



# **Amazon FSX上のSAP HANA for NetApp ONTAP - SnapCenter を使用したバックアップとリカバリ NetApp solutions for SAP**

NetApp  
December 10, 2025

# 目次

Amazon FSX上のSAP HANA for NetApp ONTAP - SnapCenter を使用したバックアップとリカバリ .....	1
TR-4926：『SAP HANA on Amazon FSX for NetApp ONTAP - Backup and Recovery with SnapCenter 』 .....	1
Amazon FSX for ONTAP を使用したバックアップとリカバリ .....	1
Snapshotバックアップおよびリストア処理の実行時間 .....	2
目標復旧時間の比較 .....	2
バックアップとクローニング処理の高速化のユースケースと価値 .....	4
SnapCenter アーキテクチャ .....	6
SnapCenter コンポーネント .....	6
SnapCenter SAP HANA Backup 解決策 の略 .....	7
本ドキュメントの内容 .....	9
データ保護戦略 .....	9
ラボのセットアップ例 .....	11
SnapCenter 構成 .....	12
設定手順の概要 .....	12
SAP HANA のバックアップユーザと hdbuserstore の設定を指定します .....	12
ストレージを設定する .....	14
SAP HANAホストを追加します .....	17
ポリシーを設定する .....	19
HANAリソースを構成して保護 .....	23
SnapCenter バックアップ処理 .....	28
オンデマンドのSnapshotバックアップを作成します .....	28
オンデマンドのブロック整合性チェック処理を作成する .....	33
データボリューム以外のボリュームのバックアップ .....	38
リストアとリカバリ .....	45
SnapVault を使用したバックアップレプリケーション .....	53
概要- SnapVault によるバックアップレプリケーション .....	53
ONTAP ファイルシステムのレプリケーション関係をFSXに設定します .....	54
SnapCenter にバックアップSVMを追加 .....	59
バックアップレプリケーション用の新しいSnapCenter ポリシーを作成します .....	60
リソースの保護にポリシーを追加します .....	62
レプリケーションを使用してバックアップを作成します .....	63
セカンダリストレージからリストアおよびリカバリする .....	67
追加情報の参照先 .....	68
バージョン履歴 .....	69

# Amazon FSX上のSAP HANA for NetApp ONTAP - SnapCenter を使用したバックアップとリカバリ

## TR-4926 : 『SAP HANA on Amazon FSX for NetApp ONTAP - Backup and Recovery with SnapCenter 』

このテクニカルレポートでは、Amazon FSX上でNetApp ONTAP とNetApp SnapCenter を使用したSAP HANAデータ保護のベストプラクティスについて説明します。このドキュメントでは、SnapCenter の概念、設定に関する推奨事項、設定やバックアップ処理などの運用ワークフローについて説明します。 リストア処理とリカバリ処理を行うことができます。

作成者：Nils Bauer、NetApp

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す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え続けています。そのため、バックアップを実行してもビジネスプロセスへの影響を最小限に抑えることができれば、時間を見つけることは困難です。本番環境と非本番環境のSAPシステムのダウンタイムは、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は重要です。

## Amazon FSX for ONTAP を使用したバックアップとリカバリ

NetApp Snapshotテクノロジーを使用すれば、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 テクノロジーを使用しても、稼働中の SAP システムのパフォーマンスには影響しません。そのため、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考慮せずに、Snapshot コピーの作成をスケジュールできます。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、一般的には6時間おきにバックアップを作成します。作成されたSnapshot/バックアップは、通常、長期間保持するために低コストのストレージに移動したり、削除される前にプライマリストレージシステムに3~5日間保持されています。

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 テクノロジーを使用すると、データベース全体またはデータベースの一部を、現在使用可能なSnapshotコピーに基づいて任意の時点にリストアすることができます。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秒で完了します。オンラインのSnapshot/バックアップは1日に複数作成できるため、リカバリプロセスに要する時間は、従来の1日1回のバックアップ方式に比べて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、フォワードリカバリで適用するトランザクションログの数を少なくします。そのため、従来のストリーミング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。リストア処理とリカバリ処理のほとんどは、プライマリストレージシステムでSnapRestore を使用して管理されます。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。プライマリロケーションで使用でき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は、セカンダリロケーションも使用できます。

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 機能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レプリケートします。

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ると、以降のバックアップコピーでは、変更されたブロックだけがセカンダリストレージに移動されます。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を追加するとディスクスペースの消費量を大幅に削減できます。

## Snapshotバックアップおよびリストア処理の実行時間

次の図に、Snapshotバックアップ操作を使用したお客様のHANA Studioを示します。図に示すように、HANA データベース（約4TBのサイズ）は、Snapshotバックアップテクノロジーを使用して1分20秒以内にバックアップされ、ファイルベースのバックアップ処理を実行して4時間以上経過しています。

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のバックアップ保存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。

Backup Catalog					
<input type="checkbox"/> Show Log Backups <input type="checkbox"/> Show Delta Backups					
Stat...	Started	Duration	Size	Backup Ty...	Destinati...
■	Jan 11, 2022 10:26:59 AM	00h 01m 17s	4.51 TB	Data Back...	Snapshot
■	Jan 11, 2022 8:40:02 AM	00h 27m 11s	4.51 TB	Data Back...	Snapshot
■	Jan 11, 2022 1:00:58 AM	04h 05m 39s	3.82 TB	Data Back...	File
■	Jan 9, 2022 4:40:03 PM	00h 01m 23s	4.51 TB	Data Back...	Snapshot
■	Jan 9, 2022 8:00:02 AM	02h 39m 04s	3.82 TB	Data Back...	File
■	Jan 9, 2022 12:40:03 AM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 4:40:03 PM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 8:40:03 AM	00h 01m 22s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 12:40:03 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 4:40:03 PM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 8:40:02 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 12:40:02 AM	00h 01m 20s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 4:40:02 PM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 8:40:03 AM	00h 01m 17s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 12:40:03 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 5, 2022 4:40:03 PM	00h 01m 19s	4.51 TB	Data Back...	Snapshot

File-based backup: **4 hours 05 min**

(~270 MB/s throughput)

04h 05m 39s	3.82 TB	Data Back...	File
-------------	---------	--------------	------

Snapshot backup: **1 min 20 sec**

00h 01m 18s	4.51 TB	Data Back...	Snapshot
00h 01m 22s	4.51 TB	Data Back...	Snapshot
00h 01m 19s	4.51 TB	Data Back...	Snapshot

**Backup runtime reduced by 99%**

## 目標復旧時間の比較

ここでは、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Recovery Time Objective (RTO；目標復旧時間)を比較します。RTOは、データベースのリストア、リカバリ、および起動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、4TBのデータベースを永続性を維持した状態でリストアするには約4.5時間かかります。

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、常に数秒の範囲になります。

## 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、データベースのサイズと、データをメモリにロードするのに必要な時間によって異なります。次の例では、データを1000Mbpsでロードできると仮定しています。4TBのメモリをメモリに装着するには、約1時間10分かかります。開始時間は、ファイルベースおよびSnapshotベースのリストア処理とリカバリ処理の場合と同じです。

## 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。

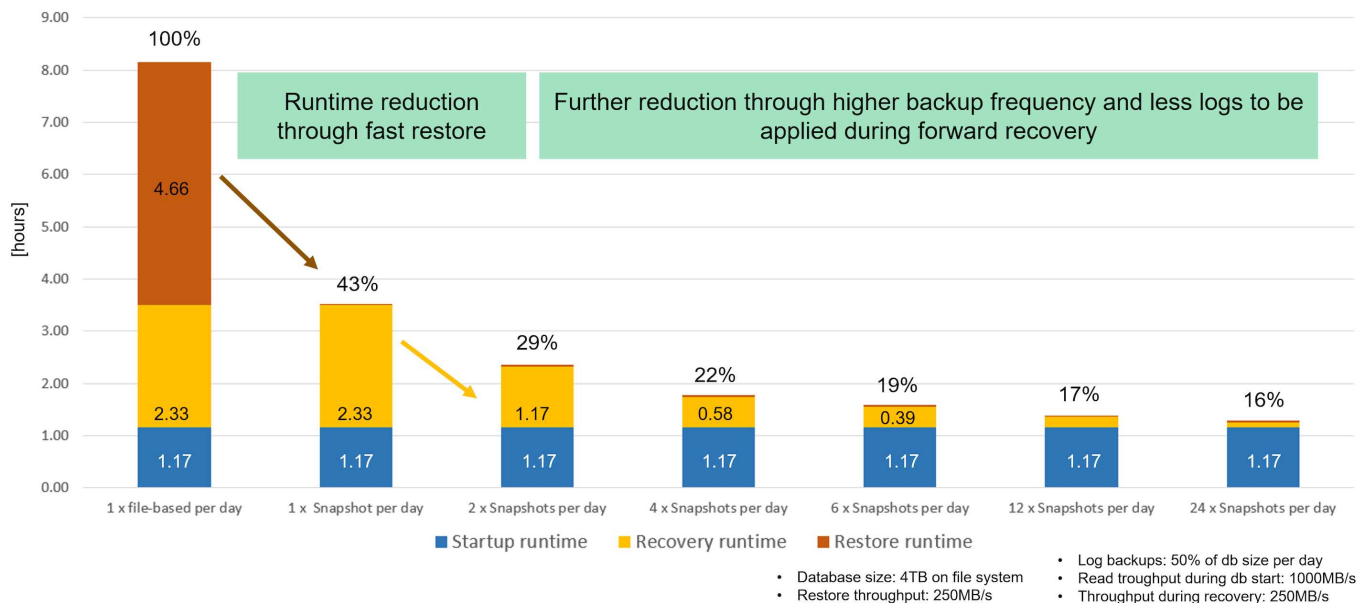
Snapshotバックアップは通常、SAP HANAデータベースのパフォーマンスに影響しないため、頻繁にスケジュールされます。たとえば、Snapshotバックアップが6時間ごとにスケジュールされている場合、最悪の場合、ファイルベースのバックアップに関しては、リカバリ時間の4分の1（6時間/24時間=.25）になります。

次の図に、リストア処理とリカバリ処理の比較を示します。毎日のファイルベースのバックアップとSnapshotバックアップでスケジュールが異なります。

最初の2つのバーは、1日に1つのSnapshotバックアップを作成した場合でも、Snapshotバックアップからのリストア処理の速度が原因で、リストアとリカバリが43%に削減されることを示しています。1日に複数のSnapshotバックアップを作成すると、フォワードリカバリで適用するログが少なくなるため、ランタイムがさらに短縮されます。

また、次の図では、1日に4~6つのSnapshotバックアップを作成することを推奨しています。頻度を高くしても、全体的な実行時間に大きな影響はありません。

## Restore and Recovery of a 4TB HANA Database (8TB RAM)



### バックアップとクローニング処理の高速化のユースケースと価値

バックアップの実行は、あらゆるデータ保護戦略に欠かせない要素です。バックアップは定期的にスケジュールされ、システム障害からリカバリできます。これは最も分かりやすいユースケースですが、SAPライフサイクル管理タスクにはバックアップとリカバリの高速化が不可欠なものもあります。

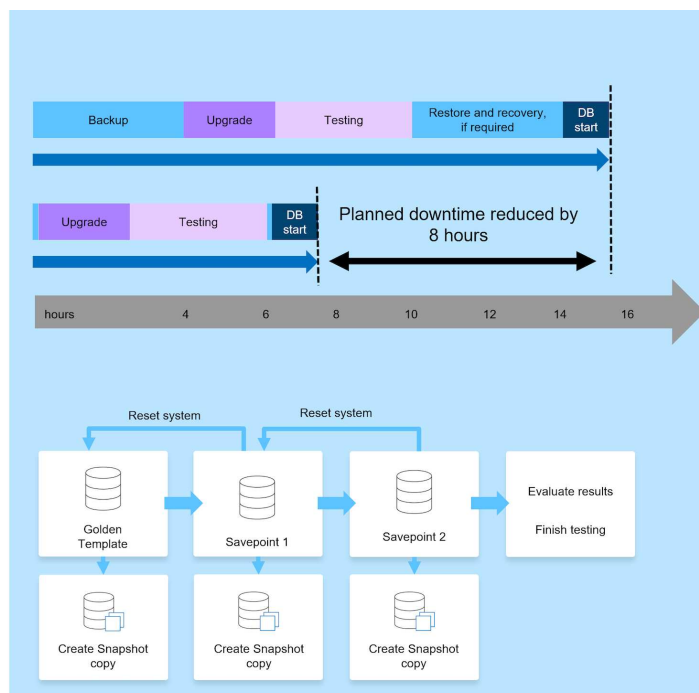
SAP HANAシステムのアップグレードは、たとえば、アップグレード前のオンデマンドバックアップと、アップグレードが失敗した場合のリストア処理が計画的停止全体に大きく影響する例です。4TBのデータベースの例を使用すると、Snapshotベースのバックアップおよびリストア処理を使用して、計画的なダウンタイムを8時間短縮できます。

別のユースケース例としては、一般的なテストサイクルが挙げられます。このテストサイクルでは、異なるデータセットまたはパラメータを使用して複数のイテレーションを行ってテストを実施する必要があります。高速バックアップおよびリストア操作を利用すると、テストサイクル内にセーブポイントを簡単に作成し、テストに失敗した場合やテストを繰り返す必要がある場合に、システムをこれらの以前のセーブポイントのいずれかにリセットできます。これにより、テストを早期に完了させることも、より多くのテストを同時に実行してテスト結果を改善することもできます。

## Use Cases for Backup and Recovery Operations

- Accelerate HANA system upgrade operations
  - Fast on-demand backup before HANA system upgrade
  - Fast restore operation in case of an upgrade failure
  - Reduction of planned downtime

- Accelerate test cycles
  - Fast creation of savepoints after a successful step
  - Fast reset of system to any savepoint
  - Repeat step until successful



Snapshotバックアップを実装したら、HANAデータベースのコピーを必要とするその他の複数のユースケースに対応できます。FSX for ONTAP を使用すると、使用可能な任意のSnapshotバックアップの内容に基づいて新しいボリュームを作成できます。この処理は、ボリュームのサイズに関係なく数秒で実行されます。

最も一般的なユースケースはSAPシステムの更新です。本番システムのデータをテストシステムまたはQAシステムにコピーする必要があります。FSX for ONTAP クローニング機能を利用すると、本番システムの任意のSnapshotコピーから、わずか数秒でテストシステム用のボリュームをプロビジョニングできます。その後、新しいボリュームをテストシステムに接続し、HANAデータベースをリカバリする必要があります。

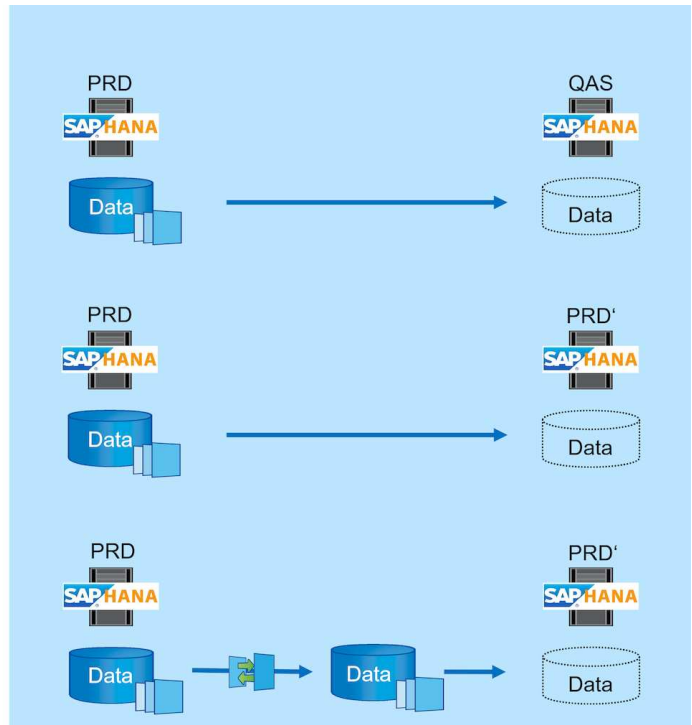
2つ目のユースケースは、リペアシステムを作成したもので、本番システムでの論理的な破損に対処するために使用されます。この場合、本番システムの古いSnapshotバックアップを使用して修復システムが開始されます。これは、破損が発生する前のデータと同一の、本番システムのクローンです。その後、リペアシステムを使用して問題を分析し、破損する前に必要なデータをエクスポートします。

最後のユースケースは、レプリケーションを停止することなくディザスタリカバリのフェイルオーバーテストを実行できるため、ディザスタリカバリの設定のRTOとRecovery Point Objective (RPO；目標復旧時点)に影響を及ぼすことなく、FSX for ONTAP NetApp SnapMirrorレプリケーションを使用してデータをディザスタリカバリサイトにレプリケートすると、本番用Snapshotバックアップをディザスタリカバリサイトでも使用できるようになり、ディザスタリカバリテスト用の新しいボリュームを作成できるようになります。



## Use Cases for Cloning Operations

- SAP System Refresh
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the test system and recover HANA database with SID change
- Repair System creation to address logical corruption
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the repair system and recover HANA database w/o SID change
- Disaster Recovery testing
  - Combined with SnapMirror Replication
  - Attach storage clone from a replicated production Snapshot backup to a DR test system



## SnapCenter アーキテクチャ

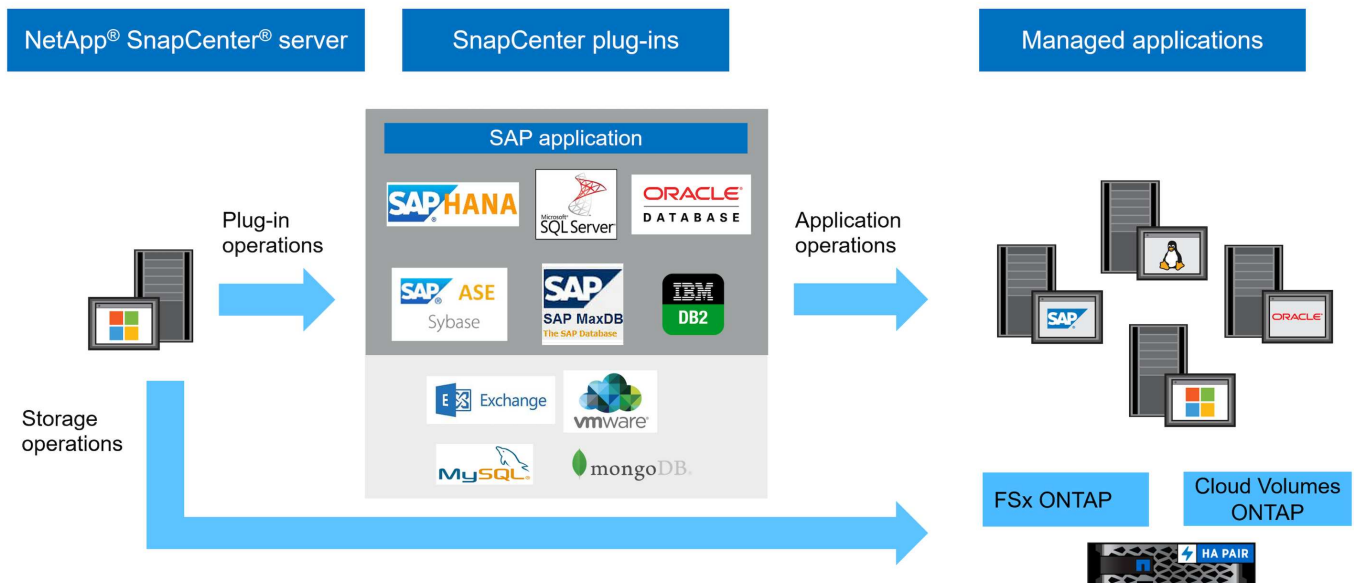
SnapCenter は、アプリケーションと整合性のあるデータ保護を実現する拡張性に優れたユニファイドプラットフォームです。SnapCenter では一元的な管理と監視が可能です。一方、アプリケーション固有のバックアップ、リストア、クローニングのジョブの管理を各ユーザに委譲することができます。SnapCenter を使用すれば、データベース管理者やストレージ管理者は、さまざまなアプリケーションやデータベースのバックアップ、リストア、クローニングの処理を 1 つのツールで管理できます。

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、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、SnapCenter Plug-in Package for Windows、および SnapCenter Plug-in Package for Linux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 SAP HANA Backup 解決策 の略

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

- バックアップ処理、スケジュール設定、保持の管理
  - 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
  - ストレージ・ベースのSnapshotコピーを使用した非データ・ボリューム・バックアップ（例：/hana/shared）
  - 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
  - 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
- 不要な SAP HANA バックアップカタログの削除
  - HANAデータのバックアップ（Snapshotとファイルベース）
  - HANAのログバックアップ
- リストア処理とリカバリ処理
  - リストアとリカバリの自動化
  - SAP HANA（MDC）システムの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ることで実行されます。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SnapMirror機能を使用して、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。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。

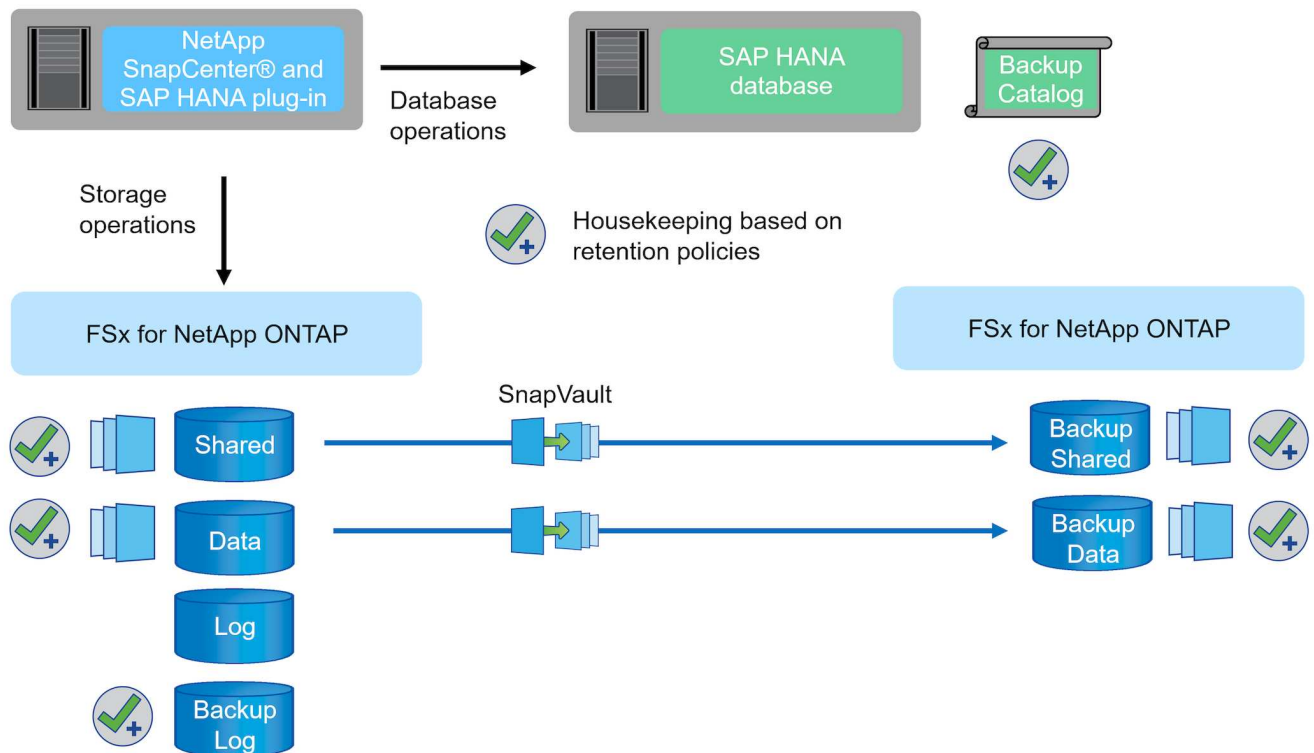
SnapCenter では、SAP HANA関連のすべてのリソースを完全にバックアップするために、ストレージベース

のSnapshotコピーにSAP HANAプラグインを使用して、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を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して、個別の保持ポリシーや保護ポリシーを有効にすることができます。

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。SnapCenter 内からブロック整合性チェックを実行できます。設定された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、ログファイルのバックアップ、およびSAP HANAのバックアップカタログの管理を行います。

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

次の図は、SnapCenter のバックアップおよび保持の管理処理の概要を示しています。



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のバックアップ保存ポイントを作成し、永続性レイヤに整合性のあるイメージを作成します。
2. データボリュームのストレージベースのSnapshotコピーを作成します。
3. ストレージベースのSnapshotバックアップをSAP HANAバックアップカタログに登録します。
4. SAP HANAのバックアップ保存ポイントを解放します。
5. データ・ボリュームに対してSnapVault またはSnapMirrorの更新を実行します（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すべてのログバックアップも削除します。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。

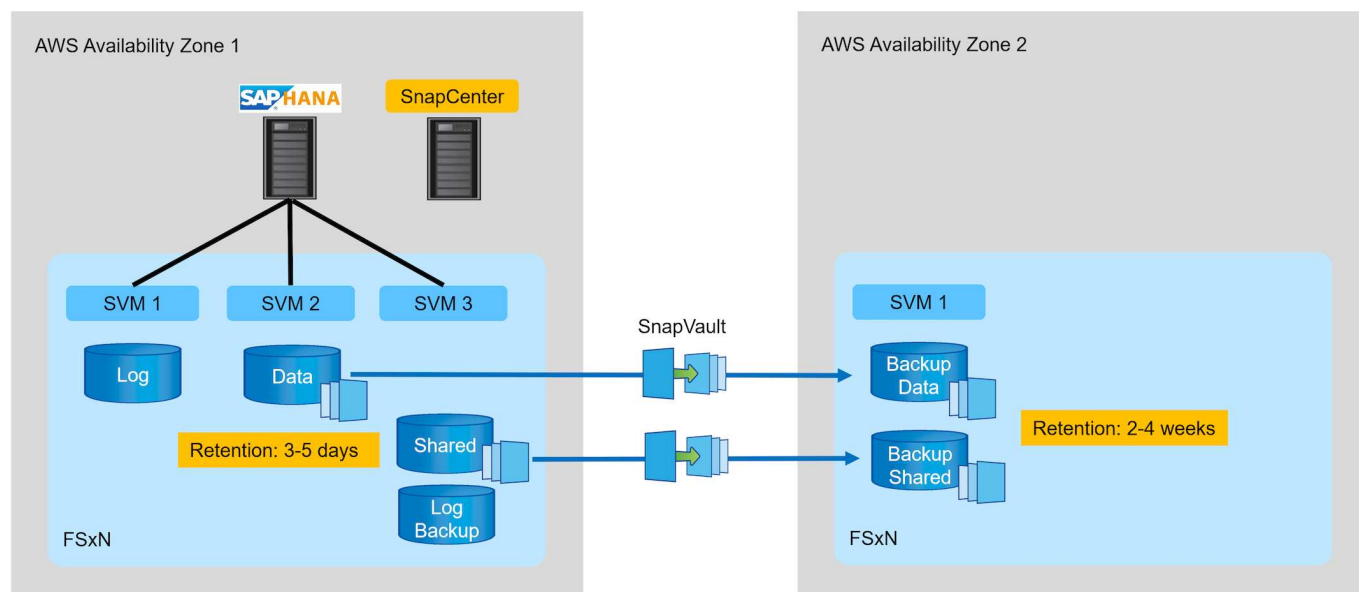
## 本ドキュメントの内容

このドキュメントでは、FSx for ONTAP上の単一テナントを持つ SAP HANA MDC 単一ホスト システムの最も一般的なSnapCenter構成オプションについて説明します。その他の構成オプションも可能であり、場合によっては、複数のホスト システムなど、特定の SAP HANA システムで必要になることがあります。その他の設定オプションの詳細については、"[SnapCenter の概念とベストプラクティス \(netapp.com\)](https://netapp.com/snapcenter-concepts)"。

このドキュメントでは、Amazon Web Services (AWS) コンソールとFSX for ONTAP CLIを使用して、ストレージレイヤで必要な設定手順を実行します。また、NetApp Cloud Managerを使用してONTAP 向けのFSXを管理することもできますが、これは本ドキュメントの対象外です。ONTAP でのFSXに対するNetApp Cloud Managerの使用については、を参照してください "[Amazon FSX for ONTAP \(netapp.com\)](https://netapp.com/fsx-aws) の詳細"。

## データ保護戦略

次の図は、FSX for ONTAP 上のSAP HANAの一般的なバックアップアーキテクチャを示しています。HANA システムは、AWSアベイラビリティゾーン1にあり、同じアベイラビリティゾーン内でONTAP ファイルシステム用のFSXを使用しています。Snapshotバックアップ処理は、HANAデータベースのデータと共有ボリュームに対して実行されます。3〜5日間保持されるローカルSnapshotバックアップに加えて、バックアップは長期保存用にオフサイトのストレージにもレプリケートされます。オフサイトバックアップストレージは、別のAWSアベイラビリティゾーンに配置されたONTAP ファイルシステム用の2番目のFSXです。HANAデータと共有ボリュームのバックアップは、SnapVault を使用して2番目のONTAP ファイルシステムのFSXにレプリケートされ、2~3週間保持されます。



SnapCenter 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。

次のパラメータを定義する必要があります。

- 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、本番、開発、テストの各システムタイプ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	6 時間ごと	6 時間ごと	6 時間ごと
プライマリの保持	3 日	3 日	3 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	ポリシー <b>LocalSnap</b> です	ポリシー <b>LocalSnapAndSnapVault</b>	ポリシーブロック整合性チェック
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。

- プロダクション：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
- Test：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。

- 本番：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。本番システムおよび開発システムでは、ファイルベースのバックアップを使用して、週単位のブロック整合性チェックをカバーするために「BlockIntegrityCheck」ポリシーを使用します。

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。

- プロダクション：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。

次の例では、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週間の保持を定義します。

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。

## ラボのセットアップ例

このあとのセクションでは、以下のラボ環境の設定例を使用しました。

HANAシステムPFX：

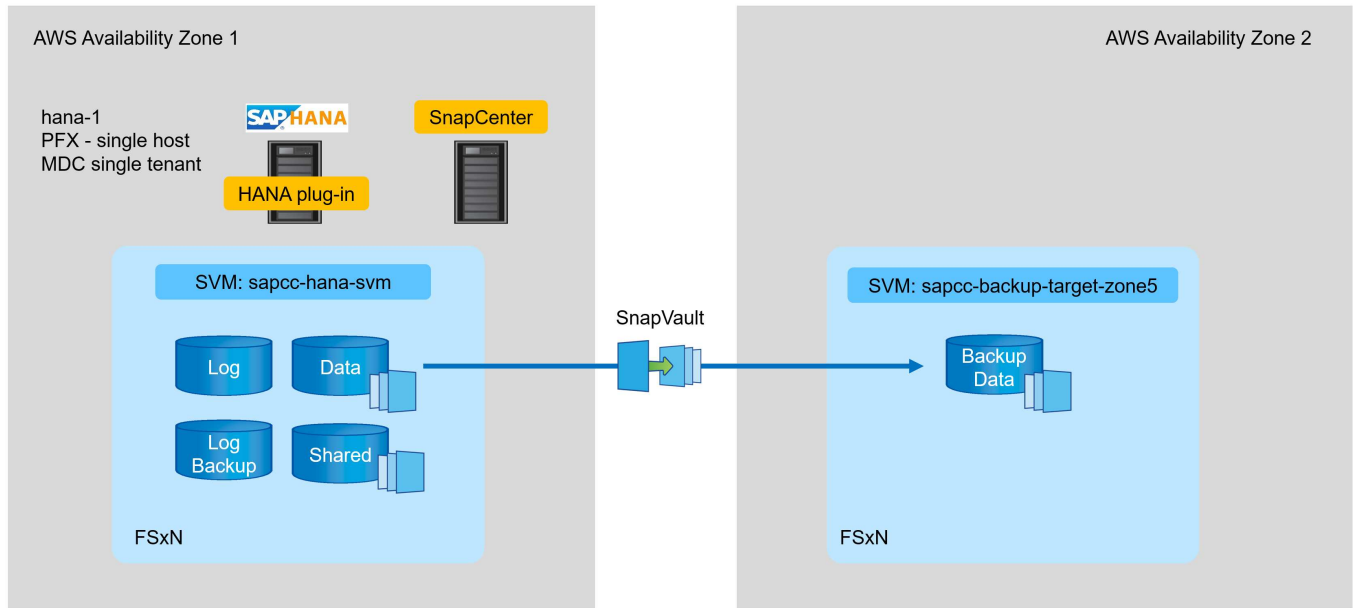
- シングルテナントのシングルホストMDCシステム
- HANA 2.0 SPS 6リビジョン60
- SLES for SAP 15SP3』を参照してください

SnapCenter：

- バージョン4.6
- HANAデータベースホストに導入されたHANAとLinuxのプラグイン

ONTAP ファイルシステムのFSx：

- ONTAP ファイルシステム用のFSX 2（単一のStorage Virtual Machine（SVM））
- 異なるAWSアベイラビリティゾーンにあるONTAP システムの各FSX
- ONTAP ファイルシステム用の2番目のFSXにHANAデータボリュームがレプリケートされます



## SnapCenter 構成

ベースのSnapCenter 構成とHANAリソースの保護については、このセクションの手順を実行する必要があります。

### 設定手順の概要

ベースSnapCenter 構成とHANAリソースの保護について、次の手順を実行する必要があります。各手順の詳細については、以降の章で説明します。

1. SAP HANAバックアップユーザとhdbuserstoreキーを設定します。hdbsqlクライアントでHANAデータベースにアクセスするために使用します。
2. SnapCenter でストレージを設定します。SnapCenter からONTAP SVMのFSXにアクセスするためのクレデンシャル
3. プラグイン導入のクレデンシャルを設定する。必要なSnapCenter プラグインをHANAデータベースホストに自動的に導入してインストールするために使用します。
4. SnapCenter にHANAホストを追加します。必要なSnapCenter プラグインを導入してインストールします。
5. ポリシーを設定する。バックアップ処理のタイプ（Snapshot、ファイル）、保持設定、およびSnapshotバックアップのオプションレプリケーションを定義します。
6. HANAのリソース保護を設定する。hdbuserstoreキーを入力し、HANAリソースにポリシーとスケジュールを適用します。

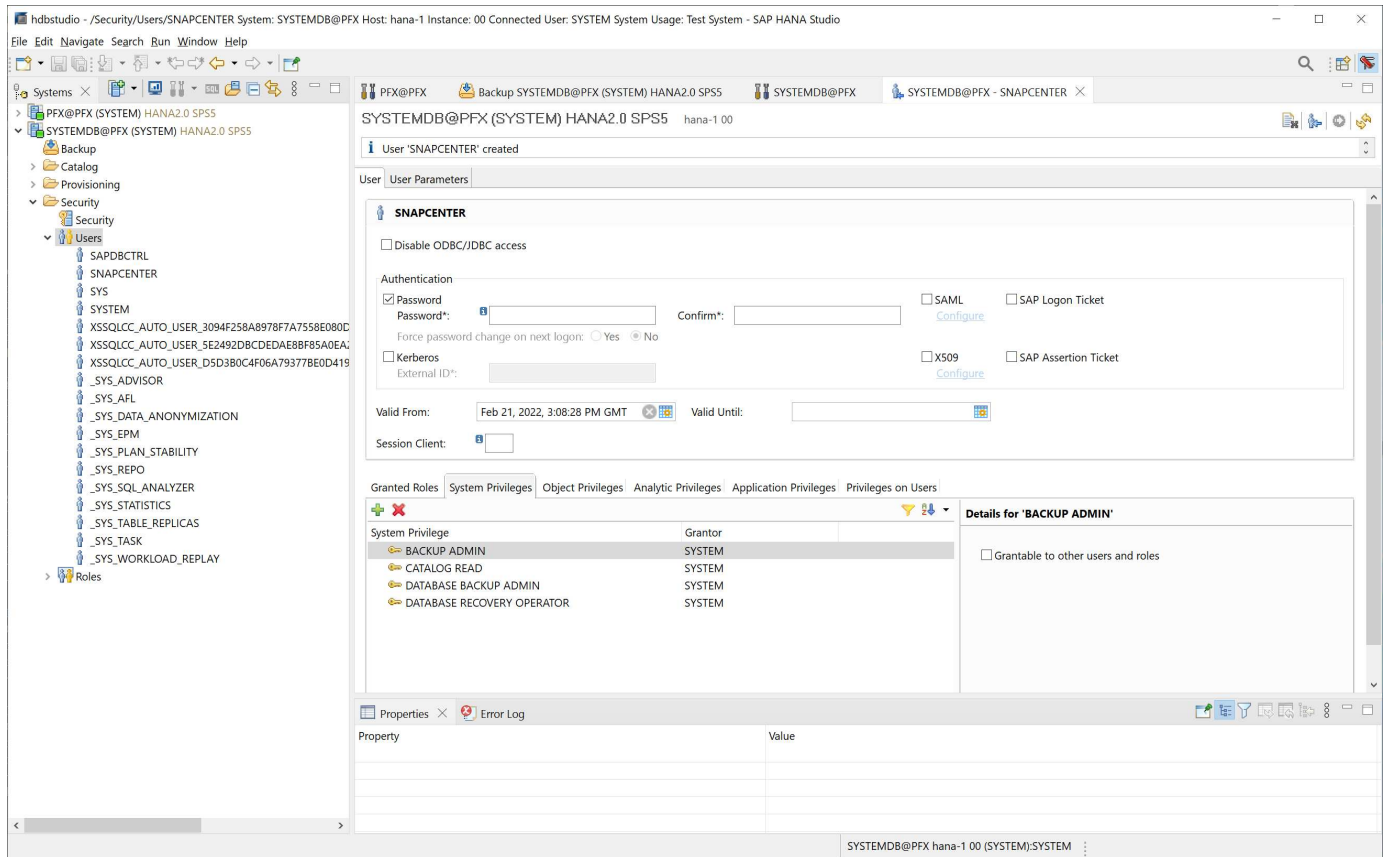
### SAP HANA のバックアップユーザと hdbuserstore の設定を指定します

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とテナントデータベースのすべてのバックアップコマンドがシステムデータベースを使用して実行されるためです。



次のコマンドは'<sid>adm'ユーザを使用したユーザストア設定に使用されます

```
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。

SAP HANA MDCの設定では、ポート「3<instanceNo>13」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の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、すべてのホストに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。ラボのセットアップでは、システムPFXのユーザ「pfxadm」のユーザストアキーを設定しました。これは、シングルテナントのシングルホス



トHANA MDCシステムです。

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore set PFXKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore list
DATA FILE      : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE       : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.KEY
ACTIVE RECORDS : 7
DELETED RECORDS : 0
KEY PFXKEY
  ENV : hana-1:30013
  USER: SNAPCENTER
KEY PFXSAPDBCTRL
  ENV : hana-1:30013
  USER: SAPDBCTRL
Operation succeed.
```

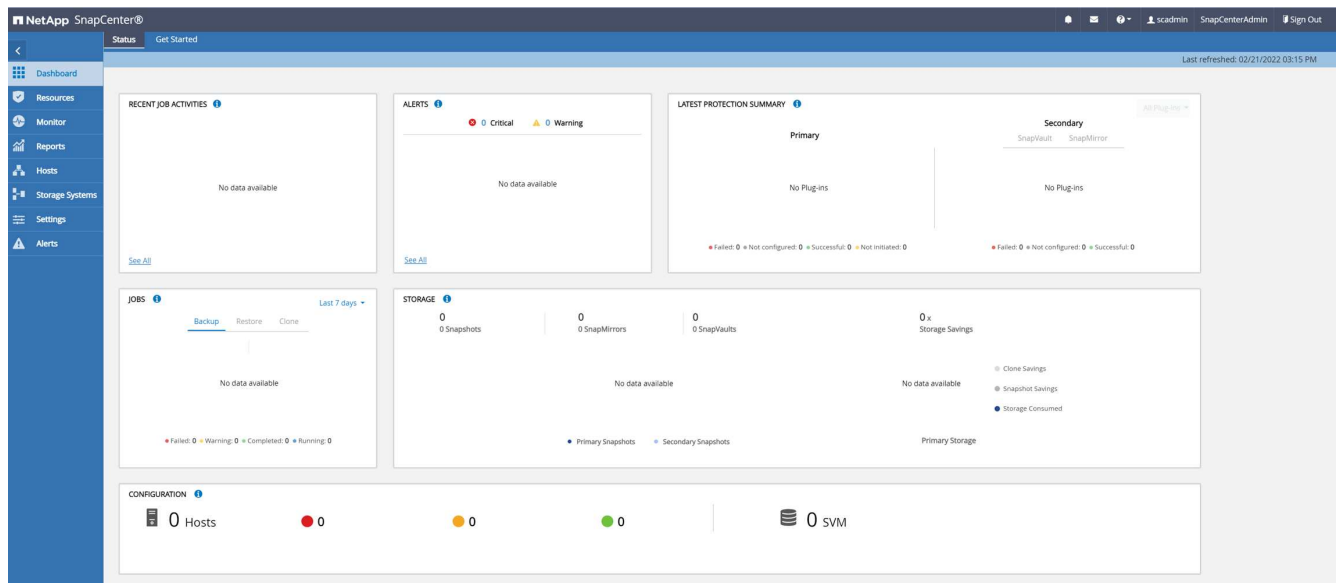
キーを使用するHANAシステムデータベースへのアクセスは、「hdbsql」コマンドで確認できます。

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbsql -U PFXKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=>
```

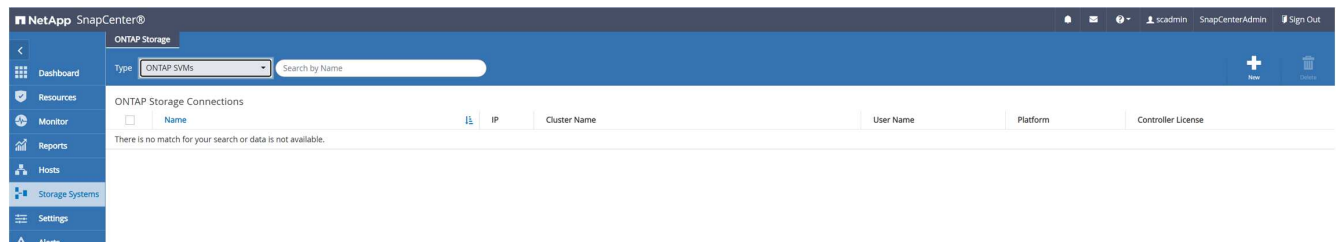
## ストレージを設定する

SnapCenter でストレージを設定するには、次の手順を実行します。

1. SnapCenter UIで、ストレージシステムを選択します。

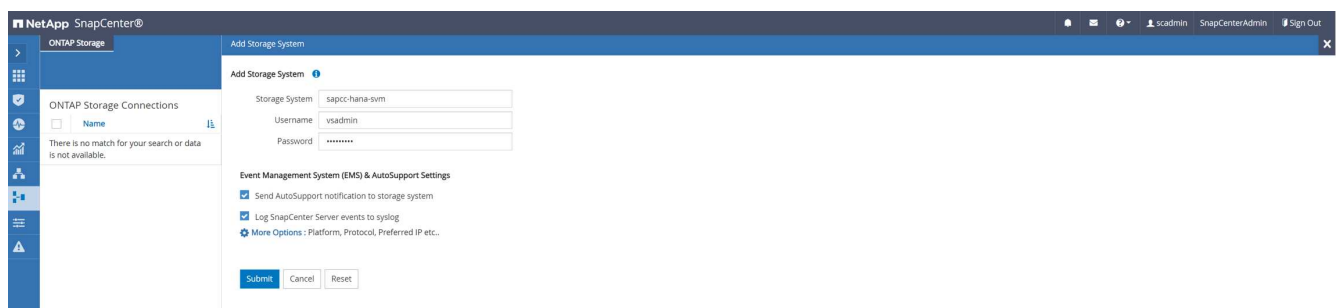


ストレージシステムのタイプとして、ONTAP SVMまたはONTAP クラスタを選択できます。次の例では、SVM管理を選択しています。



2. 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するには、Newをクリックします。

次の図に示すように、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。



3. ストレージプラットフォームを構成するには、[その他のオプション]をクリックします。
4. ストレージシステムとしてAll Flash FAS を選択して、FSX for ONTAP に含まれているライセンスがSnapCenter で使用可能になっていることを確認します。

More Options

Platform
All Flash FAS
Secondary
Protocol
HTTPS
Port
443
Timeout
60
seconds
Preferred IP
Save
Cancel

SVM「sapcc-sana-svm」がSnapCenterで設定されました。

NetApp SnapCenter®

ONTAP Storage
Type: ONTAP SVMs
Search by Name

ONTAP Storage Connections

	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	sapcc-hana-svm	198.19.255.9		vsadmin	AFF	✓

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

プラグイン導入用のクレデンシャルを作成します

SnapCenter を有効にして必要なプラグインをHANAホストに導入できるようにするには、ユーザクレデンシャルを設定する必要があります。

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

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software
Search by Credential Name

Credential Name
Authentication Mode
Details

There is no match for your search or data is not available.

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

2. ラボのセットアップでは、プラグインの導入に使用されるHANAホストに新しいユーザー「SnapCenter」を設定しました。次の図に示すように、sudo prvilleeを有効にする必要があります。

Credential

Credential Name

PluginOnLinux

Authentication Mode

Linux

Username

snapcenter

Password

\*\*\*\*\*

☒ Use sudo privileges

Cancel

OK

```
hana-1:/etc/sudoers.d # cat /etc/sudoers.d/90-cloud-init-users
# Created by cloud-init v. 20.2-8.48.1 on Mon, 14 Feb 2022 10:36:40 +0000
# User rules for ec2-user
ec2-user ALL=(ALL) NOPASSWD:ALL
# User rules for snapcenter user
snapcenter ALL=(ALL) NOPASSWD:ALL
hana-1:/etc/sudoers.d #
```

## SAP HANAホストを追加します

SAP HANAホストを追加すると、SnapCenter によって必要なプラグインがデータベースホストに導入され、自動検出処理が実行されます。

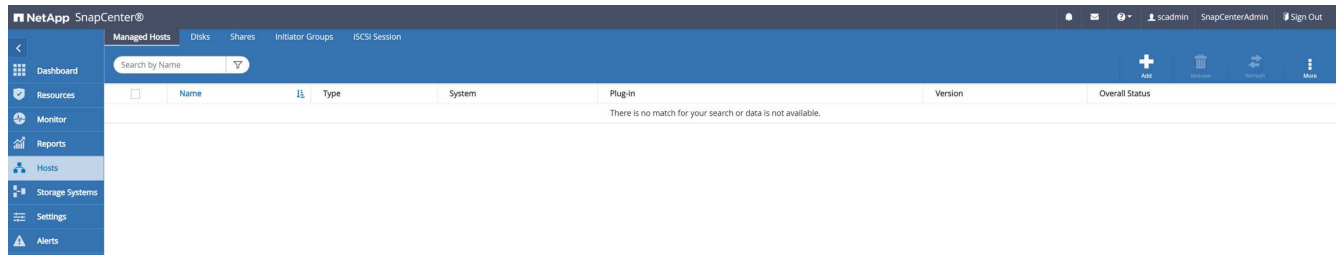
SAP HANA プラグインには、Java 64 ビットバージョン 1.8 が必要です。ホストをSnapCenter に追加する前に、ホストにJavaをインストールする必要があります。

```
hana-1:/etc/ssh # java -version
openjdk version "1.8.0_312"
OpenJDK Runtime Environment (IcedTea 3.21.0) (build 1.8.0_312-b07 suse-
3.61.3-x86_64)
OpenJDK 64-Bit Server VM (build 25.312-b07, mixed mode)
hana-1:/etc/ssh #
```

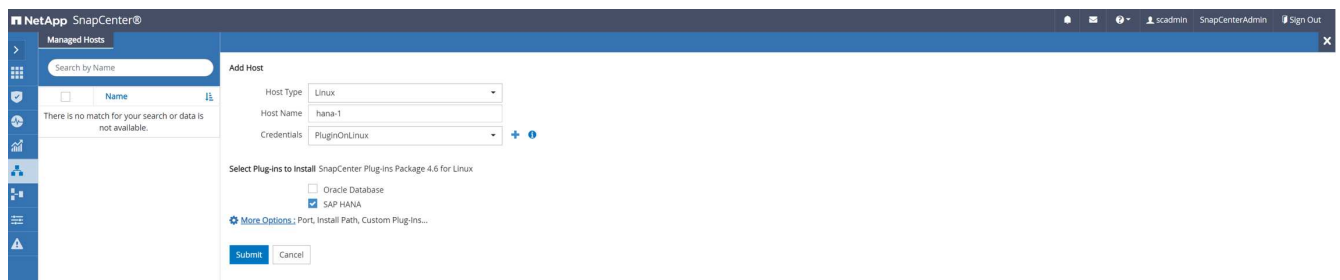
OpenJDKまたはOracle JavaはSnapCenter でサポートされています。

SAP HANAホストを追加するには、次の手順を実行します。

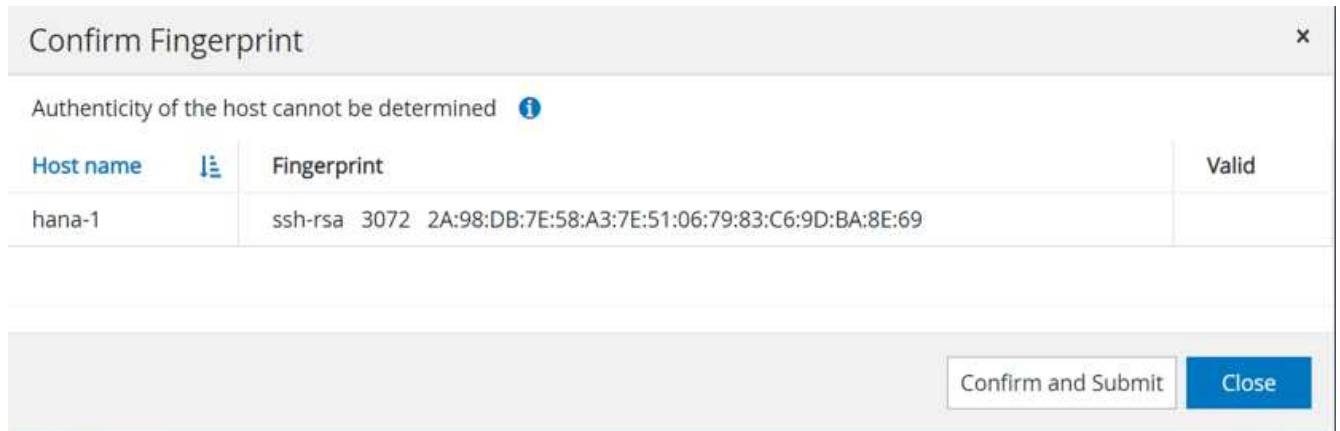
1. ホストタブで、追加をクリックします。



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。

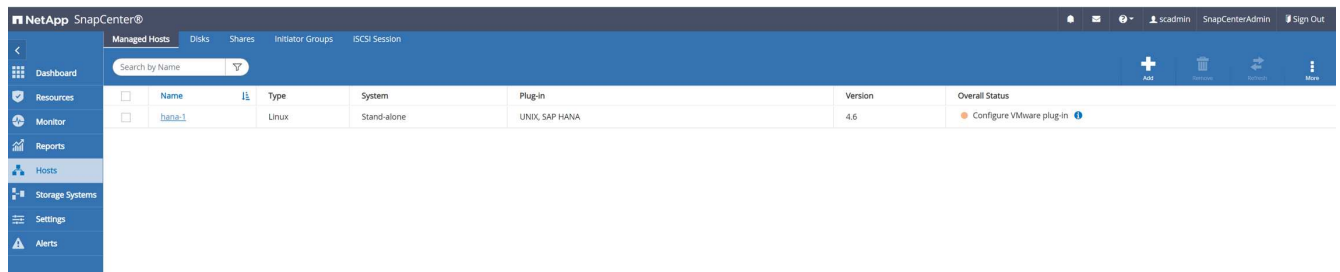


3. フィンガープリントを確認します。

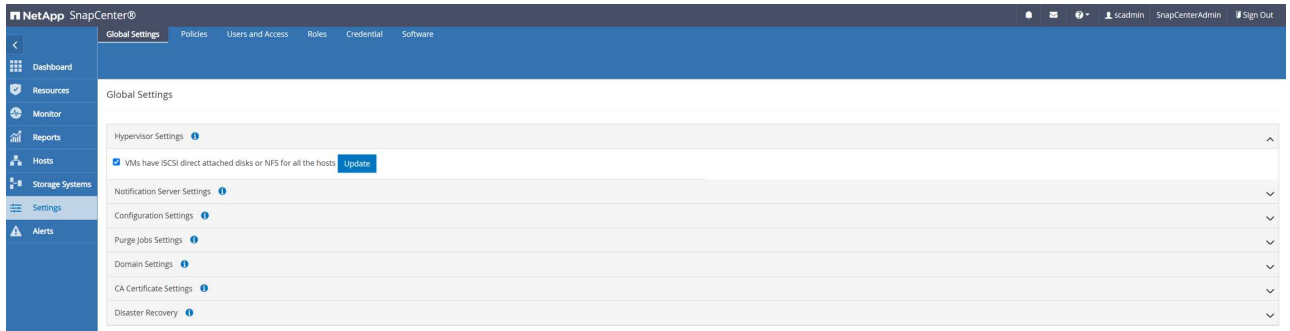


HANAとLinuxプラグインのインストールが自動的に開始されます。インストールが完了すると、ホストのステータス列にConfigure VMware Plug-inと表示されます。SnapCenter は、SAP HANA プラグインが仮想環境にインストールされているかどうかを検出します。これは、VMware環境か、パブリッククラウドプロバイダの環境です。この場合、SnapCenter はハイパーバイザーを設定するように警告を表示します。

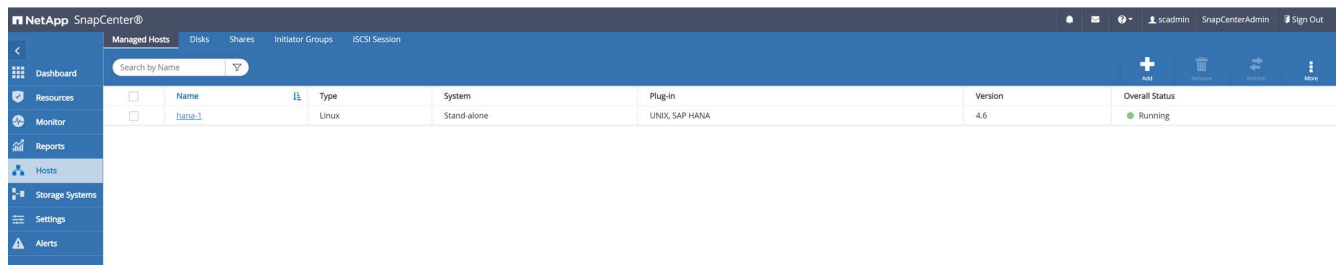
この警告メッセージを削除するには、次の手順を実行します。



- [ 設定 ] タブで、[ グローバル設定 ] を選択します。
- 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。



画面にLinuxプラグインとHANAプラグインのステータスがrunningと表示されます。



## ポリシーを設定する

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。

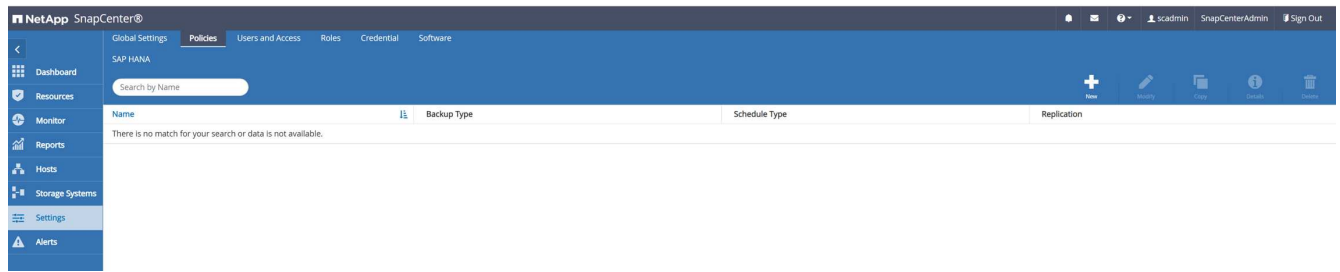
- レプリケーションを行わずに1時間ごとのバックアップを行うためのポリシー：LocalSnap
- ファイル・ベースのバックアップを使用した週次ブロック整合性チェックのポリシー：BlockIntegrityCheck

以降のセクションでは、これらのポリシーの設定について説明します。

### Snapshotバックアップのポリシー

Snapshotバックアップポリシーを設定するには、次の手順を実行します。

- [ 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。

New SAP HANA Backup Policy

1 Name

Provide a policy name

Policy name: LocalSnap

Details: Snapshot backup at primary volume

2 Settings

3 Retention

4 Replication

5 Summary

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。

スケジュール自体は、あとでHANAのリソース保護構成で設定します。

New SAP HANA Backup Policy

1 Name

2 Settings

Select backup settings

Backup Type: ☒ Snapshot Based ☐ File-Based

Schedule Frequency

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

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

3 Retention

4 Replication

5 Summary

4. オンデマンドバックアップの保持を設定します。



New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

Hourly retention settings

☒ Total Snapshot copies to keep 7

☐ Keep Snapshot copies for 14 days

5. 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。

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Choose

Error retry count 3

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnap
Details	Snapshot backup at primary volume
Backup Type	Snapshot Based Backup
Schedule Type	Hourly
Hourly backup retention	Total backup copies to retain : 7
Replication	none

これで新しいポリシーが設定されました。

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

SAP HANA

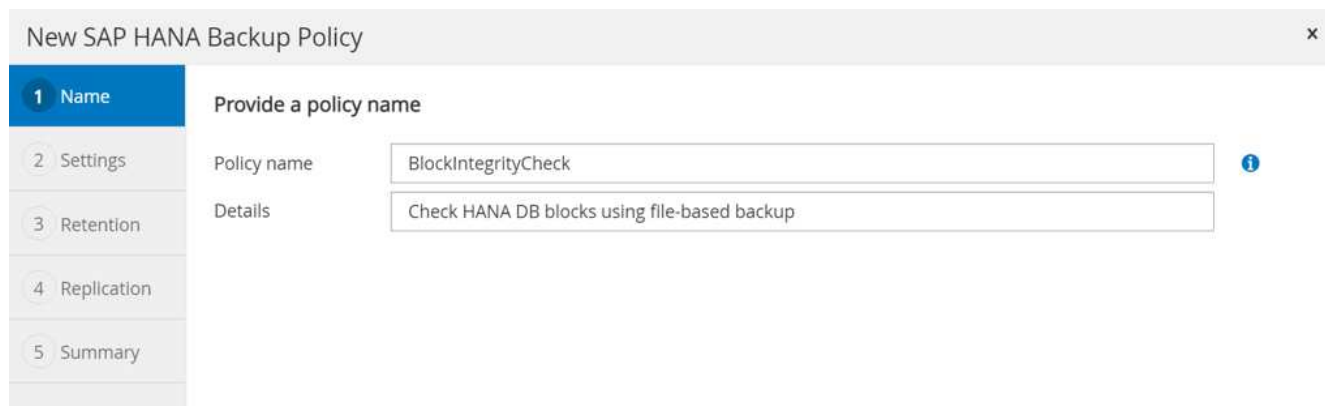
Search by Name

Name	Backup Type	Schedule Type	Replication
LocalSnap	Data Backup	Hourly	

## ブロック整合性チェックのポリシー

ブロック整合性チェックポリシーを設定する手順は、次のとおりです。

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。



New SAP HANA Backup Policy

1 Name

Provide a policy name

Policy name: BlockIntegrityCheck

Details: Check HANA DB blocks using file-based backup

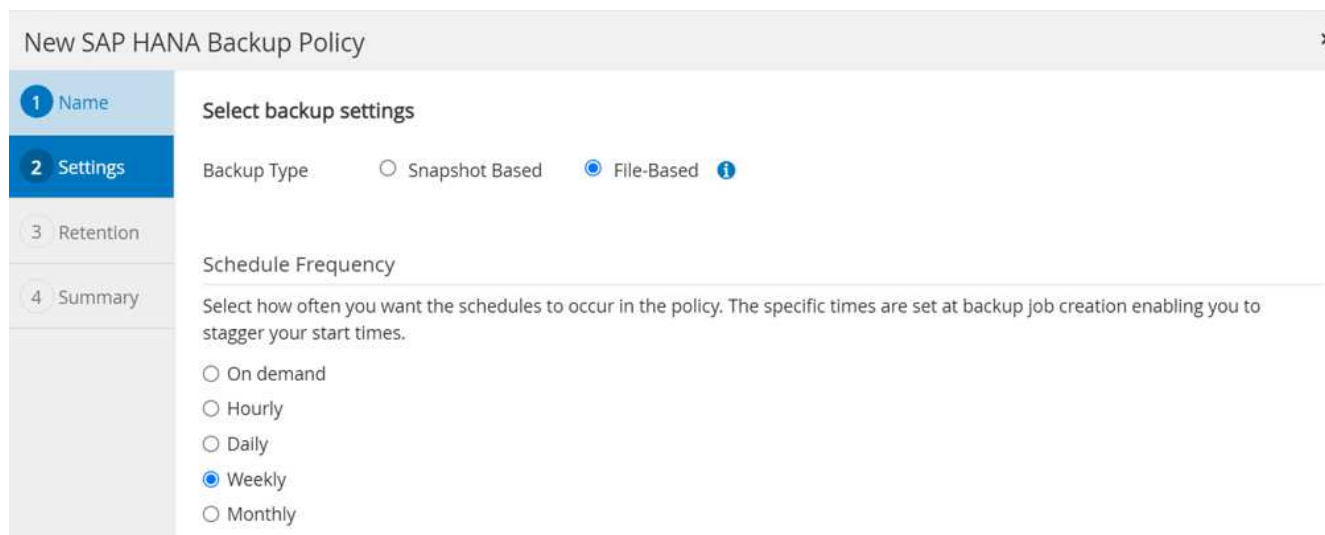
2 Settings

3 Retention

4 Replication

5 Summary

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。スケジュール自体は、あとでHANAのリソース保護構成で設定します。



New SAP HANA Backup Policy

1 Name

2 Settings

Select backup settings

Backup Type: ☐ Snapshot Based ☒ File-Based

Schedule Frequency

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

☐ On demand

☐ Hourly

☐ Daily

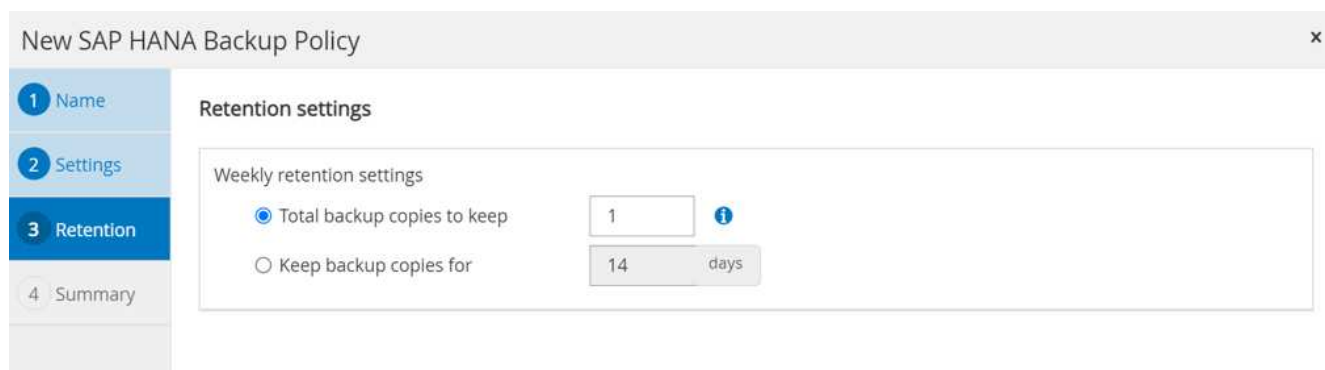
☒ Weekly

☐ Monthly

3 Retention

4 Summary

4. オンデマンドバックアップの保持を設定します。



New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

Retention settings

Weekly retention settings

☒ Total backup copies to keep: 1

☐ Keep backup copies for: 14 days

4 Summary

5. [概要] ページで、[完了] をクリックします。

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Summary

Policy name

BlockIntegrityCheck

Details

Check HANA DB blocks using file-based backup

Backup Type

File-Based Backup

Schedule Type

Weekly

Weekly backup retention

Total backup copies to retain : 1

**NetApp SnapCenter®**

Global Settings **Policies** Users and Access Roles Credential Software

SAP HANA

Search by Name

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	

Actions: New, Modify, Copy, Details, Delete

Left Sidebar: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, Alerts

Top Right: User: scadmin, SnapCenterAdmin, Sign Out

## HANAリソースを構成して保護

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。新しいHANAリソースを設定して保護するには、次の手順を実行します。

1. を選択し、リソース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。

The screenshot shows the NetApp SnapCenter web interface. The top navigation bar includes the NetApp SnapCenter logo, a user profile icon, and a 'Sign Out' button. The left sidebar contains a 'Dashboard' button and a list of navigation links: Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'SAP HANA' and shows a 'View' dropdown set to 'Multitenant Database Container'. Below this is a search bar and a table with the following columns: System, System ID (SID), Tenant Databases, Replication, Plug-in Host, Resource Groups, Policies, Last backup, and Overall Status. The table contains one row for a system named 'PFX', which is marked with a red status icon and has an 'Overall Status' of 'Not protected'.

System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX	PFX	PFX	None	hana-1				Not protected

2. HANA データベースのユーザストアキーを指定します。

## Configure Database ✕

Plug-in host

hana-1

HDBSQL OS User

pfxadm

HDB Secure User Store Key

PFXKEY

i

Cancel
OK

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。

NetApp SnapCenter®

SAP HANA

Resource - Details

Search databases

System

PFX

Details for selected resource

Type	Multitenant Database Container
HANA System Name	PFX
SID	PFX
Tenant Databases	PFX
Plug-in Host	hana-1
HDB Secure User Store Key	PFXKEY
HDBSQL OS User	pfxadm
Log backup location	/backup/log
Backup catalog location	/backup/log
System Replication	None
plug-in name	SAP HANA
Last backup	None
Resource Groups	None
Policy	None
Discovery Type	Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
sapcc-hana-svm	PFX_data_mnt00001	/PFX_data_mnt00001	

3. [リソース]タブで、リソースをダブルクリックしてリソース保護を構成します。

NetApp SnapCenter®

SAP HANA

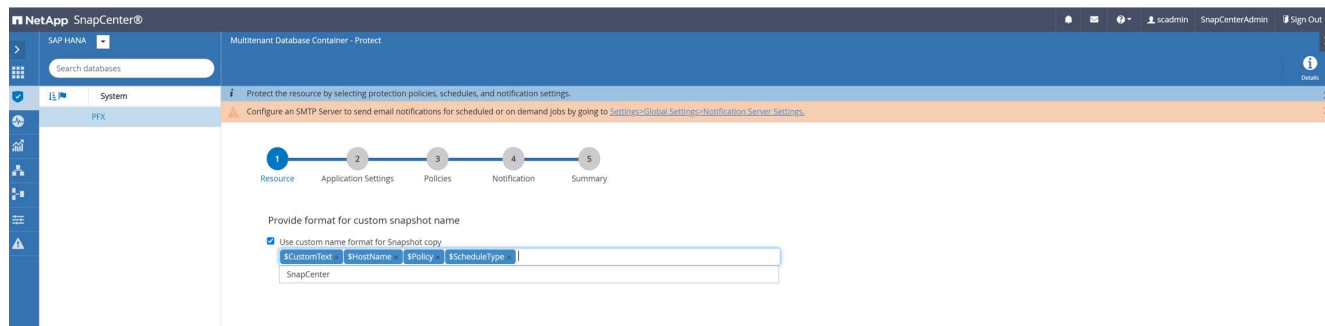
View Multitenant Database Container Search databases

Resources

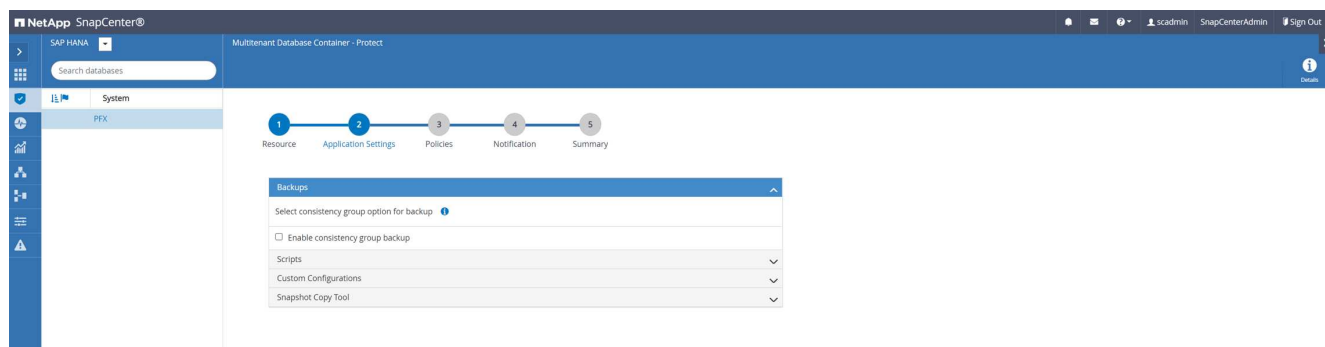
System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX	PFX	PFX	None	hana-1				Not protected

4. Snapshot コピーにカスタムの名前形式を設定します。

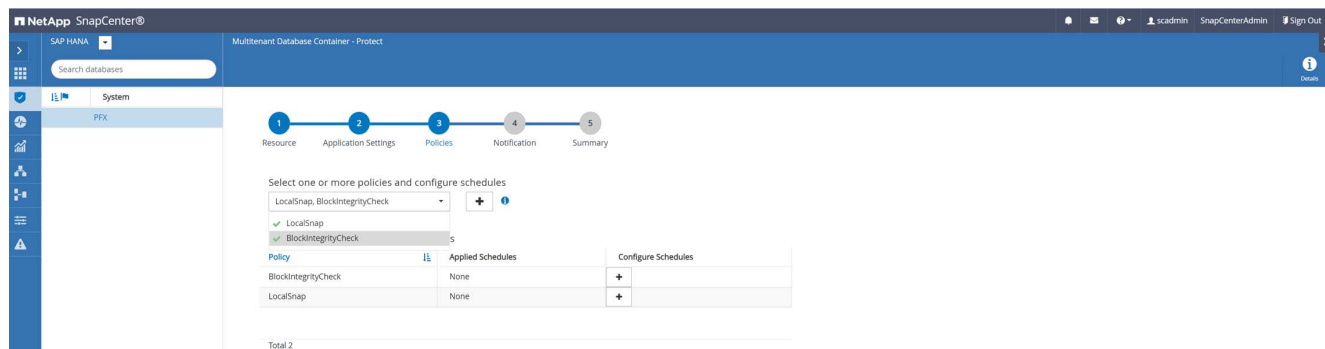
カスタムの Snapshot コピー名を使用して、どのバックアップがどのポリシーおよびスケジュールタイプで作成されたかを簡単に識別することを推奨します。Snapshot コピー名にスケジュールタイプを追加することで、スケジュールバックアップとオンデマンドバックアップを区別できます。オンデマンドバックアップの「スケジュール名」文字列は空ですが、スケジュールバックアップには「毎時」、「毎日」、または「毎週」という文字列が含まれます。



5. [ 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。



6. リソースに追加するポリシーを選択してください。



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回に設定されています。

## Add schedules for policy BlockIntegrityCheck



### Weekly

Start date

02/22/2022 12:00 pm



☐ Expires on

03/22/2022 12:00 pm



Days

Sunday

✓ Sunday

Monday

Tuesday

Wednesday

Thursday

Friday



The schedules are triggered in the SnapCenter Server time zone.



Cancel

OK

8. ローカルSnapshotポリシーのスケジュールを定義します。

この例では、6時間ごとに設定されています。

## Modify schedules for policy LocalSnap



### Hourly

Start date

02/22/2022 02:00 pm



☐ Expires on

04/28/2022 11:57 am



Repeat every

6

hours

0

mins



The schedules are triggered in the SnapCenter Server time zone.



Cancel

OK

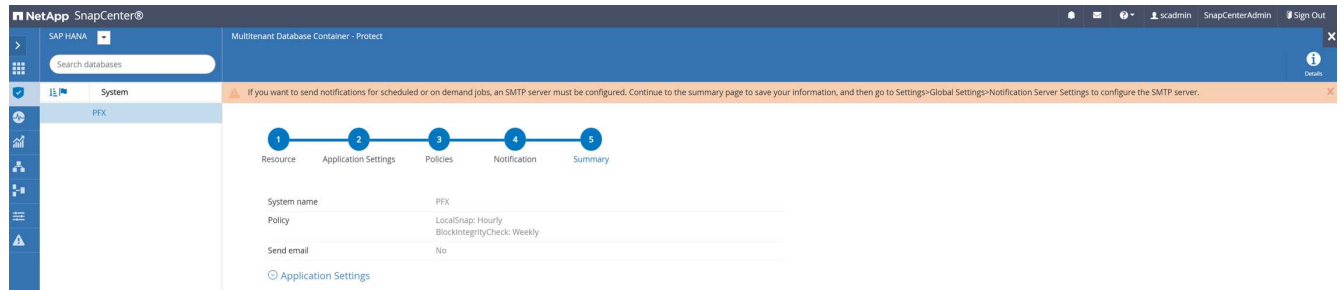
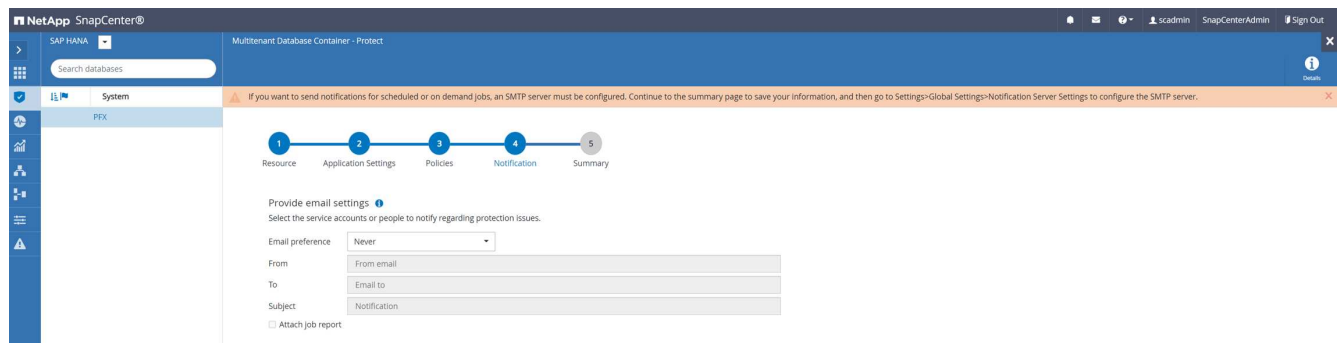
The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains navigation icons for System, PFX, and other resources. The main content area displays a configuration wizard for the 'LocalSnap' policy. The wizard has five steps: 1. Resource, 2. Application Settings, 3. Policies, 4. Notification, and 5. Summary. The 'Policies' step is currently active. Below the step indicator, there is a section titled 'Select one or more policies and configure schedules' which shows a dropdown menu with 'LocalSnap, BlockIntegrityCheck' selected. Below this, there is a table titled 'Configure schedules for selected policies'.

Policy	Applied Schedules	Configure Schedules
BlockIntegrityCheck	Weekly: Run on days: Sunday	
LocalSnap	Hourly: Repeat every 6 hours	

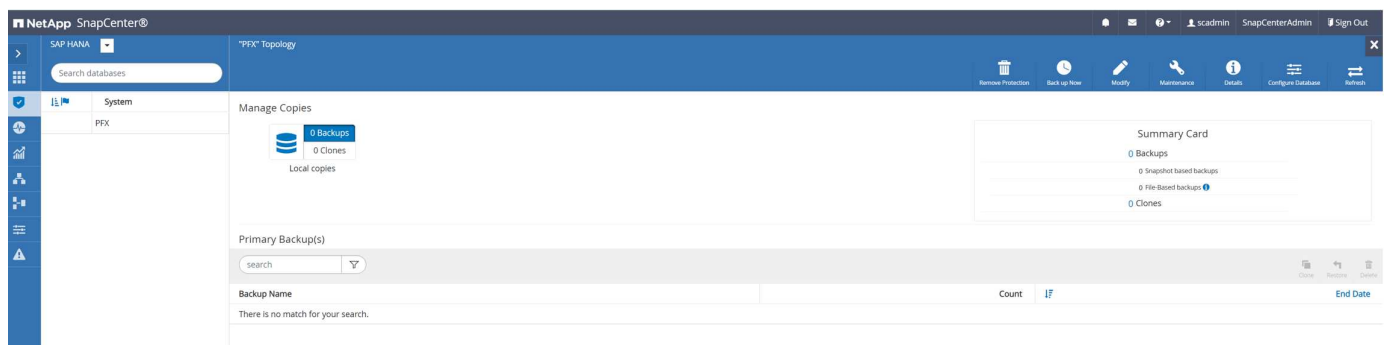
Total 2

9. E メール通知に関する情報を指定します。





HANAのリソース構成が完了し、バックアップを実行できるようになります。



## SnapCenter バックアップ処理

オンデマンドのSnapshotバックアップ処理とオンデマンドのブロック整合性チェック処理を作成できます。

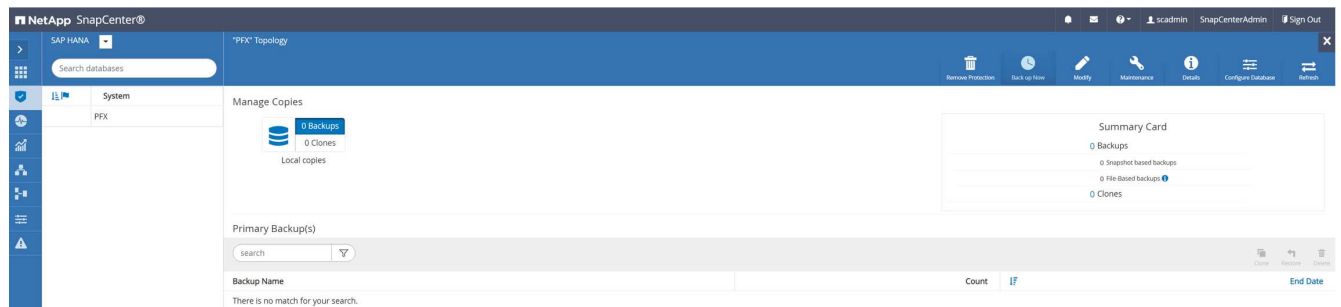
### オンデマンドのSnapshotバックアップを作成します

オンデマンドのSnapshotバックアップを作成するには、次の手順を実行します。

1. リソースビューで、リソースを選択し、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。上部には、プライマリストレージのバックアップ（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）のバックアップトポロジが表示されます。

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。



3. 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

Backup

Create a backup for the selected resource

Resource Name

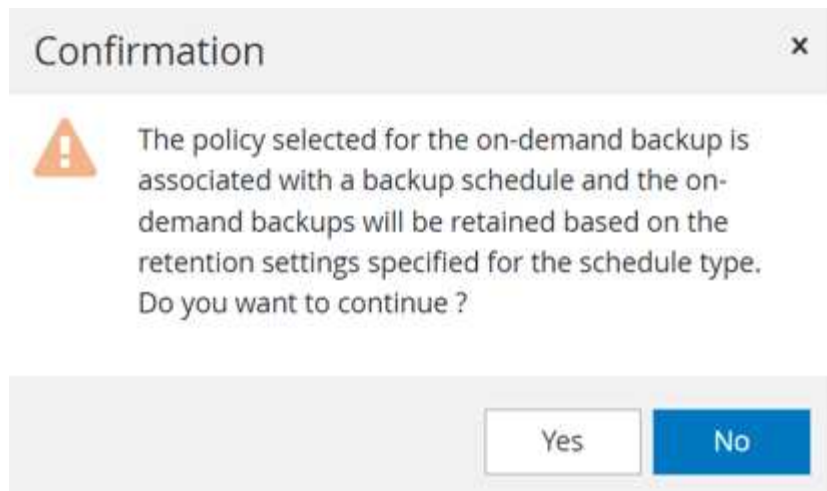
PFX

Policy

LocalSnap

Cancel

Backup



前の5つのジョブのログは、Topologyビューの下部にあるActivity領域に表示されます。

4. 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

Job Details

Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'LocalSnap'

▼ Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'LocalSnap'

▼ hana-1

Backup

▶ Validate Dataset Parameters

▶ Validate Plugin Parameters

▶ Complete Application Discovery

▶ Initialize Filesystem Plugin

▶ Discover Filesystem Resources

▶ Validate Retention Settings

▶ Quiesce Application

▶ Quiesce Filesystem

▶ Create Snapshot

▶ UnQuiesce Filesystem

▶ UnQuiesce Application

▶ Get Snapshot Details

▶ Get Filesystem Meta Data

▶ Finalize Filesystem Plugin

▶ Collect Autosupport data

▶ Register Backup and Apply Retention

▶ Register Snapshot attributes

▶ Application Clean-Up

▶ Data Collection

▶ Agent Finalize Workflow

Task Name: Backup Start Time: 02/22/2022 12:08:58 PM End Time: 02/22/2022 12:10:21 PM

View Logs

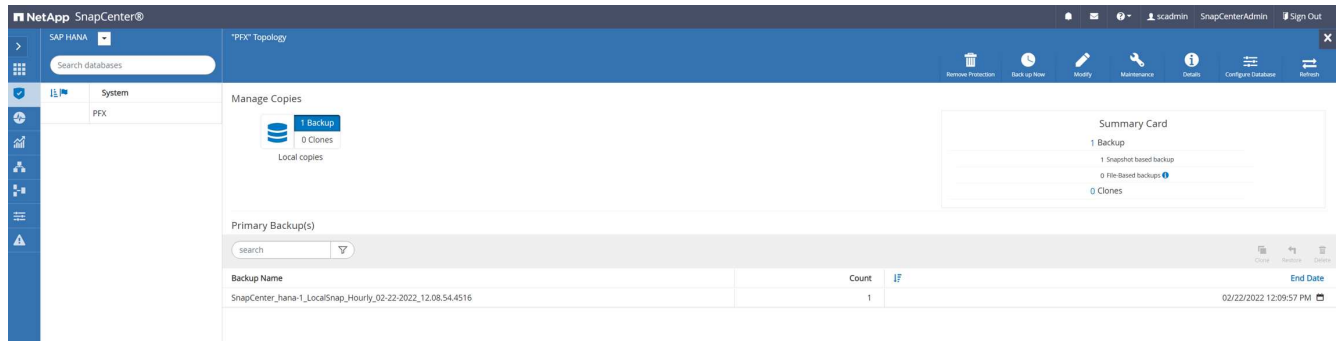
Cancel Job

Close

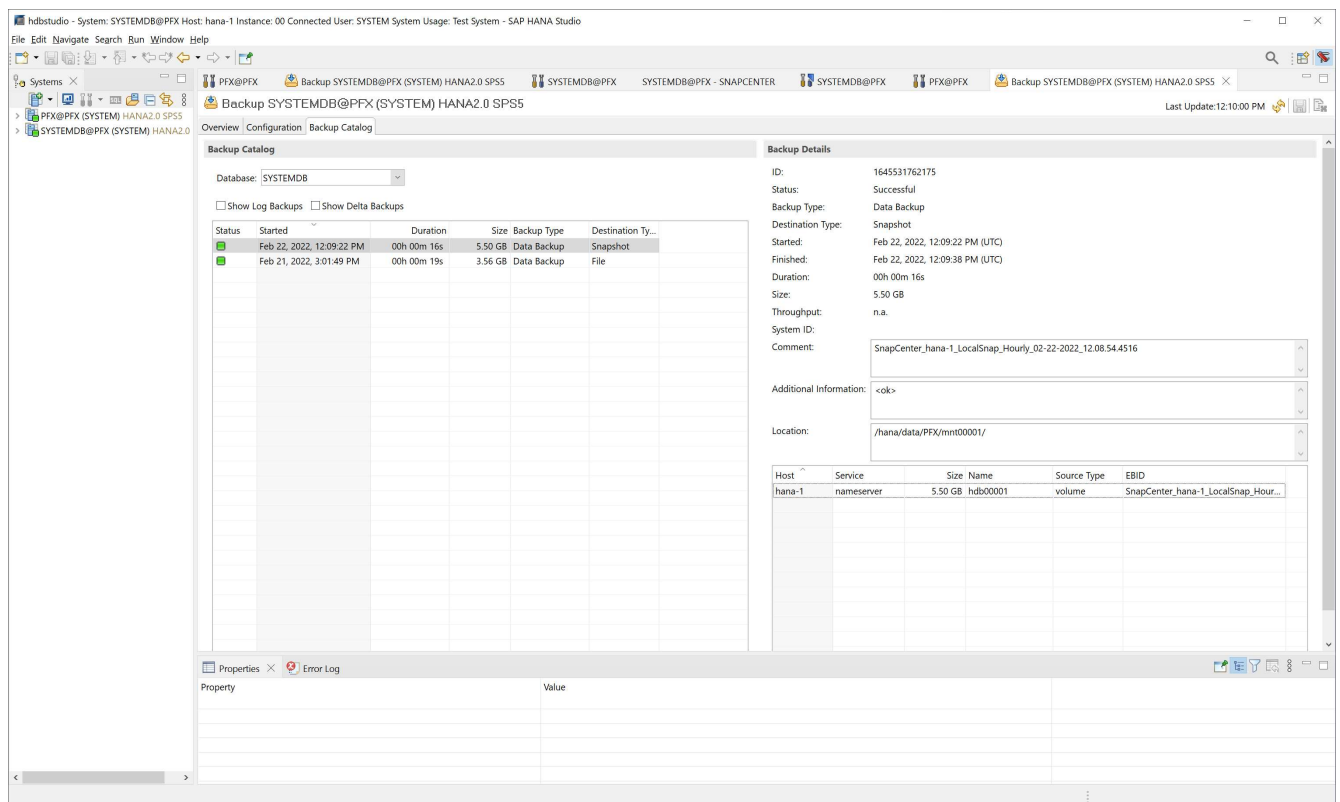
バックアップが完了すると、トポロジビューに新しいエントリが表示されます。バックアップ名は、セクションで定義したSnapshot名と同じ命名規則に従います。"「[HANAリソースを構成して保護する](#)」"

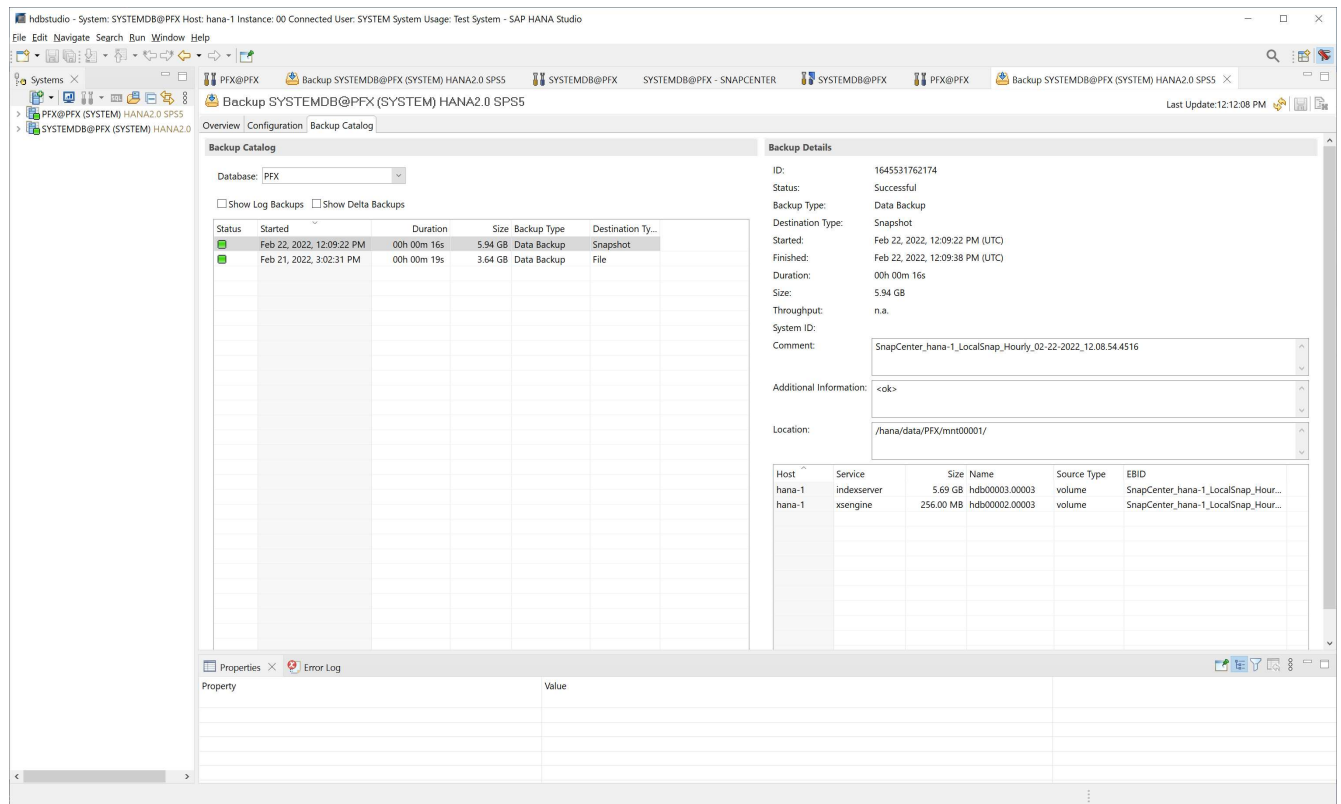
31

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。



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。次の図に、システムデータベースとテナントデータベースPFXの次の図を示します。





ONTAP ファイルシステムのFSXでは、SVMのコンソールに接続してSnapshotバックアップを表示できます。

```
sapcc-hana-svm::> snapshot show -volume PFX_data_mnt00001
---Blocks---
Vserver   Volume   Snapshot                                     Size Total%
Used%
-----
sapcc-hana-svm
          PFX_data_mnt00001
          SnapCenter_hana-1_LocalSnap_Hourly_02-22-
2022_12.08.54.4516
                                     126.6MB      0%
2%
sapcc-hana-svm::>
```

## オンデマンドのブロック整合性チェック処理を作成する

ポリシーBlockIntegrityCheckを選択すると、Snapshotバックアップジョブと同様にオンデマンドでブロック整合性チェック処理が実行されます。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。

## Backup



Create a backup for the selected resource

Resource Name

PFX

Policy

BlockIntegrityCheck



Cancel

Backup



Job Details

Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ hana-1

✓ ▾ File-Based Backup

✓ ▶ Validate Plugin Parameters

✓ ▶ Start File-Based Backup

✓ ▶ Check File-Based Backup

✓ ▶ Register Backup and Apply Retention

✓ ▶ Data Collection

Task Name: File-Based Backup Start Time: 02/22/2022 12:55:21 PM End Time: 02/22/2022 12:56:36 PM

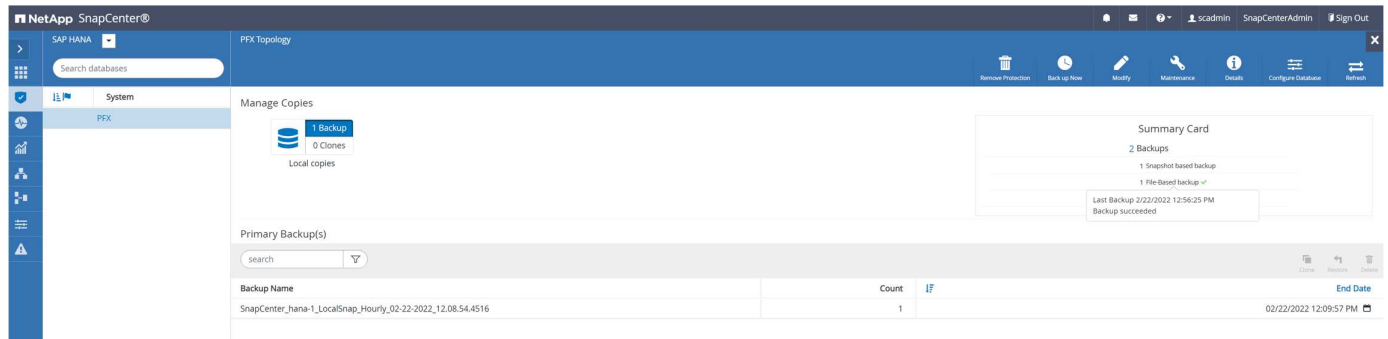
View Logs

Cancel Job

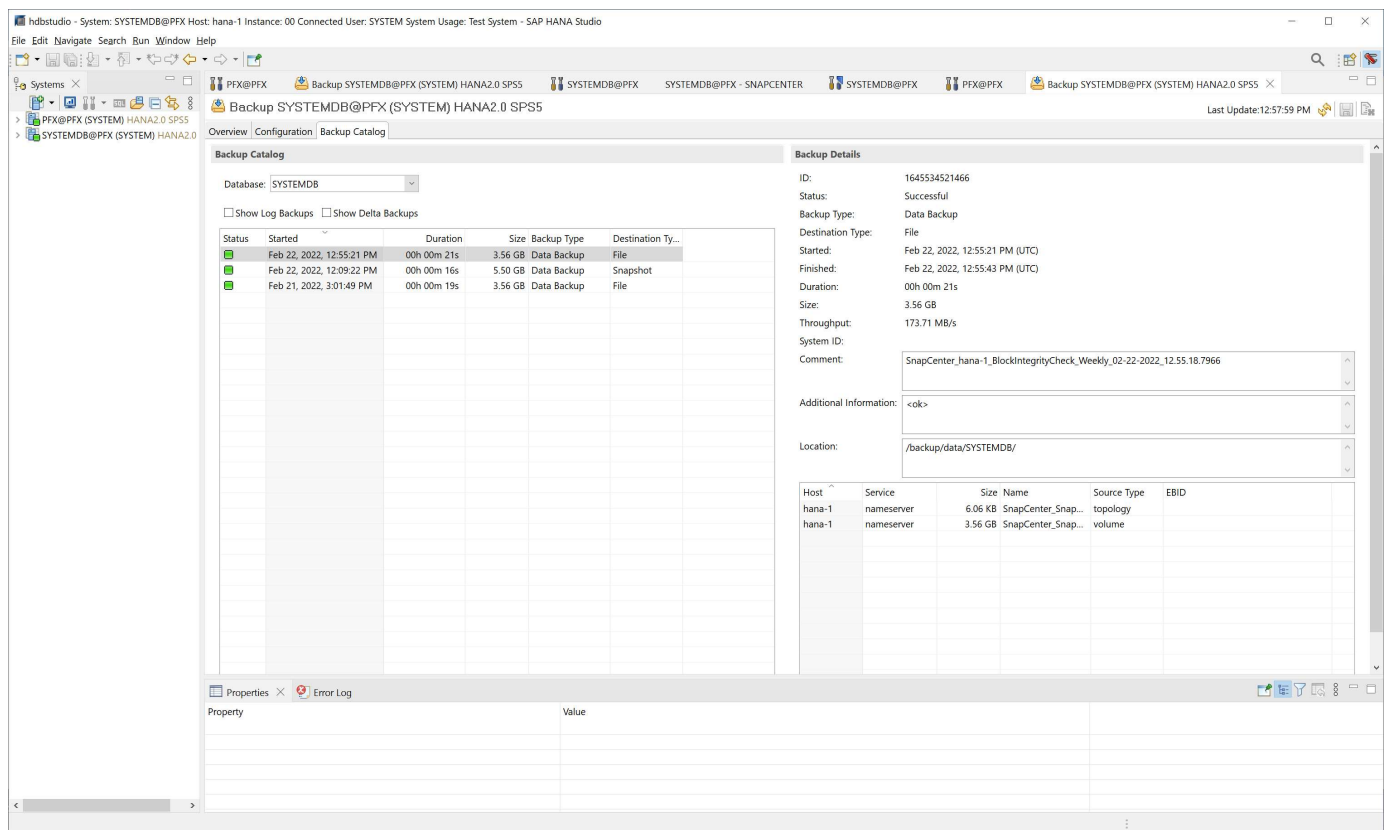
Close

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。



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。次の図は、システムとテナントデータベースのバックアップカタログ内のSnapCenter ブロックの整合性チェックを示しています。



hdbstudio - System: SYSTEMDB@PFX Host: hana-1 Instance: 00 Connected User: SYSTEM System Usage: Test System - SAP HANA Studio

File Edit Navigate Search Run Window Help

Systems ×

Backup SYSTEMDB@PFX (SYSTEM) HANA2.0 SPS5

Last Update: 12:58:19 PM

Overview Configuration Backup Catalog

Database: PFX

☐ Show Log Backups ☐ Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination Ty...
✓	Feb 22, 2022, 12:55:34 PM	00h 00m 27s	3.64 GB	Data Backup	File
✓	Feb 22, 2022, 12:09:22 PM	00h 00m 16s	5.94 GB	Data Backup	Snapshot
✓	Feb 21, 2022, 3:02:31 PM	00h 00m 19s	3.64 GB	Data Backup	File

Backup Details

ID: 1645534534230

Status: Successful

Backup Type: Data Backup

Destination Type: File

Started: Feb 22, 2022, 12:55:34 PM (UTC)

Finished: Feb 22, 2022, 12:56:01 PM (UTC)

Duration: 00h 00m 27s

Size: 3.64 GB

Throughput: 138.07 MB/s

System ID:

Comment: SnapCenter\_hana-1\_BlockIntegrityCheck\_Weekly\_02-22-2022\_12:55:18.7966

Additional Information: <ok>

Location: /backup/data/DB\_PFX/

Host	Service	Size	Name	Source Type	EBID
hana-1	indexserver	1.58 KB	SnapCenter_Snap...	topology	
hana-1	xsengine	80.00 MB	SnapCenter_Snap...	volume	
hana-1	indexserver	3.56 GB	SnapCenter_Snap...	volume	

Properties × Error Log

Property Value

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 では、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たバックアップパスが使用されます。

```

hana-1:~ # ls -al /backup/data/*
/backup/data/DB_PFX:
total 7665384
drwxr-xr-- 2 pfxadm sapsys      4096 Feb 22 12:56 .
drwxr-xr-x 4 pfxadm sapsys      4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys    155648 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys    83894272 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_2_1
-rw-r----- 1 pfxadm sapsys   3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_3_1
-rw-r----- 1 pfxadm sapsys      155648 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys    83894272 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_2_1
-rw-r----- 1 pfxadm sapsys   3825213440 Feb 22 12:56
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_3_1
/backup/data/SYSTEMDB:
total 7500880
drwxr-xr-- 2 pfxadm sapsys      4096 Feb 22 12:55 .
drwxr-xr-x 4 pfxadm sapsys      4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys    159744 Feb 21 15:01
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys   3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_1_1
-rw-r----- 1 pfxadm sapsys    159744 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys   3825213440 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_1_1
hana-1:~ #

```

## データボリューム以外のボリュームのバックアップ

非データボリュームのバックアップは、SnapCenter と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

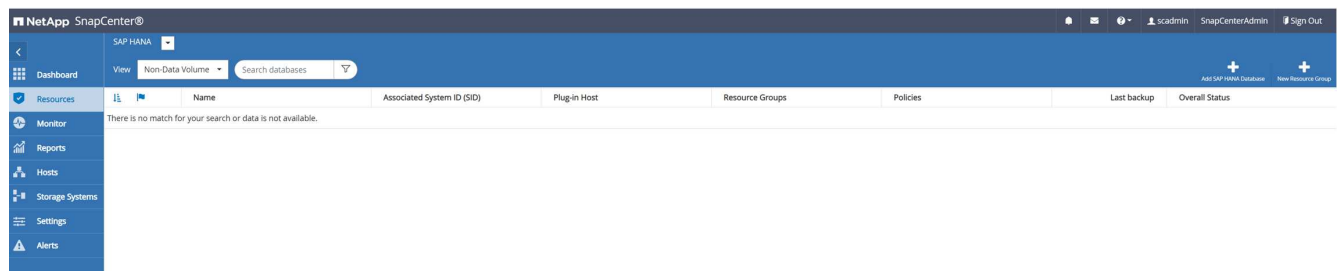
プを補うために、データボリューム以外のボリュームに対する追加のバックアップ戦略を開発することを推奨します。固有の要件に応じて、非データボリュームのバックアップはスケジュールの頻度と保持の設定が異なる場合があります。また、非データファイルを変更する頻度も考慮する必要があります。たとえば、HANA ボリューム「/hana/shared」には、実行可能ファイルと SAP HANA トレースファイルが格納されています。実行ファイルが変更されるのは SAP HANA データベースがアップグレードされた場合だけですが、SAP HANA の問題を分析するためには、SAP HANA のトレースファイルのバック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

データボリューム以外のリソースを設定するには、次の手順を実行します。

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。

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

Resource Type

Non-data Volume

Resource Name

PFX-Shared-Volume

Associated SID

PFX

Plug-In Host

hana-1

Previous

Next

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。

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Storage Footprint Details

Storage Type ☒ ONTAP

Add Storage Footprint

Storage System sapcc-hana-svm

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name

LUNs or Qtrees

PFX\_shared

Default is 'None' or type to find

Save

Previous

Next

4. 設定を保存するには、概要手順で[完了]をクリックします。

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Summary

Resource Type	Non-data Volume
Resource Name	PFX-Shared-Volume
Associated SID	PFX
Plug-in Host	hana-1

Storage Footprint

Storage System	Volume	LUN/Qtree
sapcc-hana-svm	PFX_shared	

Previous
Finish

これで、新しい非データボリュームがSnapCenter に追加されます。新しいリソースをダブルクリックして、リソースの保護を実行します。

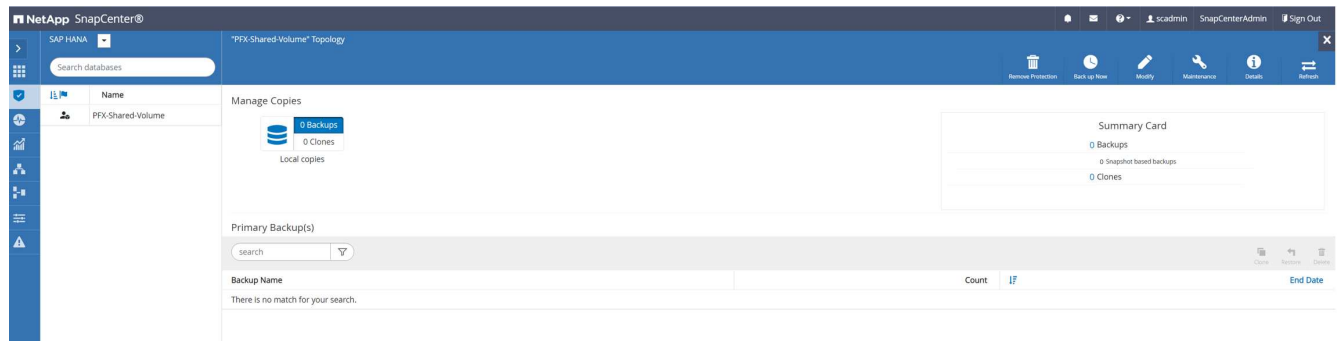
The screenshot shows the NetApp SnapCenter interface. On the left is a navigation sidebar with options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table of resources under the 'SAP HANA' view. The table has columns for Name, Associated System ID (SID), Plug-in Host, Resource Groups, Policies, Last backup, and Overall Status. One resource is listed: 'PFX-Shared-Volume' with SID 'PFX' and Plug-in Host 'hana-1'. The overall status is 'Not protected'. At the top right of the main area, there are buttons for 'Add SAP HANA Database' and 'New Resource Group'.

Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX-Shared-Volume	PFX	hana-1				Not protected

リソースの保護は、HANAデータベースのリソースで前述した方法と同じ方法で行われます。

5. [今すぐバックアップ]をクリックして、バックアップを実行できるようになりました。





6. ポリシーを選択し、バックアップ処理を開始します。

Backup

Create a backup for the selected resource

Resource Name

PFX-Shared-Volume

Policy

LocalSnap

Cancel

Backup

SnapCenter ジョブログには、個々のワークフロー手順が表示されます。

Job Details

Backup of Resource Group 'hana-1\_hana\_NonDataVolume\_PFX\_PFX-Shared-Volume' with policy 'LocalSnap'

▼ Backup of Resource Group 'hana-1\_hana\_NonDataVolume\_PFX\_PFX-Shared-Volume' with policy 'LocalSnap'

▼ hana-1

▼ Backup

▶ Validate Dataset Parameters

▶ Validate Plugin Parameters

▶ Validate Retention Settings

▶ Create Snapshot

▶ Get Snapshot Details

▶ Collect Autosupport data

▶ Register Backup and Apply Retention

▶ Register Snapshot attributes

▶ Data Collection

▶ Agent Finalize Workflow

Task Name: Backup Start Time: 02/22/2022 3:27:48 PM End Time:

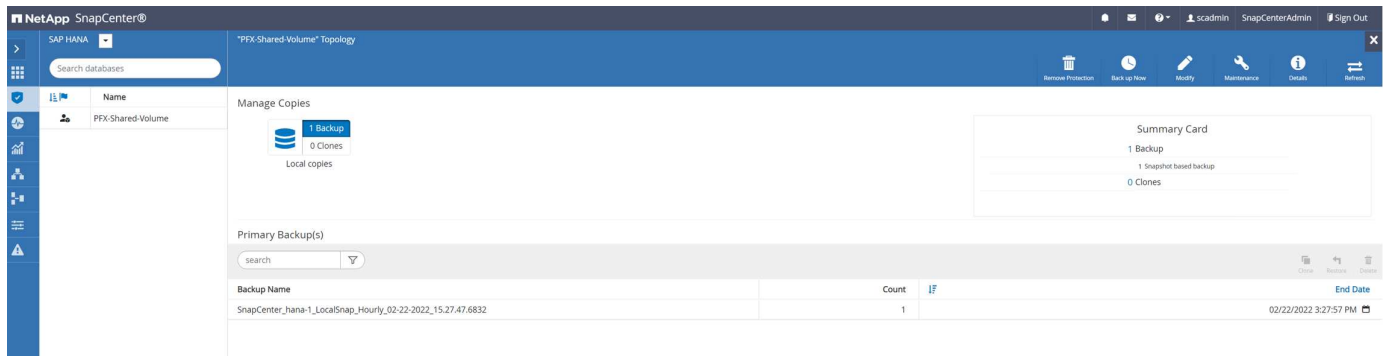
View Logs

Cancel Job

Close

これで、新しいバックアップがデータボリューム以外のリソースのリソースビューに表示されます。

44



## リストアとリカバリ

SnapCenter では、単一テナントのHANAシングルホストMDCシステムに対して自動リストア処理とリカバリ処理がサポートされます。複数のテナントを持つマルチホストシステムまたはMDCシステムの場合は、SnapCenter はリストア処理のみを実行し、手動でリカバリを実行する必要があります。

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。
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。
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。

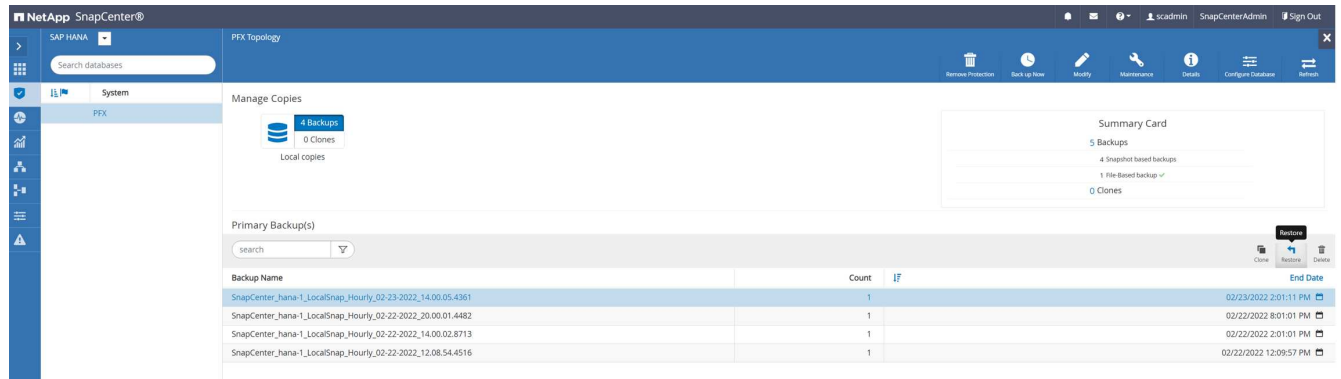
次に、SnapCenter は次の処理を実行します。

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に応じて、異なる処理が実行されます。
  - ボリューム復元が選択されている場合、SnapCenter は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SnapRestore を使用してボリュームを復元し、ボリュームをマウントします。
  - ボリュームリバートを選択しない場合、SnapCenter は、ストレージレイヤで単一ファイルのSnapRestore 処理を使用してすべてのファイルをリストアします。
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をリカバリする
  - b. テナントデータベースをリカバリします
  - c. HANAデータベースを起動しています

No Recoveryを選択すると、SnapCenter が終了し、システムとテナントデータベースのリストア処理を手動で実行する必要があります。

手動でリストアを実行するには、次の手順を実行します。

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。



2. リストアの範囲とタイプを選択します。

HANA MDC シングルテナント システムの標準的なシナリオは、ボリュームの復元を伴う完全なリソースを使用することです。複数のテナントを持つ HANA MDC システムの場合、1 つのテナントのみを復元する必要がある場合があります。単一テナントの復元の詳細については、以下を参照してください。"[リストアとリカバリ \(netapp.com\)](https://netapp.com)"。

Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ⓘ

☒ Volume Revert

⚠ As part of Complete Resource restore, if a resource contains volumes as Storage Footprint, then the latest Snapshot copies on such volumes will be deleted permanently. Also, if there are other resources hosted on the same volumes, then it will result in data loss for such resources.

☐ Tenant Database

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

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。

Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☒ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☐ No recovery

Specify log backup locations

Add

/backup/log

Specify backup catalog location

/backup/log

Recovery options are applicable to both system database and tenant database.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

4. オプションのリストア前のコマンドを入力します。

Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation ⓘ

Pre restore command

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#). ×

Previous

Next

5. オプションのリストア後のコマンドを入力します。

Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation ⓘ

Post restore command

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#) ×

Previous

Next

6. リストアおよびリカバリ操作を開始するには[完了]をクリックします



Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361
Backup date	02/23/2022 2:01:11 PM
Restore scope	Complete Resource with Volume Revert
Recovery scope	Recover to most recent state
Log backup locations	/backup/log
Backup catalog location	/backup/log
Pre restore command	
Post restore command	
Send email	No

If you want to send notifications for Restore Jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

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。

## Job Details



Restore 'hana-1\hana\MDC\PFX'

- ✓ ▼ Restore 'hana-1\hana\MDC\PFX'
- ✓ ▼ hana-1
  - ✓ ▼ Restore
    - ✓ ▶ Validate Plugin Parameters
    - ✓ ▼ Pre Restore Application
      - ✓ ▶ Stopping HANA instance
    - ✓ ▶ Filesystem Pre Restore
    - ✓ ▼ Restore Filesystem
    - ✓ ▶ Filesystem Post Restore
    - ✓ ▼ Recover Application
      - ✓ ▶ Recovering system database
      - ✓ ▶ Checking HDB services status
      - ✓ ▶ Recovering tenant database 'PFX'
      - ✓ ▶ Starting HANA instance
    - ✓ ▶ Clear Catalog on Server
    - ✓ ▶ Application Clean-Up
    - ✓ ▶ Data Collection
    - ✓ ▶ Agent Finalize Workflow

**i** Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:

View Logs

Cancel Job

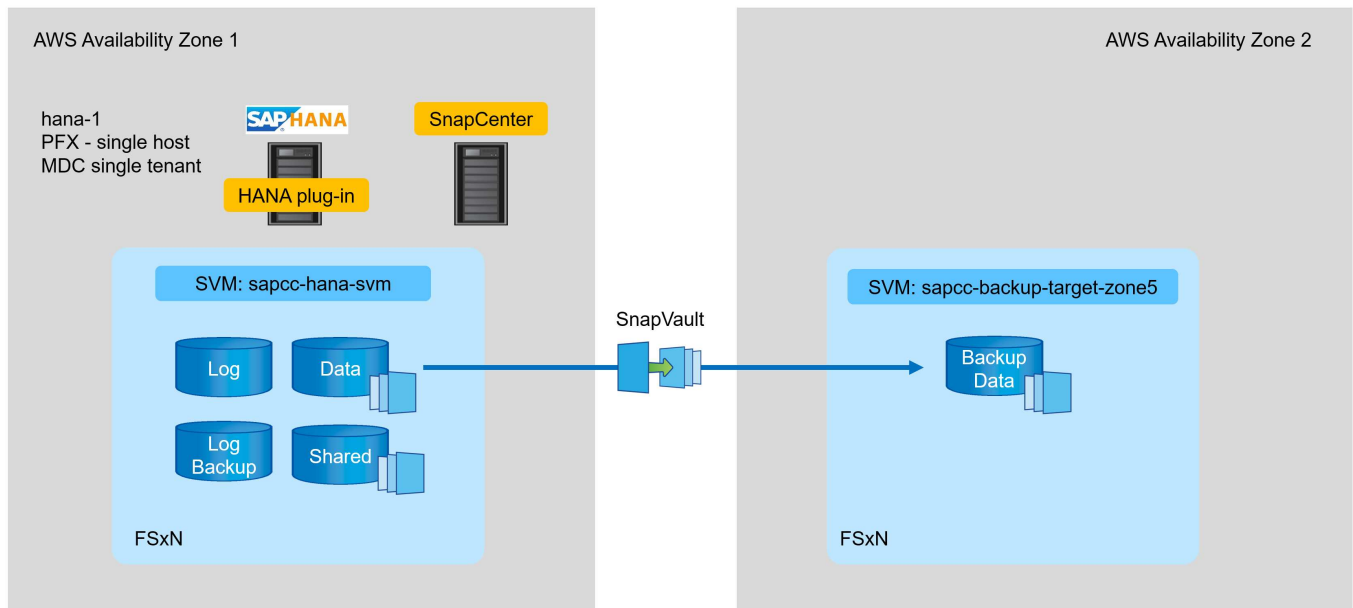
Close

# SnapVault を使用したバックアップレプリケーション

## 概要- SnapVault によるバックアップレプリケーション

このラボ環境では、2つ目のAWSアベイラビリティゾーンでFSX for ONTAP ファイルシステムを2つ目にして、HANAデータボリュームのバックアップレプリケーションを紹介します。

第章で説明したように、"「データ保護戦略」"レプリケーションターゲットは、プライマリFSx for ONTAPファイルシステムの障害から保護するために、別のアベイラビリティゾーンにある2つ目のFSx for ONTAPファイルシステムである必要があります。また、HANA共有ボリュームをONTAP ファイルシステムのセカンダリFSXにレプリケートする必要があります。



### 設定手順の概要

FSX for ONTAP レイヤで実行する必要がある設定手順はいくつかあります。これは、NetApp Cloud Manager またはONTAP コマンドラインのFSXで実行できます。

1. ONTAP ファイルシステム用のピアFSX。ONTAP ファイルシステムのFSXは、相互のレプリケーションを許可するためにピア関係を設定する必要があります。
2. SVMをピアリングSVM間のレプリケーションを許可するには、SVM間にピア関係を設定する必要があります。
3. ターゲットボリュームを作成します。ターゲットSVMにボリュームタイプ「DP」を指定してボリュームを作成します。レプリケーション・ターゲット・ボリュームとして使用するにはDPタイプが必要です。
4. SnapMirrorポリシーを作成する。これは' vaultタイプのレプリケーションのポリシーを作成するために使用されます。
  - a. ポリシーにルールを追加します。このルールには、セカンダリサイトでのバックアップのSnapMirrorラベルと保持に関する情報が含まれています。このラベルが含まれているソースボリュームにSnapCenter によってSnapshotバックアップが作成されるように、SnapCenter ポリシーの後半で同じSnapMirrorラベルを設定する必要があります。

5. SnapMirror関係を作成ソースボリュームとターゲットボリュームの間のレプリケーション関係を定義し、ポリシーを適用します。
6. SnapMirrorを初期化最初のレプリケーションが開始され、ソースのすべてのデータがターゲットボリュームに転送されます。

ボリュームレプリケーションの設定が完了したら、SnapCenter で次のようにバックアップレプリケーションを設定する必要があります。

1. ターゲットSVMをSnapCenter に追加します。
2. Snapshot/バックアップとSnapVault レプリケーション用に新しいSnapCenter ポリシーを作成します。
3. HANAのリソース保護にポリシーを追加します。
4. 新しいポリシーを使用してバックアップを実行できるようになりました。

以降の章では、個々の手順について詳しく説明します。

## ONTAP ファイルシステムのレプリケーション関係をFSXに設定します

SnapMirrorの設定オプションに関する追加情報 については、ONTAP のドキュメントを参照してください "[SnapMirrorレプリケーションのワークフロー \(netapp.com\)](https://netapp.com) "。

- ONTAP ファイルシステムのソースFSX : `FsxId00fa9e3c784b6abb`
- ソースSVM : 「sapcc-sana-svm
- ONTAP ファイル・システム用のターゲットFSX : FsxId05f7f00af49dc7a3e
- ターゲットSVM : sapcc-backup-target-zone5`

### ONTAP ファイルシステム用のピアFSX

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
      Logical      Status      Network      Current      Current
Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
----
FsxId00fa9e3c784b6abbb
      inter_1      up/up      10.1.1.57/24
FsxId00fa9e3c784b6abbb-01
                                     e0e
true
      inter_2      up/up      10.1.2.7/24
FsxId00fa9e3c784b6abbb-02
                                     e0e
true
2 entries were displayed.
```

```

FsxId05f7f00af49dc7a3e::> network interface show -role intercluster

```

Is	Logical	Status	Network	Current	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
----					
FsxId05f7f00af49dc7a3e	inter_1	up/up	10.1.2.144/24		
FsxId05f7f00af49dc7a3e-01					e0e
true					
	inter_2	up/up	10.1.2.69/24		
FsxId05f7f00af49dc7a3e-02					e0e
true					

2 entries were displayed.

```

FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-addr 10.1.1.57, 10.1.2.7
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command
in the other cluster.

```



「peer-addr」は、デスティネーションクラスタのクラスタIPです。

```

FsxId00fa9e3c784b6abbb:> cluster peer create -address-family ipv4 -peer
-addr 10.1.2.144, 10.1.2.69
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
FsxId00fa9e3c784b6abbb:>
FsxId00fa9e3c784b6abbb:> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
-----
FsxId05f7f00af49dc7a3e    1-80-000011          Available      ok

```

## SVMをピアリング

```

FsxId05f7f00af49dc7a3e:> vserver peer create -vserver sapcc-backup-
target-zone5 -peer-vserver sapcc-hana-svm -peer-cluster
FsxId00fa9e3c784b6abbb -applications snapmirror
Info: [Job 41] 'vserver peer create' job queued

```

```

FsxId00fa9e3c784b6abbb:> vserver peer accept -vserver sapcc-hana-svm
-peer-vserver sapcc-backup-target-zone5
Info: [Job 960] 'vserver peer accept' job queued

```

```

FsxId05f7f00af49dc7a3e:> vserver peer show
Peer Peer Peering
Remote
Vserver Vserver State Peer Cluster Applications
Vserver
-----
sapcc-backup-target-zone5
peer-source-cluster
peered FsxId00fa9e3c784b6abbb
snapmirror
sapcc-hana-svm

```

ターゲットボリュームを作成します

レプリケーションターゲットとしてフラグを設定するには、「dp」タイプのターゲットボリュームを作成する必要があります。

```
FsxId05f7f00af49dc7a3e::> volume create -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -aggregate aggr1 -size 100GB -state online
-policy default -type DP -autosize-mode grow_shrink -snapshot-policy none
-foreground true -tiering-policy all -anti-ransomware-state disabled
[Job 42] Job succeeded: Successful
```

### SnapMirror ポリシーを作成する

SnapMirrorポリシーと追加ルールで保持とSnapMirrorラベルを定義し、レプリケートするSnapshotを特定します。あとでSnapCenter ポリシーを作成するときは、同じラベルを使用する必要があります。

```
FsxId05f7f00af49dc7a3e::> snapmirror policy create -policy snapcenter-
policy -tries 8 -transfer-priority normal -ignore-atime false -restart
always -type vault -vserver sapcc-backup-target-zone5
```

```
FsxId05f7f00af49dc7a3e::> snapmirror policy add-rule -vserver sapcc-
backup-target-zone5 -policy snapcenter-policy -snapmirror-label
snapcenter -keep 14
```

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
Policy Number          Transfer
Name      Name          Type    Of Rules Tries Priority Comment
-----
FsxId00fa9e3c784b6abbb
      snapcenter-policy vault          1      8  normal  -
      SnapMirror Label: snapcenter                                Keep:      14
                                                                Total Keep: 14
```

### SnapMirror関係を作成

これで、ソースボリュームとターゲットボリュームの関係に加え、XDPタイプと前の手順で作成したポリシーが定義されます。

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-
svm:PFX_data_mnt00001 -destination-path sapcc-backup-target-
zone5:PFX_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle
unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with
destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

## SnapMirrorを初期化

このコマンドを使用すると、最初のレプリケーションが開始されます。これは、ソースボリュームからターゲットボリュームへのすべてのデータのフル転送です。

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-
backup-target-zone5:PFX_data_mnt00001 -source-path sapcc-hana-
svm:PFX_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-
target-zone5:PFX_data_mnt00001".
```

レプリケーションのステータスは'snapmirror show'コマンドを使用して確認できます

```
FsxId05f7f00af49dc7a3e::> snapmirror show
```

Progress						
Source		Destination	Mirror	Relationship	Total	
Last						
Path	Type	Path	State	Status	Progress	Healthy
Updated						
-----						
-----						
sapcc-hana-svm:PFX_data_mnt00001						
	XDP	sapcc-backup-target-zone5:PFX_data_mnt00001				
			Uninitialized			
			Transferring	1009MB	true	
02/24 12:34:28						



```
FsxId05f7f00af49dc7a3e::> snapmirror show
```

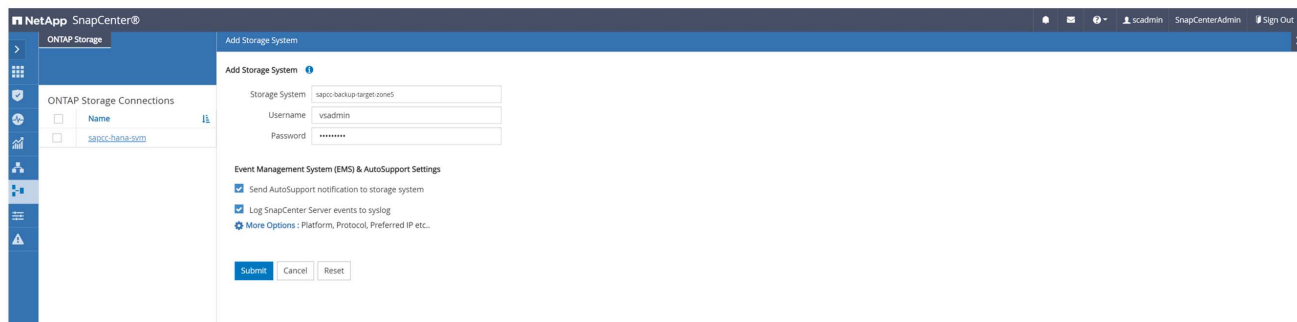
Progress

Source	Destination	Mirror	Relationship	Total		
Last						
Path	Type	Path	State	Status	Progress	Healthy
Updated						
-----						
-----						
sapcc-hana-svm:PFX_data_mnt00001						
	XDP	sapcc-backup-target-zone5:PFX_data_mnt00001				
		Snapmirrored				
			Idle		-	true -

## SnapCenter にバックアップSVMを追加

SnapCenter にバックアップSVMを追加するには、次の手順を実行します。

1. SnapVault ターゲットボリュームが配置されているSVMをSnapCenter に設定します。



2. [その他のオプション]ウィンドウで、プラットフォームとして[すべてのFlash FAS ]を選択し、[セカンダリ]を選択します。

More Options
×

Platform
All Flash FAS
Secondary
Protocol
HTTPS
Port
443
Timeout
60
seconds
☐ Preferred IP

Save
Cancel

これで、SVMをSnapCenter で使用できるようになります。

NetApp SnapCenter®
scadmin SnapCenterAdmin Sign Out

ONTAP Storage
Type: ONTAP SVMs Search by Name

ONTAP Storage Connections

	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	sapcc-backup-targetzone5	10.1.2.31		vsadmin	AFF	Not applicable
<input type="checkbox"/>	sapcc-hana-svm	198.19.255.9		vsadmin	AFF	✓

バックアップレプリケーション用の新しい**SnapCenter** ポリシーを作成します  
バックアップレプリケーションのポリシーは次のように設定する必要があります。

1. ポリシーの名前を指定します。

NetApp SnapCenter®
scadmin SnapCenterAdmin Sign Out

Global Settings Policies Users and Access Roles Credential Software

SAP HANA
Search by Name

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	

2. Snapshot/バックアップとスケジュール頻度を選択します。通常、Dailyはバックアップのレプリケーションに使用されます。

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name

LocalSnapAndSnapVault

Details

Replication to backup volume

3. Snapshotバックアップの保持期間を選択します。

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type

☒ Snapshot Based
 ☐ File-Based

Schedule Frequency

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

☐ On demand
 ☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

これは、プライマリストレージで作成された日単位のSnapshotバックアップの保持です。SnapVault ターゲットでのセカンダリバックアップの保持設定は、ONTAP レベルでadd ruleコマンドを使用してすでに設定されています。「ONTAP ファイルシステムのFSXでのレプリケーション関係の構成」(xref)を参照してください。

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

Daily retention settings

☒ Total Snapshot copies to keep
 

3

☐ Keep Snapshot copies for
 

14 days

4. Update SnapVault フィールドを選択し、カスタムラベルを指定します。

このラベルは、「add rule」コマンドでONTAP レベルで指定されたSnapMirrorラベルと一致する必要があります。

New SAP HANA Backup Policy

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Custom Label ⓘ

snapcenter

Error retry count: 3 ⓘ

New SAP HANA Backup Policy

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Summary

Policy name	LocalSnapAndSnapVault
Details	Replication to backup volume
Backup Type	Snapshot Based Backup
Schedule Type	Daily
Daily backup retention	Total backup copies to retain : 3
Replication	SnapVault enabled , Secondary policy label: Custom Label : snapcenter , Error retry count: 3

これで新しいSnapCenter ポリシーが設定されました。

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

SAP HANA

Search by Name

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault

リソースの保護にポリシーを追加します

次の図に示すように、新しいポリシーをHANAのリソース保護構成に追加する必要があります。

NetApp SnapCenter®

SAP HANA PFX Topology Multitenant Database Container - Protect

Search databases

System PFX

Manage Copies Primary Backup(s)

search

Backup Name

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-24-2022\_14.00.03.6698

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-24-2022\_08.00.02.2808

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-24-2022\_02.00.02.1758

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_20.00.02.3280

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-22-2022\_20.00.01.4482

SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-22-2022\_14.00.02.8713

1 Resource 2 Application Settings 3 Policies 4 Notification 5 Summary

Select one or more policies and configure schedules

LocalSnap, BlockIntegrityCheck + ⓘ

LocalSnap

BlockIntegrityCheck

LocalSnapAndSnapVault

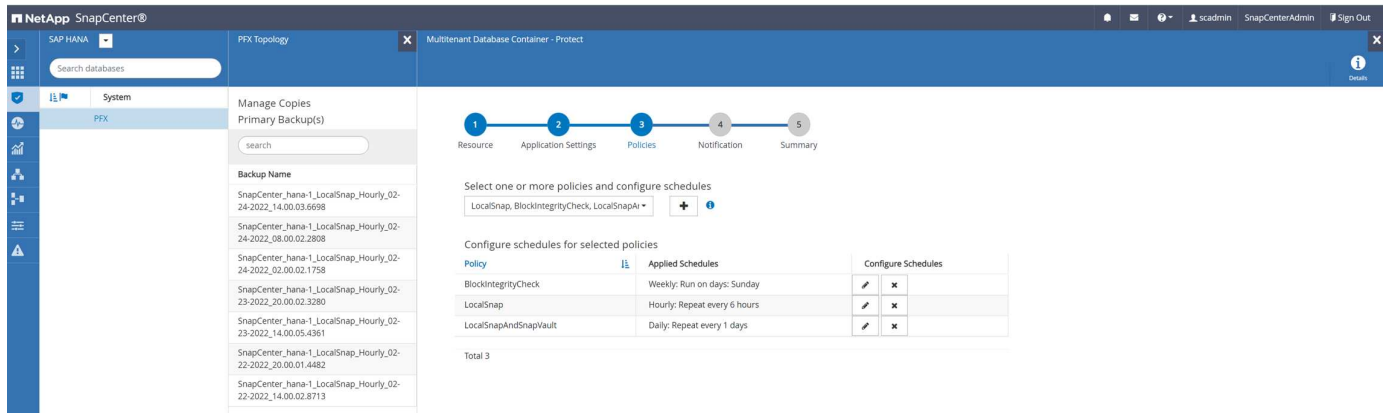
BlockIntegrityCheck Weekly: Run on days: Sunday

LocalSnap Hourly: Repeat every 6 hours

Configure Schedules

Total 2

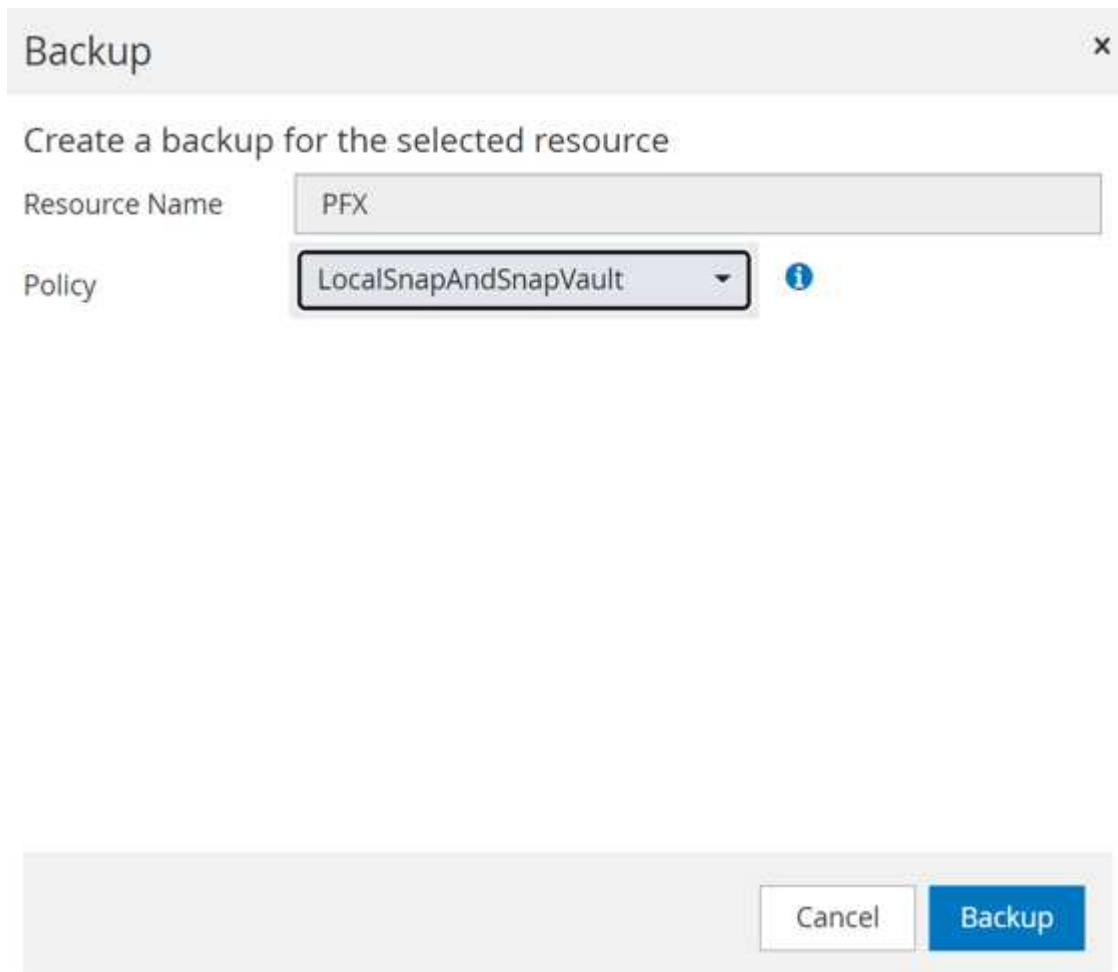
セットアップでは、日次スケジュールを定義します。



レプリケーションを使用してバックアップを作成します

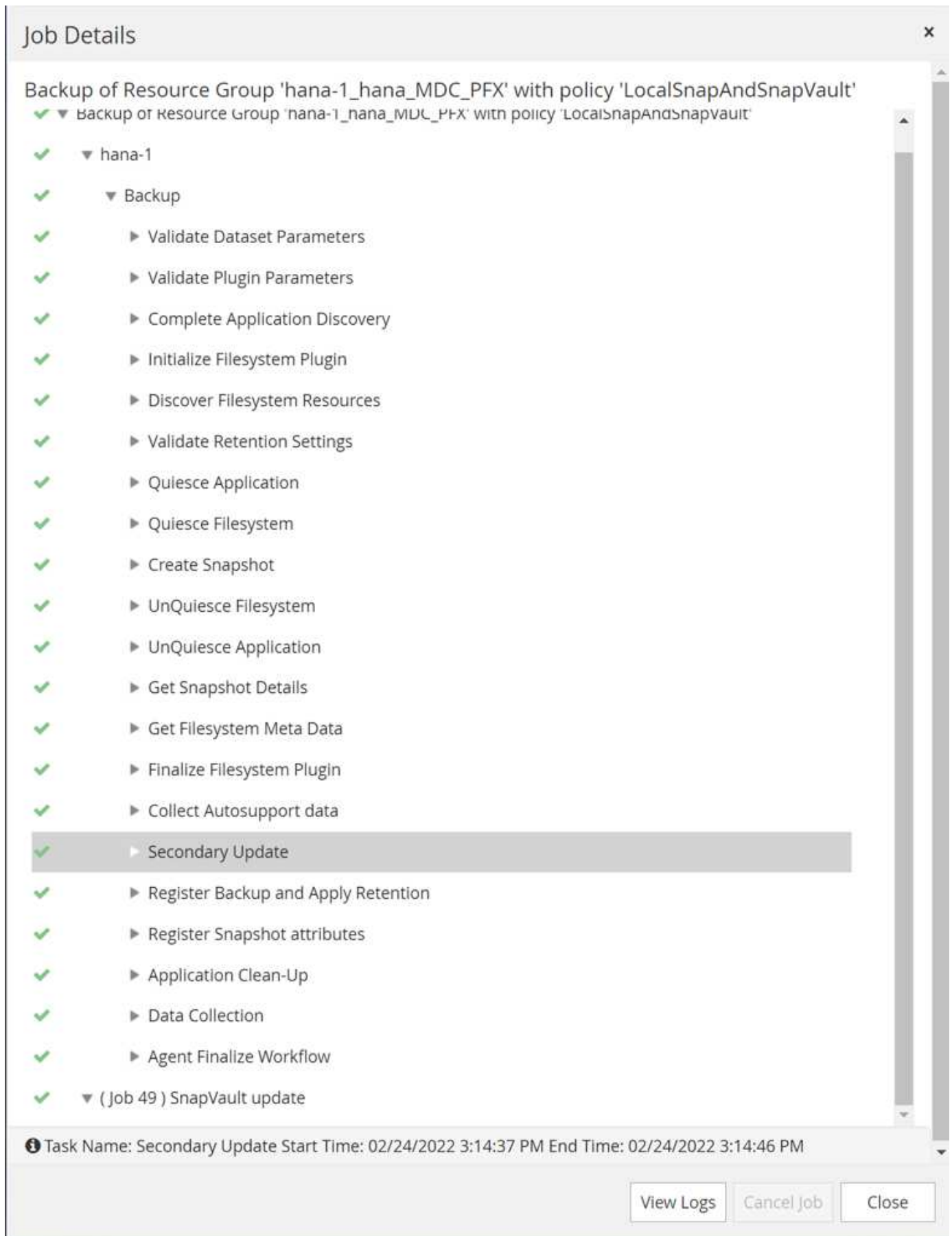
バックアップは、ローカルSnapshotコピーと同じ方法で作成します。

レプリケーションを伴うバックアップを作成するには、バックアップレプリケーションを含むポリシーを選択し、バックアップをクリックします。



SnapCenter ジョブログには、SnapVault 更新処理を開始するセカンダリアップデートステップが表示されま

す。レプリケーションによって変更されたブロックがソースボリュームからターゲットボリュームにレプリケートされます。



ONTAP ファイル・システムのFSXでは、SnapCenter ポリシーで設定されているように、SnapMirrorラベ

ル「SnapCenter」を使用してソース・ボリューム上のSnapshotが作成されます。

```
FsxId00fa9e3c784b6abbb::> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver          volume          snapshot
snapmirror-label
-----
-----
-----
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_13.10.26.5482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_14.00.05.2023 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_08.00.06.3380 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_14.00.01.6482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-14-
2022_20.00.05.0316 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_08.00.06.3629 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_14.00.01.7275 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853

snapcenter
8 entries were displayed.
```

ターゲットボリュームに、同じ名前のSnapshotコピーが作成されます。

```
FsxId05f7f00af49dc7a3e::> snapshot show -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -fields snapmirror-label
vserver          volume          snapshot
snapmirror-label
-----
-----
-----
sapcc-backup-target-zone5 PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 snapcenter
FsxId05f7f00af49dc7a3e::>
```

HANAのバックアップカタログにも新しいSnapshotバックアップが表示されます。



Backup Catalog						Backup Details					
Database: SYSTEMDB						ID: 1651162926424					
<input type="checkbox"/> Show Log Backups <input type="checkbox"/> Show Delta Backups						Status: Successful					
Status	Started	Duration	Size	Backup Type	Destination Ty...	Destination Type:	Started:	Finished:	Duration:	Size:	Throughput:
✓	Apr 28, 2022, 4:22:06 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Snapshot	Apr 28, 2022, 4:22:06 PM (UTC)	Apr 28, 2022, 4:22:21 PM (UTC)	00h 00m 15s	5.50 GB	n.a.
✓	Apr 28, 2022, 2:00:26 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Apr 28, 2022, 8:00:35 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Apr 15, 2022, 5:00:44 PM	00h 06m 59s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Apr 14, 2022, 8:00:32 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Apr 5, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Apr 5, 2022, 8:00:39 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Mar 31, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Mar 31, 2022, 1:10:57 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot	Snapshot					
✓	Feb 22, 2022, 12:55:21 PM	00h 00m 21s	3.56 GB	Data Backup	File	File					
						System ID: SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853					
						Additional Information: <ok>					
						Location: /hana/data/PFX/mnt00001/					
Host	Service	Size	Name	Source Type	EBID						
hana-1	nameserver	5.50 GB	hdb00001	volume	SnapCent...						

SnapCenterでは、トポロジビューのバックアップコピーをクリックして、レプリケートされたバックアップのリストを表示できます。

セカンダリストレージからリストアおよびリカバリする

セカンダリストレージから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。

セカンダリストレージ上のすべてのバックアップのリストを取得するには、SnapCenter トポロジビューでVault Copies（ヴォールトコピー）をクリックし、バックアップを選択してRestore（復元）をクリックします。

リストアダイアログにセカンダリの場所が表示されます。

Restore from SnapCenter\_hana-1\_LocalSnapAndSnapVault\_Daily\_04-28-2022\_16.21.41.5853 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ?

☐ Tenant Database

Choose archive location

sapcc-hana-svm:PFX\_data\_mnt00001

sapcc-backup-target-zone5:PFX\_data\_mnt00 ▼

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation. ×

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#) ×

Previous

Next

さらに、リストアとリカバリの手順は、プライマリストレージにあるSnapshotバックアップでこれまで説明されていた手順と同じです。

## 追加情報の参照先

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。

- 『FSX for NetApp ONTAP user guide—What is Amazon FSX for NetApp ONTAP ?』

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

- SnapCenter のリソースページ

["https://www.netapp.com/us/documentation/snapcenter-software.aspx"](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"](https://docs.netapp.com/us-en/snapcenter/index.html)

- TR-4667 : 『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』

["SnapCenter を使用して SAP HANA システムのコピーおよびクローン処理を自動化"](#)

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

["SnapCenterによるバックアップとリカバリ"](#)

## 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	2022年5月	初版リリース

## 著作権に関する情報

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

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

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

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

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

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

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。