたはクラウド階層コピーが存在していたバックアップ コピーは、次の手動ジョブまたはスケジュール設定されたジョブ時に複製またはクラウド階層化されます。

リカバリー モード

導入時に [After restore, keep the product in recovery mode so that scheduled workflows are not triggered] を選択した場合は、PowerProtect Data Manager により、リカバリー モードが有効になります。

リカバリー モードがアクティブな場合は、PowerProtect Data Manager にログ インすると次のようになります。

- PowerProtect Data Manager UI の上部に赤いバナーが表示されます。バナーは、PowerProtect Data Manager システムが作動しているものの、スケジュール設定されたワークフローが無効になっていることを示します。

- バックアップ ストレージを変更する保護ポリシーによって定義されているすべてのジョブ（バックアップの作成、バックアップの削除、および PowerProtect Data Manager Server DR のジョブなど）は、トリガーされません。
- バックアップ ストレージに書き込むすべての操作は無効になります。

PowerProtect Data Manager をフル動作モードに戻し、スケジュール設定されたワークフローを有効にするには、［Return to full operational mode］をクリックします。

DR バックアップからの検索エンジンのリカバリー

PowerProtect Data Manager システムのディザスター リカバリーが完了した後、PowerProtect Data Manager が検索クラスターを自動的にリストアします。PowerProtect Data Manager システムが検索クラスターを自動的にリストアできなかった場合は、この手順のステップを使用して、REST API を通じて検索クラスターのみをリストアします。検索クラスターのリカバリーは、運用可能な PowerProtect Data Manager システムで実行する必要があります 。検索クラスターをリストアできるのは、管理者ロールのみです。

前提条件

［System Settings］ > ［Disaster Recovery］ > ［Manage Backups］の順に移動し、検索クラスター バックアップの名前を取得します。

このタスクについて

バックアップ マニフェスト ファイルを使用して、REST API で POST コマンドを実行するために使用する新しいテキスト ドキュメントを次の手順に従って作成します。

注意: マニフェスト ファイルを編集しないでください。

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。
   PowerProtect Data Manager をリストアする前に使用したものと同じ認証情報を使用します。
2. 管理者ユーザーとして PowerProtect Data Manager コンソールに接続します。
3. ディレクトリーを`/data01/server_backups/<PowerProtect Data Manager Hostname>_<NodeID>`に変更し、バックアップ マニフェスト ファイルを見つけます。
   通常は、`/data01/server_backups` に 1 個のサブディレクトリーしかないため、そのサブディレクトリーに変更します。ただし、複数のサブディレクトリーがあり、正しい*<NodeID>*がわからない場合は、次のサブステップを実行します。
   a. `/data01/server_backups` から次のコマンドを実行し、必要に応じてユーザー名とパスワードを変更します。

```
TOKEN=$(curl -X POST https://localhost:8443/api/v2/login -k -d '{ "username":
"admin","password": "admin_password" }' --header "Content-Type: application/json" |
python3 -c "import sys, json; print(json.load(sys.stdin)['access_token'])")
```

```
curl -X GET https://localhost:8443/api/v2/nodes -k --header "Content-Type: application/
json" --header "Authorization:Bearer $TOKEN"
```

   b. `grep -Rnwa -e '<Name>' --include=*.manifest` コマンドを実行します。
4. マニフェスト ファイルを一時ファイルにコピーします。
5. 一時ファイルを開きます。
6. 次の例を確認し、//コメント エントリーに記載されている変更を行います。

メモ: ここに表示されている//コメント エントリーは、一時ファイルに含まれていません。これらのコメント エントリーは、ここにのみ表示され、ガイドの役割を果たします。

```
{
  "id": "ca8cbb13-6f3d-4ac5-87e5-de47a634379f",
  "jobId": "990b4ea7-c0e4-4069-8dd5-7d0e084370fc",  // DELETE LINE
  "creationTime": "2022-08-25T19:38:54.622275+0000",
  "lastUpdated": "2022-08-25T19:40:18.165497Z",// DELETE LINE
  "elapsedSeconds": 11,
  "sequenceNumber": 2,
  "state": "Successful",// DELETE LINE
  "version": "19.12.0-1-SNAPSHOT", // DELETE LINE
  "hostname": "ldpdb141.hop.lab.emc.com", // DELETE LINE
```

```
  "name": "mercijTestDr", // DELETE LINE
  "nodeId": "a8d2df8e-5c3e-4160-87d4-32b9bfe6c283", // DELETE LINE
  "sizeInBytes": 29759075,
  "consistency": "CRASH_CONSISTENT", // DELETE LINE
  "checksum": "bbd97a04f296a8ed116e4a9272982d8e8411f3d0cf50dea131d5c2cd4ce224f8", //
DELETE LINE
  "backupConsistencyType": "FULL", // DELETE LINE
  "esSnapshotState": "UNKNOWN", // DELETE LINE
  "backupTriggerSource": "USER", // DELETE LINE
  "configType": "standalone", // DELETE LINE
  "deployedPlatform": "vmware", // DELETE LINE
  "replicationTargets": [], // DELETE LINE
  "repositoryFileSystem": "BOOST_FILE_SYSTEM", // DELETE LINE
  "ddHostname": "ldpdg251.hop.lab.emc.com", // DELETE LINE and add line "recover":true,
  "Components": [   // change Components to components with lower case c
    {  // DELETE WHOLE PPDM COMPONENT LEAVING ONLY SEARCHCLUSTER
      "name": "PPDM",
      "id": "ca7cbb13-6f3d-4ac5-87e5-de47a634379f",
      "lastActivityId": "2bdbe7a8-7c57-446d-b072-ad8081e2953d",
      "version": "v2",
      "backupPath": "ldpdg251.hop.lab.emc.com:SysDR_ldpdb141/
ldpdb141_a8d2df8e-5c3e-4160-87d4-32b9bfe6c283/PPDM",
      "backupStatus": "SUCCESSFUL",
      "backupsEnabled": true,
      "errorResults": []
    }, // STOP DELETING HERE
    {
      "name": "SearchCluster",
      "id": "ca7cbb13-6f3d-4ac5-87e5-de47a634379f",
      "lastActivityId": "198a93b1-7382-474b-89c8-c7b6b0ab4987",
      "version": "v2",
      "backupPath": "ldpdg251.hop.lab.emc.com:SysDR_ldpdb141/
ldpdb141_a8d2df8e-5c3e-4160-87d4-32b9bfe6c283/SearchCluster",
      "backupStatus": "SUCCESSFUL",
      "backupsEnabled": true, // DELETE TRAILING COMMA
      "errorResults": [] // DELETE LINE
    }
  ]
}
```

まとめると、次のようになります。

- ここに表示されている`// DELETE LINE`コメント エントリーの行をすべて削除します。
- `recover: true`を追加します。
- `Components`を`components`に変更します。
- リストに記載されている、`Search Cluster`以外のコンポーネント ブロックをすべて削除します。
- `"backupsEnabled": true,`から末尾のコンマを削除します。

このように変更すると、次のようになります。

```
{
  "id": "ca8cbb13-6f3d-4ac5-87e5-de47a634379f",
  "creationTime": "2022-08-25T19:38:54.622275+0000",
  "elapsedSeconds": 11,
  "sequenceNumber": 2,
  "sizeInBytes": 29759075,
  "recover" : true,
  "components": [
    {
      "name": "SearchCluster",
      "id": "ca7cbb13-6f3d-4ac5-87e5-de47a634379f",
      "lastActivityId": "198a93b1-7382-474b-89c8-c7b6b0ab4987",
      "version": "v2",
      "backupPath": "ldpdg251.hop.lab.emc.com:SysDR_ldpdb141/
ldpdb141_a8d2df8e-5c3e-4160-87d4-32b9bfe6c283/SearchCluster",
      "backupStatus": "SUCCESSFUL",
      "backupsEnabled": true
    }
  ]
}
```

7. `"id":`の後の引用符で囲まれたテキストの値をコピーします。
   ステップ 11 で使用する変数*<backupID>*をこの値に置き換えます。この例では、*<backupID>*は `ca8cbb13-6f3d-4ac5-87e5-de47a634379f` です。
8. 一時ファイルからキャリッジ リターンをすべて削除し、すべてのテキストを 1 行で表します。
9. 一時ファイルからテキストをすべてコピーします。
   ステップ 11 で使用する変数*<manifestText>*をこの値に置き換えます。
10. 次のコマンドを実行し、必要に応じてユーザー名とパスワードの認証情報を変更します。

    メモ: このコマンドをステップ 3.a で実行した場合でも、もう一度実行してください。`TOKEN` の値には有効期限があります。

```
TOKEN=$(curl -X POST https://localhost:8443/api/v2/login -k -d '{ "username":
"admin","password": "admin_password" }' --header "Content-Type: application/json" |
python3 -c "import sys, json; print(json.load(sys.stdin)['access_token'])")
```

11. 次のコマンドを実行します。

```
curl -X PUT 'https://localhost:8443/api/v2/server-disaster-recovery-backups/<backupID>' --
header "Authorization: Bearer $TOKEN" --header 'Content-Type: application/json' -k -d
'<manifestText>'
```

    - *<backupID>*をステップ 7 で取得した値に置き換えます。
    - *<manifestText>*をステップ 9 で取得したすべてのテキストに置き換えます。
12. リストア プロセスのステータスをモニタリングするには、PowerProtect Data Manager UI で、［Jobs］ > ［System Jobs］の順に選択して、説明欄に［Restoring backup Search Node］の記載があるジョブを検索します。

次の手順

ステップ 4 で作成した一時ファイルを削除します。

DD システムの IP アドレスまたはホスト名の変更

サーバー DR に影響を与えることなく、DD システムの IP アドレスまたはホスト名を変更できます。

このタスクについて

DD システムの IP アドレスまたはホスト名を変更する前に、次の手順を実行します。

メモ: 次に示されている手順を実行せずに DD システムの IP アドレスまたはホスト名を変更した場合は、DR 機能のリカバリーを行うことができます。詳細については、DD システムの IP アドレスまたはホスト名変更からのリカバリーを参照してください。

手順

1. サーバー DR バックアップを無効にします。
2. SSH を使用して PowerProtect Data Manager サーバーにログインします。
3. 次のコマンドを実行します。
   `sudo umount /data01/server_backups`
4. 各 Search Engine ノード, Search Engine node に対して、次のサブステップを実行します。
   a. SSH を使用して Search Engine ノード, Search Engine node にログ インをします。
   b. 次のコマンドを実行します。
      `sudo umount /mnt/PPDM_Snapshots`
5. 次のように、DD システムを PowerProtect Data Manager から削除します。
   a. PowerProtect Data Manager UI から、［Infrastructure］ > ［Storage］の順に選択します。
   b. 削除する DD システムを選択します。
   c. ［Delete］をクリックします。
6. DD システムの IP アドレスまたはホスト名を変更します。
7. DD を PowerProtect Data Manager に追加し直します。
8. サーバー DR バックアップを有効にします。

DD システムの IP アドレスまたはホスト名変更からのリカバリー

サポートされている手順に従わずに DD システムの IP アドレスまたはホスト名を変更した場合は、サーバー DR 機能のリカバリーを行うことができます。

このタスクについて

手順

1. サーバー DR バックアップを無効にします。
2. SSH を使用して PowerProtect Data Manager サーバーにログインします。
3. 次のコマンドを実行します。
   ```
   ps aux | grep /data01/server_backups | grep boostfs
   ```
   コマンド出力の `boostfs` エントリーの横にあるプロセス ID をメモに残します。
4. 次のコマンドを実行し、`<processID>`をステップ 3 で取得したプロセス ID に置き換えます。
   ```
   sudo kill -9 <processID>
   ```
5. 次のコマンドを実行します。
   ```
   sudo umount /data01/server_backups
   ```
6. 各 Search Engine ノード, Search Engine node に対して、次のサブステップを実行します。
   a. SSH を使用して Search Engine ノード, Search Engine node にログ インをします。
   b. 次のコマンドを実行します。
      ```
      sudo umount /mnt/PPDM_Snapshots
      ```
7. 次のように、DD システムを PowerProtect Data Manager から削除します。
   a. PowerProtect Data Manager UI から、[Infrastructure] > [Storage] の順に選択します。
   b. 削除する DD システムを選択します。
   c. [Delete] をクリックします。
8. DD を PowerProtect Data Manager に追加し直します。
9. サーバー DR バックアップを有効にします。

NFS バックアップ構成に関する問題のトラブルシューティング

次のセクションでは、NFS を使用するサーバー DR バックアップ構成を構成するときに表示されることのあるエラー メッセージのリストを示します。

DD ストレージ ユニットのマウント コマンドが次のエラーで失敗しました：「Cannot mount *full path*: Access is denied」

このエラー メッセージは、サーバー DR ストレージ ユニットへのフル パス用の NFS エクスポートが DD システム上に存在しない場合に表示されます。このエラー メッセージは、再導入された仮想アプライアンスが NFS エクスポートにアクセスするためのクライアントとして追加されていない場合にも表示されます。

この問題を解決するには、DD Boost ストレージ ユニットのフル パス用の NFS エクスポートを構成してあることと、アプライアンスがエクスポート クライアントであることを確認します。

DD ストレージ ユニットのマウント コマンドが次のエラーで失敗しました：「Cannot resolve *FQDN*: The name or service not known」

このエラー メッセージは、指定された FQDN を使用して PowerProtect Data Manager が DD システムに接続できない場合に表示されます。この問題を解決するには、DD システムの FQDN と IP アドレスを解決できることを確認します。

PowerProtect Data Manager のリカバリーに関するトラブルシューティング

リカバリ サイトの FQDN がプライマリー サイトの FQDN と異なる場合は、マウント エラーが発生することがあり、リカバリ プロセスにいくつかの追加手順が必要になる場合があります。

このタスクについて

リカバリ中にマウントエラーが発生した場合は、次の回避手順に従います。

手順

1. バックアップが配置されている DD システムで、レプリケーション ペアを削除して、PowerProtect Data Manager にマウントします。
2. リカバリが完了したら、PowerProtect Data Manager で、次のコマンドを使用して証明書を再生成します。
   `sudo -H -u admin /usr/local/brs/puppet/scripts/generate_certificates.sh -c`
3. システムを再起動し、プライマリ PowerProtect Data Manager システムの URL を選択します。
   `https://PowerProtect Data Manager IP/#/progress` ページが表示され、リカバリーが再開されます。
4. プライマリ PowerProtect Data Manager にログインします。
   PowerProtect Data ManagerVM vCenter コンソールにエラーが表示されます。これは無視してかまいません。
5. 元の IP アドレスを使用してプライマリ PowerProtect Data Manager を開き、ログインします。

タスクの結果

リカバリが完了しました。

失敗した PowerProtect Data Manager リストアのリカバリー

手順

1. 新しい PowerProtect Data Manager 仮想アプライアンスを導入します。
   該当するプラットフォームの *PowerProtect Data Manager* 導入ガイドに手順が記載されています。
2. カスタマー サポートにお問い合わせください。

サーバー DR バックアップの無効化

一部のメンテナンス手順では、手順の途中でサーバー DR バックアップの無効化が必要な場合があります。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。

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、［Disaster Recovery］を選択して、［Configuration］をクリックします。
3. ［Configuration］ページの既存サーバー DR 設定を記録します。
4. ［Enable backup］の選択を解除します。
5. ［Save］をクリックします。

次の手順

メンテナンス手順が完了したら、サーバー DR バックアップを再度有効にします。手順については、手動構成の手順を参照してください。

サーバー DR のクイック リカバリー

災害後に、クイック リカバリー機能を使用すると、リモート サイトのデスティネーション システムに複製した資産およびデータをリストアできます。

メモ: クイック リカバリーでは、リストアされた資産を保護する元のバックアップ環境とソース システムは再作成されません。したがって、クイック リカバリーはサーバー DR リストアに代わるものではありません。リモート サイトで、リストアされた資産のバック アップを続行するには、リストアされた資産をデスティネーション システムの保護ポリシーに追加します。

クイック リカバリーは、PowerProtect Data Manager の保護対象である次の資産でサポートされています。

- 仮想マシン
  メモ: このサポートに、アプリケーション認識 VADP ワークロードは含まれません。
- Kubernetes ネームスペースと PVC
- ファイル システム
  注意: システム パーティションまたは起動ディスクのクイック リカバリーを試みないでください。

クイック リカバリーは、ファイル レベルまたはフォルダー レベルでのユーザー データのリストアをサポートしていません。

クイック リカバリーでは、バックアップ コピーのフローに従って、ソース システムからデスティネーション システムにメタデータを送信します。このメタデータによって、レプリケーション デスティネーションにコピーが認識され、リカバリー ビューが有効になります。ソース PowerProtect Data Manager システムをリストアする機会が来る前でも、リモート サイトのワークロードをリカバリーできます。

例えば、次の図に独立型の PowerProtect Data Manager と保護ストレージ用の DD システムを備える、A と B という名前の 2 か所のサイトを示しています。サイトには、それぞれに固有の資産が含まれています。災害前の個々のデータセンターの図は、両方のサイトが相互にコピーのレプリケートを行う初期構成を示しています。災害後の個々のデータセンターの図は、サイト A が停止した後の状態を示しています。クイック リカバリーによってレプリケートしたコピーからサイト B 環境に、サイト A の資産のリストアが行われています。

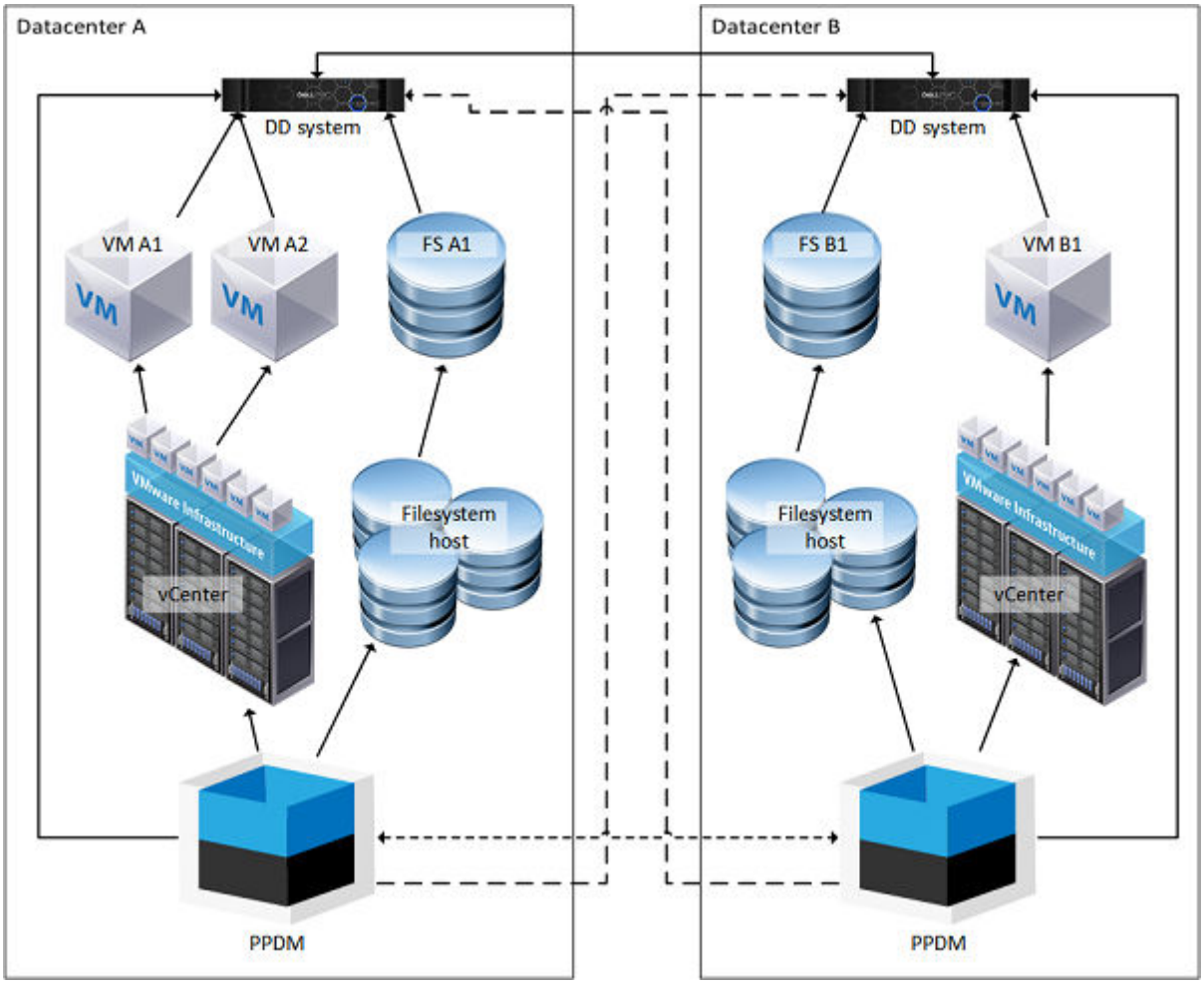


図 3. 災害前の個々のデータセンター

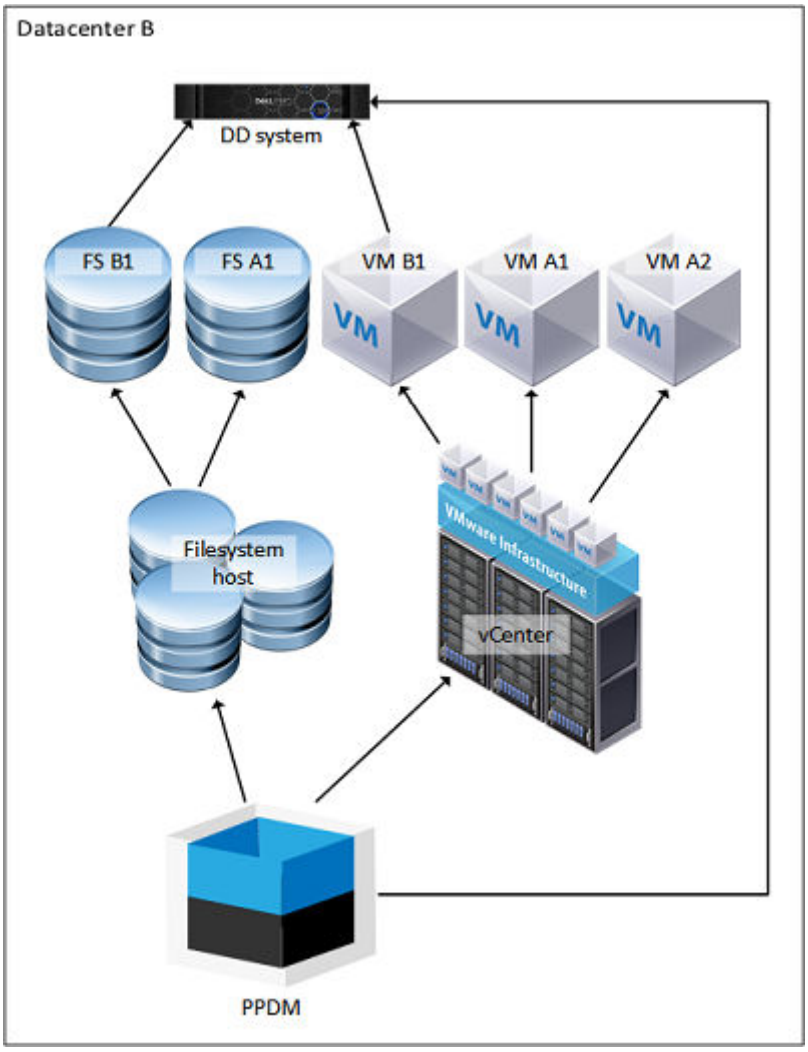


図 4. 災害後の個々のデータセンター

PowerProtect Data Manager は、代替トポロジーのクイック リカバリーをサポートしています。個から多へ、および多から個へのレプリケーションのクイック リカバリーを構成できます。例えば、次の図はソース PowerProtect Data Manager が、スタンバイ DD システムに自らの PowerProtect Data Manager のレプリケートを行う様子を示しています。これらはすべて同じデータ センター内に存在します。ソース システムに障害が発生した場合でも、クイック リカバリー機能によって、ソースのリストアを行う前に、レプリケートしたこれらのコピーからリストアを行うことができます。

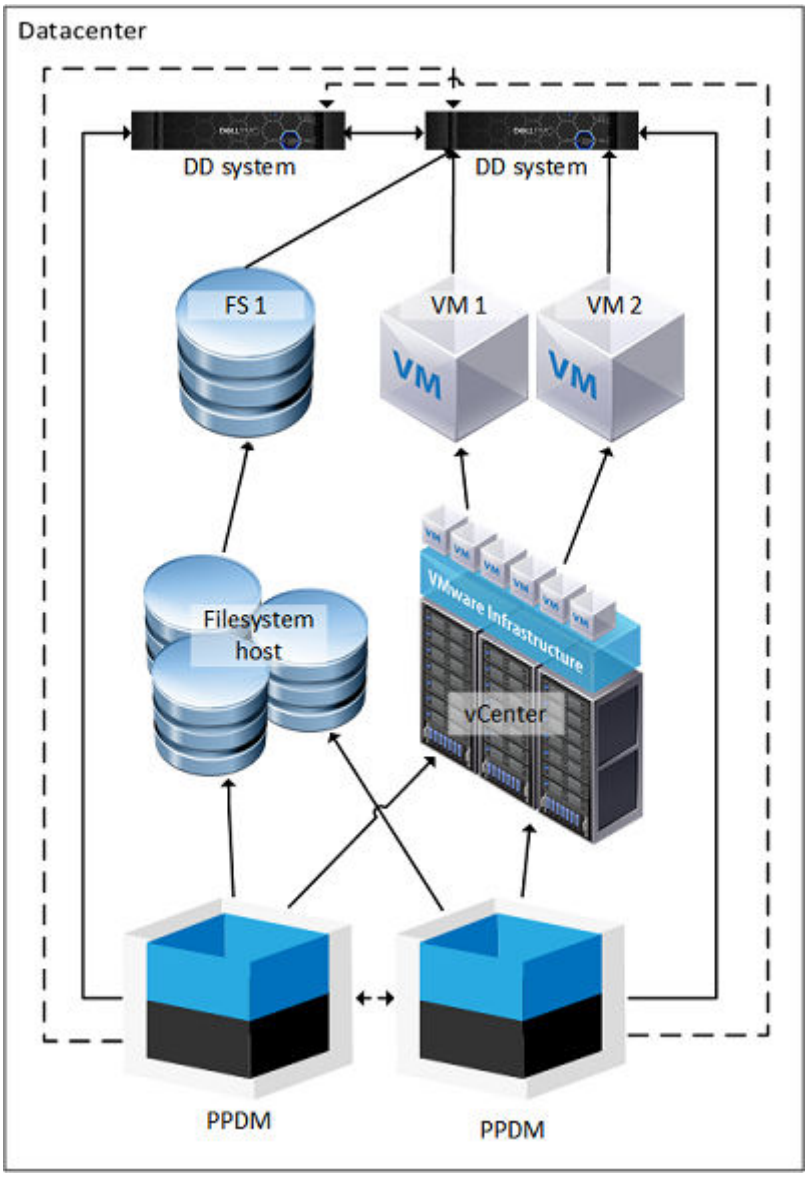


図 5. スタンバイ DD システム

次に続くトピックでは、前提条件に加え、PowerProtect Data Manager を構成してクイック リカバリーに対応させる方法と、リカバリー ビューを使用して資産をリストアする方法について説明します。

クイック リカバリーの前提条件

クイック リカバリーを設定する前に、次の項目を完了させてください。

- ソース システムとデスティネーション システムが、同じ方法（ホスト名または IP アドレス）を使用して相互に Ping を実行できることを確認します。
- ソース システムとリモート（デスティネーション）システムの両方で、PowerProtect Data Manager のバージョンが同じであることを確認します。
- 少なくとも 2 個の保護ストレージ システム（1 個はローカルの保護ストレージ用で、もう 1 個はレプリケーション用）をソース システムに接続します。
- ソース システムに資産ソースを登録し、それらの資産を保護するための保護ポリシーを構成します。
- リモート サイトの保護ストレージ システムにバックアップ コピーをレプリケートするための保護ポリシーを構成します。
- 保護された資産のバック アップを行い、デスティネーション保護ストレージ システムでバックアップ データのレプリケートが正常に行われていることを確認します。
- レプリケーション保護ストレージがリモート（デスティネーション）システムで検出されていることを確認します。
- リモート PowerProtect Data Manager インスタンスで資産ソースを追加および有効化します。
- Kubernetes クイック リカバリー操作の場合は、同じ Kubernetes クラスターが複数の PowerProtect Data Manager インスタンスによって管理されていないことを確認します。

クイック リカバリーのリモート ビューを使用する前に、ソース上のリモート システムのリストにデスティネーション システムを追加します。クイック リカバリーを構成した後に PowerProtect Data Manager セキュリティ証明書を変更している場合、『*PowerProtect Data Manager* セキュリティ構成ガイド』の手順に従って、証明書を再同期してください。

リモート システムの識別

クイック リカバリー用に PowerProtect Data Manager に追加されたリモート システムは、完全修飾ドメイン名(FQDN)または Internet Protocol (IP)アドレスのいずれかを使用して識別できます。誤った ID を使用した場合、クイック リカバリーは証明書エラーで失敗します。

リモート システムがすでに PowerProtect Data Manager 証明書リストで識別されている場合は、クイック リカバリー用に PowerProtect Data Manager に同じ ID で追加する必要があります。

すべてのリモート システムで常に FQDN または IP アドレスのいずれかを使用する場合は、クイック リカバリー用に同じ操作を行います。

リモート システムの証明書エントリーが存在する場合は、クイック リカバリー用に追加するときに同じ ID を使用する必要があります。クイック リカバリー用に追加するリモート システムがすでに PowerProtect Data Manager 証明書リストに含まれているかどうかわからない場合は、次の手順を実行します。

- root ユーザーとしてコンソールにログインします。
- 「`keytool -list -keystore`」と入力します。
- 出力を確認し、リモート システムの FQDN または IP アドレスのいずれかに対応する証明書エントリーを探します。

クイック リカバリー用リモート システムの追加

バックアップのレプリケート先のもう 1 台のシステムにメタデータを送信するように PowerProtect Data Manager を構成します。リモート システムを追加できるのは、管理者ロールのみです。

手順

1. をクリックし、[Disaster Recovery] を選択して [Remote Systems] をクリックします。

   [[リモート システム]] タブが開き、構成済みのリモート PowerProtect Data Manager システムの表が表示されます。
2. [Add] をクリックします。
   [[リモート PowerProtect システムの追加]] ウィンドウが開きます。
3. [名前] と [FQDN/IP] フィールドに入力します。

   [名前] フィールドは、リモート システムを識別できる記述名にします。リモート システムの FQDN または IP アドレスを入力する必要があるかどうかを確認するには、「リモート システムの識別」を参照してください。
4. [ポート] フィールドに、リモート システムの REST API のポート番号を入力します。

   REST API のデフォルトのポート番号は 8443 です。
5. [Credentials] フィールドで、リストから管理者ロールが割り当てられた既存の認証情報セットを選択します。

   または、このリストの [Add Credentials] をクリックして、管理者ロールが割り当てられた新しい認証情報を追加することもできます。認証情報、ユーザー名、パスワード用の記述名を入力します。次に、[保存] をクリックして認証情報を保存します。
6. [検証] をクリックします。

   PowerProtect Data Manager によるリモート システムへの問い合わせが行われ、本人確認のためのセキュリティ証明書が取得されます。

   [[証明書の検証]] ウィンドウが開き、証明書の詳細が表示されます。
7. 証明書の詳細を確認し、リモート システムの期待値に対する各フィールドの内容を確認します。次に、[承諾] をクリックして証明書を保存します。
   [証明書] フィールドが `VERIFIED` に変更され、サーバーの ID がリスト表示されます。
8. [保存] をクリックします。
   PowerProtect Data Manager によって、[[ディザスター リカバリー]] ウィンドウの [[リモート システム]] タブに戻ります。構成の変更が完了するまでしばらく時間がかかる場合があります。
9. [[キャンセル]] をクリックします。
   [[ディザスター リカバリー]] ウィンドウが閉じます。
10. をクリックし、[Disaster Recovery] を選択して [Remote Systems] をクリックします。

    [[リモート システム]] タブが開きます。
11. リモート システムの表に新しい PowerProtect Data Manager システムが含まれていることを確認します。
12. [[キャンセル]] をクリックします。

[[ディザスター リカバリー]] ウィンドウが閉じます。

次の手順

リモート システムでは、このシステムで有効になっているのと同じ資産ソースを有効にします。 資産ソースの有効化 で詳細を参照してください。リモート システム上の資産ソースを有効にすると、そのタイプのレプリケートされたバックアップが表示され、アクセスできるようになります。

リモート システムで、[リカバリー] ビューを開き、バックアップが表示されてアクセス可能であることを確認します。テスト リストアの実行が推奨されています。

ソース システムとデスティネーション システム間では 3 時間ごとにメタデータが同期されます。バックアップが表示されない場合は、最初の同期のための十分な時間をとった後でトラブルシューティングを行ってください。

リモート システムの編集

PowerProtect Data Manager ユーザー インターフェイスを使用して、リモート システムの記述名を変更したり、REST API のポート番号や認証情報を変更したりできます。リモート システムとの同期を有効または無効にすることもできます。リモート システムを編集できるのは、管理者ロールのみです。

手順

1. をクリックし、[Disaster Recovery] を選択して [Remote Systems] をクリックします。
   [[リモート システム]] タブが開き、構成済みのリモート PowerProtect Data Manager システムの表が表示されます。
2. 該当するリモート システムに対応する行を見つけ、その行のチェック ボックスをオンにします。
   PowerProtect Data Manager によって [編集] ボタンが有効になります。
3. [編集] をクリックします。
   [[リモート PowerProtect システムの編集]] ウィンドウが開きます。
4. 該当するパラメーターを変更し、[保存] をクリックします。
   同期を有効または無効にするには、[Enable sync] を選択または選択解除します。ポート番号を変更する場合は、リモート システムのセキュリティ証明書の再確認が必要になる場合があります。
   PowerProtect Data Manager によって、[[ディザスター リカバリー]] ウィンドウの [[リモート システム]] タブに戻ります。構成の変更が完了するまでしばらく時間がかかる場合があります。
5. [[キャンセル]] をクリックします。
   [[ディザスター リカバリー]] ウィンドウが閉じます。

クイック リカバリーのリモート ビュー

リモート ビューは、ソースが使用できなくなった後、デスティネーション システム上にレプリケートしたコピーを操作するために使用します。例えば、ソース システムのリストアが可能になる前に、重要な資産をリストアする場合などです。

デスティネーション システムで、管理者ロールを持つユーザーとしてログ インします。リモート サーバーは、バナーに が表示されます。

をクリックし、[Remote Systems] を選択すると、PowerProtect Data Manager にローカル システムおよび接済済みのすべてのシステムの名前を含むドロップダウンが表示されます。各エントリーには、識別用のサフィックスとして `(Local)` または `(Remote)` が含まれています。

バックアップのレプリケート元のソース システムを選択します。PowerProtect Data Manager によってリモート ビューが開き、次のような標準 UI ナビゲーション ツールのサブセットが表示されます。

- [Restore]
  - [Assets]：レプリケートされたコピーが表示されます。
  - [Running Sessions]：インスタント アクセス セッションを管理し、監視することができます。
- [Alerts]：監査ログを含むアラート情報が表で示されます。
- [Jobs]：実行中のリストア ジョブのステータスが表示されます。

各ツールの機能は、ローカル システムと同じです。ただし、リモート ビューはリストア操作のみを目的としているため、選択したソース システムからレプリケートしたコピーの範囲は限定されています。リモート ビューでは、バナーで選択したシステムを識別できます。

メモ: 仮想マシンの場合、クイック リカバリー リストアのワークフローには、バックアップから vCenter のタグとカテゴリーのリストアを行うための [VM タグのリストア] オプションが含まれていません。

[リストア] > [Assets] を使用してコピーを検索します。リストア操作の詳細については、各資産タイプのリストア手順を参照してください。

リカバリーが完了したら、［リモート システム］をクリックしてローカル システムの名前を選択し、リモート ビューを終了します。

失敗したクイック リカバリー ジョブのトラブルシューティング

次のセクションでは、クイック リカバリー ジョブが失敗した場合のトラブルシューティングについて説明します。

クイック リカバリー ジョブが実行されない

予想されるクイック リカバリー ジョブが実行されていないことが分る場合があります。

ファイルを `sync.log` ファイルを確認すると、次のようなエントリーが表示されています。

```
2022-07-14T00:10:03.235Z ERROR [] [scheduling-1] [][][][][]
[c.e.b.s.e.r.i.ServerRestClient.checkHttpStatus(441)][441 ] - Return code = 401 UNAUTHORIZED,
expected = 200 OK
2022-07-14T00:10:03.236Z ERROR [] [scheduling-1] [][][][][]
[c.e.b.s.c.s.i.SyncHandshakeServiceImpl.syncHandshake(133)][133 ] - Failed to perform
handshake, version check failed.
com.emc.brs.sync.external.remote.VersionCheckResponseException: 500 INTERNAL_SERVER_ERROR
"Unexpected error occured during version check."; nested exception is
com.emc.brs.sync.external.remote.RemoteRestException: Incorrect credentials.
2022-07-14T00:10:03.236Z ERROR [] [scheduling-1] [][][][][]
[c.e.b.s.c.s.i.SyncInstanceServiceImpl.syncHandshake(236)][236 ] - Failed to handshake with
the remote system: com.emc.brs.sync.model.SyncInstance
```

このエラーは、リモート PowerProtect Data Manager システムのパスワードが変更されたことを示します。

この問題を解決するには、リモート PowerProtect Data Manager システムで使用されている認証情報を変更します。

PowerProtect Data Manager クラウド ディザスター リカバリーの概要

クラウド ディザスター リカバリー（DR）機能を使用すると、クラウド DR サーバーをパブリック クラウドに導入することによって、クラウド DR サイトを利用できます。クラウドで VM 保護と DR ワークフローを実行するために、PowerProtect Data Manager UI を使用できます。

クラウド DR のワークフローには、次のような例があります。

- クラウド DR サイト コピー管理：PowerProtect Data Manager UI で VM 保護ポリシーを作成することによって、クラウド DR サイトを設定します。
- VM コピーのフェールオーバー検証：災害が発生する前に、DR テストを実行してからテストの進行状況をモニタリングすることで、PowerProtect Data Manager 内のクラウドへの、VM コピーのフェールオーバーを検証することができます。
- 本番 VM のフェールオーバー：DR フェールオーバー作動を実行することにより、PowerProtect Data Manager 内の本番仮想マシンをフェールオーバーしてから、リストアされた VM が Amazon Web Services（AWS）または Microsoft Azure クラウド内にあることを確認できます。
- 本番 VM のリストア：クラウド アカウント（Amazon Web Services (AWS)または Microsoft Azure クラウド）に保存されているコピーから vCenter に直接仮想マシンをリストアできます。リストア処理は、1 度に 1 個の仮想マシンで実行されます。ターゲットの vCenter Server を手動で選択する必要があります。

PowerProtect Data Manager 内での Cloud DR ワークフローの詳細については、*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 ガイドを参照してください。

9

アラート、ジョブ、およびタスクの管理

トピック：

アラート通知の構成

PowerProtect Data Manager UI の［Alert Notifications］ウィンドウでは、PowerProtect Data Manager のアラートに E メール通知を構成できます。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインから、［Alerts］を選択してから、［Alert Notifications］タブを選択します。
   ［Alert Notifications］ウィンドウに、既存の通知の詳細を表示する表が表示されます。
2. ［Add］をクリックします。
   ［Add Alert Notification］ダイアログが表示されます。
   メモ: ［Add］ボタンは、E メール サーバーを設定するまで無効になっています。アラート通知を追加するには、［System Settings］ > ［Support］ > ［Email Setup］の順に移動して、E メール サーバーを設定します。 E メール サーバーの設定 で詳細を参照してください。
3. ［Name］フィールドに、通知 E メールを受信する個人またはグループの名前を入力します。
4. ［Email］フィールドで、次の手順を実行します。
   a. 通知を受信する E メールまたは別名を指定します。このフィールドは、アラート通知を作成するために必要です。複数のエントリーはコンマで区切ります。
   b. ［Test Email］をクリックして、有効な SMTP 設定が存在することを確認します。
5. ［Category］リストから、次のいずれかの通知カテゴリーを選択します。
   - All
   - エージェント
   - アプリケーション ホスト構成
   - クラウド階層
   - コンプライアンス
   - 検出
   - Export Application Log
   - License
   - NAS Server Disaster Recovery
   - 保護
   - Protection Copy
   - Protection Infrastructure
   - 保護ポリシー
   - Protection Rule

- Protection Source
- プッシュ アップデート
- レプリケーション
- レポート作成
- Restore
- セキュリティ
- セルフ サービス
- サーバ ディザスタリカバリ
- システム

6. ［Severity］リストから、次のいずれかの通知重大度を選択します。
   - All
   - Critical
   - Warning
   - Information
7. ［Duration］フィールドで、通知 E メールの送信頻度を指定します。例えば、通知 E メールを 60 分ごとに送信するには、期間を 60 分に設定します。期間を 0 に設定した場合、PowerProtect Data Manager は E メール通知を送信しません。
8. ［Subject］フィールドに、通知 E メールに添付する件名を任意で入力します。
9. ［Save］をクリックして変更を保存し、ダイアログを閉じます。

タスクの結果

［Alert Notifications］ウィンドウに、新しいアラート通知が表示されます。通知の［Edit］、［Delete］、または［Disable］を行うには、表内のエントリーを選択し、このウィンドウのボタンを使用します。

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、［Alerts］を選択します。

   上部バナーの  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字は、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、  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ーすると、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、カテゴリー、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. 過去 24 時間、過去 3 日間、過去 7 日間、過去 30 日間から期間を選択するか、アラートを表示する特定の日を選択するか、カスタム時間範囲を指定します。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 タグもクリアーされます。
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、［Add/Edit Note］をクリックし、終了したら［Save］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。

監査ログの表示と管理

監査ログを使用することで、PowerProtect Data Manager で開始されたジョブに関する特定の情報を表示することができます。これにより、サービス レベル目標に対するコンプライアンスを確認できます。［Administration］ > ［Audit Logs］ウィンドウから監査ログにアクセスできます。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Administration］ > ［Audit Logs］の順に選択します。
   ［Audit Logs］ウィンドウには、監査情報がテーブルとして表示されます。
2. （オプション）監査情報の分類とフィルタリング：
   - ［Audit Type］、［Changed By］、［Object Changed］のいずれかで監査をフィルタリングするには、 をクリックします。
   - ［Changed At］、［Audit Type］、［Changed By］、［Object Changed］のいずれかで監査を分類するには、列の見出しをクリックします。
   - 検索文字列に基づいて監査をフィルタリングするには、［Search］フィールドにキーワードを入力します。
3. 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。
   - 監査ログの情報を確認します。
   - 必要に応じて、［Notes］フィールドにこの監査ログのメモを追加します。
4. 監査ログのレポートを Excel ファイルとして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: 表のなかでフィルターを適用すると、エクスポートされる監査ログにはフィルター条件を満たす監査ログのみが含まれます。
5. 監査ログの保存期間を変更するには、［境界の設定］をクリックし、［保存期間］メニューで日数を選択して、［保存］をクリックします。

ジョブとタスクのモニタリング

ジョブについては、ジョブ　タイプに基づいて、PowerProtect Data Manager UI に［Protection Jobs］、［Asset Jobs］、［System Jobs］の 3 つのウィンドウ ビューが用意されています。これらのウィンドウでは、データ保護、システム、メンテナンス ジョブのステータスをモニターし、失敗したジョブ、進行中のジョブ、最近完了したジョブの詳細を表示できます。失敗したジョブやタスクの詳細ログ、発生したエラーなどを表示して、分析またはトラブルシューティングを実行できます。

各ウィンドウのフィルタリングと分類のオプションを使用して、特定のジョブやタスクを検索し、表示される情報を管理します。 ジョブのフィルタリング、グループ化、分類 で詳細を参照してください。個別のジョブやタスクに加えて、ジョブ グループの詳細を表示することもできます。

- 保護ジョブとシステム ジョブの場合、ジョブ エントリーの横にあるジョブ ID をクリックすると、［Job ID Summary］ウィンドウが開き、このジョブ グループ、ジョブ、またはタスクの情報のみが表示されます。
- 資産ジョブの場合、テーブル内のジョブの行を選択すると、ウィンドウの右側にペインが開き、この資産ジョブの情報が表示されます。

これらのビューから、［Step Log］タブで個々のジョブやタスクのステータスをモニターし、［Details］タブでジョブやタスクの詳細を確認し、資格があれば、ジョブやタスクに［Restart］や［Cancel］などの特定の操作を実行できます。

メモ: ［Jobs］ウィンドウは、100%のスケーリングを使用して、1920 x 1080 以上の画面解像度向けに最適化されています。小さな画面では、表示の問題が発生する可能性があります。100%のスケーリングを使用して、画面解像度を 1920 x 1080 以上に設定します。

ジョブと資産のモニタリングと表示

［Protection Jobs］ウィンドウ、［Asset Jobs］ウィンドウ、［System Jobs］ウィンドウを使用して、PowerProtect Data Manager 操作のステータス情報をモニタリングおよび表示します。

これらのウィンドウ内では、［Export All］機能を使用して、ジョブ レコードと資産アクティビティーをエクスポートできます。

保護ジョブ

保護ジョブとジョブ グループを表示するには、PowerProtect Data Manager UI の左ナビゲーション ペインで、[Jobs] > [Protection Jobs] の順に選択します。

[Protection Jobs] ウィンドウが開き、保護ジョブとジョブ グループのリストが表示されます。

保護ジョブには、次が含まれます。

- クラウド階層
- クラウド保護
- 統合済みの Cloud Snapshot Manager ジョブ
  メモ: このジョブ タイプは、SAP HANA データベースには適用されません。
- エクスポートの再使用
- インデックス作成
- 保護
- レプリケート
- リストア

データベース アプリケーション資産の一元化されたバックアップとセルフサービスのバックアップとリストアの両方について、詳細情報を監視および表示できます。

メモ: [Cancel] および [Retry] オプションは、データベース アプリケーション エージェントによって作成されたセルフサービス ジョブでは使用できません。

アプリケーション資産については、ホストまたは個別の資産レベルで、[Protect] ジョブ タイプ、[Restore] ジョブ タイプ、[Replicate] ジョブ タイプをモニタリングできます。他のすべての資産タイプについては、ホストまたは個別の資産レベルで、[Protect] ジョブ タイプと [Replicate] ジョブ タイプをモニタリングできます。

資産ジョブ

[Asset Jobs] ウィンドウでは、特定の資産またはアプリケーション エージェント ホストのジョブをすべて表示したり、資産/エージェント ホスト レベルで保護アクティビティーの履歴を表示したりできます。

ジョブが実行された資産に関する情報を表示するには、PowerProtect Data Manager UI の左ナビゲーション ペインで、[Jobs] > [Asset Jobs] の順に選択します。

[Asset Jobs] ウィンドウが開き、資産のリストが表示されます。アプリケーション エージェント資産の場合は、関連付けられているホストを表示することもできます。資産名/ホスト名またはジョブ タイプでフィルタリングできます。

資産ジョブ タイプの例を次に示します。

- アプリケーション ホスト構成
- クラウド コピー リカバリー
- Cloud Disaster Recovery
- クラウド保護
- クラウド階層
- Config
- 削除
- ディザスター リカバリー
- エクスポートの再使用
- インデックス作成
- 管理
- Notify
- 保護
- プッシュ アップデート
- レプリケート
- リストア
- システム
- 確認

メモ: PowerProtect Data Manager UI の［Dashboard］には、資産/ホスト レベルで正常に実行されたジョブ、一部正常に実行されたジョブ、失敗したジョブ、キャンセルされたジョブの詳細も表示されます。

システム ジョブ

システム ジョブとジョブ グループを表示するには、PowerProtect Data Manager UI の左ナビゲーション ペインから、［Jobs］ > ［System Jobs］の順に選択します。

［System Jobs］ウィンドウが開き、システム ジョブとジョブ グループのリストが表示されます。

システム ジョブには、次が含まれます。

- Config
- コンソール
- 削除
- ディザスター リカバリー
- Cloud Disaster Recovery
- クラウド コピー リカバリー
- 検出
- 管理
- Notify
- システム
- 確認

システム ジョブは、ジョブ グループやジョブごとにモニタリングできます。

ジョブの情報

メインの［Protection Jobs］ウィンドウと［System Jobs］ウィンドウには、基本的なジョブ情報が一覧表示されます。

次の情報は、［Protection Jobs］ウィンドウおよび［System Jobs］ウィンドウで利用可能です。

表 30. ジョブの情報

列	説明
ジョブ ID	ジョブの一意の検索可能な識別子。
Status	ジョブの現在の状態を示します。ジョブのステータスは以下のいずれかになります。 ● Success ● Completed with Exceptions ● Failed ● Canceled ● Unknown ● Skipped ● Running ● Queued ● Canceling `Success` ステータスがないジョブの場合、ジョブの数がステータスの横に表示されます。
Description	ジョブの説明。
Policy Name	ジョブを開始した保護ポリシーの名前。
Assets	ジョブ グループ内の個々の資産またはタスクの数。
Job Type	保護ジョブまたはシステム ジョブのタイプ。
Asset Type	資産のタイプ。
Start Time	このジョブの開始をスケジュール設定した日付と時刻。

表 30. ジョブの情報 （続き）

列	説明
End Time	このジョブが完了した日付と時刻。 デフォルトでは、この列は表示されません。列のフィルタリングと分類の一覧を表示するには、をクリックします。
Duration	ジョブの全体的な期間。 デフォルトでは、この列は表示されません。列のフィルタリングと分類の一覧を表示するには、をクリックします。

保護ジョブの詳細の表示

保護ジョブの［Job ID Summary］ウィンドウに、特定のジョブの詳細とステータスを表示することができます。アプリケーション保護ジョブの場合は、特定のジョブと資産に関する詳細とステータスを表示することができます。この情報は、トラブルシューティングの際に、1 個または複数の資産でジョブが失敗したかどうかを判断するのに役立ちます。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Jobs］ > ［Protection Jobs］の順に選択します。
2. ジョブ名の横にあるジョブ ID をクリックします。

   ［Job ID Summary］ウィンドウが開き、すべてのジョブが表の エントリーとして一覧表示されます。

   ウィンドウに表示される情報をフィルタリング、グループ化、分類することができます。 ジョブのフィルタリング、グループ化、分類 で詳細を参照してください。

   ［Job ID Summary］ウィンドウの上部には、ポリシー名、ジョブ タイプ、および資産タイプが表示されます。

   次の図に示すように、全体的なジョブ グループのメトリックと詳細も表示されます。

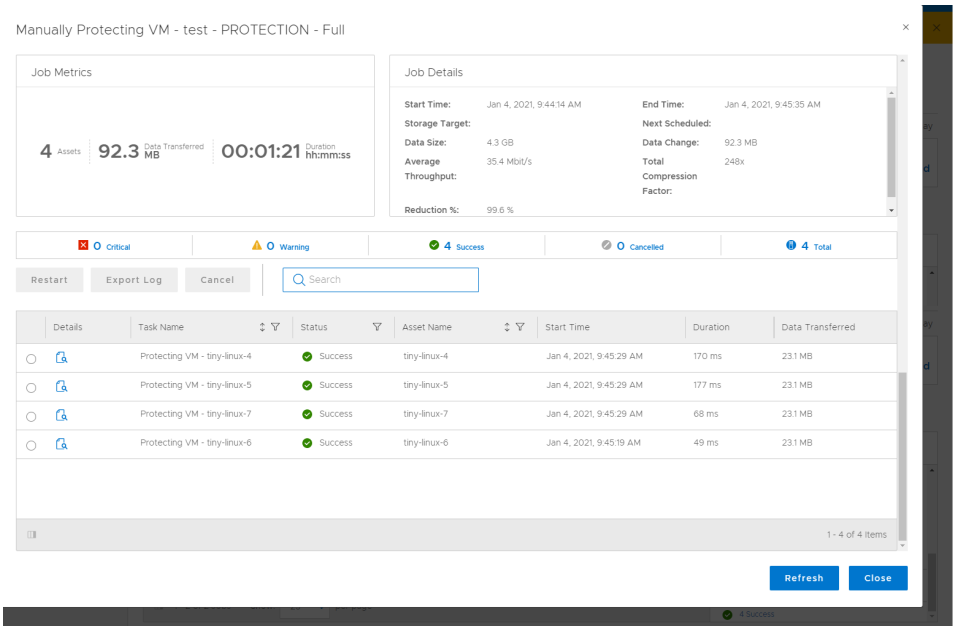


図 6. ジョブ メトリックとジョブの詳細

［Job Metrics］セクションには、資産の数、転送されたデータの合計サイズ、ジョブ グループの全体の期間が表示されます。ジョブ グループ内のジョブの合計継続期間は、ジョブ メトリックに示されている期間よりも短くなります。完了したジョブ グループの一部である保護ジョブを再開すると、ジョブ メトリックに示されている期間には、ジョブ グループが完了してからジョブが再開されるまでの経過時間は含まれません。また、再試行されたジョブの実行にかかる時間は含まれません。

［Job Details］セクションには、ジョブの開始と終了時刻、保護ストレージ ターゲット、平均データ転送レート、最後の保護ジョブ以降に変更されたデータの量、平均スループット、適用された圧縮率などの具体的な情報が表示されます。Microsoft SQL Server データベースのリストア ジョブの場合、一部のフィールドは適用されないか、ゼロに設定されます。

Oracle データベース資産が含まれているジョブ グループに対しては、ジョブのメトリックと詳細が表示されない、または不完全である場合があります。

［Hide Summary］をクリックしてジョブのメトリックと詳細を非表示にするか、［Show Summary］をクリックしてジョブのメトリックと詳細を表示します。

ジョブの上にマウスを置くと、［Job ID Summary］にそのジョブの進行状況を示すメッセージが表示されます。ジョブによっては、あるいは問題が検出されると、次のいずれかのステータスが表示されます。

- `No reported issues`：ジョブに影響する問題はありません。
- `Timeout issues`：タイムアウトの問題がジョブに影響している可能性があります。
- `Connectivity issues`：ネットワーク接続の問題がジョブに影響している可能性があります。
- `Stats stall issues`：このジョブの進行状況は停止しています。

［Job ID Summary］ウィンドウには、特定のジョブと資産のサマリー データがテーブル ビューに表示されます。グループ化された資産の場合、ホスト レベルのエントリーは、ホスト上のすべての資産に対する特定のメトリックの集計値を示します。

次の表に、ウィンドウに表示される可能性がある列を示します。すべての資産タイプの［Job ID Summary］ウィンドウに、すべての列が表示されるわけではありません。

表 31. ［Job ID Summary］ウィンドウの詳細

列	説明
Details	［Details］列の🔍をクリックすると、ジョブの統計情報とサマリー情報が表示されます。
Asset	資産のジョブ名。
Status	ジョブの現在の状態を示します。ジョブのステータスは以下のいずれかになります。 ● Success ● Completed with Exceptions ● Failed ● Canceled ● Unknown ● Skipped ● Running ● Queued ● Canceling
Size	資産のジョブのサイズ。
Data Transferred	ストレージに転送されるデータの合計。
Reduction %	ジョブのストレージ容量の合計削減率。
Start Time	このジョブの開始をスケジュール設定した日付と時刻。
End Time	このジョブが完了した日付と時刻。
Error Code	ジョブが正常に完了しなかった場合、数値のエラー コードが表示されます。エラー コードをダブル クリックすると、詳細な説明が表示されます。
Host/Cluster/Group Name	資産に関連づけられているホスト名、クラスター、またはグループ名。
Duration	ジョブの全体的な期間。この列は、アプリケーション資産のジョブ タイプが［Protect］および［Replicate］である場合にのみ表示されます。
Asset Size	資産の合計サイズ（バイト単位）。
Data Compressed	クライアントによるデータの圧縮後に使用される容量（バイト単位）。この列は、アプリケーション資産のジョブ タイプが［Protect］および［Replicate］である場合にのみ表示されます。
Download log	エクスポートおよびダウンロードできる資産、またはタスクの詳細ログ。

3. ジョブの詳細とサマリー情報を表示するには、ジョブの隣にある［Details］列の🔍をクリックするか、 > をクリックしてジョブ グループのエントリーを展開します。

   グループ化された資産の場合、［Job ID Summary］ウィンドウには、ジョブ グループ内の各資産に関する個々のジョブが一覧表示されます。

   右のペインに、ジョブまたはタスクに関する次の情報が表示されます。

- ［Step Log］：ジョブまたはタスクの完了したステップ、または進行中のステップのリストを表示し、各ステップを完了するまでに要した時間を示します。ジョブ ステップがまだアクティブな場合は、［Step Log］には、ステップの実行中の側面に関する詳細な説明も表示されます。
- ［Details］：開始時間と終了時間、資産のサイズ、期間、その他の詳細などの統計情報とサマリー情報が表示されます。
- ［Error］：失敗したジョブのエラーに関する詳細を表示します。
- ［Canceled］：キャンセルされたジョブの詳細を表示します。
- ［Skipped］：スキップされたジョブの詳細を表示します。
- ［Unknown］：不明なステータスのジョブの詳細を表示します。

資産ジョブの詳細の表示

［Asset Jobs］ウィンドウの右ペインで、PowerProtect Data Manager のアクティブなジョブ、完了したジョブ、または失敗したジョブに含まれている資産の詳細とステータス情報を表示できます。この情報は、ジョブの進行状況を追跡する場合、またはトラブルシューティングを行って特定の資産の構成または保護が失敗した理由を判断する場合に役立ちます。

このタスクについて

ジョブが進行中の場合、または過去 45 日以内に資産に対して実行された場合、その資産は［Infrastructure］ > ［Assets］ウィンドウにリンク付きで表示されます。このリンクをクリックすると、［Jobs］ > ［Asset Jobs］ウィンドウが開きます。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Jobs］ > ［Asset Jobs］の順に選択します。
   デフォルトでは、過去 24 時間以内にジョブが実行された資産のリストが表に表示されます。

   次の表に、カスタマイズされた列に応じて表示される可能性のある資産ジョブの詳細を示します。

表 32. ［Asset Jobs］ウィンドウの詳細

列	説明
Asset	保護ジョブ内の資産の名前。
Host	アプリケーション エージェント資産の場合、資産に関連付けられているホスト名。
Status	ジョブの現在の状態を示します。ジョブのステータスは以下のいずれかになります。 ● Success ● Completed with Exceptions ● Failed ● Canceled ● Unknown ● Skipped ● %（ジョブの進行状況を示す） ● Queued ● Canceling
Policy Name	この資産を含む保護ポリシー
Job Type	サポートされる資産ジョブ タイプには、構成、保護、レプリケート、リストア、クラウド階層があります。
Asset Type	特定のタイプの資産を示します。例：VMware の仮想マシン。
Start Time	このジョブの開始をスケジュール設定した日付と時刻。
Duration	ジョブの全体的な期間。
Details	資産の行を選択すると、右ペインに［Details］タブが表示され、統計情報とサマリー情報を確認できます。
Step Log	右ペインで［Step Log］タブを選択すると、資産ジョブに対して完了したステップのリストと、各ステップの完了にかかった時間を表示できます。
Errors	ジョブを正常に完了できなかった場合は、資産の行を選択して右ペインで［Errors］タブを開きます。ここで、エラーと数値エラー コードを確認できます。

2. 必要に応じて、表示可能な資産ジョブを次のようにカスタマイズします。
   a. 別の期間を選択するか、［Start Time］ボックスをクリックして時間範囲を指定します。

b. 各列のフィルターを使用して、検索条件に一致する資産のみを表示します。
c. ウィンドウのサマリー情報に表示されるステータスをクリックすると、特定のジョブ ステータスの資産のみが表示されます。
d. 各列内の上下の矢印をクリックして、情報を分類します。

ビューをカスタマイズすると、時間範囲、検索フィルター、ステータス フィルターは、フィルターがクリアされるまで PowerProtect Data Manager UI で維持されます。 ジョブのフィルタリング、グループ化、分類 で詳細を参照してください。

3. 資産ジョブの行を選択します。

次の図に示すように、ウィンドウの右側にペインが表示されます。ペインの上部にある→|をクリックすると、詳細をいつでも非表示または表示にすることができます。このペインには次のタブがあります。

- [Step Log]：資産ジョブの完了したステップ、または進行中のステップのリストを表示し、各ステップを完了するまでに要した時間を示します。ジョブ ステップがまだアクティブな場合は、[Step Log] には、ステップの実行中の側面に関する詳細な説明も表示されます。

  メモ: [Step Log] と説明は、バックアップ、リストア、ディザスター リカバリー操作に関連するジョブに対してのみ表示されます。
- [Details]：開始時間と終了時間、資産のサイズ、期間、その他の詳細などの統計情報とサマリー情報が表示されます。
- [Error]：資産ジョブが失敗した場合、または完了したが例外が発生した場合に、発生したエラーを表示します。

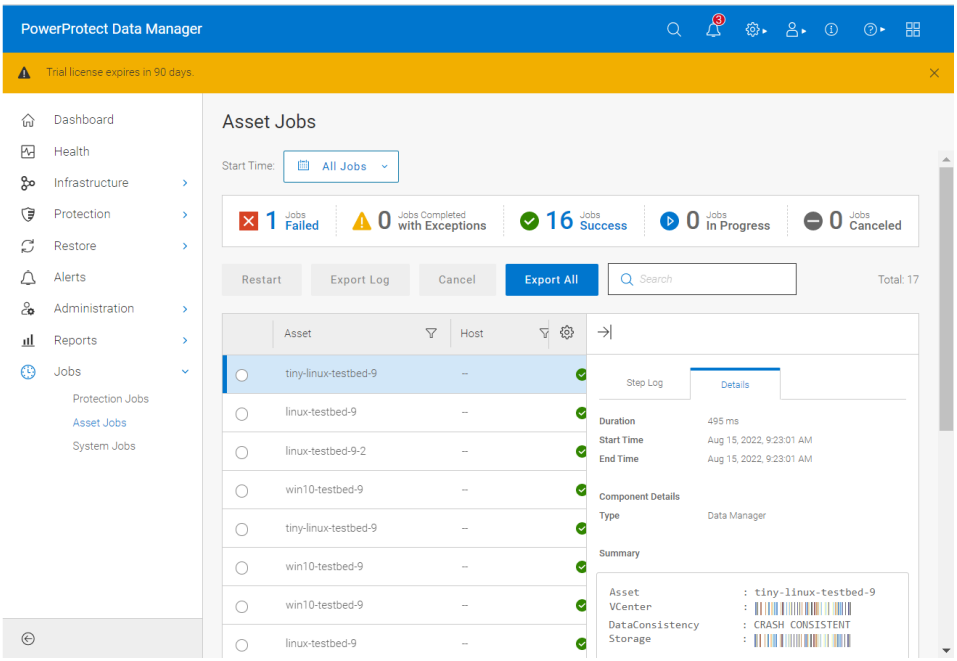


図 7. 資産の詳細、ステップ ログ、エラー

4. ジョブが失敗した場合、キャンセルされた場合、完了したが例外が発生した場合、再開の対象である場合は、資産の横にあるラジオ ボタンを選択し、[Restart] をクリックします。
5. 資産ジョブのステップ ログをエクスポートするには、資産ジョブの横にあるラジオ ボタンを選択して [Export Log] をクリックするか、[Export All] をクリックしてすべての資産ジョブを含む `.csv` ファイルを作成します。

システム ジョブおよびタスクの詳細の表示

システム ジョブの [Job ID Summary] ウィンドウで、特定のジョブやタスクの詳細とステータスを表示できます。この情報は、トラブルシューティングの際に、1 個または複数のジョブやタスクのうちどれがジョブの失敗の原因となったかを判断するのに役立ちます。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、[Jobs] > [System Jobs] の順に選択します。
2. ジョブ名の横にあるジョブ ID をクリックします。

   [Job ID Summary] ウィンドウが開き、すべてのシステム ジョブまたはタスクのリストが表示されます。

   ウィンドウに表示される情報をフィルタリング、グループ化、分類することができます。 ジョブのフィルタリング、グループ化、分類 で詳細を参照してください。

   ジョブとタスクでは、ウィンドウの下部に表が表示されます。個々のタスクの成功または失敗は、[Status] 列に示されます。失敗したジョブやタスクにアクションが必要な場合は、[Critical] ステータスが表示されます。

アプリケーション資産とアプリケーション システムのスケジュールされた検出のジョブ ステータスとサマリー情報を表示できます。検出ジョブが失敗した場合、PowerProtect Data Manager はエラーの詳細と問題を解決するための手順を表示します。アラートは［Alerts］ウィンドウにも生成されます。

ジョブやタスクの上にマウスを置くと、［Job ID Summary］にそのジョブの進行状況を示すメッセージが表示されます。ジョブによっては、あるいは問題が検出されると、次のいずれかのステータスが表示されます。

- `No reported issues`：ジョブに影響する問題はありません。
- `Timeout issues`：タイムアウトの問題がジョブに影響している可能性があります。
- `Connectivity issues`：ネットワーク接続の問題がジョブに影響している可能性があります。
- `Stats stall issues`：このジョブの進行状況は停止しています。

［Job ID Summary］ウィンドウには、特定のジョブとタスクのサマリー データがテーブル ビューに表示されます。次の表に、ウィンドウに表示される可能性がある列を示します。すべての資産タイプの［Job ID Summary］ウィンドウに、すべての列が表示されるわけではありません。

表 33. ［Job ID Summary］ウィンドウの詳細

列	説明
Details	［Details］列の🔍をクリックすると、ジョブやタスクの統計情報とサマリー情報を表示できます。
Task Name	タスクの名前。
Status	ジョブやタスクの現在の状態を示します。ジョブやタスクは、次のいずれかの状態になります。 ● Success ● Completed with Exceptions ● Failed ● Canceled ● Unknown ● Skipped ● Running ● Queued ● Canceling
Asset	資産の名前。
Start Time	ジョブやタスクが開始される日付と時刻。
Duration	ジョブやタスクの全体的な期間。
Data Transferred	ストレージに転送されるデータの合計。

3. ジョブやタスクの詳細とサマリー情報を表示するには、個々のジョブやタスクの横にある［Details］列の🔍をクリックします。

   右のペインに、ジョブまたはタスクに関する次の情報が表示されます。

   - ［Step Log］：ジョブまたはタスクの完了したステップ、または進行中のステップのリストを表示し、各ステップを完了するまでに要した時間を示します。ジョブ ステップがまだアクティブな場合は、［Step Log］には、ステップの実行中の側面に関する詳細な説明も表示されます。

     メモ: ［Step Log］と説明は、バックアップ、リストア、ディザスター リカバリー操作に関連するジョブに対してのみ表示されます。
   - ［Details］：開始時間と終了時間、資産のサイズ、期間、その他の詳細などの統計情報とサマリー情報が表示されます。
   - ［Error］：失敗したジョブのエラーに関する詳細を表示します。
   - ［Canceled］：キャンセルされたジョブの詳細を表示します。
   - ［Skipped］：スキップされたジョブの詳細を表示します。
   - ［Unknown］：不明なステータスのジョブの詳細を表示します。

ジョブのフィルタリング、グループ化、分類

［Protection Jobs］ウィンドウ、［Asset Jobs］ウィンドウ、［System Jobs］ウィンドウには、表示される情報をフィルタリング、グループ化、分類するためのオプションがあります。

ステータスごとのジョブのフィルタリング

ウィンドウの上部にあるクイック フィルターを使用して、ステータスごとにジョブをフィルタリングします。デフォルトでは、ステータスに関係なくすべてのジョブが表示されます。特定のステータスのジョブのみを表示するには、ウィンドウの上部で、次のいずれかのオプションを選択します。

- ［失敗］
- ［Completed with Exceptions（完了したが例外発生）］
- ［成功］
- ［キャンセル済み］
- ［進行中］

［In Progress］のジョブには、［Running］、［Queued］、および［Canceling］のジョブが含まれます。

特定のステータスごとにジョブをフィルタリングするクイック フィルターを選択すると、ウィンドウの表の上にフィルターが表示されます。選択したステータスごとのフィルタリングを停止するには、［x］をクリックします。

ジョブの開始時間ごとのフィルタリング

指定された期間に開始したジョブを表示するには、［Start Time］フィルターを使用します。ジョブは最大 45 日間保持されます。以下オプションのいずれかを選択してください。

- すべてのジョブ
- 直近 24 時間
- 直近 3 日間
- 直近 7 日間
- Last 30 days
- 特定の日付
- カスタムの日付範囲

ジョブのグループ化

［Protection Jobs］ウィンドウと［System Jobs］ウィンドウで、ジョブを選択し、［Job ID Summary］ウィンドウを表示します。［Job ID Summary］ウィンドウの［Group by］機能には、保護ジョブ内の資産をグループ化するオプションがあります。

次の資産タイプは、［Group by］機能をサポートしています。

- Microsoft SQL Server データベース
- Microsoft Exchange Server データベース
- Oracle Database
- ファイル システム s
- SAP HANA データベース
- Kubernetes クラスター
- ネットワーク接続型ストレージ(NAS)共有
- VMware 仮想マシン

保護ジョブの資産をグループ化するには、そのジョブの ［Job ID Summary］ウィンドウで、［Group By］ドロップダウン リストからオプションを選択します。すべての資産を表示するには、［Group by］ > ［None］の順に選択します。例えば、ESX ホスト別に仮想マシン資産をグループ化するには、［Group by］ > ［ESX Host］をクリックします。

次の表に、使用可能な［Group by］オプションを示します。

表 34. Group by オプション

資産タイプ	オプション
Microsoft SQL Server データベース	SQL ホスト
	SQL インスタンス
Oracle データベース	Oracle ホスト
	Oracle インスタンス
ファイル システム	ファイル システム ホスト

表 34. Group by オプション （続き）

資産タイプ	オプション
	ファイル システム ホスト OS
Microsoft Exchange Server データベース	Exchange ホスト
SAP HANA データベース	SAP HANA ホスト
Kubernetes	Kubernetes クラスター
	Kubernetes ネームスペース
NAS	NAS サーバ
	NAS アプライアンス
VMware 仮想マシン	データストア
	ESX ホスト
	仮想データセンター
	VM ゲスト OS
	VMware クラスター

メモ: 現在、［Group by］フィルターは、［Protect］ジョブ タイプでのみ使用可能です。

Search Filter

［Search］フィールドを使用して、検索文字列に基づいてジョブをフィルタリングできます。［Search］フィールドにキーワードを入力すると、入力結果が PowerProtect Data Manager UI によってフィルターされます。検索フィルターをクリアするには、［Search］フィールドからすべてのキーワードを削除します。

表内の情報のフィルタリングと分類

表の列に表示される情報をフィルタリングしたり分類したりすることができます。列見出しの をクリックすると、表の列の情報をフィルタリングできます。または、表の列見出しをクリックすると、その列を分類できます。

列のフィルタリングと分類の一覧を表示するには、 をクリックします。ジョブのタイプによっては、使用可能なフィルタリングと分類の列が異なる場合があります。

ジョブやタスクでは、次のフィルタリングと分類のオプションを使用できます。

表 35. 保護ジョブ、資産ジョブ、システム ジョブのウィンドウ

フィルタリング オプション	分類オプション
［Job ID］、［Status］、［Description］、［Policy Name］、［Job Type］、［End Time］、および［Asset Type］ごとにジョブやタスクをフィルタリングします。	［Job ID］、［Description］、［Policy Name］、［Job Type］、［Asset Type］、［Start Time］、および［End Time］ごとにジョブやタスクを分類します。

表 36. 保護ジョブの［Job ID Summary］ウィンドウ

フィルタリング オプション	分類オプション
［Asset］、［Status］、［Error Code］、［Start Time］、または［End Time］ごとにジョブをフィルタリングします。 アプリケーション資産については、［Host/Cluster/Group Name］ごとにジョブをフィルタリングすることもできます。 **メモ:** アプリケーション資産の場合、これらのオプションは［Group by］> ［None］を選択した場合にのみ使用できます。	［Asset］、［Status］、［Error Code］、［Size］、［Data Transferred］、［Reduction %］、［Start Time］、［End Time］、または［Duration］ごとにジョブを分類します。 アプリケーション資産については、［Host/Cluster/Group Name］ごとにジョブを分類することもできます。 **メモ:** アプリケーション資産の場合、これらのオプションは［Group by］> ［None］を選択した場合にのみ使用できます。

表 37. システム ジョブの［Job ID Summary］ウィンドウ

フィルタリング オプション	分類オプション
［Task Name］、［Status］、［Asset］、または［Start Time］ごとにジョブやタスクをフィルタリングします。	［Task Name］、［Status］、［Asset］、［Start Time］、［Duration］、または［Data Transferred］ごとにジョブやタスクを分類します。

ジョブまたはタスクの手動再開

失敗した仮想マシンのバックアップを手動で再開できます。

このタスクについて

［Restart］をクリックすると、スケジュール設定されたアクティビティ ウィンドウに関係なく、ジョブまたはタスクがただちに再起動します。

次の点に注意してください。

- 保護とクラウド データ リカバリーの両方の目的に関するポリシーが失敗した場合、クラウド データ リカバリーのジョブはキャンセルとなり、再開できません。
- Cloud Snapshot Manager ジョブを再開することはできません。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Jobs］ > ［Protection Jobs］、［Jobs］ > ［Asset Jobs］、［Jobs］ > ［System Jobs］のいずれかを選択します。
   ウィンドウに、完了したジョブと実行中のジョブがすべて表示されます。
2. 失敗したジョブまたはジョブ グループを再開するには、リストから失敗したジョブまたはジョブ グループを選択して、［Restart］をクリックします。ジョブが再開の対象外である場合、ボタンはグレー表示されます。
3. ［Job ID Summary］ウィンドウから失敗したシステム、保護ジョブ、タスクを再開するには、次の手順を実行します。
   a. ジョブまたはジョブ グループの名前の横にあるジョブ ID をクリックします。
      ［Job ID Summary］ウィンドウが開き、すべてのジョブまたはタスクのリストが表示されます。
   b. リストからジョブまたはタスクを選択し、［Restart］をクリックします。

タスクの結果

ジョブまたはタスクの再開後、ステータスは［Running］または［Queued］を示します。

メモ: 完了したジョブ グループに含まれている保護ジョブを再開すると、［Job Metrics］には、再試行されたジョブの実行にかかる時間に加えて、ジョブ グループが完了してからジョブが再開されるまでの経過時間を含む期間が表示されます。

ジョブまたはタスクの自動再開

バックアップ ジョブが失敗した場合、またはジョブ内のタスクのいずれかが失敗した場合は、`entrypoint.sh` ファイルで自動再試行を構成して、障害の自動再起動を有効にすることができます。自動再試行は、ネットワークまたはサービスの割り込みなど断続的な問題が原因で発生した場合に役立つことがあります。

前提条件

PowerProtect Data Manager では、ワークフロー サービスなどの自動再試行に必要な一部のサービスは、ドッカー コンテナーに移動されました。自動再試行を有効にするには、ワークフロー サービスが ドッカーで実行されていることを確認します。

このタスクについて

自動再試行は、仮想マシンと File System agent の保護操作の日次、週次、または月次のスケジュールでのみサポートされています。

手順

1. SSH を使用して PowerProtect Data Manager サーバーにログインします。
2. 次のように入力して、ワークフロー コンテナーから `entrypoint.sh` ファイルをコピーします。

```
docker cp workflow:/workflow/bin/entrypoint.sh .
```

3. 次の行を `entrypoint.sh` に追加して、自動再試行を構成します。
   a. 「**vi entrypoint.sh**」と入力します
   b. 出力の最後の行の前に、次を追加します。
      **-Denable.auto.retry.scheduler=true **
      メモ: 自動再試行はデフォルトで無効になっています。この行を追加した後、任意の時点でこの設定を無効にするには、エントリーを「**-Denable.auto.retry.scheduler=false **」に変更します

4. オプションとして、次のアプリケーション プロパティをファイルに追加して、自動再試行の最大数と、以降の自動再試行する時間間隔を指定します。
   **-Dfailed.job.retry.max.count=2 **
   **-Dfailed.job.retry.interval=PT30M **
   メモ: 前記で指定した値が推奨されるデフォルト値です。自動再試行は、アクティビティ ウィンドウ中にのみ行われます。PowerProtect Data Manager UI で手動再試行を実行した場合、この再試行は自動再試行最大数にカウントされません。
   インターバル期間には、ISO-8601 形式で値を指定する必要があります。

5. 次のように入力して、`entrypoint.sh` ファイルをワークフロー コンテナーに保存します。
   docker cp entrypoint.sh workflow:/workflow/bin/
6. 次のいずれかの方法で、ワークフロー サービスを再開します。
   - 「**docker container restart workflow**」と入力します
     メモ: この方法を使用して構成を正常に適用するには、コンテナーを再起動する必要があります。ワークフロー サービスまたは PowerProtect Data Manager オペレーティング システムを再起動すると、構成が失われます。
   - 次のように入力して、ドッカー イメージを保存し、ワークフロー サービスを再起動します。例：
     docker commit workflow dpd/ppdm/ppdmc-workflow:*PowerProtect Data Manager version*
     workflow restart
     ここで、*PowerProtect Data Manager version* は、システムに導入されている PowerProtect Data Manager バージョンです。
     この方法を使用して、ドッカー イメージをリストアした後で、構成の変更を恒久的に適用することができます。

タスクの結果

構成後、ワークフロー サービスは 30 分ごとに実行するようにスケジュール設定されており、ジョブまたはタスクが失敗したかどうかを判断します。再起動が発生した場合、ステータスは［Running］または［Queued］と表示されます。失敗したジョブまたはタスクが再開されたかどうかを表示するには、PowerProtect Data Manager UI の［Jobs］ウィンドウに移動して、［Running］または［Queued］を選択します。

PowerProtect Data Manager アップグレード後のミスファイア ジョブの再開

アップグレード中に、PowerProtect Data Manager システムはメンテナンス モードに入ります。PowerProtect Data Manager システムのメンテナンス モード中に、キューに登録されていないジョブや、実行がスケジュール設定されているジョブはすべて失われます。このような失われたジョブを、ミスファイアと呼びます。このリリース時点で、PowerProtect Data Manager は Quartz Scheduler を使用して、サービスのリカバリー時またはスケジュールの再開時にスケジュール設定されたワークフローを再開しています。

このタスクについて

ジョブのトリガーおよびデータの消失は、データベース アプリケーションに格納されます。アップデート中など、スケジュール設定されたサービスが停止している場合、PowerProtect Data Manager システムの再作動時に、Quartz Scheduler によってこのデータのリカバリーとジョブの再開が行われます。

メモ: 現在のリリースでは、この機能はデフォルトで有効になっています。

このミスファイア機能は、`entrypoint.sh` ファイルを構成することで有効または無効にできます。

手順

1. SSH を使用して PowerProtect Data Manager サーバーにログインします。
2. 次のように入力して、スケジューラー コンテナーから `entrypoint.sh` ファイルのコピーを行います。
   docker cp scheduler:/scheduler/bin/entrypoint.sh .

3. `entrypoint.sh` ファイル内のミスファイア条件を次のように構成します。

   メモ: 出力の最後の行である「 **-jar/$ {APP_NAME}/lib/scheduler-core.jar**)」の前に、それぞれのミスファイア条件の行を追加します。

   a. 各ジョブのミスファイアとトリガーを一度で有効にするには、次のプロパティとそれに対応する値を追加します。

   **-Dspring.quartz.properties.misfire.cron.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_FIRE_AND_PROCEED **

   メモ: この条件は、デフォルトで有効です。

   **-Dspring.quartz.properties.misfire.calendar.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_FIRE_AND_PROCEED **

   b. ミスファイアの発生回数に応じた各ジョブのミスファイアとトリガーを有効にするには、次のプロパティとそれに対応する値を追加します。

   **-Dspring.quartz.properties.misfire.cron.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_IGNORE_MISFIRES **

   **-Dspring.quartz.properties.misfire.calendar.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_IGNORE_MISFIRES **

   c. ミスファイアを無効にするには、次のプロパティとそれに対応する値を追加します。

   **-Dspring.quartz.properties.misfire.cron.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_DO_NOTHING **

   **-Dspring.quartz.properties.misfire.calendar.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_DO_NOTHING **

4. 次のように入力して、`entrypoint.sh` ファイルをスケジューラー コンテナーに保存します。

   docker cp entrypoint.sh scheduler:/scheduler/bin/

5. 次のいずれかの方法で、スケジューラー サービスを再起動します。
   - 「**docker container restart scheduler**」と入力します

     メモ: この方法を使用して構成を正常に適用するには、コンテナーを再起動する必要があります。スケジューラー サービスまたは PowerProtect Data Manager オペレーティング システムを再起動すると、構成が失われます。
   - 次のように入力して、ドッカー イメージを保存し、スケジューラー サービスを再起動します。

     docker commit scheduler dpd/ppdm/ppdmc-scheduler:*PowerProtect Data Manager version*

     scheduler restart

     ここで、*PowerProtect Data Manager version* は、システムに導入されている PowerProtect Data Manager バージョンです。

     この方法を使用して、ドッカー イメージをリストアした後で、構成の変更を恒久的に適用することができます。

     メモ: `commit` コマンドで指定した PowerProtect Data Manager バージョンが、システムに導入されている PowerProtect Data Manager バージョンと一致していることを確認します。

ジョブまたはタスクのキャンセル

PowerProtect Data Manager UI で、まだ進行中のバックアップやリストア、またはタスクがキューに登録されたときに、資産保護とレプリケーションのアクティビティーをキャンセルできます。

このタスクについて

メモ: [Cancel] 操作は、以下のサポートされているジョブとタスクでのみ使用できます。

- バックアップおよびリストア：
  - 仮想マシン資産
  - Kubernetes 資産
  - NAS 資産
  - ファイル システム資産
  - Microsoft SQL Server 資産

- ブロック ボリューム資産
- サーバーの DR
- Cloud DR

- バックアップ（のみ）：
  - Microsoft Exchange Server 資産
  - Oracle 資産
  - SAP HANA 資産
  - アプリケーション対応資産バックアップのトランザクション ログ
- レプリケーション
- コンプライアンス
  - コピーの削除
  - コンプライアンスの確認
  - フル バックアップへの自動プロモーション
  - MTree のクリーニングまたはユーザーの削除
  - オンデマンド アップデート保存
- サポート
  - テレメトリー データの通信
  - ジョブおよびジョブ グループ ログのエクスポート
  - ログ バンドルの追加

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Jobs］ > ［Protection Jobs］、［Jobs］ > ［Asset Jobs］、［Jobs］ > ［System Jobs］のいずれかを選択します。
   関連する［Jobs］ウィンドウに、完了したジョブと実行中のジョブがすべて表示されます。
2. ジョブまたはジョブ グループをキャンセルするには、進行中のジョブやジョブ グループを選択して、［Cancel］をクリックします。
   メモ: ジョブがほぼ完了していると、キャンセルが失敗する場合があります。キャンセルが失敗した場合は、ジョブをキャンセルできないことを示すメッセージが表示されます。

   ウィンドウには、キャンセルされたジョブまたはジョブ グループのステータスが表示されます。キャンセルが成功した場合、ステータスは最終的に［Canceled］に変わります。キャンセルに失敗した場合は、ステータスが［Success］または［Critical］のいずれかである可能性があります。
3. 保護ジョブとシステム ジョブの場合、［Job ID Summary］ウィンドウでジョブやタスクを個別にキャンセルするには、次の手順を実行します。
   a. ジョブまたはジョブ グループの名前の横にあるジョブ ID をクリックします。
      ［Job ID Summary］ウィンドウが開き、すべてのジョブまたはタスクのリストが表示されます。
   b. 進行中のジョブやタスクを選択して、［Cancel］をクリックします。
      メモ: ジョブやタスクがほぼ完了していると、キャンセルが失敗する場合があります。キャンセルが失敗した場合は、タスクをキャンセルできないことを示すメッセージが表示されます。
   c. ［Close］をクリックします。
   ［Job ID Summary］ウィンドウには、キャンセルされたジョブやタスクのステータスが表示されます。キャンセルが成功した場合、ステータスは最終的に［Canceled］に変わります。キャンセルに失敗した場合は、ステータスが［］または［Critical］のいずれかである可能性があります。

ログのエクスポート

PowerProtect Data Manager UI を使用して、ジョブ、資産、またはタスクの詳細なログをエクスポートおよびダウンロードして、分析やトラブルシューティングを実行できます。

ステータスにかかわらず、ジョブ、資産またはタスクのログをエクスポートおよびダウンロードできます。ログをエクスポートした後、をクリックしてダウンロードできます。

ジョブのログのエクスポート

PowerProtect Data Manager UI を使用して、保護ジョブまたはシステム ジョブのログをエクスポートおよびダウンロードできます。

このタスクについて

次の状況では、PowerProtect Data Manager により、ログ エクスポート機能が制限されます。

- ジョブが別の PowerProtect Data Manager テナントのジョブである。
- 現段階で、次の資産ソースについて、ジョブが外部ログのエクスポートに対応している。
  - 仮想マシン
  - Kubernetes
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - ファイル システム
  - Oracle
  - SAP HANA
  - Network-attached storage (NAS)

このような状況では、代わりにログ バンドルを作成します。ログ バンドルを追加するには、PowerProtect Data Manager UI で、［Settings］ > ［Support］ > ［Logs］を選択します。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Jobs］ > ［Protection Jobs］、［Jobs］ > ［Asset Jobs］、［Jobs］ > ［System Jobs］のいずれかを選択します。
   関連する［Jobs］ウィンドウに、すべてのジョブが表示されます。
2. リストからジョブを選択し、［Export Log］をクリックします。
   ［Download Log］列の資産またはタスクの横にある にカーソルを合わせると、進行状況が表示されます。ログのエクスポートが完了したら、ログをダウンロードできます。
3. ジョブの ID の横にあるをクリックして、エクスポートされたログをダウンロードします。

資産またはタスクのログのエクスポート

個々の資産またはタスクのログをエクスポートおよびダウンロードできます。

手順

1. PowerProtect Data Manager UI の左ナビゲーション ペインで、［Jobs］ > ［Asset Jobs］の順に選択します。
   ［Asset Jobs］ウィンドウが表示されます。
2. 資産の行を選択し、［Export Log］をクリックします。
   ［Download Log］列の資産またはタスクの横にある にカーソルを合わせると、進行状況が表示されます。ログのエクスポートが完了したら、ログをダウンロードできます。
3. ［Download Log］列のをクリックして、エクスポートされたログをダウンロードします。

アラート、ジョブ、タスクの制限事項

アラート、ジョブ、タスクに関連する次の制限事項を確認してください。

進行中のジョブの場合、詳細ペインに「エラー」タブが表示され、「失敗」と表示されます

進行中のジョブの［Details］ペインを開くと、［Error］タブが表示され、エラーの詳細に［Failed］と誤って表示されます。

［解決策］

進行中のジョブの［Error］タブは無視します。

ロックボックス エントリーを再作成後、PowerProtect Data Manager の［Protection Jobs］ウィンドウにセルフサービス ジョブが表示されない

Windows と Linux の両方でロックボックス エントリーを再作成すると、PowerProtect Data Manager の［Protection Jobs］ウィンドウにセルフサービス ジョブが表示されません。

［解決策］

エージェント サービスを再起動するか、システム時間を変更します（+24 時間）。

表示可能なバックアップ ジョブの履歴を直近 10,000 件に制限

バックアップ ジョブの履歴を表示している際に、インターフェイスで 10,000 個より前のバックアップ ジョブを表示するページに移動しようとすると、次のエラーが表示されます。

```
error: 416: "The query will return too many results."
```

［解決策］

以前のバックアップ ジョブを表示するには、以前のバックアップ ジョブを含むフィルターを使用しますが、エントリー数を 10,000 個未満に制限します。

PowerProtect Data Manager ダッシュボードの合計保護ジョブ数にスキップされたジョブが含まれていない

ダッシュボードの［Jobs | Protection］ウィジェットに表示される［Total Jobs］数に、スキップされたジョブは含まれていません。そのため、この数は［Protection Jobs］ウィンドウに表示される保護ジョブの合計数を反映したものではありません。

10

システム設定の変更

トピック：

システム設定

PowerProtect Data Manager UI を使用して、PowerProtect Data Manager の導入時に通常構成されるシステム設定を変更することができます。

［System Settings］にアクセスするには、  をクリックします。

ネットワーク設定の変更

PowerProtect Data Manager アプライアンスのホスト名または IP アドレスを変更する場合、またはサブネット マスク、ゲートウェイ、DNS サーバーなどの他のネットワークの設定を変更する場合は、次の手順を実行します。

このタスクについて

注意: PowerProtect Data Manager アプライアンスのホスト名または IP アドレスを変更するには、外部コンポーネントの継続的な動作を確認するため、さらにアクションが必要になる場合があります。詳細については、ホスト名または IP アドレスの変更を参照してください。

手順

1. PowerProtect Data Manager UI で  をクリックしてから、［Default Network］をクリックします。
2. 必要に応じて次のフィールドのアップデートを行います。
   - ［Hostname］
   - ［Primary DNS］
   - ［Secondary DNS］
3. ［Configuration Details］ペインで、［Edit］をクリックし、必要に応じて次に示されている IP アドレスに関するフィールドのアップデートを行います。
   - ［IP Address］
   - ［Subnet Mask］
   - ［Gateway］
4. ［Save］をクリックします。

ホスト名または IP アドレスの変更

PowerProtect Data Manager アプライアンスのホスト名または IP アドレスを変更すると、登録済みのアプリケーション ホストや VM Direct Engine に影響が出ることかあります。

File System Agent を使用していて、PowerProtect Data Manager の IP アドレスが変更された場合、PowerProtect Data Manager で新しい IP アドレスを使用して File System agent ホストを再登録する必要があります。PowerProtect Data Manager の IP アドレスの変更後にエージェントを再登録するには、『*PowerProtect Data Manager* ファイル システム ユーザー ガイド』に記載されている手順を参照してください。

VM Direct Engine が VMware 仮想マシン、Tanzu Kubernetes、NAS 保護用に導入されている場合は、保護エンジンを再導入します。『*PowerProtect Data Manager* 仮想マシン ユーザー ガイド』に、手順が記載されています。

DNS 検索ドメインの変更

PowerProtect Data Manager アプライアンスの DNS 検索ドメインを変更するには、次の手順を実行します。

このタスクについて

PowerProtect Data Manager は、アプライアンスのドメイン名に基づいて検索ドメインを自動的に構成します。たとえば、PowerProtect Data Manager の FQDN が `ppdm.subdomain.domain.com` の場合、検索ドメインは `subdomain.domain.com` として構成されます。この値は変更でき、複数の検索ドメインを使用できます。

手順

1. `ssh` を使用して PowerProtect Data Manager にログ インします。
2. 次のコマンドを実行します。

```
cd /usr/local/brs/puppet/scripts
./search_domains.sh
```

3. プロンプトに従って、新しい検索ドメインの情報を入力します。
   次の例では、検索ドメイン `domain2.com` を既存の検索ドメイン `subdomain.domain.com` に追加します。

```
Setting search domains.
Current search domains: subdomain.domain.com
Change search domains to: subdomain.domain.com domain2.com
Applying search domains to [subdomain.domain.com domain2.com], input root password to
continue
[sudo] password for root:
New search domains: subdomain.domain.com domain2.com
```

PowerProtect Data Manager と他のシステム時刻の同期

PowerProtect Data Manager のシステム時刻は、ESXi ホストのシステムと同期されます。

PowerProtect Data Manager のシステム時刻がインターフェイスで接続するシステムの時刻と一致しない場合は、コンプライアンス チェックが失敗します。すべてのシステムで NTP サーバーを使用した構成を推奨しています。

メモ: UI に表示される時刻には、各ブラウザーのタイム ゾーンを使用するか、ローカル タイム ゾーンに関係なく、すべてのアクセスに適用される構成可能なタイム ゾーンを使用できます。PowerProtect Data Manager システムのタイム ゾーンが、UI に表示されるタイム ゾーンとは異なる場合があります。すべてのログファイル エントリーは UTC タイム ゾーンを使用します。ただし、サーバーのタイム ゾーンを使用するクライアント ブラウザー接続に関連するエントリーを除きます。

ユーザー インターフェイスのタイム ゾーン、システム タイム ゾーン、NTP サーバーの変更

タイム ゾーンと NTP サーバーを変更するには、次の手順を実行します。

手順

1. PowerProtect Data Manager UI で  をクリックしてから、[Time Zone] をクリックします。
2. [User Interface Time Zone] リストから、該当するユーザー インターフェイスのタイム ゾーンを選択します。Web ブラウザーのタイム ゾーンではなく特定のタイム ゾーンが設定されている場合、ユーザー インターフェイスに情報を表示するときに Web ブラウザーで使用されるタイム ゾーンをそのタイム ゾーンがオーバーライドします。
3. [Server Time Zone] リストから、PowerProtect Data Manager が使用する該当するタイム ゾーンを選択します。このタイム ゾーンは、コンポーネントの通信に使用されます。

4. （オプション）NTP サーバーを変更するには、次の手順を実行します。
   a. ⊕ をクリックします。
   b. ［NTP Server］で、NTP サーバーのホスト名または IP アドレスを入力します。
5. ［Save］をクリックします。

転送中の暗号化

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。転送中の暗号化は、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、PowerStore ブロック ボリューム資産、VMware 仮想マシン資産にのみ使用できます。

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。

転送中の暗号化は、新規インストールに対して有効になっています。PowerProtect Data Manager UI を使用して転送中の暗号化を有効化または無効化できます。すべてのインストールで転送中の暗号化を有効にすることを強くお勧めします。

次の表に、転送中の暗号化をサポートしているワークロードと操作を示します。

メモ: サポートされている、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 38. 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 ダイレクトを使用した 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 ダイレクトを使用した 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
仮想マシン	可	可	N/A	N/A
PowerStore	可	可	N/A	N/A

転送中の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。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が 5～20%の影響を受ける可能性があります。

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転送中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。

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、ターゲットに保存される前に復号できます。

前提条件

転送中の暗号化の詳細については、「転送中の暗号化」の情報を確認してください。

暗号化設定により、バックアップおよびリストアの操作中に、データ転送が暗号化されるかどうかが決まります。

- ファイル システム、Microsoft Exchange Server、Oracle、SAP HANA、ネットワーク接続型ストレージ(NAS)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 ダイレクト ホストでのみサポートされます。Microsoft SQL Server 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 ダイレクト ホストと VM Direct ホストでサポートされています。
- 新しいホストを PowerProtect Data Manager に追加すると、ホスト構成によってバックアップとリストアの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。

手順

1. PowerProtect Data Manager UI で、  をクリックし、［Security］を選択します。
   ［Security］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転送中の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 PowerProtect Data Manager 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 ダイレクト 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 エージェントに転送中の暗号化設定がプッシュされます。

［Backup/Restore Encryption］スイッチをクリックして、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、バックアップおよびリストアの暗号化を無効にします。

レプリケーション暗号化の有効化

レプリケーションされたコンテンツがターゲット ストレージに対して未了(in-flight)中に暗号化され、ターゲット ストレージに保存される前に復号化されるようにすることができます。

このタスクについて

レプリケーションを正常に行うためには、ソース システムとターゲット システムの両方の暗号化設定が一致している必要があります。たとえば、PowerProtect Data Manager でレプリケーション暗号化を有効にする場合は、レプリケーション目的を定義する前に、ソースとターゲットの両方の設定を有効にします。レプリケーション目的の初期定義後に暗号化を有効にした場合、ソースおよびターゲットの暗号化設定が一致しなかった期間中に開始されたレプリケーション ジョブは失敗します。

手順

1. PowerProtect Data Manager UI で、  をクリックし、［Security］を選択します。
   ［Security］ダイアログ ボックスが表示されます。
2. ［Replication Encryption］スイッチをクリックして有効化し、［Save］をクリックします。

次の手順

PowerProtect Data Manager UI の［Infrastructure］ > ［Storage］ウィンドウに、接続されているすべてのストレージ システムのレプリケーション暗号化設定が表示されます。

メモ: DDOS バージョン 6.2 以前がインストールされている保護ストレージシステムでは、ステータスが `Unknown` として表示されることがあります。DDOS バージョン 6.3 以降では、認証モードがサポートされています。DDOS バージョン 6.2 以前では、匿名認証モードのみがサポートされています。PowerProtect Data Manager では、匿名双方向認証モードのみがサポートされています。ソースとターゲットの両方で必ず同じ認証モードを使用します。

『*DDOS 管理ガイド*』の説明に従って、PowerProtect Data Manager サーバーで追加のステップを実行し、［DD System Manager］を使用して、接続された DD システムでインフライト暗号化を有効にできます。

その他の考慮事項

転送中の暗号化に関するその他の考慮事項は以下のとおりです。

暗号化が使用されているかどうかを検証するには、DD Boost CLI で `ddboost show connections` コマンドを実行して、DD システム上の既存の接続ステータスを確認します。

暗号化された接続が確立されていれば、[Encrypted] 列の値は `Yes` です。

クライアントが暗号化された接続を確立し、別の接続を暗号化せず確立する場合、[Encrypted] 列の値は `Mixed` です。この状況は、次のいずれかの理由で発生する場合があります。

- クライアント単位で定義された暗号化設定は、クライアントが切断された後も、しばらくの間は設定されたままになります。クライアントが先に暗号化せず接続を確立し、その後に暗号化された接続を確立した場合、値は `Mixed` になります。
- 暗号化設定は、アプリケーション エージェントで作成された DD Boost 接続には指定されません。詳細については、個々のエージェント ユーザー ガイドを参照してください。

DD に暗号化設定が存在し、PowerProtect Data Manager でも有効になっている場合は、上位の設定が優先されます。その結果、[Encrypted] 列には常に `Mixed` と `Yes` のいずれかが表示されます。

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、*PowerProtect Data Manager* セキュリティ構成ガイドにリスト表示されている必要なポートを使用して PowerProtect Data Manager からデータを受信するように構成されています。リスト表示されていないポートが Syslog サーバーで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。

次の情報については、*PowerProtect Data Manager* セキュリティ構成ガイドを参照してください。

- ポートの使用方法
- ファイアウォール ルールを変更してカスタム ポートを追加する手順

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 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* セキュリティ構成ガイドに、手順が記載されています。
- 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。

4. 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。
5. 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。

6. 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。
7. ［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。

8. 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。
9. ［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。

10. ［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。

追加のシステム設定

一部のシステム設定は、PowerProtect Data Manager の導入とメンテナンスに直接関連しています。

次のトピックの詳細については、「システム メンテナンス」を参照してください。

- PowerProtect Data Manager のライセンス取得
- PowerProtect Data Manager ホストの指定

PowerProtect Data Manager 仮想マシンのディスク設定の変更

データ ディスクとシステム ディスクのサイズを拡張するには、カスタマー サポートのガイダンスと推奨事項に従い、このセクションの手順を実行します。

データ ディスク サイズの変更

単一パーティション構成で、システム ディスクにログ パーティションが存在するデータ ディスクのサイズを拡張するには、次の手順に従います。

手順

1. ［vSphere Web Client］から次の手順を実行します。

a. VM Direct アプライアンスを右クリックし、[Shut Down Guest OS] を選択します。
b. 電源オフの完了後、アプライアンスを右クリックして、[Edit Settings] を選択します。
[Edit Settings] ウィンドウが表示されます。[Virtual Hardware] ボタンが選択されています。
c. ハード ディスク 2 のプロビジョニングされたサイズを目的のサイズに増やし、[OK] をクリックします。

メモ: プロビジョニングされたディスク サイズを減らすことはできません。

d. VM Direct アプライアンスを右クリックして、[Power On] を選択します。

2. アプライアンス コンソールから、root ユーザーとして次の手順を実行します。

メモ: `ssh` を使用してアプライアンスに接続する場合、管理者アカウントを使用してログ インし、次に `su` コマンドを使用して root アカウントに変更します。

a. **`reboot`** と入力して、アプライアンスを再起動します。
b. [GNU GRUB] メニューで、**`Esc`** を押して GNU GRUB メニューを編集します。
c. 編集画面で、*Linux* で始まる行を検索し、*splash=0* というエントリーの前に *single* という単語を追加します。
次の図に、更新されたテキストが入力された編集画面の例を示します。

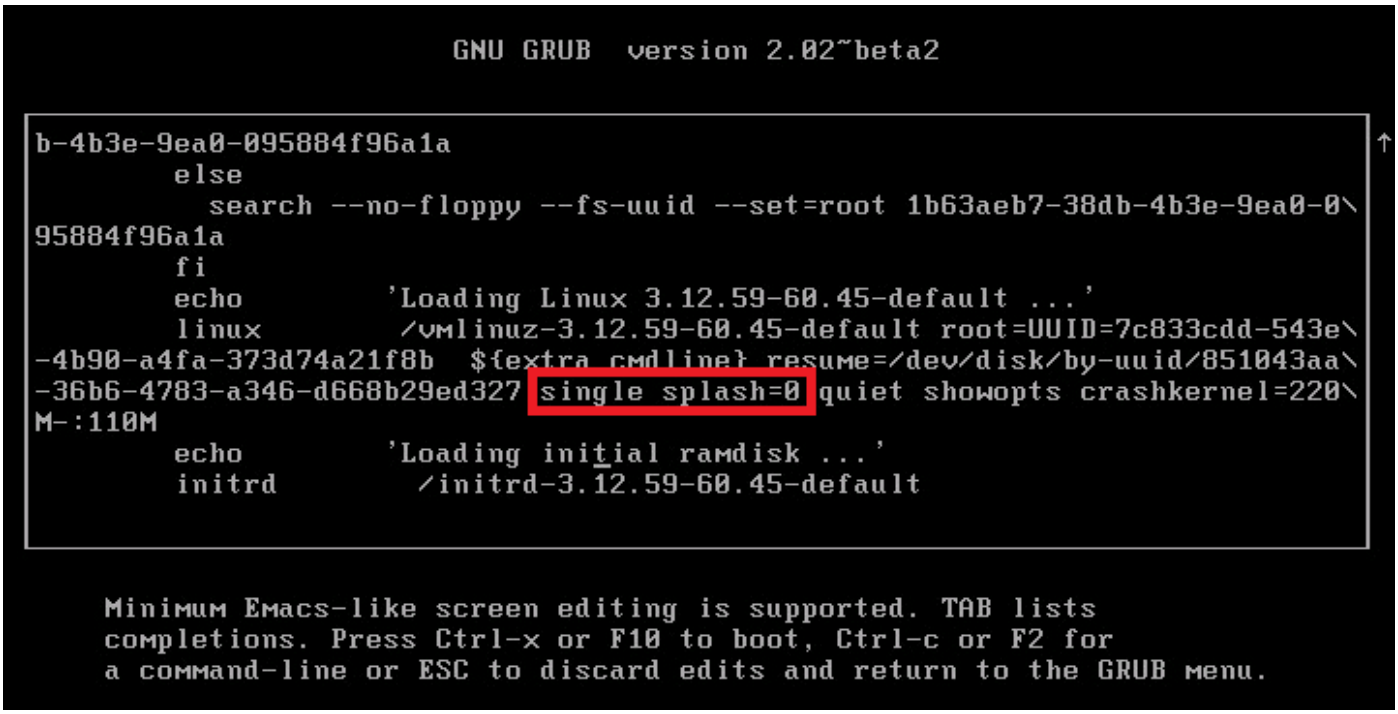


図 8. GNU GRUB メニューの編集

d. [Ctrl-x] キーを押して、シングルユーザー モードで再起動します。
e. プロンプトが表示されたら、root アカウントのパスワードを入力します。
f. **`umount /data01`** と入力してデータ ディスクをアンマウントします。
g. **`parted`** と入力してパーティション ユーティリティを起動し、次のタスクを実行します。
   i. **`select /dev/sdb`** と入力します。
   ii. **`print`** と入力します。問題を修正するように要求されたら、各プロンプトで **`fix`** と入力します。[Size] フィールドに新しいディスク サイズが表示され、テーブルに現在のサイズが表示されます。
   iii. **`resize 1 new_size`** と入力します。 ここで、*new_size* は `print` コマンドの出力の [Size] フィールドに表示されている値です。
   たとえば、ディスクのサイズを 700 GB に変更するには、**`resize 1 752GB`** と入力します。
   iv. **`quit`** と入力します。

3. 「**`systemctl reboot`**」と入力して、VM Direct アプライアンスを再起動します。
4. root ユーザーとしてコンソールにログインします。

メモ: ssh プロトコルを使用して VM Direct アプライアンスに接続する場合、管理者アカウントを使用してログ インし、次に su コマンドを使用して root アカウントに変更します。

5. **xfs_growfs -d /data01** と入力して xfs ファイル システムを拡張します。
6. **df -h** と入力して、新しいパーティション サイズを確認します。

システム ディスク サイズの変更

システム ディスクの最後のパーティションがログ パーティションである場合にデータ ディスクのサイズを拡張するには、次の手順に従います。

手順

1. [vSphere Web Client] から次の手順を実行します。
   a. VM Direct アプライアンスを右クリックし、[Shut Down Guest OS] を選択します。
   b. 電源オフの完了後、アプライアンスを右クリックして、[Edit Settings] を選択します。
   [Edit Settings] ウィンドウが表示されます。[Virtual Hardware] ボタンが選択されています。
   c. ハード ディスク 1 のプロビジョニングされたサイズを目的のサイズに増やし、[OK] をクリックします。

   メモ: プロビジョニングされたディスク サイズを減らすことはできません。

   d. VM Direct アプライアンスを右クリックして、[Power On] を選択します。
2. SuSE Linux Enterprise Server（SLES）バージョン 12 CD から起動します。
3. **parted** と入力してパーティション ユーティリティを起動し、次のタスクを実行します。
   a. **select /dev/sdx** と入力します。
   b. **print** と入力します。問題を修正するように要求されたら、各プロンプトで **fix** と入力します。[Size] フィールドに新しいディスク サイズが表示され、テーブルに現在のサイズが表示されます。
   c. **quit** と入力します。
4. 「**systemctl reboot**」と入力して、VM Direct アプライアンスを再起動します。
5. root ユーザーとしてコンソールにログインします。

   メモ: ssh プロトコルを使用して VM Direct アプライアンスに接続する場合、管理者アカウントを使用してログ インし、次に su コマンドを使用して root アカウントに変更します。

6. **xfs_growfs -d /data01** と入力して xfs ファイル システムを拡張します。
7. **df -h** と入力して、新しいパーティション サイズを確認します。

DD システムの構成

前提条件

DD によってシステムを保護するには、NFS を使用して、PowerProtect Data Manager が DD システムで使用する MTree をエクスポートします。DD システムでのセットアップには、no_root_squash で PowerProtect Data Manager クライアントを追加する必要があります。

手順

1. web ブラウザーを使用してシステム管理者ユーザーとして [DD System Manager] にログ インします。
2. [Summary] タブの [Protocols] ペインで、[NFS export] > [create export] を選択します。
   [Create NFS Exports] ウィンドウが表示されます。
3. [Create NFS Exports] ウィンドウで、次の手順を実行します。
   a. [Export Name] フィールドに、DD MTree の名前を指定します。
   b. DD MTree をまだ作成していない場合は、プロンプトに従って MTree を作成し、[Close] をクリックします。
   c. [Directory path] フィールドに、作成した DD MTree のフル ディレクトリー パスを指定します。ディレクトリに同じ名前を使用していることを確認します。
   d. [OK] をクリックします。
   NFS エクスポート構成を保存中というメッセージの次に完了メッセージが表示されます。
   e. [Close] をクリックします。

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。

デフォルトの構成では、管理トラフィックのルーティングにバックアップ トラフィックと同じネットワークを経由させます。すべての資産が、同じネットワーク内に構成されます。

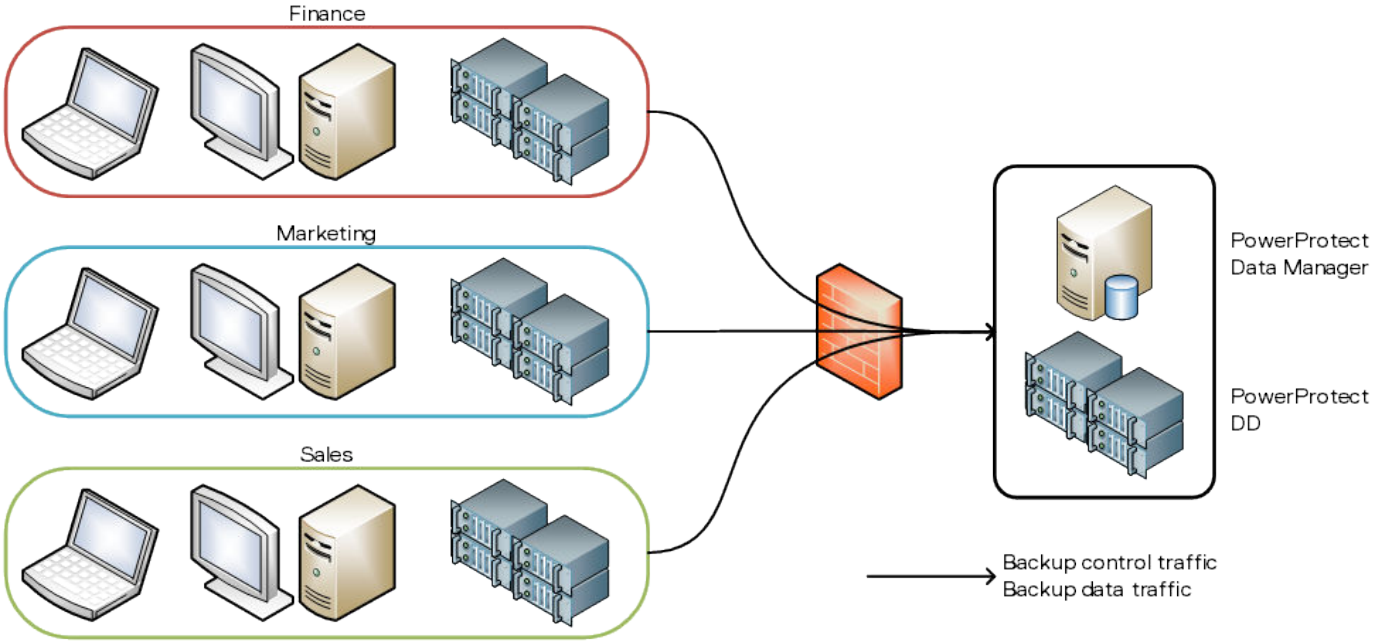


図 9. フラットなネットワーク

仮想ネットワークを構成して、バックアップ トラフィックから管理トラフィックを分離することもできます。この構成では、異なるネットワークを起点とするトラフィックを分離することもできます。その場合は、管理トラフィックとバックアップ トラフィックに同じ仮想ネットワークを使用することも、それぞれに別の仮想ネットワークを使用することもできます。

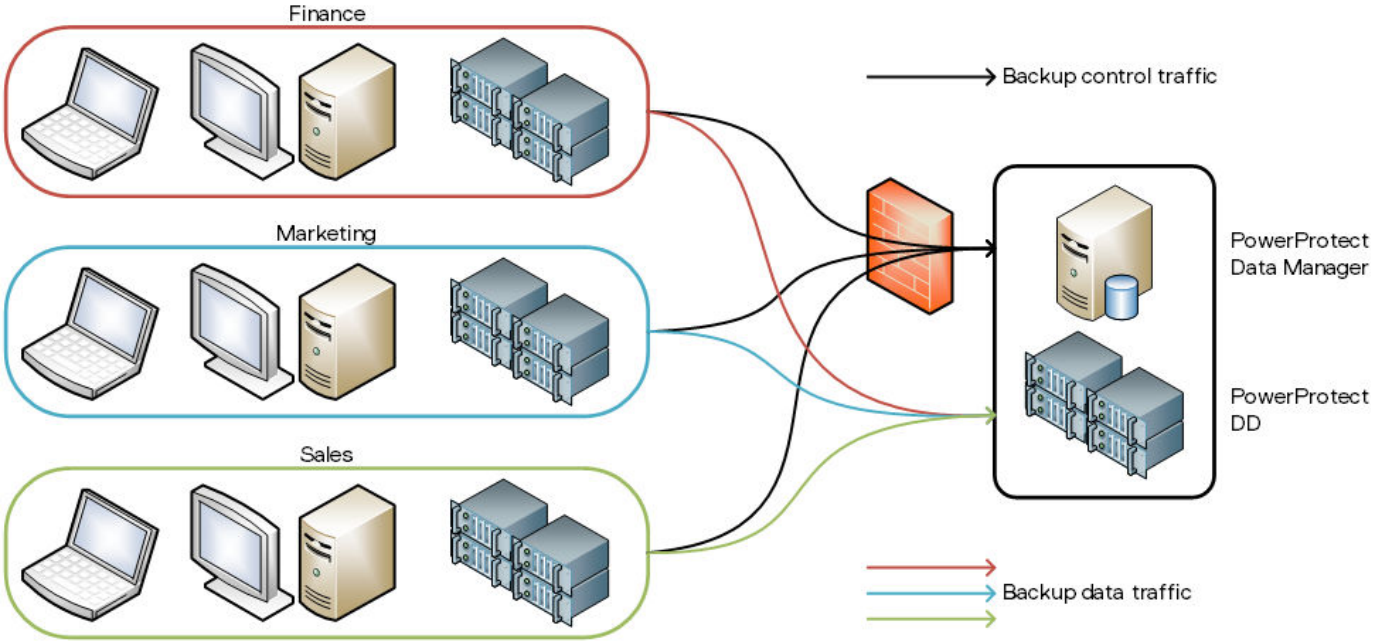


図 10. 仮想ネットワーク

PowerProtect Data Manager で仮想ネットワークを使用するには、PowerProtect Data Manager を構成する前、または資産にネットワークを割り当てる前に、DD とネットワーク インフラストラクチャを構成する必要があります。

構成は、次に示す複数ステップのワークフローに従ってください。

1. DD 上に仮想ネットワークを構成します。
2. DD をストレージとして追加し、ネットワーク インターフェイスに名前を付けます。
3. 仮想ネットワークを PowerProtect Data Manager に追加します。
4. PowerProtect Data Manager に資産を登録します。
5. 保護ポリシーを作成（または既存のポリシーを編集）して、優先仮想ネットワークを割り当てます。
6. オプションとして、個々の資産に仮想ネットワークを割り当てます。このアクションは、保護ポリシーで優先仮想ネットワークを指定していた場合、そのネットワークをオーバーライドします。

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。

構成は、無停止で行うことができます。バックグラウンド アクティビティへの影響、ネットワーク インターフェイスの切断、PowerProtect Data Manager ユーザー インターフェイスへの影響なしに、仮想ネットワークの追加、編集、削除を行うことができます。

PowerProtect Data Manager によってネットワークの変更が監査ログに記録されます。ネットワークの変更に失敗した場合は、［システム］アラートに表示されます。

仮想ネットワーク トラフィック タイプ

PowerProtect Data Manager では、次のトラフィック タイプの仮想ネットワークをサポートしています。

表 39. トラフィック タイプ

タイプ	説明
管理	トラフィックの制御（通常は HTTPS REST API 操作）。ログやアップデート パッケージなどの小容量ファイル転送や、ID プロバイダー認証など、その他の重要なトラフィック。
データ	バックアップおよびリストア トラフィック、クラウド階層化、CloudDR トラフィックなど、大量のお客様データ。
管理コンポーネントのデータ, Data for Management Components	ServerDR、インデックス作成と検索、レプリケーション監視、コピー削除など、管理および制御操作に関連するお客様データ。

この管理コンポーネントのデータ, Data for Management Components タイプは、管理操作に関連するトラフィックを伝送しますが、お客様の情報を含めることができます。必要に応じて、このトラフィックを管理ネットワーク、データネットワーク、またはその両方から分離できます。

例えば、一部の環境では、管理用の 1 Gbps ネットワークとデータ用の 10 Gbps ネットワークなど、ネットワークごとに異なるスピードをサポートする場合があります。その他の環境には、お客様のデータが管理ネットワーク経由で流れるかどうかを制御するポリシーまたはルールがある場合があります。管理コンポーネントのデータ, Data for Management Components トラフィックを分離することで、セキュリティ、スピード、その他の優先事項に合わせてフローを最適化できます。

仮想ネットワーク計画

仮想ネットワーク構成を計画する場合は、次の要件に従ってください。

表 40. コンポーネント トラフィック タイプの要件

コンポーネント	互換性のあるタイプ	互換性のないタイプ
PowerProtect Data Manager	管理、管理コンポーネントのデータ, Data for Management Components	データ
保護エンジン s	管理コンポーネントのデータ, Data for Management Components、データ	管理
Search Engine ノード, Search Engine nodes	管理コンポーネントのデータ, Data for Management Components	管理、データ
Reporting Engine	管理、管理コンポーネントのデータ, Data for Management Components	データ

この表は互換性のあるトラフィック タイプを示していますが、保護エンジンは仮想ネットワークなしで動作できます。

管理コンポーネントのデータ, Data for Management Components トラフィックを管理トラフィックから分離するには、保護ストレージの仮想ネットワークに名前を付ける必要があります。 保護ストレージのネットワーク設定の変更 で手順を参照してください。 保護ストレージの仮想ネットワークに名前を付けなければ、このトラフィックはデフォルトで管理ネットワークに設定されます。

並列仮想ネットワーク

各トラフィック タイプに対して複数の仮想ネットワーク（部門ごとに異なるデータネットワークなど）が環境に含まれる場合があります。並列仮想ネットワークが存在する場合、すべての保護エンジンは、必要なタイプごとに少なくとも 1 個の仮想ネットワークへのインターフェイスを必要とします。ただし、各保護エンジンは、必要なタイプのすべての仮想ネットワークへの接続を必要としません。

例：

- お客様の環境には、独自の資産を持つ財務部門とエンジニアリング部門があります。
- お使いの環境には、次の仮想ネットワークがあります。管理、`Finance` データ、`Engineering` データ。

次の表は、両方の部門が保護エンジンを共有し、各部門がプライベートな保護エンジンを持つシナリオの各仮想ネットワークへの接続について説明しています。

表 41. 例：仮想ネットワーク インターフェイス

仮想ネットワーク名	共有保護エンジン	プライベート保護エンジン	
		財務保護エンジン	エンジニアリング保護エンジン
管理	可	可	可
`Finance` データ	可	可	不可
`Engineering` データ	可	不可	可

保護エンジンにはデータトラフィックの接続が必要ですが、プライベート保護エンジンは各部門の仮想ネットワーク間の分離を維持します。

サポートされる仮想ネットワーク トポロジーのいくつかの図には、並列仮想ネットワークが含まれています。

仮想ネットワーク トポロジー

次の図は、サポートされている仮想ネットワーク トポロジーと、それらがトラフィック タイプにどのように関連しているかを示しています。

単一ネットワーク

このトポロジーでは、すべてのトラフィック タイプが同じネットワークに割り当てられます。管理とデータ、または異なる論理組織に属するエージェント間の分離はありません。

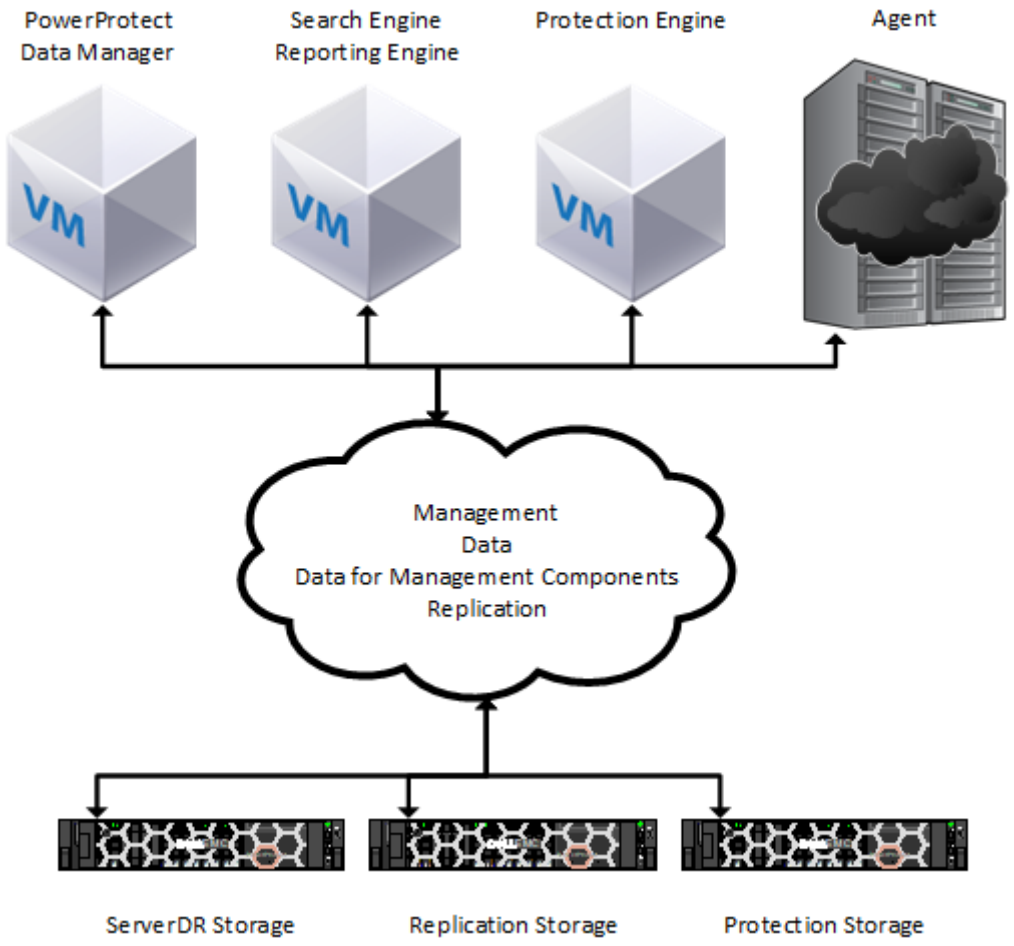


図 11. 単一ネットワーク

管理ネットワーク上の管理コンポーネントのデータ, Data for Management Components トラフィック

このトポロジーは管理トラフィックをデータトラフィックから分離しますが、 管理コンポーネントのデータ, Data for Management Components トラフィックを管理トラフィックに保持します。

このトレードオフは、 管理ネットワークが頻繁に大規模なデータ転送をサポートでき、 管理ネットワーク上のお客様のデータを許可する環境で適切に動作します。

太い線は、ファイルやアップデート パッケージなど、比較的多くのデータを転送するパスを示します。 細い線は、 HTTPS API トラフィックのみなど、比較的少ないデータを転送するパスを示します。

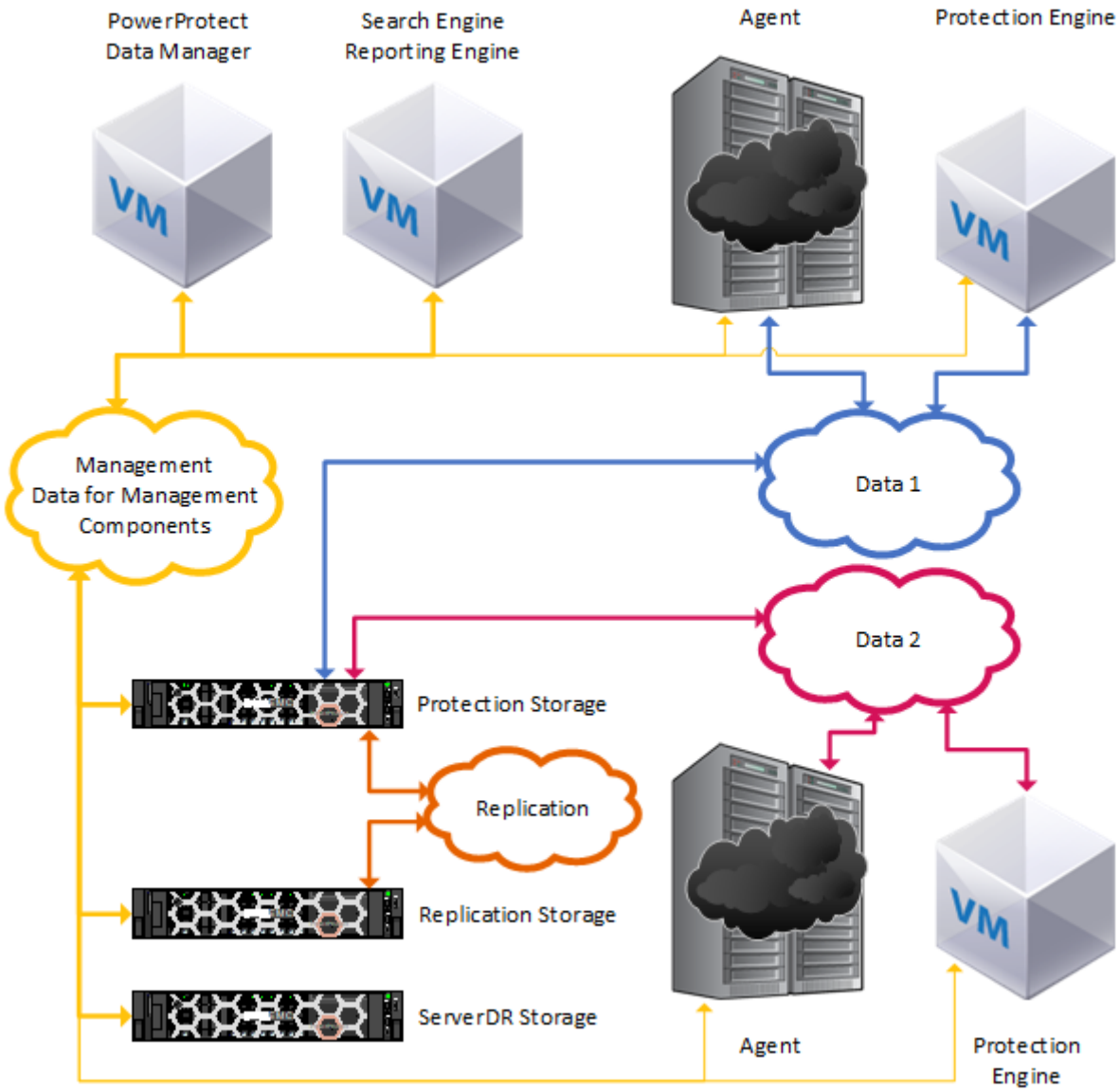


図 12. 管理ネットワーク上の管理コンポーネントのデータ, Data for Management Components トラフィック

データネットワーク上の管理コンポーネントのデータ, Data for Management Components トラフィック

このトポロジーは管理トラフィックをデータトラフィックから分離しますが、 管理コンポーネントのデータ, Data for Management Components トラフィックをデータトラフィックに保持します。

このトレードオフは、管理ネットワークが頻繁に大規模な転送をサポートできない、または管理ネットワーク上のお客様のデータを許可しない環境で適切に動作します。 ただし、 バックアップ データと制御データは分離されておらず、 管理コンポーネントのデータ, Data for Management Components トラフィックは他のトラフィックと競合します。

太い線は、 ファイルやアップデート パッケージなど、 比較的多くのデータを転送するパスを示します。 細い線は、 HTTPS API トラフィックのみなど、 比較的少ないデータを転送するパスを示します。

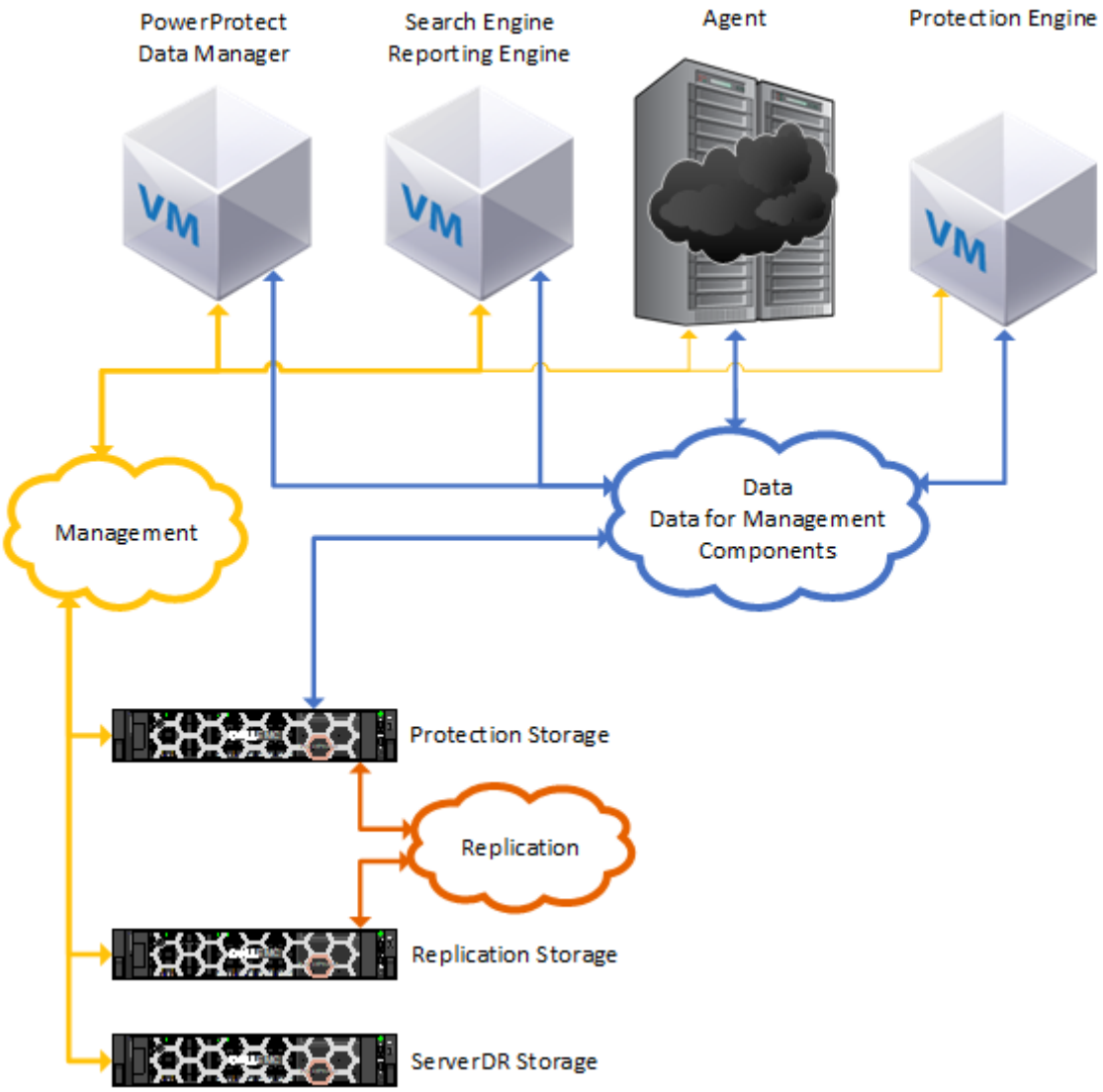


図 13. データネットワーク上の管理コンポーネントのデータ, Data for Management Components トラフィック

完全な分離

このトポロジーでは、スループットとセキュリティを最大限に高めるために、すべてのトラフィック タイプを完全に分離します。お客様のデータが管理ネットワーク経由で流れることはありません。

太い線は、ファイルやアップデート パッケージなど、比較的多くのデータを転送するパスを示します。細い線は、HTTPS API トラフィックのみなど、比較的少ないデータを転送するパスを示します。

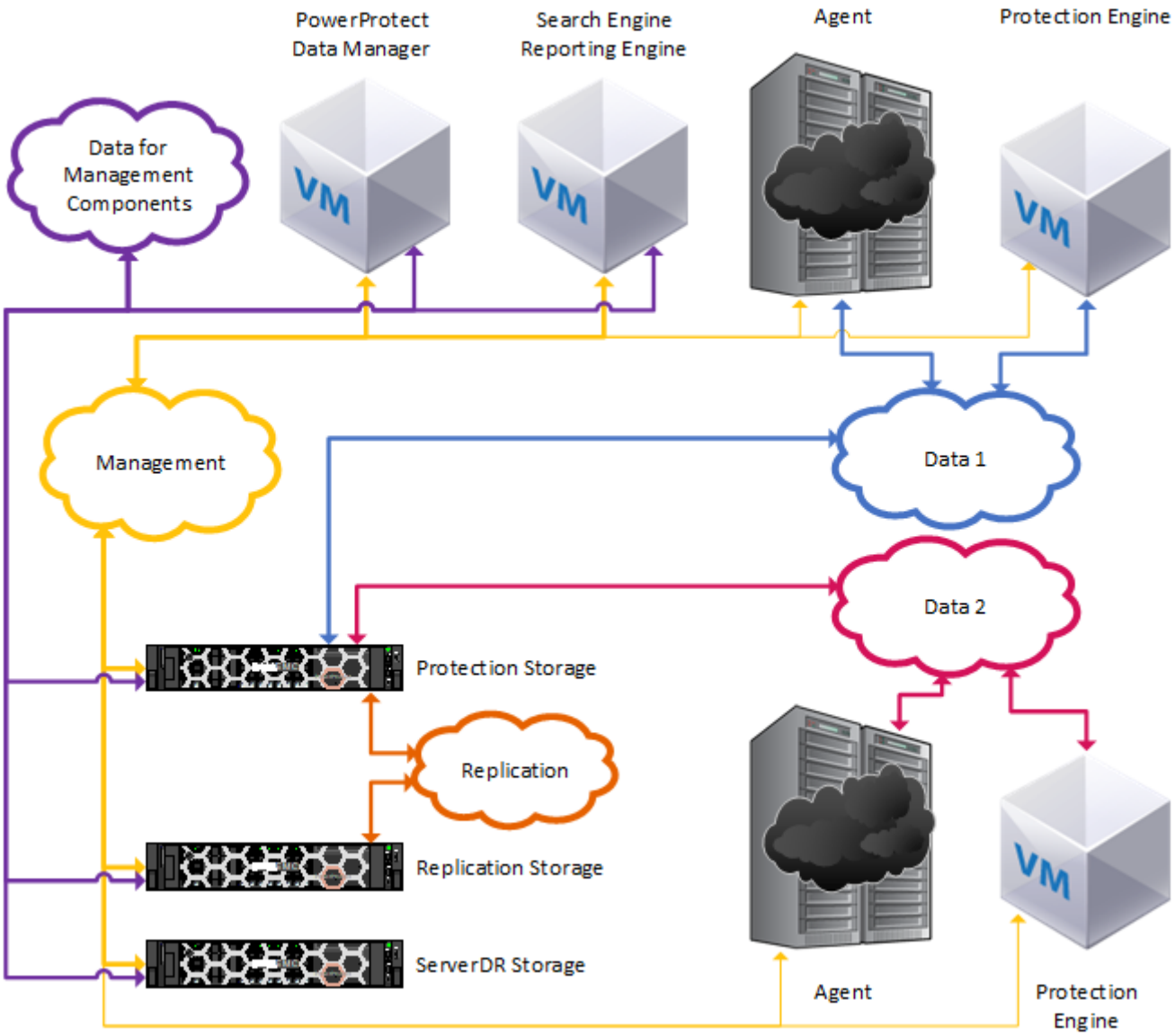


図 14. 完全な分離

サポートされているシナリオ

PowerProtect Data Manager では、次のユース ケースの仮想ネットワークをサポートしています。

- 仮想マシンのバックアップ
- Kubernetes のバックアップ
- データベース バックアップ
- Microsoft Exchange Server バックアップ
- ファイル システムのバックアップ
- レプリケーション
- ディザスター リカバリー
- Cloud DR
- ストレージ データ管理
- Search Engine

メモ: [Networks] ページを使用して、最初に既存の Search Engine ノード, Search Engine nodes がある環境に仮想ネットワークを追加する場合、PowerProtect Data Manager は、自動的に仮想ネットワークを Search Engine に追加しません。代わりに、各 Search Engine ノード, Search Engine node を手動で編集して、仮想ネットワークを追加します。このアクションにより、Search Engine は仮想ネットワークを認識します。以降のすべての新しい仮想ネットワークは、自動的に Search Engine に追加されます。

仮想ネットワークの前提条件

仮想ネットワークを構成する前に、次の操作を完了させてください。

- PowerProtect Data Manager が導入されている vCenter Server を登録します。これを確認するには、[[資産ソース]] ページの［vCenter］タブを使用します。ホスティング vCenter を追加することもできます。 PowerProtect Data Manager ホストの指定 で手順を参照してください。
- トランク モード用のネットワーク スイッチ ポートを構成します。この設定により、ポートは複数の VLAN のトラフィックを伝送できます。
- PowerProtect Data Manager に対する VMware ESXi 仮想ネットワーク スイッチ ポートの仮想ゲスト タグ付け(VGT)モードまたは仮想スイッチ タグ付け(VST)モードを有効にします。標準ポート グループまたは分散ポート グループを使用できます。
  - VGT：標準仮想スイッチのポート グループの場合、VLAN ID 4095 に対する仮想スイッチ ポートを構成します。これにより、すべての VLAN がアクセス可能になります。分散仮想スイッチのポート グループの場合は、ID または範囲による複数の VLAN の指定をサポートする VLAN トランキングを使用します。詳細については、VMware ESXi のドキュメントを参照してください。
  - VST：1～4094 の VLAN ID を使用してポート グループを構成できます。
- DD System Manager の［Hardware］ > ［Ethernet］ウィンドウにある［Interfaces］タブで、DD の VLAN インターフェイスを構成します。詳細については、DD のドキュメントを参照してください。

  VLAN ID が含まれているインターフェイス名を選択することをお勧めします。例えば、VLAN ID 850 であればインターフェイス名を `ethV1.850` にするなどです。
- DD を PowerProtect Data Manager の保護ストレージとして追加します。

PowerProtect Data Manager では、ネットワーク スイッチ構成の検証が行われません。物理または仮想のネットワーク スイッチが正しく構成されていない場合、仮想ネットワークの構成は失敗します。

仮想ネットワークの構成

次に続くトピックでは、異なる VLAN 上の資産で使用する仮想ネットワークを PowerProtect Data Manager で作成して維持する方法を説明しています。

PowerProtect Data Manager では、各仮想ネットワークの命名を保護ストレージ システム用のインターフェイスと保護資産用のインターフェイスの 2 か所で行っています。これらの名前を一致させる必要はありません。ただし、両方の場所の仮想ネットワークで同じネットワーク名を使用することを強くお勧めします。後で使用するために、各ネットワーク名を記録しておきます。

また、VLAN ID が含まれているネットワーク名を選択することをお勧めします。例えば、VLAN ID 850 であれば、`sales-vlan850` などです。

仮想ネットワークの追加には、固定 IP アドレスのプールの作成が含まれます。PowerProtect Data Manager は、これらのアドレスを仮想ネットワークのローカル インターフェイスと、このネットワークに導入する VM Direct 保護エンジンまたは Search Engine ノード, Search Engine nodes に使用します。

各 VM Direct 保護エンジンまたは Search Engine ノード, Search Engine node には、仮想ネットワーク上の IP アドレスが必要です。PowerProtect Data Manager インターフェイスには、1 個の IP アドレスが必要です。この要件を満たすために、各ネットワーク上に十分な数の IP アドレスを用意します。将来の拡張に備えるため、最初の必要数よりも多い IP アドレスを追加できます。

仮想ネットワークのリストを確認すると、注意が必要な行は名前の横に⚠と表示されます。詳細については、ネットワークの詳細を表示してください。

仮想ネットワークの追加

資産および保護ポリシーで使用する新しい仮想ネットワークを構成します。

このタスクについて

新しい仮想ネットワークごとに、少なくとも 1 個の各 PowerProtect Data Manager ネットワーク インターフェイス用 IP アドレスが必要です。必要数の固定 IP アドレスを入力する前に、［必要な IP アドレスの数］フィールドを確認します。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［ネットワーク］の順に選択します。
   [[ネットワーク]] ウィンドウが表示されます。
2. ［Add］をクリックします。
   [[ネットワークの追加]] ウィザードが開きます。
3. ［Purpose］で、1 個以上のトラフィック タイプを選択します。
   仮想ネットワーク トラフィック タイプ で詳細を参照してください。
4. ［ネットワーク名］フィールドに新しい仮想ネットワークの名前を入力します。
   各 VLAN でネットワーク名に一貫性を持たせることをお勧めします。

5. ［VLAN ID］フィールドに、この仮想ネットワークが表す VLAN に対応する数値 1～4094 を入力します。
6. ［MTU］を指定します（最大 trr 仮想ネットワーク）。
   許容される［MTU］値の範囲は 1500～9000 です。
7. ［次へ］をクリックします。
   ［Add Network］ウィザードから［Static IP Pool］ページに移動します。
8. ［Static IP Pool］ページで、次の手順を実行します。
   a. IP プールの［Type］を選択します。
      複数のタイプの IP プールが必要な場合は、［Add Alternate Configuration Details］をクリックします。この追加の IP プールを編集するには、［Edit］をクリックします。削除する場合は、［Delete］をクリックします。
   b. IPv4 プールの［Subnet Mask］または IPv6 プールの［Prefix］を指定します。
   c. この仮想ネットワーク上の通信に使用する PowerProtect Data Manager の予約済み IP アドレスの数を指定します。
      IP アドレスまたは IP アドレスの範囲を個別に追加または削除できます。
      - IP アドレスまたは IP アドレスの範囲を個別に追加するには、 をクリックし、［Value］または［Range］を選択して値または範囲を指定します。
      - IP アドレスまたは IP アドレスの範囲を個別に削除するには、エントリーの横にある をクリックします。
9. 固定 IP アドレス プールに仮想ネットワークを追加するための十分な数のアドレスが含まれていることを確認します。
10. ［次へ］をクリックします。
    ［［ネットワークの追加］］ウィザードから［［ルート］］ページに移動します。
11. 該当する場合は、［追加］をクリックして必要なルートを定義します。
    ［［ルートの追加］］ページが開きます。次のサブステップを実行します。
    a. ルート タイプを選択します。
       - ［サブネット］を選択した場合は、CIDR 形式でサブネットを定義します。たとえば、IPv4 の場合は `10.0.0.0/24`、IPv6 の場合は `fe80:7f03:79a5:2d11::f9a5/64` です。
       - ［ホスト］を選択した場合は、IP アドレスを入力します。
    b. PowerProtect Data Manager がサブネットまたはホストに到達するために通過するデフォルト ゲートウェイの IP アドレスを入力します。
    c. ［Add］をクリックします。
       ［［ルートの追加］］ページが閉じます。［ルート］リストに新しいルートが表示されます。
    d. ルート情報を確認します。
       パラメーターが正しくない場合は、そのルートのチェックボックスを選択して、［削除］をクリックします。
    e. これらのサブステップを繰り返して、必要数のルートを追加します。
12. ［次へ］をクリックします。
    ［［ネットワークの追加］］ウィザードから［［サマリー］］ページに移動します。
13. ネットワーク構成情報を確認し、［完了］をクリックします。
    ［［ネットワークの追加］］ウィザードが閉じます。［［ネットワーク］］ページには、ステータスが `Initiating` となっている新しいネットワークが表示されます。

次の手順

PowerProtect Data Manager による仮想ネットワークの構成には若干時間がかかる場合があります。

仮想ネットワークのステータスが `Failed` に変わった場合は、対応するシステム アラートに障害の原因に関する詳細情報が含まれます。問題のトラブルシューティングを行ってから、次のいずれかの操作を実行します。

- 構成の問題によって障害が発生した場合は、［編集］をクリックしてネットワーク構成のアップデートを行います。
- 障害が一時的なものや、外部要因によるもので、構成に問題がない場合は、［再試行］をクリックして同じ設定を使用します。

メモ:

失敗した仮想ネットワーク操作を編集または再試行し、アドレス プールに追加の IP アドレスがある場合、PowerProtect Data Manager は最後に失敗した IP アドレスを破棄済みとマークします。PowerProtect Data Manager は、破棄済みとマークされている IP アドレスを再使用しません。UI では、この状態は表示されません。

REST API を使用して、IP アドレスが破棄済みとマークされていることを検出する方法の詳細については、KB 記事 000181120 を参照してください。この記事では、破棄された IP アドレスを再び使用するために検出条件を修正する手順についても説明されています。

仮想ネットワークの詳細の表示

仮想ネットワーク名があいまいな場合は、変更を行う前に、詳細を表示して仮想ネットワークをより明確に特定することができます。また、変更後に注意が必要なコンポーネントを特定することもできます。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［ネットワーク］の順に選択します。
   ［[ネットワーク]］ウィンドウが表示されます。
2. 該当する仮想ネットワークに対応する行を見つけます。

   各行の列には、関連付けられている VLAN ID とネットワーク ステータスが示されています。注意が必要な行は、名前の横に⚠と表示されます。
3. その行の🔍をクリックします。

   ［[詳細]］ペインが右側に表示されます。

   このペインには、仮想ネットワーク構成に関する情報が表示されます。これには、固定 IP アドレス プールの詳細、割り当てられたトラフィック タイプ、構成済みのルートなどが含まれます。このペインには、このネットワーク上のインターフェイスで構成されているコンポーネント、そのタイプ、割り当てられた IP アドレスもリスト表示されます。
4. 詳細ペインを閉じるには、［X］をクリックします。

構成後の仮想ネットワーク トラフィック タイプの変更

通常のオペレーションでは、仮想ネットワークを構成し、選択したトラフィック タイプをサポートする新規または既存のコンポーネントにインターフェイスを割り当てます。ただし、環境が変更された場合は、後で仮想ネットワークのトラフィック タイプ設定を変更できます。

仮想ネットワークを再構成した後、新しいトラフィック タイプの設定が、その仮想ネットワーク上の既存コンポーネントのインターフェイス割り当てと一致しなくなることがあります。このような場合、PowerProtect Data Manager は、トラフィック タイプとインターフェイス割り当ての間の競合について通知しますが、自動アクションは実行しません。

代わりに、UI により警告の記号（⚠）で競合がマークされます。管理者は、警告を確認し、示されたコンポーネントを編集して、互換性のないネットワーク インターフェイスを手動で削除する必要があります。例：

- Search Engine ノード, Search Engine node は、データトラフィックを伝送する仮想ネットワークへのインターフェイスであり、管理コンポーネントのデータ, Data for Management Components トラフィックを伝送するものではありません。
- 保護エンジンは、管理コンポーネントのデータ, Data for Management Components のトラフィックを伝送する仮想ネットワークへのインターフェイスを提供します。
- PowerProtect Data Manager は、データトラフィックを伝送する仮想ネットワークへのインターフェイスであり、管理コンポーネントのデータ, Data for Management Components トラフィックを伝送するものではありません。

このような状況では、PowerProtect Data Manager は正常に動作し続けます。ただし、競合を解決すると、IP アドレスがアドレス プールに返されます。

仮想ネットワークの編集

ネットワークを削除せずに、仮想ネットワークの任意のパラメーターを変更できます。例えば、IP アドレスを固定 IP プールに追加するには、次の操作を行います。

前提条件

固定 IP プールの IP アドレスがすでに使用されている場合は、そのアドレスをプールから削除できません。

ネットワークのトラフィック タイプを変更する前に、インデックス作成を無効にします。 インデックス作成の設定と管理 で手順を参照してください。

このタスクについて

導入後、デフォルトのネットワークではすべてのトラフィック タイプが有効になります。データおよび管理コンポーネントのデータ, Data for Management Components タイプはこのネットワークから削除できますが、管理タイプは削除できません。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［ネットワーク］の順に選択します。
   ［[ネットワーク]］ウィンドウが表示されます。
2. 該当する仮想ネットワークに対応する行を見つけ、ラジオ ボタンをクリックしてその行を選択します。

PowerProtect Data Manager によって、［編集］と［削除］ボタンが有効になります。

3. ［編集］をクリックします。
［[サマリー]］ページに、［[ネットワークの編集]］ウィザードが開きます。
4. ［Configuration］セクション、［Static IP Pool］セクション、［Routes］セクションの［Edit］をクリックします。
［Edit Network］ウィザードから、それぞれ［Configuration］ページ、［Static IP Pool］ページ、［Routes］ページに移動します。
5. 目的のネットワーク パラメーターを変更し、［次へ］をクリックします。
より多くの IP アドレスが必要となる方法で仮想ネットワークを変更した場合は、固定 IP アドレス プールにアドレスを追加するまで続行できません。
［[ネットワークの編集]］ウィザードから［[サマリー]］ページに移動します。
6. ネットワーク構成情報を確認し、［完了］をクリックします。
［[ネットワークの編集]］ウィザードが閉じます。［[ネットワーク]］ページに、アップデートした情報が必要に応じて反映されます。
一部の変更については、仮想ネットワークの詳細を表示して確認することが必要になる場合があります。

次の手順

インデックス作成を無効にした場合は、インデックス作成を再度有効にします。 インデックス作成の設定と管理 で手順を参照してください。

仮想ネットワークの削除

不要になった仮想ネットワークを削除することをお勧めします（オプション）。

前提条件

- 該当する資産から仮想ネットワークの割り当てを解除します。
- インデックス作成を無効にします。 インデックス作成の設定と管理 で手順を参照してください。
- 仮想ネットワークを使用するように構成されたすべての VM Direct Engine を無効にします。
- 仮想ネットワークを使用するすべての検索クラスターを無効にします。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［ネットワーク］の順に選択します。
［[ネットワーク]］ウィンドウが表示されます。
2. 該当する仮想ネットワークに対応する行を見つけ、ラジオ ボタンをクリックしてその行を選択します。
PowerProtect Data Manager によって［編集］と［削除］のボタンが有効になります。
3. ［Delete］をクリックします。
4. ネットワーク情報を確認し、［OK］をクリックして、削除の警告を承認します。
PowerProtect Data Manager によって［[ネットワーク]］ページのリストから仮想ネットワークが削除されます。

次の手順

インデックス作成、VM Direct Engine、検索クラスターを再度有効にします。

保護ストレージのネットワーク設定の変更

保護ストレージを追加した後、仮想ネットワーク、または PowerProtect Data Manager と保護ストレージ システムの間のネットワークに名前を付けます。仮想ネットワークの名前を変更する（ネットワーク名を編集する）には、これらの手順を繰り返します。

このタスクについて

管理コンポーネントのデータ, Data for Management Components トラフィックを管理トラフィックから分離するには、保護ストレージの仮想ネットワークに名前を付ける必要があります。保護ストレージの仮想ネットワークに名前を付けない場合、PowerProtect Data Manager や Search Engine ノード, Search Engine nodes などのコンポーネントは、管理コンポーネントのデータ, Data for Management Components ネットワーク経由で保護ストレージに向かうルートがありません。このトラフィックはデフォルトで管理ネットワークに設定されます。

メモ: DD 7.4.x 以前のシステムにあり、伸長されている IPv6 形式を使用するように構成されたネットワーク インターフェイスは、検出できません。伸長されている IPv6 形式は、`2620:0000:0170:0597:0000:0000:0001:001a` のようになります。短縮された IPv6 形式は、`2620:0:170:597::1:1a` のようになります。これらのネットワーク インターフェイスを使用するには、IPv4 アドレスまたは短縮された IPv6 アドレスのいずれかを使用するように再構成してから、検出を開始してください。

手順

1. PowerProtect Data Manager UI から、［インフラストラクチャ］ > ［ストレージ］の順に選択します。
［Storage］ウィンドウが表示されます。
2. ［Protection Storage］タブでストレージ システムを選択してから、［More Actions］ > ［Change Network Settings］の順に選択します。
［Change Network Settings］ウィンドウが開き、既知のネットワーク インターフェイス、割り当て済みの IP アドレス、リンク スピード、ネットワークの目的が一覧表示されます。
3. 新しい仮想ネットワークごとにインターフェイスを特定し、対応するフィールドにある仮想ネットワークの名前を選択または入力します。
各インターフェイスには、IP アドレス、リンク スピード、ネットワークの目的が表示されます。
4. ステップ 3 で仮想ネットワークの名前を入力した場合は、仮想ネットワークのネットワーク目的を 1 個以上選択します。
5. ［Save］をクリックします。
PowerProtect Data Manager にネットワーク名が格納されます。

仮想ネットワーク資産の割り当て

割り当てによって、どの資産に各仮想ネットワークを使用すべきかを明確化できます。資産を仮想ネットワークに関連付けるには、次の 2 通りの方法があります。

- 保護ポリシーによる関連付け

  PowerProtect Data Manager を構成して、保護ポリシーに含まれたすべての資産に対応させる優先仮想ネットワークを選択できます。
- 資産による関連付け

  個々の資産に仮想ネットワークを割り当てることができます。この方法はオプションであり、保護ポリシーによる仮想ネットワークの割り当てを上書きします。個別に割り当てられていない資産は、優先仮想ネットワークを自動的に使用します。

  この方法を使用することで、任意の資産に対して仮想ネットワークを指定できます。ただし、この方法はルールに対して例外となる資産の構成に特に適しています。また、同じアプリケーション ホスト上の資産を複数の仮想ネットワークに分割することもできます。例えば、資産に独自のネットワーク インターフェイスがある場合や、資産が別の部門に属する場合などです。

可能であれば、保護ポリシーで仮想ネットワークに資産を割り当てることをお勧めします。

資産を割り当てる前に、次の操作を実行します。

- 仮想ネットワーク上の PowerProtect Data Manager IP アドレスに ping を実行して、資産ホストから PowerProtect Data Manager への接続テストを行います。
- PowerProtect Data Manager で資産ソースを登録します。
- 資産ソースを承認します。

保護ポリシーによる仮想ネットワークの割り当て

次の手順では、仮想ネットワークを既存の保護ポリシーに適用します。保護ポリシーの作成時に、仮想ネットワークを割り当てることもできます。

このタスクについて

［Network Interface］フィールドでは、デスティネーション保護ストレージ システムと通信するためのネットワーク インターフェイスを選択できます。このネットワークを、バックアップ データが移動します。

手順

1. PowerProtect Data Manager UI から、［Protection］ > ［Protection Policies］の順に選択します。
［Protection Policies］ウィンドウが表示されます。
2. 仮想ネットワークを構成する既存の保護ポリシーを見つけます。
3. 保護ポリシーのラジオ ボタンを選択し、［Edit］をクリックします。
［Summary］ページで、［Edit Policy］ウィザードが開きます。
4. ［Objectives］ブロックで、［Edit］をクリックします。
［Edit Policy］ウィザードから［Objectives］ページに移動します。
5. 該当するスケジュールのチェックボックスをオンにします。
6. ［ネットワーク インターフェイス］フィールドで、リストから適切な仮想ネットワークを選択します。ネットワークの目的が［Data］であるネットワーク インターフェイスのみが一覧表示されます。ネットワーク設定を変更する場合は、セクション「保護ストレージのネットワーク設定の変更」を確認してください。

   各リストのエントリーは、インターフェイス名、インターフェイス スピード、仮想ネットワーク名を示します。

ネットワークに名前が付いていない場合、インターフェイス名と VLAN ID を組み合わせたものが仮想ネットワーク名に置き換えられます。たとえば、`ethV1.850` です。仮想ネットワーク名のないインターフェイスは、仮想ネットワークが構成されていないように作動します。

7. ［Next］をクリックします。
   ［Edit Policy］ウィザードから［Summary］ページに移動します。
8. ポリシーの情報を確認し、［Finish］をクリックします。
   選択した資産が仮想ネットワークの一部を構成していることを確認します。
   ［Edit Policy］ウィザードが閉じます。
9. ［OK］をクリックしてアップデートを承認するか、［Go to Jobs］をクリックしてアップデートを監視します。

資産別の仮想ネットワークの割り当て

この手順はオプションです。仮想ネットワークは、個々の資産に対しても、特定のアプリケーション ホスト上のすべての資産に対しても割り当てることができます。

このタスクについて

この設定は、保護ポリシーによるネットワークの割り当てをオーバーライドします。何らかの理由で PowerProtect Data Manager がこのネットワークの割り当てを使用できない場合、設定のフォール バックが行われて保護ポリシーによる割り当てが使用されます。

メモ: 同じ保護ポリシーおよびアプリケーション ホスト上の異なるネットワーク間で個々の資産をバック アップできません。代わりに、各ネットワーク上の資産に対して個別の保護ポリシーを作成してください。

手順

1. PowerProtect Data ManagerUI から、［インフラストラクチャ］ > ［資産］の順に選択します。
   ［Assets］ウィンドウが表示されます。
2. いずれかのタブのリストから目的の資産を見つけます。
   各資産の選択には、チェックボックスを使用します。一度に複数の資産を選択できます。
3. ［その他のアクション］ > ［ネットワークの割り当て］をクリックします。
   ［[関連付けられた資産]］ウィンドウが開きます。
4. 仮想ネットワークを同じアプリケーション ホスト上のすべての資産で使用するには、［含める］をクリックします。
   それ以外の場合で、選択した資産にのみ仮想ネットワークを使用するには、［含めない］をクリックします。異なるネットワーク上の資産に別の保護ポリシーが必要かどうかを検討します。
   ［[ネットワークの割り当て]］ウィンドウが開きます。
5. ［ネットワーク ラベル］リストから仮想ネットワークを選択し、［保存］をクリックします。

タスクの結果

PowerProtect Data Manager によって選択した資産に選択したネットワークが適用されます。各タブの資産リストの［ネットワーク］列に、選択した仮想ネットワークが表示されるようになりました。

Syslog サーバーのディザスター リカバリー

サーバーのディザスター リカバリー(DR)の際に、Syslog サーバーのログ マネージャー サービスを再起動するには、次の手順を実行します。

前提条件

PowerProtect Data Manager システムのディザスター リカバリーが完了したら、リストア後の PowerProtect Data Manager システムで次の手順を実行します。

手順

1. ［System Settings］ > ［Support］ > ［System Services Status］で、すべての PowerProtect Data Manager サービスが実行中であることを確認します。
2. コマンド `logmgr restart` を実行して `logmgr` 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。

次の手順

Syslog サーバーでカスタム ポートが使用されている場合は、リストア後の PowerProtect Data Manager システムで対応するポートを開きます。詳細については、*PowerProtect Data Manager* セキュリティ構成ガイドを参照してください。

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。

1. 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。
2. 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。
3. 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。

11

レポートの管理

トピック：

PowerProtect Data Manager レポート作成

PowerProtect Data Manager には、PowerProtect Data Manager ユーザー インターフェイス内でレポート作成機能を提供する reporting engine が搭載されています。レポートの生成を直接実行できる、組み込みのレポート テンプレートにアクセスできます。今後のリリースに向けて、フィードバックも受け付けています。

これらのレポートは、環境内のデータ保護アクティビティーに関する情報を取得するのに役立ちます。これらのレポートを利用することで、問題を診断し、リスクの移行を計画して、今後の傾向を予測できます。レポートをオンデマンドで実行したり、CSV 形式でレポートのエクスポートをしたりすることもできます。

レポート データ内のイベントは、UTC ですべて表示されます。

PowerProtect Data Manager のレポート作成は、オンプレミスの PowerProtect Data Manager 導入で使用できます。

メモ: PowerProtect Data Manager のレポート作成は、クラウド環境の PowerProtect Data Manager ではサポートされていません。

レポート エンジン, reporting engine を構成して、PowerProtect Data Manager のレポート作成機能を設定します。レポート エンジン, reporting engine が構成されると、［Reports］ > ［Report Browser］でレポートを実行できます。

メモ: CloudIQ など別のレポート作成ツールを使用している場合は、PowerProtect Data Manager のレポート作成を構成しないことを選ぶことができます。

ポート要件

次の表に、PowerProtect Data Manager と Reporting Engine のポート要件をまとめています。PowerProtect Data Manager のポートに関する詳細については、*PowerProtect Data Manager* セキュリティ構成ガイドを参照してください。この表は、PowerProtect Data Manager のポートの使用に関するトピックとあわせてお読みください。

表 42. Reporting Engine 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
PowerProtect Data Manager	Reporting Engine	9002	TCP	TLS 1.2	REST API サービス。
PowerProtect Data Manager	Reporting Engine	9613d	独自のプロトコル	TLS 1.2	レポート エンジン, reporting engine のインフラストラクチャ ノード エージェントの管理。

表 42. Reporting Engine 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
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。
ユーザー	Reporting 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。

サーバーの要件

Reporting Engine に関する次の要件を確認してください。

- SUSE Linux Enterprise Server (SLES)バージョン 12 SP5
- 8 x vCPU、16 GB RAM
- ディスク 01：48 GB（オペレーティング システムとレポート作成アプリケーション サーバーのインストール用）
- ディスク 02：512 GB（レポート データの保存用）
- ディスク 03：8 GB（ログ情報の保存用）

メモ: レポート エンジンは IPv4 通信のみをサポートしています。

サポートされていない vCenter のレポート エンジン関連の操作

レポート エンジンは、常にのドキュメントとガイダンスに従って管理する必要があります。

カスタマー サポートからお知らせがない限り、レポート エンジンが導入されている仮想マシンを、vCenter を使用して変更または制御することはサポートされていません。サポートされていない vCenter 操作には次のようのものがあります。

- 仮想マシンの電源状態の変更
- 仮想マシンのプロパティの変更
- 仮想マシンのクローニング
- 仮想マシンの削除
- 手動 vMotion の実行
- スナップショットの作成またはリストア

レポート エンジン, reporting engine および Report Browser に関する既知の問題

管理者は、新しいレポート作成機能を使用する前に、既知の問題について十分に理解しておく必要があります。機能のメンテナンスとレポートの解釈には、既知の問題を理解しておくことが役立ちます。

次の表で、新しいレポート作成機能に関する既知の問題について説明します。

表 43. レポート エンジン, reporting engine および［Report Browser］に関する既知の問題

問題

Report Browser を構成またはレポートを生成しようとすると、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。
`The reporting engine is not configured`
`Configure the reporting engine to access reports.`
`An error occurred in obtatining the reporting engine configuration details.`
この問題を解決するには、次の手順に従います。
1. Report Browser が構成されていない場合は、構成します。
2. Report Browser が構成されている場合、または構成しようとしている場合は、Web ブラウザーでダッシュボードを再ロードします。

表 43. レポート エンジン, reporting engine および［Report Browser］に関する既知の問題 （続き）

問題
メモ: PowerProtect Data Manager は、Google Chrome の最新バージョンのみをサポートします。
Report Browser は、Cloud Snapshot Manager と統合されていません。Report Browser には Cloud Snapshot Manager のジョブが表示されないため、表示される総ジョブ数が、［Protection Jobs］ウィンドウに表示される総ジョブ数よりも少なくなることがあります。
Report Browser には、元々ステータスが `Failed` だったジョブが再試行されるたびにエントリーが 1 つ表示されます。このエントリーの複数表示は、失敗したジョブに対してエントリーが 1 つだけ表示される［Protection Jobs］ウィンドウの動作と一致しません。この不一致の結果、Report Browser に表示される総ジョブ数が、［Protection Jobs］ウィンドウに表示される総ジョブ数より多くなることがあります。
ジョブの転送されたデータの合計量が 1 MB 未満の場合、ジョブ エントリーには［Data Transferred］列に `0 bytes` が表示されます。
レポート エンジンが［Application Agents］ペインに未確認のエントリーとして表示されます。 **注意: このエントリーを削除しないでください。削除してしまった場合は、レポート エンジン, reporting engine の構成と導入を参照してください。**
カスタム フィルターからの SMIS 資産の選択は無視されます。これらの資産が選択されている場合でも、このフィルターを使用しているレポートには表示されません。
［Jobs Summary - Table View］レポートでは、検索機能は「equals」フィルター タイプのみをサポートします。
既存のカスタム スコープを編集するときに、検索機能を使用すると、以前に選択した資産が削除されます。新しい資産を追加し、以前に選択した資産を保持するには、検索機能を使用しないでください。すべての資産のリストをスクロールし、現在の選択内容を変更して、新しい資産を追加します。

レポート エンジン, reporting engine の構成と導入

PowerProtect Data Manager UI で次の手順を実行して、レポート エンジン, reporting engine を構成および導入します。

前提条件

- レポート エンジン, reporting engine を別の仮想マシンに導入する必要があります。
- vCenter Server を、［Infrastructure］ > ［Asset Sources］から資産ソースとして追加する必要があります。
- 仮想マシンが正常に機能するには、500 GB が必要です。

このタスクについて

レポート エンジン, reporting engine を PowerProtect Data Manager のホストである vCenter Server に導入することが推奨されています。ホスティング vCenter を確認するには、次の手順を実行します。

1. ［Settings］ > ［Hosting vCenter］のリンクをクリックします。
2. PowerProtect Data Manager のホストである vCenter Server の詳細を入力するか、資産ソースからホスティング vCenter Server を選択します。

手順

1. PowerProtect Data Manager UI で、［Reports］ > ［Reporting Engine］の順に選択します。
2. ［Configure］をクリックします。
   ［Configure Reporting Engine］ダイアログ ボックスが開きます。
3. ［Configure Reporting Engine］ダイアログ ボックスで、次の必須入力フィールドに入力します。
   - ［vCenter server to deploy］：レポート エンジン, reporting engine を導入する vCenter サーバーを指定します。
     ホスティング vCenter Server を指定した場合、必要な情報が PowerProtect Data Manager によってフィールドに入力されます。
   - ［ESX host or cluster］：レポート エンジン, reporting engine をどのクラスターまたは ESXi ホストで構成するかを選択します。
   - ［Host FQDN］：完全修飾ドメイン名(FQDN)を指定します。
   - ［IP address］、［Gateway］、［Netmask］、［Primary DNS］：IPv4 アドレスのみがサポートされています。
   - ［Network］：選択した ESXi ホストまたはクラスターで使用可能なすべてのネットワークが表示されます。
     仮想ネットワーク(VLAN)の場合、このネットワークは管理トラフィックを伝送します。

- ［Data Store］：選択した ESXi ホストまたはクラスターにアクセスできるすべてのデータストアが表示されます。データストアを選択します。

4. ［Deploy］をクリックします。

タスクの結果

PowerProtect Data Manager により、構成プロセスが開始されます。［Reporting Engine］に移動して、ステータスを確認します。［System Jobs］ウィンドウに移動して、構成ジョブの進行状況を監視することもできます。

プロセスが完了すると、構成が正常に完了したことを示す通知が［Reporting Engine］ウィンドウに表示されます。これで、［Reports］ > ［Report Browser］からレポートにアクセスできます。

レポート エンジン, reporting engine バージョン 19.10 からのアップデート

PowerProtect Data Manager バージョン 19.10 からアップデートをする際に特定の手順を実行していない場合、導入済みのレポート エンジン, reporting engine のアップデートに失敗します。

すでにレポート エンジン, reporting engine を導入していて、PowerProtect Data Manager バージョン 19.10 からアップデートをする場合は、既存のレポート データを保持するか、削除するかを決定する必要があります。

レポート データの保持

PowerProtect Data Manager のアップデートを行ってレポート データを保持するには、KB 記事 000199837：*PowerProtect Data Manager (PPDM) 19.10* レポート アップデート手順を参照してください。

レポート データの削除

PowerProtect Data Manager のアップデートを行ってレポート データを削除するには、次の手順を実行します。

1. レポート エンジン, reporting engine を削除します。詳細については、レポート エンジン, reporting engine の削除を参照してください。
2. PowerProtect Data Manager アップデート パッケージのインストールを行います。
3. レポート エンジン, reporting engine を再構成して再導入します。

レポート ブラウザー

環境内のデータ保護アクティビティーに関する詳細なレポートを表示するには、［Report Browser］を使用します。

レポート テンプレート

レポート テンプレートは、レポートの生成に使用します。テンプレートを選択すると、特定のレポート タイプが使用されます。このレポート タイプは、フィルターを適用することでさらに変更できます。レポート テンプレートとレポートは、ジョブ アクティビティ カテゴリーまたは資産保護カテゴリーのいずれかに属します。

システム標準のレポート テンプレート

［Report Browser］には、ジョブ アクティビティ用の 6 つのシステム標準レポート テンプレートと資産保護用の 4 つのシステム標準レポート テンプレートが用意されています。［Report Browser］ペインのタブに表示されるレポートがない場合は、システム標準のレポート テンプレートが表示されます。［Report Browser］ペインのタブに 1 つ以上のレポートが表示されている場合は、レポートの生成時にシステム標準のレポート テンプレートが表示されます。

システム標準のレポート テンプレートは編集も削除もできませんが、レポートとレポートに基づくカスタム レポート テンプレートは編集と削除ができます。

カスタム レポート テンプレート

カスタム レポート テンプレートは、次の方法で作成、編集、削除できます。

- レポートが生成されると、レポートに関連付けられたカスタム レポート テンプレートも作成されます。
- ［Report Browser］ペインからレポートを編集すると、関連付けられたレポート テンプレートがアップデートされます。
- すべてのカスタム レポート テンプレートを表示するには、［Reports］ > ［Report Templates］に進みます。
- カスタム レポート テンプレートを作成するには、以下の手順に従います。
  1. ［Report Templates］ペインからテンプレートの名前をクリックします。
  2. テンプレートを選択すると、UI が［Report Browser］ペインに変更され、関連付けられたレポートのタブが選択されます。
  3. ⋮ をクリックして、［Edit］を選択します。
  4. レポートの名前を変更するには、名前の右側にある をクリックし、名前を編集した後、 をクリックします。
  5. レポートの説明を変更するには、説明の右側にある をクリックし、説明を編集した後、 をクリックします。
  6. レポートに適用するフィルターをアップデートし、［Apply］をクリックします。

     メモ: フィルターをデフォルト値にリセットするには、［Reset］をクリックします。
  7. ⋮ をクリックして、［Save Template］を選択します。
- カスタム レポート テンプレートを削除するには、［Report Templates］ペインでエントリーの左側にあるラジオ ボタンを選択し、［Delete］をクリックします。

レポート

［Report Browser］で閲覧可能なレポートについて説明します。

次の図は、［Backup Jobs Summary］レポートの例です。

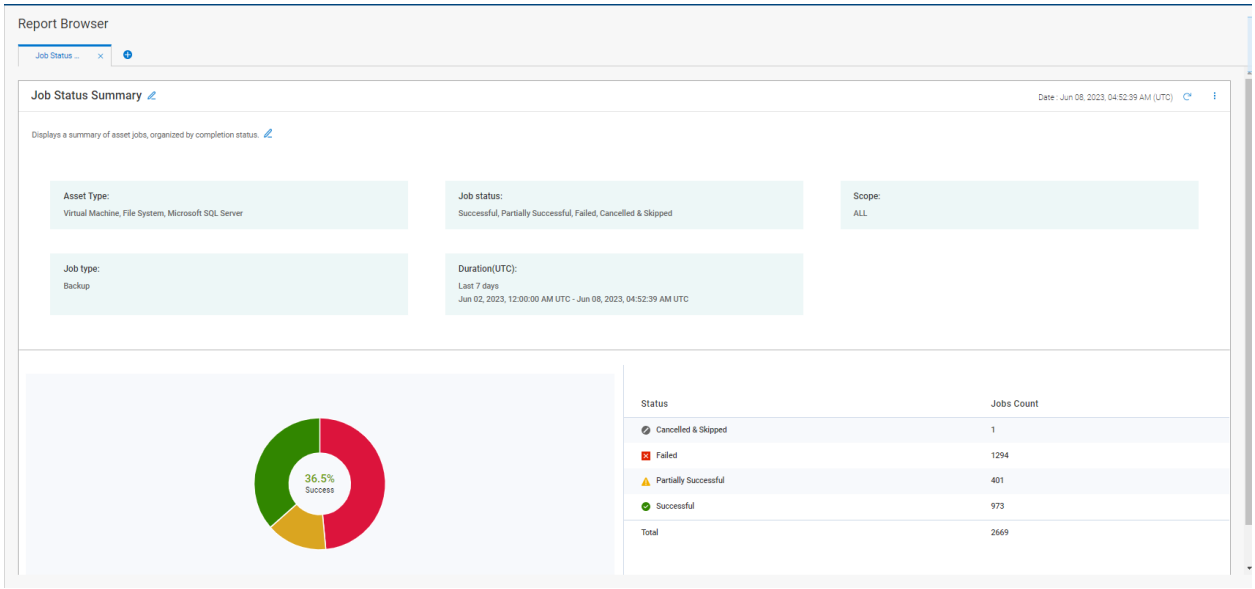


図 15. ［Jobs Status Summary］レポート

レポートごとに、次の操作を実行できます。

- 特定のメトリクスの選択によるレポートのフィルタリング。
- サマリー レポートの詳細情報を表示します。

レポートの生成

レポートを生成するには、次のアクションを実行します。

1. システム標準のレポート テンプレートに基づいてレポートを生成するには、次の手順を実行します。
   a. ［Reports］ > ［Report Browser］に進みます。

b. レポートのベースになるテンプレートの下にある［Generate Report］をクリックします。

メモ: システム標準のレポート テンプレートが表示されない場合は、⊕をクリックします。

2. カスタム レポート テンプレートに基づいてレポートを生成するには、次の手順を実行します。
   a. ［Reports］ > ［Report Templates］に進みます。
   b. レポートのベースになるテンプレートの名前をクリックします。
3. レポートの名前を変更するには、名前の右側にあるをクリックし、名前を編集した後、をクリックします。
4. レポートの説明を変更するには、説明の右側にあるをクリックし、説明を編集した後、をクリックします。
5. レポートに適用するフィルターを選択し、［Apply］をクリックします。

メモ: フィルターをデフォルト値にリセットするには、［Reset］をクリックします。

レポートの編集

レポートを編集するには、次の手順を実行します。

- ［Report Browser］ペインで、レポートのタブを選択します。
- ⋮をクリックして、［Edit］を選択します。
- レポートの名前を変更するには、名前の右側にあるをクリックし、名前を編集した後、をクリックします。
- レポートの説明を変更するには、説明の右側にあるをクリックし、説明を編集した後、をクリックします。
- レポートに適用するフィルターをアップデートし、［Apply］をクリックします。

  メモ: フィルターをデフォルト値にリセットするには、［Reset］をクリックします。

データ コレクションの頻度

PowerProtect Data Manager では、定期的にレポート データが収集されます。次の表に、PowerProtect Data Manager で収集されるデータのタイプとデータ収集の頻度に関する情報を示します。

表 44. データ コレクションの頻度

データのタイプ	説明	データ コレクションの頻度
Status	PowerProtect Data Manager サーバー全体のステータス。	15 分ごと。
Configuration	資産に関する情報。	1 時間ごと。
Protection jobs	［Protect］、［Restore］、［Replicate］のジョブを含む、データ保護アクティビティーに関する情報。	5 分ごと。

メモ: レポート データは現在のものではなく、最後に成功したデータ コレクション リクエストと同じ時期のものです。そのため、過去データを確認するためにのみレポートを使用する必要があります。

- 現在のジョブ データを表示するには、［Jobs］ > ［Protection Jobs］に移動します。
- 現在の資産データを表示するには、［Infrastructure］ > ［Assets］に移動します。
- PowerProtect Data Manager システム全体の状態の大まかなビューを表示するには、［Dashboard］に移動します。

詳細レポートの情報とレポートのタイミング

サマリー レポートのチャートをクリックして詳細情報を表示すると、新しいレポートが実行され、最新のデータが表示されます。2 つのレポートがいつ実行されるかに応じて、詳細レポートとサマリー レポートに表示されるジョブ数が一致しないことがあります。ジョブ数が異なる場合、詳細レポートに表示されるジョブ数の方が正確です。サマリー レポート ページを更新すると、情報をアップデートできます。

レポート ブラウザーのオプション

［Report Browser］ペインで⋮をクリックして、レポートのオプションを構成します。

次の表で、レポートのメニュー項目について説明します。

表 45. レポート オプション

メニュー項目	メニュー項目を選択して、次を実行できます。
編集	フィルターとカスタマイズのオプションを構成します。
メール	1 人以上の受信者に E メールでレポートを送信します。
エクスポート	レポートを .csv ファイルとしてエクスポートします。
テンプレートの保存	このレポートのテンプレートを保存します。
スケジュール	定期的なスケジュールで、1 人以上の E メール受信者にレポートを自動的に送信します。

1 人以上の受信者にレポートを E メールで送信

レポートを .csv 添付ファイルとして送信するには、次の手順を実行します。

メモ: これらの操作を実行する前に、SMTP を構成する必要があります。詳細については、E メール サーバーの設定を参照してください。

1. [Report Browser] ペインで、レポートのタブを選択します。
2. ⋮ クリックし、[Email] を選択します。[Email Report] ウィンドウが開きます。
3. [Report Name] に情報を入力します。
4. [To]、[Subject]、[Body] に情報を入力します。
5. [] をクリックします。

自動レポートのスケジュール設定

定期的なスケジュールでレポートを .csv 添付ファイルとして自動的に送信するには、次の手順を実行します。

1. カスタム レポート テンプレートに基づいてレポートを送信するには、 [Report Templates] ペインで、レポートの基になるテンプレートの名前をクリックします。
2. [Report Browser] ペインで、レポートのタブを選択します。
3. ⋮ をクリックして、[Schedule] を選択します。[Schedule Report] ペインが開きます。
4. [Report Name] と [Schedule Name] の情報を入力します。
5. [Frequency] ドロップダウンリストから、日単位、週次、または月次のスケジュールを選択します。
6. [At] ドロップダウン リストから時刻の情報を入力します。
7. 週次または月次のスケジュールが選択されている場合は、適切なコントロールから曜日または月を選択します。
8. [Next] をクリックします。
9. [To]、[Subject]、[Body] に情報を入力します。
10. [Next] をクリックして、レポート名、スケジュール、E メールの詳細のサマリーを表示します。
11. [Override Schedule] をクリックします。

メモ: レポートの自動レポートがスケジュール設定された後、[Report Browser] ペインでレポート名のタブを選択するか、[Report Templates] ペインで関連付けられたテンプレートを選択すると、レポートとそのスケジュールに関する情報を確認できます。スケジュール情報を表示した際には、スケジュールの無効化または有効化、スケジュールの削除、スケジュールの編集を行うことができます。

レポート情報のタイプ

レポートはさまざまな種類の情報を提示します。利用可能な情報のタイプを知っておくと役立ちます。

次の表に、さまざまなタイプのレポートと、レポートが提示する情報を示します。この表は、カテゴリー別にグループ化されています。

メモ: この情報は、複数のレポートと構成で使用できます。個々のレポートには、情報のサブセットが含まれている場合があります。

表 46. ジョブ アクティビティ別のレポート タイプ

レポート タイプ	表示される情報
Job Status Summary	バックアップ、リストア、またはレプリケーションの成功したジョブと失敗したジョブの合計数に加え、割合のサマリー

表 46. ジョブ アクティビティ別のレポート タイプ （続き）

レポート タイプ	表示される情報
Job Status by Asset Type	バックアップ、リストア、またはレプリケーションの成功したジョブと失敗したジョブの資産タイプに基づく合計数
Time-based Job Status	バックアップ、リストア、またはレプリケーションの成功したジョブと失敗したジョブの数、一定期間のリストア ジョブの数
Data Transfer Rate	一定期間のデータ転送速度
Asset Failure Rate	プライマリー バックアップの連続失敗回数が最も多い資産。失敗回数と最後にバックアップまたはリストアに成功した時刻を示します。
Jobs Summary - Table View	次に示す、すべてのジョブの詳細とステータスが表示されます。 • 資産名 • 資産タイプ • ホスト • 開始時間 • ジョブ ステータス • ポリシー名 • データ転送

表 47. 資産保護別のレポート タイプ

レポート タイプ	表示される情報
Asset Protection	保護されている資産と保護されていない資産の合計数と、［Exclusion］保護ポリシーに含まれる資産の合計数のサマリー。
Asset Protection by Asset Type	保護されている資産と保護されていない資産の合計数と、［Exclusion］保護ポリシーに含まれる資産の合計数のサマリー。この情報は、資産タイプ別にグループ化されています。
Time-based Asset Protection	保護された資産と保護されていない資産の合計数と、［Exclusion］保護ポリシーに含まれる資産の過去 7 日間のサマリー。この情報はグラフ化されています。
Asset Jobs Distribution	次に示す、すべてのジョブの詳細とステータスが表示されます。 • 名前 • 資産タイプ • ホスト • ポリシー名 • セルフ サービス • 最後のコピー • 資産ステータス • 保護ステータス

レポートのフィルタリングとカスタマイズ

［Report Browser］には、レポート データのフィルタリングとカスタマイズを行うためのオプションがあります。

ブラウザー セッションの期間中は、開いているレポートに適用されるフィルターが保持されます。ただし、同じブラウザー セッション中にレポートを閉じてから再び開いた場合、適用されたフィルターは保持されません。

カスタム スコープに資産を追加する際の検索機能の使用

検索機能を使用して、カスタム スコープ内の資産を選択できます。検索を実行すると、検索結果から選択した資産のみがカスタム スコープに追加されます。

注意: 既存のカスタム スコープを編集するときに、検索機能を使用すると、以前に選択した資産が削除されます。新しい資産を追加し、以前に選択した資産を保持するには、検索機能を使用しないでください。すべての資産のリストをスクロールし、現在の選択内容を変更して、新しい資産を追加します。

レポート エンジン, reporting engine の削除

レポート エンジン, reporting engine の削除に関する次の情報を確認してください。

注意: レポート エンジン, reporting engine を削除すると、すべてのレポート データが削除されます。

レポート エンジン, reporting engine を削除しないことをお勧めします。

PowerProtect Data Manager からレポート エンジン, reporting engine を削除するには、［Reports］ > ［Reporting Engine］に移動し、［Delete］をクリックします。レポート エンジン, reporting engine を削除するとデータ ロスが発生するという通知がウィンドウに表示されます。

削除後のレポート エンジン, reporting engine の再構成

レポート エンジン, reporting engine を再構成するには、［Reports］ > ［Reporting Engine］に移動し、［Configure］をクリックします。レポート エンジン, reporting engine の構成方法に関する詳細な手順については、「レポート エンジン, reporting engine の構成と導入」を参照してください。

レポート エンジン, reporting engine のディザスター リカバリーの管理

管理者は、レポート エンジン, reporting engine がディザスターから保護されていることを確認する必要があります。

メモ: サーバー ディザスター リカバリー(DR)のレポート作成をサポートしているのは、DD Boost ストレージ タイプのみです。NFS はサポートされていません。

レポート エンジン, reporting engine が導入されると、次の処理が実行されます。

- 構成済みのサーバー DR バックアップによって、レポート エンジン, reporting engine およびすべてのレポート作成データのバック アップが自動的に行われます。
- サーバー DR バックアップから PowerProtect Data Manager のリカバリーが行われた場合、レポート エンジン, reporting engine およびすべてのレポート作成データのリカバリーも行われます。

DR バックアップからのレポート エンジン, reporting engine のリカバリー

PowerProtect Data Manager システムのディザスター リカバリーが完了した後、PowerProtect Data Manager でレポート エンジン, reporting engine が自動的にリストアされます。PowerProtect Data Manager システムでレポート エンジン, reporting engine を自動的にリストアできなかった場合は、この手順のステップを使用し、REST API を経由してレポート エンジン, reporting engine のみをリストアしてください。レポート エンジン, reporting engine のリカバリーは、運用可能な PowerProtect Data Manager システムで実行する必要があります。レポート エンジン, reporting engine をリストアできるのは、管理者ロールのみです。

前提条件

［System Settings］ > ［Disaster Recovery］ > ［Manage Backups］の順に移動し、レポート エンジン, reporting engine バックアップの名前を取得します。

このタスクについて

バックアップ マニフェスト ファイルを使用して、REST API で POST コマンドを実行するために使用する新しいテキスト ドキュメントを次の手順に従って作成します。

注意: マニフェスト ファイルは編集しないでください。

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。
   PowerProtect Data Manager をリストアする前に使用したものと同じ認証情報を使用します。
2. 管理者ユーザーとして PowerProtect Data Manager コンソールに接続します。
3. ディレクトリーを`/data01/server_backups/<PowerProtect Data Manager Hostname>_<NodeID>`に変更し、バックアップ マニフェスト ファイルを見つけます。

通常は、/data01/server_backups に 1 個のサブディレクトリーしかないため、そのサブディレクトリーに変更します。ただし、複数のサブディレクトリーがあり、正しい<*NodeID*>がわからない場合は、次のサブステップを実行します。

a. /data01/server_backups から次のコマンドを実行し、必要に応じてユーザー名とパスワードを変更します。

```
TOKEN=$(curl -X POST https://localhost:8443/api/v2/login -k -d '{ "username":
"admin","password": "admin_password" }' --header "Content-Type: application/json" |
python3 -c "import sys, json; print(json.load(sys.stdin)['access_token'])")
```

```
curl -X GET https://localhost:8443/api/v2/nodes -k --header "Content-Type: application/
json" --header "Authorization:Bearer $TOKEN"
```

b. grep -Rnwa -e '<*Name*>' --include=*.manifest コマンドを実行します。

4. マニフェスト ファイルを一時ファイルにコピーします。
5. 一時ファイルを開きます。
6. 次の例を確認し、//コメント エントリーに記載されている変更を行います。

メモ: ここに表示されている//コメント エントリーは、一時ファイルに含まれていません。これらのコメント エントリーは、ここにのみ表示され、ガイドの役割を果たします。

```
{
  "id": "ca8cbb13-6f3d-4ac5-87e5-de47a634379f",
  "jobId": "990b4ea7-c0e4-4069-8dd5-7d0e084370fc",  // DELETE LINE
  "creationTime": "34e1c9dd-1b54-48b4-8283-151331d193ff",
  "lastUpdated": "2022-08-25T19:40:18.165497Z",// DELETE LINE
  "elapsedSeconds": 115,
  "sequenceNumber": 89
  "state": "Successful",// DELETE LINE
  "version": "19.12.0-1-SNAPSHOT", // DELETE LINE
  "hostname": "ldpdb141.hop.lab.emc.com", // DELETE LINE
  "name": "mercijTestDr", // DELETE LINE
  "nodeId": "a8d2df8e-5c3e-4160-87d4-32b9bfe6c283", // DELETE LINE
  "sizeInBytes": 18244130,
  "consistency": "CRASH_CONSISTENT", // DELETE LINE
  "checksum": "bbd97a04f296a8ed116e4a9272982d8e8411f3d0cf50dea131d5c2cd4ce224f8", //
DELETE LINE
  "backupConsistencyType": "FULL", // DELETE LINE
  "esSnapshotState": "UNKNOWN", // DELETE LINE
  "backupTriggerSource": "USER", // DELETE LINE
  "configType": "standalone", // DELETE LINE
  "deployedPlatform": "vmware", // DELETE LINE
  "replicationTargets": [], // DELETE LINE
  "repositoryFileSystem": "BOOST_FILE_SYSTEM", // DELETE LINE
  "ddHostname": "ldpdg251.hop.lab.emc.com", // DELETE LINE and add line "recover":true,
  "Components": [   // change Components to components with lower case c
    {  // DELETE WHOLE PPDM COMPONENT LEAVING ONLY REPORTING
      "name": "PPDM",
      "id": "ca7cbb13-6f3d-4ac5-87e5-de47a634379f",
      "lastActivityId": "2bdbe7a8-7c57-446d-b072-ad8081e2953d",
      "version": "v2",
      "backupPath": "ldpdg251.hop.lab.emc.com:SysDR_ldpdb141/
ldpdb141_a8d2df8e-5c3e-4160-87d4-32b9bfe6c283/PPDM",
      "backupStatus": "SUCCESSFUL",
      "backupsEnabled": true,
      "errorResults": []
    }, // STOP DELETING HERE
    {
      "name": "REPORTING",
      "id": "34e1c9dd-1b54-48b4-8283-151331d193ff",
      "lastActivityId": "ed2dc805-c1f7-42fd-b9af-71897fc1da01",
      "version": "v2",
      "backupPath": "192.168.100.109:SysDR_DPDII2201IDPA10/
ppdm_64d2f00a-1ce0-47b5-9c60-914ea7d0e1e8/REPORTING",
      "backupStatus": "SUCCESSFUL",
      "backupsEnabled": true, // DELETE TRAILING COMMA
      "errorResults": [] // DELETE LINE
    }
  ], // DELETE TRAILING COMMA
  "componentVersions": [],// DELETE LINE
```

```
  "expirationTime": "2023-06-11T09:41:20.383633Z",// DELETE LINE
  "protectionCopySetId": "07e7af37-1a80-5436-b320-9e537fba1317"// DELETE LINE
}
```

まとめると、次のようになります。

- ここに表示されている`// DELETE LINE`コメント エントリーの行をすべて削除します。
- `recover: true`を追加します。
- `Components`を`components`に変更します。
- リストに記載されている、`REPORTING`以外のコンポーネント ブロックをすべて削除します。
- `"backupsEnabled": true,`から末尾のコンマを削除します。
- `[,`から末尾のコンマを削除します。

このように変更すると、次のようになります。

```
{
    "id":"ca8cbb13-6f3d-4ac5-87e5-de47a634379f",
    "creationTime":"2022-10-12T15:01:13.476401+0000",
    "elapsedSeconds":115,
    "sequenceNumber":89,
    "sizeInBytes":18244130,
    "recover":true,
    "components":[
        {
            "name":"REPORTING",
            "id":"ca8cbb13-6f3d-4ac5-87e5-de47a634379f",
            "lastActivityId":"ed2dc805-c1f7-42fd-b9af-71897fc1da01",
            "version":"v2",
            "backupPath":"192.168.100.109:SysDR_DPDII2201IDPA10/
ppdm_64d2f00a-1ce0-47b5-9c60-914ea7d0e1e8/REPORTING",
            "backupStatus":"SUCCESSFUL",
            "backupsEnabled":true
        }
    ]
}
```

7. `"id":`の後の引用符で囲まれたテキストの値をコピーします。

   ステップ 11 で使用する変数*<backupID>*をこの値に置き換えます。この例では、*<backupID>*は`ca8cbb13-6f3d-4ac5-87e5-de47a634379f`です。

8. 一時ファイルからキャリッジ リターンをすべて削除し、すべてのテキストを 1 行で表します。
9. 一時ファイルからすべてのテキストをコピーします。

   ステップ 11 で使用する変数*<manifestText>*をこの値に置き換えます。

10. 次のコマンドを実行し、必要に応じてユーザー名とパスワードの認証情報を変更します。

    メモ: このコマンドをステップ 3.a で実行した場合でも、もう一度実行してください。`TOKEN`の値には有効期限があります。

```
TOKEN=$(curl -X POST https://localhost:8443/api/v2/login -k -d '{ "username":
"admin","password": "admin_password" }' --header "Content-Type: application/json" |
python3 -c "import sys, json; print(json.load(sys.stdin)['access_token'])")
```

11. 次のコマンドを実行します。

```
curl -X PUT 'https://localhost:8443/api/v2/server-disaster-recovery-backups/<backupID>' --
header "Authorization: Bearer $TOKEN" --header 'Content-Type: application/json' -k -d
'<manifestText>'
```

- *<backupID>*をステップ 7 で取得した値に置き換えます。
- *<manifestText>*をステップ 9 で取得したすべてのテキストに置き換えます。

12. リストア プロセスのステータスをモニタリングするには、PowerProtect Data Manager UI で、［Jobs］ > ［System Jobs］の順に選択して、説明欄に［Server Disaster Recovery Restore］の記載があるジョブを検索します。

次の手順

ステップ 4 で作成した一時ファイルを削除します。

12

PowerProtect Agent Service の構成と管理

トピック：

PowerProtect エージェント サービスについて

PowerProtect エージェント サービスは、アプリケーション ホスト上のアプリケーション エージェントによってインストールされる REST API ベースのサービスです。エージェント サービスは、検出、保護、リストア、インスタント アクセス、その他の関連する操作を実行するためのサービスと API を提供します。PowerProtect Data Manager は、エージェント サービスを使用してアプリケーション資産に統合データ保護を提供します。

このセクションでは、*<agent_service_installation_location>*を使用した PowerProtect エージェント サービスのインストール ディレクトリーを示します。デフォルトでは、エージェント サービスをインストールする場所は Windows の場合 `C:\Program Files\DPSAPPS\AgentService` で、Linux の場合は`/opt/dpsapps/agentsvc` です。このセクションで参照されるすべてのファイルは、エージェント サービスをインストールする場所への相対パスです。

PowerProtect エージェント サービスは次の操作を実行します。

- アドオン検出：アドオンは、アプリケーション エージェントをエージェント サービスに統合します。エージェント サービスは各アプリケーションの資産タイプのシステム上にあるアドオンを自動的に検出し、PowerProtect Data Manager に通知します。さまざまな資産タイプに対して複数のアドオンを実行できますが、アプリケーション ホストで実行できるエージェント サービスは 1 個だけです。特定の資産タイプは同じアプリケーション ホストで共存できます。
- 検出：エージェント サービスは、アプリケーション エージェント ホスト上のスタンドアロンおよびクラスタ化されたデータベース サーバー（アプリケーション システム）、データベースとファイル システム（資産）、バックアップ コピーを検出します。最初の検出後にエージェント サービスが新しいアプリケーション システム、資産、コピーを検出すると、PowerProtect Data Manager に通知します。
- セルフサービス構成：エージェント サービスは、PowerProtect Data Manager によって提供される情報を使用してアプリケーション エージェントを構成し、セルフサービス操作を実行できます。セルフサービスまたは一元化された保護のために資産を保護ポリシーに追加するか、DD Boost の認証情報の変更など保護ポリシーを変更すると、PowerProtect Data Manager は保護構成を自動的にエージェントにプッシュします。

  メモ: DD Boost の認証情報でパスワードに\を入れるように変更した場合、[Protection Policies] ウィンドウで保護ポリシーも選択して [Set LockBox] をクリックしない限り、保護ポリシーの構成がエージェントにプッシュされません。
- 一元的なバックアップ：エージェント サービスは、PowerProtect Data Manager によって要求されたとおりに一元的なバックアップを実行します。
- 一元的なリストア：エージェント サービスは、PowerProtect Data Manager によって要求されたとおりに一元的なリストアを実行します。

  メモ: 現在のリリースの場合、一元的なリストアは File System agent、Microsoft SQL Server エージェント、Storage Direct エージェントでのみ利用できます。
- バックアップの削除とカタログのクリーンアップ：PowerProtect Data Manager は、バックアップの有効期限が切れるか、明示的な削除リクエストを受信し、従属の（増分またはログ）バックアップがない場合は、バックアップ ファイルを保護ストレージから直接削除します。PowerProtect Data Manager は、エージェント サービスを通じて、データベース ベンダーのカタログとエージェントのローカル データストアからカタログ エントリーを削除します。

  メモ:

  手動またはコマンド ラインを使用したバックアップ コピーの削除は推奨されません。PowerProtect Data Manager は、必要に応じて期限切れのコピーをすべて削除します。

  エージェント サービスは、*<install_directory>*`/dbs/v1/backups` ディレクトリーに SQLite データベースのバックアップを保持します。このバックアップは、`config.yml` ファイル内の保存時間に基づいてクリーンアップされます。エージェント サービスは、バックアップ数が 10 を超えた場合にのみバックアップをクリーンアップします(10 番目以降のバックアップのみがクリーンアップされます)。

エージェント サービスは、インストーラーによってエージェントがインストールされている間に開始されます。エージェント サービスはバックグラウンドでアズ アサービスとして実行されるため、ユーザーが直接操作することはありません。

config.yml ファイルには、ファイル内で変更できるいくつかのパラメーター設定などエージェント サービスの構成情報が含まれています。config.yml ファイルは<agent_service_installation_location>ディレクトリーにあります。

config.yml ファイルが破損した場合は、次のコマンドを実行してファイルをリストアし、エージェント サービスによる保護を継続できます。

- Windows の場合：

```
agentService.exe config=config.yml service=false restoreConfig=true
```

- Linux および AIX の場合：

```
agentService config=config.yml service=false restoreConfig=true
```

エージェント サービスは、検出ジョブを実行するためにサブプロセスを定期的に開始します。これらのジョブのタイプと頻度は、config.yml ファイルの jobs:セクションで確認できます。ジョブ間隔の単位は分です。

エージェント サービスは<agent_service_installation_location>/dbs/v1 ディレクトリーでデータストアを維持します。データストアには、システム上で検出されたアプリケーション システム、資産、およびバックアップに関する情報が含まれています。データストア ファイルのサイズは、ホスト上のアプリケーションとコピーの数によって異なります。エージェント サービスはデータストアのバックアップを <agent_service_installation_location>/dbs/v1/backups ディレクトリーに定期的に作成し、このデータストアが失われた場合にデータストアをリカバリーするために使用します。

メモ: 各データストア バックアップのサイズは、データストア自体と同じです。デフォルトで、バックアップは 1 時間ごとに作成されます。ファイル システム上のスペースを節約するために、データストアが大きい場合はデータストアのバックアップ頻度を減らすことができます。デフォルトで、データストアのバックアップは 1 週間保持されます。データストアのバックアップ頻度、保存期間、およびバックアップする場所は config.yml ファイルで変更できます。

PowerProtect エージェント サービスの開始、停止、またはステータスの取得

PowerProtect エージェント サービスは、インストーラーによるエージェントのインストール中に開始されます。必要に応じて、適切な手順を使用してエージェント サービスの開始、停止、またはステータスの取得を実行できます。

Linux の場合、<agent_service_installation_location>ディレクトリーにある register.sh スクリプトを実行することによって、エージェント サービスの開始、停止、またはステータスの取得を実行できます。

- エージェント サービスを開始するには、次のようにします。

```
# register.sh --start

Started agent service with PID - 1234
```

- エージェント サービスを停止するには、次のようにします。

```
# register.sh --stop

Successfully stopped agent-service.
```

- エージェント サービスの実行中にステータスを取得するには、次のようにします。

```
# register.sh --status

Agent-service is running with PID - 1234
```

- エージェント サービスが実行されていないときにステータスを取得するには、次のようにします。

```
# register.sh --status

Agent-service is not running.
```

Windows では、他の Windows サービスと同様に、サービス マネージャーから PowerProtect エージェント サービスの開始、停止、またはステータスの取得を行うことができます。サービス マネージャーにおけるサービス名は、［PowerProtect Agent Service］です。

別のサーバー アドレスへの PowerProtect エージェント サービスの登録

PowerProtect エージェント サービスは、インストーラーによってエージェントがインストールされている間に特定の PowerProtect Data Manager サーバーに登録されます。必要に応じて、エージェント サービスを別の PowerProtect Data Manager サーバー アドレスに登録できます。

エージェント サービスは、1 個の PowerProtect Data Manager サーバーにのみ登録できます。新しいサーバーにエージェント サービスを登録すると、エージェント サービスは以前のサーバー アドレスでの登録を自動的に解除します。

エージェント サービスを新しいサーバーに登録する前に、次の手順を実行してください。

1. 前のトピックの説明に従って、エージェント サービスを停止します。
2. *<agent_service_installation_location>*/ssl フォルダーと*<agent_service_installation_location>*/dbs/v1/objects.db を削除します。

Linux では、*<agent_service_installation_location>*ディレクトリーにある register.sh スクリプトを実行して、エージェント サービスを別のサーバー アドレスに登録できます。

メモ: register.sh スクリプトにより、現在実行中のエージェント サービスを停止させます。

- 次のコマンドを実行すると、新しい IP アドレスまたはホストネームを要求するプロンプトが表示されます。

```
# register.sh

Enter the PowerProtect Data Manager IP address or hostname: 10.0.01

Warning: Changing IP of PowerProtect Server from 192.168.0.1 to 10.0.0.1

Started agent service with PID - 1234
```

- 次のコマンドには、コマンド ラインに新しい IP アドレスが含まれています。

```
#  register.sh --ppdmServer=10.0.0.1

Warning: Changing IP of PowerProtect Server from 192.168.0.1 to 10.0.0.1

Started agent service with PID - 1234
```

Windows では、エージェント インストーラーを起動して change オプションを選択することで、PowerProtect Data Manager サーバー アドレスを変更できます。「[Configuration Install Options]」ページから PowerProtect Data Manager サービスのアドレスを変更してください。

災害からの PowerProtect エージェント サービスのリカバリー

エージェント サービスまたは PowerProtect Data Manager の状態に関係なく、ファイル システムまたはアプリケーション エージェントを使用してアプリケーション資産のセルフサービス リストアを実行できます。このセクションでは、災害が発生してエージェント サービスのデータストアが失われた場合に、エージェント サービスを稼働状態にして続行させる方法について説明されています。

エージェント サービスは、*<agent_service_installation_location>*/dbs/v1/backups リポジトリーにデータストアのバックアップを定期的に作成します。これらすべてのバックアップが失われた場合でも、エージェント サービスは起動できます。エージェント サービスは、システム上のすべてのアプリケーション システム、資産、およびバックアップ コピーを再び検出し、PowerProtect Data Manager に通知します。障害が発生したタイミングによっては、エージェント サービスが一部の資産タイプの古いバックアップ コピーを検出できない場合があります。その結果、データベース ベンダー カタログをクリーン アップするまたは資産を PowerProtect Data Manager に追加する前に作成された古いバックアップを削除するときに、一元的な削除操作が失敗する可能性があります。

デフォルトでは、エージェント サービスはデータストア ファイルの整合性のあるコピーを 1 時間ごとにローカル ディスクにバック アップし、7 日間コピーを保持します。エージェント サービスは、データストアの内容をバック アップするたびに*<agent_service_installation_location>*/dbs/v1/backups リポジトリーにサブディレクトリーを作成します。サブディレクトリーには、操作が実行された時刻に基づいて YYYY-MM-DD_HH-MM-SS_epochTime の形式で名前が付けられます。

デフォルトでは、データストア リポジトリーはローカル ディスク上にあります。エージェント サービスのデータストアとそのローカル バックアップが失われないようにするために、ファイル システムのバックアップによってデータストアをバック アップすることをお勧めします。また、データストアをバックアップする場所をシステムに対してローカルではない別の場所に変更することもできます。データストアをバックアップする場所を変更するには、config.yml ファイルの値をアップデートします。

PowerProtect Data Manager エージェント サービスのデータストアのリストア

前提条件

メモ: エージェント サービスの電源がオフになっていることを確認してください。ディザスター リカバリーが完了するまでエージェント サービスを開始しないでください。

このタスクについて

データストア バックアップ リポジトリーからデータストアをリストアできます。リポジトリーがローカル ディスク上にない場合は、最初にファイル システムのバックアップからデータストアをリストアします。

データストア バックアップ リポジトリーのバックアップからデータストアをリストアするには、次の手順を実行します。

手順

1. *<agent_service_installation_location>*/dbs/v1 ディレクトリーのファイルを、安全に保管できる場所に移動させます。

   メモ: *<agent_service_installation_location>*/dbs/v1 のサブディレクトリーを移動させたり、削除したりしないでください。

2. 最新のデータストア バックアップを選択します。
   データストア バックアップ リポジトリー内のディレクトリーには、バックアップが作成された時刻に基づいて名前が付けられます。
3. データストア バックアップ ディレクトリーの内容を*<agent_service_installation_location>*/dbs/v1 ディレクトリーにコピーします。
   コピー操作が完了すると、*<agent_service_installation_location>*/dbs/v1 ディレクトリーには次のファイルが含まれているはずです。
   - copies.db
   - objects.db
   - resources.db
   - sessions.db
4. エージェント サービスを開始します。

エージェント登録のトラブルシューティング

エージェント登録の問題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ます。

Windows では、エージェントが PowerProtect Data Manager サーバーとの接続を確立できない場合、エージェントの登録が失敗し、次のエラー メッセージが表示されることがあります。

```
During a network connectivity test, the agent is unable to reach the PowerProtect Data
Manager server by using ping.

1.    If the ping command is blocked in the environment, the agent registration can still
complete successfully.
Review the agent service logs at INSTALL_DIR\DPSAPPS\AgentService\logs to verify that the
registration is successful. If the registration is successful, the status of the agent host
indicates [Registered] in the PowerProtect Data Manager UI.
2.    If the ping command is not blocked in the environment, the agent registration might not
complete successfully because a network connection cannot be started. If this occurs,
complete the following steps to troubleshoot the issue:
```

Linux または AIX では、エージェントが PowerProtect Data Manager サーバーとの接続を確立できない場合、エージェントの登録が失敗し、次のエラー メッセージが表示されることがあります。

```
During a network connectivity test, the agent is unable to reach the PowerProtect Data
Manager server by using ping and curl.

1.    If the ping command is blocked in the environment and curl is not installed, the agent
registration can still complete successfully.
Review the agent service logs at /opt/dpsapps/agentsvc/logs to verify that the registration
is successful. If the registration is successful, the status of the agent host indicates
[Registered] in the PowerProtect Data Manager UI.
2.    If the ping command is not blocked in the environment, the agent registration might not
```

```
complete successfully because a network connection cannot be started. If this occurs,
complete the following steps to troubleshoot the issue:
```

エージェントの登録が失敗し、これらのエラー メッセージが表示された場合は、次の操作を完了します。

1. 任意のネットワーク パケット トレーシング ツールを使用して、エージェント システムから PowerProtect Data Manager へのパケットをトレースします。
2. エージェント システムのソース IP と PowerProtect Data Manager デスティネーション IP の間のパケット トレーシングを開始します。
3. エージェント システムと PowerProtect Data Manager の間のネットワーク トラフィックを開始します。

   10～15 秒待ちます。

4. 保存されたパケットを分析します。
5. SYN と SYN_ACK パケットを探して、3 ウェイ ハンドシェイクが実行されているかどうかを確認します。

   ソース エージェントまたはデスティネーション PowerProtect Data Manager が接続をブロックしているかどうかを確認します。

   ネットワーク トラフィックがブロックされている場合は、ネットワーク セキュリティ チームに連絡してポート通信の問題を解決してください。

用語集

この用語集では、一連のマニュアル セット製品ドキュメントで使用されている頭字語の定義について説明します。

Special Terms

導入
Dell では、仮想マシンは仮想環境に `deployed` しますが、ソフトウェア コンポーネントとハードウェア デバイスは `installed` します。PowerProtect Data Manager と DDVE は、どちらも導入される仮想マシンです。このソフトウェア ガイドで `install` を検索し、適切なものが見つからない場合は、代わりに `deploy` を検索してください。

A

AAG : Always On availability group

ACL : access control list

AD : Active Directory

AKS : Azure Kubernetes Service

API : application programming interface

ARM : Azure Resource Manager

AVS : Azure VMware Solution

AWS : Amazon Web Services

AZ : availability zone

B

BBB : block-based backup

C

CA : certificate authority

CBT : Changed Block Tracking

CDC : change data capture

CIFS : Common Internet File System

CLI : command-line interface

CLR : Common Language Runtime

CN : common name

CPU : central processing unit

CRD : custom resource definition

CR : custom resource

CSI : container storage interface

CSV : Cluster Shared Volume

D

DAG : database availability group

DBA : database administrator

DBID : database identifier

DDMC : DD Management Center

DDOS : DD Operating System

DDVE : DD Virtual Edition

DFC : DD Boost over Fibre Channel

DNS : Domain Name System

DPC : Data Protection Central

DRS : Distributed Resource Scheduler

DR : disaster recovery

DSA : Dell security advisory

E

EBS : Elastic Block Store

EC2 : Elastic Compute Cloud

eCDM : Enterprise Copy Data Management

ECS : Elastic Cloud Storage

EFI : Extensible Firmware Interface

EKS : Elastic Kubernetes Service

ENI : Elastic Network Interface

EULA : end-user license agreement

F

FCD : first class disk

FCI : failover cluster instance

FC : Fibre Channel

FETB : front-end protected capacity by terabyte

FLR : file-level restore

FQDN：fully qualified domain name

FTP：File Transfer Protocol

G

Gb/s：gigabits per second
Dell では、2^{30} ビット/秒です。

GB：ギガバイト
Dell では、2^{30} バイトです。

GCP：Google Cloud Platform

GCVE：Google Cloud Virtual Edition

GID：group identifier

GLR：granular-level restore

GUID：globally unique identifier

GUI：graphical user interface

H

HANA：high-performance analytic appliance

HA：High Availability

HTML：Hypertext Markup Language

HTTPS：Hypertext Transfer Protocol Secure

HTTP：Hypertext Transfer Protocol

I

IAM：identity and access management

IDE：Integrated Device Electronics

IPv4：Internet Protocol version 4

IPv6：Internet Protocol version 6

IP：Internet Protocol

K

KB：kilobyte
Dell では、2^{10} バイトです。

L

LAC：License Authorization Code

LAN： local area network

M

MB： megabyte
Dell では、2^{20} バイトです。

ms： millisecond

MTU： maximum transmission unit

N

NAS： network-attached storage

NBDSSL： network block device over SSL

NBD： network block device

NDMP： Network Data Management Protocol

NFC： Network File Copy

NFS： Network File System

NIC： network interface card

NTFS： New Technology File System

NTP： Network Time Protocol

O

OSS： open-source software

OS： operating system

OVA： Open Virtualization Appliance

P

PCS： Protection Copy Set

PDF： Portable Document Format

PEM： Privacy-enhanced Electronic Mail

PIN： personal identification number

PIT： point in time

PKCS： Public Key Cryptography Standards

PSC： Platform Service Controller

PVC (Kubernetes)： Persistent Volume Claim

PVC（クラウド コンピューティング）： private virtual cloud

R

RAC： Real Application Cluster

RAM： random-access memory

RBAC： role-based access control

ReFS： Resilient File System

REST API： representational-state transfer API

RHEL： RedHat Enterprise Linux

RMAN： Recovery Manager

RPO： recovery-point objective

RSA： Rivest-Shamir-Adleman

S

S3： Simple Storage Services

SaaS： software as a service

SAP： System Analysis Program Development
SAP の Web サイト（2022 年）より：「この会社名は、当社の最初のドイツ語名である Systemanalyse Programmentwicklung（英語名：System Analysis Program Development）の頭字語です。現在、当社の法律上の会社名は SAP SE です。SE は、societas Europaea の略で、欧州連合の会社法に従って登録された公開会社です。」

SCSI： Small Computer System Interface

SDDC： software-defined data center

SELinux： Security-Enhanced Linux

SFTP： Secure File Transfer Protocol

SLA： service-level agreement

SLES： SuSE Linux Enterprise Server

SLO： service-level objective

SPBM： Storage Policy Based Management

SQL： Structured Query Language

SRS： Secure Remote Services

SSD：ソリッドステート ドライブ

SSH： Secure Shell

SSL： Secure Sockets Layer

SSMS： SQL Server Management Studio

SSV： System Stable Values

T

TB：terabyte
Dell では、2^{40} バイトです。

TCP：Transmission Control Protocol

TDE：Transparent Data Encryption

TLS：Transport Layer Security

TPM：Trusted Platform Module

TSDM：Transparent Snapshots Data Mover

T-SQL：Transact-SQL

U

UAC：user account control

UDP：User Datagram Protocol

UID：user identifier

UI：user interface

update
Dell では、ソフトウェアは `updated` するもので、ハードウェアは `upgraded` するものです。このソフトウェア ガイドで `upgrade` を検索し、見つからない場合は、代わりに `update` を検索してください。

UTC：Coordinated Universal Time
Wikipedia（2022 年）より：「この略語は、国際電気通信連合と国際天文学連合がすべての言語で同じ略語を使用したいと考えた結果、作成されました。英語を話す人は当初、CUT（「協定世界時間」）を提案し、フランス語を話す人は TUC（「Temps Universel Coordonné」）を提案しました」

V

VADP：VMware vStorage API for Data Protection

VBS：virtualization-based security

VCF：VMware Cloud Foundation

vCLS：vSphere Cluster Service

vCSA：vCenter Server Appliance

VCSA：vCenter Server Appliance

vDisk：virtual disk

VDI：Virtual Device Interface

vDS：virtual distributed switch

vFRC：Virtual Flash Read Cache

VGT：Virtual Guest Tagging

VIB : vSphere Installation Bundle

VLAN : virtual LAN

VMC : VMware Cloud

VMDK : virtual machine disk

VM : virtual machine

VNet : virtual network

VPC : virtual private cloud

vRSLCM : vRealize Suite Lifecycle Manager

VST : Virtual Switch Tagging

vTPM : Virtual Trusted Platform Module

VVD : VMware Validated Design

vVol : virtual volume

W

WAN : wide area network