



# **SAP HANA**リソースのバックアップ SnapCenter Software 5.0

NetApp  
October 15, 2025

# 目次

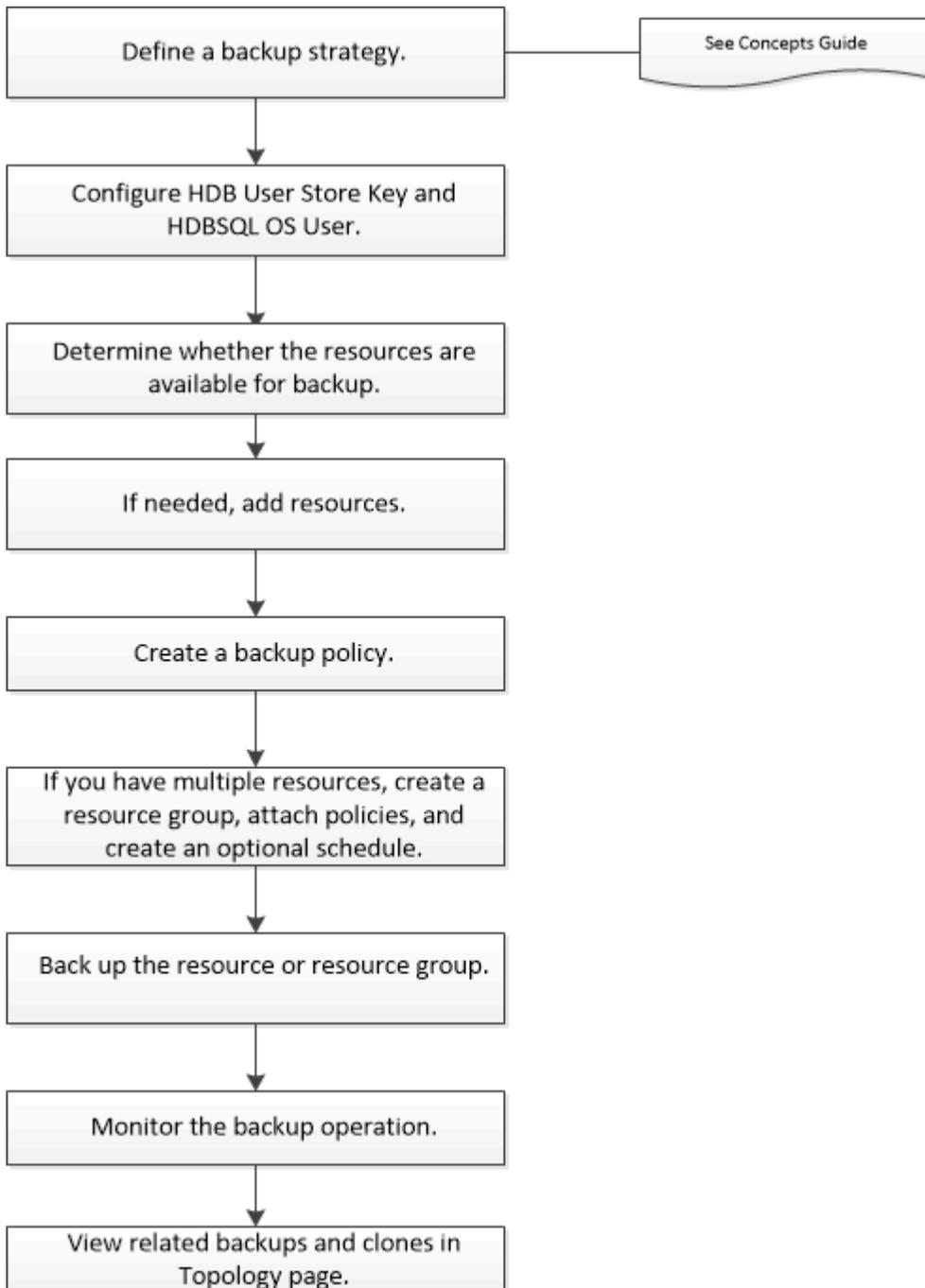
SAP HANAリソースのバックアップ	1
SAP HANAリソースのバックアップ	1
SAP HANAデータベースのHDBユーザストアキーとHDBSQL OSユーザを設定	2
リソースを検出し、データ保護のためのマルチテナントデータベースコンテナを準備する	2
データベースの自動検出	3
データ保護のためのマルチテナントデータベースコンテナの準備	4
プラグインホストに手動でリソースを追加する	5
SAP HANAデータベースのバックアップポリシーの作成	7
リソースグループを作成してポリシーを適用	13
SAP HANAデータベースのバックアップ	16
リソースグループのバックアップ	20
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	21
PowerShellコマンドレットを使用したデータベースのバックアップ	23
バックアップ処理の監視	26
SAP HANAデータベースのバックアップ処理を監視する	26
[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	27
SAP HANAのバックアップ処理をキャンセルする	27
[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	28

# 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-50/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 データベースと非データボリュームです。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・システム接続の設定などの作業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。

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. [\* 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。

- 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 。

- 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。

- 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、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。

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。



プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

## 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. [ 名前 ] ページで、ポリシー名と概要を入力します。
5. 設定ページで、次の手順を実行します。

- バックアップタイプを選択：

状況	操作
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。
Snapshotテクノロジーを使用したバックアップの作成	「* Snapshot Based *」を選択します。

- 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。

**Schedule frequency**

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

Daily

Weekly

Monthly



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。

- [\* カスタム・バックアップ設定 \*] セクションで、キー値形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキー値は複数指定できます。

6. [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 data-bbox="842 159 1463 226">[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 data-bbox="842 264 1463 331">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 data-bbox="873 369 1463 617"> <p data-bbox="873 470 927 527">i</p> <p data-bbox="989 380 1455 611">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。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。</p> </div> <div data-bbox="873 667 1463 978"> <p data-bbox="873 789 927 846">i</p> <p data-bbox="989 674 1455 974">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。</p> </div> <div data-bbox="873 1029 1463 1239"> <p data-bbox="873 1108 927 1165">i</p> <p data-bbox="989 1035 1455 1234">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。</p> </div> <div data-bbox="873 1289 1463 1877"> <p data-bbox="873 1558 927 1614">i</p> <p data-bbox="989 1295 1455 1871">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。</p> </div>

状況	作業
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。
Snapshotコピーのロック期間	Snapshotコピーのロック期間を選択し、日、月、または年を選択します。  SnapLock保持期間は100年未満にする必要があります。

7. Snapshot コピーベースのバックアップの場合は、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	操作
<ul style="list-style-type: none"> <li>ローカル Snapshot コピー作成後に SnapMirror を更新 *</li> </ul>	<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>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。</p> <p>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。</p> <p>[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。</p> <p>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"</p>

フィールド	操作
<ul style="list-style-type: none"> <li>ローカル Snapshot コピー作成後に SnapVault を更新 *</li> </ul>	<p>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。</p> <p>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。</p> <p>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。</p> <p>SnapLock Vaultの詳細については、を参照してください。 "<a href="#">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</a>"</p> <p>を参照して "<a href="#">[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</a>"</p>
<ul style="list-style-type: none"> <li>二次ポリシーラベル *</li> </ul>	<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 style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <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>
<ul style="list-style-type: none"> <li>エラー再試行回数 *</li> </ul>	<p>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。</p>



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。

8. 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。

## 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。

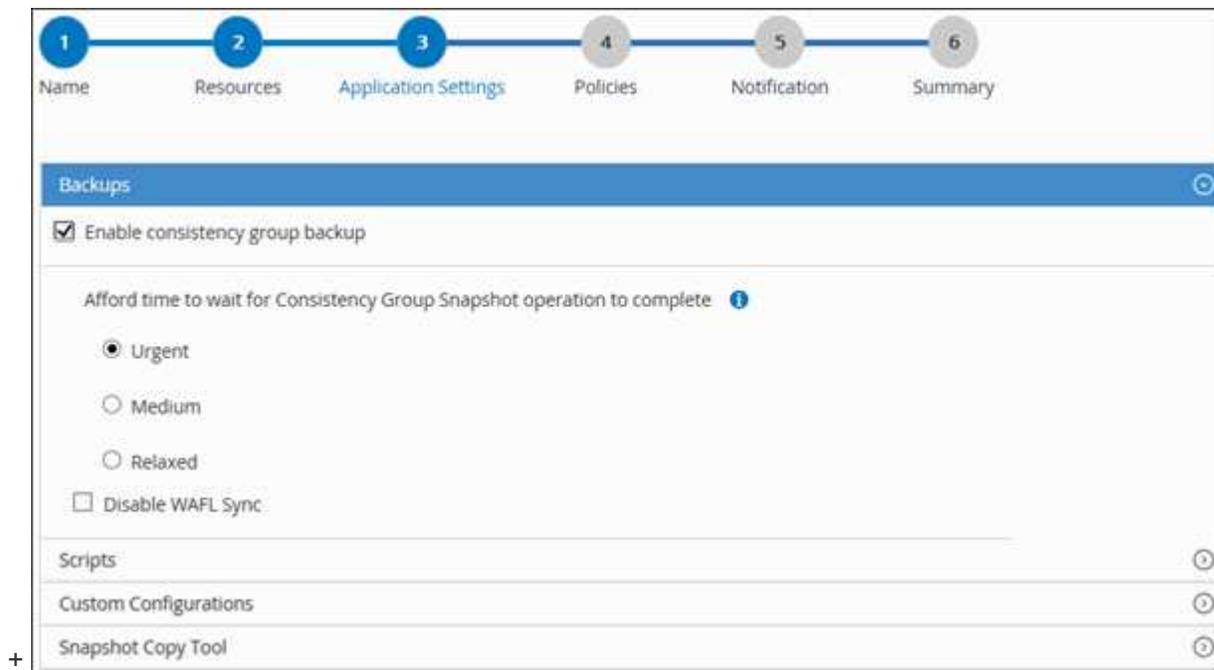
4. Resources ページで、\* Host \* ドロップダウン・リストからホスト名を選択し、\* Resource Type \* ドロップダウン・リストからリソース・タイプを選択します。

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。
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。

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。
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 。

ポリシーは、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。

## 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、こ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。

#### 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。

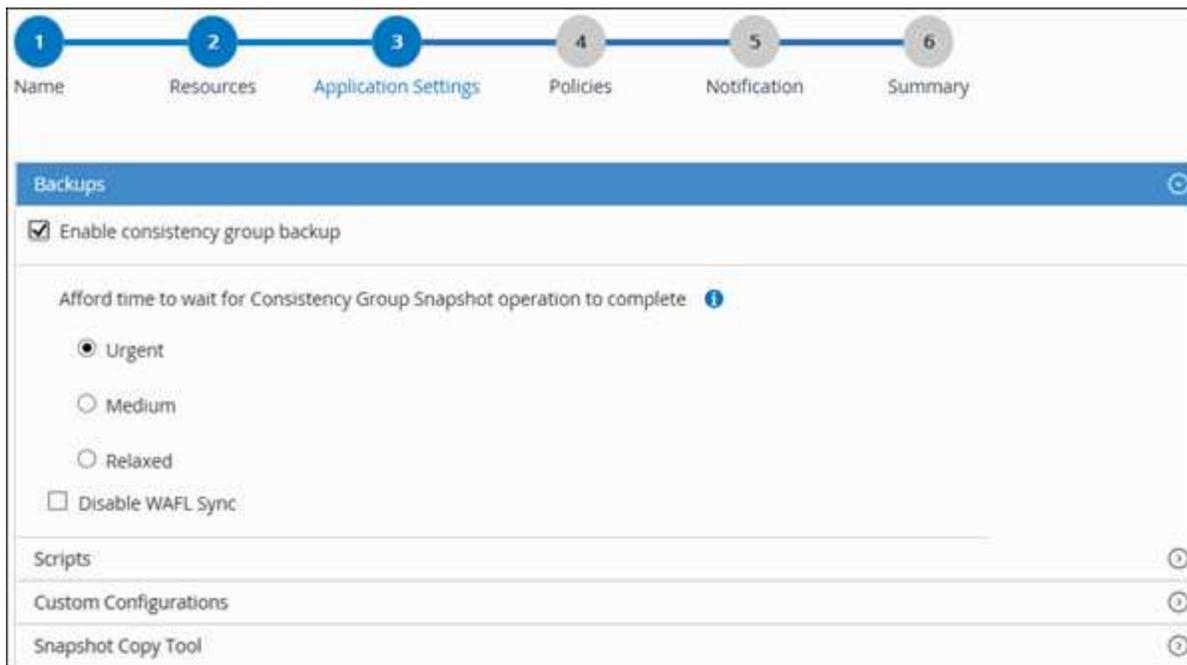
フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent、Medium、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

- [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。
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せん。

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`

## 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せん。
  - 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。

## 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 -Storage test_vs1 -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"。

## PowerShellコマンドレットを使用したデータベースのバックアップ

データベースをバックアップするときは、SnapCenter サーバとの接続を確立してから、リソースの追加、ポリシーの追加、バックアップリソースグループの作成を行って、バックアップを実行します。

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。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。

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.netapp.  
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.sscore.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.sscore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sscore.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.sscore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="NonDataVolume\
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](#)"。

## バックアップ処理の監視

### 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
-  完了済み

-  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、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]ペインでをクリックして、  ペインアイコン" 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。
-  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、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。



SAP HANAシステムレプリケーションのプライマリリソースの場合はリストア処理と削除処理がサポートされ、セカンダリリソースの場合はクローニング処理がサポートされます。

[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。

#### 手順

- 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。
- [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。
- 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。

- 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。

オンデマンドバックアップのあと、\*[リフレッシュ]\*ボタンをクリックすると、バックアップまたはクロー

ンの詳細がリフレッシュされます。

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

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

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

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

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

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

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

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、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。