SAP HANA データベースを保護します

SnapCenter Software 4.5

NetApp
September 29, 2025

目次

SAP HANA データベースを保護します

SnapCenter Plug-in for SAP HANA Databases の略

SnapCenter Plug-in for SAP HANA Database の概要

SnapCenter Plug-in for SAP HANA Database は、 SAP HANA データベースに対応したデータ保護管理を提供する、 NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。Plug-in for SAP HANA Database は、 SnapCenter 環境での SAP HANA データベースのバックアップ、リストア、およびクローニングを自動化します。

SnapCenter は、単一コンテナおよびマルチテナントデータベースコンテナ（ MDC ）をサポートしています。Plug-in for SAP HANA Database は、 Windows と Linux のどちらの環境でも使用できます。HANA データベースホストにインストールされていないプラグインは、一元化されたホストプラグインと呼ばれます。一元化されたホストプラグインで、複数のホストにまたがる複数の HANA データベースを管理できます。

Plug-in for SAP HANA Database がインストールされている場合は、 SnapCenter で NetApp SnapMirror テクノロジを使用して、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できます。また、このプラグインと NetApp SnapVault テクノロジを併用して、標準への準拠を目的とした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を実行することもできます。

SnapCenter Plug-in for SAP HANA Database の機能

Plug-in for SAP HANA Database をインストールした環境では、 SnapCenter を使用して SAP HANA データベースとそのリソースをバックアップ、リストア、クローニングできます。これらの処理をサポートするタスクを実行することもできます。

- データベースを追加します。
- バックアップを作成します。
- バックアップからリストアします
- バックアップをクローニングする。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視する。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

SnapCenter Plug-in for SAP HANA Database の特長

SnapCenter は、プラグインアプリケーションと統合されるほか、ストレージシステム上でネットアップのテクノロジと統合されます。Plug-in for SAP HANA Database の操作には、 SnapCenter のグラフィカルユーザインターフェイスを使用します。

- * 統一されたグラフィカル・ユーザー・インターフェイス *

  SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter インターフェイスを使用すると、すべてのプラグインでバックアップ、リストア、クロ

ーニングの各処理を一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（ RBAC ）を設定したり、ジョブを監視したりすることができます。

- * 中央管理の自動化 *

  バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenter から E メールアラートを送信するように設定して、環境をプロアクティブに監視することもできます。

- * 無停止の NetApp Snapshot コピー・テクノロジー *

  SnapCenter では、 Plug-in for SAP HANA Database でネットアップの Snapshot コピーテクノロジを使用してリソースがバックアップされます。

Plug-in for SAP HANA Database を使用すると、次のメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます

  また、許可された SnapCenter ユーザにアプリケーションレベルの権限を付与するようにクレデンシャルを設定することもできます。

- NetApp FlexClone テクノロジを使用して、スペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

  クローンを作成するストレージシステムに FlexClone ライセンスが必要です。

- バックアップの作成で ONTAP の整合グループ（ CG ）の Snapshot コピー機能がサポートされます。
- 複数のリソースホストで同時に複数のバックアップを実行できます

  1 回の処理で、 1 つのホストの複数のリソースが同じボリュームを共有する場合に複数の Snapshot コピーが統合されます。

- 外部コマンドを使用して Snapshot コピーを作成できます。
- ファイルベースのバックアップがサポートされます。
- XFS ファイルシステムで Linux LVM がサポートされています。

SnapCenter Plug-in for SAP HANA Database でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシン（ VM ）の両方でさまざまなストレージタイプをサポートしています。SnapCenter Plug-in for SAP HANA Database をインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージタイプ
物理サーバと仮想サーバ	FC 接続 LUN

マシン	ストレージタイプ
物理サーバ	iSCSI で接続された LUN
物理サーバと仮想サーバ	NFS-connected ボリューム

必要な最小 **ONTAP** 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： **ONTAP 8.2_x_and later** に必要な最小権限
event generate-autosupport-log を指定します
ジョブ履歴の表示 ジョブが停止しました

フルアクセスコマンド： **ONTAP 8.2_x_and later** に必要な最小権限
LUN lun create をクリックします lun delete LUN igroup add lun igroup create を追加します lun igroup delete LUN igroup の名前を変更します lun igroup show を参照してください LUN マッピングの追加 - レポートノード LUN マッピングが作成されます LUN マッピングが削除されます LUN マッピングの削除 - レポートノード lun mapping show lun modify を追加します LUN のボリューム内移動 LUN はオフラインです LUN はオンラインです LUN の永続的予約はクリアします LUN のサイズ変更 LUN シリアル lun show をクリックします

フルアクセスコマンド： **ONTAP 8.2_x_and later** に必要な最小権限
SnapMirror ポリシー追加ルール snapmirror policy modify-rule snapmirror policy remove-rule 」を実行します snapmirror policy show の略 SnapMirror リストア snapmirror show の略 snapmirror show -history の略 SnapMirror の更新 SnapMirror の update-ls-set snapmirror list-destinations
バージョン

フルアクセスコマンド： **ONTAP 8.2_x_and later** に必要な最小権限
volume clone create を実行します
volume clone show を実行します
ボリュームクローンスプリット開始
ボリュームクローンスプリットは停止します
volume create を実行します
ボリュームを削除します
volume file clone create を実行します
volume file show-disk-usage
ボリュームはオフラインです
ボリュームはオンラインです
volume modify を使用します
volume qtree create を実行します
volume qtree delete
volume qtree modify の略
volume qtree show の略
ボリュームの制限
volume show のコマンドです
volume snapshot create を実行します
ボリューム Snapshot の削除
volume snapshot modify の実行
ボリューム Snapshot の名前が変更されます
ボリューム Snapshot リストア
ボリューム Snapshot の restore-file
volume snapshot show の実行
ボリュームのアンマウント

フルアクセスコマンド： **ONTAP 8.2_x_and later** に必要な最小権限
SVM CIFS です
vserver cifs share create の場合
SVM CIFS 共有が削除されます
vserver cifs shadowcopy show
vserver cifs share show のコマンドです
vserver cifs show のコマンドです
SVM エクスポートポリシー
vserver export-policy create を参照してください
vserver export-policy delete
vserver export-policy rule create
vserver export-policy rule show
vserver export-policy show のコマンドを入力します
Vserver iSCSI
vserver iscsi connection show
vserver show のコマンドです

読み取り専用コマンド： **ONTAP 8.2_x_and later** に必要な最小権限
Network Interface の略
network interface show の略
Vserver

SAP HANA データベースの SnapMirror および SnapVault レプリケーション用のストレージシステムを準備する

SnapCenter プラグインと ONTAP の SnapMirror テクノロジを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、 ONTAP SnapVault テクノロジを使用すると、標準への準拠やその他のガバナンス関連の目的で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を実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、 ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。

SnapCenter は、 SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（ * プライマリ * > * ミラー * > * バックアップ * ）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください "ONTAP のドキュメント"。

SAP HANA データベースのバックアップ戦略

SAP HANA データベースのバックアップ戦略を定義する

バックアップジョブを作成する前にバックアップ戦略を定義しておくと、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービスレベルアグリーメント（ SLA ）、目標復旧時間（ RTO ）、および目標復旧時点（ RPO ）によって決まります。

- このタスクについて *

SLA では、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処するために必要なサービスレベルを定義します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA 、 RTO 、および RPO は、データ保護戦略に関与します。

- 手順 *

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. Snapshot コピーベースのポリシーを作成してアプリケーションと整合性のあるデータベースの Snapshot コピーをバックアップするかどうかを決定します。
5. データベースの整合性を検証するかどうかを決定します。
6. レプリケーションのために NetApp SnapMirror テクノロジを使用するか、または長期保持のために NetApp SnapVault テクノロジを使用するかを決定します。
7. ソースストレージシステムおよび SnapMirror デスティネーションでの Snapshot コピーの保持期間を確認します。
8. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

Linux ホスト上のリソースの自動検出

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。SnapCenter Plug-in for SAP HANA Database プラグインをインストールすると、その Linux ホスト上の SAP HANA データベ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。

自動検出は、次の SAP HANA リソースでサポートされています。

- 単一のコンテナ

  プラグインをインストールまたはアップグレードしたあと、中央ホストプラグインにある単一コンテナリソースは、手動で追加したリソースとして引き続き使用されます。

  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、 SnapCenter に直接登録されている SAP HANA Linux ホストでのみ、 SAP HANA データベースが自動的に検出されます。

- マルチテナントデータベースコンテナ（ MDC ）

  プラグインをインストールまたはアップグレードした後、中央ホストプラグインにある MDC リソースは、手動で追加したリソースとして続行されます。

  SnapCenter 4.3 へのアップグレード後も、中央ホストプラグインに MDC リソースを手動で追加する必要があります。

  SnapCenter に直接登録された SAP HANA Linux ホストの場合、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、ホスト上のリソースが自動で検出されます。プラグインをアップグレードした後、プラグインホスト上にあるすべての MDC リソースに対して、別の MDC リソースが自動的に別の GUID 形式で検出され、 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。

  たとえば、 SnapCenter 4.2 では、 E90 MDC リソースがプラグインホスト上にあり、手動で登録されている場合、 SnapCenter 4.3 にアップグレードした後に、別の 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。

データ保護処理用の SnapCenter プラグインホスト上の新しい MDC リソースを使用する方法の詳細については、『 SAP HANA データベースデータ保護ガイド』を参照してください

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、これらのリソースではデータ保護処理はサポートされていません。

- HANA マルチホスト構成
- HANA システムレプリケーション
- 同じホスト上の複数のインスタンス

サポートされるバックアップのタイプ

バックアップタイプでは、作成するバックアップのタイプを指定します。SnapCenter では、 SAP HANA データベースについて、ファイルベースのバックアップと Snapshot コピーベースのバックアップをサポートしています。

File-Based バックアップ

ファイルベースのバックアップでは、データベースの整合性が検証されます。ファイルベースのバックアップの処理は一定の間隔で実行するようにスケジュールを設定できます。アクティブなテナントのみがバックアップされます。ファイルベースのバックアップは SnapCenter からリストアおよびクローニングできません。

Snapshot コピーベースのバックアップ

Snapshot コピーベースのバックアップでは、 NetApp Snapshot コピーテクノロジを利用して、 SAP HANA データベースが格納されたボリュームのオンラインの読み取り専用コピーが作成されます。

SnapCenter Plug-in for SAP HANA Database での整合グループ Snapshot コピーの使用方法

プラグインを使用して、リソースグループの整合グループ Snapshot コピーを作成することができます。整合グループとはボリュームのコンテナであり、複数のボリュームを格納して 1 つのエンティティとして管理できます。整合グループには複数のボリュームの Snapshot コピーが同時に格納されるため、一連のボリュームのコピーの整合性が確保されます。

ストレージコントローラが整合性を確保しながら Snapshot コピーをグループ化するのを待機する時間も指定できます。使用可能な待機時間のオプションは、 * Urgent * 、 * Medium * 、 * Relaxed * です。また、整合グループ Snapshot コピーの処理で Write Anywhere File Layout （ WAFL ）の同期を有効または無効にすることもできます。WAFL 同期を使用すると、整合グループの Snapshot コピーのパフォーマンスが向上します。

SnapCenter による不要なログおよびデータバックアップの削除の管理

SnapCenter は、ストレージシステムレベルおよびファイルシステムレベルでの不要なログおよびデータバックアップの削除を、 SAP HANA のバックアップカタログ内で管理します。

保持設定に基づいて、プライマリストレージまたはセカンダリストレージの Snapshot コピーと SAP HANA のカタログ内の対応するエントリが削除されます。SAP HANA のカタログのエントリは、バックアップやリソースグループを削除したときにも削除されます。

SAP HANA データベースのバックアップスケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）などがあります。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度（バックアップを実行する間隔）

  バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュールタイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップスケジュール（バックアップが実行される日時

バックアップスケジュールは、リソースまたはリソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます

SAP HANA データベースに必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービスレベルアグリーメント（ SLA ）などがあります。

Plug-in for SAP HANA Database のバックアップ命名規則

Snapshot コピーのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。

「 resourcegroupname_hostname_timestamp 」

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- _dts1_は リソースグループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、「 * Snapshot コピーにカスタム名形式を使用」を選択して、リソースまたはリソースグループを保護しながら Snapshot コピー名の形式を指定することもできます。たとえば、customtext_resourcegroup_policy_hostname や resourcegroup_hostname などの形式です。デフォルトでは、 Snapshot コピー名にタイムスタンプのサフィックスが追加されます。

SAP HANA データベースのリストアとリカバリの戦略

SAP HANA リソースのリストアとリカバリの戦略を定義する

データベースのリストアとリカバリを行う前に戦略を定義しておくと、リストア処理とリカバリ処理を正常に実行できるようになります。

- 手順 *
  1. 手動で追加した SAP HANA リソースでサポートされるリストア戦略を決定します
  2. 自動検出された SAP HANA データベースに対するリストア戦略を決定します
  3. 実行するリカバリ処理のタイプを決定します。

手動で追加した **SAP HANA** リソースでサポートされるリストア戦略のタイプ

SnapCenter を使用してリストア処理を正常に実行するには、事前に戦略を定義しておく必要があります。SAP HANA リソースを手動で追加する場合のリストア戦略には、 2 つのタイプがあります。手動で追加した SAP HANA リソースはリカバリできません。

手動で追加した SAP HANA リソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、 qtree 、および LUN をリストアします

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

ファイルレベルのリストア

- ボリューム、 qtree 、またはディレクトリからファイルをリストアします
- 選択した LUN のみをリストアします

自動検出された **SAP HANA** データベースでサポートされるリストア戦略のタイプ

SnapCenter を使用してリストア処理を正常に実行するには、事前に戦略を定義しておく必要があります。自動検出された SAP HANA データベースには、 2 種類のリストア戦略があります。

リソース全体のリストア

- リソースのすべてのボリューム、 qtree 、および LUN をリストアします
  - ボリューム全体をリストアするには、 * Volume Revert * オプションを選択する必要があります。

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

テナントデータベース

- テナントデータベースをリストアします

「 * テナントデータベース * 」オプションが選択されている場合は、 SnapCenter 外部の HANA Studio または HANA リカバリスクリプトを使用してリカバリ処理を実行する必要があります。

自動検出された **SAP HANA** データベースのリストア処理のタイプ

SnapCenter では、自動検出された SAP HANA データベースについて、 Volume-Based

SnapRestore （ VBSR ）、 Single File SnapRestore 、 Connect and Copy のリストアタイプがサポートされています。

NFS 環境で **Volume-Based SnapRestore** （ **VBSR** ）を使用すると、次のようなシナリオが発生します。

- リストア用に選択されたバックアップが SnapCenter 4.3 より前のリリースで実行され ' **Complete Resource** オプションが選択されている場合のみ
- リストア用に選択されたバックアップが SnapCenter 4.3 で選択されていて、 * Volume Revert * オプションが選択されている場合

NFS 環境で単一ファイル **SnapRestore** を実行するシナリオを次に示します。

- リストア用に選択したバックアップが SnapCenter 4.3 で実行されていて、 [リソースを完全にバックアップ] オプションのみが選択されている場合
- マルチテナントデータベースコンテナ（ MDC ）の場合は、リストア対象に選択されたバックアップが SnapCenter 4.3 で作成され、「 * テナントデータベース * 」オプションが選択されているとみなされます
- バックアップを SnapMirror または SnapVault セカンダリの場所から選択し、 * Complete Resource * オプションが選択されている場合

単一ファイル **SnapRestore** は、次のような状況で **SAN** 環境で実行されます。

- SnapCenter 4.3 より前のリリースでバックアップを作成する場合、 [リソースの完了] オプションが選択されている場合のみ
- SnapCenter 4.3 でバックアップを実行する場合、 * Complete Resource * オプションが選択されている場合のみ
- SnapMirror または SnapVault セカンダリストレージからバックアップを選択し、 * Complete Resource * オプションを選択した場合

Connect and Copy ベースのリストアは、 **SAN** 環境で次のシナリオに基づいて実行されます。

- MDC の場合は、リストア用に選択されたバックアップが SnapCenter 4.3 で作成され、 * テナントデータベース * オプションが選択されている場合

* リソース全体 * 、 * ボリューム復帰 * 、 * テナントデータベース * の各オプションは、 [リストア範囲] ページから選択できます。

SAP HANA データベースでサポートされるリカバリ処理のタイプ

SnapCenter を使用すると、 SAP HANA データベースに対してさまざまなタイプのリカバリ処理を実行できます。

- データベースを最新の状態にリカバリします
- 特定の時点までデータベースをリカバリします

  リカバリの日時を指定する必要があります。

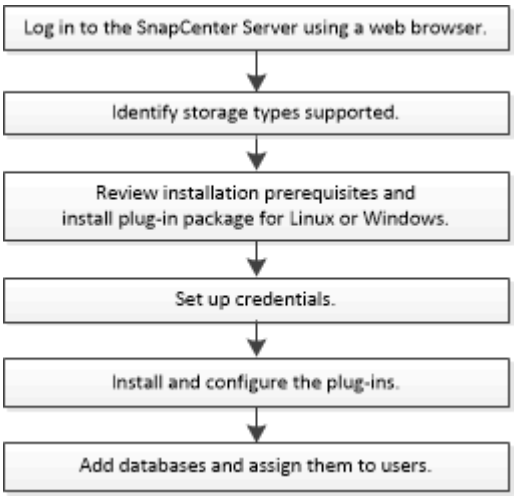
- 特定のデータバックアップまでデータベースをリカバリします

SnapCenter には、 SAP HANA データベースをリカバリするオプションもありません。

SnapCenter Plug-in for SAP HANA Database をインストールする準備をします

SnapCenter Plug-in for SAP HANA Database のインストールワークフロー

SAP HANA データベースを保護する場合は、 SnapCenter Plug-in for SAP HANA Database をインストールしてセットアップする必要があります。



ホストを追加して SnapCenter Plug-in for SAP HANA Database をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。SnapCenter Plug-in for SAP HANA Database は、 Windows と Linux のどちらの環境でも使用できます。

- ホストに Java 1.8 64 ビットがインストールされている必要があります。

  IBM Javaはサポートされていません。

- SAP HANA データベースの対話型端末（ HDBSQL クライアント）をホストにインストールしておく必要があります。
- Windows の場合は、「 LocalSystem 」 Windows ユーザを使用してプラグインの Creator Service が実行されている必要があります。これは、 Plug-in for SAP HANA Database がドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windows の場合は、ユーザストアキーを SYSTEM ユーザとして作成する必要があります。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。SnapCenter Plug-in for Microsoft Windows は、 Windows ホストに SAP HANA プラグインを使用してデフォルトで導入されます。
- Linux ホストの場合は、 HDB Secure User Store キーに HDBSQL OS ユーザとしてアクセスします。

- SnapCenter サーバが、 Plug-in for SAP HANA Database ホストの 8145 ポートまたはカスタムポートにアクセスできる必要があります。

Windows ホスト

- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。
- Plug-in for SAP HANA Database を Windows ホストにインストールする際に、 SnapCenter Plug-in for Microsoft Windows が自動的にインストールされます。
- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Windows ホストに Java 1.8 64 ビットがインストールされている必要があります。

  "すべてのオペレーティングシステム用の Java のダウンロード"

  。 "Interoperability Matrix Tool で確認してください" 要件に関する最新情報が含まれています。

Linux ホスト

- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Linux ホストに Java 1.8 64 ビットがインストールされている必要があります。

  "すべてのオペレーティングシステム用の Java のダウンロード"

  。 "Interoperability Matrix Tool で確認してください" 要件に関する最新情報が含まれています。

- Linux ホストで実行されている SAP HANA データベースを Plug-in for SAP HANA Database のインストール時にインストールすると、 SnapCenter Plug-in for UNIX が自動的にインストールされます。

SnapCenter Plug-ins Package for Linux をインストールするためのホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストシステムの基本的なスペースとサイジング要件を理解しておく必要があります。

項目	要件
オペレーティングシステム	• Red Hat Enterprise Linux の場合 • SUSE Linux Enterprise Server （ SLES ） サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB

項目	要件
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	2 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	Java 1.8.x （ 64 ビット）の Oracle Java と OpenJDK のバージョン Java を最新バージョンにアップグレードした場合は、 /var/opt/snapcenter /etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。。

SnapCenter Plug-in for SAP HANA Database のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますSnapCenter プラグインのインストールに必要なクレデンシャル、およびデータベースや Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- このタスクについて *
- Linux ホスト

  Linux ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。

  プラグインプロセスをインストールして開始するための sudo 権限がある root ユーザまたは root 以外のユーザのクレデンシャルを設定する必要があります。

  * ベストプラクティス： * ホストを導入してプラグインをインストールしたあとに Linux のクレデンシャルを作成することは可能ですが、 SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

- Windows ホスト

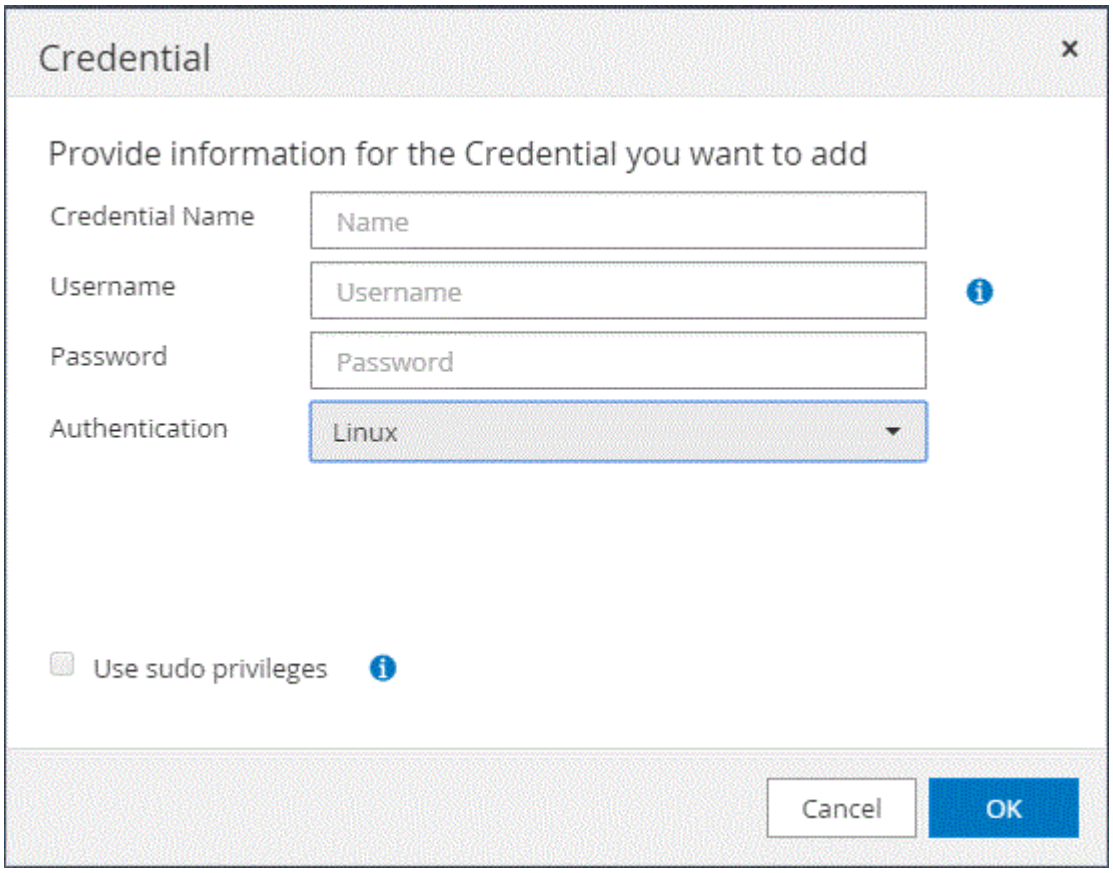
  プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。

リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定する必要があります。

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

- 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 * （ * Settings * ）] ページで、 [* 資格情報 * （ * Credential * ）] を
3. [新規作成（ New ）] をクリックする。



4. [**Credential**] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	手順
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。 ◦ NETBIOS_USERNAME_ ◦ _ ドメイン FQDN\ ユーザ名 _ • ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Username フィールドの有効な形式は、*username* です パスワードに二重引用符（"）またはバックティック（`）を使用しないでください。小なり（<）と感嘆符（！）は使用しないでください。 パスワードに記号を追加します。たとえば、lessthan <！10、lessthan10 <！、backtick 12とします。
パスワード	認証に使用するパスワードを入力します。
認証モード	使用する認証モードを選択します。
sudo 権限を使用する	root 以外のユーザのクレデンシャルを作成する場合は、「 * sudo 権限を使用する * 」チェックボックスをオンにします。 Linux ユーザのみに該当します。

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、「 * User and Access * 」ページで、ユーザまたはユーザグループにク

レデンシャルのメンテナンスを割り当てることができます。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
   a. 次の形式でユーザグループアカウントを作成します。

```
 domainName\accountName$
.. グループにコンピュータオブジェクトを追加します。
.. 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 「 Get-ADServiceAccount
」コマンドを実行して、サービスアカウントを確認します。
```

4. ホストで gMSA を設定します。
   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. ホストを再起動します。

b. PowerShell コマンド・プロンプトの「 Install-AdServiceAccount <gMSA > 」から次のコマンドを実行して ' ホストに gMSA をインストールします

c. 次のコマンドを実行して 'gMSA アカウントを確認します 'Test-AdServiceAccount <gMSA >

1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

   SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

SnapCenter Plug-in for SAP HANA Databases をインストールします

ホストを追加し、プラグインパッケージをリモートホストにインストールする

ホストの追加ページを使用 SnapCenter してホストを追加し、プラグインパッケージをインストールする必要があります。プラグインは、自動的にリモートホストにインストールされます。ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。

- 必要なもの *
- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- メッセージキューサービスが実行されていることを確認してください。

- 管理マニュアルには、ホストの管理に関する情報が記載されています。
- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

  "Windows Server 2012 以降で SAP HANA 用のグループマネージドサービスアカウントを設定します"

- このタスクについて *

SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加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、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. [**Hosts**] ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	ホストのタイプを選択します。 • Windows の場合 • Linux の場合 Plug-in for SAP HANA は、 HDBSQL クライアントホストにインストールされます。このホストは、 Windows システムでも Linux システムでもかまいません。
ホスト名	通信ホスト名を入力します。ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。 HDBSQL クライアントと HDBUserStore をこのホスト上に設定する必要があります。

フィールド	手順
クレデンシャル	作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。
6. （オプション） * その他のオプション * をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	Plug-in for SAP HANA は、 HDBSQL クライアントホストにインストールされます。このホストは、 Windows システムでも Linux システムでもかまいません。 • Windows 用 SnapCenter Plug-ins パッケージのデフォルトパスは C ： \Program Files\NetApp\SnapManager です。必要に応じて、パスをカスタマイズできます。 • Linux 用 SnapCenter Plug-ins パッケージのデフォルトパスは /opt/NetApp/SnapCenter です。必要に応じて、パスをカスタマイズできます。

フィールド	手順
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	Windows ホストの場合、プラグインサービスの実行にグループ管理サービスアカウント（ gMSA ）を使用する場合は、このチェックボックスをオンにします。 gMSA 名を domainName\accountName$ の形式で指定します。 gMSA は、 SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されます。

7. [Submit （送信）] をクリックします。

   [事前確認をスキップする] チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。ディスクスペース、 RAM 、 PowerShell のバージョン、 .NET のバージョン、場所（ Windows プラグインの場合）、および Java のバージョン（ Linux プラグインの場合）が、最小要件に照らして検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

   エラーがディスクスペースまたは RAM に関連している場合は、 C ： \Program Files\NetApp\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

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

8. ホストタイプが Linux の場合は、フィンガープリントを確認し、 * Confirm and Submit * をクリックします。

   クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。

   同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

1. インストールの進行状況を監視します。

   インストール固有のログファイルは、 /custom_location/snapcenter /logs にあります。

コマンドレットを使用して、複数のリモートホストに **Linux** または **Windows** 用の **SnapCenter** プラグインパッケージをインストールします

Install-SmHostPackage PowerShell コマンドレットを使用すると、複数のホストに Linux または Windows 向け SnapCenter プラグインパッケージを同時にインストールできます。

- 必要なもの *

プラグインパッケージをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 Open-SmConnection コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

   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、 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"。

プラグインを手動でインストールし、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、 -skipprecheck オプションを使用できます。

1. リモートインストールのクレデンシャルを入力します。

コマンドラインインターフェイスを使用して、 **Linux** ホストに **SnapCenter Plug-in for SAP HANA Database** をインストールします

SnapCenter ユーザインターフェイス（ UI ）を使用して、 SnapCenter Plug-in for SAP HANA Database をインストールする必要があります。環境で SnapCenter UI からプラグインのリモートインストールが許可されていない場合は、コマンドラインインターフェイス（ CLI ）を使用して、 Plug-in for SAP HANA Database をコンソールモードまたはサイレントモードでインストールできます。

- 必要なもの *
- HDBSQL クライアントが配置された各 Linux ホストに Plug-in for SAP HANA Database をインストールする必要があります。
- SnapCenter Plug-in for SAP HANA Database をインストールする Linux ホストは、依存するソフトウェア、データベース、オペレーティングシステムの要件を満たしている必要があります。

  サポートされる構成の最新情報については、 Interoperability Matrix Tool （ IMT ）を参照してください。

  "NetApp Interoperability Matrix Tool で確認できます"
- SnapCenter Plug-in for SAP HANA Database は、 SnapCenter Plug-ins Package for Linux の一部で

す。SnapCenter Plug-ins Package for Linux をインストールする前に、 Windows ホストに SnapCenter がインストールされている必要があります。

- 手順 *

1. Linux インストールファイル（ snapcenter _ linux_host_plugin.bin ）の SnapCenter Plug-ins パッケージを C ： \ProgramData\NetApp\SnapCenter \Package リポジトリから、 Plug-in for SAP HANA Database をインストールするホストにコピーします。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

2. コマンドプロンプトで、インストールファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。 'path-to_installation_bin_file/ snapcenter_linux_host_plugin.bin -i silent -dport=port_number_for _host-DSERVER_IP=server_name_or_IP_address -DSERVER_HTTPS_port=port_number_for _server

   - -dport には、 SMCore HTTPS 通信ポートを指定します。
   - - DSERVER_IP は、 SnapCenter サーバの IP アドレスを指定します。
   - - DSERVER_HTTPS_PORT には、 SnapCenter サーバの HTTPS ポートを指定します。
   - -duser_install_DIR - SnapCenter Plug-ins Package for Linux をインストールするディレクトリを指定します
   - DINSTALL_LOG_name は、ログファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

1. 次のコマンドを入力して、 =<installation directory>/NetApp/snapcenter /cscc /etc/SC_SMS_Services.properties ファイルを編集し、 plugins/enabled=hana ： 3.0 パラメータを追加します。
2. Add-Smhost コマンドレットと必要なパラメータを使用して、ホストを SnapCenter サーバに追加します。

   コマンドで使用できるパラメータとその説明については、 RUNNING Get Help command_name _ を使用して参照できます。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"。

Plug-in for SAP HANA のインストールのステータスを監視します

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

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

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

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [* Monitor*] ページで、 [* Jobs] をクリックします。
3. [* ジョブ *] ページで、プラグインのインストール操作のみが表示されるようにリストをフィルタリングするには、次の手順に従います。
   a. [* フィルタ * （ Filter * ）] をクリック
   b. オプション：開始日と終了日を指定します。
   c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
   d. Status ドロップダウンメニューから、インストールステータスを選択します。
   e. [適用（ Apply ）] をクリックします。
4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
5. ［ * ジョブの詳細 * ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。証明書を更新するには、証明書を取得する前に Subject Alternative Name （ SAN ）フィールドに値を入力します。ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA

証明書をインポートする必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除 *] ウィンドウで、 [* 証明書] を選択し、 [* 追加] をクリックします。
3. [* 証明書スナップイン *] ウィンドウで、 [* コンピュータアカウント *] オプションを選択し、 [* 完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

- 手順 *

1. GUI で次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
   c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
   d. ボックスから 16 進文字をコピーします。
   e. 16 進数の間のスペースを削除します。

たとえば、サムプリントが「A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

2. PowerShell で次の手順を実行します。
   a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

      Get-ChildItem - パス証明書： *localmachine\My*

   b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して **CA** 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   >netsh http delete sslcertipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   . 次のコマンドを実行して、新しくインストールした証明書を Windows ホストプラグインサービスにバインドします。

   [>$cert=<*certificate thumbprint*>]

   $GUID=[GUID]: NewGuid().ToString("B")

   ```
   >netsh http add sslcertipport=0.0.0.0:_<SMCore Port>_certthash=$cert
   appid="$GUID"
   ```

   例：

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Linux ホストで SnapCenter SAP HANA Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードの管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、 SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

カスタムプラグインでは、ファイル「 keystore.JKS 」を使用します。このファイルは、信頼ストアおよびキーストアとして _/opt/NetApp/snapcenter / scc /etc/both にあります。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

- 手順 *

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   キー「 keystore.pass 」に対応する値です。

2. キーストアのパスワードを変更します。

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

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

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

3. パスワードを変更したら、サービスを再起動してください。

> カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *

1. カスタムプラグインキーストアを含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア .jks

4. ルート証明書または中間証明書を追加します。

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```
.
カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

- 手順 *
  1. カスタムプラグインキーストア /opt/NetApp/snapcenter / scc などが含まれているフォルダに移動します
  2. ファイル 'keystore.jkS' を探します。
  3. キーストアに追加された証明書を表示します。

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

     keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.JKS -deststoretype JKS `
  5. キーストアに追加された証明書を表示します。

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

     デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

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

```
 keytool -changealias -alias "long_alias_name" -destalias
"simple_alias" -keystore keystore.jks
```
. agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値をキー SCC_CERTIFICATE_ALIAS に更新します。

8. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ CRL ）を設定します

- このタスクについて *
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、「 /opt/netapp/snapcenter /sscc /etc/crl 」です。
- 手順 *

1. agent.properties ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。

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

Windows ホストで SnapCenter SAP HANA Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードの管理、 CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、 SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

カスタムプラグインは、 _ C ： \Program Files\NetApp\SnapManager \Snapcenter Plug-in Creator\etc_both にある file_keystore.JKS_を 信頼ストアおよびキーストアとして使用します。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

- 手順 *

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   key_keystore.pass_ に対応する値です。

2. キーストアのパスワードを変更します。

   keytool -storepasswd -keystore keystore.JKS

   > Windows のコマンドプロンプトで「 keytool 」コマンドが認識されない場合は、keytool コマンドを完全なパスに置き換えます。

   C ： \Program Files\Java\<JDK_version >\bin\keytool .exe "-storepasswd -keystore keystore.JKS

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

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.JKS

agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

1. パスワードを変更したら、サービスを再起動してください。

   カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

- 手順 *

1. カスタムプラグインの keystore _C ： \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. ルート証明書または中間証明書を追加します。

   keytool -import-trustcacerts -alias myRootCA -file/root/USERTrustRSA_Root.cer -keystore keystore.JKS

5. カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

- 手順 *

1. カスタムプラグインの keystore _C ： \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. file_keystore.JKS_</Z1> を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

   keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.JKS -deststoretype JKS

5. キーストアに追加された証明書を表示します。

keytool -list -v キーストア *.JKS*

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

   デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

*keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

1. *agent.properties* ファイルの CA 証明書からエイリアス名を設定します。

   この値をキー SCC_CERTIFICATE_ALIAS に更新します。

2. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ **CRL** ）を設定します

- このタスクについて *
- 関連する CA 証明書の最新の CRL ファイルをダウンロードするには、を参照してください "SnapCenter CA 証明書の証明書失効リストファイルを更新する方法"。
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、 *'C:\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\crl'* です。
- 手順 *
  1. *agent.properties* ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。
  2. このディレクトリに複数の CRL ファイルを配置できます。

     着信証明書は各 CRL に対して検証されます。

プラグインの **CA** 証明書を有効にします

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

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで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"。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。

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

- 終了後 *

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

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

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

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

データベースが仮想マシン（ VM ）に格納されている場合や VM とデータストアを保護する場合は、 SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください "導入の概要"。

CA 証明書を導入する

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

CRL ファイルを設定します

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

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

データ保護を準備

SnapCenter Plug-in for SAP HANA Database を使用するための前提条件

SnapCenter Plug-in for SAP HANA Database を使用するには、 SnapCenter 管理者が事前に SnapCenter サーバをインストールして設定し、前提条件となるタスクを実行する

必要があります。

- SnapCenter サーバをインストールして設定します。
- SnapCenter サーバにログインします。
- 必要に応じて、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、 SnapCenter 環境を設定します。
- Java 1.7 または Java 1.8 を Linux ホストまたは Windows ホストにインストールします。

  ホストマシンの環境パス変数に Java パスを設定する必要があります。
- バックアップレプリケーションが必要である場合は、 SnapMirror と SnapVault をセットアップします。
- Plug-in for SAP HANA Database をインストールするホストに HDBSQL クライアントをインストールします。

  このホストで管理する SAP HANA ノードのユーザストアキーを設定します。
- SAP HANA データベース 2.0SPS05 で SAP HANA データベースのユーザアカウントを使用している場合は、 SnapCenter サーバでバックアップ、リストア、およびクローニングの処理を実行するための次の権限があることを確認します。
  - バックアップ管理者
  - カタログの読み取り
  - データベースバックアップ管理者
  - データベースリカバリオペレータ

SAP HANA データベースの保護におけるリソース、リソースグループ、ポリシーの使用方法

SnapCenter を使用する前に、実行するバックアップ、クローニング、およびリストアの処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- リソースとは、通常は SnapCenter でバックアップまたはクローニングする SAP HANA データベースのことです。
- SnapCenter リソースグループは、ホスト上のリソースの集まりです。

  リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているリソースに対して処理が実行されます。

  単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。スケジュールされたバックアップを単一のリソースおよびリソースグループに対して実行することもできます。
- ポリシーは、バックアップ頻度、レプリケーション、スクリプト、およびデータ保護処理のその他の特性を指定するものです。

  リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。単一のリソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

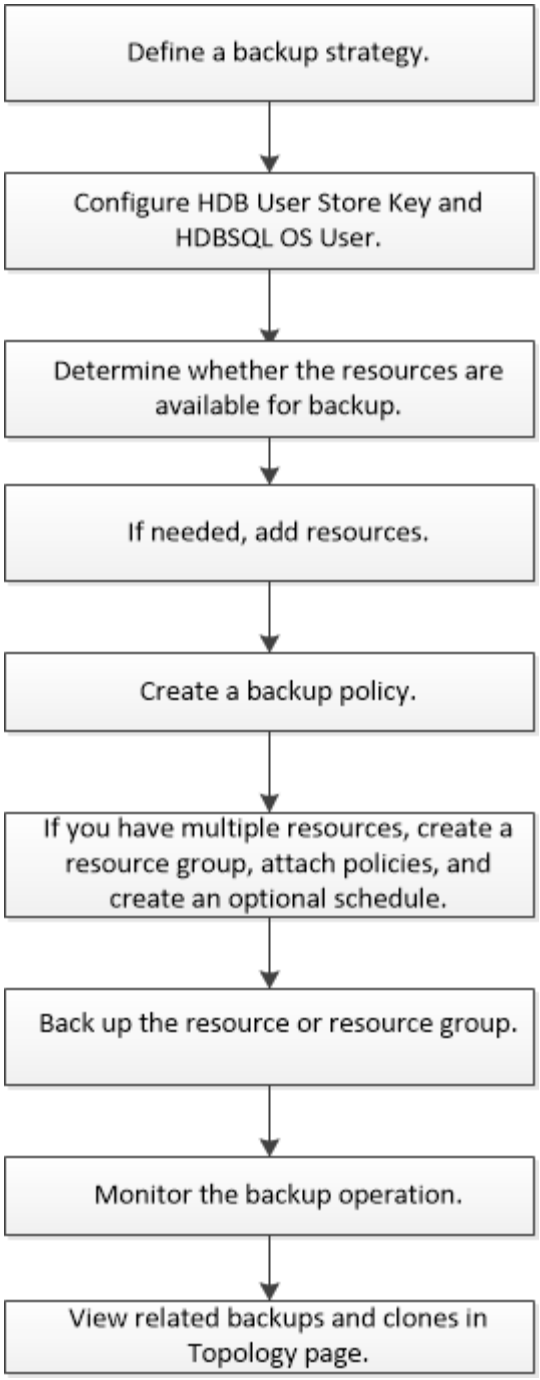
リソースグループは、保護対象となるものを定義するものであり、日と時間の観点から保護する必要がある場合に考えてみてください。ポリシーは、保護方法を定義するものと考えてください。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。リソースグループを作成してポリシーを適用する際に、フルバックアップを毎日実行するようにリソースグループを設定できます。

SAP HANA のリソースをバックアップ

SAP HANA のリソースをバックアップ

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://library.netapp.com/ecm/ecm_download_file/ECMLP2877143["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 データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します

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

- 必要なもの *
- SAP HANA データベースで HDB Secure User Store Key および HDB SQL OS User が設定されていない場合は、自動検出されたリソースにのみ赤い南京錠のアイコンが表示されます。その後の検出操作中に、設定されている HDB Secure User Store Key が正しくないか、データベース自体へのアクセスを提供していない場合は、赤い南京錠のアイコンが再表示されます。
- データ保護処理を実行するには、 HDB Secure User Store Key および HDB SQL OS ユーザーがデータベースを保護できるように設定するか、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 ユーザーを構成する必要があります。HDB SQL OS ユーザがテナントデータベースのみにアクセスするように設定されていると、検出処理が失敗します。
- 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）をクリックします をクリックし、ホスト名を選択します。

     をクリックします をクリックしてフィルタペインを閉じます。
  4. 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. [データベース設定の構成] 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 ページからデータベースの設定を変更できます。

リソースを検出し、マルチテナントデータベースコンテナでデータ保護を準備

データベースを自動的に検出します

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、そ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。

- 必要なもの *
- 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 Secure User Store Key および HDB SQL OS ユーザを設定しておく必要があります。
  - SID adm ユーザーを使用して HDB ユーザーストアキーを構成する必要がありますたとえば、 A22 を SID として使用する HANA システムの場合、 HDB User Store Key は a22adm で構成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場合は、仮想環境のストレージ情報を指定する必要があります。
- このタスクについて *

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、リソースページに表示されます。

自動で検出されたリソースは変更または削除できません。

- 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. [* 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） * をクリックします* をクリックし、ホスト名を選択します。

     次に、 * をクリックします* 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。

     - データベースがネットアップストレージ上にあり、保護されていない場合は、総体的なステータス列に Not protected と表示されます。
     - データベースがネットアップストレージシステム上にあり、保護されている場合に、バックアップ処理が実行されていないと、 [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 Secure User Store Key が設定されていない場合は、リソースの横に赤い南京錠のアイコンが表示されます。その後の検出操作中に、設定されている HDB Secure User Store Key が正しくないか、データベース自体へのアクセスを提供していない場合は、赤い南京錠のアイコンが再表示されます。

- 終了後 *

データ保護処理を実行するには、データベースを保護できるように HDB Secure User Store Key および HDBSQL OS ユーザを設定するか、またはリソースグループにこのキーを追加する必要があります。

"SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します"

マルチテナントデータベースコンテナでデータ保護を準備

SnapCenter に直接登録された 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が自動的に検出されます。プラグインをインストールまたはアップグレードした後、プラグインホスト上にあるすべてのマルチテナントデータベースコンテナ（ MDC ）リソースに対して、別の MDC リソースが自動的に検出されて 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。

- このタスクについて *

たとえば、 SnapCenter 4.2 では、 E90 MDC リソースがプラグインホスト上にあり、手動で登録されている場合、 SnapCenter 4.3 にアップグレードした後に、別の 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付けられたバックアップは、保持期間が満了するまで保持される必要があります。保存期間が終了したら、古い MDC リソースを削除して、新しい自動検出された MDC リソースを引き続き管理できます。

「古い MDC リソース」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使用してデータ保護処理を開始するには、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] 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. リソースページから新しいリソースを選択して、 SnapCenter 4.3 にアップグレードした後に検出された新しい MDC リソースを構成します。

   「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、古い MDC リソースと同じ SID を持つリソース、特定のホスト、およびリソースページのその横に赤い南京錠のアイコンで識別できます。

3. SnapCenter 4.3 へのアップグレード後に検出された新しい MDC リソースを保護するには ' 保護ポリシー ' スケジュール ' 通知設定を選択します
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. [リソース] 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 コピーの保持期間が 7 日で、セカンダリ Snapshot コピーの保持期間が 45 日の場合、 45 日が完了してすべてのバックアップが削除されたあとに、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。

- 詳細はこちら *

"SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します"

"Topology ページで、 SAP HANA データベースのバックアップとクローンを表示します"

プラグインホストにリソースを手動で追加します

自動検出は、特定の HANA インスタンスではサポートされていません。これらのリソースは手動で追加する必要があります。

- 必要なもの *

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。

- このタスクについて *

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、これらのリソースではデータ保護処理はサポートされていません。

- HANA マルチホスト構成
- HANA システムレプリケーション
- 同じホスト上の複数のインスタンス
- 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	手順
リソースタイプ（ Resource Type ）	リソースタイプを入力します。リソースタイプは、単一コンテナ、マルチテナントデータベースコンテナ（ MDC ）、非データボリュームです。
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。

フィールド	手順
hdb セキュアユーザストアキー	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。
HDBSQL OS ユーザ	HDB Secure User Store Key が設定されているユーザー名を入力します。Windows の場合は、HDBSQL OS ユーザがシステムユーザであることが必須です。そのため、システムユーザーに対して HDB Secure User Store Key を設定する必要があります。

4. [ストレージ容量の確保 *] 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：「 * 」をクリックします  * 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 、および 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ます。

"ユーザまたはグループを追加し、ロールとアセットを割り当てます"

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 リソースにバックアップが関連付けられている場合、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を作成する

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、バックアップを管理、スケジューリング、および保持する方法を定めた一連のルールです。

- 必要なもの *
- 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。
- ユーザが Snapshot コピー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 SnapCenter に SVM を割り当てる必要があります。

  また、ポリシーでレプリケーション、スクリプト、およびアプリケーションの設定を指定することもできます。こ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。

- 手順 *

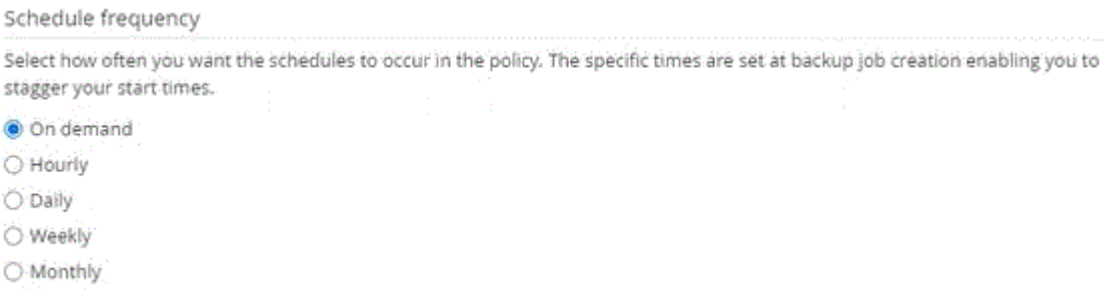
1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [* 設定 *] ページで、 [* ポリシー *] をクリックします。
3. [新規作成（ New ）] をクリックする。
4. [* 名前 *] ページで、ポリシー名と概要を入力します。
5. [* 設定 * （ * Settings * ）] ページで、次の手順を実行します。

   - バックアップタイプを選択します。

状況	手順
データベースの整合性チェックを実行します	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 コピーテクノロジを使用してバックアップを作成します	「 * 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と値の組み合わせを複数指定することができます。

1. [* Retention *] 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 コピーを保持します	保持する Snapshot コピーの総数 * を選択し、保持する Snapshot コピーの数を指定します。 Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。 最大保持数は、 ONTAP 9.4 以降のリソースでは 1018 、 ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。 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 コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。
Snapshot コピーを特定の日数だけ保持します	「 * Snapshot コピーを保持する期間」を選択し、 Snapshot コピーを削除するまで保持する日数を指定します。

2. Snapshot コピーベースのバックアップの場合は、 * Replication * ページでレプリケーション設定を指定します。

フィールド	手順
• ローカル Snapshot コピー作成後に 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。 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 コピー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 コピー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。
• 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。
• 二次ポリシーラベル *	Snapshot ラベルを選択します。 選択した Snapshot コピーラベルに応じて、 ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。 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。
• 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の Snapshot コピー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。

3. 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。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。

- 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	手順
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検索するときに役立つ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。
Snapshot コピーには、カスタムの名前形式を使用します	Snapshot コピー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 などですデフォルトでは、Snapshot コピー名の後ろにタイムスタンプが追加されます。

4. [* リソース] ページで、 [* ホスト **]** ドロップダウン・リストからホスト名を選択し、 **[** 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。

   これにより、画面上の情報をフィルタリングできます。

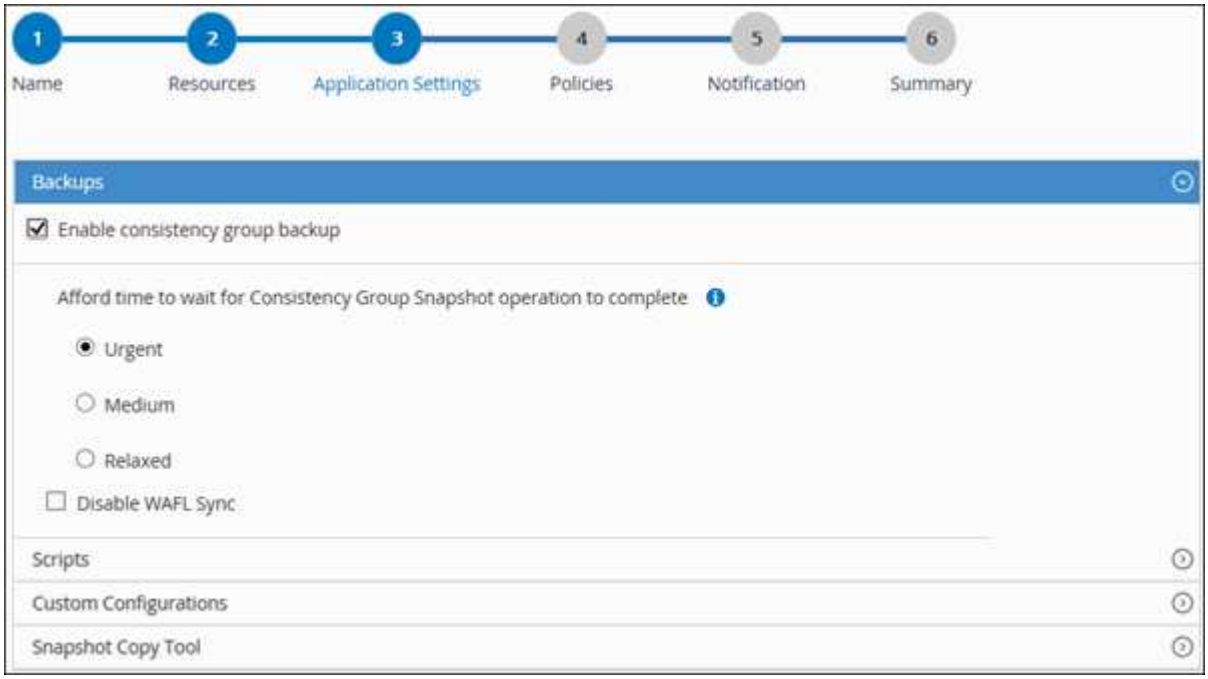
5. [使用可能なリソース（ Available Resources ）] セクションからリソースを選択し、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。
6. [アプリケーションの設定 *] ページで、次の操作を行います。

   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、次の作業を実行します。

フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot コピー処理が完了するまでの待機時間を指定するには、「至急」、「 * 中」、または「 * relaxed 」を選択します。 Urgent = 5 秒、 Medium = 7 秒、 Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

+



a. * Scripts * の矢印をクリックして、休止、 Snapshot コピー、および休止解除の各処理に対する PRE / POST 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	（はい / いいえ）	アーカイブログ管理を有効にしてアーカイブログを削除できます。

パラメータ	設定	説明
archive_log_retention の略	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	（はい / いいえ）	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ており、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ていません。

c. Snapshot コピーツールの * 矢印をクリックして、 Snapshot コピーを作成するツールを選択します。

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 コピーを作成する。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 を使用して、ストレージレベルの Snapshot コピーを作成します	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
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	「 * other * 」を選択し、ホストで実行するコマンドを入力して Snapshot コピーを作成します。

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。

      また、 * 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. Configure Schedules （スケジュールの設定）列で、 * をクリックします * 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。

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

1. [**Notification**] ページの **[*Email preference**] 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。

2. 概要を確認し、 [完了] をクリックします。

SAP HANA データベースをバックアップする

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。

- 必要なもの *
- 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になっていることを確認してください。
- 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、 Set-SmConfigSettings コマンドレットを使用して、 HANA プロパティファイルの allow_file_by_backup_IFINACTIVE_tenants_present パラメータを * YES * に設定します。

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、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"

- 手順 *

1. 左側のナビゲーションペインで、 * 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、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リングします。

- をクリックします * をクリックし、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。をクリックします をクリックしてフィルタペインを閉じます。

1. バックアップするリソースをクリックします。
2. リソース * ページで、 Snapshot コピーにカスタム名形式を使用する * を選択し、 Snapshot コピー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_or_resource_hostname_hostname_1 です。デフォルトでは、 Snapshot コピー名の後ろにタイムスタンプが追加されます。

3. [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] 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。

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

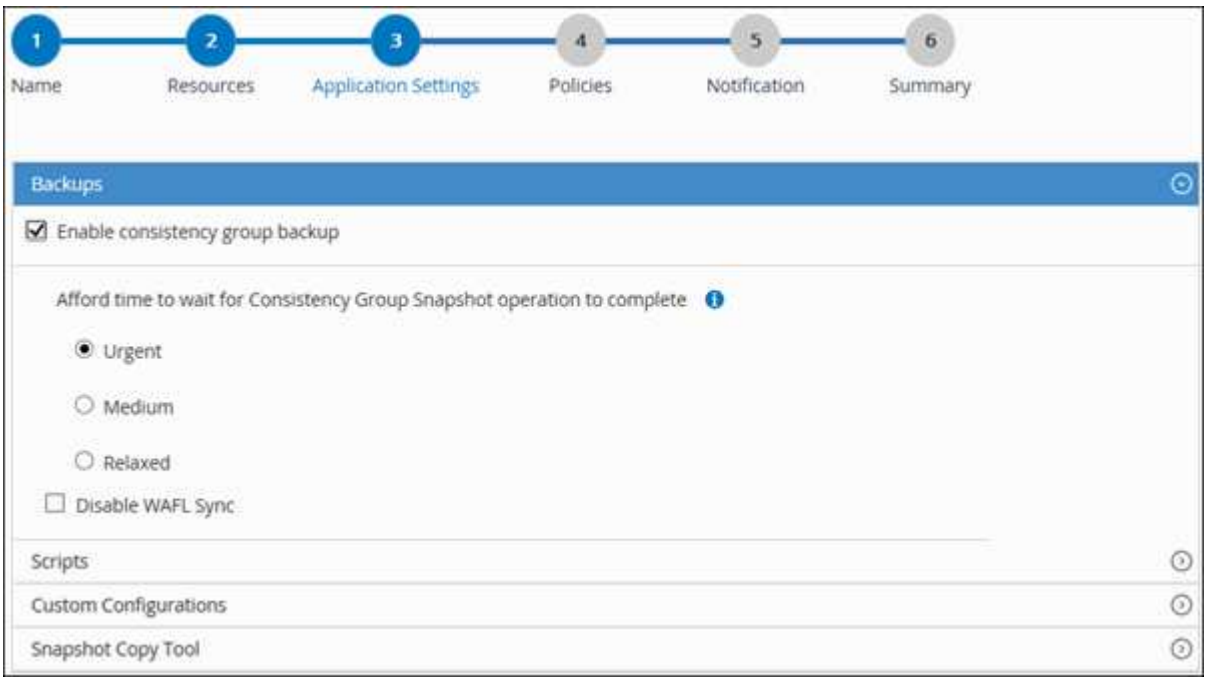
フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot コピー処理が完了するまでの待機時間を指定するには、「至急」、「 * 中」、または「 * relaxed 」を選択します。Urgent = 5 秒、 Medium = 7 秒、 Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

   - [* Scripts] の矢印をクリックすると、休止、 Snapshot コピー、および休止解除の各処理に対して PRE および POST のコマンドが実行されます。

     バックアップ処理を終了する前にプリ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。

   - [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 * 矢印をクリックして、 Snapshot コピーを作成するツールを選択します。

状況	作業
SnapCenter を使用してストレージレベルの Snapshot コピーを作成する	ファイルシステムの整合性なしで SnapCenter * を選択します。
SnapCenter ： 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 コピーを作成する	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 コピーを作成するコマンドを入力するには、次のコマンドを入力します	「 * other * 」を選択し、コマンドを入力して Snapshot コピーを作成します。



4. [**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。

   また、 * 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。

   a. * をクリックします * 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。

   b. [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、 [適用されたスケジュール] 列に一覧表示されます。

1. [**Notification**] ページの [***Email preference**] 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。

2. 概要を確認し、 [完了] をクリックします。

   リソースのトポロジページが表示されます。

3. [今すぐバックアップ] をクリックします。

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

   b. [バックアップ] をクリックします。

5. 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 が保護関係を検出できない場合があります。

     詳細については、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 関係を検出できません"

   - VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、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*

リソースグループをバックアップする

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。

- 必要なもの *
- 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。
- このタスクについて *

リソースグループは、必要に応じて * Resources * ページから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 * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* 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、をクリックします をクリックし、タグを選択します。をクリックします をクリックしてフィルタペインを閉じます。

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

   b. [バックアップ] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

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

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には、 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。

- 必要なもの *
- 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 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てデータベースをバックアップします

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。

- 必要なもの *
- 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.neta
pp.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. Add-SmResourceGroup コマンドレットを使用して、リソースを保護するか、新しいリソースグループを SnapCenter に追加します。

   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"="scc
orelinux62.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ています。

```
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";"Plug
inName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDa
taVolume\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する。

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
```

1. 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、または

失敗）を監視します。

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

2. Get-SmBackupReport コマンドレットを使用して、リストア処理やクローニング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"。

バックアップ処理を監視する

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

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

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

- 手順 *

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

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

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

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

アクティビティペインで、 **SAP HANA** データベースに対するデータ保護処理を監視します

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

[Activity （アクティビティ）] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

- 手順 *

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

2. をクリックします をクリックして、最近の 5 つの操作を表示します。

   いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

Topology ページで、 SAP HANA データベースのバックアップとクローンを表示します

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。

- このタスクについて *

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

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

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

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

[* トポロジ *] 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すべてのバックアップとクローンを表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、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 コピーバックアップ、およびクローンの合計数が表示されます。

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

1. [コピーの管理] 表示で、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。

2. 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。

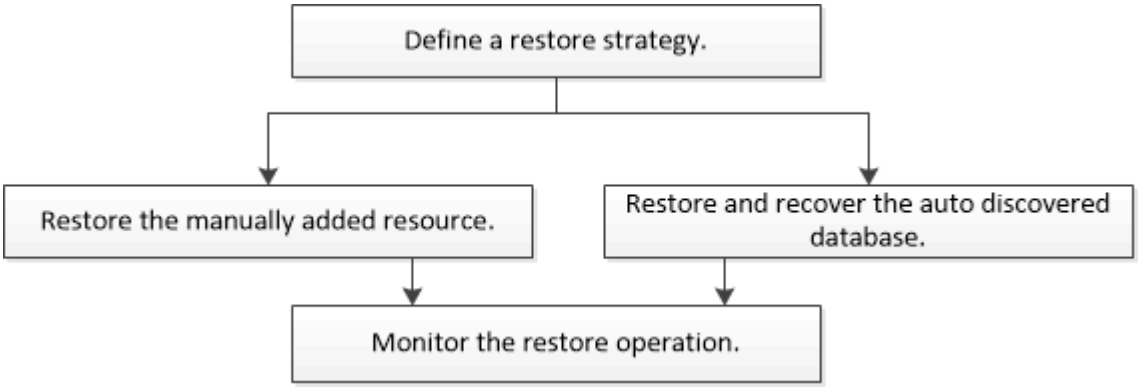
3. クローンを削除する場合は、表でクローンを選択し、をクリックします 。
4. クローンをスプリットする場合は、表でクローンを選択し、をクリックします 。

SAP HANA データベースをリストア

リストアワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア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。

"SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

手動で追加したリソースバックアップをリストアおよびリカバリする

SnapCenter を使用して、 1 つ以上のバックアップからデータをリストアおよびリカバリできます。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- このタスクについて *
- ファイルベースのバックアップのコピーを SnapCenter からリストアすることはできません。
- SnapCenter 4.3 にアップグレードすると、 SnapCenter 4.2 で作成されたバックアップはリストアできますが、リカバリすることはできません。SnapCenter 4.2 で作成されたバックアップをリカバリするには、SnapCenter の外部で HANA Studio または HANA リカバリスクリプトを使用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、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。

   リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、およびステータスとともに表示されます。

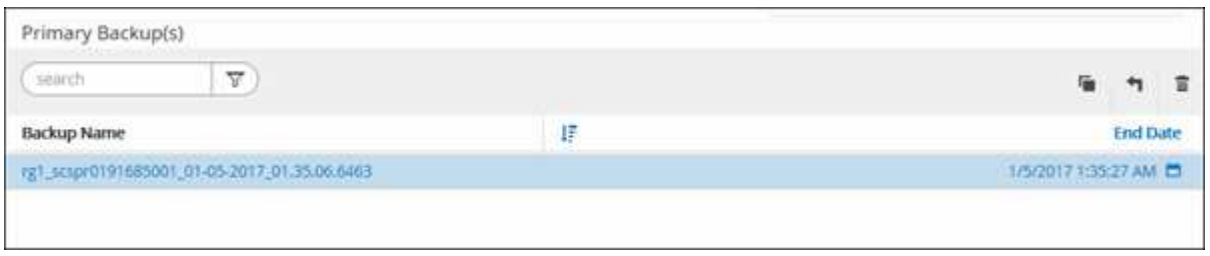
   リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。

   リソースが保護されていない場合は ' 保護されていないというメッセージが [全体のステータス] 列に表示されますこれは、リソースが保護されていないこと、またはリソースが別のユーザによってバックアップされていることを意味します。

3. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

   リソースのトポロジページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。
5. [プライマリ・バックアップ] テーブルで、リストア元のバックアップを選択し、 [*] をクリックします *



6. ［ * リストア範囲 * ］ ページで、 ［ * リソース全体 ］ または ［ * ファイルレベル * ］ を選択します。

   a. Complete Resource * を選択すると、 SAP HANA データベースに設定されているすべてのデータボリュームがリストアされます。

      リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

   b. 「 * ファイルレベル * 」を選択した場合は、「 * すべて * 」を選択するか、特定のボリュームまたは qtree を選択してから、それらのボリュームまたは qtree に関連するパスをカンマで区切って入力できます

      - ボリュームと qtree は複数選択できます。
      - リソースタイプが LUN の場合は、 LUN 全体がリストアされます。

        LUN は複数選択できます。

「 * all * 」を選択すると、ボリューム、 qtree 、または LUN 上のすべてのファイルがリストアされます。

1. リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを、 [*Pre ops *] ページで入力します。

   自動検出されたリソースにはアンマウントコマンドを使用できません。

2. [*Post ops *] ページで、 mount コマンドおよび post restore コマンドを入力して、リストア・ジョブの実行後に実行します。

   自動検出されたリソースに対しては、 mount コマンドを使用できません。

3. [**Notification**] ページの **[*Email preference**] 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 メールアドレスと E メールの件名を指定する必要があります。また、 [* 設定 * （ Settings * ）] > [* グローバル設定 * （ * Global Settings * ）] ページでも SMTP を設定する必要があります。

4. 概要を確認し、 [完了] をクリックします。
5. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

自動検出されたデータベースバックアップをリストアおよびリカバリする

SnapCenter を使用して、 1 つ以上のバックアップからデータをリストアおよびリカバリできます。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。

- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- このタスクについて *
- ファイルベースのバックアップのコピーを SnapCenter からリストアすることはできません。
- SnapCenter 4.3 にアップグレードすると、 SnapCenter 4.2 で作成されたバックアップはリストアできますが、リカバリすることはできません。SnapCenter 4.2 で作成されたバックアップをリカバリするには、SnapCenter の外部で HANA Studio または HANA リカバリスクリプトを使用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、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。

   リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、およびステータスとともに表示されます。

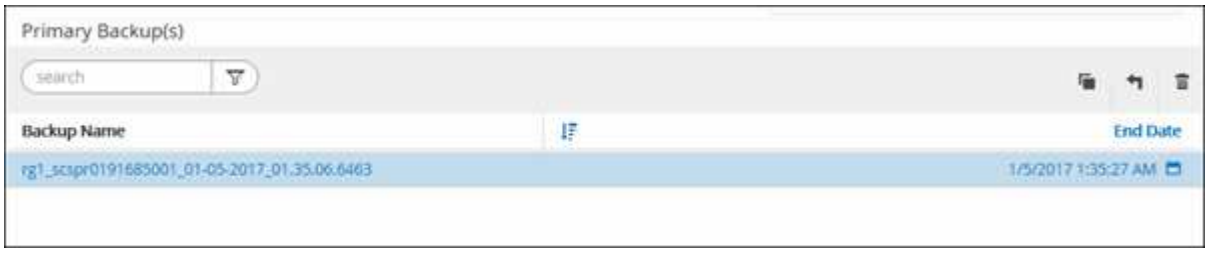
   リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。

   リソースが保護されていない場合は ' 保護されていないというメッセージが [全体のステータス] 列に表示されますこれは、リソースが保護されていないこと、またはリソースが別のユーザによってバックアップされていることを意味します。

3. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

   リソースのトポロジページが表示されます。

4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。
5. [プライマリ・バックアップ] テーブルで、リストア元のバックアップを選択し、 [*] をクリックします *



6. [* リストア範囲 *] ページで、 [* リソース全体 *] を選択して、 SAP HANA データベースの構成済みデータボリュームをリストアします。

   Complete Resource * （ * Volume Revert * あり / なし）または * Tenant Database * のいずれかを選択できます。

   ユーザが * テナントデータベース * オプションまたは * Complete Restore * オプションを選択した場

合、複数のテナントに対して SnapCenter サーバがリカバリ処理をサポートしていません。リカバリ処理を実行するには、 HANA Studio または HANA Python スクリプトを使用する必要があります。

a. ボリューム全体をリストアする場合は、 * Volume Revert * を選択します。

このオプションは、 NFS 環境における SnapCenter 4.3 で作成されたバックアップに使用できます。

リソースにボリュームまたは qtree が含まれている場合、そのボリュームまたは qtree でリストア対象として選択された Snapshot コピーのあとに作成された Snapshot コピーは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。このオプションは、リストア対象として「 * Volume Revert * 」オプションを指定した状態で * Complete Resource * を選択した場合に使用できます。

b. [* Tenant Database] を選択します。

このオプションは MDC リソースでのみ使用できます。

リストア処理を実行する前にテナントデータベースを停止する必要があります。

「 * テナントデータベース * 」オプションを選択した場合は、リカバリ処理を実行するために、 HANA Studio を使用するか、 SnapCenter 外部の HANA リカバリスクリプトを使用する必要があります。

1. [* Recovery scope] ページで、次のいずれかのオプションを選択します。

状況	手順
現在までできるだけ近い時間にリカバリする必要がある	[* 最新の状態に回復する *] を選択します。単一のコンテナリソースについては、 1 つ以上のログとカタログのバックアップ先を指定します。 マルチテナントデータベースコンテナ（ MDC ）リソースの場合は、 1 つ以上のログバックアップの場所とバックアップカタログの場所を指定 MDC リソースの場合は、パスにシステムデータベースとテナントデータベースのログの両方が含まれている必要があります。

状況	手順
指定した時点までリカバリする場合	[* 特定の時点にリカバリする *] を選択します。 a. タイムゾーンを選択します。 ブラウザのタイムゾーンはデフォルトで入力されています。 選択したタイムゾーンと入力時間が絶対 GMT に変換されます。 b. 日時を入力します。たとえば、 HANA Linux ホストは CA のサニーベールにあり、 Raleigh のユーザは SnapCenter にログインをリカバリしています。 これらのロケーション間の時間差は 3 時間で、ユーザは NC の Raleigh からログインしているため、 GUI で選択されるデフォルトのブラウザタイムゾーンは GMT-04 ： 00 です。 ユーザが CA のサニーベールから 5 午前 6 時までのリカバリを実行する場合は、ブラウザのタイムゾーンを HANA Linux ホストのタイムゾーン（ GMT-07 ： 00 ）に設定し、日時を午前 5 時に指定する必要があります 単一のコンテナリソースについては、 1 つ以上のログとカタログのバックアップ先を指定します。 MDC リソースの場合は、 1 つ以上のログバックアップの場所とバックアップカタログの場所を指定します。 MDC リソースの場合は、パスにシステムデータベースとテナントデータベースのログの両方が含まれている必要があります。
特定のデータ・バックアップにリカバリする場合	［ * 指定されたデータバックアップにリカバリする * ］ を選択します。
リカバリが不要である場合	「リカバリなし」を選択します。リカバリ処理は HANA Studio から手動で実行する必要があります。

リカバリできるの SnapCenter は、ホストとプラグインの両方が SnapCenter 4.3 にアップグレードされ、リストア用に選択されたバックアップがリソースの変換後または自動検出されたあとに実行される場合に限られます。

2. リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを、 [*Pre ops *] ページで入力します。

   自動検出されたリソースにはアンマウントコマンドを使用できません。

3. [*Post ops *] ページで、 mount コマンドおよび post restore コマンドを入力して、リストア・ジョブの実行後に実行します。

   自動検出されたリソースに対しては、 mount コマンドを使用できません。

4. [**Notification**] ページの **[*Email preference**] 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 メールアドレスと E メールの件名を指定する必要があります。また、 [* 設定 * （ Settings * ）] > [* グローバル設定 * （ * Global Settings * ）] ページでも SMTP を設定する必要があります。

5. 概要を確認し、 [完了] をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

PowerShell コマンドレットを使用して SAP HANA データベースをリストアする

SAP HANA データベースのバックアップをリストアするときは、 SnapCenter サーバとの接続セッションを開始し、バックアップをリストしてバックアップ情報を取得し、バックアップをリストアします。

- 必要なもの *

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。

- 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/
   ```

2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップを特定します。

   この例では、リストアできるバックアップが 2 つあります。

```
 PS C:\> Get-SmBackup

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM  Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

この例では、 2015 年 1 月 29 日から 2015 年 2 月 3 日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. HANA Studio でリカバリプロセスを開始します。

   データベースがシャットダウンされます。

4. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

   AppObjectId は「 Host\Plugin\UID 」です。 UID=SID は単一コンテナタイプのリソース用で、 UID=MDC\SID は複数コンテナのリソース用です。ResourceID は、 Get-smResources コマンドレットから取得できます。

   ```
   Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
   ```

   この例は、プライマリストレージからデータベースをリストアする方法を示しています。

   ```
   Restore-SmBackup -PluginCode HANA -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 3
   ```

   この例は、セカンダリストレージからデータベースをリストアする方法を示しています。

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

+ バックアップが HANA Studio でリカバリに使用できるようになります。

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、 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 データベースのリストア処理を監視する

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

- このタスクについて *

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

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました

- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- キャンセルされました
- 手順 *

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

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

ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

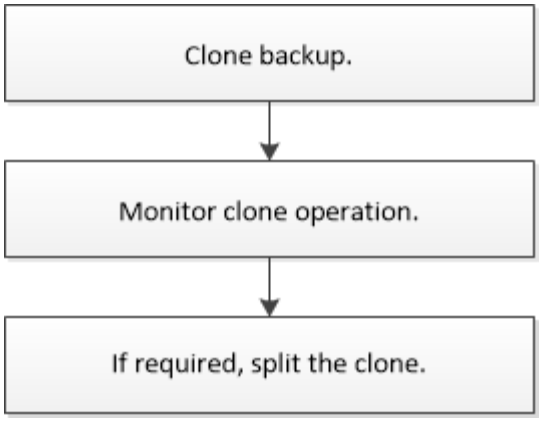
SAP HANA リソースのバックアップをクローニングする

クローニングワークフロー

クローニングワークフローには、クローニング処理の実行と処理の監視が含まれます。

- このタスクについて *
- ソースの SAP HANA サーバでクローニングを実行できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
  - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
  - データの抽出と操作を行うツールで、データウェアハウスにデータを取り込むため
  - 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング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。

SAP HANA データベースのバックアップをクローニングします

SnapCenter を使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

- 必要なもの *
- リソースまたはリソースグループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine （ SVM ）に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- ファイルベースのバックアップはクローニングできません。
- ターゲットクローンサーバの SAP HANA インスタンス SID が、 Target Clone SID フィールドに入力されたものと同じであることが必要です。
- このタスクについて * クローン・スプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。
- 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、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。

   リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、ステータスなどの情報とともに表示されます。
3. リソースまたはリソースグループを選択します。

   リソースグループを選択する場合は、リソースを選択する必要があります。

   リソースまたはリソースグループのトポロジページが表示されます。
4. Manage Copies （コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはバックアップ）ストレージシステムから * Backups （バックアップ）を選択します。

5. 表からデータバックアップを選択し、をクリックします 。
6. [* Location * （場所 * ）] ページで、次の操作を実行します。

フィールド	手順
プラグインホスト	クローンのマウント先のプラグインがインストールされたホストを選択します。
ターゲットクローンの SID	既存のバックアップからクローニングする SAP HANA インスタンス ID を入力します。
NFS エクスポートの IP アドレス	クローニングしたボリュームをエクスポートする IP アドレスまたはホスト名を入力します。
iSCSI イニシエータ	LUN のエクスポート先であるホストの iSCSI イニシエータ名を入力します。このオプションは、 LUN リソースタイプを選択した場合にのみ使用できます。
プロトコル	LUN プロトコルを入力します。このオプションは、 LUN リソースタイプを選択した場合にのみ使用できます。

リソースとして LUN を選択し、セカンダリバックアップからクローニングする場合、デスティネーションボリュームのリストが表示されます。1 つのソースについて複数のデスティネーションボリュームを選択することができます。

クローニングを実行する前に、 iSCSI イニシエータまたは FCP が存在し、代替ホストに設定およびログインしていることを確認する必要があります。

7. [* Scripts] ページで、次の手順を実行します。

スクリプトはプラグインホストで実行されます。

a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
   - クローニング前のコマンド：同じ名前の既存のデータベースを削除します
   - クローニング後のコマンド：データベースの検証やデータベースの起動
b. ホストにファイルシステムをマウントするには、 mount コマンドを入力します。

Linux マシンのボリュームまたは qtree に対する mount コマンド：

NFS の例：

```
mount VSERVER_DATA_IP:%{VOLUME_NAME_Clone} /mnt
```

8. [**Notification**] ページの [***Email preference**] 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。

9. 概要を確認し、 [完了] をクリックします。
10. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

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をクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

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。

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"。

- 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/
```

2. Get-SmBackup コマンドレットを使用して、クローニング処理を実行するバックアップを取得します。

   この例では、クローニングできるバックアップが 2 つあります。

```
 C:\PS> Get-SmBackup

        BackupId                        BackupName
BackupTime                    BackupType
        --------                        ----------
----------                    ----------
         1                       Payroll Dataset_vise-f6_08... 8/4/2015
11:02:32 AM          Full Backup
         2                       Payroll Dataset_vise-f6_08... 8/4/2015
11:23:17 AM
```

3. 既存のバックアップからクローニング処理を開始し、クローニングされたボリュームをエクスポートする NFS エクスポートの IP アドレスを指定します。

   この例では、 NFSExportIPs のアドレスを 10.232.206.169 と指定してバックアップをクローニングし

ています。

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

NFSExportIPs を指定しない場合、デフォルトでクローンターゲットホストにエクスポートされます。

4. Get-SmCloneReport コマンドレットを使用してクローニングジョブの詳細を表示し、バックアップが正常にクローニングされたことを確認します。

   クローン ID 、開始日時、終了日時などの詳細を確認できます。

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

SAP HANA データベースのクローニング処理を監視する

Jobs ページを使用して、 SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

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

クローンをスプリットします。

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

- このタスクについて *
- 中間のクローンに対してクローンスプリット処理を実行することはできません。

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

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

- クローンをスプリットすると、クローンのバックアップコピーとクローンジョブが削除されます。
- クローンスプリット処理の制限事項については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。

- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。
- 手順 *

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

オプション	説明
データベースアプリケーション用	[表示] リストから [*Database] を選択します。
ファイルシステムの場合	[表示] リストから [* パス *] を選択します。

3. リストから適切なリソースを選択します。

   リソースのトポロジページが表示されます。

4. [コピーの管理] ビューで、クローン作成されたリソース（データベースや LUN など）を選択し、 [*] をクリックします  *
5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、 * Start * をクリックします。
6. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。

   SMCore サービスが再起動すると、クローンスプリット処理が応答しなくなります。Stop-SmJob コマンドレットを実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

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

   例：

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

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

- 詳細はこちら *

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

SnapCenter のアップグレード後に、 SAP HANA データベースのクローンを削除またはスプリットします

SnapCenter 4.3 にアップグレードすると、クローンは表示されなくなります。クローン

を削除するか、クローンが作成されたリソースのトポロジページからクローンをスプリットします。

- このタスクについて *

非表示クローンのストレージフットプリントを確認するには、「 Get-SmClone-ListStorageFootprint 」コマンドを実行します

- 手順 *

1. remove-smbackup コマンドレットを使用して、クローニングしたリソースのバックアップを削除します。
2. remove-smresourcegroup コマンドレットを使用して、クローニングされたリソースのリソースグループを削除します。
3. remove-smprotectresource コマンドレットを使用して、クローニングされたリソースの保護を解除します。
4. [* リソース] ページから親リソースを選択します。

   リソースのトポロジページが表示されます。

5. [コピーの管理] ビューで ' プライマリ・ストレージ・システムまたはセカンダリ（ミラーまたはレプリケートされた）ストレージ・システムからクローンを選択します
6. クローンを選択し、をクリックします  クローンを削除するには、をクリックします  をクリックしてクローンをスプリットします。
7. [OK] 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