



UNIXファイルシステムの保護

SnapCenter Software 6.0

NetApp
September 17, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter/protect-scu/concept_overview_snapcenter_plug_in_for_UNIX_file_systems.html on September 17, 2024. Always check docs.netapp.com for the latest.

目次

UNIXファイルシステムの保護	1
UNIXファイルシステム用SnapCenterプラグインの機能	1
SnapCenter Plug-in for Unixファイルシステムのインストール	2
SnapCenter Plug-in for VMware vSphere をインストール	13
UNIXファイルシステムの保護の準備	13
UNIXファイルシステムのバックアップ	14
UNIXファイル・システムのリストアとリカバリ	25
UNIXファイルシステムのクローニング	28

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を設定します
- ファイルシステムのバックアップをリストア
- ファイルシステムのバックアップをクローニングする
- バックアップ、リストア、クローニングの各処理を監視する

サポートされている構成

項目	サポートされる構成
環境	<ul style="list-style-type: none">• 物理サーバ• 仮想サーバ <p>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。</p>
オペレーティングシステム	<ul style="list-style-type: none">• Red Hat Enterprise Linux の場合• Oracle Linux の場合• SUSE Linux Enterprise Server （ SLES ）
ファイルシステム	<ul style="list-style-type: none">• SAN ：<ul style="list-style-type: none">◦ 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

項目	サポートされる構成
プロトコル	<ul style="list-style-type: none"> • FC • FCoE • iSCSI • NFS
マルチパス	はい。

制限

- 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できるように root 以外のユーザに sudo 権限を設定する必要があります。プラグインをインストールすると、有効なroot以外のユーザとしてプロセスが実行されるようになります。

- 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 のダウンロード方法については、次を参照してください。 ["すべてのオペレーティングシステム用の"](#)

Java のダウンロード"

- 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	<ul style="list-style-type: none">• Red Hat Enterprise Linux の場合• Oracle Linux の場合• SUSE Linux Enterprise Server (SLES)
ホスト上の SnapCenter プラグインの最小 RAM	2 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	2 GB  十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	Java 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、 <code>/var/opt/snapcenter/etc/sp/etc/spl.properties</code> にある <code>JAVA_HOME</code> オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。

サポートされ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 Tool¹]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、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、* Hosts *（ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（Add）] をクリックします。
4. Hosts ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	ホストタイプとして* Linux *を選択します。
ホスト名	<p>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。</p> <p>SnapCenter は、DNS の適切な設定によって異なります。そのため、FQDN を入力することを推奨します。</p> <p>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。</p>
クレデンシャル	<p>作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。</p> <p>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。</p> <p>クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。</p> <div><p>クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。</p></div>

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	手順
ポート	<p>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。</p> <p>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。</p> <div>  <p>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。</p> </div>
インストールパス	<p>デフォルトパスは、 <code>_/opt/NetApp/snapcenter _</code> です。</p> <p>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、<code>sudoers</code>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。</p>
オプションのプレインストールチェックを省略します	<p>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。</p>

7. [Submit（送信）] をクリックします。

[事前確認をスキップする] チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。



ファイアウォールの拒否ルールで指定されているプラグインポートのファイアウォールステータスは、事前確認スクリプトで検証されません。

最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。エラーがディスクスペースまたは RAM に関連している場合は、`C : \Program Files\NetApp\Virtual\SnapCenter WebApp` にある `web.config` ファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連する場合は、問題を修正する必要があります。



HA セットアップで `web.config` ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. 指紋を確認し、 * 確認して送信 * をクリックします。



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を監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

このタスクについて

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [* 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 サービスを設定します

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します

spl.properties ファイルは、`/custom_location/NetApp/snapcenter /spl/etc/` にあり、次のパラメータを含みます。これらのパラメータにはデフォルト値が割り当てられています。

パラメータ名	説明
LOG_LEVEL の値	サポートされるログレベルを表示します。 指定できる値は、trace、debug、info、warn、error、致命的だ
SPL プロトコル	SnapCenter Plug-in Loader でサポートされているプロトコルを表示します。 HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
SNAPCENTER_server_protocol」を参照してください	SnapCenter サーバでサポートされているプロトコルを表示します。 HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
ske_JAVAHOME_update を実行します	デフォルトでは、SPL サービスは Java パスを検出し、JAVA_HOME パラメータを更新します。 したがって、デフォルト値は FALSE に設定されます。デフォルトの動作を無効にして Java パスを手動で修正する場合は、true に設定します。
SPL キーストアパス	キーストアファイルのパスワードを表示します。 この値は、パスワードを変更する場合や新しいキーストアファイルを作成する場合にのみ変更できません。

パラメータ名	説明
SPL ポート	<p>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。</p> <p>デフォルト値がない場合は、値を追加できます。</p> <div>  <p>プラグインのインストール後は値を変更しないでください。</p> </div>
SNAPCENTER_server_host が必要です	SnapCenter サーバの IP アドレスまたはホスト名を表示します。
SPL キーストアパス	キーストアファイルの絶対パスを表示します。
SNAPCENTER_SERVER_PORT	SnapCenter サーバが稼働しているポート番号を表示します。
logs_MAX_COUNT	<p>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。</p> <p>デフォルト値は 5000 に設定されています。指定した値よりも多い数のファイルがある場合は、変更後の最新の 5000 個のファイルが保持されます。ファイル数のチェックは、SnapCenter Plug-in Loader サービスが開始されたときから 24 時間ごとに自動的に行われます。</p> <div>  <p>spl.properties ファイルを手動で削除すると、保持されるファイル数は 9999 に設定されます。</p> </div>
JAVA_HOME にアクセスします	<p>SPL サービスの開始に使用される JAVA_HOME の絶対ディレクトリパスを表示します。</p> <p>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。</p>
LOG_MAX_SIZE	<p>ジョブログファイルの最大サイズを表示します。</p> <p>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。</p>
retain_logs_of_last_days	ログを保持する日数が表示されます。

パラメータ名	説明
enable_certificate_validationを実行します	<p>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。</p> <p>このパラメータを有効または無効にするには、spl.propertiesを編集するか、SnapCenter GUIまたはコマンドレットを使用します。</p>

これらのパラメータのいずれかがデフォルト値に割り当てられていない場合、または値を割り当てたり変更したりする場合は、spl.properties ファイルを変更します。また、spl.properties ファイルを確認して編集し、パラメータに割り当てられている値に関連する問題のトラブルシューティングを行うこともできます。spl.properties ファイルを変更したら、SnapCenter Plug-in Loader サービスを再起動する必要があります。

• 手順 *

1. 必要に応じて、次のいずれかの操作を実行します。

- 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 コマンドに -force オプションを指定すると、SnapCenter Plug-in Loader サービスを強制的に停止できます。ただし、既存の処理が終了するため、実行する前に十分に注意する必要があります。

- SnapCenter Plug-in Loader サービスを再起動します。
 - 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 ホストに **SnapCenter Plug-in Loader (SPL)** サービスを使用して **CA** 証明書を設定します

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 は、ファイル 'keystore.jks' を使用します。このファイルは、'/var/opt/snapcenter /spl/etc' にあり、どちらもトラストストアおよびキーストアとして使用されます。

SPL キーストアのパスワードと使用中の **CA** 署名済みキーペアのエイリアスを管理します

• 手順 *

1. SPL プロパティファイルから SPL キーストアのデフォルトパスワードを取得できます。

これはキー 'PL_keystore.pass' に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

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

spl.properties ファイル内のキー SPL の _keystore.pass に対しても同じ内容を更新します。

3. パスワードを変更したら、サービスを再起動してください。



SPL キーストアのパスワードと秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書を **SPL** の信頼ストアに設定します

SPL の信頼ストアへの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

• 手順 *

1. SPL キーストアが格納されているフォルダ（/var/opt/snapcenter /spl/etc_）に移動します。

2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v -keystore keystore.jks  
． ルート証明書または中間証明書を追加します。
```

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath>  
-keystore keystore.jks  
． SPL  
の信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動します。
```



ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアを SPL の信頼ストアに設定します

CA 署名鍵ペアを SPL 信頼ストアに設定する必要があります。

• 手順 *

1. SPL のキーストア /var/opt/snapcenter /spl/ などを含むフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v -keystore keystore.jks  
． 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS  
． キーストアに追加された証明書を表示します。
```

```
keytool -list -v -keystore keystore.jks  
． キーストアに、キーストアに追加された新しい CA  
証明書に対応するエイリアスが含まれていることを確認します。  
． CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。
```

デフォルトの SPL キーストアパスワードは、spl.properties ファイル内のキー SPL の keystore.pass の値です。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"  
-keystore keystore.jks  
・ CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「 *  
」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias  
"<NewAliasName>" -keystore keystore.jks  
・ spl.properties ファイルにあるキーストアからエイリアス名を設定します。
```

この値をキー SPL の certificate_alias に更新します。

4. CA 署名済みキーペアを SPL 信頼ストアに設定したら、サービスを再起動します。

SPL の証明書失効リスト（CRL）を設定します

SPL 用に CRL を設定する必要があります

- ・ このタスクについて *
- ・ SPL は、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- ・ SPL の CRL ファイルのデフォルトディレクトリは、_var/opt/snapcenter /spl/etc/crl_ です。
- ・ 手順 *
- 1. spl.properties ファイル内のデフォルトディレクトリを、キー SPL_CRL_PATH に対して変更および更新できます。
- 2. このディレクトリに複数の CRL ファイルを配置できます。

着信証明書は各 CRL に対して検証されます。

プラグインの CA 証明書を有効にします

CA 証明書を設定し、SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。プラグインの CA 証明書検証を有効にする必要があります。

作業を開始する前に

- ・ 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。

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





手順

1. 左側のナビゲーションペインで、* Hosts *（ホスト）をクリックします。
2. [Hosts] ページで、[*Managed Hosts] をクリックします。

3. 1 つまたは複数のプラグインホストを選択します。
4. [* その他のオプション *] をクリックします。
5. [証明書の検証を有効にする] を選択します。

完了後

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

-  は、CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
-  CA 証明書が正常に検証されたことを示します。
-  は、CA 証明書を検証できなかったことを示します。
-  接続情報を取得できなかったことを示します。



ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

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

データベース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。

導入の詳細については、を参照してください ["導入の概要"](#)。

CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください ["SSL 証明書を作成またはインポートします"](#)。

CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere は、事前に設定されたディレクトリ内の CRL ファイルを検索します。VMware vSphere 用 SnapCenter プラグインの CRL ファイルのデフォルトディレクトリは、`_opt/NetApp/config/crl_` です。

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

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 テクノロジを活用するには、ストレージデバイス上のソースボリュームとデスティネーションボリューム間のデータ保護関係を設定して初期化する必要があります。これらのタスク

を実行するには、NetAppSystem Manager を使用するか、ストレージコンソールのコマンドラインを使用します。

Plug-in for 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。 ["詳細はこちら。"](#)
- ストレージシステム接続を追加して SnapCenter 環境を設定します。 ["詳細はこちら。"](#)



SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SVM 登録またはクラスタ登録を使用して SnapCenter に登録する SVM は、それぞれ一意である必要があります。

- 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。

作業を開始する前に

- SnapCenterサーバのインストール、ホストの追加、ストレージシステム接続の作成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 を導入"](#)。

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、バックアップを管理、スケジューリング、および保持する方法を定めた一連のルールです。レプリケーション、スクリプト、バックアップタイプの設定を指定することもできます。ポリシーを作成することで、別のリソースやリソースグループでポリシーを再利用して時間を節約することができます。

作業を開始する前に

- 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. [保持] ページで ' バックアップ・タイプの保持設定と [バックアップ・タイプ] ページで選択したスケジュール・タイプを指定します

状況	作業
----	----

一定数のSnapshotを保持	<p>[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。</p> <p>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。</p> <div> <p> 最大保持数は、ONTAP 9.4 以降のリソースでは 1018、ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。</p> <p> 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。</p> </div>
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、アーカイブログファイルをバックアップの一部として選択した場合だけです。

8. Replication（レプリケーション）ページで、レプリケーション設定を指定します。

フィールド	手順
ローカル Snapshot コピーの作成後に SnapMirror を更新します	<p>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。</p> <p>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。</p>
ローカル Snapshot コピーの作成後に SnapVault を更新します	ディスクツーディスクのバックアップレプリケーション（SnapVault バックアップ）を実行する場合は、このオプションを選択します。

フィールド	手順
セカンダリポリシーのラベル	<p>Snapshot ラベルを選択します。</p> <p>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。</p> <div>  <p>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。</p> </div>
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。

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

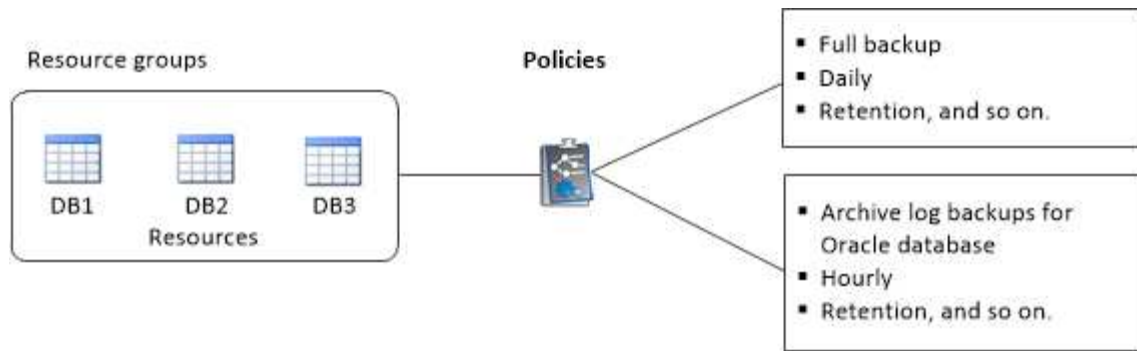
リソースグループはコンテナであり、バックアップして保護するリソースを追加します。リソースグループを使用すると、ファイルシステムに関連付けられているすべてのデータをバックアップできます。

このタスクについて

- Oracle DBVERIFYユーティリティを使用してバックアップを検証するには、ASMディスクグループ内のファイルを含むデータベースが「mount」または「open」状態である必要があります。

リソースグループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義します。

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



- 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、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. 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。最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

5. [使用可能なリソース (Available Resources)] セクションからリソースを選択し、[選択したリソース (Selected Resources)] セクションに移動する。
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。

- 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。

- をクリックします  スケジュールを設定するポリシーの Configure Schedules （スケジュールの設定）列。
- [Add schedules for policy_name] ウィンドウで、スケジュールを設定し、[OK] をクリックします。

ここで、_policy_name_ は 選択したポリシーの名前です。

設定されたスケジュールは、[適用されたスケジュール] 列に一覧表示されます。

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

8. [通知] ページの [電子メールの設定 *] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、[ジョブレポートの添付 (Attach Job Report)] を選択します。




Eメール通知を利用する場合は、GUI または PowerShell コマンド Set-SmtpServer を使用して、SMTP サーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了] をクリックします。

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含まれていないリソースは、のリソースページからバックアップすることができます。

手順


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

例： `customtext_policy_hostname` または `resource_hostname`。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. をクリックします  [Configure Schedules]列で、ポリシーのスケジュールを設定します。
- c. [Add schedules for policy_policy_name_]ウィンドウでスケジュールを設定し、を選択します OK。

_policy_name_ は、選択したポリシーの名前です。

設定されたスケジュールは、[適用されたスケジュール] 列に一覧表示されます。

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-SmSmtServer`。

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がバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されません。


- 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、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、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、をクリックします  をクリックし、タグを選択します。

をクリックします  をクリックしてフィルタペインを閉じます。

4. [Resource Group] ページで、バックアップするリソースグループを選択します。
5. Backup (バックアップ) ページで、次の手順を実行します。
 - a. リソースグループに複数のポリシーが関連付けられている場合は、*[ポリシー]*ドロップダウンリストから使用するバックアップポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されません。

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、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

このタスクについて


以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され
-  キャンセルされました

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [モニター] ページで、[* ジョブ *] をクリックします。
3. Jobs (ジョブ) ページで、次の手順を実行します。
 - a. をクリックします  バックアップ処理だけが表示されるようにリストをフィルタリングします。
 - b. 開始日と終了日を指定します。
 - c. [* タイプ] ドロップダウン・リストから、[*Backup] を選択します。
 - d. [Status](ステータス*) ドロップダウンから、バックアップステータスを選択します。
 - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
4. バックアップジョブを選択し、[* 詳細 *] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスがと表示されます  で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

5. [ジョブの詳細] ページで、[* ログの表示 *] をクリックします。


View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity] ペインでデータ保護操作を監視します

[アクティビティ (Activity)] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity (アクティビティ)] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。

手順

1. 左側のナビゲーションペインで、* リソース * をクリックし、リストから適切なプラグインを選択します。
2. をクリックします  をクリックして、最近の 5 つの操作を表示します。

いずれかの処理をクリックすると、*[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。

[コピーの管理] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ (ミラーコピーまたはバックアップコピー) でバックアップとクローンが使用可能かどうかを判断できます。




-  には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
-  には、SnapMirror テクノロジ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たバックアップとクローンの数が表示されます。
-  には、SnapVault テクノロジーを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。

表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、4 つのバックアップだけを保持するポリシーを使用して 6 つのバックアップを作成した場合、バックアップの数は 6 と表示されます。



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

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. 概要カードを確認して、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数をサマリで確認します。

サマリカードセクションには、バックアップとクローンの合計数が表示されます。

「* Refresh *」 ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

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

コマンドで利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メール通知を利用する場合は、GUI または PowerShell コマンド `Set-SmtpServer` を使用して、SMTP サーバの詳細を指定しておく必要があります。

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、SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。


このタスクについて

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され
-  キャンセルされました

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. **[* 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. をクリックします  リストをフィルタリングして、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. **[* タイプ *]** ドロップダウン・リストから、**[リストア *]** を選択します。
 - d. **[* Status *]** ドロップダウン・リストから、**リストア・ステータス**を選択します。
 - e. **[適用 (Apply)]** をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、*** Details *** をクリックして、ジョブの詳細を表示します。
5. **[* ジョブの詳細 *]** ページで、**[* ログの表示 *]** をクリックします。

View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

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。

作業を開始する前に

- 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、次の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、バックアップを[ローカルコピー]（プライマリ）、[ミラーコピー]（セカンダリ）、または[バックアップコピー]（セカンダリ）から選択します。
5. 表からバックアップを選択し、*****をクリックします  *****
6. Location ページで、次のアクションを実行します。

フィールド	手順
クローンサーバ	ソースホストがデフォルトで入力されています。
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メール通知を利用する場合は、GUI または PowerShell コマンド `Set-SmtpServer` を使用して、SMTP サーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了] をクリックします。
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します。

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

このタスクについて

- 中間のクローンに対してクローンスプリット処理を実行することはできません。

たとえば、データベースバックアップから clone1 を作成したあとで、Clone1 のバックアップを作成し、そのバックアップ（Clone2）をクローニングできます。Clone2 を作成すると、clone1 は中間クローンであり、clone1 でクローンスプリット処理を実行することはできません。ただし、Clone2 でクローンスプリット処理を実行することはできます。

Clone2 をスプリットしたあとは、clone1 が中間クローンではなくなるため、clone1 でクローンスプリット処理を実行できます。

- クローンをスプリットすると、クローンのバックアップコピーとクローンジョブが削除されます。
- クローンスプリット処理の制限事項については、を参照してください ["ONTAP 9 論理ストレージ管理ガイド"](#)。
- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順


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

リソースの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しなくなります。Stop-SmJob コマンドレットを実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、_SMCoreServiceHost.exe.config_file の_CloneSplitStatusCheckPollTime_Parameter の値を変更して、SMCore がクローンスプリット処理のステータスをポーリングする間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローンスプリットの実行中は、クローンスプリットの開始処理が失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

関連情報




"「aggregate does not exist」 というメッセージが表示されて、SnapCenter クローンまたは検証が失敗する"


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。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

このタスクについて

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-

 警告で終了したか、警告が原因で起動できませんでした

-  キューに登録され
-  キャンセルされました
- 手順 *
 1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
 2. [* 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. をクリックします  をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
 - b. 開始日と終了日を指定します。
 - c. [Type](タイプ) ドロップダウンリストから '[*Clone](クローン *)' を選択します
 - d. [* Status *] ドロップダウン・リストから、クローンのステータスを選択します。
 - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
 4. クローンジョブを選択し、 * Details * をクリックして、ジョブの詳細を表示します。
 5. [ジョブの詳細] ページで、 [* ログの表示 *] をクリックします。

著作権に関する情報

Copyright © 2024 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权を有し、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权については、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。