UNIXファイルシステムの保護

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter-61/protect-scu/concept_overview_snapcenter_plug_in_for_UNIX_file_systems.html on November 06, 2025. Always check docs.netapp.com for the latest.

目次

UNIXファイルシステムの保護

SnapCenter Plug-in for UNIX File Systemsの機能

Plug-in for UNIX File Systems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することができます。これらの処理をサポートするタスクも実行できます。

- 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の設定
- 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

サポートされている構成

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の両方に存在するvVolデータストア。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はサポートされていません。
- プロビジョニングはサポートされていません。

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により、Oracleデータベースに対してデータ保護処理を実行できるようになります。
- ONTAPを実行するストレージ システムで、Network File System（NFS）プロトコルとストレージ エリア ネットワーク（SAN）プロトコルがサポートされます。
- Linuxシステムでは、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録した場合、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ファイルシステムおよびLVMレイアウトでAIXのマウント ガードがサポートされます。
- AIXシステムの場合のみ、Enhanced Journaled File System（JFS2）およびSANファイルシステムとLVMレイアウトでのインライン ロギングがサポートされます。

  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、クローニングの各処理が自動化されます。

SnapCenter Plug-in for UNIX File Systemsのインストール

ホストを追加して**Plug-in 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Plug-in Package for Linux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。
- パスワードベースの認証またはSSHキーベースの認証を使用できます。パスワードベースの認証はrootユーザとroot以外のユーザが使用できます。

SnapCenter Plug-in for UNIX File Systemsは、root以外のユーザもインストールできます。ただし、プラグイン プロセスをインストールして開始できるよう、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、プロセスは有効なroot以外の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、以下を参照してください。 "すべてのオペレーティング システム用のJavaのダウンロード"

- 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** を使用する必要があります。

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プラグインに必要な最小RAM	2 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB 十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護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は、最近実行した処理のログが作成されません。

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。 Javaを最新バージョンにアップグレードした場合は、/var/opt/snapcenter/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJava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

[Add Host]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、自動的にリモート ホスト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、[ホスト] をクリックします。
2. 上部の*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。

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が機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。 SnapCenterを使用してサブドメインの一部であるホストを追加する場合は、FQDNを指定する必要があります。

フィールド	操作
Credentials	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、[Add Host]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の選択」セクションで、「**Unix** ファイル システム」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 Server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てカスタム 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、処理が失敗します。
Installation Path	デフォルトのパスは */opt/ NetApp/snapcenter* です。 必要に応じて変更できます。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。
Skip optional preinstall checks	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オンにします。

7. *送信*をクリックします。

   [Skip prechecks]チェック ボックスをオンにしていない場合、プラグインをインストールするための要件を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。

   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に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、エラーまたは警告メッセージが表示されます。エラーがディスク容量または 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のセットアップで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. 指紋を確認して、「確認して送信」をクリックします。

   SnapCenterでは、ECDSAアルゴリズムがサポートされていません。

   前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

   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。

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、[リソースの更新] をクリックします。

インストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。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。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリスト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. *フィルター*をクリックします。
   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、[プラグインのインストール] を選択します。
   d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
   e. *適用*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プラグインLoaderサービスは、Linux がSnapCenterサーバーと対話するためのプラグイン 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のインストール後に、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、次の作業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ます。
- Java仮想マシンに割り当てられているメモリ容量を増やします。

/custom_location/ NetApp/snapcenter/spl/etc/ にある spl.properties ファイルには、次のパラメータが含まれています。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	サポートされるログ レベルを表示します。 有効な値は、TRACE、DEBUG、INFO、WARN、ERROR、およびFATALです。
SPL_PROTOCOL	SnapCenter Plug-in Loaderでサポートされるプロトコルを表示します。 HTTPSプロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。

パラメータ名	説明
SNAPCENTER_SERVER_PROTOCOL	SnapCenter Serverでサポートされるプロトコルを表示します。 HTTPSプロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
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には、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場合や新しいキーストア ファイルを作成する場合にのみ変更できます。
SPL_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_SERVER_HOST	SnapCenter Server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 Serverが実行され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	*/custom_location/snapcenter/spl/logs* フォルダに保存されているSnapCenterプラグLoaderログ 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より大きい場合は、最後に変更されたものから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時点から24時間ごとに自動的に行われます。 spl.propertiesファイルを手動で削除する場合、保持されるファイル数は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、インストール時にSPLを開始する段階で決定されます。
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、そのログ ファイルはzipされ、そのジョブの新しいファイルにログが書き込まれます。
RETAIN_LOGS_OF_LAST_DAYS	ログが保持される最大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にデフォルト値が割り当てられていない場合や、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。パラメータに割り当てられている値に関連する問題をトラブルシューティングするために、spl.propertiesファイルを検証および編集することもできます。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プラグインLoaderサービスを開始します。
     - ルートユーザーとして、次を実行します:
       `/custom_location/NetApp/snapcenter/spl/bin/spl start`

- 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

◦ SnapCenterプラグインLoaderサービスを停止します。

- ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- 非ルートユーザーとして、次を実行します。 `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、既存の処理も終了してしまうため、このコマンドを使用する際は十分に注意してください。

◦ SnapCenterプラグインLoaderサービスを再起動します。

- ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ SnapCenterプラグインLoaderサービスのステータスを確認します。

- ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- 非ルートユーザーとして、次を実行します: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ SnapCenterプラグインLoaderサービスの変更を見つけます。

- ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Linuxホストでの**SnapCenter Plug-in Loader**（**SPL**）サービスを使用した**CA**証明書の設定

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には、 SnapCenterプラグインLoaderサービスを使用して、SPL キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、SPL 信頼ストアにルート証明書または中間証明書を構成し、CA 署名キー ペアを SPL 信頼ストアに構成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、トラストストアとキーストアのどちらにも使用します。

SPLキーストアのパスワードと、使用中の**CA**署名キー ペアのエイリアスの管理

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「SPL_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キー
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ファイルのキーSPL_KEYSTORE_PASSについても、同様に更新します。

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、秘密キーに関連付けられているエイリアス パスワードをすべて同じにする必要があります。

ルート証明書または中間証明書の**SPL**トラストストアへの設定

ルート証明書や中間証明書は、SPLトラストストアへの秘密キーなしで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ー (*/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の一覧を表示します。

```
 keytool -list -v -keystore keystore.jks
. ルート証明書か中間証明書を追加します。
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
.
SPLトラストストアへの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証明書を追加してから、中間CA証明書を追加する必要があります。

SPLトラストストアに対する**CA**署名付きキー ペアの設定

SPLトラストストアに対して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. 「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の一覧を表示します。

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

. 秘密キーと公開キー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の一覧を表示します。

```
 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キーのパスワードを、キーストアのパスワードに変更します。

SPLキーストアのデフォルトのパスワードは、spl.propertiesファイルのキーSPL_KEYSTORE_PASSの値です。

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

. CA 証明書のエイリアス名が長く、スペースや特殊文字 （「*」、「」）
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。

SPL_CERTIFICATE_ALIASキーに対するこの値を更新します。

4. SPLトラストストアにCA署名キー ペアを設定したら、サービスを再起動します。

SPLの証明書失効リスト（**CRL**）の設定

SPLにCRLを設定する必要があります。

このタスクについて

- SPLは、あらかじめ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に照らして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ファイルを格納できます。

   受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインの**CA**証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインで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

- 実行 *Set-SmCertificateSettings* コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- *Get-SmCertificateSettings* を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用できるパラメータとその説明に関する情報は、*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、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] 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。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Server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いないか、プラグイン ホストに割り当てられていないことを示します。
- * * 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。

展開方法については、 "導入プロセスの概要" 。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。 "SSL証明書を作成またはインポートする" 。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere 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ファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

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。SnapMirrorテクノロジとSnapVaultテクノロジを使用できるようにSnapCenter Serverをセットアップ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 デバイス上のソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、初期化する必要があります。この作業を実行するには、NetApp System Managerを使用するか、ストレージ コンソールのコマンドラインを使用します。

ユーザがPlug-in for UNIX File Systemsを使用するためには、SnapCenter管理者が事前に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 Server をインストールして構成します。"詳細情報"
- ストレージ システム接続を追加して、 SnapCenter環境を構成します。"詳細情報"

> SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることは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 Serverを使用してVMware RDM LUNまたはVMDK上の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 Server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、以下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 ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。レプリケーション、スクリプト、バックアップ タイプの設定を指定することもできます。ポリシーを作成することで、別のリソースやリソース グループでポリシーを再利用したい場合に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ユーザには、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、 "SnapMirrorアクティブ同期のオブジェクト数の制限" 。

タスク概要

- SnapLock
  - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで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、ポリシーで指定した数よりも多くの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が、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、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 ファイル システム*を選択します。
4. *新規*をクリックします。
5. 「名前」ページで、ポリシー名と詳細を入力します。
6. 「バックアップとレプリケーション」ページで、次のアクションを実行します。
   a. バックアップ設定を指定します。
   b. オンデマンド、時間別、日次、週次、または*月次*を選択して、スケジュールの頻度を指定します。
   c. [セカンダリ レプリケーション オプションの選択] 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 1 つまたは両方を選択します。

フィールド	操作
Update SnapMirror after creating a local Snapshot copy	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アクティブ同期に対して有効にする必要があります。
Update SnapVault after creating a local Snapshot copy	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。
Error retry count	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. [保持] ページで、[バックアップとレプリケーション] 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	操作

特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順に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バージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。 SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshot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ことがあります。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
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. [Script]ページで、バックアップ処理の前またはあと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。

   _ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_ パスからプラグイン ホスト上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

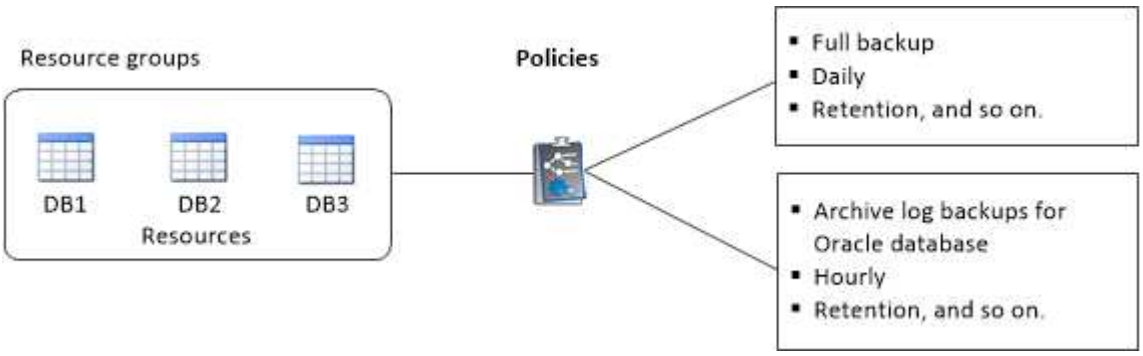
リソース グループはコンテナであり、バックアップして保護するリソースをここに追加します。リソース グループを使用することで、ファイルシステムに関連付けられているすべてのデータをバックアップできます。

タスク概要

- 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 グループにファイルが格納されているデータベースが「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、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の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あと、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アクティブ同期のフェイルオーバー モードである既存のリソース 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リソース グループのみです。

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. [Name]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文字以内で指定する必要があります。

   b. あとでリソース グループを検索できるように、[Tag]フィールドに1つ以上のラベルを入力します。

      たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

   c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を

入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

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。

   [Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [Available Resources]セクションでリソースを選択し、[Selected Resources]セクションに移動します。
6. [Application Settings]ページで、次の操作を実行します。
   - [Scripts]の矢印を選択し、休止、Snapshot、および休止解除の処理を行うプリコマンドとポストコマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
   - 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。
     - バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされ、バックアップの作成中にファイル 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 システムの一貫性] を選択します。

       [File System Consistent]を選択した場合、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 システムのキャッシュ データがフラッシュされるようにする場合は、クラッシュ整合性 を選択します。

       リソース グループに複数の異なる種類のファイルシステムを追加した場合は、リソース グループ内の各種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。

      [Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

   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. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[**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。

      設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 通知ページの 電子メール設定 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」を選択します。

   Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtpServer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。

9. 概要を確認し、[完了] をクリックします。

ASA r2 システム上の Unix ファイルシステムのリソースグループを作成し、二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成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 グループに追加していないことを確認する必要があります。
- 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存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっている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すると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

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. [Name]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文字以内で指定する必要があります。

   b. あとでリソース グループを検索できるように、[Tag]フィールドに1つ以上のラベルを入力します。

      たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

   たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。

   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。

   [Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、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。

      [Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

   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. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[**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。

      設定したスケジュールが[Applied Schedules]列にリストされます。

   サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、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. 使用する整合性グループのサフィックスを指定します。

c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。

クラスターと 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 [セカンダリ保護リソース] 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. 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で検証を実行します。
   b. クリック + ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で 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	*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*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

   d. 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 ロケーションで検証] 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が、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 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」を選択します。

   Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtpServer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。

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

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから パス を選択します。
3. クリック  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ーします。
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]ページで実行できる手順は次のとおりです。
   a. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

      例えば、 `customtext_policy_hostname`または `resource_hostname`。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。
6. [Application Settings]ページで、次の操作を実行します。
   - [Scripts]の矢印を選択し、休止、Snapshot、および休止解除の処理を行うプリコマンドとポストコマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
   - 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。
     - バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされ、バックアップの作成中にファイル システムで操作が実行されないようにするには、[ファイル システムの整合性] を選択します。
     - バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされるようにする場合は、クラッシュ整合性 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。

      クリックするとポリシーを作成できます  。

      [Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。
   b. クリック  必要なポリシーのスケジュールを構成するには、[スケジュールの構成] 列をクリックします。
   c. 「ポリシー_policy_name_のスケジュールを追加」ウィンドウでスケジュールを設定し、 `OK`。

      policy_name は、選択したポリシーの名前です。

   設定したスケジュールが[Applied Schedules]列にリストされます。
8. 通知ページで、*電子メール設定*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。

   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。リソースに対して実行されたバックアップ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」を選択します。

電子メール通知の場合は、GUIまたはPowerShellコマンドを使用してSMTPサーバーの詳細を指定する必要があります。 `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]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、バックアップに使用するポリシーを[Policy]ドロップダウン リストから選択します。

       オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの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. モニター > ジョブ をクリックして、操作の進行状況を監視します。

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、かつスケジュールが設定されている場合は、スケジュールに従って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]ページで次の手順を実行します。
    a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから使用するバックアップ ポリシーを選択します。

       オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

    b. *バックアップ*を選択します。
6. モニター > ジョブ を選択して進行状況を監視します。

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の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、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。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] 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]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*バックアップ*を選択します。
   d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
   e. 正常に完了した操作を表示するには、[適用] をクリックします。
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 ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

   ログを表示 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

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各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. クリック アクティビティ ペインで、最新の 5 つの操作を表示します。

   いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

[Topology]ページで保護されているUNIXファイルシステムの表示

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際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップ、リストアしたファイル システム、およびクローンの図を表示すると役に立ちます。

このタスクについて

[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップ、リストアしたファイルシステム、およびクローンをすべて表示できます。これらのバックアップ、リストアしたファイルシステム、およびクローンの詳細を参照し、対象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）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 ストレージで使用可能なバックアップとクローンの数を表示します。
- SnapMirrorテクノロジー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とクローンの数を表示します。
- SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。

  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個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。

mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数にはバージョンに依存しないバックアップは含まれません。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

- レプリカサイトが稼働しています。
- レプリカサイトはダウンしています。

- ? セカンダリ ミラーまたはボールト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[Topology]ページが表示されます。

4. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上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開始され、正確な数が表示されます。

   SnapLock対応バックアップが取得された場合、[更新] 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も、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

   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有効期限はONTAPから取得されます。

   SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAP を照会して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も、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

   - SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、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または非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、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。バックアップが作成された後にのみ、「更新」をクリックできます。

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 ストレージ上のバックアップは、名前変更または削除できません。

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

- 次の各コマンドを実行して、SnapCenter Serverとの接続を確立し、バックアップをリストしてその情報を取得し、バックアップをリストアする必要があります。

  コマンドで使用できるパラメータとその説明に関する情報は、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アクティブ同期でリストア処理を実行するには、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] のいずれかを選択します。

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、プライマリまたはセカンダリ (ミラーリングまたは複製された) ストレージ システムから [バックアップ] を選択します。

5. 表からバックアップを選択し、*をクリックします。  *。

6. [Restore Scope]ページ：

   - NFS ファイル システムの場合、デフォルトで 接続とコピー 復元が選択されます。 *ボリュームの復元*または*高速復元*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範囲が選択されます。

     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処理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処理のコマンドを入力します。

   プラグイン ホスト上の */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config* パスにあるコマンド 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。実行された復元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」を選択する必要があります。

   Eメール通知を利用する場合は、GUIまたはPowerShellコマンドSet-SmSmtpServer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のロールバックはサポートされていません。

    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、デフォルトのNFSファイルシステムがリストアされる場合に該当します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

UNIXファイルシステムのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどう

かを確認できます。

タスク概要

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]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、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*復元*を選択します。
   d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
   e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[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。

   ログを表示 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

- */opt/ NetApp/snapcenter/scc/etc* にある *agent.properties* ファイルで *SKIP_FSTAB_UPDATE* の値を **true** に設定することで、fstab ファイルの更新をスキップできます。
- */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** に設定することで、静的なクローン ボリューム名とジャンクション パスを設定できます。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: このプロパティがない場合、クローン ボリューム名とジャンクション パスは <Source_volume_name>_Clone_<Timestamp> のようになりますが、このプロパティを使用すると <Source_volume_name>_Clone_<Clone_Name> になります。

これにより名前が一定に保たれ、SnapCenterによってfstabが更新されるのが好ましくない場合に、fstab ファイルを手動で更新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 [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] のいずれかを選択します。
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]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、次の操作を実行します。

フィールド	操作
Clone server	ソース ホストがデフォルトで入力されています。
Clone mount point	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。

   ⓘ *_/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_* パスからプラグイン ホスト上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確認する必要があります。

8. 通知ページの 電子メール設定 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。実行されたクローン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」を選択します。

   ⓘ Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtpServer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。

9. 概要を確認し、[完了] をクリックします。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

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。

タスク概要

- 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 バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。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。

  クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- 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ボリューム分割操作の詳細については、以下を参照してください。 "親ボリュームからのFlexCloneボリュームのスプリット" 。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース*ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

   リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

   SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。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。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり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 がクローン分割操作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。

関連情報

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

UNIXファイルシステムのクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、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. *タイプ*ドロップダウンリストから*クローン*を選択します。
   d. *ステータス*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. 正常に完了した操作を表示するには、[適用] をクリックします。

4. クローンジョブを選択し、[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。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。