SnapCenter ソフトウェアのドキュメント

SnapCenter Software 4.8

NetApp
January 18, 2024

目次

SnapCenter ソフトウェアのドキュメント

リリースノート

このリリースの SnapCenter サーバおよび SnapCenter プラグインパッケージに関する重要な情報を提供します。これには、解決済みの問題、既知の問題、注意事項、および制限事項が含まれます。

詳細については、を参照してください "SnapCenterソフトウェア4.8リリースノート"。

概念

SnapCenter の概要

SnapCenter ソフトウェアは、シンプルで拡張性に優れた一元的なプラットフォームです。ハイブリッドクラウド内の任意の場所にある ONTAP システムで実行されているアプリケーション、データベース、ホストファイルシステム、 VM に対して、アプリケーションと整合性のあるデータ保護を提供します。

SnapCenter では、ネットアップの Snapshot 、 SnapRestore 、 FlexClone 、 SnapMirror 、および SnapVault テクノロジを活用して、次の機能を提供します。

- アプリケーションと整合性のある、高速でスペース効率に優れたディスクベースのバックアップ
- 迅速できめ細かなリストアと、アプリケーションと整合性のあるリカバリを実現
- スペース効率に優れた高速クローニング

SnapCenter には、 SnapCenter サーバと個々の軽量プラグインの両方が含まれています。リモートアプリケーションホストへのプラグインの導入を自動化したり、バックアップ、検証、クローニングの処理をスケジュールしたり、すべてのデータ保護処理を監視したりできます。

SnapCenter は、次の方法で導入できます。

- オンプレミスで保護：
  - ONTAP FAS または AFF のプライマリシステム上にあり、 ONTAP FAS または AFF のセカンダリシステムにレプリケートされるデータ
  - ONTAP Select プライマリシステム上のデータ
  - ONTAP FAS またはAFF プライマリ/セカンダリシステム上にあり、ローカルStorageGRID オブジェクトストレージに保護されているデータ（ネットアップのBlueXPクラウドバックアップ統合を使用）
- ハイブリッドクラウドのオンプレミスで以下を保護：
  - ONTAP FAS またはAFF プライマリシステム上にあり、Cloud Volumes ONTAP にレプリケートされるデータ
  - ONTAP FAS またはAFF のプライマリシステムとセカンダリシステム上にあり、クラウド上のオブジェクトストレージとアーカイブストレージに保護されているデータ（NetApp BlueXP Cloud Backup統合を使用）
- パブリッククラウドで次のデータを保護：
  - Cloud Volumes ONTAP （旧 ONTAP Cloud ）プライマリシステム上のデータ
  - Amazon FSX for ONTAP 上にあるデータ

SnapCenter の主な機能は次のとおりです。

- アプリケーションと整合性のある一元的なデータ保護

  データ保護は、 ONTAP システムで実行されている Microsoft Exchange Server 、 Microsoft SQL Server 、 Linux または AIX 上の Oracle データベース、 SAP HANA データベース、および Windows ホストファ

イルシステムでサポートされます。

ユーザ定義の SnapCenter プラグインを作成するためのフレームワークを提供することで、他の標準またはカスタムのアプリケーションやデータベースでもデータ保護がサポートされます。これにより、 1 つの画面で他のアプリケーションやデータベースのデータを保護することができます。このフレームワークを活用して、ネットアップは IBM DB2 、 MongoDB 、 MySQL など用の SnapCenter カスタムプラグインを NetApp Automation Store でリリースしました。

"NetApp Storage Automation Store の略"

- ポリシーベースのバックアップ

  ポリシーベースのバックアップでは、 NetApp Snapshot コピーテクノロジを利用して、アプリケーションと整合性のある高速なディスクベースのバックアップを、スペース効率に優れた方法で作成します。必要に応じて、既存の保護関係を更新することで、セカンダリストレージに対するこれらのバックアップの保護を自動化することができます。

- 複数のリソースのバックアップ

  SnapCenter リソースグループを使用して、同じタイプの複数のリソース（アプリケーション、データベース、またはホストファイルシステム）を同時にバックアップできます。

- リストアとリカバリ

  SnapCenter を使用すると、バックアップとアプリケーションと整合性のある、時間ベースのリカバリを迅速かつきめ細かくリストアできます。ハイブリッドクラウドの任意のデスティネーションからリストアできます。

- クローニング

  SnapCenter は、スペース効率に優れた、アプリケーションと整合性のある高速クローニングを実現し、ソフトウェア開発期間を短縮します。ハイブリッドクラウドの任意のデスティネーションにクローニングできます。

- 単一のユーザ管理グラフィカルユーザインターフェイス（ GUI ）

  SnapCenter GUI では、ハイブリッドクラウドの任意のデスティネーションにあるリソースのバックアップとクローンを管理するための単一の停止インターフェイスが提供されます。

- REST API 、 Windows コマンドレット、 UNIX コマンド

  SnapCenter には、ほとんどの機能をオーケストレーションソフトウェアと統合するための REST API 、および Windows PowerShell コマンドレットとコマンドラインインターフェイスが含まれています。

  REST APIの詳細については、を参照してください "REST APIの概要"。

  Windowsコマンドレットの詳細については、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

  UNIXコマンドの詳細については、を参照してください "SnapCenter ソフトウェアコマンドリファレンスガイド"。

- 一元化されたデータ保護ダッシュボードとレポート作成

- セキュリティと委譲のためのロールベースアクセス制御（ RBAC ）。
- 高可用性を備えたリポジトリデータベース

  SnapCenter には、すべてのバックアップメタデータを格納するための高可用性機能を備えたリポジトリデータベースが組み込まれています。

- プラグインの自動プッシュインストール

  SnapCenter サーバホストからアプリケーションホストへの SnapCenter プラグインのリモートプッシュを自動化できます。

- 高可用性

  SnapCenter のハイアベイラビリティは、外部ロードバランサ（ F5 ）を使用して設定されています。同じデータセンター内で最大 2 つのノードがサポートされます。

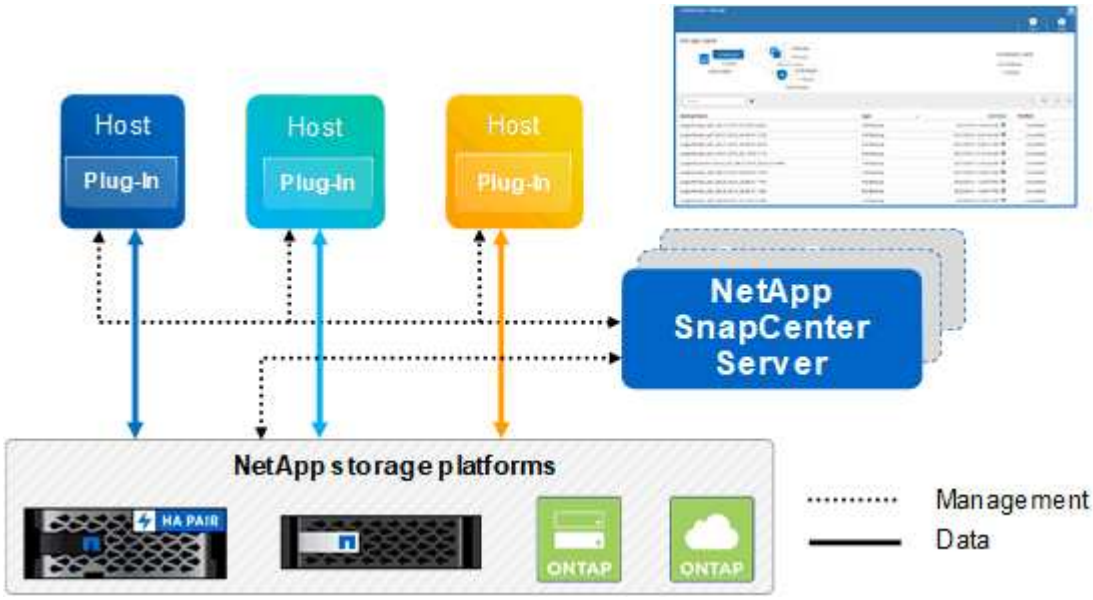
- ディザスタリカバリ（ DR ）

  リソースの破損やサーバのクラッシュなどの災害が発生した場合に SnapCenter サーバをリカバリできます。

SnapCenter アーキテクチャ

SnapCenter プラットフォームは、集中管理サーバー（ SnapCenter サーバー）と SnapCenter プラグインホストを含む多層アーキテクチャに基づいています。

SnapCenter はマルチサイトデータセンターをサポートしている。SnapCenter サーバとプラグインホストは、地理的に離れた場所に配置することもできます。



SnapCenter コンポーネント

SnapCenter は、 SnapCenter Server と SnapCenter プラグインで構成されています。インストールするプラグインは、保護するデータに適したプラグインだけにしてください。

- SnapCenter サーバ
- SnapCenter Plug-ins Package for Windows には次のプラグインが含まれています。
  - SnapCenter Plug-in for Microsoft SQL Server
  - SnapCenter Plug-in for Microsoft Windows の略
  - SnapCenter Plug-in for Microsoft Exchange Server の略
  - SAP HANA データベース向け SnapCenter プラグイン
- SnapCenter Plug-ins Package for Linux 。 Linux には次のプラグインが含まれています。
  - SnapCenter Plug-in for Oracle Database
  - SAP HANA データベース向け SnapCenter プラグイン
  - SnapCenter Plug-in for UNIX の略

  SnapCenter Plug-in for UNIX はスタンドアロンのプラグインではなく、個別にインストールすることはできません。このプラグインは、 SnapCenter Plug-in for Oracle Database または SnapCenter Plug-in for SAP HANA Database のインストール時に自動的にインストールされます。
- SnapCenter Plug-ins Package for AIX ：以下のプラグインが含まれています。
  - SnapCenter Plug-in for Oracle Database
  - SnapCenter Plug-in for UNIX の略

  SnapCenter Plug-in for UNIX はスタンドアロンのプラグインではなく、個別にインストールすることはできません。このプラグインは、 SnapCenter Plug-in for Oracle Database のインストール時に自動的にインストールされます。
- SnapCenter カスタムプラグイン

  カスタムプラグインはコミュニティでサポートされており、からダウンロードできます "NetApp Storage Automation Store の略"。

SnapCenter Plug-in for VMware vSphere は、ネットアップのデータブローカーです。仮想化されたデータベースやファイルシステムに対する SnapCenter のデータ保護処理をサポートする、スタンドアロンの仮想アプライアンスです。

SnapCenter サーバ

SnapCenter サーバには、 Web サーバ、一元化された HTML5 ベースのユーザインターフェイス、 PowerShell コマンドレット、 REST API 、および SnapCenter リポジトリが含まれています。

SnapCenter を使用すると、単一のユーザインターフェイスで複数の SnapCenter サーバ間の高可用性とスケールアウトを実現できます。外部ロードバランサ（ F5 ）を使用して高可用性を実現できます。数千台ものホストで構成される大規模な環境では、複数の SnapCenter Server を追加して負荷を分散すると便利です。

- SnapCenter Plug-ins Package for Windows を使用している場合、ホストエージェントは SnapCenter サーバおよび Windows プラグインホストで実行されます。ホストエージェントは、リモート Windows ホストまたは Microsoft SQL Server でスケジュールをネイティブに実行します。スケジュールはローカル SQL インスタンスで実行されます。

SnapCenter サーバは、ホストエージェントを介して Windows プラグインと通信します。

- SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX を使用している場合、 SnapCenter サーバでスケジュールが Windows タスクスケジュールとして実行されます。
  - SnapCenter Plug-in for Oracle Database の場合、 SnapCenter サーバホストで実行されるホストエージェントは、 Linux ホストまたは AIX ホストで実行される SnapCenter Plug-in Loader （ SPL ）と通信して、異なるデータ保護処理を実行します。
  - SnapCenter Plug-in for SAP HANA Database および SnapCenter Custom Plug-ins の場合、 SnapCenter サーバはホストで実行されている SCCore エージェントを通じてこれらのプラグインと通信します。

SnapCenter サーバとプラグインは、 HTTPS を使用してホストエージェントと通信します。

SnapCenter 処理に関する情報は、 SnapCenter リポジトリに保存されます。

SnapCenter プラグイン

各 SnapCenter プラグインは、特定の環境、データベース、およびアプリケーションをサポートしています。

プラグイン名	インストールパッケージに含まれています	他のプラグインが必要です	ホストにインストール済みである	サポートされているプラットフォーム
Plug-in for SQL Server のこと	Windows 用プラグインパッケージ	Plug-in for Windows のこと	SQL Server ホスト	Windows の場合
Plug-in for Windows のこと	Windows 用プラグインパッケージ		Windows ホスト	Windows の場合
Plug-in for Exchange の略	Windows 用プラグインパッケージ	Plug-in for Windows のこと	Exchange Server ホスト	Windows の場合
Plug-in for Oracle Database の略	Linux 用プラグインパッケージおよび AIX 用プラグインパッケージ	Plug-in for UNIX のこと	Oracle ホスト	Linux または AIX
Plug-in for SAP HANA Database の略	Plug-in Package for Linux and Plug-ins Package for Windows	Plug-in for UNIX or Plug-in for Windows のいずれかです	HDBSQL クライアントホスト	Linux または Windows
カスタムプラグイン	"NetApp Storage Automation Store の略"	ファイルシステムのバックアップについては、 Plug-in for Windows を参照してください	カスタムアプリケーションホスト	Linux または Windows

SnapCenter Plug-in for VMware vSphere は、仮想マシン（ VM ）、データストア、および仮想マシンディスク（ VMDK ）に対して crash-consistent で VM と整合性のあるバックアップおよびリストア処理をサポートし、 SnapCenter アプリケーション固有のプラグインをサポートして、仮想化されたデータベースおよびファイルシステムに対してアプリケーションと整合性のあるバックアップおよびリストア処理を保護します。

SnapCenter 4.1.1 ユーザの場合、 SnapCenter Plug-in for VMware vSphere 4.1.1 のドキュメントには、仮想化されたデータベースとファイルシステムの保護に関する情報が記載されています。SnapCenter 4.2.x ユーザの場合、 NetApp Data Broker 1.0 および 1.0.1 のドキュメントでは、 Linux ベースの NetApp Data Broker 仮想アプライアンス（オープン仮想アプライアンス形式）が提供する SnapCenter Plug-in for VMware vSphere を使用して、仮想化されたデータベースとファイルシステムを保護する方法について説明しています。SnapCenter 4.3 以降を使用しているユーザの場合は、を参照してください "SnapCenter Plug-in for VMware vSphere のドキュメント" Linux ベースの SnapCenter Plug-in for VMware vSphere 仮想アプライアンス（ Open Virtual Appliance 形式）を使用した、仮想化されたデータベースとファイルシステムの保護に関する情報を提供します。

SnapCenter Plug-in for Microsoft SQL Server の特長

- SnapCenter 環境で、アプリケーションに対応したバックアップ、リストア、およびクローニングの処理を自動化します。
- SnapCenter Plug-in for VMware vSphere を導入して SnapCenter に登録すると、 VMDK および raw デバイスマッピング（ RDM ） LUN 上の Microsoft SQL Server データベースがサポートされます
- SMB 共有のプロビジョニングのみをサポートします。SMB 共有での SQL Server データベースのバックアップはサポートされていません。
- SnapManager for Microsoft SQL Server から SnapCenter へのバックアップのインポートをサポートします。

SnapCenter Plug-in for Microsoft Windows の特長

- SnapCenter 環境の Windows ホストで実行されている他のプラグインに対して、アプリケーション対応のデータ保護を有効にします
- SnapCenter 環境で、アプリケーションに対応したバックアップ、リストア、およびクローニングの処理を自動化します
- Windows ホストのストレージのプロビジョニング、整合性のある Snapshot コピーの作成、およびスペースの再生をサポートします

Plug-in for Windows では、 SMB 共有および Windows ファイルシステムを物理 RDM LUN 上にプロビジョニングしますが、 SMB 共有上での Windows ファイルシステムのバックアップ処理はサポートされません。

SnapCenter Plug-in for Microsoft Exchange Server の特長

- SnapCenter 環境での Microsoft Exchange Server データベースおよび Database Availability Group （ DAG ；データベース可用性グループ）で、アプリケーションに対応したバックアップおよびリストア処理を自動化します
- は、 SnapCenter Plug-in for VMware vSphere を導入して SnapCenter に登録する際に、 RDM LUN 上の仮想 Exchange Server をサポートします

SnapCenter Plug-in for Oracle Database の特長

- アプリケーションに対応したバックアップ、リストア、リカバリ、検証、マウント、 SnapCenter 環境での Oracle データベースのアンマウントおよびクローニング処理
- SAP 対応の Oracle データベースをサポートしますが、 SAP BR * Tools との統合は提供されません

SnapCenter Plug-in for UNIX の特長

- Plug-in for Oracle Database で、 Linux または AIX システム上の基盤となるホストストレージスタックを処理することで、 Oracle データベースに対するデータ保護処理を実行できます
- ONTAP を実行するストレージシステムで、 Network File System （ NFS ；ネットワークファイルシステム）プロトコルおよび Storage Area Network （ SAN ；ストレージエリアネットワーク）プロトコルをサポートします。
- Linux システムの場合、 VMDK および RDM LUN 上の Oracle データベースは、 SnapCenter Plug-in for VMware vSphere を導入して SnapCenter に登録するとサポートされます。
- SAN ファイルシステムおよび LVM レイアウトで AIX 用のマウントガードをサポートします。
- SAN ファイルシステムのインラインロギングと AIX システムの LVM レイアウトでのみ、 Enhanced Journaled File System （ JFS2 ）をサポートします。

  SAN デバイス上に構築された SAN ネイティブデバイス、ファイルシステム、 LVM のレイアウトがサポートされます。

SnapCenter Plug-in for SAP HANA Database の特長

- SnapCenter 環境で、アプリケーションに対応した SAP HANA データベースのバックアップ、リストア、クローニングを自動化します

SnapCenter Custom Plug-ins の特長

- は、他の SnapCenter プラグインでサポートされていないアプリケーションやデータベースを管理するためのカスタムプラグインをサポートしています。カスタムプラグインは、 SnapCenter のインストールには含まれていません。
- では、別のボリュームにバックアップセットのミラーコピーを作成し、ディスクツーディスクのバックアップレプリケーションを実行できます。
- Windows 環境と Linux 環境の両方をサポートします。Windows 環境では、カスタムプラグインに SnapCenter Plug-in for Microsoft Windows を組み合わせて使用することで、ファイルシステムの整合性のあるバックアップを作成することができます。

SnapCenter ソフトウェア用の MySQL 、 DB2 、 MongoDB カスタムプラグインのサンプルは、からダウンロードできます "NetApp Storage Automation Store の略"。

MySQL 、 DB2 、 MongoDB のカスタムプラグインは、ネットアップのコミュニティでのみサポートされます。

ネットアップでは、カスタムプラグインの作成と使用をサポートしていますが、作成したカスタムプラグインはネットアップではサポートしていません。

詳細については、を参照してください "アプリケーション用のプラグインを開発します"

SnapCenter リポジトリ

SnapCenter リポジトリは NSM データベースとも呼ばれ、 SnapCenter のすべての処理の情報とメタデータを格納します。

MySQL Server リポジトリデータベースは、 SnapCenter Server のインストール時にデフォルトでインストールされます。MySQL Server がすでにインストールされていて、 SnapCenter Server を新規にインストールする場合は、 MySQL Server をアンインストールする必要があります。

SnapCenter では、 SnapCenter リポジトリデータベースとして MySQL Server 5.7.25 以降をサポートしています。以前のリリースの SnapCenter を搭載した以前のバージョンの MySQL Server を使用していた場合、 SnapCenter のアップグレード中に MySQL Server が 5.7.25 以降にアップグレードされます。

SnapCenter リポジトリには、次の情報とメタデータが格納されます。

- バックアップ、クローニング、リストア、検証の各メタデータ
- レポート作成、ジョブ、イベントの情報
- ホストおよびプラグインの情報
- ロール、ユーザ、および権限の詳細
- ストレージシステムの接続情報

セキュリティ機能

SnapCenter では、データのセキュリティを確保するために厳格なセキュリティおよび認証機能を採用しています。

SnapCenter には、次のセキュリティ機能が含まれています。

- SnapCenter へのすべての通信には、 HTTP over SSL （ HTTPS ）が使用されます。
- SnapCenter のすべてのクレデンシャルは、 Advanced Encryption Standard （ AES ）暗号化を使用して保護されます。
- SnapCenter で使用しているセキュリティアルゴリズムは、 Federal Information Processing Standard （ FIPS ；連邦情報処理標準）に準拠しています。
- SnapCenter では、お客様から提供された承認済みの CA 証明書の使用がサポートされます。
- SnapCenter 4.1.1 以降では、 ONTAP との Transport Layer Security （ TLS ） 1.2 通信がサポートされています。クライアントとサーバの間の通信にも TLS 1.2 を使用できます。
- SnapCenter は、一連のSSL暗号スイートをサポートしており、ネットワーク通信全体のセキュリティを提供します。

  詳細については、を参照してください "サポートされているSSL暗号スイートを設定する方法"。

- SnapCenter は、会社のファイアウォールの内側にインストールされ、 SnapCenter サーバへのアクセス、および SnapCenter サーバとプラグイン間の通信を可能にします。
- SnapCenter API および操作アクセスでは、 AES 暗号化で暗号化されたトークンが使用されます。このトークンの有効期限は 24 時間です。
- SnapCenter は、ログイン用に Windows Active Directory と統合されているほか、アクセス権限を制御す

るロールベースアクセス制御（ RBAC ）も統合されています。

- IPSecは、WindowsおよびLinuxホスト・マシン用のONTAP 上のSnapCenter でサポートされます。 "詳細はこちら。"。
- SnapCenter PowerShell コマンドレットセッションはセキュリティで保護されます。
- デフォルトでは、操作を行わないまま 15 分が経過すると、 5 分後に SnapCenter からログアウトすることを示す警告が表示されます。操作を行わないまま 20 分が経過すると、 SnapCenter からログアウトされ、再度ログインする必要があります。ログアウト期間を変更できます。
- ログインに 5 回以上失敗すると、一時的にログインが無効になります。
- SnapCenter サーバとONTAP 間のCA証明書認証をサポートします。 "詳細はこちら。"。
- SnapCenter サーバとプラグインに整合性検証機能が追加され、新規インストールおよびアップグレード処理中に出荷されたすべてのバイナリが検証されます。

CA 証明書の概要

SnapCenter サーバーインストーラを使用すると、インストール中に集中型 SSL 証明書サポートを有効にできます。サーバとプラグイン間のセキュアな通信を強化するために、 SnapCenter では、お客様から提供された許可済み CA 証明書の使用をサポートしています。

SnapCenterサーバとそれぞれのプラグインをインストールしたあとに、CA証明書を導入する必要があります。
詳細については、を参照してください "CA 証明書 CSR ファイルを生成します"。

また、 SnapCenter Plug-in for VMware vSphere の CA 証明書を導入することもできます。詳細については、を参照してください "証明書を作成してインポートします"。

多要素認証（ MFA ）

MFAでは、Security Assertion Markup Language（SAML）を使用してサードパーティのアイデンティティプロバイダ（IdP）を使用してユーザセッションを管理します。この機能は、TOTP、生体認証、プッシュ通知などの複数の要素を既存のユーザ名とパスワードとともに使用するオプションを備えているため、認証セキュリティが強化されます。また、お客様は独自のユーザアイデンティティプロバイダを使用して、ポートフォリオ全体でユニファイドユーザログイン（SSO）を取得できます。

MFAは、SnapCenter サーバUIへのログインにのみ適用されます。 ログインは、IdPのActive Directoryフェデレーションサービス（AD FS）を使用して認証されます。 AD FSでは、さまざまな認証要素を構成できます。SnapCenter はサービスプロバイダであり、AD FSの証明書利用者としてSnapCenter を設定する必要があります。SnapCenter でMFAを有効にするには、AD FSメタデータが必要です。

MFAを有効にする方法については、を参照してください "多要素認証を有効にします"。

SnapCenter の RBAC

RBAC のタイプ

SnapCenter のロールベースアクセス制御（ RBAC ）と ONTAP 権限を使用して、SnapCenter 管理者は SnapCenter リソースの制御を別のユーザまたはユーザのグループに委譲できます。この方法でアクセスを一元管理することで、アプリケーション管理者

は委譲された環境で安全に作業することができ

ロールの作成と変更、ユーザへのリソースアクセスの追加はいつでも実行できますが、 SnapCenter を初めて設定するときは、少なくとも Active Directory ユーザまたはグループをロールに追加してから、そのユーザまたはグループにリソースアクセスを追加する必要があります。

SnapCenter を使用してユーザアカウントまたはグループアカウントを作成することはできません。ユーザアカウントまたはグループアカウントは、オペレーティングシステムまたはデータベースの Active Directory に作成する必要があります。

SnapCenter では、次のタイプのロールベースアクセス制御を使用します。

- SnapCenter RBAC
- SnapCenter プラグインの RBAC （一部のプラグイン）
- アプリケーションレベルの RBAC
- ONTAP 権限

SnapCenter RBAC

ロールと権限

SnapCenter には、権限がすでに割り当てられている事前定義されたロールが付属してこれらのロールにユーザまたはユーザのグループを割り当てることができます。また、新しいロールを作成して権限とユーザを管理することもできます。

- ユーザーまたはグループへのアクセス権の割り当て *

ユーザまたはグループに権限を割り当てて、ホスト、ストレージ接続、リソースグループなどの SnapCenter オブジェクトにアクセスすることができます。SnapCenterAdmin ロールの権限は変更できません。

RBAC の権限は、同じフォレスト内のユーザとグループ、および別のフォレストに属しているユーザに割り当てることができます。フォレストにまたがってネストされたグループに属するユーザには、 RBAC の権限を割り当てることはできません。

カスタムロールを作成する場合は、 SnapCenter Admin ロールのすべての権限を含める必要があります。「 Host add 」や「 Host remove 」など、一部の権限しかコピーしなかった場合、それらの処理を実行することはできません。

認証

ユーザは、グラフィカルユーザインターフェイス（ GUI ）または PowerShell コマンドレットを使用して、ログイン時に認証情報を指定する必要があります。ユーザが複数のロールに属している場合は、ログインクレデンシャルの入力後に、使用するロールを指定するように求められます。また、 API を実行する際にも認証が必要になります。

アプリケーションレベルの **RBAC**

SnapCenter では、クレデンシャルを使用して、許可された SnapCenter ユーザにアプリケーションレベルの権限もあるかどうかが検証されます

たとえば、 SQL Server 環境で Snapshot コピーやデータ保護の処理を実行する場合は、 Windows または SQL の適切なクレデンシャルを設定する必要があります。SnapCenter サーバは、どちらの方法で設定されたクレデンシャルも認証します。ONTAP ストレージ上の Windows ファイルシステム環境で Snapshot コピーやデータ保護の処理を実行する場合は、 SnapCenter の admin ロールに Windows ホストに対する管理者権限が必要です。

同様に、 Oracle データベースに対してデータ保護処理を実行する場合、データベースホストでオペレーティングシステム（ OS ）認証が無効なときは、 Oracle データベースまたは Oracle ASM のクレデンシャルを使用してクレデンシャルを設定する必要があります。SnapCenter サーバは、処理に応じて、いずれかの方法で設定されたクレデンシャルを認証します。

SnapCenter Plug-in for VMware vSphere の RBAC をサポートしています

VM と整合性のあるデータ保護に SnapCenter VMware プラグインを使用している場合、 vCenter Server によってさらに細かく RBAC を実装できます。SnapCenter VMware プラグインは、 vCenter Server RBAC と Data ONTAP RBAC の両方をサポートしています。

詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere の RBAC をサポートしています"

ONTAP 権限

ストレージシステムにアクセスするには、必要な権限を持つ vsadmin アカウントを作成する必要があります。

アカウントの作成と権限の割り当てについては、を参照してください "最小限の権限で ONTAP クラスタロールを作成します"

RBAC の権限とロール

SnapCenter のロールベースアクセス制御（ RBAC ）では、ロールを作成して権限を割り当てることができ、そのロールにユーザやそのグループを割り当てることができます。これにより、 SnapCenter 管理者は環境を一元的に管理しながら、アプリケーション管理者はデータ保護ジョブを管理できます。SnapCenter には、事前定義されたロールと権限がいくつか付属してい

SnapCenter ロール

SnapCenter には、次のロールがあらかじめ定義されています。これらのロールにユーザやグループを割り当てて使用できるほか、新しいロールを作成することもできます。

ロールをユーザに割り当てると、 SnapCenter Admin ロールを割り当てていない限り、そのユーザに関連するジョブだけが Jobs ページに表示されます。

- App Backup and Clone Admin の登録を確認します
- Backup and Clone Viewer に表示されます
- インフラ管理者
- SnapCenter Admin

SnapCenter Plug-in for VMware vSphere のロール

VM 、 VMDK 、およびデータストアの VM 整合性のあるデータ保護を管理するために、 SnapCenter Plug-in for VMware vSphere によって vCenter で次のロールが作成されます。

- SCV 管理者
- SCV ビュー
- SCV バックアップ
- SCV Restore （ SCV リストア）
- SCV ゲストファイルのリストア

詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere ユーザ用の RBAC のタイプ"

* ベストプラクティス： * SnapCenter Plug-in for VMware vSphere の処理用に ONTAP ロールを 1 つ作成し、必要な権限をすべて割り当てることを推奨します。

SnapCenter 権限

SnapCenter から提供される権限は次のとおりです。

- リソースグループ
- ポリシー
- バックアップ
- ホスト
- ストレージ接続
- クローン
- Provision （ Microsoft SQL データベースのみ）
- ダッシュボード
- レポート
- リストア
  - Full Volume Restore （ Custom Plug-ins のみ）
- リソース

  管理者以外のユーザがリソース検出処理を実行する場合、管理者からプラグインの権限が求められます。

- プラグインのインストールまたはアンインストール

  Plug-in Installation 権限を有効にする場合は、 Host 権限も変更して読み取りと更新を有効にする必要があります。

- データ移行
- mount （ Oracle データベースのみ）

- Unmount （ Oracle データベースのみ）
- Job Monitor サービスの略

  ジョブ監視権限を使用すると、さまざまなロールのメンバーが、割り当てられているすべてのオブジェクトの処理を確認できます。

事前定義された **SnapCenter** ロールと権限

SnapCenter には、事前定義されたロールが用意されており、それぞれ一連の権限がすでに有効になっています。ロールベースアクセス制御（ RBAC ）をセットアップして管理するときは、これらの事前定義されたロールを使用するか、新しいロールを作成できます。

SnapCenter には、次の事前定義されたロールが含まれています。

- SnapCenter 管理者ロール
- App Backup and Clone Admin ロール
- Backup and Clone Viewer ロール
- Infrastructure Admin ロール

ロールにユーザを追加するときは、 Storage Connection 権限を割り当てて Storage Virtual Machine （ SVM ）の通信を有効にするか、 SVM をユーザに割り当ててその SVM を使用する権限を有効にする必要があります。Storage Connection 権限を割り当てられたユーザは SVM 接続を作成できます。

たとえば、 SnapCenter Admin ロールのユーザは、 SVM 接続を作成し、 App Backup and Clone Admin ロールのユーザに割り当てることができます。 App Backup and Clone Admin ロールには、デフォルトでは SVM 接続を作成または編集する権限は付与されていません。SVM 接続がないと、ユーザはバックアップ、クローニング、リストアの処理を実行できません。

SnapCenter 管理者ロール

SnapCenter Admin ロールでは、すべての権限が有効になっています。このロールの権限は変更できません。ロールにユーザやグループを追加したり削除したりできます。

App Backup and Clone Admin ロール

App Backup and Clone Admin ロールには、アプリケーションバックアップとクローン関連のタスクに対して管理操作を実行するために必要な権限が付与されています。このロールには、ホストの管理、プロビジョニング、ストレージ接続の管理、リモートインストールを行うための権限はありません。

権限	有効	作成	読み取り	更新	削除
リソースグループ	該当なし	はい。	はい。	はい。	はい。
ポリシー	該当なし	はい。	はい。	はい。	はい。

権限	有効	作成	読み取り	更新	削除
バックアップ	該当なし	はい。	はい。	はい。	はい。
ホスト	該当なし	はい。	はい。	はい。	はい。
ストレージ接続	該当なし	いいえ	はい。	いいえ	いいえ
クローン	該当なし	はい。	はい。	はい。	はい。
プロビジョニング	該当なし	いいえ	はい。	いいえ	いいえ
ダッシュボード	はい。	該当なし	該当なし	該当なし	該当なし
レポート	はい。	該当なし	該当なし	該当なし	該当なし
リストア	はい。	該当なし	該当なし	該当なし	該当なし
リソース	はい。	はい。	はい。	はい。	はい。
プラグインのインストールとアンインストール	いいえ	該当なし		該当なし	該当なし
データ移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウント	はい。	はい。	該当なし	該当なし	該当なし
アンマウント	はい。	はい。	該当なし	該当なし	該当なし
フルボリュームリストア	いいえ	いいえ	該当なし	該当なし	該当なし
Job Monitor サービスの略	はい。	該当なし	該当なし	該当なし	該当なし

Backup and Clone Viewer ロール

Backup and Clone Viewer ロールには、すべての権限の読み取り専用権限が付与されています。また、検出、レポート、およびダッシュボードへのアクセスに必要な権限も有効になっています。

権限	有効	作成	読み取り	更新	削除
リソースグループ	該当なし	いいえ	はい。	いいえ	いいえ
ポリシー	該当なし	いいえ	はい。	いいえ	いいえ
バックアップ	該当なし	いいえ	はい。	いいえ	いいえ
ホスト	該当なし	いいえ	はい。	いいえ	いいえ
ストレージ接続	該当なし	いいえ	はい。	いいえ	いいえ
クローン	該当なし	いいえ	はい。	いいえ	いいえ
プロビジョニング	該当なし	いいえ	はい。	いいえ	いいえ
ダッシュボード	はい。	該当なし	該当なし	該当なし	該当なし
レポート	はい。	該当なし	該当なし	該当なし	該当なし
リストア	いいえ	いいえ	該当なし	該当なし	該当なし
リソース	いいえ	いいえ	はい。	はい。	いいえ
プラグインのインストールとアンインストール	いいえ	該当なし	該当なし	該当なし	該当なし
データ移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウント	はい。	該当なし	該当なし	該当なし	該当なし
アンマウント	はい。	該当なし	該当なし	該当なし	該当なし
フルボリュームリストア	いいえ	該当なし	該当なし	該当なし	該当なし
Job Monitor サービスの略	はい。	該当なし	該当なし	該当なし	該当なし

Infrastructure Admin ロール

Infrastructure Admin ロールでは、ホストの管理、ストレージの管理、プロビジョニング、リソースグルー

プ、リモートインストールのレポートに対して権限が有効になっています。 ダッシュボードにアクセスします。

権限	有効	作成	読み取り	更新	削除
リソースグループ	該当なし	はい。	はい。	はい。	はい。
ポリシー	該当なし	いいえ	はい。	はい。	はい。
バックアップ	該当なし	はい。	はい。	はい。	はい。
ホスト	該当なし	はい。	はい。	はい。	はい。
ストレージ接続	該当なし	はい。	はい。	はい。	はい。
クローン	該当なし	いいえ	はい。	いいえ	いいえ
プロビジョニング	該当なし	はい。	はい。	はい。	はい。
ダッシュボード	はい。	該当なし	該当なし	該当なし	該当なし
レポート	はい。	該当なし	該当なし	該当なし	該当なし
リストア	はい。	該当なし	該当なし	該当なし	該当なし
リソース	はい。	はい。	はい。	はい。	はい。
プラグインのインストールとアンインストール	はい。	該当なし	該当なし	該当なし	該当なし
データ移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウント	いいえ	該当なし	該当なし	該当なし	該当なし
アンマウント	いいえ	該当なし	該当なし	該当なし	該当なし
フルボリュームリストア	いいえ	いいえ	該当なし	該当なし	該当なし
Job Monitor サービスの略	はい。	該当なし	該当なし	該当なし	該当なし

SnapCenter ディザスタリカバリ

SnapCenter ディザスタリカバリ（DR）機能を使用すると、リソースの破損やサーバのクラッシュなどの災害が発生した場合にSnapCenter サーバをリカバリできます。SnapCenter リポジトリ、サーバスケジュール、およびサーバ構成コンポーネントをリカバリできます。また、 SnapCenter Plug-in for SQL Server および SnapCenter Plug-in for SQL Server ストレージをリカバリすることもできます。

ここでは、SnapCenter での2種類のディザスタリカバリ（DR）について説明します。

SnapCenter サーバDR

- SnapCenter サーバのデータはバックアップされ、SnapCenter サーバにプラグインを追加したり、管理したりすることなくリカバリできます。
- セカンダリSnapCenter サーバは、プライマリSnapCenter サーバと同じインストールディレクトリと同じポートにインストールする必要があります。
- 多要素認証（MFA）の場合、SnapCenterサーバDR中にブラウザのすべてのタブを閉じ、ブラウザを再度開いて再度ログインします。これにより、既存またはアクティブなセッションCookieがクリアされ、正しい設定データが更新されます。
- SnapCenter のディザスタリカバリ機能では、 REST API を使用して SnapCenter サーバをバックアップします。を参照してください "SnapCenter サーバのディザスタリカバリ用の REST API のワークフロー"。
- 監査設定に関連する構成ファイルはDRバックアップにバックアップされず、リストア処理後にDRサーバにもバックアップされません。監査ログの設定を手動で繰り返す必要があります。

SnapCenter プラグインとストレージDR

DR は、 SnapCenter Plug-in for SQL Server でのみサポートされます。SnapCenter Plug-in for SQL Server がダウンしたときに、別の SQL ホストに切り替えてデータをリカバリする手順はいくつかあります。を参照してください "SnapCenter Plug-in for SQL Server のディザスタリカバリ"。

SnapCenter は、 ONTAP の SnapMirror テクノロジを使用してデータをレプリケートします。DR 用にセカンダリサイトにデータをレプリケートして同期し続けることができます。フェイルオーバーは、 SnapMirror のレプリケーション関係を解除することによって開始できます。フェイルバック中に、同期を反転させて DR サイトのデータをプライマリサイトにレプリケートすることができます。

リソース、リソースグループ、ポリシー

SnapCenter を使用する前に、実行するバックアップ、クローニング、およびリストアの処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- * リソース * は、通常、 SnapCenter でバックアップまたはクローンを作成するデータベース、 Windows ファイルシステム、またはファイル共有です。

  ただし、環境によっては、データベースインスタンス、 Microsoft SQL Server の可用性グループ、 Oracle データベース、 Oracle RAC データベース、 Windows ファイルシステム、カスタムアプリケーションのグループなどのリソースが該当します。

- * リソースグループ * は、ホストまたはクラスタ上のリソースの集まりです。リソースグループには、複数のホストおよび複数のクラスタのリソースを含めることもできます。

  リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているすべてのリソースに対してその処理が実行されます。

  単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一のリソースおよびリソースグループに対して設定することもできます。

  > 共有リソースグループの 1 つのホストをメンテナンスモードにし、同じ共有リソースグループに関連付けられているスケジュールがある場合は、共有リソースグループの他のすべてのホストに対してスケジュールされた処理がすべて中断されます。

  データベース、ファイルシステムのバックアップにはデータベースのプラグイン、 VM とデータストアのバックアップには SnapCenter Plug-in for VMware vSphere を使用します。

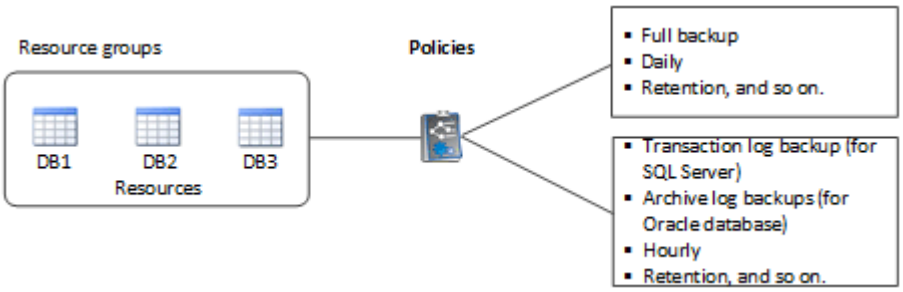
- * ポリシー * では、バックアップ頻度、コピーの保持、レプリケーション、スクリプトなど、データ保護処理の特性を指定します。

  リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。また、オンデマンドでバックアップを実行するときにポリシーを選択することもできます。

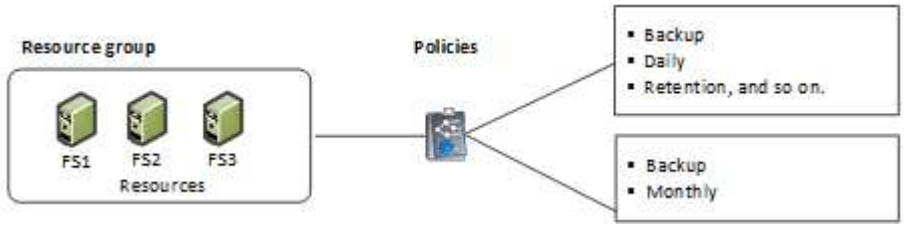
リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、すべてのデータベースをバックアップする場合や、ホストのすべてのファイルシステムをバックアップする場合は、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。

リソースグループを作成してポリシーを適用する際に、フルバックアップを 1 日 1 回実行するようにリソースグループを設定し、別のスケジュールでログバックアップを 1 時間おきに実行するように設定します。

次の図は、データベースのリソース、リソースグループ、およびポリシーの関係を示しています。



次の図は、 Windows ファイルシステムのリソース、リソースグループ、およびポリシーの関係を示しています。



プリスクリプトとポストスクリプト

カスタムのプリスクリプトとポストスクリプトをデータ保護処理の一部として使用することができます。これらのスクリプトにより、データ保護ジョブの前後の処理を自動化できます。たとえば、データ保護ジョブのエラーや警告を自動的に通知するスクリプトを組み込むことができます。プリスクリプトとポストスクリプトを設定する前に、スクリプトを作成するための要件を理解しておく必要があります。

サポートされているスクリプトタイプ

Windowsでは、次の種類のスクリプトがサポートされています。

- バッチファイル
- PowerShell スクリプト
- Perl スクリプト

UNIXでは、次のタイプのスクリプトがサポートされています。

- Perl スクリプト
- Pythonスクリプト
- シェルスクリプト

> デフォルトのbashシェルに加えて、sh-sshell、k-sshell、c-shellなどの他のシェルもサポートされています。

スクリプトパス

プラグインホストで、非仮想化ストレージシステムおよび仮想ストレージシステム上で SnapCenter 処理の一部として実行されるすべてのプリスクリプトとポストスクリプトが実行されます。

- Windowsスクリプトはプラグインホストに配置する必要があります。

> プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

- UNIXスクリプトはプラグインホストに配置する必要があります。

> スクリプトパスは実行時に検証されます。

スクリプトを指定する場所

スクリプトはバックアップポリシーに指定します。バックアップジョブが開始されると、ポリシーによってスクリプトがバックアップ対象のリソースに自動的に関連付けられます。バックアップポリシーを作成する際には、プリスクリプトとポストスクリプトの引数を指定できます。

複数のスクリプトを指定することはできません。

スクリプトのタイムアウト

デフォルトでは、タイムアウトは60秒に設定されています。タイムアウト値を変更できます。

スクリプトの出力

Windowsのプリスクリプトとポストスクリプトの出力ファイルのデフォルトディレクトリは、Windows\System32です。

UNIXのプリスクリプトとポストスクリプトには、デフォルトの場所はありません。出力ファイルは任意の場所にリダイレクトできます。

REST API を使用した SnapCenter の自動化

REST API を使用して、 SnapCenter のいくつかの管理操作を実行できます。REST API は Swagger Web ページから利用できます。REST API ドキュメントを表示する場合、および API 呼び出しを手動で問題する場合は、 Swagger Web ページにアクセスします。REST API を使用して、 SnapCenter サーバや SnapCenter vSphere ホストを管理できます。

対象の **REST API**	場所
SnapCenter サーバ	\https：//<SnapCenter_IP_address_or_name>：<SnapCenter_port>/swagger/
SnapCenter Plug-in for VMware vSphere	https://<OVA_IP_address_or_host_name>：<scv_plugin_port>/api/swagger -ui.html#

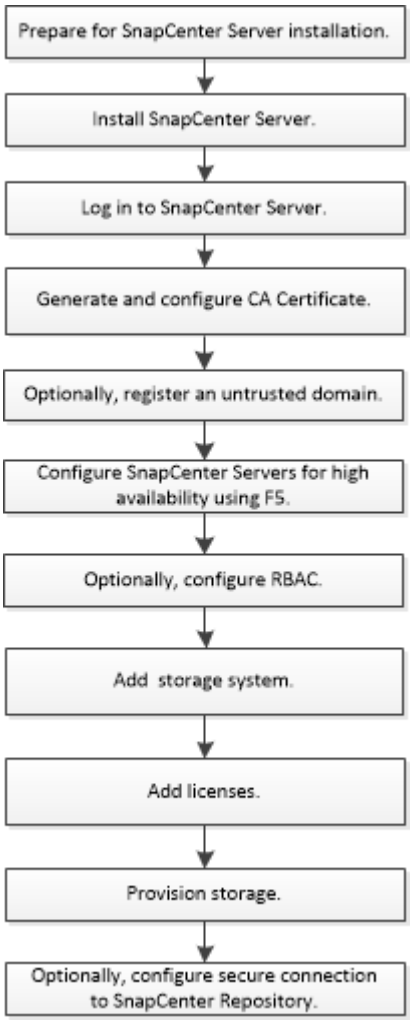
SnapCenter REST API については、を参照してください "REST API の概要"

SnapCenter Plug-in for VMware vSphere REST API については、を参照してください "SnapCenter Plug-in for VMware vSphere REST API"

SnapCenter サーバのインストール

インストールワークフロー

このワークフローでは、 SnapCenter サーバのインストールと設定に必要なさまざまなタスクについて説明します。



SnapCenter サーバをインストールする準備をします

ドメインとワークグループの要件

SnapCenter サーバは、ドメインまたはワークグループ内のシステムにインストールできます。インストールに使用するユーザには、ワークグループとドメインの両方の場合に、マシンに対する管理者権限が必要です。

Windows ホストに SnapCenter Server プラグインと SnapCenter プラグインをインストールするには、次のいずれかを使用する必要があります。

- * Active Directory ドメイン *

ローカル管理者の権限を持つドメインユーザを使用する必要があります。ドメインユーザは、 Windows ホストのローカル管理者グループのメンバーである必要があります。

- * ワークグループ *

  ローカル管理者の権限があるローカルアカウントを使用する必要があります。

ドメイントラスト、マルチドメインフォレスト、およびクロスドメイントラストはサポートされていますが、クロスフォレストドメインはサポートされません。詳細については、 Microsoft の Active Directory ドメインと信頼関係に関するドキュメントを参照してください。

SnapCenter サーバをインストールしたあとに、 SnapCenter ホストが配置されているドメインを変更しないでください。SnapCenter サーバをインストールした時点のドメインから SnapCenter サーバホストを削除して、 SnapCenter サーバをアンインストールしようとすると、アンインストール処理は失敗します。

スペースとサイジングの要件

SnapCenter サーバをインストールする前に、スペースとサイジングの要件を十分に理解しておく必要があります。また、利用可能なシステムおよびセキュリティの更新も適用する必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているのは、英語版、ドイツ語版、日本語版、簡体字中国語版のオペレーティングシステムのみです。 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
最小 CPU 数	4 コア
最小 RAM	8 GB MySQL Server のバッファプールでは、 RAM の合計の 20% が使用されます。
SnapCenter サーバソフトウェアおよびログ用のハードドライブの最小容量	4 GB SnapCenter サーバがインストールされているドライブに SnapCenter リポジトリがある場合は、 10GB にすることを推奨します。

項目	要件
SnapCenter リポジトリ用のハードドライブの最小容量	6 GB メモ： SnapCenter リポジトリがインストールされているドライブに SnapCenter サーバがある場合は、10GB にすることを推奨します。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 **NET**固有のトラブルシューティング情報については、を参照してください "インターネットに接続されていないレガシーシステムでは、**SnapCenter** のアップグレードまたはインストールが失敗します"。 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

SANホストの要件

SnapCenter ホストが FC / iSCSI 環境に配置されている場合、 ONTAP ストレージへのアクセスを有効にするために、システムに追加のソフトウェアのインストールが必要になることがあります。

SnapCenter には、 Host Utilities と DSM は含まれていません。SnapCenter ホストが SAN 環境に配置されている場合は、次のソフトウェアのインストールと設定が必要になることがあります。

- Host Utilities のことです

  Host Utilities は FC および iSCSI をサポートしており、 Windows サーバ上で MPIO を使用することができます。
  詳細については、を参照してください "Host Utilities のマニュアル"。

- Microsoft DSM for Windows MPIO

  このソフトウェアは Windows MPIO ドライバと連携して、ネットアップと Windows のホストコンピュータ間の複数のパスを管理します。

  ハイアベイラビリティ構成には DSM が必要です。

  ONTAP DSM を使用していた場合は、 Microsoft DSM に移行する必要があります。詳細については、を参照してください "ONTAP DSM から Microsoft DSM への移行方法"。

サポートされるストレージシステムおよびアプリケーション

サポートされるストレージシステム、アプリケーション、およびデータベースを確認しておく必要があります。

- SnapCenter では、データを保護するために ONTAP 8.3.0 以降がサポートされています。
- SnapCenter は、 ONTAP ソフトウェア 4.5 P1 パッチリリースからデータを保護するために、 NetApp SnapCenter 用の Amazon FSX をサポートしています。

  NetApp ONTAP に Amazon FSX を使用している場合、データ保護処理を実行するには、 SnapCenter サーバホストプラグインを 4.5 P1 以降にアップグレードする必要があります。

  NetApp ONTAP の Amazon FSX の詳細については、を参照してください "Amazon FSX for NetApp ONTAP のドキュメント"。

- SnapCenter では、さまざまなアプリケーションやデータベースの保護がサポートされます。

  サポートされているアプリケーションおよびデータベースの詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

サポートされているブラウザ

SnapCenter ソフトウェアは、複数のブラウザで使用できます。

- クロム

  v66 を使用している場合、 SnapCenter GUI の起動に失敗することがあります。

- Internet Explorer の略

  IE 10 以前のバージョンを使用している場合、 SnapCenter UI が正しくロードされません。IE 11 にアップグレードする必要があります。

  - デフォルトレベルのセキュリティのみがサポートされています。

    Internet Explorer のセキュリティ設定を変更すると、ブラウザの表示に重大な問題が発生します。

  - Internet Explorer の互換表示を無効にする必要があります。

- Microsoft Edge の場合

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

接続とポートの要件

SnapCenter サーバとアプリケーションまたはデータベースのプラグインをインストールする前に、接続とポートの要件が満たされていることを確認する必要があります。

- アプリケーションはポートを共有できません。

各ポートは、適切なアプリケーション専用にする必要があります。

- デフォルトのポートを使用しない場合は、インストール時にカスタムポートを選択できます。

  プラグインポートは、インストール後にホストの変更ウィザードを使用して変更できます。

- 固定ポートの場合は、デフォルトのポート番号を受け入れる必要があります。
- ファイアウォール
  - ファイアウォール、プロキシ、またはその他のネットワークデバイスが接続を妨げないようにしてください。
  - SnapCenter のインストール時にカスタムポートを指定した場合は、プラグインホストに、SnapCenter Plug-in Loader のそのポート用のファイアウォールルールを追加する必要があります。

次の表に、各ポートとそのデフォルト値を示します。

ポートのタイプ	デフォルトのポート
SnapCenter ポート	8146（HTTPS）、URL _\https://server:8146_のように双方向、カスタマイズ可能 SnapCenter クライアント（ SnapCenter ユーザ）と SnapCenter サーバ間の通信に使用されます。プラグインホストから SnapCenter サーバへの通信にも使用されます。 ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。"
SnapCenter SMCore の通信ポート	8145 （ HTTPS ）、双方向、カスタマイズ可能 このポートは、 SnapCenter サーバと SnapCenter プラグインがインストールされているホストの間の通信に使用されます。 ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。"
MySQL ポート	3306 （ HTTPS ）、双方向 このポートは、 SnapCenter と MySQL リポジトリデータベースの間の通信に使用されます。 SnapCenter サーバから MySQL サーバへのセキュアな接続を作成できます。 "詳細はこちら。"

ポートのタイプ	デフォルトのポート
Windows プラグインホスト	135 、 445 （ TCP ） ポート 135 および 445 に加え、 Microsoft が指定したダイナミックポート範囲も開いている必要があります。リモートインストール操作では、このポート範囲を動的に検索する Windows Management Instrumentation （ WMI ）サービスを使用します。 サポートされているダイナミックポート範囲については、を参照してください "Windows のサービス概要とネットワークポート要件" ポートは、 SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Windows プラグインホストにプッシュするには、プラグインホストでのみポートを開く必要があります。このポートはインストール後に閉じることができます。
Linux または AIX プラグインホスト	22 （ SSH ） ポートは、 SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Linux または AIX プラグインのホストにコピーするために SnapCenter で使用されます。これらのポートを開いておくか、ファイアウォールまたは iptables から除外しておく必要があります。
SnapCenter Plug-ins Package for Windows 、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX のいずれかです	8145 （ HTTPS ）、双方向、カスタマイズ可能 ポートは、 SMCore とプラグインパッケージがインストールされているホストの間の通信に使用されます。 通信パスも、 SVM 管理 LIF と SnapCenter サーバの間で開いている必要があります。 ポートをカスタマイズするには、を参照してください "ホストを追加し、 SnapCenter Plug-in for Microsoft Windows をインストールします" または "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。"

ポートのタイプ	デフォルトのポート
SnapCenter Plug-in for Oracle Database	27216 、カスタマイズ可能 デフォルトの JDBC ポートは、 Oracle データベースに接続するためにプラグイン for Oracle で使用されます。 ポートをカスタマイズするには、を参照してください "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。"
SnapCenter 用のカスタムプラグイン	9090 （ HTTPS ）、固定 これはカスタムプラグインホストでのみ使用される内部ポートで、ファイアウォールの例外は不要です。 SnapCenter サーバとカスタムプラグイン間の通信はポート 8145 を介してルーティングされます。
ONTAP クラスタまたは SVM の通信ポート	443 （ HTTPS ）、双方向 80 （ HTTP ）、双方向 このポートは、 SnapCenter サーバを実行するホストと SVM の間の通信に SAL （ストレージ抽象化レイヤ）で使用されます。現時点では、 SnapCenter プラグインホストと SVM の間の通信に、 SnapCenter for Windows プラグインホストの SAL でもポートが使用されています。
SnapCenter Plug-in for SAP HANA Database vCode スペルチェッカーポート	3instance_number13 または 3instance_number15 、 HTTP または HTTPS 、双方向、カスタマイズ可能です マルチテナントデータベースコンテナ（ MDC ）のシングルテナントの場合は、ポート番号は 13 で終わり、 MDC 以外の場合はポート番号は 15 で終わります。 たとえば、 32013 はインスタンス 20 のポート番号で、 31015 はインスタンス 10 のポート番号です。 ポートをカスタマイズするには、を参照してください "ホストを追加し、プラグインパッケージをリモートホストにインストールする。"

ポートのタイプ	デフォルトのポート
ドメインコントローラの通信ポート	認証が適切に機能するために、 Microsoft のマニュアルを参照して、ドメインコントローラのファイアウォールで開く必要があるポートを確認してください。 SnapCenter サーバ、プラグインホスト、またはその他の Windows クライアントがユーザを認証できるように、ドメインコントローラで Microsoft の必要なポートを開く必要があります。

ポートの詳細を変更する手順については、を参照してください "プラグインホストを変更します"。

SnapCenter ライセンス

SnapCenter では、アプリケーション、データベース、ファイルシステム、および仮想マシンのデータを保護するために、複数のライセンスが必要になります。インストールする SnapCenter ライセンスのタイプは、ストレージ環境および使用する機能によって異なります。

使用許諾	必要に応じて
SnapCenter 標準のコントローラベース	FAS およびAFF に必要です SnapCenter Standard ライセンスはコントローラベースのライセンスで、 Premium Bundle に含まれています。SnapManager スイートのライセンスをお持ちの場合は、 SnapCenter Standard のライセンスもご利用いただけます。FAS または AFF ストレージを使用した SnapCenter の試用版をインストールする場合は、営業担当者にお問い合わせください。 SnapCenter は、データ保護バンドルの一部としても提供されます。A400 以降を購入している場合は、データ保護バンドルを購入する必要があります。
SnapCenter - 容量ベース	ONTAP Select および Cloud Volumes ONTAP で必要です Cloud Volumes ONTAP または ONTAP Select を使用している場合は、 SnapCenter で管理するデータに基づいて、容量ベースのライセンスを 1TB 単位で購入する必要があります。デフォルトでは、 SnapCenter には 90 日間の 100TB SnapCenter の標準容量ベースの試用版ライセンスが組み込まれています。その他の詳細については、営業担当者にお問い合わせください。

使用許諾	必要に応じて
SnapMirror または SnapVault	ONTAP SnapCenter でレプリケーションを有効にする場合は、 SnapMirror または SnapVault のライセンスが必要です。
SnapRestore	バックアップのリストアおよび検証に必要です。 プライマリストレージシステム • リモート検証に加えてバックアップからのリストアを実行するには、 SnapVault デスティネーションシステムに必要です。 • リモート検証を実行する場合は、 SnapMirror デスティネーションシステムに必要です。
FlexClone	データベースのクローニングおよび検証処理に必要です。 プライマリストレージシステムおよびセカンダリストレージシステム。 • セカンダリ SnapVault バックアップからクローンを作成する場合、 SnapVault デスティネーションシステムに必要です。 • セカンダリ SnapMirror バックアップからクローンを作成するには、 SnapMirror デスティネーションシステムに必要です。
プロトコル	• LUN 用の iSCSI または FC ライセンス • SMB 共有の CIFS ライセンス • NFS タイプの VMDK 用の NFS ライセンスです • VMFS タイプの VMDK 用の iSCSI または FC ライセンス ソースボリュームを利用できない場合に SnapMirror デスティネーションシステムからデータを提供するには、 SnapMirror デスティネーションシステムに必要です。

使用許諾	必要に応じて
SnapCenter 標準ライセンス（オプション）	セカンダリデスティネーション セカンダリデスティネーションに SnapCenter Standard ライセンスを追加することを推奨しますが、必須ではありません。セカンダリデスティネーションで SnapCenter 標準ライセンスが有効になっていない場合、フェイルオーバー処理の実行後に、SnapCenter を使用してセカンダリデスティネーションのリソースをバックアップすることはできません。ただし、クローニング処理と検証処理を実行するには、セカンダリデスティネーションに FlexClone ライセンスが必要です。

SnapCenter Advanced および SnapCenter NAS ファイルサービスのライセンスは廃止され、現在は提供されていません。

1 つ以上の SnapCenter ライセンスをインストールする必要があります。ライセンスの追加方法については、を参照してください "SnapCenter の標準コントローラベースのライセンスを追加します" または "SnapCenter の Standard 容量ベースのライセンスを追加"。

Single Mailbox Recovery （ SMBR ）ライセンス

SnapCenter Plug-in for Exchange を使用して Microsoft Exchange Server データベースと Single Mailbox Recovery （ SMBR ）を管理している場合は、 SMBR のライセンスが追加で必要です。 SMBR の場合は、ユーザのメールボックスに基づいて別途購入する必要があります。

NetApp®Single Mailbox Recoveryは、2023年5月12日に販売終了（EOA）になりました。詳細については、を参照してください "CPC-00507"。NetAppは、2020年6月24日に導入されたマーケティング用パーツ番号を通じて、メールボックスの容量、メンテナンス、サポートを購入したお客様をサポート対象期間中も引き続きサポートします。

NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsには、NetApp Single Mailbox Recoveryと同様の機能が用意されています。お客様は、新しいOntrack PowerControlsソフトウェアライセンスとOntrack PowerControlsメンテナンスおよびサポートの更新をOntrackから（licensingteam@ontrack.com経由で）調達し、2023年5月12日のEOA日以降にメールボックスをきめ細かくリカバリできます。

クレデンシャルの認証方式を指定します

クレデンシャルは、アプリケーションや環境に応じて異なる認証方式を使用します。クレデンシャルで認証されたユーザは、 SnapCenter の処理を実行できます。プラグインのインストール用とデータ保護処理用に 1 組のクレデンシャルを作成する必要があります。

Windows 認証

Windows 認証方式は、 Active Directory に照らして認証します。Windows 認証の場合、 Active Directory は SnapCenter の外部で設定されます。SnapCenter の認証に追加の設定は必要ありません。Windows クレデンシャルは、ホストの追加、プラグインパッケージのインストール、ジョブのスケジュール設定などのタスクを実行する際に必要になります。

信頼されないドメイン認証です

SnapCenter では、信頼されていないドメインに属するユーザとグループを使用して Windows クレデンシャルを作成できます。認証を成功させるには、信頼されていないドメインを SnapCenter に登録する必要があります。

ローカルワークグループ認証

SnapCenter では、ローカルのワークグループユーザとグループを使用して Windows クレデンシャルを作成できます。ローカルワークグループのユーザとグループの Windows 認証は、 Windows クレデンシャルの作成時には行われませんが、ホストの登録やその他のホスト処理が実行されるまで保留されます。

SQL Server 認証

SQL 認証方式は、 SQL Server インスタンスに照らして認証します。つまり、 SnapCenter で SQL Server インスタンスが検出されている必要があります。そのため、 SQL クレデンシャルを追加する前に、ホストの追加とプラグインパッケージのインストールを行って、リソースを更新しておく必要があります。SQL Server 認証は、 SQL Server でのスケジュールの設定やリソースの検出などの処理を実行する際に必要になります。

Linux 認証

Linux 認証方式は、 Linux ホストに照らして認証します。Linux 認証は、 SnapCenter の GUI からリモートで Linux ホストを追加して SnapCenter Plug-ins Package for Linux をインストールする最初のステップで必要になります。

AIX認証

AIX 認証方式は、 AIX ホストに照らして認証します。AIX 認証は、 SnapCenter の GUI からリモートで AIX ホストを追加して SnapCenter Plug-ins Package for AIX をインストールする最初のステップで必要になります。

Oracle データベース認証

Oracle データベース認証方式は、 Oracle データベースに照らして認証します。データベースホストでオペレーティングシステム（ OS ）認証が無効な場合、 Oracle データベースに対して処理を実行するには、 Oracle データベース認証が必要です。そのため、 Oracle データベースのクレデンシャルを追加する前に、 Oracle データベースで sysdba 権限を持つ Oracle ユーザを作成しておく必要があります。

Oracle ASM 認証

Oracle ASM 認証方式は、 Oracle Automatic Storage Management （ ASM ）インスタンスに照らして認証します。Oracle ASM 認証は、 Oracle ASM インスタンスにアクセスする際、データベースホストでオペレーティングシステム（ OS ）認証が無効になっている場合に必要になります。したがって、 Oracle ASM クレデンシャルを追加する前に、 ASM インスタンスで SYSASM 権限を持つ Oracle ユーザを作成する必要があります。

RMAN カタログ認証

RMAN カタログ認証方式は、 Oracle Recovery Manager （ RMAN ）カタログデータベースに照らして認証します。外部のカタログメカニズムを設定し、データベースをカタログデータベースに登録している場合は、RMAN カタログ認証を追加する必要があります。

ストレージ接続およびクレデンシャル

データ保護処理を実行する前に、ストレージ接続をセットアップし、 SnapCenter サーバおよび SnapCenter プラグインで使用するクレデンシャルを追加する必要があります。

- * ストレージ接続 *

  ストレージ接続を使用すると、 SnapCenter サーバおよび SnapCenter プラグインから ONTAP ストレージにアクセスできるようになります。この接続のセットアップには、 AutoSupport 機能と Event Management System （ EMS ；イベント管理システム）機能の設定も含まれます。

- * 資格情報 *

  - ドメイン管理者または管理者グループの任意のメンバー

    ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。

    - NETBIOS_USERNAME_
    - _ ドメイン FQDN\ ユーザ名 _
    - *Username@UPN*

  - ローカル管理者（ワークグループのみ）

    ワークグループに属するシステムの場合は、 SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。

  Username フィールドの有効な形式は、 *username* です

  - 個々のリソースグループのクレデンシャル

    個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

多要素認証（**MFA**）を管理します。

このトピックでは、Active Directoryフェデレーションサービス(AD FS)サーバーとSnapCenter サーバーで多要素認証(MFA)機能を管理する方法について説明します。

多要素認証（MFA）を有効にする

このトピックでは、Active Directoryフェデレーションサービス(AD FS)サーバーとSnapCenter サーバーでMFA機能を有効にする方法について説明します。

このタスクについて

- SnapCenter は、他のアプリケーションが同じAD FSで構成されている場合にSSOベースのログインをサポートします。AD FSの構成によっては、AD FSセッションの持続性に応じて、セキュリティ上の理由からSnapCenter でユーザ認証が必要になる場合があります。
- コマンドレットで使用できるパラメータとその説明は、を実行して確認できます `Get-Help command_name`。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

必要なもの

- Windows Active Directoryフェデレーションサービス（AD FS）がそれぞれのドメインで稼働している必要があります。
- Azure MFA、Cisco Duoなど、AD FSがサポートする多要素認証サービスが必要です。
- SnapCenter およびAD FSサーバのタイムスタンプは、タイムゾーンに関係なく同じである必要があります。
- SnapCenter サーバの認証済みCA証明書を取得して設定します。

  CA証明書は、次の理由で必須です。

  - 自己署名証明書はノードレベルで一意であるため、ADFS-F5通信が切断されないようにします。
  - スタンドアロン構成またはハイアベイラビリティ構成でのアップグレード、修復、またはディザスタリカバリ（DR）の実行時に、自己署名証明書が再作成されないようにしてMFAの再設定を回避します。
  - IP-FQDNの解決を保証します。

    CA証明書の詳細については、を参照してください "CA 証明書 CSR ファイルを生成します"。

手順

1. Active Directoryフェデレーションサービス（AD FS）ホストに接続します。
2. AD FSフェデレーションメタデータファイルをからダウンロードします "https://<host Fqdn>/FederationMetadata/2007-06/FederationMetadata.xml」を参照してください。
3. ダウンロードしたファイルをSnapCenter サーバにコピーしてMFA機能を有効にします。
4. PowerShellを使用して、SnapCenter 管理者ユーザとしてSnapCenter サーバにログインします。
5. PowerShellセッションを使用して、_New-SmMultifactorAuthenticationMetadata-path_cmdletを使用して、SnapCenter MFAメタデータファイルを生成します。

   pathパラメータでは、SnapCenter サーバホストにMFAメタデータファイルを保存するパスを指定します。
6. 生成されたファイルをAD FSホストにコピーし、SnapCenter をクライアントエンティティとして設定します。
7. を使用して、SnapCenter サーバのMFAを有効にします `Set-SmMultiFactorAuthentication`

`-Enable -Path` コマンドレット。

pathパラメータでは、手順3でSnapCenter サーバにコピーされたAD FS MFAメタデータXMLファイルの場所を指定します。

8. （オプション）を使用して、MFAの設定のステータスと設定を確認します `Get-SmMultiFactorAuthentication` コマンドレット。
9. Microsoft管理コンソール（MMC）に移動し、次の手順を実行します。
   a. [ファイル>*スナップインの追加と削除*]をクリックします。
   b. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
   c. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
   d. ［コンソールルート］>［証明書–ローカルコンピューター］>［個人］>［証明書］の順にクリックします。
   e. SnapCenter にバインドされているCA証明書を右クリックし、すべてのタスク>*秘密鍵の管理*を選択します。
   f. 許可ウィザードで、次の手順を実行します。
      i. [追加（ Add ）] をクリックします。
      ii. [場所]*をクリックし、該当するホスト（階層の最上位）を選択します。
      iii. 「場所」ポップアップウィンドウで「* OK」をクリックします。
      iv. [オブジェクト名]フィールドに「IIS_IUSRS」と入力し、[名前の確認]をクリックして、[OK]をクリックします。

      チェックが正常に終了したら、* OK *をクリックします。
10. AD FSホストで、AD FS管理ウィザードを開き、次の手順を実行します。
    a. [証明書利用者信頼（Rel証明 書利用者信頼）]>[証明書利用者信頼の追加（Add Rel証明 書利用者信頼）]>[開始
    b. 2番目のオプションを選択してSnapCenter MFAメタデータファイルを参照し、*次へ*をクリックします。
    c. 表示名を指定し、*次へ*をクリックします。
    d. 必要に応じてアクセス制御ポリシーを選択し、*[Next]*をクリックします。
    e. 次のタブでデフォルトに設定を選択します。
    f. [完了] をクリックします。

    指定した表示名の証明書利用者としてSnapCenter が反映されるようになりました。
11. 名前を選択し、次の手順を実行します。
    a. ［クレーム発行ポリシーの編集］をクリックします。
    b. [ルールの追加]をクリックし、[次へ]をクリックします。
    c. クレームルールの名前を指定します。
    d. 属性ストアとして「* Active Directory *」を選択します。

e. 属性として「* User-Principal-Name 」を選択し、発信クレームタイプとして「 Name-ID *」を選択します。

f. [完了] をクリックします。

12. ADFSサーバで次のPowerShellコマンドを実行します。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. メタデータが正常にインポートされたことを確認するには、次の手順を実行します。

a. 証明書利用者信頼を右クリックし、* Properties *を選択します。

b. [エンドポイント]、[識別子]、および[署名]フィールドに値が入力されていることを確認します

14. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFA機能は、REST APIを使用して有効にすることもできます。

トラブルシューティング情報については、を参照してください "複数のタブで同時にログインを試行すると、MFAエラーが表示されます"。

AD FS MFAメタデータを更新します

AD FSサーバでアップグレード、CA証明書の更新、DRなどの変更が行われた場合は、SnapCenter でAD FS MFAメタデータを更新する必要があります。

手順

1. AD FSフェデレーションメタデータファイルをからダウンロードします "https://<host fqdn>/FederationMetadata/2007-06/FederationMetadata.xml"
2. ダウンロードしたファイルをSnapCenter サーバにコピーしてMFA設定を更新します。
3. 次のコマンドレットを実行して、SnapCenter 内のAD FSメタデータを更新します。

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFAメタデータを更新します

ADFSサーバで修復、CA証明書の更新、DRなどに変更があった場合は、AD FSでSnapCenter MFAメタデータを更新する必要があります。

手順

1. AD FSホストで、AD FS管理ウィザードを開き、次の手順を実行します。

a. [証明書利用者信頼]をクリックします。

b. SnapCenter 用に作成された証明書利用者信頼を右クリックし、*削除*をクリックします。

ユーザが定義した証明書利用者信頼の名前が表示されます。

c. 多要素認証（MFA）を有効にします。

を参照してください "多要素認証を有効にします"。

2. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

多要素認証（**MFA**）を無効にする

手順

1. MFAを無効にし、を使用してMFAを有効にしたときに作成された構成ファイルをクリーンアップします `Set-SmMultiFactorAuthentication -Disable` コマンドレット。
2. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter サーバをインストールします

SnapCenter サーバインストーラの実行ファイルを実行して、 SnapCenter サーバをインストールできます。

必要に応じて、 PowerShell コマンドレットを使用して複数のインストール手順や設定手順を実行することができます。

コマンドラインからの SnapCenter サーバのサイレントインストールはサポートされていません。

- 必要なもの *
- SnapCenter サーバホストは、保留中のシステムの再起動がない Windows アップデートで最新の状態になっている必要があります。
- SnapCenter サーバをインストールするホストに MySQL サーバがインストールされていないことを確認しておく必要があります。
- Windows インストーラのデバッグを有効にしておく必要があります。

  有効にする方法については、 Microsoft の Web サイトを参照してください "Windows インストーラのログ"。

  SnapCenter サーバは、 Microsoft Exchange サーバ、 Active Directory サーバ、またはドメインネームサーバが配置されたホストにはインストールしないでください。

- 手順 *

1. から SnapCenter Server インストールパッケージをダウンロードします "NetApp Support Site"。
2. ダウンロードした .exe ファイルをダブルクリックして、 SnapCenter Server のインストールを開始します。

インストールの開始後、すべての事前確認が実行され、最小要件を満たしていない場合には、対応するエラーまたは警告メッセージが表示されます。

警告メッセージは無視してインストールを続行できますが、エラーは修正しておく必要があります。

3. SnapCenter サーバのインストールに必要な設定済みの値を確認し、必要に応じて変更します。

   MySQL Server リポジトリデータベースのパスワードを指定する必要はありません。SnapCenter サーバのインストール時に、パスワードは自動生成されます。

   特殊文字です%`" is not supported in the custom path for the repository database. If you include "`パスに%`があると'インストールは失敗します

4. [今すぐインストール] をクリックします。

   無効な値を指定すると、該当するエラーメッセージが表示されます。値を再入力してからインストールを開始してください。

   [Cancel] * ボタンをクリックすると、実行中のステップが完了し、ロールバック操作が開始されます。SnapCenter サーバがホストから完全に削除されます。

   ただし、「 SnapCenter サーバサイトの再起動」または「 SnapCenter サーバの起動を待機中」の処理が実行されているときに「 * キャンセル」をクリックすると、処理はキャンセルされずにインストールが続行されます。

ログファイルは常に、 admin ユーザの %temp% フォルダに古いものから順番に表示されます。ログの場所をリダイレクトする場合は、コマンドプロンプトから次のコマンドを実行してSnapCenter Serverのインストールを開始します。`C:\installer_location\installer_name.exe /log"C:\"`

RBAC許可を使用してSnapCenter にログインします

SnapCenter では、 Role-Based Access Control （ RBAC ；ロールベースアクセス制御）がサポートされています。SnapCenter 管理者が、 SnapCenter RBAC を使用して、ロールとリソースをワークグループまたは Active Directory 内のユーザまたは Active Directory 内のグループに割り当てます。RBAC ユーザは、割り当てられたロールを使用して SnapCenter にログインできるようになりました。

- 必要なもの *
- Windows Server Manager で Windows Process Activation Service （ WAS ）を有効にする必要があります。
- Internet Explorer をブラウザとして使用して SnapCenter サーバにログインする場合は、 Internet Explorer の保護モードが無効になっていることを確認する必要があります。
- このタスクについて *

インストール中に、 SnapCenter サーバーインストールウィザードによってショートカットが作成され、SnapCenter がインストールされているホストのデスクトップと [スタート] メニューに表示されます。また、インストールが終了すると、インストールウィザードに、インストール時に指定した情報に基づいて SnapCenter の URL が表示されます。この URL は、リモートシステムからログインする場合にコピーできま

す。

Web ブラウザで複数のタブを開いている場合は、 SnapCenter ブラウザのタブだけを閉じても SnapCenter からはログアウトされません。SnapCenter との接続を終了するには、 [* サインアウト *] ボタンをクリックするか、 Web ブラウザ全体を閉じて、 SnapCenter からログアウトする必要があります。

* ベストプラクティス：セキュリティ上の理由から、ブラウザで SnapCenter パスワードを保存しないことを推奨します。

デフォルトのGUI URLは、SnapCenterサーバがインストールされているサーバ（*https://server:8146*).）のデフォルトポート8146へのセキュアな接続ですSnapCenter のインストール時に別のサーバポートを指定した場合は、そのポートが代わりに使用されます。

ハイアベイラビリティ（HA）環境では、仮想クラスタ\https://Virtual_Cluster_IP_or_FQDN:8146_.を使用してSnapCenterにアクセスする必要がありますInternet Explorer（IE）で_\https://Virtual_Cluster_IP_or_FQDN:8146_に移動してもSnapCenter UIが表示されない場合は、各プラグインホストのIEで仮想クラスタのIPアドレスまたはFQDNを信頼済みサイトとして追加するか、各プラグインホストでIEのセキュリティ強化を無効にする必要があります。
詳細については、を参照してください "ネットワーク外からクラスタ IP アドレスにアクセスできません"。

PowerShell コマンドレットを使用すると、 SnapCenter GUI に加え、設定、バックアップ、リストアの各処理を実行するスクリプトを作成できます。一部のコマンドレットは、各 SnapCenter リリースで変更された可能性があります。。 "SnapCenter ソフトウェアコマンドレットリファレンスガイド" に詳細を示します。

SnapCenter への初回ログイン時は、インストールプロセスで指定したクレデンシャルを使用してログインする必要があります。

- 手順 *

1. ローカルホストのデスクトップにあるショートカット、インストールの終了時に表示された URL 、または SnapCenter 管理者から提供された URL から、 SnapCenter を起動します。
2. ユーザクレデンシャルを入力します

指定する項目	次のいずれかの形式を使用 ...
ドメイン管理者	• NETBIOs\ ユーザー名 • ユーザー名 @UPN サフィックス たとえば、「 username@netapp.com 」と入力します • ドメイン FQDN\ ユーザ名
ローカル管理者	ユーザ名

3. 複数のロールが割り当てられている場合は、 [ロール] ボックスで、このログインセッションに使用するロールを選択します。

   ログインすると、現在のユーザとそのロールが SnapCenter の右上に表示されます。

- 結果 *

ダッシュボードページが表示されます。

ログにサイトにアクセスできないというエラーが表示されて失敗した場合は、 SSL 証明書を SnapCenter にマッピングする必要があります。 "詳細はこちら。"

- 終了後 *

SnapCenter サーバに初めて RBAC ユーザとしてログインしたあと、リソースのリストを更新します。

SnapCenter でサポートされる信頼されていない Active Directory ドメインがある場合は、信頼されていないドメインのユーザにロールを設定する前に、それらのドメインを SnapCenter に登録する必要があります。 "詳細はこちら。"

多要素認証（**MFA**）を使用した**SnapCenter** へのログイン

SnapCenter サーバでは、Active Directoryに含まれるドメインアカウントに対してMFAがサポートされます。

- 必要なもの *
- MFAを有効にしておく必要があります。

  MFAを有効にする方法については、を参照してください "多要素認証を有効にします"

- このタスクについて *
- FQDNのみがサポートされます
- ワークグループユーザとクロスドメインユーザはMFAを使用してログインできません
- 手順 *
  1. ローカルホストのデスクトップにあるショートカット、インストールの終了時に表示された URL 、または SnapCenter 管理者から提供された URL から、 SnapCenter を起動します。
  2. AD FSのログインページで、ユーザ名とパスワードを入力します。

     AD FSページにユーザ名またはパスワードが無効であることを示すエラーメッセージが表示された場合は、次の点を確認してください。

     - ユーザ名またはパスワードが有効かどうか

       ユーザアカウントがActive Directory（AD）に存在している必要があります。

     - ADで設定された最大試行回数を超えたかどうか
     - ADおよびAD FSが稼働しているかどうか

SnapCenter のデフォルトの **GUI** セッションタイムアウトを変更します

SnapCenter GUI のセッションタイムアウト時間を変更して、デフォルトのタイムアウト時間である 20 分以上に設定できます。

セキュリティ機能として、デフォルトでは、操作を行わないまま 15 分が経過すると、 SnapCenter は GUI セ

ッションから 5 分後にログアウトすることを警告するメッセージを表示します。デフォルトでは、操作を行わないまま 20 分が経過すると SnapCenter によって GUI セッションからログアウトされ、再度ログインする必要があります。

- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * > * グローバル設定 * をクリックします。
  2. [グローバル設定] ページで、 [* 構成設定 *] をクリックします。
  3. [Session Timeout] フィールドに、新しいセッションタイムアウトを分単位で入力し、 [**Save**] をクリックします。

SSL 3.0 を無効にして、 SnapCenter Web サーバを保護します

セキュリティ上の理由から、 SnapCenter Web サーバで SSL (Secure Socket Layer) 3.0 プロトコルが有効になっている場合は、 Microsoft IIS で無効にする必要があります。

SSL 3.0 プロトコルに脆弱性が存在します。攻撃者はこの脆弱性を悪用して、原因接続に失敗したり、中間者攻撃を実行したり、 Web サイトと訪問者の間の暗号化トラフィックを監視したりできます。

- 手順 *
  1. SnapCenter Web サーバ・ホストでレジストリ・エディタを起動するには、 [スタート **>*Run**] をクリックし、 regedit と入力します。
  2. レジストリエディタで、 HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\ に移動します。
     - サーバキーがすでに存在する場合：
       i. 有効な DWORD を選択し、 * 編集 * > * 変更 * をクリックします。
       ii. 値を 0 に変更し、 * OK * をクリックします。
     - サーバキーが存在しない場合は、次の手順を実行します。
       i. [* 編集 *] 、 [* 新規 *] 、 [* キー *] の順にクリックし、キーサーバーに名前を付けます。
       ii. 新しいサーバーキーを選択した状態で、 * 編集 * > * 新規 * > * DWORD * をクリックします。
       iii. 新しい DWORD に有効という名前を付け、値として 0 を入力します。
  3. レジストリエディタを閉じます。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *

1. GUI で次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
   c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
   d. ボックスから 16 進文字をコピーします。
   e. 16 進数の間のスペースを削除します。

      たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

2. PowerShell で次の手順を実行します。
   a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

      Get-ChildItem - パス証明書： *\localmachine\My*

   b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して CA 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

. 次のコマンドを実行して、新しくインストールした証明書を Windows ホストプラグインサービスにバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
certhash=$cert appid="$guid"
```

例：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

SnapCenter サイトで CA 証明書を設定します

CA 証明書は、 Windows ホスト上で SnapCenter サイトを使用して設定する必要があります。

- 手順 *

1. SnapCenter がインストールされている Windows サーバーで IIS マネージャーを開きます。
2. 左側のナビゲーションペインで、 * 接続 * をクリックします。
3. サーバー名と * Sites * を展開します。
4. SSL 証明書をインストールする SnapCenter Web サイトを選択します。
5. >[サイトの編集]に移動し、[バインド]*をクリックします。
6. バインディングページで、「 https * のバインディング」を選択します。
7. [編集（ Edit ）] をクリックします。
8. [SSL certificate] ドロップダウンリストから、最近インポートした SSL 証明書を選択します。
9. [OK] をクリックします。

最近導入した CA 証明書がドロップダウンメニューに表示されない場合は、 CA 証明書が秘密鍵に関連付けられているかどうかを確認します。

証明書が次のパスを使用して追加されていることを確認します。 * コンソールルート > 証明書–ローカルコンピュータ > 信頼されたルート証明機関 > 証明書 * 。

SnapCenter の CA 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバの CA 証明書検証を有効にする必要があります。

- 必要なもの *

- CA 証明書は、 Set-SmCertificateSettings コマンドレットを使用して有効または無効にできます。
- Get-SmCertificateSettings コマンドレットを使用すると、 SnapCenter サーバの証明書のステータスを表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * CA 証明書設定 * と進みます。
  2. [証明書の検証を有効にする] を選択します。
  3. [適用（ Apply ）] をクリックします。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- ：有効な CA 証明書がないか、プラグインホストに割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

Active Directory 、 LDAP 、 LDAPS を設定します

信頼できない Active Directory ドメインを登録します

信頼されていない複数の Active Directory ドメインのホスト、ユーザ、およびグループを管理するには、 Active Directory を SnapCenter サーバに登録する必要があります。

- 必要なもの *
- LDAP および LDAPS プロトコル *
- LDAP または LDAPS プロトコルを使用して、信頼されていない Active Directory ドメインを登録できます。
- プラグインホストと SnapCenter サーバ間の双方向通信を有効にしておく必要があります。
- DNS 解決は、 SnapCenter サーバからプラグインホスト、およびその逆にセットアップする必要があります。
- LDAP プロトコル *
- Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を SnapCenter サーバから解決できる必要があります。

  信頼されていないドメインは FQDN に登録できます。FQDN を SnapCenter サーバから解決できない場合

は、ドメインコントローラの IP アドレスを使用して登録できます。これは、 SnapCenter サーバが解決できる必要があります。

- LDAPSプロトコル*
- Active Directory 通信でエンドツーエンドの暗号化を行うには、 LDAPS で CA 証明書が必要です。

  "LDAPS の CA クライアント証明書を設定します"

- ドメインコントローラのホスト名（ DCHostName ）に SnapCenter サーバからアクセスできる必要があります。
- このタスクについて *
- 信頼されていないドメインを登録するには、 SnapCenter ユーザインターフェイス、 PowerShell コマンドレット、または REST API を使用します。
- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. 設定ページで、 * グローバル設定 * をクリックします。
  3. [グローバル設定] ページで、 [* ドメイン設定 *] をクリックします。
  4. をクリックします  新しいドメインを登録します。
  5. [新しいドメインの登録] ページで、 **LDAP** または *LDAPS * のいずれかを選択します。
     a. 「 * ldap * 」を選択した場合は、 LDAP の信頼されていないドメインを登録するために必要な情報を指定します。

フィールド	手順
ドメイン名（ Domain Name ）	ドメインの NetBIOS 名を指定します。
ドメイン FQDN	FQDN を指定し、 * resolve * をクリックします。
ドメインコントローラの IP アドレス	ドメイン FQDN を SnapCenter サーバから解決できない場合は、ドメインコントローラの IP アドレスを 1 つ以上指定します。 詳細については、を参照してください "GUI から信頼できないドメインのドメインコントローラ IP を追加します"。

     b. 「 * LDAPS * 」を選択した場合は、 LDAPS の信頼されていないドメインの登録に必要な情報を指定します。

フィールド	手順
ドメイン名（ Domain Name ）	ドメインの NetBIOS 名を指定します。

フィールド	手順
ドメイン FQDN	FQDNを指定します。
ドメインコントローラ名	1 つまたは複数のドメインコントローラ名を指定し、 * Resolve.* をクリックします。
ドメインコントローラの IP アドレス	ドメインコントローラ名が SnapCenter サーバから解決できない場合は、 DNS 解決を修正する必要があります。

6. [OK] をクリックします。

LDAPS の CA クライアント証明書を設定します

Windows Active Directory LDAPS に CA 証明書が設定されている場合は、 SnapCenter サーバで LDAPS の CA クライアント証明書を設定する必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
ウィザードの 2 ページ目に表示されます	[* 参照] をクリックし、 *Root Certificate* を選択して、 [* 次へ *] をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

7. 中間証明書について、手順5と6を繰り返します。

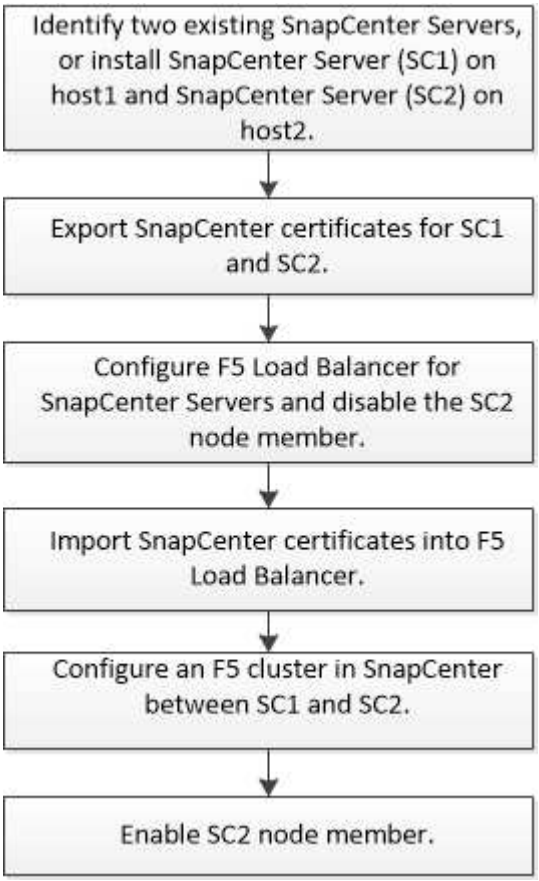
ハイアベイラビリティを設定する

F5 を使用して SnapCenter サーバのハイアベイラビリティを構成します

SnapCenter でハイアベイラビリティ（ HA ）をサポートするには、 F5 ロードバランサをインストールします。F5 によって、 SnapCenter サーバは、同じ場所にある最大 2 台のホストでアクティブ / パッシブ構成をサポートできます。SnapCenter で F5 ロードバランサを使用するには、 SnapCenter サーバを設定し、 F5 ロードバランサを設定する必要があります。

SnapCenter 4.2.x からアップグレードし、以前に Network Load Balancing （ NLB ）を使用していた場合は、引き続きその構成を使用するか、 F5 に切り替えることができます。

ワークフローイメージには、 F5 ロードバランサを使用して SnapCenter サーバのハイアベイラビリティを設定する手順が記載されています。詳細な手順については、を参照してください "F5 ロードバランサを使用して SnapCenter サーバのハイアベイラビリティを設定する方法"。



次のコマンドレットを使用して F5 クラスタを追加および削除するには、 SnapCenter サーバのローカル管理者グループのメンバーである必要があります（ SnapCenterAdmin ロールに割り当てられることに加えて）。

- Add - SmServerCluster をクリックします
- add-SmServer
- remove-SmServerCluster を実行しました

詳細については、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

F5 のその他の設定情報

- SnapCenter をインストールしてハイアベイラビリティ用に設定したら、 F5 クラスタ IP を指すように SnapCenter デスクトップのショートカットを編集します。
- SnapCenter サーバ間でフェイルオーバーが発生し、既存の SnapCenter セッションも存在する場合は、ブラウザを閉じてから再度 SnapCenter にログオンする必要があります。
- ロードバランサのセットアップ（ NLB または F5 ）で、 NLB ノードまたは F5 ノードによって一部解決されているノードを追加し、 SnapCenter ノードがこのノードに到達できない場合、 SnapCenter ホストページでホストが停止して実行中の状態になる頻度が高くなります。この問題を解決するには、両方の SnapCenter ノードが NLB ノードまたは F5 ノードでホストを解決できることを確認する必要があります。
- MFA設定のSnapCenter コマンドは、すべてのノードで実行する必要があります。証明書利用者設定は、Active Directoryフェデレーションサービス（AD FS）サーバで、F5クラスタの詳細を使用して行う必要があります。 ノードレベルのSnapCenter UIアクセスはMFAが有効になったあとはブロックされます。
- フェイルオーバー時、監査ログの設定が2つ目のノードに反映されません。 このため、F5パッシブノードがアクティブになった場合は、そのノードで監査ログ設定を手動で繰り返してください。

Microsoft Network Load Balancer を手動で設定します

SnapCenter ハイアベイラビリティを設定するには、 Microsoft Network Load Balancing （ NLB ）を設定します。SnapCenter 4.2 以降では、高可用性を実現するために、 SnapCenter 以外のインストール環境で NLB を手動で設定する必要があります。

SnapCenter でネットワーク負荷分散 (NLB) を構成する方法の詳細については、を参照してください "NLB に SnapCenter を設定する方法"。

SnapCenter 4.1.1 以前では、 SnapCenter のインストール時にネットワーク負荷分散 (NLB) の構成がサポートされていました。

NLB から F5 に切り替えて高可用性を実現します

SnapCenter HA 構成を Network Load Balancing （ NLB ）から変更して、 F5 ロードバランサを使用することができます。

- 手順 *
  1. F5 を使用して SnapCenter サーバのハイアベイラビリティを設定します。 "詳細はこちら。"。
  2. SnapCenter サーバホストで、 PowerShell を起動します。
  3. Open-SmConnection コマンドレットを使用してセッションを開始し、クレデンシャルを入力します。
  4. SnapCenter サーバを更新して、 Update-SmServerCluster コマンドレットを使用して F5 クラスタの IP アドレスを指すようにします。

     コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapCenter MySQL リポジトリの高可用性

MySQL Server の機能である MySQL レプリケーションを使用すると、 MySQL データベースサーバ（マスター）から別の MySQL データベースサーバ（スレーブ）にデータをレプリケートできます。SnapCenter では、 Network Load Balancing （ NLB ）が有効な 2 つのノード間でのみ、高可用性実現のために MySQL レプリケーションをサポートしています。

SnapCenter は、マスターリポジトリに対して読み取りまたは書き込み操作を実行し、マスターリポジトリに障害が発生した場合はスレーブリポジトリに接続をルーティングします。スレーブリポジトリがマスターリポジトリになります。SnapCenter は逆方向のレプリケーションもサポートしており、これはフェイルオーバー時にのみ有効になります。

MySQL の高可用性（ HA ）機能を使用する場合は、 1 つ目のノードに Network Load Balancer （ NLB ）を設定する必要があります。MySQL リポジトリは、インストール中にこのノードにインストールされます。2 つ目のノードに SnapCenter をインストールするときは、 1 つ目のノードの F5 に参加して、 2 つ目のノードに MySQL リポジトリのコピーを作成する必要があります。

SnapCenter には、 MySQL レプリケーションを管理するための _Get-SmRepositoryConfig_and _Set -SmRepositoryConfig_PowerShell コマンドレットが用意されています。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

MySQL HA 機能に関連する次の制限事項を確認しておく必要があります。

- NLB と MySQL HA がサポートされるのは、 2 つのノードまでです。
- SnapCenter スタンドアロンインストールから NLB インストールまたはその逆の切り替えや、 MySQL スタンドアロンセットアップから MySQL HA への切り替えはサポートされていません。
- スレーブリポジトリのデータがマスターリポジトリのデータと同期されていない場合、自動フェイルオーバーはサポートされません。

  強制フェイルオーバーを開始するには、 _Set-SmRepositoryConfig_cmdlet を使用します。

- フェイルオーバーが開始されると、実行中のジョブが失敗する可能性があります。

  MySQL Server または SnapCenter Server がダウンしたためにフェイルオーバーが発生した場合、実行中のすべてのジョブが失敗する可能性があります。2 つ目のノードへのフェイルオーバー後、後続のすべてのジョブは正常に実行されます。

ハイアベイラビリティの設定については、を参照してください "SnapCenter で NLB と ARR を設定する方法"。

SnapCenter 証明書をエクスポートする

- 手順 *

  1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [* スナップインの追加と削除] の順にクリックします。

2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [マイユーザーアカウント *] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>*Certificates - Current User**>*Trusted Root Certification Authorities*>*Certificates*] をクリックします。
5. SnapCenter フレンドリ名が表示されている証明書を右クリックし、 * すべてのタスク * > * エクスポート * を選択してエクスポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をエクスポートします	[はい] を選択し、秘密鍵 * をエクスポートして、 [次へ] をクリックします。
エクスポートファイル形式（ Export File Format ）	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
エクスポートするファイル	エクスポートされた証明書のファイル名を指定し（ .pfx を使用する必要があります）、 * 次へ * をクリックします。
証明書のエクスポートウィザードの完了	概要を確認し、 * 完了 * をクリックしてエクスポートを開始します。

- 結果 *

証明書は .pfx 形式でエクスポートされます。

ロールベースアクセス制御（ RBAC ）の設定

ユーザまたはグループを追加し、ロールとアセットを割り当てます

SnapCenter ユーザのロールベースアクセス制御を設定するには、ユーザまたはグループを追加してロールを割り当てます。ロールに基づいて、 SnapCenter ユーザがアクセスできるオプションが決まります。

- 必要なもの *
- 「 SnapCenterAdmin 」ロールでログインする必要があります。
- ユーザまたはグループのアカウントを、オペレーティングシステムまたはデータベースの Active Directory に作成しておく必要があります。SnapCenter を使用してこれらのアカウントを作成することはできません。

SnapCenter 4.5 では、ユーザ名とグループ名に次の特殊文字のみを使用できます。スペース（）、ハイフン（ - ）、アンダースコア（ _ ）、コロン（ : ）。
これらの特殊文字を使用して以前のリリースの SnapCenter で作成したロールを使用する場合は、 SnapCenter WebApp がインストールされている web.config ファイルで「 isableSQLInjionValidation 」パラメータの値を true に変更することで、ロール名の検証を無効にできます。値を変更した場合、サービスを再起動する必要はありません。

- SnapCenter には、事前定義されたロールが複数あり

  これらのロールをユーザに割り当てるか、新しいロールを作成できます。

- SnapCenter RBAC に追加される AD ユーザと AD グループには、 Active Directory 内の Users コンテナと Computers コンテナに対する読み取り権限が必要です。
- 適切な権限が割り当てられたユーザまたはグループにロールを割り当てたら、ホストやストレージ接続などの SnapCenter アセットへのユーザアクセスを割り当てる必要があります。

  これにより、ユーザは、自身に割り当てられたアセットに対して権限のある処理を実行できます。

- RBAC の権限と効率性を利用するには、いずれかの時点でロールをユーザまたはグループに割り当てる必要があります。
- ホスト、リソースグループ、ポリシー、ストレージ接続、プラグインなどのアセットを割り当てることができます。 ユーザまたはグループの作成時にユーザにクレデンシャルを付与する必要があります。
- 特定の処理を実行するためにユーザに割り当てる必要がある最小アセットは次のとおりです。

操作	資産の割り当て
リソースを保護	ホスト、ポリシー
バックアップ	ホスト、リソースグループ、ポリシー
リストア	ホスト、リソースグループ
クローン	ホスト、リソースグループ、ポリシー
クローンのライフサイクル	ホスト
リソースグループを作成します	ホスト

- Windows クラスタまたは DAG （ Exchange Server データベース可用性グループ）のアセットに新しいノードを追加したときに、その新しいノードをユーザに割り当てた場合は、新しいノードを追加するアセットをユーザまたはグループに再割り当てする必要があります。

  RBAC ユーザまたはグループをクラスタまたは DAG に再割り当てして、新しいノードを RBAC ユーザまたはグループに追加する必要があります。たとえば、 2 ノードクラスタで RBAC ユーザまたはグループをクラスタに割り当てているとします。クラスタに別のノードを追加した場合は、 RBAC のユーザまたはグループをクラスタに再割り当てして、 RBAC ユーザまたはグループの新しいノードを追加します。

- Snapshot コピーをレプリケートする場合は、処理を実行するユーザにソースボリュームとデスティネー

ションボリュームの両方のストレージ接続を割り当てる必要があります。

ユーザにアクセスを割り当てる前にアセットを追加しておく必要があります。

SnapCenter Plug-in for VMware vSphere の機能を使用して VM 、 VMDK 、またはデータストアを保護している場合は、 VMware vSphere GUI を使用して、 SnapCenter Plug-in for VMware vSphere ロールに vCenter ユーザを追加する必要があります。VMware vSphere のロールについては、を参照してください "SnapCenter Plug-in for VMware vSphere に組み込みの事前定義のロール"。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ユーザーとアクセス >] をクリックします *
3. [Add Users/Groups from Active Directory or Workgroup] ページで、次の手順を実行します。

フィールド	手順
アクセスタイプ	ドメインまたはワークグループのいずれかを選択します ドメイン認証タイプには、ロールにユーザを追加するユーザまたはグループのドメイン名を指定する必要があります。 デフォルトでは、ログインしているドメイン名があらかじめ入力されています。 信頼されていないドメインは、 [* 設定 * > * グローバル設定 * > * ドメイン設定 * （ * Settings * > * Global Settings * ）] ページで登録する必要があります。
を入力します	[ユーザー] または [グループ] を選択します SnapCenter でサポートされるのはセキュリティグループのみで、配信グループはサポートされません。

フィールド	手順
ユーザ名	a. 部分的なユーザー名を入力し、 * 追加 * をクリックします。 ユーザ名では大文字と小文字が区別されます。 b. 検索リストからユーザ名を選択します。 別のドメインまたは信頼されていないドメインのユーザを追加する場合は、ユーザ名を完全に入力する必要があります。これは、クロスドメインユーザの検索リストがないためです。 この手順を繰り返して、選択したロールにユーザまたはグループを追加します。
ロール	ユーザを追加するロールを選択します。

4. [**Assign**] をクリックし、 [Assign Assets] ページで次の手順を実行します。
   a. [* アセット *] ドロップダウン・リストからアセットのタイプを選択します。
   b. [アセット] リストで、アセットを選択します。

      アセットは、ユーザが SnapCenter にアセットを追加した場合にのみ表示されます。

   c. 必要なすべてのアセットについて、この手順を繰り返します。
   d. [保存（ Save ）] をクリックします。
5. [Submit （送信）] をクリックします。

   ユーザまたはグループを追加してロールを割り当てたら、リソースのリストを更新します。

ロールを作成します

既存の SnapCenter ロールに加えて、独自のロールを作成して権限をカスタマイズできます。

「 SnapCenterAdmin 」ロールでログインする必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. 設定ページで、 * 役割 * をクリックします。
3. をクリックします 。

4. [Add Role] ページで、新しいロールの名前と概要を指定します。

> SnapCenter 4.5 では、ユーザ名とグループ名に次の特殊文字のみを使用できます。スペース（）、ハイフン（ - ）、アンダースコア（ _ ）、コロン（ : ）。
> これらの特殊文字を使用して以前のリリースの SnapCenter で作成したロールを使用する場合は、 SnapCenter WebApp がインストールされている web.config ファイルで「 isableSQLInjionValidation 」パラメータの値を true に変更することで、ロール名の検証を無効にできます。値を変更した場合、サービスを再起動する必要はありません。

5. このロールのすべてのメンバーは、他のメンバーのオブジェクトを表示できます * を選択すると、そのロールの他のメンバーは、リソースリストの更新後にボリュームやホストなどのリソースを参照できます。

   他のメンバーが割り当てられているオブジェクトをこのロールのメンバーに表示しないようにするには、このオプションを選択解除する必要があります。

> このオプションを有効にすると、オブジェクトまたはリソースを作成したユーザと同じロールにユーザが属している場合に、オブジェクトまたはリソースへのアクセスをユーザに割り当てる必要がなくなります。

1. [アクセス許可] ページで、そのロールに割り当てるアクセス許可を選択するか、 [すべて選択] をクリックしてそのロールにすべてのアクセス許可を付与します。
2. [Submit （送信）] をクリックします。

security login コマンドを使用して、 ONTAP RBAC ロールを追加します

ストレージシステムで clustered ONTAP を実行している場合、 security login コマンドを使用して ONTAP RBAC ロールを追加できます。

- 必要なもの *
- clustered ONTAP を実行しているストレージシステム用に ONTAP RBAC ロールを作成する前に、次の項目について確認しておく必要があります。
  - 実行するタスク
  - これらのタスクを実行するために必要な権限
- RBAC ロールを設定するには、次の操作を実行する必要があります。
  - コマンドおよびコマンドディレクトリ、またはその両方に権限を付与します。

    コマンドおよびコマンドディレクトリのアクセスには、フルアクセスと読み取り専用の 2 つのレベルがあります。

  フルアクセス権限は、常に最初に割り当てる必要があります。

  - ユーザにロールを割り当てます。
  - SnapCenter プラグインがクラスタ全体のクラスタ管理者 IP に接続されているか、またはクラスタ内の SVM に直接接続されているかに応じて、設定は異なります。
- このタスクについて *

RBAC User Creator for Data ONTAP ツールを使用して、これらのロールのストレージシステムへの設定を簡素化することができます。このツールは、ネットアップコミュニティフォーラムに掲載されています。

このツールは、 ONTAP 権限の適切な設定を自動的に処理します。たとえば、 Data ONTAP フルアクセス権限が最初に表示されるように、権限が自動的に正しい順序で追加されます。読み取り専用権限を最初に追加し、次にフルアクセス権限を追加すると、 ONTAP はフルアクセス権限を重複するものとしてマーキングし、無視します。

SnapCenter または ONTAP をあとからアップグレードする場合は、 RBAC User Creator for Data ONTAP ツールを再度実行して、以前に作成したユーザロールを更新する必要があります。以前のバージョンの SnapCenter または ONTAP 用に作成したユーザロールは、アップグレード後のバージョンでは正常に機能しません。ツールを再実行すると、アップグレードが自動的に処理されます。ロールを再作成する必要はありません。

ONTAP RBAC ロールの設定の詳細については、を参照してください "ONTAP 9 管理者認証と RBAC パワーガイド"。

SnapCenter のドキュメントではロールに割り当てる要素を「権限」と呼びますが、OnCommand システムマネージャGUIでは、_privilegeではなく、TERM_attribute__が使用されます。ONTAP RBACロールを設定する場合は、この2つの用語は同じ意味です。

- 手順 *

1. ストレージシステムで次のコマンドを入力して、新しいロールを作成します。

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - svm_name は、 SVM ユーザの名前です。空白のままにすると、デフォルトでクラスタ管理者が指定されます。
   - role_name は、ロールに指定する名前です。
   - command は、 ONTAP の機能です。

     このコマンドは権限ごとに実行する必要があります。フルアクセスコマンドは、読み取り専用コマンドの前にリストする必要があります。

   権限のリストについては、を参照してください "ロールの作成および権限の割り当てに使用する ONTAP CLI コマンド"。

2. 次のコマンドを入力して、ユーザ名を作成します。

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name は、作成するユーザの名前です。
   - <password> は、パスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。
   - svm_name は、 SVM ユーザの名前です。

3. 次のコマンドを入力して、ユーザにロールを割り当てます。

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod
   <password\>
   ```

   - <user_name> は、手順 2 で作成したユーザの名前です。このコマンドでは、ロールに関連付けるユーザを変更できます。
   - <svm_name> は SVM の名前です。
   - <role_name> は、手順 1 で作成したロールの名前です。
   - <password> は、パスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。

4. 次のコマンドを入力して、ユーザが正しく作成されたことを確認します。

   ```
   security login show -vserver <svm_name\> -user-or-group-name <user_name\>
   ```

user_name は、手順 3 で作成したユーザの名前です。

最小権限を持つ **SVM** ロールを作成します

ONTAP で新しい SVM ユーザのロールを作成する場合、実行する必要がある ONTAP CLI コマンドがいくつかあります。ONTAP 内の SVM を SnapCenter で使用するように設定し、 vsadmin ロールを使用したくない場合、このロールが必要です。

- 手順 *

1. ストレージシステムで、ロールを作成し、そのロールにすべての権限を割り当てます。

   ```
   security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   このコマンドは権限ごとに実行する必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   ontapi -authmethod password -role <SVM_Role_Name\>
   ```

2. ユーザのロックを解除します。

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

SVM ロールの作成および権限の割り当てに使用する **ONTAP CLI** コマンド

SVM ロールを作成して権限を割り当てるには、いくつかの ONTAP CLI コマンドを実行する必要があります。

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"snapmirror list-destinations" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume file clone create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`

最小限の権限で **ONTAP** クラスタロールを作成します

最小限の権限で ONTAP クラスタロールを作成して、 SnapCenter の admin ロールを使用して ONTAP で処理を実行する必要がないようにする必要があります。ONTAP のいくつかの CLI コマンドを実行して、 ONTAP クラスタロールを作成し、最小限の権限を割り当てることができます。

- 手順 *

1. ストレージシステムで、ロールを作成し、そのロールにすべての権限を割り当てます。

   ```
   security login role create -vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   このコマンドは権限ごとに実行する必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

```
security login create -user <user_name\> -vserver <cluster_name\>
-application ontapi -authmethod password -role <role_name\>
```

2. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

クラスタロールの作成および権限の割り当てに使用する **ONTAP CLI** コマンド

クラスタロールを作成して権限を割り当てるには、いくつかの ONTAP CLI コマンドを実行する必要があります。

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"lun igroup modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly

- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"system node show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"vserver export-policy delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

Active Directory の読み取り権限を有効にするように **IIS** アプリケーションプールを設定します

SnapCenter の Active Directory 読み取り権限を有効にする必要がある場合は、 Windows Server でインターネットインフォメーションサービス (IIS) を構成して、カスタムのアプリケーションプールアカウントを作成できます。

- 手順 *
  1. SnapCenter がインストールされている Windows サーバーで IIS マネージャーを開きます。
  2. 左側のナビゲーションペインで、 * アプリケーションプール * をクリックします。
  3. ［アプリケーションプール］ リストで ［ SnapCenter ］ を選択し、 ［アクション］ ペインで ［ * 詳細設定 * ］ をクリックします。
  4. [ID] を選択し、 [*...] をクリックして SnapCenter アプリケーションプール ID を編集します。
  5. [カスタムアカウント] フィールドに、 Active Directory の読み取り権限を持つドメインユーザーまたはドメイン管理者アカウント名を入力します。
  6. [OK] をクリックします。

     カスタムアカウントは、 SnapCenter アプリケーションプールに組み込まれている ApplicationPoolIdentity アカウントに代わるものです。

監査ログを設定します

監査ログは、SnapCenter サーバのすべてのアクティビティについて生成されます。デフォルトでは、監査ログはインストールされているデフォルトの場所である_ C

：\Program Files\NetApp\Virtual \SnapCenter WebApp\audit_にあります。

監査ログは、各監査イベントに対してデジタル署名されたダイジェストを生成することで保護され、不正な変更から保護されます。生成されたダイジェストは個別の監査チェックサムファイルに保持され、の定期的な整合性チェックでコンテンツの整合性を確保します。

「 SnapCenterAdmin 」ロールでログインする必要があります。

- このタスクについて *
- アラートは次のシナリオで送信されます。
  - 監査ログの整合性チェックのスケジュール、またはsyslogサーバが有効または無効になっています
  - 監査ログの整合性チェック、監査ログ、またはsyslogサーバのログに障害が発生しました
  - ディスクスペースが不足しています
- 整合性チェックが失敗した場合にのみ、電子メールが送信されます。
- 監査ログディレクトリと監査チェックサムログディレクトリの両方のパスを一緒に変更する必要があります。変更できるのはどちらか一方だけです。
- 監査ログディレクトリと監査チェックサムログディレクトリのパスが変更された場合、以前の場所にある監査ログに対して整合性チェックを実行することはできません。
- 監査ログディレクトリと監査チェックサムログディレクトリのパスは、SnapCenter サーバのローカルドライブにある必要があります。

  共有ドライブまたはネットワークマウントドライブはサポートされません。

- syslogサーバ設定でUDPプロトコルが使用されている場合、ポートが停止しているか使用できないことによるエラーは、SnapCenter ではエラーまたはアラートとしてキャプチャできません。
- 監査ログを設定するには、Set-SmAuditSettingsコマンドとGet-SmAuditSettingsコマンドを使用します。

  コマンドレットで使用できるパラメータとその説明については、 Get-Help コマンドレットを実行して確認できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. [設定]ページで、[設定]>[グローバル設定]>[監査ログ設定]の順に選択します。
  2. 監査ログセクションに詳細を入力します。
  3. 監査ログ・ディレクトリ*および*監査チェックサム・ログ・ディレクトリ*を入力します
     a. 最大ファイルサイズを入力します
     b. 最大ログファイル数を入力します
     c. アラートを送信するためのディスクスペース使用率を入力します
  4. （任意）*Log UTC time *をイネーブルにします。
  5. （オプション）* Audit Log Integrity Check Schedule を有効にし、 Start Integrity Check * for On Demand integrity checkをクリックします。

     また、*Start-SmAuditIntegrityCheck*コマンドを実行して、必要に応じて整合性チェックを開始することもできます。

6. （任意）転送された監査ログをリモートsyslogサーバに対してイネーブルにし、Syslogサーバの詳細を入力します。

   syslogサーバからTLS 1.2プロトコルの「信頼されたルート」に証明書をインポートする必要があります。

   a. 「Syslog Server Host」と入力します
   b. 「Syslog Server Port」と入力します
   c. 「Syslog Server Protocol」と入力します
   d. RFC形式を入力します

7. [保存（ Save ）] をクリックします。
8. 監査整合性チェックとディスク領域チェックは、* Monitor > Jobs *をクリックすると表示できます。

ストレージシステムを追加

データ保護処理とプロビジョニング処理を実行するためには、 ONTAP ストレージまたは NetApp ONTAP 用の Amazon FSX に SnapCenter アクセスを付与するストレージシステムをセットアップする必要があります。

スタンドアロンの SVM を追加したり、複数の SVM で構成されるクラスタを追加したりできます。NetApp ONTAP に Amazon FSX を使用している場合は、 fsxadmin アカウントを使用して複数の SVM で構成される FSX 管理 LIF を追加するか、 SnapCenter に FSX SVM を追加できます。

- 必要なもの *
- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

- このタスクについて *
- ストレージシステムを設定する際に、 Event Management System （ EMS ；イベント管理システム）と AutoSupport の機能を有効にすることもできます。AutoSupport ツールは、システムの健常性に関するデータを収集し、そのデータをシステムのトラブルシューティング用にネットアップテクニカルサポートに自動的に送信します。

  これらの機能を有効にすると、リソースが保護されたとき、リストアまたはクローニング処理が正常に完了したとき、または処理が失敗したときに、 SnapCenter からストレージシステムに AutoSupport 情報が、ストレージシステムの syslog に EMS メッセージが送信されます。

- SnapMirror デスティネーションまたは SnapVault デスティネーションに Snapshot コピーをレプリケートする場合は、デスティネーション SVM またはクラスタとソース SVM またはクラスタへのストレージシステム接続をセットアップする必要があります。

> ストレージシステムのパスワードを変更すると、スケジュールされたジョブ、オンデマンドバックアップ、およびリストア処理が失敗する場合があります。ストレージ・システムのパスワードを変更した後、 Storage （ストレージ）タブで * Modify （変更） * をクリックしてパスワードを更新できます。

- 手順 *

1. 左側のナビゲーションペインで、 * ストレージシステム * をクリックします。
2. [ストレージシステム] ページで、 [新規作成] をクリックします。
3. Add Storage System （ストレージシステムの追加）ページで、次の情報を入力します。

フィールド	手順
ストレージシステム	ストレージシステムの名前または IP アドレスを入力します。 ドメイン名を含まないストレージ・システム名は、 15 文字以内で、名前を解決できる必要があります。15 文字を超える名前のストレージシステム接続を作成するには、 Add-SmStorageConnectionPowerShell コマンドレットを使用します。 MetroCluster 構成（ MCC ）を使用するストレージシステムでは、ノンストップオペレーションを実現するためにローカルクラスタとピアクラスタの両方を登録することを推奨します。 SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SnapCenter でサポートされる SVM には、それぞれ一意の名前を付ける必要があります。 SnapCenter へのストレージ接続の追加後は、 ONTAP を使用して SVM またはクラスタの名前を変更しないでください。 SVM に短い名前または FQDN を追加した場合は、 SnapCenter とプラグインホストの両方から解決できる必要があります。
ユーザ名 / パスワード	ストレージシステムにアクセスするために必要な権限を持つストレージユーザのクレデンシャルを入力します。

フィールド	手順
Event Management System （ EMS ；イベント管理システム）および AutoSupport の設定	保護適用、リストア処理の完了、または処理の失敗のために AutoSupport メッセージをストレージシステムに送信する場合は、該当するチェックボックスを選択します。 AutoSupport 通知を有効にするには AutoSupport メッセージが必要であるため、［* 失敗した処理に対する SnapCenter 通知をストレージ・システムに送信する *］ チェックボックスをオンにすると、［* サーバ・イベントを syslog に記録する *］ チェックボックスもオンになります。

4. プラットフォーム、プロトコル、ポート、およびタイムアウトに割り当てられたデフォルト値を変更する場合は、 [その他のオプション *] をクリックします。
   a. プラットフォームで、ドロップダウンリストからいずれかのオプションを選択します。

      SVM がバックアップ関係のセカンダリストレージシステムの場合は、 * Secondary * チェックボックスを選択します。[* Secondary] オプションを選択すると、 SnapCenter はすぐにライセンスチェックを実行しません。

   b. プロトコルで、 SVM またはクラスタのセットアップ時に設定したプロトコル（通常は HTTPS ）を選択します。
   c. ストレージシステムが受け入れるポートを入力します。

      通常、デフォルトポート 443 は使用可能です。

   d. 通信が中断されるまでの経過時間を秒単位で入力します。

      デフォルト値は60秒です。

   e. SVM に複数の管理インターフェイスがある場合は、「 * 優先 IP 」チェックボックスを選択し、 SVM 接続用の優先 IP アドレスを入力します。
   f. [保存（ Save ）] をクリックします。
5. [Submit （送信）] をクリックします。

- 結果 *

Storage Systems （ストレージシステム）ページの * Type （タイプ） * ドロップダウンから、次のいずれかの操作を実行します。

- 追加されたすべての ONTAP を表示する場合は、「 * SVM SVM * 」を選択します。

  FSX SVM を追加した場合は、ここに FSX SVM が表示されます。

- 追加されたすべてのクラスタを表示するには、「 * ONTAP クラスタ * 」を選択します。

  fsxadmin を使用して FSX クラスタを追加した場合、 FSX クラスタがここに表示されます。

  クラスタ名をクリックすると、クラスタに含まれるすべての SVM が SVM セクションに表示されます。

ONTAP の GUI を使用して ONTAP クラスタに新しい SVM を追加した場合は、 * Rediscover* をクリックすると、新しく追加した SVM が表示されます。

- 終了後 *

クラスタ管理者は、ストレージシステムのコマンドラインから次のコマンドを実行して、各ストレージシステムノードで AutoSupport を有効にし、 SnapCenter がアクセス可能なすべてのストレージシステムから E メール通知を送信する必要があります。

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
enable -noteto enable
```

Storage Virtual Machine （ SVM ）管理者には AutoSupport へのアクセス権はありません。

SnapCenter の標準コントローラベースのライセンスを追加します

FAS または AFF ストレージコントローラを使用する場合は、 SnapCenter の標準コントローラベースのライセンスが必要です。

コントローラベースのライセンスには次のような特徴があります。

- Premium Bundle または Flash Bundle （ベースパックには含まれません）の購入に SnapCenter Standard のライセンスが含まれます。
- 無制限のストレージ使用
- ONTAP System Manager またはストレージクラスタのコマンドラインを使用して、 FAS または AFF のストレージコントローラに直接追加して有効にします

SnapCenter コントローラベースのライセンスについては、 SnapCenter GUI にライセンス情報を入力しません。

- コントローラのシリアル番号にロックされています

必要なライセンスの詳細については、を参照してください "SnapCenter ライセンス"。

手順1：SnapManager Suiteライセンスがインストールされているかどうかを確認します

SnapCenter の GUI を使用して、 SnapManager スイートライセンスが FAS または AFF のプライマリストレージシステムにインストールされているかどうかを表示したり、 SnapManager スイートライセンスが必要なストレージシステムを特定したりできます。SnapManager スイートのライセンスは、プライマリストレージシステム上の FAS および AFF SVM またはクラスタにのみ適用されます。

お使いのコントローラにすでに SnapManagerSuite ライセンスがある場合は、 SnapCenter の標準コントローラベースのライセンス使用権が自動的に提供されます。SnapManagerSuite ライセンスと SnapCenter 標準のコントローラベースのライセンスは同じ意味で使用されますが、同じライセンスを指します。

手順

1. 左側のナビゲーションペインで、*[ストレージシステム]*を選択します。
2. ストレージシステムページの * タイプドロップダウンから、追加したすべての SVM またはクラスタを表示するかどうかを選択します。
   - 追加されたすべての SVM を表示するには、 * ONTAP SVM * を選択します。
   - 追加されたすべてのクラスタを表示するには、 * ONTAP クラスタ * を選択します。

     クラスタ名を選択すると、そのクラスタに含まれるすべてのSVMが[Storage Virtual Machine]セクションに表示されます。
3. ストレージ接続リストで、コントローラライセンス列を探します。

   Controller License 列には、次のステータスが表示されます。

   -  FAS スイートライセンスが AFF または SnapManager プライマリストレージシステムにインストールされていることを示します。
   -  FAS スイートライセンスが AFF または SnapManager プライマリストレージシステムにインストールされていないことを示します。
   - 該当しない場合は、ストレージコントローラが Cloud Volumes ONTAP 、 ONTAP Select 、またはセカンダリストレージプラットフォーム上にあるため、 SnapManager スイートのライセンスは適用されません。

手順2：コントローラにインストールされているライセンスを特定します

ONTAP コマンドラインを使用すると、コントローラにインストールされているすべてのライセンスを表示できます。FAS または AFF システムのクラスタ管理者である必要があります。

SnapCenter の標準コントローラベースのライセンスが、 SnapManagerSuite ライセンスとしてコントローラに表示されます。

手順

1. ONTAP コマンドラインを使用してネットアップコントローラにログインします。
2. license show コマンドを入力し、出力を表示して SnapManagerSuite ライセンスがインストールされているかどうかを確認します。

出力例

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

この例では、 SnapManagerSuite ライセンスをインストールするため、 SnapCenter の追加ライセンスは必要ありません。

手順3：コントローラのシリアル番号を取得します

コントローラベースのライセンスのシリアル番号を取得するには、コントローラのシリアル番号が必要です。ONTAP コマンドラインを使用すると、コントローラのシリアル番号を取得できます。FAS または AFF システムのクラスタ管理者である必要があります。

手順

1. ONTAP コマンドラインを使用してコントローラにログインします。
2. system show -instance コマンドを入力し、出力を確認してコントローラのシリアル番号を確認します。

出力例

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. シリアル番号を記録します。

手順4：コントローラベースライセンスのシリアル番号を取得します

FAS または AFF ストレージを使用している場合、NetApp Support Siteから SnapCenter コントローラベースのライセンスを取得してから、 ONTAP コマンドラインを使用してインストールできます。

作業を開始する前に

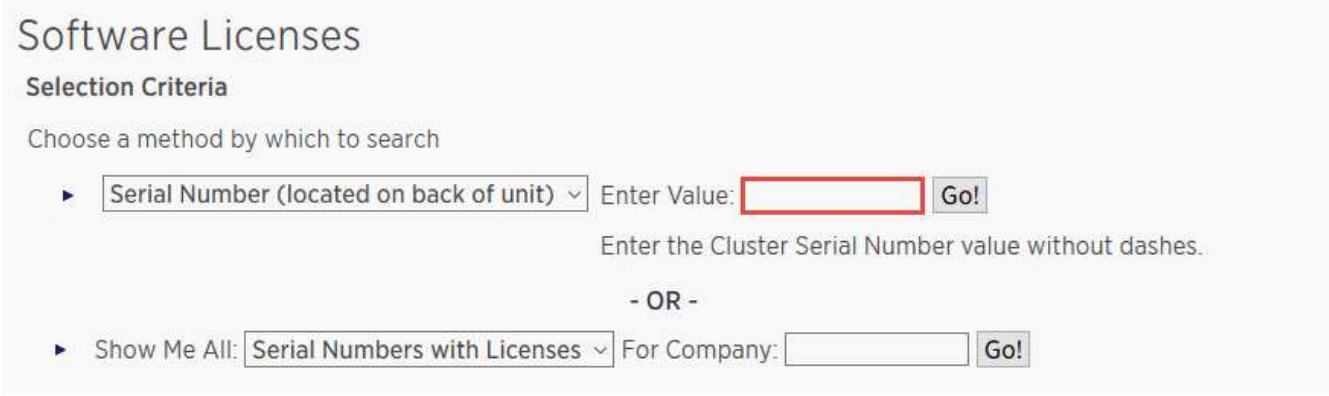
- 有効なNetApp Support Siteのログインクレデンシャルが必要です。

有効なクレデンシャルを入力しないと、検索結果は返されません。

- コントローラのシリアル番号を確認しておく必要があります。

手順

1. にログインします "NetApp Support Site"。
2. [システム] 、 [* ソフトウェアライセンス] の順に移動します。
3. [Selection Criteria]領域で、[Serial Number（located on back of unit）]が選択されていることを確認し、コントローラのシリアル番号を入力して*[Go ！]*を選択します。



指定したコントローラのライセンスのリストが表示されます。

4. SnapCenter Standard または SnapManagerSuite ライセンスを探して記録します。

手順5：コントローラベースのライセンスを追加する

FAS または AFF システムを使用していて、 SnapCenter 標準ライセンスまたは SnapManagerSuite ライセンスがある場合は、 ONTAP コマンドラインを使用して SnapCenter コントローラベースライセンスを追加できます。

作業を開始する前に

- FAS または AFF システムのクラスタ管理者である必要があります。
- SnapCenter Standard または SnapManagerSuite のライセンスが必要です。

このタスクについて

FAS または AFF ストレージを使用した SnapCenter の試用版をインストールする場合は、 Premium Bundle 評価ライセンスを取得してコントローラにインストールできます。

SnapCenter を試用版としてインストールする場合は、営業担当者にお問い合わせいただき、 Premium Bundle 評価ライセンスを取得してコントローラにインストールしてください。

手順

1. ONTAP コマンドラインを使用してネットアップクラスタにログインします。
2. SnapManagerSuite ライセンスキーを追加します。

```
system license add -license-code license_key
```

このコマンドは、 admin 権限レベルで使用できます。

3. SnapManagerSuite ライセンスがインストールされていることを確認します。

```
license show
```

ステップ6:試用版ライセンスを削除します

コントローラベースの SnapCenter 標準ライセンスを使用していて、容量ベースの試用版ライセンス (シリアル番号は「 50 」で終わる) を削除する必要がある場合は、 MySQL コマンドを使用して、試用版ライセンスを手動で削除する必要があります。SnapCenter GUI でトライアルライセンスを削除することはできません。

トライアルライセンスを手動で削除する必要があるのは、 SnapCenter の標準コントローラベースのライセンスを使用している場合のみです。SnapCenter の Standard 容量ベースのライセンスを調達し、 SnapCenter の GUI に追加すると、試用版ライセンスが自動的に上書きされます。

手順

1. SnapCenter サーバで、 PowerShell ウィンドウを開き、 MySQL パスワードをリセットします。
   a. Open-SmConnection コマンドレットを実行して、 SnapCenterAdmin アカウントの SnapCenter サーバとの接続セッションを開始します。
   b. Set-SmRepositoryPassword を実行して、 MySQL パスワードをリセットします。

      コマンドレットの詳細については、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

2. コマンドプロンプトを開き、 mysql -u root -p を実行して MySQL にログインします。

   パスワードの入力を求めるプロンプトが MySQL から表示されます。パスワードのリセット時に指定したクレデンシャルを入力します。

3. データベースから試用版ライセンスを削除します。

```
use nsm;``DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

SnapCenter の Standard 容量ベースのライセンスを追加

ONTAP Select 標準容量ライセンスは、 Cloud Volumes ONTAP プラットフォームと SnapCenter プラットフォームのデータを保護するために使用します。

容量ライセンスには次のような特徴があります。

- 51xxxxxxx の形式の 9 桁のシリアル番号で構成されます

  SnapCenter GUI を使用してライセンスを有効にするには、ライセンスのシリアル番号と有効なNetApp Support Siteのログインクレデンシャルを使用します。

- 個別の永続ライセンスとして提供され、使用済みストレージ容量または保護するデータのサイズのいずれか小さい方に基づくコストと、データは SnapCenter によって管理されます

- テラバイトあたりの利用可能容量

  たとえば、 1TB 、 2TB 、 4TB などの容量ベースのライセンスを取得できます。

- 100TB の容量が使用可能な 90 日間の試用版ライセンスです

  必要なライセンスの詳細については、を参照してください "SnapCenter ライセンス"。

SnapCenter は、管理対象の ONTAP Select および Cloud Volumes ONTAP ストレージ上で、 1 日に 1 回、午前 0 時に使用容量を自動的に計算します。Standard 容量ライセンスを使用している場合、 SnapCenter は、ライセンスで許可された合計容量から、すべてのボリュームの使用済み容量を差し引くことによって、未使用の容量を計算します。使用容量がライセンスで許可された容量を超えた場合、 SnapCenter ダッシュボードに警告が表示されます。SnapCenter で容量のしきい値と通知を設定している場合は、使用容量が指定したしきい値に達すると E メールが送信されます。

ステップ**1**：必要な容量を計算する

SnapCenter の容量ベースのライセンスを取得する前に、 SnapCenter で管理するホストの容量を計算する必要があります。

Cloud Volumes ONTAP または ONTAP Select システムのクラスタ管理者である必要があります。

このタスクについて

SnapCenter は、使用済み容量を計算します。ファイルシステムまたはデータベースのサイズが 1TB で、使用スペースが 500GB の場合、 SnapCenter は 500GB の使用容量を計算します。重複排除と圧縮のあとにボリューム容量が計算され、ボリューム全体の使用容量に基づいて算出されます。

手順

1. ONTAP コマンドラインを使用してネットアップコントローラにログインします。
2. 使用済みボリューム容量を表示するには、コマンドを入力します。

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

   2 つのボリュームの使用済み容量の合計が 5TB 未満であるため、 5TB のデータをすべて保護する場合は、 SnapCenter の容量ベースの最小ライセンス要件は 5TB です。

   ただし、合計で 5TB の使用容量のうち 2TB しか保護しない場合は、 2TB の容量ベースライセンスを取得できます。

手順**2**：容量ベースライセンスのシリアル番号を取得します

SnapCenter の容量ベースのライセンスのシリアル番号は、注文の確認やドキュメントパッケージに記載され

ています。このシリアル番号がない場合は、NetApp Support Siteから取得できます。

有効なNetApp Support Siteのログインクレデンシャルが必要です。

手順

1. にログインします "NetApp Support Site"。
2. [システム] 、 [* ソフトウェアライセンス] の順に移動します。
3. [選択基準] 領域で、 [すべてを表示：シリアル番号とライセンス] ドロップダウンメニューから **SC_standard** を選択します。

4. 会社名を入力し、* Go ！ *を選択します。

   SnapCenter ライセンスの 9 桁のシリアル番号が 51xxxxxxx の形式で表示されます。

5. シリアル番号を記録します。

ステップ**3**：ネットアップライセンスファイルを生成する

NetApp Support Site のクレデンシャルとSnapCenter ライセンスのシリアル番号をSnapCenter のGUIに入力しない場合や、SnapCenter からNetApp Support Site にインターネットアクセスできない場合は、ネットアップライセンスファイル（NLF）を生成できます。その後、SnapCenter ホストからアクセスできる場所にファイルをダウンロードして格納できます。

作業を開始する前に

- SnapCenter を ONTAP Select または Cloud Volumes ONTAP で使用する必要があります。
- 有効なNetApp Support Siteのログインクレデンシャルが必要です。
- ライセンスの 9 桁のシリアル番号を 51xxxxxxx の形式で用意しておく必要があります。

手順

1. に移動します "ネットアップライセンスファイルジェネレータ"。
2. 必要な情報を入力します。
3. [製品ライン] フィールドで、プルダウンメニューから **SnapCenter Standard (capacity based-)** を選択します。
4. [製品シリアル番号] フィールドに、 SnapCenter ライセンスのシリアル番号を入力します
5. ネットアップのデータプライバシーポリシーを読んで同意し、*[送信]*を選択します。

6. ライセンスファイルを保存し、ファイルの場所を記録します。

手順4：容量ベースのライセンスを追加する

SnapCenter を ONTAP Select プラットフォームまたは Cloud Volumes ONTAP プラットフォームで使用している場合は、 1 つ以上の SnapCenter 容量ベースのライセンスをインストールする必要があります。

作業を開始する前に

- SnapCenter 管理者ユーザとしてログインする必要があります。
- 有効なNetApp Support Siteのログインクレデンシャルが必要です。
- ライセンスの 9 桁のシリアル番号を 51xxxxxxx の形式で用意しておく必要があります。

  ネットアップライセンスファイル（ NLF ）を使用してライセンスを追加する場合は、ライセンスファイルの場所を確認しておく必要があります。

このタスクについて

設定ページでは、次のタスクを実行できます。

- ライセンスを追加します
- ライセンスの詳細を表示して、各ライセンスに関する情報を簡単に確認できます。
- ライセンス容量を更新したり、しきい値通知の設定を変更したりする場合など、既存のライセンスを置き換えるときにライセンスを変更します。
- 既存のライセンスを置き換える場合やライセンスが不要になった場合は、ライセンスを削除します。

トライアルライセンス（ 50 で終わるシリアル番号）は、 SnapCenter GUI では削除できません。購入した SnapCenter Standard 容量ベースのライセンスを追加すると、試用版ライセンスが自動的に上書きされます。

手順

1. 左側のナビゲーションペインで、*[設定]*を選択します。
2. [設定]ページで、*[ソフトウェア]*を選択します。
3. [Software]ページの[License]セクションで、**[Add]**（を選択します ）。
4. SnapCenter ライセンスの追加ウィザードで、次のいずれかの方法を選択して、追加するライセンスを取得します。

フィールド	手順
ライセンスをインポートするには、NetApp Support Site（ NSS ）のログインクレデンシャルを入力します	a. NSS のユーザ名を入力します。 b. NSS パスワードを入力します。 c. コントローラベースのライセンスのシリアル番号を入力します。

フィールド	手順
ネットアップライセンスファイル	a. ライセンスファイルの場所を参照し、選択します。 b. 「 * 開く * 」を選択します。

5. 通知ページで、 SnapCenter が E メール、 EMS 、および AutoSupport 通知を送信する容量のしきい値を入力します。

   デフォルトのしきい値は 90% です。

6. Eメール通知に使用するSMTPサーバを設定するには、**[設定]>*>**[通知サーバ設定]*を選択し、次の詳細を入力します。

フィールド	手順
E メール設定	「 * Always * 」または「 * Never * 」のいずれかを選択します。
E メールの設定を指定します	[* 常に * （ Always * ）] を選択した場合は、次のように指定します • 送信者の E メールアドレス • 受信者の E メールアドレス • オプション：デフォルトの件名を編集します デフォルトの件名は「 SnapCenter ライセンス容量通知」です。

7. 処理に失敗した場合に Event Management System （ EMS ；イベント管理システム）メッセージをストレージシステムの syslog に送信、または AutoSupport メッセージをストレージシステムに送信するには、該当するチェックボックスを選択します。AutoSupport を有効にすると、発生する可能性のある問題のトラブルシューティングに役立つことを推奨します。
8. 「 * 次へ * 」を選択します。
9. 概要を確認し、*[終了]*を選択します。

ストレージシステムをプロビジョニング

Windows ホストでストレージをプロビジョニングする

LUN ストレージを設定します

SnapCenter を使用して、 FC 接続 LUN または iSCSI 接続 LUN を設定できます。SnapCenter を使用して、既存の LUN を Windows ホストに接続することもできます。

LUN は、 SAN 構成におけるストレージの基本単位です。Windows ホストは、システム上の LUN を仮想ディスクとして認識します。詳細については、を参照してください "ONTAP 9 SAN 構成ガイド"。

iSCSI セッションを確立します

iSCSI を使用して LUN に接続する場合は、 LUN を作成して通信を有効にする前に、 iSCSI セッションを確立する必要があります。

- 始める前に *
- ストレージシステムのノードを iSCSI ターゲットとして定義しておく必要があります。
- ストレージシステムで iSCSI サービスを開始しておく必要があります。 "詳細はこちら。"
- このタスクについて *

iSCSI セッションは、 IPv6 と IPv6 のどちらか、または IPv4 と IPv4 の同じ IP バージョンの間でのみ確立できます。

iSCSI セッションの管理、およびホストとターゲットの間の通信には、両方が同じサブネット内にある場合にのみ、リンクローカル IPv6 アドレスを使用できます。

iSCSI イニシエータの名前を変更すると、 iSCSI ターゲットへのアクセスに影響します。名前を変更した場合、新しい名前が認識されるように、イニシエータがアクセスするターゲットの再設定が必要になることがあります。iSCSI イニシエータの名前を変更した場合、ホストを必ず再起動してください。

ホストに複数の iSCSI インターフェイスがある場合、最初のインターフェイスで IP アドレスを使用して SnapCenter への iSCSI セッションを確立したあとで、別の IP アドレスを使用して別のインターフェイスから iSCSI セッションを確立することはできません。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * iSCSI Session （ iSCSI セッション） * をクリックします。
  3. Storage Virtual Machine * ドロップダウンリストから、 iSCSI ターゲットの Storage Virtual Machine （ SVM ）を選択します。
  4. [**Host**] ドロップダウン・リストから ' セッションのホストを選択します
  5. [セッションの確立] をクリックします。

     セッションの確立ウィザードが表示されます。
  6. Establish Session ウィザードで ' ターゲットを指定します

フィールド	入力するコマンド
ターゲットノード名	iSCSI ターゲットのノード名 既存のターゲットノード名がある場合は、その名前が読み取り専用形式で表示されます。
ターゲットポータルのアドレス	ターゲットネットワークポータルの IP アドレス

フィールド	入力するコマンド
ターゲットポータルポート	ターゲットネットワークポータルの TCP ポート
イニシエータポータルのアドレス	イニシエータネットワークポータルの IP アドレス

7. 入力が完了したら、 * 接続 * をクリックします。

   SnapCenter が iSCSI セッションを確立します。

8. この手順を繰り返して、各ターゲットのセッションを確立します。

iSCSI セッションを切断します

複数のセッションを実行しているターゲットから iSCSI セッションを切断しなければならない場合があります。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * iSCSI Session （ iSCSI セッション） * をクリックします。
  3. Storage Virtual Machine * ドロップダウンリストから、 iSCSI ターゲットの Storage Virtual Machine （ SVM ）を選択します。
  4. [**Host**] ドロップダウン・リストから ' セッションのホストを選択します
  5. iSCSI セッションのリストから、切断するセッションを選択し、 * セッションの切断 * をクリックします。
  6. [セッションの切断] ダイアログボックスで、 [OK] をクリックします。

     SnapCenter によって iSCSI セッションが切断されます。

igroup を作成して管理します

イニシエータグループ（ igroup ）を作成して、ストレージシステム上の特定の LUN にアクセスできるホストを指定します。SnapCenter を使用して、 Windows ホストの igroup の作成、名前変更、変更、削除を行うことができます。

igroup を作成

SnapCenter を使用して、 Windows ホスト上に igroup を作成できます。igroup を LUN にマッピングすると、ディスクの作成ウィザードまたはディスク接続ウィザードでこの igroup を使用できるようになります。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts ページで、 * igroup * をクリックします。
  3. [イニシエータグループ] ページで、 [* 新規作成] をクリックします。

4. igroup の作成ダイアログボックスで、 igroup を定義します。

フィールド	手順
ストレージシステム	igroup にマッピングする LUN の SVM を選択します。
ホスト	igroup を作成するホストを選択します。
igroup 名	igroup の名前を入力します。
イニシエータ	イニシエータを選択します。
を入力します	イニシエータタイプとして、 iSCSI 、 FCP 、または混在（ FCP と iSCSI ）のいずれかを選択します。

5. 入力に問題がなければ、「 * OK * 」をクリックします。

   SnapCenter により、ストレージシステムに igroup が作成されます。

igroup の名前を変更する

SnapCenter を使用して、既存の igroup の名前を変更できます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts ページで、 * igroup * をクリックします。
  3. イニシエータグループページで、 * Storage Virtual Machine * フィールドをクリックして使用可能な SVM のリストを表示し、名前を変更する igroup の SVM を選択します。
  4. SVM の igroup のリストで、名前を変更する igroup を選択し、 * Rename * をクリックします。
  5. igroup の名前変更ダイアログボックスで、 igroup の新しい名前を入力し、 * 名前の変更 * をクリックします。

igroup を変更する

SnapCenter を使用すると、既存の igroup にイニシエータを追加できます。igroup の作成時に追加できるホストは 1 つだけです。クラスタに対して igroup を作成するには、 igroup を変更して他のノードをその igroup に追加します。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts ページで、 * igroup * をクリックします。
  3. イニシエータグループページで、 * Storage Virtual Machine * フィールドをクリックして使用可能な SVM のドロップダウンリストを表示し、変更する igroup の SVM を選択します。

4. igroup のリストで igroup を選択し、 * イニシエータを igroup に追加 * をクリックします。
5. ホストを選択します。
6. イニシエータを選択し、 * OK * をクリックします。

igroup を削除する

SnapCenter を使用して、不要になった igroup を削除できます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts ページで、 * igroup * をクリックします。
  3. イニシエータグループページで、 * Storage Virtual Machine * フィールドをクリックして使用可能な SVM のドロップダウンリストを表示し、削除する igroup の SVM を選択します。
  4. SVM の igroup のリストで、削除する igroup を選択し、 * Delete * をクリックします。
  5. igroup の削除ダイアログボックスで、 * OK * をクリックします。

     SnapCenter によって igroup が削除されます。

ディスクを作成および管理する

Windows ホストは、ストレージシステム上の LUN を仮想ディスクとして認識します。SnapCenter を使用して、 FC 接続 LUN または iSCSI 接続 LUN を作成および設定できます。

- SnapCenter では基本ディスクのみがサポートされます。ダイナミックディスクはサポートされていません。
- GPT には、 NTFS または CSVFS でフォーマットされたボリュームとマウントパスが 1 つのボリュームを含むデータパーティションと MBR 1 つのプライマリパーティションのみが許可されます。
- サポートされるパーティションスタイル： GPT 、 MBR 。 VMware UEFI VM では、 iSCSI ディスクのみがサポートされます

> SnapCenter では、ディスク名の変更はサポートされていません。SnapCenter で管理しているディスクの名前を変更すると、 SnapCenter 処理は正常に終了しません。

ホスト上のディスクを表示します

SnapCenter で管理している各 Windows ホスト上のディスクを表示できます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します

     ディスクのリストが表示されます。

クラスタディスクを表示します

SnapCenter で管理しているクラスタ上のクラスタディスクを表示できます。クラスタ化されたディスクは、 Hosts （ホスト）ドロップダウンからクラスタを選択した場合にのみ表示されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからクラスタを選択します

     ディスクのリストが表示されます。

FC 接続または **iSCSI** 接続の **LUN** またはディスクを作成します

Windows ホストは、ストレージシステム上の LUN を仮想ディスクとして認識します。SnapCenter を使用して、 FC 接続 LUN または iSCSI 接続 LUN を作成および設定できます。

SnapCenter の外部でディスクを作成してフォーマットする場合は、 NTFS と CSVFS ファイルシステムのみがサポートされます。

- 必要なもの *
- ストレージシステム上に LUN 用のボリュームを作成しておく必要があります。

  このボリュームには、 SnapCenter で作成した LUN のみを格納します。

  > SnapCenter で作成したクローンボリュームには、クローンがすでにスプリットされている場合を除き、 LUN を作成することはできません。

- ストレージシステムで FC サービスまたは iSCSI サービスを開始しておく必要があります。
- iSCSI を使用している場合は、ストレージシステムとの iSCSI セッションを確立しておく必要があります。
- SnapCenter Plug-ins Package for Windows は、ディスクを作成するホストにのみインストールする必要があります。
- このタスクについて *
- Windows Server フェイルオーバークラスタ内のホストで共有する場合を除き、 LUN を複数のホストに接続することはできません。
- Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）を使用する Windows Server フェイルオーバークラスタ内のホストで LUN を共有する場合、クラスタグループを所有するホストにディスクを作成する必要があります。
- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します
  4. [新規作成（ New ）] をクリックする。

Create Disk （ディスクの作成）ウィザードが開きます。

5. LUN Name ページで、 LUN を特定します。

フィールド	手順
ストレージシステム	LUN の SVM を選択します。
LUN パス	「 * Browse * 」をクリックして、 LUN を含むフォルダのフルパスを選択します。
LUN 名	LUN の名前を入力します。
クラスタサイズ	クラスタの LUN のブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティングシステムとアプリケーションによって異なります。
LUN ラベル	必要に応じて、 LUN の説明を入力します。

6. ディスクタイプページで、ディスクタイプを選択します。

選択するオプション	状況
専用ディスク	LUN にアクセスできるホストは 1 つだけです。 [* リソースグループ *] フィールドは無視してください。
共有ディスク	Windows Server フェイルオーバークラスタ内のホストで LUN を共有します。 [* リソースグループ *] フィールドにクラスタリソースグループの名前を入力します。ディスクはフェイルオーバークラスタ内の 1 つのホストだけに作成する必要があります。
Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）	CSV を使用する Windows Server フェイルオーバークラスタ内のホストで LUN を共有します。 [* リソースグループ *] フィールドにクラスタリソースグループの名前を入力します。ディスクを作成するホストがクラスタグループの所有者であることを確認します。

7. ドライブのプロパティページで、ドライブのプロパティを指定します。

プロパティ（ **Property** ）	説明
マウントポイントの自動割り当て	SnapCenter では、システムドライブに基づいてボリュームマウントポイントが自動的に割り当てられます。 たとえば、システムドライブが C: の場合、自動割り当てでは C: ドライブ (C:\scmnpt) の下にボリュームマウントポイントが作成されます。 自動割り当ては共有ディスクではサポートされません。
ドライブ文字を割り当てます	隣接するドロップダウンリストで選択したドライブにディスクをマウントします。
ボリュームマウントポイントを使用する	隣接するフィールドで指定したドライブパスにディスクをマウントします。 ボリュームマウントポイントのルートは、ディスクを作成するホストが所有している必要があります。
ドライブレターまたはボリュームマウントポイントを割り当てないでください	ディスクを Windows で手動でマウントする場合は、このオプションを選択します。
LUNサイズ	LUN のサイズを 150MB 以上指定します。 ドロップダウンリストから MB 、 GB 、または TB を選択します。
この LUN をホストしているボリュームにシンプロビジョニングを使用します	LUN をシンプロビジョニングします。 シンプロビジョニングでは、ストレージスペースが必要なときに必要な分だけ割り当てられるため、 LUN は使用可能な最大容量まで効率的に拡張されます。 必要になるすべての LUN ストレージに対応できるだけの十分なスペースがボリュームにあることを確認してください。

プロパティ（ **Property** ）	説明
パーティションタイプを選択します	GUID パーティションテーブルの場合は GPT パーティション、マスターブートレコードの場合は MBR パーティションを選択します。 MBR パーティションを Windows Server フェイルオーバークラスタで使用した場合、原因のミスアライメントが発生することがあります。 UEFI （ Unified Extensible Firmware Interface ）パーティションディスクはサポートされていません。

8. LUN のマッピングページで、ホストの iSCSI イニシエータまたは FC イニシエータを選択します。

フィールド	手順
ホスト	クラスタグループ名をダブルクリックし、ドロップダウンリストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。 このフィールドは、 Windows Server フェイルオーバークラスタ内のホストで LUN を共有する場合にのみ表示されます。
ホストイニシエータを選択します	Fibre Channel * または * iSCSI * を選択し、ホスト上のイニシエータを選択します。 FC で Multipath I/O （ MPIO ；マルチパス I/O ）を使用する場合は、 FC イニシエータを複数選択できます。

9. Group Type ページで、既存の igroup を LUN にマッピングするか、新しい igroup を作成するかを指定します。

選択するオプション	状況
選択したイニシエータ用に新しい igroup を作成します	選択したイニシエータ用に新しい igroup を作成します。

選択するオプション	状況
既存の igroup を選択するか、選択したイニシエータ用に新しい igroup を指定します	選択したイニシエータ用に既存の igroup を指定するか、指定した名前で新しい igroup を作成します。 igroup name * フィールドに igroup 名を入力します。既存の igroup 名の最初の数文字を入力すると、残りの文字が自動的に入力されます。

10. [概要] ページで選択内容を確認し、 [完了] をクリックします。

    SnapCenter によって LUN が作成され、ホスト上の指定したドライブまたはドライブパスに接続されます。

ディスクのサイズ変更

ストレージシステムのニーズの変化に応じて、ディスクのサイズを拡張または縮小できます。

- このタスクについて *
- シンプロビジョニングされた LUN の場合、 ONTAP の LUN ジオメトリサイズは最大サイズとして表示されます。
- シックプロビジョニング LUN の場合、拡張可能なサイズ（ボリューム内の使用可能なサイズ）が最大サイズとして表示されます。
- MBR パーティション方式を使用した LUN の場合、最大サイズは 2TB です。
- GPT パーティション方式を使用した LUN の場合、ストレージシステムの最大サイズは 16TB です。
- LUN のサイズを変更する前に Snapshot コピーを作成しておくことを推奨します。
- LUN のサイズの変更前に作成された Snapshot コピーから LUN をリストアすると、 SnapCenter によって LUN のサイズが Snapshot コピーのサイズに自動的に変更されます。

  リストア処理のあと、サイズ変更後に LUN に追加されたデータを、サイズ変更後に作成された Snapshot コピーからリストアする必要があります。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. ホストドロップダウンリストからホストを選択します。

     ディスクのリストが表示されます。

  4. サイズを変更するディスクを選択し、 * サイズ変更 * をクリックします。
  5. ディスクのサイズ変更ダイアログボックスで、スライダツールを使用してディスクの新しいサイズを指定するか、サイズフィールドに新しいサイズを入力します。

サイズを手動で入力する場合は、 [縮小] または [展開] ボタンを適切に有効にする前に、 [サイズ] フィールドの外側をクリックする必要があります。また、単位を指定するには、 MB 、 GB 、または TB をクリックする必要があります。

6. 入力内容に問題がなければ、必要に応じて、 [* 縮小（ * Shrink ）] または [* 展開（ * Expand ）] をクリックします。

   SnapCenter はディスクのサイズを変更します。

ディスクを接続します

ディスク接続ウィザードを使用して、既存の LUN をホストに接続したり、切断された LUN を再接続したりできます。

- 必要なもの *
- ストレージシステムで FC サービスまたは iSCSI サービスを開始しておく必要があります。
- iSCSI を使用している場合は、ストレージシステムとの iSCSI セッションを確立しておく必要があります。
- Windows Server フェイルオーバークラスタ内のホストで共有する場合を除き、 LUN を複数のホストに接続することはできません。
- Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）を使用する Windows Server フェイルオーバークラスタ内のホストで LUN を共有する場合、クラスタグループを所有するホストにディスクを接続する必要があります。
- Plug-in for Windows をインストールする必要があるのは、ディスクを接続するホストだけです。
- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します
  4. [接続] をクリックします。

     ディスクの接続ウィザードが開きます。

  5. LUN Name ページで、接続先の LUN を特定します。

フィールド	手順
ストレージシステム	LUN の SVM を選択します。
LUN パス	[* Browse] をクリックして、 LUN を含むボリュームの完全パスを選択します。
LUN 名	LUN の名前を入力します。

フィールド	手順
クラスタサイズ	クラスタの LUN のブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティングシステムとアプリケーションによって異なります。
LUN ラベル	必要に応じて、 LUN の説明を入力します。

6. ディスクタイプページで、ディスクタイプを選択します。

選択するオプション	状況
専用ディスク	LUN にアクセスできるホストは 1 つだけです。
共有ディスク	Windows Server フェイルオーバークラスタ内のホストで LUN を共有します。 ディスクはフェイルオーバークラスタ内の 1 つのホストだけに接続します。
Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）	CSV を使用する Windows Server フェイルオーバークラスタ内のホストで LUN を共有します。 ディスクを接続するホストがクラスタグループの所有者であることを確認します。

7. ドライブのプロパティページで、ドライブのプロパティを指定します。

プロパティ（ **Property** ）	説明
自動割り当て	システムドライブに基づいて、 SnapCenter で自動的にボリュームマウントポイントを割り当てます。 たとえば、システムドライブが C: の場合、自動割り当てプロパティは C: ドライブ (C:\scmnpt) の下にボリュームマウントポイントを作成します。 自動割り当てプロパティは共有ディスクではサポートされません。
ドライブ文字を割り当てます	ドロップダウンリストで選択したドライブにディスクをマウントします。

プロパティ（ **Property** ）	説明
ボリュームマウントポイントを使用する	フィールドで指定したドライブパスにディスクをマウントします。 ボリュームマウントポイントのルートは、ディスクを作成するホストが所有している必要があります。
ドライブレターまたはボリュームマウントポイントを割り当てないでください	ディスクを Windows で手動でマウントする場合は、このオプションを選択します。

8. LUN のマッピングページで、ホストの iSCSI イニシエータまたは FC イニシエータを選択します。

フィールド	手順
ホスト	クラスタグループ名をダブルクリックし、ドロップダウンリストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。 このフィールドは、 Windows Server フェイルオーバークラスタ内のホストで LUN を共有する場合にのみ表示されます。
ホストイニシエータを選択します	Fibre Channel * または * iSCSI * を選択し、ホスト上のイニシエータを選択します。 FC で MPIO を使用している場合は、 FC イニシエータを複数選択できます。

9. Group Type ページで、既存の igroup を LUN にマッピングするか、新しい igroup を作成するかを指定します。

選択するオプション	状況
選択したイニシエータ用に新しい igroup を作成します	選択したイニシエータ用に新しい igroup を作成します。
既存の igroup を選択するか、選択したイニシエータ用に新しい igroup を指定します	選択したイニシエータ用に既存の igroup を指定するか、指定した名前で新しい igroup を作成します。 igroup name * フィールドに igroup 名を入力します。既存の igroup 名の最初の数文字を入力すると、残りの文字が自動的に入力されます。

10. [概要] ページで選択内容を確認し、 [完了] をクリックします。

    SnapCenter は、ホスト上の指定したドライブまたはドライブパスに LUN を接続します。

ディスクの切断

LUN は内容を残したままホストから切断できます。ただし、スプリットせずにクローンを切断した場合、クローンの内容は失われます。

- 必要なもの *
- LUN を使用しているアプリケーションがないことを確認します。
- LUN が監視ソフトウェアで監視されていないことを確認します。
- LUN が共有されている場合は、 LUN からクラスタリソースの依存関係を解除し、クラスタ内のすべてのノードの電源がオンで正常に機能しており、 SnapCenter からアクセスできることを確認します。
- このタスクについて *

SnapCenter が作成した FlexClone ボリュームの LUN を切断した場合、そのボリュームに他の LUN が接続されていなければ、 SnapCenter はボリュームを削除します。この場合、 LUN が切断される前に、 FlexClone ボリュームが削除される可能性があることを警告するメッセージが SnapCenter に表示されます。

FlexClone ボリュームが自動で削除されないようにするには、最後の LUN を切断する前にボリュームの名前を変更します。ボリュームの名前を変更するときは、最後の 1 文字だけでなく複数の文字を変更してください。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します

     ディスクのリストが表示されます。
  4. 切断するディスクを選択し、 * 切断 * をクリックします。
  5. [ディスクの切断] ダイアログボックスで、 [OK] をクリックします。

     SnapCenter によってディスクが切断されます。

ディスクを削除します

不要になったディスクは削除できます。削除したディスクは復元できません。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します

     ディスクのリストが表示されます。
  4. 削除するディスクを選択し、 * 削除 * をクリックします。
  5. [ディスクの削除] ダイアログボックスで、 [OK] をクリックします。

SnapCenter によってディスクが削除されます。

SMB 共有を作成および管理する

Storage Virtual Machine （ SVM ）上に SMB3 共有を設定するには、 SnapCenter ユーザインターフェイスまたは PowerShell コマンドレットを使用できます。

* ベストプラクティス： * SnapCenter に付属のテンプレートを利用して共有の設定を自動化できるため、コマンドレットの使用を推奨します。

テンプレートには、ボリュームおよび共有の設定に関するベストプラクティスが組み込まれています。テンプレートは、 SnapCenter Plug-ins Package for Windows のインストールフォルダの Templates フォルダにあります。

必要に応じて、提供されているモデルに従って独自のテンプレートを作成できます。カスタムテンプレートを作成する場合は、コマンドレットのドキュメントでパラメータを確認してください。

SMB 共有を作成

SnapCenter 共有ページを使用すると、 Storage Virtual Machine （ SVM ）に SMB3 共有を作成できます。

SnapCenter を使用して、 SMB 共有上のデータベースをバックアップすることはできません。SMB のサポートはプロビジョニングのみに限定されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. ホストページで、 * 共有 * をクリックします。
  3. Storage Virtual Machine * ドロップダウンリストから SVM を選択します。
  4. [新規作成（ New ）] をクリックする。

     [新しい共有] ダイアログが開きます。
  5. [新しい共有] ダイアログで、共有を定義します。

フィールド	手順
説明	共有の説明を入力します。

フィールド	手順
共有名	共有名を入力します（例： test_share ）。 入力した共有の名前はボリューム名としても使用されます。 共有名： • UTF-8 文字列である必要があります。 • 0x00から0x1Fまでの制御文字、0x22（二重引用符）、および特殊文字は使用できません `\ / [ ] : (vertical bar) < > + = ; , ?`
共有パス	• フィールド内をクリックして、新しいファイルシステムパス（/ など）を入力します。 • フィールドをダブルクリックして、既存のファイルシステムパスのリストから選択します。

6. 入力に問題がなければ、「 * OK * 」をクリックします。

   SnapCenter により、 SVM に SMB 共有が作成されます。

SMB 共有を削除する

不要になった SMB 共有は削除できます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. ホストページで、 * 共有 * をクリックします。
  3. 共有ページで、 * Storage Virtual Machine * フィールドをクリックして、ドロップダウンと使用可能な Storage Virtual Machine （ SVM ）のリストを表示し、削除する共有の SVM を選択します。
  4. SVM 上の共有のリストから削除する共有を選択し、 * Delete * をクリックします。
  5. 共有の削除ダイアログボックスで、 * OK * をクリックします。

     SnapCenter によって SVM から SMB 共有が削除されます。

ストレージシステム上のスペースを再生する

ファイルが削除または変更された場合、 NTFS は LUN 上の使用可能なスペースを追跡しますが、この情報はストレージシステムには報告されません。新たに解放されたブロックがストレージで空きスペースとしてマークされるようにするには、 Plug-in for Windows ホストでスペース再生用 PowerShell コマンドレットを実行します。

リモートのプラグインホストでコマンドレットを実行する場合は、 SnapCenterOpen-SMConnection コマンドレットを実行して SnapCenter サーバへの接続を確立する必要があります。

- 必要なもの *
- リストア処理を実行する前に、スペース再生プロセスが完了していることを確認する必要があります。
- Windows Server フェイルオーバークラスタ内のホストで LUN を共有している場合は、クラスタグループを所有するホストでスペース再生を実行する必要があります。
- ストレージのパフォーマンスを最適化するには、できるだけ頻繁にスペース再生を実行します。

  NTFS ファイルシステム全体がスキャンされたことを確認してください。

- このタスクについて *
- スペース再生には時間がかかり、 CPU を大量に消費するため、通常はストレージシステムと Windows ホストがあまり使用されていない時間帯に実行することを推奨します。
- 使用可能なほぼすべてのスペースが再生されますが、 100% ではありません。
- スペース再生の実行中にディスクのデフラグは実行しないでください。

  再生プロセスの速度が低下する可能性があります。

- ステップ *

アプリケーションサーバの PowerShell コマンドプロンプトで、次のコマンドを入力します。

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path は、 LUN にマッピングされているドライブパスです。

PowerShell コマンドレットを使用してストレージをプロビジョニング

SnapCenter GUI を使用してホストのプロビジョニングやスペース再生のジョブを実行しない場合は、 SnapCenter Plug-in for Microsoft Windows から提供される PowerShell コマンドレットを使用できます。コマンドレットは直接使用できるほか、スクリプトに追加することもできます。

リモートのプラグインホストでコマンドレットを実行する場合は、 SnapCenter Open-SMConnection コマンドレットを実行して SnapCenter サーバへの接続を確立する必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapDrive for Windows をサーバから削除したために SnapCenter PowerShell コマンドレットが破損した場合は、を参照してください "SnapDrive コマンドレットは、 SnapCenter for Windows をアンインストールすると解除されます"。

VMware 環境でストレージをプロビジョニング

VMware環境でSnapCenter Plug-in for Microsoft Windowsを使用すると、LUNの作成と管

理、およびSnapshotコピーの管理を行うことができます。

サポートされている **VMware** ゲスト **OS** プラットフォーム

- サポートされている Windows Server のバージョン
- Microsoft クラスタ構成

  VMware 上でサポートされるノードは、 Microsoft iSCSI Software Initiator を使用する場合は最大 16 、 FC を使用する場合は最大 2 つです

- RDM LUN

  通常の RDMS では、最大 56 の RDM LUN と 4 つの LSI Logic SCSI コントローラがサポートされます。 VMware VM MSCS のボックスツーボックスの Plug-in for Windows 構成では、最大 42 の RDM LUN と 3 つの LSI Logic SCSI コントローラがサポートされます

  VMware 準仮想 SCSI コントローラをサポートします。RDM ディスクでは 256 本のディスクをサポートできます。

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

VMware ESXi サーバ関連の制限事項

- ESXi クレデンシャルを使用して仮想マシン上の Microsoft クラスタに Plug-in for Windows をインストールすることはできません。

  クラスタ化された仮想マシンに Plug-in for Windows をインストールする場合、 vCenter のクレデンシャルを使用する必要があります。

- クラスタ化されたすべてのノードで、同じクラスタディスクに同じ（仮想 SCSI アダプタ上の）ターゲット ID を使用する必要があります。
- Plug-in for Windows を使用せずに RDM LUN を作成した場合、プラグインサービスを再起動して、新しく作成したディスクを認識させる必要があります。
- VMware ゲスト OS で iSCSI イニシエータと FC イニシエータを同時に使用することはできません。

SnapCenter RDM の処理に必要な最小限の **vCenter** 権限

ゲスト OS で RDM の処理を実行するには、ホストに対する次の vCenter 権限が必要です。

- データストア：ファイルを削除します
- ホスト： [Configuration] > [Storage Partition] の順に選択します
- 仮想マシン：構成

これらの権限は、 Virtual Center Server レベルのロールに割り当てる必要があります。これらの権限を割り当てるロールは、 root 権限を持たないユーザには割り当てることができません。

これらの権限を割り当てたら、ゲスト OS に Plug-in for Windows をインストールできます。

Microsoft クラスタで FC RDM LUN を管理します

Plug-in for Windows を使用して、 FC RDM LUN を使用する Microsoft クラスタを管理することができます。そのためには、プラグインの外部で共有 RDM クォーラムと共有ストレージを作成し、クラスタ内の仮想マシンにディスクを追加しておく必要があります。

ESXi 5.5 以降では、 ESX の iSCSI ハードウェアや FCoE ハードウェアを使用して Microsoft クラスタを管理することもできます。Plug-in for Windows では、設定作業なしで Microsoft クラスタがサポートされます。

要件

Plug-in for Windows では、特定の構成要件を満たしていれば、 2 つの異なる ESX サーバまたは ESXi サーバに属する 2 台の仮想マシンで構成された Microsoft クラスタで FC RDM LUN の使用がサポートされます。この構成は、クラスタ全体のボックスとも呼ばれます。

- 仮想マシン（ VM ）で同じバージョンの Windows Server を実行している必要があります。
- ESX サーバまたは ESXi サーバのバージョンが VMware の各親ホストで同じである必要があります。
- 各親ホストに少なくとも 2 つのネットワークアダプタが必要です。
- 2 台の ESX サーバまたは ESXi サーバ間で VMFS （ VMware Virtual Machine File System ）データストアを少なくとも 1 つ共有している必要があります。
- VMware では、共有データストアを FC SAN 上に作成することを推奨しています。

  共有データストアは、必要に応じて iSCSI で作成することもできます。
- 共有 RDM LUN が物理互換モードである必要があります。
- 共有 RDM LUN は、 Plug-in for Windows の外部で手動で作成する必要があります。

  共有ストレージに仮想ディスクを使用することはできません。
- クラスタ内の各仮想マシンに、 SCSI コントローラが物理互換モードで設定されている必要があります。

  Windows Server 2008 R2 では、各仮想マシンに LSI Logic SAS SCSI コントローラを構成する必要があります。LSI Logic SAS タイプのコントローラが 1 台しかなく、すでに C ：ドライブに接続されている場合、そのコントローラを共有 LUN で使用することはできません。

  準仮想化タイプの SCSI コントローラは VMware Microsoft クラスタではサポートされていません。

  > 物理互換モードで仮想マシン上の共有 LUN に SCSI コントローラを追加する場合は、 VMware Infrastructure Client の * Create a new disk* オプションではなく、 * Raw Device Mappings * （ RDM ）オプションを選択する必要があります。

- Microsoft 仮想マシンクラスタを VMware クラスタに含めることはできません。
- Microsoft クラスタに属する仮想マシンに Plug-in for Windows をインストールする場合は、 ESX または ESXi のクレデンシャルではなく vCenter のクレデンシャルを使用する必要があります。
- Plug-in for Windows では、複数のホストのイニシエータを含む igroup を作成することはできません。

  共有クラスタディスクとして使用する RDM LUN を作成する前に、すべての ESXi ホストのイニシエータを含む igroup をストレージコントローラ上に作成しておく必要があります。

- ESXi 5.0 で FC イニシエータを使用して RDM LUN を作成します。

  RDM LUN を作成すると、 ALUA でイニシエータグループが作成されます。

制限

Plug-in for Windows では、異なる ESX サーバまたは ESXi サーバに属する異なる仮想マシン上の FC / iSCSI RDM LUN を使用する Microsoft クラスタがサポートされます。

この機能は、 ESX 5.5i よりも前のリリースではサポートされていません。

- Plug-in for Windows では、 ESX iSCSI および NFS データストア上のクラスタはサポートされません。
- Plug-in for Windows では、クラスタ環境でのイニシエータの混在はサポートされません。

  イニシエータは FC と Microsoft iSCSI のどちらか一方にする必要があります。

- ESX iSCSI イニシエータと HBA は、 Microsoft クラスタ内の共有ディスクではサポートされません。
- Plug-in for Windows では、 Microsoft クラスタに属する仮想マシンの vMotion による移行はサポートされません。
- Plug-in for Windows では、 Microsoft クラスタ内の仮想マシンでの MPIO はサポートされません。

共有 **FC RDM LUN** を作成

FC RDM LUN を使用して Microsoft クラスタ内のノード間でストレージを共有する前に、共有クォーラムディスクと共有ストレージディスクを作成し、それらをクラスタ内の両方の仮想マシンに追加しておく必要があります。

共有ディスクの作成に Plug-in for Windows は使用しません。共有 LUN を作成し、クラスタ内の各仮想マシンに追加する必要があります。
詳細については、を参照してください "物理ホスト間で仮想マシンをクラスタ化します"。

SnapCenter サーバとの安全な MySQL 接続を設定します

SnapCenter サーバと MySQL サーバ間の通信をスタンドアロン構成または Network Load Balancing （ NLB ）構成で保護する場合は、 Secure Sockets Layer （ SSL ）証明書とキーファイルを生成できます。

スタンドアロン SnapCenter サーバ構成用にセキュアな MySQL 接続を設定します

SnapCenter サーバと MySQL サーバ間の通信を保護する場合は、 Secure Sockets Layer （ SSL ）証明書およびキーファイルを生成できます。証明書とキーファイルは MySQL Server と SnapCenter Server で設定する必要があります。

次の証明書が生成されます。

- CA 証明書
- サーバのパブリック証明書と秘密鍵ファイル

- クライアントのパブリック証明書と秘密鍵ファイル
- 手順 *

1. openssl コマンドを使用して、 Windows 上の MySQL サーバおよびクライアントの SSL 証明書とキーファイルをセットアップします。

   詳細については、を参照してください "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

   > サーバ証明書、クライアント証明書、およびキーファイルに使用される共通名の値は、 CA 証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、 OpenSSL を使用してコンパイルされたサーバーの証明書とキーファイルは失敗します。

   * ベストプラクティス： * サーバ証明書の共通名として、サーバの Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用してください。

2. SSL 証明書とキーファイルを MySQL Data フォルダにコピーします。

   MySQLデータフォルダのデフォルトのパスはです `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`。

3. MySQL サーバ構成ファイル（ my.in ）で、 CA 証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

   MySQLサーバのデフォルトの構成ファイル（my.in）のパスはです `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`。

   > MySQL サーバ構成ファイル（ my.in ）の [mysqld] セクションで、 CA 証明書、サーバパブリック証明書、サーバ秘密鍵のパスを指定する必要があります。

   MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、クライアントパブリック証明書、およびクライアント秘密鍵のパスを指定する必要があります。

   次の例は、デフォルトのフォルダにあるmy.iniファイルの[mysqld]セクションにコピーされた証明書とキーファイルを示しています `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

次の例は、 my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. インターネットインフォメーションサーバー (IIS) で SnapCenter サーバーの Web アプリケーションを停止します。
5. MySQL サービスを再起動します。
6. web.config ファイルで MySQLProtocol キーの値を更新します。

   次の例は、 web.config ファイルで更新された MySQLProtocol キーの値を示しています。

```
<add key="MySQLProtocol" value="SSL" />
```

7. my.ini ファイルの [client] セクションに指定されたパスで web.config ファイルを更新します。

   次の例は、 my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

+

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem" />
```

+

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem" />
```

1. IIS で SnapCenter サーバー Web アプリケーションを起動します。

HA 構成用にセキュアな MySQL 接続を設定します

SnapCenter サーバと MySQL サーバ間の通信を保護する場合は、ハイアベイラビリティ（ HA ）ノードの両方について Secure Sockets Layer （ SSL ）証明書とキーファイルを生成できます。証明書とキーファイルは MySQL サーバと HA ノードで設定する必要があります。

次の証明書が生成されます。

- CA 証明書

  いずれかの HA ノードで CA 証明書が生成され、この CA 証明書がもう一方の HA ノードにコピーされます。

- 両方の HA ノードのサーバパブリック証明書とサーバの秘密鍵ファイル
- 両方の HA ノードのクライアントパブリック証明書とクライアント秘密鍵ファイル
- 手順 *

1. 最初の HA ノードに対して、 openssl コマンドを使用して、 Windows 上の MySQL サーバおよびクライアントの SSL 証明書とキーファイルをセットアップします。

   詳細については、を参照してください "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

   > サーバ証明書、クライアント証明書、およびキーファイルに使用される共通名の値は、 CA 証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、 OpenSSL を使用してコンパイルされたサーバーの証明書とキーファイルは失敗します。

   * ベストプラクティス： * サーバ証明書の共通名として、サーバの Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用してください。

2. SSL 証明書とキーファイルを MySQL Data フォルダにコピーします。

   MySQL のデフォルトのフォルダパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\\です 。

3. MySQL サーバ構成ファイル（ my.in ）で、 CA 証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

   デフォルトの MySQL サーバ構成ファイル（ my.in l ）のパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\my.in です

   > MySQL サーバ構成ファイル（ my.in ）の [mysqld] セクションで、 CA 証明書、サーバパブリック証明書、サーバ秘密鍵のパスを指定する必要があります。

   MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、クライアントパブリック証明書、およびクライアント秘密鍵のパスを指定する必要があります。

   次の例は、 my.ini ファイルの mysqld セクションにコピーされた証明書とキーファイルを示しています。このデフォルトフォルダは C ： /ProgramData\NetApp/SnapCenter /MySQL Data\Data です。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

次の例は、 my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. 2 つ目の HA ノードについて、 CA 証明書をコピーし、サーバのパブリック証明書、サーバの秘密鍵ファイル、クライアントのパブリック証明書、およびクライアントの秘密鍵ファイルを生成します。次の手順を実行します。

   a. 1 つ目の HA ノードで生成された CA 証明書を、 2 つ目の NLB ノードの MySQL Data フォルダにコピーします。

      MySQL のデフォルトのフォルダパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\\です 。

      再度 CA 証明書を作成することはできません。作成するのは、サーバのパブリック証明書、クライアントのパブリック証明書、サーバの秘密鍵ファイル、およびクライアントの秘密鍵ファイルだけにしてください。

   b. 最初の HA ノードに対して、 openssl コマンドを使用して、 Windows 上の MySQL サーバおよびクライアントの SSL 証明書とキーファイルをセットアップします。

      "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

      サーバ証明書、クライアント証明書、およびキーファイルに使用される共通名の値は、 CA 証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、 OpenSSL を使用してコンパイルされたサーバーの証明書とキーファイルは失敗します。

サーバ証明書の共通名としてサーバ FQDN を使用することを推奨します。

c. SSL 証明書とキーファイルを MySQL Data フォルダにコピーします。

d. MySQL サーバ構成ファイル（ my.in ）で、 CA 証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

MySQL サーバ構成ファイル（ my.in ）の [mysqld] セクションで、 CA 証明書、サーバパブリック証明書、サーバ秘密鍵のパスを指定する必要があります。

MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、クライアントパブリック証明書、およびクライアント秘密鍵のパスを指定する必要があります。

次の例は、 my.ini ファイルの mysqld セクションにコピーされた証明書とキーファイルを示しています。このデフォルトフォルダは C ： /ProgramData\NetApp/SnapCenter /MySQL Data\Data です。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

次の例は、 my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. 両方の HA ノードのインターネットインフォメーションサーバ (IIS) で、 SnapCenter サーバ Web アプリケーションを停止します。

6. 両方の HA ノードで MySQL サービスを再起動します。

7. 両方の HA ノードについて、 web.config ファイルで MySQLProtocol キーの値を更新します。

   次の例は、 web.config ファイルで更新された MySQLProtocol キーの値を示しています。

```
<add key="MySQLProtocol" value="SSL" />
```

8. 両方の HA ノードについて、 my.ini ファイルの [client] セクションで指定したパスで web.config ファイルを更新します。

   次の例は、 my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

+

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

+

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

1. 両方の HA ノードの IIS で SnapCenter サーバー Web アプリケーションを起動します。
2. いずれかの HA ノードで Set-SmRepositoryConfig-RebuildSlave -Force PowerShell コマンドレットを使用して、両方の HA ノードでセキュアな MySQL レプリケーションを確立します。

   レプリケーションステータスが正常であっても、 -Force オプションを使用してスレーブリポジトリを再構築できます。

インストール中に **Windows** ホストで有効になる機能

SnapCenter Server インストーラを使用すると、インストール中に Windows ホストで Windows の機能とロールが有効になります。これらの情報は、トラブルシューティングやホストシステムのメンテナンスに役立つ場合があります。

カテゴリ	フィーチャー（ **Feature** ）
Web サーバ	• インターネットインフォメーションサービス • World Wide Web Services の略 • Common HTTP Features （共通 HTTP 機能） ◦ 既定のドキュメント ◦ ディレクトリの参照 ◦ HTTP エラー ◦ HTTP リダイレクション ◦ 静的なコンテンツ ◦ WebDAV 発行 • 正常性と診断 ◦ カスタムログ ◦ HTTP ログ ◦ ログツール ◦ Request Monitor サービスの略 ◦ トレース • パフォーマンス機能 ◦ 静的なコンテンツの圧縮 • セキュリティ ◦ IP セキュリティ ◦ Basic Authentication の略 ◦ 一元的な SSL 証明書のサポート ◦ クライアント証明書マッピング認証 ◦ IIS クライアント証明書マッピング認証 ◦ IP およびドメインの制限 ◦ 要求フィルタリング ◦ URL 承認 ◦ Windows 認証 • アプリケーション開発機能 ◦ .NET 拡張機能 4.5 ◦ アプリケーションの初期化 ◦ ASP.NET 4.7.2. ◦ サーバー側インクルード ◦ WebSocket プロトコル 管理ツール IIS Management Console の略

カテゴリ	フィーチャー（ **Feature** ）
IIS 管理スクリプトおよびツール	• IIS 管理サービス • Web 管理ツール
.NET Framework 4.7.2の機能	• .NET Framework 4.7.2 • ASP.NET 4.7.2. • Windows Communication Foundation (WCF) HTTP Activation 45 ◦ TCP のアクティブ化 ◦ HTTP アクティブ化 ◦ メッセージキュー（ MSMQ ）のアクティブ化
メッセージキュー	• メッセージキューサービス SnapCenter が作成および管理する MSMQ サービスを他のアプリケーションが使用していないことを確認します。 • MSMQサーバ
Windows プロセスアクティブ化サービス	• プロセスモデル
設定 API	すべて

Microsoft SQL Server データベースを保護する

SnapCenter Plug-in for Microsoft SQL Server

SnapCenter Plug-in for Microsoft SQL Server の概要

SnapCenter Plug-in for Microsoft SQL Server は、 Microsoft SQL Server データベースに対応したデータ保護管理を提供する、 NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。Plug-in for SQL Server を使用することで、 SnapCenter 環境での SQL Server データベースのバックアップ、検証、リストア、およびクローニングの処理を自動化できます。

Plug-in for SQL Server をインストールすると、 SnapCenter で NetApp SnapMirror テクノロジを使用して別のボリュームにバックアップセットのミラーコピーを作成できるほか、 NetApp SnapVault テクノロジを使用して標準への準拠やアーカイブを目的としたディスクツーディスクのバックアップレプリケーションを実行できます。

SnapCenter Plug-in for Microsoft SQL Server の機能

SnapCenter Plug-in for Microsoft SQL Server をインストールした環境では、 SnapCenter を使用して SQL Server データベースをバックアップ、リストア、およびクローニングすることができます。

SQL Server データベースおよびデータベースリソースのバックアップ処理、リストア処理、およびクローニング処理で実行できるタスクを次に示します。

- SQL Server データベースおよび関連するトランザクションログをバックアップする

  master システムデータベースと msdb システムデータベースについては、ログバックアップを作成できません。model システムデータベースのログバックアップは作成できます。

- データベースリソースをリストアする
  - master システムデータベース、 msdb システムデータベース、および model システムデータベースをリストアできます。
  - 複数のデータベース、インスタンス、および可用性グループをリストアすることはできません。
  - システムデータベースを別のパスにリストアすることはできません。
- 本番環境のデータベースのポイントインタイムクローンを作成します

  tempdb システムデータベースでは、バックアップ、リストア、クローニング、クローニングのライフサイクル処理を実行できません。

- バックアップ処理をただちに検証するか、あとで検証する

  SQL Server システムデータベースの検証はサポートされていません。SnapCenter がデータベースのクローンを作成し、検証処理を実行します。SnapCenter では SQL Server システムデータベースをクローニングできないため、これらのデータベースの検証はサポートされていません。

- バックアップ処理とクローニング処理のスケジュールを設定する
- バックアップ処理、リストア処理、クローニング処理を監視する

Plug-in for SQL Server では、 SMB 共有の SQL Server データベースのバックアップとリカバリはサポートされません。

SnapCenter Plug-in for Microsoft SQL Server の特長

Plug-in for SQL Server は、 Windows ホスト上で Microsoft SQL Server と統合されるほか、ストレージシステム上でネットアップの Snapshot コピーテクノロジと統合されます。Plug-in for SQL Server を操作するには、 SnapCenter インターフェイスを使用します。

Plug-in for SQL Server の主な機能は次のとおりです。

- * SnapCenter * による統一されたグラフィカル・ユーザー・インターフェイス

  SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter インターフェイスを使用すると、すべてのプラグインでバックアッププロセスとリストアプロセスを一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（ RBAC ）を設定したり、ジョブを監視したりすることができます。SnapCenter では、バックアップ処理とクローニング処理に対応したスケジュールとポリシーの一元管理も可能です。

- * 中央管理の自動化 *

  日常的な SQL Server バックアップのスケジュールを設定したり、ポリシーベースのバックアップ保持、ポイントインタイムのリストア処理、および最新の状態へのリストア処理を設定することができます。SnapCenter から E メールアラートを送信するように設定して、 SQL Server 環境をプロアクティブに監視することもできます。

- * 無停止の NetApp Snapshot コピー・テクノロジー *

  Plug-in for SQL Server では、 NetApp SnapCenter Plug-in for Microsoft Windows でネットアップの Snapshot コピーテクノロジを使用します。これにより、データベースを数秒でバックアップし、 SQL Server をオフラインにすることなく迅速にリストアすることが可能です。Snapshot コピーはストレージスペースを最小限しか消費しません。

Plug-in for SQL Server には、上記の主要な機能以外にも次のようなメリットがあります。

- バックアップ、リストア、クローニング、および検証のワークフローがサポートされます
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます
- NetApp FlexClone テクノロジを使用して、本番環境のデータベースのスペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

  クローンを保持するストレージシステムに FlexClone ライセンスが必要です。

- 自動化された無停止のバックアップ検証
- 複数のサーバで同時に複数のバックアップを実行できます

- PowerShell コマンドレットを使用して、バックアップ、検証、リストア、クローニングの各処理のスクリプトを作成できます
- SQL Server の AlwaysOn 可用性グループ（ AG ）をサポートしているため、 AG のセットアップ、バックアップ、リストアの各処理を迅速に実行できます
- SQL Server 2014 の機能であるインメモリデータベースとバッファプール拡張（ BPE ）がサポートされます
- LUN と仮想マシンディスク（ VMDK ）のバックアップがサポートされます。
- 物理インフラと仮想インフラがサポートされます
- iSCSI 、ファイバチャネル、 FCoE 、 raw デバイスマッピング（ RDM ）、および NFS / VMFS 経由の VMDK がサポートされます

> NAS ボリュームには、 Storage Virtual Machine （ SVM ）内にデフォルトのエクスポートポリシーが必要です。

- SQL Server スタンドアロンデータベースでの FileStream とファイルグループのサポート。

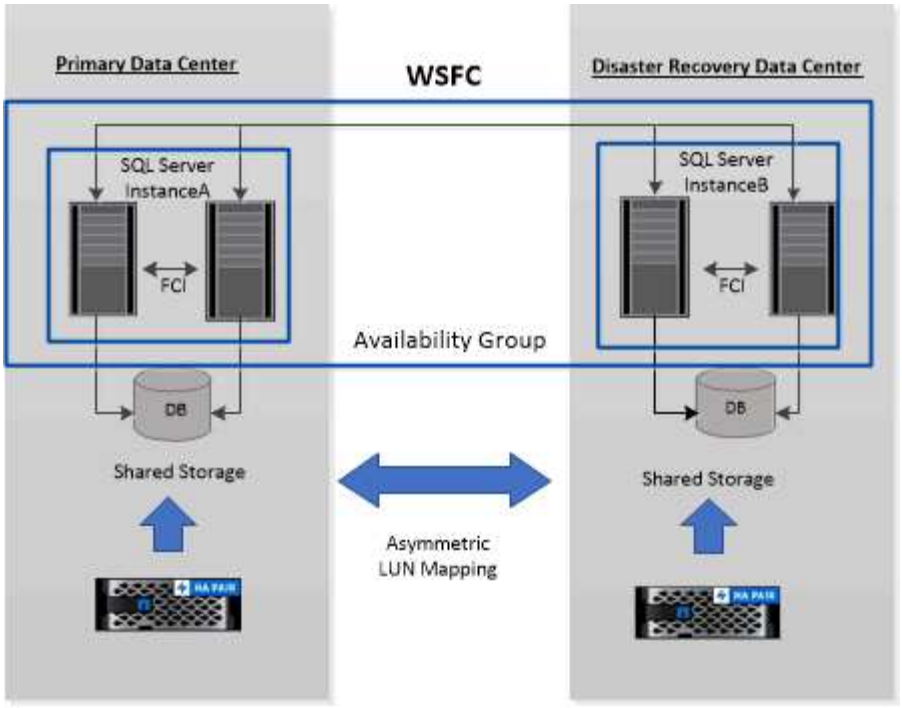
Windows クラスタでの非対称 LUN マッピングのサポート

SnapCenter Plug-in for Microsoft SQL Server では、 SQL Server 2012 以降、非対称 LUN マッピング（ ALM ）構成の高可用性、およびディザスタリカバリ用の可用性グループの検出がサポートされます。SnapCenter は、リソースを検出する際に、 ALM 構成のローカルホストとリモートホストにあるデータベースを検出します。

ALM 構成は、プライマリデータセンターとディザスタリカバリデータセンターそれぞれに 1 つ以上のノードを配置した、単一の Windows Server フェイルオーバークラスタです。

ALM 構成の例を次に示します。

- マルチサイトデータセンターにフェイルオーバークラスタインスタンス（ FCI ） × 2 つ
- ディザスタリカバリサイトにスタンドアロンインスタンスを配置したディザスタリカバリ用のローカルの高可用性（ HA ）用 FCI および Availability Group （ AG ）



WSFC----Windows Server Failover Cluster

プライマリデータセンター内のストレージは、プライマリデータセンター内の FCI ノード間で共有されます。ディザスタリカバリデータセンター内のストレージは、ディザスタリカバリデータセンター内の FCI ノード間で共有されます。

プライマリデータセンターのストレージは、ディザスタリカバリデータセンターのノードでは認識されず、逆も同様です。

ALM アーキテクチャは、 FCI で使用される 2 つの共有ストレージ解決策と、 SQL AG で使用される非共有または専用のストレージ解決策を組み合わせたものです。AG 解決策は、複数のデータセンターでディスクリソースを共有するために、同一のドライブレターを使用します。このストレージの配置では、 WSFC 内のノードのサブセット間でクラスタディスクを共有します。この構成を ALM と呼びます。

SnapCenter Plug-in for Microsoft Windows および Microsoft SQL Server でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシンの両方でさまざまなストレージタイプをサポートしています。ホストに対応したパッケージをインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

Windows Server では、 SnapCenter プロビジョニングとデータ保護がサポートされます。サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
物理サーバ	FC 接続 LUN	SnapCenter のグラフィカルユーザインターフェイス（ GUI ）または PowerShell コマンドレット	
物理サーバ	iSCSI で接続された LUN	SnapCenter GUI または PowerShell コマンドレット	
物理サーバ	Storage Virtual Machine （ SVM ）上の SMB3 （ CIFS ）共有	SnapCenter GUI または PowerShell コマンドレット	プロビジョニングのみがサポートされます。 SnapCenter プロトコルを使用してデータや共有をバックアップすることはできません。
VMware VM	FC または iSCSI HBA で接続された RDM LUN	PowerShell コマンドレット	
VMware VM	iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN	SnapCenter GUI または PowerShell コマンドレット	
VMware VM	Virtual Machine File Systems （ VMFS ）または NFS データストア	VMware vSphere の場合	
VMware VM	SVM 上の SMB3 共有に接続されたゲストシステム	SnapCenter GUI または PowerShell コマンドレット	プロビジョニングのみがサポートされます。 SnapCenter プロトコルを使用してデータや共有をバックアップすることはできません。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
Hyper-V VM	仮想ファイバチャネルスイッチで接続された仮想 FC （ vFC ） LUN	SnapCenter GUI または PowerShell コマンドレット	仮想ファイバチャネルスイッチで接続された仮想 FC （ vFC ） LUN のプロビジョニングには、Hyper-V Manager を使用する必要があります。 Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （ x ）でのデータベースのバックアップはサポートされていません。
Hyper-V VM	iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN	SnapCenter GUI または PowerShell コマンドレット	Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （ x ）でのデータベースのバックアップはサポートされていません。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
Hyper-V VM	SVM 上の SMB3 共有に接続されたゲストシステム	SnapCenter GUI または PowerShell コマンドレット	プロビジョニングのみがサポートされます。 SnapCenter プロトコルを使用してデータや共有をバックアップすることはできません。 Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （ x ）でのデータベースのバックアップはサポートされていません。

SnapCenter Plug-in for Microsoft SQL Server のストレージレイアウトに関する推奨事項

ストレージレイアウトが適切に設計されているため、 SnapCenter サーバでデータベースをバックアップして、リカバリの目標を達成できます。ストレージレイアウトを定義する際には、データベースのサイズ、データベースの変更率、バックアップの実行頻度など、いくつかの要素を考慮する必要があります。

以降のセクションでは、 SnapCenter Plug-in for Microsoft SQL Server がインストールされている環境での、 LUN と仮想マシンディスク（ VMDK ）のストレージレイアウトに関する推奨事項と制限について説明します。

この場合、 LUN には、 VMware RDM ディスクと、ゲストにマッピングされた iSCSI 直接接続 LUN を含めることができます。

LUN と VMDK の要件

必要に応じて、次のデータベースのパフォーマンスと管理を最適化するために、専用の LUN または VMDK を使用できます。

- マスターデータベースとモデルシステムデータベース
- tempdb
- ユーザデータベースファイル（ .mdf および .ndf ）

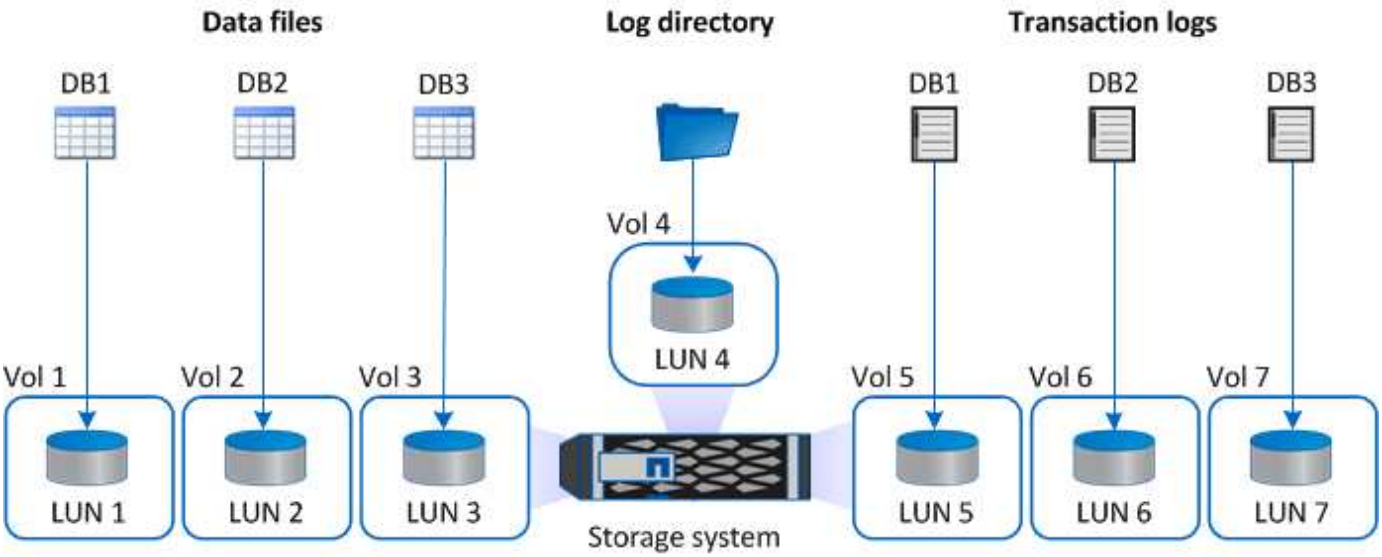
- ユーザデータベーストランザクションログファイル（ .ldf ）
- ログディレクトリ

大規模なデータベースをリストアする場合は、専用の LUN または VMDK を使用することを推奨します。LUN または VMDK 全体のリストアにかかる時間は、 LUN または VMDK に格納されている個々のファイルのリストアにかかる時間よりも短くなります。

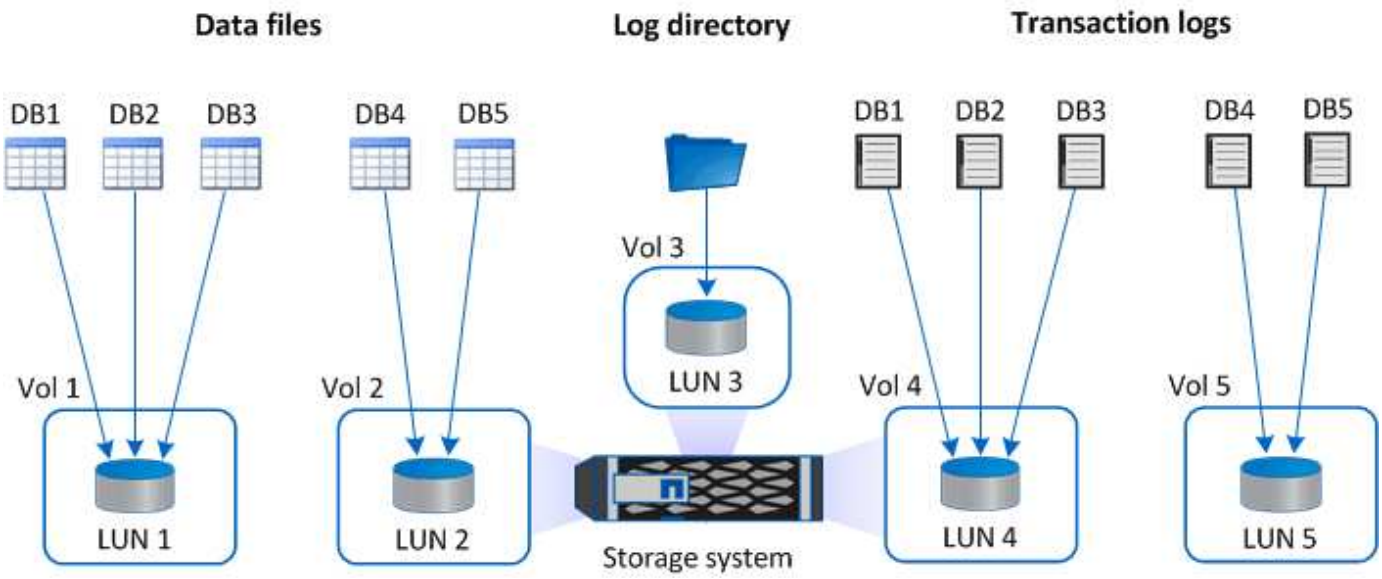
ログディレクトリについては、データファイルディスクまたはログファイルディスクに十分な空きスペースを確保できるように、別個の LUN または VMDK を作成する必要があります。

LUN および **VMDK** のサンプルレイアウト

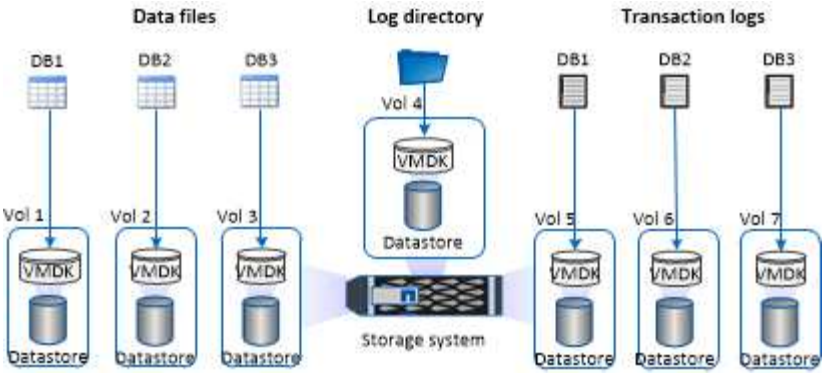
次の図は、 LUN 上の大規模データベース用のストレージレイアウトを設定する方法を示しています。



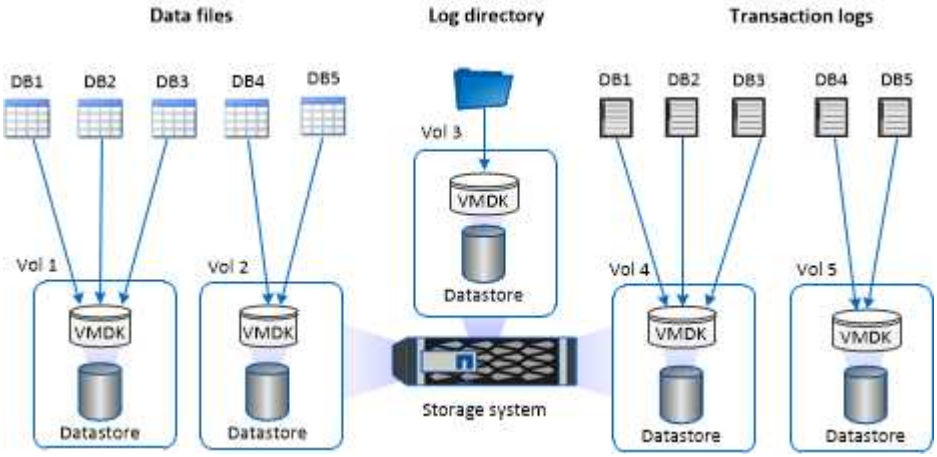
次の図は、 LUN 上の中規模または小規模のデータベースのストレージレイアウトを構成する方法を示しています。



次の図は、 VMDK 上の大規模データベース用のストレージレイアウトを設定する方法を示しています。



次の図は、 VMDK 上の中規模または小規模のデータベースのストレージレイアウトを設定する方法を示しています。



SQL プラグインに必要な最小限の ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
event generate-autosupport-log を指定します
ジョブ履歴の表示 ジョブが停止しました

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
LUN
lun create をクリックします
lun delete
LUN igroup add
lun igroup create を追加します
lun igroup delete
LUN igroup の名前を変更します
lun igroup show を参照してください
LUN マッピングの追加 - レポートノード
LUN マッピングが作成されます
LUN マッピングが削除されます
LUN マッピングの削除 - レポートノード
lun mapping show
lun modify を追加します
LUN のボリューム内移動
LUN はオフラインです
LUN はオンラインです
LUN のサイズ変更
LUN シリアル
lun show をクリックします

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SnapMirror ポリシー追加ルール snapmirror policy modify-rule snapmirror policy remove-rule 」を実行します snapmirror policy show の略 SnapMirror リストア snapmirror show の略 snapmirror show -history の略 SnapMirror の更新 SnapMirror の update-ls-set snapmirror list-destinations
バージョン

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
volume clone create を実行します
volume clone show を実行します
ボリュームクローンスプリット開始
ボリュームクローンスプリットは停止します
volume create を実行します
ボリュームを削除します
volume file clone create を実行します
volume file show-disk-usage
ボリュームはオフラインです
ボリュームはオンラインです
volume modify を使用します
volume qtree create を実行します
volume qtree delete
volume qtree modify の略
volume qtree show の略
ボリュームの制限
volume show のコマンドです
volume snapshot create を実行します
ボリューム Snapshot の削除
volume snapshot modify の実行
ボリューム Snapshot の名前が変更されます
ボリューム Snapshot リストア
ボリューム Snapshot の restore-file
volume snapshot show の実行
ボリュームのアンマウント

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SVM CIFS です vserver cifs share create の場合 SVM CIFS 共有が削除されます vserver cifs shadowcopy show vserver cifs share show のコマンドです vserver cifs show のコマンドです SVM エクスポートポリシー vserver export-policy create を参照してください vserver export-policy delete vserver export-policy rule create vserver export-policy rule show vserver export-policy show のコマンドを入力します Vserver iSCSI vserver iscsi connection show vserver show のコマンドです
Network Interface の略 network interface show の略 Vserver MetroCluster のショーをご覧ください

Plug-in for SQL Server で、 **SnapMirror** と **SnapVault** のレプリケーションに使用するストレージシステムを準備します

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenter は、Snapshotコピー処理の完了後に、SnapMirrorとSnapVault に対する更新を実行しま

す。SnapMirror更新とSnapVault 更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SnapCenter は * sync-mirror * レプリケーションをサポートしていません。

SQL Server リソースのバックアップ戦略

SQL Server リソースのバックアップ戦略を定義する

バックアップジョブを作成する前にバックアップ戦略を定義しておくと、データベースの正常なリストアやクローニングに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービスレベルアグリーメント（ SLA ）、目標復旧時間（ RTO ）、および目標復旧時点（ RPO ）によって決まります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA 、 RTO 、および RPO は、バックアップ戦略に関与します。

サポートされるバックアップのタイプ

SnapCenter を使用して SQL Server システムおよびユーザデータベースをバックアップするときは、データベース、 SQL Server インスタンス、可用性グループ（ AG ）などのリソースタイプを選択する必要があります。Snapshot コピーテクノロジを使用して、リソースが存在するボリュームのオンラインの読み取り専用コピーが作成されます。

コピーのみのオプションを選択して、 SQL Server がトランザクションログを切り捨てないように指定できます。SQL Server の管理に他のバックアップアプリケーションも使用している場合は、このオプションを使用します。トランザクションログが変更されずに保持されるため、任意のバックアップアプリケーションでシステムデータベースをリストアできます。コピーのみのバックアップは、スケジュールされたバックアップとは関係なく実行され、データベースのバックアップおよびリストア手順には影響しません。

バックアップタイプ	説明	コピーのみのオプションでバックアップタイプを指定
フルバックアップとログバックアップ	システムデータベースがバックアップされ、トランザクションログが切り捨てられます。 SQL Server は、データベースにコミット済みのエントリを削除することによってトランザクションログを切り捨てます。 このオプションを選択すると、フルバックアップの完了後にトランザクションログが作成されてトランザクション情報がキャプチャされます。通常は、このオプションを選択します。ただし、バックアップ時間が短い場合は、フルバックアップでトランザクションログバックアップを実行しないように選択することもできます。 master システムデータベースと msdb システムデータベースについては、ログバックアップを作成できません。model システムデータベースのログバックアップは作成できます。	システムデータベースファイルとトランザクションログがバックアップされ、ログは切り捨てられません。 コピーのみのバックアップは差分ベースまたは差分バックアップとしては使用できず、差分ベースには影響しません。コピーのみのフルバックアップのリストアは、他のフルバックアップのリストアと同じです。
フルデータベースバックアップ	システムデータベースファイルがバックアップされます。 master 、 model 、 msdb の各システムデータベースのフルデータベースバックアップを作成できます。	システムデータベースファイルがバックアップされます。
トランザクションログバックアップ	切り捨てられたトランザクションログがバックアップされ、最新のトランザクションログのバックアップ後にコミットされたトランザクションのみがコピーされます。 フルデータベースバックアップに加えてトランザクションログを頻繁にバックアップするスケジュールを設定すると、リカバリポイントをさらに細かく選択できます。	トランザクションログが切り捨てられずにバックアップされます。 このバックアップタイプは、定期的なログバックアップには影響しません。コピーのみのログバックアップは、オンラインのリストア処理を実行する場合に便利です。

Plug-in for SQL Server のバックアップスケジュール

バックアップ頻度（スケジュールタイプ）はポリシーで指定され、バックアップスケジュールはリソースグループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA と RPO は、データ保護戦略に関与します。

使用頻度の高いリソースであっても、フルバックアップは 1 日に 1~2 回で十分です。たとえば、定期的なトランザクションログバックアップを実行すれば、必要なバックアップが作成されます。データベースをバックアップする回数が多いほど、リストア時に SnapCenter が使用する必要のあるトランザクションログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度

  バックアップ頻度（バックアップを実行する間隔）は、ポリシー設定の一部であり、一部のプラグインでは _ schedule type__ と呼ばれます。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しない場合は、オンデマンドのみのポリシーが作成されます。ポリシーにアクセスするには、 * Settings * > * Policies * をクリックします。

- バックアップスケジュール

  バックアップスケジュール（バックアップが実行される日時）は、リソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます。リソースグループのスケジュールにアクセスするには、 * リソース * > * リソースグループ * をクリックします。

データベースに必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、データベースのサイズ、使用中のボリュームの数、データベースの変更率、サービスレベルアグリーメント（ SLA ）などがあります。

データベースバックアップの場合、選択するバックアップジョブの数は、通常、データベースが配置されているボリュームの数に応じて決まります。たとえば、あるボリュームに小規模なデータベースのグループを配置しており、別のボリュームに 1 つの大規模なデータベースを配置している場合は、小規模なデータベース用のバックアップジョブと大規模なデータベース用のバックアップジョブを 1 つずつ作成できます。

Plug-in for SQL Server のバックアップ命名規則

Snapshot コピーのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使

用できます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- _dts1_は リソースグループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、「 * Snapshot コピーにカスタム名形式を使用」を選択して、リソースまたはリソースグループを保護しながら Snapshot コピー名の形式を指定することもできます。たとえば、customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名にタイムスタンプのサフィックスが追加されます。

Plug-in for SQL Server のバックアップ保持オプション

バックアップコピーを保持する日数を選択するか、保持するバックアップコピーの数を指定できます。指定できる最大数は ONTAP で 255 個です。たとえば、組織の必要に応じて、 10 日分のバックアップコピーや 130 個のバックアップコピーを保持できます。

ポリシーを作成する際に、バックアップタイプおよびスケジュールタイプの保持オプションを指定できます。

SnapMirror レプリケーションを設定すると、デスティネーションボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、保持されているバックアップの保持ラベルがスケジュールタイプと一致する場合には、バックアップを削除します。リソースまたはリソースグループに対してスケジュールタイプが変更された場合、古いスケジュールタイプラベルのバックアップがシステムに残ることがあります。

バックアップコピーを長期にわたって保持する場合は、 SnapVault バックアップを使用する必要があります。

ソースストレージシステムにトランザクションログバックアップを保持する期間

SnapCenter Plug-in for Microsoft SQL Server では、最新の状態へのリストア処理を実行するために、トランザクションログバックアップが必要です。この場合、 2 つのフルバックアップの間の任意の時点の状態にデータベースがリストアされます。

たとえば、 Plug-in for SQL Server で午前 8 時にフルバックアップを作成しもう 1 つのフルバックアップを午後 5 時に作成した場合は、最新のトランザクションログバックアップを使用して、午前 8 時から午後 5 時ま

での任意の時点の状態にデータベースをリストアできます午後 5 時までオープントランザクションログがない場合、 Plug-in for SQL Server ではポイントインタイムリストア処理のみを実行できます。この場合、 Plug-in for SQL Server がフルバックアップを完了した時点の状態にデータベースがリストアされます。

通常、最新の状態へのリストア処理が必要になるのは 1~2 日のみです。デフォルトでは、 SnapCenter は 2 日以上保持します。

同じボリューム上の複数のデータベース

バックアップポリシーには、バックアップあたりの最大データベース数を設定するオプション（デフォルト値は 100 ）があるため、すべてのデータベースを同じボリュームに配置できます。

たとえば、同じボリュームに 200 個のデータベースがある場合、 100 個のデータベースを含む Snapshot コピーが 2 つ作成されます。

Plug-in for SQL Server でのプライマリストレージボリュームまたはセカンダリストレージボリュームを使用したバックアップコピーの検証

プライマリストレージボリュームまたは SnapMirror または SnapVault セカンダリストレージボリュームでバックアップコピーを検証することができます。セカンダリストレージボリュームを使用して検証を実行すると、プライマリストレージボリュームの負荷が軽減されます。

プライマリストレージボリュームまたはセカンダリストレージボリュームにあるバックアップを検証すると、すべてのプライマリ Snapshot コピーとセカンダリ Snapshot コピーが検証済みとマークされます。

SnapMirror および SnapVault セカンダリストレージボリューム上のバックアップコピーを検証するには、SnapRestore ライセンスが必要です。

検証ジョブをスケジュールするタイミング

SnapCenter では、バックアップの作成直後にそのバックアップを検証できますが、その場合、バックアップジョブの完了に必要な時間が大幅に増加し、大量のリソースが必要となります。したがって、ほとんどの場合、別のジョブであとから検証を行うようにスケジュールを設定することを推奨します。たとえば、午後 5 時にデータベースをバックアップする場合などです1 時間後の午後 6 時に検証を実行するようにスケジュールを設定できます

同じ理由で、通常、バックアップを実行するたびにバックアップの検証を行う必要はありません。通常、バックアップの整合性を確保するには、少ない頻度で定期的に検証を実行すれば十分です。1 つの検証ジョブで複数のバックアップを同時に検証できます。

SQL Server のリストア戦略

SQL Server のリストア戦略を定義する

SQL Server のリストア戦略を定義しておくと、それに従ってデータベースをリストアすることができます。

リストア処理のソースとデスティネーション

プライマリストレージまたはセカンダリストレージにあるバックアップコピーから SQL Server データベースをリストアすることができます。元の場所だけでなく別のデスティネーションにデータベースをリストアして、要件に対応するデスティネーションを選択することもできます。

リストア処理のソース

データベースはプライマリストレージまたはセカンダリストレージからリストアできます。

リストア処理のデスティネーション

データベースはさまざまなデスティネーションにリストアできます。

宛先	説明
元の場所	デフォルトでは、 SnapCenter は同じ SQL Server インスタンスの同じ場所にデータベースをリストアします。
別の場所です	同じホスト内の任意の SQL Server インスタンス上の別の場所にデータベースをリストアできます。
元の場所または別の場所で別のデータベース名を使用しています	バックアップを作成したホスト上の任意の SQL Server インスタンスに、別の名前でデータベースをリストアできます。

VMDK （ NFS データストアと VMFS データストア）上の SQL データベースの代替ホストを ESX サーバ間でリストアすることはできません。

SnapCenter でサポートされている **SQL Server** 復旧モデル

デフォルトでは、各データベースタイプに特定の復旧モデルが割り当てられます。SQL Server データベース管理者は、各データベースを別の復旧モデルに再割り当てできます。

SnapCenter は、 3 種類の SQL Server 復旧モデルをサポートしています。

- 単純復旧モデル

  単純復旧モデルを使用する場合は、トランザクションログをバックアップできません。

- 完全復旧モデル

  完全復旧モデルを使用する場合は、障害発生時点からデータベースを以前の状態にリストアできます。

- 一括ログ復旧モデル

一括ログ復旧モデルを使用する場合は、ログに一括記録された処理を手動で再実行する必要があります。ログに一括記録された処理のコミットレコードを含むトランザクションログがリストア前にバックアップされていない場合は、一括記録された処理を実行する必要があります。ログに一括記録された処理でデータベースに 1 、 000 万行が挿入され、トランザクションログがバックアップされる前にデータベースで障害が発生した場合、リストアされたデータベースに挿入された行は反映されません。

リストア処理のタイプ

SnapCenter を使用すると、 SQL Server リソースに対してさまざまなタイプのリストア処理を実行できます。

- 最新の状態にリストアします
- 前の時点にリストアします

最新の状態または過去のある時点にリストアできるのは、次の場合です。

- SnapMirror または SnapVault セカンダリストレージからリストアする
- 別のパス（場所）にリストアする

SnapCenter はボリュームベースの SnapRestore をサポートしていません。

最新の状態にリストアします

最新の状態へのリストア処理（デフォルト）では、障害発生時点までデータベースがリカバリされます。SnapCenter では、この処理が次の順序で行われます。

1. データベースをリストアする前に、最後のアクティブトランザクションログがバックアップされます。
2. 選択したフルデータベースバックアップからデータベースがリストアされます。
3. データベースにコミットされていないすべてのトランザクションログが適用されます（バックアップ作成時から現時点までのバックアップのトランザクションログを含む）。

   トランザクションログは事前に移動され、選択したデータベースに適用されます。

最新の状態へのリストア処理を実行するには、連続したトランザクションログセットが必要です。

SnapCenter では、ログ配布バックアップファイルから SQL Server データベーストランザクションログをリストアできないため（ログ配布はプライマリサーバインスタンス上のプライマリデータベースから別のセカンダリサーバインスタンス上の 1 つ以上のセカンダリデータベースにトランザクションログバックアップを自動的に送信する機能です）。 トランザクションログバックアップから最新の状態へのリストア処理を実行することはできません。このため、 SnapCenter を使用して SQL Server データベースのトランザクションログファイルをバックアップする必要があります。

すべてのバックアップに最新の状態へのリストア機能を使用する必要がない場合は、バックアップポリシーを使用してシステムのトランザクションログバックアップ保持を設定できます。

最新の状態へのリストア処理の例

SQL Server バックアップを毎日正午に実行している状況で、水曜日の午後 4 時に実行しているとしますバックアップからリストアする必要があります。何らかの理由により、水曜日の正午のバックアップの検証に失敗

したため、火曜日の正午のバックアップを使用してリストアを実行することにしました。バックアップのリストアが終了すると、火曜日のバックアップの作成時にコミットされていなかったトランザクションログから、水曜日の午後 4 時に書き込まれた最新のトランザクションログまでの、すべてのトランザクションログが再生され、リストアしたデータベースに適用されます（トランザクションログがバックアップされていた場合）。

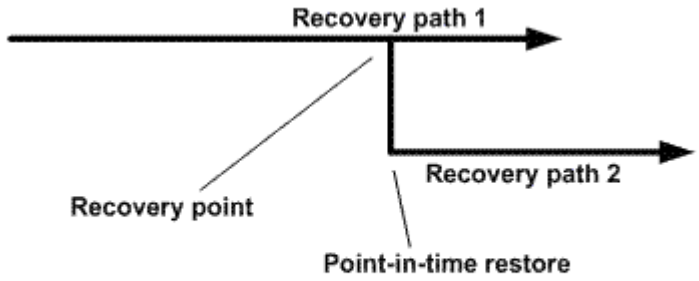
前の時点にリストアします

ポイントインタイムリストア処理では、データベースが過去の特定の時点にリストアされます。ポイントインタイムリストア処理は次の状況で発生します。

- バックアップトランザクションログの所定の時刻までデータベースをリストアする。
- データベースをリストアし、一部のバックアップトランザクションログだけを適用する。

データベースをある時点までリストアすると、新しいリカバリパスが発生します。

次の図は、ポイントインタイムリストア処理を実行した場合の問題を示しています。



この図のリカバリパス 1 では、フルバックアップが作成され、その後複数のトランザクションログバックアップが作成されます。データベースをある時点にリストアします。ポイントインタイムリストア処理のあとに新しいトランザクションログバックアップが作成されるため、リカバリパス 2 になります。新しいトランザクションログバックアップが作成されるときに、新しいフルバックアップは作成されません。データ破損などの問題が原因で、新しいフルバックアップが作成されるまで現在のデータベースをリストアできません。また、リカバリパス 2 で作成されたトランザクションログを、リカバリパス 1 のフルバックアップに適用することはできません。

トランザクションログバックアップを適用する場合は、バックアップされたトランザクションの適用を終了する日時も指定できます。このためには、指定可能な範囲内の日時を指定します。指定した時点より前にコミットされていないトランザクションは SnapCenter によって削除されます。この方法を使用すると、破損が発生する前の時点にデータベースをリストアしたり、誤って削除したデータベースやテーブルをリカバリしたりすることができます。

ポイントインタイムリストア処理の例

フルデータベースバックアップを午前 0 時に 1 回、トランザクションログバックアップを 1 時間ごとに実行しているとします。午前 9 時 45 分にデータベースがクラッシュしましたが、その後も障害が発生したデータベースのトランザクションログのバックアップは続けたとします。次に示すポイントインタイムリストアのシナリオの中から選択できます。

- 午前 0 時に作成されたフルデータベースバックアップをリストアし、それ以後のデータベース変更については復元をあきらめる。（オプション： None ）
- フルデータベースバックアップをリストアし、午前 9 ： 45 までのすべてのトランザクションログバックアップを適用する（オプション： Log until ）
- フルデータベースバックアップをリストアし、最後のトランザクションログバックアップセットからリストアするトランザクションの時刻を指定して、トランザクションログバックアップを適用する。（オプション： By specific time ）

この場合、特定のエラーが報告された日時を計算します。指定した日時までにコミットされていなかったトランザクションはすべて削除されます。

SQL Server のクローニング戦略を定義する

クローニング戦略を定義しておくと、それに従ってデータベースのクローニングを実行することができます。

1. クローニング処理に関する制限事項を確認します。
2. 必要なクローンのタイプを決定します。

クローニング処理の制限事項

データベースをクローニングする前に、クローニング処理の制限事項を確認しておく必要があります。

- 11.2.0.4から12.1.0.1のいずれかのバージョンのOracleを使用している場合、クローニング処理はにあります
  _renamedg_commandを実行するとハング状態になります。Oracleパッチ19544733を適用できます
  をクリックしてこの問題を修正します。
- ホストに直接接続されたLUNからのデータベースのクローニング（など）
  Windowsホスト上のMicrosoft iSCSIイニシエータ）から同じ上のVMDKまたはRDM LUNに接続します
  Windowsホスト、または別のWindowsホスト（またはその逆）はサポートされていません。
- ボリュームマウントポイントのルートディレクトリを共有ディレクトリにすることはできません。
- クローンが含まれている LUN を新しいボリュームに移動した場合、そのクローンは削除できません。

クローニング処理のタイプ

SnapCenter を使用して、 SQL Server データベースのバックアップまたは本番環境のデータベースをクローニングすることができます。

- データベースバックアップからのクローニング

  クローニングされたデータベースは、新しいアプリケーションを開発する際のベースラインとして機能し、分離に役立ちます
  本番環境で発生するアプリケーションエラー。クローニングされたデータベースをにすることもできます
  データベースのソフトエラーからのリカバリに使用されます。

- クローンのライフサイクル

  SnapCenterを使用すると、本番環境との間に定期的なクローンジョブをスケジュール設定できます
  データベースがビジーではありません。

SnapCenter Plug-in for Microsoft SQL Server のインストールのクイックスタート

SnapCenter サーバとプラグインのインストールを準備します

SnapCenter ServerおよびSnapCenter Plug-in for Microsoft SQL Serverをインストールするための準備手順をまとめたものです。

ドメインとワークグループの要件

SnapCenter サーバは、ドメインまたはワークグループ内のシステムにインストールできます。

Active Directory ドメインを使用している場合は、ローカル管理者の権限を持つドメインユーザを使用する必要があります。ドメインユーザは、 Windows ホストのローカル管理者グループのメンバーである必要があります。

ワークグループを使用している場合は、ローカル管理者の権限を持つローカルアカウントを使用します。

ライセンス要件

インストールするライセンスのタイプは環境によって異なります。

使用許諾	必要に応じて
SnapCenter 標準のコントローラベース	FAS または AFF ストレージコントローラの場合は必須です SnapCenter Standard ライセンスはコントローラベースのライセンスで、 Premium Bundle に含まれています。SnapManager スイートのライセンスをお持ちの場合は、 SnapCenter Standard のライセンスもご利用いただけます。 FAS または AFF ストレージを使用した SnapCenter の試用版をインストールする場合は、営業担当者にお問い合わせください。
SnapCenter - 容量ベース	ONTAP Select および Cloud Volumes ONTAP で必要です Cloud Volumes ONTAP または ONTAP Select を使用している場合は、 SnapCenter で管理するデータに基づいて、容量ベースのライセンスを 1TB 単位で購入する必要があります。 デフォルトでは、 SnapCenter には 90 日間の 100TB SnapCenter の標準容量ベースの試用版ライセンスが組み込まれています。その他の詳細については、営業担当者にお問い合わせください。
SnapMirror または SnapVault	ONTAP SnapCenter でレプリケーションを有効にする場合は、 SnapMirror または SnapVault のライセンスが必要です。
追加ライセンス（オプション）	を参照してください "SnapCenter ライセンス"。

使用許諾	必要に応じて
SnapCenter 標準ライセンス（オプション）	セカンダリデスティネーション セカンダリデスティネーションに SnapCenter Standard ライセンスを追加することを推奨しますが、必須ではありません。セカンダリデスティネーションで SnapCenter 標準ライセンスが有効になっていない場合、フェイルオーバー処理の実行後に、SnapCenter を使用してセカンダリデスティネーションのリソースをバックアップすることはできません。ただし、クローニング処理と検証処理を実行するには、セカンダリデスティネーションに FlexClone ライセンスが必要です。

ホストおよびポートの要件

ONTAP およびアプリケーションプラグインの最小要件については、を参照してください "Interoperability Matrix Tool で確認してください"。

ホスト	最小要件
オペレーティングシステム（ 64 ビット）	を参照してください "Interoperability Matrix Tool で確認してください"
CPU	• サーバホスト： 4 コア • プラグインホスト： 1 コア
RAM	• サーバホスト： 8GB • プラグインホスト： 1GB
ハードドライブの空き容量	サーバホスト： • SnapCenter サーバソフトウェアとログの場合は 4GB • SnapCenter リポジトリ用に 6GB • 各プラグインホスト：プラグインのインストールとログ用に 2GB 。専用のホストにプラグインがインストールされている場合にのみ必要です。
サードパーティのライブラリ	SnapCenter サーバホストおよびプラグインホストで必要： • Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降
ブラウザ	Chrome 、 Internet Explorer 、および Microsoft Edge

ポートタイプ	デフォルトのポート
SnapCenter ポート	8146（HTTPS）、URL _\https://server:8146_のように双方向、カスタマイズ可能
SnapCenter SMCore の通信ポート	8145 （ HTTPS ）、双方向、カスタマイズ可能
リポジトリデータベース	3306 （ HTTPS ）、双方向
Windows プラグインホスト	135 、 445 （ TCP ） ポート 135 および 445 に加え、 Microsoft が指定したダイナミックポート範囲も開いている必要があります。リモートインストール操作では、このポート範囲を動的に検索する Windows Management Instrumentation （ WMI ）サービスを使用します。 サポートされているダイナミックポート範囲については、を参照してください "Windows のサービス概要とネットワークポート要件"。
SnapCenter Plug-in for Windows の略	8145 （ HTTPS ）、双方向、カスタマイズ可能
ONTAP クラスタまたは SVM の通信ポート	443（HTTPS）、双方向 80（HTTP）、双方向 このポートは、 SnapCenter サーバホスト、プラグインホスト、 SVM または ONTAP クラスタ間の通信に使用されます。

SnapCenter Plug-in for Microsoft SQL Server の要件

ローカル管理者の権限を持つユーザが、リモートホストに対してローカルログインの権限を持っている必要があります。クラスタノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限を持つユーザが必要です。

SQL Server に対して sysadmin 権限を持つユーザが必要です。このプラグインは Microsoft VDI Framework を使用しますが、これには sysadmin アクセスが必要です。

SnapManager for Microsoft SQL Server を使用していて、 SnapManager for Microsoft SQL Server から SnapCenter にデータをインポートする場合は、を参照してください "アーカイブバックアップをインポートする"

SnapCenter Server for Microsoft SQL Serverをインストールします

SnapCenter Server for Microsoft SQL Serverのインストール手順をまとめたものです。

ステップ**1: SnapCenter** サーバーをダウンロードしてインストールします

1. から SnapCenter Server インストールパッケージをダウンロードします "NetApp Support Site" 次に、こ

の exe をダブルクリックします。

インストールの開始後、すべての事前確認が実行され、最小要件を満たしていない場合には、対応するエラーまたは警告メッセージが表示されます。警告メッセージは無視してインストールを続行できますが、エラーは修正しておく必要があります。

2. SnapCenter サーバのインストールに必要な設定済みの値を確認し、必要に応じて変更します。

   MySQL Server リポジトリデータベースのパスワードを指定する必要はありません。SnapCenter サーバのインストール時に、パスワードは自動生成されます。

   インストール用のカスタムパスでは、特殊文字“ % ”はサポートされていません。パスに「 % 」を含めると、インストールは失敗します。

3. [今すぐインストール] をクリックします。

ステップ**2**：**SnapCenter** にログインします

1. ホストデスクトップ上のショートカットまたはインストール時に表示されたURL（SnapCenterサーバがインストールされているデフォルトポート8146の場合は_\https://server:8146_）からSnapCenterを起動します。
2. クレデンシャルを入力します。

   組み込みのドメイン管理者ユーザ名の形式には、 *NetBIOS*<username>_ または *<username>*@*<domain>* または *<DomainFQDN>**<username>* を使用します。

   組み込みのローカル管理者ユーザ名の形式には、 *<username>* を使用します。

3. [* サインイン *] をクリックします。

手順**3**：**SnapCenter Standard**コントローラベースライセンスを追加する

1. ONTAP コマンドラインを使用してコントローラにログインし、次のように入力します。

   ```
   system license add -license-code <license_key>
   ```

2. ライセンスを確認します。

   ```
   license show
   ```

手順**4**：**SnapCenter** 容量ベースライセンスを追加する

1. SnapCenter GUI の左ペインで、 **Settings > Software** をクリックし、 License セクションで **+** をクリックします。
2. ライセンスを取得するには、次の 2 つの方法のいずれかを選択します。
   - ライセンスをインポートするには、NetApp Support Siteのログインクレデンシャルを入力します。
   - ネットアップライセンスファイルの場所を参照し、 * Open * をクリックします。
3. ウィザードの通知ページで、デフォルトの容量しきい値 90% を使用します。

4. [完了] をクリックします。

手順**5**：ストレージシステム接続をセットアップする

1. 左側のペインで、 * ストレージ・システム > 新規 * をクリックします。
2. Add Storage System ページで、次の手順を実行します。
   a. ストレージシステムの名前または IP アドレスを入力します。
   b. ストレージシステムへのアクセスに使用するクレデンシャルを入力します。
   c. イベント管理システム（ EMS ）と AutoSupport を有効にするには、チェックボックスを選択します。
3. プラットフォーム、プロトコル、ポート、およびタイムアウトに割り当てられたデフォルト値を変更する場合は、 [その他のオプション *] をクリックします。
4. [Submit （送信）] をクリックします。

SnapCenter Plug-in for Microsoft SQL Server をインストールします

SnapCenter Plug-in for Microsoft SQL Serverのインストール手順をまとめたものです。

手順**1**：**Run As**クレデンシャルをセットアップして**Plug-in for Microsoft SQL Server**をインストールする

1. 左側のペインで、 * Settings > Credentials > New * をクリックします。
2. クレデンシャルを入力します。

   組み込みのドメイン管理者ユーザ名の形式には、 *NetBIOS*<username>_ または *<username>*@*<domain>* または *<DomainFQDN>**<username>* を使用します。

   組み込みのローカル管理者ユーザ名の形式には、 *<username>* を使用します。

手順**2**：ホストを追加して**Plug-in for Microsoft SQL Server**をインストールする

1. SnapCenter GUI の左ペインで、 **Hosts > Managed Hosts > Add** の順にクリックします。
2. ウィザードのホストページで、次の手順を実行します。
   a. Host Type ： Windows ホストタイプを選択します。
   b. ホスト名： SQL ホストを使用するか、専用の Windows ホストの FQDN を指定します。
   c. credentials ：作成したホストの有効なクレデンシャル名を選択するか、新しいクレデンシャルを作成します。
3. インストールするプラグインの選択セクションで、 * Microsoft SQL Server * を選択します。
4. [その他のオプション] をクリックして、次の詳細を指定します。
   a. Port ：デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。
   b. インストールパス：デフォルトのパスは、 _C ： \Program Files\NetApp\SnapManager _ です。必要に応じて、パスをカスタマイズできます。
   c. Add all hosts in the cluster ： SQL in WSFC を使用している場合は、このチェックボックスを選択します。

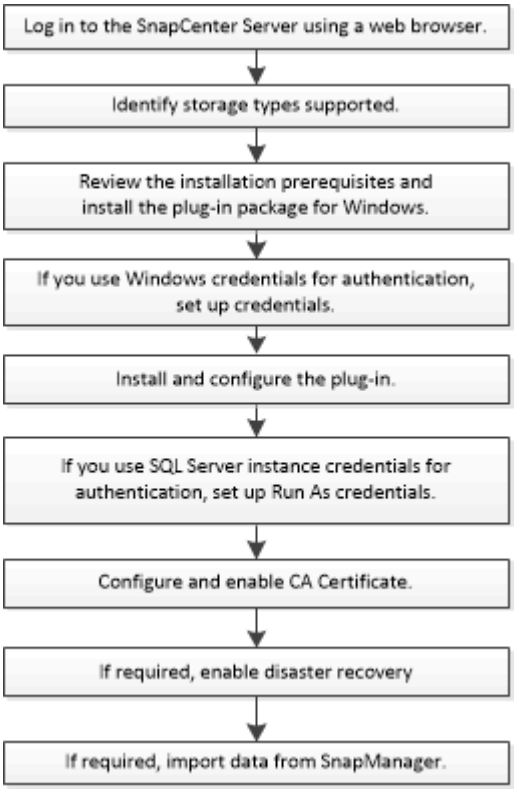
d. インストール前チェックをスキップ：プラグインを手動でインストール済みの場合、またはプラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。

5. [Submit （送信）] をクリックします。

SnapCenter Plug-in for Microsoft SQL Server をインストールする準備をします

SnapCenter Plug-in for Microsoft SQL Server のインストールワークフロー

SQL Server データベースを保護する場合は、 SnapCenter Plug-in for Microsoft SQL Server をインストールしてセットアップする必要があります。



ホストを追加して SnapCenter Plug-in for Microsoft SQL Server をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSI を使用している場合は、 iSCSI サービスが実行されている必要があります。
- リモートホストに対するローカルログイン権限を持つローカル管理者の権限を持つユーザが必要です。
- SnapCenter でクラスタノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限を持つユーザが必要です。
- SQL Server に対して sysadmin 権限を持つユーザが必要です。

SnapCenter Plug-in for Microsoft SQL Server は Microsoft VDI Framework を使用しますが、これには sysadmin アクセスが必要です。

"Microsoft のサポート記事 2926557 ：「 SQL Server VDI backup and restore operations require Sysadmin privileges"

- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- SnapManager for Microsoft SQL Server がインストールされている場合は、サービスとスケジュールを停止または無効にしておく必要があります。

  バックアップジョブまたはクローンジョブを SnapCenter にインポートする予定の場合は、SnapManager for Microsoft SQL Server をアンインストールしないでください。

- ホストがサーバから完全修飾ドメイン名（ FQDN ）に解決できる必要があります。

  hosts ファイルが解決可能になるように変更され、短縮名と FQDN の両方が hosts ファイルに指定されている場合は、 SnapCenter hosts ファイルに <IP_address> <host_fqdn><host_name> の形式でエントリを作成します

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。

項目	要件
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

SnapCenter Plug-ins Package for Windows のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますSnapCenter プラグインのインストールに必要なクレデンシャル、およびデータベースや Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- 必要なもの *
- プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。
- リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定する必要があります。
- Windows ホストでの SQL 認証

  プラグインのインストール後に SQL クレデンシャルを設定する必要があります。

  SnapCenter Plug-in for Microsoft SQL Server を導入する場合は、プラグインのインストール後に SQL クレデンシャルを設定する必要があります。このクレデンシャルは、 SQL Server の sysadmin 権限を持つユーザに対して設定します。

  SQL 認証方式は、 SQL Server インスタンスに照らして認証します。つまり、 SnapCenter で SQL Server インスタンスが検出されている必要があります。そのため、 SQL クレデンシャルを追加する前に、ホストの追加とプラグインパッケージのインストールを行って、リソースを更新しておく必要があります。SQL Server 認証は、スケジュール設定やリソース検出などの処理を実行する際に必要になります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* 資格情報] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	手順
ユーザ名 / パスワード	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者 SnapCenter プラグインをインストールするシステムのドメイン管理者を指定します。Username フィールドの有効な形式は次のとおりです。 ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Usernameフィールドの有効な形式は次のとおりです。 `UserName` パスワードに二重引用符（"）またはバックティック（`）を使用しないでください。 小なり（<）と感嘆符（！）は使用しないでください。 パスワードに記号を追加します。たとえば、lessthan <！10、lessthan10 <！、backtick 12とします。
認証モード	使用する認証モードを選択します。SQL 認証モードを選択した場合は、 SQL Server インスタンスとその SQL インスタンスのホストも指定する必要があります。

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、 [ユーザとアクセス（ User and Access ）] ページで、ユーザまたはユーザグループにクレデンシャルのメンテナンスを割り当てることができます。

個々の **SQL Server** リソースのクレデンシャルを設定する

クレデンシャルを設定して、各ユーザに対して個々の SQL Server リソースに対してデータ保護ジョブを実行することができます。クレデンシャルはグローバルに設定することもできますが、必要に応じて特定のリソースに対してのみ設定することもできます。

このタスクについて

- Windows クレデンシャルを認証に使用している場合は、プラグインのインストール前にクレデンシャルを設定する必要があります。

  ただし、 SQL Server インスタンスを認証に使用している場合は、プラグインのインストール後にクレデンシャルを追加する必要があります。

- クレデンシャルの設定時に SQL 認証を有効にしている場合は、検出されたインスタンスまたはデータベースに赤色の南京錠のアイコンが表示されます。

  南京錠のアイコンが表示された場合は、インスタンスまたはデータベースのクレデンシャルを指定して、インスタンスまたはデータベースをリソースグループに追加する必要があります。

- 次の条件に該当する場合、 sysadmin アクセスがないロールベースアクセス制御（ RBAC ）ユーザにクレデンシャルを割り当てる必要があります。
  - SQL インスタンスに資格情報が割り当てられます。
  - SQL インスタンスまたはホストが RBAC ユーザに割り当てられている。

    ユーザにはリソースグループとバックアップの両方の権限が必要です。

手順**1**：クレデンシャルを追加して設定します

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* 資格情報] をクリックします。
   a. 新しい資格情報を追加するには、 * New * をクリックします。
   b. [Credential] ページで、クレデンシャルを設定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名	SQL Server 認証に使用するユーザ名を入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。[**Username**] フィールドの有効な形式は次のとおりです。 ◦ NETBIOS_USERNAME_ ◦ _ ドメイン FQDN\ ユーザ名 _ • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、 SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限またはユーザがある場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます ホストシステムでアクセス制御機能が無効になっています。[* ユーザー名 *] フィールドの有効な形式は、 *username* です

フィールド	手順
パスワード	認証に使用するパスワードを入力します。
認証モード	SQL Server 認証モードを選択します。 SQL Server に対する sysadmin 権限がある Windows ユーザの場合は、Windows 認証を選択することもできます。
ホスト	ホストを選択します。
SQL Serverインスタンス	SQL Server インスタンスを選択します。

c. [OK] をクリックしてクレデンシャルを追加します。

ステップ**2**：インスタンスを構成します

1. 左側のナビゲーションペインで、 * リソース * をクリックします。
2. [リソース] ページで、 [* 表示 *] リストから [* インスタンス *] を選択します。
   a. をクリックします をクリックし、ホスト名を選択してインスタンスをフィルタリングします。
   b. をクリックします をクリックしてフィルタペインを閉じます。
3. Instance Protect （インスタンス保護）ページで、インスタンスを保護し、必要に応じて、 Configure Credentials （資格情報の設定） * をクリックします。

   SnapCenter サーバにログインしているユーザが SnapCenter プラグイン for Microsoft SQL Server にアクセスできない場合は、そのユーザがクレデンシャルを設定する必要があります。

   クレデンシャルオプションは、データベースおよび可用性グループには適用されません。

4. [リソースの更新] をクリックします。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient

3. GMSA を作成して構成します。

   a. 次の形式でユーザグループアカウントを作成します。

      ```
       domainName\accountName$
      .. グループにコンピュータオブジェクトを追加します。
      .. 作成したユーザグループを使用して gMSA を作成します。
      ```

      例：

      ```
       New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
      <fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      .. を実行します `Get-ADServiceAccount`
      サービスアカウントを確認するコマンド。
      ```

4. ホストで gMSA を設定します。

   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. ホストを再起動します。

   b. PowerShellコマンドプロンプトから次のコマンドを実行して、ホストにgMSAをインストールします。 `Install-AdServiceAccount <gMSA>`

   c. 次のコマンドを実行して'gMSAアカウントを確認します `Test-AdServiceAccount <gMSA>`

1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

   SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

SnapCenter Plug-in for Microsoft SQL Server をインストールします

ホストを追加し、 **SnapCenter Plug-ins Package for Windows** をインストールします

ホストの追加およびプラグインパッケージのインストールには、 SnapCenter * ホストの追加ページを使用する必要があります。プラグインは、自動的にリモートホストにインストールされます。

- 必要なもの *
- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windows ホストにプラグインをインストールするときに、ビルトインでないクレデンシャルを指定する場合は、ホストで UAC を無効にします。
- メッセージキューイングサービスが実行中状態であることを確認する必要があります。
- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

  "Windows Server 2012 以降で SQL 用のグループマネージドサービスアカウントを設定します"

- このタスクについて *

SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。

ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。クラスタまたは Windows Server Failover Clustering （ WSFC ）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

ホストの管理の詳細については、を参照してください "ホストを管理します"。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の手順を実行します。

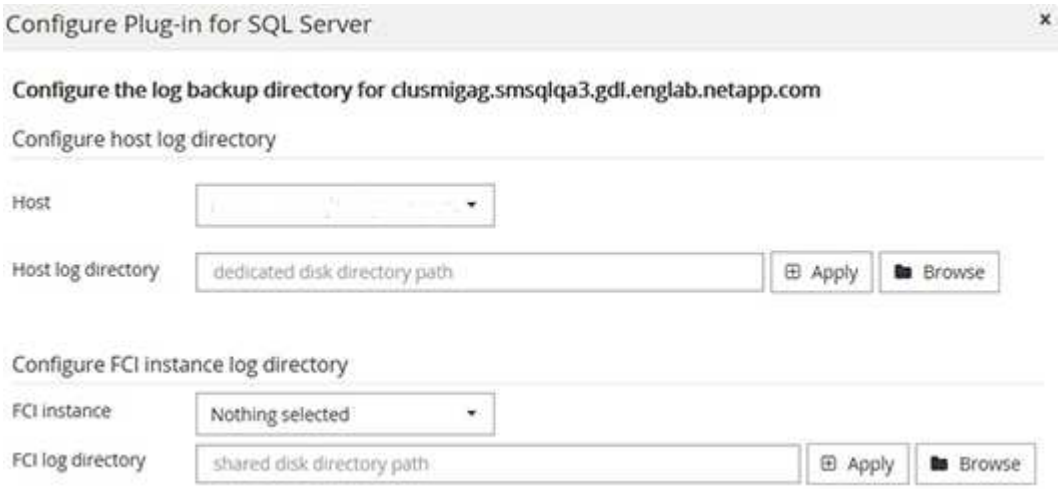
フィールド	手順
ホストタイプ	ホストタイプとして Windows を選択します。SnapCenter サーバによってホストが追加され、ホストに Plug-in for Windows がインストールされていない場合はインストールされます。 [プラグイン] ページで [Microsoft SQL Server] オプションを選択すると、 SnapCenter サーバによって Plug-in for SQL Server がインストールされます。
ホスト名	ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。 信頼されていないドメインホストの IP アドレスは、 FQDN に解決される場合にのみサポートされます。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • WSFC SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。
クレデンシャル	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. [インストールするプラグインを選択してください *] セクションで、インストールするプラグインを選択します。
6. [* その他のオプション *] をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	デフォルトパスは C ： \Program Files\NetApp\SnapManager です。必要に応じて、パスをカスタマイズできます。
クラスタ内のすべてのホストを追加します	WSFC または SQL 可用性グループ内のすべてのクラスタノードを追加するには、このチェックボックスを選択します。 クラスタ内の複数の使用可能な SQL 可用性グループを管理および識別するには、 GUI で適切なクラスタチェックボックスを選択して、すべてのクラスタノードを追加する必要があります。
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	グループ管理サービスアカウント（ GMSA ）を使用してプラグインサービスを実行する場合は、このチェックボックスをオンにします。 gMSA 名を domainName\accountName$ の形式で指定します。 ホストが gMSA とともに追加され 'gMSA にログイン権限と sys 管理権限がある場合は 'gMSA を使用して SQL インスタンスに接続します

7. [Submit （送信）] をクリックします。
8. SQL Plug-in の場合、ログディレクトリを設定するホストを選択します。
   a. ログディレクトリの設定 * をクリックし、ホストログディレクトリの設定ページで * 参照 * をクリックして、次の手順を実行します。

ネットアップ LUN （ドライブ）のみが選択対象として表示されます。SnapCenter は、バックアップ処理の一環として、ホストログディレクトリをバックアップしてレプリケートします。



i. ホストログを格納するホスト上のドライブレターまたはマウントポイントを選択します。

ii. 必要に応じてサブディレクトリを選択します。

iii. [保存（ Save ）] をクリックします。

9. [Submit （送信）] をクリックします。

[事前確認をスキップ] チェックボックスをオンにしていない場合、プラグインをインストールするための要件をホストが満たしているかどうかが検証されます。ディスクスペース、 RAM 、 PowerShell のバージョン、 .NET のバージョン、場所（ Windows プラグインの場合）、および Java のバージョン（ Linux プラグインの場合）が、最小要件に照らして検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

エラーがディスクスペースまたは RAM に関連している場合は、 C ： \Program Files\NetApp\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

1. インストールの進行状況を監視します。

コマンドレットを使用して、複数のリモートホストに **SnapCenter Plug-in for Microsoft SQL Server** をインストールします

SmHostPackage PowerShell コマンドレットを使用して、複数のホストに SnapCenter Plug-in for Microsoft SQL Server を同時にインストールできます。

- 必要なもの *

プラグインパッケージをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 Open-SmConnection コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のリモートホストに SnapCenter Plug-in for Microsoft SQL Server をインストールします。

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、 -skipprecheck オプションを使用できます。

1. リモートインストールのクレデンシャルを入力します。

コマンドラインから **SnapCenter Plug-in for Microsoft SQL Server** をサイレントインストールします

SnapCenter Plug-in for Microsoft SQL Server は、 SnapCenter ユーザインターフェイス内からインストールする必要があります。ただし、何らかの理由でインストールできない場合は、 Windows のコマンドラインから、 Plug-in for SQL Server のインストールプログラムをサイレントモードで自動的に実行できます。

- 必要なもの *
- をインストールする前に、以前のバージョンの SnapCenter Plug-in for Microsoft SQL Server を削除する必要があります。

  詳細については、を参照してください "SnapCenter Plug-in をプラグインホストから手動で直接インストールする方法"。

- 手順 *

1. C ： \temp フォルダがプラグインホストに存在し、ログインしているユーザにそのフォルダへのフルアクセス権があるかどうかを確認してください。
2. C ： \ProgramData\NetApp\SnapCenter \Package Repository から Plug-in for SQL Server ソフトウェアをダウンロードします。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

3. プラグインをインストールするホストにインストールファイルをコピーします。
4. ローカルホストの Windows コマンドプロンプトで、プラグインのインストールファイルを保存したディレクトリに移動します。
5. Plug-in for SQL Server ソフトウェアをインストールします。

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

プレースホルダの値をデータに置き換えます

- debug_log_Path は、スイートインストーラログファイルの名前と場所です。
- LOG_Path はプラグインコンポーネント（ SCW 、 SCSQL 、および SMCore ）のインストールログの場所です。
- num は、 SnapCenter が SMCore と通信するポートです
- install_Directory_Path は、ホストプラグインパッケージのインストールディレクトリです。
- domain\administrator は、 SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントです。
- password は、 SnapCenter Plug-in for Microsoft Windows Web サービスアカウントのパスワードです。
  [+]
  ```
  "snapcenter_windows_host_plugin.exe"/silent
  /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
  SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
  BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
  ISFeatureInstall=SCW,SCSQL
  ```

Plug-in for SQL Server のインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

1. Windows タスクスケジューラ、メインインストールログファイル C:\Installdebug.log 、および C:\Temp 内の追加インストールファイルを監視します。
2. %temp% ディレクトリを監視して、 msiexe.exe インストーラがエラーなしでソフトウェアをインストールしていることを確認します。

Plug-in for SQL Server をインストールすると、 SnapCenter Server ではなくホストにプラグインが登録されます。SnapCenter サーバにプラグインを登録するには、 SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加します。ホストを追加すると、プラグインが自動的に検出されます。

Plug-in for SQL Server のインストールのステータスを監視します

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした

- キューに登録され
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
     a. [* フィルタ * （ Filter * ）] をクリック
     b. オプション：開始日と終了日を指定します。
     c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
     d. Status ドロップダウンメニューから、インストールステータスを選択します。
     e. [適用（ Apply ）] をクリックします。
  4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

- 手順 *
  1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
  2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。

3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *
  1. GUI で次の手順を実行します。
     a. 証明書をダブルクリックします。
     b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
     c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
     d. ボックスから 16 進文字をコピーします。
     e. 16 進数の間のスペースを削除します。

        たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

  2. PowerShell で次の手順を実行します。
     a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近イ

ンストールされた証明書を件名で識別します。

Get-ChildItem - パス証明書： *\localmachine\My*

b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して **CA** 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   . 次のコマンドを実行して、新しくインストールした証明書を Windows ホストプラグインサービスにバインドします。

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
   certhash=$cert appid="$guid"
   ```

   例：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

プラグインの **CA** 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *

- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

ディザスタリカバリを設定

SnapCenter Plug-in for SQL Server のディザスタリカバリ

SnapCenter Plug-in for SQL Serverが停止した場合は、次の手順を実行して別のSQLホストに切り替え、データをリカバリします。

必要なもの

- セカンダリホストのオペレーティングシステム、アプリケーション、およびホスト名は、プライマリホストと同じにする必要があります。
- [ホストの追加] または [ホストの変更] ページを使用して、 SnapCenter Plug-in for SQL Server を別のホストにプッシュします。を参照してください "ホストを管理します" を参照してください。

手順

1. [*Hosts] ページからホストを選択して、 SnapCenter Plug-in for SQL Server を変更およびインストールします。
2. （オプション） SnapCenter Plug-in for SQL Server の構成ファイルをディザスタリカバリ（ DR ）バックアップから新しいマシンに置き換えます。

3. Windows スケジュールと SQL スケジュールを、 DR バックアップから SnapCenter Plug-in for SQL Server フォルダからインポートします。

を参照してください。

を参照してください "ディザスタリカバリ API" ビデオ：

SnapCenter Plug-in for SQL Server の **Storage Disaster Recovery** （ **DR** ；ストレージディザスタリカバリ）

SnapCenter Plug-in for SQL Server ストレージをリカバリするには、グローバル設定ページでストレージの DR モードを有効にします。

- 必要なもの *
- プラグインがメンテナンスモードになっていることを確認します。
- SnapMirror / SnapVault 関係を解除
  "SnapMirror 関係を解除します"
- セカンダリの LUN を、同じドライブレターを使用してホストマシンに接続します。
- DR の前に使用したのと同じドライブレターを使用して、すべてのディスクが接続されていることを確認してください。
- MSSQL サーバサービスを再起動します。
- SQL リソースがオンラインに戻っていることを確認します。
- このタスクについて *

ディザスタリカバリ（ DR ）は、 VMDK 構成と RDM 構成ではサポートされていません。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * ディザスタ・リカバリ * と進みます。
  2. [Enable Disaster Recovery] を選択します。
  3. [適用（ Apply ）] をクリックします。
  4. DR ジョブが有効になっているかどうかを確認するには、 * Monitor * > * Jobs * をクリックします。
- 終了後 *
- フェイルオーバー後に新しいデータベースが作成されると、データベースは非 DR モードになります。

  新しいデータベースは、フェイルオーバー前と同様に動作します。

- DR モードで作成された新しいバックアップは、トポロジページの SnapMirror または SnapVault （セカンダリ）の下に表示されます。

  新しいバックアップの横に「 i 」アイコンが表示され、 DR モードで作成されたバックアップであることが示されます。

- フェイルオーバー時に作成されたSnapCenter Plug-in for SQL Serverのバックアップは、UIまたは次のコマンドレットを使用して削除できます。 `Remove-SmBackup`
- フェイルオーバー後、一部のリソースをDR以外のモードにするには、次のコマンドレットを使用しま

す。 `Remove-SmResourceDRMode`

詳細については、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- SnapCenter サーバは、 DR モードまたは非 DR モードの個々のストレージリソース（ SQL データベース）を管理しますが、 DR モードまたは非 DR モードのストレージリソースを含むリソースグループは管理しません。

SnapCenter Plug-in for SQL Server のセカンダリストレージからプライマリストレージへのフェイルバック

SnapCenter Plug-in for SQL Server のプライマリストレージがオンラインに戻ったら、プライマリストレージにフェイルバックする必要があります。

- 必要なもの *
- Managed Hosts ページから SnapCenter Plug-in for SQL Server を * Maintenance * モードにします。
- セカンダリストレージをホストから切断して、プライマリストレージから接続します。
- プライマリストレージにフェイルバックするには、逆再同期処理を実行して、フェイルオーバー前と同じ関係の方向が維持されることを確認します。

  逆再同期処理後もプライマリストレージとセカンダリストレージの役割を維持するには、逆再同期処理をもう一度実行します。

  詳細については、を参照してください "ミラー関係を逆再同期しています"

- MSSQL サーバサービスを再起動します。
- SQL リソースがオンラインに戻っていることを確認します。

> プラグインのフェイルオーバーまたはフェイルバックの実行中は、プラグインの全体的なステータスはすぐには更新されません。ホストおよびプラグインの全体的なステータスは、以降のホスト更新処理中に更新されます。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * ディザスタ・リカバリ * と進みます。
  2. [Enable Disaster Recovery] を選択解除します。
  3. [適用（ Apply ）] をクリックします。
  4. DR ジョブが有効になっているかどうかを確認するには、 * Monitor * > * Jobs * をクリックします。
- 終了後 *
- フェイルオーバー時に作成されたSnapCenter Plug-in for SQL Serverのバックアップは、UIまたは次のコマンドレットを使用して削除できます。 `Remove-SmDRFailoverBackups`

SnapCenter Plug-in for VMware vSphere をインストール

データベースが仮想マシン（ VM ）に格納されている場合や VM とデータストアを保護する場合は、 SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください "導入の概要"。

CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください "SSL 証明書を作成またはインポートします"。

CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere は、事前に設定されたディレクトリ内の CRL ファイルを検索します。VMware vSphere 用 SnapCenter プラグインの CRL ファイルのデフォルトディレクトリは、_/opt/NetApp/config/crl_です 。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

データ保護を準備

SnapCenter Plug-in for Microsoft SQL Server を使用するための前提条件

ユーザが Plug-in for SQL Server の使用を開始するためには、 SnapCenter 管理者が事前に SnapCenter サーバをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。
- SnapCenter にログインします。
- ストレージシステム接続を追加または割り当て、クレデンシャルを作成して、 SnapCenter 環境を設定します。

  SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SnapCenter でサポートする SVM には、それぞれ一意の名前を付ける必要があります。

- ホストを追加し、プラグインをインストールし、リソースを検出（更新）し、プラグインを設定します。
- Invoke-NaSmConfigureResources を実行して既存の Microsoft SQL Server データベースをローカルディスクからネットアップ LUN に移動したり、その逆を実行したりします。

  コマンドレットの実行方法については、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

- VMware RDM LUN または VMDK に存在する SQL データベースを SnapCenter Server で保護する場合は、 SnapCenter Plug-in for VMware vSphere を導入して、 SnapCenter にプラグインを登録する必要があります。詳細については、 SnapCenter Plug-in for VMware vSphere のドキュメントを参照してください。

  "SnapCenter Plug-in for VMware vSphere のドキュメント"

- SnapCenter Plug-in for Microsoft Windows を使用して、ホスト側のストレージをプロビジョニングします。

- バックアップレプリケーションが必要である場合は、 SnapMirror 関係と SnapVault 関係をセットアップします。

詳細については、 SnapCenter のインストールに関する説明を参照してください。

SnapCenter 4.1.1 ユーザの場合、 SnapCenter Plug-in for VMware vSphere 4.1.1 のドキュメントには、仮想化されたデータベースとファイルシステムの保護に関する情報が記載されています。SnapCenter 4.2.x ユーザの場合、 NetApp Data Broker 1.0 および 1.0.1 のドキュメントでは、 Linux ベースの NetApp Data Broker 仮想アプライアンス（オープン仮想アプライアンス形式）が提供する SnapCenter Plug-in for VMware vSphere を使用して、仮想化されたデータベースとファイルシステムを保護する方法について説明しています。SnapCenter 4.3.x を使用する場合は、 Linux ベースの SnapCenter Plug-in for VMware vSphere 仮想アプライアンス（オープン仮想アプライアンス形式）を使用して仮想化されたデータベースとファイルシステムを保護する方法について、 SnapCenter Plug-in for VMware vSphere 4.3 のドキュメントを参照してください。

"SnapCenter Plug-in for VMware vSphere のドキュメント"

SQL Server の保護におけるリソース、リソースグループ、ポリシーの使用方法

SnapCenter を使用する前に、実行するバックアップ、クローニング、およびリストアの処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- リソースとは、 SnapCenter でバックアップやクローンを作成するデータベース、データベースインスタンス、または Microsoft SQL Server 可用性グループのことです。
- SnapCenter リソースグループは、ホストまたはクラスタ上のリソースの集まりです。

  リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているリソースに対して処理が実行されます。

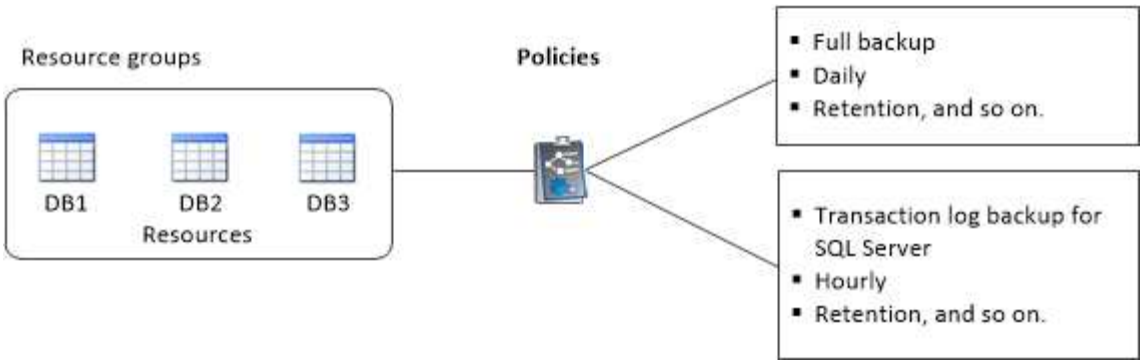
  単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。スケジュールされたバックアップを単一のリソースおよびリソースグループに対して実行することもできます。

- ポリシーは、バックアップ頻度、コピーの保持、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

  リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。単一のリソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、すべてのデータベースをバックアップする場合や、ホストのすべてのファイルシステムをバックアップする場合は、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。リソースグループを作成してポリシーを適用する際に、フルバックアップを 1 日 1 回実行するようにリソースグループを設定し、別のスケジュールでログバックアップを 1 時間おきに実行するように設定します。

次の図は、データベースのリソース、リソースグループ、およびポリシーの関係を示しています。



SQL Server データベース、インスタンス、または可用性グループをバックアップする

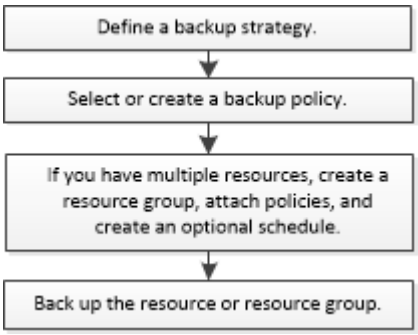
バックアップのワークフロー

SnapCenter Plug-in for Microsoft SQL Server をインストールした環境では、SnapCenter を使用して SQL Server リソースをバックアップすることができます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。

バックアップ処理とリストア処理を同じリソースで同時に実行することはできません。

次のワークフローは、バックアップ処理の実行順序を示しています。



NetApp 以外の LUN 、破損したデータベース、またはリストア中のデータベースを選択すると、 Resources ページの Backup Now 、 Restore 、 Manage Backups 、および Clone の各オプションが無効になります。

PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、リカバリ、検証、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

SnapCenter でのデータベースのバックアップ方法

SnapCenter は、 Snapshot コピーテクノロジを使用して、 LUN または VMDK に格納されている SQL Server データベースをバックアップします。SnapCenter は、データベースの Snapshot コピーを作成することによってバックアップを作成します。

リソースページでフルデータベースバックアップの対象としてデータベースを選択すると、同じストレージボリューム上の他のすべてのデータベースが SnapCenter によって自動的に選択されます。LUN または VMDK にデータベースが 1 つだけ格納されている場合は、そのデータベースを個別に選択解除したり、再度選択したりできます。LUN または VMDK に複数のデータベースが格納されている場合は、それらのデータベースをグループとして選択解除したり、再度選択したりする必要があります。

1 つのボリューム上のすべてのデータベースが、 Snapshot コピーを使用して同時にバックアップされます。同時にバックアップ可能なデータベースの最大数が 35 で、ストレージボリュームに格納されているデータベースが 35 個よりも多い場合、データベース数を 35 で割った数の Snapshot コピーが作成されます。

Snapshot コピーごとのデータベースの最大数は、バックアップポリシーで設定できます。

SnapCenter で作成される Snapshot コピーには、ストレージシステムボリューム全体がキャプチャされます。ただし、バックアップは、バックアップが作成された SQL ホストサーバに対してのみ有効になります。

他の SQL ホストサーバのデータが同じボリュームに含まれている場合、それらのデータを Snapshot コピーからリストアすることはできません。

- 詳細はこちら *

"PowerShell コマンドレットを使用してリソースをバックアップします"

"リソースの休止処理またはグループ化処理が失敗します"

バックアップに使用できるリソースがあるかどうかを確認する

リソースとは、インストールしたプラグインで管理されるデータベース、アプリケーションインスタンス、可用性グループなどのコンポーネントのことです。リソースをリソースグループに追加することでデータ保護ジョブを実行できますが、その前に利用可能なリソースを特定しておく必要があります。使用可能なリソースを確認することで、プラグインのインストールが正常に完了したことの確認にもなります。

必要なもの

- SnapCenter サーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- Microsoft SQL データベースを検出するには、次のいずれかの条件を満たしている必要があります。
  - SnapCenter サーバにプラグインホストを追加したユーザには、 Microsoft SQL Server に対して必要な権限（ sysadmin ）が割り当てられている必要があります。
  - 上記の条件を満たしていない場合は、 SnapCenter サーバで、 Microsoft SQL Server に対して必要な権限（ sysadmin ）を持つユーザを設定する必要があります。ユーザは Microsoft SQL Server インスタンスレベルで設定する必要があり、ユーザは SQL または Windows ユーザに設定できます。
- Windows クラスタで Microsoft SQL データベースを検出するには、フェイルオーバークラスタインスタンス（ FCI ）の TCP / IP ポートのブロックを解除する必要があります。
- データベースが VMware RDM LUN または VMDK にある場合は、 SnapCenter Plug-in for VMware vSphere を導入し、 SnapCenter に登録する必要があります。

  詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere を導入"

- ホストを gMSA とともに追加し 'gMSA にログイン権限とシステム管理権限がある場合 'gMSA を使用して SQL インスタンスに接続します

このタスクについて

[詳細] ページの [全体のステータス *] オプションが [バックアップに使用できない] に設定されている場合は、データベースをバックアップできません。次のいずれかに該当する場合、 * Overall Status * オプションはバックアップに使用できない状態に設定されます。

- データベースが NetApp LUN 上にない。
- データベースが正常な状態でない。

  データベースがオフライン、リストア中、リカバリの保留中、サスペクトなどの状態です。

- データベースに必要な権限がありません。

  たとえば、ユーザにデータベースへの表示アクセス権しかない場合、データベースのファイルとプロパティを識別できないため、バックアップすることはできません。

SnapCenter でバックアップできるのは、 SQL Server Standard Edition で可用性グループを設定している場合のみです。

手順

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースページで、 * View * ドロップダウン・リストから * Database * 、 * Instance * 、または * Availability Group * を選択します。

   をクリックします をクリックし、ホスト名と SQL Server インスタンスを選択してリソースをフィルタリングします。をクリックします をクリックしてフィルタペインを閉じます。

3. [リソースの更新] をクリックします。

   新しく追加、名前変更、または削除されたリソースは、 SnapCenter サーバインベントリに更新されます。

   データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

   リソースは、リソースタイプ、ホストまたはクラスタ名、関連するリソースグループ、バックアップタイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

   - データベースがネットアップ以外のストレージにある場合、 `Not available for backup` は、* Overall Status *列に表示されます。

     ネットアップ以外のストレージにあるデータベースには、データ保護処理を実行できません。

   - データベースがネットアップストレージ上にあり、保護されていない場合は、 `Not protected` は、* Overall Status *列に表示されます。
   - データベースがネットアップストレージシステム上にあり、保護されている場合は、ユーザインターフェイスが表示されます `Backup not run` [**Overall Status**]列のメッセージ。

◦ データベースがネットアップストレージシステム上にあり、保護されている場合、データベースのバックアップが実行されると、ユーザインターフェイスが表示されます `Backup succeeded` [**Overall Status**]列のメッセージ。

クレデンシャルの設定時に SQL 認証を有効にしている場合は、検出されたインスタンスまたはデータベースに赤い鍵のアイコンが表示されます。鍵のアイコンが表示された場合、リソースグループに追加するインスタンスまたはデータベースのクレデンシャルを指定する必要があります。

1. SnapCenter 管理者がリソースを RBAC ユーザに割り当てたら、 RBAC ユーザはログインし、 [* リソースの更新 *] をクリックして、リソースの最新の * 全体的なステータス * を確認する必要があります。

ネットアップストレージシステムにリソースを移行

SnapCenter Plug-in for Microsoft Windows を使用してネットアップストレージシステムをプロビジョニングしたら、 SnapCenter グラフィカルユーザインターフェイス（ GUI ）または PowerShell コマンドレットを使用して、リソースをネットアップストレージシステムに移行するか、またはあるネットアップ LUN から別のネットアップ LUN に移行できます。

- 必要なもの *
- SnapCenter サーバにストレージシステムを追加しておく必要があります。
- SQL Server リソースを更新（検出）しておく必要があります。

ウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要な一部のフィールドを取り上げます。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. [リソース] ページで、 [* 表示 *] ドロップダウン・リストから [* データベース *] または [* インスタンス *] を選択します。
  3. リストからデータベースまたはインスタンスを選択し、 * Migrate * をクリックします。
  4. リソースページで、次の操作を実行します。

フィールド	手順
• データベース名 * （オプション）	移行用のインスタンスを選択した場合は、そのインスタンスのデータベースを「 * Databases * 」ドロップダウンリストから選択する必要があります。

フィールド	手順
• 目的地を選択 *	データファイルとログファイルの保存先を選択します。 データファイルとログファイルは、選択したネットアップドライブの下の Data フォルダと Log フォルダにそれぞれ移動されます。フォルダ構造内にフォルダがない場合は、フォルダが作成され、リソースが移行されます。
• データベースファイルの詳細を表示 * （オプション）	このオプションは、 1 つのデータベースの複数のファイルを移行する場合に選択します。 このオプションは、 * Instance * リソースを選択した場合には表示されません。
• オプション *	「 * 元の場所にある移行済みデータベースのコピーを削除する * 」を選択して、ソースからデータベースのコピーを削除します。 オプション： * データベースの接続を解除する前にテーブルに対して UPDATE STATISTICS を実行します。 *

5. 検証ページで、次の操作を実行します。

フィールド	手順
• データベース整合性チェックオプション *	移行前にデータベースの整合性をチェックするには、 * Run Before * を選択します。 移行後にデータベースの整合性をチェックするには、 * Run After * を選択します。

フィールド	手順
*DBCC CHECKDB オプション *	• 整合性チェックの対象をデータベースの物理構造に限定し、データベースに影響を与える正しくないページ、チェックサム障害、および一般的なハードウェア障害を検出するには、「 * physical_only * 」オプションを選択します。 • すべての情報メッセージを停止するには、「 * NO_INFOMSGS * 」オプションを選択します。 • レポートされたエラーをオブジェクトごとにすべて表示するには、 * ALLERRORGS* オプションを選択します。 • 非クラスタ化インデックスをチェックしない場合は、 * noindex * オプションを選択します。 SQL Server データベースは、 Microsoft SQL Server の Database Consistency Checker （ DBCC ）を使用して、データベース内のオブジェクトの論理的な整合性と物理的な整合性をチェックします。 このオプションを選択すると、実行時間を短縮できます。 • 内部データベースの Snapshot コピーを使用する代わりに、チェックを制限してロックを取得するには、 **TABLOCK** オプションを選択します。

6. 概要を確認し、 [終了] をクリックします。

SQL Server データベースのバックアップポリシーを作成する

SnapCenter を使用して SQL Server リソースをバックアップする前に、リソースまたはリソースグループのバックアップポリシーを作成することができます。また、リソースグループの作成時や単一のリソースのバックアップ時にバックアップポリシーを作成することもできます。

必要なもの

- データ保護戦略を定義しておく必要があります。
- SnapCenter のインストール、ホストの追加、リソースの特定、ストレージシステム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- ログバックアップ用のホストログディレクトリを設定しておく必要があります。
- SQL Server リソースを更新（検出）しておく必要があります。

- Snapshot コピーをミラーまたはバックアップにレプリケートするユーザには、 SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に Storage Virtual Machine （ SVM ）を割り当てる必要があります。

  管理者によるユーザへのリソースの割り当て方法については、 SnapCenter のインストール情報を参照してください。

- プリスクリプトとポストスクリプトで PowerShell スクリプトを実行する場合は、 web.config ファイルで usePowershellProcessforScripts パラメータの値を true に設定する必要があります。

  デフォルト値は false です。

このタスクについて

バックアップポリシーとは、バックアップを管理および保持する方法やリソースやリソースグループをバックアップする頻度を定めた一連のルールです。レプリケーションとスクリプトの設定を指定することもできます。ポリシーでオプションを指定しておくことで、別のリソースグループにポリシーを再利用して時間を節約することができます。

scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

手順**1**：ポリシー名を作成します

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。

ステップ**2**：バックアップオプションを設定します

1. バックアップタイプを選択します

フルバックアップとログバックアップ

データベースファイルとトランザクションログをバックアップし、トランザクションログを切り捨てます。

1. [フルバックアップおよびログバックアップ *] を選択します。
2. 各 Snapshot コピーにバックアップするデータベースの最大数を入力します。

同時に複数のバックアップ処理を実行する場合は、この値を増やす必要があります。

フル・バックアップ

データベースファイルをバックアップします。

1. [* Full backup*] を選択します。
2. 各 Snapshot コピーにバックアップするデータベースの最大数を入力します。
デフォルト値は 100 です

同時に複数のバックアップ処理を実行する場合は、この値を増やす必要があります。

ログバックアップ

トランザクションログをバックアップします。
。「 * Log backup * 」を選択します。

コピーのみのバックアップ

1. 別のバックアップ・アプリケーションを使用してリソースをバックアップする場合は、 [* コピーのみのバックアップ *] を選択します。

トランザクションログが変更されずに保持されるため、任意のバックアップアプリケーションでデータベースをリストアできます。通常、他の状況ではコピーのみのオプションを使用しないでください。

Microsoft SQL では、セカンダリ・ストレージのフル・バックアップおよびログ・バックアップ * オプションと * コピーのみのバックアップ * オプションはサポートされていません。

1. 可用性グループの設定セクションで、次の操作を実行します。
   a. 優先バックアップレプリカのみにバックアップ。

      優先バックアップレプリカのみをバックアップする場合は、このオプションを選択します。 優先バックアップレプリカは、 SQL Server の AG に対して設定されているバックアップ設定によって決まります。

   b. バックアップするレプリカを選択します。

      バックアップするプライマリまたはセカンダリの AG レプリカを選択します。

   c. バックアップ優先度の選択（最小および最大バックアップ優先度）

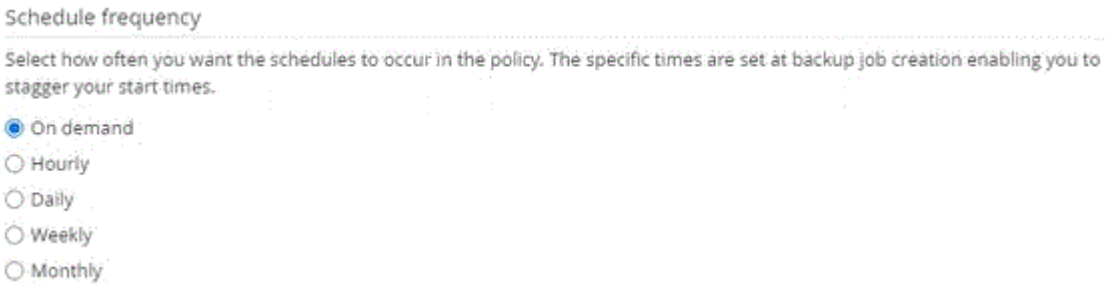
バックアップする AG レプリカを決めるための、バックアップの最小優先順位と最大優先順位を指定します。 たとえば、最小優先度を 10 、最大優先度を 50 に設定できます。この場合、優先順位が 10 より高く 50 より低いすべての AG レプリカがバックアップ用とみなされます。

デフォルトでは、最小プライオリティは 1 、最大プライオリティは 100 です。

クラスタ構成では、ポリシーで設定された保持設定に従って、クラスタの各ノードにバックアップが保持されます。AG の所有者ノードが変更された場合は、保持設定に従ってバックアップが作成され、以前の所有者ノードのバックアップが保持されます。AG の保持設定はノードレベルでのみ適用されます。

2. このポリシーのバックアップ頻度をスケジュールします。スケジュールタイプを指定するには、オンデマンド、毎時、毎日、毎週、または*毎月*を選択します。

   ポリシーに対して選択できるスケジュールタイプは1つだけです。



リソースグループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。

午前 2 時にスケジュールを設定した場合、夏時間（ DST ）中はスケジュールはトリガーされません。

ステップ**3**：保持設定を構成する

[保持] ページでは、 [バックアップ・タイプ] ページで選択したバックアップ・タイプに応じて、次のアクションを 1 つ以上実行します。

1. [最新の状態へのリストア処理の保持の設定] セクションで、次のいずれかを実行します。

特定のコピー数

特定の数のSnapshotコピーのみを保持します。

1. ［ * 最新の < 日数 > 日数に適用可能なログバックアップを保持する ］ オプションを選択し、保持する日数を指定します。この上限に近づいた場合は、古いコピーを削除できます。

特定の日数

バックアップコピーを特定の日数だけ保持します。

1. ［ * 最新の < 日数 > フル・バックアップに適用可能なログ・バックアップを保持する ］ オプションを選択し、ログ・バックアップ・コピーを保持する日数を指定します。

1. On Demand の保持設定の「 * フルバックアップの保持設定 * 」セクションで、次の操作を実行します。
   a. 保持するSnapshotコピーの総数を指定します
      i. 保持するSnapshotコピーの数を指定するには、*保持するSnapshotコピーの総数*を選択します。
      ii. Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。

デフォルトでは、保持数の値は 2 に設定されます。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。

最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。

1. Snapshotコピーを保持する期間
   a. Snapshot コピーを削除するまで保持しておく日数を指定する場合は、「 * Snapshot コピーを保持する期間」を選択します。
2. [毎時] 、 [毎日] 、 [毎週] 、および [毎月] の保持設定の [フルバックアップ保持設定 *] セクションで、 [バックアップタイプ] ページで選択したスケジュールタイプの保持設定を指定します。
   a. 保持するSnapshotコピーの総数を指定します
      i. 保持するSnapshotコピーの数を指定するには、*保持するSnapshotコピーの総数*を選択します。Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。

SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。

1. Snapshotコピーを保持する期間
   a. Snapshotコピーを削除するまで保持する日数を指定するには、*[Keep Snapshot copies for]*を選択します。

ログの Snapshot コピーの保持期間は、デフォルトで 7 日に設定されています。ログの Snapshot コピーの保持期間を変更するには、 Set-SmPolicy コマンドレットを使用します。

ログの Snapshot コピーの保持を 2 に設定する例を次に示します。

例 **1.** 例を示します

```
Set-SmPolicy-PolicyName 'newpol'-PolicyType 'Backup'-PluginPolicyType 'SCSQL'-sqlbackuptype
'FullBackupAndLogBackup'-RetentionSettings@｛backupType='Hourly'；RetentionCount=2｝、@
｛backupType='log_snapshot'；ScheduleType=2｝
```

"SnapCenter はデータベースの Snapshot コピーを保持します"

ステップ**4**：レプリケーション設定を構成します

1. Replication （レプリケーション）ページで、セカンダリストレージシステムへのレプリケーションを指定します。

SnapMirrorを更新します

ローカルSnapshotコピーの作成後にSnapMirrorを更新します。

1. 別のボリュームにバックアップセットのミラーコピーを作成する場合（ SnapMirror ）は、このオプションを選択します。

SnapVault を更新します

Snapshotコピーの作成後にSnapVault を更新

1. ディスクツーディスクのバックアップレプリケーションを実行する場合は、このオプションを選択します。

セカンダリポリシーラベル

1. Snapshot ラベルを選択します。

選択した Snapshot コピーラベルに応じて、 ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。

ローカル Snapshot コピーの作成後に「 * SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できます。ただし、ローカル Snapshot コピーの作成後に「 * Update SnapVault 」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。

エラー再試行回数

1. レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。

手順**5**：スクリプト設定を構成します

1. スクリプトページで、バックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

セカンダリストレージが Snapshot コピーの最大数に達しないように、 ONTAP で SnapMirror 保持ポリシーを設定する必要があります。

手順**6**：検証設定を構成します

[Verification] ページで、次の手順を実行します。

1. Run verification for following backup schedules セクションで、スケジュール頻度を選択します。
2. Database consistency check options セクションで、次の操作を実行します。
   a. 整合性構造をデータベースの物理構造に制限する（ physical_only ）
      i. 整合性チェックの対象をデータベースの物理構造に限定し、データベースに影響を与える正しくないページ、チェックサム障害、および一般的なハードウェア障害を検出するには、「 * 」を選択します。
   b. すべての情報メッセージを抑制（INFOMSGSなし）
      i. すべての情報メッセージを停止するには、「 * 」を選択します（ NO_INFOMSGS ）。デフォルトで選択されています。
   c. レポートされたすべてのエラー・メッセージをオブジェクトごとに表示する（ All_ERRORGS ）
      i. レポートされたエラーをオブジェクトごとにすべて表示する場合は、このオプションを選択します。
   d. 非クラスタ化インデックス（ noindex ）をチェックしない
      i. 非クラスタ化インデックスをチェックしない場合は、「 * 非クラスタ化インデックスをチェックしない」を選択します。 SQL Server データベースは、 Microsoft SQL Server の Database Consistency Checker （ DBCC ）を使用して、データベース内のオブジェクトの論理的な整合性と物理的な整合性をチェックします。
   e. 内部データベースの Snapshot コピー（ TABLOCK ）を使用せずに、チェックを制限してロックを取得します。
      i. 内部データベースの Snapshot コピーを使用する代わりに、チェックを制限してロックを取得する場合は、「 * 」を選択します。このオプションを選択すると、チェックが制限され、内部データベースの Snapshot コピーを使用する代わりにロックが取得されます。
3. [ログ・バックアップ *] セクションで、 [完了時にログ・バックアップを検証する *] を選択し、完了時にログ・バックアップを検証します。
4. 検証スクリプトの設定 * セクションで、検証処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

ステップ**7**：概要を確認します

1. 概要を確認し、 [完了] をクリックします。

SQL Server のリソースグループを作成してポリシーを適用します

リソースグループはコンテナであり、一緒にバックアップして保護するリソースをここに追加します。リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。リソースグループはすべてのデータ保護ジョブに必要です。リソースグループに 1 つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

リソースを個別に保護する場合、新しいリソースグループを作成する必要はありません。保護されたリソースでバックアップを作成することができます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。

   最近 SnapCenter にリソースを追加した場合は、 [* リソースの更新 *] をクリックして、新しく追加したリソースを表示します。

3. [New Resource Group] をクリックします。
4. [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループ名を入力します。 リソースグループ名は 250 文字以内にする必要があります。
タグ	リソースグループを検索するときに役立つラベルを入力します。 たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。
Snapshot コピーには、カスタムの名前形式を使用します	オプション： Snapshot コピー名のカスタムの名前形式を入力します。 たとえば、 customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

5. Resources ページで、次の手順を実行します。

a. ホスト名、リソースタイプ、および SQL Server インスタンスをドロップダウンリストから選択して、リソースのリストをフィルタリングします。

最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

b. [使用可能なリソース] セクションから [選択したリソース] セクションにリソースを移動するには、次のいずれかの手順を実行します。

- 同じボリューム上のすべてのリソースを [選択したリソース] セクションに移動するには、 * 同一ストレージボリューム上のすべてのリソースを自動選択 * を選択します。
- [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動する。

6. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

また、 * をクリックしてポリシーを作成することもできます *

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

b. [選択したポリシーのスケジュールを設定] セクションで、 * をクリックします * スケジュールを設定するポリシーの [スケジュールの設定] 列。

c. [Add schedules for policy_name_] ダイアログボックスで、開始日、有効期限、頻度を指定してスケジュールを設定し、 [*OK] をクリックします。

この処理は、ポリシーに指定されている頻度ごとに実行する必要があります。設定されたスケジュールは、 [選択したポリシーのスケジュールの設定 *] セクションの [適用されたスケジュール] 列に一覧表示されます。

d. Microsoft SQL Server スケジューラを選択します。

スケジューリングポリシーに関連付けるスケジューラインスタンスも選択する必要があります。

Microsoft SQL Server スケジューラを選択しなかった場合、デフォルトでは Microsoft Windows スケジューラが使用されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。Windowsスケジューラまたはは SQL Serverエージェントで作成されたバックアップジョブは、スケジュールを変更したり、名前を変更したりしないでください。

7. [Verification] ページで、次の手順を実行します。

a. [* Verification server*] ドロップダウン・リストから検証サーバを選択します。

このリストには、 SnapCenter で追加されたすべての SQL Server が含まれます。検証サーバ（ローカルホストまたはリモートホスト）は複数選択できます。

検証サーバのバージョンが、プライマリデータベースをホストしている SQL Server のバージョンとエディションと一致している必要があります。

a. Load locators * （ロケータのロード）をクリックして、 SnapMirror ボリュームと SnapVault ボリュームをロードし、セカンダリ・ストレージ上で検証を実行します。

b. 検証スケジュールを設定するポリシーを選択し、 * をクリックします + *

c. Add Verification Schedules policy_name ダイアログボックスで、次の操作を実行します。

状況	手順
バックアップ後に検証を実行します	[Run verification after backup] を選択します。
検証をスケジュールします	[スケジュールされた検証を実行する] を選択します。

d. [OK] をクリックします。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。確認して編集するには、 * をクリックします * または * をクリックして削除します *

8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、 [ジョブレポートの添付（ Attach Job Report ）] を選択します。

E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、 [完了] をクリックします。

- 詳細はこちら *

"SQL Server データベースのバックアップポリシーを作成する"

SQL リソースのバックアップに関する要件

SQL リソースをバックアップする前に、いくつかの要件を満たしていることを確認する必要があります。

- ネットアップ以外のストレージシステムからネットアップストレージシステムにリソースを移行しておく必要があります。
- バックアップポリシーを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合は、ストレージユーザに割り当てられた ONTAP ロールに「「 "napmirror all" 」権限を含める必要があります。ただし、「

vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。

- Active Directory （ AD ）ユーザによって開始されたバックアップ処理は、 SQL インスタンスのクレデンシャルが AD ユーザまたはグループに割り当てられていないと失敗します。SQL インスタンスの資格情報は、 * 設定 * > * ユーザーアクセス * ページから AD ユーザーまたはグループに割り当てる必要があります。
- ポリシーを適用したリソースグループを作成しておく必要があります。
- リソースグループに異なるホストの複数のデータベースが含まれている場合は、ネットワークの問題が原因で、一部のホストでバックアップ処理が遅く実行される可能性があります。Set-SmConfigSettings PS コマンドレットを使用して、 Web.config の FMaxRetryForUninitializedHosts の値を設定する必要があります。

SQL リソースをバックアップする

どのリソースグループにも含まれていないリソースは、のページからバックアップすることができます。

- このタスクについて *
- Windows クレデンシャル認証の場合は、プラグインをインストールする前にクレデンシャルを設定する必要があります。
- SQL Server インスタンス認証の場合、プラグインのインストール後にクレデンシャルを追加する必要があります。
- gMSA 認証の場合 'gMSA を有効にして使用するには '**Add Host** ページまたは **Modify Host** ページで SnapCenter にホストを登録するときに gMSA を設定する必要があります
- ホストを gMSA とともに追加し 'gMSA にログイン権限とシステム管理権限がある場合 'gMSA を使用して SQL インスタンスに接続します
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースページで、 * 表示 * ドロップダウン・リストから * データベース * 、 * インスタンス * 、または * 可用性グループ * を選択します。

   a. バックアップするデータベース、インスタンス、または可用性グループを選択します。

      インスタンスをバックアップする場合、そのインスタンスの前回のバックアップステータスやタイムスタンプに関する情報はリソースページに表示されません。

   トポロジビューでは、バックアップステータス、タイムスタンプ、またはバックアップがインスタンスのものかデータベースのものかを区別できません。

3. リソースページで、 Snapshot コピーの * カスタム名形式 * チェックボックスを選択し、 Snapshot コピー名に使用するカスタム名形式を入力します。

   たとえば 'customText_policy_hostname や resource_hostname などですデフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

4. [Policies] ページで、次のタスクを実行します。

a. [Policies] セクションで、ドロップダウンリストから 1 つ以上のポリシーを選択します。

ポリシーを作成するには、 * をクリックします * をクリックして、ポリシーウィザードを起動します。

[選択したポリシーのスケジュールを設定する *] セクションに、選択したポリシーが一覧表示されます。

b. * をクリックします * スケジュールを設定するポリシーの [スケジュールの設定] 列。

c. をクリックし、ポリシー*のスケジュールを追加します `policy_name` ダイアログボックスでスケジュールを設定し、* OK *をクリックします。

こちらをご覧ください `policy_name` は、選択したポリシーの名前です。

設定されたスケジュールは、 [* Applied Schedules] 列に表示されます。

a. Microsoft SQL Server スケジューラを使用する * を選択し、スケジューリング・ポリシーに関連付けられているスケジューラ・インスタンス * ドロップダウンリストからスケジューラ・インスタンスを選択します。

5. [Verification] ページで、次の手順を実行します。

a. [* Verification server*] ドロップダウン・リストから検証サーバを選択します。

検証サーバ（ローカルホストまたはリモートホスト）は複数選択できます。

検証サーバのバージョンは、プライマリデータベースをホストしている SQL Server のエディションと同じかそれ以上である必要があります。

a. セカンダリ・ストレージ・システム上のバックアップを検証するには ' セカンダリ・ロケータをロードを選択します

b. 検証スケジュールを設定するポリシーを選択し、 * をクリックします *

c. Add Verification Schedules_policy_name_dialog box で、次の処理を実行します。

状況	手順
バックアップ後に検証を実行します	[バックアップ後に検証を実行] を選択します。
検証をスケジュールします	[スケジュールされた検証を実行する] を選択します。

検証サーバでストレージ接続が確立されていないと、検証処理は失敗して「 Failed to mount disk 」というエラーメッセージが表示されます。

d. [OK] をクリックします。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

6. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、 [ジョブレポートの添付（ Attach Job Report ）] を選択します。

   E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して SMTP サーバの詳細を指定しておく必要があります。

7. 概要を確認し、 [完了] をクリックします。

   データベーストポロジのページが表示されます。

8. [今すぐバックアップ] をクリックします。
9. Backup （バックアップ）ページで、次の手順を実行します。

   a. リソースに複数のポリシーを適用している場合は、「 * Policy * 」ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. 「 * Verify after backup * 」を選択して、バックアップを検証します。
   c. [バックアップ] をクリックします。

      WindowsスケジューラまたはSQL Serverエージェントで作成されたバックアップジョブの名前は変更しないでください。

   オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

暗黙的なリソースグループが作成されます。これを表示するには、 [ユーザーアクセス（ User Access ）] ページで該当するユーザーまたはグループを選択します。暗黙的なリソースグループタイプは「リソース」です。

1. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

- 終了後 *
- MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。

  "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"

- VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。Java のヒープサイズを増やすには、スクリプトファイル /opt/NetApp/init_scripts/scvservice を探します。このスクリプトでは、を実行します `do_start method` コマンドは、SnapCenter VMwareプラグインサービスを開始します。このコマンドを次のように更新します。 `Java -jar -Xmx8192M -Xms4096M`。

- 詳細はこちら *

"SQL Server データベースのバックアップポリシーを作成する"

"PowerShell コマンドレットを使用してリソースをバックアップします"

"TCP_TIMEOUT での遅延のために MySQL 接続エラーが発生して、バックアップ処理が失敗します"

"Windows スケジューラのエラーでバックアップが失敗します"

"リソースの休止処理またはグループ化処理が失敗します"

SQL Server リソースグループをバックアップする

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。

   リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 * をクリックします* をクリックし、タグを選択します。次に、 * をクリックします* をクリックすると、フィルタペインが閉じます。

3. [リソースグループ] ページで、バックアップするリソースグループを選択し、 [今すぐバックアップ *] をクリックします。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. バックアップ後、 **verify** を選択して、オンデマンドバックアップを検証します。

      ポリシーの * verify * オプションは、スケジュールされたジョブにのみ適用されます。

   c. [バックアップ] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

- 詳細はこちら *

"SQL Server データベースのバックアップポリシーを作成する"

"SQL Server のリソースグループを作成してポリシーを適用します"

"PowerShell コマンドレットを使用してリソースをバックアップします"

"TCP_TIMEOUT での遅延のために MySQL 接続エラーが発生して、バックアップ処理が失敗します"

"Windows スケジューラのエラーでバックアップが失敗します"

バックアップ処理を監視する

SnapCenter Jobs ページで、 **SQL** リソースのバックアップ処理を監視します

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. Jobs （ジョブ）ページで、次の手順を実行します。
     a. をクリックします バックアップ処理だけが表示されるようにリストをフィルタリングします。
     b. 開始日と終了日を指定します。
     c. [* タイプ] ドロップダウン・リストから、 **[*Backup]** を選択します。
     d. [**Status**](ステータス *) ドロップダウンから、バックアップステータスを選択します。
     e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
  4. バックアップジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

     バックアップジョブのステータスがと表示されます で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

     View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

［ アクティビティ ］ ペインで、 **SQL** リソースのデータ保護操作を監視します

[アクティビティ（ Activity ）] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity （アクティビティ）] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. をクリックします をクリックして、最近の 5 つの操作を表示します。

   いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

PowerShell コマンドレットを使用してストレージシステム接続とクレデンシャルを作成します

PowerShell コマンドレットを使用してデータ保護処理を実行するには、 Storage Virtual Machine （ SVM ）接続とクレデンシャルを作成する必要があります。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前および管理 LIF の IP アドレスを割り当てる必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、 PowerShell 接続セッションを開始します。

   PowerShell セッションを開く例を次に示します。

   ```
   PS C:\> Open-SmConnection
   ```

2. Add-SmStorageConnection コマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

この例では、新しいストレージシステム接続を作成しています。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Add-SmCredential コマンドレットを使用して新しいクレデンシャルを作成します。

   この例は、 Windows クレデンシャルを使用して FinanceAdmin という名前の新しいクレデンシャルを作成します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

PowerShell コマンドレットを使用してリソースをバックアップします

PowerShell コマンドレットを使用して、 SQL Server データベースや Windows ファイルシステムをバックアップできます。たとえば、 SQL Server データベースまたは Windows ファイルシステムのバックアップでは、 SnapCenter サーバとの接続の確立、 SQL Server データベースインスタンスまたは Windows ファイルシステムの検出、ポリシーの追加、バックアップリソースグループの作成、バックアップ、およびバックアップの検証が行われます。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。
- ホストを追加し、リソースを検出しておく必要があります。
- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmPolicy コマンドレットを使用してバックアップポリシーを作成します。

   この例では、 SQL のバックアップタイプ「 FullBackup 」を指定して新しいバックアップポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

この例では、 Windows ファイルシステムのバックアップタイプ「 CrashConsistent 」を指定して新しいバックアップポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResources コマンドレットを使用して、ホストリソースを検出します。

   この例では、指定したホスト上で Microsoft SQL プラグインのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   この例では、指定したホスト上で Windows ファイルシステムのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add-SmResourceGroup コマンドレットを使用して、新しいリソースグループを SnapCenter に追加します。

   この例では、ポリシーとリソースを指定して新しい SQL データベースバックアップリソースグループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   この例では、ポリシーとリソースを指定して新しい Windows ファイルシステムバックアップリソースグループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackup コマンドレットを使用して、新しいバックアップジョブを開始する。

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Get-SmBackupReport コマンドレットを使用して、バックアップジョブのステータスを表示します。

   次の例は、指定した日付に実行されたすべてのジョブの概要レポートを表示します。

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapCenter Plug-in for Microsoft SQL Server のバックアップ処理をキャンセルします

実行中、キューに登録済み、または応答しないバックアップ処理をキャンセルできます。バックアップ処理をキャンセルすると、 SnapCenter サーバは処理を停止し、作成されたバックアップが SnapCenter サーバに登録されていない場合は、ストレージからすべての Snapshot コピーを削除します。バックアップがすでに SnapCenter サーバに登録されている場合、キャンセル後も、作成済みの Snapshot コピーはロールバックされません。

- 必要なもの *
- リストア処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。
- キャンセルできるのは、キューに登録されたか実行中のログ処理またはフルバックアップ処理のみです。
- 検証の開始後に処理をキャンセルすることはできません。

  検証前に処理をキャンセルした場合、処理はキャンセルされ、検証処理は実行されません。

- バックアップ処理は、 Monitor （モニタ）ページまたは Activity （アクティビティ）ペインからキャンセルできます。
- PowerShell コマンドレットを使用すると、 SnapCenter GUI に加え、処理をキャンセルできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っているバックアップ操作をキャンセルできます
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. ジョブを選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. バックアップジョブを開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ジョブの詳細］ページで、 ［* ジョブのキャンセル *］ をクリックします。

- 結果 *

処理がキャンセルされ、リソースが以前の状態に戻ります。キャンセルまたは実行状態でキャンセルした処理が応答しない場合は、を実行する必要があります `Cancel-SmJob -JobID <int> -Force` コマンドレットを使用して、バックアップ処理を強制的に停止できます。

トポロジページで **SQL Server** のバックアップとクローンを表示します

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

- このタスクについて *

トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

[コピーの管理（ Manage Copies ）] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップとクローンが使用可能かどうかを判断できます。

- には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
- には、 SnapMirror テクノロジを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。
- には、 SnapVault テクノロジを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。
  - 表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれま

す。

たとえば、 4 つのバックアップだけを保持するポリシーを使用して 6 つのバックアップを作成した場合、バックアップの数は 6 と表示されます。

mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

   選択したリソースがクローンデータベースの場合、クローンデータベースを保護すると、トポロジページにクローンのソースが表示されます。詳細 * をクリックして、クローニングに使用されたバックアップを表示します。

   リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. 概要カードを確認して、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数をサマリで確認します。

   サマリカード * セクションには、バックアップとクローンの合計数が表示されます。

「 * Refresh * 」ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

1. [コピーの管理] 表示で、プライマリ・ストレージまたはセカンダリ・ストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

   バックアップとクローンの詳細が表形式で表示されます。

2. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。

   セカンダリストレージ上のバックアップは、名前変更または削除できません。

3. テーブルからクローンを選択し、 * Clone Split * をクリックします。
4. クローンを削除する場合は、表でクローンを選択し、をクリックします 。

PowerShell コマンドレットを使用してバックアップを削除します

Remove-SmBackup コマンドレットを使用すると、他のデータ保護処理に不要になったバックアップを削除できます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Remove-SmBackup コマンドレットを使用して 1 つ以上のバックアップを削除します。

   この例では、バックアップ ID を指定してバックアップを 2 つ削除しています。

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

PowerShell コマンドレットを使用してセカンダリバックアップ数をクリーンアップします

Remove-SmBackup コマンドレットを使用して、 Snapshot コピーがないセカンダリバックアップのバックアップ数をクリーンアップできます。Manage Copies （コピーの管理）トポロジに表示される Snapshot コピーの合計数が、セカンダリ・ストレージの Snapshot コピーの保持設定と一致しない場合に、このコマンドレットを使用できます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. CleanupSecondaryBackups パラメータを使用して、セカンダリバックアップ数をクリーンアップします。

   この例では、 Snapshot コピーがないセカンダリバックアップのバックアップ数をクリーンアップし

ています。

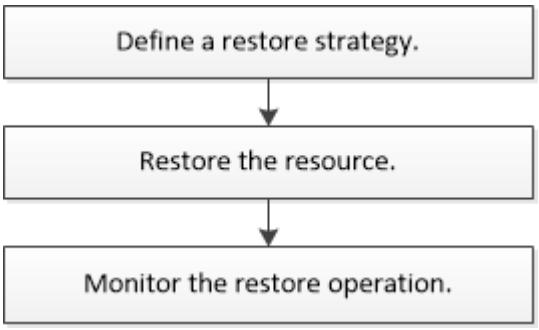
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

SQL Server リソースをリストアする

リストアワークフロー

SnapCenter を使用して SQL Server データベースをリストアするには、 1 つ以上のバックアップからアクティブファイルシステムにデータをリストアし、データベースをリカバリします。可用性グループ内のデータベースをリストアし、リストアしたデータベースを可用性グループに追加することもできます。SQL Server データベースをリストアする前に、いくつかの準備作業を実行する必要があります。

次のワークフローは、データベースリストア処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、リカバリ、検証、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェア 4.4 コマンドレットリファレンスガイド"

- 詳細はこちら *

"セカンダリストレージから SQL Server データベースをリストアする"

"PowerShell コマンドレットを使用してリソースをリストアおよびリカバリする"

"Windows 2008 R2 でリストア処理が失敗することがあります"

データベースをリストアするための要件

SnapCenter Plug-in for Microsoft SQL Server のバックアップから SQL Server データベースをリストアする前に、以下の要件を満たしていることを確認する必要があります。

- データベースをリストアするには、ターゲットの SQL Server インスタンスがオンラインで稼働している必要があります。

  この環境では、ユーザデータベースのリストア処理とシステムデータベースのリストア処理の両方が実行されます。

- リモートアドミニストレーションサーバまたはリモート検証サーバでスケジュール設定しているジョブも含め、リストアする SQL Server データに対して実行されるスケジュール設定されている SnapCenter 処理を無効にする必要があります。
- システムデータベースが機能していない場合は、まず SQL Server ユーティリティを使用してシステムデータベースを再構築する必要があります。
- プラグインをインストールするときは、可用性グループ（ AG ）バックアップをリストアする権限を他のロールに付与します。

  次のいずれかの条件に該当する場合、 AG のリストアが失敗します。

  - RBAC ユーザがプラグインをインストールし、管理者が AG バックアップをリストアしようとした場合
  - 管理者がプラグインをインストールし、 RBAC ユーザが AG バックアップをリストアしようとした場合
- カスタム・ログ・ディレクトリのバックアップを代替ホストにリストアする場合は、 SnapCenter サーバとプラグイン・ホストに同じバージョンの SnapCenter がインストールされている必要があります。
- Microsoft の修正プログラム KB2887595 をインストールしておく必要があります。マイクロソフトサポートサイトには、 KB2887595 に関する詳細情報が記載されています。

  "Microsoft のサポート記事 2887595 ：「 Windows RT 8.1 、 Windows 8.1 、 and Windows Server 2012 R2 update rollup ： November 2013"

- リソースグループまたはデータベースをバックアップしておく必要があります。
- Snapshot コピーをミラーまたはバックアップにレプリケートするユーザには、 SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に Storage Virtual Machine （ SVM ）を割り当てる必要があります。

  管理者によるユーザへのリソースの割り当て方法については、 SnapCenter のインストール情報を参照してください。

- データベースをリストアする前に、バックアップジョブとクローニングジョブをすべて停止する必要があります。
- データベースサイズがテラバイト（ TB ）単位の場合、リストア処理がタイムアウトすることがあります。

  次のコマンドを実行して、 SnapCenter サーバの RESTTimeout パラメータの値を 20000000ms に増やす必要があります。 Set-SmConfigSettings -Agent -configSettings @ ｛ "RESTTimeout" = "20000000" ｝ 。データベースのサイズによっては、タイムアウト値を変更できます。また、設定できる最大値は86400000msです。

データベースをオンラインにしたままリストアする場合は、リストアページでオンラインリストアオプションを有効にする必要があります。

SQL Server データベースのバックアップをリストアする

SnapCenter を使用して、バックアップされた SQL Server データベースをリストアできます。データベースのリストアは段階的に実施され、すべてのデータページとログページが指定した SQL Server バックアップから指定したデータベースにコピーされます。

- このタスクについて *
- バックアップされた SQL Server データベースを、バックアップが作成されたホスト上の別の SQL Server インスタンスにリストアすることができます。

  本番バージョンを置き換えないように、 SnapCenter を使用して、バックアップされた SQL Server データベースを別のパスにリストアすることができます。

- SnapCenter では、 SQL Server クラスタグループをオフラインにすることなく、 Windows クラスタ内のデータベースをリストアできます。
- リストア処理中に、リソースを所有するノードがダウンするなどのクラスタ障害（クラスタグループの移動処理）が発生した場合は、 SQL Server インスタンスに再接続してからリストア処理を再開する必要があります。
- ユーザまたは SQL Server Agent ジョブがデータベースにアクセスしている間は、データベースをリストアできません。
- システムデータベースは別のパスにリストアできません。
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

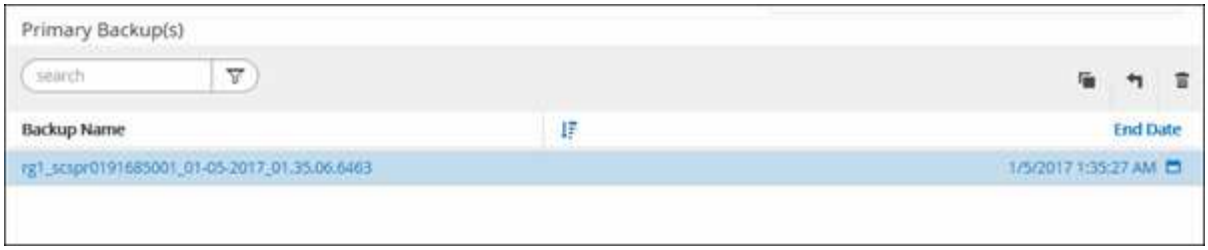
  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- リストアウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要なフィールドを取り上げます。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. リストからデータベースまたはリソースグループを選択します。

   トポロジページが表示されます。

4. [コピーの管理] ビューで、ストレージ・システムから [* バックアップ *] を選択します。
5. 表からバックアップを選択し、をクリックします  をクリックします。



6. [リストア範囲] ページで、次のいずれかのオプションを選択します。

オプション	説明
バックアップが作成されたホストにデータベースをリストアします	バックアップを作成した SQL Server にデータベースをリストアする場合は、このオプションを選択します。
データベースを代替ホストにリストアします	バックアップを作成したホストと同じまたは別のホストの別の SQL Server にデータベースをリストアする場合は、このオプションを選択します。 ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。 代替パスに指定するファイル拡張子は、元のデータベースファイルのファイル拡張子と同じにする必要があります。 [リストア範囲] ページに [データベースを別のホストにリストアする *] オプションが表示されない場合は、ブラウザキャッシュをクリアします。
既存のデータベースファイルを使用してデータベースをリストアします	バックアップを作成したホストと同じまたは別のホストの代替 SQL Server にデータベースをリストアする場合は、このオプションを選択します。 指定した既存のファイルパスには、データベースファイルがすでに存在している必要があります。ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。

7. Recovery Scope ページで、次のいずれかのオプションを選択します。

オプション	説明
なし	ログなしでフルバックアップのみをリストアする必要がある場合は、「 * なし」を選択します。

オプション	説明
すべてのログバックアップ	フルバックアップ後に使用可能なすべてのログバックアップをリストアするには、「 * all log backups * up-to-the-minute backup restore operation 」を選択します。
までログバックアップでバックアップします	「ログバックアップによる * 」を選択してポイントインタイムリストア処理を実行します。この場合、選択した日付のバックアップログまで、バックアップログに基づいてデータベースがリストアされます。
期限までの特定の日付	リストアされたデータベースにトランザクション・ログを適用しない日時を指定するには、 [* までの特定の日付] を選択します。 ポイントインタイムリストア処理では、指定した日時以降に記録されたトランザクションログエントリがリストアされません。
カスタムログディレクトリを使用します	すべてのログ・バックアップ * 、ログ・バックアップ * 、または * を指定日までに * とログがカスタム・ロケーションにある場合は、 * カスタム・ログ・ディレクトリを使用 * を選択し、ログの場所を指定します。 オプションは、[Restore the database to an alternate host]または[Restore the database using existing database files]*を選択した場合にのみ使用できます。共有パスを使用することもできますが、そのパスにSQLユーザがアクセスできることを確認してください。 可用性グループデータベースではカスタムログディレクトリはサポートされません。

8. Pre Ops ページで、次の手順を実行します。

   a. [リストア前のオプション] ページで、次のいずれかのオプションを選択します。

      - [リストア時に同じ名前でデータベースを上書きする] を選択して、同じ名前でデータベースをリストアします。
      - データベースをリストアし、既存のレプリケーション設定を保持するには、「 * SQL データベースのレプリケーション設定を保持 * 」を選択します。
      - リストア処理を開始する前にトランザクションログバックアップを作成する場合は、「リストア前にトランザクションログバックアップを作成」を選択します。
      - トランザクションログのバックアップに失敗した場合は、「 * リストアの終了」を選択して、リストア処理を中止します。

b. リストアジョブの実行前に実行するオプションのスクリプトを指定します。

たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

9. Post Ops ページで、次の手順を実行します。

a. リストア完了後のデータベース状態の選択セクションで、次のいずれかのオプションを選択します。

- 必要なすべてのバックアップを今すぐリストアする場合は、「動作中ですが、追加のトランザクション・ログをリストアできません」を選択します。

  これはデフォルトの動作で、コミットされていないトランザクションをロールバックすることでデータベースを使用可能な状態にします。バックアップを作成するまで追加のトランザクションログはリストアできません。

- [非運用時] を選択します。ただし、トランザクションログを追加でリストアすることができます。 * を選択すると、コミットされていないトランザクションをロールバックせずに、データベースが非運用状態のままになります。

  追加のトランザクションログをリストアできます。データベースはリカバリされるまで使用できません。

- データベースを読み取り専用モードのままにするには、追加のトランザクションログのリストアに使用できる * 読み取り専用モードを選択します。

  コミットされていないトランザクションはロールバックされますが、ロールバックされた操作がスタンバイファイルに保存されるため、リカバリ前の状態に戻すことができます。

[ディレクトリを元に戻す] オプションが有効になっている場合は、さらに多くのトランザクションログがリストアされます。トランザクションログのリストア処理が失敗した場合は、変更をロールバックできます。詳細については、 SQL Server のマニュアルを参照してください。

a. リストアジョブの実行後に実行するオプションのスクリプトを指定します。

たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。

2. 概要を確認し、 [完了] をクリックします。
3. [* Monitor * > * Jobs *] ページを使用してリストア・プロセスを監視します。

- 詳細はこちら *

"PowerShell コマンドレットを使用してリソースをリストアおよびリカバリする"

"セカンダリストレージから SQL Server データベースをリストアする"

セカンダリストレージから **SQL Server** データベースをリストアする

セカンダリストレージシステム上の物理 LUN （ RDM 、 iSCSI 、または FCP ）から、バックアップされた SQL Server データベースをリストアすることができます。リストアは段階的に実施され、すべてのデータとログページがセカンダリストレージシステム上の指定した SQL Server バックアップから指定したデータベースにコピーされます。

- 必要なもの *
- プライマリストレージシステムからセカンダリストレージシステムに Snapshot コピーをレプリケートしておく必要があります。
- SnapCenter サーバおよびプラグインホストがセカンダリストレージシステムに接続できることを確認する必要があります。
- リストア・ウィザードの各ページのフィールドのほとんどについては、基本的なリストア・プロセスで説明しています。以下の手順では、説明が必要な一部のフィールドを取り上げます。
- 手順 *
  1. 左側のナビゲーションペインで、 [* リソース **]** をクリックし、リストから **[** SnapCenter Plug-in for SQL Server] を選択します。
  2. [リソース] ページで、 [*View] ドロップダウン・リストから [*Database] または [*Resource Group] を選択します。
  3. データベースまたはリソースグループを選択します。

     データベースまたはリソースグループのトポロジページが表示されます。
  4. [コピーの管理] セクションで、セカンダリ・ストレージ・システム（ミラーまたはバックアップ）から * バックアップ * を選択します。
  5. リストからバックアップを選択し、をクリックします  。
  6. [場所] ページで、選択したリソースを復元する宛先ボリュームを選択します。
  7. リストア・ウィザードを完了し ' 概要を確認してから '[* 終了 *] をクリックします

他のデータベースが共有している別のパスにデータベースをリストアした場合は、フルバックアップとバックアップ検証を実行して、リストアしたデータベースが物理レベルで破損していないことを確認してください。

可用性グループデータベースを再シードしています

再シードは、可用性グループ（ AG ）データベースをリストアするためのオプションです。セカンダリデータベースが AG 内のプライマリデータベースと同期していない場合は、セカンダリデータベースを再シードできます。

- 必要なもの *
- リストアするセカンダリ AG データベースのバックアップを作成しておく必要があります。
- SnapCenter サーバとプラグインホストに同じ SnapCenter バージョンがインストールされている必要があります。
- このタスクについて *
- プライマリデータベースには再シード処理を実行できません。
- 可用性グループからレプリカデータベースが削除された場合は、再シード処理を実行できません。レプリカを削除すると、再シード処理が失敗します。
- SQL 可用性グループデータベースで再シード処理を実行する場合、その可用性グループデータベースのレプリカデータベースでログバックアップをトリガーしないでください。再シード処理中にログバックアップをトリガーすると、ミラーデータベースの再シード処理が失敗し、「 database_name 」にはプリンシパルデータベースのログバックアップチェーンを保持するための十分なトランザクションログデータがありませんというエラーメッセージが表示されます。
- 手順 *
  1. 左側のナビゲーションペインで、 [* リソース **]** をクリックし、リストから **[** SnapCenter Plug-in for SQL Server] を選択します。
  2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。
  3. リストからセカンダリ AG データベースを選択します。
  4. [Reseed-*] をクリックします。
  5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用してリソースをリストアする

リソースのバックアップをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *
  1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

     ```
     Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
     ```

  2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップに関する情報を取得します。

     この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

この例では、 2015 年 1 月 29 日から 2015 年 2 月 3 日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

1. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SQL リソースのリストア処理を監視する

Jobs ページを使用して、 SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします リストをフィルタリングして、リストア処理のみを表示します。
   b. 開始日と終了日を指定します。
   c. [* タイプ] ドロップダウン・リストから、 [リストア *] を選択します。
   d. [* Status *] ドロップダウン・リストから、リストア・ステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

   View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

SQL リソースのリストア処理をキャンセルします

キューに格納されているリストアジョブをキャンセルできます。

リストア処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *
- キューに登録されたリストア処理は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、キューに登録されたリ

ストア処理をキャンセルできます。

- キャンセルできないリストア処理の場合、 [ジョブのキャンセル] ボタンは使用できません。
- ロールの作成中に [ユーザー \ グループ] ページで [このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できる] を選択した場合は、そのロールを使用している間に、他のメンバーのキューに登録されているリストア操作をキャンセルできます。
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. ジョブを選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. リストア処理を開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ ジョブの詳細 ］ ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

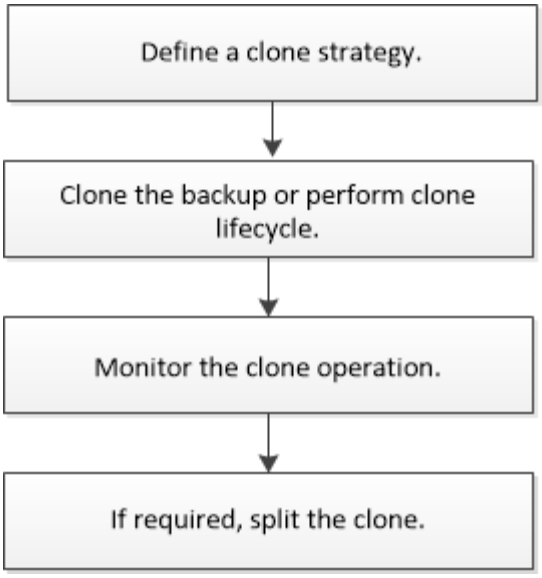
SQL Server データベースリソースのクローニング

クローニングワークフロー

バックアップからデータベースリソースをクローニングする前に、 SnapCenter Server でいくつかのタスクを実行する必要があります。データベースのクローニングは、本番環境のデータベースまたはそのバックアップセットのポイントインタイムコピーを作成するプロセスです。アプリケーション開発サイクル中に実装が必要な機能を現在のデータベースの構造およびコンテンツを使用してテストする場合、データの抽出と操作を行うツールを使用してデータウェアハウスにデータを取り込む場合、誤って削除または変更されたデータをリカバリする場合などに実行します。

データベースのクローニング処理では、ジョブ ID に基づいてレポートが生成されます。

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、リカバリ、検証、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

- 詳細はこちら *

"SQL Server データベースバックアップからのクローニング"

"クローンライフサイクルの実行"

"デフォルトの TCP_TIMEOUT 値を使用すると、クローニング処理が失敗するか所要時間が長くなる可能性があります"

SQL Server データベースバックアップからのクローニング

SnapCenter を使用して、 SQL Server データベースバックアップをクローニングすることができます。古いバージョンのデータにアクセスしたりリストアしたりする場合は、データベースバックアップをオンデマンドでクローニングできます。

- 必要なもの *
- データ保護の準備として、ホストの追加、リソースの特定、ストレージシステム接続の作成などのタスクを完了しておく必要があります。
- データベースまたはリソースグループをバックアップしておく必要があります。
- ログバックアップを使用した代替ホストへのクローニング中にセカンダリロケータを検出するには、データ LUN およびログ LUN のミラー、バックアップ、ミラー - ヴォールトなどの保護タイプを同じにする必要があります。
- SnapCenter のクローン処理中にマウントされたクローンドライブが見つからない場合は、 SnapCenter サーバの CloneRetryTimeout パラメータを 300 に変更する必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine （ SVM ）に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- このタスクについて *

- スタンドアロンデータベースインスタンスにクローニングする際には、マウントポイントパスが存在し、専用ディスクであることを確認してください。
- フェイルオーバークラスタインスタンス（ FCI ）にクローニングする際は、マウントポイントが存在すること、共有ディスクであること、およびパスと FCI が同じ SQL リソースグループに属していることを確認してください。
- 各ホストに接続された vFC または FC イニシエータが 1 つだけであることを確認します。これは、SnapCenter でサポートされるホストあたりのイニシエータの数が 1 つであるためです。
- ソースデータベースまたはターゲットインスタンスがクラスタ共有ボリューム（ CSV ）上にある場合、クローニングされたデータベースは CSV 上に作成されます。
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

仮想環境（ VMDK / RDM ）の場合は、マウントポイントが専用ディスクであることを確認します。

- 手順 *

1. 左側のナビゲーションペインで、 [* リソース **]** をクリックし、リストから **[** SnapCenter Plug-in for SQL Server] を選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。

   インスタンスのバックアップのクローニングはサポートされていません。

- 手順 *

1. データベースまたはリソースグループを選択します。
2. Manage Copies （コピーの管理）ビューページから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムからバックアップを選択します。
3. バックアップを選択し、 * をクリックします *
4. Clone Options ページで、次の操作を実行します。

フィールド	手順
クローンサーバ	クローンを作成するホストを選択します。

フィールド	手順
インスタンスをクローニングします	データベースバックアップのクローニング先となるクローンインスタンスを選択します。 指定したクローンサーバ上の SQL インスタンスを選択する必要があります。
クローンのサフィックス	クローンファイル名に付加される、データベースがクローンであることを示すサフィックスを入力します。 たとえば、 *db1_clone*.元のデータベースと同じ場所にクローニングする場合、クローニングされたデータベースを元のデータベースと区別するためにサフィックスを指定する必要があります。そうしないと、処理は失敗します。
Auto assign mount point または Auto assign volume mount point under path	マウントポイントを自動的に割り当てるか、パスを指定してボリュームマウントポイントを自動的に割り当てるかを選択します。 Auto assign volume mount point under path ：特定のディレクトリのパスを指定できます。指定したディレクトリにマウントポイントが作成されます。このオプションを選択する前に、ディレクトリが空であることを確認する必要があります。ディレクトリにデータベースが格納されている場合、そのデータベースはマウント処理後に無効な状態になります。

5. Logs ページで、次のいずれかのオプションを選択します。

フィールド	手順
なし	ログなしでフルバックアップのみをクローニングする場合は、このオプションを選択します。
すべてのログバックアップ	フルバックアップ後の日付のログバックアップをすべてクローニングする場合は、このオプションを選択します。
までログバックアップでバックアップします	選択した日付のバックアップログまでに作成されたバックアップログに基づいてデータベースをクローニングする場合、このオプションを選択します。

フィールド	手順
期限までの特定の日付	クローニングされたデータベースにトランザクションログを適用する最終日時を指定します。 ポイントインタイムのクローニングでは、指定した日時以降に記録されたトランザクションログエントリがクローニングされません。

6. スクリプトページで、クローニング処理の前後に実行するスクリプトのタイムアウト、パス、および引数をプリスクリプトまたはポストスクリプトで入力します。

   たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   > プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

   デフォルトのスクリプトタイムアウトは 60 秒です。

7. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、 * ジョブレポートの添付 * を選択します。

   > E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

EMS については、を参照してください "EMS データ収集を管理します"

1. 概要を確認し、 [完了] をクリックします。
2. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

- 終了後 *

作成したクローンは、名前を変更しないでください。

- 詳細はこちら *

"SQL Server データベース、インスタンス、または可用性グループをバックアップする"

"PowerShell コマンドレットを使用してバックアップをクローニングする"

"デフォルトの TCP_TIMEOUT 値を使用すると、クローニング処理が失敗するか所要時間が長くなる可能性があります"

"フェイルオーバークラスタインスタンスのデータベースクローンが失敗します"

PowerShell コマンドレットを使用してバックアップをクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup コマンドレットまたは Get-SmResourceGroup コマンドレットを使用して、クローニングできるバックアップのリストを表示します。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                      BackupTime   BackupType
--------   ----------                      ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   この例では、指定したリソースグループとそのリソース、および関連ポリシーに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
```

```
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
```

```
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. New-SmClone コマンドレットを使用して、既存のバックアップからクローニング処理を開始する。

   この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

この例では、指定した Microsoft SQL Server インスタンスのクローンを作成しています。

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Get-SmCloneReport コマンドレットを使用して、クローニングジョブのステータスを表示します。

   この例では、指定したジョブ ID のクローンレポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

クローンライフサイクルの実行

SnapCenter を使用すると、リソースグループまたはデータベースからクローンを作成できます。クローニングはオンデマンドで実行することも、リソースグループまたはデータベースの定期的なクローニング処理をスケジュール設定することもできます。バックアップを定期的にクローニングすると、クローンを使用してアプリケーションの開発、データの取り込み、またはデータのリカバリを行うことができます。

SnapCenter では、複数のサーバで同時に複数のクローニング処理を実行するようにスケジュールを設定できます。

- 必要なもの *
- スタンドアロンデータベースインスタンスにクローニングする際には、マウントポイントパスが存在し、専用ディスクであることを確認してください。
- フェイルオーバークラスタインスタンス（ FCI ）にクローニングする際は、マウントポイントが存在すること、共有ディスクであること、およびパスと FCI が同じ SQL リソースグループに属していることを確認してください。
- ソースデータベースまたはターゲットインスタンスがクラスタ共有ボリューム（ CSV ）上にある場合、クローニングされたデータベースは CSV 上に作成されます。

仮想環境（ VMDK / RDM ）の場合は、マウントポイントが専用ディスクであることを確認します。

- このタスクについて *
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- クローンライフサイクルウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要なフィールドを取り上げます。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. リソースグループまたはデータベースを選択し、 * クローンライフサイクル * をクリックします。
4. [オプション] ページで、次の操作を実行します。

フィールド	手順
クローンジョブ名	クローンライフサイクルジョブの名前を指定します。この名前は、クローンライフサイクルジョブを監視および変更する際に役立ちます。
クローンサーバ	クローンをどのホストに配置するかを選択します。
インスタンスをクローニングします	データベースのクローニング先となるクローンインスタンスを選択します。 指定したクローンサーバ上の SQL インスタンスを選択する必要があります。

フィールド	手順
クローンのサフィックス	クローンデータベースに付加される、クローンであることを示すサフィックスを入力します。 クローンリソースグループの作成に使用する各 SQL インスタンスには、一意のデータベース名が必要です。たとえば、クローンリソースグループに SQL インスタンス「 inst1 」からのソースデータベース「 `d b1' 」が含まれ、「 `db1' 」が「 `inst1' 」にクローンされている場合、クローンデータベース名は「 `d b1_clone_ 」になります。データベースが同じインスタンスにクローンされるため '`__ clone は ' ユーザー定義の必須サフィックスです「 `db1' 」が `SQL` インスタンス「 `inst2` 」にクローンされている場合、データベースは別のインスタンスにクローンされるため、クローンデータベース名は「 `db1' 」のままでかまいません（サフィックスはオプションです）。
Auto assign mount point または Auto assign volume mount point under path	マウントポイントを自動的に割り当てるか、またはパスを指定してボリュームマウントポイントを自動的に割り当てるかを選択します。 パスの下にボリュームマウントポイントを自動で割り当てることを選択すると、特定のディレクトリを指定できます。指定したディレクトリにマウントポイントが作成されます。このオプションを選択する前に、ディレクトリが空であることを確認する必要があります。ディレクトリにデータベースが格納されている場合、そのデータベースはマウント処理後に無効な状態になります。

5. [場所] ページで、クローンを作成するストレージの場所を選択します。
6. スクリプトページで、クローニング処理の実行前または実行後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

   たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

   デフォルトのスクリプトタイムアウトは 60 秒です。

7. [スケジュール] ページで、次のいずれかの操作を実行します。
   - クローニングジョブをすぐに実行する場合は、「 * Run Now * 」を選択します。
   - クローン処理の実行頻度、クローンスケジュールの開始日時、クローニング処理の実行日、スケジュールの期限、スケジュールの期限が切れたあとにクローンを削除する必要があるかどうかを指定する場合は、 * Configure schedule * を選択します。

8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、 * ジョブレポートの添付 * を選択します。

   E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

EMS については、を参照してください "EMS データ収集を管理します"

1. 概要を確認し、 [完了] をクリックします。

クローニング処理は、 * Monitor * > * Jobs * ページで監視する必要があります。

SQL データベースのクローニング処理を監視する

Jobs ページを使用して、 SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. Jobs （ジョブ）ページで、次の手順を実行します。
     a. をクリックします をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
     b. 開始日と終了日を指定します。
     c. [**Type**](タイプ **)** ドロップダウンリストから **'[*Clone**](クローン *) を選択します
     d. [* Status *] ドロップダウン・リストから、クローンのステータスを選択します。
     e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
  4. クローンジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。

5. ［ジョブの詳細］ページで、［ * ログの表示 * ］をクリックします。

SQL リソースのクローニング処理をキャンセルする

キューに登録されているクローニング処理をキャンセルできます。

クローニング処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *
- キューに登録されたクローン処理は、 * Monitor * ページまたは * Activity * ペインからキャンセルできます。
- 実行中のクローン処理はキャンセルできません。
- キューに登録されたクローニング処理をキャンセルするには、 SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用します。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用しているときに ' 他のメンバーのキューに登録されているクローン操作をキャンセルできます
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. 操作を選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. クローニング処理を開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ジョブの詳細］ページで、［ * ジョブのキャンセル * ］をクリックします。

クローンをスプリットします。

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

- このタスクについて *
- 中間のクローンに対してクローンスプリット処理を実行することはできません。

  たとえば、データベースバックアップから clone1 を作成したあとで、 Clone1 のバックアップを作成し、そのバックアップ（ Clone2 ）をクローニングできます。Clone2 を作成すると、 clone1 は中間クローン

であり、 clone1 でクローンスプリット処理を実行することはできません。ただし、 Clone2 でクローンスプリット処理を実行することはできます。

Clone2 をスプリットしたあとは、 clone1 が中間クローンではなくなるため、 clone1 でクローンスプリット処理を実行できます。

- クローンをスプリットすると、クローンのバックアップコピーとクローンジョブが削除されます。
- クローンスプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。
- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [表示] リストから適切なオプションを選択します。

オプション	説明
データベースアプリケーション用	[表示] リストから [*Database] を選択します。
ファイルシステムの場合	[表示] リストから [* パス *] を選択します。

3. リストから適切なリソースを選択します。

   リソースのトポロジページが表示されます。

4. [コピーの管理] ビューで、クローン作成されたリソース（データベースや LUN など）を選択し、 [*] をクリックします *
5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   SMCore サービスが再起動すると、クローンスプリット処理が応答しなくなります。Stop-SmJob コマンドレットを実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

   クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、 _SMCoreServiceHost.exe.config_file の _CloneSplitStatusCheckPollTime_Parameter の値を変更して、 SMCore がクローンスプリット処理のステータスをポーリングする間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

   例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

+
バックアップ、リストア、または別のクローンスプリットの実行中は、クローンスプリットの開始処理が

失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

- 詳細はこちら *

"「 aggregate does not exist 」というメッセージが表示されて、 SnapCenter クローンまたは検証が失敗する"

SAP HANA データベースを保護します

SnapCenter Plug-in for SAP HANA Databases の略

SnapCenter Plug-in for SAP HANA Database の概要

SnapCenter Plug-in for SAP HANA Database は、 SAP HANA データベースに対応したデータ保護管理を提供する、 NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。Plug-in for SAP HANA Database は、 SnapCenter 環境での SAP HANA データベースのバックアップ、リストア、およびクローニングを自動化します。

SnapCenter は、単一コンテナおよびマルチテナントデータベースコンテナ（ MDC ）をサポートしています。Plug-in for SAP HANA Database は、 Windows と Linux のどちらの環境でも使用できます。HANA データベースホストにインストールされていないプラグインは、一元化されたホストプラグインと呼ばれます。一元化されたホストプラグインで、複数のホストにまたがる複数の HANA データベースを管理できます。

Plug-in for SAP HANA Database がインストールされている場合は、 SnapCenter で NetApp SnapMirror テクノロジを使用して、別のボリュームにバックアップセットのミラーコピーを作成できます。また、このプラグインと NetApp SnapVault テクノロジを併用して、標準への準拠を目的としたディスクツーディスクのバックアップレプリケーションを実行することもできます。

SnapCenter Plug-in for SAP HANA Database の機能

Plug-in for SAP HANA Database をインストールした環境では、 SnapCenter を使用して SAP HANA データベースとそのリソースをバックアップ、リストア、クローニングできます。これらの処理をサポートするタスクを実行することもできます。

- データベースを追加します。
- バックアップを作成します。
- バックアップからリストアします
- バックアップをクローニングする。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視する。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

SnapCenter Plug-in for SAP HANA Database の特長

SnapCenter は、プラグインアプリケーションと統合されるほか、ストレージシステム上でネットアップのテクノロジと統合されます。Plug-in for SAP HANA Database の操作には、 SnapCenter のグラフィカルユーザインターフェイスを使用します。

- * 統一されたグラフィカル・ユーザー・インターフェイス *

  SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter インターフェイスを使用すると、すべてのプラグインでバックアップ、リストア、クロ

ーニングの各処理を一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（ RBAC ）を設定したり、ジョブを監視したりすることができます。

- * 中央管理の自動化 *

  バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenter から E メールアラートを送信するように設定して、環境をプロアクティブに監視することもできます。

- * 無停止の NetApp Snapshot コピー・テクノロジー *

  SnapCenter では、 Plug-in for SAP HANA Database でネットアップの Snapshot コピーテクノロジを使用してリソースがバックアップされます。

Plug-in for SAP HANA Database を使用すると、次のメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます

  また、許可された SnapCenter ユーザにアプリケーションレベルの権限を付与するようにクレデンシャルを設定することもできます。

- NetApp FlexClone テクノロジを使用して、スペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

  クローンを作成するストレージシステムに FlexClone ライセンスが必要です。

- バックアップの作成で ONTAP の整合グループ（ CG ）の Snapshot コピー機能がサポートされます。
- 複数のリソースホストで同時に複数のバックアップを実行できます

  1 回の処理で、 1 つのホストの複数のリソースが同じボリュームを共有する場合に複数の Snapshot コピーが統合されます。

- 外部コマンドを使用して Snapshot コピーを作成できます。
- ファイルベースのバックアップがサポートされます。
- XFS ファイルシステムで Linux LVM がサポートされています。

SnapCenter Plug-in for SAP HANA Database でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシン（ VM ）の両方でさまざまなストレージタイプをサポートしています。SnapCenter Plug-in for SAP HANA Database をインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージタイプ
物理サーバと仮想サーバ	FC 接続 LUN

マシン	ストレージタイプ
物理サーバ	iSCSI で接続された LUN
物理サーバと仮想サーバ	NFS-connected ボリューム

SAP HANA プラグインに必要な最小限の ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
event generate-autosupport-log を指定します
ジョブ履歴の表示 ジョブが停止しました

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
LUN
lun create をクリックします
lun delete
LUN igroup add
lun igroup create を追加します
lun igroup delete
LUN igroup の名前を変更します
lun igroup show を参照してください
LUN マッピングの追加 - レポートノード
LUN マッピングが作成されます
LUN マッピングが削除されます
LUN マッピングの削除 - レポートノード
lun mapping show
lun modify を追加します
LUN のボリューム内移動
LUN はオフラインです
LUN はオンラインです
LUN の永続的予約はクリアします
LUN のサイズ変更
LUN シリアル
lun show をクリックします

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SnapMirror ポリシー追加ルール snapmirror policy modify-rule snapmirror policy remove-rule 」を実行します snapmirror policy show の略 SnapMirror リストア snapmirror show の略 snapmirror show -history の略 SnapMirror の更新 SnapMirror の update-ls-set snapmirror list-destinations
バージョン

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
volume clone create を実行します
volume clone show を実行します
ボリュームクローンスプリット開始
ボリュームクローンスプリットは停止します
volume create を実行します
ボリュームを削除します
volume file clone create を実行します
volume file show-disk-usage
ボリュームはオフラインです
ボリュームはオンラインです
volume modify を使用します
volume qtree create を実行します
volume qtree delete
volume qtree modify の略
volume qtree show の略
ボリュームの制限
volume show のコマンドです
volume snapshot create を実行します
ボリューム Snapshot の削除
volume snapshot modify の実行
ボリューム Snapshot の名前が変更されます
ボリューム Snapshot リストア
ボリューム Snapshot の restore-file
volume snapshot show の実行
ボリュームのアンマウント

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SVM CIFS です
vserver cifs share create の場合
SVM CIFS 共有が削除されます
vserver cifs shadowcopy show
vserver cifs share show のコマンドです
vserver cifs show のコマンドです
SVM エクスポートポリシー
vserver export-policy create を参照してください
vserver export-policy delete
vserver export-policy rule create
vserver export-policy rule show
vserver export-policy show のコマンドを入力します
Vserver iSCSI
vserver iscsi connection show
vserver show のコマンドです

読み取り専用コマンド： **ONTAP 8.3.0** 以降で必要な最小権限
Network Interface の略
network interface show の略
Vserver

SAP HANA データベースの **SnapMirror** および **SnapVault** レプリケーション用のストレージシステムを準備する

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenter は、Snapshotコピー処理の完了後に、SnapMirrorとSnapVault に対する更新を実行します。SnapMirror更新とSnapVault 更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SnapCenter は * sync-mirror * レプリケーションをサポートしていません。

SAP HANA データベースのバックアップ戦略

SAP HANA データベースのバックアップ戦略を定義する

バックアップジョブを作成する前にバックアップ戦略を定義しておくと、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービスレベルアグリーメント（ SLA ）、目標復旧時間（ RTO ）、および目標復旧時点（ RPO ）によって決まります。

- このタスクについて *

SLA では、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処するために必要なサービスレベルを定義します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA 、 RTO 、および RPO は、データ保護戦略に関与します。

- 手順 *

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. Snapshot コピーベースのポリシーを作成してアプリケーションと整合性のあるデータベースの Snapshot コピーをバックアップするかどうかを決定します。
5. データベースの整合性を検証するかどうかを決定します。
6. レプリケーションのために NetApp SnapMirror テクノロジを使用するか、または長期保持のために NetApp SnapVault テクノロジを使用するかを決定します。

7. ソースストレージシステムおよび SnapMirror デスティネーションでの Snapshot コピーの保持期間を確認します。
8. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

Linux ホスト上のリソースの自動検出

リソースとは、 SnapCenter で管理されている Linux ホスト上の SAP HANA データベースと非データボリュームです。SnapCenter Plug-in for SAP HANA Database プラグインをインストールすると、その Linux ホスト上の SAP HANA データベースが自動的に検出されてリソースページに表示されます。

自動検出は、次の SAP HANA リソースでサポートされています。

- 単一のコンテナ

  プラグインをインストールまたはアップグレードしたあと、中央ホストプラグインにある単一コンテナリソースは、手動で追加したリソースとして引き続き使用されます。

  プラグインをインストールまたはアップグレードすると、 SnapCenter に直接登録されている SAP HANA Linux ホストでのみ、 SAP HANA データベースが自動的に検出されます。

- マルチテナントデータベースコンテナ（ MDC ）

  プラグインをインストールまたはアップグレードした後、中央ホストプラグインにある MDC リソースは、手動で追加したリソースとして続行されます。

  SnapCenter 4.3 へのアップグレード後も、中央ホストプラグインに MDC リソースを手動で追加する必要があります。

  SnapCenter に直接登録された SAP HANA Linux ホストの場合、プラグインをインストールまたはアップグレードすると、ホスト上のリソースが自動で検出されます。プラグインをアップグレードした後、プラグインホスト上にあるすべての MDC リソースに対して、別の MDC リソースが自動的に別の GUID 形式で検出され、 SnapCenter に登録されます。新しいリソースはロック状態になります。

  たとえば、 SnapCenter 4.2 では、 E90 MDC リソースがプラグインホスト上にあり、手動で登録されている場合、 SnapCenter 4.3 にアップグレードした後に、別の GUID を持つ別の E90 MDC リソースが検出されて SnapCenter に登録されます。

自動検出は、次の構成ではサポートされません。

- RDM と VMDK のレイアウト

  上記のリソースが検出された場合、これらのリソースではデータ保護処理はサポートされていません。

- HANA マルチホスト構成
- 同じホスト上の複数のインスタンス
- マルチティアスケールアウト HANA システムレプリケーション

- システムレプリケーションモードでのカスケードレプリケーション環境

サポートされるバックアップのタイプ

バックアップタイプでは、作成するバックアップのタイプを指定します。SnapCenter では、 SAP HANA データベースについて、ファイルベースのバックアップと Snapshot コピーベースのバックアップをサポートしています。

File-Based バックアップ

ファイルベースのバックアップでは、データベースの整合性が検証されます。ファイルベースのバックアップの処理は一定の間隔で実行するようにスケジュールを設定できます。アクティブなテナントのみがバックアップされます。ファイルベースのバックアップは SnapCenter からリストアおよびクローニングできません。

Snapshot コピーベースのバックアップ

Snapshot コピーベースのバックアップでは、 NetApp Snapshot コピーテクノロジを利用して、 SAP HANA データベースが格納されたボリュームのオンラインの読み取り専用コピーが作成されます。

SnapCenter Plug-in for SAP HANA Database での整合グループ Snapshot コピーの使用方法

プラグインを使用して、リソースグループの整合グループ Snapshot コピーを作成することができます。整合グループとはボリュームのコンテナであり、複数のボリュームを格納して 1 つのエンティティとして管理できます。整合グループには複数のボリュームの Snapshot コピーが同時に格納されるため、一連のボリュームのコピーの整合性が確保されます。

ストレージコントローラが整合性を確保しながら Snapshot コピーをグループ化するのを待機する時間も指定できます。使用可能な待機時間のオプションは、 * Urgent * 、 * Medium * 、 * Relaxed * です。また、整合グループ Snapshot コピーの処理で Write Anywhere File Layout （ WAFL ）の同期を有効または無効にすることもできます。WAFL 同期を使用すると、整合グループの Snapshot コピーのパフォーマンスが向上します。

SnapCenter による不要なログおよびデータバックアップの削除の管理

SnapCenter は、ストレージシステムレベルおよびファイルシステムレベルでの不要なログおよびデータバックアップの削除を、 SAP HANA のバックアップカタログ内で管理します。

保持設定に基づいて、プライマリストレージまたはセカンダリストレージの Snapshot コピーと SAP HANA のカタログ内の対応するエントリが削除されます。SAP HANA のカタログのエントリは、バックアップやリソースグループを削除したときにも削除されます。

SAP HANA データベースのバックアップスケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度（バックアップを実行する間隔）

  バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュールタイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップスケジュール（バックアップが実行される日時

  バックアップスケジュールは、リソースまたはリソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます

SAP HANA データベースに必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービスレベルアグリーメント（ SLA ）などがあります。

Plug-in for SAP HANA Database のバックアップ命名規則

Snapshot コピーのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- _dts1_は リソースグループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、「 * Snapshot コピーにカスタム名形式を使用」を選択して、リソースまたはリソースグループを保護しながら Snapshot コピー名の形式を指定することもできます。たとえば、customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名にタイムスタンプのサフィックスが追加されます。

SAP HANA データベースのリストアとリカバリの戦略

SAP HANA リソースのリストアとリカバリの戦略を定義する

データベースのリストアとリカバリを行う前に戦略を定義しておくと、リストア処理とリカバリ処理を正常に実行できるようになります。

- 手順 *
  1. 手動で追加した SAP HANA リソースでサポートされるリストア戦略を決定します
  2. 自動検出された SAP HANA データベースに対するリストア戦略を決定します
  3. 実行するリカバリ処理のタイプを決定します。

手動で追加した SAP HANA リソースでサポートされるリストア戦略のタイプ

SnapCenter を使用してリストア処理を正常に実行するには、事前に戦略を定義しておく必要があります。SAP HANA リソースを手動で追加する場合のリストア戦略には、 2 つのタイプがあります。手動で追加した SAP HANA リソースはリカバリできません。

手動で追加した SAP HANA リソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、 qtree 、および LUN をリストアします

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

ファイルレベルのリストア

- ボリューム、 qtree 、またはディレクトリからファイルをリストアします
- 選択した LUN のみをリストアします

自動検出された SAP HANA データベースでサポートされるリストア戦略のタイプ

SnapCenter を使用してリストア処理を正常に実行するには、事前に戦略を定義しておく必要があります。自動検出された SAP HANA データベースには、 2 種類のリストア戦略があります。

リソース全体のリストア

- リソースのすべてのボリューム、 qtree 、および LUN をリストアします
  - ボリューム全体をリストアするには、 * Volume Revert * オプションを選択する必要があります。

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

テナントデータベース

- テナントデータベースをリストアします

「 * テナントデータベース * 」オプションが選択されている場合は、 SnapCenter 外部の HANA Studio または HANA リカバリスクリプトを使用してリカバリ処理を実行する必要があります。

自動検出された **SAP HANA** データベースのリストア処理のタイプ

SnapCenter では、自動検出された SAP HANA データベースについて、 Volume-Based SnapRestore （ VBSR ）、 Single File SnapRestore 、 Connect and Copy のリストアタイプがサポートされています。

NFS 環境で **Volume-Based SnapRestore** （ **VBSR** ）を使用すると、次のようなシナリオが発生します。

- リストア用に選択されたバックアップが SnapCenter 4.3 より前のリリースで実行され ' **Complete Resource** オプションが選択されている場合のみ
- リストア用に選択されたバックアップが SnapCenter 4.3 で選択されていて、 * Volume Revert * オプションが選択されている場合

NFS 環境で単一ファイル **SnapRestore** を実行するシナリオを次に示します。

- リストア用に選択したバックアップが SnapCenter 4.3 で実行されていて、 [リソースを完全にバックアップ] オプションのみが選択されている場合
- マルチテナントデータベースコンテナ（ MDC ）の場合は、リストア対象に選択されたバックアップが SnapCenter 4.3 で作成され、「 * テナントデータベース * 」オプションが選択されているとみなされます
- バックアップを SnapMirror または SnapVault セカンダリの場所から選択し、 * Complete Resource * オプションが選択されている場合

単一ファイル **SnapRestore** は、次のような状況で **SAN** 環境で実行されます。

- SnapCenter 4.3 より前のリリースでバックアップを作成する場合、 [リソースの完了] オプションが選択されている場合のみ
- SnapCenter 4.3 でバックアップを実行する場合、 * Complete Resource * オプションが選択されている場合のみ
- SnapMirror または SnapVault セカンダリストレージからバックアップを選択し、 * Complete Resource * オプションを選択した場合

Connect and Copy ベースのリストアは、 **SAN** 環境で次のシナリオに基づいて実行されます。

- MDC の場合は、リストア用に選択されたバックアップが SnapCenter 4.3 で作成され、 * テナントデータベース * オプションが選択されている場合

* リソース全体 * 、 * ボリューム復帰 * 、 * テナントデータベース * の各オプションは、 [リストア範囲] ページから選択できます。

SAP HANA データベースでサポートされるリカバリ処理のタイプ

SnapCenter を使用すると、 SAP HANA データベースに対してさまざまなタイプのリカバリ処理を実行できます。

- データベースを最新の状態にリカバリします
- 特定の時点までデータベースをリカバリします

  リカバリの日時を指定する必要があります。

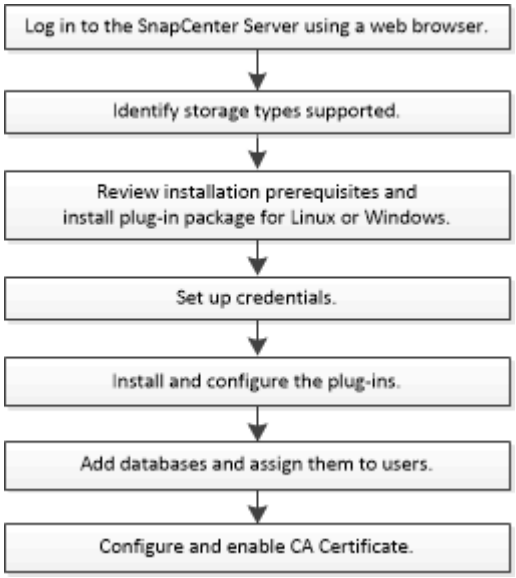
- 特定のデータバックアップまでデータベースをリカバリします

SnapCenter には、 SAP HANA データベースをリカバリするオプションもありません。

SnapCenter Plug-in for SAP HANA Database をインストールする準備をします

SnapCenter Plug-in for SAP HANA Database のインストールワークフロー

SAP HANA データベースを保護する場合は、 SnapCenter Plug-in for SAP HANA Database をインストールしてセットアップする必要があります。



ホストを追加して SnapCenter Plug-in for SAP HANA Database をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。SnapCenter Plug-in for SAP HANA Database は、 Windows と Linux のどちらの環境でも使用できます。

- ホストに Java 1.8 64 ビットがインストールされている必要があります。

  IBM Javaはサポートされていません。

- SAP HANA データベースの対話型端末（ HDBSQL クライアント）をホストにインストールしておく必要があります。
- Windows の場合は、「 LocalSystem 」 Windows ユーザを使用してプラグインの Creator Service が実行されている必要があります。これは、 Plug-in for SAP HANA Database がドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windows の場合は、ユーザストアキーを SYSTEM ユーザとして作成する必要があります。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。SnapCenter Plug-in for Microsoft Windows は、 Windows ホストに SAP HANA プラグインを使用してデフォルトで導入されます。
- Linux ホストの場合は、 HDB Secure User Store キーに HDBSQL OS ユーザとしてアクセスします。
- SnapCenter サーバが、 Plug-in for SAP HANA Database ホストの 8145 ポートまたはカスタムポートにアクセスできる必要があります。

Windows ホスト

- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。
- Plug-in for SAP HANA Database を Windows ホストにインストールする際に、 SnapCenter Plug-in for Microsoft Windows が自動的にインストールされます。
- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Windows ホストに Java 1.8 64 ビットがインストールされている必要があります。

  "すべてのオペレーティングシステム用の Java のダウンロード"

  "NetApp Interoperability Matrix Tool で確認できます"

Linux ホスト

- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Linux ホストに Java 1.8 64 ビットがインストールされている必要があります。

  "すべてのオペレーティングシステム用の Java のダウンロード"

  "NetApp Interoperability Matrix Tool で確認できます"

- Linux ホストで実行されている SAP HANA データベースを Plug-in for SAP HANA Database のインストール時にインストールすると、 SnapCenter Plug-in for UNIX が自動的にインストールされます。

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

SnapCenter Plug-ins Package for Linux をインストールするためのホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストシステムの基本的なスペースとサイジング要件を理解しておく必要があります。

項目	要件
オペレーティングシステム	• Red Hat Enterprise Linux の場合 • SUSE Linux Enterprise Server （ SLES ） サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	2 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	Java 1.8.x （ 64 ビット）の Oracle Java と OpenJDK のバージョン Java を最新バージョンにアップグレードした場合は、 /var/opt/snapcenter /etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

SnapCenter Plug-in for SAP HANA Database のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますSnapCenter プラグインのインストールに必要なクレデンシャル、およびデータベースや Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- このタスクについて *
- Linux ホスト

  Linux ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。

  プラグインプロセスをインストールして開始するための sudo 権限がある root ユーザまたは root 以外のユ

ーザのクレデンシャルを設定する必要があります。

* ベストプラクティス： * ホストを導入してプラグインをインストールしたあとに Linux のクレデンシャルを作成することは可能ですが、 SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

- Windows ホスト

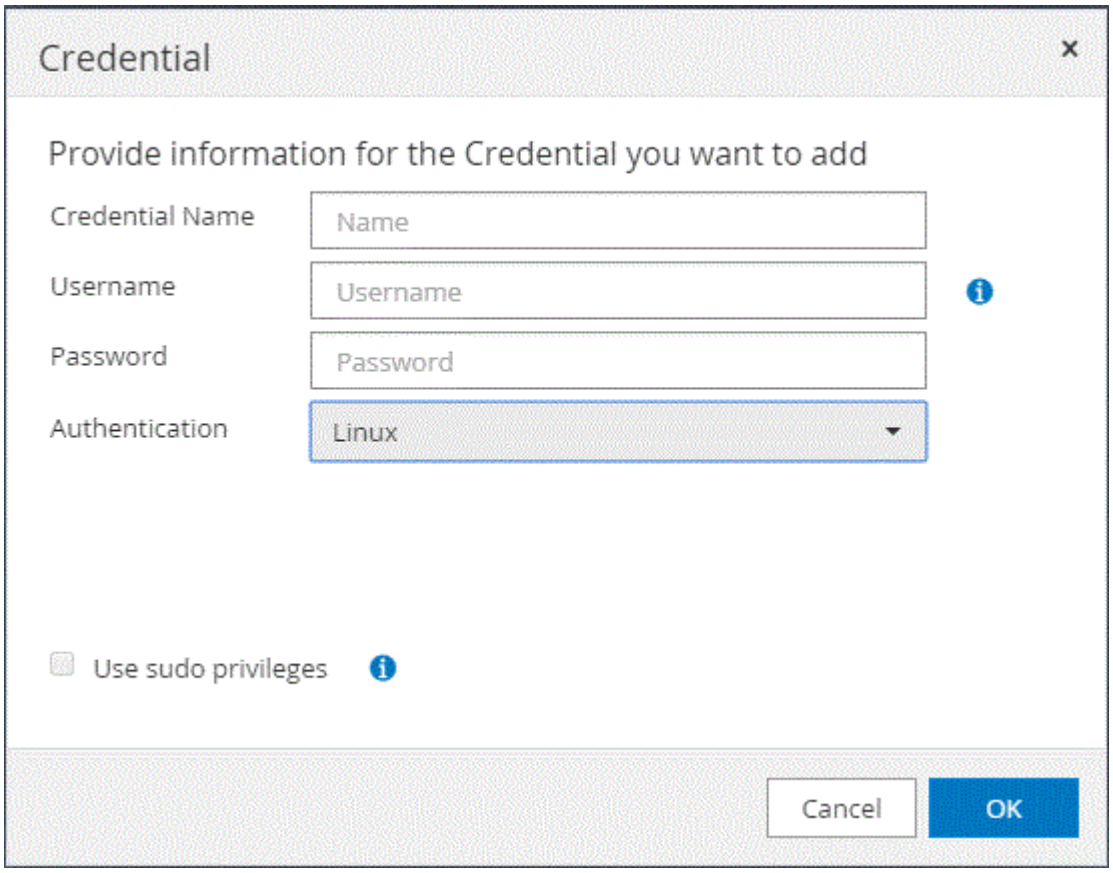
  プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。

  リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定する必要があります。

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* 資格情報] をクリックします。
3. [新規作成（ New ）] をクリックする。



4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。 ◦ NETBIOS_USERNAME_ ◦ _ ドメイン FQDN\ ユーザ名 _ • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Username フィールドの有効な形式は、*username* です パスワードに二重引用符（"）またはバックティック（`）を使用しないでください。小なり（<）と感嘆符（！）は使用しないでください。 パスワードに記号を追加します。たとえば、lessthan <！10、lessthan10 <！、backtick 12とします。
パスワード	認証に使用するパスワードを入力します。
認証モード	使用する認証モードを選択します。
sudo 権限を使用する	root 以外のユーザのクレデンシャルを作成する場合は、「 * sudo 権限を使用する * 」チェックボックスをオンにします。 Linux ユーザのみに該当します。

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、 [ユーザとアクセス（ User and Access ）] ページで、ユーザまたはユーザグループにクレデンシャルのメンテナンスを割り当てることができます。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
   a. 次の形式でユーザグループアカウントを作成します。

```
 domainName\accountName$
. . グループにコンピュータオブジェクトを追加します。
. . 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
. . を実行します `Get-ADServiceAccount`
サービスアカウントを確認するコマンド。
```

4. ホストで gMSA を設定します。
   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. ホストを再起動します。

b. PowerShellコマンドプロンプトから次のコマンドを実行して、ホストにgMSAをインストールします。 `Install-AdServiceAccount <gMSA>`

c. 次のコマンドを実行して'gMSAアカウントを確認します `Test-AdServiceAccount <gMSA>`

1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

   SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

SnapCenter Plug-in for SAP HANA Databases をインストールします

ホストを追加し、プラグインパッケージをリモートホストにインストールする

ホストの追加ページを使用 SnapCenter してホストを追加し、プラグインパッケージをインストールする必要があります。プラグインは、自動的にリモートホストにインストールされます。ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。

- 必要なもの *
- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- メッセージキューサービスが実行されていることを確認してください。

- 管理マニュアルには、ホストの管理に関する情報が記載されています。
- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

  "Windows Server 2012 以降で SAP HANA 用のグループマネージドサービスアカウントを設定します"

- このタスクについて *
- SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。
- SAP HANAシステムレプリケーションでプライマリシステムとセカンダリシステムの両方のリソースを検出するには、rootユーザまたはsudoユーザを使用してプライマリシステムとセカンダリシステムの両方を追加することを推奨します。
- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	ホストのタイプを選択します。 • Windows の場合 • Linux の場合 Plug-in for SAP HANA は、 HDBSQL クライアントホストにインストールされます。このホストは、 Windows システムでも Linux システムでもかまいません。
ホスト名	通信ホスト名を入力します。ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。 HDBSQL クライアントと HDBUserStore をこのホスト上に設定する必要があります。

フィールド	手順
クレデンシャル	作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。
6. （オプション） * その他のオプション * をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	Plug-in for SAP HANA は、 HDBSQL クライアントホストにインストールされます。このホストは、 Windows システムでも Linux システムでもかまいません。 • Windows 用 SnapCenter Plug-ins パッケージのデフォルトパスは C ： \Program Files\NetApp\SnapManager です。必要に応じて、パスをカスタマイズできます。 • Linux 用 SnapCenter Plug-ins パッケージのデフォルトパスは /opt/NetApp/SnapCenter です。必要に応じて、パスをカスタマイズできます。

フィールド	手順
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	Windows ホストの場合、プラグインサービスの実行にグループ管理サービスアカウント（ gMSA ）を使用する場合は、このチェックボックスをオンにします。 gMSA 名を domainName\accountName$ の形式で指定します。 gMSA は、 SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されます。

7. [Submit （送信）] をクリックします。

   [事前確認をスキップする] チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。ディスクスペース、 RAM 、 PowerShell のバージョン、 .NET のバージョン、場所（ Windows プラグインの場合）、および Java のバージョン（ Linux プラグインの場合）が、最小要件に照らして検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

   エラーがディスクスペースまたは RAM に関連している場合は、 C ： \Program Files\NetApp\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

   HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. ホストタイプが Linux の場合は、フィンガープリントを確認し、 * Confirm and Submit * をクリックします。

   クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。

   同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

1. インストールの進行状況を監視します。

   インストール固有のログファイルは、 /custom_location/snapcenter /logs にあります。

コマンドレットを使用して、複数のリモートホストに **Linux** または **Windows** 用の **SnapCenter** プラグインパッケージをインストールします

Install-SmHostPackage PowerShell コマンドレットを使用すると、複数のホストに Linux または Windows 向け SnapCenter プラグインパッケージを同時にインストールできます。

- 必要なもの *

プラグインパッケージをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 Open-SmConnection コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

プラグインを手動でインストールし、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、 -skipprecheck オプションを使用できます。

1. リモートインストールのクレデンシャルを入力します。

コマンドラインインターフェイスを使用して、 **Linux** ホストに **SnapCenter Plug-in for SAP HANA Database** をインストールします

SnapCenter ユーザインターフェイス（ UI ）を使用して、 SnapCenter Plug-in for SAP HANA Database をインストールする必要があります。環境で SnapCenter UI からプラグインのリモートインストールが許可されていない場合は、コマンドラインインターフェイス（ CLI ）を使用して、 Plug-in for SAP HANA Database をコンソールモードまたはサイレントモードでインストールできます。

- 必要なもの *
- HDBSQL クライアントが配置された各 Linux ホストに Plug-in for SAP HANA Database をインストールする必要があります。
- SnapCenter Plug-in for SAP HANA Database をインストールする Linux ホストは、依存するソフトウェア、データベース、オペレーティングシステムの要件を満たしている必要があります。

  サポートされる構成の最新情報については、 Interoperability Matrix Tool （ IMT ）を参照してください。

  "NetApp Interoperability Matrix Tool で確認できます"
- SnapCenter Plug-in for SAP HANA Database は、 SnapCenter Plug-ins Package for Linux の一部で

す。SnapCenter Plug-ins Package for Linux をインストールする前に、 Windows ホストに SnapCenter がインストールされている必要があります。

- 手順 *

1. Linux インストールファイル（ snapcenter _ linux_host_plugin.bin ）の SnapCenter Plug-ins パッケージを C ： \ProgramData\NetApp\SnapCenter \Package リポジトリから、 Plug-in for SAP HANA Database をインストールするホストにコピーします。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

2. コマンドプロンプトで、インストールファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。
   `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
   - -dport には、 SMCore HTTPS 通信ポートを指定します。
   - - DSERVER_IP は、 SnapCenter サーバの IP アドレスを指定します。
   - - DSERVER_HTTPS_PORT には、 SnapCenter サーバの HTTPS ポートを指定します。
   - -duser_install_DIR - SnapCenter Plug-ins Package for Linux をインストールするディレクトリを指定します
   - DINSTALL_LOG_name は、ログファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

1. 次のコマンドを入力して、 =<installation directory>/NetApp/snapcenter /cscc /etc/SC_SMS_Services.properties ファイルを編集し、 plugins/enabled=hana ： 3.0 パラメータを追加します。
2. Add-Smhost コマンドレットと必要なパラメータを使用して、ホストを SnapCenter サーバに追加します。

   コマンドで使用できるパラメータとその説明については、 RUNNING Get Help command_name _ を使用して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

Plug-in for SAP HANA のインストールのステータスを監視します

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
   a. [* フィルタ * （ Filter * ）] をクリック
   b. オプション：開始日と終了日を指定します。
   c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
   d. Status ドロップダウンメニューから、インストールステータスを選択します。
   e. [適用（ Apply ）] をクリックします。
4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *

1. GUI で次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。

c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。

d. ボックスから 16 進文字をコピーします。

e. 16 進数の間のスペースを削除します。

たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

2. PowerShell で次の手順を実行します。

a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

Get-ChildItem - パス証明書： *\localmachine\My*

b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して **CA** 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

例：

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. 次のコマンドを実行して、新しくインストールした証明書を Windows
ホストプラグインサービスにバインドします。
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
certhash=$cert appid="$guid"
```

例：

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux ホストで **SnapCenter SAP HANA Plug-ins** サービスの **CA** 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードを管理し、CA証明書を設定し、カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定し、インストールされたデジタル証明書をアクティブ化するために、SnapCenterカスタムプラグインサービスを使用してカスタムプラグインの信頼ストアにCA署名キーペアを設定する必要があります。

カスタムプラグインでは、ファイル「 keystore.JKS 」を使用します。このファイルは、信頼ストアおよびキーストアとして _/opt/NetApp/snapcenter / scc /etc/both にあります。

カスタムプラグインのキーストアのパスワード、および使用中の **CA** 署名済みキーペアのエイリアスを管理します

- 手順 *

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   キー「 keystore.pass 」に対応する値です。

2. キーストアのパスワードを変更します。

   ```
   keytool -storepasswd -keystore keystore.jks
   ```

   .
   キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

3. パスワードを変更したら、サービスを再起動してください。

> カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *

1. カスタムプラグインキーストアが格納されているフォルダ（/opt/NetApp/snapcenter/scc/etc）に移動します。
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書または中間証明書を追加します。

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

.
カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

- 手順 *

1. カスタムプラグインキーストア /opt/NetApp/snapcenter / scc などが含まれているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

```
keytool -importkeystore -srckeystore
/root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore
keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

   デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
```

. CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「 *
」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
 keytool -changealias -alias "long_alias_name" -destalias
"simple_alias" -keystore keystore.jks
```

. agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値をキー SCC_CERTIFICATE_ALIAS に更新します。

8. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ CRL ）を設定します

- このタスクについて *
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、「 /opt/netapp/snapcenter /sscc /etc/crl 」です。
- 手順 *

1. agent.properties ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。

   このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

Windows ホストで SnapCenter SAP HANA Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードを管理し、CA証明書を設定し、カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定し、インストールされたデジタル証明書をアクティブ化するために、SnapCenterカスタムプラグインサービスを使用してカスタムプラグインの信頼ストアにCA署名キーペアを設定する必要があります。

カスタムプラグインは、 _ C ： \Program Files\NetApp\SnapManager \Snapcenter Plug-in Creator\etc_both にある file_keystore.JKS_を 信頼ストアおよびキーストアとして使用します。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

- 手順 *

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   key_keystore.pass_ に対応する値です。

2. キーストアのパスワードを変更します。

   keytool -storepasswd -keystore keystore.JKS

   > Windows のコマンドプロンプトで「 keytool 」コマンドが認識されない場合は、keytool コマンドを完全なパスに置き換えます。

   C ： \Program Files\Java\<JDK_version >\bin\keytool .exe "-storepasswd -keystore keystore.JKS

3. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.JKS

agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

1. パスワードを変更したら、サービスを再起動してください。

   > カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *

1. カスタムプラグインkeystore_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_が格納されているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. ルート証明書または中間証明書を追加します。

   keytool -import-trustcacerts -alias myRootCA -file/root/USERTrustRSA_Root.cer -keystore keystore.JKS

5. カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

> ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

- 手順 *

1. カスタムプラグインの keystore _C ： \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. file_keystore.JKS_</Z1> を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

   keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.JKS -deststoretype JKS

5. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

   デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

*keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

1. *agent.properties* ファイルの CA 証明書からエイリアス名を設定します。

   この値をキー SCC_CERTIFICATE_ALIAS に更新します。

2. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ **CRL** ）を設定します

- このタスクについて *
- 関連する CA 証明書の最新の CRL ファイルをダウンロードするには、を参照してください "SnapCenter CA 証明書の証明書失効リストファイルを更新する方法"。
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、 *'C:\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\crl'* です。
- 手順 *

1. *agent.properties* ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。
2. このディレクトリに複数の CRL ファイルを配置できます。

   着信証明書は各 CRL に対して検証されます。

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphere をインストール

データベースが仮想マシン（ VM ）に格納されている場合や VM とデータストアを保護する場合は、 SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください "導入の概要"。

CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください "SSL 証明書を作成またはインポートします"。

CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere は、事前に設定されたディレクトリ内の CRL ファイルを検索します。VMware vSphere 用 SnapCenter プラグインの CRL ファイルのデフォルトディレクトリは、_/opt/NetApp/config/crl_です 。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

データ保護を準備

SnapCenter Plug-in for SAP HANA Database を使用するための前提条件

SnapCenter Plug-in for SAP HANA Database を使用するには、 SnapCenter 管理者が事前に SnapCenter サーバをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。
- SnapCenter サーバにログインします。
- 必要に応じて、ストレージシステム接続を追加し、クレデンシャルを作成して、 SnapCenter 環境を設定します。
- Java 1.7 または Java 1.8 を Linux ホストまたは Windows ホストにインストールします。

  ホストマシンの環境パス変数に Java パスを設定する必要があります。

- バックアップレプリケーションが必要である場合は、 SnapMirror と SnapVault をセットアップします。
- Plug-in for SAP HANA Database をインストールするホストに HDBSQL クライアントをインストールします。

  このホストで管理する SAP HANA ノードのユーザストアキーを設定します。

- SAP HANA データベース 2.0SPS05 で SAP HANA データベースのユーザアカウントを使用している場合は、 SnapCenter サーバでバックアップ、リストア、およびクローニングの処理を実行するための次の権限があることを確認します。
  - バックアップ管理者
  - カタログの読み取り
  - データベースバックアップ管理者
  - データベースリカバリオペレータ

SAP HANA データベースの保護におけるリソース、リソースグループ、ポリシーの使用方法

SnapCenter を使用する前に、実行するバックアップ、クローニング、およびリストアの処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- リソースとは、通常は SnapCenter でバックアップまたはクローニングする SAP HANA データベースの

ことです。

- SnapCenter リソースグループは、ホスト上のリソースの集まりです。

  リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているリソースに対して処理が実行されます。

  単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。スケジュールされたバックアップを単一のリソースおよびリソースグループに対して実行することもできます。

- ポリシーは、バックアップ頻度、レプリケーション、スクリプト、およびデータ保護処理のその他の特性を指定するものです。

  リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。単一のリソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

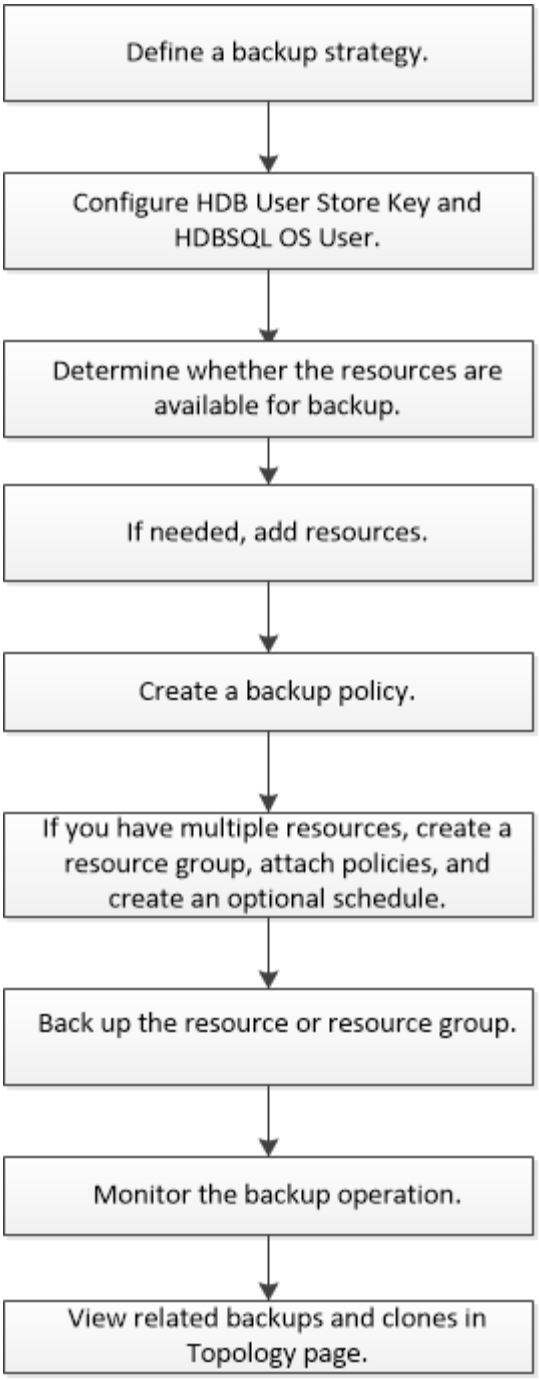
リソースグループは、保護対象となるものを定義するものであり、日と時間の観点から保護する必要がある場合に考えてみてください。ポリシーは、保護方法を定義するものと考えてください。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。リソースグループを作成してポリシーを適用する際に、フルバックアップを毎日実行するようにリソースグループを設定できます。

SAP HANA のリソースをバックアップ

SAP HANA のリソースをバックアップ

リソース（データベース）またはリソースグループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするデータベースの特定、バックアップポリシーの管理、リソースグループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、 SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。
"SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します

SAP HANA データベースでデータ保護処理を実行するには、 HDB User Store Key および HDBSQL OS ユーザを設定する必要があります。

- 必要なもの *

- SAP HANA データベースで HDB Secure User Store Key および HDB SQL OS User が設定されていない場合は、自動検出されたリソースにのみ赤い南京錠のアイコンが表示されます。その後の検出操作中に、設定されている HDB Secure User Store Key が正しくないか、データベース自体へのアクセスを提供していない場合は、赤い南京錠のアイコンが再表示されます。
- データ保護処理を実行するには、 HDB Secure User Store Key および HDB SQL OS ユーザーがデータベースを保護できるように設定するか、またはデータベースをリソースグループに追加する必要があります。
- システムデータベースにアクセスするには、 HDB SQL OS ユーザーを構成する必要があります。HDB SQL OS ユーザがテナントデータベースのみにアクセスするように設定されていると、検出処理が失敗します。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから SnapCenter Plug-in for SAP HANA Database を選択します。
2. [リソース] ページで、 [* 表示 *] リストからリソースタイプを選択します。
3. （オプション）をクリックします をクリックし、ホスト名を選択します。

   をクリックします をクリックしてフィルタペインを閉じます。
4. データベースを選択し、 * データベースの設定 * をクリックします。
5. [データベース設定の構成] セクションで、 HDB Secure User Store Key と入力します。

   プラグインのホスト名が表示され、 HDB SQL OS ユーザーが <sid>adm に自動的に入力されます。
6. [OK] をクリックします。

Topology ページからデータベースの設定を変更できます。

リソースを検出し、マルチテナントデータベースコンテナでデータ保護を準備

データベースを自動的に検出します

リソースとは、 SnapCenter で管理されている Linux ホスト上の SAP HANA データベースと非データボリュームです。使用可能な SAP HANA データベースを検出したあと、それらのリソースをリソースグループに追加してデータ保護処理を実行できます。

- 必要なもの *
- SnapCenter サーバのインストール、 HDB ユーザ・ストア・キーの追加、ホストの追加、ストレージ・システム接続の設定などの作業を完了しておく必要があります。
- Linux ホストで HDB Secure User Store Key および HDB SQL OS ユーザを設定しておく必要があります。
  - SID adm ユーザーを使用して HDB ユーザーストアキーを構成する必要がありますたとえば、 A22 を SID として使用する HANA システムの場合、 HDB User Store Key は a22adm で構成する必要があります。
- SnapCenter Plug-in for SAP HANA Database では、 RDM / VMDK 仮想環境にあるリソースの自動検出はサポートされません。データベースを手動で追加する場合は、仮想環境のストレージ情報を指定する必要

があります。

- このタスクについて *

プラグインをインストールすると、その Linux ホスト上のすべてのリソースが自動的に検出され、リソースページに表示されます。

自動で検出されたリソースは変更または削除できません。

- 手順 *

1. 左側のナビゲーションペインで、 * Resources * をクリックし、リストから Plug-in for SAP HANA Database を選択します。
2. [リソース] ページで、 [表示] リストからリソースタイプを選択します。
3. （オプション） * をクリックします* をクリックし、ホスト名を選択します。

   次に、 * をクリックします* をクリックすると、フィルタペインが閉じます。

4. [* リソースの更新 *] をクリックして、ホストで使用可能なリソースを検出します。

   リソースは、リソースタイプ、ホスト名、関連するリソースグループ、バックアップタイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

   - データベースがネットアップストレージ上にあり、保護されていない場合は、総体的なステータス列に Not protected と表示されます。
   - データベースがネットアップストレージシステム上にあり、保護されている場合に、バックアップ処理が実行されていないと、 [全体のステータス] 列に [バックアップが実行されていません] と表示されます。それ以外の場合は、前回のバックアップステータスに基づいて、「 Backup failed 」または「 Backup succeeded 」に変わります。

SAP HANA データベースで HDB Secure User Store Key が設定されていない場合は、リソースの横に赤い南京錠のアイコンが表示されます。その後の検出操作中に、設定されている HDB Secure User Store Key が正しくないか、データベース自体へのアクセスを提供していない場合は、赤い南京錠のアイコンが再表示されます。

データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

- 終了後 *

データ保護処理を実行するには、データベースを保護できるように HDB Secure User Store Key および HDBSQL OS ユーザを設定するか、またはリソースグループにこのキーを追加する必要があります。

"SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します"

マルチテナントデータベースコンテナでデータ保護を準備

SnapCenter に直接登録された SAP HANA ホストの場合、 SnapCenter Plug-in for SAP HANA Database をインストールまたはアップグレードすると、ホスト上のリソースが自動的に検出されます。プラグインをインストールまたはアップグレードした後、プラグインホスト上にあるすべてのマルチテナントデータベースコンテナ（ MDC ）リソース

に対して、別の MDC リソースが自動的に検出されて SnapCenter に登録されます。新しいリソースは「ロック」状態になります。

- このタスクについて *

たとえば、 SnapCenter 4.2 では、 E90 MDC リソースがプラグインホスト上にあり、手動で登録されている場合、 SnapCenter 4.3 にアップグレードした後に、別の GUID を持つ別の E90 MDC リソースが検出されて SnapCenter に登録されます。

SnapCenter 4.2 以前のバージョンのリソースに関連付けられたバックアップは、保持期間が満了するまで保持される必要があります。保存期間が終了したら、古い MDC リソースを削除して、新しい自動検出された MDC リソースを引き続き管理できます。

`Old MDC resource` は、SnapCenter 4.2以前のリリースで手動で追加されたプラグインホストのMDCリソースです。

SnapCenter 4.3 で検出された新しいリソースを使用してデータ保護処理を開始するには、次の手順を実行します。

- 手順 *

1. リソースページで ' 以前の SnapCenter リリースにバックアップが追加されている古い MDC リソースを選択し ' トポロジーページからメンテナンス・モードにします

   リソースがリソースグループの一部である場合は、リソースグループを「メンテナンスモード」にします。

2. リソースページから新しいリソースを選択して、 SnapCenter 4.3 にアップグレードした後に検出された新しい MDC リソースを構成します。

   「新しい MDC リソース」は、 SnapCenter サーバとプラグインホストが 4.3 にアップグレードされたときに検出された、新しく検出された MDC リソースです。新しい MDC リソースは、古い MDC リソースと同じ SID を持つリソース、特定のホスト、およびリソースページのその横に赤い南京錠のアイコンで識別できます。

3. SnapCenter 4.3 へのアップグレード後に検出された新しい MDC リソースを保護するには ' 保護ポリシー ' スケジュール ' 通知設定を選択します
4. 保持設定に基づいて、 SnapCenter 4.2 以前のリリースで作成されたバックアップを削除します。
5. Topology ページからリソースグループを削除します。
6. [リソース] ページから古い MDC リソースを削除します。

   たとえば、プライマリ Snapshot コピーの保持期間が 7 日で、セカンダリ Snapshot コピーの保持期間が 45 日の場合、 45 日が完了してすべてのバックアップが削除されたあとに、リソースグループと古い MDC リソースを削除する必要があります。

- 詳細はこちら *

"SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します"

"Topology ページで、 SAP HANA データベースのバックアップとクローンを表示します"

プラグインホストにリソースを手動で追加します

自動検出は、特定の HANA インスタンスではサポートされていません。これらのリソースは手動で追加する必要があります。

- 必要なもの *
- SnapCenter サーバのインストール、ホストの追加、ストレージシステム接続のセットアップ、 HDB ユーザストアキーの追加などのタスクを完了しておく必要があります。
- SAP HANA システムのレプリケーションでは、その HANA システムのすべてのリソースを 1 つのリソースグループに追加して、リソースグループのバックアップを作成することを推奨します。これにより、テイクオーバー / フェイルバックモードでのシームレスなバックアップが可能になります。

"リソースグループを作成してポリシーを適用"。

- このタスクについて *

自動検出は、次の構成ではサポートされません。

- RDM と VMDK のレイアウト

> 上記のリソースが検出された場合、これらのリソースではデータ保護処理はサポートされていません。

- HANA マルチホスト構成
- 同じホスト上の複数のインスタンス
- マルチティアスケールアウト HANA システムレプリケーション
- システムレプリケーションモードでのカスケードレプリケーション環境
- 手順 *

1. 左側のナビゲーションペインで、ドロップダウンリストから SnapCenter Plug-in for SAP HANA Database を選択し、 * Resources * をクリックします。
2. リソースページで、 * SAP HANA データベースの追加 * をクリックします。
3. [Provide Resource Details] ページで、次の操作を実行します。

フィールド	手順
リソースタイプ（ Resource Type ）	リソースタイプを入力します。 リソースタイプは、単一コンテナ、マルチテナントデータベースコンテナ（ MDC ）、非データボリュームです。
HANA システム名	SAP HANA システムのわかりやすい名前を入力します。 このオプションは、単一コンテナまたは MDC リソースタイプを選択した場合にのみ使用できます。

フィールド	手順
SID	システム ID （ SID ）を入力します。 インストールされた SAP HANA システムは単一の SID で識別されます。
プラグインホスト	プラグインホストを選択します。
hdb セキュアユーザストアキー	SAP HANA システムに接続するためのキーを入力します。 このキーには、データベースに接続するためのログイン情報が含まれています。 SAP HANA システムレプリケーションでは、セカンダリユーザキーは検証されません。 この値はテイクオーバー時に使用されます。
HDBSQL OS ユーザ	HDB Secure User Store Key が設定されているユーザー名を入力します。 Windows の場合は、 HDBSQL OS ユーザがシステムユーザであることが必須です。そのため、システムユーザーに対して HDB Secure User Store Key を設定する必要があります。

4. ストレージ容量の提供ページで、ストレージシステムを選択し、ボリューム、 LUN 、および qtree を 1 つ以上選択して、 * 保存 * をクリックします。

   オプション：「 * 」をクリックします * アイコンをクリックして、他のストレージ・システムからボリューム、 LUN 、および qtree を追加します。

5. 概要を確認し、 [完了] をクリックします。

   データベースは、 SID 、プラグインホスト、関連するリソースグループとポリシー、全体的なステータスなどの情報とともに表示されます

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して権限のある処理を実行できます。

"ユーザまたはグループを追加し、ロールとアセットを割り当てます"

データベースの追加が完了したら、 SAP HANA データベースの詳細を変更できます。

SAP HANA リソースにバックアップが関連付けられている場合、次の項目は変更できません。

- マルチテナントデータベースコンテナ（ MDC ）： SID または HDBSQL Client （プラグイン）ホスト
- Single Container ： SID または HDBSQL Client （プラグイン）ホスト
- データボリューム以外：リソース名、関連付けられた SID 、またはプラグインホスト

SAP HANA データベースのバックアップポリシーを作成する

SnapCenter を使用して SAP HANA データベースのリソースをバックアップする前に、バックアップ対象のリソースまたはリソースグループのバックアップポリシーを作成する必要があります。バックアップポリシーとは、バックアップを管理、スケジューリング、および保持する方法を定めた一連のルールです。

- 必要なもの *
- バックアップ戦略を定義しておく必要があります。

  詳細については、 SAP HANA データベースのデータ保護戦略の定義に関する情報を参照してください。

- SnapCenter のインストール、ホストの追加、ストレージシステム接続のセットアップ、リソースの追加などのタスクを実行して、データ保護の準備をしておく必要があります。
- ユーザが Snapshot コピーをミラーまたはバックアップにレプリケートする場合は、ソースボリュームとデスティネーションボリューム両方の SnapCenter に SVM を割り当てる必要があります。

  また、ポリシーでレプリケーション、スクリプト、およびアプリケーションの設定を指定することもできます。これらのオプションを指定しておくことで、別のリソースグループにポリシーを再利用して時間を節約することができます。

- このタスクについて *
- SAP HANA システムレプリケーション
  - プライマリ SAP HANA システムとすべてのデータ保護処理を実行できます。
  - セカンダリ SAP HANA システムは保護できますが、バックアップは作成できません。

    フェイルオーバー後は、セカンダリ SAP HANA システムがプライマリ SAP HANA システムになるため、すべてのデータ保護処理を実行できます。

  SAP HANA データボリュームのバックアップは作成できませんが、 SnapCenter は非データボリューム（ NDV ）の保護を継続します。

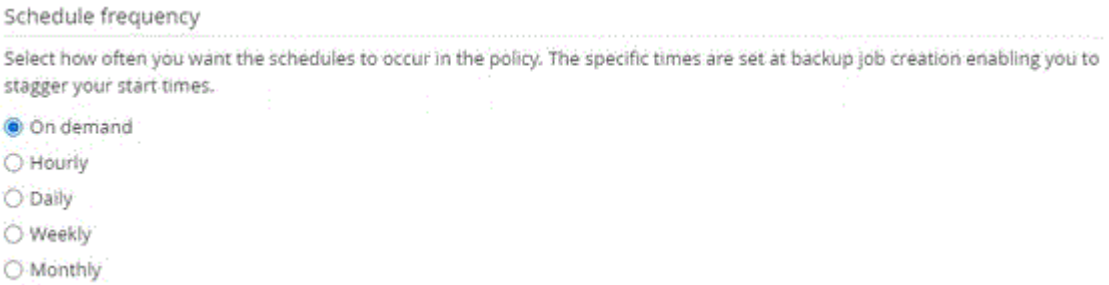
- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. 設定ページで、次の手順を実行します。
   - バックアップタイプを選択します。

状況	手順
データベースの整合性チェックを実行します	ファイルベースのバックアップ * を選択します。 アクティブなテナントのみがバックアップされます。
Snapshot コピーテクノロジを使用してバックアップを作成します	「 * Snapshot Based * 」を選択します。

- スケジュールタイプを指定するには、「 * on demand * 」、「 * Hourly * 」、「 * Daily * 」、「 * Weekly * 」、または「 * Monthly * 」を選択します。

リソースグループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間（ DST ）中はスケジュールはトリガーされません。

◦ [* カスタム・バックアップ設定 *] セクションで、キー値形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキーと値の組み合わせを複数指定することができます。

1. [保持] ページで ' バックアップ・タイプの保持設定と [バックアップ・タイプ] ページで選択したスケジュール・タイプを指定します

状況	作業
一定数の Snapshot コピーを保持します	保持する Snapshot コピーの総数 * を選択し、保持する Snapshot コピーの数を指定します。 Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。 最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。 Snapshot コピーベースのバックアップで SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。 SAP HANA システムのレプリケーションでは、 SAP HANA システムのすべてのリソースを 1 つのリソースグループに追加することを推奨します。 これにより、適切な数のバックアップが保持されます。

状況	作業
Snapshot コピーを特定の日数だけ保持します	「 * Snapshot コピーを保持する期間」を選択し、 Snapshot コピーを削除するまで保持する日数を指定します。

2. Snapshot コピーベースのバックアップの場合は、 Replication（レプリケーション）プリケーション設定を指定します。

れた保持数と同じになります。最も古い Snapshot コピーの削除は、最も古い Snapshot コピーが配置されているノードに基づい

フィールド	手順
• ローカル Snapshot コピー作成後に SnapMirror を更新 *	別のボリュームにバックアップセットのミラーコピーを作成する場合（ SnapMirror レプリケーション）は、このフィールドを選択します。 ONTAP の保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成された Snapshot コピーがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。この Snapshot コピーがリストア処理の対象としてデスティネーションで選択されると、「 Secondary Location is not available for the selected vaulted/mirrored backup 」というエラーメッセージが表示されます。
• ローカル Snapshot コピー作成後に SnapVault を更新 *	ディスクツーディスクのバックアップレプリケーション（ SnapVault バックアップ）を実行する場合は、このオプションを選択します。
• 二次ポリシーラベル *	Snapshot ラベルを選択します。 選択した Snapshot コピーラベルに応じて、 ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。 ローカル Snapshot コピーの作成後に「 * SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できます。ただし、ローカル Snapshot コピーの作成後に「 * Update SnapVault 」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。
• エラー再試行回数 *	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。

セカンダリストレージでの Snapshot コピーの最大数に達しないように、 ONTAP でセカンダリストレージの SnapMirror 保持ポリシーを設定する必要があります。

3. 概要を確認し、 [完了] をクリックします。

リソースグループを作成してポリシーを適用

リソースグループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。リソースグループはすべてのデータ保護ジョブに必要です。リソースグループに 1 つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

- このタスクについて *

SAP HANA システムのレプリケーションバックアップを作成するには、 SAP HANA システムのすべてのリソースを 1 つのリソースグループに追加することを推奨します。これにより、テイクオーバー / フェイルバックモードでのシームレスなバックアップが可能になります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 新しいリソースグループ *] をクリックします。
3. [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループの名前を入力します。 リソースグループ名は 250 文字以内にする必要があります。
タグ	リソースグループを検索するときに役立つラベルを入力します。 たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。

フィールド	手順
Snapshot コピーには、カスタムの名前形式を使用します	Snapshot コピー名にカスタムの名前形式を使用する場合は、このチェックボックスをオンにして名前形式を入力します。 たとえば 'customText_resource group_policy_hostname や resource group_hostname などですデフォルトでは、Snapshot コピー名の後ろにタイムスタンプが追加されます。

4. Resources ページで、 * Host * ドロップダウン・リストからホスト名を選択し、 * Resource Type * ドロップダウン・リストからリソース・タイプを選択します。

   これにより、画面上の情報をフィルタリングできます。

5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。

6. [アプリケーションの設定] ページで、次の操作を行います。

   a. [*Backups] の矢印をクリックして、追加のバックアップ・オプションを設定します。

      整合グループのバックアップを有効にし、次の作業を実行します。

フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot コピー処理が完了するまでの待機時間を指定するには、「至急」、「 * 中」、または「 * relaxed 」を選択します。 Urgent = 5 秒、 Medium = 7 秒、 Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

+

a. * Scripts * の矢印をクリックして、休止、 Snapshot コピー、および休止解除の各処理に対する PRE / POST コマンドを入力します。障害発生時に終了する前に実行する PRE コマンドを入力することもできます。

b. [カスタム構成 *] の矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムキーと値のペアを入力します。

パラメータ	設定	説明
archive_log_enable	（はい / いいえ）	アーカイブログの管理を有効にします をクリックして、アーカイブログを削除します。
archive_log_retention の略	日数	に日数を指定します アーカイブログは保持されます。 この設定 以上でなければなりません NTAP_SNAPSHOT_ 保持：
ARCHIVE_LOG_DIR	change_info_directory/logs	ディレクトリへのパスを指定します アーカイブログが格納されます。

パラメータ	設定	説明
archive_log_EXT	ファイル拡張子	アーカイブログファイルを指定します 延長の長さ。 たとえば、がの場合などです アーカイブログはです LOG_BACKUP_0_0_0.161518551942 9で、file_extensionの値が5の場合は、 その後、ログの拡張が行われます 5桁（16151）を保持します。
ARCHIVE_LOG_RECURSIVE_SE アーチ	（はい / いいえ）	アーカイブの管理を可能にします サブディレクトリ内にログを記録します。 あなた このパラメータは、で使用します アーカイブログはにあります サブディレクトリ：

カスタムのキーと値のペアは、 SAP HANA Linux プラグインシステムでサポートされており、一元化された Windows プラグインとして登録された SAP HANA データベースではサポートされていません。

c. Snapshot コピーツールの * 矢印をクリックして、 Snapshot コピーを作成するツールを選択します。

状況	作業
SnapCenter で Plug-in for Windows を使用してファイルシステムを整合性のある状態にしてから Snapshot コピーを作成する。Linux リソースの場合、このオプションは適用されません。	ファイルシステムの整合性を維持した状態で SnapCenter を選択します。 このオプションは、 SnapCenter Plug-in for SAP HANA Database には適用されません。
SnapCenter を使用して、ストレージレベルの Snapshot コピーを作成します	ファイルシステムの整合性なしで SnapCenter * を選択します。
Snapshot コピーを作成するためにホストで実行するコマンドを入力する	「 * other * 」を選択し、ホストで実行するコマンドを入力して Snapshot コピーを作成します。

7. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

また、 * をクリックしてポリシーを作成することもできます *

ポリシーは、 Configure schedules for selected policies セクションに表示されます。

b. Configure Schedules （スケジュールの設定）列で、 * をクリックします * をクリックします。

c. [Add schedules for policy_name_] ダイアログボックスで、スケジュールを設定し、 [OK] をクリックします。

policy_name は、選択したポリシーの名前です。

設定されたスケジュールは、 [* Applied Schedules] 列に表示されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。SMTP サーバーは、 * Settings * > * Global Settings * で設定する必要があります。

2. 概要を確認し、 [完了] をクリックします。

SAP HANA データベースをバックアップする

どのリソースグループにも含まれていないリソースは、のページからバックアップすることができます。

- 必要なもの *
- バックアップポリシーを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- Snapshot コピーベースのバックアップ処理の場合は、すべてのテナントデータベースが有効でアクティブになっていることを確認してください。
- SAP HANA システムのレプリケーションバックアップを作成するには、 SAP HANA システムのすべてのリソースを 1 つのリソースグループに追加することを推奨します。これにより、テイクオーバー / フェイルバックモードでのシームレスなバックアップが可能になります。

"リソースグループを作成してポリシーを適用"。

"リソースグループをバックアップする"

- 1つ以上のテナントデータベースが停止しているときにファイルベースのバックアップを作成する場合は、を使用して、HANAプロパティファイルのallow_file_based_backup_IFINACTIVE_tenants_Present/パ

ラメータを* YES *に設定します `Set-SmConfigSettings` コマンドレット。

コマンドレットで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

- 休止、Snapshotコピー、および休止解除のプリコマンドおよびポストコマンドについては、プラグインホストで次のパスから使用可能なコマンドリストにコマンドが含まれていないかどうかを確認する必要があります。

  Windowsの場合：_ C：\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\allowed_commands *list .txt*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _commands _list.txt*

  コマンドリストにコマンドがない場合、処理は失敗します。

- 手順 *

  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. リソースページで、リソースタイプに基づいて **View**] ドロップダウンリストからリソースをフィルタリングします。

- をクリックします* をクリックし、ホスト名とリソースタイプを選択してリソースをフィルタリングします。をクリックします をクリックしてフィルタペインを閉じます。

  1. バックアップするリソースをクリックします。
  2. リソースページで、 Snapshot コピーに * カスタム名形式を使用する * を選択し、 Snapshot コピー名に使用するカスタム名形式を入力します。

     たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

  3. [アプリケーションの設定] ページで、次の操作を行います。

     - [*Backups] の矢印をクリックして、追加のバックアップ・オプションを設定します。

       必要に応じて、整合グループのバックアップを有効にし、次の作業を実行します。

フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot コピー処理が完了するまでの待機時間を指定するには、「至急」、「 * 中」、または「 * relaxed 」を選択します。 Urgent = 5 秒、 Medium = 7 秒、 Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

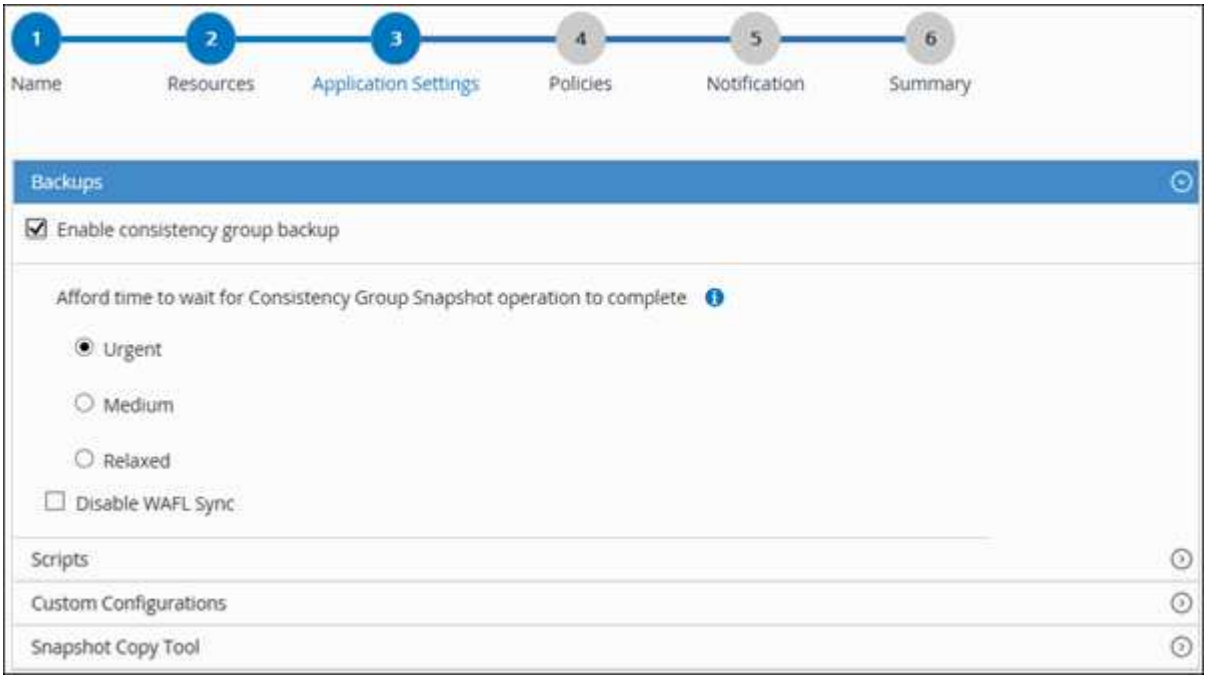
     - [* Scripts] の矢印をクリックすると、休止、 Snapshot コピー、および休止解除の各処理に対して

PRE および POST のコマンドが実行されます。

バックアップ処理を終了する前にプリコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

- [カスタム構成] 矢印をクリックし、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- Snapshot コピーツールの * 矢印をクリックして、 Snapshot コピーを作成するツールを選択します。

状況	作業
SnapCenter を使用してストレージレベルの Snapshot コピーを作成する	ファイルシステムの整合性なしで SnapCenter * を選択します。
SnapCenter ： Plug-in for Windows を使用してファイルシステムを整合性のある状態にしてから Snapshot コピーを作成する	ファイルシステムの整合性を維持した状態で SnapCenter を選択します。
Snapshot コピーを作成するコマンドを入力するには、次のコマンドを入力します	「 * other * 」を選択し、コマンドを入力して Snapshot コピーを作成します。



4. [Policies] ページで、次の手順を実行します。

   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

   また、 * をクリックしてポリシーを作成することもできます + *

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

a. * をクリックします  * スケジュールを設定するポリシーの [スケジュールの設定] 列。

b. [Add schedules for policy_name_] ダイアログボックスで、スケジュールを設定し、 [OK] をクリックします。

_policy_name_は 、選択したポリシーの名前です。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

2. 概要を確認し、 [完了] をクリックします。

   リソースのトポロジページが表示されます。

3. [今すぐバックアップ] をクリックします。

4. Backup （バックアップ）ページで、次の手順を実行します。

   a. リソースに複数のポリシーを適用した場合は、 [* Policy] ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. [バックアップ] をクリックします。

5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   - MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。

     詳細については、を参照してください "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"

   - VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。

     Java のヒープサイズを増やすには、スクリプトファイル /opt/NetApp/init_scripts/scvservice_. を探します。このスクリプトでは、 *DO_START METHOD_Command* によって、 *SnapCenter VMware* プラグインサービスが開始されます。このコマンドを次のように更新します。 *_java -jar -Xmx8192M -Xms4096M*

リソースグループをバックアップする

リソースグループは、ホスト上のリソースの集まりです。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースを対象に実行されます。

- 必要なもの *
- ポリシーを適用したリソースグループを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- このタスクについて *

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。

     リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックします をクリックし、タグを選択します。をクリックします をクリックしてフィルタペインを閉じます。
  3. [リソースグループ] ページで、バックアップするリソースグループを選択し、 [今すぐバックアップ *] をクリックします。
  4. Backup （バックアップ）ページで、次の手順を実行します。
     a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

        オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

     b. [バックアップ] をクリックします。
  5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用して SAP HANA データベース用のストレージシステム接続とクレデンシャルを作成します

PowerShell コマンドレットを使用して SAP HANA データベースのバックアップ、リストア、クローニングを行うには、 Storage Virtual Machine （ SVM ）接続とクレデンシャルを作成する必要があります。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホス

ト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

- 手順 *

  1. Open-SmConnection コマンドレットを使用して、 PowerShell 接続セッションを開始します。

     ```
     PS C:\> Open-SmStorageConnection
     ```

  2. Add-SmStorageConnection コマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

     ```
     PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
     -Timeout 60
     ```

  3. Add-SmCredential コマンドレットを使用して新しいクレデンシャルを作成します。

     次の例は、 Windows クレデンシャルを使用して FinanceAdmin という名前の新しいクレデンシャルを作成する方法を示しています。

     ```
     PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
     -Credential sddev\administrator
     ```

  4. SnapCenter サーバに SAP HANA 通信ホストを追加します。

     ```
     PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
     FinanceAdmin -PluginCode hana
     ```

  5. パッケージと SnapCenter Plug-in for SAP HANA Database をホストにインストールします。

     Linux の場合：

     ```
     PS C:> Install-SmHostPackage -HostNames 10.232.204.61
     -ApplicationCode hana
     ```

     Windows の場合：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. HDBSQL クライアントのパスを設定します。

   Windows の場合：

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61
-PluginCode hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

   Linux の場合：

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

PowerShell コマンドレットを使用してデータベースをバックアップします

データベースをバックアップするときは、 SnapCenter サーバとの接続を確立してから、リソースの追加、ポリシーの追加、バックアップリソースグループの作成を行って、バックアップを実行します。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。
- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
```

   ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResources コマンドレットを使用してリソースを追加します。

   この例は、 SingleContainer タイプの SAP HANA データベースを追加する方法を示しています。

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"
}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

この例は、 MultipleContainers タイプの SAP HANA データベースを追加する方法を示しています。

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.neta
pp.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

次の例は、データボリューム以外のリソースを作成する方法を示しています。

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Add-SmPolicy コマンドレットを使用してバックアップポリシーを作成します。

   この例では、 Snapshot コピーベースのバックアップのバックアップポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
-PluginPolicyType hana -BackupType SnapShotBasedBackup
```

   この例では、ファイルベースのバックアップのバックアップポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Add-SmResourceGroup コマンドレットを使用して、リソースを保護するか、新しいリソースグループを SnapCenter に追加します。

   この例では、単一コンテナのリソースを保護しています。

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

この例では、複数コンテナのリソースを保護しています。

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

この例では、ポリシーとリソースを指定して新しいリソースグループを作成しています。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="scc
orelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

この例では、データボリューム以外のリソースグループを作成しています。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="
hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Plug
inName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDa
taVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. New-SmBackup コマンドレットを使用して、新しいバックアップジョブを開始する。

   この例は、リソースグループをバックアップする方法を示しています。

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

この例では、保護されたリソースをバックアップしています。

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"} -Policy
hana_Filebased
```

1. Get-smJobSummaryReport コマンドレットを使用して、ジョブのステータス（実行中、完了、または失敗）を監視します。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

2. Get-SmBackupReport コマンドレットを使用して、リストア処理やクローニング処理を実行するバックアップ ID とバックアップ名など、バックアップジョブの詳細を監視します。

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

バックアップ処理を監視する

SAP HANA データベースのバックアップ処理を監視する

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします バックアップ処理だけが表示されるようにリストをフィルタリングします。
   b. 開始日と終了日を指定します。
   c. [* タイプ] ドロップダウン・リストから、 **[*Backup]** を選択します。
   d. [**Status**](ステータス *) ドロップダウンから、バックアップステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. バックアップジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

   バックアップジョブのステータスがと表示されます で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

   View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

アクティビティペインで、 **SAP HANA** データベースに対するデータ保護処理を監視します

[アクティビティ（ Activity ）] パネルには、最近実行された 5 つの操作が表示されます。また、操作が開始された日時と操作のステータスも表示されます。

[Activity （アクティビティ）] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. をクリックします をクリックして、最近の 5 つの操作を表示します。

     いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

SAP HANA のバックアップ処理をキャンセルします

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの *
- 処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。
- バックアップ操作は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のバックアップ処理をキャンセルすることはできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、バックアップ処理をキャンセルできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っているバックアップ操作をキャンセルできます
- 手順 *
  1. 次のいずれかを実行します。

方法	アクション
監視ページ	a. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 b. 操作を選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	a. バックアップ処理を開始したら、 * をクリックします * ［ アクティビティ ］ パネルには、最近の 5 つの操作が表示されます。 b. 処理を選択します。 c. ［ ジョブの詳細 ］ ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

処理がキャンセルされ、リソースが以前の状態に戻ります。

Topology ページで、 SAP HANA データベースのバックアップとクローンを表示します

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

- このタスクについて *

[コピーの管理] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップとクローンが使用可能かどうかを判断できます。

-  には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
-  には、 SnapMirror テクノロジを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。
-  には、 SnapVault テクノロジを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。

表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、 4 つのバックアップだけを保持するポリシーを使用して 6 つのバックアップを作成した場合、バックアップの数は 6 と表示されます。

mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

SAP HANA システムレプリケーションのプライマリリソースの場合は、リストア処理と削除処理がサポートされ、セカンダリリソースの場合はクローン処理がサポートされます。

トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. サマリー・カード * を確認して、プライマリ・ストレージとセカンダリ・ストレージで使用可能なバックアップとクローンの数を確認します。

   「 * サマリカード * 」セクションには、ファイルベースのバックアップ、 Snapshot コピーバックアップ、およびクローンの合計数が表示されます。

「 * Refresh * 」ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

1. [コピーの管理] ビューで、プライマリストレージまたはセカンダリストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

   バックアップとクローンの詳細が表形式で表示されます。

2. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。

   セカンダリストレージ上のバックアップは、名前変更または削除できません。

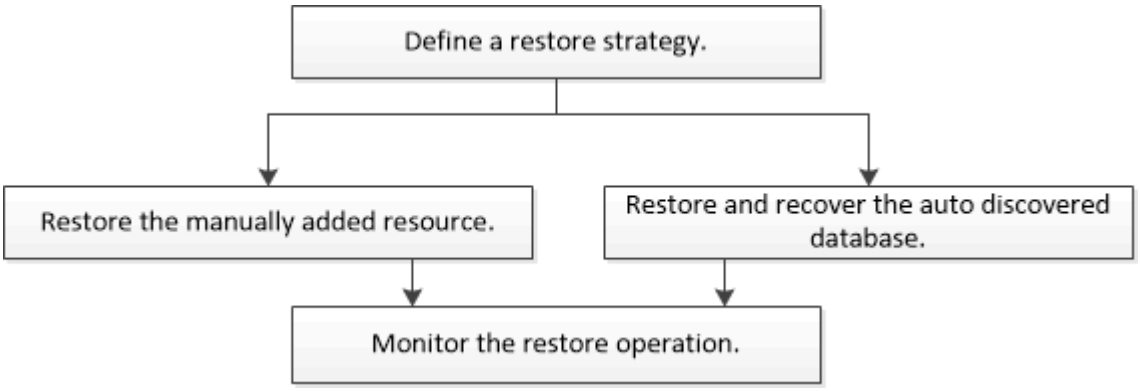
3. クローンを削除する場合は、表でクローンを選択し、をクリックします 。
4. クローンをスプリットする場合は、表でクローンを選択し、をクリックします 。

SAP HANA データベースをリストア

リストアワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、 SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

"SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

手動で追加したリソースバックアップをリストアおよびリカバリする

SnapCenter を使用して、 1 つ以上のバックアップからデータをリストアおよびリカバリできます。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドについて、プラグインホストのコマンドリストに以下のパスからコマンドが含まれていないか確認してください。

  Windowsの場合：_ C：\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\allowed_commands *list .txt*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _commands _list.txt*

  コマンドリストにコマンドがない場合、処理は失敗します。

- このタスクについて *
- ファイルベースのバックアップのコピーを SnapCenter からリストアすることはできません。
- SnapCenter 4.3 にアップグレードすると、 SnapCenter 4.2 で作成されたバックアップはリストアできますが、リカバリすることはできません。SnapCenter 4.2 で作成されたバックアップをリカバリするには、SnapCenter の外部で HANA Studio または HANA リカバリスクリプトを使用する必要があります。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、 **View**] ドロップダウンリストからリソースをフィルタリングします。

   リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、およびステータスとともに表示されます。

   リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。

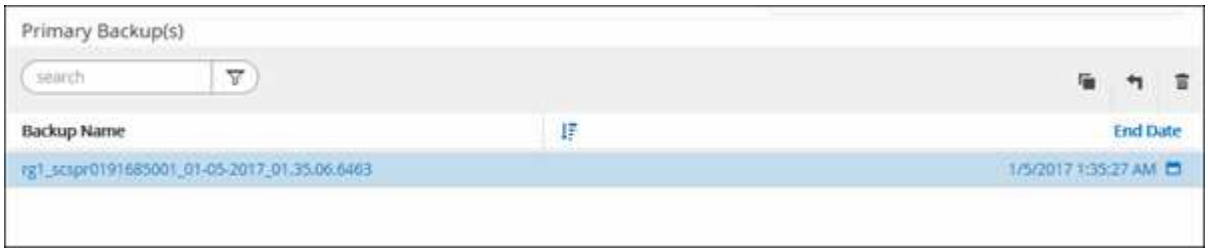
   リソースが保護されていない場合は ' 保護されていないというメッセージが [全体のステータス] 列に表示されますこれは、リソースが保護されていないこと、またはリソースが別のユーザによってバックアップされていることを意味します。

3. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

   リソースのトポロジページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。

5. [プライマリ・バックアップ] テーブルで、リストア元のバックアップを選択し、 [*] をクリックします *



6. [リストア範囲] ページで、 [* リソース全体 *] または [* ファイルレベル *] を選択します。

   a. Complete Resource * を選択すると、 SAP HANA データベースに設定されているすべてのデータボリュームがリストアされます。

      リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

   b. 「 * ファイルレベル * 」を選択した場合は、「 * すべて * 」を選択するか、特定のボリュームまたは qtree を選択してから、それらのボリュームまたは qtree に関連するパスをカンマで区切って入力できます

      - ボリュームと qtree は複数選択できます。
      - リソースタイプが LUN の場合は、 LUN 全体がリストアされます。

        LUN は複数選択できます。

「 * all * 」を選択すると、ボリューム、 qtree 、または LUN 上のすべてのファイルがリストアされます。

1. [リストア前] ページで、リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを入力します。

   自動検出されたリソースにはアンマウントコマンドを使用できません。

2. [ポスト・オペレーション] ページで、マウントおよびリストア後のコマンドを入力して、リストア・ジョブの実行後に実行します。

   自動検出されたリソースに対しては、 mount コマンドを使用できません。

3. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレスと E メールの件名を指定する必要があります。また、 [* 設定 * （ Settings * ）] > [* グローバル設定 * （ * Global Settings * ）] ページでも SMTP を設定する必要があります。

4. 概要を確認し、 [完了] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

自動検出されたデータベースバックアップをリストアおよびリカバリする

SnapCenter を使用して、 1 つ以上のバックアップからデータをリストアおよびリカバリできます。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドについて、プラグインホストのコマンドリストに以下のパスからコマンドが含まれていないか確認してください。

  Windowsの場合：_ C：\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\allowed_commands *list .txt*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _commands _list.txt*

  コマンドリストにコマンドがない場合、処理は失敗します。

- このタスクについて *
- ファイルベースのバックアップのコピーを SnapCenter からリストアすることはできません。
- SnapCenter 4.3 にアップグレードすると、 SnapCenter 4.2 で作成されたバックアップはリストアできますが、リカバリすることはできません。SnapCenter 4.2 で作成されたバックアップをリカバリするには、SnapCenter の外部で HANA Studio または HANA リカバリスクリプトを使用する必要があります。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、 **View**] ドロップダウンリストからリソースをフィルタリングします。

   リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、およびステータスとともに表示されます。

   リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。

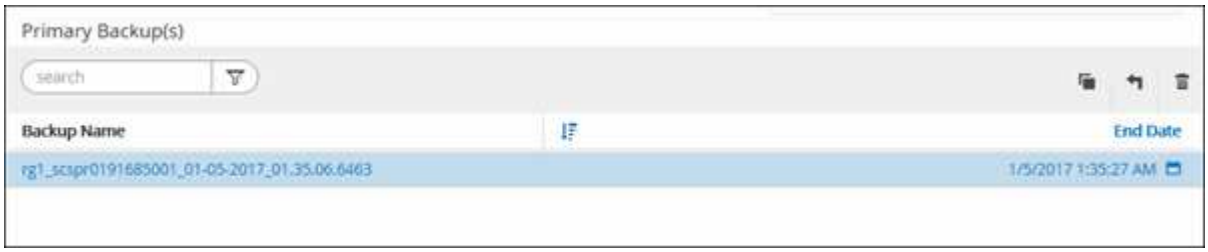
   リソースが保護されていない場合は ' 保護されていないというメッセージが [全体のステータス] 列に表示されますこれは、リソースが保護されていないこと、またはリソースが別のユーザによってバックアップされていることを意味します。

3. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

   リソースのトポロジページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。

5. [プライマリ・バックアップ] テーブルで、リストア元のバックアップを選択し、 [*] をクリックします *



6. Restore Scope ページで、 **Complete Resource** を選択して、 SAP HANA データベースの設定済みデータボリュームをリストアします。

Complete Resource * （ * Volume Revert * あり / なし）または * Tenant Database * のいずれかを選択できます。

ユーザが * テナントデータベース * オプションまたは * Complete Restore * オプションを選択した場合、複数のテナントに対して SnapCenter サーバがリカバリ処理をサポートしていません。リカバリ処理を実行するには、 HANA Studio または HANA Python スクリプトを使用する必要があります。

a. ボリューム全体をリストアする場合は、 * Volume Revert * を選択します。

このオプションは、 NFS 環境における SnapCenter 4.3 で作成されたバックアップに使用できます。

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。このオプションは、リストア対象として「 * Volume Revert * 」オプションを指定した状態で * Complete Resource * を選択した場合に使用できます。

b. [* Tenant Database] を選択します。

このオプションは MDC リソースでのみ使用できます。

リストア処理を実行する前にテナントデータベースを停止する必要があります。

「 * テナントデータベース * 」オプションを選択した場合は、リカバリ処理を実行するために、 HANA Studio を使用するか、 SnapCenter 外部の HANA リカバリスクリプトを使用する必要があります。

1. Recovery スコープページで、次のいずれかのオプションを選択します。

状況	手順
現在までできるだけ近い時間にリカバリする必要がある	[* 最新の状態に回復する *] を選択します。 単一のコンテナリソースについては、 1 つ以上のログとカタログのバックアップ先を指定します。 マルチテナントデータベースコンテナ（ MDC ）リソースの場合は、 1 つ以上のログバックアップの場所とバックアップカタログの場所を指定 MDC リソースの場合は、パスにシステムデータベースとテナントデータベースのログの両方が含まれている必要があります。

状況	手順
指定した時点までリカバリする場合	[* 特定の時点にリカバリする *] を選択します。 a. タイムゾーンを選択します。 ブラウザのタイムゾーンはデフォルトで入力されています。 選択したタイムゾーンと入力時間が絶対 GMT に変換されます。 b. 日時を入力します。 たとえば、 HANA Linux ホストは CA のサニーベールにあり、 Raleigh のユーザは SnapCenter にログインをリカバリしています。 これらのロケーション間の時間差は 3 時間で、ユーザは NC の Raleigh からログインしているため、 GUI で選択されるデフォルトのブラウザタイムゾーンは GMT-04 ： 00 です。 ユーザが CA のサニーベールから 5 午前 6 時までのリカバリを実行する場合は、ブラウザのタイムゾーンを HANA Linux ホストのタイムゾーン（ GMT-07 ： 00 ）に設定し、日時を午前 5 時に指定する必要があります 単一のコンテナリソースについては、 1 つ以上のログとカタログのバックアップ先を指定します。 MDC リソースの場合は、 1 つ以上のログバックアップの場所とバックアップカタログの場所を指定します。 MDC リソースの場合は、パスにシステムデータベースとテナントデータベースのログの両方が含まれている必要があります。
特定のデータ・バックアップにリカバリする場合	［ * 指定されたデータバックアップにリカバリする * ］ を選択します。
リカバリが不要である場合	「 * リカバリなし * 」を選択します。 リカバリ処理は HANA Studio から手動で実行する必要があります。

リカバリできるの SnapCenter は、ホストとプラグインの両方が SnapCenter 4.3 にアップグレードされ、リストア用に選択されたバックアップがリソースの変換後または自動検出されたあとに実行される場合に限られます。

2. [リストア前] ページで、リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを入力します。

   自動検出されたリソースにはアンマウントコマンドを使用できません。

3. [ポスト・オペレーション] ページで、マウントおよびリストア後のコマンドを入力して、リストア・ジョブの実行後に実行します。

   自動検出されたリソースに対しては、 mount コマンドを使用できません。

4. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレスと E メールの件名を指定する必要があります。また、 [* 設定 * （ Settings * ）] > [* グローバル設定 * （ * Global Settings * ）] ページでも SMTP を設定する必要があります。

5. 概要を確認し、 [完了] をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用して SAP HANA データベースをリストアする

SAP HANA データベースのバックアップをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

- 必要なもの *

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップを特定します。

   この例では、リストアできるバックアップが 2 つあります。

```
 PS C:\> Get-SmBackup

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM  Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

この例では、 2015 年 1 月 29 日から 2015 年 2 月 3 日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. HANA Studio でリカバリプロセスを開始します。

   データベースがシャットダウンされます。

4. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

   AppObjectId は「 Host\Plugin\UID 」です。 UID=SID は単一コンテナタイプのリソース用で、 UID=MDC\SID は複数コンテナのリソース用です。ResourceID は、 Get-smResources コマンドレットから取得できます。

   ```
   Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
   ```

   この例は、プライマリストレージからデータベースをリストアする方法を示しています。

   ```
   Restore-SmBackup -PluginCode HANA -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 3
   ```

   この例は、セカンダリストレージからデータベースをリストアする方法を示しています。

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

+
バックアップが HANA Studio でリカバリに使用できるようになります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

PowerShell コマンドレットを使用してリソースをリストアする

リソースのバックアップをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップに関する情報を取得します。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

   この例では、 2015 年 1 月 29 日から 2015 年 2 月 3 日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

1. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SAP HANA データベースのリストア処理を監視する

Jobs ページを使用して、 SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします リストをフィルタリングして、リストア処理のみを表示します。
   b. 開始日と終了日を指定します。
   c. [* タイプ] ドロップダウン・リストから、 [リストア *] を選択します。
   d. [* Status *] ドロップダウン・リストから、リストア・ステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

   View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

SAP HANA リソースのバックアップをクローニングする

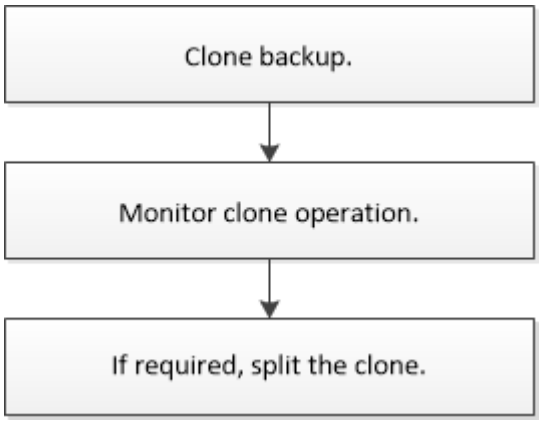
クローニングワークフロー

クローニングワークフローには、クローニング処理の実行と処理の監視が含まれます。

- このタスクについて *
- ソースの SAP HANA サーバでクローニングを実行できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
  - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
  - データの抽出と操作を行うツールで、データウェアハウスにデータを取り込むため

◦ 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、 SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

SAP HANA データベースのバックアップをクローニングします

SnapCenter を使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine （ SVM ）に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- ファイルベースのバックアップはクローニングできません。
- ターゲットクローンサーバの SAP HANA インスタンス SID が、 Target Clone SID フィールドに入力されたものと同じであることが必要です。
- クローニング前またはクローニング後のPREコマンドについては、次のパスから、プラグインホストのコマンドリストにコマンドが含まれているかどうかを確認する必要があります。

  Windowsの場合：_ C：\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\allowed_commands *list .txt*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _commands _list.txt*

  コマンドリストにコマンドがない場合、処理は失敗します。

- このタスクについて *

クローンスプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、 **View**] ドロップダウンリストからリソースをフィルタリングします。

   リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、ステータスなどの情報とともに表示されます。
3. リソースまたはリソースグループを選択します。

   リソースグループを選択する場合は、リソースを選択する必要があります。

   リソースまたはリソースグループのトポロジページが表示されます。
4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。
5. 表からデータバックアップを選択し、をクリックします  。
6. Location ページで、次のアクションを実行します。

フィールド	手順
プラグインホスト	クローンのマウント先のプラグインがインストールされたホストを選択します。
ターゲットクローンの SID	既存のバックアップからクローニングする SAP HANA インスタンス ID を入力します。
NFS エクスポートの IP アドレス	クローニングしたボリュームをエクスポートする IP アドレスまたはホスト名を入力します。
iSCSI イニシエータ	LUN のエクスポート先であるホストの iSCSI イニシエータ名を入力します。 このオプションは、 LUN リソースタイプを選択した場合にのみ使用できます。
プロトコル	LUN プロトコルを入力します。 このオプションは、 LUN リソースタイプを選択した場合にのみ使用できます。

   リソースとして LUN を選択し、セカンダリバックアップからクローニングする場合、デスティネーションボリュームのリストが表示されます。1 つのソースについて複数のデスティネーションボリュームを選択することができます。

   クローニングを実行する前に、 iSCSI イニシエータまたは FCP が存在し、代替ホストに設定およびログインしていることを確認する必要があります。
7. Scripts ページで、次の手順を実行します。

スクリプトはプラグインホストで実行されます。

a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
   - クローニング前のコマンド：同じ名前の既存のデータベースを削除します
   - クローニング後のコマンド：データベースの検証やデータベースの起動

b. ホストにファイルシステムをマウントするには、 mount コマンドを入力します。

   Linux マシンのボリュームまたは qtree に対する mount コマンド：

NFS の例：

```
mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
```

8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。

9. 概要を確認し、 [完了] をクリックします。
10. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用して SAP HANA データベースのバックアップをクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup コマンドレットを使用して、クローニング処理を実行するバックアップを取得します。

   この例では、クローニングできるバックアップが 2 つあります。

```
 C:\PS> Get-SmBackup

        BackupId                        BackupName
BackupTime                      BackupType
        --------                        ----------
----------                      ----------
         1                       Payroll Dataset_vise-f6_08... 8/4/2015
11:02:32 AM          Full Backup
         2                       Payroll Dataset_vise-f6_08... 8/4/2015
11:23:17 AM
```

3. 既存のバックアップからクローニング処理を開始し、クローニングされたボリュームをエクスポートする NFS エクスポートの IP アドレスを指定します。

   この例では、 NFSExportIPs のアドレスを 10.232.206.169 と指定してバックアップをクローニングしています。

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

   NFSExportIPs を指定しない場合、デフォルトでクローンターゲットホストにエクスポートされます。

4. Get-SmCloneReport コマンドレットを使用してクローニングジョブの詳細を表示し、バックアップが正常にクローニングされたことを確認します。

   クローン ID 、開始日時、終了日時などの詳細を確認できます。

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

SAP HANA データベースのクローニング処理を監視する

Jobs ページを使用して、 SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。

3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
   b. 開始日と終了日を指定します。
   c. [**Type**](タイプ) ドロップダウンリストから **'[*Clone**](クローン *) を選択します
   d. [* Status *] ドロップダウン・リストから、クローンのステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. クローンジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

クローンをスプリットします。

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

- このタスクについて *
- 中間のクローンに対してクローンスプリット処理を実行することはできません。

  たとえば、データベースバックアップから clone1 を作成したあとで、 Clone1 のバックアップを作成し、そのバックアップ（ Clone2 ）をクローニングできます。Clone2 を作成すると、 clone1 は中間クローンであり、 clone1 でクローンスプリット処理を実行することはできません。ただし、 Clone2 でクローンスプリット処理を実行することはできます。

  Clone2 をスプリットしたあとは、 clone1 が中間クローンではなくなるため、 clone1 でクローンスプリット処理を実行できます。

- クローンをスプリットすると、クローンのバックアップコピーとクローンジョブが削除されます。
- クローンスプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。
- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [表示] リストから適切なオプションを選択します。

オプション	説明
データベースアプリケーション用	[表示] リストから [*Database] を選択します。
ファイルシステムの場合	[表示] リストから [* パス *] を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジページが表示されます。

4. [コピーの管理] ビューで、クローン作成されたリソース（データベースや LUN など）を選択し、 [*] をクリックします *
5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   SMCore サービスが再起動すると、クローンスプリット処理が応答しなくなります。Stop-SmJob コマンドレットを実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

   クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、 _SMCoreServiceHost.exe.config_file の _CloneSplitStatusCheckPollTime_Parameter の値を変更して、 SMCore がクローンスプリット処理のステータスをポーリングする間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

   例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

+
バックアップ、リストア、または別のクローンスプリットの実行中は、クローンスプリットの開始処理が失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

- 詳細はこちら *

"「 aggregate does not exist 」というメッセージが表示されて、 SnapCenter クローンまたは検証が失敗する"

SnapCenter のアップグレード後に、 SAP HANA データベースのクローンを削除またはスプリットします

SnapCenter 4.3 にアップグレードすると、クローンは表示されなくなります。クローンを削除するか、クローンが作成されたリソースのトポロジページからクローンをスプリットします。

- このタスクについて *

非表示クローンのストレージ設置面積を確認するには、次のコマンドを実行します。 `Get-SmClone -ListStorageFootprint`

- 手順 *

1. remove-smbackup コマンドレットを使用して、クローニングしたリソースのバックアップを削除します。
2. remove-smresourcegroup コマンドレットを使用して、クローニングされたリソースのリソースグループを削除します。
3. remove-smprotectresource コマンドレットを使用して、クローニングされたリソースの保護を解除します。

4. [リソース] ページから親リソースを選択します。

   リソースのトポロジページが表示されます。

5. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムからクローンを選択します。
6. クローンを選択し、をクリックします  クローンを削除するには、をクリックします  をクリックしてクローンをスプリットします。
7. [OK] をクリックします。

Oracle データベースを保護します

SnapCenter Plug-in for Oracle Database の概要を参照してください

Plug-in for Oracle Database の機能

SnapCenter Plug-in for Oracle Database は、 Oracle データベースに対応したデータ保護管理を提供する、 NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。

Plug-in for Oracle Database によって、 Oracle Recovery Manager （ RMAN ）、検証、マウント、アンマウント、リストア、 SnapCenter 環境での Oracle データベースのリカバリとクローニング
Plug-in for Oracle Database は、すべてのデータ保護処理を実行するために SnapCenter Plug-in for UNIX をインストールします。

Plug-in for Oracle Database では、 SAP アプリケーションを実行している Oracle データベースのバックアップを管理することができます。ただし、 SAP BR * Tools との統合はサポートされません。

- データファイル、制御ファイル、およびアーカイブログファイルをバックアップします。

  バックアップはコンテナデータベース（ CDB ）レベルでのみサポートされます。

- データベース、 CDB 、および Pluggable Database （ PDB ）のリストアとリカバリを行います。

  PDB の不完全リカバリはサポートされていません。

- ある時点までの本番環境データベースのクローンを作成します。

  クローニングは CDB レベルでのみサポートされます。

- バックアップをただちに検証します。
- リカバリ処理のためにデータバックアップとログバックアップのマウントとアンマウントを行います。
- バックアップ処理と検証処理をスケジュールします。
- すべての処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

Plug-in for Oracle Database の特長

Plug-in for Oracle Database は、 Linux または AIX ホスト上で Oracle データベースと統合されるほか、ストレージシステム上でネットアップのテクノロジと統合されます。

- 統一されたグラフィカルユーザインターフェイス

  SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter のインターフェイスから、すべてのプラグインで、バックアップ、リストア、リカバリ、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（ RBAC ）を設定したり、ジョブを監視したりすることができます。

- 中央管理の自動化

  バックアップ処理とクローニング処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenter から E メールアラートを送信するように設定して、環境をプロアクティブに監視することもできます。

- 無停止の NetApp Snapshot コピーテクノロジ

  SnapCenter では、 Plug-in for Oracle Database および Plug-in for UNIX でネットアップの Snapshot コピーテクノロジを使用してデータベースがバックアップされます。Snapshot コピーはストレージスペースを最小限しか消費しません。

Plug-in for Oracle Database には、次のようなメリットもあります。

- バックアップ、リストア、クローニング、マウント、アンマウント、 検証ワークフローなどがあります
- ホストに設定されているOracleデータベースの自動検出
- Oracle Recovery Manager （ RMAN ）を使用したカタログ化とカタログ化解除がサポートされます。
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます

  また、許可された SnapCenter ユーザにアプリケーションレベルの権限を付与するようにクレデンシャルを設定することもできます。

- アーカイブログ管理（ALM）でリストア処理とクローニング処理がサポートされます
- NetApp FlexClone テクノロジを使用して、本番環境のデータベースのスペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

  クローンを作成するストレージシステムに FlexClone ライセンスが必要です。

- SAN 環境および ASM 環境でバックアップを作成する際に、 ONTAP の整合グループ（ CG ）機能がサポートされます
- 自動化された無停止のバックアップ検証
- 複数のデータベースホストで同時に複数のバックアップを実行できます

  1 回の処理で、 1 つのホストのデータベースが同じボリュームを共有する場合に複数の Snapshot コピーが統合されます。

- 物理インフラと仮想インフラがサポートされます
- NFS 、 iSCSI 、ファイバチャネル（ FC ）、 RDM 、 NFS および VMFS 経由の VMDK 、 NFS 、 SAN 、 RDM 、および VMDK 経由の ASM がサポートされます
- ONTAP の選択的 LUN マップ（ SLM ）機能がサポートされます

  デフォルトで有効になる SLM 機能は、最適パスを持たない LUN を定期的に検出して修正します。SLM を設定するには、 /var/opt/snapcenter /scu/etc. にある scu.properties ファイル内のパラメータを変更します

  - この機能を無効にするには、ENABLE_LUNPATH_MONITORINGパラメータの値をfalseに設定します。
  - LUNパスが自動的に修正される頻度を指定するには、LUNPATH_MONITORING_INTERVALパラメー

タに値（時間単位）を割り当てます。
SLM の詳細については、を参照してください "ONTAP 9 SAN アドミニストレーションガイド"。

- LinuxでのNon-Volatile Memory Express（NVMe）のサポート
  - NVMe utilをホストにインストールする必要があります。

    代替ホストにクローニングまたはマウントするには、NVMe utilをインストールする必要があります。

  - バックアップ、リストア、クローニング、マウント、アンマウント、 VMDKやRDMなどの仮想環境を除き、NVMeハードウェアでカタログ化、カタログ化解除、および検証の処理がサポートされます。

    上記の操作は、パーティションがないデバイスまたはシングルパーティションでサポートされています。

NVMeデバイス用のマルチパス解決策 は、カーネルで標準のマルチパスオプションを設定することで設定できます。Device Mapper（DM）マルチパスはサポートされていません。

- OracleおよびGRIDではなく、デフォルト以外のすべてのユーザをサポートします。

  デフォルト以外のユーザをサポートするには、_ file /var/opt/snapcenter/sco/etc/_にある* sco.properties* ファイルのパラメータの値を変更して、デフォルト以外のユーザを設定する必要があります。

  パラメータのデフォルト値は、OracleとGridに設定されています。

  - db_user = Oracleの場合
  - db_group=oinstall
  - gi_user = grid
  - gi_group = oinstall

Plug-in for Oracle Database でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシンの両方でさまざまなストレージタイプをサポートしています。SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

SnapCenter では、 Linux および AIX のストレージプロビジョニングはサポートされていません。

Linux でサポートされているストレージタイプ

次の表に、 Linux でサポートされるストレージタイプを示します。

マシン	ストレージタイプ
物理サーバ	• FC 接続 LUN • iSCSI で接続された LUN • NFS-connected ボリューム

マシン	ストレージタイプ
VMware ESXi	• FC または iSCSI ESXi HBA によって接続された RDM LUN は、ホストに存在するすべてのホストバスアダプタを SnapCenter がスキャンするため、完了までに時間がかかることがあります。 /opt/NetApp/SnapCenter /spl/plugins/SCU/scucore /modules/SCU/ConfigU/Config_に ある * LinuxConfig.pm * ファイルを編集して、 * scsi_hosts _optimized_rescan * パラメーターの値を 1 に設定し、 ha_driver_names にリストされている HBA のみを再スキャンすることができます。 • iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN • VMFS データストアまたは NFS データストア上の VMDK • ゲストシステムに直接接続された NFS ボリューム

AIX でサポートされているストレージタイプ

次の表に、 AIX でサポートされるストレージタイプを示します。

マシン	ストレージタイプ
物理サーバ	• FC 接続 LUN と iSCSI 接続 LUN ： SAN 環境では、 ASM 、 LVM 、および SAN のファイルシステムがサポートされます。 AIX およびファイルシステムでの NFS はサポートされていません。 • 拡張ジャーナルファイルシステム（ JFS2 ） SAN ファイルシステムおよび LVM レイアウトでのインラインロギングをサポートします。

。 "NetApp Interoperability Matrix Tool で確認できます" サポートされているバージョンに関する最新情報が含まれています。

Plug-in for Oracle の **SnapMirror** と **SnapVault** のレプリケーションに使用するストレージシステムを準備

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアッ

プセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenter は、Snapshotコピー処理の完了後に、SnapMirrorとSnapVault に対する更新を実行します。SnapMirror更新とSnapVault 更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SnapCenter は * sync-mirror * レプリケーションをサポートしていません。

Plug-in for Oracle に必要な最小 ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
• event generate-autosupport-log を指定します
• ジョブ履歴の表示 • ジョブが停止しました

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限

- LUN
- lun attribute show
- lun create をクリックします
- lun delete
- LUN ジオメトリ
- LUN igroup add
- lun igroup create を追加します
- lun igroup delete
- LUN igroup の名前を変更します
- lun igroup show を参照してください
- LUN マッピングの追加 - レポートノード
- LUN マッピングが作成されます
- LUN マッピングが削除されます
- LUN マッピングの削除 - レポートノード
- lun mapping show
- lun modify を追加します
- LUN のボリューム内移動
- LUN はオフラインです
- LUN はオンラインです
- LUN の永続的予約はクリアします
- LUN のサイズ変更
- LUN シリアル
- lun show をクリックします

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
• SnapMirror ポリシー追加ルール • snapmirror policy modify-rule • snapmirror policy remove-rule 」を実行します • snapmirror policy show の略 • SnapMirror リストア • snapmirror show の略 • snapmirror show -history の略 • SnapMirror の更新 • SnapMirror の update-ls-set • snapmirror list-destinations
• バージョン

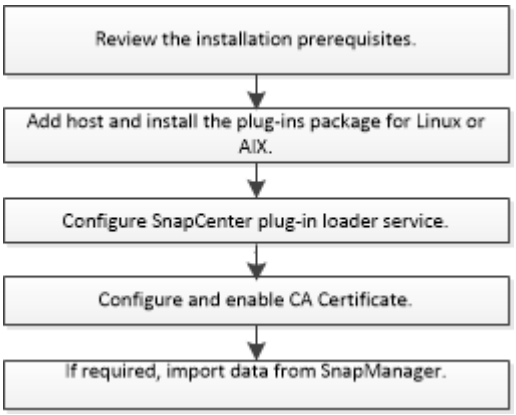
フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
• volume clone create を実行します • volume clone show を実行します • ボリュームクローンスプリット開始 • ボリュームクローンスプリットは停止します • volume create を実行します • ボリュームを削除します • volume file clone create を実行します • volume file show-disk-usage • ボリュームはオフラインです • ボリュームはオンラインです • volume modify を使用します • volume qtree create を実行します • volume qtree delete • volume qtree modify の略 • volume qtree show の略 • ボリュームの制限 • volume show のコマンドです • volume snapshot create を実行します • ボリューム Snapshot の削除 • volume snapshot modify の実行 • ボリューム Snapshot の名前が変更されます • ボリューム Snapshot リストア • ボリューム Snapshot の restore-file • volume snapshot show の実行 • ボリュームのアンマウント
• Vserver • SVM CIFS です • vserver cifs shadowcopy show • vserver show のコマンドです
• Network Interface の略 • network interface show の略

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
• MetroCluster のショーをご覧ください

SnapCenter Plug-in for Oracle Database をインストールします

SnapCenter Plug-in for Oracle Database のインストールワークフロー

Oracle データベースを保護する場合は、 SnapCenter Plug-in for Oracle Database をインストールしてセットアップする必要があります。



ホストを追加して **Plug-in Package for Linux** または **AIX** をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSI を使用している場合は、 iSCSI サービスが実行されている必要があります。
- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。

  SnapCenter Plug-in for Oracle Database は、 root 以外のユーザがインストールできます。ただし、プラグインプロセスをインストールして開始できるように root 以外のユーザに sudo 権限を設定する必要があります。プラグインをインストールすると、有効なroot以外のユーザとしてプロセスが実行されるようになります。

- AIX ホストに SnapCenter Plug-ins Package for AIX をインストールする場合は、ディレクトリレベルのシンボリックリンクを手動で解決しておく必要があります。

  SnapCenter Plug-ins Package for AIX は、ファイルレベルのシンボリックリンクを自動的に解決しますが、 JAVA_HOME の絶対パスを取得するためのディレクトリレベルのシンボリックリンクは解決しません。

- インストールユーザ用に、認証モードを Linux または AIX に設定してクレデンシャルを作成します。
- LinuxまたはAIXホストにJava 1.8.xまたはJava 11（64ビット）をインストールしておく必要があります。

Linuxホスト にJava 11の認定エディションのみがインストールされていることを確認します。

Java のダウンロード方法については、次を参照してください。

- "すべてのオペレーティングシステム用の Java のダウンロード"
- "IBM Java for AIX の場合"

- Linux または AIX ホストで Oracle データベースを実行している場合は、 SnapCenter Plug-in for Oracle Database と SnapCenter Plug-in for UNIX の両方をインストールする必要があります。

Plug-in for Oracle Database では、 SAP を対象とした Oracle データベースの管理も可能です。ただし、 SAP BR * Tools との統合はサポートされません。

- Oracle データベース 11.2.0.3 以降を使用している場合は、 13366202 Oracle パッチをインストールする必要があります。

/etc/fstab ファイル内の UUID マッピングは SnapCenter でサポートされません。

- プラグインのインストールには、デフォルトのシェルとして* bash *が必要です。

Linux ホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストが要件を満たしていることを確認する必要があります。

項目	要件
オペレーティングシステム	• Red Hat Enterprise Linux の場合 • Oracle Linux の場合 Oracle Linux または Red Hat Enterprise Linux 6.6 または 7.0 オペレーティングシステムの LVM で Oracle データベースを使用している場合は、最新バージョンの論理ボリュームマネージャ（ LVM ）をインストールする必要があります。 • SUSE Linux Enterprise Server （ SLES ）
ホスト上の SnapCenter プラグインの最小 RAM	1 GB

項目	要件
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	2 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Java 1.8.x（64ビット）のOracle JavaとOpenJDKのバージョン • Java 11（64ビット）のOracle JavaとOpenJDKのバージョン LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。 Java を最新バージョンにアップグレードした場合は、 /var/opt/snapcenter /etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Linux ホストの root 以外のユーザに sudo 権限を設定する

SnapCenter 2.0 以降のリリースでは、 root 以外のユーザが SnapCenter Plug-ins Package for Linux をインストールしてプラグインプロセスを開始できます。プラグインプロセスは、有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。

- 必要なもの *
- sudoバージョン1.8.7以降。
- /etc/ssh/sshd_config_file を編集して、メッセージ認証コードアルゴリズム MACs HMAC-sha2-256 および MACs HMAC-sha2-512 を設定します。

  構成ファイルを更新したら、 sshd サービスを再起動します。

  例

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

- このタスクについて *

次のパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。

- /home/*linux_user*/.sc_netapp / snapcenter_linux_host_plugin.bin
- /custom_location/NetApp/snapcenter /spl/installing/plugins/uninstall
- /custom_location/NetApp/snapcenter /spl/bin/spl になります
- 手順 *

1. SnapCenter Plug-ins Package for Linux をインストールする Linux ホストにログインします。
2. visudo Linux ユーティリティを使用して、 /etc/sudoers ファイルに次の行を追加します。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

RACセットアップを実行している場合は、他の許可されているコマンドとともに、/etc/sudoersファイルに次のように追加します。'/RAC/bin/olsnodes'<crs_home>

_crs_home_fileの値は、/etc/oracle/olr.loc_fileから取得できます。

_linux_user_は、作成したroot以外のユーザの名前です。

checksum_value_xは、_ C：\ProgramData\NetApp\SnapCenter \Package Repository_に ある* ORACLE_checksum.txt *ファイルから取得できます。

カスタムの場所を指定した場合、場所は _custom_path \NetApp\SnapCenter \Package Repository_に なります。

この例は、独自のデータを作成するための参照としてのみ使用してください。

AIX ホストの要件

SnapCenter Plug-ins Package for AIX をインストールする前に、ホストが要件を満たしていることを確認する必要があります。

SnapCenter Plug-ins Package for AIX に含まれている SnapCenter Plug-in for UNIX では、同時ボリュームグループはサポートされていません。

項目	要件
オペレーティングシステム	AIX 6.1以降
ホスト上の SnapCenter プラグインの最小 RAM	4 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	1 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Java 1.8.x（64ビット）IBM Java • Java 11（64ビット）IBM Java Java を最新バージョンにアップグレードした場合は、 /var/opt/snapcenter /etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

AIX ホストの root 以外のユーザに sudo 権限を設定します

SnapCenter 4.4 以降では、 root 以外のユーザが SnapCenter Plug-ins Package for AIX をインストールしてプラグインプロセスを開始できます。プラグインプロセスは、有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。

- 必要なもの *
- sudoバージョン1.8.7以降。
- /etc/ssh/sshd_config_file を編集して、メッセージ認証コードアルゴリズム MACs HMAC-sha2-256 および MACs HMAC-sha2-512 を設定します。

  構成ファイルを更新したら、 sshd サービスを再起動します。

  例

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

- このタスクについて *

次のパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。

- /home/*aix_user*//.sc_netapp /snapcenter aix_host_plugin.bsx
- /custom_location/NetApp/snapcenter /spl/installing/plugins/uninstall
- /custom_location/NetApp/snapcenter /spl/bin/spl になります
- 手順 *
  1. SnapCenter Plug-ins Package for AIX をインストールする AIX ホストにログインします。
  2. visudo Linux ユーティリティを使用して、 /etc/sudoers ファイルに次の行を追加します。

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

RACセットアップを実行している場合は、他の許可されているコマンドとともに、/etc/sudoersファイルに次のように追加します。'/RAC/bin/olsnodes'<crs_home>

_crs_home_fileの値は、/etc/oracle/olr.loc_fileから取得できます。

_aix_user_は 、作成した root 以外のユーザの名前です。

checksum_value_xは、_ C：\ProgramData\NetApp\SnapCenter \Package Repository_に ある* ORACLE_checksum.txt *ファイルから取得できます。

カスタムの場所を指定した場合、場所は _custom_path \NetApp\SnapCenter \Package Repository_に なります。

この例は、独自のデータを作成するための参照としてのみ使用してください。

クレデンシャルを設定する

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますLinux または AIX ホストにプラグインパッケージをインストールするためのクレデンシャルを作成する必要があります。

- このタスクについて *

このクレデンシャルは、 root ユーザに対して作成されるほか、プラグインプロセスをインストールして開始する sudo 権限がある root 以外のユーザに対しても作成されます。

詳細については、を参照してください Linux ホストの root 以外のユーザに sudo 権限を設定する または AIX ホストの root 以外のユーザに sudo 権限を設定します

* ベストプラクティス： * ホストを導入してプラグインをインストールしたあとでクレデンシャルを作成することは可能ですが、 SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* 資格情報] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [Credential] ページで、クレデンシャル情報を入力します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名 / パスワード	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者 SnapCenter プラグインをインストールするシステムのドメイン管理者を指定します。Username フィールドの有効な形式は次のとおりです。 ◦ NETBIOS_USERNAME_ ◦ _ ドメイン FQDN\ ユーザ名 _ • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Username フィールドの有効な形式は、*username* です
認証モード	使用する認証モードを選択します。 プラグインホストのオペレーティングシステムに応じて、 Linux または AIX のいずれかを選択します。
sudo 権限を使用する	root 以外のユーザのクレデンシャルを作成する場合は、「 * sudo 権限を使用する * 」チェックボックスをオンにします。

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、「 * User and Access * 」ページで、ユーザまたはユーザグループにク

レデンシャルのメンテナンスを割り当てることができます。

Oracle データベースのクレデンシャルを設定します

Oracle データベースに対してデータ保護処理を実行するために使用するクレデンシャルを設定する必要があります。

- このタスクについて *

Oracle データベースでサポートされているさまざまな認証方式を確認しておく必要があります。詳細については、を参照してください
"クレデンシャルの認証方式を指定します"。

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、ユーザ名に少なくともリソースグループとバックアップ権限が必要です。

Oracle データベース認証を有効にしている場合、リソースビューに赤い鍵のアイコンが表示されます。データベースを保護できるようにデータベースのクレデンシャルを設定するか、データベースをリソースグループに追加してデータ保護処理を実行する必要があります。

クレデンシャルの作成時に誤った詳細を指定すると、エラーメッセージが表示されます。[キャンセル] をクリックしてから、もう一度実行してください。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。
3. をクリックします をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。

   をクリックします をクリックしてフィルタペインを閉じます。

4. データベースを選択し、 * データベース設定 * > * データベースの設定 * をクリックします。
5. [データベース設定の設定] セクションの [既存の資格情報を使用する *] ドロップダウンリストから、Oracle データベースでデータ保護ジョブを実行するために使用する資格情報を選択します。

   Oracle ユーザには sysdba 権限が必要です。

   をクリックしてクレデンシャルを作成することもできます 。

6. ASM 設定の設定セクションの既存の認証情報を使用ドロップダウンリストから、 ASM インスタンスでデータ保護ジョブを実行するために使用する認証情報を選択します。

   ASM ユーザには SYSASM 権限が必要です。

   をクリックしてクレデンシャルを作成することもできます 。

7. [RMAN カタログ設定の構成] セクションの [既存のクレデンシャルを使用する *] ドロップダウンリストから、 Oracle Recovery Manager （ RMAN ）カタログデータベースでデータ保護ジョブを実行す

るために使用するクレデンシャルを選択します。

をクリックしてクレデンシャルを作成することもできます 。

TNSNAME フィールドに、 SnapCenter サーバーがデータベースとの通信に使用する透過ネットワーク印刷材 (TNS) ファイル名を入力します。

8. [* Preferred RAC Nodes] フィールドで、バックアップに優先する Real Application Cluster （ RAC ）ノードを指定します。

   優先ノードには、 RAC データベースインスタンスが存在するクラスタノードを 1 つまたはすべて指定できます。バックアップ処理は、指定したノードでのみ、指定した順序で実行されます。

   RAC One Node では、優先ノードにリストされるノードは 1 つだけで、この優先ノードはデータベースが現在ホストされているノードです。

   RAC One Node データベースのフェイルオーバーまたは再配置後に、 SnapCenter リソースページでリソースを更新すると、データベースが以前にホストされていた優先 RAC ノード * リストからホストが削除されます。データベースを再配置する RAC ノードは *RAC ノード * に表示され、手動で優先 RAC ノードとして設定する必要があります。

詳細については、を参照してください "RAC セットアップで優先ノードを指定します"。

1. [OK] をクリックします。

GUI を使用して、 Linux または AIX 用のホストを追加し、 Plug-ins Package をインストールします

ホストの追加ページを使用してホストを追加し、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールできます。プラグインは、自動的にリモートホストにインストールされます。

- このタスクについて *

ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。クラスタ（ Oracle RAC ）にプラグインをインストールする場合は、クラスタのすべてのノードにプラグインがインストールされている必要があります。Oracle RAC One Node の場合、このプラグインはアクティブノードとパッシブノードの両方にインストールする必要があります。

SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限があるロールが割り当てられている必要があります。

SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（ Add ）] をクリックします。

4. Hosts ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	ホストタイプとして「 * Linux * 」または「 * AIX * 」を選択します。 ホストが追加され、 Plug-in for Oracle Database と Plug-in for UNIX がホストにインストールされていない場合はインストールされます。 SnapCenter
ホスト名	ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • Oracle Real Application Clusters （ RAC ）環境内の任意のノード ⓘ ノード VIP や SCAN IP はサポートされていません SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。
クレデンシャル	作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 ⓘ クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。

6. （オプション） * その他のオプション * をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	デフォルトパスは、 _/opt/NetApp/snapcenter _ です。 必要に応じて、パスをカスタマイズできます。
Oracle RAC のすべてのホストを追加します	Oracle RAC のすべてのクラスタノードを追加するには、このチェックボックスを選択します。 Flex ASM セットアップでは、ハブノードとリーフノードのどちらであるかに関係なく、すべてのノードが追加されます。
オプションのプレインストールチェックを省略します	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。

7. [Submit （送信）] をクリックします。

[事前確認をスキップする] チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。

ファイアウォールの拒否ルールで指定されているプラグインポートのファイアウォールステータスは、事前確認スクリプトで検証されません。

最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。エラーがディスクスペースまたは RAM に関連している場合は、 *C ： \Program Files\NetApp\Virtual \SnapCenter WebApp* にある web.config ファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連する場合は、問題を修正する必要があります。

HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. 指紋を確認し、 * 確認して送信 * をクリックします。

   クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。

   SnapCenter は ECDSA アルゴリズムをサポートしていません。

   同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

1. インストールの進行状況を監視します。

   インストール固有のログファイルは、 _ / custom_location / snapcenter / log_ にあります。

- 結果 *

ホスト上のすべてのデータベースが自動的に検出され、リソースページに表示されます。何も表示されない場合は、 * リソースを更新 * をクリックします。

インストールステータスを監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
   a. [* フィルタ * （ Filter * ）] をクリック
   b. オプション：開始日と終了日を指定します。
   c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。

d. Status ドロップダウンメニューから、インストールステータスを選択します。

e. [適用（ Apply ）] をクリックします。

4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

Linux または AIX 用のプラグインパッケージをインストールする別の方法

コマンドレットまたはCLIを使用して、LinuxまたはAIX用のPlug-ins Packageを手動でインストールすることもできます。

プラグインを手動でインストールする前に、_ C：\ProgramData\NetApp\SnapCenter \Package Repository_にあるキー* snapcenter public_key.pub と snapcenter _ linux_host_plugin.bin .sig *を使用して、バイナリパッケージの署名を検証する必要があります。

プラグインをインストールするホストに* OpenSSL 1.0.2G*がインストールされていることを確認します。

次のコマンドを実行して、バイナリパッケージの署名を検証します。

- Linuxホストの場合： `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- AIXホストの場合： `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

コマンドレットを使用して複数のリモートホストにインストールします

Linux 用 SnapCenter Plug-ins Package または SnapCenter Plug-ins Package for AIX を複数のホストにインストールするには、 _ Install -SmHostPackage_PowerShell コマンドレットを使用する必要があります。

- 必要なもの *

プラグインパッケージをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインする必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 _Open-SmConnection_cmdlet を使用してセッションを確立し、クレデンシャルを入力します。
3. _ Install -SmHostPackage_cmdlet と、必要なパラメータを使用して、 Linux または SnapCenter Plug-in Package for AIX をインストール SnapCenter します。

   プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、 -skipprecheck _ オプションを使用できます。

ファイアウォールの拒否ルールで指定されているプラグインポートのファイアウォールステータスは、事前確認スクリプトで検証されません。

1. リモートインストールのクレデンシャルを入力します。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

クラスタホストにをインストールします

クラスタホストの両方のノードに、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールする必要があります。

クラスタホストの各ノードには 2 つの IP があります。IP の 1 つが各ノードのパブリック IP で、 2 つ目の IP が両方のノードで共有されるクラスタ IP になります。

- 手順 *

1. クラスタホストの両方のノードに、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールします。
2. SNAPCENTER_server_host 、 SPL_PORT 、 SNAPCENTER_server_port 、および SPL_enabled_plugins パラメータの正しい値が、 /var/opt/snapcenter /spl/etc/_ にある spl.properties ファイルで指定されていることを確認します。

   spl.properties で SPL_enabled_plugins が指定されていない場合は、 SPL_enabled_plugins を追加して値 sco 、 SCU を割り当てることができます。

3. SnapCenter サーバホストで、 _Open-SmConnection_cmdlet を使用してセッションを確立し、クレデンシャルを入力します。
4. 各ノードで、 _Set-PreferredHostIPsInStorageExportPolicy_sccli コマンドおよび必要なパラメータを使用して、ノードの優先 IP を設定します。
5. SnapCenter サーバホストで、クラスタ IP のエントリと、対応する DNS 名を _C ： \Windows\System32\drivers\etc\hosts_に 追加します。
6. ホスト名に対応するクラスタ IP を指定して、 _Add-SmHost_cmdlet を使用して SnapCenter サーバにノードを追加します。

ノード 1 で Oracle データベースを検出し（クラスタ IP がノード 1 でホストされていることが前提）、データベースのバックアップを作成します。フェイルオーバーが発生した場合は、ノード 1 に作成されたバックアップを使用して、ノード 2 のデータベースをリストアできます。ノード 1 に作成したバックアップを使用して、ノード 2 にクローンを作成することもできます。

他の SnapCenter 処理の実行中にフェイルオーバーが発生すると、古いボリューム、ディレクトリ、およびロックファイルが存在します。

Linux用の**Plug-ins Package**をサイレントモードでインストールします

コマンドラインインターフェイス（CLI）を使用して、SnapCenter Plug-ins Package for Linuxをサイレントモードでインストールできます。

- 必要なもの *
- プラグインパッケージをインストールするための前提条件を確認しておく必要があります。
- DISPLAY 環境変数が設定されていないことを確認する必要があります。

  DISPLAY 環境変数が設定されている場合は、 UNSET DISPLAY を実行してから、プラグインを手動でインストールする必要があります。

- このタスクについて *

コンソールモードでのインストール中に必要なインストール情報を指定する必要がありますが、サイレントモードでのインストールでは、インストール情報を指定する必要はありません。

- 手順 *

1. SnapCenter Plug-ins Package for Linux を SnapCenter Server のインストール場所からダウンロードします。

   デフォルトのインストールパスは、 _C ： \ProgramData\NetApp\SnapCenter \PackageRepository_です 。このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

2. コマンドプロンプトで、インストールファイルをダウンロードしたディレクトリに移動します。
3. を実行します

   ```
   ./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-
   DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
   DUSER_INSTALL_DIR==/opt/custom_path
   ```

4. /var/opt/snapcenter /spl/etc/__ にある spl.properties ファイルを編集して、 spl_enabled_plugins/SCO 、 SCU を追加し、 SnapCenter Plug-in Loader サービスを再起動します。

> プラグインパッケージのインストールでは、 SnapCenter サーバではなく、ホストにプラグインが登録されます。SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加し、 SnapCenter サーバにプラグインを登録します。ホストの追加中に、クレデンシャルとして [None] を選択します。ホストを追加すると、インストールしたプラグインが自動的に検出されます。

AIX 用プラグインパッケージをサイレントモードでインストールします

コマンドラインインターフェイス（ CLI ）を使用して、 SnapCenter Plug-ins Package for AIX をサイレントモードでインストールできます。

- 必要なもの *
- プラグインパッケージをインストールするための前提条件を確認しておく必要があります。
- DISPLAY 環境変数が設定されていないことを確認する必要があります。

  DISPLAY 環境変数が設定されている場合は、 UNSET DISPLAY を実行してから、プラグインを手動でインストールする必要があります。

- 手順 *

1. SnapCenter Server のインストール場所から、 SnapCenter Plug-ins Package for AIX をダウンロードします。

   デフォルトのインストールパスは、 _C ： \ProgramData\NetApp\SnapCenter \PackageRepository_です 。このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

2. コマンドプロンプトで、インストールファイルをダウンロードしたディレクトリに移動します。
3. を実行します

   ```
   ./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
   DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
   DUSER_INSTALL_DIR==/opt/custom_path-
   DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
   DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
   ```

4. /var/opt/snapcenter /spl/etc/__ にある spl.properties ファイルを編集して、 spl_enabled_plugins/SCO 、 SCU を追加し、 SnapCenter Plug-in Loader サービスを再起動します。

> プラグインパッケージのインストールでは、 SnapCenter サーバではなく、ホストにプラグインが登録されます。SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加し、 SnapCenter サーバにプラグインを登録します。ホストの追加中に、クレデンシャルとして [None] を選択します。ホストを追加すると、インストールしたプラグインが自動的に検出されます。

SnapCenter Plug-in Loader サービスを設定します

SnapCenter Plug-in Loader サービスは、 Linux または AIX 用のプラグインパッケージをロードして、 SnapCenter サーバーと通信します。SnapCenter Plug-in Loader サービスは、 Linux 用の SnapCenter Plug-ins Package または AIX 用 SnapCenter Plug-ins Package をインストールするとインストールされます。

- このタスクについて *

SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールすると、SnapCenter Plug-in Loader サービスが自動的に開始されます。SnapCenter Plug-in Loader サービスが自動的に開始されない場合は、次のことを行う必要があります。

- プラグインが動作しているディレクトリが削除されていないことを確認してください
- Java 仮想マシンに割り当てられているメモリ容量を増やします

spl.properties ファイルは、 */custom_location/NetApp/snapcenter /spl/etc/* にあり、次のパラメータを含みます。これらのパラメータにはデフォルト値が割り当てられています。

パラメータ名	説明
LOG_LEVEL の値	サポートされるログレベルを表示します。 指定可能な値は、 INFO 、 DEBUG 、 TRACE 、 ERROR 、 FATAL 、 警告を表示します。

パラメータ名	説明
SPL プロトコル	SnapCenter Plug-in Loader でサポートされているプロトコルを表示します。 HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
SNAPCENTER_server_protocol 」を参照してください	SnapCenter サーバでサポートされているプロトコルを表示します。 HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
ske_JAVAHOME_update を実行します	デフォルトでは、 SPL サービスは Java パスを検出し、 JAVA_HOME パラメータを更新します。 したがって、デフォルト値は FALSE に設定されます。デフォルトの動作を無効にして Java パスを手動で修正する場合は、 true に設定します。
SPL キーストアパス	キーストアファイルのパスワードを表示します。 この値は、パスワードを変更する場合や新しいキーストアファイルを作成する場合にのみ変更できます。
SPL ポート	SnapCenter Plug-in Loader サービスが実行されているポート番号を表示します。 デフォルト値がない場合は、値を追加できます。 プラグインのインストール後は値を変更しないでください。
SNAPCENTER_server_host が必要です	SnapCenter サーバの IP アドレスまたはホスト名を表示します。
SPL キーストアパス	キーストアファイルの絶対パスを表示します。
SNAPCENTER_SERVER_PORT	SnapCenter サーバが稼働しているポート番号を表示します。

パラメータ名	説明
logs_MAX_COUNT	SnapCenter Plug-in Loader ログファイルのうち、_/custom_location/snapcenter /spl/logs_folder に保持されているファイルの数を表示します。 デフォルト値は 5000 に設定されています。指定した値よりも多い数のファイルがある場合は、変更後の最新の 5000 個のファイルが保持されます。ファイル数のチェックは、 SnapCenter Plug-in Loader サービスが開始されたときから 24 時間ごとに自動的に行われます。 spl.properties ファイルを手動で削除すると、保持されるファイル数は 9999 に設定されます。
JAVA_HOME にアクセスします	SPL サービスの開始に使用される JAVA_HOME の絶対ディレクトリパスを表示します。 このパスは、インストール時および SPL の開始時に決定されます。
LOG_MAX_SIZE	ジョブログファイルの最大サイズを表示します。 最大サイズに達すると、ログファイルが圧縮され、そのジョブの新しいファイルにログが書き込まれます。
retain_logs_of _last_days	ログを保持する日数が表示されます。
enable_certificate_validationを実行します	ホストでCA証明書の検証が有効になっている場合はtrueと表示されます。 このパラメータを有効または無効にするには、spl.propertiesを編集するか、SnapCenter GUIまたはコマンドレットを使用します。

これらのパラメータのいずれかがデフォルト値に割り当てられていない場合、または値を割り当てたり変更したりする場合は、 spl.properties ファイルを変更します。また、 spl.properties ファイルを確認して編集し、パラメータに割り当てられている値に関連する問題のトラブルシューティングを行うこともできます。spl.properties ファイルを変更したら、 SnapCenter Plug-in Loader サービスを再起動する必要があります。

- 手順 *
  1. 必要に応じて、次のいずれかの操作を実行します。
     - root ユーザとして SnapCenter Plug-in Loader サービスを開始します。

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl start`
** SnapCenter Plug-in Loader サービスを停止します。
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```

stop コマンドに -force オプションを指定すると、 SnapCenter Plug-in Loader サービスを強制的に停止できます。ただし、既存の処理が終了するため、実行する前に十分に注意する必要があります。

- SnapCenter Plug-in Loader サービスを再起動します。

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
** SnapCenter Plug-in Loader サービスのステータスを確認します。
```

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl status`
** SnapCenter Plug-in Loader サービスで変更を探します。
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

Linux ホストに SnapCenter Plug-in Loader （ SPL ）サービスを使用して CA 証明書を設定します

インストールされているデジタル証明書をアクティブ化するには、SPLキーストアとその証明書のパスワードの管理、CA証明書の設定、ルート証明書または中間証明書のspl trust-storeへの設定、およびSnapCenter Plug-in Loaderサービスを使用したspl trust-storeへのCA署名キーペアの設定を行う必要があります。

SPL は、ファイル 'keystore.jkS' を使用します。このファイルは、 '/var/opt/snapcenter /spl/etc にあり、どちらもトラストストアおよびキーストアとして使用されます。

SPL キーストアのパスワードと使用中の CA 署名済みキーペアのエイリアスを管理します

- 手順 *

1. SPL プロパティファイルから SPL キーストアのデフォルトパスワードを取得できます。

   これはキー 'PL_keystore.pass' に対応する値です。

2. キーストアのパスワードを変更します。

```
 keytool -storepasswd -keystore keystore.jks
```
.
キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

spl.properties ファイル内のキー SPL の _keystore.pass に対しても同じ内容を更新します。

3. パスワードを変更したら、サービスを再起動してください。

SPL キーストアのパスワードと秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書を **SPL** の信頼ストアに設定します

SPL の信頼ストアへの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *
  1. SPL キーストアが格納されているフォルダ（ /var/opt/snapcenter /spl/etc_ ）に移動します。
  2. ファイル 'keystore.jkS' を探します。
  3. キーストアに追加された証明書を表示します。

```
 keytool -list -v -keystore keystore.jks
```
. ルート証明書または中間証明書を追加します。

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath>
-keystore keystore.jks
```
. SPL
の信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動します。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアを **SPL** の信頼ストアに設定します

CA 署名鍵ペアを SPL 信頼ストアに設定する必要があります。

- 手順 *
  1. SPL のキーストア /var/opt/snapcenter /spl/ などを含むフォルダに移動します
  2. ファイル 'keystore.jkS' を探します。

3. キーストアに追加された証明書を表示します。

```
 keytool -list -v -keystore keystore.jks
. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. キーストアに追加された証明書を表示します。
```

```
 keytool -list -v -keystore keystore.jks
. キーストアに、キーストアに追加された新しい CA
証明書に対応するエイリアスが含まれていることを確認します。
. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。
```

デフォルトの SPL キーストアパスワードは、 spl.properties ファイル内のキー SPL の keystore.pass の値です。

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"
-keystore keystore.jks
. CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「 *
」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. spl.properties ファイルにあるキーストアからエイリアス名を設定します。
```

この値をキー SPL の certificate_alias に更新します。

4. CA 署名済みキーペアを SPL 信頼ストアに設定したら、サービスを再起動します。

SPL の証明書失効リスト（ **CRL** ）を設定します

SPL 用に CRL を設定する必要があります

- このタスクについて *
- SPL は、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SPL の CRL ファイルのデフォルトディレクトリは、 _var/opt/snapcenter /spl/etc/crl_です 。
- 手順 *
  1. spl.properties ファイル内のデフォルトディレクトリを、キー SPL_CRL_PATH に対して変更および更新できます。

2. このディレクトリに複数の CRL ファイルを配置できます。

   着信証明書は各 CRL に対して検証されます。

プラグインの **CA** 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

SnapManager for Oracle および **SnapManager for SAP** から **SnapCenter** にデータをインポートします

SnapManager for Oracle および SnapManager for SAP から SnapCenter にデータをインポートすると、以前のバージョンのデータを引き続き使用することができます。

コマンドラインインターフェイス（ Linux ホストの CLI ）からインポートツールを実行して、 SnapManager for Oracle および SnapManager for SAP から SnapCenter にデータをインポートできます。

インポートツールを使用すると、 SnapCenter にポリシーとリソースグループが作成されます。SnapCenter で作成されるポリシーとリソースグループは、 SnapManager for Oracle および SnapManager for SAP のプロファイルとそれらのプロファイルを使用して実行される処理に対応しています。SnapCenter インポートツールでは、 SnapManager for Oracle および SnapManager for SAP のリポジトリデータベースとインポートするデータベースが処理されます。

- プロファイル、スケジュール、およびプロファイルを使用して実行される処理がすべて取得されます。
- 一意の処理ごと、およびプロファイルに関連付けられているスケジュールごとに、 SnapCenter バックアップポリシーを作成します。
- ターゲットデータベースごとにリソースグループを作成します。

インポートツールは、 /opt/NetApp/SnapCenter /spl/bin_ にある sc-migrate スクリプトを実行することによって実行できます。インポートするデータベースホストに Linux 用の SnapCenter Plug-ins パッケージをインストールすると、 sc-migrate スクリプトが */opt/NetApp/snapcenter / spl/bin* にコピーされます。

データのインポートは、 SnapCenter のグラフィカルユーザインターフェイス（ GUI ）ではサポートされていません。

SnapCenter では、 Data ONTAP 7-Mode はサポートされていません。7-Mode Transition Tool を使用して、 Data ONTAP 7-Mode を実行するシステムに格納されているデータと構成を ONTAP システムに移行できます。

データのインポートがサポートされる構成

SnapManager 3.4.x for Oracle および SnapManager 3.4.x for SAP から SnapCenter にデータをインポートする前に、 SnapCenter Plug-in for Oracle Database でサポートされる構成を確認しておく必要があります。

SnapCenter Plug-in for Oracle Database でサポートされる構成をに示します "NetApp Interoperability Matrix Tool で確認できます"。

データが **SnapCenter** にインポートされます

プロファイル、スケジュール、およびプロファイルを使用して実行される処理をインポートできます。

SnapManager for Oracle および **SnapManager for SAP** から入手できます	を **SnapCenter** に移動します
処理とスケジュールが設定されていないプロファイル	ポリシーは、デフォルトのバックアップタイプを「 Online 」、バックアップスコープを「 Full 」に設定して作成されます。
1 つ以上の処理が設定されたプロファイル	プロファイルとそのプロファイルを使用して実行される処理の一意の組み合わせに基づいて複数のポリシーが作成されます。 SnapCenter で作成されるポリシーには、プロファイルおよび対応する処理から取得されたアーカイブ・ログの削除および保持の詳細が含まれます。

SnapManager for Oracle および **SnapManager for SAP** から入手できます	を **SnapCenter** に移動します
Oracle Recovery Manager （ RMAN ）の設定を含むプロファイル	Oracle Recovery Manager * オプションを有効にした場合、 * Catalog backup でポリシーが作成されます。 SnapManager で外部 RMAN のカタログ化を使用していた場合は、 SnapCenter で RMAN カタログの設定を行う必要があります。既存のクレデンシャルを選択するか、新しいクレデンシャルを作成できます。 SnapManager で制御ファイルを使用して RMAN を設定した場合は、 SnapCenter で RMAN を設定する必要はありません。
プロファイルに関連付けられたスケジュール	スケジュールに対してのみポリシーが作成されます。
データベース	インポートしたデータベースごとにリソースグループが作成されます。 Real Application Clusters （ RAC ）セットアップでは、インポート後にインポートツールを実行したノードが優先ノードになり、そのノードに対してリソースグループが作成されます。

プロファイルをインポートすると、バックアップポリシーと一緒に検証ポリシーが作成されます。

SnapManager for Oracle および SnapManager for SAP のプロファイル、スケジュール、およびプロファイルを使用して実行されるすべての処理を SnapCenter にインポートすると、異なるパラメータの値もインポートされます。

SnapManager for Oracle および **SnapManager for SAP** のパラメータと値	**SnapCenter** のパラメータと値	注：
バックアップの範囲 • フル • データ • ログ	バックアップの範囲 • フル • データ • ログ	

SnapManager for Oracle および **SnapManager for SAP** のパラメータと値	**SnapCenter** のパラメータと値	注：
バックアップモード • 自動 • オンライン • オフラインです	バックアップタイプ • オンライン • オフラインシャットダウン	バックアップモードが自動の場合、インポートツールは処理の実行時にデータベースの状態を確認し、バックアップタイプをオンラインまたはオフラインシャットダウンに適切に設定します。
保持 • 日 • カウント	保持 • 日 • カウント	SnapManager for Oracle および SnapManager for SAP では ' 日数とカウントの両方を使用して保存期間を設定します SnapCenter には、 days_or_Counts があります。したがって、 SnapManager for Oracle と SnapManager for SAP で個数よりも日数が優先されることから、日数に基づいて保持が設定されます。
スケジュールのプルーニング • すべて • システム変更番号（ SCN ） • 日付 • 指定した時間、日、週、および月よりも前に作成されたログです	スケジュールのプルーニング • すべて • 指定した時間および日数より前に作成されたログです	SnapCenter は、 SCN 、日付、週、および月に基づくプルーニングをサポートしていません。
通知 • 成功した処理のためにのみ送信される E メールです • 処理に失敗した場合にのみ送信される E メールです • 処理の成功と失敗の両方について送信される E メールです	通知 • 常に • 失敗した場合 • 警告 • エラー	E メール通知はインポートされます。 ただし、 SnapCenter GUI を使用して SMTP サーバを手動で更新する必要があります。E メールの件名は、設定できるように空白になります。

SnapCenter にインポートされないデータ

インポートツールは、すべてのデータを SnapCenter にインポートするわけではありません。

次のものを SnapCenter にインポートすることはできません。

- バックアップメタデータ
- パーシャル・バックアップ
- raw デバイスマッピング（ RDM ）および Virtual Storage Console （ VSC ）関連のバックアップ
- SnapManager for Oracle および SnapManager for SAP のリポジトリで使用可能なロールとクレデンシャル
- 検証、リストア、クローニングの処理に関するデータ
- 処理の削除
- SnapManager for Oracle および SnapManager for SAP のプロファイルで指定されたレプリケーションの詳細

  インポートの完了後に、 SnapCenter で作成した対応するポリシーを手動で編集してレプリケーションの詳細を含める必要があります。

- カタログ化されたバックアップの情報

データをインポートする準備をします

SnapCenter へのデータのインポート処理を正常に実行するには、データをインポートする前に特定のタスクを実行する必要があります。

- 手順 *

1. インポートするデータベースを特定します。
2. SnapCenter を使用して、データベースホストを追加し、 SnapCenter Plug-ins Package for Linux をインストールします。
3. SnapCenter を使用して、ホスト上のデータベースで使用される Storage Virtual Machine （ SVM ）の接続を設定します。
4. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
5. リソースページで、インポートするデータベースが検出されて表示されていることを確認します。

   インポートツールを実行する場合は、データベースにアクセスできる必要があります。アクセスできないと、リソースグループの作成が失敗します。

   データベースにクレデンシャルが設定されている場合は、 SnapCenter で対応するクレデンシャルを作成し、そのクレデンシャルをデータベースに割り当ててから、データベースの検出を再度実行する必要があります。データベースが Automatic Storage Management （ ASM ）にある場合は、 ASM インスタンスのクレデンシャルを作成し、そのクレデンシャルをデータベースに割り当てる必要があります。

6. インポートツールを実行 SnapManager するユーザに、 SnapManager for Oracle または SnapManager for SAP ホストから Oracle for Oracle または SnapManager for SAP CLI コマンド（スケジュールを一時停止するコマンドなど）を実行するための十分な権限があることを確認します。
7. SnapManager for Oracle または SnapManager for SAP ホストで次のコマンドを実行して、スケジュールを一時停止します。
   a. SnapManager for Oracle ホストでスケジュールを一時停止する場合は、次のコマンドを実行します。

- `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smo credential set -profile -name profile_name`

> smo credential set コマンドは、ホストのプロファイルごとに実行する必要があります。

b. SnapManager for SAP ホストでスケジュールを一時停止する場合は、次のコマンドを実行します。

- `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smsap credential set -profile -name profile_name`

> SMSAP のクレデンシャルセットコマンドは、ホストの各プロファイルに対して実行する必要があります。

1. hostname-f を実行するときに、データベースホストの Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）が表示されることを確認します

   FQDN が表示されない場合は、 /etc/hosts を変更してホストの FQDN を指定する必要があります。

データをインポートする

データベースホストからインポートツールを実行して、データをインポートできます。

- このタスクについて *

インポート後に作成される SnapCenter バックアップポリシーの名前の形式は、次のとおりです。

- 処理とスケジュールが設定されていないプロファイルに対して作成されたポリシーの場合、 sm_created 形式は「 sm_created 」です。

  プロファイルを使用して処理を実行しない場合は、対応するポリシーが作成され、デフォルトのバックアップタイプは online 、バックアップスコープは full になります。

- 1 つ以上の操作を持つプロファイルに対して作成されたポリシーには、 SM_profileName_BACKUPMODE_BACKUPSCOPE_Migrated 形式があります。
- プロファイルに関連付けられたスケジュールに対して作成されたポリシーは、 SM_profileName_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_Migrated 形式です。
- 手順 *

1. インポートするデータベースホストにログインします。
2. /opt/NetApp/SnapCenter /spl/bin_ にある sc-migrate スクリプトを実行して、インポートツールを実行します。
3. SnapCenter サーバのユーザ名とパスワードを入力します。

   クレデンシャルの検証後、 SnapCenter との接続が確立されます。

4. SnapManager for Oracle または SnapManager for SAP のリポジトリデータベースの詳細を入力します。

   リポジトリデータベースのホストで使用できるデータベースが表示されます。

5. ターゲットデータベースの詳細を入力します。

   ホスト上のすべてのデータベースをインポートする場合は、「 all 」と入力します。

6. 処理に失敗した場合のシステムログの生成や ASUP メッセージの送信を有効にする場合は、 _Add-SmStorageConnection_or_Set-SmStorageConnection_command を実行して有効にする必要があります。

   インポート処理をキャンセルする場合は、インポートツールの実行中またはインポートの完了後に、インポート処理で作成された SnapCenter ポリシー、クレデンシャル、およびリソースグループを手動で削除する必要があります。

- 結果 *

プロファイル、スケジュール、およびプロファイルを使用して実行される処理に対応した SnapCenter バックアップポリシーが作成されます。各ターゲットデータベースのリソースグループも作成されます。

データのインポートが正常に完了すると、 SnapManager for Oracle および SnapManager for SAP で、インポートしたデータベースに関連付けられたスケジュールが一時停止されます。

インポートの完了後は、 SnapCenter を使用してインポートしたデータベースまたはファイルシステムを管理する必要があります。

インポートツールを実行するたびに、 spl_migration_timestamp.log という名前の _/var/opt/snapcenter /spl/logs_directory にログが格納されます。このログを参照して、インポートエラーを確認し、トラブルシューティングを行うことができます。

SnapCenter Plug-in for VMware vSphere をインストール

データベースが仮想マシン（ VM ）に格納されている場合や VM とデータストアを保護する場合は、 SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください "導入の概要"。

CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください "SSL 証明書を作成またはインポートします"。

CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere は、事前に設定されたディレクトリ内の CRL ファイルを検索します。VMware vSphere 用 SnapCenter プラグインの CRL ファイルのデフォルトディレクトリは、_/opt/NetApp/config/crl_です 。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

Oracle データベースの保護を準備する

バックアップ、クローニング、リストアなどのデータ保護処理を実行する場合は、事前に戦略を定義し、環境をセットアップする必要があります。また、 SnapVault サーバで SnapMirror テクノロジと SnapCenter テクノロジを使用するように設定することもできます。

SnapVault テクノロジと SnapMirror テクノロジを活用するには、ストレージデバイス上のソースボリュームとデスティネーションボリューム間のデータ保護関係を設定して初期化する必要があります。これらのタスクを実行するには、 NetAppSystem Manager を使用するか、ストレージコンソールのコマンドラインを使用します。

Plug-in for Oracle Database を使用する前に、 SnapCenter 管理者が SnapCenter Server のインストールと設定を行い、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。 "詳細はこちら。"
- ストレージシステム接続を追加して SnapCenter 環境を設定します。 "詳細はこちら。"

> SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SVM 登録またはクラスタ登録を使用して SnapCenter に登録する SVM は、それぞれ一意である必要があります。

- インストールユーザ用に、認証モードを Linux または AIX に設定してクレデンシャルを作成します。 "詳細はこちら。"
- ホストを追加し、プラグインをインストールし、リソースを検出します。
- VMware RDM LUN または VMDK に存在する Oracle データベースを SnapCenter Server で保護する場合は、 SnapCenter Plug-in for VMware vSphere を導入して、 SnapCenter にプラグインを登録する必要があります。
- Linux または AIX ホストに Java をインストールします。

  を参照してください "Linux ホストの要件" または "AIXホストの要件" を参照してください。

- アプリケーションファイアウォールのタイムアウト値は 3 時間以上に設定する必要があります。
- NFS 環境で Oracle データベースを使用している場合は、マウント、クローニング、検証、リストアの各処理を実行できるように、プライマリストレージまたはセカンダリストレージ用に少なくとも 1 つの

NFS データ LIF を設定しておく必要があります。

- データパス（ LIF ）が複数ある場合、または dNFS 構成を使用している場合は、データベースホストで SnapCenter CLI を使用して次の作業を実行できます。
  - デフォルトでは、データベースホストのすべての IP アドレスが、クローンボリュームの Storage Virtual Machine （ SVM ）の NFS ストレージエクスポートポリシーに追加されます。特定の IP アドレスを使用する場合、または IP アドレスのサブセットに制限する場合は、 Set-PreferredHostIPsInStorageExportPolicy CLI を実行します。
  - SVM に複数のデータパス（ LIF ）がある場合は、 NFS クローンボリュームをマウントするための適切なデータパス（ LIF ）が SnapCenter によって選択されます。ただし、特定のデータパス（ LIF ）を指定する場合は、 Set-SvmPreferredDataPath CLI を実行する必要があります。
    詳細については、コマンドリファレンスガイドを参照してください。
- SAN 環境で Oracle データベースを使用している場合は、次のガイドに記載された推奨事項に従って SAN 環境が設定されていることを確認してください。
  - "Linux Unified Host Utilities の推奨されるホスト設定"
  - "Using Linux Hosts with ONTAP storage"
  - "AIX Host Utilities の影響を受けるホスト設定"
- Oracle Linux または RHEL オペレーティングシステムの LVM で Oracle データベースを使用している場合は、最新バージョンの論理ボリューム管理（ LVM ）をインストールします。
- SnapManager for Oracle を使用していて、 SnapCenter Plug-in for Oracle Database に移行する場合は、 sccli コマンド sc-migrate を使用して、プロファイルを SnapCenter のポリシーおよびリソースグループに移行できます。
- バックアップレプリケーションが必要である場合は、 ONTAP で SnapMirror と SnapVault を設定します

SnapCenter 4.1.1 ユーザの場合、 SnapCenter Plug-in for VMware vSphere 4.1.1 のドキュメントには、仮想化されたデータベースとファイルシステムの保護に関する情報が記載されています。SnapCenter 4.2.x ユーザの場合、 NetApp Data Broker 1.0 および 1.0.1 のドキュメントでは、 Linux ベースの NetApp Data Broker 仮想アプライアンス（オープン仮想アプライアンス形式）が提供する SnapCenter Plug-in for VMware vSphere を使用して、仮想化されたデータベースとファイルシステムを保護する方法について説明しています。SnapCenter 4.3.x を使用する場合は、 Linux ベースの SnapCenter Plug-in for VMware vSphere 仮想アプライアンス（オープン仮想アプライアンス形式）を使用して仮想化されたデータベースとファイルシステムを保護する方法について、 SnapCenter Plug-in for VMware vSphere 4.3 のドキュメントを参照してください。

- 詳細はこちら *
- "Interoperability Matrix Tool で確認してください"
- "SnapCenter Plug-in for VMware vSphere のドキュメント"
- "RHEL 7 以降の非マルチパス環境でデータ保護処理が失敗する"

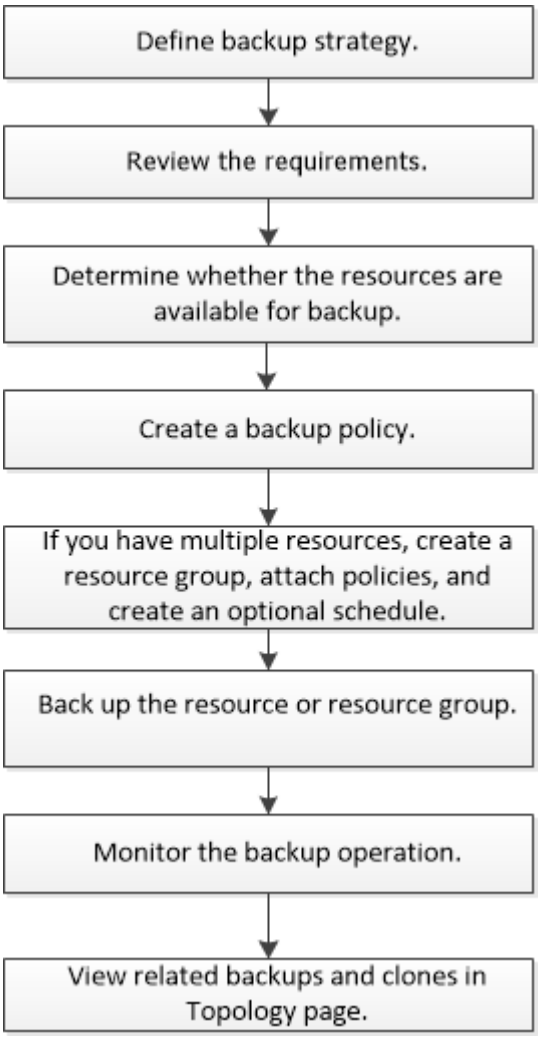
Oracle データベースをバックアップする

バックアップ手順 の概要

リソース（データベース）またはリソースグループのバックアップを作成することができます。バックアップ手順 には、計画、バックアップするリソースの特定、バックアップポリシーの作成、リソースグループの作成とポリシーの適用、バックアップの作成、

処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



Oracleデータベースのバックアップを作成する際に、データベースで複数の処理が実行されないように、Oracleデータベースホスト上の_/var/opt/snapcenter/sco/lockディレクトリに処理ロックファイル（*.SM_lock_dbsid*）が作成されます。処理ロックファイルは、データベースのバックアップが完了すると自動的に削除されます。

ただし、前回のバックアップが警告付きで完了していた場合、処理ロックファイルが削除されず、次回のバックアップ処理が待機キューに登録される可能性があります。*.SM_LOCK_dbsid * ファイルが削除されていない場合、このファイルは最終的にはキャンセルされる可能性があります。このような場合は、次の手順を実行して処理ロックファイルを手動で削除する必要があります。

1. コマンドプロンプトで、_/var/opt/snapcenter/sco/lockに移動します。
2. 処理ロックを削除します。`rm -rf .sm_lock_dbsid.`

構成情報をバックアップします

バックアップ対象としてサポートされる **Oracle** データベース構成

SnapCenter では、各種の Oracle データベース構成のバックアップがサポートされま

す。

- Oracle スタンドアロン構成
- Oracle Real Application Clusters （ RAC ）
- Oracle スタンドアロンレガシーです
- Oracle スタンドアロンコンテナデータベース（ CDB ）
- Oracle Data Guard スタンバイ

  Data Guard スタンバイデータベースのオフラインマウントバックアップだけを作成できます。オフラインシャットダウンバックアップ、アーカイブログのみのバックアップ、およびフルバックアップはサポートされていません。

- Oracle Active Data Guard スタンバイ

  Active Data Guard スタンバイデータベースのオンラインバックアップだけを作成できます。アーカイブログのみのバックアップとフルバックアップはサポートされていません。

  Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースのバックアップを作成する前に、管理されたリカバリプロセス（ MRP ）が停止し、バックアップが作成されたあとに MRP が開始されます。

- Automatic Storage Management （ ASM ；自動ストレージ管理）
  - 仮想マシンディスク（ VMDK ）上の ASM スタンドアロンおよび ASM RAC

    Oracle データベースでサポートされるどのリストア方式でも、 VMDK 上で実行できるのは ASM RAC データベースの Connect and Copy リストアだけです。

  - ASMスタンドアロンおよびASM RAC on Raw Device Mapping（RDM）
    [+]
    ASM上のOracleデータベースに対するバックアップ、リストア、クローニングの処理は、ASMLibの有無に関係なく実行できます。
  - Oracle ASM フィルタドライバ (ASMFD)

    PDB 移行処理と PDB クローニング処理はサポートされていません。

  - Oracle Flex ASM

サポートされている Oracle のバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Oracle データベースでサポートされるバックアップのタイプ

バックアップタイプでは、作成するバックアップのタイプを指定します。SnapCenter では、 Oracle データベースに対してオンラインバックアップタイプとオフラインバックアップタイプがサポートされます。

オンラインバックアップ

データベースがオンライン状態のときに作成されるバックアップを、オンラインバックアップと呼びます。ホ

ットバックアップとも呼ばれるオンラインバックアップでは、データベースをシャットダウンすることなくバックアップを作成できます。

オンラインバックアップでは、次のファイルのバックアップを作成できます。

- データ・ファイルと制御ファイルのみ
- アーカイブログファイルのみ（この場合はデータベースがバックアップモードになりません）
- データ・ファイル、制御ファイル、およびアーカイブ・ログ・ファイルを含むフル・データベース

オフラインバックアップ

データベースがマウント済み状態またはシャットダウン状態のときに作成されるバックアップを、オフラインバックアップと呼びます。オフラインバックアップはコールドバックアップとも呼ばれます。オフラインバックアップに含めることができるのは、データファイルと制御ファイルだけです。オフラインマウントバックアップまたはオフラインシャットダウンバックアップのいずれかを作成できます。

- オフラインマウントバックアップを作成する場合は、データベースがマウント済み状態であることを確認する必要があります。

  データベースがそれ以外の状態の場合は、バックアップ処理が失敗します。

- オフラインシャットダウンバックアップを作成する場合、データベースはどの状態でもかまいません。

  データベースは、バックアップを作成するために必要な状態に変更されます。バックアップが作成されると、データベースは元の状態に戻ります。

SnapCenter による **Oracle** データベースの検出方法

リソースとは、SnapCenter で管理されるホスト上のOracleデータベースです。使用可能なデータベースを検出したあとに、それらのデータベースをリソースグループに追加してデータ保護処理を実行できます。

次のセクションでは、SnapCenter がさまざまなタイプおよびバージョンのOracleデータベースを検出するために使用するプロセスについて説明します。

Oracle バージョン **11___** ～ **12_c_R1**

RACデータベース

RACデータベースは、/etc/oratab`エントリに基づいてのみ検出されます。/etc/oratab ファイル内にデータベース・エントリが必要です。

スタンドアロン

スタンドアロンデータベースは、/etc/oratabエントリに基づいてのみ検出されます。

ASM

ASMインスタンスエントリが/etc/oratabファイルにある必要があります。

RAC 1ノード

RAC One Nodeデータベースは、/etc/oratabエントリに基づいてのみ検出されます。
データベースがnomount、mount、またはopenのいずれかの状態である必要があります。/etc/oratab ファイル

内にデータベース・エントリが必要です。

データベースがすでに検出され、バックアップが関連付けられている場合、 RAC One Node データベースのステータスは「 Renamed 」または「 deleted 」とマークされます。

データベースを再配置する場合は、次の手順を実行する必要があります。

1. フェイルオーバーが発生した RAC ノードの /etc/oratab ファイルに、再配置されたデータベース・エントリを手動で追加します。
2. リソースを手動で更新する。
3. リソースページからRAC One Nodeデータベースを選択し、[データベース設定]をクリックします。
4. データベースを設定して、データベースを現在ホストしている RAC ノードに優先クラスタノードを設定します。
5. SnapCenter 処理を実行します。
6. あるノードから別のノードにデータベースを再配置し、以前のノードのoratabエントリが削除されていない場合は、同じデータベースが2回表示されないように、oratabエントリを手動で削除します。

Oracleバージョン**12cR2**～**18c**の場合

RACデータベース

RACデータベースはsrvctl configコマンドを使用して検出されます。
/etc/oratab ファイル内にデータベース・エントリが必要です。

スタンドアロン

スタンドアロンデータベースは、/etc/oratabファイルのエントリとsrvctl configコマンドの出力に基づいて検出されます。

ASM

ASMインスタンスエントリが/etc/oratabファイルに含まれている必要はありません。

RAC 1ノード

RAC One Nodeデータベースは、srvctl configコマンドのみを使用して検出されます。
データベースがnomount、mount、またはopenのいずれかの状態である必要があります。データベースがすでに検出され、バックアップが関連付けられている場合、 RAC One Node データベースのステータスは「 Renamed 」または「 deleted 」とマークされます。

データベースを再配置する場合は、次の手順を実行する必要があります。
。リソースを手動で更新する。
。リソースページからRAC One Nodeデータベースを選択し、[データベース設定]をクリックします。
。データベースを設定して、データベースを現在ホストしている RAC ノードに優先クラスタノードを設定します。
。SnapCenter 処理を実行します。

> /etc/oratab ファイル内に Oracle 12_c__R2 および 18_c_database のエントリがあり、同じデータベースが srvctl config コマンドで登録されている場合、 SnapCenter は重複するデータベースエントリを削除します。
> 古いデータベースエントリがある場合は、データベースは検出されますが、データベースにアクセスできず、ステータスはオフラインになります。

RAC セットアップで優先ノードを指定します

Oracle Real Application Clusters（RAC）セットアップでは、SnapCenterがバックアップ処理の実行に使用する優先ノードを指定できます。優先ノードを指定しない場合は、SnapCenter によって自動的に優先ノードが割り当てられ、そのノードにバックアップが作成されます。

優先ノードには、 RAC データベースインスタンスが存在するクラスタノードを 1 つまたはすべて指定できます。バックアップ処理は、これらの優先ノードで優先順にトリガーされます。

例

RACデータベースcdbracには3つのインスタンスがあります。cdbrac1はnode1に、cdbrac2はnode2に、cdbrac3はnode3にあります。

node1 インスタンスと node2 インスタンスが優先ノードとして設定され、 node2 に最初の優先順位、 node1 に 2 番目の優先順位が指定されます。バックアップ処理を実行すると、まず第 1 優先ノードである node2 で処理が試行されます。

node2 がバックアップの状態になっていない場合は、プラグインエージェントがホストで実行されていないなどの複数の理由で、ホスト上のデータベースインスタンスが指定したバックアップタイプに必要な状態になっていない可能性があります。 または、 FlexASM 構成内の node2 上のデータベースインスタンスがローカル ASM インスタンスで提供されていない場合は、 node1 で処理が試行されます。

node3 は、優先ノードのリストに含まれていないため、バックアップには使用されません。

Flex ASMセットアップ

Flex ASM 設定では、カード濃度が RAC クラスタ内のノード数より少ない場合、リーフノードは優先ノードとして表示されません。Flex ASM クラスタノードのロールに変更がある場合は、優先ノードが更新されるように、手動で検出する必要があります。

必要なデータベースの状態

バックアップを正常に完了するには、優先ノード上の RAC データベースインスタンスが必要な状態であることが必要です。

- オンラインバックアップを作成する場合は、設定された優先ノードの RAC データベースインスタンスの 1 つがオープン状態であることが必要です。
- オフラインマウントバックアップを作成する場合は、設定された優先ノードの RAC データベースインスタンスの 1 つがマウント状態であり、かつ他の優先ノードを含むその他すべてのインスタンスがマウント状態またはそれより低いレベルの状態であることが必要です。
- オフラインシャットダウンバックアップを作成する場合は、 RAC データベースインスタンスはどの状態でもかまいませんが、優先ノードを指定する必要があります。

Oracle Recovery Manager を使用してバックアップをカタログ化する方法

Oracle Recovery Manager（RMAN）を使用してOracleデータベースのバックアップをカタログ化し、Oracle RMANリポジトリにバックアップ情報を格納できます。

カタログ化されたバックアップは、あとでブロックレベルのリストア処理や表領域のポイントインタイムリカ

バリ処理に使用できます。カタログ化されたバックアップが不要となった場合は、カタログ情報を削除できます。

カタログ化するためには、データベースの状態が少なくともマウント済み状態であることが必要です。カタログ化を実行できるのは、データバックアップ、アーカイブログバックアップ、およびフルバックアップです。複数のデータベースを含むリソースグループのバックアップに対してカタログ化を有効にすると、データベースごとにカタログ化が実行されます。Oracle RAC データベースの場合は、データベースが少なくともマウント済み状態にある優先ノードでカタログ化が実行されます。

RAC データベースのバックアップをカタログ化する場合は、そのデータベースに対して他のジョブが実行されていないことを確認します。別のジョブが実行されている場合は、カタログ化処理がキューに登録されずに失敗します。

外部カタログデータベース

デフォルトでは、ターゲットデータベースの制御ファイルがカタログ化に使用されます。外部カタログデータベースを追加する場合は、 SnapCenter グラフィカルユーザーインタフェース（ GUI ）のデータベース設定ウィザードを使用して、外部カタログの資格情報と透過ネットワーク印刷材（ TNS ）名を指定して構成できます。CLI から外部カタログデータベースを設定するには、 Configure-SmOracleDatabase コマンドで -OracleRmanCatalogCredentialName オプションおよび -OracleRmanCatalogTnsName オプションを実行します。

RMANコマンド

SnapCenter GUI から Oracle バックアップポリシーを作成する際にカタログ化オプションを有効にした場合は、バックアップ処理の一環として Oracle RMAN を使用してバックアップがカタログ化されます。を実行して、バックアップのカタログ化を遅らせて実行することもできます `Catalog-SmBackupWithOracleRMAN` コマンドを実行します

バックアップをカタログ化したら、を実行できます `Get-SmBackupDetails` コマンドを使用して、カタログ化されたバックアップの情報（カタログ化されたデータファイルのタグ、制御ファイルのカタログパス、カタログ化されたアーカイブログの場所など）を取得します。

命名形式

SnapCenter 3.0 では、 ASM ディスクグループ名が 16 文字以上である場合、バックアップに使用される命名形式は SC_HASHCODEofDISKGROUP_DBSID_backupid です。ただし、ディスク・グループ名が 16 文字未満の場合、バックアップに使用される命名形式は DISKGROUPNAME_DBSID_backupid です。これは、 SnapCenter 2.0 で使用される形式と同じです。

HASHCODEofDISKGROUP は、各 ASM ディスクグループに固有の自動生成番号（ 2 ～ 10 桁）です。

クロスチェック処理

バックアップに関する RMAN リポジトリ情報が古くなってバックアップのリポジトリレコードがその物理ステータスと一致しなくなった場合は、クロスチェックを実行してリポジトリ情報を更新できます。たとえば、ユーザがオペレーティングシステムコマンドでディスクからアーカイブログを削除した場合、実際にはディスクにログがないにもかかわらず、制御ファイルにはディスクにログがあることが示されます。

クロスチェック処理では、制御ファイルを情報で更新できます。クロスチェックをイネーブルにするには、 Set-SmConfigSettings コマンドを実行して、 enable_croscHCK パラメータに値 true を割り当てます。デフォルト値は FALSE です。

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
```

```
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

カタログ情報を削除します

カタログ情報を削除するには、 Uncatalog-SmBackupWithOracleRMAN コマンドを実行します。SnapCenter GUI ではカタログ情報を削除できません。ただし、バックアップを削除するとき、またはカタログ化されたバックアップに関連する保持設定とリソースグループを削除するときに、カタログ化されたバックアップの情報も削除されます。

> SnapCenter ホストを強制的に削除する場合は、そのホストに関連するカタログ化されたバックアップの情報が削除されません。ホストを強制的に削除する場合は、事前にそのホストに関連するすべてのカタログ化されたバックアップの情報を削除しておく必要があります。

ORACLE_PLUGIN_RMAN_CATALE_TIMEOUT パラメータに指定されたタイムアウト値を超えたためにカタログ化とカタログ化解除が失敗した場合は、次のコマンドを実行して、パラメータの値を変更する必要があります。

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

パラメータの値を変更したら、次のコマンドを実行して SnapCenter Plug-in Loader （ SPL ）サービスを再起動します。

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

コマンドで使用できるパラメータとその説明に関する情報は、 Get-Help コマンド _name を実行して取得できます。または、を参照してください "SnapCenter ソフトウェアコマンドリファレンスガイド"。

バックアップ固有のプリスクリプトおよびポストスクリプト用の事前定義された環境変数

SnapCenter では、バックアップポリシーの作成時にプリスクリプトおよびポストスクリプトを実行する際に、事前定義された環境変数を使用できます。この機能は、 VMDK を除くすべての Oracle 構成でサポートされます。

SnapCenter は、シェルスクリプトが実行される環境で直接アクセス可能なパラメータの値を事前定義します。スクリプトの実行時にこれらのパラメータの値を手動で指定する必要はありません。

バックアップポリシーを作成するためにサポートされる事前定義された環境変数

- * sc_job_ID * は、処理のジョブ ID を指定します。

  例：256

- *SC_ORACLE_SID * はデータベースのシステム識別子を指定します

  複数のデータベースを処理する場合は、パラメータにパイプで区切られたデータベース名が含まれます。

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例： NFSB32 | NFSB31

- *sc_host * は、データベースのホスト名を指定します。

  RAC の場合、ホスト名はバックアップが実行されるホストの名前になります。

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例：scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** は、データベースのオペレーティング・システムの所有者を指定します。

  このデータは、 <db1><osuser1>|<db2><osuser2> の形式になります。

  例： NFSB31@Oracle|NFSB32@Oracle

- * SC_OS_GROUP * はデータベースのオペレーティング・システム・グループを指定します

  データは <db1><osgroup1><osgroup>|<db2>@<osgroup2> の形式で表示されます。

  例： NFSB31@ INSTALL | NFSB32@oinstall

- * SC_BACKUP _ TYPE * 」にはバックアップ・タイプ（オンライン・フル、オンライン・データ、オンライン・ログ、オフライン・シャットダウン、オフライン・マウント）を指定します。

  例

  - フルバックアップの場合： ONLINEFULL
  - データのみのバックアップ :ONLINEDATA
  - ログのみのバックアップ： ONLINELOG

- * SC_backup_name * はバックアップ名です

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例： DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1 | AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- * SC_BACKUP ID * にはバックアップ ID を指定します

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例： DATA @203 | LOG@205 | AV@207

- **SC_ORACLE_HOME** は Oracle ホーム・ディレクトリのパスを指定します

  例： NFSB32@ /ora01/app/oracle/product/18.1.0/db_1 | NFSB31@ /ora01/app/oracle/product/18.1.0/db_1

- * SC_BACKUP _retention-* はポリシーに定義されている保持期間です

  例

  - フルバックアップの場合：毎時 | データ @ 日数： 3 | log@ count ： 4
  - オンデマンドデータのみのバックアップの場合： OnDemand | data@ count ： 2

◦ オンデマンドログのみのバックアップの場合： OnDemand | log@count ： 2

- * sc_resource_group_name * で、リソースグループの名前を指定します。

  例：RG1

- * SC_BACKUP _policy_name * はバックアップ・ポリシーの名前です

  例： backup_policy

- * sc_av_name * は、アプリケーション・ボリュームの名前を指定します。

  例： AV1|AV2

- * SC_primary_data_volume_full_path * は、データファイルディレクトリに対する SVM からボリュームへのストレージマッピングを指定します。LUN と qtree の親ボリュームの名前になります。

  データの形式は、 <db1 >@<SVM1 ： volume1 >|<db2 >@<SVM2 ： volume2> となります。

  例

  ◦ 同じリソースグループ内の 2 つのデータベース： NFSB32@buck ： /vol/scspr2417819002_NFS_CDB_NFSB32_DATA | NFSB31@buck ： /vol/scspr2417819002_NFS_CDB_NFSB31_DATA

  ◦ データファイルが複数のボリュームに分散されている単一のデータベースの場合： buck ： /vol/scspro2417819002_nfs_cdb31_data 、 herculus ： /vol/scspr2417819002_nfs

- * SC_primary_archivelogs_volume_full_path * は、ログファイルディレクトリに対する SVM のボリュームへのストレージマッピングを指定します。LUN と qtree の親ボリュームの名前になります。

  例

  ◦ 単一データベースインスタンスの場合： buck ： /vol/scspr2417819002_NFS_CDB_NFSB31_redo

  ◦ 複数のデータベースインスタンスの場合： NFSB31@ バック： /vol/scspr2417819002_NFS_CDB_NFSB31_redo | NFSB32@ バック： /vol/scspr2417819002_NFS_CDB_NFSB32_redo

- * SC_primary_full_snapshot_name_for_tag * は、ストレージ・システム名とボリューム名を含む Snapshot のリストを指定します。

  例

  ◦ 単一データベースインスタンスの場合： buck ： /vol/scspr2417819002_nfs_cdb_NFSB32_data/Rg2_scspr2417819002_07-21-202_02.28.26.3973_0 、バック： /vol/scspr2417819002_nfs_cda_2.2B32_redo 01726.21_r19821_scspr1972_j21_j21_scspr2002_2002_17202_017202_019002_019002_019002_019002_019002_017

  ◦ 複数のデータベースインスタンスの場合： NFSB32@buck ： /vol/scspr2417819002_NFS_CDB32_data/Rg2_scspr2417819002_07-021_2021_21_219002_0226.3973_0 、バック： /vol/scspr2417819002_NFS21_2.17002_NFS017002_NFS019002_002_NFS019002_42002_4_017202_NFS122_1821_CD21_2.17202_NFS017202_41_CD21_2.17202_17202_17202_17202_17202_17202_17202_17202_17202_122_17202_17202_0.2_ R17202_17202_17202_17202_17202_17202_0.2_

NFS 9_17202_17202_122_17202_122_DATA 、 NFS 017202_17202_17202_17202_17202_0.2_ NFS 9_R17202_122_17202_

- * SC_primary_snapshot_names * には、バックアップ中に作成されたプライマリ Snapshot の名前を指定します。

  例

  - 単一データベースインスタンスの場合： RG2_scspr2417819002_07-021-021-02.28.26.3973_0 、 RG2_scspr2417819002_07-021-202_02.28.26.3973_1
  - 複数のデータベースインスタンスの場合： NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973 _0 、 Rg2_scspr2417819002_07-01-202_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973 _0 、 Rg2_scspr2417819002_07-021-02.28.26.3973_1
  - 整合グループの Snapshot に 2 つのボリュームが含まれる場合： CG3_R80404CBEF5V1_04-05-050202_003.4945_bfc279cc-28ad-465c-9d60-5487ac17b25d_202_4_3_8_58_350

- * SC_primary_mount_points * は、バックアップに含まれるマウントポイントの詳細を指定します。

  詳細には、バックアップでファイルの直接の親ではなく、ボリュームがマウントされているディレクトリが含まれます。ASM 構成の場合は、ディスクグループの名前です。

  データの形式は、 <db1><mountpoint1, mountpoint2>|<DB2><mountpoint1, mountpoint2> のようになります。

  例

  - シングルデータベースインスタンスの場合： /mnt/nfsdb3_data 、 /mnt/nfsdb3_log 、 /mnt/nfsdb3_data1
  - 複数のデータベースインスタンスの場合： NFSB31@/mnt/nfsdb31_data 、 /mnt/nfsdb31_log 、 /mnt/nfsdb31_log 、 /mnt/nfsdb32_data, /mnt/nfsdb32_log 、 /mnt/nfsdb32_data1
  - ASM の場合： +DATA2DG 、 +LOG2DG

- * SC_primary_snapshots および _mount_points * には、各マウントポイントのバックアップ中に作成された Snapshot の名前を指定します。

  例

  - シングルデータベースインスタンスの場合： Rg2_scspr2417819002_07-02-2202_02.28.26.3973_0 ： /mnt/nfsb32_data 、 Rg2_scspr2417819002_07-021 - 202_02.28.26.3973_1 ： /mnt/bnfs31_log
  - 複数のデータベースインスタンスの場合： NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973 _0 ： /mnt/nfsb32_data 、 Rg2_scspr2417819002_07-021 - 202_02.28.26.3973_1 ： /mnt/nfsb31_log | NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973 _0 ： /mnt/nfsb31_data 、 Rg2_scspr24178219002_07819002_302_log - nfs3/026.32_nfmnt_302_log

- **SC_archivelogs_locations** はアーカイブ・ログ・ディレクトリの場所を指定します

  ディレクトリ名はアーカイブログファイルの直下の親になります。アーカイブログを複数の場所に配置すると、すべての場所がキャプチャされます。これには FRA シナリオも含まれます。ディレクトリにソフトリンクが使用されている場合は、同じ情報が入力されます。

  例

- NFS 上の単一データベースの場合： /mnt/nfsdb2_log
- NFS 上の複数のデータベースおよび NFSB31 データベースアーカイブログが 2 つの異なる場所に格納されている場合： NFSB31@/mnt/nfsdb31_log1 、 /mnt/nfsdb31_log2 | NFSB32@/mnt/nfsdb32_log
- ASM の場合： +LOG2DG/ASMDB2/ARCHIVE/2021 _ 07_15

- * SC_redo _logs_locations * は 'redo ログ・ディレクトリの場所を指定します

  ディレクトリ名は REDO ログファイルの直下の親になります。ディレクトリにソフトリンクが使用されている場合は、同じ情報が入力されます。

  例

  - NFS 上の単一データベースの場合： /mnt/nfsdb2_data/newdb1
  - NFS 上の複数のデータベース： NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
  - ASM の場合： +LOG2DG/ASMDB2/ONLINELOG

- * sc_control_files_location* には、制御ファイルディレクトリの場所を指定します。

  このディレクトリ名は制御ファイルの直下の親になります。ディレクトリにソフトリンクが使用されている場合は、同じ情報が入力されます。

  例

  - NFS 上の単一データベースの場合： /mnt/nfsdb2_data/FRA/newdb1 、 /mnt/nfsdb2_data/newdb1
  - NFS 上の複数のデータベース： NFSB3@/mnt/nfsdb31_data/FRA/newdb31 、 /mnt/nfsdb31_data/newdb31/NFSB32@/mnt/nfsdb32_data/FRA/newdb32 、 /mnt/nfsdb32_data/newdb32
  - ASM の場合： +LOG2DG/ASMDB2/CONTROLFILE

- *SC_data_files_locations" にはデータ・ファイル・ディレクトリの場所を指定します

  ディレクトリ名はデータファイルの直下の親になります。ディレクトリにソフトリンクが使用されている場合は、同じ情報が入力されます。

  例

  - NFS 上の単一データベースの場合： /mnt/nfsdb3_data1 、 /mnt/nfsdb3_data/newDB3/datafile
  - NFS 上の複数のデータベース： NFSB31@/mnt/nfsdb31_data1 、 /mnt/nfsdb31_data/newDB31/datafile | NFSB32@/mnt/nfsdb32_data1 、 /mnt/nfsdb32_data/newDB32/data/newDB32/datafile
  - ASM の場合： +DATA2D2/ASMDB2/datafile 、 +DATA2D2/ASMDB2/tempfile

- * SC_SNAPSHOT_LABEL * はセカンダリ・ラベルの名前を指定します

  例： Hourly 、 Daily 、 Weekly 、 Monthly 、 Custom Label

サポートされるデリミタ

- * ： * は、 SVM 名とボリューム名を区切るために使用します

例： buck ： /vol/scspr2417819002_nfs_cdb32_data/Rg2_scspr2417819002_07-021 - 202_02.28.26.3973_0 、バック： /vol/scspr2417819002_cda_2.2/Rg2_scr21_scspr2004_17821_scspr2002_240021_scspr2004_17202_j21 _scspr2002_0.21_j21_j21_j21_scspr2002_0

- **@** は、データベース名からデータを分離し、キーから値を分離するために使用されます。

  例

  - NFSB32@buck ： /vol/scspr2417819002_NFSB32_CDB_data/Rg2_scspr2417819002_019002_019002_019002_07-21- 202_02.28.26.3973_0 、バック： /vol/scspr2417819002_CD21_NFS21_24002_NFS017002_002_002_NFS21_24002_NFS21_24002_1 7002_172021_2.17002_17002_17002_17002_17002_17002_17202_17202_17002_17002_17002_17 202_17002_17002_17202_17202_17202_17202_17202_17202_17202_17202_17002_17002_17002_ 17002_17202_17202_17202_17202_17202_17202_17202_17202_17202_17202_17202_1720 2_17202_17202_17
  - NFSB3@ Oracle | NFSB32@ Oracle

- * | * は、 2 つの異なるデータベース間でデータを分離するため、および SC_BACKUP ID 、 SC_BACKUP _retention 、および SC_BACKUP _name の各パラメータの 2 つのエンティティ間でデータを分離するために使用されます。

  例

  - データ @203| ログ @205
  - 毎時 | データ @ 日数： 3 | ログ @ カウント： 4
  - DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | LOG@RG2_scspr2417819002_07- 20-2021_12.16.48.9267 _1

- * / * を使用して、 SC_primary_snapshot_names パラメータと SC_primary_full_snapshot_name_for_tag パラメータのボリューム名を Snapshot と区切ります。

  例： NFSB32@buck ： /vol/scspr2417819002_NFS_CDB_NFSB32_data/Rg2_scspr2417819002_07-021 - 202_02.28.26.3973_0 、バック： /vol/scspr2417819002_NFS_CDB_2.2BNFS32_bNFS32_26.21_R1726.21_scspr702- 1721_scspr1973.0021_r21_scspr21_scspr2002_1772.1773.190021_scspr21_sc2002_

- * 、 * は、同じ DB の変数のセットを区切るために使用されます。

  例： NFSB32@buck ： /vol/scspr2417819002_NFS_CDB_NFSB32_data/Rg2_scspr2417819002_07-21- 202_02.28.26.3973_0 、 NFS19002_017819002_nfs_sc019002_002_41_scspbucK_24002_24002_24002_cdr21_nfs21_sc1621_r1 7202_17202_17202_17202_17202_17202_17202_17202_122_122_17202_122_17202_17202_122_ NFS 9_17202_17202_17202_17202_17202_17202_017202_017202_122_ NFS 9_172_ NFS 9_R17202_017202_017202_017202_017202_017202_017202_017202_017202_017202_017202_01720 2_017202_017202_

バックアップ保持オプション

バックアップコピーを保持する日数を選択するか、保持するバックアップコピーの数を指定できます。指定できる最大数は ONTAP で 255 個です。たとえば、組織の必要に応

じて、 10 日分のバックアップコピーや 130 個のバックアップコピーを保持できます。

ポリシーを作成する際に、バックアップタイプおよびスケジュールタイプの保持オプションを指定できます。

SnapMirror レプリケーションを設定すると、デスティネーションボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、保持されているバックアップの保持ラベルがスケジュールタイプと一致する場合には、バックアップを削除します。リソースまたはリソースグループに対してスケジュールタイプが変更された場合、古いスケジュールタイプラベルのバックアップがシステムに残ることがあります。

バックアップコピーを長期にわたって保持する場合は、 SnapVault バックアップを使用する必要があります。

バックアップスケジュール

バックアップ頻度（スケジュールタイプ）はポリシーで指定され、バックアップスケジュールはリソースグループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA と RPO は、データ保護戦略に関与します。

使用頻度の高いリソースであっても、フルバックアップは 1 日に 1~2 回で十分です。たとえば、定期的なトランザクションログバックアップを実行すれば、必要なバックアップが作成されます。データベースをバックアップする回数が多いほど、リストア時に SnapCenter が使用する必要のあるトランザクションログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度

  バックアップ頻度（バックアップを実行する間隔）は、ポリシー設定の一部であり、一部のプラグインでは _ schedule type__ と呼ばれます。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しない場合は、オンデマンドのみのポリシーが作成されます。ポリシーにアクセスするには、 * Settings * > * Policies * をクリックします。

- バックアップスケジュール

  バックアップスケジュール（バックアップが実行される日時）は、リソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます。リソースグループのスケジュールにアクセスするには、 * リソース * > * リソースグループ * をクリックします。

Snapshot コピーのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- _dts1_は リソースグループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、「 * Snapshot コピーにカスタム名形式を使用」を選択して、リソースまたはリソースグループを保護しながら Snapshot コピー名の形式を指定することもできます。たとえば、customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名にタイムスタンプのサフィックスが追加されます。

Oracle データベースをバックアップするための要件

Oracle データベースをバックアップする前に、前提条件を満たしていることを確認する必要があります。

- ポリシーを適用したリソースグループを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- バックアップ処理で使用されるアグリゲートを、データベースが使用する Storage Virtual Machine （ SVM ）に割り当てておく必要があります。
- データベースでセカンダリ保護が有効になっている場合は、そのデータベースに属するすべてのデータボリュームとアーカイブログボリュームが保護されていることを確認しておく必要があります。
- ASM ディスク・グループ上にファイルがあるデータベースが 'Oracle DBVERIFY ユーティリティを使用してバックアップを検証するには ' マウント状態またはオープン状態であることを確認しておく必要があります
- ボリュームマウントポイントの長さが 240 文字を超えないことを確認しておく必要があります。
- バックアップするデータベースが大容量（TB単位）の場合は、SnapCenter サーバホストでRESTTimeoutの値を86400000msに増やして、C：\Program Files\NetApp\SMCore \SMCoreServiceHost.exe.config_fileに設定してください。

値を変更するときに実行中のジョブがないことを確認し、値を増やしたあとに SnapCenter SMCore サービスを再起動します。

バックアップに使用できる**Oracle**データベースを検出します

リソースとは、 SnapCenter で管理されているホスト上の Oracle データベースのことです。使用可能なデータベースを検出したあとに、それらのデータベースをリソースグループに追加してデータ保護処理を実行できます。

- 必要なもの *
- SnapCenter サーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- データベースが仮想マシンディスク（ VMDK ）または raw デバイスマッピング（ RDM ）上にある場合は、 SnapCenter Plug-in for VMware vSphere を導入し、 SnapCenter にプラグインを登録する必要があります。

  詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere を導入"。
- データベースが VMDK ファイルシステムにある場合は、 vCenter にログインして * VM オプション * > * Advanced * > * Edit configuration * に移動し、 VM の DISK.enableUUID_true の値を設定しておく必要があります。
- SnapCenter データベースのさまざまなタイプやバージョンを検出するための、 Oracle のプロセスを確認しておく必要があります。

手順**1**：**SnapCenter** でデータベース以外のエントリが検出されないようにする

oratabファイル内に追加された非データベースエントリをSnapCenter で検出できません。

- 手順 *

1. Oracle用プラグインをインストールしたあと、rootユーザはディレクトリ_/var/opt/snapcenter/sco/etc/に*SC_oratab .config *ファイルを作成する必要があります。

   Oracleバイナリの所有者とグループに書き込み権限を付与して、ファイルを将来的に保持できるようにします。

2. データベース管理者は、* SC_oratab .config *ファイルに非データベース・エントリを追加する必要があります。

   /etc/oratabファイル内の非データベース・エントリに定義されている形式を同じにするか、またはユーザが非データベース・エンティティ・ストリングだけを追加できるようにすることを推奨します。

   文字列では大文字と小文字が区別されます。先頭に#が付いているテキストはコメントとして扱われます。コメントは、の後に追加できます
   非データベース名。

```
For example:
-----------------------------------------
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar  # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----------------------------------------------
```

1. リソースを確認

   データベース以外のエントリがリソースページにリストされません。* SC_oratab .config *に追加されているエントリはありません。

SnapCenter プラグインをアップグレードする前に、SC_AGENT構成ファイルのバックアップを作成することを常に推奨します。

ステップ**2**：リソースを検出する

プラグインをインストールすると、そのホスト上のすべてのデータベースが自動的に検出され、リソースページに表示されます。

データベースが検出されるためには、データベースが少なくともマウント済み状態であることが必要です。Oracle Real Application Clusters （ RAC ）環境で、検出が実行されるホスト内の RAC データベースインスタンスが検出されるためには、データベースインスタンスが少なくともマウント済み状態であることが必要です。リソースグループには、正常に検出されたデータベースのみを追加できます。

ホスト上で Oracle データベースを削除した場合、 SnapCenter サーバは認識しないため、削除されたデータベースのリストが表示されます。SnapCenter リソースのリストを更新するには、リソースを手動で更新する必要があります。

- 手順 *

  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。

     をクリックします をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。次に、をクリックします アイコンをクリックして、フィルタペインを閉じます。

  3. [リソースの更新] をクリックします。

     RAC One Node シナリオでは、データベースが現在ホストされているノード上の RAC データベースとして検出されます。

- 結果 *

データベースは、データベースタイプ、ホストまたはクラスタ名、関連するリソースグループとポリシー、ステータスなどの情報とともに表示されます。

データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

- データベースがネットアップ以外のストレージシステム上にある場合、ユーザインターフェイスの総体的なステータス列にはバックアップに使用できないメッセージが表示されます。

  ネットアップ以外のストレージシステム上のデータベースには、データ保護処理を実行できません。

- データベースがネットアップストレージシステム上にあり、保護されていない場合は、ユーザインターフェイスの総体的なステータス列に Not protected というメッセージが表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合、ユーザインターフェイスの総体的なステータス列には、バックアップに使用可能なメッセージが表示されます。

Oracle データベース認証を有効にしている場合、リソースビューに赤い鍵のアイコンが表示されます。データベースを保護できるようにデータベースのクレデンシャルを設定するか、データベースをリソースグループに追加してデータ保護処理を実行する必要があります。

Oracle データベースのバックアップポリシーの作成

SnapCenter を使用して Oracle データベースリソースをバックアップする前に、バックアップ対象のリソースまたはリソースグループのバックアップポリシーを作成する必要があります。バックアップポリシーとは、バックアップを管理、スケジューリング、および保持する方法を定めた一連のルールです。レプリケーション、スクリプト、バックアップタイプの設定を指定することもできます。ポリシーを作成することで、別のリソースやリソースグループでポリシーを再利用して時間を節約することができます。

- 始める前に *
- バックアップ戦略を定義しておく必要があります。
- SnapCenter のインストール、ホストの追加、データベースの検出、ストレージシステム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Snapshot コピーをミラーセカンダリストレージまたはバックアップセカンダリストレージにレプリケートするユーザには、 SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に SVM を割り当てる必要があります。
- root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。
- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. ドロップダウン・リストから「 * Oracle Database * 」を選択します。
4. [新規作成（ New ）] をクリックする。
5. [名前] ページで、ポリシー名と概要を入力します。

6. [Backup Type] ページで、次の手順を実行します。

   - オンライン・バックアップ * を作成する場合は、 * オンライン・バックアップ * を選択します。

     バックアップの対象として、すべてのデータファイル、制御ファイル、アーカイブログファイル、データファイルと制御ファイル、またはアーカイブログファイルのみを指定する必要があります。

   - オフライン・バックアップ * を作成する場合は、 * オフライン・バックアップ * を選択し、次のいずれかのオプションを選択します。

     - データベースがマウント状態のときにオフラインバックアップを作成する場合は、 * Mount * を選択します。
     - データベースをシャットダウン状態に変更してオフラインシャットダウンバックアップを作成する場合は、 * Shutdown * を選択します。

       Pluggable Database （ PDB ）がある場合、バックアップ作成前に PDB の状態を保存するには、「 * PDB の状態を保存」を選択する必要があります。これにより、バックアップ作成後に PDB を元の状態に戻すことができます。

   - オンデマンド * 、 * 毎時 * 、 * 毎日 * 、 * 毎週 * 、または * 毎月 * を選択して、スケジュールの頻度を指定します。

     リソースグループを作成する際に、バックアップ処理のスケジュール（開始日と終了日）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。

     午前 2 時にスケジュールを設定した場合、夏時間（ DST ）中はスケジュールはトリガーされません。

   - Oracle Recovery Manager （ RMAN ）を使用してバックアップをカタログ化する場合は、 [* Catalog backup with Oracle Recovery Manager （ RMAN ） *] を選択します。

     一度に 1 つのバックアップのカタログ化を実行するには、 GUI を使用するか、 SnapCenter CLI コマンド Catalog-SmBackupWithOracleRMAN を使用します。

     RAC データベースのバックアップをカタログ化する場合は、そのデータベースに対して他のジョブが実行されていないことを確認します。別のジョブが実行されている場合は、カタログ化処理がキューに登録されずに失敗します。

   - バックアップ後にアーカイブ・ログのプルーニングを行う場合は、バックアップ後にアーカイブ・ログをプルーニング * を選択します。

     データベースで設定されていないアーカイブ・ログ・デスティネーションからのアーカイブ・ログの削除は、スキップされます。

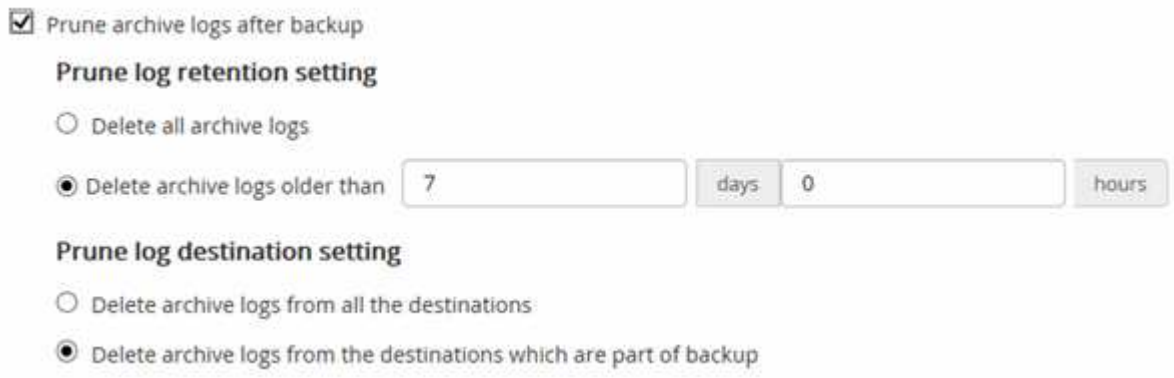
     Oracle Standard Edition を使用している場合は、アーカイブログのバックアップ中に log_archive_dest パラメータと log_archive_duplex_dest パラメータを使用できます。

- アーカイブログを削除できるのは、アーカイブログファイルをバックアップの一部として選択した場合だけです。

削除処理を正常に行うには、 RAC 環境のすべてのノードがすべてのアーカイブログの場所にアクセスできることを確認する必要があります。

状況	作業
すべてのアーカイブログを削除します	[Delete all archive logs*] を選択します。
古いアーカイブログを削除します	「 * 次より古いアーカイブログを削除」を選択し、削除するアーカイブログの経過時間を日数と時間数で指定します。
すべてのデスティネーションからアーカイブログを削除します	すべての保存先からアーカイブ・ログを削除する * を選択します。
バックアップの一部であるログデスティネーションからアーカイブログを削除します	[* バックアップの一部である保存先からアーカイブ・ログを削除する *] を選択します。

+



7. [保持] ページで ' バックアップ・タイプの保持設定と [バックアップ・タイプ] ページで選択したスケジュール・タイプを指定します

状況	作業

一定数の Snapshot コピーを保持します	保持する Snapshot コピーの総数 * を選択し、保持する Snapshot コピーの数を指定します。 Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。 最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。 SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。
Snapshot コピーを特定の日数だけ保持します	「 * Snapshot コピーを保持する期間」を選択し、 Snapshot コピーを削除するまで保持する日数を指定します。

アーカイブログバックアップを保持できるのは、アーカイブログファイルをバックアップの一部として選択した場合だけです。

8. Replication （レプリケーション）ページで、レプリケーション設定を指定します。

フィールド	手順
ローカル Snapshot コピーの作成後に SnapMirror を更新します	別のボリュームにバックアップセットのミラーコピーを作成する場合（ SnapMirror レプリケーション）は、このフィールドを選択します。
ローカル Snapshot コピーの作成後に SnapVault を更新します	ディスクツーディスクのバックアップレプリケーション（ SnapVault バックアップ）を実行する場合は、このオプションを選択します。

フィールド	手順
セカンダリポリシーのラベル	Snapshot ラベルを選択します。 選択した Snapshot コピーラベルに応じて、 ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。 ローカル Snapshot コピーの作成後に「 * SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できます。ただし、ローカル Snapshot コピーの作成後に「 * Update SnapVault 」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。
エラー再試行回数	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。

セカンダリストレージでの Snapshot コピーの最大数に達しないように、 ONTAP でセカンダリストレージの SnapMirror 保持ポリシーを設定する必要があります。

9. スクリプトページで、バックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

   プリスクリプトとポストスクリプトは、 /var/opt/snapcenter /spl/scripts_or に保存するか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

   スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

   SnapCenter では、プリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。 "詳細はこちら。"

10. [Verification] ページで、次の手順を実行します。

    a. 検証処理を実行するバックアップスケジュールを選択します。

    b. 検証スクリプトのコマンドセクションで、検証処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

       プリスクリプトとポストスクリプトは、 /var/opt/snapcenter /spl/scripts_or に保存するか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

1. 概要を確認し、 [完了] をクリックします。

Oracle データベースのリソースグループを作成してポリシーを適用します

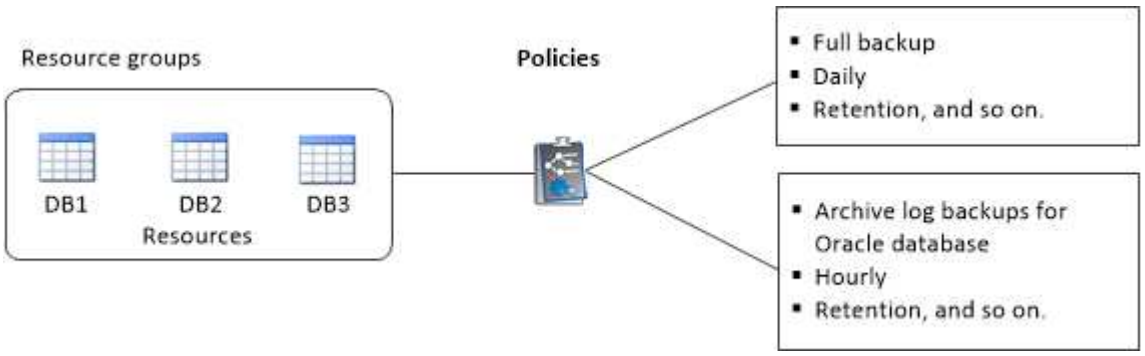
リソースグループはコンテナであり、バックアップして保護するリソースを追加します。リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。

このタスクについて

Oracle DBVERIFYユーティリティを使用してバックアップを検証するには、ASMディスクグループ内のファイルを含むデータベースが「mount」または「open」状態である必要があります。

リソースグループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義します。

次の図は、データベースのリソース、リソースグループ、およびポリシーの関係を示しています。



手順

1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 新しいリソースグループ *] をクリックします。
3. [名前] ページで、次の操作を実行します。
   a. [Name]フィールドにリソースグループの名前を入力します。

      リソースグループ名は 250 文字以内にする必要があります。

   b. 後でリソースグループを検索できるように、[Tag]フィールドに1つ以上のラベルを入力します。

      たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。

   c. Snapshot コピー名にカスタムの名前形式を使用する場合は、このチェックボックスをオンにして名前形式を入力します。

      たとえば 'customText_resource group_policy_hostname や resource group_hostname などですデフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

   d. バックアップの対象から外すアーカイブログファイルのデスティネーションを指定します。
4. Resources ページで、 * Host * ドロップダウン・リストから Oracle データベース・ホスト名を選択します。

リソースが Available Resources セクションに表示されるのは、リソースが正常に検出された場合のみです。最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、 [選択したリソース（ Selected Resources ）] セクションに移動する。

1 つのリソースグループ内の Linux ホストと AIX ホストの両方からデータベースを追加することができます。

6. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

をクリックしてポリシーを作成することもできます + 。

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

b. をクリックします + スケジュールを設定するポリシーの Configure Schedules （スケジュールの設定）列。

c. [Add schedules for policy_name] ウィンドウで、スケジュールを設定し、 [**OK**] をクリックします。

ここで、 _policy_name_は 選択したポリシーの名前です。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。

7. [Verification] ページで、次の手順を実行します。

a. Load locators * （ロケータのロード）をクリックして、 SnapMirror または SnapVault ボリュームをロードし、セカンダリ・ストレージ上で検証を実行します。

b. をクリックします + [Configure Schedules]列で、ポリシーのすべてのスケジュールタイプに対して検証スケジュールを設定します。

c. Add Verification Schedules policy_name ダイアログボックスで、次の操作を実行します。

状況	手順
バックアップ後に検証を実行します	[Run verification after backup] を選択します。
検証をスケジュールします	[Run scheduled verification] を選択し、ドロップダウン・リストからスケジュール・タイプを選択します。

d. セカンダリ・ストレージ・システムのバックアップを検証するには、セカンダリ・サイトで * Verify on secondary location * を選択します。

e. [OK] をクリックします。

設定した検証スケジュールは、 Applied Schedules 列にリスト表示されます。

8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、 [ジョブレポートの添付（ Attach Job Report ）] を選択します。

E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

9. 概要を確認し、 [完了] をクリックします。

Oracle リソースのバックアップ

どのリソースグループにも含まれていないリソースは、のリソースページからバックアップすることができます。

手順

1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [表示] リストから [* データベース *] を選択します。
3. をクリックします をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。

をクリックします をクリックしてフィルタペインを閉じます。

4. バックアップするデータベースを選択します。

Database - Protect （データベース - 保護）ページが表示されます。

5. [Resources]ページでは、次の手順を実行できます。
   a. チェックボックスを選択し、Snapshotコピー名に使用するカスタムの名前形式を入力します。

   例： `customtext_policy_hostname` または `resource_hostname`。デフォルトでは、Snapshotコピー名にタイムスタンプが付加されます。

   b. バックアップの対象から外すアーカイブログファイルのデスティネーションを指定します。
6. [Policies] ページで、次の手順を実行します。
   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

   ポリシーを作成するには、をクリックします 。

   [選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

b. をクリックします [Configure Schedules]列で、ポリシーのスケジュールを設定します。

c. [Add schedules for policy_policy_name_]ウィンドウでスケジュールを設定し、を選択します `OK`。

_policy_name_は 、選択したポリシーの名前です。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

7. [Verification] ページで、次の手順を実行します。

a. [Load locators]*をクリックしてSnapMirrorまたはSnapVault ボリュームをロードし、セカンダリストレージを検証します。

b. をクリックします Configure Schedules （スケジュールの設定）列で、ポリシーのすべてのスケジュールタイプの検証スケジュールを設定します。
[+]
[Add Verification Schedules_policy_name_]ダイアログボックスでは、次の手順を実行できます。

c. [Run verification after backup] を選択します。

d. [スケジュールされた検証を実行する]*を選択し、ドロップダウンリストからスケジュールタイプを選択します。

Flex ASM 設定では、カードの数が RAC クラスタ内のノード数より少ない場合、リーフノードで検証操作を実行できません。

e. セカンダリストレージ上のバックアップを検証するには、セカンダリストレージ上で * Verify on secondary location * を選択します。

f. [OK] をクリックします。

設定した検証スケジュールは、 Applied Schedules 列にリスト表示されます。

8. [Notification]ページで、*[Email preference]*ドロップダウンリストからEメールを送信するシナリオを選択します。

送信者と受信者のEメールアドレス、およびEメールの件名を指定する必要があります。リソース上で実行されたバックアップ処理のレポートを添付する場合は、 [ジョブレポートの添付（ Attach Job Report ）] を選択します。

Eメール通知を使用する場合は、GUIまたはPowerShellコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります `Set-SmSmtpServer`。

9. 概要を確認し、 [完了] をクリックします。

データベーストポロジのページが表示されます。

10. [今すぐバックアップ] をクリックします。

11. Backup （バックアップ）ページで、次の手順を実行します。

a. リソースに複数のポリシーを適用している場合は、ポリシーのドロップダウンリストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

b. [バックアップ] をクリックします。

12. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

完了後

- AIXのセットアップでは、を使用できます `lkdev` コマンドを使用してロックします `rendev` コマンドを使用して、バックアップされたデータベースが格納されているディスクの名前を変更します。

  デバイスのロックまたは名前変更は、そのバックアップを使用してリストアしても、リストア処理には影響しません。

- データベースクエリの実行時間がタイムアウト値を超えたためにバックアップ処理が失敗した場合は、を実行してORACLE_SQL_QUERY_TIMEOUTおよびORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する必要があります `Set-SmConfigSettings` コマンドレット：

  パラメータの値を変更したら、次のコマンドを実行してSnapCenter Plug-in Loader（SPL）サービスを再起動します `/opt/NetApp/snapcenter/spl/bin/spl restart`

- ファイルにアクセスできず、検証プロセス中にマウントポイントを使用できないと、エラーコード DBV-00100 specified file が表示されて処理が失敗することがあります。sco.properties の verification_delay パラメータと verification_retry_count パラメータの値を変更する必要があります。

  パラメータの値を変更したら、次のコマンドを実行してSnapCenter Plug-in Loader（SPL）サービスを再起動します `/opt/NetApp/snapcenter/spl/bin/spl restart`

- MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。
- VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。

  Java のヒープサイズを増やすには、スクリプトファイル /opt/NetApp/init_scripts/scvservice_. を探します。このスクリプトでは、を実行します `do_start method` コマンドは、SnapCenter VMwareプラグインサービスを開始します。このコマンドを次のように更新します。 `Java -jar -Xmx8192M -Xms4096M`。

詳細については、こちらをご覧ください

- "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"
- "SnapCenter 処理では、 Oracle RAC One Node データベースがスキップされます"
- "Oracle 12c ASM データベースの状態を変更できませんでした"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできます" （ログインが必要）

Oracle データベースのリソースグループをバックアップする

リソースグループは、ホストまたはクラスタ上のリソースの集まりです。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースを対

象に実行されます。

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

手順

1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。
3. 検索ボックスにリソースグループ名を入力するか、をクリックします をクリックし、タグを選択します。

   をクリックします をクリックしてフィルタペインを閉じます。

4. [Resource Group]ページで、バックアップするリソースグループを選択します。

   2つのデータベースが統合されたリソースグループがあり、一方のデータベースにネットアップ以外のストレージにデータがある場合は、もう一方のデータベースがネットアップストレージにあるにもかかわらず、バックアップ処理が中止されます。

5. Backup （バックアップ）ページで、次の手順を実行します。
   a. リソースグループに複数のポリシーが関連付けられている場合は、*[ポリシー]*ドロップダウンリストから使用するバックアップポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. 「 * Backup * 」を選択します。
6. 進捗状況を監視するには、*[監視]>[ジョブ]*を選択します。

完了後

- AIXのセットアップでは、を使用できます `lkdev` コマンドを使用してロックします `rendev` コマンドを使用して、バックアップされたデータベースが格納されているディスクの名前を変更します。

  デバイスのロックまたは名前変更は、そのバックアップを使用してリストアしても、リストア処理には影響しません。

- データベースクエリの実行時間がタイムアウト値を超えたためにバックアップ処理が失敗した場合は、を実行してORACLE_SQL_QUERY_TIMEOUTおよびORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する必要があります `Set-SmConfigSettings` コマンドレット：

  パラメータの値を変更したら、次のコマンドを実行してSnapCenter Plug-in Loader（SPL）サービスを再起動します `/opt/NetApp/snapcenter/spl/bin/spl restart`

- ファイルにアクセスできず、検証プロセス中にマウントポイントを使用できないと、エラーコード DBV-00100 specified file が表示されて処理が失敗することがあります。sco.propertiesのverification_delay_and verification_retry_countパラメータの値を変更する必要があります。

  パラメータの値を変更したら、次のコマンドを実行してSnapCenter Plug-in Loader（SPL）サービスを再

起動します `/opt/NetApp/snapcenter/spl/bin/spl restart`

Oracleデータベースのバックアップを監視します

バックアップ処理とデータ保護処理の進捗状況を監視する方法について説明します。

Oracle データベースのバックアップ処理を監視する

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. Jobs （ジョブ）ページで、次の手順を実行します。
     a. をクリックします バックアップ処理だけが表示されるようにリストをフィルタリングします。
     b. 開始日と終了日を指定します。
     c. [* タイプ] ドロップダウン・リストから、 **[*Backup]** を選択します。
     d. [**Status**](ステータス *) ドロップダウンから、バックアップステータスを選択します。
     e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
  4. バックアップジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

     バックアップジョブのステータスがと表示されます で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

     View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity] ペインでデータ保護操作を監視します

[アクティビティ（ Activity ）] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity （アクティビティ）] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. をクリックします  をクリックして、最近の 5 つの操作を表示します。

     いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

その他のバックアップ処理

UNIX コマンドを使用して **Oracle** データベースをバックアップします

バックアップのワークフローには、計画、バックアップするリソースの特定、バックアップポリシーの作成、リソースグループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

- 必要なもの *
- ストレージシステム接続を追加し、 SmStorageConnection_or_Add-SmCredential_ のコマンドを使用してクレデンシャルを作成しておく必要があります。
- Command_Open-SmConnection_ を使用して SnapCenter サーバとの接続セッションを確立しておく必要があります。

  SnapCenter アカウントでのログインセッションは 1 つしか確立できず、トークンはユーザのホームディレクトリに保存されます。

  接続セッションは 24 時間のみ有効です。ただし、 TokenNeverExpires オプションを使用して期限切れにならないトークンを作成し、セッションを常に有効にすることができます。

- このタスクについて *

次のコマンドを実行して、 SnapCenter サーバとの接続の確立、 Oracle データベースインスタンスの検出、ポリシーとリソースグループの追加、バックアップの作成と検証を行います。

コマンドで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドリファレンスガイド"。

- 手順 *
  1. 指定されたユーザ用に SnapCenter サーバとの接続セッションを開始します： *Open-SmConnection*
  2. ホストリソースの検出処理を実行します： *Get-SmResources*

3. Real Application Cluster （ RAC ）データベースのバックアップ処理に使用する Oracle データベースのクレデンシャルと優先ノードを設定します： *Configure - SmOracleDatabase*
4. バックアップポリシーを作成します。 *Add-SmPolicy*
5. セカンダリ（ SnapVault または SnapMirror ）ストレージの場所に関する情報を取得します： *get -SmSecondaryDetails*

   このコマンドは、指定したリソースのプライマリストレージからセカンダリストレージへのマッピングの詳細を取得します。バックアップリソースグループを作成する際に、このマッピングの詳細を使用してセカンダリの検証を設定できます。

6. リソースグループを SnapCenter に追加します： *Add-SmResourceGroup*
7. バックアップを作成する： *New-SmBackup*

   WaitForCompletion オプションを使用してジョブをポーリングすることができます。このオプションを指定した場合は、バックアップジョブが完了するまでコマンドが引き続きサーバをポーリングします。

8. SnapCenter からログを取得します： *Get-SmLogs*

Oracle データベースのバックアップ処理をキャンセルします

実行中、キューに登録済み、または応答しないバックアップ処理をキャンセルできます。

バックアップ処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *

バックアップ処理をキャンセルすると、 SnapCenter サーバは処理を停止し、作成されたバックアップが SnapCenter サーバに登録されていない場合は、ストレージからすべての Snapshot コピーを削除します。バックアップがすでに SnapCenter サーバに登録されている場合、キャンセル後も、作成済みの Snapshot コピーはロールバックされません。

- キャンセルできるのは、キューに登録されたか実行中のログ処理またはフルバックアップ処理のみです。
- 検証の開始後に処理をキャンセルすることはできません。

  検証前に処理をキャンセルした場合、処理はキャンセルされ、検証処理は実行されません。

- カタログ処理の開始後にバックアップ処理をキャンセルすることはできません。
- バックアップ処理は、 Monitor （モニタ）ページまたは Activity （アクティビティ）ペインからキャンセルできます。
- SnapCenter GUI に加え、 CLI コマンドを使用して処理をキャンセルすることもできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っているバックアップ操作をキャンセルできます
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. 操作を選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. バックアップジョブを開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ジョブの詳細］ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

- 結果 *

処理がキャンセルされ、リソースが元の状態に戻ります。

キャンセル中または実行中の状態でキャンセルした処理が応答しない場合は、 Cancel-SmJobID<int> -Force を実行してバックアップ処理を強制的に停止する必要があります。

Topology ページで、 **Oracle** データベースのバックアップとクローンを表示します

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

- このタスクについて *

トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

[コピーの管理] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップとクローンが使用可能かどうかを判断できます。

- には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
- には、 SnapMirror テクノロジを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。
- には、 SnapVault テクノロジを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。

表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、 4 つのバックアップだけを保持するポリシーを使用して 6 つのバックアップを作成した場合、バックアップの数は 6 と表示されます。

mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

   リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. 概要カードを確認して、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数をサマリで確認します。

   サマリカードセクションには、バックアップとクローンの合計数とログバックアップの合計数が表示されます。

   「 * Refresh * 」ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

5. [コピーの管理] ビューで、プライマリストレージまたはセカンダリストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

   バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、マウント、アンマウント、名前変更を実行します。 カタログ化、カタログ化解除、および削除の各処理。

   セカンダリストレージ上のバックアップは、名前変更または削除できません。

   - ログバックアップを選択した場合は、名前変更、マウント、アンマウント、カタログ化解除、 および DELETE 処理が含まれます。
   - Oracle Recovery Manager （ RMAN ）を使用してバックアップをカタログ化した場合、そのカタログ化されたバックアップの名前は変更できません。

7. クローンを削除する場合は、表でクローンを選択し、をクリックします 。

SnapmirrorStatusUpdateWaitTime に割り当てられた値がより小さい場合、データボリュームとログボリュームが正常に保護されても、ミラーとバックアップのバックアップコピーはトポロジページに表示されません。SnapmirrorStatusUpdateWaitTime に割り当てられた値は、 _Set-SmConfigSettings_PowerShell コマンドレットを使用して増やす必要があります。

コマンドで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。

または、を参照することもできます "SnapCenter ソフトウェアコマンドリファレンスガイド" または "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

データベースバックアップのマウントとアンマウント

バックアップ内のファイルにアクセスする必要がある場合は、 1 つまたは複数のデータバックアップおよびログのみのバックアップをマウントできます。バックアップは、バックアップが作成されたホストにも、同じタイプの Oracle およびホスト構成を使用するリモートホストにもマウントできます。バックアップを手動でマウントした場合は、処理の完了後にバックアップを手動でアンマウントする必要があります。任意のインスタンスで、データベースのバックアップを任意のホストにマウントできます。処理を実行する際には、バックアップを 1 つだけマウントできます。

Flex ASM 設定では、カードの数が RAC クラスタ内のノード数より少ない場合、リーフノードでマウント操作を実行できません。

データベースバックアップをマウント

バックアップ内のファイルにアクセスする場合は、データベースバックアップを手動でマウントする必要があります。

- 必要なもの *
- NFS 環境に Automatic Storage Management （ ASM ）データベースインスタンスがあり、 ASM バックアップをマウントする場合は、 ASM_diskstring パラメータで定義されている既存のパスに ASM ディスクパス /var/opt/snapcenter /scors/backup_*/*/*/* を追加しておく必要があります。
- NFS 環境に ASM データベースインスタンスがあり、リカバリ操作の一環として ASM ログバックアップをマウントする場合は、 ASM_diskstring パラメータで定義されている既存のパスに ASM ディスクパス /var/opt/snapcenter /scu/clones/*_*_ を追加しておく必要があります。
- ASM_diskstring パラメータで、 ASMFD または configure _ORCL ： * _ を使用する場合は、 _AFD ： * _ を設定します。

asm_diskstring パラメータの編集方法については、を参照してください "asm_diskstring にディスクパスを追加する方法"。

- バックアップのマウント時にソースデータベースホストと異なる ASM ポートを使用する場合は、 ASM のクレデンシャルと ASM ポートを設定する必要があります。
- 代替ホストにマウントする場合は、代替ホストが次の要件を満たしていることを確認する必要があります。
  - UID と GID が元のホストと同じである
  - Oracle のバージョンが元のホストと同じである
  - OS のディストリビューションとバージョンが元のホストと同じである
  - NVMeの場合、NVMe utilをインストールする必要があります
- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認してください。詳細については、を参照してください "LUNのデバイスを検出できませんというエラーが表示されて処理に失敗します"。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

   データベーストポロジのページが表示されます。
4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムから * Backups （バックアップ） * を選択します。
5. 表からバックアップを選択し、をクリックします  。
6. バックアップのマウントページで、バックアップをマウントするホストを * から選択し、バックアップをマウントするホストを * ドロップダウン・リストから選択します。

   mount path_/var/opt/snapcenter /scx/backup_mount/backup_name/database-name_name _ が表示されます。

ASM データベースのバックアップをマウントする場合は、マウントパス + diskgroupname_SID_backupid が表示されます。

1. [マウント] をクリックします。

- 終了後 *
- マウントされたバックアップに関する情報を取得するには、次のコマンドを実行します。

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- ASM データベースをマウントした場合、マウントされたバックアップに関する情報を取得するには、次のコマンドを実行します。

```
./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- バックアップ ID を取得するには、次のコマンドを実行します。

```
./sccli Get-Smbackup-BackupNamebackup_name
```

コマンドで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。
または、を参照することもできます "SnapCenter ソフトウェアコマンドリファレンスガイド"。

データベースバックアップをアンマウント

マウントされたデータベースバックアップ上のファイルにアクセスする必要がなくなった場合は、そのバックアップを手動でアンマウントできます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

   データベーストポロジのページが表示されます。

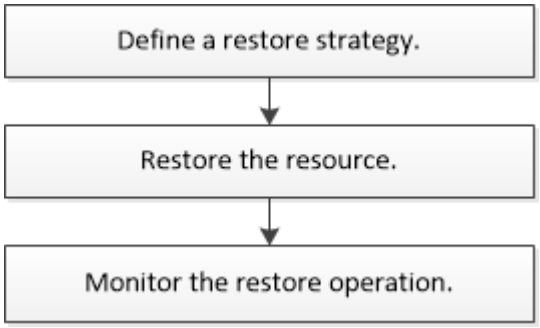
4. マウントされているバックアップを選択し、をクリックします 。
5. [OK] をクリックします。

Oracle データベースのリストアとリカバリを行う

リストアワークフロー

リストアワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



Oracle データベースのリストアとリカバリの戦略を定義する

データベースのリストアとリカバリを行う前に戦略を定義しておくと、リストア処理とリカバリ処理を正常に実行できるようになります。

リストア処理とリカバリ処理でサポートされるバックアップのタイプ

SnapCenter では、各種の Oracle データベースバックアップのリストアとリカバリがサポートされます。

- オンラインデータバックアップ
- オフラインシャットダウンデータバックアップ
- オフラインマウントデータバックアップ

> オフラインシャットダウンまたはオフラインマウントデータバックアップをリストアする場合、 SnapCenter はデータベースをオフライン状態のままにします。データベースを手動でリカバリし、ログをリセットする必要があります。

- フルバックアップ
- Data Guard スタンバイデータベースのオフラインマウントバックアップ
- Active Data Guard スタンバイデータベースの、データのみのオンラインバックアップ

> Active Data Guard スタンバイデータベースのリカバリは実行できません。

- Real Application Clusters （ RAC ）構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ
- Automatic Storage Management （ ASM ）構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ

Oracle データベースでサポートされるリストア方式のタイプ

SnapCenter では、 Oracle データベースに対して Connect and Copy リストアと In Place リストアがサポートされます。SnapCenter は、リストア処理中に、データを失うことなくリストアに使用するファイルシステムに適したリストア方式を決定します。

> SnapCenter はボリュームベースの SnapRestore をサポートしていません。

Connect and Copy リストア

データベースレイアウトがバックアップと異なる場合や、バックアップ作成後に新しいファイルがある場合は、 Connect and Copy リストアが実行されます。Connect and Copy リストア方式では、次のタスクが実行されます。

- 手順 *
  1. ボリュームは Snapshot コピーからクローニングされ、ファイルシステムスタックは、クローニングされた LUN またはボリュームを使用してホスト上に構築されます。
  2. クローニングされたファイルシステムから元のファイルシステムにファイルがコピーされます。
  3. クローニングされたファイルシステムがホストからアンマウントされ、クローニングされたボリュームが ONTAP から削除されます。

> Flex ASM 設定（カードの数が RAC クラスタ内のノード数より少ない場合）または VMDK または RDM 上の ASM RAC データベースでは、 Connect and Copy リストア方式のみがサポートされます。

In Place リストアを強制的に有効にした場合でも、次のシナリオでは SnapCenter によって Connect and Copy リストアが実行されます。

- 8.3 より前のバージョンの Data ONTAP でセカンダリストレージシステムからリストアする
- データベースインスタンスが設定されていない Oracle RAC セットアップのノードに存在する ASM ディスクグループをリストアする場合
- Oracle RAC セットアップで、いずれかのピアノードで ASM インスタンスまたはクラスタインスタンスが実行されていない場合、またはピアノードが停止している場合
- 制御ファイルのみをリストア
- ASM ディスクグループに存在する表領域の一部をリストアします

- ディスクグループは、データファイル、 SP ファイル、パスワードファイルの間で共有されます
- RAC 環境のリモートノードに SnapCenter Plug-in Loader （ SPL ）サービスがインストールされていないか実行されていない場合
- Oracle RAC に新しいノードが追加され、 SnapCenter サーバは新しく追加されたノードを認識しません

In Place リストアを実行します

データベースレイアウトがバックアップとほぼ同じであり、かつストレージとデータベーススタックで設定変更が行われていない場合は、 In Place リストアが実行されて、ファイルまたは LUN のリストアが ONTAP 上で実行されます。SnapCenter では、 In Place リストア方式の一環として Single File SnapRestore （ SFSR ）のみがサポートされます。

Data ONTAP 8.3 以降では、セカンダリサイトからの In Place リストアがサポートされます。

データベースで In Place リストアを実行する場合は、 ASM ディスクグループにデータファイルだけがあることを確認してください。ASM ディスクグループまたはデータベースの物理構造に変更を加えた場合は、バックアップを作成する必要があります。In Place リストアを実行すると、ディスクグループにバックアップ時と同じ数のデータファイルが格納されます。

ディスクグループまたはマウントポイントが次の基準に一致する場合は、 In Place リストアが自動的に適用されます。

- バックアップ後に新しいデータファイルが追加されていない（外部ファイルチェック）
- バックアップ後に ASM ディスクまたは LUN の追加、削除、または再作成が行われていない（ ASM ディスクグループの構造変更チェック）
- LVM ディスクグループに対して LUN の追加、削除、または再作成が行われていない（ LVM ディスクグループの構造変更チェック）

In Place リストアを強制的に有効にすることもできます。有効にするには、 GUI 、 SnapCenter CLI 、または PowerShell コマンドレットを使用して、外部ファイルチェックおよび LVM ディスクグループの構造変更チェックを無効にします。

ASM RAC で In Place リストアを実行します

SnapCenter では、リストアを実行するノードがプライマリノードと呼ばれ、 ASM ディスクグループがある RAC 上のその他すべてのノードがピアノードと呼ばれます。SnapCenter は、ストレージリストア処理を実行する前に、 ASM ディスクグループがマウント状態にあるすべてのノードで、ディスマウントする ASM ディスクグループの状態を変更します。ストレージのリストアが完了すると、 SnapCenter はリストア処理前と同じ状態で ASM ディスクグループの状態を変更します。

SAN 環境では、ストレージリストア処理の前に、 SnapCenter がすべてのピアノードからデバイスを削除し、 LUN のマッピング解除処理を実行します。ストレージリストア処理が完了すると、 SnapCenter は LUN マップ処理を実行し、すべてのピアノードでデバイスを構築します。SAN 環境の LUN 上に Oracle RAC ASM レイアウトが存在する場合は、 SnapCenter のリストア中に、 ASM ディスクグループが存在する RAC クラスタのすべてのノードで LUN のマッピング解除、 LUN のリストア、および LUN のマッピングが実行されます。リストア前に RAC ノードのすべてのイニシエータが LUN に使用されていなかった場合でも、 SnapCenter をリストアすると、すべての RAC ノードのすべてのイニシエータを含む新しい igroup が作成されます。

- ピアノードでリストア前の処理中にエラーが発生した場合は、リストア前の処理が成功したピアノードで

SnapCenter が自動的に ASM ディスクグループの状態をリストア実行前の状態にロールバックします。プライマリノードおよび処理が失敗したピアノードでは、ロールバックはサポートされていません。新たなリストアを実行する前に、ピアノードの問題を手動で修正し、プライマリノード上の ASM ディスクグループをマウント状態に戻す必要があります。

- リストア処理中にエラーが発生した場合は、リストア処理が失敗し、ロールバックは実行されません。新たなリストアを実行する前に、ストレージリストア問題を手動で修正し、プライマリノード上の ASM ディスクグループをマウント状態に戻す必要があります。
- いずれかのピアノードでリストア後の処理中にエラーが発生した場合、 SnapCenter は他のピアノードでリストア処理を続行します。ピアノードでリストア後の問題を手動で修正する必要があります。

Oracle データベースでサポートされるリストア処理のタイプ

SnapCenter では、 Oracle データベースに対してさまざまなタイプのリストア処理を実行できます。

データベースをリストアする前に、バックアップが検証されて、実際のデータベースファイルと比較して足りないファイルがないかどうかが確認されます。

フルリストア

- データファイルのみをリストアします
- 制御ファイルのみをリストアします
- データファイルと制御ファイルをリストアします
- Data Guard スタンバイデータベースと Active Data Guard スタンバイデータベースにあるデータファイル、制御ファイル、および REDO ログファイルをリストアします

部分リストア

- 選択した表領域のみをリストアします
- 選択した Pluggable Database （ PDB ）のみをリストア
- 1 つの PDB の選択した表領域のみをリストアします

Oracle データベースでサポートされるリカバリ処理のタイプ

SnapCenter では、 Oracle データベースに対してさまざまなタイプのリカバリ処理を実行できます。

- 最後のトランザクションまで（すべてのログ）のデータベース
- 特定の System Change Number （ SCN ）までのデータベース
- 特定の日時までのデータベース

  リカバリの日時はデータベースホストのタイムゾーンに基づいて指定する必要があります。

  SnapCenter には 'Oracle データベースのリカバリ・オプションはありません

スタンバイとしてのデータベースロールで作成されたバックアップを使用してリストアを実行した場合、 Plug-in for Oracle Database ではリカバリがサポートされません。物理スタンバイデータベースは、常に手動でリカバリする必要があります。

Oracle データベースのリストアとリカバリに関する制限事項

リストア処理とリカバリ処理を実行する前に、制限事項を確認しておく必要があります。

11.2.0.4 から 12.1.0.1 までの Oracle のいずれかのバージョンを使用している場合、 _renamedg_command の実行時にリストア処理がハング状態になります。この問題を修正するには、 Oracle パッチ 19544733 を適用します。

次のリストア処理とリカバリ処理はサポートされていません。

- ルートコンテナデータベース（ CDB ）の表領域のリストアとリカバリ
- 一時表領域および PDB に関連付けられた一時表領域のリストア
- 複数の PDB から同時に行う表領域のリストアとリカバリ
- ログバックアップのリストア
- 別の場所へのバックアップのリストア
- Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベース以外の構成での redo ログファイルのリストア
- SPFILE およびパスワード・ファイルのリストア
- 同じホスト上の既存のデータベース名を使用して再作成され、 SnapCenter で管理されていて、有効なバックアップがあるデータベースに対してリストア処理を実行すると、 DBID が異なる場合でも、新しく作成されたデータベースファイルが上書きされます。

  これを回避するには、次のいずれかの操作を実行します。

  - データベースを再作成したら、 SnapCenter リソースを検出します
  - 再作成したデータベースのバックアップを作成します

表領域のポイントインタイムリカバリに関する制限事項

- SYSTEM 、 SYSAUX 、 UNDO の PITR （ポイント・イン・タイム・リカバリ）はサポートされていません
- 表領域の PITR は、他のタイプのリストアと同時には実行できません
- テーブルスペースの名前を変更したあと、名前を変更する前に名前を特定の時点にリカバリする場合は、以前の表領域名を指定する必要があります
- 1 つの表領域内の表に対する制約が別の表領域に含まれている場合は、両方の表領域をリカバリする必要があります
- テーブルとそのインデックスが異なるテーブルスペースに格納されている場合は、 PITR を実行する前にインデックスを削除する必要があります
- PITR を使用して、現在のデフォルトテーブルスペースを回復することはできません
- PITR を使用して、次のオブジェクトを含む表領域を回復することはできません。
  - 基になるオブジェクト（実体化ビュー (Materialized View) など）または含まれるオブジェクト（パーティション化されたテーブルなど）を含むオブジェクトは ' 基になるオブジェクトまたは含まれるオブジェクトがすべてリカバリ・セットに含まれている場合を除きます

    また、分割されたテーブルのパーティションが異なるテーブルスペースに格納されている場合は、

PITR を実行する前にテーブルを削除するか、すべてのパーティションを同じテーブルスペースに移動してから PITR を実行する必要があります。

- セグメントを元に戻すかロールバックします
- Oracle 8 では、複数の受信者と互換性のある拡張キューを使用でき
- SYS ユーザが所有するオブジェクト

  これらのタイプのオブジェクトの例としては、 PL/SQL 、 Java クラス、呼び出しプログラム、ビュー、同義語、 ユーザー、特権、寸法、ディレクトリ、およびシーケンス。

Oracle データベースをリストアするためのソースとデスティネーション

プライマリストレージまたはセカンダリストレージにあるバックアップコピーから Oracle データベースをリストアすることができます。データベースは、同じデータベースインスタンスの同じ場所にのみリストアできます。ただし、 Real Application Cluster （ RAC ）セットアップでは、データベースを他のノードにリストアできます。

リストア処理のソース

プライマリストレージまたはセカンダリストレージ上のバックアップからデータベースをリストアすることができます。複数ミラー構成でセカンダリストレージ上のバックアップからリストアする場合は、セカンダリストレージミラーをソースとして選択できます。

リストア処理のデスティネーション

データベースは、同じデータベースインスタンスの同じ場所にのみリストアできます。

RAC セットアップでは、クラスタ内の任意のノードから RAC データベースをリストアできます。

特定のプリスクリプトとポストスクリプトをリストアするための事前定義された環境変数

SnapCenter では、データベースのリストア時にプリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。

- データベースをリストアするためにサポートされている定義済み環境変数 *
- * sc_job_ID * は、処理のジョブ ID を指定します。

  例：257

- *SC_ORACLE_SID * はデータベースのシステム識別子を指定します

  複数のデータベースを使用する処理の場合は、パイプで区切られたデータベース名が含まれます。

  例：NFSB31

- *sc_host * は、データベースのホスト名を指定します。

  このパラメータは、アプリケーションボリュームに対して入力されます。

例：scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** は、データベースのオペレーティング・システムの所有者を指定します。

  例： oracle

- * SC_OS_GROUP * はデータベースのオペレーティング・システム・グループを指定します

  例： oinstall

- * SC_backup_name * はバックアップ名です

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例

  - データベースが ARCHIVELOG モードで実行されていない場合： DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1
  - データベースが ARCHIVELOG モードで実行されている場合： DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1 、 Rg2_scspr2417819002_07 -21-2021 、 112.16.48.9267_1 、 Rg2_scspr2417819002_07 -22-2021 、 116.48.9267_1

- * SC_BACKUP ID * はバックアップの ID です

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例

  - データベースが ARCHIVELOG モードで実行されていない場合： DATA @203 | LOG@205
  - データベースが ARCHIVELOG モードで実行されている場合： DATA @203 | LOG @ 205,206,207

- * sc_resource_group_name * で、リソースグループの名前を指定します。

  例：RG1

- **SC_ORACLE_HOME** は Oracle ホーム・ディレクトリのパスを指定します

  例： /ora01/app/oracle/product/18.1.0/db_1

- * SC_RECOVERY_TYPE * はリカバリされるファイルとリカバリ範囲を指定します

  例：
  RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,nologs=false,UntilTime=false,untilscn=false

区切り記号の詳細については、を参照してください "サポートされるデリミタ"。

Oracle データベースをリストアするための要件

Oracle データベースをリストアする前に、前提条件を満たしていることを確認する必要があります。

- リストアとリカバリの戦略を定義しておく必要があります。
- ユーザが Snapshot コピーをミラーまたはバックアップにレプリケートする場合は、ソースボリュームとデスティネーションボリューム両方の Storage Virtual Machine （ SVM ）を SnapCenter 管理者がユーザに割り当てておく必要があります。
- バックアップの一環としてアーカイブログが削除される場合は、必要なアーカイブログのバックアップを手動でマウントしておく必要があります。
- 仮想マシンディスク（ VMDK ）上にある Oracle データベースをリストアする場合は、クローン VMDK を割り当てるための必要な数の空きスロットがゲストマシンにあることを確認してください。
- データベースでセカンダリ保護が有効になっている場合は、そのデータベースに属するすべてのデータボリュームとアーカイブログボリュームが保護されていることを確認する必要があります。
- 制御ファイルまたはフルデータベースのリストアを実行するには、 RAC One Node データベースが「 nomount 」状態であることを確認する必要があります。
- NFS 環境に ASM データベースインスタンスがある場合は、 ASM ディスクパス /var/opt/snapcenter /cu/clones/*/*_ を asm_diskstring パラメータで定義された既存のパスに追加して、リカバリ操作の一環として ASM ログバックアップを正常にマウントする必要があります。
- ASM_diskstring パラメータで、 ASMFD または configure _ORCL ： * _ を使用する場合は、 _AFD ： * _ を設定します。

  asm_diskstring パラメータの編集方法については、を参照してください "asm_diskstring にディスクパスを追加する方法"

- OS 認証を無効にし、 Oracle データベースの Oracle データベース認証を有効にしている場合は、 _$ORACLE_HOME/network/admin_for ASM データベースで使用可能な * listener.ora * ファイルに静的リスナーを設定し、そのデータベースのデータファイルと制御ファイルをリストアする必要があります。
- データベースサイズがテラバイト（ TB ）単位の場合は、 Set-SmConfigSettings コマンドを実行して、 SCORestoreTimeout パラメータの値を増やす必要があります。
- vCenter に必要なすべてのライセンスがインストールされ、最新の状態であることを確認する必要があります。

  ライセンスがインストールされていない場合、または最新の状態でない場合は、警告メッセージが表示されます。警告を無視して続行すると、 RDM からのリストアが失敗します。

- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認してください。詳細については、を参照してください "LUNのデバイスを検出できませんというエラーが表示されて処理に失敗します"。

Oracle データベースのリストアとリカバリを行う

データ損失が発生した場合は、 SnapCenter を使用して 1 つ以上のバックアップからアクティブファイルシステムにデータをリストアし、そのあとにデータベースをリカバリできます。

- 始める前に *

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。

• このタスクについて *

リカバリは、設定したアーカイブログの場所にあるアーカイブログを使用して実行します。データベースがARCHIVELOG モードで実行されている場合、 Oracle データベースは、アーカイブ REDO ログと呼ばれる 1 つ以上のオフラインデスティネーションに、満杯の REDO ログファイルを保存します。SnapCenter は、指定された SCN 、選択された日時、またはすべてのログオプションに基づいて、最適な数のログバックアップを特定してマウントします。
リカバリに必要なアーカイブログが設定済みの場所にない場合は、ログを含む Snapshot コピーをマウントし、外部アーカイブログとしてパスを指定する必要があります。

ASM データベースを ASMlib から ASMFD に移行する場合、 ASMlib で作成されたバックアップは、データベースのリストアには使用できません。ASMFD 構成にバックアップを作成し、これらのバックアップを使用してリストアする必要があります。同様に、 ASM データベースを ASMFD から ASMlib に移行する場合は、リストアする ASMlib 構成にバックアップを作成する必要があります。

データベースをリストアすると、データベースで複数の処理が実行されないように、Oracleデータベースホスト上の_/var/opt/snapcenter/sco/lockディレクトリに運用ロックファイル（.SM_lock_dbsid）が作成されます。処理ロックファイルは、データベースのリストアが完了すると自動的に削除されます。

SPFILE およびパスワード・ファイルのリストアはサポートされていません。

• 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

   データベーストポロジのページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムから * Backups （バックアップ） * を選択します。
5. 表からバックアップを選択し、 * をクリックします *
6. Restore Scope ページで、次のタスクを実行します。

   a. Real Application Clusters （ RAC ）環境でデータベースのバックアップを選択した場合は、 RAC ノードを選択します。

   b. ミラーデータまたはバックアップデータを選択した場合：

      ▪ ミラーまたはボルトにログバックアップがない場合、何も選択されず、ロケータは空です。

      ▪ ミラーまたはバックアップにログバックアップが存在する場合は、最新のログバックアップが選択され、対応するロケータが表示されます。

      選択したログバックアップがミラーとバックアップの場所の両方に存在する場合、両方のロケータが表示されます。

   c. 次の操作を実行します。

リストアの対象	手順
データベースのすべてのデータファイル	「 * すべてのデータファイル * 」を選択します。 データベースのデータファイルのみがリストアされます。制御ファイル、アーカイブログ、または REDO ログファイルはリストアされません。
表領域	[* 表領域 *] を選択します。 リストアする表領域を指定できます。
制御ファイル	「 * 制御ファイル * 」を選択します。 制御ファイルをリストアするときは、ディレクトリ構造が存在するか、または正しいユーザおよびグループの所有権を持つディレクトリ構造が作成されていることを確認してください（存在する場合）。これにより、リストアプロセスによってファイルがターゲットの場所にコピーされるようになります。 ディレクトリが存在しない場合、リストアジョブは失敗します。
REDO ログファイル	[再実行ログファイル] を選択します。 このオプションは、 Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースに対してのみ使用できます。 REDO ログファイルは、 Data Guard 以外のデータベースにはバックアップされません。Data Guard 以外のデータベースの場合、リカバリはアーカイブログを使用して実行されます。
Pluggable Database （ PDB ）	Pluggable Database * を選択し、リストアする PDB を指定します。

リストアの対象	手順
Pluggable Database （ PDB ）の表領域	Pluggable Database （ PDB ） tablespaces * を選択し、リストアする PDB とその PDB の表領域を指定します。 このオプションは、リストア対象に PDB を選択した場合にのみ選択できます。

d. リストアとリカバリに必要な場合は、「 * データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

   データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。リストア処理を実行するために、データベースの状態を高いレベルから低いレベルに変更する必要がある場合は、このチェックボックスをオンにします。リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。

データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある場合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。

a. バックアップ後に新しいデータファイルが追加された場合や、 LUN が LVM ディスクグループに追加、削除、再作成された場合にインプレースリストアを実行するには、 * Force in place restore * を選択します。

7. Recovery Scope ページで、次のアクションを実行します。

状況	手順
最後のトランザクションまでリカバリする場合	[* すべてのログ *] を選択します。
特定の System Change Number （ SCN ）までリカバリする場合	[* Until SCN （ System Change Number ）] を選択します。
特定の日時までリカバリする必要がある	[* 日付と時刻 *] を選択します。 データベースホストのタイムゾーンの日付と時刻を指定する必要があります。
リカバリが不要である場合	「 * リカバリなし * 」を選択します。

状況	手順
外部アーカイブログの場所を指定する	データベースが ARCHIVELOG モードで実行されている場合、 SnapCenter は、指定された SCN 、選択された日時、またはすべてのログオプションに基づいて、最適な数のログバックアップを特定してマウントします。 外部アーカイブログファイルの場所を指定する場合は、 * 外部アーカイブログの場所を指定 * を選択します。 バックアップの一環としてアーカイブログが削除される場合に、必要なアーカイブログのバックアップを手動でマウントしたときは、リカバリのために、マウントしたバックアップのパスを外部アーカイブログの場所として指定する必要があります。 マウントパスを外部のログの場所としてリストする前に、マウントパスのパスと内容を確認する必要があります。 • "ネットアップテクニカルレポート 4591 ：『 Database Data Protection Backup 、 Recovery 、 Replication 、 and DR 』" • "ORA-00308 エラーで処理が失敗します"

アーカイブログボリュームが保護されておらず、データボリュームが保護されている場合は、セカンダリバックアップからリカバリを伴うリストアを実行できません。リストアするには、「 * リカバリなし * 」を選択する必要があります。

オープンデータベースオプションを選択して RAC データベースをリカバリする場合は、リカバリ処理が開始された RAC インスタンスのみがオープン状態に戻ります。

Data Guard スタンバイデータベースおよび Active Data Guard スタンバイデータベースでは、リカバリがサポートされません。

8. PreOps ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

   プリスクリプトは、 _ /var/opt/snapcenter /spl/scripts_path またはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

   スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

   SnapCenter では、プリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。 "詳細はこちら。"

9. PostOps ページで、次の手順を実行します。

   a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。

      ポストスクリプトは、 _ /var/opt/snapcenter /spl/scripts_or のいずれか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

      リストア処理が失敗すると、ポストスクリプトは実行されず、クリーンアップアクティビティが直接トリガーされます。

   b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。

      リカバリ後にデータベースを開くように指定した場合は、制御ファイル付きまたは制御ファイルなしのコンテナデータベース（ CDB ）をリストアしたあと、または CDB 制御ファイルのみをリストアしたあとに CDB のみが開き、 CDB 内の Pluggable Database （ PDB ）は開きません。

      RAC セットアップでは、リカバリに使用される RAC インスタンスのみがリカバリ後に開きます。

      制御ファイル付きのユーザ表領域、制御ファイル付きまたは制御ファイルなしのシステム表領域、あるいは制御ファイル付きまたは制御ファイルなしの PDB をリストアすると、リストア処理に関連する PDB の状態のみが元の状態に変更されます。リストアに使用されなかった他の PDB の状態は保存されていないため、元の状態に変更されません。リストアに使用されなかった PDB の状態は、手動で変更する必要があります。

10. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メール通知を送信するシナリオを選択します。

    また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。実行したリストア処理のレポートを添付する場合は、 [ジョブレポートの添付] を選択する必要があります。

    E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

11. 概要を確認し、 [完了] をクリックします。
12. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

- 詳細はこちら *
- "SnapCenter 処理では、 Oracle RAC One Node データベースがスキップされます"
- "セカンダリの SnapMirror または SnapVault の場所からリストアできませんでした"
- "孤立したインカネーションのバックアップからのリストアに失敗しました"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできます"

ポイントインタイムリカバリを使用した表領域のリストアとリカバリ

データベース内の他の表領域に影響を与えずに、破損または削除された表領域のサブセットをリストアできます。SnapCenter では、 RMAN を使用して表領域のポイントインタイムリカバリ（ PITR ）を実行します。

- 始める前に *
- 表領域の PITR を実行するために必要なバックアップは、カタログ化されてマウントされている必要があります。
- root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。
- このタスクについて *

PITR 操作中に、 RMAN は指定された補助宛先に補助インスタンスを作成します。補助デスティネーションは、マウントポイントまたは ASM ディスクグループです。マウント先に十分なスペースがある場合は、専用のマウントポイントではなく、マウントされた場所の 1 つを再利用できます。

ソースデータベースに表領域がリストアされるように、日時または SCN を指定する必要があります。

ASM 、 NFS 、および SAN 環境上の複数の表領域を選択してリストアできます。たとえば、 TS2 および TS3 の表領域が NFS 上にあり、 TS4 が SAN 上にある場合は、 1 回の PITR 処理ですべての表領域をリストアできます。

RAC セットアップでは、 RAC の任意のノードから表領域の PITR を実行できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、タイプがシングルインスタンス（マルチテナント）のデータベースを選択します。

   データベーストポロジのページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムから * Backups （バックアップ） * を選択します。

   バックアップがカタログ化されていない場合は、バックアップを選択し、 * Catalog * をクリックします。

5. カタログ化されたバックアップを選択し、 * をクリックします  *
6. Restore Scope ページで、次のタスクを実行します。
   a. Real Application Clusters （ RAC ）環境でデータベースのバックアップを選択した場合は、 RAC ノードを選択します。
   b. [* 表領域 *] を選択し、リストアする表領域を指定します。

SYSAUX ' システム ' および UNDO の各テーブルスペースでは 'PITR を実行できません

c. リストアとリカバリに必要な場合は、「 * データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

7. Recovery Scope ページで、次のいずれかを実行します。
   - 特定の System Change Number （ SCN ）までリカバリする場合は、「 * Until SCN * 」を選択し、 SCN と補助のデスティネーションを指定します。
   - 特定の日時にリカバリする場合は、 [* 日付と時刻 * （ * Date and Time * ）] を選択して、日時と補助的な保存先を指定します。

     SnapCenter は、指定されたSCNまたは選択された日時に基づいて、PITRの実行に必要なデータバックアップおよびログバックアップの最適な数を特定してマウントし、カタログ化します。

8. PreOps ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

   プリスクリプトは、 /var/opt/snapcenter /spl/scripts パスまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts パスが読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

   スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

SnapCenter では、プリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。 "詳細はこちら。"

1. PostOps ページで、次の手順を実行します。

   a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。

   リストア処理が失敗すると、ポストスクリプトは実行されず、クリーンアップアクティビティが直接トリガーされます。

   b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。

2. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メール通知を送信するシナリオを選択します。
3. 概要を確認し、 [完了] をクリックします。
4. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

ポイントインタイムリカバリを使用して、プラグイン可能なデータベースをリストアおよびリカバリします

コンテナデータベース（ CDB ）内の他の PDB に影響を与えることなく、破損または破棄された Pluggable Database （ PDB ）をリストアおよびリカバリできます。SnapCenter は、 RMAN を使用して PDB のポイントインタイムリカバリ（ PITR ）を実行します。

- 始める前に *

- PDB の PITR を実行するために必要なバックアップは、カタログ化してマウントする必要があります。

  RAC セットアップでは、 RAC セットアップのすべてのノードの PDB を手動で閉じます（状態を mounted に変更します）。

- root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。
- このタスクについて *

PITR 操作中に、 RMAN は指定された補助宛先に補助インスタンスを作成します。補助デスティネーションは、マウントポイントまたは ASM ディスクグループです。マウント先に十分なスペースがある場合は、専用のマウントポイントではなく、マウントされた場所の 1 つを再利用できます。

PDB の PITR を実行するには、日時または SCN を指定する必要があります。RMAN は、データファイルを含む読み取り / 書き込み、読み取り専用、またはドロップされた PDB をリカバリできます。

リストアとリカバリが可能なのは次の場合だけです。

- 一度に 1 つの PDB
- PDB 内の 1 つの表領域
- 同じ PDB の複数の表領域

RAC セットアップでは、 RAC の任意のノードから表領域の PITR を実行できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、タイプがシングルインスタンス（マルチテナント）のデータベースを選択します。

   データベーストポロジのページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムから * Backups （バックアップ） * を選択します。

   バックアップがカタログ化されていない場合は、バックアップを選択し、 * Catalog * をクリックします。

5. カタログ化されたバックアップを選択し、 * をクリックします  *
6. Restore Scope ページで、次のタスクを実行します。
   a. Real Application Clusters （ RAC ）環境でデータベースのバックアップを選択した場合は、 RAC ノードを選択します。
   b. PDB 内の PDB または表領域をリストアするかどうかに応じて、次のいずれかの操作を実行します。

状況	手順
PDB をリストアします	i. Pluggable Database （ PDB ） * を選択します。 ii. リストアする PDB を指定します。 PDB$SEED データベースで PITR を実行することはできません。
PDB のリストア表領域	i. Pluggable Database （ PDB ） tablespaces * を選択します。 ii. PDB を指定します。 iii. リストアする表領域を 1 つまたは複数指定します。 SYSAUX ' システム ' および UNDO の各テーブルスペースでは 'PITR を実行できません

c. リストアとリカバリに必要な場合は、「 * データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

7. Recovery Scope ページで、次のいずれかを実行します。
   - 特定の System Change Number （ SCN ）までリカバリする場合は、「 * Until SCN * 」を選択し、 SCN と補助のデスティネーションを指定します。
   - 特定の日時にリカバリする場合は、 [* 日付と時刻 * （ * Date and Time * ）] を選択して、日時と補助的な保存先を指定します。

     SnapCenter は、指定されたSCNまたは選択された日時に基づいて、PITRの実行に必要なデータバックアップおよびログバックアップの最適な数を特定してマウントし、カタログ化します。

8. PreOps ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

   プリスクリプトは、 /var/opt/snapcenter /spl/scripts パスまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts パスが読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

   スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

SnapCenter では、プリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。 "詳細はこちら。"

1. PostOps ページで、次の手順を実行します。
   a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。

リストア処理が失敗すると、ポストスクリプトは実行されず、クリーンアップアクティビティが直接トリガーされます。

b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。

RAC セットアップでは、データベースがリカバリされたノードでのみ PDB が開きます。RAC セットアップの他のすべてのノードで、リカバリされた PDB を手動で開く必要があります。

2. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メール通知を送信するシナリオを選択します。
3. 概要を確認し、 [完了] をクリックします。
4. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

UNIX コマンドを使用して Oracle データベースをリストアおよびリカバリする

リストアとリカバリのワークフローには、計画、リストア処理とリカバリ処理の実行、および処理の監視が含まれます。

- このタスクについて *

次のコマンドを実行して、 SnapCenter サーバとの接続を確立し、バックアップをリストしてその情報を取得し、バックアップをリストアする必要があります。

コマンドで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドリファレンスガイド"。

- 手順 *

1. 指定されたユーザ用に SnapCenter サーバとの接続セッションを開始します： *Open-SmConnection*
2. リストアするバックアップに関する情報を取得します： *Get-SmBackup*
3. 指定したバックアップに関する詳細情報を取得します： *Get-SmBackupDetails*

このコマンドは、指定されたバックアップ ID に一致する指定されたリソースのバックアップに関する詳細情報を取得します。情報には、データベース名、バージョン、ホーム、開始 SCN と終了 SCN 、表領域、 Pluggable Database とその表領域などがあります。

4. バックアップからデータをリストアする： *Restore-SmBackup*

Oracle データベースのリストア処理を監視する

Jobs ページを使用して、 SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします リストをフィルタリングして、リストア処理のみを表示します。
   b. 開始日と終了日を指定します。
   c. [* タイプ] ドロップダウン・リストから、 [リストア *] を選択します。
   d. [* Status *] ドロップダウン・リストから、リストア・ステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

Oracle データベースのリストア処理をキャンセルします

キューに格納されているリストアジョブをキャンセルできます。

リストア処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *
- キューに登録されたリストア処理は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、キューに登録されたリ

ストア処理をキャンセルできます。

- キャンセルできないリストア処理の場合、 [ジョブのキャンセル] ボタンは使用できません。
- ロールの作成中に [ユーザー \ グループ] ページで [このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できる] を選択した場合は、そのロールを使用している間に、他のメンバーのキューに登録されているリストア操作をキャンセルできます。
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. ジョブを選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. リストア処理を開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ ジョブの詳細 ］ ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

Oracle データベースのクローニング

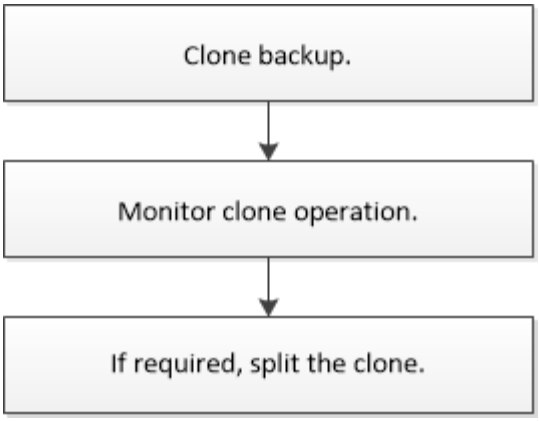
クローニングワークフロー

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

データベースをクローニングする理由には次のものがあります。

- アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のデータベースの構造およびコンテンツを使用してテストするため。
- データの抽出と操作を行うツールを使用してデータウェアハウスにデータを取り込むため。
- 誤って削除または変更されたデータをリカバリするため。

次のワークフローは、クローニング処理の実行順序を示しています。



Oracle データベースのクローニング戦略を定義する

データベースをクローニングする前に戦略を定義しておくと、クローニング処理を確実に成功させることができます。

クローニングでサポートされるバックアップのタイプ

SnapCenter では、 Oracle データベースの各種バックアップのクローニングがサポートされます。

- オンラインデータバックアップ
- オンラインフルバックアップ
- オフラインマウントバックアップ
- オフラインシャットダウンバックアップ
- Data Guard スタンバイデータベースおよび Active Data Guard スタンバイデータベースのバックアップ
- Real Application Clusters （ RAC ）構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ
- Automatic Storage Management （ ASM ）構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ

マルチパス構成ファイルの user_friendy_names オプションが yes に設定されている場合、 SAN 構成はサポートされません。

アーカイブログのバックアップのクローニングはサポートされていません。

Oracle データベースでサポートされるクローニングのタイプ

Oracle データベース環境では、 SnapCenter がデータベースバックアップのクローニングをサポートします。バックアップのクローニングは、プライマリストレージシステムおよびセカンダリストレージシステムから行うことができます。

SnapCenter サーバは、 NetApp FlexClone テクノロジを使用してバックアップをクローニングします。

クローンを更新するには、「 Refresh-SmClone 」コマンドを実行します。このコマンドは、データベースのバックアップを作成し、既存のクローンを削除し、同じ名前でクローンを作成します。

クローンの更新処理は、 UNIX コマンドでのみ実行できます。

Oracle データベースのクローンの命名規則

SnapCenter 3.0 以降では、ファイルシステムのクローンに、 ASM ディスクグループのクローンとは異なる命名規則が使用されます。

- SAN または NFS ファイルシステムの命名規則は、 FileSystemNameofsourcedatabE_CLONESID です。
- ASM ディスクグループの命名規則は、 SC_HASHCODEofDISKGROUP_CLONESID です。

  HASHCODEofDISKGROUP は、 ASM ディスクグループごとに一意の自動生成番号（ 2 ～ 10 桁）です。

Oracle データベースのクローニングの制限

データベースをクローニングする前に、クローニング処理の制限事項を確認しておく必要があります。

- Oracle 11.2.0.4 ～ 12.1.0.1 のいずれかのバージョンを使用している場合、 _renamedg_command の実行時にクローン操作がハング状態になります。この問題を修正するには、 Oracle パッチ 19544733 を適用します。
- ホストに直接接続された LUN （ Windows ホストで Microsoft iSCSI イニシエータを使用した場合など）から、同じ Windows ホストまたは別の Windows ホスト上の VMDK または RDM LUN に、あるいはその逆に、データベースをクローニングすることはできません。
- ボリュームマウントポイントのルートディレクトリを共有ディレクトリにすることはできません。
- クローンが含まれている LUN を新しいボリュームに移動した場合、そのクローンは削除できません。

特定のプリスクリプトおよびポストスクリプトをクローニングするための事前定義された環境変数

SnapCenter では、データベースのクローニング時にプリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。

- データベースを複製するためにサポートされている定義済み環境変数 *
- * SC_ORIGIY_SID * はソース・データベースの SID を指定します

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例：NFSB32

- * SC_original_host * にはソース・ホストの名前を指定します

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例：asmrac1.gdl.englab.netapp.com

- * SC_ORACLE_HOME * は ' ターゲット・データベースの Oracle ホーム・ディレクトリのパスを指定します

  例： /ora01/app/oracle/product/18.1.0/db_1

- * SC_backup_name * 」はバックアップ名です。

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例

  - データベースが ARCHIVELOG モードで実行されていない場合： DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1
  - データベースが ARCHIVELOG モードで実行されている場合： DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | log ： RG2_scspr2417819002_07-020-20-220_1120-216.48.7_1 、RG2_scspr2417819002_07-021 - 202_112.16.48.9267_1 、RG2_scspr2417819002_0.267_2.162.16_2.168.267_2.162.168.267_12.16_2.16_2.168.2.168.267_1
- * sc_av_name * は、アプリケーション・ボリュームの名前を指定します。

  例： AV1|AV2
- * SC_ORIGIY_OS_USER * はソース・データベースのオペレーティング・システムの所有者を指定します

  例： oracle
- * SC_ORIGIY_OS_GROUP * はソース・データベースのオペレーティング・システム・グループを指定します

  例： oinstall
- * SC_TARY_SID * 」はクローン・データベースの SID を指定します。

  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例： clonedb
- * SC_TARGET_HOST* は、データベースをクローニングするホストの名前を指定します。

  このパラメータは、アプリケーションボリュームに対して入力されます。

  例：asmrac1.gdl.englab.netapp.com
- * SC_TARGET_OS_USER * は、クローンデータベースのオペレーティング・システムの所有者を指定します。

  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。

  例： oracle
- * SC_TARGET_OS_GROUP * は、クローンデータベースのオペレーティング・システム・グループを指定します。

  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。

  例： oinstall

- * SC_TARGET_DB_PORT * は、クローンデータベースのデータベースポートを指定します。

  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。

  例： 1521

区切り記号の詳細については、を参照してください "サポートされるデリミタ"。

Oracle データベースをクローニングするための要件

Oracle データベースをクローニングする前に、前提条件を満たしていることを確認する必要があります。

- SnapCenter を使用してデータベースのバックアップを作成しておく必要があります。

  クローニング処理が成功するためには、オンラインデータバックアップとログバックアップ、またはオフライン（マウントまたはシャットダウン）バックアップが正常に作成されている必要があります。

- 制御ファイルまたは REDO ログファイルのパスをカスタマイズする場合は、必要なファイルシステムまたは Automatic Storage Management （ ASM ）ディスクグループを事前にプロビジョニングしておく必要があります。

  デフォルトでは、クローンデータベースの REDO ログおよび制御ファイルは、 ASM ディスクグループ、またはクローンデータベースのデータファイル用に SnapCenter でプロビジョニングされたファイルシステムに作成されます。

- NFS 経由で ASM を使用している場合は、 ASM_diskstring パラメータで定義された既存のパスに /var/opt/snapcenter /scu/clones/*/*_ を追加する必要があります。
- ASM_diskstring パラメータで、 ASMFD または configure _ORCL ： * _ を使用する場合は、 _AFD ： * _ を設定します。

  asm_diskstring パラメータの編集方法については、を参照してください "asm_diskstring にディスクパスを追加する方法"。

- 代替ホストでクローンを作成する場合、代替ホストは次の要件を満たす必要があります。
  - SnapCenter Plug-in for Oracle Database を代替ホストにインストールする必要があります。
  - クローンホストは、プライマリストレージまたはセカンダリストレージから LUN を検出できる必要があります。
    - プライマリストレージまたはセカンダリ（バックアップまたはミラー）ストレージから代替ホストにクローニングする場合は、セカンダリストレージと代替ホストの間に iSCSI セッションが確立されているか、 FC 用に適切にゾーニングされていることを確認してください。
    - バックアップ・ストレージまたはミラー・ストレージから同じホストにクローニングする場合は、バックアップまたはミラー・ストレージとホストの間に iSCSI セッションが確立されているか、 FC 用に適切にゾーニングされているかを確認してください。
    - 仮想環境でクローニングを行う場合は、プライマリストレージまたはセカンダリストレージと、代替ホストをホストする ESX サーバの間で iSCSI セッションが確立されていること、または FC 用に適切にゾーニングされていることを確認してください。
      [+]
      詳細については、を参照してください "Host Utilitiesのマニュアル"。

- ソースデータベースが ASM データベースの場合は、次の手順を実行します。
  - クローンを実行するホスト上で、 ASM インスタンスが稼働している必要があります。
  - クローニングされたデータベースのアーカイブログファイルを専用の ASM ディスクグループに配置する場合は、クローン処理の前に ASM ディスクグループをプロビジョニングする必要があります。
  - データディスクグループの名前は設定できますが、クローンを実行するホスト上の他の ASM ディスクグループでは名前が使用されないようにしてください。

    ASM ディスクグループにあるデータファイルは、 SnapCenter のクローニングワークフローの一環としてプロビジョニングされます。
- NVMeの場合、NVMe utilをインストールする必要があります

- データ LUN の保護タイプと、ミラー、バックアップ、ミラー - ヴォールトなどのログ LUN は、ログバックアップを使用して代替ホストへのクローニング中にセカンダリロケータを検出するために同じである必要があります。
- 12_c_databaseのバックアップをクローニングするためのシードPDB関連情報を取得するには、ソースデータベースのパラメータファイルでexclude_seed_cdb_viewの値をFALSEに設定する必要があります。

  シード PDB とは、 CDB が PDB を作成する際に使用する、システム付属のテンプレートです。シード PDB の名前は PDB$SEED です。PDB$SEED については、 Oracle Doc ID 1940806.1 を参照してください。

  この値は、12_c_databaseをバックアップする前に設定する必要があります。

- SnapCenter は 'autofs サブシステムによって管理されるファイル・システムのバックアップをサポートしますデータベースを複製する場合は ' データ・マウント・ポイントが autofs マウント・ポイントのルートにないことを確認してくださいこれは ' プラグイン・ホストのルート・ユーザには 'autofs マウント・ポイントのルートの下にディレクトリを作成する権限がないためです

  制御ログファイルと REDO ログファイルがデータマウントポイントにある場合は、制御ファイルのパスを変更し、それに応じてログファイルのパスをやり直す必要があります。

  新しいクローン・マウント・ポイントを 'autofs サブシステムに手動で登録できます新しいクローンマウントポイントは自動的には登録されません。

- TDE （自動ログイン）を使用していて、同じホストまたは代替ホスト上にデータベースのクローンを作成する場合は、 /etc/oracle/ウォ レット /$ORACLE_SID_ の下にあるウォレット（キーファイル）をソースデータベースからクローンデータベースにコピーする必要があります。
- Oracle Linux 7 以降または Red Hat Enterprise Linux （ RHEL ） 7 以降の Storage Area Network （ SAN ；ストレージエリアネットワーク）環境でのクローニングを正常に実行するには、の値として、 /etc/lvm/lvmlvm/lvmmetad=0 を設定し、 lvm2-lvmetad サービスを停止する必要があります。
- Oracle データベース 11.2.0.3 以降を使用していて、 NID スクリプトを使用して補助インスタンスのデータベース ID を変更している場合は、 13366202 Oracle パッチをインストールする必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine （ SVM ）に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- NVMeの場合、接続から除外するターゲットポートがあるときは、/var/opt/snapcenter/scu/etc/nvme.conf ファイルにターゲットノード名とポート名を追加します。

ファイルが存在しない場合は、次の例に示すようにファイルを作成する必要があります。

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認してください。詳細については、を参照してください "LUNのデバイスを検出できませんというエラーが表示されて処理に失敗します"。

Oracle データベースバックアップをクローニングする

SnapCenter を使用して、データベースのバックアップを使用して Oracle データベースをクローニングすることができます。

- 始める前に *

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。

- このタスクについて *

クローニング処理では、データベースデータファイルのコピーが作成され、新しいオンライン REDO ログファイルと制御ファイルが作成されます。指定したリカバリ・オプションに基づいて、データベースを指定した時刻までリカバリすることもできます。

Linux ホストで作成されたバックアップを AIX ホストにクローニングしようとすると、クローニングが失敗します。その逆も同様です。

SnapCenter では、 Oracle RAC データベースのバックアップからクローニングした場合にスタンドアロンデータベースが作成されます。SnapCenter では、 Data Guard スタンバイデータベースおよび Active Data Guard スタンバイデータベースのバックアップからのクローニングをサポートしています。

クローニング中に、 SnapCenter は、 SCN または dat に基づいて、リカバリ処理のために最適な数のログバックアップをマウントします。リカバリ後、ログバックアップはアンマウントされます。これらのクローンはすべて、 /var/opt/snapcenter /scu/clones/_ の下にマウントされます。NFS 経由で ASM を使用している場合は、 ASM_diskstring パラメータで定義された既存のパスに /var/opt/snapcenter /scu/clones/*/*_ を追加する必要があります。

SAN 環境で ASM データベースのバックアップをクローニングする際には、クローニングされるホストデバイスの udev ルールが /etc/udev/rules.d/ 999-scu-netapp.rules_ に作成されます。クローニングされるホストデバイスに関連付けられた udev ルールは、クローンを削除すると削除されます。

Flex ASM 設定では、カードの数が RAC クラスタ内のノード数より少ない場合、リーフノードでクローン操作を実行できません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

   データベーストポロジのページが表示されます。
4. [コピーの管理] ビューで、バックアップを [ローカルコピー]（プライマリ）、 [ミラーコピー]（セカンダリ）、または [バックアップコピー]（セカンダリ）から選択します。
5. 表からデータバックアップを選択し、 * をクリックします  *
6. [名前] ページで、次のいずれかの操作を実行します。

状況	手順
データベース（ CDB または CDB 以外）のクローンを作成します。	a. クローンの SID を指定します。 クローンの SID はデフォルトでは使用できず、 SID の最大長は 8 文字です。 クローンを作成するホストに、同じ SID を持つデータベースが存在しないようにします。
Pluggable Database （ PDB ）のクローニング	a. **[PDB Clone]** を選択します。 b. クローニングする PDB を指定します。 c. クローニングされた PDB の名前を指定します。 PDB をクローニングする詳細な手順については、を参照してください "プラグイン可能なデータベースをクローニングします"。

   ミラーデータまたはバックアップデータを選択した場合：

   - ミラーまたはボルトにログバックアップがない場合、何も選択されず、ロケータは空です。
   - ミラーまたはバックアップにログバックアップが存在する場合は、最新のログバックアップが選択され、対応するロケータが表示されます。

     選択したログバックアップがミラーとバックアップの場所の両方に存在する場合、両方のロケータが表示されます。
7. [場所] ページで、次の操作を実行します。

フィールド	手順
ホストをクローニングする	ソースデータベースホストがデフォルトで入力されています。 代替ホスト上にクローンを作成する場合は、ソース・データベース・ホストと同じバージョンの Oracle および OS を持つホストを選択します。
データファイルの場所	データファイルの場所がデフォルトで入力されています。 SAN または NFS ファイルシステムの SnapCenter のデフォルトの命名規則は、FileSystemNameofsourcedatabE_CLONESID です。 ASM ディスクグループの SnapCenter のデフォルトの命名規則は、SC_HASHCODEofDISKGROUP_CLONESID です。HASHCODEofDISKGROUP は、 ASM ディスクグループごとに一意の自動生成番号（ 2 ～ 10 桁）です。 ASM ディスクグループ名をカスタマイズする場合は、 Oracle がサポートする最大長に名前の長さが準拠していることを確認してください。 別のパスを指定する場合は、クローンデータベースのデータファイルマウントポイントまたは ASM ディスクグループ名を入力する必要があります。データファイルパスをカスタマイズする場合は、制御ファイルと REDO ログファイルの ASM ディスクグループ名またはファイルシステムも、データファイルに使用されている名前か、既存の ASM ディスクグループまたはファイルシステムに変更する必要があります。

フィールド	手順
制御ファイル	制御ファイルのパスがデフォルトで入力されています。 制御ファイルは、データファイルと同じ ASM ディスクグループまたはファイルシステムに配置されます。制御ファイルのパスを無効にする場合は、別の制御ファイルのパスを指定します。 ファイルシステムまたは ASM ディスクグループがホストに存在する必要があります。 デフォルトでは、制御ファイルの数はソースデータベースの数と同じになります。制御ファイルの数は変更できますが、データベースをクローニングするには少なくとも 1 つの制御ファイルが必要です。 制御ファイルのパスを、ソースデータベースとは異なるファイルシステム（既存）にカスタマイズできます。

フィールド	手順
REDO ログ	redo ログファイルグループ、パス、およびサイズがデフォルトで入力されています。 REDO ログは、クローンデータベースのデータファイルと同じ ASM ディスクグループまたはファイルシステムに配置されます。REDO ログファイルのパスを上書きする場合は、ソースデータベースとは別のファイルシステムに REDO ログファイルのパスをカスタマイズできます。 新しいファイルシステムまたは ASM ディスクグループがホストに存在する必要があります。 デフォルトでは、 Redo ロググループの数、 Redo ログファイルのサイズはソースデータベースのサイズと同じになります。次のパラメータを変更できます。 • Redo ロググループの数 データベースをクローニングするには、少なくとも 2 つの REDO ロググループが必要です。 • 各グループの REDO ログファイルとそのパス REDO ログファイルのパスを、ソースデータベースとは別のファイルシステム（既存）にカスタマイズできます。 データベースをクローニングするには、 Redo ロググループに少なくとも 1 つの REDO ログファイルが必要です。 • Redo ログファイルのサイズ

8. [Credentials] ページで、次の操作を実行します。

フィールド	手順
sys ユーザのクレデンシャル名	クローンデータベースのシステムユーザパスワードを定義するために使用するクレデンシャルを選択します。 ターゲットホストの sqlnet.ora ファイルで SQLNET.authentication_services が none に設定されている場合は、 SnapCenter GUI で Credential として *None を選択しないでください。
ASM インスタンス資格情報名	クローンホスト上の ASM インスタンスへの接続に対して OS 認証が有効な場合は、「 * なし」を選択します。 それ以外の場合は、「 'sys' 」ユーザまたはクローン・ホストに適用可能な「 'ysasm' 」権限を持つユーザで構成された Oracle ASM クレデンシャルを選択します。

Oracle ホーム、ユーザ名、およびグループの詳細が、ソースデータベースから自動的に入力されます。この値は、クローンを作成するホストの Oracle 環境に基づいて変更できます。

9. PreOps ページで、次の手順を実行します。
   a. クローニング処理の前に実行するプリスクリプトのパスと引数を入力します。

      プリスクリプトは、 _ /var/opt/snapcenter /spl/scripts_or 内のいずれかのフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。

SnapCenter では、プリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。 "詳細はこちら。"

   a. Database Parameter settings セクションで、データベースの初期化に使用される、すでに入力されているデータベースパラメータの値を変更します。

- をクリックすると、パラメータを追加できます + *

Oracle Standard Edition を使用していて、データベースがアーカイブログモードで実行されている場合、またはアーカイブ REDO ログからデータベースをリストアする場合は、パラメータを追加してパスを指定します。

  - LOG_ARCHIVE _ dest の略
  - log_archive_duplex_dest

Fast Recovery Area （ FRA ）は、すでに格納されているデータベースパラメータに定義されていません。関連パラメータを追加することで、 FRA を構成できます。

LOG_ARCHIVE のデフォルト値は $ORACLE_HOME/clone_sid で、クローンデータベースのアーカイブログはこの場所に作成されます。log_archive_dest_1 パラメータを削除した場合、アーカイブ・ログの場所は Oracle によって決定されます。log_archive_dest_1 を編集して、アーカイブ・ログの新しい場所を定義できます。ただし、ファイル・システムまたはディスク・グループが、ホスト上に存在し、使用可能になっている必要があります。

a. [*Reset] をクリックして、データベースパラメータのデフォルト設定を取得します。

1. PostOps ページで、 * Recover database * および * Until Cancel * がデフォルトで選択されて、クローンデータベースのリカバリを実行します。

   SnapCenter は、クローニング用に選択されたデータバックアップ後に、破損していない一連のアーカイブログを含む最新のログバックアップをマウントすることによってリカバリを実行します。セカンダリストレージでクローンを実行するには、プライマリストレージでログとデータのバックアップを実行し、セカンダリストレージでログとデータのバックアップを実行する必要があります。

   SnapCenter が適切なログ・バックアップを検出できない場合は、 [データベースのリカバリ *] および [キャンセルまで *] オプションは選択されません。外部アーカイブログの場所を指定する： * でログバックアップを使用できない場合は、外部アーカイブログの場所を指定します。 *複数のログの場所を指定できます。

   フラッシュリカバリ領域（ FRA ）と Oracle Managed Files （ OMF ）をサポートするように設定されているソースデータベースをクローニングする場合は、リカバリのログデスティネーションも OMF ディレクトリ構造に従っている必要があります。

ソースデータベースが Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースの場合、 PostOps ページは表示されません。Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースの場合、 SnapCenter には SnapCenter GUI でリカバリのタイプを選択するオプションはありませんが、ログを適用せずに、 Cancel リカバリタイプを使用してデータベースをリカバリします。

フィールド名	説明
キャンセルするまで	SnapCenter は、クローニング用に選択されたデータバックアップのあとに、アーカイブログの連続が解除された最新のログバックアップをマウントすることによってリカバリを実行します。 クローンデータベースは、欠落または破損したログファイルまでリカバリされます。
日付と時刻	SnapCenter は、指定された日時までデータベースをリカバリします。指定できる形式は、 mm/dd/yyyy hh:mm:ss です 時刻は 24 時間形式で指定できます。

フィールド名	説明
Until SCN （システム変更番号）	SnapCenter は、指定された System Change Number （ SCN ）までデータベースをリカバリします。
外部アーカイブログの場所を指定します	データベースが ARCHIVELOG モードで実行されている場合、 SnapCenter は、指定した SCN または選択した日時に基づいて、最適な数のログバックアップを特定してマウントします。 外部アーカイブログの場所を指定することもできます。 キャンセルするまでログバックアップを選択した場合、 SnapCenter は自動的にはログバックアップを識別してマウントしません。
新しい DBID を作成します	デフォルトでは、 * 新しい DBID * を作成チェックボックスが選択され、ソース・データベースとは別の、クローン・データベースに一意の番号（ DBID ）が生成されます。 ソースデータベースの DBID をクローンデータベースに割り当てる場合は、このチェックボックスをオフにします。このシナリオでは、ソースデータベースがすでに登録されている外部の RMAN カタログにクローニングされたデータベースを登録する場合に、処理が失敗します。
一時表領域用の tempfile を作成します	クローニングされたデータベースのデフォルトの一時表領域に対して一時ファイルを作成する場合は、チェックボックスをオンにします。 このチェックボックスをオフにすると、 tempfile を使用せずにデータベースクローンが作成されます。
クローン作成時に適用する SQL エントリを入力します	クローン作成時に適用する SQL エントリを追加します。

フィールド名	説明
クローニング処理のあとに実行するスクリプトを入力します	クローニング処理の実行後に実行するポストスクリプトのパスと引数を指定します。 PostScript は /var/opt/snapcenter /spl/scripts_or に保存するか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、/var/opt/snapcenter /spl/scripts_path が読み込まれます。 このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。 クローニング処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップアクティビティは直接トリガーされます。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、 * ジョブレポートの添付 * を選択します。

E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、 [完了] をクリックします。

クローニング処理の一環としてリカバリを実行する場合は、リカバリが失敗してもクローンが作成され、警告が表示されます。このクローンに対して手動リカバリを実行することで、クローンデータベースの整合性を確保できます。

2. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

- 結果 *

データベースをクローニングしたあとにリソースページを更新すると、クローンデータベースが、バックアップに使用できるリソースの 1 つとしてリストに追加されます。クローンデータベースは、標準バックアップワークフローを使用して他のデータベースと同様に保護することも、リソースグループ（新規作成または既存）に含めることもできます。クローニングされたデータベースは、さらにクローニング（クローンのクローニング）が可能です。

クローニング後は、クローンデータベースの名前を絶対に変更しないでください。

クローニング中にリカバリを実行しなかった場合は、不適切なリカバリが原因でクローンデータベースのバックアップが失敗し、手動によるリカバリが必要になることがあります。また、アーカイブログが格納されたデフォルトの場所がネットアップ以外のストレージにある場合や、ストレージシステムに SnapCenter が設定されていない場合も、ログバックアップが失敗することがあります。

AIX のセットアップでは、 lkdev コマンドを使用して、クローニングされたデータベースが存在するディスクの名前をロックし、 rendev コマンドを使用して変更できます。

デバイスをロックしたり名前を変更したりしても、クローンの削除処理には影響しません。SAN デバイス上に構築された AIX LVM レイアウトの場合、クローニングされた SAN デバイスではデバイスの名前変更はサポートされません。

- 詳細はこちら *
- "リストアまたはクローニングが失敗して ORA-00308 エラーメッセージが表示されます"
- "クローンデータベースをリカバリできませんでした"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできます"

プラグイン可能なデータベースをクローニングします

プラグイン可能なデータベース（ PDB ）を、同じホストまたは代替ホスト上にある別のターゲット CDB にクローニングすることができます。クローニングした PDB を目的の SCN または日時にリカバリすることもできます。

- 始める前に *

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] または [* リソースグループ *] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、タイプがシングルインスタンス（マルチテナント）のデータベースを選択します。

   データベーストポロジのページが表示されます。

4. [コピーの管理] ビューで、バックアップを [ローカルコピー]（プライマリ）、 [ミラーコピー]（セカンダリ）、または [バックアップコピー]（セカンダリ）から選択します。
5. 表からバックアップを選択し、 * をクリックします  *
6. [名前] ページで、次の操作を実行します。
   a. [**PDB Clone**] を選択します。

b. クローニングする PDB を指定します。

一度にクローニングできる PDB は 1 つだけです。

c. クローン PDB の名前を指定します。

7. [場所] ページで、次の操作を実行します。

フィールド	手順
ホストをクローニングする	ソースデータベースホストがデフォルトで入力されています。 代替ホスト上にクローンを作成する場合は、ソース・データベース・ホストと同じバージョンの Oracle および OS を持つホストを選択します。
ターゲット CDB	クローニングされた PDB を含める CDB を選択します。 ターゲット CDB が実行されていることを確認します。
データベースの状態	PDB を読み取り / 書き込みモードで開く場合は、「 * クローン PDB を読み取り / 書き込みモードで開く」チェックボックスをオンにします。

データファイルの場所	データファイルの場所がデフォルトで入力されています。 SAN または NFS ファイルシステムの SnapCenter のデフォルトの命名規則は、FileSystemNameofsourcedatabE_SCJOBID です。 ASM ディスクグループの SnapCenter のデフォルトの命名規則は、SC_HASHCODEofDISKGROUP_SCJOBID です。HASHCODEofDISKGROUP は、 ASM ディスクグループごとに一意の自動生成番号（ 2 ～ 10 桁）です。 ASM ディスクグループ名をカスタマイズする場合は、 Oracle がサポートする最大長に名前の長さが準拠していることを確認してください。 別のパスを指定する場合は、クローンデータベースのデータファイルマウントポイントまたは ASM ディスクグループ名を入力する必要があります。

Oracle ホーム、ユーザ名、およびグループの詳細が、ソースデータベースから自動的に入力されます。この値は、クローンを作成するホストの Oracle 環境に基づいて変更できます。

8. PreOps ページで、次の手順を実行します。

   a. クローニング処理の前に実行するプリスクリプトのパスと引数を入力します。

      プリスクリプトは /var/opt/snapcenter /spl/scripts またはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts パスが読み込まれます。このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。

   SnapCenter では、プリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。 "詳細はこちら。"

   a. 補助 CDB クローンデータベースのパラメータ設定セクションで、データベースの初期化に使用される、すでにデータが格納されているデータベースパラメータの値を変更します。

9. [*Reset] をクリックして、データベースパラメータのデフォルト設定を取得します。
10. PostOps ページで、 * Until Cancel * がデフォルトで選択され、クローンデータベースのリカバリを実行します。

    SnapCenter が適切なログ・バックアップを見つけられない場合は、 * Until Cancel * オプションは選択されません。外部アーカイブログの場所を指定する： * でログバックアップを使用できない場合は、外部アーカイブログの場所を指定します。 *複数のログの場所を指定できます。

フラッシュリカバリ領域（ FRA ）と Oracle Managed Files （ OMF ）をサポートするように設定されているソースデータベースをクローニングする場合は、リカバリのログデスティネーションも OMF ディレクトリ構造に従っている必要があります。

フィールド名	説明
キャンセルするまで	SnapCenter は、クローニング用に選択されたデータバックアップのあとに、アーカイブログの連続が解除された最新のログバックアップをマウントすることによってリカバリを実行します。 セカンダリストレージでクローンを実行するには、プライマリストレージでログとデータのバックアップを実行し、セカンダリストレージでログとデータのバックアップを実行する必要があります。 クローンデータベースは、欠落または破損したログファイルまでリカバリされます。
日付と時刻	SnapCenter は、指定された日時までデータベースをリカバリします。 時刻は 24 時間形式で指定できます。
Until SCN （システム変更番号）	SnapCenter は、指定された System Change Number （ SCN ）までデータベースをリカバリします。
外部アーカイブログの場所を指定します	外部アーカイブログの場所を指定します。
新しい DBID を作成します	デフォルトでは、補助クローンデータベースに対して新しい DBID * を作成チェック・ボックスは選択されません。 補助クローンデータベースとソースデータベースを区別するために一意の番号（ DBID ）を生成する場合は、このチェックボックスを選択します。
一時表領域用の tempfile を作成します	クローニングされたデータベースのデフォルトの一時表領域に対して一時ファイルを作成する場合は、チェックボックスをオンにします。 このチェックボックスをオフにすると、 tempfile を使用せずにデータベースクローンが作成されます。
クローン作成時に適用する SQL エントリを入力します	クローン作成時に適用する SQL エントリを追加します。

フィールド名	説明
クローニング処理のあとに実行するスクリプトを入力します	クローニング処理の実行後に実行するポストスクリプトのパスと引数を指定します。 PostScript は /var/opt/snapcenter /spl/scripts_or に保存するか、このパス内の任意のフォルダに保存する必要があります。 デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。 クローニング処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップアクティビティは直接トリガーされます。

11. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

    また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、 * ジョブレポートの添付 * を選択します。

    E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、 [完了] をクリックします。
2. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

- 終了後 *

クローニングされた PDB のバックアップを作成する場合は、クローン PDB のみをバックアップできないため、 PDB がクローニングされたターゲット CDB をバックアップしてください。セカンダリ関係を使用してバックアップを作成する場合は、ターゲット CDB のセカンダリ関係を作成する必要があります。

RAC セットアップでは、クローニングされた PDB のストレージは、 PDB クローンが実行されたノードにのみ接続されます。RAC の他のノードの PDB はマウント状態です。クローニングした PDB に他のノードからアクセスできるようにするには、その PDB を他のノードに手動で接続してください。

- 詳細はこちら *
- "リストアまたはクローニングが失敗して ORA-00308 エラーメッセージが表示されます"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできます"

UNIX コマンドを使用して Oracle データベースバックアップをクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

- このタスクについて *

次のコマンドを実行して、 Oracle データベースのクローン仕様ファイルを作成し、クローニング処理を開始する必要があります。

コマンドで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドリファレンスガイド"。

- 手順 *

1. 指定したバックアップから Oracle データベースのクローン仕様を作成します： *New-SmOracleCloneSpecification*

   セカンダリデータ保護ポリシーが Unified mirror-vault の場合は、 -IncludeSecondaryDetails のみを指定します。SecondaryStorageType を指定する必要はありません。

   このコマンドは、指定したソースデータベースとそのバックアップに対して、 Oracle データベースのクローン仕様ファイルを自動的に作成します。作成するクローンデータベースに対して自動的に生成される値がこの仕様ファイルに取り込まれるようにするために、クローンデータベースの SID も指定する必要があります。

   クローン仕様ファイルは、 /var/opt/snapcenter /sca/clone_specs__ に作成されます。

2. クローンリソースグループまたは既存のバックアップからクローン処理を開始する： *New-SmClone*

   このコマンドによってクローニング処理が開始されます。クローニング処理では、 Oracle クローン仕様ファイルのパスも指定する必要があります。リカバリオプション、クローニング処理が実行されるホスト、プリスクリプト、ポストスクリプト、およびその他の詳細を指定することもできます。

デフォルトでは、クローンデータベースのアーカイブログデスティネーションファイルには、 *$ORACLE_HOME/clone_SID* が自動的に入力されます。

Oracle データベースクローンをスプリットします

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

- このタスクについて *
- 中間のクローンに対してクローンスプリット処理を実行することはできません。

  たとえば、データベースバックアップから clone1 を作成したあとで、 Clone1 のバックアップを作成し、そのバックアップ（ Clone2 ）をクローニングできます。Clone2 を作成すると、 clone1 は中間クローンであり、 clone1 でクローンスプリット処理を実行することはできません。ただし、 Clone2 でクローンスプリット処理を実行することはできます。

Clone2 をスプリットしたあとは、 clone1 が中間クローンではなくなるため、 clone1 でクロームスプリット処理を実行できます。

- クローンをスプリットすると、クローンのバックアップコピーが削除されます。
- クローンスプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。
- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。
3. クローニングされたリソース（データベースや LUN など）を選択し、をクリックします  。
4. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   SMCore サービスが再起動され、クローンスプリット処理が実行されたデータベースがリソースページにクローンとして表示される場合、クローンスプリット処理が停止します。_Stop-SmJob_cmdlet を実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

   クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、 SMCoreServiceHost.exe.config ファイルの CloneSplitStatusCheckPollTime パラメータの値を変更して、クローンスプリット処理のステータスをポーリングする SMCore の時間間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

   例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、またはその他のクローンスプリットの実行中は、クローンスプリットの開始処理が失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

プラグイン可能なデータベースのスプリットクローン

SnapCenter を使用して、クローニングされた Pluggable Database （ PDB ）をスプリットできます。

- このタスクについて *

PDB がクローニングされたターゲット CDB のバックアップを作成した場合は、 PDB クローンをスプリットすると、クローン PDB を含むターゲット CDB のすべてのバックアップからもクローニングされた PDB が削除されます。

PDB クローンは、インベントリビューやリソースビューに表示されません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースまたはリソースグループのビューからソースコンテナデータベース（ CDB ）を選択します。
3. [コピーの管理] ビューで ' プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージ・システムから [クローン *] を選択します
4. PDB クローン（ targetCDB ： PDBClone ）を選択し、をクリックします  。
5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

Oracle データベースのクローニング処理を監視する

Jobs ページを使用して、 SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました

- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします  をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
   b. 開始日と終了日を指定します。
   c. [**Type**](タイプ **)** ドロップダウンリストから **'[*Clone**](クローン *) を選択します
   d. [* Status *] ドロップダウン・リストから、クローンのステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。

4. クローンジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ジョブの詳細］ページで、 ［ * ログの表示 * ］ をクリックします。

クローンをリフレッシュします

クローンを更新するには、 *Refresh-SmClone* コマンドを実行します。このコマンドは、データベースのバックアップを作成し、既存のクローンを削除し、同じ名前でクローンを作成します。

PDB クローンは更新できません。

- 必要なもの *
- スケジュールされたバックアップが有効になっていない状態で、オンラインフルバックアップまたはオフラインデータバックアップポリシーを作成します。
- バックアップエラーのみに関する E メール通知をポリシーで設定します。
- オンデマンドバックアップの保持数を適切に定義して、不要なバックアップがないことを確認します。
- 更新クローン処理で特定されるリソースグループには、オンラインフルバックアップまたはオフラインデータバックアップポリシーのみが関連付けられていることを確認します。
- データベースが 1 つだけのリソースグループを作成する。
- clone refresh コマンドに対して cron ジョブが作成される場合は、 SnapCenter スケジュールおよび cron スケジュールがデータベースリソースグループに対して重複しないようにしてください。

  clone refresh コマンド用に作成された cron ジョブの場合、 24 時間ごとに Open-SmConnection を実行してください。

- クローンの SID がホストで一意であることを確認します。

  複数の更新クローン処理で同じクローン仕様ファイルを使用する場合、または同じクローン SID を持つクローン仕様ファイルを使用する場合は、ホスト上で SID を持つ既存のクローンが削除され、そのクローンが作成されます。

- セカンダリ・バックアップを使用してクローンを作成するには ' バックアップ・ポリシーがセカンダリ保護で有効になっていること ' およびクローン仕様ファイルが作成されていることを確認してください
  - プライマリクローン仕様ファイルを指定し、ポリシーでセカンダリ更新オプションを選択した場合、バックアップが作成され、セカンダリに更新が転送されます。ただし、クローンはプライマリバックアップから作成されます。
  - プライマリクローン仕様ファイルを指定し、ポリシーでセカンダリ更新オプションが選択されていない場合、プライマリ上にバックアップが作成され、プライマリからクローンが作成されます。
- 手順 *

1. 指定されたユーザ用に SnapCenter サーバとの接続セッションを開始します： *Open-SmConnection*
2. 指定したバックアップから Oracle データベースのクローン仕様を作成します： *New-SmOracleCloneSpecification*

セカンダリデータ保護ポリシーが Unified mirror-vault の場合は、 -IncludeSecondaryDetails のみを指定します。SecondaryStorageType を指定する必要はありません。

このコマンドは、指定したソースデータベースとそのバックアップに対して、 Oracle データベースのクローン仕様ファイルを自動的に作成します。作成するクローンデータベースに対して自動的に生成される値がこの仕様ファイルに取り込まれるようにするために、クローンデータベースの SID も指定する必要があります。

クローン仕様ファイルは、 /var/opt/snapcenter /sca/clone_specs__ に作成されます。

3. Run_Refresh - SmClone_ 。

"PL-SCO-20032: CanExecute 操作がエラーで失敗した場合 : PL-SCO-300331: Redo ログファイル +SC_2959770772_clmdb/clredolog/redo01_01.log Exist" エラーメッセージが表示されたときに、操作が失敗した場合は、 -WaitToTriggerClone_" に高い値を指定してください。

UNIX コマンドの詳細については、を参照してください "SnapCenter ソフトウェアコマンドリファレンスガイド"。

プラグイン可能なデータベースのクローンを削除します

不要になった Pluggable Database （ PDB ）のクローンは削除できます。

PDB がクローニングされたターゲット CDB のバックアップを作成した場合、 PDB クローンを削除すると、クローン PDB もターゲット CDB のバックアップから削除されます。

PDB クローンは、インベントリビューやリソースビューに表示されません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースまたはリソースグループのビューからソースコンテナデータベース（ CDB ）を選択します。
3. [コピーの管理] ビューで ' プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージ・システムから [クローン *] を選択します
4. PDB クローン（ targetCDB ： PDBClone ）を選択し、をクリックします 。
5. [OK] をクリックします。

アプリケーションボリュームを管理する

アプリケーションボリュームを追加します

SnapCenter では、 Oracle データベースのアプリケーションボリュームのバックアップとクローニングがサポートされます。アプリケーションボリュームは手動で追加する必要があります。アプリケーションボリュームの自動検出はサポートされていません。

アプリケーションボリュームでは、直接NFS接続と直接iSCSI接続のみがサポートされます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
2. [アプリケーションボリュームの追加] をクリックします。
3. [名前] ページで、次の操作を実行します。
   - Name フィールドに、アプリケーションボリュームの名前を入力します。
   - Host Name フィールドに、ホストの名前を入力します。
4. ストレージ容量ページで、ストレージシステムの名前を入力し、 1 つ以上のボリュームを選択して、関連付けられている LUN または qtree を指定します。

   複数のストレージシステムを追加できます。
5. 概要を確認し、 [完了] をクリックします。
6. [リソース] ページで、 **View** リストから * アプリケーションボリューム * を選択すると、追加したすべてのアプリケーションボリュームが表示されます。

アプリケーションボリュームを変更します

バックアップが作成されていない場合は、アプリケーションボリュームの追加時に指定したすべての値を変更できます。バックアップが作成されている場合は、ストレージシステムの詳細だけを変更できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* アプリケーションボリューム *] を選択します。
3. をクリックします  をクリックして値を変更します。

アプリケーションボリュームを削除します

アプリケーションボリュームを削除する際、アプリケーションボリュームに関連付けられたバックアップがあると、アプリケーションボリュームはメンテナンスモードになり、新しいバックアップは作成されず、それ以前のバックアップは保持されません。関連付けられているバックアップがない場合は、すべてのメタデータが削除されます。

必要に応じて、 SnapCenter で削除処理を元に戻すことができます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* アプリケーションボリューム *] を選択します。
3. をクリックします  をクリックして値を変更します。

アプリケーションボリュームのバックアップ

アプリケーションボリュームをバックアップ

アプリケーションボリュームがどのリソースグループにも含まれていない場合は、リソースページからアプリケーションボリュームをバックアップできます。

- このタスクについて *

デフォルトでは、整合グループ（ CG ）バックアップが作成されます。ボリュームベースのバックアップを作成する場合は、 _web.config ファイルで **EnableOracleNdvVolumeBasedBackup** の値を true に設定する必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* アプリケーションボリューム *] を選択します。
3. * をクリックします* をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。

   次に、 * をクリックします* をクリックすると、フィルタペインが閉じます。
4. バックアップするアプリケーションボリュームを選択します。

   Application volume-Protect ページが表示されます。
5. リソースページで、次の操作を実行します。

フィールド	手順
Snapshot コピーには、カスタムの名前形式を使用します	Snapshot コピー名にカスタムの名前形式を使用する場合は、このチェックボックスをオンにして名前形式を入力します。 たとえば 'customText_policy_hostname や resource_hostname などですデフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。
バックアップからアーカイブログデスティネーションを除外します	バックアップの対象から外すアーカイブログファイルのデスティネーションを指定します。

6. [Policies] ページで、次の手順を実行します。
   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

   また、 * をクリックしてポリシーを作成することもできます *

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

b. をクリックします  スケジュールを設定するポリシーの Configure Schedules （スケジュールの設定）列。

c. [Add schedules for policy_name] ウィンドウで、スケジュールを設定し、 [**OK**] をクリックします。

_policy_name_は 、選択したポリシーの名前です。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

7. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。リソース上で実行されたバックアップ処理のレポートを添付する場合は、 [ジョブレポートの添付] を選択します。

E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、 [完了] をクリックします。

アプリケーションボリュームのトポロジページが表示されます。

2. [今すぐバックアップ] をクリックします。
3. Backup （バックアップ）ページで、次の手順を実行します。
   a. リソースに複数のポリシーを適用している場合は、「 * Policy * 」ドロップダウン・リストから、バックアップに使用するポリシーを選択します。
   b. [バックアップ] をクリックします。
4. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

アプリケーションボリュームのリソースグループをバックアップします

アプリケーションボリュームのみ、またはアプリケーションボリュームとデータベースが混在しているリソースグループをバックアップできます。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースを対象に実行されます。

リソースグループに複数のアプリケーションボリュームが含まれている場合は、すべてのアプリケーションボリュームに SnapMirror または SnapVault のレプリケーションポリシーを適用する必要があります。

- このタスクについて *

デフォルトでは、整合グループ（ CG ）バックアップが作成されます。ボリュームベースのバックアップを作成する場合は、 _web.config ファイルで **EnableOracleNdvVolumeBasedBackup** の値を true に設定する必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。

   リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 * をクリックします* をクリックし、タグを選択します。次に、 * をクリックします* をクリックすると、フィルタペインが閉じます。
3. [リソースグループ] ページで、バックアップするリソースグループを選択し、 [今すぐバックアップ *] をクリックします。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。
   b. [バックアップ] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   検証処理はデータベースに対してのみ実行され、アプリケーションボリュームに対しては実行されません。

アプリケーションボリュームのバックアップをクローニングする

SnapCenter を使用して、アプリケーションボリュームのバックアップをクローニングできます。

- 始める前に *

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプトディレクトリとポストスクリプトディレクトリに手動で割り当てる必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* アプリケーションボリューム *] を選択します。
3. アプリケーションボリュームの詳細ビューまたはリソースグループの詳細ビューでアプリケーションボリュームを選択します。

   アプリケーションボリュームのトポロジページが表示されます。
4. [コピーの管理] ビューで、バックアップを [ローカルコピー] （プライマリ）、 [ミラーコピー] （セカンダリ）、または [バックアップコピー] （セカンダリ）から選択します。

5. 表からバックアップを選択し、 * をクリックします *
6. Location ページで、次のアクションを実行します。

フィールド	手順
プラグインホスト	クローンを作成するホストを選択します。
ターゲットリソース名	リソース名を指定します。

7. Scripts ページで、クローニング前に実行するスクリプトの名前、ファイルシステムをマウントするコマンド、およびクローニング後に実行するスクリプトの名前を指定します。
8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、 * ジョブレポートの添付 * を選択します。

   E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、 [完了] をクリックします。

アプリケーションボリュームクローンをスプリットします

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* アプリケーションボリューム *] を選択します。
  3. クローニングされたリソースを選択し、をクリックします 。
  4. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
  5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

アプリケーションボリュームのクローンを削除する

不要になったクローンは削除できます。他のクローンのソースと同様に機能するクローンは削除できません。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから Oracle データベースプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* アプリケーションボリューム *] を選択します。
  3. リストからリソースまたはリソースグループを選択します。

リソースまたはリソースグループのトポロジページが表示されます。

4. [コピーの管理] ビューで ' プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージ・システムから [クローン *] を選択します
5. クローンを選択し、をクリックします  。
6. Delete Clone ページで、次の操作を実行します。
   a. [* Preclone delete *] フィールドに、クローンを削除する前に実行するスクリプトの名前を入力します。
   b. Unmount * フィールドで、クローンを削除する前にクローンをアンマウントするコマンドを入力します。
7. [OK] をクリックします。

Windows ファイルシステムを保護

SnapCenter Plug-in for Microsoft Windows の概念

SnapCenter Plug-in for Microsoft Windows の概要を参照してください

SnapCenter Plug-in for Microsoft Windows は、 Microsoft ファイルシステムリソースに対してアプリケーション対応のデータ保護管理を可能にする、 NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。また、 Windows ファイルシステムのストレージのプロビジョニング、整合性のある Snapshot コピーの作成、およびスペースの再生が可能です。Plug-in for Windows を使用することで、 SnapCenter 環境でのファイルシステムのバックアップ、リストア、およびクローニングの処理を自動化できます。

Plug-in for Windows がインストールされている場合は、 SnapCenter で NetApp SnapMirror テクノロジを使用して別のボリュームにバックアップセットのミラーコピーを作成できるほか、 NetApp SnapVault テクノロジを使用してアーカイブや標準への準拠を目的としたディスクツーディスクバックアップレプリケーションを実行できます。

SnapCenter Plug-in for Microsoft Windows の機能

Plug-in for Windows をインストールした環境では、 SnapCenter を使用して Windows ファイルシステムのバックアップ、リストア、クローニングを実行することができます。これらの処理をサポートするタスクを実行することもできます。

- リソースの検出
- Windows ファイルシステムのバックアップ
- バックアップ処理のスケジュールを設定します
- ファイルシステムのバックアップをリストア
- ファイルシステムのバックアップをクローニングする
- バックアップ、リストア、クローニングの各処理を監視する

Plug-in for Windows では、 SMB 共有のファイルシステムのバックアップとリストアはサポートされていません。

SnapCenter Plug-in for Windows の特長

Plug-in for Windows は、ストレージシステム上でネットアップの Snapshot コピーテクノロジと統合されます。Plug-in for Windows の操作には、 SnapCenter インターフェイスを使用します。

Plug-in for Windows の主な機能は次のとおりです。

- * SnapCenter * による統一されたグラフィカル・ユーザー・インターフェイス

SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter インターフェイスを使用すると、すべてのプラグインでバックアッププロセスとリストアプロセスを一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（ RBAC ）を設定したり、ジョブを監視したりすることができます。SnapCenter では、バックアップ処理とクローニング処理に対応したスケジュールとポリシーの一元管理も可能です。

- * 中央管理の自動化 *

  日常的なファイルシステムのバックアップのスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理をセットアップしたりできます。SnapCenter から E メールアラートを送信するように設定して、ファイルシステム環境をプロアクティブに監視することもできます。

- * 無停止の NetApp Snapshot コピー・テクノロジー *

  Plug-in for Windows では、ネットアップの Snapshot コピーテクノロジを使用しています。これにより、ファイルシステムを数秒でバックアップし、ホストをオフラインにすることなく迅速にリストアすることが可能です。Snapshot コピーはストレージスペースを最小限しか消費しません。

Plug-in for Windows には、上記の主要な機能以外にも次のようなメリットがあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます
- NetApp FlexClone テクノロジを使用して、本番用ファイルシステムのスペース効率に優れたコピーを作成し、テストまたはデータの抽出を行います

  FlexClone のライセンス情報については、を参照してください "SnapCenter ライセンス"。

- 複数のサーバで同時に複数のバックアップを実行できます
- PowerShell コマンドレットを使用して、バックアップ、リストア、クローニングの各処理のスクリプトを作成できます
- ファイルシステムと仮想マシンディスク（ VMDK ）のバックアップがサポートされます。
- 物理インフラと仮想インフラがサポートされます
- iSCSI 、ファイバチャネル、 FCoE 、 raw デバイスマッピング（ RDM ）、非対称 LUN マッピング（ ALM ）、 NFS および VMFS 経由の VMDK 、および仮想 FC がサポートされます

SnapCenter での Windows ファイルシステムのバックアップ方法

SnapCenter では、 Snapshot コピーテクノロジを使用して Windows ファイルシステムのリソースがバックアップされます。これには、 Windows クラスタの LUN 、 CSV （クラスタ共有ボリューム）、 RDM （ raw デバイスマッピング）ボリューム、 ALM （非対称 LUN マッピング）、および VMFS / NFS （ NFS を使用する VMware Virtual Machine File System ）に基づく VMDK にあるリソースが含まれます。

SnapCenter は、ファイルシステムの Snapshot コピーを作成することによってバックアップを作成します。ボリュームに複数のホストの LUN が含まれている場合は、フェデレーテッドバックアップを使用すると、各 LUN を個別にバックアップするよりも迅速かつ効率的に処理できます。ボリュームの Snapshot コピーを 1 つだけ作成すれば、各ファイルシステムの Snapshot を個別に作成しなくても済むからです。

SnapCenter で作成される Snapshot コピーには、ストレージシステムボリューム全体がキャプチャされます。ただし、バックアップは、バックアップが作成されたホストサーバに対してのみ有効になります。

他のホストサーバのデータが同じボリュームに含まれている場合、それらのデータを Snapshot コピーからリストアすることはできません。

Windows ファイルシステムにデータベースが含まれている場合、ファイルシステムをバックアップしてもデータベースがバックアップされるわけではありません。データベースをバックアップするには、いずれかのデータベースプラグインを使用する必要があります。

SnapCenter Plug-in for Microsoft Windows でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシンの両方でさまざまなストレージタイプをサポートしています。ホストに対応したパッケージをインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

Windows Server では、 SnapCenter プロビジョニングとデータ保護がサポートされます。サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
物理サーバ	FC 接続 LUN	SnapCenter のグラフィカルユーザインターフェイス（ GUI ）または PowerShell コマンドレット	
物理サーバ	iSCSI で接続された LUN	SnapCenter GUI または PowerShell コマンドレット	
物理サーバ	Storage Virtual Machine （ SVM ）上の SMB3 （ CIFS ）共有	SnapCenter GUI または PowerShell コマンドレット	プロビジョニングのみがサポートされます。 SnapCenter プロトコルを使用してデータや共有をバックアップすることはできません。
VMware VM	FC または iSCSI HBA で接続された RDM LUN	PowerShell コマンドレット	
VMware VM	iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN	SnapCenter GUI または PowerShell コマンドレット	

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
VMware VM	Virtual Machine File Systems （ VMFS ）または NFS データストア	VMware vSphere の場合	
VMware VM	SVM 上の SMB3 共有に接続されたゲストシステム	SnapCenter GUI または PowerShell コマンドレット	プロビジョニングのみがサポートされます。 SnapCenter プロトコルを使用してデータや共有をバックアップすることはできません。
Hyper-V VM	仮想ファイバチャネルスイッチで接続された仮想 FC （ vFC ） LUN	SnapCenter GUI または PowerShell コマンドレット	仮想ファイバチャネルスイッチで接続された仮想 FC （ vFC ） LUN のプロビジョニングには、 Hyper-V Manager を使用する必要があります。 Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （ x ）でのデータベースのバックアップはサポートされていません。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
Hyper-V VM	iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN	SnapCenter GUI または PowerShell コマンドレット	Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （x）でのデータベースのバックアップはサポートされていません。
Hyper-V VM	SVM 上の SMB3 共有に接続されたゲストシステム	SnapCenter GUI または PowerShell コマンドレット	プロビジョニングのみがサポートされます。 SnapCenter プロトコルを使用してデータや共有をバックアップすることはできません。 Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （x）でのデータベースのバックアップはサポートされていません。

Windows プラグインに必要な最小限の ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
event generate-autosupport-log を指定します
ジョブ履歴の表示 ジョブが停止しました
LUN lun create をクリックします lun delete LUN igroup add lun igroup create を追加します lun igroup delete LUN igroup の名前を変更します lun igroup show を参照してください LUN マッピングの追加 - レポートノード LUN マッピングが作成されます LUN マッピングが削除されます LUN マッピングの削除 - レポートノード lun mapping show lun modify を追加します LUN のボリューム内移動 LUN はオフラインです LUN はオンラインです LUN のサイズ変更 LUN シリアル lun show をクリックします

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SnapMirror ポリシー追加ルール snapmirror policy modify-rule snapmirror policy remove-rule 」を実行します snapmirror policy show の略 SnapMirror リストア snapmirror show の略 snapmirror show -history の略 SnapMirror の更新 SnapMirror の update-ls-set snapmirror list-destinations
バージョン

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
volume clone create を実行します
volume clone show を実行します
ボリュームクローンスプリット開始
ボリュームクローンスプリットは停止します
volume create を実行します
ボリュームを削除します
volume file clone create を実行します
volume file show-disk-usage
ボリュームはオフラインです
ボリュームはオンラインです
volume modify を使用します
volume qtree create を実行します
volume qtree delete
volume qtree modify の略
volume qtree show の略
ボリュームの制限
volume show のコマンドです
volume snapshot create を実行します
ボリューム Snapshot の削除
volume snapshot modify の実行
ボリューム Snapshot の名前が変更されます
ボリューム Snapshot リストア
ボリューム Snapshot の restore-file
volume snapshot show の実行
ボリュームのアンマウント

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SVM CIFS です
vserver cifs share create の場合
SVM CIFS 共有が削除されます
vserver cifs shadowcopy show
vserver cifs share show のコマンドです
vserver cifs show のコマンドです
SVM エクスポートポリシー
vserver export-policy create を参照してください
vserver export-policy delete
vserver export-policy rule create
vserver export-policy rule show
vserver export-policy show のコマンドを入力します
Vserver iSCSI
vserver iscsi connection show
vserver show のコマンドです

読み取り専用コマンド： **ONTAP 8.3.0** 以降で必要な最小権限
Network Interface の略
network interface show の略
Vserver

SnapMirror レプリケーションと **SnapVault** レプリケーションのためのストレージシステムを準備

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenter は、Snapshotコピー処理の完了後に、SnapMirrorとSnapVault に対する更新を実行します。SnapMirror更新とSnapVault 更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SnapCenter は * sync-mirror * レプリケーションをサポートしていません。

Windows ファイルシステムのバックアップ戦略を定義する

バックアップを作成する前にバックアップ戦略を定義しておくと、ファイルシステムの正常なリストアやクローニングに必要なバックアップを作成できます。バックアップ戦略の大部分は、サービスレベルアグリーメント（ SLA ）、目標復旧時間（ RTO ）、および目標復旧時点（ RPO ）によって決まります。

SLA では、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処するために必要なサービスレベルを定義します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA 、 RTO 、および RPO は、データ保護戦略に関与します。

Windows ファイルシステムのバックアップスケジュール

バックアップ頻度はポリシーで指定され、バックアップスケジュールはリソースグループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA と RPO は、データ保護戦略に関与します。

使用頻度の高いリソースであっても、フルバックアップは 1 日に 1~2 回で十分です。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度

  バックアップ頻度（バックアップを実行する間隔）は、ポリシー設定の一部であり、一部のプラグインでは _ schedule type__ と呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定したり、「 * なし」を指定してオンデマンドのみのポリシーにすることができます。ポリシーにアクセスするには、 * Settings * > * Policies * をクリックします。

- バックアップスケジュール

  バックアップスケジュール（バックアップが実行される日時）は、リソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます。リソースグループのスケジュールにアクセスするには、 * リソース * > * リソースグループ * をクリックします。

Windows ファイルシステムに必要なバックアップの数

必要なバックアップの数を左右する要因としては、 Windows ファイルシステムのサイズ、使用中のボリュームの数、ファイルシステムの変更率、サービスレベルアグリーメント（ SLA ）などがあります。

Windows ファイルシステムのバックアップ命名規則

Windows ファイルシステムのバックアップでは、 Snapshot コピーのデフォルトの命名規則が使用されます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。
resourcegroupname_hostname_timestamp

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- `dts1` は、リソースグループ名です。
- `mach1x88` はホスト名です。
- `03-12-2016_23.17.26` は、日付とタイムスタンプです。

バックアップの作成時に、バックアップを識別するためのタグを追加することもできます。一方、カスタマイズしたバックアップ命名規則を使用する場合は、バックアップ処理の完了後にバックアップの名前を変更する必要があります。

バックアップ保持オプション

バックアップコピーを保持する日数を選択するか、保持するバックアップコピーの数を指定できます。指定できる最大数は ONTAP で 255 個です。たとえば、組織の必要に応じて、 10 日分のバックアップコピーや 130 個のバックアップコピーを保持できます。

ポリシーを作成する際に、バックアップタイプおよびスケジュールタイプの保持オプションを指定できます。

SnapMirror レプリケーションを設定すると、デスティネーションボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、保持されているバックアップの保持ラベルがスケジュールタイプと一致する場合には、バックアップを削除します。リソースまたはリソースグループに対してスケジュールタイプが変更された場合、古いスケジュールタイプラベルのバックアップがシステムに残ることがあります。

バックアップコピーを長期にわたって保持する場合は、 SnapVault バックアップを使用する必要があります。

Windows ファイルシステムのクローンのソースとデスティネーション

ファイルシステムのクローニングは、プライマリストレージまたはセカンダリストレージから実行できます。デスティネーションについても、要件に応じて、バックアップの元の場所のほか、同じホストまたは別のホストの別の場所を選択することができます。クローンのデスティネーションは、ソースのバックアップと同じボリュームになければなりません。

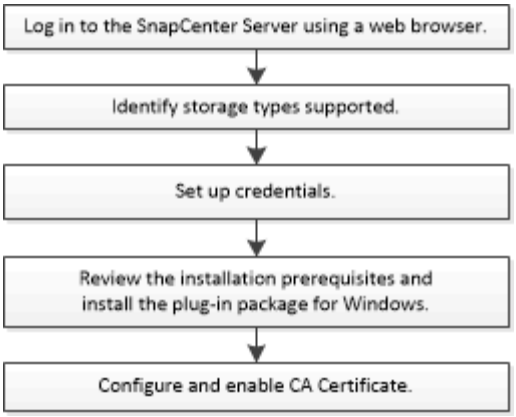
デスティネーションをクローニングします	説明
オリジナル、ソース、場所	デフォルトでは、 SnapCenter はクローンを作成するバックアップと同じホストの同じ場所に格納します。
別の場所	同じホストまたは別のホストの別の場所にクローンを格納できます。ホストで Storage Virtual Machine （ SVM ）への接続が設定されている必要があります。

クローニング処理の完了後にクローンの名前を変更できます。

SnapCenter Plug-in for Microsoft Windows をインストールします

SnapCenter Plug-in for Microsoft Windows のインストールワークフロー

データベースファイル以外の Windows ファイルを保護する場合は、 SnapCenter Plug-in for Microsoft Windows をインストールしてセットアップする必要があります。



SnapCenter Plug-in for Microsoft Windows のインストール要件

Plug-in for Windows をインストールする前に、一定のインストール要件について理解しておく必要があります。

ユーザが Plug-in for Windows の使用を開始するためには、 SnapCenter 管理者が事前に SnapCenter サーバをインストールして設定し、前提条件となるタスクを実行する必要があります。

- Plug-in for Windows をインストールするには、 SnapCenter 管理者権限が必要です。

  SnapCenter 管理者ロールには管理者権限が必要です。

- SnapCenter サーバをインストールして設定しておく必要があります。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- バックアップレプリケーションが必要な場合は、 SnapMirror と SnapVault をセットアップする必要があります。

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB

項目	要件
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Plug-in for Windows のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますSnapCenter プラグインのインストールに必要なクレデンシャル、および Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- 必要なもの *
- プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。
- リモートホストで、管理者権限を含む管理者権限でクレデンシャルを設定する必要があります。
- 個々のリソースグループのクレデンシャルを設定していて、そのユーザにフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザに割り当てる必要があります。
- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. [設定] ページで、 [* 資格情報] をクリックします。
  3. [新規作成（ New ）] をクリックする。
  4. [クレデンシャル] ページで、次の操作を実行します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	手順
ユーザ名 / パスワード	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。 ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Usernameフィールドの有効な形式は次のとおりです。 `UserName` パスワードに二重引用符（"）またはバックティック（`）を使用しないでください。小なり（<）と感嘆符（！）は使用しないでください。 パスワードに記号を追加します。たとえば、lessthan <！10、lessthan10 <！、backtick 12とします。
パスワード	認証に使用するパスワードを入力します。

5. [OK] をクリックします。

   クレデンシャルの設定が完了したら、 [ユーザとアクセス（ User and Access ）] ページで、ユーザまたはユーザグループにクレデンシャルのメンテナンスを割り当てることができます。

Windows Server 2012 以降で **gMSA** を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
   a. 次の形式でユーザグループアカウントを作成します。

```
 domainName\accountName$
.. グループにコンピュータオブジェクトを追加します。
.. 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. を実行します `Get-ADServiceAccount`
サービスアカウントを確認するコマンド。
```

4. ホストで gMSA を設定します。
   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. ホストを再起動します。

b. PowerShellコマンドプロンプトから次のコマンドを実行して、ホストにgMSAをインストールします。 `Install-AdServiceAccount <gMSA>`

c. 次のコマンドを実行して'gMSAアカウントを確認します `Test-AdServiceAccount <gMSA>`

1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

   SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

ホストを追加し、 **SnapCenter Plug-in for Microsoft Windows** をインストールします

SnapCenter のホストの追加ページを使用して、 Windows ホストを追加できます。指定したホストには、 SnapCenter Plug-in for Microsoft Windows が自動的にインストールされます。これはプラグインのインストールに推奨される方法です。ホストを追加してプラグインをインストールするには、個々のホストまたはクラスタを使用します。

- 必要なもの *
- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- SnapCenter ユーザーは 'Windows Server のサービスとしてログオンロールに追加する必要があります
- メッセージキューイングサービスが実行中状態であることを確認する必要があります。

- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

  "Windows ファイルシステム用に、 Windows Server 2012 以降のグループマネージドサービスアカウントを設定します"

- このタスクについて *
- SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。
- Windows プラグイン
  - Microsoft Windows の場合
  - Microsoft Exchange Server の略
  - Microsoft SQL Server の場合
  - SAP HANA のサポート
  - カスタムプラグイン
- クラスタへのプラグインのインストール

  クラスタ（ WSFC 、 Oracle RAC 、または Exchange DAG ）にプラグインをインストールすると、クラスタのすべてのノードにインストールされます。

- E シリーズストレージ

  E シリーズストレージに接続された Windows ホストに Plug-in for Windows をインストールすることはできません。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] が選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の手順を実行します。

フィールド	手順
ホストタイプ	Windows * タイプのホストを選択します。 SnapCenter Server によってホストが追加され、 Plug-in for Windows がまだホストにインストールされていない場合はインストールされます。

フィールド	手順
ホスト名	ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、ベストプラクティスは Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を入力することです。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • Windows Server フェイルオーバークラスタリング（ WSFC ） SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。
クレデンシャル	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 ユーザ名、ドメイン、ホストタイプなど、クレデンシャルの詳細は、指定したクレデンシャル名にカーソルを合わせると表示されます。 認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。

   新規導入の場合、プラグインパッケージは表示されません。

6. （オプション） * その他のオプション * をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	デフォルトパスは C ： \Program Files\NetApp\SnapManager です。 必要に応じて、パスをカスタマイズできます。SnapCenter Plug-ins Package for Windows のデフォルトパスは C ： \Program Files\NetApp\SnapManager です。ただし、必要に応じて、デフォルトパスをカスタマイズできます。
クラスタ内のすべてのホストを追加します	WSFC のすべてのクラスタノードを追加するには、このチェックボックスを選択します。
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	グループ管理サービスアカウント（ GMSA ）を使用してプラグインサービスを実行する場合は、このチェックボックスをオンにします。 gMSA 名を *domainName\accountName$* の形式で指定します。 gMSA は、 SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されます。

7. [Submit （送信）] をクリックします。

「 * 事前確認をスキップ」チェックボックスを選択していない場合、プラグインのインストール要件をホストが満たしているかどうかが検証されます。ディスクスペース、 RAM 、 PowerShell のバージ

ョン、 .NET のバージョン、および場所が、最小要件に照らして検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

エラーがディスクスペースまたはRAMに関連している場合は、にあるweb.configファイルを更新できます `C:\Program Files\NetApp\SnapCenter` Webappを使用して、デフォルト値を変更します。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

1. インストールの進行状況を監視します。

PowerShell コマンドレットを使用して、複数のリモートホストに SnapCenter Plug-in for Microsoft Windows をインストールします

SnapCenter Plug-in for Microsoft Windowsを複数のホストに一度にインストールする場合は、を使用します `Install-SmHostPackage` PowerShellコマンドレット：

プラグインをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、を使用してセッションを確立します `Open-SmConnection` コマンドレットを実行し、クレデンシャルを入力します。
3. を使用して、スタンドアロンホストまたはクラスタをSnapCenter に追加します `Add-SmHost` コマンドレットと必要なパラメータ

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

4. を使用して、複数のホストにプラグインをインストールします `Install-SmHostPackage` コマンドレットと必要なパラメータ

   を使用できます `-skipprecheck` オプション：プラグインを手動でインストールし、ホストがプラグインのインストール要件を満たしているかどうかを検証しない場合に使用します。

コマンドラインから SnapCenter Plug-in for Microsoft Windows をサイレントにインストールします

SnapCenter Plug-in for Microsoft Windows を SnapCenter の GUI からリモートでインストールできない場合は、 Windows ホスト上にローカルにインストールできます。SnapCenter Plug-in for Microsoft Windows のインストールプログラムを、 Windows のコマンドラインからサイレントモードで自動的に実行できます。

- 必要なもの *

- Microsoft .Net 4.7.2以降がインストールされている必要があります。
- PowerShell 4.0 以降がインストールされている必要があります。
- Windows メッセージキューをオンにしておく必要があります。
- ホストのローカル管理者である必要があります。
- 手順 *

1. インストールの場所から、 SnapCenter Plug-in for Microsoft Windows をダウンロードします。

   たとえば、デフォルトのインストールパスは C ： \ProgramData\NetApp\SnapCenter \Package Repository です。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

2. プラグインをインストールするホストにインストールファイルをコピーします。
3. コマンドプロンプトで、インストールファイルをダウンロードしたディレクトリに移動します。
4. 変数を実際のデータに置き換えて、次のコマンドを入力します。

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   例：

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Plug-in for Windows のインストール中に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

   次の変数の値を入力します。

変数（ **Variable** ）	価値
	インストーラのログファイルの名前と場所を次のように指定します。 Setup.exe /debuglog "C:\PathToLog\setupexe.log"
BI _ SNAPCENTER_PORT	SnapCenter が SMCore と通信するポートを指定します。

変数（ **Variable** ）	価値
SUITE_INSTALLDIR	ホストのプラグインパッケージのインストールディレクトリを指定します。
BY_ServiceAccount の場合	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントを指定します。
BI_SERVVICEPWD	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントのパスワードを指定します。
ISFeatureInstall	SnapCenter によってリモートホストに導入される解決策を指定します。

_debuglog_parameter には、 SnapCenter のログファイルのパスが含まれます。このログファイルにはインストールで実行されるプラグインの前提条件に関するチェック結果が記録されるため、トラブルシューティング情報を入手する方法としてこのログファイルに書き込むことを推奨します。

必要に応じて、 SnapCenter for Windows パッケージのログファイルでその他のトラブルシューティング情報を確認できます。パッケージのログファイルは、 *%Temp_folder* に（最も古いものから）一覧表示されます（例： *_C ： \temp* ）。

Plug-in for Windows をインストールすると、 SnapCenter サーバではなくホストにプラグインが登録されます。SnapCenter サーバにプラグインを登録するには、 SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加します。ホストを追加すると、プラグインが自動的に検出されます。

SnapCenter プラグインパッケージのインストールステータスを監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
   a. [* フィルタ * （ Filter * ）] をクリック
   b. オプション：開始日と終了日を指定します。
   c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
   d. Status ドロップダウンメニューから、インストールステータスを選択します。
   e. [適用（ Apply ）] をクリックします。
4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。

4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *
  1. GUI で次の手順を実行します。
     a. 証明書をダブルクリックします。
     b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
     c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
     d. ボックスから 16 進文字をコピーします。
     e. 16 進数の間のスペースを削除します。

        たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。
  2. PowerShell で次の手順を実行します。
     a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

        Get-ChildItem - パス証明書： *\localmachine\My*

b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して **CA** 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   . 次のコマンドを実行して、新しくインストールした証明書を Windows ホストプラグインサービスにバインドします。

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
   certhash=$cert appid="$guid"
   ```

   例：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

プラグインの **CA** 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphere をインストール

データベースが仮想マシン（ VM ）に格納されている場合や VM とデータストアを保護する場合は、 SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください "導入の概要"。

CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください "SSL 証明書を作成またはインポートします"。

CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere は、事前に設定されたディレクトリ内の CRL ファイルを検索します。VMware vSphere 用 SnapCenter プラグインの CRL ファイルのデフォルトディレクトリは、_/opt/NetApp/config/crl_です 。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

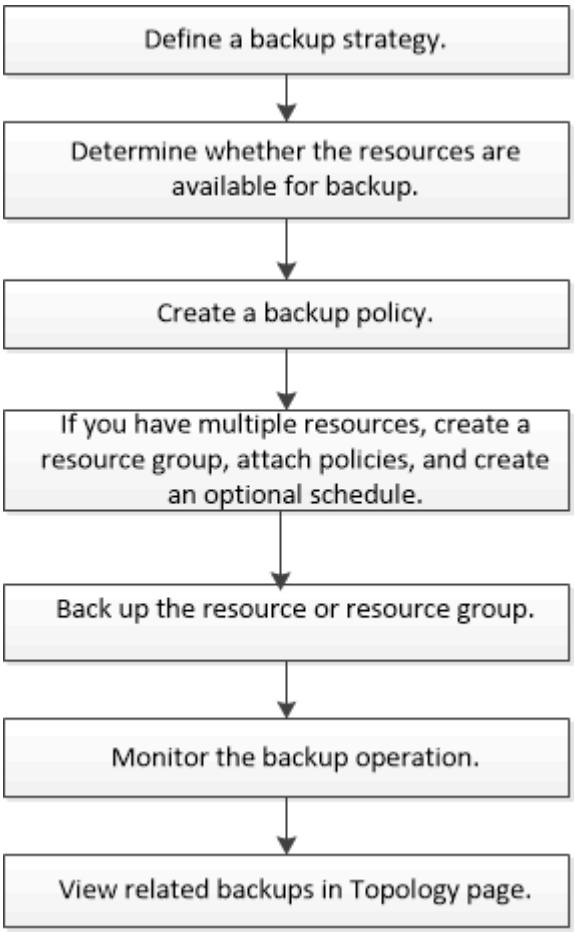
Windows ファイルシステムのバックアップ

Windows ファイルシステムのバックアップ

SnapCenter Plug-in for Microsoft Windows をインストールした環境では、 SnapCenter を使用して Windows ファイルシステムをバックアップすることができます。単一のファイルシステム、または複数のファイルシステムを含むリソースグループをバックアップできます。バックアップは、オンデマンドで実行することも、定義した保護スケジュールに従って実行することもできます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。バックアップ処理とリストア処理を同じリソースで同時に実行することはできません。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。SnapCenter コマンドレットのヘルプまたはを使用します "SnapCenter ソフトウェアコマンドレットリファレンスガイド" PowerShell コマンドレットの詳細については、を参照してください。

Windows ファイルシステムで使用可能なリソースを確認します

リソースとは、インストールしたプラグインで管理されるファイルシステム内の LUN な

どのコンポーネントのことです。これらのリソースをリソースグループに追加することで複数のリソースに対してデータ保護ジョブを実行できますが、その前に利用可能なリソースを特定しておく必要があります。使用可能なリソースを検出することで、プラグインのインストールが正常に完了したことの確認にもなります。

- 必要なもの *
- SnapCenter サーバのインストール、ホストの追加、 Storage Virtual Machine （ SVM ）接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- ファイルが VMware RDM LUN または VMDK にある場合は、 SnapCenter Plug-in for VMware vSphere を導入し、 SnapCenter に登録する必要があります。詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere のドキュメント"。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースページで、リストから * ファイルシステム * を選択します。
3. ホストを選択してリソースのリストをフィルタリングし、 * リソースの更新 * をクリックします。

   新しく追加、名前変更、または削除されたファイルシステムは、 SnapCenter サーバインベントリに更新されます。

データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

Windows ファイルシステムのバックアップポリシーの作成

SnapCenter を使用して Windows ファイルシステムをバックアップする前に、リソースの新しいバックアップポリシーを作成することができます。また、リソースグループの作成時やリソースのバックアップ時に新しいバックアップポリシーを作成することもできます。

- 必要なもの *
- バックアップ戦略を定義しておく必要があります。 "詳細はこちら。"
- データ保護の準備が完了している必要があります。

  データ保護の準備として、 SnapCenter のインストール、ホストの追加、リソースの検出、 Storage Virtual Machine （ SVM ）接続の作成などのタスクを完了しておく必要があります。

- Snapshot コピーをミラーセカンダリストレージまたはバックアップセカンダリストレージにレプリケートするユーザには、 SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に SVM を割り当てる必要があります。
- プリスクリプトとポストスクリプトで PowerShell スクリプトを実行する場合は、 web.config ファイルで usePowershellProcessforScripts パラメータの値を true に設定する必要があります。

  デフォルト値は false です。

- このタスクについて *
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. 既存のポリシーを使用できるかどうかを確認するには、ポリシー名を選択し、 [* 詳細 *] をクリックします。

   既存のポリシーを確認したあと、次のいずれかを実行できます。

   - 既存のポリシーを使用する。
   - 既存のポリシーをコピーしてポリシー設定を変更する。
   - 新しいポリシーを作成します。
4. 新しいポリシーを作成するには、 * New * をクリックします。
5. [名前] ページで、ポリシー名と概要 を入力します。
6. [バックアップオプション] ページで、次のタスクを実行します。

   a. バックアップ設定を選択します。

オプション	説明
File System Consistent Backup の略	ファイルシステムが配置されたディスクドライブをバックアップ処理の開始前に SnapCenter で休止し、バックアップ処理の終了後に再開する場合は、このオプションを選択します。
ファイルシステムのクラッシュ整合性バックアップ	ファイルシステムが配置されたディスクドライブを SnapCenter で休止しない場合は、このオプションを選択します。

   b. スケジュール頻度（ポリシータイプ）を選択します。

      ポリシーではバックアップの頻度のみを指定します。バックアップの具体的なスケジュールは、リソースグループで定義します。したがって、複数のリソースグループで同じポリシーとバックアップ頻度を使用している場合でも、別々のバックアップスケジュールを設定できます。

午前 2 時にスケジュールを設定した場合、夏時間（ DST ）中はスケジュールはトリガーされません。

7. [保持] ページで ' オン・デマンド・バックアップおよび選択した各スケジュール頻度の保持設定を指定します

オプション	説明
保持する Snapshot コピーの総数	SnapCenter ストアを自動的に削除する前に Snapshot コピー数を指定する場合は、このオプションを選択します。
より古い Snapshot コピーを削除します	SnapCenter がバックアップコピーを保持する日数を指定する場合は、このオプションを選択します。指定した日数を過ぎると削除されます。

保持数を2以上に設定してください。保持数の最小値は2です。

最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。

8. Replication （レプリケーション）ページで、セカンダリストレージシステムへのレプリケーションを指定します。

フィールド	手順
ローカル Snapshot コピーの作成後に SnapMirror を更新します	別のボリュームにバックアップセットのミラーコピーを作成する場合（ SnapMirror ）は、このオプションを選択します。
Snapshot コピーの作成後に SnapVault を更新します	ディスクツーディスクのバックアップレプリケーションを実行する場合は、このオプションを選択します。

フィールド	手順
セカンダリポリシーのラベル	Snapshot ラベルを選択します。 選択した Snapshot コピーラベルに応じて、 ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。 ローカル Snapshot コピーの作成後に「 * SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できます。ただし、ローカル Snapshot コピーの作成後に「 * Update SnapVault 」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。
エラー再試行回数	レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。

セカンダリストレージでの Snapshot コピーの最大数に達しないように、 ONTAP でセカンダリストレージの SnapMirror 保持ポリシーを設定する必要があります。

9. スクリプトページで、 SnapCenter サーバでバックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと、 SnapCenter がスクリプトの実行を待機してからタイムアウトするまでの時間を入力します。

   たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

1. 概要を確認し、 [完了] をクリックします。

Windows ファイルシステムのリソースグループを作成する

リソースグループとは、保護する複数のファイルシステムを追加できるコンテナです。リソースグループに 1 つ以上のポリシーを適用して実行するデータ保護ジョブのタイプを定義し、バックアップスケジュールを指定することも必要です。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースページで、リストから * ファイルシステム * を選択します。

最近 SnapCenter にファイルシステムを追加した場合は、 [* リソースを更新 * （ Refresh Resources ）] をクリックして、新しく追加されたリソースを表示します。

3. [New Resource Group] をクリックします。
4. ウィザードの [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループ名を入力します。 リソースグループ名は 250 文字以内にする必要があります。
Snapshot コピーには、カスタムの名前形式を使用します	オプション： Snapshot コピー名のカスタムの名前形式を入力します。 たとえば、 customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。
タグ（ Tag ）	リソースグループを検索するときに役立つわかりやすいタグを入力します。

5. Resources ページで、次のタスクを実行します。
   a. ホストを選択してリソースのリストをフィルタリングします。

      最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

   b. [使用可能なリソース] セクションで、バックアップするファイルシステムをクリックし、右矢印をクリックして [追加済み] セクションに移動します。

      [同じストレージボリューム上のすべてのリソースを自動選択 *] オプションを選択すると、同じボリューム上のすべてのリソースが選択されます。それらを Added セクションに移動すると、そのボリューム上のすべてのリソースが一緒に移動します。

   単一ファイルシステムを追加するには、同じストレージボリューム上のすべてのリソースを自動選択 * オプションを選択解除し、追加したセクションに移動するファイルシステムを選択します。

6. [Policies] ページで、次のタスクを実行します。
   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

      既存のポリシーを選択し、 ［ * 詳細 * ］ をクリックすると、そのポリシーを使用できるかどうかを確認できます。

      既存のポリシーがいずれも要件を満たさない場合は、 * をクリックして新しいポリシーを作成でき

ます + * をクリックして、ポリシーウィザードを起動します。

選択したポリシーは、 [Configure schedules for selected policies] セクションの [Policy （ポリシー）] カラムに表示されます。

a. [選択したポリシーのスケジュールを設定] セクションで、 * をクリックします + * スケジュールを設定するポリシーの [スケジュールの設定] 列。

b. ポリシーが複数のスケジュールタイプ（頻度）に関連付けられている場合は、設定する頻度を選択します。

c. [Add schedules for policy_name_] ダイアログボックスで、開始日、有効期限、頻度を指定してスケジュールを設定し、 [*Finish] をクリックします。

設定されたスケジュールは、 [Configure schedules for selected policies] セクションの [Applied Schedules] カラムに表示されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。Windows タスクスケジューラと SQL Server エージェントからスケジュールを変更しないでください。

1. [通知] ページで、次の通知情報を指定します。

フィールド	手順
E メール設定	バックアップリソースグループの作成、ポリシーの適用、スケジュールの設定のあとに受信者に E メールを送信するには、「 * Always * 」、「 * On Failure * 」、または「 * on failure or warning * 」を選択します。SMTP サーバ、 E メールのデフォルトの件名、および送信先と送信元の E メールアドレスを入力します。
移動元	E メールアドレス
終了：	E メールの送信先アドレス
件名	E メールのデフォルトの件名

2. 概要を確認し、 [完了] をクリックします。

オンデマンドでバックアップを実行できるほか、スケジュールされたバックアップが実行されるまで待つこともできます。

Windows ファイルシステムの単一のリソースをオンデマンドでバックアップする

リソースグループに含まれていないリソースは、のリソースページからオンデマンドでバックアップすることができます。

• このタスクについて *

セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられたロールには「 '"napmirror all" 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。

ファイルシステムをバックアップする場合、 SnapCenter は、バックアップするファイルシステムのボリュームマウントポイント（ VMP ）にマウントされている LUN をバックアップしません。

Windows ファイルシステムのコンテキストで作業している場合は、データベースファイルをバックアップしないでください。バックアップを作成しても整合性に欠け、リストア時にデータが失われる可能性があります。データベースファイルを保護するには、データベースに適した SnapCenter プラグイン（ SnapCenter Plug-in for Microsoft SQL Server 、 SnapCenter Plug-in for Microsoft Exchange Server 、データベースファイル用のカスタムプラグインなど）を使用する必要があります。

• 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [ファイルシステム] リソースタイプを選択し、バックアップするリソースを選択します。
3. File System-Protect ウィザードが自動的に起動しない場合は、 [*Protect] をクリックしてウィザードを開始します。

   「リソースグループの作成」のタスクの説明に従って、保護設定を指定します。

4. オプション：ウィザードのリソースページで、 Snapshot コピーのカスタム名形式を入力します。

   たとえば、 customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

5. [Policies] ページで、次のタスクを実行します。

   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

      既存のポリシーを選択し、 [**Details**] をクリックすると、そのポリシーを使用できるかどうかを確認できます。

      既存のポリシーがいずれも要件を満たさない場合は、既存のポリシーをコピーして変更するか、

      をクリックして新しいポリシーを作成できます ＋ ポリシーウィザードを起動します。

   選択したポリシーは、 [Configure schedules for selected policies] セクションの [Policy （ポリシー）] カラムに表示されます。

   a. Configure schedules for selected policies セクションで、をクリックします ＋ スケジュールを設定するポリシーの Configure Schedules （スケジュールの設定）列。
   b. [Add schedules for policy_name_] ダイアログボックスで、開始日、有効期限、頻度を指定してス

ケジュールを設定し、 [*Finish] をクリックします。

設定されたスケジュールは、 [Configure schedules for selected policies] セクションの [Applied Schedules] カラムに表示されます。

"スケジュールされた処理が失敗する可能性が"

1. [通知] ページで、次のタスクを実行します。

フィールド	手順
E メール設定	バックアップリソースグループの作成後、ポリシーの適用後、スケジュールの設定後に受信者に E メールを送信するには、「 Always * 」、「 On Failure * 」、または「 On Failure * 」または「 On Failure / Warning * 」を選択します。 SMTP サーバの情報 ' デフォルトの電子メールの件名 ' およびからの電子メールアドレスを入力します
移動元	E メールアドレス
終了：	E メールの送信先アドレス
件名	E メールのデフォルトの件名

2. 概要を確認し、 [完了] をクリックします。

   データベーストポロジのページが表示されます。

3. [今すぐバックアップ] をクリックします。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. リソースに複数のポリシーを適用している場合は、ポリシーのドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. [バックアップ] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

Windows ファイルシステムのリソースグループをバックアップする

リソースグループは、ホストまたはクラスタ上のリソースの集まりです。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースを対象に実行されます。リソースグループは、リソースページからオンデマンドでバックア

ップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

- 必要なもの *
- ポリシーを適用したリソースグループを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられるロールには「 '"napmirror all" 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- リソースグループに異なるホストの複数のデータベースが含まれている場合は、ネットワークの問題が原因で、一部のホストでのバックアップ処理が遅くなる可能性があります。Set-SmConfigSettings PowerShell コマンドレットを使用して、 web.config で MaxRetryForUninitializedHosts の値を設定する必要があります

ファイルシステムをバックアップする場合、 SnapCenter は、バックアップするファイルシステムのボリュームマウントポイント（ VMP ）にマウントされている LUN をバックアップしません。

Windows ファイルシステムのコンテキストで作業している場合は、データベースファイルをバックアップしないでください。バックアップを作成しても整合性に欠け、リストア時にデータが失われる可能性があります。データベースファイルを保護するには、データベースに適した SnapCenter プラグイン（ SnapCenter Plug-in for Microsoft SQL Server 、 SnapCenter Plug-in for Microsoft Exchange Server 、データベースファイル用のカスタムプラグインなど）を使用する必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。

   リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックします タグを選択します。をクリックします をクリックしてフィルタペインを閉じます。
3. [リソースグループ] ページで、バックアップするリソースグループを選択し、 [今すぐバックアップ *] をクリックします。

   SnapCenter Plug-in for Oracle Database では、 2 つのデータベースが統合されたリソースグループがある場合に、一方のデータベースのデータファイルがネットアップ以外のストレージにあると、もう一方のデータベースがネットアップストレージにあっても、バックアップ処理は中止されます。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

b. [バックアップ] をクリックします。

5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   - MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。

     "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"

   - VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。Javaのヒープサイズを増やすには、スクリプトファイルを探します `/opt/netapp/init_scripts/scvservice`。このスクリプトでは、を実行します `do_start method` コマンドは、SnapCenter VMwareプラグインサービスを開始します。このコマンドを次のように更新します。 `Java -jar -Xmx8192M -Xms4096M`。

PowerShell コマンドレットを使用してストレージシステム接続とクレデンシャルを作成します

PowerShell コマンドレットを使用してデータ保護処理を実行するには、 Storage Virtual Machine （ SVM ）接続とクレデンシャルを作成する必要があります。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前および管理 LIF の IP アドレスを割り当てる必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、 PowerShell 接続セッションを開始します。

   PowerShell セッションを開く例を次に示します。

   ```
   PS C:\> Open-SmConnection
   ```

2. Add-SmStorageConnection コマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

   この例では、新しいストレージシステム接続を作成しています。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Add-SmCredential コマンドレットを使用して新しいクレデンシャルを作成します。

   この例は、 Windows クレデンシャルを使用して FinanceAdmin という名前の新しいクレデンシャルを作成します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

PowerShell コマンドレットを使用してリソースをバックアップします

PowerShell コマンドレットを使用して、 SQL Server データベースや Windows ファイルシステムをバックアップできます。たとえば、 SQL Server データベースまたは Windows ファイルシステムのバックアップでは、 SnapCenter サーバとの接続の確立、 SQL Server データベースインスタンスまたは Windows ファイルシステムの検出、ポリシーの追加、バックアップリソースグループの作成、バックアップ、およびバックアップの検証が行われます。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。
- ホストを追加し、リソースを検出しておく必要があります。
- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmPolicy コマンドレットを使用してバックアップポリシーを作成します。

   この例では、 SQL のバックアップタイプ「 FullBackup 」を指定して新しいバックアップポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

この例では、 Windows ファイルシステムのバックアップタイプ「 CrashConsistent 」を指定して新しいバックアップポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResources コマンドレットを使用して、ホストリソースを検出します。

   この例では、指定したホスト上で Microsoft SQL プラグインのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   この例では、指定したホスト上で Windows ファイルシステムのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add-SmResourceGroup コマンドレットを使用して、新しいリソースグループを SnapCenter に追加します。

   この例では、ポリシーとリソースを指定して新しい SQL データベースバックアップリソースグループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   この例では、ポリシーとリソースを指定して新しい Windows ファイルシステムバックアップリソースグループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackup コマンドレットを使用して、新しいバックアップジョブを開始する。

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Get-SmBackupReport コマンドレットを使用して、バックアップジョブのステータスを表示します。

   次の例は、指定した日付に実行されたすべてのジョブの概要レポートを表示します。

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

バックアップ処理を監視する

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. Jobs （ジョブ）ページで、次の手順を実行します。
     a. をクリックします バックアップ処理だけが表示されるようにリストをフィルタリングします。
     b. 開始日と終了日を指定します。
     c. [* タイプ] ドロップダウン・リストから、 **[*Backup]** を選択します。
     d. **[Status]**(ステータス *) ドロップダウンから、バックアップステータスを選択します。

e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。

4. バックアップジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

バックアップジョブのステータスがと表示されます で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

アクティビティペインで操作を監視します

[アクティビティ（ Activity ）] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity （アクティビティ）] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. をクリックします をクリックして、最近の 5 つの操作を表示します。

いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

バックアップ処理をキャンセルします

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの *
- 処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。
- バックアップ操作は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のバックアップ処理をキャンセルすることはできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、バックアップ処理をキャンセルできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っているバックアップ操作をキャンセルできます
- 手順 *

1. 次のいずれかを実行します。

方法	アクション
監視ページ	a. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 b. 操作を選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	a. バックアップ処理を開始したら、 * をクリックします* ［アクティビティ］ パネルには、最近の 5 つの操作が表示されます。 b. 処理を選択します。 c. ［ジョブの詳細］ ページで、 ［* ジョブのキャンセル *］ をクリックします。

処理がキャンセルされ、リソースが以前の状態に戻ります。

トポロジページで関連するバックアップとクローンを表示します

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示できます。トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

- このタスクについて *

[コピーの管理] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップとクローンが使用可能かどうかを判断できます。

-  には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
-  には、 SnapMirror テクノロジを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。

  mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数には、バージョンに依存しないバックアップは含まれません。

-  には、 SnapVault テクノロジを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。
  - 表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、 4 個のバックアップだけを保持するポリシーを使用して 6 個のバックアップを作成し

た場合、バックアップの数は 6 個と表示されます。

- SnapCenter 1.1 からアップグレードした場合、セカンダリ（ミラーまたはバックアップ）上のクローンは、トポロジページのミラーコピーまたはバックアップコピーの下に表示されません。SnapCenter 3.0 では、 SnapCenter 1.1 で作成されたすべてのクローンがローカルコピーの下に表示されます。

mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数には、バージョンに依存しないバックアップは含まれません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

   リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. 概要カードを確認して、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数をサマリで確認します。

   サマリカードセクションには、バックアップとクローンの合計数が表示されます。Oracle データベースの場合のみ、サマリカードセクションにはログバックアップの合計数も表示されます。

   更新ボタンをクリックすると、ストレージのクエリが実行されて正確な数が表示されます。

5. [コピーの管理] ビューで、プライマリストレージまたはセカンダリストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

   バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。

   セカンダリストレージシステム上のバックアップは、名前変更または削除できません。

   SnapCenter Custom Plug-ins を使用している場合、プライマリストレージシステムにあるバックアップの名前は変更できません。

   - Oracle のリソースまたはリソースグループのバックアップを選択した場合、マウントおよびアンマウントの処理も実行できます。
   - Oracle のリソースまたはリソースグループのログバックアップを選択した場合、名前変更、マウント、アンマウント、および削除の処理を実行できます。
   - SnapCenter Plug-ins Package for Linux を使用していて、 Oracle Recovery Manager （ RMAN ）を使用してバックアップをカタログ化した場合、カタログ化されたバックアップの名前は変更できません。

7. クローンを削除する場合は、表でクローンを選択し、をクリックします をクリックしてクローンを削除します。

• プライマリストレージ上のバックアップとクローンを示す例 *

PowerShell コマンドレットを使用してバックアップを削除します

Remove-SmBackup コマンドレットを使用すると、他のデータ保護処理に不要になったバックアップを削除できます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

• 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Remove-SmBackup コマンドレットを使用して 1 つ以上のバックアップを削除します。

   この例では、バックアップ ID を指定してバックアップを 2 つ削除しています。

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

PowerShell コマンドレットを使用してセカンダリバックアップ数をクリーンアップします

Remove-SmBackup コマンドレットを使用して、 Snapshot コピーがないセカンダリバックアップのバックアップ数をクリーンアップできます。Manage Copies （コピーの管

理）トポロジに表示される Snapshot コピーの合計数が、セカンダリ・ストレージの Snapshot コピーの保持設定と一致しない場合に、このコマンドレットを使用できます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. CleanupSecondaryBackups パラメータを使用して、セカンダリバックアップ数をクリーンアップします。

   この例では、 Snapshot コピーがないセカンダリバックアップのバックアップ数をクリーンアップしています。

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Windows ファイルシステムをリストア

Windows ファイルシステムのバックアップをリストアする

SnapCenter を使用すると、ファイルシステムのバックアップをリストアできます。ファイルシステムのリストアは段階的に実施され、指定したバックアップのすべてのデータがファイルシステムの元の場所にコピーされます。

- 必要なもの *
- ファイルシステムをバックアップしておく必要があります。
- ファイルシステムに対してバックアップ処理などのスケジュールが設定された処理が現在実行中の場合は、リストア処理を開始する前にキャンセルしておく必要があります。
- ファイルシステムのバックアップは元の場所にのみリストアでき、別のパスを指定することはできません。

  ファイルシステムのリストアでは、ファイルシステムの元の場所にあるデータはすべて上書きされるため、バックアップからファイルを 1 つずつリストアすることはできません。ファイルシステムのバックア

ップから単一のファイルをリストアするには、バックアップをクローニングし、クローン内のファイルにアクセスする必要があります。

- システムボリュームやブートボリュームはリストアできません。
- SnapCenter では、クラスタグループをオフラインにすることなく、 Windows クラスタのファイルシステムをリストアできます。
- このタスクについて *
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースのリストをフィルタリングするには、 [ファイルシステム（ File System ）] および [リソースグループ（ Resource Group ）] オプションを選択します。
3. リストからリソースグループを選択し、 * リストア * をクリックします。
4. バックアップページで、プライマリストレージシステムとセカンダリストレージシステムのどちらからリストアするかを選択し、リストアするバックアップを選択します。
5. リストアウィザードでオプションを選択します。
6. リストア処理の実行前や実行後に SnapCenter で実行するプリスクリプトやポストスクリプトのパスと引数を入力できます。

   たとえば、 SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

1. [通知] ページで、次のいずれかのオプションを選択します。

フィールド	手順
SnapCenter サーバイベントをストレージシステムの syslog に記録します	SnapCenter サーバのイベントをストレージ・システムの syslog に記録する場合は、このオプションを選択します。
失敗した処理についての AutoSupport 通知をストレージシステムに送信します	失敗した処理に関する情報を AutoSupport を使用してネットアップに送信する場合は、このオプションを選択します。

フィールド	手順
E メール設定	バックアップのリストア後に受信者にメールを送信するには、「 * Always * 」、「 * On Failure * 」、または「 * on failure or warning * 」を選択します。SMTP サーバ、 E メールのデフォルトの件名、および送信先と送信元の E メールアドレスを入力します。

2. 概要を確認し、 [完了] をクリックします。
3. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

リストアしたファイルシステムにデータベースが含まれている場合は、データベースもリストアする必要があります。データベースをリストアしないと、データベースが無効な状態になる可能性があります。データベースのリストアの詳細については、そのデータベースの『データ保護ガイド』を参照してください。

PowerShell コマンドレットを使用してリソースをリストアする

リソースのバックアップをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップに関する情報を取得します。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

この例では、 2015 年 1 月 29 日から 2015 年 2 月 3 日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

1. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

リストア処理を監視する

Jobs ページを使用して、 SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします リストをフィルタリングして、リストア処理のみを表示します。
   b. 開始日と終了日を指定します。
   c. [* タイプ] ドロップダウン・リストから、 [リストア *] を選択します。
   d. [* Status *] ドロップダウン・リストから、リストア・ステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

   View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

リストア処理をキャンセルします

キューに格納されているリストアジョブをキャンセルできます。

リストア処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *
- キューに登録されたリストア処理は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、キューに登録されたリ

ストア処理をキャンセルできます。

- キャンセルできないリストア処理の場合、 [ジョブのキャンセル] ボタンは使用できません。
- ロールの作成中に [ユーザー \ グループ] ページで [このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できる] を選択した場合は、そのロールを使用している間に、他のメンバーのキューに登録されているリストア操作をキャンセルできます。
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. ジョブを選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. リストア処理を開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ ジョブの詳細 ］ ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

Windows ファイルシステムのクローニング

Windows ファイルシステムのバックアップからのクローニング

SnapCenter を使用して、 Windows ファイルシステムのバックアップをクローニングすることができます。誤って削除または変更された単一のファイルのコピーが必要な場合は、バックアップをクローニングし、クローン内のファイルを使用できます。

- 必要なもの *
- データ保護の準備として、ホストの追加、リソースの特定、 Storage Virtual Machine （ SVM ）接続の作成などのタスクを完了しておく必要があります。
- ファイルシステムのバックアップを作成しておく必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine （ SVM ）に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- リソースグループはクローニングできません。クローニングできるのは、個々のファイルシステムのバックアップだけです。
- VMDK ディスクを使用した仮想マシン上にあるバックアップは、 SnapCenter で物理サーバにクローニングできません。
- 共有 LUN やクラスタ共有ボリューム（ CSV ） LUN などの Windows クラスタをクローニングした場合、クローンは指定したホストに専用の LUN として格納されます。

- クローニング処理では、ボリュームマウントポイントのルートディレクトリを共有ディレクトリにすることはできません。
- クローンは、アグリゲートのホームノード以外のノードには作成できません。
- Windows ファイルシステムのクローニング処理では、定期的なスケジュール（クローンライフサイクル）は設定できません。バックアップのクローニングはオンデマンドでのみ実行できます。
- クローンが含まれている LUN を新しいボリュームに移動すると、 SnapCenter でそのクローンをサポートできなくなります。たとえば、 SnapCenter を使用してそのクローンを削除することはできません。
- 環境間でクローンを作成することはできません。たとえば、物理ディスクから仮想ディスクへのクローニングやその逆のクローニングがあります。
- このタスクについて *
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. リソースページで、リストから * ファイルシステム * を選択します。
3. ホストを選択します。

   リソースが保護されている場合は、トポロジビューが自動的に表示されます。

4. リソースのリストからクローニングするバックアップを選択し、クローンアイコンをクリックします。
5. [オプション] ページで、次の操作を実行します。

フィールド	手順
クローンサーバ	クローンを作成するホストを選択します。
「 Auto assign mount point 」または「 Auto assign volume mount point under path 」	マウントポイントを自動的に割り当てるか、パスを指定してボリュームマウントポイントを自動的に割り当てるかを選択します。 Auto assign volume mount point under path ：マウントポイントを作成する特定のディレクトリのパスを指定できます。このオプションを選択する場合は、ディレクトリが空であることを事前に確認しておく必要があります。ディレクトリにバックアップが格納されている場合、そのバックアップはマウント処理後に無効な状態になります。

フィールド	手順
アーカイブの場所	セカンダリバックアップをクローニングする場合にアーカイブの場所を選択します。

6. スクリプトページで、実行するプリスクリプトまたはポストスクリプトを指定します。

   プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

7. 概要を確認し、 [完了] をクリックします。
8. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用してバックアップをクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup コマンドレットまたは Get-SmResourceGroup コマンドレットを使用して、クローニングできるバックアップのリストを表示します。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                      BackupTime   BackupType
--------   ----------                      ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   この例では、指定したリソースグループとそのリソース、および関連ポリシーに関する情報を表示しています。

```
```

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
```

```
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
```

```
IsClone : False
```

3. New-SmClone コマンドレットを使用して、既存のバックアップからクローニング処理を開始する。

   この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

   この例では、指定した Microsoft SQL Server インスタンスのクローンを作成しています。

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Get-SmCloneReport コマンドレットを使用して、クローニングジョブのステータスを表示します。

   この例では、指定したジョブ ID のクローンレポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

クローニング処理を監視する

Jobs ページを使用して、 SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
   b. 開始日と終了日を指定します。
   c. [**Type**](タイプ **)** ドロップダウンリストから **'[*Clone**](クローン *) を選択します
   d. [* Status *] ドロップダウン・リストから、クローンのステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. クローンジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

クローニング処理をキャンセルします

キューに登録されているクローニング処理をキャンセルできます。

クローニング処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *
- キューに登録されたクローン処理は、 * Monitor * ページまたは * Activity * ペインからキャンセルできます。
- 実行中のクローン処理はキャンセルできません。
- キューに登録されたクローニング処理をキャンセルするには、 SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用します。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用しているときに ' 他のメンバーのキューに登録されているクローン操作をキャンセルできます
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. 操作を選択し、 * ジョブのキャンセル * をクリックします。

方法	アクション
アクティビティペイン	1. クローニング処理を開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ジョブの詳細］ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

クローンをスプリットします。

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

- このタスクについて *
- 中間のクローンに対してクローンスプリット処理を実行することはできません。

  たとえば、データベースバックアップから clone1 を作成したあとで、 Clone1 のバックアップを作成し、そのバックアップ（ Clone2 ）をクローニングできます。Clone2 を作成すると、 clone1 は中間クローンであり、 clone1 でクローンスプリット処理を実行することはできません。ただし、 Clone2 でクローンスプリット処理を実行することはできます。

  Clone2 をスプリットしたあとは、 clone1 が中間クローンではなくなるため、 clone1 でクローンスプリット処理を実行できます。
- クローンをスプリットすると、クローンのバックアップコピーとクローンジョブが削除されます。
- クローンスプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。
- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [表示] リストから適切なオプションを選択します。

オプション	説明
データベースアプリケーション用	[表示] リストから [*Database] を選択します。
ファイルシステムの場合	[表示] リストから [* パス *] を選択します。

3. リストから適切なリソースを選択します。

   リソースのトポロジページが表示されます。

4. [コピーの管理] ビューで、クローン作成されたリソース（データベースや LUN など）を選択し、 [*

] をクリックします *

5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   SMCore サービスが再起動すると、クローンスプリット処理が応答しなくなります。Stop-SmJob コマンドレットを実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

   クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、 _SMCoreServiceHost.exe.config_file の _CloneSplitStatusCheckPollTime_Parameter の値を変更して、 SMCore がクローンスプリット処理のステータスをポーリングする間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

   例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

+
バックアップ、リストア、または別のクローンスプリットの実行中は、クローンスプリットの開始処理が失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

- 詳細はこちら *

"「 aggregate does not exist 」というメッセージが表示されて、 SnapCenter クローンまたは検証が失敗する"

Microsoft Exchange Server データベースを保護する

SnapCenter Plug-in for Microsoft Exchange Server の概念

SnapCenter Plug-in for Microsoft Exchange Server の概要

SnapCenter Plug-in for Microsoft Exchange Server は、 Exchange データベースに対応したデータ保護管理を提供する、 NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。Plug-in for Exchange を使用すると、 SnapCenter 環境での Exchange データベースのバックアップとリストアが自動的に実行されます。

Plug-in for Exchange をインストールすると、 SnapCenter で NetApp SnapMirror テクノロジを使用して別のボリュームにバックアップセットのミラーコピーを作成できるほか、 NetApp SnapVault テクノロジを使用して標準への準拠やアーカイブを目的としたディスクツーディスクのバックアップレプリケーションを実行できます。

Exchange データベース全体ではなくメールやメールボックスのリストアとリカバリを行う場合は、 Single Mailbox Recovery （ SMBR ）ソフトウェアを使用します。
NetApp®Single Mailbox Recoveryは、2023年5月12日に販売終了（EOA）になりました。NetAppは、2020年6月24日に導入されたマーケティング用パーツ番号を通じて、メールボックスの容量、メンテナンス、サポートを購入したお客様をサポート対象期間中も引き続きサポートします。

NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsには、NetApp Single Mailbox Recoveryと同様の機能が用意されています。お客様は、新しいOntrack PowerControlsソフトウェアライセンスとOntrack PowerControlsメンテナンスおよびサポート更新をOntrackから（licensingteam@ontrack.com経由で）購入して、メールボックスをきめ細かくリカバリできます。

SnapCenter Plug-in for Microsoft Exchange Server の機能

Plug-in for Exchange を使用して、 Exchange Server データベースのバックアップとリストアを行うことができます。

- Exchange Database Availability Group （ DAG ；データベース可用性グループ）、データベース、およびレプリカセットのアクティブなインベントリを表示および管理する
- バックアップの自動化の保護設定を提供するポリシーを定義します
- ポリシーをリソースグループに割り当てる
- DAG とデータベースを個別に保護する
- プライマリとセカンダリの Exchange メールボックスデータベースをバックアップします
- プライマリバックアップとセカンダリバックアップからデータベースをリストアする

SnapCenter Plug-in for Microsoft Windows および Microsoft Exchange Server でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシンの両方でさまざまなストレージタイプをサポー

トしています。ホストに対応したパッケージをインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

Windows Server では、 SnapCenter プロビジョニングとデータ保護がサポートされます。サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
物理サーバ	FC 接続 LUN	SnapCenter のグラフィカルユーザインターフェイス（ GUI ）または PowerShell コマンドレット	
物理サーバ	iSCSI で接続された LUN	SnapCenter GUI または PowerShell コマンドレット	
VMware VM	FC または iSCSI HBA で接続された RDM LUN	PowerShell コマンドレット	物理的な互換性のみ VMDK はサポートされません。
VMware VM	iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN	SnapCenter GUI または PowerShell コマンドレット	VMDK はサポートされません。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
Hyper-V VM	仮想ファイバチャネルスイッチで接続された仮想 FC （ vFC ） LUN	SnapCenter GUI または PowerShell コマンドレット	仮想ファイバチャネルスイッチで接続された仮想 FC （ vFC ） LUN のプロビジョニングには、 Hyper-V Manager を使用する必要があります。 Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （ x ）でのデータベースのバックアップはサポートされていません。
Hyper-V VM	iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN	SnapCenter GUI または PowerShell コマンドレット	Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされた VHD （ x ）でのデータベースのバックアップはサポートされていません。

Exchange プラグインに必要な最小 ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
event generate-autosupport-log を指定します
ジョブ履歴の表示 ジョブが停止しました
LUN lun create をクリックします lun delete LUN igroup add lun igroup create を追加します lun igroup delete LUN igroup の名前を変更します lun igroup show を参照してください LUN マッピングの追加 - レポートノード LUN マッピングが作成されます LUN マッピングが削除されます LUN マッピングの削除 - レポートノード lun mapping show lun modify を追加します LUN のボリューム内移動 LUN はオフラインです LUN はオンラインです LUN の永続的予約はクリアします LUN のサイズ変更 LUN シリアル lun show をクリックします

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SnapMirror ポリシー追加ルール snapmirror policy modify-rule snapmirror policy remove-rule 」を実行します snapmirror policy show の略 SnapMirror リストア snapmirror show の略 snapmirror show -history の略 SnapMirror の更新 SnapMirror の update-ls-set snapmirror list-destinations
バージョン

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
volume clone create を実行します
volume clone show を実行します
ボリュームクローンスプリット開始
ボリュームクローンスプリットは停止します
volume create を実行します
ボリュームを削除します
volume file clone create を実行します
volume file show-disk-usage
ボリュームはオフラインです
ボリュームはオンラインです
volume modify を使用します
volume qtree create を実行します
volume qtree delete
volume qtree modify の略
volume qtree show の略
ボリュームの制限
volume show のコマンドです
volume snapshot create を実行します
ボリューム Snapshot の削除
volume snapshot modify の実行
ボリューム Snapshot の名前が変更されます
ボリューム Snapshot リストア
ボリューム Snapshot の restore-file
volume snapshot show の実行
ボリュームのアンマウント

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SVM CIFS です
vserver cifs share create の場合
SVM CIFS 共有が削除されます
vserver cifs shadowcopy show
vserver cifs share show のコマンドです
vserver cifs show のコマンドです
SVM エクスポートポリシー
vserver export-policy create を参照してください
vserver export-policy delete
vserver export-policy rule create
vserver export-policy rule show
vserver export-policy show のコマンドを入力します
Vserver iSCSI
vserver iscsi connection show
vserver show のコマンドです

読み取り専用コマンド： **ONTAP 8.3.0** 以降で必要な最小権限
Network Interface の略
network interface show の略
Vserver

SnapMirror レプリケーションと **SnapVault** レプリケーションのためのストレージシステムを準備

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenter は、Snapshotコピー処理の完了後に、SnapMirrorとSnapVault に対する更新を実行します。SnapMirror更新とSnapVault 更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SnapCenter は * sync-mirror * レプリケーションをサポートしていません。

Exchange Server リソースのバックアップ戦略を定義する

バックアップジョブを作成する前にバックアップ戦略を定義しておくと、データベースの正常なリストアに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービスレベルアグリーメント（ SLA ）、目標復旧時間（ RTO ）、および目標復旧時点（ RPO ）によって決まります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA 、 RTO 、および RPO は、バックアップ戦略に関与します。

Exchange データベースでサポートされるバックアップのタイプ

SnapCenter を使用して Exchange メールボックスをバックアップするには、データベースやデータベース可用性グループ（ DAG ）などのリソースタイプを選択する必要があります。Snapshot コピーテクノロジを使用して、リソースが存在するボリュームのオンラインの読み取り専用コピーが作成されます。

バックアップタイプ	説明
フルバックアップとログバックアップ	データベースおよび切り捨てられたログを含むすべてのトランザクションログがバックアップされます。 フルバックアップが完了すると、 Exchange Server はデータベースにコミット済みのトランザクションログを切り捨てます。 通常は、このオプションを選択します。ただし、バックアップ時間が短い場合は、フルバックアップでトランザクションログバックアップを実行しないように選択することもできます。
フルバックアップ	データベースとトランザクションログがバックアップされます。 切り捨てられたトランザクションログはバックアップされません。
ログバックアップ	すべてのトランザクションログがバックアップされます。 データベースにコミット済みの切り捨てられたログはバックアップされません。フルデータベースバックアップ間にトランザクションログを頻繁にバックアップするようにスケジュールを設定すると、リカバリポイントをさらに細かく選択できます。

データベースプラグインのバックアップスケジュール

バックアップ頻度（スケジュールタイプ）はポリシーで指定され、バックアップスケジュールはリソースグループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA と RPO は、データ保護戦略に関与します。

使用頻度の高いリソースであっても、フルバックアップは 1 日に 1~2 回で十分です。たとえば、定期的なトランザクションログバックアップを実行すれば、必要なバックアップが作成されます。データベースをバックアップする回数が多いほど、リストア時に SnapCenter が使用する必要のあるトランザクションログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度

バックアップ頻度（バックアップを実行する間隔）は、ポリシー設定の一部であり、一部のプラグインでは _ schedule type__ と呼ばれます。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しない場合は、オンデマンドのみのポリシーが作成されます。ポリシーにアクセスするには、 * Settings * > * Policies * をクリックします。

- バックアップスケジュール

  バックアップスケジュール（バックアップが実行される日時）は、リソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます。リソースグループのスケジュールにアクセスするには、 * リソース * > * リソースグループ * をクリックします。

データベースに必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービスレベルアグリーメント（ SLA ）などがあります。

バックアップの命名規則

Snapshot コピーのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- _dts1_は リソースグループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、「 * Snapshot コピーにカスタム名形式を使用」を選択して、リソースまたはリソースグループを保護しながら Snapshot コピー名の形式を指定することもできます。たとえば、customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名にタイムスタンプのサフィックスが追加されます。

バックアップ保持オプション

バックアップコピーを保持する日数を選択するか、保持するバックアップコピーの数を指定できます。指定できる最大数は ONTAP で 255 個です。たとえば、組織の必要に応じて、 10 日分のバックアップコピーや 130 個のバックアップコピーを保持できます。

ポリシーを作成する際に、バックアップタイプおよびスケジュールタイプの保持オプションを指定できます。

SnapMirror レプリケーションを設定すると、デスティネーションボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、保持されているバックアップの保持ラベルがスケジュールタイプと一致する場合には、バックアップを削除します。リソースまたはリソースグループに対してスケジュールタイプが変更された場合、古いスケジュールタイプラベルのバックアップがシステムに残ることがあります。

バックアップコピーを長期にわたって保持する場合は、 SnapVault バックアップを使用する必要があります。

Exchange Server のソースストレージボリュームにトランザクションログバックアップを保持する期間

SnapCenter Plug-in for Microsoft Exchange Server で最新の状態へのリストア処理を実行するには、トランザクションログバックアップが必要です。この場合、 2 つのフルバックアップの間の任意の時点の状態にデータベースがリストアされます。

たとえば、 Plug-in for Exchange で午前 8 時にフルとトランザクションログバックアップを作成しもう 1 つのフルおよびトランザクションログバックアップを午後 5 時に作成した場合は、最新のトランザクションログバックアップを使用して、午前 8 時から午後 5 時までの任意の時点の状態にデータベースをリストアできます午後 5 時までオープントランザクションログがない場合、 Plug-in for Exchange ではポイントインタイムリストア処理のみを実行できます。この場合、 Plug-in for Exchange がフルバックアップを完了した時点の状態にデータベースがリストアされます。

通常、最新の状態へのリストア処理が必要になるのは 1~2 日のみです。デフォルトでは、 SnapCenter は 2 日以上保持します。

Exchange データベースのリストア戦略を定義する

Exchange Server のリストア戦略を定義しておくと、それに従ってデータベースをリストアすることができます。

Exchange Server でのリストア処理のソースとなります

プライマリストレージ上のバックアップコピーから Exchange Server データベースをリストアすることができます。

データベースはプライマリストレージからのみリストアできます。

Exchange Server でサポートされるリストア処理のタイプ

SnapCenter を使用すると、 Exchange リソースに対してさまざまなタイプのリストア処理を実行できます。

- 最新の状態にリストアします
- 前の時点にリストアします

最新の状態にリストアします

最新の状態へのリストア処理では、障害発生時点までのデータベースのリカバリが行われます。SnapCenter では、この処理が次の順序で行われます。

1. 選択したフルデータベースバックアップからデータベースがリストアされます。

2. バックアップされたすべてのトランザクション・ログ、および最新のバックアップ以降に作成された新しいログを適用します。

   トランザクションログは事前に移動され、選択したデータベースに適用されます。

   リストアの完了後に、 Exchange は新しいログチェーンを作成します。

   * ベストプラクティス： * リストアの完了後に、新しいフルバックアップとログバックアップを実行することを推奨します。

   最新の状態へのリストア処理を実行するには、連続したトランザクションログセットが必要です。

   最新の状態へのリストアを実行すると、リストアに使用したバックアップを使用できるのはポイントインタイムリストア処理だけになります。

   すべてのバックアップに最新の状態へのリストア機能を使用する必要がない場合は、バックアップポリシーを使用してシステムのトランザクションログバックアップ保持を設定できます。

前の時点にリストアします

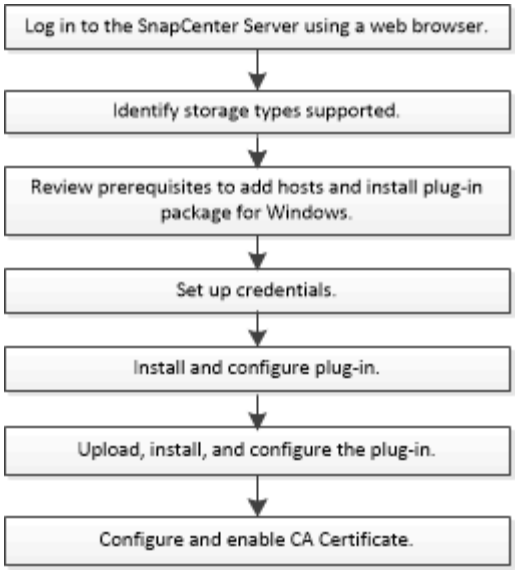
ポイントインタイムリストア処理では、データベースが過去の特定の時点にリストアされます。ポイントインタイムリストア処理は次の状況で発生します。

- バックアップトランザクションログの所定の時刻までデータベースをリストアする。
- データベースをリストアし、一部のバックアップトランザクションログだけを適用する。

SnapCenter Plug-in for Microsoft Exchange Server をインストールします

SnapCenter Plug-in for Microsoft Exchange Server のインストールワークフロー

Exchange データベースを保護する場合は、 SnapCenter Plug-in for Microsoft Exchange Server をインストールしてセットアップする必要があります。



ホストを追加して **SnapCenter Plug-in for Microsoft Exchange Server** をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSI を使用している場合は、 iSCSI サービスが実行されている必要があります。
- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。
- スタンドアロン構成およびデータベース可用性グループ構成で Microsoft Exchange Server 2013 、 2016 、または 2019 を使用している必要があります。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- SnapCenter でクラスタノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限を持つユーザが必要です。
- Exchange Server に対する管理者権限を持つユーザが必要です。
- SnapManager for Microsoft Exchange Server および SnapDrive for Windows がすでにインストールされている場合は、 SnapDrive を使用してデータを確実に保護するために、同じ Exchange サーバに Plug-in for Exchange をインストールする前に、 SnapCenter for Windows で使用する VSS ハードウェアプロバイダの登録を解除する必要があります。
- SnapManager for Microsoft Exchange Server と Plug-in for Exchange が同じサーバにインストールされている場合は、 SnapManager for Microsoft Exchange Server で作成されたすべてのスケジュールを Windows スケジューラから一時停止または削除する必要があります。
- ホストがサーバから完全修飾ドメイン名（ FQDN ）に解決できる必要があります。hosts ファイルが解決可能になるように変更され、短縮名と FQDN の両方が hosts ファイルに指定されている場合は、 SnapCenter hosts ファイルに次の形式でエントリを作成します： _<IP_address> <host_fqdn><host_name> _ 。
- 次のポートがファイアウォールでブロックされていないことを確認してください。ブロックされていないとホストの追加操作が失敗します。この問題を解決するには、ダイナミックポート範囲を設定する必要が

あります。詳細については、を参照してください "Microsoft のドキュメント"。

- Windows 2016 および Exchange 2016 のポート範囲 50000 ~ 51000
- Windows Server 2012 R2 および Exchange 2013 用のポート範囲 6000-6500
- Windows 2019 のポート範囲は 49152~65536 です

ポート範囲を特定するには、次のコマンドを実行します。

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp を実行します
- netsh int ipv6 show dynamicport udp

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Exchange Server の権限が必要です

SnapCenter で Exchange サーバまたは DAG を追加し、ホストまたは DAG に SnapCenter Plug-in for Microsoft Exchange Server をインストールできるようにするには、最小限の権限と権限を持つユーザのクレデンシャルを SnapCenter に設定する必要があります。

ローカル管理者の権限を持つドメインユーザと、リモート Exchange ホストに対するローカルログイン権限、および DAG 内のすべてのノードに対する管理権限を持つドメインユーザが必要です。ドメインユーザには、次の最小権限が必要です。

- Add-MailboxDatabaseCopy を追加します
- dismount - データベース
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup 」を参照してください
- Get-ExchangeServer
- MailboxDatabase を取得します
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics を実行します
- Get-PublicFolderDatabase を参照してください
- MOVE - ActiveMailboxDatabase
- move-DatabasePath-ConfigurationOnly:$true
- mount - データベース
- New-MailboxDatabase
- 新規 - PublicFolderDatabase
- MailboxDatabase を削除します
- MailboxDatabaseCopy を削除します
- -PublicFolderDatabase を削除します
- 履歴書 -MailboxDatabaseCopy
- 「設定」 -「サーバ設定
- MailboxDatabase-allowfilerestore を $true に設定します
- MailboxDatabaseCopy を設定します
- 「 - PublicFolderDatabase 」を設定します
- Suspend-MailboxDatabaseCopy を実行します
- Update-MailboxDatabaseCopy

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

SnapCenter Plug-in for Windows のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますプラグインパッケージをインストールするためのクレデンシャル、およびデータベースでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- このタスクについて *

Windows ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。ホストを導入してプラグインをインストールしたあとに Windows のクレデンシャルを作成することもできますが、SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定します。

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* 資格情報] をクリックします。
3. [新規作成（ New ）] をクリックする。

   [資格情報] ウィンドウが表示されます。

4. [クレデンシャル] ページで、次の操作を実行します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名	認証に使用するユーザ名を入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。 ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Usernameフィールドの有効な形式は次のとおりです。 `UserName`
パスワード	認証に使用するパスワードを入力します。
認証	認証モードとして Windows を選択します。

5. [OK] をクリックします。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
   a. 次の形式でユーザグループアカウントを作成します。

```
 domainName\accountName$
.. グループにコンピュータオブジェクトを追加します。
.. 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. を実行します `Get-ADServiceAccount`
サービスアカウントを確認するコマンド。
```

4. ホストで gMSA を設定します。
   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. ホストを再起動します。

b. PowerShellコマンドプロンプトから次のコマンドを実行して、ホストにgMSAをインストールします。 `Install-AdServiceAccount <gMSA>`

c. 次のコマンドを実行して'gMSAアカウントを確認します `Test-AdServiceAccount <gMSA>`

1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

   SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

ホストを追加し、 **Plug-in for Exchange** をインストールします

SnapCenter のホストの追加ページを使用して、 Windows ホストを追加できます。指定したホストに Plug-in for Exchange が自動的にインストールされます。これはプラグインのインストールに推奨される方法です。ホストを追加してプラグインをインストールするには、個々のホストまたはクラスタを使用します。

- 必要なもの *
- SnapCenter Admin など、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- メッセージキューサービスが実行されている必要があります。
- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。詳細については、を参照してください

"Microsoft Exchange Server 2012 以降でグループマネージドサービスアカウントを設定します"。

- このタスクについて *
- SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。
- ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。
- Exchange ノードが DAG の一部である場合、 SnapCenter サーバに追加できるノードは 1 つだけです。
- クラスタ（ Exchange DAG ）にプラグインをインストールする場合は、ネットアップ LUN 上にデータベースがないノードがある場合でも、クラスタのすべてのノードにインストールされます。

SnapCenter 4.6 以降では、 SCE はマルチテナンシーをサポートしており、次の方法を使用してホストを追加できます。

ホスト追加処理	**4.5**以前	**4.6**以降
IP なしの DAG をクロスドメインまたは別のドメインに追加	サポート対象外	サポートされます
同じドメインまたはクロスドメインにそれぞれ固有の名前を持つ複数の IP DAG を追加します	サポートされます	サポートされます
クロスドメインに、ホスト名と DB 名が同じ IP DAG または IP レス DAG を複数追加する	サポート対象外	サポートされます
同じ名前でクロスドメインに属する IP/IP を行わない DAG を複数追加します	サポート対象外	サポートされます
同じ名前とクロスドメインを持つ複数のスタンドアロンホストを追加します	サポート対象外	サポートされます

Plug-in for Exchange は Windows 用 SnapCenter プラグインパッケージによって異なり、バージョンも同じである必要があります。Plug-in for Exchange のインストール時に、デフォルトで SnapCenter Plug-ins Package for Windows が選択され、 VSS Hardware Provider とともにインストールされます。

SnapManager for Microsoft Exchange Server と SnapDrive for Windows がすでにインストールされている場合は、 同じ Exchange サーバに Plug-in for Exchange をインストールする場合は、 Plug-in for Exchange および SnapCenter Plug-ins Package for Windows と互換性がないため、 SnapDrive for Windows で使用する VSS ハードウェアプロバイダの登録を解除する必要があります。詳細については、を参照してください "Data ONTAP VSS ハードウェアプロバイダを手動で登録する方法"。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] が選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の手順を実行します。

フィールド	手順
ホストタイプ	ホストタイプとして * windows * を選択します。 SnapCenter サーバによってホストが追加され、 Plug-in for Windows と Plug-in for Exchange がまだインストールされていない場合はホストにインストールされます。 Plug-in for Windows および Plug-in for Exchange のバージョンが同じである必要があります。以前に別のバージョンの Plug-in for Windows がインストールされていた場合、 SnapCenter のインストール時にこのバージョンが更新されます。

フィールド	手順
ホスト名	ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、ベストプラクティスは Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を入力することです。 信頼されていないドメインホストの IP アドレスは、 FQDN に解決される場合にのみサポートされます。 SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • Exchange DAG Exchange DAG の場合、次の操作を実行できます。 ◦ DAG 名、 DAG の IP アドレス、ノード名、またはノードの IP アドレスを指定して DAG を追加します。 ◦ DAG クラスタのいずれかのノードの IP アドレスまたは FQDN を指定して、 IP なしの DAG クラスタを追加します。 ◦ 同じドメインまたは別のドメインに属する IP なしの DAG を追加します。同じ名前でドメインが異なる複数の IP/IP が少ない DAG を追加することもできます。 スタンドアロンホストまたは Exchange DAG （クロスドメインまたは同じドメイン）の場合は、ホストまたは DAG の FQDN または IP アドレスを指定することを推奨します。

フィールド	手順
クレデンシャル	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 資格情報認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。

   Plug-in for Exchange を選択すると、 SnapCenter Plug-in for Microsoft SQL Server の選択が自動的に解除されます。Microsoft では、 Exchange で必要とされるメモリの使用量やその他のリソースの使用量が原因で、 SQL Server と Exchange サーバを同じシステムにインストールしないことを推奨しています。

6. （オプション） * その他のオプション * をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	デフォルトパスはです `C:\Program Files\NetApp\SnapCenter`。 必要に応じて、パスをカスタマイズできます。
DAG 内のすべてのホストを追加します	DAG を追加する場合は、このチェックボックスを選択します。

フィールド	手順
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	グループ管理サービスアカウント（ GMSA ）を使用してプラグインサービスを実行する場合は、このチェックボックスをオンにします。 gMSA 名を *domainName\accountName$* の形式で指定します。 gMSA は、 SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されます。

7. [Submit （送信）] をクリックします。

   Skip ケーブルの事前確認チェックボックスを選択しなかった場合は、プラグインのインストール要件を満たすかどうかをホストが検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

   エラーがディスクスペースまたはRAMに関連している場合は、にあるweb.configファイルを更新できます `C:\Program Files\NetApp\SnapCenter` Webappを使用して、デフォルト値を変更します。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

   HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

1. インストールの進行状況を監視します。

PowerShell コマンドレットを使用して、 SnapCenter サーバホストから Plug-in for Exchange をインストールします

Plug-in for Exchange は SnapCenter の GUI からインストールする必要があります。GUI を使用しない場合は、 SnapCenter サーバホストまたはリモートホストで PowerShell コマンドレットを使用できます。

- 必要なもの *
- SnapCenter サーバがインストールおよび設定されている必要があります。
- ホストのローカル管理者または管理者権限を持つユーザである必要があります。
- SnapCenter Admin など、プラグイン、インストール、およびアンインストールの権限のあるロールが割り当てられているユーザが必要です
- Plug-in for Exchange をインストールする前に、サポートされている構成のインストール要件と種類を確

認しておく必要があります。

- Plug-in for Exchange をインストールするホストには Windows ホストを使用する必要があります。
- 手順 *

1. SnapCenter サーバホストで、 _Open-SmConnection_cmdlet を使用してセッションを確立し、クレデンシャルを入力します。
2. Plug-in for Exchange をインストールするホストを追加するには、 _Add-SmHost_cmdlet と必要なパラメータを使用します。

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

ホストは、スタンドアロンホストでも DAG ホストでもかまいません。DAG を指定する場合は、 -IsDAG_parameter が必要です。

1. 必要なパラメータを指定して、 _Install-SmHostPackage_cmdlet を使用し、 Plug-in for Exchange をインストールします。

   このコマンドは、指定したホストに Plug-in for Exchange をインストールし、 SnapCenter にプラグインを登録します。

コマンドラインから **SnapCenter Plug-in for Exchange** をサイレントにインストールします

Plug-in for Exchange は、 SnapCenter ユーザインターフェイス内からインストールする必要があります。ただし、何らかの理由でインストールできない場合は、 Windows のコマンドラインから、 Plug-in for Exchange のインストールプログラムをサイレントモードで自動的に実行できます。

- 必要なもの *
- Microsoft Exchange Server リソースをバックアップしておく必要があります。
- SnapCenter プラグインパッケージをインストールしておく必要があります。
- をインストールする前に、以前のリリースの SnapCenter Plug-in for Microsoft SQL Server を削除する必要があります。

  詳細については、を参照してください "SnapCenter Plug-in をプラグインホストから手動で直接インストールする方法"。

- 手順 *

1. プラグインホストに _C ： \temp_folder が存在し、ログインしているユーザにフルアクセス権があるかどうかを確認します。
2. C ： \ProgramData\NetApp\SnapCenter \Package_Repository から SnapCenter Plug-in for Microsoft Windows をダウンロードします。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

3. プラグインをインストールするホストにインストールファイルをコピーします。
4. ローカルホストの Windows コマンドプロンプトで、プラグインのインストールファイルを保存したディレクトリに移動します。
5. 次のコマンドを入力して、プラグインをインストールします。

   _snapcenter _windows_host_plugin.exe "/silent/debuglog "<Debug_Log_Path>" /log" <Log_Path>" b_SNAPCENTER_port=<Num>Suite_INSTALLDIR="<Install_Directory_Path>" BV_ServiceAccount=<domain\administrator> BV_SERVICEPCPWD = <SCW> インストール、 ISW>

   例：

   C ： \ProgramData\NetApp\SnapCenter \Package Repository_snapcenter _windows_host_plugin.exe "/silent/debuglog" C ： \HPPW_SCSQL_Install.log "/log" C ： \temp\temp\b_SNAPCENTER_PORT = 8145 Suite_INSTALLDIR=" C ： \Program Files\NetApp\SnapManager SnapCenter \BIT_VISPRI 管理者パスワードです

   Plug-in for Exchange のインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

   変数には次の値を入力します。

変数（ **Variable** ）	価値
	インストーラのログファイルの名前と場所を次のように指定します。 *Setup.exe /debuglog "C:\PathToLog\setupexe.log*
BI _ SNAPCENTER_PORT	SnapCenter が SMCore と通信するポートを指定します。
SUITE_INSTALLDIR	ホストのプラグインパッケージのインストールディレクトリを指定します。
BY_ServiceAccount の場合	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントを指定します。
BI_SERVVICEPWD	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントのパスワードを指定します。
ISFeatureInstall	SnapCenter によってリモートホストに導入される解決策を指定します。

1. Windows タスクスケジューラ、メインインストールログファイル *C:\Installdebug.log* 、およびその他のインストールファイルを *C:\Temp*. で監視します。
2. *%temp%* ディレクトリを監視して、 _msiexe.exe_installers がエラーなしでソフトウェアをインストールしているかどうかを確認します。

Plug-in for Exchange をインストールすると、 SnapCenter サーバではなくホストにプラグインが登録されます。SnapCenter サーバにプラグインを登録するには、SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加します。ホストを追加すると、プラグインが自動的に検出されます。

SnapCenter プラグインパッケージのインストールステータスを監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
     a. [* フィルタ * （ Filter * ）] をクリック
     b. オプション：開始日と終了日を指定します。
     c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
     d. Status ドロップダウンメニューから、インストールステータスを選択します。
     e. [適用（ Apply ）] をクリックします。
  4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *

1. GUI で次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
   c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
   d. ボックスから 16 進文字をコピーします。
   e. 16 進数の間のスペースを削除します。

      たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

2. PowerShell で次の手順を実行します。
   a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

      Get-ChildItem - パス証明書： *\localmachine\My*

   b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して **CA** 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

. 次のコマンドを実行して、新しくインストールした証明書を `Windows` ホストプラグインサービスにバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
certhash=$cert appid="$guid"
```

例：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

プラグインの **CA** 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

Exchange と SnapCenter が共存するように SnapManager 7.x を設定します

SnapCenter Plug-in for Microsoft Exchange Server を SnapManager for Microsoft Exchange Server と共存できるようにするには、 SnapManager for Microsoft Exchange Server がインストールされている Exchange Server と同じ Exchange Server に SnapCenter Plug-in for Microsoft Exchange Server をインストールし、 SnapManager for Exchange のスケジュールを無効にする必要があります。 および SnapCenter Plug-in for Microsoft Exchange Server を使用して新しいスケジュールとバックアップを設定します。

- 必要なもの *
- SnapManager for Microsoft Exchange Server と SnapDrive for Windows がすでにインストールされており、システムおよび SnapInfo ディレクトリに SnapManager for Microsoft Exchange Server のバックアップが存在します。
- SnapManager for Microsoft Exchange Server で作成された不要なバックアップを削除または再利用しておく必要があります。
- SnapManager for Microsoft Exchange Server で作成されたすべてのスケジュールを、 Windows スケジューラから一時停止または削除しておく必要があります。
- SnapManager Plug-in for Microsoft Exchange Server と SnapCenter for Microsoft Exchange Server は同じ Exchange サーバ上に共存できますが、既存の SnapManager for Microsoft Exchange Server を SnapCenter にアップグレードすることはできません。

  SnapCenter には、アップグレードのオプションはありません。

- SnapCenter では、 SnapManager for Microsoft Exchange Server バックアップからの Exchange データベースのリストアはサポートされていません。

  SnapCenter Plug-in for Microsoft Exchange Server のインストール後に SnapManager for Microsoft Exchange Server をアンインストールしないで、 SnapManager for Microsoft Exchange Server のバックアップをリストアする場合は、追加の手順を実行する必要があります。

- 手順 *

1. すべての DAG ノードで PowerShell を使用して、 SnapDrive for Windows VSS ハードウェアプロバイダが登録されているかどうかを確認します。 *vssadmin list provider*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
   Version: 7. 1. 4. 6845
```

2. SnapDrive ディレクトリから、 SnapDrive for Windows から VSS ハードウェアプロバイダの登録を解除します。 *navssprv.exe -r service – u*
3. VSS ハードウェアプロバイダが削除されたことを確認します。 *vssadmin list providers*
4. SnapCenter に Exchange ホストを追加し、 SnapCenter Plug-in for Microsoft Windows および SnapCenter Plug-in for Microsoft Exchange Server をインストールします。
5. すべての DAG ノードの SnapCenter Plug-in for Microsoft Windows ディレクトリで、 VSS ハードウェアプロバイダが登録されていることを確認します： *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. SnapManager for Microsoft Exchange Server のバックアップスケジュールを停止します。
7. SnapCenter GUI を使用して、オンデマンドバックアップの作成、スケジュールされたバックアップの設定、保持の設定を行います。
8. SnapManager for Microsoft Exchange Server をアンインストールします。

   SnapManager for Microsoft Exchange Server を今すぐアンインストールしないで、 SnapManager for Microsoft Exchange Server のバックアップをリストアする場合は、次の手順を実行します。

   a. すべての DAG ノードから SnapCenter Plug-in for Microsoft Exchange Server の登録を解除します。 _navssprv.exe -r service -u _

      ```
      C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for
      Microsoft Windows>navssprv.exe -r service -u
      ```

   b. C ： \Program Files\NetApp\SnapManager \SnapDrive_directory から、すべての DAG ノードに

SnapDrive for Windows を登録します。 _navssprv.exe -r service -c hostname \\username -p password_

SnapCenter Plug-in for VMware vSphere をインストール

データベースが仮想マシン（ VM ）に格納されている場合や VM とデータストアを保護する場合は、 SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください "導入の概要"。

CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください "SSL 証明書を作成またはインポートします"。

CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere は、事前に設定されたディレクトリ内の CRL ファイルを検索します。VMware vSphere 用 SnapCenter プラグインの CRL ファイルのデフォルトディレクトリは、_/opt/NetApp/config/crl_です 。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

データ保護を準備

バックアップ、クローニング、リストアなどのデータ保護処理を実行する場合は、事前に戦略を定義し、環境をセットアップする必要があります。また、 SnapVault サーバで SnapMirror テクノロジと SnapCenter テクノロジを使用するように設定することもできます。

SnapVault テクノロジと SnapMirror テクノロジを活用するには、ストレージデバイス上のソースボリュームとデスティネーションボリューム間のデータ保護関係を設定して初期化する必要があります。これらのタスクを実行するには、 NetAppSystem Manager を使用するか、ストレージコンソールのコマンドラインを使用します。

- 詳細はこちら *

"REST API の使用を開始する"

SnapCenter Plug-in for Microsoft Exchange Server を使用するための前提条件

Plug-in for Exchange を使用するには、 SnapCenter 管理者が事前に SnapCenter サーバをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。
- SnapCenter にログインします。
- ストレージシステム接続を追加または割り当て、クレデンシャルを作成して、 SnapCenter 環境を設定し

ます。

SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SnapCenter でサポートする SVM には、それぞれ一意の名前を付ける必要があります。

- ホストを追加し、 SnapCenter Plug-in for Microsoft Windows と SnapCenter Plug-in for Microsoft Exchange Server をインストールし、それらのリソースを検出（更新）します。
- SnapCenter Plug-in for Microsoft Windows を使用して、ホスト側のストレージをプロビジョニングします。
- VMware RDM LUN に存在する Exchange データベースを SnapCenter Server で保護する場合は、 SnapCenter Plug-in for VMware vSphere を導入し、 SnapCenter に登録する必要があります。詳細については、 SnapCenter Plug-in for VMware vSphere のドキュメントを参照してください。

  VMDK はサポートされません。

- Microsoft Exchange ツールを使用して、既存の Microsoft Exchange Server データベースをローカルディスクからサポートされているストレージに移動します。
- バックアップレプリケーションが必要である場合は、 SnapMirror 関係と SnapVault 関係をセットアップします。

SnapCenter 4.1.1 ユーザの場合、 SnapCenter Plug-in for VMware vSphere 4.1.1 のドキュメントには、仮想化されたデータベースとファイルシステムの保護に関する情報が記載されています。SnapCenter 4.2.x ユーザの場合、 NetApp Data Broker 1.0 および 1.0.1 のドキュメントでは、 Linux ベースの NetApp Data Broker 仮想アプライアンス（オープン仮想アプライアンス形式）が提供する SnapCenter Plug-in for VMware vSphere を使用して、仮想化されたデータベースとファイルシステムを保護する方法について説明しています。SnapCenter 4.3.x を使用する場合は、 Linux ベースの SnapCenter Plug-in for VMware vSphere 仮想アプライアンス（オープン仮想アプライアンス形式）を使用して仮想化されたデータベースとファイルシステムを保護する方法について、 SnapCenter Plug-in for VMware vSphere 4.3 のドキュメントを参照してください。

"SnapCenter Plug-in for VMware vSphere のドキュメント"

Exchange Server の保護におけるリソース、リソースグループ、ポリシーの使用方法

SnapCenter を使用する前に、実行するバックアップ、リストア、および再シードの処理に関する基本的な概念を理解しておくと役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- リソースとは、通常は SnapCenter でバックアップするメールボックスデータベースまたは Microsoft Exchange データベース可用性グループ（ DAG ）のことです。
- SnapCenter リソースグループは、ホストまたは Exchange DAG のリソースの集まりで、リソースグループには DAG 全体または個別データベースのいずれかを含めることができます。

  リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているリソースに対して処理が実行されます。

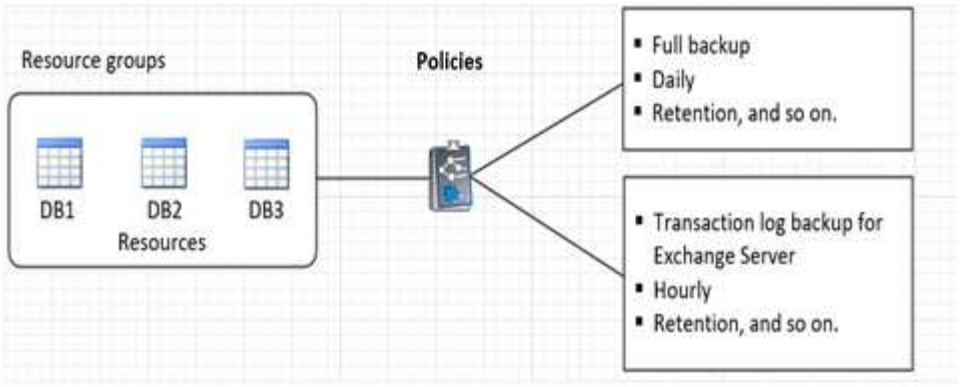
  単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。スケジュールされたバックアップを単一のリソースおよびリソースグループに対して実行することもできます。

  リソースグループは、以前はデータセットと呼ばれていました。

- ポリシーは、バックアップ頻度、コピーの保持、スクリプト、およびデータ保護処理のその他の特性を指定するものです。

  リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。単一のリソースに対してオンデマンドでバックアップを実行する場合は、ポリシーを 1 つ以上選択することもできます。

リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、ホストのすべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。リソースグループを作成してポリシーを適用する際に、フルバックアップを 1 日 1 回実行するようにリソースグループを設定し、別のスケジュールでログバックアップを 1 時間おきに実行するように設定します。次の図は、データベースのリソース、リソースグループ、およびポリシーの関係を示しています。



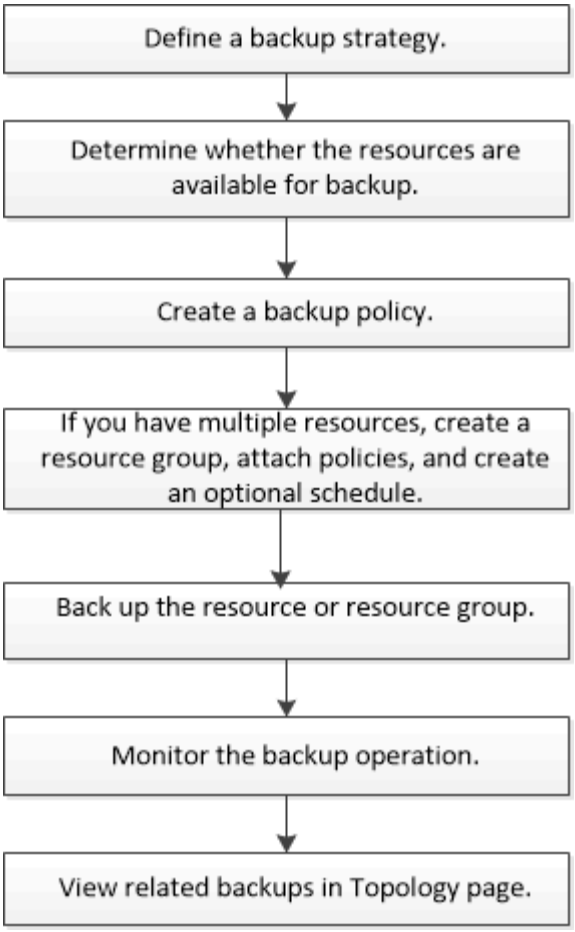
Exchange リソースをバックアップする

バックアップのワークフロー

SnapCenter Plug-in for Microsoft Exchange Server をインストールした環境では、SnapCenter を使用して Exchange リソースをバックアップすることができます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。バックアップ処理とリストア処理を同じリソースで同時に実行することはできません。同じボリューム上のアクティブおよびパッシブバックアップコピーはサポートされません。

次のワークフローは、バックアップ処理の実行順序を示しています。



Exchange データベースおよびバックアップの検証

SnapCenter Plug-in for Microsoft Exchange Server ではバックアップの検証は実行されませんが、 Exchange の Eseutil ツールを使用して Exchange データベースとバックアップを検証することができます。

Microsoft Exchange Eseutil ツールは、 Exchange サーバに組み込まれているコマンド・ライン・ユーティリティです。このユーティリティを使用すると、 Exchange データベースおよびバックアップの整合性チェックを実行して整合性を検証できます。

* ベストプラクティス： * 最低 2 つのレプリカを含む DAG 構成の一部であるデータベースに対して、整合性チェックを実行する必要はありません。

追加情報の場合は、を参照してください "Microsoft Exchange Server のマニュアル"。

Exchange リソースをバックアップに使用できるかどうかを確認します

リソースとは、インストールしたプラグインで管理されているデータベースと Exchange データベース可用性グループです。リソースをリソースグループに追加することでデータ保護ジョブを実行できますが、その前に利用可能なリソースを特定しておく必要があります。使用可能なリソースを確認することで、プラグインのインストールが正常に完了したことの確認にもなります。

- 必要なもの *
- SnapCenter サーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加、 Plug-in for Exchange のインストールなどのタスクを完了しておく必要があります。
- Single Mailbox Recovery ソフトウェアの機能を利用するには、 Single Mailbox Recovery ソフトウェアがインストールされている Exchange サーバ上に、アクティブデータベースを配置する必要があります。
- データベースが VMware RDM LUN にある場合は、 SnapCenter Plug-in for VMware vSphere を導入し、SnapCenter に登録する必要があります。。 "SnapCenter Plug-in for VMware vSphere のドキュメント" に詳細を示します。
- このタスクについて *
- [詳細] ページの [全体のステータス *] オプションが [バックアップに使用できない] に設定されている場合は、データベースをバックアップできません。次のいずれかに該当する場合、 * Overall Status * オプションはバックアップに使用できない状態に設定されます。
  - データベースが NetApp LUN 上にない。
  - データベースが正常な状態でない。

    マウント、アンマウント、再シード、またはリカバリを保留中の状態のデータベースは、正常な状態ではありません。
- Database Availability Group （ DAG ；データベース可用性グループ）がある場合は、 DAG からバックアップジョブを実行して、グループ内のすべてのデータベースをバックアップできます。
- 手順 *

1. 左側のナビゲーションペインで、 [リソース] をクリックし、 [リソース] ページの左上にあるプラグインのドロップダウンリストから [Microsoft Exchange Server*] を選択します。
2. リソースページで、 * 表示 * ドロップダウン・リストから * データベース * 、 * データベース可用性グループ * 、または * リソース・グループ * を選択します。

   複数のデータベースを区別できるよう、 DAG またはホスト名を FQDN 形式ですべて表示するデータベースと DAG があります。

   をクリックします をクリックし、ホスト名と Exchange サーバを選択してリソースをフィルタリングします。をクリックします をクリックしてフィルタペインを閉じます。
3. [リソースの更新] をクリックします。

   新しく追加、名前変更、または削除されたリソースは、 SnapCenter サーバインベントリに更新されます。

   データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

   リソースは、リソース名、データベース可用性グループ名、データベースが現在アクティブであるサーバ、コピーを備えたサーバ、前回のバックアップ時刻、全体的なステータスなどの情報とともに表示されます。

   - ネットアップ以外のストレージにデータベースがある場合、バックアップに使用できない状態は Overall Status 列に表示されます。

DAG では、アクティブなデータベースコピーがネットアップ以外のストレージにある場合に、少なくとも 1 つのパッシブデータベースコピーがネットアップストレージにあると、「全体のステータス」列には保護されていないと表示されます。

ネットアップ以外のストレージタイプのデータベースには、データ保護処理を実行できません。

- データベースがネットアップストレージ上にあり、保護されていない場合は、「 * Overall Status * 」列に保護されていないことが表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合、ユーザインターフェイスの「バックアップ実行なし」というメッセージが「総合ステータス」列に表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合に、データベースのバックアップがトリガされると、ユーザインターフェイスの「 Backup succeeded 」というメッセージが「 * Overall Status * 」列に表示されます。

Exchange Server データベースのバックアップポリシーを作成する

SnapCenter を使用して Microsoft Exchange Server リソースをバックアップする前に、Exchange リソースまたはリソースグループのバックアップポリシーを作成することができます。また、リソースグループの作成時や単一のリソースのバックアップ時にバックアップポリシーを作成することもできます。

- 必要なもの *
- データ保護戦略を定義しておく必要があります。

  詳細については、 Exchange データベースのデータ保護戦略の定義に関する情報を参照してください。

- SnapCenter のインストール、ホストの追加、リソースの特定、ストレージシステム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Exchange Server リソースを更新（検出）しておく必要があります。
- Snapshot コピーをミラーまたはバックアップにレプリケートするユーザには、 SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に Storage Virtual Machine （ SVM ）を割り当てる必要があります。
- プリスクリプトとポストスクリプトでPowerShellスクリプトを実行する場合は、の値を設定する必要があります `usePowershellProcessforScripts` パラメータをTRUEに設定します `web.config` ファイル。

  デフォルト値は false です。

- このタスクについて *
- バックアップポリシーとは、バックアップを管理および保持する方法やリソースやリソースグループをバックアップする頻度を定めた一連のルールです。また、スクリプト設定を指定することもできます。ポリシーでオプションを指定しておくことで、別のリソースグループにポリシーを再利用して時間を節約することができます。
- フルバックアップの保持は指定されたポリシーに固有です。フルバックアップ保持が 4 に設定されたポリシー A を使用するデータベースまたはリソースはフルバックアップを 4 つ保持し、同じデータベースまたはリソースのポリシー B には影響しません。これにより、フルバックアップを 3 つ保持するように 3 つ保持できます。

- ログバックアップの保持は、ポリシーを問わず有効であり、データベースやリソースのすべてのログバックアップを環境で保持できます。したがって、ポリシー B を使用してフルバックアップを実行すると、同じデータベースまたはリソース上のポリシー A で作成されるログバックアップにログ保持設定が適用されます。同様に、ポリシー A のログ保持設定は、同じデータベースのポリシー B で作成されるログバックアップに影響します。
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

* ベストプラクティス： * 維持するフルバックアップとログバックアップの総数に基づいて、セカンダリ保持ポリシーを設定することを推奨します。セカンダリの保持ポリシーを設定する場合、異なるボリュームにあるデータベースとログの Snapshot コピーは、各バックアップに 3 つ作成できます。また、データベースとログが同じボリュームにある場合、各バックアップに 2 つの Snapshot コピーを保持できます。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. [Backup Type] ページで、次の手順を実行します。

   a. バックアップタイプを選択します。

状況	手順
データベースファイルと必要なトランザクションログをバックアップします	[フルバックアップおよびログバックアップ *] を選択します。 データベースはログを切り捨ててバックアップされ、切り捨てられたログを含むすべてのログがバックアップされます。 これは推奨されるバックアップタイプです。
データベースファイルおよびコミットされていないトランザクションログをバックアップします	[* Full backup*] を選択します。 ログを切り捨ててデータベースをバックアップし、切り捨てられたログはバックアップされません。

状況	手順
すべてのトランザクションログをバックアップします	「 * Log backup * 」を選択します。 アクティブファイルシステムのすべてのトランザクションログがバックアップされており、ログが切り捨てられていません。 ライブログと同じディスクに _scebackupinfo_directory が作成されます。このディレクトリには、 Exchange データベースの増分変更へのポインタが格納されます。このディレクトリは、完全なログファイルには相当しません。
トランザクションログファイルを切り捨てずに、すべてのデータベースファイルとトランザクションログをバックアップします	Copy Backup （バックアップのコピー） * を選択します。 すべてのデータベースとすべてのログがバックアップされ、ログが切り捨てられることはありません。通常、このバックアップタイプは、レプリカの再シード、または問題のテストや診断に使用します。

ログバックアップに必要なスペースは、最新の状態への（ UTM ）保持にではなく、フルバックアップ保持に基づいて定義する必要があります。

Exchangeボリューム（LUN）を扱う場合は、ログとデータベースに対して個別のバックアップポリシーを作成し、同じラベルを使用して、ログポリシーのkeep（retention）をデータベースポリシーの2倍の数に設定します。詳細については、を参照してください。 "SnapCenter for Exchangeバックアップでは、バックアップデスティネーションログボリュームに保持されるSnapshotの半分だけが保持されます"

b. Database Availability Group Settings セクションで、次の操作を選択します。

フィールド	手順
アクティブなコピーをバックアップする	選択したデータベースのアクティブコピーのみをバックアップする場合は、このオプションを選択します。 Database Availability Group （ DAG ；データベース可用性グループ）の場合、このオプションは DAG 内のすべてのデータベースのアクティブコピーのみをバックアップします。 パッシブコピーはバックアップされません。

フィールド	手順
バックアップジョブの作成時に選択されるサーバ上のバックアップコピー	このオプションは、アクティブとパッシブの両方で、選択したサーバ上のデータベースのコピーをバックアップする場合に選択します。 DAG では、選択したサーバ上のすべてのデータベースのアクティブコピーとパッシブコピーの両方がバックアップされます。

クラスタ構成では、ポリシーで設定された保持設定に従って、クラスタの各ノードにバックアップが保持されます。クラスタの所有者ノードが変更された場合、以前の所有者ノードのバックアップは保持されます。保持設定はノードレベルでのみ適用できます。

c. [スケジュール頻度] セクションで、 1 つ以上の頻度タイプを選択します。 * オンデマンド * 、 * 毎時 * 、 * 毎日 * 、 * 毎週 * 、および * 毎月 * 。

リソースグループを作成する際に、バックアップ処理のスケジュール（開始日、終了日）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。

午前 2 時にスケジュールを設定した場合、夏時間（ DST ）中はスケジュールはトリガーされません。

6. [保持] ページで ' 保持設定を構成します

表示されるオプションは、以前に選択したバックアップのタイプと頻度のタイプによって異なります。

最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。

SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。

a. [Log backups retention settings] セクションで、次のいずれかを選択します。

状況	手順
特定の数のログバックアップだけを保持します	ログを保持するフルバックアップの数を * 選択し、最新の状態へのリストアを実行するフルバックアップの数を指定します。 UTM （最新状態）保持の環境ログバックアップは、フルバックアップまたはログバックアップを使用して作成されます。たとえば、 UTM 保持設定が、最新の 5 つのフルバックアップのログバックアップを保持するように設定されている場合、最新の 5 つのフルバックアップのログバックアップが保持されます。 フルバックアップとログバックアップの一部として作成されたログフォルダは、 UTM の一部として自動的に削除されます。ログフォルダは手動で削除できません。たとえば、フルバックアップまたはフルバックアップの保持設定が 1 カ月に設定されていて、 UTM 保持が 10 日に設定されている場合、これらのバックアップの一部として作成されたログフォルダは UTM のように削除されます。そのため、ログフォルダは 10 日しか作成されず、それ以外のバックアップはすべてポイントインタイムリストアの対象としてマークされます。 最新の状態へのリストアを実行しない場合は、 UTM 保持値を 0 に設定できます。これにより、ポイントインタイムリストア処理が有効になります。 • ベストプラクティス： * フルバックアップ保持の設定セクションの「 Total Snapshot copies （フルバックアップ）」の設定と同じにすることを推奨します。これにより、フルバックアップのたびにログファイルが保持されます。
バックアップコピーを特定の日数だけ保持します	「 * Keep log backups for last * 」オプションを選択し、ログバックアップコピーを保持する日数を指定します。 フルバックアップを保持する日数までのログバックアップが作成されます。

バックアップタイプとして * Log backup * を選択した場合は、フルバックアップの最新の状態へのリストア保持設定の一部としてログバックアップが保持されます。

b. [フル・バックアップ保持設定] セクションで、オンデマンド・バックアップ用に次のいずれかを選択し、フル・バックアップ用に 1 つ選択します。

フィールド	手順
特定の数の Snapshot コピーだけを保持します	保持するフルバックアップの数を指定する場合は、「保持する Snapshot コピーの総数」オプションを選択し、保持する Snapshot コピー（フルバックアップ）の数を指定します。 フルバックアップの数が指定した数を超えると、指定した数を超えるフルバックアップが削除され、古いコピーから順番に削除されます。
フルバックアップを特定の日数だけ保持します	「 * Snapshot コピーを保持する期間」オプションを選択し、 Snapshot コピーを保持する日数（フルバックアップ）を指定します。

DAG 構成のホストにはログバックアップのみを使用し、フルバックアップは実行しないデータベースがある場合、ログバックアップは次の方法で保持されます。

- デフォルトでは、 SnapCenter は DAG 内の他のすべてのホストでこのデータベースの最も古いフルバックアップを検出し、フルバックアップの前に作成されたこのホスト上のすべてのログバックアップを削除します。
- ログバックアップのみを使用する DAG 内のホストのデフォルトの保持設定を上書きするには、 _C ： \Program Files\NetApp\SnapManager WebApp\web.config_file にキー * MaxLogBackupOnlyCountWithoutFullBackup * を追加します。

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

この例では、 10 という値は、ホストに最大 10 個のログバックアップを保持することを意味します。

7. レプリケーションページで、次のセカンダリレプリケーションオプションのいずれかまたは両方を選択します。

フィールド	手順
ローカル Snapshot コピーの作成後に SnapMirror を更新します	別のボリュームにバックアップセットのミラーコピーを保持する場合（ SnapMirror ）は、このオプションを選択します。
ローカル Snapshot コピーの作成後に SnapVault を更新します	ディスクツーディスクのバックアップレプリケーションを実行する場合は、このオプションを選択します。

フィールド	手順
セカンダリポリシーのラベル	Snapshot ラベルを選択します。 選択した Snapshot コピーラベルに応じて、ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。 ローカル Snapshot コピーの作成後に「 * SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できます。ただし、ローカル Snapshot コピーの作成後に「 * Update SnapVault 」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。
エラー再試行回数	レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。

セカンダリストレージでの Snapshot コピーの最大数に達しないように、 ONTAP でセカンダリストレージの SnapMirror 保持ポリシーを設定する必要があります。

8. スクリプトページで、バックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。
   - プリスクリプトのバックアップ引数には、「 $Database 」および「 $ServerInstance 」が含まれます。
   - PostScript バックアップ引数には、「 $Database 」、「 $ServerInstance 」、「 $BackupName 」、「 $LogDirectory 」、「 $LogSnapshot 」が含まれます。

     SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

1. 概要を確認し、 [完了] をクリックします。

Exchange Server のリソースグループを作成してポリシーを適用します

リソースグループはすべてのデータ保護ジョブに必要です。リソースグループに 1 つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプと保護スケジュールを定義することも必要です。

- このタスクについて *
- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- 手順 *

1. 左側のナビゲーションペインで、 [* リソース] をクリックし、リストから Microsoft Exchange Server プラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。

   最近 SnapCenter にリソースを追加した場合は、 [* リソースの更新 *] をクリックして、新しく追加したリソースを表示します。

3. [New Resource Group] をクリックします。
4. [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループ名を入力します。 リソースグループ名は 250 文字以内にする必要があります。
タグ	リソースグループを検索するときに役立つラベルを入力します。 たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。
Snapshot コピーには、カスタムの名前形式を使用します	オプション： Snapshot コピー名のカスタムの名前形式を入力します。 たとえば、_customtext_resourcegroup_policy_hostname_or_resourcegroup_hostname_hostname_or_resourcegroup_hostname_hostname_1 のようになります。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

5. Resources ページで、次の手順を実行します。
   a. リソースタイプと Database Availability Group from ドロップダウンリストを選択して、使用可能なリソースのリストをフィルタリングします。

最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

Available Resources セクションおよび Selected Resources セクションに、ホストの FQDN がデータベース名として表示されます。この FQDN は、指定したホスト上でデータベースがアクティブであり、このホストでバックアップを作成しない可能性があることを示します。バックアップ・ジョブ作成時に選択するサーバ上の * バックアップ・コピーのバックアップ・オプションを選択した場合に、バックアップを作成するサーバ選択オプションから 1 つ以上のバックアップ・サーバを選択する必要があります。

b. 検索テキストボックスにリソースの名前を入力するか、スクロールしてリソースを探します。

c. [使用可能なリソース] セクションから [選択したリソース] セクションにリソースを移動するには、次のいずれかの手順を実行します。

- 同じボリューム上のすべてのリソースを [選択したリソース] セクションに移動するには、 * 同一ストレージボリューム上のすべてのリソースを自動選択 * を選択します。
- [使用可能なリソース] セクションからリソースを選択し、右矢印をクリックして [選択したリソース] セクションに移動します。

SnapCenter for Microsoft Exchange Server のリソースグループに、 Snapshot コピー 1 つあたりのデータベース数を 30 個以下にする必要があります。1 つのリソースグループに 30 個を超えるデータベースがある場合、追加のデータベース用に 2 つ目の Snapshot コピーが作成されます。したがって、メインバックアップジョブの下に 2 つのサブジョブが作成されます。セカンダリレプリケーションがあるバックアップの場合、 SnapMirror または SnapVault の更新が進行中に、サブジョブが重複する状況が発生することがあります。メインのバックアップジョブは、ジョブが完了したことがログに記録されていても、常時稼働し続けます。

6. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

また、 * をクリックしてポリシーを作成することもできます *

バックアップ・ジョブ作成時に選択するサーバ上の * バックアップ・コピーがポリシーに含まれている場合は、サーバ選択オプションが表示され、 1 つ以上のサーバを選択できます。サーバを選択するオプションでは、選択したデータベースがネットアップストレージ上にあるサーバのみが表示されます。

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

b. [選択したポリシーのスケジュールを設定] セクションで、 * をクリックします * スケジュールを設定するポリシーの [スケジュールの設定 *] 列。

c. [Add schedules for policy_name_] ダイアログボックスで、開始日、有効期限、頻度を指定してスケジュールを設定し、 [*OK] をクリックします。

この処理は、ポリシーに指定されている頻度ごとに実行する必要があります。設定されたスケジュールは、 [選択したポリシーのスケジュールの設定] セクションの [適用されたスケジュール *] 列に一覧表示されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。

7. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、 [ジョブレポートの添付（ Attach Job Report ）] を選択します。

   Eメール通知を利用する場合は、GUIまたはPowerShellコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります `Set-SmSmtpServer`。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

1. 概要を確認し、 [完了] をクリックします。

Exchange データベースをバックアップします

データベースがどのリソースグループにも含まれていない場合は、のリソースページからデータベースまたはデータベース可用性グループをバックアップできます。

- 必要なもの *
- バックアップポリシーを作成しておく必要があります。
- バックアップ処理で使用されるアグリゲートを、データベースが使用する SVM に割り当てておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられるロールには「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- ネットアップストレージとネットアップ以外のストレージ上にアクティブ / パッシブデータベースコピーのあるデータベースまたはデータベース可用性グループのバックアップを実行する場合は、 また、ポリシーのバックアップ・ジョブ作成時間 * オプションで、サーバ上のバックアップ・アクティブ・コピー * またはバックアップ・コピーを選択した場合、バックアップ・ジョブは警告状態になります。ネットアップストレージ上のアクティブ / パッシブデータベースコピーのバックアップは成功し、ネットアップ以外のストレージ上のアクティブ / パッシブデータベースコピーのバックアップは失敗します。

  * ベストプラクティス： * アクティブデータベースとパッシブデータベースのバックアップは同時に実行しないでください。競合状態が発生し、いずれかのバックアップが失敗する可能性があります。

- 手順 *

1. 左側のナビゲーションペインで、 [* リソース] をクリックし、リストから [Microsoft Exchange Server プラグイン *] を選択します。
2. リソースページで、 * 表示 * リストから * データベース * または * データベース可用性グループ * のいずれかを選択します。

   リソースページで、を参照してください  アイコンは、データベースがネットアップ以外のストレ

ージにあることを示します。

DAG では、アクティブなデータベースコピーがネットアップ以外のストレージにあり、データベースのパッシブコピーが少なくとも 1 つネットアップストレージにある場合、データベースを保護できます。

- をクリックします* をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。次に、 * をクリックします* をクリックすると、フィルタペインが閉じます。
  - データベースをバックアップする場合は、データベース名をクリックします。
    i. Topology ビューが表示されたら、 **Protect** をクリックします。
    ii. Database Protect Resource （データベースの保護）ウィザードが表示された場合は、手順 3 に進みます。
  - データベース可用性グループをバックアップする場合は、データベース可用性グループの名前をクリックします。

1. カスタム Snapshot コピー名を指定する場合は、リソースページで Snapshot コピーにカスタム名形式を使用する * チェックボックスを選択し、 Snapshot コピー名に使用するカスタム名形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

2. [Policies] ページで、次の手順を実行します。
   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

   また、 * をクリックしてポリシーを作成することもできます *

   バックアップ・ジョブ作成時に選択するサーバ上の * バックアップ・コピーがポリシーに含まれている場合は、サーバ選択オプションが表示され、 1 つ以上のサーバを選択できます。サーバを選択するオプションでは、選択したデータベースがネットアップストレージ上にあるサーバのみが表示されます。

   [選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

   b. * をクリックします * スケジュールを設定するポリシーの [スケジュールの設定] 列。
   c. [Add schedules for policy_name] ウィンドウで、スケジュールを設定し、 [**OK**] をクリックします。

   ここで、 _policy_name_は 選択したポリシーの名前です。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。リソース上で実行されたバックアップ処理のレポートを添付する場合は、 [ジョブレポートの添付（ Attach Job Report ）] を選択します。

E メール通知を利用する場合は、 GUI または PowerShell コマンド Set-SmtpServer を使用して、 SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、 [完了] をクリックします。

   データベーストポロジのページが表示されます。

2. [今すぐバックアップ] をクリックします。
3. Backup （バックアップ）ページで、次の手順を実行します。
   a. リソースに複数のポリシーを適用している場合は、「 * Policy * 」ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. [バックアップ] をクリックします。
4. ページ下部の [アクティビティ] ペインでジョブをダブルクリックして、バックアップの進行状況を監視し、 [ジョブの詳細] ページを表示します。
   - MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。

     詳細については、を参照してください "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"

   - VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。

     Java のヒープサイズを増やすには、スクリプトファイル /opt/NetApp/init_scripts/scvservice_. を探します。このスクリプトでは、 *DO_START METHOD_Command* によって、 *SnapCenter VMware* プラグインサービスが開始されます。このコマンドを次のように更新します。 *_java -jar -Xmx8192M -Xms4096M*

Exchange リソースグループをバックアップする

リソースグループはホストまたは Exchange DAG のリソースの集まりで、リソースグループには DAG 全体または個々のデータベースを含めることができます。リソースグループは、のリソースページからバックアップできます。

- 必要なもの *
- ポリシーを適用したリソースグループを作成しておく必要があります。
- バックアップ処理で使用されるアグリゲートを、データベースが使用する Storage Virtual Machine （ SVM ）に割り当てておく必要があります。

- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられるロールには「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- リソースグループに異なるホストの複数のデータベースが含まれている場合は、ネットワークの問題が原因で一部のホストでのバックアップ処理が遅くなる可能性があります。の値を設定する必要があります `MaxRetryForUninitializedHosts` インチ `web.config` を使用します `Set-SmConfigSettings` PowerShellコマンドレット：
- リソースグループに、ネットアップストレージとネットアップ以外のストレージ上にアクティブ / パッシブデータベースコピーのあるデータベースまたはデータベース可用性グループが含まれていて、ポリシーでバックアップジョブの作成時に選択するサーバでアクティブ / パッシブデータベースコピーのバックアップ * または * バックアップコピーの選択が完了している場合： その後、バックアップジョブが警告状態になります。

  ネットアップストレージ上のアクティブ / パッシブデータベースコピーのバックアップは成功し、ネットアップ以外のストレージ上のアクティブ / パッシブデータベースコピーのバックアップは失敗します。

- このタスクについて *

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

- 手順 *

1. 左側のナビゲーションペインで、 [* リソース] をクリックし、リストから [Microsoft Exchange Server プラグイン *] を選択します。
2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。

   リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 * をクリックします * をクリックし、タグを選択します。次に、 * をクリックします * をクリックすると、フィルタペインが閉じます。

3. [リソースグループ] ページで、バックアップするリソースグループを選択し、 [今すぐバックアップ *] をクリックします。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. [バックアップ] をクリックします。
5. ページ下部の [アクティビティ] ペインでジョブをダブルクリックして、バックアップの進行状況を監視し、 [ジョブの詳細] ページを表示します。

Exchange Server 用の PowerShell コマンドレットを使用して、ストレージシステム接続とクレデンシャルを作成します

PowerShell コマンドレットを使用してバックアップとリストアを実行するには、

Storage Virtual Machine （ SVM ）接続とクレデンシャルを作成する必要があります。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

- 手順 *

1. を使用して、PowerShell接続セッションを開始します `Open-SmConnection` コマンドレット。

   PowerShell セッションを開く例を次に示します。

   ```
   PS C:\> Open-SmConnection
   ```

2. を使用して、ストレージシステムへの新しい接続を作成します `Add-SmStorageConnection` コマンドレット。

   この例では、新しいストレージシステム接続を作成しています。

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. を使用して、新しいRun Asアカウントを作成します `Add-Credential` コマンドレット。

   次の例では、 Windows クレデンシャルを使用して ExchangeAdmin という名前の新しい Run As アカウントを作成します。

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
-Credential sddev\administrator
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

PowerShell コマンドレットを使用して Exchange リソースをバックアップします

Exchange Server データベースをバックアップする場合は、 SnapCenter サーバとの接続を確立し、 Exchange サーバデータベースを検出し、ポリシーの追加、バックアップリソースグループの作成、バックアップ、およびバックアップステータスの表示を行います。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。
- ホストを追加し、リソースを検出しておく必要があります。

Plug-in for Exchange ではクローン操作はサポートされません。そのため、 Add-SmPolicy コマンドレットの CloneType パラメータは Plug-in for Exchange ではサポートされていません

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmPolicy コマンドレットを使用してバックアップポリシーを作成します。

この例では、フルバックアップとログバックアップの Exchange バックアップタイプを指定して新しいバックアップポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

この例では、時間単位のフルバックアップとログバックアップ Exchange バックアップを指定して、新しいバックアップポリシーを作成します。

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

この例では、 Exchange ログのみをバックアップする新しいバックアップポリシーを作成しています。

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Get-SmResources コマンドレットを使用して、ホストリソースを検出します。

   この例では、指定したホスト上で Microsoft Exchange Server プラグインのリソースを検出しています。

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

4. Add-SmResourceGroup コマンドレットを使用して、新しいリソースグループを SnapCenter に追加します。

   この例では、ポリシーとリソースを指定して新しい Exchange Server データベースバックアップリソースグループを作成しています。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log
_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

   この例では、ポリシーとリソースを指定して新しい Exchange Database Availability Group （ DAG ；データベース可用性グループ）バックアップリソースグループを作成しています。

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log
_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

5. New-SmBackup コマンドレットを使用して、新しいバックアップジョブを開始する。

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

   この例では、セカンダリストレージに新しいバックアップを作成します。

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Get-SmBackupReport コマンドレットを使用して、バックアップジョブのステータスを表示します。

   次の例は、指定した日付に実行されたすべてのジョブの概要レポートを表示します。

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

   次の例は、特定のジョブ ID のジョブ概要レポートを表示します。

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

バックアップ処理を監視する

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. Jobs （ジョブ）ページで、次の手順を実行します。
     a. をクリックします バックアップ処理だけが表示されるようにリストをフィルタリングします。
     b. 開始日と終了日を指定します。

c. [* タイプ] ドロップダウン・リストから、 **[*Backup]** を選択します。

d. [**Status**](ステータス *) ドロップダウンから、バックアップステータスを選択します。

e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。

4. バックアップジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

バックアップジョブのステータスがと表示されます で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

アクティビティペインで操作を監視します

[アクティビティ（ Activity ）] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity （アクティビティ）] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. をクリックします をクリックして、最近の 5 つの操作を表示します。

いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

Exchange データベースのバックアップ処理をキャンセルします

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの *
- 処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。
- バックアップ操作は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のバックアップ処理をキャンセルすることはできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、バックアップ処理をキャンセルできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っているバックアップ操作をキャンセルできます

- 手順 *

1. 次のいずれかを実行します。

方法	アクション
監視ページ	a. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 b. 操作を選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	a. バックアップ処理を開始したら、 * をクリックします* ［アクティビティ］ パネルには、最近の 5 つの操作が表示されます。 b. 処理を選択します。 c. ［ジョブの詳細］ ページで、 ［* ジョブのキャンセル *］ をクリックします。

処理がキャンセルされ、リソースが以前の状態に戻ります。

PowerShell コマンドレットを使用して Exchange バックアップを削除します

Remove-SmBackup コマンドレットを使用すると、他のデータ保護処理に Exchange バックアップが不要になった場合に Exchange バックアップを削除できます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

2. を使用して1つ以上のバックアップを削除します `Remove-SmBackup` コマンドレット。

   この例では、バックアップ ID を指定してバックアップを 2 つ削除しています。

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Topology ページで Exchange バックアップを表示します

リソースのバックアップを準備する際に、プライマリストレージとセカンダリストレージのすべてのバックアップの図を表示すると便利です。

- このタスクについて *

トポロジページでは、選択したリソースまたはリソースグループに使用できるすべてのバックアップを確認できます。これらのバックアップの詳細を確認し、対象を選択してデータ保護処理を実行できます。

[コピーの管理] ビューで次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップが使用可能かどうかを判断できます。

-  プライマリストレージにあるバックアップの数が表示されます。
-  には、 SnapMirror テクノロジを使用してセカンダリストレージにミラーリングされているバックアップの数が表示されます。
-  SnapVault テクノロジを使用してセカンダリストレージにレプリケートされたバックアップの数が表示されます。

  ◦ 表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。

  たとえば、 4 つのバックアップだけを保持するポリシーを使用して 6 つのバックアップを作成した場合、バックアップの数は 6 と表示されます。

* ベストプラクティス： * 正しい数のレプリケートされたバックアップが表示されるように、トポロジを更新することを推奨します。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、データベース、リソース、またはリソースグループを *View * ドロップダウン・リストから選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. 概要カードのセクションを参照して、プライマリストレージとセカンダリストレージで使用可能なバックアップ数の概要を確認します。

   Summary Card セクションには、バックアップの総数およびログ・バックアップの総数が表示されます。

「 * Refresh * 」ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

1. [コピーの管理] ビューで、 [プライマリストレージまたはセカンダリストレージからの * バックアップ *] をクリックして、バックアップの詳細を表示します。

   バックアップの詳細が表形式で表示されます。

2. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、名前変更、削除の各処理を実行します。

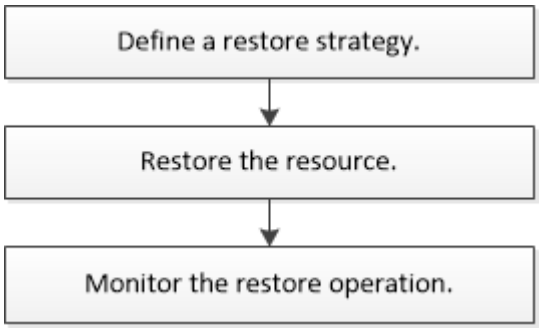
   セカンダリストレージ上のバックアップは、名前変更または削除できません。Snapshot コピーの削除は、 ONTAP の保持設定によって行います。

Exchange リソースをリストアします

リストアワークフロー

SnapCenter を使用して、 1 つ以上のバックアップをアクティブファイルシステムにリストアすることにより、 Exchange データベースをリストアできます。

次のワークフローは、 Exchange データベースのリストア処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップとリストアの処理を実行することもできます。PowerShell コマンドレットの詳細については、 SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

Exchange データベースをリストアするための要件

SnapCenter Plug-in for Microsoft Exchange Server のバックアップから Exchange Server データベースをリストアする前に、以下の要件を満たしていることを確認する必要があります。

復元機能を完全に使用するには、 SnapCenter Server と SnapCenter Plug-in for Exchange データベースの両方を 4.6 にアップグレードする必要があります。

- データベースをリストアするには、 Exchange Server がオンラインで稼働している必要があります。
- データベースが Exchange Server 上に存在している必要があります。

削除済みデータベースのリストアはサポートされていません。

- データベースの SnapCenter スケジュールを一時停止する必要があります。
- SnapCenter サーバおよび SnapCenter Plug-in for Microsoft Exchange Server ホストが、リストアするバックアップを含むプライマリストレージとセカンダリストレージに接続されている必要があります。

Exchange データベースをリストアします

SnapCenter を使用して、バックアップされた Exchange データベースをリストアできます。

- 必要なもの *
- リソースグループ、データベース、または Database Availability Group （ DAG ；データベース可用性グループ）をバックアップしておく必要があります。
- Exchange データベースを別の場所に移動した場合、古いバックアップのリストア処理は実行できません。
- Snapshot コピーをミラーまたはバックアップにレプリケートするユーザには、 SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に SVM を割り当てる必要があります。
- DAG では、ネットアップ以外のストレージにアクティブなデータベースコピーがあり、ネットアップストレージにあるデータベースのパッシブコピーバックアップからリストアする場合、パッシブコピー（ネットアップストレージ）をアクティブコピーとして作成し、リソースを更新してリストア処理を実行します。

  を実行します `Move-ActiveMailboxDatabase` データベースのパッシブコピーをアクティブコピーにするコマンドです。

  。 "Microsoft のドキュメント" に、このコマンドに関する情報を示します。

- このタスクについて *
- データベースに対してリストア処理を実行すると、データベースは同じホストにマウントされ、新しいボリュームは作成されません。
- DAG レベルのバックアップは、個々のデータベースからリストアする必要があります。
- Exchange データベース（ .edb ）ファイル以外のファイルが存在する場合は、フルディスクリストアはサポートされません。

  Plug-in for Exchange は、レプリケーションに使用されるなどの Exchange ファイルがディスクに格納されている場合、ディスク上でフルリストアを実行しません。フルリストアが Exchange の機能に影響を与える可能性がある場合、 Plug-in for Exchange は単一ファイルのリストア処理を実行します。

- Plug-in for Exchange では、 BitLocker 暗号化ドライブをリストアできません。

- scripts_pathは、プラグインホストのSMCoreServiceHost.exe.Configファイルにあ るPredefinedWindowsScriptsDirectoryキーを使用して定義されます。

  必要に応じて、このパスを変更し、SMcoreサービスを再起動できます。 セキュリティのためにデフォルトパスを使用することを推奨します。

  キーの値は、api/4.7/configsettingsを介してスワッガーから表示できます

  GET APIを使用してキーの値を表示することができます。set APIはサポートされません。

- 手順 *

1. 左側のナビゲーションペインで、リソースページの左上にある * リソース * をクリックします。
2. ドロップダウン・リストから Exchange Server プラグインを選択します。
3. [リソース] ページで、 [表示] リストから [* データベース *] を選択します。
4. リストからデータベースを選択します。
5. [コピーの管理] ビューで、 [プライマリ・バックアップ] テーブルから [* バックアップ] を選択し、[] をクリックします
6. [オプション] ページで、次のいずれかのログバックアップオプションを選択します。

オプション	説明
すべてのログバックアップ	フルバックアップ後に使用可能なすべてのログバックアップをリストアするには、「 * All log backups * 」を選択して最新の状態へのバックアップリストア処理を実行します。
までログバックアップでバックアップします	「 * までログバックアップ」を選択してポイントインタイムリストア処理を実行します。このリストア処理では、選択したログまでのログバックアップに基づいてデータベースがリストアされます。 ドロップダウンリストに表示されるログ数は UTM に基づいています。たとえば、フルバックアップ保持が 5 で UTM 保持が 3 の場合、使用可能なログバックアップの数は 5 ですが、ドロップダウンにはリストア処理を実行するログが 3 つしか表示されません。
期限までの特定の日付	リストアしたデータベースにトランザクション・ログを適用する日時を指定するには、 [指定の期限まで *] を選択します。このポイントインタイムリストア処理では、指定した日時の最後のバックアップまでに記録されたトランザクションログエントリがリストアされます。

オプション	説明
なし	ログ・バックアップを行わずにフル・バックアップのみをリストアする必要がある場合は、「 * なし」を選択します。

次のいずれかを実行できます。

- * リストア後にデータベースをリカバリしてマウント * - このオプションはデフォルトで選択されています。
- * リストア前にバックアップ内のトランザクション・ログの整合性を検証しない * - デフォルトでは、 SnapCenter はリストア処理を実行する前にバックアップ内のトランザクション・ログの整合性を検証します。

* ベストプラクティス： * このオプションは選択しないでください。

7. スクリプトページで、リストア処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

   リストアプリスクリプトの引数には、 $Database と $ServerInstance が含まれています。

   リストアポストスクリプトの引数には、 $Database 、 $ServerInstance 、 $BackupName 、 $LogDirectory 、および $TargetServerInstance があります。

   SNMP トラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathに対する相対パスでなければなりません。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。

2. 概要を確認し、 [完了] をクリックします。
3. リストア・ジョブのステータスを表示するには、ページ下部の ［ アクティビティ ］ パネルを展開します。

   リストア・プロセスを監視するには、 * Monitor * > * Jobs * ページを使用します。

アクティブデータベースをバックアップからリストアすると、レプリカとアクティブデータベースの間に遅延が発生した場合に、パッシブデータベースが中断状態または障害状態になることがあります。

状態の変更は、アクティブデータベースのログチェーンがフォークし、レプリケーションを中断する新しいブランチを開始すると発生します。Exchange Server はレプリカの修正を試みますが、修正できない場合は、リストア後に新しいバックアップを作成し、レプリカを再シードする必要があります。

メールとメールボックスのきめ細かいリカバリ

Single Mailbox Recovery （ SMBR ）ソフトウェアを使用すると、 Exchange データベース全体ではなく、メールやメールボックスのリストアとリカバリが可能です。

1 つのメールをリカバリするためだけにデータベース全体をリストアすると、時間とリソースが大量に消費されます。SMBR を使用すると、 Snapshot のクローンコピーを作成し、 Microsoft API を使用して SMBR 内のメールボックスをマウントすることで、メールを迅速にリカバリできます。
SMBR の使用方法については、を参照してください "『 SMBR アドミニストレーションガイド』"。

SMBRの追加情報については、次の資料を参照してください。

- "SMBRを使用して単一アイテムを手動でリストアする方法（Ontrack電源制御リストアにも適用可能）"
- "SnapCenter を使用して SMBR のセカンダリストレージからリストアする方法"
- "SMBR を使用した SnapVault からの Microsoft Exchange メールのリカバリ"

セカンダリストレージから **Exchange Server** データベースをリストアする

セカンダリストレージ（ミラーまたはバックアップ）から、バックアップされた Exchange Server データベースをリストアすることができます。

プライマリストレージからセカンダリストレージに Snapshot コピーをレプリケートしておく必要があります。

- 手順 *
  1. 左側のナビゲーションペインで、 [* リソース] をクリックし、リストから [Microsoft Exchange Server プラグイン *] を選択します。
  2. [リソース] ページで、 [*View] ドロップダウン・リストから [*Database] または [*Resource Group] を選択します。
  3. データベースまたはリソースグループを選択します。

     データベースまたはリソースグループのトポロジページが表示されます。
  4. [コピーの管理] セクションで、セカンダリ・ストレージ・システム（ミラーまたはバックアップ）から * バックアップ * を選択します。
  5. リストからバックアップを選択し、をクリックします  。
  6. [場所] ページで、選択したリソースを復元する宛先ボリュームを選択します。
  7. リストア・ウィザードを完了し ' 概要を確認してから '[* 終了 *] をクリックします

PowerShell コマンドレットを使用して **Exchange** リソースをリストアします

Exchange データベースをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

• 手順 *

1. を使用して、指定されたユーザのSnapCenter サーバとの接続セッションを開始します `Open-SmConnection` コマンドレット。

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

2. を使用して、リストアする1つ以上のバックアップに関する情報を取得します `Get-SmBackup` コマンドレット。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
PS C:\> Get-SmBackup

BackupId                        BackupName
BackupTime                      BackupType
--------                        ----------
----------                      ----------
341                             ResourceGroup_36304978_UTM... 12/8/2017
4:13:24 PM          Full Backup
342                             ResourceGroup_36304978_UTM... 12/8/2017
4:16:23 PM          Full Backup
355                             ResourceGroup_06140588_UTM... 12/8/2017
6:32:36 PM          Log Backup
356                             ResourceGroup_06140588_UTM... 12/8/2017
6:36:20 PM          Full Backup
```

3. を使用して、バックアップからデータをリストアします `Restore-SmBackup` コマンドレット。

   この例では、最新の状態へのバックアップをリストアしています。

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

   この例では、ポイントインタイムバックアップをリストアします。

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

   この例では、セカンダリストレージのバックアップをプライマリストレージにリストアします。

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BackupId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

。 `-archive` パラメータを使用すると、リストアに使用するプライマリボリュームとセカンダリボリュームを指定できます。

。 `-IsRecoverMount:$true` パラメータを使用すると、リストア後にデータベースをマウントできます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

Exchange のパッシブノードレプリカを再シードします

レプリカコピーを再シードする必要がある場合、たとえばコピーが破損した場合は、SnapCenter の再シード機能を使用して最新のバックアップに再シードできます。

- 必要なもの *
- SnapCenter サーバ 4.1 以降および Plug-in for Exchange 4.1 以降を使用している必要があります。

  レプリカの再シードは、 4.1 より前のバージョンの SnapCenter ではサポートされていません。

- 再シードするデータベースのバックアップを作成しておく必要があります。

* ベストプラクティス：ノード間の遅延を回避するために、再シード処理を実行する前に新しいバックアップを作成するか、最新のバックアップを実行しているホストを選択することを推奨します。

- 手順 *

1. 左側のナビゲーションペインで、 [* リソース] をクリックし、リストから [Microsoft Exchange Server プラグイン *] を選択します。
2. [リソース] ページで、 [表示] リストから適切なオプションを選択します。

オプション	説明
単一のデータベースを再シードする場合	[表示] リストから [*Database] を選択します。
DAG 内のデータベースを再シードする場合	ビューリストから * データベース可用性グループ * を選択します。

3. 再シードするリソースを選択します。
4. Manage Copies （コピーの管理）ページで、 * Reseed-* をクリックします。
5. 再シードウィザードで問題のあるデータベースコピーのリストから、再シードするデータベースコピ

ーを選択し、 * Next * をクリックします。

6. Host ウィンドウで、再シードするバックアップを含むホストを選択し、 * Next * をクリックします。
7. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。

8. 概要を確認し、 [完了] をクリックします。
9. ジョブのステータスを表示するには、ページの下部にある ［ アクティビティ ］ パネルを展開します。

   パッシブデータベースコピーがネットアップ以外のストレージにある場合は、再シード処理はサポートされません。

PowerShell コマンドレットを使用した Exchange データベースの再シード

PowerShell コマンドレットを使用すると、問題のあるレプリカをリストアできます。そのためには、同じホストの最新のコピーを使用するか、代替ホストの最新のコピーを使用します。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. を使用して、指定されたユーザのSnapCenter サーバとの接続セッションを開始します `Open-SmConnection` コマンドレット。

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. を使用してデータベースを再シードします `reseed-SmDagReplicaCopy` コマンドレット。

   この例では、ホスト「 mva-rx200.netapp.com" 」上の execdb という名前のデータベースの失敗したコピーを、そのホスト上の最新のバックアップを使用して再シードします。

   ```
   reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
   execdb
   ```

   この例では、代替ホスト「 mva-rx201.netapp.com." 」上のデータベースの最新バックアップ（本番 / コピー）を使用して、 execdb という名前のデータベースの失敗したコピーを再シードします

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

リストア処理を監視する

Jobs ページを使用して、 SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします リストをフィルタリングして、リストア処理のみを表示します。
   b. 開始日と終了日を指定します。
   c. [* タイプ **]** ドロップダウン・リストから、 **[** リストア *] を選択します。
   d. [* Status *] ドロップダウン・リストから、リストア・ステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

   View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

Exchange データベースのリストア処理をキャンセルします

キューに格納されているリストアジョブをキャンセルできます。

リストア処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて *
- キューに登録されたリストア処理は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、キューに登録されたリストア処理をキャンセルできます。
- キャンセルできないリストア処理の場合、 [ジョブのキャンセル] ボタンは使用できません。
- ロールの作成中に [ユーザー \ グループ] ページで [このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できる] を選択した場合は、そのロールを使用している間に、他のメンバーのキューに登録されているリストア操作をキャンセルできます。
- ステップ *

次のいずれかを実行します。

方法	アクション
監視ページ	1. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 2. ジョブを選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	1. リストア処理を開始したら、をクリックします をクリックして、最近の 5 つの操作を表示します。 2. 処理を選択します。 3. ［ ジョブの詳細 ］ ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

カスタムアプリケーションを保護

SnapCenter カスタムプラグイン

SnapCenter Custom Plug-ins の概要

使用するアプリケーション用のカスタムプラグインを開発し、 SnapCenter を使用してそれらのアプリケーションのバックアップ、リストア、クローニングを行うことができます。カスタムプラグインは、他の SnapCenter プラグインと同様に NetApp SnapCenter ソフトウェアのホスト側コンポーネントとして機能し、アプリケーションに対応したリソースのデータ保護と管理を実現します。

Custom Plug-ins をインストールすると、 SnapCenter と NetApp SnapMirror テクノロジを使用して別のボリュームのバックアップセットのミラーコピーを作成し、 NetApp SnapVault テクノロジを使用してディスクツーディスクのバックアップレプリケーションを実行できます。Custom Plug-ins は、 Windows と Linux のどちらの環境でも使用できます。

SnapCenter CLI では、 SnapCenter Custom Plug-ins コマンドはサポートされていません。

ネットアップは、 SnapCenter に組み込まれているカスタムプラグインフレームワークを使用して、 ONTAP ストレージ上でデータボリュームのデータ保護処理を実行するためのストレージプラグインを提供しています。

カスタムプラグインとストレージプラグインは、ホストの追加ページからインストールできます。

"ホストを追加し、プラグインパッケージをリモートホストにインストールする。"

ネットアップでは、 MySQL 、 MaxDB 、 DB2 、 Sybase 、 DPGLUE も提供しています。 MongoDB 、 ORASCPM 、 PostgreSQL のカスタムプラグイン。これらのプラグインは、からダウンロードできます "NetApp Storage Automation Store の略"。

SnapCenter のサポートポリシーでは、 SnapCenter カスタムプラグインフレームワーク、コアエンジン、および関連する API のサポートについて説明します。サポートは、プラグインのソースコードと、カスタムプラグインフレームワーク上に構築された関連スクリプトについては説明しません。

独自のカスタムプラグインは、を参照して作成できます "アプリケーション用のプラグインを開発します"。

SnapCenter Custom Plug-ins および Storage プラグインの機能

SnapCenter Custom Plug-ins を使用してデータ保護処理を実行できます。

- カスタムプラグイン *
- データベース、インスタンス、ドキュメント、表領域などのリソースを追加します。
- バックアップを作成します。
- バックアップからリストアします

- バックアップをクローニングする。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視する。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。
- ストレージプラグイン *

このプラグインは、データ保護処理に使用できます。

- 複数の ONTAP クラスタ間でストレージボリュームの整合グループ Snapshot コピーを作成する。
- 組み込みのプレ / ポストスクリプトフレームワークを使用してカスタムアプリケーションをバックアップします

  ONTAP ボリューム、 LUN 、または qtree をバックアップできます。

- SnapCenter ポリシーを使用して、プライマリで作成された Snapshot コピーを ONTAP セカンダリに対して更新し、既存のレプリケーション関係（ SnapVault/SnapMirror/ユニ ファイドレプリケーション）を利用します

  ONTAP のプライマリとセカンダリには、 ONTAP FAS 、 AFF 、 Select 、 Cloud ONTAP があります。

- ONTAP ボリューム、 LUN 、またはファイルの完全なリカバリ

  参照機能またはインデックス付け機能が製品に組み込まれていないため、それぞれのファイルパスを手動で指定する必要があります。

  qtree またはディレクトリのリストアはサポートされませんが、バックアップの範囲が qtree レベルで定義されている場合にのみ、 qtree のクローニングとエクスポートを実行できます。

SnapCenter Custom Plug-ins の特長

SnapCenter は、プラグインアプリケーションと統合されるほか、ストレージシステム上でネットアップのテクノロジと統合されます。Custom Plug-ins の操作には、SnapCenter のグラフィカルユーザインターフェイスを使用します。

- * 統一されたグラフィカル・ユーザー・インターフェイス *

  SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter のインターフェイスから、すべてのプラグインで、バックアップ、リストア、リカバリ、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（ RBAC ）を設定したり、ジョブを監視したりすることができます。

- * 中央管理の自動化 *

  バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenter から E メールアラートを送信するように設定して、環境をプロアクティブに監視することもできます。

- * 無停止の NetApp Snapshot コピー・テクノロジー *

SnapCenter では、 SnapCenter Custom Plug-ins でネットアップの Snapshot コピーテクノロジを使用してリソースがバックアップされます。Snapshot コピーはストレージスペースを最小限しか消費しません。

Custom Plug-ins 機能を使用すると、次のメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます

  また、許可された SnapCenter ユーザにアプリケーションレベルの権限を付与するようにクレデンシャルを設定することもできます。

- NetApp FlexClone テクノロジを使用して、スペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

  クローンを作成するストレージシステムに FlexClone ライセンスが必要です。

- バックアップの作成で ONTAP の整合グループ（ CG ）の Snapshot コピー機能がサポートされます。
- 複数のリソースホストで同時に複数のバックアップを実行できます

  1 回の処理で、 1 つのホストの複数のリソースが同じボリュームを共有する場合に複数の Snapshot コピーが統合されます。

- 外部コマンドを使用して Snapshot コピーを作成できます。
- Windows 環境でファイルシステムと整合性のある Snapshot コピーを作成できます。

SnapCenter Custom Plug-ins でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシンの両方でさまざまなストレージタイプをサポートしています。SnapCenter カスタムプラグインをインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージタイプ
VMホストへの物理およびNFSの直接マウント（VMDKおよびRDM LUNはサポートされません）。	FC 接続 LUN
VMホストへの物理およびNFSの直接マウント（VMDKおよびRDM LUNはサポートされません）。	iSCSI で接続された LUN
VMホストへの物理およびNFSの直接マウント（VMDKおよびRDM LUNはサポートされません）。	NFS-connected ボリューム

カスタムプラグインに必要な最小 ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
event generate-autosupport-log を指定します
ジョブ履歴の表示 ジョブが停止しました
lun attribute show lun create をクリックします lun delete LUN ジオメトリ LUN igroup add lun igroup create を追加します lun igroup delete LUN igroup の名前を変更します lun igroup show を参照してください LUN マッピングの追加 - レポートノード LUN マッピングが作成されます LUN マッピングが削除されます LUN マッピングの削除 - レポートノード lun mapping show lun modify を追加します LUN のボリューム内移動 LUN はオフラインです LUN はオンラインです LUN のサイズ変更 LUN シリアル lun show をクリックします
Network Interface の略

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SnapMirror ポリシー追加ルール snapmirror policy modify-rule snapmirror policy remove-rule 」を実行します snapmirror policy show の略 SnapMirror リストア snapmirror show の略 snapmirror show -history の略 SnapMirror の更新 SnapMirror の update-ls-set snapmirror list-destinations
バージョン

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
volume clone create を実行します
volume clone show を実行します
ボリュームクローンスプリット開始
ボリュームクローンスプリットは停止します
volume create を実行します
ボリュームを削除します
volume file clone create を実行します
volume file show-disk-usage
ボリュームはオフラインです
ボリュームはオンラインです
volume modify を使用します
volume qtree create を実行します
volume qtree delete
volume qtree modify の略
volume qtree show の略
ボリュームの制限
volume show のコマンドです
volume snapshot create を実行します
ボリューム Snapshot の削除
volume snapshot modify の実行
ボリューム Snapshot の名前が変更されます
ボリューム Snapshot リストア
ボリューム Snapshot の restore-file
volume snapshot show の実行
ボリュームのアンマウント

フルアクセスコマンド： **ONTAP 8.3.0** 以降で必要な最小権限
SVM CIFS です vserver cifs share create の場合 SVM CIFS 共有が削除されます vserver cifs shadowcopy show vserver cifs share show のコマンドです vserver cifs show のコマンドです vserver export-policy create を参照してください vserver export-policy delete vserver export-policy rule create vserver export-policy rule show vserver export-policy show のコマンドを入力します vserver iscsi connection show vserver show のコマンドです

読み取り専用コマンド： **ONTAP 8.3.0** 以降で必要な最小権限
Network Interface の略

カスタムプラグインの **SnapMirror** および **SnapVault** レプリケーション用のストレージシステムを準備する

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenter は、Snapshotコピー処理の完了後に、SnapMirrorとSnapVault に対する更新を実行します。SnapMirror更新とSnapVault 更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SnapCenter は * sync-mirror * レプリケーションをサポートしていません。

バックアップ戦略を定義する

バックアップジョブを作成する前にバックアップ戦略を定義しておくと、リソースの正常なリストアやクローニングに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービスレベルアグリーメント（ SLA ）、目標復旧時間（ RTO ）、および目標復旧時点（ RPO ）によって決まります。

- このタスクについて *

SLA では、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処するために必要なサービスレベルを定義します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA 、 RTO 、および RPO は、データ保護戦略に関与します。

- 手順 *

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. 整合グループ Snapshot コピーを保持するかどうかを決定し、保持する場合は整合グループ Snapshot コピーを削除する適切なオプションを決定します。
5. レプリケーションのために NetApp SnapMirror テクノロジを使用するか、または長期保持のために NetApp SnapVault テクノロジを使用するかを決定します。
6. ソーシャルストレージシステムおよび SnapMirror デスティネーションでの Snapshot コピーの保持期間を確認します。
7. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

カスタムプラグインのバックアップ戦略

カスタムプラグインリソースのバックアップスケジュール

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。リソースをバックアップする回数が多いほど、リストア時に SnapCenter で使用する必要のあるアーカイブログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

SLA は、サービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA と RPO はデータ保護戦略に関与します。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度

  バックアップ頻度（バックアップを実行する間隔）は、ポリシー設定の一部であり、一部のプラグインではスケジュールタイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。SnapCenter GUI でポリシーにアクセスするには、 * Settings * > * Policies * をクリックします。

- バックアップスケジュール

  バックアップスケジュール（バックアップが実行される日時）は、リソースまたはリソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できますSnapCenter GUI でリソースグループのスケジュールにアクセスするには、 [* リソース] をクリックし、適切なプラグインを選択して、 [* 表示 **>]** 、 **[** リソースグループ *] の順にクリックします。

必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービスレベルアグリーメント（ SLA ）などがあります。

通常、選択するバックアップジョブの数は、リソースが配置されているボリュームの数によって異なります。たとえば、あるボリュームに小規模なリソースのグループを配置しており、別のボリュームに 1 つの大規模なリソースを配置している場合は、小規模なリソース用のバックアップジョブと大規模なリソース用のバックアップジョブを 1 つずつ作成できます。

カスタムプラグインリソースを手動で追加する場合にサポートされるリストア戦略のタイプ

SnapCenter を使用してリストア処理を正常に実行するには、事前に戦略を定義しておく必要があります。カスタムプラグインリソースを手動で追加する場合のリストア戦略には、 2 種類あります。

手動で追加したカスタムプラグインリソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、 qtree 、および LUN をリストアします

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

ファイルレベルのリストア

- ボリューム、 qtree 、またはディレクトリからファイルをリストアします
- 選択した LUN のみをリストアします

アプリケーション用のプラグインを開発します

概要

SnapCenter サーバを使用すると、 SnapCenter へのプラグインとしてアプリケーションを導入および管理できます。
任意のアプリケーションをSnapCenterサーバに接続して、データを保護できます
管理機能：

SnapCenter では、さまざまなプログラミング言語を使用してカスタムプラグインを開発できます。可能です Perl、Java、バッチ、またはその他のスクリプト言語を使用してカスタムプラグインを開発します。

SnapCenter でカスタムプラグインを使用するには、次のタスクを実行する必要があります。

- このガイドの手順に従って、使用するアプリケーション用のプラグインを作成します
- 概要ファイルを作成します
- カスタムプラグインをエクスポートして SnapCenter ホストにインストールする
- プラグインの zip ファイルを SnapCenter サーバにアップロードします

すべての **API** 呼び出しでの汎用プラグインの処理

すべての API 呼び出しについて、次の情報を使用します。

- プラグインパラメータ
- 終了コード
- エラーメッセージを記録します
- データの整合性

一連のパラメータは、作成されたすべての API 呼び出しの一環としてプラグインに渡されます。次の表に、パラメータの具体的な情報を示します。

パラメータ	目的
アクション	ワークフロー名を指定します。たとえば、discover 、backup、fileOrVolRestore、などです cloneVolAndLunの略
リソース	保護対象のリソースが表示されます。リソースは UID とタイプで識別されます。次の形式でプラグインに表示されます。 「 <UID> 、 <type>; <UID> 、 <type> 」のように入力します。例： インスタンス1、インスタンス、インスタンス 2\\DB1、データベース
APP_NAME を使用している	使用するプラグインを指定します。たとえば、 db2 、 mysql のように指定します。SnapCenter サーバには、リストされているアプリケーションに対するサポートが組み込まれています。このパラメータでは大文字と小文字が区別されます。
APP_IGNORE_ERROR	（ Y または N ）これにより、アプリケーションエラーが発生した場合、 SnapCenter が終了するか、終了しません。これは、複数のデータベースをバックアップし、単一の障害が発生しないようにする場合に便利です バックアップ処理を停止します。
<resource_name> ____APP_INSTANY_USERNAME	SnapCenter クレデンシャルは、リソースに対して設定されます。
<resource_name> _APP_INSTANY_PASSWORD	SnapCenter クレデンシャルは、リソースに対して設定されます。
<resource_name> _<custom_param> です	各リソースレベルのカスタムキー値はです プレフィックスが付いたプラグインで使用できます 「<RESOURCE_NAME>_」を参照してください。たとえば、を指定します カスタムキーは、リソースの「MASTER_SLAVE」です 「MySQLDB」という名前の場合は、として使用できます MySQLDB_MASTER_SLAVE

終了コードを使用します

プラグインは、終了コードを使用して処理のステータスをホストに戻します。各
コードには特定の意味があり、プラグインは正しい終了コードを使用して同じことを示します。

次の表に、エラーコードとその意味を示します。

終了コード	目的
0	処理に成功しました。
99ドル	要求された処理はサポートされていないか実装されて
100です	処理に失敗しました。休止解除をスキップして終了します。デフォルトでは休止解除が実行されます。
101です	処理に失敗しました。バックアップ処理を続行してください。
その他	処理に失敗しました。休止解除を実行して終了します。

エラーメッセージを記録します

エラーメッセージは、プラグインから SnapCenter サーバーに渡されます。メッセージです
メッセージ、ログレベル、およびタイムスタンプが含まれます。

次の表に、レベルとその目的を示します。

パラメータ	目的
情報	情報メッセージ
警告	警告メッセージ
エラー	エラーメッセージです
デバッグ	デバッグメッセージ
トレース	メッセージをトレースします

データの整合性を維持

カスタムプラグインでは、同じワークフローの実行操作間でデータが保持されます。の場合
たとえば、休止の終了時にプラグインにデータを格納し、休止解除時にこのデータを使用できます
操作。

保持するデータはプラグインによって Result オブジェクトの一部として設定されます。それが特定のフォーマットに従います
とについては、プラグイン開発の各スタイルで詳しく説明しています。

Perl ベースの開発

Perl を使用してプラグインを開発するには、特定の規則に従う必要があります。

- 内容は読み取り可能である必要があります
- setenv 、 quiesce 、および unquiesce の必須処理を実装する必要があります
- 結果をエージェントに戻すには、特定の構文を使用する必要があります
- 内容は <plugin_name>.pm ファイルとして保存してください

使用可能な処理はです

- setenv
- バージョン
- 休止
- 休止解除
- clone_pre 、 clone_post
- restore_pre 、 restore を実行します
- クリーンアップ

一般的なプラグイン処理

結果オブジェクトを使用する

カスタムプラグイン処理では、必ず結果オブジェクトを定義する必要があります。このオブジェクトは、メッセージ、終了コード、 stdout 、 stderr をホストエージェントに送信します。

結果オブジェクト：

```
my $result = {
```

```
      exit_code => 0,
      stdout => "",
      stderr => "",
};
```

結果オブジェクトを返します。

```
return $result;
```

同じワークフローの実行の一部として、処理間でデータを保持（クリーンアップを除く）できます。この設定には、キーと値のペアを使用します。キーと値のデータペアは結果オブジェクトの一部として設定され、保持され、同じワークフローの後続の操作で使用できます。

次のコードサンプルは、保持するデータを設定します。

```
my $result = {
  exit_code => 0,
  stdout => "",
  stderr => "",
};
  $result->{env}->{'key1'} = 'value1';
  $result->{env}->{'key2'} = 'value2';
  ….
  return $result
```

上記のコードでは、 2 つのキーと値のペアを設定します。これらのペアは、後続の操作で入力として使用できます。2 つのキーと値のペアには、次のコードを使用してアクセスできます。

```
sub setENV {
    my ($self, $config) = @_;
    my $first_value = $config->{'key1'};
    my $second_value = $config->{'key2'};
    …
}
```

```
 === Logging error messages
```

各処理では、メッセージをホストエージェントに送信して戻すことができます。エージェントは、コンテンツを表示して保存します。メッセージには、メッセージレベル、タイムスタンプ、およびメッセージテキストが含まれます。複数行のメッセージがサポートされます。

```
Load the SnapCreator::Event Class:
my $msgObj = new SnapCreator::Event();
my @message_a = ();
```

msgObj を使用して、 Collect メソッドを使用してメッセージをキャプチャします。

```
$msgObj->collect(\@message_a, INFO, "My INFO Message");
$msgObj->collect(\@message_a, WARN, "My WARN Message");
$msgObj->collect(\@message_a, ERROR, "My ERROR Message");
$msgObj->collect(\@message_a, DEBUG, "My DEBUG Message");
$msgObj->collect(\@message_a, TRACE, "My TRACE Message");
```

結果オブジェクトにメッセージを適用します。

```
$result->{message} = \@message_a;
```

プラグインスタブを使用する

カスタムプラグインでは、プラグインのスタブを公開する必要があります。これらは、 SnapCenter サーバがワークフローに基づいて呼び出すメソッドです。

プラグインスタブ	オプション / 必須	目的
setenv	必須	このスタブは、環境と構成オブジェクトを設定します。 ここでは、環境の解析または処理を行う必要があります。スタブが呼び出されるたびに、 setenv スタブが直前に呼び出されます。これは Perl 形式のプラグインの場合にのみ必要です。
バージョン	任意。	このスタブは、アプリケーションのバージョンを取得するために使用されます。

プラグインスタブ	オプション / 必須	目的
調査	任意。	このスタブは、エージェントまたはホストでホストされているインスタンスまたはデータベースなどのアプリケーションオブジェクトを検出するために使用されます。 このプラグインは、検出されたアプリケーションオブジェクトを応答の一部として特定の形式で返す必要があります。このスタブは、アプリケーションが SnapDrive for Unix に統合されている場合にのみ使用されます。 Linux ファイルシステム（ Linux フレーバ）がサポートされています。AIX/Solaris （ UNIX 版）はサポートされていません。
Discovery_complete の手順を実行します	任意。	このスタブは、エージェントまたはホストでホストされているインスタンスまたはデータベースなどのアプリケーションオブジェクトを検出するために使用されます。 このプラグインは、検出されたアプリケーションオブジェクトを応答の一部として特定の形式で返す必要があります。このスタブは、アプリケーションが SnapDrive for Unix に統合されている場合にのみ使用されます。 Linux ファイルシステム（ Linux フレーバ）がサポートされています。AIX および Solaris （ UNIX 版）はサポートされていません。

プラグインスタブ	オプション / 必須	目的
休止	必須	このスタブは、アプリケーションを Snapshot コピーの作成が可能な状態にする休止を実行します。これは、 Snapshot コピー処理の前に呼び出されます。保持するアプリケーションのメタデータは応答の一部として設定する必要があります。これは、対応するストレージ Snapshot コピーの以降のクローニング処理またはリストア処理中に、構成パラメータの形式で返されます。
休止解除	必須	このスタブは、アプリケーションを通常の状態に戻すことを意味し、休止解除を実行します。この呼び出しは、 Snapshot コピーの作成後に行われます。
clone_pre	任意。	このスタブは、クローニング前タスクを実行する役割を果たします。このパラメータは、組み込みの SnapCenter サーバクローニングインターフェイスを使用していることを前提としており、クローニング処理の実行時にトリガーされます。
clone_post をクリックしてください	任意。	この STUB は、クローニング後のタスクの実行を担当します。このパラメータは、組み込みの SnapCenter サーバクローニングインターフェイスを使用していることを前提としており、クローニング処理の実行時にのみトリガーされます。
restore_pre	任意。	このスタブは、リストア前のタスクの実行を担当します。これは、組み込みの SnapCenter Server リストアインターフェイスを使用しており、リストア処理中にトリガされることを前提としています。

プラグインスタブ	オプション / 必須	目的
リストア	任意。	このスタブは、アプリケーションのリストアタスクを実行する役割を果たします。この要件は、組み込みの SnapCenter Server リストアインターフェイスを使用していることを前提としており、リストア処理の実行時にのみトリガーされます。
クリーンアップ	任意。	この STUB は、バックアップ、リストア、またはクローン処理後にクリーンアップを実行する場合の説明です。クリーンアップは、通常のワークフローの実行中またはワークフローの失敗時に実行できます。このワークフロー名では、バックアップ、 cloneVolAndLun 、または fileOrVolRestore などの設定パラメータアクションを参照して、クリーンアップを呼び出すことができます。設定パラメータ ERROR_MESSAGE は ' ワークフローの実行中にエラーが発生したかどうかを示しますERROR_MESSAGE が定義されていて NULL ではない場合 ' ワークフロー失敗の実行中にクリーンアップが呼び出されます
APP_VERSION	任意。	このスタブは、SnapCenterがアプリケーションを取得するために使用します プラグインで管理されるバージョンの詳細。

プラグインパッケージの情報

すべてのプラグインについて、次の情報が必要です。

```
package MOCK;
our @ISA = qw(SnapCreator::Mod);
=head1 NAME
MOCK - class which represents a MOCK module.
=cut
=head1 DESCRIPTION
MOCK implements methods which only log requests.
=cut
use strict;
use warnings;
use diagnostics;
use SnapCreator::Util::Generic qw ( trim isEmpty );
use SnapCreator::Util::OS qw ( isWindows isUnix getUid
createTmpFile );
use SnapCreator::Event qw ( INFO ERROR WARN DEBUG COMMENT ASUP
CMD DUMP );
my $msgObj = new SnapCreator::Event();
my %config_h = ();
```

処理

ブート時、バージョン、休止、休止解除など、カスタムプラグインでサポートされるさまざまな処理をコード化できます。

setENV 動作

Perl を使用して作成されたプラグインに対して、 setENV 操作が必要です。ENV を設定すると、プラグインパラメータに簡単にアクセスできます。

```
sub setENV {
    my ($self, $obj) = @_;
    %config_h = %{$obj};
    my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
    };
    return $result;
}
```

バージョン処理

バージョン処理は、アプリケーションのバージョン情報を返します。

```
sub version {
  my $version_result = {
    major => 1,
    minor => 2,
    patch => 1,
    build => 0
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $version_result->{message} = \@message_a;
  return $version_result;
}
```

休止処理

休止処理を実行すると、 resources パラメータにリストされているリソースに対してアプリケーション休止処理が実行されます。

```
sub quiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

休止解除処理

アプリケーションの休止解除には休止解除処理が必要です。リソースのリストは、 resources パラメータで指定できます。

```
sub unquiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::unquiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

ネイティブ形式

SnapCenter では、 Perl 以外のプログラミング言語やスクリプト言語を使用してプラグインを作成できます。これは、スクリプトまたはバッチファイルとして使用できるネイティブスタイルプログラミングと呼ばれます。

ネイティブ形式のプラグインは、次に示す特定の表記規則に従う必要があります。

プラグインが実行可能である必要があります

- UNIX システムの場合、エージェントを実行するユーザにはプラグインに対する実行権限が必要です
- Windowsシステムの場合、PowerShellプラグインにはサフィックス.ps1、その他のWindowsが必要です スクリプトは、.cmdまたは.batサフィックスを持ち、ユーザが実行可能である必要があります
- プラグインは、「 -quiesce 」、「 -unquiesce 」などのコマンドライン引数に対応する必要があります。
- 操作または関数が実装されていない場合、プラグインは終了コード 99 を返す必要があります
- プラグインは、特定の構文を使用して結果をサーバに渡す必要があります

一般的なプラグイン処理

エラーメッセージのロギング

各オペレーションは ' サーバにメッセージを送信することができますサーバは ' コンテンツを表示して保存しますメッセージには、メッセージレベル、タイムスタンプ、およびメッセージテキストが含まれます。複数行のメッセージがサポートされます。

の形式で入力し

```
SC_MSG#<level>#<timestamp>#<message>
SC_MESSAGE#<level>#<timestamp>#<message>
```

SnapCenter プラグインはプラグインスタブを実装する必要があります。SnapCenter サーバが呼び出すメソッドは、特定のワークフローに基づいています。

プラグインスタブ	オプション / 必須	目的
休止	必須	このスタブは休止を実行します。が配置されます Snapshotコピーを作成できる状態に適用します。これは、ストレージ Snapshot コピー処理の前に呼び出されます。
休止解除	必須	休止解除を実行する場合は、このスタブを指定します。配置されます 通常の状態のアプリケーション。これは保管後に呼び出されます Snapshotコピー処理
clone_pre	任意。	このスタブは、クローニング前のタスクを実行する役割を果たします。この場合、組み込みの SnapCenter クローニングインターフェイスを使用しており、「 clone_vol または clone_lun 」操作の実行時にのみトリガーされることを前提としています。
clone_post をクリックしてください	任意。	この STUB は、クローニング後のタスクの実行を担当します。このパラメータは、組み込みの SnapCenter クローニングインターフェイスを使用していること、および「 clone_vol 」または「 clone_lun 」処理を実行するときにのみトリガーされることを前提としています。
restore_pre	任意。	このスタブはリストア前のタスクを実行するためのものです。この処理は、組み込みの SnapCenter リストアインターフェイスを使用していることを前提としており、リストア処理の実行中にのみ実行されます。

プラグインスタブ	オプション / 必須	目的
リストア	任意。	このスタブは、すべてのリストアアクションを実行するためのものです。これ 組み込みのリストアインターフェイスを使用していないことを前提としています。このコマンドはリストア処理の実行中にトリガーされます。

例

Windows PowerShell の場合

スクリプトをシステムで実行できるかどうかを確認します。スクリプトを実行できない場合は、スクリプトに対して Set-ExecutionPolicy bypass を設定して、操作を再試行します。

```
if ($args.length -ne 1) {
  write-warning "You must specify a method";
  break;
}
function log ($level, $message) {
  $d = get-date
  echo "SC_MSG#$level#$d#$message"
}
function quiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Quiescing application using script $app_name";
  log "INFO" "Quiescing application finished successfully"
}
function unquiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Unquiescing application using script $app_name";
  log "INFO" "Unquiescing application finished successfully"
}
  switch ($args[0]) {
    "-quiesce" {
    quiesce;
}
"-unquiesce" {
    unquiesce;
}
default {
    write-error "Function $args[0] is not implemented";
    exit 99;
  }
}
exit 0;
```

Java スタイル

Java カスタムプラグインは、データベースやインスタンスなどのアプリケーションと直接対話します。

制限

Java プログラミング言語を使用してプラグインを開発する場合は、一定の制限事項に注意する必要があります。

プラグインの特性	Java プラグイン
複雑さ	低 ~ 中

プラグインの特性	**Java** プラグイン
メモリフットプリント	最大 10 ～ 20 MB
他のライブラリとの依存関係	アプリケーション通信用ライブラリ
スレッド数	1.
スレッドランタイム	1 時間未満

Java の制限の理由

SnapCenter エージェントの目標は、継続的、安全、堅牢なアプリケーション統合を実現することです。Java プラグインをサポートすることで、プラグインがメモリリークなどの不要な問題をもたらす可能性があります。これらの課題に取り組むことは困難です。特に、使いやすいものを維持することが目的である場合には困難です。プラグインの複雑さがそれほど複雑でない場合は、開発者がエラーを発生させてしまう可能性ははるかに低くなります。Javaプラグインの危険性は、プラグインがあることです
SnapCenterエージェント自体と同じJVM内で実行されています。プラグインがクラッシュしたりメモリがリークしたりすると、 Agent に悪影響を与える可能性もあります。

サポートされている方法

メソッド	必須	説明	いつ、誰が電話をかけましたか？
バージョン	はい。	プラグインのバージョンを返す必要があります。	のバージョンを要求するSnapCenterサーバまたはエージェント プラグイン。
休止	はい。	アプリケーションで休止を実行する必要があります。ほとんどの場合、この状態になると、SnapCenter サーバでバックアップ（ Snapshot コピーなど）を作成できるようになります。	SnapCenterサーバがSnapshotコピーまたはを作成する前に 一般的なバックアップを実行します。
休止解除	はい。	アプリケーションに対して休止解除を実行する必要があります。ほとんどの場合、これ アプリケーションを通常の動作状態に戻すことを意味します。	SnapCenterサーバがSnapshotコピーまたはを作成したあと 一般的にバックアップを実行しました。

メソッド	必須	説明	いつ、誰が電話をかけましたか？
クリーンアップ	いいえ	プラグインがクリーンアップする必要があるすべての項目をクリーンアップする責任があります。	SnapCenter サーバでワークフローが完了したとき（正常終了したとき、または障害が発生したとき）。
clonePre-	いいえ	クローニング処理を実行する前に、必要な処理を実行する必要があります。	ユーザが「 cloneVol 」または「 cloneLun 」アクションをトリガーし、組み込みのクローニングウィザード（ GUI / CLI ）を使用する場合。
clonePost を実行します	いいえ	クローニング処理の実行後に必要な処理を実行する必要があります。	ユーザが「 cloneVol 」または「 cloneLun 」アクションをトリガーし、組み込みのクローニングウィザード（ GUI / CLI ）を使用する場合。
restorePre	いいえ	は、リストア処理が呼び出される前に実行する必要がある操作を実行します。	ユーザがリストア処理をトリガーした場合。
リストア	いいえ	アプリケーションのリストア / リカバリを実行します。	ユーザがリストア処理をトリガーした場合。
AppVersion （アプリバージョン）	いいえ	プラグインによって管理されているアプリケーションバージョンを取得する。	バックアップ / リストア / クローンなど、すべてのワークフローで ASUP データ収集の一部として実行

チュートリアル

このセクションでは、 Java プログラミング言語を使用してカスタムプラグインを作成する方法について説明します。

Eclipse のセットアップ

1. Eclipse で新しい Java プロジェクト「 TutorialPlugin 」を作成します
2. [完了] をクリックします。
3. 新しいプロジェクト * → * プロパティ * → * Java ビルドパス * → * ライブラリ * → * 外部 JAR の追加 * を右クリックします

4. ホスト・エージェントの ./lib/folder に移動し 'jar scAgent-5.0-core.jar と common-5.0.jar を選択します
5. プロジェクトを選択し、 * src フォルダー * → * New * → * Package * を右クリックして、 com.netapp.snapcreator.agent.plugin.TutorialPlugin という名前で新しいパッケージを作成します
6. 新しいパッケージを右クリックし ' 新規作成 > Java クラスを選択します
   a. TutorialPlugin という名前を入力してください。
   b. スーパークラスの参照ボタンをクリックし、「 * AbstractPlugin 」を検索します。表示される結果は 1 つだけです。

```
 "AbstractPlugin - com.netapp.snapcreator.agent.nextgen.plugin".
.. [ 完了 ] をクリックします。
.. Java クラス :
```

```
package com.netapp.snapcreator.agent.plugin.TutorialPlugin;
import
com.netapp.snapcreator.agent.nextgen.common.result.Describe
Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.VersionR
esult;
import
com.netapp.snapcreator.agent.nextgen.context.Context;
import
com.netapp.snapcreator.agent.nextgen.plugin.AbstractPlugin;
public class TutorialPlugin extends AbstractPlugin {
  @Override
  public DescribeResult describe(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result quiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result unquiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public VersionResult version() {
    // TODO Auto-generated method stub
    return null;
  }
}
```

必要なメソッドを実装する

カスタム Java プラグインを実装するには、休止、休止解除、およびバージョンの各必須メソッドが必要です。

以下は、プラグインのバージョンを返すバージョンメソッドです。

```
@Override
public VersionResult version() {
    VersionResult versionResult = VersionResult.builder()
                                                .withMajor(1)
                                                .withMinor(0)
                                                .withPatch(0)
                                                .withBuild(0)
                                                .build();
    return versionResult;
}
```

```
Below is the implementation of quiesce and unquiesce method. These will be
interacting with   the application, which is being protected by SnapCenter
Server. As this is just a tutorial, the
application part is not explained, and the focus is more on the
functionality that SnapCenter   Agent provides the following to the plug-
in developers:
```

```
@Override
  public Result quiesce(Context context) {
    final Logger logger = context.getLogger();
    /*
      * TODO: Add application interaction here
    */
```

```
logger.error("Something bad happened.");
logger.info("Successfully handled application");
```

```
    Result result = Result.builder()
                    .withExitCode(0)
                    .withMessages(logger.getMessages())
                    .build();
    return result;
}
```

メソッドは Context オブジェクトで渡されます。これには、ロガーとコンテキストストアなどの複数のヘルパーと、現在の操作に関する情報（ワークフロー ID 、ジョブ ID ）が含まれます。ロガーは、最終ロガーロガー = context.getLogger(); を呼び出すことで取得できます。logger オブジェクトは、 logback などの他のロギングフレームワークで知られている同様のメソッドを提供します。結果オブジェクトでは、終了コードを指定することもできます。この例では、問題が存在しないため 0 が返されます。その他の終了コードは、さまざまな障害シナリオに対応する場合があります。

result オブジェクトには、次のパラメータが含まれます。

パラメータ	デフォルト	説明
構成	空です 構成	このパラメータを使用すると、設定パラメータをサーバに返送できます。それは には、プラグインで更新するパラメータを指定できます。この変化がそうであるかどうか SnapCenterサーバの設定に実際に反映されるのは、に依存します CONFIG のAPP_CONF_PERSISTENCY = YまたはNパラメータ。
イキシコード	0	処理のステータスを示します。「0」は、操作が行われたことを示します が実行されました。その他の値は、エラーまたは警告を示します。
標準出力	空です リスト	これは、stdoutメッセージをSnapCenterに送信するために使用できます サーバ：
stderr	空です リスト	これは、stderrメッセージをSnapCenterに送信するために使用できます サーバ：
メッセージ	空です リスト	このリストには、プラグインがに返すすべてのメッセージが含まれています サーバこれらのメッセージは、SnapCenter サーバの CLI または GUI に表示されます。

SnapCenter エージェントはビルダーを提供します ("ビルダパターン")すべてのために
結果タイプ。これにより、これらの機能を非常に簡単に使用できます。

```
Result result = Result.builder()
                      .withExitCode(0)
                      .withStdout(stdout)
                      .withStderr(stderr)
                      .withConfig(config)
                      .withMessages(logger.getMessages())
                      .build()
```

たとえば、終了コードを 0 に設定し、 stdout と stderr のリストを設定し、 config パラメータを設定して、サーバに送信されるログメッセージを追加します。すべてのパラメータが不要な場合は、必要なパラメータのみを送信します。各パラメータにはデフォルト値が設定されているため、以下のコードから .withExitCode(0) を削除しても、結果は影響を受けません。

```
Result result = Result.builder()
                       .withExitCode(0)
                       .withMessages(logger.getMessages())
                       .build();
```

VersionResult

VersionResult は、 SnapCenter サーバにプラグインのバージョンを通知します。それはまた継承します
結果から、config、exitCode、stdout、stderr、およびmessagesパラメータが含まれます。

パラメータ	デフォルト	説明
メジャー（ Major ）	0	プラグインのメジャーバージョンフィールド。
マイナー	0	プラグインのマイナーバージョンフィールド。
パッチ	0	プラグインの PATCH version フィールド。
構築	0	プラグインのビルドバージョンフィールド。

例：

```
VersionResult result = VersionResult.builder()
                                    .withMajor(1)
                                    .withMinor(0)
                                    .withPatch(0)
                                    .withBuild(0)
                                    .build();
```

コンテキストオブジェクトの使用

コンテキストオブジェクトには、次のメソッドがあります。

コンテキストメソッド	目的
文字列 getWorkflowId();	にSnapCenterサーバで使用されているワークフローIDを返します 現在のワークフロー。
Config GetConfig （） ；	SnapCenterサーバからに送信中の設定を返します 捜査官

ワークフロー **ID**

ワークフローIDは、SnapCenterサーバが特定の実行を参照するために使用するIDです
ワークフロー：

構成

このオブジェクトには、の設定でユーザが設定できるパラメータのほとんどが含まれています
SnapCenterサーバ。ただし、セキュリティ上の理由により、これらのパラメータの一部が取得される可能性があります
サーバー側でフィルタリングされます。次に、Config and Retrieveにアクセスする例を示します
パラメータ：

```
final Config config = context.getConfig();
String myParameter =
config.getParameter("PLUGIN_MANDATORY_PARAMETER");
```

"//MyParameter"には、SnapCenterサーバの設定から読み取ったパラメータが含まれるようになりました
設定パラメータキーが存在しない場合は、空の文字列("")を返します。

プラグインのエクスポート

SnapCenter ホストにインストールするには、プラグインをエクスポートする必要があります。

Eclipse では、次のタスクを実行します。

1. プラグインの基本パッケージを右クリックします(この例では

com.netapp.snapcreator.agent.plugin.TutorialPluginを参照）。

2. 「 * Export * → * Java * → * JAR File * 」を選択します
3. 「 * 次へ * 」をクリックします。
4. 次のウィンドウで、jarファイルの保存先パスtutorial_plugin.jarを指定します
   プラグインの基本クラスはTutorialPlugin.classという名前で、プラグインをフォルダに追加する必要があります
   同じ名前で

プラグインが追加のライブラリに依存している場合は、 lib/ というフォルダを作成できます

jar ファイルを追加できます。このプラグインは従属ファイルに依存します（たとえば、データベース・ドライバ）。いつ
SnapCenterはプラグインをロードし、このフォルダ内のすべてのjarファイルをとに自動的に関連付けます
クラスパスに追加します。

SnapCenter のカスタムプラグイン

SnapCenter のカスタムプラグイン

Java 、 Perl 、またはネイティブ形式を使用して作成したカスタムプラグインを、 SnapCenter サーバを使用してホストにインストールし、アプリケーションのデータを保護することができます。このチュートリアルで提供されている手順を使用して SnapCenter ホストにインストールするには、プラグインをエクスポートしておく必要があります。

プラグイン概要ファイルを作成しています

プラグインを作成するたびに、概要ファイルが必要になります。概要ファイルには、プラグインの詳細が記述されています。ファイルの名前は、プラグイン記述子 .xml である必要があります。

プラグイン記述子ファイルの属性とその重要度を使用する

属性	説明
名前	プラグインの名前。英数字を使用できます。たとえば、 DB2 、 MySQL 、 MongoDB などです ネイティブ形式で作成したプラグインの場合は、ファイルの拡張子を指定しないでください。たとえば、プラグインの名前が MongoDB である場合は、MongoDB という名前を指定します。
バージョン	プラグインのバージョン。メジャーバージョンとマイナーバージョンの両方を含めることができます。たとえば、 1.0 、 1.1 、 2.0 、 2.1 のようになります
表示名	SnapCenterサーバーに表示するプラグイン名。同じプラグインの複数のバージョンが書き込まれている場合は、表示名がすべてのバージョンで同じであることを確認してください。

属性	説明
プラグインタイプ（ PluginType ）	プラグインの作成に使用する言語。サポートされている値は Perl 、 Java 、および Native です。 標準のプラグインタイプには、 Unix/Linux シェルスクリプト、 Windows スクリプト、 Python 、またはその他のスクリプト言語が含まれています。
osname のように指定し	プラグインがインストールされているホスト OS の名前。有効な値はWindowsとです Linux：1 つのプラグインを、 Perl タイププラグインなど、複数の OS タイプに導入できます。
osVersion をクリックします	プラグインがインストールされているホスト OS のバージョン。
ResourceName の略	プラグインでサポート可能なリソースタイプの名前。例：database、instance、 コレクション。
親（ Parent ）	ResourceNameが別のリソースタイプに階層的に依存している場合は 親(Parent)-親リソースタイプを決定します たとえば、 DB2 プラグインの場合、 ResourceName 「 Database 」には親の「 Instance 」があります。
FileSystemPlugin が必要です	はいまたはいいえリカバリタブがであるかどうかを指定します リストアウィザードに表示されます。
ResourceRequiresAuthentication の略	はいまたはいいえリソースが自動検出されたかどうかを指定します 自動検出のあとにデータ保護処理を実行するにはクレデンシャルが必要です ストレージを検出しています。
FileSystemClone が必要です	はいまたはいいえプラグインでクローン用にファイルシステムプラグインの統合が必要かどうかを指定します ワークフロー：

カスタムプラグイン DB2 の Plugin_descriptor.xml ファイルの例は次のとおりです。

```
<Plugin>
<SMSServer></SMSServer>
<Name>DB2</Name>
<Version>1.0</Version>
<PluginType>Perl</PluginType>
<DisplayName>Custom DB2 Plugin</DisplayName>
<SupportedOS>
<OS>
<OSName>windows</OSName>
<OSVersion>2012</OSVersion>
</OS>
<OS>
<OSName>Linux</OSName>
<OSVersion>7</OSVersion>
</OS>
</SupportedOS>
<ResourceTypes>
<ResourceType>
<ResourceName>Database</ResourceName>
<Parent>Instance</Parent>
</ResourceType>
<ResourceType>
<ResourceName>Instance</ResourceName>
</ResourceType>
</ResourceTypes>
<RequireFileSystemPlugin>no</RequireFileSystemPlugin>
<ResourceRequiresAuthentication>yes</ResourceRequiresAuthentication>
<SupportsApplicationRecovery>yes</SupportsApplicationRecovery>
</Plugin>
```

ZIP ファイルを作成しています

プラグインが開発され、記述子ファイルが作成されたら、プラグインファイルとを追加する必要があります Plugin_descriptor.xmlファイルをフォルダに移動してzip圧縮します。

ZIP ファイルを作成する前に、次の点を考慮してください。

- スクリプト名はプラグイン名と同じである必要があります。
- Perlプラグインの場合、ZIPフォルダにスクリプトファイルとが格納されたフォルダが含まれている必要があります
  ディスクリプタファイルはこのフォルダの外にある必要があります。フォルダ名はと同じである必要があります
  プラグイン名。
- Perlプラグイン以外のプラグインの場合は、ZIPフォルダに記述子とが含まれている必要があります
  スクリプトファイル。

- OS のバージョンは番号である必要があります。

例

- DB2 プラグイン： DB2.pm と Plugin_descriptor.xml ファイルを「 DB2.zip 」に追加します。
- Javaを使用して開発されたプラグイン：jarファイル、依存するjarファイル、およびを追加します Plugin_descriptor.xmlファイルをフォルダに保存してzip圧縮します。

プラグインの **ZIP** ファイルをアップロードしています

プラグインをで使用できるように、プラグインのZIPファイルをSnapCenterサーバにアップロードする必要があります
目的のホストへの導入

UI またはコマンドレットを使用して、プラグインをアップロードできます。

- UI ： *
- プラグインの ZIP ファイルを * Add * または * Modify Host * ワークフローウィザードの一部としてアップロードします
- [選択] をクリックしてカスタムプラグインをアップロードします。 *
- PowerShell ： *
- uploadSmPluginPackage コマンドレット

  たとえば、 PS> Upload-SmPluginPackage-AbsolutePath c ： \DB2_1.zip のように入力します

  PowerShellコマンドレットの詳細については、SnapCenterコマンドレットのヘルプまたはを使用してください
  コマンドレットのリファレンス情報を参照してください。

"SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

カスタムプラグインの導入

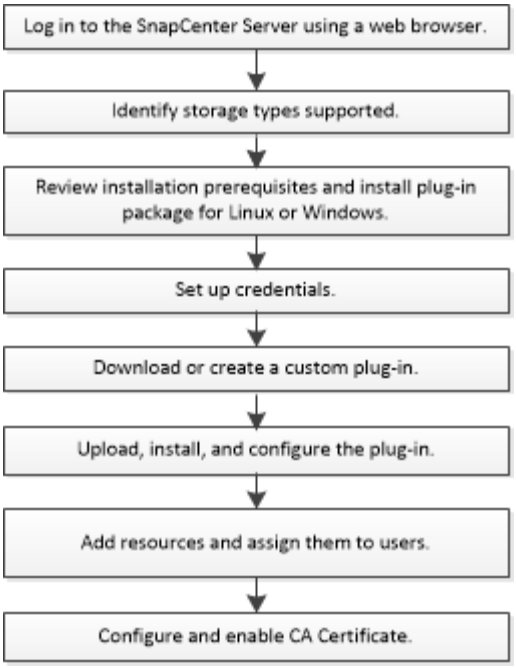
アップロードしたカスタムプラグインが、の一部として目的のホストに導入できるようになります
*[ホストの追加]および[ホストの変更]ワークフロー。には複数のバージョンのプラグインをアップロードできます
SnapCenterサーバを選択すると、特定のホストに導入するバージョンを選択できます。

プラグインのアップロード方法の詳細については、を参照してください。 "ホストを追加し、プラグインパッケージをリモートホストにインストールする"

SnapCenter カスタムプラグインをインストールする準備をします

SnapCenter Custom Plug-ins のインストールワークフロー

カスタムプラグインリソースを保護する場合は、 SnapCenter Custom Plug-ins をインストールしてセットアップする必要があります。



"アプリケーション用のプラグインを開発します"

ホストを追加して **SnapCenter Custom Plug-ins** をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。Custom Plug-ins は、 Windows と Linux のどちらの環境でも使用できます。

- カスタムプラグインを作成しておく必要があります。詳細については、開発者情報を参照してください。

  "アプリケーション用のプラグインを開発します"

- MySQL または DB2 アプリケーションを管理する場合は、ネットアップが提供している MySQL および DB2 のカスタムプラグインをダウンロードしておく必要があります。
- Java 1.8またはJava 11（64ビット）がLinuxホストまたはWindowsホストにインストールされている必要があります。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- カスタムプラグインが、ホストの追加処理を実行するクライアントホストにインストールされている必要があります。

全般

iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。

SHA512ハッシュ

- ネットアップが提供するカスタムプラグインでは、カスタムプラグインファイルのSHA512ハッシュを_custom_plugin_checksum_list _ fileに追加しておく必要があります。

- Linuxホストでは、SHA512ハッシュは、_/var/opt/snapcenter/scc/custom plugin _checksum_list .txt_ にあります
- Windowsホストの場合、SHA512ハッシュはにあります
  C：\Program Files\NetApp\SnapCenter Plug-in Creator\etc\custom_plugin_checksum_list.txt_

  カスタムのインストールパスでは、SHA512ハッシュは_<custom path>\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\custom_plugin_checksum_list .txt_にあります

custom_plugin_schecksum_listは、SnapCenter によってホストにインストールされたカスタムプラグインの一部です。

- アプリケーション用に作成したカスタムプラグインについては、次の手順を実行しておく必要があります。

  a. プラグインzipファイルのSHA512ハッシュを生成しました。

     などのオンラインツールを使用できます "SHA512ハッシュ"。

  b. 生成されたSHA512ハッシュを新しい行のcustom_plugin_schecksum_listファイルに追加しました。

     コメントは、ハッシュが属するプラグインを識別するために#記号で始まります。

     次に、チェックサムファイルでSHAN512ハッシュを使用する例を示します。

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Windows ホスト

- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。
- SnapCenter でクラスタノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限を持つユーザが必要です。

Linux ホスト

- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Java 1.8またはJava 11（64ビット）をLinuxホストにインストールしておく必要があります。

  SnapCenter ServerホストにWindows Server 2019またはWindows Server 2016を使用している場合は、Java 1.8またはJava 11（64ビット）をインストールする必要があります。要件の最新情報については、 Interoperability Matrix Tool （ IMT ）を参照してください。

  "すべてのオペレーティングシステム用の Java のダウンロード"

  "NetApp Interoperability Matrix Tool で確認できます"

- いくつかのパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。visudo Linux ユーティリティを使用して、 /etc/sudoers ファイルに次の行を追加します。

  Sudoバージョン1.8.7以降を使用していることを確認します。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

_linux_user_は、作成したroot以外のユーザの名前です。

checksum_value_xは、_ C：\ProgramData\NetApp\SnapCenter \Package Repository_に ある* ORACLE_checksum.txt *ファイルから取得できます。

この例は、独自のデータを作成するための参照としてのみ使用してください。

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB

項目	要件
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

SnapCenter Plug-ins Package for Linux をインストールするためのホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストが要件を満たしていることを確認する必要があります。

項目	要件
オペレーティングシステム	• Red Hat Enterprise Linux の場合 • Oracle Linux の場合 • SUSE Linux Enterprise Server （ SLES ）
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	2 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。

項目	要件
必要なソフトウェアパッケージ	Java 1.8 （ 64 ビット） Oracle Java または OpenJDK Java を最新バージョンにアップグレードした場合は、 /var/opt/snapcenter /etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"

SnapCenter Custom Plug-ins のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますSnapCenter プラグインのインストールに必要なクレデンシャル、およびデータベースや Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- 必要なもの *
- Linux ホスト

  Linux ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。

  プラグインプロセスをインストールして開始するための sudo 権限がある root ユーザまたは root 以外のユーザのクレデンシャルを設定する必要があります。

  * ベストプラクティス： * ホストを導入してプラグインをインストールしたあとに Linux のクレデンシャルを作成することは可能ですが、 SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

- Windows ホスト

  プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。

  リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定する必要があります。

- Custom Plug-ins アプリケーション

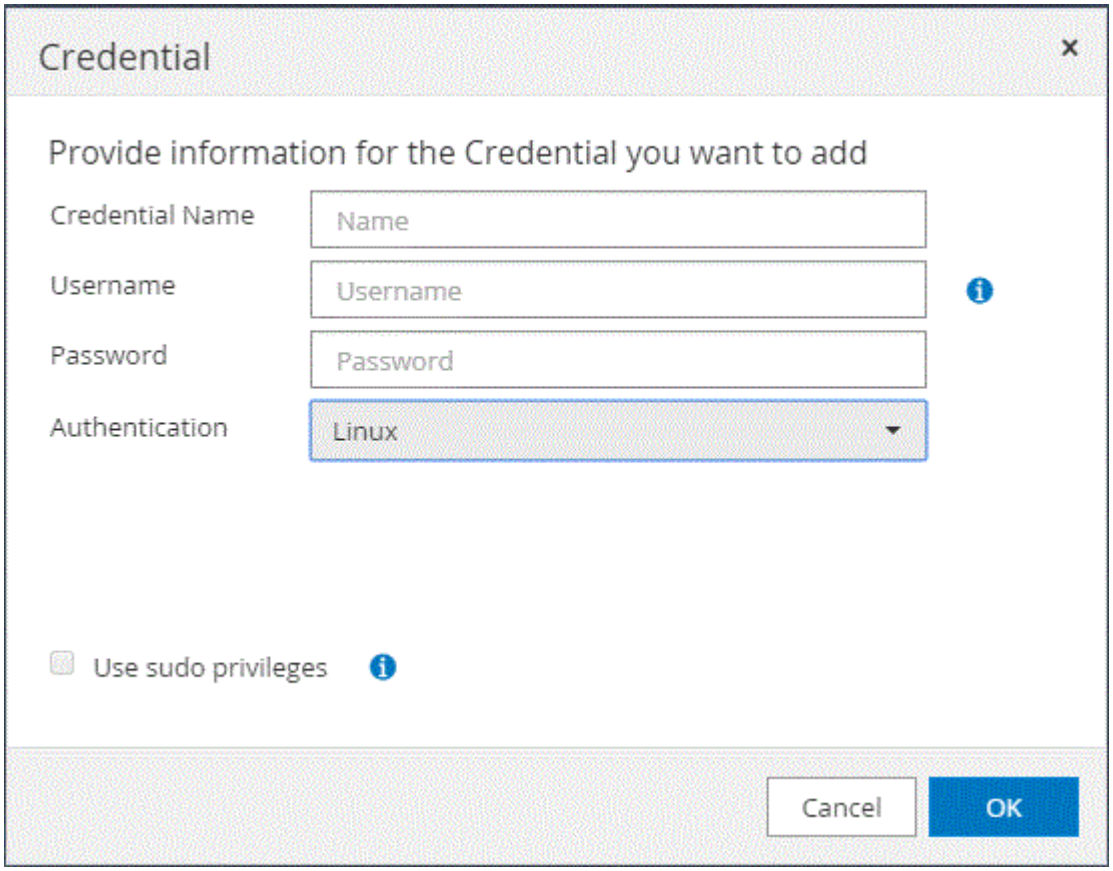
  プラグインは、リソースの追加時に選択または作成されたクレデンシャルを使用します。データ保護処理中にクレデンシャルが不要なリソースの場合は、クレデンシャルを「 * なし」に設定できます。

- このタスクについて *

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* 資格情報] をクリックします。
3. [新規作成（ New ）] をクリックする。



4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	手順
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。 ◦ NETBIOS_USERNAME_ ◦ _ ドメイン FQDN\ ユーザ名 _ • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Username フィールドの有効な形式は、*username* です
パスワード	認証に使用するパスワードを入力します。
認証モード	使用する認証モードを選択します。
sudo 権限を使用する	root 以外のユーザのクレデンシャルを作成する場合は、「 * sudo 権限を使用する * 」チェックボックスをオンにします。 Linux ユーザのみに該当します。

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、 [ユーザとアクセス（ User and Access ）] ページで、ユーザまたはユーザグループにクレデンシャルのメンテナンスを割り当てることができます。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成

できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
   a. 次の形式でユーザグループアカウントを作成します。

```
 domainName\accountName$
.. グループにコンピュータオブジェクトを追加します。
.. 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. を実行します `Get-ADServiceAccount`
サービスアカウントを確認するコマンド。
```

4. ホストで gMSA を設定します。
   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. ホストを再起動します。

b. PowerShellコマンドプロンプトから次のコマンドを実行して、ホストにgMSAをインストールします。 `Install-AdServiceAccount <gMSA>`

c. 次のコマンドを実行して'gMSAアカウントを確認します `Test-AdServiceAccount <gMSA>`

   1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
   2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

      SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

SnapCenter Custom Plug-ins をインストールします

ホストを追加し、プラグインパッケージをリモートホストにインストールする

ホストを追加するには、 SnapCenterAdd Host ページを使用して、プラグインパッケージをインストールする必要があります。プラグインは、自動的にリモートホストにインストールされます。ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。

- 必要なもの *
- SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- メッセージキューサービスが実行されていることを確認してください。
- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

"カスタムアプリケーション用に、 Windows Server 2012 以降のグループマネージドサービスアカウントを設定します"

- このタスクについて *

SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。

クラスタ（ WSFC ）にプラグインをインストールすると、クラスタのすべてのノードにプラグインがインストールされます。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	ホストタイプを選択します。 • Windows の場合 • Linux の場合 カスタムプラグインは、 Windows と Linux のどちらの環境でも使用できます。
ホスト名	ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。 Windows 環境の場合、信頼されていないドメインホストの IP アドレスは、 FQDN に解決される場合にのみサポートされます。 スタンドアロンホストの IP アドレスまたは FQDN を入力できます。 SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。

フィールド	手順
クレデンシャル	作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. [インストールするプラグインを選択してください *] セクションで、インストールするプラグインを選択します。
6. （オプション） * その他のオプション * をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。

フィールド	手順
インストールパス	カスタムプラグインは、 Windows システムと Linux システムのどちらにもインストールできます。 • Windows 用 SnapCenter Plug-ins パッケージのデフォルトパスは C ： \Program Files\NetApp\SnapManager です。 必要に応じて、パスをカスタマイズできます。 • SnapCenter Plug-ins Package for Linux のデフォルトパスは /opt/NetApp/SnapCenter です。 必要に応じて、パスをカスタマイズできます。 • SnapCenter Custom Plug-ins の場合： i. Custom Plug-ins （カスタムプラグイン）セクションで * Browse （参照） * をクリックし、 zip 形式のカスタムプラグインフォルダーを選択します。 zip 形式のフォルダには、カスタムプラグインコードと DESCRIPTOR .xml ファイルが含まれています。 Storage Plug-inの場合は、_C ：\ProgramData\NetApp\SnapCenter \Package Repository_に 移動して、を選択します `Storage.zip` フォルダ。 ii. [アップロード] をクリックします。 パッケージをアップロードする前に zip 形式のカスタムプラグインフォルダ内の記述子 .xml ファイルが検証されます。 SnapCenter サーバにアップロードされたカスタムプラグインが表示されます。 MySQL または DB2 アプリケーションを管理する場合は、ネットアップが提供している MySQL および DB2 のカスタムプラグインを使用できます。MySQL と DB2 のカスタムプラグインについては、を参照してください "NetApp Automation Store の略"

フィールド	手順
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	Windows ホストの場合、プラグインサービスの実行にグループ管理サービスアカウント（ gMSA ）を使用する場合は、このチェックボックスをオンにします。 gMSA 名を domainName\accountName$ の形式で指定します。 gMSA は、 SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されます。

7. [Submit （送信）] をクリックします。

「 * 事前確認をスキップ」チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかが検証されます。ディスクスペース、 RAM 、 PowerShell のバージョン、 .NET のバージョン、場所（ Windows プラグインの場合）、および Java のバージョン（ Linux プラグインの場合）が、最小要件に照らして検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

エラーがディスクスペースまたは RAM に関連している場合は、 C ： \Program Files\NetApp\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

1. ホストタイプが Linux の場合は、フィンガープリントを確認し、 * Confirm and Submit * をクリックします。

同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

2. インストールの進行状況を監視します。

インストール固有のログファイルは、 /custom_location/snapcenter /logs にあります。

コマンドレットを使用して、複数のリモートホストに **Linux** または **Windows** 用の **SnapCenter** プラグインパッケージをインストールします

Install-SmHostPackage PowerShell コマンドレットを使用すると、複数のホストに Linux または Windows 向け SnapCenter プラグインパッケージを同時にインストールできます。

- 必要なもの *

ホストを追加するユーザには、ホストに対する管理者権限が必要です。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 Open-SmConnection コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

プラグインを手動でインストールし、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、 -skipprecheck オプションを使用できます。

1. リモートインストールのクレデンシャルを入力します。

コマンドラインインターフェイスを使用して、 **Linux** ホストに **SnapCenter** カスタムプラグインをインストールします

SnapCenter カスタムプラグインは、 SnapCenter ユーザインターフェイス（ UI ）を使用してインストールする必要があります。環境内で SnapCenter UI からプラグインのリモートインストールが許可されていない場合は、カスタムプラグインをコンソールモードまたはサイレントモードでインストールできます。そのためには、コマンドラインインターフェイス（ CLI ）を使用します。

- 手順 *

1. SnapCenter Plug-ins Package for Linux のインストールファイル（ snapcenter linux_host_plugin.bin ）を C ： \ProgramData\NetApp\SnapCenter \Package Repository から、カスタムプラグインをインストールするホストにコピーします。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

2. コマンドプロンプトで、インストールファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -dport には、 SMCore HTTPS 通信ポートを指定します。
- - DSERVER_IP は、 SnapCenter サーバの IP アドレスを指定します。
- - DSERVER_HTTPS_PORT には、 SnapCenter サーバの HTTPS ポートを指定します。
- -duser_install_DIR - SnapCenter Plug-ins Package for Linux をインストールするディレクトリを指定します
- DINSTALL_LOG_name は、ログファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Add-Smhost コマンドレットと必要なパラメータを使用して、ホストを SnapCenter サーバに追加します。

   コマンドで使用できるパラメータとその説明については、 RUNNING Get Help command_name _ を使用して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

5. SnapCenter にログインし、 UI または PowerShell コマンドレットを使用してカスタムプラグインをアップロードします。

   カスタムプラグインを UI からアップロードする方法については、を参照してください "ホストを追加し、プラグインパッケージをリモートホストにインストールする" セクション。

   PowerShell コマンドレットの詳細については、 SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

"SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

カスタムプラグインのインストールのステータスを監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした

- キューに登録され
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
     a. [* フィルタ * （ Filter * ）] をクリック
     b. オプション：開始日と終了日を指定します。
     c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
     d. Status ドロップダウンメニューから、インストールステータスを選択します。
     e. [適用（ Apply ）] をクリックします。
  4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

- 手順 *
  1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
  2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。

3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *
  1. GUI で次の手順を実行します。
     a. 証明書をダブルクリックします。
     b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
     c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
     d. ボックスから 16 進文字をコピーします。
     e. 16 進数の間のスペースを削除します。

        たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

  2. PowerShell で次の手順を実行します。
     a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近イ

ンストールされた証明書を件名で識別します。

Get-ChildItem - パス証明書： *\localmachine\My*

b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して **CA** 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   . 次のコマンドを実行して、新しくインストールした証明書を Windows ホストプラグインサービスにバインドします。

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
   certhash=$cert appid="$guid"
   ```

   例：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux ホストで **SnapCenter Custom Plug-ins** サービスの **CA** 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードを管理し、CA証明書を設定し、カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定し、インストールされたデジタル証明書をアクティブ化するために、SnapCenterカスタムプラグインサービスを使用してカスタムプラグインの信頼ストアにCA署名キーペアを設定する

必要があります。

カスタムプラグインでは、ファイル「 keystore.JKS 」を使用します。このファイルは、信頼ストアおよびキーストアとして _/opt/NetApp/snapcenter / scc /etc/both にあります。

カスタムプラグインのキーストアのパスワード、および使用中の **CA** 署名済みキーペアのエイリアスを管理します

- 手順 *

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   キー「 keystore.pass 」に対応する値です。

2. キーストアのパスワードを変更します。

   ```
   keytool -storepasswd -keystore keystore.jks
   ```

   .
   キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

3. パスワードを変更したら、サービスを再起動してください。

> ⓘ カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *

1. カスタムプラグインキーストアが格納されているフォルダ（/opt/NetApp/snapcenter/scc/etc）に移動します。
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. ルート証明書または中間証明書を追加します。

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```
.
カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

- 手順 *
  1. カスタムプラグインキーストア /opt/NetApp/snapcenter / scc などが含まれているフォルダに移動します
  2. ファイル 'keystore.jkS' を探します。
  3. キーストアに追加された証明書を表示します。

     ```
     keytool -list -v -keystore keystore.jks
     ```

  4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

     ```
     keytool -importkeystore -srckeystore
     /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore
     keystore.jks -deststoretype JKS
     ```

  5. キーストアに追加された証明書を表示します。

     ```
     keytool -list -v -keystore keystore.jks
     ```

  6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
  7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

     デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

     ```
      keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
     keystore.jks
     ```
     . CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「 * 」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
 keytool -changealias -alias "long_alias_name" -destalias
"simple_alias" -keystore keystore.jks
. agent.properties ファイルの CA 証明書からエイリアス名を設定します。
```

この値をキー SCC_CERTIFICATE_ALIAS に更新します。

8. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ CRL ）を設定します

- このタスクについて *
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、「 /opt/netapp/snapcenter /sscc /etc/crl 」です。
- 手順 *
  1. agent.properties ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。

     このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

Windows ホストで SnapCenter Custom Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードを管理し、CA証明書を設定し、カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定し、インストールされたデジタル証明書をアクティブ化するために、SnapCenterカスタムプラグインサービスを使用してカスタムプラグインの信頼ストアにCA署名キーペアを設定する必要があります。

カスタムプラグインは、 _C ： \Program Files\NetApp\SnapManager \Snapcenter Plug-in Creator\etc_both にある file_keystore.JKS_を 信頼ストアおよびキーストアとして使用します。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

- 手順 *
  1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

     key_keystore.pass_ に対応する値です。

  2. キーストアのパスワードを変更します。

     keytool -storepasswd -keystore keystore.JKS

     Windows のコマンドプロンプトで「 keytool 」コマンドが認識されない場合は、keytool コマンドを完全なパスに置き換えます。

C ： \Program Files\Java\<JDK_version >\bin\keytool .exe "-storepasswd -keystore keystore.JKS

3. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.JKS

agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

1. パスワードを変更したら、サービスを再起動してください。

   カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *

1. カスタムプラグインkeystore_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_が格納されているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. ルート証明書または中間証明書を追加します。

   keytool -import-trustcacerts -alias myRootCA -file/root/USERTrustRSA_Root.cer -keystore keystore.JKS

5. カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

- 手順 *

1. カスタムプラグインの keystore _C ： \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. file_keystore.JKS_</Z1> を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

   keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.JKS -deststoretype JKS

5. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

   デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

*keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

1. *agent.properties* ファイルの CA 証明書からエイリアス名を設定します。

   この値をキー SCC_CERTIFICATE_ALIAS に更新します。

2. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ **CRL** ）を設定します

- このタスクについて *
- 関連する CA 証明書の最新の CRL ファイルをダウンロードするには、を参照してください "SnapCenter CA 証明書の証明書失効リストファイルを更新する方法"。
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、 *'C:\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\crl'* です。
- 手順 *
  1. *agent.properties* ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。
  2. このディレクトリに複数の CRL ファイルを配置できます。

     着信証明書は各 CRL に対して検証されます。

プラグインの **CA** 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

データ保護を準備

SnapCenter Custom Plug-ins を使用するための前提条件

SnapCenter Custom Plug-ins を使用するには、 SnapCenter 管理者が SnapCenter サーバをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。
- SnapCenter サーバにログインします。
- 必要に応じて、ストレージシステム接続を追加し、クレデンシャルを作成して、 SnapCenter 環境を設定します。
- ホストを追加し、プラグインをインストールしてアップロードします。
- 必要に応じて、 Java 1.7 または Java 1.8 をプラグインホストにインストールします。
- データパス（ LIF ）が複数ある場合、または dNFS 構成を使用している場合は、データベースホストで SnapCenter CLI を使用して次の作業を実行できます。
  - デフォルトでは、データベースホストのすべての IP アドレスが、クローンボリュームの Storage Virtual Machine （ SVM ）の NFS ストレージエクスポートポリシーに追加されます。特定の IP アドレスを使用する場合、または IP アドレスのサブセットに制限する場合は、 Set-PreferredHostIPsInStorageExportPolicy CLI を実行します。

- SVM に複数のデータパス（ LIF ）がある場合は、 NFS クローンボリュームをマウントするための適切なデータパス（ LIF ）が SnapCenter によって選択されます。ただし、特定のデータパス（ LIF ）を指定する場合は、 Set-SvmPreferredDataPath CLI を実行する必要があります。
  コマンドで使用できるパラメータとその説明については、 RUNNING Get Help command_name _ を使用して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドリファレンスガイド"。

- バックアップレプリケーションが必要である場合は、 SnapMirror と SnapVault をセットアップします。
- ポート 9090 がホストの他のアプリケーションで使用されていないことを確認します。

  SnapCenter で必要な他のポートに加え、ポート 9090 を SnapCenter カスタムプラグイン用に確保しておく必要があります。

カスタムプラグインリソースの保護におけるリソース、リソースグループ、ポリシーの使用方法

SnapCenter を使用する前に、実行するバックアップ、クローニング、およびリストアの処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- リソースとは、 SnapCenter でバックアップやクローンを作成するデータベース、 Windows ファイルシステム、 VM などです。
- SnapCenter リソースグループは、ホストまたはクラスタ上のリソースの集まりです。

  リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているリソースに対して処理が実行されます。

  単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。スケジュールされたバックアップを単一のリソースおよびリソースグループに対して実行することもできます。

- ポリシーは、バックアップ頻度、コピーの保持、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

  リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。単一のリソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、すべてのデータベースをバックアップする場合や、ホストのすべてのファイルシステムをバックアップする場合は、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。リソースグループを作成してポリシーを適用する際に、ファイルベースのバックアップを 1 日 1 回実行するようにリソースグループを設定し、別のスケジュールで Snapshot ベースのバックアップを 1 時間おきに実行するように設定します。

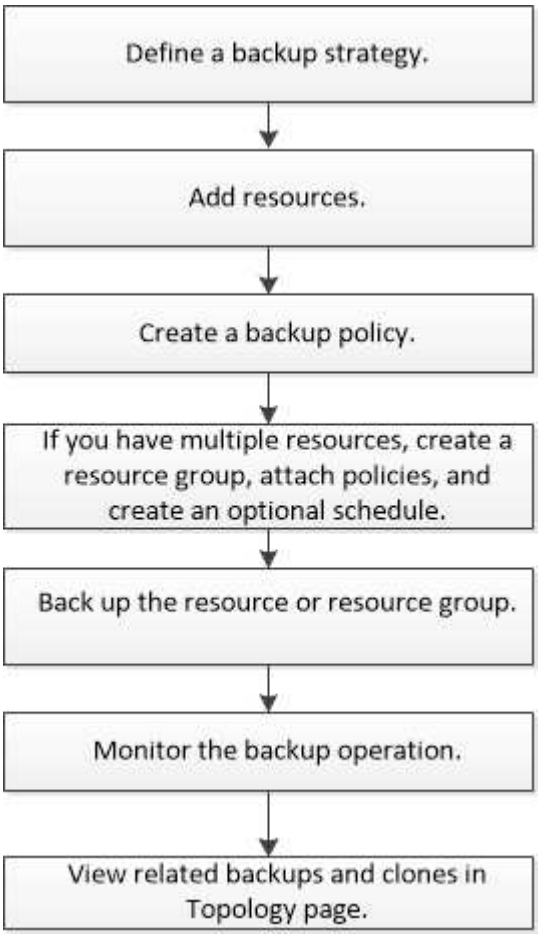
カスタムプラグインリソースをバックアップする

カスタムプラグインリソースをバックアップする

バックアップのワークフローには、計画、バックアップするリソースの特定、バックア

ップポリシーの管理、リソースグループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、 SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

SnapCenter Custom Plug-ins にリソースを追加します

バックアップまたはクローンを作成するリソースを追加する必要があります。環境によっては、バックアップまたはクローンを作成するデータベースインスタンスやそのコレクションもリソースに含まれます。

作業を開始する前に

- SnapCenter サーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- が必要です "アプリケーション用のカスタムプラグインを作成しました"。
- SnapCenter サーバにプラグインをアップロードしておく必要があります。

このタスクについて

MySQL や DB2 のアプリケーション用のリソースを追加することもできます。これらのプラグインは、からダウンロードできます "NetApp Storage Automation Store の略"。

手順

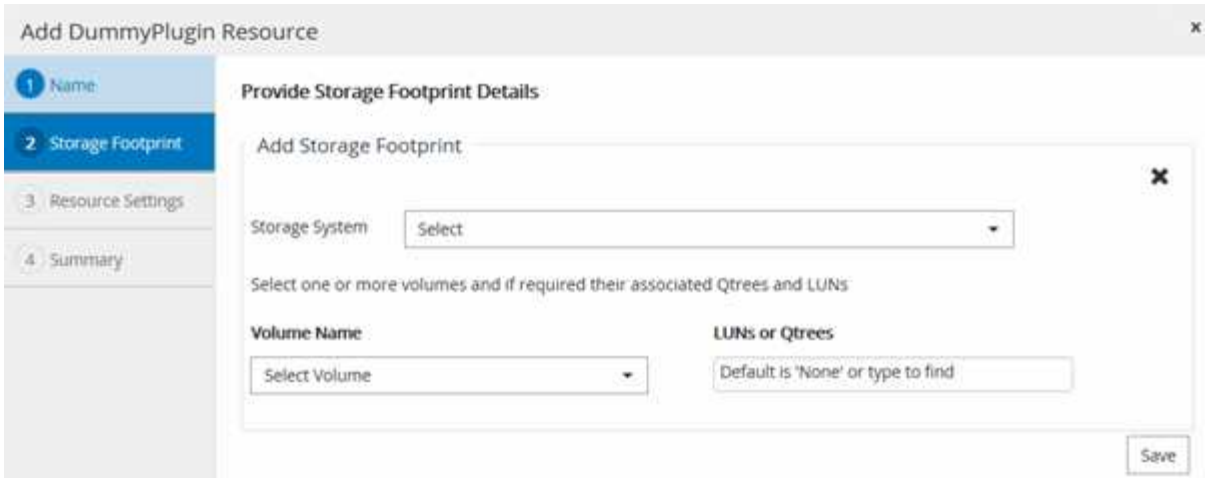
1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [リソース]ページで、*[リソースの追加]*を選択します。
3. [Provide Resource Details] ページで、次の操作を実行します。

フィールド	手順
名前	リソースの名前を入力します。
ホスト名	ホストを選択します。
を入力します	タイプを選択します。type は、プラグインの概要ファイルに基づいてユーザが定義します。たとえば、データベースやインスタンスなどです。 選択したタイプに親がある場合は、親の詳細を入力します。たとえば、タイプがデータベースで親がインスタンスの場合、インスタンスの詳細を入力します。
クレデンシャル名	[資格情報] を選択するか、新しい資格情報を作成します。
マウントパス	リソースのマウント先のマウントパスを入力します。 これは Windows ホストにのみ適用されます。

4. [ストレージフットプリントの入力]ページで、ストレージシステムを選択して1つ以上のボリューム、LUN、およびqtreeを選択し、*[保存]*を選択します。

   オプション：を選択します  アイコンをクリックして、他のストレージシステムからボリューム、LUN 、および qtree を追加します。

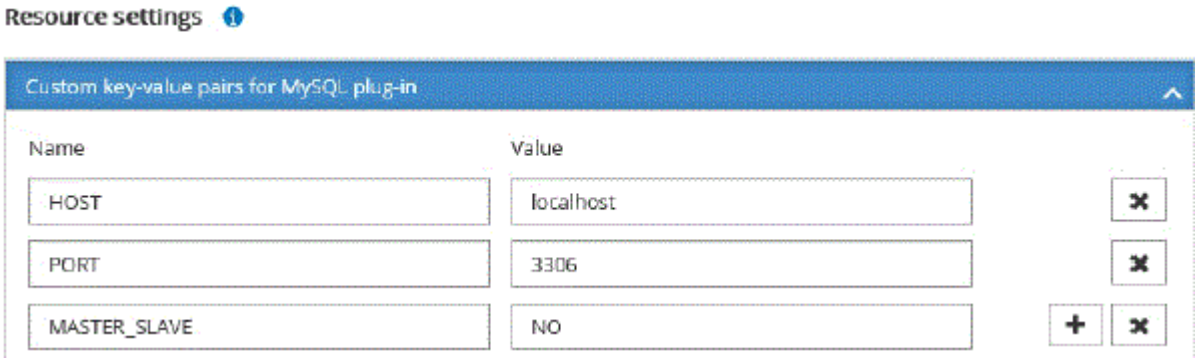
   SnapCenter Custom Plug-ins では、リソースの自動検出がサポートされておらず、物理環境と仮想環境のストレージの詳細は取得されません。リソースの作成時に、物理環境と仮想環境のストレージの情報を指定する必要があります。



5. リソース設定ページで、リソースのカスタムキーと値のペアを指定します。

   リソース固有の情報を渡す場合は、カスタムのキーと値のペアを使用します。たとえば 'MySQL プラグインを使用する場合 ' ホストを host=hostname'port=port -no と指定して MySQL に使用し ' マスター / スレーブ構成を master_slave="YES" または「 no` 」と指定する必要があります (名前は master_slave で ' 値は "YES" または "no")

   host および port という単語が大文字であることを確認します。



6. 概要を確認し、*[終了]*を選択します。

結果

リソースは、タイプ、ホストまたはクラスタ名、関連するリソースグループとポリシー、全体的なステータスなどの情報とともに表示されます。

データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

完了後

アセットへのアクセスを他のユーザに許可する場合は、 SnapCenter 管理者が対象のユーザにアセットを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して権限のある処理を実行できます。

リソースを追加したあとに、リソースの詳細を変更することができます。カスタムプラグインリソースにバックアップが関連付けられている場合、リソース名、リソースタイプ、およびホスト名のフィールドは変更できません。

カスタムプラグインリソースのポリシーを作成する

SnapCenter を使用してカスタムプラグイン固有のリソースをバックアップする前に、バックアップ対象のリソースまたはリソースグループのバックアップポリシーを作成する必要があります。

- 必要なもの *
- バックアップ戦略を定義しておく必要があります。

  詳細については、カスタムプラグインのデータ保護戦略の定義に関する情報を参照してください。

- データ保護の準備が完了している必要があります。

  データ保護の準備作業には、 SnapCenter のインストール、ホストの追加、ストレージシステム接続の作成、リソースの追加などがあります。

- ミラー処理またはバックアップ処理を実行する場合は、 Storage Virtual Machine （ SVM ）をユーザに割り当てる必要があります。

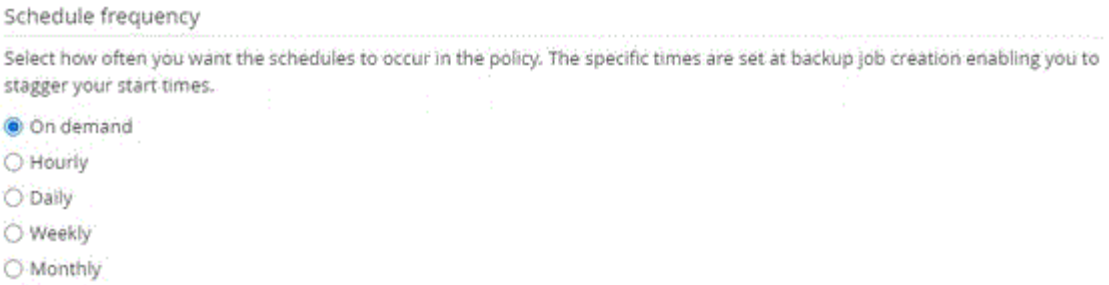
  ユーザが Snapshot コピーをミラーまたはバックアップにレプリケートする場合は、ソースボリュームとデスティネーションボリューム両方の SnapCenter に SVM を割り当てる必要があります。

- 保護するリソースを手動で追加しておく必要があります。
- このタスクについて *
- バックアップポリシーとは、バックアップを管理、スケジューリング、および保持する方法を定めた一連のルールです。レプリケーション、スクリプト、アプリケーション設定を指定することもできます。
- ポリシーでオプションを指定しておくことで、別のリソースグループにポリシーを再利用して時間を節約することができます。
- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. 設定ページで、次の手順を実行します。

   - スケジュールタイプを指定するには、「 * on demand * 」、「 * Hourly * 」、「 * Daily * 」、「 * Weekly * 」、または「 * Monthly * 」を選択します。

   リソースグループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間（ DST ）中はスケジュールはトリガーされません。

- Custom backup settings （カスタムバックアップ設定）セクションで、プラグインにキーバリュー形式で渡す必要がある特定のバックアップ設定を指定します。プラグインに渡すキーと値の組み合わせを複数指定することができます。

1. [保持] ページで ' バックアップ・タイプの保持設定と [バックアップ・タイプ] ページで選択したスケジュール・タイプを指定します

状況	作業
一定数の Snapshot コピーを保持します	保持する Snapshot コピーの総数 * を選択し、保持する Snapshot コピーの数を指定します。 Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。 SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。 最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。
Snapshot コピーを特定の日数だけ保持します	「 * Snapshot コピーを保持する期間」を選択し、 Snapshot コピーを削除するまで保持する日数を指定します。

2. Replication （レプリケーション）ページで、レプリケーション設定を指定します。

フィールド	手順
• ローカル Snapshot コピー作成後に SnapMirror を更新 *	別のボリュームにバックアップセットのミラーコピーを作成する場合（ SnapMirror レプリケーション）は、このフィールドを選択します。 ONTAP の保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成された Snapshot コピーがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。この Snapshot コピーがリストア処理の対象としてデスティネーションで選択されると、「 Secondary Location is not available for the selected vaulted/mirrored backup 」というエラーメッセージが表示されます。
• ローカル Snapshot コピー作成後に SnapVault を更新 *	ディスクツーディスクのバックアップレプリケーション（ SnapVault バックアップ）を実行する場合は、このオプションを選択します。
• 二次ポリシーラベル *	Snapshot ラベルを選択します。 選択した Snapshot コピーラベルに応じて、 ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。 ローカル Snapshot コピーの作成後に「 * SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できます。ただし、ローカル Snapshot コピーの作成後に「 * Update SnapVault 」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。
• エラー再試行回数 *	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。

セカンダリストレージでの Snapshot コピーの最大数に達しないように、 ONTAP でセカンダリストレージの SnapMirror 保持ポリシーを設定する必要があります。

3. 概要を確認し、 [完了] をクリックします。

SnapCenter でリソースグループを作成し、ポリシーを適用します

リソースグループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップでき、あらゆるデータ保護ジョブに必要になります。リソースグループに 1 つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

手順

1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [Resources]ページで、[New Resource Group]を選択します。
3. [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループの名前を入力します。 注：リソースグループ名は250文字以内にする必要があります。
タグ	リソースグループを検索するときに役立つラベルを入力します。 たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。
Snapshot コピーには、カスタムの名前形式を使用します	Snapshot コピー名にカスタムの名前形式を使用する場合は、このチェックボックスをオンにして名前形式を入力します。 たとえば、 _customText_resource group_policy_hostname や resource group_hostname_hostname などです。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

4. オプション：[リソース]ページで、**[ホスト]***ドロップダウンリストからホスト名を選択し、[リソースタイプ]*ドロップダウンリストからリソースタイプを選択します。

   これにより、画面上の情報をフィルタリングできます。

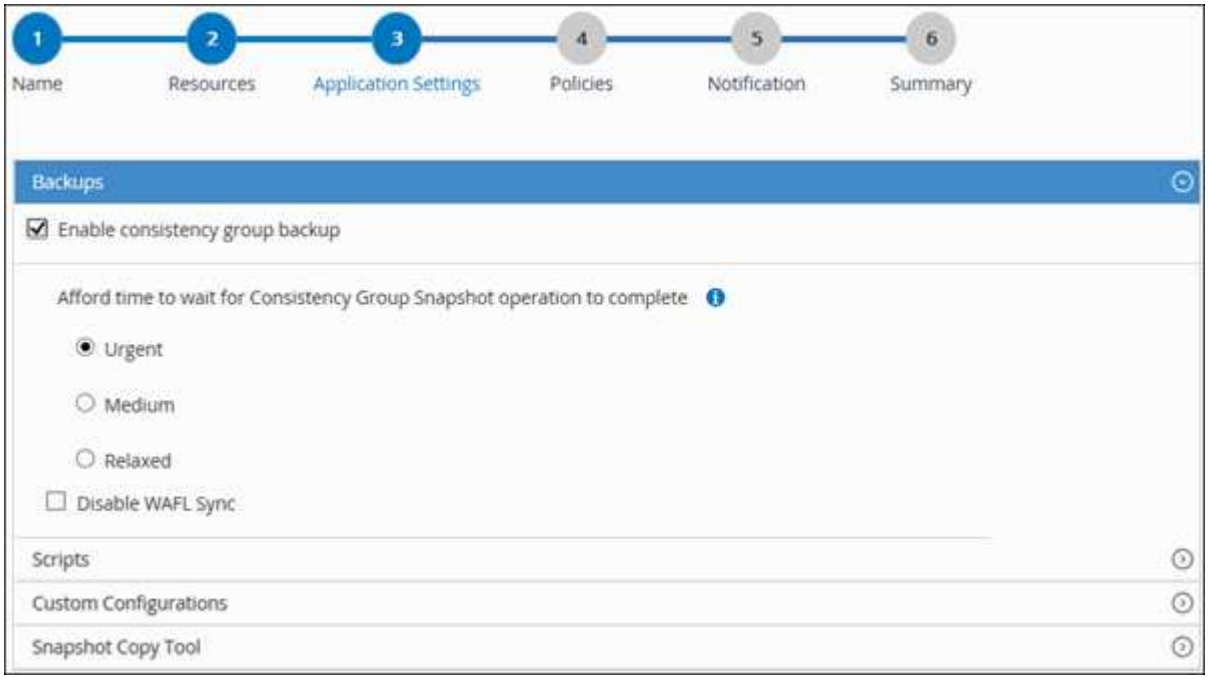
5. [Available Resources]セクションからリソースを選択し、右矢印を選択して[Selected Resources]セクションに移動します。
6. オプション：[Application Settings]ページで、次の手順を実行します。

   a. [Backups]の矢印を選択して、追加のバックアップオプションを設定します。

      整合グループのバックアップを有効にし、次の作業を実行します。

フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot コピー処理が完了するまでの待機時間を指定するには、「至急」、「中」、または「不完全」を選択します。 Urgent = 5 秒、 Medium = 7 秒、 Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

+



a. [Scripts]の矢印を選択し、休止、Snapshotコピー、および休止解除の処理を実行するプリコマンドとポストコマンドを入力します。障害発生時に終了する前に実行する PRE コマンドを入力することもできます。

b. [Custom Configurations]の矢印を選択し、このリソースを使用するすべてのデータ保護処理に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
archive_log_enable	（はい / いいえ）	アーカイブログ管理を有効にしてアーカイブログを削除できます。

パラメータ	設定	説明
archive_log_retention の略	日数	に日数を指定します アーカイブログは保持されます。 この設定 以上でなければなりません NTAP_SNAPSHOT_ 保持：
ARCHIVE_LOG_DIR	change_info_directory/logs	ディレクトリへのパスを指定します アーカイブログが格納されます。
archive_log_EXT	ファイル拡張子	アーカイブログファイルを指定します 延長の長さ。 たとえば、がの場合などです アーカイブログはです LOG_BACKUP_0_0_0.1615185 51942 9で、file_extensionの値が5の場合は、 その後、ログの拡張が行われます 5桁（16151）を保持します。
ARCHIVE_LOG_RECURSIVE_ SE アーチ	（はい / いいえ）	アーカイブの管理を可能にします サブディレクトリ内にログを記録します。 あなた このパラメータは、で使用します アーカイブログはにあります サブディレクトリ：

c. [Snapshot Copy Tool]*の矢印を選択して、Snapshotコピーを作成するツールを選択します。

状況	作業
SnapCenter で Plug-in for Windows を使用してファイルシステムを整合性のある状態にしてから Snapshot コピーを作成する。Linux リソースの場合、このオプションは適用されません。	ファイルシステムの整合性を使用した SnapCenter を選択します。 このオプションは、 SnapCenter Plug-in for SAP HANA Database には適用されません。

状況	作業
SnapCenter を使用して、ストレージレベルの Snapshot コピーを作成します	ファイルシステムの整合性なしで SnapCenter を選択します。
Snapshot コピーを作成するためにホストで実行するコマンドを入力する	Other を選択し、ホストで実行するコマンドを入力して Snapshot コピーを作成します。

7. [Policies] ページで、次の手順を実行します。

   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

      []を選択してポリシーを作成することもできます

      ポリシーは、 [選択したポリシーのスケジュールの設定 *] セクションに一覧表示されます。

   b. [スケジュールの設定]列で、を選択します をクリックします。

   c. [Add schedules for policy_policy_name_]ダイアログボックスで、スケジュールを設定して[OK]を選択します。

      policy_nameは、選択したポリシーの名前です。

   設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。
   サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。

8. [Notification]ページの[Email preference]*ドロップダウンリストから、Eメールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。SMTP サーバーは、 * Settings * > * Global Settings * で設定する必要があります。

9. 概要を確認し、*[終了]*を選択します。

個々のカスタムプラグインリソースをバックアップする

個々のカスタムプラグインリソースがどのリソースグループにも含まれていない場合は、のリソースページからリソースをバックアップできます。リソースはオンデマンドでバックアップすることも、リソースにポリシーが適用されてスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われるようにすることもできます。

- 必要なもの *
- バックアップポリシーを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、 **View**] ドロップダウンリストからリソースをフィルタリングします。

   をクリックします をクリックし、ホスト名とリソースタイプを選択してリソースをフィルタリングします。をクリックします をクリックしてフィルタペインを閉じます。
3. バックアップするリソースをクリックします。
4. リソースページで、カスタム名を使用する場合は、 Snapshot コピーに * カスタムの名前形式を使用する * チェックボックスをオンにし、 Snapshot コピー名のカスタム名形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。
5. [アプリケーションの設定] ページで、次の操作を行います。

   a. [*Backups] の矢印をクリックして、追加のバックアップ・オプションを設定します。

      必要に応じて、整合グループのバックアップを有効にし、次の作業を実行します。

フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot コピー処理が完了するまでの待機時間を指定するには、「至急」、「中」、または「不完全」を選択します。 Urgent = 5 秒、 Medium = 7 秒、 Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

   +

a. [* Scripts] の矢印をクリックすると、休止、 Snapshot コピー、および休止解除の各処理に対して PRE および POST のコマンドが実行されます。バックアップ処理を終了する前にプリコマンドを実行することもできます。

   プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

b. 「カスタム構成」の矢印をクリックし、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。

c. Snapshot コピーツールの * 矢印をクリックして、 Snapshot コピーを作成するツールを選択します。

状況	作業
SnapCenter でストレージレベルの Snapshot コピーを作成します	ファイルシステムの整合性なしで SnapCenter * を選択します。
SnapCenter で Plug-in for Windows を使用してファイルシステムを整合性のある状態にしてから Snapshot コピーを作成する	ファイルシステムの整合性を維持した状態で SnapCenter を選択します。
Snapshot コピーを作成するコマンドを入力するには、次のコマンドを入力します	「 * other * 」を選択し、コマンドを入力して Snapshot コピーを作成します。

6. [Policies] ページで、次の手順を実行します。

   a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

      をクリックしてポリシーを作成することもできます + 。

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

a. をクリックします  スケジュールを設定するポリシーの Configure Schedules （スケジュールの設定）列。

b. [Add schedules for policy_name_] ダイアログボックスで、スケジュールを設定し、 [OK] をクリックします。

ここで、 _policy_name_は 選択したポリシーの名前です。

設定されたスケジュールは、 [適用されたスケジュール] 列に一覧表示されます。

1. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

2. 概要を確認し、 [完了] をクリックします。

リソースのトポロジページが表示されます。

3. [今すぐバックアップ] をクリックします。
4. Backup （バックアップ）ページで、次の手順を実行します。

a. リソースに複数のポリシーを適用している場合は、「 * Policy * 」ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

b. [バックアップ] をクリックします。

5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

カスタムプラグインリソースのリソースグループをバックアップする

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

- 必要なもの *
- ポリシーを適用したリソースグループを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'napmirror all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックします タグを選択します。をクリックします をクリックしてフィルタペインを閉じます。

3. [リソースグループ] ページで、バックアップするリソースグループを選択し、 [今すぐバックアップ *] をクリックします。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

   b. [バックアップ] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。
   - MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。

     "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"

   - VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。Java のヒープサイズを増やすには、スクリプトファイル /opt/NetApp/init_scripts/scvservice を探します。このスクリプトでは、を実行します `do_start method` コマンドは、SnapCenter VMwareプラグインサービスを開始します。このコマンドを次のように更新します。 `Java -jar -Xmx8192M -Xms4096M`。

PowerShell コマンドレットを使用してストレージシステム接続とクレデンシャルを作成します

PowerShell コマンドレットを使用してデータ保護処理を実行するには、 Storage Virtual Machine （ SVM ）接続とクレデンシャルを作成する必要があります。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前および管理 LIF の IP アドレスを割り当てる必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、 PowerShell 接続セッションを開始します。

   PowerShell セッションを開く例を次に示します。

   ```
   PS C:\> Open-SmConnection
   ```

2. Add-SmStorageConnection コマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

   この例では、新しいストレージシステム接続を作成しています。

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Add-SmCredential コマンドレットを使用して新しいクレデンシャルを作成します。

   この例は、 Windows クレデンシャルを使用して FinanceAdmin という名前の新しいクレデンシャルを作成します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

PowerShell コマンドレットを使用してリソースをバックアップします

リソースをバックアップするときは、 SnapCenter サーバとの接続を確立してから、リソースの追加、ポリシーの追加、バックアップリソースグループの作成を行って、バックアップを実行します。

- 必要なもの *
- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。
- このタスクについて *

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッ

ションを開始します。

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResources コマンドレットを使用してリソースを追加します。

   リソースを追加する例を次に示します。

```
Add-SmResource -HostName '10.232.206.248' -PluginCode 'DB2'
-ResourceName NONREC1 -ResourceType Database -StorageFootPrint ( @
{"VolumeName"="DB2_NONREC1DB";"LunName"="DB2_NONREC1DB";"Vserver"="vs
erver_scauto_secondary"}) -Instance db2inst1
```

3. Add-SmPolicy コマンドレットを使用してバックアップポリシーを作成します。

   この例では、新しいバックアップポリシーを作成しています。

```
Add-SMPolicy -PolicyName 'db2VolumePolicy' -PolicyType 'Backup'
-PluginPolicyType DB2  -description 'VolumePolicy'
```

4. Add-SmResourceGroup コマンドレットを使用して、新しいリソースグループを SnapCenter に追加します。

   この例では、ポリシーとリソースを指定して新しいリソースグループを作成しています。

```
Add-SmResourceGroup -ResourceGroupName
'Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix' -Resources
@(@
{"Host"="10.232.206.248";"Uid"="db2inst2\NONREC"},@{"Host"="10.232.20
6.248";"Uid"="db2inst1\NONREC"}) -Policies db2ManualPolicy
```

5. New-SmBackup コマンドレットを使用して、新しいバックアップジョブを開始する。

```
New-SMBackup -DatasetName
Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix -Policy
db2ManualPolicy
```

6. Get-SmBackupReport コマンドレットを使用して、バックアップジョブのステータスを表示します。

   次の例は、指定した日付に実行されたすべてのジョブの概要レポートを表示します。

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

カスタムプラグインリソースのバックアップ処理を監視する

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され

- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. Jobs （ジョブ）ページで、次の手順を実行します。
     a. をクリックします バックアップ処理だけが表示されるようにリストをフィルタリングします。
     b. 開始日と終了日を指定します。
     c. [* タイプ] ドロップダウン・リストから、 **[*Backup]** を選択します。
     d. [**Status**](ステータス *) ドロップダウンから、バックアップステータスを選択します。
     e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
  4. バックアップジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。

     バックアップジョブのステータスがと表示されます で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

     View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

カスタムプラグインのバックアップ処理をキャンセルする

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの *
- 処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。
- バックアップ操作は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のバックアップ処理をキャンセルすることはできません。
- SnapCenter GUI 、 PowerShell コマンドレット、または CLI コマンドを使用して、バックアップ処理をキャンセルできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っているバックアップ操作をキャンセルできます
- 手順 *
  1. 次のいずれかを実行します。

方法	アクション
監視ページ	a. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 b. 操作を選択し、 * ジョブのキャンセル * をクリックします。
アクティビティペイン	a. バックアップ処理を開始したら、 * をクリックします* ［ アクティビティ ］ パネルには、最近の 5 つの操作が表示されます。 b. 処理を選択します。 c. ［ ジョブの詳細 ］ ページで、 ［ * ジョブのキャンセル * ］ をクリックします。

処理がキャンセルされ、リソースが以前の状態に戻ります。

Topology ページで、カスタムプラグインリソースに関連するバックアップとクローンを表示します

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

- このタスクについて *

[コピーの管理] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップとクローンが使用可能かどうかを判断できます。

-  には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
-  には、 SnapMirror テクノロジを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。

   mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数には、バージョンに依存しないバックアップは含まれません。

-  には、 SnapVault テクノロジを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。

表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、 4 個のバックアップだけを保持するポリシーを使用して 6 個のバックアップを作成した場合、バックアップの数は 6 個と表示されます。

mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数には、バージョンに依存しないバックアップは含まれません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

   リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. 概要カードを確認して、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数をサマリで確認します。

   サマリカードセクションには、バックアップとクローンの合計数が表示されます。

   更新ボタンをクリックすると、ストレージのクエリが実行されて正確な数が表示されます。

5. [コピーの管理] ビューで、プライマリストレージまたはセカンダリストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

   バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。

   セカンダリストレージシステム上のバックアップは、名前変更または削除できません。

   プライマリストレージシステムにあるバックアップは名前を変更できません。

1. クローンを削除する場合は、表でクローンを選択し、をクリックします をクリックしてクローンを削除します。

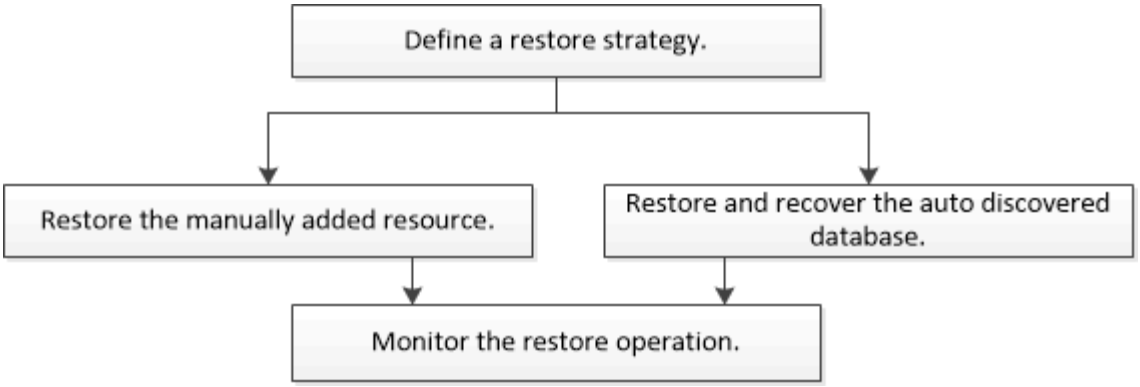
カスタムプラグインリソースをリストアする

カスタムプラグインリソースをリストアする

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

- このタスクについて *

次のワークフローは、リストア処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットについては、 SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

リソースのバックアップをリストアする

SnapCenter を使用してリソースをリストアすることができます。リストア処理の機能は、使用するプラグインによって異なります。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- ユーザが Snapshot コピーをミラーまたはバックアップにレプリケートする場合は、ソースボリュームとデスティネーションボリューム両方の Storage Virtual Machine （ SVM ）を SnapCenter 管理者がユーザに割り当てる必要があります。
- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- このタスクについて *

デフォルトのリストア処理でリストアされるのは、ストレージオブジェクトのみです。アプリケーションレベルのリストア処理は、その機能がカスタムプラグインで提供されている場合にのみ実行できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、 **View**] ドロップダウンリストからリソースをフィルタリングします。

   リソースは、タイプ、ホストまたはクラスタ名、関連するリソースグループとポリシー、ステータスなどの情報とともに表示されます。

   リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。

   リソースが保護されていない場合は、 [**Overall Status**] 列に _NOT PROTECTED _ が表示されます。

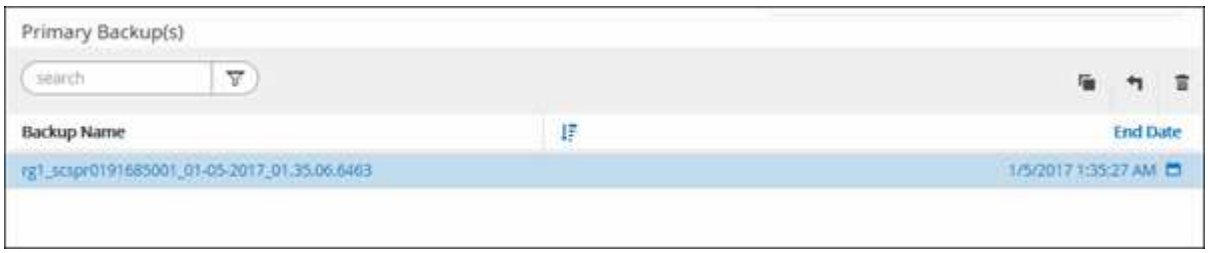
ステータス * 全体のステータス * 列の status_not protected _ は、リソースが保護されていないか、リソースが別のユーザによってバックアップされていることを意味します。

1. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

   リソースのトポロジページが表示されます。

2. [コピーの管理] 表示から、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから [* バックアップ] を選択します。

3. [Primary backup （ s ）] テーブルで、リストア元のバックアップを選択し、をクリックします  。



4. [リストア範囲] ページで、 [* リソース全体 *] または [* ファイルレベル *] を選択します。

   a. [*Complete Resource] を選択した場合、リソースのバックアップがリストアされます。

      リソースにストレージ容量としてボリュームまたは qtree が含まれている場合、それらのボリュームまたは qtree の以降の Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

   b. 「 * ファイルレベル * 」を選択した場合は、「 * すべて * 」を選択するか、ボリュームまたは qtree を選択して、カンマで区切って選択したボリュームまたは qtree に関連するパスを入力できます。

      - ボリュームと qtree は複数選択できます。
      - リソースタイプが LUN の場合は、 LUN 全体がリストアされます。LUN は複数選択できます。
        [+]
        注：*[すべて]*を選択すると、ボリューム、qtree、またはLUN上のすべてのファイルがリストアされます。

5. [Recovery Type] ページで、次の手順を実行します。 select オプションは、ログを適用します。プラグインがリストア・タイプを選択する前に、プラグインがすべてのログとログをサポートしていることを確認してください。

状況	手順
すべてのログをリストアします	[* すべてのログ *] を選択します。 プラグインが * すべてのログ * をサポートしていることを確認します。
指定した時刻まですべてのログをリストアします	[* までログ] を選択します。 プラグインが * Logs Until * をサポートしていることを確認します。

状況	手順
リソースのバックアップをリストアする	「 * なし * 」を選択します。

6. [リストア前] ページで、リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを入力します。
7. [ポスト・オペレーション] ページで、マウントおよびリストア後のコマンドを入力して、リストア・ジョブの実行後に実行します。
8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。SMTP は、 [* 設定 * > * グローバル設定 * （ * Settings * > * Global Settings * ）] ページでも設定する必要があります。

9. 概要を確認し、 [完了] をクリックします。
10. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用してリソースをリストアする

リソースのバックアップをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップに関する情報を取得します。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

この例では、 2015 年 1 月 29 日から 2015 年 2 月 3 日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

1. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

カスタムプラグインリソースのリストア処理を監視する

Jobs ページを使用して、 SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします リストをフィルタリングして、リストア処理のみを表示します。
   b. 開始日と終了日を指定します。
   c. [* タイプ] ドロップダウン・リストから、 [リストア *] を選択します。
   d. [* Status *] ドロップダウン・リストから、リストア・ステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

   View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

カスタムプラグインリソースのバックアップをクローニングする

カスタムプラグインリソースのバックアップをクローニングする

クローニングワークフローには、クローニング処理の実行と処理の監視が含まれます。

- このタスクについて *

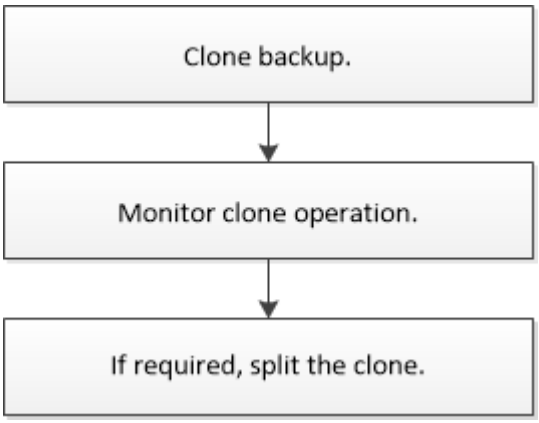
リソースのバックアップをクローニングする理由には次のものがあります。

- アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテン

ツを使用してテストするため

- データの抽出と操作を行うツールで、データウェアハウスにデータを取り込むため
- 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、 SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

バックアップからのクローニング

SnapCenter を使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。クローニング処理の機能は、使用するプラグインによって異なります。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- デフォルトのクローニング処理でクローニングされるのは、ストレージオブジェクトのみです。アプリケーションレベルのクローニング処理は、その機能がカスタムプラグインで提供されている場合にのみ実行できます。
- ボリュームをホストするアグリゲートが Storage Virtual Machine （ SVM ）に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、 **View**] ドロップダウンリストからリソースをフィルタリングします。

   リソースは、タイプ、ホストまたはクラスタ名、関連するリソースグループとポリシー、ステータスなどの情報とともに表示されます。
3. リソースまたはリソースグループを選択します。

リソースグループを選択する場合は、リソースを選択する必要があります。

リソースまたはリソースグループのトポロジページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。
5. 表からデータバックアップを選択し、をクリックします  。
6. [ロケーション] ページで、次の手順を実行します。

フィールド	手順
クローンサーバ	ソースホストがデフォルトで入力されています。 別のホストを指定する場合は、クローンのマウント先の、プラグインがインストールされたホストを選択します。
クローンのサフィックス	クローンデスティネーションがソースと同じ場合は必須です。 クローニングされた新しいリソース名に付けるサフィックスを入力します。サフィックスにより、クローニングされたリソースがホストで一意になります。 たとえば、 rs1_clone と指定します。元のリソースと同じホストにクローニングする場合、クローニングされたリソースを元のリソースと区別するためにサフィックスを指定する必要があります。これを行わないと処理は失敗します。

リソースとして LUN を選択し、セカンダリバックアップからクローニングする場合、デスティネーションボリュームのリストが表示されます。1 つのソースについて複数のデスティネーションボリュームを選択することができます。

7. [設定] ページで、次の手順を実行します。

フィールド	手順
イニシエータ名	IQDN または WWPN のホストイニシエータ名を入力します。
igroup プロトコル	igroup プロトコルを選択します。

設定ページは、ストレージタイプが LUN の場合にのみ表示されます。

8. Scripts ページで、クローン処理の前後に実行するプリクローンまたはポストクローン用のコマンドを入力します。ホストにファイルシステムをマウントするには、 mount コマンドを入力します。

例：

- クローニング前のコマンド：同じ名前の既存のデータベースを削除します
- クローニング後のコマンド：データベースの検証やデータベースの起動

  Linux マシンのボリュームまたは qtree に対する mount コマンド： mount<VSERVER_NAME> ： %<VOLUME_NAME_Clone /mnt>

9. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

   また、送信者と受信者の E メールアドレス、および E メールの件名を指定する必要があります。

10. 概要を確認し、 [完了] をクリックします。
11. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用してバックアップをクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

- 必要なもの *

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

PowerShell コマンドレットについては、 SnapCenter コマンドレットのヘルプを使用するか、を参照してください "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

- 手順 *

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

   ```
   Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Get-SmBackup コマンドレットまたは Get-SmResourceGroup コマンドレットを使用して、クローニングできるバックアップのリストを表示します。

   この例は、使用可能なすべてのバックアップに関する情報を表示します。

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
   1              Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                    Full Backup
   2              Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

この例では、指定したリソースグループに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup

    Description                 :
    CreationTime                : 10/10/2016 4:45:53 PM
    ModificationTime            : 10/10/2016 4:45:53 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               :
SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Completed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassCredential            : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
```

```
    IsInternal                    : False
    EnableEmailAttachment         : False
    VerificationSettings          : {}
    Name                          : NFS_DB
    Type                          : Group
    Id                            : 2
    Host                          :
    UserName                      :
    Passphrase                    :
    Deleted                       : False
    Auth                          : SMCoreContracts.SmAuth
    IsClone                       : False
    CloneLevel                    : 0
    Hosts                         :
    StorageName                   :
    ResourceGroupNames            :
    PolicyNames                   :

    Description                   :
    CreationTime                  : 10/10/2016 4:51:36 PM
    ModificationTime              : 10/10/2016 5:27:57 PM
    EnableEmail                   : False
    EmailSMTPServer               :
    EmailFrom                     :
    EmailTo                       :
    EmailSubject                  :
    EnableSysLog                  : False
    ProtectionGroupType           : Backup
    EnableAsupOnFailure           : False
    Policies                      : {}
    HostResourceMaping            : {}
    Configuration                 :
SMCoreContracts.SmCloneConfiguration
    LastBackupStatus              : Failed
    VerificationServer            :
    EmailBody                     :
    EmailNotificationPreference : Never
    VerificationServerInfo        :
    SchedulerSQLInstance          :
    CustomText                    :
    CustomSnapshotFormat          :
    SearchResources               : False
    ByPassRunAs                   : False
    IsCustomSnapshot              :
    MaintenanceStatus             : Production
    PluginProtectionGroupTypes    : {SMSQL}
```

```
    Tag                             :
    IsInternal                      : False
    EnableEmailAttachment           : False
    VerificationSettings            : {}
    Name                            : Test
    Type                            : Group
    Id                              : 3
    Host                            :
    UserName                        :
    Passphrase                      :
    Deleted                         : False
    Auth                            : SMCoreContracts.SmAuth
    IsClone                         : False
    CloneLevel                      : 0
    Hosts                           :
    StorageName                     :
    ResourceGroupNames              :
    PolicyNames                     :
```

3. New-SmClone コマンドレットを使用して、クローンリソースグループまたは既存のバックアップからクローニング処理を開始する。

   この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```
New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"}  -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

4. Get-SmCloneReport コマンドレットを使用して、クローニングジョブのステータスを表示します。

   この例では、指定したジョブ ID のクローンレポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

カスタムプラグインリソースのクローニング処理を監視する

Jobs ページを使用して、 SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。

3. Jobs （ジョブ）ページで、次の手順を実行します。
   a. をクリックします  をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
   b. 開始日と終了日を指定します。
   c. [**Type**](タイプ **)** ドロップダウンリストから **'[*Clone**](クローン *) を選択します
   d. [* Status *] ドロップダウン・リストから、クローンのステータスを選択します。
   e. [適用（ Apply ）] をクリックして、正常に完了した操作を表示する。
4. クローンジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

SnapCenter サーバとプラグインを管理します

ダッシュボードを表示します

ダッシュボードの概要

SnapCenter の左側のナビゲーションペインで、ダッシュボードを使用すると、最近のジョブアクティビティ、アラート、保護の概要、ストレージの効率性と使用状況、SnapCenter ジョブのステータス（バックアップ、クローン、リストア）、スタンドアロンおよび Windows クラスタホストの構成ステータスなど、システムの健全性を一目で把握できます。 SnapCenter で管理されている Storage Virtual Machine （ SVM ）の数とライセンス容量。

ダッシュボードビューに表示される情報は、 SnapCenter に現在ログインしているユーザに割り当てられたロールによって異なります。ユーザにその情報を表示する権限がない場合、一部のコンテンツが表示されないことがあります。

多くの場合、 * i * にカーソルを合わせると、ディスプレイに関する詳細情報を表示できます。状況によっては、リソース、モニタ、レポートなどの SnapCenter GUI ページの詳細なソース情報にダッシュボードの情報がリンクされていることがあります。

最近のジョブアクティビティ

[最近のジョブアクティビティ] タイルには、アクセス可能なバックアップ、リストア、クローンジョブの最新のジョブアクティビティが表示されます。この表示のジョブには、完了、警告、失敗、実行中、キューに登録済み、 キャンセルされました。

ジョブにカーソルを合わせると、詳細が表示されます。特定のジョブ番号をクリックすると、追加のジョブ情報が表示されます。これにより、 [モニタ] ページにリダイレクトされます。そこからジョブの詳細またはログ情報を取得し、そのジョブに固有のレポートを生成できます。

すべての SnapCenter ジョブの履歴を表示するには、 * すべて表示 * をクリックします。

アラート

アラートタイルには、ホストおよび SnapCenter サーバに関する最新の未解決の重大アラートと警告アラートが表示されます。

重大および警告カテゴリのアラートの総数が、ディスプレイの上部に表示されます。[Critical] または [Warning] の合計をクリックすると、 [Alerts] ページに特定のフィルタが適用された状態で [Alerts] ページにリダイレクトされます。

特定のアラートをクリックすると、そのアラートの詳細が [Alerts] ページに表示されます。ディスプレイの下部にある [**See All**](すべてを表示) をクリックすると、 [Alerts] ページにすべてのアラートのリストが表示されます。

最新の保護の概要

最新の保護サマリタイルには、アクセス可能なすべてのエンティティの保護ステータスが表示されます。デフ

ォルトでは、すべてのプラグインにステータスが表示されるように設定されています。ステータス情報は、プライマリストレージに Snapshot コピーとしてバックアップされたリソース、および SnapMirror テクノロジと SnapVault テクノロジを使用してセカンダリストレージに提供されます。セカンダリストレージの保護ステータス情報は、選択したプラグインタイプに基づいています。

ミラーバックアップ保護ポリシーを使用している場合は、 SnapMirror チャートではなく、保護の概要のカウンタが SnapVault の概要チャートに表示されます。

ドロップダウンメニューからプラグインを選択すると、個々のプラグインの保護ステータスを確認できます。ドーナツグラフには、選択したプラグインの保護されているリソースの割合が表示されます。ドーナツスライスをクリックすると、 **Reports**>*Plug-In * ページに移動します。このページには、指定されたプラグインのすべてのプライマリおよびセカンダリストレージアクティビティの詳細なレポートが表示されます。

セカンダリストレージに関するレポートは SnapVault のみに適用されます。 SnapMirror レポートはサポートされません。

SAP HANA は、 Snapshot コピーのプライマリストレージとセカンダリストレージの保護ステータス情報を提供します。ファイルベースのバックアップでは、プライマリストレージの保護ステータスのみを使用できます。

保護ステータス	プライマリストレージ	セカンダリストレージ
失敗しました	リソースグループに属しているエンティティの数。リソースグループでバックアップが実行されましたが、バックアップは失敗しました。	セカンダリデスティネーションへのバックアップの転送に失敗したエンティティの数。
成功しました	リソースグループが正常にバックアップされた、リソースグループ内のエンティティの数。	バックアップがセカンダリデスティネーションに正常に転送されたエンティティの数。
未設定	いずれのリソースグループにも属しておらず、バックアップされていないエンティティの数。	1 つ以上のリソースグループに属しており、セカンダリデスティネーションにバックアップを転送するように設定されていないエンティティの数。
開始されていません	リソースグループに属しているが、バックアップが実行されていないエンティティの数。	該当なし。

SnapCenter Server 4.2 以前のバージョンのプラグイン（ 4.2 より前）を使用してバックアップを作成している場合、最新の保護概要 * タイルには、これらのバックアップの SnapMirror 保護ステータスは表示されません。

ジョブ

Jobs タイルには、アクセス可能なバックアップ、リストア、およびクローニングのジョブの概要が表示され

ます。ドロップダウンメニューを使用して、レポートの期間をカスタマイズできます。期間のオプションは、過去 24 時間、過去 7 日間、および過去 30 日間で固定されます。デフォルトのレポートには、過去 7 日間に実行されたデータ保護ジョブが表示されます。

バックアップ、リストア、およびクローニングのジョブ情報がドーナツグラフに表示されます。ドーナツスライスをクリックすると、選択項目にあらかじめ適用されているジョブフィルタを含む [モニタ] ページに移動します。

ジョブステータス	説明
失敗しました	失敗したジョブの数。
警告	エラーが発生したジョブの数。
成功しました	正常に完了したジョブの数。
実行中です	現在実行中のジョブの数。

ストレージ

ストレージタイルには、 90 日間の保護ジョブで使用されるプライマリストレージとセカンダリストレージが表示され、消費傾向をグラフィカルに表示して、プライマリストレージの削減量を計算します。ストレージ情報は、 24 時間ごとに午前 12 時に更新されます

この日の合計消費量は、 SnapCenter で使用できるバックアップの合計数と、これらのバックアップが占有するサイズで構成され、画面の上部に表示されます。1 つのバックアップに複数の Snapshot コピーが関連付けられることがあり、その数は同じになります。これは、プライマリとセカンダリの両方の Snapshot コピーに当てはまります。たとえば、バックアップを 10 個作成し、そのうち 2 個はポリシーベースのバックアップ保持のために削除され、 1 個はユーザが明示的に削除するように設定したとします。したがって、この 7 つのバックアップが占有している数と 7 個のバックアップが表示されます。

プライマリストレージのストレージ削減率係数は、プライマリストレージの物理容量に対する論理容量（クローンと Snapshot コピーによる削減量とストレージ消費量）の比率です。棒グラフは、ストレージの削減量を示します。

このグラフには、連続した 90 日間におけるプライマリとセカンダリのストレージ消費量が 1 日単位で表示されます。グラフにカーソルを合わせると、詳細な日単位の結果が表示されます。

SnapCenter Server 4.2 以前のバージョンのプラグイン（ 4.2 より前）を使用してバックアップを作成する場合、「ストレージ」タイルには、バックアップ数、バックアップで消費されるストレージ容量、 Snapshot の削減量、クローンの削減量、および Snapshot のサイズは表示されません。

設定

[構成] タイルには、 SnapCenter が管理しているすべてのアクティブなスタンドアロンホストと Windows クラスタホストのステータス情報が統合されて表示され、にアクセスできます。これには、ホストに関連付けられているプラグインのステータス情報も含まれます。

Hosts （ホスト）の横にある数字をクリックすると、 Hosts （ホスト）ページの Managed Hosts （管理対象

ホスト）セクションにリダイレクトされます。このページから、選択したホストの詳細情報を取得できます。

さらに、 SnapCenter で管理しているスタンドアロンの ONTAP ONTAP とクラスタ SVM の合計と、アクセス権があることが表示されます。SVM の横にある番号をクリックすると、ストレージシステムのページに移動します。このページから、選択した SVM の詳細情報を取得できます。

ホストの構成状態は、それぞれの状態のホストの数に加えて、赤（重大）、黄（警告）、緑（アクティブ）で表示されます。ステータスメッセージは各状態について表示されます。

設定ステータス	説明
アップグレードは必須です	サポートされていないプラグインを実行していてアップグレードが必要なホストの数。サポートされていないプラグインは、このバージョンの SnapCenter と互換性がありません。
移行は必須です	サポート対象外のプラグインを実行し、移行が必要なホストの数。サポートされていないプラグインは、このバージョンの SnapCenter と互換性がありません。
プラグインがインストールされていません	正常に追加されたがプラグインのインストールが必要なホストの数、またはプラグインのインストールが失敗したホストの数。
中断しました	スケジュールが一時停止されている、かつメンテナンス中のホストの数。
停止しました	稼働しているホストのうち、プラグインサービスが実行されていないホストの数。
ホストが停止しています	停止しているか到達できないホストの数。
アップグレード可能（オプション）	新しいバージョンのプラグインパッケージをアップグレードに使用できるホストの数。
移行を利用可能（オプション）	新しいバージョンのプラグインを移行可能なホストの数。
ログディレクトリを設定します	SCSQL がトランザクションログバックアップを実行するようにログディレクトリを設定する必要があるホストの数。
VMware プラグインを設定	SnapCenter Plug-in for VMware vSphere を追加する必要のあるホストの数。
不明です	登録されているがインストールがまだトリガーされていないホストの数。

設定ステータス	説明
実行中です	稼働しているホストおよびプラグインの数。また、SCSQL プラグインの場合は、ログディレクトリとハイパーバイザーが設定されます。
プラグインのインストール / アンインストール	プラグインのインストールまたはアンインストールを実行中のホストの数。

ライセンス容量

Licensed Capacity タイルには、 SnapCenter の標準容量ベースのライセンスの合計ライセンス容量、使用済み容量、容量しきい値アラート、およびライセンスの有効期限に関する情報が表示されます。

この画面が表示されるのは、 Cloud Volumes ONTAP または ONTAP Select プラットフォームで SnapCenter の容量ベースのライセンスを使用している場合のみです。FAS プラットフォームまたは AFF プラットフォームの場合、 SnapCenter ライセンスはコントローラベースであり、容量無制限のライセンスです。容量ライセンスは必要ありません。

ライセンスステータス	説明
使用中	現在使用中の容量。
通知	容量のしきい値。ダッシュボードに通知が表示され、設定している場合は E メール通知が送信されます。
使用許諾	ライセンスに設定されている容量。
オーバー	ライセンスの容量を超えた容量。

ダッシュボードに情報を表示する方法

SnapCenter の左側のナビゲーションペインでは、ダッシュボードの各種タイルや、関連するシステムの詳細を表示できます。ダッシュボードに表示される表示数は固定で、変更することはできません。各画面に表示される内容は、 Role-Based Access Control （ RBAC ；ロールベースアクセス制御）によって異なります。

- 手順 *

1. 左側のナビゲーションペインで、 * ダッシュボード * をクリックします。
2. 各ディスプレイのアクティブな領域をクリックすると、追加情報が表示されます。

   たとえば、 * ジョブ * でドーナツグラフをクリックすると、選択の詳細がモニタページに表示されます。[保護の概要] でドーナツグラフをクリックすると、 [レポート] ページに移動します。このページには、選択に関する詳細情報が表示されます。

ダッシュボードからジョブのステータスレポートを要求します

バックアップ、リストア、およびクローニングのジョブに関するレポートは、ダッシュボードページで要求できます。これは、 SnapCenter 環境で成功または失敗したジョブの総数を確認する場合に便利です。

- 手順 *

1. 左側のナビゲーションペインで、 * ダッシュボード * をクリックします
2. ダッシュボードで [ジョブ] タイルを見つけ、 [* バックアップ *] 、 [* リストア *] 、または [* クローン *] を選択します。
3. プルダウンメニューを使用して、ジョブ情報を表示する期間（ 24 時間、 7 日間、または 30 日間）を選択します。

   システムには、データをカバーするドーナツグラフが表示されます。

4. レポートを作成するジョブ情報を表すドーナツスライスをクリックします。

   ドーナツグラフをクリックすると、ダッシュボードページからモニタページにリダイレクトされます。[モニタ] ページには、ドーナツグラフから選択したステータスのジョブが表示されます。

5. [モニタ] ページリストで、特定のジョブをクリックして選択します。
6. [モニター] ページの上部で、 [* レポート *] をクリックします。

- 結果 *

レポートには、選択したジョブの情報のみが表示されます。レポートは、確認するか、ローカルシステムにダウンロードできます。

ダッシュボードから保護ステータスのレポートを要求します

ダッシュボードを使用して、特定のプラグインで管理されるリソースの保護の詳細を要求できます。データ保護の概要には、データバックアップのみが表示されます。

- 手順 *

1. 左側のナビゲーションペインで、 * ダッシュボード * をクリックします。
2. Dashboard で最新の Protection Summary タイルを見つけ、プルダウンメニューを使用してプラグインを選択します。

   ダッシュボードには、プライマリストレージにバックアップされているリソースのドーナツグラフと、プラグインに該当する場合はセカンダリストレージにバックアップされているリソースのドーナツグラフが表示されます。

   > ⓘ データ保護レポートは、特定のプラグインタイプにのみ使用できます。すべてのプラグイン * を指定することはできません。

3. レポートを表示するステータスを表すドーナツスライスをクリックします。

   ドーナツグラフをクリックすると、ダッシュボードページからレポート、およびプラグインページに

リダイレクトされます。レポートには、選択したプラグインのステータスのみが表示されます。レポートは、確認するか、ローカルシステムにダウンロードできます。

SnapMirror ドーナツグラフおよびファイルベースの SAP HANA バックアップのレポートページへのリダイレクトはサポートされていません。

RBACの管理

SnapCenter では、ロール、ユーザ、およびグループを変更できます。

ロールを変更します

SnapCenter ロールを変更して、ユーザまたはグループを削除したり、そのロールに関連付けられている権限を変更したりできます。ロールの変更は、ロール全体で使用される権限を変更または削除する場合に特に便利です。

- 必要なもの *

「 SnapCenterAdmin 」ロールでログインする必要があります。

SnapCenterAdmin ロールの権限は変更または削除できません。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. 設定ページで、 * 役割 * をクリックします。
3. [役割名] フィールドで、変更する役割をクリックします。
4. [役割の詳細] ページで、権限を変更するか、必要に応じてメンバーの割り当てを解除します。
5. このロールのすべてのメンバーは、他のメンバーのオブジェクトを表示できます * を選択すると、そのロールの他のメンバーは、リソースリストの更新後にボリュームやホストなどのリソースを参照できます。

   他のメンバーが割り当てられているオブジェクトをこのロールのメンバーに表示しない場合は、このオプションを選択解除します。

   このオプションを有効にすると、オブジェクトまたはリソースを作成したユーザと同じロールにユーザが属している場合に、オブジェクトまたはリソースへのアクセスをユーザに割り当てる必要がなくなります。

1. [Submit （送信）] をクリックします。

ユーザとグループを変更します

SnapCenter のユーザまたはグループを変更して、ロールとアセットを変更できます。

- 必要なもの *

SnapCenter 管理者としてログインする必要があります。

- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. [設定] ページで、 [* ユーザーとアクセス *] をクリックします。
  3. [ユーザ名またはグループ名] リストで、変更するユーザまたはグループをクリックします。
  4. [ユーザーまたはグループの詳細] ページで、役割とアセットを変更します。
  5. [Submit （送信）] をクリックします。

ホストを管理します

ホストを追加して、 SnapCenter プラグインパッケージをインストールしたり、検証サーバを追加したり、ホストを削除したり、バックアップジョブを移行したり、ホストを更新してプラグインパッケージをアップグレードしたりすることができます。使用するプラグインに応じて、ディスクのプロビジョニング、 SMB 共有の管理、イニシエータグループ（ igroup ）の管理、 iSCSI セッションの管理、データの移行も可能です。

実行できるタスク	**Microsoft Exchange Server** の場合	**Microsoft SQL Server** の場合	（ **Microsoft Windows** の場合）	**for Oracle Database** の略	**for SAP HANA Database** の略	**Custom Plug-ins** の場合
ホストを追加してプラグインパッケージをインストールする	はい。	はい。	はい。	はい。	はい。	はい。
ホストの ESXi 情報を更新します	いいえ	はい。	いいえ	いいえ	いいえ	いいえ
スケジュールを一時停止し、ホストをメンテナンスモードにします	はい。	はい。	はい。	はい。	はい。	はい。
プラグインを追加、アップグレード、削除して、ホストを変更する	はい。	はい。	はい。	はい。	はい。	はい。

実行できるタスク	Microsoft Exchange Server の場合	Microsoft SQL Server の場合	（Microsoft Windows の場合）	for Oracle Database の略	for SAP HANA Database の略	Custom Plug-ins の場合
SnapCenter からホストを削除します	はい。	はい。	はい。	はい。	はい。	はい。
プラグインサービスを開始する	はい。	はい。	はい。	はい。	はい。	はい。
ディスクをプロビジョニング	いいえ	いいえ	はい。	いいえ	いいえ	いいえ
SMB 共有を管理します	いいえ	いいえ	はい。	いいえ	いいえ	いいえ
igroup を管理します	いいえ	いいえ	はい。	いいえ	いいえ	いいえ
iSCSI セッションを管理します	いいえ	いいえ	はい。	いいえ	いいえ	

仮想マシン情報を更新します

VMware vCenter のクレデンシャルに変更があった場合、またはデータベースまたはファイルシステムホストが再起動した場合は、仮想マシン情報を更新する必要があります。SnapCenter で仮想マシン情報を更新すると、 VMware vSphere vCenter との通信が開始され、 vCenter クレデンシャルが取得されます。

RDM ベースのディスクは、データベースホストにインストールされた SnapCenter Plug-in for Microsoft Windows で管理されます。RDM を管理するために、 SnapCenter Plug-in for Microsoft Windows は、データベースホストを管理する vCenter Server と通信します。

- 手順 *
  1. SnapCenter の左ナビゲーションペインで、 * Hosts * をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. [Managed Hosts] ページで、更新するホストを選択します。
  4. [* VM の更新 *] をクリックします。

プラグインホストを変更します

プラグインのインストール後に、必要に応じてプラグインホストの詳細を変更できます。SnapCenter Plug-in for Microsoft SQL Server 、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント

）、およびプラグインポートのクレデンシャル、インストールパス、プラグイン、ログディレクトリの詳細を変更できます。

プラグインのバージョンが SnapCenter サーバのバージョンと同じであることを確認します。

- このタスクについて *
- プラグインポートを変更できるのは、プラグインのインストール後です。

  アップグレード処理の実行中は、プラグインポートを変更できません。

- プラグインポートを変更する際には、次のポートのロールバックシナリオに注意する必要があります。
  - スタンドアロンセットアップでは、 SnapCenter がいずれかのコンポーネントのポート変更に失敗した場合、処理は失敗し、すべてのコンポーネントで古いポートが保持されます。

    すべてのコンポーネントでポートが変更されたものの、いずれかのコンポーネントが新しいポートでの起動に失敗した場合、すべてのコンポーネントで古いポートが保持されます。たとえば、スタンドアロンホスト上の 2 つのプラグインのポートを変更しようとして、 SnapCenter がどちらかのプラグインに新しいポートを適用できなかった場合、処理は失敗し（該当するエラーメッセージが表示される）、両方のプラグインで古いポートが保持されます。

  - クラスタセットアップでは、 SnapCenter がいずれかのノードにインストールされているプラグインのポート変更に失敗した場合、処理は失敗し、すべてのノードで古いポートが保持されます。

    たとえば、クラスタセットアップの 4 つのノードにプラグインがインストールされていて、いずれか 1 つのノードでポートが変更されなかった場合、すべてのノードで古いポートが保持されます。

GMSA と一緒にプラグインをインストールした場合、 * その他のオプション * ウィンドウで変更できます。GMSA をインストールせずにプラグインをインストールする場合、 GMSA アカウントを指定してプラグインサービスアカウントとして使用できます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. 上部で [Managed Hosts] が選択されていることを確認します。
  3. 変更するホストを選択し、任意のフィールドを変更します。

     一度に変更できるフィールドは 1 つだけです。

  4. [Submit （送信）] をクリックします。
- 結果 *

ホストが検証され、 SnapCenter サーバに追加されます。

プラグインサービスを開始または再起動します

SnapCenter プラグインサービスを開始すると、サービスが実行されていない場合は開始し、サービスが実行されている場合は再起動することができます。サービスの再起動は、メンテナンスの実行後などに必要になることがあります。

サービスの再開時にジョブが実行されていないことを確認してください。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
3. [Managed Hosts] ページで、開始するホストを選択します。
4. をクリックします アイコンをクリックし、 [サービスの開始] または [サービスの再起動] をクリックします。

   複数のホストのサービスを同時に開始または再開できます。

ホストメンテナンスのスケジュールを一時停止します

ホストで SnapCenter のスケジュールされたジョブの実行を停止するには、ホストをメンテナンスモードにします。この処理は、プラグインをアップグレードする前、またはホストでメンテナンス作業を行う場合に実行してください。

SnapCenter がそのホストと通信できないため、停止しているホストではスケジュールを一時停止できません。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
3. [Managed Hosts] ページで、サスペンドするホストを選択します。
4. をクリックします アイコンをクリックし、 * スケジュールの一時停止 * をクリックして、このプラグインのホストをメンテナンスモードにします。

   複数のホストのスケジュールを同時に一時停止することができます。

   最初にプラグインサービスを停止する必要はありません。プラグインサービスの状態は running または stopped のいずれかになります。

- 結果 *

ホストでスケジュールを一時停止すると、ホストの [全般的なステータス] フィールドに [Managed Hosts] ページに [*suspended] と表示されます。

ホストのメンテナンスが完了したら、 * スケジュールのアクティブ化 * をクリックして、ホストのメンテナンスモードを解除できます。
複数のホストのスケジュールを同時にアクティブ化できます。

Resources ページでサポートされている操作

リソースの検出とデータ保護処理の実行については、のリソースページを参照してください。実行できる処理は、リソースの管理に使用するプラグインによって異なります。

Resources ページでは、次のタスクを実行できます。

実行できるタスク	**Microsoft Exchange Server** の場合	**Microsoft SQL Server** の場合	（ **Microsoft Windows** の場合）	**for Oracle Database** の略	**for SAP HANA Database** の略	**Custom Plug-ins** の場合
バックアップに使用できるリソースがあるかどうかを確認する	はい。	はい。	はい。	はい。	はい。	はい。
リソースのオンデマンドバックアップを実行する	はい。	はい。	はい。	はい。	はい。	はい。
バックアップからリストアします	はい。	はい。	はい。	はい。	はい。	はい。
バックアップをクローニングする	いいえ	はい。	はい。	はい。	はい。	はい。
バックアップを管理します	はい。	はい。	はい。	はい。	はい。	はい。
クローンを管理します	いいえ	はい。	はい。	はい。	はい。	はい。
ポリシーを管理する	はい。	はい。	はい。	はい。	はい。	はい。
ストレージ接続を管理する	はい。	はい。	はい。	はい。	はい。	はい。
バックアップをマウントします	いいえ	いいえ	いいえ	はい。	いいえ	いいえ
バックアップをアンマウント	いいえ	いいえ	いいえ	はい。	いいえ	いいえ
詳細を表示します	はい。	はい。	はい。	はい。	はい。	はい。

ポリシーを管理する

リソースまたはリソースグループからポリシーの適用を解除したり、ポリシーの変更、削除、表示、コピーを行ったりすることができます。

ポリシーを変更する

リソースまたはリソースグループにポリシーが適用されている場合は、レプリケーションのオプション、Snapshot コピーの保持の設定、エラーの再試行回数、またはスクリプトの情報を変更できます。スケジュールタイプ（頻度）は、ポリシーを適用解除しないと変更できません。

- このタスクについて *

SnapCenter サーバでは、リソースまたはリソースグループにポリシーが適用されるときにのみスケジュールタイプが登録されるため、ポリシーのスケジュールタイプを変更するには追加の手順が必要です。

状況	作業
新しいスケジュールタイプを追加します	新しいポリシーを作成し、必要なリソースまたはリソースグループに適用します。 たとえば、リソースグループポリシーで毎時バックアップのみが指定されている場合に、日次バックアップの追加が必要となったときは、日次スケジュールタイプを設定したポリシーを作成してリソースグループに追加できます。リソースグループには、「 hourly 」と「 daily 」の 2 つのポリシーが設定されます。
スケジュールタイプを削除または変更	次の手順を実行します。 1. そのポリシーを使用するすべてのリソースとリソースグループからポリシーを適用解除します。 2. スケジュールタイプを変更 3. すべてのリソースとリソースグループにポリシーを適用し直します。 たとえば、ポリシーで毎時バックアップが指定されている場合に、これを日次バックアップに変更するには、まずポリシーを適用解除する必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. ポリシーを選択し、 * 変更 * をクリックします。
4. 情報を変更して、 [完了] をクリックします。

ポリシーを適用解除

リソースのデータ保護を管理するポリシーが不要となった場合は、リソースまたはリソースグループからいつでもポリシーの適用を解除できます。ポリシーを削除する場合やスケジュールタイプを変更する場合は、事前にポリシーの適用を解除する必要があります。

- 手順 *
  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。
  3. リソースグループを選択し、 * リソースグループの変更 * をクリックします。
  4. リソースグループの変更ウィザードのポリシーページで、ドロップダウンリストから、適用解除するポリシーの横にあるチェックマークをオフにします。
  5. ウィザードの残りの部分でリソースグループに追加の変更を加えてから、 [完了] をクリックします。

ポリシーを削除する

不要になったポリシーは削除することができます。

- 必要なもの *

ポリシーがいずれかのリソースまたはリソースグループに関連付けられている場合は、リソースまたはリソースグループからポリシーの適用を解除する必要があります。

- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. [設定] ページで、 [* ポリシー *] をクリックします。
  3. ポリシーを選択し、 * 削除 * をクリックします。
  4. 「 * はい * 」をクリックします。

リソースグループの管理

リソースグループに対してさまざまな処理を実行できます。

リソースグループに関連して次のタスクを実行できます。

- リソースグループを変更するには、リソースグループを選択し、 * リソースグループの変更 * をクリックして、リソースグループの作成時に指定した情報を編集します。

  リソースグループを変更する際にスケジュールを変更することができます。ただし、スケジュールタイプを変更するには、ポリシーを変更する必要があります。

  リソースグループからリソースを削除した場合、リソースグループに現在適用されているポリシーに定義されたバックアップ保持の設定は、削除したリソースに引き続き適用されます。

- リソースグループのバックアップを作成する。
- バックアップのクローンを作成します。

  クローニングは、 SQL 、 Oracle 、 Windows の各ファイルシステムのバックアップ、カスタムアプリケーションのバックアップ、および SAP HANA データベースのリソースまたはリソースグループのバックアップから実行できます。

- リソースグループのクローンを作成する。

  この処理は、 SQL リソースグループ（データベースのみを含むグループ）でのみサポートされます。リソースグループのクローニングのスケジュール（クローニングライフサイクル）を設定することができます。

- リソースグループでスケジュールされている処理が開始されないようにする。
- リソースグループを削除する。

リソースグループに対する処理を停止および再開する

スケジュールされた処理を一時的に無効にして、リソースグループで開始されないように設定できます必要に応じて、あとからこれらの処理を有効にすることができます。

- 手順 *

  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。
  3. リソースグループを選択し、 * Maintenance * （メンテナンス）をクリックします。
  4. [OK] をクリックします。

保守モードにしたリソースグループの操作を再開する場合は ' リソースグループを選択して ' 本番環境をクリックします

リソースグループを削除する

リソースグループ内のリソースを保護する必要がなくなった場合は、リソースグループを削除することができます。SnapCenter からプラグインを削除する前に、リソースグループを削除する必要があります。

- このタスクについて *

リソースグループ内のリソースに対して作成されたすべてのクローンを手動で削除する必要があります。必要に応じて、リソースグループに関連付けられているすべてのバックアップ、メタデータ、ポリシー、Snapshot コピーを強制的に削除することができます。

- 手順 *

  1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
  2. [リソース] ページで、 [* 表示] リストから [* リソースグループ *] を選択します。
  3. リソースグループを選択し、 * 削除 * をクリックします。

4. オプション：リソースグループに関連付けられたバックアップ、メタデータ、ポリシー、 Snapshot コピーをすべて削除するには、 * このリソースグループに関連付けられたバックアップとバックアップポリシーの削除 * チェックボックスを選択します。
5. [OK] をクリックします。

バックアップを管理します

バックアップは、名前変更および削除することができます。複数のバックアップを同時に削除することもできます。

バックアップの名前を変更する

検索を簡単にするために、バックアップの名前を変更できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リストからリソースまたはリソースグループを選択します。

   リソースまたはリソースグループのトポロジページが表示されます。リソースまたはリソースグループがデータ保護用に設定されていない場合は、トポロジページの代わりに Protect （保護）ウィザードが表示されます。

4. [コピーの管理] ビューで、プライマリ・ストレージ・システムから [* バックアップ] を選択します。

   セカンダリストレージシステムにあるバックアップは名前を変更できません。

Oracle Recovery Manager （ RMAN ）を使用して Oracle データベースのバックアップをカタログ化した場合、そのカタログ化されたバックアップの名前は変更できません。

1. バックアップを選択し、をクリックします 。
2. [バックアップ名を * に変更] フィールドに新しい名前を入力し、 [OK] をクリックします。

バックアップを削除します

他のデータ保護処理に使用する必要がなくなったバックアップは、削除することができます。

- 必要なもの *

バックアップを削除する前に、関連付けられているクローンを削除しておく必要があります。

クローンリソースに関連付けられたバックアップは削除できません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リストからリソースまたはリソースグループを選択します。

   リソースまたはリソースグループのトポロジページが表示されます。
4. [コピーの管理] ビューで、プライマリ・ストレージ・システムから [* バックアップ] を選択します。

   セカンダリストレージシステム上のバックアップは削除できません。
5. バックアップを選択し、をクリックします 。

   SAP HANA データベースのバックアップを削除する場合は、バックアップに関連付けられている SAP HANA カタログも削除されます。

   最後の残りのバックアップを削除すると、関連付けられている HANA カタログのエントリを削除できなくなります。

1. [OK] をクリックします。

   SnapCenter に、対応するバックアップがストレージシステムに存在しない古いデータベースバックアップがある場合は、 remove-smbackup コマンドを使用して、これらの古いバックアップエントリをクリーンアップする必要があります。古いバックアップがカタログ化されている場合は、リカバリカタログデータベースからカタログ化が解除されます。

クローンを削除します。

不要になったクローンは削除できます。

- このタスクについて *

他のクローンのソースと同様に機能するクローンは削除できません。

たとえば、本番環境のデータベースが db1 の場合は、データベース clone1 が db1 のバックアップからクローニングされ、その後 Clone1 が保護されます。データベース clone2 は Clone1 のバックアップからクローニングされます。clone1 を削除するには、先に Clone2 を削除してから Clone1 を削除する必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リストからリソースまたはリソースグループを選択します。

   リソースまたはリソースグループのトポロジページが表示されます。

4. [コピーの管理] ビューで ' プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージ・システムから [クローン *] を選択します
5. クローンを選択し、をクリックします 。

   SAP HANA データベースのクローンを削除する場合は、クローンの削除ページで次の操作を実行します。

   a. 「 * Pre-clone delete * 」フィールドに、クローンを削除する前に実行するコマンドを入力します。
   b. Unmount * フィールドで、クローンを削除する前にクローンをアンマウントするコマンドを入力します。
6. [OK] をクリックします。

- 終了後 *

ファイルシステムが削除されない場合があります。次のコマンドを実行して、clone_delete_delayパラメータの値を増やす必要があります。`./sccli Set-SmConfigSettings`

clone_delete_delay パラメータでは、アプリケーションクローンの削除が完了してからファイルシステムの削除が開始されるまでに待機する秒数を指定します。

パラメータの値を変更したら、 SnapCenter Plug-in Loader （ SPL ）サービスを再起動します。

ジョブ、スケジュール、イベント、およびログを監視する

ジョブの進捗状況の監視、スケジュールされたジョブに関する情報の取得、およびイベントとログの確認は、 [監視] ページから実行できます。

ジョブを監視する

SnapCenter のバックアップ、クローニング、リストア、検証の各ジョブに関する情報を表示できます。開始日と終了日、ジョブのタイプ、リソースグループ、ポリシー、または SnapCenter プラグインに基づいて、表示される情報を絞り込むことができます。指定したジョブの詳細情報やログファイルを確認することもできます。

SnapMirror 処理と SnapVault 処理に関連するジョブも監視できます。

SnapCenter Admin ロールまたはその他のスーパーユーザロールが割り当てられている場合を除き、監視できるのは自分で作成したジョブと自分に関連するジョブだけです。

ジョブの監視に関連して次のタスクを実行できます。

- バックアップ、クローニング、リストア、検証の各処理を監視する。
- ジョブの詳細とレポートを表示します。
- スケジュールされたジョブを停止する。

スケジュールを監視

現在のスケジュールを表示して、処理の開始日時、前回の実行日時、および次回の実行日時を確認できます。処理が実行されるホストのほか、処理のリソースグループやポリシーに関する情報も確認できます。

- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* スケジュール *] をクリックします。
3. リソースグループとスケジュールタイプを選択します。
4. スケジュールされた処理のリストを表示します。

イベントを監視する

ユーザによるリソースグループの作成、システムによるアクティビティの開始、スケジュールされたバックアップの作成など、システム内の SnapCenter イベントのリストを表示できます。イベントを表示して、バックアップやリストアなどの処理が現在実行中であるかどうかを確認できます。

- このタスクについて *

[イベント] ページにすべてのジョブ情報が表示されます。たとえば ' バックアップ・ジョブが開始されると 'backup start' イベントが表示されますバックアップが完了すると ' backup complete イベントが表示されます

- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* イベント *] をクリックします。
3. （任意） [フィルタ] ボックスに、開始日または終了日、イベントのカテゴリ（バックアップ、リソースグループ、ポリシーなど）、および重大度レベルを入力し、 [適用 *] をクリックします。または、検索ボックスに文字を入力します。
4. イベントのリストを表示します。

ログを監視する

SnapCenter サーバログ、 SnapCenter ホストエージェントログ、およびプラグインログを表示およびダウンロードできます。ログを表示してトラブルシューティングに役立てることができます。

- このタスクについて *

フィルタを使用して、特定の重大度レベルのログだけを表示するように絞り込むことができます。

- デバッグ
- 情報
- 警告
- エラー
- 致命的

バックアップジョブが失敗した理由を特定する目的で、ジョブレベルのログを取得することもできます。ジョ

ブ・レベル・ログの場合は、 * Monitor * > * Jobs * オプションを使用します。

- 手順 *

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [ジョブ] ページでジョブを選択し、 [ログのダウンロード] をクリックします。

   ダウンロードされた zip 形式のフォルダには、ジョブログと一般的なログが含まれています。zip 形式のフォルダ名には、選択したジョブ ID とジョブタイプが含まれています。

3. [モニター] ページで、 [* ログ *] をクリックします。
4. ログタイプ、ホスト、およびインスタンスを選択します。

   ログタイプとして * plugin * を選択すると、ホストまたは SnapCenter プラグインを選択できます。ログタイプが * server * の場合、この処理は実行できません。

5. 特定のソース、メッセージ、またはログレベルでログをフィルタリングするには、列見出しにあるフィルタアイコンをクリックします。

   すべてのログを表示するには、として「* greater than or equal to *」を選択します `Debug` レベル。

6. [* 更新 *] をクリックします。
7. ログの一覧を確認します。
8. ログをダウンロードするには、 * Download * をクリックします。

   ダウンロードされた zip 形式のフォルダには、ジョブログと一般的なログが含まれています。zip 形式のフォルダ名には、選択したジョブ ID とジョブタイプが含まれています。

大規模な構成で最適なパフォーマンスを実現するには、 PowerShell コマンドレットを使用して、SnapCenter のログ設定を最小レベルに設定する必要があります。

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

フェイルオーバージョブの完了後に健常性や設定の情報にアクセスするには、コマンドレットを実行します `Get-SmRepositoryConfig`。

SnapCenter からジョブとログを削除します

バックアップ、リストア、クローニング、および検証の各ジョブとそのログを SnapCenter から削除できます。SnapCenter では、ジョブの成否にかかわらず、削除しないかぎりログは永久に保存されます。ジョブのログを削除することで、ストレージの空きを増やすことができます。

- このタスクについて *

実行中のジョブがないことを確認してください。
特定のジョブを削除するには、ジョブ ID を指定するか、指定した期間内にジョブを削除します。

ジョブを削除する際、ホストをメンテナンスモードにする必要はありません。

- 手順 *

1. PowerShell を起動します。
2. コマンドプロンプトで、次のように入力します。 `Open-SMConnection`
3. コマンドプロンプトで、次のように入力します。 `Remove-SmJobs`
4. 左側のナビゲーションペインで、 **Monitor** をクリックします。
5. [モニター] ページで、 [* ジョブ *] をクリックします。
6. [ジョブ] ページで、ジョブのステータスを確認します。

- 詳細はこちら *

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapCenter のレポート機能の概要

SnapCenter には、システムの健常性や処理の状況を監視および管理するためのさまざまなレポートオプションが用意されています。

レポートタイプ	説明
バックアップレポート	Backup Report には、 SnapCenter 環境のバックアップ状況に関する全体的なデータ、バックアップの成功率、および指定した期間に実行された各バックアップに関する情報が表示されます。バックアップが削除された場合、そのバックアップのステータス情報はレポートに表示されません。Backup Detail Report には、指定したバックアップジョブに関する詳細情報に加え、バックアップに成功したリソースと失敗したリソースの一覧が表示されます。
クローンレポート	Clone Report には、 SnapCenter 環境のクローニング状況に関する全体的なデータ、クローニングの成功率、および指定した期間に実行された各クローニングジョブに関する情報が表示されます。クローンが削除された場合、そのクローンのステータス情報はレポートに表示されません。Clone Detail Report には、指定したクローン、クローニングホスト、クローニングジョブタスクのステータスに関する詳細情報が表示されます。タスクが失敗した場合は、Clone Detail Report にその情報が表示されます。

レポートタイプ	説明
リストアレポート	Restore Report には、リストアジョブに関する全体的な情報が表示されます。Restore Detail Report には、指定したリストアジョブについて、ホスト名、バックアップ名、ジョブの開始日時と期間、個々のジョブタスクのステータスなどの詳細情報が表示されます。タスクが失敗した場合は、 Restore Detail Report にその情報が表示されます。
保護レポート	これらのレポートには、すべての SnapCenter プラグインインスタンスで管理されているリソースの保護の詳細が表示されます。このレポートには、すべてのプラグインインスタンスで管理されているリソースの保護の詳細が表示されます。概要、保護されていないリソースの詳細、レポート生成時にバックアップされなかったリソース、バックアップ処理が失敗したリソースグループのリソース、および SnapVault のステータスを確認できます。
スケジュールされたレポート	これらのレポートは、毎日、毎週、または毎月のように定期的に実行されるようにスケジュールされています。レポートは、指定した日時に自動的に生成され、レポートは電子メールを介して各ユーザーに送信されますスケジュールを有効化、無効化、変更、または削除できます。有効なスケジュールは、 [今すぐ実行] ボタンをクリックして、オンデマンドで実行できます。管理者は任意のスケジュールを実行できますが、生成されるレポートには、スケジュールを作成したユーザから割り当てられた権限に基づいてデータが含まれます。 Administrator 以外のユーザは、権限に基づいてスケジュールを表示または変更できます。このロールのすべてのメンバーが [ロールの追加] ページで [他のメンバーのオブジェクトを表示できる] オプションを選択すると、そのロールの他のメンバーは表示および変更できます。

レポートにアクセスする

SnapCenter のダッシュボードを使用すると、システムヘルスの概要を簡単に確認できます。ダッシュボードで詳細にドリルダウンできます。または、詳細レポートに直接アクセスすることもできます。

レポートには、次のいずれかの方法でアクセスできます。

- 左側のナビゲーションペインで、 * ダッシュボード * をクリックし、 * 前回の保護の概要 * 円グラフをクリックして、レポートページに詳細を表示します。
- 左側のナビゲーションペインで、 * Reports * をクリックします。

レポートをフィルタします

必要な情報や期間に応じて、パラメータの範囲に基づいてレポートデータをフィルタリングできます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Reports * をクリックします。
  2. パラメータービューが表示されていない場合は、レポートツールバーの * パラメーター領域の切り替え * アイコンをクリックします。
  3. レポートを実行する時間範囲を指定します。
     [+]
     終了日を省略すると、使用可能なすべての情報が取得されます。
  4. 次のいずれかの条件に基づいて、レポート情報をフィルタリングします。
     - リソースグループ
     - ホスト
     - ポリシー
     - リソース
     - ステータス
     - プラグイン名
  5. [適用（ Apply ）] をクリックします。

レポートをエクスポートまたは印刷します

SnapCenter レポートをエクスポートすると、さまざまな形式でレポートを表示できます。レポートを印刷することもできます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Reports * をクリックします。
  2. レポートツールバーで、次のいずれかを実行します。
     - プリント可能なレポートをプレビューするには、 * プリントプレビューの切り替え * アイコンをクリックします。
     - レポートを別の形式にエクスポートするには、 * Export * icon ドロップダウンリストから形式を選択します。
  3. レポートを印刷するには、 * 印刷 * アイコンをクリックします。
  4. 特定のレポートの概要を表示するには、レポートの該当するセクションまでスクロールします。

E メール通知に使用する SMTP サーバを設定します

データ保護ジョブのレポートを自分または他のユーザに送信するときに使用する SMTP サーバを指定できます。テスト E メールを送信して設定を確認することもできます。この設定は、 E メール通知を設定したすべての SnapCenter ジョブにグローバルに適用されます。

このオプションは、すべてのデータ保護ジョブレポートの送信に使用する SMTP サーバを設定します。ただし、特定のリソースに対する SnapCenter データ保護ジョブの更新情報を定期的に自分または他のユーザに送

信し、更新ステータスを監視できるようするには、リソースグループの作成時に SnapCenter レポートを E メールで送信するオプションを設定できます。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. 設定ページで、 * グローバル設定 * をクリックします。
3. SMTP サーバーを入力し、 * 保存 * をクリックします。
4. テスト用 E メールを送信するには、 E メールの送信元と送信先の E メールアドレスを入力し、件名を入力して、「 * 送信 * 」をクリックします。

レポートを **E** メールで送信するオプションを設定します

SnapCenter データ保護ジョブの更新情報を定期的に自分または他のユーザに送信し、更新ステータスを監視できるようするには、リソースグループの作成時に SnapCenter レポートを E メールで送信するオプションを設定します。

- 必要なもの *

SMTP サーバーは、 [設定] の [グローバル設定] ページで設定しておく必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. 表示するリソースのタイプを選択し、 * 新規リソースグループ * をクリックするか、既存のリソースグループを選択して * 変更 * をクリックし、既存のリソースグループの E メールレポートを設定します。
3. 新しいリソースグループウィザードの通知パネルで、レポートを常に受信するか、エラーが発生したか、またはエラーや警告を受信するかをプルダウンメニューから選択します。
4. E メールの送信元アドレス、 E メールの送信先アドレス、および E メールの件名を入力します。

SnapCenter サーバリポジトリを管理します

SnapCenter から実行される各種の処理に関する情報は、 SnapCenter サーバのデータベースリポジトリに格納されます。SnapCenter サーバをデータ損失から保護するには、リポジトリのバックアップを作成する必要があります。

SnapCenter サーバリポジトリは、 NSM データベースと呼ばれることもあります。

SnapCenter リポジトリを保護するための前提条件

SnapCenter リポジトリを保護するには、一定の前提条件を満たしている必要があります。

- Storage Virtual Machine （ SVM ）接続の管理

  ストレージクレデンシャルを設定する必要があります。

- ホストのプロビジョニング

SnapCenter リポジトリのホストに、ネットアップストレージディスクが少なくとも 1 つ必要です。SnapCenter リポジトリのホストにネットアップディスクがない場合は作成する必要があります。

ホストの追加、 SVM 接続のセットアップ、およびホストのプロビジョニングの詳細については、インストール手順を参照してください。

- iSCSI LUN または VMDK のプロビジョニング

ハイアベイラビリティ（ HA ）構成の場合は、いずれかの SnapCenter Server で iSCSI LUN または VMDK のいずれかをプロビジョニングできます。

SnapCenter リポジトリをバックアップします

SnapCenter サーバリポジトリをバックアップしておくと、データ損失からの保護に役立ちます。リポジトリは、 _Protect -SmRepository_cmdlet を実行してバックアップできます。

- このタスクについて *

_Protect -SmRepository_cmdlet では、次のタスクを実行します。

- リソースグループとポリシーを作成します
- SnapCenter リポジトリのバックアップスケジュールを作成します
- 手順 *
  1. PowerShell を起動します。
  2. SnapCenter サーバホストで、 _Open-SmConnection_cmdlet を使用してセッションを確立し、クレデンシャルを入力します。
  3. _Protect -SmRepository_cmdlet と必要なパラメータを使用して、リポジトリをバックアップします。

SnapCenter リポジトリのバックアップを表示する

SnapCenter サーバデータベースリポジトリのバックアップのリストを表示するには、 _Get-SmRepositoryBackups_cmdlet を実行します。

リポジトリのバックアップは、 _Protect -SmRepository_cmdlet で指定されたスケジュールに従って作成されます。

- 手順 *
  1. PowerShell を起動します。
  2. コマンドプロンプトで、次のコマンドレットを入力し、 SnapCenter サーバに接続するためのクレデンシャルを指定します。 *Open-SMConnection*
  3. Get-SmRepositoryBackups_cmdlet を使用して、使用可能な SnapCenter データベースのバックアップの一覧を表示します。

SnapCenter データベースリポジトリをリストアします

SnapCenter リポジトリをリストアするには、 _Restore-SmRepositoryBackup_cmdlet を実行します。

SnapCenter リポジトリをリストアする場合は、リストア処理中にリポジトリデータベースにアクセスできないため、実行中の他の SnapCenter 処理に影響します。

- 手順 *

1. PowerShell を起動します。
2. コマンドプロンプトで、次のコマンドレットを入力し、 SnapCenter サーバに接続するためのクレデンシャルを指定します。 *Open-SMConnection*
3. _Restore-SmRepositoryBackup_cmdlet を使用して、リポジトリのバックアップをリストアします。

   次のコマンドレットでは、 iSCSI LUN または VMDK にあるバックアップから SnapCenter MySQL データベースリポジトリをリストアします。

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName
   MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
   ```

   次のコマンドレットは、バックアップファイルが iSCSI LUN 内で誤って削除された場合に、 SnapCenter MySQL データベースをリストアします。VMDK の場合、 ONTAP Snapshot コピーからバックアップを手動でリストアします。

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

リポジトリのリストア処理の実行に使用されたバックアップは、リストア処理の実行後にリポジトリのバックアップを取得したときに表示されません。

SnapCenter リポジトリを移行する

SnapCenter サーバのデータベースリポジトリをデフォルトの場所から別のディスクに移行することができます。リポジトリの移行は、より多くのスペースを持つディスクに再配置する場合などに行います。

- 手順 *

1. Windows で MYSQL57 サービスを停止します。
2. MySQL のデータディレクトリを探します。

   通常、このデータディレクトリは C ： \ProgramData\MySQL\MySQL Server 5.7.\Data にあります。

3. MySQL のデータディレクトリを新しい場所（例： E ： \Data\nsm ）にコピーします。
4. 新しいディレクトリを右クリックし、 * プロパティ * > * セキュリティ * を選択して、ネットワークサービスローカルサーバーアカウントを新しいディレクトリに追加し、アカウントにフルコントロールを割り当てます。
5. 元のデータベースディレクトリの名前を変更します（例： NSM_COPY ）。
6. Windows のコマンドプロンプトで、 _mklink_command を使用してディレクトリのシンボリックリンクを作成します。

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
```

7. Windows で MYSQL57 サービスを開始します。
8. SnapCenter にログインしてリポジトリのエントリを確認するか、 MySQL ユーティリティにログインして新しいリポジトリに接続して、データベースの場所が正しく変更されたことを確認します。
9. 名前を変更した元のデータベースリポジトリディレクトリ（ NSM_COPY ）を削除します。

SnapCenter リポジトリのパスワードをリセットします

MySQL Server リポジトリデータベースのパスワードは、 SnapCenter 4.2 以降の SnapCenter Server のインストール時に自動的に生成されます。この自動生成されたパスワードは、 SnapCenter ユーザにはいかなる時点でも知られていません。リポジトリデータベースにアクセスする場合は、パスワードをリセットする必要があります。

- 必要なもの *

パスワードをリセットするには、 SnapCenter 管理者の権限が必要です。

- 手順 *

1. PowerShell を起動します。
2. コマンドプロンプトで、次のコマンドを入力し、 SnapCenter サーバに接続するためのクレデンシャルを指定します。 *Open-SMConnection*
3. リポジトリのパスワードをリセットします。 *Set-SmRepositoryPassword*

   次に、リポジトリのパスワードをリセットするコマンドを示します。

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

- 詳細はこちら *

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

信頼できないドメインのリソースを管理します

SnapCenter は、 Active Directory （ AD ）の信頼できるドメイン内のホストの管理に加えて、複数の AD の信頼されていないドメイン内のホストも管理します。信頼されていない AD ドメインを SnapCenter サーバに登録する必要があります。SnapCenter では、複数の信頼されていない AD ドメインのユーザとグループがサポートされます

SnapCenter サーバは、ドメインまたはワークグループ内のマシンにインストールできます。SnapCenter サーバをインストールするには、マシンがドメイン内にある場合はドメインのクレデンシャル、ワークグループ内にある場合はローカルの管理者クレデンシャルを指定する必要があります。

SnapCenter サーバに登録されていないドメインに属する Active Directory （ AD ）グループはサポートされていません。これらの AD グループを使用して SnapCenter ロールを作成できますが、 SnapCenter サーバへのログインが失敗し、次のエラーメッセージが表示されます。 The user are trying to login does not belong to any roles管理者に問い合わせてください。

信頼できないドメインを変更します

信頼されていないドメインを変更するのは、ドメインコントローラの IP アドレスまたは Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を更新する場合です。

- このタスクについて *

FQDN を変更すると、関連付けられているアセット（ホスト、ユーザ、およびグループ）が想定どおりに機能しなくなる場合があります。

信頼されていないドメインを変更するには、 SnapCenter ユーザインターフェイスまたは PowerShell コマンドレットを使用します。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. 設定ページで、 * グローバル設定 * をクリックします。
3. [グローバル設定] ページで、 [* ドメイン設定 *] をクリックします。
4. をクリックします  をクリックし、次の情報を指定します。

フィールド	手順
ドメイン FQDN	FQDN を指定し、 * resolve * をクリックします。
ドメインコントローラの IP アドレス	ドメイン FQDN を解決できない場合は、ドメインコントローラの IP アドレスを 1 つ以上指定します。

5. [OK] をクリックします。

信頼されていない **Active Directory** ドメインの登録を解除

ドメインに関連付けられたアセットを使用しないようにするには、信頼されていない Active Directory ドメインの登録を解除します。

- 必要なもの *

信頼されていないドメインに関連付けられているホスト、ユーザ、グループ、およびクレデンシャルを削除しておく必要があります。

- このタスクについて *
- ドメインを SnapCenter サーバから登録解除すると、そのドメインのユーザは SnapCenter サーバにアクセスできなくなります。
- 関連付けられているアセット（ホスト、ユーザ、およびグループ）がある場合、ドメインの登録を解除すると、アセットを操作できなくなります。
- 信頼されていないドメインの登録を解除するには、 SnapCenter ユーザインターフェイスまたは PowerShell コマンドレットを使用します。
- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. 設定ページで、 * グローバル設定 * をクリックします。
  3. [グローバル設定] ページで、 [* ドメイン設定 *] をクリックします。
  4. ドメインのリストから、登録を解除するドメインを選択します。
  5. をクリックします をクリックし、 * OK * をクリックします。

ストレージシステムを管理

ストレージシステムを追加したあとで、ストレージシステムの設定や接続を変更したり、ストレージシステムを削除したりできます。

ストレージシステム構成を変更する

ユーザ名、パスワード、プラットフォーム、ポート、プロトコルを変更する場合、 SnapCenter を使用してストレージシステムの設定を変更できます。 タイムアウト時間、優先 IP アドレス、またはメッセージングオプション。

- このタスクについて *

個々のユーザまたはグループのストレージ接続を変更できます。同じストレージシステムに対する権限を持つ 1 つ以上のグループに所属している場合は、ストレージ接続リストにストレージ接続名が複数回表示されます。ストレージシステムへの権限を持つ各グループに対して 1 回ずつ表示されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * ストレージシステム * をクリックします。
  2. Storage Systems （ストレージシステム）ページの * Type （タイプ） * ドロップダウンから、次のいずれかの操作を実行します。

選択するオプション	手順
ONTAP SVMs	追加されたすべての Storage Virtual Machine （ SVM ）を表示し、必要な SVM の設定を変更するには、次の手順を実行します。 a. ストレージ接続ページで、適切な SVM 名をクリックします。 b. 次のいずれかを実行します。 ◦ SVM がどのクラスタにも含まれていない場合は、ストレージシステムの変更ページで、ユーザ名、パスワード、 EMS および AutoSupport の設定、プラットフォーム、プロトコル、ポート、タイムアウト、 優先 IP アドレスを指定します。 ◦ SVM がクラスタの一部である場合は、ストレージシステムの変更ページで「 SVM の個別管理」を選択し、ユーザ名、パスワード、 EMS および AutoSupport の設定、プラットフォーム、プロトコル、ポート、タイムアウト、 優先 IP アドレスを指定します。 SVM を個別に管理できるように変更した場合は、クラスタから SVM を削除し、 * 再検出 * をクリックしてください。SVM が ONTAP クラスタに追加されます。 SnapCenter GUI でストレージシステムのパスワードが更新された場合、更新されたパスワードが SMCore に反映されないために、該当するプラグインまたはサーバホストの SMCore サービスを再起動する必要があります。この場合、バックアップジョブが誤ったクレデンシャルエラーで失敗します。

選択するオプション	手順
ONTAP クラスタ	追加されたすべてのクラスタを表示し、必要なクラスタ設定を変更するには、次の手順を実行します。 a. ストレージ接続ページで、クラスタ名をクリックします。 b. Modify Storage System ページで、 Username の横の編集アイコンをクリックして、ユーザ名とパスワードを変更します。 c. EMS と AutoSupport の設定を選択またはクリアします。 d. [* その他のオプション *] をクリックして、プラットフォーム、プロトコル、ポート、タイムアウト、優先 IP などの他の設定を変更します。

3. [Submit （送信）] をクリックします。

ストレージシステムを削除

SnapCenter を使用して、使用していないストレージシステムを削除できます。

- このタスクについて *

個々のユーザまたはグループのストレージ接続を削除できます。同じストレージシステムに対する権限を持つ 1 つ以上のグループに所属している場合は、ストレージシステム名がストレージ接続リストに複数回表示されます。ストレージシステムへの権限を持つ各グループに 1 回ずつ表示されます。

ストレージシステムを削除すると、そのストレージシステムで実行されているすべての処理が失敗します。

- 手順 *

1. 左側のナビゲーションペインで、 * ストレージシステム * をクリックします。
2. ストレージシステムページの * タイプドロップダウンから、 * ONTAP SVM * または * ONTAP クラスタ * のいずれかを選択します。
3. ストレージ接続ページで、 SVM の横にあるチェックボックスまたは削除するクラスタを選択します。

   クラスタに含まれる SVM は選択できません。

4. [削除（ Delete ）] をクリックします。
5. Delete Storage System Connection Settings （ストレージシステム接続設定の削除）ページで、 * OK * をクリックします。

ONTAP GUI を使用して ONTAP クラスタから SVM を削除した場合は、 SnapCenter GUI で * Rediscover* をクリックして SVM リストを更新します。

EMS データ収集を管理します

PowerShell コマンドレットを使用すると、 Event Management System （ EMS ；イベント管理システム）でのデータ収集をスケジュール設定および管理できます。EMS データ収集では、 SnapCenter サーバ、インストールされている SnapCenter プラグインパッケージ、ホストに関する情報などが収集され、指定した ONTAP Storage Virtual Machine （ SVM ）に送信されます。

データ収集タスクの実行中、システムの CPU 利用率が高くなります。CPU 利用率は、データサイズに関係なく処理が進行しているかぎり高くなります。

EMS データ収集を停止します

EMS データ収集は、デフォルトで有効になっており、インストールした日から 7 日ごとに実行されます。データ収集は、 PowerShell コマンドレットの *Disable -SmDataCollectionEMS* を使用していつでも無効にできます。

- 手順 *

1. PowerShell コマンドラインから「 *Open-SmConnection* 」と入力して、 SnapCenter とのセッションを確立します。
2. *Disable-SmDataCollectionEms* と入力して、 EMS データ収集を無効にします。

EMS データ収集を開始します

EMS データ収集はデフォルトで有効になっており、インストールした日から 7 日ごとに実行するようにスケジュールされています。無効にした場合は、 _Enable-SmDataCollectionEMS_cmdlet を使用して、 EMS データ収集を再開できます。

Data ONTAP event generate-autosupport-log 権限が Storage Virtual Machine （ SVM ）ユーザに付与されている必要があります。

- 手順 *

1. PowerShell コマンドラインから「 *Open-SmConnection* 」と入力して、 SnapCenter とのセッションを確立します。
2. EMS データ収集を有効にするには、「 *Enable -SmDataCollectionEMS* 」と入力します。

EMS データ収集のスケジュールとターゲット SVM を変更します

PowerShell コマンドレットを使用して、 EMS データ収集のスケジュールやターゲット Storage Virtual Machine （ SVM ）を変更することができます。

- 手順 *

1. PowerShell コマンドラインを使用して SnapCenter とのセッションを確立するには、 _Open-SmConnection_cmdlet を入力します。
2. EMS データ収集のターゲットを変更するには、 _Set-SmDataCollectionEmsTarget_cmdlet を入力します。
3. EMS データ収集のスケジュールを変更するには、 _Set-SmDataCollectionEmsSchedule_cmdlet を入力します。

EMS データ収集のステータスを監視します

いくつかの PowerShell コマンドレットを使用して、 EMS データ収集のステータスを監視できます。スケジュール、 Storage Virtual Machine （ SVM ）ターゲット、およびステータスに関する情報を取得できます。

- 手順 *
  1. PowerShell コマンドラインから「 *Open-SmConnection* 」と入力して、 SnapCenter とのセッションを確立します。
  2. *Get-SmDataCollectionEmsSchedule* と入力して、 EMS データ収集スケジュールに関する情報を取得します。
  3. *Get-SmDataCollectionEmsStatus* と入力して、 EMS データ収集のステータスに関する情報を取得します。
  4. *Get-SmDataCollectionEmsTarget* と入力して、 EMS データ収集ターゲットに関する情報を取得します。
- 詳細はこちら *

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapCenter サーバとプラグインをアップグレードします

利用可能なアップデートを確認するように SnapCenter を設定します

SnapCenter は、NetApp Support Siteと定期的に通信し、利用可能なソフトウェアアップデートがあればユーザに通知します。スケジュールを作成して、利用可能な更新に関する情報の受信間隔を指定することもできます。

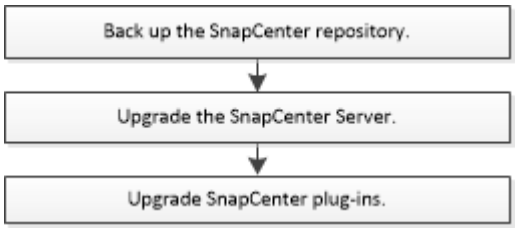
- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. [設定] ページで、 [* ソフトウェア] をクリックします。

     Available Software ページには、使用可能なプラグインパッケージ、使用可能なバージョン、およびインストールステータスが表示されます。
  3. [* アップデートの確認 *] をクリックして、新しいバージョンのプラグインパッケージが利用可能かどうかを確認します。
  4. [スケジュール更新] をクリックして、利用可能な更新に関する情報を受け取る間隔を指定するスケジュールを作成します。
     a. [更新の確認 *] で間隔を選択します。
     b. SnapCenter サーバ管理ウィンドウの資格情報を選択し、 * OK * をクリックします。

アップグレードワークフロー

SnapCenter の各リリースには、更新された SnapCenter Server およびプラグインパッケージが含まれています。プラグインパッケージの更新は、 SnapCenter インストーラで配布されます。利用可能なアップデートをチェックするように SnapCenter を設定できます。

このワークフローは、 SnapCenter サーバとプラグインパッケージのアップグレードに必要なさまざまなタスクを示しています。



サポートされているアップグレードパス

SnapCenter サーバのバージョン	SnapCenter サーバの直接アップグレード先	サポートされるプラグインのバージョン
4.5.x	4.6.x	• 4.5.x • 4.6.x
	4.7.	• 4.7.
4.6.x	4.7.	• 4.6.x • 4.7.
	4.8	• 4.8
4.7.	4.8	• 4.7. • 4.8

たとえば、SnapCenterバージョン4.5.xを使用していて、4.8にアップグレードする場合は、まず4.6.xにアップグレードしてから、4.8へのローリングアップグレードを実行する必要があります。

SnapCenter Plug-in for VMware vSphere のアップグレードについては、を参照してください "SnapCenter Plug-in for VMware vSphere をアップグレードします"。

SnapCenter サーバをアップグレードします

SnapCenter サーバインストーラの実行ファイルを使用して、 SnapCenter サーバをアップグレードできます。

- 必要なもの *
- SnapCenter サーバホストは、 Windows アップデートが適用された最新の状態である必要があります。システムの再起動が保留されることはありません。
- アップグレード処理を開始する前に、他の処理が実行されていないことを確認する必要があります。
- ジョブが実行されていないことを確認したら、 SnapCenter リポジトリ（ MySQL ）データベースをバックアップする必要があります。この方法は、 SnapCenter サーバおよび Exchange プラグインをアップグレードする前に推奨されます。

  詳細については、を参照してください "SnapCenter リポジトリをバックアップします"。

- SnapCenter サーバホストまたはプラグインホストで変更した SnapCenter 構成ファイルをすべてバックアップしておく必要があります。

  SnapCenter 構成ファイルの例： SnapDrive Service.exe.config 、 SMCoreServiceHost.exe.config など。

- このタスクについて *
- アップグレード中、ホストは自動的にメンテナンスモードになり、スケジュールされたジョブをホストが

実行できなくなります。アップグレード後、ホストは自動的にメンテナンスモードから解除されます。

- アップグレード時に、 NSM データベースの Exchange データを更新するために SQL スクリプトが実行されます。これにより、 DAG およびホストの短縮名が FQDN に変換されます。これは、 SnapCenter サーバと Exchange プラグインを使用している場合にのみ該当します。
- アップグレード操作を開始する前に、ホストを手動でメンテナンスモードにした場合は、アップグレード後に、 [**Hosts**>*Activate Schedule] をクリックして、ホストを手動でメンテナンスモードから解除する必要があります。
- SnapCenter Plug-in for Microsoft SQL Server、SnapCenter Plug-in for Microsoft Exchange Server、およびSnapCenter Plug-in for Microsoft Windowsの場合、サーバーとプラグインホストの両方を、scripts_pathを実行するために4.7バージョンにアップグレードすることをお勧めします。

  ポリシーでプリスクリプトとポストスクリプトが有効になっている既存のバックアップスケジュールと検証スケジュールについては、アップグレード後もバックアップ処理が続行されます。

  ［ジョブの詳細］ページで、スクリプトをscripts_pathにコピーし、ポリシーを編集してscripts_pathに対するパスを指定するように警告メッセージが表示されます。クローンライフサイクルジョブの場合、サブジョブレベルで警告メッセージが表示されます。

- 手順 *

1. NetApp Support Siteから SnapCenter サーバインストールパッケージをダウンロードします。

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. C ： \Program Files\NetApp\Virtual \SnapCenter WebApp にある Web.config のコピーを作成します。
3. Windows タスクスケジュールからプラグインホストに関連する SnapCenter スケジュールをエクスポートして、アップグレードが失敗した場合にプラグインホストを使用してスケジュールをリストアできるようにします。

   ```
   md d:\\SCBackup``schtasks /query /xml /TN taskname >>
   "D:\SCBackup\taskname.xml"
   ```

4. リポジトリのバックアップが設定されていない場合は、 SnapCenter MySQL データベースダンプを作成します。

   ```
   md d:\\SCBackup``mysqldump --all-databases --single-transaction --add-drop
   -database --triggers --routines --events -u root -p >
   D:\SCBackup\SCRepoBackup.dmp
   ```

   プロンプトが表示されたら、パスワードを入力します。

5. ダウンロードした .exe ファイルをダブルクリックして、 SnapCenter Server のアップグレードを開始します。

   アップグレードを開始すると、すべての事前確認が実行され、最小要件が満たされていない場合には、対応するエラーまたは警告メッセージが表示されます。警告メッセージは無視してインストールを続行できます。ただし、エラーは修正する必要があります。

   SnapCenter では、以前のバージョンの SnapCenter Server のインストール時に提供された既存の MySQL Server リポジトリデータベースのパスワードが引き続き使用されます。

6. [* アップグレード] をクリックします。

   どの段階でも、 **Cancel** ボタンをクリックすると、アップグレードワークフローがキャンセルされます。SnapCenter サーバを以前の状態にロールバックしません。

* ベストプラクティス： * SnapCenter からログアウトしてログインするか、新しいブラウザを開いて SnapCenter GUI にアクセスしてください。

- 終了後 *

- sudo ユーザを使用してプラグインをインストールした場合は、 *C ： \ProgramData\NetApp\SnapCenter \Package Repository\ORACLE_checksum.txt* にある sha224 キーをコピーして、 /etc/sudoers_file を更新します。
- ホスト上のリソースの新規検出を実行する必要があります。

  ホストのステータスが stopped と表示される場合は、しばらく待ってから新しい検出を実行できます。また、 **HostRefreshInterval** パラメータの値（デフォルト値は 3600 秒）を 10 分を超える任意の値に変更することもできます。

- アップグレードに失敗した場合は、失敗したインストールをクリーンアップし、以前のバージョンの SnapCenter を再インストールして、 NSM データベースを以前の状態にリストアする必要があります。
- SnapCenter サーバホストをアップグレードしたあと、ストレージシステムを追加する前にプラグインもアップグレードする必要があります。

プラグインパッケージをアップグレードします

プラグインパッケージは、 SnapCenter アップグレードの一環として配布されます。

アップグレード手順は 'Windows’Linux’AIX ホストをメンテナンスモードにしますこれにより ' ホストはスケジュールされたジョブを実行できなくなります

- 必要なもの *

- Linux マシンにアクセスできる root 以外のユーザの場合は、アップグレード操作を実行する前に、 _/etc/sudoers_file を最新のチェックサム値で更新する必要があります。
- デフォルトでは、 SnapCenter は環境から JAVA_HOME を検出します。修正された JAVA_HOME を使用する場合、 Linux ホストでプラグインをアップグレードする場合は、 /var/opt/snapcenter /spl/etc/_ にある *_spl.properties* ファイルに skip_JAVAHOME_update パラメータを手動で追加し、値を true に設定する必要があります。

  JAVA_HOME の値は、プラグインがアップグレードされるか、 SnapCenter Plug-in Loader （ SPL ）サービスが再起動されると更新されます。SPL をアップグレードまたは再起動する前に、 skip_JAVAHOME_update パラメータを追加して値を true に設定した場合、 JAVA_HOME の値は更新されません。

- SnapCenter サーバホストまたはプラグインホストで変更したすべての SnapCenter 構成ファイルをバックアップしておく必要があります。

  SnapCenter 構成ファイルの例： SnapDrive Service.exe.config 、 SMCoreServiceHost.exe.config など。

- このタスクについて *

- アップグレード手順は 'Windows’Linux’AIX ホストをメンテナンスモードにしますこれにより ' ホストはスケジュールされたジョブを実行できなくなります
- SnapCenter Plug-in for Microsoft SQL Server、SnapCenter Plug-in for Microsoft Exchange Server、およびSnapCenter Plug-in for Microsoft Windowsの場合、サーバとプラグインホストの両方を、scripts_pathを実行する最新バージョンにアップグレードすることを推奨します。

  ポリシーでプリスクリプトとポストスクリプトが有効になっている既存のバックアップスケジュールと検証スケジュールについては、アップグレード後もバックアップ処理が続行されます。

  ［ジョブの詳細］ページで、スクリプトをscripts_pathにコピーし、ポリシーを編集してscripts_pathに対するパスを指定するように警告メッセージが表示されます。クローンライフサイクルジョブの場合、サブジョブレベルで警告メッセージが表示されます。

- 手順 *

  1. 左側のナビゲーションペインで、 * Hosts * > * Managed Hosts * をクリックします。
  2. 次のいずれかの手順を実行して、ホストをアップグレードします。

     - いずれかのホストについて、 [Overall Status] 列に [Upgrade Available] と表示されている場合は、ホスト名をクリックして、次の手順を実行します。
       i. [* その他のオプション *] をクリックします。
       ii. ホストがプラグインのアップグレード要件を満たしているかどうかを検証しない場合は、「 * 事前確認をスキップ」を選択します。
       iii. [* アップグレード] をクリックします。
     - 複数のホストをアップグレードする場合は、すべてのホストを選択し、をクリックします をクリックし、 * アップグレード * > * OK * をクリックします。

       関連するすべてのサービスは、プラグインのアップグレード中に再開されます。

       パッケージ内のすべてのプラグインが選択されますが、以前のバージョンの SnapCenter でインストールされていたプラグインのみがアップグレードされ、残りのプラグインはインストールされません。新しいプラグインをインストールするには、 * Add plug-ins * オプションを使用する必要があります。

  [事前確認をスキップ] チェックボックスをオンにしていない場合、プラグインをインストールするための要件をホストが満たしているかどうかが検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。問題を修正したら、 [* アップグレード] をクリックします。

  エラーがディスクスペースまたは RAM に関連している場合は、 C ： \Program Files\NetApp\SnapManager WebApp にある Web.config ファイルまたは C ： \Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter にある PowerShell 構成ファイルを更新して、デフォルト値を変更できます。エラーがそれ以外のパラメータに関連している場合は、問題を修正してから要件を再度検証する必要があります。

SnapCenter Server とプラグインをアンインストールします

SnapCenter プラグインパッケージをアンインストールします

ホストを削除するための前提条件

SnapCenter GUI を使用して、ホストを削除し、個々のプラグインまたはプラグインパッケージをアンインストールできます。また、 SnapCenter Server ホストのコマンドラインインターフェイス（ CLI ）を使用するか、または任意のホストでローカルに Windows * プログラムのアンインストール * オプションを使用して、リモートホスト上の個々のプラグインまたはプラグインパッケージをアンインストールすることもできます。

SnapCenter サーバからホストを削除する前に、前提条件を完了しておく必要があります。

- 管理者としてログインする必要があります。
- SnapCenter Custom Plug-ins を使用している場合は、ホストに関連付けられている SnapCenter からすべてのクローンを削除する必要があります。
- ホストで検出ジョブが実行されていないことを確認する必要があります。
- ホストに関連付けられているすべてのオブジェクトを削除するために必要な権限を持つロールが割り当てられている必要があります。削除しないと、削除処理は失敗します。
- SnapCenter へのホストの追加後に SSH キーが変更された場合は、フィンガープリントを確認する必要があります。
- SnapCenter ホストが新しいバージョンの SnapCenter にアップグレードされ、プラグインホストで以前のバージョンのプラグインが実行されている場合は、フィンガープリントを確認する必要があります。

ロールベースアクセス制御を使用するホストを削除する場合の前提条件

- ホストの読み取りと削除、プラグインのインストールとアンインストール、およびオブジェクトの削除を行う権限を持つ RBAC ロールを使用してログインしておく必要があります。

  オブジェクトは、クローン、バックアップ、リソースグループ、ストレージシステムなどです。

- RBAC ロールに RBAC ユーザを追加しておく必要があります。
- 削除するホスト、プラグイン、クレデンシャル、リソースグループ、およびストレージシステム（クローンの場合）に RBAC ユーザを割り当てる必要があります。
- SnapCenter に RBAC ユーザとしてログインしておく必要があります。

クローンライフサイクル処理で作成されたクローンを含むホストを削除する場合の前提条件

- SQL データベースのクローンライフサイクル管理を使用してクローニングジョブを作成しておく必要があります。
- クローンの読み取りと削除、リソースの読み取りと削除、リソースグループの読み取りと削除、ストレー

ジの読み取りと削除、プロビジョニングの読み取りと削除、マウント、アンマウント、プラグインのインストールとアンインストール、およびホストの読み取りと削除を行う権限を持つ RBAC ロールを作成しておく必要があります。

- RBAC ロールに RBAC ユーザを割り当てておく必要があります。
- ホスト、 SnapCenter Plug-in for Microsoft SQL Server 、クレデンシャル、クローンライフサイクルリソースグループ、およびストレージシステムに RBAC ユーザを割り当てておく必要があります。
- SnapCenter に RBAC ユーザとしてログインしておく必要があります。

SnapCenter Plug-in for VMware vSphere のアンインストールについては、を参照してください "SnapCenter Plug-in for VMware vSphere を削除します"。

ホストを削除します

SnapCenter サーバはホストを削除すると、最初にそのホストに対してリストされているバックアップ、クローン、ジョブ、リソースグループ、およびリソースを SnapCenter のリソースページから削除したあと、ホスト上のプラグインパッケージをアンインストールします。

- このタスクについて *
- ホストを削除すると、そのホストに関連付けられているバックアップ、クローン、およびリソースグループも削除されます。
- リソースグループを削除すると、関連付けられているスケジュールもすべて削除されます。
- ホストに別のホストと共有されているリソースグループがある場合にそのホストを削除すると、リソースグループも削除されます。
- 運用停止されたプラグインホストまたは到達不能なプラグインホストを削除するには、 _Remove-SmHost_cmdlet を使用してください。

  コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

- ホストの削除にかかる時間は、バックアップの数と保持設定によって異なります。これは、各コントローラから Snapshot コピーが削除され、メタデータが消去されるためです。
- 手順 *

  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
  3. 削除するホストを選択し、 * Remove * をクリックします。
  4. Oracle RAC クラスタの場合、クラスタ内のすべてのホストから SnapCenter ソフトウェアを削除するには、 * クラスタのすべてのホストを含める * を選択します。

     クラスタの 1 つのノードを削除して、すべてのノードを 1 つずつ削除することもできます。

  5. [OK] をクリックします。

クラスタでホストプラグインをアンインストールして再インストールしても、クラスタリソースは自動的に検出されません。クラスタのホスト名を選択し、 * リソースの更新 * をクリックすると、クラスタ・リソースが自動的に検出されます。

SnapCenter GUI を使用してプラグインをアンインストールします

個々のプラグインまたはプラグインパッケージが不要になった場合は、 SnapCenter インターフェイスを使用してアンインストールできます。

- 必要なもの *
- アンインストールするプラグインパッケージのリソースグループを削除しておく必要があります。
- アンインストールするプラグインパッケージのリソースグループに関連付けられているポリシーを解除しておく必要があります。
- このタスクについて *

個々のプラグインをアンインストールできます。たとえば、あるホストのリソースが不足している場合に、そのプラグインをより強力なホストに移動するために、 SnapCenter Plug-in for Microsoft SQL Server のアンインストールが必要になることがあります。プラグインパッケージ全体をアンインストールすることもできます。たとえば、 SnapCenter Plug-in for Oracle Database と SnapCenter Plug-in for UNIX が含まれている Linux 用 SnapCenter Plug-ins Package のアンインストールが必要になることがあります。

- ホストの削除には、すべてのプラグインのアンインストールが含まれます。

  SnapCenter からホストを削除する場合、 SnapCenter はホストを削除する前にホスト上のすべてのプラグインパッケージをアンインストールします。

- SnapCenter GUI は、一度に 1 つのホストからプラグインを削除します。

  SnapCenter GUI を使用する場合、プラグインをアンインストールできるホストは一度に 1 つです。ただし、複数のアンインストール処理を同時に実行できます。

  また、 *Uninstall-sSmHostPackage* コマンドレットと必要なパラメータを使用して、複数のホストからプラグインをアンインストールすることもできます。コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapCenter Server がインストールされているホストから SnapCenter Plug-ins Package for Windows をアンインストールすると、 SnapCenter Server のインストールが破損します。SnapCenter Server が不要になったことが確実である場合を除き、 SnapCenter Plug-ins Package for Windows をアンインストールしないでください。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
3. Managed Hosts ページで、プラグインまたはプラグインパッケージをアンインストールするホストを選択します。

4. 削除するプラグインの横にある * 削除 * > * 送信 * をクリックします。

- 終了後 *

5 分待ってから、そのホストにプラグインを再インストールします。この時間は、 SnapCenter GUI が管理対象ホストのステータスを更新するのに十分です。プラグインをすぐに再インストールすると、のインストールが失敗します。

Linux 用の SnapCenter Plug-ins パッケージをアンインストールしている場合は、アンインストール固有のログファイルが _ / custom_location / snapcenter / log_ にあります。

PowerShell コマンドレットを使用して Windows プラグインをアンインストールします

SnapCenter サーバホストのコマンドラインインターフェイスで _Uninstall-SmHostPackage_cmdlet を使用すると、 1 つ以上のホストから個々のプラグインまたはプラグインパッケージをアンインストールできます。

プラグインをアンインストールする各ホストに対するローカル管理者権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenterサーバホストで、_Open-SMConnection-SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME_コマンドを入力し、クレデンシャルを入力します。
3. Uninstall -SmHostPackage_cmdlet と、必要なパラメータを使用して、 Windows プラグインをアンインストールします。

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

プラグインをホスト上でローカルにアンインストールします

SnapCenter サーバからホストにアクセスできない場合は、ホスト上でローカルに SnapCenter プラグインをアンインストールできます。

- このタスクについて *

個々のプラグインまたはプラグインパッケージをアンインストールする際のベストプラクティスは、 SnapCenter Server ホストのコマンドラインインターフェイスで SnapCenter GUI を使用するか、 Uninstall-SmHostPackage コマンドレットを使用することです。これらの手順を使用すると、 SnapCenter サーバは変更を反映して最新の状態に保たれます。

ただしまれに、プラグインをローカルにアンインストールしなければならない場合があります。たとえば、 SnapCenter サーバからアンインストールジョブを実行したにもかかわらずジョブが失敗した場合や、 SnapCenter サーバをアンインストールしてプラグインだけがホストに残った場合などです。

ホスト上でローカルにプラグインパッケージをアンインストールしても、スケジュールされたジョブやバックアップメタデータなど、ホストに関連付けられているデータは削除されません。

SnapCenter Plug-ins Package for Windows は、コントロールパネルからローカルにアンインストールしないでください。SnapCenter GUI を使用して、 SnapCenter Plug-in for Microsoft Windows が正しくアンインストールされていることを確認する必要があります。

- 手順 *

1. ホストシステムで、 [コントロールパネル] に移動し、 [プログラムのアンインストール] をクリックします。
2. プログラムのリストで、アンインストールする SnapCenter プラグインまたはプラグインパッケージを選択し、 [アンインストール] をクリックします。

   選択したパッケージ内のすべてのプラグインがアンインストールされます。

CLI を使用して、 Linux または AIX 用のプラグインパッケージをアンインストールします

コマンドラインインターフェイスを使用して、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をアンインストールできます。

- 必要なもの *
- スケジュール済みのジョブが削除されていることを確認します
- 実行中のジョブがすべて完了していることを確認します。
- ステップ *

Run _ /custom_location / netapp / snapcenter / spl / installation /plugins/uninstall_ to uninstall.

SnapCenter サーバをアンインストールします

データ保護ジョブの管理に SnapCenter サーバを使用しない場合は、 SnapCenter サーバホストの [プログラムと機能] コントロールパネルを使用して SnapCenter サーバをアンインストールできます。SnapCenter サーバをアンインストールすると、そのコンポーネントがすべて削除されます。

- 必要なもの *
- SnapCenter サーバがインストールされているドライブに、少なくとも 2 GB の空き領域があることを確認します。
- SnapCenter サーバがインストールされているドメインが削除されていないことを確認します。

  SnapCenter サーバがインストールされていたドメインを削除してからアンインストールしようとすると、処理に失敗します。

- リポジトリデータベースがクリーンアップされてアンインストールされるため、リポジトリデータベース

をバックアップしておく必要があります。

- 手順 *

1. SnapCenter サーバーホストで、コントロールパネルに移動します。
2. 「 * カテゴリ * 」ビューにいることを確認します。
3. [プログラム] の下にある [プログラムのアンインストール] をクリックします。

   [プログラムと機能] ウィンドウが開きます。

4. NetApp SnapCenter Server を選択し、 * Uninstall * をクリックします。

   SnapCenter 4.2 では、 SnapCenter サーバをアンインストールすると、 MySQL Server リポジトリデータベースを含むすべてのコンポーネントがアンインストールされます。

   - NLB クラスタから NLB ノードを削除した場合、 SnapCenter サーバホストを再起動する必要があります。ホストを再起動しないと、 SnapCenter サーバを再インストールしようとしたときにエラーが発生することがあります。
   - アンインストール時に削除されない .NET Framework を手動でアンインストールする必要があります。

REST API を使用して自動化

REST API の概要

REST API を使用して、 SnapCenter のいくつかの管理処理を実行できます。REST API は Swagger Web ページから利用できます。

<SnapCenter_IP_address_or_name>のドキュメントを表示したり、<SnapCenter_port>呼び出しを手動で問題したりするには、Swagger Webページ（\ *https*：//：/ *swagger* /）にアクセスします。

REST API をサポートするプラグインは次のとおりです。

- Microsoft SQL Server 用プラグイン
- Plug-in for SAP HANA Database の略
- カスタムプラグイン
- Plug-in for Oracle Database の略

SnapCenter REST API にネイティブでアクセスする方法

SnapCenter REST API には、 REST クライアントをサポートする任意のプログラミング言語を使用して直接アクセスできます。代表的な言語の選択肢は、 Python 、 PowerShell 、 Java です。

基盤としての REST Web サービス

Representational State Transfer （ REST ）は、分散 Web アプリケーションの作成に使用される形式です。Web サービス API の設計においては、サーバベースのリソースを公開してその状態を管理するための一連のテクノロジとベストプラクティスが確立されます。主流のプロトコルと標準を使用して、 SnapCenter を管理するための柔軟な基盤を提供しています。

リソースと状態の表示

リソースは、 Web ベースシステムの基本コンポーネントです。REST Web サービスアプリケーションを作成する場合、設計の早い段階で次の作業を行います。

システムまたはサーバベースのリソースの識別

すべてのシステムは、リソースを使用および管理します。リソースには、ファイル、ビジネストランザクション、プロセス、管理エンティティなどがあります。REST Web サービスに基づいてアプリケーションを設計する際に行う最初の作業の 1 つは、リソースを識別することです。

リソースの状態および関連する状態操作の定義

リソースの状態の数は有限で、リソースは必ずそのいずれかの状態にあります。状態、および状態の変化に影

響する関連操作を明確に定義する必要があります。

URI エンドポイント

すべての REST リソースは、明確に定義されたアドレス指定方式を使用して定義および使用可能にする必要があります。 リソースが置かれているエンドポイントは、 Uniform Resource Identifier （ URI ）で識別されます。

URI は、ネットワーク内の各リソースに一意の名前を作成するための一般的なフレームワークです。Uniform Resource Locator （ URL ）は、リソースを識別してアクセスするために Web サービスで使用される URI の一種です。リソースは通常、ファイルディレクトリに似た階層構造で公開されます。

HTTP メッセージ

Hypertext Transfer Protocol （ HTTP ）は、 Web サービスのクライアントとサーバがリソースに関する要求と応答のメッセージを交換する際に使用するプロトコルです。

Web サービスアプリケーションの設計の一環として、 HTTP メソッドはリソースおよび対応する状態管理アクションにマッピングされます。HTTP はステートレスです。したがって、関連する一連の要求と応答を 1 つのトランザクションの一部として関連付けるには、要求と応答のデータフローで伝送される HTTP ヘッダーに追加情報を含める必要があります。

JSON 形式

Web サービスのクライアントとサーバの間で情報を構造化して転送する方法は複数ありますが、最も広く使用されているのは JavaScript Object Notation （ JSON ）です。

JSON は、単純なデータ構造をプレーンテキストで表すための業界標準であり、リソースについての状態情報の転送に使用されます。SnapCenter REST API では、 JSON を使用して、各 HTTP 要求と応答の本文で伝送されるデータをフォーマットします。

基本的な動作特性

REST で共通のテクノロジとベストプラクティスは確立されますが、各 API の詳細は設計内容に応じて異なる場合があります。

要求と応答の API トランザクション

すべての REST API 呼び出しは、 SnapCenter サーバシステムへの HTTP 要求として実行され、クライアントへの関連する応答が生成されます。この要求と応答のペアで API トランザクションが構成されます。

API を使用する前に、要求の制御に使用できる入力変数と応答出力の内容を理解しておく必要があります。

CRUD 操作のサポート

SnapCenter REST API で使用できる各リソースへのアクセスは CRUD モデルに基づきます。

- 作成
- 読み取り

- 更新
- 削除

一部のリソースでは、一部の処理のみがサポートされます。

オブジェクト ID

各リソースインスタンスまたはオブジェクトには、作成時に一意の識別子が割り当てられます。ほとんどの場合、識別子は 128 ビットの UUID です。これらの識別子は、特定の SnapCenter サーバ内でグローバルに一意です。

新しいオブジェクトインスタンスを作成する API 呼び出しを実行すると、関連付けられた ID を含む URL が HTTP 応答の場所ヘッダーにある呼び出し元に返されます。リソースインスタンスを以降の呼び出しで参照する際には、この識別子を抽出して使用できます。

オブジェクト識別子の内容と内部構造は、いつでも変更される可能性があります。識別子を使用するのは、該当する API 呼び出しで関連付けられているオブジェクトを参照するときに必要に応じてのみです。

オブジェクトのインスタンスとコレクション

リソースパスと HTTP メソッドに応じて、 API 呼び出しを特定のオブジェクトインスタンスまたはオブジェクトのコレクションに適用できます。

同期操作と非同期操作

SnapCenter は、クライアントから同期または非同期で受信した HTTP 要求を実行します。

同期処理

SnapCenter は要求をただちに実行し、成功した場合は HTTP ステータスコード 200 または 201 を返します。

GET メソッドを使用する要求は、いずれも常に同期的に実行されます。また、 POST を使用する要求は、完了までに 2 秒かからないと予想される場合に、同期的に実行されるように設計されています。

非同期処理

非同期要求が有効な場合、 SnapCenter は要求を処理するバックグラウンドタスクと、タスクのアンカーを設定するジョブオブジェクトを作成します。HTTP ステータスコード 202 がジョブオブジェクトとともに呼び出し元に返されます。成功または失敗を確認するには、ジョブの状態を取得する必要があります。

POST メソッドと DELETE メソッドを使用する要求は、完了までに 2 秒以上かかると予想される場合に非同期で実行するように設計されています。

セキュリティ

REST API のセキュリティは、主に SnapCenter で利用可能な既存のセキュリティ機能に基づいています。API で使用されるセキュリティは次のとおりです。

トランスポートレイヤのセキュリティ

SnapCenter サーバとクライアントの間でネットワークを介して送信されるすべてのトラフィックは、通常、SnapCenter 設定に基づいて TLS を使用して暗号化されます。

HTTP認証

HTTP レベルでは、 API トランザクションにベーシック認証が使用されます。base64 文字列のユーザ名とパスワードを含む HTTP ヘッダーが各要求に追加されます。

API 要求を制御する入力変数

API 呼び出しの処理方法は、 HTTP 要求で設定されたパラメータと変数を使用して制御できます。

HTTP メソッド

次の表に、 SnapCenter REST API でサポートされる HTTP メソッドを示します。

REST エンドポイントのそれぞれですべての HTTP メソッドを使用できるわけではありません。

HTTP メソッド	説明
取得	リソースインスタンスまたはコレクションのオブジェクトプロパティを取得します。
投稿（ Post ）	指定した入力に基づいて新しいリソースインスタンスを作成します。
削除	既存のリソースインスタンスを削除します。
PUT	既存のリソースインスタンスを変更します。

要求ヘッダー

HTTP 要求には複数のヘッダーを含める必要があります。

コンテンツタイプ

要求の本文に JSON が含まれている場合は、このヘッダーを *application/json* に設定する必要があります。

同意します

このヘッダーは、 *application/json* に設定してください。

承認

base64 文字列としてエンコードされたユーザ名とパスワードを使用するベーシック認証を設定する必要があります。

本文を要求します

要求の本文の内容は、それぞれの呼び出しに応じて異なります。HTTP 要求の本文は、次のいずれかで構成されます。

- JSON オブジェクトと入力変数
- 空です

オブジェクトのフィルタリング

GET を使用する API 呼び出しを発行する際、返されるオブジェクトを任意の属性に基づいて制限またはフィルタできます。たとえば、一致する正確な値を指定できます。

```
<field>=<query value>
```

完全一致に加えて、他の演算子を使用して、一連のオブジェクトを一定範囲の値で返すことができます。次の表に、 SnapCenter REST API でサポートされるフィルタ演算子を示します。

演算子	説明
=	等しい
<	より小さい
>	が次の値より大きい
⇐	が次の値以下です
>=	が次の値以上である必要があります
更新	または
！	と等しくない
*	すべてに一致するワイルドカード

また、クエリの一部として **null** キーワードまたはその negation*!null* を使用して、特定のフィールドが設定されているかどうかに基づいてオブジェクトのコレクションを返すこともできます。

通常、設定されていないフィールドはクエリの照合から除外されます。

特定のオブジェクトフィールドを要求しています

デフォルトでは、 GET を使用する API 呼び出しを発行すると、オブジェクトを一意に識別する属性のみが返されます。この最小のフィールドセットは、各オブジェクトのキーとして機能し、オブジェクトタイプによって異なります。を使用して、追加のオブジェクトプロパティを選択できます `fields` 次の方法でクエリパラメータを指定します。

共通または標準のフィールド

fields=* を指定すると、最もよく使用されるオブジェクトフィールドが取得されます。これらのフィールドは、通常、ローカルサーバメモリに保持されるか、ほとんど処理を必要としません。これらのプロパティは、URL パスキー（ UUID ）を指定して GET を使用した場合にオブジェクトに対して返されるプロパティと同じです。

すべてのフィールド

fields=** を指定すると ' アクセスするために追加のサーバ処理が必要なフィールドも含め ' すべてのオブジェクトフィールドが取得されます

カスタムフィールドの選択

fields=<field_name> を使用すると、必要なフィールドを正確に指定できます。複数のフィールドを要求する場合は、スペースを入れずにカンマで区切る必要があります。

ベストプラクティスとして、必要なフィールドを常に個別に指定することを推奨します。一連の共通フィールドまたはすべてのフィールドを取得するのは、必要な場合だけにしてください。共通として分類されるフィールドで、 *fields=** を使用して返されるフィールドは、ネットアップの内部パフォーマンス分析に基づいて決定されます。フィールドの分類は、今後のリリースで変更される可能性があります。

出力セット内のオブジェクトのソート

リソースコレクション内のレコードは、オブジェクトによって定義されたデフォルトの順序で返されます。を使用して順序を変更できます `order_by` フィールド名とソート順序を指定したクエリパラメータ。

```
order_by=<field name> asc|desc
```

たとえば、タイプフィールドを降順でソートし、 ID を昇順でソートできます。

```
order_by=type desc, id asc
```

- ソートフィールドを指定してソートの方向を指定しなかった場合、値は昇順でソートされます。
- 複数のパラメータを指定する場合は、各フィールドをカンマで区切る必要があります。

オブジェクトのコレクションを取得するときのページ付けです

GET を使用する API 呼び出しを発行して同じタイプのオブジェクトのコレクションにアクセスする場合、SnapCenter では 2 つの制約に基づいて可能なかぎり多くのオブジェクトを返します。これらの各制約は、要求に対する追加のクエリパラメータを使用して制御できます。特定の GET 要求に対する最初の制約に達した時点で要求が終了されるため、返されるレコードの数が制限されます。

すべてのオブジェクトについての処理が完了する前に要求が終了した場合、次のレコードのバッチを取得するために必要なリンクが応答に含まれます。

オブジェクト数の制限

デフォルトでは、 SnapCenter は GET 要求に対して最大 10 、 000 個のオブジェクトを返します。この制限は、 _max_records_query パラメータを使用して変更できます。例：

```
max_records=20
```

実際に返されるオブジェクトの数は、関連する時間の制約やシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

オブジェクトを読み出す時間を制限しています

デフォルトでは、 SnapCenter は GET 要求に許可された時間内にできるだけ多くのオブジェクトを返します。デフォルトのタイムアウトは 15 秒です。この制限は、 _return_timeout_query パラメータを使用して変更できます。例：

```
return_timeout=5
```

実際に返されるオブジェクトの数は、関連するオブジェクト数の制約やシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

結果セットの絞り込み

必要に応じて、これらの 2 つのパラメータを追加のクエリパラメータと組み合わせて、結果セットを絞り込むことができます。たとえば、次の例では、指定した時間のあとに生成された EMS イベントを最大 10 件まで返します。

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

複数の要求を問題で処理して、オブジェクトをページングできます。以降の API 呼び出しでは、前回の結果セットの最新イベントに基づいて新しい時間の値を使用する必要があります。

サイズのプロパティ

一部の API 呼び出しおよびクエリパラメータでは、入力値として数値が使用されます。バイト単位で整数を指定する代わりに、必要に応じて次の表に示すサフィックスを使用できます。

サフィックス	説明
KB	KB キロバイト（ 1024 バイト）またはキビバイト
MB	MB （ KB x 1024 バイト）またはメビバイト
GB	ギガバイト（ MB x 1024 バイト）またはギビバイト
容量	TB （ GB x 1024 バイト）またはテビバイト
PB	PB ペタバイト（ TB x 1024 バイト）またはペビバイト

API 応答の解釈

各 API 要求でクライアントへの応答が生成されます。応答を調べて成功したかどうかを確認し、必要に応じて追加データを取得します。

HTTP ステータスコード

SnapCenter REST API で使用される HTTP ステータスコードを次に示します。

コード	説明
200です	わかりました 新しいオブジェクトを作成しない呼び出しが成功したことを示します。
201年だ	作成済み オブジェクトが作成されました。応答の location ヘッダーにオブジェクトの一意の識別子が含まれます。
202です	承認済み バックグラウンドジョブで要求の実行が開始されましたが、まだ完了していません。
400だ	無効な要求です 要求の入力が認識されないか不適切です。
401	権限がありません ユーザ認証に失敗しました。
403です	禁止されている 認証（ RBAC ）エラーによりアクセスが拒否されました。
404です	が見つかりません 要求で参照されているリソースが存在しません。
405です	メソッドを使用できません 要求の HTTP メソッドがリソースに対してサポートされていません。
409だ	競合しています 先に別のオブジェクトを作成する必要があるか、要求されたオブジェクトがすでに存在するため、オブジェクトの作成に失敗しました。
500ドル	内部エラー サーバで一般的な内部エラーが発生しました。

応答ヘッダー

SnapCenter によって生成される HTTP 応答には、いくつかのヘッダーが含まれています。

場所

オブジェクトが作成されると、オブジェクトに割り当てられた一意の識別子を含む、新しいオブジェクトへの完全な URL が location ヘッダーに含まれます。

コンテンツタイプ

通常はです `application/json`。

応答の本文

API要求の結果として返される応答の本文の内容は、オブジェクト、処理タイプ、および要求の成否によって異なります。応答は常に JSON 形式になります。

単一のオブジェクト

1 つのオブジェクトを要求に基づいて一連のフィールドとともに返すことができます。たとえば、 GET では、一意の識別子を使用してクラスタの選択したプロパティを取得できます。

複数のオブジェクト

リソースコレクションから複数のオブジェクトを返すことができます。いずれの場合も、で一貫した形式が使用されます `num_records` オブジェクトインスタンスの配列を含むレコードとレコードの数を示します。たとえば、特定のクラスタで定義されているノードを取得できます。

ジョブオブジェクト

API 呼び出しが非同期で処理されると、バックグラウンドタスクのアンカーを設定するジョブオブジェクトが返されます。たとえば、クラスタ構成の更新に使用される PATCH 要求は非同期で処理され、ジョブオブジェクトが返されます。

エラーオブジェクト

エラーが発生した場合は、常にエラーオブジェクトが返されます。たとえば、クラスタに定義されていないフィールドを変更しようとするとエラーが表示されます。

空です

場合によっては、データが返されず、応答の本文に空の JSON オブジェクトが含まれることがあります。

エラー

エラーが発生した場合は、応答の本文でエラーオブジェクトが返されます。

の形式で入力し

エラーオブジェクトの形式は次のとおりです。

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

code の値で一般的なエラーの種類やカテゴリを特定し、 message で具体的なエラーの内容を確認できます。該当する場合、エラーに関連する特定のユーザ入力がターゲットフィールドに表示されます。

一般的なエラーコード

次の表に、一般的なエラーコードを示します。特定の API 呼び出しについては、追加のエラーコードが含まれる場合があります。

コード	説明
409だ	同じ識別子のオブジェクトがすでに存在します。
400だ	フィールドの値が無効であるか、値が指定されていないか、余分なフィールドが指定されています。
400だ	この処理はサポートされません。
405です	指定した識別子のオブジェクトが見つかりません。
403です	要求を実行する権限が拒否されました。
409だ	リソースが使用中です。

サポートされている REST API

SnapCenter サーバとプラグインでサポートされるREST API

SnapCenter REST API で使用できるリソースは、 SnapCenter API ドキュメントページに表示されるカテゴリ別に分類されています。以下に、各リソースの簡単な概要とベースリソースパスを示し、使用に際しての追加の考慮事項がある場合はその情報も示します。

認証

このAPIを使用して、SnapCenter サーバにログインできます。この API は、以降の要求の認証に使用するユーザ認証トークンを返します。

ドメイン

APIを使用してさまざまな処理を実行できます。

- SnapCenter 内のすべてのドメインを取得します
- 特定のドメインの詳細を取得します
- ドメインを登録または登録解除します
- ドメインを変更します

ジョブ

APIを使用してさまざまな処理を実行できます。

- SnapCenter のすべてのジョブを取得します

- ジョブのステータスを取得します
- ジョブをキャンセルまたは停止します

設定

APIを使用してさまざまな処理を実行できます。

- クレデンシャルを登録、変更、または削除します
- SnapCenter サーバに登録されているクレデンシャル情報を表示します
- 通知を設定します
- Eメール通知を送信するように現在設定されているSMTPサーバに関する情報を取得し、SMTPサーバの名前、受信者の名前、および送信者の名前を表示します
- SnapCenter サーバログインの多要素認証（MFA）設定を表示します
- SnapCenter サーバログインに対してMFAを有効または無効にして設定します
- MFAの設定に必要な構成ファイルを作成します

ホスト

APIを使用してさまざまな処理を実行できます。

- すべてのSnapCenter ホストを照会します
- SnapCenter から1つ以上のホストを削除します
- 名前でホストを取得します
- ホストのすべてのリソースを取得します
- リソースIDを使用してリソースを取得する
- プラグイン設定の詳細を取得します
- プラグインホストを設定します
- Microsoft SQL Serverホスト用プラグインのすべてのリソースを取得します
- Oracleデータベース・ホスト用プラグインのすべてのリソースを取得します
- カスタムアプリケーションホスト用のプラグインのすべてのリソースを取得します
- SAP HANAホスト用プラグインのすべてのリソースを取得します
- インストールされているプラグインを取得します
- 既存のホストにプラグインをインストールする
- ホストパッケージをアップグレードします
- 既存のホストからプラグインを削除します
- ホストにプラグインを追加します
- ホストを追加または変更します
- Linuxホストの署名を取得します
- Linuxホストの署名を登録します

- ホストをメンテナンスモードまたは本番モードにします
- ホストでプラグインサービスを開始または再起動します
- ホストの名前を変更します

リソース

APIを使用してさまざまな処理を実行できます。

- すべてのリソースを取得します
- リソースIDを使用してリソースを取得する
- Microsoft SQL Serverホスト用プラグインのすべてのリソースを取得します
- Oracleデータベース・ホスト用プラグインのすべてのリソースを取得します
- カスタムアプリケーションホスト用のプラグインのすべてのリソースを取得します
- SAP HANAホスト用プラグインのすべてのリソースを取得します
- キーを使用してMicrosoft SQL Serverリソースを取得します
- キーを使用してカスタムリソースを取得します
- カスタムアプリケーションホスト用のプラグインのリソースを変更します
- キーを使用して、カスタムアプリケーションホスト用プラグインのリソースを削除します
- キーを使用してSAP HANAリソースを取得する
- SAP HANAホスト用プラグインのリソースを変更します
- キーを使用して、SAP HANAホスト用プラグインのリソースを削除します
- キーを使用してOracleリソースを取得します
- Oracleアプリケーションボリュームリソースを作成します
- Oracleアプリケーションボリュームリソースを変更します
- キーを使用してOracleアプリケーションボリュームのリソースを削除します
- Oracleリソースのセカンダリの詳細を取得します
- Plug-in for Microsoft SQL Serverを使用して、Microsoft SQL Serverリソースをバックアップします
- Plug-in for Oracle Databaseを使用してOracleリソースをバックアップします
- カスタムアプリケーション用のプラグインを使用して、カスタムリソースをバックアップします
- SAP HANAデータベースを設定します
- Oracleデータベースを設定します
- SQLデータベースのバックアップをリストアする
- Oracleデータベースバックアップをリストアする
- カスタムアプリケーションのバックアップをリストアする
- カスタムプラグインリソースを作成する
- SAP HANAリソースを作成します

- カスタムアプリケーション用のプラグインを使用してカスタムリソースを保護する
- Plug-in for Microsoft SQL Serverを使用してMicrosoft SQL Serverリソースを保護します
- 保護されたMicrosoft SQL Serverリソースを変更します
- Microsoft SQL Serverリソースの保護を解除します
- Plug-in for Oracle Databaseを使用してOracleリソースを保護します
- 保護されたOracleリソースを変更します
- Oracleリソースの保護を解除します
- カスタムアプリケーションのプラグインを使用して、バックアップからリソースをクローニングする
- Plug-in for Oracle Databaseを使用して、バックアップからOracleアプリケーションボリュームをクローニングします
- Plug-in for Microsoft SQL Serverを使用して、バックアップからMicrosoft SQL Serverリソースのクローンを作成します
- Microsoft SQL Serverリソースのクローンライフサイクルを作成します
- Microsoft SQL Serverリソースのクローンのライフサイクルを変更します
- Microsoft SQL Serverリソースのクローンライフサイクルを削除します
- 既存のMicrosoft SQL ServerデータベースをローカルディスクからNetApp LUNに移動します
- Oracleデータベースのクローン仕様ファイルを作成します
- Oracleリソースのクローン更新ジョブをオンデマンドで開始する
- クローン仕様ファイルを使用して、バックアップからOracleリソースを作成します
- データベースをセカンダリレプリカにリストアし、データベースを可用性グループに再び参加させます
- Oracleアプリケーションボリュームリソースを作成します

バックアップ

APIを使用してさまざまな処理を実行できます。

- バックアップの名前、タイプ、プラグイン、リソース、または日付別にバックアップの詳細を取得する
- すべてのバックアップを取得します
- バックアップの詳細を取得します
- バックアップの名前変更または削除
- Oracleバックアップをマウント
- Oracleバックアップをアンマウント
- Oracleバックアップをカタログ化
- Oracleバックアップをカタログ化解除します
- ポイントインタイムリカバリを実行するためにマウントが必要なすべてのバックアップを取得します

クローン

APIを使用してさまざまな処理を実行できます。

- Oracleデータベースのクローン仕様ファイルを作成、表示、変更、および削除します
- Oracleデータベースのクローン階層を表示します
- クローンの詳細を取得します
- すべてのクローンを取得します
- クローンを削除します。
- IDを使用してクローンの詳細を取得します
- Oracleリソースのクローン更新ジョブをオンデマンドで開始する
- クローン仕様ファイルを使用して、バックアップからOracleリソースをクローニングします

クローンスプリット

APIを使用してさまざまな処理を実行できます。

- クローニングされたリソースのクローンスプリット処理を見積もります
- クローンスプリット処理のステータスを取得します
- クローンスプリット処理を開始または停止します

リソースグループ

APIを使用してさまざまな処理を実行できます。

- すべてのリソースグループの詳細を取得します
- リソースグループを名前で取得します
- カスタムアプリケーション用のプラグインのリソースグループを作成します
- Microsoft SQL Server用プラグインのリソースグループを作成します
- Oracleデータベース用プラグインのリソースグループを作成します
- カスタムアプリケーションのプラグインのリソースグループを変更する
- Plug-in for Microsoft SQL Serverのリソースグループを変更します
- Oracleデータベース用プラグインのリソースグループを変更する
- Plug-in for Microsoft SQL Serverのリソースグループのクローンライフサイクルを作成、変更、または削除します
- リソースグループをバックアップする
- リソースグループをメンテナンスモードまたは本番モードにします
- リソースグループを削除する

ポリシー

APIを使用してさまざまな処理を実行できます。

- ポリシーの詳細を取得します
- ポリシーの詳細を名前で取得します
- ポリシーを削除する
- 既存のポリシーのコピーを作成する
- カスタムアプリケーション用のプラグインのポリシーを作成または変更する
- Microsoft SQL Server用プラグインのポリシーを作成または変更します
- Oracleデータベース用プラグインのポリシーを作成または変更します
- SAP HANAデータベース用プラグインのポリシーを作成または変更します

ストレージ

APIを使用してさまざまな処理を実行できます。

- すべての共有を取得します
- 名前を指定して共有を取得します
- 共有を作成または削除します
- ストレージの詳細を取得します
- 名前を指定してストレージの詳細を取得します
- ストレージを作成、変更、または削除する
- ストレージクラスタ上のリソースを検出
- ストレージクラスタのリソースを取得する

共有

APIを使用してさまざまな処理を実行できます。

- 共有の詳細を取得します
- すべての共有の詳細を取得します
- ストレージ上に共有を作成するか、削除します
- 名前を指定して共有を取得します

プラグイン

APIを使用してさまざまな処理を実行できます。

- ホストのすべてのプラグインを一覧表示します
- キーを使用してMicrosoft SQL Serverリソースを取得します
- キーを使用してカスタムリソースを変更します

- キーを使用してカスタムリソースを削除します
- キーを使用してSAP HANAリソースを取得する
- キーを使用してSAP HANAリソースを変更します
- キーを使用してSAP HANAリソースを削除します
- キーを使用してOracleリソースを取得します
- Oracleアプリケーションのボリュームリソースをキーを使用して変更します
- キーを使用してOracleアプリケーションボリュームのリソースを削除します
- Plug-in for Microsoft SQL Serverとキーを使用して、Microsoft SQL Serverリソースをバックアップします
- Oracleデータベース用プラグインとキーを使用して、Oracleリソースをバックアップします
- カスタムアプリケーション用のプラグインとキーを使用して、カスタムアプリケーションリソースをバックアップします
- キーを使用してSAP HANAデータベースを設定します
- キーを使用してOracleデータベースを設定します
- カスタムアプリケーションのバックアップをキーを使用してリストアする
- カスタムプラグインリソースを作成する
- SAP HANAリソースを作成します
- Oracleアプリケーションボリュームリソースを作成します
- カスタムアプリケーション用のプラグインを使用してカスタムリソースを保護する
- Plug-in for Microsoft SQL Serverを使用してMicrosoft SQL Serverリソースを保護します
- 保護されたMicrosoft SQL Serverリソースを変更します
- Microsoft SQL Serverリソースの保護を解除します
- Plug-in for Oracle Databaseを使用してOracleリソースを保護します
- 保護されたOracleリソースを変更します
- Oracleリソースの保護を解除します
- カスタムアプリケーションのプラグインを使用して、バックアップからリソースをクローニングする
- Plug-in for Oracle Databaseを使用して、バックアップからOracleアプリケーションボリュームをクローニングします
- Plug-in for Microsoft SQL Serverを使用して、バックアップからMicrosoft SQL Serverリソースのクローンを作成します
- Microsoft SQL Serverリソースのクローンライフサイクルを作成します
- Microsoft SQL Serverリソースのクローンのライフサイクルを変更します
- Microsoft SQL Serverリソースのクローンライフサイクルを削除します
- Oracleデータベースのクローン仕様ファイルを作成します
- Oracleリソースのクローンライフサイクルをオンデマンドで開始する
- クローン仕様ファイルを使用して、バックアップからOracleリソースをクローニングします

レポート

APIを使用してさまざまな処理を実行できます。

- 対応するプラグインのバックアップ、リストア、クローニングの各処理に関するレポートを取得できます
- スケジュールを追加、実行、削除、または変更します
- スケジュール済みレポートのデータを取得します

アラート

APIを使用してさまざまな処理を実行できます。

- すべてのアラートを取得します
- IDを使用してアラートを取得します
- 複数のアラートを削除するか、ID別にアラートを削除します

RBAC

APIを使用してさまざまな処理を実行できます。

- ユーザ、グループ、およびロールの詳細を取得します
- ユーザを追加または削除します
- ロールにユーザを割り当てます
- ロールへのユーザの割り当てを解除します
- ロールを作成、変更、または削除します
- グループをロールに割り当てます
- ロールからグループの割り当てを解除します
- グループを追加または削除します
- 既存のロールのコピーを作成します
- ユーザまたはグループにリソースを割り当てまたは割り当て解除します

設定

APIを使用してさまざまな処理を実行できます。

- 構成設定を表示します
- 設定を変更します

CertificateSettings

APIを使用してさまざまな処理を実行できます。

- SnapCenter サーバまたはプラグインホストの証明書ステータスを表示します
- SnapCenter サーバまたはプラグインホストの証明書設定を変更します

リポジトリ

APIを使用してさまざまな処理を実行できます。

- リポジトリのバックアップを取得する
- リポジトリの設定情報を表示します
- SnapCenter リポジトリを保護し、リストアします
- SnapCenter リポジトリの保護を解除します
- リポジトリを再構築してフェイルオーバーします

バージョン

このAPIを使用して、SnapCenter のバージョンを表示できます。

ディザスタリカバリ（DR）REST API

SnapCenter ディザスタリカバリ（ DR ）機能では、 REST API を使用して SnapCenter サーバをバックアップします。DR REST APIを使用する前に、次の手順を実行します。

- 手順 *

1. DRバックアップREST APIを使用して、指定したサーバDRバックアップからSnapCenter サーバをリストアする新しいサーバDRバックアップを作成します。
   `/4.5/disasterrecovery/server/backup`
2. セカンダリサーバマシンを起動しますが、セカンダリサーバにSnapCenter サーバをインストールする前に、前提条件を満たしておく必要があります。
   - 代替サーバのホスト名/ホストのFQDNはプライマリサーバのホスト名と同じである必要がありますが、IPアドレスは同じであってもかまいません。
   - セカンダリサーバのバージョンは、プライマリサーバと同じである必要があります。
   - セカンダリSnapCenter は、プライマリと同じ場所と同じポートにインストールする必要があります。
3. サーバのDRリストア処理を開始する前に、災害後にDRバックアップが保存されるターゲットパスまたはパスを起動する必要があります。
   - 次のコマンドを使用して、DRバックアップファイルが新しいSnapCenter サーバにコピーされていることを確認します。
     `xcopy <Ssource_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X /E /H /K {ex : xcopy C:\DRBackup \\10.225.81.114\c$\DRBackup /O /X /E /H /K}`
4. セカンダリマシンにSnapCenter サーバをインストールします。
   - DRリストア処理の実行中は、SnapCenter サーバに関連するジョブが実行されていないことを確認する必要があります。
5. セカンダリSnapCenter サーバをプライマリサーバと同じ場所に、同じポートにインストールします。
   - DRリストアAPIを使用して、サーバDRリストア処理を実行します。
     `/4.5/disasterrecovery/server/restore`

     プラグインがサーバのホスト名を解決できない場合は、各プラグインホストにログインし、新し

いIPのetc/hostエントリを<New IP> SC_Server_Name形式で追加します。
例： `10.225.81.35 SCServer1`

サーバの /etc/hosts エントリはリストアされません。DR バックアップフォルダから手動でリストアできます。

F5セットアップの場合、リストア処理はスタンドアロンとして実行されます。F5を再度作成するには、一連のコマンドを実行する必要があります。を参照してください。リンク： "SnapCenter を別のサーバに移行する方法"

DRのリストア後にホストが追加されますが、プラグインを手動でインストールする必要があります。

リポジトリのバックアップスケジュールは、SnapCenter Plug-in for WindowsをインストールしてサーバマシンにネットアップLUNを接続した場合にのみリストアされます。

DLLが破損している場合は、SnapCenterサーバを修復したり、問題のあるインストールを修正したりできます。

NSMファイルまたは構成ファイルが破損している場合は、同じバージョンのSnapCenterサーバをアンインストールして再インストールできます。

リポジトリのバックアップスケジュールは、SnapCenter Plug-in for Windowsをインストールしてサーバマシンにネットアップ LUNを接続した場合にのみリストアされます。

SnapCenter サーバのディザスタリカバリでサポートされる **REST API**

REST API を使用すると、 REST API Swagger ページで次の処理を実行できます。Swagger ページへのアクセス方法については、を参照してください "swagger API Web ページを使用して REST API にアクセスする方法"。

- 必要なもの *
- SnapCenter 管理者ユーザとしてログインする必要があります。
- DR リストア API を実行するには、 SnapCenter サーバが稼働している必要があります。
- このタスクについて *

SnapCenter Server DR はすべてのプラグインをサポートします。

説明	REST API	HTTP メソッド
既存の SnapCenter サーバ DR バックアップを取得します DRバックアップを格納するターゲットパスを指定する必要があります。	`/4.5/disasterrecovery/server/backup?targetpath={path}`	取得
新しいサーバ DR バックアップを作成します。	`/4.5/disasterrecovery/server/backup`	投稿（ Post ）
指定したサーバ DR バックアップから SnapCenter サーバをリストアします。	`/4.5/disasterrecovery/server/restore`	投稿（ Post ）
バックアップ名に基づいて Server DR バックアップを削除します。	`/4.5/disasterrecovery/server/backup`	削除
ストレージ DR を有効または無効にします	`/4.5/disasterrecovery/storage`	投稿（ Post ）

詳細については、を参照してください "ディザスタリカバリ API" ビデオ：

Swagger API Web ページから REST API にアクセスする方法

REST API は Swagger Web ページから利用できます。Swagger Web ページにアクセスして SnapCenter サーバ REST API を表示したり、 API を手動で問題呼び出したりできます。REST API を使用して、 SnapCenter サーバの管理やデータ保護処理を行うことができます。

REST API を実行する SnapCenter サーバの管理 IP アドレスまたはドメイン名を確認しておく必要があります。

REST API クライアントを実行するための特別な権限は必要ありません。すべてのユーザが Swagger Web ページにアクセスできます。REST API を使用してアクセスするオブジェクトに対する各権限は、 REST API へのログイン時にトークンを生成するユーザに基づいています。

- 手順 *

1. ブラウザで、「\ *https*：//<*SnapCenter_IP_address_or_name*>：<*SnapCenter_port*>/*swagger/*」の形式でWebページにアクセスするためのURLを入力します。

   REST API URL に、 + 、 . 、 % 、 & の文字が含まれていないことを確認してください。

2. SwaggerのExplore *フィールドに、Swagger APIドキュメントが自動的に表示されない場合は、次の

ように入力します。
\ *https：//<SnapCenter_IP_address_or_name>*
：<SnapCenter_port>/Content/swagger/SnapCenter.yaml

3. [* Explore] をクリックします。

   API のリソースタイプまたはカテゴリのリストが表示されます。

4. API リソースタイプをクリックすると、そのリソースタイプの API が表示されます。

SnapCenter REST API の実行時に予期しない動作が発生した場合は、ログファイルを使用して原因を特定し、問題を解決することができます。
SnapCenter ユーザー・インターフェイスからログ・ファイルをダウンロードするには、 * Monitor * > * Logs * > * Download * をクリックします。

REST API の使用を開始する

SnapCenter REST API はすぐに使用を開始できます。API にアクセスすると、ライブセットアップでより複雑なワークフロープロセスを使用する前にいくつかの情報を確認できます。

Hello world

システムで簡単なコマンドを実行して、 SnapCenter REST API の使用を開始し、利用可能かどうかを確認できます。

- 必要なもの *
- Curl ユーティリティがシステムで使用できることを確認します。
- SnapCenter サーバの IP アドレスまたはホスト名
- SnapCenter REST API にアクセスする権限を持つアカウントのユーザ名とパスワード。

> クレデンシャルに特殊文字が含まれている場合は、使用するシェルに基づいて Curl で許容される形式で指定する必要があります。たとえば、各特殊文字の前にバックスラッシュを挿入したり、全体を折り返すことができます `username:password` 一重引用符で囲んだ文字列。

- ステップ *

コマンドラインインターフェイスで、次のコマンドを実行してプラグイン情報を取得します。

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

例

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

"SnapCenter 4.8の注意事項は以下のとおりです"