SnapCenter を使用した SAP HANA のバックアップとリカバリ

NetApp Solutions SAP

NetApp
March 11, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions-sap/backup/saphana-br-scs-overview.html on March 11, 2024. Always check docs.netapp.com for the latest.

目次

SnapCenter を使用した SAP HANA のバックアップとリカバリ . . . 1
- TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』 . . . 1
- SnapCenter アーキテクチャ . . . 6
- SnapCenter SAP HANA Backup 解決策 の略 . . . 7
- SnapCenter の概念とベストプラクティス . . . 11
- このレポートで使用するラボのセットアップ . . . 30
- SnapCenter 構成 . . . 32
- SnapCenter の初期設定 . . . 33
- SAP HANA データベースのバックアップ用の SnapCenter リソース固有の構成 . . . 46
- データボリューム以外のバックアップ用の SnapCenter リソース固有の設定 . . . 65
- データベースのバックアップ . . . 70
- ブロック整合性チェック . . . 79
- リストアとリカバリ . . . 83
- 高度な設定と調整 . . . 138
- 追加情報およびバージョン履歴の参照先 . . . 146

SnapCenter を使用した SAP HANA のバックアップとリカバリ

TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』

ネットアップ Nils Bauer

今日の企業には、 SAP アプリケーションを中断なく継続的に利用できることが求められています。データ量が増え続け、システムバックアップなどの日常的な保守作業が必要になった場合に、一貫したパフォーマンスレベルが期待されます。SAP データベースのバックアップは重要な作業であり、本番用 SAP システムのパフォーマンスに大きく影響する可能性があります。

バックアップウィンドウは短くなっている一方で、バックアップするデータの量は増加しています。そのため、ビジネスプロセスへの影響を最小限に抑えながらバックアップを実行できるタイミングを見つけ出すのは困難です。本番環境と非本番環境の SAP システムのダウンタイムは、データの損失とビジネスコストを削減するために最小化する必要があるため、 SAP システムのリストアとリカバリに要する時間が重要になります。

SAP のバックアップとリカバリに関する課題を以下にまとめます。

- * 本番用 SAP システムのパフォーマンスへの影響。 * 通常、従来のコピーベースのバックアップは、データベースサーバ、ストレージシステム、ストレージネットワークに大きな負荷がかかるため、本番用 SAP システムのパフォーマンスが大幅に低下します。
- * バックアップ・ウィンドウの短縮 * 従来のバックアップは 'SAP システムでの対話またはバッチ・アクティビティが少ない場合にのみ可能ですSAP システムが 24 時間稼働していると、バックアップのスケジュール設定がさらに難しくなります。
- * データの急増。 * データの急増とバックアップ・ウィンドウの短縮には、バックアップ・インフラへの継続的な投資が必要です。つまり、より多くのテープドライブを調達し、追加のバックアップディスクスペースを確保し、より高速なバックアップネットワークを構築する必要があります。また、これらのテープ資産の格納と管理にかかる継続的なコストについても説明する必要があります。こうした問題には差分バックアップで対処することもできますが、リストアプロセスが煩雑で非常に時間がかかるうえ、複雑なため検証も難しくなります。このようなシステムでは、通常、 Recovery Time Objective （ RTO ；目標復旧時間）と Recovery Point Objective （ RPO ；目標復旧時点）が長くなり、ビジネスには受け入れられません。
- * ダウンタイムのコスト増加。 * SAP システムの計画外のダウンタイムは、通常、ビジネスの財務に影響を及ぼします。計画外停止の大部分は、 SAP システムのリストアとリカバリの要件に応じて消費されます。そのため、必要な RTO は、バックアップとリカバリのアーキテクチャの設計を決定します。
- * SAP アップグレード・プロジェクトのバックアップ / リカバリ時間。 * SAP アップグレードのプロジェクト計画には、 SAP データベースのバックアップが 3 つ以上含まれています。これらのバックアップにより、アップグレードプロセスにかかる時間が大幅に短縮されます。通常、続行するかどうかは、以前に作成したバックアップからデータベースをリストアおよびリカバリするのに要する時間に基づいて判断します。システムを以前の状態にリストアするだけでなく、アップグレード中に発生する可能性のある問題を迅速にリストアすることで解決できます。

NetApp 解決策の略

ネットアップの Snapshot テクノロジを使用すれば、データベースのバックアップを数分で作成できま

す。Snapshot コピーではストレージプラットフォーム上の物理データブロックは移動されないため、Snapshot コピーの作成に要する時間はデータベースのサイズに左右されません。また、 Snapshot コピーの作成時やアクティブファイルシステムのデータが変更されたときにデータブロックの移動やコピーが NetApp Snapshot テクノロジによって行われないため、稼働中の SAP システムのパフォーマンスに影響がありません。そのため、 Snapshot コピーの作成スケジュールは、対話形式またはバッチでのアクティビティのピーク期間を気にせずに作成できます。SAP とネットアップのお客様は、通常、複数のオンライン Snapshot バックアップを 1 日に行うようにスケジュールを設定します。たとえば、一般に 4 時間ごとなどです。作成された Snapshot バックアップをプライマリストレージシステムに 3~5 日間保持しています。

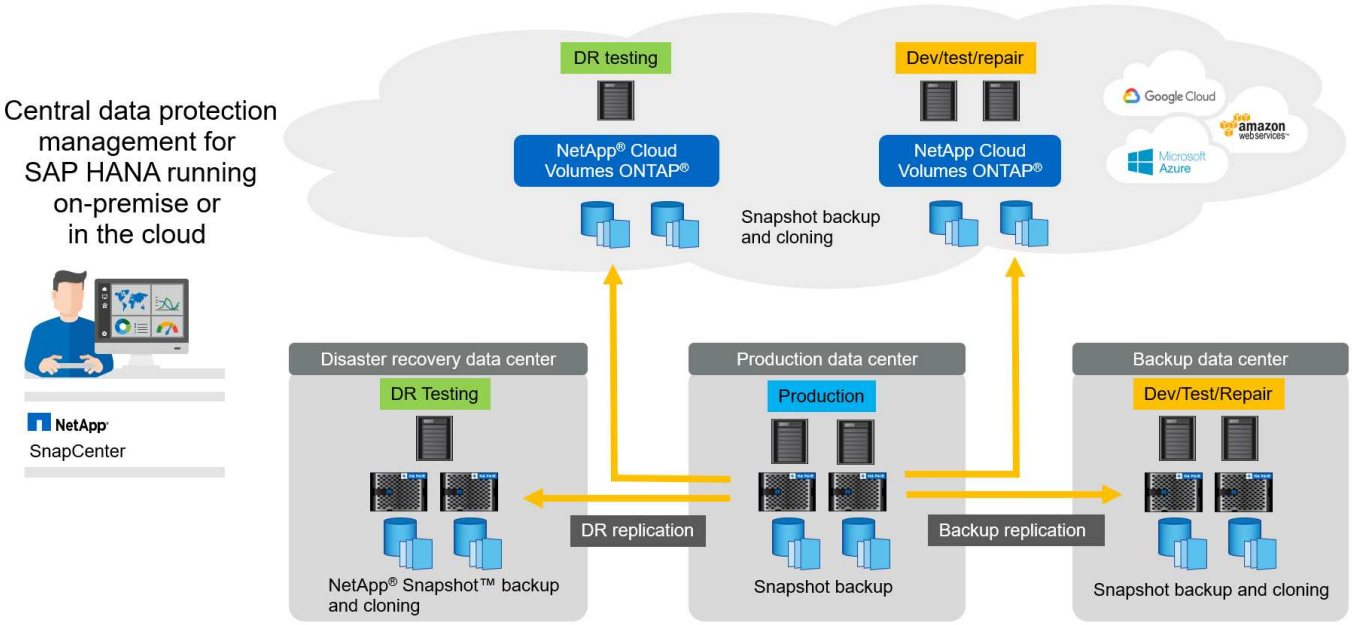
Snapshot コピーは、リストア処理とリカバリ処理にも大きなメリットがあります。NetApp SnapRestore データリカバリソフトウェアを使用すると、データベース全体または利用可能な Snapshot コピーに基づいて、データベースの一部を任意の時点にリストアできます。このようなリストアプロセスは、データベースのサイズに関係なく数分で完了します。オンラインの Snapshot バックアップは 1 日に数回作成されるため、従来のバックアップ方式に比べて、リカバリプロセスに要する時間が大幅に短縮されます。24 時間以内ではなく数時間前の Snapshot コピーを使用してリストアできるため、適用するトランザクションログの数を少なくする必要があります。そのため、従来のシングルサイクルのテープバックアップでは数時間かかるのに対し、RTO が数分に短縮されます。

Snapshot コピーバックアップは、アクティブなオンラインデータと同じディスクシステムに格納されます。セカンダリストレージへのバックアップに代わる手段としてではなく、補助的な用途で使用することを推奨します。リストアとリカバリのほとんどはプライマリストレージシステムで SnapRestore を使用して実行されます。セカンダリストレージからのリストアが必要になるのは、 Snapshot コピーが格納されているプライマリストレージシステムが損傷している場合のみです。セカンダリストレージは、たとえば月末のバックアップのように、 Snapshot コピーからは提供されなくなったバックアップをリストアする必要がある場合にも使用できます。

セカンダリストレージへのバックアップは、プライマリストレージに作成された Snapshot コピーがベースとなります。そのため、プライマリストレージシステムから直接データが読み取られ、 SAP データベースサーバに負荷は生成されません。プライマリストレージはセカンダリストレージと直接通信し、 NetApp SnapVault のディスクツーディスクバックアップを使用してバックアップデータをデスティネーションに送信します。

SnapVault には、従来のバックアップに比べて大きな利点があります。最初のデータ転送でソースからデスティネーションにすべてのデータが転送され、以降のバックアップでは変更されたブロックだけがセカンダリストレージにコピーされます。そのため、プライマリストレージシステムへの負荷およびフルバックアップに要する時間が大幅に削減されます。SnapVault では変更されたブロックだけがデスティネーションに格納されるため、データベースのフルバックアップに必要なディスクスペースも少なくて済みます。

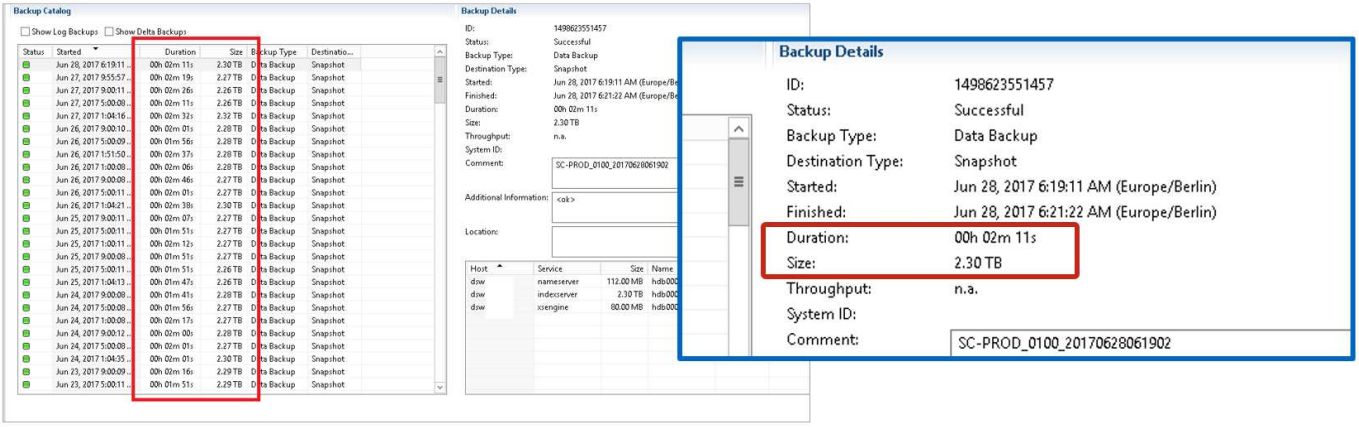
解決策 は、ハイブリッドクラウド運用モデルにシームレスに拡張することもできます。ディザスタリカバリやオフサイトのバックアップを目的としたデータレプリケーションは、オンプレミスの NetApp ONTAP システムから、クラウドで実行されている Cloud Volumes ONTAP インスタンスに実施できます。SnapCenter は、 SAP HANA システムをオンプレミスで実行する場合でも、クラウドで実行する場合でも、データ保護とデータレプリケーションを一元的に管理するツールとして使用できます。次の図に、バックアップ解決策 の概要を示します。



Snapshot バックアップの実行時間

次のスクリーンショットは、ネットアップストレージ上で SAP HANA を実行しているお客様の HANA Studio を示しています。Snapshot コピーを使用して HANA データベースをバックアップしている。この図では、Snapshot バックアップテクノロジを使用して、 HANA データベース（約 2.3TB のサイズ）を 2 分 11 秒でバックアップしています。

全体的なバックアップワークフローランタイムの最大の部分は、 HANA のバックアップセーブポイント処理を実行するために必要な時間です。この手順は、 HANA データベースの負荷によって異なります。ストレージ Snapshot バックアップ自体は、数秒で完了します。



目標復旧時間の比較

このセクションでは、ファイルベースとストレージベースの Snapshot バックアップの RTO 比較を示します。RTO は、データベースのリストアに必要な時間と、データベースの起動およびリカバリに必要な時間の合計によって定義されます。

データベースのリストアに必要な時間

ファイルベースのバックアップでは、リストア時間はデータベースのサイズとバックアップインフラによって異なり、リストア速度は 1 秒あたりのメガバイト数で定義されます。たとえば、インフラで 250MBps の高速なリストア処理がサポートされている場合、データベースのサイズが 1TB にリストアされるまでに約 1 時間 10 分かかります。

ストレージ Snapshot コピーバックアップでは、リストア時間はデータベースのサイズに左右されず、プライマリストレージからリストアを実行できる数秒の範囲になります。セカンダリストレージからのリストアが必要になるのは、プライマリストレージが使用できなくなったときに災害が発生した場合だけです。

データベースの起動に必要な時間

データベースの開始時間は、行および列ストアのサイズによって異なります。列ストアの場合、開始時間は、データベースの起動時にプリロードされるデータの量によっても異なります。次の例では、開始時間は 30 分であると想定しています。開始時刻は、ファイルベースのリストアとリカバリ、および Snapshot に基づくリストアとリカバリで同じです。

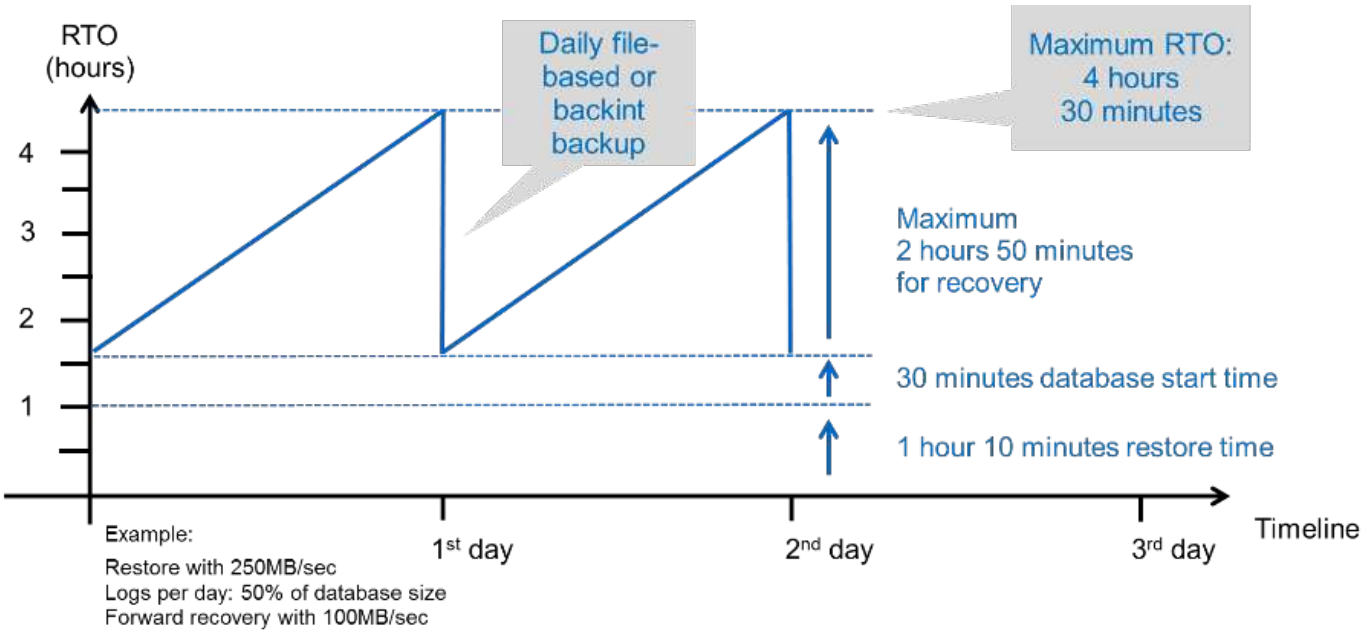
データベースのリカバリに要する時間

リカバリ時間は、リストア後に適用する必要があるログの数によって異なります。この数は、データバックアップを実行する頻度によって決まります。

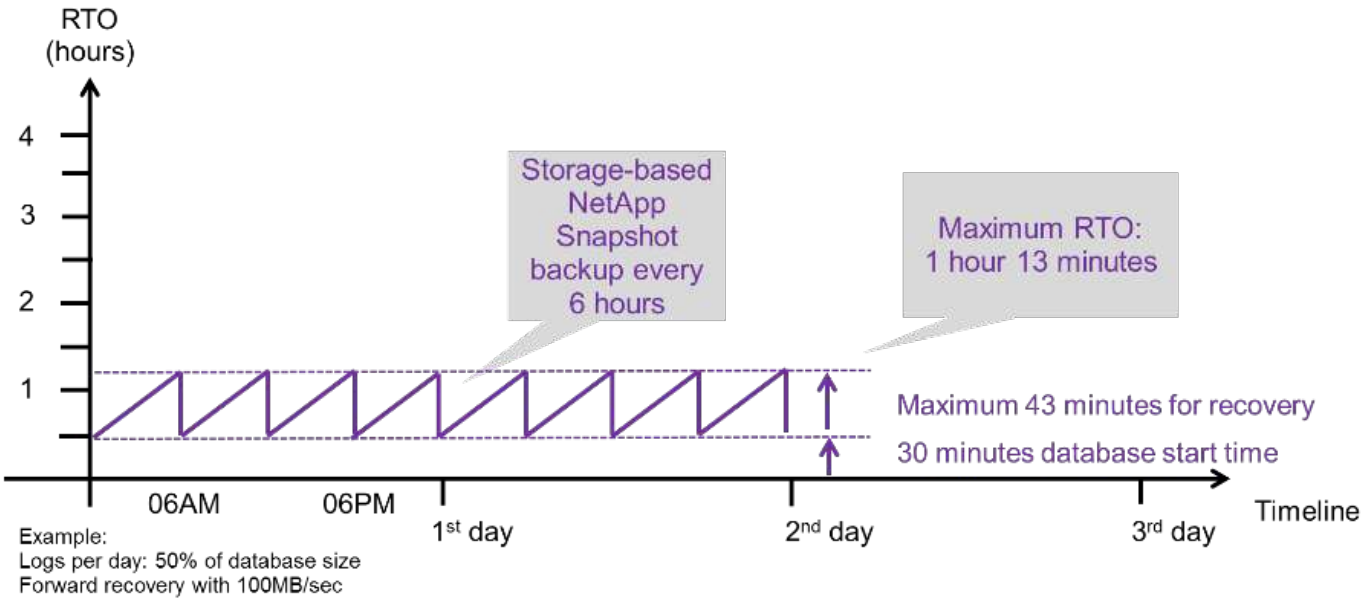
ファイルベースのデータバックアップでは、通常、バックアップスケジュールは 1 日に 1 回となります。バックアップによって本番環境のパフォーマンスが低下するため、通常はバックアップ頻度を高くすることはできません。したがって、最悪の場合は、フォワードリカバリ時に 1 日中に書き込まれたすべてのログを適用する必要があります。

ストレージ Snapshot コピーのデータバックアップは、通常、 SAP HANA データベースのパフォーマンスに影響しないため、頻繁にスケジュールされます。たとえば、 Snapshot コピーのバックアップを 6 時間ごとに実行するようにスケジュールした場合、最大でファイルベースのバックアップのリカバリ時間の 4 分の 1 （ 6 時間 /24 時間 = ¼ ）というリカバリ時間がかかります。

次の図に、ファイルベースのデータバックアップを使用する場合の 1TB データベースの RTO の例を示します。この例では、バックアップが 1 日に 1 回作成されます。RTO は、リストアとリカバリの実行タイミングによって異なります。バックアップの作成直後にリストアとリカバリを実行した場合の RTO は、主にリストア時間に基づきます。この例では、 1 時間 10 分です。リカバリ時間は、次のバックアップが作成される直前にリストアとリカバリが実行され、最大 RTO は 4 時間 30 分になりました。

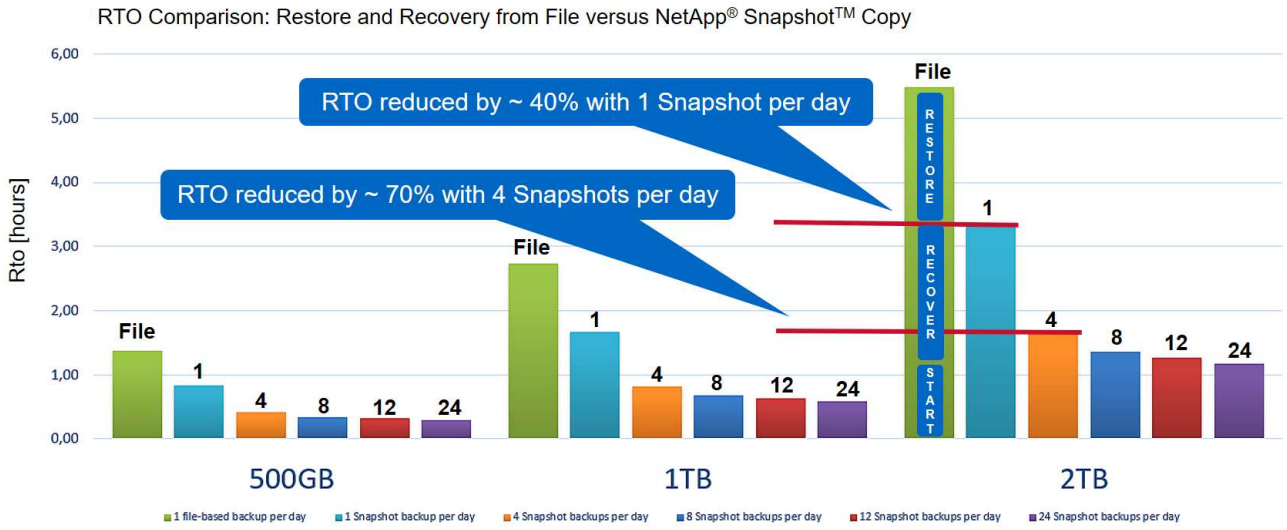


次の図に、 Snapshot バックアップの使用時の 1TB データベースの RTO の例を示します。ストレージベースの Snapshot バックアップでは、データベースのサイズに関係なく数秒でリストアが完了するため、 RTO はデータベースの開始時間と転送リカバリ時間にのみ左右されます。また、リストアとリカバリの実行タイミングによってもフォワードリカバリの時間が長くなりますが、バックアップの頻度が高い（この例では 6 時間ごと）ため、最大で 43 分までリカバリ時間が短縮されます。この例では、最大 RTO は 1 時間 13 分です。



次の図に、データベースサイズや Snapshot バックアップの頻度に応じた、ファイルベースとストレージベースの Snapshot バックアップの RTO 比較を示します。緑のバーは、ファイルベースのバックアップを示しています。その他のバーには、バックアップ頻度が異なる Snapshot コピーのバックアップが表示されます。

1 日に 1 回の Snapshot コピーでデータをバックアップする RTO は、ファイルベースのデータバックアップに比べてすでに 40% 短縮されています。1 日に 4 つの Snapshot バックアップを作成すると、削減率は 70% になります。また、 Snapshot のバックアップ頻度を 1 日あたり 4~6 個の Snapshot バックアップに増やすと、この図ではフラットな状態になります。したがって、お客様は通常、 1 日に 4~6 個の Snapshot バックアップを作成します。



Assumptions: Restore from file with 250MB/sec; database start with 400MB/s; log files per day: 50% of database size; forward recovery with 250MB/sec

このグラフには、 HANA サーバの RAM サイズが表示されます。メモリ内のデータベースサイズは、サーバの RAM サイズの半分になるように計算されます。

リストアとリカバリの所要時間は、次の前提に基づいて計算します。データベースは 250MBps でリストアできます。1 日のログファイルの数は、データベースサイズの 50% です。たとえば、 1TB のデータベースでは、 1 日 500MB のログファイルが作成されます。リカバリは 100Mbps で実行できます。

SnapCenter アーキテクチャ

SnapCenter は、アプリケーションと整合性のあるデータ保護を実現する拡張性に優れたユニファイドプラットフォームです。SnapCenter では一元的な管理と監視が可能ですが、一方で、アプリケーション固有のバックアップ、リストア、クローニングのジョブの管理を各ユーザに委譲することができます。SnapCenter を使用すれば、データベース管理者やストレージ管理者は、さまざまなアプリケーションやデータベースのバックアップ、リストア、クローニングの処理を 1 つのツールで管理できます。

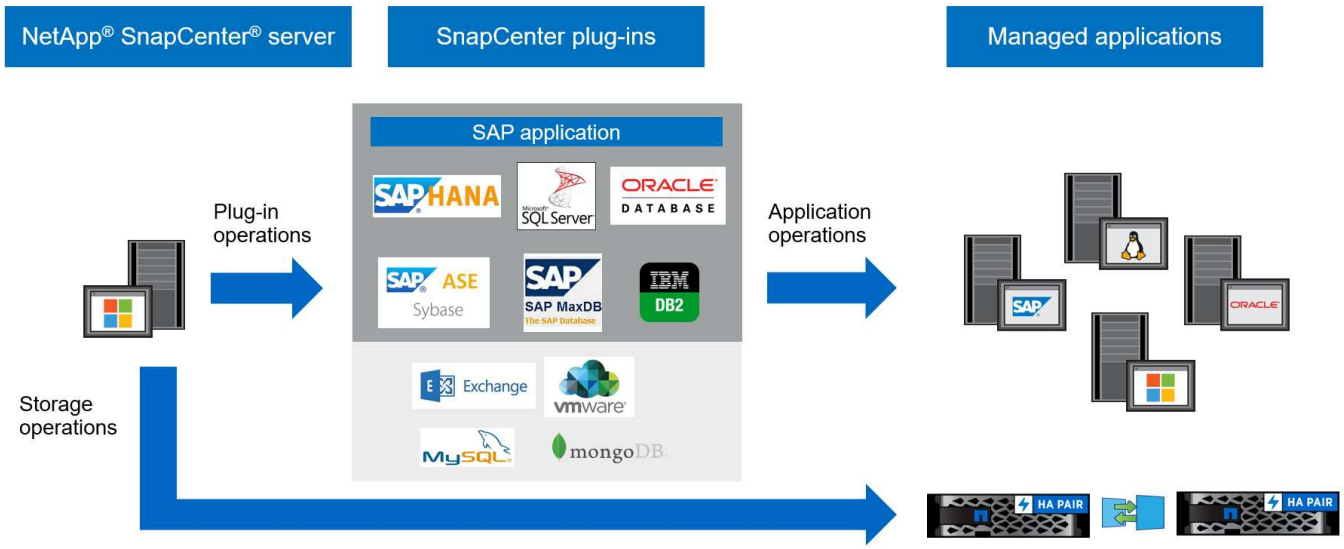
SnapCenter は、ネットアップのデータファブリック内のすべてのエンドポイントのデータを管理します。SnapCenter を使用して、オンプレミス環境間、オンプレミス環境とクラウド間、およびプライベートクラウド、ハイブリッドクラウド、パブリッククラウド間でデータをレプリケートできます。

SnapCenter コンポーネント

SnapCenter には、 SnapCenter サーバ、 Windows 用 SnapCenter プラグインパッケージ、および Linux 用 SnapCenter プラグインパッケージが含まれています。各パッケージには、さまざまなアプリケーションやインフラコンポーネント用の SnapCenter へのプラグインが含まれています。

SnapCenter のカスタムプラグインを使用すると、独自のプラグインを作成し、同じ SnapCenter インターフェイスを使用してアプリケーションを保護できます。

次の図は、 SnapCenter のコンポーネントを示しています。



SnapCenter SAP HANA Backup 解決策 の略

このセクションでは、この解決策 で使用されているコンポーネント、サポートされている SAP HANA のリリースと構成、および SnapCenter 4.6 の拡張機能について説明します。

解決策コンポーネント

SnapCenter Backup 解決策 for SAP HANA には、次の領域があります。

- ストレージベースの Snapshot コピーを使用した SAP HANA データのバックアップ：
  - バックアップのスケジュール設定
  - 保持管理
  - 不要な SAP HANA バックアップカタログの削除
- 非データ・ボリューム（例： /hana/shared ）バックアップとストレージ・ベースの Snapshot コピー：
  - バックアップのスケジュール設定
  - 保持管理
- オフサイトのバックアップまたはディザスタリカバリロケーションへのレプリケーション：
  - SAP HANA データの Snapshot バックアップ
  - データボリューム以外のボリューム
  - オフサイトのバックアップストレージに保持管理を設定
  - 不要な SAP HANA バックアップカタログの削除
- ファイルベースのバックアップを使用したデータベースブロックの整合性チェック：
  - バックアップのスケジュール設定
  - 保持管理
  - 不要な SAP HANA バックアップカタログの削除

- HANA データベースログバックアップの保持管理：
  - データバックアップの保持に基づく保持管理
  - 不要な SAP HANA バックアップカタログの削除
- HANA データベースの自動検出
- リストアとリカバリの自動化
- SAP HANA マルチテナントデータベースコンテナ（ MDC ）システムを使用したシングルテナントのリストア処理

データベースデータファイルのバックアップは、 SnapCenter と SAP HANA 向けプラグインを組み合わせて実行されます。このプラグインは、 SAP HANA データベースのバックアップ保存ポイントをトリガーして、プライマリストレージシステムで作成された Snapshot コピーが SAP HANA データベースの整合性のあるイメージに基づいて作成されるようにします。

SnapCenter では、 SnapVault または NetApp SnapMirror を使用して、整合性のあるデータベースイメージをオフサイトのバックアップまたはディザスタリカバリロケーションにレプリケートできます。フィーチャー（ Feature ）：通常は、プライマリストレージとオフサイトのバックアップストレージに異なる保持ポリシーが定義されます。SnapCenter はプライマリストレージでの保持を処理し、 ONTAP はオフサイトのバックアップストレージでの保持を処理します。

SnapCenter では、 SAP HANA 関連のすべてのリソースを完全にバックアップするために、ストレージベースの Snapshot コピーを使用して SAP HANA プラグインを使用し、データ以外のすべてのボリュームをバックアップすることもできます。非データ・ボリュームは、データベース・データ・バックアップとは別にスケジュール設定できるため、保持ポリシーや保護ポリシーを個別に設定することができます。

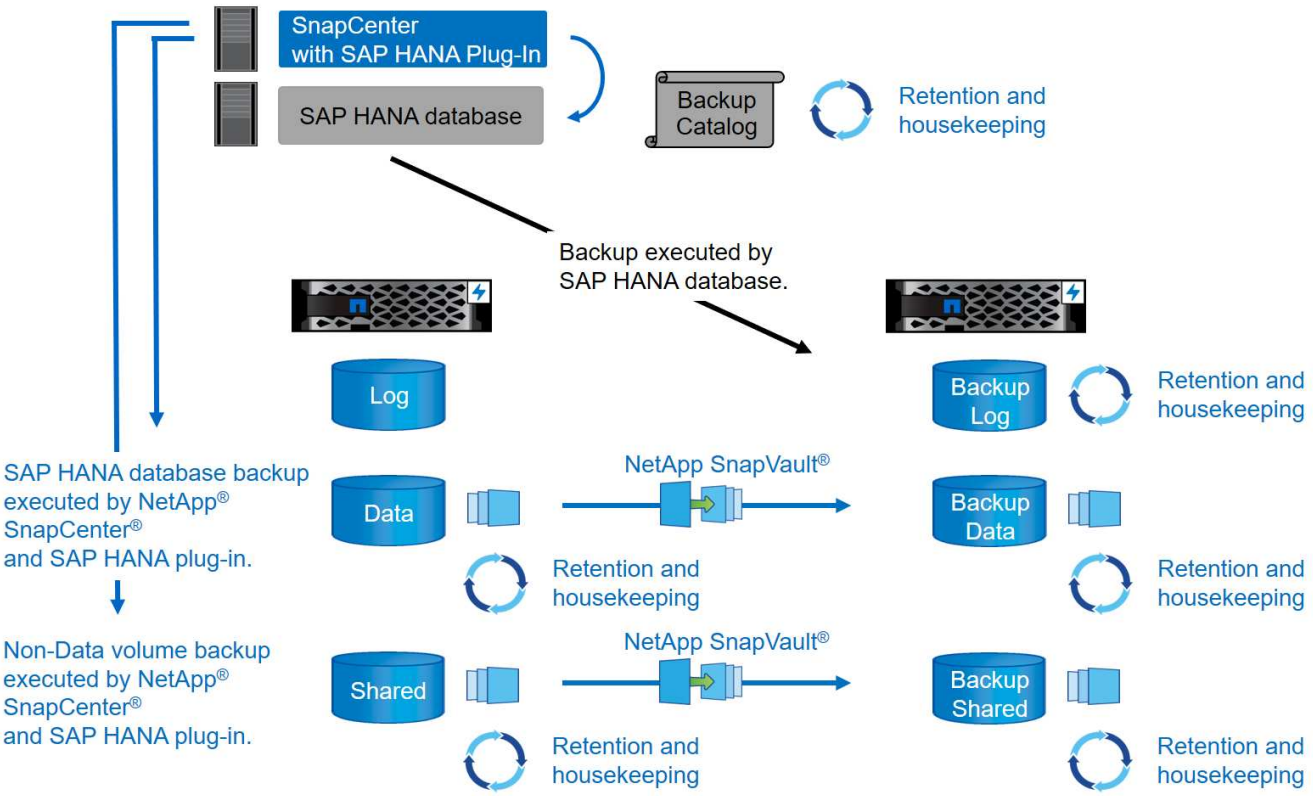
SAP HANA データベースは、ログバックアップを自動的に実行します。目標復旧時点に応じて、ログ・バックアップの保存場所に関するいくつかのオプションがあります。

- ログバックアップは、 NetApp MetroCluster ハイアベイラビリティ（ HA ）およびディザスタリカバリストレージソフトウェアを使用してデータを別の場所に同期的にミラーリングするストレージシステムに書き込まれます。
- ログバックアップのデスティネーションは、同じプライマリストレージシステムで設定し、 SnapMirror によって同期または非同期でセカンダリストレージにレプリケートできます。
- ログバックアップのデスティネーションは、 SnapVault を使用してデータベースバックアップをレプリケートする、同じオフサイトのバックアップストレージに設定できます。この構成では、オフサイトのバックアップストレージに、ログバックアップをオフサイトのバックアップストレージに書き込むことができるように、プライマリストレージと同様の可用性要件があります。

SAP では、ブロックの整合性チェックを実行するために、ストレージベースの Snapshot バックアップと週次ファイルベースのバックアップを組み合わせることを推奨しています。ブロック整合性チェックは、 SnapCenter 内から実行できます。設定可能な保持ポリシーに基づいて、 SnapCenter は、プライマリストレージでのデータファイルバックアップの削除、ログファイルバックアップ、および SAP HANA のバックアップカタログを管理します。

SnapCenter はプライマリストレージでの保持を処理し、 ONTAP はセカンダリバックアップの保持を管理します。

次の図に、データベースとログのバックアップ構成の概要を示します。この図では、ログバックアップがオフサイトのバックアップストレージの NFS マウントに書き込まれます。



SnapCenter では、データボリューム以外のボリュームのストレージベースの Snapshot バックアップを実行する際に、次のタスクを実行します。

1. データボリューム以外のストレージ Snapshot コピーの作成。
2. データボリュームの SnapVault 更新または SnapMirror 更新の実行（設定されている場合）。
3. 定義された保持ポリシーに基づいて、プライマリストレージのストレージ Snapshot コピーを削除します。

SAP HANA データベースのストレージベースの Snapshot バックアップを実行する場合、 SnapCenter は次のタスクを実行します。

1. SAP HANA バックアップ保存ポイントを作成して、永続性レイヤに整合性のあるイメージを作成する。
2. データボリュームのストレージ Snapshot コピーの作成。
3. SAP HANA バックアップカタログへのストレージ Snapshot バックアップの登録。
4. SAP HANA バックアップセーブポイントのリリース。
5. データボリュームの SnapVault 更新または SnapMirror 更新の実行（設定されている場合）。
6. 定義された保持ポリシーに基づいて、プライマリストレージのストレージ Snapshot コピーを削除します。
7. プライマリまたはオフサイトのバックアップストレージにバックアップが存在しなくなった場合は、 SAP HANA のバックアップカタログのエントリを削除します。
8. 保持ポリシーに基づいてバックアップが削除された場合、または手動で削除された場合、 SnapCenter は最も古いデータバックアップよりも古いログバックアップをすべて削除します。ログバックアップは、ファイルシステムと SAP HANA のバックアップカタログから削除されます。

サポートされている **SAP HANA** リリースと構成

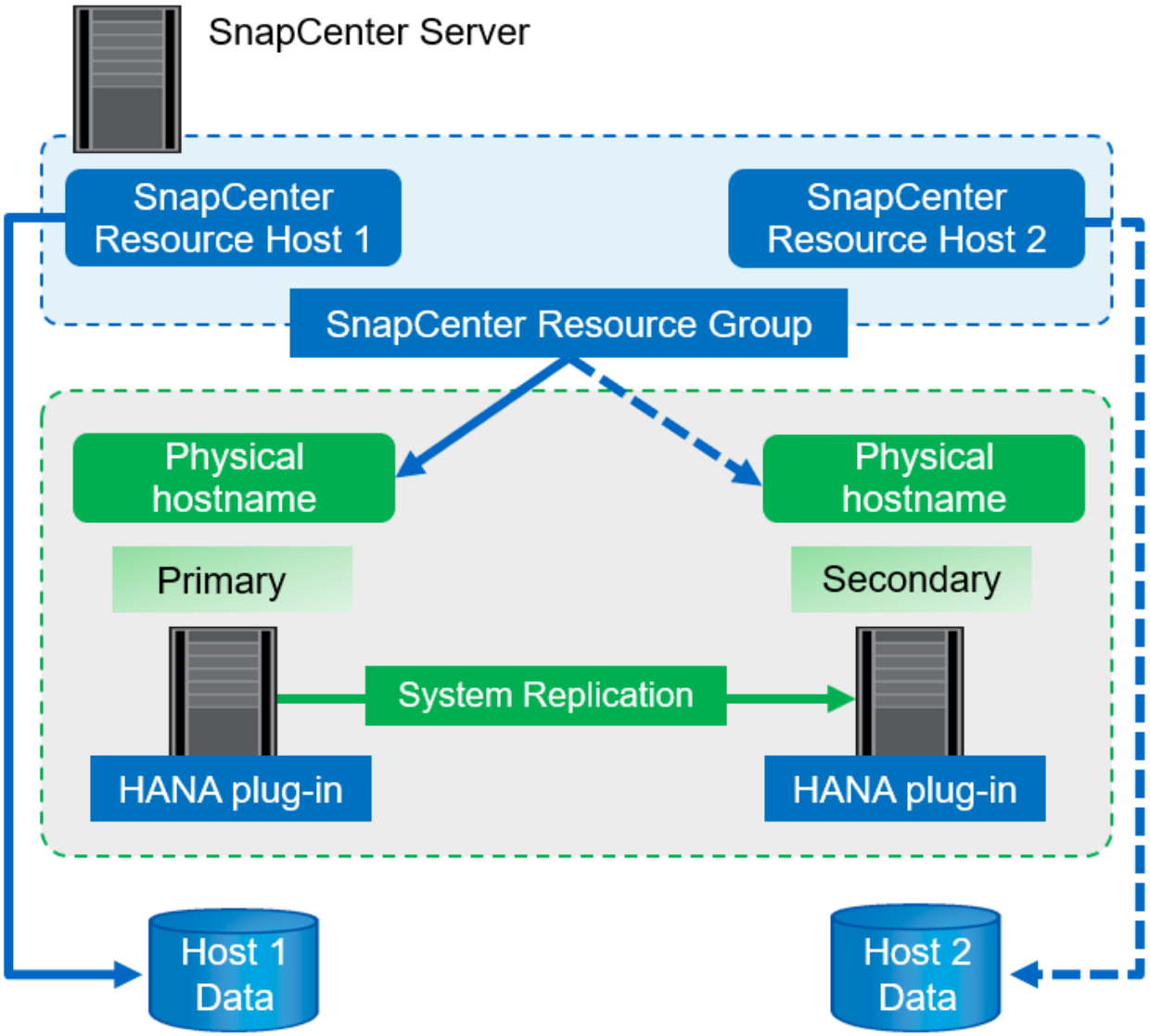
SnapCenter は、 NFS または FC 接続のネットアップストレージシステム（ AFF および FAS ）を使用した SAP HANA シングルホスト構成とマルチホスト構成、および NFS を使用した AWS 、 Azure 、 Google Cloud Platform 、 AWS FSX ONTAP で Cloud Volumes ONTAP を実行している SAP HANA システムをサポートしています。

SnapCenter は、次の SAP HANA アーキテクチャとリリースをサポートしています。

- SAP HANA の単一コンテナ： SAP HANA 1.0 SPS12
- SAP HANA マルチテナントデータベースコンテナ（ MDC ）のシングルテナント： SAP HANA 2.0 SPS3 以降
- SAP HANA マルチテナントデータベースコンテナ（ MDC ）の複数のテナント： SAP HANA 2.0 SPS4 以降

SnapCenter 4.6 の機能強化

バージョン 4.6 以降の SnapCenter では、 HANA システムレプリケーション関係で設定された HANA システムの自動検出がサポートされます。各ホストは、物理 IP アドレス（ホスト名）とストレージレイヤ上の個々のデータボリュームを使用して設定されます。2 つの SnapCenter リソースが 1 つのリソースグループに統合されている場合、 SnapCenter はプライマリまたはセカンダリのホストを自動的に識別し、必要なバックアップ処理を適宜実行します。SnapCenter で作成された Snapshot とファイルベースのバックアップの保持の管理は、両方のホストで実行されます。これにより、現在のセカンダリホストでも古いバックアップが削除されるようになります。次の図に概要を示します。SnapCenter の HANA システムレプリケーション対応 HANA システムの構成と運用の詳細概要 については、を参照してください "TR-4719 『 SAP HANA System Replication 、 Backup and Recovery with SnapCenter 』"。



SnapCenter の概念とベストプラクティス

このセクションでは、 SnapCenter の概念と、 SAP HANA のリソース構成と導入に関連するベストプラクティスについて説明します。

SAP HANA のリソース構成オプションと概念

SnapCenter では、 SAP HANA データベースのリソース構成を 2 つの異なるアプローチで実行できます。

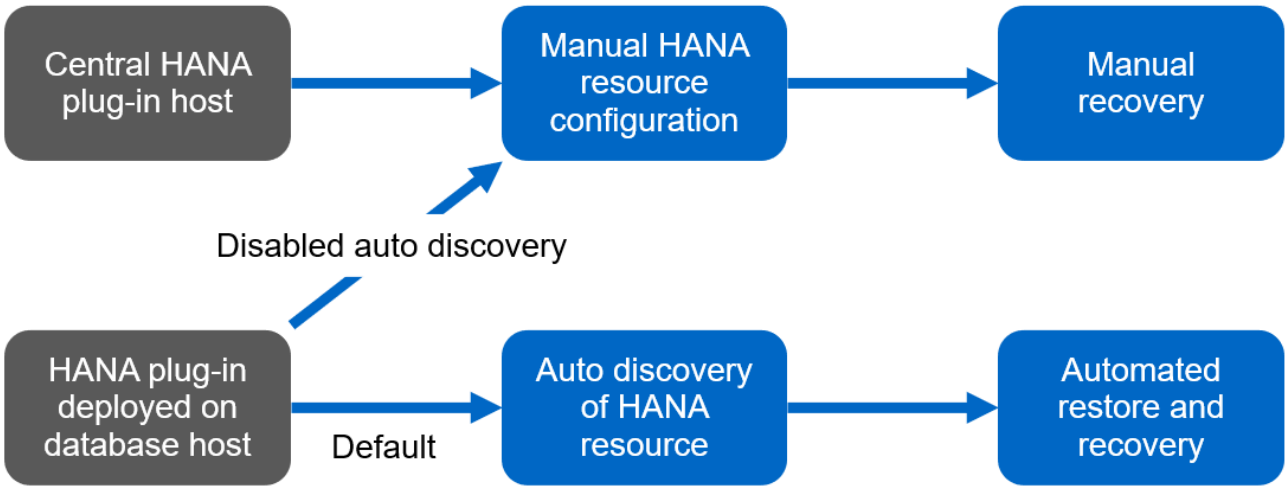
- * リソースを手動で構成。 * HANA のリソースとストレージの設置面積に関する情報は、手動で提供する必要があります。
- * HANA リソースの自動検出。 * 自動検出により、 SnapCenter での HANA データベースの設定が簡易化され、リストアとリカバリが自動化されます。

SnapCenter では、自動検出された HANA データベースのリソースのみがリストアとリカバリの自動化を有効にしていることを理解しておくことが重要です。SnapCenter で手動で設定した HANA データベースリソースは、 SnapCenter でリストア処理を実行したあとに手動でリカバリする必要があります。

一方、 SnapCenter による自動検出は、 HANA のすべてのアーキテクチャとインフラ構成でサポートされているわけではありません。そのため、 HANA 環境では、混在するアプローチが必要になる場合があります。一部の HANA システム（ HANA マルチホストシステム）では手動でリソース設定を行う必要があり、それ以外はすべて自動検出を使用して設定できます。

リストアとリカバリの自動検出は、データベースホストで OS コマンドを実行できるかどうかによって異なります。たとえば、ファイルシステムやストレージの設置面積の検出、アンマウント、マウント、 LUN 検出などの処理が該当します。これらの処理は、 HANA プラグインと自動的に導入される SnapCenter Linux プラグインを使用して実行されます。そのため、自動検出とリストアとリカバリを可能にするためには、データベースホストに HANA プラグインを導入する必要があります。データベースホストに HANA プラグインを導入したあとに、自動検出を無効にすることもできます。この場合、リソースは手動で設定されたリソースになります。

次の図は、依存関係をまとめたものです。HANA の導入オプションの詳細については、「 SAP HANA プラグインの導入オプション」を参照してください。



HANA と Linux のプラグインは、現在、インテルベースのシステムでのみ使用できます。HANA データベースを IBM Power Systems で実行している場合は、中央の HANA プラグインホストを使用する必要があります。

自動検出と自動リカバリのためにサポートされている **HANA** アーキテクチャ

SnapCenter では、ほとんどの HANA 構成で自動検出と自動リストア / リカバリがサポートされていますが、HANA の複数ホストシステムでは手動構成が必要です。

次の表に、自動検出がサポートされる HANA 構成を示します。

HANA プラグインのインストール場所：	**HANA** のアーキテクチャ	**HANA** システム構成	インフラ
HANA データベースホスト	シングルホスト	• HANA の単一コンテナ • シングルテナントまたは複数テナントの SAP HANA マルチテナントデータベースコンテナ（ MDC • HANA システムレプリケーション	• NFS のベアメタル • Linux の論理ボリュームマネージャ（ LVM ）の有無に関係なく、 XFS と FC を使用するベアメタル • VMware ： OS を直接 NFS マウント

複数のテナントを持つ HANA MDC システムは自動検出がサポートされていますが、現在の SnapCenter リリースでの自動リストアとリカバリはサポートされていません。

HANA の手動リソース構成でサポートされている **HANA** アーキテクチャ

HANA のリソースの手動構成は、すべての HANA アーキテクチャでサポートされていますが、 HANA の中央プラグインホストが必要です。中央のプラグインホストには、 SnapCenter サーバ自体、または独立した Linux または Windows ホストを使用できます。

HANA プラグインが HANA データベースホストに導入されている場合、リソースはデフォルトで自動検出されます。自動検出を個々のホストに対して無効にして、プラグインを展開できます。たとえば、アクティブな HANA システムレプリケーションが有効になっているデータベースホストでは、自動検出がサポートされていない SnapCenter リリース 4.6 では、自動検出を無効にできます。詳細については、を参照してください ""HANA プラグインホストで自動検出を無効にします。 ""

次の表に、 HANA の手動リソース構成でサポートされる HANA 構成を示します。

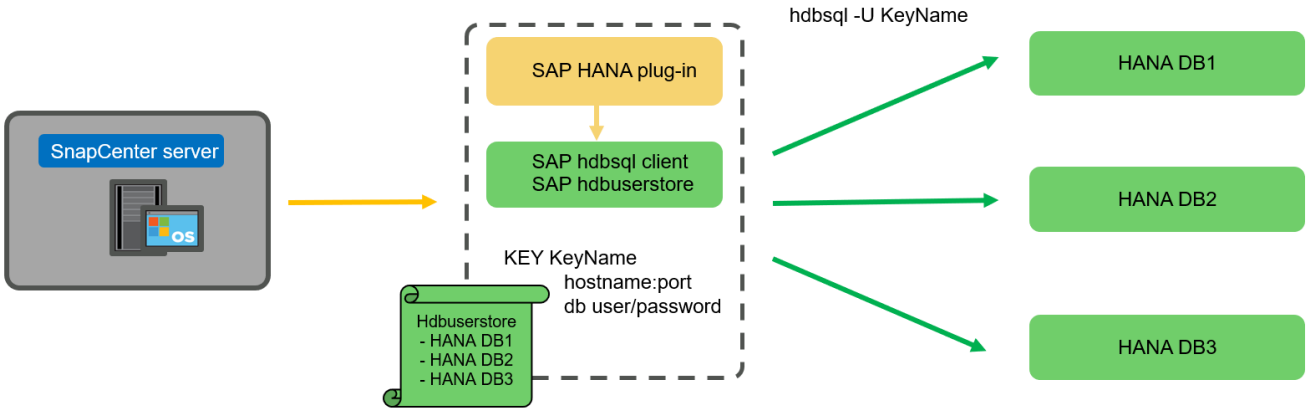
HANA プラグインのインストール場所：	**HANA** のアーキテクチャ	**HANA** システム構成	インフラ
中央プラグインホスト（ SnapCenter サーバまたは個別の Linux ホスト）	単一または複数のホスト	• HANA の単一コンテナ • シングルテナントまたはマルチテナントの HANA MDC • HANA システムレプリケーション	• NFS のベアメタル • Linux LVM の有無に関係なく、 XFS と FC を使用するベアメタル • VMware ： OS を直接 NFS マウント

SAP HANA プラグインの導入オプション

次の図は、 SnapCenter サーバと SAP HANA データベースの論理ビューと通信を示しています。

SnapCenter サーバは、 SAP HANA プラグインを介して SAP HANA データベースと通信します。SAP HANA

プラグインは、 SAP HANA hdbsql クライアントソフトウェアを使用して、 SAP HANA データベースに対して SQL コマンドを実行します。SAP HANA の hdbuserstore は、 SAP HANA データベースにアクセスするためのユーザクレデンシャル、ホスト名、ポート情報を提供するために使用されます。



SAP HANA プラグインと SAP hdbsql クライアントソフトウェア（ hdbuserstore 設定ツールを含む）は、同じホストに一緒にインストールする必要があります。

ホストには、 SnapCenter サーバ自体、独立した中央プラグインホスト、または個々の SAP HANA データベースホストを使用できます。

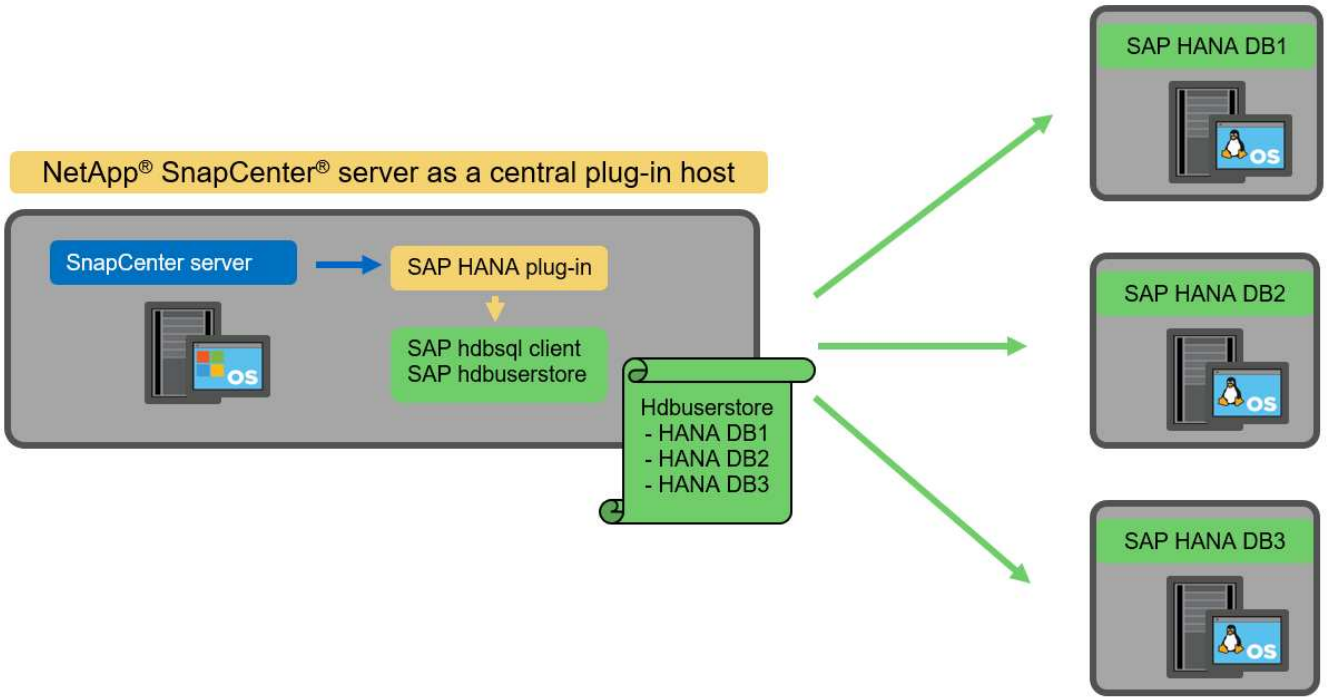
SnapCenter サーバの高可用性

SnapCenter は 2 ノード HA 構成でセットアップできます。このような構成では、アクティブ / パッシブモードでロードバランサ（ F5 など）を使用し、アクティブ SnapCenter ホストを指す仮想 IP アドレスを使用します。SnapCenter リポジトリ（ MySQL データベース）は、 SnapCenter データが常に同期されるように、 2 つのホスト間で SnapCenter によってレプリケートされます。

HANA プラグインが SnapCenter サーバにインストールされている場合、 SnapCenter サーバ HA はサポートされません。HA 構成で SnapCenter をセットアップする場合は、 SnapCenter サーバに HANA プラグインをインストールしないでください。SnapCenter HA の詳細については、こちらを参照してください "ネットアップのナレッジベースのページ"。

SnapCenter サーバを中央の **HANA** プラグインホストとして使用

次の図に、 SnapCenter サーバを中央プラグインホストとして使用する場合の設定を示します。SAP HANA プラグインと SAP hdbsql クライアントソフトウェアは、 SnapCenter サーバにインストールされています。



HANA プラグインは、ネットワーク経由で hdbclient を使用して管理対象 HANA データベースと通信できるため、個々の HANA データベースホストに SnapCenter コンポーネントをインストールする必要はありません。SnapCenter では、管理対象データベースに対してすべてのユーザストアキーが設定された中央の HANA プラグインホストを使用して、 HANA データベースを保護できます。

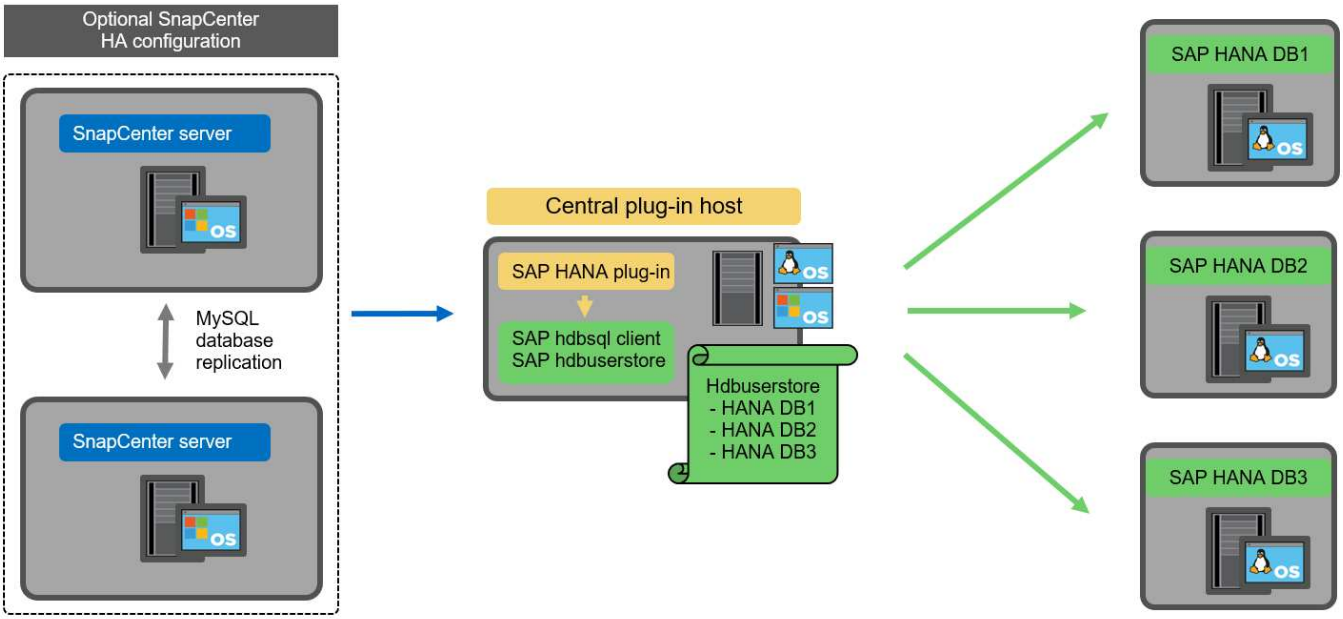
一方、自動検出のワークフロー自動化の強化、リストアとリカバリの自動化、 SAP システムの更新処理を行う際には、データベースホストに SnapCenter コンポーネントをインストールする必要があります。中央の HANA プラグインホストを使用している場合、これらの機能は使用できません。

また、 HANA プラグインが SnapCenter サーバにインストールされている場合、インビルドの HA 機能を使用した SnapCenter サーバの高可用性は使用できません。SnapCenter サーバが VMware クラスタ内の VM で実行されている場合は、 VMware HA を使用して高可用性を実現できます。

ホストを中央の **HANA** プラグインホストとして分離

次の図は、独立した Linux ホストを中央のプラグインホストとして使用した場合の構成を示しています。この場合、 SAP HANA プラグインと SAP hdbsql クライアントソフトウェアが Linux ホストにインストールされています。

また、個別の中央プラグインホストを Windows ホストにすることもできます。

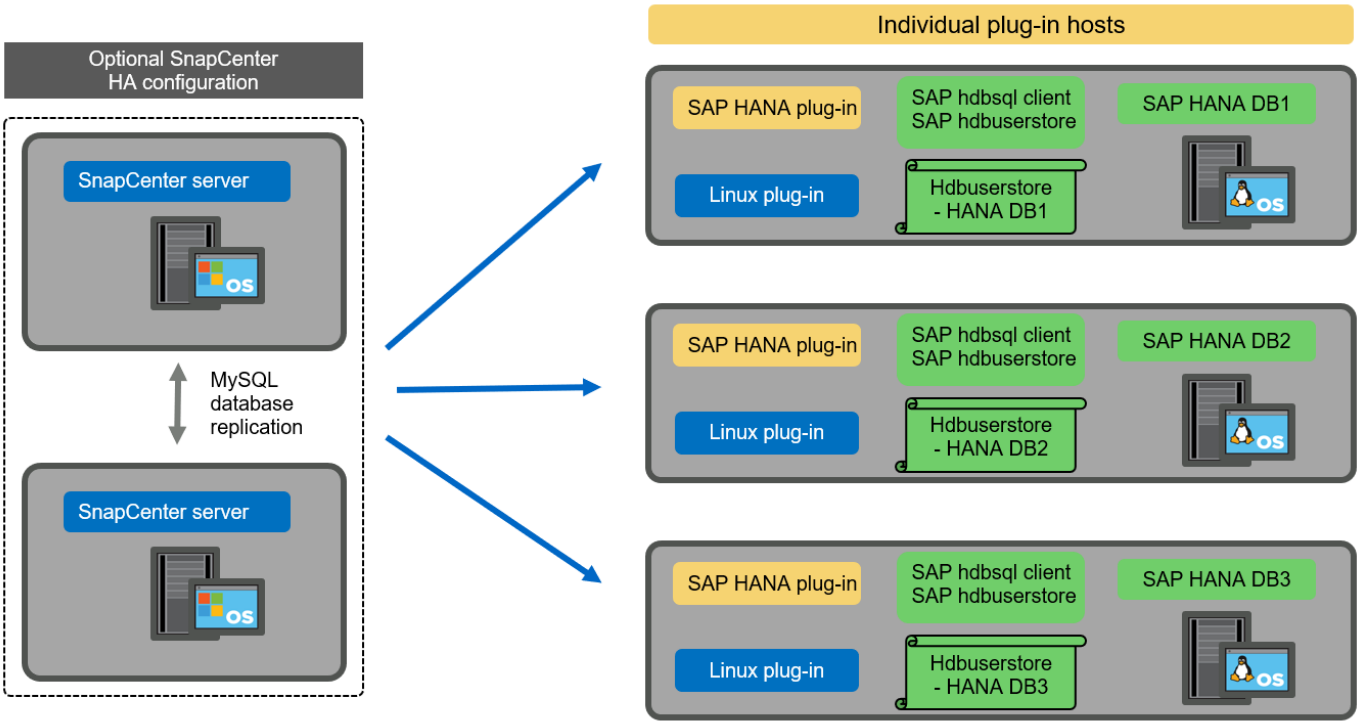


前のセクションで説明した機能の可用性に関する同様の制限は、別の中央プラグインホストにも適用されます。

ただし、この導入オプションでは、 SnapCenter サーバに組み込みの HA 機能を設定できます。また、 Linux クラスタ解決策 などを使用して、中央のプラグインホストも HA である必要があります。

HANA プラグインを個々の **HANA** データベースホストに導入

次の図は、 SAP HANA プラグインが各 SAP HANA データベースホストにインストールされた構成を示しています。



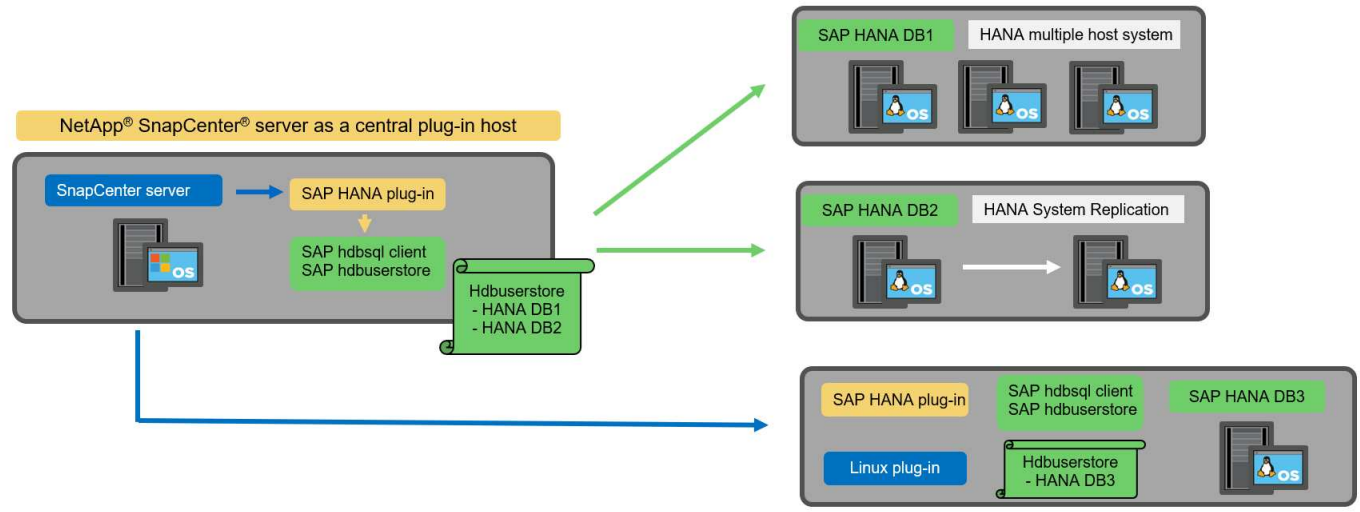
HANA プラグインを各 HANA データベースホストにインストールすると、自動検出やリストアとリカバリの自動化などのすべての機能を使用できるようになります。また、 SnapCenter サーバは HA 構成でセットアップできます。

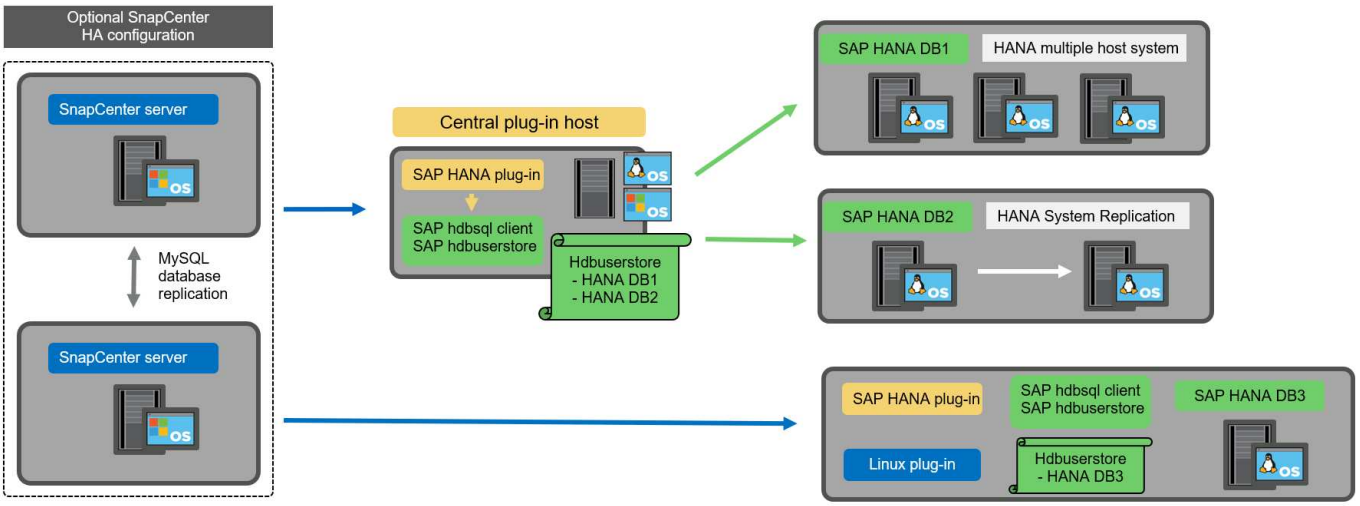
HANA 混在プラグイン環境をサポート

このセクションの冒頭で説明したように、マルチホストシステムなど、一部の HANA システム構成には、中央のプラグインホストが必要です。そのため、ほとんどの SnapCenter 構成では HANA プラグインを混在させる必要があります。

自動検出がサポートされているすべての HANA システム構成に対して、 HANA プラグインを HANA データベースホストに導入することを推奨します。マルチホスト構成などの他の HANA システムは、中央の HANA プラグインホストで管理する必要があります。

次の 2 つの図に、 SnapCenter サーバまたは別の Linux ホストを中央プラグインホストとして使用したプラグインの混在環境を示します。どちらの構成の場合も、オプションの HA 構成だけが違います。





まとめと推奨事項

一般に、使用可能なすべての SnapCenter HANA 機能を有効にし、ワークフローの自動化を強化するために、

各 SAP HANA ホストに HANA プラグインを導入することを推奨します。

HANA と Linux のプラグインは、現在、インテルベースのシステムでのみ使用できます。HANA データベースを IBM Power Systems で実行している場合は、中央の HANA プラグインホストを使用する必要があります。

HANA マルチホスト構成など、自動検出がサポートされない HANA 構成では、追加の中央 HANA プラグインホストを設定する必要があります。VMware HA を SnapCenter HA に利用できる場合は、中央のプラグインホストを SnapCenter サーバにすることができます。SnapCenter の組み込みの HA 機能を使用する場合は、別の Linux プラグインホストを使用します。

次の表は、さまざまな導入オプションをまとめたものです。

導入オプション	依存関係
SnapCenter サーバに中央 HANA プラグインホストプラグインがインストールされている	長所： * シングル HANA プラグイン、中央 HDB ユーザストア構成 * 個別の HANA データベースホストに SnapCenter ソフトウェアコンポーネントは不要 * すべての HANA アーキテクチャのサポート * 手動リソース構成 * 手動リカバリ * シングルテナントリストアのサポートなし * 中央プラグインホストでのプリスクリプトとポストスクリプトの手順の実行 * インビルド SnapCenter ハイアベイラビリティはサポートされていません * SID とテナント名の組み合わせは、すべての管理対象 HANA データベースで一意である * ログすべての管理対象 HANA データベースでバックアップ保持管理が有効 / 無効になっています
別々の Linux サーバまたは Windows サーバにインストールされた中央 HANA プラグインホストプラグイン	長所： * シングル HANA プラグイン、中央 HDB ユーザストア構成 * 個別の HANA データベースホストに SnapCenter ソフトウェアコンポーネントは不要 * すべての HANA アーキテクチャのサポート * インビルド SnapCenter 高可用性サポートされる構成： * 手動リソース構成 * 手動リカバリ * シングルテナントリストアのサポートなし * 中央プラグインホストで実行されるプリスクリプトとポストスクリプトの手順 * SID とテナント名の組み合わせは、すべての管理対象 HANA データベースで一意である * ログバックアップの保持管理が有効 / 無効になっているすべての管理対象です HANA データベース
HANA データベースサーバに個別の HANA プラグインをインストール	長所： * HANA リソースの自動検出 * リストアとリカバリの自動化 * シングルテナントリストア * SAP システム更新のためのプレスクリプトとポストスクリプトの自動化 * インビルド SnapCenter 高可用性サポート * 各 HANA データベースのログバックアップ保持管理を有効 / 無効にできます。 * HANA のアーキテクチャによってはサポートされていません。HANA マルチホストシステムには、追加の中央プラグインホストが必要です。* HANA プラグインは、 HANA データベースの各ホストに導入する必要があります

データ保護戦略

SnapCenter と SAP HANA プラグインを設定する前に、各種 SAP システムの RTO と RPO の要件に基づいてデータ保護戦略を定義する必要があります。

一般的なアプローチとしては、本番システム、開発システム、テストシステム、サンドボックスシステムなどのシステムタイプを定義します。通常、システムタイプが同じ SAP システムのデータ保護パラメータはすべて同じです。

定義する必要があるパラメータは次のとおりです。

- Snapshot バックアップを実行する頻度
- Snapshot コピーバックアップをプライマリストレージシステムに保存する期間
- ブロック整合性チェックはどのくらいの頻度で実行する必要がありますか。
- プライマリバックアップをオフサイトのバックアップサイトにレプリケートする必要があるか。
- バックアップをオフサイトのバックアップストレージに保管する期間

次の表に、システムタイプの本番、開発、およびテストのデータ保護パラメータの例を示します。本番用システムでは、高いバックアップ頻度が定義されており、バックアップはオフサイトのバックアップサイトに 1 日に 1 回レプリケートされます。テスト用システムの要件は低く、バックアップのレプリケーションはありません。

パラメータ	本番用システム	開発システム	システムをテストする
バックアップ頻度	4 時間ごと	4 時間ごと	4 時間ごと
プライマリの保持	2 日	2 日	2 日
ブロック整合性チェック	週に 1 回	週に 1 回	いいえ
オフサイトのバックアップサイトへのレプリケーション	1 日に 1 回	1 日に 1 回	いいえ
オフサイトへのバックアップの保持	2 週間	2 週間	該当なし

次の表に、データ保護パラメータに設定する必要があるポリシーを示します。

パラメータ	**PolicyLocalSnap** というプロンプトに対して表示され	**PolicyLocalSnapAndSnapVault**	**PolicyBlockIntegrityCheck** 」を参照してください
バックアップタイプ	Snapshot ベース	Snapshot ベース	ファイルベース
スケジュール頻度	毎時	毎日	毎週
プライマリの保持	カウント = 12	カウント = 3	count = 1
SnapVault レプリケーション	いいえ	はい。	該当なし

LocalSnapshot ポリシーは ' 本番システム ' 開発システム ' およびテスト・システムに使用され '2 日間の保持期間を持つローカル Snapshot バックアップをカバーします

リソース保護設定では、スケジュールはシステムタイプごとに異なります。

- * 製造 * 4 時間ごとにスケジュールを設定します。
- * 開発。 * 4 時間ごとにスケジュールを設定します。
- * テスト * 4 時間ごとにスケジュールを設定します。

「 LocalSnapAndSnapVault' 」ポリシーは、本番システムおよび開発システムで、オフサイトのバックアップストレージへの日次レプリケーションをカバーするために使用されます。

リソース保護構成では、スケジュールは本番環境と開発環境に対して定義されます。

- * 生産。 * 毎日スケジュールを設定します。
- * 開発。 * 毎日スケジュールを設定します。

「 BlockIntegrityCheck 」ポリシーは、本番システムおよび開発システムで、ファイルベースのバックアップを使用した週次ブロック整合性チェックをカバーするために使用されます。

リソース保護構成では、スケジュールは本番環境と開発環境に対して定義されます。

- * 生産。 * 毎週スケジュールを設定します。
- * 開発。 * 毎週スケジュールを設定します。

オフサイトのバックアップポリシーを使用する個々の SAP HANA データベースに対して、ストレージレイヤで保護関係を設定する必要があります。保護関係は、レプリケートされるボリュームとバックアップの保持をオフサイトのバックアップストレージで定義します。

この例では、本番用システムと開発用システムごとに、オフサイトのバックアップストレージに 2 週間のデータ保持期間を定義します。

この例では、 SAP HANA データベースのリソースと非データボリュームのリソースの保護ポリシーと保持方法は異なりますが、

バックアップ処理

SAP は、 HANA 2.0 SPS4 を使用する MDC のマルチテナントシステムの Snapshot バックアップをサポートするようになりました。SnapCenter は、複数のテナントを持つ HANA MDC システムの Snapshot バックアップ処理をサポートしています。SnapCenter は、 HANA MDC システムの 2 つの異なるリストア処理もサポートしています。システム全体、システム DB 、およびすべてのテナントをリストアすることも、テナントを 1 つだけリストアすることもできます。SnapCenter でこれらの処理を実行するための前提条件がいくつかあります。

MDC システムでは、テナント設定が静的であるとは限りません。テナントを追加したり、テナントを削除したりできます。SnapCenter は、 HANA データベースが SnapCenter に追加されたときに検出された構成に依存しません。バックアップ処理の実行時に使用可能なテナントを SnapCenter が把握しておく必要があります。

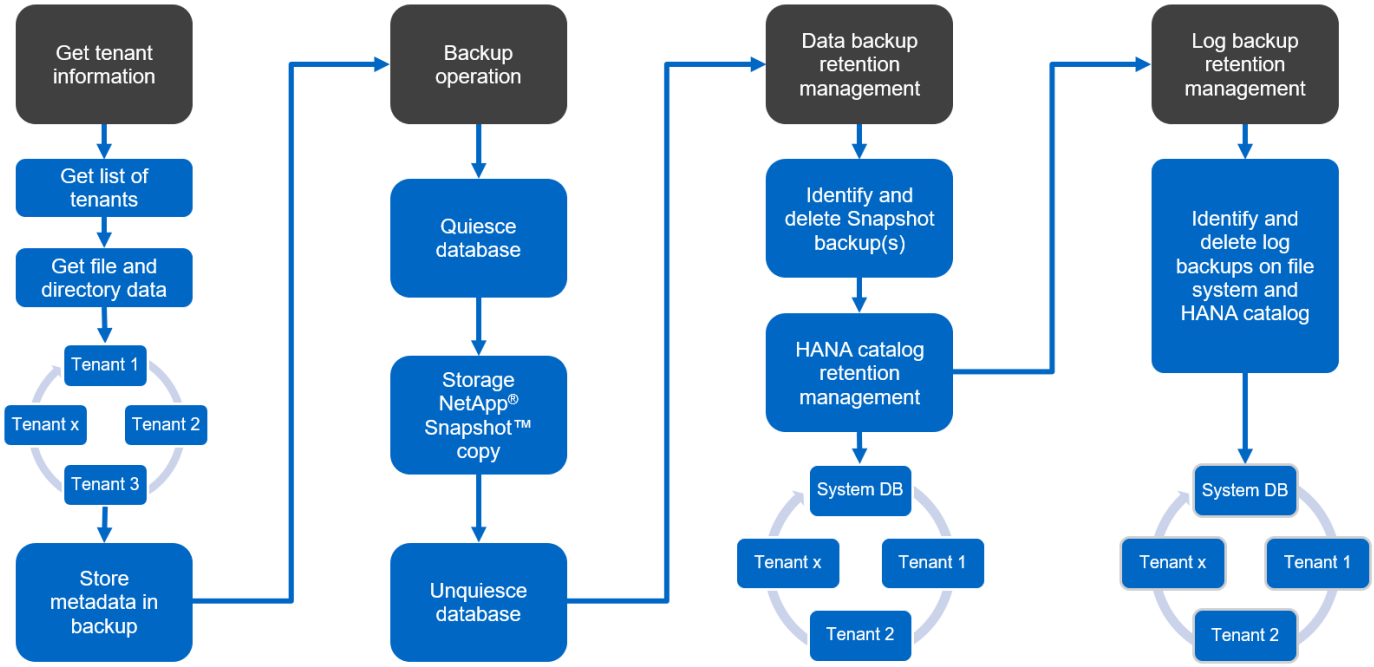
シングルテナントのリストア処理を有効にするには、各 Snapshot バックアップに含まれるテナントが SnapCenter に認識されている必要があります。また、 Snapshot バックアップに含まれる各テナントにどのファイルおよびディレクトリが属するかを把握しておく必要があります。

したがって、バックアップ処理を実行するたびに、テナント情報を取得する必要があります。これには、テナント名、および対応するファイルとディレクトリの情報が含まれます。シングルテナントのリストア処理をサポートできるようにするには、このデータを Snapshot バックアップのメタデータに格納する必要があります。次のステップは、 Snapshot バックアップ処理そのものです。この手順には、 HANA のバックアップセーブポイント、ストレージの Snapshot バックアップ、および SQL コマンドをトリガーして Snapshot 処理を終了する SQL コマンドが含まれています。close コマンドを使用すると、 HANA データベースがシステム DB と各テナントのバックアップカタログを更新します。

SAP では、 1 つ以上のテナントが停止している場合に MDC システムの Snapshot バックアップ処理はサポートされません。

データバックアップの保持管理と HANA のバックアップカタログ管理のために、 SnapCenter では、最初の手順で特定されたシステムデータベースとすべてのテナントデータベースに対してカタログ削除処理を実行する必要があります。ログバックアップの場合と同様に、 SnapCenter ワークフローは、バックアップ処理の一部であった各テナントに対して実行する必要があります。

次の図に、バックアップワークフローの概要を示します。



HANA データベースの **Snapshot** バックアップのワークフロー

SnapCenter では、次の順序で SAP HANA データベースがバックアップされます。

1. SnapCenter が HANA データベースからテナントのリストを読み取ります。
2. SnapCenter は、各テナントのファイルとディレクトリを HANA データベースから読み取ります。
3. テナント情報は、このバックアップ処理の SnapCenter メタデータに格納されます。
4. SnapCenter が SAP HANA のグローバル同期バックアップ保存ポイントをトリガーし、整合性が取れたデータベースイメージを永続性レイヤに作成します。

SAP HANA MDC のシングルまたはマルチテナントシステムの場合は、システムデータベースと各テナントデータベースの同期されたグローバルバックアップの保存ポイントが作成されます。

5. SnapCenter は、リソースに対して設定されたすべてのデータボリュームのストレージ Snapshot コピーを作成します。このシングルホスト HANA データベースの例には、データボリュームが 1 つしかありません。SAP HANA マルチホストデータベースには、複数のデータボリュームがあります。
6. SnapCenter を使用して、ストレージ Snapshot バックアップが SAP HANA バックアップカタログに登録されます。
7. SnapCenter によって、 SAP HANA のバックアップ保存ポイントが削除されます。
8. SnapCenter は、リソース内に設定されているすべてのデータボリュームに対して SnapVault または SnapMirror の更新を開始します。

この手順は、選択したポリシーに SnapVault または SnapMirror のレプリケーションが含まれている場合にのみ実行されます。

9. SnapCenter は、プライマリストレージで定義されたバックアップの保持ポリシーに基づいて、データベース内のストレージ Snapshot コピーとバックアップエントリ、および SAP HANA のバックアップカタログを削除します。HANA のバックアップカタログ処理は、システムデータベースとすべてのテナントに対して実行されます。

バックアップがセカンダリストレージに残っている場合、 SAP HANA のカタログのエントリは削除されません。

10. SnapCenter は、ファイルシステムと SAP HANA のバックアップカタログにある、 SAP HANA のバックアップカタログにある最も古いデータバックアップよりも古いすべてのログバックアップを削除します。これらの処理はシステムデータベースおよびすべてのテナントに対して実行されます。

この手順は、ログバックアップの不要ファイルの削除が無効になっていない場合にのみ実行します。

ブロック整合性チェック処理のバックアップワークフロー

SnapCenter は、次の順序でブロック整合性チェックを実行します。

1. SnapCenter が HANA データベースからテナントのリストを読み取ります。
2. SnapCenter は、システムデータベースと各テナントに対してファイルベースのバックアップ処理をトリガーします。
3. SnapCenter は、ブロック整合性チェック処理用に定義された保持ポリシーに基づいて、データベース、ファイルシステム、および SAP HANA のバックアップカタログからファイルベースのバックアップを削除します。ファイルシステムと HANA のバックアップカタログに関するバックアップの削除は、システムデータベースとすべてのテナントに対して実行されます。
4. SnapCenter は、ファイルシステムと SAP HANA のバックアップカタログにある、 SAP HANA のバックアップカタログにある最も古いデータバックアップよりも古いすべてのログバックアップを削除します。これらの処理はシステムデータベースおよびすべてのテナントに対して実行されます。

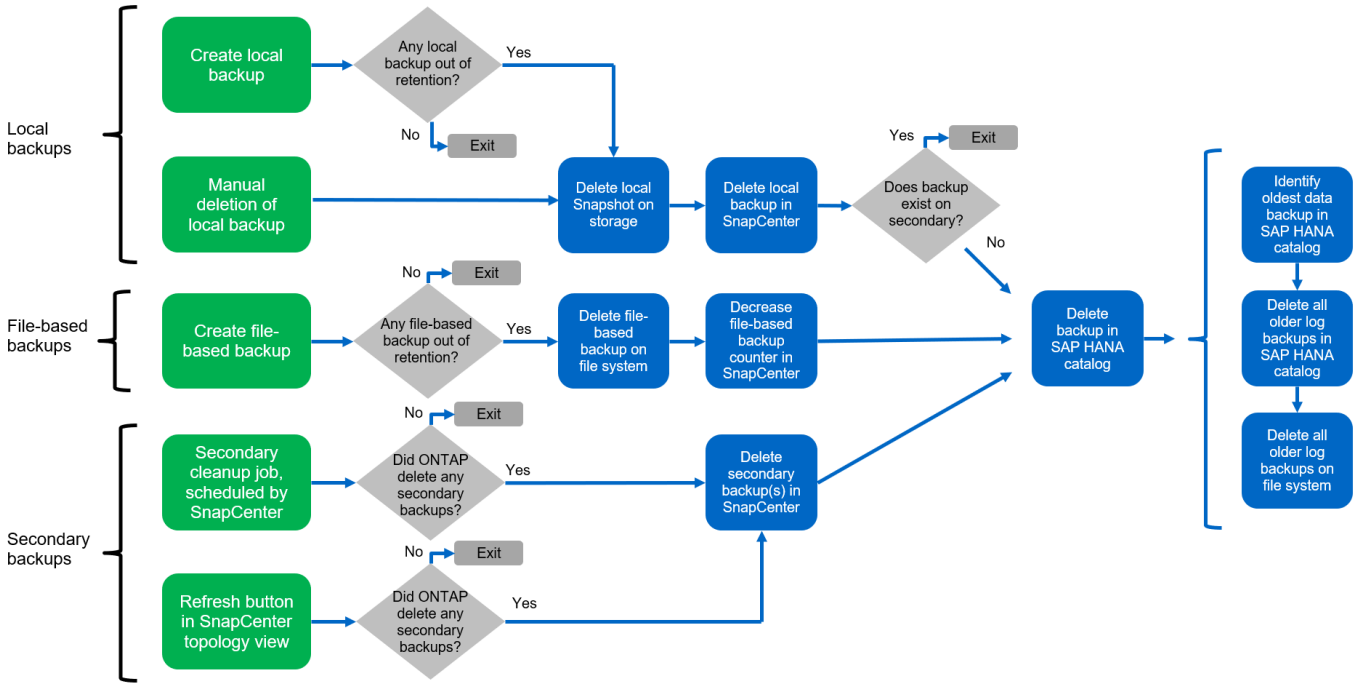
この手順は、ログバックアップの不要ファイルの削除が無効になっていない場合にのみ実行します。

バックアップ保持管理、および不要なデータバックアップとログバックアップの削除

データバックアップ保持管理とログバックアップの不要ファイルの削除は、次の保持管理を含む 5 つのメイン領域に分割できます。

- プライマリストレージでのローカルバックアップ
- ファイルベースのバックアップ
- セカンダリストレージでバックアップを実行する
- SAP HANA のバックアップカタログでのデータのバックアップ
- SAP HANA のバックアップカタログとファイルシステムにバックアップを記録します

次の図は、各種ワークフローの概要と各処理の依存関係を示しています。以降のセクションでは、さまざまな処理について詳しく説明します。



プライマリストレージでのローカルバックアップの保持管理

SnapCenter は、 SnapCenter バックアップポリシーに定義された保持設定に従って、プライマリストレージと SnapCenter リポジトリの Snapshot コピーを削除することで、 SAP HANA データベースのバックアップと非データボリュームのバックアップを削除します。

保持管理ロジックは、 SnapCenter の各バックアップワークフローで実行されます。

SnapCenter では、スケジュールされたバックアップとオンデマンドバックアップの両方で保持管理を個別に処理できることに注意してください。

プライマリストレージのローカルバックアップは、 SnapCenter で手動で削除することもできます。

ファイルベースのバックアップの保持管理

SnapCenter は、 SnapCenter バックアップポリシーに定義された保持設定に従ってファイルシステム上のバックアップを削除することで、ファイルベースのバックアップを削除します。

保持管理ロジックは、 SnapCenter の各バックアップワークフローで実行されます。

スケジュールバックアップまたはオンデマンドバックアップでは、 SnapCenter で保持管理を個別に実行できることに注意してください。

セカンダリストレージでのバックアップの保持管理

セカンダリストレージでのバックアップの保持管理は、 ONTAP 保護関係に定義された保持設定に基づいて ONTAP によって処理されます。

SnapCenter リポジトリ内のセカンダリストレージでこれらの変更内容を同期するために、 SnapCenter ではスケジュールされたクリーンアップジョブを使用します。このクリーンアップジョブは、すべての SnapCenter プラグインとすべてのリソースについて、すべてのセカンダリストレージのバックアップを SnapCenter リポジトリと同期します。

デフォルトでは、クリーンアップジョブは週に 1 回スケジュールされます。この週次スケジュールでは、 SnapCenter および SAP HANA Studio でのバックアップの削除は、セカンダリストレージですでに削除されているバックアップと比較して遅延します。この不整合を回避するために、 1 日に 1 回など、スケジュールを高い頻度に変更することができます。

リソースのトポロジビューで更新ボタンをクリックして、個々のリソースのクリーンアップジョブを手動でトリガーすることもできます。

クリーンアップジョブのスケジュールを変更する方法、または手動で更新を開始する方法については、を参照してください "「オフサイトバックアップストレージとのバックアップ同期のスケジューリング頻度を変更します。」"

SAP HANA のバックアップカタログ内でのデータバックアップの保持管理

SnapCenter がバックアップ、ローカル Snapshot またはファイルベースを削除した場合、またはセカンダリストレージでバックアップの削除を特定した場合は、 SAP HANA のバックアップカタログからこのデータバックアップも削除されます。

SnapCenter は、プライマリストレージでローカル Snapshot バックアップの SAP HANA カタログエントリを削除する前に、セカンダリストレージにバックアップが残っているかどうかを確認します。

ログバックアップの保持管理

SAP HANA データベースでは、ログバックアップが自動的に作成されます。このログバックアップでは、 SAP HANA で構成されたバックアップディレクトリに、個々の SAP HANA サービスごとにバックアップファイルが作成されます。

最新のデータバックアップよりも古いログバックアップはフォワードリカバリで不要になり、削除可能です。

SnapCenter は、ファイルシステムレベルおよび SAP HANA のバックアップカタログでの不要なログファイ

ルバックアップの削除を次の手順で処理します。

1. SnapCenter は、 SAP HANA のバックアップカタログを読み取り、成功した最も古いファイルベースバックアップまたは Snapshot バックアップのバックアップ ID を取得します。
2. SnapCenter は、 SAP HANA カタログ内のすべてのログバックアップと、このバックアップ ID よりも古いファイルシステムを削除します。

> SnapCenter では、 SnapCenter で作成されたバックアップの不要な削除のみが処理されます。SnapCenter の外部で追加のファイルベースのバックアップを作成する場合は、ファイルベースのバックアップがバックアップカタログから削除されていることを確認する必要があります。このようなデータバックアップがバックアップカタログから手動で削除されないと、最も古いデータバックアップになる可能性があります。また、このファイルベースのバックアップが削除されるまで、古いログバックアップは削除されません。

> ポリシー設定でオンデマンドバックアップに対して保持が定義されていても、不要なファイルの削除は別のオンデマンドバックアップが実行されたときにのみ実行されます。そのため、通常、 SnapCenter でオンデマンドバックアップを手動で削除して、これらのバックアップが SAP HANA バックアップカタログからも削除され、ログバックアップの不要な削除が古いオンデマンドバックアップに基づいていないことを確認する必要があります。

ログバックアップ保持管理は、デフォルトで有効になっています。必要に応じて、の説明に従って無効にすることができます ""HANA プラグインホストで自動検出を無効にします。 ""

Snapshot バックアップに必要な容量

従来のデータベースの変更率と比較して、ストレージレイヤのブロック変更率が高いことを考慮する必要があります。列ストアの HANA テーブルのマージプロセスにより、テーブル全体が変更されたブロックだけでなくディスクに書き込まれます。

1 日に複数の Snapshot バックアップを作成した場合、顧客ベースから得られるデータの日次変更率は 20~50% です。SnapVault ターゲットでレプリケーションを 1 日に 1 回しか実行しない場合、通常は日単位の変更率が小さくなります。

リストア処理とリカバリ処理

SnapCenter を使用したリストア処理

HANA データベースに関しては、 SnapCenter は 2 つの異なるリストア処理をサポートしています。

- * リソース全体のリストア。 * HANA システムのすべてのデータがリストアされます。HANA システムに 1 つ以上のテナントがある場合は、システムデータベースのデータとすべてのテナントのデータがリストアされます。
- * 単一テナントのリストア。 * 選択したテナントのデータのみがリストアされます。

ストレージに関して言えば、上記のリストア処理は、使用するストレージプロトコル（ NFS またはファイバチャネル SAN ）、設定されているデータ保護（プライマリストレージにオフサイトのバックアップストレージがあるかどうかに関係なく）、それぞれ別の方法で実行する必要があります。 また、リストア処理に使用するバックアップを選択します（プライマリまたはオフサイトのバックアップストレージからリストアします）。

プライマリストレージからのリソース全体のリストア

プライマリストレージからリソース全体をリストアする場合、 SnapCenter では、リストア処理を実行するために 2 つの異なる ONTAP 機能がサポートされます。次の 2 つの機能から選択できます。

- * ボリューム・ベース SnapRestore 。 * ボリューム・ベースの SnapRestore は、ストレージ・ボリュームの内容を、選択した Snapshot バックアップの状態に戻します。
  - NFS を使用して自動検出されたリソースで利用可能なボリュームリバートチェックボックス。
  - 手動で構成されたリソースの [Complete Resource] オプションボタン。
- * ファイル・ベースの SnapRestore * 単一ファイル SnapRestore とも呼ばれるファイル・ベースの SnapRestore は ' すべての個別ファイル（ NFS ）またはすべての LUN （ SAN ）をリストアします
  - 自動検出されたリソースのデフォルトのリストア方法。NFS のボリュームリバートチェックボックスを使用して変更できます。
  - 手動で構成されたリソース用のファイルレベルオプションボタン。

次の表に、各種のリストア方式の比較を示します。

	ボリュームベース **SnapRestore**	ファイルベースの **SnapRestore**
リストア処理の速度	ボリュームサイズに関係なく、非常に高速です	リストア処理は非常に高速ですが、ストレージシステムでバックグラウンドコピージョブが使用されるため、新しい Snapshot バックアップの作成がブロックされます
Snapshot バックアップ履歴	古い Snapshot バックアップにリストアすると、新しい Snapshot バックアップがすべて削除されます。	影響はありません
ディレクトリ構造のリストア	ディレクトリ構造もリストアされます	nfs ：個々のファイルのみをリストアし、ディレクトリ構造はリストアしません。ディレクトリ構造も失われた場合は、リストア処理の実行前に手動で作成する必要があります。 SAN ：ディレクトリ構造もリストアされます
オフサイトのバックアップストレージにレプリケーションするように構成されたリソース	ボリュームベースのリストアを、 SnapVault 同期に使用されている Snapshot コピーよりも古い Snapshot コピーバックアップには実行できません	Snapshot バックアップを選択できます

オフサイトのバックアップストレージから完全なリソースをリストア

オフサイトのバックアップストレージからのリストアは、必ず SnapVault リストア処理を使用して実行します。この場合、ストレージボリュームのすべてのファイルまたはすべての LUN が、 Snapshot バックアップの内容で上書きされます。

単一テナントのリストア

単一のテナントをリストアするには、ファイルベースのリストア処理が必要です。使用するストレージプロト

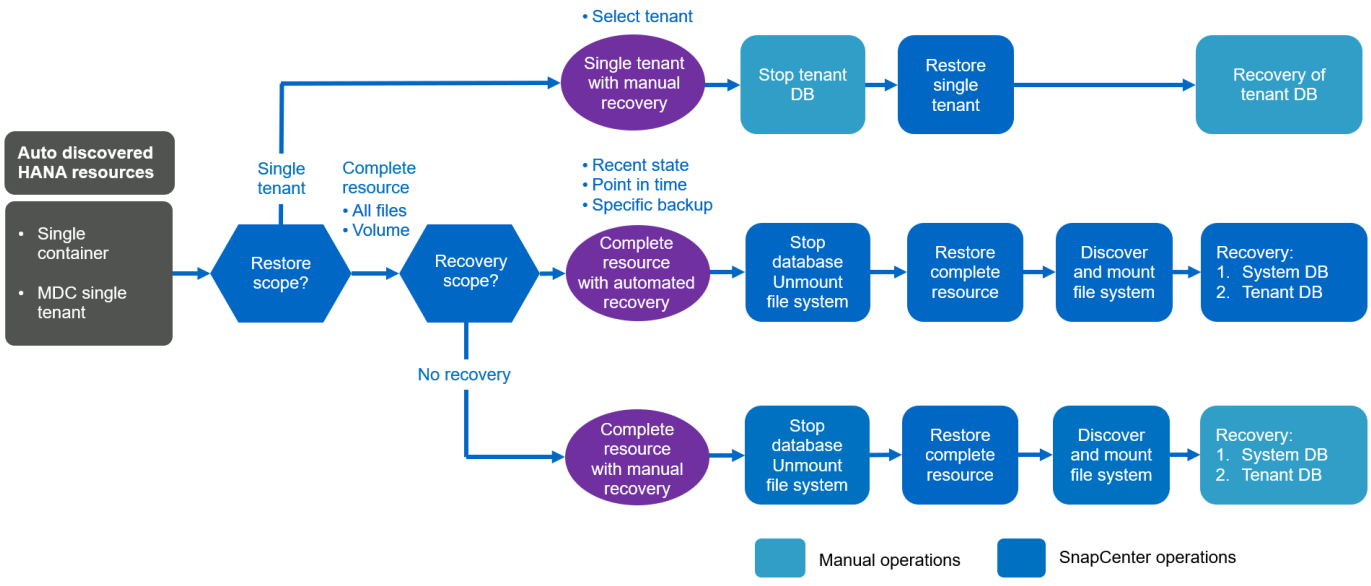
コルに応じて、 SnapCenter で実行されるリストアワークフローは異なります。

- NFS ：
  - プライマリストレージ。ファイルベースの SnapRestore 処理は、テナントデータベースのすべてのファイルに対して実行されます。
  - オフサイトのバックアップストレージ： SnapVault リストア処理は、テナントデータベースのすべてのファイルに対して実行されます。
- SAN ：
  - プライマリストレージ。LUN をクローニングしてデータベースホストに接続し、テナントデータベースのすべてのファイルをコピーします。
  - オフサイトのバックアップストレージ。LUN をクローニングしてデータベースホストに接続し、テナントデータベースのすべてのファイルをコピーします。

自動検出された **HANA** シングルコンテナおよび **MDC** シングルテナントシステムのリストアとリカバリ

自動検出された HANA シングルコンテナシステムと HANA MDC シングルテナントシステムは、 SnapCenter を使用した自動リストアとリカバリが有効になります。これらの HANA システムについては、次の図に示すように、 SnapCenter では 3 種類のリストアとリカバリのワークフローがサポートされています。

- * シングルテナントで手動リカバリ * 。シングルテナントのリストア処理を選択すると、選択した Snapshot バックアップに含まれるすべてのテナントが SnapCenter に表示されます。テナントデータベースは手動で停止してリカバリする必要があります。SnapCenter でのリストア処理は、 NFS での単一ファイルの SnapRestore 処理、または SAN 環境でのクローニング、マウント、コピーの処理で行われます。
- * 自動リカバリ機能を備えた完全なリソース。 * 完全なリソースのリストア操作と自動リカバリを選択した場合、 SnapCenter により完全なワークフローが自動化されます。SnapCenter では、最新の状態、ポイントインタイム、または特定のバックアップリカバリ処理がサポートされます。選択したリカバリ処理は、システムとテナントデータベースに使用されます。
- * 手動リカバリを伴う完全なリソース。 * リカバリなしを選択すると、 SnapCenter は HANA データベースを停止し、必要なファイルシステム（アンマウント、マウント）およびリストア処理を実行します。システムデータベースとテナントデータベースを手動でリカバリする必要があります。

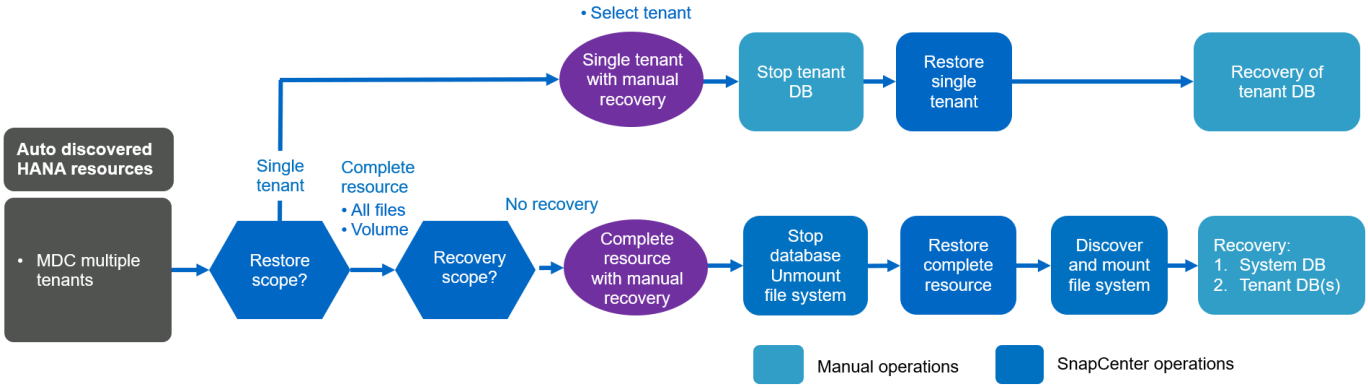


自動検出された **HANA MDC** のマルチテナントシステムのリストアとリカバリ

複数のテナントを持つ HANA MDC システムは自動的に検出されますが、自動リストアとリカバリは現在の SnapCenter リリースではサポートされていません。複数のテナントを持つ MDC システムの場合は、次の図に示すように、 SnapCenter では 2 つの異なるリストアとリカバリのワークフローがサポートされています。

- シングルテナントと手動リカバリ
- 手動リカバリでリソースを完全にリカバリ

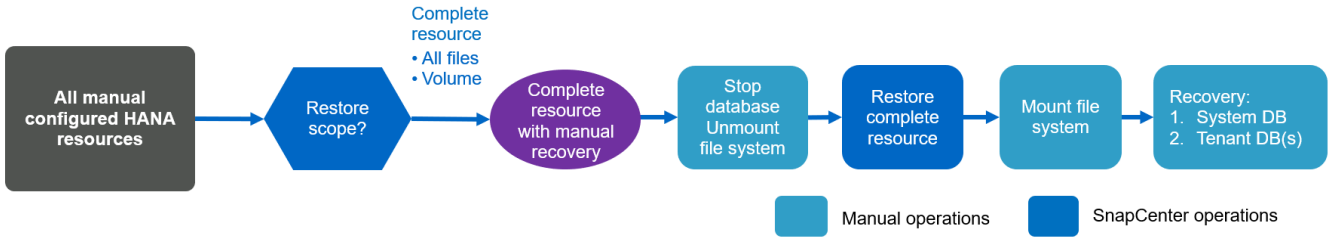
ワークフローは、前のセクションで説明したものと同じです。



手動で構成した **HANA** リソースのリストアとリカバリ

手動構成の HANA リソースは、リストアとリカバリの自動化が有効になっていません。また、シングルテナントまたは複数テナントの MDC システムでは、単一テナントのリストア処理はサポートされていません。

構成した HANA の手動リソースの場合、 SnapCenter では、次の図に示すように手動リカバリのみがサポートされます。手動リカバリのワークフローは、前のセクションで説明したものと同じです。



リストア処理とリカバリ処理の概要

次の表は、 SnapCenter の HANA リソース構成に応じたリストア処理とリカバリ処理をまとめたものです。

SnapCenter リソース構成	リストアとリカバリのオプション	**HANA** データベースを停止します	マウント前にアンマウントし、リストア後にマウントします	リカバリ処理
自動検出単一コンテナ MDC のシングルテナント	• どちらかを使用してリソースを完了します • デフォルト（すべてのファイル） • ボリュームのリバート（プライマリストレージからの NFS のみ） • 自動リカバリが選択されました	SnapCenter による自動化	SnapCenter による自動化	SnapCenter による自動化
	• どちらかを使用してリソースを完了します • デフォルト（すべてのファイル） • ボリュームのリバート（プライマリストレージからの NFS のみ） • リカバリが選択されていません	SnapCenter による自動化	SnapCenter による自動化	手動
	• テナントのリストア	手動	必要ありません	手動

SnapCenter リソース構成	リストアとリカバリのオプション	**HANA** データベースを停止します	マウント前にアンマウントし、リストア後にマウントします	リカバリ処理
MDC の複数のテナントを自動検出	• どちらかを使用してリソースを完了します • デフォルト（すべてのファイル） • ボリュームのリバート（プライマリストレージからの NFS のみ） • 自動リカバリはサポートされていません	SnapCenter による自動化	SnapCenter による自動化	手動
	• テナントのリストア	手動	必要ありません	手動
すべての手動設定リソース	• 完全なリソース（ = ボリュームの復元、 NFS および SAN でプライマリストレージからのみ使用可能） • ファイルレベル（すべてのファイル） • 自動リカバリはサポートされていません	手動	手動	手動

このレポートで使用するラボのセットアップ

このテクニカルレポートで使用するラボセットアップには、次の 5 種類の SAP HANA 構成が含まれています。

- * MS1.*
  - SAP HANA マルチホスト MDC のシングルテナントシステム
  - 中央のプラグインホスト（ SnapCenter サーバ）で管理
  - ストレージプロトコルとして NFS を使用します
- * SS1.*

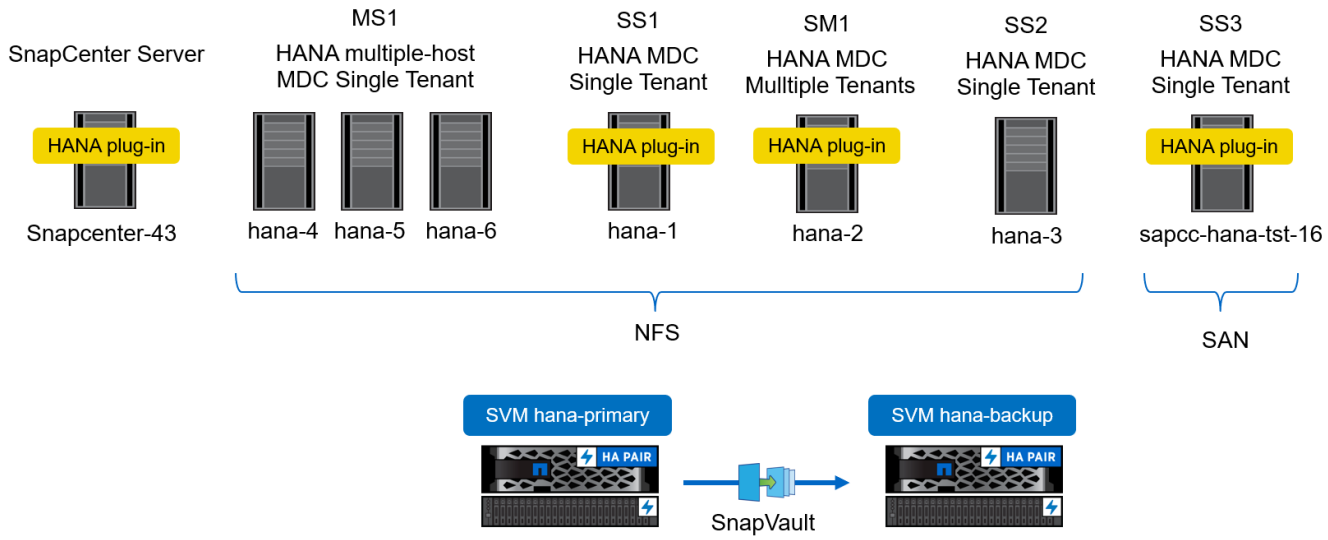
- SAP HANA シングルホスト MDC のシングルテナントシステム
- HANA プラグインが HANA データベースホストにインストールされている状態で自動検出されます
- ストレージプロトコルとして NFS を使用します

- * SM1. *
  - SAP HANA シングルホスト MDC のマルチテナントシステム
  - HANA プラグインが HANA データベースホストにインストールされている状態で自動検出されます
  - ストレージプロトコルとして NFS を使用します
- * SS2.*
  - SAP HANA シングルホスト MDC のシングルテナントシステム
  - 中央のプラグインホスト（ SnapCenter サーバ）で管理
  - ストレージプロトコルとして NFS を使用します
- * SS3.*
  - SAP HANA シングルホスト MDC のシングルテナントシステム
  - HANA プラグインが HANA データベースホストにインストールされている状態で自動検出されます
  - ストレージプロトコルとして Fibre Channel SAN を使用します

以降のセクションでは、設定、バックアップ、リストア、リカバリの各ワークフローについて説明します。概要 では、ローカル Snapshot バックアップに加え、 SnapVault を使用したバックアップストレージへのレプリケーションも実行できます。Storage Virtual Machine （ SVM ）は、プライマリストレージは「 HANA プライマリ」、オフサイトバックアップストレージは「 HANA プライマリ」です。

SnapCenter サーバは、 HANA システム MS1 および SS2 の中央 HANA プラグインホストとして使用されます。

次の図は、ラボのセットアップを示しています。

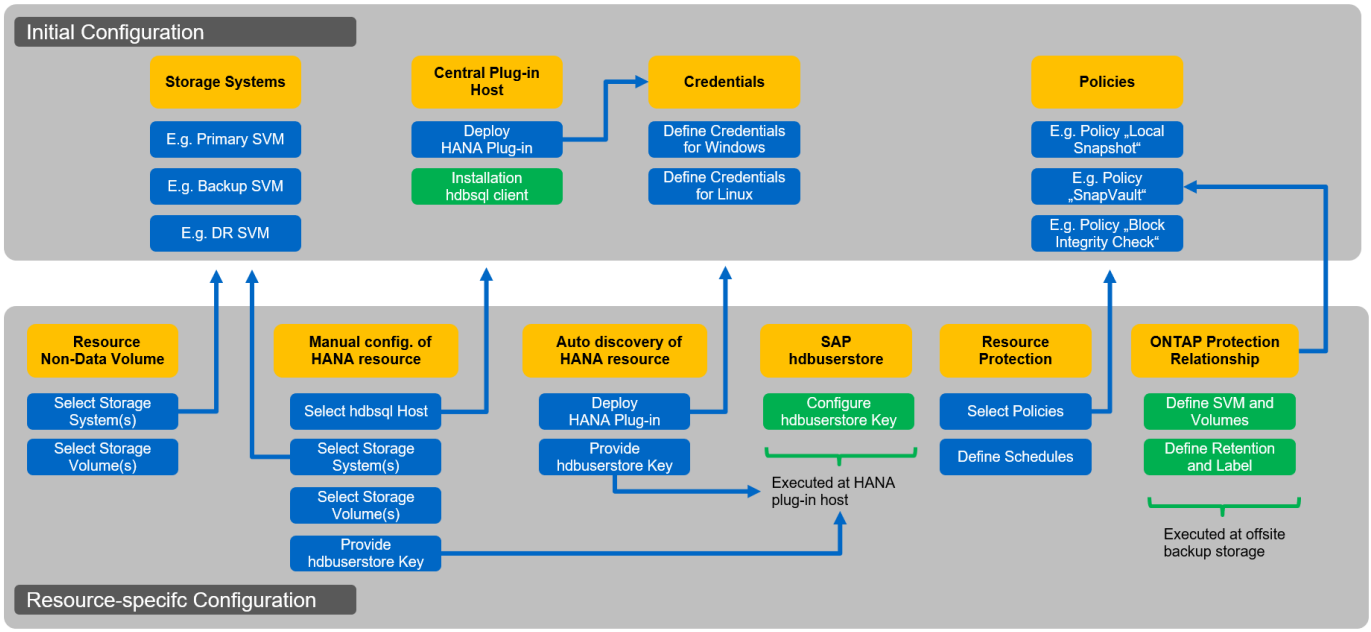


SnapCenter 構成

SnapCenter の設定は、次の 2 つの主要な領域に分けることができます。

- * 初期構成。 * 個々の SAP HANA データベースに依存しない一般的な構成を取り上げます。リソース固有の設定を実行する際に選択される、ストレージシステム、中央 HANA プラグインホスト、ポリシーなどの構成。
- * リソース固有の構成。 * SAP HANA システム固有の構成を対象としており、各 SAP HANA データベースに対して実行する必要があります。

次の図に、構成コンポーネントとその依存関係の概要を示します。緑のボックスは、 SnapCenter の外部で実行する必要がある設定手順を示しています。青いボックスは、 SnapCenter GUI を使用して実行する手順を示しています。



初期設定では、次のコンポーネントがインストールおよび設定されます。

- * ストレージシステム。 * SAP HANA システムで使用されるすべての SVM のクレデンシャル設定。通常は、プライマリストレージ、オフサイトバックアップストレージ、ディザスタリカバリストレージを構成します。

> ストレージクラスタのクレデンシャルは、個々の SVM のクレデンシャルの代わりにを設定することもできます。

- * 資格情報。 * SAP HANA プラグインをホストに導入するために使用する資格情報の設定。
- * ホスト（中央 HANA プラグインホスト用）。 * SAP HANA プラグインの導入。SAP HANA hdbclient ソフトウェアのホストへのインストールSAP hdbclient ソフトウェアは手動でインストールする必要があります
- * ポリシー。 * バックアップタイプ、保持、およびレプリケーションの構成。通常、ローカル Snapshot コピー用、 SnapVault レプリケーション用、およびファイルベースのバックアップ用に、少なくとも 1 つのポリシーが必要です。

リソース固有の設定は、 SAP HANA データベースごとに実行する必要があります。これには、次の設定が含まれます。

- SAP HANA の非データボリュームのリソース構成：
  - ストレージシステムおよびボリューム
- SAP hdbuserstore キーの設定：
  - 特定の SAP HANA データベースの SAP hdbuserstore キー設定は、 HANA プラグインの導入場所に応じて、中央のプラグインホストまたは HANA データベースホストのいずれかで実行する必要があります。
- 自動検出された SAP HANA データベースのリソース：
  - データベースホストへの SAP HANA プラグインの導入
  - hdbuserstore キーを入力します
- SAP HANA データベースの手動リソース構成：
  - SAP HANA データベースの SID 、プラグインホスト、 hdbuserstore キー、ストレージシステム、ボリューム
- リソース保護の構成：
  - 必要なポリシーを選択できます
  - 各ポリシーのスケジュールの定義
- ONTAP データ保護構成：
  - バックアップをオフサイトのバックアップストレージにレプリケートする場合にのみ必要です。
  - 関係と保持の定義。

SnapCenter の初期設定

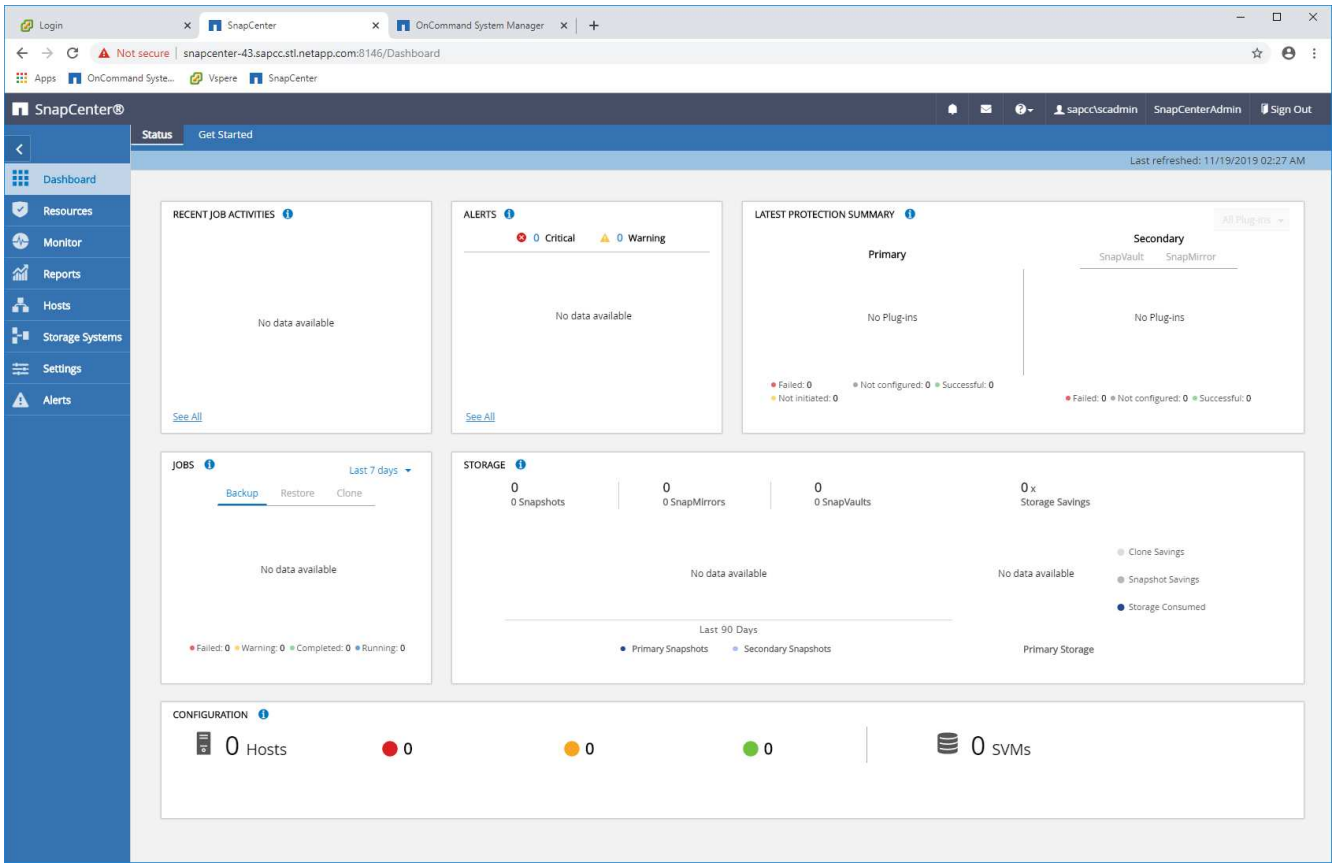
初期設定には、次の手順が含まれます。

1. ストレージシステムの構成：
2. プラグインのインストールに使用するクレデンシャルの設定
3. 中央の HANA プラグインホストの場合：
   a. ホスト構成と SAP HANA プラグインの導入
   b. SAP HANA hdbsql クライアントソフトウェアのインストールと設定
4. ポリシー設定

以降のセクションでは、初期設定手順について説明します。

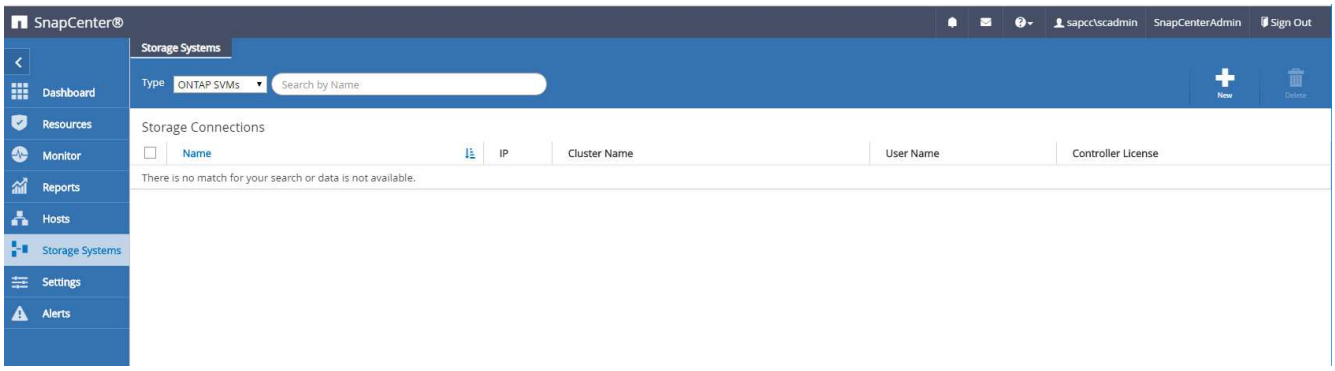
ストレージシステムの構成：

1. SnapCenter サーバ GUI にログインします。



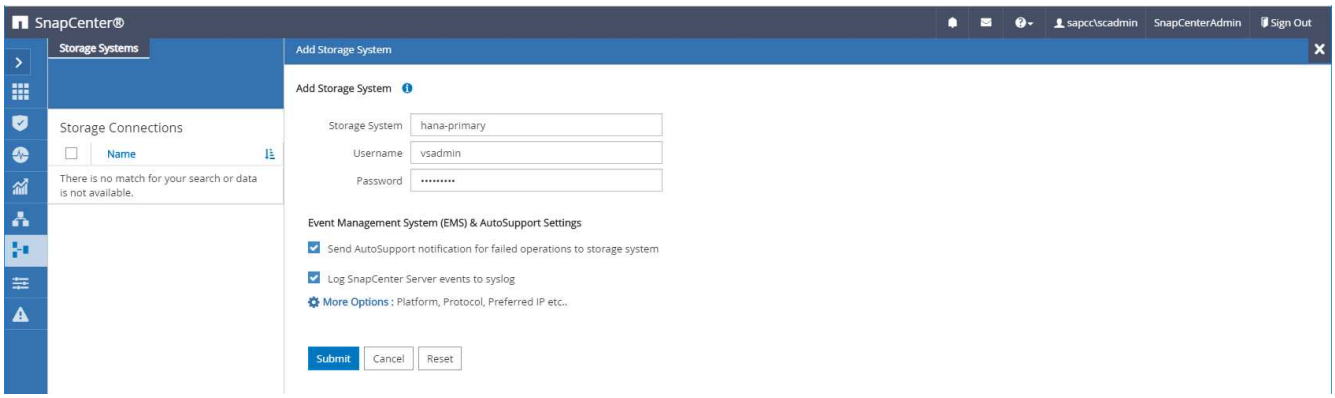
2. [ストレージシステム] を選択します。

画面では、 ONTAP SVM または ONTAP クラスタなどのストレージシステムタイプを選択できます。ストレージシステムを SVM レベルで構成する場合は、各 SVM に対して管理 LIF を設定する必要があります。代わりに、クラスタレベルで SnapCenter 管理アクセスを使用することもできます。SVM 管理を使用する例を次に示します。



3. New をクリックしてストレージシステムを追加し、必要なホスト名とクレデンシャルを入力します。

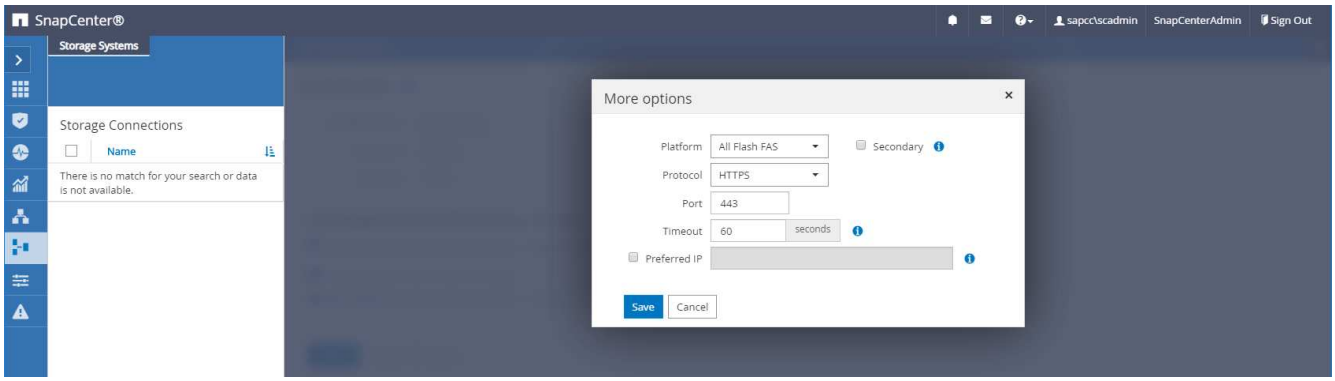
スクリーンショットに示されているように、 SVM ユーザを vsadmin ユーザにする必要はありません。通常、ユーザは SVM 上で設定し、バックアップとリストアの処理を実行するために必要な権限を割り当てます。必要な権限の詳細については、を参照してください "SnapCenter インストールガイド" 「 Minimum ONTAP Privileges Required 」の項を参照してください。



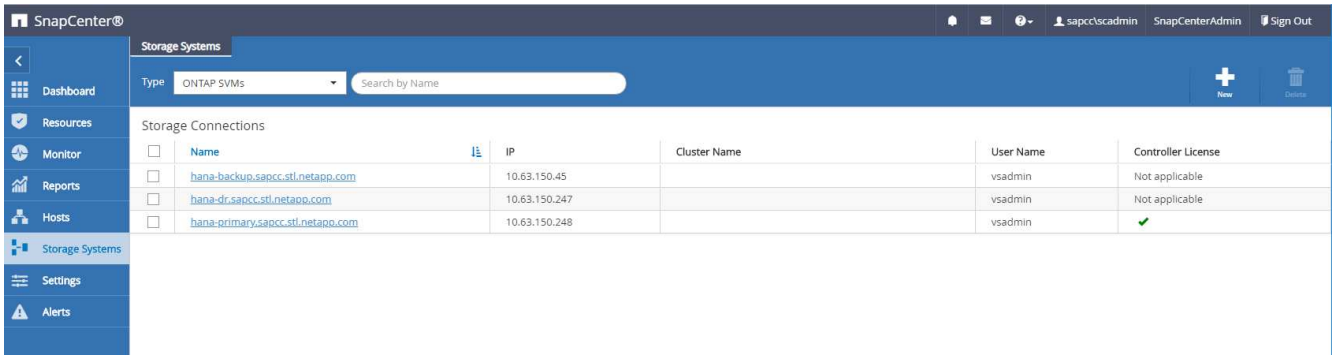
4. [その他のオプション] をクリックして、ストレージプラットフォームを構成します。

   ストレージプラットフォームは、 FAS 、 AFF 、 ONTAP Select 、 Cloud Volumes ONTAP のいずれかです。

   SnapVault ターゲットまたは SnapMirror ターゲットとして使用されているシステムの場合は、セカンダリアイコンを選択します。

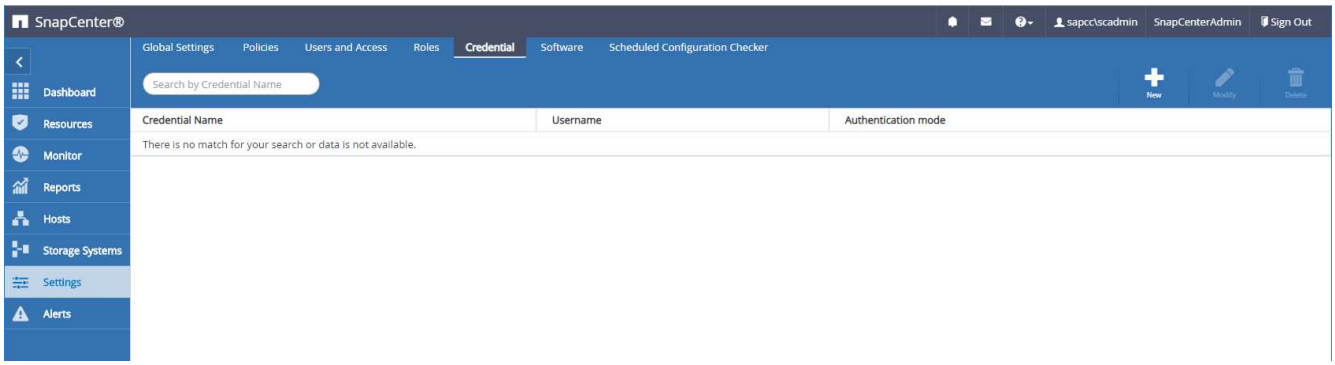


5. 必要に応じてストレージシステムを追加この例では、追加のオフサイトバックアップストレージとディザスタリカバリ用ストレージが追加されています。

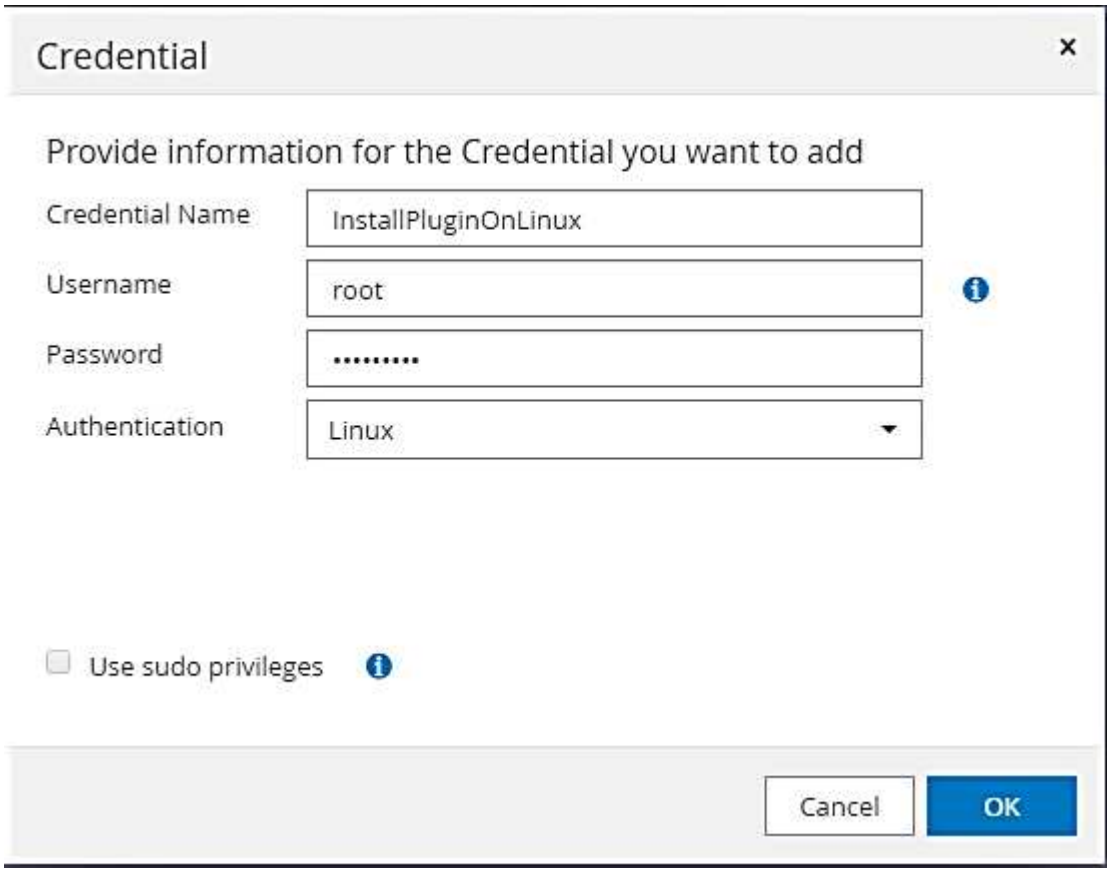


クレデンシャルの設定

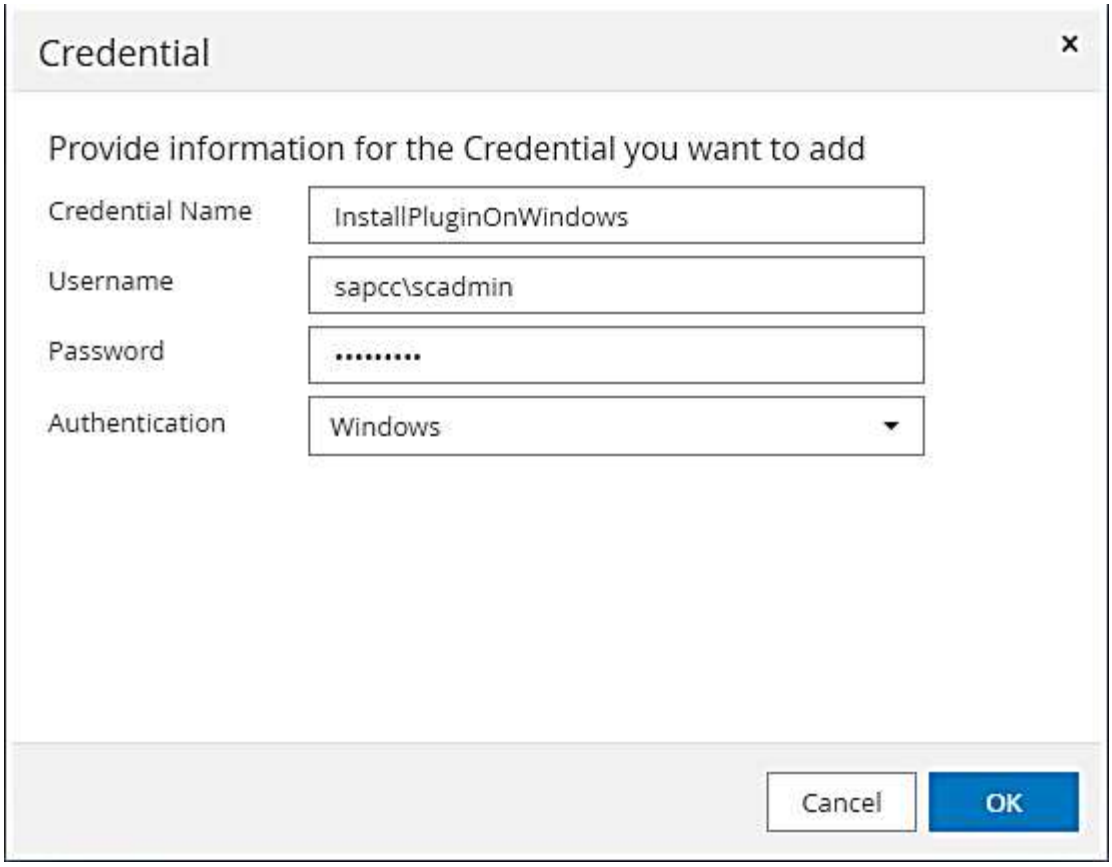
1. [設定] に移動し、 [資格情報] を選択して、 [新規] をクリックします



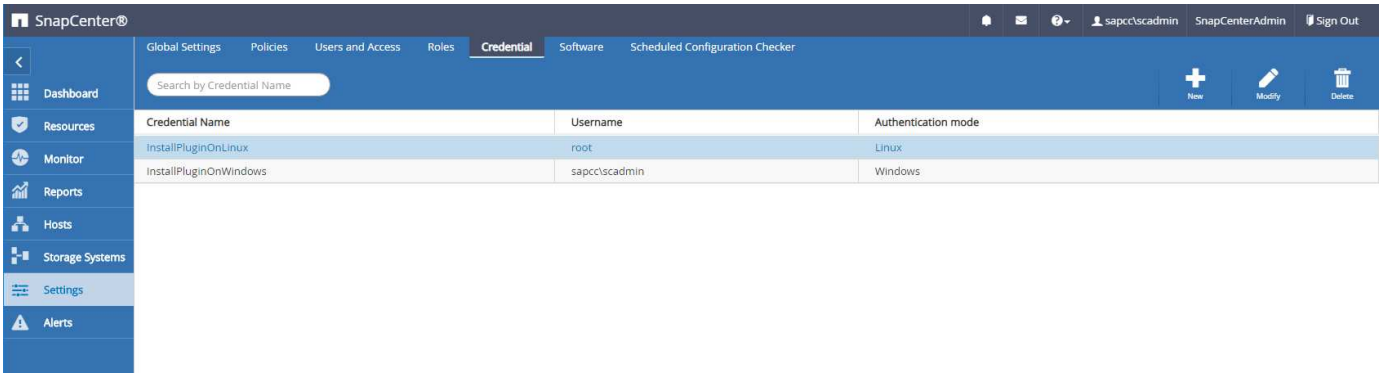
2. Linux システムへのプラグインのインストールに使用するユーザのクレデンシャルを入力します。



3. Windows システムへのプラグインのインストールに使用するユーザのクレデンシャルを入力します。



次の図に、設定されたクレデンシャルを示します。

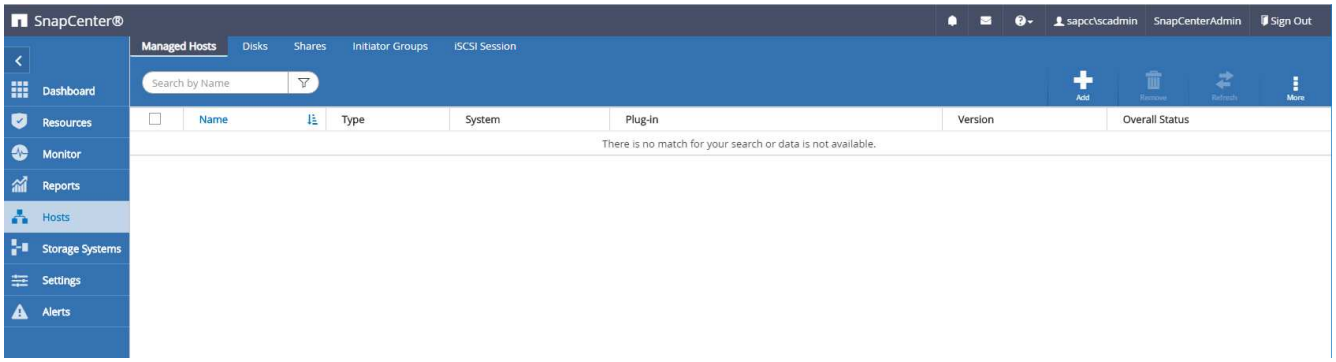


中央のプラグインホストへの **SAP HANA** プラグインのインストール

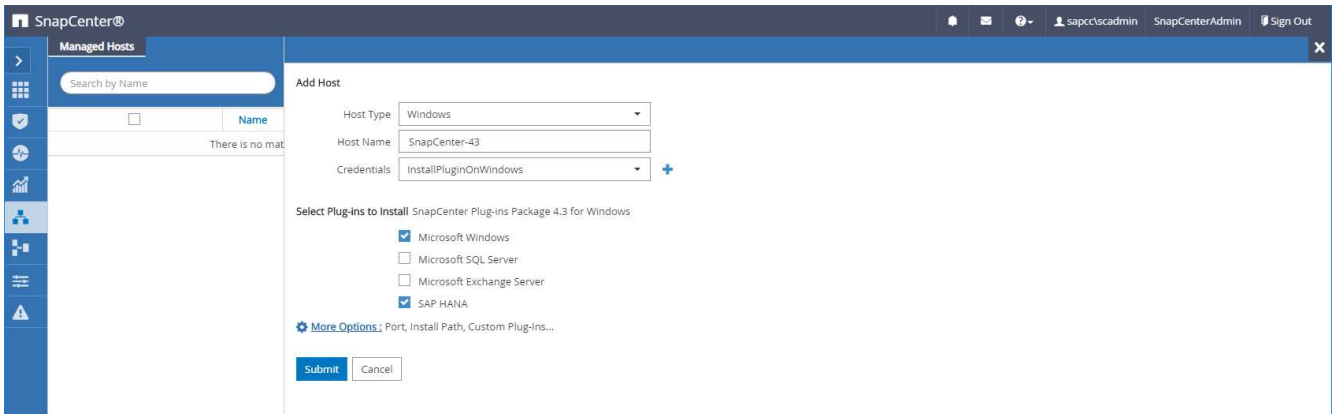
ラボのセットアップでは、 SnapCenter サーバは中央の HANA プラグインホストとしても使用されます。SnapCenter サーバを実行する Windows ホストがホストとして追加され、 SAP HANA プラグインが Windows ホストにインストールされます。

SAP HANA プラグインには、 Java 64 ビットバージョン 1.8 が必要です。SAP HANA プラグインを導入する前に、ホストに Java をインストールする必要があります。

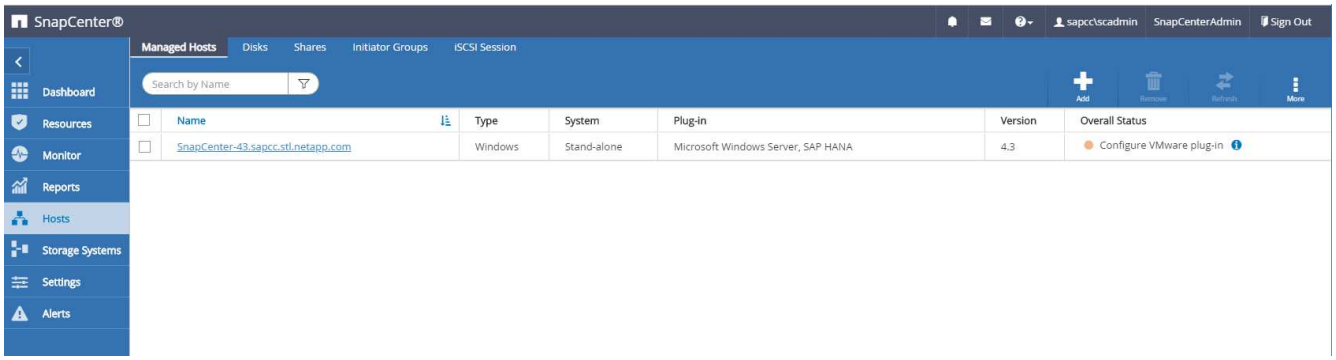
1. Hosts に移動し、 Add をクリックします。



2. 必要なホスト情報を指定します。Submit をクリックします。



次の図は、 HANA プラグインの導入後に構成されたすべてのホストを示しています。



SAP HANA hdbsql クライアントソフトウェアのインストールと設定

SAP HANA hdbsql クライアントソフトウェアは、 SAP HANA プラグインがインストールされているホストと同じホストにインストールする必要があります。ソフトウェアはからダウンロードできます "SAP サポートポータル"。

リソース設定中に設定された HDBSQL OS ユーザは、 hdbsql 実行可能ファイルを実行できる必要があります。hdbsql 実行ファイルへのパスは 'hana.properties` ファイルで設定する必要があります

- Windows の場合

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

- Linux ：

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties
HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

ポリシー設定

の項で説明したように "「データ保護戦略」" ポリシーは通常、リソースとは別に設定され、複数の SAP HANA データベースで使用できます。

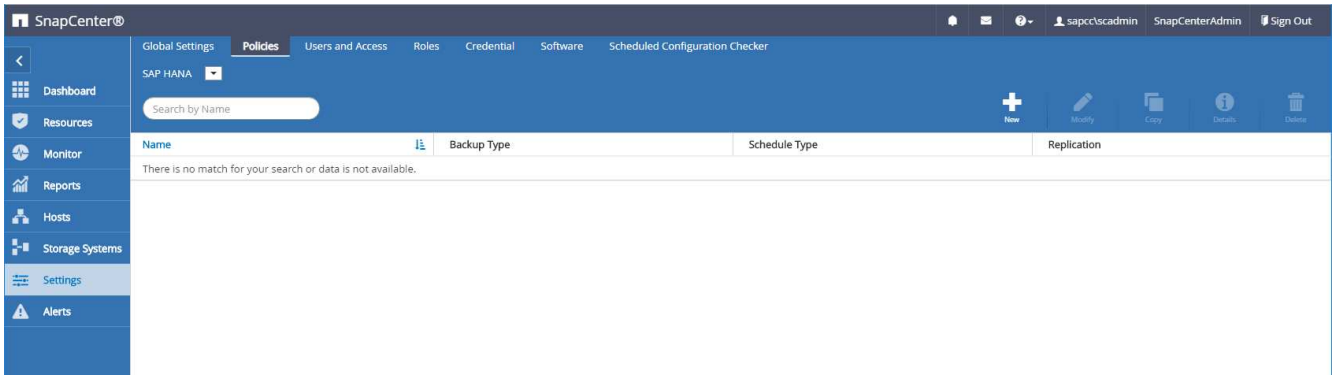
一般的な最小構成は、次のポリシーで構成されます。

- レプリケーションを行わずに 1 時間ごとのバックアップを行うためのポリシー： LocalSnap
- SnapVault レプリケーションを使用した日次バックアップのポリシー：「 LocalSnapAndSnapVault'
- ファイル・ベースのバックアップを使用した週次ブロック整合性チェックのポリシー： BlockIntegrityCheck

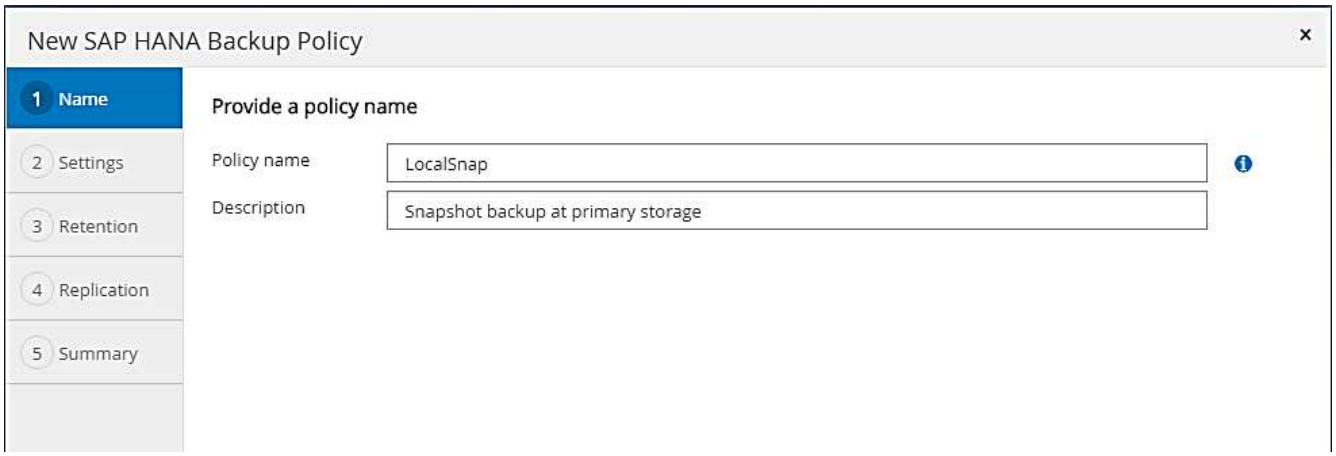
以降のセクションでは、これら 3 つのポリシーの設定について説明します。

1 時間ごとの **Snapshot** バックアップのポリシー

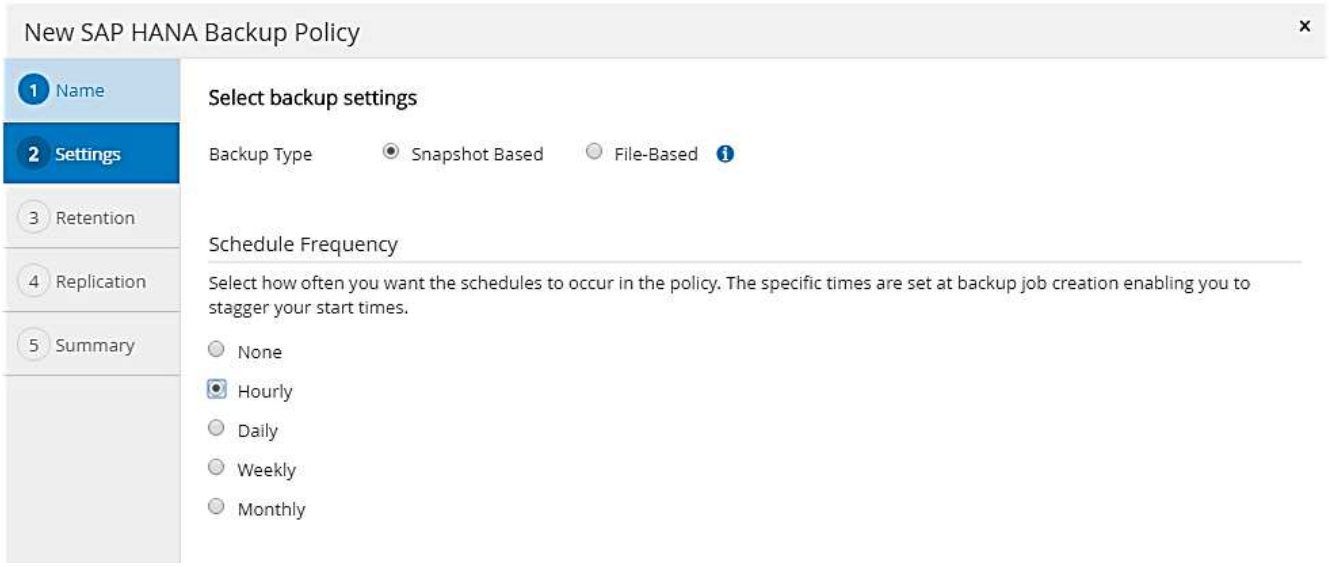
1. [設定] 、 [ポリシー] の順に移動し、 [新規] をクリックします



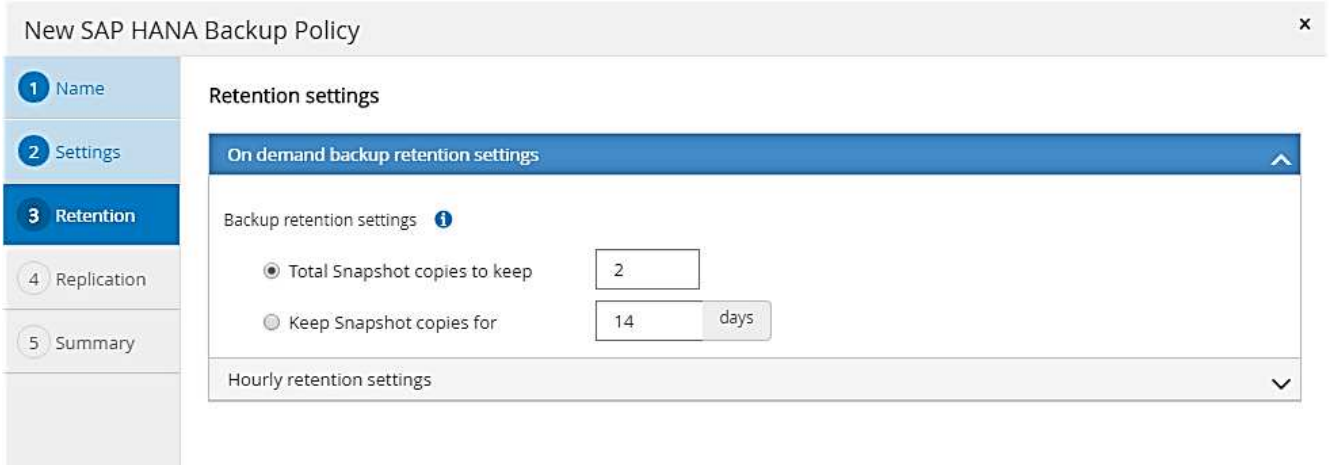
2. ポリシー名と概要を入力します。次へをクリックします。



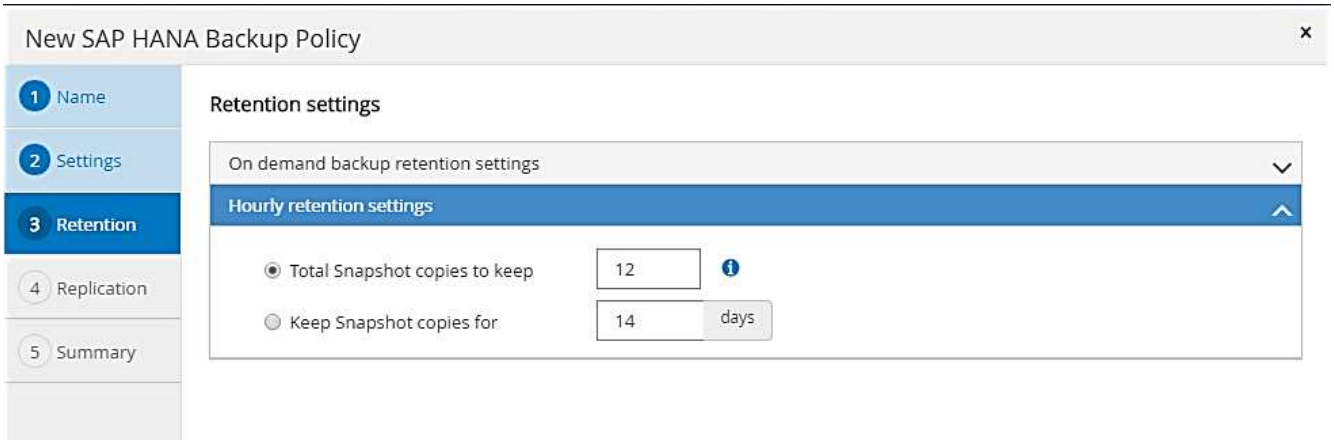
3. バックアップタイプとして「 Snapshot Based 」を選択し、スケジュール頻度を選択するには「 Hourly 」を選択します。



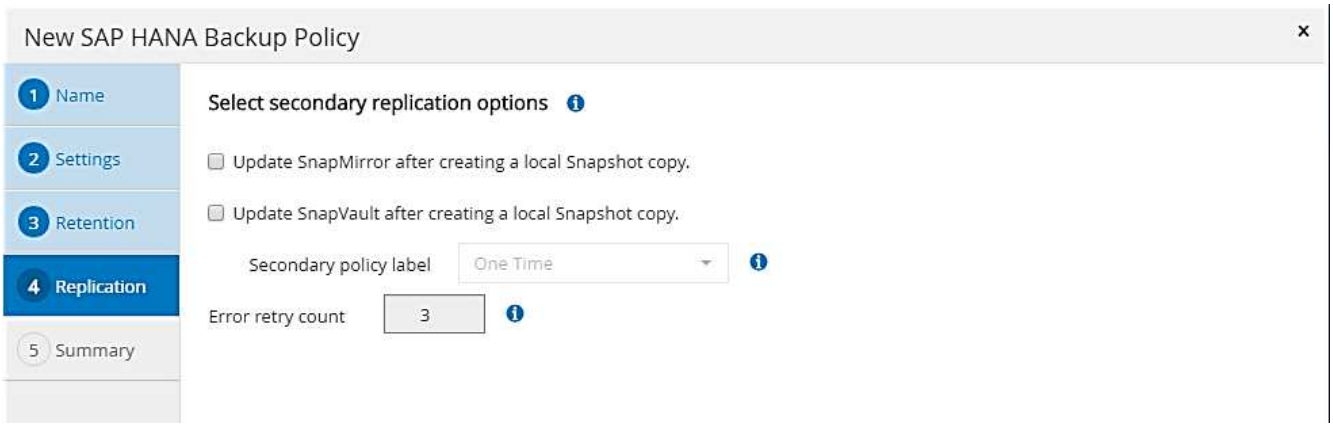
4. オンデマンドバックアップの保持を設定します。



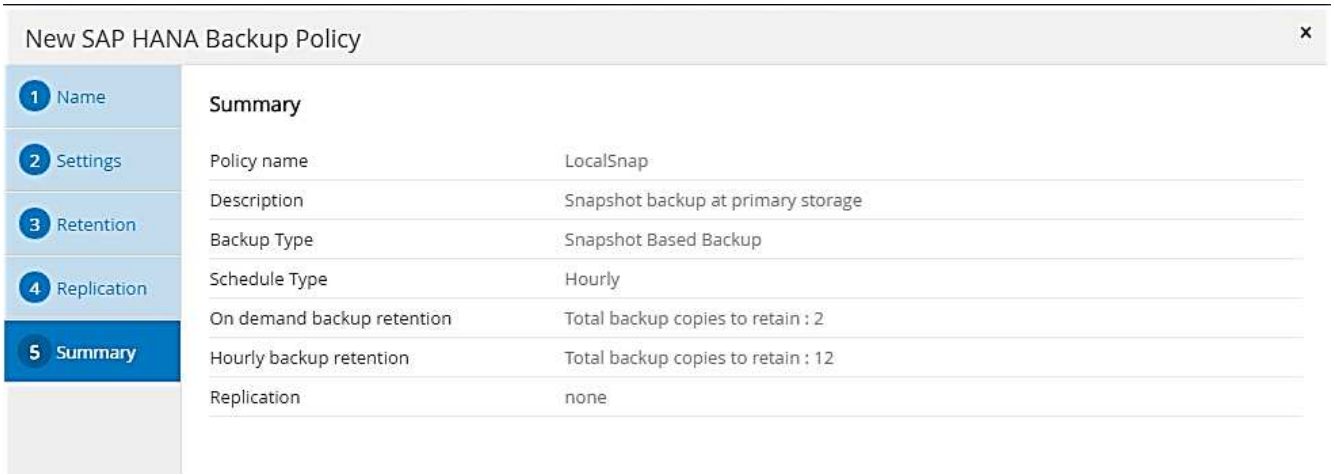
5. スケジュールされたバックアップの保持を設定します。



6. レプリケーションオプションを設定します。この場合、 SnapVault または SnapMirror の更新は選択されていません。

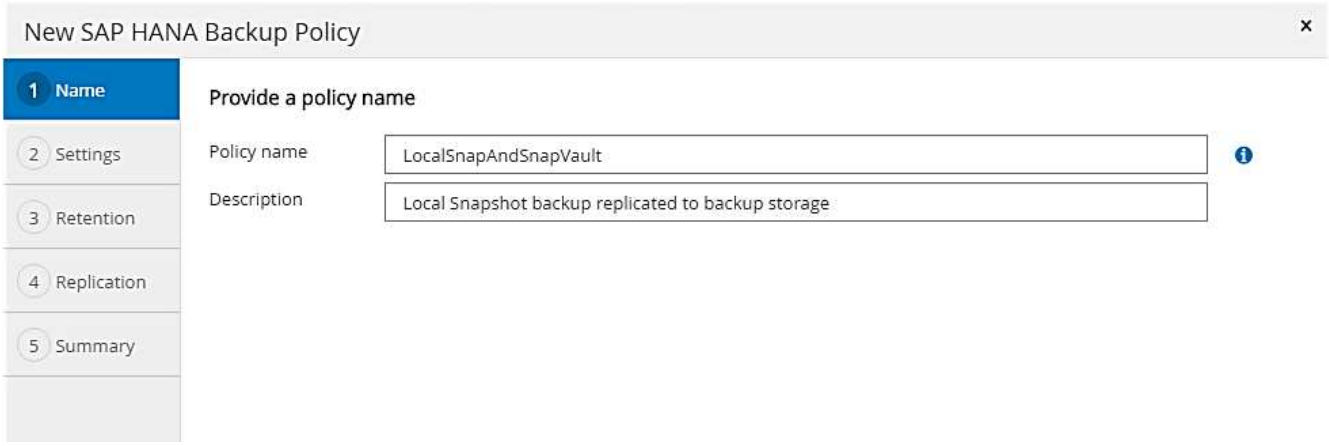


7. [概要] ページで、 [完了] をクリックします。

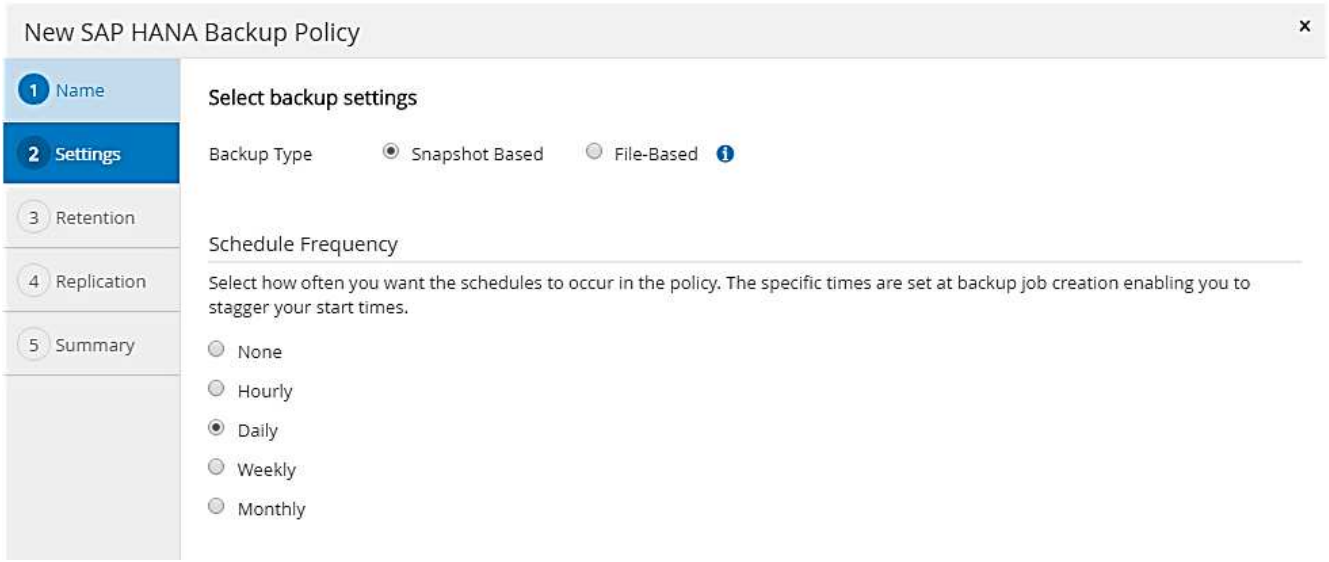


SnapVault レプリケーションを行う日次 **Snapshot** バックアップのポリシー

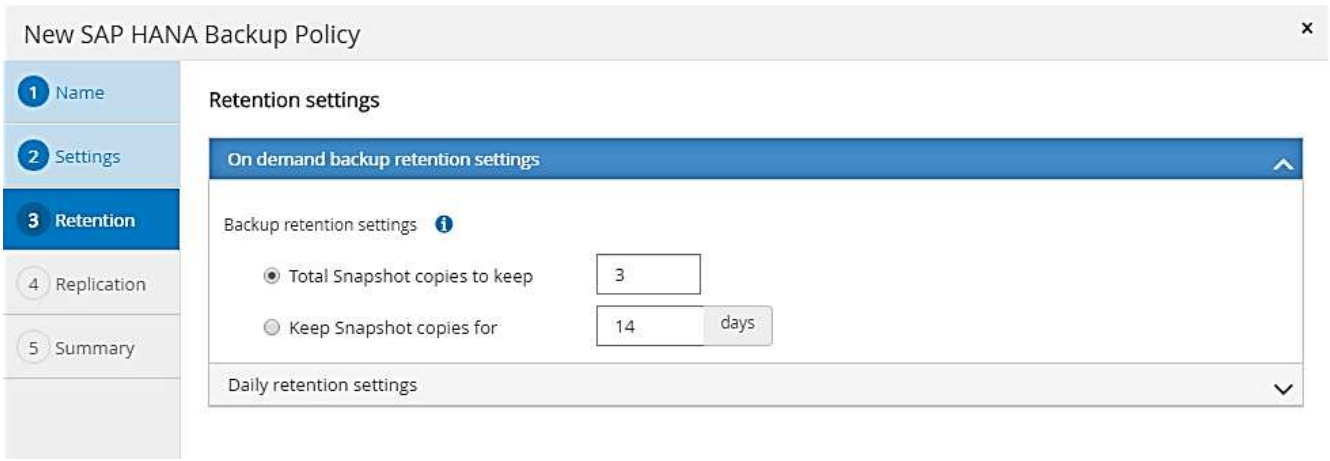
1. [設定] 、 [ポリシー] の順に移動し、 [新規] をクリックします
2. ポリシー名と概要を入力します。次へをクリックします。



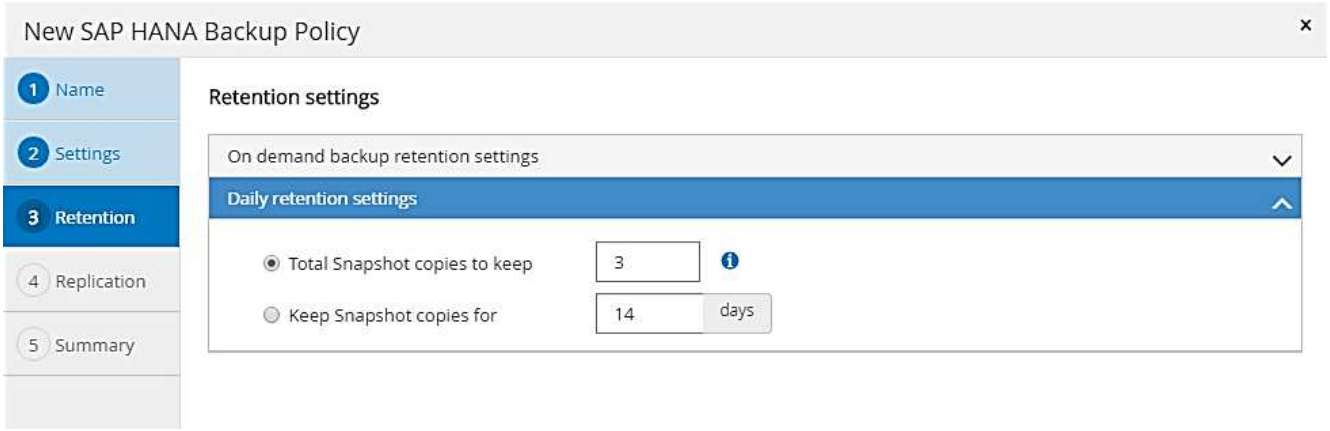
3. バックアップタイプを Snapshot ベースに、スケジュール頻度を「毎日」に設定します。



4. オンデマンドバックアップの保持を設定します。

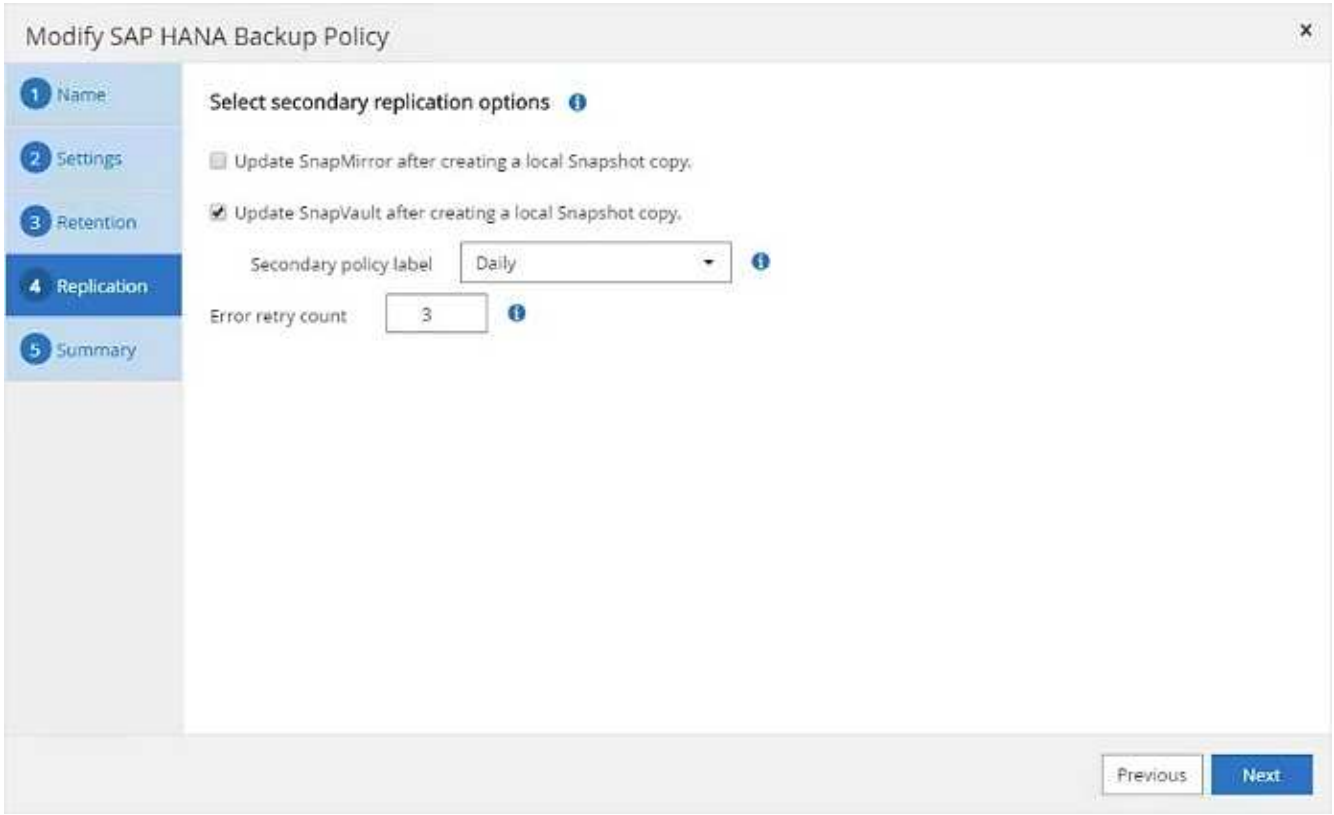


5. スケジュールされたバックアップの保持を設定します。

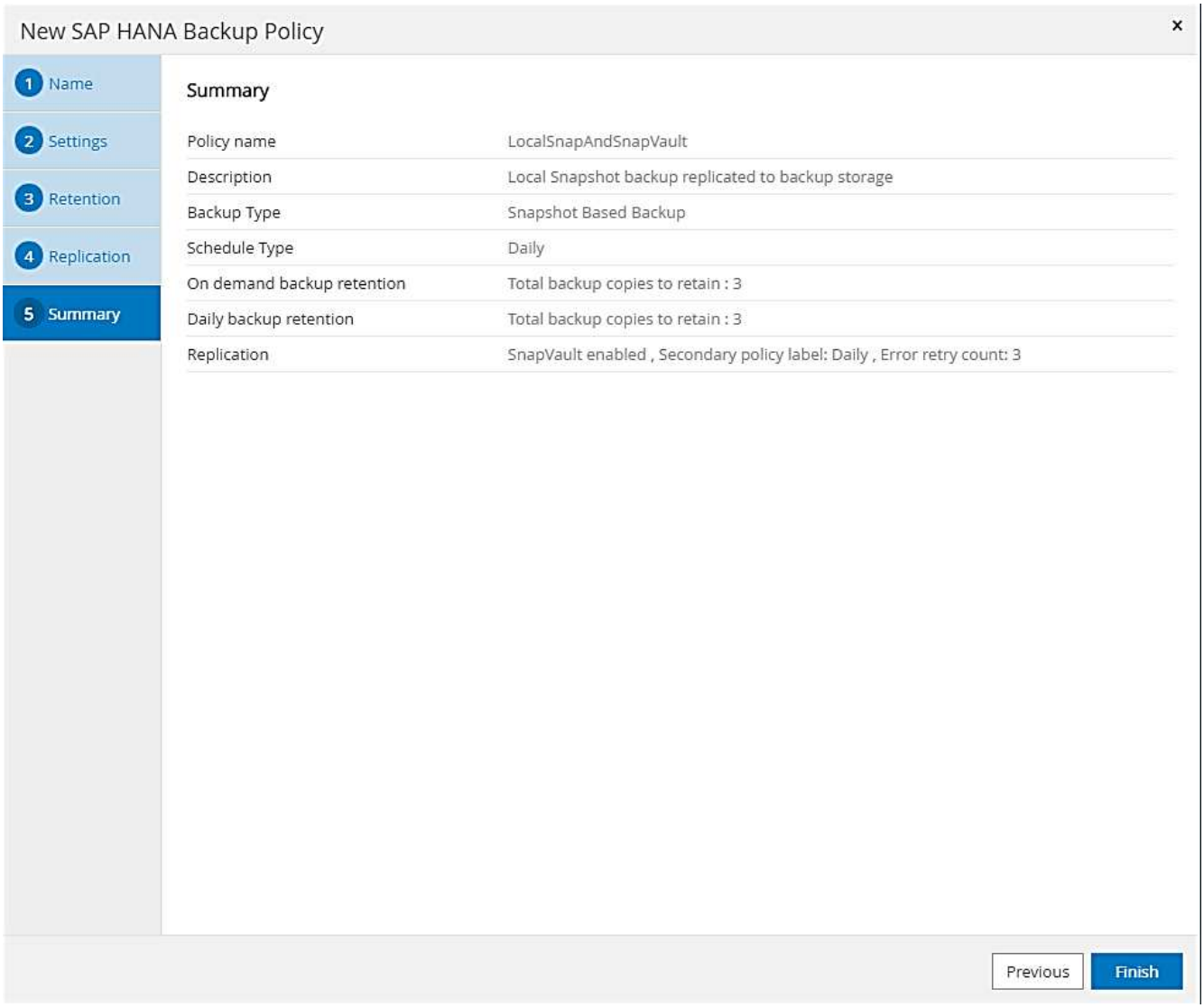


6. ローカル Snapshot コピーの作成後に SnapVault を更新するを選択します。

セカンダリポリシーのラベルは、ストレージレイヤのデータ保護設定の SnapMirror ラベルと同じにする必要があります。を参照してください "「オフサイトのバックアップストレージへのデータ保護の構成」"

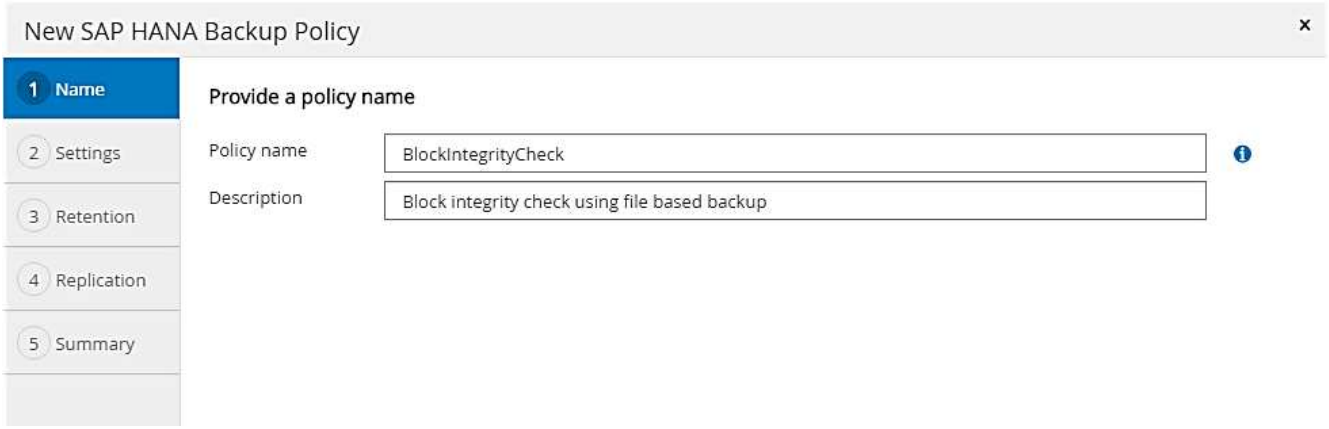


7. [概要] ページで、 [完了] をクリックします。

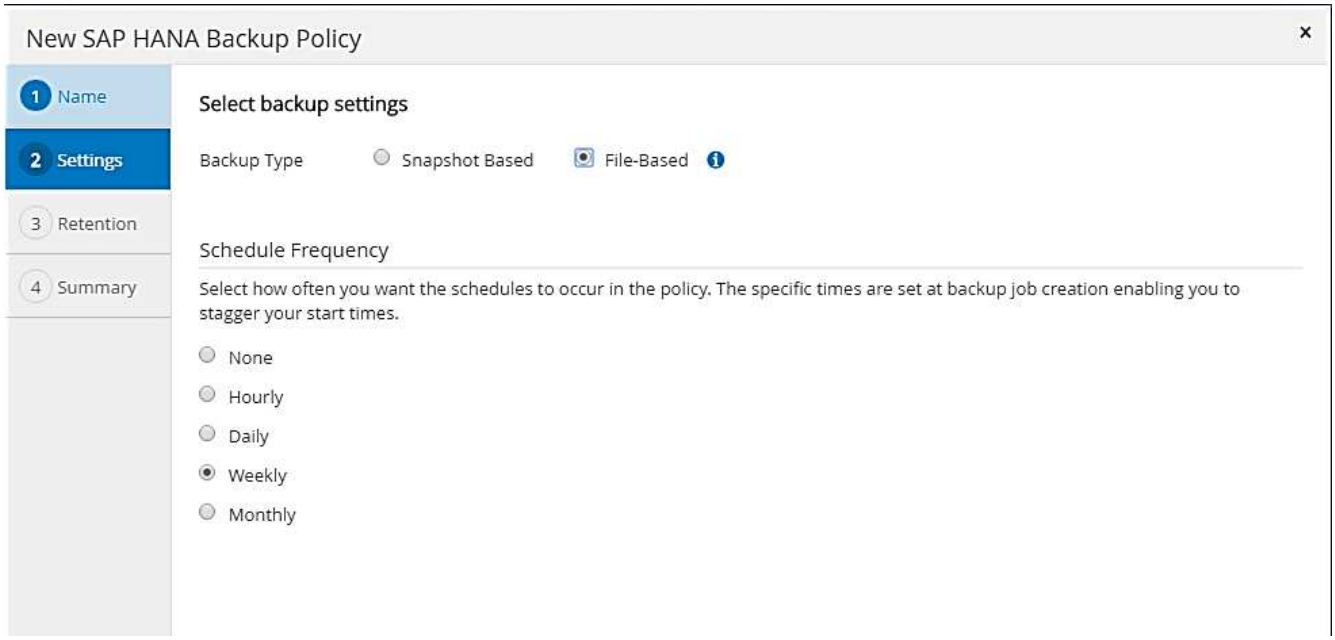


週次ブロック整合性チェックのポリシー

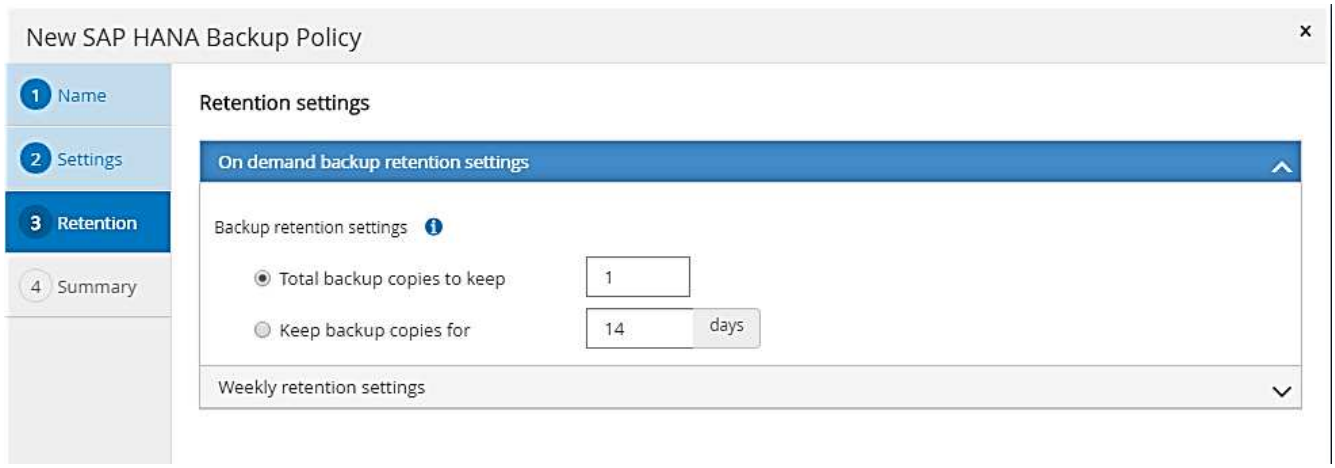
1. [設定] 、 [ポリシー] の順に移動し、 [新規] をクリックします
2. ポリシー名と概要を入力します。次へをクリックします。



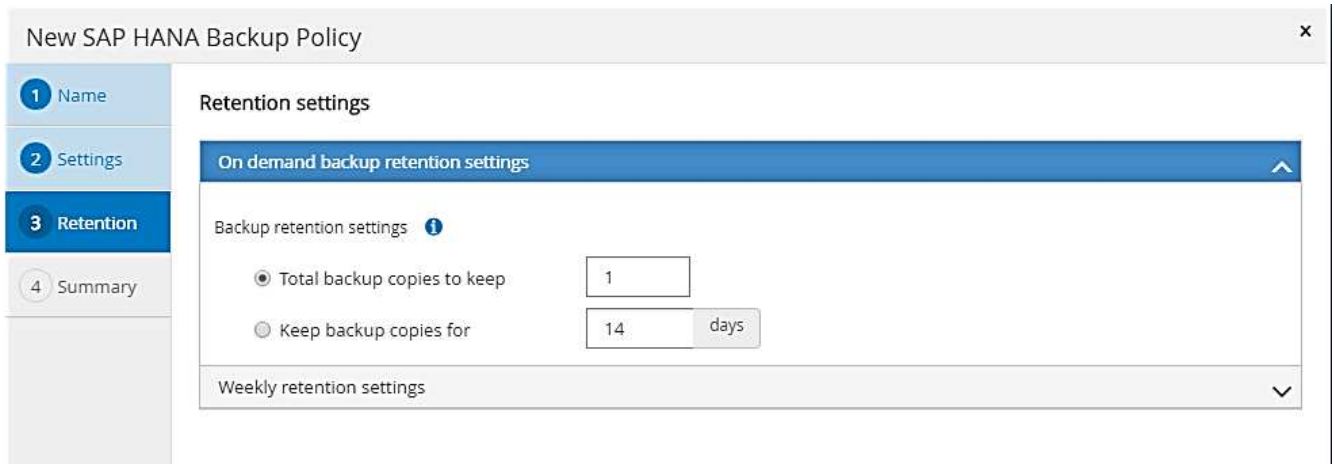
3. バックアップタイプを「ファイルベース」に、スケジュール頻度を「毎週」に設定します。



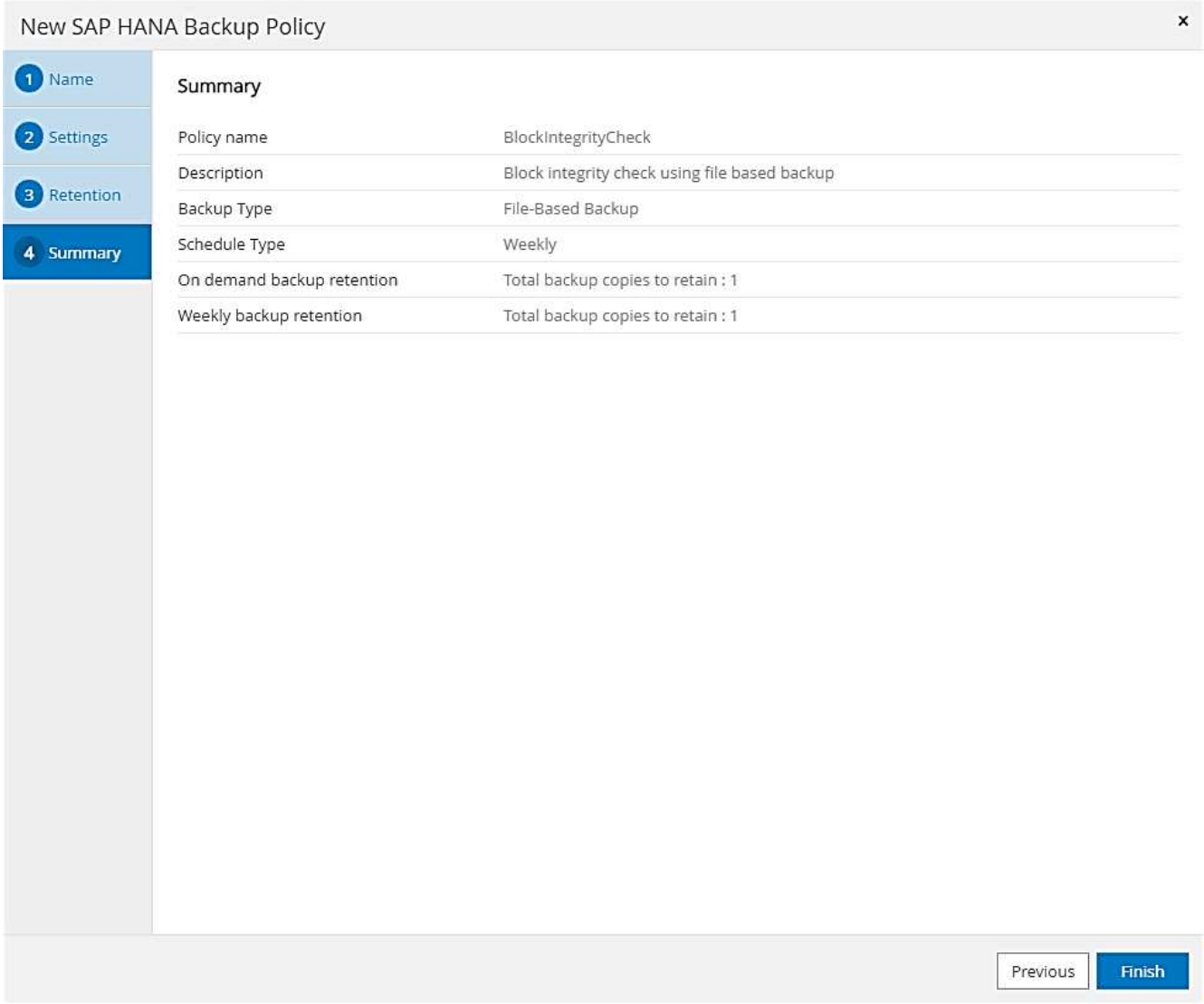
4. オンデマンドバックアップの保持を設定します。



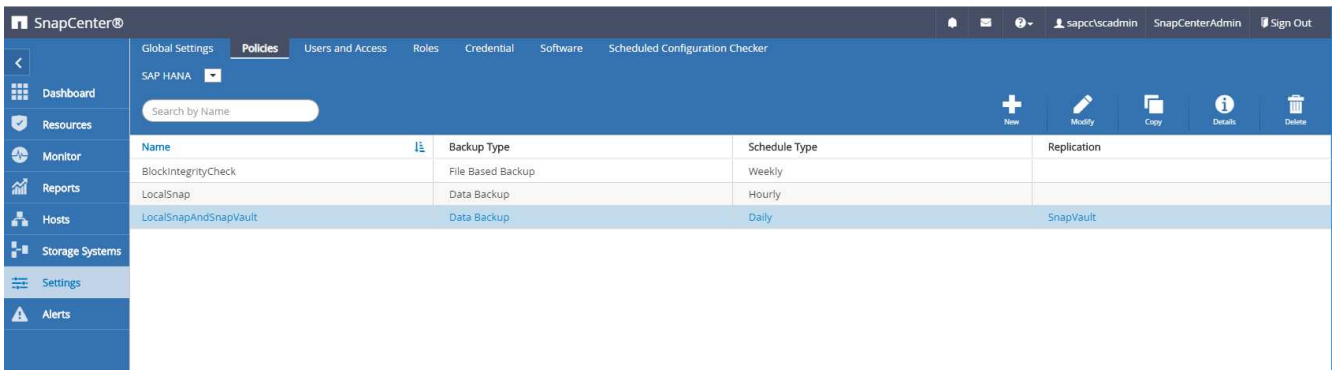
5. スケジュールされたバックアップの保持を設定します。



6. [概要] ページで、 [完了] をクリックします。



次の図に、設定されているポリシーの概要を示します。



SAP HANA データベースのバックアップ用の SnapCenter リソース固有の構成

ここでは、 2 つの設定例の設定手順について説明します。

- * SS2.*
  - ストレージアクセスに NFS を使用するシングルホスト SAP HANA MDC のシングルテナントシステム
  - リソースは SnapCenter で手動で設定されます。
  - リソースは、週単位のファイルベースのバックアップを使用して、 SAP HANA データベースのローカル Snapshot バックアップを作成し、ブロック整合性チェックを実行するように設定されています。
- * SS1.*
  - ストレージアクセスに NFS を使用するシングルホスト SAP HANA MDC のシングルテナントシステム
  - リソースは SnapCenter で自動検出されます。
  - リソースは、ローカル Snapshot バックアップを作成し、 SnapVault を使用してオフサイトのバックアップストレージにレプリケートし、週 1 回のファイルベースのバックアップを使用して SAP HANA データベースのブロック整合性チェックを実行するように設定されます。

SAN 接続、シングルコンテナ、またはマルチホストシステムの違いは、対応する設定またはワークフローの手順に反映されます。

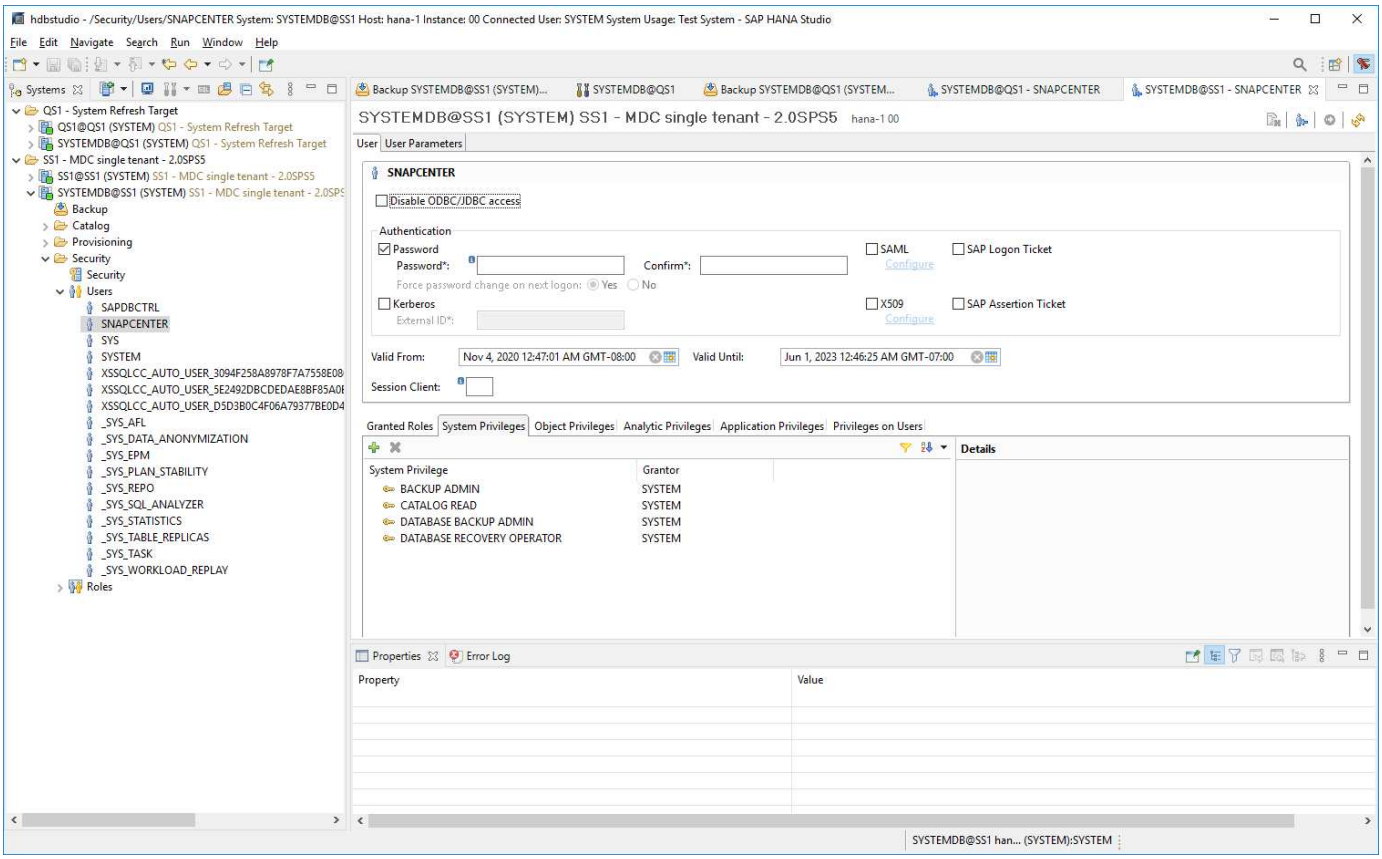
SAP HANA のバックアップユーザと hdbuserstore の設定を指定します

SnapCenter でバックアップ処理を実行するには、 HANA データベースに専用のデータベースユーザを設定することを推奨します。2 番目の手順では、このバックアップユーザ用に SAP HANA ユーザストアキーが設定され、このユーザストアキーは SnapCenter SAP HANA プラグインの構成で使用されます。

次の図は、バックアップユーザの作成に使用できる SAP HANA Studio を示しています。

必要な権限は、 HANA 2.0 SPS5 リリースで変更されています。 backup admin 、 catalog read 、 database backup admin 、および database recovery operator以前のリリースの場合は、バックアップ管理者とカタログの読み取りで十分です。

SAP HANA MDC システムの場合は、システムデータベース内にユーザを作成する必要があります。これは、システムデータベースを使用してシステムとテナントデータベースのバックアップコマンドがすべて実行されるためです。



SAP HANA プラグインと SAP hdbsql クライアントがインストールされている HANA プラグインホストで、userstore キーを設定する必要があります。

中央の **HANA** プラグインホストとして使用される **SnapCenter** サーバでのユーザストア設定

SAP HANA プラグインと SAP hdbsql クライアントが Windows にインストールされている場合、ローカルシステムユーザーは hdbsql コマンドを実行し、デフォルトでリソース設定に設定されます。システムユーザはログオンユーザではないため、ユーザストア設定は別のユーザと「 -u <User>` 」オプションを使用して行う必要があります。

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user>
<password>
```

まず、 SAP HANA hdbclient ソフトウェアを Windows ホストにインストールする必要があります。

Central HANA プラグインホストとして使用される別の **Linux** ホストでのユーザストア設定

SAP HANA プラグインと SAP hdbsql クライアントが別の Linux ホストにインストールされている場合は、リソース設定で定義されているユーザのストア設定に次のコマンドが使用されます。

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

まず、 SAP HANA hdbclient ソフトウェアを Linux ホストにインストールする必要があります。

HANA データベースホスト上のユーザストア設定

SAP HANA プラグインが HANA データベースホストに導入されている場合、ユーザストア設定には次のコマンドが使用されます。ユーザ名は「 sid>adm 」です。

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

SnapCenter は、「 <sid>adm 」ユーザを使用して HANA データベースと通信します。したがって、ユーザストアキーは、データベースホスト上の <%sid>adm` ユーザを使用して設定する必要があります。

通常、 SAP HANA hdbsql クライアントソフトウェアは、データベースサーバのインストールと一緒にインストールされます。そうでない場合は、先に hdbclient をインストールする必要があります。

ユーザストアの構成は、 **HANA** システムのアーキテクチャに応じて異なります

SAP HANA MDC のシングルテナント構成では、ポート「 3 」はシステムデータベースへの SQL アクセス用の標準ポートであり、 hdbuserstore 構成で使用する必要があります。

SAP HANA シングルコンテナ設定の場合、ポート「 3<instanceNo>15 」はインデックスサーバへの SQL アクセス用の標準ポートであり、 hdbuserstore 設定で使用する必要があります。

SAP HANA マルチホストを設定する場合は、すべてのホストのユーザストアキーを設定する必要があります。SnapCenter は指定された各キーを使用してデータベースへの接続を試みます。そのため、異なるホストへの SAP HANA サービスのフェイルオーバーとは独立して動作します。

Userstore の構成例

このラボ環境では、 SAP HANA プラグインが混在した環境を使用します。HANA プラグインは、一部の HANA システムの SnapCenter サーバにインストールされ、他のシステムの個々の HANA データベースサーバに導入されます。

- SAP HANA システム SS1 、 MDC のシングルテナント、インスタンス 00 *

HANA プラグインがデータベースホストに導入されている。したがって ' キーは 'ss1adm というユーザを持つデータベース・ホストで構成する必要があります

```
hana-1:/ # su - ss1adm
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE       : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

- SAP HANA システム MS1 、マルチホスト MDC のシングルテナント、インスタンス 00 *

HANA マルチホストシステムの場合、 SnapCenter サーバを使用したセットアップでは、中央のプラグインホストが必要です。そのため、ユーザストア設定は SnapCenter サーバ上で行う必要があります。

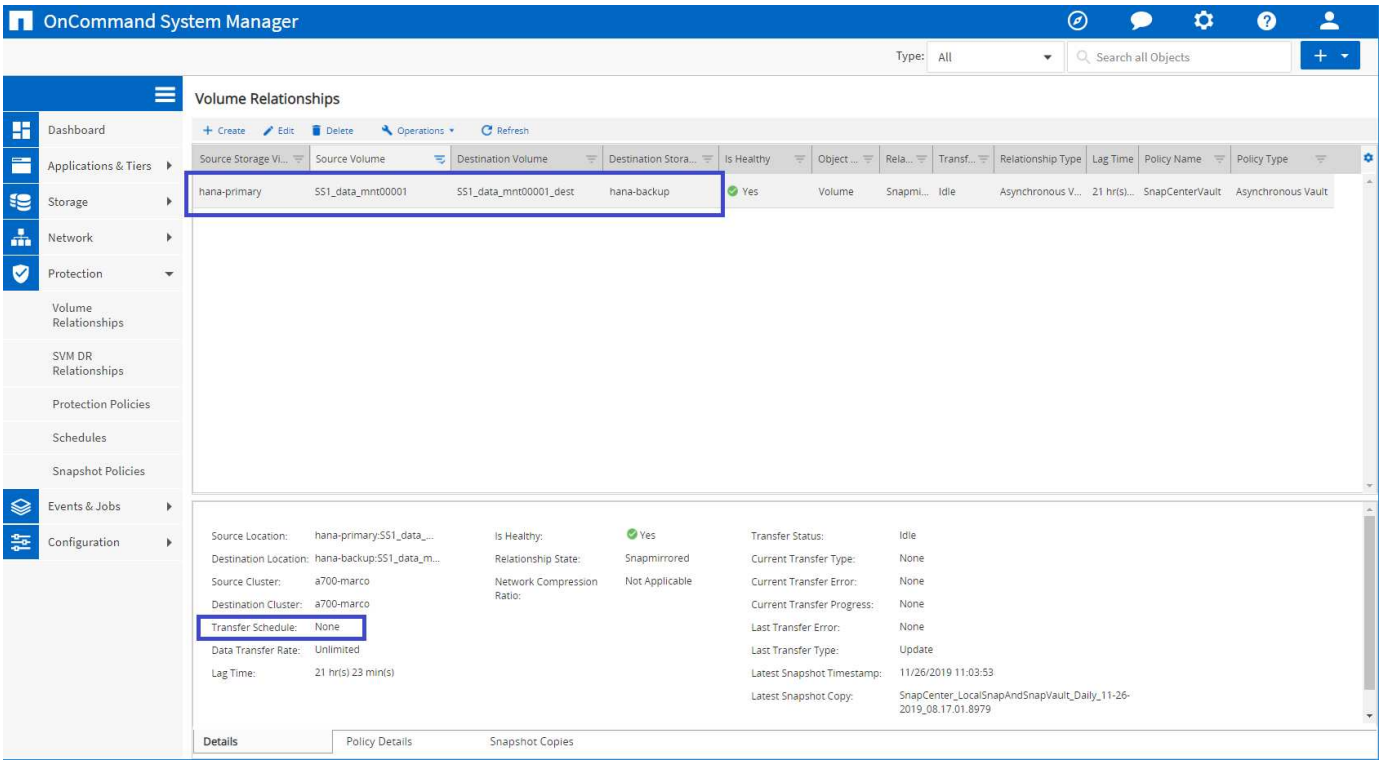
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE       : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.DAT
KEY FILE        : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
  ENV : hana-4:30013
  USER: SNAPCENTER
KEY MS1KEYHOST2
  ENV : hana-5:30013
  USER: SNAPCENTER
KEY MS1KEYHOST3
  ENV : hana-6:30013
  USER: SNAPCENTER
KEY SS2KEY
  ENV : hana-3:30013
  USER: SNAPCENTER
C:\Program Files\sap\hdbclient>
```

オフサイトのバックアップストレージにデータ保護を設定する

SnapCenter でレプリケーションの更新を管理するには、データ保護関係および最初のデータ転送の設定を実行する必要があります。

次の図は、 SAP HANA システム SS1 用に設定された保護関係を示しています。この例では、 SVM 「 HANA プライマリ」のソースボリューム「 SS1_data_mnt00001 」が SVM 「 HANA - バックアップ」とターゲットボリューム「 SS1_data_mnt00001_dest 」にレプリケートされます。

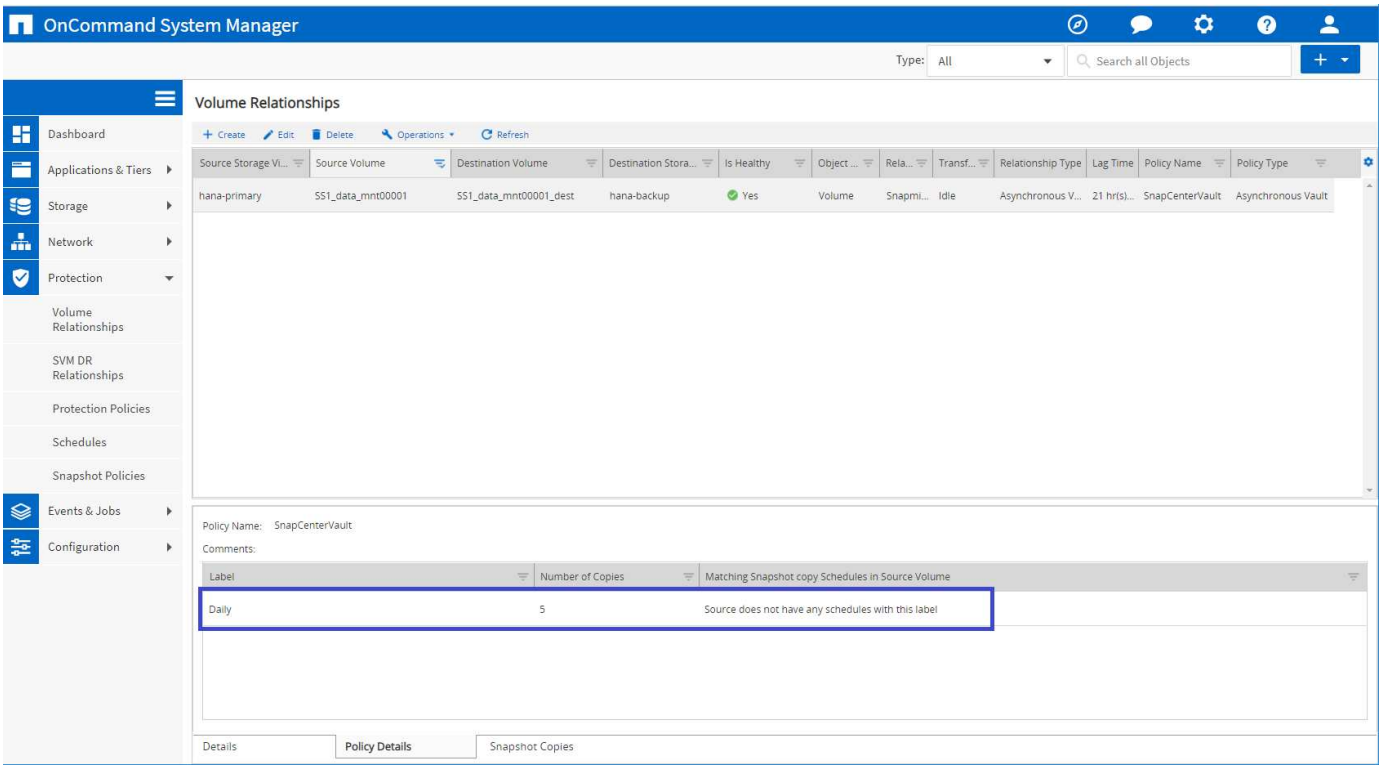
SnapCenter によって SnapVault の更新がトリガーされるため、関係のスケジュールは None に設定する必要があります。



次の図に、保護ポリシーを示します。保護関係に使用される保護ポリシーでは、セカンダリストレージでのバックアップの保持に加え、 SnapMirror ラベルも定義されます。この例では ' 使用されているラベルは毎日 ' 保存期間は 5 に設定されています

作成するポリシーの SnapMirror ラベルは、 SnapCenter ポリシーの設定で定義されたラベルと一致する必要があります。詳細については、「」を参照してくださいSnapVault レプリケーションを行う日次 Snapshot バックアップのポリシー」

オフサイトのバックアップストレージでのバックアップの保持は、ポリシーに定義され、 ONTAP によって制御されます。



HANA のリソースを手動で構成

このセクションでは、 SAP HANA リソース SS2 と MS1 を手動で設定する方法について説明します。

- SS2 は、シングルホスト MDC のシングルテナントシステムです
- MS1 は、マルチホスト MDC のシングルテナントシステムです。

a. リソースタブで、 SAP HANA を選択し、 SAP HANA データベースの追加をクリックします。

b. SAP HANA データベースを設定するための情報を入力し、 Next （次へ）をクリックします。

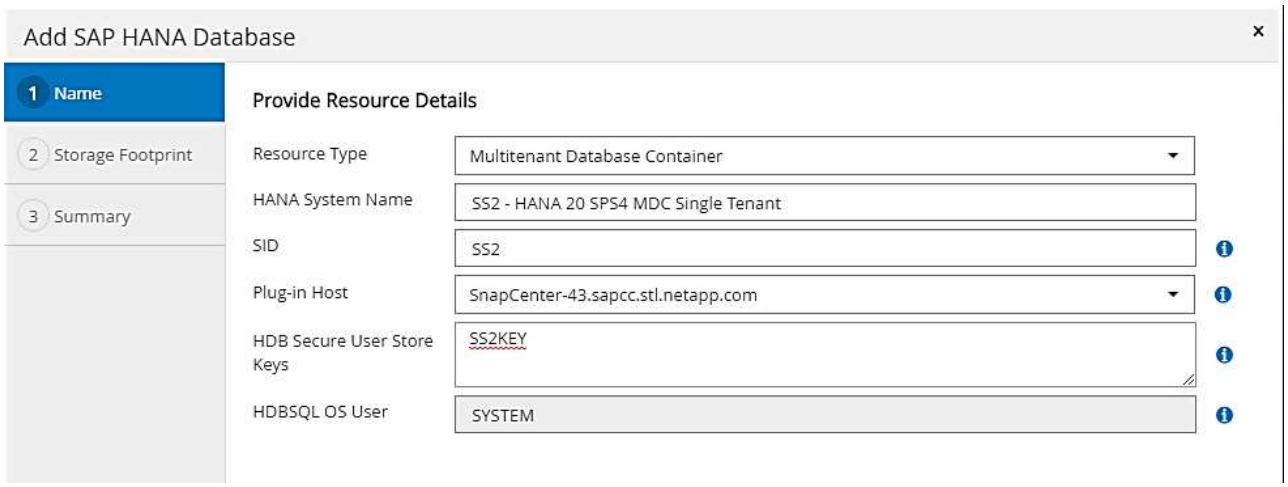
この例では、マルチテナントデータベースコンテナのリソースタイプを選択します。

> HANA シングルコンテナシステムの場合は、リソースタイプとしてシングルコンテナを選択する必要があります。他の設定手順はすべて同じです。

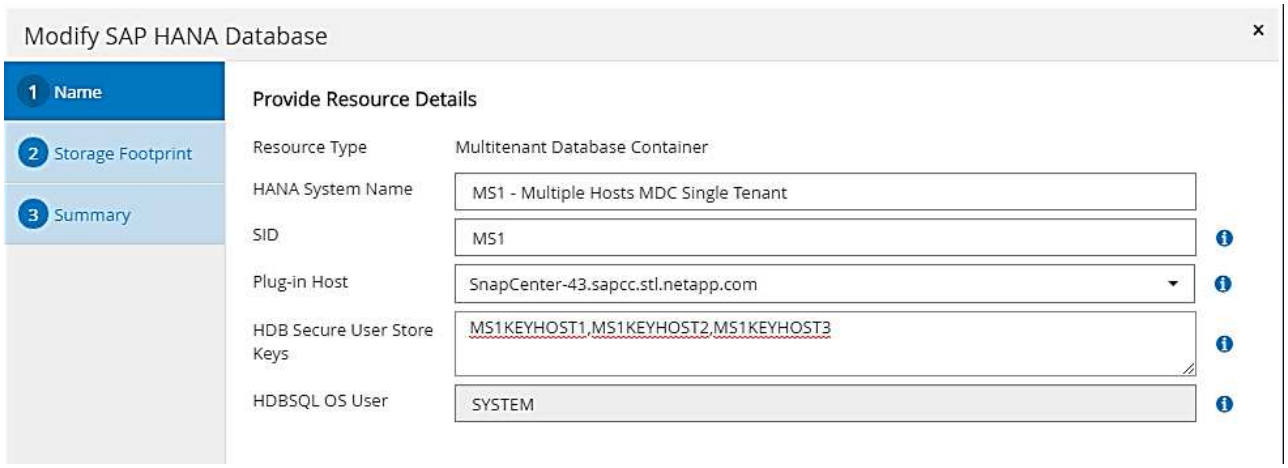
SAP HANA システムの場合、 SID は SS2 です。

この例の HANA プラグインホストは、 SnapCenter サーバです。

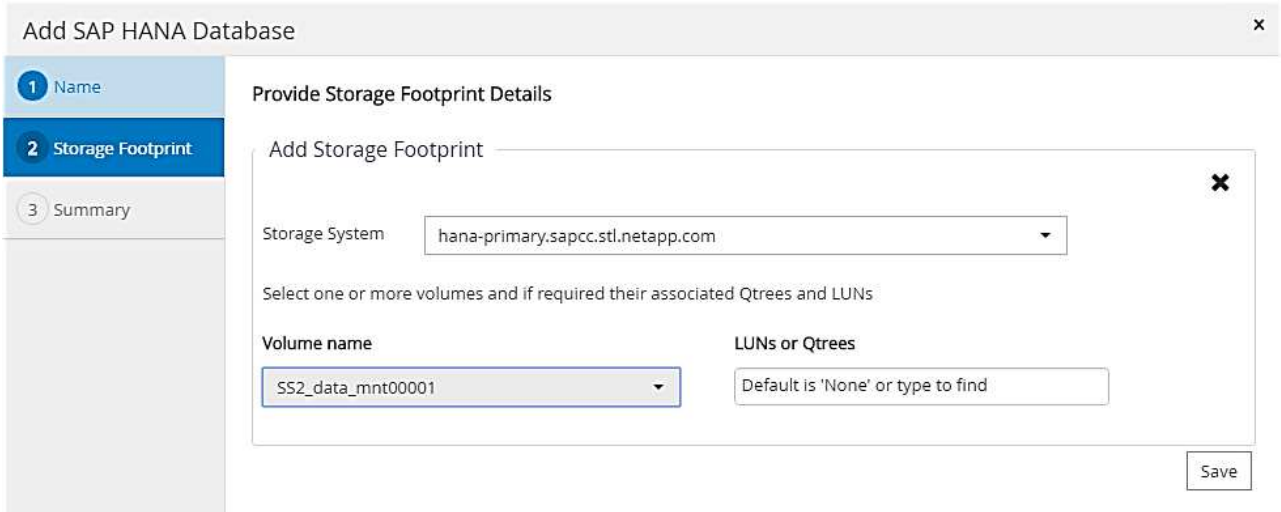
hdbuserstore キーは、 HANA データベース SS2 用に設定されたキーと一致している必要があります。この例では、 SS2KEY です。



SAP HANA マルチホストシステムの場合、次の図に示すように、すべてのホストの hdbuserstore キーを含める必要があります。SnapCenter は、リストの最初のキーとの接続を試行し、最初のキーが機能しない場合には、他のケースとの接続を続行します。これは、ワーカーホストとスタンバイホストを使用するマルチホストシステムで HANA フェイルオーバーをサポートするために必要です。

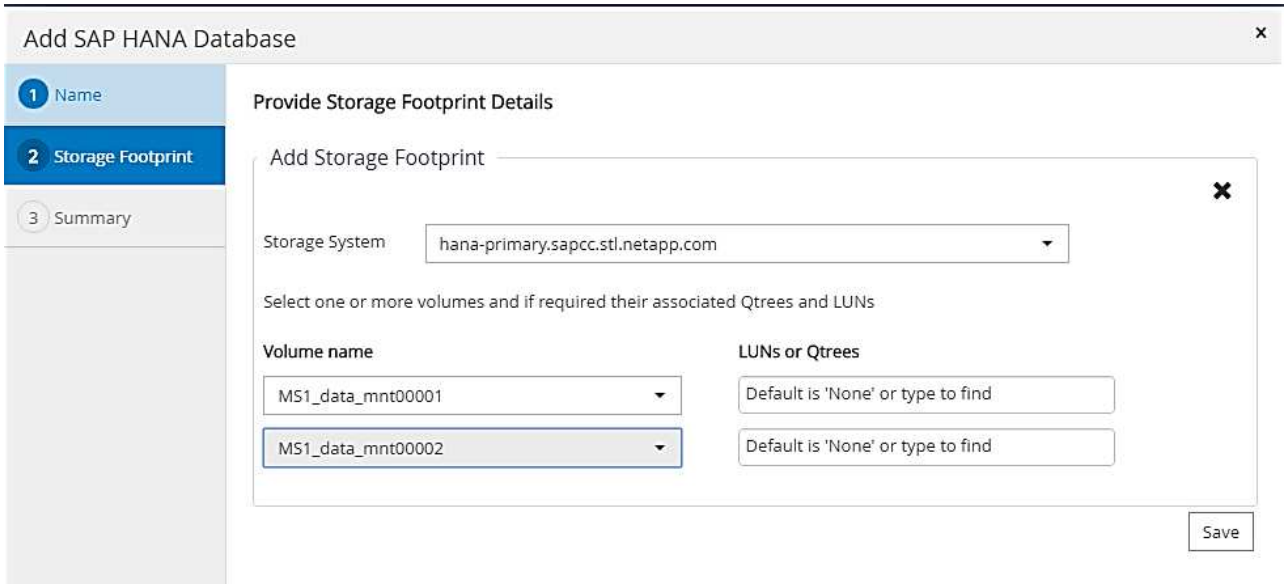


c. ストレージシステム（ SVM ）とボリューム名に必要なデータを選択します。



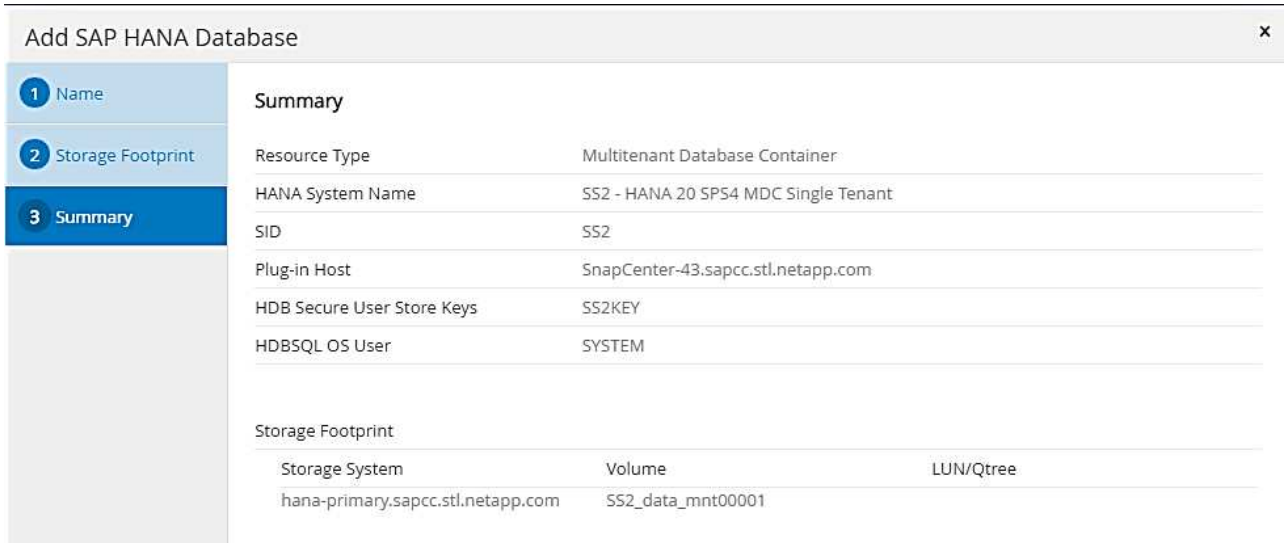
ファイバチャネル SAN 構成の場合は、 LUN も選択する必要があります。

SAP HANA マルチホストシステムの場合は、次の図に示すように、 SAP HANA システムのすべてのデータボリュームを選択する必要があります。



リソース構成の概要画面が表示されます。

a. Finish をクリックして、 SAP HANA データベースを追加します。



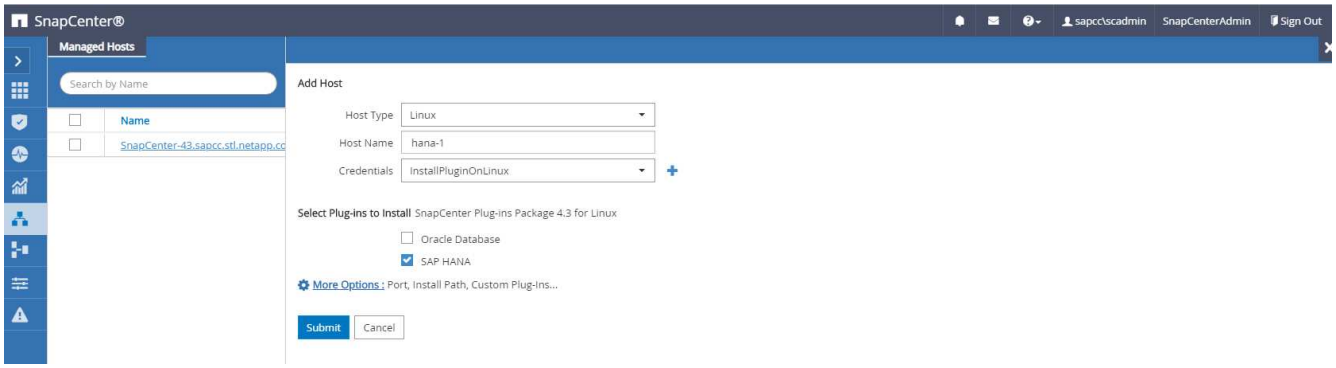
b. リソース構成が完了したら、「」の説明に従って、リソース保護の構成を実行します[リソース保護の設定]」

HANA データベースの自動検出

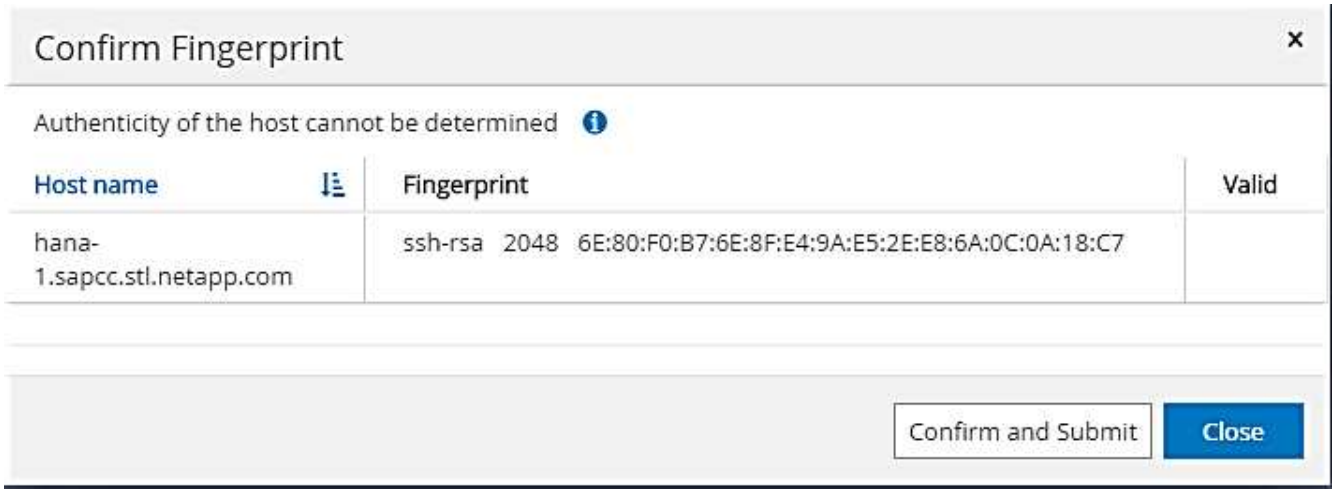
このセクションでは、 SAP HANA リソース SS1 （ NFS を使用するシングルホスト MDC シングルテナントシステム）の自動検出について説明します。ここで説明する手順はすべて、 HANA シングルコンテナ、 HANA MDC マルチテナントシステム、およびファイバチャネル SAN を使用する HANA システムで同じです。

SAP HANA プラグインには、 Java 64 ビットバージョン 1.8 が必要です。SAP HANA プラグインを導入する前に、ホストに Java をインストールする必要があります。

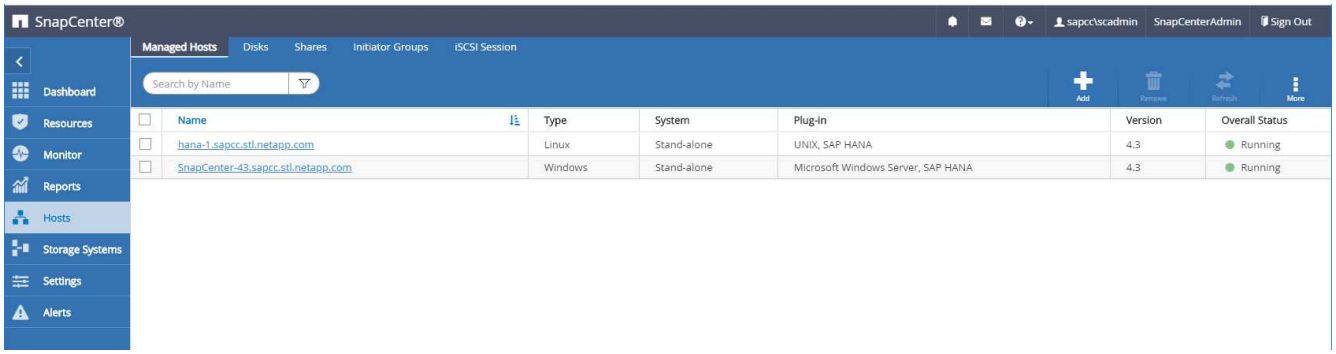
1. ホストタブで、追加をクリックします。
2. ホスト情報を入力し、インストールする SAP HANA プラグインを選択します。Submit をクリックします。



3. フィンガープリントを確認します。



HANA プラグインと Linux プラグインのインストールが自動的に開始されます。インストールが完了すると、ホストの status 列に running と表示されます。画面には、 Linux プラグインが HANA プラグインと一緒にインストールされていることも表示されます。

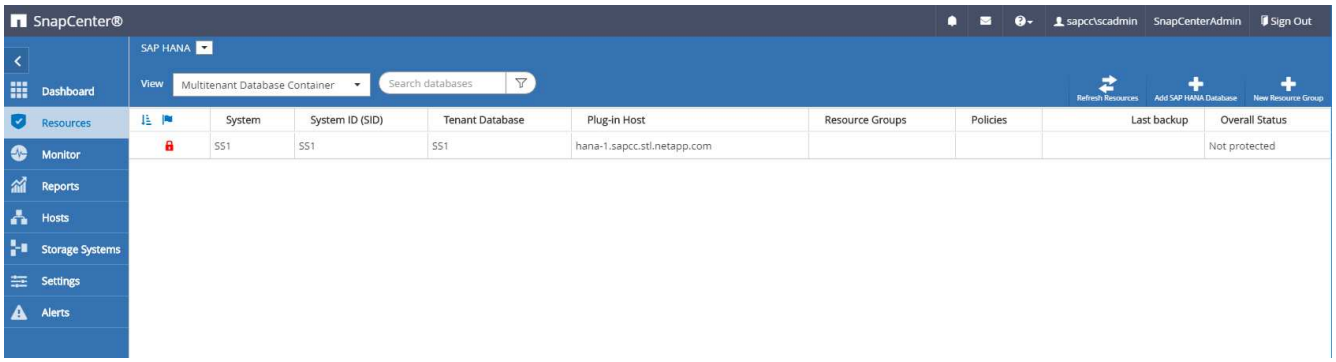


プラグインのインストール後、 HANA リソースの自動検出プロセスが自動的に開始されます。[リソース] 画面で、新しいリソースが作成されます。このリソースは、赤い南京錠のアイコンでロックされている

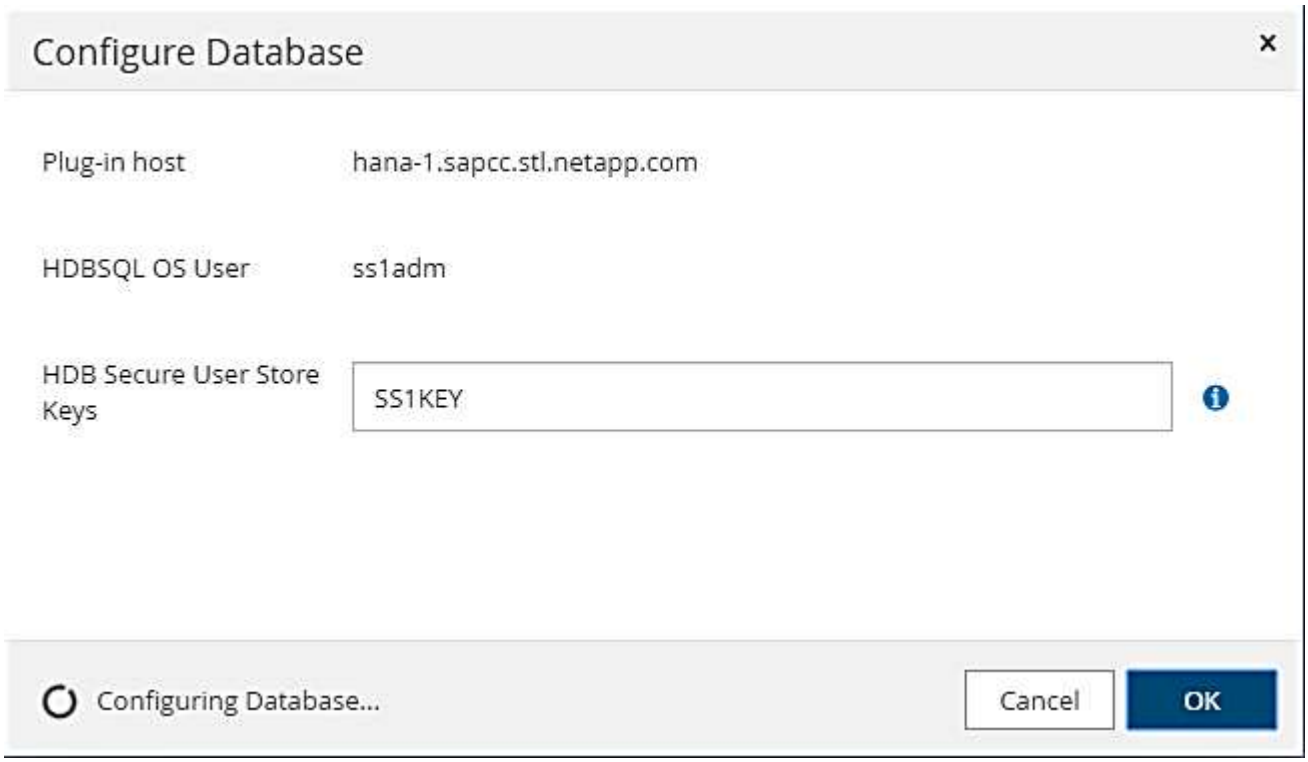
ことが示されます。

4. を選択し、をクリックして設定を続行します。

[リソースの更新] をクリックして、 [リソース] 画面で自動検出プロセスを手動で開始することもできます。

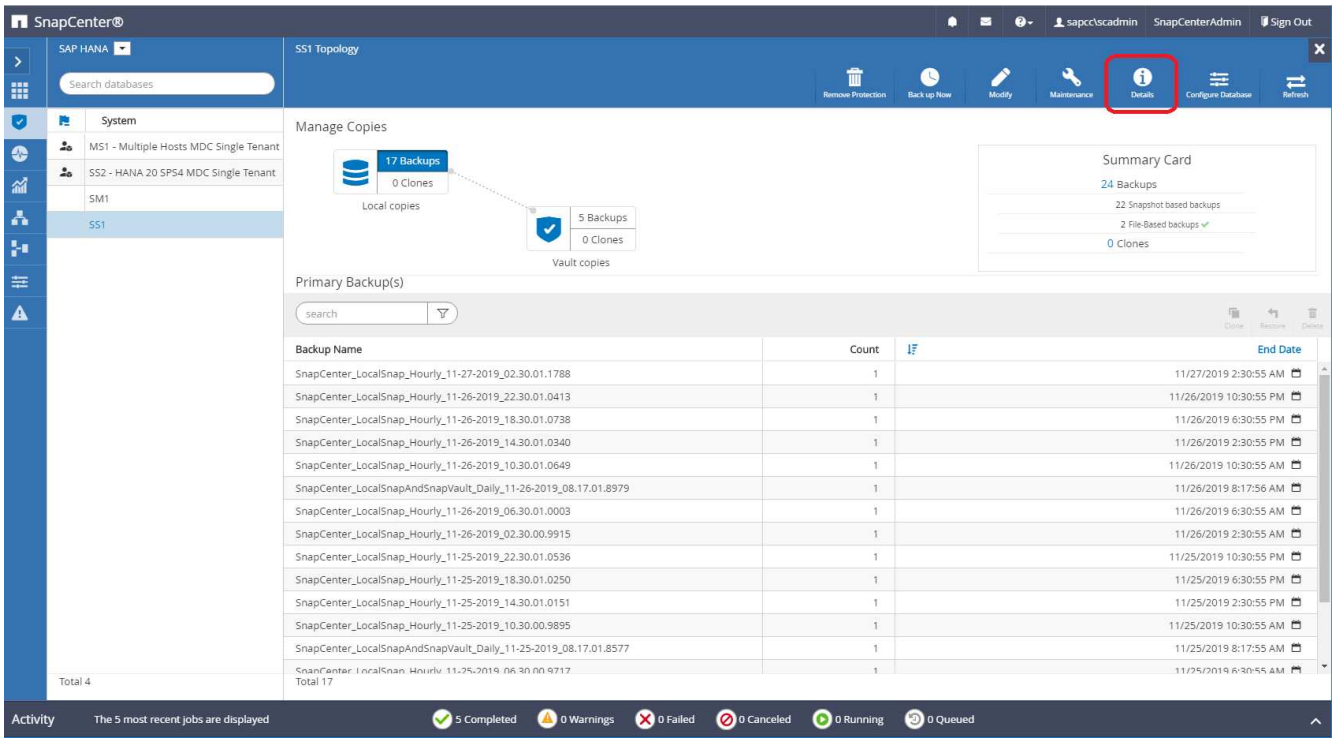


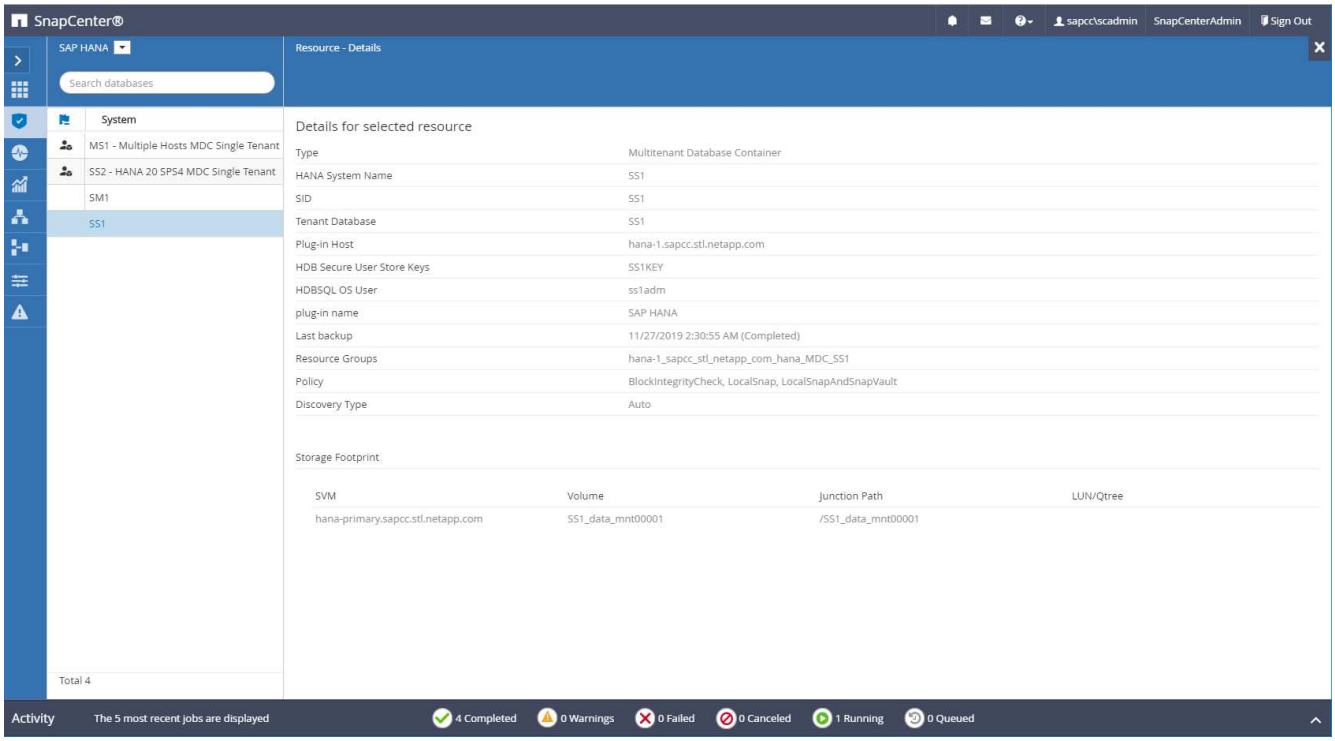
5. HANA データベースのユーザストアキーを指定します。



第 2 レベルの自動検出プロセスでは、テナントのデータとストレージのフットプリントの情報が検出されます。

6. Details をクリックして、リソーストポロジビューで HANA リソース構成情報を確認します。





リソース構成が終了したら ' 次のセクションの説明に従ってリソース保護構成を実行する必要があります

リソース保護の設定

ここでは、リソース保護の設定について説明します。リソースが自動検出されたか手動で設定されたかに関係なく、リソース保護の設定は同じです。また、すべての HANA アーキテクチャ、単一または複数のホスト、単一コンテナ、 MDC システムでも同じです。

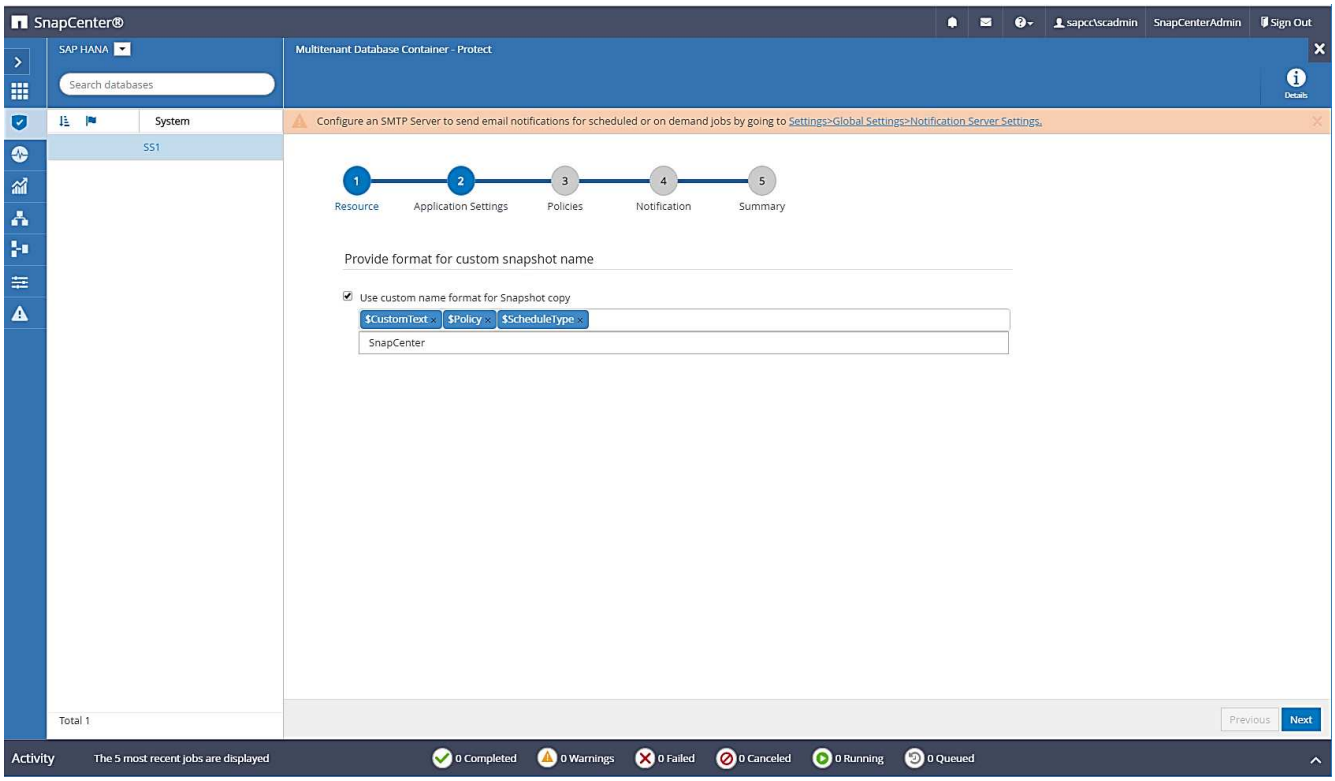
1. [リソース] タブで、リソースをダブルクリックします。
2. Snapshot コピーにカスタムの名前形式を設定します。

> カスタムの Snapshot コピー名を使用して、どのバックアップがどのポリシーおよびスケジュールタイプで作成されたかを簡単に識別することを推奨します。Snapshot コピー名にスケジュールタイプを追加することで、スケジュールバックアップとオンデマンドバックアップを区別できます。オンデマンドバックアップの「スケジュール名」文字列は空ですが、スケジュールバックアップには「毎時」、「毎日」、または「毎週」という文字列が含まれます。

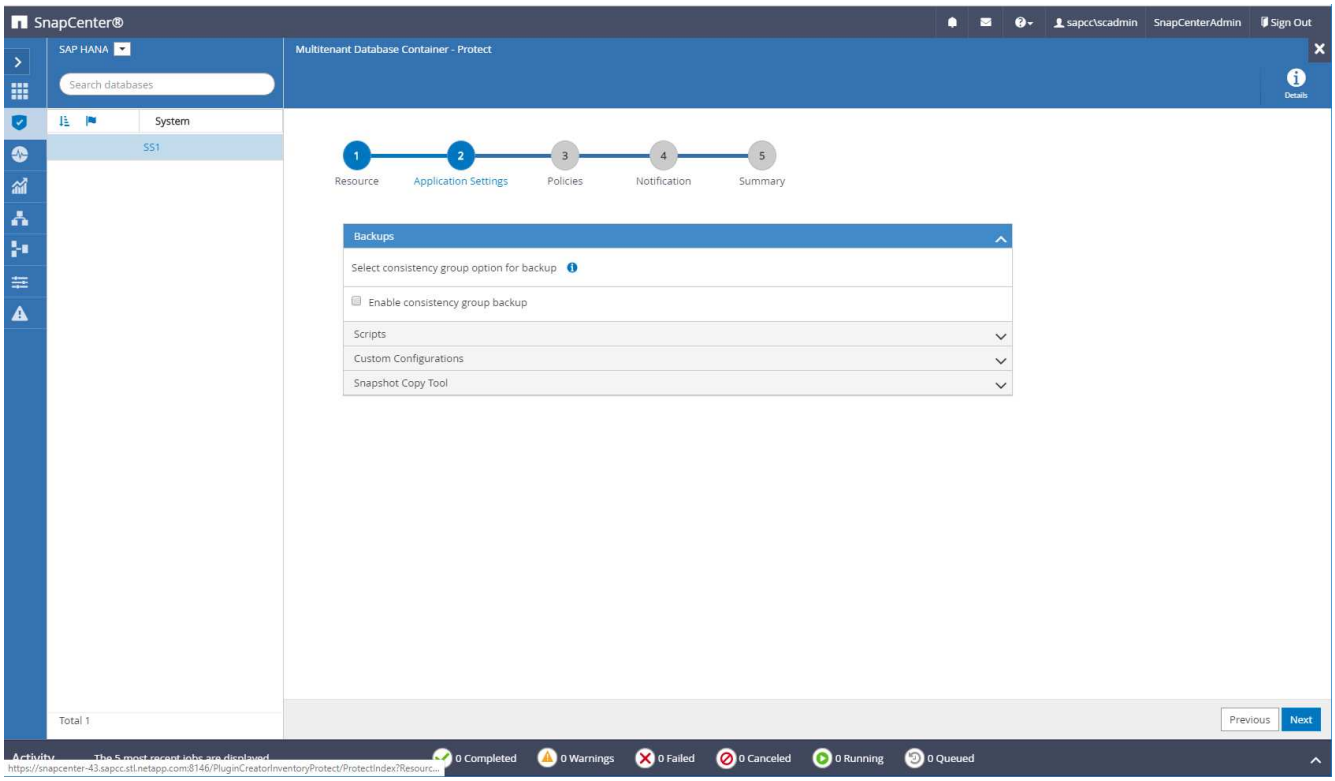
次の図に示す構成では、バックアップ名と Snapshot コピー名の形式は次のとおりです。

- 1 時間ごとのバックアップをスケジュール：「 SnapCenter *LocalSnap_Hourly*<time_stamp>` 」
- 日次バックアップのスケジュール：「 SnapCenter *LocalSnapAndSnapVault_daily*<time_stamp>`
- 時間単位のバックアップをオンデマンドで実行：「 SnapCenter *LocalSnap*<time_stamp>`
- 毎日のオンデマンドバックアップ：「 SnapCenter *LocalSnapAndSnapVault*<time_stamp>`

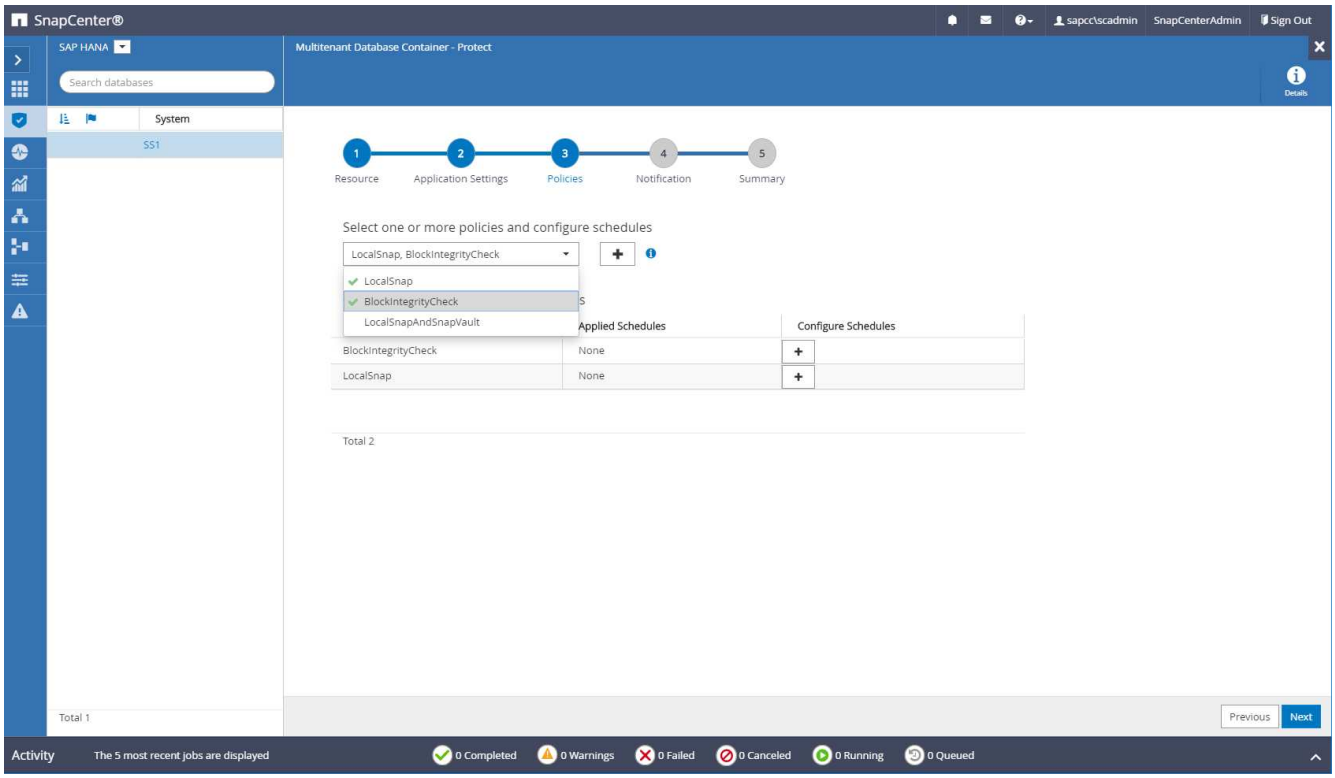
> ポリシー設定でオンデマンドバックアップに対して保持が定義されていても、不要なファイルの削除は別のオンデマンドバックアップが実行されたときにのみ実行されます。そのため、通常、 SnapCenter でオンデマンドバックアップを手動で削除して、これらのバックアップが SAP HANA バックアップカタログからも削除され、ログバックアップの不要な削除が古いオンデマンドバックアップに基づいて行われないようにする必要があります。



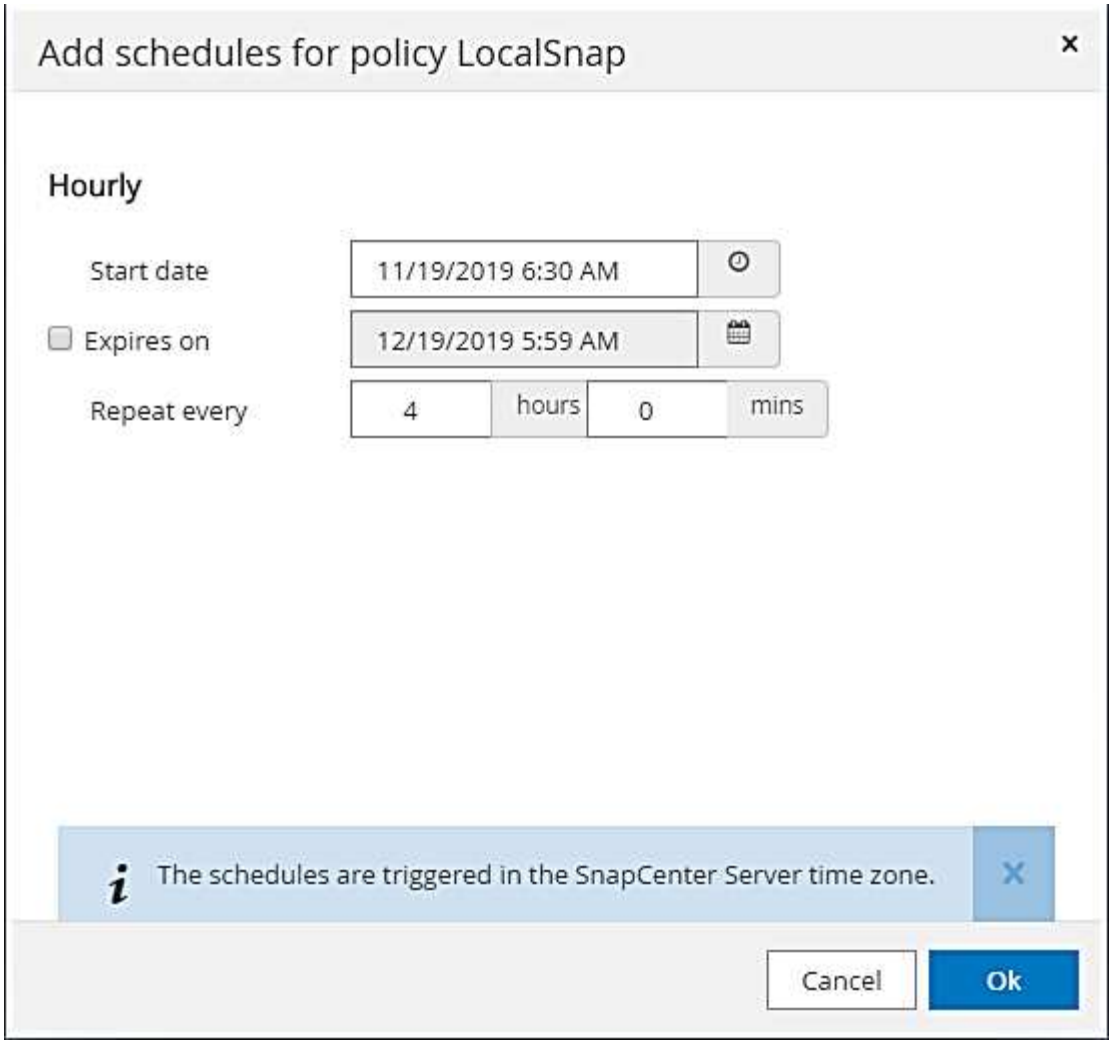
3. [アプリケーションの設定] ページで、特定の設定を行う必要はありません。次へをクリックします。



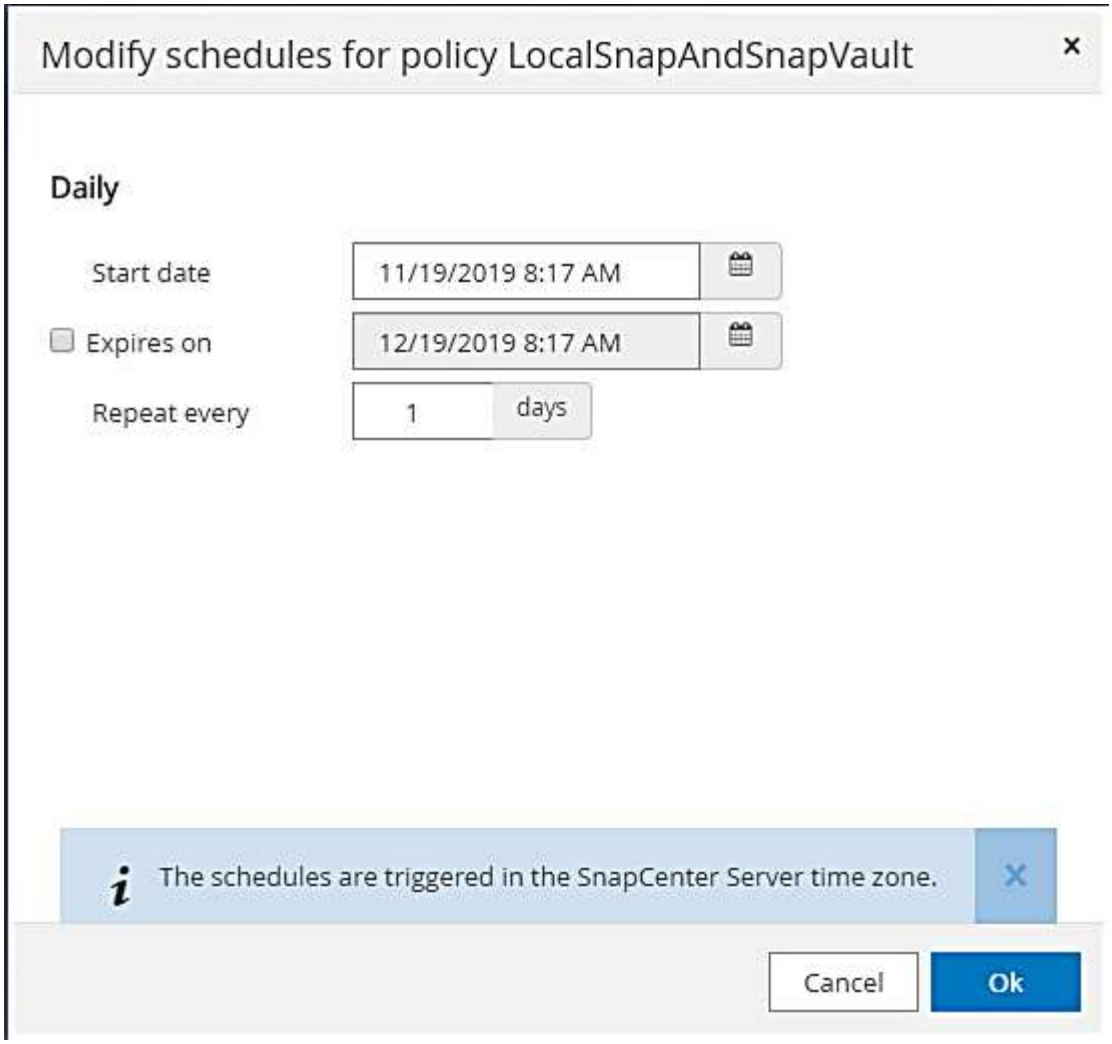
4. リソースに追加するポリシーを選択してください。



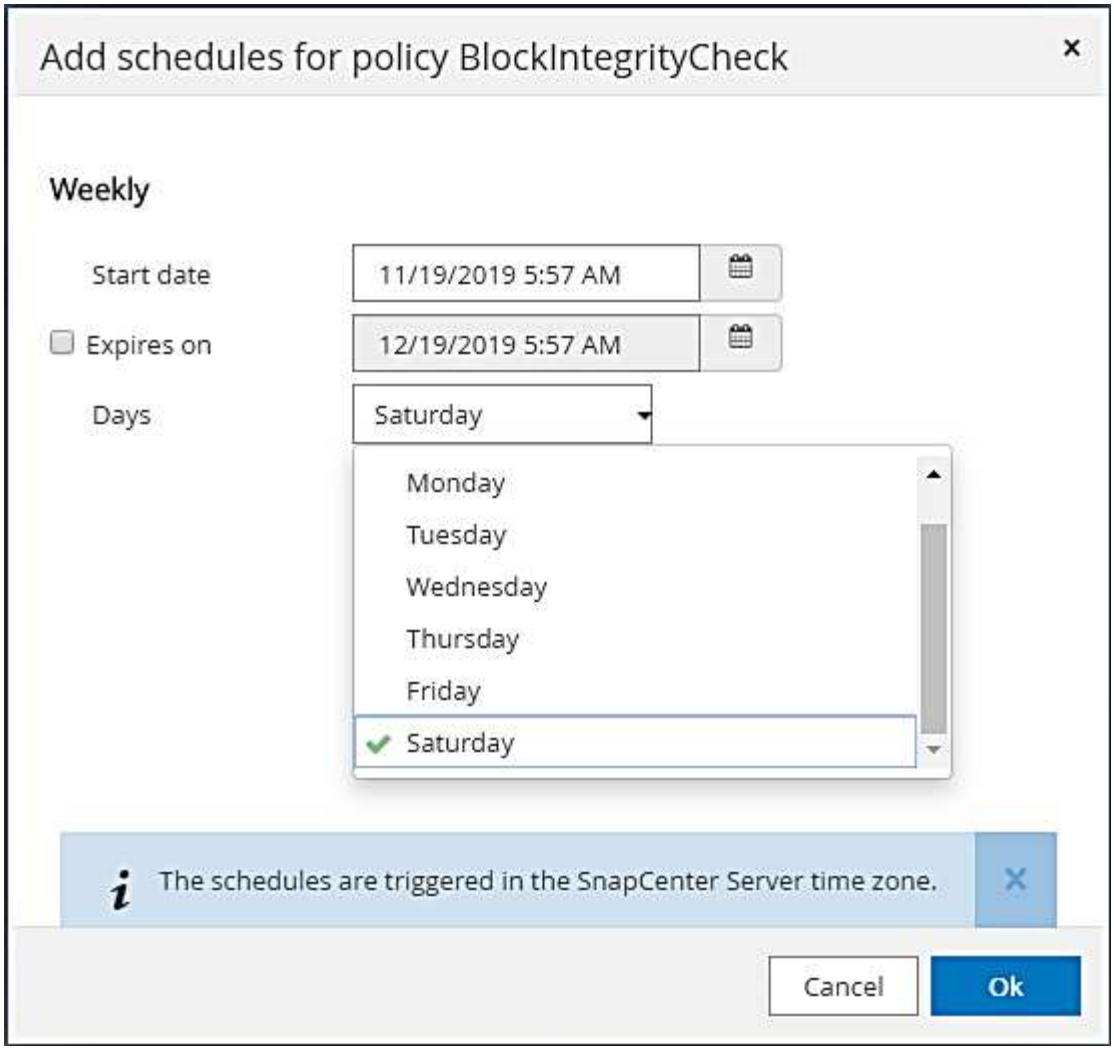
5. LocalSnap ポリシーのスケジュールを定義します（この例では 4 時間ごと）。



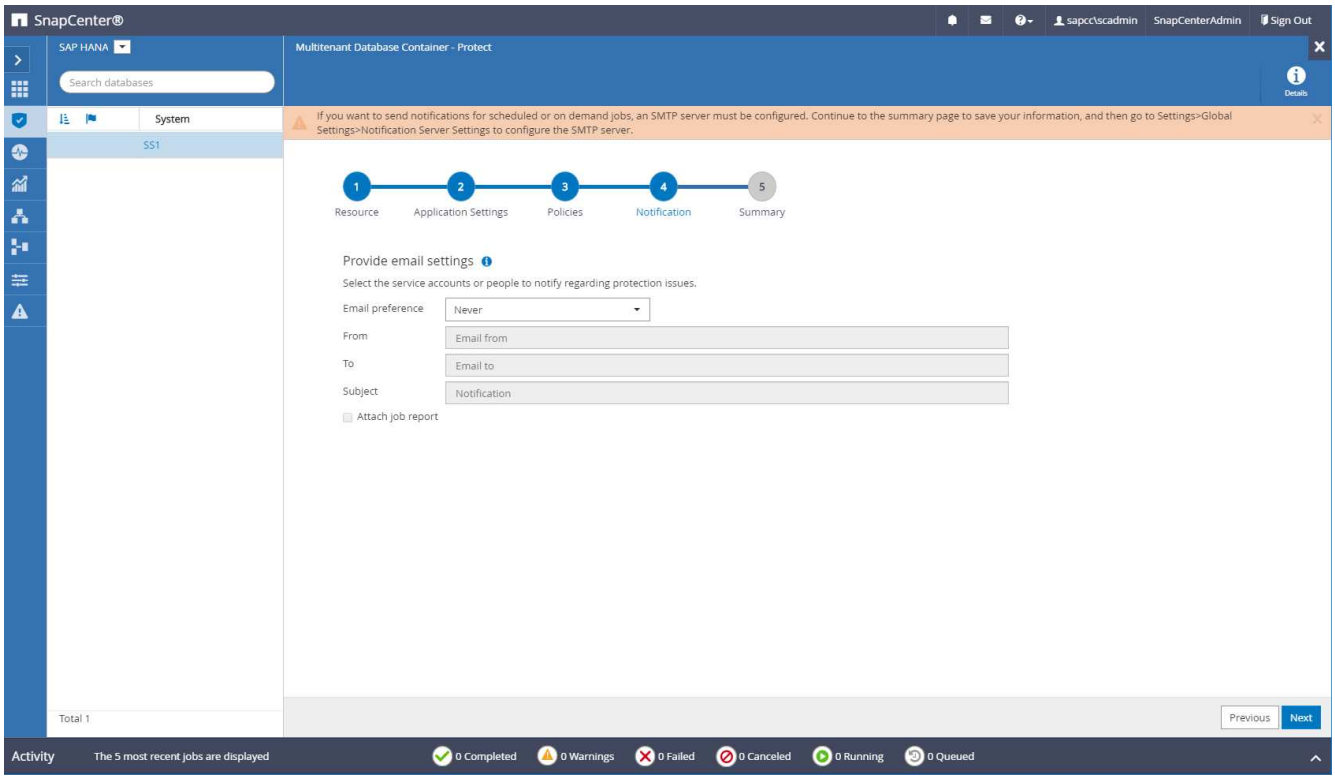
6. LocalSnapAndSnapVault ポリシーのスケジュールを定義します（この例では 1 日に 1 回）。



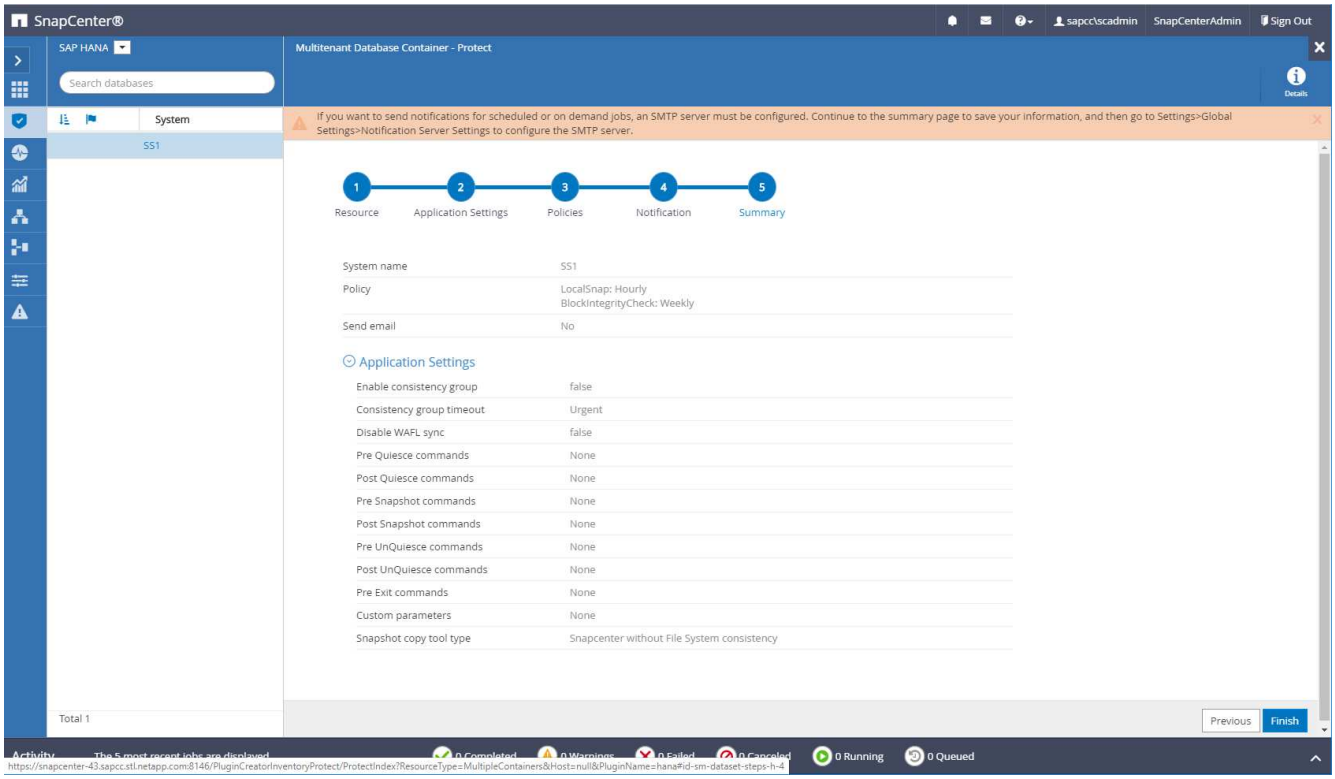
7. ブロック整合性チェックポリシーのスケジュールを定義します（この例では週に 1 回）。



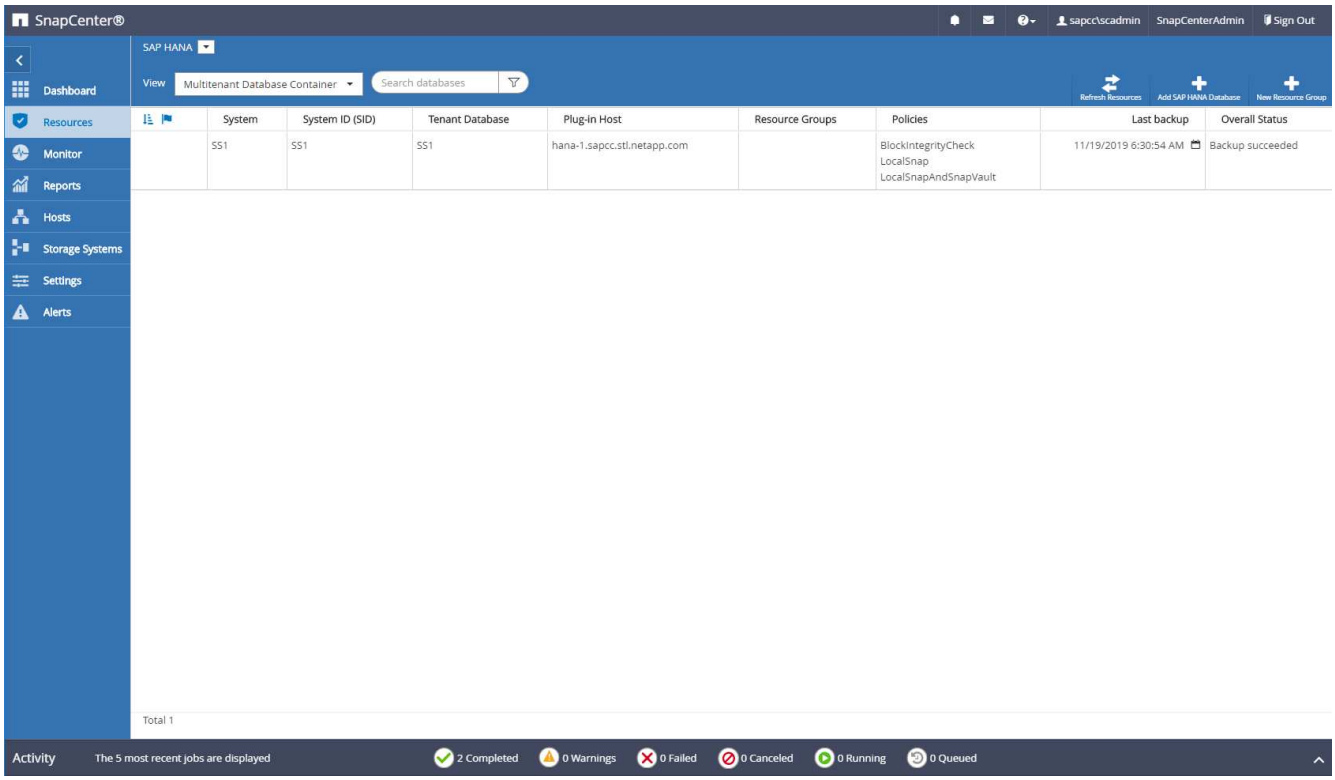
8. E メール通知に関する情報を指定します。



9. [概要] ページで、 [完了] をクリックします。



10. トポロジページでオンデマンドバックアップを作成できるようになりました。スケジュールされたバックアップは、設定に基づいて実行されます。



Fibre Channel SAN 環境向けのその他の設定手順

HANA リリースと HANA プラグインの導入方法に応じて、 SAP HANA システムがファイバチャネルと XFS ファイルシステムを使用している環境では追加の設定手順が必要です。

これらの追加の設定手順は、 SnapCenter で手動で設定した HANA リソースにのみ必要です。また、 HANA 1.0 リリースおよび HANA 2.0 リリース（ SPS2 まで）でのみ必要です。

SAP HANA の SnapCenter によって HANA のバックアップ保存ポイントがトリガーされると、 SAP HANA は、最後の手順として、テナントとデータベースサービスごとに Snapshot ID ファイルを書き込みます（例：「 /hana/data/side/mnt00001/hdb00001/snapshot_databackup_0_1 」）。これらのファイルはストレージ上のデータボリュームの一部であるため、ストレージ Snapshot コピーの一部です。このファイルは、バックアップがリストアされる場合にリカバリを実行する際に必須です。Linux ホスト上の XFS ファイルシステムを使用してメタデータをキャッシングするため、ストレージレイヤでファイルがすぐに認識されることはありません。メタデータキャッシングの標準 XFS 設定は 30 秒です。

HANA 2.0 SPS3 では、メタデータのキャッシングが問題にならないように、 SAP はこれらの Snapshot ID ファイルの書き込み処理を同期に変更しました。

SnapCenter 4.3 では、 HANA プラグインがデータベースホストに導入されている場合、ストレージの Snapshot がトリガーされる前に Linux プラグインによってホスト上でファイルシステムフラッシュ処理が実行されます。この場合、メタデータのキャッシングは問題になりません。

SnapCenter では 'XFS メタデータ・キャッシュがディスク・レイヤーにフラッシュされるまで待機する 'postquiesce コマンドを設定する必要があります

メタデータのキャッシングの実際の設定を確認するには、次のコマンドを使用します。

```
stlrx300s8-2:/ # sysctl -A | grep xfssyncd_centisecs
fs.xfs.xfssyncd_centisecs = 3000
```

「 fs.xfs.xfssyncd_centiseconds 」パラメータの 2 倍の待ち時間を使用することを推奨します。デフォルト値は 30 秒であるため、 sleep コマンドは 60 秒に設定します。

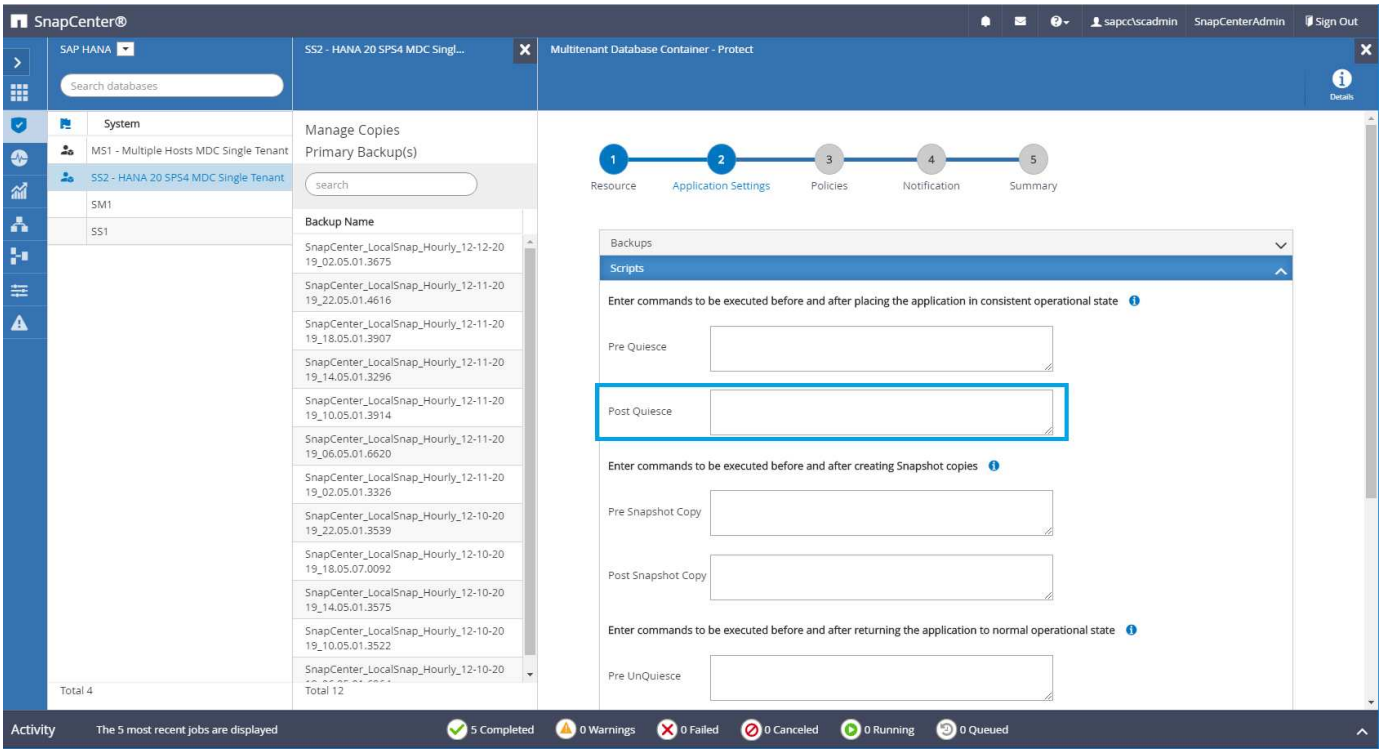
SnapCenter サーバが中央の HANA プラグインホストとして使用されている場合は、バッチファイルを使用できます。バッチファイルには、次の内容が含まれている必要があります。

```
@echo off
waitfor AnyThing /t 60 2>NUL
Exit /b 0
```

バッチファイルは、「 C ： \Program Files\NetApp\Wait60Sec.bat 」のように保存できます。リソース保護構成では、バッチファイルを [休止後に追加] コマンドとして追加する必要があります。

別の Linux ホストを中央の HANA プラグイン・ホストとして使用する場合は、 SnapCenter UI で POST Quiesce コマンドとしてコマンドの /bin/sleep 60 を設定する必要があります。

次の図に、リソース保護設定画面での休止後のコマンドを示します。



データボリューム以外のバックアップ用の **SnapCenter** リソース固有の設定

非データボリュームのバックアップは、 SAP HANA プラグインに統合された機能です。

データベースインストールリソースと必要なログが残っていれば、データベースデータボリュームを保護して特定の時点に SAP HANA データベースをリストアおよびリカバリするだけで十分です。

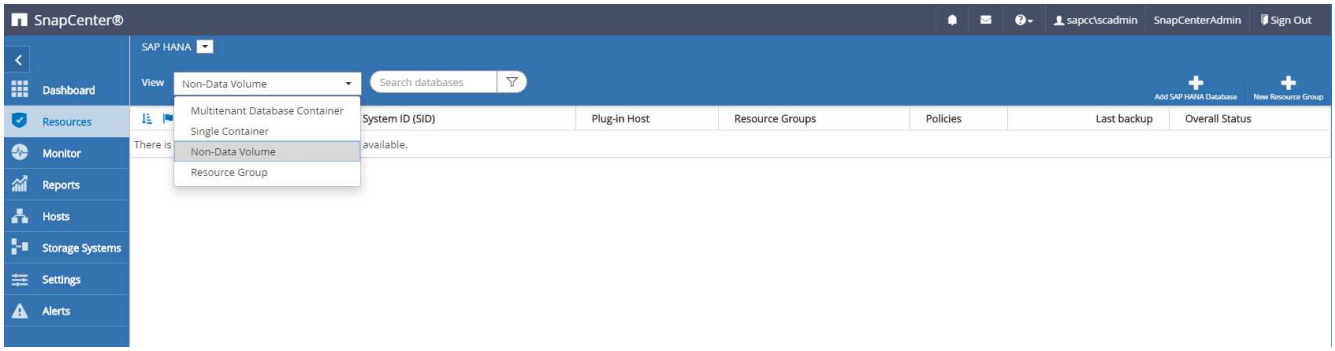
他のデータファイルのリストアが必要な状況からリカバリするには、 SAP HANA データベースのバックアップを補うために、データボリューム以外のボリュームに対する追加のバックアップ戦略を開発することを推奨します。固有の要件に応じて、非データボリュームのバックアップはスケジュールの頻度と保持の設定が異なる場合があります。また、非データファイルを変更する頻度も考慮する必要があります。たとえば、 HANA ボリューム「 /hana/shared 」には、実行可能ファイルと SAP HANA トレースファイルが格納されています。実行ファイルが変更されるのは SAP HANA データベースがアップグレードされた場合だけですが、 SAP HANA の問題を分析するためには、 SAP HANA のトレースファイルのバックアップ頻度を高くする必要があります。

SnapCenter の非データボリュームバックアップを使用すると、関連するすべてのボリュームの Snapshot コピーを数秒で作成でき、 SAP HANA データベースのバックアップと同じスペース効率化を実現できます。両者の違いは、 SAP HANA データベースとの SQL 通信は不要なことです。

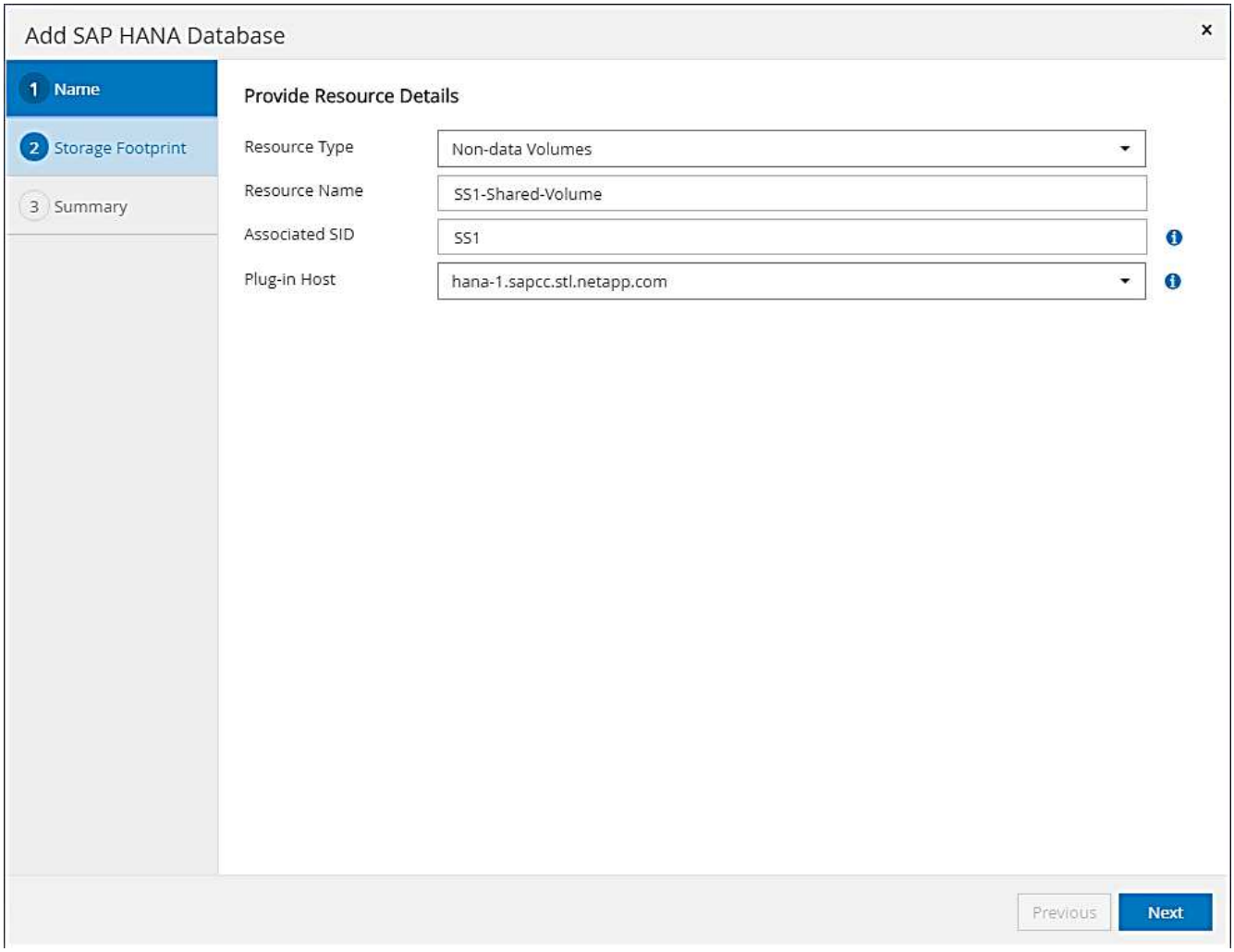
データボリューム以外のリソースの構成

この例では、 SAP HANA データベース SS1 の非データボリュームを保護します。

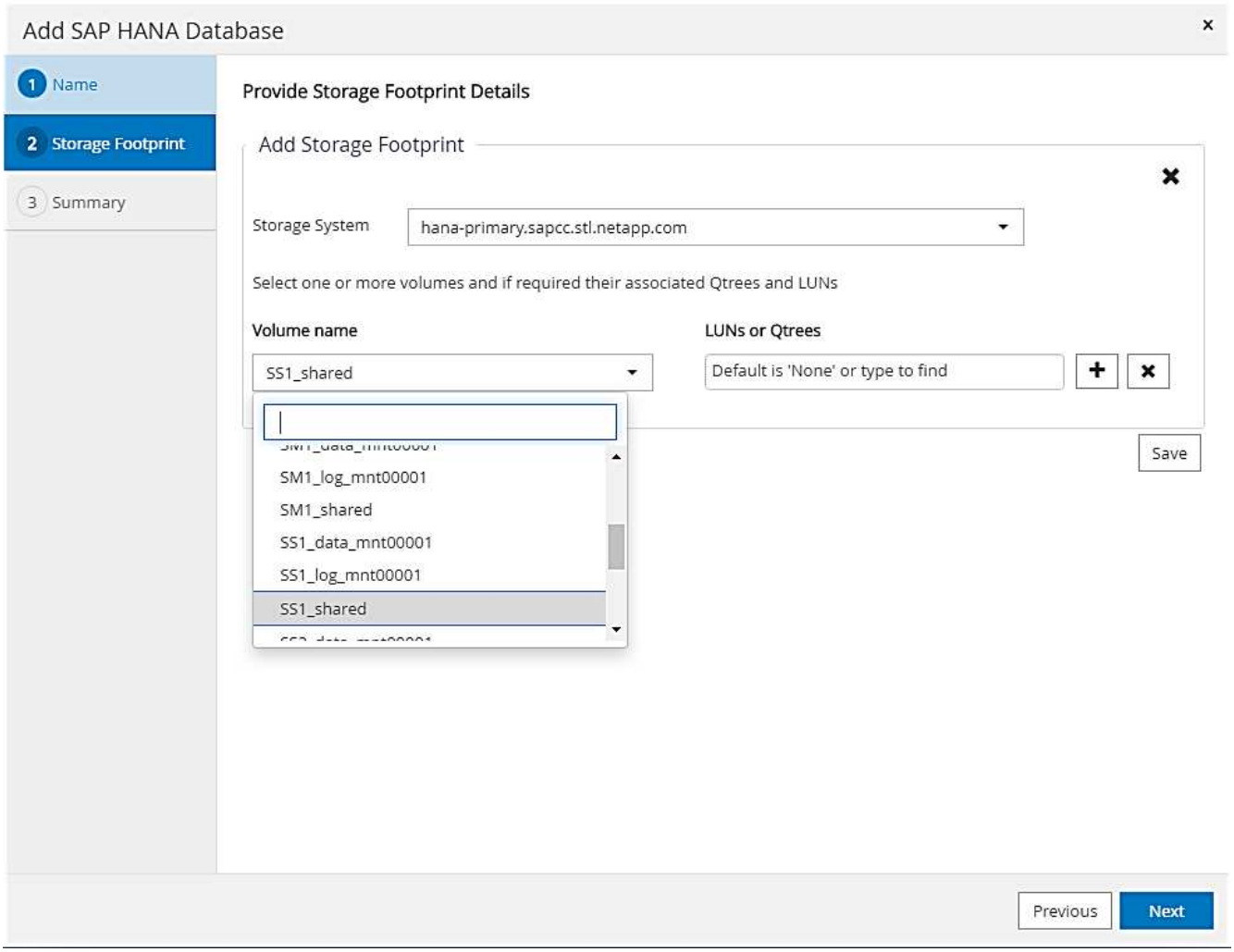
1. [リソース] タブで、 [データボリュームではない] を選択し、 [SAP HANA データベースの追加] をクリックします。



2. SAP HANA データベースの追加ダイアログのステップ 1 で、リソースタイプリストから非データボリュームを選択します。リソースの名前、およびリソースに使用する関連 SID と SAP HANA プラグインホストを指定し、 [次へ] をクリックします。



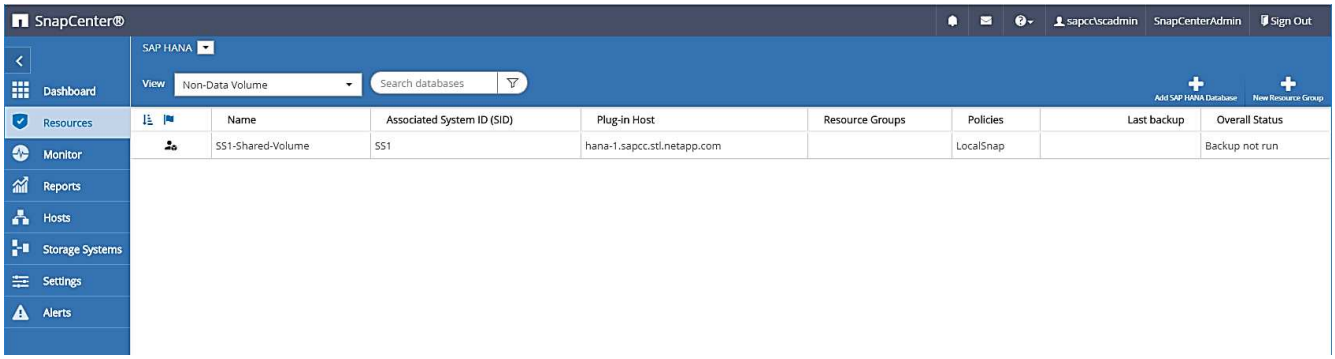
3. SVM とストレージボリュームをストレージ容量として追加し、次へをクリックします。



4. 概要ステップで、完了をクリックして設定を保存します。
5. 必要なすべてのデータボリューム以外のボリュームについて、同じ手順を繰り返します。
6. 新しいリソースの保護設定に進みます。

> 非データボリュームリソースのデータ保護は、 SAP HANA データベースリソースのワークフローと同じで、個々のリソースレベルで定義できます。

次の図に、設定されているデータボリューム以外のリソースのリストを示します。



リソースグループ

リソースグループを使用すると、同じ保護ポリシーとスケジュールを必要とする複数のリソースの保護を定義できます。リソースグループの一部である単一のリソースは、個別のレベルで保護することができます。

リソースグループには次の機能があります。

- リソースグループには 1 つ以上のリソースを追加できます。すべてのリソースが同じ SnapCenter プラグインに属している必要があります。
- 保護はリソースグループレベルで定義できます。リソースグループ内のすべてのリソースは、保護されている場合は同じポリシーとスケジュールを使用します。
- SnapCenter リポジトリ内のすべてのバックアップとストレージ Snapshot コピーには、リソース保護に定義されているものと同じ名前が付けられます。
- リストア処理は、リソースグループの一部としてではなく、単一のリソースレベルに適用されます。
- SnapCenter を使用して、リソースグループレベルで作成されたリソースのバックアップを削除する場合、このバックアップはリソースグループ内のすべてのリソースについて削除されます。バックアップを削除する場合は、 SnapCenter リポジトリからバックアップを削除するか、ストレージ Snapshot コピーを削除します。
- リソースグループの主なユースケースは、 SnapCenter で作成したバックアップを使用して、 SAP Landscape Management でシステムをクローニングする場合です。これについては、次のセクションで説明します。

SnapCenter と SAP ランドスケープ管理の併用

SAP Landscape Management （ SAP LaMa ）を使用すると、オンプレミスのデータセンターやクラウドで実行されているシステムでも、複雑な SAP システム環境を管理できます。SAP LaMa は、ネットアップの Storage Services Connector （ SSC ）と連携して、 SAP システムのクローニングやレプリケーション、 Snapshot や FlexClone テクノロジを使用したコピー、更新などのストレージ運用を実行できます。そのため、ストレージクローニングテクノロジに基づいて SAP システムのコピーを完全に自動化し、必要な SAP のポストプロセスも含めて実行できます。ネットアップの SAP LaMa 対応ソリューションの詳細については、を参照してください "TR-4018 ：『 Integrating NetApp ONTAP Systems with SAP Landscape Management 』"。

NetApp SSC と SAP LaMa は、 NetApp SSC を使用してオンデマンドで Snapshot コピーを直接作成できますが、 SnapCenter を使用して作成した Snapshot コピーを利用することもできます。SnapCenter バックアップをシステムのクローニング処理やコピー処理のベースとして SAP LaMa を使って実行するには、次の前提条件を満たしている必要があります。

- SAP LaMa では、すべてのボリュームをバックアップに含める必要があります。これには、 SAP HANA のデータ、ログ、共有ボリュームが含まれます。
- ストレージの Snapshot 名はすべて同じにする必要があります。
- ストレージスナップショット名は VCM で始める必要がある。

> ⓘ 通常のバックアップ処理では、ログボリュームを含めることは推奨されません。バックアップからログボリュームをリストアすると、最後のアクティブな REDO ログが上書きされ、データベースを最後の最新状態にリカバリできなくなります。

SnapCenter リソースグループは、上記のすべての要件を満たしています。SnapCenter では、 3 つのリソースが構成されます。各リソースはデータボリューム用、ログボリューム用、および共有ボリューム用の 1 つ

です。リソースはリソースグループに追加され、保護はリソースグループレベルで定義されます。リソースグループ保護では、最初に VCM を使用してカスタムスナップショット名を定義する必要がある。

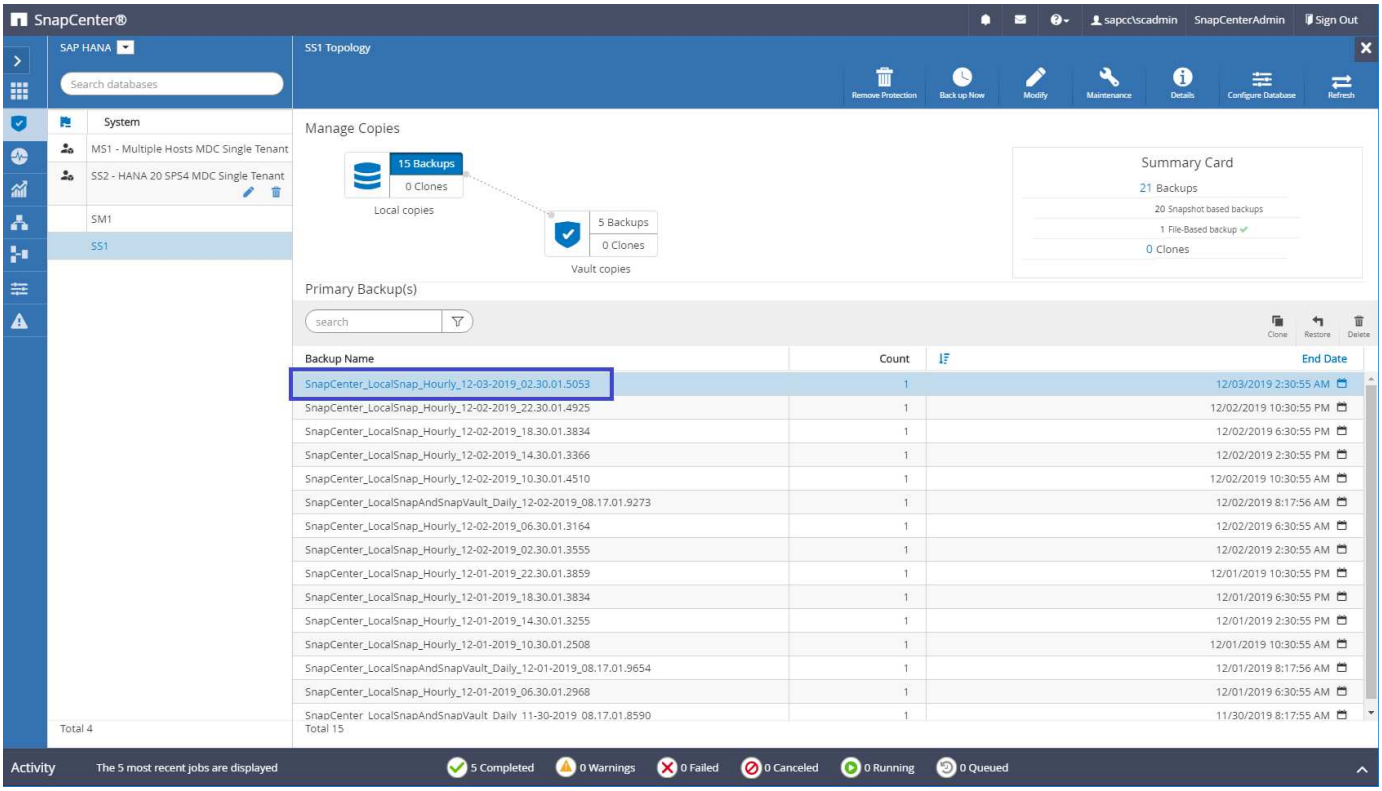
データベースのバックアップ

SnapCenter では、一般に、各 HANA データベースのリソース保護構成で定義されたスケジュールを使用してデータベースのバックアップが実行されます。

オンデマンドデータベースバックアップを実行するには、 SnapCenter GUI 、 PowerShell コマンドライン、または REST API を使用します。

SAP HANA Studio での SnapCenter バックアップの識別

SnapCenter のリソーストポロジには、 SnapCenter を使用して作成されたバックアップのリストが表示されます。次の図に、プライマリストレージ上のバックアップと、最新のバックアップを示します。



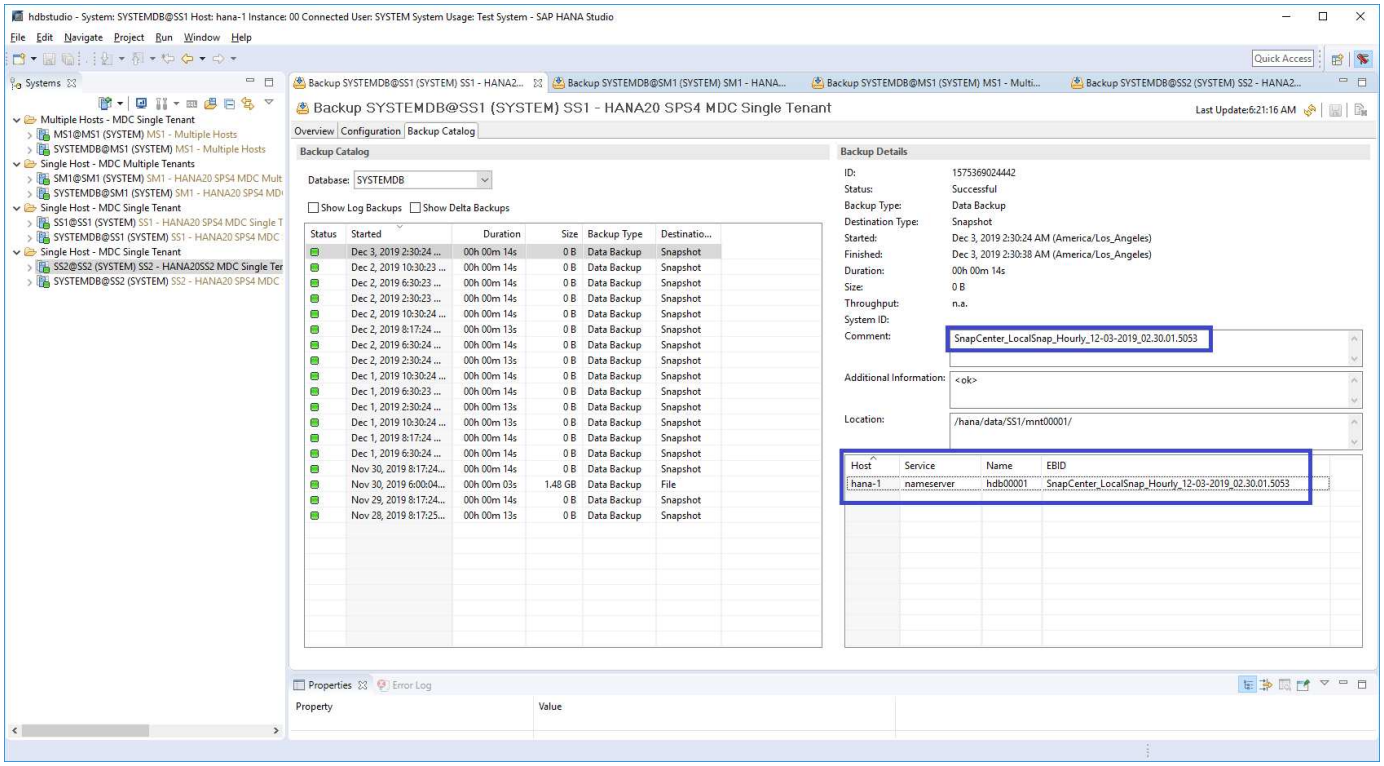
SAP HANA MDC システムのストレージ Snapshot コピーを使用したバックアップを実行する場合は、データボリュームの Snapshot コピーが作成されます。このデータボリュームには、システムデータベースのデータおよびすべてのテナントデータベースのデータが含まれます。この物理アーキテクチャを反映するため、 SnapCenter によって Snapshot バックアップがトリガーされるたびに、 SAP HANA はシステムデータベースとすべてのテナントデータベースの統合バックアップを内部的に実行します。その結果、 SAP HANA のバックアップカタログに、システムデータベース用とテナントデータベース用に 1 つずつ、合計複数のバックアップエントリが作成されます。

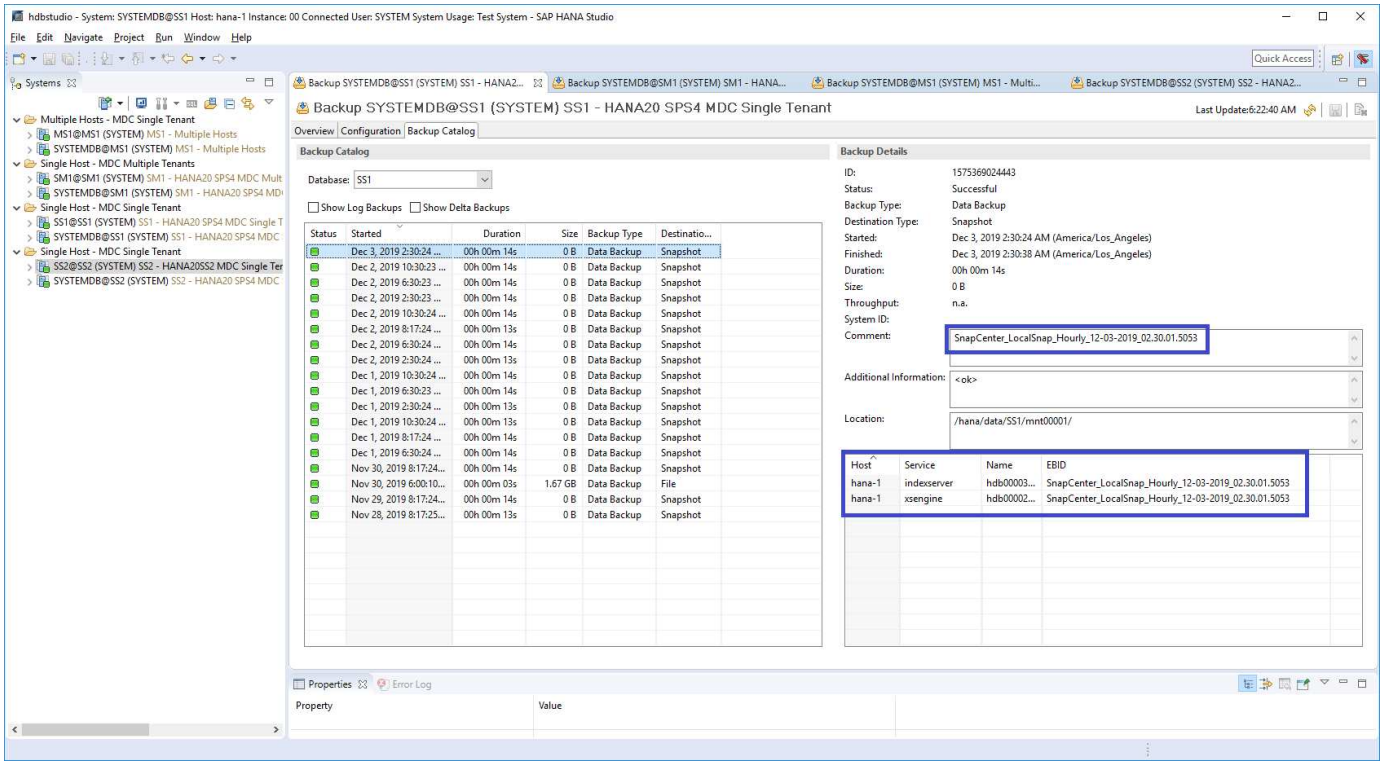
SAP HANA シングルコンテナシステムの場合、データベースボリュームにはデータベースが 1 つだけ格納され、 SAP HANA のバックアップカタログにはエントリが 1 つしかありません。

SAP HANA のバックアップ・カタログでは、 SnapCenter のバックアップ名は「 Comment 」フィールド

と「 External Backup ID （ EBID ）」フィールドとして保存されます。システムデータベースの次のスクリーンショットと、テナントデータベース SS1 のスクリーンショットに表示されています。どちらの図も、コメントフィールドに格納されている SnapCenter バックアップ名と EBID を示しています。

Snapshot ベースのバックアップについては、 HANA 2.0 SPS4 （リビジョン 40 および 41 ）リリースでは常にバックアップサイズがゼロになっています。これは、リビジョン 42 で修正されました。詳細については、『 SAP ノート』を参照してください "https://launchpad.support.sap.com/#/notes/2795010"。

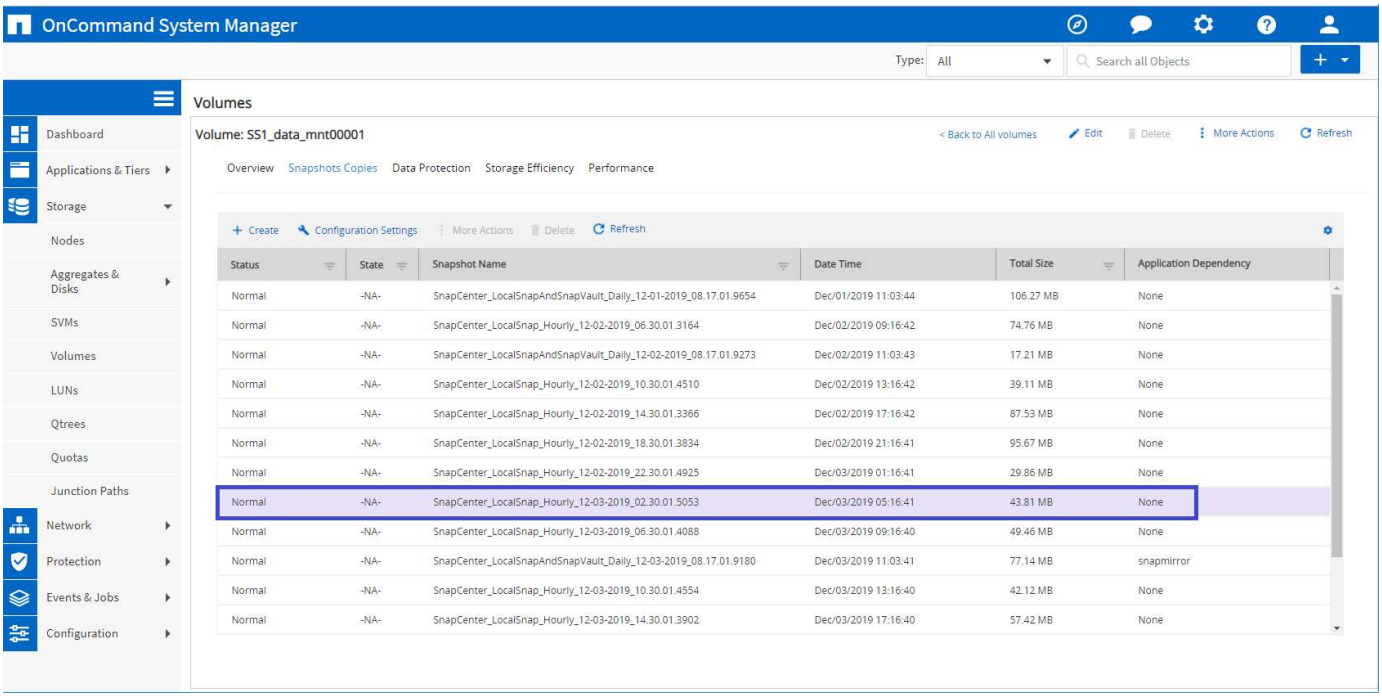




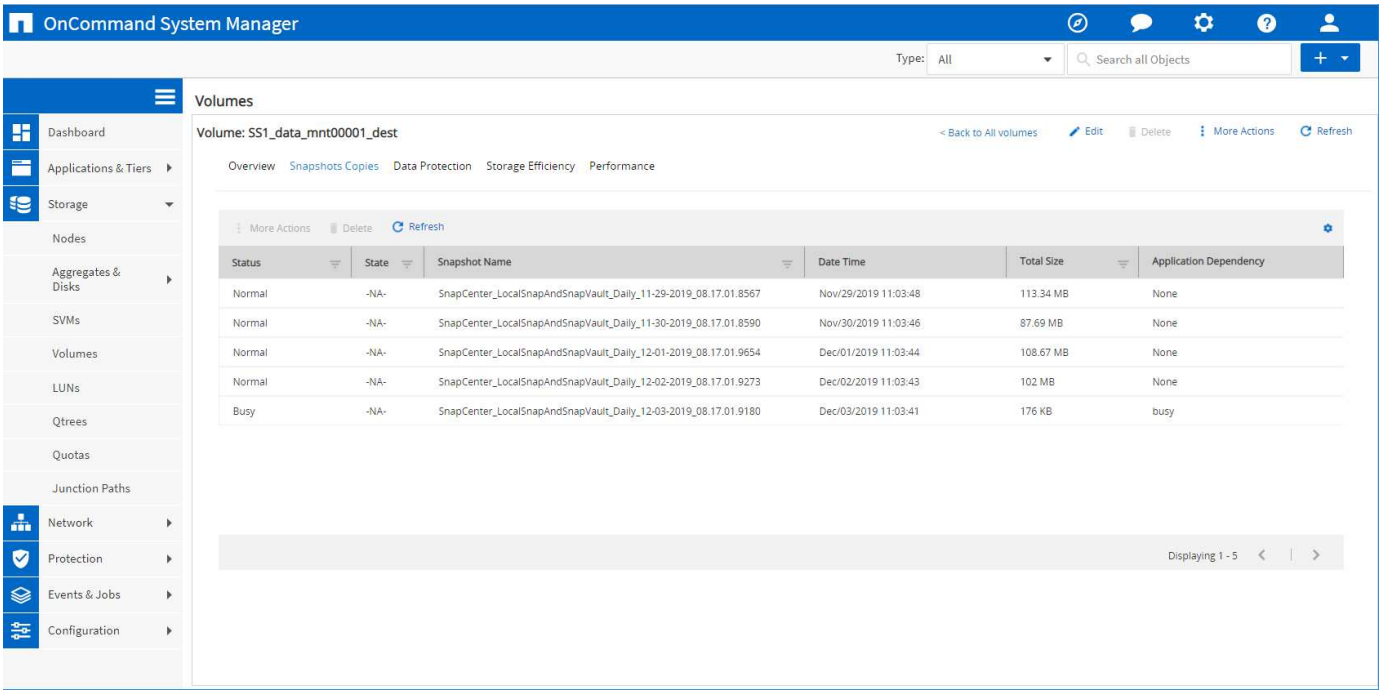
SnapCenter で認識されるのは、それ自体のバックアップだけです。SAP HANA Studio などで作成された追加のバックアップは、 SAP HANA のカタログには表示されますが、 SnapCenter には表示されません。

ストレージシステム上での **SnapCenter** バックアップの特定

ストレージレイヤのバックアップを表示するには、 NetApp OnCommand System Manager を使用して、 SVM のボリュームビューでデータベースボリュームを選択します。下部の Snapshot コピータブには、ボリュームの Snapshot コピーが表示されます。次のスクリーンショットは ' プライマリ・ストレージで使用可能なデータベース・ボリューム SS1_data_mnt00001 のバックアップを示しています強調表示されているバックアップは、前のイメージの SnapCenter と SAP HANA Studio に表示されているバックアップで、同じ命名規則が使用されています。



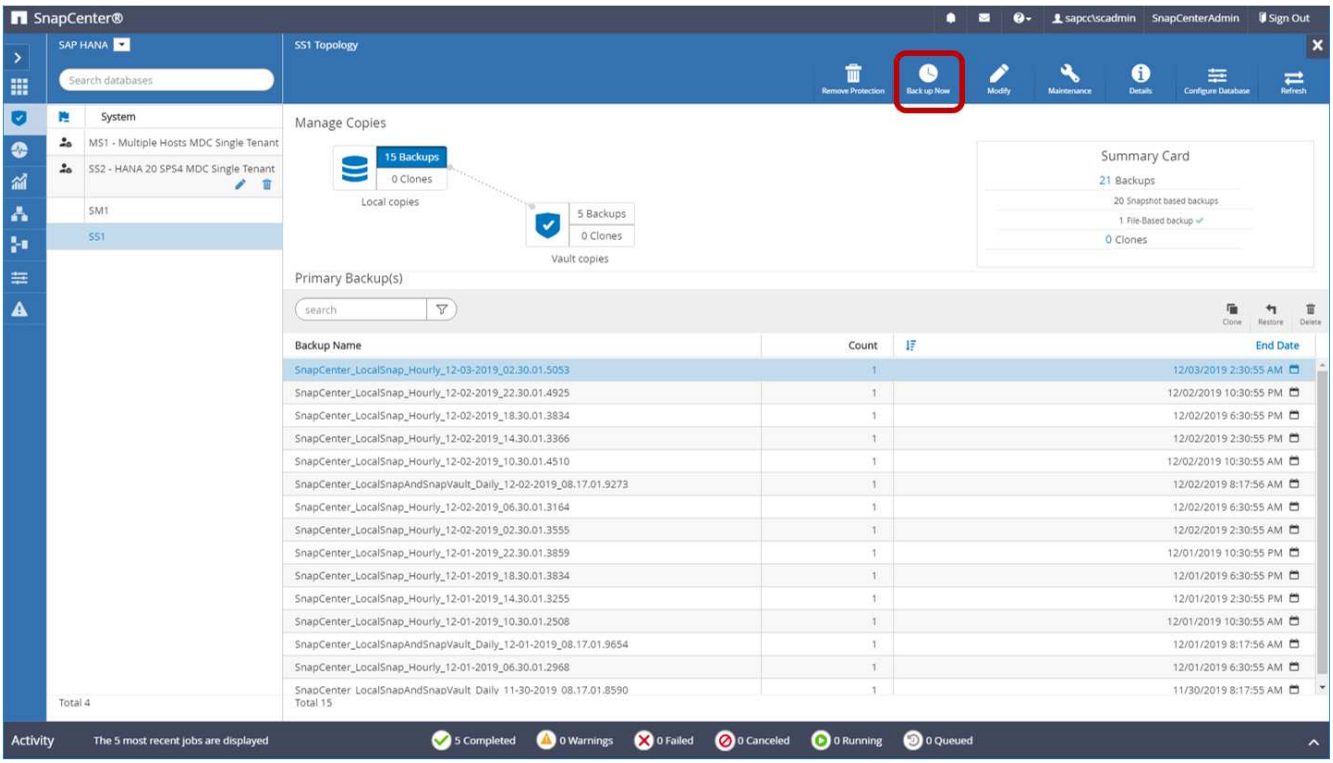
次のスクリーンショットは、セカンダリ・ストレージ・システムにあるレプリケーション・ターゲット・ボリューム「 hana_sa1_data_mnt00001_dest 」で使用可能なバックアップを示しています。



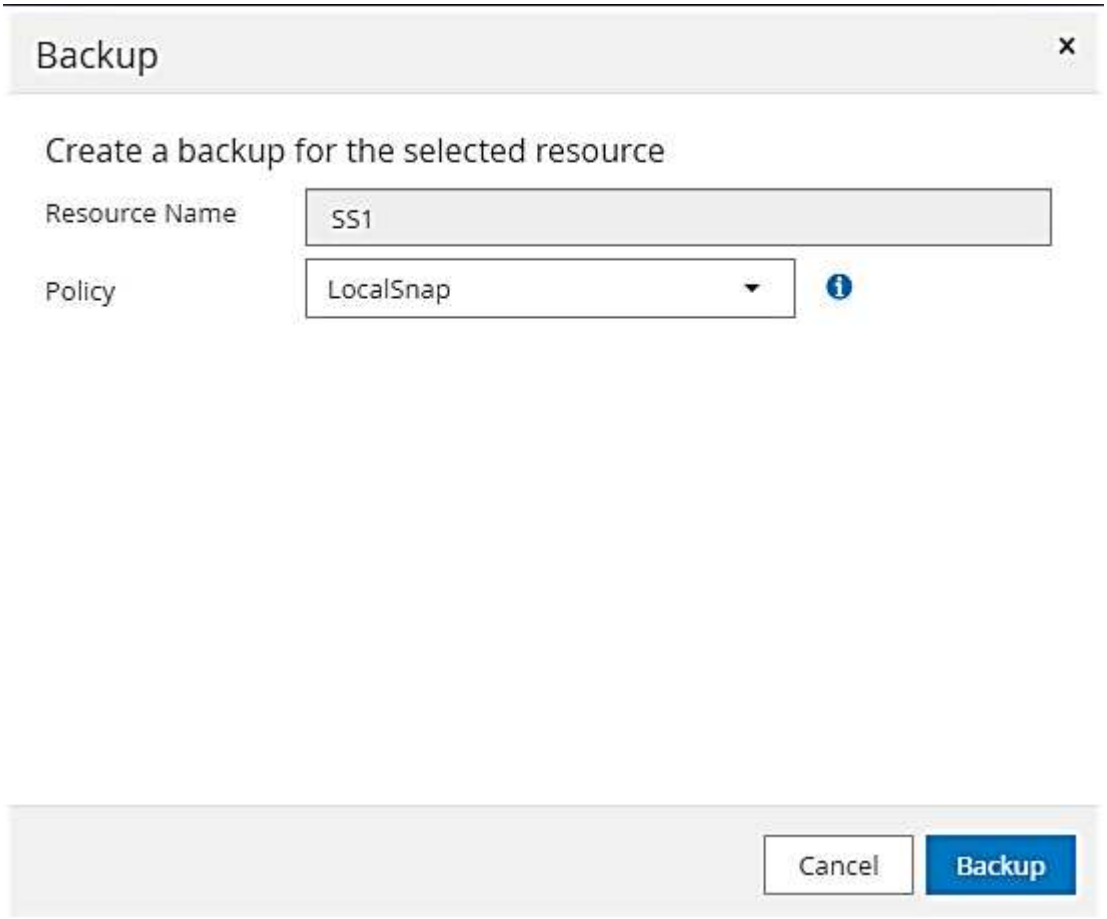
プライマリストレージでのオンデマンドのデータベースバックアップ

1. リソースビューでリソースを選択し、その行をダブルクリックしてトポロジビューに切り替えます。

   リソーストポロジビューには、 SnapCenter を使用して作成された、使用可能なすべてのバックアップの概要が表示されます。上部の領域には、プライマリストレージ上のバックアップ（ローカルコピー）と、オフサイトのバックアップストレージ（バックアップコピー）にあるバックアップ（バックアップコピー）が表示されます。

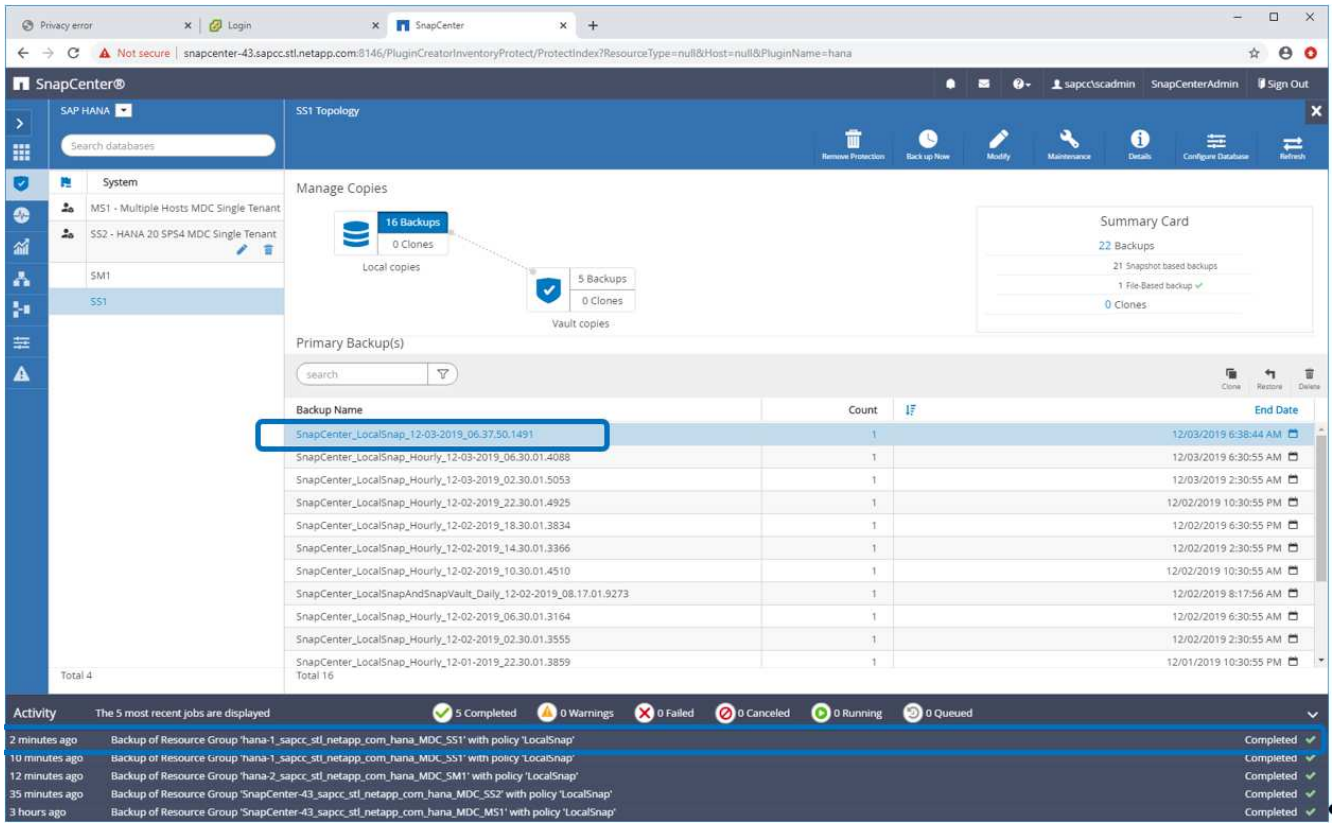


2. 一番上の行で、 Back Up Now （今すぐバックアップ）アイコンを選択して、オンデマンドバックアップを開始します。ドロップダウン・リストから ' バックアップ・ポリシー LocalSnap を選択し '[Backup] をクリックして ' オンデマンド・バックアップを開始します

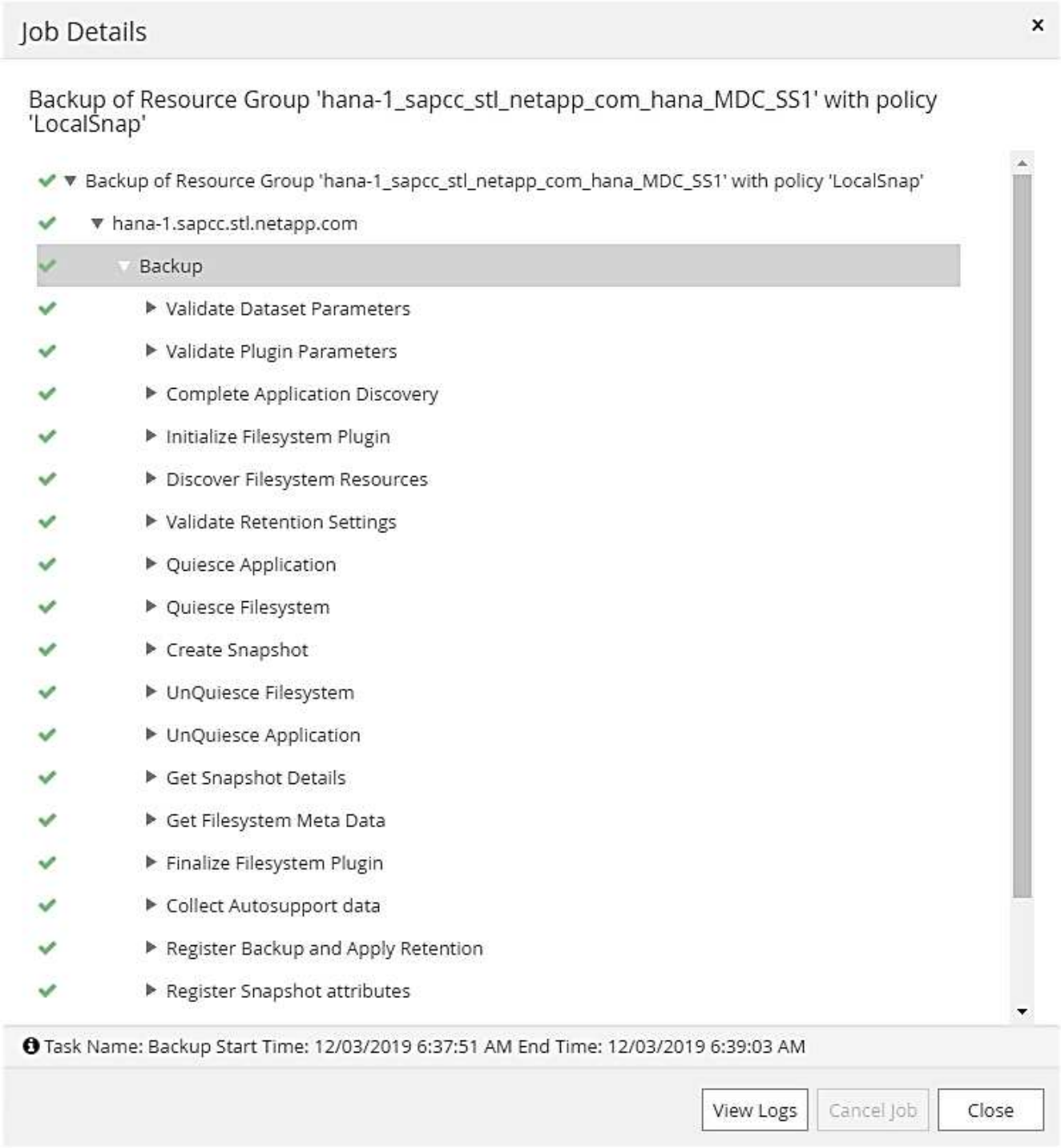


バックアップジョブが開始されます。トポロジビューの下のアクティビティ領域に、前の 5 つのジョブのログが表示されます。バックアップが完了すると、トポロジビューに新しいエントリが表示されます。バックアップ名は、セクションで定義した Snapshot 名と同じ命名規則に従っています "「リソース保護の設定」"

トポロジビューを閉じてから再度開いて、更新されたバックアップリストを確認する必要があります。



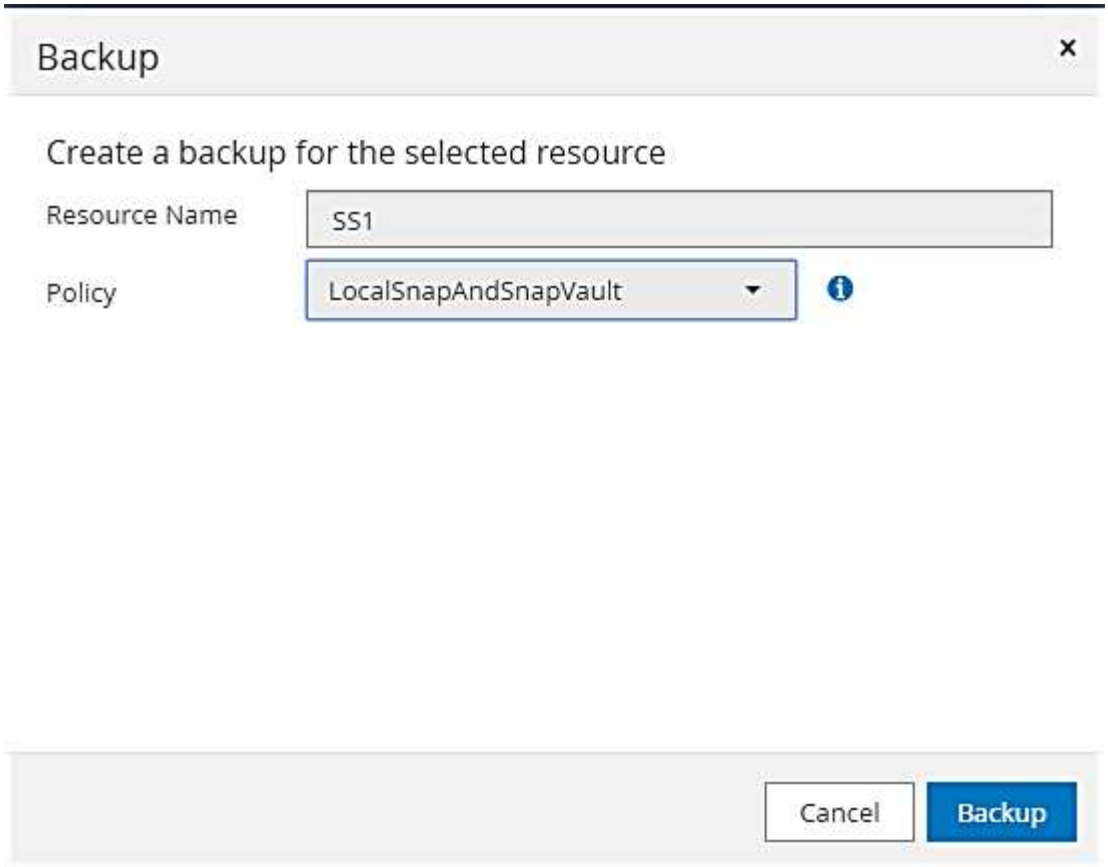
3. ジョブの詳細は、 [アクティビティ] 領域でジョブのアクティビティ行をクリックすると表示されます。ログの表示をクリックすると、詳細なジョブログを開くことができます。



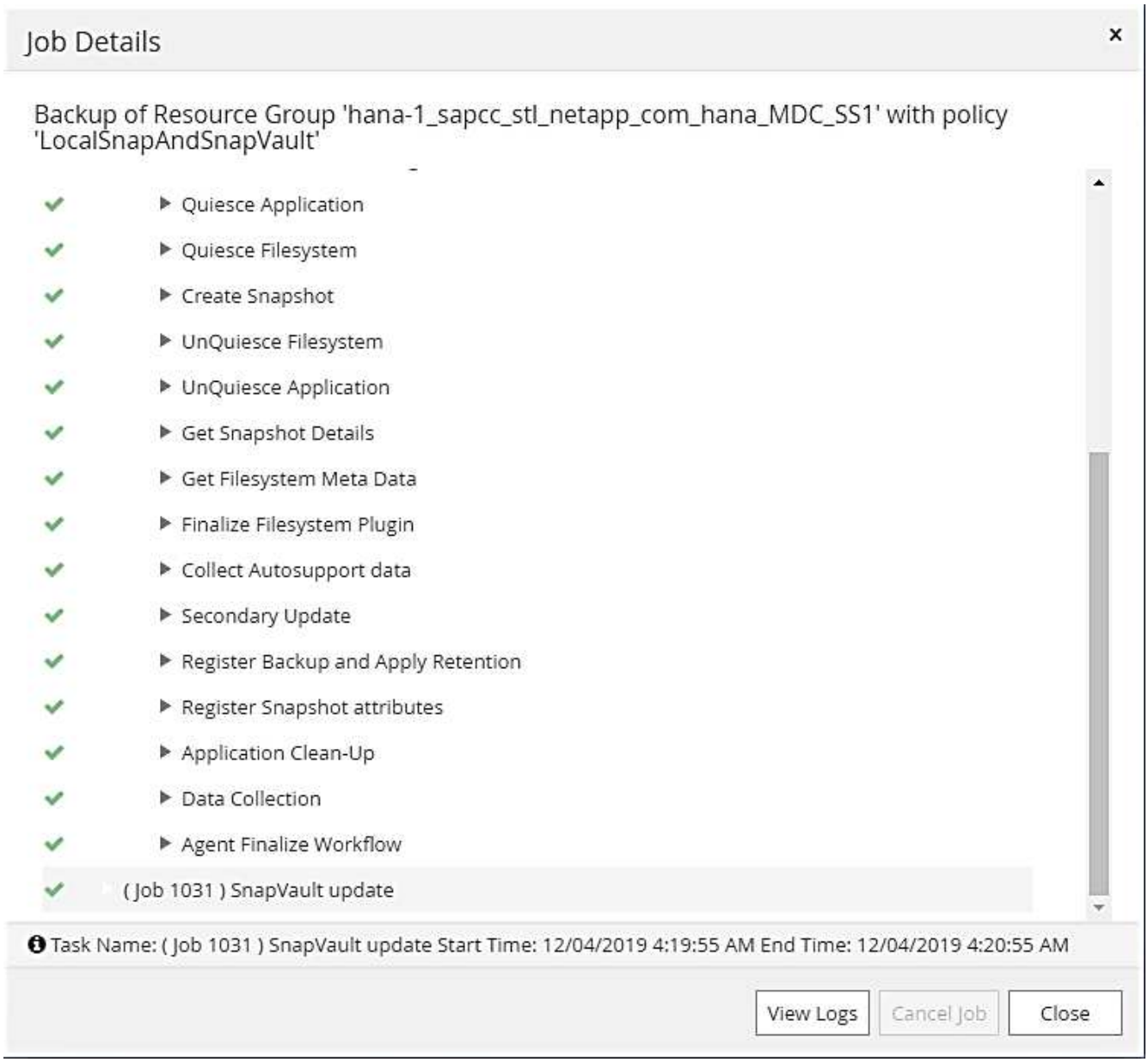
4. SAP HANA Studio では、バックアップカタログに新しいバックアップが表示されます。バックアップカタログのコメントフィールドと EBID フィールドには、 SnapCenter と同じバックアップ名が使用されます。

SnapVault レプリケーションを使用したオンデマンドのデータベースバックアップ

1. リソースビューでリソースを選択し、その行をダブルクリックしてトポロジビューに切り替えます。
2. 一番上の行で [Backup Now] アイコンを選択して、オンデマンド・バックアップを開始します。ドロップダウン・リストから ' バックアップ・ポリシー LocalSnapAndSnapVault' を選択し '[Backup] をクリックして ' オン・デマンド・バックアップを開始します

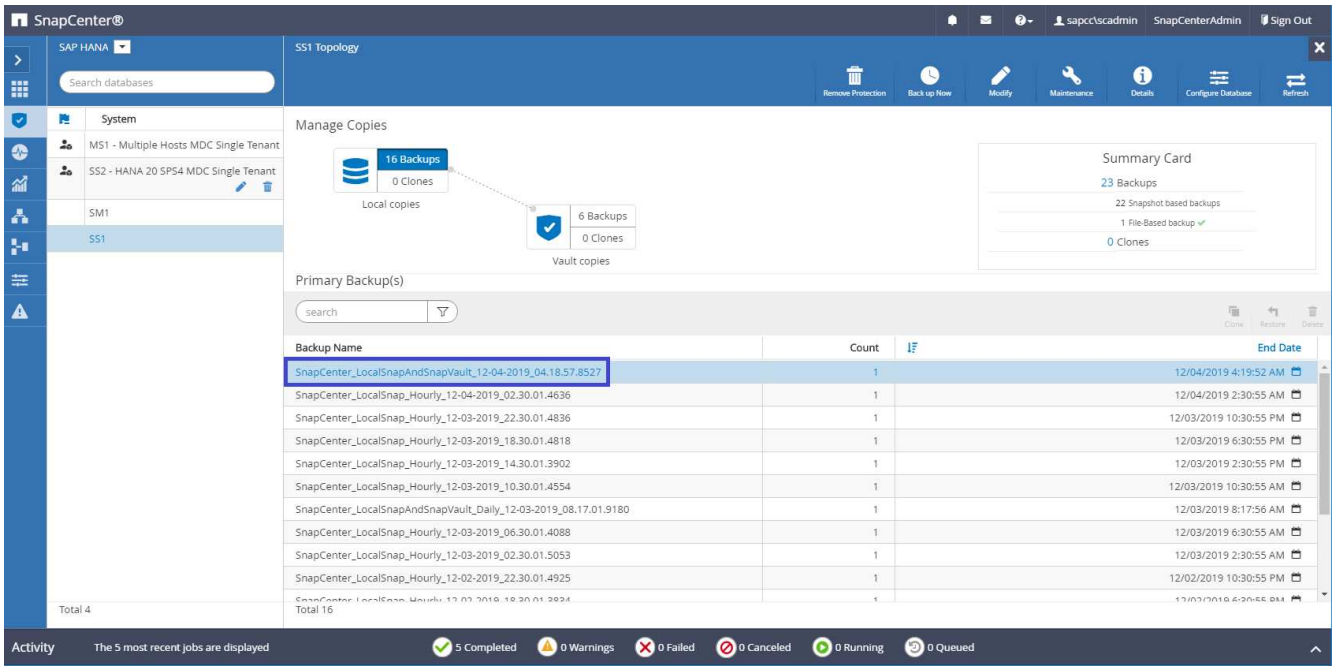


3. ジョブの詳細は、 [アクティビティ] 領域でジョブのアクティビティ行をクリックすると表示されます。

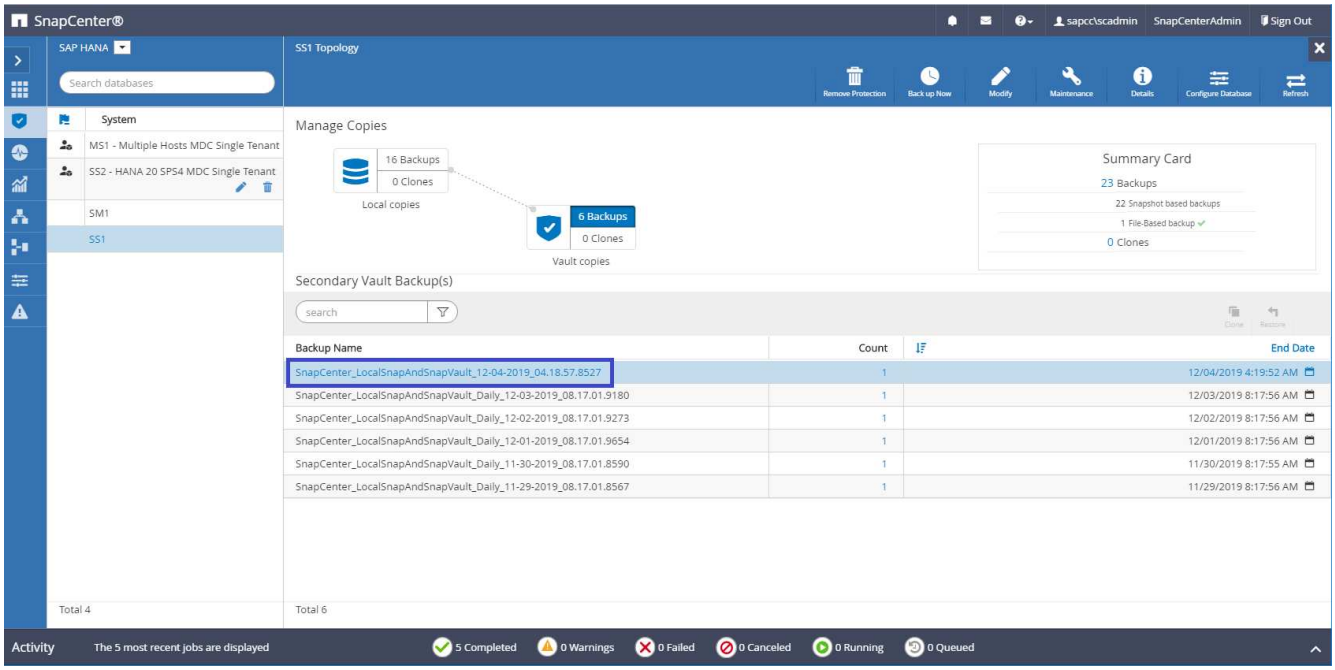


4. バックアップが完了すると、トポロジビューに新しいエントリが表示されます。バックアップ名は、セクションで定義した Snapshot 名と同じ命名規則に従っています "「リソース保護の設定」"

トポロジビューを閉じてから再度開いて、更新されたバックアップリストを確認する必要があります。



5. バックアップコピーを選択すると、セカンダリストレージのバックアップが表示されます。レプリケートされたバックアップの名前は、プライマリストレージのバックアップ名と同じです。



6. SAP HANA Studio では、バックアップカタログに新しいバックアップが表示されます。バックアップカタログのコメントフィールドと EBID フィールドには、 SnapCenter と同じバックアップ名が使用されます。

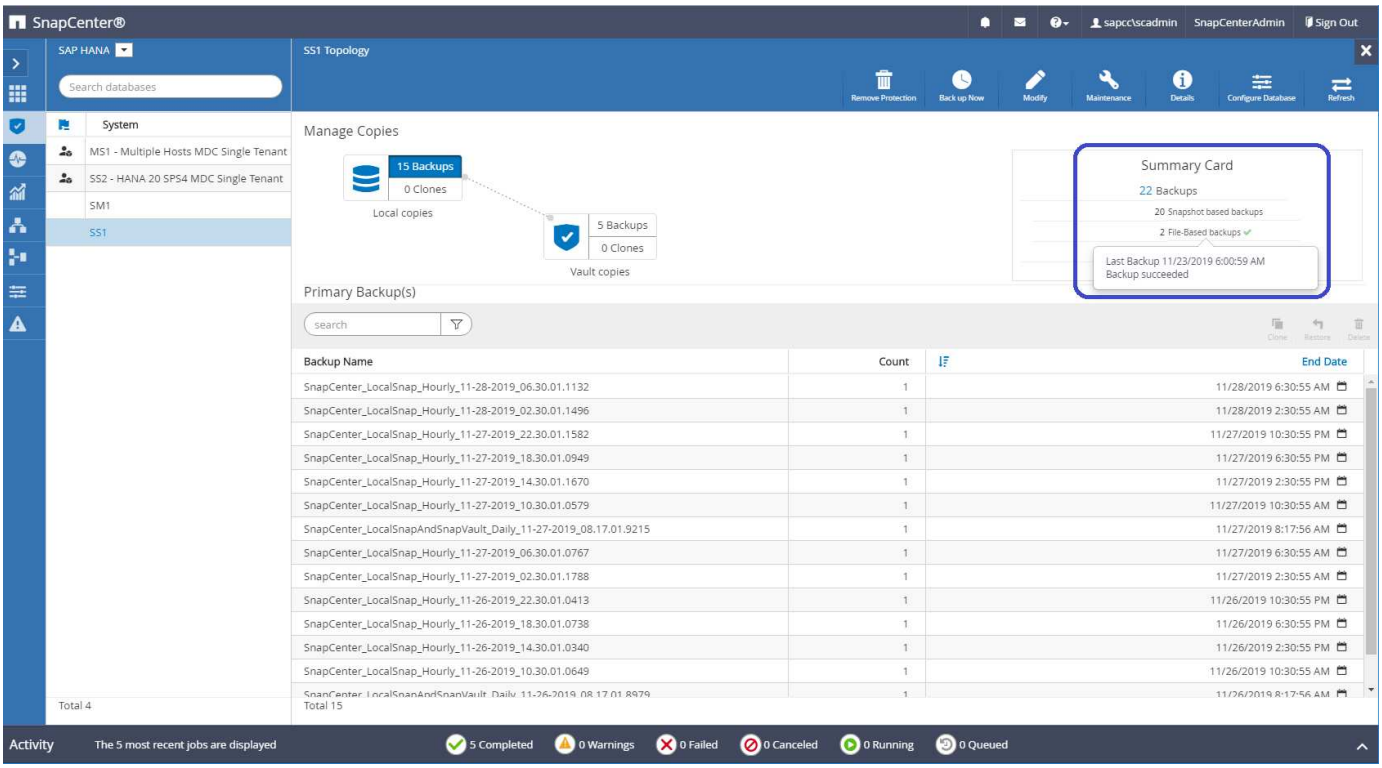
ブロック整合性チェック

SAP では、ブロックの整合性チェックを実行するために、ストレージベースの Snapshot バックアップと週次ファイルベースのバックアップを組み合わせることを推奨しています。SnapCenter では、バックアップタイプとしてファイルベースのバックアッ

プを選択するポリシーを使用して、ブロック整合性チェックを実行できます。

このポリシーを使用してバックアップをスケジュールすると、 SnapCenter によってシステムデータベースとテナントデータベース用の標準の SAP HANA ファイルバックアップが作成されます。

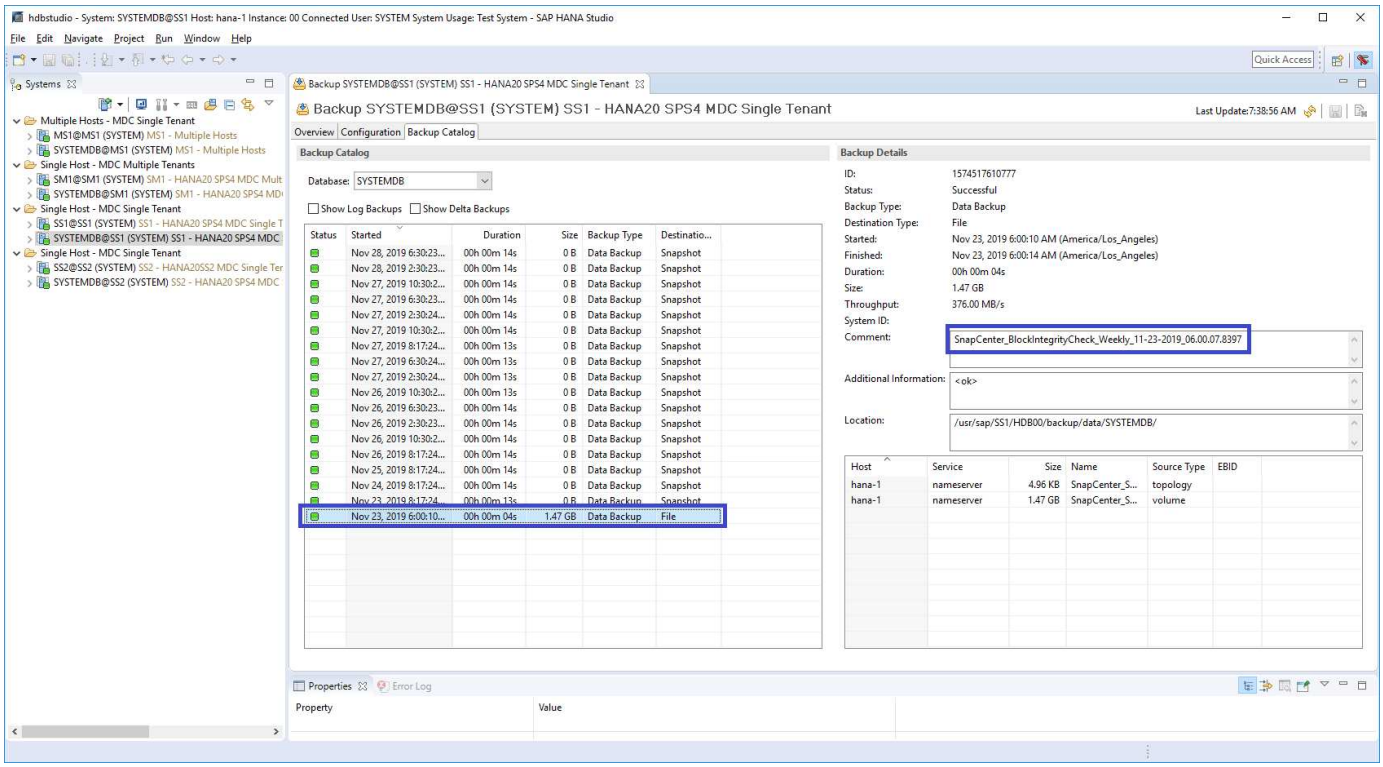
SnapCenter では、 Snapshot コピーベースのバックアップと同じ方法でブロック整合性チェックが表示されません。代わりに、サマリーカードには、ファイルベースのバックアップの数と、以前のバックアップのステータスが表示されます。



ブロック整合性チェックのバックアップは、 SnapCenter UI では削除できませんが、 PowerShell コマンドを使用して削除することはできます。

```
PS C:\Users\scadmin> Get-SmBackupReport -Resource SS1
SmBackupId                 : 9
SmJobId                    : 42
StartDateTime              : 11/19/2019 8:26:32 AM
EndDateTime                : 11/19/2019 8:27:33 AM
Duration                   : 00:01:00.7652030
CreatedDateTime            : 11/19/2019 8:27:24 AM
Status                     : Completed
ProtectionGroupName        : hana-1_sapcc_stl_netapp_com_hana_MDC_SS1
SmProtectionGroupId        : 1
PolicyName                 : BlockIntegrityCheck
SmPolicyId                 : 5
BackupName                 : SnapCenter_BlockIntegrityCheck_11-19-
2019_08.26.33.2913
VerificationStatus         : NotApplicable
VerificationStatuses       :
SmJobError                 :
BackupType                 : SCC_BACKUP
CatalogingStatus           : NotApplicable
CatalogingStatuses         :
ReportDataCreatedDateTime :
PluginCode                 : SCC
PluginName                 : hana
JobTypeId                  : 0
JobHost                    :

PS C:\Users\scadmin> Remove-SmBackup -BackupIds 9

Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): y


BackupResult : {}
Result       : SMCoreContracts.SMResult
TotalCount   : 0
DisplayCount : 0
Context      :
Job          : SMCoreContracts.SmJob



PS C:\Users\scadmin>
```

SAP HANA のバックアップカタログには、システムデータベースとテナントデータベースの両方のエントリが表示されます。次の図に、システムデータベースのバックアップカタログにおける SnapCenter ブロックの整合性チェックを示します。



ブロック整合性チェックが成功すると、標準の SAP HANA データバックアップファイルが作成されます。SnapCenter は、ファイルベースのデータバックアップ処理に、 HANA データベースで設定されているバックアップパスを使用します。

```
hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:25 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys   83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ss1adm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_3_1
SYSTEMDB:
total 1546340
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:24 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_1_1
```

リストアとリカバリ

以降のセクションでは、 3 種類のシナリオと設定例について、リストアとリカバリのワークフローを説明します。

- リストアとリカバリの自動化：
  - 自動検出された HANA システム SS1
  - NFS を使用した SAP HANA シングルホスト MDC のシングルテナントシステム
- シングルテナントのリストアとリカバリ：
  - 自動検出された HANA システム SM1
  - SAP HANA シングルホスト MDC の NFS を使用したマルチテナントシステム
- 手動リカバリによるリストア：
  - 手動構成の HANA システム SS2
  - SAP HANA シングルホスト MDC の NFS を使用したマルチテナントシステム

以降のセクションでは、 SAP HANA シングルホストと複数のホストおよび Fibre Channel SAN Attached HANA システムの違いを示します。

以下の例では、手動リカバリを実行するツールとして SAP HANA Studio を使用しています。SAP HANA Cockpit または HANA の SQL ステートメントを使用することもできます。

リストアとリカバリの自動化

SnapCenter 4.3 では、 SnapCenter によって自動検出された HANA シングルコンテナシステムまたは MDC シングルテナントシステムで自動リストア処理とリカバリ処理がサポートされています。

リストア処理とリカバリ処理の自動化は、次の手順で実行できます。

1. リストア処理に使用するバックアップを選択します。バックアップは、次のストレージ・オプションから選択できます。
   - プライマリストレージ
   - オフサイトのバックアップストレージ（ SnapVault ターゲット）
2. リストアタイプを選択します。[Complete Restore with Volume Revert or Without Volume Revert] を選択します。

   ボリュームリバートオプションを使用できるのは、プライマリストレージからのリストア処理と、 HANA データベースでストレージプロトコルとして NFS を使用している場合のみです。

3. 次のオプションからリカバリタイプを選択します。
   - を最新の状態に変更します
   - ポイントインタイム
   - 特定のデータのバックアップ
   - リカバリなし

   選択したリカバリタイプは、システムとテナントデータベースのリカバリに使用されます。

次に、 SnapCenter は次の処理を実行します。

1. HANA データベースが停止します。
2. データベースがリストアされます。

   選択したリストアタイプと使用するストレージプロトコルに応じて、異なる処理が実行されます。

   - NFS と Volume Revert を選択した場合は、 SnapCenter がボリュームをアンマウントし、ストレージレイヤのボリュームベースの SnapRestore を使用してボリュームをリストアし、ボリュームをマウントします。
   - NFS を選択し、ボリュームの復元を選択しない場合、 SnapCenter はストレージレイヤで単一ファイルの SnapRestore 操作を使用してすべてのファイルを復元します。
   - ファイバチャネル SAN を選択した場合、 SnapCenter は LUN をアンマウントし、ストレージレイヤでの単一ファイルの SnapRestore 処理を使用して LUN をリストアし、その LUN を検出してマウントします。

3. データベースをリカバリします。
   a. システムデータベースがリカバリされます。
   b. テナントデータベースがリカバリされます。

      または、 HANA のシングルコンテナシステムの場合、リカバリは 1 つの手順で実行されます。

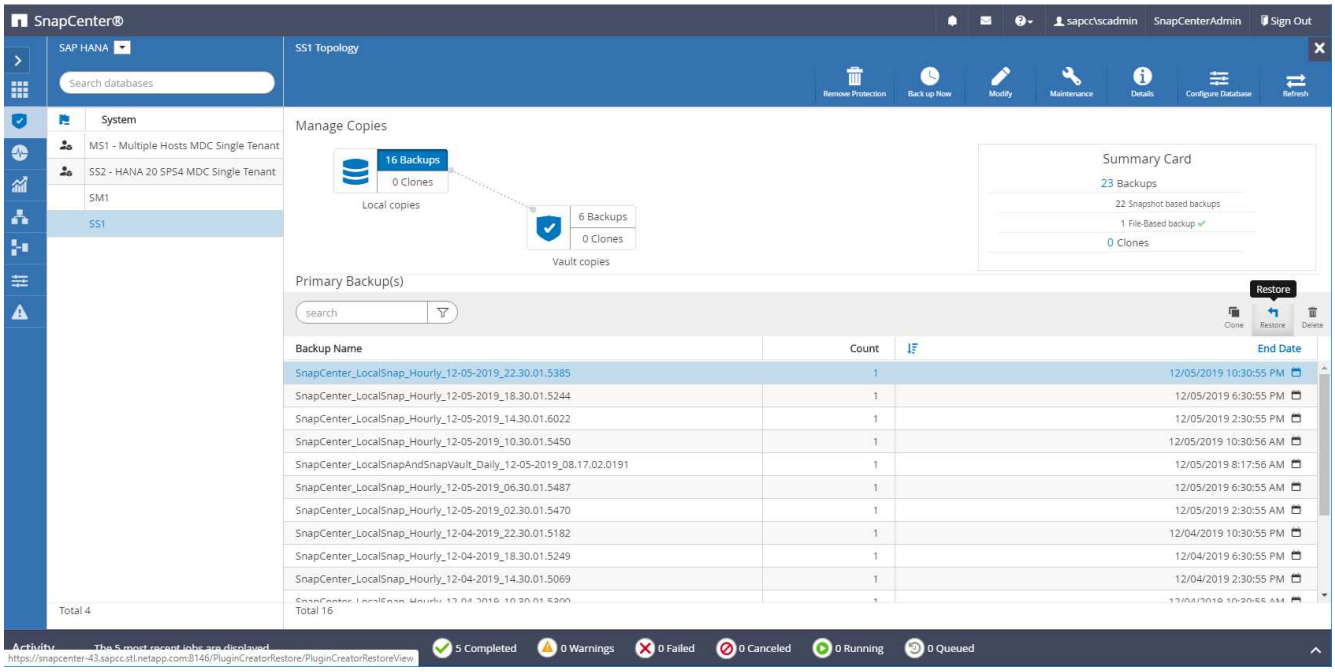
   c. HANA データベースが起動します。

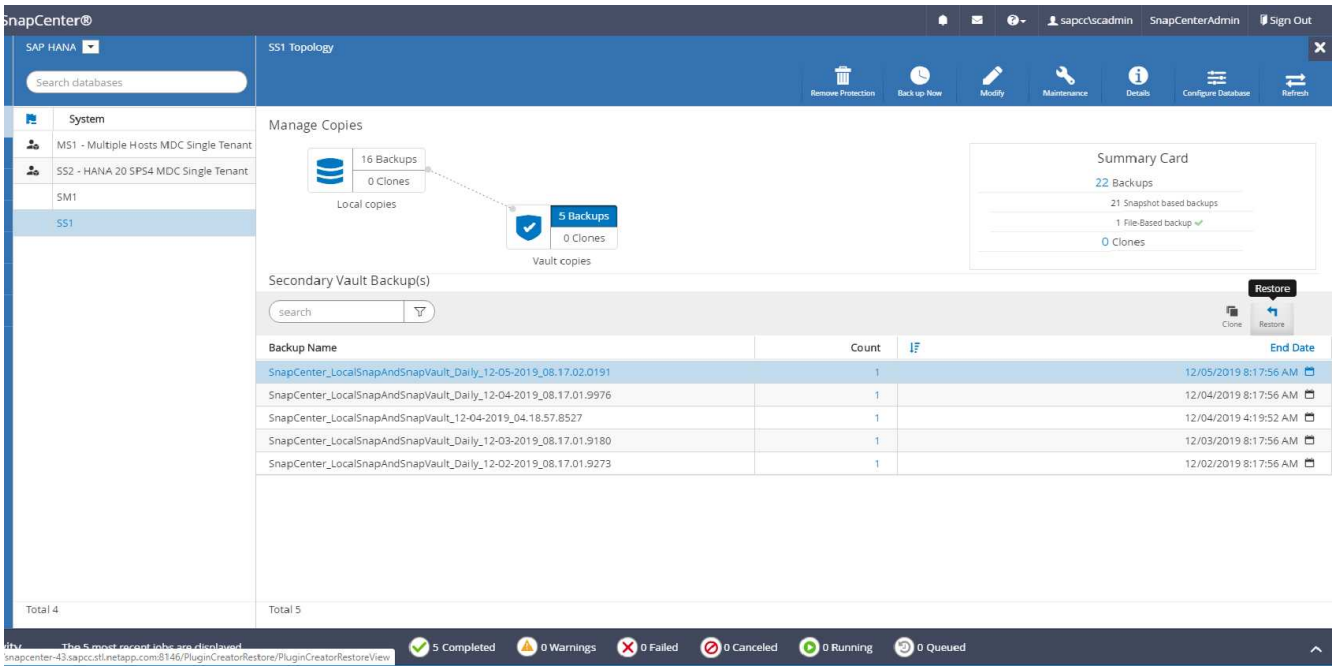
> リカバリなしを選択した場合は、 SnapCenter が終了し、システムとテナントデータベースのリカバリ処理を手動で実行する必要があります。

このセクションでは、自動検出された HANA システム SS1 （ SAP HANA シングルホスト、 NFS を使用した MDC シングルテナントシステム）の自動リストア処理とリカバリ処理の手順を説明します。

1. SnapCenter で、リストア処理に使用するバックアップを選択します。

> プライマリまたはオフサイトのバックアップストレージからリストアを選択できます。



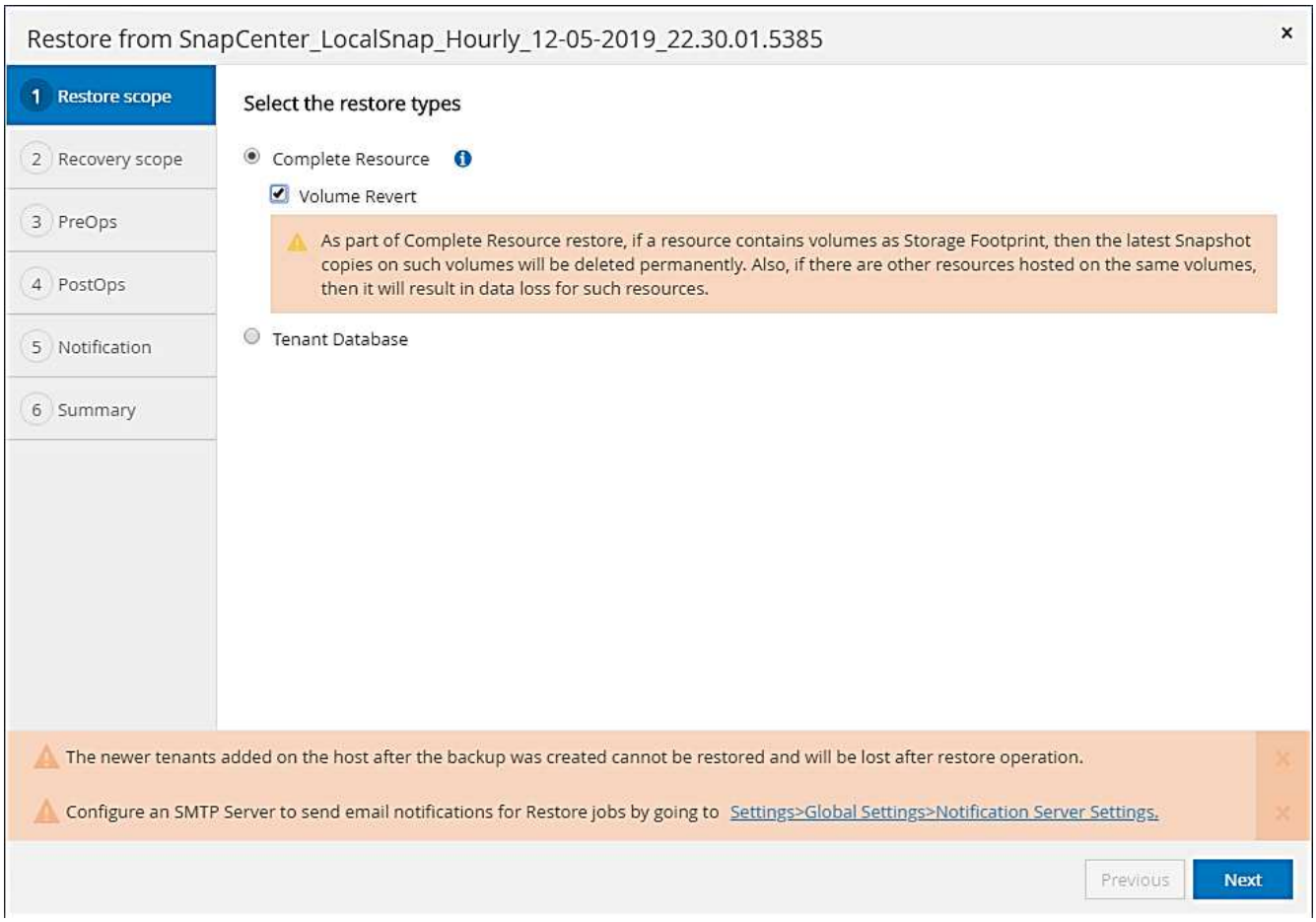


2. リストアの範囲とタイプを選択します。

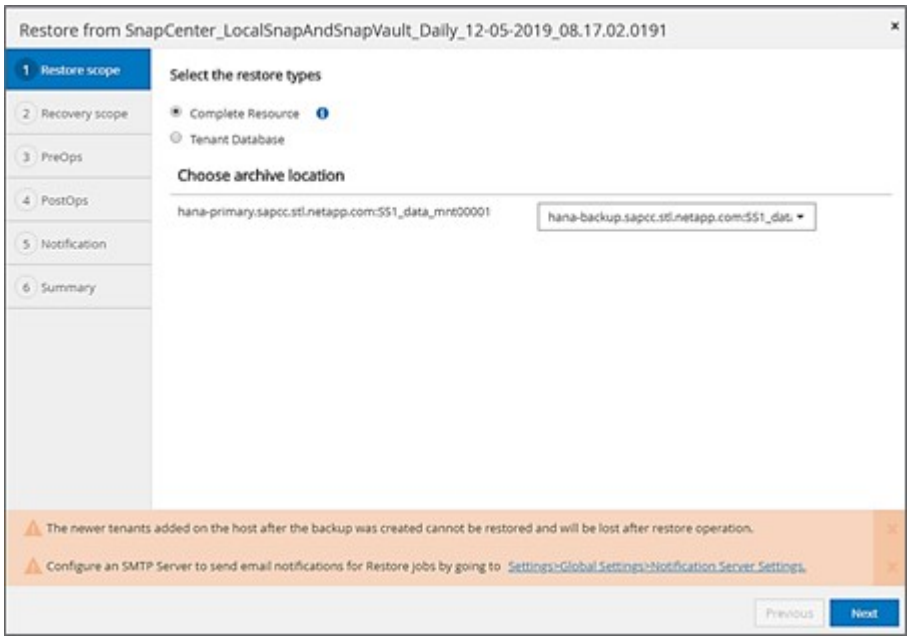
   次の 3 つのスクリーンショットは、 NFS を使用したプライマリからのリストア、 NFS を使用したセカンダリからのリストア、ファイバチャネル SAN を使用したプライマリからのリストアのリストアオプションを示しています。

   プライマリストレージからリストアする場合のリストアタイプのオプション。

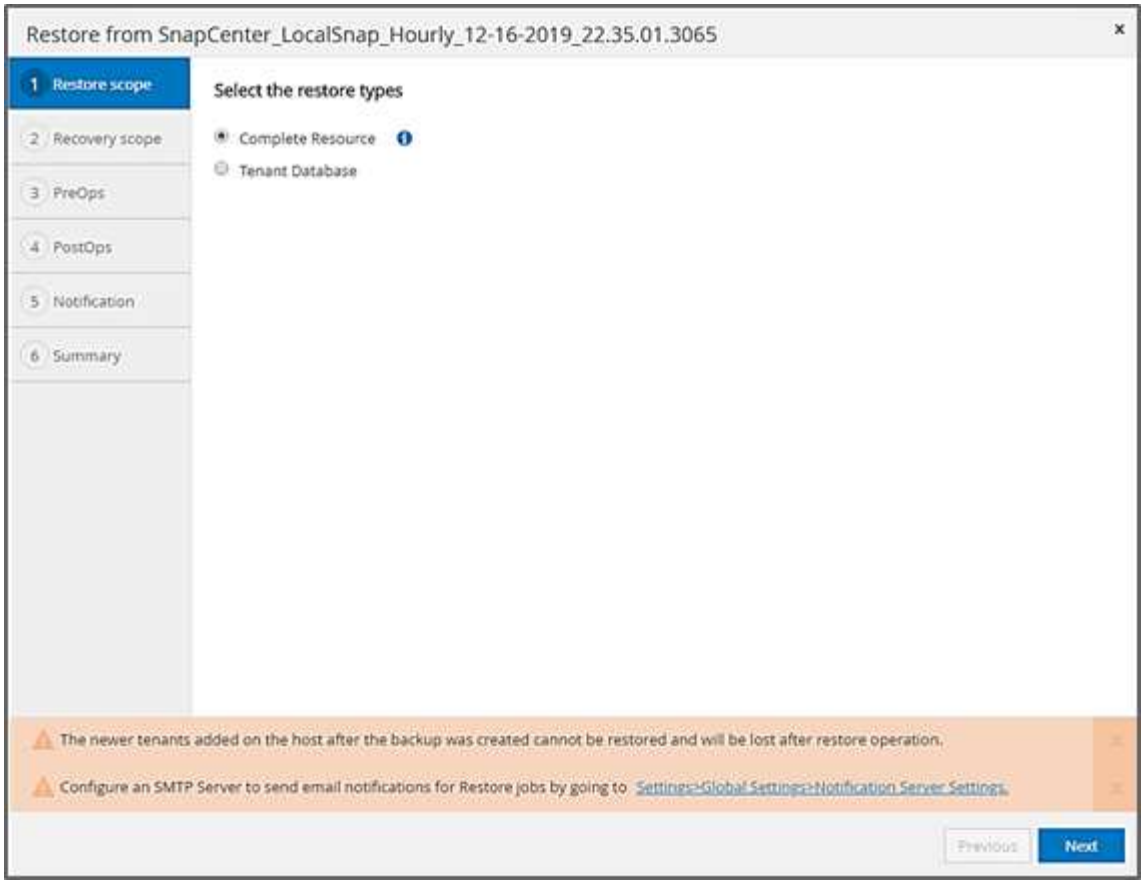
   ボリュームリバートオプションは、 NFS でプライマリからのリストア処理でのみ使用できます。



オフサイトのバックアップストレージからリストアする場合のリストアタイプのオプション。

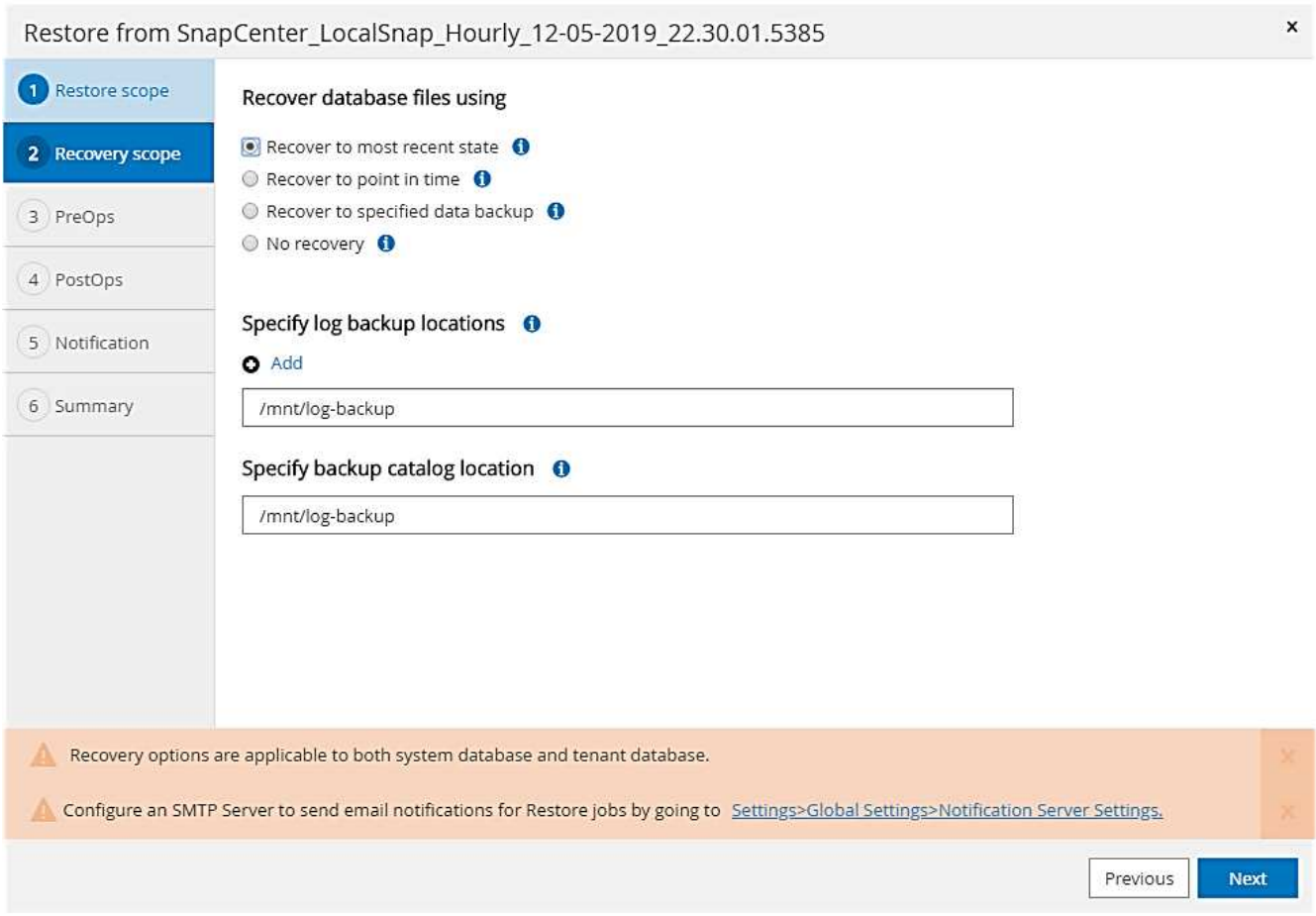


ファイバチャネル SAN を使用してプライマリストレージからリストアする場合のリストアタイプのオプション。

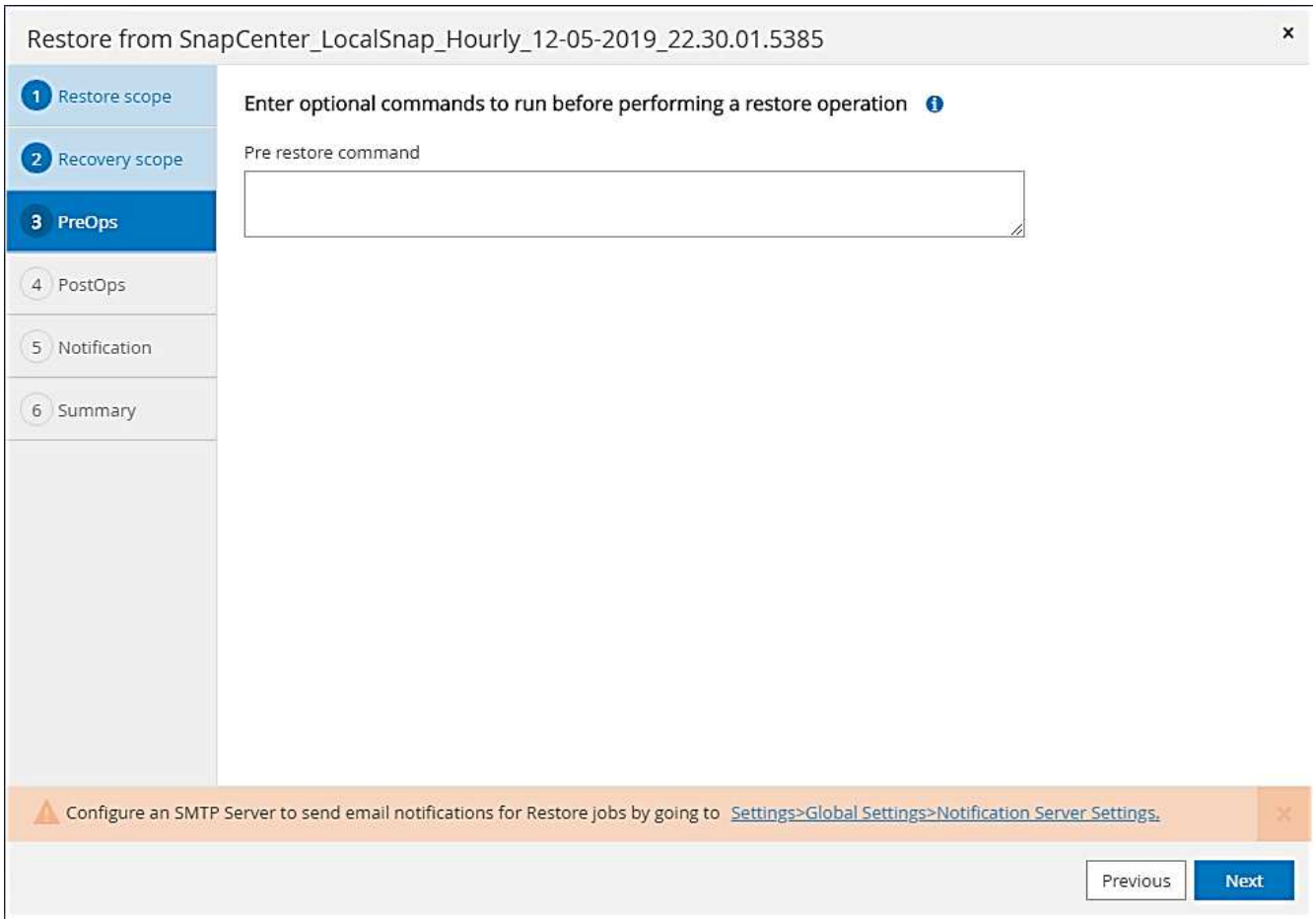


3. Recovery Scope を選択し、ログバックアップとカタログバックアップの場所を指定します。

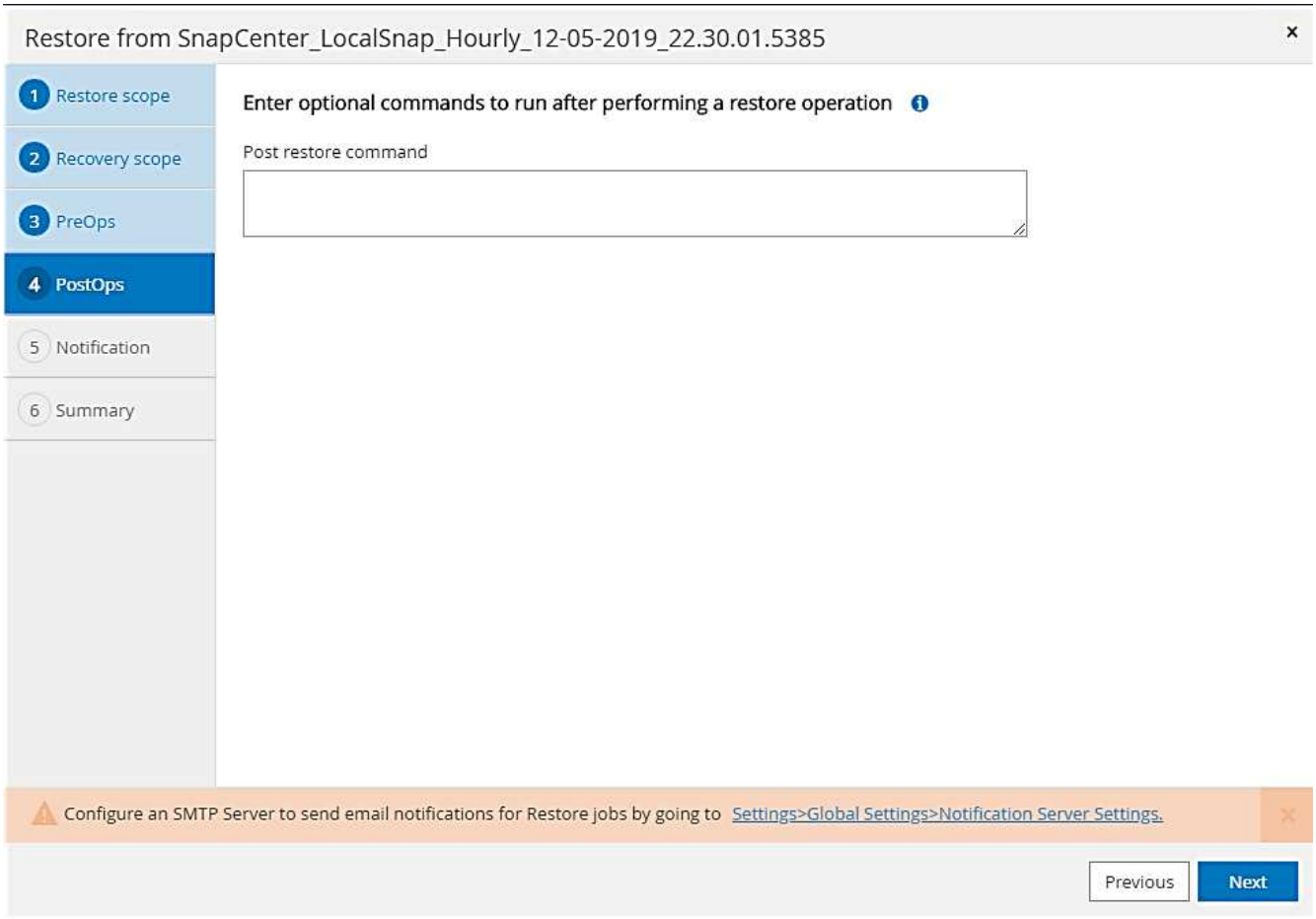
SnapCenter では、 HANA の global.ini ファイルのデフォルトパスまたは変更されたパスを使用して、ログとカタログのバックアップの場所が事前に入力されます。



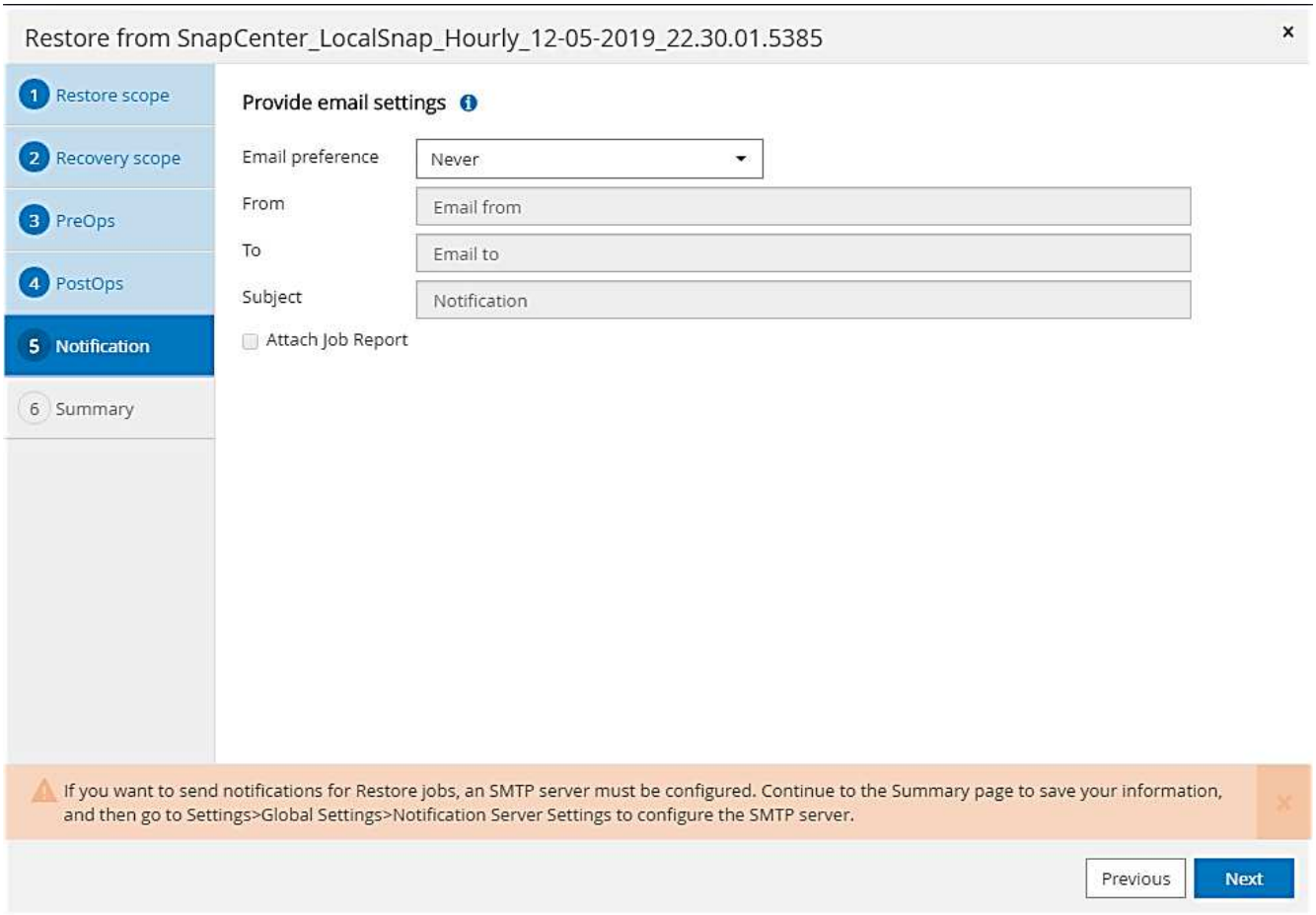
4. オプションのリストア前のコマンドを入力します



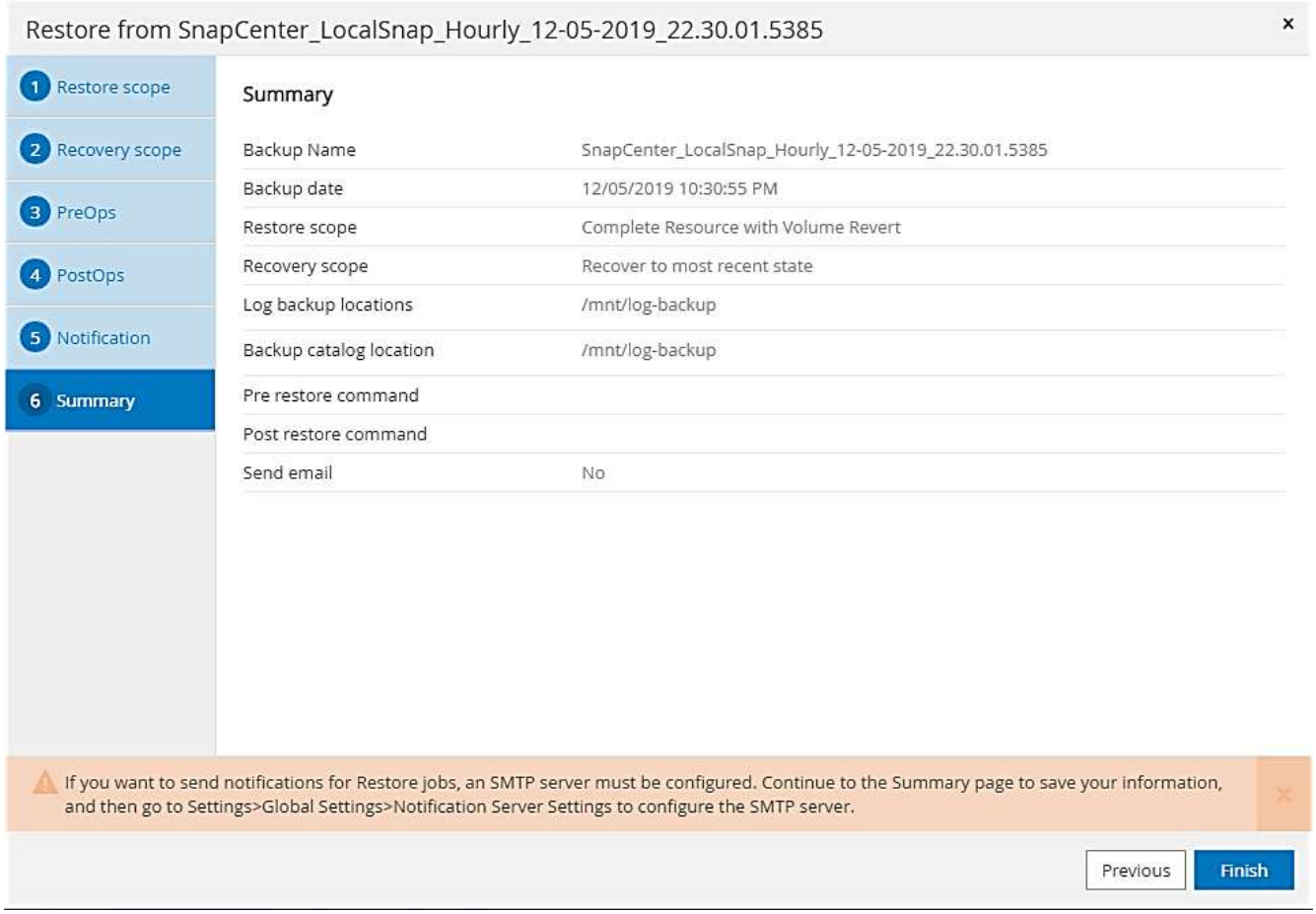
5. オプションのリストア後のコマンドを入力します。



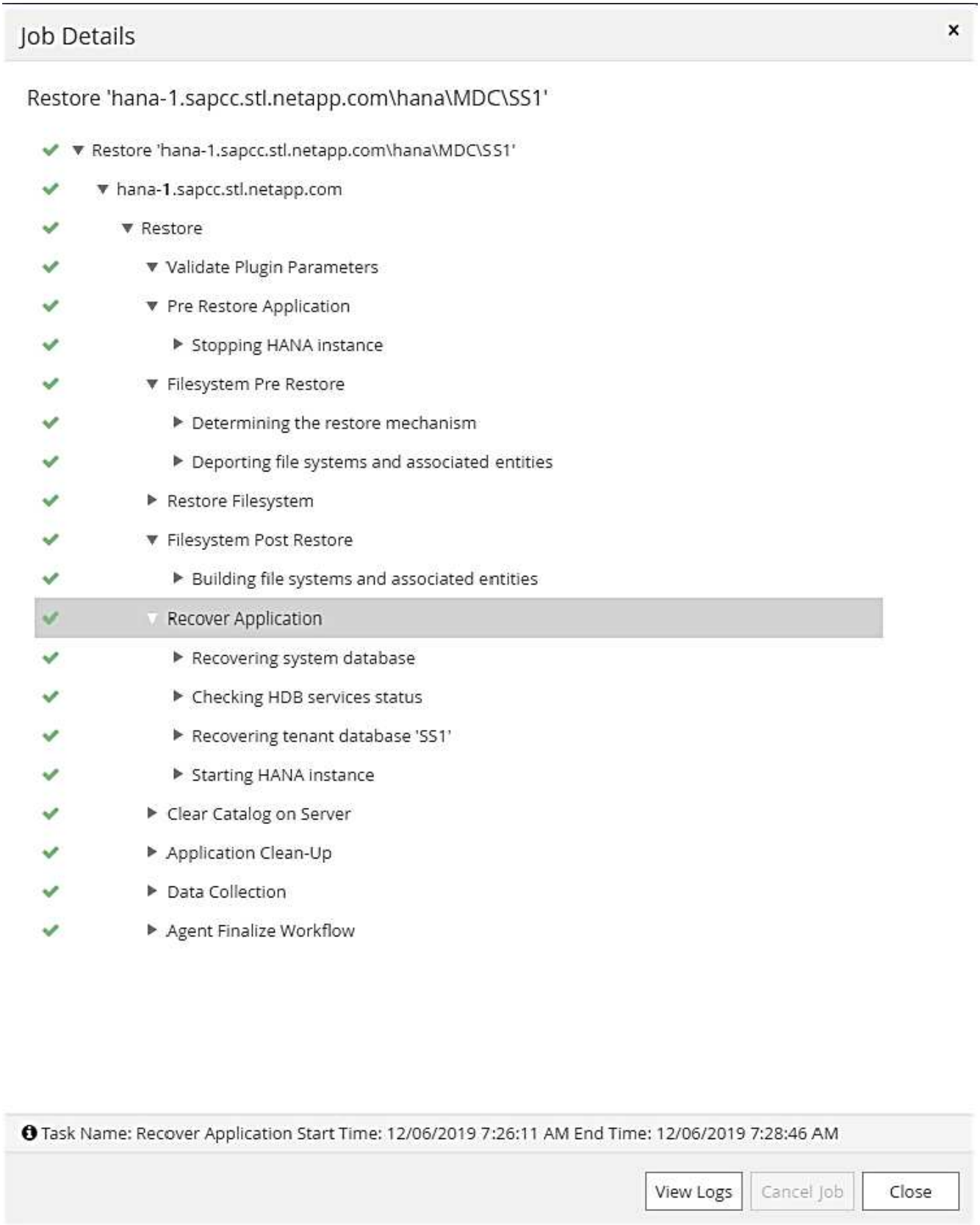
6. オプションの E メール設定を入力します。



7. リストア処理を開始するには、 [完了] をクリックします。



8. SnapCenter によってリストアおよびリカバリ処理が実行されます。この例は、リストアジョブとリカバリジョブのジョブの詳細を表示しています。



シングルテナントでのリストアおよびリカバリ処理

SnapCenter 4.3 では、シングルテナントを使用する HANA MDC システム、または SnapCenter によって自動検出された複数のテナントを使用する場合に、シングルテナントのリストア処理がサポートされます。

シングルテナントのリストアおよびリカバリ処理は、次の手順で実行できます。

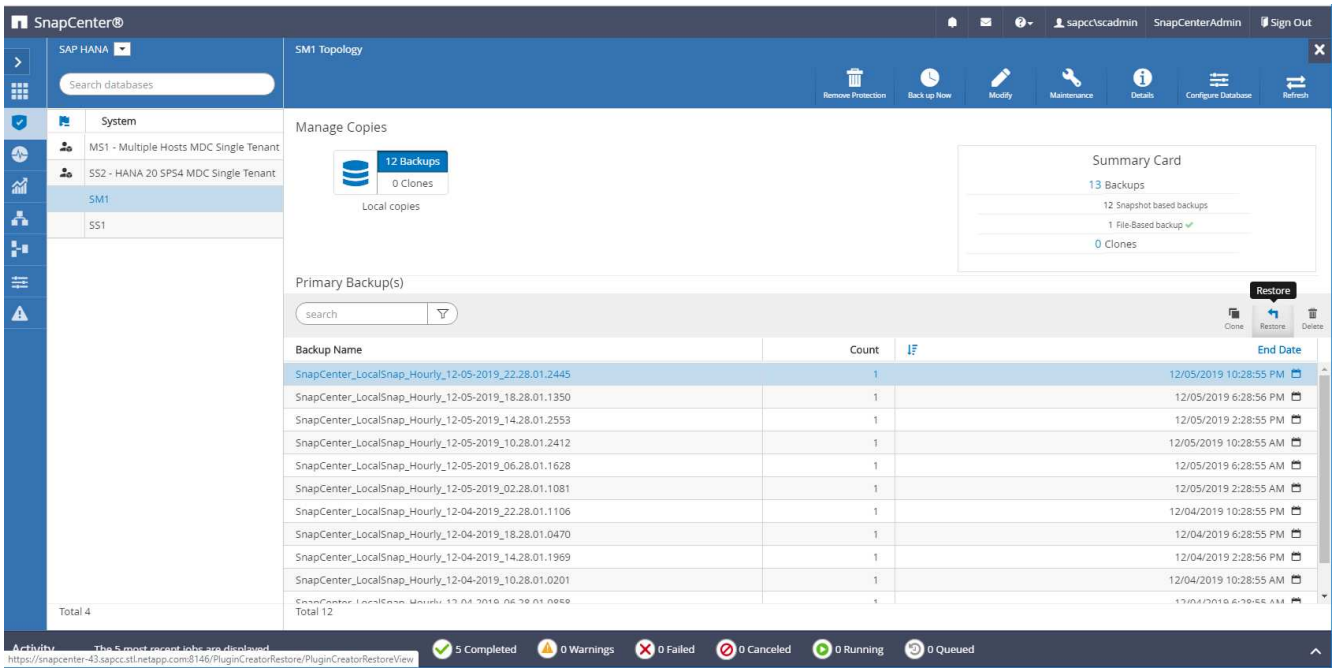
1. リストアおよびリカバリするテナントを停止します。
2. SnapCenter でテナントをリストアします。
   - プライマリストレージからリストアする場合、 SnapCenter は次の処理を実行します。
     - * NFS. * ストレージの単一ファイルの SnapRestore 操作は、テナントデータベースのすべてのファイルに対応しています。
     - * SAN. * LUN のクローンを作成してデータベースホストに接続し、テナント・データベースのすべてのファイルをコピーします。
   - セカンダリストレージからリストアする場合、 SnapCenter は次の処理を実行します。
     - * nfs.* テナントデータベースのすべてのファイルに対する Storage SnapVault リストア処理
     - * SAN. * LUN のクローンを作成してデータベースホストに接続し、テナント・データベースのすべてのファイルをコピーします
3. HANA Studio 、 Cockpit 、または SQL ステートメントを使用してテナントをリカバリします。

このセクションでは、自動検出された HANA システム SM1 （ SAP HANA シングルホスト、 MDC マルチテナントシステム、 NFS を使用）のプライマリストレージからリストアとリカバリの処理を実行する手順を説明します。ユーザ入力の観点では、ファイバチャネル SAN の設定でセカンダリまたはリストアを実行する場合のワークフローは同じです。

1. テナントデータベースを停止します。

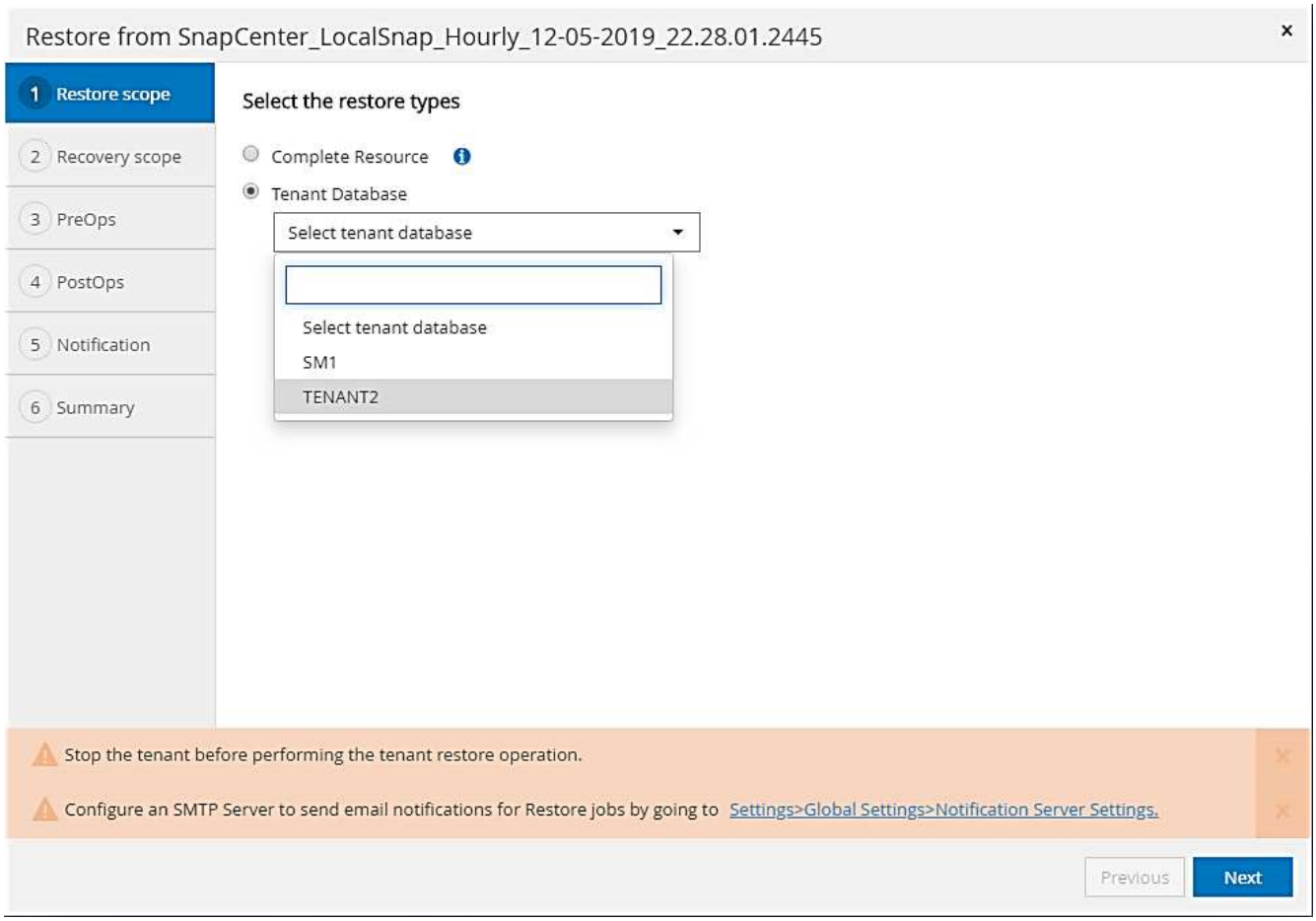
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

2. SnapCenter で、リストア処理に使用するバックアップを選択します。

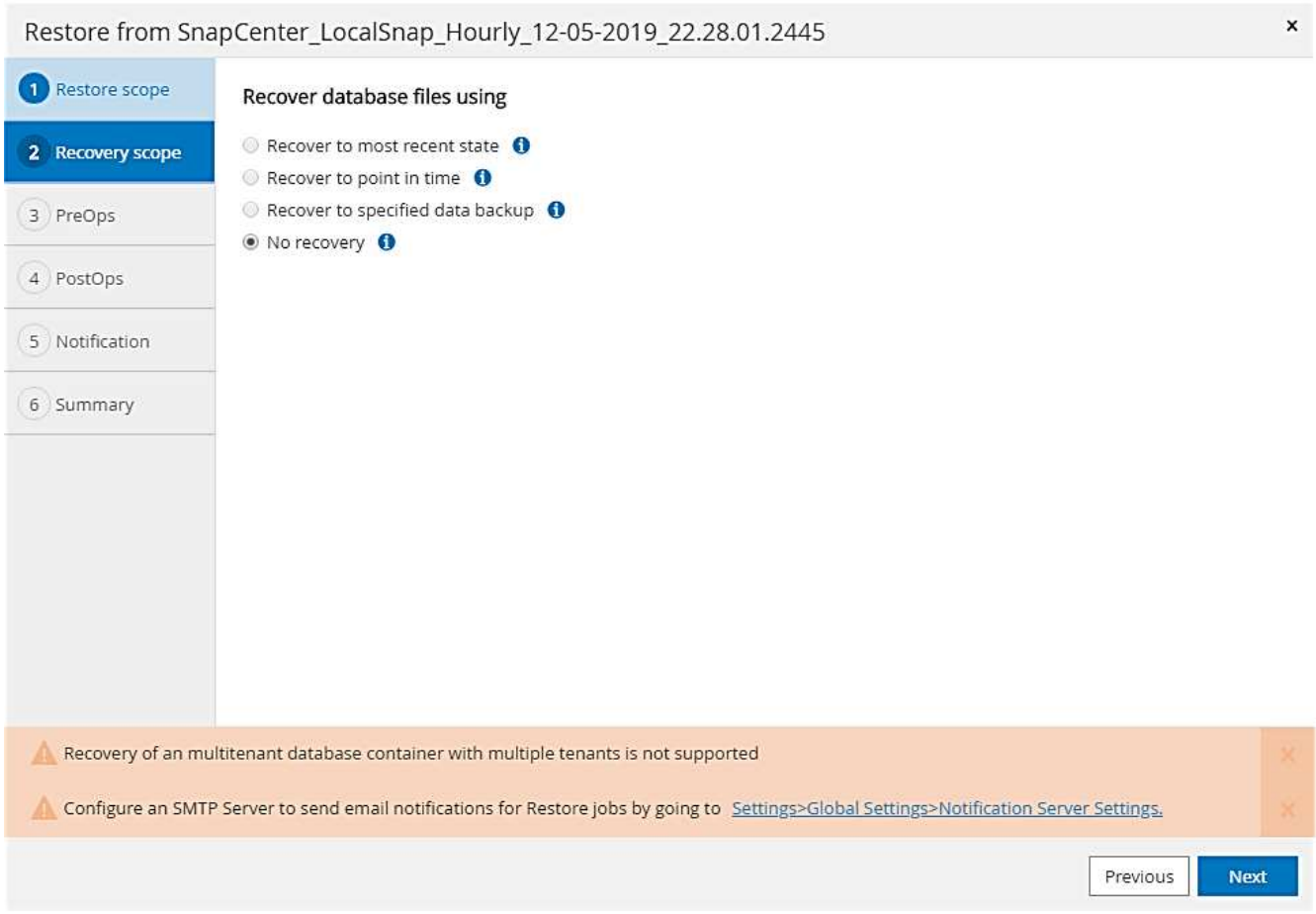


3. リストアするテナントを選択します。

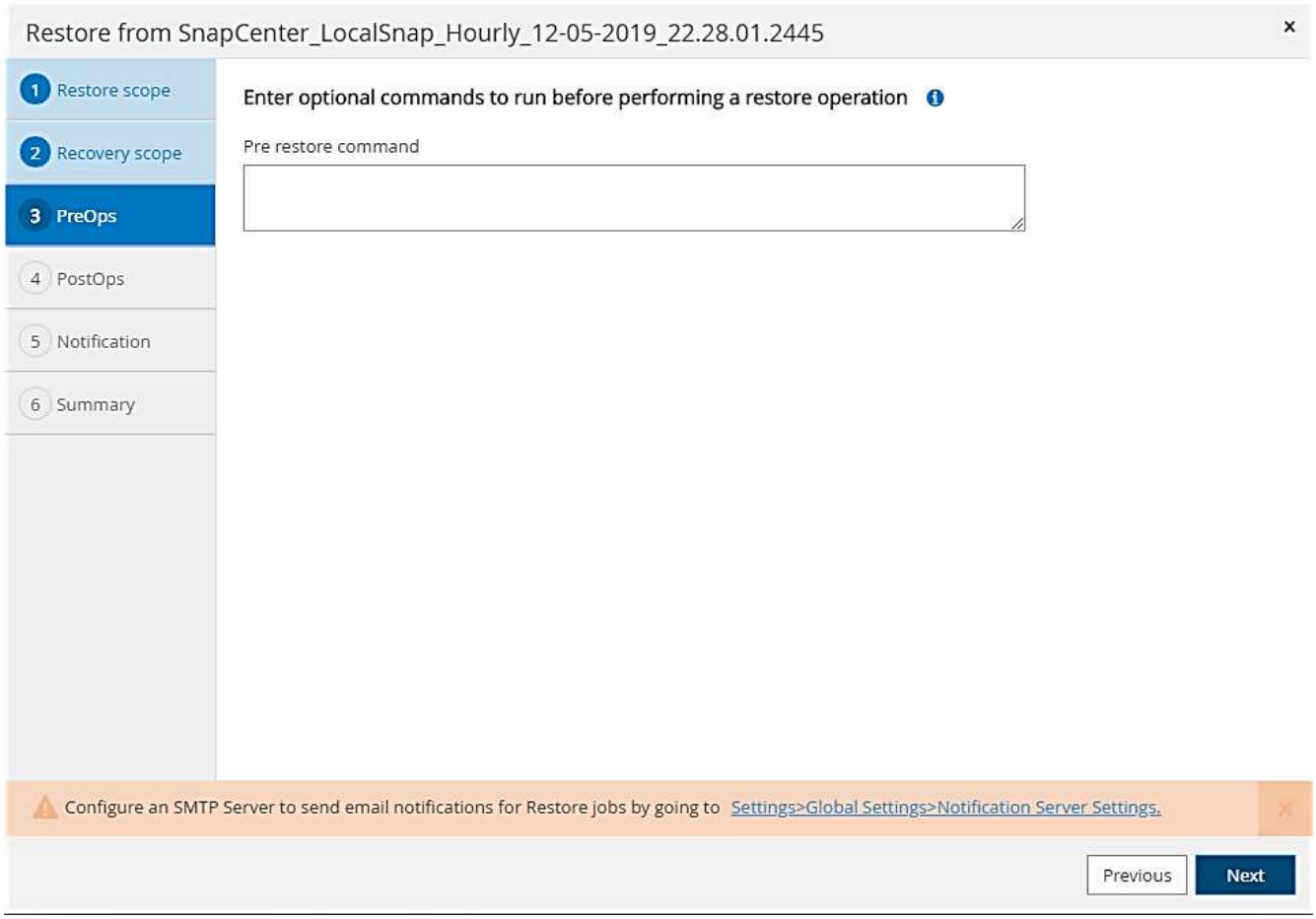
SnapCenter に、選択したバックアップに含まれるすべてのテナントのリストが表示されます。



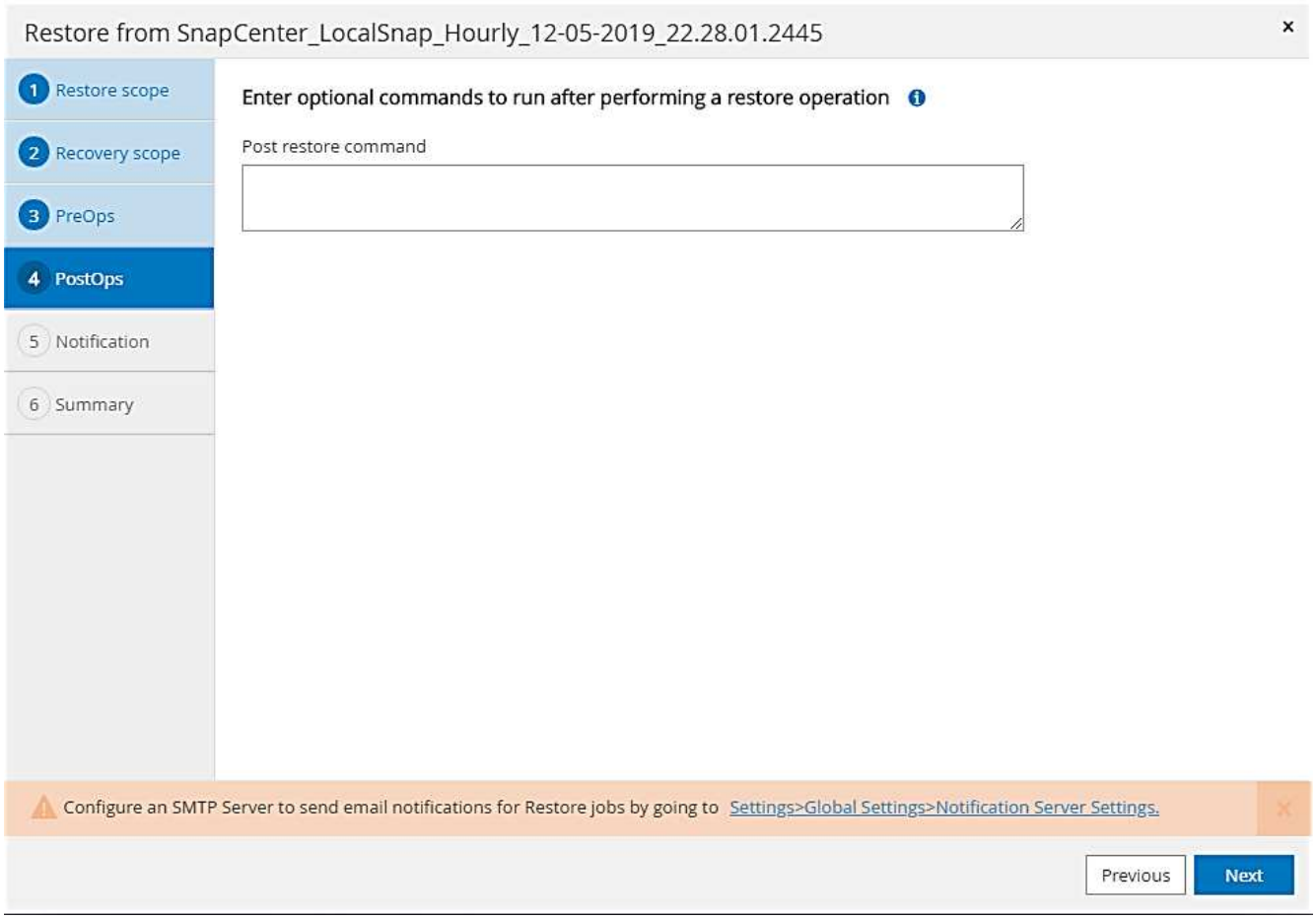
シングルテナントリカバリは、 SnapCenter 4.3 ではサポートされていません。リカバリは事前に選択されておらず、変更することはできません。



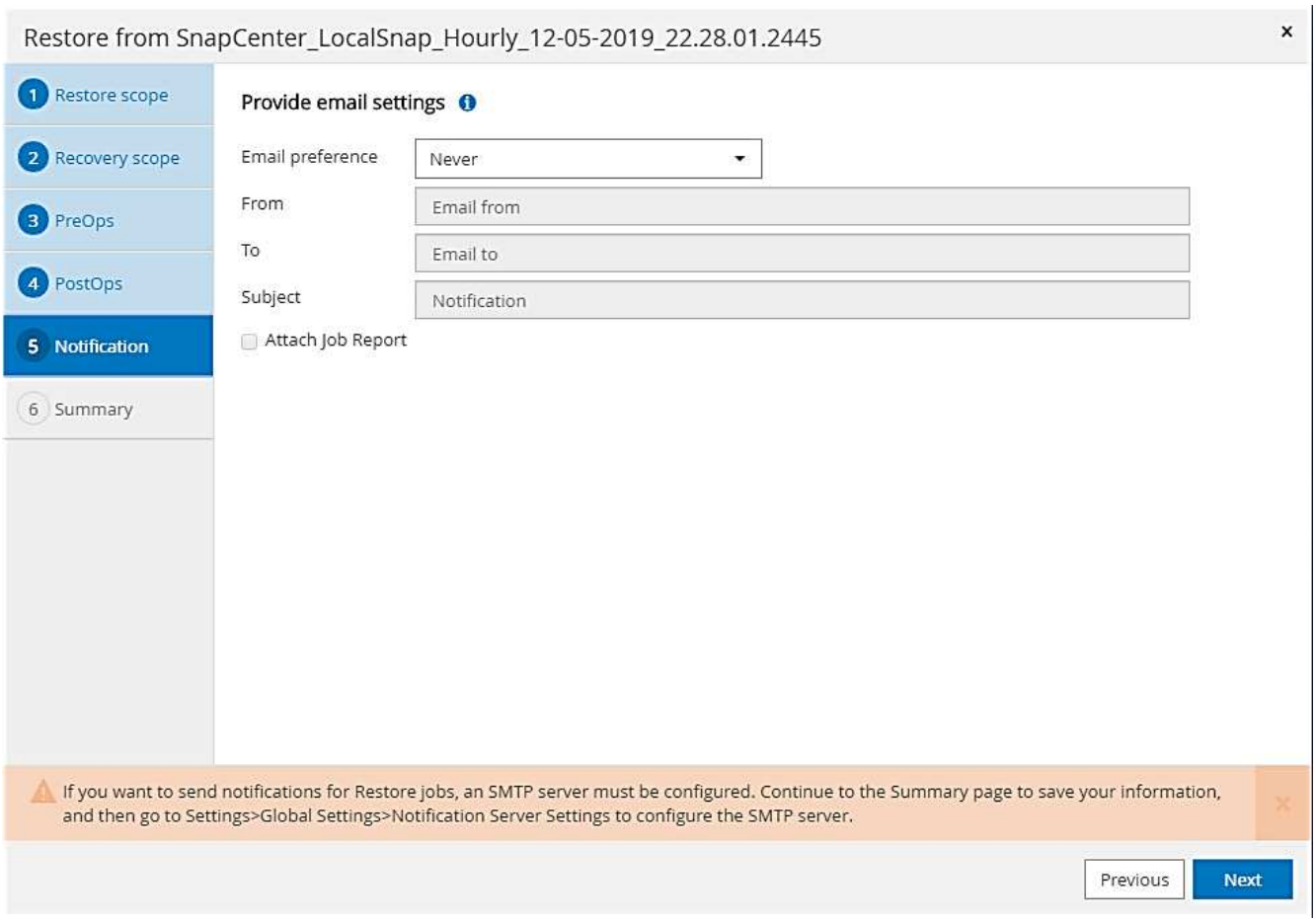
4. オプションのリストア前のコマンドを入力します



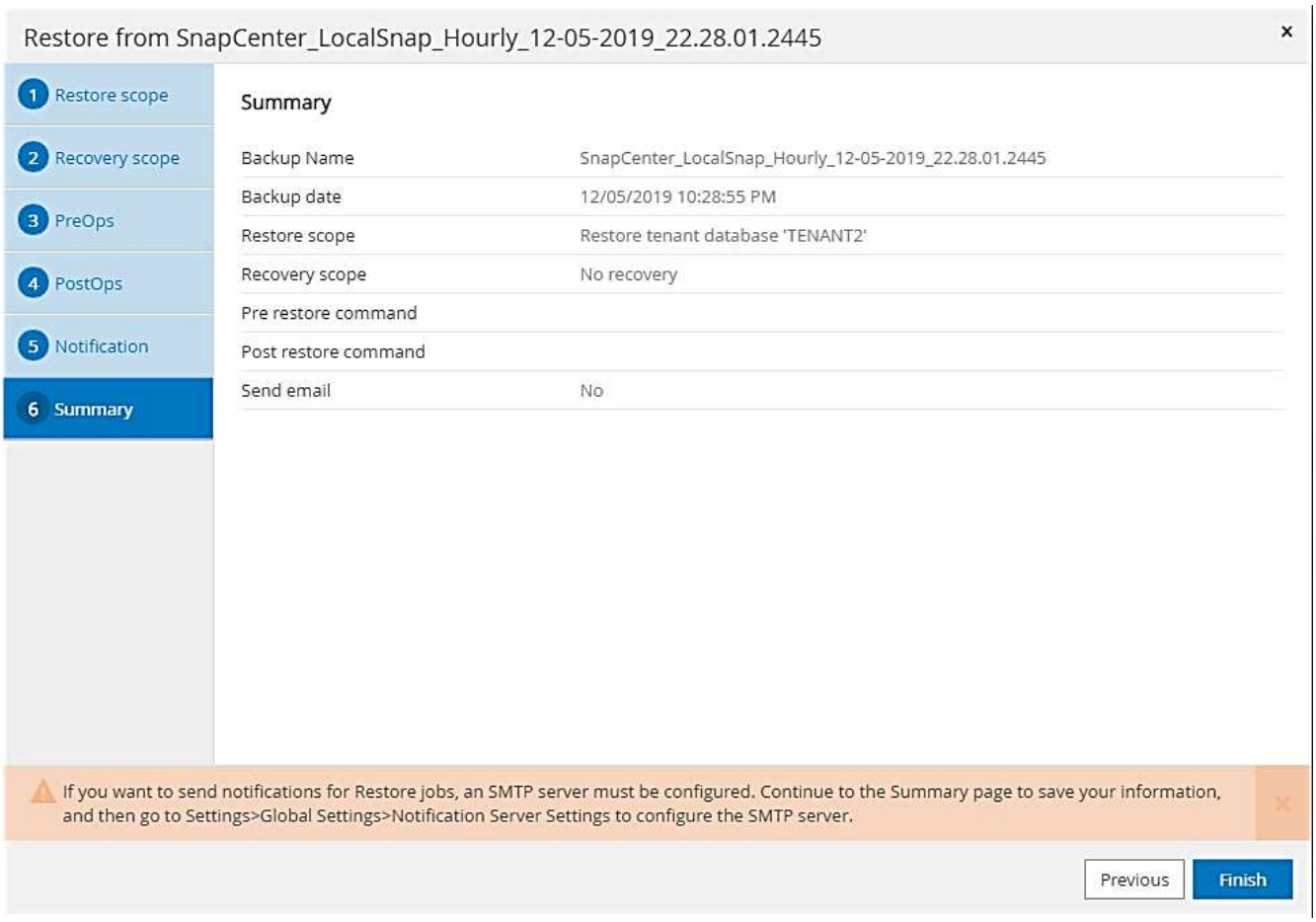
5. オプションのリストア後のコマンドを入力します。



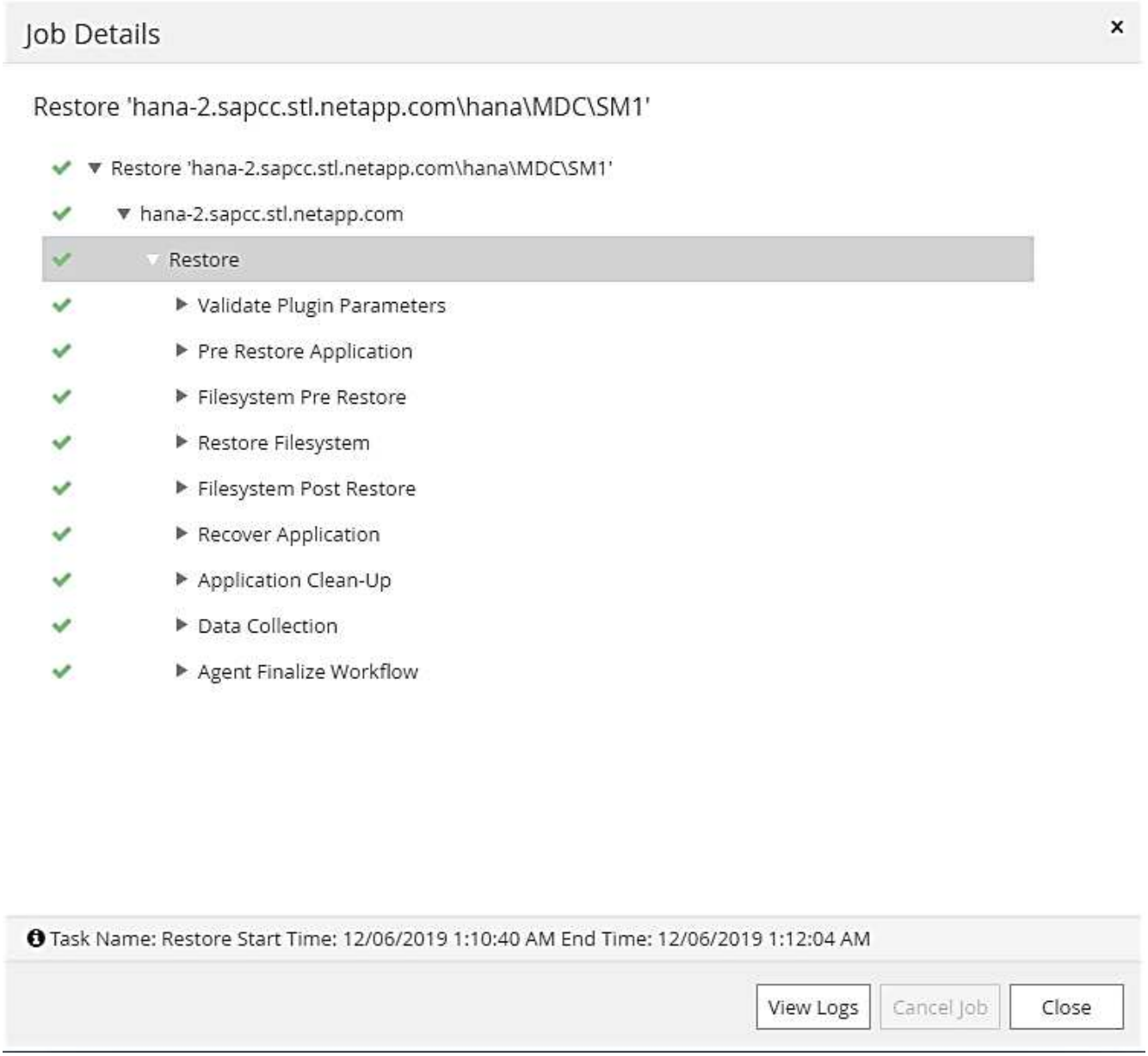
6. オプションの E メール設定を入力します。



7. リストア処理を開始するには、 [完了] をクリックします。



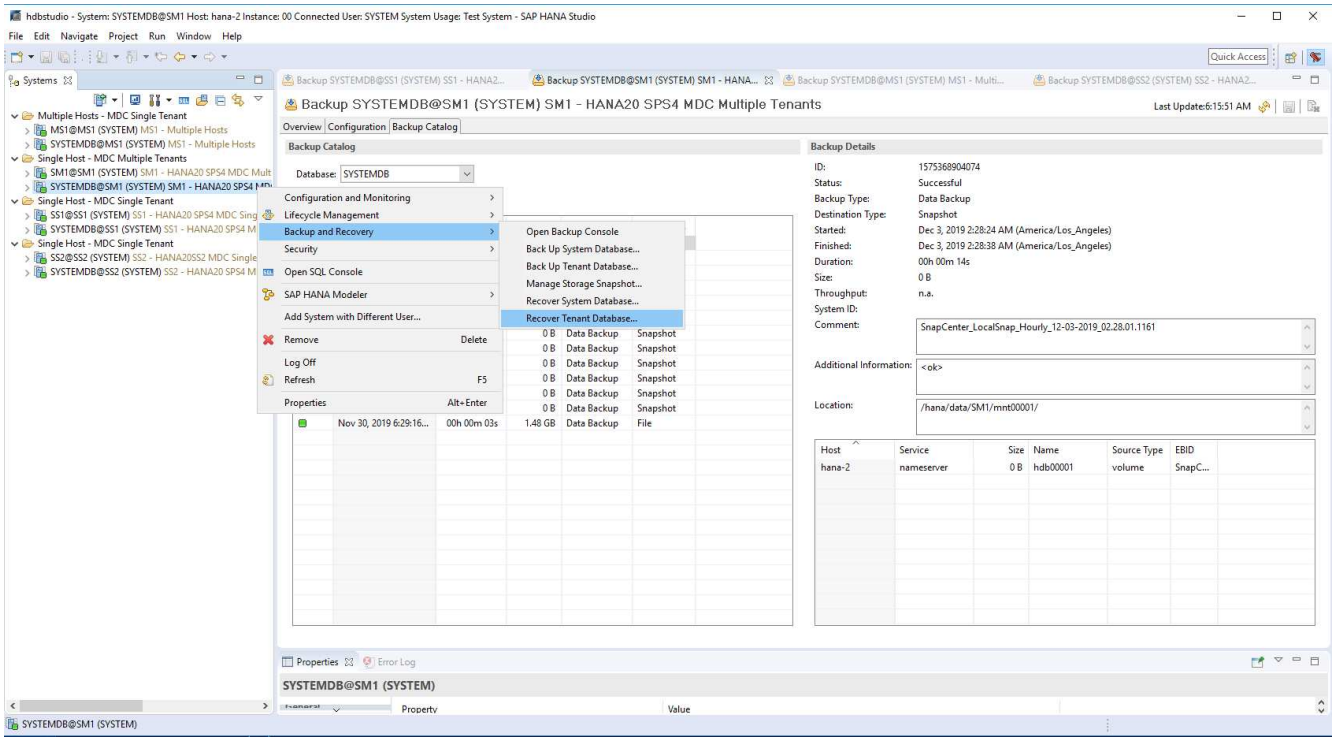
リストア処理は SnapCenter によって実行されます。この例は、リストアジョブのジョブの詳細を表示します。



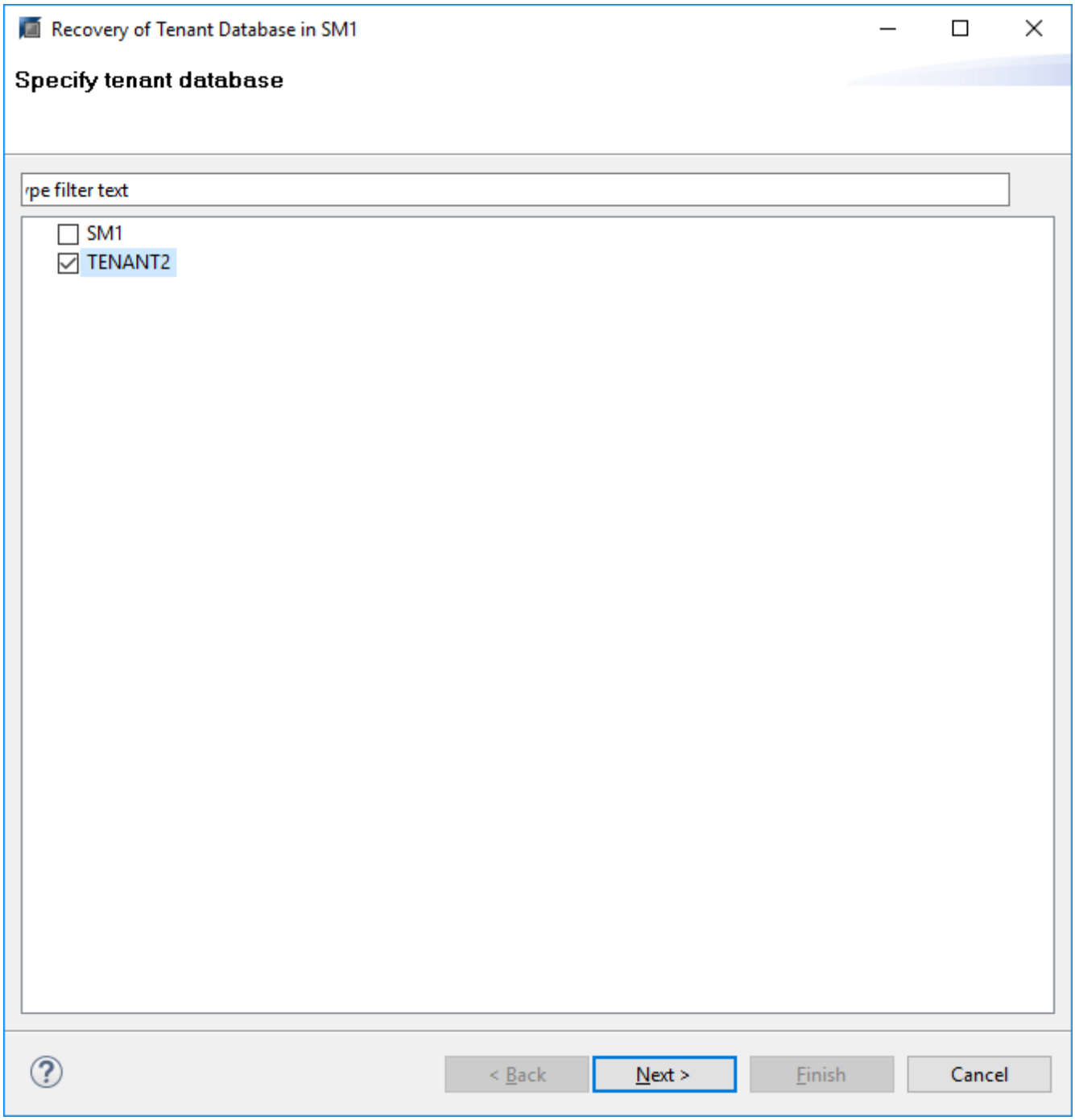
テナントのリストア処理が終了すると、テナントに関連するデータのみがリストアされます。HANA データベースホストのファイルシステムで、リストアしたデータファイルとテナントの Snapshot バックアップ ID ファイルを使用できます。

```
sm1adm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 sm1adm sapsys   17 Dec  6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r----- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r----- 1 sm1adm sapsys          0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys         36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 sm1adm sapsys      4096 Nov 20 08:37 .
drwxr-x--- 6 sm1adm sapsys      4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 201441280 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys         0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 03:57 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 01:14 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys     155648 Dec  6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
sm1adm@hana-2:/usr/sap/SM1/HDB00>
```

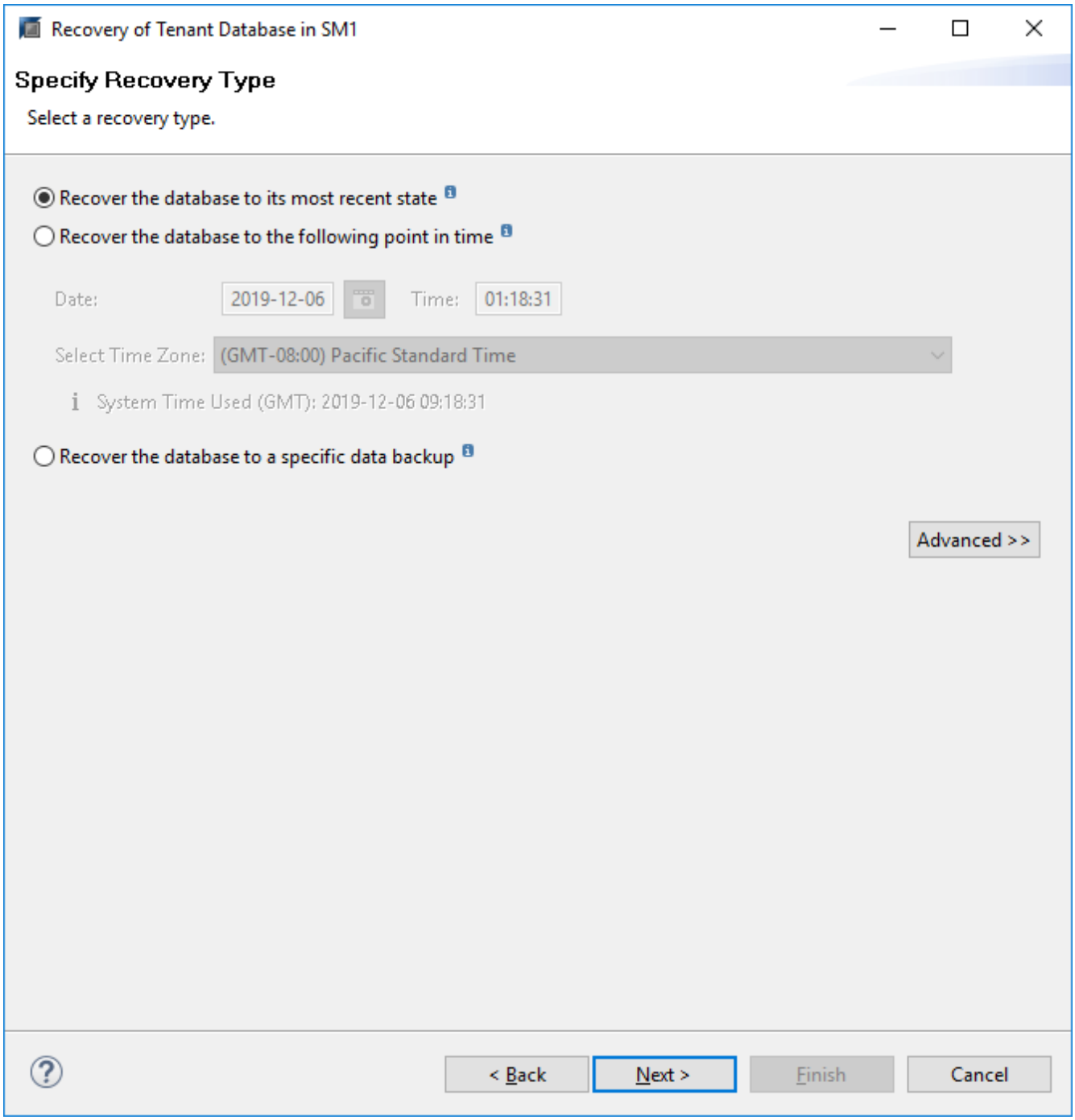
8. HANA Studio でリカバリを開始します。



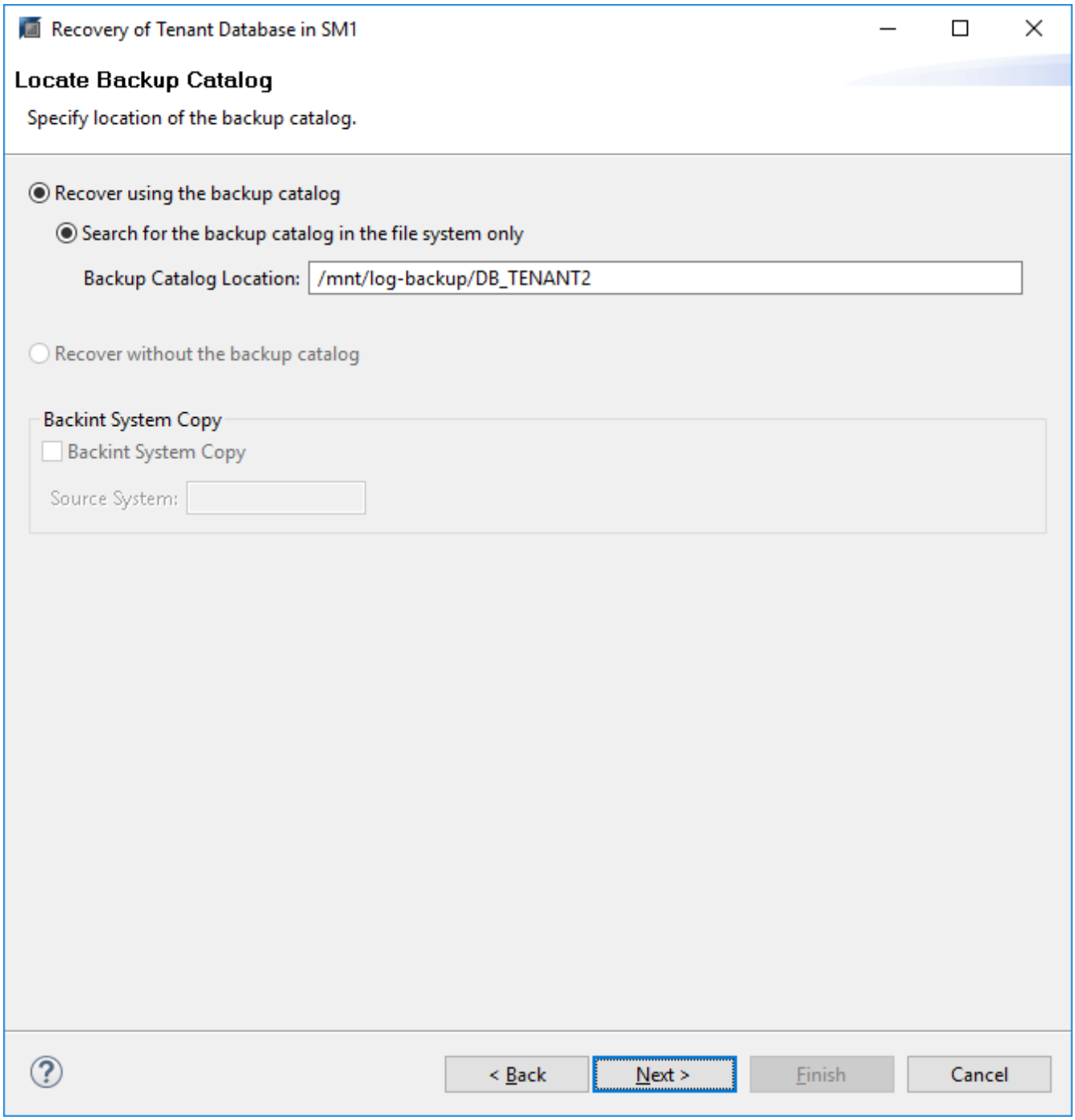
9. テナントを選択します。

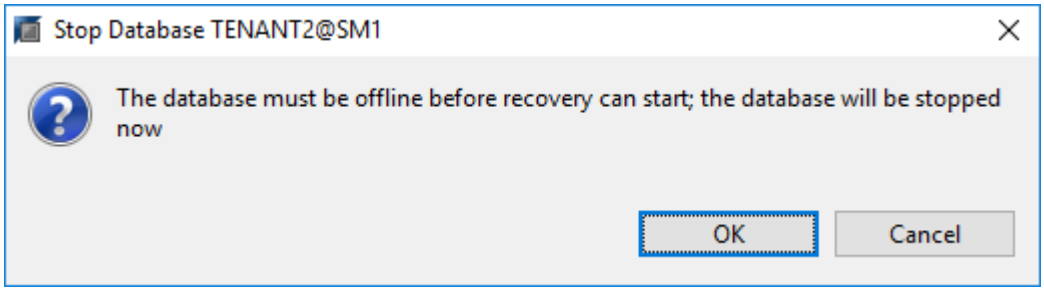


10. リカバリのタイプを選択します。



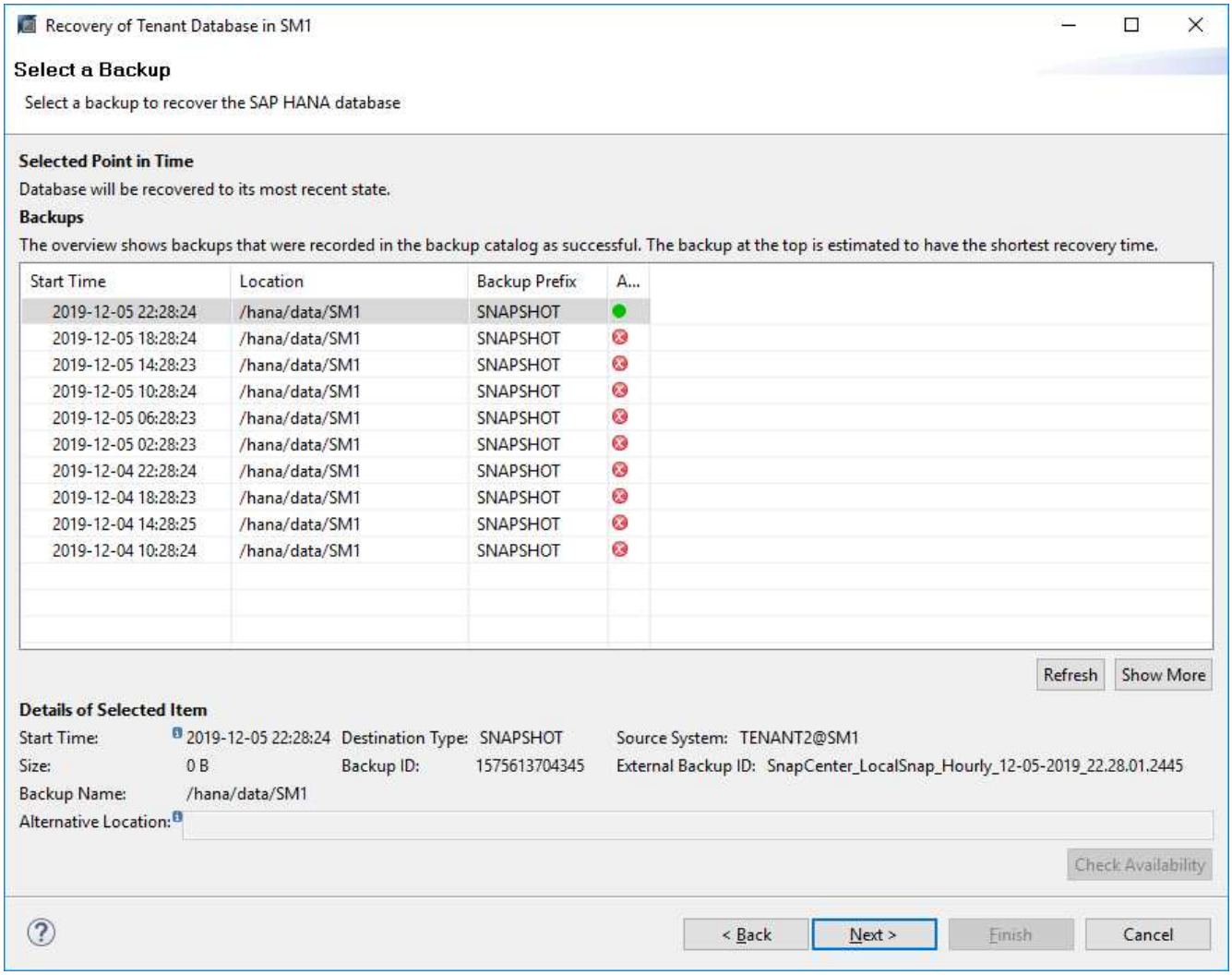
11. バックアップカタログの場所を指定します。



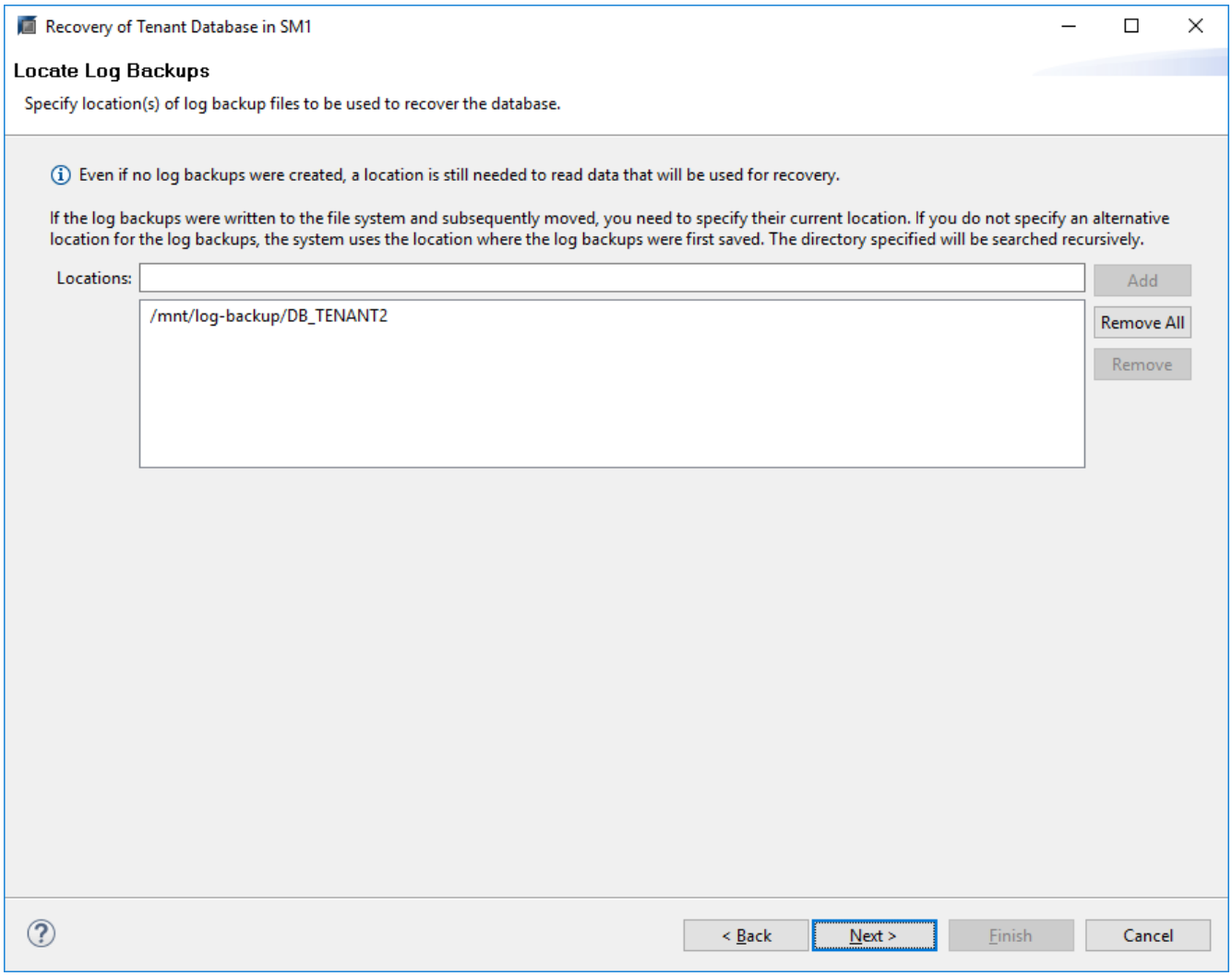


バックアップカタログ内で、リストアされたバックアップが緑のアイコンで強調表示されます。外部バックアップ ID には、 SnapCenter で以前に選択されたバックアップ名が表示されます。

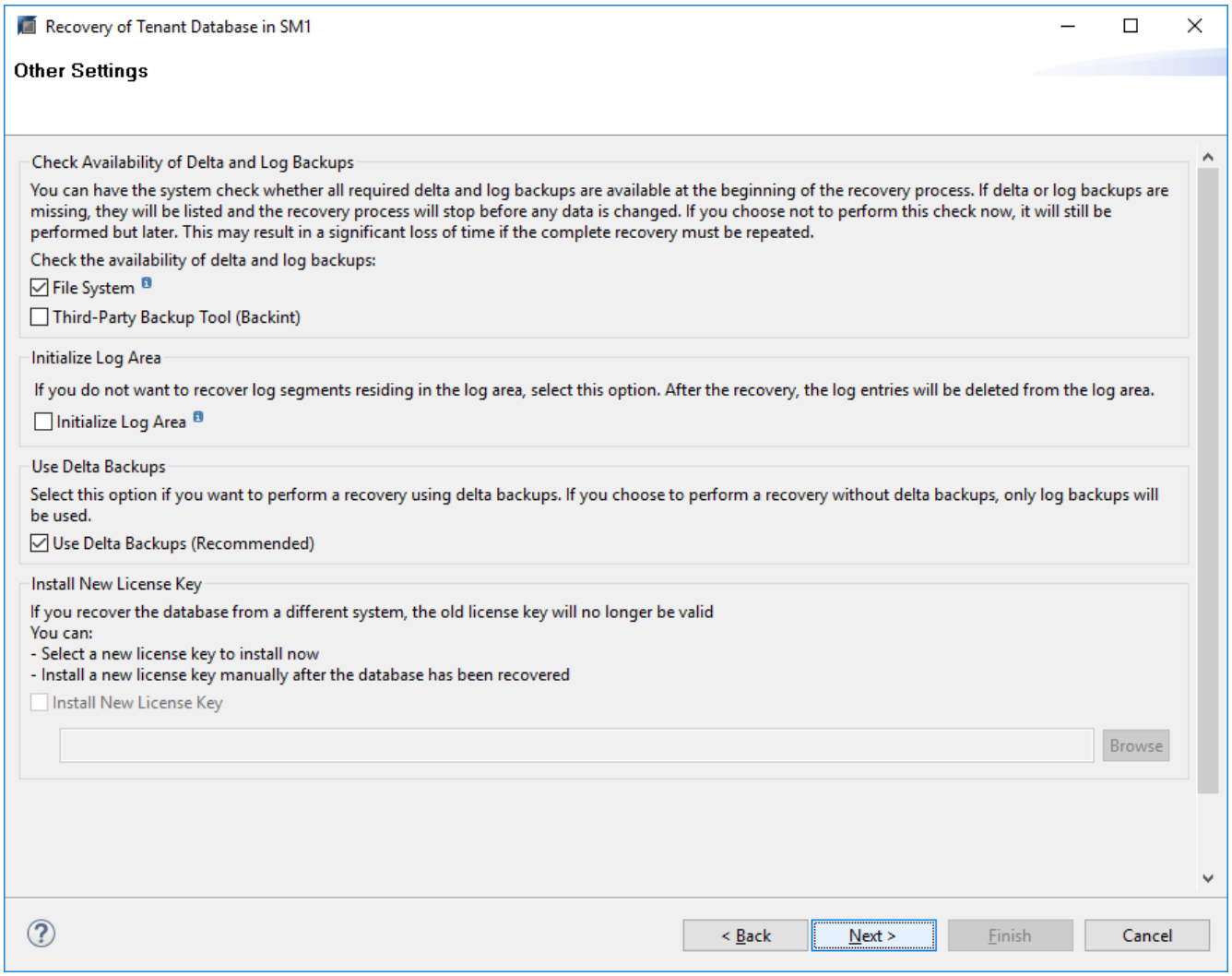
12. 緑のアイコンが表示されたエントリを選択し、次へをクリックします。



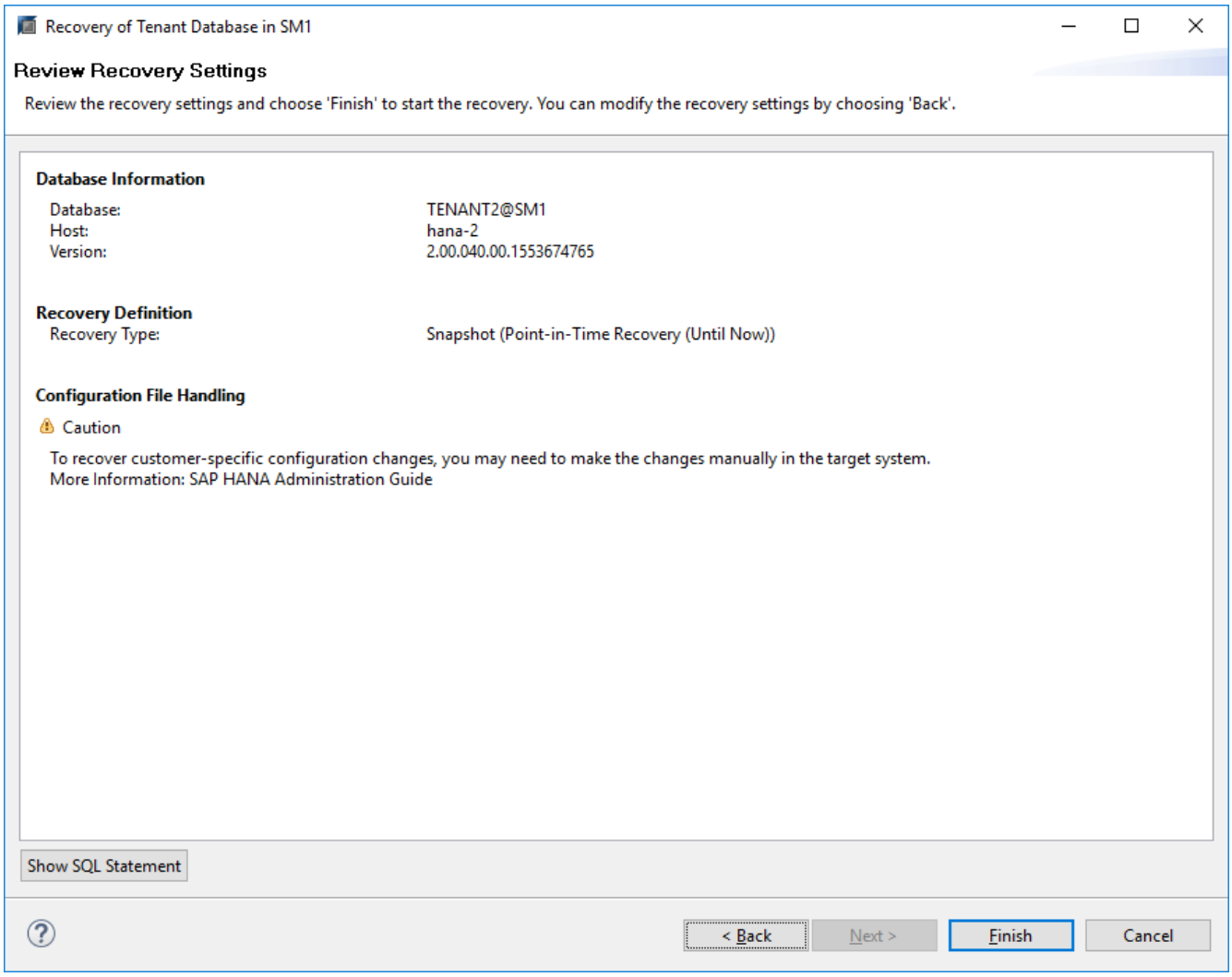
13. ログのバックアップ先を指定します。

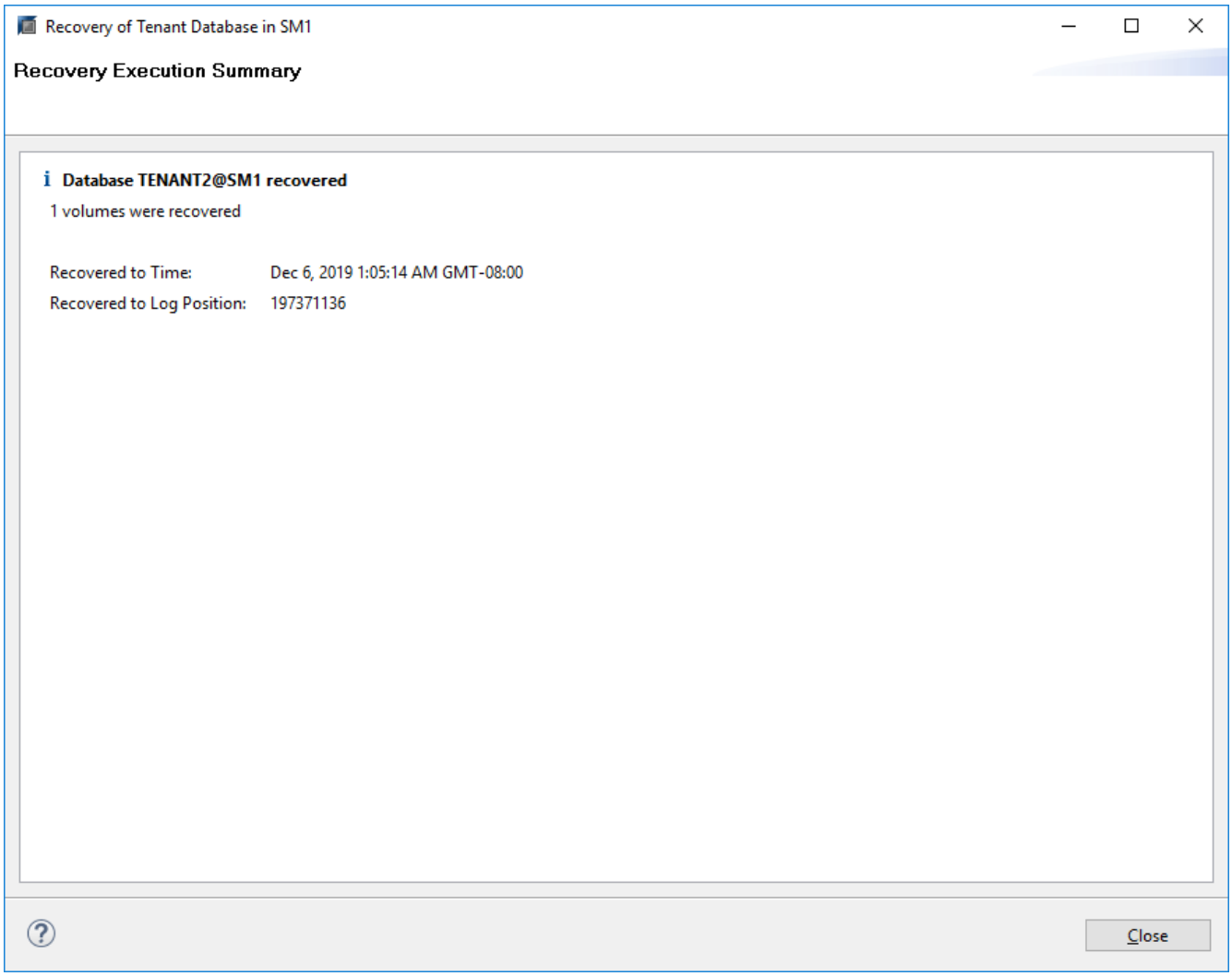


14. 必要に応じて、他の設定を選択します。



15. テナントのリカバリ処理を開始します。


Recovery of Tenant Database in SM1
Review Recovery Settings
Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.
Database Information
Database: TENANT2@SM1
Host: hana-2
Version: 2.00.040.00.1553674765
Recovery Definition
Recovery Type: Snapshot (Point-in-Time Recovery (Until Now))
Configuration File Handling
Caution
To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide
Show SQL Statement
< Back
Next >
Finish
Cancel



手動リカバリによるリストア

SAP HANA Studio および SnapCenter を使用して SAP HANA MDC のシングルテナントシステムをリストアおよびリカバリするには、次の手順を実行します。

1. SAP HANA Studio でリストアとリカバリのプロセスを準備します。
   a. システムデータベースのリカバリを選択し、 SAP HANA システムのシャットダウンを確認します。
   b. リカバリタイプとログのバックアップ先を選択します。
   c. データバックアップのリストが表示されます。外部バックアップ ID を表示するには、 Backup を選択します。
2. SnapCenter でリストアプロセスを実行します。
   a. リソースのトポロジビューで、オフサイトのバックアップストレージからリストアする場合は、プライマリストレージまたはバックアップコピーからリストアするローカルコピーを選択します。
   b. SAP HANA Studio の外部バックアップの ID またはコメントフィールドと一致する SnapCenter バックアップを選択します。
   c. リストアプロセスを開始します。

プライマリストレージからボリュームベースのリストアを選択した場合は、リストアプロセスの完了後に、すべての SAP HANA データベースホストからデータボリュームをアンマウントして再度マウントする必要があります。

FC を使用する SAP HANA マルチホスト環境では、データベースのシャットダウンと起動のプロセスの一環として、 SAP HANA ネームサーバによってアンマウントとマウントの処理が実行されます。

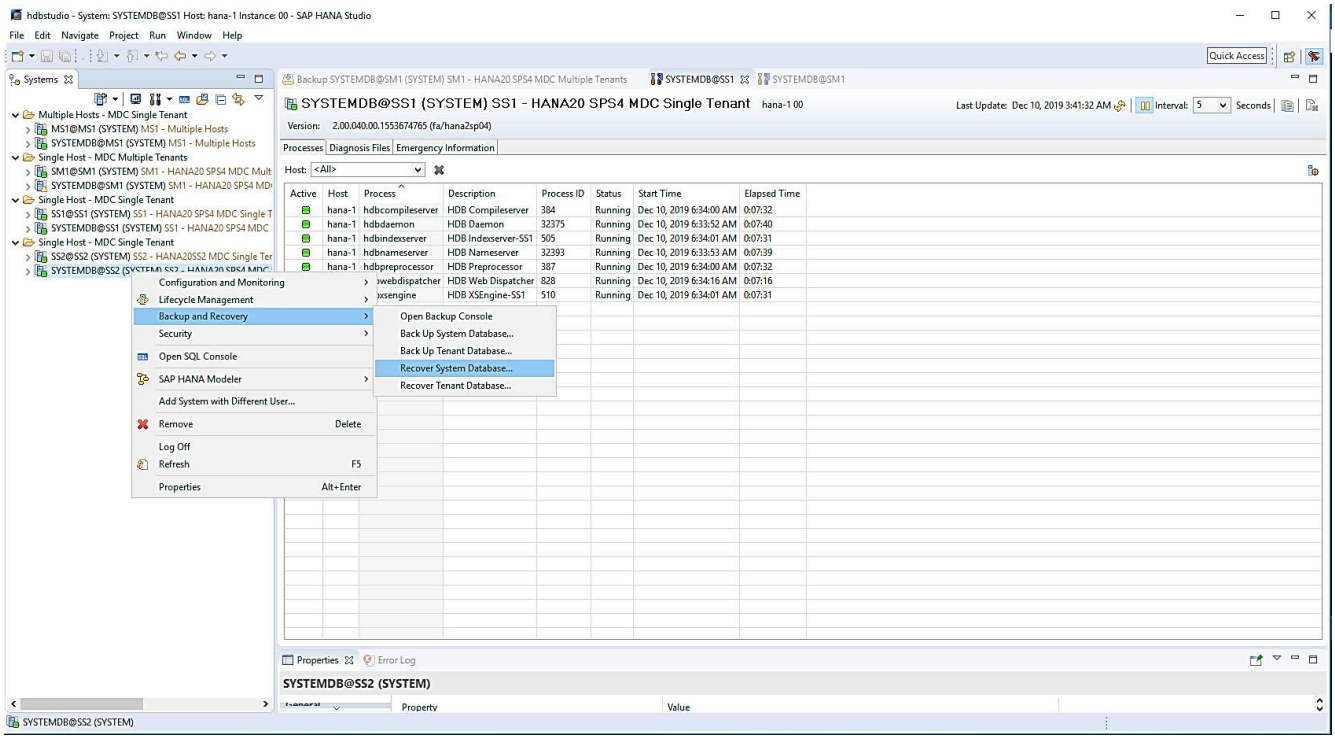
3. SAP HANA Studio を使用して、システムデータベースのリカバリプロセスを実行します。
   a. バックアップ・リストから [更新] をクリックし ' リカバリに使用できるバックアップを選択します（緑色のアイコンが表示されます）
   b. リカバリプロセスを開始します。リカバリプロセスが完了すると、システムデータベースが起動します。
4. SAP HANA Studio を使用してテナントデータベースのリカバリプロセスを実行します。
   a. [Recover Tenant Database] を選択して、リカバリするテナントを選択します。
   b. リカバリタイプとログのバックアップ先を選択します。

      データバックアップのリストが表示されます。データボリュームはすでにリストアされているため、テナントのバックアップは使用可能（緑）と表示されます。

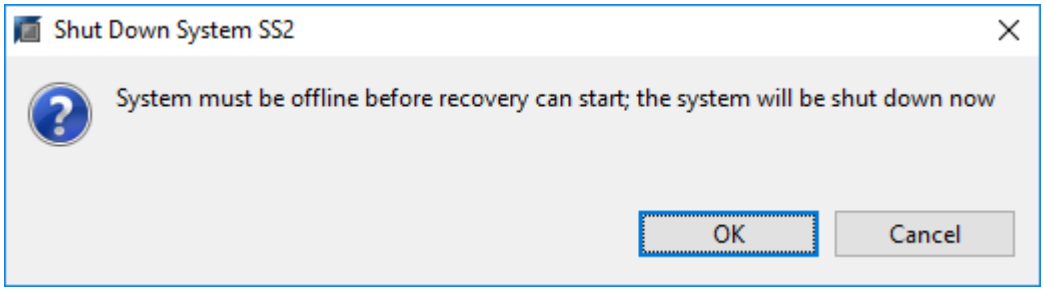
   c. このバックアップを選択し、リカバリプロセスを開始します。リカバリプロセスが完了すると、テナントデータベースが自動的に起動します。

次のセクションでは、手動で設定した HANA システム SS2 （ SAP HANA シングルホスト、 NFS を使用した MDC マルチテナントシステム）のリストア処理とリカバリ処理の手順について説明します。

1. SAP HANA Studio で、 Recover System Database オプションを選択して、システムデータベースのリカバリを開始します。

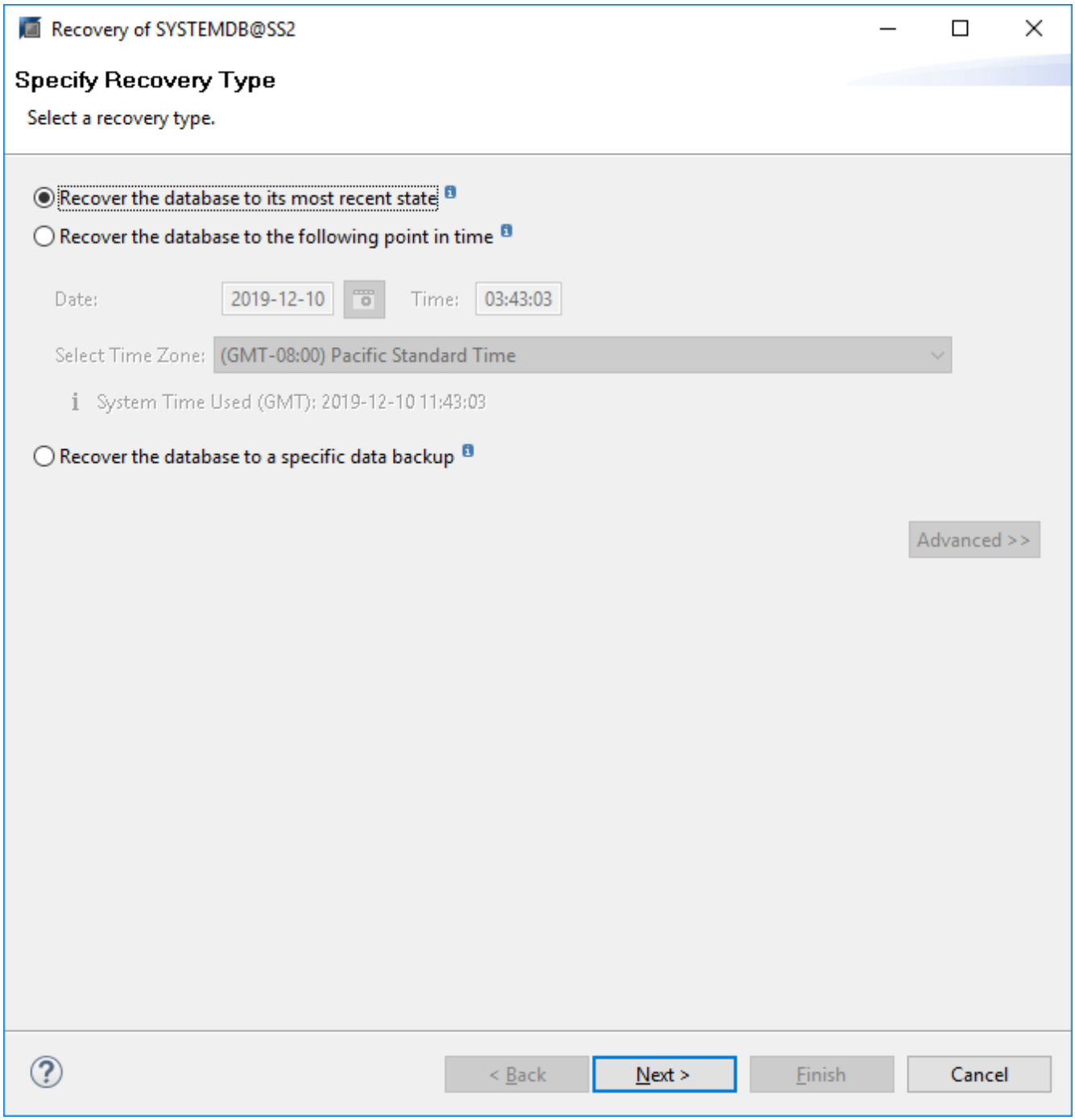


2. [OK] をクリックして、 SAP HANA データベースをシャットダウンします。

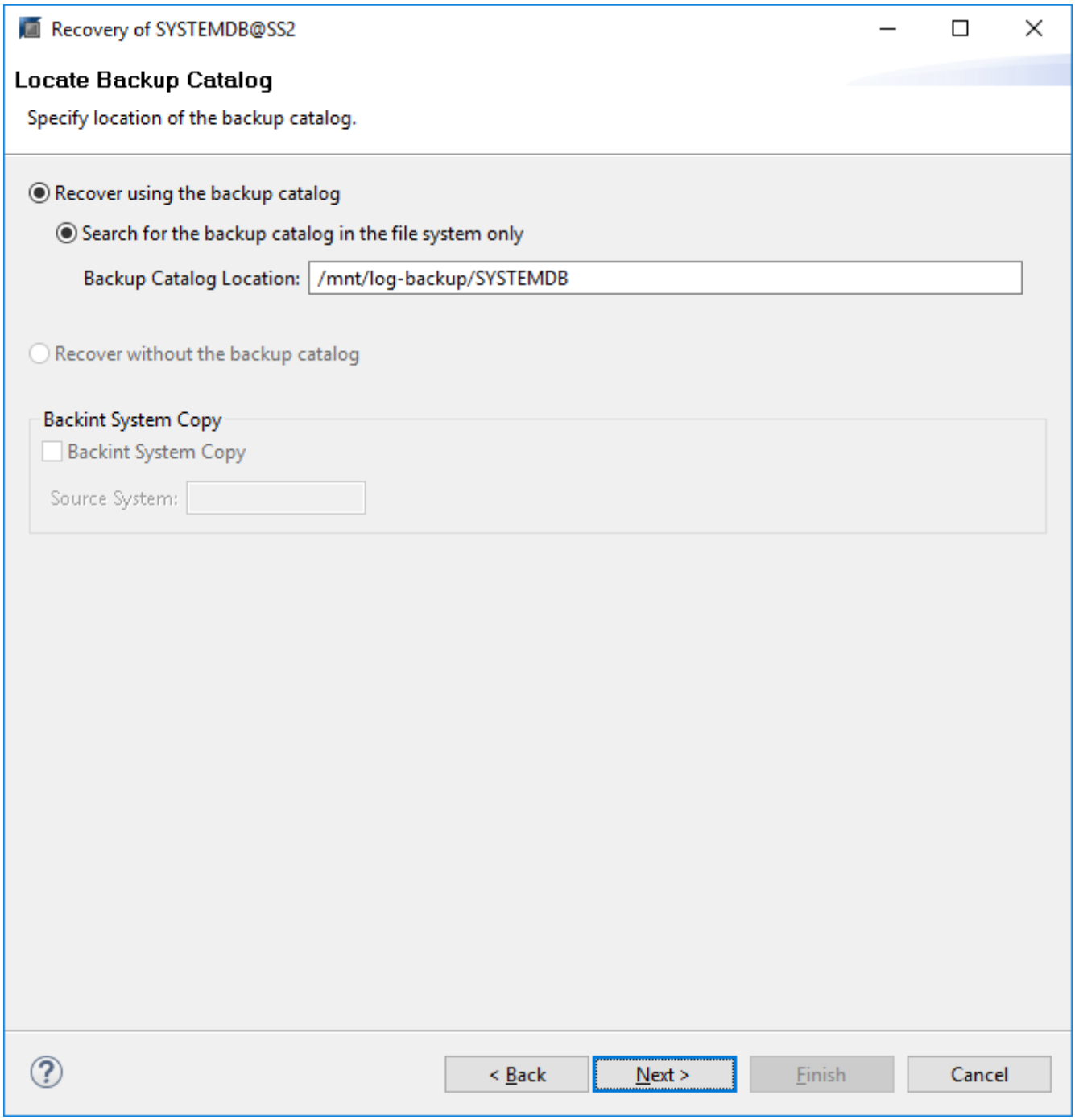


SAP HANA システムがシャットダウンし、リカバリウィザードが起動します。

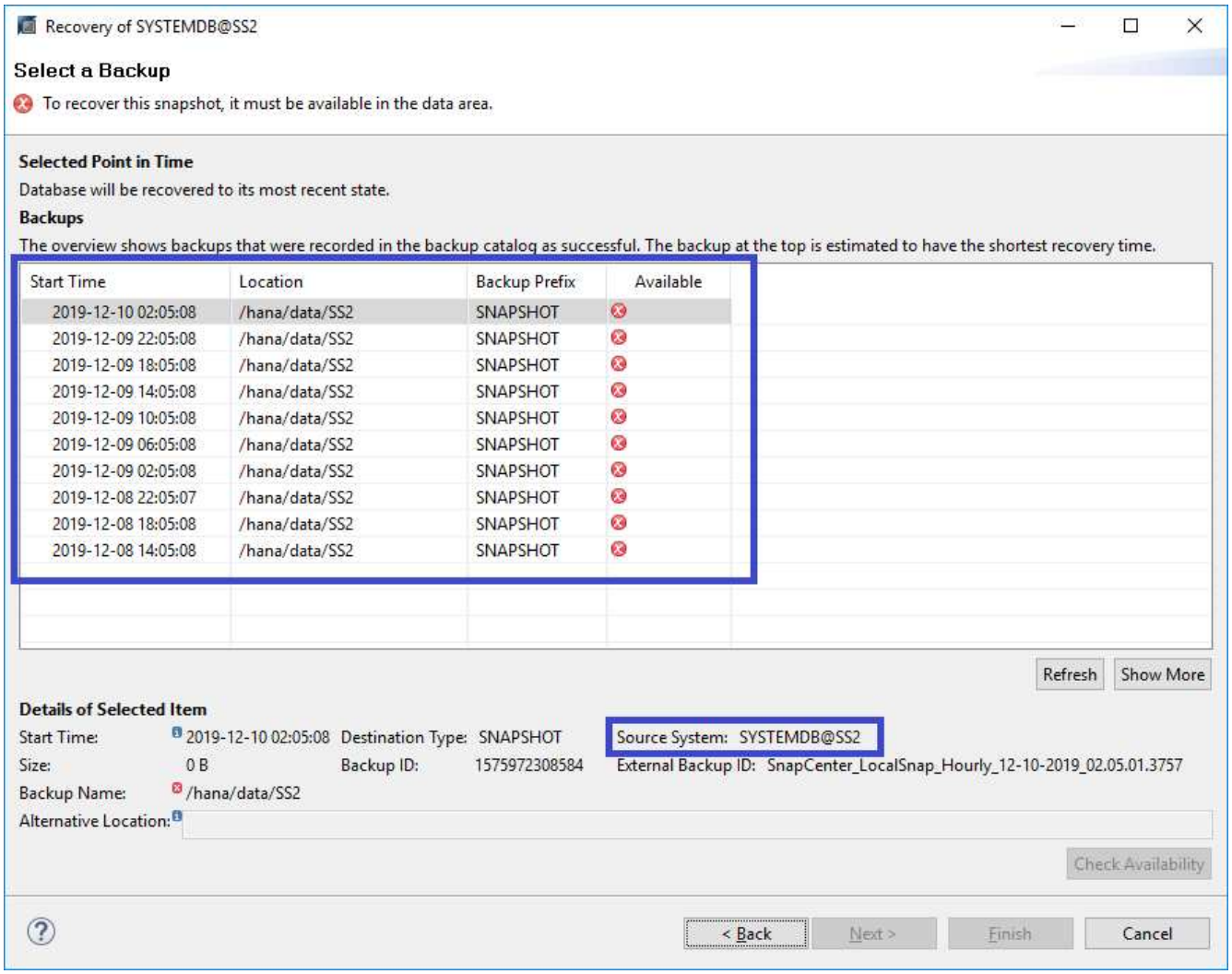
3. リカバリタイプを選択して、 Next （次へ）をクリックします。



4. バックアップカタログの場所を指定し、 [次へ] をクリックします。



5. バックアップカタログの内容に基づいて、使用可能なバックアップのリストが表示されます。必要なバックアップを選択し、外部バックアップ ID をメモします。この例では、最新バックアップを選択します。



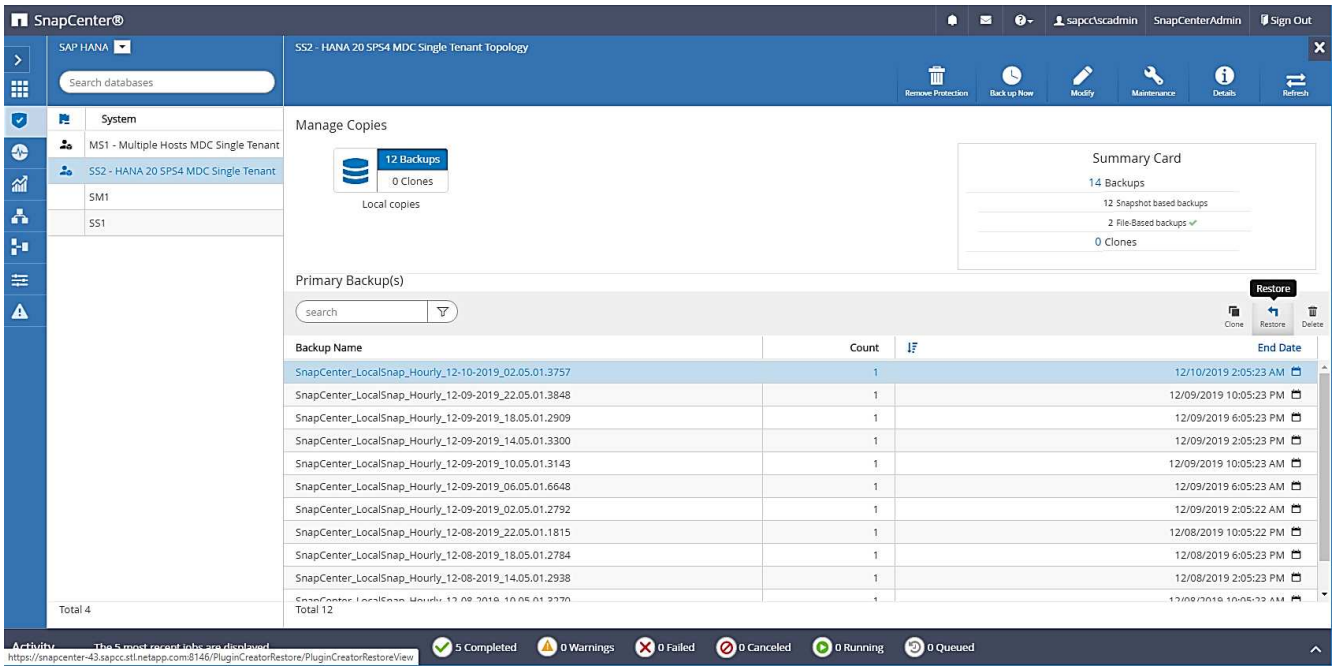
6. すべてのデータボリュームをアンマウントします。

```
umount /hana/data/SS2/mnt00001
```

NFS を使用する SAP HANA マルチホストシステムの場合は、各ホスト上のすべてのデータボリュームをアンマウントする必要があります。

FC を使用する SAP HANA マルチホストセットアップでは、シャットダウンプロセスの一環として、 SAP HANA ネームサーバによってアンマウント処理が実行されます。

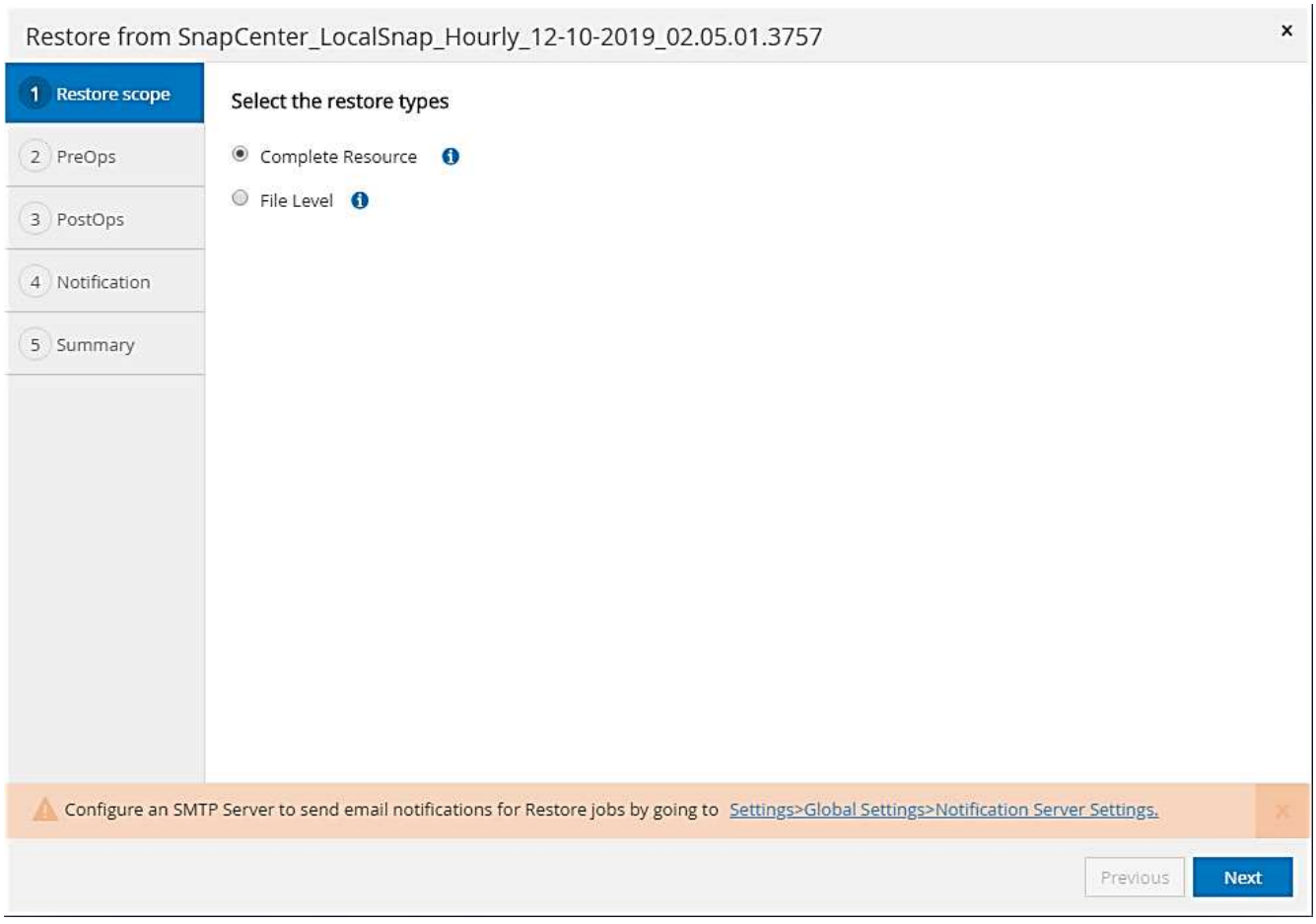
7. SnapCenter の GUI で、リソーストポロジビューを選択し、リストアするバックアップを選択します。この例では、最新のプライマリバックアップを選択します。リストアアイコンをクリックして、リストアを開始します。



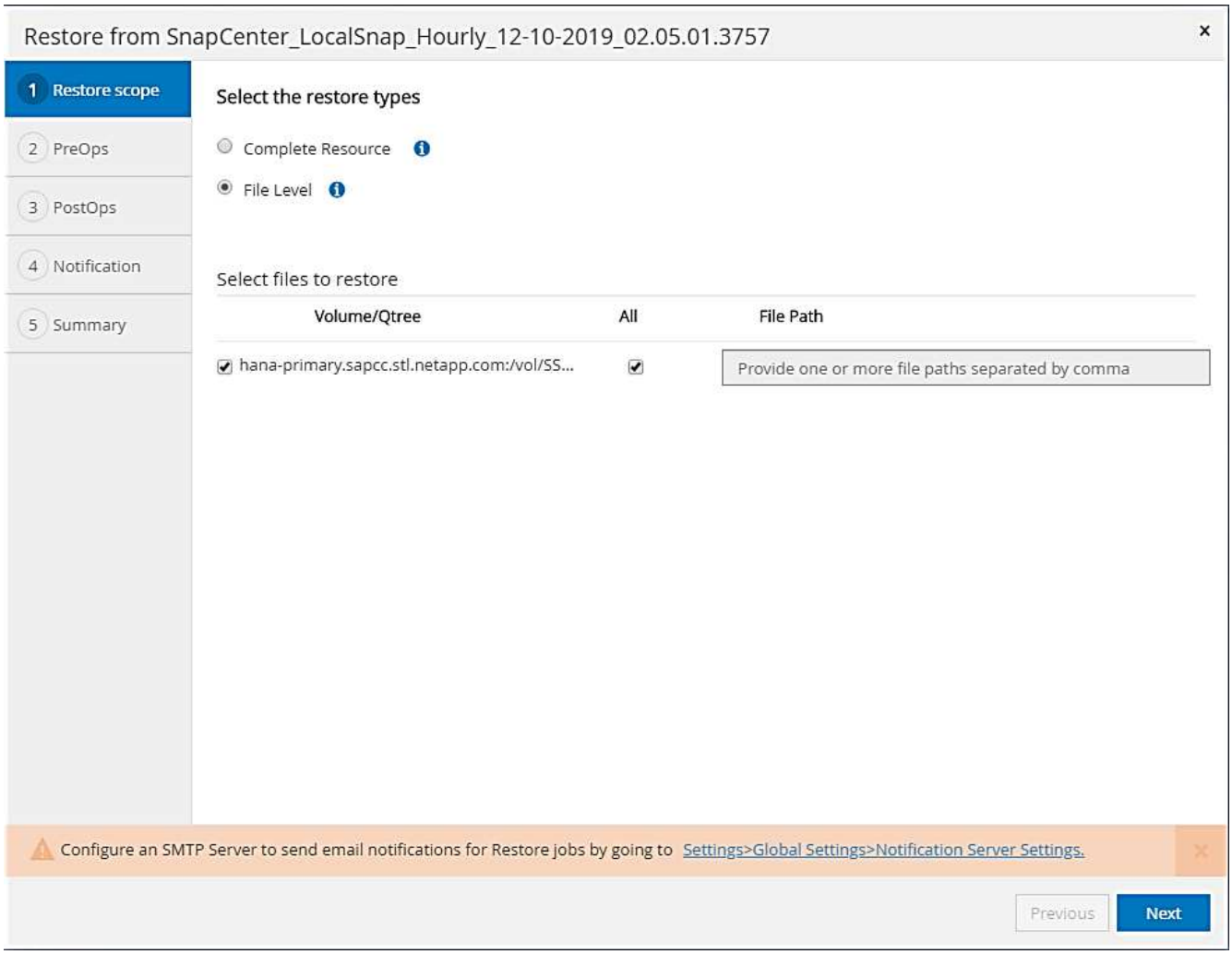
SnapCenter リストアウィザードが起動します。

8. リストア・タイプとして ［ 完全なリソース ］ または ［ ファイル・レベル ］ を選択します

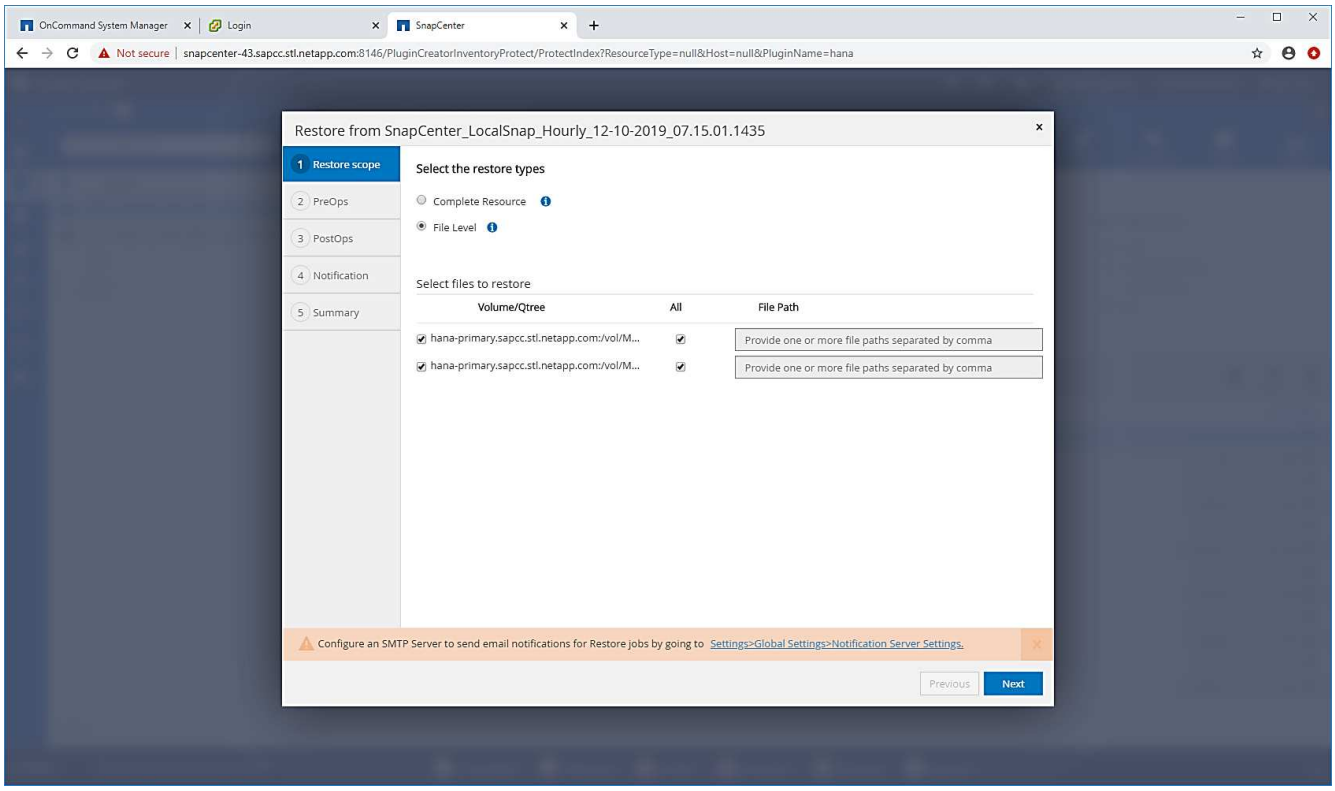
ボリュームベースのリストアを使用するには、 [リソース全体] を選択します。



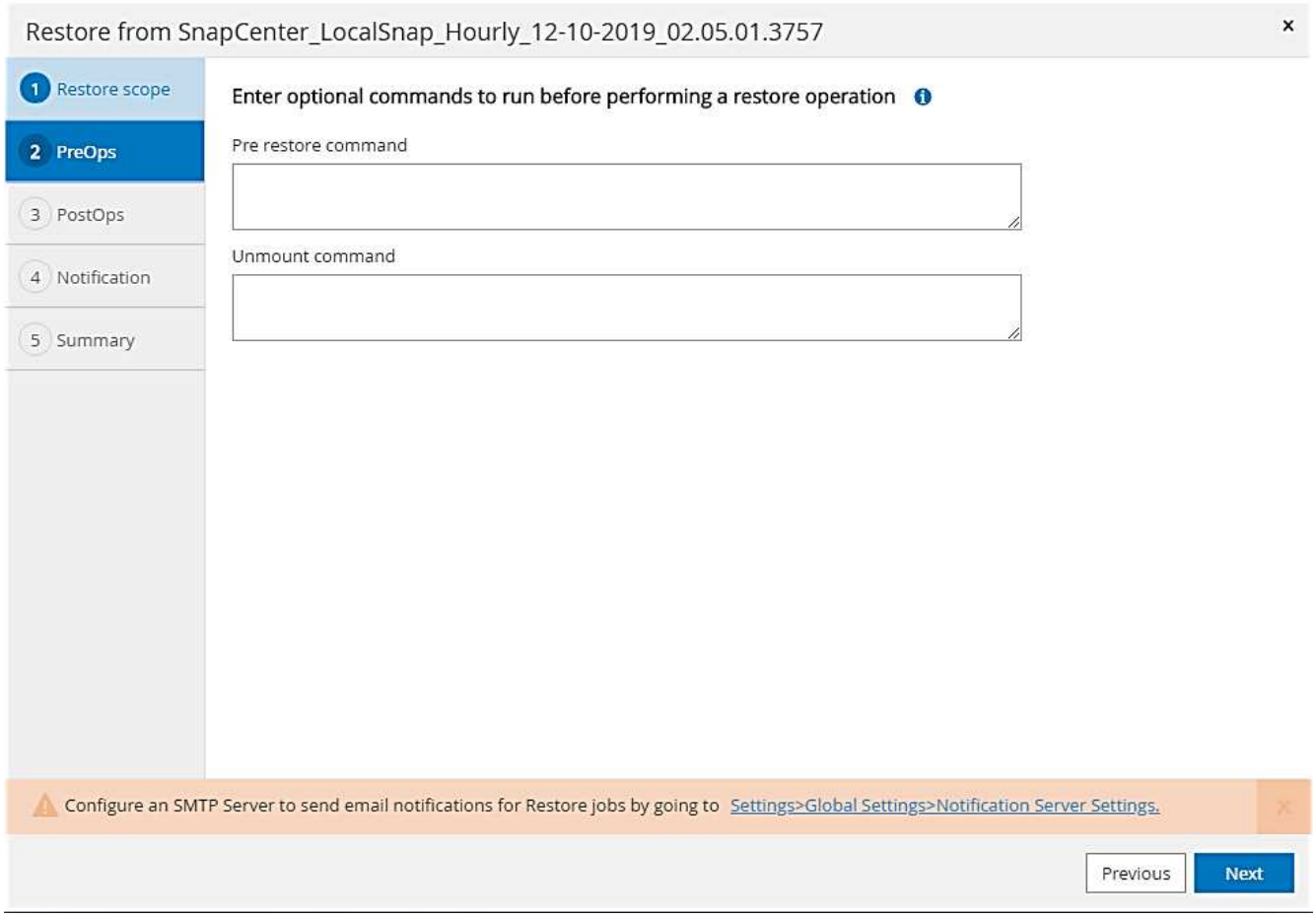
9. すべてのファイルに単一ファイルの SnapRestore 操作を使用するには、 [ファイルレベルとすべて] を選択します。



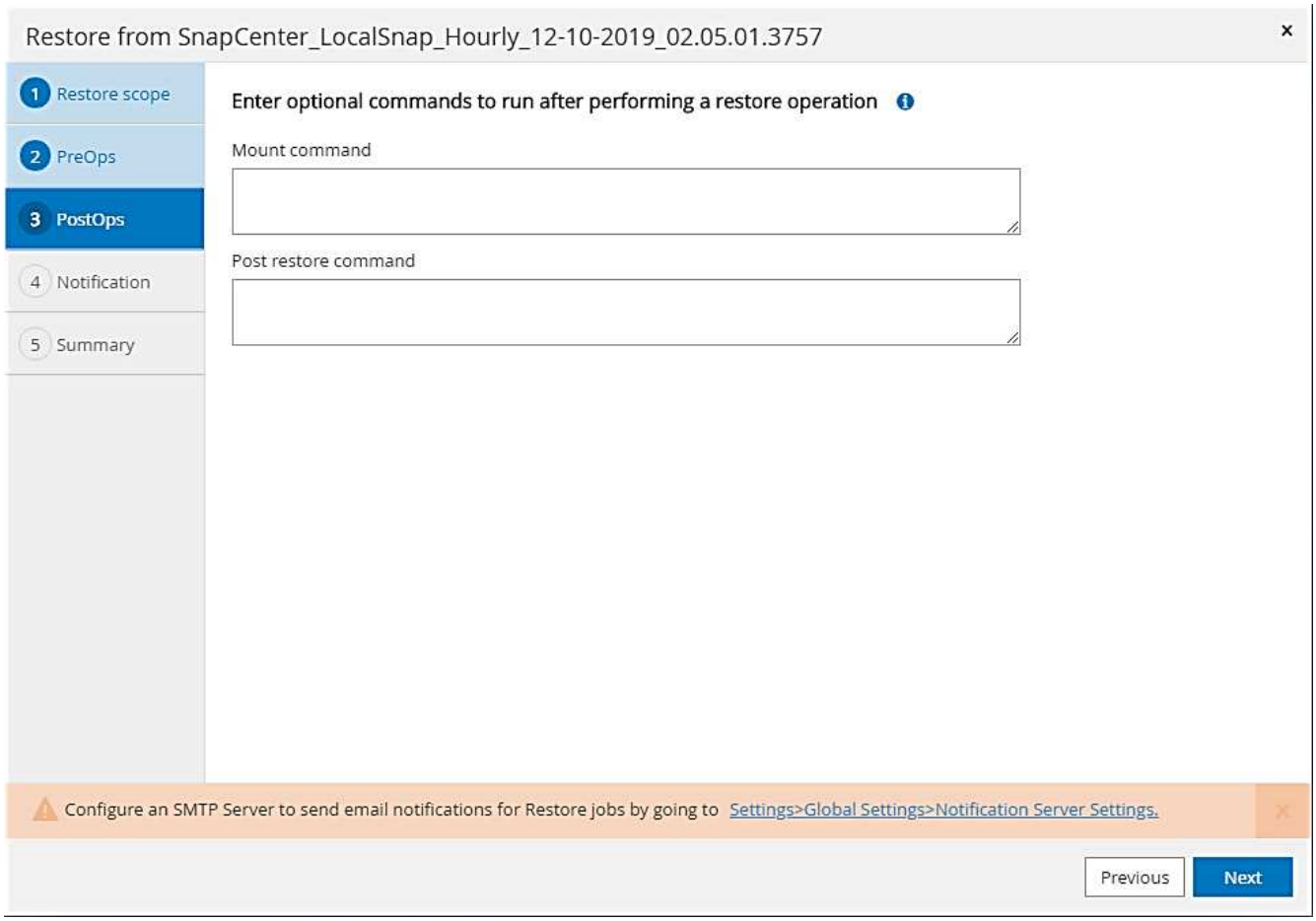
SAP HANA マルチホストシステムのファイルレベルのリストアを実行する場合は、すべてのボリュームを選択します。



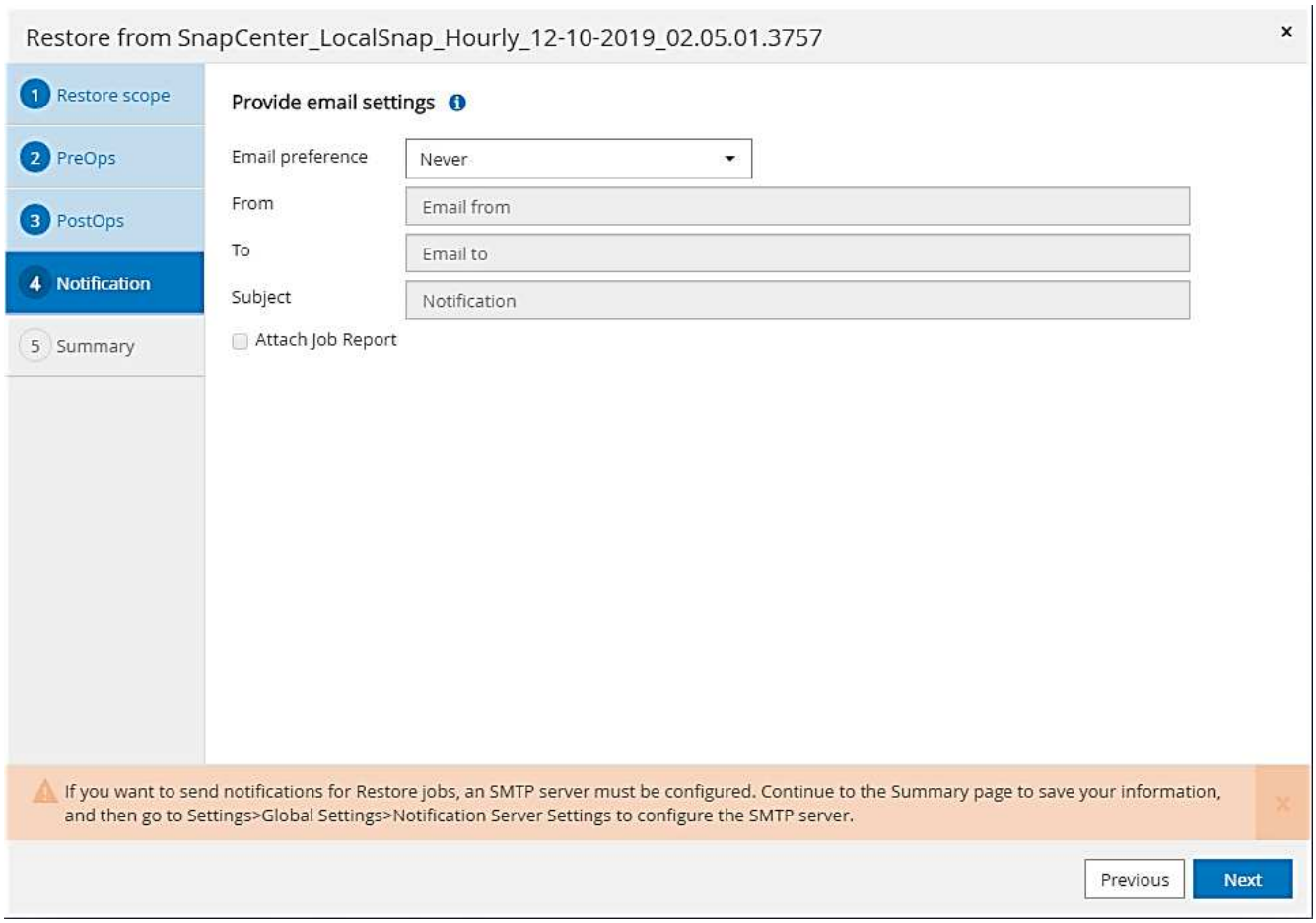
10. （オプション）中央の HANA プラグインホストで実行されている SAP HANA プラグインから実行するコマンドを指定します。次へをクリックします。



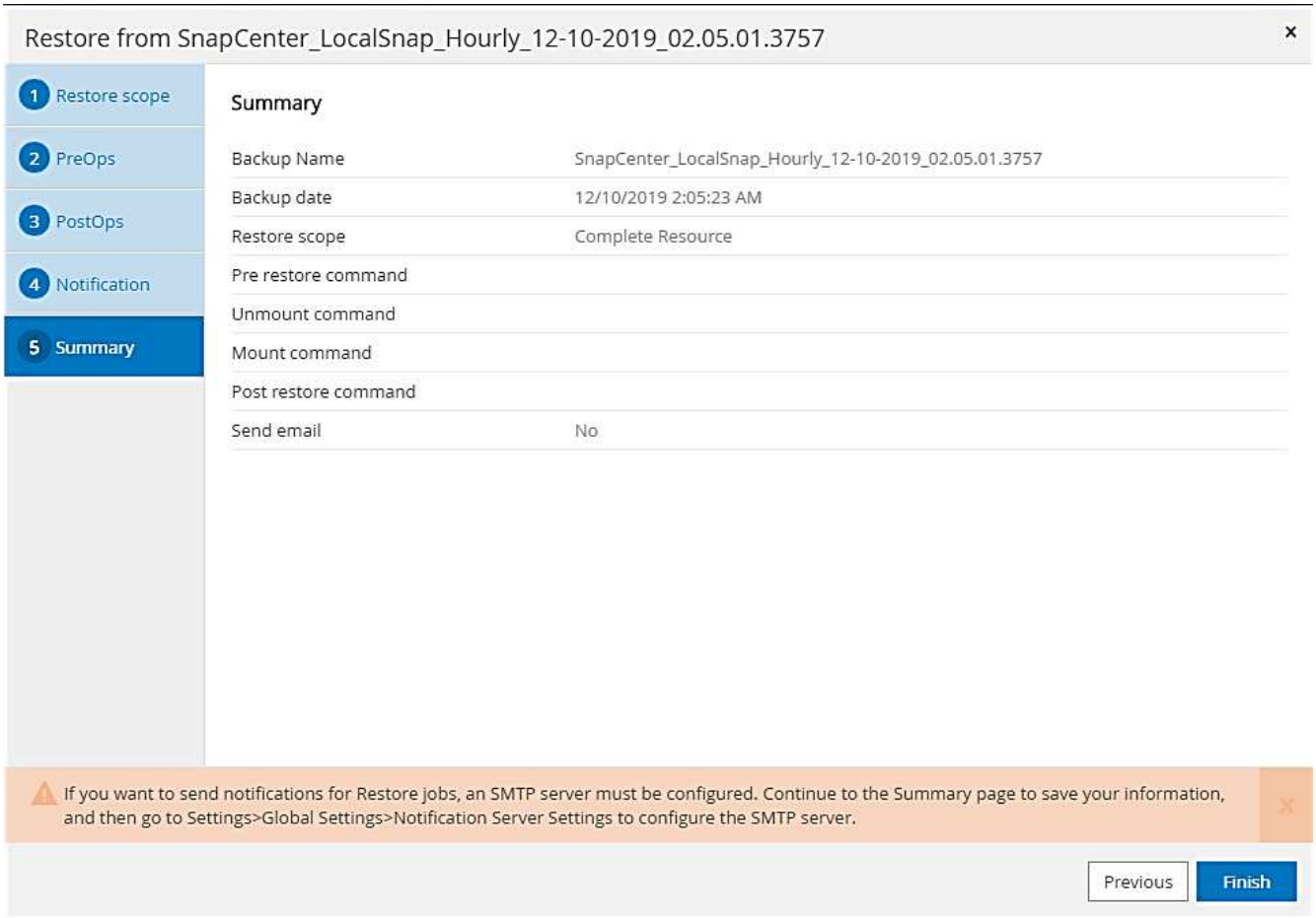
11. オプションのコマンドを指定し、次へをクリックします。



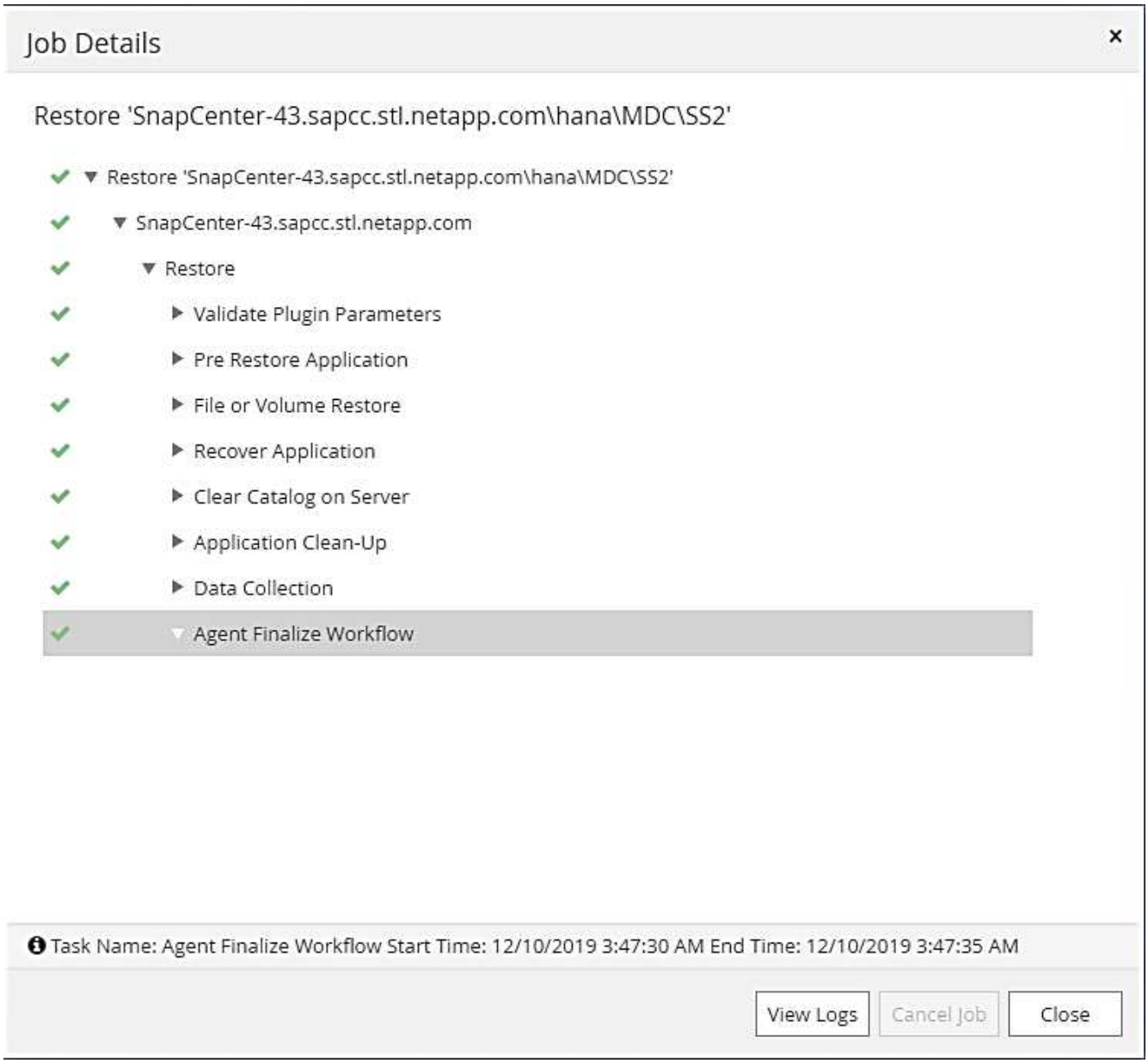
12. 通知設定を指定して、 SnapCenter からステータス E メールとジョブログを送信できるようにします。次へをクリックします。



13. 概要を確認し、 [完了] をクリックしてリストアを開始します。



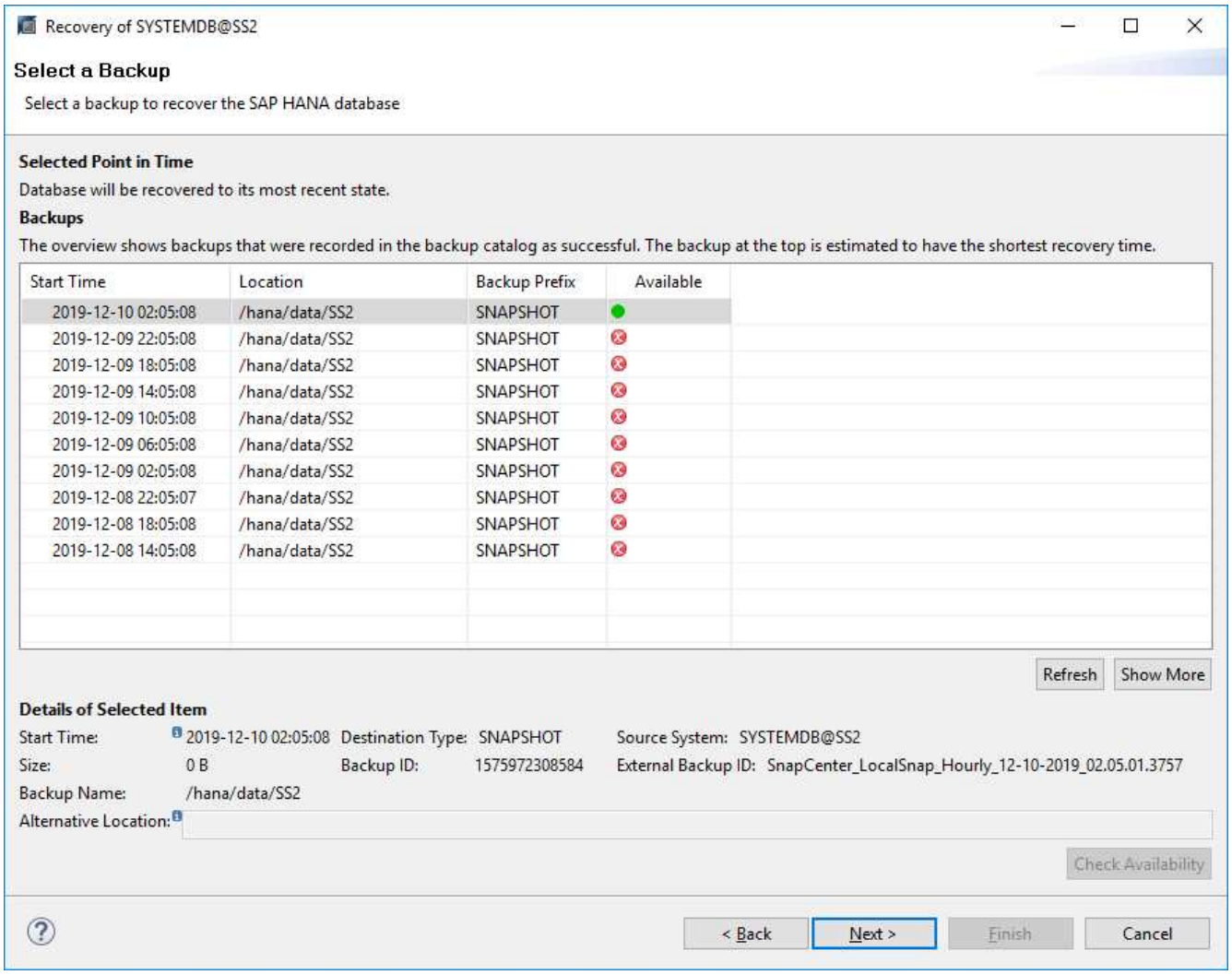
14. リストアジョブが開始され、アクティビティペインのログ行をダブルクリックするとジョブログが表示されます。



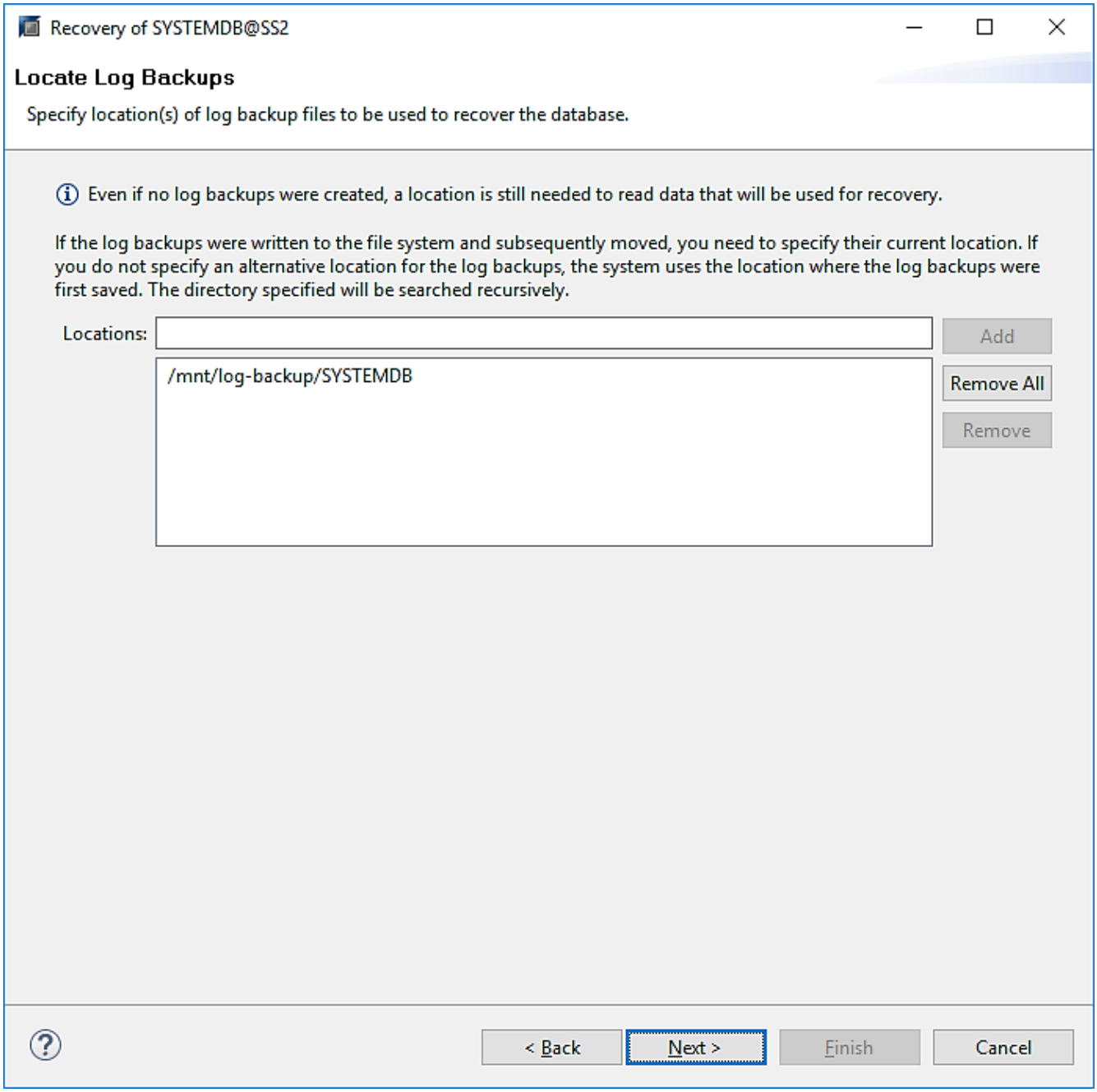
15. リストアプロセスが完了するまで待ちます。各データベースホストで、すべてのデータボリュームをマウントします。この例では、データベースホスト上で再マウントが必要なボリュームは 1 つだけです。

```
mount /hana/data/SP1/mnt00001
```

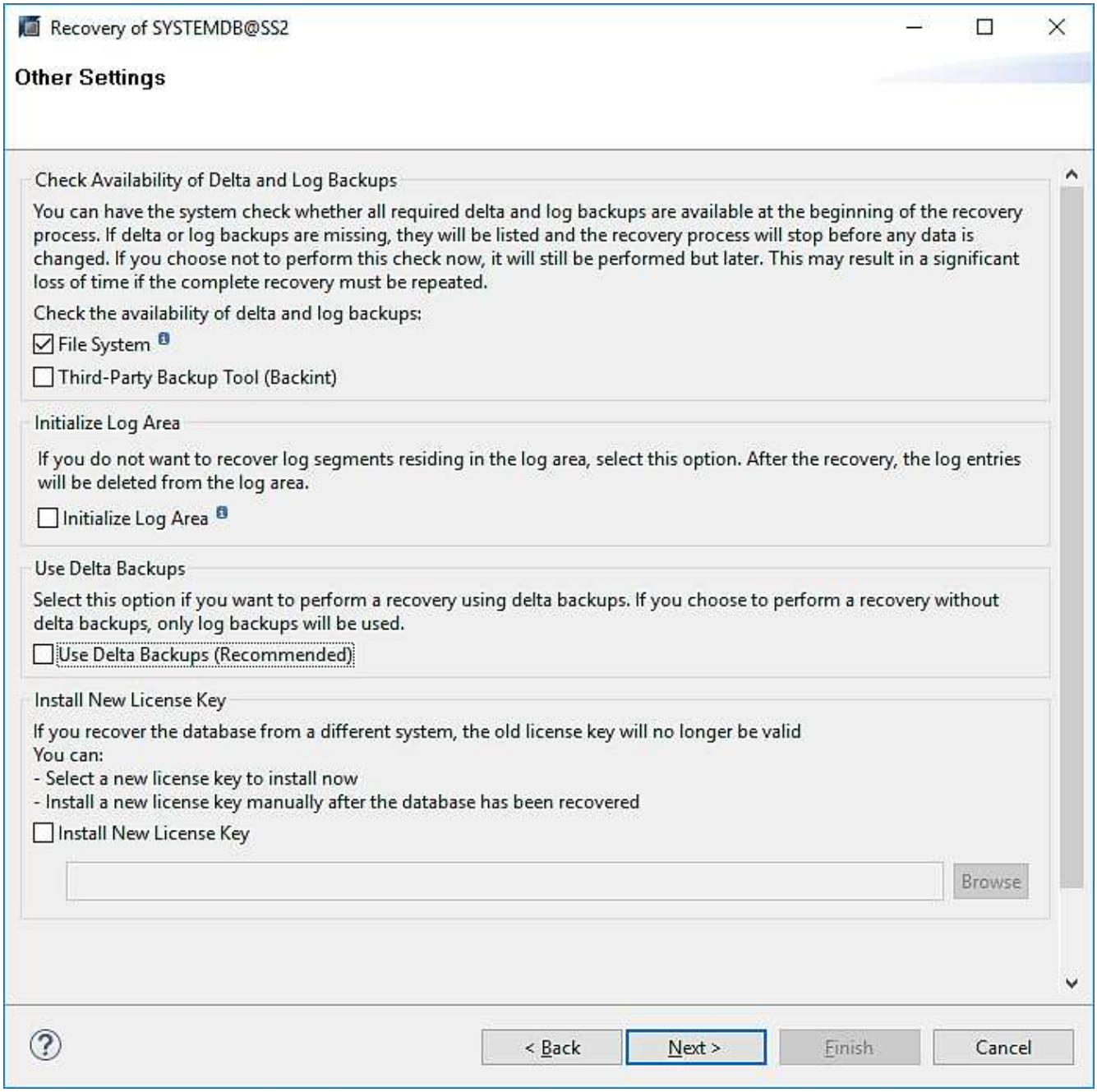
16. SAP HANA Studio に移動し、 Refresh をクリックして、使用可能なバックアップのリストを更新します。SnapCenter でリストアされたバックアップは、バックアップのリストに緑のアイコンで表示されます。バックアップを選択し、 Next （次へ）をクリックします。



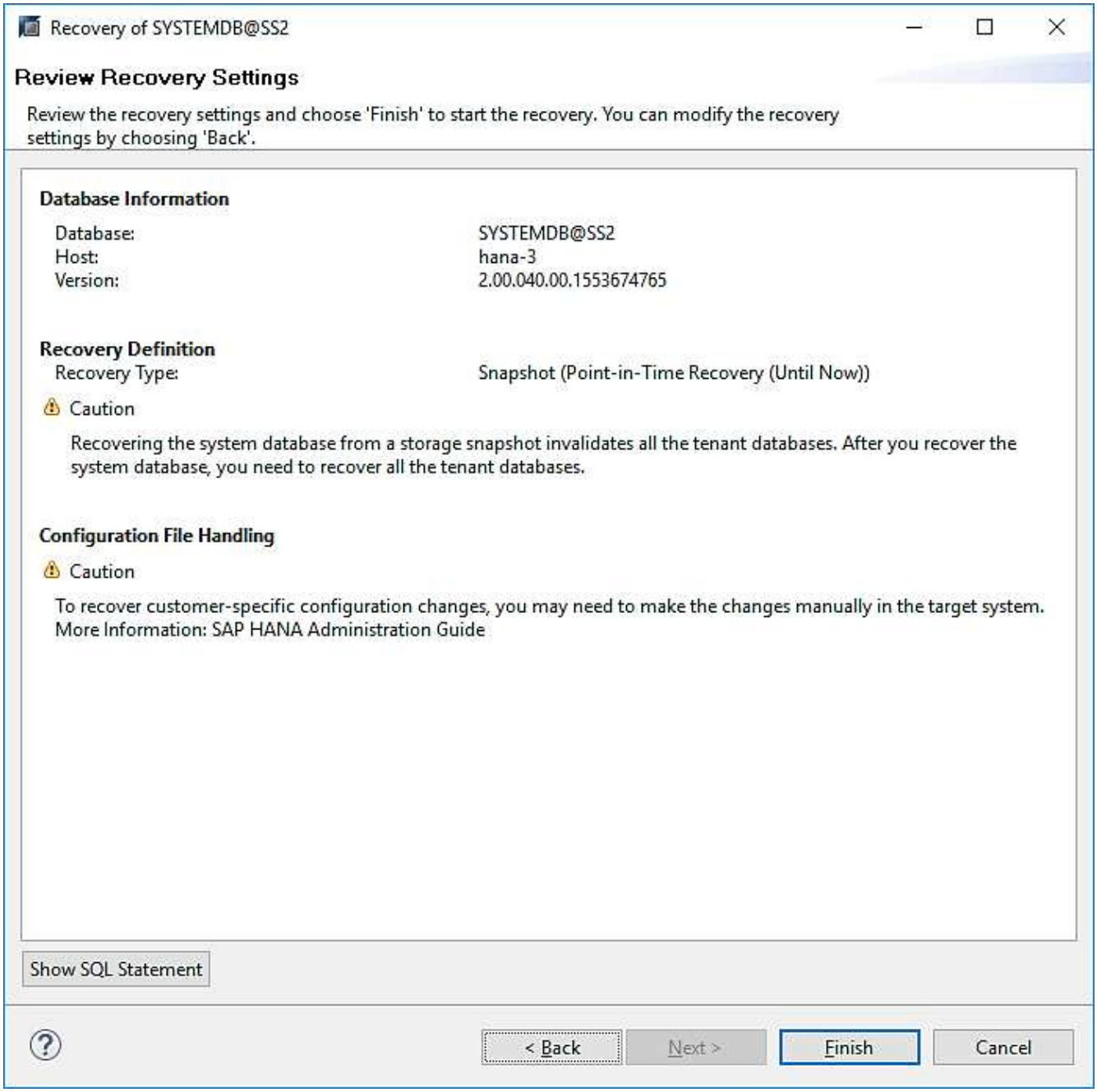
17. ログバックアップの場所を指定します。次へをクリックします。



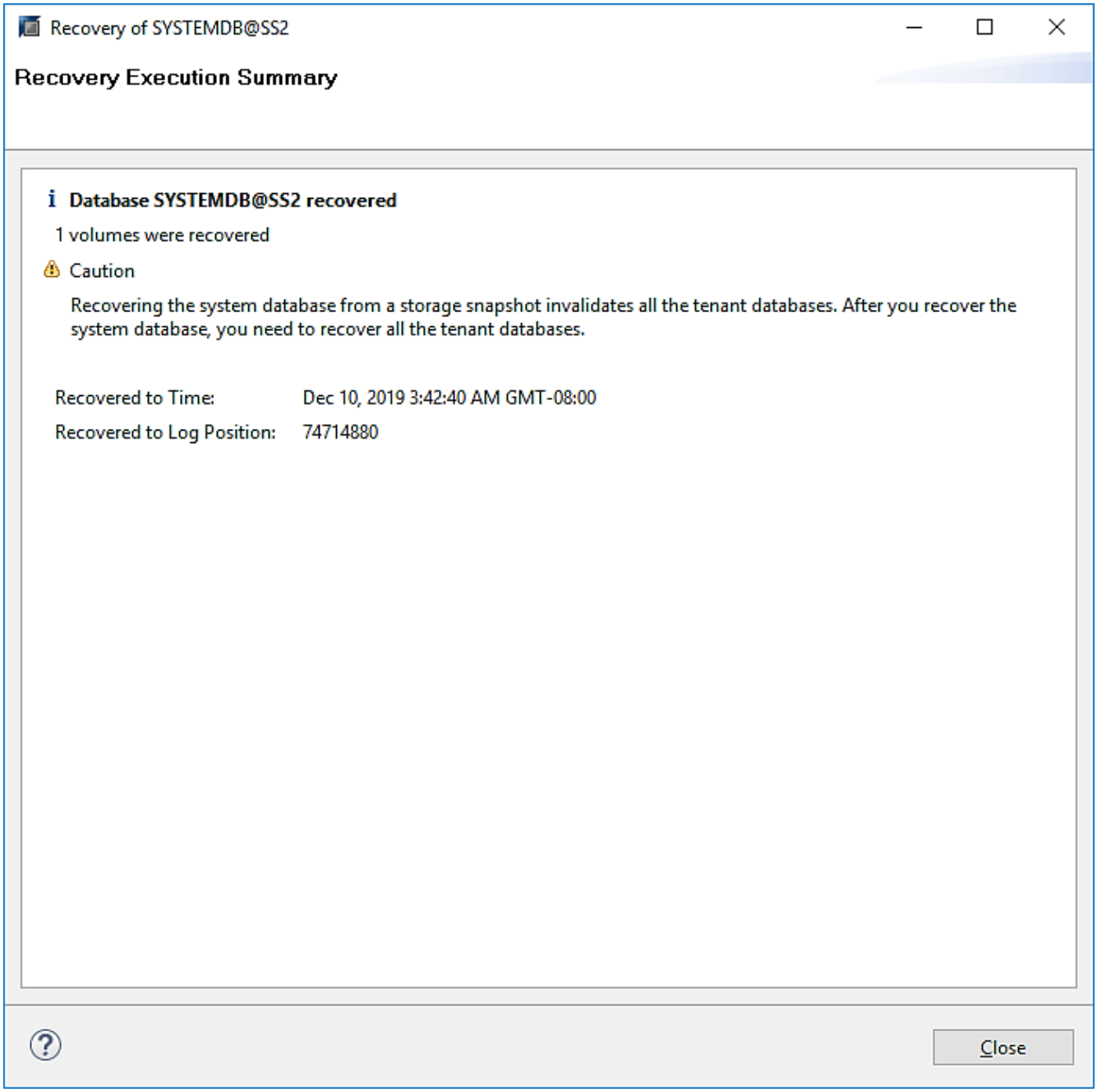
18. 必要に応じて、他の設定を選択します。［ デルタバックアップを使用 ］ が選択されていないことを確認します。次へをクリックします。



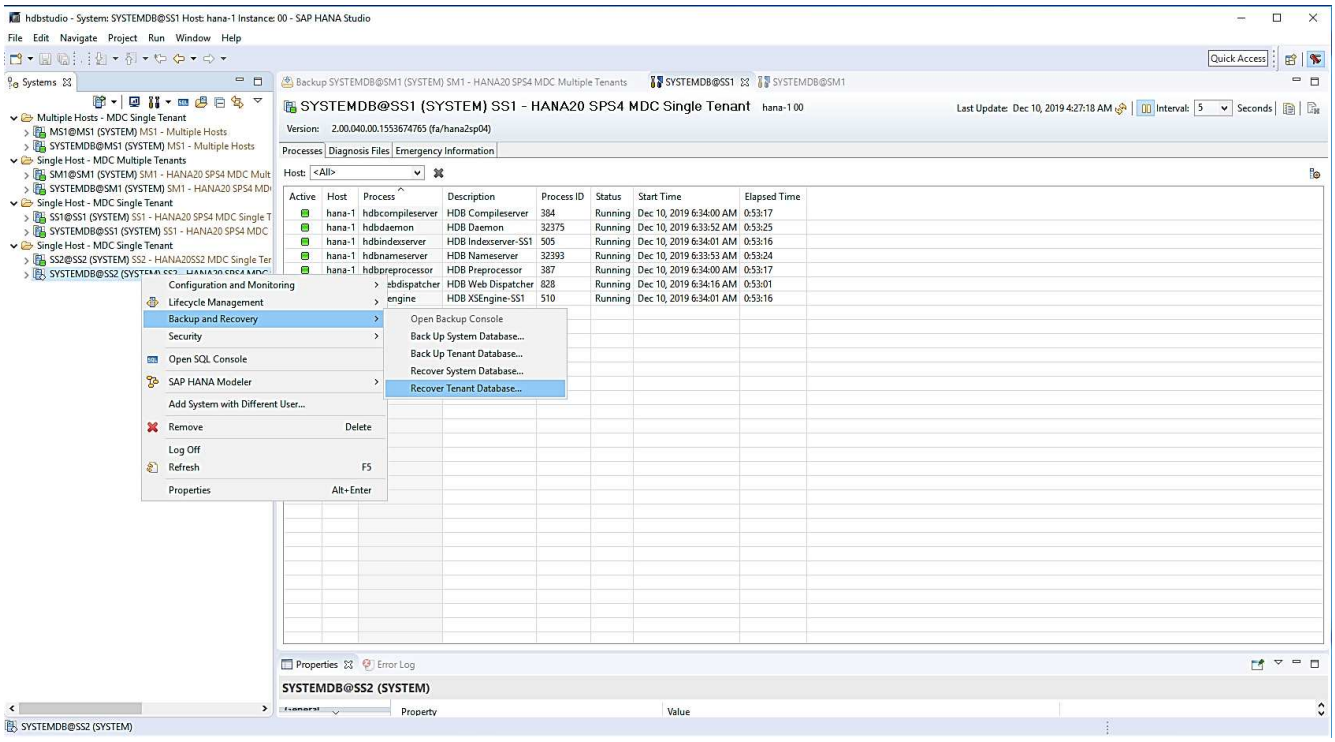
19. リカバリ設定を確認し、 [完了] をクリックします。



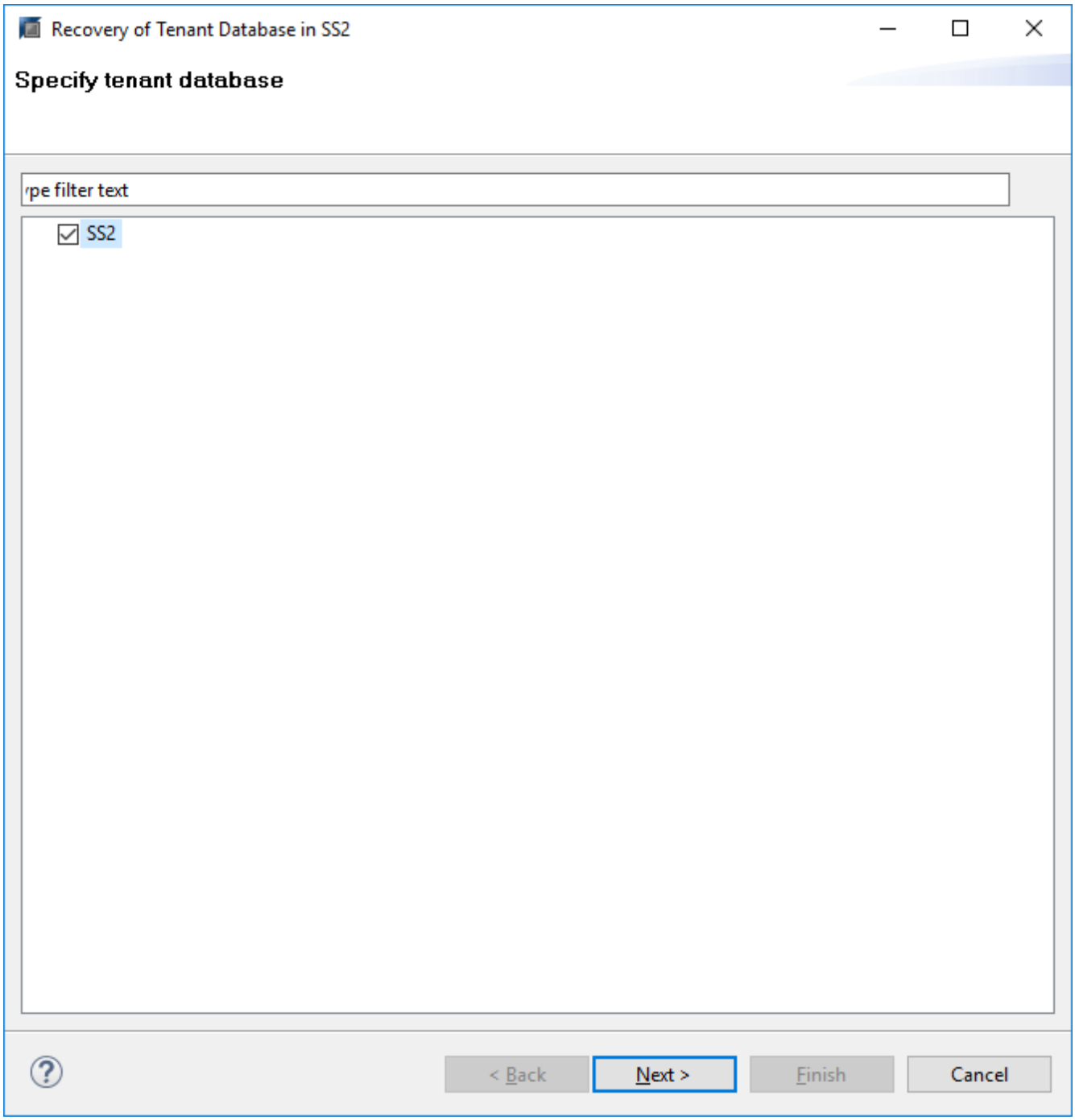
20. リカバリプロセスが開始されます。システムデータベースのリカバリが完了するまで待ちます。



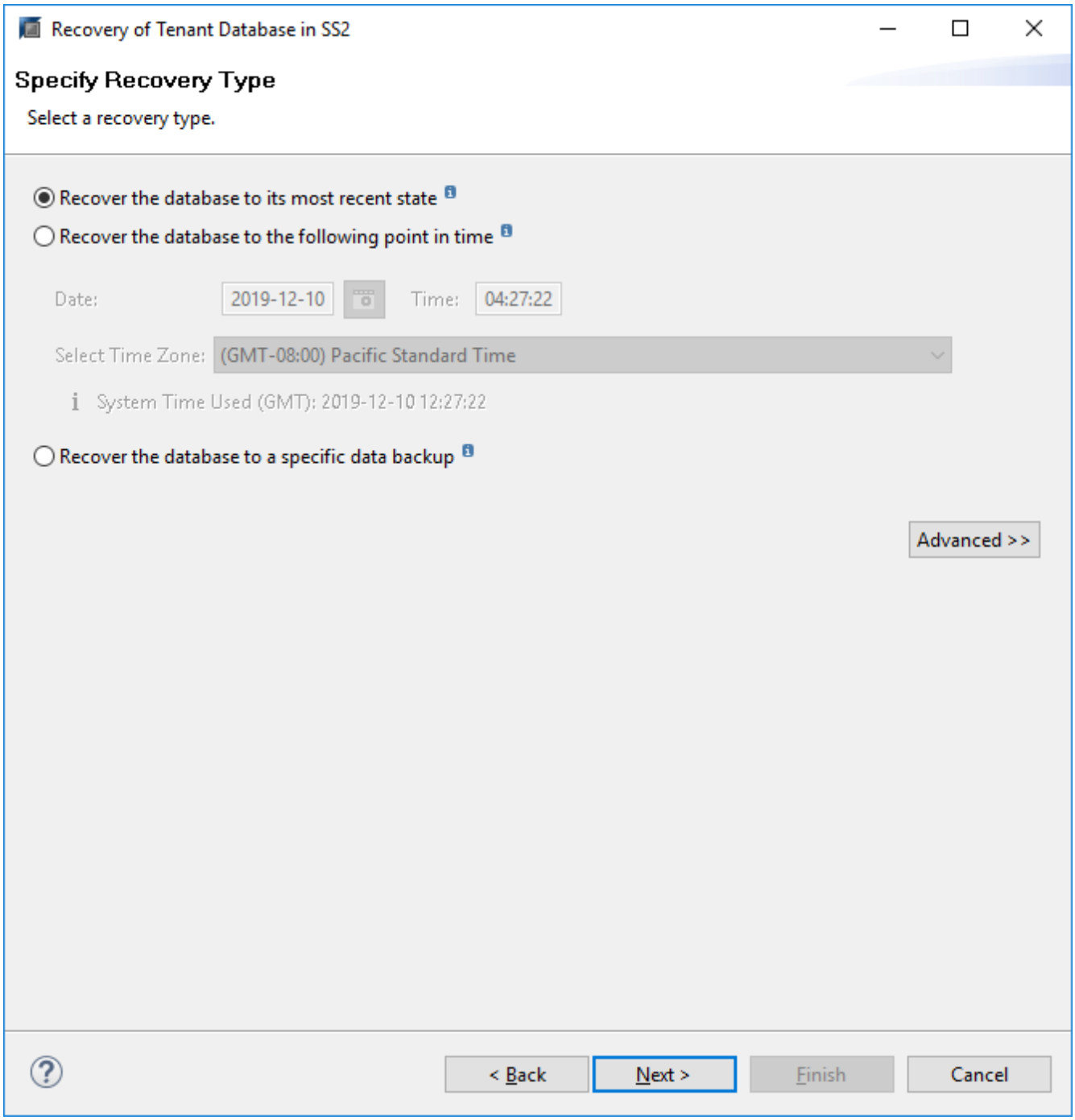
21. SAP HANA Studio で、システムデータベースのエントリを選択し、 Backup Recovery - Recover Tenant Database を開始します。



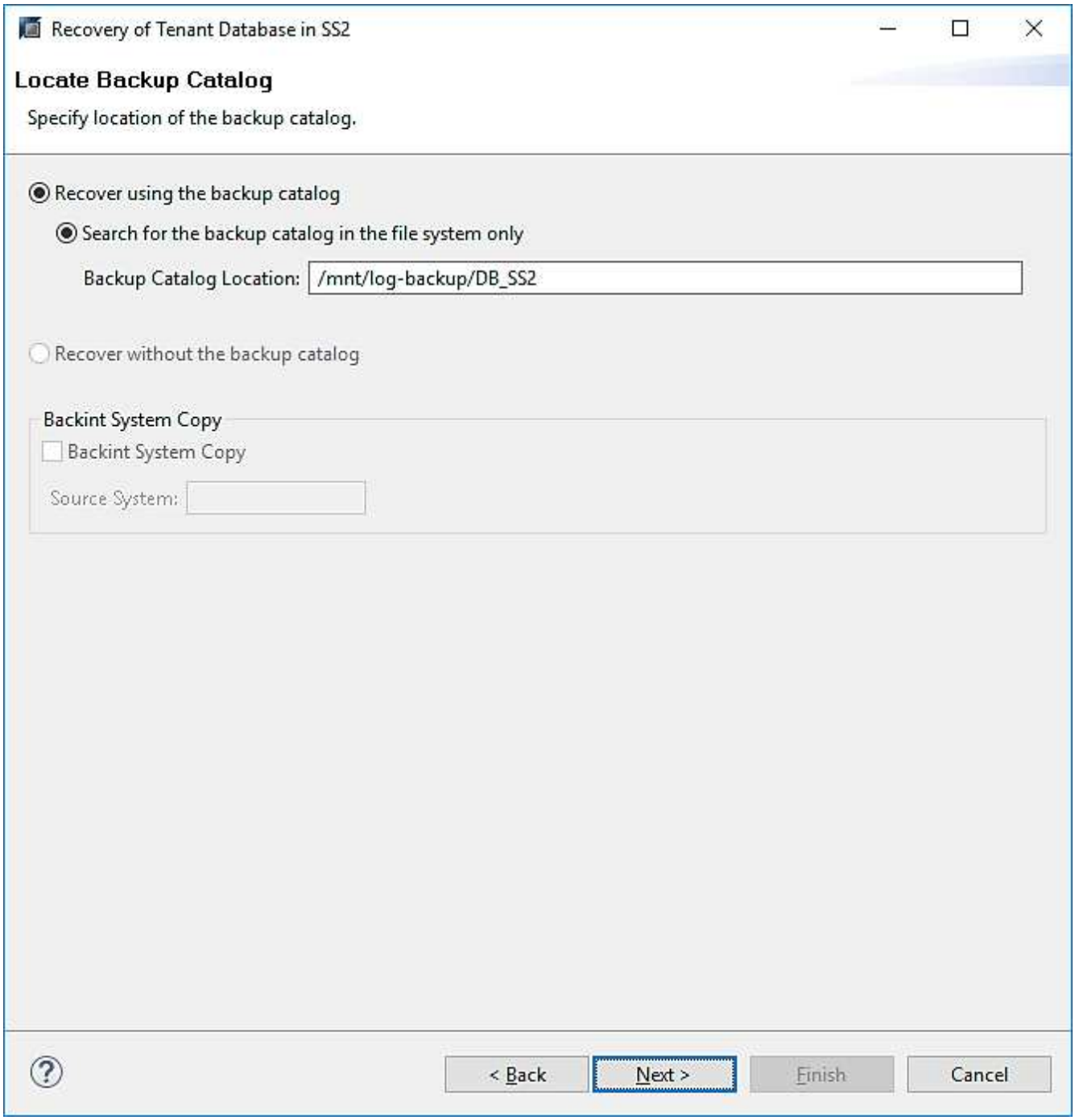
22. リカバリするテナントを選択し、 Next （次へ）をクリックします。



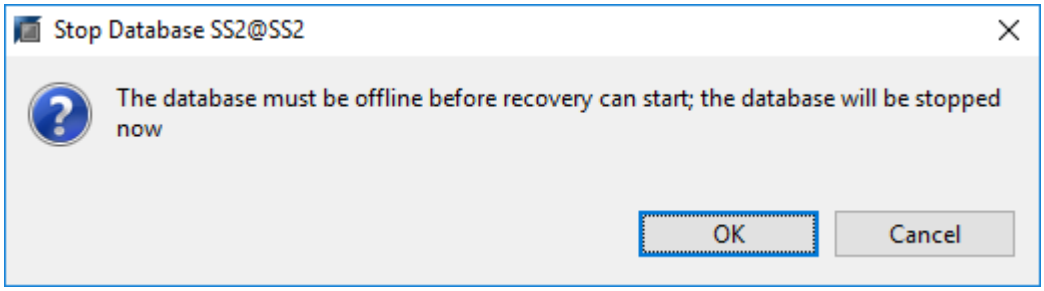
23. リカバリタイプを指定して、 Next （次へ）をクリックします。



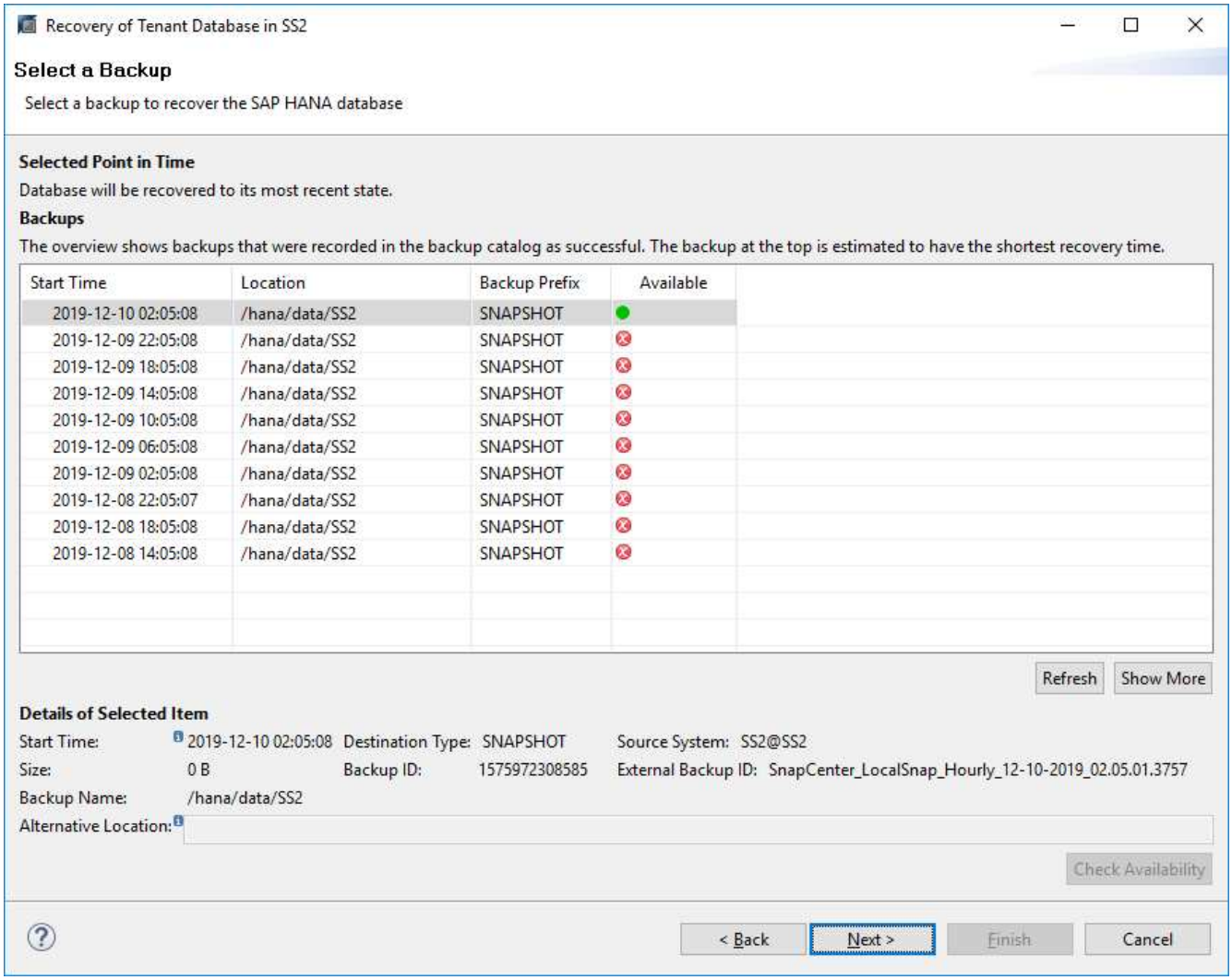
24. バックアップカタログの場所を確認し、 Next （次へ）をクリックします。



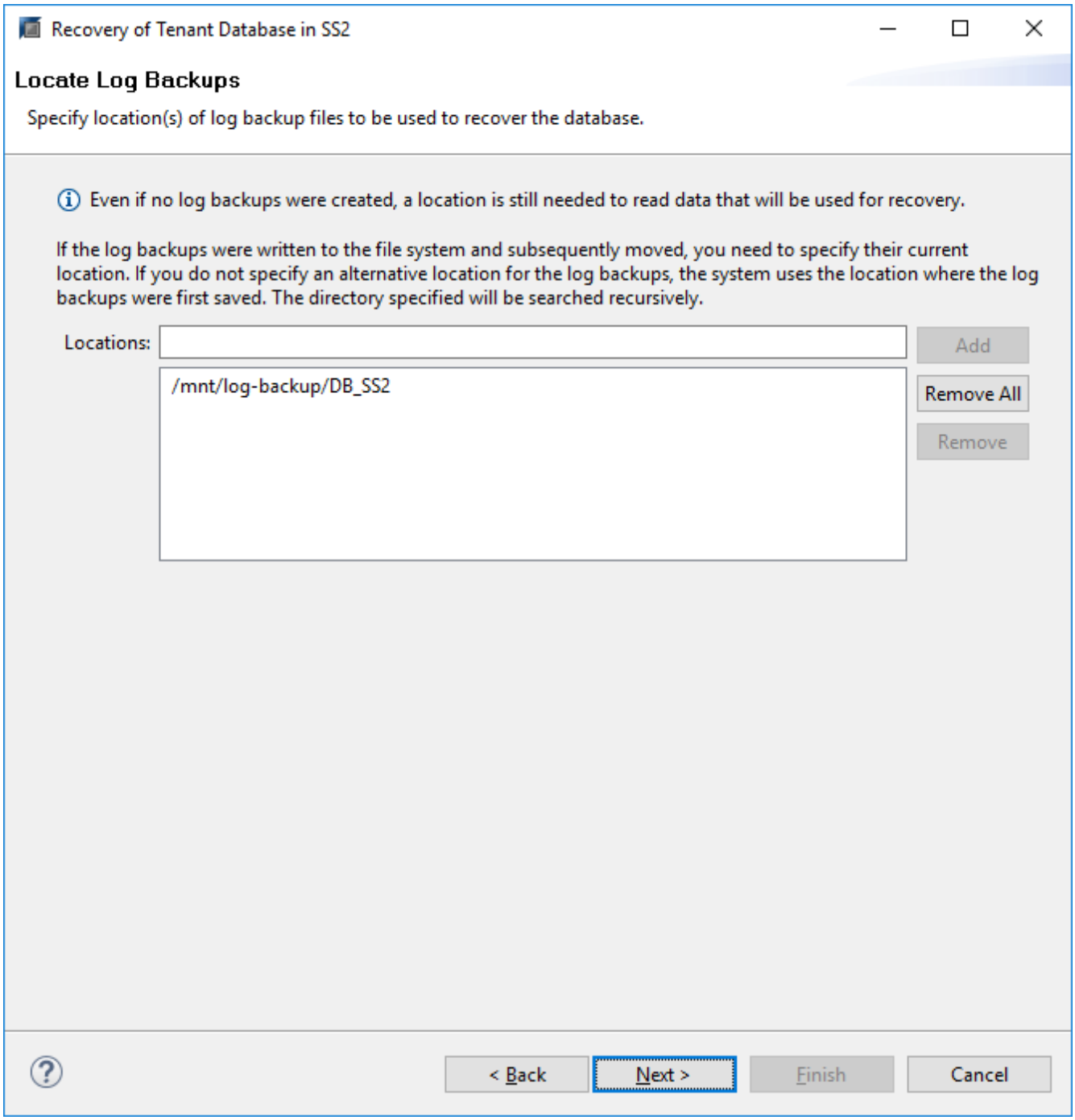
25. テナントデータベースがオフラインであることを確認します。[OK] をクリックして続行します。



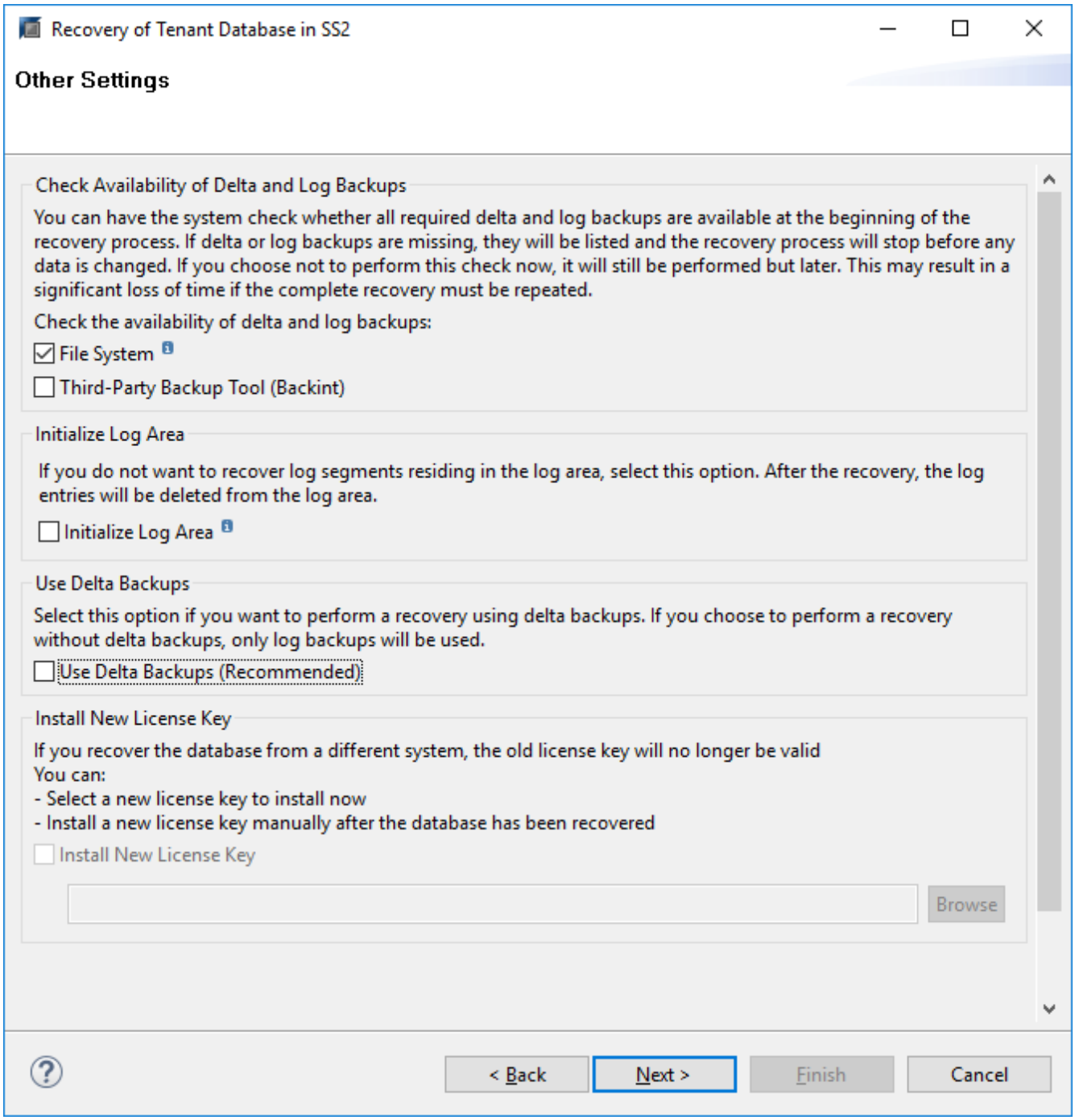
26. システムデータベースのリカバリ前にデータボリュームのリストアが実行されたため、テナントバックアップをすぐに使用できます。緑色でハイライトされたバックアップを選択し、次へをクリックします。



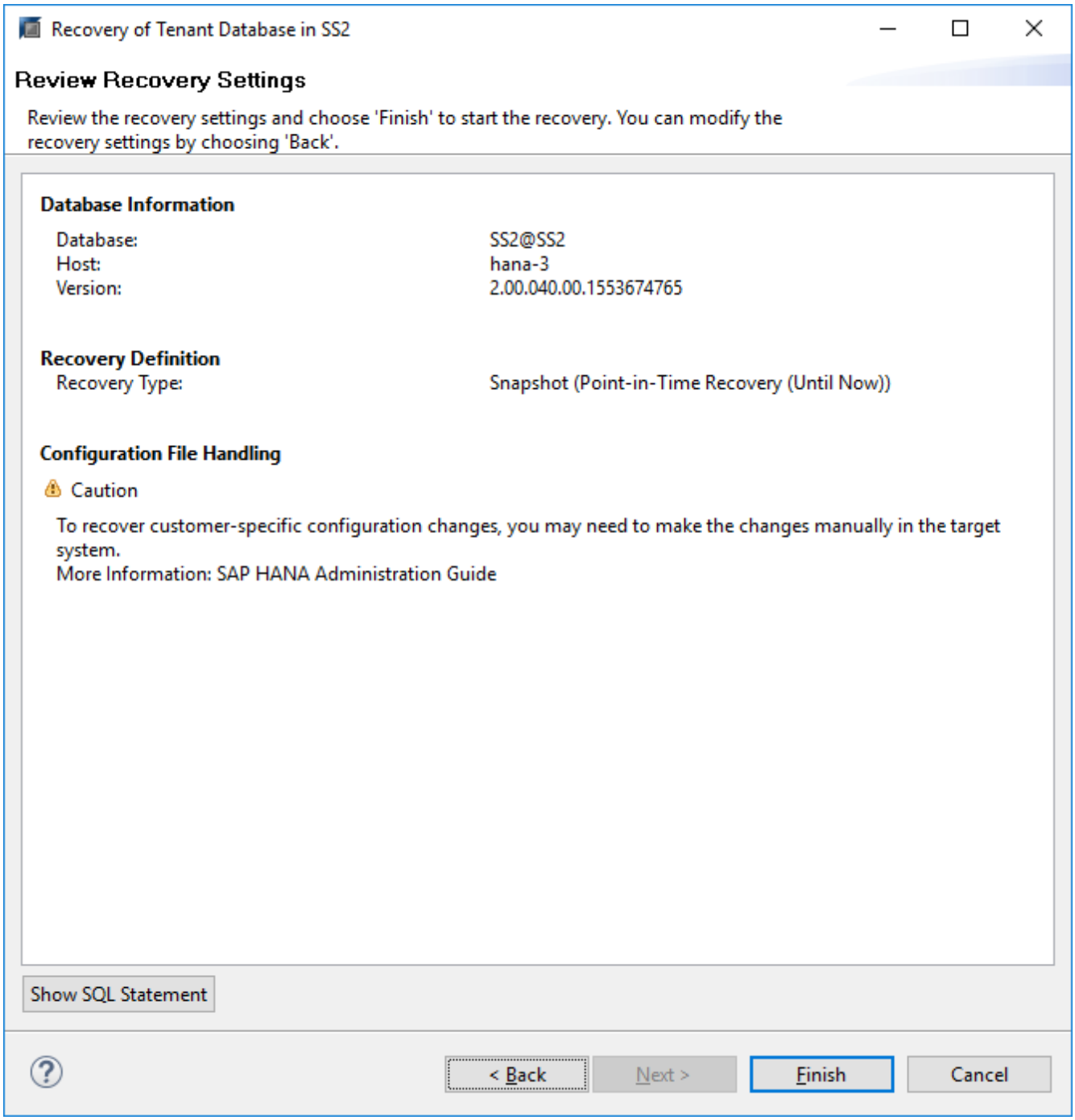
27. ログのバックアップ先を確認し、 Next （次へ）をクリックします。



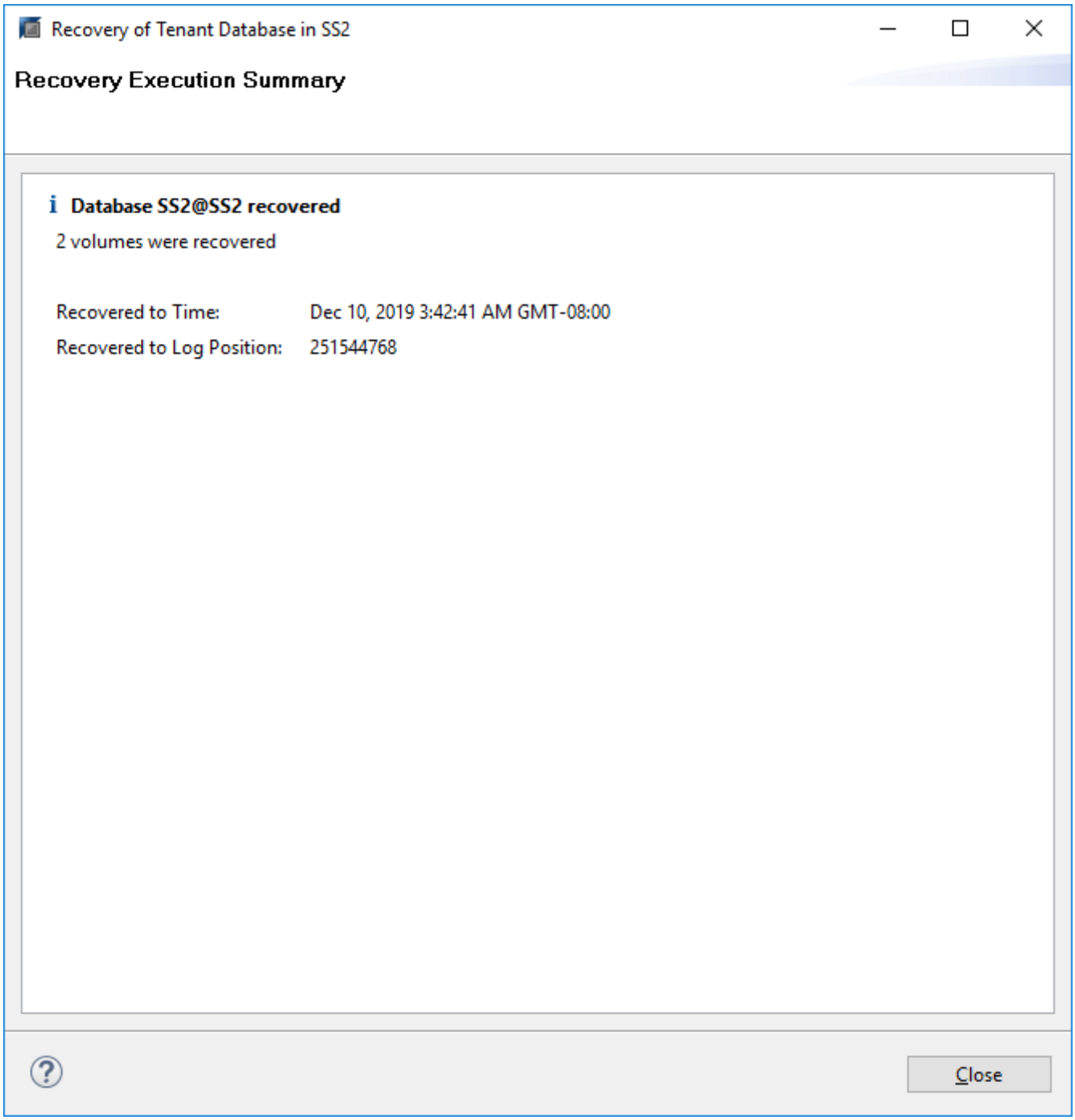
28. 必要に応じて、他の設定を選択します。［デルタバックアップを使用］が選択されていないことを確認します。次へをクリックします。



29. [完了] をクリックして、リカバリ設定を確認し、テナントデータベースのリカバリプロセスを開始します。



30. リカバリが完了してテナントデータベースが起動するまで待ちます。



SAP HANA システムは稼働中です。

複数のテナントを使用する SAP HANA MDC システムの場合は、テナントごとに手順 20~29 を繰り返す必要があります。

高度な設定と調整

このセクションでは、 SnapCenter の設定を特定のニーズに合わせるためにお客様が使用できる設定および調整オプションについて説明します。すべての設定がすべてのお客様のシナリオに適用されるわけではありません。

HANA データベースとのセキュアな通信を有効にします

HANA データベースにセキュアな通信が設定されている場合、 SnapCenter によって実行される「 hdbsql 」コマンドでは、追加のコマンドラインオプションを使用する必要があります。これは、必要なオプションを指定して「 hdbsql 」を呼び出すラッパースクリプトを使用して実現できます。

SSL 通信を設定するには、さまざまなオプションがあります。次の例では、コマンドラインオプションを使用して最も単純なクライアント設定について説明します。この場合、サーバ証明書の検証は行われません。サーバー側またはクライアント側で証明書の検証が必要な場合は、hdbsql コマンドラインオプションを変更する必要があります。また、『 SAP HANA Security Guide 』の説明に従って、 PSE 環境を設定する必要があります。

hana.properties` ファイルで「 hdbsql 」実行可能ファイルを設定する代わりに、ラッパースクリプトが追加されます。

SnapCenter Windows サーバ上の中央 HANA プラグインホストの場合、「 C ： \Program Files\NetApp\SnapManager \Snapcenter Plug-in Creator\etc\hana.properties` 」に次のコンテンツを追加する必要があります。

```
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql-ssl.cmd
```

ラッパースクリプト「 hdbsql-ssl.cmd 」は、必要なコマンドラインオプションを指定して「 hdbsql.exe 」を呼び出します。

```
@echo off
"C:\Program Files\sap\hdbclient\hdbsql.exe" -e -ssltrustcert %*
```

-e-ssltrustcert'hdbsql コマンドライン・オプションは 'SSL が有効になっていない HANA システムでも機能しますそのため、すべての HANA システムで SSL が有効または無効になっているわけではなく、このオプションを中央の HANA プラグインホストでも使用できます。

HANA プラグインが個々の HANA データベースホストに導入されている場合は、それに応じて各 Linux ホストで設定を行う必要があります。

```
HANA_HDBSQL_CMD = /usr/sap/SM1/HDB12/exe/hdbsqls
```

ラッパースクリプト「 hdbsqls 」は、必要なコマンドラインオプションを指定して「 hdbsql 」を呼び出します。

```
#/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql -e -ssltrustcert $*
```

HANA プラグインホストで自動検出を無効にします

HANA プラグインホストで自動検出を無効にするには、次の手順を実行します。

1. SnapCenter サーバで、 PowerShell を開きます。「 Open-SmConnectコネクション 」コマンドを実行して SnapCenter サーバに接続し、最初のログインウィンドウでユーザ名とパスワードを指定します。
2. 自動検出をディセーブルにするには、「 Set-SmConfigSettings 」コマンドを実行します。

   HANA ホストの「 HANA -2' 」の場合、このコマンドは次のようになります。

```
PS C:\Users\administrator.SAPCC> Set-SmConfigSettings -Agent -Hostname
hana-2 -configSettings @{"DISABLE_AUTO_DISCOVERY"="true"}
Name                           Value
----                           -----
DISABLE_AUTO_DISCOVERY         true
PS C:\Users\administrator.SAPCC>
```

3. 「 Get-SmConfigSettings 」コマンドを実行して、設定を確認します。

```
PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all
Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC            Value: 3600000
Details: Plug-in API operation Timeout
Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC   Value: 1800
Details: Web Service API Timeout
Key: CUSTOMPLUGINS_ALLOWED_CMDS                         Value: *;
Details: Allowed Host OS Commands
Key: DISABLE_AUTO_DISCOVERY                             Value: true
Details:
Key: PORT                                               Value: 8145
Details: Port for server communication
PS C:\Users\administrator.SAPCC>
```

   構成はホスト上のエージェント構成ファイルに書き込まれ、 SnapCenter によるプラグインのアップグレード後も引き続き使用できます。

```
hana-2:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/agent.properties | grep DISCOVERY
DISABLE_AUTO_DISCOVERY = true
hana-2:/opt/NetApp/snapcenter/scc/etc #
```

ログバックアップの自動削除を非アクティブ化します

ログバックアップの不要ファイルの削除はデフォルトで有効になっており、 HANA プラグインのホストレベルで無効にすることができます。これらの設定を変更するには、 2 つのオプションがあります。

hana.property ファイルを編集します

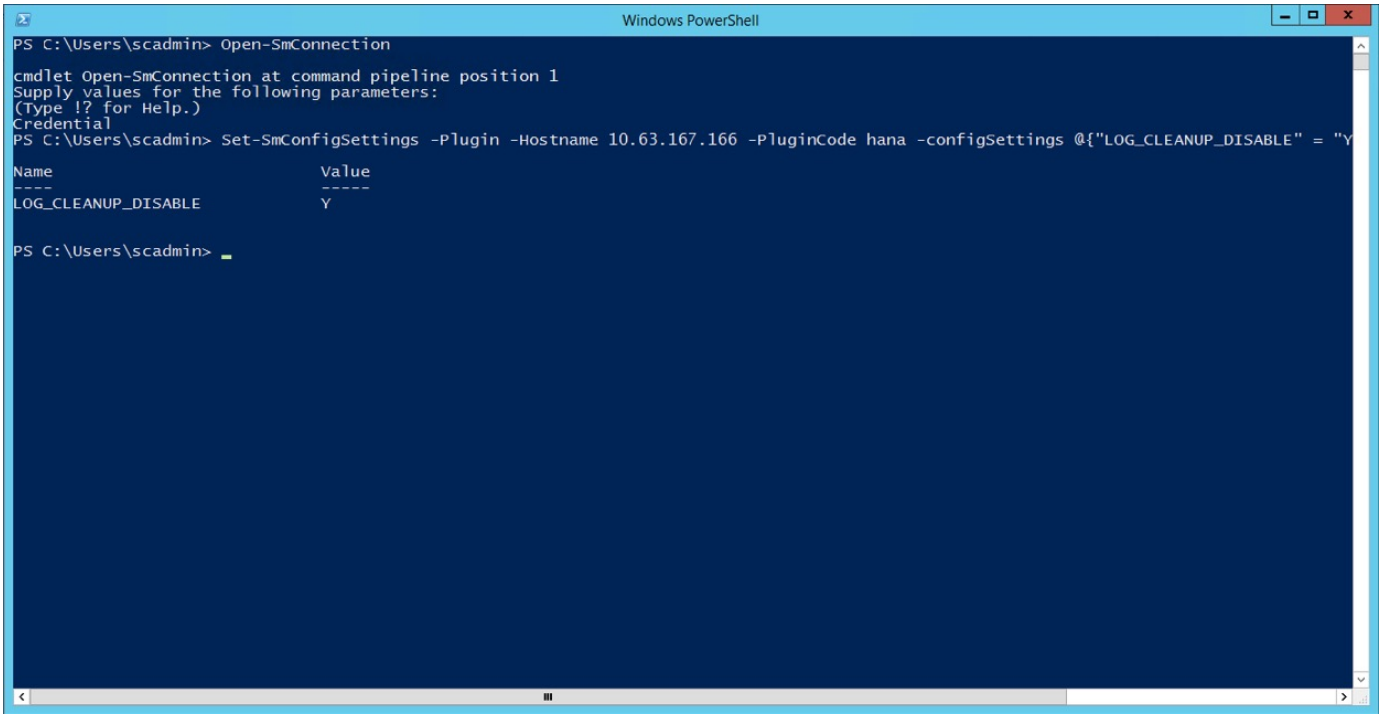
hana.property` 構成ファイルのパラメータ log_cleanup_disable=Y' を指定すると ' この SAP HANA プラグイン・ホストを通信ホストとして使用して ' すべてのリソースのログ・バックアップ・ハウスキーピングが無効になります

- Windows 上の Hdbsql 通信ホストの場合、「 hana.property` 」ファイルは C:\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc にあります。
- Linux 上の Hdbsql 通信ホストの場合、「 hana.property` 」ファイルは「 /opt/NetApp/snapcenter /sscc /etc 」にあります。

PowerShell コマンドを使用します

2 つ目のオプションでは、 SnapCenter PowerShell コマンドを使用します。

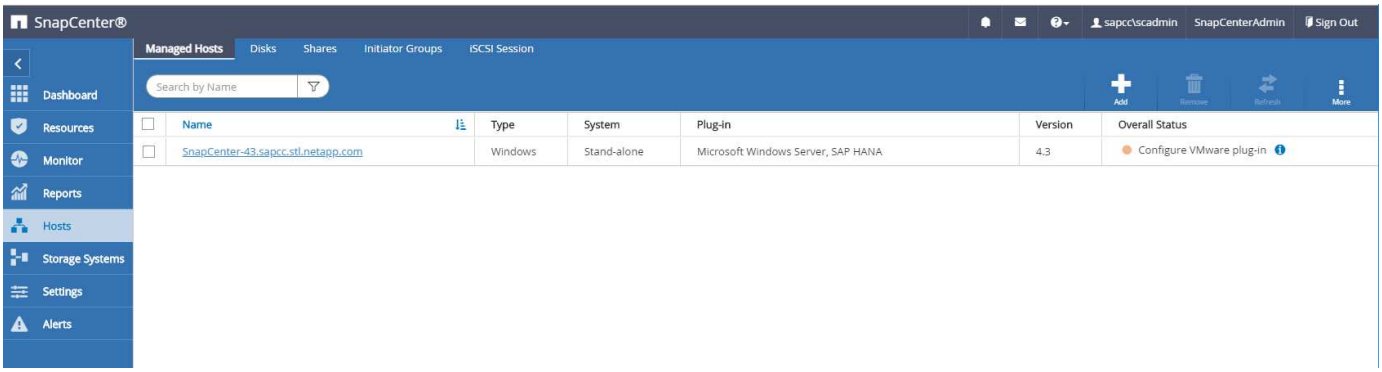
1. SnapCenter サーバで、 PowerShell を開きます。「 Open-SmConnection 」コマンドを使用して SnapCenter サーバに接続し、最初のログインウィンドウでユーザ名とパスワードを指定します。
2. 「 Set-SmConfigSettings-Plugin-hostname <pluginhostname>-PluginCode HANA -configSettings@{"log_cleanup_disable"="Y"}" 」コマンドを使用すると、 IP またはホスト名で指定した SAP HANA プラグインホスト「 <plughostname> 」に変更が設定されます（次の図を参照）。



仮想環境で **SAP HANA** プラグインを実行する際の警告を無効にします

SnapCenter は、 SAP HANA プラグインが仮想環境にインストールされているかどうかを検出します。これは、パブリッククラウドプロバイダでの VMware 環境や SnapCenter 環境の場合があります。この場合、次

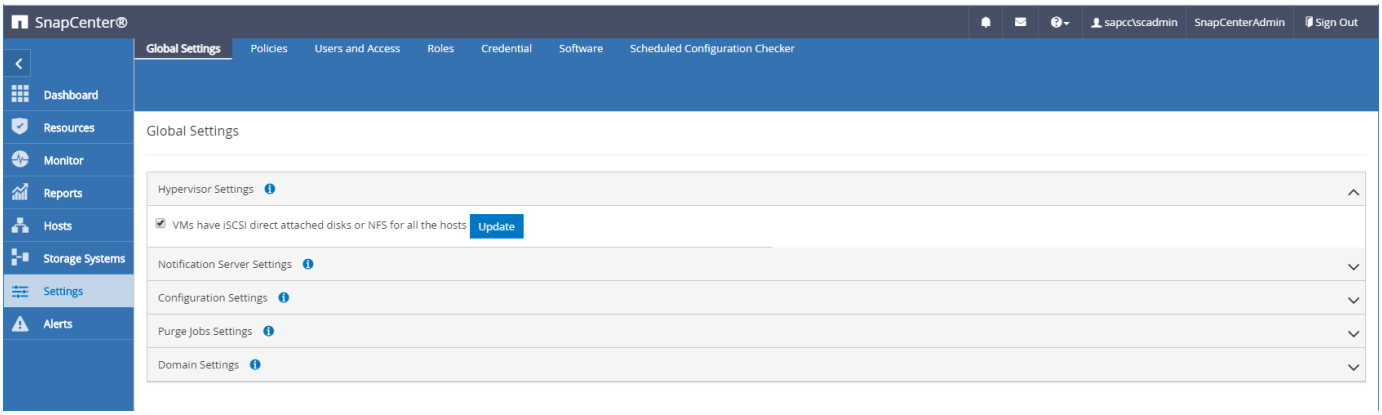
の図に示すように、ハイパーバイザーの設定に関する警告が SnapCenter に表示されます。



この警告をグローバルに抑制することができます。この場合、 SnapCenter は仮想環境を認識しないため、警告は表示されません。

この警告を抑制するように SnapCenter を設定するには、次の設定を適用する必要があります。

1. [設定] タブで、 [グローバル設定] を選択します。
2. ハイパーバイザー設定で、すべてのホストに対して VM に iSCSI Direct Attached Disks または NFS を選択し、設定を更新します。



オフサイトのバックアップストレージとのバックアップ同期のスケジュール頻度を変更します

を参照してください "「セカンダリ・ストレージでのバックアップの保持管理」" オフサイトのバックアップストレージへのデータバックアップの保持管理は ONTAP で行います。SnapCenter は、週次のデフォルトスケジュールを設定してクリーンアップジョブを実行することにより、オフサイトのバックアップストレージで ONTAP がバックアップを削除したかどうかを定期的にチェックします。

SnapCenter のクリーンアップジョブでは、オフサイトのバックアップストレージで削除したバックアップが見つかった場合に、 SnapCenter リポジトリおよび SAP HANA のバックアップカタログからバックアップが削除されます。

クリーンアップジョブは、不要な SAP HANA ログバックアップの削除も実行します。

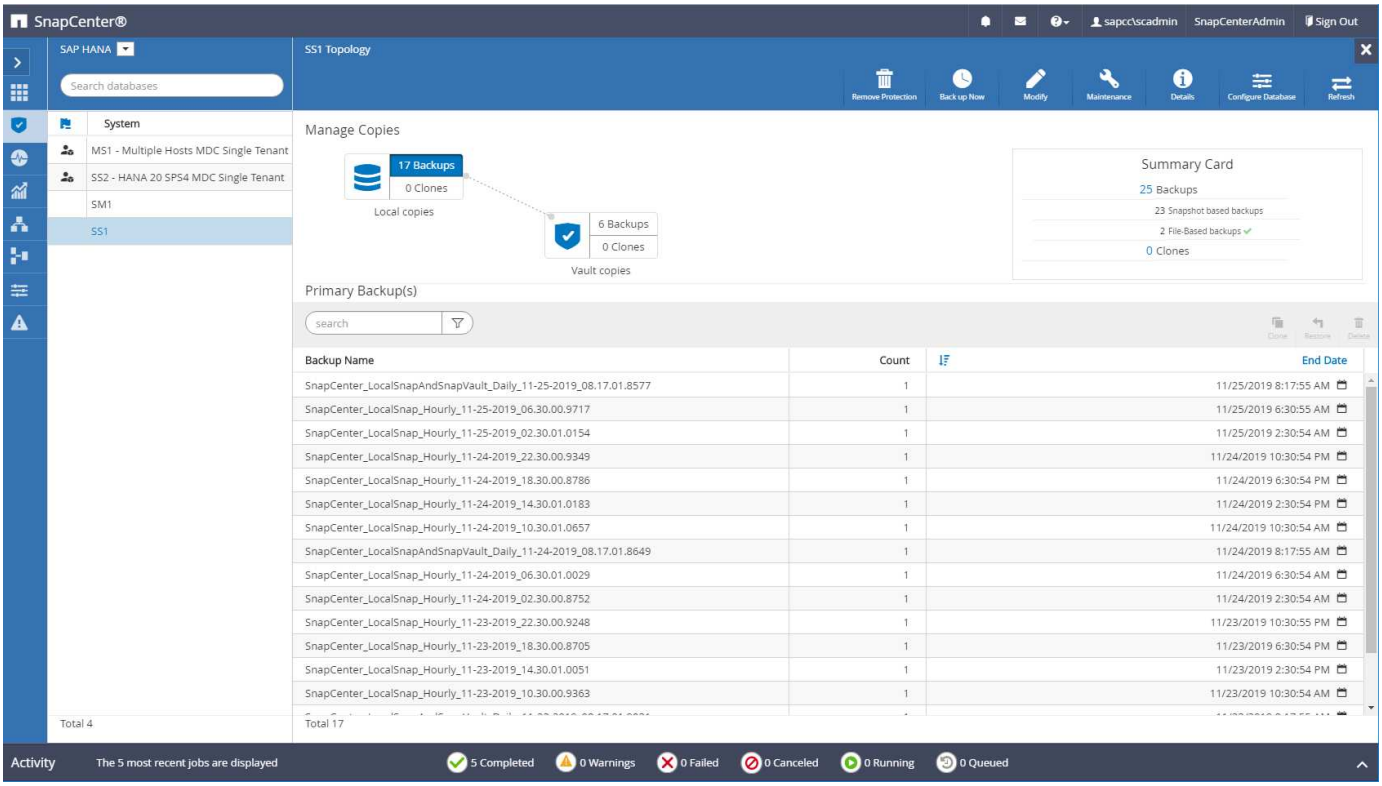
スケジュールされたこのクリーンアップが完了するまでの間、 SAP HANA と SnapCenter では、オフサイトのバックアップストレージからすでに削除されたバックアップが引き続き表示されることがあります。

その結果、オフサイトのバックアップストレージ上の対応するストレージベースの Snapshot バックアップがすでに削除されている場合でも、ログバックアップが新たに保持されることがあります。

次のセクションでは、この一時的な不一致を回避する 2 つの方法について説明します。

リソースレベルの手動更新

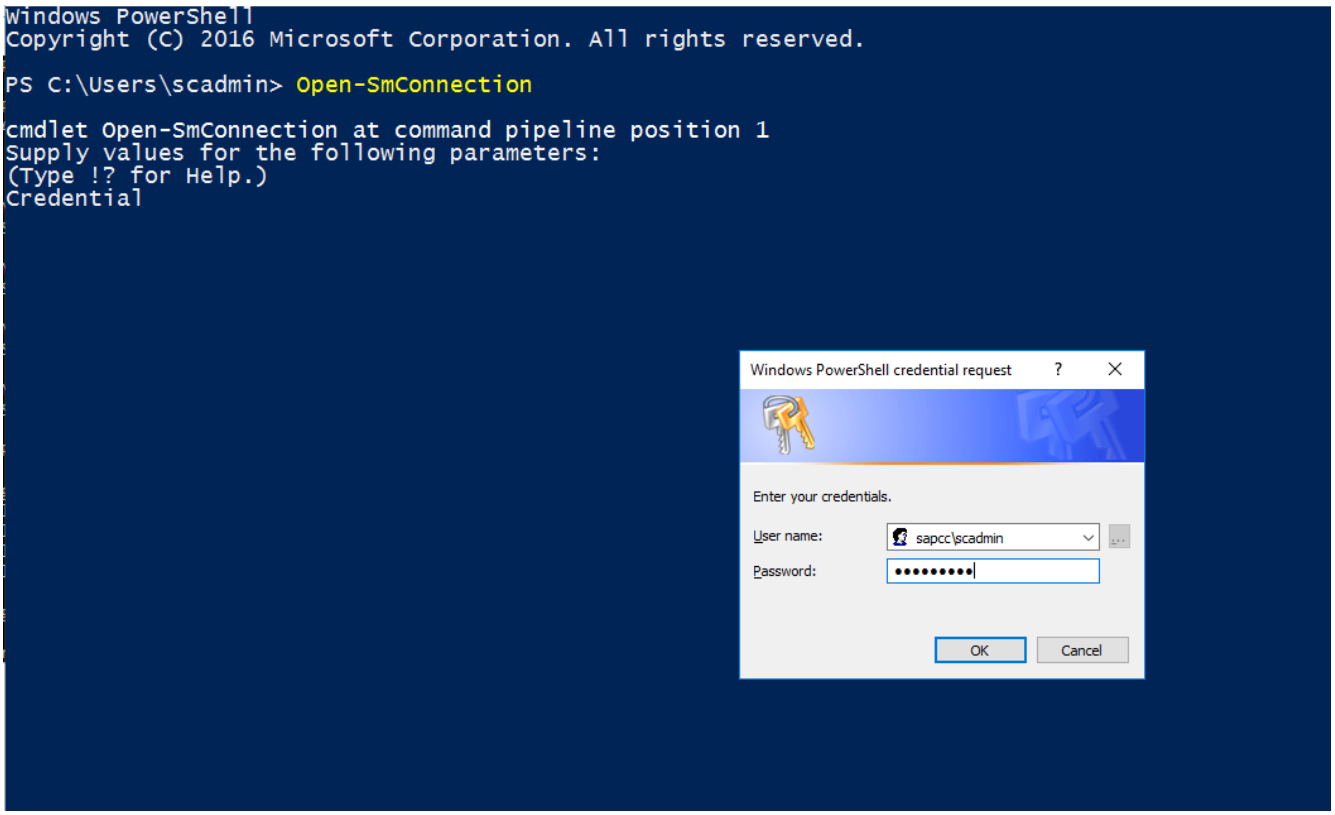
リソースのトポロジビューでは、次のスクリーンショットに示すように、セカンダリバックアップを選択する際に、 SnapCenter によってオフサイトのバックアップストレージにバックアップが表示されます。SnapCenter は、更新アイコンを使用してクリーンアップ処理を実行し、このリソースのバックアップを同期します。



SnapCenter クリーンアップジョブの頻度を変更します

SnapCenter は、 Windows タスクのスケジュールメカニズムを使用して、すべてのリソースに対してデフォルトでクリーンアップジョブ「 SnapCenter _ RemoveSecondaryBackup 」を毎週実行します。これは、 SnapCenter PowerShell コマンドレットを使用して変更できます。

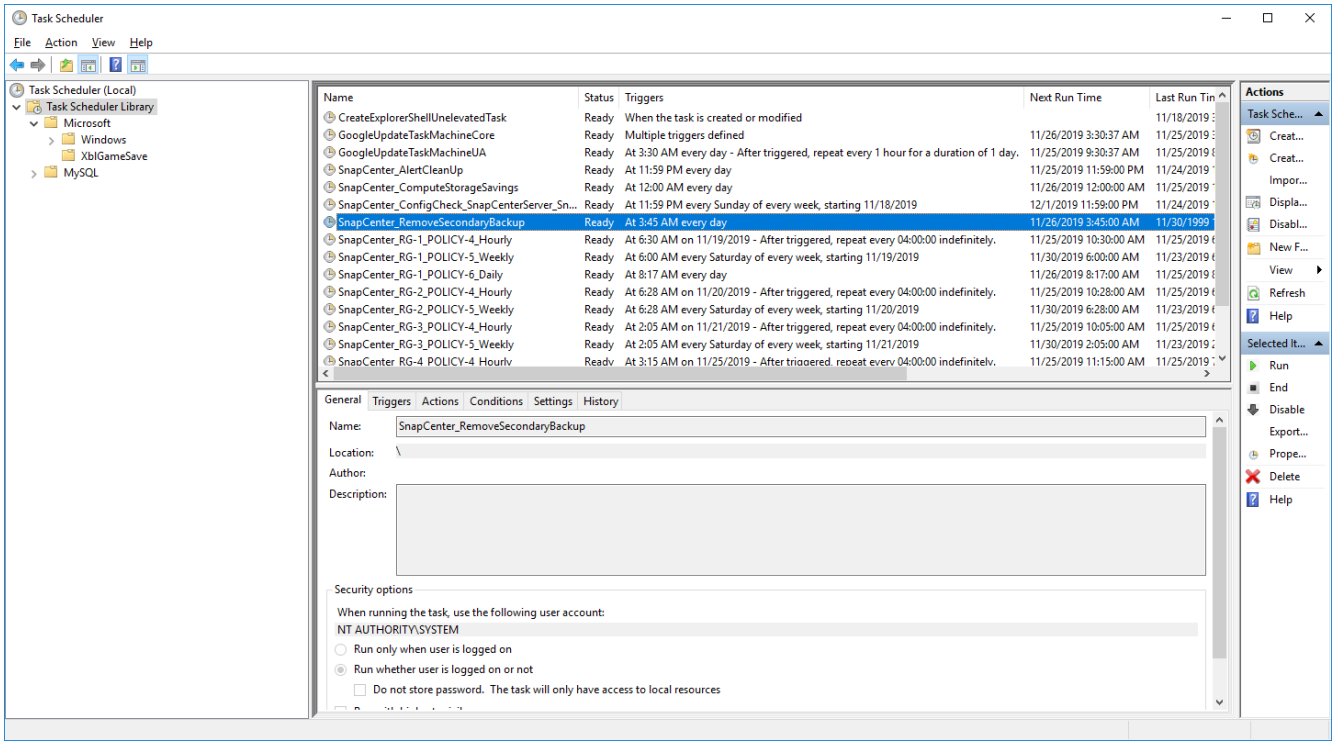
1. SnapCenter サーバで PowerShell コマンドウィンドウを起動します。
2. SnapCenter サーバへの接続を開き、ログインウィンドウに SnapCenter 管理者のクレデンシャルを入力します。



3. スケジュールを週単位から日単位に変更するには、「 Set-SmSchedule 」コマンドレットを使用します。

```
PS C:\Users\scadmin> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"=
"1"} -TaskName SnapCenter_RemoveSecondaryBackup
TaskName              : SnapCenter_RemoveSecondaryBackup
Hosts                 : {}
StartTime             : 11/25/2019 3:45:00 AM
DaysoftheMonth        :
MonthsofTheYear       :
DaysInterval          : 1
DaysOfTheWeek         :
AllowDefaults         : False
ReplaceJobIfExist     : False
UserName              :
Password              :
SchedulerType         : Daily
RepeatTask_Every_Hour :
IntervalDuration      :
EndTime               :
LocalScheduler        : False
AppType               : False
AuthMode              :
SchedulerSQLInstance  : SMCoreContracts.SmObject
MonthlyFrequency      :
Hour                  : 0
Minute                : 0
NodeName              :
ScheduleID            : 0
RepeatTask_Every_Mins :
CronExpression        :
CronOffsetInMinutes   :
StrStartTime          :
StrEndTime            :
PS C:\Users\scadmin> Check the configuration using the Windows Task
Scheduler.
```

4. Windows タスクスケジューラでジョブのプロパティを確認できます。



追加情報およびバージョン履歴の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- SnapCenter のリソースページ

  "https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- SnapCenter ソフトウェアのドキュメント

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- TR-4667 ：『 Automating SAP System Copies Using the SnapCenter 』

  https://www.netapp.com/pdf.html?item=/media/17111-tr4667pdf.pdf

- TR-4719 ：『 SAP HANA System Replication 、 Backup and Recovery with SnapCenter 』

  https://www.netapp.com/pdf.html?item=/media/17030-tr4719pdf.pdf

- TR-4018 ：『 Integrating NetApp ONTAP Systems with SAP Landscape Management 』

  https://www.netapp.com/pdf.html?item=/media/17195-tr4018pdf.pdf

- TR-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』

  https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf

バージョン履歴

バージョン	日付	ドキュメントのバージョン履歴
バージョン 1.0 以降	2017年7月	• 初版リリース
バージョン 1.1 以降	2017年9月	• 「高度な設定とチューニング」の項を追加しました。 • 微修正。
バージョン 2.0 以降	2018年3月	• SnapCenter 4.0を対象としたアップデート： 新しいデータボリュームリソース Single File SnapRestore処理の向上
バージョン 3.0 以降	2020年1月	• 「 SnapCenter の概念とベストプラクティス」の項を追加。 • SnapCenter 4.3を対象としたアップデート： 自動検出 リストアとリカバリの自動化 HANA MDCの複数テナントをサポート タンイツテナントノリストアシヨリ
バージョン 3.1 以降	2020 年 7 月	• マイナーな更新と修正： SnapCenter 4.3.1でのNFSv4のサポート SSL通信の設定 IBM Power上でのLinux用の中央プラグインの導入
バージョン 3.2 以降	2020年11月	• HANA 2.0 SPS5 に必要なデータベースユーザー権限を追加。
バージョン 3.3 以降	2021年5月	• SSL hdbsql 設定セクションを更新しました。 • Linux LVM のサポートが追加されました。
バージョン 3.4 以降	2021年8月	• 自動検出を無効にする設定の概要 が追加されました。

バージョン	日付	ドキュメントのバージョン履歴
バージョン 3.5 以降	2022年2月	• SnapCenter 4.6 に対応したマイナーアップデートと、 HANA システムレプリケーション対応 HANA システムの自動検出サポート。

著作権に関する情報

Copyright © 2024 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権を有し、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権については、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。