UNIXファイルシステムのバックアップ

SnapCenter software

NetApp
November 06, 2025

目次

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

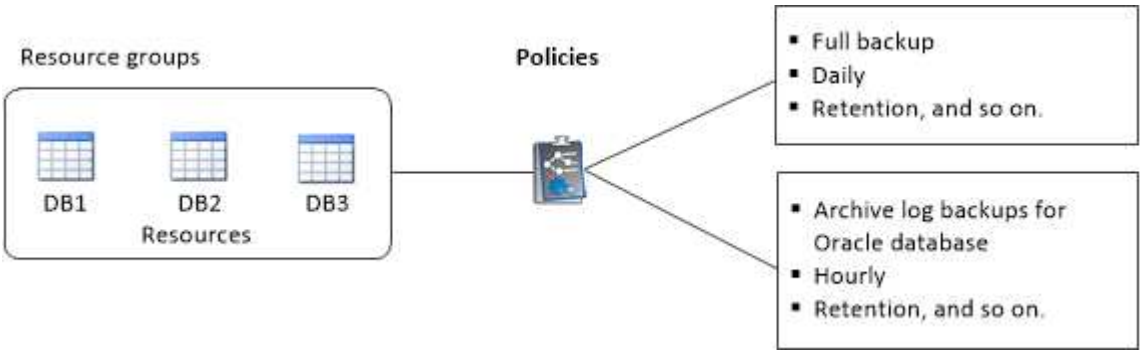
リソース グループはコンテナであり、バックアップして保護するリソースをここに追加します。リソース グループを使用することで、ファイルシステムに関連付けられているすべてのデータをバックアップできます。

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

著作権に関する情報

商標に関する情報