SAP HANAリソースのバックアップ

SnapCenter software

NetApp
January 09, 2026

目次

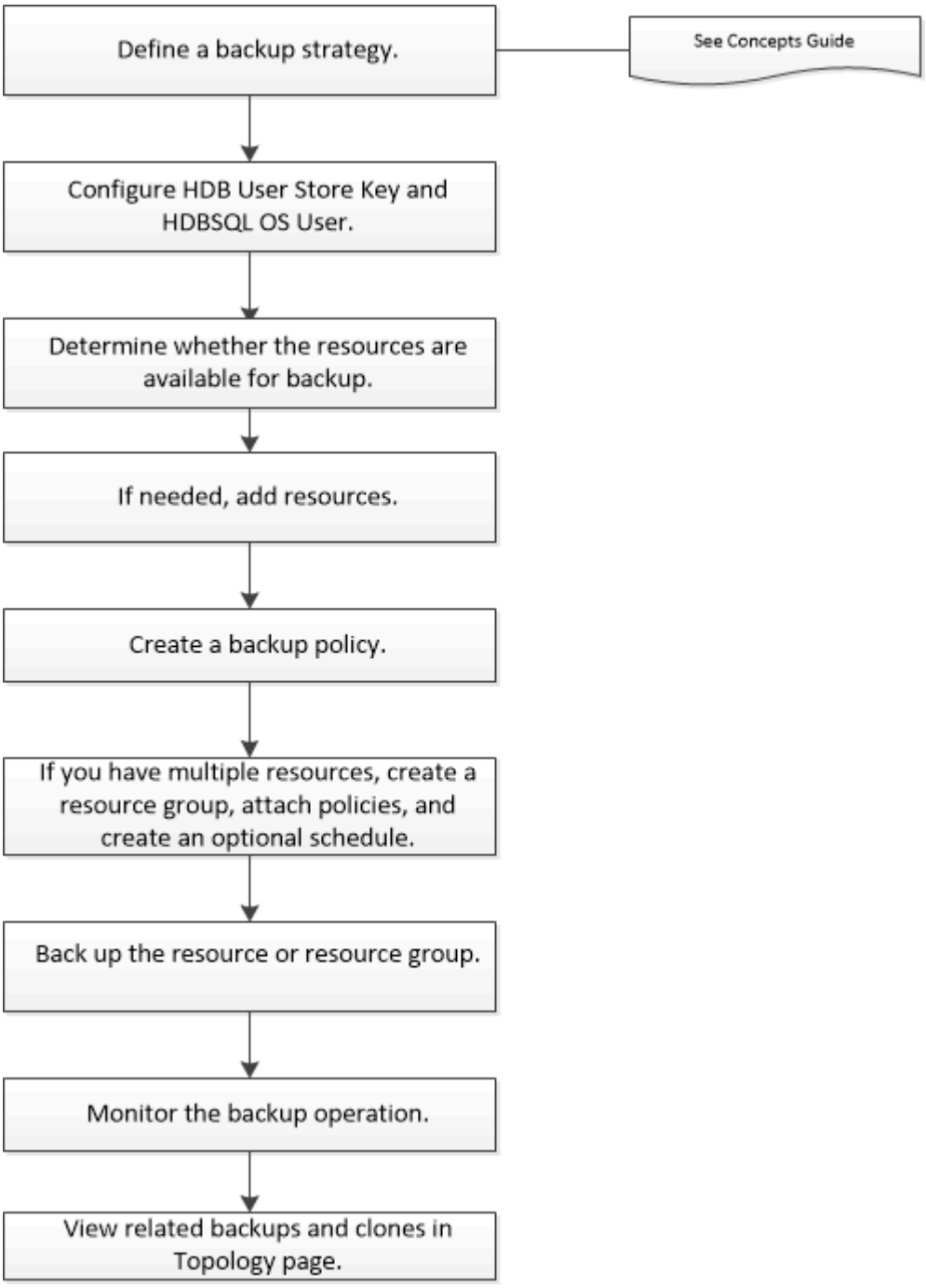
SAP HANAリソースのバックアップ . . . 1
SAP HANAリソースのバックアップ . . . 1
SAP HANAデータベースのHDBユーザストアキーとHDBSQL OSユーザを設定 . . . 2
リソースを検出し、データ保護のためのマルチテナントデータベースコンテナを準備する . . . 2
データベースの自動検出 . . . 3
データ保護のためのマルチテナントデータベースコンテナの準備 . . . 4
プラグインホストに手動でリソースを追加する . . . 5
SAP HANAデータベースのバックアップポリシーの作成 . . . 7
リソースグループを作成してポリシーを適用 . . . 11
リソースグループを作成し、ASA R2システムでSAP HANAリソースのセカンダリ保護を有効にする . . . 15
PowerShellコマンドレットを使用してSAP HANAデータベース用にストレージシステム接続とクレデンシャルを作成 . . . 18
SAP HANAデータベースのバックアップ . . . 19
リソースグループのバックアップ . . . 27
SAP HANAデータベースのバックアップ処理を監視する . . . 27
[Activity]ペインでSAP HANAデータベースのデータ保護処理を監視する . . . 28
SAP HANAのバックアップ処理をキャンセルする . . . 29
[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 . . . 29

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"^]です。

SAP HANAデータベースのHDBユーザストアキーとHDBSQL OSユーザを設定

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が設定されておらず、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。以降の検出処理で、設定されている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ことが判明した場合は、赤い南京錠のアイコンが再度表示されます。
- 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には、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）をクリックし、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、 * データベースの設定 * 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 ユーザーが <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。

リソースを検出し、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を準備する

データベースの自動検出

リソースとは、SnapCenterで管理されている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。使用可能な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サーバのインストール、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HDB SQL 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に設定する必要があります。
- 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は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。

タスクの内容

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的に検出されて[リソース]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、 * Resources * をクリックし、リストから Plug-in for SAP HANA Database 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）*をクリックし、ホスト名を選択します。

   次に、**をクリックしてフィルタペインを閉じることができます。
4. [* リソースの更新 *] をクリックして、ホストで使用可能なリソースを検出します。

   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ストレージにあり、保護されていない場合は、[全体のステータス]列に「保護されていません」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り保護されていて、実行されたバックアップ処理がない場合は、[全体のステータス]列に[バックアップが実行されていません]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、「 Backup failed 」または「 Backup succeeded 」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。以降の検出処理で、設定されている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ことが判明した場合は、赤い南京錠のアイコンが再度表示されます。

SnapCenter以外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

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、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ユーザを設定"

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。プラグインをインストールまたはアップグレードすると、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）リソースごとに別のMDCリソースが自動的に検出され、SnapCenterに登録されます。新しいリソースは「ロック」状態になります。

タスクの内容

たとえば、SnapCenter 4.2では、E90MDC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る場合、SnapCenter 4.3へのアップグレード後に、別のGUIDを持つ別のE90MDC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リソースを削除して、自動検出された新しいMDCリソースの管理を続行できます。

`Old MDC resource` は、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データ保護処理に使用するには、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ている古い MDC リソースを選択し ' トポロジーページからメンテナンス・モードにします

   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リソースを構成するには、[Resources]ページで新しいリソースを選択します。

   「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ときに検出された、新しく検出された MDC リソースです。新しいMDCリソースは、特定のホストについ

て、古いMDCリソースと同じSIDを持つリソースとして識別できます。[Resources]ページでは、その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Snapshotの保持期間が7日、セカンダリSnapshotの保持期間が45日の場合、45日が経過してすべてのバックアップが削除されたあとは、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ユーザを設定"

"[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"]

プラグインホストに手動でリソースを追加する

一部のHANAインスタンスでは自動検出がサポートされません。これらの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。

"リソースグループを作成してポリシーを適用"です。

タスクの内容

自動検出は、次の構成ではサポートされません。

- RDMとVMDKのレイアウト

  上記のリソースが検出された場合、そ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で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 SnapCenter Plug-in for SAP HANA Database を選択し、 * Resources * 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、[Single Container]、[Multitenant Database Container]（MDC）、および[Non-data Volume]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。インストールされている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ています。 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。テイクオーバー時に使用されます。
HDBSQL OS ユーザ	HDBのセキュアなユーザストアキーを設定するユーザ名を入力します。Windowsの場合、[HDBSQL OS User]にはシステムユーザを指定する必要があります。そのため、システムユーザのHDBのセキュアなユーザストアキーを設定する必要があります。

4. ストレージ容量の提供ページで、ストレージシステムを選択し、ボリューム、 LUN 、および qtree を 1 つ以上選択して、 * 保存 * をクリックします。

   オプション：*アイコンをクリックすると、他のストレージシステムからボリューム、LUN、およびqtree を追加できます  。

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、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

"ユーザまたはグループを追加してロールとアセットを割り当てる"

データベースを追加したら、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 Client （プラグイン）ホスト
- Single Container ： SID または HDBSQL Client （プラグイン）ホスト
- データボリューム以外：リソース名、関連付けられた 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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

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。

- データ保護の準備として、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セットアップ、リソースの追加などのタスクを実行しておく必要があります。
- 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の両方に対応するSVMをSnapCenter管理者がユーザに割り当てておく必要があります。

  また、レプリケーション、スクリプト、およびアプリケーションの設定をポリシーで指定することもできます。これらのオプションを使用することで、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。詳しくは、を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"。

タスクの内容

- SAP HANAシステムレプリケーション
  - プライマリSAP HANAシステムを保護し、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システムは保護できますが、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
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [Name]ページで、ポリシーの名前と詳細を入力します。
5. [Policy type]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：

状況	操作
Snapshotテクノロジを使用したバックアップの作成	「 * Snapshot Based * 」を選択します。
データベースの整合性チェックの実行	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. [Snapshot and Replication]ページで、次の手順を実行します。
   - スケジュールタイプを指定するには、「 * on demand * 」、「 * Hourly * 」、「 * Daily * 」、「 * Weekly * 」、または「 * Monthly * 」を選択します。

> 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）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ている場合、夏時間（DST）中はスケジュールはトリガーされません。

7. [Snapshot and Replication]ページで、[Backup Type]ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。

状況	作業
一定数のSnapshotを保持	[保持するコピー数]*を選択し、保持するSnapshotの数を指定します。 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可能性があります。 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、作成されたSnapshotの合計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の削除は、最も古いSnapshotが配置されているノードに基づいて行われます。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を含むリソースグループの保持期間は7に設定されます。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含め、最大7つです。

状況	作業
Snapshotを特定の日数だけ保持	[コピーを保持する期間]*を選択し、Snapshotを削除するまでの日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、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. Snapshotコピーベースのバックアップの場合は、[Select secondary replication options]セクションで、次のセカンダリレプリケーションオプションの一方または両方を選択します。

フィールド	操作
• ローカル Snapshot コピー作成後に SnapMirror を更新 *	別のボリュームにバックアップセットのミラーコピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。 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はデスティネーションに転送されず、デスティネーションのリストに表示されます。このSnapshotをリストア処理の対象としてデスティネーションで選択すると、「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では、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。 [Topology]ページの[Refresh]*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のSnapLock有効期限が更新されます。 を参照して "[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 Snapshot コピー作成後に SnapVault を更新 *	ディスクツーディスクのバックアップレプリケーション（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*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のSnapLock有効期限が更新されます。 SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得し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、を参照してください。 "SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする" を参照して "[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。

10. 概要を確認し、 [完了] をクリックします。

リソースグループを作成してポリシーを適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを追加する必要があります。リソースグループを使用すると、特定のアプリケーションに関連付けられてい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すべてのデータ保護ジョブに必要です。また、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必要があります。

タスクの内容

- 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ヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定された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データベース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. [名前] ページで、次の操作を実行します。

フィールド	操作
名前	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。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。 たとえば、customText_resource group_policy_hostnameやresource group_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

4. Resources ページで、 * Host * ドロップダウン・リストからホスト名を選択し、 * Resource Type * 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。

   これは、画面上の情報をフィルタリングするのに役立ちます。

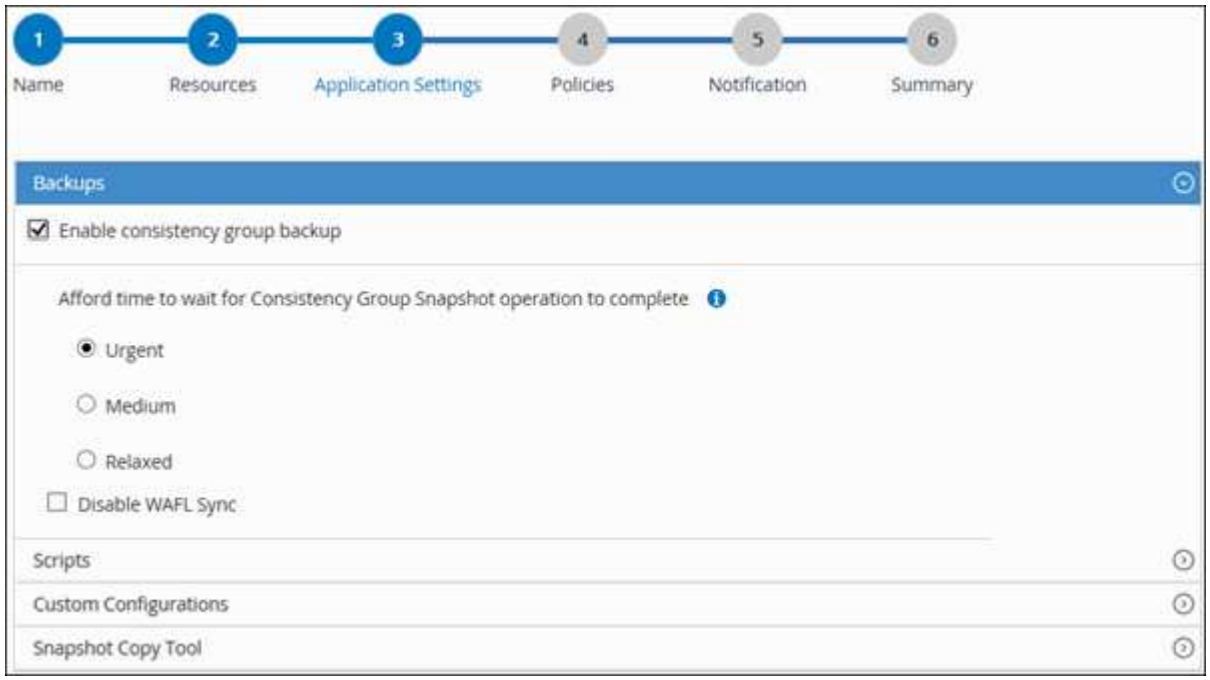
5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。
6. [アプリケーションの設定] ページで、次の操作を行います。

   a. [*Backups] の矢印をクリックして、追加のバックアップ・オプションを設定します。

      整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
整合グループSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+



a. [Scripts]*の矢印をクリックし、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。

b. [カスタム構成 *] の矢印をクリックし、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でアーカイブログを削除できます。
アーカイブログの保持	日数	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	アーカイブログが格納されているディレクトリのパスを指定します。
ARCHIVE_LOG_EXT	ファイル拡張子	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_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

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サポートされ、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. Snapshotコピーツール*の矢印をクリックして、Snapshotを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、ファイルシステムを整合性のある状態にしてからSnapshotを作成します。Linuxリソースの場合、このオプションは適用されません。	ファイルシステムの整合性を維持した状態で 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：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで 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します。	[その他]*を選択し、ホストで実行するSnapshotを作成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]セクションに表示されます。

b. [スケジュールの設定]列で、設定するポリシーの**をクリックします + 。

c. [Add schedules for policy_name_] ダイアログボックスで、スケジュールを設定し、 [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。

設定されたスケジュールは、 [* Applied Schedules] 列に表示されます。

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

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

また、送信者と受信者のEメールアドレス、およびEメールの件名を指定する必要があります。SMTP サーバーは、 * Settings * > * Global Settings * 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**システムで**SAP HANA**リソースのセカンダリ保護を有効にする

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

開始する前に

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

タスクの内容

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

手順

1. 左側のナビゲーションペインで、*[リソース]*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 新しいリソースグループ *] をクリックします。
3. [名前] ページで、次の操作を実行します。

a. [Name]フィールドにリソースグループの名前を入力します。

リソースグループ名は250文字以内にする必要があります。

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

たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。

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

たとえば、customText_resource group_policy_hostnameやresource group_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

d. バックアップしないアーカイブログファイルのデスティネーションを指定します。

必要に応じて、プレフィックスを含め、アプリケーションで設定されたものとまったく同じ宛先を使用する必要があります。

4. [リソース]ページで、*[ホスト]*ドロップダウンリストからデータベースホスト名を選択します。

リソースが Available Resources セクションに表示されるのは、リソースが正常に検出された場合のみです。最近追加したリソースは、リソースリストを更新するまで使用可能なリソースのリストに表示されません。

5. [Available Resources]セクションからASA R2リソースを選択し、[Selected Resources]セクションに移動します。
6. [Application Settings]ページで、バックアップオプションを選択します。
7. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから1つ以上のポリシーを選択します。

をクリックしてポリシーを作成することもできます。

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。

c. [Add schedules for policy_name] ウィンドウで、スケジュールを設定し、 [**OK**] をクリックします。

ここで、 _policy_name_は 選択したポリシーの名前です。

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

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

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

a. レプリケーションポリシーのタイプを選択します。

同期レプリケーションポリシーはサポートされていません。

b. 使用する整合グループサフィックスを指定します。

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

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

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

1. [Verification]ページで、次の手順を実行します。

a. Load locators * （ロケータのロード）をクリックして、 SnapMirror または SnapVault ボリュームをロードし、セカンダリ・ストレージ上で検証を実行します。

b. [Configure Schedules]列内をクリックし て、ポリシーのすべてのスケジュールタイプに対して検証スケジュールを設定します。

c. [Add Verification Schedules policy_name]ダイアログボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	[Run verification after backup] を選択します。
検証のスケジュールを設定	[Run scheduled verification] を選択し、ドロップダウン・リストからスケジュール・タイプを選択します。

d. セカンダリ・ストレージ・システムのバックアップを検証するには、セカンダリ・サイトで * Verify on secondary location * を選択します。

e. [OK]*をクリックします。

設定した検証スケジュールは、 Applied Schedules 列にリスト表示されます。

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

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

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

3. 概要を確認し、 [完了] をクリックします。

PowerShellコマンドレットを使用してSAP HANAデータベース用にストレージシステム接続とクレデンシャルを作成

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ロールに必要な権限が必要です。
- 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。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

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。

   次に、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例を示します。

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

4. SnapCenterサーバに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の場合：

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

   Windowsの場合：

   ```
   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の場合：

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

   Linuxの場合：

   ```
   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"。

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含まれていないリソースは、の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 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro 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。

  "リソースグループを作成してポリシーを適用"です。

  "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停止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、コマンドレットを使用して、HANAの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 `Set-SmConfigSettings` ます。

  コマンドレットで使用できるパラメータとその説明については、 Get-Help_command_name _ を実行して取得できます。または、 "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、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用できるかどうかを確認する必要があります。
  - Windowsホストのデフォルトの場所：*C：\Program NetApp SnapCenter SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Linuxホストのデフォルトの場所：*/opt/linux/scc/etc/allowed_commands.config* NetApp SnapCenter

  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 **View**] ドロップダウンリストからリソースをフィルタリングします。

   *を選択し、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リングします。その後、を選択してフィルタペインを閉じることができます 。
3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 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。
5. [アプリケーションの設定] ページで、次の操作を行います。

   ◦ [Backups]*矢印を選択して、追加のバックアップオプションを設定します。

   必要に応じて整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

   ◦ [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

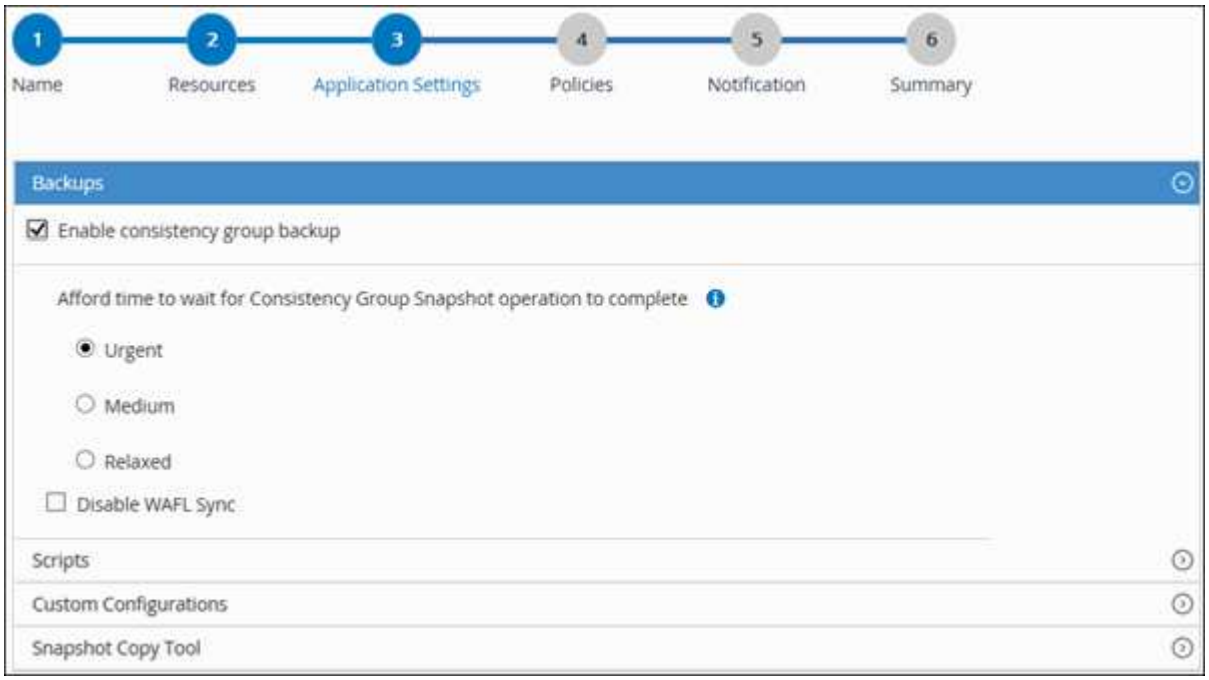
   バックアップ処理を終了する前にPREコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

   ◦ [**Custom Configurations**]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。

   ◦ Snapshotコピーツール*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * を選択します。

状況	作業
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整合性を維持した状態でSnapCenter を選択します。
Snapshotを作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshotを作成します。



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 + 。

      [選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

   b. スケジュールを設定するポリシーの[スケジュールの設定]列で**を選択します + 。

   c. [Add schedules for policy_policy_name_]ダイアログボックスで、スケジュールを設定し、*[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。

7. [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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。

   リソース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 （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た場合は、 [* Policy] ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

       オンデマンドバックアップ用に選択したポリシーにバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

    b. 「 * Backup * 」を選択します。
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。

    ◦ 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、次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ヒープサイズが十分でないと、バックアップが失敗することがあります。

      Java の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_. を探します。このスクリプトでは、 *DO_START METHOD_Command* 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、指定したユーザのSnapCenterサーバ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）を監視します。

```
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、バックアップ名などの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"。

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に対して実行されます。

開始する前に

- ポリシーを適用して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 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all 」権限は必要ありません。

タスクの内容

リソースグループは、[Resources]ページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、スケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

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。

   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、を選択し、タグを選択します。その後、を選択してフィルタペインを閉じることができます 。
3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
4. Backup （バックアップ）ページで、次の手順を実行します。
   a. 複数のポリシーをリソースグループに関連付けている場合は、「 * Policy * 」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

      オンデマンドバックアップ用に選択したポリシーにバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

SAP HANAデータベースのバックアップ処理を監視する

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

-

実行中

- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

手順

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

   バックアップジョブのステータスは表示されますが 、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部が進行中であるか、警告サインが表示されていることがあります。

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

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

[Activity]ペインでSAP HANAデータベースのデータ保護処理を監視する

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

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

手順

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [Activity]ペインでをクリックすると、 ペインアイコン"] 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

SAP HANAのバックアップ処理をキャンセルする

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの *
- 操作をキャンセルするには、SnapCenter管理者または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、 **Monitor** ページまたは **Activity** 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。
- SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用して、バックアップ処理をキャンセルできます。
- キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に ' このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は ' そのロールを使用している間に ' 他のメンバーのキューに入っている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。

アクセス元	アクション
監視ページ	a. 左側のナビゲーションペインで、 * Monitor * > * Jobs * 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. バックアップ処理を開始したら、[Activity]ペインの**をクリックしペインアイコン"]て、最新の5つの処理を表示します。 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、リソースが以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とクローンの図を表示すると役立つことがあります。

タスクの内容

プライマリストレージとセカンダリストレージ（ミラーコピーまたはバックアップコピー）にバックアップと

クローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

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

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

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

[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とクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

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

手順

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示 *] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

   リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。
4. サマリー・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を確認します。

   [サマリカード]セクションには、ファイルベースのバックアップ、Snapshotコピーベースのバックアッ

プ、およびクローンの総数が表示されます。

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

SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

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有効期限がONTAPから取得されます。

SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

5. [コピーの管理] ビューで、プライマリストレージまたはセカンダリストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

   バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。

   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。

7. クローンを削除する場合は、表でクローンを選択し、をクリックします。
8. クローンをスプリットする場合は、テーブルでクローンを選択し、をクリックします 。

著作権に関する情報

商標に関する情報