SnapCenterソフトウェアのドキュメント

SnapCenter Software 6.0

NetApp
September 23, 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 "SnapCenterソフトウェア6.0リリースノート"ください。

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管理型プラットフォームです。ハイブリッドクラウドのどこにいても、ONTAPシステムで実行され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は、NetAppのSnapshot、SnapRestore、FlexClone、SnapMirror、SnapVaultのテクノロジを活用して、次の機能を提供します。

- 高速で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、アプリケーションと整合性のあるリカバリ
- スペース効率に優れた高速クローニング

SnapCenterには、SnapCenter Serverと個別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、クローニング処理のスケジュールを設定したり、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。

- オンプレミスで次のデータを保護：
  - ONTAP FAS、AFF、またはAll SAN Array（ASA）プライマリシステム上にあり、ONTAP FAS、AFF、またはASA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、AFF、またはASAのプライマリシステムとセカンダリシステムにあり、ローカルのStorageGRIDオブジェクトストレージで保護されているデータ
- ハイブリッドクラウドにオンプレミスで導入し、以下のデータを保護
  - ONTAP FAS、AFF、またはASA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、AFF、ASAのプライマリシステムとセカンダリシステムにあり、クラウドのオブジェクトストレージとアーカイブストレージで保護されているデータ（BlueXPのバックアップとリカバリの統合を使用）
- パブリッククラウドに導入し、以下のデータを保護
  - Cloud Volumes ONTAP（旧ONTAP Cloud）プライマリシステム上のデータ
  - Amazon FSx for ONTAP上のデータ
  - プライマリAzure NetApp Files上のデータ（Oracle、Microsoft SQL、SAP HANA）

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、IBM DB2、およびWindowsホストの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、同じ単一コンソールから他のアプリケーションやデータベースのデータを保護できます。このフレームワークを活用して、NetAppはMongoDB、MySQL、PostgreSQL、ストレージ、MaxDB向けのSnapCenterプラグインをリリースしました。 Sybase ASE、ORASCPM、MongoDB、DPGlue。これとは別に、開発者ガイドを使用して独自のプラグインを作成できます。

"アプリケーション用のプラグインを開発"

- 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テクノロジを活用して、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ディスクベースのバックアップを高速で作成できます。必要に応じて、既存の保護関係を更新して、セカンダリストレージへのバックアップの保護を自動化することもできます。

- 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すると、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は、バックアップの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時間ベースのリカバリを実現します。ハイブリッドクラウド内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、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、ソフトウェア開発を高速化します。クローニングは、ハイブリッドクラウド内の任意のデスティネーションで実行できます。

- 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のGUIを使用すると、ハイブリッドクラウド内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一元的に管理できます。

- 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REST APIが含まれており、任意のオーケストレーションソフトウェアと統合できます。また、Windows PowerShellコマンドレットやコマンドラインインターフェイスも使用できます。

  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"。

- データ保護のダッシュボードとレポートの一元化
- セキュリティと委任のためのRole-Based Access Control（RBAC；ロールベースアクセス制御）。
- 高可用性を備えたリポジトリデータベース

  SnapCenterは、高可用性を備えた組み込みのリポジトリデータベースを提供し、すべてのバックアップメタデータを格納します。

- プラグインのプッシュインストールを自動化

  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、外部のロードバランサ（F5）を使用して設定します。同じデータセンター内では、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。

- SnapLock

  SnapLockは、規制やガバナンスに準拠するためにWrite Once、Read Many（WORM）ストレージを使用して変更不可能な状態でファイルを保管する組織向けの、ハイパフォーマンスなコンプライアンス解決策です。

  SnapLockの詳細については、 "SnapLockとは"

- SnapMirrorアクティブ同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）

  SnapMirror Active Syncを使用すると、サイト全体に障害が発生してもビジネスサービスの運用を継続できるため、アプリケーションをセカンダリコピーを使用して透過的にフェイルオーバーできます。SnapMirror Active Syncでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

  この機能でサポートされるプラグインは、SnapCenter Plug-in for SQL Server、SnapCenter Plug-in for Windows、SnapCenter Plug-in for Oracle Database、SnapCenter Plug-in for SAP HANA Database、SnapCenter Plug-in for Microsoft Exchange Server、SnapCenter Plug-in for UNIXです。

  > SnapCenterでホストイニシエータとの近接をサポートするには、この値（sourceまたはdestination）をONTAPで設定する必要があります。

  SnapCenterでサポートされないSnapMirrorアクティブ同期機能：

  - ONTAPでSnapMirrorアクティブ同期関係のポリシーを_automatedfailover_to_automatedfailoverduplex_inから変更して、既存の非対称SnapMirrorアクティブ同期ワークロードを対称に変換する場合、SnapCenterでも同じ処理はサポートされません。
  - リソースグループ（SnapCenterですでに保護されている）のバックアップがある場合に、ONTAPのアクティブなSnapMirror同期関係のストレージポリシー

が_automatedfailover_to_automatedfailoverduplex_inから変更された場合、SnapCenterでも同じ設定はサポートされません。

SnapMirrorアクティブ同期の詳細については、 "SnapMirror Active Syncの概要"

SnapMirrorのアクティブな同期を行うには、ハードウェア、ソフトウェア、およびシステム構成に関するさまざまな要件を満たしている必要があります。詳細については、 "前提条件"

- 同期ミラーリング

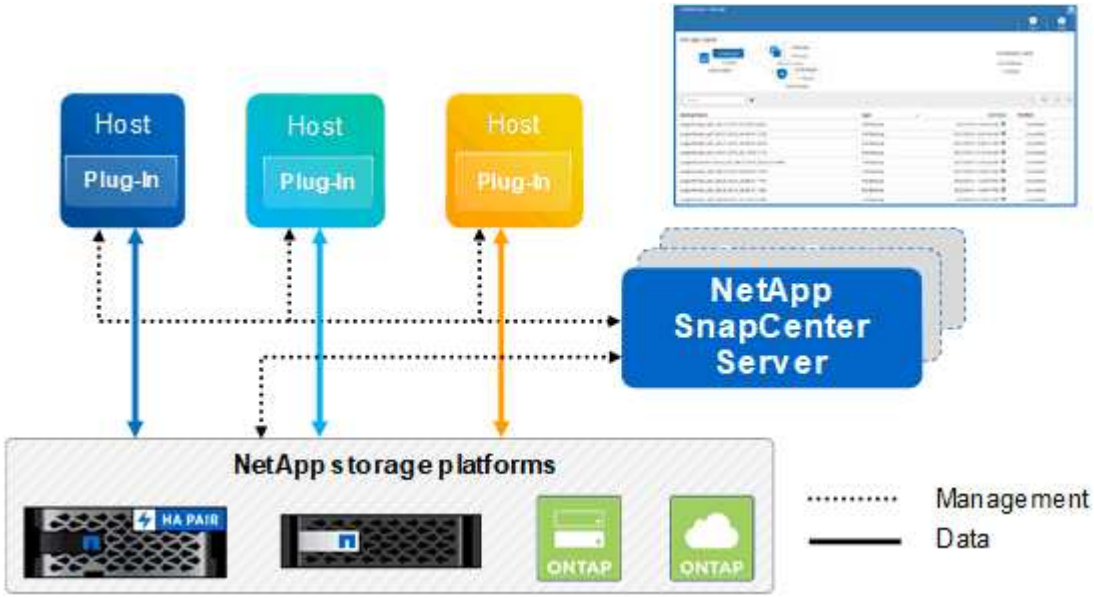
  同期ミラーリング機能は、遠隔地にあるストレージアレイ間で、オンラインのリアルタイムデータレプリケーションを提供します。

  同期ミラーの詳細については'を参照してください "同期ミラーリングの概要"

SnapCenterのアーキテクチャ

SnapCenterプラットフォームは、一元管理サーバ（SnapCenterサーバ）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ます。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できます。



SnapCenterコンポーネント

SnapCenterは、SnapCenter ServerプラグインとSnapCenterプラグインで構成されています。保護するデータに適したプラグインのみをインストールしてください。

- 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
  - Microsoft Windows用SnapCenterプラグイン

- SnapCenter Plug-in for Microsoft Exchange Server
- SAP HANAデータベース向けSnapCenterプラグイン
- IBM DB2用SnapCenterプラグイン
- PostgreSQL向けSnapCenterプラグイン
- MySQL用SnapCenterプラグイン

- SnapCenter Plug-ins Package for 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
  - UNIXファイルシステム用SnapCenterプラグイン
  - IBM DB2用SnapCenterプラグイン
  - PostgreSQL向けSnapCenterプラグイン
  - MySQL用SnapCenterプラグイン
- SnapCenter Plug-ins Package for AIXには、次のプラグインが含まれています。
  - SnapCenter Plug-in for Oracle Database
  - UNIXファイルシステム用SnapCenterプラグイン
- SnapCenter NetAppでサポートされるプラグイン

SnapCenter Plug-in for VMware vSphere（旧NetAppデータブローカー）は、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、SnapCenterリポジトリが含まれています。

SnapCenter Serverは、Microsoft WindowsとLinuxの両方をサポートしています（RHEL 8.x、RHEL 9.x 、SLES 15 SP5）。

SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXを使用する場合、スケジュールはQuartzスケジューラを使用して一元的に実行されます。

- 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サーバおよびプラグインは、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は、Windowsホスト用に分離されたネームスペースをサポートします。分離ネームスペースの使用時に問題が発生した場合は、を参照してください "分離されたネームスペースを使用しているときにSnapCenterでリソースを検出できない"。

Linuxホストで実行されているSnapCenterコンポーネントのステータスを確認するには、次のコマンドを実行する必要があります。

- `systemctl status snapmanagerweb`
- `systemctl status scheduler`
- `systemctl status smcore`
- `systemctl status nginx`
- `systemctl status rabbitmq-server`

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、アプリケーションをサポートします。

プラグイン名	インストールパッケージに含まれる	他のプラグインが必要	ホストにインストール済み	サポートされているプラットフォーム
SQL Server用プラグイン	Plug-ins Package for Windows	Plug-in for Windows	SQL Serverホスト	ウィンドウ
Plug-in for Windows	Plug-ins Package for Windows		Windowsホスト	ウィンドウ
Plug-in for Exchange	Plug-ins Package for Windows	Plug-in for Windows	Exchange Serverホスト	ウィンドウ
Oracleデータベース向けプラグイン	Plug-ins Package for LinuxおよびPlug-ins Package for AIX	Plug-in for UNIX のこと	Oracleホスト	LinuxまたはAIX
SAP HANAデータベース向けプラグイン	Plug-ins Package for LinuxおよびPlug-ins Package for Windows	Plug-in for UNIXまたはPlug-in for Windows	HDBSQLクライアントホスト	LinuxまたはWindows
カスタムプラグイン	Plug-ins Package for LinuxおよびPlug-ins Package for Windows	ファイルシステムノハツクアツフ、Plug-in for Windows	カスタムアプリケーションホスト	LinuxまたはWindows
IBM DB2用プラグイン	Plug-ins Package for LinuxおよびPlug-ins Package for Windows	Plug-in for UNIXまたはPlug-in for Windows	DB2ホスト	LinuxまたはWindows

プラグイン名	インストールパッケージに含まれる	他のプラグインが必要	ホストにインストール済み	サポートされているプラットフォーム
PostgreSQL用プラグイン	Plug-ins Package for LinuxおよびPlug-ins Package for Windows	Plug-in for UNIXまたはPlug-in for Windows	PostgreSQLホスト	LinuxまたはWindows
MySQL用プラグイン	Plug-ins Package for LinuxおよびPlug-ins Package for Windows	Plug-in for UNIXまたはPlug-in for Windows	Db2MySQL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）のcrash-consistentおよびvm-consistentバックアップおよびリストア処理をサポートします。また、SnapCenterアプリケーション固有のプラグインをサポートして、仮想データベースおよびファイルシステムの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 Plug-in for VMware vSphere 4.1.1のドキュメントには、SnapCenter 4.1.1のユーザ向けに、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。NetAppデータブローカー1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetAppデータブローカー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を使用した仮想データベースおよび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。には、SnapCenter 4.3以降を使用しているユーザ向けに "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（オープン仮想アプライアンス形式）を使用した仮想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 Plug-in for Microsoft SQL Serverの機能

- SnapCenter環境で使用するMicrosoft SQL Serverデータベースのアプリケーション対応のバックアップ、リストア、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上のMicrosoft SQL Serverデータベースおよび Raw Device Mapping（RDM；rawデバイスマッピング）LUN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の機能

- 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実現
- SnapCenter環境内のMicrosoftファイルシステムに対するアプリケーション対応のバックアップ、リストア、クローニングの処理を自動化
- Windowsホストのストレージプロビジョニング、整合性のあるSnapshot、スペース再生をサポート

Plug-in for Windowsは、物理LUNとRDM LUNにSMB共有とWindowsファイルシステムをプロビジョニングしますが、SMB共有上の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の機能

- SnapCenter環境のMicrosoft Exchange ServerデータベースとDatabase Availability Group（DAG；データベース可用性グループ）に対して、アプリケーション対応のバックアップ処理とリストア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、RDM LUN上の仮想Exchange Serverがサポートされます。

SnapCenter Plug-in for Oracle Database の特長

- アプリケーション対応のバックアップ、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処理とクローニング処理
- 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の機能

- 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、Plug-in for Oracle DatabaseでOracleデータベースのデータ保護処理を実行できます。
- ONTAPを実行してい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）プロトコルと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システムでは、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録すると、VMDKおよびRDM LUN上のOracleデータベースがサポートされます。
- SANファイルシステムでのAIX用マウントガードとLVMレイアウトをサポートします。
- SANファイルシステムでのインラインロギングとAIXシステムでのLVMレイアウトでの拡張ジャーナルファイルシステム（JFS2）のみをサポートします。

  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レイアウトがサポートされます。

- SnapCenter環境でのUNIXファイルシステムに対するアプリケーション対応のバックアップ、リストア、クローニングの処理を自動化

SnapCenter Plug-in for SAP HANA Databaseの特長

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

NetAppでサポートされるプラグイン機能

- 他のプラグインをサポートして、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します。NetAppでサポートされるプラグインは、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を使用したカスタムアプリケーションで、必要に応じてSnapCenter Plug-in for Microsoft Windowsを使用してファイルシステムの整合性のあるバックアップを作成できます。

NetAppでは、サポートされているプラグインの作成と使用がサポートされていますが、作成するプラグインはNetAppでサポートされていません。

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"

IBM DB2用SnapCenterプラグイン

SnapCenter環境でのIBM DB2データベースのアプリケーション対応のバックアップ、リストア、クローニングを自動化します。

PostgreSQL向けSnapCenterプラグイン

SnapCenter環境で、アプリケーションに対応したPostgreSQLインスタンスのバックアップ、リストア、クローニングを自動化します。

MySQL用SnapCenterプラグイン

SnapCenter環境でのMySQLインスタンスの、アプリケーションに対応したバックアップ、リストア、クローニングを自動化します。

SnapCenterリポジトリ

SnapCenterリポジトリ（NSMデータベースと呼ばれることもあります）には、すべてのSnapCenter処理の情報とメタデータが格納されます。

MySQLサーバリポジトリデータベースは、SnapCenterサーバ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サーバーがすでにインストールされていて、SnapCenterサーバーを新規インストールする場合は、MySQLサーバー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 8.0.37以降がサポートされます。以前のリリースのSnapCenterで以前のバージョンのMySQL Serverを使用していた場合は、SnapCenterのアップグレード時に、MySQL Serverが8.0.37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CA証明書の使用がサポートされています。
- SnapCenter 4.1.1以降では、ONTAPとの通信にTransport Layer Security（TLS）1.2がサポートされています。クライアントとサーバ間の通信にもTLS 1.2を使用できます。

  5.0以降、SnapCenterはONTAPとの通信用に(TLS) 1.3をサポートしています。

- SnapCenterは、ネットワーク通信全体のセキュリティを提供するために、特定のSSL暗号スイートのセット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 "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。このトークンは24時間後に期限切れになります。
- 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、SnapCenter on ONTAP for WindowsおよびLinuxホストマシンでサポートされています。 "詳細"です。
- SnapCenter PowerShellコマンドレットはセッションで保護されます。
- 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。ログアウト期間は変更できます。
- ログインに5回以上失敗すると、ログインが一時的に無効になります。
- SnapCenterサーバとONTAP間のCA証明書認証をサポートします。 "詳細"です。
- 整合性検証ツールはSnapCenterサーバとプラグインに追加され、新規インストールおよびアップグレード処理の際に、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サーバインストーラは、インストール中に集中型SSL証明書のサポートを有効にします。SnapCenterでは、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、お客様から提供された承認済み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ファイルの生成"。

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 "証明書の作成とインポート"。

双方向SSL通信

双方向SSL通信は、SnapCenterサーバとプラグイン間の相互通信を保護します。

証明書ベースの認証の概要

証明書ベースの認証は、SnapCenterプラグインホストにアクセスしようとする各ユーザの信頼性を検証します。秘密鍵なしでSnapCenterサーバ証明書をエクスポートし、プラグインホストの信頼されたストアにインポートする必要があります。証明書ベースの認証は、双方向SSL機能が有効になっている場合にのみ機能します。

多要素認証（MFA）

MFAは、Security Assertion Markup Language（SAML）を介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、既存のユーザー名とパスワードとともに、TOTP、生体認証、プッシュ通知などの複数の要素を使用するオプションを持つことで、認証セキュリティを強化します。また、お客様は独自のユーザIDプロバイダを使用して、ポートフォリオ全体で統合ユーザログイン（SSO）を取得できます。

MFAは、SnapCenterサーバUIログインにのみ適用されます。ログインはIdP 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設定できます。SnapCenterはサービスプロバイダであるため、AD FSでSnapCenterを証明書利用者として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のロールベースアクセス制御（RBAC）

RBACノシユルイ

SnapCenterのロールベースアクセス制御（RBAC）とONTAP権限を使用すると、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グループに委譲できます。この一元管理されたアクセスにより、アプリケーション管理者は委任された環境で安全に作業を行うことができます。

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。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ケンケン

SnapCenter RBAC

ロールと権限

SnapCenterには、権限が割り当てられた事前定義されたロールが付属していますこれらのロールには、ユーザまたはユーザ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ロールの権限を変更することはできません。

RBACの権限は、同じフォレスト内のユーザとグループ、および異なるフォレストに属するユーザに割り当てることができます。フォレスト間でネストされたグループに属するユーザにRBAC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が含まれている必要があります。Host addやHost removeなど、一部の権限のみをコピーした場合は、それらの処理を実行できません。

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、ログイン時に認証を指定する必要があります。ユーザが複数のロールのメンバーである場合は、ログインクレデンシャルを入力すると、使用するロールを指定するように求められます。また、APIを実行するための認証も必要です。

アプリケーションレベルの**RBAC**

SnapCenterは、クレデンシャルを使用して、許可されたSnapCenterユーザがアプリケーションレベルの権限も持っていることを確認します。

たとえば、SQL Server環境でSnapshot処理やデータ保護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、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。Windowsファイルシステム環境でONTAPストレージ上でSnapshot処理とデータ保護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admin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に、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、操作に応じて、次のいずれかの方法を使用して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は、vCenter ServerでRBACをさらに強化できます。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。

詳しくは、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ケンケン

ストレージシステムへのアクセスに必要な権限を持つ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Role-Based Access Control（RBAC；ロールベースアクセス制御）を使用すると、ロールを作成して権限を割り当て、そのロールにユーザまたはユーザ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。

- アプリケーションのバックアップとクローンの管理
- バックアップ/クローンビューア
- インフラ管理者
- SnapCenterAdmin

SnapCenter Plug-in for VMware vSphere のロール

VM、VMDK、およびデータストアのVMと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では次のロールがvCenterで作成されます。

- 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ユーザ向けの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。
- 移行
- Mount（Oracleデータベースのみ）
- unmount（Oracleデータベースのみ）
- ジョブモニタ

  Job Monitor権限を使用すると、さまざまなロールのメンバーは、割り当てられているすべてのオブジェクトに対する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）を設定および管理する場合は、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、アプリケーションの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あります。このロールには、ホスト管理、プロビジョニング、ストレージ接続管理、またはリモートインストールに関する権限はありません。

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
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

権限	有効	作成	読み取り	更新	削除
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/アンインストール	いいえ	該当なし		該当なし	該当なし
移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウントする	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
ジョブモニタ	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、すべての権限が読み取り専用で表示されます。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

権限	有効	作成	読み取り	更新	削除
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/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
移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウントする	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
ジョブモニタ	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、ホスト管理、ストレージ管理、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レポート、 をクリックし、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

権限	有効	作成	読み取り	更新	削除
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/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
移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウントする	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
ジョブモニタ	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。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 "SnapCenterサーバのディザスタリカバリ用のREST APIワークフロー"
- 監査設定関連の構成ファイルは、リストア処理後にDRバックアップにも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が停止したら、別のSQLホストに切り替えて、いくつかの手順を実行してデータをリカバリします。を参照して "SnapCenter Plug-in for SQL Serverのディザスタリカバリ"

SnapCenterでは、ONTAP 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、同期を維持するために使用できます。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で開始できます。フェイルバック中は同期を元に戻し、DRサイトのデータをプライマリサイトにレプリケートできます。

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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- * 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もあります。

- * 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、複数のホストと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できます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを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た場合、同じ共有リソースグループにスケジュールが関連付けられていると、その共有リソースグループの他のすべてのホストでスケジュールされたすべての処理が中断されます。

  データベースのバックアップにはデータベースプラグイン、ファイルシステムのバックアップにはファイルシステムプラグイン、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。

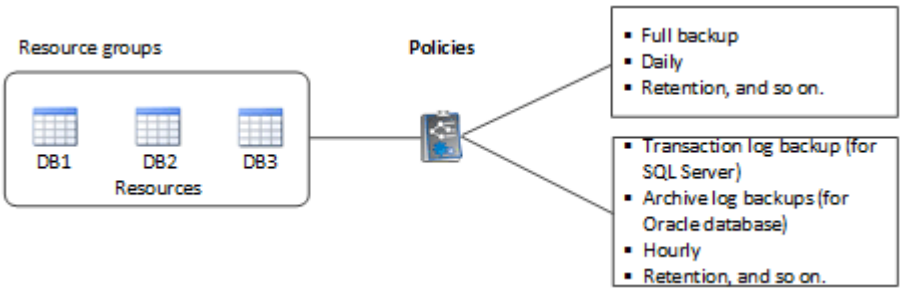
- * ポリシー * では、バックアップ頻度、コピーの保持、レプリケーション、スクリプトなど、データ保護処理の特性を指定します。

リソースグループを作成するときに、そのグループのポリシーを1つ以上選択します。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。

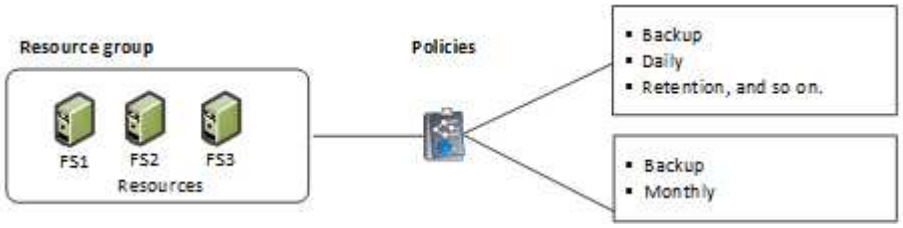
リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、すべてのデータベースまたはホストのすべてのファイルシステムをバックアップする場合は、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソースグループを作成します。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。

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時間ごと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を使用すると、データ保護ジョブの実行前または実行後に自動化を実行できます。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スクリフト

UNIXでは、次の種類のスクリプトがサポートされています。

- Perlスクリフト
- 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-shell、k-shell、c-shellのような他のシェルもサポートされています。

スクリプトパス

仮想化されていないストレージシステムおよび仮想化されたストレージシステムでSnapCenter処理の一環として実行されるプリスクリプトとポストスクリプトは、すべてプラグインホストで実行されます。

- Windowsスクリプトがプラグインホストにある必要があります。

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からの相対パスである必要があります。

- UNIXスクリプトがプラグインホスト上にある必要があります。

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で指定されます。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の作成時に、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。タイムアウト値は変更できます。

スクリプト出力

Windows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のディレクトリは、Windows\System32です。

UNIXのプリスクリプトとポストスクリプトの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。Swagger Webページにアクセスして、REST APIドキュメントを表示したり、APIを手動で呼び出したりできます。REST APIを使用すると、SnapCenterサーバやSnapCenter vSphereホストの管理に役立ちます。

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#

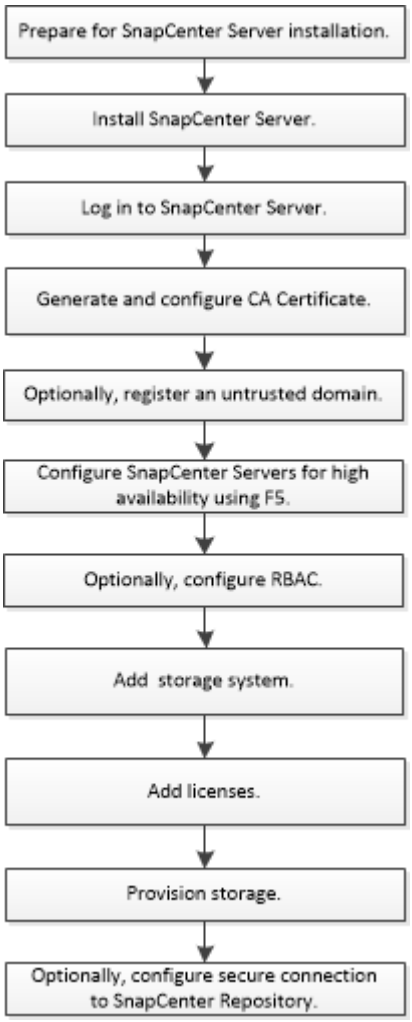
SnapCenter REST APIの詳細については、を参照してください。 "REST APIの概要"

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を示しています。



SnapCenterサーバのインストールの準備

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。ワークグループとドメインの両方の場合、インストールに使用するユーザーには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を持つ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、Active Directoryドメインと信頼に関するMicrosoftの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更新プログラムを適用する必要があります。

項目	**Windows**ホストノヨウケン	**Linux** ホストの要件
オペレーティングシステム	Microsoft Windows 英語版、ドイツ語版、日本語版、簡体字中国語版のみがサポートされています。 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"。	• Red Hat Enterprise Linux（RHEL）8および9 • SUSE Linux Enterprise Server（SLES）15 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"。
最小CPU数	4コア	4コア
最小RAM	8GB MySQL Serverのバッファプールは、RAMの合計容量の20%を使用します。	8GB

項目	**Windows**ホストノヨウケン	**Linux** ホストの要件
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	7GB SnapCenterサーバがインストールされているドライブと同じドライブにSnapCenterリポジトリがある場合は、15 GBを使用することを推奨します。	15GB
SnapCenterリポジトリ用の最小ハードドライブ容量	8GB 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、15GB にすることを推奨します。	該当なし
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • ASP。 Net Core Hosting Bundle（8.0.5以降） • PowerShell 7.4.2以降 用。 NET固有のトラブルシューティング情報。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"	• ASP。 Net Core Runtime 8.0.5 以降 • PowerShell 7.4.2以降 • nginxはリバースプロキシとして使用できるWebサーバ • PAM -デベル PAM（Pluggable Authentication Modules）は、システム管理者が認証を行うプログラムを再コンパイルすることなく認証ポリシーを設定できるシステムセキュリティツールです。

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。

- ホストユーティリティ

  Host UtilitiesはFCとiSCSIをサポートしており、WindowsサーバでMPIOを使用できます。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、NetAppとWindows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とアプリケーション

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は、データを保護するためにONTAP 9 12.1以降をサポートしています。
- SnapCenterはAmazon FSx for NetApp ONTAPをサポートしており、SnapCenterソフトウェア4.5 P1パッチリリースからデータを保護します。

  Amazon FSx for NetApp ONTAPを使用している場合は、データ保護処理を実行するために、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してください。

  Non-Volatile Memory Express（NVMe）over Transport Control Protocol（TCP）をサポートします。

  Amazon FSx for NetApp ONTAP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は、さまざまなアプリケーションやデータベースの保護をサポートしています。

  サポートされているアプリケーションと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"。

- SnapCenter 4.9 P1以降では、Amazon Web Services（AWS）のSoftware-Defined Data Center（SDDC）環境上のVMware Cloudで、OracleとMicrosoft SQLのワークロードの保護がサポートされます。

  詳細については、を参照してください "VMware Cloud on AWS SDDC環境でNetApp SnapCenterを使用してOracleやMS SQLのワークロードを保護"。

サポートされるブラウザ

SnapCenterソフトウェアは複数のブラウザで使用できます。

- Chromeバージョン125以降
- Microsoft Edge 110.0.1587.17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"。

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1つの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に干渉し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。"

ポートのタイプ	デフォルトポート
スケジューラサービスポート	8154（HTTPS） このポートは、SnapCenterサーバホスト内で管理されるすべてのプラグインのSnapCenterスケジューラワークフローを一元的にオーケストレーションするために使用されます。 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。"
RabbitMQポート	5672（TCP） これはRabbitMQがリッスンするデフォルトポートで、スケジューラサービスとSnapCenter間のパブリッシャ/サブスクライバモデル通信に使用されます。
MySQLのポート	3306（HTTPS）、双方向、カスタマイズ可能 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確立できます。 "詳細" 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。"
Windowsプラグインホスト	135、445（TCP） ポート135と445に加えて、Microsoftが指定したダイナミックポート範囲もオープンにする必要があります。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、インストール後に閉じることができます。

ポートのタイプ	デフォルトポート
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 、SnapCenter Plug-ins Package for AIX	8145（HTTPS）、双方向、カスタマイズ可能 このポートは、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、またはを参照してください。 "ホストを追加してSnapCenter Plug-in for Microsoft Windowsをインストールする" "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 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データベースへの接続にOracle用プラグインで使用されます。 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 Plug-in for Exchangeデータベース	909、カスタマイズ可能 デフォルトのNETです。 TCPポートは、Plug-in for WindowsでExchange VSSコールバックに接続するために使用されます。 ポートをカスタマイズするには、を参照してください "ホストを追加してPlug-in for Exchangeをインストールする"。

ポートのタイプ	デフォルトポート
NetAppでサポートされるSnapCenter用プラグイン	9090（HTTPS）、固定 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す。ファイアウォールの例外は必要ありません。 SnapCenterサーバとカスタムプラグインの間の通信は、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）、bidirectional80（HTTP）、bidirectional 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。現在、このポートは、SnapCenterプラグインホストとSVMの間の通信にSnapCenter for Windows Plug-inホストの SALでも使用されています。
SnapCenter Plug-in for SAP HANA Database vCodeのスペルチェックポート	3instance_number13または3instance_number15、HTTPまたはHTTPS、双方向、カスタマイズ可能 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、ポート番号は13で終わります。MDC以外の場合、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。"
ドメインコントローラの通信ポート	認証が正しく機能するために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については、Microsoftのドキュメントを参照してください。 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には、を参照してください "プラグインホストの変更"。

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、仮想マシンの

データ保護を実現するために複数のライセンスが必要です。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。

ライセンス	必要な場合
SnapCenter Standard（コントローラベース）	FAS、AFF、オールSANアレイ（ASA）に必要 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 Suiteライセンスをお持ちの場合は、SnapCenter Standardライセンスの使用権も取得できます。FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールする場合は、営業担当者に連絡してPremium Bundleの評価ライセンスを取得してください。 SnapCenterは、Data Protection Bundleの一部としても提供されます。A400以降を購入済みの場合は、Data Protection Bundleを購入する必要があります。
SnapMirrorまたはSnapVault	ONTAP SnapCenterでレプリケーションが有効になっている場合は、SnapMirrorまたはSnapVaultのいずれかのライセンスが必要です。
SnapRestore	バックアップのリストアと検証に必要です。 フライマリストレエシシステム • リモート検証を実行し、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には、SnapMirrorデスティネーションシステムに必要です。

ライセンス	必要な場合
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。 フライマリストレシシステムトセカンタリストレシシステム • セカンダリバックアップからクローンを作成するには、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のiSCSIまたはFCライセンス • SMB共有用のCIFSライセンス • NFSタイプのVMDK用のNFSライセンス • 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使用できない場合に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。
SnapCenter Standard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 Standard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で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。Amazon FSx for NetApp ONTAPおよびCloud Volumes ONTAPでは、容量ベースのライセンスは不要になりました。Azure NetApp Filesには標準ライセンスと容量ベースライセンスは必要ありません。

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 Standardコントローラベースライセンスを追加"。

Single Mailbox Recovery（SMBR）ライセンス

SnapCenter Plug-in for Exchangeを使用してMicrosoft Exchange Serverデータベースおよび Single Mailbox Recovery（SMBR）を管理する場合は、SMBR用の追加ライセンスが必要です。このライセンス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。

登録して**SnapCenter**ソフトウェアにアクセス

Amazon FSx for NetApp ONTAPまたはAzure NetApp Filesを初めて使用し、既存のNetAppアカウントを持っていない場合は、SnapCenterソフトウェアにアクセスできます。

開始する前に

- 会社のEメールIDにアクセスできる必要があります。
- Azure NetApp Filesを使用している場合は、AzureサブスクリプションIDが必要です。
- Amazon FSx for NetApp ONTAPを使用している場合は、FSx for ONTAPファイルシステムのファイルシステムIDが必要です。

タスクの内容

登録には情報が検証される必要があります。新しいNetAppサポートサイト（NSS）アカウントの確認とアップグレードが完了するまで、「ゲスト」から「フル」アクセスになるまで、最大1日かかる場合があります。

手順

1. をクリックし https://mysupport.netapp.com/site/user/registration て登録します。
2. 会社のEメールアドレスを入力し、キャプチャを完了してネットアップのプライバシーポリシーに同意し、*[送信]*をクリックします。
3. EメールIDに送信されたOTPを入力して登録を認証し、* Continue *をクリックします。
4. 登録完了ページで、以下の詳細を入力して登録を完了します。
   a. NetApp Customer/End User *を選択します。
   b. [Serial Number]フィールドに、次のいずれかを入力します。
      - Azure NetApp Filesを使用している場合はAzureサブスクリプションID。
      - ファイルシステムID（Amazon FSx for NetApp ONTAPを使用している場合）。

登録中に問題が発生した場合、またはステータスを確認する場合は、でチケットを発行できます https://mysupport.netapp.com/site/help 。

クレデンシャルの認証方式

クレデンシャルで使用される認証方法は、アプリケーションや環境に応じて異なります。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に使用するクレデンシャルとデータ保護処理に使用するクレデンシャルをそれぞれ1組ずつ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。

信頼されていないドメイン認証

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に対するWindows認証は、Windowsクレデンシャルの作成時に実行されるのではなく、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完了し、リソースを更新する必要があります。SQL Server認証は、SQL Serverでのスケジュール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 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、AIXホストを追加し、SnapCenter Plug-ins Package for AIXをSnapCenter GUIからリモートで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）認証が無効になっている場合は、Oracleデータベースで処理を実行するためにOracleデータベース認証が必要になります。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インスタンスにアクセスする必要があり、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は、Oracle ASM認証が必要です。そのため、Oracle ASMの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ユーザを作成しておく必要があります。

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た場合は、RMANカタログ認証を追加する必要があります。

ストレージ接続とクレデンシャル

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サーバと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 *

  ストレージ接続により、SnapCenter ServerプラグインとSnapCenterプラグインはONTAPストレージにアクセスできます。これらの接続の設定には、AutoSupportおよび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。ユーザ名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、ユーザ名に完全なadmin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の権限を割り当てる必要があります。

多要素認証（MFA）

多要素認証（**MFA**）を管理します。

Active Directoryフェデレーションサービス（AD FS）サーバとSnapCenterサーバで多要素認証（MFA）機能を管理できます。

多要素認証（**MFA**）を有効にする

SnapCenterサーバのMFA機能は、PowerShellコマンドを使用して有効にできます。

タスクの内容

- 同じAD FSで他のアプリケーションが設定されている場合、SnapCenterはSSOベースのログインをサポートします。一部のAD FS構成では、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"。

開始する前に

- 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サーバと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にする必要があります。
- SnapCenterサーバ用に許可された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）中に自己署名証明書が再作成されないようにすることで、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ファイルの生成"。

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. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。
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パラメータには、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ホストにコピーして、SnapCenterをクライアントエンティティとして設定します。
7. コマンドレットを使用して、SnapCenterサーバのMFAを有効にします `Set-SmMultiFactorAuthentication` 。
8. （オプション）コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。
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. Permissionsウィザードで、次の手順を実行します。
      i. [追加]*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。

       SnapCenterが、指定した表示名の証明書利用者として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. [Endpoints]、[Identifiers]、および[Signature]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メタデータの更新

アップグレード、CA証明書の更新、DRなど、AD FSサーバで変更があった場合は、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. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。"

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で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メタデータの更新

ADFSサーバで修復、CA証明書の更新、DRなどの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。

      証明書利用者信頼のユーザ定義名が表示されます。

   c. 多要素認証（MFA）を有効にします。

      を参照して "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、コマンドレットを使用して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` 。
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。

REST API、**PowerShell**、**SCCLI**を使用して多要素認証（**MFA**）を管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIからサポートされます。MFAは、AD FSアイデンティティマネージャを介してサポートされます。GUI、REST API、PowerShell、SCCLIを使用して、MFAの有効化、MFAの無効化、およびMFAの設定を行うことができます。

AD FSを**OAuth/OIDC**としてセットアップします

- Windows GUIウィザードを使用してAD FSを構成します*
  1. Server Manager Dashboard **>** Tools **>** ADFS Management *に移動します。
  2. **>**[アプリケーショングループ]*に移動します。
     a. [アプリケーショングループ]を右クリックします。
     b. を選択し、[アプリケーション名]*と入力します。
     c. [サーバーアプリケーション]*を選択します。
     d. 「 * 次へ * 」をクリックします。
  3. コピー*クライアントID *。

     これはクライアントIDです。..リダイレクトURLにコールバックURL（SnapCenterサーバURL）を追加します。..「 * 次へ * 」をクリックします。

  4. [Generate shared secret]*を選択します。

     シークレット値をコピーします。これはクライアントの秘密です。..「 * 次へ * 」をクリックします。

5. [概要]ページで、*[次へ]*をクリックします。
   a. [完了]ページで、*[閉じる]*をクリックします。
6. 新しく追加した*アプリケーショングループ*を右クリックし、*プロパティ*を選択します。
7. [アプリケーションのプロパティ]から*[アプリケーションの追加]*を選択します。
8. [アプリケーションの追加]*をクリックします。

   [Web API]を選択し、*[Next]*をクリックします。

9. [Web APIの構成]ページで、前の手順で作成したSnapCenterサーバのURLとクライアント識別子を[識別子]セクションに入力します。
   a. [追加]*をクリックします。
   b. 「 * 次へ * 」をクリックします。
10. [Choose Access Control Policy]ページで、要件に基づいて制御ポリシーを選択し（[Permit Everyone and Require MFA]など）、*[Next]*をクリックします。
11. [アプリケーション権限の設定]ページでは、デフォルトでOpenIDがスコープとして選択されており、*[次へ]*をクリックします。
12. [概要]ページで、*[次へ]*をクリックします。

    [完了]ページで、*[閉じる]*をクリックします。

13. [サンプルアプリケーションのプロパティ]ページで、*[OK]*をクリックします。
14. 承認サーバー(AD FS)によって発行され、リソースによって消費されることを意図したJWTトークン。

    このトークンの「AUD」またはオーディエンス要求は、リソースまたはWeb APIの識別子と一致している必要があります。

15. 選択したWebAPIを編集し、コールバックURL（SnapCenterサーバURL）とクライアント識別子が正しく追加されていることを確認します。

    ユーザー名を要求として提供するようにOpenID Connectを設定します。

16. サーバーマネージャの右上にある* Tools メニューの下にある AD FS Management *ツールを開きます。
    a. 左側のサイドバーから* Application Groups *フォルダを選択します。
    b. Web APIを選択し、* edit *をクリックします。
    c. [発行トランスフォームルール]タブに移動します
17. [* ルールの追加 *] をクリックします。
    a. [Claim rule template]ドロップダウンで、*[Send LDAP Attributes as Claims]*を選択します。
    b. 「 * 次へ * 」をクリックします。
18. [Claim rule]*の名前を入力します。
    a. [属性ストア]ドロップダウンで*[Active Directory]*を選択します。
    b. [LDAP Attribute]ドロップダウンで*を選択し、**[O*utgoing Claim Type]***ドロップダウンで[UPN]*を選択します。

c. [完了] をクリックします。

PowerShellコマンドを使用してアプリケーショングループを作成します

PowerShellコマンドを使用して、アプリケーショングループ、Web APIを作成し、スコープと要求を追加できます。これらのコマンドは、自動スクリプト形式で使用できます。詳細については、<link to KB article>を参照してください。

1. 次のコマンドを使用して、AD FSに新しいアプリケーショングループを作成します。

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier` アプリケーショングループの名前

`redirectURL` 許可後のリダイレクションの有効なURL

2. AD FSサーバアプリケーションを作成し、クライアントシークレットを生成します。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
-Identifier $identifier -GenerateClientSecret
```

3. ADFS Web APIアプリケーションを作成し、使用するポリシー名を設定します。

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. クライアントIDとクライアントシークレットは1回しか表示されないため、次のコマンドの出力から取得します。

```
"client_id = $identifier"

"client_secret: "$($ADFSApp.ClientSecret)
```

5. AD FSアプリケーションにallatclaims権限とOpenID権限を付与します。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
```

```
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 変換ルールファイルを書き出します。

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Web APIアプリケーションに名前を付け、外部ファイルを使用してその発行トランスフォームルールを定義します。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

アクセストークンの有効期限を更新します

アクセストークンの有効期限は、PowerShellコマンドを使用して更新できます。

- このタスクについて *
- アクセストークンは、ユーザー、クライアント、およびリソースの特定の組み合わせに対してのみ使用できます。アクセストークンは無効にすることはできず、有効期限が切れるまで有効です。
- デフォルトでは、アクセストークンの有効期限は60分です。この最小限の有効期限は十分であり、拡張されています。ビジネスクリティカルなジョブが継続的に発生しないように、十分な価値を提供する必要があります。
- ステップ *

アプリケーショングループWebAPIのアクセストークンの有効期限を更新するには、AD FSサーバで次のコマンドを使用します。

+
```
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

AD FSから**Bearer**トークンを取得します

RESTクライアント（Postmanなど）で以下のパラメータを入力する必要があり、ユーザクレデンシャルを入力するように求められます。さらに、ベアラートークンを取得するには、第2要素認証(あなたが持っているものとあなたがいるもの)を入力する必要があります。

+ベアラートークンの有効期間は、アプリケーションごとにAD FSサーバから設定できます。デフォルトの有

効期間は60分です。

フィールド	値
付与タイプ	承認コード
コールバックURL	コールバックURLがない場合は、アプリケーションのベースURLを入力します。
認証URL	[ADFS-domain-name]/ADFS/OAuth2/authorize
アクセストークンURL	[ADFS-domain-name]/ADFS/OAuth2/token
クライアントID	AD FSクライアントIDを入力します
クライアントシークレット	AD FSクライアントシークレットを入力します
適用範囲	OpenID
クライアント認証	基本認証ヘッダーとして送信します
リソース	[詳細オプション]タブで、[コールバックURL]と同じ値を持つ[リソース]フィールドを追加します。この値は、JWTトークンでは「AUD」値として表示されます。

PowerShell、**SCCLI**、**REST API**を使用して**SnapCenter**サーバで**MFA**を設定します

SnapCenter Serverでは、PowerShell、SCCLI、およびREST APIを使用してMFAを設定できます。

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレット（Open-SmConnection）を「AccessToken」というもう1つのフィールドで拡張し、ベアラートークンを使用してユーザを認証します。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

上記のコマンドレットを実行すると、それぞれのユーザがSnapCenterコマンドレットを実行できるようにセッションが作成されます。

SnapCenter MFA REST API認証

REST <access token>クライアント(Postmanやswaggerなど)でBearerトークンを_Authorization = Bearer _の形式で使用し、ヘッダーにユーザRoleNameを指定すると、SnapCenterからの応答が成功します。

MFA REST APIワークフロー

MFAがAD FSで設定されている場合、REST APIを使用してSnapCenterアプリケーションにアクセスするには、アクセス（Bearer）トークンを使用して認証する必要があります。

- このタスクについて *
- Postman、Swagger UI、FireCampなど、任意のRESTクライアントを使用できます。
- アクセストークンを取得し、それを使用して以降の要求（SnapCenter REST API）を認証し、あらゆる処理を実行します。
- 手順 *
- AD FS MFAを介して認証する場合*

1. AD FSエンドポイントを呼び出してアクセストークンを取得するようにRESTクライアントを設定します。

   ボタンを押してアプリケーションのアクセストークンを取得すると、AD FS SSOページにリダイレクトされ、ADクレデンシャルを入力してMFAで認証する必要があります。1.[AD FS SSO]ページで、[Username]テキストボックスにユーザ名または電子メールを入力します。

+ユーザ名は、user@domainまたはdomain\userの形式で指定する必要があります。

1. [パスワード]テキストボックスにパスワードを入力します。
2. *ログイン*をクリックします。
3. [サインインオプション]*セクションで、認証オプションを選択し、（設定に応じて）認証します。
   - プッシュ：電話機に送信されるプッシュ通知を承認します。
   - QRコード: AUTH Pointモバイルアプリを使用してQRコードをスキャンし、アプリに表示される認証コードを入力します
   - ワンタイムパスワード:トークンのワンタイムパスワードを入力します。
4. 認証が成功すると、Access、ID、およびRefresh Tokenを含むポップアップが開きます。

   アクセストークンをコピーし、SnapCenter REST APIで使用して操作を実行します。

5. REST APIでは、ヘッダーセクションでアクセストークンとロール名を渡す必要があります。
6. SnapCenterは、AD FSからこのアクセストークンを検証します。

   有効なトークンである場合、SnapCenterはそれをデコードし、ユーザー名を取得します。

7. SnapCenterは、ユーザ名とロール名を使用して、API実行のためにユーザを認証します。

   認証に成功した場合、SnapCenterは結果を返します。成功しなかった場合は、エラーメッセージが表示されます。

REST API、**CLI**、**GUI**の**SnapCenter MFA**機能を有効または無効にします

- GUI *
- 手順 *

1. SnapCenter管理者としてSnapCenterサーバにログインします。
2. **>**[グローバル設定]**>**[MultiFactorAuthentication（MFA）設定]*をクリックします
3. インターフェイス（GUI/RST API/CLI）を選択してMFAログインを有効または無効にします。

- PowerShellインターフェイス*
- 手順 *

1. PowerShellまたはCLIコマンドを実行して、GUI、REST API、PowerShell、SCCLIのMFAを有効にします。

   ```
   Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
   -IsCliMFAEnabled -Path
   ```

   pathパラメータは、AD FS MFAメタデータXMLファイルの場所を指定します。

指定したAD FSメタデータファイルパスを使用して設定されたSnapCenter GUI、REST API、PowerShell、およびSCCLIのMFAを有効にします。

1. コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。

- SCCLIインターフェイス*
- 手順 *

1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. `# sccli Get-SmMultiFactorAuthentication`

- REST API *

1. GUI、REST API、PowerShell、SCCLIでMFAを有効にするには、次のPOST APIを実行します。

パラメータ	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
リクエストボディ	{"IsGuiMFAEnabled"：false、"IsRestApiMFAEnabled"：true、"IsCliMFAEnabled"：false、"ADFSConfigFilePath"："C:\\ADFS_METADATA\\abc.xml"}

応答本文	{"MFAConfiguration"： {"IsGuiMFAEnabled "：false、"ADFSConfigFilePath"："C：\\ADFS_METADATA\\abc.xml"、"SCConfigFilePath"：null、"IsRestApiMFAEnabled"：true、"IsCliMFAEnabled"：false、 "ADFSHostName"：" win-adfs-sc49.winscedom2.com}

2. 以下のAPIを使用してMFA構成のステータスと設定を確認します。

パラメータ	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	取得
応答本文	{"MFAConfiguration"： {"IsGuiMFAEnabled "：false、"ADFSConfigFilePath"："C：\\ADFS_METADATA\\abc.xml"、"SCConfigFilePath"：null、"IsRestApiMFAEnabled"：true、"IsCliMFAEnabled"：false、 "ADFSHostName"：" win-adfs-sc49.winscedom2.com}

WindowsホストへのSnapCenterサーバのインストール

SnapCenterサーバインストーラの実行可能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、いくつかのインストールと設定の手順を実行できます。

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。

開始する前に

- SnapCenterサーバホストにWindowsの更新プログラムが適用されていて、システムの再起動が保留されていないことが必要です。
- 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。

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

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サーバインストールパッケージをダウンロードし "NetAppサポートサイト"ます。
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サーバのインストールを開始します。

   インストールを開始すると、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。

   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、エラーは修正する必要があります。

3. SnapCenterサーバのインストールに必要な値があらかじめ入力されていることを確認し、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中に、パスワードが自動的に生成されます。

   パスに特殊文字「%」が含まれ%`" is not supported in the custom path for the repository database. If you include "`ていると、インストールが失敗します。

4. [今すぐインストール] をクリックします。

   無効な値を指定した場合は、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、管理者ユーザの%temp%フォルダに（古いものから順に）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サーバのインストールを開始します。`C:\installer_location\installer_name.exe /log"C:\"`

製品を登録してサポートを有効にする

NetApp製品を初めてご利用になり、既存のNetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

手順

1. SnapCenterのインストール後、*[ヘルプ]>[バージョン情報]*に移動します。
2. [_About SnapCenter _]ダイアログボックスで、971で始まる20桁のSnapCenterインスタンスをメモします。
3. をクリックします https://register.netapp.com
4. [* I am not a registered NetApp Customer*] をクリックします。
5. 自分自身を登録するには、詳細を指定してください。

6. NetApp Reference SNフィールドは空白のままにします。
7. [Product Line]ドロップダウンから[* SnapCenter *]を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. [Submit （送信）] をクリックします。

LinuxホストへのSnapCenterサーバのインストール

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

開始する前に

- SnapCenterをインストールするための十分な権限がないroot以外のユーザを使用してSnapCenterサーバをインストールする場合は、NetAppサポートサイトからsudoersチェックサムファイルを入手してください。Linuxのバージョンに基づいて適切なチェックサムファイルを使用する必要があります。
- のインストール中。 NETランタイム。インストール時に_libicu_libraryの依存関係の解決に失敗した場合は、次のコマンドを実行してinstall_libicu_を実行します。 `yum install -y libicu`
- _perl_が使用できないためにSnapCenterサーバのインストールが失敗した場合は、次のコマンドを実行してinstall_perl_をインストールします。 `yum install -y perl`
- SUSE Linuxでsudoパッケージを使用できない場合は、認証エラーを回避するためにsudoパッケージをインストールします。
- SUSE Linuxの場合は、インストールの失敗を回避するためにホスト名を設定します。
- コマンドを実行して、セキュアなLinuxのステータスを確認します `sestatus`。SELinux status_が「enabled」で、_current mode_が「enforcing」の場合は、次の手順を実行します。
  - 次のコマンドを実行します。 `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    _webapp_external_port_のデフォルト値は8146です。
  - ファイアウォールがポートをブロックしている場合は、 `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    _webapp_external_port_のデフォルト値は8146です。
  - 読み取りおよび書き込み権限があるディレクトリから、次のコマンドを実行します。
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

      コマンドから「Nothing to do」が返された場合は、SnapCenterサーバのインストール後にコマンドを再実行します。
    - コマンドがcreates_my-nginx.pp_を作成する場合は、コマンドを実行してポリシーパッケージをアクティブにします。 `sudo semodule -i my-nginx.pp`
  - MySQL PIDディレクトリに使用されるパスは_/ var/opt/mysqld_です。次のコマンドを実行して、MySQLインストールの権限を設定します。

- `mkdir /var/opt/mysqld`
- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
- `sudo restorecon -Rv /var/opt/mysqld`

◦ MySQLのデータディレクトリのパスは、_/ INSTALL_DIR /NetApp/snapcenter/SnapManagerWeb/Repository/mysql/_です。次のコマンドを実行して、MySQLのデータディレクトリの権限を設定します。

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

タスクの内容

- SnapCenterサーバをLinuxホストにインストールすると、MySQL、RabbitMQ、Errlangなどのサードパーティサービスがインストールされます。アンインストールしないでください。
- Linuxホストにインストールされ ているSnapCenterサーバは、次の機能をサポートしていません。
  - 高可用性
  - Windowsプラグイン
  - Active Directory（Credを使用するrootユーザとroot以外のユーザの両方で、ローカルユーザのみをサポート）
  - SnapCenterへのログインに使用するキーベースの認証

手順

1. 次のファイルをから_/ホームディレクトリ_にダウンロードし "NetAppサポートサイト" ます。
   - SnapCenterサーバインストールパッケージ-* snapcenter-linux-server-(el8/el9/sles15).bin*
   - 公開キーファイル-* snapcenter_public_key.pub *
   - それぞれのシグネチャファイル-* snapcenter-linux-server-(el8/el9/sles15).bin.sig*
2. 署名ファイルを検証します。
   `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. root以外のユーザをインストールする場合は、.binインストーラとともに* snapcenter_server_checksum_（el8/el9/sles15）.txt *で指定したvisudoコンテンツを追加します。
4. .binインストーラの実行権限を割り当てます。
   `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. いずれかの操作を実行して、SnapCenterサーバをインストールします。

実行する処理	操作
対話型インストール	`./snapcenter-linux-server-(el8/el9/sles15).bin` 次の詳細を入力するように求められます。 • Linuxホスト外のSnapCenterサーバにアクセスするために使用されるwebapp外部ポート。デフォルト値は8146です。 • SnapCenterサーバをインストールするSnapCenterサーバユーザ。 • パッケージがインストールされるインストールディレクトリ。

実行する処理	操作
非対話型インストール	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` 例：sudo ./ snapcenter_linux_server.bin -i silent -dwebapp_external_port=8146 -DSNAPCENTER_SERVER_USER=root -Duser_install_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log ログは_/var/opt/snapcenter/logs _に保存されます。 SnapCenterサーバをインストールするために渡されるパラメータ： • DWEBAPP_EXTERNAL_PORT：Linuxホスト外のSnapCenterサーバにアクセスするために使用されるwebapp外部ポート。デフォルト値は8146です。 • DWEBAPP_INTERNAL_PORT：Linuxホスト内のSnapCenterサーバへのアクセスに使用されるwebapp内部ポート。デフォルト値は8147です。 • DSMCORE_PORT：smcoreサービスが実行されているSMCoreポート。デフォルト値は8145です。 • DSCHEDULER_PORT：スケジューラサービスが実行されているスケジューラポート。デフォルト値は8154です。 • DSNAPCENTER_SERVER_USER ：SnapCenterサーバをインストールするSnapCenterサーバユーザ。DSNAPCENTER_SERVER_USER_の場合、デフォルトはインストーラを実行しているユーザです。 • DUSER_INSTALL_DIR:パッケージがインストールされるインストールディレクトリ。*DUSER_INSTALL_DIR_*の場合、デフォルトのインストールディレクトリは/ opt_です。 • DINSTALL_LOG_NAME：インストールログを格納するログファイルの名前。これはオプションパラメータで、指定するとログはコンソールに表示されません。 このパラメータを指定しない場合、ログはコンソールに表示され、デフォルトのログファイルにも格納されます。 DSELINUX：_SELinux STATUS_が「

次の手順

- _SELinux status_が「enabled」で、_current mode_が「enforcing」の場合、*nginx*サービスは起動しません。次のコマンドを実行する必要があります。
  a. ホームディレクトリに移動します。
  b. コマンドを実行します `journalctl -x|grep nginx`。
  c. webapp内部ポート（8147）がリッスンできない場合は、次のコマンドを実行します。
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. 実行 `setsebool -P httpd_can_network_connect on`

- Enabled」、_CURRENT MODE_が Enforcing」で、「Before You Begin」セクションで説明したコマンドを実行した場合は、このパラメータを指定して値を1に割り当てる必要があります。デフォルト値は0です。
- UPGRADE コマンドを実行します。値は0です。SnapCenterサーバをアップグレードするには、このパラメータと0以外の任意の整数を指定します。

製品を登録してサポートを有効にする

NetAppを初めてご利用になり、NetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

手順

1. SnapCenterのインストール後、*[ヘルプ]>[バージョン情報]*に移動します。
2. [_About SnapCenter _]ダイアログボックスで、971で始まる20桁のSnapCenterインスタンスをメモします。
3. をクリックします https://register.netapp.com
4. [* I am not a registered NetApp Customer*] をクリックします。
5. 自分自身を登録するには、詳細を指定してください。
6. NetApp Reference SNフィールドは空白のままにします。
7. [Product Line]ドロップダウンから[* SnapCenter *]を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. [Submit （送信）] をクリックします。

RBAC許可を使用したSnapCenterへのログイン

SnapCenterはロールベースアクセス制御（RBAC）をサポートしています。SnapCenter管理者は、SnapCenter RBACを使用して、ワークグループまたはActive Directory内のユーザ、またはActive Directory内のグループにロールとリソースを割り当てます。これで、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す。

開始する前に

- Windows Server ManagerでWindowsプロセスアクティブ化サービス（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サーバー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。

- SnapCenterサーバがLinuxホストにインストールされている場合は、SnapCenterサーバのインストールに使用したユーザアカウントを使用してログイン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および[スタート]メニューに配置されます。また、インストールの最後に、インストールウィザードには、インストール中に指定した情報に基づいてSnapCenter URLが表示されます。リモートシステムからログインする場合は、このURLをコピーできます。

Webブラウザで複数のタブを開いている場合は、SnapCenterブラウザタブだけを閉じてもSnapCenterから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 "外部ネットワークからクラスタIPアドレスにアクセスできない"。

SnapCenter GUIに加えて、PowerShellコマンドレットを使用してスクリプトを作成し、設定、バックアップ、リストアの各処理を実行できます。一部のコマンドレットは、SnapCenterのリリースごとに変更されている場合があります。詳細については、を "SnapCenter ソフトウェアコマンドレットリファレンスガイド" 参照してください。

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. ユーザー資格情報を入力します。

指定する項目	使用する形式
ドメイン管理者	• NetBIOS\ユーザ名 • ユーザ名@UPNサフィックス 例：username@netapp.com • 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 *

[Dashboard]ページが表示されます。

サイトに到達できないというエラーが表示されてロギングが失敗した場合は、SSL証明書をSnapCenterにマッピングする必要があります。 "詳細"

- 終了後 *

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

SnapCenterでサポートす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"です。

Linuxホストで実行されているSnapCenterにプラグインホストを追加する場合は、_/opt/NetApp/snapcenter/SnapManagerWeb/Repository _からチェックサムファイルを取得する必要があります。

6.0リリース以降、デスクトップにSnapCenter PowerShellのショートカットが作成されます。ショートカットを使用すると、SnapCenter PowerShellコマンドレットに直接アクセスできます。

多要素認証（MFA）を使用したSnapCenterへのログイン

SnapCenterサーバは、Active Directoryの一部であるドメインアカウントに対してMFAをサポートしています。

開始する前に

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ない

- 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ログインページで、[Username]と[Password]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というエラーメッセージが表示された場合は、次の点を確認する必要があります。

   - 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 FSと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サーバを保護する

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プロトコルには、接続障害を引き起こしたり、中間者攻撃を実行したり、Webサイトと訪問者間の暗号化トラフィックを観察したりするために攻撃者が使用できる欠陥があります。

- 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\SYSTEM\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enabled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。

WindowsホストのCA証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストのプラグインサービスとバインドします。

   ```
   > $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

WindowsホストのSnapCenterサイトでCA証明書を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. [* アクション * （ Actions * ）] > [* サイトの編集 * （ * Edit Site * ）] に移動し、 [* バインド * （

Bind

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証明書]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。

SnapCenterスケジューラサイト（デフォルトポート：8154、HTTPS）には自己署名証明書が設定されています。このポートはSnapCenterサーバホスト内で通信しており、CA証明書を使用してを設定する必要はありません。ただし、CA証明書の使用が必要な環境の場合は、SnapCenterスケジューラサイトを使用して手順5から9を繰り返します。

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証明書を有効にする

CA証明書を設定し、SnapCenterサーバに対してCA証明書の検証を有効にする必要があります。

開始する前に

- CA証明書を有効または無効にするには、Set-SmCertificateSettingsコマンドレットを使用します。
- SnapCenterサーバの証明書のステータスは、Get-SmCertificateSettingsコマンドレット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、を参照して "SnapCenter ソフトウェアコマンドレットリファレンスガイド"ください。

- 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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * 🔒 *は、有効になっているかプラグインホストに割り当てられているCA証明書がないことを示します。
- ** 🔒 は、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。

- ** 🔒 は、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場合は、データ保護処理が正常に完了しています。

LinuxホストのCA証明書の設定

LinuxにSnapCenterサーバをインストールすると、インストーラによって自己署名証明書が作成されます。CA証明書を使用する場合は、nginxリバースプロキシ、監査ログ、およびSnapCenterサービスの証明書を設定する必要があります。

nginx証明書の設定

手順

1. /etc/nginx/conf.d_に移動します。 `cd /etc/nginx/conf.d`
2. viまたは任意のテキストエディタを使用して* snapcenter.conf *を開きます。
3. 構成ファイルのserverセクションに移動します。
4. _SSL_CERTIFICATE_AND_SSL_CERTIFICATE_KEY_のパスをCA証明書を指すように変更します。
5. ファイルを保存して閉じます。
6. nginxを再ロード： `$nginx -s reload`

監査ログ証明書の設定

手順

1. viまたは任意のテキストエディタを使用して_install_DIR /NetApp/snapcenter/SnapManagerWeb/SnapManagerWeb.UI.dll.config_を開きます。

   *INSTALL_DIR_IS_*のデフォルト値は/ opt_です。

2. AUDILOG_CERTIFICATE_PATH キーと AUDILOG_CERTIFICATE_PASSWORD *キーを編集して、それぞれCA証明書のパスとパスワードを含めます。

   監査ログ証明書では、_.pfx_formatのみがサポートされます。

3. ファイルを保存して閉じます。
4. snapmanagerweb *サービスを再起動します。 `$ systemctl restart snapmanagerweb`

SnapCenterサービス証明書の設定

手順

1. viまたは任意のテキストエディタを使用して、次の設定ファイルを開きます。
   - *INSTALL_DIR /NetApp/snapcenter/SnapManagerWeb/SnapManagerWeb.UI.dll.config*
   - *INSTALL_DIR /NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
   - *install_DIR /NetApp/snapcenter/Scheduler/Scheduler.api.dll.config*

*INSTALL_DIR_IS_*のデフォルト値は/ opt_です。

2. SERVICE_CERTIFICATE_PATH キーと SERVICE_CERTIFICATE_PASSWORD *キーを編集して、CA証明書のパスとパスワードをそれぞれ追加します。

   SnapCenterサービス証明書では、_.pfx_formatのみがサポートされます。

3. ファイルを保存して閉じます。
4. すべてのサービスを再起動します。
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Windowsホストで双方向SSL通信を設定して有効にする

Windowsホストでの双方向SSL通信の設定

Windowsホスト上のSnapCenterサーバとプラグインの間の相互通信を保護するために、双方向SSL通信を設定する必要があります。

開始する前に

- サポートされるキーの最小長が3072のCA証明書CSRファイルを生成しておく必要があります。
- CA証明書でサーバ認証とクライアント認証がサポートされている必要があります。
- 秘密鍵とサムプリントの詳細が記載されたCA証明書が必要です。
- 一方向SSL設定を有効に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。 "CA証明書の設定セクション"

- すべてのプラグインホストとSnapCenterサーバで双方向SSL通信を有効にしておく必要があります。

  一部のホストまたはサーバで双方向SSL通信が有効になっていない環境はサポートされません。

手順

1. ポートをバインドするには、PowerShellコマンドを使用して、SnapCenter IIS Webサーバポート8146（デフォルト）およびSMCoreポート8145（デフォルト）のSnapCenterサーバホストで次の手順を実行します。

   a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポートバインドを削除します。

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      例えば、

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

      > netsh http delete sslcert ipport=0.0.0.0:8146
      ```

b. 新しく取得したCA証明書をSnapCenterサーバとSMCoreポートにバインドします。

```
> $cert = "<CA_certificate thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
certhash=$cert appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

例えば、

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

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

2. CA証明書の権限にアクセスするには、次の手順を実行して新しく取得したCA証明書にアクセスし、SnapCenterのデフォルトのIIS Webサーバユーザ「* IIS AppPool\SnapCenter *」を証明書の権限のリストに追加します。
   a. Microsoft管理コンソール（MMC）に移動し、**[**ファイル**]**>*[SnapIn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証明書を選択します。
   f. ユーザー/権限の追加ウィザードを開始するには、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。
   g. [追加]*をクリックし、[ユーザーとグループの選択]ウィザードで場所をローカルコンピュータ名（階層の最上位）に変更します。
   h. IIS AppPool\SnapCenterユーザを追加し、フルコントロール権限を付与します。
3. CA証明書IIS権限*の場合、次のパスからSnapCenterサーバーに新しいDWORDレジストリキーエントリを追加します。

Windowsレジストリエディタで、次のパスに移動します。

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
ders\SCHANNEL
```

4. SCHANNELレジストリ設定のコンテキストで、新しいDWORDレジストリキーエントリを作成します。

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

双方向**SSL**通信用の**SnapCenter Windows**プラグインを設定します

SnapCenter Windowsプラグインは、PowerShellコマンドを使用して双方向SSL通信用に設定する必要があります。

開始する前に

CA証明書サムプリントが使用可能であることを確認します。

手順

1. ポートをバインドするには、WindowsプラグインホストでSMCoreポート8145（デフォルト）に対して次の操作を実行します。

   a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポートバインドを削除します。

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

   例えば、

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

   b. 新しく取得したCA証明書をSMCoreポートにバインドします。

   ```
   > $cert = "<CA_certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid"
   clientcertnegotiation=enable verifyclientcertrevocation=disable

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

   例えば、

   ```
   > $cert = "abc123abc123abc123abc123"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
   ```

```
    clientcertnegotiation=enable verifyclientcertrevocation=disable

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

Windowsホストで双方向SSL通信を有効にする

PowerShellコマンドを使用して、Windowsホスト上のSnapCenterサーバとプラグインの間の相互通信を保護するために、双方向SSL通信を有効にすることができます。

- 始める前に *

すべてのプラグインとSMCoreエージェントのコマンドを最初に実行し、次にサーバのコマンドを実行します。

- 手順 *

1. 双方向SSL通信を有効にするには、プラグイン、サーバー、および双方向SSL通信が必要な各エージェントに対して、SnapCenterサーバーで次のコマンドを実行します。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

1. 次のコマンドを使用して、IIS SnapCenterアプリケーションプールのリサイクル操作を実行します。
   `> Restart-WebAppPool -Name "SnapCenter"`
2. Windowsプラグインの場合は、次のPowerShellコマンドを実行してSMCoreサービスを再起動します。

```
> Restart-Service -Name SnapManagerCoreService
```

双方向SSL通信を無効にします

PowerShellコマンドを使用して、双方向SSL通信を無効にすることができます。

- このタスクについて *
- すべてのプラグインとSMCoreエージェントのコマンドを最初に実行し、次にサーバのコマンドを実行します。
- 双方向SSL通信を無効にしても、CA証明書とその設定は削除されません。
- SnapCenterサーバに新しいホストを追加するには、すべてのプラグインホストで双方向SSLを無効にする必要があります。
- NLBとF5はサポートされません。
- 手順 *

1. 双方向SSL通信を無効にするには、すべてのプラグインホストとSnapCenterホストに対し

てSnapCenterサーバで次のコマンドを実行します。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

1. 次のコマンドを使用して、IIS SnapCenterアプリケーションプールのリサイクル操作を実行します。
   `> Restart-WebAppPool -Name "SnapCenter"`
2. Windowsプラグインの場合は、次のPowerShellコマンドを実行してSMCoreサービスを再起動します。

   ```
   > Restart-Service -Name SnapManagerCoreService
   ```

Linuxホストでの双方向SSL通信の設定と有効化

Linuxホストでの双方向SSL通信の設定

双方向SSL通信を設定して、Linuxホスト上のSnapCenterサーバとプラグインの間の相互通信を保護する必要があります。

開始する前に

- LinuxホストのCA証明書を設定しておく必要があります。
- すべてのプラグインホストとSnapCenterサーバで双方向SSL通信を有効にしておく必要があります。

手順

1. certificate.pem *を_/etc/pki/ca-trust/source/anchors/_にコピーします。
2. Linuxホストの信頼リストに証明書を追加します。
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. 証明書が信頼リストに追加されたかどうかを確認します。
   `trust list | grep "<CN of your certificate>"`
4. SnapCenter * nginx ファイルの ssl_certificate と ssl_certificate_key *を更新して再起動してください。
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. SnapCenterサーバGUIリンクを更新します。
6. */<installation path>/NetApp/snapcenter/SnapManagerWeb_*および* SMCoreServiceHost.dll.config *（/<installation path>/NetApp/snapcenter/SMCore_）で次のキーの値を更新します。
   - <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />

- <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>

7. 次のサービスを再起動します。
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. 証明書がSnapManager Webポートに接続されていることを確認します。
   `openssl s_client -connect localhost:8146 -brief`
9. 証明書がsmcoreポートに接続されていることを確認します。
   `openssl s_client -connect localhost:8145 -brief`
10. SPLキーストアとエイリアスのパスワードを管理します。
    a. SPLプロパティファイルの* spl_keystore_pass *キーに割り当てられたSPLキーストアのデフォルトパスワードを取得します。
    b. キーストアのパスワードを変更します。
       `keytool -storepasswd -keystore keystore.jks`
    c. 秘密鍵エントリのすべてのエイリアスのパスワードを変更します。
       `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. _spl.properties_のキー* spl_keystore_pass *と同じパスワードを更新します。
    e. サービスを再起動します。
11. プラグインLinuxホストで、SPLプラグインのキーストアにルート証明書と中間証明書を追加します。
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
      i. keystore.jksのエントリを確認します。
         `keytool -list -v -keystore <path to keystore.jks>`
      ii. 必要に応じてエイリアスの名前を変更します。
          `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. _spl.properties_ファイルの* spl_certificate_alias の値を**_keystore.jks_**に格納されている certificate.pfx * のエイリアスで更新し、SPLサービスを再起動します。 `systemctl restart spl`
13. 証明書がsmcoreポートに接続されていることを確認します。
    `openssl s_client -connect localhost:8145 -brief`

Linuxホストで**SSL**通信を有効にする

PowerShellコマンドを使用して双方向SSL通信を有効にすると、Linuxホスト上のSnapCenterサーバとプラグインの間の相互通信を保護できます。

ステップ

1. 一方向SSL通信を有効にするには、次の手順を実行します。

a. SnapCenter GUIにログインします。

b. **>**[グローバル設定]をクリックし、[SnapCenterサーバーで証明書の検証を有効にする]*を選択します。

c. **>**[管理対象ホスト]*をクリックし、一方向SSLを有効にするプラグインホストを選択します。

d. アイコンをクリックし  、*[証明書の検証を有効にする]*をクリックします。

2. SnapCenterサーバLinuxホストからの双方向SSL通信を有効にします。

   ◦ `Open-SmConnection`

   ◦ `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`

   ◦ `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`

   ◦ `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

証明書ベースの認証の設定

SnapCenterサーバから認証局（CA）証明書をエクスポートします

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバからプラグインホストにCA証明書をエクスポートする必要があります。

開始する前に

双方向SSLを設定しておく必要があります。

- 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*オプションを選択し、[完了]*をクリックします。
4. **>**[証明書-ローカルコンピュータ]**>**[個人]**>**[証明書]*をクリックします。
5. SnapCenterサーバーで使用される調達CA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. ウィザードで次の操作を実行します。

オプション	操作
秘密キーのエクスポート	を選択し、[次へ]*をクリックします。
エクスポートファイル形式	「 * 次へ * 」をクリックします。
ファイル名	をクリックし、証明書を保存するファイルパスを指定して[次へ]*をクリックします。

オプション	操作
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。

証明書ベースの認証は、SnapCenter HA構成およびSnapCenter Plug-in for VMware vSphereではサポートされません。

認証局（CA）証明書をWindowsプラグインホストにインポートします

エクスポートしたSnapCenterサーバCA証明書を使用するには、Microsoft管理コンソール（MMC）を使用して、関連する証明書をSnapCenter Windowsプラグインホストに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*オプションを選択し、[完了]*をクリックします。
4. **>**[証明書-ローカルコンピュータ]**>**[個人]**>**[証明書]*をクリックします。
5. 「個人」フォルダを右クリックし、すべてのタスク>*インポート*を選択してインポートウィザードを開始します。
6. ウィザードで次の操作を実行します。

オプション	操作
ストアの場所	「 * 次へ * 」をクリックします。
インポートするファイル	拡張子.cerで終わるSnapCenterサーバ証明書を選択します。
証明書ストア	「 * 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] をクリックしてインポートを開始します。

UNIXホストプラグインにCA証明書をインポートし、SPL trust-storeにルート証明書または中間証明書を設定する

CA証明書をUNIXプラグインホストにインポートします

CA証明書をUNIXプラグインホストにインポートする必要があります。

- このタスクについて *

- SPLキーストアのパスワード、および使用中のCA署名キーペアのエイリアスを管理できます。
- 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は同じである必要があります。
- 手順 *
  1. SPLキーストアのデフォルトパスワードは、SPLプロパティファイルから取得できます。キーに対応する値です `SPL_KEYSTORE_PASS`。
  2. キーストアのパスワードを変更します。
     `$ keytool -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、キーストアと同じパスワードに変更します。
     `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. ファイルのSPL_KEYSTORE_PASSキーについても同じ内容を更新し `spl.properties` ます。
  5. パスワードを変更したら、サービスを再起動します。

spl trust-storeに対するルート証明書または中間証明書の設定

ルート証明書または中間証明書をspl trust-storeに設定する必要があります。ルートCA証明書のあとに中間CA証明書を追加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に移動します `/var/opt/snapcenter/spl/etc`。
  2. ファイルを探します `keystore.jks`。
  3. キーストアに追加された証明書を一覧表示します。
     `$ 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 <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
  5. spl trust-store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。

SPL trust-storeへの**CA**署名済みキーペアの設定

SPL trust-storeにCA署名付きキーペアを設定する必要があります。

- 手順 *
  1. SPLのキーストアが格納されているフォルダに移動し `/var/opt/snapcenter/spl/etc` ます。
  2. ファイルを探します `keystore.jks`。
  3. キーストアに追加された証明書を一覧表示します。
     `$ keytool -list -v -keystore keystore.jks`
  4. 秘密鍵と公開鍵の両方が設定されたCA証明書を追加します。
     `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`

5. キーストアに追加された証明書を一覧表示します。
   `$ keytool -list -v -keystore keystore.jks`
6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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、ファイル内のキーspl_keystore_passの値です `spl.properties`。

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

1. 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`
2. ファイルにあるキーストアからエイリアス名を設定し `spl.properties` ます。この値をSPL_CERTIFICATE_ALIASキーに対して更新します。
3. SPL trust-storeにCA署名キーペアを設定したら、サービスを再起動します。

証明書ベースの認証を有効にします

SnapCenter ServerおよびWindowsプラグインホストに対して証明書ベースの認証を有効にするには、次のPowerShellコマンドレットを実行します。Linuxプラグインホストで双方向SSLを有効にすると、証明書ベースの認証が有効になります。

- クライアント証明書ベースの認証を有効にするには：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- クライアント証明書ベースの認証を無効にするには：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Active Directory、LDAP、LDAPSの設定

信頼されていない**Active Directory**ドメインの登録

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。

開始する前に

- LDAP および LDAPS プロトコル *
- 信頼されていないActive Directoryドメインは、LDAPまたはLDAPSプロトコルを使用して登録できます。

- プラグインホストとSnapCenterサーバの間の双方向の通信を有効にしておく必要があります。
- DNSによる解決は、SnapCenterサーバからプラグインホストへ（またはその逆）設定する必要があります。
- LDAPプロトコル*
- 完全修飾ドメイン名（FQDN）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を使用して登録できます。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。このアドレスはSnapCenterサーバから解決できる必要があります。

- LDAPSプロトコル*
- CA証明書は、Active Directory通信中にLDAPSでエンドツーエンドの暗号化を提供するために必要です。

  "LDAPS用のCAクライアント証明書の設定"

- ドメインコントローラのホスト名（DCHostName）にSnapCenterサーバから到達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を使用して登録できます。
- 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. [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. をクリックして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	操作
ドメイン名	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	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDNを指定します。
トメインコントロオラメイ	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をSnapCenterサーバから解決できない場合は、DNSの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用のCAクライアント証明書の設定

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	操作
ウィザードの2ページ目	[* 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の完了	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の設定

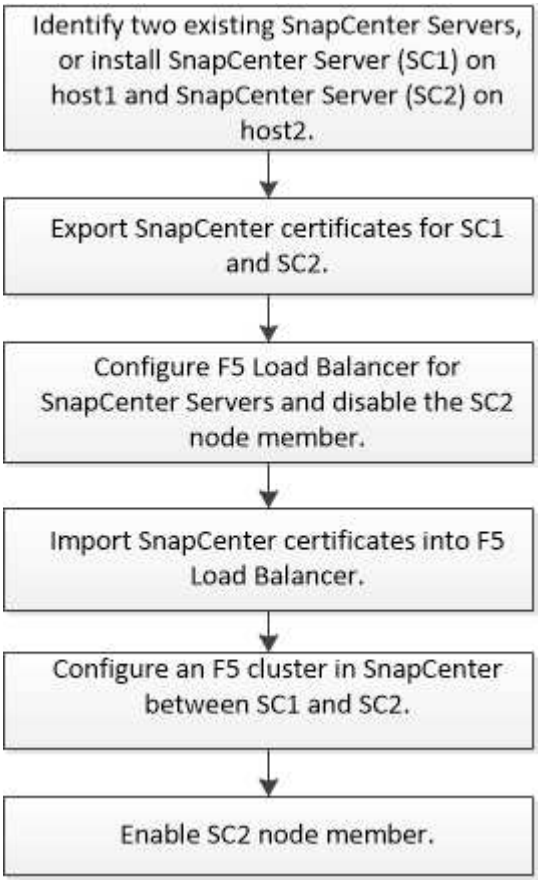
F5を使用した高可用性のためのSnapCenterサーバの設定

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は、AWS Elastic Load Balancing（ELB）とAzureのロードバランシングもサポートしています。

以前にネットワークロードバランシング（NLB）を使用していたSnapCenter 4.2.xからアップグレードした場合は、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。

ワークフロー図は、F5ロードバランサを使用してSnapCenterサーバーを高可用性に設定する手順を示しています。詳細については、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、（SnapCenterAdminロールが割り当てられていることに加えて）SnapCenter Server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。

- Add-SmServerCluster
- アドSmServer
- 削除- SmServerCluster

  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サーバ間でフェー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SnapCenterに再度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）では、NLBまたはF5ノードによって部分的に解決されたノードを追加し、SnapCenterノードがこのノードにアクセスできない場合は、SnapCenterホストページでホストの停止状態と実行状態が頻繁に切り替わります。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ノードのホストを解決できることを確認する必要があります。
- MFA設定用のSnapCenterコマンドをすべてのノードで実行する必要があります。証明書利用者の設定は、F5クラスタの詳細を使用してActive Directoryフェデレーションサービス（AD FS）サーバで行う必要があります。MFAを有効にすると、ノードレベルのSnapCenter UIアクセスがブロックされます。
- フェイルオーバー中は、2つ目のノードに監査ログの設定が反映されません。そのため、監査ログの設定は、F5パッシブノードがアクティブになったときに手動で繰り返す必要があります。

Microsoft Network Load Balancerの手動設定

Microsoftネットワークロードバランシング（NLB）を設定して、SnapCenterの高可用性をセットアップできます。SnapCenter 4.2以降では、高可用性を実現するために、SnapCenterインストールの外部でNLBを手動で設定する必要があります。

SnapCenterを使用したネットワークロードバランシング（NLB）の設定方法については、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

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を使用して高可用性を実現するようにSnapCenterサーバを設定します。 "詳細"です。
  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. 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SnapCenterサーバを更新します。

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。その後、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のハイアベイラビリティ（HA）機能を使用する場合は、1つ目のノードでNetwork Load Balancer（NLB）を設定する必要があります。MySQLリポジトリは、インストール時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場合は、1つ目のノードのF5に参加し、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は、2つ以上のノードではサポートされません。
- 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ことがあります。

  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つ目のノードにフェイルオーバーすると、以降のジョブはすべて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証明書のエクスポート

- 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	操作
秘密キーのエクスポート	[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	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てロールとアセットを割り当てる

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。ロールによって、SnapCenterユーザがアクセスできるオプションが決まります。

開始する前に

- 「SnapCenterAdmin」ロールでログインする必要があります。

- オペレーティングシステムまたはデータベースのActive Directoryでユーザまたはグループのアカウントを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（:）。以前のリリースのSnapCenterで作成したロールをこれらの特殊文字で使用する場合は、SnapCenter WebAppがインストールされているweb.configファイルで'DisableSQLInjectionValidation'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。値を変更したら、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に追加するADユーザとADグループには、Active Directory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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

- RBACの権限と効率性を活用するには、いずれかの時点でユーザまたはグループにロールを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、 ユーザまたはグループの作成時のユーザに対するクレデンシャル。
- 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	アセットの割り当て
リソースの保護	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	ホスト

- WindowsクラスタまたはDAG（Exchange Server Database Availability Group）アセットに新しいノードを追加したときに、この新しいノードがユーザに割り当てられている場合は、アセットをユーザまたはグループに再割り当てして新しいノードをユーザまたはグループに追加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ノードクラスタにRBACユーザまたはグループを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に新しいノードを追加する必要があります。

- Snapshot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に対する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する必要があります。

> 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する場合は、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に付属の事前定義されたロール"。

- 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	操作
アクセスタイプ	[ドメイン]または[ワークグループ]を選択します。 [ドメイン]認証タイプの場合は、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。
タイプ	[ユーザ]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	操作
ユーザー名	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、ドメイン間ユーザの検索リストがないため、ユーザ名を完全に入力する必要があります。 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。
役割	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]テーブルで、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、リソースリストを更新します。

ロールの作成

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、 * 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（ : ）。以前のリリースのSnapCenterで作成したロールをこれらの特殊文字で使用する場合は、SnapCenter WebAppがインストールされているweb.configファイルで'DisableSQLInjectionValidation'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。値を変更したら、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。

   このロールのメンバーに他のメンバーが割り当てられているオブジェクトが表示されないようにするには、このオプションの選択を解除してください。

   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属するユーザにオブジェクトまたはリソースへのアクセス権を割り当てる必要はありません。

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ロールを追加する

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

開始する前に

- clustered ONTAPを実行す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（複数可）
  - これらのタスクの実行に必要な権限
- 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（あるいはその両方）に権限を付与します。

    各コマンド/コマンドディレクトリには、フルアクセスと読み取り専用の2つのアクセスレベルがあります。

  フルアクセス権限は必ず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 *

これらのロールをストレージシステムで簡単に設定するには、NetAppコミュニティフォーラムに掲載されているRBAC User Creator for Data ONTAPツールを使用します。

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、RBAC User Creator for Data ONTAPツールでは、フルアクセス権限が最初に表示されるように、権限が正しい順序で自動的に追加されます。読み取り専用権限を最初に追加してから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としてマークし、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、これらの用語はどちらも同じ意味です。

- 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には、SVMの名前を指定します。空白のままにすると、デフォルトでクラスタ管理者が設定されます。
   - role_nameは、ロールに指定する名前です。
   - commandはONTAP機能です。

     > このコマンドは権限ごとに繰り返す必要があります。フルアクセスコマンドは、読み取り専用コマンドの前に指定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 "ロールの作成と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には、SVMの名前を指定します。

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。

最小限の権限でSVMロールを作成する

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、ロールを作成して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繰り返す必要があります。

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ロールの作成と権限の割り当て用のONTAP CLIコマンド

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

5.0以降では、SVM管理者ユーザはREST APIでのみサポートされます。SVM管理者以外を使用してロールを作成する場合は、ZAPIを使用してください。

- `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 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 modify-snaplock-expiry-time" -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 snapshot show-delta" -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`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"nvme subsystem delete" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

最小限の権限で**ONTAP**クラスタロールを作成する

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。複数のONTAP 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、ロールを作成して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繰り返す必要があります。

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と権限の割り当て用の**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ために実行する必要があるONTAP CLIコマンドがいくつかあります。

SnapCenter 5.0以降では、クラスタ管理者ユーザはREST APIでのみサポートされます。クラスタ管理者以外のユーザを使用してロールを作成する場合は、ZAPIを使用してください。

- `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 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 snapshot modify-snaplock-expiry-time" -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 snapshot show-delta" -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構成する

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。

監査ログの設定

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、すべての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して保護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別の監査チェックサムファイルで保持され、その下ではコンテンツの整合性を保証するために定期的な整合性チェックが行われます。

「SnapCenterAdmin」ロールでログインしておく必要があります。

- 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サーバログの障害
  - ディスクスペースが少ない
- 整合性チェックに失敗した場合にのみE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同時に変更する必要があります。いずれか1つだけを変更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を変更すると、以前の場所にある監査ログで整合性チェックを実行できません。
- 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配置する必要があります。

  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ていません。
- syslogサーバの設定で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でエラーまたはアラートとしてキャプチャできません。
- Set-SmAuditSettingsコマンドとGet-SmAuditSettingsコマンドを使用して、監査ログを構成できます。

  コマンドレットで使用できるパラメータとその説明は、Get-Help Command_name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. [Audit log]セクションで、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. ログファイルの最大数を入力
     c. アラートを送信するためのディスクスペース使用量のパーセンテージを入力します
  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. （オプション）リモートsyslogサーバへの転送監査ログを有効にし、syslogサーバの詳細を入力します。

   TLS 1.2プロトコルの場合、syslogサーバから「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サーバホストの入力
   b. syslogサーバポートの入力
   c. syslogサーバプロトコルの入力
   d. RFC形式の入力

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する

データ保護とプロビジョニングの処理を実行するために、SnapCenterからONTAPストレージまたはAmazon FSx for NetApp ONTAPへのアクセスを許可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を追加することも、複数のSVMで構成されるクラスタを追加することもできます。Amazon FSx for NetApp ONTAP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でFSx SVMを追加できます。

開始する前に

- 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、イベント管理システム（EMS）および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、システムのトラブルシューティング用にNetApp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終了したとき、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またはデスティネーションクラスタとソース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ことがあります。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]ページで、次の情報を入力します。

フィールド	操作
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。 ストレージシステム名は、ドメイン名を含めずに15文字以下にする必要があり、解決可能な名前である必要があります。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）のストレージシステムでノンストップオペレーションを実現するには、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へのアクセス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	操作
イベント管理システム（EMS）とAutoSupportの設定	保護が適用された場合、リストア処理が完了した場合、または処理が失敗した場合にEMSメッセージをストレージシステムのsyslogに送信したり、AutoSupportメッセージをストレージシステムに送信したりする場合は、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。

SnapCenterでSVMを追加した場合は、ドロップダウンからプラットフォームタイプを手動で選択する必要があります。

   a. [Protocol]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。
   b. ストレージシステムが受け入れるポートを入力します。

      通常はデフォルトのポート443を使用できます。

   c. 通信の試行が停止す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。

   d. 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。
   e. [保存（ Save ）] をクリックします。
      1. [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は、ここにFSxクラスタが表示されます。

  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。

FASまたはAFFストレージシステムをオールSANアレイ（ASA）にアップグレードした場合は、SnapCenterサーバのストレージ接続を更新して、SnapCenterの新しいストレージタイプを反映する必要があります。

- 終了後 *

SnapCenterがアクセスできる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には、クラスタ管理者が各ストレージシステムノードでAutoSupportを有効にする必要があります。そのためには、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ます。

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to 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 Standardコントローラベースライセンスを追加

FAS、AFF、またはオールSANアレイ（ASA）ストレージコントローラを使用している場合は、コントローラベースのSnapCenterライセンスが必要です。

コントローラベース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量
- 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、AFF、またはASA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 GUIを使用して、SnapManager SuiteライセンスがFAS、AFF、またはASA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確認し、SnapManager Suiteライセンスが必要なストレージシステムを特定できます。SnapManager Suiteライセンスは、プライマリストレージシステム上のFAS、AFF、ASA SVMまたはクラスタにのみ適用されます。

コントローラにSnapManager Suiteライセンスがすでにある場合は、SnapCenter Standardコントローラベースライセンス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、AFF、またはASAプライマリストレージシステムにSnapManager Suiteライセンスがインストールされていることを示します。
   - FAS、AFF、またはASAプライマリストレージシステムにSnapManager Suiteライセンスがインストールされていないことを示します。
   - [Not Applicable]は、Amazon FSx for NetApp ONTAP、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ストレージコントローラがあるため、SnapManager Suiteライセンスが適用されないことを示します。

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して、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、AFF、またはASAシステムのクラスタ管理者である必要があります。

コントローラでは、SnapCenter Standardコントローラベースライセンスが SnapManagerSuite ライセンスとして表示されます。

手順

1. ONTAPコマンドラインを使用してNetApp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、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。

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してコントローラのシリアル番号を取得できます。FAS、AFF、またはASA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特定します。

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。

開始する前に

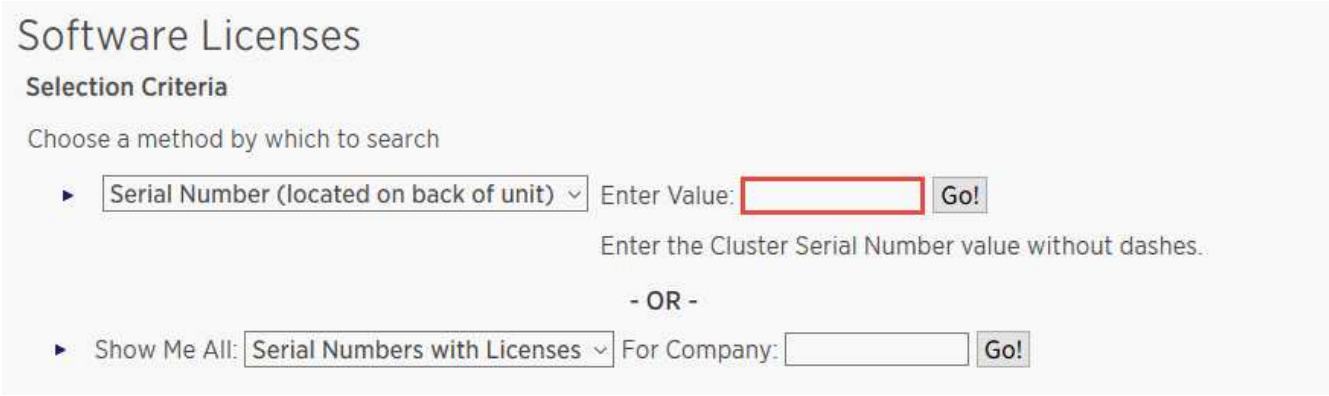
- NetAppサポートサイトの有効なログインクレデンシャルが必要です。

有効なクレデンシャルを入力しないと、検索のための情報は返されません。

- コントローラのシリアル番号が必要です。

手順

1. にログインし "NetAppサポートサイト"ます。
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、AFF、またはASAシステムを使用していて、SnapCenter StandardまたはSnapManager Suiteの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。

開始する前に

- FAS、AFF、またはASA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SnapManager Suiteのライセンスが必要です。

タスクの内容

FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールする場合は、Premium Bundleの評価版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. SnapManager Suite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. SnapManager Suite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。試用版ライセンスは、SnapCenter GUIでは削除できません。

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。

手順

1. SnapCenterサーバで、PowerShellウィンドウを開いてMySQLパスワードをリセットします。
   a. SnapCenterAdminアカウントのSnapCenterサーバとの接続セッションを開始するには、Open-SmConnectionコマンドレットを実行します。
   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られます。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';
```

ストレージシステムのプロビジョニング

Windowsホストでのストレージのプロビジョニング

LUNストレージの設定

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セッションを確立する

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"
- このタスクについて *

iSCSIセッションは、同じバージョンのIP間（IPv6とIPv6、またはIPv4とIPv4）でのみ確立できます。

リンクローカルIPv6アドレスは、iSCSIセッションの管理や、ホストとターゲットの両方が同じサブネット内にある場合にのみ使用できます。

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は、ホストを再起動する必要があります。

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
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、ターゲットごとにセッションを確立します。

iSCSIセッションの切断

複数のセッションを使用しているターゲットからiSCSIセッションの切断が必要になる場合があります。

- 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の作成と管理

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を作成する

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	操作
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。

フィールド	操作
イニシエータ	イニシエータを選択します。
タイプ	イニシエータタイプ、iSCSI、FCP、または混在（FCPとiSCSI）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。クラスタ用のigroupを作成する場合は、igroupを変更してそのigroupに他のノードを追加できます。

- 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、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。

ディスクの作成と管理

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はベーシックディスクのみをサポートします。ダイナミックディスクはサポートされていません。
- GPTの場合は1つのデータパーティションのみ、MBRの場合は1つのプライマリパーティションが許可されます。このパーティションには、NTFSまたはCSVFSでフォーマットされた1つのボリュームと、1つのマウントパスがあります。
- 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の表示

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。

クラスタ化ディスクの表示

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

開始する前に

- 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LUNを共有しないかぎり、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を共有する場合は、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	操作
ストレージシステム	LUN の SVM を選択します。

フィールド	操作
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. [Disk Type]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つのホストにのみ作成する必要があります。
クラスタ共有ボリューム（CSV）	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. [Drive Properties]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	説明
マウントポイントを自動割り当て	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。
ドライブ文字の割り当て	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	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	Windowsでディスクを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サイズを指定します（150MB以上）。 ドロップダウンリストでMB、GB、またはTBを選択します。
このLUNをホストするボリュームにシンプロビジョニングを使用する	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、一度に必要な量のストレージスペースのみが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。 必要になると思われるすべてのLUNストレージを格納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	説明
パーティションタイプを選択	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パーティションは、Windows Serverフェイルオーバークラスタでミスアライメントの問題を引き起こす可能性があります。 Unified Extensible Firmware Interface（UEFI）パーティションディスクはサポートされていません。

8. [Map LUN]ページで、ホスト上の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	操作
ホスト	クラスタグループ名をダブルクリックして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一覧から、イニシエータの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を共有している場合にのみ表示されます。
ホストイニシエータを選択	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	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既存のigroupを選択するか、新しいigroupを指定する	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、このフィールドに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増減できます。

- このタスクについて *
- シンプロビジョニングLUNの場合、ONTAP LUNジオメトリのサイズが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（ボリューム内の利用可能なサイズ）が最大サイズとして表示されます。
- MBRパーティション形式のLUNのサイズの上限は2TBです。
- GPTパーティション形式のLUNのストレージシステムサイズの上限は16TBです。
- LUNのサイズを変更する前にSnapshotを作成しておくことを推奨します。
- LUNのサイズ変更前に作成されたSnapshotからLUNをリストアする必要がある場合は、SnapCenterによってLUNのサイズがSnapshotのサイズに自動的に変更されます。

  リストア処理後、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. [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. 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。

ディスクの接続

[Connect Disk]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。

開始する前に

- 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LUNを共有しないかぎり、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を共有する場合は、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。

   [Connect Disk]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	操作
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。
クラスタサイズ	クラスタのLUN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. [Disk Type]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。

選択するオプション	状況
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つのホストにのみ接続する必要があります。
クラスタ共有ボリューム（CSV）	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。 ディスクに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. [Drive Properties]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	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ていません。
ドライブ文字の割り当て	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	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	Windowsでディスクを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. [Map LUN]ページで、ホスト上の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	操作
ホスト	クラスタグループ名をダブルクリックして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うち、イニシエータに使用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を共有している場合にのみ表示されます。
ホストイニシエータを選択	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	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既存のigroupを選択するか、新しいigroupを指定する	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、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。

開始する前に

- LUNがどのアプリケーションでも使用されてい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ボリュームが自動的に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する必要があります。ボリュームの名前を変更するときは、最後の文字だけでなく、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。

ディスクの削除

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共有の作成と管理

Storage Virtual Machine（SVM）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します。

* 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前に、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共有を作成する

SnapCenter共有ページを使用して、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	操作
説明	共有の説明を入力します。
共有名	共有名を入力します（例：test_share）。 入力した共有名は、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。 • 次の文字は使用できません：0x00～0x1Fの制御文字（両方を含む）、0x22（二重引用符）、および特殊文字 `\ / [ ] : (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の再生

ファイルが削除または変更されると、NTFSはLUN上の使用可能なスペースを追跡しますが、新しい情報はストレージシステムには報告しません。新しく解放されたブロックがストレージで使用可能と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PowerShellコマンドレットを実行します。

コマンドレットをリモートのプラグインホストで実行する場合は、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しておく必要があります。

開始する前に

- 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ホストの使用率が低いときに処理を実行することを推奨します。
- スペース再生では、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。

  再利用プロセスに時間がかかることがあります。

- 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にマッピングされたドライブパスです。

PowerShellコマンドレットを使用したストレージのプロビジョニング

ホストのプロビジョニングやスペース再生のジョブにSnapCenter GUIを使用しない場合は、SnapCenter Plug-in for Microsoft Windowsに付属のPowerShellコマンドレットを使用します。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がサーバから削除されたために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環境でのストレージのプロビジョニング

VMware環境では、SnapCenter Plug-in for Microsoft Windowsを使用して、LUNの作成と管理やSnapshotの管理を行うことができます。

サポートされるVMwareゲストOSプラットフォーム

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

  VMware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"。

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。

- すべてのクラスタノードで、同じクラスタディスクに対して同じターゲットID（仮想SCSIアダプタ上）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たロールを、root権限を持たないユーザに割り当てることはできません。

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クラスタの**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クラスタを管理できますが、まず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する必要があります。

ESXi 5.5以降では、ESX iSCSIおよび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またはESXiサーバのバージョンは、各VMware親ホストで同じである必要があります。
- 各親ホストには、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VMware Virtual Machine File System（VMFS）データストアを少なくとも1つ共有する必要があります。
- 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。

  必要に応じて、共有データストアをiSCSI経由で作成することもできます。

- 共有RDM LUNが物理互換モードになっている必要があります。
- 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。

- SCSIコントローラは、クラスタ内の各仮想マシンで物理互換モードで構成する必要があります。

  Windows Server 2008 R2では、各仮想マシンで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コントローラのタイプが1つしかなく、すでにC：ドライブに接続されている場合、共有LUNで既存のLSI Logic SASコントローラを使用することはできません。

  準仮想タイプの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する必要があります。

- ESXi 5.0では、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を使用してイニシエータグループが作成されます。

制限事項

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のどちらかである必要があります。両方は使用できません。

- 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ていません。
- 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**の作成

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には、まず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する必要があります。

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サーバとのセキュアなMySQL接続の設定

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サーバ構成用のセキュアなMySQL接続の設定

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設定します。

   詳しくは、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、それぞれ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のデータ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サーバ構成ファイル（my.in）のデフォルトパスはです `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。

次の例では、デフォルトフォルダ内のmy.iniファイルの[mysqld]セクションに証明書とキーファイルがコピーされ `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`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"
```

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. MySQLProtocolキーの値をSnapManager .Web.UI.dll.configファイルで更新します。

   次の例は、SnapManager .Web.UI.dll.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ているパスを使用して、SnapManager .Web.UI.dll.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構成用のセキュアなMySQL接続の設定

SnapCenterサーバとMySQLサーバ間の通信を保護する場合は、高可用性（HA）ノードの両方に対して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

  一方のHAノードでCA証明書が生成され、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. 1つ目のHAノードで、openssl コマンドを使用して、WindowsのMySQLサーバとクライアントのSSL証明書とキーファイルを設定します。

   詳しくは、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、それぞれ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のデータフォルダにコピーします。

   MySQLのデータフォルダのデフォルトパスは、C：\ProgramData\NetApp\SnapCenter\MySQL 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。

   MySQLサーバ構成ファイル（my.in）のデフォルトのパスは、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ノードで、次の手順に従ってCA証明書をコピーし、サーバ パブリック証明書、サーバ秘密鍵ファイル、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ファイルを生成します。

   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のデータフォルダにコピーします。

      MySQLのデータフォルダのデフォルトパスは、C：\ProgramData\NetApp\SnapCenter\MySQL Data\Data\です。

      CA証明書は今後作成しないでください。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、サーバ秘密鍵ファイル、およびクライアント秘密鍵ファイルのみを作成する必要があります。

   b. 1つ目のHAノードで、openssl コマンドを使用して、WindowsのMySQLサーバとクライアントのSSL証明書とキーファイルを設定します。

      "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、それぞれ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の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のデータ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ノードのMySQLProtocolキーの値をSnapManager .Web.UI.dll.configファイルで更新します。

   次の例は、SnapManager .Web.UI.dll.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を使用してSnapManagerの.Web.UI.dll.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Webアプリケーションを起動します。
2. 一方のHAノードでSet-SmRepositoryConfig -RebuildSlave -Force PowerShellコマンドレットに-Forceオプションを指定して使用し、両方のHAノードにセキュアな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。

インストール時に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	機能
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サービス • 一般的な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 • 健全性と診断 ◦ カスタムログ ◦ HTTPロギング ◦ ログツール ◦ リクエストモニター ◦ 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 ◦ 一元化された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認証 ◦ Windows認証 • アプリケーション開発機能 ◦ です。 NET拡張性4.5 ◦ アプリケーションの初期化 ◦ ASP。 Net Core Hosting Bundle（8.0.5以降） ◦ サーバー側インクルード ◦ WebSocketプロトコル 管理ツール
	IIS管理コンソール

カテゴリ	機能
IIS管理スクリプトとツール	• IIS管理サービス • Web管理ツール
.NET Framework 8.0.5の機能	• .NET Framework 8.0.5 • ASP。 正味8.0.5 • Windows Communication Foundation (WCF) HTTPアクティブ化45 ◦ TCPのアクティブ化 ◦ HTTPアクティブ化 用。 NET固有のトラブルシューティング情報。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"
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。 • RabbitMQ
Windowsプロセスアクティブ化サービス	• プロセスモデル
セツテイAPI	すべて

インストルチユウニLinuxホストテユウコウニナルキノウ

SnapCenterサーバは以下のソフトウェアパッケージをインストールします。これらのパッケージは、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ちます。

- RabbitMQ
- nginx
- アーラン
- .NET Framework 8.0.5
- PAM -デベル
- PowerShell

Microsoft SQL Serverデータベースの保護

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を使用すると、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データベースと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をサポートする次のタスクを実行できます。

- 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およびmsdb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せん。ただし、モデル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のリストア
  - マスターシステムデータベース、msdbシステムデータベース、およびモデル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

  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、およびクローンライフサイクルの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は、検証処理を実行するためにデータベースのクローニングを行います。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の機能

Plug-in for SQL Serverは、Windowsホスト上でMicrosoft SQL Serverと統合され、ストレージシステム上でNetApp Snapshot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を設定したり、ポイントインタイムリストア処理と最新の状態へのリストア処理を設定したりできます。SnapCenter から E メールアラートを送信するように設定して、 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**スナップショットテクノロジ

  Plug-in for SQL Serverでは、NetApp SnapCenter Plug-in for Microsoft WindowsでNetAppのSnapshot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できます。Snapshot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。
- RBACでサポートされるセキュリティと一元化されたロール委譲
- 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可能
- 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、クローニングの処理のスクリプトを作成できます。

- SQL ServerでAlwaysOn可用性グループ（AG）がサポートされ、AGのセットアップ、バックアップ、リストアの処理を高速化
- SQL Server 2014の一部としてのインメモリデータベースとバッファプール拡張（BPE）
- LUNおよび仮想マシンディスク（VMDK）のバックアップのサポート
- 物理インフラと仮想インフラをサポート
- iSCSI、ファイバチャネル、FCoE、rawデバイスマッピング（RDM）、NFSおよびVMFS経由のVMDKがサポートされます。

  Storage Virtual Machine（SVM）にNASボリュームの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およびファイルグループのサポート。
- Windows Server 2022でのNon-Volatile Memory Express（NVMe）のサポート
  - NVMe over TCP / IPで作成されたVMDKレイアウト上のバックアップ、リストア、クローニング、検証のワークフロー
  - ESX 8.0 Update 2以降のNVMeファームウェアバージョン1.3をサポートします。Virtualハードウェアバージョン21が必要です。
  - Windows Serverフェイルオーバークラスタリング（WSFC）は、NVMe over TCP/IP上のVMDKを介したアプリケーションではサポートされません。
- SnapMirror Active Sync（当初はSnapMirror Business Continuity [SM-BC]としてリリース）をサポート。これにより、サイト全体に障害が発生してもビジネスサービスの運用を継続でき、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirror Active Syncでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

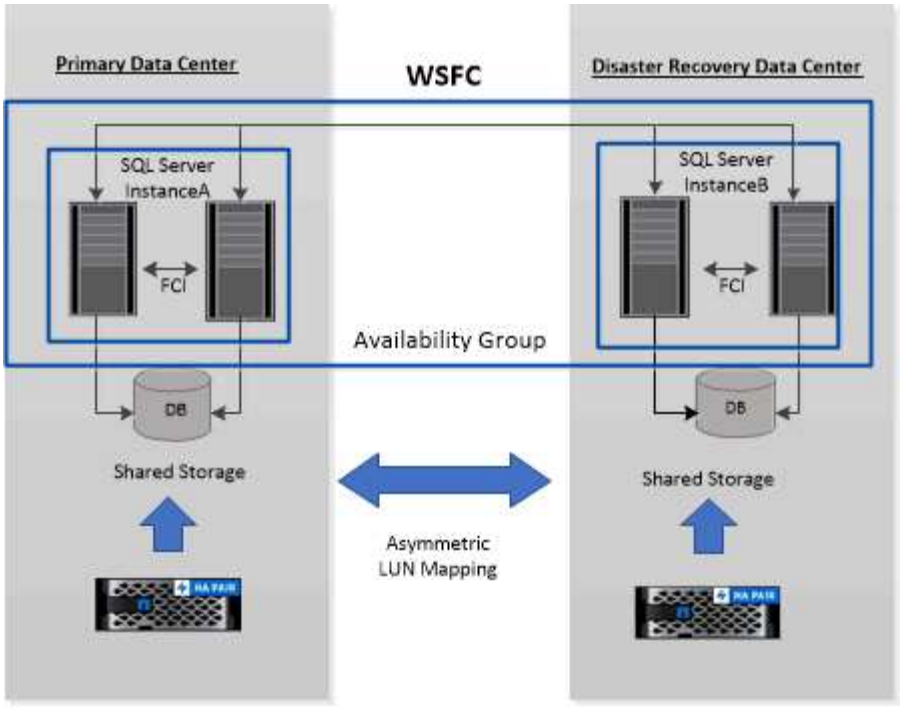
Windowsクラスタでの非対称LUNマッピングのサポート

SnapCenter Plug-in for Microsoft SQL Serverでは、SQL Server 2012以降での検出、高可用性用の非対称LUNマッピング（ALM）構成、ディザスタリカバリ用の可用性グループ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に1つ以上のノード、ディザスタリカバリセンターに1つ以上のノードを含む、単一のWindowsサーバフェイルオーバークラスタです。

次に、ALM設定の例を示します。

- マルチサイトデータセンターに2つのフェイルオーバークラスタインスタンス（FCI）
- ローカルのハイアベイラビリティ（HA）にはFCI、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には可用性グループ（AG）を使用



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には認識されず、その逆も同様です。

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ソリューションと、SQL AGで使用される非共有または専用ストレージソリューションを組み合わせたものです。AGソリューションでは、データセンター間で共有ディスクリソースに同じドライブレターを使用します。このストレージの配置（WSFC内のノードのサブセット間でクラスタディスクが共有される）は、ALMと呼ばれます。

SnapCenter Plug-in for 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 "NetApp Interoperability Matrix Tool"ください。

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セツソク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セツソク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。
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	
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。
VMware VM	NFSとSANの両方にVVOLデータストアを配置	VMware vSphere 向け ONTAP ツール	

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をプロビジョニングするには、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。 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

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、必要に応じて専用のLUNまたはVMDKを使用できます。

- マスターおよび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のトランザクションログファイル（.ldf）
- ログディレクトリ

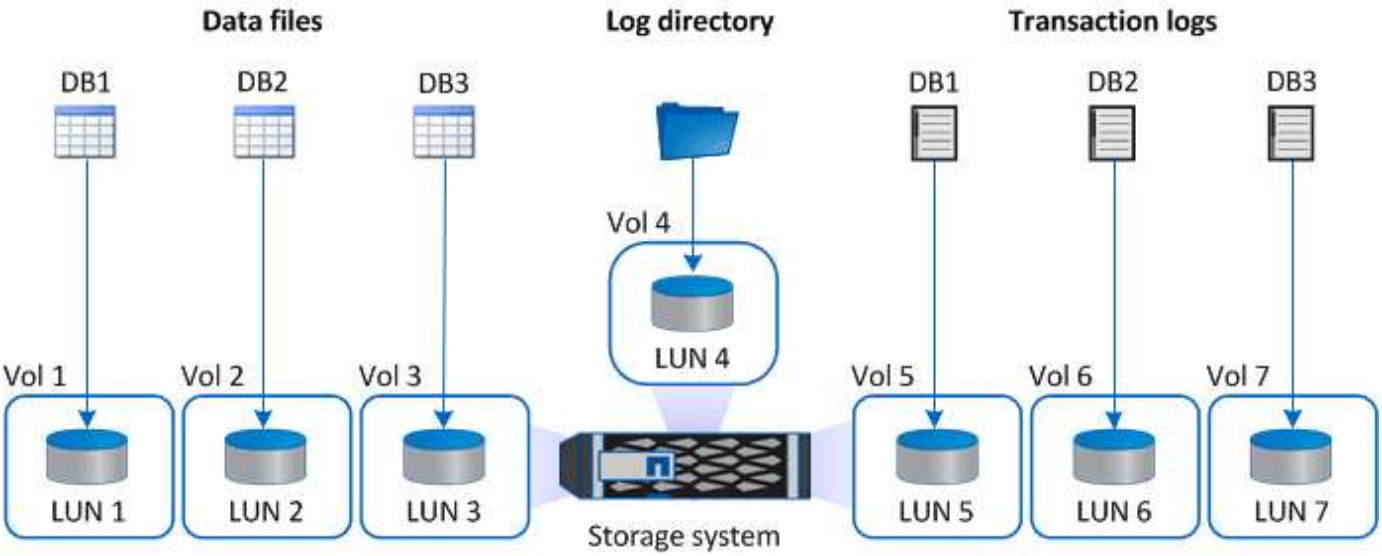
大規模なデータベースをリストアする場合は、専用のLUNまたはVMDKを使用することを推奨します。LUNま

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。

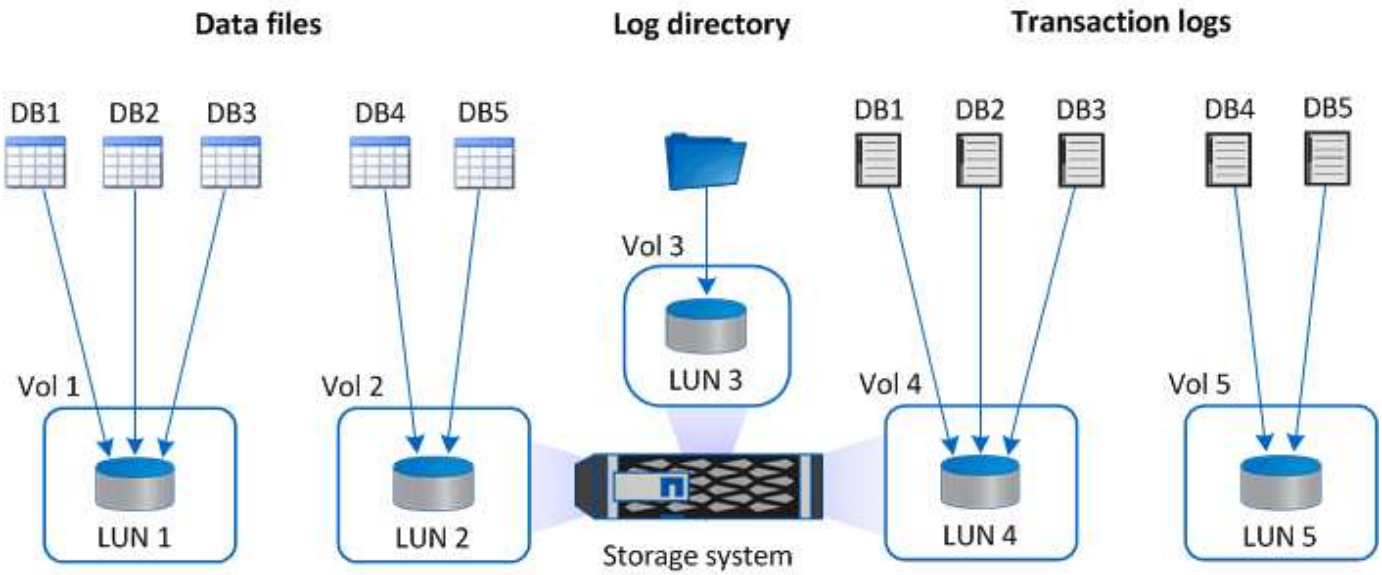
ログディレクトリについては、データファイルまたはログファイルのディスクに十分な空きスペースを確保するために、独立したLUNまたはVMDKを作成する必要があります。

LUNおよび**VMDK**のサンプルレイアウト

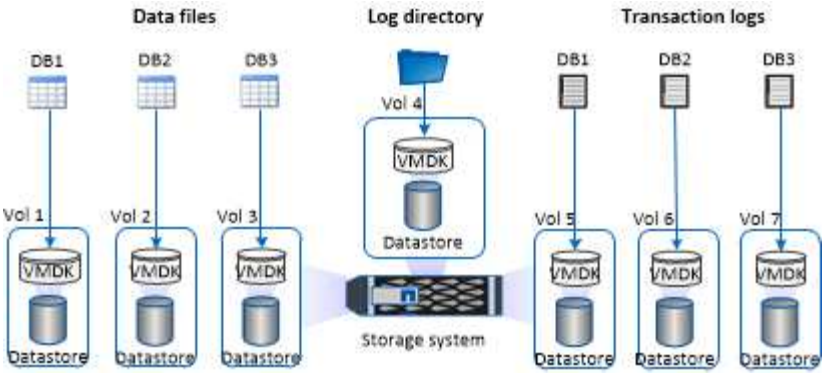
次の図は、LUN上の大規模データベースのストレージレイアウトを設定する方法を示しています。



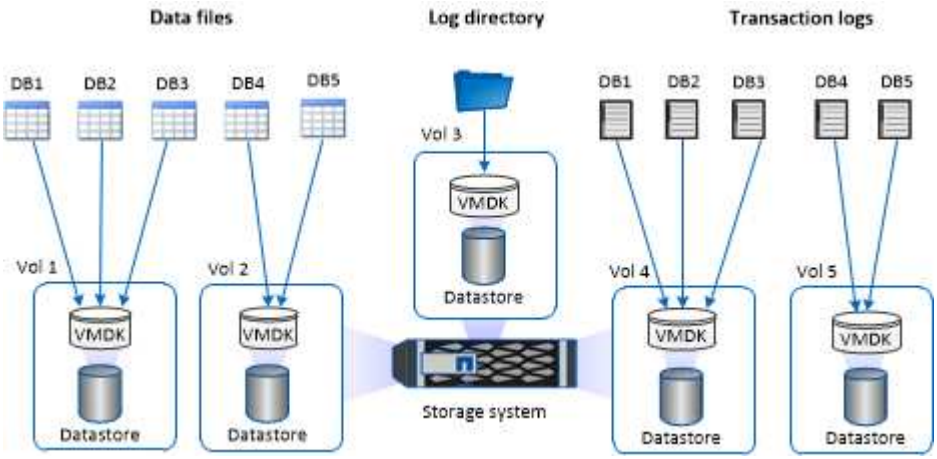
次の図は、LUN上の中規模または小規模データベースのストレージレイアウトを設定する方法を示しています。



次の図は、VMDK上の大規模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。



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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN
  - LUNの作成
  - lun delete
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード

- LUNマッピングの作成
- LUNマッピングの削除
- lun mapping remove-reporting-nodes
- lun mapping show
- LUN変更
- ボリューム内でのLUNの移動
- LUNオフライン
- LUNオンライン
- LUNのサイズ変更
- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete

- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show
- ネットワークインターフェイス
- network interface show
- SVM
- MetroClusterショー

Plug-in for SQL Server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 SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

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リソスノハツクアツフセンリヤク

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するのに役立ちます。バックアップ戦略の大部分は、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

SLAは、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要があるまでの時間です。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、RPOがバックアップ戦略に影響します。

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テクノロジを使用して、リソースが配置されてい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すると、SQL Serverでトランザクションログが切り捨てられないように指定

できます。このオプションは、他のバックアップアプリケーションでSQL Serverを管理する場合に使用します。トランザクションログをそのまま保持することで、すべて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の順序とは関係なく、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	バックアップタイプを指定したコピーのみのオプション
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で、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、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する必要があります。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できます。 masterおよびmsdb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せん。ただし、モデル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、およびmsdb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。

バックアップタイプ	説明	バックアップタイプを指定したコピーのみのオプション
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ます。コピーされるのは、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だけです。 フルデータベースバックアップととも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場合は、リカバリポイントをきめ細かく選択できます。	トランザクションログを切り捨てずにバックアップします。 このバックアップタイプは、定期的なログバックアップの順序には影響しません。コピーのみのログバックアップは、オンラインリストア処理を実行する場合に役立ちます。

Plug-in for SQL Serverノハツクアツフスケシユウル

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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。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とRPOはデータ保護戦略に影響します。

使用頻度の高いリソースであっても、フルバックアップを1日に1~2回以上実行する必要はありません。たとえば、定期的なトランザクションログバックアップで十分な場合は、必要なバックアップを作成できます。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つの部分があります。

- 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タイミング）は、リソースグループ設定の一部です。たとえば、リソースグループのポリシーで週単位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には、データベースのサイズ、使用されているボリュームの数、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よって決まります。たとえば、あるボリュームに小規模データベースのグループを配置し、別のボリュームに大規模データベースを配置した場合は、小規模データベース用に1つのバックアップジョブを作成し、大規模データベース用に1つのバックアップジョブを作成できます。

Plug-in for SQL Serverのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

Plug-in for SQL Serverノハツクアツフホシオフシヨン

バックアップコピーを保持する日数を選択することも、保持するバックアップコピーの数（ONTAPの最大コピー数255）を指定することもできます。たとえば、組織で、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する必要があるとします。

ポリシーの作成時に、バックアップタイプと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のスケジュールタイプを変更した場合、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が作成され、午後5時に別のフルバックアップが作成された場合、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にデータベースをリストアできます。トランザクションログが使用できない場合、Plug-in for SQL Server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。このリストア処理では、Plug-in for SQL Serverがフルバックアップが完了した時点のフルバックアップが完了した時点でデータベースが完了した時点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日です。デフォルトでは、SnapCenterの保持期間は最低2日です。

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では、バックアップあたりの最大データベース数を設定できるため（デフォルト値は100）、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、同じボリューム内に200個のデータベースがある場合、2つのSnapshotがそれぞれ100個のデータベースで作成されます。

Plug-in for SQL Server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

バックアップコピーは、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検証できます。セカンダリストレージボリュームを使用した検証により、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とセカンダリSnapshot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。そのため、ほとんどの場合、別のジョブであとで検証を実行する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、毎日午後5時にデータベースをバックアップする場合は、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、より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ノリストアセンリヤク

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、データベースを正常にリストアできます。

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のバックアップコピーからSQL Serverデータベースをリストアできます。また、データベースを元の場所だけでなく別の場所にリストアすることもできるため、要件に応じてリストア先を選択できます。

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。

デスティネーション	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	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異なるデータベース名を使用	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、別の名前のデータベースをリストアできます。

VMDK上のSQLデータベース（NFSおよびVMFSデータストア）については、ESXサーバ間の代替ホストへのリストアはサポートされていません。

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 々 のリカバリ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

  フルリカバリモデルを使用すると、障害ポイント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は、ログに一括記録された処理で挿入された行は含まれません。

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。

- 最新の状態へのリストア
- 過去のポイントインタイムへのリストア

最新の状態へのリストアまたは過去の特定の時点へのリストアは、次の状況で実行できます。

- SnapMirrorまたはSnapVaultセカンダリストレージからリストア
- 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。

最新の状態へのリストア

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をバックアップします。

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をリストアします。
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（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）が適用されます。

   トランザクションログは先に移動され、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では、連続する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対して最新の状態へのリストア機能を実行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の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、水曜日の午後4時にバックアップからリストアする必要があるとします。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。その後、バックアップがリストアされると、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（トランザクションログがバックアップされている場合）まで、すべてのトランザクションログが転送され、リストアされたデータベースに適用されます。

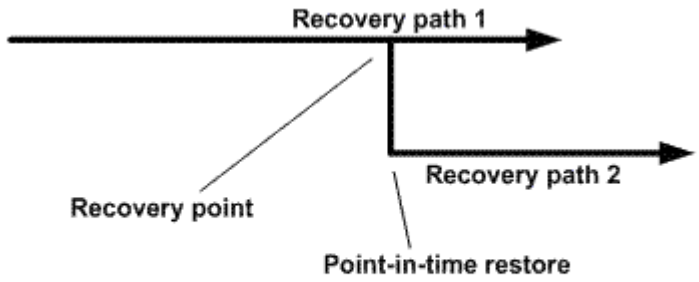
過去のポイントインタイムへのリストア

ポイントインタイムリストア処理では、データベースは過去の特定の時刻にのみリストアされます。ポイントインタイムリストア処理は、次の状況で実行されます。

- データベースは、バックアップトランザクションログの所定の時間にリストアされます。
- データベースがリストアされ、一部のバックアップトランザクションログのみが適用されます。

ある時点までデータベースをリストアすると、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、その後に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、リカバリパス2が発生します。新しいトランザクションログバックアップは、新しいフルバックアップを作成せずに作成されます。データの破損やその他の問題が原因で、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することはできません。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、バックアップトランザクションの適用を停止する日時を指定することもできます。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時間ごとに作成するとします。午前9時45分にデータベースがクラッシュしましたが、障害が発生したデータベースのトランザクションログは引き続きバックアップされます。ポイントインタイムリストアのシナリオは、次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、それ以降に行われたデータベース変更は失われます。（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時45分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します（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、トランザクションログバックアップを適用します。最後のトランザクションログバックアップセットからトランザクションをリストアする時間を指定します。（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。指定した日時より前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。

- 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ているLUN（たとえば、WindowsホストでMicrosoft iSCSIイニシエータを使用）から、同じWindowsホスト上のVMDKまたはRDM LUN、または別のWindowsホスト（またはその逆）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。
- クローンを含む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

  クローンデータベースは、新しいアプリケーションを開発する場合のベースラインとして使用でき、本番環境で発生したアプリケーションエラーの切り分けにも役立ちます。データベースのソフトエラーからのリカバリにも使用できます。

- クローンのライフサイクル

  SnapCenter を使用して、本番環境のデータベースがビジー状態でないときに定期的なクローニングジョブをスケジュール設定できます。

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ホストのローカルの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てください。

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。

ライセンス	必要な場合
SnapCenter Standard（コントローラベース）	FASマタハAFFストレエシコントロオラニヒツヨウ 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 Suiteライセンスをお持ちの場合は、SnapCenter Standardライセンスの使用権も取得できます。FASまたはAFFストレージに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。
SnapMirrorまたはSnapVault	ONTAP SnapCenterでレプリケーションが有効になっている場合は、SnapMirrorまたはSnapVaultのいずれか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 "SnapCenterライセンス"
SnapCenter Standard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 Standard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で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 https://imt.netapp.com/matrix/imt.jsp?components=121030;&solution=1259&isHWU&src=IMT、[Interoperability Matrix Tool^]を参照してください。

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 "Interoperability Matrix Tool"
CPU	• サーバホスト：4コア • プラグインホスト：4コア
RAM	• サーバホスト：8 GB • プラグインホスト：4GB

ホスト	最小要件
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およびログ用に7 GB • SnapCenterリポジトリ用に8GB • 各プラグインホスト：2GB（プラグインのインストールとログ用）。プラグインが専用ホストにインストールされている場合にのみ必要です。
サードパーティライブラリ	SnapCenter Serverホストおよびプラグインホストに必要： • Microsoft .NET Framework 4.7.2以降 • ASP。 Net Core Hosting Bundle（8.0.5以降） • PowerShell 7.4.2以降
ブラウザ	Chrome、Internet Explorer、Microsoft Edge

ポートタイプ	デフォルトポート
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と445に加えて、Microsoftが指定したダイナミックポート範囲もオープンにする必要があります。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"。
Windows向けSnapCenterプラグイン	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、および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

ローカル管理者権限があり、リモートホストに対するローカルログイン権限があるユーザが必要です。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に対する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サーバインストールパッケージをダウンロードし "NetAppサポートサイト" 、exeファイルをダブルクリックします。

   インストールを開始すると、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。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、エラーは修正する必要があります。

2. SnapCenterサーバのインストールに必要な値があらかじめ入力されていることを確認し、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中に、パスワードが自動的に生成されます。

   インストール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**：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. チェックボックスをオンにして、イベント管理システム（EMS）とAutoSupportを有効にします。
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のインストール

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

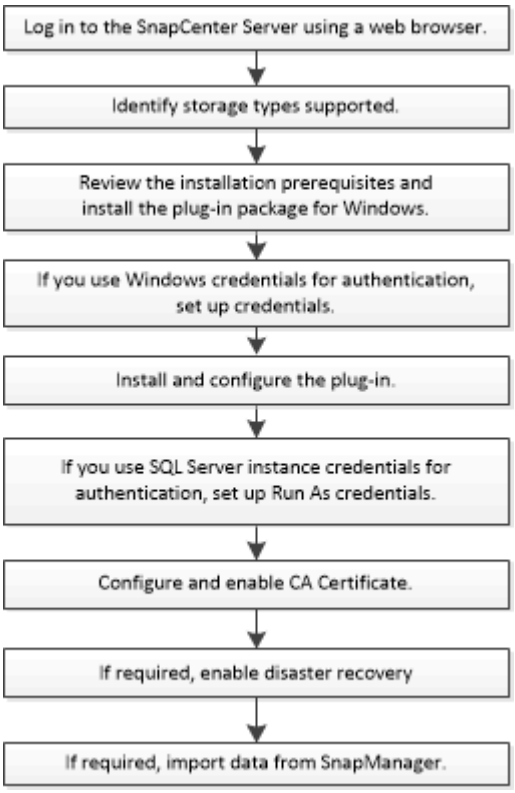
1. SnapCenter GUI の左ペインで、 **Hosts > Managed Hosts > Add** の順にクリックします。
2. ウィザードの[Hosts]ページで、次の手順を実行します。
   a. Host Type：Windowsホストタイプを選択します。
   b. ホスト名：SQLホストを使用するか、専用のWindowsホストのFQDNを指定します。
   c. Credentials：作成したホストの有効なクレデンシャル名を選択するか、新しいクレデンシャルを作成します。
3. インストールするプラグインの選択セクションで、 * Microsoft SQL Server * 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. 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。
   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. クラスタ内のすべてのホストを追加：WSFCでSQLを使用している場合は、このチェックボックスをオンにします。
   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オンにします。
5. [Submit （送信）] をクリックします。

SnapCenter Plug-in for Microsoft SQL Serverのインストールの準備

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に対する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ときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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。

- ホストを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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB

項目	要件
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Windowsのクレデンシャルを設定する

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースまたは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クレデンシャルをそれぞれ作成する必要があります。

開始する前に

- プラグインをインストールする前にWindows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には、管理者権限（リモートホストに対する管理者権限を含む）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。SQL Serverのsysadmin権限を持つユーザのクレデンシャルを設定します。

  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完了し、リソースを更新する必要があります。SQL

Server認証は、リソースのスケジュール設定や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. [クレデンシャル]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	操作
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` ◦ `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インスタンスが配置されている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、必要に応じて[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の設定

各ユーザの個 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ためのクレデンシャルを設定できます。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。

タスクの内容

- 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認証を有効にした場合は、検出されたインスタンスまたはデータベースに赤い南京錠のアイコンが表示されます。

  南京錠アイコンが表示された場合、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には、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する必要があります。

- 次の条件に該当する場合は、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。
  - クレデンシャルがSQLインスタンスに割り当てられます。
  - 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]*を選択します。
2. [設定]ページで、*[クレデンシャル]*を選択します。
   a. 新しいクレデンシャルを追加するには、*[New]*を選択します。
   b. [クレデンシャル]ページで、クレデンシャルを設定します。

フィールド	操作
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	操作
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は、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または管理者グループの任意のメンバーを指定します。 [ユーザ名]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（ワークグループの場合のみ）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のビルトイン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。[* ユーザー名 *] 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	SQL Server認証モードを選択します。WindowsユーザにSQL Serverに対するsysadmin権限がある場合は、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]*を選択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]*を選択します。
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. を選択し、ホスト名を選択してインスタンスをフィルタします。
   b. フィルタペインを閉じる場合に選択し ます。
3. [インスタンスの保護]ページで、インスタンスを保護し、必要に応じて*[クレデンシャルの設定]*を選択します。

   SnapCenterサーバにログインしているユーザがSnapCenter Plug-in for Microsoft SQL Serverにアクセスできない場合は、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. [リソースを更新]を選択します。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
. . コンピュータオブジェクトをグループに追加します。
. . 作成したユーザグループを使用してgMSAを作成します。
```

   例えば、

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
. . コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。
```

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。

6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスの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のインストール

ホストを追加して**SnapCenter Plug-ins Package for Windows**をインストールする

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。プラグインはリモートホストに自動的にインストールされます。

開始する前に

- SnapCenter Serverホストのオペレーティングシステムが Windows 2019で、プラグインホストのオペレーティングシステムが Windows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- 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。

- 組み込みでないクレデンシャルを指定してWindowsホストにプラグインをインストールする場合は、ホストの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running状態であることを確認する必要があります。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理Privilegesを使用してgMSAを設定する必要があります。

  "Windows Server 2016 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"

タスクの内容

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、ホストごとまたはクラスタごとに実行できます。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。

ホストの管理については、を参照してください "ホストの管理"。

手順

1. 左側のナビゲーションペインで、 **Hosts** を選択します。
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」を選択します。
4. [Hosts]ページで、次の手順を実行します。

フィールド	操作
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。 [Plug-ins]ページで[Microsoft SQL Server]オプションを選択すると、SnapCenter ServerによってPlug-in for SQL Serverがインストールされます。

フィールド	操作
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が適切に設定されているかどうか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ときに、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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

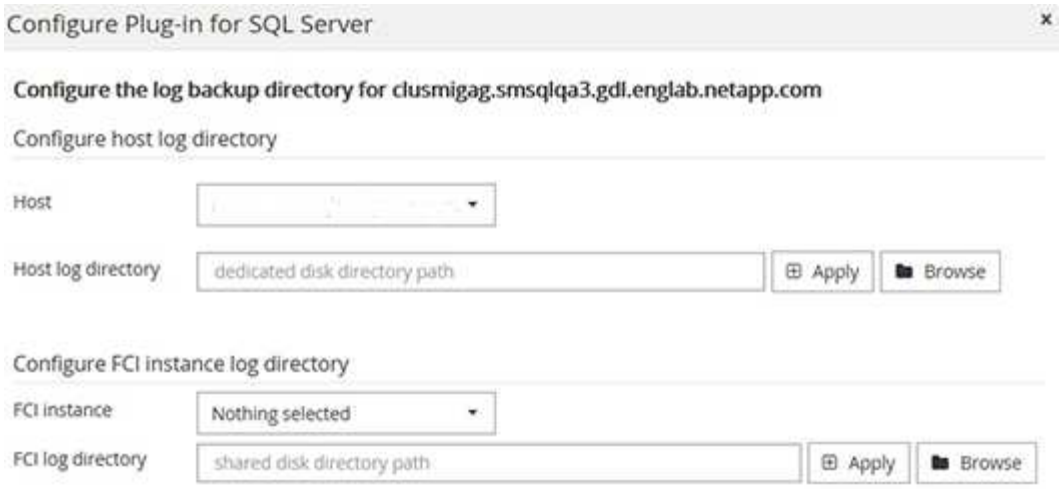
5. [インストールするプラグインを選択してください *] セクションで、インストールするプラグインを選択します。
6. [* その他のオプション *] を選択します。

フィールド	操作
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	操作
インストールパス	デフォルトのパスはC：\Program Files\NetApp\SnapCenter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	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オンにします。クラスタ内で使用可能な複数のSQL可用性グループを管理および識別する場合は、GUIで該当するクラスタの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。
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	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選択します。 gMSA名をdomainName\accountName$の形式で指定してください。 ホストにgMSAを追加し、gMSAにログインしてsys admin Privilegesがある場合、gMSAはSQLインスタンスへの接続に使用されます。

7. [送信] を選択します。
8. SQL Plug-inの場合は、ログディレクトリを設定するホストを選択します。
   a. を選択し、**[**ホストログディレクトリの設定**]**ページで[参照]*を選択して、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 ）] を選択します。

9. [送信] を選択します。

[インストール前チェックをスキップ]*チェックボックスを選択していない場合は、プラグインをインストールするための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バージョン、場所（Windowsプラグインの場合）、およびJava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、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\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。

10. 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た複数のリモートホストへの**SnapCenter Plug-in for Microsoft SQL Server**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、SnapCenter Plug-in for Microsoft SQL Serverを複数のホストに同時にインストールできます。

開始する前に

プラグインパッケージを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にログインしておく必要があります。

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。

4. 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の**SnapCenter Plug-in for Microsoft SQL Server**のサイレントインストール

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。

開始する前に

- 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があるかどうかを検証します。
2. Plug-in for SQL ServerソフトウェアをC：\ProgramData\NetApp\SnapCenter\Package Repositoryから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。

6. 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。
7. %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く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 GUIまたはPowerShellコマンドレットを使用してホストを追加することで、SnapCenterサーバにプラグインを登録できます。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のインストールステータスの監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

```
> 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ホストのプラグインサービスとバインドします。

```
> $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"
```

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、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の設定

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、次の手順に従って別のSQLホストに切り替えてデータをリカバリします。

開始する前に

- 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である必要があります。
- [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。詳細については、を参照してください "ホストの管理" 。

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およびSQLスケジュールを、DRバックアップのSnapCenter Plug-in for SQL Serverフォルダからインポートします。

関連情報

ビデオを参照してください "ディザスタリカバリ API" 。

SnapCenter Plug-in for SQL Server向けストレージディザスタリカバリ（**DR**）

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。

開始する前に

- プラグインがメンテナンスモードであることを確認します。
- SnapMirror / SnapVault関係を解除 "SnapMirror関係の解除"
- セカンダリのLUNを同じドライブレターでホストマシンに接続します。
- すべてのディスクが、DRの前に使用していたのと同じドライブレターを使用して接続されていることを確認します。
- MSSQLサーバー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。

タスクの内容

VMDKおよびRDM構成ではディザスタリカバリ（DR）はサポートされません。

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じように動作し続けます。

- DRモードで作成された新しいバックアップは、[Topology]ページの[SnapMirror]またはSnapVault（secondary）]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、これらのバックアップがDRモード中に作成されたことを示します。

- フェイルオーバー中に作成された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に一部のリソースをDR以外のモードにする場合は、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 "SnapCenter ソフトウェアコマンドレットリファレンスガイド"ください。

- 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。

開始する前に

- 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、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、関係の方向がフェイルオーバー前と同じであることを確認します。

  逆再同期処理の実行後もプライマリストレージとセカンダリストレージのロールを保持するには、逆再同期処理をもう一度実行します。

  詳細については、 "ミラー関係を逆再同期しています"

- MSSQLサーバー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中、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、次回のホスト更新処理で更新されます。

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

フェイルオーバー中に作成された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のインストール

データベースまたはファイルシステムが仮想マシン（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。

展開の詳細については、を参照してください "導入の概要"。

CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、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ファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリで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は、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

データ保護の準備

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。
- SnapCenter環境を設定するために、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-SmConfigureResources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から NetApp LUN（またはその逆）に移動します。

  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にあるSQLデータベースをSnapCenter Serverを使用して保護する場合は、SnapCenter Plug-in for VMware vSphereを導入して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。

  "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な場合は、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。NetAppデータブローカー1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetAppデータブローカー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を使用した仮想データベースおよび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 4.3.xのユーザ向けに、SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、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）を使用した仮想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 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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- 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。

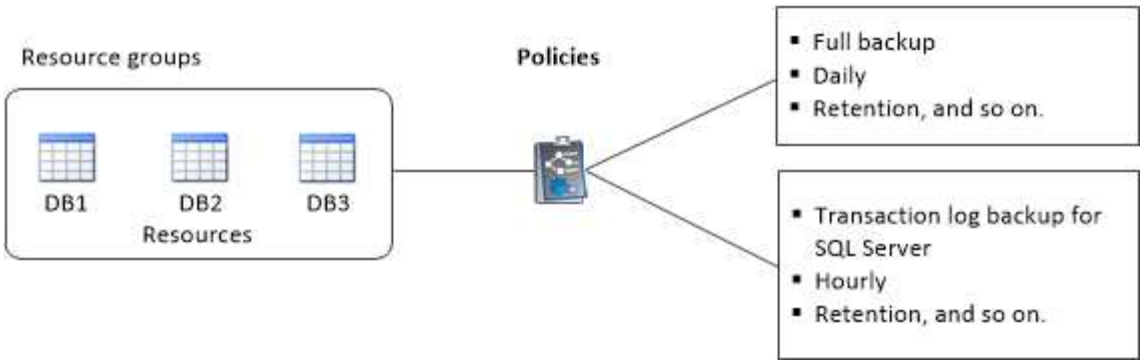
  単一のリソースまたはリソースグループをオンデマンドでバックアップできます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを実行することもできます。

- 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、そのグループのポリシーを1つ以上選択します。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または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。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。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時間ごと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、可用性グループをバックアップする

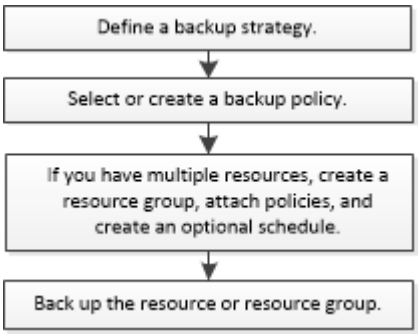
バックアップのワークフロー

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。

同じリソースに対してバックアップ処理とリストア処理を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。



ネットアップ以外の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した場合、[Resources]ページの[Backup Now]、[Restore]、[Manage Backups]、および[Clone]オプションは無効になります。

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、クローニングの各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、 "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では、Snapshotテクノロジを使用して、LUNまたはVMDK上にある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を作成することによってバックアップを作成します。

[Resources]ページでフルデータベースバックアップの対象となる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、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は、Snapshotを使用して同時にバックアップされます。同時バックアップ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を超える場合は、データベース数を35で割った数のSnapshotが作成されます。

バックアップポリシーでは、Snapshotごとの最大データベース数を設定できます。

SnapCenterがSnapshotを作成すると、ストレージ・システム・ボリューム全体がSnapshotに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です。

他のSQLホストサーバのデータが同じボリューム上にある場合、このデータをSnapshot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たリソースのバックアップ"

"リソースの休止処理またはグループ化処理が失敗する"

リソースをバックアップに使用できるかどうかの確認

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です。こ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ジョブを実行できますが、その前に使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。

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。
- 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ます。ユーザはSQLユーザまたはWindowsユーザです。
- Windowsクラスタ内の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）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上にある場合は、SnapCenter Plug-in for VMware vSphereを導入して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の導入"

- ホストにgMSAを追加し、gMSAにログインしてシステム管理Privilegesがある場合は、gMSAを使用してSQLインスタンスに接続されます。

タスクの内容

[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。

- データベースに十分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特定できないため、バックアップすることはできません。

SQL Server Standard Editionで可用性グループが設定されている場合、SnapCenterでバックアップできるのはプライマリデータベースのみです。

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、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。そのあとにをクリックすると、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。

   SnapCenter以外でデータベースの名前が変更された場合は、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NetApp以外のストレージにある場合は、 `Not available for backup` *[全体のステータス]*列にと表示されます。

     NetApp以外のストレージにあるデータベースに対しては、データ保護処理を実行できません。

   - データベースがNetAppストレージにあり、保護されていない場合は、 `Not protected` *[全体のステータス]*列にと表示されます。
   - データベースがNetApp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の*[全体のステータス]*列にメッセージが表示されます `Backup not run` 。

◦ データベースがNetAppストレージシステム上にあり、保護されている場合に、そのデータベースのバックアップがトリガーされると、ユーザインターフェイスの* Overall Status *列にメッセージが表示されます `Backup succeeded` 。

クレデンシャルの設定時にSQL認証を有効にした場合は、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。南京錠のアイコンが表示された場合は、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。

NetAppストレージシステムへのリソースの移行

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。

開始する前に

- 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リソースをリフレッシュ（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	操作
• 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	操作
• 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存在しない場合は、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）	1つのデータベースの複数のファイルを移行する場合は、このオプションを選択します。 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	操作
• 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	操作
*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 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および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。 • 内部データベーススナップショット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の作成

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。

開始する前に

- 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リソースをリフレッシュ（検出）しておく必要があります。
- Snapshot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、SnapCenter管理者が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Storage Virtual Machine（SVM）をユーザに割り当てておく必要があります。

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。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

タスクの内容

- バックアップポリシーは、バックアップを管理および保持する方法、およびリソースまたはリソースグループをバックアップする頻度を規定する一連のルールです。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することで、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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- SnapLock

  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。

    Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。

    ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

    プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

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]*を選択します。
2. [設定]ページで、*[ポリシー]*を選択します。
3. [New]*を選択します。
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. Snapshotごと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. Snapshotごと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

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。です。「 * 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をそのまま保持すると、すべて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に対して設定された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）

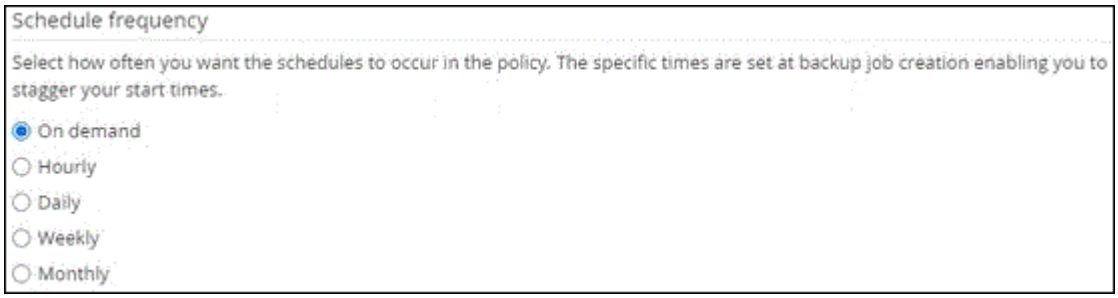
バックアップのAGレプリカを決定する最小バックアップ優先順位と最大バックアップ優先順位を指定します。たとえば、最小優先度を10、最大優先度を50に設定できます。この場合、優先度が10より大きく50未満のすべてのAGレプリカがバックアップ対象とみなされます。

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、バックアップがクラスタの各ノードで保持されます。AGの所有者ノードが変更された場合、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）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ができます。

午前2時にスケジュールを設定している場合、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. [Retention settings for the up-to-the-minute restore operation]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の総数を指定
      i. 保持するSnapshot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の数が指定した数を超えると、最も古いコピーから順にSnapshotが削除されます。

デフォルトでは、保持数の値は2に設定されています。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。

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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。

1. Snapshotを保持する期間
   a. Snapshotを保持してから削除するまでの日数を指定する場合は、*[Keep Snapshot copies for]*を選択します。
2. Snapshotのロック期間を指定する場合は、*[Snapshot copy locking period（Snapshotコピーロック期間）]*を選択し、日数、月数、または年数を選択します。

   SnapLock保持期間は100年未満にする必要があります。

3. [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の総数を指定
      i. 保持するSnapshot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の数が指定した数を超えると、最も古いコピーから順にSnapshot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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。

1. Snapshotを保持する期間

a. Snapshot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。

2. Snapshotのロック期間を指定する場合は、*[Snapshot copy locking period（Snapshotコピーロック期間）]*を選択し、日数、月数、または年数を選択します。

   SnapLock保持期間は100年未満にする必要があります。

   ログSnapshotの保持期間は、デフォルトで7日に設定されています。Set-SmPolicyコマンドレットを使用して、ログのSnapshot保持期間を変更します。

この例では、ログのSnapshot保持数を2に設定しています。

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がデータベースのSnapshotコピーを保持"

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の更新

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。

   このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。

   セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。

   を参照して "[Topologyページでの SQL Serverのバックアップとクローンの表示"]

SnapVaultの更新

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。

   セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。

   SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。

   SnapLock Vaultの詳細については、を参照してください。 "SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする"

   を参照して "[Topologyページでの SQL Serverのバックアップとクローンの表示"]

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ラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。

> 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、ログの送信を行うスクリプトを実行できます。

   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からの相対パスである必要があります。

   セカンダリストレージがSnapshot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_ERRORMSGS）
      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. クラスタ化されていないインデックスをチェックしない（NOINDEX）
      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 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および物理的な整合性をチェックします。
   e. 内部データベーススナップショット（TABLOCK）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
      i. 内部データベースSnapshot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、*[内部データベースSnapshotコピー（TABLOCK）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]*を選択します。
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からの相対パスである必要があります。

ステップ**7**：概要を確認します

1. 概要を確認し、*[終了]*を選択します。

SQL Serverのリソースグループの作成とポリシーの適用

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す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。また、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必要があります。

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。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定されたリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいデータベースを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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、 [* 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	操作
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。

フィールド	操作
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	オプション：Snapshotのカスタムの名前と形式を入力します。たとえば、customText_resourcegroup_policy_hostnameやresourcegroup_hostnameなどです。デフォルトでは、Snapshot名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。

      **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. [Configure schedules for selected policies]セクションで、スケジュールを設定するポリシーの[Configure Schedules]列にある***をクリックします + 。
   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、 [*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。

スケジュール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 scheduler]を選択しない場合、デフォルトは[Microsoft Windows scheduler]になります。

サードパーティの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はサポートされません。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は、プライマリデータベースをホストしているSQLサーバのバージョンおよび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	操作
バックアップ後に検証を実行	[Run verification after backup] を選択します。
検証のスケジュールを設定	[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、削除するに はをクリックします ✖ 。

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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。

関連情報

"SQL Serverデータベースのバックアップポリシーの作成"

SQLリソスノハツクアツフノヨウケン

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NetApp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）ユーザが開始したバックアップ処理は、そのADユーザまたはグループにSQLインスタンスクレデンシャルが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。
- ポリシーを適用して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、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トリガーされることがあります。Set-SmConfigSettings PSコマンドレットを使用して、web.configでFMaxRetryForUninitializedHostsの値を設定する必要があります。

SQL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、のページからバックアップすることができます。

タスクの内容

- Windowsクレデンシャル認証の場合、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。
- 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
- gMSAを使用してホストを追加し、gMSAにログインおよびシステム管理者権限があれば、gMSAからSQLインスタンスへの接続が許可されます。
  - SnapCenterは、SQLインスタンスの認証が設定されているかどうかを検証します。認証が設定されている場合、このクレデンシャルを使用してSQLインスタンスにアクセスします。
  - 認証が設定されていない場合は、gMSAを使用してSQLプラグインが現在動作しているかどうかを確認します。プラグインが動作している場合は、SQLインスタンスへの接続の確立に使用されます。
  - SQLインスタンスの両方の認証が設定されておらず、プラグインが動作していない場合、SQLインスタンスはWindowsクレデンシャル認証を介してアクセスされます。

SnapCenter UI

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 * 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。

      インスタンスのバックアップを作成する場合、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、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名に使用するカスタムの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名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、**を選択し てポリシーウィザードを開始します。

      [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. 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]列で**を選択します 。

   c. [ポリシーのスケジュールを追加]* `policy_name` ダイアログボックスで、スケジュールを設定し、*[OK]*を選択します。

      `policy_name`選択したポリシーの名前が表示されます。

   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のエディションのバージョン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、**を選択します  。

c. Add Verification Schedules_policy_name_dialog box で、次の処理を実行します。

状況	操作
バックアップ後に検証を実行	[バックアップ後に検証を実行] を選択します。
検証のスケジュールを設定	[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 *」を選択します。

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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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、*[終了]*を選択します。

データベーストポロジページが表示されます。

8. [今すぐバックアップ]*を選択します。

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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

b. 「 * Verify after backup * 」を選択して、バックアップを検証します。

c. 「 * Backup * 」を選択します。

> 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

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、[User Access]ページでそれぞれのユーザ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。

10. 処理の進捗状況を監視するために、**[監視]>*[ジョブ]*を選択します。

終了後

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

  "MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

- VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、バックアップが失敗することがあります。Java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、コマンドによって `do_start method` 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 `Java -jar -Xmx8192M -Xms4096M`ます。

関連情報

"SQL Serverデータベースのバックアップポリシーの作成"

"PowerShellコマンドレットを使用したリソースのバックアップ"

"TCP_TIMEOUTでの遅延が原因で、MySQL接続エラーが発生してバックアップ処理が失敗する"

"Windowsスケジューラエラーでバックアップが失敗する"

"リソースの休止処理またはグループ化処理が失敗する"

PowerShellコマンドレット

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バックアップタイプがFULLBACKUPの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がcrashConsistentの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、指定したホスト上の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、SnapCenterに新しいリソースグループを追加します。

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します。

```
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。

   次に、指定した日付に実行されたすべてのジョブのジョブ概要レポートを表示する例を示します。

```
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"。

SQL Serverリソースグループのバックアップ

リソースグループは、[Resources]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、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。

   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、を選択し  てタグを選択します。その後、を選択してフィルタペインを閉じることができます  。

3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   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. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

関連情報

"SQL Serverデータベースのバックアップポリシーの作成"

"SQL Serverのリソースグループの作成とポリシーの適用"

"PowerShellコマンドレットを使用したリソースのバックアップ"

"TCP_TIMEOUTでの遅延が原因で、MySQL接続エラーが発生してバックアップ処理が失敗する"

"Windowsスケジューラエラーでバックアップが失敗する"

バックアップ処理の監視

SnapCenterジョブページで**SQL**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、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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、**SQL**リソースに対するデータ保護処理を監視する

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

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する

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しておく必要があります。

開始する前に

- 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でサポートする各ストレージシステムには、一意の名前と一意の管理LIF IPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

この例では、PowerShellセッションを開きます。

```
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。

   新しいストレージシステム接続を作成する例を次に示します。

```
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。

   この例では、Windowsクレデンシャルを使用してFinanceAdminという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"。

SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理をキャンセルする

実行中、キューに格納されている、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、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、SnapCenterサーバは処理を停止し、ストレージからすべてのSnapshot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、キャンセルがトリガーされても、作成済みのSnapshotはロールバックされません。

開始する前に

- 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、キューに登録されているか実行中のログ処理またはフルバックアップ処理だけです。
- 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すると、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]ページまたは[Activity]ペインからキャンセルできます。
- SnapCenter GUIに加え、PowerShellコマンドレット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

手順

次のいずれかを実行します。

アクセス元	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、**[モニタ]**>*[ジョブ]*を選択します。 2. ジョブを選択し、*[ジョブのキャンセル]*を選択します。
[Activity]ペイン	1. バックアップジョブを開始したら、[Activity]ペインでを選択して、 ペインアイコン"] 最新の5つの処理を表示します。 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]*を選択します。

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。キャンセルした処理がキャンセルまたは実行中の状態で応答しない場合は、コマンドレット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 `Cancel-SmJob -JobID <int> -Force` 。

[Topology]ページでのSQL Serverのバックアップとクローンの表示

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ときに、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立つことがあります。

タスクの内容

[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、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。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-

 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。

-  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、バックアップを4つだけ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。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。

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はクローンデータベースを保護し、[Topology]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. [Summary]カードで、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の概要を確認します。

   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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールで

は、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

5. [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。

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にあるバックアップは、名前の変更や削除はできません。

7. テーブルからクローンを選択し、 * Clone Split * をクリックします。
8. 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たバックアップの削除

Remove-SmBackupコマンドレットを使用すると、他のデータ保護処理で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。

```
PS C:\> Open-SmConnection
```

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を使用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たセカンダリバックアップ数のクリーンアップ

Snapshot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するには、Remove-SmBackupコマンドレットを使用します。このコマンドレットは、[Manage Copies]トポロジに表示されるSnapshotの総数が、セカンダリストレージのSnapshotの保持設定と一致しない場合に使用できます。

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を含ま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。

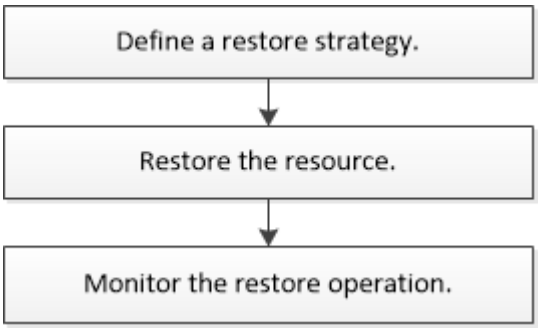
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

SQL Serverリソースのリストア

リストアのワークフロー

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、クローニングの各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、 "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 *

"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たリソースのリストアとリカバリ"

"Windows 2008 R2でリストア処理が失敗することがある"

データベースをリストアする際の要件

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SQL Serverインスタンスがオンラインで実行されている必要があります。

  これは、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に該当します。

- 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場合は、可用性グループ（AG）のバックアップをリストアする権限を他

のロールに付与してください。

次のいずれかの条件が満たされると、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別の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。KB2887595の詳細については、Microsoftサポートサイトを参照してください。

  "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、SnapCenter管理者が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に対してStorage Virtual Machine（SVM）を割り当てておく必要があります。

  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、すべてのバックアップジョブとクローンジョブを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応じてタイムアウト値を変更でき、設定可能な最大値は86400000ミリ秒です。

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データベースバックアップのリストア

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。データベースリストアは複数の段階からなるプロセスで、指定したSQL Serverバックアップのすべてのデータページとログページが指定したデータベースにコピーされます。

タスクの内容

- バックアップしたSQL Serverデータベースは、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（リソースを所有するノードがダウンした場合など）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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

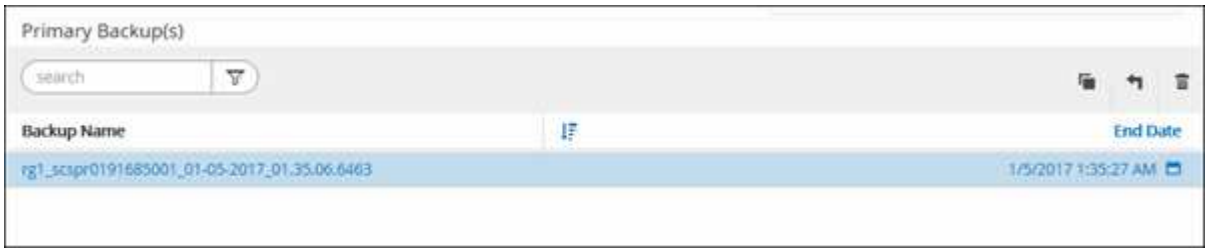
- リストアウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要なフィールドを取り上げます。
- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択する必要があります。
- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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、アイコンをクリックします  。



6. [Restore 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
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する	このオプションは、バックアップが作成されたSQL Serverにデータベースをリストアする場合に選択します。
別のホストへのデータベースのリストア	このオプションは、バックアップを作成するホストまたは別のホストにある別のSQL Serverにデータベースをリストアする場合に選択します。 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である必要があります。 [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。

オプション	説明
既存のデータベースファイルを使用したデータベースのリストア	このオプションは、バックアップが作成されたホストと同じホスト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に選択します。 指定した既存のファイルパスに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。
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。
次のログバックアップまで：	「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。
次の日付まで	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。

オプション	説明
カスタムログディレクトリを使用	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。 カスタムログディレクトリは可用性グループデータベースではサポートされていません。

8. [PreOps]ページで、次の手順を実行します。

   a. [PreRestore Options]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、ログの送信などを行うスクリプトを実行できます。

      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からの相対パスである必要があります。

9. [Post Ops]ページで、次の手順を実行します。

   a. [Choose database state after restore completes]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して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。

  このオプションはコミットされていないトランザクションを元に戻しますが、元に戻したアクションをスタンバイファイルに保存して、リカバリ効果を元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のドキュメントを参照してください。

b. 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、ログの送信などを行うスクリプトを実行できます。

   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からの相対パスである必要があります。

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。

11. 概要を確認し、 [完了] をクリックします。
12. [* Monitor * > * Jobs *] ページを使用してリストア・プロセスを監視します。

PowerShellコマンドレット

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

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できます。リストア機能は段階的に行われ、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されたSQL Serverバックアップから指定されたデータベースにコピーされます。

開始する前に

- 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をレプリケートしておく必

要があります。

- SnapCenterサーバと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。

タスクの内容

SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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 **[** 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. [Location]ページで、選択したリソースをリストアするデスティネーション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

他のデータベースで共有され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に物理レベルの破損がないことを確認する必要があります。

PowerShellコマンドレットを使用したリソースのリストア

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

可用性グループデータベースの再シード

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。

開始する前に

- 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。

タスクの内容

- プライマリデータベースで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ると、再シード処理を実行できません。レプリカが削除されると、再シード処理は失敗します。
- 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際には、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、再シード処理が失敗し、ミラーデータベース「database_name」にプリンシパルデータベースエラーメッセージ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。

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。

SQLリソースのリストア処理の監視

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

SQLリソースのリストア処理をキャンセルします。

キューに登録されているリストアジョブは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。

タスクの内容

- 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。
- キューに格納されているリストア処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用して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。

アクセス元	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。
[Activity]ペイン	1. リストア処理を開始したら、[Activity]ペインをクリックして、 最新の5つの処理を表示します。 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。

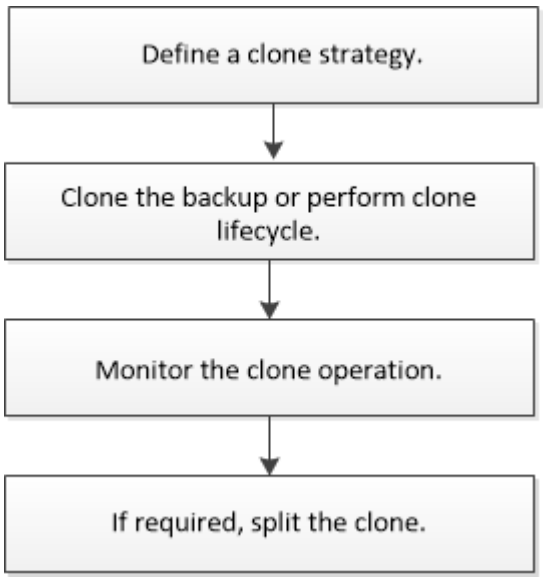
SQL Serverデータベースリソースのクローニング

クローニングのワークフロー

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サーバを使用して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。データベースをクローニングして、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構造とコンテンツを使用してテストしたり、データウェアハウスへのデータの取り込み時にデータの抽出と操作のツールを使用したり、誤って削除または変更されたデータをリカバリしたりできます。

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、クローニングの各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、 "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したり完了までに時間がかかることがある"

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。

開始する前に

- 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実行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て代替ホストにクローニングする際にセカンダリロケータを検出するには、データLUNとログLUNの保護タイプ（mirror、vault、mirror-vaultなど）を同じにする必要があります。
- SnapCenter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）の割り当て済みアグリゲートリストに含まれている必要があります。

タスクの内容

- 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場合は、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場合は、マウントポイントが存在し、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ているvFCイニシエータまたは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でサポートされるイニシエータはホストごとに1つだけであるためです。
- 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上に配置されます。
- 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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

  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。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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 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。

3. データベースまたはリソースグループを選択します。
4. [* コピーの管理 *] 表示ページで、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。
5. バックアップを選択し、**を選択します。
6. [クローンオプション]*ページで、次の操作を実行します。

フィールド	操作
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。
クローンインスタンス	データベースバックアップをクローニングす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インスタンスを指定する必要があります。
クローンサフィックス	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。

フィールド	操作
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、パスを使用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。マウントポイントは、そのディレクトリ内に作成されます。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。

7. 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	操作
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。
次のログバックアップまで：	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は、このオプションを選択します。
次の日付まで	クローンデータベースにトランザクションログを適用するまでの日時を指定します。 このポイントインタイムクローンは、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のクローニングを停止します。

8. [Script *]ページで、クローニング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スクリプトタイムアウト、パス、および引数を入力します。

   たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などを行うスクリプトを実行できます。

   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からの相対パスである必要があります。

   デフォルトのスクリプトタイムアウトは60秒です。

9. [**Notification**] ページの **[*Email preference**] 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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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の場合は、 "EMSデータ収集の管理"

10. 概要を確認し、*[終了]*を選択します。
11. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

終了後

クローンの作成後は、名前を変更しないでください。

関連情報

"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したり完了までに時間がかかることがある"

"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する"

PowerShellコマンドレット

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一覧を表示します。

次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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します。

   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、クローン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に対して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。

開始する前に

- 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場合は、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場合は、マウントポイントが存在し、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上に配置されます。

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。

タスクの内容

- 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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- 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。
- ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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 *] 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	操作
クローンジョブ名	クローンライフサイクルジョブの監視や変更に役立つ名前を指定します。
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。
クローンインスタンス	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インスタンスを指定する必要があります。

フィールド	操作
クローンサフィックス	クローンデータベースに付加される、クローンデータベース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、パスを使用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。パスを使用してボリュームマウントポイントを自動割り当てするように選択すると、特定のディレクトリを指定できます。マウントポイントは、そのディレクトリ内に作成されます。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、ログの送信などを行うスクリプトを実行できます。

   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からの相対パスである必要があります。

   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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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の場合は、 "EMSデータ収集の管理"

9. 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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。
  3. [* ジョブ *] ページで、次の手順を実行します。
     a. をクリックしてリストをフィルタリングし、クローニング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. [**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。

タスクの内容

- 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。
- キューに登録されているクローン処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用してキャンセルできます。
- 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。

アクセス元	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。
[Activity]ペイン	1. クローン処理を開始したら、[Activity]ペインでをクリックして、 最新の5つの処理を表示します。 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する

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングまたは検証が失敗する"

SAP HANAデータベースを保護

SAP HANAデータベース向けSnapCenterプラグイン

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、単一コンテナとマルチテナントデータベースコンテナ（MDC）をサポートします。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 プラグインでは、異なる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とNetApp SnapMirrorテクノロジを使用して、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、本プラグインをNetApp SnapVaultテクノロジとともに使用して、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。

Plug-in for SAP HANA Databaseは、SnapMirrorのアクティブな同期（当初はSnapMirror Business Continuity [SM-BC]としてリリース）をサポートしています。この同期機能を使用すると、サイト全体に障害が発生してもビジネスサービスの運用を継続でき、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirror Active Syncでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

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します。
- 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およびストレージシステム上でNetApp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は、Plug-in for SAP HANA DatabaseでNetAppのSnapshotテクノロジを使用してリソースをバックアップします。

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。
- RBACでサポートされるセキュリティと一元化されたロール委譲

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルの権限を付与することもできます。

- NetApp FlexCloneテクノロジを使用して、テストまたはデータ抽出に使用するリソ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できます。

  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。

- バックアップ作成時に、ONTAPの整合グループ（CG）Snapshot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可能

  1回の処理では、1つのホスト内のリソースが同じボリュームを共有する場合にSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成する機能。
- 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のLinux LVMのサポート。

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	iSCSIセツソクLUN
物理サーバと仮想サーバ	• FCセツソクLUN • NFS接続ボリューム
VMware ESXi	NFSとSANの両方にVVOLデータストアを配置 VVOLデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

SAP HANA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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN
  - LUNの作成
  - LUNの作成
  - LUNの作成
  - lun delete
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード
  - LUNマッピングの作成
  - LUNマッピングの削除
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - LUN変更
  - ボリューム内でのLUNの移動

- LUNオフライン
- LUNオンライン
- LUN永続的予約のクリア
- LUNのサイズ変更
- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成

- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- volume snapshot modify -snaplock-expiry-time
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限
  - ネットワークインターフェイス
  - network interface show
  - SVM

SAP HANAデータベース向けに、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 SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

タスクの内容

SLAは、期待されるサービスレベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要がある時間です。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ます。SLA、RTO、RPOは、データ保護戦略に影響します。

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. アプリケーションと整合性のあるデータベースのSnapshotをバックアップするSnapshotコピーベースのポリシーを作成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. レプリケーションにNetApp SnapMirrorテクノロジを使用するか、長期保持に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とSnapMirrorデスティネーションのSnapshotの保持期間を決定します。

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データベースとデータボリューム以外のボリュームです。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

  プラグインのインストールまたはアップグレード後、一元化された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続行されます。

  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）

  プラグインのインストールまたはアップグレード後、一元化された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にアップグレードしたあとも、一元化された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に直接登録されている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の自動検出がトリガーされます。プラグインをアップグレードすると、プラグインホストに配置されていたすべてのMDCリソースについて、別のGUID形式で別の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。

  たとえば、SnapCenter 4.2では、E90MDCリソースがプラグインホストにあり、手動で登録されている場合、SnapCenter 4.3へのアップグレード後に、別のGUIDを持つ別のE90MDC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、それらのリソースではデータ保護処理がサポートされません。

- 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

Backup typeには、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。

ファイルベースのバックアップ

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テクノロジを活用して、SAP HANAデータベースが格納されているボリュームのオンラインの読み取り専用コピーを作成します。

SnapCenter Plug-in for SAP HANA Databaseでの整合グループ**Snapshot**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を作成できます。整合グループはコンテナであり、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。整合グループは、複数のボリュームの同時Snapshotであり、ボリュームグループの整合性のあるコピーを提供します。

ストレージコントローラが整合性のあるSnapshotをグループ化するまでの待機時間を指定することもできます。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の処理中に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の同期により、整合グループSnapshot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と、SAP HANA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の削除時にも削除されます。

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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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つの部分があります。

- 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タイミング）

  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単位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には、リソースのサイズ、使用されているボリュームの数、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テタヘスノハツクアツフノメイメイキソク

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

SAP HANAデータベースのリストアとリカバリ戦略

SAP HANAリソースのリストアとリカバリの戦略を定義

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リソースに対してサポートされるリストア戦略を確認する
2. 自動検出されたSAP HANAデータベースに対してサポートされるリストア戦略を確認する
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、戦略を定義する必要があります。手動で追加したSAP HANAリソースには、2種類のリストア戦略があります。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

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のあとに作成されたSnapshot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
- 選択したLUNのみをリストア

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、戦略を定義する必要があります。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
  - 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のあとに作成されたSnapshot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

「 * 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データベースに対して、ボリュームベースSnapRestore（VBSR）、単一ファイルSnapRestore、および接続とコピーのリストアタイプがサポートされます。

ボリュームベース**SnapRestore**（**VBSR**）は、**NFS**環境で次のシナリオで実行されます。

- 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**Single File SnapRestore**を実行するシナリオは、次のとおりです。

- 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

接続およびコピーベースのリストアは、**SAN**環境で次のシナリオで実行されます。

- 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では、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。

- 最新の状態までデータベースをリカバリします。
- 特定のポイントインタイム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。

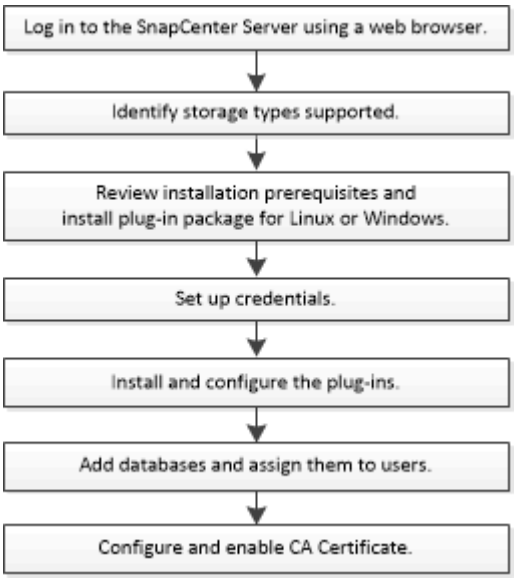
- 特定のデータバックアップまでデータベースをリカバリ

SnapCenterでは、SAP HANAデータベースに対して[No recovery]オプションも用意されています。

SnapCenter Plug-in for SAP HANA Databaseのインストールの準備

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。

- Java 11をホストにインストールしておく必要があります。

  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システム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ときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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、HDBのセキュアなユーザストアキーには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Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- Plug-in for SAP HANA DatabaseをWindowsホストにインストールすると、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以外のユーザに対して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 11をWindowsホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

Linuxホスト

- rootユーザまたはroot以外のユーザに対して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 11をLinuxホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

- LinuxホストでSAP HANAデータベースを実行している場合は、Plug-in for SAP HANA Databaseのインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- 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。

補助コマンド

SnapCenter Plug-in for SAP HANAで補足コマンドを実行するには、ファイルにそのコマンドを含める必要があります `allowed_commands.config` 。

`allowed_commands.config` ファイルは、SnapCenter Plug-in for SAP HANAディレクトリの「etc」サブデ

ィレクトリにあります。

Windowsホスト

デフォルト： `C:\Program Files\NetApp\SnapCenter\HANA\etc\allowed_commands.config`

カスタムパス：
`<Custome_Directory>\NetApp\SnapCenter\HANA\etc\allowed_commands.config` Windowsホスト：

Linuxホスト

デフォルト： `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

カスタムパス： `<Custome_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config`

プラグインホストで追加のコマンドを許可するには、エディタでファイルを開きます `allowed_commands.config` 。各コマンドを別 々 の行に入力します。大文字と小文字は区別されません。例えば、

コマンド:mount

コマンド：umount

完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符（"）で囲みます。例えば、

コマンド："C：\Program Files\NetApp\SnapCreator commands\sdcli.exe"

コマンド：myscript.bat

ファイルが存在しない場合は `allowed_commands.config` 、コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

コマンドまたはスクリプトがに存在しないと、 `allowed_commands.config`コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

ワイルドカードエントリ（*）を使用してすべてのコマンドを許可しないでください。

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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、基本的なホストシステムのスペースとサイジングの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 • 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 "NetApp Interoperability Matrix Tool" ください。

項目	要件
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量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、最近実行した処理の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 11 Oracle JavaおよびOpenJDK を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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 "NetApp Interoperability Matrix Tool" ください。

SnapCenter Plug-in for SAP HANA Databaseのクレデンシャルを設定する

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースまたは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クレデンシャルをそれぞれ作成する必要があります。

タスクの内容

- Linuxホスト

  Linuxホストにプラグインをインストールするには、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、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo Privilegesがあるroot以外のユーザに対して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

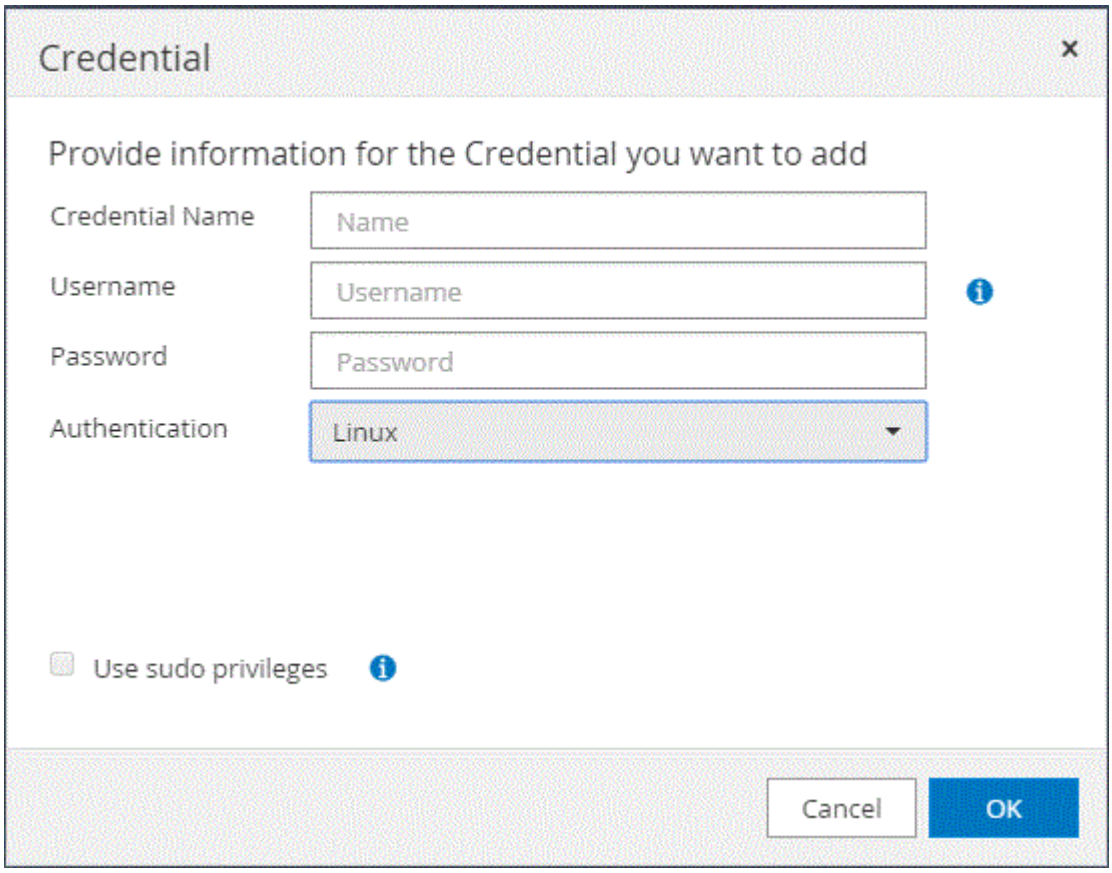
  プラグインをインストールする前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモートホストに対する管理者権限を含む）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、ユーザ名に完全なadmin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の権限を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、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	操作
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	操作
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。ユーザ名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	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ユーザのみに適用されます。

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、必要に応じて[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を割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
      ```

      . . コンピュータオブジェクトをグループに追加します。
      . . 作成したユーザグループを使用してgMSAを作成します。

      例えば、

      ```
      New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
      -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      ```

      . . コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。

6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスの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のインストール

ホストを追加してリモートホストにプラグインパッケージをインストールする

SnapCenterの[ホストを追加]ページを使用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。プラグインはリモートホストに自動的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、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- 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、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストの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する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理Privilegesを使用してgMSAを設定する必要があります。

  "Windows Server 2016 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"

タスクの内容

- 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場合は、 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]*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	操作
ホストタイプ	ホストのタイプを選択します。 • ウィンドウ • Linux 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が適切に設定されているかどうか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をこのホストに設定する必要があります。

フィールド	操作
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]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	操作
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。
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。

フィールド	操作
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	Windowsホストで、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$の形式で指定してください。 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 prechecks]チェック ボックスを選択していない場合、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を検証するためにホストが検証されます。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）、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、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\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。

9. 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た複数のリモートホストへの**SnapCenter Plug-in Package for Linux / Windows**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、複数のホストにSnapCenter Plug-in Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグインパッケージを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にログインしておく必要があります。

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。
4. 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**をインストールする

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。

開始する前に

- Plug-in for SAP HANA Databaseは、HDBSQLクライアントが配置されている各Linuxホストに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。

  https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT
- SnapCenter Plug-in for SAP HANA Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

手順

1. SnapCenter Plug-ins Package for SnapCenterのインストールファイル（SAP_Linux_host_plugin.bin）をC：\ProgramData\SAP\Package RepositoryからPlug-in for NetApp SnapCenterデータベース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. 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。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenterサーバにホストを追加します。

   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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

```
> 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ホストのプラグインサービスとバインドします。
```

```
> $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ホスト上の**SnapCenter SAP HANA**プラグインサービスの**CA**証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストア

への CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中の**CA**署名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ます。

> カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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を含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   ```
   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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

手順

1. カスタムプラグインキーストア/opt/NetApp/snapcenter/scc/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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SCC_CERTIFICATE_ALIASキーに対して更新します。

8. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（CRL）を設定する

タスクの内容

- 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で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/scc/etc/crl」です。

手順

1. crl_pathキーに対して、agent.propertiesファイルのデフォルトディレクトリを変更および更新できます。

   このディレクトリには、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

Windowsホスト上のSnapCenter SAP HANAプラグインサービス用のCA証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中のCA署名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。

4. パスワードを変更したら、サービスを再起動します。

> カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   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ます。

> ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

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一覧表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   keytool -list -v キーストア *.JKS*

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルのキーkeystore_passの値です。

   *keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

8. *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SCC_CERTIFICATE_ALIASキーに対して更新します。

9. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（**CRL**）を設定する

タスクの内容

- 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で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は、複数のCRLファイルを配置できます。

   受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（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。

展開の詳細については、を参照してください "導入の概要"。

CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、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ファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリで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は、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

データ保護の準備

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。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

  Javaのパスは、ホストマシンの環境パス変数で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な場合は、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データベースユーザアカウントを使用している場合は、SnapCenter Serverでバックアップ、リストア、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てください。
  - 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でのリソース、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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- 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できます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを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、そのグループのポリシーを1つ以上選択します。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にも、ポリシーを選択できます。

リソースグループは、保護する対象と保護するタイミング（日時）を定義するものと考えてください。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。そのあとに、日次ポリシーと時間

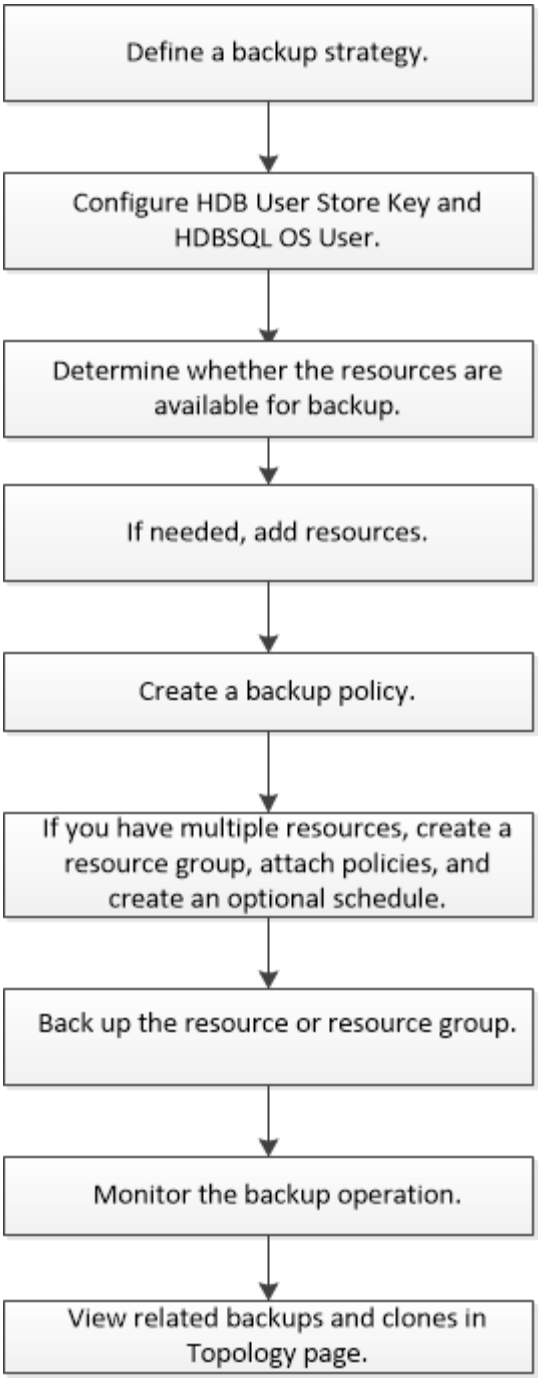
次ポリシーの2つのポリシーをリソースグループに適用できます。リソースグループを作成してポリシーを適用する際に、フルバックアップを毎日実行するようにリソースグループを設定できます。

SAP HANAリソースのバックアップ

SAP HANAリソースのバックアップ

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。https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenter ソフトウェアコマンドレットリファレンスガイド"^]です。

SAP HANAデータベースのHDBユーザストアキーとHDBSQL OSユーザを設定

SAP HANAデータベースでデータ保護処理を実行するには、HDBユーザストアキーとHDBSQL OSユーザを設定する必要があります。

開始する前に

- SAP HANAデータベースにHDBのセキュアなユーザストアキーが設定されておらず、HDB SQL OSユーザが設定されていない場合は、自動検出されたリソースに対してのみ赤い南京錠アイコンが表示されます。以降の検出処理で、設定されているHDBのセキュアなユーザストアキーが正しくないか、データベース自体へのアクセスが提供されていないことが判明した場合は、赤い南京錠のアイコンが再度表示されます。
- データベースを保護できるようにHDBのセキュアなユーザストアキーとHDB SQL OSユーザを設定するか、またはデータベースをリソースグループに追加してデータ保護処理を実行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ユーザを設定する必要があります。テナントデータベースにのみアクセスするようにHDB SQL OSユーザが設定されている場合、検出処理は失敗します。

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 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、ホスト名を選択します。

   そのあとにをクリックすると、フィルタ ペインが閉じます。
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. [Configure database settings]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]ページでデータベース設定を変更できます。

リソースを検出し、データ保護のためのマルチテナントデータベースコンテナを準備する

データベースの自動検出

リソースとは、SnapCenterで管理されているLinuxホスト上のSAP HANAデータベースとデータボリューム以外のボリュームです。使用可能なSAP HANAデータベースを検出したあとに、こ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。

開始する前に

- 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セットアップなどのタスクを完了しておく必要があります。
- LinuxホストでHDBのセキュアなユーザストアキーとHDB SQL OSユーザを設定しておく必要があります。
  - SID admユーザを使用してHDBユーザストアキーを設定する必要があります。たとえば、SIDとしてA22を使用するHANAシステムの場合は、HDBユーザストアキーをa22admに設定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ていません。データベースを手動で追加する際に、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。

タスクの内容

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て[リソース]ページに表示されます。

自動検出されたリソースを変更または削除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、 * 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. [Resources]ページで、[View]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、ホスト名を選択します。

   次に、**をクリックしてフィルタペインを閉じることができます。
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NetAppストレージにあり、保護されていない場合は、[全体のステータス]列に「保護されていません」と表示されます。
   - データベースがNetAppストレージシステム上にあり保護されていて、実行されたバックアップ処理がない場合は、[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のセキュアなユーザストアキーが設定されていない場合は、リソースの横に赤い南京錠アイコンが表示されます。以降の検出処理で、設定されているHDBのセキュアなユーザストアキーが正しくないか、データベース自体へのアクセスが提供されていないことが判明した場合は、赤い南京錠のアイコンが再度表示されます。

SnapCenter以外でデータベースの名前が変更された場合は、リソースを更新する必要があります。

終了後

データベースを保護できるようにHDBのセキュアなユーザストアキーとHDBSQL OSユーザを設定するか、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。

"SAP HANAデータベースのHDBユーザストアキーとHDBSQL OSユーザを設定"

データ保護のためのマルチテナントデータベースコンテナの準備

SnapCenterに直接登録されている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の自動検出がトリガーされます。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、プラグインホストに配置されていたマルチテナントデータベースコンテナ（MDC）リソースごとに別のMDCリソースが自動的に検出され、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。

タスクの内容

たとえば、SnapCenter 4.2では、E90MDCリソースがプラグインホストにあり、手動で登録されている場合、SnapCenter 4.3へのアップグレード後に、別のGUIDを持つ別のE90MDC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するバックアップは、保持期間が終了するまで保持する必要があります。保持期間が終了したら、古いMDCリソースを削除して、自動検出された新しいMDCリソースの管理を続行できます。

`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データ保護処理に使用するには、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. SnapCenter 4.3へのアップグレード後に検出された新しいMDCリソースを構成するには、[Resources]ページで新しいリソースを選択します。

   「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、特定のホストについて、古いMDCリソースと同じSIDを持つリソースとして識別できます。[Resources]ページでは、その横に赤い南京錠のアイコンが表示されます。

3. 保護ポリシー、スケジュール、および通知設定を選択して、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. [Resources]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の保持期間が7日、セカンダリSnapshotの保持期間が45日の場合、45日が経過してすべてのバックアップが削除されたあとは、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。

関連情報

"SAP HANAデータベースのHDBユーザストアキーとHDBSQL OSユーザを設定"

"[TopologyページでのSAP HANAデータベースのバックアップとクローンの表示"]

プラグインホストに手動でリソースを追加する

一部のHANAインスタンスでは自動検出がサポートされません。これらのリソースは手動で追加する必要があります。

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、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保証されます。

"リソースグループを作成してポリシーを適用"です。

タスクの内容

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、それらのリソースではデータ保護処理がサポートされません。

- 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	操作
リソースタイプ	リソースタイプを入力します。リソースタイプは、[Single Container]、[Multitenant Database Container]（MDC）、および[Non-data Volume]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	操作
SID	システムID（SID）を入力します。インストールされている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のセキュアなユーザストアキー	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。テイクオーバー時に使用されます。
HDBSQL OS ユーザ	HDBのセキュアなユーザストアキーを設定するユーザ名を入力します。Windowsの場合、[HDBSQL OS User]にはシステムユーザを指定する必要があります。そのため、システムユーザのHDBのセキュアなユーザストアキー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：*アイコンをクリックすると、他のストレージシステムからボリューム、LUN、およびqtreeを追加できます + 。

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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

"ユーザまたはグループを追加してロールとアセットを割り当てる"

データベースを追加したら、SAP HANAデータベースの詳細を変更できます。

SAP HANAリソースに関連付けられているバックアップがある場合、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の作成

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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

  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。

- 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、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おく必要があります。
- Snapshot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の両方に対応する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。

  また、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ポリシーで指定することもできます。これらのオプションを使用することで、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できます。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳しくは、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

タスクの内容

- SAP HANAシステムレプリケーション
  - プライマリSAP HANAシステムを保護し、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、バックアップを作成することはできません。

    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を作成することはできませんが、SnapCenterはデータ以外のボリューム（NDV）の保護を継続します。

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

> プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

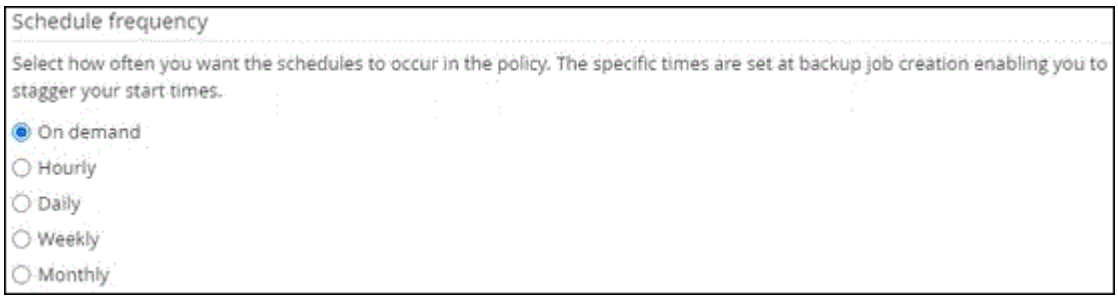
手順

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：

状況	操作
データベースの整合性チェックの実行	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テクノロジを使用したバックアップの作成	「 * 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）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ている場合、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値は複数指定できます。

6. [Retention]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業
一定数のSnapshotを保持	[保持するSnapshotコピーの総数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshot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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。 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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。 SAP HANAシステム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。 SAP HANAシステムレプリケーションでは、作成されたSnapshotの合計数はリソースグループに設定された保持数と同じになります。最も古いSnapshotの削除は、最も古いSnapshotが配置されているノードに基づいて行われます。たとえば、SAP HANAシステムレプリケーションプライマリとSAP HANAシステムレプリケーションセカンダリを含むリソースグループの保持期間は7に設定されます。一度に作成できるSnapshotの数は、SAP HANAシステムレプリケーションプライマリとSAP HANAシステムレプリケーションセカンダリの両方を含め、最大7つです。

状況	作業
Snapshotを特定の日数だけ保持	[Keep Snapshot copies for]*を選択し、Snapshotを削除するまでの日数を指定します。
Snapshotコピーのロック期間	Snapshotコピーのロック期間を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

7. 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）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	操作
• 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。 このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。 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はデスティネーションに転送されず、デスティネーションのリストに表示されます。このSnapshotをリストア処理の対象としてデスティネーションで選択すると、「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。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。 [Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 を参照して "[TopologyページでのSAP HANAデータベースのバックアップとクローンの表示"]

フィールド	操作
• 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。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、を参照してください。 "SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする" を参照して "[TopologyページでのSAP HANAデータベースのバックアップとクローンの表示"]
• 二次ポリシーラベル *	Snapshotラベルを選択します。 選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。 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のSnapshot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. 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、バックアップおよび保護するリソースを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。また、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必要があります。

タスクの内容

- SAP HANAシステムレプリケーションの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保証されます。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定されたリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいデータベースを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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、 [* 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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。

フィールド	操作
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名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。

   これは、画面上の情報をフィルタリングするのに役立ちます。

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、次のタスクを実行します。

フィールド	操作
整合グループSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+

a. [Scripts]*の矢印をクリックし、休止、Snapshot、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. [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	（Y/N）	アーカイブログ管理でアーカイブログを削除できます。
アーカイブログの保持	日数	アーカイブログを保持する日数を指定します。 この設定は NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。

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の拡張子の長さを指定します。 たとえば、アーカイブログが LOG_BACKUP _0_0_0_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

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、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ません。

c. Snapshotコピーツール*の矢印をクリックして、Snapshotを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、ファイルシステムを整合性のある状態にしてからSnapshotを作成します。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：ストレージレベルのSnapshotを作成	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します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。

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 + 。

ポリシーが[Configure schedules for selected policies]セクションに表示されます。

b. [スケジュールの設定]列で、設定するポリシーの**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。

サードパーティの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はサポートされません。

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 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、 [完了] をクリックします。

SAP HANAデータベ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、のページからバックアップすることができます。

開始する前に

- 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であることを確認してください。
- SAP HANAシステムレプリケーションの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保証されます。

  "リソースグループを作成してポリシーを適用"です。

  "リソースグループのバックアップ"

- 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、コマンドレットを使用して、HANAのプロパティファイルでallow_file_based_backup_IFINACTIVE_Tenants_presentパラメータを* YES *に設定し `Set-SmConfigSettings` 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_command_name _ を実行して取得できます。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"

- 休止、Snapshot、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の場合は、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用でき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*

コマンドがコマンドリストに存在しない場合、処理は失敗します。

SnapCenter UI

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。

   *を選択し、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。その後、を選択してフィルタペインを閉じることができます 。
3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名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。

   ◦ [Backups]*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。

   必要に応じて整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

   ◦ [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

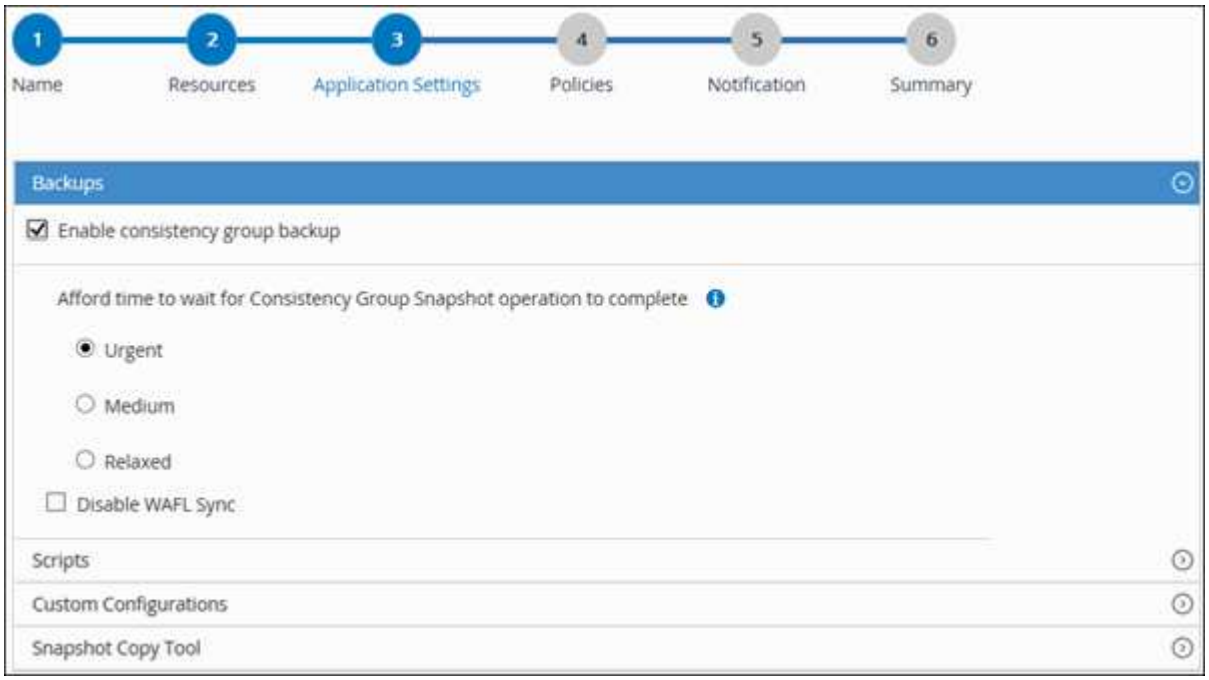
   バックアップ処理を終了する前にPREコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

   ◦ [**Custom Configurations**]矢印を選択し、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*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * 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を作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshot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。

   b. 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]列で**を選択します + 。

   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、*[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。

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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。

   リソーストポロジページが表示されます。

9. [今すぐバックアップ]*を選択します。
10. 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    b. 「 * Backup * 」を選択します。
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。

    ◦ MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

      詳細については、次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関係を検出できない"

    ◦ VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、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*

PowerShellコマンドレット

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.net
app.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. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソースグループを追加します。

   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"="sc
corelinux62.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";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="No
nDataVolume\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します。

   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
```

6. 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、失敗）を監視します。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップID、バックアップ名などの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"。

リソースグループのバックアップ

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に対して実行されます。

開始する前に

- ポリシーを適用して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。

タスクの内容

リソースグループは、[Resources]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、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。

   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、を選択し、タグを選択します。その後、を選択してフィルタペインを閉じることができます 。
3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

PowerShellコマンドレットを使用してSAP HANAデータベース用にストレージシステム接続とクレデンシャルを作成

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前に、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。

開始する前に

- 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 -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -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。

   次に、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例を示します。

```
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"。

バックアップ処理の監視

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、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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**SAP HANA**データベースのデータ保護処理を監視する

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

SAP HANA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 *
- 操作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、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。

アクセス元	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。
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックし  て、最新の5つの処理を表示します。 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]ページでのSAP HANAデータベースのバックアップとクローンの表示

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ときに、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立つことがあります。

タスクの内容

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-  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。
-  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、バックアップを4つだけ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。

[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。

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コピーベースのバックアップ、およびクローン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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

   SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理

が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

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、削除の各処理を実行します。

   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。

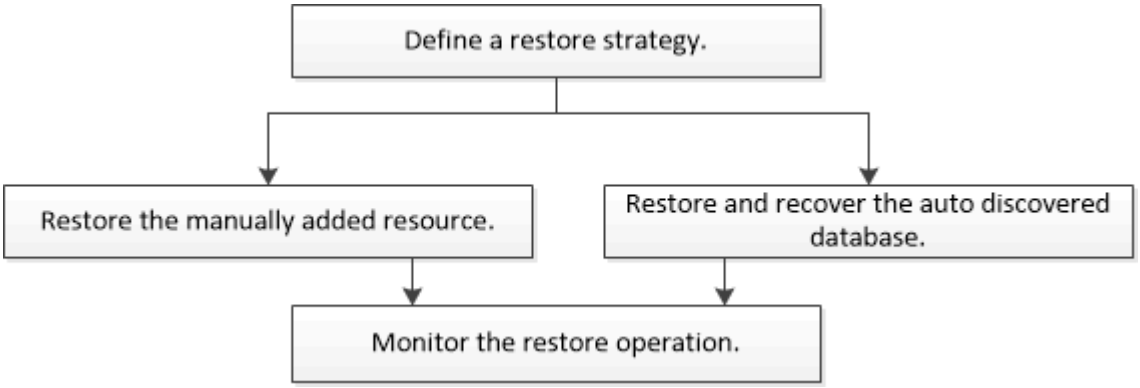
7. クローンを削除する場合は、表でクローンを選択し、をクリックします。
8. クローンをスプリットする場合は、テーブルでクローンを選択し、をクリックします 。

SAP HANAデータベースのリストア

リストアのワークフロー

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"です。

手動で追加したリソースバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- ファイルベースのバックアップコピーを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で作成し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外部の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。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択する必要があります。

SnapCenter UI

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。

   リソースがタイプ、ホスト、関連す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。

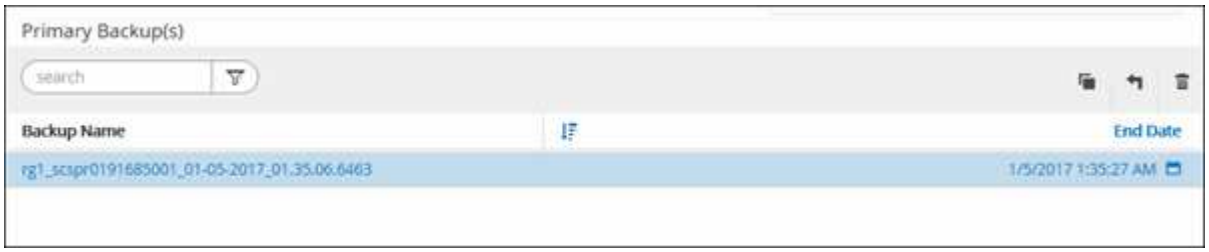
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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
   。



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のあとに作成されたSnapshot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

      - 複数のボリュームとqtreeを選択できます。

- 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。

7. [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。

8. [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はマウントコマンドを使用できません。

   休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_からプラグインホストで使用できるコマンドリストにコマンドがあるかどうかを確認する必要があります。

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。

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

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

自動検出されたデータベースバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- ファイルベースのバックアップコピーを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で作成し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外部の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。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択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。

   リソースがタイプ、ホスト、関連す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。

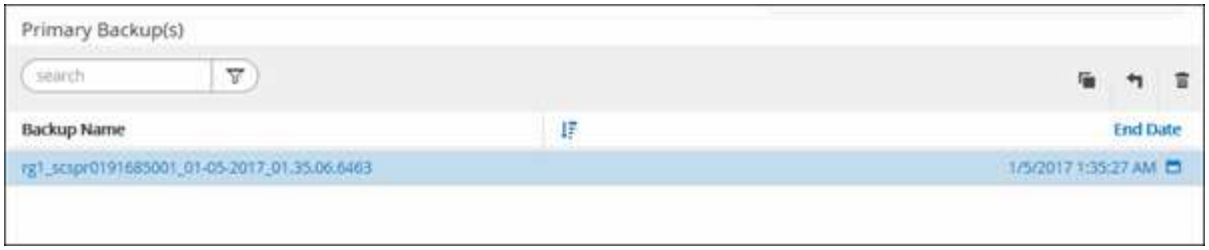
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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 。



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スクリプトまたは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環境の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のあとに作成されたSnapshot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リソースに対してのみ使用できます。

      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してください。

   「 * 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。

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。

状況	操作
できるだけ現在の時刻に近い場所でリカバリしたい	[* 最新の状態に回復する *] を選択します。単一コンテナリソースの場合は、ログおよびカタログバックアップの場所を1つ以上指定します。 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、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1つ以上指定します。 MDCリソースの場合、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両方のログが含まれている必要があります。

状況	操作
指定した時点にリカバリする	[* 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設定されています。 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ホストがカリフォルニア州サニーベールにあり、ローリーのユーザがSnapCenterにログインをリカバリしているとします。 これらのロケーション間の時間差は3時間で、ユーザはローリー（NC）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。 ユーザがカリフォルニア州サニーベール5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。 単一コンテナリソースの場合は、ログおよびカタログバックアップの場所を1つ以上指定します。 MDCリソースの場合は、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1つ以上指定します。 MDCリソースの場合、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両方のログ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必要がある	［* 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。

SnapCenter 4.3へのアップグレード後に作成されたバックアップのみをリカバリできます。ただし、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、自動検出されたリソースが変換または検出されたあとにリストア対象として選択されたバックアップが作成されている必要があります。

8. [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。

9. [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はマウントコマンドを使用できません。

   休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path 、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_からプラグインホストで使用できるコマンドリストにコマンドがあるかどうかを確認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。

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。

PowerShellコマンドレットを使用したリソースのリストア

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。

   ```
   PS C:\> Open-Smconnection
   ```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

SAP HANAリソースのバックアップのクローニング

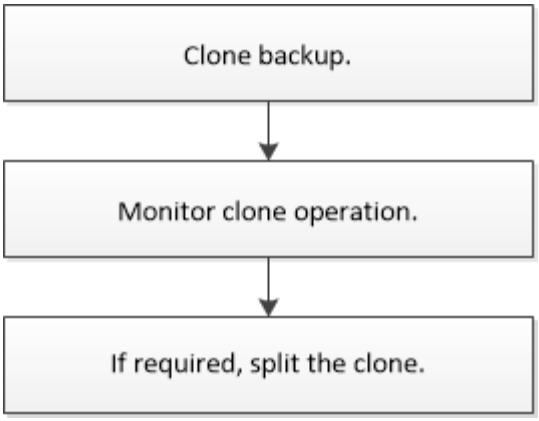
クローニングのワークフロー

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。

タスクの内容

- は、ソースSAP HANAサーバでクローニングできます。
- 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
  - データウェアハウスにデータを取り込む際のデータ抽出および操作ツール用
  - 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

SnapCenterを使用してバックアップをクローニングできます。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。

開始する前に

- 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）の割り当て済みアグリゲートリストに含まれている必要があります。
- 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。
- ターゲットのクローンサーバのSAP HANAインスタンスSIDは、[Target Clone SID]フィールドで指定したSIDと同じである必要があります。
- クローニング前またはクローニング後のコマンドについては、次のパスからプラグインホストで使用できるコマンドリストにコマンドが存在す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*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- クロー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"。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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. Location ページで、次のアクションを実行します。

フィールド	操作
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。
ターゲットのクローン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IPアドレス	クローンボリュームをエクスポートするホスト名またはIPアドレスを入力します。
iSCSIイニシエータ	LUNのエクスポート先ホストの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は、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つのソースに複数のデスティネーションボリュームを設定できます。

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、代替ホストが設定されて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の削除
      - 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. mountコマンドを入力して、ファイルシステムをホストにマウントします。

      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
      ```

      休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_からプラグインホストで使用できるコマンドリストにコマンドがあるかどうかを確認する必要があります。

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。

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

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、クローニングに2つのバックアップを使用できます。

```
 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のアドレスが10.232.206.169に設定されている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ン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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。

3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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する

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニング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する

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。クローンを作成したリソースの[Topology]ページで、クローンを削除したり、クローンをスプリットしたりできます。

タスクの内容

非表示のクローンのストレージフットプリントを特定するには、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、クローニングされ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。

   リソーストポロジページが表示されます。

5. [Manage Copies]ビューで、プライマリまたはセカンダリ（ミラーリング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、をクリックしてクローンを削除するか、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データベースの保護

SnapCenter Plug-in for Oracle Databaseの概要

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。

Plug-in for Oracle Databaseは、Oracle Recovery Manager（RMAN）を使用したバックアップ、カタログ化とカタログ化解除、検証、マウント、アンマウント、リストアを自動化します。 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を使用して、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できます。ただし、SAP BR * Toolsとの統合はサポートされていません。

- 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、プラガブルデータベース（PDB）のリストアとリカバリ

  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。

- バックアップをすぐに検証します。
- リカバリ処理用にデータバックアップとログバックアップをマウントおよびアンマウントします。
- 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の機能

Plug-in for Oracle Databaseは、LinuxホストまたはAIXホスト上でOracleデータベースと統合され、ストレージシステム上でNetAppテクノロジと統合されます。

- 統合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、プラグインと環境全体で標準化され、一貫性があります。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できます。

- 自動化された集中管理

  バックアップ処理とクローン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テクノロジ

  SnapCenterでは、Plug-in for Oracle DatabaseおよびPlug-in for UNIXでNetAppのSnapshot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、 ケンショウワークフロー
- ホストで設定されている 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のサポート
- RBACでサポートされるセキュリティと一元化されたロール委譲

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルの権限を付与することもできます。

- リストア処理とクローニング処理でのアーカイブログ管理（ALM）のサポート
- 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可能

  単一のホストのデータベースが同じボリュームを共有している場合、1回の処理でSnapshotが統合されます。

- 物理インフラと仮想インフラをサポート
- NFS、iSCSI、ファイバチャネル（FC）、RDM、NFSおよびVMFS経由のVMDK、NFS、SAN、RDM、VMDK経由のASMをサポート
- ONTAPの選択的LUNマップ（SLM）機能のサポート

  デフォルトで有効になっているSLM機能は、最適パスのない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 "ONTAP 9 SANアドミニス

トレーションガイド"ください。

- LinuxでのNon-Volatile Memory Express（NVMe）のサポート
  - NVMe utilがホストにインストールされている必要があります。

    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、 カタログ化、カタログ化解除、および検証の処理は、RDMなどの仮想環境を除き、NVMeハードウェアでサポートされます。

    上記の操作は、パーティションのないデバイスまたは単一パーティションのデバイスでサポートされています。

    NVMeデバイス用のマルチパスソリューションを設定するには、カーネルでネイティブマルチパスオプションを設定します。Device Mapper（DM）マルチパスはサポートされていません。
  - 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、 NVMe over TCP/IPでは、カタログ化、カタログ化解除、および検証のワークフローがサポートされます。
  - 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、 NVMe over TCP / IPで作成されたVMDKレイアウトでは、カタログ、カタログ解除、および検証のワークフローがサポートされます。
- SnapMirror Active Sync（当初はSnapMirror Business Continuity [SM-BC]としてリリース）をサポート。これにより、サイト全体に障害が発生してもビジネスサービスの運用を継続でき、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirror Active Syncでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。
- OracleとGRIDではなく、デフォルト以外の任意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* ファイル内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およびgridに設定されています。
  - db_user = oracle
  - db_group=oinstall
  - GI_USER =グリッド
  - 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こと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セツソクLUN • iSCSIセツソクLUN • NFS接続ボリューム • NVMe-FC • nvme-tcpが表示されます
VMware ESXi	• FCまたはiSCSI ESXi HBAで接続されたRDM LUN Host Bus Adapter（HBA；ホストバスアダプタ）のスキャンは、SnapCenterがホストに存在するすべてのホストバスアダプタをスキャンするため、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 • NFSデータストア上のVMDK • NVMe-TCP経由で作成されたVMFS上のVMDK RACは、共有VMDKをサポートするESX 8.0U2でサポートされます。 • ゲストシステムに直接接続されたNFSボリューム • NFSとSANの両方にVVOLデータストアを配置 VVOLデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

AIXでサポートされ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。 • 拡張ジャーナリング・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。

サポートされるバージョンの最新情報については、を参照 "NetApp Interoperability Matrix Tool" してください。

Plug-in for Oracle用に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 SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN
  - lun attribute show
  - LUNの作成
  - lun delete
  - LUNジオメトリ
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード
  - LUNマッピングの作成
  - LUNマッピングの削除
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - LUN変更
  - ボリューム内でのLUNの移動
  - LUNオフライン
  - LUNオンライン
  - LUN永続的予約のクリア
  - LUNのサイズ変更
  - LUNシリアル
  - lun show
  - SnapMirrorポリシーadd-rule
  - snapmirror policy modify-rule
  - snapmirror policy remove-rule

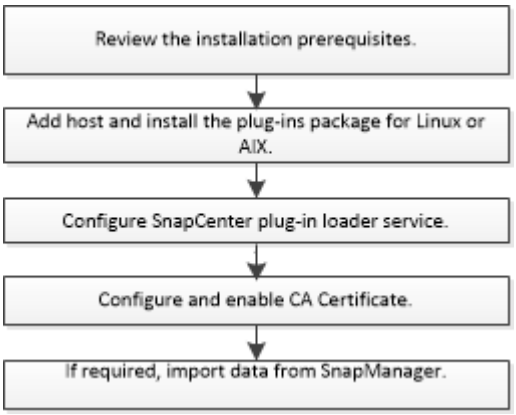
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM
- SVM CIFS

- vserver cifs shadowcopy show
- vserver show
- ネットワークインターフェイス
- network interface show
- MetroClusterショー

SnapCenter Plug-in for Oracle Databaseのインストール

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-ins Package for Linux / 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以外のユーザに対して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するには、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスはroot以外の有効なユーザとして実行されます。

- 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のクレデンシャルを、認証モードをLinuxまたはAIXに設定して作成します。
- Java 11をLinuxホストまたはAIXホストに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ていません。

- 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ファイルのUUIDマッピングはSnapCenterでサポートされていません。

- 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 • Oracle Linux 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プラグイン用の最小RAM	2GB

項目	要件
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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 11 Oracle JavaおよびOpenJDK 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。 を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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 "NetApp Interoperability Matrix Tool"ください。

Linuxホストの**root**以外のユーザに対する**sudo Privileges**の設定

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をroot以外の有効なユーザとして実行します。複数のパスにアクセスできるようにroot以外のユーザにsudo Privileges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
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- /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。

  構成ファイルの更新後に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/installation/plugins/uninstall
- /custom_location /NetApp/snapcenter/spl/bin/spl
- 手順 *

1. SnapCenter Plug-ins Package for Linuxをインストールする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_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- *C：\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt* SnapCenter ServerがWindowsホストにインストールされている場合。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc _ unix_plugins_checksum.txt _ SnapCenterサーバーがLinuxホストにインストールされている場合。

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-in for UNIXはSnapCenter Plug-ins Package for AIXに含まれており、同時ボリュームグループはサポートされません。

項目	要件
オペレーティングシステム	AIX 7.1以降
ホスト上のSnapCenterプラグイン用の最小RAM	4GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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 11 IBM Java を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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 "NetApp Interoperability Matrix Tool"ください。

AIXホストのroot以外のユーザに対するsudo Privilegesの設定

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をroot以外の有効なユーザとして実行します。複数のパスにアクセスできるようにroot以外のユーザにsudo Privileges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。

  構成ファイルの更新後に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/installation/plugins/uninstall
- /custom_location /NetApp/snapcenter/spl/bin/spl
- 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_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- *C：\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt* SnapCenter ServerがWindowsホストにインストールされている場合。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc _ unix_plugins_checksum.txt _ SnapCenterサーバーがLinuxホストにインストールされている場合。

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。

クレデンシャルの設定

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ホストまたは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 *

クレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限を持つroot以外のユーザに対して作成されます。

詳細については、またはを参照してください Linuxホストのroot以外のユーザに対するsudo Privilegesの設定 。 AIXホストのroot以外のユーザに対するsudo Privilegesの設定

* 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. [クレデンシャル]ページで、クレデンシャル情報を入力します。

フィールド	操作
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を選択します。
sudo権限を使用	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

Oracleデータベースに対してデータ保護処理を実行する際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ください。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"。

個 々 のリソースグループのクレデンシャルを設定する場合にユーザ名に完全なadmin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の権限が必要です。

Oracleデータベース認証を有効にしている場合は、リソースビューに赤い南京錠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、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します。

   そのあとにをクリックすると、フィルタ ペインが閉じます。
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。

   RACデータベースインスタンスが存在する1つまたはすべてのクラスタノードを優先ノードとして指定できます。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、優先ノードに表示されるノードは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セットアツフノユウセンノオト"。

1. [OK]*をクリックします。

GUIを使用したホストの追加とPlug-ins Package for Linux / AIXのインストール

[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。プラグインはリモートホストに自動的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、ホストごとまたはクラスタごとに実行できます。クラスタ（Oracle RAC）にプラグインをインストールする場合、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。Oracle RAC One Nodeの場合は、アクティブノードとパッシブノードの両方にプラグインをインストールする必要があります。

Oracle RACにプラグインをインストールする場合は、パスワードベースの認証のみがサポートされます。SSHキーベースの認証はサポートされていません。

この処理には、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]*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	操作
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が適切に設定されているかどうか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またはスキャン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場合、そのホストがサブドメインの一部であるときは、FQDNを指定する必要があります。

フィールド	操作
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]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	操作
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内のすべてのホストを追加	Oracle RAC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。 Flex ASMセットアップでは、ハブノードかリーフノードかに関係なく、すべてのノードが追加されます。

フィールド	操作
オプションの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。

   [インストール前チェックをスキップ]チェックボックスを選択していない場合は、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するためにホストが検証されます。

   事前確認スクリプトでは、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. 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、[Resources]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の監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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。

Plug-ins Package for Linux / AIXの別のインストール方法

コマンドレットまたはCLIを使用して、Plug-ins Package for LinuxまたはAIX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た複数のリモートホストへのインストール

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。

   事前確認スクリプトでは、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"。

クラスタホストにインストール

SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXは、クラスタホストの両方のノードに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。いずれかのIPがそれぞれのノードのパブリックIPになり、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に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場合）、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にデータベースをリストアできます。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。

Plug-ins Package for Linuxをサイレントモードでインストールする

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してください。

- 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は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サーバのインストール先からSnapCenter Plug-ins Package for Linux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. 実行

     ```
     ./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。ホストの追加時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。

サイレントモードでの**Plug-ins Package for AIX**のインストール

コマンドラインインターフェイス（CLI）を使用して、AIX用SnapCenter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してください。

- 手順 *

1. SnapCenterサーバのインストール先から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. 実行

   ```
   ./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。ホストの追加時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サービスの設定

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、SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIX

のインストール時に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	サポートされているログレベルを表示します。 指定できる値は、trace、debug、info、warn、error、致命的だ
spl_protocol	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	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ます。デフォルト値がない場合は、値を追加できます。
SKIP_JAVAHOME_UPDATE	SPLサービスはデフォルトで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_keystore_pass	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か、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。

パラメータ名	説明
spl_port	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に値を変更しないでください。
SnapCenterサーバホスト	SnapCenter サーバの IP アドレスまたはホスト名を表示します。
spl_keystore_path	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。
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。この数が指定した値を超える場合は、最後に変更された5、000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した場合、保持するファイル数は9999に設定されます。
JAVA_HOME	SPLサービスの開始に使用されるJAVA_HOMEディレクトリの絶対パスを表示します。 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。
最後の日数のログの保持	ログが保持されるまでの日数が表示されます。

パラメータ名	説明
enable_certificate_validation	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の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ファイルを変更できます。また、spl.propertiesファイルを確認し、ファイルを編集して、パラメータに割り当てられた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。
   - SnapCenter Plug-in Loaderサービスを開始します。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - SnapCenter Plug-in Loader サービスを停止します。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

       stopコマンドで-forceオプションを使用すると、SnapCenter Plug-in Loaderサービスを強制的に停止できます。ただし、既存の処理も終了するため、この処理を実行する場合は注意が必要です。

   - SnapCenter Plug-in Loader サービスを再起動します。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /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。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - SnapCenter Plug-in Loader サービスで変更を探します。

- rootユーザとして、次のコマンドを実行します。
  `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- root以外のユーザとして、次のコマンドを実行します。 `sudo`
  `/custom_location/NetApp/snapcenter/spl/bin/spl change`

Linuxホストで**SnapCenter Plug-in Loader**（**SPL**）サービスを使用して**CA**証明書を設定する

SPL 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、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、 CA 署名キーペアを SPL の信頼ストアと SnapCenter Plug-in Loader サービスを使用して設定して、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。

SPLでは、「/var/opt/snapcenter/spl/etc」にある「keystore.jks」ファイルをtrust-storeとkey-storeの両方として使用します。

SPLキーストアのパスワードと、使用中の**CA**署名キーペアのエイリアスを管理します。

- 手順 *

1. SPLキーストアのデフォルトパスワードは、SPLプロパティファイルから取得できます。

   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ファイルのSPL_KEYSTORE_PASSキーについ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ます。

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を同じにする必要があります。

spl trust-storeに対するルート証明書または中間証明書の設定

SPL trust-store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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
 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 trust-
store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証明書のあとに中間CA証明書を追加する必要があります。

SPL trust-storeへの**CA**署名済みキーペアの設定

SPL trust-storeに対してCA署名付きキーペアを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/etcが格納されているフォルダに移動します。
  2. 「keystore.jks」ファイルを探します。
  3. キーストアに追加された証明書を一覧表示します。

```
 keytool -list -v -keystore keystore.jks
. 秘密鍵と公開鍵の両方が設定された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一覧表示します。
```

```
 keytool -list -v -keystore keystore.jks
. 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キーストアに含まれていることを確認します。
. CA証明書に追加し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ファイルのSPL_KEYSTORE_PASSキーの値です。

```
 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SPL_CERTIFICATE_ALIASキーに対して更新します。

4. SPL trust-storeにCA署名キーペアを設定したら、サービスを再起動します。

SPLの証明書失効リスト（**CRL**）を設定する

SPLの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で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. キーSPL_CRL_PATHに対して、spl.propertiesファイルのデフォルトディレクトリを変更および更新できます。
  2. このディレクトリには、複数のCRLファイルを配置できます。

     受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、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へのデータのインポート

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。

- すべてのプロファイル、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処理を取得します。
- 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を実行しているシステムに格納されたデータと構成を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については、を参照して "NetApp Interoperability Matrix Tool"ください。

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	デフォルトのバックアップタイプを[Online]、バックアップ範囲を[Full]に設定してポリシーが作成されます。
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。
Oracle Recovery Manager（RMAN）構成のプロファイル	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	スケジュール専用のポリシーが作成されます。
データベース	インポートする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、そのノード用の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	脚注
バックアップ対象 • フル • データ • ログ	バックアップ対象 • フル • データ • ログ	
バックアップモード • 自動 • オンライン • オフライン	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[Auto]の場合は、処理が実行されたときのデータベースの状態がインポートツールによってチェックされ、バックアップタイプが[Online]または[Offline Shutdown]に適切に設定されます。
保持 • 日 • 数	保持 • 日 • 数	SnapManager for Oracle とSnapManager for SAPでは、[Days]と[Counts]の両方を使用して保持が設定されます。 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。
スケジュールの削除 • すべて • システム変更番号（SCN） • 日付 • 指定した時間、日、週、月の前に作成されたログ	スケジュールの削除 • すべて • 指定した時間と日の前に作成されたログ	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。

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	脚注
通知 • 処理が成功した場合にのみEメールを送信 • 処理が失敗した場合にのみEメールを送信 • 処理が成功した場合も失敗した場合もEメールを送信	通知 • 常に • 障害発生時 • 警告 • エラー	Eメール通知が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、設定するために空白のままにします。

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

データのインポートの準備

SnapCenterにデータをインポートする前に、インポート処理を正常に実行するため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. [Resources]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、ホスト上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 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。

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。

データのインポート

データをインポートするには、データベースホストからインポートツールを実行します。

- 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。

- 処理や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
は、sm_profileName_online_full_default_migrated形式のポリシーが作成されます。

  プロファイルを使用して実行される処理がない場合は、デフォルトのバックアップタイプがオンライン、バックアップ範囲がフルで対応するポリシーが作成されます。

- 1つ以上の操作を持つプロファイルに対して作成されるポリシー
は、SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGHTED形式になります。
- 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るポリシー
は、SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED形式になります。
- 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に、ホストで使用可能なデータベースが一覧表示されます。

  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。また、ターゲットデータベースごとに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のインストール

データベースまたはファイルシステムが仮想マシン（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。

展開の詳細については、を参照してください "導入の概要"。

CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、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ファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリで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は、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

Oracleデータベースを保護する準備

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テクノロジを利用するには、ストレージデバイス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て実行できます。

Plug-in for Oracle Databaseを使用する前に、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。 "詳細"
- 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"

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の登録またはクラスタの登録を使用してSnapCenterに登録される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のクレデンシャルを、認証モードをLinuxまたはAIXに設定して作成します。 "詳細"
- 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にあるOracleデータベースをSnapCenterサーバを使用して保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。
- LinuxホストまたはAIXホストにJavaをインストールします。

  詳細については、またはを参照してください "Linux ホストの要件" "AIXホストの要件" 。

- 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、およびリストアの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）が複数ある場合や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、SAN環境が次のガイドに記載されている推奨事項に従って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にOracleデータベースがある場合は、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、scccliコマンドsc-migrateを使用して、SnapCenterのポリシーとリソースグループにプロファイルを移行できます。
- バックアップレプリケーションが必要な場合は、ONTAPでSnapMirrorとSnapVaultを設定する

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。NetAppデータブローカー1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetAppデータブローカー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を使用した仮想データベースおよび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 4.3.xのユーザ向けに、SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、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）を使用した仮想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。

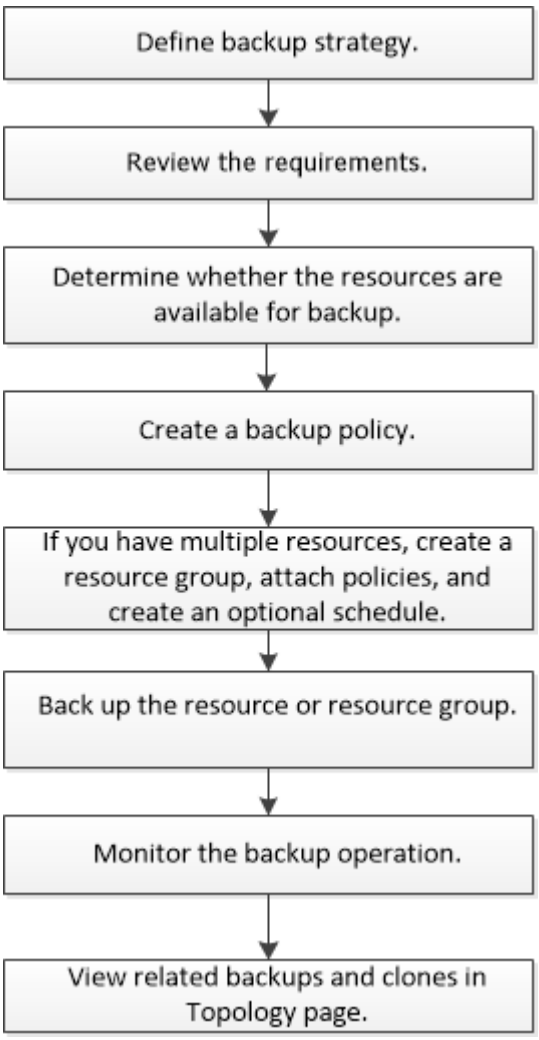
- 詳細はこちら *
- "Interoperability Matrix Tool"
- "SnapCenter Plug-in for VMware vSphereのドキュメント"
- "RHEL 7以降の非マルチパス環境でデータ保護処理が失敗する"

Oracleデータベースのバックアップ

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、前のバックアップが完了して警告が表示された場合は、処理ロックファイルが削除されず、次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

バックアップでサポートされる**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
- Oracle Real Application Clusters（RAC）
- Oracleスタンドアロンレガシー
- 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

  オフラインマウントバックアップは、Data Guardスタンバイデータベースのみ作成できます。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

  オンラインバックアップは、Active Data Guardスタンバイデータベースのみ作成できます。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、Managed Recovery Process（MRP；管理リカバリプロセス）が停止し、バックアップが作成されると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ているすべてのリストア方式の中で、VMDK上で実行できるのはASM RACデータベースの接続およびコピーリストアだけです。

  - ASMスタンドアロンおよびASM RAC on Raw Device Mapping（RDM）+ ASMLibの有無にかかわらず、ASM上のOracleデータベースに対してバックアップ、リストア、およびクローニングの操作を実行できます。
  - Oracle ASMフィルタドライバ（ASMFD）

PDB移行および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 "NetApp Interoperability Matrix Tool"ください。

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

Backup typeには、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の一環として、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（このシナリオではデータベースは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。

  データベースがその他の状態の場合、バックアップ処理は失敗します。

- 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、こ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ファイルにデータベースエントリが格納されている必要があります。

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ファイルにデータベースエントリが格納されている必要があります。

データベースがすでに検出され、バックアップがデータベースに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名前変更または削除とマークされます。

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. フェイルオーバーされた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します。
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ファイルにデータベースエントリが格納されている必要があります。

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、

バックアップがデータベースに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名前変更または削除とマークされます。

データベースが再配置された場合は、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します。です。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。です。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。です。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、データベースは検出されますが、データベースは到達不能になり、ステータスはオフラインになります。

RACセツトアツフノユウセンノオト

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の1つまたはすべてを指定できます。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とnode2のインスタンスが優先ノードとして設定され、node2が第1優先ノード、node1が第2優先ノードとして設定されます。バックアップ処理を実行すると、最初の優先ノードであるnode2で最初に処理が試行されます。

node2がバックアップ対象の状態でない場合（ホストでプラグインエージェントが実行されていないなどの複数の原因が考えられます）、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ではありません。 または、FlexASM構成のnode2上のデータベースインスタンスがローカルASMインスタンスによって処理されていない場合、node1で処理が試行されます。

node3は優先ノードのリストにないため、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セットアップでは、カーディナリティが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リストされません。Flex ASMクラスタノードのロールに変更があった場合は、優先ノードが更新されるように手動でを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必要があります。

- オンラインバックアップを作成するには、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OPEN状態である必要があります。

- オフラインマウントバックアップを作成するには、設定された優先ノード内の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、他のすべてのインスタンス（他の優先ノードを含む）がマウント状態以下である必要があります。
- 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、オフラインシャットダウンバックアップを作成するには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が有効になっている場合は、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、データベースが少なくともマウント済み状態で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インターフェイス（GUI）のデータベース設定ウィザードを使用して、外部カタログのクレデンシャル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、-OracleRmanCatalogCredentialNameオプションと-OracleRmanCatalogTnsNameオプションを指定してConfigure-SmOracleDatabaseコマンドを実行します。

RMANコマンド

SnapCenter GUIでOracleバックアップポリシーを作成するとき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。コマンドを実行して、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` 。

バックアップをカタログ化したら、コマンドを実行して、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）を取得できます `Get-SmBackupDetails` 。

命名形式

SnapCenter 3.0以降では、ASMディスクグループ名が16文字以上の場合、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で使用されている形式と同じです。

HASHCODEofDISKGROUPは、ASMディスクグループごとに一意の、自動的に生成される番号（2～10桁）です。

クロスチェック処理

クロスチェックを実行すると、リポジトリレコードが物理ステータスと一致しないバックアップに関するRMAN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を使用してディスクからアーカイブログを削除しても、実際にはディスクにログがない場合でも、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、制御ファイルの情報を更新できます。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、ENABLE_CROSSCHECKパラメータに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付けられている保持期間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が削除されます。

> 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。

処理時間がORACLE_PLUGIN_RMAN_CATALOG_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ついては、Get-Help Command_nameを実行して確認できます。または、を参照して "SnapCenter ソフトウェアコマンドリファレンスガイド"ください。

バックアップ固有のプリスクリプトとポストスクリプト用に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。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できるパラメータの値を事前に定義します。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。

- * 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

  処理に複数のデータベースが含まれる場合、パラメータには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設定されます。

  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、host nameはバックアップが実行されるホストの名前です。

  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設定されます。

  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。

  データは <db1><osuser1><osgroup>|<db2>@<osuser2> の形式で表示されます。

  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設定されます。

  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設定されます。

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および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している単一データベースの場合：buck ：/vol/scspr2417819002_NFS_CDB_NFSB31_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およびqtreeの親ボリュームの名前になります。

  例：

  - 単一の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：

- 単一のデータベースインスタンスの場合：buck ：/vol/scspr2417819002_NFS_CDB_NFSB32_data/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0、buck：/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- 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
  - 2つのボリュームを含む整合グループSnapshotの場合：CG3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_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、バックアップ対象の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接の親になります。アーカイブログが複数の場所に配置されている場合は、すべての場所がキャプチャされます。これにはFRAのシナリオも含まれます。ソフトリンクがディレクトリに使用されている場合は、同じものが入力されます。

  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ログファイルの直接の親になります。ソフトリンクがディレクトリに使用されている場合は、同じものが入力されます。

  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。

  ディレクトリ名は制御ファイルの直接の親になります。ソフトリンクがディレクトリに使用されている場合は、同じものが入力されます。

  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接の親になります。ソフトリンクがディレクトリに使用されている場合は、同じものが入力されます。

  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_CDB_NFSB32_data/rg2_scspr2417819002_07-21-2021_02.28.26.3973_0、buck：/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- **@** 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_NFS_CDB_NFSB32_DATA /RG2_scspr2417819002_07-21-2021_02.28.26.3973_0、buck：/vol/scspr2417819002_NFS_CDB_NFSB32_redo /RG2_sc002
  - NFSB31@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：

  - data@203|log@205
  - 時間単位|データ@日数：3|log@count：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_r17202_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ことも、保持するバックアップコピーの数（ONTAPの最大コピー数255）を指定することもできます。たとえば、組織で、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する必要があるとします。

ポリシーの作成時に、バックアップタイプと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のスケジュールタイプを変更した場合、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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。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とRPOはデータ保護戦略に影響します。

使用頻度の高いリソースであっても、フルバックアップを1日に1~2回以上実行する必要はありません。たとえば、定期的なトランザクションログバックアップで十分な場合は、必要なバックアップを作成できます。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つの部分があります。

- 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タイミング）は、リソースグループ設定の一部です。たとえば、リソースグループのポリシーで週単位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。

バックアップの命名規則

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

Oracleデータベースのバックアップ要件

Oracleデータベースをバックアップする前に、前提条件が満たされていることを確認する必要があります。

- ポリシーを適用して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、データベースで使用される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。

  値を変更する場合は実行中のジョブがないことを確認し、値を大きくしたあとにSnapCenter SMCoreサービスを再起動してください。

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、こ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。

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。
- 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）にある場合は、SnapCenter Plug-in for VMware vSphereを導入して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が実行するプロセスを確認して、さまざまなタイプとバージョンのOracleデータベースを検出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ファイルに追加されたデータベース以外のエントリがSnapCenterで検出されないようにすることができます。

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、将来ファイルを維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。データベース以外の名前の後ろにコメントを追加できます。

```
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
-----------------------------------------------
```

3. リソースを検出します。

   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_oratab.config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て[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）環境でデータベースインスタンスが検出されるためには、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少なくともマウント済み状態である必要があります。正常に検出されたデータベースのみをリソースグループに追加できます。

ホスト上のOracleデータベースを削除した場合、SnapCenterサーバは認識せず、削除されたデータベースのリストを表示します。SnapCenterリソース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、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します。その後、アイコンをクリックしてフィルタペインを閉じることができます 。

3. [リソースの更新] をクリックします。

   RAC One Nodeのシナリオでは、データベースが現在ホストされているノードで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。

SnapCenter以外でデータベースの名前が変更された場合は、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にある場合は、ユーザインターフェイスの[Overall Status]列に「Not available for backup」という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にあるデータベースに対しては、データ保護処理を実行できません。

- データベースがNetApp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[Overall Status]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NetApp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の[Overall Status]列に「Available for backup」という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は、リソースビューに赤い南京錠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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。レプリケーション、スクリプト、および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と、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場合は、SnapCenter管理者が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を割り当てておく必要があります。
- 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。
- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

タスクの内容

- SnapLock

◦ [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。

Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。

ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

- 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。

     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、アーカイブログファイルのいずれをバックアップするか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）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ができます。

     午前2時にスケジュールを設定している場合、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。

  GUIまたはSnapCenter CLIコマンドCatalog-SmBackupWithOracleRMANを使用して、一度に1つのバックアップに対して遅延カタログ化を実行できます。

  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。

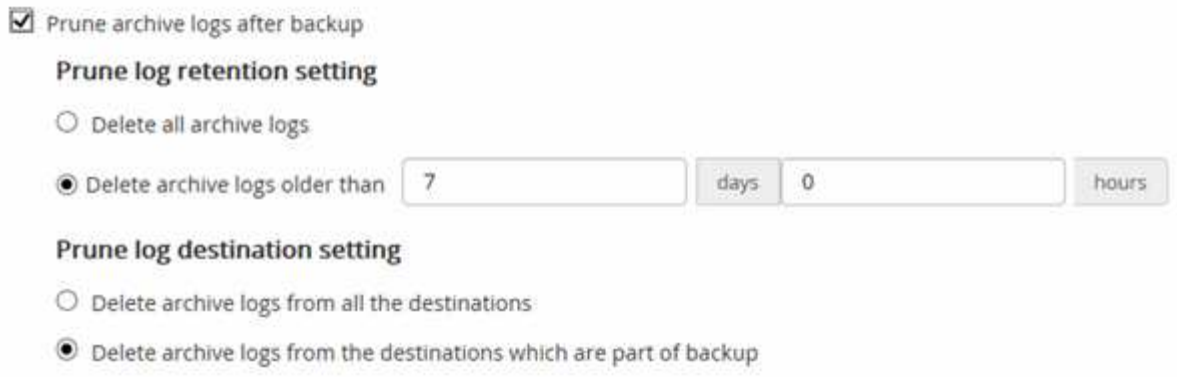
  Oracle Standard Editionを使用している場合は、アーカイブログのバックアップ中にlog_archive_destパラメータとlog_archive_duplex_destパラメータを使用できます。

- アーカイブログを削除できるのは、バックアップの一部としてアーカイブログファイルを選択した場合だけです。

  削除処理を成功させるには、RAC環境内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	[Delete all archive logs*] を選択します。
古いアーカイブログを削除	「 * 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	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。
バックアップに含まれるログデスティネーションからアーカイブログを削除	[* 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. [Retention]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業
一定数のSnapshotを保持	[保持するSnapshotコピーの総数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshot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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。 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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。
Snapshotを特定の日数だけ保持	[Keep Snapshot copies for]*を選択し、Snapshotを削除するまでの日数を指定します。
Snapshotロック期間	Snapshotコピーのロック期間を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

アーカイブログバックアップを保持できるのは、バックアップの一部としてアーカイブログファイルを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	操作
ローカルSnapshot作成後にSnapMirrorを更新する	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。 このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。 [Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。
ローカルSnapshot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。 SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、を参照してください。 "SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする" を参照して "[TopologyページでのOracleデータベースのバックアップとクローンの表示"]

フィールド	操作
セカンダリポリシーラベル	Snapshotラベルを選択します。 選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。 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。
エラー時の再試行回数	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のSnapshot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の実行時に、事前定義された環境変数を使用できます。 "詳細"

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. [Verification script commands]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データベース用のリソースグループの作成とポリシーの適用

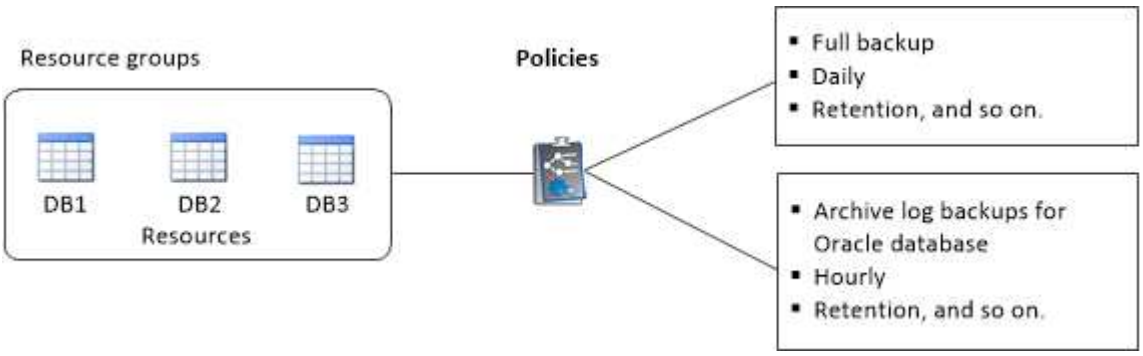
リソースグループはコンテナであり、バックアップして保護するリソースを追加します。リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。

タスクの内容

- 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。



- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定されたリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいデータベースを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。

   c. このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名にタイムスタンプが追加されます。

d. バックアップしない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。

必要に応じて、プレフィックスも含めて、Oracleで設定されたものとまったく同じデスティネーションを使用する必要があります。

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。最近追加したリソースは、リソースリストを更新するまで使用可能なリソースのリストに表示されません。

5. [Available Resources]セクションからリソースを選択し、[Selected Resources]セクションに移動します。

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. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。

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。

サードパーティの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. [Configure Schedules]列内をクリックし て、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	操作
バックアップ後に検証を実行	[Run verification after backup] を選択します。
検証のスケジュールを設定	[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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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

いずれのリソースグループにも含まれていないリソースは、[Resources]ページから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、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します。

そのあとにをクリックすると、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名に使用するカスタムの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名にタイムスタンプが追加されます。

b. バックアップしない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. [Configure Schedules]列内をクリックし  て、目的の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. [Configure Schedules]列内をクリックし  て、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。+[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セットアップでは、カーディナリティがRACクラスタ内のノード数より小さい場合、リーフノードで検証処理を実行できません。

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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    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。

終了後

- AIXのセットアップでは、コマンドを使用してロックしたり、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たディスクの名前を変更したりできます `lkdev rendev` 。

  デバイスをロックまたは名前変更しても、そのバックアップを使用してリストアを実行しても、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、次のコマンドレットを実行してORACLE_SQL_QUERY_TIMEOUTパラメータとORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する `Set-SmConfigSettings`

  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場合、処理が失敗し、エラーコードDBV-00100 specified fileが表示されることがあります。sco.propertiesのverification_delayおよび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で保護関係を検出できないことがあります。
- VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、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、コマンドによって `do_start method` 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 `Java -jar -Xmx8192M -Xms4096M`ます。

詳細情報

- "MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"
- "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のバックアップ

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。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に対して実行されます。

リソースグループは、[Resources]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、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バックアップが作成されます。

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  てタグを選択します。

   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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   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。

終了後

- AIXのセットアップでは、コマンドを使用してロックしたり、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たディスクの名前を変更したりできます `lkdev rendev` 。

  デバイスをロックまたは名前変更しても、そのバックアップを使用してリストアを実行しても、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、次のコマンドレットを実行してORACLE_SQL_QUERY_TIMEOUTパラメータとORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する `Set-SmConfigSettings`

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場合、処理が失敗し、エラーコードDBV-00100 specified fileが表示されることがあります。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、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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処理を監視する

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

その他のバックアップ処理

UNIXコマンドを使用した**Oracle**データベースのバックアップ

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アカウントのログインセッションは1つだけで、トークンはユーザのホームディレクトリに格納されます。

  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トークンを作成すると、期限切れにならず、セッションが常に有効になるトークンを作成できます。

- 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。このマッピングの詳細を使用して、バックアップリソースグループを作成する際に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できます。このオプションを指定すると、バックアップジョブが完了するまで、コマンドはサーバをポーリングし続けます。

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、キューに格納されている、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、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、SnapCenterサーバは処理を停止し、ストレージからすべてのSnapshot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、キャンセルがトリガーされても、作成済みのSnapshotはロールバックされません。

- キャンセルできるのは、キューに登録されているか実行中のログまたはフルバックアップ処理だけです。
- 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すると、処理はキャンセルされ、検証処理は実行されません。

- カタログ化処理を開始したあと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]ページまたは[Activity]ペインからキャンセルできます。
- SnapCenter GUIに加えて、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。

アクセス元	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。
[Activity]ペイン	1. バックアップジョブを開始したら、[Activity]ペインでをクリックして、 最新の5つの処理を表示します。 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]ページでの**Oracle**データベースのバックアップとクローンの表示

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ときに、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立つことがあります。

- このタスクについて *

[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-

 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。

-  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、バックアップを4つだけ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。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。
- 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. [Summary]カードで、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の概要を確認します。

     [Summary Card]セクションには、バックアップとクローンの総数、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。

     SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

     アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長

のSnapLock有効期限がONTAPから取得されます。

SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

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、カタログ化、カタログ解除、および削除の各処理を実行します。

   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。

   - 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に割り当てられている値がより小さい場合は、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いても、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、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" "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、単一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マウントすることも、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マウントすることもできます。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。処理の実行中にマウントできるバックアップは1つだけです。

Flex ASMセットアップでは、カーディナリティが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のマウント

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ASMクレデンシャルとASMポートをソースデータベースホストと異なる場合は、ASM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
  - 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の場合は、NVMe utilがインストールされている必要があります
- 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は、次のコマンドを実行して、マウントされたバックアップに関連する情報を取得できます。

```
./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のアンマウント

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。

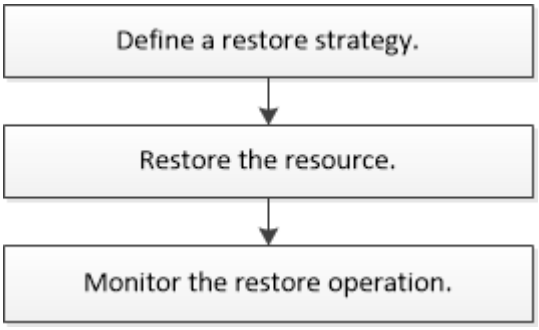
4. マウントされているバックアップを選択し、をクリックします  。
5. [OK]*をクリックします。

Oracleデータベースのリストアとリカバリ

リストアのワークフロー

リストア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。



Oracleデータベースのリストアとリカバリの戦略を定義

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、さまざまなタイプの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専用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、および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、またはバックアップ作成後に新しいファイルが存在する場合は、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からクローニングされ、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ファイルシステムスタックが構築されます。
  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セットアップ（RACクラスタ内のノード数よりも基数が少ない）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。

- セカンダリストレージシステムからのリストア（Data ONTAP 8.3より前のバージョンの場合）
- 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あるASMディスクグループのリストア
- Oracle RACセットアップで、いずれかのピアノード（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）
- 制御ファイルのみのリストア
- ASMディスクグループに存在する表領域のサブセットをリストアする
- 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たが、SnapCenterサーバは新たに追加されたノードを認識しない

In Placeリストア

データベースレイアウトがバックアップとほぼ同じで、ストレージとデータベーススタックで設定を変更していない場合は、In Placeリストアが実行され、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あとに、バックアップを作成する必要があります。In Placeリストアの実行後、ディスクグループには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条件に一致すると、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、再作成が行われない（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するLUNの追加、削除、または再作成が行われない（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での**In Place**リストアの実行

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ASMディスクグループの状態をリストア処理前の状態に変更します。

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。ロールバックは、処理が失敗したプライマリノードおよびピアノードではサポートされていません。別の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、プライマリノードのASMディスクグループをMOUNT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。別のリストアを実行する前に、ストレージリストアの問題を手動で修正し、プライマリノードのASMディスクグループをMOUNT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、実際のデータベースファイルと比較して欠落している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
- 制御ファイルのみをリストア
- データファイルと制御ファイルをリストア
- 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のデータファイル、制御ファイル、REDOログファイルをリストア

パーシャルリストア

- 選択した表領域のみをリストア
- 選択したプラガブルデータベース（PDB）のみをリストア
- PDBの選択した表領域のみをリストア

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
- 特定のシステム変更番号（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

> データベースロールをスタンバイとして作成されたバックアップを使用してリストアした場合、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のリカバリは、常に手動で実行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

- PDBに関連付けられた一時表領域および一時表領域のリストア
- 複数のPDBから同時に表領域をリストアおよびリカバリ
- 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復元
- 同じホスト上に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、およびUNDO表領域のポイントインタイムリカバリ（PITR）はサポートされない
- 表領域のPITRを他のタイプのリストアと一緒に実行することはできない
- テーブルスペースの名前を変更し、名前を変更する前の状態に戻す場合は、テーブルスペースの以前の名前を指定する必要があります。
- ある表領域のテーブルの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表領域をリカバリすることはできません
- PITRを使用して、次のいずれかのオブジェクトを含む表領域をリカバリ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、パーティション化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、PITRを実行する前に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’ディメンション’ディレクトリ’シーケンス

Oracleデータベースをリストアする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のバックアップコピーからOracleデータベースをリストアできます。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できます。複数ミラー構成の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。

リストア固有のプリスクリプトとポストスクリプト用に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ときに、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

  処理に複数のデータベースが含まれている場合は、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設定されます。

  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設定されます。

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設定されます。

  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

区切り文字の詳細については、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際の要件

Oracleデータベースをリストアする前に、前提条件が満たされ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。
- Snapshot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の両方の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を削除する場合は、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、クローニングされたVMDKを割り当てるために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する必要があります。
- 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、最新の状態になっていることを確認してください。

  ライセンスがインストールされていないか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。この警告を無視して続行すると、RDMからのリストアは失敗します。

- 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

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されます。データベースがARCHIVELOGモードで実行されている場合は、REDOログファイルのいっぱいになったグループが1つ以上のオフラインデスティネーション（まとめてアーカイブREDOログ）に保存されます。SnapCenterは、指定したSCN、選択した日時、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された場所にない場合は、ログを含むSnapshotをマウントし、パスを外部アーカイブログとして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を使用してデータベースをリストアすることはできません。ASMFD設定でバックアップを作成し、リストアに使用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、リストアするバックアップをASMlib構成で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。

- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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 *] 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する場合：

      - ミラーまたはバックアップにログバックアップがない場合は、何も選択されず、ロケータは空になります。
      - ログバックアップがミラーまたはバックアップに存在する場合は、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両方の場所に存在する場合は、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	操作
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でのみ使用できます。 Data Guard以外のデータベースのREDOログファイルはバックアップされません。Data Guard以外のデータベースでは、リカバリはアーカイブログを使用して実行されます。
プラガブルデータベース（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	操作
プラガブルデータベース（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、リストア対象としてPDBを選択した場合にのみ使用できます。

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には、open、mounted、started、およびshutdownがあります。データベースの状態が上位で、リストア処理を実行するために下位の状態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する必要があります。データベースの状態が低いものの、リストア処理を実行するために高い状態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ていなくても、データベースの状態が自動的に変更されます。

データベースがOPEN状態であり、リストアのためにデータベースをMOUNTED状態にする必要がある場合は、このチェック・ボックスを選択した場合にのみ、データベースの状態が変更されます。

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	操作
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；システム変更番号）にリカバリする場合	[* Until SCN （ System Change Number ）] を選択します。
特定のデータと時間に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時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	操作
外部アーカイブログの場所を指定	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、選択した日時、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た場合に、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場合は、リカバリ用の外部アーカイブログの場所として、マウントしたバックアップのパスを指定する必要があります。 外部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。 • "ONTAPによるOracleデータ保護" • "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。

OPEN DATABASE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、リカバリ処理が開始されたRACインスタンスだけがOPEN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の実行時に、事前定義された環境変数を使用できます。 "詳細"

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、この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、制御ファイルがあるかどうかに関係なく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かれます。

ⓘ 制御ファイルを含むユーザ表領域、制御ファイルを含む/含まないシステム表領域、制御ファイルを含む/含まないPDBをリストアすると、リストア処理に関連するPDBの状態だけ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の状態を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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。

- 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ることなく、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をカタログ化してマウントする必要があります。
- 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処理中、RMANは指定された補助デスティネーション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には、マウントポイントまたはASMディスクグループを指定できます。マウントされた場所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の代わりにいずれかのマウントされた場所を再利用できます。

日時またはSCNを指定すると、ソースデータベースに表領域がリストアされます。

ASM、NFS、SAN環境にある複数の表領域を選択してリストアできます。たとえば、表領域TS2とTS3がNFS上にあり、TS4がSAN上にある場合、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、タイプが単一インスタンス（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、SYSTEM、およびUNDO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、指定したSCNまたは選択した日時に基づいて、PITRの実行に必要なデータバックアップとログバックアップの最適な数を特定し、マウントしてカタログ化します。

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してください。デフォルトでは、/var/opt/snapcenter/spl/scriptsパスが入力されています。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の実行時に、事前定義された環境変数を使用できます。 "詳細"

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、この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たプラガブルデータベースのリストアとリカバリ

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、破損またはドロップされたプラガブルデータベース（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を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でPDBを手動で閉じる（状態をMOUNTEDに変更する）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処理中、RMANは指定された補助デスティネーション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には、マウントポイントまたはASMディスクグループを指定できます。マウントされた場所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の代わりにいずれかのマウントされた場所を再利用できます。

PDBのPITRを実行するには、日付と時刻またはSCNを指定する必要があります。RMANは、読み取り/書き込み、読み取り専用、またはデータファイルを含むドロップされたPDBをリカバリできます。

リストアおよびリカバリを実行できるのは、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、タイプが単一インスタンス（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と表領域のどちらをリストアするかに応じて、次のいずれかの操作を実行します。

状況	手順

PDBのリストア	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データベースではPITRを実行できません。
PDB内の表領域のリストア	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、SYSTEM、およびUNDO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、指定したSCNまたは選択した日時に基づいて、PITRの実行に必要なデータバックアップとログバックアップの最適な数を特定し、マウントしてカタログ化します。

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してください。デフォルトでは、/var/opt/snapcenter/spl/scriptsパスが入力されています。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の実行時に、事前定義された環境変数を使用できます。 "詳細"

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、この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。リカバリしたPDBは、RACセットアップの他のすべてのノードで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コマンドを使用したOracleデータベースのリストアとリカバリ

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表示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"。

- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択する必要があります。
- 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. 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、指定したバックアップIDで指定し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、プラガブルデータベース、およびその表領域が含まれます。

  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、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

Oracleデータベースのリストア処理をキャンセルします。

キューに登録されているリストアジョブは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。

タスクの内容

- 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。
- キューに格納されているリストア処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用して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。

アクセス元	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。
[Activity]ペイン	1. リストア処理を開始したら、[Activity]ペインをクリックして、 最新の5つの処理を表示します。 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

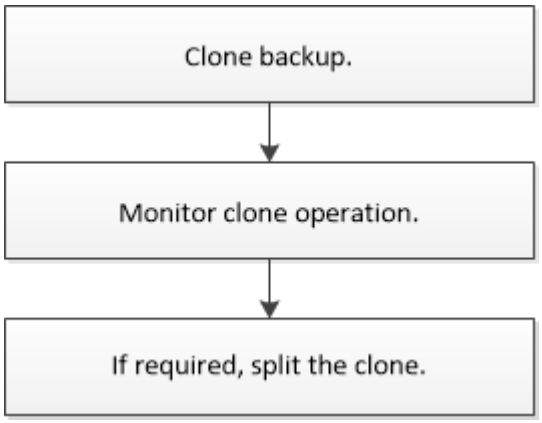
クローニングのワークフロー

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。
- データ抽出および操作ツールを使用してデータウェアハウスにデータを入力する。
- 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データベースのさまざまなタイプの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、および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_friendly_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。バックアップは、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からクローニングできます。

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て、同じ名前の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ファイルシステムまたはNFSファイルシステムの命名規則は、FileSystemNameofsourcedatabase_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、自動的に生成される番号（2～10桁）です。

Oracleデータベースのクローニングに関する制限事項

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。

- 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ているLUN（たとえば、WindowsホストでMicrosoft iSCSIイニシエータを使用）から、同じWindowsホスト上のVMDKまたはRDM LUN、または別のWindowsホスト（またはその逆）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。
- クローンを含む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。

クローン固有のプリスクリプトとポストスクリプト用に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、定義済みの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設定されます。

  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設定されます。

  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設定されます。

  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設定されます。

  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設定されます。

  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ません。

  例：1521

区切り文字の詳細については、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、前提条件が完了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。

  クローニング処理を成功させるには、オンラインの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ログファイルと制御ファイルは、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によって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は、代替ホストが次の要件を満たしている必要があります。
  - 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 "Host Utilitiesのマニュアル"ください。

  - 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ディスクグループ上のデータファイルは、SnapCenterクローンワークフローの一部としてプロビジョニングされます。

◦ NVMeの場合は、NVMe utilがインストールされている必要があります

- ログバックアップを使用して代替ホストにクローニングする際にセカンダリロケータを検出するには、データLUNとログLUNの保護タイプ（mirror、vault、mirror-vaultなど）を同じにする必要があります。
- 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は、CDBがPDBを作成するために使用できるシステム提供のテンプレートです。シードPDBの名前はPDB$SEEDです。PDB$SEEDの詳細については、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クローニングする場合は、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の下にないようにしてください。プラグインホストのroot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REDOログファイルのパスを変更する必要があります。

  クローンされた新しいマウント・ポイントは'autofsサブシステムに手動で登録できますクローニングされた新しい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）の割り当て済みアグリゲートリストに含まれている必要があります。
- NVMeで接続から除外するターゲットポートがある場合は、/var/opt/snapcenter/scu/etc/nvme.confファイルにターゲットの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のクローニング

SnapCenterを使用すると、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、データベースの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。データベースは、指定されたリカバリ・オプションに基づいて、指定された時間に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。

  SnapCenterでは、Oracle RACデータベースバックアップからクローニングすると、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ンの作成がサポートされています。

  クローニング中、SnapCenterでは、SCNまたはDATとリカバリ処理の時間に基づいて、最適な数のログバックアップがマウントされます。リカバリが完了すると、ログバックアップが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。クローニングされたホストデバイスに関連付けられているudevルールは、クローンを削除すると削除されます。

  Flex ASMセットアップでは、カーディナリティが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。

- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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 *] 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ページが表示されます。

4. [コピーの管理]ビューで、ローカルコピー（プライマリ）、ミラーコピー（セカンダリ）、バックアップコピー（セカンダリ）のいずれかの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. [Name]ページで、次のいずれかの操作を実行します。

状況	手順
データベースのクローニング（CDBまたは非CDB）	a. クローンのSIDを指定します。 クローン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のデータベースが存在しないことを確認してください。
プラガブルデータベース（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 "プラガブルデータベースのクローニング"。

ミラーデータまたはバックアップデータを選択する場合：

- ミラーまたはバックアップにログバックアップがない場合は、何も選択されず、ロケータは空になります。
- ログバックアップがミラーまたはバックアップに存在する場合は、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両方の場所に存在する場合は、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	操作
クローンホスト	デフォルトでは、ソースデータベースホストが入力されています。 別のホスト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がインストールされているホストを選択します。

フィールド	操作
データファイルの場所	デフォルトでは、データファイルの場所が入力されています。 SANファイルシステムまたはNFSファイルシステムのSnapCenterのデフォルトの命名規則は、FileSystemNameofsourcedatabase_CLONESIDです。 SnapCenterディスクグループ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、自動的に生成される番号（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、名前の長さがOracleでサポートされる最大長に従っ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、制御ファイルおよび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、データファイルと同じ名前か、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	操作
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上書きする場合は、別の制御ファイルのパスを指定できます。 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している必要があります。 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は、ソースデータベースとは別のファイルシステム（既存のファイルシステム）にカスタマイズできます。

フィールド	操作
Redoログ	デフォルトでは、REDOログファイルグループ、パス、およびサイズが入力されます。 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、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に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している必要があります。 デフォルトでは、REDOロググループ、REDOログファイル、およびサイズはソースデータベースの数と同じになります。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は、ソースデータベースとは別のファイルシステム（既存のファイルシステム）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	操作
sysユーザのクレデンシャル名	クローンデータベースのsysユーザパスワードの定義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インスタンスのクレデンシャル名	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は、ソースデータベースから自動的に入力されます。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。スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトを配置す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の実行時に、事前定義された環境変数を使用できます。 "詳細"

   b. [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事前入力された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

      > ⓘ データが格納されているデータベースパラメータでは、高速リカバリ領域（FRA）は定義されていません。FRAを設定するには、関連パラメータを追加します。

log_archive_dest_1のデフォルト値は$ORACLE_HOME/clone_sidで、この場所にクローンデータベースのアーカイブログが作成されます。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が、ファイルシステムまたはディスクグループが存在し、ホスト上で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。

10. 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では、クローニング対象として選択したデータバックアップのあとに、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がマウントされてリカバリが実行されます。プライマリストレージでクローンを実行するには、ログとデータのバックアップをプライマリストレージに配置し、セカンダリストレージでクローンを実行するには、ログとデータのバックアップをセカンダリストレージに配置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。 *ログの場所は複数指定できます。

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た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う必要があります。

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[キャンセル]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、クローニング対象として選択されたデータバックアップのあとに、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で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。有効な形式はmm/dd/yyyy hh:mm:ssです。 時刻は24時間形式で指定できます。
SCN（システム変更番号）まで	SnapCenterは、指定されたシステム変更番号（SCN）までデータベースをリカバリします。

フィールド名	説明
外部アーカイブログの場所を指定	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識別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。 [Until Cancel]を選択した場合、SnapCenterはログバックアップを自動的に識別してマウントしません。
新しいDBIDの作成	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、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カタログにクローンデータベースを登録すると、処理は失敗します。
一時表領域用の一時ファイルの作成	クローンデータベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、このチェックボックスを選択します。 このチェックボックスをオフにすると、一時ファイルなしでデータベースクローンが作成されます。
クローンの作成時に適用するSQLエントリを入力してください	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てください	クローニング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。 スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトを配置す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が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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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と、クローンデータベースの整合性を維持できます。

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ら、リソースページをリフレッシュして、クローンデータベースがバックアップに使用可能なリソースの1つとして表示されます。クローニングされたデータベースは、標準の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することができます（クローンのクローン）。

クローニング後は、クローンデータベースの名前を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ていないと、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、アーカイブログ用に設定されてい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、ログの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ロックし、rendevコマンドを使用してクローンデータベースが配置されているディスクの名前を変更できます。

デバイスをロックまたは名前変更しても、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レイアウトでは、クローンSANデバイスのデバイス名の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"

プラガブルデータベースのクローニング

プラガブルデータベース（PDB）は、同じホストまたは代替ホスト上の別のターゲットCDBまたは同じターゲットCDBにクローニングできます。クローニングされた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、タイプが単一インスタンス（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ページが表示されます。

4. [コピーの管理]ビューで、ローカルコピー（プライマリ）、ミラーコピー（セカンダリ）、バックアップコピー（セカンダリ）のいずれかの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. [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	操作
クローンホスト	デフォルトでは、ソースデータベースホストが入力されています。 別のホスト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がインストールされているホストを選択します。
ターゲット CDB	クローン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する必要があります。
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	デフォルトでは、データファイルの場所が入力されています。 SANファイルシステムまたはNFSファイルシステムのSnapCenterのデフォルトの命名規則は、FileSystemNameofsourcedatabase_SCJOBIDです。 SnapCenterディスクグループ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、自動的に生成される番号（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、名前の長さがOracleでサポートされる最大長に従っ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は、ソースデータベースから自動的に入力されます。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してください。デフォルトでは、/var/opt/snapcenter/spl/scriptsパスが入力されています。スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトを配置す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の実行時に、事前定義された環境変数を使用できます。 "詳細"

   a. [Auxiliary CDB clone 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事前入力された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。 *ログの場所は複数指定できます。

    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た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う必要があります。

フィールド名	説明
キャンセルするまで	SnapCenterは、クローニング対象として選択されたデータバックアップのあとに、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でリカバリを実行します。 プライマリストレージでクローンを実行するには、ログとデータのバックアップをプライマリストレージに配置し、セカンダリストレージでクローンを実行するには、ログとデータのバックアップをセカンダリストレージに配置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。

フィールド名	説明
SCN（システム変更番号）まで	SnapCenterは、指定されたシステム変更番号（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	外部アーカイブログの場所を指定します。
新しいDBIDの作成	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。 ソースデータベースと区別する補助クローンデータベースの一意の番号（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。
一時表領域用の一時ファイルの作成	クローンデータベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、このチェックボックスを選択します。 このチェックボックスをオフにすると、一時ファイルなしでデータベースクローンが作成されます。
クローンの作成時に適用するSQLエントリを入力してください	クローン作成時に適用するSQLエントリを追加します。
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てください	クローニング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。スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトを配置す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が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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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 *

PDBのクローンのバックアップを作成する場合は、PDBのクローン先のCDBをバックアップする必要があります。これは、PDBのクローンのみをバックアップすることはできないためです。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、PDBクローンのストレージは、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がMOUNT状態です。クローニングされたPDBに他のノードからアクセスできるようにするには、ストレージを他のノードに手動で接続する必要があります。

- 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コマンドを使用したOracleデータベースバックアップのクローニング

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用に、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。また、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を仕様ファイルに含めるために、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、クローニング処理を実行するホスト、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のスプリット

SnapCenterを使用して、クローン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から独立します。

- このタスクについて *
- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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 "ONTAP 9 論理ストレージ管理ガイド"ください。
- 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サービスが再起動し、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と、クローンスプリット処理が応答を停止します。_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くしたりする場合は、SMCoreServiceHost.exe.configファイルのCloneSplitStatusCheckPollTimeパラメータの値を変更して、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時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば、

```
<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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

プラガブルデータベースのスプリットクローン

SnapCenterを使用して、プラガブルデータベース（PDB）のクローン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るターゲットCDBのバックアップを作成した場合、PDBクローンをスプリットすると、クローニングされたPDBがそのPDBを含むターゲットCDBのすべてのバックアップからも削除されます。

PDBクローンは、インベントリビューまたは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. リソースビューまたはリソースグループ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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中

- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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。

クローンを更新します。

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て、同じ名前の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を有効にしないで、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。
- バックアップが失敗した場合にのみ、ポリシーでEメール通知を設定します。
- 不要なバックアップがないように、オンデマンドバックアップの保持数を適切に定義します。
- クローン更新処理用に指定した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てください。
- データベースが1つだけのリソースグループを作成します。
- clone refreshコマンド用にcronジョブを作成する場合は、SnapCenterスケジュールとcronスケジュールがデータベースリソースグループで重複していないことを確認してください。

  clone refreshコマンド用に作成されたcronジョブの場合は、必ず24時間ごとにOpen-SmConnectionを実行してください。

- クローンSIDがホストで一意であることを確認します。

  複数のクローン更新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のクローン仕様ファイルを使用する場合は、ホスト上のSIDを持つ既存のクローンが削除され、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用に、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。また、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を仕様ファイルに含めるために、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"。

プラガブルデータベースのクローンを削除する

不要になった場合は、プラガブルデータベース（PDB）のクローンを削除できます。

PDBがクローニングされるターゲット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、クローニングされた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または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. リソースビューまたはリソースグループ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します。

アプリケーションボリュームとは

Application Volumesは、Oracleデータベースに関連する設定、インストーラ、その他のデータ以外のファイルなどの情報を格納するストレージです。

SnapCenter Plug-in for Oracle Databaseでは、アプリケーションボリューム（データボリューム以外のボリューム）とOracleデータベースの整合性のあるバックアップを作成できます。

このプラグインは、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を自動化します。

- アプリケーションボリュームとOracleデータベースボリュームを1つのリソースグループで保護します。
- アプリケーションボリュームのバックアップを作成します。
- Oracleデータベースとアプリケーションボリュームのバックアップを作成します。
- ポイントインタイムまでのアプリケーションボリュームとともに、データベースのクローンを作成します。
- バックアップ処理のスケジュールを設定します。
- すべての処理を監視します。
- バックアップ処理とクローニング処理のレポートを表示します。

アプリケーションボリュームを追加

SnapCenter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をサポートしています。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. [Storage Footprint]ページで、ストレージシステム名を入力し、1つ以上のボリュームを選択し、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の変更

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た場合、変更できるのはストレージシステムの詳細だけです。

- 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 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  て値を変更します。

アプリケーションボリュームを削除する

アプリケーションボリュームを削除すると、アプリケーションボリュームに関連付けられているバックアップがある場合、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、以前のバックアップは保持されません。バックアップが関連付けられていない場合は、すべてのメタデータが削除されます。

必要に応じて、SnapCenterで削除操作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  て値を変更します。

バックアップアプリケーションボリューム

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がいずれのリソースグループにも属していない場合は、[Resources]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、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、**をクリックしてフィルタペインを閉じることができます。

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. [Resource]ページで、次の操作を実行します。

フィールド	操作
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名にタイムスタンプが追加されます。
アーカイブログデスティネーションをバックアップから除外	バックアップしない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。

      **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. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。

   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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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リソースグループをバックアップする

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た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に対して実行されます。

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レプリケーションポリシーを設定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、をクリックしてタグを選択します。次に、をクリックしてフィルタペインを閉じることができます。

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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

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

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、ローカルコピー（プライマリ）、ミラーコピー（セカンダリ）、バックアップコピー（セカンダリ）のいずれかの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. Location ページで、次のアクションを実行します。

フィールド	操作
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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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クローンをスプリットする

SnapCenterを使用して、クローン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から独立します。

- 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 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ファイルシステムの保護

SnapCenter Plug-in for Microsoft Windowsの概念

SnapCenter Plug-in for Microsoft Windowsの概要

SnapCenter Plug-in for Microsoft Windowsは、Microsoftファイルシステムリソースに対する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プロビジョニング、整合性のあるSnapshot、スペース再生も可能です。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ファイルシステムをバックアップ、リストア、および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。

- 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設定
- ファイルシステムのバックアップのリストア
- ファイルシステムのバックアップのクローニング
- 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共有上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の機能

Plug-in for Windowsは、ストレージシステム上でNetApp Snapshot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**スナップショットテクノロジ

  Plug-in for Windowsでは、NetAppのSnapshot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、クローニングのワークフローがサポートされます。
- RBACでサポートされるセキュリティと一元化されたロール委譲
- 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可能
- 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をサポート
- 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をサポート
- Windows Server 2022でのNon-Volatile Memory Express（NVMe）のサポート
  - NVMe over TCP / IPで作成されたVMDKレイアウト上のバックアップ、リストア、クローニング、検証のワークフロー
  - ESX 8.0 Update 2以降のNVMeファームウェアバージョン1.3をサポートします。Virtualハードウェアバージョン21が必要です。
  - Windows Serverフェイルオーバークラスタリング（WSFC）は、NVMe over TCP/IP上のVMDKを介したアプリケーションではサポートされません。
- SnapMirror Active Sync（当初はSnapMirror Business Continuity [SM-BC]としてリリース）をサポート。これにより、サイト全体に障害が発生してもビジネスサービスの運用を継続でき、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirror Active Syncでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

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テクノロジを使用して、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仮想マシンファイルシステム）に基づくVMDKに存在するWindowsファイルシステムリソースをバックアップします。

SnapCenterでは、ファイルシステムのSnapshotを作成し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が含まれているフェデレーテッドバックアップは、各LUNを個別にバックアップするよりも高速で効率的です。これは、各ファイルシステムの個 々 のSnapshotと比較して、ボリュームのSnapshotが1つだけ作成されるためです。

SnapCenterがSnapshotを作成すると、ストレージ・システム・ボリューム全体がSnapshotに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です。

他のホストサーバのデータが同じボリューム上にある場合、このデータをSnapshot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、ファイルシステムのバックアップはデータベースのバックアップとは異なります。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 "NetApp Interoperability Matrix Tool"ください。

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セツソク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セツソク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。

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	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	
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。
VMware VM	NFSとSANの両方にVVOLデータストアを配置	VMware vSphere 向け ONTAP ツール	
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をプロビジョニングするには、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。 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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN

- LUNの作成
- lun delete
- LUN igroupの追加
- lun igroup create
- lun igroup delete
- LUN igroupの名前変更
- lun igroup show
- LUNマッピングの追加-レポートノード
- LUNマッピングの作成
- LUNマッピングの削除
- lun mapping remove-reporting-nodes
- lun mapping show
- LUN変更
- ボリューム内でのLUNの移動
- LUNオフライン
- LUNオンライン
- LUNのサイズ変更
- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成

- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限

- ネットワークインターフェイス
- network interface show
- SVM

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の準備

SnapCenterプラグインとONTAP SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

SLAは、期待されるサービスレベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要がある時間です。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ます。SLA、RTO、RPOは、データ保護戦略に影響します。

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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。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とRPOはデータ保護戦略に影響します。

使用頻度の高いリソースであっても、フルバックアップを1日に1~2回以上実行する必要はありません。

バックアップスケジュールには、次の2つの部分があります。

- 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タイミング）は、リソースグループ設定の一部です。たとえば、リソースグループのポリシーで週単位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ファイルシステムのバックアップ数

必要なバックアップの数を決定する要因には、Windowsファイルシステムのサイズ、使用されているボリュームの数、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名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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ことも、保持するバックアップコピーの数（ONTAPの最大コピー数255）を指定することもできます。たとえば、組織で、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する必要があるとします。

ポリシーの作成時に、バックアップタイプと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のスケジュールタイプを変更した場合、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バックアップは、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クローニングできます。また、要件に合わせてバックアップ先を選択することもできます。バックアップ元の場所と、同じホストまたは別のホスト上の別のデスティネーションのどちらかを選択することもできます。デスティネーションは、クローンソースのバックアップと同じボリュームに配置する必要があります。

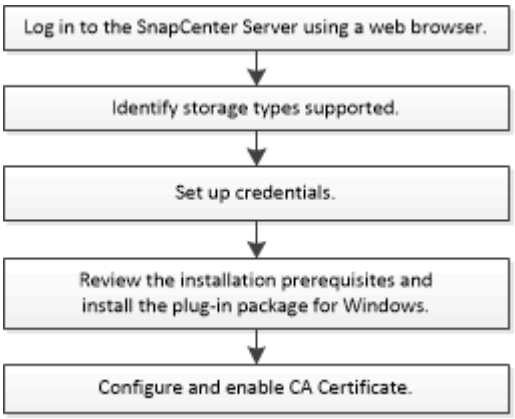
デスティネーションをクローニングします	説明
元の、ソース、場所	デフォルトでは、 SnapCenter はクローンを作成するバックアップと同じホストの同じ場所に格納します。
別の場所	同じホストまたは別のホストの別の場所にクローンを格納できます。ホストでStorage Virtual Machine（SVM）への接続が設定されている必要があります。

クローン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のインストール

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ときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

Plug-in for Windowsの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 *
- プラグインをインストールする前にWindows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には、リモートホストに対する管理者権限（管理者権限を含む）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する場合で、ユーザに完全なadmin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の権限を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、次の手順を実行します。

フィールド	操作
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。ユーザ名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、必要に応じて[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を割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
. . コンピュータオブジェクトをグループに追加します。
. . 作成したユーザグループを使用してgMSAを作成します。
```

   例えば、

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
. . コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。
```

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。

6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

ホストを追加して**SnapCenter Plug-in for Microsoft Windows**をインストールする

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。SnapCenter Plug-in for Microsoft Windowsは、指定したホストに自動的にインストールされます。プラグインのインストールには、この方法を推奨します。ホストの追加とプラグインのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- 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、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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
- メッセージキューサービスがrunning状態であることを確認する必要があります。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理Privilegesを使用してgMSAを設定する必要があります。

  "Windows Server 2016以降でのWindowsファイルシステム用のグループ管理サービスアカウントの設定"

タスクの内容

- 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
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
  - 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。

SnapCenterでは、すでにワークグループに属していて別のドメインに変更されたホスト（プラグインホスト）をSnapCenterに追加することはできません。その逆も同様です。同じホストを追加する場合は、SnapCenterからホストを削除して再度追加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. 上部で [Managed Hosts] が選択されていることを確認します。
3. [追加]*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	操作
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	操作
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、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）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 • 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、ホストタイプなどの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、[ホスト追加]ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]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。

   新規導入の場合は、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	操作
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	デフォルトのパスはC：\Program Files\NetApp\SnapCenter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の場合、デフォルトパスはC：\Program Files\NetApp\SnapCenterです。ただし、必要に応じて、デフォルトの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	WSFC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オンにします。
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。
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	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選択します。 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。

[事前チェックをスキップ]*チェックボックスを選択していない場合、プラグインをインストールするための要件を満たしているかどうかを確認するためにホストが検証されます。 ディスクスペース、RAM、PowerShellのバージョン、 ネットバージョンと場所は、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、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、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 `C:\Program Files\NetApp\SnapCenter` 。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. 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た、複数のリモートホストへのSnapCenter Plug-in for Microsoft Windowsのインストール

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、PowerShellコマンドレットを使用し `Install-SmHostPackage` ます。

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、コマンドレットを使用してセッションを確立し `Open-SmConnection` 、クレデンシャルを入力します。
3. コマンドレットと必要なパラメータを使用して、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. 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 `Install-SmHostPackage` ます。

   オプションは、プラグインを手動でインストールしたあとに、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に使用でき `-skipprecheck` ます。

コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレントインストール

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。

開始する前に

- Microsoftがインストールされている必要があります。 Net 4.7.2以降。

- PowerShell 7.4.2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. 次のコマンドを入力し、変数をデータに置き換えます。

   ```
   "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。

   次の変数の値を入力します。

変数	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。

変数	値
BI_ServiceAccount	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントを指定します。
BI_SERVICEPWD	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時に実行されるプラグインの前提条件に関するチェックの結果が含まれているため、トラブルシューティング情報を取得するには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 GUIまたはPowerShellコマンドレットを使用してホストを追加することで、SnapCenterサーバにプラグインを登録できます。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の監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストのプラグインサービスとバインドします。

   ```
   > $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"
   ```

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（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。

展開の詳細については、を参照してください "導入の概要"。

CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、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ファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリで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は、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

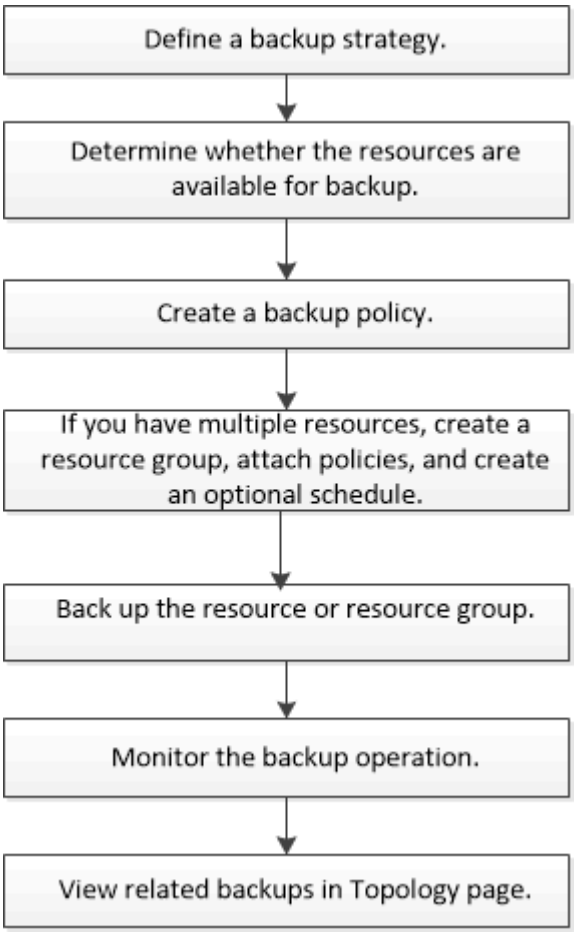
Windowsファイルシステムのバックアップ

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。同じリソースに対してバックアップ処理とリストア処理を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。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 "SnapCenter ソフトウェアコマンドレットリファレンスガイド" 参照してください。

Windowsファイルシステムの使用可能なリソースを確認する

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ファイルシステム内のLUNや類似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と、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、その前に使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と、プラグイ

ンのインストールが正常に完了したことも確認されます。

開始する前に

- 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を導入して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。

   SnapCenter以外でデータベースの名前が変更された場合は、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。

開始する前に

- バックアップ戦略を定義しておく必要があります。 "詳細"
- 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する必要があります。

- Snapshot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場合は、SnapCenter管理者が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を割り当てておく必要があります。
- 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。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

タスクの内容

- 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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

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. 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ら、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
ファイルシステム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。

オプション	説明
ファイルシステム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保護スケジュールは、リソースグループで定義します。そのため、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共有していても、バックアップスケジュールが異なる場合があります。

午前2時にスケジュールを設定している場合、夏時間（DST）中はスケジュールはトリガーされません。

7. [Retention]ページで、オンデマンドバックアップおよび選択した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ストアのSnapshot数を指定してからSnapshotを自動的に削除する場合は、このオプションを選択します。
次の期間を経過したSnapshotコピーを削除	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。
Snapshotコピーのロック期間	[Snapshot locking period]を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

保持数は2以上に設定する必要があります。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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。

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	操作
• 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）は、このオプションを選択します。 このオプションは、SnapSnapMirrorのアクティブな同期に対して有効にする必要があります。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 を参照して "[Topologyページで関連するバックアップとクローンを表示する"]
Snapshotコピーの作成後に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。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合は、[Topology]ページの[Refresh]ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、を参照してください。 "SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする"

フィールド	操作
セカンダリポリシーラベル	Snapshotラベルを選択します。 選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。 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。
エラー時の再試行回数	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のSnapshot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、ログの送信を行うスクリプトを実行できます。

   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からの相対パスである必要があります。

10. 概要を確認し、 [完了] をクリックします。

Windowsファイルシステムのリソースグループの作成

リソースグループは、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。また、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必要があります。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用しない新しいファイルシステムを、SnapMirrorアクティブ同期を使用するリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいファイルシス

テムを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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、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[Name]ページで、次の手順を実行します。

フィールド	操作
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コピーにカスタムの名前形式を使用する	オプション：Snapshotのカスタムの名前と形式を入力します。 たとえば、customText_resourcegroup_policy_hostnameやresourcegroup_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されます。
タグ	リソースグループの検索に役立つ説明タグを入力します。

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。

      最近追加したリソースは、リソースリストを更新するまで使用可能なリソースのリストに表示されません。

   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。

      要件を満たす既存のポリシーがない場合は、**をクリックしてポリシーウィザードを開始することで、新しいポリシーを作成できます + 。

      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。

   b. [Configure schedules for selected policies]セクションで、スケジュールを設定するポリシーの[Configure Schedules]列にある***をクリックします + 。

   c. 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。

   d. [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。

   サードパーティの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はサポートされません。WindowsタスクスケジューラとSQL Server Agentからスケジュールを変更しないでください。

7. [通知] ページで、次の通知情報を指定します。

フィールド	操作
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。
開始	Eメールアドレス
宛先	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

8. 概要を確認し、 [完了] をクリックします。

   バックアップはオンデマンドで実行することも、スケジュールされたバックアップが実行されるまで待機することもできます。

Windowsファイルシステムの単一リソースをオンデマンドでバックアップ

リソースグループに含まれていないリソースは、[Resources]ページからオンデマンドでバックアップできます。

タスクの内容

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。

SnapCenter UI

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[Resource]ページで、Snapshot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などです。デフォルトでは、Snapshot名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、 をクリックしてポリシー ウィザードで新しいポリシーを作成できます。

      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。

   b. [Configure schedules for selected policies]セクションで、スケジュールを設定するポリシーの[Configure Schedules]列内をクリックします 。

   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。

   "スケジュールされた処理が失敗する"

6. [通知] ページで、次のタスクを実行します。

フィールド	操作
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
開始	Eメールアドレス
宛先	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

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、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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   b. [バックアップ] 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

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バックアップタイプがFULLBACKUPの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がcrashConsistentの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、指定したホスト上の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、SnapCenterに新しいリソースグループを追加します。

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します。

```
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。

   次に、指定した日付に実行されたすべてのジョブのジョブ概要レポートを表示する例を示します。

```
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"。

Windowsファイルシステムのリソースグループのバックアップ

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に対して実行されます。リソースグループは、[Resources]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、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。

開始する前に

- ポリシーを適用して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、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に時間がかかることがあります。Web.config でMaxRetryForUninitializedHostsの値を設定するには、PowerShellのSet-SmConfigSettingsコマンドレットを使用します。

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ことができます。そのためには、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、タグを選択します。そのあとにをクリックすると、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。

   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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   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で保護関係を検出できないことがあります。

     "MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

   - VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、バックアップが失敗することがあります。Javaヒープサイズを大きくするには、スクリプトファイルを探し `/opt/netapp/init_scripts/scvservice`ます。このスクリプトでは、コマンドによって `do_start method` 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 `Java -jar -Xmx8192M -Xms4096M`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する

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しておく必要があります。

開始する前に

- 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でサポートする各ストレージシステムには、一意の名前と一意の管理LIF IPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

   この例では、PowerShellセッションを開きます。

   ```
   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。

   新しいストレージシステム接続を作成する例を次に示します。

   ```
   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。

   この例では、Windowsクレデンシャルを使用してFinanceAdminという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"。

バックアップ処理の監視

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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]ペインでの処理の監視

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

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 *
- 操作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、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。

アクセス元	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。
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックして、最新の5つの処理を表示します。 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]ページで関連するバックアップとクローンを表示する

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ときに、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。[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

タスクの内容

プライマリストレージと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）にバックアップと

クローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-  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。

-  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、バックアップを4つだけ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。
  - 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。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。

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. [Summary]カードで、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

の概要を確認します。

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。

「 * 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。

SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

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カスタムプラグインを使用している場合、プライマリストレージシステム上の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、をクリックして削除します。

プライマリストレージのバックアップとクローンの例

PowerShellコマンドレットを使用したバックアップの削除

Remove-SmBackupコマンドレットを使用すると、他のデータ保護処理で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。

```
PS C:\> Open-SmConnection
```

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を使用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たセカンダリバックアップ数のクリーンアップ

Snapshot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するには、Remove-SmBackupコマンドレットを使用します。このコマンドレットは、[Manage Copies]トポロジに表示されるSnapshotの総数が、セカンダリストレージのSnapshotの保持設定と一致しない場合に使用できます。

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を含ま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ファイルシステムのリストア

Windowsファイルシステムのバックアップのリストア

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、指定したバックアップのすべてのデータをファイルシステムの元の場所にコピーする複数の段階からなるプロセスです。

開始する前に

- 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その処理をキャンセルする必要があります。
- 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、別のパスにはリストアできません。

  リストアされたファイルシステムはファイルシステムの元の場所のデータを上書きするため、バックアップから単一のファイルを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またはブートボリュームを復元することはできません。
- 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。

タスクの内容

- 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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するため に、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択する必要があります。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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、ログの送信などを行うスクリプトを実行できます。

   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からの相対パスである必要があります。

7. [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	操作
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。
失敗した処理に関するAutoSupport通知をストレージシステムに送信	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。
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、送信先と送信元のEメールアドレスを入力します。

8. 概要を確認し、 [完了] をクリックします。
9. 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ってい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

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

PowerShellコマンドレットを使用したリソースのリストア

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

リストア処理の監視

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

リストア処理をキャンセルする

キューに登録されているリストアジョブは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。

タスクの内容

- 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。
- キューに格納されているリストア処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用して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。

アクセス元	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。
[Activity]ペイン	1. リストア処理を開始したら、[Activity]ペインをクリックして、 最新の5つの処理を表示します。 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。

開始する前に

- 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）の割り当て済みアグリゲートリストに含まれている必要があります。
- 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すると、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。
- アグリゲートのホームノード以外のノードにクローンを作成することはできません。
- Windowsファイルシステムでは、定期的なクローニング（クローンライフサイクル）処理のスケジュールを設定することはできません。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。
- 複数の環境間でのクローニングは実行できません。たとえば、物理ディスクから仮想ディスクへ、またはその逆のクローンを作成します。

タスクの内容

- 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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するため に、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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、クローニング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	操作
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、パスを使用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。
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は、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からの相対パスである必要があります。
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

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一覧を表示します。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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します。

   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、クローン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"。

クローニング処理の監視

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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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。

タスクの内容

- 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。
- キューに登録されているクローン処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用してキャンセルできます。
- 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。

アクセス元	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。
[Activity]ペイン	1. クローン処理を開始したら、[Activity]ペインでをクリックして、 最新の5つの処理を表示します。 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する

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングまたは検証が失敗する"

Microsoft Exchange Serverデータベースの保護

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。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化されます。

Plug-in for Exchangeがインストールされている場合は、SnapCenterと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したり、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したりできます。

Exchangeデータベース全体ではなく、Eメールまたはメールボックス全体をリストアおよびリカバリする場合は、Single Mailbox Recovery（SMBR）ソフトウェアを使用できます。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。

Plug-in for ExchangeはSnapMirror Active Sync（当初はSnapMirror Business Continuity [SM-BC]としてリリース）をサポートしています。これにより、サイト全体に障害が発生してもビジネスサービスの運用を継続でき、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirror Active Syncでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SnapMirror Active Syncの非対称モード、フェイルオーバーモード、または二重モード以外のモードがサポートされます。これは、最適パスがプライマリ側のLUNの所有者ノードからのみ作成されるソリューションを意味します。セカンダリクラスタパス上のI/Oは、プライマリクラスタにプロキシ経由で処理されます。同期レプリケーションは、プライマリからセカンダリへの単方向です。

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実行できます。

- 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の表示と管理
- バックアップ自動化の保護設定を提供するポリシーを定義
- リソースグループへのポリシーの割り当て
- 個 々 のDAGとデータベースを保護

- プライマリおよびセカンダリのExchangeメールボックスデータベースをバックアップする
- 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のデータベースのリストア

SnapCenter Plug-in for Microsoft WindowsおよびSnapCenter Plug-in for 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。サポートされるバージョンの最新情報については https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT、NetApp Interoperability Matrix Tool^]を参照してください。

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セツソク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セツソク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をプロビジョニングするには、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

- ジョブ履歴の表示
- ジョブの停止
- LUN
- LUNの作成
- LUNの作成
- LUNの作成
- lun delete
- LUN igroupの追加
- lun igroup create
- lun igroup delete
- LUN igroupの名前変更
- LUN igroupの名前変更
- lun igroup show
- LUNマッピングの追加-レポートノード
- LUNマッピングの作成
- LUNマッピングの削除
- lun mapping remove-reporting-nodes
- lun mapping show
- LUN変更
- ボリューム内でのLUNの移動
- LUNオフライン
- LUNオンライン
- LUN永続的予約のクリア
- LUNのサイズ変更
- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set

- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- volume snapshot modify -snaplock-expiry-time
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create

- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限
  - ネットワークインターフェイス
  - network interface show
  - SVM

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の準備

SnapCenterプラグインとONTAP SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

SLAは、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要があるまでの時間です。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、RPOがバックアップ戦略に影響します。

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、リソースタイプ（データベースやDatabase Availability Group（DAG；データベース可用性グループ）など）を選択する必要があります。Snapshotテクノロジを使用して、リソースが配置されてい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	データベースと、切り捨てられる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する必要があります。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できます。
フルバックアップ	データベースおよび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の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きめ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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。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とRPOはデータ保護戦略に影響します。

使用頻度の高いリソースであっても、フルバックアップを1日に1~2回以上実行する必要はありません。たとえば、定期的なトランザクションログバックアップで十分な場合は、必要なバックアップを作成できます。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つの部分があります。

- 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タイミング）は、リソースグループ設定の一部です。たとえば、リソースグループのポリシーで週単位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には、リソースのサイズ、使用されているボリュームの数、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のデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

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ことも、保持するバックアップコピーの数（ONTAPの最大コピー数255）を指定することもできます。たとえば、組織で、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する必要があるとします。

ポリシーの作成時に、バックアップタイプと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のスケジュールタイプを変更した場合、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 Exchangeで午前8時にフルバックアップとトランザクションログバックアップが、午後5時に別のフルバックアップとトランザクションログバックアップが作成された場合、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時の任意の時点にデータベースをリストアできます。トランザクションログが使用できない場合、Plug-in for Exchange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はフルバックアップがフルバックアップを完了した時点のフルバックアップが完了した時点にデータベースをリストアできます。

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日です。デフォルトでは、SnapCenterの保持期間は最低2日です。

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、データベースを正常にリストアできます。

Exchange Serverでのリストア処理のソース

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。

- 最新の状態へのリストア
- 過去のポイントインタイムへのリストア

最新の状態へのリストア

最新の状態へのリストア処理では、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実行されます。

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をリストアします。
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が適用されます。

   トランザクションログは先に移動され、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、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では、連続する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の実行後は、リストアに使用したバックアップをポイントインタイムリストア処理でのみ使用できます。

   すべてのバックアップに対して最新の状態へのリストア機能を実行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の保持を設定できます。

過去のポイントインタイムへのリストア

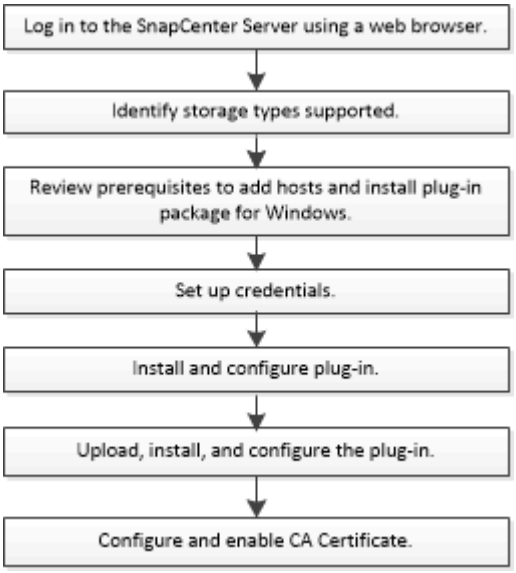
ポイントインタイムリストア処理では、データベースは過去の特定の時刻にのみリストアされます。ポイントインタイムリストア処理は、次の状況で実行されます。

- データベースは、バックアップトランザクションログの所定の時間にリストアされます。
- データベースがリストアされ、一部のバックアップトランザクションログのみが適用されます。

SnapCenter Plug-in for Microsoft Exchange Serverのインストール

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Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- 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に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ときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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の管理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、SnapCenterを使用したデータ保護を確実に行うために、同じExchange ServerにPlug-in for Exchangeをインストールする前に、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。
- 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。

- ホストを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、ホストの追加処理が失敗します。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"。
  - ポート範囲50000～51000（Windows 2016およびExchange 2016の場合）
  - Windows Server 2012 R2およびExchange 2013のポート範囲6000~6500
  - Windows 2019のポート範囲49152~65536

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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

必要な**Exchange Server**の権限

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。

ドメインユーザには、ローカル管理者権限、リモートExchangeホストに対するローカルログイン権限、DAG内のすべてのノードに対する管理権限が必要です。ドメインユーザに必要な最小権限は次のとおりです。

- Add-MailboxDatabaseCopy
- Dismount -データベース
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- MOVE-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly：$true
- マウント-データベース
- New-MailboxDatabase
- 新規- PublicFolderDatabase
- Remove-MailboxDatabase
- 削除-MailboxDatabaseCopy
- 削除- PublicFolderDatabase
- 再開- MailboxDatabaseCopy

- Set-AdServerSettings
- set-MailboxDatabase-allowfilerestore：$true
- MailboxDatabaseCopyの設定
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- 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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-in for Windowsの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プラグインパッケージのインストールに使用するクレデンシャルと、データベースでデータ保護処理を実行するためのクレデンシャルをそれぞれ作成する必要があります。

タスクの内容

Windowsホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。Windowsのクレデンシャルは、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作成することもできますが、SVMを追加したあと、ホストの導入とプラグインのインストールを開始する前に作成することを推奨します。

このクレデンシャルには、管理者権限（リモートホストに対する管理者権限を含む）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、ユーザ名に完全なadmin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の権限を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。

   [クレデンシャル]ウィンドウが表示されます。

4. [Credential]ページで、次の手順を実行します。

フィールド	操作
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	操作
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。ユーザ名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 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
      .. コンピュータオブジェクトをグループに追加します。
      .. 作成したユーザグループを使用してgMSAを作成します。
      ```

      例えば、

      ```
       New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
      -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      .. コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。
      ```

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

ホストを追加して**Plug-in for Exchange**をインストールする

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。Plug-in for Exchangeは指定したホストに自動的にインストールされます。プラグインのインストールには、この方法を推奨します。ホストの追加とプラグインのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- この処理は、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実行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ときに、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストの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。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理者権限で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 2016 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"。

タスクの内容

- 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、ホストごとまたはクラスタごとに実行できます。
- ExchangeノードがDAGの一部である場合、SnapCenterサーバにノードを1つだけ追加することはできません。
- 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、次の方法で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を使用しないDAGをクロスドメインまたは別のドメインに追加する	サポート対象外	サポート対象

ホスト追加処理	**4.5**以前	**4.6**以降
同じドメインまたはクロスドメインに存在する一意の名前を持つ複数のIP DAGを追加する	サポート対象	サポート対象
クロスドメインに同じホスト名またはDB名を持つIPまたはIPを使用しないDAGを複数追加する	サポート対象外	サポート対象
同じ名前でクロスドメインのIP/IPを使用しないDAGを複数追加する	サポート対象外	サポート対象
同じ名前でクロスドメインの複数のスタンドアロンホストを追加する	サポート対象外	サポート対象

Plug-in for ExchangeはSnapCenter Plug-ins Package for Windowsに依存し、同じバージョンである必要があります。Plug-in for Exchangeのインストール時には、SnapCenter Plug-ins Package for Windowsがデフォルトで選択され、VSSハードウェアプロバイダとともにインストールされます。

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、 また、Plug-in for Exchangeを同じExchangeサーバにインストールする場合は、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。これは、Plug-in for ExchangeおよびSnapCenter Plug-ins Package for WindowsとともにインストールされたVSSハードウェアプロバイダとの互換性がないためです。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]*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	操作
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	操作
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、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を入力することを推奨します。 信頼されていないドメインホストのIPアドレスは、そのIPアドレスが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の場合は、次の操作を実行できます。 ◦ DAG名、DAG IPアドレス、ノード名、またはノードIPアドレスを指定してDAGを追加します。 ◦ いずれかのDAGクラスタノードのIPアドレスまたはFQDNを指定して、IPのない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存在するIPのないDAGを追加します。IP/IPを含まないDAGは、同じ名前でドメインが異なる複数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（ドメイン間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	操作
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 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. [Select Plug-ins to Install]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に必要なメモリ使用量やその他のリソース使用量を考慮して、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	操作
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	デフォルトのパスはです `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	DAGを追加する場合は、このチェックボックスをオンにします。

フィールド	操作
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。
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	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選択します。 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 prechecks]チェック ボックスをオフにしていると、ホストがプラグインをインストールするための要件を満たしているかどうかを確認するための検証が行われます。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、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 `C:\Program Files\NetApp\SnapCenter` 。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. インストールの進行状況を監視します。

ネット**TCP**通信用のカスタムポートの設定

SnapCenter 6.0リリース以降、SnapCenter Plug-in for Windowsでは、デフォルトでポート909がネットTCP通信に使用されます。ポート909が使用中の場合は、ネットTCP通信用に別のポートを設定できます。

手順

1. _C：\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config_にある_NetTCPPort_keyの値を必要なポート番号に変更します。
   `<add key="NetTCPPort" value="new_port_number" />`
2. C：\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config_にある_NetTCPPort_keyの値を必要なポート番号に変更します。
   `<add key="NetTCPPort" value="new_port_number" />`
3. 次のコマンドを実行して、Data ONTAP VSSハードウェアプロバイダサービスの登録を解除します。
   `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft`

```
Windows\navssprv.exe" -r service -u
```

サービスが_services.msc_のサービスのリストに表示されていないことを確認します。

4. 次のコマンドを実行して、_ Data ONTAP VSS Hardware Provider_serviceを登録します。
```
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`
```

サービスが_services.msc_のサービスのリストに表示されていることを確認します。

5. _Plug-in for windows_serviceを再起動します。

PowerShellコマンドレットを使用したSnapCenter ServerホストからのPlug-in for Exchangeのインストール

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。

開始する前に

- 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。
- この処理は、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実行する必要があります。
- 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でもかまいません。DAG を指定する場合は、 -IsDAG_parameterが必要です。

3. 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の**SnapCenter Plug-in for Exchange**のサイレントインストール

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。

開始する前に

- 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	値
	次の例のように、スイートインストーラログファイルの名前と場所を指定します。 *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。
BI_ServiceAccount	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントを指定します。
BI_SERVICEPWD	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。

6. 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。
7. *%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 GUIまたはPowerShellコマンドレットを使用してホストを追加することで、SnapCenterサーバにプラグインを登録できます。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の監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
-

完了（警告あり）または警告のため開始できませんでした

- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストのプラグインサービスとバインドします。

   ```
   > $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"
   ```

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、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**を設定する

SnapCenter Plug-in for Microsoft Exchange ServerをSnapManager for Microsoft Exchange Serverと共存させるには、SnapManager for Microsoft Exchange Serverがインストールされている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して、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する必要があります。

開始する前に

- SnapManager for Microsoft Exchange ServerおよびSnapDrive for Windowsがすでにインストールされており、SnapManager for Microsoft Exchange Serverのバックアップがシステム上およびSnapInfoディレク

トリに存在します。

- 不要になったSnapManager for Microsoft Exchange Serverで作成した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で作成したすべてのスケジュールをWindowsスケジューラで一時停止または削除しておく必要があります。
- SnapCenter Plug-in for Microsoft Exchange ServerとSnapManager for Microsoft Exchange Serverは同じExchange Serverに共存できますが、既存のSnapManager for Microsoft Exchange Server環境を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オプションがありません。

- SnapCenterでは、SnapManager for Microsoft Exchange Serverバックアップからの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せずに、あとで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のインストール

データベースまたはファイルシステムが仮想マシン（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。

展開の詳細については、を参照してください "導入の概要"。

CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、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ファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリで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は、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

データ保護の準備

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テクノロジを利用するには、ストレージデバイス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て実行できます。

- 詳細はこちら *

"REST APIの使用"

SnapCenter Plug-in for Microsoft Exchange Serverを使用するための前提条件

Plug-in for Exchangeを使用する前に、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 にログインします。
- SnapCenter環境を設定するために、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をインストールして、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。
- SnapCenterサーバを使用してVMware RDM LUN上にあるExchangeデータベースを保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してプラグインを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対象の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な場合は、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。NetAppデータブローカー1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetAppデータブローカー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を使用した仮想データベースおよび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 4.3.xのユーザ向けに、SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、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）を使用した仮想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 Plug-in for VMware vSphereのドキュメント"

Exchange Serverを保護するためのリソース、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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- 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）です。
- SnapCenterリソースグループは、ホストまたはExchange DAG上のリソースの集まりであり、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。

  リソースグループに対して処理を実行すると、リソースグループに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。

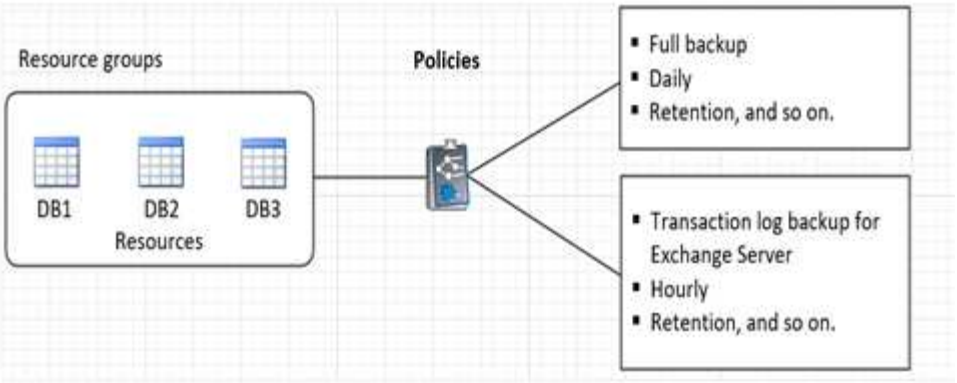
  単一のリソースまたはリソースグループをオンデマンドでバックアップできます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを実行することもできます。

  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、そのグループのポリシーを1つ以上選択します。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。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。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時間ごと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。



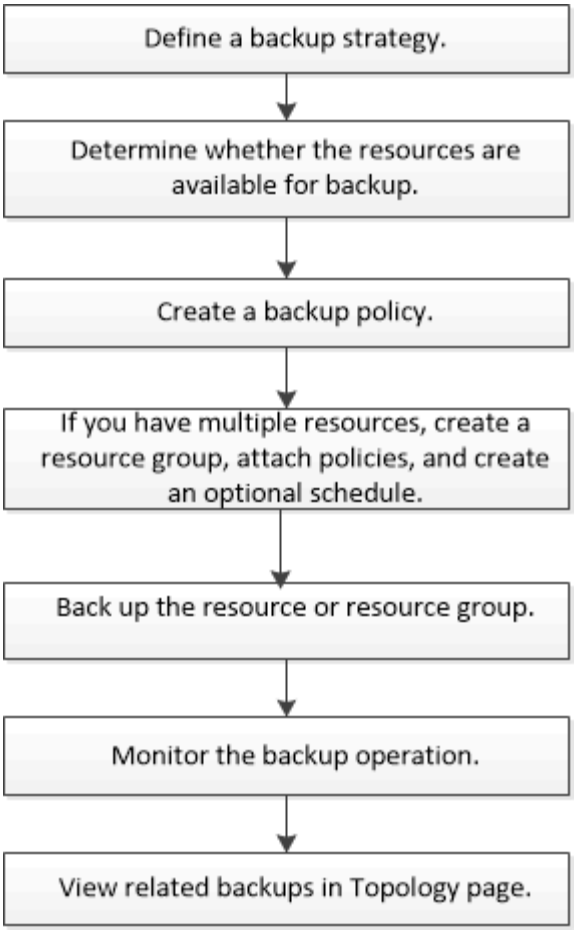
Exchangeリソースのバックアップ

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。同じリソースに対してバックアップ処理とリストア処理を同時に実行することはできません。同じボリューム上でのアクティブバックアップコピーとパッシブバックアップコピーはサポートされていません。

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データベースと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行われませんが、Exchangeに付属のEseutilツールを使用して、Exchangeデータベースおよびバックアップを検証できます。

Microsoft Exchange Eseutilツールは、Exchangeサーバに付属の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、整合性チェックを実行して、Exchangeデータベースおよびバックアップの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。

詳細については、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の確認

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、Exchangeデータベース可用性グループです。こ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ジョブを実行できますが、その前に使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。

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、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 Server上にアクティブ・データベースを配置しておく必要があります。
- データベースがVMware RDM LUN上にある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。詳細については、を "SnapCenter Plug-in for VMware vSphere のドキュメント" 参照してください。

タスクの内容

- [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mount、unmount、reseed、またはrecovery pending状態のとき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。

   すべてのデータベースとDAGは、それぞれのDAGまたはホスト名とともにFQDN形式で表示されるため、複数のデータベースを区別できます。

   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。そのあとにをクリックすると、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。

   SnapCenter以外でデータベースの名前が変更された場合は、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なサーバ、コピーがあるサーバ、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。

   - 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は、[Overall Status]列に「Not available for backup」と表示されます。

     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では、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の作成

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。

開始する前に

- 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リソースをリフレッシュ（検出）しておく必要があります。
- Snapshot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、SnapCenter管理者が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Storage Virtual Machine（SVM）をユーザに割り当てておく必要があります。
- 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、ファイルでパラメータの値をtrueに設定する必要があります `usePowershellProcessforScripts` `web.config` 。

  デフォルト値はfalseです。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

タスクの内容

- バックアップポリシーは、バックアップを管理および保持する方法、およびリソースまたはリソースグループをバックアップする頻度を規定する一連のルールです。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することで、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できます。
- フルバックアップの保持は、特定のポリシーに固有です。フルバックアップの保持数が4のポリシーAを使用するデータベースまたはリソースでは、4つのフルバックアップが保持され、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。保持数を3に設定すると、3つのフルバックアップが保持される場合があります。

- ログバックアップの保持はポリシーに関係なく有効で、データベースまたはリソースのすべてのログバックアップに適用されます。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場合、ログ保持設定は、ポリシーAで同じデータベースまたはリソース上に作成されたログバックアップに影響します。同様に、ポリシーAのログ保持設定は、同じデータベース上にポリシーBで作成された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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

  * 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は、異なるボリュームにあるデータベースとログの場合、各バックアップに3つのSnapshotを保持でき、データベースとログが同じボリュームにある場合は、各バックアップに2つのSnapshotを保持できることに注意してください。

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。

    Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。

    ONTAP 9.12.1以前のバージョンでは、SnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

    プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

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：

状況	操作
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する	[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と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する	[* Full backup*] 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はバックアップされません。
すべてのトランザクションログをバックアップする	「 * Log backup * 」を選択します。 アクティブファイルシステム上のすべてのトランザクションログがバックアップされ、ログの切り捨ては行われません。 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ており、完全なログ・ファイルとは異なります。
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する	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、ログの切り捨ては行われません。このバックアップタイプは、通常、レプリカの再シードや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、up-to-the-minute（UTM；最新の状態へのリストア）ではなく、フルバックアップの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、処理を選択します。

フィールド	操作
アクティブなコピーをバックアップ	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がバックアップされます。 パッシブコピーはバックアップされません。
バックアップジョブの作成時に選択するサーバ上のコピーをバックアップする	選択したサーバ上のデータベースのコピー（アクティブとパッシブの両方）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。 DAGの場合は、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、バックアップがクラスタの各ノードで保持されます。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が保持されます。保持期間はノードレベルでのみ適用されます。

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）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ができます。

午前2時にスケジュールを設定している場合、夏時間（DST）中はスケジュールはトリガーされません。

6. [Retention]ページで、保持を設定します。

表示されるオプションは、以前に選択したバックアップタイプと頻度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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。

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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。

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	操作
特定の数のログバックアップのみを保持	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。 up-to-the-minute（UTM；最新の状態へのリストア）の保持は、フルバックアップまたはログバックアップで作成されたログバックアップに適用されます。たとえば、過去5回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UTM保持設定が設定されている場合、過去5回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。 フルおよび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。ログフォルダを手動で削除することはできません。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、ログバックアップの保持期間が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に従って削除されます。そのため、ログフォルダは10日間しか保持されず、その他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保持の値を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：[Full backup retention settings]セクションの[Total Snapshots（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、フルバックアップごと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	「 * 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。 フルバックアップが保持される日数までのログバックアップが保持されます。
Snapshotロック期間	[Snapshotコピーロック期間]*を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

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. [Full backup retention settings]セクションで、オンデマンドバックアップの場合は次のいずれかを選択し、フルバックアップの場合は1つを選択します。

フィールド	操作
特定の数のSnapshotのみを保持	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（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、最も古いコピーから順に削除されます。
フルバックアップを特定の日数だけ保持	[Keep Snapshot copies for]*オプションを選択し、Snapshot（フルバックアップ）を保持する日数を指定します。
Snapshotロック期間	[Snapshotコピーロック期間]*を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

DAG構成のホストにログバックアップのみのデータベースがあり、フルバックアップがない場合は、次の方法でログバックアップが保持されます。

- 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">
```

この例の値が10の場合、ホストで保持できるログバックアップは最大10個です。

7. [Replication]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	操作
ローカルSnapshot作成後にSnapMirrorを更新する	バックアップセットのミラーコピーを別のボリューム（SnapMirror）に保持する場合は、このオプションを選択します。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。 このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。 プライマリのみのポリシーは、Exchange ONTAPボリュームに対してSnapMirrorのアクティブな同期が設定されている場合は使用できません。SnapCenterではこれが許可されていません。「ミラー」オプションを有効にする必要があります。 [Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 を参照して "[TopologyページでのExchangeバックアップの表示"]
ローカルSnapshot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	Snapshotラベルを選択します。 選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。 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。
エラー時の再試行回数	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のSnapshot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。

   スクリプトを実行して、SNMPトラップの更新、アラートの自動化、ログの送信などを行うことができます。

   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からの相対パスである必要があります。

9. 概要を確認し、 [完了] をクリックします。

Exchange Serverのリソースグループの作成とポリシーの適用

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。また、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必要があります。

タスクの内容

- 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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定されたリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいデータベースを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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 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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	オプション：Snapshotのカスタムの名前と形式を入力します。 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名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. リソースタイプとデータベース可用性グループをドロップダウンリストから選択して、使用可能なリソースのリストをフィルタリングします。

      最近追加したリソースは、リソースリストを更新するまで[Available Resources]のリストに表示されません。

      [Available Resources]セクションと[Selected Resources]セクションに、データベース名とホストのFQDNが表示されます。このFQDNは、データベースが特定のホストでアクティブであり、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含めることができるデータベースは、Snapshotあたり30個までです。1つのリソースグループに30を超えるデータベースがある場合は、追加のデータベース用に2つ目のSnapshotが作成されます。そのため、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設定されたバックアップで、SnapMirrorまたはSnapVaultの更新の実行中に、両方のサブジョブの更新が重複する場合があります。ログにジョブが完了したことが記録されている場合でも、メインのバックアップジョブは無期限に実行され続けます。

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。

      **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。サーバ選択オプションでは、選択したデータベースがNetApp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、スケジュールを設定するポリシーの*列にある*をクリックし + 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、 [*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。

   サードパーティの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`。

   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、『Software Cmdlet Reference Guide ^]』も参照して

https://docs.netapp.com/us-en/snapcenter-cmdlets/index.htmlnapCenter ください。

8. 概要を確認し、 [完了] をクリックします。

Exchangeデータベースのバックアップ

いずれのリソースグループにも含まれていないデータベースは、[Resources]ページからバックアップできます。

開始する前に

- 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、データベースで使用される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。NetApp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。

SnapCenter UI

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。

   [Resources]ページの  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、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、少なくとも1つのパッシブデータベースコピーがNetAppストレージにある場合は、データベースを保護できます。

   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、*をクリックしてフィルタペインを閉じることができます  。

   - 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]ウィザードが表示されたら、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。
3. カスタムのSnapshot名を指定する場合は、[リソース]ページで*[Snapshotコピーにカスタムの名前形式を使用する]*チェックボックスを選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名にタイムスタンプが追加されます。
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。

      **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。サーバ選択オプションでは、選択したデータベースがNetApp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. 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]列で**をクリックします  。
   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。

5. [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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。

6. 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ページが表示されます。

7. [今すぐバックアップ] をクリックします。
8. 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   b. [バックアップ] をクリックします。
9. ページ下部の[Activity]ペインでジョブをダブルクリックして[Job Details]ページを表示し、バックアップの進捗状況を監視します。
   - MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

     詳細については、次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関係を検出できない"

   - VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、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*

PowerShellコマンドレット

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、1時間ごとの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_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、SnapCenterに新しいリソースグループを追加します。

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_Lo
g_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_Lo
g_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します。

```
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。

次に、指定した日付に実行されたすべてのジョブのジョブ概要レポートを表示する例を示します。

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

次に、特定のジョブIDのジョブサマリレポートを表示する例を示します。

```
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、『Software Cmdlet Reference Guide ^]』を参照してください

https://docs.netapp.com/us-en/snapcenter-cmdlets/index.htmlnapCenter 。

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上のリソースの集まりであり、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[リソース]ページでバックアップできます。

開始する前に

- ポリシーを適用して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、データベースで使用される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、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の開始に時間がかかることがあります。PowerShellコマンドレットを使用して、の値を設定します `MaxRetryForUninitializedHosts` `web.config` `Set-SmConfigSettings` 。
- 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。

  NetApp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。

タスクの内容

リソースグループは、[Resources]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、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、をクリックしてタグを選択します。次に、をクリックしてフィルタペインを閉じることができます。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

b. [バックアップ] をクリックします。

5. ページ下部の[Activity]ペインでジョブをダブルクリックして[Job Details]ページを表示し、バックアップの進捗状況を監視します。

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する

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前に、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。

開始する前に

- 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. 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 `Open-SmConnection` 。

   この例では、PowerShellセッションを開きます。

   ```
   PS C:\> Open-SmConnection
   ```

2. 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 `Add-SmStorageConnection` ます。

   新しいストレージシステム接続を作成する例を次に示します。

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. コマンドレットを使用して、新しいRun Asアカウントを作成し `Add-Credential` ます。

この例では、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"。

バックアップ処理の監視

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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]ペインでの処理の監視

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

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 *
- 操作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、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。

アクセス元	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。

アクセス元	アクション
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックして、最新の5つの処理を表示します。 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たExchangeバックアップの削除

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. 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 `Remove-SmBackup` 。

   この例では、バックアップIDを使用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]ページでのExchangeバックアップの表示

リソースのバックアップを準備する際には、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の図を表示すると役立つことがあります。

タスクの内容

[Topology]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可能な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表示し、選択してデータ保護処理を実行できます。

プライマリストレージと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）のどちらにバックアップがあるかを確認するには、[コピーの管理]ビューの次のアイコンを確認します。

-  プライマリストレージで使用可能なバックアップの数が表示されます。
-  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、バックアップを4つだけ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。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。

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. [Summary card]セクションで、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と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。

SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。フェイルオーバー後。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

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。

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、名前変更、削除の各処理を実行します。

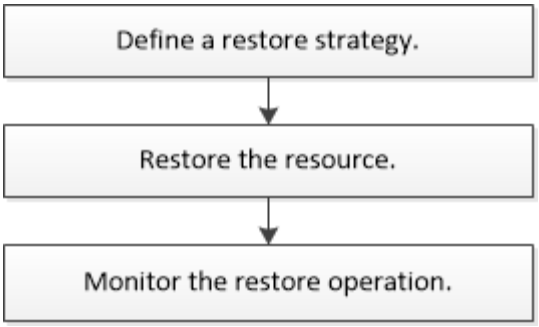
   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。Snapshotの削除は、ONTAPの保持設定で処理されます。

Exchangeリソースのリストア

リストアのワークフロー

SnapCenterを使用すると、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して、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、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。

リストア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がオンラインで実行され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。

  削除した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 Server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データベースのリストア

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。

開始する前に

- 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行した場合、古いバックアップに対してリストア処理を実行できません。
- Snapshot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、SnapCenter管理者が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にSVMを割り当てておく必要があります。
- DAGで、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、NetApp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には、そのパッシブコピー（NetApp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。

コマンドを実行して `Move-ActiveMailboxDatabase` 、データベースのパッシブコピーをアクティブデータベースコピーとして設定します。

このコマンドについては、を参照して "Microsoftのドキュメント" ください。

タスクの内容

- 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再度マウントされ、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、フルディスクリストアはサポートされません。

  Plug-in for Exchangeでは、ディスクにレプリケーションに使用するExchangeファイルなどのExchangeファイルが含まれている場合、ディスク上でフルリストアは実行されません。フルリストアがExchangeの機能に影響を及ぼす可能性がある場合、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で暗号化された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します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトの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を使用すると、キーの値を表示できます。Set APIはサポートされていません。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択する必要があります。

SnapCenter UI

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. [Manage Copies]ビューで、[Primary Backups]テーブルから*を選択し、**をクリックします  。
6. [Options]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。
次のログバックアップまで：	「 * 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の数は、UTMに基づいています。たとえば、フルバックアップの保持が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ためのログが3つだけ表示されます。
次の日付まで	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。
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。

次のいずれかの操作を実行できます。

- * 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。

   リストアプレスクリプトの引数には、$Databaseと$ServerInstanceがあります。

   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。

   スクリプトを実行して、SNMPトラップの更新、アラートの自動化、ログの送信などを行うことができます。

   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からの相対パスである必要があります。

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。

9. 概要を確認し、 [完了] をクリックします。
10. ページ下部の[Activity]パネルを展開すると、リストアジョブのステータスを確認できます。

    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。

バックアップからアクティブデータベースをリストアするときに、レプリカとアクティブデータベースの間に遅延があると、パッシブデータベースが一時停止状態または障害状態になることがあります。

状態の変化は、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したときに発生します。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。

PowerShellコマンドレット

手順

1. コマンドレットを使用して、指定したユーザでSnapCenterサーバとの接続セッションを開始します `Open-SmConnection` 。

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

2. コマンドレットを使用して、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` 。

次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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. 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` 。

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 -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ーリーにリストアします。

```
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
```

パラメータを使用 `-archive` 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。

パラメータを指定する `-IsRecoverMount:$true` 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"。

メールとメールボックスのきめ細かなリカバリ

Single Mailbox Recovery（SMBR）ソフトウェアを使用すると、Exchangeデータベース全体の代わりに、メールまたはメールボックスをリストアおよびリカバリできます。

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、多くの時間とリソースが消費されます。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に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

バックアップしたExchange Serverデータベースは、セカンダリストレージ（ミラーまたはバックアップ）からリストアできます。

プライマリストレージからセカンダリストレージにSnapshotをレプリケートしておく必要があります。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択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 [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. [Location]ページで、選択したリソースをリストアするデスティネーション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

Exchangeのパッシブノードレプリカの再シード

コピーが破損している場合などにレプリカコピーを再シードする必要がある場合は、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。

開始する前に

- 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、バージョン4.1より前の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. [Resources]ページで、[View]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には	[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には	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. ページ下部の[Activity]パネルを展開すると、ジョブのステータスを表示できます。

データベースのパッシブコピーがネットアップ以外のストレージにある場合、再シード処理はサポートされません。

Exchangeデータベースヨウノ**PowerShell**コマントレツトヲシヨウシタレプリカノサイシード

PowerShellコマンドレットを使用すると、同じホスト上の最新のコピーまたは代替ホストからの最新のコピーを使用して、正常でないレプリカをリストアできます。

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. コマンドレットを使用して、指定したユーザでSnapCenterサーバとの接続セッションを開始します `Open-SmConnection` 。

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. コマンドレットを使用して、データベースを再シードし `reseed-SmDagReplicaCopy` ます。

   この例では、ホスト「mva-rx200.netapp.com"」上のexecdbという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（production/copy）の最新のバックアップを使用して、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"
```

リストア処理の監視

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中

- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

Exchangeデータベースのリストア処理をキャンセルします

キューに登録されているリストアジョブは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。

タスクの内容

- 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。
- キューに格納されているリストア処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用して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。

アクセス元	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。
[Activity]ペイン	1. リストア処理を開始したら、[Activity]ペインをクリックして、 最新の5つの処理を表示します。 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。

IBM DB2の保護

IBM DB2用SnapCenterプラグイン

SnapCenter Plug-in for IBM DB2の概要

SnapCenter Plug-in for IBM DB2 Databaseは、IBM DB2データベースに対応した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。Plug-in for IBM DB2 Databaseは、SnapCenter環境でのIBM DB2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、シングル・インスタンスおよびマルチ・インスタンスのDB2セットアップをサポートしています。Plug-in for IBM DB2 Databaseは、Linux環境とWindows環境の両方で使用できます。Windows環境では、DB2は手動リソースとしてサポートされます。

Plug-in for IBM DB2 Databaseがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジを使用して、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、本プラグインをNetApp SnapVaultテクノロジとともに使用して、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 DB2は、ONTAPおよびAzure NetAppのファイルストレージレイアウトでNFSとSANをサポートします。

VMDKまたは仮想ストレージレイアウトはサポートされていません。

SnapCenter Plug-in for IBM DB2の機能

Plug-in for IBM DB2 Databaseをインストールした環境では、SnapCenterを使用して、IBM DB2データベースとそのリソースをバックアップ、リストア、および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します。
- 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 IBM DB2の機能

SnapCenterは、プラグインアプリケーションおよびストレージシステム上でNetAppテクノロジと統合されます。Plug-in for IBM DB2 Databaseを操作するには、SnapCenterグラフィカルユーザー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

  SnapCenterは、Plug-in for IBM DB2 DatabaseでNetAppスナップショットテクノロジを使用してリソースをバックアップします。

Plug-in for IBM DB2を使用すると、次のようなメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます。
- RBACでサポートされるセキュリティと一元化されたロール委譲

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルの権限を付与することもできます。

- NetApp FlexCloneテクノロジを使用して、テストまたはデータ抽出に使用するリソ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できます。

  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。

- バックアップ作成時にONTAPの整合グループ（CG）Snapshot機能がサポートされるようになりました。
- 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可能

  1回の操作で、1つのホスト内のリソースが同じボリュームを共有すると、スナップショットが統合されます。

- 外部コマンドを使用してスナップショットを作成する機能。
- XFSファイルシステムでのLinux LVMのサポート。

SnapCenter Plug-in for IBM DB2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 IBM DB2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こと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セツソクLUN

マシン	ストレージタイプ
物理サーバ	iSCSIセツソクLUN
物理サーバと仮想サーバ	NFS接続ボリューム

IBM DB2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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN
  - LUNの作成
  - LUNの作成
  - LUNの作成
  - lun delete
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード
  - LUNマッピングの作成
  - LUNマッピングの削除
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - LUN変更
  - ボリューム内でのLUNの移動
  - LUNオフライン
  - LUNオンライン
  - LUN永続的予約のクリア
  - LUNのサイズ変更

- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- volume snapshot modify -snaplock-expiry-time
- ボリュームSnapshotの名前変更

- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限
  - ネットワークインターフェイス
  - network interface show
  - SVM

IBM DB2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 SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

IBM DB2のバックアップ戦略

IBM DB2のバックアップ戦略の定義

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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

タスクの内容

SLAは、期待されるサービスレベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要がある時間です。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ます。SLA、RTO、RPOは、データ保護戦略に影響します。

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. アプリケーションと整合性のあるデータベースのSnapshotをバックアップするSnapshotコピーベースのポリシーを作成するかどうかを決定します。
5. レプリケーションにNetApp SnapMirrorテクノロジを使用するか、長期保持にNetApp SnapVaultテクノロジを使用するかを決定します。
6. ソースストレージシステムとSnapMirrorデスティネーションでのSnapshotの保持期間を決定します。
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。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterによって管理されるLinuxホスト上のIBM DB2データベースとインスタンスです。SnapCenter Plug-in for IBM DB2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インスタンスのIBM DB2データベースが自動的に検出され、[Resources]ページに表示されます。

サポートされるバックアップのタイプ

Backup typeには、作成するバックアップのタイプを指定します。SnapCenterでは、IBM DB2データベースに対してSnapshotコピーベースのバックアップタイプがサポートされます。

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テクノロジを利用して、IBM DB2データベースが格納されているボリュームのオンラインの読み取り専用コピーを作成します。

SnapCenter Plug-in for IBM DB2での整合グループ**Snapshot**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性グループのSnapshotを作成できます。整合グループはコンテナであり、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。整合グループは、複数のボリュームの同時Snapshotであり、ボリュームグループの整合性のあるコピーを提供します。

ストレージコントローラが整合性のあるSnapshotをグループ化するまでの待機時間を指定することもできます。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の処理中に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の同期により、整合性グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なデータバックアップの削除の管理方法

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データバックアップの削除を管理します。

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上のSnapshotと、IBM DB2カタログ内の対応するエントリが削除されます。

IBM DB2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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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つの部分があります。

- 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タイミング）

  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単位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。

IBM DB2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には、リソースのサイズ、使用されているボリュームの数、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 IBM DB2テエタヘエスノハツクアツフノメイメイキソク

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

IBM DB2のリストアおよびリカバリ戦略

IBM DB2リソースのリストアおよびリカバリ戦略の定義

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。

データベースの手動リカバリのみがサポートされます。

手順

1. 手動で追加したIBM DB2リソースでサポートされるリストア戦略を確認する
2. 自動検出されたIBM DB2データベースでサポートされているリストア戦略を確認する

手動で追加した**IBM DB2**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、戦略を定義する必要があります。手動で追加したIBM DB2リソースには、2種類のリストア戦略があります。

手動で追加したIBM DB2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

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のあとに作成されたSnapshotは削除され、リカバリできません。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。

自動検出された**IBM DB2**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、戦略を定義する必要があります。

完全リソースリストアは、自動的に検出されたIBM DB2データベースに対してサポートされるリストア戦略です。これにより、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

自動検出された**IBM DB2**のリストア処理のタイプ

SnapCenter Plug-in for IBM DB2は、自動検出されたIBM DB2データベースに対して、Single File SnapRestoreおよびConnect-and-Copyリストアタイプをサポートしています。

NFS環境で**Single File SnapRestore**を実行するシナリオは、次のとおりです。

- [Complete Resource]オプションのみが選択されている場合
- 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。

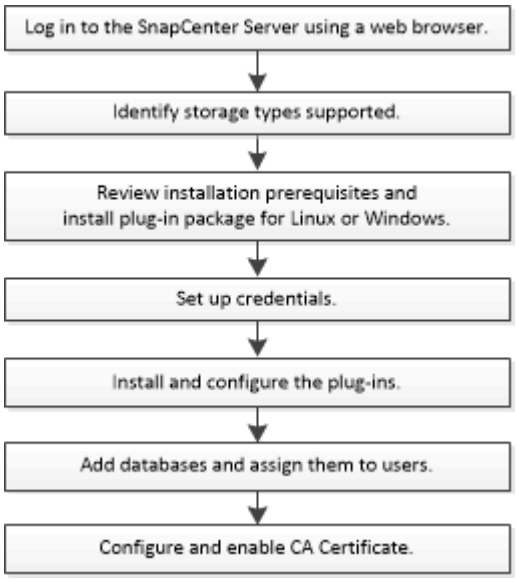
- [Complete Resource]オプションのみが選択されている場合
- SnapMirror または SnapVault セカンダリストレージからバックアップを選択し、 * Complete Resource * オプションを選択した場合

SnapCenter Plug-in for IBM DB2のインストールの準備

SnapCenter Plug-in for IBM DB2のインストールワークフロー

IBM DB2データベースを保護する場合は、SnapCenter Plug-in for IBM DB2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 IBM DB2**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 IBM DB2は、Windows環境とLinux環境の両方で使用できます。

- Java 11をホストにインストールしておく必要があります。

  IBM Javaはサポートされていません。

- Windowsの場合、Plug-in CreatorサービスはWindowsユーザ「LocalSystem」を使用して実行する必要があります。これは、Plug-in for IBM DB2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ホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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IBM DB2プラグインを使用してデフォルトで導入されます。
- SnapCenterサーバがPlug-in for IBM DB2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Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- Plug-in for IBM DB2をWindowsホストにインストールすると、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以外のユーザに対して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 11をWindowsホストにインストールしておく必要があります。

"すべてのオペレーティングシステム用のJavaダウンロード"

"NetApp Interoperability Matrix Tool"

Linuxホスト

- rootユーザまたはroot以外のユーザに対して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* mksh *ライブラリがインストールされている必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

- LinuxホストでIBM DB2データベースを実行している場合は、Plug-in for IBM DB2のインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- 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。

補助コマンド

SnapCenter Plug-in for IBM DB2で補足コマンドを実行するには、ファイルにそのコマンドを含める必要があります `allowed_commands.config` 。

`allowed_commands.config` ファイルは、SnapCenter Plug-in for IBM DB2ディレクトリの「etc」サブディレクトリにあります。

Windowsホスト

デフォルト： `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

カスタムパス： `<Custom_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Linuxホスト

デフォルト： `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

カスタムパス： `<custom_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config`

プラグインホストで追加のコマンドを許可するには、エディタでファイルを開きます `allowed_commands.config` 。各コマンドを別 々 の行に入力します。大文字と小文字は区別されません。例えば、

コマンド:mount

コマンド：umount

完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符（"）で囲みます。例えば、

コマンド："C：\Program Files\NetApp\SnapCreator commands\sdcli.exe"

コマンド：myscript.bat

ファイルが存在しない場合は `allowed_commands.config` 、コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

コマンドまたはスクリプトがに存在しないと、 `allowed_commands.config`コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

ワイルドカードエントリ（*）を使用してすべてのコマンドを許可しないでください。

Linuxホストの**root**以外のユーザに対する**sudo Privileges**の設定

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をroot以外の有効なユーザとして実行します。複数のパスにアクセスできるようにroot以外のユーザにsudo Privileges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
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- /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。

  構成ファイルの更新後に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/installation/plugins/uninstall
- /custom_location /NetApp/snapcenter/spl/bin/spl
- 手順 *

1. SnapCenter Plug-ins Package for Linuxをインストールする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_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- *C：\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt* SnapCenter ServerがWindowsホストにインストールされている場合。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc _ unix_plugins_checksum.txt _ SnapCenterサーバーがLinuxホストにインストールされている場合。

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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、基本的なホストシステムのスペースとサイジングの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 • 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量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、最近実行した処理の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 11 Oracle JavaおよびOpenJDK を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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 "NetApp Interoperability Matrix Tool" ください。

SnapCenter Plug-in for IBM DB2のクレデンシャルを設定する

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースまたは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クレデンシャルをそれぞれ作成する必要があります。

タスクの内容

- Linuxホスト

  Linuxホストにプラグインをインストールするには、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、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo Privilegesがあるroot以外のユーザに対して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

  プラグインをインストールする前にWindows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には、管理者権限（リモートホストに対する管理者権限を含む）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、ユーザ名に完全なadmin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の権限を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、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	操作
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	操作
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。ユーザ名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	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ユーザのみに適用されます。

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、必要に応じて[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を割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
      ```

      .. コンピュータオブジェクトをグループに追加します。
      .. 作成したユーザグループを使用してgMSAを作成します。

      例えば、

      ```
      New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
      -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      ```

      .. コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

SnapCenter Plug-in for IBM DB2のインストール

ホストを追加してリモートホストにプラグインパッケージをインストールする

SnapCenterの[ホストを追加]ページを使用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。プラグインはリモートホストに自動的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、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- 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、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストの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する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理Privilegesを使用してgMSAを設定する必要があります。

  "IBM DB2用のWindows Server 2016以降でのグループ管理サービスアカウントの設定"

タスクの内容

- 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]*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	操作
ホストタイプ	ホストのタイプを選択します。 • ウィンドウ • Linux Plug-in for IBM DB2はIBM DB2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が適切に設定されているかどうか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。

フィールド	操作
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]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。

   REST APIを使用してPlug-in for DB2をインストールする場合は、バージョンを3.0として渡す必要があります。例：DB2：3.0

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	操作
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 IBM DB2はIBM DB2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	操作
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。
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	Windowsホストで、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$の形式で指定してください。 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。

   [インストール前チェックをスキップ]チェックボックスを選択していない場合は、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するためにホストが検証されます。 ディスクスペース、RAM、PowerShellのバージョン、 NETバージョン、場所（Windowsプラグインの場合）、およびJava 11（Windowsプラグインと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、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\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。

9. インストールの進行状況を監視します。
   - Windowsプラグインの場合、インストールログとアップグレードログは_C：\Windows\SnapCenter <JOBID>\にあります。
   - Linuxプラグインの場合、インストールログは_/var/opt/snapcenter/logs/SnapCenter *Linux_Host_Plug-in_Install_Install_Linux.log <JOBID>*にあり、アップグレードログ

は/var/opt/snapcenter/logs/SnapCenter <JOBID>.logにあります。

終了後

SnapCenter 6.0バージョンにアップグレードする場合は、既存のPerlベースのPlug-in for DB2がリモートプラグインサーバからアンインストールされます。

コマンドレットを使用した複数のリモートホストへの**SnapCenter Plug-in Package for Linux / Windows**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、複数のホストにSnapCenter Plug-in Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグインパッケージを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にログインしておく必要があります。

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。
4. 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 IBM DB2**をインストールする

SnapCenter Plug-in for IBM DB2 Databaseは、SnapCenterの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。ご使用の環境でSnapCenter UIからの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、コンソールモードまたはサイレントモードでPlug-in for IBM DB2 Databaseをインストールできます。

開始する前に

- Plug-in for IBM DB2 Databaseは、IBM DB2クライアントが配置されている各Linuxホストにインストールする必要があります。
- SnapCenter Plug-in for IBM DB2 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、および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"

- SnapCenter Plug-in for IBM DB2 Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

タスクの内容

パラメータが指定されていない場合、SnapCenterはデフォルト値でインストールされます。

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Plug-in for IBM DB2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. /<installation directory>/NetApp/snapcenter/scc/etc/SC _ SMS_Services.propertiesファイルを編集し、plugins_enabled=DB2：3.0パラメータを追加します。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenterサーバにホストを追加します。

   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 IBM DB2のインストールステータスの監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストのプラグインサービスとバインドします。

```
> $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ホスト上の**SnapCenter IBM DB2 Plug-ins**サービスの**CA**証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中の**CA**署名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ます。

カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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を含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

手順

1. カスタムプラグインキーストア/opt/NetApp/snapcenter/scc/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

6. 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キーストアに含まれていることを確認

します。

7. CA証明書に追加し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SCC_CERTIFICATE_ALIASキーに対して更新します。

8. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（CRL）を設定する

タスクの内容

- 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で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/scc/etc/crl」です。

手順

1. crl_pathキーに対して、agent.propertiesファイルのデフォルトディレクトリを変更および更新できます。

   このディレクトリには、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

Windowsホスト上のSnapCenter IBM DB2 Plug-insサービス用のCA証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中のCA署名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。

4. パスワードを変更したら、サービスを再起動します。

   カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   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ます。

   ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

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一覧表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   keytool -list -v キーストア *.JKS*

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルのキーkeystore_passの値です。

   *keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

8. *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SCC_CERTIFICATE_ALIASキーに対して更新します。

9. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（**CRL**）を設定する

タスクの内容

- 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で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は、複数のCRLファイルを配置できます。

受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for IBM DB2を使用するための前提条件

SnapCenter Plug-in for IBM DB2を使用する前に、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。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

  Javaのパスは、ホストマシンの環境パス変数で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な場合は、SnapMirrorとSnapVaultをセットアップします。

IBM DB2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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- 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IBM DB2データベースです。
- 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できます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを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、そのグループのポリシーを1つ以上選択します。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にも、ポリシーを選択できます。

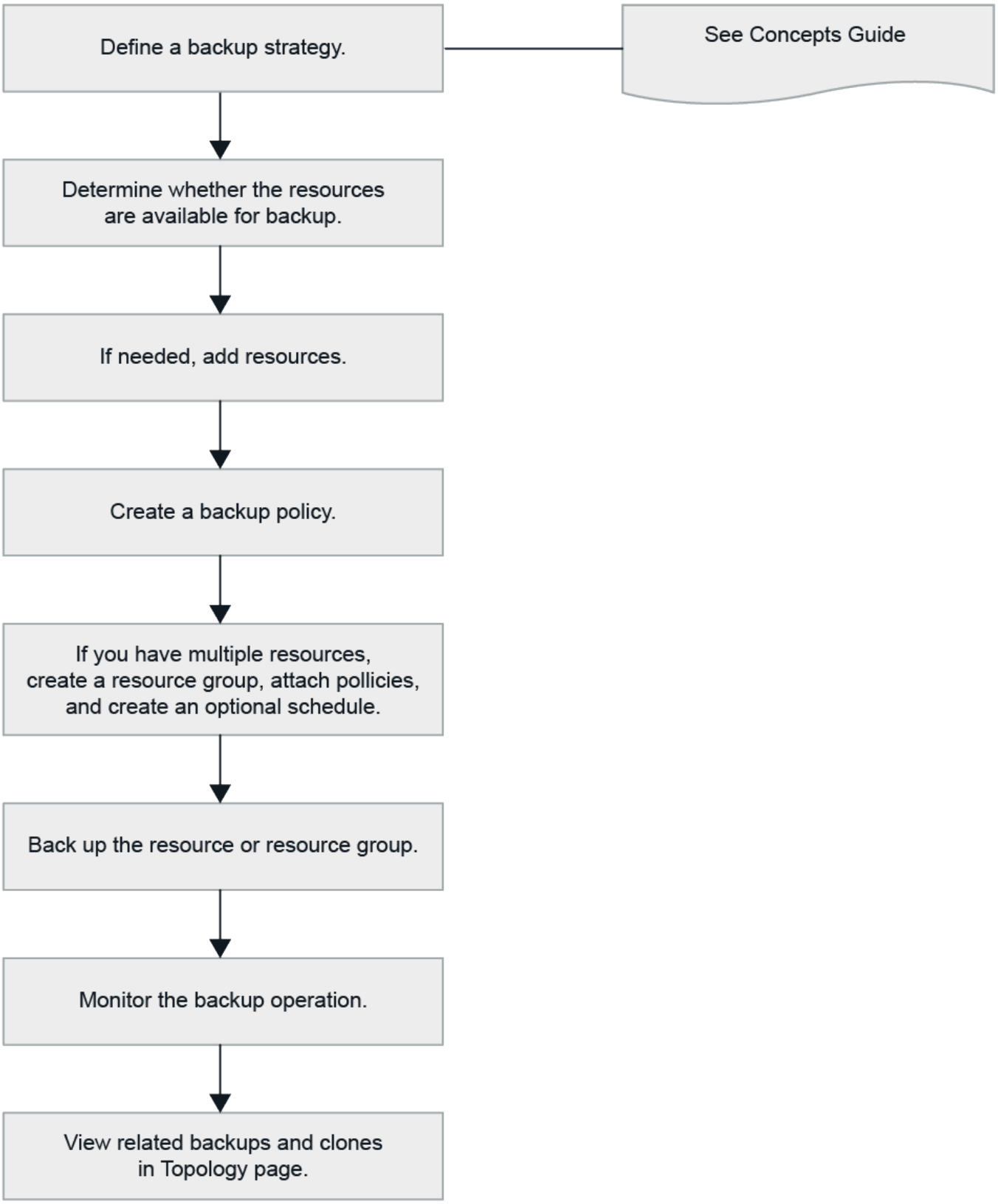
リソースグループは、保護する対象と保護するタイミング（日時）を定義するものと考えてください。ポリシーは、保護方法を定義するものと考えてください。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソースグループを作成します。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。リソースグループを作成してポリシーを適用する際に、フルバックアップを毎日実行するようにリソースグループを設定できます。

IBM DB2リソースのバックアップ

IBM DB2リソースのバックアップ

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。https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenter ソフトウェアコマンドレットリファレンスガイド"^]です。

データベースの自動検出

リソースとは、SnapCenterで管理されるLinuxホスト上のIBM DB2データベースです。使用可能なIBM DB2データベースを検出したあとに、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。

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セットアップなどのタスクを完了しておく必要があります。
- SnapCenter Plug-in for IBM DB2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ていません。データベースを手動で追加する際に、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。

タスクの内容

- 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。
- 自動検出されるのはデータベースだけです。

自動検出されたリソースを変更または削除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、*[リソース]*をクリックし、リストからPlug-in for IBM DB2を選択します。
2. [Resources]ページで、[View]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、ホスト名を選択します。

   次に、**をクリックしてフィルタペインを閉じることができます。

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NetAppストレージにあり、保護されていない場合は、[全体のステータス]列に「保護されていません」と表示されます。
   - データベースがNetAppストレージシステム上にあり保護されていて、実行されたバックアップ処理がない場合は、[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。

SnapCenter以外でデータベースの名前が変更された場合は、リソースを更新する必要があります。

プラグインホストに手動でリソースを追加する

自動検出はWindowsホストではサポートされていません。DB2インスタンスとデータベースリソースは手動で追加する必要があります。

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セットアップなどのタスクを完了しておく必要があります。

タスクの内容

手動検出は、次の構成ではサポートされません。

- RDMとVMDKのレイアウト

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、ドロップダウンリストからSnapCenter Plug-in for IBM DB2を選択します。
2. [リソース]ページで、*[IBM DB2リソースの追加]*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	操作
名前	データベース名を指定します。
ホスト名	ホスト名を入力します。
タイプ	データベースまたはインスタンスを選択します。
インスタンス	データベースの親であるインスタンスの名前を指定します。
クレデンシャル	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージフットプリントの入力]ページで、ストレージタイプを選択して1つ以上のボリューム、LUN、およびqtreeを選択し、*[保存]*をクリックします。

   オプション：*アイコンをクリックすると、他のストレージシステムからボリューム、LUN、およびqtreeを追加できます  。

5. オプション：[Resource Settings]ページで、WindowsホストのリソースにIBM DB2プラグインのカスタムのキーと値のペアを入力します。
6. 概要を確認し、 [完了] をクリックします。

   データベースは、ホスト名、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。

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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

"ユーザまたはグループを追加してロールとアセットを割り当てる"

データベースを追加したら、IBM DB2データベースの詳細を変更できます。

IBM DB2のバックアップポリシーの作成

SnapCenterを使用してIBM DB2リソースをバックアップする前に、バックアップする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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

  詳細については、IBM DB2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。

- 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、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おく必要があります。
- Snapshot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の両方に対応する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。

  また、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ポリシーで指定することもできます。これらのオプションを使用することで、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できます。

タスクの内容

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されなくなります。その結果、ポリシーで指定された数よりも多くのSnapshotが保持される可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

> プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

手順

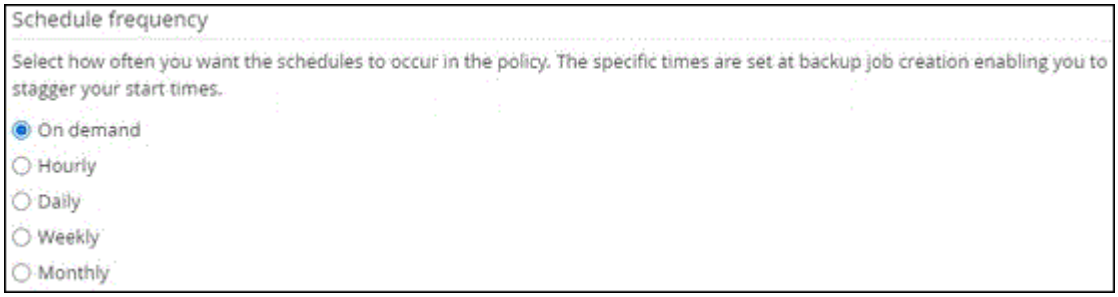
1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. [Policy type]ページで、次の手順を実行します。
   a. ストレージタイプを選択します。

b. [* 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値は複数指定できます。

6. [Snapshot]ページで、* on demand 、 Hourly 、 Daily 、 Weekly 、または Monthly *を選択してスケジュールタイプを指定します。

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、終了日、頻度）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ている場合、夏時間（DST）中はスケジュールはトリガーされません。

7. [Snapshot settings]セクションで、保持するSnapshotの数を指定します。

状況	作業
一定数のSnapshotを保持	[保持するコピー数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshotが削除されます。

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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。

8. [Retention and backup]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。
9. 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、バックアップおよび保護するリソースを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。また、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必要があります。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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、 [* 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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名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。

   これは、画面上の情報をフィルタリングするのに役立ちます。

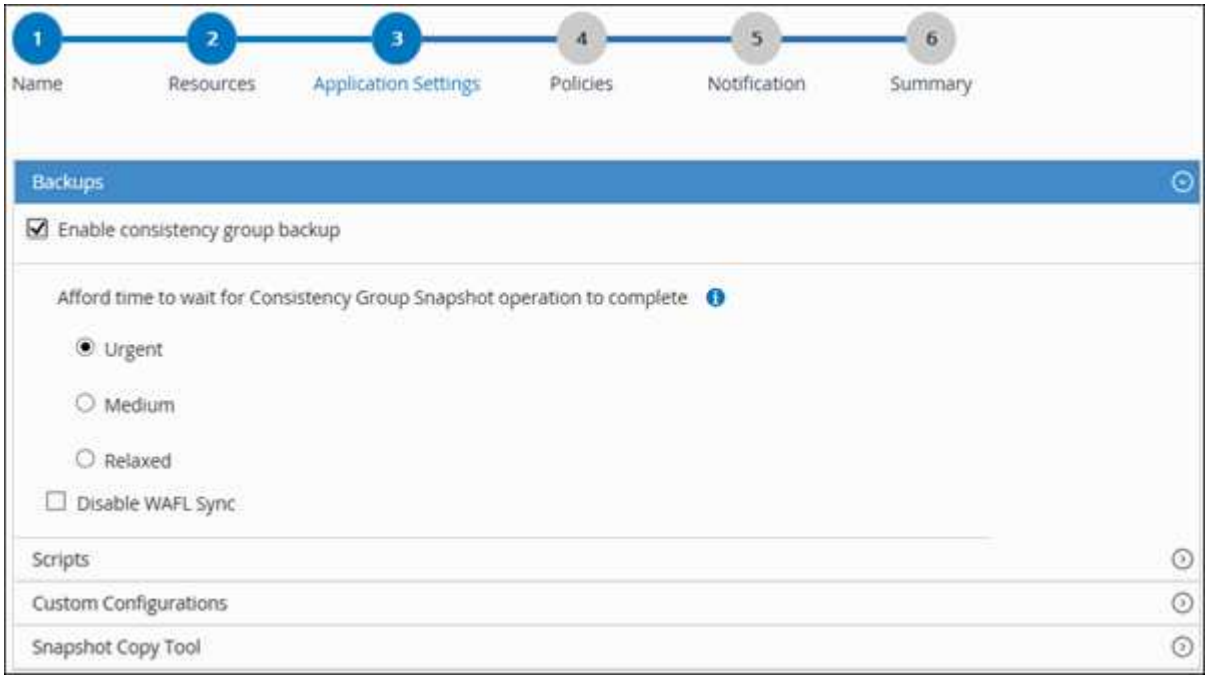
5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。
6. [アプリケーションの設定] ページで、次の操作を行います。

   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、次のタスクを実行します。

フィールド	操作
整合グループのSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+



a. [Scripts]*の矢印をクリックし、休止、Snapshot、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. [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	（Y/N）	アーカイブログ管理でアーカイブログを削除できます。
アーカイブログの保持	日数	アーカイブログを保持する日数を指定します。 この設定はNTAP_SNAPSHOT_RETENTIONS 以上である必要があります。

パラメータ	設定	説明
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。
ARCHIVE_LOG_EXT	ファイル拡張子	アーカイブログファイルの拡張子の長さを指定します。 たとえば、アーカイブログが LOG_BACKUP _0_0_0_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

カスタムのキーと値のペアは、IBM DB2 Linuxプラグインシステムでサポートされ、一元化されたWindowsプラグインとして登録されたIBM DB2データベースではサポートされません。

c. Snapshotコピーツール*の矢印をクリックして、スナップショットを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、スナップショットを作成する前にファイルシステムを整合性のある状態にします。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。
SnapCenter：ストレージレベルのSnapshotを作成	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します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。

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 。

ポリシーが[Configure schedules for selected policies]セクションに表示されます。

b. [スケジュールの設定]列で、設定するポリシーの**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。

サードパーティの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はサポートされません。

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 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、 [完了] をクリックします。

DB2データベースのバックアップ

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、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い、バックアップを実行します。

開始する前に

- 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であることを確認してください。
- 休止、Snapshot、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の場合は、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用でき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.config*

Linuxの場合：*/var/opt/snapcenter/scc/allowed _ commands.config*

ⓘ コマンドがコマンドリストに存在しない場合、処理は失敗します。

SnapCenter UI

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。

   *を選択し、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。その後、を選択してフィルタペインを閉じることができます 。
3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名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。

   ◦ [Backups]*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。

   必要に応じて整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

   ◦ [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

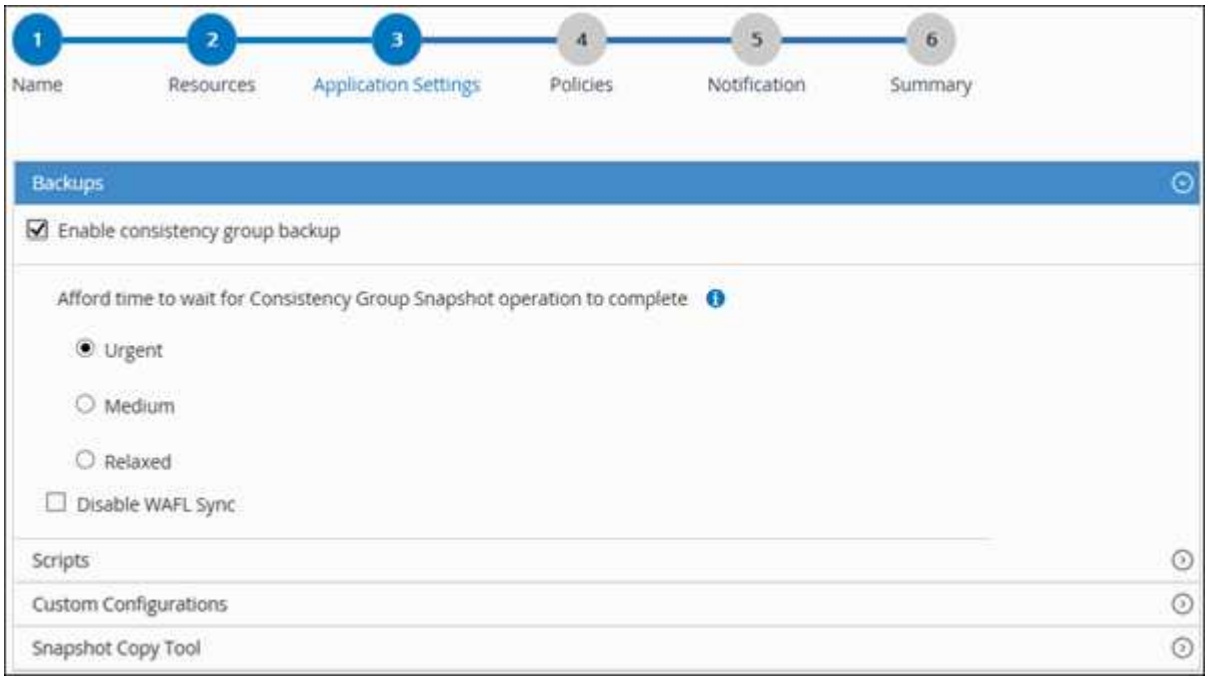
   バックアップ処理を終了する前にPREコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

   ◦ [**Custom Configurations**]矢印を選択し、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*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * 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を作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshot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。

   b. 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]列で**を選択します + 。

   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、*[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。

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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。

   リソーストポロジページが表示されます。

9. [今すぐバックアップ]*を選択します。
10. 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    b. 「 * Backup * 」を選択します。
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。
    ◦ MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

      詳細については、次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関係を検出できない"

PowerShellコマンドレット

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。

```
PS C:\> Open-SmConnection
```

   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、手動でリソースを追加します。

   次に、IBM DB2インスタンスを追加する例を示します。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\"
```

   DB2データベースの場合：

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

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。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソースグループを追加します。
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します。

   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_Db2_Resources' -Policy db2_policy1
   ```

   次に、DB2インスタンスをバックアップする例を示します。

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
   db2_policy
   ```

   次に、DB2データベースをバックアップする例を示します。

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDB";"PluginName"="DB2"
   } -Policy db2_policy
   ```

6. 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、失敗）を監視します。

```
PS C:\> Get-SmJobSummaryReport -JobId 467

SmJobId             : 467
JobCreatedDateTime :
JobStartDateTime    : 27-Jun-24 01:40:09
JobEndDateTime      : 27-Jun-24 01:41:15
JobDuration         : 00:01:06.7013330
JobName             : Backup of Resource Group
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
'snapshot-based-db2'
JobDescription      :
Status              : Completed
IsScheduled         : False
JobError            :
JobType             : Backup
PolicyName          : db2_policy
JobResultData       :
```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップID、バックアップ名などのバックアップジョブの詳細を監視します。

```
PS C:\> Get-SmBackupReport -JobId 467

BackedUpObjects           : {WINCIR}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 84
SmJobId                   : 467
StartDateTime             : 27-Jun-24 01:40:09
EndDateTime               : 27-Jun-24 01:41:15
Duration                  : 00:01:06.7013330
CreatedDateTime           : 27-Jun-24 18:39:45
Status                    : Completed
ProtectionGroupName       : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId       : 23
PolicyName                : db2_policy
SmPolicyId                : 13
BackupName                : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DB2
PluginDisplayName         : IBM DB2
JobTypeId                 :
JobHost                   : HOSTFQDN
```

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"。

リソースグループのバックアップ

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に対して実行されます。

開始する前に

- ポリシーを適用して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。

タスクの内容

リソースグループは、[Resources]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、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。

   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、を選択し、タグを選択します。その後、を選択してフィルタペインを閉じることができます 。
3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。
   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

IBM DB2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する

PowerShellコマンドレットを使用してIBM DB2データベースをバックアップ、リストア、またはクローニングするには、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。

開始する前に

- 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. [SnapCenterPS]*をクリックしてPowerShell Coreを起動します。
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 -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -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。

   次に、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例を示します。

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux
-AuthenticationType PasswordBased -Credential db2hostuser
-EnableSudoPrevileges:$true
```

4. IBM DB2通信ホストをSnapCenterサーバに追加します。

   Linuxの場合：

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

   Windowsの場合：

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. パッケージとSnapCenter Plug-in for IBM DB2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' -PluginCodes
DB2
```

   Windowsの場合：

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2,SCW
```

6. SQLLIBへのパスを設定します。

   Windowsの場合、DB2プラグインはSQLLIBフォルダのデフォルトパス「C：\Program Files\IBM\SQLLIB\bin」を使用します。

   デフォルトのパスを上書きする場合は、次のコマンドを使用します。

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
```

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"。

バックアップ処理の監視

IBM DB2バックアップ処理の監視

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。

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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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、**IBM DB2**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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

IBM DB2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 *
- 操作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、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。

アクセス元	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。
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックして、最新の5つの処理を表示します。 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]ページでのIBM DB2のバックアップとクローンの表示

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ときに、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立つことがあります。

タスクの内容

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-  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。
-  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、バックアップを4つだけ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。

[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、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、Snapshotコピーベースのバックアップとクローン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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

   オンデマンドバックアップのあと、*[リフレッシュ]*ボタンをクリックすると、バックアップまたはクローンの詳細がリフレッシュされます。
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、削除の各処理を実行します。

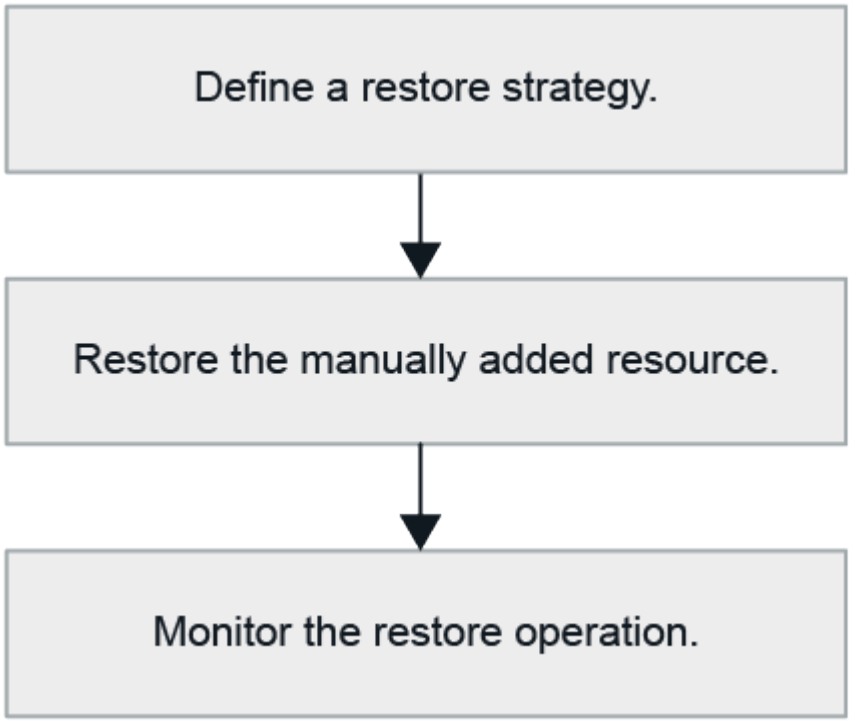
   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。
8. クローンをスプリットする場合は、テーブルでクローンを選択し、をクリックします 。

IBM DB2のリストア

リストアのワークフロー

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"です。

手動で追加したリソースバックアップのリストア

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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.config*

Linuxの場合：*/opt/NetApp/snapcenter/scc/etc/allowed _ commands.config*

コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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。

   リソースがタイプ、ホスト、関連す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。

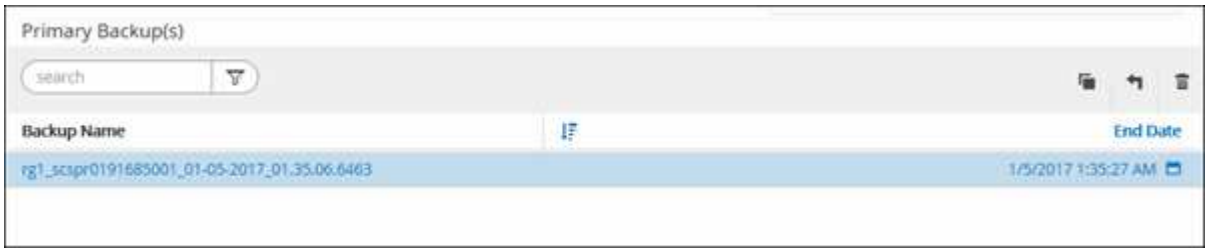
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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
   。



6. [Restore Scope]ページで、*[Complete Resource]*を選択します。

   a. [Complete Resource]*を選択すると、IBM DB2データベースの設定済みデータボリュームがすべてリストアされます。

      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のあとに作成されたSnapshot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。

      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。

7. [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。
8. [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。

   休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

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。

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。

終了後

ロールフォワードステータスが「DB PENDING」の場合にのみリカバリが可能です。このステータスは、アーカイブログが有効なDB2データベースに適用されます。

PowerShellコマンドレット

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。

   ```
   PS C:\> Open-SmConnection
   ```

2. Get-SmBackupコマンドレットおよび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、リストアに使用できるバックアップが2つあります。

```
 PS C:\> Get-SmBackup -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\Library

        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情報を表示しています。

```
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. 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 =<instance_name>は手動で検出されたインスタンスリソースの場合、UID =<instance_name>\<databse_name>はIBM DB2データベースリソースの場合です。ResourceIDは、Get-smResourcesコマンドレットで取得できます。

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode DB2
```

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 DB2 -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -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 'DB2' -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

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"。

自動検出されたデータベースバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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.config*

  Linuxの場合：*/opt/NetApp/snapcenter/scc/etc/allowed _ commands.config*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- 自動検出されたリソースについては、SFSRでリストアがサポートされます。
- 自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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。

   リソースがタイプ、ホスト、関連す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。

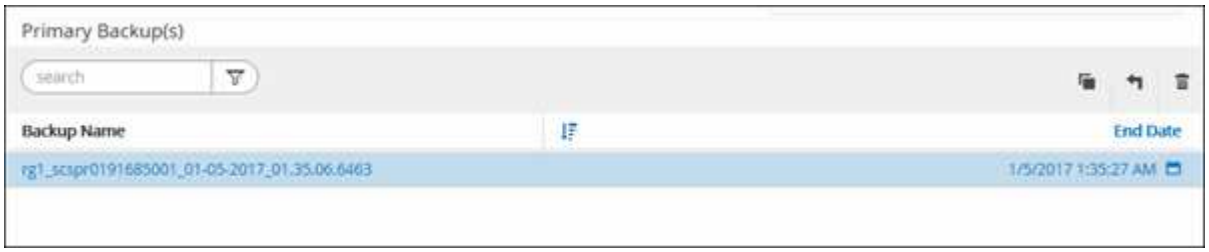
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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 。



6. [Restore Scope]ページで*[Complete Resource]*を選択し、IBM DB2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。
7. [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は必要ありません。

8. [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はマウントコマンドは必要ありません。

   休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path 、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

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。

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。

終了後

ロールフォワードステータスが「DB PENDING」の場合にのみリカバリが可能です。このステータスは、アーカイブログが有効なDB2データベースに適用されます。

IBM DB2リストア処理の監視

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

IBM DB2リソースバックアップのクローニング

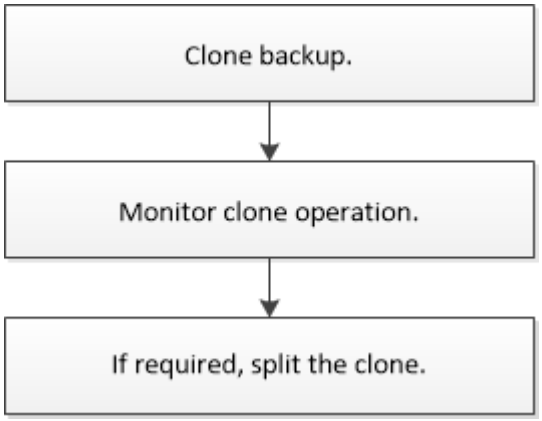
クローニングのワークフロー

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。

タスクの内容

- クローンは、ソースIBM DB2サーバ上で作成できます。
- 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
  - データウェアハウスにデータを取り込む際のデータ抽出および操作ツール用
  - 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。

終了後

自動検出されたDB2リソースをクローニングすると、クローニングされたリソースは手動リソースとしてマークされます。クローンDB2リソースをリカバリするには、*[リソースをリフレッシュ]*をクリックします。クローンを削除すると、ストレージとホストもクリーンアップされます。

クローン処理後にリソースを更新せずにクローンを削除しようとすると、ストレージとホストはクリーンアップされません。fstabでエントリを手動で削除する必要があります。

IBM DB2バックアップのクローニング

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。

開始する前に

- 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）の割り当て済みアグリゲートリストに含まれている必要があります。
- クローニング前またはクローニング後のコマンドについては、次のパスからプラグインホストで使用できるコマンドリストにコマンドが存在す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.config*

  Linuxの場合：*/opt/NetApp/snapcenter/scc/etc/allowed _ commands.config*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- 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"。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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. Location ページで、次のアクションを実行します。

フィールド	操作
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。
ターゲットのクローンインスタンス	既存のバックアップからクローニングするターゲットDB2クローンインスタンスIDを入力します。 これは、ANFストレージタイプのリソースにのみ該当します。
ターゲットクローン名	クローンの名前を入力します。 これは、DB2データベースリソースにのみ適用されます。
NFSエクスポートIPアドレス	クローンボリュームをエクスポートするホスト名またはIPアドレスを入力します。 これは、NFSストレージタイプリソースにのみ該当します。
容量プール最大 スループット（MiB/秒）	容量プールの最大スループットを入力します。

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の削除
   - 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. mountコマンドを入力して、ファイルシステムをホストにマウントします。

   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
```

休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

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。

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。

終了後

自動検出されたDB2リソースをクローニングすると、クローニングされたリソースは手動リソースとしてマークされます。クローンDB2リソースをリカバリするには、*[リソースをリフレッシュ]*をクリックします。クローンを削除すると、ストレージとホストもクリーンアップされます。

クローン処理後にリソースを更新せずにクローンを削除しようとすると、ストレージとホストはクリーンアップされません。fstabでエントリを手動で削除する必要があります。

PowerShellコマンドレット

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一覧を表示します。

次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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します。

   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、クローン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"。

IBM DB2のクローニング処理の監視

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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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する

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[表示] リストから [*Database] を選択します。

オプション	説明
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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングまたは検証が失敗する"

SnapCenterのアップグレード後にIBM DB2データベースクローンを削除またはスプリットする

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。クローンを作成したリソースの[Topology]ページで、クローンを削除したり、クローンをスプリットしたりできます。

タスクの内容

非表示のクローンのストレージフットプリントを特定するには、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、クローニングされ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。

   リソーストポロジページが表示されます。
5. [Manage Copies]ビューで、プライマリまたはセカンダリ（ミラーリング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、をクリックしてクローンを削除するか、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。

PostgreSQLの保護

PostgreSQL向けSnapCenterプラグイン

SnapCenter Plug-in for PostgreSQLの概要

SnapCenter Plug-in for PostgreSQLクラスタは、PostgreSQLクラスタに対する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。Plug-in for PostgreSQLクラスタは、SnapCenter環境でのPostgreSQLクラスタのバックアップ、リストア、クローニングを自動化します。

SnapCenterは、単一クラスタとマルチクラスタのPostgreSQLセットアップをサポートしています。Plug-in for PostgreSQL Clustersは、Linux環境とWindows環境の両方で使用できます。Windows環境では、PostgreSQLは手動リソースとしてサポートされます。

Plug-in for PostgreSQLクラスタがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジを使用して、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、本プラグインをNetApp SnapVaultテクノロジとともに使用して、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 PostgreSQLは、ONTAPおよびAzure NetAppのファイルストレージレイアウトでNFSとSANをサポートします。

VMDKまたは仮想ストレージレイアウトがサポートされます。

SnapCenter Plug-in for PostgreSQLの使用方法

Plug-in for PostgreSQLクラスタを環境にインストールすると、SnapCenterを使用して、PostgreSQLクラスタとそのリソースをバックアップ、リストア、および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。

- クラスタを追加
- 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します。
- 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 PostgreSQLの機能

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 PostgreSQL Clusterを操作するには、SnapCenterグラフィカルユーザー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

  SnapCenterでは、Plug-in for PostgreSQLクラスタでNetAppのSnapshot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 PostgreSQLを使用すると、次のようなメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます。
- RBACでサポートされるセキュリティと一元化されたロール委譲

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルの権限を付与することもできます。

- NetApp FlexCloneテクノロジを使用して、テストまたはデータ抽出に使用するリソ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できます。

  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。

- バックアップ作成時にONTAPの整合グループ（CG）Snapshot機能がサポートされるようになりました。
- 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可能

  1回の操作で、1つのホスト内のリソースが同じボリュームを共有すると、スナップショットが統合されます。

- 外部コマンドを使用してスナップショットを作成する機能。
- XFSファイルシステムでのLinux LVMのサポート。

SnapCenter Plug-in for PostgreSQL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 PostgreSQL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こと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セツソクLUN

マシン	ストレージタイプ
物理サーバ	iSCSIセツソクLUN
物理サーバと仮想サーバ	NFS接続ボリューム

PostgreSQL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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN
  - LUNの作成
  - LUNの作成
  - LUNの作成
  - lun delete
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード
  - LUNマッピングの作成
  - LUNマッピングの削除
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - LUN変更
  - ボリューム内でのLUNの移動
  - LUNオフライン
  - LUNオンライン
  - LUN永続的予約のクリア
  - LUNのサイズ変更

- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- volume snapshot modify -snaplock-expiry-time
- ボリュームSnapshotの名前変更

- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限
  - ネットワークインターフェイス
  - network interface show
  - SVM

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**PostgreSQL**向けに準備する

SnapCenterプラグインとONTAP SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

PostgreSQLのバックアップ戦略

PostgreSQLのバックアップ戦略を定義

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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

タスクの内容

SLAは、期待されるサービスレベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要がある時間です。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ます。SLA、RTO、RPOは、データ保護戦略に影響します。

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. クラスタのアプリケーションと整合性のあるSnapshotをバックアップするためにSnapshotコピーベースのポリシーを作成するかどうかを決定します。
5. レプリケーションにNetApp SnapMirrorテクノロジを使用するか、長期保持にNetApp SnapVaultテクノロジを使用するかを決定します。
6. ソースストレージシステムとSnapMirrorデスティネーションでのSnapshotの保持期間を決定します。
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。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterによって管理されるLinuxホスト上のPostgreSQLクラスタとインスタンスです。SnapCenter Plug-in for PostgreSQL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インスタンスのPostgreSQLクラスタが自動的に検出され、[Resources]ページに表示されます。

サポートされるバックアップのタイプ

Backup typeには、作成するバックアップのタイプを指定します。SnapCenterでは、PostgreSQLクラスタに対してSnapshotコピーベースのバックアップタイプがサポートされます。

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テクノロジを利用して、PostgreSQLクラスタが配置されているボリュームのオンラインの読み取り専用コピーを作成します。

SnapCenter Plug-in for PostgreSQLでの整合グループ**Snapshot**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性グループのSnapshotを作成できます。整合グループはコンテナであり、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。整合グループは、複数のボリュームの同時Snapshotであり、ボリュームグループの整合性のあるコピーを提供します。

ストレージコントローラが整合性のあるSnapshotをグループ化するまでの待機時間を指定することもできます。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の処理中に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の同期により、整合性グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なデータバックアップの削除の管理方法

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データバックアップの削除を管理します。

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上のSnapshotと、PostgreSQLカタログ内の対応するエントリが削除されます。

PostgreSQL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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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つの部分があります。

- 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タイミング）

  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単位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。

PostgreSQL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には、リソースのサイズ、使用されているボリュームの数、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 PostgreSQLクラスタのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

PostgreSQLのリストアおよびリカバリ戦略

PostgreSQLリソースのリストアおよびリカバリ戦略の定義

クラスタのリストアとリカバリを実行する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。

クラスタの手動リカバリのみがサポートされます。

手順

1. 手動で追加したPostgreSQLリソースでサポートされているリストア戦略を確認する
2. 自動検出されたPostgreSQLクラスタでサポートされているリストア戦略を確認する

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**PostgreSQL**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、戦略を定義する必要があります。

手動で追加したPostgreSQLリソースは回復できません。

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

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のあとに作成されたSnapshotは削除され、リカバリできません。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。

注：Plug-in for PostgreSQLでは、手動でのリカバリに役立つように、_/<OS_temp_folder>/<Restore_JobId>/_フォルダにbackup_labelとtablespace_mapが作成されます。

自動検出された**PostgreSQL**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、戦略を定義する必要があります。

完全なリソースリストアは、自動的に検出されたPostgreSQLクラスタに対してサポートされるリストア戦略です。これにより、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

自動検出された**PostgreSQL**のリストア処理のタイプ

SnapCenter Plug-in for PostgreSQLは、自動的に検出されたPostgreSQLクラスタに対して、Single File SnapRestoreおよびConnect-and-Copyリストアタイプをサポートしています。

NFS環境で**Single File SnapRestore**を実行するシナリオは、次のとおりです。

- [Complete Resource]オプションのみが選択されている場合
- 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。

- [Complete Resource]オプションのみが選択されている場合
- 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

PostgreSQLクラスタ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、PostgreSQLクラスタに対してさまざまな種類のリカバリ操作を実行できます。

- クラスタを最新の状態までリカバリします。
- 特定のポイントインタイムまでクラスタをリカバリします。

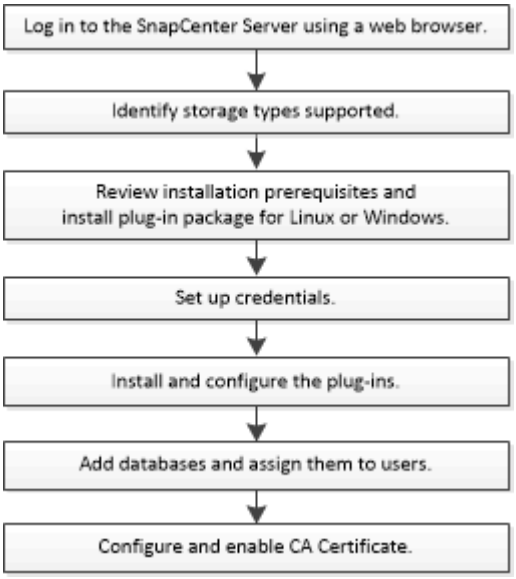
  リカバリの日時を指定する必要があります。

SnapCenterには、PostgreSQLクラスタ用のNo recoveryオプションも用意されています。

SnapCenter Plug-in for PostgreSQLのインストールの準備

SnapCenter Plug-in for PostgreSQLのインストールワークフロー

PostgreSQLクラスタを保護する場合は、SnapCenter Plug-in for PostgreSQL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 PostgreSQL**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 PostgreSQLは、WindowsとLinuxの両方の環境で使用できます。

- Java 11をホストにインストールしておく必要があります。

  IBM Javaはサポートされていません。

- Windowsの場合、Plug-in CreatorサービスはWindowsユーザ「LocalSystem」を使用して実行する必要が

あります。これは、Plug-in for PostgreSQL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ホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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PostgreSQLプラグインとともにデフォルトで導入されます。
- SnapCenter ServerがPlug-in for PostgreSQL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Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- Plug-in for PostgreSQLをWindowsホストにインストールすると、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以外のユーザに対して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 11をWindowsホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

Linuxホスト

- rootユーザまたはroot以外のユーザに対して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 11をLinuxホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

- Linuxホストで実行されているPostgreSQLクラスタの場合は、Plug-in for PostgreSQLのインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- 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。

補助コマンド

SnapCenter Plug-in for PostgreSQLで補助コマンドを実行するには、ファイルにコマンドを含める必要があります `allowed_commands.config` 。

`allowed_commands.config` ファイルはSnapCenter Plug-in for PostgreSQLディレクトリの「etc」サブディレクトリにあります。

Windowsホスト

デフォルト： `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

カスタムパス： `<Custom_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Linuxホスト

デフォルト： `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

カスタムパス： `<Custom_Directory>allowed_commands.config`

プラグインホストで追加のコマンドを許可するには、エディタでファイルを開きます `allowed_commands.config` 。各コマンドを別 々 の行に入力します。大文字と小文字は区別されません。例えば、

コマンド:mount

コマンド：umount

完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符（"）で囲みます。例えば、

コマンド："C：\Program Files\NetApp\SnapCreator commands\sdcli.exe"

コマンド：myscript.bat

ファイルが存在しない場合は `allowed_commands.config` 、コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

コマンドまたはスクリプトがに存在しないと、 `allowed_commands.config`コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

ワイルドカードエントリ（*）を使用してすべてのコマンドを許可しないでください。

Linuxホストの**root**以外のユーザに対する**sudo Privileges**の設定

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をroot以外の有効なユーザとして実行します。複数のパスにアクセスできるようにroot以外のユーザにsudo Privileges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
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- /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。

構成ファイルの更新後に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/installation/plugins/uninstall
- /custom_location /NetApp/snapcenter/spl/bin/spl
- 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_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- _C：\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt（SnapCenter ServerがWindowsホストにインストールされている場合）。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc _ unix_plugins_checksum.txt _ LinuxホストにSnapCenterサーバがインストールされている場合。

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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• DOTNETコア8.0.5 • PowerShell Core 7.4.2 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、基本的なホストシステムのスペースとサイジングの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 • 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB

項目	要件
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量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、最近実行した処理の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 11 Oracle JavaおよびOpenJDK を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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 "NetApp Interoperability Matrix Tool" ください。

SnapCenter Plug-in for PostgreSQLのクレデンシャルを設定する

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、クラスタまたは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クレデンシャルをそれぞれ作成する必要があります。

タスクの内容

- Linuxホスト

  Linuxホストにプラグインをインストールするには、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、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo Privilegesがあるroot以外のユーザに対して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

  プラグインをインストールする前にWindows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には、管理者権限（リモートホストに対する管理者権限を含む）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、ユーザ名に完全なadmin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の権限を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、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	操作
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。ユーザ名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。

フィールド	操作
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	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ユーザのみに適用されます。

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、必要に応じて[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を割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
. . コンピュータオブジェクトをグループに追加します。
. . 作成したユーザグループを使用してgMSAを作成します。
```

例えば、

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
. . コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。
```

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。

6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

SnapCenter Plug-in for PostgreSQLのインストール

ホストを追加してリモートホストにプラグインパッケージをインストールする

SnapCenterの[ホストを追加]ページを使用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。プラグインはリモートホストに自動的にインストールされます。ホストを追加して、個 々 のホスト用のプラグインパッケージをインストールできます。

開始する前に

- SnapCenter Serverホストのオペレーティングシステムが Windows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- 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、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストの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する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理Privilegesを使用してgMSAを設定する必要があります。

  "Windows Server 2016以降でPostgreSQL用にグループ管理サービスアカウントを設定する"

タスクの内容

- 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]*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	操作
ホストタイプ	ホストのタイプを選択します。 • ウィンドウ • Linux Plug-in for PostgreSQL はPostgreSQL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システムとLinuxシステムのどちらにも配置できます。
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が適切に設定されているかどうか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。

フィールド	操作
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]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。

   REST APIを使用してPlug-in for PostgreSQLをインストールする場合は、バージョンを3.0に渡す必要があります。例：postgresql:3.0

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	操作
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 PostgreSQLはPostgreSQL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システムとLinuxシステムのどちらにも配置できます。 • 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。 • 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	操作
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。
クラスタ内のすべてのホストを追加	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オンにします。
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	Windowsホストで、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$の形式で指定してください。 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 prechecks]チェック ボックスを選択していない場合、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を検証するためにホストが検証されます。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）、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、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\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。

9. インストールの進行状況を監視します。

   - Windowsプラグインの場合、インストールログとアップグレードログは_C：\Windows\SnapCenter

<JOBID>にあります。

- Linuxプラグインの場合、インストールログは_/var/opt/snapcenter/logs/SnapCenter *Linux_Host_Plug-in_Install_Install_Linux.log*<JOBID>にあり、アップグレードログは_/var/opt/snapcenter/logs/SnapCenter <JOBID>.log_にあります。

コマンドレットを使用した複数のリモートホストへの**SnapCenter Plug-in Package for Linux / Windows**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、複数のホストにSnapCenter Plug-in Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグインパッケージを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にログインしておく必要があります。

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。
4. 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**SnapCenter Plug-in for PostgreSQL**を**Linux**ホストにインストールする

SnapCenter Plug-in for PostgreSQLクラスタは、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。ご使用の環境でSnapCenter UIからの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、コンソールモードまたはサイレントモードでPlug-in for PostgreSQLクラスタをインストールできます。

開始する前に

- Plug-in for PostgreSQLクラスタは、PostgreSQLクライアントが配置されているLinuxホストごとにインストールする必要があります。
- SnapCenter Plug-in for PostgreSQLクラスタをインストールするLinuxホストは、依存するソフトウェア、クラスタ、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"

- SnapCenter Plug-in for PostgreSQLクラスタは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

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Plug-in for PostgreSQL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. /<installation directory>/NetApp/snapcenter/scc/etc/SC _ SMS_Services.propertiesファイルを編集し、plugins_enabled=postgresql:3.0パラメータを追加します。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenterサーバにホストを追加します。

   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 PostgreSQLのインストールステータスの監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

```
> 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ホストのプラグインサービスとバインドします。
```

```
> $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ホスト上の**SnapCenter PostgreSQL Plug-in**サービス用の**CA**証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中の**CA**署名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ます。

> カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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を含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

手順

1. カスタムプラグインキーストア/opt/NetApp/snapcenter/scc/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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SCC_CERTIFICATE_ALIASキーに対して更新します。

8. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（CRL）を設定する

タスクの内容

- 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で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/scc/etc/crl」です。

手順

1. crl_pathキーに対して、agent.propertiesファイルのデフォルトディレクトリを変更および更新できます。

   このディレクトリには、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

Windowsホスト上のSnapCenter PostgreSQL Plug-inサービス用のCA証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中のCA署名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。

4. パスワードを変更したら、サービスを再起動します。

カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

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一覧表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   keytool -list -v キーストア *.JKS*

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルのキーkeystore_passの値です。

   *keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

8. *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SCC_CERTIFICATE_ALIASキーに対して更新します。

9. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（**CRL**）を設定する

タスクの内容

- 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で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は、複数のCRLファイルを配置できます。

   受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for PostgreSQLを使用するための前提条件

SnapCenter Plug-in for PostgreSQLを使用する前に、SnapCenter管理者がSnapCenter Server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。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

  Javaのパスは、ホストマシンの環境パス変数で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な場合は、SnapMirrorとSnapVaultをセットアップします。

PostgreSQLを保護するためのリソース、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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- リソースとは、SnapCenterでバックアップまたはクローニングするPostgreSQLクラスタのことです。
- 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できます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを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、そのグループのポリシーを1つ以上選択します。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、すべてのクラスタをバックアップする場合は、ホストのすべてのクラスタを含むリソースグループを作成します。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。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。

PostgreSQLリソースのバックアップ

PostgreSQLリソースのバックアップ

リソース（クラスタ）またはリソースグループのバックアップを作成できます。バックアップのワークフローには、計画、バックアップするクラスタの特定、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。

[PostgreSQLバックアップのワークフロー] | *../media/db2_backup_workflow.gif*

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。https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenter ソフトウェアコマンドレットリファレンスガイド"^]です。

クラスタの自動検出

リソースとは、SnapCenterで管理されるLinuxホスト上のPostgreSQLクラスタです。使用可能なPostgreSQLクラスタを検出したら、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。

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セットアップなどのタスクを完了しておく必要があります。
- SnapCenter Plug-in for PostgreSQL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ていません。

タスクの内容

- 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クラスタが自動的に検出されて[リソース]ページに表示されます。
- 自動検出されるのはクラスタのみです。

自動検出されたリソースを変更または削除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*[リソース]*をクリックし、リストからPlug-in for PostgreSQLを選択します。
2. [Resources]ページで、[View]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、ホスト名を選択します。

   次に、**をクリックしてフィルタペインを閉じることができます。

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。

   - クラスタがNetAppストレージに配置されていて保護されていない場合は、[全体のステータス]列に「保護されていません」と表示されます。
   - クラスタがNetAppストレージシステム上にあり保護されている場合、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。

SnapCenterの外部でクラスタの名前を変更した場合は、リソースを更新する必要があります。

プラグインホストに手動でリソースを追加する

自動検出はWindowsホストではサポートされていません。PostgreSQLクラスタリソースを手動で追加する必要があります。

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セットアップなどのタスクを完了しておく必要があります。

タスクの内容

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

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 PostgreSQLを選択し、*[リソース]*をクリックします。
2. [Resources]ページで、*[Add PostgreSQL resources]*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	操作
名前	クラスタ名を指定します。
ホスト名	ホスト名を入力します。
タイプ	クラスタを選択します。
インスタンス	クラスタの親であるインスタンスの名前を指定します。
クレデンシャル	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージフットプリントの入力]ページで、ストレージタイプを選択して1つ以上のボリューム、LUN、およびqtreeを選択し、*[保存]*をクリックします。

   オプション：*アイコンをクリックすると、他のストレージシステムからボリューム、LUN、およびqtreeを追加できます。

5. オプション：[Resource Settings]ページで、WindowsホストのリソースにPostgreSQLプラグインのカスタムのキーと値のペアを入力します。
6. 概要を確認し、 [完了] をクリックします。

   クラスタは、ホスト名、関連付けられてい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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

"ユーザまたはグループを追加してロールとアセットを割り当てる"

終了後

- クラスタを追加したら、PostgreSQLクラスタの詳細を変更できます。
- SnapCenter 5.0から移行されたリソース（表領域とクラスタ）は、SnapCenter 6.0ではPostgreSQLクラスタタイプとしてタグ付けされます。
- SnapCenter 5.0以前から移行された手動で追加したリソースを変更する場合は、カスタムキーと値のペアの*[リソースの設定]*ページで次の手順を実行します。
  - 「* Name *」フィールドに「port」という用語を指定します。
  - 「* value *」フィールドにポート番号を指定します。

PostgreSQLのバックアップポリシーの作成

SnapCenterを使用してPostgreSQL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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

  詳細については、PostgreSQLクラスタ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。

- データ保護の準備として、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おく必要があります。
- Snapshot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の両方に対応する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。

  また、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ポリシーで指定することもできます。これらのオプションを使用することで、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できます。

タスクの内容

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されなくなります。その結果、ポリシーで指定された数よりも多くのSnapshotが保持される可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

> プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

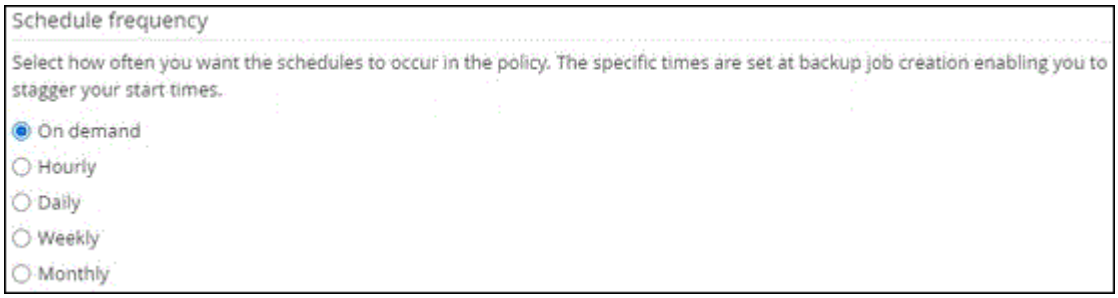
手順

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. [Policy type]ページで、次の手順を実行します。
   a. ストレージタイプを選択します。
   b. [* 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値は複数指定できます。
6. [Snapshot]ページで、* on demand 、 Hourly 、 Daily 、 Weekly 、または Monthly *を選択してスケジュールタイプを指定します。

   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、終了日、頻度）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ている場合、夏時間（DST）中はスケジュールはトリガーされません。
7. [Snapshot settings]セクションで、保持するSnapshotの数を指定します。
8. [Retention]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業
一定数のSnapshotを保持	[保持するコピー数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshotが削除されます。

   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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。

9. 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、バックアップおよび保護するリソースを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。また、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必要があります。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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、 [* 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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名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。

   これは、画面上の情報をフィルタリングするのに役立ちます。

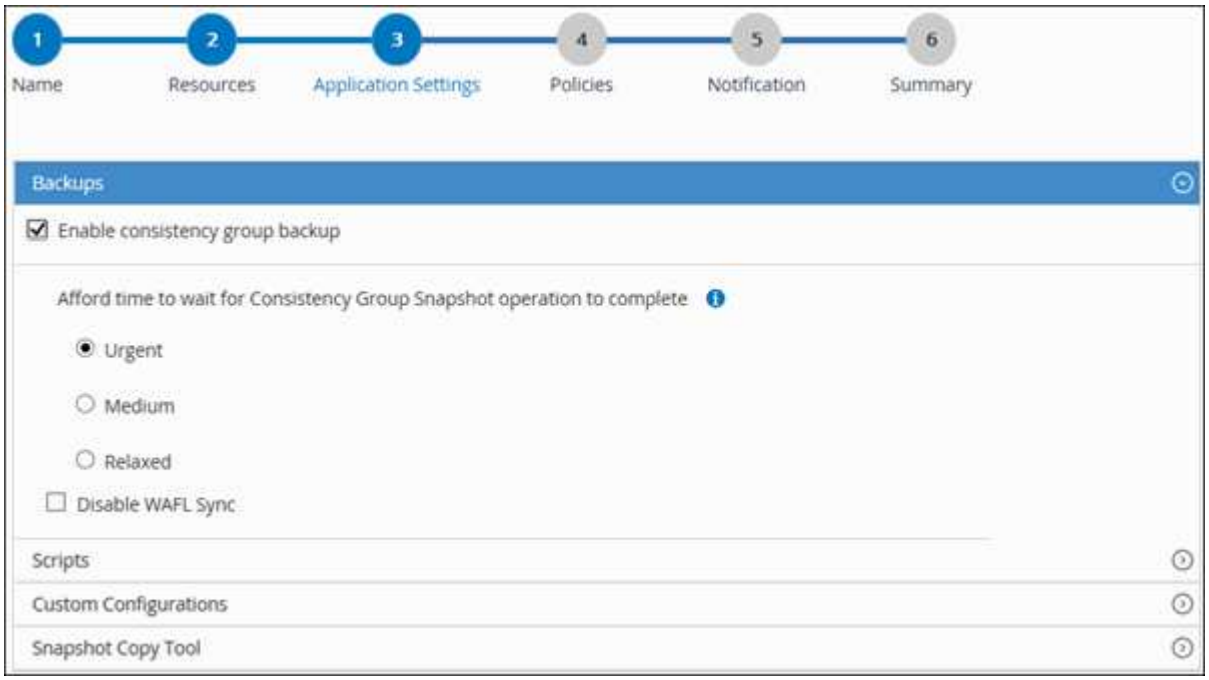
5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。
6. [アプリケーションの設定] ページで、次の操作を行います。

   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、次のタスクを実行します。

フィールド	操作
整合グループのSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+



   a. [Scripts]*の矢印をクリックし、休止、Snapshot、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. [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	（Y/N）	アーカイブログ管理でアーカイブログを削除できます。

パラメータ	設定	説明
アーカイブログの保持	日数	アーカイブログを保持する日数を指定します。 この設定は NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。
ARCHIVE_LOG_EXT	ファイル拡張子	アーカイブログファイルの拡張子の長さを指定します。 たとえば、アーカイブログが LOG_BACKUP _0_0_0_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

カスタムのキーと値のペアは、PostgreSQL Linuxプラグインシステムでサポートされ、一元化されたWindowsプラグインとして登録されたPostgreSQLクラスタではサポートされません。

c. Snapshotコピーツール*の矢印をクリックして、スナップショットを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、スナップショットを作成する前にファイルシステムを整合性のある状態にします。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。
SnapCenter：ストレージレベルのSnapshotを作成	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します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。

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 。

      ポリシーが[Configure schedules for selected policies]セクションに表示されます。

   b. [スケジュールの設定]列で、設定するポリシーの**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。

   サードパーティの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はサポートされません。

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 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、 [完了] をクリックします。

PostgreSQL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、のページからバックアップすることができます。

開始する前に

- 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、すべてのテナントクラスタが有効でアクティブであることを確認してください。
- 休止、Snapshot、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の場合は、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用でき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*

コマンドがコマンドリストに存在しない場合、処理は失敗します。

SnapCenter UI

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。

   *を選択し、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。その後、を選択してフィルタペインを閉じることができます 。
3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名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。

   ◦ [Backups]*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。

   必要に応じて整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

   ◦ [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

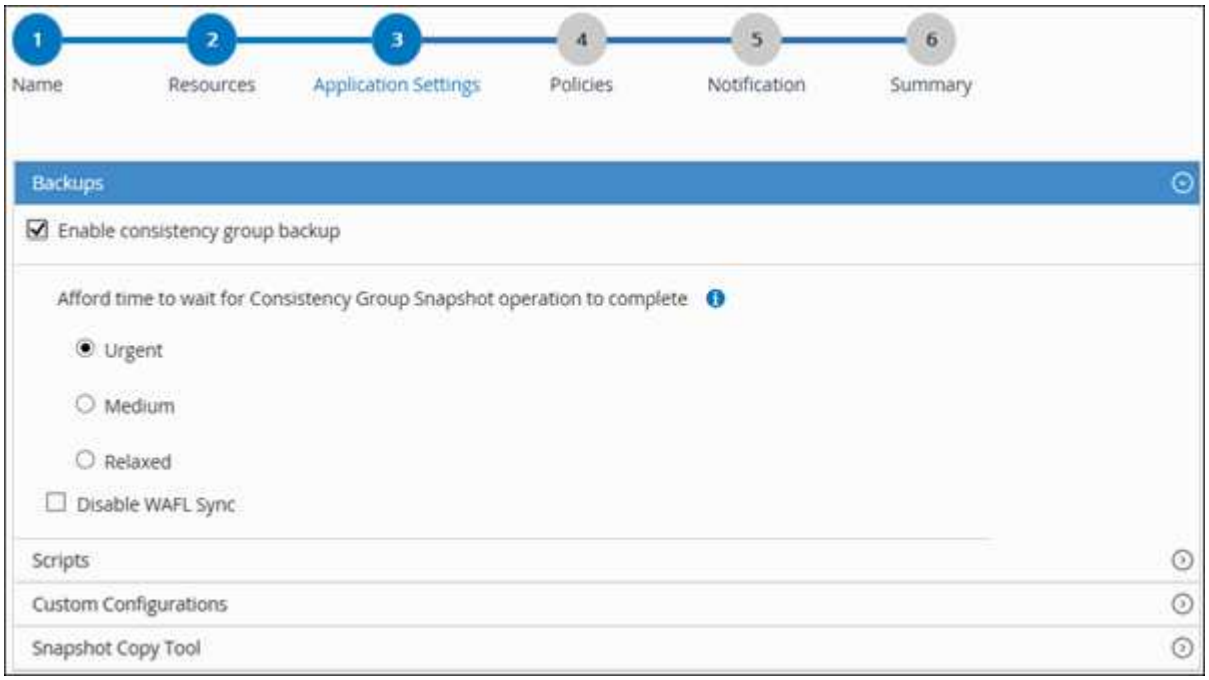
   バックアップ処理を終了する前にPREコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

   ◦ [**Custom Configurations**]矢印を選択し、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*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * 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を作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshot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。

   b. 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]列で**を選択します + 。

   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、*[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。

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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。

   リソーストポロジページが表示されます。

9. [今すぐバックアップ]*を選択します。
10. 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    b. 「 * Backup * 」を選択します。
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。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

  詳細については、次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関係を検出できない"

- VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、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*

PowerShellコマンドレット

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。

```
PS C:\> Open-SmConnection
```

   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、手動でリソースを追加します。

   次に、PostgreSQLインスタンスを追加する例を示します。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

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。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソースグループを追加します。
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します。

   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_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   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"="postgresql"}
   -Policy postgresql_policy2
   ```

6. 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、失敗）を監視します。

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップID、バックアップ名などの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"。

リソースグループのバックアップ

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に対して実行されます。

開始する前に

- ポリシーを適用して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。

タスクの内容

リソースグループは、[Resources]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、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。

   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、を選択し、タグを選択します。その後、を選択してフィルタペインを閉じることができます 。
3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。
   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

PostgreSQL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する

PowerShellコマンドレットを使用してPostgreSQLクラスタをバックアップ、リストア、またはクローニングするには、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。

開始する前に

- 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。

  ストレージシステム接続の追加中にホストプラグインのインストールを実行しないでください。ホストキャッシュが更新されず、SnapCenter GUIでクラスタのステータスが「Not available for backup」または「Not on NetApp storage」と表示されることがあります。
- 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 Core接続セッションを開始します。

```
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。

```
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。

   次に、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例を示します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. SnapCenterサーバにPostgreSQL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 PostgreSQL
```

5. パッケージとSnapCenter Plug-in for PostgreSQL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
PostgreSQL
```

   Windowsの場合：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIBへのパスを設定します。

   Windowsの場合、PostgreSQLプラグインはSQLLIBフォルダのデフォルトパス「C：\Program Files\IBM\SQLLIB\bin」を使用します。

   デフォルトのパスを上書きする場合は、次のコマンドを使用します。

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{"PostgreSQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN"}
```

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、『Software Cmdlet Reference Guide ^]』も参照して https://docs.netapp.com/us-en/snapcenter-cmdlets/index.htmlnapCenter ください。

バックアップ処理の監視

PostgreSQLバックアップ処理の監視

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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、**PostgreSQL**クラスタの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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

PostgreSQL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 *
- 操作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、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。

アクセス元	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。

アクセス元	アクション
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックし  て、最新の5つの処理を表示します。 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PostgreSQLのバックアップとクローンを表示

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ときに、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立つことがあります。

タスクの内容

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-  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。
-  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、バックアップを4つだけ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。

[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、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、Snapshotコピーベースのバックアップとクローン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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

   オンデマンドバックアップのあと、*[リフレッシュ]*ボタンをクリックすると、バックアップまたはクローンの詳細がリフレッシュされます。
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、削除の各処理を実行します。

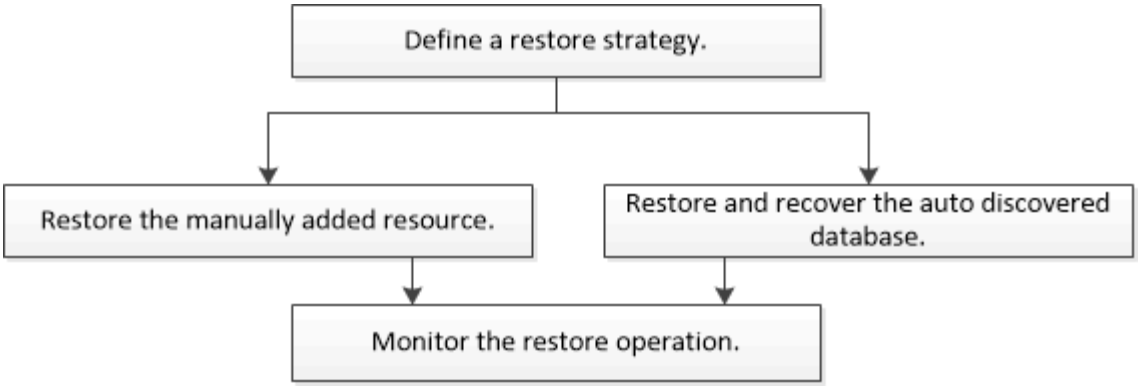
   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。
8. クローンをスプリットする場合は、テーブルでクローンを選択し、をクリックします 。

PostgreSQLのリストア

リストアのワークフロー

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"です。

手動で追加したリソースバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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.config*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _ commands.config*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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。

   リソースがタイプ、ホスト、関連す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。

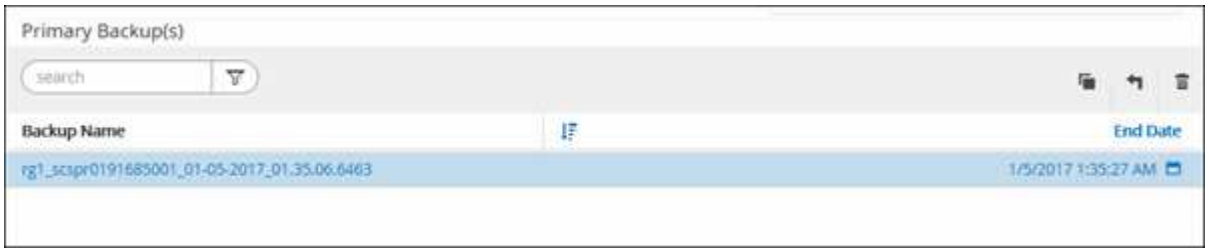
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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  。



6. [Restore Scope]ページで、*[Complete Resource]*を選択します。

   a. [Complete Resource]*を選択すると、PostgreSQLクラスタのすべての設定済みデータボリュームが復元されます。

      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のあとに作成されたSnapshot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。

      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。

7. [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。

8. [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はマウントコマンドを使用できません。

   休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_ からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

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。

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

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。

   ```
   PS C:\> Open-Smconnection
   ```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

自動検出されたクラスタバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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.config*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _ commands.config*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- ファイルベースのバックアップコピーをSnapCenterからリストアすることはできません。
- 自動検出されたリソースについては、SFSRでリストアがサポートされます。
- 自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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。

   リソースがタイプ、ホスト、関連す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。

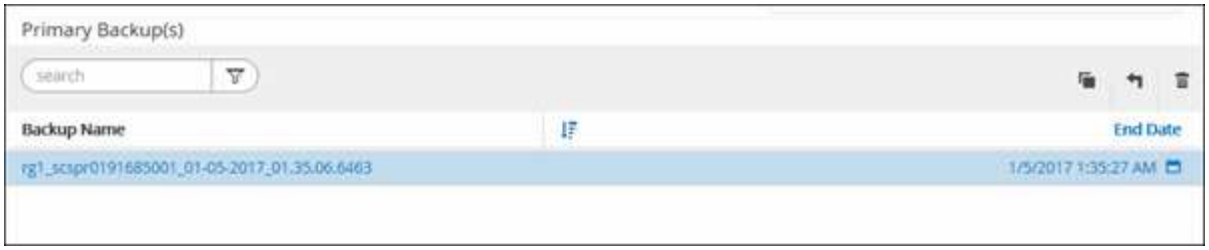
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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 。



6. [Restore Scope]ページで*[Complete Resource]*を選択して、PostgreSQLクラスタの構成済みデータボリュームをリストアします。
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。

状況	操作
できるだけ現在の時刻に近い場所でリカバリしたい	[* 最新の状態に回復する *] を選択します。単一コンテナリソースの場合は、ログおよびカタログバックアップの場所を1つ以上指定します。
指定した時点にリカバリする	[* 特定の時点にリカバリする *] を選択します。 a. 日時を入力します。日時を入力します。たとえば、PostgreSQL Linuxホストがカリフォルニア州サニーベールにあり、ローリーのユーザがSnapCenterにログインしているとします。 ユーザーが5 a.mまでのリカバリを実行する場合。 次に、ユーザはブラウザのタイムゾーンをPostgreSQL Linuxホストのタイムゾーン（GMT-07:00）に設定し、日時を午前5:00に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。

手動で追加したPostgreSQLリソースは回復できません。

SnapCenter Plug-in for PostgreSQLは、手動でのリカバリに役立つように、_/<OS_temp_folder>/<Restore_JobId>/_フォルダにbackup_labelとtablespace_mapを作成します。

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はマウントコマンドを使用できません。

休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path 、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

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。

PowerShellコマンドレットを使用したリソースのリストア

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

PostgreSQLリストア処理の監視

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

PostgreSQLリソースバックアップのクローニング

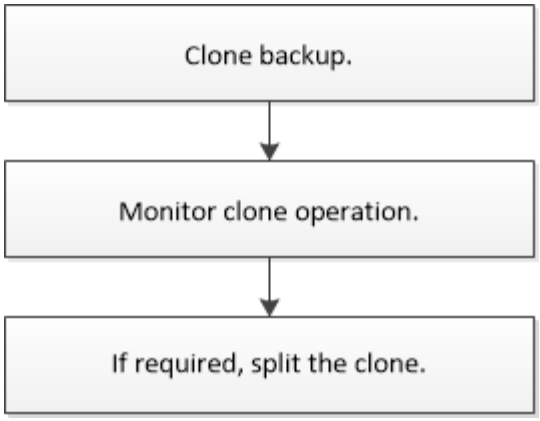
クローニングのワークフロー

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。

タスクの内容

- クローニングはソースのPostgreSQLサーバで実行できます。
- 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
  - データウェアハウスにデータを取り込む際のデータ抽出および操作ツール用
  - 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。

PostgreSQLバックアップをクローニング

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。

開始する前に

- 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）の割り当て済みアグリゲートリストに含まれている必要があります。
- クローニング前またはクローニング後のコマンドについては、次のパスからプラグインホストで使用できるコマンドリストにコマンドが存在す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*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- 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"。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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. Location ページで、次のアクションを実行します。

フィールド	操作
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。
ターゲットポート	既存のバックアップからクローニングするPostgreSQLターゲットポートを入力します。
NFSエクスポートIPアドレス	クローンボリュームをエクスポートするホスト名またはIPアドレスを入力します。 これは、NFSストレージタイプリソースにのみ該当します。
容量プール最大 スループット（MiB/秒）	容量プールの最大スループットを入力します。 これは、ANFストレージタイプのリソースにのみ該当します。

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：同じ名前の既存のクラスタを削除

- クローニング後のコマンド：クラスタの検証またはクラスタの開始を行います。

b. mountコマンドを入力して、ファイルシステムをホストにマウントします。

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
```

休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_からプラグインホストで使用できるコマンドリストにコマンドがあるかどうかを確認する必要があります。

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。

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

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。

```
PS C:\> Open-SmConnection
```

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、クローニングに2つのバックアップを使用できます。

```
 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アドレスが10.32.212.14であるバックアップをクローニングしています。

   PostgreSQLクラスタの場合：

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```

   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ン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          :
```

PostgreSQL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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。

3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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する

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングまたは検証が失敗する"

SnapCenterのアップグレード後に**PostgreSQL**クラスタクローンを削除または分割する

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。クローンを作成したリソースの[Topology]ページで、クローンを削除したり、クローンをスプリットしたりできます。

タスクの内容

非表示のクローンのストレージフットプリントを特定するには、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、クローニングされ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。

   リソーストポロジページが表示されます。

5. [Manage Copies]ビューで、プライマリまたはセカンダリ（ミラーリング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、をクリックしてクローンを削除するか、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。

MySQLの保護

MySQL用SnapCenterプラグイン

SnapCenter Plug-in for MySQLの概要

SnapCenter Plug-in for MySQL Databaseは、MySQLデータベースに対応した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。Plug-in for MySQL Databaseは、SnapCenter環境でのMySQL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では、シングルインスタンスのMySQLセットアップがサポートされます。Plug-in for MySQL Databaseは、LinuxとWindowsのどちらの環境でも使用できます。Windows環境では、MySQLは手動リソースとしてサポートされます。

Plug-in for MySQL Databaseがインストールされている場合は、SnapCenterと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、本プラグインをNetApp SnapVaultテクノロジとともに使用して、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 MySQLは、ONTAPおよびAzure NetAppのファイルストレージレイアウトでNFSとSANをサポートします。

VMDKまたは仮想ストレージレイアウトがサポートされます。

シンボリックリンクはサポートされません。

SnapCenter Plug-in for MySQLの機能

Plug-in for MySQL Databaseをインストールした環境では、SnapCenterを使用してMySQLインスタンスをバックアップ、リストア、および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。

- インスタンスを追加します。
- 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します。
- 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 MySQL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 MySQL Databaseを操作する

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

  SnapCenterでは、Plug-in for MySQL DatabaseでNetAppのSnapshot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 MySQLを使用すると、次のようなメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます。
- RBACでサポートされるセキュリティと一元化されたロール委譲

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルの権限を付与することもできます。

- NetApp FlexCloneテクノロジを使用して、テストまたはデータ抽出に使用するリソ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できます。

  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。

- バックアップ作成時にONTAPの整合グループ（CG）Snapshot機能がサポートされるようになりました。
- 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可能

  1回の操作で、1つのホスト内のリソースが同じボリュームを共有すると、スナップショットが統合されます。

- 外部コマンドを使用してスナップショットを作成する機能。
- XFSファイルシステムでのLinux LVMのサポート。

SnapCenter Plug-in for MySQL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 MySQL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こと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セツソクLUN
物理サーバ	iSCSIセツソクLUN
物理サーバと仮想サーバ	NFS接続ボリューム

MySQL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
  - ジョブ履歴の表示
  - ジョブの停止
  - LUN
  - LUNの作成
  - LUNの作成
  - LUNの作成
  - lun delete
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード
  - LUNマッピングの作成
  - LUNマッピングの削除
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - LUN変更
  - ボリューム内でのLUNの移動
  - LUNオフライン
  - LUNオンライン
  - LUN永続的予約のクリア

- LUNのサイズ変更
- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set
- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- volume snapshot modify -snaplock-expiry-time

- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- SVM iSCSI
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限
  - ネットワークインターフェイス
  - network interface show
  - SVM

MySQL用の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 SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

MySQLノハツクアツフセンリヤク

MySQL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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

タスクの内容

SLAは、期待されるサービスレベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要がある時間です。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ます。SLA、RTO、RPOは、データ保護戦略に影響します。

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. アプリケーションと整合性のあるデータベースのSnapshotをバックアップするSnapshotコピーベースのポリシーを作成するかどうかを決定します。
5. レプリケーションにNetApp SnapMirrorテクノロジを使用するか、長期保持にNetApp SnapVaultテクノロジを使用するかを決定します。
6. ソースストレージシステムとSnapMirrorデスティネーションでのSnapshotの保持期間を決定します。
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。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterで管理されるLinuxホスト上のMySQLインスタンスで

す。SnapCenter Plug-in for MySQLプラグインをインストールすると、そのLinuxホスト上のMySQLインスタンスが自動的に検出されて[Resources]ページに表示されます。

サポートされるバックアップのタイプ

Backup typeには、作成するバックアップのタイプを指定します。SnapCenterでは、MySQLデータベースに対してSnapshotコピーベースのバックアップタイプがサポートされます。

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のSnapshotテクノロジを利用して、MySQLデータベースが格納されているボリュームのオンラインの読み取り専用コピーを作成します。

SnapCenter Plug-in for MySQLでの整合グループ**Snapshot**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性グループのSnapshotを作成できます。整合グループはコンテナであり、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。整合グループは、複数のボリュームの同時Snapshotであり、ボリュームグループの整合性のあるコピーを提供します。

ストレージコントローラが整合性のあるSnapshotをグループ化するまでの待機時間を指定することもできます。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の処理中に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の同期により、整合性グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なログバックアップの削除の管理方法

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データバックアップの削除を管理します。

MySQL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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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つの部分があります。

- 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タイミング）

  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単位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。

MySQL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には、リソースのサイズ、使用されているボリュームの数、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 MySQLテタヘスノハツクアツフノメイメイキソク

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshot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、*[Use custom name format for Snapshot copy]*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などです。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

MySQLノリストアオヨヒリカハリセンリヤク

MySQL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。

データベースの手動リカバリのみがサポートされます。

手順

1. 手動で追加したMySQLリソースでサポートされるリストア戦略を確認する
2. 自動検出されたMySQLデータベースに対してサポートされるリストア戦略を確認する

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**MySQL**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、戦略を定義する必要があります。手動で追加したMySQLリソースには、2種類のリストア戦略があります。

手動で追加したMySQL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

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のあとに作成されたSnapshotは削除され、リカバリできません。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。

自動検出された**MySQL**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、戦略を定義する必要があります。

リソースの完全リストアは、自動検出されたMySQLデータベースに対してサポートされるリストア戦略です。これにより、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

自動検出された**MySQL**のリストア処理のタイプ

SnapCenter Plug-in for MySQLでは、自動的に検出されたMySQLデータベースに対して、Single File SnapRestoreおよびConnect and Copyリストアタイプがサポートされます。

NFS環境で**Single File SnapRestore**を実行するシナリオは、次のとおりです。

- [Complete Resource]オプションのみが選択されている場合
- 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

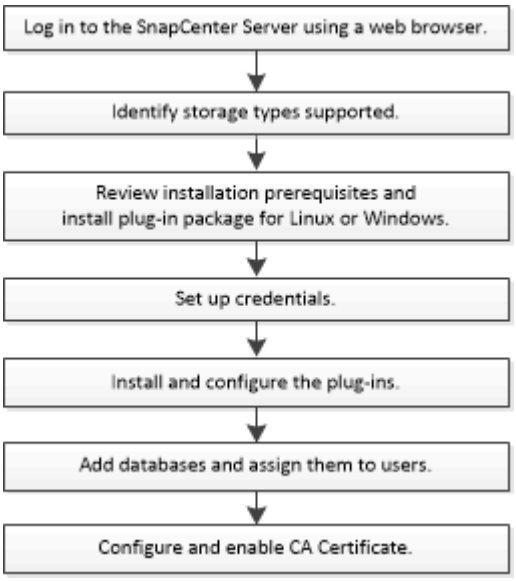
単一ファイル **SnapRestore** は、次のような状況で **SAN** 環境で実行されます。

- [Complete Resource]オプションのみが選択されている場合
- 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

SnapCenter Plug-in for MySQLのインストールの準備

SnapCenter Plug-in for MySQLのインストールワークフロー

MySQLデータベースを保護する場合は、SnapCenter Plug-in for MySQL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 MySQL**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 MySQLは、WindowsとLinuxの両方の環境で使用できます。

- Java 11をホストにインストールしておく必要があります。

  IBM Javaはサポートされていません。

- Windowsの場合、Plug-in CreatorサービスはWindowsユーザ「LocalSystem」を使用して実行する必要があります。これは、Plug-in for MySQL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ホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。SnapCenter Plug-in for Microsoft Windowsは、WindowsホストへのMySQLプラグインと一緒にデフォルトで導入されます。
- SnapCenterサーバがPlug-in for MySQL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。
- MySQL 5.7の場合は、MySQLの設定ファイル（my.cnfまたはmysql-server.cnf）にbinlogを指定する必要があります。

Windowsホスト

- ローカル管理者Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。

- Plug-in for MySQLをWindowsホストにインストールすると、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以外のユーザに対して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 11をWindowsホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

Linuxホスト

- rootユーザまたはroot以外のユーザに対して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 11をLinuxホストにインストールしておく必要があります。

  "すべてのオペレーティングシステム用のJavaダウンロード"

  "NetApp Interoperability Matrix Tool"

- LinuxホストでMySQLデータベースを実行している場合は、Plug-in for MySQLのインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- 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。

補助コマンド

SnapCenter Plug-in for MySQLで補助的なコマンドを実行するには、ファイルにそのコマンドを含める必要があります `allowed_commands.config` 。

`allowed_commands.config` ファイルは、SnapCenter Plug-in for MySQLディレクトリの「etc」サブディレクトリにあります。

Windowsホスト

デフォルト： `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

カスタムパス： `<Custom_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Linuxホスト

デフォルト： `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

カスタムパス： `<Custom_Directory>allowed_commands.config`

プラグインホストで追加のコマンドを許可するには、エディタでファイルを開きます `allowed_commands.config` 。各コマンドを別 々 の行に入力します。大文字と小文字は区別されません。例えば、

コマンド:mount

コマンド：umount

完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符（"）で囲みます。例えば、

コマンド："C：\Program Files\NetApp\SnapCreator commands\sdcli.exe"

コマンド：myscript.bat

ファイルが存在しない場合は `allowed_commands.config` 、コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

コマンドまたはスクリプトがに存在しないと、 `allowed_commands.config`コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

ワイルドカードエントリ（*）を使用してすべてのコマンドを許可しないでください。

Linuxホストの**root**以外のユーザに対する**sudo Privileges**の設定

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をroot以外の有効なユーザとして実行します。複数のパスにアクセスできるようにroot以外のユーザにsudo Privileges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
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- /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。

  構成ファイルの更新後に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/installation/plugins/uninstall
- /custom_location /NetApp/snapcenter/spl/bin/spl
- 手順 *
  1. SnapCenter Plug-ins Package for Linuxをインストールする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_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- _C：\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt（SnapCenter ServerがWindowsホストにインストールされている場合）。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc _ unix_plugins_checksum.txt _ LinuxホストにSnapCenterサーバがインストールされている場合。

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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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	• DOTNETコア8.0.5 • PowerShell Core 7.4.2 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、基本的なホストシステムのスペースとサイジングの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 • 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量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、最近実行した処理の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 11 Oracle JavaおよびOpenJDK を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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 "NetApp Interoperability Matrix Tool" ください。

SnapCenter Plug-in for MySQLのクレデンシャルを設定

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースまたは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クレデンシャルをそれぞれ作成する必要があります。

タスクの内容

- Linuxホスト

  Linuxホストにプラグインをインストールするには、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、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo Privilegesがあるroot以外のユーザに対して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

  プラグインをインストールする前にWindows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には、管理者権限（リモートホストに対する管理者権限を含む）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、ユーザ名に完全なadmin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の権限を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、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	操作
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。ユーザ名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	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ユーザのみに適用されます。

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、必要に応じて[User and Access]ページでユーザまたはユーザグループ

にクレデンシャルを割り当てることができます。

SnapCenter Plug-in for MySQLのインストール

ホストを追加してリモートホストにプラグインパッケージをインストールする

SnapCenterの[ホストを追加]ページを使用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。プラグインはリモートホストに自動的にインストールされます。ホストを追加して、個 々 のホスト用のプラグインパッケージをインストールできます。

開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
  - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- 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、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストの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する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。

タスクの内容

- 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]*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	操作
ホストタイプ	ホストのタイプを選択します。 • ウィンドウ • Linux Plug-in for MySQLをMySQLデータベースサーバにインストールする必要があります。

フィールド	操作
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が適切に設定されているかどうか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。
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]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。

   REST APIを使用してPlug-in for MySQLをインストールする場合は、バージョンを3.0として渡す必要があります。例：mysql：3.0

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	操作
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	操作
インストールパス	Plug-in for MySQLはMySQL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。
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。
クラスタ内のすべてのホストを追加	該当なし。
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	該当なし。

7. [Submit （送信）] をクリックします。

   [Skip prechecks]チェック ボックスを選択していない場合、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を検証するためにホストが検証されます。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）、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、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\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。

9. インストールの進行状況を監視します。

- Windowsプラグインの場合、インストールログとアップグレードログは_C：\Windows\SnapCenter <JOBID>にあります。
- Linuxプラグインの場合、インストールログは_/var/opt/snapcenter/logs/SnapCenter *Linux_Host_Plug-in_Install_Install_Linux.log*<JOBID>にあり、アップグレードログは_/var/opt/snapcenter/logs/SnapCenter <JOBID>.log_にあります。

終了後

SnapCenter 6.0にアップグレードする場合は、既存のPerlベースのPlug-in for MySQLがリモートプラグインサーバからアンインストールされます。

コマンドレットを使用した複数のリモートホストへの**SnapCenter Plug-in Package for Linux / Windows**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、複数のホストにSnapCenter Plug-in Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグインパッケージを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にログインしておく必要があります。

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。
4. 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 MySQL**をインストールする

SnapCenterユーザインターフェイス（UI）を使用して、SnapCenter Plug-in for MySQL Databaseをインストールする必要があります。ご使用の環境でSnapCenter UIからの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、コンソールモードまたはサイレントモードでPlug-in for MySQL Databaseをインストールできます。

開始する前に

- Plug-in for MySQL Databaseは、MySQLインスタンスを保護する必要がある各Linuxホストにインストールする必要があります。

- SnapCenter Plug-in for MySQL Databaseをインストールするホストは、依存するソフトウェア、データベース、および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"

- SnapCenter Plug-in for MySQL Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

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Plug-in for MySQL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. /<installation directory>/NetApp/snapcenter/scc/etc/SC _ SMS_Services.propertiesファイルを編集し、plugins_enabled=mysql：3.0パラメータを追加します。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenterサーバにホストを追加します。

   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 MySQLのインストールステータスの監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストのプラグインサービスとバインドします。

```
> $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ホストでの**SnapCenter MySQL**プラグインサービス用の**CA**証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中の**CA**署名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ます。

カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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を含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

手順

1. カスタムプラグインキーストア/opt/NetApp/snapcenter/scc/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

6. 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キーストアに含まれていることを確認

します。

7. CA証明書に追加し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SCC_CERTIFICATE_ALIASキーに対して更新します。

8. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（CRL）を設定する

タスクの内容

- 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で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/scc/etc/crl」です。

手順

1. crl_pathキーに対して、agent.propertiesファイルのデフォルトディレクトリを変更および更新できます。

   このディレクトリには、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

Windowsホスト上のSnapCenter MySQLプラグインサービス用のCA証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中のCA署名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。

4. パスワードを変更したら、サービスを再起動します。

   カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   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ます。

   ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

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一覧表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   keytool -list -v キーストア *.JKS*

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルのキーkeystore_passの値です。

   *keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

8. *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SCC_CERTIFICATE_ALIASキーに対して更新します。

9. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（**CRL**）を設定する

タスクの内容

- 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で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は、複数のCRLファイルを配置できます。

受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for MySQLを使用するための前提条件

SnapCenter Plug-in for MySQLを使用する前に、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。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

  Javaのパスは、ホストマシンの環境パス変数で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な場合は、SnapMirrorとSnapVaultをセットアップします。

MySQLを保護するためのリソース、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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- 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MySQLインスタンスです。
- 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できます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを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、そのグループのポリシーを1つ以上選択します。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にも、ポリシーを選択できます。

リソースグループは、保護する対象と保護するタイミング（日時）を定義するものと考えてください。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。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。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。

MySQLリソースのバックアップ

MySQLリソースのバックアップ

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。

[MySQLバックアップのワークフロー] | *../media/db2_backup_workflow.gif*

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。https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenter ソフトウェアコマンドレットリファレンスガイド"^]です。

データベースの自動検出

リソースとは、SnapCenterで管理されているLinuxホスト上のMySQLデータベースです。使用可能なMySQLデータベースを検出したあとに、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。

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セットアップなどのタスクを完了しておく必要があります。
- SnapCenter Plug-in for MySQL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ていません。データベースを手動で追加する際に、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。

タスクの内容

- 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。
- 自動検出されるのはデータベースだけです。

自動検出されたリソースを変更または削除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、*[リソース]*をクリックし、リストからPlug-in for MySQLを選択します。
2. [Resources]ページで、[View]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、ホスト名を選択します。

   次に、**をクリックしてフィルタペインを閉じることができます。
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NetAppストレージにあり、保護されていない場合は、[全体のステータス]列に「保護されていません」と表示されます。
   - データベースがNetAppストレージシステム上にあり保護されていて、実行されたバックアップ処理がない場合は、[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。

SnapCenterの外部でインスタンスの名前を変更した場合は、リソースを更新する必要があります。

プラグインホストに手動でリソースを追加する

自動検出はWindowsホストではサポートされていません。MySQLインスタンスとデータベースリソースを手動で追加する必要があります。

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セットアップなどのタスクを完了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、ドロップダウンリストからSnapCenter Plug-in for MySQLを選択し、*[リソース]*をクリックします。
2. [リソース]ページで、*[MySQLリソースの追加]*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	操作
名前	データベース名を指定します。
ホスト名	ホスト名を入力します。
タイプ	インスタンスを選択します。
インスタンス	該当なし。
クレデンシャル	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージフットプリントの入力]ページで、ストレージタイプを選択して1つ以上のボリューム、LUN、およびqtreeを選択し、*[保存]*をクリックします。

   オプション：*アイコンをクリックすると、他のストレージシステムからボリューム、LUN、およびqtreeを追加できます  。

5. オプション：[Resource Settings]ページで、MySQLプラグインのカスタムのキーと値のペアを入力します。
6. 概要を確認し、 [完了] をクリックします。

   データベースは、ホスト名、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。

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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

"ユーザまたはグループを追加してロールとアセットを割り当てる"

データベースを追加したら、MySQLデータベースの詳細を変更できます。

MySQLのバックアップポリシーの作成

SnapCenterを使用してMySQLリソースをバックアップする前に、バックアップする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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

  詳細については、MySQL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。

- 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、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おく必要があります。
- Snapshot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の両方に対応する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。

  また、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ポリシーで指定することもできます。これらのオプションを使用することで、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できます。

タスクの内容

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されなくなります。その結果、ポリシーで指定された数よりも多くのSnapshotが保持される可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

手順

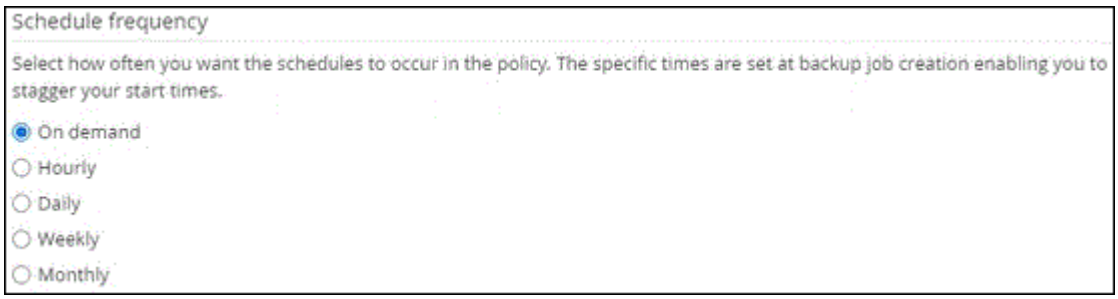
1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. [Policy type]ページで、次の手順を実行します。
   a. ストレージタイプを選択します。
   b. [* カスタム・バックアップ設定 *] セクションで、キー値形式でプラグインに渡す必要がある特定の

バックアップ設定を指定します。

プラグインに渡すキー値は複数指定できます。

6. [Snapshot]ページで、* on demand 、 Hourly 、 Daily 、 Weekly 、または Monthly *を選択してスケジュールタイプを指定します。

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、終了日、頻度）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ている場合、夏時間（DST）中はスケジュールはトリガーされません。

7. [Snapshot settings]セクションで、保持するSnapshotの数を指定します。
8. [Retention]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業
一定数のSnapshotを保持	[保持するコピー数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshotが削除されます。

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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。

9. 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、バックアップおよび保護するリソースを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。また、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必要があります。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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、 [* 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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名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。

   これは、画面上の情報をフィルタリングするのに役立ちます。

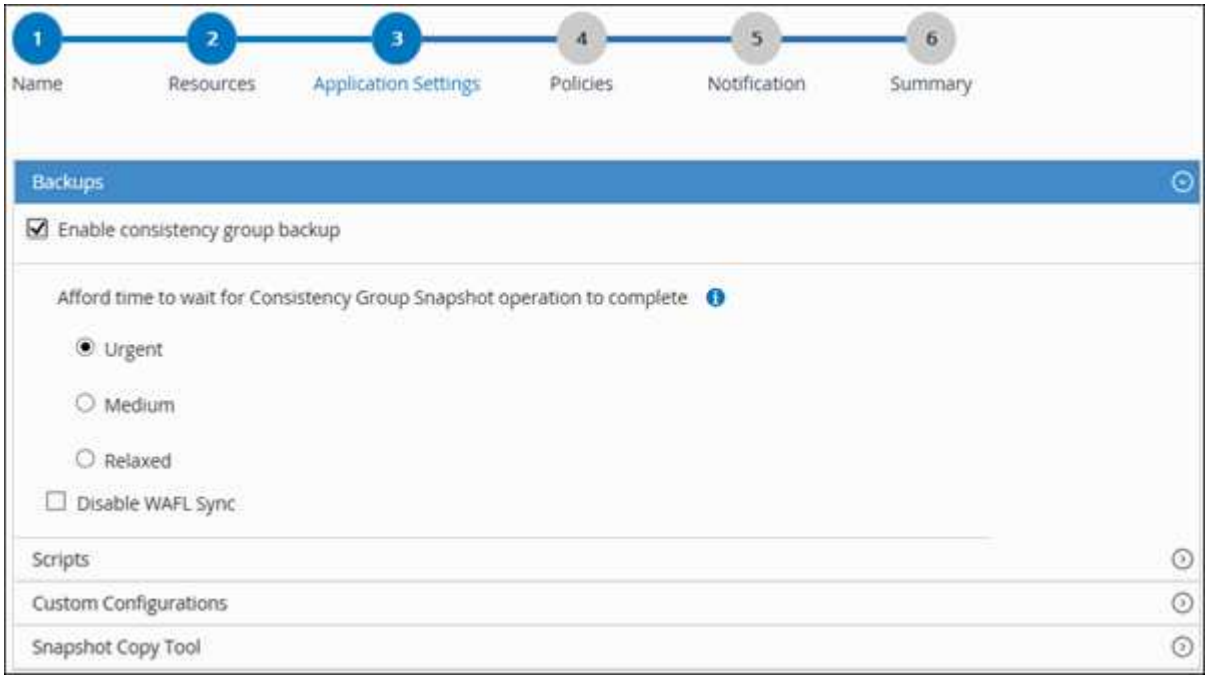
5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。
6. [アプリケーションの設定] ページで、次の操作を行います。

   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、次のタスクを実行します。

フィールド	操作
整合グループのSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+



a. [Scripts]*の矢印をクリックし、休止、Snapshot、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. [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	（Y/N）	アーカイブログ管理でアーカイブログを削除できます。
アーカイブログの保持	日数	アーカイブログを保持する日数を指定します。 この設定はNTAP_SNAPSHOT_RETENTIONS 以上である必要があります。

パラメータ	設定	説明
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。
ARCHIVE_LOG_EXT	ファイル拡張子	アーカイブログファイルの拡張子の長さを指定します。 たとえば、アーカイブログが LOG_BACKUP _0_0_0_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

カスタムのキーと値のペアは、MySQL Linuxプラグインシステムでサポートされ、一元化されたWindowsプラグインとして登録されたMySQLデータベースではサポートされません。

c. Snapshotコピーツール*の矢印をクリックして、スナップショットを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、スナップショットを作成する前にファイルシステムを整合性のある状態にします。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。
SnapCenter：ストレージレベルのSnapshotを作成	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します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。

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 + 。

ポリシーが[Configure schedules for selected policies]セクションに表示されます。

b. [スケジュールの設定]列で、設定するポリシーの**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。

サードパーティの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はサポートされません。

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 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、 [完了] をクリックします。

MySQL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、のページからバックアップすることができます。

開始する前に

- 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であることを確認してください。
- 休止、Snapshot、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の場合は、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用でき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*

ⓘ コマンドがコマンドリストに存在しない場合、処理は失敗します。

SnapCenter UI

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。

   *を選択し、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。その後、を選択してフィルタペインを閉じることができます 。

3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名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。

   ◦ [Backups]*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。

   必要に応じて整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

   ◦ [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

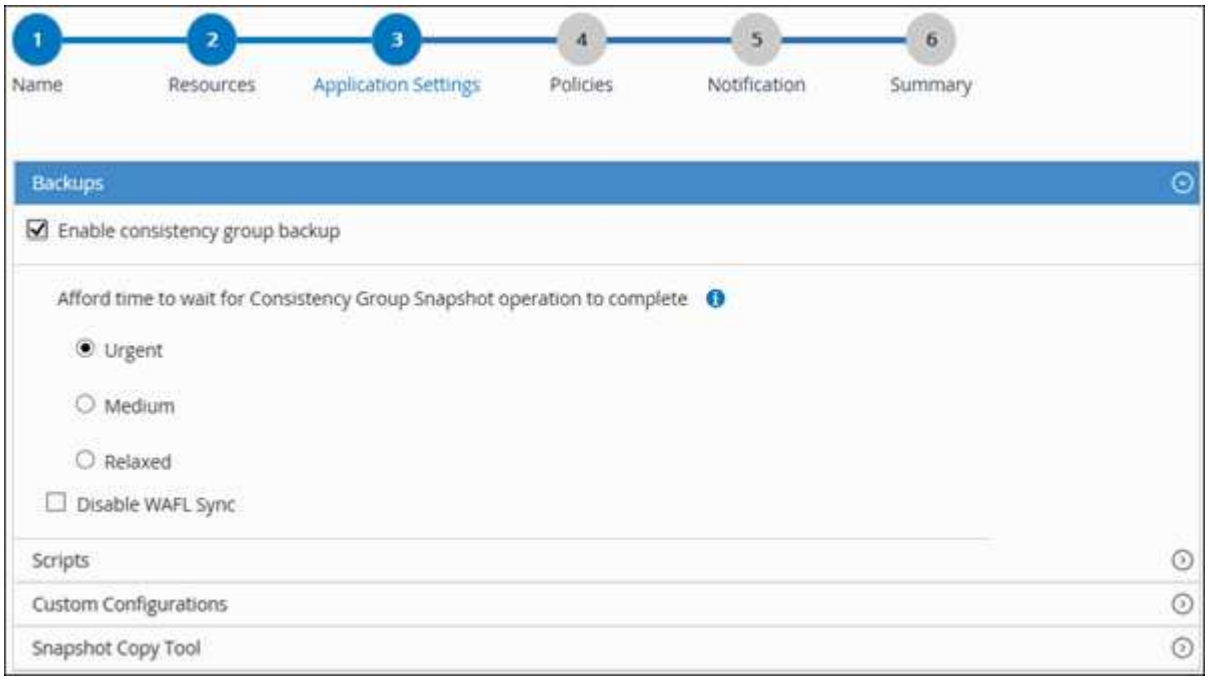
   バックアップ処理を終了する前にPREコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

   ◦ [**Custom Configurations**]矢印を選択し、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*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * 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を作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshot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。

   b. 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]列で**を選択します + 。

   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、*[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。

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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。

   リソーストポロジページが表示されます。

9. [今すぐバックアップ]*を選択します。
10. 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    b. 「 * Backup * 」を選択します。
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。

    ◦ MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

      詳細については、次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関係を検出できない"

    ◦ VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、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*

PowerShellコマンドレット

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、手動でリソースを追加します。

   次に、MySQLインスタンスを追加する例を示します。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

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。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソースグループを追加します。
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します。

   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 -Resources
   @{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
   luginName"="MySQL"} -Policy "MySQL_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 mysql_policy2
   ```

6. 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、失敗）を監視します。

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップID、バックアップ名などの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"。

リソースグループのバックアップ

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に対して実行されます。

開始する前に

- ポリシーを適用して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。

タスクの内容

リソースグループは、[Resources]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、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。

   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、を選択し、タグを選択します。その後、を選択してフィルタペインを閉じることができます 。
3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。
   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

MySQL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する

PowerShellコマンドレットを使用してMySQLデータベースをバックアップ、リストア、またはクローニングするには、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。

開始する前に

- 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 Core接続セッションを開始します。

```
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。

```
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。

   次に、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例を示します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. MySQL通信ホストをSnapCenterサーバに追加します。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode mysql
```

5. パッケージとSnapCenter Plug-in for MySQL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
mysql
```

   Windowsの場合：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIBへのパスを設定します。

   Windowsの場合、MySQLプラグインはSQLLIBフォルダのデフォルトパス「C：\Program Files\IBM\SQLLIB\bin」を使用します。

   デフォルトのパスを上書きする場合は、次のコマンドを使用します。

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{"MySQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN"}
```

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"。

バックアップ処理の監視

MySQLバックアップ処理を監視する

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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、**MySQL**インスタンスのデータ保護処理を監視する

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

MySQL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 *
- 操作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、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。

アクセス元	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。

アクセス元	アクション
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックし  て、最新の5つの処理を表示します。 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]ページでのMySQLのバックアップとクローンの表示

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ときに、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立つことがあります。

タスクの内容

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-  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。
-  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、バックアップを4つだけ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。

[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、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、Snapshotコピーベースのバックアップとクローン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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

   オンデマンドバックアップのあと、*[リフレッシュ]*ボタンをクリックすると、バックアップまたはクローンの詳細がリフレッシュされます。
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、削除の各処理を実行します。

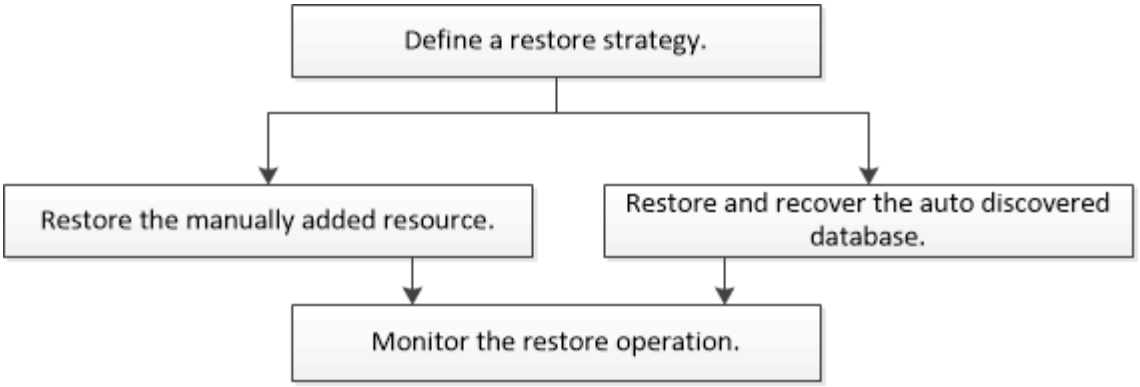
   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。
8. クローンをスプリットする場合は、テーブルでクローンを選択し、をクリックします 。

MySQLのリストア

リストアのワークフロー

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"です。

手動で追加したリソースバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから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.config*

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _ commands.config*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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。

   リソースがタイプ、ホスト、関連す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。

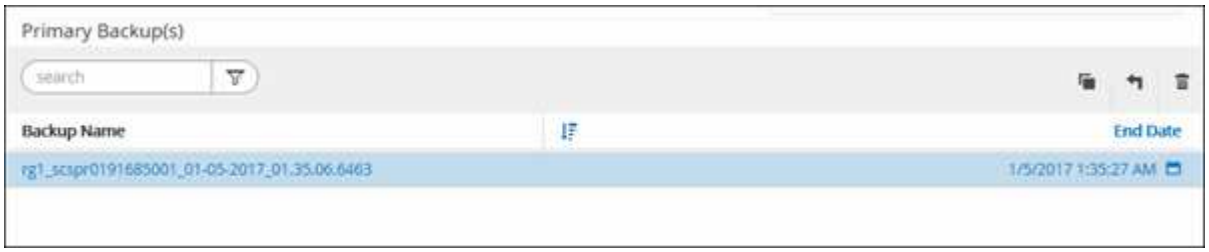
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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
   。



6. [Restore Scope]ページで、*[Complete Resource]*を選択します。

   a. [Complete Resource]*を選択すると、MySQL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のあとに作成されたSnapshot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。

      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。

7. [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。

8. [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はマウントコマンドを使用できません。

   > ⓘ 休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_ からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

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。

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

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。

   ```
   PS C:\> Open-Smconnection
   ```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

自動検出されたデータベースバックアップのリストアとリカバリ

SnapCenterを使用すると、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。

開始する前に

- 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実行中のバックアップ処理がある場合は、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、およびアンマウントの各コマンドを実行する場合は、プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを次のパスから確認する必要があります。

  Linuxの場合：*/var/opt/snapcenter/scc/allowed _ commands.config*

  コマンドがコマンドリストに存在しない場合、処理は失敗します。

タスクの内容

- 自動検出されたリソースについては、SFSRでリストアがサポートされます。
- ポイントインタイムと最新の状態への自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップ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。

   リソースがタイプ、ホスト、関連す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。

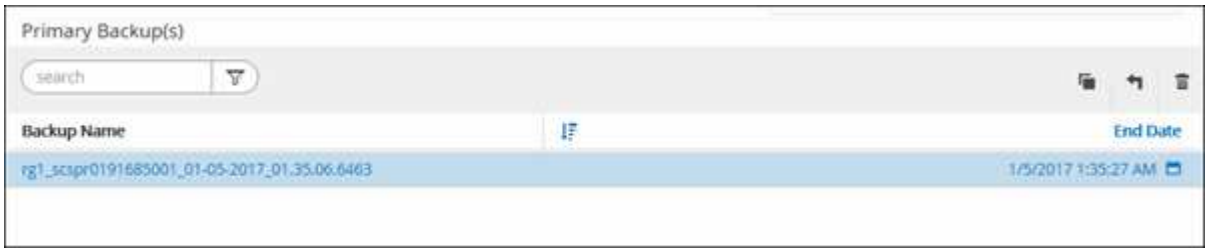
   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

   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] 列に表示されますリソースが保護されていないか、別のユーザによってバックアップされている可能性があります。

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. [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 。



6. [Restore Scope]ページで、*[Complete Resource]*を選択してMySQL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。

7. [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。

8. [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はマウントコマンドを使用できません。

   休止、Snapshot、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の場合は、Linuxの_/opt/snapcenter/snapenter/scc/allowed _ commands.config_pathからプラグインホストで使用できるコマンドリストに該当するコマンドがあるかどうかを確認する必要があります。

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。

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たリソースのリストア

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。

   ```
   PS C:\> Open-Smconnection
   ```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

MySQLのリストア処理を監視する

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

MySQLリソースのバックアップをクローニング

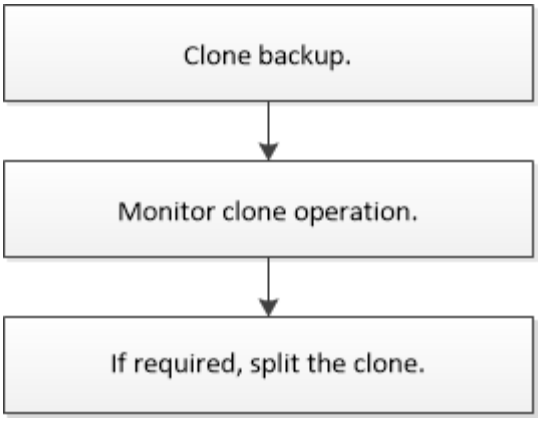
クローニングのワークフロー

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。

タスクの内容

- のクローンはソースのMySQLサーバで作成できます。
- 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
  - データウェアハウスにデータを取り込む際のデータ抽出および操作ツール用
  - 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。

MySQLバックアップをクローニング

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。

開始する前に

- 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）の割り当て済みアグリゲートリストに含まれている必要があります。
- クローニング前またはクローニング後のコマンドについては、次のパスからプラグインホストで使用できるコマンドリストにコマンドが存在す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*

> コマンドがコマンドリストに存在しない場合、処理は失敗します。* MySQL 5.7のバージョンでは、MySQLでIGNORE_MYSQLX_PORT = true（デフォルトではfalse）に設定する必要があります。 プロパティファイル。

タスクの内容

- クローンされたMySQLインスタンスを保護することはできません。
- 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"。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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. Location ページで、次のアクションを実行します。

フィールド	操作
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。
ポート	クローニングしたMySQLインスタンスを起動するポートを指定します。
NFSエクスポートIPアドレス	クローンボリュームをエクスポートするホスト名またはIPアドレスを入力します。

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の削除
      - 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. mountコマンドを入力して、ファイルシステムをホストにマウントします。

      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
```

休止、Snapshot、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の場合は、Linuxの場合は_/opt/snapcenter/snapenter/scc/allowed commands.config_path、Windowsの場合は_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_からプラグインホストで使用できるコマンドリストにコマンドがあるかどうかを確認する必要があります。

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。

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

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。

```
PS C:\> 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、クローニングに2つのバックアップを使用できます。

```
 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アドレスが10.32.212.14であるバックアップをクローニングしていま

す。

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName
"scs000211748_gdl_englab_netapp_com_MySQL_mysqld_3306_scs000211748_0
6-26-2024_06.08.35.4307" -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306"}
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```

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ン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          :
```

MySQL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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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する

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングまたは検証が失敗する"

SnapCenterのアップグレード後に**MySQL**データベースクローンを削除またはスプリットする

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

を作成したリソースの[Topology]ページで、クローンを削除したり、クローンをスプリットしたりできます。

タスクの内容

非表示のクローンのストレージフットプリントを特定するには、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、クローニングされ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。

   リソーストポロジページが表示されます。

5. [Manage Copies]ビューで、プライマリまたはセカンダリ（ミラーリング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、をクリックしてクローンを削除するか、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。

UNIXファイルシステムの保護

UNIXファイルシステム用SnapCenterプラグインの機能

Plug-in for UNIXファイルシステムをインストールした環境では、SnapCenterを使用してUNIXファイルシステムをバックアップ、リストア、および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。

- リソースの検出
- UNIX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設定
- ファイルシステムのバックアップのリストア
- ファイルシステムのバックアップのクローニング
- 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

サポートされる構成

項目	サポートされる構成
環境	• 物理サーバ • 仮想サーバ NFSとSANの両方にVVOLデータストアを配置します。 VVOLデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。
オペレーティングシステム	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server（SLES）
ファイルシステム	• SAN ： ◦ LVMベースと非LVMベースの両方のファイルシステム ◦ VMDK ext3、ext4、xfs経由のLVM • NFS：NFS v3、NFS v4.x
プロトコル	• FC • FCoE • iSCSI • NFS

項目	サポートされる構成
マルチパス	はい

制限事項

- ボリュームグループでのRDMと仮想ディスクの混在はサポートされていません。
- ファイルレベルのリストアはサポートされていません。

  ただし、バックアップをクローニングし、ファイルを手動でコピーすることで、ファイルレベルのリストアを手動で実行できます。

- NFSデータストアとVMFSデータストアの両方からの複数のVMDKにまたがるファイルシステムの混在はサポートされていません。
- NVMeはサポートされません。
- プロビジョニングはサポートされていません。

SnapCenter Plug-in for Unixファイルシステムのインストール

ホストを追加して**Plug-ins Package for Linux**をインストールするための前提条件

ホストを追加してLinux用の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、またはSSHキーベースの認証にはパスワードベースの認証を使用できます。

  SnapCenter Plug-in for Unix File Systems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するには、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスはroot以外の有効なユーザとして実行されます。

- インストールユーザのクレデンシャルを、認証モードをLinuxに設定して作成します。
- Java 11をLinuxホストに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ダウンロード"

- 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 • Oracle Linux • SUSE Linux Enterprise Server（SLES）
ホスト上のSnapCenterプラグイン用の最小RAM	2GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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 11 Oracle JavaおよびOpenJDK 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。 を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設定されていることを確認する必要があります。

サポートされるバージョンの最新情報については https://imt.netapp.com/matrix/imt.jsp?components=121073;&solution=1257&isHWU&src=IMT、NetApp Interoperability Matrix Tool^]を参照してください。

GUIを使用したホストの追加とPlug-ins Package for Linuxのインストール

[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をインストールできます。プラグインはリモートホストに自動的に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]*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	操作
ホストタイプ	ホストタイプとして* Linux *を選択します。
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が適切に設定されているかどうか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。 SnapCenterを使用してホストを追加する場合、そのホストがサブドメインの一部であるときは、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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]セクションで、*[Unix File Systems]*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	操作
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。カスタムパスを使用する場合は、sudoersのデフォルトのコンテンツがカスタムパスで更新されていることを確認してください。
オプションの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。

   [インストール前チェックをスキップ]チェックボックスを選択していない場合は、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するためにホストが検証されます。

   事前確認スクリプトでは、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. 指紋を確認し、 * 確認して送信 * をクリックします。

   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 *

ホストにマウントされているすべてのファイルシステムが自動的に検出され、[Resources]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の監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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。

SnapCenter Plug-in Loaderサービスの設定

SnapCenter Plug-in Loaderサービスは、SnapCenterサーバと対話するために、Linux用のプラグインパッケージをロードします。SnapCenter Plug-in Loaderサービスは、SnapCenter Plug-ins Package for Linux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	サポートされているログレベルを表示します。 指定できる値は、trace、debug、info、warn、error、致命的だ
spl_protocol	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	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ます。デフォルト値がない場合は、値を追加できます。
SKIP_JAVAHOME_UPDATE	SPLサービスはデフォルトで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_keystore_pass	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か、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。

パラメータ名	説明
spl_port	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に値を変更しないでください。
SnapCenterサーバホスト	SnapCenter サーバの IP アドレスまたはホスト名を表示します。
spl_keystore_path	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。
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。この数が指定した値を超える場合は、最後に変更された5、000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した場合、保持するファイル数は9999に設定されます。
JAVA_HOME	SPLサービスの開始に使用されるJAVA_HOMEディレクトリの絶対パスを表示します。 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。
最後の日数のログの保持	ログが保持されるまでの日数が表示されます。

パラメータ名	説明
enable_certificate_validation	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の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ファイルを変更できます。また、spl.propertiesファイルを確認し、ファイルを編集して、パラメータに割り当てられた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。
   - SnapCenter Plug-in Loaderサービスを開始します。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - SnapCenter Plug-in Loader サービスを停止します。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

       stopコマンドで-forceオプションを使用すると、SnapCenter Plug-in Loaderサービスを強制的に停止できます。ただし、既存の処理も終了するため、この処理を実行する場合は注意が必要です。

   - SnapCenter Plug-in Loader サービスを再起動します。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /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。
     - rootユーザとして、次のコマンドを実行します。
       `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - SnapCenter Plug-in Loader サービスで変更を探します。

- rootユーザとして、次のコマンドを実行します。
  `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Linuxホストで**SnapCenter Plug-in Loader**（**SPL**）サービスを使用して**CA**証明書を設定する

SPL 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、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、 CA 署名キーペアを SPL の信頼ストアと SnapCenter Plug-in Loader サービスを使用して設定して、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。

SPLでは、「/var/opt/snapcenter/spl/etc」にある「keystore.jks」ファイルをtrust-storeとkey-storeの両方として使用します。

SPLキーストアのパスワードと、使用中の**CA**署名キーペアのエイリアスを管理します。

- 手順 *
  1. SPLキーストアのデフォルトパスワードは、SPLプロパティファイルから取得できます。

     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ファイルのSPL_KEYSTORE_PASSキーについ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ます。

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を同じにする必要があります。

spl trust-storeに対するルート証明書または中間証明書の設定

SPL trust-store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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
 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 trust-
store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証明書のあとに中間CA証明書を追加する必要があります。

SPL trust-storeへの**CA**署名済みキーペアの設定

SPL trust-storeに対してCA署名付きキーペアを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/etcが格納されているフォルダに移動します。
  2. 「keystore.jks」ファイルを探します。
  3. キーストアに追加された証明書を一覧表示します。

```
 keytool -list -v -keystore keystore.jks
. 秘密鍵と公開鍵の両方が設定された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一覧表示します。
```

```
 keytool -list -v -keystore keystore.jks
. 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キーストアに含まれていることを確認します。
. CA証明書に追加し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ファイルのSPL_KEYSTORE_PASSキーの値です。

```
 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SPL_CERTIFICATE_ALIASキーに対して更新します。

4. SPL trust-storeにCA署名キーペアを設定したら、サービスを再起動します。

SPLの証明書失効リスト（**CRL**）を設定する

SPLの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で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. キーSPL_CRL_PATHに対して、spl.propertiesファイルのデフォルトディレクトリを変更および更新できます。
  2. このディレクトリには、複数のCRLファイルを配置できます。

     受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（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。

展開の詳細については、を参照してください "導入の概要"。

CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、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ファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリで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は、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

UNIXファイルシステムの保護の準備

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前に、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テクノロジを利用するには、ストレージデバイス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

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て実行できます。

Plug-in for UNIXファイルシステムを使用する前に、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。 "詳細"
- 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"

> 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の登録またはクラスタの登録を使用してSnapCenterに登録されるSVMは、それぞれ一意である必要があります。

- ホストを追加し、プラグインをインストールし、リソースを検出します。
- SnapCenterサーバを使用してVMware RDM LUNまたはVMDKにあるUNIXファイルシステムを保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。
- LinuxホストにJavaをインストールします。
- バックアップレプリケーションが必要な場合は、ONTAPでSnapMirrorとSnapVaultを設定します。

UNIXファイルシステムのバックアップ

バックアップに使用できるUNIXファイルシステムの検出

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ファイルシステムが自動的に検出されて[Resources]ページに表示されます。これらのファイルシステム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。

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）にある場合は、SnapCenter Plug-in for VMware vSphereを導入して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の導入"。

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*[パス]*を選択します。
3. [リソースの更新] をクリックします。

   ファイルシステムは、タイプ、ホスト名、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。

UNIX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UNIXファイルシステム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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。レプリケーション、スクリプト、および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と、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できます。

開始する前に

- SnapCenterのインストール、ホストの追加、ファイルシステムの検出、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場合は、SnapCenter管理者が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を割り当てておく必要があります。
- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

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* Unix File Systems *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. 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。
7. [Retention]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業

一定数のSnapshotを保持	[保持するSnapshotコピーの総数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshot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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。 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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。
Snapshotを特定の日数だけ保持	[Keep Snapshot copies for]*を選択し、Snapshotを削除するまでの日数を指定します。

アーカイブログバックアップを保持できるのは、バックアップの一部としてアーカイブログファイルを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	操作
ローカルSnapshotコピーの作成後にSnapMirrorを更新する	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。 このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。
ローカルSnapshotコピーの作成後に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。

フィールド	操作
セカンダリポリシーラベル	Snapshotラベルを選択します。 選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。 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。
エラー時の再試行回数	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のSnapshot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。

   プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを、_/opt/NetApp/snapcenter/scc/etc/allowed _ commands.config_pathから確認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。

10. 概要を確認し、 [完了] をクリックします。

UNIXファイルシステムのリソースグループの作成とポリシーの適用

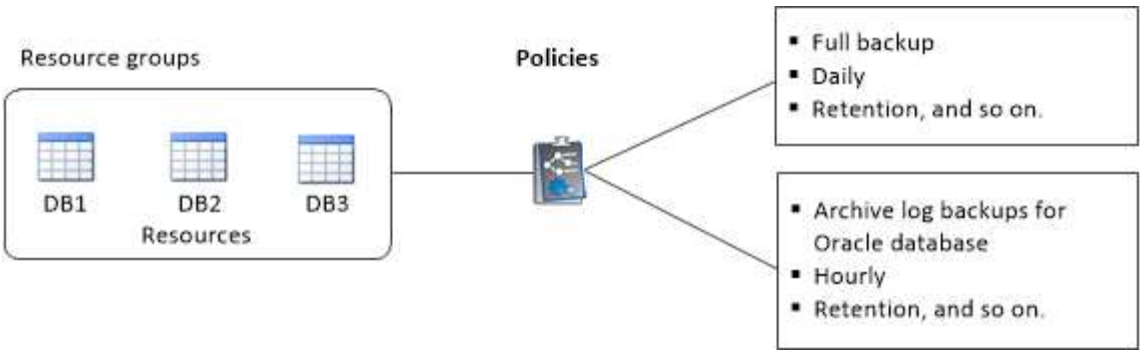
リソースグループはコンテナであり、バックアップして保護するリソースを追加します。リソースグループを使用すると、ファイルシステムに関連付けられているすべてのデータをバックアップできます。

タスクの内容

- 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。



- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirror Active Syncを使用しない新しいファイルシステムを、SnapMirror Active Syncを使用するリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいファイルシステムを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。

   c. チェックボックスを選択し、Snapshot名に使用するカスタムの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名にタイムスタンプが追加されます。

4. [リソース]ページで、*[ホスト]*ドロップダウンリストからUNIXファイルシステムの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。最近追加したリソースは、リソースリストを更新するまで使用可能なリソースのリストに表示されません。

5. [Available Resources]セクションからリソースを選択し、[Selected Resources]セクションに移動します。
6. [Application Settings]ページで、次の手順を実行します。

- [Scripts]の矢印を選択し、休止、Snapshot、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。
- 次のいずれかのバックアップ整合性オプションを選択します。
  - バックアップの作成前にファイルシステムにキャッシュされたデータがフラッシュされ、バックアップの作成時にファイルシステムで入出力操作が許可されないようにするには、*[ファイルシステム整合性]*を選択します。

    ファイルシステム整合性の場合、ボリュームグループに含まれるLUNに対して整合グループSnapshotが作成されます。

  - バックアップを作成する前にファイルシステムにキャッシュされたデータを確実にフラッシュする場合は、* Crash consistent *を選択します。

    リソースグループに別 々 のファイルシステムを追加した場合は、リソースグループ内の別 々 のファイルシステムのすべてのボリュームが整合グループに追加されます。

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. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
   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。

   サードパーティの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はサポートされません。

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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。

UNIXファイルシステムのバックアップ

いずれのリソースグループにも含まれていないリソースは、[Resources]ページから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*[パス]*を選択します。
3. をクリックし、ホスト名とUNIXファイルシステムを選択してリソースをフィルタリングします。
4. バックアップするファイルシステムを選択します。
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名に使用するカスタムの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名にタイムスタンプが追加されます。
6. [Application Settings]ページで、次の手順を実行します。
   - [Scripts]の矢印を選択し、休止、Snapshot、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。
   - 次のいずれかのバックアップ整合性オプションを選択します。
     - バックアップの作成前にファイルシステムにキャッシュされたデータがフラッシュされ、バックアップの作成時にファイルシステムで処理が実行されないようにするには、*[ファイルシステム整合性]*を選択します。
     - バックアップを作成する前にファイルシステムにキャッシュされたデータを確実にフラッシュする場合は、* Crash consistent *を選択します。
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。

      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. [Configure Schedules]列内をクリックし て、目的の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。
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。

   トポロジ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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    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。

UNIXファイルシステムリソースグループのバックアップ

リソースグループに定義されているUNIXファイルシステムをバックアップできます。リソースグループは、[Resources]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、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バックアップが作成されます。

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、をクリックしてタグを選択します。

   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。
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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    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。

UNIXファイルシステムのバックアップの監視

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。

UNIXファイルシステムのバックアップ処理を監視する

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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処理を監視する

[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。

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. [Activity]ペインでをクリックすると、 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

[Topology]ページで保護されているUNIXファイルシステムを表示する

リソースのバックアップ、リストア、またはクローニングを準備するときに、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、リストアされたファイルシステム、およびクローンが図で表示されると役立つことがあります。

- このタスクについて *

[Topology]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可能なすべてのバックアップ、リストアされたファイルシステム、およびクローンを確認できます。これらのバックアップ、リストアされたファイルシステム、およびクローンの詳細を表示し、それらを選択してデータ保護処理を実行できます。

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

- プライマリストレージにあるバックアップとクローンの数が表示されます。
- 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。
- 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、バックアップを4つだけ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。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。

- 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. [Summary]カードで、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の概要を確認します。

   [Summary Card]セクションには、バックアップとクローン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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   ファイルシステムが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

   SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

   - SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
   - フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

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、削除の各処理を実行します。

   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。

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。

プライマリストレージのバックアップとクローンの例

UNIXファイル・システムのリストアとリカバリ

UNIXファイルシステムのリストア

データ損失が発生した場合は、SnapCenterを使用してUNIX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 *
- 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表示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

"。

- SnapMirrorのアクティブな同期のリストア処理では、プライマリの場所からバックアップを選択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[パス]または[リソースグループ]*を選択します。
3. 詳細ビューまたはリソースグループの詳細ビューでファイルシステムを選択します。

   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：
   - NFSファイルシステムの場合、デフォルトでは*リストアが選択されています。また、[ボリュームリバート]または[高速リストア]*を選択することもできます。
   - NFS以外のファイルシステムの場合は、レイアウトに応じてリストア対象が選択されます。

     ファイルシステムのタイプとレイアウトによっては、バックアップ後に作成された新しいファイルをリストア後に使用できない場合があります。
7. [PreOps]ページで、リストアジョブの実行前に実行するリストア前のコマンドを入力します。
8. [PostOps]ページで、リストアジョブの実行後に実行するリストア後のコマンドを入力します。

   プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを、_/opt/NetApp/snapcenter/scc/etc/allowed _ commands.config_pathから確認する必要があります。

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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。

10. 概要を確認し、 [完了] をクリックします。

    リストア処理が失敗した場合、ロールバックはサポートされません。

ボリュームグループ上にあるファイルシステムをリストアしても、ファイルシステム上の古いコンテンツは削除されません。クローニングされたファイルシステムのコンテンツだけがソースファイルシステムにコピーされます。これは、ボリュームグループに複数のファイルシステムがあり、NFSファイルシステムがデフォルトでリストアされている場合に該当します。

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。

UNIXファイルシステムのリストア処理を監視する

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

UNIXファイルシステムのクローニング

UNIXファイルシステムのバックアップのクローニング

SnapCenterを使用すると、ファイルシステムのバックアップを使用してUNIXファイルシステムをクローニングできます。

開始する前に

- fstabファイルの更新をスキップするには、_/opt/NetApp/snapcenter/scc/etc _にある_agent.properties_ファイルで_skip_fstab_update_to * true *の値を設定します。
- 静的なクローンボリューム名とジャンクションパスを設定するには、_/opt/NetApp/snapcenter/scc/etc _にある_agent.properties_ファイルで_use_custom_clone_volume_name_format_の値を* true *に設定します。ファイルを更新したら、コマンドを実行してSnapCenter forカスタムプラグインサービスを再起動する必要があります `/opt/NetApp/snapcenter/scc/bin/scc restart`。

  例：このプロパティを指定しない場合、クローンボリュームの名前とジャンクションパスは<Source_volume_name>_<Timestamp>のようになりますが、<Source_volume_name>_<Clone_Name>になります。

  これにより、SnapCenterでfstabを更新したくない場合にfstabファイルを手動で更新できるように、名前が一定に保たれます。

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[パス]または[リソースグループ]*を選択します。
3. 詳細ビューまたはリソースグループの詳細ビューでファイルシステムを選択します。

   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、ローカルコピー（プライマリ）、ミラーコピー（セカンダリ）、バックアップコピー（セカンダリ）のいずれかの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. Location ページで、次のアクションを実行します。

フィールド	操作
クローンサーバ	デフォルトでは、ソースホストが入力されています。
クローンマウントポイント	ファイルシステムをマウントするパスを指定します。

7. [Scripts]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。

プラグインホストで使用可能なコマンドリストにコマンドが存在するかどうかを、_/opt/NetApp/snapcenter/scc/allowed _ commands.config_pathから確認する必要があります。

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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。
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。

クローンをスプリットする

SnapCenterを使用して、クローン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から独立します。

タスクの内容

- 中間クローンではクローンスプリット処理を実行できません。

  たとえば、データベースバックアップからClone1を作成したあとに、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は中間クローンになり、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、クローン2に対してはクローンスプリット処理を実行できます。

  Clone1は中間クローンではなくなるため、Clone2をスプリットしたら、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、その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 * （ * Resources * ）] ページで、 [表示（ View ）] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション	[表示] リストから [*Database] を選択します。

オプション	説明
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。

   リソーストポロジページが表示されます。

4. ビューで、クローンリソース（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を停止します。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てから、クローンスプリット処理を再試行してください。

   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。値はミリ秒単位で、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が実行中の場合、クローンスプリットの開始処理は失敗します。クローンスプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングまたは検証が失敗する"

UNIXファイルシステム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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗

- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、クローニング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. [**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。

Azure NetApp Filesで実行されているアプリケーションを保護

SnapCenterのインストールとクレデンシャルの作成

Azure仮想マシンへのSnapCenterのインストール

NetApp Support SiteからSnapCenterソフトウェアをダウンロードし、Azure仮想マシンにインストールできます。

開始する前に

- Azure Windows仮想マシンがSnapCenterサーバのインストール要件を満たしていることを確認します。詳細については、を参照してください "SnapCenterサーバのインストールの準備"。
- Azure NetApp Filesを初めてお使いで、既存のNetAppアカウントをお持ちでない場合は、SnapCenterソフトウェアにアクセスできるように登録済みであることを確認してください。

手順

1. 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 "NetAppサポートサイト"ます。
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サーバのインストールを開始します。

   インストールを開始すると、すべての事前チェックが実行され、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。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、エラーは修正する必要があります。

3. SnapCenterサーバのインストールに必要な値があらかじめ入力されていることを確認し、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中に、パスワードが自動的に生成されます。

   リポジトリデータベース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。

4. [今すぐインストール] をクリックします。

   無効な値を指定した場合は、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。

製品を登録してサポートを有効にする

NetAppを初めてご利用になり、NetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

手順

1. SnapCenterのインストール後、*[ヘルプ]>[バージョン情報]*に移動します。
2. [_About SnapCenter _]ダイアログボックスで、971で始まる20桁のSnapCenterインスタンスをメモします。
3. をクリックします https://register.netapp.com
4. [* I am not a registered NetApp Customer*] をクリックします。
5. 自分自身を登録するには、詳細を指定してください。
6. NetApp Reference SNフィールドは空白のままにします。
7. [Product Line]ドロップダウンから[* SnapCenter *]を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. [Submit （送信）] をクリックします。

SnapCenterでAzureクレデンシャルを作成する

Azure NetAppアカウントにアクセスするには、SnapCenterでAzureクレデンシャルを作成する必要があります。

Azureクレデンシャルを作成する前に、Azureでサービスプリンシパルを作成しておく必要があります。Azureクレデンシャルを作成するには、サービスプリンシパルに関連付けられたテナントID、クライアントID、およびシークレットキーが必要です。

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、クレデンシャルの作成に必要な次の情報を指定します。

フィールド	操作
クレデンシャル名	クレデンシャルの名前を入力します。
認証モード	ドロップダウンリストから*[Azure Credential]*を選択します。
テナントID	テナントIDを入力します。
クライアントID	クライアントIDを入力します。

フィールド	操作
クライアントシークレットキー	クライアントシークレットキーを入力します。

5. [OK]*をクリックします。

Azureストレージアカウントの設定

SnapCenterでAzureストレージアカウントを設定する必要があります。

Azureストレージアカウントには、サブスクリプションID、Azureクレデンシャル、およびAzure NetAppアカウントの詳細が含まれます。

Azure NetApp Filesには標準ライセンスと容量ベースライセンスは必要ありません。

手順

1. 左側のナビゲーションペインで、 * 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、**[Azure NetApp Files]***を選択し、[新規]*をクリックします。
3. クレデンシャル、サブスクリプションID、およびNetAppアカウントをそれぞれのドロップダウンリストから選択します。
4. [Submit （送信）] をクリックします。

クレデンシャルを作成してプラグインホストを追加

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使用するクレデンシャルと、データ保護処理を実行するためのクレデンシャルをそれぞれ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、 * 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、クレデンシャルの作成に必要な次の情報を指定します。

フィールド	操作
クレデンシャル名	クレデンシャルの名前を入力します。
認証モード	ドロップダウンリストから認証モードを選択します。

フィールド	操作
認証タイプ	パスワードベース*または SSHキーベース*（Linuxホストのみ）を選択します。
ユーザ名	ユーザ名を指定します。
パスワード	[パスワードベースの認証]を選択した場合は、パスワードを指定します。
SSH秘密鍵	SSHキーベースの認証を選択した場合は、秘密鍵を指定します。
sudo権限を使用	root以外のユーザのクレデンシャルを作成する場合は、[Use sudo privileges]チェックボックスを選択します。 これはLinuxユーザにのみ該当します。

5. [OK]*をクリックします。

SAP HANAデータベースを保護

ホストを追加して**SnapCenter Plug-in for SAP HANA Database**をインストールする

SnapCenterの[ホストを追加]ページを使用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。プラグインはリモートホストに自動的にインストールされます。

開始する前に

- 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、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。
- 一元化されたホストにインストールする場合は、SAP HANAクライアントソフトウェアがそのホストにインストールされていることを確認し、SAP HANAデータベースホストで必要なポートを開いてHDB SQLクエリをリモートで実行します。

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. [管理対象ホスト]*タブが選択されていることを確認します。
3. [追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

a. [Host Type]フィールドで、ホストタイプを選択します。

b. [Host name]フィールドに、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。

c. [Credentials]フィールドに、作成したクレデンシャルを入力します。

5. [Select Plug-ins to Install]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、詳細を指定します。

7. [Submit （送信）] をクリックします。

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。

9. インストールの進行状況を監視します。

SAP HANAデータベースの追加

SAP HANAデータベースは手動で追加する必要があります。

タスクの内容

プラグインが一元化されたサーバにインストールされている場合は、リソースを手動で追加する必要があります。SAP HANAプラグインがHANAデータベースホストにインストールされている場合は、HANAシステムが自動的に検出されます。

自動検出はHANAマルチホスト構成ではサポートされていません。追加するには一元化されたプラグイン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、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。

   a. リソースタイプとして、[Single Container]、[Multitenant Database Container]、または[Non-data Volume]のいずれかを入力します。

   b. SAP HANAシステムの名前を入力します。

   c. システムID（SID）を入力します。

   d. プラグインホストを選択します。

   e. SAP HANAシステムに接続するためのキーを入力します。

   f. HDBのセキュアなユーザストアキーを設定するユーザ名を入力します。

4. [Provide Storage Footprint]ページで、ストレージタイプとして* Azure NetApp Files *を選択します。

   a. Azure NetAppアカウントを選択します。

   b. 容量プールと関連付けられているボリュームを選択します。

   c. [保存（ Save ）] をクリックします。

5. 概要を確認し、 [完了] をクリックします。

SAP HANA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 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。

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。
   a. バックアップタイプを選択します。
      i. データベースの整合性チェックを実行する場合は、*[ファイルベースのバックアップ]*を選択します。
      ii. Snapshotテクノロジを使用してバックアップを作成する場合は、* Snapshotベース*を選択します。
   b. スケジュールタイプを指定します。
6. [Retention]ページで、選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

   セカンダリストレージへのレプリケーションはサポートされていません。

7. 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SAP HANAバックアップポリシーを適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを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。また、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、 [* 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	操作
名前	リソースグループの名前を入力します。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。

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。
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. [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。
   b. [スケジュールの設定]列で、設定するポリシーの**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。
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。
8. 概要を確認し、 [完了] をクリックします。

Azure NetApp Filesで実行されているSAP HANAデータベ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、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。
3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。
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]*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。
   b. [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。
   c. [Custom Configurations]*の矢印を選択し、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。

d. Snapshotコピーツール> SnapCenter without File System Consistency *を選択してSnapshotを作成します。

[ファイルシステムの整合性]オプションは、Windowsホストで実行されているアプリケーションにのみ適用されます。

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。
   b. 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]列で**を選択します  。
   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、*[OK]*を選択します。

      _policy_name_は 、選択したポリシーの名前です。

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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。
9. [今すぐバックアップ]*を選択します。
10. 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、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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

11. 「 * Backup * 」を選択します。
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。

SAP HANAリソースグループのバックアップ

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に対して実行されます。

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. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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、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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

b. 「 * Backup * 」を選択します。

5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

SAP HANAデータベースのリストアとリカバリ

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。

タスクの内容

自動検出されたHANAシステムでは、* Complete Resource *オプションを選択した場合、単一ファイルのSnapshotリストアテクノロジを使用してリストアが実行されます。[高速リストア]チェックボックスが選択されている場合は、ボリューム復帰テクノロジが使用されます。

手動で追加したリソースには、常にボリュームリバートテクノロジが使用されます。

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、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。
3. リソースを選択するか、リソースグループを選択してから、そのグループ内のリソースを選択します。
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. [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  。
6. [Restore Scope]ページで、*[Complete Resource]*を選択します。

   SAP HANAデータベースの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。

7. 自動検出されたHANAシステムの場合は、[Recovery scope]ページで次の操作を実行します。
   a. 可能な限り現在の時刻に近い状態にリカバリする場合は、* Recover to most recent state *を選択します。
   b. 指定した時点にリカバリする場合は、*[ポイントインタイムにリカバリ]*を選択します。
   c. 特定のデータバックアップにリカバリする場合は、*指定したデータバックアップにリカバリする*を選択します。
   d. 今すぐリカバリしない場合は、*[リカバリなし]*を選択します。
   e. ログバックアップの場所を指定します。
   f. バックアップカタログの場所を指定します。
8. [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。

9. [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。
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。

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。

SAP HANAデータベースのバックアップのクローニング

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。

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。
3. リソースまたはリソースグループを選択します。
4. [Manage Copies]ビューで、プライマリストレージシステムから*[Backups]*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。
   a. クローンHANAシステムを管理するためのSAP HANAプラグインがインストールされているホストを選択します。

      一元化されたプラグインホストでもHANAシステムホストでもかまいません。

   b. 既存のバックアップからクローニングするSAP HANA SIDを入力します。
   c. クローンボリュームをエクスポートするホスト名またはIPアドレスを入力します。
   d. SAP HANAデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

      クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

7. [Scripts]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。
   b. mountコマンドを入力して、ファイルシステムをホストにマウントします。

      ソースHANAシステムが自動検出され、クローンターゲットホストプラグインがSAP HANAホストにインストールされている場合、SnapCenterはクローンターゲットホスト上の既存のHANAデータボリ

ュームを自動的にアンマウントし、新しくクローニングされたHANAデータボリュームをマウントします。

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。
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。

ANFクローンはすでに選択したSnapshotから作成された独立したボリュームであるため、ANFクローンではクローンスプリットは無効になります。

Microsoft SQL Serverデータベースの保護

ホストを追加して**SnapCenter Plug-in for SQL Server Database**をインストールする

SnapCenterは、Azure NetApp Files上のSMB共有上のSQLインスタンスのデータ保護をサポートしています。スタンドアロン構成と可用性グループ（AG）構成がサポートされます。

SnapCenterの[ホストを追加]ページを使用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。プラグインはリモートホストに自動的にインストールされます。

開始する前に

- 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、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストのUACを無効に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** を選択します。
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」を選択します。
4. [Hosts]ページで、次の手順を実行します。
   a. [Host Type]フィールドで、ホストタイプを選択します。
   b. [Host name]フィールドに、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。
   c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
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、詳細を指定します。
7. [送信] を選択します。
8. を選択し、**[**ホストログディレクトリの設定**]**ページでホストログディレクトリの**SMB**パスを入力し、[保存]*をクリックします。

9. [送信]*をクリックし、インストールの進行状況を監視します。

SQL Server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 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。

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。
   a. バックアップタイプを選択します。
      i. 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する場合は、*[フルバックアップとログバックアップ]*を選択します。
      ii. データベースファイルのみをバックアップする場合は、*[フルバックアップ]*を選択します。
      iii. トランザクションログのみをバックアップする場合は、*[ログバックアップ]*を選択します。
      iv. 別の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、*[バックアップのみをコピー]*を選択します。
   b. 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。
      i. レプリカのみにバックアップする場合は、[Backup on preferred backup replica]を選択します。
      ii. バックアップのプライマリAGレプリカまたはセカンダリAGレプリカを選択します。
      iii. バックアップ優先度を選択します。
   c. スケジュールタイプを指定します。
6. [Retention]ページで、選択したバックアップタイプに応じて保持設定を指定します。

   セカンダリストレージへのレプリケーションはサポートされていません。

7. [Verification] ページで、次の手順を実行します。
   a. 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。
   b. Database consistency check options セクションで、次の操作を実行します。
      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。
      ii. すべての情報メッセージを非表示にするには、*[すべての情報メッセージを非表示（NO_INFOMSGS）]*を選択します。

デフォルトで選択されています。

iii. 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。

iv. 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 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および物理的な整合性をチェックします。

v. 内部データベースSnapshot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、*[内部データベースSnapshotコピー（TABLOCK）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]*を選択します。

c. [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。

d. 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。

8. 概要を確認し、 [完了] をクリックします。

リソースグループの作成とSQLバックアップポリシーの適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを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。また、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、 [* 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	操作
名前	リソースグループの名前を入力します。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。

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。
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. [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。
   b. [スケジュールの設定]列で、設定するポリシーの**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。
   d. Microsoft SQL Server スケジューラを選択します。
7. [Verification] ページで、次の手順を実行します。
   a. 検証サーバを選択します。
   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. または[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。
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。
9. 概要を確認し、 [完了] をクリックします。

Azure NetApp Filesで実行されているSQL Serverデータベ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、のページからバックアップすることができます。

開始する前に

Azure Windowsフェイルオーバークラスタにクラスタ IPが割り当てられていない場合やSnapCenterから到達できない場合は、ロードバランサを作成する必要があります。ロードバランサのIPが設定され、SnapCenterサーバから到達可能である必要があります。

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]ドロップダウンリストから*、[インスタンス]、または[可用性グループ]*を選択します。
3. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。
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。
   b. 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]列で**を選択します + 。
   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、*[OK]*を選択します。

      _policy_name_は 、選択したポリシーの名前です。

d. を選択し、スケジュール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. 検証サーバを選択します。
   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. または[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。
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。
7. 概要を確認し、 [完了] をクリックします。
8. [今すぐバックアップ]*を選択します。
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、バックアップに使用するポリシーを選択します。
   b. [Verify after backup]*を選択します。
   c. 「 * Backup * 」を選択します。
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。

SQL Serverリソースグループのバックアップ

複数のリソースで構成され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に対して実行されます。

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. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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、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。
   c. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

SQL Serverデータベースのリストアとリカバリ

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。データベースリストアは複数の段階からなるプロセスで、すべてのデータ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。

タスクの内容

リストアのターゲットインスタンスに、SMB ADActive Directoryドメインに属し、ファイル権限を適切に設定する権限があるActive Directoryユーザが設定されていることを確認する必要があります。クレデンシャルはSnapCenterでインスタンスレベルで設定する必要があります。

ターゲットインスタンスのSQL認証は、SMB構成ではサポートされません。ターゲットインスタンスは、必要な権限を持つActive Directoryユーザを使用してSnapCenterで設定する必要があります。

SnapCenter Plug-inサービスのサービスアカウントが Active Directoryユーザでない場合は、代替ホストへのリストアの実行中にソースボリュームを偽装して必要な処理を実行できるように、ソースボリュームを完全に制御できるユーザが必要です。

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、[表示]リストから*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。
4. [コピーの管理]ビューで、*[バックアップ]*をストレージシステムから選択します。
5. 表からバックアップを選択し、アイコンをクリックします  。
6. [Restore Scope]ページで、次のいずれかのオプションを選択します。
   a. 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、*[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する]*を選択します。
   b. バックアップを作成するホストまたは別のホストにある別のSQL Serverにデータベースをリストアする場合は、*[別のホストにデータベースをリストアする]*を選択します。
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。
   a. 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。
   b. 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場合は、*[すべてのログバックアップ*最新の状態へのバックアップリストア処理]を選択します。
   c. 「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。
   d. 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。
   e. 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。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
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。

10. 概要を確認し、 [完了] をクリックします。
11. [* Monitor * > * Jobs *] ページを使用してリストア・プロセスを監視します。

SQL Serverデータベースバックアップのクローニング

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。

タスクの内容

クローンのターゲットインスタンスに、SMB ADActive Directoryドメインに属し、ファイル権限を適切に設定する権限があるActive Directoryユーザが設定されていることを確認する必要があります。クレデンシャルはSnapCenterでインスタンスレベルで設定する必要があります。

ターゲットインスタンスのSQL認証は、SMB構成ではサポートされません。ターゲットインスタンスは、必要な権限を持つActive Directoryユーザを使用してSnapCenterで設定する必要があります。

SnapCenter Plug-inサービスのサービスアカウントがActive Directoryユーザでない場合は、クローンの実行中にソースボリュームを偽装して必要な処理を実行できるように、ソースボリュームを完全に制御できるユーザが必要です。

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. [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. データベースまたはリソースグループを選択します。
4. [コピーの管理]ビューページで、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。
5. バックアップを選択し、**を選択します  。
6. [クローンオプション]*ページで、必要なすべての詳細を指定します。
7. [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。

   SQL ServerデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

   クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. Logs ページで、次のいずれかのオプションを選択します。
   a. 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、*[なし]*を選択します。
   b. 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、*[すべてのログバックアップ]*を選択します。
   c. 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は、*[By log backups until *]を選択します。
   d. 指定した日時以降にトランザクションログを適用しない場合は、*[By specific date until]*を選択します。

9. [Script *]ページで、クローニング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スクリプトタイムアウト、パス、および引数を入力します。
10. [**Notification]** ページの **[*Email preference**] 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。
11. 概要を確認し、*[終了]*を選択します。
12. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

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に対して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。

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 *] または [* リソースグループ *] 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。
4. [コピーの管理]ビューページで、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。
5. バックアップを選択し、**を選択します  。
6. [クローンオプション]*ページで、必要なすべての詳細を指定します。
7. [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。

   SQL ServerデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

   クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. [Script *]ページで、クローニング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スクリプトタイムアウト、パス、および引数を入力します。
9. [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。
   - クローニング処理の実行頻度、クローニングスケジュールを開始するタイミング、クローニング処理を実行する曜日、スケジュールの有効期限、およびスケジュールの有効期限が切れたあとにクローンを削除するかどうかを指定する場合は、*[スケジュールの設定]*を選択します。
10. [**Notification]** ページの **[*Email preference**] 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。
11. 概要を確認し、*[終了]*を選択します。
12. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

Oracleデータベースの保護

ホストを追加して**SnapCenter Plug-in for Oracle Database**をインストールする

[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。プラグインはリモートホストに自動的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、ホストごとまたはクラスタごとに実行できます。クラスタ（Oracle RAC）にプラグインをインストールする場合、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。Oracle RAC One Nodeの場合は、アクティブノードとパッシブノードの両方にプラグインをインストール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. [管理対象ホスト]*タブが選択されていることを確認します。
3. [追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。
   a. [Host Type]フィールドで、ホストタイプを選択します。
   b. [Host name]フィールドに、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。
   c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. [Select Plug-ins to Install]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、詳細を指定します。
7. [Submit （送信）] をクリックします。
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。
9. インストールの進行状況を監視します。

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。

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。
   a. バックアップタイプとして、オンラインバックアップまたはオフラインバックアップを選択します。
   b. スケジュール頻度を指定します。
   c. 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。
   d. 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。
   e. アーカイブログの削除設定を指定します。
7. [Retention]ページで、保持設定を指定します。
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。
9. [Verification]ページで、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、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。
10. 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**Oracle**バックアップポリシーを適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを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。また、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、 [* 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	操作
名前	リソースグループの名前を入力します。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。
アーカイブログファイルのデスティネーション	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。

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. [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。
   b. [スケジュールの設定]列で、設定するポリシーの**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。
7. [Verification] ページで、次の手順を実行します。
   a. 検証サーバを選択します。
   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. または[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。
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。
9. 概要を確認し、 [完了] をクリックします。

Azure NetApp Filesで実行されているOracle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。

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]ドロップダウンリストから*[データベース]*を選択します。
3. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。
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。
   b. 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]列で**を選択します + 。
   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、*[OK]*を選択します。
5. [Verification] ページで、次の手順を実行します。
   a. 検証サーバを選択します。
   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. または[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。

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。
7. 概要を確認し、 [完了] をクリックします。
8. [今すぐバックアップ]*を選択します。
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、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。
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。

Oracleリソースグループのバックアップ

複数のリソースで構成され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に対して実行されます。

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. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
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、バックアップに使用するポリシーを選択します。
   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

Oracleデータベースのリストアとリカバリ

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。

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*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。
4. [Manage Copies]ビューで、プライマリストレージシステムから*[Backups]*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. 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を選択します。
   b. 次の操作を実行します。
      i. データベースファイルのみをリストアする場合は、*[すべてのデータファイル]*を選択します。
      ii. 表領域のみをリストアする場合は、*[表領域]*を選択します。
      iii. 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REDOログファイルをリストアする場合は、* Redo log files *を選択します。
      iv. [プラガブルデータベース]*を選択し、リストアするPDBを指定します。
      v. 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。
      vi. 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、*[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する]*を選択します。
      vii. バックアップを作成するホストまたは別のホストにある別のSQL Serverにデータベースをリストアする場合は、*[別のホストにデータベースをリストアする]*を選択します。
      viii. 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。
      ix. 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、次のいずれかのオプションを選択します。
   a. 最後のトランザクションまでリカバリする場合は、*[すべてのログ]*を選択します。
   b. 特定のSCNにリカバリする場合は、* Until SCN（System Change Number）*を選択します。
   c. 特定の日時にリカバリする場合は、*[日時]*を選択します。
   d. リカバリしない場合は*[リカバリなし]*を選択します。
   e. 外部アーカイブログファイルの場所を指定する場合は、*[Specify external archive log locations]*を選択します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
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。
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。

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ることなく、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。

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*または[リソースグループ]*を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
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。

   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. 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 *を選択します。
   b. 表領域のみをリストアする場合は、*[表領域]*を選択します。
   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、次のいずれかのオプションを選択します。
   a. 特定のSCNにリカバリする場合は、* Until SCN（System Change Number）*を選択します。
   b. 特定の日時にリカバリする場合は、*[日時]*を選択します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
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。
10. 概要を確認し、 [完了] をクリックします。
11. [* Monitor * > * Jobs *] ページを使用してリストア・プロセスを監視します。

ポイントインタイムリカバリを使用したプラガブルデータベースのリストアとリカバリ

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、破損またはドロップされたプラガブルデータベース（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。

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*または[リソースグループ]*を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
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。

   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. 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 *を選択します。

b. PDB内のPDBと表領域のどちらをリストアするかに応じて、次のいずれかの操作を実行します。

- PDBをリストアする場合は、*[Pluggable databases（PDB）]*を選択します。
- PDB内の表領域をリストアする場合は、*[Pluggable database（PDB）tablespaces]*を選択します。

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。
   a. 特定のSCNにリカバリする場合は、* Until SCN（System Change Number）*を選択します。
   b. 特定の日時にリカバリする場合は、*[日時]*を選択します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
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。
10. 概要を確認し、 [完了] をクリックします。
11. [* Monitor * > * Jobs *] ページを使用してリストア・プロセスを監視します。

Oracleデータベースバックアップのクローニング

SnapCenterを使用すると、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*または[リソースグループ]*を選択します。
3. データベースを選択します。
4. [Manage Copies]ビューページで、プライマリストレージシステムのバックアップを選択します。
5. データバックアップを選択し、**をクリックします  。
6. [Name]ページで、データベース（CDBまたは非CDB）をクローニングするか、プラガブルデータベース（PDB）をクローニングするかを選択します。
7. [Locations]ページで、必要な詳細を指定します。

   OracleデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

   クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. [Credentials]ページで、次のいずれかを実行します。
   a. [Credential name for sys user]で、クローンデータベースのsysユーザパスワードの定義に使用するクレデンシャルを選択します。
   b. 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認証が有効になっている場合は、ASMインスタンスのクレデンシャル名で*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できる「SYSASM」権限を持つユーザ

が設定されたOracle ASMクレデンシャルを選択します。

9. [Pre-Ops]ページでプリスクリプトのパスと引数を指定し、[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事前入力済みのデータベースパラメータの値を変更します。
10. クローンデータベースのリカバリを実行する場合は、[Post-Ops]ページで、**[Recover database]***と[Until Cancel]*がデフォルトで選択されます。
    a. [Until Cancel]*を選択すると、SnapCenterは、クローニング対象として選択されたデータバックアップのあとに、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でリカバリを実行します。
    b. [日付と時刻]*を選択すると、SnapCenterは指定した日時までデータベースをリカバリします。
    c. [Until SCN]*を選択すると、SnapCenterは指定したSCNまでデータベースをリカバリします。
    d. [外部アーカイブログの場所を指定する]*を選択すると、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。
    e. デフォルトでは、クローンデータベースにソースデータベースと区別する一意の番号（DBID）を生成する場合は、*[Create new DBID]*チェックボックスが選択されています。

       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、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カタログにクローンデータベースを登録すると、処理は失敗します。

    f. クローンデータベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、*[一時表領域用の一時ファイルを作成する]*チェックボックスを選択します。
    g. [クローンの作成時に適用するSQLエントリを入力してください]*に、クローン作成時に適用するSQLエントリを追加します。
    h. [クローン処理後に実行するスクリプトの入力]*で、クローン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指定します。
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。
12. 概要を確認し、*[終了]*を選択します。
13. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

プラガブルデータベースのクローニング

プラガブルデータベース（PDB）は、同じホストまたは代替ホスト上の別のターゲットCDBまたは同じターゲットCDBにクローニングできます。クローニングされた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。

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*または[リソースグループ]*を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
4. [Manage Copies]ビューページで、プライマリストレージシステムのバックアップを選択します。
5. 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*[PDBクローン]*を選択し、その他の詳細を指定します。
7. [Locations]ページで、必要な詳細を指定します。
8. [Pre-Ops]ページでプリスクリプトのパスと引数を指定し、[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事前入力済みのデータベースパラメータの値を変更します。
9. [Post-Ops]ページでは、クローンデータベースのリカバリが実行される場合、デフォルトで*[Until Cancel]*が選択されます。
   a. [Until Cancel]*を選択すると、SnapCenterは、クローニング対象として選択されたデータバックアップのあとに、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でリカバリを実行します。
   b. [日付と時刻]*を選択すると、SnapCenterは指定した日時までデータベースをリカバリします。
   c. [外部アーカイブログの場所を指定する]*を選択すると、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。
   d. デフォルトでは、クローンデータベースにソースデータベースと区別する一意の番号（DBID）を生成する場合は、*[Create new DBID]*チェックボックスが選択されています。

      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、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カタログにクローンデータベースを登録すると、処理は失敗します。

   e. クローンデータベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、*[一時表領域用の一時ファイルを作成する]*チェックボックスを選択します。
   f. [クローンの作成時に適用するSQLエントリを入力してください]*に、クローン作成時に適用するSQLエントリを追加します。
   g. [クローン処理後に実行するスクリプトの入力]*で、クローン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指定します。
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、電子メールを送信するシナリオを選択します。
11. 概要を確認し、*[終了]*を選択します。
12. 処理の進捗状況を監視するために、**[監視]>*[ジョブ]*を選択します。

Oracleデータベースのクローンをスプリットする

SnapCenterを使用して、クローン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から独立します。

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. クローンリソース（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。

プラガブルデータベースのスプリットクローン

SnapCenterを使用して、プラガブルデータベース（PDB）のクローンをスプリットできます。

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. リソースビューまたはリソースグループ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. [Manage Copies]ビューで、プライマリストレージシステムから*[Clones]*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。

NetAppでサポートされているプラグインの保護

NetAppでサポートされるプラグイン

NetAppでサポートされるプラグインの概要

NetAppでサポートされているプラグインを使用するか、使用しているアプリケーション用のカスタムプラグインを開発してから、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。NetAppでサポートされるプラグインは、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可能にします。

NetAppでサポートされるプラグインがインストールされている場合は、SnapCenterと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。NetAppでサポートされているプラグインは、WindowsとLinuxのどちらの環境でも使用できます。

SnapCenterCLIでは、NetAppでサポートされるプラグインコマンドはサポートされません。

NetAppにはStorageプラグインが用意されており、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ストレージ上のデータボリュームのデータ保護処理を実行できます。

NetAppでサポートされるプラグイン、カスタムプラグイン、およびストレージプラグインは、[ホストを追加]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。"

NetAppは、MongoDB、MySQL、PostgreSQL、Storage、MaxDB、 Sybase ASE、ORASCPM、MongoDB、DPGlueプラグイン。

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、関連するAPIのサポートが対象になります。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はサポート対象外です。

ガイドを参照して、独自のカスタムプラグインを作成できます "アプリケーション用のプラグインを開発" 。

NetAppでサポートされるプラグインとストレージプラグインの機能

NetAppでサポートされているプラグインをデータ保護処理に使用できます。

- NetApp対応プラグイン*
- 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します。

- 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 *

ストレージプラグインはデータ保護処理に使用できます。

- 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を作成します。
- 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

  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、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）を利用して、プライマリで作成されたSnapshotをONTAPセカンダリに更新します。

  ONTAPのプライマリとセカンダリには、ONTAP FAS、AFF、All SAN Array（ASA）、Select、Cloud ONTAPがあります。

- ONTAPボリューム、LUN、またはファイル全体をリカバリ

  ブラウズ機能またはインデックス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ていませんが、バックアップ範囲が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。

NetAppでサポートされるプラグイン機能

SnapCenterは、プラグインアプリケーションおよびストレージシステム上でNetAppテクノロジと統合されます。NetAppでサポートされているプラグインを操作するには、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、プラグインと環境全体で標準化され、一貫性があります。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**スナップショットテクノロジ

  SnapCenterでは、NetAppのSnapshotテクノロジとNetAppでサポートされているプラグインを使用してリソースがバックアップされます。Snapshotはストレージスペースを最小限しか消費しません。

NetAppでサポートされるプラグイン機能を使用すると、次の利点もあります。

- 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。
- RBACでサポートされるセキュリティと一元化されたロール委譲

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルの権限を付与することもできます。

- NetApp FlexCloneテクノロジを使用して、テストまたはデータ抽出に使用するリソ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できます。

  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。

- バックアップ作成時に、ONTAPの整合グループ（CG）Snapshot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可能

  1回の処理では、1つのホスト内のリソースが同じボリュームを共有する場合にSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成する機能。
- Windows環境でファイルシステムと整合性のあるSnapshotを作成する機能。

NetAppでサポートされるプラグイン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。NetAppでサポートされている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セツソク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セツソク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接続ボリューム
VMware ESXi	NFSとSANの両方にVVOLデータストアを配置 VVOLデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

NetAppでサポートされる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
  - ジョブ履歴の表示
  - ジョブの停止
  - lun attribute show
  - LUNの作成
  - lun delete
  - LUNジオメトリ
  - LUN igroupの追加
  - lun igroup create
  - lun igroup delete
  - LUN igroupの名前変更
  - lun igroup show
  - LUNマッピングの追加-レポートノード
  - LUNマッピングの作成
  - LUNマッピングの削除
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - LUN変更
  - ボリューム内でのLUNの移動
  - LUNオフライン
  - LUNオンライン
  - LUNのサイズ変更
  - LUNシリアル
  - lun show
  - ネットワークインターフェイス
  - SnapMirrorポリシーadd-rule
  - snapmirror policy modify-rule
  - snapmirror policy remove-rule
  - snapmirror policy show
  - SnapMirrorリストア
  - snapmirror show
  - snapmirror show-history
  - SnapMirrorの更新
  - snapmirror update-ls-set

- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create

- vserver export-policy rule show
- vserver export-policy show
- vserver iscsi connection show
- vserver show

- 読み取り専用コマンド： ONTAP 8.3.0 以降で必要な最小権限
  - ネットワークインターフェイス

NetAppでサポートされるプラグインに対応したSnapMirrorおよびSnapVaultレプリケーションのためのストレージシステムの準備

SnapCenterプラグインとONTAP SnapMirrorテクノロジを併用すると、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テクノロジを併用すると、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処理の完了後にSnapMirrorとSnapVaultの更新を実行します。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、ソースボリュームで参照されるデータブロックがONTAPからデスティネーションボリュームに転送されます。

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関係の詳細とその設定方法については、を参照して "ONTAPのドキュメント"ください。

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、Service Level Agreement（SLA；サービスレベルアグリーメント）、Recovery Time Objective（RTO；目標復旧時間）、Recovery Point Objective（RPO；目標復旧時点）によって決まります。

タスクの内容

SLAは、期待されるサービスレベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする

必要がある時間です。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ます。SLA、RTO、RPOは、データ保護戦略に影響します。

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が必要かどうかを決定し、整合グループSnapshotを削除するための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. ソースストレージシステムとSnapMirrorデスティネーションのSnapshotの保持期間を決定します。
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。

NetAppでサポートされるプラグインのバックアップ戦略

NetAppでサポートされている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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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、期待されるサービスレベルと、サービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対処方法を定義したものです。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ます。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つの部分があります。

- 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頻度）は、ポリシー設定の一部です。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タイミング）は、リソースまたはリソースグループの設定に含まれます。たとえば、リソースグループのポリシーで週単位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]*をクリックします。

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には、リソースのサイズ、使用されているボリュームの数、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、別のボリュームに大規模なリソースを配置した場合は、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それぞれ1つずつ作成できます。

手動で追加した**NetApp**でサポートされるプラグイン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、戦略を定義する必要があります。手動で追加したNetAppでサポートされるプラグインリソースには、2種類のリストア戦略があります。

手動で追加したNetApp対応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

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のあとに作成されたSnapshot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
- 選択したLUNのみをリストア

アプリケーション用のプラグインを開発

概要

SnapCenterサーバを使用すると、アプリケーションをSnapCenterのプラグインとして導入および管理できます。データ保護機能と管理機能を備えた SnapCenter サーバに、お好みのアプリケーションを接続できます。

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。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できます。

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、アプリケーション用のプラグインを作成します。
- 記述ファイルの作成
- 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する

すべての**API**呼び出しでの汎用プラグインの処理

API呼び出しごとに、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ログに記録
- データの整合性

プラグインパラメータを使用

API呼び出しごとに一連のパラメータがプラグインに渡されます。次の表に、各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 、または cloneVolAndLun などです
リソース	保護するリソースを一覧表示します。リソースはUIDとタイプで識別されます。リストは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：「 Instance1 、 Instance ； Instance2\\DB1 、 Database 」
app_name	使用しているプラグインを指定します。たとえば、DB2、MySQLなどです。SnapCenterサーバには、リストされているアプリケーションの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ときに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する場合に、単一障害でバックアップ処理を停止しないようにする場合に便利です。

パラメータ	目的
<resource_name> ____APP_INSTANY_USERNAME	リソースに対してSnapCenterクレデンシャルが設定されている。
<resource_name> _APP_INSTANY_PASSWORD	リソースに対してSnapCenterクレデンシャルが設定されている。
<resource_name> _<custom_param> です	すべてのリソースレベルのカスタムキー値は、先頭に「 <resource_name>_ 」を付けたプラグインで使用できます。たとえば、カスタムキーが「 MySQLDB 」という名前のリソースの「 MASTER_SLAVE 」である場合、このキーは MySQLDB_MASTER_SLAVE として使用できます

終了コードを使用する

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返します。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	要求された操作はサポートされていないか、
100	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選択されます。
101	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ログに記録

エラー・メッセージは、プラグインからSnapCenterサーバに渡されます。メッセージには、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

パラメータ	目的
警告	警告メッセージ
エラー	エラーメッセージ
デバッグ	デバッグメッセージ
トレース	トレースメッセージ

データの整合性を維持

カスタムプラグインでは、同じワークフローを実行してもデータが保持されます。たとえば、プラグインは休止の終了時にデータを格納でき、休止解除処理に使用できます。

保持するデータは、プラグインによって結果オブジェクトの一部として設定されます。 特定の形式に従っており、プラグイン開発の各スタイルで詳細に説明されています。

Perlベースの開発

Perlを使用してプラグインを開発するときは、特定の規則に従う必要があります。

- コンテンツは読み取り可能でなければなりません
- setenv、quiesce、およびunquiesceの必須処理を実装する必要がある
- 結果をエージェントに渡すには、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

実行可能な処理：

- setenv
- バージョン
- 休止
- 休止解除
- clone_pre、clone_post
- restore_pre、リストア
- クリーンアップ

一般的なプラグイン処理

結果オブジェクトの使用

すべてのカスタムプラグイン処理で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、および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;
```

データの整合性の維持

同じワークフローの実行中に、処理間（クリーンアップを除く）でデータを保持することができます。これにはキーと値のペアを使用します。データのキーと値のペアは結果オブジェクトの一部として設定され、同じワークフローの後続の操作で保持されて使用できます。

次のコード例では、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
```
各処理は、コンテンツを表示して保存するホストエージェントにメッセージを送信できます。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。複数行メッセージがサポートされています。

```
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;
```

プラグインスタブの使用

カスタムプラグインはプラグインスタブを公開する必要があります。これらは、ワークフローに基づいてSnapCenterサーバが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、環境と設定オブジェクトを設定します。 環境の解析や処理はここで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。Perl形式のプラグインでのみ必要です。
バージョン	オプション	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
検出	オプション	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や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。 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特定の形式で応答の一部として返します。このスタブは、アプリケーションがSnapDrive for Unixと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フレーバー）がサポートされています。AIX/Solaris（Unixフレーバー）はサポートされていません。
検出_完了	オプション	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や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。 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特定の形式で応答の一部として返します。このスタブは、アプリケーションがSnapDrive for Unixと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フレーバー）がサポートされています。AIXおよびSolaris（Unixフレーバー）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	このスタブは休止を実行します。つまり、アプリケーションをSnapshotを作成できる状態にします。これは、Snapshot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。このメタデータは、対応するストレージSnapshotでの後続のクローニング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することを意味する休止解除を実行します。これは、Snapshotの作成後に呼び出されます。
clone_pre	オプション	このスタブは、クローニング前タスクを実行します。これは、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	オプション	このスタブは、クローニング後のタスクを実行します。これは、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	オプション	このスタブは、リストア前のタスクを実行します。ここでは、組み込みのSnapCenterサーバリストアインターフェイスを使用しており、リストア処理の実行中にトリガー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	オプション	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します。これは、組み込みのSnapCenterサーバ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	オプション	このスタブは、バックアップ、リストア、またはクローン処理のあとにクリーンアップを実行します。クリーンアップは、通常のワークフロー実行中またはワークフローの障害発生時に実行できます。設定パラメータaction（backup、cloneVolAndLun、fileOrVolRestore）を参照して、クリーンアップが呼び出されるワークフロー名を推測できます。構成パラメータ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NULLではなく定義されている場合、ワークフローエラーの実行中にクリーンアップが呼び出されます。
APP_VERSION	オプション	このスタブは、 SnapCenter がプラグインによって管理されるアプリケーションバージョンの詳細を取得するために使用されます。

プラグインパッケージ情報

各プラグインには、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 = ();
```

運用

カスタムプラグインでは、setenv、バージョン、休止、休止解除など、さまざまな処理をコーディングできます。

setenv処理**setenv**ショリ

setenv処理は、Perlを使用して作成されたプラグインに必要です。ENVを設定し、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resourcesパラメータに指定されたリソースに対してアプリケーション休止処理を実行します。

```
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パラメータで確認できます。

```
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、プラグインを作成するためにPerl以外のプログラミング言語やスクリプト言語がサポートされています。これはネイティブスタイルプログラミングと呼ばれ、スクリプトファイルまたはバッチファイルを使用できます。

ネイティブ形式のプラグインは、以下に示す特定の規則に従う必要があります。

プラグインは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ー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 プラグインのサフィックスは .ps1 に、その他の Windows スクリプトのサフィックスは .cmd または .bat にする必要があり、ユーザによって実行可能である必要があります
- プラグインは、コマンドライン引数に対して「-quiesce」、「-unquiesce」のように応答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、結果をサーバーに返すために特定の構文を使用する必要があります。

一般的なプラグイン処理

エラーメッセージのロギング

各操作は、コンテンツを表示して保存するサーバーにメッセージを送り返すことができます。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。複数行メッセージがサポートされています。

形式：

```
SC_MSG#<level>#<timestamp>#<message>
SC_MESSAGE#<level>#<timestamp>#<message>
```

プラグインスタブの使用

SnapCenterプラグインにはプラグインスタブが実装されている必要があります。これらは、SnapCenterサーバが特定の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
休止	必須	このスタブは休止を実行します。これにより、アプリケーションがスナップショットを作成できる状態になります。これは、ストレージSnapshot処理の前に呼び出されます。
休止解除	必須	このスタブは休止解除を実行します。アプリケーションは通常の状態になります。この処理は、ストレージSnapshot処理のあとに呼び出されます。
clone_pre	オプション	このスタブは、クローニング前のタスクを実行します。ここでは、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おり、「clone_vol or clone_lun」アクションの実行時にのみトリガーされます。
clone_post	オプション	このスタブは、クローニング後のタスクを実行します。これは、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おり、「clone_volまたはclone_lun」処理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。
restore_pre	オプション	このスタブは、リストア前のタスクを実行します。ここでは、組み込みのSnapCenterリストアインターフェイスを使用しており、リストア処理の実行中にのみトリガーされます。

プラグインスタブ	オプション / 必須	目的
リストア	オプション	このスタブは、すべてのリストア処理を実行します。この要件は、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。リストア処理の実行中にトリガーされます。

例

Windows PowerShell

システムでスクリプトを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Set-ExecutionPolicyバイパスを設定し、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。

制限事項

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ときは、いくつか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
他のライブラリへの依存	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制限の理由

SnapCenterエージェントの目標は、継続的かつ安全で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望ましくない問題を引き起こす可能性があります。これらの問題は、特に物事を使いやすくすることを目的としている場合には、取り組むのが難しいです。プラグインの複雑さがそれほど複雑でない場合、開発者がエラーを導入した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、 SnapCenter エージェント自体と同じ JVM で実行されていることです。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に悪影響を及ぼす可能性があります。

サポートされる方法

方法	必須	説明	いつ誰に電話したの**?**
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。	SnapCenter サーバまたはエージェントがプラグインのバージョンを要求します。
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、これは、アプリケーションをSnapCenterサーバがバックアップ（スナップショットなど）を作成できる状態にすることを意味します。	SnapCenter サーバが Snapshot コピーを作成する前、または一般的なバックアップを実行します。
休止解除	はい	アプリケーションで休止解除を実行する必要があります。ほとんどの場合、これは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サーバがスナップショットを作成した後、または一般的にバックアップを実行した後。

方法	必須	説明	いつ誰に電話したの?
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処理を担当します。	SnapCenterサーバ上のワークフローが終了したとき（正常に完了したとき、または失敗したとき）。
clonePre	いいえ	クローニング処理の実行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）を使用した場合。
clonePost	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）を使用した場合。
restorePre	いいえ	は、リストア処理の呼び出し前に実行する必要があるアクションを実行する必要があります。	ユーザがリストア処理をトリガーしたとき。
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とき。
アプリケーションバージョン	いいえ	プラグインで管理されているアプリケーションのバージョンを取得します。	ASUPデータ収集の一環として、バックアップ/リストア/クローンなどのすべてのワークフローで使用できます。

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の設定

1. Eclipseで新しいJavaプロジェクト「TutorialPlugin」を作成する
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/フォルダに移動し、jars scAgent-5.0-core.jarおよび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> Javaクラスを選択します
   a. 名前に「TutorialPlugin」と入力します。
   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;
  }
}
```

必要なメソッドの実装

休止、休止解除、およびバージョンは、各カスタムJavaプラグインで実装する必要がある必須のメソッドです。

プラグインのバージョンを返すversionメソッドを次に示します。

```
@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、LoggerやContext Store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。ロガーを取得するには、final Logger logger=context.getLogger();を呼び出します。loggerオブジェクトは、logbackなど、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。この例では問題がなかったため、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マッピングできます。

resultオブジェクトには、次のパラメータが含まれています。

パラメータ	デフォルト	説明
構成	構成が空です	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。プラグインで更新するパラメータを指定できます。この変更が SnapCenter サーバの構成に実際に反映されるかどうかは、設定の APP_CONF_PERSISTENCE = Y または N パラメータに依存します。
終了コード	0	処理のステータスを示します。「 0 」は、操作が正常に実行されたことを示します。その他の値はエラーまたは警告を示します。
標準出力	リストが空です	これは、 stdout メッセージを SnapCenter サーバに返送するために使用できます。
標準エラー	リストが空です	このオプションを使用すると、 stderr メッセージを SnapCenter サーバに返送できます。
メッセージ	リストが空です	このリストには、プラグインがサーバーに返すすべてのメッセージが含まれています。SnapCenterサーバは、これらのメッセージをCLIまたはGUIに表示します。

SnapCenterエージェントは、すべての結果タイプに対してビルダーを提供し ("ビルダパターン"ます。これにより、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、サーバに返送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必要ない場合は、必要なパラメータのみを送信してください。各パラメータにはデフォルト値があるため、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サーバーにプラグインのバージョンを通知します。また、 result から継承されるため、 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	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	プラグインのパッチバージョンフィールド。
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

context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();	現在のワークフローで SnapCenter サーバによって使用されているワークフロー ID を返します。

コンテキストメソッド	目的
config getconfig();	SnapCenter サーバからエージェントに送信されている設定を返します。

ワークフロー**ID**

ワークフロー ID は、実行中の特定のワークフローを SnapCenter サーバが参照するために使用する ID です。

構成

このオブジェクトには、ユーザが SnapCenter サーバの設定で設定できるパラメータのほとんどが含まれます。ただし、セキュリティ上の理由から、これらのパラメータの一部はサーバ側でフィルタリングされる場合があります。次に、 Config にアクセスしてパラメータを取得する例を示します。

```
final Config config = context.getConfig();
String myParameter =
config.getParameter("PLUGIN_MANDATORY_PARAMETER");
```

""//MyParameter"に、SnapCenterサーバ上のconfigから読み込まれたパラメータが含まれるようになりました。config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で次のタスクを実行します。

1. プラグインのベース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 ）。
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、インストール先の jar ファイルのパスを指定します。 tutorial_plugin.jar プラグインのベースクラスは TutorialPlugin.class という名前で、同じ名前のフォルダにプラグインを追加する必要があります。

プラグインが他のライブラリに依存している場合は、次のフォルダを作成できます。lib/

プラグインが依存するjarファイル（データベースドライバなど）を追加できます。SnapCenter は、プラグインをロードすると、このフォルダ内のすべての jar ファイルを自動的に関連付けて、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で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保護を有効にすることができます。このチュートリアルで説明す

る手順に従って、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しておく必要があります。

プラグイン記述ファイルの作成

作成するプラグインごとに、説明ファイルが必要です。定義ファイルには、プラグインの詳細が定義されています。ファイル名はPlugin_descriptor.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重要度の使用

属性	説明
名前	プラグインの名前。英数字を使用できます。例：DB2、MySQL、MongoDB ネイティブ形式で作成され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、プラグイン名がMongoDB.shの場合は、名前をMongoDBと指定します。
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。例：1.0、1.1、2.0、2.1
DisplayName	SnapCenter サーバに表示されるプラグインの名前。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。
プラグインタイプ	プラグインの作成に使用した言語。サポートされている値は、Perl、Java、およびNativeです。ネイティブ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ます。
OSNAME	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 Linux です。1つのプラグインを複数のOSタイプ（Perlタイプのプラグインなど）に導入することができます。
osVersion	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。
リソース名	プラグインがサポートできるリソースタイプの名前。たとえば、データベース、インスタンス、コレクションなどです。

属性	説明
親	場合、 ResourceName は階層的に別のリソースタイプに依存し、 Parent は親の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の「Database」には親の「Instance」があります。
RequireFileSystemPlugin	YesまたはNo リストアウィザードにリカバリタブを表示するかどうかを指定します。
ResourceRequiresAuthentication	YesまたはNo ストレージの検出後にデータ保護処理を実行するために、自動検出されたリソースと自動検出されなかったリソースのどちらにクレデンシャルが必要かを指定します。
RequireFileSystemClone	YesまたはNo クローンワークフローで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。

カスタムプラグインDB2のPlugin_descriptor.xmlファイルの例を次に示します。

```
<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ファイルの作成

プラグインが開発されて記述子ファイルが作成されたら、プラグインファイルと Plugin_descriptor.xml ファイルをフォルダに追加して zip する必要があります。

ZIPファイルを作成する前に、次の点を考慮する必要があります。

- スクリプト名はプラグイン名と同じにする必要があります。
- Perl プラグインの場合、 ZIP フォルダにスクリプトファイルが格納されているフォルダと、記述ファイルがこのフォルダの外部にある必要があります。フォルダ名はプラグイン名と同じである必要があります。
- Perl プラグイン以外のプラグインを使用する場合は、 ZIP フォルダに記述子とスクリプトファイルが含まれている必要があります。
- OSのバージョンは数字である必要があります。

例：

- DB2プラグイン：db2.pmファイルと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、 Plugin_descriptor.xml ファイルをフォルダに追加して zip ファイルを保存します。

プラグインの**ZIP**ファイルのアップロード

プラグインを目的のホストに導入できるように、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。

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 ： *
- Upload-SmPluginPackageコマンドレット

  例：PS>Upload -SmPluginPackage -AbsolutePath c:\DB2_1.zip

  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"です。

カスタムプラグインの導入

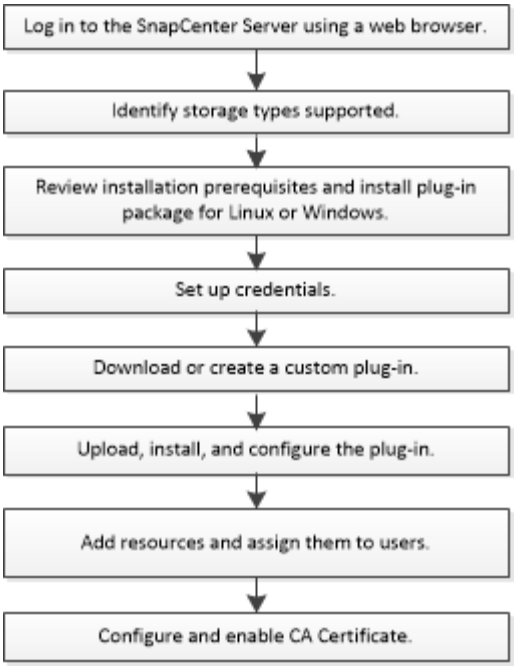
アップロードしたカスタムプラグインを、 * Add * および * Modify Host * ワークフローの一環として、目的のホストに導入できるようになりました。SnapCenter サーバに複数のバージョンのプラグインをアップロードして、特定のホストに導入するバージョンを選択できます。

プラグインをアップロードする方法の詳細については、を参照してください。 "ホストを追加してリモートホストにプラグインパッケージをインストールする"

NetApp対応プラグインのインストール準備

SnapCenter NetAppでサポートされるプラグインのインストールワークフロー

NetAppでサポートされるプラグインリソースを保護する場合は、SnapCenter NetAppでサポートされるプラグイン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"

ホストを追加して**NetApp**でサポートされるプラグイン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。NetAppでサポートされているプラグインは、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、開発者向け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"

- Java 11をLinuxホストまたはWindowsホストにインストール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ときに、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。
- ホストの追加処理を実行するクライアントホストに、NetAppでサポートされているプラグインが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

- NetAppでサポートされるプラグインの場合は、NetAppでサポートされる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ホストでは、SHA512ハッシュは_ C：\Program Files\NetApp\SnapManager Plug-in Creator\etc\custom_plugin_schecksum_list .txt_にあります

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_checksum_listは、SnapCenterによるNetApp対応プラグインのホストへのインストールに含まれています。

- アプリケーション用に作成されたNetApp対応プラグインの場合は、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ハッシュが生成されました。

のような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custom_plugin_checksum_listファイルの新しい行に追加しました。

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内のSHA512ハッシュのエントリ例を示します。

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Windowsホスト

- ローカル管理者Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- 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。

Linuxホスト

- rootユーザまたはroot以外のユーザに対して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 11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 11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ダウンロード"

"NetApp Interoperability Matrix Tool"

- 複数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_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- *C：\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt* SnapCenter ServerがWindowsホストにインストールされている場合。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc _ unix_plugins_checksum.txt _ SnapCenterサーバーがLinuxホストにインストールされている場合。

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、基本的なホストシステムのスペース要件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	Microsoft Windows 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB

項目	要件
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理のログは作成されません。
必要なソフトウェアパッケージ	• です。 ネットコア8.0.5 • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK 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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

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 • Oracle Linux • SUSE Linux Enterprise Server（SLES）
ホスト上のSnapCenterプラグイン用の最小RAM	1GB

項目	要件
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	2GB 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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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 11 Oracle JavaまたはOpenJDK を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/ spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenterバージョンと正しいパスに設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"

NetAppでサポートされるプラグインのクレデンシャルの設定

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースまたは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クレデンシャルをそれぞれ作成する必要があります。

開始する前に

- Linuxホスト

  Linuxホストにプラグインをインストールするには、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、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo Privilegesがあるroot以外のユーザに対して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

  プラグインをインストールする前にWindows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には、管理者権限（リモートホストに対する管理者権限を含む）を設定する必要があ

ります。

- NetAppでサポートされるプラグインアプリケーション

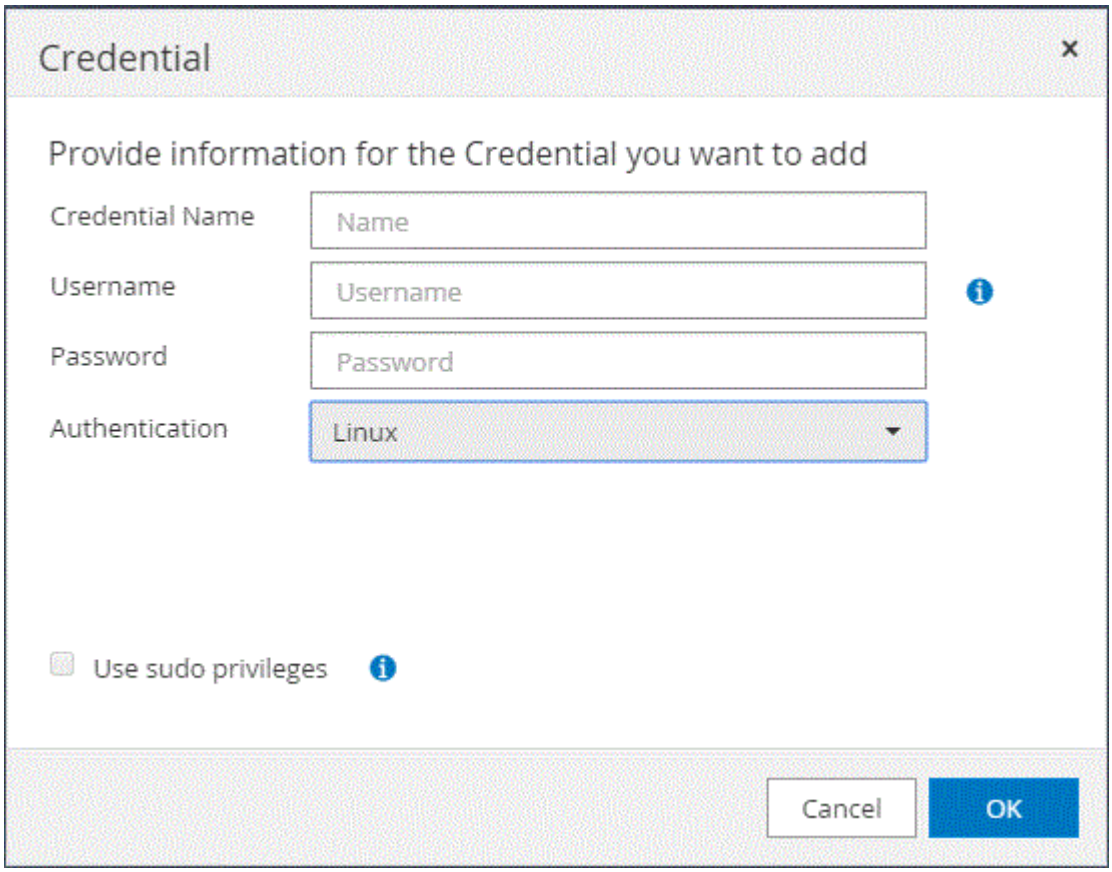
  プラグインは、リソースの追加時に選択または作成されたクレデンシャルを使用します。データ保護処理中にクレデンシャルが不要なリソースの場合は、クレデンシャルを「 * なし」に設定できます。

タスクの内容

個 々 のリソースグループのクレデンシャルを設定し、ユーザ名に完全なadmin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の権限を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	操作
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	操作
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。ユーザ名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	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ユーザのみに適用されます。

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、必要に応じて[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を割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- Windows Server 2016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 2016以降のホストが必要です。

手順

1. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
      .. コンピュータオブジェクトをグループに追加します。
      .. 作成したユーザグループを使用してgMSAを作成します。
      ```

      例えば、

      ```
      New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
      -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      .. コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。
      ```

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

NetApp対応プラグインのインストール

ホストを追加してリモートホストにプラグインパッケージをインストールする

[SnapCenter][ホストの追加]ページを使用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。プラグインはリモートホストに自動的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、ホストごとまたはクラスタごとに実行できます。

開始する前に

- この処理は、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実行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する必要があります。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理Privilegesを使用してgMSAを設定する必要があります。

"Windows Server 2016以降でカスタムアプリケーション用にグループ管理サービスアカウントを設定する"

タスクの内容

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、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。

手順

1. 左側のナビゲーションペインで、 **Hosts** を選択します。
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」を選択します。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホストタイプを選択します。 • ウィンドウ • Linux NetAppでサポートされているプラグインは、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が適切に設定されているかどうか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環境では、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場合、そのホストがサブドメインの一部であるときは、FQDNを指定する必要があります。

フィールド	操作
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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定する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。

   リストから次のプラグインをインストールできます。

   - MongoDB
   - ORASCPM（Oracleアプリケーションとして表示）
   - SAP ASE
   - ORASCPM
   - SAP MaxDB
   - ストレージ

6. （オプション）*[その他のオプション]*を選択して、他のプラグインをインストールします。

フィールド	操作
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	操作
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の場合、デフォルトパスはです `/opt/NetApp/snapcenter`。 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]セクションで、*[Browse]*を選択し、zip形式のカスタムプラグインフォルダを選択します。 zip形式のフォルダには、カスタムプラグインコードと記述子.xmlファイルが含まれています。 Storage Plug-inの場合は、フォルダに移動し *`C:\ProgramData\NetApp\SnapCenter\Package Repository`* て選択します `Storage.zip`。 ii. [アップロード]*を選択します。 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。
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。

フィールド	操作
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	Windowsホストで、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$の形式で指定してください。 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. [送信] を選択します。

   [インストール前チェックをスキップ]*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バージョン、場所（Windowsプラグインの場合）、およびJava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、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\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、*[確認して送信]*を選択します。

   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。

9. 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logsにあり `/custom_location/snapcenter/` ます。

コマンドレットを使用した複数のリモートホストへの**SnapCenter Plug-in Package for Linux / Windows**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、複数のホストにSnapCenter Plug-in Package for Linux / Windowsを同時にインストールできます。

開始する前に

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。
4. 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、**NetApp**でサポートされているプラグインを**Linux**ホストにインストールする

NetAppでサポートされているプラグインは、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。SnapCenter UIからの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環境では、NetAppでサポートされるプラグインを、コマンドラインインターフェイス（CLI）を使用して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。

手順

1. SnapCenter Plug-ins Package for Linuxインストールファイル（snapcenter_linux_host_plugin.bin）をC：\ProgramData\NetApp\SnapCenter\Package RepositoryからNetApp対応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、SnapCenterサーバにホストを追加します。

   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、NetAppでサポートされているプラグインをアップロードします。

   NetAppでサポートされるプラグインは、のセクションを参照してUIからアップロードできます "ホストを追加してリモートホストにプラグインパッケージをインストールする" 。

   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"です。

NetApp対応プラグインのインストールステータスの監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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証明書の設定

CA証明書CSRファイルの生成

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のブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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の完了	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」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

証明書サムプリントは、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進数の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から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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      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での**CA**証明書の設定

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、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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストのプラグインサービスとバインドします。

   ```
   > $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ホストでの**NetApp**でサポートされるプラグインサービスの**CA**証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中のCA署名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ます。

   カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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を含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   ```
   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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

手順

1. カスタムプラグインキーストア/opt/NetApp/snapcenter/scc/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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SCC_CERTIFICATE_ALIASキーに対して更新します。

8. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（**CRL**）を設定する

タスクの内容

- 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で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/scc/etc/crl」です。

手順

1. crl_pathキーに対して、agent.propertiesファイルのデフォルトディレクトリを変更および更新できます。

   このディレクトリには、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されます。

NetAppでサポートされるプラグインサービス（**Windows**ホスト）用の**CA**証明書の設定

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の管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

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キーストアのパスワードと使用中の**CA**署名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。

4. パスワードを変更したら、サービスを再起動します。

   カスタムプラグイン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を同じにする必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

   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ます。

ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへの**CA**署名キーペアの設定

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。

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一覧表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

   keytool -list -v キーストア *.JKS*

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルのキーkeystore_passの値です。

*keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

8. *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SCC_CERTIFICATE_ALIASキーに対して更新します。

9. 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したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト（**CRL**）を設定する

タスクの内容

- 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で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は、複数のCRLファイルを配置できます。

   受信証明書は、各CRLに対して検証されます。

プラグインに対して**CA**証明書を有効にする

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証明書の検証を有効にする必要があります。

開始する前に

- 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. プラグインホストを1つまたは複数選択します。
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]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間

の接続のステータスを示します。

- * *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。
- ** は、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。
- ** は、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場合は、データ保護処理が正常に完了しています。

データ保護の準備

NetAppでサポートされるプラグインを使用するための前提条件

SnapCenter NetAppでサポートされるプラグインを使用する前に、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、プラグインホストにJava 11をインストールします。
- データパス（LIF）が複数ある場合や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な場合は、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。

  ポート9090は、SnapCenterで必要な他のポートに加えて、NetAppでサポートされるプラグイン用にリザーブする必要があります。

NetAppでサポートされる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、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- リソースとは、SnapCenterでバックアップまたはクローニングするデータベース、Windowsファイルシステム、VM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できます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを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、そのグループのポリシーを1つ以上選択します。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。

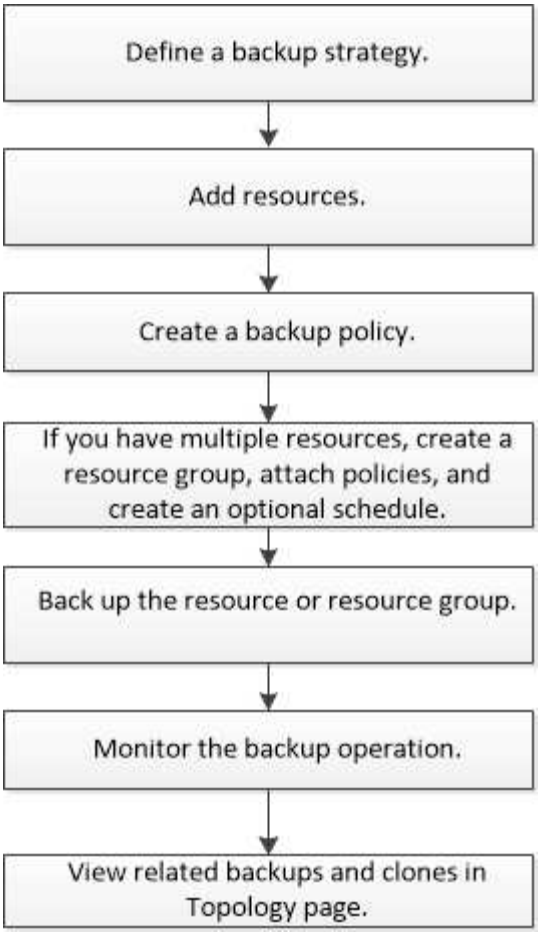
リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、すべてのデータベースまたはホストのすべてのファイルシステムをバックアップする場合は、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソースグループを作成します。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。リソースグループを作成してポリシーを適用する際に、ファイルベースのバックアップを1日1回実行するようにリソースグループを設定し、別のスケジュールでSnapshotベースのバックアップを1時間ごとに実行するように設定します。

NetAppでサポートされているプラグインリソースのバックアップ

NetAppでサポートされているプラグインリソースのバックアップ

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、 "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

NetAppがサポートするプラグインにリソースを追加する

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がリソースに含まれる場合があります。

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。
- そうだろうな "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。

手順

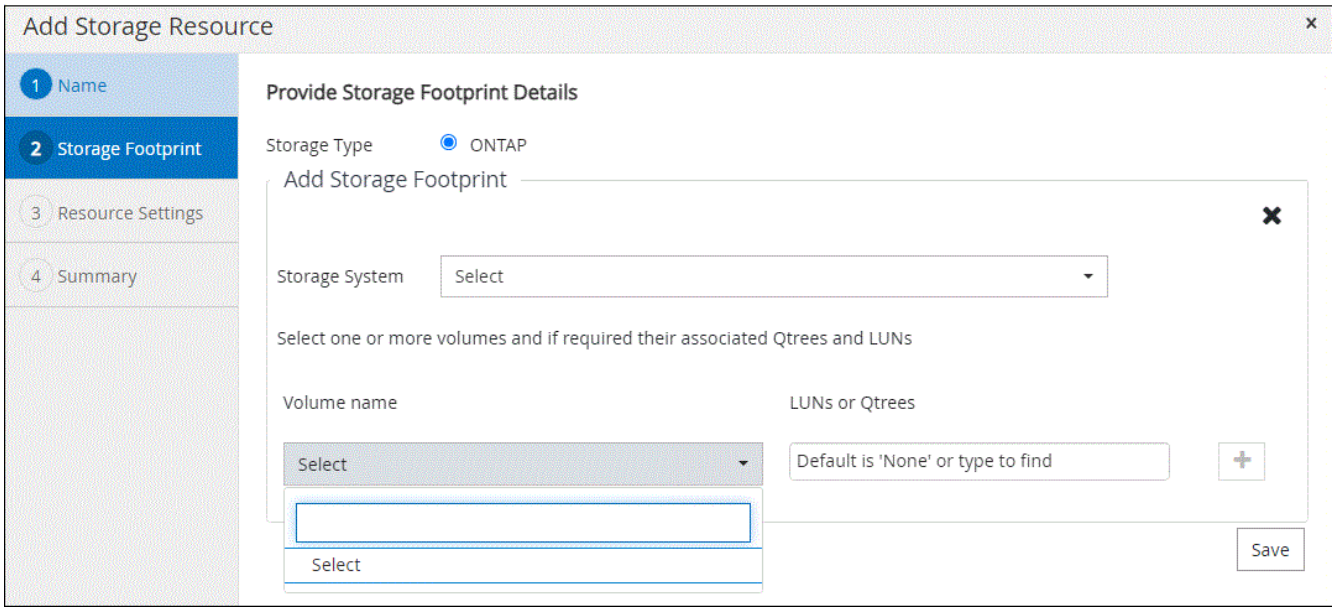
1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [リソース]ページで、*[リソースの追加]*を選択します。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
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。
タイプ	タイプを選択します。タイプは、プラグインの説明ファイルに従ってユーザー定義されています。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は、インスタンスの詳細を入力します。
クレデンシャル名	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します。
マウントパス	リソースがマウントされているマウントパスを入力します。これは、Windowsホストにのみ該当します。

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。

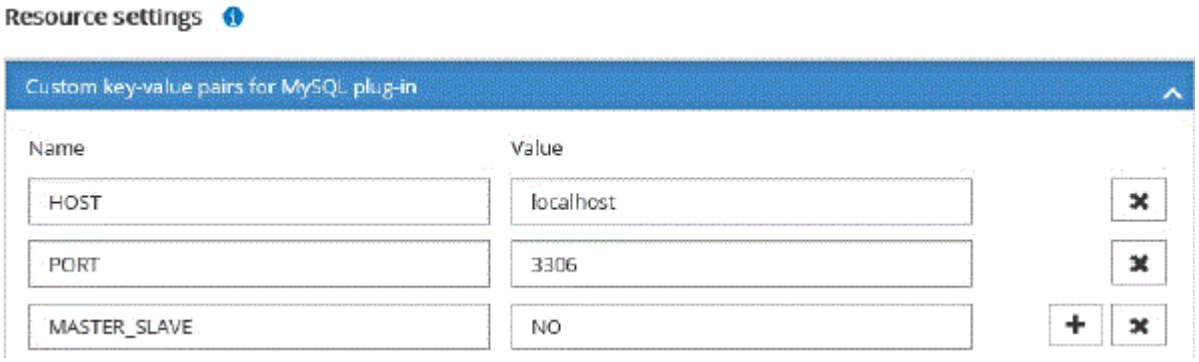
   オプション：他のストレージシステムからボリューム、LUN、およびqtreeを追加する場合は、アイコンを選択します + 。

   NetAppでサポートされているプラグインでは、リソースの自動検出がサポートされていません。物理環境と仮想環境のストレージの詳細も自動検出されません。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. [Resource Settings]ページで、リソースのカスタムのキーと値のペアを指定します。

   カスタムキー名が大文字であることを確認します。



   各プラグインパラメータについては、を参照してください。 "リソースを構成するパラメータ"

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。

SnapCenter以外でデータベースの名前が変更された場合は、リソースを更新する必要があります。

終了後

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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

リソースを追加したら、リソースの詳細を変更できます。NetAppでサポートされる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。

リソースを構成するパラメータ

プラグインを手動で追加する場合は、[Resource Settings]ページで次のパラメータを使用してリソースを設定できます。

MongoDB向けプラグイン

リソース設定：

- MongoDB_APP_SERVER=（リソースタイプが共有クラスタの場合）または
  はMongoDB_ReplicaSet_SERVER=（リソースタイプがレプリカセットの場合）
- oplog_path=（MongoDB.propertiesfileから提供される場合はオプションパラメータ）
- MongoDB_authentication_type=（LDAP認証の場合はplain、その他の場合はNone）

MongoDB.propertiesファイルには、次のパラメータを指定する必要があります。

- disable_starting_stoping_services=
  - n：プラグインによって開始/停止サービスが実行される場合。
  - ユーザがSTART/** STOPサービスを実行した場合はY。
  - オプションのパラメータをデフォルト値としてNに設定します。
- oplog_path_=（SnapCenterでカスタムのキーと値のペアとしてすでに指定されている場合はオプションパラメータ）

MaxDB用プラグイン

リソース設定：

- XUSER_ENABLE(Y|N)データベースユーザにパスワードを要求しないように、MaxDBのxuserの使用を有効または無効にします。
- HANDLE_LOGWRITER(Y|N)一時停止Logwriter(N)または再開Logwriter(Y)操作を実行します。
- DBMCLICMD（path_to_dbmcli_cmd）は、MaxDBのdbmcliコマンドへのパスを指定します。設定しない場合は、検索パスのdbmcliが使用されます。

  Windows環境では、パスは二重引用符（"…"）で囲む必要があります。

- SQLCLICMD（path_to_sqlcli_cmd）は、MaxDB sqlcliコマンドへのパスを指定します。パスが設定されていない場合は、検索パスにsqlcliが使用されます。
- MaxDB_UPDATE_HIST_LOG (Y|N)は、MaxDBバックアッププログラムにMaxDB履歴ログを更新するかどうかを指示します。
- MaxDB_CHECK_SNAPSHOT_DIR：例、SID1：DIRECTORY [、DIRECTORY …]；[SID2：DIRECTORY [、DIRECTORY …] Snap CreatorのSnapshotコピー処理が成功したこと、およびSnapshotが作成されたことを確認します。

  この環境 NFS のみ。このディレクトリには、 .snapshot ディレクトリが含まれている場所を指定する必要があります。複数のディレクトリを指定する場合は、カンマで区切って指定できます。

  MaxDB 7.8 以降のバージョンでは、データベースバックアップ要求がバックアップ履歴で失敗とマークされています。

- maxDB_backup_templates：各データベースのバックアップテンプレートを指定します。

  テンプレートが存在し、外部タイプのバックアップテンプレートである必要があります。MaxDB 7.8以降でスナップショット統合を有効にするには、MaxDBバックグラウンドサーバ機能があり、外部タイプのMaxDBバックアップテンプレートがすでに設定されている必要があります。

- MaxDB_BG_SERVER_PREFIX：バックグラウンドサーバ名のプレフィックスを指定します。

  MaxDB のバックアップテンプレートパラメータを設定する場合は、 MaxDB の BG_server_prefix パラメータも設定する必要があります。プレフィックスを設定しない場合は、デフォルト値na_bg_が使用されます。

Sybase ASE用プラグイン

リソース設定：

- sybase_server（data_server_name）は、Sybaseデータサーバ名を指定します（isqlコマンドの-Sオプション）。たとえば、p_testのように指定します。
- sybase_databases_exclude（db_name）を使用すると、「all」構成要素が使用されている場合にデータベースを除外できます。

  複数のデータベースを指定するには、セミコロンで区切ったリストを使用します。例：pubs2;test_db1。

- sybase_user: user_nameには'isqlコマンドを実行できるオペレーティング・システム・ユーザを指定します

  UNIXの場合は必須です。このパラメータは、Snap Creatorエージェントのstartコマンドとstopコマンドを実行するユーザ（通常はrootユーザ）とisqlコマンドを実行するユーザが異なる場合に必要です。

- Sybase_Tran_dump db_name：directory_pathを使用すると'スナップショットの作成後にSybaseトランザクションダンプを実行できます例：pubs2:/sybasedumps/pubs2

  トランザクションダンプが必要な各データベースを指定する必要があります。

- Sybase_Tran_dump_compress (Y|N) Sybaseトランザクションダンプのネイティブ圧縮を有効または無効にします。
- Sybase_ISQL_CMD（たとえば、/opt/Sybase/OCS-15_0/bin/isql）は、isqlコマンドへのパスを定義します。
- Sybase_exclude_tempdb（Y|N）を使用すると、ユーザが作成した一時データベースを自動的に除外できます。

Oracleアプリケーション向けプラグイン（**ORASCPM**）

リソース設定：

- sqlplus_cmdは、sqlplusへのパスを指定します。
- ORACLE_DATABASESには、バックアップするOracleデータベースと対応するユーザ（database：user）が一覧表示されます。
- CNTL_FILE_BACKUP_DIRは、制御ファイルのバックアップ先ディレクトリを指定します。
- ORA_TEMPは、一時ファイルのディレクトリを指定します。
- ORACLE_HOMEには、Oracleソフトウェアがインストールされているディレクトリを指定します。
- archive_log_onlyは、アーカイブログをバックアップするかどうかを指定します。
- oracle_backup_modeは、オンラインバックアップとオフラインバックアップのどちらを実行するかを指定します。

NetAppでサポートされるプラグインリソースのポリシーの作成

SnapCenterを使用してNetAppでサポートされる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。

開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、NetAppでサポートされる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には、Storage Virtual Machine（SVM）を割り当てる必要があります。

  Snapshot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の両方に対応する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。

- 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。

タスクの内容

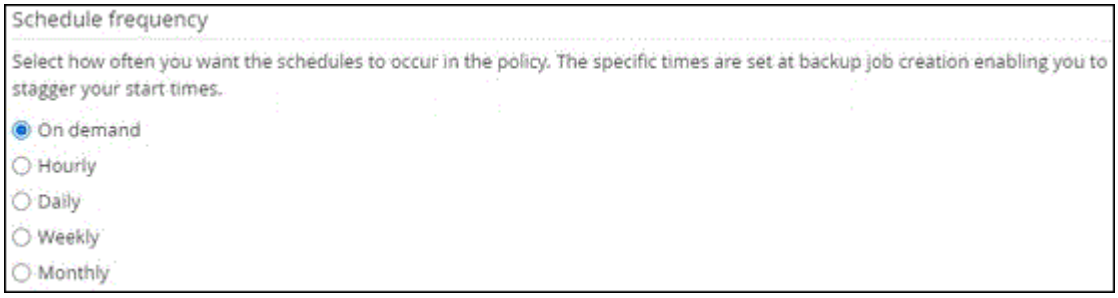
- バックアップポリシーは、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。レプリケーション、スクリプト、アプリケーション設定を指定することもできます。
- ポリシーでオプションを指定することで、別のリソースグループにポリシーを再利用して時間を節約できます。
- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

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）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ができます。



午前2時にスケジュールを設定している場合、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値は複数指定できます。

6. ページで、[Backup Type]*ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業
一定数のSnapshotを保持	[保持するSnapshotコピーの総数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshot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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。 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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。

状況	作業
Snapshotを特定の日数だけ保持	[Keep Snapshot copies for]*を選択し、Snapshotを削除するまでの日数を指定します。
Snapshotコピーのロック期間	[Snapshot locking period]を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

7. [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	操作
• 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は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をリストア処理の対象としてデスティネーションで選択すると、「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。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。 [Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 を参照して "NetAppでサポートされている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[Topologyページで表示する"]

フィールド	操作
• 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。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、「SnapVaultデスティネーションでSnapshotをWORM状態にコミットする」を参照してください。 を参照して "NetAppでサポートされている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[Topologyページで表示する"]
• 二次ポリシーラベル *	Snapshotラベルを選択します。 選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。 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のSnapshot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. 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、バックアップおよび保護するリソースを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するすべてのデータを同時にバックアップできます。また、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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、複数のリソースグループにHRをタグとして追加した場合、そのHRタグに関連付けられているすべてのリソースグループを後から検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名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。

   これは、画面上の情報をフィルタリングするのに役立ちます。

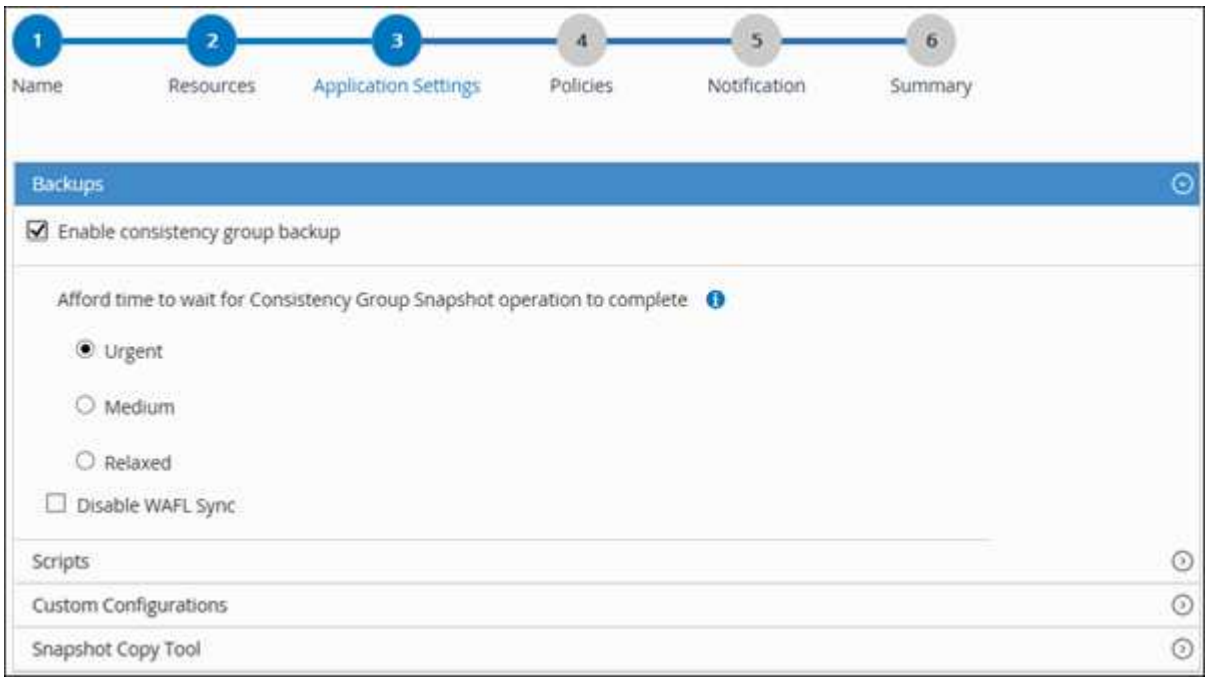
5. [Available Resources]セクションからリソースを選択し、右矢印を選択して[Selected Resources]セクションに移動します。
6. オプション：[アプリケーションの設定]ページで、次の手順を実行します。

   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、次のタスクを実行します。

フィールド	操作
整合グループSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間として、[Urgent]、[Medium]、または[Relaxed]のいずれかを選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+



a. [Scripts]の矢印を選択し、休止、Snapshot、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	（Y/N）	アーカイブログ管理でアーカイブログを削除できます。
アーカイブログの保持	日数	アーカイブログを保持する日数を指定します。 この設定はNTAP_SNAPSHOT_RETENTIONS 以上である必要があります。

パラメータ	設定	説明
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。
ARCHIVE_LOG_EXT	ファイル拡張子	アーカイブログファイルの拡張子の長さを指定します。 たとえば、アーカイブログが LOG_BACKUP _0_0_0_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

c. Snapshotコピーツール*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、ファイルシステムを整合性のある状態にしてからSnapshotを作成します。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：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * を選択します。
Snapshotを作成するためにホストで実行するコマンドを入力します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。

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. 列で、設定するポリシーの*を選択します + 。

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。サードパーティの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。

NetAppでサポートされているプラグインリソースを個別にバックアップする

どのリソースグループにも含まれていない個 々 のNetAppサポートプラグインリソースは、[Resources]ページから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できます。また、リソースにポリシーが適用され、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。

開始する前に

- 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。

SnapCenter UI

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、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。そのあとにをクリックすると、フィルタ ペインが閉じます。
3. バックアップするリソースをクリックします。
4. カスタムの名前を使用する場合は、[Resource]ページで*[Use custom name format for Snapshot copy]*チェックボックスを選択し、Snapshot名のカスタムの名前形式を入力します。

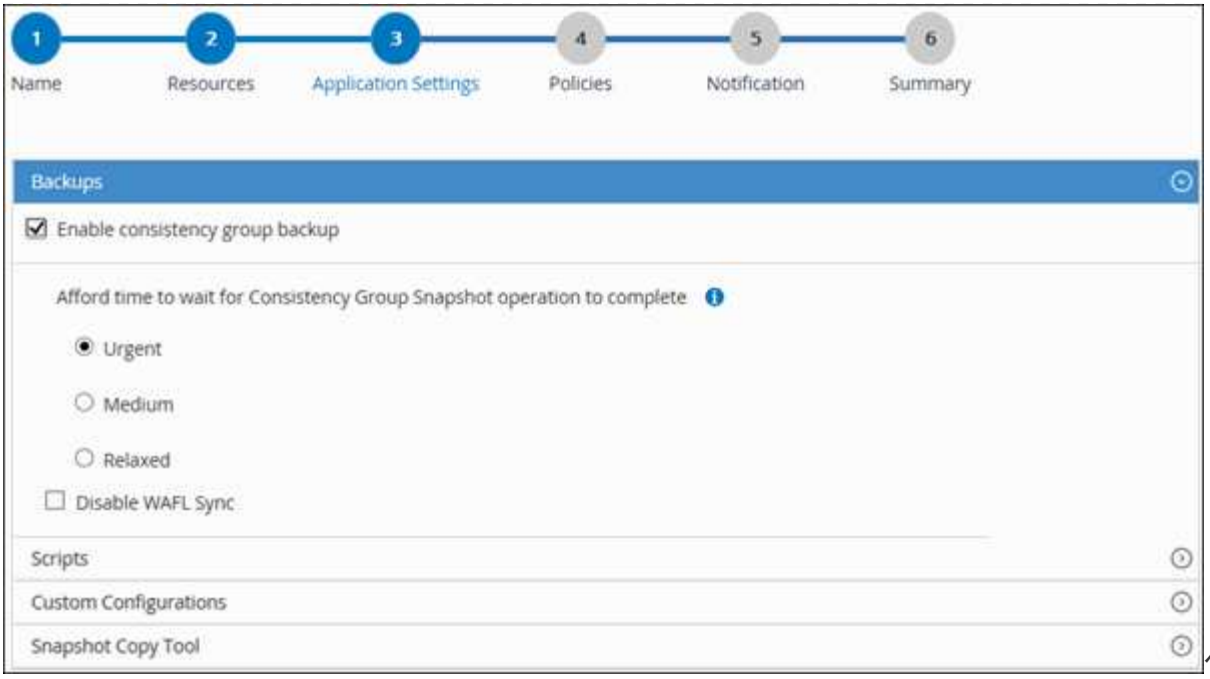
   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名にタイムスタンプが追加されます。
5. [アプリケーションの設定] ページで、次の操作を行います。

   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、次のタスクを実行します。

フィールド	操作
整合グループSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間として、[Urgent]、[Medium]、または[Relaxed]のいずれかを選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+



ページ"]

a. [Scripts]*の矢印をクリックして、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。バックアップ処理を終了する前にPRE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を作成	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を作成	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を作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshot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。

b. スケジュールを設定するポリシーの[Configure Schedules]列で、 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。

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。

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。SMTP は、 * Settings * > * Global Settings * でも設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。

リソーストポロジページが表示されます。

9. [今すぐバックアップ] をクリックします。

10. 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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

b. [バックアップ] 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

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"="v
server_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。

   新しいバックアップポリシーを作成する例を次に示します。

```
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、SnapCenterに新しいリソースグループを追加します。

   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"="10.232.2
06.248";"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します。

```
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。

   次に、指定した日付に実行されたすべてのジョブのジョブ概要レポートを表示する例を示します。

```
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 :
```

NetAppでサポートされているプラグインリソースのリソースグループのバックアップ

リソースグループは、[Resources]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、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。

開始する前に

- ポリシーを適用して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ことができます。そのためには、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、タグを選択します。そのあとにをクリックすると、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にバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   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で保護関係を検出できないことがあります。

     "MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

   - VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、バックアップが失敗することがあります。Java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、コマンドによって `do_start method` 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 `Java -jar -Xmx8192M -Xms4096M`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する

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しておく必要があります。

開始する前に

- 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でサポートする各ストレージシステムには、一意の名前と一意の管理LIF IPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

   この例では、PowerShellセッションを開きます。

   ```
   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。

   新しいストレージシステム接続を作成する例を次に示します。

   ```
   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。

   この例では、Windowsクレデンシャルを使用してFinanceAdminという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"。

NetAppでサポートされる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、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
   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は表示されますが 、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進行中であるか、警告サインが表示されていることがあります。

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。

NetAppでサポートされている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 *
- 操作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、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。

アクセス元	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。
[Activity]ペイン	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックして、最新の5つの処理を表示します。 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。

NetAppでサポートされている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[Topology]ページで表示する

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ときに、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立つことがあります。[Topology]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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

タスクの内容

プライマリストレージと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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージにあるバックアップとクローンの数が表示されます。
-  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。

-  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、バックアップを4つだけ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. [Summary]カードで、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の概要を確認します。

   [Summary Card]セクションには、バックアップとクローンの総数が表示されます。

   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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

   オンデマンドバックアップのあと、*[リフレッシュ]*ボタンをクリックすると、バックアップまたはクローンの詳細がリフレッシュされます。

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、 をクリックして削除します。

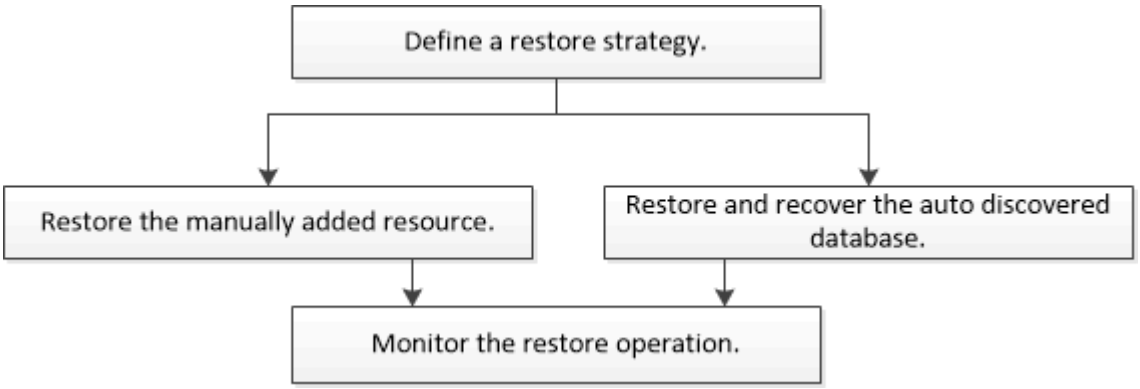
NetAppでサポートされているプラグインリソースのリストア

NetAppでサポートされているプラグインリソースのリストア

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。

タスクの内容

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のリストア

SnapCenterを使用してリソースをリストアできます。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。

開始する前に

- 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。
- Snapshot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、SnapCenter管理者が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Storage Virtual Machine（SVM）を割り当て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実行中のバックアップ処理がある場合は、キャンセルしておく必要があります。

タスクの内容

- デフォルトのリストア処理では、ストレージオブジェクトのみがリストアされます。アプリケーションレベルのリストア処理は、NetAppでサポートされているプラグインでその機能が提供されている場合にのみ実行できます。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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。

   バックアップはリソースグループのものである場合もありますが、リストアするリソースを個別に選択する必要があります。

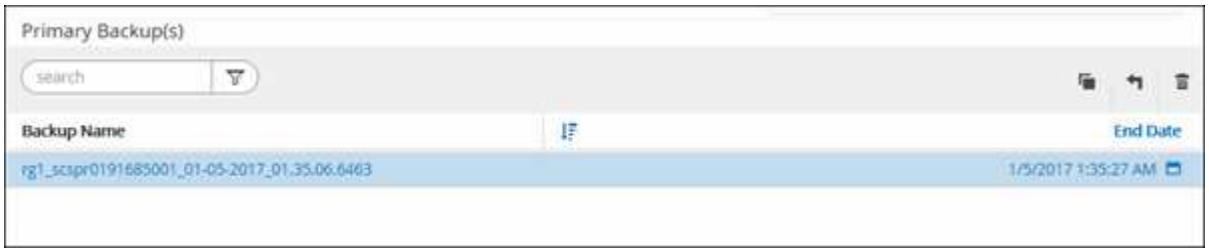
   リソースが保護されていない場合は、 [**Overall Status**] 列に _NOT PROTECTED _ が表示されます。

   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。

3. リソースを選択するか、リソースグループを選択してから、そのグループ内のリソースを選択します。

   リソーストポロジページが表示されます。

4. [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。
5. [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 。



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フットプリント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の新しいSnapshot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。

      - 複数のボリュームとqtreeを選択できます。

- 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。

7. 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、 [*Pre ops *] ページに入力します。
8. [*Post ops *] ページで、 mount コマンドおよび post restore 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。
9. [**Notification]** ページの **[*Email preference**] 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。

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

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

PowerShellコマンドレットを使用したリソースのリストア

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。

```
PS C:\> Open-Smconnection
```

2. Get-SmBackupおよびGet-SmBackupReportコマンドレットを使用して、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。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
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情報を表示しています。

```
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. 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"。

NetAppでサポートされる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、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

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。

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

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. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、次の手順を実行します。
   a. をクリックしてリストをフィルタリングし、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。

Clone NetAppでサポートされるプラグインリソースのバックアップ

Clone NetAppでサポートされるプラグインリソースのバックアップ

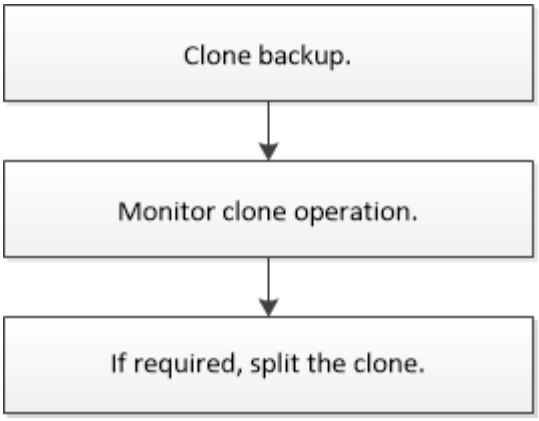
クローニングワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスクの内容

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
- データウェアハウスにデータを取り込む際のデータ抽出および操作ツール用
- 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、ソフトウェアコマンドレットリファレンスガイド^]を参照して https://docs.netapp.com/us-en/snapcenter-cmdlets/index.htmlnapCenter ください。

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。

開始する前に

- 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、NetAppでサポートされているプラグインでその機能が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）の割り当て済みアグリゲートリストに含まれている必要があります。

タスクの内容

ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

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 [* 表示 *] 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	操作
クローンサーバ	デフォルトでは、ソースホストが入力されています。 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。サフィックスを使用すると、クローニングされたリソースがホスト上で一意になります。 たとえば、rs1_cloneと入力します。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は、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つのソースに複数のデスティネーションボリュームを設定できます。

7. [* 設定 * （ * Settings * ）] ページで、次の手順を実行します。

フィールド	操作
イニシエータ名	ホストイニシエータ名（IQDNまたはWWPN）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。mountコマンドを入力して、ファイルシステムをホストにマウントします。

   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の削除
   - 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. [**Notification]** ページの **[*Email preference**] 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

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一覧を表示します。

   次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
 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します。

   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、クローン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          :
```

NetAppでサポートされる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。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには、処理の状態を示す次のアイコンが表示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み
- 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. [* Monitor*] ページで、 [* Jobs] をクリックします。

3. [* ジョブ *] ページで、次の手順を実行します。
    a. をクリックしてリストをフィルタリングし、クローニング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. [**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の管理

ダッシュボードを表示

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。ジョブ番号をクリックすると[監視]ページにリダイレクトされ、その他のジョブ情報を表示できます。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サーバに関する未解決の重大アラートと警告アラートの最新情報が表示されます。

重大アラートと警告アラートの総数が画面上部に表示されます。重大または警告の合計をクリックすると、[アラート]ページにリダイレクトされ、[アラート]ページで特定のフィルタが適用されます。

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表示される[アラート]ページにリダイレクトされます。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。

最新の保護サマリ

[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のステータスが表示されます。ステータス情報は、Snapshotとしてプラ

イマリストレージに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バックアップされたリソースについて提供されます。セカンダリストレージの保護ステータス情報が表示されるかどうかは、選択したプラグインタイプによって決まります。

mirror-vault保護ポリシーを使用している場合は、保護概要のカウンタがSnapVaultの概要グラフに表示され、SnapMirrorのグラフには表示されません。

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。ドーナツチャートには、選択したプラグインで保護されているリソースの割合が表示されます。 ドーナツチャートのスライスをクリックすると、**[**レポート**]**>*[プラグイン]*ページにリダイレクトされます。このページには、指定したプラグインのすべてのプライマリストレージとセカンダリストレージのアクティビティに関する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にのみ適用されます。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	バックアップに失敗したリソースグループに属しているエンティティの数。	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	バックアップに成功したリソースグループに所属しているエンティティの数。	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が完了し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。	バックアップをセカンダリデスティネーションに転送するように設定されていないリソースグループに属しているエンティティの数。
未開始	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

[ジョブ]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日間に固定されています。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ジョブの情報がドーナツチャートに表示されます。ドーナツチャートのスライスをクリックすると[モニタ]ページにリダイレクトされ、選択したジョブにフィルタが適用されます。

ジョブステータス	説明
失敗	失敗したジョブ数。
警告	エラーが発生したジョブ数。
成功	正常に完了したジョブ数。
実行中	実行中のジョブ数。

ストレージ

[ストレージ]タイルには、90日間に保護ジョブで使用された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ます。消費傾向とプライマリストレージの削減量が図で示されます。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が関連付けられている場合、その数には同じSnapshotが含まれます。これは、プライマリSnapshotとセカンダリSnapshotの両方に該当します。たとえば、バックアップを10個作成し、そのうちの2個はポリシーベースのバックアップ保持に基づいて削除され、1個はユーザが明示的に削除したとします。したがって、バックアップ数が7個と、これら7個のバックアップが占有するサイズが表示されます。

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による削減量とストレージ消費量の合計）の比率です。棒グラフはストレージ削減量を示しています。

折れ線グラフには、過去90日間のプライマリストレージとセカンダリストレージの日単位の消費量が表示されます。グラフにカーソルを合わせると、1日ごとの詳細な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。

構成

[設定]タイルには、SnapCenterで管理していてアクセス可能な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]の横にある数字をクリックすると、[Hosts]ページの[Managed Hosts]セクションにリダイレクトされます。そこから、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]の横にある数字をクリックすると、[ストレージシステム]ページにリ

ダイレクトされます。そこから、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、赤（重大）、黄（警告）、緑（アクティブ）のほか、各状態のホスト数も表示されます。状態ごとにステータスメッセージが表示されます。

設定ステータス	説明
アップグレードが必要	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。
移行が必要	実行しているプラグインがサポートされておらず、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	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、またはプラグインのインストールに失敗したホストの数。
中断	スケジュールが中断されてメンテナンス中のホストの数。
停止	稼働しているがプラグインサービスが実行されていないホストの数。
ホスト停止	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にアップグレード可能なホストの数。
移行可能（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。
ログディレクトリの設定	SCSQLでトランザクションログバックアップを作成するためにログディレクトリの設定が必要なホストの数。
VMware プラグインを設定	SnapCenter Plug-in for VMware vSphereを追加する必要があるホストの数。
不明	登録されているがインストールがまだ開始されていないホストの数。
実行中	稼働していてプラグインが実行されているホストの数。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ています。

設定ステータス	説明
プラグインをインストール中/アンインストール中	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。

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。ダッシュボードで使用できる表示数は固定であり、変更することはできません。各画面に表示されるコンテンツは、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する

[ダッシュボード]ページでは、バックアップ、リストア、およびクローニングジョブに関するレポートを表示できます。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。

     ドーナツチャートにデータが表示されます。

  4. レポートを表示するジョブ情報に対応するドーナツチャートのスライスをクリックします。

     ドーナツチャートをクリックすると、[Dashboard]ページから[Monitor]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. [Monitor]ページのリストで、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する

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ているリソースの保護の詳細を要求できます。データ保護の概要では、データバックアップのみが考慮されます。

- 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. ダッシュボードで[Latest Protection Summary]タイルを探し、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たリソースのドーナツチャートが表示されます。プラグインの場合は、セカンダリストレージにバックアップされたリソースのドーナツチャートも表示されます。

   データ保護レポートを使用できるのは、特定のタイプのプラグインのみです。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に対応するドーナツチャートのスライスをクリックします。

   ドーナツチャートをクリックすると、[ダッシュボード]ページから[レポート]、[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ドーナツチャートおよびファイルベースのSAP HANAバックアップの[レポート]ページにリダイレクトすることはできません。

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。ロール全体で使用されている権限を変更または削除する場合は、ロールを変更すると特に便利です。

開始する前に

「SnapCenterAdmin」ロールでログインする必要があります。

SnapCenterAdminロールの権限を変更または削除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、 * 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. [ロール名]フィールドで、変更するロールをクリックします。

4. [ロールの詳細]ページで、必要に応じて権限を変更するか、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。

   このロールのメンバーに他のメンバーが割り当てられているオブジェクトが表示されないようにするには、このオプションの選択を解除します。

   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属するユーザにオブジェクトまたはリソースへのアクセス権を割り当てる必要はありません。

1. [Submit （送信）] をクリックします。

ユーザとグループの変更

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。

開始する前に

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. [ユーザまたはグループの詳細]ページで、ロールとアセットを変更します。
  5. [Submit （送信）] をクリックします。

ホストの管理

ホストの追加、SnapCenterプラグインパッケージのインストール、検証サーバの追加、ホストの削除、バックアップジョブの移行、ホストの更新（プラグインパッケージのアップグレードや新しいプラグインパッケージの追加）を行うことができます。使用してい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	（NetAppでサポートされるプラグイン）	DB2の場合	PostgreSQL用PostgreSQL よう	MySQL用
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	はい	はい	はい
ホストのESXi情報の更新	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
スケジュールの一時停止とホストのメンテナンスモードへの切り替え	はい	はい	はい	はい	はい	はい	はい	はい	はい
プラグインの追加、アップグレード、または削除によるホストの変更	はい	はい	はい	はい	はい	はい	はい	はい	はい
SnapCenterからのホストの削除	はい	はい	はい	はい	はい	はい	はい	はい	はい
プラグインサービスの開始	はい	はい	はい	はい	はい	はい	はい	はい	はい
ディスクのプロビジョニング	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

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	（NetApp でサポートされるプラグイン）	DB2の場合	PostgreSQL用PostgreSQL よう	MySQL用
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	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	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	いいえ	いいえ	いいえ	いいえ

仮想マシン情報の更新

VMware vCenterのクレデンシャルが変更されたとき、またはデータベースまたはファイルシステムのホストが再起動されたときに、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の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ているSnapCenter Plug-in for Microsoft Windowsで管理されます。SnapCenter Plug-in for Microsoft Windowsは、RDMを管理するために、データベースホストを管理するvCenterサーバと通信します。

- 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。

プラグインホストの変更

プラグインのインストール後、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、グループ管理サービスアカウント（gMSA）、およびプラグインポートを変更できます。

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だけです。

  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場合は、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のポートが変更されたにもかかわらず、いずれかのコンポーネントが新しいポートで開始できない場合、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、いずれかのノードでポートが変更されていない場合、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なしでプラグインをインストールした場合は、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の起動と再起動

SnapCenterプラグインサービスを起動すると、サービスが実行されていない場合は開始し、実行中の場合は再開できます。メンテナンスの実行後にサービスの再起動が必要になる場合があります。

サービスの再起動時に実行中のジョブがない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、 * 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. アイコンをクリックし、**[サービスの開始]***または[サービスの再開]*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の一時停止

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タスクを実行するときに実行する必要があります。

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. アイコンをクリックし、*[スケジュールの中断]*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中断できます。

   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」です。

- 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る処理

[リソース]ページでは、リソースを検出してデータ保護処理を実行できます。実行できる処理は、リソースの管理に使用してい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
リソースをバックアップに使用できるかどうかの確認	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
リソースのオンデマンドバックアップの実行	はい	はい	はい	はい	はい	はい
バックアップからのリストア	はい	はい	はい	はい	はい	はい
バックアップのクローニング	いいえ	はい	はい	はい	はい	はい
バックアップの管理	はい	はい	はい	はい	はい	はい
クローンの管理	いいえ	はい	はい	はい	はい	はい
ポリシーの管理	はい	はい	はい	はい	はい	はい
ストレージ接続の管理	はい	はい	はい	はい	はい	はい
バックアップのマウント	いいえ	いいえ	いいえ	はい	いいえ	いいえ
バックアップのアンマウント	いいえ	いいえ	いいえ	はい	いいえ	いいえ
詳細を表示	はい	はい	はい	はい	はい	はい

ポリシーの管理

リソースまたはリソースグループからポリシーの適用解除、変更、削除、表示、コピーを行うことができます。

ポリシーの変更

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、レプリケーションオプション、Snapshotの保持設定、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）を変更するには、ポリシーを適用解除する必要があります。

- 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
スケジュールタイプを追加する	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、日次バックアップも追加するには、dailyスケジュールタイプのポリシーを作成してリソースグループに追加します。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する	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の適用を解除します。 2. スケジュールタイプを変更します。 3. すべてのリソースとリソースグループにポリシーを再度適用します。 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、それを日次バックアップに変更するには、最初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、 * 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。

ポリシーの適用解除

リソースのデータ保護を管理するポリシーが不要になった場合は、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前、またはスケジュールタイプを変更する前に、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。

ポリシーの削除

不要になったポリシーは削除することができます。

開始する前に

ポリシーが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、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。

  スケジュールはリソースグループの変更時に変更できます。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関連付けられているポリシーに定義されているバックアップ保持設定が、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ファイルシステム、カスタムアプリケーション、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既存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します。

  この処理は、（データベースのみを含む）SQLリソースグループに対して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（クローンライフサイクル）を設定できます。

- リソースグループに対してスケジュールされた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の停止と再開

スケジュールされた処理がリソースグループで開始されないように一時的に無効にすることができます。これらの処理は、必要に応じてあとで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

リソースグループの削除

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いずれか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、およびSnapshot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ているバックアップ、メタデータ、ポリシー、およびSnapshotをすべて削除する場合は、*[Delete backups and detach policies associated with this Resource Group]*チェックボックスを選択します。
5. [OK]*をクリックします。

バックアップの管理

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変更

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上の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。

バックアップの削除

他のデータ保護処理に不要になったバックアップは削除できます。

開始する前に

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ている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と、関連付けられているSAP HANAカタログも削除されます。

   最後に残っているバックアップが削除されると、関連付けられているHANAカタログのエントリを削除できません。

1. [OK]*をクリックします。

   SnapCenterに古いデータベースバックアップがあり、ストレージシステム上の対応するバックアップがない場合は、remove-smbackupコマンドを使用して、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。

保護の解除

保護の解除：すべてのバックアップが削除され、すべてのポリシーが解除されます。保護を解除する前に、バックアップがマウントされておらず、バックアップにクローンが関連付けられていない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、 [* 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. バックアップを選択し、*[保護の削除]*をクリックします。

クローンの削除

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、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、以降clone1が保護されます。データベースClone2をClone1のバックアップからクローニングします。Clone1を削除する場合は、まず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、[Delete Clone]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ことがあります。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パラメータには、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を開始するまでの待機時間を秒数で指定します。

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、ログの監視

[監視]ページでは、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、イベントやログの確認を行うことができます。

ジョブの監視

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。このビューは、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プラグインでフィルタできます。また、指定したジョブの詳細情報やログ ファイルを取得することもできます。

SnapMirror処理とSnapVault処理に関連するジョブを監視することもできます。

監視できるのは、SnapCenter管理者または別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、自分が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。

スケジュールの監視

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。また、処理を実行するホスト、および処理のリソースグループとポリシーの情報を確認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、 **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実行中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。

ログの監視

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

ジョブレベルのログ（バックアップジョブが失敗した理由のトラブルシューティングに役立つログなど）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. [Jobs]ページで、ジョブを選択し、[Download logs]をクリックします。

   ダウンロードしたzipフォルダには、ジョブログと共通の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 を選択した場合は、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、この操作はできません。
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、列見出しの上部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、レベルとして*以上*を選択します `Debug` 。
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。

   ダウンロードしたzipフォルダには、ジョブログと共通の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。

大規模な構成でパフォーマンスを最適化するには、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します。

```
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 `Get-SmRepositoryConfig`ます。

SnapCenterからのジョブとログの削除

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。ジョブIDを指定して特定のジョブを削除することも、指定した期間内にジョブを削除することもできます。

ジョブを削除するために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. [Jobs]ページで、ジョブのステータスを確認します。

関連情報

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、システムの健全性と処理の成功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	バックアップレポートには、SnapCenter環境のバックアップ傾向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について、保護の詳細が表示されます。概要のほか、保護されていないリソース、レポートの生成時にバックアップされていないリソース、バックアップ処理に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。
スケジュール済みレポート	これらのレポートは、毎日、毎週、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。レポートは指定された日時に自動的に生成され、電子メールで各ユーザーに送信されます。スケジュールは、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提供された権限に基づいた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。 [ロールの追加]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のオブジェクトを表示できる]オプションが選択されている場合は、そのロールの他のメンバーが表示および変更できます。

レポートへのアクセス

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。ダッシュボードでは、詳細を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。

次のいずれかの方法でレポートにアクセスできます。

- 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。

レポートのフィルタ

必要な情報の詳細レベルと期間に応じて、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。

レポートのエクスポートまたは印刷

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から、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. 特定のレポートサマリーを表示するには、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メール通知用のSMTPサーバの設定

データ保護ジョブのレポートを自分や他のユーザに送信する際に使用するSMTPサーバを指定できます。テスト用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を送信するための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の設定

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。

開始する前に

[設定]の[グローバル設定]ページでSMTPサーバを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サーバリポジトリの管理

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、環境が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リポジトリのバックアップ

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
- 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の表示

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のリストア

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の場合は、ONTAPスナップショット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
```

リストア処理の実行後にリポジトリバックアップが取得されると、リポジトリのリストア処理に使用されたバックアップはリストに表示されません。

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。リポジトリは、より多くのスペースがあるディスクに再配置する場合に移行できます。

- 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、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データディレクトリを新しい場所（E：\Data\nsmなど）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（nsm_copyなど）の名前を変更します。
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する

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。

開始する前に

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*

   次のコマンドは、リポジトリパスワードをリセットします。

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

関連情報

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"。

信頼され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管理者にお問い合わせください。

信頼されていないドメインの変更

信頼されていないドメインを変更して、ドメインコントローラのIPアドレスまたは完全修飾ドメイン名（FQDN）を更新できます。

- 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いことがあります。

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  、次の詳細を指定します。

フィールド	操作
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	ドメインの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**ドメインの登録解除

信頼されていないActive Directoryドメインに関連付けられているアセットを使用しない場合は、そのドメインの登録を解除できます。

開始する前に

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、アセットは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 、* OK *をクリックします。

ストレージシステムの管理

ストレージシステムを追加したら、ストレージシステムの構成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の設定を変更する

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。あるユーザが同じストレージシステムへの権限が付与された複数のグループに属している場合、ストレージ接続リストにはそのストレージ接続の名前が複数回（権限が割り当てられたグループごとに1回）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 SVM	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. [Storage Connections]ページで、該当する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。 a. [Storage Connections]ページで、クラスタ名をクリックします。 b. [ストレージシステムを変更]ページで、[ユーザ名]の横にある編集アイコンをクリックし、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選択解除します。 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する

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。あるユーザが同じストレージシステムへの権限が付与された複数のグループに属している場合、そのストレージシステムの名前がストレージ接続リストに複数回（権限が割り当てられたグループごとに1回）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中の処理はすべて失敗します。

- 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、削除するSVMまたはクラスタの横にあるチェックボックスを選択します。

   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データ収集の管理

PowerShellコマンドレットを使用して、Event Management System（EMS；イベント管理システム）によるデータ収集のスケジュール設定と管理を行うことができます。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はシステムの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、処理の進行中は高いままです。

EMSデータ収集の停止

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データ収集の開始

EMSデータ収集はデフォルトで有効になっており、インストール日から7日ごとに実行され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。

- 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

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する

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。

関連情報

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のアップグレード

利用可能なアップデートを確認するためのSnapCenterの設定

SnapCenterは、NetAppサポートサイトと定期的に通信し、利用可能なソフトウェア更新について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を受信する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。

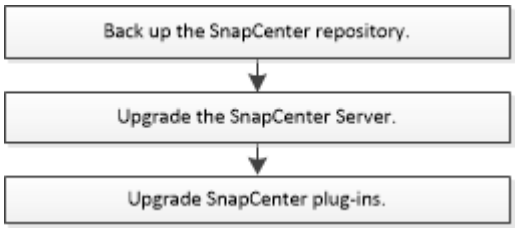
   [Available Software]ページには、使用可能なプラグインパッケージ、使用可能なバージョン、およびインストールステータスが表示されます。

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サーバと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。



サポートされるアップグレードパス

SnapCenterサーバのバージョン	SnapCenterサーバを直接アップグレードできる環境	サポートされるプラグインのバージョン
4.8	4.9	• 4.8 • 4.9
	5.0	• 5.0
4.9	5.0	• 4.9 • 5.0
	6.0	• 6.0
5.0	6.0	• 5.0 • 6.0

たとえば、SnapCenterバージョン4.8を使用していて、6.0にアップグレードする場合は、まず4.9にアップグレードしてから、6.0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"。

WindowsホストでのSnapCenterサーバのアップグレード

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。

開始する前に

- SnapCenterサーバホストにWindowsの更新プログラムが適用されていて、システムの再起動が保留されていないことが必要です。
- 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。
- 実行中のジョブが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。これは、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リポジトリのバックアップ"。

- 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。

タスクの内容

- 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実行でき

なくなります。アップグレードが完了すると、ホストのメンテナンスモードは自動的に解除されます。

- アップグレード中に、SQLスクリプトが実行されてNSMデータベース内のExchangeデータが更新され、DAGとホストのショートネームがFQDNに変換されます。これは、SnapCenter ServerとExchangeプラグインを併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では、scripts_pathを実行するために、サーバとプラグインホストの両方をバージョン4.7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の場合、バックアップ処理はアップグレード後も引き続き機能します。

  ［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は、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\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サーバ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。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する場合は、*C：\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt_*にある*sha224*キーをコピーして、/etc/sudoers_fileを更新する必要があります。
- 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」と表示されている場合は、しばらくし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。

LinuxホストでのSnapCenterサーバのアップグレード

SnapCenterサーバのインストーラ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。

- 手順 *

  1. いずれかの操作を実行して、SnapCenterサーバをアップグレードします。

実行する処理	操作
非対話型アップグレード	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename>` 例：sudo ./ snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log ログは_/var/opt/snapcenter/logs _に保存されます。 アップグレードのために渡すパラメータ： • DINSTALL_LOG_NAME：インストールログを格納するログファイルの名前。 • DUPGRADE：デフォルト値は0です。SnapCenterサーバをアップグレードするには、このパラメータと0以外の任意の整数を指定します。
対話型インストール	`./snapcenter-linux-server-(el8/el9/sles15).bin` アップグレードの確認を求められます。SnapCenterサーバのアップグレードを確認するには、0以外の値を入力してください。

SnapCenter GUIにアクセスするには、SnapCenterからログアウトしてからログインするか、ブラウザを閉じてから新しいブラウザを開いてください。

プラグインパッケージのアップグレード

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

開始する前に

- 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たとき、またはSnapCenter Plug-in Loader（SPL）サービスが再起動されたときに更新されます。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に設定すると、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。

タスクの内容

- 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では、scripts_pathを実行するために、サーバとプラグインホストの両方を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の場合、バックアップ処理はアップグレード後も引き続き機能します。

  ［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は、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. 次のいずれかのタスク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てをクリックし、**[**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がプラグインのアップグレード中に再起動されます。

     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。

     チェックボックスを選択していない場合は、プラグインをインストールするための要件を満たしているかどうかを確認するために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、該当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\SnapCenter WebAppにあるweb.config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。

Tech Refresh

SnapCenterサーバホストの機器更改

SnapCenterサーバホストの更新が必要な場合は、同じバージョンのSnapCenterサーバを新しいホストにインストールし、APIを実行して古いサーバからSnapCenterをバックアップし、新しいサーバにリストアできます。

手順

1. 新しいホストを導入し、次のタスクを実行します。
   a. 同じバージョンのSnapCenterサーバをインストールします。
   b. （任意）CA証明書を設定し、双方向SSLをイネーブルにします。詳細については、およびを参照して"CA証明書の設定" "双方向SSLの設定と有効化"ください。
   c. （任意）多要素認証を設定します。詳細については、を参照してください "多要素認証を有効にします"。
2. SnapCenter管理者ユーザとしてログインします。
3. API：またはコマンドレット：_New-SmServerBackup_を使用して、古いホストにSnapCenterサーバのバックアップを作成します `/<snapcenter_version>/server/backup` 。

   バックアップを作成する前に、スケジュールされたすべてのジョブを一時停止し、実行中のジョブがないことを確認します。

   新しいドメインで実行されているSnapCenterサーバでバックアップをリストアする場合は、バックアップを作成する前に、古いSnapCenterホストに新しいドメインユーザを追加し、SnapCenter adminロールを割り当てる必要があります。
4. 古いホストから新しいホストにバックアップをコピーします。
5. API：またはコマンドレット：_Restore -SmServerBackup_を使用して、新しいホストにSnapCenterサーバのバックアップをリストアします `/<snapcenter_version>/server/restore` 。

   リストアでは、デフォルトですべてのホストの新しいSnapCenterサーバURLが更新されます。更新をスキップする場合は、_- SkipSMSURLInHosts_attributeを使用し、API：またはコマンドレット：_Set -SmServerConfig_を使用してサーバURLを個別に更新します。
   `/<snapcenter_version>/server/configureurl`

   プラグインホスト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_entryを<New IP> SC_Server_Name形式で追加します。

   server_etc/host_entriesはリストアされません。古いサーバから手動でリストアできます。

新しいドメインで実行されているSnpCenterサーバにバックアップがリストアされ、古いドメインユーザを引き続き使用する場合は、古いドメインを新しいSnapCenterサーバに登録する必要があります。

古いSnapCenterホストでweb.configファイルを手動で更新した場合、更新は新しいホストにコピーされません。新しいホストのweb.configファイルでも、同じ変更を手動で行う必要があります。

6. SnapCenterサーバのURLの更新をスキップした場合、またはリストアプロセス中にいずれかのホストが停止していた場合は、API：またはコマンドレット：_Set -SmServerConfig_を使用して、SnapCenterで管理されているすべてのホストまたは指定したホストで新しいサーバ名を更新し `/<snapcenter_version>/server/configureurl` ます。
7. 新しいSnapCenterサーバから、すべてのホストでスケジュール済みジョブをアクティブ化します。

F5クラスタ内のノードの機器更改（Tech Refresh）

F5クラスタ内のノードを削除して新しいノードを追加すると、機器更改（Tech Refresh）を実行できます。更新が必要なノードがアクティブな場合は、クラスタの別のノードをアクティブにしてからノードを削除します。

F5クラスタにノードを追加する方法については、を参照してください "F5を使用した高可用性のためのSnapCenterサーバの設定"。

F5クラスタのURLが変更された場合は、API：またはコマンドレット：_Set-SmServerConfig_を使用して、すべてのホストでURLを更新できます `/<snapcenter_version>/server/configureurl` 。

古いSnapCenterサーバホストの運用停止

新しいSnapCenterサーバが稼働中であり、すべてのプラグインホストが新しいSnapCenterサーバホストと通信できることを確認したら、古いSnapCenterサーバホストを削除できます。

古いSnapCenterサーバホストへのロールバック

問題が発生した場合は、API：またはコマンドレット：_Set-SmServerConfig_を使用して、すべてのホストのSnapCenterサーバURLを更新することで、古いSnapCenterサーバホストを元に戻すことができます `/<snapcenter_version>/server/configureurl` 。

ディザスタリカバリ

スタンドアロンSnapCenterホストのディザスタリカバリ

サーバのバックアップを新しいホストにリストアすることで、ディザスタリカバリを実行できます。

開始する前に

古いSnapCenterサーバのバックアップがあることを確認します。

手順

1. 新しいホストを導入し、次のタスクを実行します。
   a. 同じバージョンのSnapCenterサーバをインストールします。
   b. CA証明書を設定し、双方向SSLを有効にします。詳細については、およびを参照して "CA証明書の設定" "双方向SSLの設定と有効化"ください。

2. SnapCenterサーバの古いバックアップを新しいホストにコピーします。
3. SnapCenter管理者ユーザとしてログインします。
4. API：またはコマンドレット：_Restore -SmServerBackup_を使用して、新しいホストにSnapCenterサーバのバックアップをリストアします `/<snapcenter_version>/server/restore` 。

   リストアでは、デフォルトですべてのホストの新しいSnapCenterサーバURLが更新されます。更新をスキップする場合は、_- SkipSMSURLInHosts_attributeを使用し、API：またはコマンドレット：_Set-SmServerConfig_を使用してサーバURLを個別に更新します `/<snapcenter_version>/server/configureurl` 。

   プラグインホスト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_entryを<New IP> SC_Server_Name形式で追加します。

   server_etc/host_entriesはリストアされません。古いサーバから手動でリストアできます。

5. URLの更新をスキップした場合、またはリストアプロセス中にいずれかのホストが停止した場合は、API：またはコマンドレット：_Set -SmServerConfig_を使用して、SnapCenterで管理されるすべてのホストまたは指定したホストで新しいサーバ名を更新します `/<snapcenter_version>/server/configureurl` 。

SnapCenter F5クラスタのディザスタリカバリ

ディザスタリカバリを実行するには、サーバのバックアップを新しいホストにリストアし、スタンドアロンホストをクラスタに変換します。

開始する前に

古いSnapCenterサーバのバックアップがあることを確認します。

手順

1. 新しいホストを導入し、次のタスクを実行します。
   a. 同じバージョンのSnapCenterサーバをインストールします。
   b. CA証明書を設定し、双方向SSLを有効にします。詳細については、およびを参照して "CA証明書の設定" "双方向SSLの設定と有効化"ください。
2. SnapCenterサーバの古いバックアップを新しいホストにコピーします。
3. SnapCenter管理者ユーザとしてログインします。
4. API：またはコマンドレット：_Restore -SmServerBackup_を使用して、新しいホストにSnapCenterサーバのバックアップをリストアします `/<snapcenter_version>/server/restore` 。

   リストアでは、デフォルトですべてのホストの新しいSnapCenterサーバURLが更新されます。更新をスキップする場合は、_- SkipSMSURLInHosts_attributeを使用し、API：またはコマンドレット：_Set-SmServerConfig_を使用してサーバURLを個別に更新します `/<snapcenter_version>/server/configureurl` 。

   プラグインホスト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_entryを<New IP> SC_Server_Name形式で追加します。

server_etc/host_entriesはリストアされません。古いサーバから手動でリストアできます。

5. URLの更新をスキップした場合、またはリストアプロセス中にいずれかのホストが停止した場合は、API：またはコマンドレット：_Set -SmServerConfig_を使用して、SnapCenterで管理されるすべてのホストまたは指定したホストで新しいサーバ名を更新します `/<snapcenter_version>/server/configureurl` 。
6. スタンドアロンホストをF5クラスタに変換します。

   F5の設定方法については、を参照してください "F5を使用した高可用性のためのSnapCenterサーバの設定"。

関連情報

APIの詳細については、Swaggerページにアクセスする必要があります。 を参照して "swagger API Web ページを使用して REST API にアクセスする方法"

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プラグインホストの機器更改

SnapCenterプラグインホストの更新が必要な場合は、古いホストから新しいホストにリソースを移動する必要があります。新しいホストをSnapCenterに追加すると、すべてのリソースが検出されますが、新しいリソースとして扱われます。

タスクの内容

古いホスト名と新しいホスト名を入力として使用するAPIまたはコマンドレットを実行し、リソースを名前で比較して、一致するリソースのオブジェクトを古いホストから新しいホストに再リンクする必要があります。一致するリソースは保護対象としてマークされます。

- _IsDryRun_パラメータはデフォルトでTrueに設定されており、これにより、古いホストと新しいホストの一致するリソースが識別されます。

  一致するリソースを確認したら、_IsDryRun_パラメータをFalseに設定して、一致するリソースのオブジェクトを古いホストから新しいホストに再リンクする必要があります。

- _AutoMigrateManualyAddedResources_パラメータはデフォルトでTrueに設定されており、手動で追加したリソースが古いホストから新しいホストに自動的にコピーされます。

  _AutoMigrateManuallyAddedResources_パラメータは、OracleリソースとSAP HANAリソースにのみ適用されます。

- 古いホストと新しいホストでインスタンス名が異なる場合は、_SQLInstanceMapping_パラメータを使用する必要があります。デフォルトインスタンスの場合は、_default_instance_asインスタンス名を使用します。

機器更改は次のSnapCenterプラグインでサポートされます。

- SnapCenter Plug-in for Microsoft SQL Server

- SQLデータベースがインスタンスレベルで保護されていて、ホストの機器更改の一環として一部のリソースのみが新しいホストに移動されると、既存のインスタンスレベルの保護がリソースグループ保護に変換され、両方のホストのインスタンスがリソースグループに追加されます。
- SQLホスト（host1など）が別のホスト（host2など）のリソースのスケジューラまたは検証サーバとして使用されている場合は、host1で機器更改を実行している間、スケジュールまたは検証の詳細は移行されず、host1で引き続き実行されます。変更が必要な場合は、対応するホストで手動で変更する必要があります。
- SQLフェイルオーバークラスタインスタンス（FCI）セットアップを使用している場合は、FCIクラスタに新しいノードを追加し、SnapCenterでプラグインホストを更新することで、機器更改を実行できます。
- SQL可用性グループ（AG）のセットアップを使用している場合は、機器更改は必要ありません。新しいノードをAGに追加し、SnapCenterでホストを更新できます。

- Windows向けSnapCenterプラグイン
- SnapCenter Plug-in for Oracle Database

  Oracle Real Application Cluster（RAC）セットアップを使用している場合は、RACクラスタに新しいノードを追加し、SnapCenterのプラグインホストを更新することで、機器更改を実行できます。

- SAP HANAデータベース向けSnapCenterプラグイン

サポートされるユースケースは次のとおりです。

- あるホストから別のホストへのリソースの移行。
- 複数のホストから1つ以上のホストへのリソースの移行。
- 1つのホストから複数のホストへのリソースの移行。

サポートされるシナリオは次のとおりです。

- 新しいホストの名前が古いホストと異なります
- 既存のホストの名前が変更されました

開始する前に

このワークフローではSnapCenterリポジトリのデータが変更されるため、SnapCenterリポジトリをバックアップすることを推奨します。データに問題が発生した場合は、バックアップを使用してSnapCenterリポジトリを古い状態に戻すことができます。

詳細については、を参照してください "SnapCenterリポジトリのバックアップ"。

手順

1. 新しいホストを導入し、アプリケーションをインストールします。
2. 古いホストのスケジュールを一時停止します。
3. 必要なリソースを古いホストから新しいホストに移動します。
   a. 新しいホストで同じストレージから必要なデータベースを起動します。
      - ストレージが古いホストと同じドライブまたは同じマウントパスにマッピングされていることを確認します。ストレージが正しくマッピングされていないと、古いホストで作成されたバックアップをリストアに使用できません。

デフォルトでは、次に使用可能なドライブが自動的に割り当てられます。

- Storage DRが有効になっている場合は、それぞれのストレージを新しいホストにマウントする必要があります。

b. アプリケーションのバージョンに変更がある場合は、互換性を確認してください。

c. Oracleプラグインホストの場合のみ、OracleおよびそのグループユーザのUIDとGIDが古いホストのUIDとGIDと同じであることを確認してください。

詳細については、以下を参照してください。

- "古いホストから新しいホストにSQLデータベースを移行する方法"
- "古いホストから新しいホストにOracleデータベースを移行する方法"
- "新しいホストでSAP HANAデータベースを起動する方法"

4. 新しいホストをSnapCenterに追加します。
5. すべてのリソースが検出されたかどうかを確認します。
6. ホスト更新API：またはコマンドレット：_invoke -SmTechRefreshHost_を実行します `/<snapcenter_version>/techrefresh/host` 。

ドライランはデフォルトで有効になっており、再リンクされる一致するリソースが識別されます。リソースを確認するには、API「/jobs/｛jobid｝」またはcmdlet_Get-SmJobSummaryReport_を実行します。

複数のホストからリソースを移行した場合は、すべてのホストに対してAPIまたはコマンドレットを実行する必要があります。新しいホストのドライブまたはマウントパスが古いホストと同じでない場合、次のリストア処理が失敗します。

- SQL In Placeリストアが失敗します。ただし、RTAL機能は利用できます。
- OracleデータベースとSAP HANAデータベースのリストアは失敗します。

複数のホストに移行する場合は、すべてのホストについて手順1のすべての手順を実行する必要があります。

同じホストでAPIまたはコマンドレットを複数回実行できます。再リンクは、新しいリソースが特定された場合にのみ実行されます。

7. （オプション）古いホストをSnapCenterから削除します。

関連情報

APIの詳細については、Swaggerページにアクセスする必要があります。 を参照して "swagger API Web ページを使用して REST API にアクセスする方法"

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"。

ストレージシステムの機器更改

ストレージが機器更改されると、データが新しいストレージに移行され、アプリケーションホストが新しいストレージでマウントされます。SnapCenterのバックアップワークフローで新しいストレージが特定され、新しいストレージがSnapCenterに登録されている場合はSnapshotが作成されます。

ストレージの更新後に作成された新しいバックアップでは、リストア、マウント、およびクローニングを実行できます。ただし、バックアップには古いストレージの詳細が含まれているため、ストレージの更新前に作成されたバックアップに対してこれらの処理を実行すると失敗します。ストレージ機器更改のAPIまたはコマンドレットを実行して、SnapCenterの古いバックアップを新しいストレージの詳細で更新する必要があります。

機器更改は次のSnapCenterプラグインでサポートされます。

- SnapCenter Plug-in for Microsoft SQL Server
- Windows向けSnapCenterプラグイン
- 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 Microsoft Exchange Server

サポートされるユースケースは次のとおりです。

- プライマリストレージの更新

  ストレージ機器更改（Tech Refresh）では、プライマリストレージを新しいストレージに置き換えることができます。既存のセカンダリストレージをプライマリストレージに変換することはできません。

- セカンダリストレージの更新

サポートされるその他のシナリオは次のとおりです。

- SVM名の変更
- ボリューム名の変更

プライマリストレージのバックアップを更新する

ストレージの機器更改が完了したら、storage tech refresh APIまたはコマンドレットを実行して、SnapCenter内の古いバックアップを新しいストレージの詳細で更新する必要があります。

開始する前に

このワークフローではSnapCenterリポジトリのデータが変更されるため、SnapCenterリポジトリをバックアップすることを推奨します。データに問題が発生した場合は、バックアップを使用してSnapCenterリポジトリを古い状態に戻すことができます。

詳細については、を参照してください "SnapCenterリポジトリのバックアップ"。

手順

1. 古いストレージから新しいストレージにデータを移行します。

   移行方法については、以下を参照してください。

   - "新しいストレージにデータを移行する方法"
   - "ボリュームをコピーし、すべてのSnapshotコピーを保持するにはどうすればよいですか。"

2. ホストをメンテナンスモードにします。
3. 新しいストレージをそれぞれのホストでマウントし、データベースを起動します。

   新しいストレージは、以前と同じ方法でホストに接続する必要があります。たとえば、SANとして接続されている場合は、SANとして接続する必要があります。

   新しいストレージは、古いストレージと同じドライブまたはパスにマウントする必要があります。

4. すべてのリソースが稼働していることを確認します。
5. SnapCenterで新しいストレージを追加します。

   SnapCenterのクラスタ間でSVM名が一意であることを確認します。新しいストレージで同じSVM名を使用していて、ストレージの更新を実行する前にSVMのすべてのボリュームをマイグレートできる場合は、その後、古いクラスタのSVMを削除してSnapCenterで古いクラスタを再検出し、SVMをキャッシュから削除することを推奨します。

6. ホストを本番モードにします。
7. SnapCenterで、ストレージが移行されるリソースのバックアップを作成します。SnapCenterで最新のストレージフットプリントを特定するには、新しいバックアップが必要です。このバックアップは、既存の古いバックアップのメタデータを更新するために使用されます。

   ホストに新しいLUNを接続すると、新しいシリアル番号が割り当てられます。Windowsファイルシステムの検出中、SnapCenterはすべての一意のシリアル番号を新しいリソースとして扱います。ストレージ機器更改時に、新しいストレージのLUNが同じドライブレターまたはパスでホストに接続されている場合、 SnapCenterでWindowsファイルシステムを検出すると、同じドライブレターまたはパスでマウントされていても、既存のリソースが削除済みとしてマークされ、新しいLUNが新しいリソースとして表示されます。リソースが削除済みとマークされているため、SnapCenterではストレージ機器更改の対象とはみなされず、古いリソースのバックアップはすべて失われます。ストレージの更新が発生する場合は、Windowsファイルシステムリソースの場合、ストレージの更新APIまたはコマンドレットを実行する前にリソースの検出を実行しないでください。

8. ストレージ更新API：またはコマンドレット：_invoke -SmTechRefreshPrimaryStorage_を実行します `/<snapcenter_version>/techrefresh/primarystorage` 。

   リソースにレプリケーション有効ポリシーが設定されている場合は、ストレージ更新後の最新のバックアップにセカンダリストレージの詳細が表示されます。

   a. SQLフェイルオーバークラスタインスタンス（FCI）セットアップを使用している場合、バックアップはクラスタレベルで保持されます。ストレージ機器更改の場合は、クラスタ名を入力する必要があります。

   b. SQL可用性グループ（AG）セットアップを使用している場合、バックアップはノードレベルで保持されます。ストレージ機器更改では、ノード名を入力する必要があります。

c. Oracle Real Application Clusters（RAC）セットアップを使用している場合は、任意のノードでストレージ機器更改を実行できます。

_IsDryRun_属性はデフォルトでTrueに設定されています。ストレージが更新されているリソースが特定されます。リソースと変更されたストレージの詳細を表示するには、API「<API_version>/jobs/SnapCenter｛jobid｝」またはcmdlet_Get-SmJobSummaryReport_を実行します。

9. ストレージの詳細を確認したら、_IsDryRun_属性をFalseに設定し、ストレージ更新API：またはコマンドレット：_invoke -SmTechRefreshPrimaryStorage_を実行し `/<snapcenter_version>/techrefresh/primarystorage` ます。

古いバックアップのストレージの詳細が更新されます。

APIまたはコマンドレットは同じホストで複数回実行できます。古いバックアップのストレージの詳細はストレージが更新された場合にのみ更新されます。

ONTAPでクローン階層を移行することはできません。移行対象のストレージにSnapCenter内にクローンメタデータがある場合、クローニングされたリソースは独立したリソースとしてマークされます。クローンメタデータのクローンは再帰的に削除されます。

10. （オプション）すべてのSnapshotを古いプライマリストレージから新しいプライマリストレージに移動しない場合は、次のAPIまたはcmdlet_invoke -SmPrimaryBackupsExistenceCheck_を実行し `/<snapcenter_version>/hosts/primarybackupsexistencecheck` ます。

これにより、新しいプライマリストレージでSnapshotの存在チェックが実行され、対応するバックアップがSnapCenterでの処理に使用できないことがマークされます。

セカンダリストレージのバックアップを更新する

ストレージの機器更改が完了したら、storage tech refresh APIまたはコマンドレットを実行して、SnapCenter内の古いバックアップを新しいストレージの詳細で更新する必要があります。

開始する前に

このワークフローではSnapCenterリポジトリのデータが変更されるため、SnapCenterリポジトリをバックアップすることを推奨します。データに問題が発生した場合は、バックアップを使用してSnapCenterリポジトリを古い状態に戻すことができます。

詳細については、を参照してください "SnapCenterリポジトリのバックアップ"。

手順

1. 古いストレージから新しいストレージにデータを移行します。

移行方法については、以下を参照してください。

- "新しいストレージにデータを移行する方法"
- "ボリュームをコピーし、すべてのSnapshotコピーを保持するにはどうすればよいですか。"

2. プライマリストレージと新しいセカンダリストレージの間にSnapMirror関係を確立し、関係が正常な状態であることを確認します。
3. SnapCenterで、ストレージが移行されるリソースのバックアップを作成します。

SnapCenterで最新のストレージフットプリントを特定するには、新しいバックアップが必要です。このバックアップは、既存の古いバックアップのメタデータを更新するために使用されます。

> この処理が完了するまでお待ちください。完了前に次の手順に進むと、SnapCenterによって古いセカンダリSnapshotメタデータが完全に失われます。

4. ホスト内のすべてのリソースのバックアップが作成されたら、セカンダリストレージ更新API：またはコマンドレット：_Invoke -SmTechRefreshSecondaryStorage_を実行し `/<snapcenter_version>/techrefresh/secondarystorage` ます。

   指定したホスト内の古いバックアップのセカンダリストレージの詳細が更新されます。

   この処理をリソースレベルで実行する場合は、各リソースの*[リフレッシュ]*をクリックしてセカンダリストレージのメタデータを更新します。

5. 古いバックアップが正常に更新されたら、プライマリとの古いセカンダリストレージ関係を解除できます。

SnapCenter Serverとプラグインのアンインストール

SnapCenterプラグインパッケージのアンインストール

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、前提条件を満た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カスタムプラグインを使用している場合は、ホストに関連付けられているクローンをSnapCenterからすべて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には、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。そうしないと、削除処理が失敗します。
- 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ための前提条件

- 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の権限を持つRBACロールを使用してログインしておく必要があります。

  オブジェクトには、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があります。

- 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ための前提条件

- 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ン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、ホストの読み取りと削除の権限を持つ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の削除"。

ホストを削除

SnapCenterサーバでホストを削除すると、まずSnapCenterの[Resources]ページにそのホストに対して表示されているバックアップ、クローン、クローニングジョブ、リソースグループ、およびリソースが削除され、次にホスト上のプラグインパッケージがアンインストールされます。

タスクの内容

- 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。
- 別のホストと共有しているリソースグループがホストに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、 "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. ページで、[管理対象ホスト]*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を使用したプラグインのアンインストール

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。

開始する前に

- 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。

タスクの内容

プラグインは個別にアンインストールできます。たとえば、ホストのリソースが不足している場合に、SnapCenter Plug-in for Microsoft SQL Serverをアンインストールして、もっと余裕のあるホストに移動するというケースがあり得ます。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SnapCenter Plug-ins Package for Linuxのアンインストールが必要になる場合があります。

- ホストを削除するとすべてのプラグインがアンインストールされます。

  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サーバ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サーバのインストールが破損します。SnapCenterサーバが不要になったことが確実な場合を除き、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. [管理対象ホスト]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てください。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、インストールは失敗します。

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たWindowsプラグインのアンインストール

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にログインしておく必要があります。

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"。

ホストでローカルにプラグインをアンインストールする

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。

タスクの内容

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場合は、SnapCenter GUIを使用するか、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コマンドレットを使用することを推奨します。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でアンインストールする必要が生じることがあります。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を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を使用したLinuxまたはAIX用プラグインパッケージのアンインストール

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。

開始する前に

- スケジュール済みジョブが削除されたことを確認します。
- 実行中のすべてのジョブが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.

WindowsホストでのSnapCenterサーバのアンインストール

SnapCenterサーバを使用してデータ保護ジョブを管理する必要がなくなった場合は、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。

開始する前に

- SnapCenterサーバがインストールされているドライブに2GB以上の空き容量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る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、処理は失敗します。

- リポジトリデータベースがクリーンアップおよび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。
- 手動でアンインストールする必要があります。 アンインストール中に削除されないNet Framework。

LinuxホストでのSnapCenterサーバのアンインストール

データ保護ジョブの管理にSnapCenterサーバを使用する必要がなくなった場合は、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。

手順

1. いずれかの操作を実行して、SnapCenterサーバをアンインストールします。

実行する処理	操作
非対話型アンインストール	`$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1` 例：sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall
タイワガタアンインストール	`$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall` アンインストールを確認するための確認入力に0以外の値を入力します。

REST APIによる自動化

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
- SAP HANAデータベース向けプラグイン
- カスタムプラグイン
- Oracleデータベース向けプラグイン

SnapCenter REST APIに標準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。一般的な言語には、Python、PowerShell、Javaなどがあります。

基盤となるREST Webサービス

Representational State Transfer（REST）は、分散Webアプリケーションを作成するための形式です。WebサービスAPIの設計に適用すると、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際の初期設計タスクには、次のものがあります。

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し、維持します。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、または管理エンティティがあります。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の最初のタスクの1つは、リソースを特定することです。

リソースの状態および関連する状態操作の定義

リソースは常に有限数の状態のいずれかにあります。状態、および状態の変化に影響を与えるために使用され

る関連操作は、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利用可能にする必要があります。リソースが配置され、識別されるエンドポイントでは、Uniform Resource Identifier（URI）が使用されます。

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を提供します。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ため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の形式

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いくつかありますが、最も一般的な方法は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現するための業界標準であり、リソースを記述する状態情報の転送に使用されます。SnapCenter REST API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では共通のテクノロジとベストプラクティスが確立されますが、各APIの詳細は設計の選択内容によって異なります。

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はAPIトランザクションとみなされます。

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は、CRUDモデルに基づいてアクセスされます。

- 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。

オフシエクト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呼び出しを発行すると、関連付けられたIDのURLがHTTP応答のlocationヘッダーで呼び出し元に返されます。識別子を抽出して以降の呼び出しでリソースインスタンスを参照する際に使用できます。

オブジェクトIDの内容と内部構造はいつでも変更できます。識別子は、関連するオブジェクトを参照する場合にのみ、該当するAPI呼び出しで使用してください。

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、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API呼び出しを適用できます。

同期操作と非同期操作

SnapCenterは、クライアントから受信したHTTP要求を同期または非同期で実行します。

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で応答します。

GETメソッドを使用する要求はすべて、常に同期的に実行されます。また、POSTを使用する要求は、2秒以内に完了すると予想される場合は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、タスクをアンカー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。成功または失敗を判断するには、ジョブの状態を取得する必要があります。

POSTおよび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されるように設計されています。

セキュリティ

REST APIで提供されるセキュリティは、主にSnapCenterで使用できる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。

トランスポート層セキュリティ

SnapCenterサーバとクライアントの間でネットワーク経由で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文字列に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

SnapCenter REST APIでサポートされるHTTPメソッドを次の表に示します。

RESTエンドポイントごとにすべての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	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。

同意する

このヘッダーは、 *application/json* に設定してください。

許可

ベーシック認証は、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で設定する必要があります。

リクエストの本文

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

オブジェクトのフィルタリング

GETを使用するAPI呼び出しを実行するときに、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リングできます。たとえば、次のように完全に一致する値を指定できます。

```
<field>=<query value>
```

完全一致に加えて、値の範囲内の一連のオブジェクトを返すための他の演算子も使用できます。SnapCenter REST APIでは、次の表に示すフィルタ演算子がサポートされます。

運用者	説明
=	等しい
<	より小さい
>	次の値より大きい
⇐	以下
>=	以上
更新	または
なんだ	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の要求

デフォルトでは、GETを使用してAPI呼び出しを実行すると、オブジェクトを一意に識別する属性のみが返されます。このフィールドの最小セットは、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。クエリパラメータを使用すると、次の方法で追加のオブジェクトプロパティを選択でき `fields` 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、アクセスするための処理をほとんど必要としません。これらは、URLパスキー（UUID）を指定してGETを使用したあと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、値をカンマで区切ってスペースなしで指定する必要があります。

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は、必要に応じて取得する必要があります。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。次のように、フィールド名とソート方向を指定したクエリパラメータを使用して順序を変更できます `order_by` 。

```
order_by=<field name> asc|desc
```

たとえば、typeフィールドを降順に並べ替え、idを昇順に並べ替えることができます。

```
order_by=type desc, id asc
```

- ソートフィールドを指定しても方向を指定しない場合、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。

コレクション内のオブジェクトを取得するときのページネーション

GETを使用してAPI呼び出しを発行し、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と、SnapCenterは2つの制約に基づいてできるだけ多くのオブジェクトを返します。これらの各制約は、リクエストの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要求に対して最初に到達した制約によって要求が終了するため、返されるレコード数が制限されます。

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。

オブジェクトの読み出しに使用する時間の制限

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、指定した時間が経過すると生成されたEMSイベントが最大10個返されます。

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

複数の要求を発行してオブジェクトをページングすることができます。以降の各API呼び出しでは、最後の結果セットの最新のイベントに基づいて新しい時間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呼び出しおよび特定のクエリパラメータで使用される入力値は数値です。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メガバイト（KB x 1024バイト）またはメビバイト
GB	GBギガバイト（MB x 1024バイト）またはギビバイト
TB	テラバイト（GB x 1024バイト）またはテビバイト
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判断し、必要に応じて追加のデータを取得する必要があります。

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	OK は、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	オブジェクトが作成されました。応答のlocationヘッダーには、オブジェクトの一意の識別子が含まれています。
202	承認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	要求が正しくありません。要求の入力が認識されていないか、適切でありません。
401	権限のないユーザ認証に失敗しました。
403	認証（ RBAC ）エラーにより、アクセスが禁止されています。
404	要求で参照されているリソースが見つかりません。
405	メソッドが許可されていません要求内の HTTP メソッドはリソースに対してサポートされていません
409	競合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	内部エラーサーバー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、新しいオブジェクトへの完全なURL（オブジェクトに割り当てられた一意の識別子を含む）が格納されます。

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形式で表示されます。

単一のオブジェクト

要求に基づいて一連のフィールドを含む単一のオブジェクトを返すことができます。たとえば、GETを使用すると、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、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す一貫した形式が使用され `num_records` 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をアンカー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Errorオブジェクトが返されます。たとえば、クラスタに対して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発生します。

空

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ていることがあります。

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。

形式

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>"]
}
```

コード値を使用して一般的なエラータイプまたはカテゴリを特定し、メッセージを使用して特定のエラーを特定できます。該当する場合は、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呼び出しには、追加のエラーコードが含まれることがあります。

コード	説明
409	同じ識別子のオブジェクトがすでに存在します。
400	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、追加のフィールドが指定されています。
400	この処理はサポートされていません。

コード	説明
405	指定した識別子のオブジェクトが見つかりません。
403	要求を実行する権限が拒否されました。
409	リソースが使用中です。

SnapCenter Server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。各リソースの簡単な説明と基本リソースパスを次に示します。また、必要に応じて使用上のその他の考慮事項も示します。

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、後続の要求の認証に使用され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する
- 特定のドメインの詳細を取得する
- ドメインの登録または登録解除
- ドメインを変更する

ジョブ

APIを使用してさまざまな処理を実行できます。

- SnapCenterですべてのジョブを取得する
- ジョブのステータスの取得
- ジョブをキャンセルまたは停止する

設定

APIを使用してさまざまな処理を実行できます。

- クレデンシャルの登録、変更、削除
- 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。
- 通知の設定
- 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サーバログインのMFAを有効または無効にして設定する
- MFAのセットアップに必要な構成ファイルを作成

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
- SnapCenterから1つ以上のホストを削除する
- 名前によるホストの取得
- ホスト上のすべてのリソースを取得する
- 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する
- プラグインホストの設定
- Plug-in for Microsoft SQL Serverホストのすべてのリソースを取得する
- Plug-in for Oracle Databaseホストのすべてのリソースを取得
- カスタムアプリケーションホスト用プラグインのすべてのリソースを取得する
- Plug-in for SAP HANAホストのすべてのリソースを取得する
- インストールされているプラグインの取得
- 既存のホストにプラグインをインストールする
- ホストパッケージのアップグレード
- 既存のホストからプラグインを削除する
- ホストにプラグインを追加する
- ホストの追加または変更
- Linuxホストのシグネチャの取得
- Linuxホストのシグネチャの登録
- ホストをメンテナンスモードまたは本番モードにする
- ホストでプラグインサービスを開始または再起動する
- ホストの名前を変更する

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
- リソースIDを使用してリソースを取得する
- Plug-in for Microsoft SQL Serverホストのすべてのリソースを取得する
- Plug-in for Oracle Databaseホストのすべてのリソースを取得

- カスタムアプリケーションホスト用プラグインのすべてのリソースを取得する
- Plug-in for SAP HANAホストのすべてのリソースを取得する
- キーを使用したMicrosoft SQL Serverリソースの取得
- キーを使用したカスタムリソースの取得
- 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変更する
- 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する
- キーを使用したSAP HANAリソースの取得
- Plug-in for SAP HANAホストのリソースを変更する
- キーを使用してPlug-in for SAP HANAホストのリソースを削除する
- キーを使用したOracleリソースの取得
- Oracleアプリケーションボリュームリソースを作成する
- Oracleアプリケーションボリュームリソースを変更する
- キーを使用してOracleアプリケーションボリュームリソースを削除する
- Oracleリソースのセカンダリの詳細を取得する
- Plug-in for Microsoft SQL Serverを使用したMicrosoft SQL Serverリソースのバックアップ
- Plug-in for Oracle Databaseを使用したOracleリソースのバックアップ
- カスタムアプリケーション用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する
- SAP HANAデータベースの設定
- Oracleデータベースの設定
- 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のリストア
- カスタムアプリケーションのバックアップのリストア
- カスタムプラグインリソースを作成する
- SAP HANAリソースを作成する
- 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
- Plug-in for Microsoft SQL Serverを使用したMicrosoft SQL Serverリソースの保護
- 保護されたMicrosoft SQL Serverリソースを変更する
- Microsoft SQL Serverリソースの保護の解除
- Plug-in for Oracle Databaseを使用したOracleリソースの保護
- 保護されているOracleリソースを変更する
- Oracleリソースの保護の解除
- カスタムアプリケーション用プラグインを使用したバックアップからのリソースのクローニング
- Plug-in for Oracle Databaseを使用したバックアップからのOracleアプリケーションボリュームのクローニング
- Plug-in for Microsoft SQL Serverを使用したバックアップからのMicrosoft SQL Serverリソースのクローニ

ング

- Microsoft SQL Serverリソースのクローンライフサイクルを作成する
- Microsoft SQL Serverリソースのクローンライフサイクルを変更する
- Microsoft SQL Serverリソースのクローンライフサイクルを削除する
- 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に移動する
- Oracleデータベースのクローン仕様ファイルの作成
- 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リソースを作成する
- 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結合します。
- Oracleアプリケーションボリュームリソースを作成する

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、または日付を指定して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
- バックアップの詳細を取得
- バックアップの名前変更または削除
- Oracleバックアップのマウント
- Oracleバックアップのアンマウント
- Oracleバックアップをカタログ化
- Oracleバックアップのカタログから削除
- 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に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の作成、表示、変更、削除
- 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
- すべてのクローンを取得
- クローンの削除
- IDによるクローンの詳細の取得
- 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する

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。

- クローン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の取得
- クローンスプリット処理の開始または停止

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する
- リソースグループを名前で取得
- カスタムアプリケーション用プラグインのリソースグループを作成する
- Plug-in for Microsoft SQL Serverのリソースグループを作成する
- 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する
- カスタムアプリケーション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を変更する
- Plug-in for Oracle Database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、削除する
- リソースグループのバックアップ
- 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する
- 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
- 名前によるポリシーの詳細の取得
- 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プラグインのポリシーを作成または変更する
- Plug-in for Microsoft SQL Serverのポリシーを作成または変更する
- Plug-in for Oracle Database用のポリシーの作成または変更
- Plug-in for SAP HANA Databaseのポリシーを作成または変更する

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
- 名前による共有の取得
- 共有を作成または削除する
- ストレージの詳細を取得
- 名前によるストレージの詳細の取得
- ストレージの作成、変更、削除
- ストレージクラスタ上のリソースを検出する
- ストレージクラスタ上のリソースの取得

共有

APIを使用してさまざまな処理を実行できます。

- 共有の詳細を取得する
- すべての共有の詳細を取得する
- ストレージ上の共有を作成または削除する
- 名前による共有の取得

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する
- キーを使用したMicrosoft SQL Serverリソースの取得
- キーを使用してカスタムリソースを変更する
- キーを使用してカスタムリソースを削除する
- キーを使用したSAP HANAリソースの取得
- キーを使用してSAP HANAリソースを変更する
- キーを使用してSAP HANAリソースを削除する
- キーを使用したOracleリソースの取得
- キーを使用してOracleアプリケーションボリュームリソースを変更する
- キーを使用してOracleアプリケーションボリュームリソースを削除する
- Microsoft SQL Server用プラグインとキーを使用してMicrosoft SQL Serverリソースをバックアップする
- Plug-in for Oracle Databaseとキーを使用してOracleリソースをバックアップする
- 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する

- キーを使用してSAP HANAデータベースを設定
- キーを使用してOracleデータベースを設定する
- キーを使用したカスタムアプリケーションのバックアップのリストア
- カスタムプラグインリソースを作成する
- SAP HANAリソースを作成する
- Oracleアプリケーションボリュームリソースを作成する
- 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
- Plug-in for Microsoft SQL Serverを使用したMicrosoft SQL Serverリソースの保護
- 保護されたMicrosoft SQL Serverリソースを変更する
- Microsoft SQL Serverリソースの保護の解除
- Plug-in for Oracle Databaseを使用したOracleリソースの保護
- 保護されているOracleリソースを変更する
- Oracleリソースの保護の解除
- カスタムアプリケーション用プラグインを使用したバックアップからのリソースのクローニング
- Plug-in for Oracle Databaseを使用したバックアップからのOracleアプリケーションボリュームのクローニング
- Plug-in for Microsoft SQL Serverを使用したバックアップからのMicrosoft SQL Serverリソースのクローニング
- Microsoft SQL Serverリソースのクローンライフサイクルを作成する
- Microsoft SQL Serverリソースのクローンライフサイクルを変更する
- Microsoft SQL Serverリソースのクローンライフサイクルを削除する
- Oracleデータベースのクローン仕様ファイルの作成
- 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
- 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する

レポート

APIを使用してさまざまな処理を実行できます。

- それぞれのプラグインのバックアップ、リストア、クローニング処理のレポートを取得する
- スケジュールの追加、実行、削除、変更
- スケジュール済みレポートのデータを取得する

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
- IDによるアラートの取得

- 複数のアラートの削除またはIDによるアラートの削除

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する
- ユーザの追加または削除
- ロールへのユーザの割り当て
- ロールからユーザの割り当てを解除
- ロールの作成、変更、削除
- ロールへのグループの割り当て
- ロールからのグループの割り当て解除
- グループの追加または削除
- 既存のロールのコピーを作成する
- ユーザまたはグループへのリソースの割り当てまたは割り当て解除

構成

APIを使用してさまざまな処理を実行できます。

- 構成設定の表示
- 設定の変更

証明書の設定

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の表示
- SnapCenterサーバまたはプラグインホストの証明書設定を変更する

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。

- リポジトリバックアップの取得
- リポジトリに関する設定情報を表示する
- SnapCenterリポジトリの保護とリストア
- SnapCenterリポジトリの保護を解除する
- リポジトリの再構築とフェイルオーバー

バージョン

このAPIを使用してSnapCenterのバージョンを確認できます。

Swagger API Webページを使用して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に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経由でアクセスされるオブジェクトに対する権限は、REST APIにログインするためのトークンを生成したユーザに基づきます。

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の複雑なワークフロープロセスでAPIを使用する前に、ある程度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、使用可能かどうかを確認できます。

開始する前に

- システムでCurlユーティリティが使用可能であ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、使用しているシェルに基づいてCurlが許容できる形式に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、文字列全体を一重引用符で囲むことができます `username:password` 。

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

法的通知では、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、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

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 6.0に関する注意事項"

著作権に関する情報

商標に関する情報