SAP HANAリソースのバックアップ

SnapCenter software

NetApp
November 06, 2025

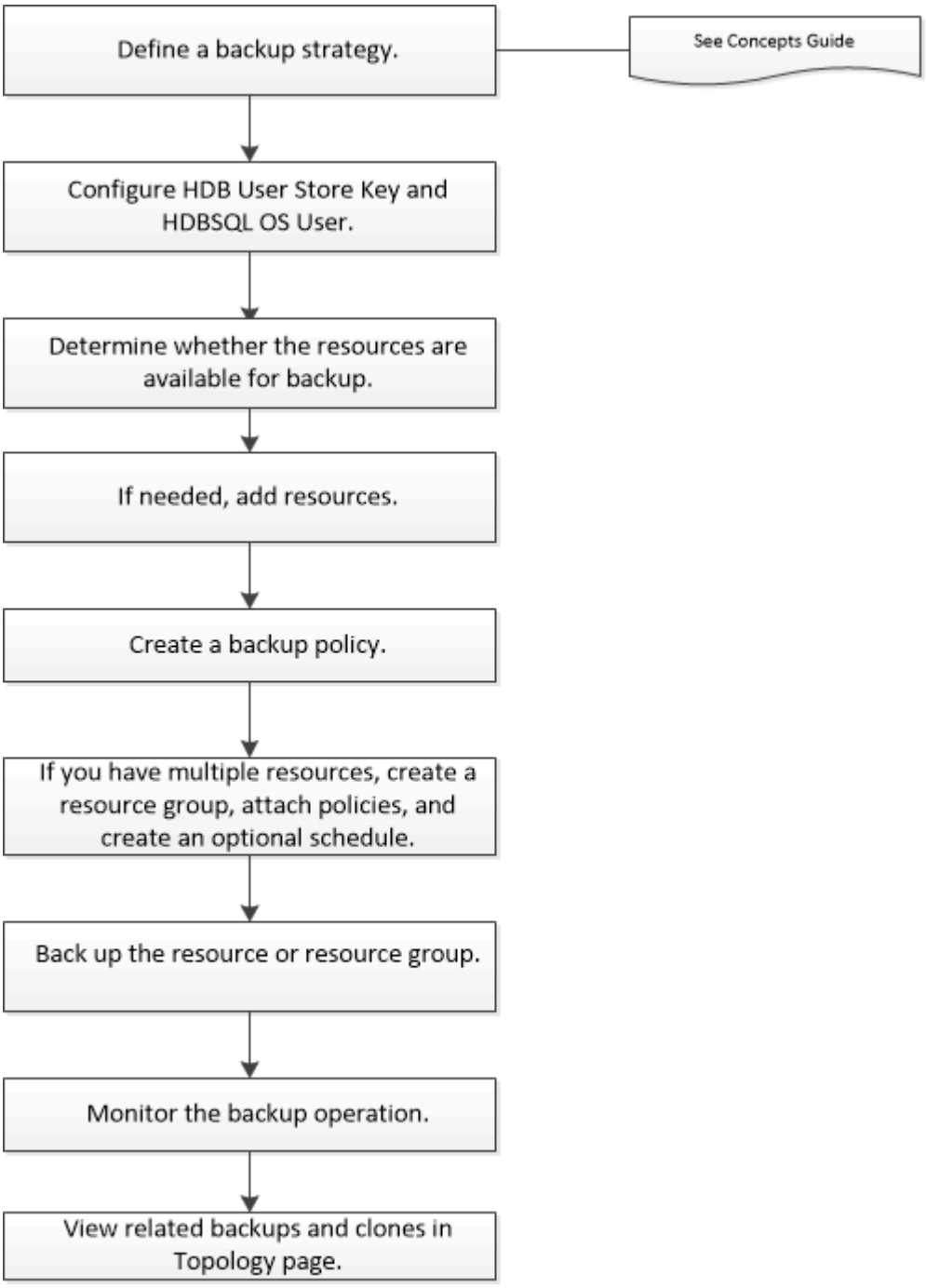
目次

SAP HANAリソースのバックアップ

SAP HANAリソースのバックアップ

リソース（データベース）またはリソース グループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするデータベースの特定、バックアップ ポリシーの管理、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenterソフトウェア コマンドレット リファレンス ガイド"^] 。

SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定

SAP HANAデータベースでデータ保護処理を実行するには、HDBユーザ ストア キーとHDBSQL OSユーザを設定する必要があります。

開始する前に

- SAP HANAデータベースにHDBのセキュアなユーザ ストア キーとHDB SQL OSユーザが設定されていない場合は、自動検出されたリソースに対してのみ赤い南京錠アイコンが表示されます。以降の検出処理中に、設定済みのHDBのセキュアなユーザ ストア キーが正しくないか、データベース自体へのアクセスが提供されていないと判断された場合は、赤い南京錠アイコンが再表示されます。
- データベースを保護できるようにHDBのセキュアなユーザ ストア キーとHDB SQL OSユーザを設定するか、またはデータベースをリソース グループに追加してデータ保護処理を実行する必要があります。
- システム データベースにアクセスするようにHDB SQL OSユーザを設定する必要があります。テナント データベースにのみアクセスするようにHDB SQL OSユーザが設定されている場合、検出処理は失敗します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから[SnapCenter Plug-in for SAP HANA Database] を選択します。
2. [リソース] ページで、[表示] リストからリソース タイプを選択します。
3. （オプション）クリック  ホスト名を選択します。

   そのあとに  をクリックすると、フィルタ ペインが閉じます。
4. データベースを選択し、「データベースの構成」をクリックします。
5. [Configure database settings]セクションで、「HDB Secure User Store Key」と入力します。

   プラグインのホスト名が表示され、HDB SQL OS ユーザーは <sid>adm に自動的に入力されます。
6. [OK]をクリックします。

[Topology]ページでデータベース設定を変更できます。

データ保護のためのリソースの検出とマルチテナント データベース コンテナの準備

データベースの自動的検出

リソースとは、SnapCenterで管理するLinuxホスト上のSAP HANAデータベースとデータ ボリューム以外のボリュームです。使用できるSAP HANAデータベースを検出したあとに、これらのリソースをリソース グループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、HDBユーザ ストア キーの追加、ホストの追加、ストレージ システム接続のセットアップなどのタスクを完了しておく必要があります。
- LinuxホストでHDBのセキュアなユーザ ストア キーとHDBSQL OSユーザを設定しておく必要があります。
  - SID admユーザを使用してHDBユーザ ストア キーを設定する必要があります。たとえば、SIDとしてA22を使用するHANAシステムの場合は、HDBユーザ ストア キーをa22admに設定します。
- SnapCenter Plug-in for SAP HANA Databaseでは、RDM / VMDK仮想環境にあるリソースの自動検出がサポートされていません。データベースを手動で追加する際に、仮想環境のストレージの情報を指定する必要があります。

タスク概要

プラグインをインストールすると、そのLinuxホスト上のすべてのリソースが自動検出されて[Resources]ページに表示されます。

自動検出されたリソースを変更または削除することはできません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから SAP HANA データベース用プラグインを選択します。
2. [Resources]ページで、[View]リストからリソース タイプを選択します。
3. （オプション）をクリック、ホスト名を選択します。

   をクリックします フィルター パネルを閉じます。
4. ホスト上で利用可能なリソースを検出するには、[リソースの更新] をクリックします。

   リソースは、リソース タイプ、ホスト名、関連するリソース グループ、バックアップ タイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

   - データベースがNetAppストレージにあって保護されていない場合は、[Overall Status]列に「Not protected」と表示されます。
   - データベースがNetAppストレージ システム上にあって保護されており、バックアップ処理が実行されていない場合は、[Overall Status]列に「Backup not run is displayed」と表示されます。それ以外の場合は、前回のバックアップ ステータスに基づいて、ステータスが「バックアップに失敗しました」または「バックアップに成功しました」に変わります。

> SAP HANAデータベースでHDBのセキュアなユーザ ストア キーが設定されていない場合は、リソースの横に赤い南京錠アイコンが表示されます。以降の検出処理中に、設定済みのHDBのセキュアなユーザ ストア キーが正しくないか、データベース自体へのアクセスが提供されていないと判断された場合は、赤い南京錠アイコンが再表示されます。

SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

終了後の操作

データベースを保護できるようにHDBのセキュアなユーザ ストア キーとHDBSQL OSユーザを設定するか、またはデータベースをリソース グループに追加してデータ保護処理を実行する必要があります。

"SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定"

データ保護のためのマルチテナント データベース コンテナの準備

SnapCenterに直接登録されているSAP HANAホストの場合、SnapCenter Plug-in for SAP HANA Databaseをインストールまたはアップグレードすると、ホスト上のリソースの自動検出がトリガーされます。プラグインのインストールまたはアップグレード後には、プラグイン ホストに配置されていたマルチテナント データベース コンテナ（MDC）リソースそれぞれが、異なるGUID形式を持つ別のMDCリソースとして自動的に検出され、SnapCenterに登録されます。新しいリソースは「ロックされた」状態になります。

タスク概要

たとえば、SnapCenter 4.2で、E90 MDCリソースがプラグイン ホストにあり、手動で登録されていた場合、SnapCenter 4.3へのアップグレード後には、異なるGUIDを持つ別のE90 MDCリソースが検出されてSnapCenterに登録されます。

SnapCenter 4.2以前のバージョンのリソースに関連するバックアップは、保持期間が終了するまで保持する必要があります。保持期間が終了したら、古いMDCリソースは削除してかまいません。自動検出された新しいMDCリソースで管理を続行できます。

`Old MDC resource`SnapCenter 4.2 以前のリリースで手動で追加されたプラグイン ホストの MDC リソースです。

SnapCenter 4.3で検出された新しいリソースを使用してデータ保護処理を行うには、次の手順を実行します。

手順

1. [リソース] ページで、以前のSnapCenterリリースにバックアップが追加された古い MDC リソースを選択し、[トポロジ] ページからそれを「メンテナンス モード」に設定します。

   リソースがリソース グループの一部である場合は、リソース グループを「メンテナンス モード」にします。

2. SnapCenter 4.3へのアップグレード後に検出された新しいMDCリソースを[Resources]ページで選択し、構成します。

   「新しい `MDC` リソース」は、 SnapCenterサーバとプラグイン ホストが 4.3 にアップグレードされた後に新しく検出された MDC リソースです。そのホストでの古いMDCリソースと同じSIDを持つリソースが新しいMDCリソースです。[Resources]ページでは、横に赤い南京錠のアイコンが表示されます。

3. 保護ポリシー、スケジュール、および通知設定を選択して、SnapCenter 4.3へのアップグレード後に検出された新しいMDCリソースを保護します。

4. 保持設定に基づいて、SnapCenter 4.2以前のリリースで作成されたバックアップを削除します。
5. [Topology]ページからリソース グループを削除します。
6. [Resources]ページから古いMDCリソースを削除します。

   たとえば、プライマリ スナップショットの保持期間が 7 日間で、セカンダリ スナップショットの保持期間が 45 日間の場合、45 日が経過し、すべてのバックアップが削除された後に、リソース グループと古い MDC リソースを削除する必要があります。

関連情報

"SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定"

"[Topologyページでの SAP HANAデータベースのバックアップとクローンの表示"]

手動でのプラグイン ホストへのリソースの追加

特定のHANAインスタンスでは、自動検出がサポートされていません。このようなリソースは手動で追加する必要があります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続のセットアップ、HDBユーザ ストア キーの追加などのタスクを完了しておく必要があります。
- SAP HANAシステム レプリケーションでは、そのHANAシステムのすべてのリソースを1つのリソース グループに追加し、リソース グループのバックアップを作成することを推奨します。これにより、テイクオーバー / フェイルバック モードでのシームレスなバックアップが保証されます。

"リソース グループの作成とポリシーの適用" 。

タスク概要

自動検出は、次の構成ではサポートされていません。

- RDMおよびVMDKレイアウト

  上記のリソースが検出された場合、これらのリソースではデータ保護処理がサポートされません。

- HANAマルチホスト構成
- 同じホスト上の複数のインスタンス
- マルチティア スケールアウトHANAシステム レプリケーション
- システム レプリケーション モードのカスケード レプリケーション環境

手順

1. 左側のナビゲーション ペインで、ドロップダウン リストから SAP HANA データベース用のSnapCenterプラグインを選択し、リソース をクリックします。
2. リソース ページで、**SAP HANA** データベースの追加 をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
リソース タイプ	リソース タイプを入力します。リソース タイプは、単一のコンテナ、マルチテナント データベース コンテナ（MDC）、データ ボリューム以外のボリュームです。
HANA システム名	SAP HANAシステムのわかりやすい名前を入力します。このオプションは、単一のコンテナまたはMDCリソース タイプを選択した場合にのみ使用できます。
SID	システムID（SID）を入力します。インストールされたSAP HANAシステムは単一のSIDで識別されます。
プラグイン ホスト	プラグイン ホストを選択します。
HDB のセキュアなユーザ ストア キー	SAP HANAシステムに接続するためのキーを入力します。 このキーには、データベースに接続するためのログイン情報が含まれます。 SAP HANAシステム レプリケーションでは、セカンダリ ユーザ キーは検証されません。これは、テイクオーバー時に使用されます。
HDBSQL OS ユーザ	HDB セキュア ユーザー ストア キーが設定されているユーザー名を入力します。 Windows の場合、HDBSQL OS ユーザーは SYSTEM ユーザーである必要があります。したがって、SYSTEM ユーザーに対して HDB セキュア ユーザー ストア キーを構成する必要があります。

4. [ストレージ フットプリントの提供] ページで、ストレージ システムを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] をクリックします。

   オプション：をクリックすることもできます  アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtree を追加します。

5. 概要を確認し、[完了] をクリックします。

   データベースは、SID、プラグイン ホスト、関連するリソース グループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

"ユーザまたはグループの追加と、ロールとアセットの割り当て"

データベースの追加が完了したら、SAP HANAデータベースの詳細を変更できます。

SAP HANAリソースに関連付けられているバックアップがある場合、次の項目は変更できません。

- マルチテナントデータベースコンテナ（MDC）：SIDまたはHDBSQLクライアント（プラグイン）ホスト
- 単一コンテナ: SID または HDBSQL クライアント (プラグイン) ホスト
- 非データボリューム: リソース名、関連SID、またはプラグインホスト

SAP HANAデータベースのバックアップ ポリシーの作成

SnapCenterを使用してSAP HANAデータベースのリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、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。

開始する前に

- バックアップ戦略を定義しておく必要があります。

  詳細については、SAP HANAデータベースのデータ保護戦略の定義に関する情報を参照してください。

- SnapCenterのインストール、ホストの追加、ストレージ システム接続の作成、リソースの追加など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。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

  ポリシーで、レプリケーション、スクリプト、アプリケーション設定を指定することもできます。それらのオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。

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

タスク概要

- SAP HANAシステム レプリケーション
  - プライマリSAP HANAシステムの保護では、すべてのデータ保護処理を実行できます。
  - セカンダリSAP HANAシステムの保護では、バックアップを作成することはできません。

    フェイルオーバー後は、セカンダリSAP HANAシステムがプライマリSAP HANAシステムになるため、すべてのデータ保護処理を実行できます。

  SAP HANAデータ ボリュームのバックアップを作成することはできませんが、SnapCenterはデータ以外のボリューム（NDV）の保護を継続します。

- SnapLock
  - [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. *新規*をクリックします。
4. 「名前」ページで、ポリシー名と詳細を入力します。
5. ポリシー タイプ ページで、次の手順を実行します。
   - ストレージタイプを選択
   - バックアップ タイプを選択します。

状況	操作
Snapshotテクノロジを使用してバックアップを作成する	*スナップショットベース*を選択します。
データベースの整合性チェックを実行する	*ファイルベースのバックアップ*を選択します。アクティブなテナントのみがバックアップされます。

6. スナップショットとレプリケーション ページで、次の手順を実行します。
   - 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 タイプを指定します。

> リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。

> 午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

7. [スナップショットとレプリケーション] ページで、[バックアップ タイプ] ページで選択したバックアップ タイプとスケジュール 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。 スナップショットの数が指定数を超えると、最も古いスナップショットが最初に削除されます。 最大保持値は 1018 です。保持期間がONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。 SnapshotコピーベースのバックアップでSnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。 SAP HANAシステム レプリケーションでは、SAP HANAシステムのすべてのリソースを1つのリソース グループに追加することを推奨します。これにより、適切な数のバックアップが保持されます。 SAP HANAシステム レプリケーションでは、作成されるSnapshotの総数はリソース グループに設定された保持数と同じになります。最も古いSnapshotが削除されるかどうかは、最も古いSnapshotが配置されているノードに基づいて決まります。たとえば、SAP HANAシステム レプリケーション プライマリとSAP HANAシステム レプリケーション セカンダリが含まれているリソース グループの保持数が7に設定されているとします。一度に作成できるSnapshotの数は、SAP HANAシステム レプリケーション プライマリとSAP HANAシステム レプリケーション セカンダリの両方を合わせて最大で7つです。

状況	操作
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、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

8. Snapshot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. スナップショット コピー ベースのバックアップの場合、[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
ローカル スナップショット コピーを作成した後、**SnapMirror** を更新します	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。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このSnapshotがリストア処理の対象としてデスティネーションで選択されると、「Secondary Location is not available for the selected vaulted/mirrored backup」というエラー メッセージが表示されます。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"[Topologyページでの](#)SAP HANAデータベースのバックアップとクローンの表示"] 。

フィールド	操作
ローカルスナップショットコピーを作成した後、**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。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、 ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、 ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、 "バックアップデスティネーションのSnapshotコピーのWORM状態へのコミット" 見る"[Topologyページでの](#)SAP HANAデータベースのバックアップとクローンの表示"] 。
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 ストレージでSnapshotの上限に達しないように、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。

10. 概要を確認し、[完了] をクリックします。

リソース グループ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する必要があります。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。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することも必要です。

タスク概要

- SAP HANAシステム レプリケーションのバックアップを作成するには、SAP HANAシステムのすべてのリソースを1つのリソース グループに追加することを推奨します。これにより、テイクオーバー / フェイルバック モードでのシームレスなバックアップが保証されます。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock 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。

- 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SnapMirrorアクティブ同期を使用しない新しいデータベースを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 グループに新しいデータベース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] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name]ページで、次の操作を実行します。

フィールド	操作
Name	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。
Tags	リソース グループを検索しやすくするために、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。
Use custom name format for Snapshot copy	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 リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。

   画面の情報がフィルタリングされます。

5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Application Settings]ページで、次の操作を実行します。

   a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。

      整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group Snapshot operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、「中」、または「緩和」を選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+ 

a. *スクリプト*矢印をクリックし、静止、スナップショット、および静止解除操作の事前コマンドと事後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。

b. *カスタム構成*矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
ARCHIVE_LOG_ENABLE	（Y / N）	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。
ARCHIVE_LOG_RETENTION	number_of_days	アーカイブ ログを保持する日数を指定します。 この設定は、NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。

パラメータ	設定	説明
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブ ログが含まれるディレクトリへのパスを指定します。
ARCHIVE_LOG_EXT	file_extension	アーカイブ ログ ファイルの拡張子の長さを指定します。 たとえば、アーカイブ ログが log_backup_0_0_0_0.16151855 1942 9 で、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。
ARCHIVE_LOG_RECURSIVE_ SE ARCH	（Y / N）	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。

カスタムのキーと値のペアは、SAP HANA Linuxプラグイン システムではサポートされますが、一元化されたWindowsプラグインとして登録されたSAP HANAデータベースではサポートされません。

c. スナップショット コピー ツール の矢印をクリックして、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する（このオプションはLinuxリソースには適用されません）	• ファイル システムの一貫性を備えたSnapCenter * を選択します。 このオプションは、SnapCenter Plug-in for SAP HANA Databaseには適用されません。
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。
Snapshotコピーを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行するコマンドを入力します。

7. [Policies]ページで、次の手順を実行します。

a. ドロップダウン リストから1つ以上のポリシーを選択します。

をクリックしてポリシーを作成することもできます 。

ポリシーが[Configure schedules for selected policies]セクションのリストに表示されます。

b. スケジュールの設定列で*をクリックします。 * 設定するポリシーの。

c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[**OK**] をクリックします。

policy_nameは、選択したポリシーの名前です。

構成されたスケジュールは、「適用されたスケジュール」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。SMTP サーバーは、設定 > グローバル設定 で設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

リソース グループを作成し、 ASA r2 システム上の SAP HANA リソースの二次保護を有効にする

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。

SAP HANAデータベース用のPowerShellコマンドレットを使用したストレージ システムへの接続とクレデンシャルの作成

PowerShellコマンドレットを使用してSAP HANAデータベースのバックアップ、リストア、クローニングを行う前に、Storage Virtual Machine（SVM）接続とクレデンシャルを作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、 SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「 NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

  SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

手順

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

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

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

   この例は、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する方法を示しています。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. SnapCenter ServerにSAP HANA通信ホストを追加します。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. パッケージとSnapCenter Plug-in for SAP HANA Databaseをホストにインストールします。

   Linux：

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

   Windows：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. HDBSQLクライアントのパスを設定します。

   Windows：

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

   Linux：

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

コマンドレットで使用できるパラメータとその説明に関する情報は、*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" 。

SAP HANAデータベースのバックアップ

どのリソース グループにも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。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「`snapmirror all`」権限が含まれている必要があります。ただし、「`vsadmin`」ロールを使用している場合は、「`snapmirror all`」権限は必要ありません。
- Snapshotコピーベースのバックアップ処理の場合は、すべてのテナント データベースが有効でアクティブであることを確認してください。
- SAP HANAシステム レプリケーションのバックアップを作成するには、SAP HANAシステムのすべてのリソースを1つのリソース グループに追加することを推奨します。これにより、テイクオーバー / フェイルバック モードでのシームレスなバックアップが保証されます。

  "リソース グループの作成とポリシーの適用" 。

  "リソース グループのバックアップ"

- 1つ以上のテナントデータベースがダウンしているときにファイルベースのバックアップを作成する場合は、HANAプロパティファイルでALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENTパラメータを*YES*に設定します。 `Set-SmConfigSettings`コマンドレット。

  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* を実行することで取得できます。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"

- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、プラグインホストで次のパスから使用できるコマンド リストにコマンドがあるかどうかを確認する必要があります。
  - Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

ⓘ コマンドがコマンド リストに存在しない場合、処理は失敗します。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。

   を選択、ホスト名とリソース タイプを選択して、リソースをフィルターします。次に選択できますフィルター パネルを閉じます。

3. バックアップするリソースを選択します。
4. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

   たとえば、*customtext_policy_hostname* または *resource_hostname* 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。

5. [Application Settings]ページで、次の操作を実行します。

   ◦ 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。

   必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for "Consistency Group Snapshot" operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、または「中」、または「緩和」を選択します。[Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

   ◦ *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。

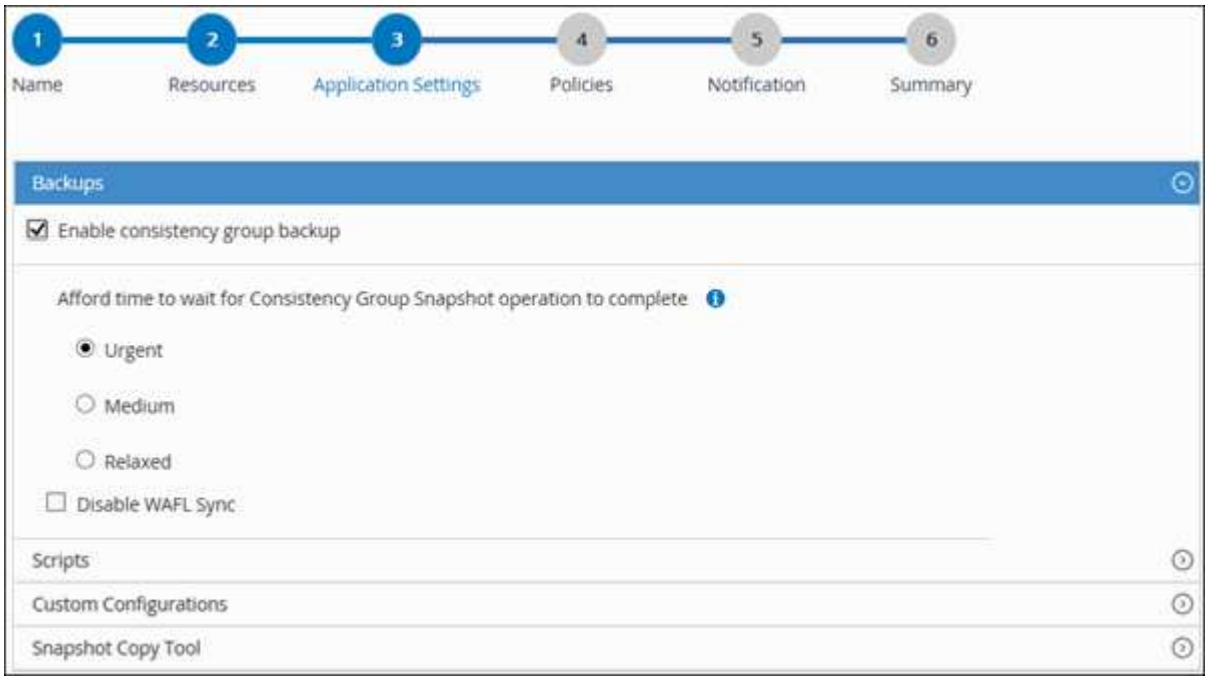
   バックアップ処理を終了する前のプリコマンドも実行できます。プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

   ◦ カスタム構成矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。

   ◦ スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	• ファイル システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。



6. [Policies]ページで、次の手順を実行します。

   a. ドロップダウン リストから1つ以上のポリシーを選択します。

      をクリックしてポリシーを作成することもできます + 。

      [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. を選択 + スケジュールを構成するポリシーの [スケジュールの構成] 列で、

   c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[**OK**] を選択します。

      policy_name は選択したポリシーの名前です。

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

7. 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。SMTP は、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] 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。

9. *今すぐバックアップ*を選択します。

10. [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、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

       オンデマンド バックアップ用に選択したポリシーがバックアップ 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。

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。

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

      詳細については、以下を参照してください。 "MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

    - VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

      Java ヒープ サイズを増やすには、スクリプト ファイル */opt/netapp/init_scripts/scvservice* を見つけます。このスクリプトでは、*do_start method* コマンドによってSnapCenter VMware プラグイン サービスが開始されます。このコマンドを次のように更新します: *Java -jar -Xmx8192M -Xms4096M*

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

   ```
   Open-smconnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、リソースを追加します。

   この例は、SingleContainerタイプのSAP HANAデータベースを追加する方法を示しています。

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary
"}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

この例は、MultipleContainersタイプのSAP HANAデータベースを追加する方法を示しています。

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

次の例は、データ ボリューム以外のリソースを作成する方法を示しています。

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。

   この例では、Snapshotコピーベースのバックアップのバックアップ ポリシーを作成しています。

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
   Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
   ```

   この例では、ファイルベースのバックアップのバックアップ ポリシーを作成しています。

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
   -PluginPolicyType hana -BackupType FileBasedBackup
   ```

4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソース グループを追加します。

   この例では、単一コンテナのリソースを保護しています。

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

この例では、複数コンテナのリソースを保護しています。

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

この例では、ポリシーとリソースを指定して新しいリソース グループを作成しています。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

この例では、データ ボリューム以外のリソース グループを作成します。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

   この例は、リソース グループをバックアップする方法を示しています。

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

この例では、保護されたリソースをバックアップしています。

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Get-smJobSummaryReportコマンドレットを使用して、ジョブのステータス（実行中、完了、失敗）を確認します。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップIDとバックアップ名など、バックアップ ジョブの詳細を監視します。

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

コマンドレットで使用できるパラメータとその説明に関する情報は、*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" 。

リソース グループのバックアップ

リソース グループは、ホスト上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「`snapmirror all`」権限が含まれている必要があります。ただし、「`vsadmin`」ロールを使用している場合は、「`snapmirror all`」権限は必要ありません。

タスク概要

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自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

   リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックして、タグを選択します。次に選択できますフィルター パネルを閉じます。
3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [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を関連付けた場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

      オンデマンド バックアップ用に選択したポリシーがバックアップ 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。
5. モニター > ジョブ を選択して、操作の進行状況を監視します。

SAP HANAデータベース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]ペインでのSAP HANAデータベースに対するデータ保護処理の監視

[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。

SAP HANAのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * 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。 b. 処理を選択します。 c. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのSAP HANAデータベースのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、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とクローンの図を表示すると役に立ちます。

タスク概要

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。

[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とクローンをすべて表示できます。これらのバックアップと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。

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 ストレージで使用可能なバックアップとクローンの数の概要を確認します。

   概要カード セクションには、ファイルベースのバックアップ、スナップショット コピー ベースのバックアップ、およびクローンの合計数が表示されます。

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。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限は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。
8. クローンを分割する場合は、テーブルからクローンを選択し、 。

著作権に関する情報

商標に関する情報