UNIXファイルシステムの保護

SnapCenter software

NetApp
January 09, 2026

目次

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。

特徴

- 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 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。

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 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に関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

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。

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、*[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。

パラメータ名	説明
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。
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。

パラメータ名	説明
logs_max_count	SnapCenter Plug-in Loader ログファイルのうち、_/custom_location/snapcenter /spl/logs_folder に保持されているファイルの数を表示します。 デフォルト値は5000に設定されています。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。
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"。

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。

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. [Name]ページで、ポリシーの名前と詳細を入力します。
6. [Backup and Replication]ページで、次の操作を実行します。
   a. バックアップ設定を指定します。
   b. 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。
   c. [Select secondary replication options]セクションで、次のセカンダリレプリケーションオプションの一方または両方を選択します。

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。
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。

7. [Retention]ページで、[Backup and Replication]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。 最大保持値は1018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	[コピーを保持する期間]*を選択し、Snapshotを削除するまでの日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。 SnapLock保持期間は100年未満にする必要があります。

8. ポリシーラベルを選択します。

   リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

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

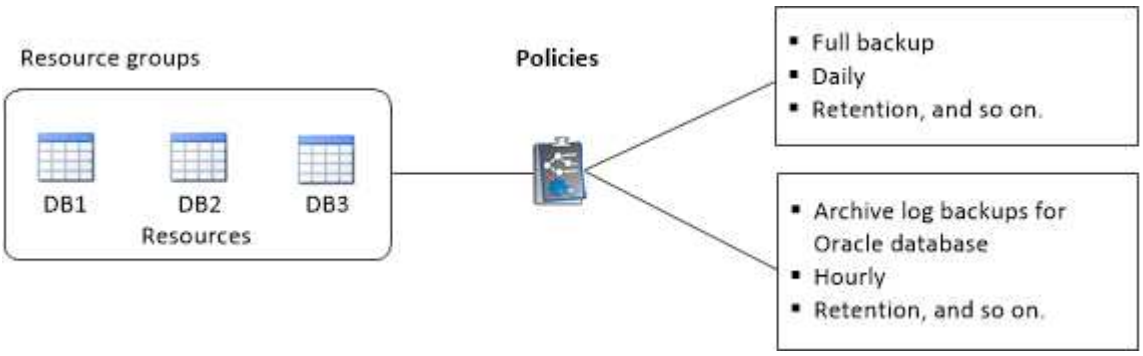
リソースグループはコンテナであり、バックアップして保護するリソースを追加します。リソースグループを使用すると、ファイルシステムに関連付けられているすべてのデータをバックアップできます。

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。

リソースグループを作成し、**ASA R2**システム上の**UNIX**ファイルシステムのセカンダリ保護を有効にする

リソースグループを作成して、ASA R2システム上のリソースを追加する必要があります。リソースグループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.xリソースとASA R2リソースの両方を同じリソースグループに追加しないでください。
- ONTAP 9.xリソースとASA R2リソースの両方を含むデータベースがないことを確認してください。

タスクの内容

- セカンダリ保護は、ログインしているユーザに「* SecondaryProtection *」機能が有効なロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にした場合、プライマリおよびセカンダリ整合グループの作成時にリソースグループがメンテナンスモードになります。プライマリとセカンダリの整合グループが作成されると、リソースグループはメンテナンスモードを終了します。
- SnapCenterでは、クローンリソースのセカンダリ保護はサポートされません。

手順

1. 左側のナビゲーションペインで、*[リソース]*を選択し、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、プレフィックスを含め、アプリケーションで設定されたものとまったく同じ宛先を使用する必要があります。

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ASA R2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、バックアップオプションを選択します。
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。

> 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. 選択したポリシーでセカンダリ保護が有効になっている場合は、[Secondary Protection]ページが表示され、次の手順を実行する必要があります。

a. レプリケーションポリシーのタイプを選択します。

> 同期レプリケーションポリシーはサポートされていません。

b. 使用する整合グループサフィックスを指定します。

c. [デスティネーションクラスタ]と[デスティネーションSVM]のドロップダウンで、使用するピアクラスタとSVMを選択します。

> クラスタとSVMのピアリングはSnapCenterではサポートされていません。クラスタとSVMのピアリングを実行するには、System ManagerまたはONTAP CLIを使用する必要があります。

リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは[Secondary Protected Resources]セクションに表示されます。

1. [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。

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。

3. 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、 ペインアイコン"] 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。

- レプリカサイトは稼働しています。
- レプリカサイトはダウンしています。
- セカンダリミラー関係またはバックアップ関係が再確立されていません。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択し

ます。

2. [リソース] ページで、 [* 表示 *] 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関する情報は、Get-Help *command_name* を実行すると取得できます。あるいは、 "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。

   プラグインホストの_/ opt/ NetApp / SnapCenter / SCC /etc/allowed_commands.config_pathにあるコマンドリストで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後、次のコマンドを実行して SnapCenter プラグイン作成者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/etc/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。
- FlexCloneのボリュームスプリット処理の詳細については、を参照してください "FlexCloneボリュームを親ボリュームからスプリットします。"。
- 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"

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。